INFOSEC Skills™

Course Catalog

Skill development and certification training

Updated February 2024

INFOSEC Skills

Table of contents

INFOSEC Skills

Customize your training experience.

Choose how, when, and where you learn.

Technical training is often more than a development goal — it is a business requirement.

At Infosec, we recognize that your learning journey is unique. Whether you seek to pass your certification exam swiftly or explore a range of cybersecurity topics at your preferred pace, we provide flexible training options that align with your team's commitments and training requirements.

Infosec Boot Camps

Infosec Boot Camps offer in-person and online **live, interactive** cybersecurity and IT certification training, led by industry experts with 10+ years of experience. Gain exam readiness and ask questions in a conducive environment. You can access on-demand resources on Infosec Skills for enhanced domain knowledge and hands-on experience.

Exam Pass Guarantee*: Don't pass the exam on the first try? Get a second attempt free.

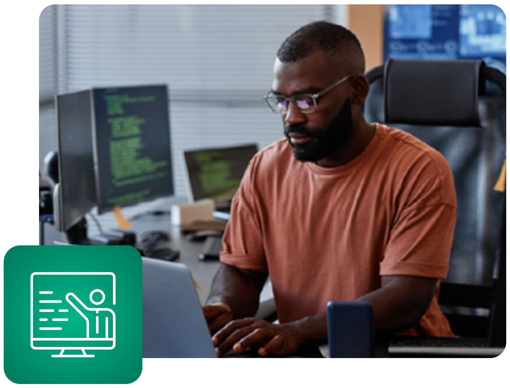
100% Satisfaction Guarantee: Not 100% satisfied at the end of day one? You may enroll in a different online or in-person course.

Knowledge Transfer Guarantee: If an employee leaves within 3 months of obtaining certification, we provide tuition-free training for another employee.

** Does not apply to CMMC-AB boot camps*

Infosec Skills Self-paced Training

Infosec Skills Self-paced Training is engineered to accommodate your busy schedule while providing a high-quality learning experience. With open enrollment, you have the **freedom to start training whenever** it suits you. Complete your training and obtain your certification at your own pace with extended course access.



Certification-focus: On-demand course materials can be accessed anytime, anywhere.

Exam voucher included: An easy way to redeem your voucher and take the exam.

Expert support: Asynchronous instructor assistance and a dedicated student advisory team give you the guidance you need to pass the exam.

Take control of your cybersecurity education and advance your skills at your own pace.

Learn more about certification training with Infosec

INFOSEC Skills

Infosec Skills

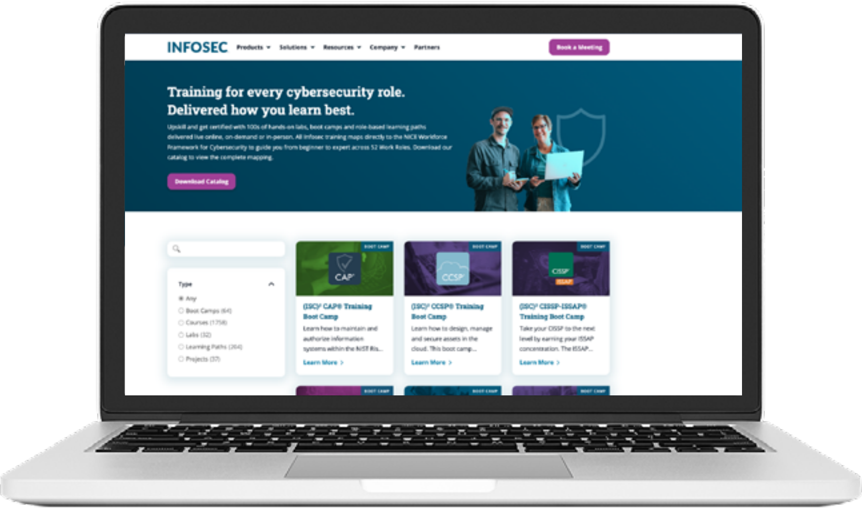
Infosec Skills provides unlimited access to an extensive library of on-demand cybersecurity training, covering every security role from beginner to advanced. Assign pre-built learning plans or customize your own to ensure training is relevant and impactful and build confidence in your team's technical skills and knowledge.

Extensive coverage: Training is mapped to industry standards like the NICE Workforce Framework for Cybersecurity, MITRE ATT&CK® Matrix and DoD 8570/8140, as well as Infosec Skills Roles for pre-built role-based training.

Guided hands-on labs: Practice through hands-on experience and real-world scenarios to accelerate skills development and enhance knowledge retention.

Measurable progress: Assess knowledge and skills to pinpoint gaps and training needs, then measure progress with team reporting.

Start your learning journey with Infosec



Training for every cybersecurity role.
Delivered how you learn best.

Upskill and get certified with 100s of hands-on labs, boot camps and role-based learning paths delivered live online, on-demand or in-person. All Infosec training maps directly to the NICE Workforce Framework for Cybersecurity to guide you from beginner to expert across 52 Work Roles. Download our catalog to view the complete mapping.

● Any
○ Boot Camps (64)
○ Courses (1758)
○ Labs (32)
○ Learning Paths (204)
○ Projects (37)

(ISC)² CAP® Training Boot Camp
Learn how to maintain and authorize information systems within the NIST Ris...

(ISC)² CCSP® Training Boot Camp
Learn how to design, manage and secure assets in the cloud. This boot camp...

(ISC)² CISSP-ISSAP® Training Boot Camp
Take your CISSP to the next level by earning your ISSAP concentration. The ISSAP...

Try Infosec Skills for $1!

Use code "**learnskills**" when you sign up to get your first month for $1 — or start a trial for for your whole team.

Information security boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

Ethical Hacking Dual Cert

5-day boot camp

Discover vulnerabilities before the bad guys do! Our most popular information security and hacking training goes in-depth into the techniques used by malicious, black-hat hackers with attention-getting lectures and hands-on labs. Certification training for CEH and PenTest+.

Advanced Ethical Hacking

5-day boot camp

Take your penetration testing skills to a new level! The industry's most advanced ethical hacking training teaches you how to orchestrate and defend against advanced persistent threats (APT) attacks. Certification training for CPT and CEPT.

Penetration Testing 10-Day

10-day boot camp

Infosec's penetration testing training — delivered in the form of a 10-day, boot-camp style course — is the information security industry's most comprehensive penetration testing course available. Certification training for CEH, PenTest+, CPT and CEPT.

Mobile and Web Application Penetration Testing

5-day boot camp

Learn how to conduct penetration tests on mobile and web applications! This boot camp goes in-depth into the tools and techniques used to exploit and defend web and mobile apps with a combination of hands-on labs and expert instruction. Certification prep for CMWAPT.

Cloud Penetration Testing

5-day boot camp

Learn how to conduct penetration tests on cloud services and applications! This boot camp goes in-depth into the tools and techniques used to exploit and defend cloud infrastructure components with a combination of hands-on labs and expert instruction. Certification training for CCPT.

Red Team Operations Training

5-day boot camp

Do good by being bad in this exclusive Red Team Operations training designed to teach you to think like a cybercriminal, help you better defend your organization, and prepare you for the Certified Red Team Operations Professional exam.

Cyber Threat Hunting

3-day boot camp

Learn how to find, assess and remove threats from your organization in our Cyber Threat Hunting Boot Camp designed to prepare you for the Certified Cyber Threat Hunting Professional exam.

Incident Response and Networking Forensics

5-day boot camp

Learn how to detect and respond to security incidents! This popular boot camp builds your knowledge around network forensics and incident response with hands-on labs and expert instruction.

Computer Forensics

5-day boot camp

Learn how to investigate cybercrime! This boot camp goes in-depth into the tools, techniques and processes used by forensics examiners to find and extract evidence from computers. Certification training for CCFE.

Mobile Forensics

2-day boot camp

Learn how to use mobile forensics to investigate cybercrime! Our Mobile Forensics Boot Camp builds your skills in a hands-on lab environment so you can apply what you learned the day you leave training. Certification training for CMFE.

Computer and Mobile Forensics

7-day boot camp

Learn how to investigate cybercrime! This popular boot camp goes in-depth into the tools, techniques and processes used by forensics examiners to find and extract evidence from computers and mobile devices. Certification training for CCFE and CMFE.

Data Recovery

5-day boot camp

Learn how to recover sensitive data from damaged or partially destroyed hard drives, solid-state media and removable media! A combination of hands-on labs and expert instruction builds your knowledge around data recovery and prepares you to become a Certified Data Recovery Professional (CDRP).

Reverse Engineering Malware

5-day boot camp

Learn how to reverse engineer and analyze malware! Reverse engineering is a vitally important skill for today's expert security professional. Keep your organization safe by digging into the viruses, Trojans and rootkits being used by cybercriminals. Certification training for CREA.

OT/ICS Certified Security Professional (ICSP)

5-day boot camp

Learn the best practices for securing Operational Technologies (OT) including Industrial Control Systems (ICS) and SCADA networks. This boot camp teaches you how to defend against both internal and external attackers to provide holistic security for critical industrial automation systems.

NIST Cybersecurity Framework

3-day boot camp

This three-day boot camp teaches you how to employ the NIST Cybersecurity Framework in order to better manage and reduce your organization's cybersecurity risk.

CSIS Top 20 Critical Security Controls

5-day boot camp

This boot camp helps you master the 20 Important Security Controls as published by the Center for Strategic and International Studies (CSIS).

DOD Risk Management Framework

4-day boot camp

Infosec's Risk Management Framework (RMF) Boot Camp is a four-day course in which you delve into the IT system authorization process and gain an understanding of the Risk Management Framework.

NERC Critical Infrastructure Protection

5-day boot camp

This five-day boot camp provides a detailed overview of and teaches how to comply with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards.

Cybersecurity Foundations

3-day boot camp

Learn topics ranging from foundational security concepts and principles to specific topics like common security tools and technologies, key security roles, common attack types, and best practice security controls or mitigation strategies. A comprehensive but beginner-friendly training for those looking to get started or expand their cybersecurity expertise.

EC-Council's Certified Network Defender

5-day boot camp

Learn to defend your organization's network in five days! This course will cover network defense techniques, incident response strategies, network perimeter and data protection.

AWS certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

AWS Certified Solutions Architect Training Boot Camp

3-day boot camp

Utilize AWS services and frameworks to create architectures! This course will cover the fundamentals of AWS architectural principles, including AWS Command Line Interface (CLI) and Virtual Private Cloud (VPC) subsets.

AWS Certified Security Engineer Training Boot Camp

3-day boot camp

Learn to mitigate threats and secure AWS Cloud services! With this course, you will understand AWS incident response, security and monitoring.

AWS Certified Cloud Operations Administrator Training Boot Camp

3-day boot camp

Implement and operate AWS security systems! This course will cover the basics of cloud networking concepts, cloud architectural requirements, monitoring, logging and troubleshooting systems.

AWS Certified DevOps Engineer Training Boot Camp

3-day boot camp

Learn to design and implement AWS infrastructure! This course will cover software development and infrastructure within AWS systems, including Git repositories and CI/CD pipelines.

ISC2 certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

CISSP

7-day boot camp

Take your career to the next level by earning one of the most in-demand security certifications. Infosec's Certified Information Systems Security Professional (CISSP) training is more than just a live boot camp. You'll get everything you need to successfully prepare for, earn and maintain your CISSP certification.

CGRC (previously - CAP)

3-day boot camp

Learn how to maintain and authorize information systems within the NIST Risk Management Framework (RMF). You'll leave this boot camp with the knowledge and domain expertise needed to pass the Certified in Governance, Risk and Compliance (CGRC) exam the first time you take it.

CCSP

5-day boot camp

Learn how to design, manage and secure assets in the cloud. This boot camp teaches you best practices around cloud data, applications and infrastructure — and prepares you to become a Certified Cloud Security Practitioner (CCSP).

CSSLP

5-day boot camp

Become a Certified Secure Software Lifecycle Professional (CSSLP). You'll leave this boot camp with the knowledge and domain expertise needed to pass the CSSLP exam the first time you take it.

ISSAP

4-day boot camp

Take your CISSP to the next level by earning your ISSAP concentration. The ISSAP builds on your CISSP knowledge and validates your expertise in developing, designing and analyzing security solutions.

ISSEP

4-day boot camp

Take your CISSP to the next level by earning your ISSEP concentration. The ISSEP builds on your CISSP knowledge and validates your ability to practically apply systems engineering principles and processes to develop secure systems.

ISSMP

4-day boot camp

Take your CISSP to the next level by earning your ISSMP concentration. The ISSMP builds on your CISSP knowledge and validates your expertise in establishing, presenting and governing information security programs.

CompTIA certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

A+

5-day boot camp

Don't be afraid, beginners! This entry-level boot camp provides the most comprehensive approach to earning your CompTIA A+ certification. A+ certification leads to career advancement, personal improvement, skills enhancement and higher salaries.

Network+

5-day boot camp

Learn how to configure, troubleshoot and oversee networks! This boot camp provides the most comprehensive approach to earning your CompTIA Network+ certification, one of the most popular certifications an IT professional can attain.

Security+

5-day boot camp

Infosec's authorized CompTIA Security+ Boot Camp teaches you information security theory and reinforces that theory with hands-on exercises to help you learn by doing. You will learn how to configure and operate many different technical security controls — and leave prepared to pass your Security+ exam.

CySA+

5-day boot camp

Learn how to use behavioral analytics to prevent, detect and combat cyber threats! This boot camp provides the most comprehensive approach to earning CompTIA's intermediate-level Cybersecurity Analyst (CySA+) certification.

Ethical Hacking Dual Cert

5-day boot camp

Discover vulnerabilities before the bad guys do! Our most popular information security and hacking training goes in-depth into the techniques used by malicious, black-hat hackers with attention-getting lectures and hands-on labs. Certification training for CEH and PenTest+.

CASP+

5-day boot camp

Take your cybersecurity skills to the next level by becoming a CompTIA Advanced Security Practitioner (CASP+). You'll learn the "how to" of implementing cybersecurity solutions and leave with one of the industries most respected certifications.

Linux+

5-day boot camp

Infosec's authorized CompTIA Linux+ Boot Camp is a hands-on training covering every important facet of the world's most popular open source operating system. You'll learn hardware and system configuration, system maintenance, troubleshooting and diagnostics, security, scripting and more.

Cloud+

5-day boot camp

Adopting a vendor-neutral approach, this course provides you with an understanding of essential cloud concepts needed to start or advance your career working with cloud technologies. You'll have the knowledge required to pass your Cloud+ exam, the only cloud-focused certification approved for DoD 8570.01-M.

Data+

5-day boot camp

With data playing an ever-increasing role in today's business and technology landscape, the demand for skilled data professionals is higher than ever. Upon completion of this course, you'll have the knowledge needed to pass the CompTIA Data+ exam as well as valuable data skills for nearly any industry or role.

ISACA certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

CISA

5-day boot camp

Infosec's Certified Information Systems Auditor (CISA) Boot Camp is a five-day training focused on preparing you for the ISACA CISA exam. You'll leave with the knowledge and domain expertise needed to pass the CISA exam the first time you take it.

CISM

5-day boot camp

Infosec's Certified Information Security Manager (CISM) Boot Camp is a five-day training focused on preparing you for the ISACA CISM exam. You'll leave with the knowledge and domain expertise needed to pass the CISM exam the first time you take it.

CRISC

3-day boot camp

Learn the principles and practices of IT governance. Build your knowledge around how IT risk relates to your organization and prepare to earn your Certified in Risk and Information Systems Control (CRISC) certification.

CGEIT

4-day boot camp

Infosec's Certified in the Governance of Enterprise IT (CGEIT) Boot Camp is a four-day training focused on preparing you for the ISACA CGEIT exam. You'll leave with the knowledge and domain expertise needed to pass the CGEIT exam the first time you take it.

CDPSE

5-day boot camp

Infosec's Certified Data and Privacy Solutions Engineer (CDPSE) Boot Camp offers a natural progression for IT professionals who are tasked with designing, implementing and managing the technology that stores, collects and transports PII, as well as ensuring that privacy is considered in the design.

COBIT 2019 Foundation

3-day boot camp

Take the first step toward strategic roles in GRC and IT governance with the Control Objectives for Information and Related Technology (COBIT) framework! Plus, the knowledge and skills gained through a deeper understanding of the COBIT framework will prepare you for the COBIT Foundation Certificate exam.

Implementing the NIST CSF Using COBIT 2019

2-day boot camp

Build on your expertise in not just understanding NIST and COBIT® 2019, but also in implementing the globally accepted frameworks together. Gain the know-how to integrate cybersecurity standards and enterprise governance of Information & technology (EGIT).

COBIT 2019 Design and Implementation

4-day boot camp

Build on your expertise in not just understanding COBIT®, but also in implementing the globally accepted framework to maximize the value of enterprise information and technology. Gain the know-how to design and implement an effective IT governance system and run governance improvement programs.

CMMC certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

Certified CMMC 2.0 Professional Boot Camp

5-day boot camp

The Certified CMMC 2.0 Professional (CCP) is the first step to becoming an assessor. It certifies you as a valuable resource for consulting agencies and organizations seeking CMMC guidance.

Certified CMMC 2.0 Assessor Boot Camp

5-day boot camp

Take your career to the next level by becoming one of the first Certified CMMC Assessors (CCA). The CMMC career path contains three levels of assessors based on the different maturity levels.

IAPP certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

CIPP/US

2-day boot camp

Infosec's two-day authorized CIPP/US boot camp provides privacy professionals with essential knowledge and understanding of important U.S. laws, regulations and enforcement models.

CIPP/E

2-day boot camp

Infosec's two-day authorized CIPP/E boot camp provides privacy professionals with essential knowledge and understanding of important European Union laws, regulations and enforcement models.

CIPM

2-day boot camp

Infosec's two-day authorized CIPM boot camp focuses on the development, implementation and management of privacy policies and frameworks.

CIPT

2-day boot camp

Infosec's two-day authorized CIPT boot camp helps you gain a deep understanding of the need of privacy in the IT environment and the common challenges enterprises are facing when factoring data privacy into their products and services.

CIPP/US and CIPT

4-day boot camp

Infosec's four-day authorized CIPP/US and CIPT boot camp provides privacy professionals with essential knowledge and understanding of both important U.S. laws, regulations and enforcement models as well as the common challenges enterprises are facing when factoring data privacy into their products and services.

CIPP/US and CIPM

4-day boot camp

Infosec's four-day authorized CIPP/US and CIPM boot camp provides privacy professionals with both essential knowledge and understanding of important U.S. laws, regulations and enforcement models as well as information on the development, implementation and management of privacy policies and frameworks.

CIPP/US, CIPT and CIPM

6-day boot camp

Infosec's six-day authorized CIPP/US, CIPT and CIPM boot camp provides privacy professionals with the essential knowledge and understanding of U.S. privacy laws, technology concerns, and privacy policies and frameworks necessary to successfully pass all three certification exams.

Cisco certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

CCNA Dual Cert

7-day boot camp

Infosec's authorized CCNA Dual Certification Boot Camp helps you build your knowledge of networking and provides hands-on experience installing, configuring and operating network devices — all while preparing you to earn two Cisco certifications.

CCNA

5-day boot camp

Infosec's authorized CCNA Boot Camp helps you build your knowledge of networking and provides hands-on experience installing, configuring and operating network devices.

Cisco Certified CyberOps Associate

2-day boot camp

Infosec's authorized Cisco Certified CyberOps Associate Boot Camp is an intense two-day training designed to build a foundation of skills around cybersecurity operations. You will acquire the skills necessary to begin a career working with associate-level cybersecurity analysts within a security operations center (SOC).

CCNP Enterprise

10-day boot camp

Take your networking professional career to the next level! Infosec's authorized CCNP Enterprise Boot Camp is a comprehensive 10-day training that prepares you to earn one of Cisco's most prestigious certifications.

Microsoft certification boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

Microsoft Azure Dual Cert

7-day boot camp

Learn how to implement, monitor, maintain and secure Microsoft Azure solutions! This boot camp provides hands-on experience and prepares you to earn two Microsoft certifications: Azure Administrator Associate and Azure Security Engineer Associate.

Microsoft Azure Administrator Training Boot Camp

4-day boot camp

Learn how to implement, monitor, maintain and secure Microsoft Azure solutions! This boot camp provides hands-on experience and prepares you to earn your Microsoft Azure Administrator certification.

Microsoft Azure Administering Windows Server Hybrid Core Infrastructure Boot Camp

4-day boot camp

Learn how to implement and manage on-premises and hybrid solutions such as identity, management, computer, networking and storage in a Windows Server hybrid environment! This boot camp provides hands-on experience and prepares you to earn your Microsoft Azure AZ-800 certification.

Microsoft Azure Configuring Windows Server Hybrid Advanced Services Boot Camp

4-day boot camp

Learn how to configure advanced Windows Server services using on-premises, hybrid and cloud technologies! This boot camp provides hands-on experience and prepares you to earn your Microsoft Azure AZ-801 certification.

Microsoft Azure Fundamentals Training Boot Camp

1-day boot camp

This course helps new and established IT professionals learn the key concepts, components and benefits of cloud computing with Microsoft Azure.

Secure coding boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

Secure Coding for C/C++

2-day boot camp

Learn the most common programming bugs and their practical mitigation techniques through hands-on exercises that provide full understanding of the root causes of security problems.

Secure Coding for Java

3-day boot camp

Learn how to develop Secure Java applications. This boot camp is designed for developers and designers of Java applications that require effective, real-world secure programming skills they can implement immediately at the workplace.

Secure Coding in PHP

3-day boot camp

Learn how to make PHP applications resistant to attacks from security issues around JavaScript, Ajax and HTML5. This boot camp is designed for PHP developers that require effective, real-world, secure programming skills they can implement immediately at the workplace.

Secure Coding for .NET Training

3-day boot camp

Learn how to develop Secure .NET applications. This boot camp is designed for ASP.NET and C# developers that require effective, real-world, secure programming skills they can implement immediately at the workplace.

Other boot camps

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on courses and cyber ranges to help you advance your skills before, during and after your boot camp.

Project Management Professional (PMP)

4-day boot camp

Infosec's Project Management Professional (PMP) Boot Camp provides a quick and convenient approach to PMP certification. You'll gain the knowledge needed to pass the PMP exam and the project management education hours required for certification all in one boot camp.

Infosec RHCSA Training Boot Camp

5-day boot camp

Infosec's RHCSA Boot Camp helps you gain the essential knowledge and hands-on skills to leverage Linux for your organizational advantage.

Don't see what you need?

Dozens of other IT and security boot camps are available for private onsites or online group training. Contact us for more information.

Infosec Skills Self-paced Training

Can't take time off? Infosec Skills Self-Paced Training is engineered to accommodate your busy schedule while providing a high-quality learning experience. With open enrollment, you have the freedom to begin your training whenever it suits you. Extended access to the course materials fits the training seamlessly into your routine. Our knowledgeable instructors are available to answer your questions offline, and a dedicated student advisory team is just a message away to support your learning journey.

AZ-104: Microsoft Azure Administrator

Course | 60 hours

You will learn to manage Azure subscriptions and resources, implement and manage storage, deploy and manage virtual machines (VMs), configure and manage virtual networks, and manage identities.

AZ-500: Microsoft Azure Security Technologies

Course | 50 hours

This course is intended for Azure and Microsoft server security professionals and those who are looking to take and pass the AZ-500: Microsoft Azure Security Technologies exam.

AZ-900: Microsoft Azure Fundamentals

Course | 40 hours

You will learn foundational level knowledge on cloud concepts; core Microsoft Azure services; security, privacy, compliance, and trust; and Azure pricing and support.

Certified AWS Cloud Practitioner

Course | 40 hours

This course is intended for IT professionals who would like to better understand AWS Cloud concepts and core AWS services.

Certified AWS Developer

Course | 40 hours

The AWS Developer course is designed for intermediate-level software developers and those looking to learn more about AWS's developing capabilities.

Certified AWS Solutions Architect

Course | 60 hours

The AWS Architect Associate course is designed for solutions architects and solution design engineers who want to learn fundamental skills to architect their IT solutions on AWS and more.

Certified AWS SysOps Administrator

Course | 60 hours

The AWS SysOps Administrator course is intended for system administrators and software developers who wish to learn related best practices and tools on the AWS platform for configuring and deploying systems.

Cloud Engineer Training

Course | 220 hours

The Cloud Engineer training will prepare you to be a certified cloud engineer, one of the 15 highest-paying IT jobs, and earn well-respected certifications that demonstrate you possess the real-world skills employers look for.

CompTIA A+

Course | 290 hours

This course prepares you for the CompTIA A+ certification. It requires passing two exams covering topics like mobile devices, networking, and troubleshooting.

CompTIA Network+

Course | 110 hours

A CompTIA Network+ certification course teaches you the basics of networking and prepares you for the certification exam (N10-008). You'll learn about network design, security, routing and switching, cloud computing, IPv6, and forensics, and have hands-on experience with a lab simulator.

CompTIA Security+

Course | 80 hours

Learn a broad range of security topics, including threat management, identity management, access control, cryptography, and network security. This course will teach you everything you need to take and successfully pass the CompTIA Security+ certification exam.

CompTIA Advanced Security Practitioner (CASP)

Course | 75 hours

Prepare for CompTIA Advanced Security Practitioner (CASP) certification, one of the most valuable certifications in the IT field.

CompTIA Cloud+

Course | 75 hours

Cloud computing is a rapidly growing field. This online course is designed for beginners and covers everything you need to know to pass the CompTIA Cloud+ certification exam and pursue a career in cloud computing.

CompTIA Linux+

Course | 75 hours

This Linux training course covers operating, maintaining, and troubleshooting Linux operating systems in a systems administrator role.

Certified Kubernetes Administrator (CKA)

Course | 130 hours

This course will teach you how to use the container management platform used by companies like Google to manage their application infrastructure.

Cisco CCNA Certification Training

Course | 225 hours

Take the next step in your IT career by preparing for the Cisco CCNA certification exam. You'll master certification-based topics for networking essentials, so you can implement and administer Cisco solutions. Exam voucher included in enrollment.

Cisco CCNP Enterprise: ENCOR & ENARSI

Course | 130 hours

This course is intended for network engineers, system engineers, network administrators, and those looking to attain their CCNP Enterprise certification.

Certified Information Security Manager (CISM)

Course | 75 hours

Prepare for the Certified Information Security Manager (CISM) certification and gain skills in four key areas: management, risk management and compliance, program development, and incident management.

Certified Information Systems Auditor (CISA)

Course | 75 hours

This online CISA training course will prepare you for the five key domains: auditing, governance, implementation, management, and protection.

Certified Information Systems Security Professional (CISSP)

Course | 150 hours

In the online world, information security is crucial for all organizations. Earning a CISSP certification can help cyber security professionals stay ahead in this field.

Certified Ethical Hacker v.12

Course | 100 hours

Certified Ethical Hacker CEH v12 will teach you the latest commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization.

Certified Penetration Testing Professional (CPENT)

Course | 200 hours

Learn how to perform an effective penetration test in an enterprise network environment that must be attacked, exploited, evaded, and defended using the EC-Council's Certified Penetration Tester (CPENT) program.

Computer Hacking Forensics Investigator (CHFI)

Course |100 hours

This course prepares for Computer Hacking Forensics Investigator (CHFI) certification exam. You will master the security discipline of digital forensics from a vendor-neutral perspective.

ITIL 4 Foundation

Course | 20 hours

Prepare for the ITIL 4 Foundation exam, a key certification for professionals managing modern IT-enabled services.

Linux Foundation Certified System Administrator

Course | 90 hours

This course will teach you the critical skills and knowledge needed to take the Linux Foundation Certified System Administrator (LFCS) exam—including all things involved with the Linux operating system.

IT and security fundamentals

IT and security fundamentals covers both broad information technology training and entry-level cybersecurity training. It is designed for those building a baseline of IT and security skills, as well as individuals who are looking to transition roles from IT and networking into cybersecurity.

Active Directory with Windows Server 2016

CERTIFICATION PATH

The Active Directory with Windows Server 2016 certification path builds your knowledge of Active Directory and prepares you to pass the Identity with Windows Server 2016 (70-742) certification exam.

Skill Assessment

Skill assessment | 20 questions

See how your Active Directory with Windows Server 2016 skills stack up against other professionals in your field.

Install and Configure Active Directory Domain Services

Course | 2 hours 10 minutes

Get started with Active Directory through this course on installing and configuring Active Directory Domain Services. Take a look at domain controllers, configuration options, managing groups and accounts and more.

NICE Knowledge and Skill Statements:

K0158, K0332, K0608, S0043, S0067, S0158, S0267

Managing and Maintaining Active Directory Domain Services

Course | 1 hour 36 minutes

Explore the intricacies of managing and maintaining AD DS with this course covering MSAs, advanced deployments and more.

NICE Knowledge and Skill Statements:

K0157, K0158, K0608, S0043, S0067, S0267, S0354

Create and Manage Group Policy

Course | 1 hour

Keep a tight rein on your system with this course on creating and managing group policies. Explore GPOs, working with templates, preferences and item-level targeting and more.

NICE Knowledge and Skill Statements:

K0158, K0608, S0043, S0067

Implement Active Directory Certificate Services

Course | 52 minutes

In this course on implementing Active Directory Certificate Services, you'll get to grips with the intricacies of certificates and certificate administration, installation, enrollment and more.

NICE Knowledge and Skill Statements:

K0019, K0056, K0403, S0043, S0067, S0138

Implement Active Directory Federation Services

Course | 36 minutes

Round out your study with this course on implementing Active Directory Federation Services, covering AD FS installation, multi-factor authentication and more.

NICE Knowledge and Skill Statements:

K0007, K0056, K0336, S0043, S0067, S0367

Advanced Intrusion Detection

SKILL PATH

This course will provide you with the practical, hands-on knowledge you need to fully understand the methodology behind intrusion detection and craft meaningful detection rules and logic.

Skill Assessment

Skill assessment | 20 questions

See how your intrusion detection skills stack up against other professionals in your field.

Advanced Intrusion Detection project

Project | 2 hours 20 minutes

This project consists of reviewing an alert for suspicious AV/Endpoint activity and connecting the dots between the event that occurred and what actions need to be taken to remediate it.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0046, K0324, K0332, K0405, K0473, S0025, S0084, S0120, S0192, S0280

Intrusion detection techniques and methods

Course | 50 minutes

We will go over the basics of intrusion detection, why it is needed for every environment, the various types (network. versus host-based) and techniques for crafting detections.

Home Lab Setup

Course | 1 hour 9 minutes

This course is a look at setting up a home detection lab.

NICE Knowledge and Skill Statements:

K0004, K0318, K0324, K0610, S0243

Network- versus host-based detection

Course | 38 minutes

This section provides a deeper dive into host- versus network-based intrusion detection.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0046, K0324, K0332, K0405, K0473, S0025, S0084, S0120, S0192, S0280

Anomaly detection

Course | 34 minutes

We will go over the basics of anomaly detection and how it can be used with other detection methods (signature) to identify malicious activity within your environment.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0046, K0324, K0332, K0343, K0405, K0473, S0025, S0280

The ATT&CK Matrix and threat intel

Course | 35 minutes

In this course, students explore the MITRE ATT&CK Framework.

NICE Knowledge and Skill Statements:

K0004, K0005, K0047, K0409, K0456, K0460, K0466, K0467, K0577, S0147

Data management

Course | 1 hour 7 minutes

In this course, we will discuss the importance of organizing how to collect, store and process the data you will eventually use for detections.

NICE Knowledge and Skill Statements:

K0043, K0142, K0377, K0382, K0386, K0387, K0389, K0404, K0500, K0567, S0017, S0126, S0183, S0217, S0218, S0252

Tactical data

Course | 51 minutes

In this course, the student expands on the topic of data management to explore tactical data.

NICE Knowledge and Skill Statements:

K0046, K0054, K0110, K0324, S0025, S0084, S0187

Advanced detection through deception technology

Course | 34 minutes

This section will explore the world of deception technology and how it can be used to build additional detections.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0046, K0324, K0406, K0473, K0487, K0561, S0084, S0120, S0192, S0280

AWS Certified Security Specialist

CERTIFICATION PATH

In this learning path, we will not only review key items of every exam domain but go hands-on with the AWS services that you must know to pass the exam. This course is meant to reinforce the material the exam expects you to know to pass.

AWS Certified Security Specialist Practice exam

Practice Exam | 64 questions

Prepare for your AWS Certified Security Specialist exam and test your domain knowledge.

AWS Certified Security Specialist introduction

Course | 22 minutes

We will look at the exam blueprint and setting up an AWS Free-tier account for the purposes of the course.

Infrastructure security in AWS

Course | 1 hour 10 minutes

In this course, we will review all infrastructure security areas in AWS that you will need to know for the exam.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0033, K0104, K0113, K0194, K0395, K0417, K0470, K0516, K0565, S0059, S0073, S0077, S0121

IAM security in AWS

Course | 1 hour 6 minutes

In this course, we will review all aspects of IAM security for the exam. Having an in-depth understanding of IAM is essential.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0007, K0056, K0065, K0158, K0194, K0336, S0031, S0073

Data protection in AWS

Course | 1 hour

In this course, we will review methods of data protection in AWS and the best way to use native AWS services to increase security.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0196, K0222, K0260, K0261, K0262, K0504, K0524, S0147

Logging and monitoring in AWS

Course | 36 minutes

In this course, we will review logging and monitoring. We will also discuss what aspects of this section will be most prevalent on the exam.

Incident response in AWS

Course | 25 minutes

In this course, we will review potential incident response scenarios that you will come across on the exam.

AWS Certified Security Specialist Exam tips

Course | 11 minutes

In this course, we will review exam resources that everyone should use while preparing them for the exam.

AWS Essentials & Solutions Architect Associate

CERTIFICATION PATH

The AWS Essentials & Solutions Architect Associate certification path begins by building your knowledge of essential AWS terminology, concepts and services before preparing you to pass the AWS Certified Solutions Architect - Associate exam.

Skill Assessment

Skill assessment | 20 questions

See how your AWS Essentials & Solutions Architect Associate skills stack up against other professionals in your field.

AWS Essentials Foundations and Services

Course | 1 hour 14 minutes

Start off strong with a course on AWS foundations and services such as account creation, bucket creation, using the management console and more.

NICE Knowledge and Skill Statements:

K0373, S0073

AWS Essentials Security and Costs

Course | 39 minutes

Explore AWS cost and security with this course and prepare yourself for your certification journey.

NICE Knowledge and Skill Statements:

K0056, S0073

About AWS and the Exam

Course | 53 minutes

This course introduces Amazon Web Services (AWS) and discusses the AWS CSA-A exam.

NICE Knowledge and Skill Statements:

S0073

AWS Cloud Services Overview

Course | 1 hour 8 minutes

This course provides a detailed overview of AWS Cloud Services.

NICE Knowledge and Skill Statements:

K0194, S0073

AWS Storage Design

Course | 2 hours 38 minutes

Keep your organization organized with this course on storage services in AWS.

NICE Knowledge and Skill Statements:

K0038, K0097, K0622, S0073

Virtual Private Cloud (VPC)

Course | 1 hour 31 minutes

This course covers the concept and configuration of the Virtual Private Cloud (VPC).

NICE Knowledge and Skill Statements:

K0104, S0059, S0073

Compute Services Design

Course | 39 minutes

This course introduces EC2 — the AWS cloud computing service.

NICE Knowledge and Skill Statements:

K0194, S0073

Compute Services Implementation

Course | 1 hour 4 minutes

This course walks through launching and configuring EC2 instances.

NICE Knowledge and Skill Statements:

K0073, S0073

Compute Services Management

Course | 70 minutes

Explore the ins and outs of the ongoing EC2 instance management.

NICE Knowledge and Skill Statements:

K0073, S0073

Identity and Access Management (IAM)

Course | 1 hour 26 minutes

Learn how to control access to your AWS account and the services running in it with Identity and Access Management (IAM).

NICE Knowledge and Skill Statements:

K0007, K0056, K0065, S0031, S0073

IAM Best Practices

Course | 1 hour

Explore practical application of AWS Identity and Access Management (IAM).

NICE Knowledge and Skill Statements:

K0007, K0056, K0065, S0031, S0073

Auto Scaling Solutions

Course | 51 minutes

Explore the options for dynamically growing or shrinking a set of servers in AWS.

NICE Knowledge and Skill Statements:

K0073, S0073

Virtual Network Services

Course | 50 minutes

This course focuses on DNS configuration and also explores Access Control Lists (ACLs) and flow logs.

NICE Knowledge and Skill Statements:

K0073, K0332, K0565, S0073

AWS Application Deployment

Course | 2 hours 24 minutes

This course covers an array of AWS application and deployment services, from Lambda to Trusted Advisor.

NICE Knowledge and Skill Statements:

K0049, K0073, K0487, K0561, S0073, S0084

AWS Database Design

Course | 1 hour 7 minutes

Learn how to architect and secure databases in AWS.

NICE Knowledge and Skill Statements:

K0073, K0373, K0419, K0420, S0073

Database Deployment

Course | 57 minutes

Practice creating and managing databases in AWS in this hands-on course.

NICE Knowledge and Skill Statements:

K0073, K0373, K0419, K0420, S0073

Additional AWS Services

Course | 1 hour 17 minutes

Get familiar with various AWS services developed to serve specific needs.

NICE Knowledge and Skill Statements:

K0194, S0073

Operational Excellence with AWS

Course | 1 hour 17 minutes

This scenario-based course illustrates the concepts of operational excellence.

NICE Knowledge and Skill Statements:

K0292, S0027, S0073

Cisco Certified Network Associate (CCNA)

CERTIFICATION PATH

The newest version of the Cisco Certified Network Associate (CCNA) covers the latest in the world of Cisco routing and switching. You'll explore network fundamentals such as routers and endpoints and take a closer look at network access, IP connectivity, IP services, security fundamentals and automation and programmability.

CCNA Practice Exam

Practice Exam | 569 questions

Prepare for your CCNA exam and test your domain knowledge.

Networking Cyber Range

Cyber range | 36 labs

Gain practical experience and develop your real-world networking skills through 36 hands-on labs in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0007, S0041, S0067, S0097, S0151, S0275

Network Fundamentals

Course | 4 hours 11 minutes

Dig into network components, network topology architectures, interface and cabling (and issues with them), IPv6, IP parameters and more. You'll explore switching concepts and take a look at the basics of virtual machines.

NICE Knowledge and Skill Statements:

K0011, K0034, K0057, K0061, K0108, K0113, K0174, K0221, K0255, K0393, K0395, K0417, K0471, K0486, K0489, K0491, K0516, K0555, K0556, K0565, K0610

Network Access

Course | 3 hours 13 minutes

Take a look at VLANs, inter-switch connectivity, Layer 2 discovery protocols and EtherChannel. You'll also learn Cisco Wireless Architectures and AP nodes, describe different types of connections and much more.

NICE Knowledge and Skill Statements:

K0001, K0007, K0108, K0113, K0221, K0375, K0395, K0446, K0516, K0565, K0600, K0614

IP Connectivity

Course | 2 hours 16 minutes

Explore the different concepts and challenges of IP connectivity: from interpreting the components of a routing table to configuring and verifying IPv4 and IPv6 static routing, exploring first-hop redundancy protocol and more!

NICE Knowledge and Skill Statements:

K0001, K0011, K0221, K0296, K0395, K0417, K0470, K0471, K0516, K0565, S0004, S0033, S0041, S0136

IP Services

Course | 2 hours 59 minutes

Explore configuring and verifying inside source NAT, the function of SNMP in network operations, configuring network devices for remote access using SSH, the capabilities and functions of TFTP/FTP in the network and more.

NICE Knowledge and Skill Statements:

K0001, K0071, K0111, K0221, K0332, K0334, K0395, K0398, K0452, K0471, K0565, S0004, S0033, S0041, S0136

Security Fundamentals

Course | 3 hours 14 minutes

Learn to define key security concepts, configure device access using local passwords, configure and verify access control lists, describe security program elements and more.

NICE Knowledge and Skill Statements:

K0004, K0007, K0033, K0049, K0056, K0065, K0158, K0324, K0336, K0487, K0488, K0561, S0007, S0031, S0077

Automation and Programmability

Course | 1 hour 14 minutes

In this course, you'll explore how automation impacts network management, compare traditional networks with controller-based networking, interpret JSON-encoded data and more.

NICE Knowledge and Skill Statements:

K0086, K0275, S0257

Cisco Certified CyberOps Associate

CERTIFICATION PATH

The CCNA Cyber Ops certification path prepares you to begin a career working with associate-level cybersecurity analysts within security operations centers. You'll gain the skills needed to pass the Cisco SECFND (210-250) and SECOPS (210-255) certification exams.

Skill Assessment

Skill assessment | 20 questions

See how your CCNA Cyber Ops skills stack up against other professionals in your field.

CCNA Cyber Ops Practice Exam

Practice Exam | 120 questions

Prepare for your CCNA Cyber Ops exams and test your domain knowledge.

Introduction to Cisco Certified CyberOps Associate

Course | 10 minutes

This course prepares you for your Cisco Certified CyberOps Associate training. You'll follow along with the course examples and set up your own cybersecurity lab with Kali Linux.

NICE Knowledge and Skill Statements:

K0342

Network Concepts

Course | 44 minutes

Networks can be complex, confusing and tricky. With this course, you'll dive into the devices and protocols used in networking, getting to grips with the basics of what you'll need to know for a successful security analyst career.

NICE Knowledge and Skill Statements:

K0001, K0011, K0034, K0058, K0061, K0143, K0174, K0221, K0296, K0332, K0516, K0565

Security Concepts

Course | 42 minutes

In this course, you'll get a closer introduction to some of the basic security concepts and tools that will help you later on in the Cisco Certified CyberOps Associate Learning Path — and in the rest of your career!

NICE Knowledge and Skill Statements:

K0412

Cryptography

Course | 15 minutes

This course will help you understand the differences between things like encryption, hashing and certificates, making it easier for you to understand the intricacies of data protection.

NICE Knowledge and Skill Statements:

K0190

Host-Based Analysis

Course | 39 minutes

In this course, you'll get to grips with the complexities and challenges of host-based analysis. You'll look at HBA on Microsoft and Linux, including endpoint protection, blacklisting, systems-based sandboxing and more.

NICE Knowledge and Skill Statements:

K0132, K0440, K0608

Security Monitoring

Course | 20 minutes

The best offense is a good defense ... or is it the other way around? In this course, you will learn how to stop a problem before it starts by detecting potential threats with security monitoring software features.

NICE Knowledge and Skill Statements:

K0058, K0301, K0493, S0046, S0120, S0221

Attack Methods

Course | 28 minutes

The war between hackers and security experts is ongoing, and the weapons are always evolving. In this course, you'll learn the about different strategies used by hackers to attack a network and cause damage.

NICE Knowledge and Skill Statements:

K0070, K0106, K0160, K0362, K0430, K0493

Endpoint Threat Analysis and Computer Forensics

Course | 17 minutes

In this course, you'll get a chance to explore some of the details of computer forensics. You'll take a closer look at Common Vulnerability Scoring System (CVSS) 3.0, Microsoft Windows and Linux file systems, evidence handling and more.

NICE Knowledge and Skill Statements:

K0117, K0125, K0191, K0272, K0402

Network Intrusion Analysis

Course | 16 minutes

In this course, you'll discover the types of information that you want to look for during network intrusion analysis. You'll get a look at security analysis with Wireshark, NetFlow version 5 and security events, impact flags and more.

NICE Knowledge and Skill Statements:

K0046, K0058, K0301, K0324, K0334

Incident Response and Handling

Course | 34 minutes

How you respond to an incident may mean the difference between safety or disaster on a network level. In this course, you'll be introduced to security frameworks and regulations that affect your incident response, including NIST and HIPAA.

NICE Knowledge and Skill Statements:

K0042, K0222, S0184

Data and Event Analysis

Course | 21 minutes

Once you have the data, you need to analyze it. Explore the details of data and event analysis, including retrospective analysis, data normalization and threat analysis.

NICE Knowledge and Skill Statements:

K0145, K0301, K0603, S0173

CompTIA IT Fundamentals (ITF+)

CERTIFICATION PATH

The IT Fundamentals learning path will take you through the essential knowledge, skills, tricks and tools needed to begin mastering the computer. Beginning with the basic hardware, you'll explore maintenance, troubleshooting, networking and much more.

Skill Assessment

Skill assessment | 20 questions

See how your IT Fundamentals (ITF+) skills stack up against other professionals in your field.

How People Use Computers

Course | 16 minutes

Begin your exploration of IT fundamentals with this course on how people use computers.

NICE Knowledge and Skill Statements:

K0036, K0071, K0109, K0113, K0137, K0302

System Hardware

Course | 24 minutes

System hardware can be complicated. Let's take a look at some different types of hardware.

NICE Knowledge and Skill Statements:

K0030, K0109, K0321, S0074

Device Ports and Peripherals

Course | 13 minutes

Explore device ports, peripherals and video cards with this course.

NICE Knowledge and Skill Statements:

K0109, K0192, K0491

Data Storage and Sharing

Course | 17 minutes

In this course, you'll get to grips with the technologies of data storage and sharing.

NICE Knowledge and Skill Statements:

K0097, K0109, K0114, K0373, K0622

Understanding Operating Systems

Course | 14 minutes

Begin digging into the details of operating systems with this course on OS functions and interfaces.

NICE Knowledge and Skill Statements:

K0060, K0318, K0608

Setting Up and Configuring a PC

Course | 16 minutes

Explore the details of PC setup and configuration.

NICE Knowledge and Skill Statements:

K0302

Setting Up and Configuring a Mobile Device

Course | 22 minutes

Examine the details of setting up and configuring a mobile device, including everything from syncing to storage.

NICE Knowledge and Skill Statements:

K0269, K0302

Managing Files

Course | 18 minutes

Dive deeper into the details of file management and manipulation.

NICE Knowledge and Skill Statements:

K0021, K0132, K0318, S0158

Using and Managing Application Software

Course | 16 minutes

Explore application setup and management with this course.

NICE Knowledge and Skill Statements:

K0229, K0271, K0373, K0444, K0559, K0608

Configuring Network and Internet Connectivity

Course | 25 minutes

Get to grips with the details of network connectivity and setup with this course.

NICE Knowledge and Skill Statements:

K0114, K0138, K0444, K0470, K0491, S0041

IT Security Threat Mitigation

Course | 31 minutes

Prepare to protect yourself with this course on IT security threat mitigation.

NICE Knowledge and Skill Statements:

K0004, K0158, K0297, K0362, K0480, K0527, K0603, S0067, S0121, S0229

Computer Maintenance and Management

Course | 16 minutes

Explore the crucial details of computer maintenance with this course.

NICE Knowledge and Skill Statements:

K0103, K0294, K0302, S0158, S0170

IT Troubleshooting

Course | 23 minutes

Prepare for trouble with this course on IT troubleshooting.

NICE Knowledge and Skill Statements:

S0124, S0142, S0151

Understanding Databases

Course | 17 minutes

Explore database details with this course on database purposes, functions and more.

NICE Knowledge and Skill Statements:

K0364, K0373, K0419, K0420

Developing and Implementing Software

Course | 16 minutes

Get ready for a deep dive into the details of programming with this course on developing software.

NICE Knowledge and Skill Statements:

K0016, K0068, K0266, K0372, K0373, K0396, S0060

CompTIA A+

CERTIFICATION PATH

The CompTIA A+ learning path builds a foundation of skills required for entry-level information technology careers. You'll learn about technical and support issues ranging from networking and operating systems to mobile devices and security.

Skill Assessment

Skill assessment | 20 questions

See how your A+ skills stack up against other professionals in your field.

A+ Practice Exam

Practice Exam | 229 questions

Prepare for your A+ exam and test your domain knowledge.

Introduction to CompTIA A+

Course | 24 minutes

Start your A+ journey off strong with this introductory course on the CompTIA A+ and its structure, uses and what to expect from the exam.

Safety and Professionalism

Course | 37 minutes

Professionalism and safety go hand-in-hand. Take a moment to review the fundamentals of professional communication, physical safety, troubleshooting theory and more.

NICE Knowledge and Skill Statements:

K0030, K0109, K0265, S0070

The Visible Computer

Course | 1 hour 18 minutes

Brush up on your knowledge of computer hardware and software with this course on PC components, OS types, super users and more.

NICE Knowledge and Skill Statements:

K0109, K0224, K0302

CPUs

Course | 1 hour 13 minutes

Get to grips with the details of central processing units, or CPUs, with this course covering CPU cores, caching, sockets and more.

NICE Knowledge and Skill Statements:

K0109, S0146

RAM

Course | 39 minutes

Out of RAM, out of luck. Brush up on your knowledge of RAM with this course covering RAM installation, technology, types and more.

NICE Knowledge and Skill Statements:

K0109

Firmware

Course | 35 minutes

Explore one fundamental, permanent aspect of a system: firmware. In this course, you'll look at BIOS, POST, System Setup and more.

NICE Knowledge and Skill Statements:

K0109, K0224

Motherboards

Course | 41 minutes

Brush up on your knowledge of the motherboard with this course on motherboard form factors, chipsets, installation and more.

NICE Knowledge and Skill Statements:

K0109, K0114

Power Supplies

Course | 1 hour 6 minutes

Power supplies aren't as simple as they appear. Explore the details with this course on power supply design, protection, troubleshooting and more.

NICE Knowledge and Skill Statements:

K0109, K0114

Mass Storage Technologies

Course | 39 minutes

Make sure you're storing things the smart way with this course on mass storage technologies, including solid state drives, magnetic disk drives and SCSI.

NICE Knowledge and Skill Statements:

K0109, K0114

Implementing Mass Storage

Course | 1 hour 53 minutes

There's more to storage than just keeping a backup. Expand your knowledge of RAID, file systems, dynamic disks and more.

NICE Knowledge and Skill Statements:

K0032, K0109, K0114

Essential Peripherals

Course | 1 hour 13 minutes

Update your knowledge of essential peripherals with this course on USB, optical media, Thunderbolt and more.

NICE Knowledge and Skill Statements:

K0109, K0114

Building a PC

Course | 54 minutes

Improve your knowledge of booting, installing Windows, post-installation tasks and more.

NICE Knowledge and Skill Statements:

K0035, K0036, K0060, K0109, K0114, K0271, K0608

Windows Under the Hood

Course | 1 hour 22 minutes

Take a closer look at Windows with this course covering the Windows registry, services, processes, toolset and more.

NICE Knowledge and Skill Statements:

K0116, K0129, K0132, K0192, K0271, K0318, K0608

Users, Groups and Permissions

Course | 1 hour 4 minutes

Make sure no one has access to the wrong information with this course on users, groups and permissions.

NICE Knowledge and Skill Statements:

K0117, K0608, S0267

Maintaining and Optimizing Operating Systems

Course | 43 minutes

Get the most out of your OS with this course covering maintaining and optimizing operating systems, system restore, backing up your files and more.

NICE Knowledge and Skill Statements:

K0060, K0088, K0129, K0318, K0608, S0267

Working with the Command-Line Interface

Course | 1 hour 54 minutes

Get to grips with the complexities of the command-line interface in this course that covers working with drives, files and folders, advanced Windows and Linux commands and more.

NICE Knowledge and Skill Statements:

K0060, K0068, K0192, K0318, S0267

Troubleshooting Operating Systems

Course | 45 minutes

Explore the art of troubleshooting an OS with this course covering troubleshooting boot problems and applications, kernel panic and more.

NICE Knowledge and Skill Statements:

K0060, K0224, K0318, S0067, S0142, S0151, S0267

Display Technologies

Course | 53 minutes

Keep an eye out for trouble with this course on display technologies. You'll look at the details of resolutions and aspect ratios, multiple monitors, projects, graphics cards and more.

NICE Knowledge and Skill Statements:

K0109, K0114, S0142, S0151

Essentials of Networking

Course | 1 hour 15 minutes

Keep your machines talking to each other with this course on the essentials of networking, including hubs and switches, WANs and routers, structured cabling and more.

NICE Knowledge and Skill Statements:

K0001, K0011, K0029, K0050, K0061, K0113, K0137, K0221, K0332, K0395, K0417, K0470, K0471, K0491, K0516, K0556

Local Area Networking

Course | 3 hours 26 minutes

Explore the complexities of LAN with this course covering network IDs and subnet masks, router configuration, port forwarding and more.

NICE Knowledge and Skill Statements:

K0011, K0029, K0050, K0113, K0221, K0332, K0395, K0491, K0516, K0556, S0168

Wireless Networking

Course | 1 hour 24 minutes

Explore wireless networking with this course covering wireless network hardware, enterprise wireless, troubleshooting connections and more.

NICE Knowledge and Skill Statements:

K0011, K0108, K0113, K0137, K0138, K0221, K0395, K0446, K0491, K0516, K0556, K0600, K0614

The Internet

Course | 1 hour 36 minutes

Take ninety minutes to deepen your knowledge of the internet's complexities with this ninety-minute course covering dial-up and broadband, remote desktop connections, FTP, proxy servers and more.

NICE Knowledge and Skill Statements:

K0011, K0061, K0104, K0113, K0137, K0221, K0274, K0349, K0395, K0444, K0470, K0471, K0491, K0516, K0556, K0603

Virtualization

Course | 48 minutes

Dig deeper into the real details of the virtual world with this course on virtualization, covering cloud computing, virtual machines and more.

NICE Knowledge and Skill Statements:

K0104, K0130, K0609, K0610, S0073

Portable Computing

Course | 38 minutes

Laptops aren't as simple as they appear. Improve your knowledge of portable computing with this course on laptop hardware, troubleshooting, displays and more.

NICE Knowledge and Skill Statements:

K0109, K0114, K0491

Understanding Mobile Devices

Course | 39 minutes

Brush up on your knowledge of mobile devices with this course covering mobile connections, OSes and more.

NICE Knowledge and Skill Statements:

K0109, K0114, K0138, K0224, K0269, K0438, K0600, K0614

Care and Feeding of Mobile Devices

Course | 51 minutes

Dig deeper into mobile devices with this course covering mobile devices and email, synchronization, security and more.

NICE Knowledge and Skill Statements:

K0114, K0224, K0283

Printers and Multifunction Devices

Course | 1 hour 18 minutes

Take a closer look at the world of printers with this course covering inkjet, thermal, impact and laser printers, printer installation and troubleshooting, 3D printing and more.

NICE Knowledge and Skill Statements:

K0109, K0114, K0142

Securing Computers

Course | 1 hour 31 minutes

Get to grips with system attack and defense through this course on securing computers. Includes modules on physical security, social engineering, malware, incident response and more.

NICE Knowledge and Skill Statements:

K0160, K0392, K0412, K0440, K0480, K0612, S0076

Getting Organized

Course | 36 minutes

Review your organization strategies with this course on documents, data, change management, data destruction and more.

NICE Knowledge and Skill Statements:

K0038, K0158, K0210, K0260, K0261, K0262

CompTIA Network+

CERTIFICATION PATH

The CompTIA Network+ learning path teaches you how to design, configure, troubleshoot and manage network devices. You'll learn about implementing networking concepts and using best practices to support and secure devices.

Skill Assessment

Skill assessment | 20 questions

See how your Network+ skills stack up against other professionals in your field.

Network+ Practice Exam

Practice Exam | 174 questions

Prepare for your Network+ exam and test your domain knowledge.

Understanding Networks

Course | 51 minutes

Explore network technology with this course on models, packets, ports and more.

NICE Knowledge and Skill Statements:

K0061, K0062, K0113, K0180, K0192, K0221, K0332, K0395, K0471, K0555, K0565

The Physical Network

Course | 3 hours 13 minutes

Brush up on the facts of the physical network in a course covering Ethernet, cabling, troubleshooting, Cat ratings and much more.

NICE Knowledge and Skill Statements:

K0109, K0113, K0221, K0395, K0417, K0516, K0555, S0041, S0142

The World of TCP/IP

Course | 3 hours 29 minutes

Take a close look at the world of TCP/IP with this course covering static and dynamic IP addressing, understanding routers and ports, implementing NAT and much more.

NICE Knowledge and Skill Statements:

K0192, K0332, K0417, K0471, K0516, K0555, K0565, S0162

Making TCP/IP Work

Course | 2 hours 52 minutes

Explore the complexities of making TCP/IP work with this course covering TCP and UDP, netstat, Wireshark and much more.

NICE Knowledge and Skill Statements:

K0007, K0018, K0019, K0033, K0056 , K0065, K0111, K0301, K0332, K0427, K0555, K0565, S0089

Securing TCP/IP

Course | 1 hour 19 minutes

Secure TCP/IP with this course covering encryption, cryptographic hashes, identification and everything else you need to keep your connection safe.

NICE Knowledge and Skill Statements:

K0007, K0018, K0019, K0033, K0056, K0065, K0301, K0332, K0427, K0555, K0565, S0089

Advanced IP Networking

Course | 3 hours 23 minutes

In this course, you'll explore the details of advanced IP networking with modules on VLANs, VPNs, ports and more.

NICE Knowledge and Skill Statements:

K0011 , K0071, K0104, K0192, K0324, K0417, K0437, K0471, K0516, S0162

Wireless, Virtual, Cloud and Mobile Networking

Course | 3 hours 25 minutes

Get to grips with the complexities of wireless, virtual, cloud and mobile networking with this course covering wireless security standards, Wi-Fi Protected Setup (WPS), wireless scenarios and much more.

NICE Knowledge and Skill Statements:

K0033, K0108, K0130, K0137, K0194, K0269, K0274, K0283, K0438, K0446, K0610, K0614

Building a Real-World Network

Course | 1 hour

Explore the building of a real-world network with this course covering network design, unified communications, backups and more.

NICE Knowledge and Skill Statements:

K0021, K0026, K0113, K0159, K0395, K0560, K0599, S0032

Managing Risk

Course | 3 hour 21 minutes

With this course on managing the network, you'll look at risk management, access control, network threats, testing network security and more.

NICE Knowledge and Skill Statements:

K0001, K0002, K0004, K0007, K0038, K0044, K0049, K0054, K0056, K0165, K0167, K0177, K0179, K0180, K0205, K0260, K0261, K0262, K0276, K0290, K0342, K0362, K0406, K0452, K0474, K0475, K0480, K0604, K0612, S0041, S0142, S0151

CompTIA Security+

CERTIFICATION PATH

The CompTIA Security+ certification path introduces you to a variety of information security concepts and technical controls. You'll learn about network and application security, compliance, different types of cyber threats and more.

Skill Assessment

Skill assessment | 20 questions

See how your Security+ skills stack up against other professionals in your field.

Security+ Practice Exam

Practice Exam | 525 questions

Prepare for your Security+ exam and test your domain knowledge.

Command Line Basics Cyber Range

Cyber range | 10 labs

Gain practical experience and develop your command line skills through 10 hands-on labs in the Command Line Basics Cyber Range.

NICE Knowledge and Skill Statements:

S0046, S0081, S0158, S0241, S0267, S0294

Risk Management

Course | 2 hours 9 minutes

Learn key concepts related to risk management, including policies and procedures, business impact analysis and threat and risk assessments.

NICE Knowledge and Skill Statements:

K0002, K0005, K0026, K0048, K0106, K0112, K0151, K0154, K0165, K0169, K0195, K0214, K0263, K0376, K0379, K0455, K0474, K0527, K0548, K0603

Cryptography

Course | 2 hours 27 minutes

Build a baseline of cryptography knowledge as you progress through this course covering essential cryptography concepts and use cases.

NICE Knowledge and Skill Statements:

K0018, K0019, K0056, K0104, K0190, K0201, K0305, K0308, K0403, K0427, K0428, S0089, S0138

Identity and Access Management

Course | 1 hour 38 minutes

Learn about one of the most important security concepts related to access management: identification, authentication, authorization and accounting.

NICE Knowledge and Skill Statements:

K0007, K0033, K0044, K0065, K0158, K0336, K0451, K0452, K0488, K0561, S0031

Tools of the Trade

Course | 1 hour 18 minutes

Explore the uses of common information security technology and tools.

NICE Knowledge and Skill Statements:

K0013, K0301, K0318, K0363, K0452, K0488, K0561

Securing Individual Systems

Course | 3 hours 5 minutes

Gain an entry-level understanding of essential hardware, firmware and operating system security concepts.

NICE Knowledge and Skill Statements:

K0005, K0011, K0032, K0046, K0057, K0106, K0109, K0151, K0167, K0205, K0324, K0397, K0480, K0530, K0603

The Basic LAN

Course | 1 hour 44 minutes

Learn the basics of designing secure networks.

NICE Knowledge and Skill Statements:

K0007, K0033, K0049, K0065, K0104, K0112, K0145 , K0179, K0255, K0326, K0336, K0488, K0561

Beyond the Basic LAN

Course | 3 hours 38 minutes

Explore the basics of virtualization and cloud security, including key cloud terminology and commonly used as-a-service models.

NICE Knowledge and Skill Statements:

K0033, K0108, K0130, K0167, K0205, K0230, K0322, K0428, K0600, K0603, K0609, K0610

Secure Protocols

Course | 1 hour 23 minutes

Learn the basics of secure software and application development.

NICE Knowledge and Skill Statements:

K0081, K0091, K0178, K0179, K0221, K0326, K0427

Testing Your Infrastructure

Course | 1 hour 5 minutes

Learn about vulnerability scanning and the importance of assessing the impact vulnerabilities can have on organizations.

NICE Knowledge and Skill Statements:

K0005, K0006, K0013, K0070, K0106, K0147, K0151, K0160, K0177, K0244, K0290, K0342, K0362, K0536, K0624

Dealing with Incidents

Course | 36 minutes

Explore how an incident response plan works and the basic concepts related to digital forensics.

NICE Knowledge and Skill Statements:

K0021, K0026, K0032, K0041, K0042, K0118, K0210, K0433, K0573

CompTIA Cloud+

CERTIFICATION PATH

The CompTIA Cloud+ certification path introduces you to a variety of information security concepts that affect the cloud. You'll learn about system requirements, cloud storage, security, troubleshooting and more.

Skill Assessment

Skill assessment | 20 questions

See how your Cloud+ skills stack up against other professionals in your field.

Introducing the Cloud

Course | 1 hour 17 minutes

Learn what the cloud is, how to set up various cloud accounts, and different cloud service providers.

NICE Knowledge and Skill Statements:

K0004, K0072, K0194, K0199, K0227,

System Requirements for Cloud Deployments

Course | 1 hour 50 minutes

Learn about cloud components, how to deploy the cloud and testing plans.

NICE Knowledge and Skill Statements:

K0004, K0028, K0089, K0091, K0179, K0194, K0199, K0291, K0293, K0609, S0061, S0115, S0282

Cloud Storage

Course | 1 hour 3 minutes

Learn about different storage types, how to manage storage and what to do in case the worst should happen.

NICE Knowledge and Skill Statements:

K0004, K0007, K0021, K0026, K0038, K0065, K0072, K0194, K0336, K0373, K0609, K0622

Cloud Compute

Course | 1 hour 6 minutes

Learn about cloud computing and how to run service and applications within the cloud.

NICE Knowledge and Skill Statements:

K0004, K0021, K0026, K0032, K0044, K0063, K0065, K0072, K0109, K0114, K0194, K0432, S0027

Cloud Networking

Course | 52 minutes

Learn about cloud networking, ports and protocols, and VPNs and other security technology you'll need to keep your cloud safe.

NICE Knowledge and Skill Statements:

K0004, K0044, K0109, K0179, K0194, K0435, K0488, K0561, S0077

Cloud Security

Course | 1 hour 22 minutes

Take a deep dive into cloud security, the rules and regulations governing security and various tools and services needed to protect the cloud.

NICE Knowledge and Skill Statements:

K0004, K0007, K0018, K0019, K0049, K0056, K0065, K0075, K0190, K0194, K0336, K0488, K0561, S0031, S0167

Migration Types

Course | 41 minutes

Migrating to the cloud requires planning and precision. Learn tools and techniques to consider when planning for migration.

NICE Knowledge and Skill Statements:

K0001, K0004, K0072, K0130, K0194, K0609, K0610, S0073

Planning Patch Management

Course | 1 hour 17 minutes

Get to grips with patch management and how to plan and implement patches from deployment to retirement.

NICE Knowledge and Skill Statements:

K0004, K0074, K0194, S0206

Troubleshooting Cloud Solutions

Course | 49 minutes

Learn everything you need to know about how to troubleshoot in the cloud.

NICE Knowledge and Skill Statements:

K0004, K0194, S0124, S0142, S0151

Cybersecurity Foundations

SKILL PATH

This learning path is an introductory cybersecurity path for people who have not been exposed to cybersecurity concepts in the workplace before. In these courses, a cybersecurity professional will walk the student through foundational concepts, commands and tools.

Cybersecurity Foundations skill assessment

Skill assessment | 20 questions

See how your foundational cybersecurity skills stack up against other professionals in your field.

Introduction to cybersecurity foundations

Course | 2 minutes

Learn what this learning path covers in a short and straightforward introductory video.

Cybersecurity foundations

Course | 39 minutes

This course introduces you to the basic concepts that are usually not covered in other classes and bootcamps for people entering the industry.

Operating system foundations

Course | 31 minutes

This is an introductory course to what an actual operating system is. We talk about Linux, Windows and MacOS.

Windows command line foundations

Course | 40 minutes

This course is an introduction to the Windows command line. There will be almost immediate hands-on exercises.

NICE Knowledge and Skill Statements:

K0060, K0129, K0167, K0192, K0205, K0224, K0302, K0318, K0608, S0267

Linux command line foundations

Course | 33 minutes

This course is designed to get the learner started on using Linux and the Linux command line.

NICE Knowledge and Skill Statements:

K0060, K0129, K0167, K0192, K0205, K0224, K0302, K0318, K0608, S0267

Network fundamentals

Course | 30 minutes

When data moves, it generally moves from one network to another. Here, we teach the learner about the fundamentals of networking.

NICE Knowledge and Skill Statements:

K0001, K0034, K0050, K0057, K0061, K0093, K0136, K0159, K0170, K0221, K0265, K0274, K0303, K0332, K0333,

Cloud computing fundamentals

Course | 43 minutes

This course is an introduction to cloud computing. It builds from the Network Fundamentals course in this path and prepares the learner for learning cloud security.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0179, K0194, K0230, K0255, K0489, S0073

Cybersecurity policy framework and guidelines

Course | 12 minutes

In this course, the learner will get a good look at what policies and frameworks do to keep the cybersecurity industry on-mission and formal.

NICE Knowledge and Skill Statements:

K0047, K0048, K0065, K0073, K0087, K0214, K0242, K0432, S0147

Cybersecurity auditing

Course | 12 minutes

This course is a basic introduction to cybersecurity auditing.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0043, K0090, K0154, K0165, K0198, K0257, K0363, S0038, S0085

Risk management

Course | 15 minutes

This course will take the learner on a quick trip down the road of risk management.

NICE Knowledge and Skill Statements:

K0002, K0008, K0019, K0021, K0026, K0048, K0065, K0100, K0101, K0126, K0149, K0154, K0165, K0379, K0455, K0622, S0120, S0175, S0252

Pentest demonstration: Appetizer for the beginner

Course | 25 minutes

In this course, we will take you through all five phases of a penetration test.

NICE Knowledge and Skill Statements:

K0001, K0004, K0013, K0070, K0342, S0051

Database Security

SKILL PATH

In the Database Security learning path, you'll learn about applicable rules and regulations and what it takes to protect sensitive data.

Database Security skill assessment

Skill assessment | 20 questions

See how your foundational database security skills stack up against other professionals in your field.

Who's responsible for data security?

Course | 20 minutes

This course discusses the duties of key groups, as well as giving an environment overview.

What data requires elevated security

Course | 34 minutes

Data security is an important part of the modern workplace. This course explores data classification in a security context.

When is database security important

Course | 11 minutes

Explore the three states of data in the context of database security.

Why is database security necessary

Course | 20 minutes

A look at the importance of database security.

How to secure databases in use

Course | 2 hours 15 minutes

Being aware of how to best protect data in use will be covered within this course.

NICE Knowledge and Skill Statements:

K0004, K0023, K0024, K0069, K0278, K0419, K0420, K0421, K0622, S0013, S0042, S0045, S0286

How to secure databases in motion

Course | 1 hour 15 minutes

This course will be a discussion on how to best protect data in motion, along with labs on encryption, views and triggers.

NICE Knowledge and Skill Statements:

K0004, K0023, K0024 , K0069, K0278, K0419, K0420, K0421, K0622, S0013, S0042, S0045, S0286

How to secure databases at rest

Course | 1 hour 4 minutes

This course will discuss the best methods on how to protect data in rest, and physical security of databases.

NICE Knowledge and Skill Statements:

K0004, K0023, K0024, K0069, K0278, K0419, K0420, K0421, K0622, S0013, S0042, S0045, S0286

Auditing & monitoring

Course | 1 hour 4 minutes

In this course, you'll explore the intricacies of database and server log monitoring for the purpose of database security.

NICE Knowledge and Skill Statements:

K0003, K0004, K0043, K0090, K0120, K0180, K0198, S0085

Policies & procedures

Course | 52 minutes

A look at the importance of policies and procedures, as well as a quick examination of standards and change management.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0065, K0087, K0101, K0146, K0157, K0264, S0018, S0145

ICS/SCADA Security Fundamentals

SKILL PATH

The ICS/SCADA Security Fundamentals skill path provides you with foundational knowledge about SCADA systems and security, including protocols, access controls, physical security, cybersecurity tools and more.

Skill Assessment

Skill assessment | 20 questions

See how your Linux/Unix stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

ICS/SCADA Security Fundamentals Project

Project | 1 hour 17 minutes

This project contains three parts and requires tasks across the MITRE ATT&CK for ICS Framework, the NIST CSF, risk assessment activities, ICS network architecture design, Packet Capture analysis, and reviewing IDS alert logs.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Industrial Control Systems (ICS) Introduction

Course | 27 minutes

A look at operational technology and ICS, including infrastructure, asset types and environments.

NICE Knowledge and Skill Statements:

K0137, K0437

ICS Fundamentals

Course | 33 minutes

A look at ICS fundamentals such as SCADA, SIS, DCS and ICS communications.

NICE Knowledge and Skill Statements:

K0004, K0137, K0179, K0221, K0332, K0437, K0561

ICS Operational Environment

Course | 36 minutes

A look at the ICS operational environment, exploring policies and standards, configuration management and more.

NICE Knowledge and Skill Statements:

K0002, K0054, K0137, K0154, K0157, K0158, K0200, K0267, K0437, S0167

ICS Networking

Course | 30 minutes

Explore ICS networking, including architecture, industry 4.0 and ICS network protocol analysis.

NICE Knowledge and Skill Statements:

K0027, K0049, K0056, K0075, K0113, K0137, K0170, K0221, K0240, K0322, K0332, K0417, K0437, K0491, K0561, K0565, S0077

ICS Security Introduction

Course | 31 minutes

A look at ICS security, including cybersecurity frameworks, physical security and more.

NICE Knowledge and Skill Statements:

K0007, K0047, K0048, K0049, K0054, K0056, K0065, K0084, K0137, K0170, K0179, K0200, K0233, K0240, K0437, K0561, S0031, S0077, S0144, S0147, S0256

ICS Security Management

Course | 1 hour 4 minutes

Exploring ICS security management, including asset management, mitigating cyber risk in ICS, intrusion detection and prevention and more.

NICE Knowledge and Skill Statements:

K0002, K0007, K0021, K0026, K0032, K0042, K0048, K0056, K0065, K0084, K0137, K0154, K0157, K0170, K0200, K0231, K0240, K0361, K0399, K0437, K0496, K0519, S0079, S0144, S0171

Information Security Fundamentals

SKILL PATH

The Information Security Fundamentals skill path teaches you critical knowledge of hardware, software and network security. You'll learn about popular security concepts, controls and technologies, as well an overview of risk management, incident response and disaster recovery.

Command Line Basics Cyber Range

Cyber range | 10 labs

Gain practical experience and develop your command line skills through 10 hands-on labs in the Command Line Basics Cyber Range.

NICE Knowledge and Skill Statements:

S0046, S0081, S0158, S0241, S0267, S0294

Access Control Fundamentals

Course | 21 minutes

Explore the essential concepts of access control in this four-video course covering access control models, implementation, concepts and enforcement.

NICE Knowledge and Skill Statements:

K0007, K0065, K0158, K0336

Secure Network Design

Course | 14 minutes

Lean the basics of designing secure networks, from an overview of network topologies to foundational security concepts such as segmentation and isolation.

NICE Knowledge and Skill Statements:

K0001, K0111, K0179, K0255, K0326, K0487, K0489

Identification and AAA

Course | 16 minutes

Learn about one of the most important information security concepts related to access management: identification, authentication, authorization and accounting (IAAA).

NICE Knowledge and Skill Statements:

K0007, K0056, K0336

Hardware and OS Security

Course | 16 minutes

Gain an entry-level understanding of essential hardware, firmware and operating system security concepts in this three-video introductory course.

NICE Knowledge and Skill Statements:

K0060, K0115, K0129, K0167, K0205, K0318

Software and Application Security

Course | 23 minutes

Learn the basics of secure software and application development, including secure staging, secure coding techniques, and code quality and testing.

NICE Knowledge and Skill Statements:

K0039, K0081, K0153, K0178

Physical Security

Course | 9 minutes

Discover how common physical and environment security controls relate to information security in this brief overview course.

NICE Knowledge and Skill Statements:

K0007

Security Technologies and Tools

Course | 60 minutes

Explore the uses of common information security technology and tools as you progress through this nine-video introductory course.

NICE Knowledge and Skill Statements:

K0033, K0104, K0145, K0296, K0324, K0488, K0516

Introduction to Cryptography

Course | 30 minutes

Build a baseline of cryptography knowledge as you progress through this nine-video course covering essential cryptography concepts and use cases.

NICE Knowledge and Skill Statements:

K0018, K0019, K0190, K0428

Introduction to Security Controls

Course | 17 minutes

Get an overview of common security control categories and types, and learn about important concepts such as data sanitation and data sensitivity.

NICE Knowledge and Skill Statements:

K0195, K0622

Risk Management Concepts

Course | 23 minutes

Learn the key concepts related to risk management, including policies and procedures, business impact analysis, and threat and risk assessments.

NICE Knowledge and Skill Statements:

K0002, K0006, K0066, K0165, K0263, K0527

Threats and Threat Actors

Course | 1 hour

Build your knowledge of popular threats, including malware and social engineering as well as application, wireless and cryptographic attacks.

NICE Knowledge and Skill Statements:

K0005, K0070, K0392, K0474, K0480

Business Continuity and Disaster Recovery

Course | 12 minutes

Learn the planning, procedures and concepts that go into business continuity and disaster recovery in this introductory course.

NICE Knowledge and Skill Statements:

K0021, K0210

Introduction to x86 Disassembly

SKILL PATH

Explore the foundations of x86 assembly, one of the most common assembly architectures in the world. Whether you're looking to become a better programmer or reverse engineer, a knowledge of assembly and how processors work is invaluable.

Skill Assessment

Skill assessment | 20 questions

See how your x86 disassembly skills stack up against other professionals in your field.

x86 Disassembly Project

Project | 3 challenges

Practice your x86 disassembly skills as your progress through five challenges.

What is x86 Assembly?

Course | 20 minutes

Dive into the world of assembly by learning a little about its history and some of the key differences between different assembly languages. This course takes you through a brief history of x86 Assembly and explores how it's used.

NICE Knowledge and Skill Statements:

K0051, K0139, K0227, K0372

x86 Basics

Course | 51 minutes

Learn the fundamentals of x86 Assembly. Explore the syntax, how data is represented, how to address memory and how to store information.

NICE Knowledge and Skill Statements:

K0051, K0139, K0372, S0239

Programming in x86

Course | 1 hour 13 minutes

Learn the most common x86 instructions and how to use them. With the basics down, you'll learn how to assemble and run an application fully written in x86 Assembly.

NICE Knowledge and Skill Statements:

K0139

Calls, Strings and Codes

Course | 1 hour 16 minutes

Learn how to do basic input and output, work with strings and condition codes at the x86 Assembly level. Then try your hand at your first project by building your own x86 Assembly program.

NICE Knowledge and Skill Statements:

K0051, K0068, K0139, K0372, S0239, S0257

Debugging

Course | 38 minutes

Learn how to debug at the assembly level and how to recover the assembly code from already-built binaries. Practice identifying common assembly fault conditions, then finish with a debugging project.

NICE Knowledge and Skill Statements:

K0051, K0068, K0079, K0139, K0186, K0188, K0372, K0396, S0014, S0239, S0257

Logic Flows

Course | 1 hour 2 minutes

Learn how to use logical flows in assembly to create code branches and optional code paths.

NICE Knowledge and Skill Statements:

K0051, K0068, K0139, K0372, K0396, S0239, S0257

ISACA CISA

CERTIFICATION PATH

The Certified Information Systems Auditor (CISA) certification path builds your knowledge of auditing information systems. You'll learn the tools and guidelines involved in the IT auditing process as well as concepts such as business continuity, enterprise IT governance, common security controls and more.

Skill Assessment

Skill assessment | 20 questions

See how your skills stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

Custom CISA Practice Exam

Practice Exam | 800 questions

Prepare for your ISACA CISA exam and test your domain knowledge.

NICE Knowledge and Skill Statements:

CISA Introduction

Course | 19 minutes

Introduce yourself to CISA with this course introduction covering study plans, CISA stats and details, and more.

NICE Knowledge and Skill Statements:

IS Audit Functions

Course | 8 minutes

Explore the functions of an information security audit with this course looking at auditor practices, IS audit purposes and more.

NICE Knowledge and Skill Statements:

Business Process Applications and Controls

Course | 42 minutes

Explore the Business Process section and the controls you'll need to understand during your CISA study.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0047, K0146, K0263, K0264, S0085

Types of Controls and Risk Assessments

Course | 21 minutes

Explore the types of controls and risk assessments in four parts, beginning with Control Objectives and Control Measures.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0044, K0047, K0065, K0264, S0034, S0085, S0147, S0171

Continuous Auditing

Course | 39 minutes

In this course, you'll look at the five parts of the Audit Project Management section, as well as sampling, audit report objectives and more.

NICE Knowledge and Skill Statements:

K0002, K0005, K0047, K0121, K0432, S0085

Governance and Management of IT

Course | 39 minutes

Dig deep into the details of governance and management of IT.

NICE Knowledge and Skill Statements:

K0002, K0027, K0044, K0146, K0154, K0198, K0429, K0501, K0504, S0085

IT Organizational Structure

Course | 32 minutes

Explore IT organizational structure and the critical associated concepts.

NICE Knowledge and Skill Statements:

K0002, K0004, K0027, K0043, K0044, K0047, K0267, K0429, K0598, S0085

IT Management

Course | 39 minutes

In this course, you'll review the details of IT management and more.

NICE Knowledge and Skill Statements:

K0004, K0027, K0044, K0053, K0101, K0154, K0198, K0257, K0265, K0267, K0270, K0429, S0085

CISA Day 1 Review Quiz

Skill assessment | 100 questions

Assess your new skills with a review quiz.

Information Systems Acquisition

Course | 32 minutes

Take a closer look at the first part of the Information Systems Acquisition and Development subdomain.

NICE Knowledge and Skill Statements:

K0090, K0101, K0121, K0154, K0257, K0270, S0085, S0273

Business Cases and Development

Course | 1 hour 4 minutes

Take some time to explore the second part of Information Systems Acquisition and Development.

NICE Knowledge and Skill Statements:

K0004, K0044, K0080, K0081, K0121, K0140, K0183, K0267, K0429, K0622, S0085, S0273

Information Systems Implementation

Course | 42 minutes

Wrap up Domain 3 of CISA with this course covering Control Identification and Design and Information Systems Implementation.

NICE Knowledge and Skill Statements:

K0004, K0044, K0074, K0091, K0178, K0267, K0275, K0290, K0531, K0622, S0085, S0273

CISA Day 2 Review Quiz

Skill assessment | 100 questions

Assess your new skills with a review quiz.

Information Systems Operations

Course | 1 hour 18 minutes

Dive into Part A of CISA Domain 4 in this course covering Common Technology Components and more.

NICE Knowledge and Skill Statements:

K0002, K0074, K0109, K0275, K0317, K0361, K0419, K0589, K0622, S0085, S0273

Business Resilience

Course | 23 minutes

Explore Part B of the Information Systems Operations domain.

NICE Knowledge and Skill Statements:

K0021, K0026, K0032, K0210, S0027, S0085, S0273

Business Continuity

Course | 40 minutes

Wrap up Part B of Domain 4 with this course on business continuity.

NICE Knowledge and Skill Statements:

K0021, K0026, K0210, S0027, S0032, S0085, S0273

CISA Day 3 Review Quiz

Skill assessment | 100 questions

Assess your new skills with a review quiz.

Asset Security Frameworks, Standards and Guidelines

Course | 41 minutes

In this course, you'll start on CISA Domain 5 by covering Information Asset Security and Control topics.

NICE Knowledge and Skill Statements:

K0005, K0007, K0261, K0262, K0263, K0622, S0085

Identity and Access Management

Course | 1 hour 6 minutes

Continue with Domain 5, Part A of CISA in this course covering identification and authentication topics.

NICE Knowledge and Skill Statements:

K0004, K0007, K0056, K0065, S0085

Network Infrastructure Security

Course | 52 minutes

Network infrastructure security has no secrets in this three-video course. Covers structure, auditing and more.

NICE Knowledge and Skill Statements:

K0004, K0005, K0010, K0044, K0061, K0108, K0113, K0221, K0286, K0417, K0556, K0560, K0561, K0600, S0085, S0192

Asset Security

Course | 51 minutes

Wrap up part A of CISA Domain 5 with this course covering asset security topics.

NICE Knowledge and Skill Statements:

K0004, K0005, K0018, K0019, K0044, K0065, K0113, K0136, K0159, K0190, K0195, K0230, K0287, K0322, K0427, K0609, K0622, S0085

Security Event Management

Course | 42 minutes

Explore Part B of CISA Domain 5 with this course on security event management.

NICE Knowledge and Skill Statements:

K0003, K0005, K0042, K0118, K0145, K0150, K0215, K0243, K0245, K0290, K0324, K0474, K0503, K0548, K0603, S0085, S0273

CISA Day 4 Review Quiz

Skill assessment | 100 questions

Assess your new skills with a review quiz.

ISC2 System Security Certified Practitioner (SSCP)

CERTIFICATION PATH

The System Security Certified Practitioner (SSCP) certification path will provide students with an overview of foundational information security concepts. The course will cover the seven domains that encompass the SSCP, with topics ranging from securing information systems and data to overall security operations.

SSCP Practice Exam

Practice exam | 121 questions

Prepare for your ISC2 System Security Certified Practitioner exam and test your domain knowledge.

Security Operations Architecture

Course | 1 hour 37 minutes

This course will take a closer look at different aspects of security operations from code of ethics to the security controls needed to ensure the confidentiality, integrity and availability (CIA framework) of an organization's information systems. The CIA framework will be a common reference throughout the entirety of the course.The CIA framework will be a common reference throughout the entirety of the course.

Access Controls

Course | 52 minutes

This course will walk through how organizations implement and maintain various authentication methods to those systems. We will discuss various techniques used by organizations such as single vs. multi-factor authentication and how single sign-on works.

Risk Identification, Monitoring and Analysis

Course | 1 hour 2 minutes

We'll look at how organizations identify their risk and choose how they want to treat their risk, whether they opt to accept it, mitigate it or transfer the risk to a third-party entity. We will also walk through various regulatory concerns that information security teams must be aware of, especially if organizations decide to operate in different counties or jurisdictions.

Incident Response and Recovery

Course | 49 minutes

The establishment of an incident response process will ensure that an organization can recover following the identification of a security incident. And while all alerts are not considered incidents, this section focuses on how to properly identify an security event in order to potentially declare it as an incident. In this course, you will learn how to truly define security incidents versus security events.

Overview of Cryptography

Course | 55 minutes

This course will review the core aspects of cryptography and the need for it. We take a pragmatic approach to understanding how and why cryptography and information security go hand-in-hand.

Network and Communications Security

Course | 1 hour 58 minutes

The security in your organization's network is just as important as the devices that sit on that network. In this section, we will discuss the various fundamental concepts of networking, starting with a model that helps describe a network at a logical level.

System and Application Security

Course | 1 hour and 41 minutes

Domain 7 will discuss the fundamentals of malware and the steps organizations may take to prevent or mitigate it.

Linux Fundamentals

SKILL PATH

The Linux Fundamentals learning path provides the fundamental skills and knowledge needed to successfully configure, manage and troubleshoot Linux systems. You will learn hands-on skills that are relevant for any Linux distribution (e.g., Red Hat, Ubuntu, Fedora, openSUSE).

Linux Cyber Range

Cyber range | 31 labs

Gain practical experience and build your real-world Linux skills through 31 hands-on labs in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0007, S0067, S0084, S0158, S0267

Installing Linux

Course | 14 minutes

Get an overview of the Linux platform and learn about its installation.

NICE Knowledge and Skill Statements:

K0192

Using Linux

Course | 38 minutes

Explore the basics of the Linux GUI and using command lines.

NICE Knowledge and Skill Statements:

K0192

File and Directory Management

Course | 1 hour 8 minutes

Everything you need to know about working with Linux files and directories.

NICE Knowledge and Skill Statements:

K0192

System Administration

Course | 1 hour 2 minutes

Get an comprehensive view of system admin tasks such as user and group management.

NICE Knowledge and Skill Statements:

K0192

User Environment Configuration

Course | 48 minutes

Understand the shell and environmental variables that store different information.

NICE Knowledge and Skill Statements:

K0192

Application Management

Course | 34 minutes

Learn how software installation and packages work in Linux.

NICE Knowledge and Skill Statements:

K0192

System Configuration

Course | 1 hour 4 minutes

Know what's involved in installing and managing new drives.

NICE Knowledge and Skill Statements:

S0067

Process and Module Management

Course | 45 minutes

See how processes carry out tasks within Linux.

NICE Knowledge and Skill Statements:

K0192

System Maintenance

Course | 1 hour 23 minutes

An overview of core maintenance tasks such as data backup and performance monitoring.

NICE Knowledge and Skill Statements:

K0021

Networking

Course | 1 hour 34 minutes

The fundamentals of networking, from components and addresses to protocols and DNS.

NICE Knowledge and Skill Statements:

K0221

File Sharing and Printing

Course | 20 minutes

See how NFS (network file system) is configured in the Linux system.

NICE Knowledge and Skill Statements:

K0192

Accessibility and Localization

Course | 20 minutes

Features and assistive technologies that make Linux more accessible and available to a variety of users.

NICE Knowledge and Skill Statements:

S0067

Security

Course | 1 hour 1 minute

Make your Linux system more secure with these tools and techniques.

NICE Knowledge and Skill Statements:

K0192

Web Environment

Course | 37 minutes

Learn about the modern web technologies that Linux supports.

NICE Knowledge and Skill Statements:

K0192

FTP and Email Services

Course | 47 minutes

A multi-part course introduces you to FTP, SSH and email configuration basics.

NICE Knowledge and Skill Statements:

K0192

Troubleshooting and Maintenance

Course | 1 hour 8 minutes

Take a dive into various issues you may encounter, and how to solve them.

NICE Knowledge and Skill Statements:

K0192

Network Security Fundamentals

SKILL PATH

Network security is a highly in-demand skill in the infosec world, and this learning path will teach you the fundamentals of networking and how to secure your networks.

Skill Assessment

Skill assessment | 20 questions

See how your network security fundamentals skills stack up against other professionals in your field.

Networking Fundamentals

Course | 1 hour 39 minutes

Learn about the OSI and TCP/IP models, AAA services and IAM (Identity and Access Management), and find out more about network traffic and how to secure it.

NICE Knowledge and Skill Statements:

K0001, K0007, K0056, K0061, K0065, K0221, K0332, K0395, K0471, K0565

Wireless Networks and Security

Course | 53 minutes

Uncover new information about wireless networks and security, with a focus on both Wi-Fi and cellular networks.

NICE Knowledge and Skill Statements:

K0001, K0108, K0113, K0137, K0446, K0556, K0614

Firewalls and IDS/IPS

Course | 30 minutes

Understand the fundamentals of both firewalls and IDS/IPSes, including types and architecture and what they can do to protect your network.

NICE Knowledge and Skill Statements:

K0033, K0038, K0044, K0324, K0561

VPNs and Remote Access Technologies

Course | 25 minutes

VPNs (virtual private networks) are essential to secure remote access of your network, and in this course we'll be focused on how to lock down your network using VPN tunnels and different remote access technologies.

NICE Knowledge and Skill Statements:

K0071, K0104, K0247, K0561

Endpoint Security

Course | 32 minutes

In this course, we will discuss protecting the endpoint, anti-malware and host-based IDS/IPSes, endpoint hardening and using mobile device management to lock down mobile devices.

NICE Knowledge and Skill Statements:

K0033, K0324, K0440, K0488, K0561

Preventing and Mitigating Network Attacks

Course | 20 minutes

In this course, we cover real-world network attacks and how to mitigate these potential risks.

NICE Knowledge and Skill Statements:

K0033, K0106, K0160, K0165, K0324, K0362, K0408, K0440, K0488, K0561, K0612

Network Security Principles

Course | 43 minutes

In this course, we go over some general concepts related to network security as well as how to establish these principles through policies and procedures.

NICE Knowledge and Skill Statements:

K0021, K0112, K0157, K0159, K0179, K0622

OWASP Top Ten

SKILL PATH

The OWASP Top Ten learning path will help you understand each of the security risks listed in the OWASP Top Ten. The “Top Ten” is a list of the most serious and prevalent security risks that exist for web applications today.

Skill Assessment

Skill assessment | 20 questions

See how your OWASP Top Ten skills stack up against other professionals in your field.

OWASP Top 10 Cyber Range

Cyber Range | 20 labs

Gain hands-on experience with the ten categories of web application security risks presented by OWASP

NICE Knowledge and Skill Statements:

S0022, S0025, S0051, S0084, S0172, S0174, S0293

OWASP Top Ten Overview

Course | 29 minutes

An overview of the OWASP organization and their methodology for creating and publishing the Top Ten list.

NICE Knowledge and Skill Statements:

K0004

OWASP Top Ten: Risks One through Five

Course | 3 hours 36 minutes

Explore the details of security risks one through five in the OWASP Top Ten list.

NICE Knowledge and Skill Statements:

K0004

OWASP Top Ten: Risks Six through 10

Course | 2 hours 49 minutes

Explore the details of security risks six through 10 in the OWASP Top Ten list.

NICE Knowledge and Skill Statements:

K0004, K0009

OWASP Top Ten: Scenarios

Course | 10 minutes

Take a look at five different Web application vulnerability or attack scenarios and answer challenging questions to test your OWASP Top Ten understanding.

NICE Knowledge and Skill Statements:

K0009, K0070, K0140, K0624

Python for Cybersecurity

SKILL PATH

This Python for Cybersecurity skills path helps you to master the use of Python for a wide variety of cybersecurity tasks.

Python for Cybersecurity Project

Project | 58 minutes

This project tests the understanding of the concepts and code demonstrated in this learning path.

Secure Coding - Python

Cyber range | 45 minutes

This lab covers multiple secure coding errors commonly found in Python, including deserialization and XML based attacks.

Introduction to Python for cybersecurity

Course | 26 minutes

This course provides an introduction to the Python for Cybersecurity Learning Path and introduces Python and the MITRE ATT&CK framework.

NICE Knowledge and Skill Statements:

K0004, K0039, K0068, K0070, K0079, K0080, K0082, K0139, K0140, K0236, K0559, K0624, S0060, S0130, S0172, S0266

Python for PRE-ATT&CK

Course | 59 minutes

The course demonstrates the use of Python to achieve the objectives outlined in the MITRE PRE-ATT&CK matrix.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0624, S0060, S0130, S0266

Python for initial access

Course | 38 minutes

This course demonstrates the use of Python to achieve initial access to a target system

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for execution

Course | 23 minutes

This course demonstrates the use of Python to achieve code execution on a system.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for persistence

Course | 41 minutes

This course demonstrates the use of Python to achieve persistence on a target system.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266, S0293

Python for privilege escalation

Course | 36 minutes

his course demonstrates the use of Python to achieve privilege escalation.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for defense evasion

Course | 30 minutes

In this course, you'll explore the details of using Python for defense evasion.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, K0430, K0493, S0051, S0060, S0130, S0266

Python for credential access

Course | 44 minutes

This course demonstrates the use of Python to gain access to user credentials.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, K0536, S0051, S0060, S0130, S0266

Python for discovery

Course | 35 minutes

This course demonstrates the use of Python to perform discovery on a target system.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for lateral movement

Course | 27 minutes

This course demonstrates the use of Python to move laterally through a target network.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for collection

Course | 25 minutes

This course demonstrates the use of Python for collection of data on a target system.

NICE Knowledge and Skill Statements:

K0040, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0130, S0266

Python for command-and-control

Course | 37 minutes

This course demonstrates the use of Python for command-and-control infrastructure.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, S0051, S0060, S0266

Python for exfiltration

Course | 42 minutes

This course demonstrates the use of Python for data exfiltration.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0342, K0536, S0051, S0060, S0130, S0266

Python for impact

Course | 31 minutes

This course demonstrates the use of Python to achieve an attacker's final objectives on a target system.

NICE Knowledge and Skill Statements:

K0004, K0018, K0068, K0070, K0139, K0140, K0177, K0190, K0236, K0342, K0427, S0051, S0060, S0130, S0266

Python for active defense: Decoys

Course | 48 minutes

This course demonstrates the use of Python for developing decoys for active defense.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0139, K0140, K0177, K0236, K0487, K0561, S0060, S0130, S0266

Python for active defense: Network

Course | 58 minutes

This course demonstrates the use of Python at the network level for active defense.

NICE Knowledge and Skill Statements:

K0004, K0068, K0070, K0116, K0139, K0140, K0177, K0179, K0236, K0255, K0487, K0561, K0565, S0060, S0130, S0266

Python for active defense: Monitoring

Course | 57 minutes

This course demonstrates the use of Python for monitoring for active defense.

NICE Knowledge and Skill Statements:

K0004, K0139, K0140, K0180, K0236, S0060, S0130, S0136, S0266

Securing Linux/UNIX

SKILL PATH

The Securing Linux/UNIX Learning Path will show you many facets of securing the Linux operating system. We will cover various topics, including understanding Linux users and groups, UIDs and GUIDs, file-level permissions and more.

Skill Assessment

Skill assessment | 20 questions

See how your Linux/Unix stack up against other professionals in your field.

Securing Linux/UNIX Project

Project | 2 hours 5 minutes

Get hands-on experience using sudo, configuring OpenSSH, identifying and configuring access to TCP ports, decrypting and encrypting with GPG, and using SELinux.

NICE Knowledge and Skill Statements:

S0121

Linux Users

Course | 44 minutes

This course will go over the basics of file permissions in Linux. W

NICE Knowledge and Skill Statements:

K0060, K0192, K0318, K0397, K0608, S0067

All About SSH

Course | 52 minutes

We will look at some basics of SSH and how to use it to authenticate to remote servers, both with and without passwords. Securing SSH servers is very important, and we will review the various ways to lock down this critical service.

NICE Knowledge and Skill Statements:

K0071, K0167, K0192, K0205, K0608, S0067, S0121

Linux and open ports with daemons

Course | 17 minutes

Learn what you need to know if ports on your server or a remote server are exposed. Explore why is a bad idea to run services that expose ports as the root user.

NICE Knowledge and Skill Statements:

K0167, K0192, K0205, K0342, K0491, K0608, S0067, S0121

TLS/SSL Certificates

Course | 29 minutes

TLS certs are an important part of securing traffic for applications that transfer data over the internet. Learn how to generate TLS certificates and use them on your servers.

NICE Knowledge and Skill Statements:

K0077, K0192, K0444, K0491, K0603, K0608, S0067, S0155

Firewalls on Linux

Course | 24 minutes

Learn the basics of setting up Layer 3 firewall rules on a Linux server. These days, applications need protection from attacks as well, so we'll also look at Web Application Firewalls.

NICE Knowledge and Skill Statements:

K0005, K0049, K0192, K0202, K0624, S0067, S0076

IDS/IPS on Linux

Course | 30 minutes

Learn about how Host Intrusion Detection Systems can alert you when critical changes are made to your systems. We will also cover how to stop brute-force attacks on applications running on your Linux systems by using the IPS Fail2Ban.

NICE Knowledge and Skill Statements:

K0049, K0192, K0324, K0488, S0067, S0076

Encryption using GPG

Course | 19 minutes

Email is one of the most widely used communication mediums on the internet and is typically sent in cleartext. GPG will help ensure that your communications are safe from unwanted eyes.

NICE Knowledge and Skill Statements:

K0038, K0049, K0192, K0427, S0067, S0076

SELinux

Course | 32 minutes

SELinux was designed to make Linux more secure but most people end up disabling it. Take a look at the basics of SELinux and how it works so that you don't have to change it.

NICE Knowledge and Skill Statements:

K0049, K0060, K0167, K0192, K0205, K0397, S0067, S0121

Security Scanning

Course | 16 minutes

Dive into the world of securing Linux systems and their apps (as suggested by the Department of Defense) with STIGs. We'll also cover automating system hardening with an OpenSCAP application.

NICE Knowledge and Skill Statements:

K0073, K0205, S0121, S0167, S0242

Web Server Protection

SKILL PATH

The web server protection learning path helps you to understand the different activities and processes to implement and monitor the security of a web server or web application. You will learn the basic concepts and tools to design, evaluate and monitor your web server.

Skill Assessment

Skill assessment | 20 questions

See how your web server protection stack up against other professionals in your field.

Web Server Protection Project

Project | 2 hours 42 minutes

Work with an Apache web server to implement network filtering, add cookies to access log, harden the host OS, identify tampered binary files and complete other tasks to ensure that your web server is properly protected.

NICE Knowledge and Skill Statements:

K0135, S0051, S0078, S0137, S0167

Introduction to the Web

Course | 1 hour 55 minutes

Get an introduction to the web, how it works and the basic protocols required to use it.

NICE Knowledge and Skill Statements:

K0061, K0221, K0395, K0470, K0471, K0491, K0565,

Infrastructure Components

Course | 2 hours 18 minutes

This serves as an introduction to some of the most common infrastructure components and how are they used for providing web server services.

NICE Knowledge and Skill Statements:

K0113, K0202, K0324, K0452, K0488, K0516, K0561, K0565, S0084

Preparation – Design Considerations

Course | 1 hour 9 minutes

Learn the basic considerations and implementation of diverse controls for web server platform design.

NICE Knowledge and Skill Statements:

K0011, K0057, K0170, K0180, K0286, K0322, K0333, K0491, K0516, K0560, S0152

Preparation – Hardening

Course | 2 hours 19 minutes

Learn what hardening is and identify the different components that require hardening.

NICE Knowledge and Skill Statements:

K0167, K0205, K0406, S0121

Logs

Course | 1 hour 36 minutes

Explore some of the common log formats and how to customize the web server configuration.

NICE Knowledge and Skill Statements:

K0132, K0412, S0120

Command Line

Course | 2 hours 19 minutes

Learn the purpose of some of the basic command-line tools and how to use them.

NICE Knowledge and Skill Statements:

K0129, K0318, S0019, S0267

Web Application Firewalls

Course | 1 hour 58 minutes

Learn about the different types of WAF configurations, as well as the OWASP CRS and its capabilities.

NICE Knowledge and Skill Statements:

K0049, K0202, K0487, K0561, K0624, S0170

Monitoring

Course | 2 hours 40 minutes

In this course, you'll explore the different elements involved in planning the monitoring of a web server, as well as what to look for on the logs and alarms.

NICE Knowledge and Skill Statements:

K0054, K0180, S0136, S0155

Active Defense

Course | 52 minutes

Understand how to deploy active defense mechanisms that would allow the web server to prevent or delay attacks.

NICE Knowledge and Skill Statements:

K0005, K0006, K0013

Windows 10 Host Security

SKILL PATH

This learning path is for anyone who works with Windows computers and wants to gain insights on protecting their hosts both in SOHO and enterprise environments. See how your organization can benefit by protecting your Windows 10 computers from malware, wireless hacking, open firewall ports, browsing the web and much more.

Skill Assessment

Skill assessment | 20 questions

See how your Windows 10 host security skills stack up against other professionals in your field.

Windows 10 Host Security Project

Project | 2 hours 24 minutes

Practice your Windows 10 Host Security skills by solving challenges.

NICE Knowledge and Skill Statements:

S0067, S0076, S0079, S0158, S0267, S0268

Introduction and Overview of Windows 10 Host Security

Course | 10 minutes

An introduction on the Windows 10 operating system and a history of Windows security issues and features in Windows 10 that can protect your host.

NICE Knowledge and Skill Statements:

K0060

Data Security

Course | 1 hour 13 minutes

Data security in these videos is about protecting access from people who shouldn't have access. NTFS security and share permissions are covered so you know how to properly share files and folders securely for your Windows hosts.

NICE Knowledge and Skill Statements:

K0117, K0622, S0067

Authentication Mechanisms

Course | 37 minutes

There are policies in place to allow you to log into a computer and set the security to keep non-authorized personnel from accessing that data. These policies and procedures are demonstrated in this course.

NICE Knowledge and Skill Statements:

K0065, K0336, K0452, K0608, S0067

Hardening Techniques

Course | 46 minutes

Learn how to update and patch your Windows 10 hosts both locally and through Active Directory automatically. You'll also learn about firewalls and Windows Defender.

NICE Knowledge and Skill Statements:

K0406, K0452, K0608, S0067, S0076, S0084, S0121

Local Group and Security Policy

Course | 16 minutes

Local policies drive security in Windows 10 in ways many don't realize. Learn how to configure them in a few simple steps.

NICE Knowledge and Skill Statements:

K0065, K0608, S0043, S0067, S0121

Web Browser Security

Course | 13 minutes

Browsing the web is one of the two biggest malware risks with Windows 10, with email being the second. Learn how to secure the Edge web browser in your Windows 10 hosts to keep malware away from your computer.

NICE Knowledge and Skill Statements:

K0349, K0608, S0067

User Account Management

Course | 23 minutes

There are many types of accounts, but do you know the best policy for what type you should use when logging onto your Windows 10 host? In this course, we explain and demonstrate these features and options.

NICE Knowledge and Skill Statements:

K0608, S0067, S0121

Application Management

Course | 30 minutes

Let's talk about keeping your computer safe while loading applications. Utilizing AppLocker, isolation and assigned access can help you do that. These concepts are discussed and demonstrated in this course.

NICE Knowledge and Skill Statements:

K0480, K0608, K0610, S0067, S0121

Certificates

Course | 36 minutes

Why do we need certificates on our Windows 10 host? This course covers the many different reasons for and types of certificates, helping you understand how and why you need them.

NICE Knowledge and Skill Statements:

K0056, K0608, S0067, S0121, S0138

Auditing Features

Course | 44 minutes

Windows logs tell us how our computer is doing and whether we should focus on any piece of hardware or software to fix an impending issue that could result in a breach.

NICE Knowledge and Skill Statements:

K0363, K0452, K0608, S0067

Backup and Recovery

Course | 56 minutes

In case of disaster, encryption or other malady, you can use the different types of Windows backups to bring your data back as soon as possible to your Windows 10 hosts.

NICE Knowledge and Skill Statements:

K0021, K0210, K0440, K0480, K0608, S0067

Wireless Security

Course | 35 minutes

More computers connect wirelessly to their corporate LAN and the internet than ever before. Learn about the different encryption types and the most secure way to connect.

NICE Knowledge and Skill Statements:

K0071, K0104, K0375, K0428, K0452, K0608, S0067

Remote Access Security

Course | 23 minutes

Road warriors keep companies running by being able to sell anywhere. You need a secure platform from which to do this, and in this course we discuss and demonstrate these concepts.

NICE Knowledge and Skill Statements:

K0071, K0104, K0247, K0375, K0608, S0067, S0267

Windows Server Security

SKILL PATH

Windows Server Security provides an in-depth introduction to the details of securing and handling your Windows server. You'll look at access control networks, passwords, authentication, firewall security, Edge browsing security, physical security, disaster recovery and more.

Skill Assessment

Skill assessment | 20 questions

See how your Windows Server security skills stack up against other professionals in your field.

Windows Server Security Project

Project | 2 hours 13 minutes

Practice your Windows Server security skills by solving challenges.

NICE Knowledge and Skill Statements:

S0136, S0158, S0367

Introduction and Overview of Windows Server Security

Course | 18 minutes

Microsoft has increased the amount of diversity of security features, but many of them are not well-advertised or enabled by default. In this course, you'll be introduced to the Windows Server OS and basic security.

NICE Knowledge and Skill Statements:

K0060, K0077

Access Control Network

Course | 51 minutes

Explore data security, NTFS security and share permissions so that you know how to properly share files and folders securely for your Windows servers.

NICE Knowledge and Skill Statements:

K0007, K0033, K0049, K0065, K0117, K0622, S0067

Password and Authentication

Course | 40 minutes

There are many ways to log into a computer such as two-factor authentication (2FA), picture passwords and PINs. In this course, you'll explore discussions and demos show the security values of each type.

NICE Knowledge and Skill Statements:

K0065, K0336, K0452, K0608, S0067

Updating Your Server for Security

Course | 25 minutes

WSUS can alleviate many pressures on IT administrators by allowing the approval, push and removal of updates instead of relying on Microsoft to do it for them. Explore the details of server updates in this course.

NICE Knowledge and Skill Statements:

S0067, S0121

Firewall Security, Routing and VPNs

Course | 69 minutes

Learn to protect your servers by blocking open ports in your firewall and making sure your computer is up to date. You'll also learn how to create custom firewall rules and what types of ports are most vulnerable to your host computer.

NICE Knowledge and Skill Statements:

K0104, K0406, K0452, K0608, S0067, S0076, S0084, S0121

Edge Browsing Security

Course | 17 minutes

Learn how to install and secure the Chromium Edge web browser, as well as utilizing local policies to protect everyone who uses your computer even when you're away from it.

NICE Knowledge and Skill Statements:

K0349, K0608, S0067

Local Account Security

Course | 24 minutes

Administrator and non-administrator accounts are used for different reasons. Learn how to use policies, single sign-on and UAC to protect yourself and anyone else who uses your computer.

NICE Knowledge and Skill Statements:

K0608, S0067, S0121

Malware and Certificates

Course | 67 minutes

Learn how to install a CA root server and have clients trust your certificates in order to avoid paying for costly public ones. You'll also learn about how to detect malware and protect your server from various attacks.

NICE Knowledge and Skill Statements:

K0056, K0480, K0608, S0067, S0121, S0138

Event Logs

Course | 25 minutes

Using Windows logs is a quick way to view the status of our Windows server. In this course, you'll look at the various types of logs in Windows operating systems and how to use them to troubleshoot programs and services.

NICE Knowledge and Skill Statements:

K0363, K0452, K0608, S0067

Backups and Disaster Recovery

Course | 41 minutes

When all else fails, Windows and third-party backup systems can protect your Windows servers by restoring data to new or existing server equipment. Learn how to restore and use shadow copies to enable users to restore their own files.

NICE Knowledge and Skill Statements:

K0021, K0210, K0440, K0480, K0608, S0067

Physical Security

Course | 11 minutes

Not everyone knows that there are actually multiple types of backup schemes. Learn about backup types, shadow copies and the quickest ways to restore data after a disaster.

NICE Knowledge and Skill Statements:

K0026, K0065, K0487

Hyper-V Security

Course | 14 minutes

There are multiple ways to protect your physical and virtual servers. Many of these are not enabled and some cause conflicts with other options. Learn what works well together and how they can protect your server environment.

NICE Knowledge and Skill Statements:

K0130, K0610

Pentesting and vulnerability management

Pentesting and vulnerability management training is focused on identifying, classifying, prioritizing, remediating and mitigating weaknesses in systems. It covers pentesting methodologies and vulnerability assessments, as well as exploiting systems and effectively communicating findings to key stakeholders.

Advanced Cybersecurity Concepts

SKILL PATH

The Advanced Cybersecurity Concepts skill path goes beyond the topics covered in entry-level security courses. You'll learn about reverse engineering malware, ethical hacking, Web application penetration testing and popular security frameworks.

Purple Team Privilege Escalation Project

Project | 2 hours 9 minutes

This project contains three labs focused on understanding, exploiting and mitigating vulnerabilities that allow a user to escalate their privileges.

NICE Knowledge and Skill Statements:

S0266, S0267

Introduction to Reverse Engineering

Course | 47 minutes

Take a closer look at the art and science of reverse-engineering with a course on machine code, assembly language, system-level reversing and more.

NICE Knowledge and Skill Statements:

K0175, K0372

Introduction to Ethical Hacking

Course | 38 minutes

Discover the basics of ethical hacking in this introductory course covering penetration testing methodologies and tools as well as an introduction to Linux.

NICE Knowledge and Skill Statements:

K0119, K0151, K0161, K0177, K0295, K0310, K0344, K0474, K0548

Introduction to Web Application Pentesting

Course | 19 minutes

Begin your pentesting path with this foundational introduction to Web application pentesting, covering common threats, methodologies and more.

NICE Knowledge and Skill Statements:

K0004, K0070, K0119, K0342, K0624

Information Security Frameworks

Course | 21 minutes

Get insight into a number of popular security frameworks and learn how they're used to implement controls and manage risk.

NICE Knowledge and Skill Statements:

K0002, K0047, K0165, K0261, K0297, K0527

Cloud Pentesting

SKILL PATH

Learn the basics of penetration testing in the cloud.

AWS Cloud Pentesting

Course | 40 minutes

The Cloud Pentesting with AWS learning path will give you hands-on experience with navigating, identifying, and exploiting targets located in the cloud.

NICE Knowledge and Skill Statements:

K0004, K0194, K0230, K0342, K0447, K0449, S0051, S0073, S0263

Azure Cloud Pentesting

Course | 36 minutes

The Cloud Pentesting with Azure learning path will give you hands-on experience with navigating, identifying, and exploiting targets located in the cloud.

NICE Knowledge and Skill Statements:

K0004, K0194, K0230, K0342, K0447, K0449, S0051, S0073, S0263

CompTIA PenTest+

CERTIFICATION PATH

The CompTIA PenTest+ certification path teaches you how to successfully plan, carry out and report the results of a penetration test. You'll learn the process behind penetration testing, tools and techniques used by pentesters, legal and compliance issues and more.

Skill Assessment

Skill assessment | 20 questions

See how your PenTest+ skills stack up against other professionals in your field.

PenTest+ Practice Exam

Practice Exam | 71 questions

Prepare for your PenTest+ exam and test your domain knowledge.

Introduction to PenTest+

Course | 8 minutes

This course serves as an introduction to the CompTIA PenTest+ certification.

Planning for an Engagement

Course | 29 minutes

Review the art of planning for a pentesting engagement with five videos on methodology, scoping and more.

NICE Knowledge and Skill Statements:

K0003, K0119, K0177, K0206, K0342

Scoping an Engagement

Course | 35 minutes

Learn about scoping a pentesting engagement in six videos covering assessment types, target selection and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0119, K0177, K0206, K0342, K0474, K0527

Information Gathering

Course | 1 hour 4 minutes

Ten videos take you through the many methods of information gathering, including scanning, enumeration, cryptographic inspection and eavesdropping. Includes demonstrations.

NICE Knowledge and Skill Statements:

K0004, K0005, K0119, K0177, K0206, K0342, K0409, K0536, S0051, S0081

Vulnerability Scanning

Course | 24 minutes

Review the process of vulnerability scanning, common vulnerability scanning tools and scan analysis with this four-video course.

NICE Knowledge and Skill Statements:

K0113, K0202, K0324, K0452, K0488, K0516, K0561, K0565, S0084

Preparing for Exploitation

Course | 20 minutes

Three videos help you prepare for exploitation with an in-depth review of common attack techniques, leveraging information for exploitation and weaknesses in specialized systems.

NICE Knowledge and Skill Statements:

K0005, K0070, K0106, K0119, K0147, K0177, K0206, K0314, K0322, K0342, K0437, K0536, S0051, S0242

Social Engineering and Physical Attacks

Course | 26 minutes

Social engineering takes center stage in this four-video course covering social engineering attack methods, motivation factors and physical security attacks.

NICE Knowledge and Skill Statements:

K0119, K0206, K0234, K0342, S0052

Exploiting Network and Application Vulnerabilities

Course | 47 minutes

Explore system weak points and methods of attack with this four-video course on exploiting network and application vulnerabilities.

NICE Knowledge and Skill Statements:

K0005, K0009, K0070, K0106, K0119, K0192, K0206, K0342, K0362, K0536, K0565, K0624, S0051

Exploiting Host-based Vulnerabilities

Course | 28 minutes

Learn about host-based vulnerabilities in this five-video course covering privilege escalation and escalation techniques.

NICE Knowledge and Skill Statements:

K0060, K0119, K0177, K0206, K0314, K0342, K0536, S0051

Post-exploitation Activities

Course | 29 minutes

Take a look at post-exploitation activities with four videos on lateral movement, persistence and covering your tracks.

NICE Knowledge and Skill Statements:

K0071, K0119, K0177, K0192, K0206, K0342, K0392, K0536, S0051, S0293

Using Nmap for Pentesting

Course | 24 minutes

Get to grips with the power of Nmap in this three-video course on using Nmap for pentesting.

NICE Knowledge and Skill Statements:

K0192, K0206, K0342, K0536, S0051, S0081

Use Cases of Pentesting Tools

Course | 41 minutes

Explore pentesting tools with thirteen videos on Web proxies, debuggers, exploitation frameworks and more.

NICE Knowledge and Skill Statements:

K0177, K0188, K0206, K0301, K0334, K0342, K0536, S0051

Basic Script Analysis

Course | 40 minutes

Python Code Security Cyber Range

NICE Knowledge and Skill Statements:

K0016 , K0068, K0206, K0342, K0529, S0051, S0257

Reporting and Communication

Course | 30 minutes

Make sure that critical findings reach the client with the help of this five-video course on reporting and communication.

NICE Knowledge and Skill Statements:

K0177, K0315, K0342, K0394, S0278

PenTest+ Conclusion

Course | 11 minutes

Wrap up your survey of pentesting with a tutorial on setting up your home pentesting lab.

NICE Knowledge and Skill Statements:

EC-Council CEH

CERTIFICATION PATH

The Certified Ethical Hacker (CEH) certification path teaches you the hacking skills necessary to successfully perform a penetration test. You'll learn the techniques and tools used by cybercriminals and how to apply them to conduct security assessments and report your findings.

Skill Assessment

Skill assessment | 20 questions

See how your CEH skills stack up against other professionals in your field.

CEH Practice Exam

Practice Exam | 1017 questions

Prepare for your CEH exam and test your domain knowledge.

Penetration Testing Cyber Range

Cyber range | 34 labs

Gain practical experience and build your real-world pentesting skills through 34 hands-on labs in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0001, S0025, S0046, S0051, S0052, S0078, S0081, S0094, S0137, S0156, S0167, S0221, S0267, S0293, S0295

Introduction to Ethical Hacking

Course | 38 minutes

Discover the basics of ethical hacking in this introductory course covering penetration testing methodologies and tools as well as an introduction to Linux.

NICE Knowledge and Skill Statements:

K0119, K0151, K0161, K0177, K0295, K0310, K0344, K0474, K0548

Passive Intelligence Gathering

Course | 1 hour 17 minutes

Learn about passive intelligence gathering, one of the key aspects of ethical hacking, in this four-video overview course.

NICE Knowledge and Skill Statements:

K0061, K0301, K0332, K0409, K0544, K0555, K0565, S0295

Network Recon

Course | 39 minutes

Learn the process of network reconnaissance and how it relates to ethical hacking, including tools, scan types and identifying vulnerable systems.

NICE Knowledge and Skill Statements:

K001, K0177, K0192, K0300, K0339, S0081, S0167, S0242, S0291, S0294

Fundamentals of Exploitation

Course | 47 minutes

Build your knowledge of exploitation, including types of exploits, overflows and privilege escalation, as well as tools and techniques related to ethical hacking.

NICE Knowledge and Skill Statements:

K0070, K0106, K0160, K0177, K0362, K0536, S0078

Breaking Password Security

Course | 27 minutes

Learn about breaking passwords, including different attack types and popular tools as well as tricks to retrieving passwords from Windows systems.

NICE Knowledge and Skill Statements:

K0362, K0536

Attacking Web Servers and Applications

Course | 35 minutes

Learn about attacking web servers and applications, including gathering server information and using tools to carry out ethical hacks such as cross-site scripting and SQL injection.

NICE Knowledge and Skill Statements:

K0009, K0070, K0373, K0398, K0624

Post-Exploitation Techniques

Course | 43 minutes

Learn about taking advantage of a system after it's been compromised, including leveraging post-exploitation techniques, using malware and exfiltrating data.

NICE Knowledge and Skill Statements:

K0070, K0177, K0188, K0191, K0209, K0259, K0324, K0392, K0430, K0479, K0480, S0293

Attacking Wireless Networks

Course | 21 minutes

Learn about exploiting wireless networks, including protocols and weak points as well as an overview of mobile devices.

NICE Knowledge and Skill Statements:

K0375, K0428

IoT Security

Course | 11 minutes

Learn about the Internet of Things (IoT) and how ethical hackers can exploit the growing number of internet-connected devices.

NICE Knowledge and Skill Statements:

K0115, K0147, K0309

Covering Tracks

Course | 11 minutes

Get insight into how cybercriminals and ethical hackers cover their tracks by removing evidence and any traces of their intrusion.

NICE Knowledge and Skill Statements:

K0177, K0184

Cryptography Fundamentals

Course | 38 minutes

Explore how cryptography relates to ethical hacking, including key cryptography concepts, cryptography uses and cryptanalytic attacks.

NICE Knowledge and Skill Statements:

K0018, K0019, K0305, K0308, K0427

Information Security Frameworks

Course | 21 minutes

Get insight into a number of popular security frameworks and learn how they're used to implement controls and manage risk.

NICE Knowledge and Skill Statements:

K0002, K0047, K0165, K0261, K0297, K0527

Ethical Hacking

SKILL PATH

The Ethical Hacking skill path helps you master a repeatable, documentable penetration testing methodology. You'll learn how to use the same techniques used by malicious hackers to carry out an ethical hack and assess your organization's vulnerabilities.

Penetration Testing Cyber Range

Cyber range | 34 labs

Gain practical experience and build your real-world pentesting skills through 34 hands-on labs in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0001, S0025, S0046, S0051, S0052, S0078, S0081, S0094, S0137, S0156, S0167, S0221, S0267, S0293, S0295

Purple Team Web Application Security Project

Project | 2 hours 34 minutes

This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application.

NICE Knowledge and Skill Statements:

S0022, S0025, S0051, S0084, S0172, S0174, S0293

Ethical Hacking Process

Course | 1 hour 8 minutes

Introduce yourself to ethical hacking with this course covering concepts, terminology and the ethical hacking process, step-by-step from passive reconnaissance to post-exploitation and reporting.

NICE Knowledge and Skill Statements:

K0004, K0119, K0177, K0206, K0342

Passive Intelligence Sources, Tools and Techniques

Course | 1 hour 29 minutes

Get to grips with the crucial tools and techniques associated with passive intelligence gathering. Explore intelligence-gathering goals, sources and concepts. Includes vocabulary and definitions.

NICE Knowledge and Skill Statements:

K0119, K0206, K0342, K0409, S0051

Understanding TCP/IP Communications

Course | 52 minutes

In this course, you'll explore TCP/IP communications specifically for ethical hackers. You'll take a look at TCP, UDP and ICMP, and examine TCP communications through in-depth demonstrations in Wireshark.

NICE Knowledge and Skill Statements:

K0119, K0206, K0221, K0301, K0342, K0471, K0565, S0046, S0051

Network Reconnaissance

Course | 38 minutes

You can't launch an attack without some careful reconnaissance. In this course, you'll look at network reconnaissance goals and concepts, including host discovery, port scanning and service identification.

NICE Knowledge and Skill Statements:

K0119, K0177, K0206, K0221, K0318, K0342, K0565, S0001, S0051, S0081

Stealthy Network Reconnaissance

Course | 30 minutes

Reconnaissance isn't much good if you're spotted while you're doing it. Explore what it takes to carry out stealthy network reconnaissance with this course covering strategies and stealthy scanning methods.

NICE Knowledge and Skill Statements:

K0111, K0119, K0177, K0206, K0221, K0318, K0342, K0565, S0001, S0051, S0081

Finding and Exploiting Vulnerabilities

Course | 53 minutes

A vulnerability is as good as another tool for an ethical hacker. Learn the fundamentals of finding and exploiting vulnerabilities with this course covering exploits, buffer overflows, DLL hijacking and much more.

NICE Knowledge and Skill Statements:

K0070, K0119, K0165, K0177, K0342, K0362, K0480, K0536, K0604, S0001, S0051

Sniffing

Course | 1 hour 2 minutes

There are a number of ways to carry out sniffing. In this course, you'll explore what it takes to sniff internet traffic, as well as sniffing techniques with packetrecorder, useful tips for sniffing on public Wi-Fi networks and more.

NICE Knowledge and Skill Statements:

K0058, K0061, K0108, K0111, K0119, K0177, K0342, K0446, K0536, S0051, S0052, S0156

Cracking Passwords

Course | 36 minutes

Cracking a password effectively opens the door into an account or system. Explore the details of cracking passwords, including understanding and capturing Windows passwords and useful tools such as Cain & Abel.

NICE Knowledge and Skill Statements:

K0177, K0342, K0362, K0536, S0051, S0067

Covert Channels and IDS Evasion

Course | 39 minutes

An intrusion detection system, or IDS, can be a problem for an ethical hacker. In this course, you'll get to grips with the use of covert channels and evading an intrusion detection system. Includes demonstrations.

NICE Knowledge and Skill Statements:

K0177, K0184, K0305, K0324, K0342, K0403, K0472, K0493, K0536, S0051, S0092

Using Trojans and Backdoors

Course | 31 minutes

Ethical hackers need to be familiar with hackers' tricks, and even be able to use them for helpful purposes. With this course, you'll look at using Trojans and backdoors in an ethical hack, both hiding and detecting backdoor activity.

NICE Knowledge and Skill Statements:

K0129, K0177, K0318, K0342, K0536, S0051, S0267

Exploit Writing Fundamentals: Basic Buffer Overflow Exploit

Course | 53 minutes

Get to grips with the basic buffer overflow exploit in this course. Modules cover understanding memory, initial discovery, fuzzing, vulnerability identification and more. Includes demonstrations.

NICE Knowledge and Skill Statements:

K0070, K0119, K0177, K0206, K0318, K0342, S0001, S0051, S0081

Exploiting Common Web Application Vulnerabilities

Course | 51 minutes

Learn how to carry out ethical hacks such as cross-site scripting and SQL injection.

NICE Knowledge and Skill Statements:

K0070, K0119, K0177, K0206, K0318, K0342, K0624, S0001, S0051, S0081

Certified Expert Penetration Tester (CEPT)

CERTIFICATION PATH

The Certified Expert Penetration Tester (CEPT) certification path teaches you advanced hacking tools and techniques. You'll learn how to successfully attack fully patched and hardened systems, how to circumvent common security controls, and how to defend your organization against advanced persistent threats.

Skill Assessment

Skill assessment | 20 questions

See how your CEPT skills stack up against other professionals in your field.

CEPT Practice Exam

Practice Exam | 75 questions

Prepare for your CEPT exam and test your domain knowledge.

Purple Team Privilege Escalation Project

Project | 2 hours 9 minutes

This project contains three labs focused on understanding, exploiting and mitigating vulnerabilities that allow a user to escalate their privileges.

NICE Knowledge and Skill Statements:

S0266, S0267

Introduction to Advanced Hacking

Course | 7 minutes

A brief overview of the topics that you need to know about advanced hacking.

NICE Knowledge and Skill Statements:

K0003, K0004, K0119, K0177, K0206, K0342

Advanced Reconnaissance

Course | 26 minutes

Discover some of the techniques pentesters can use in complex environments.

NICE Knowledge and Skill Statements:

K0004, K0005, K0061, K0119, K0129, K0177, K0179, K0206, K0255, K0318, K0324, K0342, K0486, K0489, K0529, K0536, S0051, S0081

Finding Vulnerabilities in Software

Course | 57 minutes

Learn both manual and automated techniques for discovering vulnerabilities in apps.

NICE Knowledge and Skill Statements:

K0004, K0005, K0013, K0119, K0177, K0186, K0188, K0206, K0342, K0529, K0536, S0051, S0081, S0137, S0167, S0242

Exploit Writing

Course | 47 minutes

Explore various exploits and how to choose the right Metasploit payload.

NICE Knowledge and Skill Statements:

K0005, K0016, K0068, K0070, K0119, K0177, K0186, K0188, K0206, K0234, K0342, K0372, K0536, S0019, S0051, S0130

Advanced Exploitation

Course | 34 minutes

Learn concepts of advanced threats and how to use them in pentesting.

NICE Knowledge and Skill Statements:

K0004, K0069, K0070, K0115, K0119, K0129, K0162, K0177, K0206, K0342, K0447, K0452, K0529, K0536, K0624, S0051, S0167, S0267

AEH Wrap Up

Course | 3 minutes

The key takeaways you need for becoming an ethical hacker.

NICE Knowledge and Skill Statements:

K0119, K0206, K0342

Certified Mobile and Web App Penetration Tester

CERTIFICATION PATH

The Certified Mobile and Web App Penetration Tester (CMWAPT) certification path teaches you the skills, tools and techniques required for conducting comprehensive security tests of mobile and Web applications.

Skill Assessment

Skill assessment | 20 questions

See how your CMWAPT skills stack up against other professionals in your field.

CMWAPT Practice Exam

Practice Exam | 44 questions

Prepare for your CMWAPT exam and test your domain knowledge.

Purple Team Web Application Security Project

Project | 2 hours 34 minutes

This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application.

NICE Knowledge and Skill Statements:

S0022, S0025, S0051, S0084, S0172, S0174, S0293

Introduction to Web Application Pentesting

Course | 19 minutes

Begin your pentesting path with this foundational introduction to Web application pentesting, covering common threats, methodologies and more.

NICE Knowledge and Skill Statements:

K0004, K0070, K0119, K0342, K0624

Target Identification and Application Mapping

Course | 54 minutes

Take a closer look at target identification and application mapping with this course covering service identification, core defense mechanisms and more. Includes vocabulary and tools.

NICE Knowledge and Skill Statements:

K0070, K0077, K0286, K0342, K0408, K0624, S0051, S0081

Attacking Web Application Access Controls

Course | 27 minutes

Learn to attack web application access controls with this course on attacking access control, attacking authentication, attacking session management and more.

NICE Knowledge and Skill Statements:

K0007, K0070, K0077, K0105, K0177, K0286, K0336, K0342, K0624, S0051

Injection Attacks

Course | 19 minutes

Learn what you need to know about injecting code or SQL queries into vulnerable applications in order to circumvent access controls. Includes vocabulary and examples.

NICE Knowledge and Skill Statements:

K0070, K0105, K0177, K0342, K0624, S0051

Common Attack Methods

Course | 37 minutes

Think like a hacker with this course on common attack methods used for pentesting, including attacking Web services, cross-site scripting and exploiting logic flaws.

NICE Knowledge and Skill Statements:

K0070, K0105, K0177, K0342, K0624, S0051

Introduction to iOS App Pentesting

Course | 33 minutes

Get an introduction to iOS app pentesting with this course covering analyzing an iOS app, binary analysis, iOS app security measures and more.

NICE Knowledge and Skill Statements:

K0060, K0070, K0224, K0269, K0342, K0438, K0624

iOS App Pentesting Tools and Techniques

Course | 45 minutes

Be ready for action with this course on iOS app pentesting tools and techniques. Covers runtime manipulation, insecure data storage, broken cryptography and other ways to get into a target system.

NICE Knowledge and Skill Statements:

K0060, K0070, K0140, K0177, K0224, K0269, K0342, K0438, K0624, S0051

Introduction to Android App Pentesting

Course | 20 minutes

Prepare for the challenge of Android app pentesting with this introductory course covering reversing Android applications, Drozer and more.

NICE Knowledge and Skill Statements:

K0060, K0070, K0224, K0269, K0342, K0438, K0624

Android App Pentesting Tools and Techniques

Course | 30 minutes

Dive deeper into Android app pentesting with this course on Android app pentesting tools and techniques. Includes vocabulary, walkthroughs and a close look at the Frida pentesting toolkit.

NICE Knowledge and Skill Statements:

K0060, K0070, K0140, K0177, K0224, K0269, K0342, K0624, S0051

Introduction to Vulnerability Management

SKILL PATH

The Introduction to Vulnerability Management Learning Path will enable you to master a repeatable, documented and continuously improving vulnerability management program. You will learn how to use the same techniques used by organizations with mature vulnerability management programs covering tens of thousands of endpoints.

Skill Assessment

Skill assessment | 20 questions

See how your vulnerability management skills stack up against other professionals in your field.

Vulnerability Management Project

Project | 2 hours 34 minutes

Put your skills to the test as you identify risky open ports, find vulnerabilities in the operating system and SMB service, verify vulnerabilities and find their CVSS score, investigate how to remediate the vulnerabilities and more.

NICE Knowledge and Skill Statements:

S0036

Introduction to Vulnerability Management

Course | 23 minutes

In the first course, we will take a look at what this learning path is all about. We will discuss what we will learn, how we will learn it and what you will be able to do with that knowledge.

NICE Knowledge and Skill Statements:

K0005

Setting Up Your System

Course | 22 minutes

This course will go over setting up the VirtualBox environment with the Kali Linux and Metasploitable 2 and 3 VMs. You will also set up Nessus, nmap and OpenVAS.

NICE Knowledge and Skill Statements:

K0013, K0610

Vulnerability Management Process

Course | 1 hour 3 minutes

Explore the vulnerability management process in detail. We go over determining the scope of the program, defining the strategy, selecting the methodology and selecting the tools, as well as engaging management and stakeholders.

NICE Knowledge and Skill Statements:

K0002, K0005, K0044, K0074, K0165

Automated Vulnerability Scanners

Course | 36 minutes

In this course, we will look at what automated vulnerability scanners are, how to use them and why they are useful.

NICE Knowledge and Skill Statements:

K0004, K0005, K0013, K0070

Manual Vulnerability

Course | 1 hour 3 minutes

In this course, we will look at how to manually verify the existence of several different vulnerabilities with a wide array of tools. We will look at Metasploit, nmap, netcat and Wireshark.

NICE Knowledge and Skill Statements:

K0005, K0013, K0070, K0342

Prioritizing Vulnerabilities

Course | 14 minutes

This course will cover how to prioritize vulnerabilities in our environment based on industry standard metrics (CVSS) as well as a risk-based approach based on what is important to our organization.

NICE Knowledge and Skill Statements:

K0165

Remediation

Course | 27 minutes

In this course, we will look at best practices for establishing and running an effective patch management program.

NICE Knowledge and Skill Statements:

K0002, K0040, K0074

Web Application Vulnerabilities

Course | 53 minutes

This course will look at some of the most common web application vulnerabilities, as well as open-source and commercial scanners that can be used to detect them.

NICE Knowledge and Skill Statements:

K0009, K0013, K0070, K0624

Frameworks

Course | 47 minutes

This course will examine what role vulnerability management plays in different industry frameworks. We will accomplish this by looking at specific requirements and controls from each of the frameworks discussed.

NICE Knowledge and Skill Statements:

K0047, K0048, K0261

Vulnerability Management Summary

Course | 1 hour 19 minutes

This course will recap everything we have learned throughout the path, including the VM process, automated scanning, manual verification (with demo), prioritization, remediation and web application vulnerabilities.

NICE Knowledge and Skill Statements:

Machine Learning for Red Team Hackers

SKILL PATH

Learn the ins and outs of hacking machine learning. The learning path covers topics such as hacking a CAPTCHA system, fuzzing a target, evading malware detection and attacking machine learning systems. You will also learn about deepfakes and how to perform backdoor attacks on machine learning.

Skill Assessment

Skill assessment | 20 questions

See how your Machine Learning for Red Team Hackers skills stack up against other professionals in your field.

Introduction to Machine Learning for Red Team Hackers

Course | 2 minutes

Get an overview of what to expect in the Machine Learning for Red Team Hackers Learning Path, including highlights of course topics and a brief description of the path's hands-on assignments.

NICE Knowledge and Skill Statements:

K0004

Hacking CAPTCHA Systems

Course | 1 hour 57 minutes

Learn how to implement and use a CAPTCHA-evading bot from scratch, including training and designing a deep neural network, using selenium to automate the CAPTCHA evasion and using the created bot on a webpage designed to be attacked.

NICE Knowledge and Skill Statements:

K0238

Smart Fuzzing

Course | 49 minutes

In this course, you'll write a custom evolutionary fuzzer that employs machine learning to fuzz a target. You'll also learn the machine learning behind, as well as how to use, AFL.

NICE Knowledge and Skill Statements:

K0238

Evading Machine Learning Malware Classifiers

Course | 21 minutes

In this course, you'll learn how to modify malware so it is able to get past neural network and gradient boosting machine learning malware classifiers.

NICE Knowledge and Skill Statements:

K0238

Adversarial Machine Learning

Course | 33 minutes

Learn how to perform white-box and black-box attacks on machine learning classifiers in this course.

NICE Knowledge and Skill Statements:

K0238

Deepfake

Course | 26 minutes

This course helps you understand the implications of the deepfake technology, setup an environment for performing deepfakes and then create a deepfake video.

NICE Knowledge and Skill Statements:

K0238

Hacking Machine Learning

Course | 14 minutes

This course will teach you some of the darker, less publicized attacks on machine learning, including how to poison, backdoor and steal machine learning models.

NICE Knowledge and Skill Statements:

K0238

Mobile Application Pentesting

SKILL PATH

The Mobile Application Pentesting skill path teaches you how to discover and exploit vulnerabilities in mobile apps. You'll learn how to use popular penetration testing tools to perform an analysis of mobile applications, assess their weaknesses and better defend them from malicious attacks.

Mobile Application Pentesting Project

Project | 4 hours

Practice your mobile application pentesting skills by working on hands-on exercises.

NICE Knowledge and Skill Statements:

S0001, S0137

Introduction to iOS App Pentesting

Course | 33 minutes

Get an introduction to iOS app pentesting with this course covering analyzing an iOS app, binary analysis, iOS app security measures and more.

NICE Knowledge and Skill Statements:

K0060, K0070, K0224, K0269, K0342, K0438, K0624

iOS App Pentesting Tools and Techniques

Course | 45 minutes

Be ready for action with this course on iOS app pentesting tools and techniques. Covers runtime manipulation, insecure data storage, broken cryptography and other ways to get into a target system.

NICE Knowledge and Skill Statements:

K0060, K0070, K0140, K0177, K0224, K0269, K0342, K0438, K0624, S0051

Introduction to Android App Pentesting

Course | 20 minutes

Prepare for the challenge of Android app pentesting with this introductory course covering reversing Android applications, Drozer and more.

NICE Knowledge and Skill Statements:

K0060, K0070, K0224, K0269, K0342, K0438, K0624

Android App Pentesting Tools and Techniques

Course | 30 minutes

Dive deeper into Android app pentesting with this course on Android app pentesting tools and techniques. Includes vocabulary, walkthroughs and a close look at the Frida pentesting toolkit.

NICE Knowledge and Skill Statements:

K0060, K0070, K0140, K0177, K0224, K0269, K0342, K0624, S0051

Offensive Bash Scripting

SKILL PATH

The Offensive Bash Scripting Learning Path is aimed at beginners and helps you learn one of the many fundamental skills of ethical hacking.

Skill Assessment

Skill assessment | 20 questions

See how your offensive Bash scripting skills stack up against other professionals in your field.

Offensive Bash Scripting Project

Project | 2 hours 58 minutes

This Offensive Bash Scripting Project will put your new skills to the test! Your mission will be to hack the virtual machine named Kioptrix 2.

NICE Knowledge and Skill Statements:

S0051, S0078

Concise History of Linux

Course | 5 minutes

This course is an introduction to offensive Bash scripting and the history of Linux and the Bourne Again shell.

NICE Knowledge and Skill Statements:

K0060

Creating the Lab

Course | 14 minutes

In this course, we'll look at hypervisors and virtual machines. We will install a Kali Linux virtual machine and create a virtual environment in which to practice Bash scripting and ethical hacking.

NICE Knowledge and Skill Statements:

K0130, K0609, K0610, S0073

Introduction to Linux, Bash and Python

Course | 2 hours 58 minutes

This will be an introduction to essential Linux commands, the basics of Bash scripting and Python. We will dig into code strings, variables, conditional statements, functions and more.

NICE Knowledge and Skill Statements:

K0016, K0068, K0129, K0318, K0396, K0529, S0130

User and Group Management

Course | 17 minutes

This course covers basic Linux Administrator tasks. We'll write a Bash script that expedites adding users to a local system, managing those users and enforcing password guidelines as well.

NICE Knowledge and Skill Statements:

K0016, K0068, K0129, K0224, K0396, K0529, K0608, S0067, S0130

File Permission and Process

Course | 26 minutes

In this course, we will segue from user and group management to focusing on file processes and permissions. We will go into the meaning of read, write and execute and more useful terms.

NICE Knowledge and Skill Statements:

K0016, K0068, K0116, K0129, K0224, K0396, K0529, K0608, S0067, S0130

Network Reconnaissance

Course | 28 minutes

Explore the uses of Bash scripts for network reconnaissance, as well as how to edit these scanning tools for class B and class C networks and their subnets.

NICE Knowledge and Skill Statements:

K0177, K0342, K0529, S0051, S0130, S0162

Scripting to Scan Web Applications

Course | 1 hour 2 minutes

In this course, we will utilize the same tools that we created in the previous course and apply them to scanning web applications and discovering vulnerabilities.

NICE Knowledge and Skill Statements:

K0009, K0070, K0339, K0342, K0529, K0624, S0001, S0051, S0081, S0130

Privilege Escalation

Course | 19 minutes

A virtual machine named Kioptrix 4 will be used to demonstrate the process of privilege escalation. You'll walk through a hands-on exercise to learn what is going on and how the process works.

NICE Knowledge and Skill Statements:

K0129, K0177, K0342, K0362, K0529, S0051, S0130

Python for Pentesters

SKILL PATH

Learn the basics of penetration testing in the cloud.

Skill Assessment

Skill assessment | 20 questions

See how your Python pentesting skills stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

Python for Pentesters Project

Project | 43 minutes

Test your skills in this project consisting of five challenges: create an email sender, create a buffer overflow exploit, write commands to conduct a Wi-Fi attack, start a new web scraping project and write a line of smtp code.

NICE Knowledge and Skill Statements:

K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266

Refresher on Python

Course | 3 hours 53 minutes

An introduction to the course and some refreshers on Python.

NICE Knowledge and Skill Statements:

K0004, K0016, K0068, K0372, K0396, S0060, S0266

Common Vulnerabilities Exploitable by Python

Course | 2 hours 20 minutes

This course explores common vulnerabilities and vulnerability exploitation in Python.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0016, K0068, K0070, K0372, K0396, S0060, S0266

Using Python for Network Penetration

Course | 4 hours 19 minutes

In this course, we will explore the uses of Python in penetration testing and attacking.

NICE Knowledge and Skill Statements:

K0004, K0016, K0068, K0070, K0160, K0177, K0221, K0234, K0332, K0362, K0372, K0396, K0408, S0060, S0266

Attacking Web Applications

Course | 1 hour 57 minutes

In this course, you'll explore the ins and outs of attacking web applications with Python.

NICE Knowledge and Skill Statements:

K0004, K0005, K0009, K0016, K0068, K0070, K0372, K0396, K0624, S0060, S0266

Reverse Engineering

SKILL PATH

The Reverse Engineering skill path will enable you to identify malware types, characteristics and behaviors. You will be able to detect, analyze and mitigate malware from any network.

Reverse Engineering Project

Project | 2 hours 57 minutes

Get to grips with a real-world challenge as you reverse-engineer a malware sample.

NICE Knowledge and Skill Statements:

K0171, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270

Malware analysis introduction

Course | 48 minutes

This course is the student's introduction to reverse engineering and malware.

NICE Knowledge and Skill Statements:

K0183, K0184, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131

Basic static analysis

Course | 1 hour 3 minutes

Learn how to conduct basic static analysis on a malicious file to gather information about the malware prior to conducting any dynamic analysis.

NICE Knowledge and Skill Statements:

K0175, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270

Advanced static analysis

Course | 1 hour 29 minutes

VPNs (virtual private networks) are essential to secure remote access of your network, and in this course we'll be focused on how to lock down your network using VPN tunnels and different remote access technologies.

NICE Knowledge and Skill Statements:

K0175, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270

Basic dynamic analysis

Course | 1 hour 20 minutes

In this course, you'll get to grips with malware and basic dynamic analysis.

NICE Knowledge and Skill Statements:

K0175, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270

Advanced dynamic analysis

Course | 2 hours 33 minutes

complete understanding of a malicious file can be best achieved during advanced dynamic analysis.

NICE Knowledge and Skill Statements:

K0175, K0183, K0188, K0189, K0259, K0479, K0480, S0003, S0087, S0131, S0270

Reporting and mitigation

Course | 21 minutes

In this course, the student will explore reporting, mitigation techniques and demonstrating mitigation.

NICE Knowledge and Skill Statements:

K0315, K0354, K0355, K0451, K0468, S0003

Web Application Pentesting

SKILL PATH

The web application penetration testing path will cover all of the essentials for those wanting to become a web app pentester. You'll learn how to ethically emulate real-world attacks in order to discover and responsibly disclose an organization's vulnerabilities.

Skill Assessment

Skill assessment | 20 questions

See how your web application pentesting skills stack up against other professionals in your field.

Purple Team Web Application Security Project

Project | 2 hours 34 minutes

This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application.

NICE Knowledge and Skill Statements:

S0022, S0025, S0051, S0084, S0172, S0174, S0293

Introduction to Web Application Pentesting

Course | 60 minutes

This course introduces students to the learning path and walks them through getting their own workstation set up and configured for use throughout the rest of the path's courses.

NICE Knowledge and Skill Statements:

K0206, K0342, K0624

OWASP Top Ten

Course | 9 hours 16 minutes

In the second course, many real-world vulnerabilities are showcased for each of the ten topics and various demos are given on how to solve related challenges in both OWASP Juice Shop and Portswigger's Web Security Academy.

NICE Knowledge and Skill Statements:

K0005, K0007, K0069 , K0070, K0624, S0001, S0130

Tool Setup and Usage

Course | 2 hours 29 minutes

The third course covers a variety of pentesting tools and Burp extensions, such as Autorize, C02, Backslash Powered Scanner, Turbo Intruder, Intruder File Payload Generator, SQLMap and many more.

NICE Knowledge and Skill Statements:

K0131, K0182, K0301, K0342, S0051, S0057, S0081, S0173

Conclusion to Web App Pentesting

Course | 1 hour 36 minutes

This course offers the student important advice on pentesting, a path recap and a close look at the learning path's final project.

NICE Knowledge and Skill Statements:

K0005, K0206, K0342, K0624

Threat intelligence, incident response and forensics

Threat intelligence, incident response and forensics training includes a variety skills related to identifying, responding to and analyzing cybersecurity incidents. It covers different types of cyberattacks and threats, the processes and policies to mitigate those threats, how to extract and report on cybercrime evidence, and more.

Advanced Adversary Tactics

SKILL PATH

The Advanced Adversary Tactics Path will give an overview of techniques and tactics used by real-world adversaries. Through completely hands-on exercises you'll get experience with some of the most common methods adversary groups use to gain access to networks and machines by trying them out yourself.

Reconnaissance and Resource Development

Course | 29 minutes

Learn some of the techniques attackers use to gain information and phish before an attack.

Initial Access, Execution, and Persistence

Course | 3 hours 27 minutes

Get hands-on experience with some of the methods used to gain initial access to a system, execute code, and gain persistence. Learn how to implant a trojanized binary, hide a reverse shell in start-up folders and files, pivot between networks, and more.

CERT-Certified Computer Security Incident Handler (CSIH)

CERTIFICATION PATH

The Certified Computer Security Incident Handler (CSIH) certification path covers the essential information you need to know in order to properly detect, contain and mitigate security incidents. You'll learn the ins and outs of incident response, as well as the tools of the trade used by incident responders on a daily basis.

CSIH Practice Exam

Practice Exam | 30 questions

Prepare for your CSIH exam and test your domain knowledge.

Network Traffic Analysis Cyber Range

Cyber range | 12 labs

Gain practical experience and build your real-world network traffic analysis skills through 12 hands-on labs in the Network Traffic Analysis Cyber Range.

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221

Building Incident Response Team

Course | 31 minutes

Review the most important aspects of incident response team members, such as technical skills, personal skills and critical knowledge.

NICE Knowledge and Skill Statements:

K0004, K0231, K0292

Reverse Engineering Concepts

Course | 33 minutes

Get to grips with the details of reverse-engineering concepts in this three-video course. Includes demonstration and tool lists.

NICE Knowledge and Skill Statements:

K0004, K0171, K0175, S0270

Cell Phone Forensics

Course | 28 minutes

Refresh your knowledge of cell phone forensics with this course covering Andriod and iPhone forensics challenges and best practices.

NICE Knowledge and Skill Statements:

K0004, K0017, K0118, K0122, K0128, K0269, K0433, K0438, K0573, S0075, S0090, S0091

Windows Swap File

Course | 27 minutes

Get familiar with the Windows swap file, a great place for evidence to hide. Includes tools and demonstration video.

NICE Knowledge and Skill Statements:

K0004, K0017, K0118, K0122, K0128, K0192, K0433, K0573, S0067, S0075

Memory Forensics

Course | 1 hour 19 minutes

Two videos take you through the fundamentals of memory forensics, including tools, techniques for dumping memory and an in-depth demonstration.

NICE Knowledge and Skill Statements:

K0004, K0017, K0118, K0122, K0128, K0433, K0573, S0062, S0075, S0091

Dealing with Passwords and Encryption

Course | 33 minutes

Deal with passwords and encryption with the help of this course covering password-cracking, public and private keys, Kerberos and more.

NICE Knowledge and Skill Statements:

K0004, K0007, K0018, K0019, K0056, K0060, K0427, S0043, S0298

Disk Forensics

Course | 55 minutes

Dive into disk forensics with this course covering bit images, restoring disk images, slack, steganography and more.

NICE Knowledge and Skill Statements:

K0004, K0017, K0038, K0117, K0118, K0122, K0128, K0129, K0132, K0133, K0304, K0433, K0573, K0622

Role of the Computer Forensic Examiner

Course | 40 minutes

Get to grips with the role of the computer forensics examiner, including duties and potential legal concerns.

NICE Knowledge and Skill Statements:

K0004, K0150, K0233, K0579

Cyber Attacks Overview

Course | 1 hour 14 minutes

Review the fundamentals of cyber-attacks with two videos on risks, attack types and the anatomy of an attack.

NICE Knowledge and Skill Statements:

K0004, K0070, K0106, K0160, K0161, K0162, K0177, K0362, K0436, K0480, K0604

Incident Response Process

Course | 1 hour 1 minute

Six videos take you through the details of the incident response process, including important tools, policies, strategies and legal concerns.

NICE Knowledge and Skill Statements:

K0004, K0042, K0231, K0292, K0317, K0399, S0365

Introduction to Incident Response

Course | 56 minutes

Get on overview of incident response, including how to respond to security incidents and common incident response definitions and concepts.

NICE Knowledge and Skill Statements:

K0004

Stages of Incident Response

Course | 1 hour

Review the stages of incident response in two separate models, covering the details and concerns for each phase.

NICE Knowledge and Skill Statements:

K0004, K0042, K0231, K0292, K0317, K0399, S0365

Email Analysis

Course | 21 minutes

Explore forensic email analysis with this course covering the structure, function and details of email.

NICE Knowledge and Skill Statements:

K0004, K0192, K0268, K0332, K0444, K0447, K0449, K0565, S0071

Web Traffic Analysis

Course | 13 minutes

Dig into Web traffic analysis with this course covering write protection, Web forensics and cookies.

NICE Knowledge and Skill Statements:

K0004, K0061, K0179, K0255, K0274, K0332, K0444, K0471, K0486, K0489, K0565, K0603

Wireless Analysis

Course | 38 minutes

Take a moment to refresh your knowledge of wireless analysis. Includes vocabulary, examples and diagrams.

NICE Knowledge and Skill Statements:

K0004, K0056, K0093, K0108, K0113, K0137, K0138, K0274, K0375, K0428, K0438, K0445, K0446, K0556, K0560, K0614, S0138

Protocol Analysis

Course | 19 minutes

Get to grips with protocol analysis through this course on TCP/IP concepts, routing, vocabulary and functions.

NICE Knowledge and Skill Statements:

K0004, K0061, K0185, K0192, K0301, K0332, K0471, K0555, K0565, S0081

Log Analysis

Course | 39 minutes

Log analysis counts for a lot in an investigation. Learn to maximize your analysis process with this course covering log management, auditing, steps, concerns and more.

NICE Knowledge and Skill Statements:

K0004, K0061, K0084, K0132, K0145, K0177, K0301, K0318, K0363, K0452, S0046, S0081, S0173, S0192, S0267

Network Security Technologies

Course | 30 minutes

Two videos reintroduce you to network security technologies, including tool families, uses and examples.

NICE Knowledge and Skill Statements:

K0004, K0007, K0011, K0056, K0061, K0111, K0158, K0180, K0221, K0324, K0334, K0336, K0452, K0516, S0136

Network Forensics Concepts

Course | 50 minutes

Develop your knowledge of network forensics concepts, tools and techniques as you progress through this five-video course.

NICE Knowledge and Skill Statements:

K0004, K0017, K0118, K0122, K0128, K0129 , K0132, K0133, K0179, K0255, K0304, K0433, K0486, K0489, K0573

Networking Fundamentals

Course | 31 minutes

Build a foundational knowledge of networking in this overview course covering key networking concepts and practices.

NICE Knowledge and Skill Statements:

K0001, K0004, K0007, K0011, K0034, K0047, K0056, K0061, K0065, K0179, K0221, K0255, K0332, K0395, K0471, K0486, K0489, K0491, K0565

CompTIA Cybersecurity Analyst (CySA+)

CERTIFICATION PATH

The CompTIA Cybersecurity Analyst (CySA+) certification path teaches you how to use behavioral analytics to prevent, detect and combat cyber threats. You'll learn how to configure and use threat detection tools, perform data analysis to identify threats and secure applications and systems.

CySA+ Practice Exam

Practice Exam | 150 questions

Prepare for your CySA+ exam and test your domain knowledge.

Introduction to CySA+

Course | 7 minutes

This two-video course is a brief introduction to the CySA+ course pathway, including the four CySA+ domains.

Introduction to Threat Management

Course | 41 minutes

Explore threat management with nine videos on key concepts such as the CIA triad, risk management controls and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0151, K0162, K0165, K0339, K0344, K0362, K0474, K0527, K0548, K0604, K0612

Network Based Threats

Course | 26 minutes

Five videos give you a step up on network-based threats. Includes information on secure endpoint management, firewall types and types of risk controls.

NICE Knowledge and Skill Statements:

K0007, K0049, K0065, K0167, K0205, K0487, K0488, K0561, K0603, K0612

Securing Corporate Environment

Course | 16 minutes

Refresh your knowledge of securing corporate environments, with a special focus on pentesting and analysis.

NICE Knowledge and Skill Statements:

K0175, K0183, K0342

Environmental Reconnaissance Techniques and Analysis

Course | 57 minutes

Sixteen videos take you through the details of environmental reconnaissance techniques and analysis, including tools and vocabulary.

NICE Knowledge and Skill Statements:

K0177, K0191, K0192, K0342, K0409, K0447, K0460, K0535, K0536, K0565

Vulnerability Management Process

Course | 55 minutes

Brush up on your knowledge of vulnerability management with fifteen videos on policy requirements, scanning and more.

NICE Knowledge and Skill Statements:

K0002, K0003, K0013, K0040, K0065, K0070, K0106, K0161, K0162, K0177, K0272, K0339, K0624, S0167

Analyzing Vulnerability Scan Results

Course | 28 minutes

Five videos help you raise your knowledge of analyzing vulnerability scan results. Explore the details of CVSS, validation of results and more.

NICE Knowledge and Skill Statements:

K0272, K0339, S0167

Common Vulnerabilities

Course | 28 minutes

Refresh your knowledge of common vulnerabilities with six videos on the many different types and sources of system weak spots.

NICE Knowledge and Skill Statements:

K0009, K0070, K0106, K0362, K0603, K0604, K0624

Incident Response Process

Course | 41 minutes

The incident response process is explored in seven videos on incident response teams, security incidents, response phases and more.

NICE Knowledge and Skill Statements:

K0041, K0042, K0150, K0292, K0317

Analyzing Common Symptoms

Course | 34 minutes

Six videos help you take your knowledge of common symptom analysis to the next level. Focuses on networks, servers and monitoring tools.

NICE Knowledge and Skill Statements:

K0106, K0145, K0301, K0339, K0362, K0567, K0603

Digital Forensics Tools and Investigation Techniques

Course | 32 minutes

Learn more about digital forensic tools and investigation techniques with this seven-video course.

NICE Knowledge and Skill Statements:

K0017, K0118, K0122, K0128, K0129, K0132, K0133, K0134, K0304, K0433, K0573

Incident Recovery and Post-Incident Response Process

Course | 18 minutes

Three videos explore incident recovery and the challenges of the post-incident response process.

NICE Knowledge and Skill Statements:

K0026, K0042, K0150, K0292, K0317, K0381

Frameworks, Policies, Controls and Procedures

Course | 36 minutes

Explore more about security architecture with this course on frameworks, policies, controls and procedures.

NICE Knowledge and Skill Statements:

K0003, K0004, K0047, K0065, K0112, K0199, K0242, K0432, K0504

Security Architecture Review and Compensating Controls

Course | 32 minutes

Seven videos take you through the details of security architecture review and compensating controls, including common issues, separation of duties, trend analysis and more.

NICE Knowledge and Skill Statements:

K0004, K0033, K0065, K0112, K0145, K0165, K0179, K0245, K0333

Identity and Access Management Security

Course | 58 minutes

Eleven videos reintroduce you to the details of identity and access management security.

NICE Knowledge and Skill Statements:

K0007, K0032, K0044, K0056, K0065, K0112, K0158, K0336, K0362, K0452

Implementing Security Best Practices in SDLC

Course | 44 minutes

Review and update your knowledge of implementing best practices in software development with six videos on coding for security, software development models and more.

NICE Knowledge and Skill Statements:

K0039, K0079, K0080, K0081, K0082, K0153, K0178, K0186, K0624

CySA+ Conclusion

Course | 18 minutes

Top off your CySA+ study with a review of performance-based questions.

NICE Knowledge and Skill Statements:

Computer Forensics

SKILL PATH

The Computer Forensics skill path teaches you critical techniques about identifying, preserving, extracting, analyzing and reporting forensic evidence through use of the most popular computer forensic tools.

Skill Assessment

Skill assessment | 20 questions

See how your computer forensics skills stack up against other professionals in your field.

Computer Forensics Cyber Range

Cyber range | 6 labs

Gain practical experience and develop your command line skills through 10 hands-on labs in the Command Line Basics Cyber Range.

NICE Knowledge and Skill Statements:

S0062, S0071, S0091, S0267

Computer Forensics as a Profession

Course | 27 minutes

Learn what it's like to be a computer forensics professional in this introductory course covering duties, procedures and practical advice.

NICE Knowledge and Skill Statements:

K0017, K0118, K0304

Digital Evidence and Legal Issues

Course | 1 hour 52 minutes

Explore potential legal issues related to digital evidence, review citizens' rights and gain insight into real-world cases in this computer forensics course.

NICE Knowledge and Skill Statements:

K0123, K0156, K0168

Computer Forensics Investigations

Course | 2 hours 21 minutes

Take a deep dive into the process of conducting computer forensics investigations, including procedures, methodology, tools and reporting.

NICE Knowledge and Skill Statements:

K0017, K0107, K0118, K0125, K0133, K0185, K0304, K0573, S0047, S0068, S0071

Aspects of Hard Drives

Course | 44 minutes

Learn about technical aspects of hard drives and how they relate to computer forensics as you progress through this course.

NICE Knowledge and Skill Statements:

K0122, K0128, K0133, K0449

File Systems

Course | 45 minutes

Learn all about file systems, including essential topics related to finding and uncovering data, as well as the tools used to do so.

NICE Knowledge and Skill Statements:

K0117, K0122, K0128, K0132, K0182

Email and Browser Forensics

Course | 2 hours

Explore a variety of concepts around email and browser forensics and learn how those concepts are applied in this eleven-video course.

NICE Knowledge and Skill Statements:

K0131, K0133, S0065

Network Forensics Concepts

Course | 50 minutes

Develop your knowledge of network forensics concepts, tools and techniques as you progress through this five-video course.

NICE Knowledge and Skill Statements:

K0001, K0100, K0122, K0371, S0120

Data Hiding

Course | 40 minutes

Explore how cryptographic hashing, stenography and other techniques are used to hide data, as well as how that data can be discovered.

NICE Knowledge and Skill Statements:

K0184, K0305, S0071, S0092

Memory Forensics

Course | 19 minutes

Learn all about memory forensics, including using popular tools, conducting live analysis and carrying out basic forensics processes in this brief course.

NICE Knowledge and Skill Statements:

K0268, S0062, S0090, S0091

Passwords and Encryption

Course | 49 minutes

Discover key forensics concepts and best practices related to passwords and encryption, including how to gain access to a suspect's device.

NICE Knowledge and Skill Statements:

K0017, K0132

New and Emerging Technologies

Course | 1 hour 5 minutes

Explore how new and emerging technologies are affecting forensics, including virtualization, social networks and gaming.

NICE Knowledge and Skill Statements:

K0130, K0610, S0090

Introduction to Mobile Forensics

Course | 43 minutes

Get an introduction to mobile forensics and the challenges mobile devices present to investigators in this overview course.

NICE Knowledge and Skill Statements:

K0438, S0075

File and Operating System Forensics

Course | 1 hour 24 minutes

Explore a variety of concepts around file and operating forensics and learn how those concepts are applied in this eight-video course.

NICE Knowledge and Skill Statements:

K0122, K0132, K0449, K0573

Cyber Threat Hunting

SKILL PATH

The Cyber Threat Hunting Learning Path helps you master a repeatable, documentable cyber threat hunting methodology. You'll learn how to leverage a variety of tools to assist with your cyber threat hunting activities.

Skill Assessment

Skill assessment | 20 questions

See how your cyber threat hunting skills stack up against other professionals in your field.

Cyber Threat Hunting Project

Project | 2 hours 31 minutes

Use your cyber threat hunting skills to identify network traffic patterns for anomalies and investigate malware. You'll use Wireshark to examine packet capture files for potential red flags. Then you'll attempt to piece together the threat.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258

Introduction to Cyber Threat Hunting Techniques

Course | 57 minutes

Increase your knowledge of cyber threat hunting techniques and resources available. Here, we will introduce you to the Cyber Threat Hunter.

NICE Knowledge and Skill Statements:

K0004, K0579

Detection

Course | 2 hours 24 minutes

In order to have an effective threat-hunting program, the hunter needs access to the tools and data necessary to perform these tasks. The best open-source tools are free and only work on Linux. Let's talk about some of those tools.

NICE Knowledge and Skill Statements:

K0004, K0013, K0111, K0129, K0145, K0229, K0318, K0334, K0339, K0603, S0081

Investigation Process

Course | 1 hour 10 minutes

The purpose of this course is to help the threat hunter to identify whether the anomalous activity is a threat. Explore how to investigate, walking through the information and identifying any issues right away.

NICE Knowledge and Skill Statements:

K0058, K0107, K0122, K0334, K0362, K0481, K0523, K0603, S0184, S0258

Remediate the Malware

Course | 25 minutes

Go through the skills and tools needed to identify and remediate malware. You'll look at identifying malware propagation techniques, ensuring it doesn't spread, preventing future infiltration attempts and more.

NICE Knowledge and Skill Statements:

K0026, K0205, K0231, K0362, K0406, K0479, K0480, K0481, K0523

Attack Simulators and Exercises

Course | 1 hour 2 minutes

In this course, we will be looking at attack simulators, which will be used to test your monitoring and alerting solutions.

NICE Knowledge and Skill Statements:

K0106, K0117, K0161, K0362, K0469, S0044, S0078

Cyber Threat Hunting Review

Course | 9 minutes

Review the steps of cyber threat hunting: Detect, Investigate and Response/Remediation. Finally, you'll recap on the threat hunter's duties and responsibilities in preparation for the final project.

NICE Knowledge and Skill Statements:

K0150

Digital Forensics Concepts

SKILL PATH

In the Digital Forensics Concepts path, the student will learn about legal considerations applicable to computer forensics and how to identify, collect and preserve digital evidence.

Digital Forensics Project

Project | 2 hours 38 minutes

Practice your digital forensics knowledge with this project.

NICE Knowledge and Skill Statements:

K0005, K0017, K0118, K0128, K0133, K0134, K0182, K0187, K0304, S0047, S0065, S0071

Introduction to Digital Forensics

Course | 33 minutes

This intro course provides a broad overview of computer forensics as an occupation by exploring methodologies used surrounding digital forensics.

NICE Knowledge and Skill Statements:

K0001, K0004, K0017, K0060, K0304, S0131

Legal considerations and search authority

Course | 39 minutes

This course demonstrates information commonly needed in a search warrant and a preservation request.

NICE Knowledge and Skill Statements:

K0003, K0017, K0123, K0125, K0155, K0156, K0168, K0304, S0047, S0133

The investigative process

Course | 16 minutes

This course covers scientific principles that apply to digital forensics.

NICE Knowledge and Skill Statements:

K0005, K0017, K0078, K0118, K0119, K0122, K0132, K0133, K0134, K0304, S0032, S0047, S0069, S0091, S0133

Recognizing and collecting digital evidence

Course | 27 minutes

This course explores what to bring to a scene and how to prepare and label digital evidence for documentation purposes.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0122, K0125, K0128, K0131, K0132, K0133, K0145, K0182, S0065, S0068, S0071, S0075, S0090, S0091

Preservation of evidence/On scene triage

Course | 27 minutes

This course discusses capturing RAM, recognizing and dealing with encryption and destructive processes and triaging devices with a forensic boot media.

NICE Knowledge and Skill Statements:

K0002, K0004, K0042, K0060, K0070, K0078, K0109, K0117, K0179, K0183, K0186, K0187, K0188, K0254, K0301, K0372, K0573, S0062, S0067, S0069, S0074, S0087, S0091, S0131, S0156, S0266

Hash values and file hashing

Course | 20 minutes

In this course, the student learns how to use hash values as a way to include or exclude files from an investigation.

NICE Knowledge and Skill Statements:

K0070, K0117, K0187, K0277, K0396, S0089, S0298

Creating a disk image

Course | 1 hour 1 minute

This course explains the importance of sterilizing media, how to validate tools, proper application of the write-blocker and validating the forensic bit-stream copy.

NICE Knowledge and Skill Statements:

K0017, K0070, K0118, K0119, K0128, K0132, K0182, K0185, K0187, K0372, K0573, S0047, S0065, S0071, S0075, S0091

Key word and grep searches

Course | 33 minutes

Explore the details of keyword and grep searches.

NICE Knowledge and Skill Statements:

K0070, K0131, K0185, K0535, S0011, S0195, S0220

Network basics

Course | 25 minutes

A look at network basics for the computer forensics investigator.

NICE Knowledge and Skill Statements:

K0001, K0004, K0034, K0058, K0106, K0179, K0221, K0332, K0393, K0471, K0489, K0565, S0187, S0236

Reporting and peer review

Course | 28 minutes

In this course, the student examiner learns what information to include and what does not belong in a final report.

NICE Knowledge and Skill Statements:

K0315, K0354, K0451, S0003

Cybersecurity Data Science

SKILL PATH

Learn everything you need to employ the latest cutting edge tools in cybersecurity data science in this hands-on, comprehensive skill path. You will set up a cybersecurity lab, construct classifiers to detect malware, utilize deep learning technology and even hack security systems with the help of machine learning.

Skill Assessment

Skill assessment | 20 questions

See how your cybersecurity data science skills stack up against other professionals in your field.

Cybersecurity Data Science Project

Project | 2 hours 12 minutes

Practice your Cybersecurity Data Science skills by solving challenges.

NICE Knowledge and Skill Statements:

S0087, S0252, S0257

Preparation for Cybersecurity Data Science

Course | 42 minutes

Set up your cybersecurity lab and acquire the background knowledge essential to success in Cybersecurity Data Science.

NICE Knowledge and Skill Statements:

K0238, K0476, K0609, K0610, S0073

Malware Detection via Machine Learning

Course | 43 minutes

Gain a practical understanding of the most successful techniques used by Cybersecurity Data Science experts for the crafting of malware classifiers.

NICE Knowledge and Skill Statements:

K0189, K0238, K0259, K0479, K0480, S0131

Machine Learning for Intrusion Detection

Course | 11 minutes

Master the most important use cases for preventing hackers, spammers and criminals from entering your network uninvited.

NICE Knowledge and Skill Statements:

K0046, K0058, K0238, K0301, K0334, S0258, S0280

Machine Learning for Social Engineering

Course | 16 minutes

Expand the impact of your social engineering by arming yourself with the latest machine learning-based social engineering tools and methods.

NICE Knowledge and Skill Statements:

K0238, K0476, K0603, S0052

Machine Learning for Pentesting

Course | 17 minutes

Employ machine learning to take your penetration testing to the next level by unlocking information and access thought impenetrable before.

NICE Knowledge and Skill Statements:

K0177, K0238, K0342, K0493, K0603, S0051, S0081

Certified Computer Forensics Examiner (CCFE)

CERTIFICATION PATH

The Certified Computer Forensics Examiner (CCFE) certification path teaches you the skills needed to investigate computer threats. You'll learn about performing forensics on hard drives, file systems and networks as well as the legal and ethical issues of investigating cybercrime.

Skill Assessment

Skill assessment | 20 questions

See how your CCFE skills stack up against other professionals in your field.

CCFE Practice Exam

Practice Exam | 50 questions

Prepare for your CCFE exam and test your domain knowledge.

Computer Forensics Cyber Range

Cyber range | 6 labs

Gain practical experience and develop your computer forensics skills through six hands-on labs in the Computer Forensics Cyber Range.

NICE Knowledge and Skill Statements:

S0062, S0071, S0091, S0267

Computer Forensics as a Profession

Course | 27 minutes

Learn what it's like to be a computer forensics professional in this introductory course covering duties, procedures and practical advice.

NICE Knowledge and Skill Statements:

K0017, K0118, K0304

Digital Evidence and Legal Issues

Course | 1 hour 52 minutes

Explore potential legal issues related to digital evidence, review citizens' rights and gain insight into real-world cases in this computer forensics course.

NICE Knowledge and Skill Statements:

K0123, K0156, K0168

Aspects of Hard Drives

Course | 44 minutes

Learn about technical aspects of hard drives and how they relate to computer forensics as you progress through this course.

NICE Knowledge and Skill Statements:

K0122, K0128, K0133, K0449

File Systems

Course | 45 minutes

Learn all about file systems, including essential topics related to finding and uncovering data, as well as the tools used to do so.

NICE Knowledge and Skill Statements:

K0117, K0122, K0128, K0132, K0182

Email and Browser Forensics

Course | 2 hours

Explore a variety of concepts around email and browser forensics and learn how those concepts are applied in this eleven-video course.

NICE Knowledge and Skill Statements:

K0131, K0133, S0065

Network Forensics Concepts

Course | 50 minutes

Develop your knowledge of network forensics concepts, tools and techniques as you progress through this five-video course.

NICE Knowledge and Skill Statements:

K0001, K0100, K0122, K0371, S0120

Data Hiding

Course | 40 minutes

Explore how cryptographic hashing, stenography and other techniques are used to hide data, as well as how that data can be discovered.

NICE Knowledge and Skill Statements:

K0184, K0305, S0071, S0092

Memory Forensics

Course | 19 minutes

Learn all about memory forensics, including using popular tools, conducting live analysis and carrying out basic forensics processes in this brief course.

NICE Knowledge and Skill Statements:

K0268, S0062, S0090, S0091

Passwords and Encryption

Course | 49 minutes

Discover key forensics concepts and best practices related to passwords and encryption, including how to gain access to a suspect's device.

NICE Knowledge and Skill Statements:

K0017, K0132

New and Emerging Technologies

Course | 1 hour 5 minutes

Explore how new and emerging technologies are affecting forensics, including virtualization, social networks and gaming.

NICE Knowledge and Skill Statements:

K0130, K0610, S0090

Introduction to Mobile Forensics

Course | 43 minutes

Get an introduction to mobile forensics and the challenges mobile devices present to investigators in this overview course.

NICE Knowledge and Skill Statements:

K0438, S0075

File and Operating System Forensics

Course | 1 hour 24 minutes

Explore a variety of concepts around file and operating forensics and learn how those concepts are applied in this eight-video course.

NICE Knowledge and Skill Statements:

K0122, K0132, K0449, K0573

Computer Forensics Investigations

Course | 2 hours 21 minutes

Take a deep dive into the process of conducting computer forensics investigations, including procedures, methodology, tools and reporting.

NICE Knowledge and Skill Statements:

K0017, K0107, K0118, K0125, K0133, K0185, K0304, K0573, S0047, S0068, S0071

Certified Mobile Forensics Examiner (CMFE)

CERTIFICATION PATH

The Certified Mobile Forensics Examiner (CMFE) certification path prepares you for the CMFE certification exam by teaching the necessary skills to investigate mobile threats and mobile cybercrime.

Skill Assessment

Skill assessment | 20 questions

See how your CMFE skills stack up against other professionals in your field.

CMFE Practice Exam

Practice Exam | 75 minutes

Prepare for your CMFE exam and test your domain knowledge.

Introduction to Mobile Forensics

Course | 43 minutes

Get an introduction to mobile forensics and the challenges mobile devices present to investigators in this overview course.

NICE Knowledge and Skill Statements:

K0138, K0269, K0438

Mobile Forensics Process

Course | 1 hour 30 minutes

Mobile forensics comes with a unique set of challenges. Explore those challenges with this course on the mobile forensics process, including phone types, volatile data recovery and evidence handling.

NICE Knowledge and Skill Statements:

K0017, K0060, K0118, K0122, K0128, K0133, K0134, K0269, K0433, K0438, K0449, K0573, S0047

Android Forensics

Course | 2 hours 2 minutes

Explore the challenges of Android mobile forensics with this course covering Android security, structure, challenges and more.

NICE Knowledge and Skill Statements:

K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091

iOS Forensics

Course | 1 hour 22 minutes

Dive deep into the details of iOS forensics with this course covering iOS structure, system security, passcodes and more.

NICE Knowledge and Skill Statements:

K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091

Windows Phone and Feature Phone Forensics

Course | 51 minutes

Discover the possible difficulties of rare models with this course on Windows Phone and feature phone forensics.

NICE Knowledge and Skill Statements:

K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091

Certified Reverse Engineering Analyst (CREA)

CERTIFICATION PATH

The Certified Reverse Engineering Analyst (CREA) certification path teaches you the analysis skills to discover the true nature of any Windows binary. You'll learn how to analyze hostile code and malware, vulnerabilities in binaries, and business intelligence used by hackers and Trojan writers.

Skill Assessment

Skill assessment | 20 questions

See how your CREA skills stack up against other professionals in your field.

CREA Practice Exam

Practice Exam | 50 questions

Prepare for your CREA exam and test your domain knowledge.

Introduction to Malware Analysis

Course | 28 minutes

Explore malware analysis with a course covering static and dynamic analysis, tools, malware types and analysis methodologies.

NICE Knowledge and Skill Statements:

K0259

Introduction to Reverse Engineering

Course | 47 minutes

Take a closer look at the art and science of reverse-engineering with a course on machine code, assembly language, system-level reversing and more.

NICE Knowledge and Skill Statements:

K0175, K0372

Disassembly

Course | 47 minutes

Examine the intricacies of assembly and disassembly in an X86 context. Includes videos on arithmetic instructions, logical instructions and operands.

NICE Knowledge and Skill Statements:

K0051

Reversing Tools

Course | 32 minutes

Explore the intricacies of multiple reversing tools, beginning with a close look at Interactive Dissasembler (IDA).

NICE Knowledge and Skill Statements:

K0188

C Code in Assembly

Course | 48 minutes

Take a closer look at C code in assembly, including loops, linked lists, stacks and heaps.

NICE Knowledge and Skill Statements:

K0068

Windows Internals

Course | 33 minutes

Explore the reverse-engineering of Windows with this course on Windows internals such as network APIs and services.

NICE Knowledge and Skill Statements:

K0608

Debugging

Course | 41 minutes

A close and personal look at debugging, with nine videos taking you through stepping, breakpoints and exceptions and more. Includes in-depth examples.

NICE Knowledge and Skill Statements:

K0079, K0186, S0014, S0093

Common Malware Behavior

Course | 55 minutes

Improve your malware-hunting skills with a course on injection types, network functions and other fundamentals of malware behavior.

NICE Knowledge and Skill Statements:

K0259, K0392, K0479, K0480, K0536, S0087, S0131

Reversing Rootkits

Course | 11 minutes

Look more closely at the challenge of reversing rootkits with four videos on rootkit structure and behavior.

NICE Knowledge and Skill Statements:

K0392, K0479

Anti-Disassembly, Anti-Debugging and Anti-VM

Course | 32 minutes

Malware doesn't want to be disassembled, and it's going to fight you. Seven videos examine anti-disassembly, anti-debugging and anti-VM strategies used by malware.

NICE Knowledge and Skill Statements:

K0189, K0479, S0093

Packed Malware

Course | 16 minutes

Sometimes, malware is just hiding. Four videos examine the issue of packed malware, including tools, tricks and popular packers.

NICE Knowledge and Skill Statements:

K0479, S0093, S0270

Obfuscation, Encoding and Encryption

Course | 40 minutes

Reintroduce yourself to three ways malware disguises itself: obfuscation, encoding and encryption.

NICE Knowledge and Skill Statements:

S0092, S0093, S0095

Reversing C++

Course | 27 minutes

Our four-video course will reintroduce you to the art of reversing C++.

NICE Knowledge and Skill Statements:

K0068

Reversing 64-bit Malware

Course | 14 minutes

Two videos take you through the ins and outs of reversing 64-bit malware, including functions, code samples and tools.

NICE Knowledge and Skill Statements:

K0479

Incident Response

SKILL PATH

The Incident Response Learning Path will give students the understanding of how incidents are responded to at a high level, as well as allow them to build important technical skills through the hands-on labs and projects.

Skill Assessment

Skill assessment | 20 questions

See how your incident response skills stack up against other professionals in your field.

Network Traffic Analysis Cyber Range

Cyber range | 12 labs

Gain practical experience and build your real-world network traffic analysis skills through 12 hands-on labs in the Network Traffic Analysis Cyber Range.

NICE Knowledge and Skill Statements:

S0046, S0051, S0120, S0156, S0199, S0221

Incident Response Project

Project | 3 hours 6 minutes

Use your incident response skills along with tools like Wireshark, Zeek and Volatility to respond to real-world scenarios.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258, S0269

Introduction to Incident Response

Course | 55 minutes

Review the fundamentals of incident response and learn how to build an IR team and effective playbook for handling incidents.

NICE Knowledge and Skill Statements:

K0026, K0042, K0150, K0412

Stage 1 – Preparation

Course | 33 minutes

This course deals briefly with some common definitions and severity criteria related to incident response. It ends with a high-level explanation of asset inventory and identification.

NICE Knowledge and Skill Statements:

K0004, K0005, K0041, K0106, K0162, K0295, K0361, K0612, S0364

Stage 2 – Identification

Course | 38 minutes

This course explores the process of identifying when there has been an event that falls into the category of becoming an incident. It also touches on classification levels for incidents.

NICE Knowledge and Skill Statements:

K0041, K0381, K0451

Stage 3 – Containment

Course | 37 minutes

Dive into determining what containment steps should be taken and when they should be taken, based on different scenarios.

NICE Knowledge and Skill Statements:

K0041, K0042, K0110, K0480, K0586

Stage 4 – Investigation

Course | 23 minutes

Learn the important role investigation plays in incident response.

NICE Knowledge and Skill Statements:

K0132, K0150, K0292

Stage 5 – Eradication

Course | 27 minutes

Ready to remove the threat from the environment? Learn how to do it right with this course on eradication.

NICE Knowledge and Skill Statements:

K0150, K0210, K0354

Stage 6 – Recovery

Course | 27 minutes

Now that we've eradicated the threats, let's learn how to go into recovery.

NICE Knowledge and Skill Statements:

K0026, K0210, K0292, K0381

Stage 7 – Follow Up/Lessons Learned

Course | 13 minutes

The dust has settled, and the incident is over. In this phase, we deal with assessing our process and looking for ways to improve.

NICE Knowledge and Skill Statements:

K0003, K0287

Technical Deep Dives with Tools of the Trade

Course | 4 hours 1 minute

Dig in for hours of deep-dive technical exercises to master memory, network and host forensics techniques.

NICE Knowledge and Skill Statements:

K0017, K0046, K0058, K0062, K0272, K0343, K0392, S0003, S0046, S0062, S0120, S0199, S0221, S0258, S0261

Malware Analysis & Reverse Engineering

SKILL PATH

This learning path takes a deep dive into taking apart and analyzing malware. As you progress through 12 courses, you'll build your skills and knowledge around the inner-workings of malware, the tools used by malware analysts, and the ins and outs of reversing different types of malware.

Disassembly

Course | 47 minutes

Examine the intricacies of assembly and disassembly in an X86 context. Includes videos on arithmetic instructions, logical instructions and operands.

NICE Knowledge and Skill Statements:

K0051

Reversing Tools

Course | 32 minutes

Explore the intricacies of multiple reversing tools, beginning with a close look at Interactive Dissasembler (IDA).

NICE Knowledge and Skill Statements:

K0188

C Code in Assembly

Course | 48 minutes

Take a closer look at C code in assembly, including loops, linked lists, stacks and heaps.

NICE Knowledge and Skill Statements:

K0068

Windows Internals

Course | 33 minutes

Explore the reverse-engineering of Windows with this course on Windows internals such as network APIs and services.

NICE Knowledge and Skill Statements:

K0608

Debugging

Course | 41 minutes

A close and personal look at debugging, with nine videos taking you through stepping, breakpoints and exceptions and more. Includes in-depth examples.

NICE Knowledge and Skill Statements:

K0079, K0186, S0014, S0093

Common Malware Behavior

Course | 55 minutes

Improve your malware-hunting skills with a course on injection types, network functions and other fundamentals of malware behavior.

NICE Knowledge and Skill Statements:

K0259, K0392, K0479, K0480, K0536, S0087, S0131

Reversing Rootkits

Course | 11 minutes

Look more closely at the challenge of reversing rootkits with four videos on rootkit structure and behavior.

NICE Knowledge and Skill Statements:

K0392, K0479

Anti-Disassembly, Anti-Debugging and Anti-VM

Course | 32 minutes

Malware doesn't want to be disassembled, and it's going to fight you. Seven videos examine anti-disassembly, anti-debugging and anti-VM strategies used by malware.

NICE Knowledge and Skill Statements:

K0189, K0479, S0093

Packed Malware

Course | 16 minutes

Sometimes, malware is just hiding. Four videos examine the issue of packed malware, including tools, tricks and popular packers.

NICE Knowledge and Skill Statements:

K0479, S0093, S0270

Obfuscation, Encoding and Encryption

Course | 40 minutes

Reintroduce yourself to three ways malware disguises itself: obfuscation, encoding and encryption.

NICE Knowledge and Skill Statements:

S0092, S0093, S0095

Reversing C++

Course | 27 minutes

Our four-video course will reintroduce you to the art of reversing C++.

NICE Knowledge and Skill Statements:

K0068

Reversing 64-bit Malware

Course | 14 minutes

Two videos take you through the ins and outs of reversing 64-bit malware, including functions, code samples and tools.

NICE Knowledge and Skill Statements:

K0479

Mobile Forensics

SKILL PATH

The Mobile Forensics skill path teaches you critical techniques about identifying, preserving, extracting, analyzing and reporting forensic evidence found on mobile devices, including Android, iOS, Windows Phone and Feature Phone.

Skill Assessment

Skill assessment | 20 questions

See how your mobile forensics skills stack up against other professionals in your field.

Introduction to Mobile Forensics

Course | 43 minutes

Get an introduction to mobile forensics and the challenges mobile devices present to investigators in this overview course.

NICE Knowledge and Skill Statements:

K0138, K0269, K0438

Mobile Forensics Process

Course | 1 hour 30 minutes

Mobile forensics comes with a unique set of challenges. Explore those challenges with this course on the mobile forensics process, including phone types, volatile data recovery and evidence handling.

NICE Knowledge and Skill Statements:

K0017, K0060, K0118, K0122, K0128, K0133, K0134, K0269, K0433, K0438, K0449, K0573, S0047

Android Forensics

Course | 2 hours 2 minutes

Explore the challenges of Android mobile forensics with this course covering Android security, structure, challenges and more.

NICE Knowledge and Skill Statements:

K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091

iOS Forensics

Course | 1 hour 22 minutes

Dive deep into the details of iOS forensics with this course covering iOS structure, system security, passcodes and more.

NICE Knowledge and Skill Statements:

K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091

Windows Phone and Feature Phone Forensics

Course | 51 minutes

Discover the possible difficulties of rare models with this course on Windows Phone and feature phone forensics.

NICE Knowledge and Skill Statements:

K0060, K0122, K0224, K0269, K0433, K0438, K0449, S0065, S0071, S0091

Network Forensics

SKILL PATH

The Network Forensics skill path helps you fully understand how systems are compromised and what traces are left behind by attackers on the network. You'll learn the concepts, techniques and tools used to analyze logs, protocols, wireless, web traffic and email.

Network Traffic Analysis Cyber Range

Cyber range | 12 labs

Gain practical experience and build your real-world network traffic analysis skills through 12 hands-on labs in the Network Traffic Analysis Cyber Range.

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221, S0258, S0267

Networking Fundamentals

Course | 31 minutes

Build a foundational knowledge of networking in this overview course covering key networking concepts and practices.

NICE Knowledge and Skill Statements:

K0001, K0004, K0007, K0011, K0034, K0047, K0056, K0061, K0065, K0179, K0221, K0255, K0332, K0395, K0471, K0486, K0489, K0491, K0565

Network Forensics Concepts

Course | 50 minutes

Develop your knowledge of network forensics concepts, tools and techniques as you progress through this five-video course.

NICE Knowledge and Skill Statements:

K0004, K0017, K0118, K0122, K0128, K0129 , K0132, K0133, K0179, K0255, K0304, K0433, K0486, K0489, K0573

Network Security Technologies

Course | 30 minutes

Two videos reintroduce you to network security technologies, including tool families, uses and examples.

NICE Knowledge and Skill Statements:

K0004, K0007, K0011, K0056, K0061, K0111, K0158, K0180, K0221, K0324, K0334, K0336, K0452, K0516, S0136

Log Analysis

Course | 39 minutes

Log analysis counts for a lot in an investigation. Learn to maximize your analysis process with this course covering log management, auditing, steps, concerns and more.

NICE Knowledge and Skill Statements:

K0004, K0061, K0084, K0132, K0145, K0177, K0301, K0318, K0363, K0452, S0046, S0081, S0173, S0192, S0267

Protocol Analysis

Course | 19 minutes

Get to grips with protocol analysis through this course on TCP/IP concepts, routing, vocabulary and functions.

NICE Knowledge and Skill Statements:

K0004, K0061, K0185, K0192, K0301, K0332, K0471, K0555, K0565, S0081

Wireless Analysis

Course | 38 minutes

Take a moment to refresh your knowledge of wireless analysis. Includes vocabulary, examples and diagrams.

NICE Knowledge and Skill Statements:

K0004, K0056, K0093, K0108, K0113, K0137, K0138, K0274, K0375, K0428, K0438, K0445, K0446, K0556, K0560, K0614, S0138

Web Traffic Analysis

Course | 13 minutes

Dig into Web traffic analysis with this course covering write protection, Web forensics and cookies.

NICE Knowledge and Skill Statements:

K0004, K0061, K0179, K0255, K0274, K0332, K0444, K0471, K0486, K0489, K0565, K0603

Email Analysis

Course | 21 minutes

Explore forensic email analysis with this course covering the structure, function and details of email.

NICE Knowledge and Skill Statements:

K0004, K0192, K0268, K0332, K0444, K0447, K0449, K0565, S0071

Network Traffic Analysis for Incident Response

SKILL PATH

This learning path covers identification and analysis of benign and malicious traffic, examples and case studies of extracting intelligence from traffic data, considerations when building a network monitoring program, and techniques for collecting and analyzing traffic data.

Skill Assessment

Skill assessment | 20 questions

See how your network traffic analysis skills stack up against other professionals in your field.

Network Traffic Analysis Cyber Range

Cyber range | 12 labs

Gain practical experience and build your real-world network traffic analysis skills through 12 hands-on labs in the Network Traffic Analysis Cyber Range.

NICE Knowledge and Skill Statements:

S0046, S0051, S0120, S0156, S0199, S0221

Network Traffic Analysis Project

Project | 1 hour 29 minutes

Practice your network traffic analysis skills by solving challenges.

NICE Knowledge and Skill Statements:

S0092, S0156, S0199, S0221, S0258, S0269

Introduction to Network Traffic Analysis

Course | 41 minutes

This course provides an introduction to network traffic analysis and describes its primary applications.

NICE Knowledge and Skill Statements:

K0042, K0058, K0334

Fundamentals of Networking

Course | 56 minutes

This course covers the fundamentals of networking and the purposes of various low-level and high-level networking protocols.

NICE Knowledge and Skill Statements:

K0004, K0034, K0061, K0221, K0332, K0471

Hands-On Traffic Analysis in Wireshark

Course | 1 hour 45 minutes

This course provides an introduction to Wireshark and an analysis of some common protocols in Wireshark.

NICE Knowledge and Skill Statements:

K0301, S0046

Alternatives to Wireshark

Course | 31 minutes

This course demonstrates some of the features of tools other than Wireshark for network traffic analysis.

NICE Knowledge and Skill Statements:

K0301, S0046

Network Traffic Intelligence Collection

Course | 1 hour 44 minutes

This course demonstrates tools and techniques for extracting useful intelligence from a network traffic capture.

NICE Knowledge and Skill Statements:

K0301, K0573, S0046

Common Network Threats

Course | 1 hour 23 minutes

This course demonstrates how scanning, data exfiltration, DDoS attacks and attacks against IoT devices can appear in network traffic.

NICE Knowledge and Skill Statements:

K0005, K0160, K0177, K0362, K0392, K0603, K0612

Traffic Analysis Case Studies

Course | 1 hour 6 minutes

This course provides four demonstrations of analysis of network traffic from different malware types.

NICE Knowledge and Skill Statements:

K0191, K0259, K0392, K0479, K0480

Data Collection for Network Traffic Analysis

Course | 1 hour

This course discusses the considerations and available technologies for developing a network traffic analysis program.

NICE Knowledge and Skill Statements:

K0058, K0061, K0143, K0334, K0424

Data Analysis for Network Traffic Analysis

Course | 2 hours 21 minutes

This course covers the fundamentals of connection and statistical and event-based analysis of network traffic data.

NICE Knowledge and Skill Statements:

K0058, K0129, K0301, K0318, K0334, S0046

Paraben DSMO Mobile Operator Certification

CERTIFICATION PATH

The path to becoming a mobile forensic investigator requires fundamental knowledge of devices and the operation of the specialized tools required to process data. The learning path will go through those specialized skills for the operation of Paraben's E3 Forensic Platform in the capture of mobile data as forensic evidence.

Installation

Course | 6 minutes

This introductory certification is designed for those just getting started with mobile forensics and want to learn the process using Paraben's E3 Forensic Platform.

NICE Knowledge and Skill Statements:

K0004, K0182, K0185, K0304, S0069

Licensing

Course | 3 minutes

This section will walk you through the licensing options available for the E3 Forensic Platform. Licensing is determined based on each individual lab design and setup.

NICE Knowledge and Skill Statements:

K0004, K0182, K0185, K0304, S0069

E3:DS Interface

Course | 4 minutes

The interface portion of this course will review the layout of the E3 Forensic Platform and how to do basic navigation in the primary interface.

NICE Knowledge and Skill Statements:

K0004, K0182, K0185, K0304, S0069, S0071

Cases and Adding Evidence

Course | 4 minutes

The Cases and Adding Evidence portion of this course will focus on the creation of cases, addition of investigator details and continue to focus on the addition of evidence.

NICE Knowledge and Skill Statements:

K0004, K0118, K0125, K0155, K0182, K0185, K0304, K0447, K0449, S0047, S0069, S0071, S0120, S0133, S0263

Acquiring Phones

Course | 13 minutes

The Acquisition portion of this course looks at the primary methods to be able to acquire and process a variety of mobile devices in a forensically sound manner.

NICE Knowledge and Skill Statements:

K0004, K0108, K0114, K0118, K0125, K0155, K0182, K0185, K0304, K0447, K0449, S0047, S0069, S0133, S0263

Importing Backups

Course | 2 minutes

The process of importing backups can offer a valuable perspective in an acquisition with iOS devices.

NICE Knowledge and Skill Statements:

K0004, K0108, K0114, K0118, K0182, K0185, K0304, S0047, S0069, S0133

Reviewing the Data

Course | 4 minutes

This course will focus on the methods for reviewing the data to ensure the most valuable information can be found in an examination.

NICE Knowledge and Skill Statements:

K0108, K0114, K0118, K0125, K0155, K0182, K0304, K0447, K0449, S0047, S0069, S0133, S0263

Cloud Data

Course | 3 minutes

This course will focus on data associated with cloud accounts that can be found via access to mobile devices.

NICE Knowledge and Skill Statements:

K0007, K0108, K0114, K0118, K0125, K0155, K0182, K0304, S0047, S0069, S0073, S0133

Searching

Course | 3 minutes

This section will focus on the different searching techniques that can be used when reviewing mobile data.

NICE Knowledge and Skill Statements:

K0007, K0108, K0114, K0118, K0125, K0131, K0155, K0182, K0304, S0047, S0069, S0073, S0133

Bookmarks and Reporting

Course | 3 minutes

This section will focus on the bookmarking and reporting of data associated with mobile devices.

NICE Knowledge and Skill Statements:

K0004, K0182, K0185, K0304, S0069, S0071

Additional Features

Course | 2 minutes

This section will cover unique features that are available when working with mobile devices in forensic investigations.

NICE Knowledge and Skill Statements:

K0118, K0125, K0182, K0304, S0047, S0069, S0133

Paraben P2C Operator Certification

CERTIFICATION PATH

This in-depth learning path leads you on an exploration of the many features and uses of the Paraben E3 Forensic Platform

Introduction to P2C

Course | 3 minutes

This course will introduce you to the basics of the Paraben E3 Forensic Platform.

NICE Knowledge and Skill Statements:

K0004, K0182, K0185, K0304, S0069

Licensing

Course | 3 minutes

A look at licensing the E3 Forensic Platform.

NICE Knowledge and Skill Statements:

K0004, K0182, K0185, K0304, S0069

Interface

Course | 4 minutes

A look at E3 Forensic Platform layout and navigation.

NICE Knowledge and Skill Statements:

K0004, K0182, K0185, K0304, S0069, S0071

Adding evidence

Course | 4 minutes

This course looks at cases and adding evidence.

NICE Knowledge and Skill Statements:

K0004, K0109, K0118, K0125, K0155, K0182, K0185, K0304, K0447, K0449, S0047, S0069, S0071, S0074, S0120, S0133, S0263

Drive triage

Course | 1 minute

A look at data triage.

NICE Knowledge and Skill Statements:

K0004, K0017, K0118, K0122, K0182, K0185, K0304, K0608, S0047, S0065, S0069, S0071, S0133

Registry

Course | 1 minute

Exploring the artifacts in a Windows system registry.

NICE Knowledge and Skill Statements:

K0004, K0017, K0122, K0132, K0185, K0304, K0608, S0065, S0069, S0091, S0133

Data processing

Course | 7 minutes

A look at data optimization techniques.

NICE Knowledge and Skill Statements:

K0004, K0017, K0122, K0182, K0185, K0304, K0608, S0065, S0068, S0069, S0071, S0090, S0091, S0133

Forensic containers

Course | 2 minutes

Data carving in digital forensics.

NICE Knowledge and Skill Statements:

K0004, K0017, K0122, K0182, K0185, K0268, K0304, K0608, S0065, S0068, S0069, S0071, S0090, S0091

Searching and sorting data

Course | 6 minutes

Data carving in digital forensics.

NICE Knowledge and Skill Statements:

K0004, K0017, K0122, K0182, K0185, K0268, K0304, K0608, S0065, S0068, S0069, S0071, S0090, S0091

Bookmarks

Course | 2 minutes

Exploring bookmarking and filtering data.

NICE Knowledge and Skill Statements:

K0004, K0182, K0185, K0304, S0069, S0071

Reporting

Course | 2 minutes

A look at data reporting.

NICE Knowledge and Skill Statements:

K0004, K0182, K0185, K0304, S0069, S0071

Windows Registry Forensics

SKILL PATH

The Windows Registry Forensics learning path will enable you to understand the purpose and structure of the files that create the Windows Registry. You will learn to identify, extract and interpret important data from a live and non-live Windows Registry.

Skill Assessment

Skill assessment | 20 questions

See how your Windows Registry forensics skills stack up against other professionals in your field.

Windows Registry Forensics Project

Project | 2 hours 37 minutes

Practice your Windows Registry forensics skills by solving challenges.

NICE Knowledge and Skill Statements:

S0071, S0091

Introduction to the Windows Registry

Course | 16 minutes

Discover what the Windows Registry is and why it is important in digital forensic investigations.

NICE Knowledge and Skill Statements:

K0060, K0133, K0433

Preparing to Examine the Windows Registry

Course | 57 minutes

This course takes a look at the location of the Registry files within the Windows OS and the many tools freely available to view the file structure and artifacts contained within the Windows Registry.

NICE Knowledge and Skill Statements:

K0132, K0133, K0433, S0069, S0071

NTUser.Dat Hive File Analysis

Course | 2 hours 26 minutes

This course demonstrates an in-depth analysis of the artifacts contained within the NTUser.Dat hive file.

NICE Knowledge and Skill Statements:

K0116, K0128, K0132, K0133, K0433, K0479, S0091

SAM Hive File

Course | 50 minutes

This course explains forensic artifacts found in the SAM (Security Account Manager) file, which stores and organizes information about each user on a system.

NICE Knowledge and Skill Statements:

K0128, K0132, K0133, K0433, S0091

Software Hive File

Course | 1 hour 4 minutes

This course will show examiners how to locate information of forensic value relating to application execution and installation contained within the software hive file.

NICE Knowledge and Skill Statements:

K0128, K0132, K0133, K0433, K0449, S0091

System Hive File

Course | 1 hour 13 minutes

This course will demonstrate evidence of forensic value contained within the system hive file.

NICE Knowledge and Skill Statements:

K0128, K0132, K0133, K0433, K0449, S0091

USRClass.dat Hive File

Course | 33 minutes

This course identifies and explains forensic artifacts found in the UsrClass.dat hive file.

NICE Knowledge and Skill Statements:

K0116, K0128, K0132, K0133, K0433, K0449, S0091

AmCache Hive File

Course | 32 minutes

This course will examine the AmCache hive file, which stores information relating to the execution of applications.

NICE Knowledge and Skill Statements:

K0128, K0132, K0133, K0433, K0449, S0089, S0091

Security architecture, engineering and management

Security architecture, engineering and management training focuses on the design, implementation and maintenance of cybersecurity systems and programs. It covers advanced understanding of information security concepts, security operations and information assurance, as well as risk management and project management skills.

Azure Security Engineer Associate

CERTIFICATION PATH

Students will explore the necessary skills and knowledge to make use of Microsoft Azure. Students will learn how to implement security controls and threat protection, managing identity and access and protecting data, applications and networks in cloud and hybrid environments as part of an end-to-end infrastructure.

Azure Security Engineer Associate Practice Exam

Practice Exam | 21 questions

Prepare for your Azure Security Engineer Associate exam and test your knowledge.

Manage Identity and Access

Course | 1 hour 28 minutes

In this course, students will learn to work with subscriptions, users and groups by configuring Microsoft Azure Active Directory.

Implement platform protection

Course | 3 hours 26 minutes

Learn to implement platform protection.

Manage security operations

Course | 1 hour 48 minutes

Learn how to configure security policies and manage security alerts with the tools and services in Azure.

Secure data and applications

Course | 1 hour 36 minutes

In this course, you will learn harden Azure apps and secure data with encryption, certificates and policies.

Fundamentals of Zero Trust

SKILL PATH

Zero trust changes how we architect and secure digital systems. It is still a relatively young but fast-maturing field. This learning path aims to give you the fundamentals of zero trust, focusing on the architecture itself. You can start your zero trust journey right here or learn to support your organization's zero trust program.

Introduction to Zero Trust

Course | 2 hours 19 minutes

Explore zero trust, including how current traditional security architectures developed, zero trust's roots, core principles and tenets.

Zero trust threat reduction: a ransomware killer?

Course | 30 minutes

Learn how to reduce your enterprise's threat landscape by up to 95% and discover what the White House sees in zero trust for reducing threats to critical national infrastructure. In this course, we assess the threat vectors that zero trust can mitigate and see it in practice with a live demo of how ransomware can be immobilized by micro-segmentation.

Zero trust tenets and NIST high-level architecture

Course | 1 hour 19 minutes

Learn how to understand zero trust architectures via the NIST High Level Design (an abstract conceptual model) as well as how the core principles of zero trust come to life in the tenets of zero trust.

Zero trust enterprise architecture: what are you protecting?

Course | 54 minutes

Zero trust is a unique transformational opportunity for you to rebuild your security architecture. In this course, we will focus on the subjects and resources in your zero trust architecture: what you can protect with zero trust and what you should protect.

Zero trust architecture (ZTA) design patterns

Course | 1 hour 15 minutes

In this course, you'll learn how to discern the differences between different patterns and gain an appreciation for when each should be used.

Zero trust policy

Course | 42 minutes

Here we will discuss types of policy with an example of a zero trust policy versus a legacy policy.

Trust me ... decision & trust algorithms

Course | 53 minutes

Here we will dissect the policy decision point into its constituent parts and discover how a policy decision point works by using trust algorithms.

Threats to a zero trust architecture

Course | 1 hour 22 minutes

Is a zero trust architecture resilient to cyberattack? What threats can it sustain? Take this course to find out.

Migrating to a zero trust architecture (ZTA)

Course | 48 minutes

How do you start your zero trust roadmap? Here we learn how to start a zero trust architecture; how it can reside alongside your traditional security architecture for dual-running; and how to operationalize the ZTA. We also assess a frequently asked question: Can I remove my network-based firewall now that I have a zero trust architecture?

IAPP CIPM

CERTIFICATION PATH

Make data privacy regulations work for your organization by understanding how to implement them in day-to-day operations. Learn to create a company vision, structure a data protection team, develop and implement system frameworks, communicate with stakeholders, measure performance and more.

CIPM practice exam

Practice Exam | 35 questions

Prepare for your IAPP CIPM exam and test your knowledge.

Developing a privacy program

Course | 41 minutes

An exploration of developing a privacy program: the dangers, the challenges and the methods.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0066, K0121, K0260, K0261, K0262, K0501, K0615, S0354, S0367, S0374

Privacy governance

Course | 37 minutes

An exploration of privacy governance challenges and skills.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0066, K0101, K0121, K0260, K0261, K0262, K0411, K0504, K0615, S0027, S0354, S0367, S0374

Privacy program frameworks

Course | 38 minutes

This course discusses existing legislation, standards and frameworks that can be utilized to build a roadmap for your privacy program.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0047, K0066, K0084, K0121, K0260, K0261, K0262, K0615, S0147, S0354, S0367, S0374

Legal jurisdictions and global data flows

Course | 52 minutes

This course discusses existing legislation, standards and frameworks that can be utilized to build a roadmap for your privacy program.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0066, K0121, K0123, K0155, K0156, K0168, K0222, K0260, K0261, K0262, K0267, K0410, K0411, K0615, S0354, S0367, S0374

Data assessments

Course | 1 hour 2 minutes

Exploring data assessments, data inventories, privacy risk assessments and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0006, K0044, K0066, K0121, K0165, K0260, K0261, K0262, K0501, K0615, S0080, S0189, S0271, S0354, S0360, S0367, S0374

Documentation

Course | 18 minutes

Exploring documentation: policies, procedures, document types and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0066, K0121, K0260, K0261, K0262, K0501, K0615, S0213, S0243, S0323, S0354, S0367, S0374

Privacy rights

Course | 53 minutes

This course looks at global privacy rights, using the EU GDPR as its focus.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0006, K0044, K0066, K0121, K0260, K0261, K0262, K0501, K0615, S0354, S0367, S0374

Training and awareness

Course | 18 minutes

Exploring training and awareness, including training methods, competency-based training and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0066, K0121, K0215, K0218, K0220, K0226, K0243, K0245, K0260, K0261, K0262, K0501, K0615, S0064, S0070, S0354, S0367, S0374

Information security and protection of data

Course | 44 minutes

This course looks at the basics of information security, focusing on risk assessment to keep the level of technical and organizational controls appropriate to the organization.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0066, K0121, K0260, K0261, K0262, K0264, K0487, K0501, K0561, K0615, S0034, S0076, S0084, S0170, S0354, S0367, S0374

Managing a security breach

Course | 37 minutes

This course looks at what happens when security is breached, including the difference between an incident and a breach and steps to be taken in order to detect, assess, respond to and learn from security incidents.

NICE Knowledge and Skill Statements:

K0003 , K0004, K0005, K0042, K0044, K0066, K0121, K0231, K0260, K0261, K0262, K0292, K0399, K0519, K0615, S0054, S0354, S0367, S0374

Continual improvement

Course | 43 minutes

A look at continual improvement: understanding performance, exploring metrics, audit methodologies and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0066, K0121, K0198, K0260, K0261, K0262, K0501, K0615

ISACA CIPT

CERTIFICATION PATH

This path explores the intersection of technology, data security, and policy. You'll learn key concepts about privacy and compliance, as well as the frameworks and tech to support these. We'll cover threats and violations, privacy by design, data management strategies, encryption and more. You'll also get tips on passing the CIPT exam, as well as practice materials.

CIPT Practice Exam

Practice exam | 70 questions

Prepare for your IAPP Certified Information Privacy Technologist exam and test your domain knowledge.

Privacy fundamentals

Course | 37 minutes

In this course, you'll learn about the origins of modern privacy law and theory. What is anonymity? How do we define privacy harms? You'll see how these relate to today's privacy questions and dilemmas. You'll also learn about commonly recognized frameworks such as the Fair Information Practice Principles, the OECD model for protecting privacy and data security and the phases of the data life cycle.

Privacy in engineering

Course | 1 hour 24 minutes

In this course, you'll cover a broad range of topics like risk management, the software development life cycle and requirements gathering. We'll also go in-depth on systems architecture, modeling and documentation, design patterns and defining privacy harms from an engineering prospective. Finally, we'll explore systems testing from all angles.

Encryption

Course | 51 minutes

In this course, students will explore privacy and encryption fundamentals. We'll start with a high-level overview, including many of the terms you'll need to fully understand encryption concepts.

Identity

Course | 32 minutes

This course discusses the concept of identity. There are many levels at which we can identify a individual, from completely identified to completely anonymous. We'll cover these in depth and explain why these concepts are important to safeguarding data and privacy. We'll also explore anonymization concepts and techniques. Finally, we'll take an in-depth look at authentication concepts and practices, as well as some of the challenges identity presents in today's privacy environment.

Designing privacy interfaces

Course | 1 hour 6 minutes

This course is all about keeping the user and privacy in focus in our designs. We'll explore some of the psychology behind how users make privacy-related decisions and why the privacy paradox sometimes prevents individuals from making the choices they really want to make.

Surveillance & tracking

Course | 1 hour 17 minutes

This course gets into the ways in which users are tracked, and how they can protect themselves. We'll look at why companies, organizations and governments track and surveil users as well as the underlying internet technologies that make tracking users possible.

Interference

Course | 29 minutes

In this course, we'll talk about the ways in which spam, behavior profiling, machine learning, cyberbullying and more can change the way people behave and the kinds of decisions they make. We'll also cover some best practices to reduce these harms.

Cybersecurity principles

Course | 29 minutes

In this course, you'll learn about how cybersecurity principles can help to protect privacy. We'll discuss concepts like the CIA Triad, dealing with adversaries and attacks and malware, and principles like least privilege and implementing multiple layers of defense.

Data governance

Course | 25 minutes

We'll talk in-depth about data governance, a few representative privacy laws and how compliance and technology intertwine. We'll also cover the principles of privacy by design, which help us put our users and their privacy needs front and center when we are creating and maintaining our apps and systems.

ISACA CISM

CERTIFICATION PATH

The Certified Information Security Manager (CISM) certification path is designed for individuals who oversee, design or assess an enterprise's information security

CISM Practice Exam

Practice Exam | 20 questions

Prepare for your CISMexam and test your knowledge.

Domain 1: Information Security Governance

Course | 2 hours 42 minutes

his course walks users through all the sections of domain 1 of the CISM exam. The topics covered range from designing a security strategy to gaining management support and putting that strategy into action.

NICE Knowledge and Skill Statements:

K0006, K0047, K0084, K0146, K0214, K0234, K0248, K0249, K0432, K0501, K0518, K0536, S0147, S0185, S0216, S0273, S0306

Domain 2: Information Risk Management

Course | 2 hours 43 minutes

The second course in the CISM learning path covers Domain 2. It has sections dedicated to risk identification as well as analysis or risk, how to treat it and the risk monitoring and reporting process.

NICE Knowledge and Skill Statements:

K0002, K0006, K0027, K0037, K0038, K0048, K0065, K0084, K0126, K0146, K0154, K0165, K0169, K0214, K0379, K0455, K0527, K0624, S0124, S0147, S0175, S0244

Domain 3: Information Security Program Development and Management

Course | 2 hours 43 minutes

This course covers Domain 3 of CISM and focuses on information security program development and management.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0043, K0047, K0072, K0090, K0121, K0146, K0150, K0257, K0270, K0287, K0432, K0501, K0518, S0185, S0209

Domain 4: Information Security Incident Management

Course | 2 hours 49 minutes

The final course of the CISM certification path focuses on Domain 4 and has sections dedicated to information security incident management.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0021, K0026, K0041, K0042, K0072, K0150, K0157, K0162, K0177, K0221, K0332, S0003, S0047, S0054, S0173, S0365

ISACA CRISC

CERTIFICATION PATH

The Certified in Risk and Information Systems Control (CRISC) exam is a certification testing a student's ability to assess and evaluate risk, as well as risk management proficiency. This learning path will provide students with the knowledge and abilities necessary to pass the CRISC exam.

CRISC Practice Exam

Practice Exam | 74 questions

Prepare for your CRISC exam and test your knowledge.

Domain 1: IT Risk Identification

Course | 2 hours 52 minutes

This module walks users through all the sections of Domain 1 of the CRISC exam. There are seven learning tasks associated with this domain.

NICE Knowledge and Skill Statements:

K0002, K0048, K0126, K0149, K0154, K0169, K0195, K0379, K0455, K0506, K0527, K0624, S0304

Domain 2: IT Risk Assessment

Course | 2 hours 16 minutes

This module walks users through all the sections of Domain 2 of the CRISC exam. There are six learning tasks associated with this domain.

NICE Knowledge and Skill Statements:

K0002, K0048, K0126, K0149, K0154, K0169, K0195, K0379, K0455, K0506, K0527, K0624, S0034, S0080, S0171, S0304

Domain 3: Risk Response and Mitigation

Course | 1 hour 46 minutes

This module walks users through all the sections of Domain 3 of the CRISC exam. There are seven learning tasks associated with this domain.

NICE Knowledge and Skill Statements:

K0002, K0041, K0042, K0048, K0126, K0149, K0150, K0154, K0169, K0195, K0379, K0506, K0527, K0624, S0079, S0080, S0304

Domain 4: Risk and Control Monitoring and Reporting

Course | 2 hours 37 minutes

This module walks users through all the sections of Domain 4 of the CRISC exam. There are seven learning tasks associated with this domain.

NICE Knowledge and Skill Statements:

K0002, K0048, K0054, K0126, K0149, K0154, K0169, K0180, K0195, K0379, K0451, K0455, K 0527, K0624, S0136, S0304

ISC2 Certified in Governance, Risk and Compliance (CGRC) (previously - CAP)

CERTIFICATION PATH

The Certified in Governance, Risk and Compliance (CGRC) certification path builds your expertise around the NIST Risk Management Framework (RMF). You'll learn best practices, policies and procedures used to authorize and maintain information systems.

Skill Assessment

Skill assessment | 20 questions

See how your CGRC skills stack up against other professionals in your field.

CGRC Practice Exam

Practice Exam | 125 questions

Prepare for your CGRC exam and test your domain knowledge.

Introduction to CGRC

Course | 2 minutes

Start off your exploration of CGRC, or Certified Authorization Professional, with this introductory course looking at the basics of your education path.

NICE Knowledge and Skill Statements:

K0004, K0048

Information Security Risk Management Program

Course | 39 minutes

This course on risk management in a CGRC context covers security objectives, risk management programs, essential laws and documents, key roles (including federal entities) and more. Includes vocabulary and diagrams.

NICE Knowledge and Skill Statements:

K0002, K0003, K0004, K0007, K0048, K0081, K0101, K0109, K0165, K0267, K0336, K0527, K0579, S0023, S0147

Risk Management Program Processes

Course | 9 minutes

In this course you'll explore the details of the risk management framework, including vocabulary, objectives and tasks.

NICE Knowledge and Skill Statements:

K0002, K0004, K0007, K0048, K0165, K0260, K0266, K0336, K0527, K0579, S0023, S0147

Regulatory and Legal Requirements

Course | 40 minutes

Take a closer look at the regulatory and legal requirements connected to risk management, including federal laws, NIST documents and the Committee on National Security.

NICE Knowledge and Skill Statements:

K0003, K0004, K0019, K0168, K0260, K0261, K0262, K0267, K0351, K0410, K0411, K0427, S0147

Categorization of Information Systems

Course | 21 minutes

Dive into CGRC Domain 2 with this course on Categorization of Information Systems. Take a look at system security plans, categorization documents, examples, exercises and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0048, K0053, K0081, K0199, K0260, K0579, S0078

Selection of Security Controls

Course | 9 minutes

Get to grips with CGRC Domain 3, Selection of Security Controls. Explore control tailoring, control selection, monitoring strategy and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0048, K0065, K0612, S0007, S0031, S0034, S0097, S0147, S0152

Risk Assessment

Course | 17 minutes

Refresh your knowledge of how bad things can get with this course on the four steps of risk assessment: Prepare, Conduct the Assessment, Report and Communicate and Maintain.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0006, K0007, K0013, K0040, K0048, K0070, K0161, K0162, K0165, K0177, K0336, K0344, K0527, K0579, S0078, S0167

Implementation of Security Controls

Course | 27 minutes

Get ready to implement security controls with this course covering applying, implementing and tailoring controls. Includes vocabulary and diagrams.

NICE Knowledge and Skill Statements:

K0002, K0004, K0042, K0048, K0065, K0179, K0202, K0276, K0480, K0612, S0007, S0031, S0032, S0034, S0097, S0147, S0152

Assessment of Security Controls

Course | 11 minutes

Prepare for security control assessment with this course covering the six key areas of control assessment, conducting the assessment and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0013, K0048, K0065, K0342, K0579, K0612, S0031, S0034, S0051, S0137, S0147, S0152, S0167

Authorization of Information Systems

Course | 11 minutes

In this course, you'll take a closer look at the authorization of information systems. Refresh your knowledge of assembling a security authorization package, determining information system risk and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0007, K0048, K0054, K0065, K0180, K0336, S0031, S0034, S0136, S0147, S0152, S0155

Continuous Monitoring

Course | 22 minutes

Review what you need to know to keep an eye on your new controls with this course on information security continuous monitoring.

NICE Knowledge and Skill Statements:

K0002, K0004, K0048, K0054, K0064, K0073, K0180, K0275, K0393, S0136, S0147, S0153, S0155

Preparing for the CGRC Exam

Course | 6 minutes

Get ready to earn your CGRC with this short course on exam preparation and study tips.

NICE Knowledge and Skill Statements:

K0004, K0048

ISC2 Certified Cloud Security Professional (CCSP)

CERTIFICATION PATH

The Certified Cloud Security Professional (CCSP) certification path teaches you the fundamentals of the cloud computing architecture framework and how to evaluate and implement appropriate controls around cloud services.

Skill Assessment

Skill assessment | 20 questions

See how your CCSP skills stack up against other professionals in your field.

CCSP Practice Exam

Practice Exam | 1,311 questions

Prepare for your CCSP exam and test your domain knowledge.

Cybersecurity Basics

Course | 1 hour

Build a baseline of cybersecurity knowledge in this introductory course.

NICE Knowledge and Skill Statements:

K0003, K0004, K0047, K0049, K0101, K0524, K0612

Cloud Concepts, Architecture and Design

Course | 3 hours 38 minutes

Get an overview of cloud computing concepts, models (services & deployments) and principles. This course will build your knowledge of virtualization, treat modeling and design cloud requirements.

NICE Knowledge and Skill Statements:

K0019, K0047, K0049, K0112, K0130, K0190, K0205, K0230, K0277, K0609, K0612

Cloud Data Security

Course | 1 hour 29 minutes

Get an overview of data classification and categorization, data lifecycle stages, data retention and auditing, as well as an introduction to information and digital rights management.

NICE Knowledge and Skill Statements:

K0004, K0007, K0025, K0038, K0065, K0158, K0195, K0287, K0377, K0622

Cloud Platform and Infrastructure Security

Course | 1 hour 41 minutes

Build a baseline of knowledge around cloud security strategies, risks and responsibilities, storage and business continuity programs.

NICE Knowledge and Skill Statements:

K0004, K0021, K0026, K0038, K0097, K0145, K0230, K0622

Cloud Application Security

Course | 38 minutes

Explore the software development lifecycle, as well as the testing, architecture and auditing of cloud services.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0081, K0090, K0153, K0339, K0342, K0373, K0624

Cloud Security Operations

Course | 1 hour 22 minutes

Learn the Uptime Institute requirements for achieving data center high availability through redundancy, capacity and maintenance monitoring, risk management, and change and configuration monitoring to achieve high availability, datacenter redundancy and standards.

NICE Knowledge and Skill Statements:

K0002, K0004, K0032, K0048, K0074, K0090, K0145, K0180, K0243

Cloud Legal, Risk and Compliance Requirements

Course | 55 minutes

Build your knowledge of relevant jurisdictional laws, statues, regulations and frameworks, as well as the doctrine of proper law for the protection of data in cloud computing.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0006, K0158, K0524

CCSP Exam Essentials

Course | 17 minutes

Review key knowledge areas to help focus your studies and prepare for the CCSP exam.

ISC2 CISSP

CERTIFICATION PATH

The Certified Information Systems Security Professional (CISSP) certification path teaches you the skills and best practices needed to create and execute enterprise-wide information security strategies.

Skill Assessment

Skill assessment | 20 questions

See how your CISSP skills stack up against other professionals in your field.

CISSP Practice Exam

Practice Exam | 2,170 questions

Prepare for your CISSP exam and test your domain knowledge.

Security Governance Principles

Course | 16 minutes

Explore security governance and how it relates to business processes and strategies in this brief overview course.

NICE Knowledge and Skill Statements:

K0004, K0006, K0047, K0146, K0261, K0295, K0511, K0579

Regulatory Compliance

Course | 30 minutes

Explore the compliance issues related to digital data, including privacy laws, regulations, intellectual property issues and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0006, K0157, K0196, K0260, K0261, K0262, K0410, K0524, K0615

Risk Management

Course | 49 minutes

Dive deep into risk management, including risk frameworks, assessments and modeling, as well as employee security awareness, vendor security and other issues.

NICE Knowledge and Skill Statements:

K0002, K0005, K0047, K0048, K0162, K0165, K0169, K0214, K0295, K0455, K0527

Security Policies

Course | 22 minutes

Explore security policies and control frameworks and how they help drive the overall security of an organization.

NICE Knowledge and Skill Statements:

K0004, K0006, K0157, K0169, K0215, K0242, K0243, K0264

Asset Security

Course | 39 minutes

Learn how to secure sensitive data, including managing and classifying data, working with data at rest and in transit, and implementing data security controls.

NICE Knowledge and Skill Statements:

K0049, K0065, K0083, K0195, K0287, K0377, K0622

Cryptography Fundamentals

Course | 41 minutes

Explore the uses and challenges of cryptography. Learn about hashing, ciphers, digital signatures, types of cryptography and more.

NICE Knowledge and Skill Statements:

K0004, K0018, K0019, K0190, K0295, K0305, K0308, K0403, K0427, K0622

Public Key Infrastructure

Course | 21 minutes

Dig into the inner-workings of Public Key Infrastructure (PKI), including key components, certificates, key management and more.

NICE Knowledge and Skill Statements:

K0004, K0018, K0019, K0056, K0190, K0285, K0403, K0427

Secure Design Principles

Course | 39 minutes

Explore the principles behind secure system design, ranging from security models to certification and accreditation.

NICE Knowledge and Skill Statements:

K0037, K0044, K0047, K0075, K0170, K0180, K0198, K0203, K0211, K0240, K0288, K0291, K0320, K0362, K0624

System Protection Mechanisms

Course | 32 minutes

Learn about different system protection mechanisms and common issues such as Web-based vulnerabilities, architecture flaws and more.

NICE Knowledge and Skill Statements:

K0004, K0070, K0077, K0090, K0109, K0199, K0209, K0271, K0322, K0392, K0493, K0624

Physical Security

Course | 52 minutes

Don’t forget about physical security! Explore how to keep your business secure starting with secure design and construction to physical intrusion detection and more.

NICE Knowledge and Skill Statements:

K0065, K0075, K0165, K0244, S0023

Data Center Security

Course | 21 minutes

Don’t let an incident at your data center disrupt your organization. Explore ways to keep data centers secure from a variety of threats.

NICE Knowledge and Skill Statements:

K0032, K0622

Database Security

Course | 20 minutes

How do you keep a database secure? Revisit the key concepts beind database security in this brief course.

NICE Knowledge and Skill Statements:

K0022, K0023, K0024, K0069, K0095, K0373, K0419, K0622

Network Fundamentals

Course | 1 hour 20 minutes

Go in-depth into networking devices and technologies. Explore network types, protocols, models, attacks, security and more.

NICE Knowledge and Skill Statements:

K0001, K0010, K0034, K0050, K0057, K0061, K0093, K0136, K0159, K0170, K0221, K0265, K0274, K0303, K0332, K0333, K0395, K0417, K0437, K0443, K0452, K0470, K0471, K0489, K0516, K0565, K0612, S0236

Secure Network Design

Course | 26 minutes

Explore key concepts behind secure network design, including tools to keep threats out and techniques to detect and deflect intruders that breach your defenses.

NICE Knowledge and Skill Statements:

K0001, K0004, K0034, K0049, K0179, K0276, K0291, K0324, K0326, K0452, K0487, K0488, K0493, K0561, S0023, S0034

Distributed System & Virtualized Networks

Course | 20 minutes

Explore the use of distributed and virtualized systems as well as the security benefits and potential drawbacks involved in their use.

NICE Knowledge and Skill Statements:

K0001, K0063, K0071, K0113, K0130, K0179, K0205, K0437, K0610

Access Control Fundamentals

Course | 1 hour 37 minutes

Take a deep dive into one of the fundamental concepts of security: access control. Learn how to give the right people access to the right information in a secure way.

NICE Knowledge and Skill Statements:

K0007, K0033, K0056, K0065, K0071, K0104, K0158, K0179, K0211, K0332, K0336, K0452, K0488, S0023, S0031

WAN & Remote Access Security

Course | 33 minutes

Learn about securing wide area networks (WAN) and remote access against different types of cyber threats in this five-video course.

NICE Knowledge and Skill Statements:

K0001, K0005, K0070, K0071, K0104, K0113, K0138, K0190, K0269, K0274, K0362, K0395, K0417, K0427, K0438

Security Assessment

Course | 20 minutes

K0001, K0005, K0070, K0071, K0104, K0113, K0138, K0190, K0269, K0274, K0362, K0395, K0417, K0427, K0438

NICE Knowledge and Skill Statements:

Computer Crime Investigations

Course | 32 minutes

Refresh your knowledge of cybercrime investigations with this overview course covering the investigation process and the discovery of digital evidence.

NICE Knowledge and Skill Statements:

K0017, K0118, K0122, K0123, K0125, K0128, K0133, K0155, K0156, K0184, K0222, K0251, K0304, K0433

Preventative & Detective Measures

Course | 39 minutes

Explore ways to prevent cyber threats from impacting your organization, and learn how to quickly detect the threats that do slip through your defenses.

NICE Knowledge and Skill Statements:

K0004, K0006, K0049, K0073, K0074, K0132, K0145, K0167, K0205, K0275, K0480, K0487, K0488, K0561

Business Continuity Planning

Course | 19 minutes

Learn how to keep your business up and running. Explore the importance of continuity planning, incident response planning and impact analysis.

NICE Knowledge and Skill Statements:

K0006, K0026, K0032, K0041, K0042, K0150, K0165, K0292

Disaster Recovery

Course | 36 minutes

Don't let a lack of preparedness compound the effects of a disaster. Learn how to create and test a disaster recovery plan in this six-video course.

NICE Knowledge and Skill Statements:

K0006, K0021, K0026, K0032, K0150, K0210, K0292, K0399, K0519, K0527

Secure Software Design

Course | 25 minutes

Explore the methods of creating secure software, including development and maturity models and the secure software development life cycle.

NICE Knowledge and Skill Statements:

K0004, K0039, K0047, K0081, K0082, K0153, K0198, K0200, K0258

Secure Software Development

Course | 43 minutes

Explore the ins and outs of secure software development as you progress through this nine-video course.

NICE Knowledge and Skill Statements:

K0039, K0070, K0153, K0276, K0373, K0396, K0480

ISC2 CISSP-ISSAP

CERTIFICATION PATH

The Information Systems Security Architecture Professional (CISSP-ISSAP) certification path teaches you how to provide risk-based guidance to senior management and develop, design and analyze security solutions that meet organizational goals.

Skill Assessment

Skill assessment | 20 questions

See how your CISSP-ISSAP skills stack up against other professionals in your field.

CISSP-ISSAP Practice Exam

Practice Exam | 125 questions

Prepare for your CISSP-ISSAP exam and test your domain knowledge.

Introduction to ISSAP

Course | 9 minutes

An overview of the CISSP-ISSAP credential and the certification exam.

NICE Knowledge and Skill Statements:

K0004, K0027, K0100, K0121, K0199, K0291

Identity and Access Management Architecture

Course | 1 hour 23 minutes

Understand the lifecycle and the design of the identity management architecture.

NICE Knowledge and Skill Statements:

K0004, K0007, K0024, K0027, K0047, K0056, K0065, K0075, K0100, K0158, K0170, K0199, K0291, K0336, S0031, S0043, S0084

Security Architecture Modeling

Course | 41 minutes

Identify the correct approach for the organization's security architecture.

NICE Knowledge and Skill Statements:

K0004, K0027, K0047, K0100, K0199, K0203, K0288, K0437

Architecture for Governance, Compliance and Risk Management

Course | 41 minutes

Discover the principles, processes and standards related to GRC (governance, risk management and compliance).

NICE Knowledge and Skill Statements:

K0002, K0004, K0006, K0027, K0047, K0048, K0100, K0101, K0202, K0260, K0261, K0262, K0267 K0455, K0527

Security Operations Architecture

Course | 1 hour 30 minutes

Know how to design and implement the appropriate architecture for security operations.

NICE Knowledge and Skill Statements:

K0004, K0021, K0026, K0027, K0046, K0047, K0093, K0100, K0242, K0299, K0324, K0417, K0432, K0440, K0481, K0531, S0032, S0145

Infrastructure Security

Course | 1 hour 29 minutes

Get an overview of various protocols, controls and activities involved in designing infrastructure security.

NICE Knowledge and Skill Statements:

K0001, K0004, K0018, K0019, K0027, K0034, K0047, K0050, K0057, K0061, K0071, K0093, K0100, K0136, K0159, K0170, K0190, K0221, K0265, K0274, K0285, K0300, K0303, K0308, K0332, K0333, K0395, K0403, K0417, K0427, K0452, K0470, K0471, K0489, K0516, K0565, K0612, S0145

Architect for Application Security

Course | 34 minutes

Learn about common app-related threats and how to address them through the development lifecycle.

NICE Knowledge and Skill Statements:

K0004, K0005, K0009, K0070, K0081, K0082, K0186, K0373, K0396, K0624

ISC2 CISSP-ISSEP

CERTIFICATION PATH

The Information Systems Security Engineering Professional (CISSP-ISSEP) certification path teaches you how to design, construct and operate a network with a defined level of availability, integrity and confidentiality.

Skill Assessment

Skill assessment | 20 questions

See how your CISSP-ISSEP skills stack up against other professionals in your field.

CISSP-ISSEP Practice Exam

Practice Exam | 100 questions

Prepare for your CISSP-ISSEP exam and test your domain knowledge.

Introduction to ISSEP

Course | 3 minutes

Get an overview of the Information Systems Security Engineering process and components.

NICE Knowledge and Skill Statements:

K0004

Security Engineering Principles

Course | 22 minutes

Review the security principles that security engineers need to know in order to implement systems.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0044, K0087, K0157, K0158, K0267, K0287, K0568, K0584

Risk Management

Course | 7 minutes

Get a basic understanding or risk management in an organization.

NICE Knowledge and Skill Statements:

K0002, K0004, K0214, K0455, K0527

System Resilience Principles

Course | 10 minutes

Dive into defense-in-depth and other principles and methods of making your systems resilient.

NICE Knowledge and Skill Statements:

K0002, K0004, K0032, K0112, K0179, K0299, K0323, K0527, S0027, S0076

Vulnerability Management Principles

Course | 13 minutes

Know why it's important to manage vulnerabilities, and what the engineer's role is.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0013, K0040, K0070, K0106, K0147, K0157, K0187, K0339, K0373, K0392, K0624, S0036, S0078

Risk Management Process

Course | 37 minutes

Walk through the security risk management process and learn best practices.

NICE Knowledge and Skill Statements:

K0002, K0004, K0047, K0048, K0165, K0214, K0264, K0455, K0527

Operational Risk Management

Course | 30 minutes

Understand how today's complex business environment impacts operational risk and related controls.

NICE Knowledge and Skill Statements:

K0004, K0047, K0048, K0084, K0154, K0169, K0214, K0264, K0379, K0455, K0527

Stakeholder Requirements Definition

Course | 14 minutes

Review how different stakeholders impact security planning, design and implementation.

NICE Knowledge and Skill Statements:

K0004, K0169, K0376, K0379

Requirements Analysis

Course | 7 minutes

Discover the process for analyzing requirements before designing security systems.

NICE Knowledge and Skill Statements:

K0004, K0028, K0035, K0073, K0086, K0090, K0091, K0102, K0164, K0291, K0475, K0480

System Security Architecture and Design

Course | 12 minutes

Review the core components and processes of security architecture and design.

NICE Knowledge and Skill Statements:

K0004, K0044, K0047, K0075, K0087, K0170, K0180, K0198, K0199, K0203, K0211, K0240, K0267, K0288, K0291, S0023

Implementation, Integration and Deployment of System Modifications

Course | 5 minutes

Learn the basics of system implementation, integration and deployment.

NICE Knowledge and Skill Statements:

K0004, K0073, K0082, K0091, K0178, K0179, K0186, K0257, K0270, K0393, K0452, K0488, S0153

Verification and Validation of Systems or System Modifications

Course | 10 minutes

Go through the post-deployments steps of ensuring the system is adequately secure.

NICE Knowledge and Skill Statements:

K0004, K0028, K0091, S0110, S0282

Secure Operations

Course | 30 minutes

Understand the basics of maintaining a secure operations strategy.

NICE Knowledge and Skill Statements:

K0004, K0006, K0026, K0041, K0042, K0074, K0086, K0150, K0167, K0292, K0324, K0333, K0403, K0488

Secure Maintenance

Course | 13 minutes

Learn about the three main areas of secure maintenance and related strategies.

NICE Knowledge and Skill Statements:

K0004, K0035, K0074 , K0103, K0167, K0294, K0419, S0027

Secure Disposal

Course | 8 minutes

Know how to handle a system at the end of its lifecycle and the key security considerations.

NICE Knowledge and Skill Statements:

K0004, K0090, K0270

Acquisition Process

Course | 15 minutes

Know what's involved in the systems acquisition phase and how to prepare for it.

NICE Knowledge and Skill Statements:

K0004, K0154, K0164, K0169, K0198, K0257, K0264, K0270, K0376, K0379

System Development Methodologies

Course | 3 minutes

Understand the advantages and disadvantages of different development methods.

NICE Knowledge and Skill Statements:

K0004, K0035, K0039, K0047, K0079, K0081, K0082, K0086, K0087, K0153, K0186, K0276

Technical Management Processes

Course | 32 minutes

Dive deep into the technical aspects of managing systems engineering.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0006, K0150, K0233, K0264, K0527, S0358

CISSP-ISSEP (2021 Update)

CERTIFICATION PATH

The Information Systems Security Engineering Professional (ISSEP) certification path is a focused study in all aspects of system security engineering.

CISSP-ISSEP Practice Exam

Practice Exam | 125 questions

Prepare for your CISSP-ISSEP exam and test your domain knowledge.

Introduction to System Security Engineering

Course | 1 hour 40 minutes

A captivating look into the world of system and security engineering.

NICE Knowledge and Skill Statements:

K0004, K0005, K0045, K0067, K0076, K0081, K0082, K0102, K0153, K0280, K0321, S0052, S0140

Domain 1: Systems Security Engineering Foundations

Course | 1 hour 48 minutes

This course covers systems security engineering and lays a foundation for both exam preparation and security engineering.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0045, K0067, K0076, K0081, K0082, K0092, K0102, K0153, K0280, K0321, K0435, K0436, K0560, S0052, S0140

Domain 2: Risk Management

Course | 1 hour 34 minutes

Domain 2 focuses on the risk management practices necessary to protect the health of our organization.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0006, K0038, K0045, K0048, K0067, K0082, K0092, K0101, K0102, K0149, K0165, K0280, K0435, K0436, K0455, K0506, K0527, S0304

Domain 3: Security Planning and Design

Course | 1 hour 4 minutes

Domain 3 introduces security planning and design, taking us from requirement to completed solutions.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0006, K0045, K0067, K0075, K0076, K0080, K0081, K0082, K0086, K0092, K0102, K0153, K0332, K0347, K0435, K0498, K0519, S0022, S0036, S0135, S0141, S0160

Domain 4: Systems Implementation, Verification and Validation

Course | 27 minutes

Domain 4 looks at deploying, verifying and validating security controls within our enterprises.

NICE Knowledge and Skill Statements:

K0004, K0006, K0028, K0045, K0054, K0067, K0073, K0075, K0076, K0080, K0081, K0082, K0102, K0153, K0347, K0488, S0032, S0036, S0040, S0135, S0141, S0160, S0218, S0282

Domain 5: Secure Operations, Change Management and Disposal

Course | 1 hour 45 minutes

Domain 5 addresses the long-term management of our enterprise, from implementation to sunsetting of our systems.

NICE Knowledge and Skill Statements:

K0004, K0006, K0028, K0045, K0073, K0075, K0080, K0081, K0102, K0153, K0299, K0347, K0488, S0027, S0032, S0036, S0040, S0135, S0141, S0160, S0280, S0282

ISC2 CISSP-ISSMP

CERTIFICATION PATH

The Information System Security Management Professional (CISSP-ISSMP) certification path teaches you the necessary skills and knowledge to successfully manage an enterprise security program.

ISSMP Practice Exam

Practice Exam | 200 questions

Prepare for your ISSMP exam and test your domain knowledge.

Leadership and Business Management

Course | 2 hours 45 minutes

In this course, you'll look at how to align your security program with your organization's governance structure and define and implement your security strategies, maintain your security framework, define metrics and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0072, K0101, K0121, K0264, K0293, K0296, K0425, K0477, K0518, K0579, S0038, S0356

Systems Life Cycle Management

Course | 2 hours 37 minutes

Learn how to integrate security into the system development life cycle, integrate new business initiatives and emerging technologies, oversee a vulnerability management program and manage the security aspects of change management.

NICE Knowledge and Skill Statements:

K0004, K0013, K0070, K0075, K0081, K0121, K0165, K0198, K0342, S0001, S0051, S0242

Risk Management

Course | 1 hour 22 minutes

In this course, you'll learn how to develop and manage a risk management program. You will also learn to conduct risk assessments and a Business Impact Analysis (BIA).

NICE Knowledge and Skill Statements:

K0002, K0004, K0048, K0084, K0149, K0154, K0165, K0169, K0214, K0263, K0264, K0267, K0379, K0455, K0527, S0171

Threat Intelligence and Incident Management

Course | 1 hour 6 minutes

Learn how to establish and maintain a threat intelligence program, conduct a baseline analysis and do threat modeling. Then you'll explore incident handling and investigations, the IR process, root cause analysis and more.

NICE Knowledge and Skill Statements:

K0004, K0021, K0026, K0041, K0042, K0146, K0150, K0231, K0267, K0292, K0317, K0343, K0381, K0399, K0519, K0543, K0586, S0032, S0054, S0080, S0175, S0365

Contingency Management

Course | 1 hour 43 minutes

In this course, you'll learn how to oversee the development of contingency plans. You'll address recovery strategy development and managing BCP and DRP plans, finally ending up with a discussion of how to manage the recovery process.

NICE Knowledge and Skill Statements:

K0004, K0021, K0026, K0032, K0041, K0042, K0046, K0150, K0157, K0210, K0292, K0353, K0399, K0519, K0584, S0032, S0054, S0186, S0365

Law, Ethics and Security Compliance Management

Course | 1 hour 54 minutes

We will discuss the ISC2 code of ethics, compliance issues with organization security policies and procedures, coordinating and assisting with auditors and the audit process, and managing exceptions to compliance.

NICE Knowledge and Skill Statements:

K0003, K0004, K0157, K0196, K0260, K0261, K0262, K0267, K0351, K0410, K0524, K0615

Blockchain Security

SKILL PATH

This learning path introduces blockchain security, including a description of how the blockchain works at each level of the ecosystem. Security discussions include everything from the fundamental cryptographic primitives to the nodes and networks that make up the blockchain ecosystem to the security of smart contracts.

Skill Assessment

Skill assessment | 20 questions

See how your blockchain security skills stack up against other professionals in your field.

Blockchain Security Project

Project | 2 hours 11 minutes

Practice your blockchain security skills as your progress through five challenges.

Fundamentals of Blockchain Security

Course | 1 hour 6 minutes

This course introduces the fundamentals of blockchain security, from foundational concepts of blockchain and how the components of the blockchain are put together to how public-key cryptography and hash functions are used.

NICE Knowledge and Skill Statements:

K0018, K0019, K0059, K0190, K0403, K0427, K0431

Consensus Algorithm Security

Course | 1 hour 28 minutes

This course describes the underlying principles of consensus algorithms, how two of the primary consensus algorithms work under the hood and how they can be attacked.

NICE Knowledge and Skill Statements:

K0015, K0059, K0431

Blockchain in Action

Course | 1 hour 17 minutes

This course investigates how blocks are created in the blockchain (and how block creation can be attacked) as well as discussing attacks targeting blockchain nodes and the network that ties them together and enables communication.

NICE Knowledge and Skill Statements:

K0019, K0059, K0106 , K0147, K0151, K0314 , K0362, K0431, K0480, K0531

Smart Contract Security

Course | 1 hour 43 minutes

This course describes what a smart contract is and explores programming vulnerabilities that exist because a smart contract is a program, runs on a blockchain or is implemented on the Ethereum smart contract platform.

NICE Knowledge and Skill Statements:

K0059, K0070, K0431

Beyond the Basics of Blockchain

Course | 55 minutes

This course goes beyond blockchain-based distributed ledgers to discuss how the protocol can be replaced, expanded or improved to overcome some of the limitations of blockchain technology.

NICE Knowledge and Skill Statements:

K0018, K0059, K0427, K0431

Certified Security Awareness Practitioner (CSAP)

CERTIFICATION PATH

Learn the basics of running a successful training and awareness program that gets people's attention and changes behavior.

Training and Awareness Basics Overview

Course | 5 minutes

Begin at the beginning with this course introducing you to security training and awareness.

NICE Knowledge and Skill Statements:

K0146

Security Basics

Course | 28 minutes

Take a look at some fundamental security basics for soft-skill-focused learners.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0007, K0104, K0145, K0162, K0412, K0480, K0487

Introduction to Training and Awareness

Course | 14 minutes

Take a look at what's going on in the world of training and awareness, including potential obstacles and concerns.

NICE Knowledge and Skill Statements:

K0252, K0313

Sales and Marketing Techniques for Training and Awareness

Course | 38 minutes

Delve into the role of sales and marketing in security awareness and training.

NICE Knowledge and Skill Statements:

K0243, K0245

Creative

Course | 18 minutes

Explore possible concerns on the creative side of security programs.

NICE Knowledge and Skill Statements:

K0252

Program Execution

Course | 1 hour 10 minutes

Move from theory to practice with this course on executing a security program.

NICE Knowledge and Skill Statements:

K0243, K0245, K0252

Cloud Security Architecture

SKILL PATH

The Cloud Security Architecture skill path teaches you enterprise security architecture concepts related to the cloud, including cloud infrastructure, data and application security.

Cloud Data Security

Course | 2 hours 35 minutes

Get to grips with cloud data security for aspiring cloud security professionals with this course covering storage types, the six phases of the data life cycle, data security technologies and more.

NICE Knowledge and Skill Statements:

K0004, K0007, K0025, K0038, K0065,

Software Vulnerabilities and Security Controls

Course | 37 minutes

In this course, we take you through the fundamentals of software vulnerabilities and security controls.

NICE Knowledge and Skill Statements:

K0005, K0049, K0070, K0140, K0624

Secure Storage Controls

Course | 29 minutes

Refresh your knowledge of secure storage controls with this course on storage types, protocols and management.

NICE Knowledge and Skill Statements:

K0021, K0038, K0097, K0622

Securing Host Devices

Course | 20 minutes

Explore the challenges of securing host devices with this course on selecting host hardware and software, host hardening and protecting bootloaders.

NICE Knowledge and Skill Statements:

K0033, K0109, K0167, K0205, K0440

Network Security Components

Course | 44 minutes

In this course, we help you explore the details of network security components: device types, component management and analyzing components and network configurations.

NICE Knowledge and Skill Statements:

K0007, K0011, K0033, K0071, K0145, K0170, K0179, K0296, K0324, K0373, K0487, K0488, K0491, K0561

Secure Software Development

Course | 43 minutes

Explore the ins and outs of secure software development as you progress through this nine-video course.

NICE Knowledge and Skill Statements:

K0039, K0070, K0153, K0276, K0373, K0396, K0480

Secure Software Design

Course | 25 minutes

Explore the methods of creating secure software, including development and maturity models and the secure software development life cycle.

NICE Knowledge and Skill Statements:

K0004, K0039, K0047, K0081, K0082, K0153, K0198, K0200, K0258

Distributed System & Virtualized Networks

Course | 20 minutes

Explore the use of distributed and virtualized systems as well as the security benefits and potential drawbacks involved in their use.

NICE Knowledge and Skill Statements:

K0001, K0063, K0071, K0113, K0130, K0179, K0205, K0437, K0610

Cloud Application Security

Course | 2 hours 18 minutes

Cloud application security challenges are no match for this course covering common pitfalls, vulnerabilities, threat modeling, security devices, secure development and more.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0081, K0090, K0153, K0339, K0342, K0373, K0624

Cryptography Fundamentals

Course | 41 minutes

Explore the uses and challenges of cryptography. Learn about hashing, ciphers, digital signatures, types of cryptography and more.

NICE Knowledge and Skill Statements:

K0004, K0018, K0019, K0190, K0295, K0305, K0308, K0403, K0427, K0622

Cloud Platform and Infrastructure Security

Course | 2 hours 44 minutes

Review the fundamentals of cloud platform and infrastructure security with this course covering both physical and virtual security concerns and concepts.

NICE Knowledge and Skill Statements:

K0004, K0021, K0026, K0038, K0097, K0145, K0230, K0622

Operations

Course | 4 hours 27 minutes

Update your knowledge of the Operations domain in cloud security with this course covering logical design, secure configurations, host types, change management and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0032, K0048, K0074, K0090, K0145, K0180, K0243

Legal and Compliance

Course | 1 hour 57 minutes

Refresh your understanding of legal and compliance issues related to cloud security with this course. Covers key concepts, privacy laws, legal frameworks, country-specific regulations and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0006, K0158, K0524

Architectural Concepts & Design Requirements

Course | 4 hours 42 minutes

Brush up on your knowledge of architectural concepts and design requirements with this in-depth course. Review cloud service models, characteristics, deployment models, security and more.

NICE Knowledge and Skill Statements:

K0019, K0047, K0049, K0112, K0130, K0190, K0205, K0230, K0277, K0609, K0612

Data Center Security

Course | 21 minutes

Don’t let an incident at your data center disrupt your organization. Explore ways to keep data centers secure from a variety of threats.

NICE Knowledge and Skill Statements:

K0032, K0622

Physical Security

Course | 52 minutes

Don't forget about physical security! Explore how to keep your business secure starting with secure design and construction to physical intrusion detection and more.

NICE Knowledge and Skill Statements:

K0065, K0075, K0165, K0244, S0023

Secure Design Principles

Course | 39 minutes

Explore the principles behind secure system design, ranging from security models to certification and accreditation.

NICE Knowledge and Skill Statements:

K0037, K0044, K0047, K0075, K0170, K0180, K0198, K0203, K0211, K0240, K0288, K0291, K0320, K0362, K0624

Cloud Security Management

SKILL PATH

The Cloud Security Management skill path teaches you important security issues related to cloud services, including legal and compliance issues as well as the security of cloud infrastructure, data and applications.

Architectural Concepts & Design Requirements

Course | 4 hours 24 minutes

Brush up on your knowledge of architectural concepts and design requirements with this in-depth course. Review cloud service models, characteristics, deployment models, security and more.

NICE Knowledge and Skill Statements:

K0019, K0047, K0049, K0112, K0130, K0190, K0205, K0230, K0277, K0609, K0612

Legal and Compliance

Course | 1 hour 57 minutes

Refresh your understanding of legal and compliance issues related to cloud security with this course. Covers key concepts, privacy laws, legal frameworks, country-specific regulations and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0006, K0158, K0524

Operations

Course | 4 hours 27 minutes

Update your knowledge of the Operations domain in cloud security with this course covering logical design, secure configurations, host types, change management and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0032, K0048, K0074, K0090, K0145, K0180, K0243

Cloud Platform and Infrastructure Security

Course | 2 hours 44 minutes

Review the fundamentals of cloud platform and infrastructure security with this course covering both physical and virtual security concerns and concepts.

NICE Knowledge and Skill Statements:

K0004, K0021, K0026, K0038, K0097, K0145, K0230, K0622

Cloud Data Security

Course | 2 hours 35 minutes

Get to grips with cloud data security for aspiring cloud security professionals with this course covering storage types, the six phases of the data life cycle, data security technologies and more.

NICE Knowledge and Skill Statements:

K0004, K0007, K0025, K0038, K0065, K0158, K0195, K0287, K0377, K0622

Cloud Application Security

Course | 2 hours 18 minutes

Cloud application security challenges are no match for this course covering common pitfalls, vulnerabilities, threat modeling, security devices, secure development and more.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0081, K0090, K0153, K0339, K0342, K0373, K0624

Cloud Service Provider (CSP) Security Features

SKILL PATH

In this learning path, students will learn about the areas they will be responsible for when choosing a service with a cloud provider and gain hands-on experience with the three major cloud providers: AWS, Azure and GCP.

Skill Assessment

Skill assessment | 20 questions

See how your CSP security skills stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

Cloud Security Provider (CSP) Roles and Responsibilities

Course | 37 minutes

An overview of the cloud service provider's roles and responsibilities.

NICE Knowledge and Skill Statements:

K0194, K0230, K0233, K0579, S0073

AWS Security

Course | 1 hour 38 minutes

In this course, we review AWS-native security solutions. Students will have an opportunity for hands-on experience with a project in the console.

NICE Knowledge and Skill Statements:

K0007, K0018, K0021, K0026, K0032, K0038, K0044, K0056, K0065, K0070, K0170, K0179, K0187, K0194, K0210, K0230, K0403, K0579, K0622, K0624, S0073, S0077, S0097

Azure Security

Course | 1 hour 58 minutes

A review of Azure-native security solutions, followed by a console project.

NICE Knowledge and Skill Statements:

K0007, K0018, K0021, K0026, K0032, K0038, K0044, K0056, K0065, K0070, K0170, K0179, K0187, K0194, K0210, K0230, K0403, K0579, K0622, K0624, S0073, S0077, S0097

GCP Security

Course | 1 hour 26 minutes

In this course, we review GCP native security solutions and practice with a console project.

NICE Knowledge and Skill Statements:

K0007, K0018, K0021, K0026, K0032, K0038, K0044, K0056, K0065, K0070, K0170, K0179, K0187, K0194, K0210, K0230, K0403, K0579, K0622, K0624, S0073, S0077, S0097

CompTIA Advanced Security Practitioner (CASP+)

CERTIFICATION PATH

The CompTIA Advanced Security Practitioner (CASP+) certification path prepares your for CompTIA's most advanced information security certification. You'll learn the skills required to conceptualize, design and engineer secure solutions across complex enterprise environments.

Skill Assessment

Skill assessment | 20 questions

See how your CASP+ skills stack up against other professionals in your field.

CASP+ Practice Exam

Practice Exam | 134 questions

Prepare for your CASP+ exam and test your domain knowledge.

Business and Industry Influences and Risks

Course | 15 minutes

Brush up on your knowledge of business and industry influences and risks with this course on enterprise risk management (ERM) and business models.

NICE Knowledge and Skill Statements:

K0002, K0146, K0527

Security & Privacy Policies and Procedures

Course | 24 minutes

This course helps you refresh your knowledge of security and privacy policies and procedures.

NICE Knowledge and Skill Statements:

K0002, K0003, K0004, K0026, K0048, K0101, K0199, K0260, K0261, K0262, K0267, K0527

Risk Mitigation Strategies and Controls

Course | 26 minutes

Dive into risk mitigation strategies and controls with this course on risk scenarios, responses and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0048, K0148, K0165, K0169, K0194, K0267, K0527, K0556

Risk Metric Scenarios

Course | 12 minutes

This course on risk metric scenarios covers analyzing scenarios to secure enterprises and reviewing existing security.

NICE Knowledge and Skill Statements:

K0002, K0183, K0527

Network Security Components

Course | 44 minutes

In this course, we help you explore the details of network security components: device types, component management and analyzing components and network configurations.

NICE Knowledge and Skill Statements:

K0007, K0011, K0033, K0071, K0145, K0170, K0179, K0296, K0324, K0373, K0487, K0488, K0491, K0561

Securing Host Devices

Course | 20 minutes

Explore the challenges of securing host devices with this course on selecting host hardware and software, host hardening and protecting bootloaders.

NICE Knowledge and Skill Statements:

K0033, K0109, K0167, K0205, K0440

Secure Storage Controls

Course | 29 minutes

Refresh your knowledge of secure storage controls with this course on storage types, protocols and management.

NICE Knowledge and Skill Statements:

K0021, K0038, K0097, K0622

Software Vulnerabilities and Security Controls

Course | 37 minutes

In this course, we take you through the fundamentals of software vulnerabilities and security controls.

NICE Knowledge and Skill Statements:

K0005, K0049, K0070, K0140, K0624

Vulnerability Assessment Methods and Tools

Course | 21 minutes

This course helps you broaden your understanding of vulnerability assessment and tools, including tool lists and test types.

NICE Knowledge and Skill Statements:

K0005, K0006, K0013, K0106, K0177, K0301, K0342

Research, Development and Collaboration

Course | 33 minutes

In this course, we take you through the details of research, development and collaboration.

NICE Knowledge and Skill Statements:

K0059, K0065, K0081, K0147, K0151, K0309, K0431

Securing Communications and Collaboration Solutions

Course | 14 minutes

Secure your communications and collaboration solutions with this course covering BYOD, mobile device management and more.

NICE Knowledge and Skill Statements:

K0136, K0445, K0446

Implementing Cryptographic Techniques

Course | 30 minutes

Brush up on your understanding of implementing cryptographic techniques with this course covering cryptographic design, techniques and implementations.

NICE Knowledge and Skill Statements:

K0004, K0018, K0019, K0025, K0104, K0201, K0277, K0285, K0305, K0308, K0403, K0427, K0428

Integrating Authentication and Authorization Technologies

Course | 22 minutes

Review and update your knowledge of integrating authentication and authorization technologies with this course covering advanced identity management and more.

NICE Knowledge and Skill Statements:

K0004, K0007, K0056, K0065, K0092

Incident Response and Recovery Procedures

Course | 16 minutes

Prepare for possible trouble with this course on incident response and recovery procedures, including designing systems to facilitate incident response.

NICE Knowledge and Skill Statements:

K0021, K0026, K0041, K0042, K0118, K0125, K0128, K0132, K0133, K0150, K0292

Integrating Hosts, Storage, Networks and Applications

Course | 28 minutes

Put the pieces together with this course on integrating hosts, storage, networks and applications. Includes vocabulary and guidelines.

NICE Knowledge and Skill Statements:

K0035, K0087, K0092, K0332, K0565, K0622

Integrating Cloud and Virtualization Technologies

Course | 33 minutes

In this course, you'll get to grips with the challenges of integrating cloud and virtualization technologies. Includes vocabulary and guidelines.

NICE Knowledge and Skill Statements:

K0004, K0130, K0167, K0230, K0609, K0610

Cybersecurity Administration

SKILL PATH

The Cybersecurity Administration skill path covers a variety of high-level tasks related to cybersecurity, including implementing identity and access management, understanding asset security, integrating enterprise security, performing assessments and more.

Risk Metric Scenarios

Course | 12 minutes

This course on risk metric scenarios covers analyzing scenarios to secure enterprises and reviewing existing security.

NICE Knowledge and Skill Statements:

K0002, K0183, K0527

Vulnerability Assessment Methods and Tools

Course | 21 minutes

This course helps you broaden your understanding of vulnerability assessment and tools, including tool lists and test types.

NICE Knowledge and Skill Statements:

K0005, K0006, K0013, K0106, K0177, K0301, K0342

Software Vulnerabilities and Security Controls

Course | 37 minutes

In this course, we take you through the fundamentals of software vulnerabilities and security controls.

NICE Knowledge and Skill Statements:

K0005, K0049, K0070, K0140, K0624

Integrating Cloud and Virtualization Technologies

Course | 33 minutes

In this course, you'll get to grips with the challenges of integrating cloud and virtualization technologies. Includes vocabulary and guidelines.

NICE Knowledge and Skill Statements:

K0004, K0130, K0167, K0230, K0609, K0610

Integrating Hosts, Storage, Networks and Applications

Course | 28 minutes

Put the pieces together with this course on integrating hosts, storage, networks and applications. Includes vocabulary and guidelines.

NICE Knowledge and Skill Statements:

K0035, K0087, K0092, K0332, K0565, K0622

Incident Response and Recovery Procedures

Course | 16 minutes

Prepare for possible trouble with this course on incident response and recovery procedures, including designing systems to facilitate incident response.

NICE Knowledge and Skill Statements:

K0021, K0026, K0041, K0042, K0118, K0125, K0128, K0132, K0133, K0150, K0292

Integrating Authentication and Authorization Technologies

Course | 22 minutes

Review and update your knowledge of integrating authentication and authorization technologies with this course covering advanced identity management and more.

NICE Knowledge and Skill Statements:

K0004, K0007, K0056, K0065, K0092

Implementing Cryptographic Techniques

Course | 30 minutes

Brush up on your understanding of implementing cryptographic techniques with this course covering cryptographic design, techniques and implementations.

NICE Knowledge and Skill Statements:

K0004, K0018, K0019, K0025, K0104, K0201, K0277, K0285, K0305, K0308, K0403, K0427, K0428

Securing Communications and Collaboration Solutions

Course | 14 minutes

Secure your communications and collaboration solutions with this course covering BYOD, mobile device management and more.

NICE Knowledge and Skill Statements:

K0136, K0445, K0446

Asset Security

Course | 39 minutes

Learn how to secure sensitive data, including managing and classifying data, working with data at rest and in transit, and implementing data security controls.

NICE Knowledge and Skill Statements:

K0049, K0065, K0083, K0195, K0287, K0377, K0622

Risk Mitigation Strategies and Controls

Course | 26 minutes

Dive into risk mitigation strategies and controls with this course on risk scenarios, responses and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0048, K0148, K0165, K0169, K0194, K0267, K0527, K0556

Business and Industry Influences and Risks

Course | 15 minutes

Brush up on your knowledge of business and industry influences and risks with this course on enterprise risk management (ERM) and business models.

NICE Knowledge and Skill Statements:

K0002, K0146, K0527

Security Assessment

Course | 20 minutes

Discover any weak spots in your cyber defense. Learn how to use security assessments to identify, analyze and report on an organization's cyber risk.

NICE Knowledge and Skill Statements:

K0002, K0013, K0028, K0037, K0048, K0091, K0165, K0177, K0214, K0342

Access Control Fundamentals

Course | 1 hour 37 minutes

Take a deep dive into one of the fundamental concepts of security: access control. Learn how to give the right people access to the right information in a secure way.

NICE Knowledge and Skill Statements:

K0007, K0033, K0056, K0065, K0071, K0104, K0158, K0179, K0211, K0332, K0336, K0452, K0488, S0023, S0031

Secure Network Design

Course | 26 minutes

Explore key concepts behind secure network design, including tools to keep threats out and techniques to detect and deflect intruders that breach your defenses.

NICE Knowledge and Skill Statements:

K0001, K0004, K0034, K0049, K0179, K0276, K0291, K0324, K0326, K0452, K0487, K0488, K0493, K0561, S0023, S0034

WAN & Remote Access Security

Course | 33 minutes

Learn about securing wide area networks (WAN) and remote access against different types of cyber threats in this five-video course.

NICE Knowledge and Skill Statements:

K0001, K0005, K0070, K0071, K0104, K0113, K0138, K0190, K0269, K0274, K0362, K0395, K0417, K0427, K0438

Network Fundamentals

Course | 1 hour 20 minutes

Go in-depth into networking devices and technologies. Explore network types, protocols, models, attacks, security and more.

NICE Knowledge and Skill Statements:

K0001, K0034, K0050, K0057, K0061, K0093, K0136, K0159, K0170, K0221, K0265, K0274, K0303, K0332, K0333, K0395, K0417, K0437, K0452, K0470, K0471, K0489, K0516, K0565, K0612, S0236

Cybersecurity Audit Fundamentals

SKILL PATH

The Cybersecurity Audit Learning Path helps you get to grips with the controls implemented by the organization to reduce the risk to confidentiality, integrity and availability down to an acceptable level.

Skill Assessment

Skill assessment | 20 questions

See how your cybersecurity audit fundamentals skills stack up against other professionals in your field.

Audit's Role in Cybersecurity

Course | 33 minutes

Understand your role as an auditor in cybersecurity by understanding defense-in-depth and digital asset protection.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0043, K0126, K0200, K0270, K0412, S0085, S0192

Governance of Cybersecurity

Course | 1 hour 23 minutes

Understand governance's role in cybersecurity by understanding how cybersecurity is framed, organized and managed.

NICE Knowledge and Skill Statements:

K0005, K0065, K0127, K0233, K0242, K0270, K0432, K0504, K0579, S0192

Cybersecurity Operations

Course | 2 hours 24 minutes

Understand your role as an auditor in reviewing the cybersecurity controls used by the organization to protect the CIA of systems and data.

NICE Knowledge and Skill Statements:

K0005, K0006, K0018, K0019, K0021, K0026, K0032, K0042, K0074, K0151, K0201, K0202, K0292, K0308, K0317, K0362, K0427, K0480, K0612, S0089, S0167, S0206

Cybersecurity Technology Topics

Course | 1 hour 24 minutes

Understand your role as an auditor in helping to define risk and controls related to specific information technologies and how they affect protection of assets.

NICE Knowledge and Skill Statements:

K0005, K0049, K0070, K0137, K0145, K0269, K0283, K0310, K0435, K0437, K0438, K0487, K0561, K0609, K0610, K0624, S0073, S0173

Cybersecurity Leadership and Management

SKILL PATH

This learning path will introduce you to cybersecurity leadership and management. Drawing on industry standards, frameworks and models, you will explore the key objective elements of cybersecurity leadership.

Cybersecurity Leadership and Management Skill Assessment

Practice Exam | 30 questions

See how your cybersecurity leadership and management skills stack up against other professionals in your field.

Cybersecurity leadership - Information security governance (ISG) overview

Course | 56 minutes

An introduction to the basic principles of cybersecurity leadership and management.

NICE Knowledge and Skill Statements:

K0005, K0072, K0121, K0248, K0477, K0506, K0518, S0018, S0216, S0273, S0309, S0323, S0359

Cybersecurity senior management and information security governance (ISG)

Course | 1 hour 16 minutes

Exploring the roles and responsibilities of senior management in information security.

NICE Knowledge and Skill Statements:

K0005, K0072, K0121, K0248, K0477, K0506, K0518, S0018, S0216, S0273, S0309, S0323, S0359

Aligning information security to the business model

Course | 1 hour 52 minutes

In this course, you'll explore aligning information security to the business model.

NICE Knowledge and Skill Statements:

K0005, K0072, K0121, K0248, K0477, K0506, K0518, S0018, S0216, S0273, S0309, S0323, S0359

Information communication reporting in the organization

Course | 1 hour 23 minutes

In this course, learners will shift the focus from leadership to management and explore cybersecurity information reporting in the organization.

NICE Knowledge and Skill Statements:

K0005, K0072, K0121, K0248, K0477, K0506, S0018, S0216, S0273, S0309, S0323, S0359

Actionable measured KPI and goals

Course | 1 hour 21 minutes

In this course, the learner will explore key risk indicators and key performance indicators in cybersecurity.

NICE Knowledge and Skill Statements:

K0005, K0072, K0121, K0248, K0477, K0506, K0518, S0018, S0216, S0273, S0309, S0323, S0359

Cybersecurity responsibilities into information security programs

Course | 1 hour 33 minutes

For this final course, the learner will explore designing and incorporating cybersecurity within the organization's security programs.

NICE Knowledge and Skill Statements:

K0072, K0121, K0350, K0506, K0512, K0582, K0598

Cybersecurity Management

SKILL PATH

The Cybersecurity Management skill path teaches you governance and risk management related to cybersecurity. You'll learn about developing and managing a security program, enterprise security operations, incident management, compliance and more.

Security & Privacy Policies and Procedures

Course | 24 minutes

This course helps you refresh your knowledge of security and privacy policies and procedures.

NICE Knowledge and Skill Statements:

K0002, K0003, K0004, K0026, K0048, K0101, K0199, K0260, K0261, K0262, K0267, K0527

IR, BC and DR Planning and Procedures

Course | 28 minutes

The fundamentals of incident response, business continuity and disaster recovery are explored in six videos.

NICE Knowledge and Skill Statements:

K0026, K0041, K0042, K0146, K0150, K0231, K0292, K0381, K0399

Effective Incident Management

Course | 25 minutes

Review effective incident management with eight videos on metrics, response procedures and more.

NICE Knowledge and Skill Statements:

K0042, K0150, K0292, K0381

Controls, Metrics and Monitoring

Course | 17 minutes

Take a closer look at what tools you have with this course on controls, metrics and monitoring for security managers.

NICE Knowledge and Skill Statements:

K0002, K0007, K0065, K0622

Security Program Activities

Course | 19 minutes

Explore security program activities with two videos on business case development, program development, documentation and more.

NICE Knowledge and Skill Statements:

K0002, K0006, K0065, K0121, K0154, K0165, K0230, K0263, K0264, K0317, K0381, K0579

Incident Response and Recovery Procedures

Course | 16 minutes

Prepare for possible trouble with this course on incident response and recovery procedures, including designing systems to facilitate incident response.

NICE Knowledge and Skill Statements:

K0021, K0026, K0041, K0042, K0118, K0125, K0128, K0132, K0133, K0150, K0292

Securing Communications and Collaboration Solutions

Course | 14 minutes

Secure your communications and collaboration solutions with this course covering BYOD, mobile device management and more.

NICE Knowledge and Skill Statements:

K0136, K0445, K0446

Security Program Architecture

Course | 22 minutes

Information security program architecture is reviewed and dissected in ten videos. Controls, objectives, program elements and more provide a strong foundation for an aspiring security manager.

NICE Knowledge and Skill Statements:

K0006, K0047, K0087, K0121

Vulnerability Assessment Methods and Tools

Course | 21 minutes

This course helps you broaden your understanding of vulnerability assessment and tools, including tool lists and test types.

NICE Knowledge and Skill Statements:

K0005, K0006, K0013, K0106, K0177, K0301, K0342

Monitoring and Communication

Course | 6 minutes

Enhance your risk management skills with three videos on risk monitoring and communication.

NICE Knowledge and Skill Statements:

K0002

Software Vulnerabilities and Security Controls

Course | 37 minutes

In this course, we take you through the fundamentals of software vulnerabilities and security controls.

NICE Knowledge and Skill Statements:

K0005, K0049, K0070, K0140, K0624

Asset Classification and Operational Considerations

Course | 10 minutes

Review asset classification and operational considerations in five videos, covering vocabulary, diagrams, key terms and important takeaways.

NICE Knowledge and Skill Statements:

K0021, K0090, K0154, K0195, K0211, K0267, K0270, K0287, K0291

Risk Assessment

Course | 17 minutes

Refresh your knowledge of how bad things can get with this course on the four steps of risk assessment: Prepare, Conduct the Assessment, Report and Communicate and Maintain.

NICE Knowledge and Skill Statements:

K0002, K0006, K0149, K0165, K0263

Risk Metric Scenarios

Course | 12 minutes

This course on risk metric scenarios covers analyzing scenarios to secure enterprises and reviewing existing security.

NICE Knowledge and Skill Statements:

K0002, K0183, K0527

Risk Mitigation Strategies and Controls

Course | 26 minutes

Dive into risk mitigation strategies and controls with this course on risk scenarios, responses and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0048, K0148, K0165, K0169, K0194, K0267, K0527, K0556

Business Continuity Planning

Course | 40 minutes

Review business continuity planning and the challenges of disaster recovery with two videos on business impact analysis, auditing business continuity and more.

NICE Knowledge and Skill Statements:

K0006, K0026, K0032, K0041, K0042, K0150, K0165, K0292

Business and Industry Influences and Risks

Course | 15 minutes

Brush up on your knowledge of business and industry influences and risks with this course on enterprise risk management (ERM) and business models.

NICE Knowledge and Skill Statements:

K0002, K0146, K0527

Strategy and Implementation

Course | 17 minutes

Take a fresh look at risk management strategy and implementation. Includes vocabulary, phases and tips for effective information risk management.

NICE Knowledge and Skill Statements:

K0002, K0006, K0165, K0263, K0527

Implementation Action Plan

Course | 11 minutes

Two videos help you review action plan types, action plan implementation strategies and information security program objectives.

NICE Knowledge and Skill Statements:

K0054, K0121, K0198, K0258, K0501

IS Resources and Constraints

Course | 12 minutes

Information security resources and constraints are examined in this two-video course covering personnel, organizational structure and more.

NICE Knowledge and Skill Statements:

K0002, K0007, K0065, K0072, K0199, K0200, K0496, K0501, K0527

Information Security Strategy

Course | 21 minutes

Five videos take you through the core tenets of information security strategy, including strategy elements and metrics.

NICE Knowledge and Skill Statements:

K0002, K0101, K0146, K0293, K0432

IS Roles and Responsibilities

Course | 6 minutes

Refresh your knowledge of information security roles and responsibilities with three videos on key roles and responsibilities, risk management and associated topics.

NICE Knowledge and Skill Statements:

K0579

Introduction to IS Governance

Course | 11 minutes

Three videos provide an introduction to information security governance, including the use of governance and why it is important for an organization.

NICE Knowledge and Skill Statements:

K0101

Disaster Recovery

Course | 36 minutes

Don't let a lack of preparedness compound the effects of a disaster. Learn how to create and test a disaster recovery plan in this six-video course.

NICE Knowledge and Skill Statements:

K0006, K0021, K0026, K0032, K0150, K0210, K0292, K0399, K0519, K0527

Preventative & Detective Measures

Course | 39 minutes

Explore ways to prevent cyber threats from impacting your organization, and learn how to quickly detect the threats that do slip through your defenses.

NICE Knowledge and Skill Statements:

K0004, K0006, K0049, K0073, K0074, K0132, K0145, K0167, K0205, K0275, K0480, K0487, K0488, K0561

Computer Crime Investigations

Course | 32 minutes

Refresh your knowledge of cybercrime investigations with this overview course covering the investigation process and the discovery of digital evidence.

NICE Knowledge and Skill Statements:

K0017, K0118, K0122, K0123, K0125, K0128, K0133, K0155, K0156, K0184, K0222, K0251, K0304, K0433

Access Control Fundamentals

Course | 1 hour 37 minutes

Take a deep dive into one of the fundamental concepts of security: access control. Learn how to give the right people access to the right information in a secure way.

NICE Knowledge and Skill Statements:

K0007, K0033, K0056, K0065, K0071, K0104, K0158, K0179, K0211, K0332, K0336, K0452, K0488, S0023, S0031

Asset Security

Course | 39 minutes

Learn how to secure sensitive data, including managing and classifying data, working with data at rest and in transit, and implementing data security controls.

NICE Knowledge and Skill Statements:

K0049, K0065, K0083, K0195, K0287, K0377, K0622

Security Policies

Course | 22 minutes

Explore security policies and control frameworks and how they help drive the overall security of an organization.

NICE Knowledge and Skill Statements:

K0004, K0006, K0157, K0169, K0215, K0242, K0243, K0264

Risk Management

Course | 49 minutes

Dive deep into risk management, including risk frameworks, assessments and modeling, as well as employee security awareness, vendor security and other issues.

NICE Knowledge and Skill Statements:

K0002, K0005, K0047, K0048, K0162, K0165, K0169, K0214, K0295, K0455, K0527

Enterprise Security Risk Management

SKILL PATH

The Enterprise Security Risk Management skill path covers essential enterprise risk topics, including risk identification and assessment, implementing security controls, regulatory compliance, strategy and culture, and more.

Key Risk Indicators and Key Performance Indicators

Course | 49 minutes

Learn key risk indicators, key performance indicators, plus monitoring and reporting tools and techniques.

NICE Knowledge and Skill Statements:

K0002, K0054, K0145, K0527

Monitoring and Communication

Course | 6 minutes

Enhance your risk management skills with three videos on risk monitoring and communication.

NICE Knowledge and Skill Statements:

K0002

Asset Classification and Operational Considerations

Course | 10 minutes

Review asset classification and operational considerations in five videos, covering vocabulary, diagrams, key terms and important takeaways.

NICE Knowledge and Skill Statements:

K0021, K0090, K0154, K0195, K0211, K0267, K0270, K0287, K0291

Risk Assessment

Course | 17 minutes

Two videos take you through risk assessment methodologies, vocabulary and examples.

NICE Knowledge and Skill Statements:

K0002, K0006, K0149, K0165, K0263

Risk Metric Scenarios

Course | 12 minutes

This course on risk metric scenarios covers analyzing scenarios to secure enterprises and reviewing existing security.

NICE Knowledge and Skill Statements:

K0002, K0183, K0527

Access Control Fundamentals

Course | 1 hour 37 minutes

Take a deep dive into one of the fundamental concepts of security: access control. Learn how to give the right people access to the right information in a secure way.

NICE Knowledge and Skill Statements:

K0007, K0033, K0056, K0065, K0071, K0104, K0158, K0179, K0211, K0332, K0336, K0452, K0488, S0023, S0031

Security Policies

Course | 22 minutes

Explore security policies and control frameworks and how they help drive the overall security of an organization.

NICE Knowledge and Skill Statements:

K0004, K0006, K0157, K0169, K0215, K0242, K0243, K0264

Risk Management

Course | 49 minutes

Dive deep into risk management, including risk frameworks, assessments and modeling, as well as employee security awareness, vendor security and other issues.

NICE Knowledge and Skill Statements:

K0002, K0005, K0047, K0048, K0162, K0165, K0169, K0214, K0295, K0455, K0527

Regulatory Compliance

Course | 30 minutes

Explore the compliance issues related to digital data, including privacy laws, regulations, intellectual property issues and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0006, K0157, K0196, K0260, K0261, K0262, K0410, K0524, K0615

Security Governance Principles

Course | 16 minutes

Explore security governance and how it relates to business processes and strategies in this brief overview course.

NICE Knowledge and Skill Statements:

K0004, K0006, K0047, K0146, K0261, K0295, K0511, K0579

Risk Mitigation Strategies and Controls

Course | 26 minutes

Dive into risk mitigation strategies and controls with this course on risk scenarios, responses and more.

NICE Knowledge and Skill Statements:

K0002, K0004, K0048, K0148, K0165, K0169

Risk Identification Frameworks and Methods

Course | 39 minutes

Review best practices for IT risk management, including the steps that risk managers need to go through.

NICE Knowledge and Skill Statements:

K0002, K0048, K0165

Control Design and Implementation

Course | 1 hour 4 minutes

Understand the major types of risk controls and their interdependencies.

NICE Knowledge and Skill Statements:

K0002, K0018, K0019, K0048, K0073, K0075, K0201, K0291, K0427, K0488, S0036

Risk Response Options

Course | 43 minutes

Alignment with business objectives is one of the drivers of risk management.

NICE Knowledge and Skill Statements:

K0002, K0005, K0101

Risk-Based Decision Making

Course | 52 minutes

Learn about different business-related and IT management aspects that factor into risk assessment.

NICE Knowledge and Skill Statements:

K0002, K0005, K0021, K0026, K0059, K0072, K0121, K0147, K0165, K0169, K0199, K0335, K0431, K0455

Risk and Control Analysis

Course | 1 hour 15 minutes

Know how to use controls, along with incident management, to determine the state of current risk.

NICE Knowledge and Skill Statements:

K0013, K0165, K0342

Risk Assessment Techniques

Course | 33 minutes

Learn how to assess the potential impacts of the various IT risks.

NICE Knowledge and Skill Statements:

K0002, K0165

IT Security Risk Concepts

Course | 1 hour 45 minutes

Understand the security risks concepts and principles that impact IT risk practitioners' jobs.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0007, K0065, K0070, K0106, K0151, K0267, K0342, K0527

Impact of Compliance

Course | 28 minutes

Refresh your awareness about the regulatory and statutory privacy and security requirements and their impact on risk.

NICE Knowledge and Skill Statements:

K0003, K0066, K0168, K0260, K0261, K0262, K0267, K0410, K0615

IT Risk Strategy

Course | 31 minutes

Dive deeper into the importance of an IT strategy and how it should align with business goals, objectives and values.

NICE Knowledge and Skill Statements:

K0002, K0003, K0101, K0293, S0038

Risk Culture and Communication

Course | 27 minutes

Risk culture, appetite and communication of risk are important in understanding how risk relates to the organization's values, goals and objectives.

NICE Knowledge and Skill Statements:

K0002, K0527, S0070

Certified SCADA Security Architect (CSSA)

CERTIFICATION PATH

The Certified SCADA Security Architect (CSSA) certification path covers everything from field-based attacks to automated vulnerability assessments for SCADA networks. You'll learn how to defend against both internal and external attackers to provide holistic security for critical industrial automation systems.

Skill Assessment

Skill assessment | 20 questions

See how your CCSA skills stack up against other professionals in your field.

CSSA Practice Exam

Practice Exam | 75 questions

Prepare for your CCSA exam and test your domain knowledge.

SCADA Cyber Range

Cyber range | 15 labs

Gain practical experience and build real-world Supervisory Control and Data Acquisition (SCADA) skills through 15 hands-on labs in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0046, S0051, S0057, S0067, S0081, S0120, S0156, S0158, S0221

Introduction to SCADA Security

Course | 19 minutes

Get an introduction to SCADA security, including ICS types, ICS components, process control and safety systems, and strengths and weaknesses.

NICE Knowledge and Skill Statements:

K0005, K0137, K0170, K0437

ICS Protocols

Course | 1 hour 7 minutes

Explore common Industrial Control System (ICS) protocols and their security features as you progress through this 15-video course.

NICE Knowledge and Skill Statements:

K0005, K0137, K0170, K0417, K0437

SCADA Security Frameworks

Course | 1 hour 7 minutes

This course will begin your reintroduction to SCADA security frameworks, covering common threats to SCADA, relevant security standards and bodies, developing SCADA security policies and more.

NICE Knowledge and Skill Statements:

K0005, K0006, K0065, K0137, K0177, K0267, K0437, K0612

SCADA Security Assessment

Course | 44 minutes

Review your understanding of SCADA security assessment with this course covering SCADA security objectives, security assessment programs and more.

NICE Knowledge and Skill Statements:

K0002, K0013, K0040, K0165, K0290, K0342, K0437

SCADA Device Identification and Analysis

Course | 43 minutes

Make sure you know what you need to know with this course on SCADA device identification and analysis.

NICE Knowledge and Skill Statements:

K0004, K0137, K0170, K0177, K0274, K0342, K0437, K0536, K0565

SCADA Vulnerabilities

Course | 26 minutes

Explore SCADA vulnerabilities with this course covering common vulnerabilities, vulnerability scanning, server OS testing and more.

NICE Knowledge and Skill Statements:

K0005, K0060, K0071, K0077, K0137, K0170, K0177, K0342, K0437, K0536, K0565

Pentesting SCADA Services and Protocols

Course | 24 minutes

Review what it takes to attack standard services, server OS, ICS protocols and more with this course on pentesting SCADA services and protocols.

NICE Knowledge and Skill Statements:

K0005, K0060, K0137, K0170, K0177, K0342, K0437, K0536, K0565

SCADA Access Controls

Course | 31 minutes

In this course, you'll look at the importance of SCADA access controls. Review physical safety, access control models and more.

NICE Knowledge and Skill Statements:

K0007, K0033, K0056, K0065, K0137, K0170, K0437

Remote Access and Field Site Security

Course | 36 minutes

Re-familiarize yourself with the challenges of remote access and field site security through this course on remote access techologies, field site firewalls and more.

NICE Knowledge and Skill Statements:

K0071, K0104, K0137, K0190, K0427, K0437, K0561

SCADA Network Security

Course | 39 minutes

In this course, you'll refresh your knowledge of SCADA network security through secure network design, firewalls and logical security zones.

NICE Knowledge and Skill Statements:

K0033, K0049, K0137, K0145, K0179, K0437, K0561, K0565

SCADA Intrusion Detection and Incident Response

Course | 61 minutes

Get to grips with what you need to know for SCADA intrusion detection and incident response.

NICE Knowledge and Skill Statements:

K0004, K0041, K0042, K0046, K0137, K0324, K0437

SCADA Preventative Controls

Course | 47 minutes

Brush up on what you need to prevent or mitigate disasters with this course on SCADA preventative controls.

NICE Knowledge and Skill Statements:

K0033, K0049, K0074, K0162, K0205, K0324, K0437, K0480

ICS/SCADA Security Best Practices

Course | 26 minutes

Learn about the three aspects of SCADA security best practices: prevention, detection and correction.

NICE Knowledge and Skill Statements:

K0004K0005, K0073, K0437, K0527

CSSA Exam Overview

Course | 4 minutes

This course will give you an overview of the Certified SCADA Security Architect (CSSA) exam and what to expect.

NICE Knowledge and Skill Statements:

NONE

IAPP Certified Information Privacy Professional/Europe (CIPP/E)

CERTIFICATION PATH

In this learning path, you will explore the details of the IAPP CIPP/E subject matter and learn more about privacy law, the rights of individuals and the common body of knowledge.

CIPP/E Practice Exam

Practice Exam | 35 questions

Prepare for your CISA exam and test your domain knowledge.

NICE Knowledge and Skill Statements:

Origins and Historical Context of Data Protection Law

Course | 36 minutes

A discussion of privacy versus data protection and different approaches around the world.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0260, K0261, K0262, K0524

European Union Institutions

Course | 42 minutes

A discussion on the differences between the Council of Europe and the EU.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0222, K0260, K0261, K0262, K0341, K0524

EU Legislative Framework

Course | 35 minutes

The timeline of data protection law and the extent of GDPR application.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0222, K0260, K0261, K0262, K0341, K0504, K0524, S0147

Data Protection Concepts and Scope

Course | 44 minutes

A discussion on types of personal data and further definitions of roles assigned by the GDPR.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0196, K0222, K0260, K0261, K0262, K0504, K0524, S0147

Data Processing Principles

Course | 39 minutes

A discussion of the application of the privacy principles and their role in data protection law.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0222, K0260, K0261, K0262, K0504, K0524, S0147

Lawful Processing Criteria

Course | 43 minutes

A discussion on how to process data with lawful reasoning.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0222, K0260, K0261, K0262, K0504, K0524

Transparency and Data Subject's Rights

Course | 55 minutes

A discussion on the rights of the data subjects under the GDPR.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0260, K0261, K0262, S0147

Obligations of Controllers and Processors

Course | 51 minutes

A discussion of controllers and processor obligations under the GDPR.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0260, K0261, K0262, S0147

Security and Data Breaches

Course | 37 minutes

Exploring security and data breaches, and what the law requires.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0168, K0222, K0260, K0261, K0262, S0147

International Data Transfer

Course | 45 minutes

Exploring international data transfer and its challenges.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0168, K0222, K0260, K0261, K0262, K0411

Powers of the Regulator

Course | 26 minutes

A discussion on the roles of the regulators and their enforcement powers.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0168, K0222, K0260, K0261, K0262, K0411

Application of the Law

Course | 38 minutes

The GDPR and its interactions with different laws.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0168, K0222, K0260, K0261, K0262, K0411

ICS/SCADA Security Analyst

SKILL PATH

The ICS/SCADA Security Analyst skill path provides you with the knowledge needed to defend the systems that control critical infrastructure. You'll learn about assessing the security of industrial control and SCADA systems and protecting them from cyber threats.

ICS/SCADA Pentesting CTF: Lights Out

Cyber range | 1 lab

You are the whitehat. You've become aware of a plot to launch a proof-of-concept cyber-attack against a large sports stadium in which the attackers will take over the facility's power management system and turn out the lights during a Sunday night sporting event.

NICE Knowledge and Skill Statements:

S0051, S0078, S0081

SCADA Security Frameworks

Course | 1 hour 6 minutes

This course will begin your reintroduction to SCADA security frameworks, covering common threats to SCADA, relevant security standards and bodies, developing SCADA security policies and more.

NICE Knowledge and Skill Statements:

K0005, K0006, K0065, K0137, K0177, K0267, K0437, K0612

SCADA Security Assessment

Course | 44 minutes

Review your understanding of SCADA security assessment with this course covering SCADA security objectives, security assessment programs and more.

NICE Knowledge and Skill Statements:

K0002, K0013, K0040, K0165, K0290, K0342, K0437

SCADA Device Identification and Analysis

Course | 43 minutes

Make sure you know what you need to know with this course on SCADA device identification and analysis.

NICE Knowledge and Skill Statements:

K0004, K0137, K0170, K0177, K0274, K0342, K0437, K0536, K0565

SCADA Vulnerabilities

Course | 26 minutes

Explore SCADA vulnerabilities with this course covering common vulnerabilities, vulnerability scanning, server OS testing and more.

NICE Knowledge and Skill Statements:

K0005, K0060, K0071, K0077, K0137, K0170, K0177, K0342, K0437, K0536, K0565

Pentesting SCADA Services and Protocols

Course | 24 minutes

Review what it takes to attack standard services, server OS, ICS protocols and more with this course on pentesting SCADA services and protocols.

NICE Knowledge and Skill Statements:

K0005, K0060, K0137, K0170, K0177, K0342, K0437, K0536, K0565

SCADA Access Controls

Course | 31 minutes

In this course, you'll look at the importance of SCADA access controls. Review physical safety, access control models and more.

NICE Knowledge and Skill Statements:

K0007, K0033, K0056, K0065, K0137, K0170, K0437

Remote Access and Field Site Security

Course | 36 minutes

Re-familiarize yourself with the challenges of remote access and field site security through this course on remote access techologies, field site firewalls and more.

NICE Knowledge and Skill Statements:

K0071, K0104, K0137, K0190, K0427, K0437, K0561

SCADA Network Security

Course | 39 minutes

In this course, you'll refresh your knowledge of SCADA network security through secure network design, firewalls and logical security zones.

NICE Knowledge and Skill Statements:

K0033, K0049, K0137, K0145, K0179, K0437, K0561, K0565

SCADA Intrusion Detection and Incident Response

Course | 61 minutes

Get to grips with what you need to know for SCADA intrusion detection and incident response.

NICE Knowledge and Skill Statements:

K0004, K0041, K0042, K0046, K0137, K0324, K0437

SCADA Preventative Controls

Course | 46 minutes

Brush up on what you need to prevent or mitigate disasters with this course on SCADA preventative controls.

NICE Knowledge and Skill Statements:

K0033, K0049, K0074, K0162, K0205, K0324, K0437, K0480

Implementing Controls for HIPAA Compliance

SKILL PATH

This path will help students and professionals understand how to maintain the confidentiality, integrity and availability of PHI and ePHI. You'll get to grips with protecting ePHI from unauthorized use and disclosure, and the importance of helping employees stay compliant with the rules.

Skill Assessment

Skill assessment | 20 questions

See how your HIPAA compliance skills stack up against other professionals in your field.

Privacy and Security in Health Care and Public Health

Course | 25 minutes

This course explores the nature and purpose of HIPAA. Beginning with why HIPAA is important, explore the advantages of HIPAA implementation and the importance of its role.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0260, K0262

HIPAA Data Privacy and Data Regulation

Course | 1 hour 26 minutes

In this course, we explore helpful suggestions on how HIPAA businesses should comply not only to HIPAA regulations but also to be more familiar with the state laws within their jurisdiction.

NICE Knowledge and Skill Statements:

K0003, K0044, K0222, K0262

How to Conduct Assessments

Course | 1 hour 9 minutes

In this course, you'll dig deeper into the how and why of assessments, as well as different assessment types. You'll learn how assessments are important to understand where you're at within the HIPAA compliance meter.

NICE Knowledge and Skill Statements:

K0003, K0044, K0066, K0222, K0262

Key Principles of Security – NIST Standards

Course | 53 minutes

In this course, you'll dive deeper into the details of NIST. Explore what NIST is, its families and security controls, and look at an introductory resource guide for implementing the HIPAA security rule.

NICE Knowledge and Skill Statements:

K0003, K0025, K0044, K0195, K0222, K0260, K0262, S0374

HIPAA Training and Awareness

Course | 26 minutes

HIPAA requires covered entities to conduct training. But do you know what areas to cover? How often you must conduct your training? This course will help you get your HIPAA training off the ground and maintain it.

NICE Knowledge and Skill Statements:

K0003, K0243, K0245, K0262, K0512

Health Care Data Breaches

Course | 29 minutes

This course will help you understand the main differences between an incident and a breach. You'll take a look at why breaches and incidents are important, and why the difference between them matters.

NICE Knowledge and Skill Statements:

K0003, K0044, K0260, K0262, K0287

HIPAA Compliance Checklist

Course | 26 minutes

Now that we have learned HIPAA and understand the importance of implementing HIPAA controls, where do we start? Take a look at building a culture of compliance, data hygiene and the importance of mobile device security.

NICE Knowledge and Skill Statements:

K0003, K0044, K0222, K0260, K0262

Introduction to Applied Cryptography and Cryptanalysis

SKILL PATH

This learning path introduces cryptography, its applications, and methods for decrypting and deobfuscating data. The fundamentals of cryptography are introduced as well as common applications of cryptography. The path also introduces weak algorithms used by malware, how to identify them and methods for deobfuscating the data.

Skill Assessment

Skill assessment | 20 questions

See how your applied cryptography and cryptanalysis skills stack up against other professionals in your field.

Cryptography and Cryptanalysis Project

Project | 2 hours 10 minutes

Practice your cryptography skills by solving challenges.

NICE Knowledge and Skill Statements:

S0089, S0199, S0221, S0258

Introduction to Cryptography

Course | 25 minutes

This course defines the basic vocabulary and concepts of cryptography.

NICE Knowledge and Skill Statements:

K0308, K0412, K0427

Fundamentals of Cryptography

Course | 20 minutes

This course describes mathematics and structures commonly used in cryptography.

NICE Knowledge and Skill Statements:

K0005, K0018, K0019, K0308, K0403, K0412, K0427

Symmetric Cryptography

Course | 45 minutes

This course provides an introduction to symmetric encryption algorithms.

NICE Knowledge and Skill Statements:

K0427, K0018, K0019, K0201, K0403

Asymmetric Cryptography

Course | 36 minutes

This course provides an introduction to asymmetric encryption algorithms.

NICE Knowledge and Skill Statements:

K0005, K0018, K0019, K0403, K0427

Hash Functions

Course | 17 minutes

This course provides an introduction to hash functions.

NICE Knowledge and Skill Statements:

K0018, K0427, S0089, S0298

Public Key Infrastructure (PKI)

Course | 18 minutes

This course describes the use of cryptography in the PKI infrastructure.

NICE Knowledge and Skill Statements:

K0004, K0019, K0056, K0427

SSL and TLS

Course | 26 minutes

This course describes the use of cryptography in SSL and TLS.

NICE Knowledge and Skill Statements:

K0005, K0018, K0019, K0308, K0427, K0603

Virtual Private Networks (VPNs)

Course | 18 minutes

This course describes the use of cryptography in Virtual Private Networks (VPNs).

NICE Knowledge and Skill Statements:

K0004, K0005, K0071, K0104, K0427, K0428, S0059

Secure Credential Management

Course | 26 minutes

This course describes the use of cryptography in securely managing user credentials.

NICE Knowledge and Skill Statements:

K0005, K0007, K0158, K0336, K0427

Full Disk Encryption

Course | 10 minutes

This course describes the use of cryptography in full disk encryption.

NICE Knowledge and Skill Statements:

K0005, K0622

Blockchain Technology

Course | 25 minutes

This course describes the use of cryptography in blockchain technology.

NICE Knowledge and Skill Statements:

K0038, K0059, K0622

Introduction to Cryptanalysis

Course | 36 minutes

This course introduces you to the field of cryptanalysis.

NICE Knowledge and Skill Statements:

K0305, K0403, K0427

Applied Cryptanalysis

Course | 25 minutes

This course provides demonstrations of using cryptanalysis for incident response.

NICE Knowledge and Skill Statements:

K0005, K0305, K0403, K0427

ISACA Certified Information Systems Auditor (CISA)

CERTIFICATION PATH

The Certified Information Systems Auditor (CISA) certification path builds your knowledge of auditing information systems. You'll learn the tools and guidelines involved in the IT auditing process as well as concepts such as business continuity, enterprise IT governance, common security controls and more.

Skill Assessment

Skill assessment | 20 questions

See how your CISA skills stack up against other professionals in your field.

CISA Practice Exam

Practice Exam | 699 questions

Prepare for your CISA exam and test your domain knowledge.

NICE Knowledge and Skill Statements:

NONE

CISA Introduction

Course | 19 minutes

Introduce yourself to CISA with this course introduction covering study plans, CISA stats and details, and more.

NICE Knowledge and Skill Statements:

NONE

IS Audit Functions

Course | 8 minutes

Explore the functions of an information security audit with this course looking at auditor practices, IS audit purposes and more.

NICE Knowledge and Skill Statements:

K0003, K0004, K0044, K0047, K0264

Business Process Applications and Controls

Course | 42 minutes

Explore the Business Process section and the controls you'll need to understand during your CISA study.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0044, K0047, K0146, K0263, K0264, S0085

Types of Controls and Risk Assessments

Course | 21 minutes

Explore the types of controls and risk assessments in four parts, beginning with Control Objectives and Control Measures.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0044, K0047, K0065, K0264, S0034, S0085, S0147, S0171

Continuous Auditing

Course | 39 minutes

In this course, you'll look at the five parts of the Audit Project Management section, as well as sampling, audit report objectives and more.

NICE Knowledge and Skill Statements:

K0002, K0005, K0047, K0121, K0432, S0085

Governance and Management of IT

Course | 39 minutes

Dig deep into the details of governance and management of IT.

NICE Knowledge and Skill Statements:

K0002 , K0027, K0044, K0146, K0154, K0198, K0429, K0501, K0504, S0085

IT Organizational Structure

Course | 32 minutes

Explore IT organizational structure and the critical associated concepts.

NICE Knowledge and Skill Statements:

K0002, K0004, K0027, K0044, K0047, K0267, K0429, K0598, S0085

IT Management

Course | 39 minutes

In this course, you'll review the details of IT management and more.

NICE Knowledge and Skill Statements:

K0004, K0027, K0044, K0053, K0101, K0154, K0198, K0257, K0265, K0267, K0270, K0429, S0085

Information Systems Acquisition

Course | 32 minutes

Take a closer look at the first part of the Information Systems Acquisition and Development subdomain.

NICE Knowledge and Skill Statements:

K0090, K0101, K0121, K0154, K0257, K0270, S0085, S0273

Business Cases and Development

Course | 1 hour 4 minutes

Take some time to explore the second part of Information Systems Acquisition and Development.

NICE Knowledge and Skill Statements:

K0004, K0044, K0080, K0081, K0121, K0140, K0183, K0267, K0429, K0622, S0085, S0273

Information Systems Implementation

Course | 42 minutes

Wrap up Domain 3 of CISA with this course covering Control Identification and Design and Information Systems Implementation.

NICE Knowledge and Skill Statements:

K0004, K0044, K0074, K0091, K0178, K0267, K0275, K0290, K0531, K0622, S0085, S0273

Information Systems Operations

Course | 1 hour 18 minutes

Dive into Part A of CISA Domain 4 in this course covering Common Technology Components and more.

NICE Knowledge and Skill Statements:

K0002, K0074, K0109, K0275, K0317, K0361, K0419, K0589, K0622, S0085, S0273

Business Resilience

Course | 23 minutes

Explore Part B of the Information Systems Operations domain.

NICE Knowledge and Skill Statements:

K0021, K0026, K0032, K0210, S0027, S0085, S0273

Business Continuity

Course | 40 minutes

Wrap up Part B of Domain 4 with this course on business continuity.

NICE Knowledge and Skill Statements:

K0021, K0026, K0210, S0027, S0032, S0085, S0273

Asset Security Frameworks, Standards and Guidelines

Course | 41 minutes

In this course, you'll start on CISA Domain 5 by covering Information Asset Security and Control topics.

NICE Knowledge and Skill Statements:

K0005, K0007, K0261, K0262, K0263, K0622, S0085

Identity and Access Management

Course | 1 hour 6 minutes

Continue with Domain 5, Part A of CISA in this course covering identification and authentication topics.

NICE Knowledge and Skill Statements:

K0004, K0007, K0056, K0065, S0085

Network Infrastructure Security

Course | 52 minutes

Network infrastructure security has no secrets in this three-video course. Covers structure, auditing and more.

NICE Knowledge and Skill Statements:

K0004, K0005, K0010, K0044, K0061, K0108, K0113, K0221, K0286, K0417, K0556, K0560, K0561, K0600, S0085, S0192

Asset Security

Course | 51 minutes

Wrap up part A of CISA Domain 5 with this course covering asset security topics.

NICE Knowledge and Skill Statements:

K0004, K0005, K0018, K0019, K0044, K0065, K0113, K0136, K0159, K0190, K0195, K0230, K0287, K0322, K0427, K0609, K0622, S0085

Security Event Management

Course | 42 minutes

Explore Part B of CISA Domain 5 with this course on security event management.

NICE Knowledge and Skill Statements:

K0003, K0005, K0042, K0118, K0145, K0150, K0215, K0243, K0245, K0290, K0324, K0474, K0503, K0548, K0603, S0085, S0273

ISACA Certified Information Security Manager (CISM)

CERTIFICATION PATH

The Certified Information Security Manager (CISM) certification path is designed for individuals that oversee, design or assess an enterprise's information security. You'll learn about information security governance, risk management, program development and incident management.

Skill Assessment

Skill assessment | 20 questions

See how your CISM skills stack up against other professionals in your field.

CISM Practice Exam

Practice Exam | 931 questions

Prepare for your CISM exam and test your domain knowledge.

Introduction to IS Governance

Course | 11 minutes

Three videos provide an introduction to information security governance, including the use of governance and why it is important for an organization.

NICE Knowledge and Skill Statements:

K0101

IS Roles and Responsibilities

Course | 6 minutes

Refresh your knowledge of information security roles and responsibilities with three videos on key roles and responsibilities, risk management and associated topics.

NICE Knowledge and Skill Statements:

K0579

Information Security Strategy

Course | 21 minutes

Five videos take you through the core tenets of information security strategy, including strategy elements and metrics.

NICE Knowledge and Skill Statements:

K0002, K0101, K0146, K0293, K0432

IS Resources and Constraints

Course | 12 minutes

Information security resources and constraints are examined in this two-video course covering personnel, organizational structure and more.

NICE Knowledge and Skill Statements:

K0002, K0007, K0065, K0072, K0199, K0200, K0496, K0501, K0527

Implementation Action Plan

Course | 11 minutes

Two videos help you review action plan types, action plan implementation strategies and information security program objectives.

NICE Knowledge and Skill Statements:

K0054, K0121, K0198, K0258, K0501

Strategy and Implementation

Course | 17 minutes

Take a fresh look at risk management strategy and implementation. Includes vocabulary, phases and tips for effective information risk management.

NICE Knowledge and Skill Statements:

K0002, K0006, K0165, K0263, K0527

Risk Assessment

Course | 17 minutes

Two videos take you through risk assessment methodologies, vocabulary and examples.

NICE Knowledge and Skill Statements:

K0002, K0006, K0149, K0165, K0263

Asset Classification and Operational Considerations

Course | 10 minutes

Review asset classification and operational considerations in five videos, covering vocabulary, diagrams, key terms and important takeaways.

NICE Knowledge and Skill Statements:

K0021, K0090, K0154, K0195, K0211, K0267, K0270, K0287, K0291

Monitoring and Communication

Course | 6 minutes

Enhance your risk management skills with three videos on risk monitoring and communication.

NICE Knowledge and Skill Statements:

K0002

Security Program Architecture

Course | 22 minutes

Information security program architecture is reviewed and dissected in ten videos. Controls, objectives, program elements and more provide a strong foundation for an aspiring security manager.

NICE Knowledge and Skill Statements:

K0006, K0047, K0087, K0121

Security Program Activities

Course | 19 minutes

Explore security program activities with two videos on business case development, program development, documentation and more.

NICE Knowledge and Skill Statements:

K0002, K0006, K0065, K0121, K0154, K0165, K0230, K0263, K0264, K0317, K0381, K0579

Controls, Metrics and Monitoring

Course | 17 minutes

Take a closer look at what tools you have with this course on controls, metrics and monitoring for security managers.

NICE Knowledge and Skill Statements:

K0002, K0007, K0065, K0622

Effective Incident Management

Course | 25 minutes

Review effective incident management with eight videos on metrics, response procedures and more.

NICE Knowledge and Skill Statements:

K0042, K0150, K0292, K0381

IR, BC and DR Planning and Procedures

Course | 28 minutes

The fundamentals of incident response, business continuity and disaster recovery are explored in six videos.

NICE Knowledge and Skill Statements:

K0026, K0041, K0042, K0146, K0150, K0231, K0292, K0381, K0399

ISACA Certified in Risk and Information Systems Control

CERTIFICATION PATH

The Certified in Risk and Information Systems Control (CRISC) certification path teaches you how to design, implement, monitor and maintain risk-based, efficient and effective IS controls.

Skill Assessment

Skill assessment | 20 questions

See how your CRISC skills stack up against other professionals in your field.

CRISC Practice Exam

Practice Exam | 156 questions

Prepare for your CRISC exam and test your domain knowledge.

Risk Identification Overview

Course | 59 minutes

Understand what you'll need to prepare for the ISACA CRISC certification exam, and learn what to expect on the exam.

NICE Knowledge and Skill Statements:

NONE

Risk Identification Frameworks and Methods

Course | 39 minutes

Review best practices for IT risk management, including the steps that risk managers need to go through.

NICE Knowledge and Skill Statements:

K0002, K0048, K0165

Risk Culture and Communication

Course | 27 minutes

Risk culture, appetite and communication of risk are important in understanding how risk relates to the organization's values, goals and objectives.

NICE Knowledge and Skill Statements:

K0002, K0527, S0070

IT Risk Strategy

Course | 31 minutes

Dive deeper into the importance of an IT strategy and how it should align with business goals, objectives and values.

NICE Knowledge and Skill Statements:

K0002, K0003, K0101, K0293, S0038

Impact of Compliance

Course | 28 minutes

Refresh your awareness about the regulatory and statutory privacy and security requirements and their impact on risk.

NICE Knowledge and Skill Statements:

K0003, K0066, K0168, K0260, K0261, K0262, K0267, K0410, K0615

IT Security Risk Concepts

Course | 1 hour 45 minutes

Understand the security risks concepts and principles that impact IT risk practitioners' jobs.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0007, K0065, K0070, K0106, K0151, K0267, K0342, K0527

Risk Assessment Overview

Course | 37 minutes

Get an overview of the IT risk assessment aspects that risk practitioners need to know.

NICE Knowledge and Skill Statements:

K0165

Risk Assessment Techniques

Course | 33 minutes

Learn how to assess the potential impacts of the various IT risks.

NICE Knowledge and Skill Statements:

K0002, K0165

Risk and Control Analysis

Course | 1 hour 15 minutes

Know how to use controls, along with incident management, to determine the state of current risk.

NICE Knowledge and Skill Statements:

K0013, K0165, K0342

Risk-Based Decision Making

Course | 52 minutes

Learn about different business-related and IT management aspects that factor into risk assessment.

NICE Knowledge and Skill Statements:

K0002, K0005, K0021, K0026, K0059, K0072, K0121, K0147, K0165, K0169, K0199, K0335, K0431, K0455

Risk Response and Mitigation Overview

Course | 18 minutes

See the learning objectives for CRISC Domain 3, Risk Response and Mitigation.

NICE Knowledge and Skill Statements:

K0002

Risk Response Options

Course | 43 minutes

Alignment with business objectives is one of the drivers of risk management.

NICE Knowledge and Skill Statements:

K0002, K0005, K0101

Control Design and Implementation

Course | 1 hour 4 minutes

Understand the major types of risk controls and their interdependencies.

NICE Knowledge and Skill Statements:

K0002, K0018, K0019, K0048, K0073, K0075, K0201, K0291, K0427, K0488, S0036

Risk and Control Monitoring and Reporting Overview

Course | 15 minutes

Gain the knowledge you need for monitoring and reporting risks.

NICE Knowledge and Skill Statements:

K0002

Key Risk Indicators and Key Performance Indicators

Course | 49 minutes

Learn key risk indicators, key performance indicators, plus monitoring and reporting tools and techniques.

NICE Knowledge and Skill Statements:

K0002, K0054, K0145, K0527

ITIL 4 Foundation

CERTIFICATION PATH

The ITIL® 4 Foundations certification path teaches you best practices for aligning IT services with business goals. You'll learn about the ITIL framework, the four dimensions of service management, best practices for implementing ITIL and more.

Skill Assessment

Skill assessment | 20 questions

See how your ITIL 4 Foundation skills stack up against other professionals in your field.

ITIl 4 Foundation Practice Exam

Practice Exam | 80 questions

Prepare for your ITIL 4 Foundation exam and test your domain knowledge.

ITIL 4 Foundation Introduction

Course | 15 minutes

Learn about the role of the ITIL framework in managing IT service in the era of the 4th industrial revolution.

NICE Knowledge and Skill Statements:

K0200, K0291

Service Management

Course | 1 hour 1 minute

Understand the service management definitions and concepts that apply to ITIL as well as other frameworks.

NICE Knowledge and Skill Statements:

K0200, K0291, K0293, S0005, S0122

Four Dimensions of Service Management

Course | 39 minutes

Take a closer look at how the model based on the four dimensions of IT service management applies within ITIL.

NICE Knowledge and Skill Statements:

K0200, K0291, K0293, S0005, S0122

Service Value System

Course | 10 minutes

Get an overview of the service value system and how the organization's systems and components work together to enable value co-creation.

NICE Knowledge and Skill Statements:

K0200, K0291, K0293, S0005, S0122

Guiding Principles

Course | 43 minutes

Discover the seven guiding principles organizations should consider while adapting ITIL guidance to their needs.

NICE Knowledge and Skill Statements:

K0200, K0291, K0293, S0005, S0122

Service Value Chain

Course | 41 minutes

Get a breakdown of the different activities in the service value chain and how they interconnect.

NICE Knowledge and Skill Statements:

K0004, K0200, K0291, K0293, S0005, S0122, S0296

Continual Improvement

Course | 23 minutes

Learn about the continual improvement model, its purpose and its place within the service value chain and the service value system.

NICE Knowledge and Skill Statements:

K0200, K0291, K0293, S0005, S0122

Categories of Practices

Course | 37 minutes

Become aware of the 34 practices that support value chain activities within the ITIL framework.

NICE Knowledge and Skill Statements:

K0200, K0291, K0293, S0005, S0122

Service Management Practices

Course | 1 hour

Dive into the ITIL service management practices category, which includes 17 practices developed over 20-30 years.

NICE Knowledge and Skill Statements:

K0200, K0291, K0293, S0005, S0122

Technical Management Practices

Course | 3 minutes

Review the three ITIL technical management practices that have been adapted from technology management domains.

NICE Knowledge and Skill Statements:

K0200, K0291, K0293, S0005, S0122

ITIL 4 Foundation Conclusion

Course | 10 minutes

Wrap up your knowledge of ITIL foundations by putting together everything you've learned.

NICE Knowledge and Skill Statements:

K0200

JNCIA-Junos

CERTIFICATION PATH

This learning path covers all exam topics for the Juniper JN0-103 exam required for the JNCIA-Junos certification. This is the recently updated exam, superseding the JN0-102.

Skill Assessment

Skill assessment | 20 questions

See how your JNCIA-Junos skills stack up against other professionals in your field.

CASP+ Practice Exam

Practice Exam | 65 questions

Prepare for your JNCIA-Junos exam and test your domain knowledge.

Junos OS Fundamentals

Course | 27 minutes

Refresh your knowledge of Juniper Networks software and device architecture with this course.

NICE Knowledge and Skill Statements:

K0060, K0061, K0255

User Interfaces

Course | 1 hour 43 minutes

Go from command-line zero to hero! In this course, we'll be covering the user interfaces and configuration concepts.

NICE Knowledge and Skill Statements:

K0036, K0318, S0267

Configuration Basics

Course | 1 hour 53 minutes

Just pulled your router out of the box? Use what you learn in this course to get it into production right away.

NICE Knowledge and Skill Statements:

K0011, K0061, K0073, K0255, K0275, K0296, K0393, K0452, K0516, S0084, S0158, S0207

Operational Monitoring and Maintenance

Course | 1 hour 20 minutes

Learn how to perform NetOps functions on Juniper devices and get your feet wet in troubleshooting and maintenance.

NICE Knowledge and Skill Statements:

K0061, K0103, K0294, K0516, S0041, S0142, S0151, S0158

Routing Fundamentals

Course | 1 hour 51 minutes

Learn fundamentals of how routers talk to each other in order to ensure your traffic gets where it needs to go, and what's unique about how Juniper devices do it!

NICE Knowledge and Skill Statements:

K0001, K0011, K0061, K0221, K0255, K0296, K0395, K0471, K0516, K0565, S0041

Routing Policy and Firewall Filters

Course | 1 hour 20 minutes

Learn how to win traffic and influence routes! In this course, we'll be covering Juniper firewall filters and routing policies.

NICE Knowledge and Skill Statements:

K0004, K0005, K0049, K0061, K0255, K0395, K0487, K0516, K0561, K0565, S0076, S0084, S0170, S0207

NIST Cybersecurity Framework

SKILL PATH

Build a basic understanding of NIST cybersecurity fundamentals, including using the RMF process and identifying, assessing and responding to risk. Additionally, you will learn how to use the framework to assess an organization's cybersecurity risk and the steps to implement or improve a cybersecurity program.

Skill Assessment

Skill assessment | 20 questions

See how your NIST Cybersecurity Framework skills stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

NIST Cybersecurity Framework Project

Project | 2 hours 13 minutes

Apply your NIST Cybersecurity Framework knowledge with this practical exercise.

NICE Knowledge and Skill Statements:

S0367, S0372

NIST Cybersecurity Basics

Course | 43 minutes

This course helps you build a baseline of cybersecurity knowledge.

NICE Knowledge and Skill Statements:

K0004, K0267, K0295, K0412, K0436

Cybersecurity Framework Components

Course | 24 minutes

This course breaks down the Cybersecurity Framework components into understandable language.

NICE Knowledge and Skill Statements:

K0044

Risk Management

Course | 36 minutes

This course describes the Risk Management Framework (RMF), as well as guidelines for applying the RMF to information systems and organizations.

NICE Knowledge and Skill Statements:

K0002, K0044, K0048, K0165, K0214, K0264, K0527

Cybersecurity Framework Core Functions

Course | 1 hour 1 minute

This course describes the five Framework Core Functions and includes descriptions of categories, subcategories and informative references.

NICE Knowledge and Skill Statements:

K0044, K0267, K0412

Cybersecurity Framework Self-Assessments

Course | 12 minutes

This course describes the new section on Self-Assessing Cybersecurity Risk and explains how the Framework can be used by organizations to understand and assess their cybersecurity risk.

NICE Knowledge and Skill Statements:

K0044, K0165, S0147

The 7-Step Cybersecurity Framework Process

Course | 8 minutes

This course illustrates the steps an organization could use to create a new cybersecurity program or improve an existing program.

NICE Knowledge and Skill Statements:

K0044, K0264, S0147

NIST Cybersecurity Framework Summary & Tips

Course | 11 minutes

Review the NIST Cybersecurity Framework path with this summary and some tips.

NICE Knowledge and Skill Statements:

K0044

NIST DoD RMF

SKILL PATH

This learning path explains the Risk Management Framework (RMF) and its processes and provides guidance for applying the RMF to information systems and organizations.

Skill Assessment

Skill assessment | 10 questions

See how your DoD RMF skills stack up against other professionals in your field.

NIST DoD RMF Project

Project | 2 hours 17 minutes

Practice your DoD RMF knowledge with this project.

NICE Knowledge and Skill Statements:

S0115, S0147, S0228

Legal and Regulatory Organizations

Course | 32 minutes

This course introduces regulatory organizations which have an impact on the development and execution of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

NICE Knowledge and Skill Statements:

K0003, K0004, K0048, K0157, K0168

Laws, Policies and Regulations

Course | 13 minutes

In this course, we discuss some of the laws, policies and regulations which mandate the implementation of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

NICE Knowledge and Skill Statements:

K0003 , K0004, K0048, K0157, K0168, K0260, K0410

Integrated Organization Wide Risk Management

Course | 52 minutes

In this course, we describe the basic concepts associated with managing information system-related security and privacy risk in organizations.

NICE Knowledge and Skill Statements:

K0002, K0004, K0048, K0149, K0165, K0169, K0214, K0263, K0264, K0527, K0579

Risk Management Framework Phases

Course | 2 hours

In this course, we discuss the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) steps.

NICE Knowledge and Skill Statements:

K0002, K0048, K0149, K0165, K0169, K0214, K0263, K0264, K0379, K0455, K0527, K0579

Risk Management Framework Review

Course | 5 minutes

This is a recap of the RMF course.

NICE Knowledge and Skill Statements:

K0002, K0048

PMI Project Management Professional (PMP)

CERTIFICATION PATH

The Project Management Professional (PMP) certification path covers the best practices and principles of project management and prepares you to pass the Project Management Institute's PMP exam. You'll learn how initiate, plan, execute, monitor and close a project.

PMP Practice Exam

Practice Exam | 1,433 questions

Prepare for your PMP exam and test your domain knowledge.

PMP Introduction

Course | 14 minutes

Introductory course for the PMP education pathway.

NICE Knowledge and Skill Statements:

K0121

Project Management Overview

Course | 1 hour 40 minutes

Get ready to dive into project management with five videos on projects and project planning.

NICE Knowledge and Skill Statements:

K0072, K0121, K0249, K0579

Initiating

Course | 30 minutes

Start off right with three videos on the Initiating process group, covering the Develop Project Charter and Identify Stakeholders processes.

NICE Knowledge and Skill Statements:

K0072, K0084, K0121, K0249, K0579

Planning I

Course | 59 minutes

Six videos begin your dive into the Planning process group, focusing on processes such as Collect Requirements, Define Scope and Plan Scope Management.

NICE Knowledge and Skill Statements:

K0072, K0084, K0121, K0249, K0506, K0512, K0579

Planning II

Course | 1 hour 26 minutes

The second part of the Planning process group covers the Schedule Management knowledge area, including defining and sequencing activities and schedule development.

NICE Knowledge and Skill Statements:

K0072, K0084, K0121, K0249, K0506, K0512, K0579

Planning III

Course | 1 hour 16 minutes

This seven-video course continues our in-depth examination of the Planning process group, including cost estimation, determining budgets and planning communications management.

NICE Knowledge and Skill Statements:

K0072, K0084, K0121, K0249, K0506, K0512, K0579

Planning IV

Course | 1 hour 32 minutes

The final course covering the Planning process group takes you through planning risk management and stakeholder engagement, procurement management and more.

NICE Knowledge and Skill Statements:

K0002, K0072, K0084, K0121, K0233, K0249, K0270, K0376, K0379, K0506, K0512, K0579

Executing

Course | 1 hour 10 minutes

Refresh your knowledge of the Executing process with this course on directing and managing project work, acquiring resources, developing teams and more.

NICE Knowledge and Skill Statements:

K0072, K0084, K0121, K0249, K0506, K0579

Monitoring and Controlling

Course | 1 hour 38 minutes

Thirteen videos take you through the details of the Monitoring and Controlling process group, including controlling quality, costs, schedule and resources.

NICE Knowledge and Skill Statements:

K0072, K0084, K0121, K0249, K0506, K0512, K0579

Closing

Course | 8 minutes

Wrap up your project right with this brief course on the Closing process group.

NICE Knowledge and Skill Statements:

K0072, K0084, K0121, K0249, K0506, K0512, K0579

Preparing for PMP Exam

Course | 25 minutes

Prepare to become a certified project manager with three videos on ethics, exam preparation and the exam application process.

NICE Knowledge and Skill Statements:

NONE

PMP (2021 Update)

CERTIFICATION PATH

The Project Management Professional learning path explores the Project Management Institute's project management practices.

PMP Practice Exam (2021)

Practice Exam | 135 questions

Prepare for your PMP exam and test your domain knowledge.

Creating a high-performing team

Course | 2 hours 20 minutes

In this course, you will explore the importance of creating a high-performing team and the means to do it.

NICE Knowledge and Skill Statements:

K0072 , K0121, K0350, K0506, K0512, K0582, K0598, S0176, S0273

Starting the project

Course | 4 hours 14 minutes

In this course, students will explore the project start process, including choosing appropriate methodology and planning scope.

NICE Knowledge and Skill Statements:

K0350, K0518, K0566, K0575, K0598, S0027, S0066, S0176, S0273, S0296, S0306

Doing the work

Course | 1 hour 57 minutes

Time to get to work! In this course, you'll see the beginning of project work and the Process domain.

NICE Knowledge and Skill Statements:

K0002, K0350, K0566, K0575, K0598, S0066, S0176, S0213, S0250, S0273, S0296, S0306

Keeping the team on track

Course | 2 hours 5 minutes

In this course, you'll work to keep the team on track as they execute the project. Explore managing conflict, stakeholder collaboration and promoting team performance.

NICE Knowledge and Skill Statements:

K0506, K0518, K0566, K0575, K0598, S0185, S0273, S0326

Keeping the business in mind

Course | 1 hour 17 minutes

In this course, you'll explore how internal and external business environments can influence the work of a project.

NICE Knowledge and Skill Statements:

K0008, K0350, K0566, K0575, K0598, S0066, S0176, S0213, S0250, S0273, S0296, S0306, S0354, S0355

Security Architecture

SKILL PATH

The Security Architecture Learning Path enables security practitioners to develop security architectures that are resilient against cyberthreats while enabling and supporting the goals of the business.

Skill Assessment

Skill assessment | 20 questions

See how your Threat Modeling skills stack up against other professionals in your field.

Security Architecture – The Essentials

Course | 44 minutes

Get an introduction to the essential elements of security architecture and why it is such an important discipline.

NICE Knowledge and Skill Statements:

K0004, K0027, K0047, K0109, K0179, K0199, K0255, K0291, K0293

Enterprise Architecture Frameworks

Course | 53 minutes

Learn about aligning business systems with information systems to achieve business goals and enable the business.

NICE Knowledge and Skill Statements:

K0047, K0199

Security Architecture Development Process

Course | 37 minutes

In this course, we will introduce a seven-step, business- and risk-driven process to develop security architectures.

NICE Knowledge and Skill Statements:

K0005, K0044, K0165, K0211, K0287, S0367

Threat Modeling

Course | 55 minutes

In this course, we examine four popular threat modeling methodologies: Microsoft STRIDE, the Process for Attack Simulation and Threat Analysis, the Operationally Critical Threat Assessment and Vulnerability Evaluation, and Trike.

NICE Knowledge and Skill Statements:

K0177, K0469, K0475, K0612, S0229

Designing for security

Course | 38 minutes

In this course, we will introduce students to security design patterns and reference security architectures as reusable solutions to solve reoccurring information security problems.

NICE Knowledge and Skill Statements:

K0075, K0170, K0291, K0297, S0022, S0036, S0122, S0141

Case Study

Course | 55 minutes

Learn to develop a security architecture that enables a remote workforce while maintaining or increasing the security posture of the organization.

NICE Knowledge and Skill Statements:

K0199, K0291, K0474, S0023, S0122

Summary and Conclusion

Course | 14 minutes

In this course, we will summarize everything we've covered in the learning path and provide final words of wisdom for anyone interested in starting or continuing a career as a security architect.

NICE Knowledge and Skill Statements:

K0047

Security Engineering

SKILL PATH

The Security Engineering skill path teaches you concepts related to security architecture and engineering, including technical integration of enterprise security, security design and implementation, secure maintenance and disposal, and more.

Secure Design Principles

Course | 39 minutes

Explore the principles behind secure system design, ranging from security models to certification and accreditation.

NICE Knowledge and Skill Statements:

K0037, K0044, K0047, K0075, K0170, K0180, K0198, K0203, K0211, K0240, K0288, K0291, K0320, K0362, K0624

Secure Network Design

Course | 26 minutes

Explore key concepts behind secure network design, including tools to keep threats out and techniques to detect and deflect intruders that breach your defenses.

NICE Knowledge and Skill Statements:

K0001, K0004, K0034, K0049, K0179, K0276, K0291, K0324, K0326, K0452, K0487, K0488, K0493, K0561, S0023, S0034

Distributed System & Virtualized Networks

Course | 20 minutes

Explore the use of distributed and virtualized systems as well as the security benefits and potential drawbacks involved in their use.

NICE Knowledge and Skill Statements:

K0001, K0063, K0071, K0113, K0130, K0179, K0205, K0437, K0610

WAN & Remote Access Security

Course | 33 minutes

Learn about securing wide area networks (WAN) and remote access against different types of cyber threats in this five-video course.

NICE Knowledge and Skill Statements:

K0001, K0005, K0070, K0071, K0104, K0113, K0138, K0190, K0269, K0274, K0362, K0395, K0417, K0427, K0438

System Protection Mechanisms

Course | 32 minutes

Learn about different system protection mechanisms and common issues such as Web-based vulnerabilities, architecture flaws and more.

NICE Knowledge and Skill Statements:

K0004, K0070, K0077, K0090, K0109, K0199, K0209, K0271, K0322, K0392, K0493, K0624

Physical Security

Course | 52 minutes

Don’t forget about physical security! Explore how to keep your business secure starting with secure design and construction to physical intrusion detection and more.

NICE Knowledge and Skill Statements:

K0065, K0075, K0165, K0244, S0023

Data Center Security

Course | 21 minutes

Don't let an incident at your data center disrupt your organization. Explore ways to keep data centers secure from a variety of threats.

NICE Knowledge and Skill Statements:

K0032, K0622

Secure Software Development

Course | 43 minutes

Explore the ins and outs of secure software development as you progress through this nine-video course.

NICE Knowledge and Skill Statements:

K0039, K0070, K0153, K0276, K0373, K0396, K0480

Disaster Recovery

Course | 36 minutes

Don't let a lack of preparedness compound the effects of a disaster. Learn how to create and test a disaster recovery plan in this six-video course.

NICE Knowledge and Skill Statements:

K0006, K0021, K0026, K0032, K0150, K0210, K0292, K0399, K0519, K0527

Business Continuity Planning

Course | 19 minutes

Learn how to keep your business up and running. Explore the importance of continuity planning, incident response planning and impact analysis.

NICE Knowledge and Skill Statements:

K0006, K0026, K0032, K0041, K0042, K0150, K0165, K0292

Network Security Components

Course | 44 minutes

In this course, we help you explore the details of network security components: device types, component management and analyzing components and network configurations.

NICE Knowledge and Skill Statements:

K0007, K0011, K0033, K0071, K0145, K0170, K0179, K0296, K0324, K0373, K0487, K0488, K0491, K0561

Securing Host Devices

Course | 20 minutes

Explore the challenges of securing host devices with this course on selecting host hardware and software, host hardening and protecting bootloaders.

NICE Knowledge and Skill Statements:

K0033, K0109, K0167, K0205, K0440

Secure Storage Controls

Course | 29 minutes

Refresh your knowledge of secure storage controls with this course on storage types, protocols and management.

NICE Knowledge and Skill Statements:

K0021, K0038, K0097, K0622

Software Vulnerabilities and Security Controls

Course | 37 minutes

In this course, we take you through the fundamentals of software vulnerabilities and security controls.

NICE Knowledge and Skill Statements:

K0005, K0049, K0070, K0140, K0624

Security Engineering Principles

Course | 22 minutes

Review the security principles that security engineers need to know in order to implement systems.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0044, K0087, K0157, K0158, K0267, K0287, K0568, K0584

Risk Management

Course | 7 minutes

Get a basic understanding or risk management in an organization.

NICE Knowledge and Skill Statements:

K0002, K0004, K0214, K0455, K0527

System Resilience Principles

Course | 10 minutes

Dive into defense-in-depth and other principles and methods of making your systems resilient.

NICE Knowledge and Skill Statements:

K0002, K0004, K0032, K0112, K0179, K0299, K0323, K0527, S0027, S0076

Vulnerability Management Principles

Course | 13 minutes

Know why it's important to manage vulnerabilities, and what the engineer's role is.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0013, K0040, K0070, K0106, K0147, K0157, K0187, K0339, K0373, K0392, K0624, S0036, S0078

Risk Management Process

Course | 37 minutes

Walk through the security risk management process and learn best practices.

NICE Knowledge and Skill Statements:

K0002, K0004, K0047, K0048, K0165, K0214, K0264, K0455, K0527

Operational Risk Management

Course | 30 minutes

Understand how today's complex business environment impacts operational risk and related controls.

NICE Knowledge and Skill Statements:

K0004, K0047, K0048, K0084, K0154, K0169, K0214, K0264, K0379, K0455, K0527

Stakeholder Requirements Definition

Course | 14 minutes

Review how different stakeholders impact security planning, design and implementation.

NICE Knowledge and Skill Statements:

K0004, K0169, K0376, K0379

Requirements Analysis

Course | 7 minutes

Discover the process for analyzing requirements before designing security systems.

NICE Knowledge and Skill Statements:

K0004, K0028, K0035, K0073, K0086, K0090, K0091, K0102, K0164, K0291, K0475, K0480

System Security Architecture and Design

Course | 12 minutes

Review the core components and processes of security architecture and design.

NICE Knowledge and Skill Statements:

K0004, K0044, K0047, K0075, K0087, K0170, K0180, K0198, K0199, K0203, K0211, K0240, K0267, K0288, K0291, S0023

Implementation, Integration and Deployment of System Modifications

Course | 5 minutes

Learn the basics of system implementation, integration and deployment.

NICE Knowledge and Skill Statements:

K0004, K0073, K0082, K0091, K0178, K0179, K0186, K0257, K0270, K0393, K0452, K0488, S0153

Verification and Validation of Systems or System Modifications

Course | 10 minutes

Go through the post-deployments steps of ensuring the system is adequately secure.

NICE Knowledge and Skill Statements:

K0004, K0028, K0091, S0110, S0282

Secure Operations

Course | 30 minutes

Understand the basics of maintaining a secure operations strategy.

NICE Knowledge and Skill Statements:

K0004, K0006, K0026, K0041, K0042, K0074, K0086, K0150, K0167, K0292, K0324, K0333, K0403, K0488

Secure Maintenance

Course | 13 minutes

Learn about the three main areas of secure maintenance and related strategies.

NICE Knowledge and Skill Statements:

K0004, K0035, K0074 , K0103, K0167, K0294, K0419, S0027

Secure Disposal

Course | 8 minutes

Know how to handle a system at the end of its lifecycle and the key security considerations.

NICE Knowledge and Skill Statements:

K0004, K0090, K0270

Acquisition Process

Course | 15 minutes

Know what's involved in the systems acquisition phase and how to prepare for it.

NICE Knowledge and Skill Statements:

K0004, K0154, K0164, K0169, K0198, K0257, K0264, K0270, K0376, K0379

System Development Methodologies

Course | 3 minutes

Understand the advantages and disadvantages of different development methods.

NICE Knowledge and Skill Statements:

K0004, K0035, K0039, K0047, K0079, K0081, K0082, K0086, K0087, K0153, K0186, K0276

Technical Management Processes

Course | 32 minutes

Dive deep into the technical aspects of managing systems engineering.

NICE Knowledge and Skill Statements:

K0002, K0004, K0005, K0006, K0150, K0233, K0264, K0527, S0358

SIEM Architecture and Process

SKILL PATH

This learning path introduces you to what SIEM is and how it operates. Next we dive in to learn about the challenges faced with modern distributed enterprise architectures and the reason why time to detection is outrageously long and completely unmanageable without a technology like SIEM.

Skill Assessment

Skill assessment | 20 questions

See how your SIEM skills stack up against other professionals in your field.

SIEM Architecture and Process Project

Project | 1 hour 13 minutes

Test your understanding of SIEM architecture and process in this project consisting of 5 challenges.

NICE Knowledge and Skill Statements:

S0173

What is SIEM

Course | 1 hour 6 minutes

In this course we will introduce what SIEM is, the problems it is designed to help address, and various vendors in the SIEM space. We will also begin setting up our SIEM environment.

NICE Knowledge and Skill Statements:

K0145, S0038, S0173

Architecture

Course | 1 hour 26 minutes

In this course we will discuss the high level components that SIEM utilizes to help store, process and provide structure around our data. We will also overview the SIEM UI we previously installed.

NICE Knowledge and Skill Statements:

K0109, K0145, K0199, K0255, S0173

Data Collection

Course | 55 minutes

In this course we will discuss various methodologies to ingest data into the SIEM. We will also be configuring our systems to ship our first logs into the SIEM.

NICE Knowledge and Skill Statements:

K0131, K0132, K0145, K0448, S0173

Data Processing

Course | 53 minutes

In this course, we discuss various data formats and data structures. We review various methods to organize our data and make the data meaningful. We also use sample log data to view how the system structures various data formats.

NICE Knowledge and Skill Statements:

K0017, K0038, K0145, S0106, S0173, S0252, S0334

Data Enrichment

Course | 38 minutes

In this course we discuss the purpose behind data enrichment and how we map data from various sources to provide contextual information in the SIEM. We also review a real-world example using event data to enrich a malware event.

NICE Knowledge and Skill Statements:

K0145, S0038, S0123, S0173, S0217

Data Indexing

Course | 17 minutes

In this course we briefly touch on various capabilities to store and manage data. This course is designed to give you ideas behind scalability and resiliency and what these capabilities mean when it comes to managing your data.

NICE Knowledge and Skill Statements:

K0145, S0173

Using Data

Course | 1 hour 43 minutes

In this course we introduce Use Cases which are a framework designed to take a detection based capability from concept to reality. We then proceed to follow the process for an example Use Case Detection.

NICE Knowledge and Skill Statements:

K0054, K0145, K0299, K0481, S0027, S0173

SIEM Wrap-Up

Course | 8 minutes

In this course we discuss the key concepts and key takeaways from each of the courses to help solidify your foundational understanding of SIEM.

NICE Knowledge and Skill Statements:

K0145, S0173

Training and Awareness Basics

SKILL PATH

Go “beyond compliance” to learn about sales and marketing techniques that can take a training and awareness program to the next level: engagement and behavior change. You’ll also learn security basics for soft-skilled professionals new to the security field, as well as how to leverage brain chemistry to be more effective.

Training and Awareness Basics Overview

Course | 5 minutes

Begin at the beginning with this course introducing you to security training and awareness.

NICE Knowledge and Skill Statements:

K0146

Security Basics

Course | 28 minutes

Take a look at some fundamental security basics for soft-skill-focused learners.

NICE Knowledge and Skill Statements:

K0003, K0004, K0005, K0007, K0104, K0145, K0162, K0412, K0480, K0487

Introduction to Training and Awareness

Course | 14 minutes

Take a look at what’s going on in the world of training and awareness, including potential obstacles and concerns.

NICE Knowledge and Skill Statements:

K0252, K0313

Sales and Marketing Techniques for Training and Awareness

Course | 38 minutes

Delve into the role of sales and marketing in security awareness and training.

NICE Knowledge and Skill Statements:

K0243, K0245

Creative

Course | 18 minutes

Explore possible concerns on the creative side of security programs.

NICE Knowledge and Skill Statements:

K0252

Program Execution

Course | 1 hour 10 minutes

Move from theory to practice with this course on executing a security program.

NICE Knowledge and Skill Statements:

K0243, K0245, K0252

Vulnerability Assessment

SKILL PATH

The vulnerability assessment learning path guides you through a holistic security assessment approach, where you will develop a well-structured framework for analyzing the security of a system. You will acquire the skills to perform custom vulnerability assessment for any computer system, application or network infrastructure.

Skill Assessment

Skill assessment | 20 questions

See how your vulnerability assessment skills stack up against other professionals in your field.

Vulnerability Assessment Project

Project | 1 hours 14 minutes

Test your vulnerability assessment skills as your progress through seven challenges leveraging free-to-use security tools and services.

NICE Knowledge and Skill Statements:

S0001, S0137, S0174

Vulnerability Management in a Nutshell

Course | 30 minutes

This course covers the basics of vulnerability assessment, including definitions, scope, policy and process.

NICE Knowledge and Skill Statements:

K0006, K0314

Vulnerability Discovery

Course | 1 hour 47 minutes

This course guides you through five different type of security tools for discovering vulnerabilities in various environments.

NICE Knowledge and Skill Statements:

K0013, K0272, K0290, K0339

Vulnerability Classification

Course | 39 minutes

This course covers three main topics: false positives, standardized vulnerabilities, and weakness classification systems and threat-based vulnerability/weakness classification.

NICE Knowledge and Skill Statements:

K0005, K0040, K0402, K0612

Prioritization and Risk Assessment

Course | 1 hour 11 minutes

This course covers how to classify and prioritize vulnerabilities based on real-world criticality measures and how to define the true risk of the vulnerabilities for a specific environment.

NICE Knowledge and Skill Statements:

K0002, K0013, K0054, K0149, K0165, K0344, K0402, K0469, K0475, S0219

Vulnerability Assessment Documentation and Maintenance

Course | 43 minutes

This course covers how to create comprehensive, clear and easy-to-understand vulnerability assessment documentation, and how to go about keeping the vulnerability findings and scoring current.

NICE Knowledge and Skill Statements:

K0013, K0054, K0165

Remediation and Mitigation

Course | 55 minutes

In this course, we will cover a wide range of topics about the vulnerability remediation and mitigation process, including the most common remediations and mitigations and strategies for deployment of security measures.

NICE Knowledge and Skill Statements:

K0002, K0205, K0275, K0440, K0527, K0531

Key Security Controls

Course | 1 hour 19 minutes

This course covers the top most effective security controls to reduce the overall risk of systems and networks. Recommendation of such controls is a perfect add-on for any vulnerability assessment.

NICE Knowledge and Skill Statements:

K0033, K0049, K0065, K0145, K0324, K0440, K0523, K0561

Secure coding and DevSecOps

Secure coding and DevSecOps training helps programmers, developers and security professionals recognize and mitigate vulnerabilities. It covers a variety of common mistakes, how those mistakes can be exploited by cybercriminals, and what can be done to correct them throughout the development life cycle.

CertNexus Certified IoT Security Practitioner

CERTIFICATION PATH

Securing Internet of Things (IoT) systems can be a complicated process. Explore the challenges and complexities of IoT.

CertNexus Certified IoT Security Practitioner Practice Exam

Practice Exam | 29 questions

Prepare for your Internet of Things Security Practitioner exam.

Managing IoT Risks

Course | 32 minutes

In this course, you will identify threats to cybersecurity and privacy throughout an IoT system and apply the principles of Security by Design to plan and design a secure IoT system.

NICE Knowledge and Skill Statements:

K0002, K0004, K0322, K0379, K0455, K0471, K0527, S0357

Securing cloud and web interfaces

Course | 1 hour 17 minutes

In this course, you will explore multiple threats and vulnerabilities that affect IoT systems in the web and the cloud.

NICE Knowledge and Skill Statements:

K0004, K0005, K0135, K0160, K0194, K0283, K0349, K0444, K0603, S0073, S0357

Securing data

Course | 1 hour 31 minutes

In this course, you will learn the details of protecting and securing data from unauthorized access.

NICE Knowledge and Skill Statements:

K0004, K0018, K0019, K0104, K0190, K0285, K0308, K0427, K0561, S0089, S0138, S0298

Controlling access to IoT resources

Course | 1 hour 1 minute

In this course, you will explore identifying relevant strategies and implementing security features to control access to IoT resources.

NICE Knowledge and Skill Statements:

K0004, K0007, K0044, K0056, K0065, K0180, K0487, K0561, S0031, S0136, S0171, S0367

Securing IoT networks

Course | 1 hour 19 minutes

In this course, you will explore the complexities of protecting IoT networks.

NICE Knowledge and Skill Statements:

K0004, K0160, K0180, K0322, K0471, K0487, K0561, S0136

Ensuring privacy

Course | 50 minutes

In this course, you will learn more about taking precautions and disposing of sensitive data in IoT systems.

NICE Knowledge and Skill Statements:

K0003, K0004, K0038, K0044, S0367

Managing software and firmware risks

Course | 59 minutes

In this course, you will explore the details of managing software and firmware risks in IoT.

NICE Knowledge and Skill Statements:

K0004, K0079, K0081, K0082, K0152, K0153, K0178, K0186, K0246, K0559, S0034, S0076, S0172

Promoting physical security

Course | 17 minutes

Explore the details of protecting local memory and storage, and protecting devices from shell access over a physical port connection.

NICE Knowledge and Skill Statements:

K0065, K0075, K0165, K0244, S0023

CertNexus CyberSec First Responder

CERTIFICATION PATH

This learning path is designed to assist students in preparing for the CertNexus CyberSec First Responder (Exam CFR-310) certification examination. It provides a comprehensive methodology for individuals responsible for defending the cybersecurity of their organization.

CertNexus CyberSec First Responder Practice Exam

Practice Exam | 41 questions

Prepare for your CertNexus CyberSec First Responder exam.

CyberSec First Responder Introduction

Course | 4 minutes

This course provides a brief overview of CertNexus CyberSec First Responder certification objectives.

Assessing Information Security Risk

Course | 1 hour, 44 minutes

This course teaches how to Identify the strategic value of risk management in the context of information assurance, assess risks that affect the organization, translate risk assessment into specific strategies for mitigation, and integrate documentation into risk management.

NICE Knowledge and Skill Statements:

Analyzing the Threat Landscape

Course | 34 minutes

This course teaches how to compare, contrast, and categorize cybersecurity threats and threat profiles and perform ongoing threat landscape research to prepare for incidents.

NICE Knowledge and Skill Statements:

K0004, K0165, K0177, K0233, K0362, K0455, K0469, K0474, K0475, K0480, K0543, K0603, K0607, K0612, S0228, S0229, S0256, S0258, S0340

Analyzing Reconnaissance Threats to Computing and Network Environments

Course | 34 minutes

This course teaches how to implement threat modeling tools and tactics and assess the impacts of reconnaissance and social engineering.

NICE Knowledge and Skill Statements:

K0004, K0058, K0165, K0177, K0334, K0362, K0474, K0475, K0480, K0603, K0612, S0046, S0056, S0156, S0228, S0229, S0256, S0258, S0340

Analyzing Attacks on Computing and Network Environments

Course | 1 hour, 7 minutes

This course teaches how to assess the impact of various attacks, including system hacking attacks, threats to web apps and services, malware, hijacking and impersonation attacks, denial of service incidents, and threats to mobile and cloud infrastructures.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0058, K0070, K0119, K0165, K0177, K0334, K0362, K0474, K0475, K0480, K0603, K0612, K0624, S0056, S0228, S0229, S0256, S0258, S0340

Analyzing Post-Attack Techniques

Course | 46 minutes

This lesson teaches how to assess various post-attack techniques, including command and control, persistence, lateral movement and pivoting, data exfiltration, and anti-forensics techniques.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0119, K0177, K0184, K0362, K0447, K0449, K0469, K0474, K0475, K0480, K0536, S0228, S0229, S0293

Managing Vulnerabilities in the Organization

Course | 29 minutes

This course teaches how to implement a vulnerability management plan, assess common vulnerabilities in the organization, and conduct vulnerability scans.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0013, K0040, K0070, K0106, K0147, K0165, K0177, K0339, K0362, K0474, K0475, K0480, K0624, S0001, S0051, S0081, S0137, S0141, S0167, S0228, S0229, S0242

Implementing Penetration Testing to Evaluate Security

Course | 24 minutes

This course teaches how to conduct authorized penetration tests to evaluate the organization's security posture and analyze and report the results of a penetration test and make mitigation recommendations.

NICE Knowledge and Skill Statements:

K0004, K0005, K0009, K0013, K0040, K0070, K0147, K0165, K0177, K0310, K0314, K0339, K0342, K0362, K0480, K0624, S0001, S0051, S0081, S0137, S0141, S0167, S0228, S 0242

Collecting Cybersecurity Intelligence

Course | 43 minutes

This course teaches how to design and implement a system of cybersecurity intelligence collection and analysis and collect data from network-based and host-based intelligence sources.

NICE Knowledge and Skill Statements:

K0004, K0040, K0131, K0165, K0177, K0339, K0352, K0358, K0388, K0409, K0457, K0460, K0462, K0464, K0480, K0503, K0525, K0544, K0577, S0167, S0210, S0212, S0228, S0247, S0256, S0303, S0316, S0318, S0335, S0339, S0340, S0343, S0372

Analyzing Log Data

Course | 30 minutes

This course teaches how to analyze a wide array of log data by using common Windows- and Linux-based security tools and incorporate a SIEM system into the analysis process.

NICE Knowledge and Skill Statements:

K0004, K0058, K0119, K0229, K0334, K0363, K0480, S0005, S0056, S0120

Performing Active Asset and Network Analysis

Course | 53 minutes

This course teaches how to analyze incidents with Windows- and Linux-based tools, use methods and tools for malware analysis, and analyze common indicators of potential compromise.

NICE Knowledge and Skill Statements:

K0004, K0058, K0324, K0334, K0339, K0449, K0480, S0056, S0081, S0181, S0187, S0194, S0197, S0218, S0277, S0288, S0359

Responding to Cybersecurity Incidents

Course | 47 minutes

Learn to design and implement a system to respond to urgent situations by mitigating immediate and potential threats, contain and mitigate incidents, and prepare to move from the incident response phase to the post-mortem forensic investigation phase.

NICE Knowledge and Skill Statements:

K0001, K0003, K0004, K0006, K0041, K0042, K0150, K0161, K0162, K0179, K0231, K0259, K0287, K0292, K0317, K0343, K0381, K0399, K0480, K0519, K0543, K0586, S0003, S0054, S0077, S0078, S0080, S0173, S0175, S0365

Investigating Cybersecurity Incidents

Course | 25 minutes

This course teaches how to create a plan for performing forensic investigations after incidents occur, collect and analyze electronic evidence in a secure manner to prevent tampering or compromise, and implement measures to follow up on an investigation.

NICE Knowledge and Skill Statements:

K0001, K0003, K0004, K0006, K0041, K0042, K0150, K0161, K0162, K0179, K0231, K0259, K0287, K0292, K0317, K0343, K0381, K0399, K0480, K0519, K0543, K0586, S0003, S0054, S0077, S0078, S0080, S0173, S0175, S0365S0003, S0054, S0077, S0078, S0080, S0173, S0175, S0365

CertNexus Cyber Secure Coder

CERTIFICATION PATH

Cyber Secure Coder is the ideal learning path for application developers, testers and architects who have previously not had to consider including security in their project. Even students who are new to programming can benefit by instilling security into their thought process before creating their first application.

CertNexus Cyber Secure Coder Practice Exam

Practice Exam | 22 questions

Prepare for your Cyber Secure Coder exam and test your domain knowledge.

Identifying the Need for Security in Your Software Projects

Course | 1 hour 59 minutes

The first step in tackling the problem of software security is to understand the challenges you're up against.

NICE Knowledge and Skill Statements:

K0001, K0003, K0005, K0006, K0028, K0044, K0068, K0080, K0082, K0084, K0105, K0139, K0178, K0261, K0624

Handling Vulnerabilities

Course | 2 hours 3 minutes

Before you focus on specific vulnerabilities and tactics for dealing with them, there are some general strategies that you can employ to prevent vulnerabilities from creeping into your software.

NICE Knowledge and Skill Statements:

K0004, K0044, K0079, K0081, K0084, K0178, S0367

Designing for Security

Course | 1 hour 4 minutes

The process you use to design your software should reflect what is important to you, your customers and other project stakeholders.

NICE Knowledge and Skill Statements:

K0005, K0006, K0178, K0624

Developing Secure Code

Course | 2 hours 30 minutes

In this course, you will follow best practices for secure coding, prevent defects that lead to security vulnerabilities common to various platforms, and prevent defects that lead to privacy vulnerabilities.

NICE Knowledge and Skill Statements:

K0039, K0044, K0070, K0105, K0140, K0178, K0260, K0624, S0367

Implementing Common Protections

Course | 3 hours 10 minutes

In this course, you will limit access using login and user roles, protect data in transit and at rest, implement error handling and logging, protect sensitive data and functions, and protect database access.

NICE Knowledge and Skill Statements:

K0039, K0044, K0079, K0178, K0260, K0262, S0014, S0022, S0031, S0034, S0138, S0149

Testing Software Security

Course | 32 minutes

In this course, you will follow an appropriate approach to security testing based on business and technical criteria, use code analysis to find security problems and use automated testing tools to find security problems.

NICE Knowledge and Skill Statements:

K0153, K0178, S0135, S0174

Maintaining Security in Deployed Software

Course | 38 minutes

In this course, you will monitor and log applications to support security, maintain security after deployment, and analyze code for suspicious or unauthorized changes.

NICE Knowledge and Skill Statements:

S0090

Container Security

SKILL PATH

Gain the advantages of running applications in Docker while maintaining a solid security posture with this Container Security Learning Path.

Skill Assessment

Skill assessment | 20 questions

See how your container security skills stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

Container Security Project

Project | 1 hour 11 minutes

Test your understanding of container security with this project. You will review images to reduce risk, make docker images follow best practices, and scan images for vulnerable software.

NICE Knowledge and Skill Statements:

K0004, K0130, K0189, K0205, K0609, K0610, S0073, S0121

Introduction and Overview of Containers

Course | 55 minutes

Gain an understanding of the role containers and Docker have in modernizing IT with this overview of container fundamentals.

NICE Knowledge and Skill Statements:

K0130, K0609, K0610, S0073

Docker Security

Course | 4 hours 46 minutes

Containers are gaining popularity and prominence in IT. This course provides methods to use Docker securely.

NICE Knowledge and Skill Statements:

K0130, K0167, K0189, K0205, K0406, K0609, K0610, S0073, S0121

Kubernetes Security

Course | 5 hours 57 minutes

Kubernetes won the container orchestration race. Learn how it works and how to deploy containers and keep your cluster secure.

NICE Knowledge and Skill Statements:

K0130, K0167, K0189, K0205, K0406, K0609, K0610, S0073, S0121

Developing in Splunk

SKILL PATH

In this path, you will learn to create effective visualizations for different stakeholders with the Splunk Web Framework, utilize tokens and event handlers, explore SDKs, interact with REST APIs and build a test lab for log analysis and incident response.

Developing in Splunk skill assessment

Skill assessment | 20 questions

See how your Splunk skills stack up against other professionals in your field.

Getting Started With Splunk

Course | 27 minutes

Understand the way of setting up Splunk on cloud and locally with this course, and choose the right platform for you.

NICE Knowledge and Skill Statements:

K0004, K0089, K0147, K0161, K0162, K0167, K0224, K0344, K0452, K0488, K0536, S0121, S0149

Introduction to Splunk

Course | 1 hour 52 minutes

Learn the features, components, types and more about Splunk through this course.

NICE Knowledge and Skill Statements:

K0004, K0089, K0147, K0161, K0162, K0167, K0224, K0344, K0452, K0488, K0536, S0121, S0149

Building Splunk Apps

Course | 50 minutes

What are Splunk apps and how do we create them? This will be the main topic of this course. We'll also learn to integrate data inputs and how to maintain Splunk apps.

NICE Knowledge and Skill Statements:

K0004, K0089, K0147, K0161, K0162, K0167, K0224, K0452, K0488, K0536, S0121, S0149

Developing with Splunk's REST API

Course | 4 hours 9 minutes

What is Splunk's REST API? What about SDK and KV-Store? We will explore all of these topics in this course. We'll also look at the HTTP Event Collector(HEC).

NICE Knowledge and Skill Statements:

K0004, K0089, K0147, K0161, K0162, K0167, K0224, K0452, K0488, K0536, S0121, S0149

DevSecOps

SKILL PATH

You will learn techniques used by leading organization to increase innovation and speed up delivery while remaining secure.

DevSecOps Skill Assessment

Skill assessment | 20 questions

See how your DevSecOps security skills stack up against other professionals in your field.

DevSecOps project

Project | 2 hours 27 minutes

Put what you've learned about DevSecOps to the test with this project.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0068, K0070, K0140, K0531, K0559, S0031, S0034, S0172, S0174

DevSecOps overview

Course | 50 minutes

An introduction to DevSecOps topics, including security models, definitions and the software development life cycle (SDLC).

NICE Knowledge and Skill Statements:

K0005, K0007, K0014, K0016, K0044, K0068, K0091, K0152, K0211, K0229, K0372, S0006, S0007, S0034, S0060, S0076, S0149, S0257, S0266, S0367

Source control management

Course | 38 minutes

This course explores source control management, GitHub, repositories and more.

NICE Knowledge and Skill Statements:

K0084, K0140, K0152, K0186, K0559, S0031, S0034, S0077, S0172

Secure CI/CD pipeline

Course | 42 minutes

This course starts with an introduction to threat modeling, using Microsoft Threat Modeling Tool to identify potential threats at the design phase of the software development life cycle.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0068, K0140, K0186, K0362, K0430, K0480, K0481, K0531, K0538, K0559, K0603, K0612, S0031, S0034, S0172, S0341

SCA in CI/CD pipeline

Course | 47 minutes

A look at software composition analysis in the CI/CD pipeline.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0068, K0140, K0186, K0531, K0559, K0624, S0031, S0034, S0172, S0341

SAST in CI/CD pipeline

Course | 53 minutes

In this course, you'll explore static application security testing (SAST) in the CI/CD pipeline.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0068, K0070, K0140, K0186, K0531, K0559, K0624, S0031, S0034, S0060, S0172, S0174, S0341

DAST in CI/CD pipeline

Course | 49 minutes

Explore the details of dynamic application security testing (DAST) in the CI/CD pipeline

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0068, K0070, K0140, K0531, K0559, K0624, S0031, S0034, S0060, S0172, S0174, S0341

Container security

Course | 50 minutes

A look at container security with an introduction to Docker and Kubernetes.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0068, K0070, K0130, K0140, K0186, K0531, K0559, K0610, K0624, S0029, S0031, S0034, S0060, S0073, S0172, S0341

JavaScript Security

SKILL PATH

In this learning path, we will go through diverse JavaScript-related attacks and learn how to build safer JavaScript applications. Most of this learning path will cover front-end JavaScript; however, we will also consider Node.js in certain parts of the learning paths.

Skill Assessment

Skill assessment | 20 questions

See how your JavaScript security skills stack up against other professionals in your field.

JavaScript Security Project

Project | 2 hours 19 minutes

In the first four challenges, you will find vulnerabilities and exploit them. In the next five challenges, you will fix the vulnerabilities.

NICE Knowledge and Skill Statements:

K0004, K0016, K0068, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213

Cyber Range

Cyber range | 30 minutes

This lab covers multiple secure coding errors commonly found in JavaScript, including DOM rewrites and the use of the eval() statement.

Secure JavaScript Programming overview

Course | 53 minutes

In this course, we will cover some base concepts of JavaScript and its runtime environments.

NICE Knowledge and Skill Statements:

K0004, K0016, K0068, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213

Authentication

Course | 49 minutes

We will cover the case of cookies and non-cookies-based front-end authentication. We will also cover best practices in term of front-end identity management.

NICE Knowledge and Skill Statements:

K0004, K0007, K0016, K0068, K0140, K0236, K0325, K0336, K0372, K0396, K0398, K0487, K0561, S0060, S0172, S0213

XSS and JavaScript remote code executions

Course | 1 hour 33 minutes

This course explores cross-site scripting (XSS) in JavaScript.

NICE Knowledge and Skill Statements:

K0004, K0016, K0061, K0068, K0070, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213

CSRF and browser security

Course | 37 minutes

An exploration of cross-site request forgery, or CSRF.

NICE Knowledge and Skill Statements:

K0004, K0016, K0061, K0068, K0070, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213

Regular expressions

Course | 34 minutes

Regular expressions are one of the most powerful, yet dangerous parts of JavaScript. In this course, we will dig into them to understand what risks they can bring and how to mitigate them.

NICE Knowledge and Skill Statements:

K0004, K0016, K0023, K0068, K0070, K0140, K0236, K0325, K0372, K0396, K0398, S0013, S0037, S0060, S0172, S0213, S0285

Prototype pollution

Course | 34 minutes

In this course, we will go through real-life examples of such attacks and learn how to protect against them.

NICE Knowledge and Skill Statements:

K0004, K0005, K0016, K0068, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213

Ecosystem modules (npm) and supply chain

Course | 1 hour 13 minutes

In this course, we will see everything we need to know to find and assess packages. We will even see what to do if one of the packages we use is flagged as vulnerable.

NICE Knowledge and Skill Statements:

K0004, K0016, K0068, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0172, S0213, S0060, S0172, S0213

Serverless JavaScript

Course | 1 hour 5 minutes

In this course, we will review the security best practices of a safe serverless project.

NICE Knowledge and Skill Statements:

K0004, K0016, K0068, K0077, K0140, K0236, K0325, K0372, K0396, K0398, S0060, S0143, S0153, S0172, S0213

Web developer desktop security

Course | 10 minutes

Building web applications can open some parts of your own workstation to attacks. In this short course, we will go through a few “gotchas” anyone building web applications should know about.

NICE Knowledge and Skill Statements:

K0004, K0016, K0068, K0105, K0140, K0236, K0325, K0349, K0372, K0396, K0398, K0444, K0624, S0060, S0172, S0213

Secure Coding Fundamentals

SKILL PATH

This path helps you understand software vulnerabilities and how to recognize them in code, demonstrates how they are exploited by attackers (including real-world case studies of vulnerable applications in production), and describes ways by which the vulnerabilities can be mitigated.

Skill Assessment

Skill assessment | 20 questions

See how your secure coding skills stack up against other professionals in your field.

Python Code Security Cyber Range

Cyber range | 10 labs

Gain practical experience and develop your secure Python coding skills through 10 hands-on labs in the Python Code Security Cyber Range.

NICE Knowledge and Skill Statements:

S0051, S0060, S0172, S0174, S0266

Secure Coding Fundamentals Project

Project | 2 hours 8 minutes

Practice your secure coding skills by solving challenges.

NICE Knowledge and Skill Statements:

S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266

Introduction to Secure Coding Fundamentals

Course | 6 minutes

This course introduces the need for secure coding and the tools used in this learning path.

NICE Knowledge and Skill Statements:

K0009, K0140

Buffer Overflows

Course | 50 minutes

This course introduces the buffer overflow vulnerability, its exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140

Integer Overflows and Underflows

Course | 53 minutes

This course introduces integer overflow and underflow vulnerabilities, their exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140

Race Conditions

Course | 48 minutes

This course introduces race conditions, their exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0063, K0070, K0140

Format String Vulnerabilities

Course | 32 minutes

This course introduces format string vulnerabilities, their exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140

Command Injection

Course | 39 minutes

This course introduces command injection vulnerabilities, their exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140, K0372

Least Privilege

Course | 33 minutes

This course introduces the principle of least privilege and its importance in secure coding.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140, K0167

Credential Management

Course | 1 hour

This course describes how poor credential management can make an application vulnerable to attack, how it can be exploited and how to manage credentials properly.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140, K0336, K0362

Cryptography

Course | 40 minutes

This course discusses how the poor use of cryptography can leave an application vulnerable to attack and how it can be exploited, as well as potential mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0190, K0362

SQL Injection

Course | 43 minutes

This course introduces SQL injection vulnerabilities, their exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0024, K0069, K0070, K0140

Cross-Site Scripting

Course | 31 minutes

This course introduces cross-site scripting vulnerabilities, their exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140

Cross-Site Request Forgery

Course | 23 minutes

This course introduces cross-site request forgery vulnerabilities, their exploitation and possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140

Poor HTTP Usage

Course | 43 minutes

This course describes how poor use of HTTP and HTML can be exploited, as well as possible mitigations.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140, K0398

Error Handling

Course | 27 minutes

This course describes how poor error handling can be exploited and possible mitigations for this problem.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140

Secure SDLC

SKILL PATH

The Secure SDLC learning path is a step-by-step approach to integrate the security controls into your software or system development life cycle. You will learn how to use each phase to develop or establish both proactive and reactive security controls across your organization.

Skill Assessment

Skill assessment | 20 questions

See how your secure SDLC skills stack up against other professionals in your field.

Secure SDLC Project

Project | 2 hours 27 minutes

Practice your secure SDLC skills by solving challenges.

NICE Knowledge and Skill Statements:

S0174

Introduction to SDLC

Course | 23 minutes

In this course, you'll be introduced to Secure SDLC, a framework to establish system development by integrating security.

NICE Knowledge and Skill Statements:

K0005, K0039, K0165

Security Awareness Training

Course | 1 hour 1 minute

Security awareness training is an education process that teaches employees and users about cybersecurity, IT best practices and even regulatory compliance.

NICE Knowledge and Skill Statements:

K0005, K0039, K0243

Secure Requirements

Course | 35 minutes

Secure requirements are security features required by system users or a quality the system must have to increase the user's trust.

NICE Knowledge and Skill Statements:

K0039, K0044, K0263, K0624

Secure Design

Course | 2 hours

Secure design applies to individual features that can correspond to their respective secure requirements.

NICE Knowledge and Skill Statements:

K0087, K0165, K0297

Secure Build

Course | 38 minutes

Secure build is a practice to apply the secure requirements and design to the software or system development.

NICE Knowledge and Skill Statements:

K0039, K0153

Secure Deploy

Course | 38 minutes

Secure deploy is for the purpose of formalizing and automating the deployment process in a secure way.

NICE Knowledge and Skill Statements:

K0178

Secure Validation

Course | 37 minutes

Secure validation is testing with a hacker's perspective to check whether the security controls are in place.

NICE Knowledge and Skill Statements:

K0028, K0091, K0290

Secure Response

Course | 34 minutes

Secure response is a structured methodology for handling security incidents, breaches and cyber threats.

NICE Knowledge and Skill Statements:

K0039, K0042

Collaborative Model

Course | 25 minutes

The collaborative model, or collaboration, is an approach that applies to a wide variety of systems and has been used to solve the security issues inherent in the enterprise systems or distributed environments.

NICE Knowledge and Skill Statements:

K0039, K0198

Software Security Testing

SKILL PATH

This pathway will help you master industry standards and enable you to carry out professional assessments to secure technologies, as well as communicate risks to high-level executives, management and technical staff.

Skill Assessment

Skill assessment | 20 questions

See how your software security testing skills stack up against other professionals in your field.

Software security testing project

Project | 2 hours 18 minutes

Test your knowledge of software security testing with this project.

Introduction to Software Security Testing

Course | 22 minutes

Environment setup is an essential process for becoming professional software security testers. This course will set up Kali Linux, a Debian-derived Linux distribution designed for digital forensics and penetration testing.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0290, K0609, K0610, K0624, S0014, S0073, S0078, S0174

Important software security testing terminology

Course | 21 minutes

It is vitally important to learn and adopt critical terminology and vocabulary. This course will highlight some essential concepts that you need to know in software security testing.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0070, K0090, K0147, K0290, K0412, K0415, K0436, K0609, K0610, K0624, S0014, S0078, S0174

Methodologies and standards

Course | 14 minutes

In this course, we will explore essential testing methodologies and standards that software security testers use regularly.

NICE Knowledge and Skill Statements:

K0001, K0004, K0005, K0006, K0009, K0054, K0059, K0070, K0075, K0087, K0090, K0147, K0154, K0260, K0261, K0262, K0290, K0377, K0624, S0014, S0078, S0174

Software testing as a process

Course | 29 minutes

Continuous learning and improvement are essential to staying relevant. Software security testing is similar to chess: easy to learn but hard to master. In this course, we will explore software testing as a process.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0043, K0070, K0075, K0087, K0090, K0147, K0290, K0624, S0014, S0078, S0174

The HTTP protocol

Course | 46 minutes

HTTP (HyperText Transfer Protocol) is the underlying protocol of the web. This course will explore the foundations of the HTTP protocol and the importance to software security.

Introduction to encoding

Course | 16 minutes

In this course, we will learn how to identify different encoding algorithms and decode them.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0068, K0070, K0075, K0090, K0140, K0147, K0290, K0624, S0014, S0078, S0095, S0174

Information gathering

Course | 1 hour 23 minutes

There are two types of methods used during information gathering: active and passive reconnaissance. You will learn the main differences and how to use both techniques to your advantage.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0290, K0315, K0408, K0624, S0014, S0078, S0174

Configuration and management testing

Course | 20 minutes

In this course, we will learn about configuration and management testing.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0070, K0073, K0075, K0090, K0275, K0290, K0624, S0014, S0078, S0153, S0174

Identity management testing

Course | 14 minutes

This course will explore identity and access management as one of the most critical provisions for IT departments.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0007, K0009, K0056, K0059, K0065, K0070, K0075, K0090, K0158, K0290, K0624, S0014, S0031, S0078, S0174

Authentication testing

Course | 12 minutes

In this course, we will explore authentication and different vulnerabilities in the implementation.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0007, K0009, K0044, K0059, K0070, K0075, K0090, K0147, K0290, K0336, K0487, K0624, S0014, S0078, S0174, S0367

Authorization testing

Course | 22 minutes

Testing for authorization means understanding how the authorization process works and using that information to circumvent the authorization mechanism. In this course, we will learn about authorization and various vulnerabilities in the implementation.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0007, K0009, K0037, K0044, K0059, K0070, K0075, K0090, K0147, K0290, K0336, K0487, K0624, S0014, S0078, S0174, S0367

Session management testing

Course | 29 minutes

In this course, we will explore some of the misconfigurations and vulnerabilities in session management.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0061, K0070, K0075, K0090, K0147, K0290, K0624, S0014, S0078, S0174

Input validation testing

Course | 39 minutes

In this course, we will explore data validation vulnerabilities and mitigation.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0160, K0290, K0624, S0014, S0019, S0078, S0174

Error handling

Course | 12 minutes

In this course, we will explore error handling vulnerabilities and mitigation.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0090, K0147, K0290, K0624, S0014, S0019, S0078, S0174

Cryptography

Course | 14 minutes

Cryptography appears to be closely linked to modern electronic communication. This course will teach you about cryptography and weak cryptographic algorithms that should be avoided while developing software.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0018, K0019, K0044, K0059, K0070, K0075, K0090, K0147, K0290, K0308, K0624, S0014, S0073

Business logic testing

Course | 14 minutes

Testing for business logic flaws in a multi-functional dynamic application requires thinking in unconventional ways. This course will teach you about the importance of business logic testing while helping you to think creatively.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0068, K0070, K0075, K0090, K0146, K0147, K0403, S0014, S0078, S0174, S0354

Client-side testing

Course | 32 minutes

Client-side testing refers to any type of testing that occurs in the user’s browser. This course will explore testing mechanisms for client-side vulnerabilities and ways to mitigate and reduce impact.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0077, K0090, K0147, K0286, K0290, K0444, K0624, S0014, S0078, S0174

Client-side testing reports

Course | 39 minutes

This course will help you learn crucial components of a software security testing report.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0009, K0059, K0070, K0075, K0077, K0090, K0147, K0286, K0290, K0315, K0354, K0444, K0451, K0624, S0014, S0037, S0078, S0174

Writing Secure Code for Android

SKILL PATH

This learning path teaches you how to incorporate security in Android application development for mobile devices. You will learn about Kotlin, best practices for addressing the most common security mistakes Android app developers make and learn to implement security into your app development.

Skill Assessment

Skill assessment | 20 questions

See how your secure coding in Android skills stack up against other professionals in your field.

Introduction to secure coding in Android

Course | 3 hours 6 minutes

Start your learning by understanding why secure coding is essential in mobile app development.

NICE Knowledge and Skill Statements:

K0014, K0016, K0068, K0372, K0624, S0060, S0257, S0266

Input validation

Course | 8 hours 11 minutes

Now that you understand the need for mobile app security, you should learn how to implement the most fundamental security mechanism of all: input validation.

NICE Knowledge and Skill Statements:

K0014, K0016, K0068, K0140, K0236, K0372, K0624, S0019, S0060, S0257, S0266

Memory corruption

Course | 46 minutes

You have learned the many ways to sanitize input in your app. It's time to turn your attention to mitigating another major application security risk: memory corruption.

NICE Knowledge and Skill Statements:

K0014, K0068, K0070, K0114, K0140, K0236, K0372, K0624, S0019, S0060, S0257, S0266

Encryption in Android

Course | 2 hours 31 minutes

You know about the most pressing security risks your app faces and how to address those risks. You can now learn how to use the one control that protects data better than any other: encryption.

NICE Knowledge and Skill Statements:

K0014, K0016, K0018, K0019, K0068, K0140, K0190, K0236, K0308, K0372, K0427, S0019, S0060, S0257, S0266

Protecting data

Course | 5 hours 12 minutes

Now that you have a good understanding of encryption, you can build on that foundation by learning additional ways to protect user data.

NICE Knowledge and Skill Statements:

K0005, K0014, K0016, K0068, K0070, K0095, K0140, K0168, K0224, K0236, K0372, K0419, K0624, S0019, S0060, S0257, S0266

Access control in Android

Course | 3 hours 12 minutes

You have learned many ways to protect data. You can now expand your security efforts by controlling access to the device and the app.

NICE Knowledge and Skill Statements:

K0005, K0007, K0014, K0016, K0033, K0056, K0068, K0070, K0095, K0372, K0488, S0007, S0019, S0031, S0060, S0097, S0257, S0266

Protecting software and system integrity

Course | 2 hours 32 minutes

You have gained a solid foundation for implementing the most common security controls in Android app development. You can now finish up your skill set by learning how to maintain application and device integrity.

NICE Knowledge and Skill Statements:

K0005, K0007, K0014, K0016, K0044, K0068, K0091, K0152, K0211, K0229, K0372, S0006, S0007, S0034, S0060, S0076, S0149, S0257, S0266, S0367

Writing Secure Code in C++

SKILL PATH

This learning path is intended for people who already know the C and C++ languages and want to improve their ability to write secure code.

Skill Assessment

Skill assessment | 20 questions

See how your secure C++ coding skills stack up against other professionals in your field.

Writing Secure Code in C++ Project

Project | 2 hours 48 minutes

Practice your secure C++ coding skills by solving challenges.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

C++ Code Security Cyber Range

Cyber range | 10 labs

Gain practical experience and develop your secure C++ coding skills through 10 hands-on labs in the C++ Code Security Cyber Range.

NICE Knowledge and Skill Statements:

S0060, S0172, S0174, S0266

Secure C/C++

Course | 13 minutes

This course is the introduction to the learning path. It presents the teacher, the tools and the content of the courses and explains why secure C/C++ is important.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0070

C/C++ Particularities

Course | 2 hours 44 minutes

This course covers all of the C/C++ particularities a programmer needs to know to create secure programs using these languages.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0070, K0372, K0396

Interacting with the World

Course | 2 hours 15 minutes

This course describes many ways a program can interact with the world.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0140, K0396

Error Handling

Course | 43 minutes

This course describes what to do and what not to do when an error occurs.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0140, K0229, K0396

Random Number Generation

Course | 21 minutes

This course explains why good random number generation is important when developing software. It also shows how the functions, the C library provides for that, are flawed. And then, it describes better way to generate random numbers.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0140, K0396

SETUID Bit

Course | 29 minutes

Some programs have "superpowers," and programming them requires special attention.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0140, K0396

Driver Development

Course | 43 minutes

Device drivers, as operating systems, are written in C. When applications interact directly with them, they become the kernel's last line of defense.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0140, K0396, K0608

Writing Secure Code in iOS

SKILL PATH

This learning path teaches you how to incorporate security in iOS application development for mobile devices. Focused mostly on Swift, Apple's new programming language, you will learn best practices for addressing the most common security mistakes iOS app developers make.

Skill Assessment

Skill assessment | 20 questions

See how your secure iOS coding skills stack up against other professionals in your field.

Penetration Testing Cyber Range

Cyber range | 7 hours 26 minutes

This cyber range helps you develop your knowledge of penetration testing and ethical hacking by practicing on cloud-hosted virtual machines.

Purple Team Web Application Security Project

Project | 2 hours 34 minuts

This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application.

NICE Knowledge and Skill Statements:

K0119, K0131, K0135, K0349, K0444, K0565, K0624, S0001

Introduction to Secure Coding

Course | 3 hours 48 minutes

Start your learning by understanding why secure coding is essential in mobile app development.

NICE Knowledge and Skill Statements:

K0004, K0039, K0068, K0070, K0079, K0080, K0082, K0139, K0140, K0269, K0559, K0624, S0060, S0172

Input Validation

Course | 5 hours 22 minutes

Now that you understand the need for mobile app security, you should learn how to implement the most fundamental security mechanism of all: input validation.

NICE Knowledge and Skill Statements:

K0004, K0039, K0059, K0068, K0070, K0080, K0082, K0140, K0624, S0019, S0060, S0172

Memory Corruption

Course | 45 minutes

You have learned the many ways to sanitize input in your app. It is time now to turn your attention to mitigating another major application security risk: memory corruption.

NICE Knowledge and Skill Statements:

K0039, K0059, K0068, K0070, K0079, K0080, K0082, K0114, K0140, K0624, S0060, S0172

Encryption

Course | 3 hours 2 minutes

You know about the most pressing security risks your app faces and how to address those risks. You can now learn how to use the one control that protects data better than any other: encryption.

NICE Knowledge and Skill Statements:

K0018, K0019, K0039, K0068, K0070, K0080, K0082, K0140, K0190, K0308, K0403, K0427, S0060, S0172, S0298

Protecting Data

Course | 2 hours 20 minutes

Now that you have a good understanding of encryption, you can build on that foundation by learning additional ways to protect user data.

NICE Knowledge and Skill Statements:

K0005, K0039, K0068, K0070, K0079, K0080, K0082, K0104, K0392, K0438, K0559, K0560, K0624, S0060, S0172

Access Control

Course | 1 hour 6 minutes

You have learned many ways to protect data. You can now expand your security efforts by controlling access to the device and the app.

NICE Knowledge and Skill Statements:

K0004, K0005, K0007, K0039, K0065, K0068, K0070, K0079, K0080, K0082, K0140, K0336, S0031, S0060, S0172

Protecting software and system integrity

Course | 1 hours 49 minutes

You have gained a solid foundation for implementing the most common security controls in iOS app development. You can now finish up your skill set by learning how to maintain application and device integrity.

NICE Knowledge and Skill Statements:

K0004, K0005, K0039, K0044, K0068, K0070, K0079, K0080, K0082, K0140, K0229, K0295, S0006, S0060, S0149, S0172

Writing Secure Code in ASP.NET

SKILL PATH

This skill path will enable you as a professional to execute secure coding practices, identify vulnerabilities in the code, remediate identified weaknesses, design with security in mind and build effective security controls to protect against breaches and malicious hackers.

ASP.NET skill assessment

Skill assessment | 20 questions

See how your secure secure coding skills stack up against other professionals in your field.

.NET project

Project | 2 hours 22 minutes

Test your knowledge of ASP.NET security with this project.

NICE Knowledge and Skill Statements:

K0004, K0005, K0016, K0068, K0140, K0372, S0060, S0148, S0172, S0266

Getting started with .NET core

Course | 45 minutes

In this course, you'll get to grips with the fundamentals of ASP.NET Core.

NICE Knowledge and Skill Statements:

K0004, K0005, K0016, K0068, K0140, K0372, S0060, S0148, S0172, S0266

.NET core vulnerabilities

Course | 1 hour 55 minutes

Without in-depth knowledge of what causes a vulnerability, it is almost impossible to deliver on the customers' expectations. This course addresses .NET Core vulnerabilities.

NICE Knowledge and Skill Statements:

K0004, K0005, K0016, K0068, K0140, K0372, S0060, S0148, S0172, S0266

.NET core vulnerabilities mitigation

Course | 2 hours 24 minutes

Mitigation of vulnerabilities is a critical statement in the fight against cybercriminals. This course explores vulnerability mitigation.

NICE Knowledge and Skill Statements:

K0004, K0005, K0006, K0016, K0068, K0140, K0372, K0527, S0060, S0148, S0172, S0266

Cryptography in .NET

Course | 59 minutes

his course will explore cryptographic operations in .NET Core that help developers code systems that protect confidentiality, integrity, non-repudiation and authenticity.

NICE Knowledge and Skill Statements:

K0004, K0005, K0016, K0018, K0019, K0068, K0140, K0308, K0372, S0060, S0148, S0172, S0266

Writing Secure Code in Java

SKILL PATH

Explore the ins and outs of writing secure coding in Java with these courses covering authentication, injection attacks, website security and more.

Skill Assessment

Skill assessment | 20 questions

See how your secure Java coding skills stack up against other professionals in your field.

Writing Secure Code in Java Project

Project | 2 hours 24 minutes

Build your Java project, then mitigate the vulnerabilities by adding validation to the inputs. You will also implement spring security on an application.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Introduction to Java

Course | 51 minutes

Take a deep dive into input validation, how to validate various input types and how to safeguard against malicious inputs that would be used for injection attacks.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0070, K0140

Injection Attacks

Course | 32 minutes

This course provides a demonstration of several SQL injection attacks and the special characters required to make them possible.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0070, K0140

Authentication

Course | 29 minutes

In this course, you'll review all the components required to secure a system.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0070, K0140, K0336

Sensitive Data

Course | 27 minutes

This course discusses sensitive data, non-sensitive data and personally identifiable information and provides examples of each.

NICE Knowledge and Skill Statements:

K0003, K0260, K0261, K0262, K0615

Input Output

Course | 49 minutes

This course reviews inputs and outputs to your system and how to move data in and out of your system securely.

NICE Knowledge and Skill Statements:

K0001, K0009, K0070, K0140

Website Security

Course | 1 hour 34 minutes

This course is a deep dive into redirects and forwards and the vulnerabilities associated with each.

NICE Knowledge and Skill Statements:

K0070, K0140, K0349, K0398

Malware

Course | 21 minutes

This course discusses malware related to Java development and how to mitigate the risks, and go over formalized code reviews.

NICE Knowledge and Skill Statements:

K0153, K0480

Writing Secure Code in Node.js

SKILL PATH

In this learning path, you will learn how to attack and protect Node.js applications.

Skill Assessment

Skill assessment | 20 questions

See how your secure node.js coding skills stack up against other professionals in your field.

NICE Knowledge and Skill Statements:

Writing Secure Code in Node.js Project

Project | 2 hours 15 minutes

There are seven challenges spread across three Node.js projects. Part 1 focuses on MongoDB injections and how to prevent them. Part 2 exploits event loop blocking. Part 3 is the one you need if you want to attack and fix a GraphQL API.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Refresher on Node.js

Course | 30 minutes

This course will cover the basics of Node.js architecture.

NICE Knowledge and Skill Statements:

K0004, K0016, K0068, K0140, K0236, K0372, S0060, S0257, S0266

Protecting databases

Course | 46 minutes

This course will focus on protecting database access.

NICE Knowledge and Skill Statements:

K0016, K0024, K0068, K0069, K0070, K0140, K0193, K0236, K0372, K0419, K0420, S0042, S0060, S0257, S0288

Node.js denial-of-service

Course | 1 hour 17 minutes

This course will focus on different ways of obtaining denial-of-service in Node.js and how to prevent them.

NICE Knowledge and Skill Statements:

K0016, K0068, K0140, K0362, K0372, K0612, S0060

Authentication and authorization

Course | 47 minutes

A look at authentication and authorization in Node.js.

NICE Knowledge and Skill Statements:

K0007, K0016, K0068, K0140, K0336, K0372

Prototype pollution

Course | 33 minutes

Exploring prototype pollution in Node.js.

NICE Knowledge and Skill Statements:

K0016, K0068, K0070, K0140, K0372, K0624

Unsafe strings

Course | 1 hour 3 minutes

Confronting the challenge of unsafe strings in Node.js.

NICE Knowledge and Skill Statements:

K0009, K0070, K0140

Error handling and asynchronous debugging monitoring

Course | 46 minutes

A look at the challenges of error handling in an asynchronous environment.

NICE Knowledge and Skill Statements:

K0016, K0068, K0079, K0140, K0186, K0372, K0396, S0014, S0149

Ecosystem modules (npm) and supply chain

Course | 55 minutes

An introduction to the challenges of npm modules.

NICE Knowledge and Skill Statements:

K0016, K0068, K0140, K0152, K0164, K0372

GraphQL security

Course | 44 minutes

This course explores mitigating the risks of GraphQL.

NICE Knowledge and Skill Statements:

K0016, K0068, K0140, K0332, K0372

Writing Secure Code in PHP

SKILL PATH

The Writing Secure Code in PHP Learning Path provides you with a foundation of secure programming techniques implemented in PHP. By the end of the learning path, you will be equipped to design and build secure and modern PHP applications.

Skill Assessment

Skill assessment | 20 questions

See how your secure PHP coding skills stack up against other professionals in your field.

Writing Secure Code in PHP Project

Project | 2 hours 15 minutes

Use your secure PHP coding skills to uncover issues in a simple application, such as cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, insecure secrets, lack of input sanitation and lack of proper error handling.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Operating Environment

Course | 36 minutes

This course takes a close look at the operating environment that your code runs in. This includes the version of PHP being used, third-party libraries and browser security such as HTTPS.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140, K0603

Cryptography Weaknesses

Course | 1 hour 24 minutes

This course provides a look at weaknesses in common cryptographic logic, including the better options that we have available to us. Also includes an overview of correctly handling our secret information.

NICE Knowledge and Skill Statements:

K0007, K0009, K0016, K0018, K0019, K0070, K0140, K0190, K0336, K0403

Code-Data Separation

Course | 1 hour 2 minutes

This course covers the separation of our code and data to prevent some of the most common types of attacks. These include SQL injection, XSS, CSRF, data leaks and source disclosure.

NICE Knowledge and Skill Statements:

K0009, K0016, K0070, K0140, K0624

Application Logic

Course | 1 hour 13 miinutes

In this course, you'll explore common types of application logic that are often sources of security vulnerabilities. These affect every part of your application and include things such as sessions, cookies, file uploads and error handling.

NICE Knowledge and Skill Statements:

K0007, K0009, K0016, K0068, K0070, K0140

APIs

Course | 25 minutes

APIs are an important part of modern web applications and require careful planning to ensure security. This course looks at how we secure APIs during authentication as well as responses.

NICE Knowledge and Skill Statements:

K0007, K0009, K0016, K0068, K0070, K0140, K0624

Development Process

Course | 1 hour 11 minutes

This course takes a look at our entire development process to ensure security at every point. This includes the tools we use and the places our code lives, as well as how we develop our code.

NICE Knowledge and Skill Statements:

K0009, K0016, K0068, K0070, K0140, K0153, K0178

Infrastructure

Course | 1 hour 6 minutes

A look at the infrastructure beneath our code, including how to set it up and secure it. This includes traditional architectures as well as modern architectures.

NICE Knowledge and Skill Statements:

K0032, K0178, K0205, K0286

Labs

Cyber ranges in Infosec Skills are cloud-hosted on virtual machines to provide the most realistic learning environment possible. With 100+ labs covering a variety of topics, you can build your cybersecurity skills through relevant, practical training — and go into your next project or job role with confidence.

C++ Code Security Cyber Range

HANDS-ON TRAINING

This cyber range helps you develop your knowledge in finding and remediating vulnerabilities in C++ code. You'll build and reinforce your skills as you progress through labs covering a wide range of C++ code security topics.

C++ – Introduction to cppcheck

Lab | 14 steps

cppcheck is a static code analysis tool for C++ code that tests for a wide number of potential vulnerabilities and other errors. This lab demonstrates some of the basic functionality and use of cppcheck.

NICE Knowledge and Skill Statements:

S0174

C++ – Control Flow Analysis in C++

Lab | 11 steps

A variety of different errors can affect the execution flow of code and its eventual result. This lab demonstrates the use of a control flow analysis tool for tracking the flow of C++ code and identifying these errors.

NICE Knowledge and Skill Statements:

S0174

C++ – Buffer Overflows

Lab | 14 steps

Buffer overflows are one of the simplest and most common programming errors in C++ code. This lab demonstrates several ways that a buffer overflow vulnerability can be introduced into code, how they can be exploited, and how to correct them.

NICE Knowledge and Skill Statements:

S0174

C++ – Integer Overflows and Underflows

Lab | 13 steps

Integer overflow and underflow vulnerabilities are created by unsafe typecasting between different integer variable types. This lab demonstrates code containing these vulnerabilities and how the vulnerabilities can be exploited.

NICE Knowledge and Skill Statements:

S0174

C++ – Format String Vulnerabilities

Lab | 13 steps

Format string specifiers are useful for building strings using variables of other types. However, if they are misused, they can have unexpected results or open up a program to exploitation.

NICE Knowledge and Skill Statements:

S0174

C++ – XPath Injection

Lab | 15 steps

XPath makes it possible to programmatically access data stored within an XML document. This lab demonstrates how poorly-designed XPath queries can be exploited and corrected.

NICE Knowledge and Skill Statements:

S0174

C++ – Type Management

Lab | 15 steps

C++ has a number of different variable types and ways of using them. This lab explores some of the ways that types and functions can be misused.

NICE Knowledge and Skill Statements:

S0174

C++ – Pointer Management

Lab | 14 steps

C++ pointers contain memory addresses and are used as a reference to arrays and other object types. This lab demonstrates some of the common mistakes made using pointers in C++.

NICE Knowledge and Skill Statements:

S0174

C++ – Sensitive Data Disclosure

Lab | 13 steps

Applications are frequently designed to process and protect sensitive information. This lab explores some of the ways that logical or implementation errors can unintentionally expose this data.

NICE Knowledge and Skill Statements:

S0174

C++ – Poor Error Handling

Lab | 15 steps

A variety of different factors can cause low-level functions and other code to fail. This lab demonstrates some ways in which errors in error handling can make code execution unpredictable or exploitable.

NICE Knowledge and Skill Statements:

S0174

Command Line Basics Cyber Range

HANDS-ON TRAINING

This cyber range introduces the most common Linux and Windows command-line tools and utilities. From basic navigation commands to port scanning and modifying file permissions, the labs in this cyber range help you practice some of the fundamental system and network administration tasks using Command-Line Interface (CLI).

Navigation

Lab | 26 steps

This lab goes through some of the basic commands for listing and navigating between files and directories on Linux and Windows systems.

NICE Knowledge and Skill Statements:

S0267

Text Control

Lab | 13 steps

Learn the basics of text control and searching for specific strings of text.

NICE Knowledge and Skill Statements:

S0267

User Accounts and Privileges

Lab | 33 steps

This lab focuses on creating and assigning users to groups as well as changing the privileges of said users and groups.

NICE Knowledge and Skill Statements:

S0158, S0267

File and Directory Permissions

Lab | 18 steps

This lab consists of editing permissions for files and directories and seeing how these permissions affect specific users.

NICE Knowledge and Skill Statements:

S0267

Basic Networking Utilities

Lab | 14 steps

This lab introduces the most popular command-line tools for testing and troubleshooting network connections, including ping, netstat, traceroute, tcpdump and others.

NICE Knowledge and Skill Statements:

S0046, S0241, S0267, S0294

Port Scanning

Lab | 15 steps

This lab walks through some of the most basic port scans that every system administrator should know.

NICE Knowledge and Skill Statements:

S0081, S0267

Introduction to PowerShell

Lab | 12 steps

In this lab we will demonstrate the uses of PowerShell as well as the functionality as a command line tool.

NICE Knowledge and Skill Statements:

S0158, S0267

File Transfer Protocol (FTP)

Lab | 20 steps

This lab uses an FTP server to demonstrate some of the utilities of the FTP protocol as well as some of the weaknesses.

NICE Knowledge and Skill Statements:

S0158, S0267

Remote Access (telnet vs. SSH)

Lab | 11 steps

This lab compares two commonly used methods of remote access — telnet and Secure Shell (SSH). You will go through steps of connecting to a remote host using both methods and try capturing login credentials.

NICE Knowledge and Skill Statements:

S0267

Computer Forensics Cyber Range

HANDS-ON TRAINING

Build and reinforce your skills as you progress through labs covering key computer forensics topics, including creating and examining forensic images, performing memory forensics to identify malware activity, data carving and more. You will practice working with poplar forensics tools, such as Volatility and Foremost.

Command Line Basics for Forensics

Lab | 13 steps

Practice basic Linux commands and some of the most useful native Linux tools for computer forensic investigations.

NICE Knowledge and Skill Statements:

S0267

Recovering data

Lab | 11 steps

In this lab, you will practice different methods of recovering data and finding out useful information straight from the command line.

NICE Knowledge and Skill Statements:

S0051, S0267

Hash Databases

Lab | 7 steps

DFIR uses hashing and it is used as a way of verifying the authenticity and structure of a file, normally with MD5 or SHA-1 checksums. We will use sha1deep and sha1sum to show how this works.

NICE Knowledge and Skill Statements:

S0071, S0267

File Carving

Lab | 13 steps

Practice carving different file types using foremost and scalpel.

NICE Knowledge and Skill Statements:

S0071, S0267

Network Forensics and Volatility

Lab | 9 steps

Use Volatility to find malware network activity from an infected Windows 7 memory dump.

NICE Knowledge and Skill Statements:

S0071, S0091, S0267

Memory Forensics with Volatility

Lab | 15 steps

Practice using Volatitliy to discover evidence on a Windows memory dump.

NICE Knowledge and Skill Statements:

S0062, S0071, S0091, S0267

ICS/SCADA Pentesting CTF: Lights Out

HANDS-ON TRAINING

You've become aware of a plot to launch a cyber-attack against a large sports stadium. Attackers plan to take over the facility's power management system and turn out the lights during a Sunday night sporting event. Your mission is to convince local authorities and stadium management the threat is real before time runs out.

Capture the Flag: Lights Out

Lab | 10 steps

Put on your white hat and try to prevent a major disaster from happening by solving 10 ICS/SCADA pentesting challenges.

NICE Knowledge and Skill Statements:

S0051, S0078, S0081

Linux Cyber Range

HANDS-ON TRAINING

Build your skills as you progress through labs covering a wide range of Linux topics, including basic commands, file and directory operations and attributes, permissions, job scheduling and much more. You'll also learn about managing SELinux, packages, extended file systems, firewalls, and units and control groups.

Basic Commands

Lab | 15 steps

Learn basic Linux commands and gain hands-on experience as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0267

VI Editor and Help

Lab | 14 steps

Learn about the visual editor as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Compressing and Archiving Tools

Lab | 18 steps

Explore compressing and archiving tools, such as gzip, gunzip, bzip2, bunzip2 and tar, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Login History and System Information

Lab | 17 steps

Learn about login user and group info, history info and system info as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0267

File Path and File Types

Lab | 12 steps

Learn about file paths and types as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

File and Directory Operations

Lab | 19 steps

Learn about file and directory operations as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

File and Directory Control Attributes

Lab | 20 steps

Learn about file and directory control attributes as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

File and Directory Permissions

Lab | 18 steps

Learn about file and directory permissions as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Special Permissions

Lab | 16 steps

Learn about special permissions as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Bash Shell

Lab | 18 steps

Learn about Bash Shell as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Regular Expressions and Metacharacters

Lab | 19 steps

Learn about regular expressions and metacharacters as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0267

Network Information and NTP

Lab | 10 steps

Learn about Network Time Protocol (NTP) as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing User and Group Accounts

Lab | 36 steps

Learn about managing user and group accounts, including creating, deleting and passwords, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Creating and Managing Partitions

Lab | 25 steps

Learn about creating and managing partitions as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Defining a NAT Virtual Network

Lab | 7 steps

Learn about defining a Network Address Translation (NAT) virtual network as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0007, S0067, S0158, S0267

Working with Processes

Lab | 13 steps

Learn about working with processes, such as nice/renice, ps and kill, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Job Scheduling

Lab | 12 steps

Learn about job scheduling as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Creating Storage Pools and Volumes

Lab | 10 steps

Learn about creating storage pools and volumes as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Working with Logical Volume Manager

Lab | 31 steps

Learn about the Logical Volume Manager (LVM) as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Understanding and Managing SELinux

Lab | 21 steps

Gain insight into managing SELinux as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0007, S0067, S0158, S0267

TCP Wrappers

Lab | 13 steps

Explore TCP wrappers as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing Packages with Yum

Lab | 18 steps

Learn about managing packages with Yum as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing Packages with RPM

Lab | 22 steps

Learn about managing packages with RPM as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Understanding Linux Kernel

Lab | 12 steps

Learn about Linux kernel as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Creating and Managing Extended File Systems

Lab | 33 steps

Learn about creating and managing extended file systems as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing Firewall

Lab | 33 steps

Learn about managing firewalls, including iptables and firewalld, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0084, S0158, S0267

Managing Units and Control Groups

Lab | 29 steps

Learn about managing units and control groups, including systemctl, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Working with XFS and VFAT File Systems

Lab | 25 steps

Learn about working with XFS and VFAT (Virtual File Allocation Table) file systems as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

System Logging

Lab | 17 steps

Learn about system logging, including syslog, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Using Swap

Lab | 11 steps

Learn about using swap as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Access Control Lists

Lab | 15 steps

Learn about access control lists (ACL), including file and directory ACLs, and default ACLs, as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0007, S0067, S0158, S0267

MITRE ATT&CK® Reconnaissance

HANDS-ON TRAINING

This cyber range will help you learn the reconnaissance tactics outlined in the MITRE ATT&CK framework. Reconnaissance is the act of gathering information about a system or target before an attack.

Building a Target Profile

Lab | 15 steps

This lab entails a series of Mitre ATT&CK techniques and sub techniques with the aim of creating a detailed profile, which includes organization, infrastructure, and human resource mapping.

Website Enumeration

Lab | 18 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how website enumeration can discover resources and underlying technology that the webserver is using.

Extracting Information from Routers and Access Points

Lab | 18 steps

This lab entails a series of Mitre ATT&CK techniques and sub techniques to learn how routers and access points can be targeted and enumerated.

Forwarding Host Traffic to the Router

Lab | 18 steps

Routers are networking devices that perform the traffic directing functions between computer networks. If adversaries gain access to these devices, an entirely internal network structure is compromised. Different attack vectors exist for exploiting these devices, allowing adversaries to gain higher access by port forwarding between machines.

Mapping DNS Information

Lab | 19 steps

This lab entails a series of Mitre ATT&CK techniques and sub-techniques with the aim of showcasing the possibility of intertwinement between them.

Planning a Spearphishing Attack

Lab | 10 steps

This lab entails a series of Mitre ATT&CK techniques and sub-techniques to identify and bypass security mechanisms to extract server information and plan a spearphishing attack.

Scanning Techniques

Lab | 13 steps

This lab will focus on teaching students to map the network structure by probing the active hosts via network traffic. The lab covers scenarios of false-positive results, packet crafting, and stealthy scanning.

MITRE ATT&CK® Resource Development

HANDS-ON TRAINING

This cyber range will help you learn the resource development tactics outlined in the MITRE ATT&CK framework. Resource development involves techniques of creating, buying, stealing, or compromising resources to carry out an attack.

Building Custom Tools

Lab | 15 steps

Understanding how tools are built allow a user to modify those tools to their needs or create new tools for the task at hand. This lab teaches the user to re-create the functionality of known tools such as Nmap and Netcat as well as tools that can be used for enumeration and vulnerability scanning.

Compromising Accounts

Lab | 18 steps

In some cases, the compromise of computer accounts can be caused by simple information leakage or profiling techniques, which give attackers the possibility to break in.

Drive-by Scenarios

Lab | 20 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show several drive-by attack scenarios and learn how to identify them.

Establishing Accounts

Lab | 22 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub techniques to identify and access website resources that could contain information of value. That information will be used to compromise accounts and establish access to target servers.

Malicious APK

Lab | 20 steps

Android Package (APK) is the Android application package file format. This package is used by the Android operating system and many other Android-based operating systems to distribute and install mobile apps, mobile games, and middleware.

Malicious Linux Packages

Lab | 20 steps

Learn how adversaries usually exploit Debian-based systems by creating malicious repositories for the APT packet manager and distributing them to the victims.

Python-based Command and Control server

Lab | 19 steps

This lab shows how to develop a stable Python-based Command and Control Server using the socket library and creating a reusable script which can be converted into an executable to be run on different targets.

Python-based Keylogger

Lab | 21 steps

Learn and create a Python-based keylogger utilizing Object-oriented programming principles to email the keystrokes to the user using a mail server as the information gathering unit.

Stored Firefox Credentials

Lab | 15 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how they can be intertwined to steal saved credentials from firefox.

Web-based Command and Control Server

Lab | 19 steps

This lab entails a series of Mitre ATT&CK techniques and sub-techniques with the aim of learning how a compromised web server can be used as a Command and Control server to launch attacks to other targets.

Webshells

Lab | 18 steps

In this lab, the student learns to develop and stage several webshells and how to determine which webshell should be uploaded to a web server. The compromised infrastructure is then used to deploy drive-by attacks.

MITRE ATT&CK® Initial Access

HANDS-ON TRAINING

This cyber range will help you learn the initial access tactics outlined in the MITRE ATT&CK framework. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network.

Drive-by Compromise

Lab | 22 steps

Learn how drive-by Compromise attacks rely on vulnerable users (targets) visiting the infected commonly used websites through which adversaries host malware.

Broken Access Control

Lab | 23 steps

Broken Access Control is one of the most encountered security issues in web applications. This lab will show different versions and exploitation scenarios for this set of security issues.

Exploiting Web Apps

Lab | 22 steps

In this lab you will complete challenges and learn about Padding Oracle Attacks, Server Side Template Injection, Union-based SQLi, Blind SQLi, and Use of a One Way Hash with a Predictable Salt.

Exploiting Public-Facing Applications

Lab | 18 steps

Learn how applications are often connected to databases, standard services (such as SMB or SSH), and other applications with internet-accessible open sockets (such as web servers).

Rubber Ducky & Bash Bunny

Lab | 26 steps

Learn how a malicious actor can use the rubber ducky to inject keystrokes into a system, hack a system, steal credentials, etc.

Log4j

Lab | 26 steps

The Apache Log4j versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack. Get hands-on experience with controlling log messages or log message parameters to execute arbitrary code loaded from LDAP servers.

Valid Accounts

Lab | 21 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to whos how adversaries can obtain and abuse credentials of existing accounts to gain Initial Access, Persistence, Privilege Escalation or Defense Evasion.

Heartbleed

Lab | 18 steps

In this lab, you'll get hands-on experience compromising secret keys used to identify the service providers and encrypt the traffic, the names and passwords of the users, and the actual content.

Initial Access - CTF

Lab | 25 steps

Exploit a vulnerable Webmin application in order to attach a code snippet to a software product which is used to establish a remote connection.

MITRE ATT&CK® Execution

HANDS-ON TRAINING

This cyber range will help you learn the execution tactics outlined in the MITRE ATT&CK framework. Execution consists of techniques that result in adversary-controlled code running on a local or remote system.

PowerShell

Lab | 22 steps

This lab will cover the basics of PowerShell and later on address scripting, command execution, and resource building utilizing this robust framework.

Unix Shell

Lab | 25 steps

Learn how adversaries may abuse command and script interpreters to execute commands, scripts, or binaries.

Visual Basic

Lab | 42 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how adversaries can abuse Visual Basic for execution.

Python

Lab | 23 steps

Python is a prevalent scripting/ programming language with capabilities to perform many functions. Get hands-on experience using Python libraries to download and execute commands to perform malicious behaviors.

JavaScript

Lab | 23 steps

Learn how adversaries abuse various implementations of JavaScript to execute various behaviors, such as hosting malicious scripts on websites or downloading and executing these scripts files as secondary payloads

Macros

Lab | 19 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub techniques to show how documents that leverage macros exploit capabilities that are provided by Microsoft Office or Libre Office for Linux Systems.

User Execution

Lab | 23 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub techniques to show how victims can be subjected to social engineering to get them to execute malicious code.

Exploitation for Client Execution

Lab | 23 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub techniques to show how adversaries may exploit software vulnerabilities in client applications to execute code.

Execution - CTF

Lab | 26 steps

This CTF highlights the range of possibilities attackers can choose from when planning to compromise a target. You will learn how to use Initial Access techniques in order to plan and orchestrate stealthy and persistent attacks.

MITRE ATT&CK® Persistence

HANDS-ON TRAINING

This cyber range will help you learn the persistence tactics outlined in the MITRE ATT&CK framework.

Traffic Signaling and Pre-OS Boot

Lab | 19 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how adversaries may use port knocking to hide open ports used for persistence and how adversaries may load a modified router configuration file from a Trivial File Transfer Protocol (TFTP) server.

Compromise Client Software Binary

Lab | 18 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub techniques to show how adversaries modified the OpenSSH binaries to establish persistent access to systems.

Authentication Process Modification

Lab | 24 steps

Learn how to alter authentication processes to gain access to user credentials and allow unwarranted access to accounts.

Maintaining Connections

Lab | 18 steps

The lab will showcase how different binaries and programming languages can be used to maintain persistent connections with the target machine.

Browser Extensions

Lab | 25 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how adversaries may abuse Internet browser extensions to establish persistent access to victim systems.

MITRE ATT&CK® Privilege Escalation

HANDS-ON TRAINING

This cyber range will help you learn the privilege escalation tactics outlined in the MITRE ATT&CK framework.

Library Hijacking and Shared Libraries

Lab | 25 steps

Get hands-on experience with privilege escalation techniques through library hijacking and shared resources for different programming languages.

Privilege Escalation Tools and Scripts

Lab | 20 steps

This lab incorporates a series of Mitre ATT&CK techniques and sub-techniques to show how adversaries may use tools and scripts to escalate their privileges.

Checklist and Commands

Lab | 24 steps

The lab highlights important Linux features, processes, and applications that can be exploited for privilege escalation and showcases best practices to protect these resources.

Exploitation For Privilege Escalation - Applications

Lab | 16 steps

This lab highlights when the adversary benefits from a programming error in a program, service, or kernel to execute malicious code.

Scheduled Tasks

Lab | 19 steps

This lab shows how task scheduling utilities can be used to run system commands on specific dates and times.

Network Traffic Analysis Cyber Range

HANDS-ON TRAINING

Gain useful skills related to analyzing network traffic as you work with Terminal Shark (TShark), Scapy and other tools to identify common network protocols, examine malware communications, extract transmitted files, filter output to display specific information, view communication statistics and much more.

Introduction to Terminal Shark

Lab | 15 steps

Terminal Shark, or TShark, is the command-line version of Wireshark, which is a commonly-used tool for network traffic analysis. This lab is designed to provide an introduction to Terminal Shark, including some of the most common command flags and uses.

NICE Knowledge and Skill Statements:

S0046, S0267

Traffic Replay and Live Traffic Analysis in TShark

Lab | 12 steps

This lab explores some of the options available when performing live traffic analysis with Terminal Shark (TShark).

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221

Extracting Files from Traffic Samples in TShark

Lab | 14 steps

Traffic captures commonly include files that are of interest to incident responders. This lab explores methods of extracting files from network traffic using Terminal Shark (or TShark).

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221

Decrypting SSL and TLS in TShark

Lab | 14 steps

Over half of all Internet traffic is encrypted, and malware makes heavy use of encryption to hide malicious content among legitimate traffic. In this lab, we will decrypt traffic encrypted with SSL and TLS using Terminal Shark.

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221

TShark and Command Line

Lab | 12 steps

Explore how Terminal Shark can be combined with Linux Terminal commands for network monitoring.

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221

Decoding and Decrypting Network Traffic Data

Lab | 13 steps

This lab demonstrates how to identify and reverse various encoding and encryption algorithms commonly used to obfuscate malware command and control traffic.

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221

Identifying Abnormal Traffic

Lab | 12 steps

Malware authors and other cybercriminals will often misuse legitimate protocols for command and control. This lab explores some of the ways that this can be accomplished.

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221, S0258

Scapy for Network Traffic Analysis

Lab | 15 steps

Scapy is a Python library for performing network traffic analysis. Using Scapy, it is possible to easily view, manipulate and write scripts using packet data.

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221

Traffic Generation with Scapy

Lab | 16 steps

The purpose of this lab is to explore the use of Scapy for building fake packets, which can be used for a variety of different purposes.

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221

Leaked Credential Extraction

Lab | 13 steps

Many commonly-used network protocols were not designed to be secure by default. This lab demonstrates how these credentials can be identified and extracted.

NICE Knowledge and Skill Statements:

S0046, S0156, S0199, S0221, S0267

Networking Cyber Range

HANDS-ON TRAINING

Build your skills as you progress through labs covering a wide range of networking topics, including switches and routers, networking protocols, configuring and verifying different networking devices, and troubleshooting issues. You'll also perform several labs designed to validate your VLAN and network management skills.

Network Data Collection

Lab | 17 steps

Learn how to use existing and custom honeyboxes and other tools to collect network traffic for further analysis.

NICE Knowledge and Skill Statements:

S0046, S0051, S0120, S0156, S0199, S0221

Connection Analysis

Lab | 17 steps

Understand connection analysis and what data can be extracted from high-level network traffic data.

NICE Knowledge and Skill Statements:

S0046, S0120, S0156, S0199, S0221

Switch Learning

Lab | 12 steps

Discover how switches learn MAC addresses and gain hands-on experience as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

VLAN Lab 1

Lab | 53 steps

Learn how to configure VLANs on Cisco switches as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S097

Switch Simlet

Lab | 24 steps

Learn about a switch simlet as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

STP Configuration and Verification

Lab | 39 steps

Explore STP configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Introduction to IP Routing

Lab | 35 steps

Learn about static and default routing as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Basic Router Configuration

Lab | 56 steps

Gain insight into basic Cisco router and switch configurations, including hostname, enable password, console and VTY passwords, as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S097, S0275

Basic Router Interface Configuration

Lab | 29 steps

Explore basic interface configuration on two routers as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S097, S0275

VLAN Lab 2 - ROAS

Lab | 35 steps

Learn about configuring Router on a Stick as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S097, S0275

Routing: Basic OSPF

Lab | 31 steps

Learn the basics of Open Shortest Path First (OSPF) routing protocol as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

OSPF Troubleshooting Examples

Lab | 34 steps

Learn about troubleshooting OSPF neighbor relationships and advertisements as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Troubleshoot & Resolve Routing Issues - OSPF

Lab | 30 steps

Explore how to troubleshoot OSPF as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0151, S0275

OSPF Area Types

Lab | 19 steps

Learn about OSPF area types as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Configuring EIGRP

Lab | 48 steps

Learn how to configure EIGRP on three routers as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

EIGRP Configuration and Verification

Lab | 30 steps

Learn about EIGRP configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

EIGRP Simulation

Lab | 33 steps

Explore EIGRP as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0151, S0275

GRE Tunnels Configuration and Verification

Lab | 25 steps

Learn about Generic Routing Encapsulation (GRE) tunnel configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Introduction to DMVPN

Lab | 15 steps

Get an introduction to DMVPN as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S097, S0275

Configuring PPP

Lab | 68 steps

Learn about PPP configuration as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

MPLS Layer VPN AToM

Lab | 15 steps

Learn about Any Transport Over MPLS (AToM) as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Introduction to MPLS Layer 3 VPN

Lab | 17 steps

Get an introduction to MPLS Layer 3 VPNs as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S097, S0275

BGP Weight, Local Preference and MED

Lab | 22 steps

Learn about BGP Weight, local preference and MED as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

HSRP Configuration and Verification

Lab | 22 steps

Learn about HSRP configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

GRE-PPP-EIGRP Troubleshooting

Lab | 33 steps

Learn about GRE-PPP-EIGRP troubleshooting as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0151, S0275

GLBP Configuration and Verification

Lab | 26 steps

Learn about GLBP configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Cisco IOS - Basic Traffic Shaping and Policing

Lab | 31 steps

Explore the basics of traffic shaping and traffic policing on a Cisco IOS router as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S097, S0275

Quality of Service Configuration and Verification

Lab | 32 steps

Learn about quality of service configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

DHCP Server Configuration and Verification

Lab | 34 steps

Explore DHCP server configuration and verification as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Basic Network Address Translation

Lab | 28 steps

Learn the basics of NAT (Network Address Translation) as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Basic Access Control Lists

Lab | 29 steps

Explore standard numbered and named ACLs (access control lists) as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0007, S0041, S0067, S0097, S0275

Basic ACL Configuration

Lab | 30 steps

Learn about configuring basic access-list with deny and permit statements as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Advanced ACL Configuration

Lab | 30 steps

Learn about extended ACLs (access control lists) as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0007, S0041, S0067, S0097, S0275

Syslog, Telnet, SSH and Banners

Lab | 40 steps

Explore four different tools available on your Cisco router's IOS as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Network Management Lab 1

Lab | 33 steps

Learn about network management on Cisco devices, including logging and SNMP, as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0275

Network Management Lab 2

Lab | 27 steps

Learn how to configure Internet Control Message Protocol (ICMP) echo-based IP Service Level Agreements (SLAs) as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0275

Cisco TCP Intercept

Lab | 23 steps

Learn about using the Cisco TCP intercept feature to protect against DoS and DDoS attacks as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0097, S0275

RIP-V2 Simulation

Lab | 33 steps

Learn about RIP-V2 as you practice in the Networking Cyber Range.

NICE Knowledge and Skill Statements:

S0041, S0067, S0275

Penetration Testing Cyber Range

HANDS-ON TRAINING

Build your skills as you progress through labs covering a wide range of pentesting topics, including abusing protocols, scanning for vulnerabilities, identifying exploits and delivering payloads, and more. You'll also perform several Capture the Flag (CTF) exercises designed to validate your new pentesting skills.

Linux Fundamentals

Lab | 23 steps

Explore the fundamentals of Linux and gain hands-on experience via the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0267

Abusing DNS

Lab | 10 steps

Learn about gathering information from DNS records as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0295

Abusing SNMP

Lab | 10 steps

Learn about getting information from SNMP as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Wi-Fi Pentesting

Lab | 4 steps

Learn about cracking WEP and WPA2 keys as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Port and Protocol Scanning with Nmap

Lab | 13 steps

Get familiar with the process of port scanning using Nmap as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

TCP/IP for Hackers

Lab | 21 steps

Learn about using TCP/IP for pentesting as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Host Discovery

Lab | 9 steps

Explore finding active hosts on a network as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Stealthy Network Reconnaissance

Lab | 19 steps

Learn stealthy scanning techniques with Nmap as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Advanced Scanning with Nmap

Lab | 7 steps

Hone your Nmap skills as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Scanning with Mobile Devices

Lab | 8 steps

Learn about running network scans from Android as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Sniffing

Lab | 18 steps

Discover why few things top having raw access to network traffic as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Service Identification

Lab | 8 steps

Learn about service identification as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

CTF 1: DNS and SNMP Reconnaissance

Lab | 4 steps

Test your DNS and SNMP reconnaissance skills as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Hacking with Android

Lab | 9 steps

Learn about launching a remote exploit from an Android device as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Credential Harvesting with SET

Lab | 14 steps

Learn about stealing passwords as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Spearphishing

Lab | 12 steps

Explore compromising a system via malicious email as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Web App Hacking

Lab | 26 steps

Gain experience with web application hacking as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Server Side Exploit

Lab | 12 steps

Learn how to exploit a web server vulnerability as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

CTF 2: Attacking FTP

Lab | 4 steps

Test your sniffing and password cracking skills as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Vulnerability Identification

Lab | 12 steps

Learn about vulnerability identification as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Basic SQL Injection

Lab | 26 steps

Discover how to exploit an SQL injection vulnerability as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Heartbleed Exploitation

Lab | 10 steps

Learn how to exploit the Heartbleed (OpenSSL) vulnerability as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Exploiting Vulnerable Services

Lab | 15 steps

Learn about gaining access to a remote systems as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

CTF 3: Web Application Exploitation

Lab | 4 steps

Test your web application hacking skills as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

SQL Injection Chained Exploitation

Lab | 11 steps

Explore combining SQL injection attacks as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Shellshock Exploitation

Lab | 11 steps

Learn about exploiting the Shellshock (GNU Bash) vulnerability as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Additional Payloads

Lab | 24 steps

Explore Metasploit payload options as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Android Exploitation

Lab | 17 steps

Learn about accessing Android devices remotely as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Client Side Exploits

Lab | 14 steps

Carry out an example of a client side exploit as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Using Ncat as a Trojan

Lab | 13 steps

Discover how to maintain access to compromised system with Ncat as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Post-Exploit Password Cracking

Lab | 12 steps

Learn about cracking hashed passwords gathered from a compromised system as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Covert Channels/Evasion

Lab | 25 steps

Learn about using encryption for covert communications and IDS evasion as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Intrusion Detection with Snort

Lab | 24 steps

Get an overview of using intrusion detection with Snort as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0025

CTF 4: Privilege Escalation

Lab | 3 steps

Test your privilege escalation skills as you practice in the Penetration Testing Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Python Code Security Cyber Range

HANDS-ON TRAINING

Build and reinforce your skills as you progress through labs covering a wide range of Python code security topics, including using Bandit, PyT and other tools to find common security issues in Python code, perform taint and control flow analysis, and recognize vulnerabilities that can lead to common application attacks.

Introduction to Python Bandit

Lab | 13 steps

Python bandit is one of the most commonly used Python linters and static analysis tools. This lab introduces the use of bandit for analysis of Python code.

NICE Knowledge and Skill Statements:

S0174

Introduction to Python Control Flow Analysis

Lab | 11 steps

Control flow analysis is useful for identifying mistakes or unexpected flows in a program. This lab demonstrates the use of staticfg for control flow analysis in Python.

NICE Knowledge and Skill Statements:

S0174

Command Injection in Python

Lab | 13 steps

A command injection vulnerability enables an attacker to run malicious code on the system where an application is running. This lab demonstrates how to identify, exploit and mitigate these vulnerabilities in Python.

NICE Knowledge and Skill Statements:

S0174

XPath Injection in Python

Lab | 15 steps

XPath is a programming language for extracting data from XML files; however, it is vulnerable to injection attacks. This lab demonstrates vulnerable code and how to exploit and remediate it.

NICE Knowledge and Skill Statements:

S0172

XML Attacks in Python

Lab | 12 steps

XML is a useful method for storing structured data, but code parsing it can be vulnerable to a number of attacks. This lab demonstrates some of the ways that different XML parsing functions can be exploited in Python.

NICE Knowledge and Skill Statements:

S0172

Race Conditions in Python

Lab | 14 steps

Race condition vulnerabilities exist when the proper operation of a program depends upon operations being run sequentially back-to-back. This lab demonstrates how to identify, exploit and remediate these vulnerabilities.

NICE Knowledge and Skill Statements:

S0172

Cross-Site Scripting in Python

Lab | 16 steps

Cross-site-scripting (XSS) is one of the most common web application vulnerabilities in existence. This lab demonstrates how to identify, exploit and remediate XSS vulnerabilities in Flask web applications.

NICE Knowledge and Skill Statements:

S0172

Cross-Site Request Forgery in Python

Lab | 11 steps

CSRF vulnerabilities allow an attacker to force unauthorized actions to be taken on an authenticated user's account. This lab demonstrates how to identify, exploit and remediate these vulnerabilities in Python code.

NICE Knowledge and Skill Statements:

S0174

Supply Chain Vulnerabilities in Python

Lab | 12 steps

Very few applications are designed to be completely standalone, and a program's dependencies can introduce vulnerabilities. This lab demonstrates the use of tools for identifying potential supply chain vulnerabilities in Python programs.

NICE Knowledge and Skill Statements:

S0174

Unsafe Deserialization in Python

Lab | 14 steps

Serialization is helpful for making Python objects and data writable to files and transferrable over the network. Learn how some serialization options can be vulnerable to exploitation in Python and how to securely serialize data.

NICE Knowledge and Skill Statements:

S0172

RHCSA Cyber Range

HANDS-ON TRAINING

This cyber range allows you to practice tasks covered in the Red Hat Certified System Administrator (RHCSA) exam objectives.

Basic Commands and Help

Lab | 20 steps

Learn basic RHEL commands and gain hands-on experience as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0267

Login History and Information

Lab | 11 steps

In this lab, you will work with common commands that display information about the system's users and groups as well as other system information, including uptime and kernel information.

NICE Knowledge and Skill Statements:

S0067, S0267

Compression and Archiving

Lab | 18 steps

Explore compressing and archiving tools, such as gzip, gunzip, bzip2, bunzip2 and tar, as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Using vi

Lab | 7 steps

Learn about the visual editor as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

File Path and File Types

Lab | 12 steps

Learn about file paths and types as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

File and Directory Operations

Lab | 19 steps

Learn about file and directory operations as you practice in the Linux Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Finding and Linking Files

Lab | 13 steps

This lab explores different options for finding files on RHEL systems, based on various criteria, such as size and permissions, and walks through the process of creating soft and hard links.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

File and Directory Permissions

Lab | 18 steps

Learn about file and directory permissions as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Special Permissions

Lab | 16 steps

Learn about special permissions as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Access Control Lists

Lab | 15 steps

Learn about access control lists (ACL), including file and directory ACLs, and default ACLs, as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0007, S0067, S0158, S0267

Managing Users

Lab | 24 steps

Practice managing user accounts on RHEL systems, including creating, deleting, and setting passwords.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing Groups

Lab | 13 steps

Practice creating, managing, and deleting group accounts on RHEL systems in this lab.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Bash Shell

Lab | 18 steps

Learn about the Bash Shell as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Regular Expressions & Metacharacters

Lab | 19 steps

Learn about regular expressions and metacharacters as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0267

Working with Processes and Jobs

Lab | 18 steps

Practice common commands for working with processes, such as top, nice/renice, ps and kill, and manage jobs with bg and fg.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Job Scheduling

Lab | 12 steps

Learn about job scheduling as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing packages with rpm

Lab | 22 steps

Learn about managing packages with RPM as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing packages with DNF

Lab | 13 steps

In this lab, you will practice working with DNF, or "Dandified yum". It is the next generation of the yum package manager that automatically computes dependencies and makes it easier to maintain groups of machines.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing Application Stream Modules

Lab | 10 steps

In this lab, you will practice working with DNF package manager to look up and manipulate application stream (AppStream) modules.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Understanding Linux Kernel

Lab | 12 steps

Learn about the Linux kernel as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing Units & System Tuning

Lab | 33 steps

Practice working with systemd to manage units and control groups, and explore tuned, a system tuning service available in RHEL.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

System Logging

Lab | 17 steps

Learn about system logging, including rsyslog, as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Creating and Managing Partitions

Lab | 25 steps

Learn about creating and managing partitions as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Storage Optimization with VDO

Lab | 10 steps

Virtual Data Optimizer (VDO) is one of the newer RHEL features, which allows conserving disk space, improving data throughput, and saving on storage costs. In this lab, we will install VDO and use it to create and remove a volume.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Working with Logical Volume Manager

Lab | 31 steps

Learn about the Logical Volume Manager (LVM) as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Working with Stratis Filesystems

Lab | 14 steps

RHEL 8 introduced a new simplified storage management solution called Stratis. In this lab, you will practice working with Stratic to create, manipulate, and destroy file systems and storage pools.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Working with XFS

Lab | 44 steps

In this lab, you will practice working with X File System (XFS), including creating, mounting, and resizing XFS file systems in VDO, LVM, and Stratis logical volumes.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Working with Swap

Lab | 11 steps

Learn about using swap as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Working with Remote File Systems and AutoFS

Lab | 18 steps

Practice working with Network File System (NFS) service and learn how to automatically mount NFS shares with AutoFS.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Network information and Chrony

Lab | 16 steps

Learn about querying network information and about chrony as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Using Key Based Authentication

Lab | 5 steps

Learn how to generate, distribute, and use key-based authentication for SSH.

NICE Knowledge and Skill Statements:

S0067, S0158, S0267

Managing Firewall

Lab | 21 steps

Learn about managing firewalls, including firewalld, as you practice in the RHCSA Cyber Range.

NICE Knowledge and Skill Statements:

S0067, S0084, S0158, S0267

Understanding & managing SELinux

Lab | 21 steps

In this lab we'll take a look at some of the tools for interacting with SELinux.

NICE Knowledge and Skill Statements:

S0067, S0121, S0158, S0267

SCADA Cyber Range

HANDS-ON TRAINING

Build your skills as you progress through labs covering a wide range of SCADA security topics, including reconnaissance, scanning, honeypots, attacks and exploits. You'll also perform several Capture the Flag (CTF) exercises designed to validate your new SCADA security skills.

Modbus PLC Introduction

Lab | 14 steps

Get an introduction to Modbus and gain hands-on experience via the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0051

SNMP Reconnaissance

Lab | 17 steps

Learn about abusing SNMP as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Datasheet Analysis

Lab | 4 steps

Explore getting valuable information from user manuals as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0268

CTF 1

Lab | 4 steps

Test your reconnaissance skills as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Scanning ICS/SCADA Networks

Lab | 17 steps

Learn about scanning SCADA networks as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Attacking the Infrastructure

Lab | 23 steps

Learn about compromising a system as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0052

Firewall Rules for SCADA

Lab | 17 steps

Get insight into SCADA firewall rules as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0076

Exploiting OS-Level Vulnerabilities

Lab | 22 steps

Learn about Shellshock exploitation on a host system as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Extracting Network Keys

Lab | 13 steps

Test your skills with exploiting ZigBee and encryption cracking as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Wi-Fi Password Cracking

Lab | 4 steps

Learn about cracking Wi-Fi passwords as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0051

Manipulating Protocol Data

Lab | 17 steps

Learn about manipulating protocol data as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0051

SCADA Honeypot

Lab | 15 steps

Explore the SCADA honeypot Conpot as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0120

Snort SCADA Rules

Lab | 19 steps

Learn about Snort SCADA rules as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0025

CTF 2

Lab | 4 steps

Test your sniffing skills as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0051

CTF 3

Lab | 4 steps

Test your SCADA defense skills as you practice in the SCADA Cyber Range.

NICE Knowledge and Skill Statements:

S0046

Projects

Projects are a series of hands-on exercises designed to reinforce your skills and provide real-world experience. Each exercise tests the practical application of topics covered in the associated learning path. As you work through the challenges, you'll put what you learned into practice and build confidence around your new skills.

Blockchain Security Project

HANDS-ON TRAINING

In this project, you'll begin by organizing information into a valid block. Then you'll answer questions related to proposed solutions to the 51% attack and performing a double-spend attack on a Proof of Stake blockchain. Finally, you'll identify smart contract vulnerabilities and the importance of binding values.

Blockchain Security Challenges

File | 1 file

Description of challenges you need to complete as part of this project.

Challenge Walkthrough Video

Video | 4 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

Challenge Hints Video

Video | 7 minutes

This video provides useful hints to help you solve the project challenges.

Blockchain Security Challenge Solutions

File | 1 file

This document contains solutions to the project challenges.

Container Security Project

HANDS-ON TRAINING

Test your understanding of container security with this project. You will review images to reduce risk, make docker images follow best practices, and scan images for vulnerable software.

Container Security Challenges

File | 1 file

A list of the challenges you will complete as part of this project.

NICE Knowledge and Skill Statements:

K0004, K0130, K0189, K0205, K0609, K0610, S0073, S0121

Container Security Project Walkthrough

Video | 23 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:

K0004, K0130, K0189, K0205, K0609, K0610, S0073, S0121

Container Security Project Hints

Video | 28 minutes

This video provides useful hints to help you solve the project challenges.

NICE Knowledge and Skill Statements:

K0004, K0130, K0189, K0205, K0609, K0610, S0073, S0121

Container Security Project Solutions

File | 1 file

This document contains solutions to the project challenges.

NICE Knowledge and Skill Statements:

K0004, K0130, K0189, K0205, K0609, K0610, S0073, S0121

Cryptography and Cryptanalysis Project

HANDS-ON TRAINING

In this project, you'll need to find information in encrypted network traffic, circumvent obfuscation to examine malware network communications and configuration samples, break down a hash function operation to find a specific input value and find the values of obfuscated passwords and cookies.

Project Walkthrough Video

Video | 5 minutes

An overview of the process and tasks involved in the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:

S0089, S0199, S0221, S0258

Project Files

File | 6 challenges

This downloadable .zip file contains challenges for the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:

S0089, S0199, S0221, S0258

Cryptography Challenge Questions

File | 1 file

This downloadable file contains challenge questions for the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:

S0089, S0199, S0221, S0258

Project Hints Video

Video | 5 minutes

Get hints to help you complete the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:

S0089, S0199, S0221, S0258

Challenge Questions Solutions

File | 1 file

View the solutions to the Cryptography and Cryptanalysis Project.

NICE Knowledge and Skill Statements:

S0089, S0199, S0221, S0258

Cyber Threat Hunting Project

HANDS-ON TRAINING

Use your cyber threat hunting skills to identify network traffic patterns for anomalies and investigate malware. You'll use Wireshark to examine packet capture files for potential red flags. Then you'll attempt to piece together the threat. Can you identify the malware?

Cyber Threat Hunting Project Walkthrough

Video | 11 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258

Traffic Analysis Exercise

File | 1 file

This contains files you will need to complete the project.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258

Cyber Threat Hunting Challenges

File | 1 file

This contains a description of challenges you need to complete as part of this project.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258

Cyber Threat Hunting Hints

Video | 3 minutes

This video provides useful hints to help you solve the project challenges.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258

Cyber Threat Hunting Challenge Answers

File | 1 file

Check your work on the Threat Hunting project.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258

Cybersecurity Data Science Project

HANDS-ON TRAINING

In this project, you'll analyze a malware sample using classifiers provided in the project files — or with ones you build yourself. You'll also recognize images created with deepfakes and determine text in a large number of CAPTCHA images.

Project Introduction Video

Video | 5 minutes

An overview of the process and tasks involved in the Cybersecurity Data Science Project.

NICE Knowledge and Skill Statements:

S0087, S0252, S0257

Project Files

File | 5 challenges

This downloadable .zip file contains challenges for the Cybersecurity Data Science Project.

NICE Knowledge and Skill Statements:

S0087, S0252, S0257

Project Hints Video

Video | 7 minutes

Get hints to help you complete the Cybersecurity Data Science Project.

NICE Knowledge and Skill Statements:

S0087, S0252, S0257

Project Solutions

File | 1 file

View the solutions to the Cybersecurity Data Science Project.

NICE Knowledge and Skill Statements:

S0087, S0252, S0257

ICS/SCADA Security Fundamentals Project

HANDS-ON TRAINING

This project contains three parts and will require you to complete tasks across the MITRE ATT&CK for ICS Framework, the NIST Cybersecurity Framework, risk assessment activities, ICS network architecture design, Packet Capture analysis, and reviewing Intrusion Detection System alert logs.

Project walkthrough

Video | 4 minutes

An overview of the project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

README

File | 1 file

Instructions for the project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Ubuntu VM

File | 1 file

The VM needed for this project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project part 1 challenges

File | 1 file

The challenges for part 1 of the project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project part 2 challenges

File | 1 file

The challenges for part 2 of the project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project part 3 challenges

File | 1 file

The challenges for part 3 of the project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project Hints

Video | 4 minutes

Some tips for completing the project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project part 1 solutions

File | 1 file

The answers for part 1 of the project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project part 2 solutions

File | 1 file

The answers for part 2 of the project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Project part 3 solutions

File | 1 file

The answers for part 3 of the project.

NICE Knowledge and Skill Statements:

K0027, K0046, K0062, K0137, K0165, K0170, K0179, K0233, K0301, K0324, K0405, K0437, K0609, S0025, S0046, S0073, S0120, S0156, S0171, S0199, S0221

Incident Response Project

HANDS-ON TRAINING

Use tools like Wireshark, Zeek and Volatility to respond to real-world scenarios. You'll investigate a "watering hole attack" that may have affected someone in the IT department and an SQL injection attack that may have led to credit card data being exfiltrated.

Incident Response Kali VM

File | 1 file

Download the files needed to set up your Kali virtual machine.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258, S0269

Kali VM Instructional Video

Video | 3 minutes

Get an overview of the virtual machine you will use to complete the two incident response projects.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258, S0269

Project 1 Walkthrough Video

Video | 2 minutes

An overview of the first incident response project. You'll respond to an incident involving an employee being compromised while using tools to practice penetration testing.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258, S0269

Project 1 Files

File | 1 file

This downloadable .zip file contains challenges for the first project, including an overview, 10 challenge questions, a memory dump and pcap file, and the answers to the challenges to verify your work.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258, S0269

Project 2 Walkthough Video

Video | 2 minutes

An overview of the second incident response project. You'll respond to an incident involving possible SQL injection that affected credit card data.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258, S0269

Project 2 Files

File | 1 file

This downloadable .zip file contains challenges for the second project, including an overview, 12 challenge questions, a pcap and a memory dump of the primary Card Data Environment (CDE) server, and the answers to the challenges.

NICE Knowledge and Skill Statements:

S0199, S0221, S0258, S0269

Mobile Application Pentesting Project

HANDS-ON TRAINING

Hone your iOS and Android application pentesting skills. You will use popular tools such as dex2jar and Hopper, practice working with ADB (Android Debug Bridge) and exploit various application vulnerabilities, including side-channel data leakage, broken cryptography, developer backdoors, insecure data storage and many others.

Mobile Application Pentesting Exercises

File | 24 challenges

An overview of the process and tasks involved in the Mobile Application Pentesting Project

NICE Knowledge and Skill Statements:

S0001, S0137

Using OVA Files

File | 1 file

A brief explanation of importing Open Virtual Appliance (OVA) files.

NICE Knowledge and Skill Statements:

S0001, S0137

Android VM

File | 1 virtual machine

An Android virtual machine to use as the pentesting target.

NICE Knowledge and Skill Statements:

S0001, S0137

Android Pentesting VM

File | 1 virtual machine

A virtual machine to be used as the attacker system for Android application pentesting exercises.

NICE Knowledge and Skill Statements:

S0001, S0137

iOS Pentesting Tools and Files

File | 1 file

A collection of tools and files needed for completing the iOS application pentesting exercises.

NICE Knowledge and Skill Statements:

S0001, S0137

Network Traffic Analysis for Incident Response Project

HANDS-ON TRAINING

In this project, you will need to apply your knowledge and use common network traffic analysis tools to solve multiple challenges. Each challenge involves examining a network traffic capture file containing evidence of malicious activity, such as malware infection, data exfiltration and C2 (command-and-control) communications.

Project Walkthrough Video

Video | 13 minutes

An overview of the process and tasks involved in the Network Traffic Analysis for Incident Response Project.

NICE Knowledge and Skill Statements:

S0092, S0156, S0199, S0221, S0258, S0269

Project Files

File | 7 challenges

This downloadable .zip file contains challenges for the Network Traffic Analysis for Incident Response Project.

NICE Knowledge and Skill Statements:

S0092, S0156, S0199, S0221, S0258, S0269

Project Hints Video

Video | 16 minutes

Get hints to help you complete the Network Traffic Analysis for Incident Response Project.

NICE Knowledge and Skill Statements:

S0092, S0156, S0199, S0221, S0258, S0269

Project Solutions

File | 1 file

View the solutions to the Network Traffic Analysis for Incident Response Project.

NICE Knowledge and Skill Statements:

S0092, S0156, S0199, S0221, S0258, S0269

NIST Cybersecurity Framework Project

HANDS-ON TRAINING

Perform a gap analysis to determine the current state of the organization compared to the target state. You'll determine and adjust impact levels with information from FIPS 199 and NIST SP 800-60 and identify the high-water mark from the impact levels. You'll select, map and tailor controls from the NIST SP 800-53 catalog.

Project Walkthrough Video

Video | 13 minutes

An overview of the process and tasks involved in the NIST Cybersecurity Framework Project.

NICE Knowledge and Skill Statements:

S0367, S0372

Project Files

File | 1 challenge

This downloadable .zip file contains challenges for the NIST Cybersecurity Framework Project.

NICE Knowledge and Skill Statements:

S0367, S0372

Project Solutions

File | 1 file

View the solutions to the NIST Cybersecurity Framework Project.

NICE Knowledge and Skill Statements:

S0367, S0372

NIST DoD RMF Project

HANDS-ON TRAINING

In this project, you'll be applying the process for selecting system impact levels and choosing security controls based on them. You'll complete the NIST FIPS 200 worksheet for system categorization and perform other tasks related to the RMF application process.

Project Walkthrough

Video | 17 minutes

An overview of the process and tasks involved in the NIST DoD RMF Project.

NICE Knowledge and Skill Statements:

S0115, S0147, S0228

Artifcats List

File | 1 challenge

This downloadable file contains a list of artifacts used in the NIST DoD RMF Project.

NICE Knowledge and Skill Statements:

S0115, S0147, S0228

Challenge Questions

File | 1 file

This downloadable file contains challenge questions for the NIST DoD RMF Project.

NICE Knowledge and Skill Statements:

S0115, S0147, S0228

Project Artifacts

File | 1 file

This downloadable file contains walkthrough artifacts for the NIST DoD RMF Project.

NICE Knowledge and Skill Statements:

S0115, S0147, S0228

Challenge Solutions

File | 1 file

View the solutions to the NIST DoD RMF Project.

NICE Knowledge and Skill Statements:

S0115, S0147, S0228

Offensive Bash Scripting Project

HANDS-ON TRAINING

This Offensive Bash Scripting Project will put your new skills to the test! Your mission will be to hack the virtual machine named Kioptrix 2. This is a scaled-down version of Kioptrix 4 but uses the exact same enumeration process. Plenty of resources will be provided to assist you along solving this puzzle.

Project Walkthrough

Video | 25 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:

S0051, S0078

Project Challenges

File | 1 file

Descriptions of the challenges you need to complete as part of this project.

NICE Knowledge and Skill Statements:

S0051, S0078

Project Resources

File | 1 file

Links and other useful information for the project.

NICE Knowledge and Skill Statements:

S0051, S0078

Project VM

File | 1 file

The VM needed for the project.

NICE Knowledge and Skill Statements:

S0051, S0078

Project Hints

Video | 3 minutes

This video provides useful hints to help you solve the project challenges.

NICE Knowledge and Skill Statements:

S0051, S0078

Project Challenges Solutions

File | 1 file

Solutions to the challenge questions so you can check your work.

NICE Knowledge and Skill Statements:

S0051, S0078

Python for Pentesters Project

HANDS-ON TRAINING

Test your understanding of Python for Pentesting in this project consisting of five challenges: create an email sender, create a buffer overflow exploit, write commands to conduct a Wi-Fi attack, start a new web scraping project and write a line of smtp code.

Project Challenges

File | 1 file

This file describes all of the challenges

NICE Knowledge and Skill Statements:

K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266

Project Walkthrough

Video | 4 minutes

This video walks you through the challenges.

NICE Knowledge and Skill Statements:

K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266

Project Hints

Video | 20 minutes

This video walks you through how to solve the project challenges.

NICE Knowledge and Skill Statements:

K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266

Project Solutions

File | 1 file

This file shares the project solutions so you can check your work.

NICE Knowledge and Skill Statements:

K0004, K0005, K0009, K0016, K0068, K0070, K0138, K0362, K0372, K0396, K0529, K0624, S0060, S0266

Purple Team Privilege Escalation Project

HANDS-ON TRAINING

This project contains three labs focused on understanding, exploiting, and mitigating vulnerabilities that allow a user to escalate their privileges. You will learn about sudo abuse, path injection attacks, and how to discover and remove sensitive information from Git repositories.

Project Files

File | 1 file

A ZIP file containing the OVA file and instructions for completing the Purple Team Privilege Escalation Project.

NICE Knowledge and Skill Statements:

S0266, S0267

Lab 1: Git Secrets Walkthrough

Video | 9 minutes

A detailed video walkthrough of the first lab in the Purple Privilege Escalation Project.

NICE Knowledge and Skill Statements:

S0266, S0267

Lab 2: Path Interception Walkthrough

Video | 14 minutes

A detailed video walkthrough of the second lab in the Purple Privilege Escalation Project.

NICE Knowledge and Skill Statements:

S0266, S0267

Lab 3: Insecure Sudo Walkthrough

Video | 8 minutes

A detailed video walkthrough of the third lab in the Purple Privilege Escalation Project.

NICE Knowledge and Skill Statements:

S0266, S0267

Project Solutions

File | 1 file

A document containing the solutions to the Purple Team Privilege Escalation Project challenges.

NICE Knowledge and Skill Statements:

S0266, S0267

Purple Team Web Application Security Project

HANDS-ON TRAINING

This project contains three labs focused on understanding, exploiting and mitigating a real vulnerability found in a real web application. You'll intercept web traffic with Burp Suite, perform a local file inclusion attack, practice using a static code analyzer, and learn about mitigation approaches and web application firewalls.

Project Files

File | 1 file

A ZIP file containing the OVA file and instructions for completing the Purple Team Web Application Security Project.

NICE Knowledge and Skill Statements:

S0022, S0025, S0051, S0084, S0172, S0174, S0293

Lab 1: Local File Inclusion (LFI) walkthrough

Video | 8 minutes

A detailed walkthrough of the first lab in the Purple Team Web Application Security Project.

NICE Knowledge and Skill Statements:

S0022, S0025, S0051, S0084, S0172, S0174, S0293

Lab 2: Secure Coding walkthrough

Video | 16 minutes

A detailed walkthrough of the second lab in the Purple Team Web Application Security Project.

NICE Knowledge and Skill Statements:

S0022, S0025, S0051, S0084, S0172, S0174, S0293

Lab 3: Web Application Firewall (WAF) walkthrough

Video | 9 minutes

A detailed walkthrough of the third lab in the Purple Team Web Application Security Project.

NICE Knowledge and Skill Statements:

S0022, S0025, S0051, S0084, S0172, S0174, S0293

Project Solutions

File | 1 file

A document containing the solutions to the Purple Team Web Application Security Project challenges.

NICE Knowledge and Skill Statements:

S0022, S0025, S0051, S0084, S0172, S0174, S0293

Secure Coding Fundamentals Project

HANDS-ON TRAINING

In this project, you'll identify vulnerabilities in the provided applications and code samples and discover how those vulnerabilities could be exploited by an attacker. See for yourself how security errors in code can lead to compromised credentials, SQL injections, and buffer overflow and Cross-Site Scripting (XSS) attacks.

Project Introduction Video

Video | 4 minutes

An overview of the process and tasks involved in the Secure Coding Fundamentals Project.

NICE Knowledge and Skill Statements:

S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266

Project Files

File | 5 challenges

This downloadable .zip file contains challenges for the Secure Coding Fundamentals Project.

NICE Knowledge and Skill Statements:

S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266

Project Hints Video

Video | 3 minutes

Get hints to help you complete the Secure Coding Fundamentals Project.

NICE Knowledge and Skill Statements:

S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266

Project Solutions

File | 1 file

View the solutions to the Secure Coding Fundamental Project.

NICE Knowledge and Skill Statements:

S0060, S0078, S0094, S0095, S0172, S0239, S0257, S0266

Secure SDLC Project

HANDS-ON TRAINING

Practice your secure SDLC skills as your progress through four exercises related to threat modeling, static application security testing and white-box security testing using both automated tool-based analysis and manual analysis.

Project Codebase

File | 1 file

Files you will need to complete the project.

NICE Knowledge and Skill Statements:

S0174

Project Applications

File | 1 file

Application needed to complete the project.

NICE Knowledge and Skill Statements:

S0174

Project Challenges

File | 1 file

Description of challenges you need to complete as part of this project.

NICE Knowledge and Skill Statements:

S0174

Exercise 1 Walkthrough

Video | 7 minutes

This video walks you through exercise 1, threat modeling approach using Microsoft Threat Modeling Tool.

NICE Knowledge and Skill Statements:

S0174

Exercises 2, 3, 4 Walkthrough

Video | 12 minutes

This video walks you through exercises 2-4: static application security testing (SAST) using codebase and VCG tool, white-box security testing and manual analysis, and white-box security testing with manual analysis.

NICE Knowledge and Skill Statements:

S0174

Project Solutions

File | 1 file

This document contains solutions to the project challenges.

NICE Knowledge and Skill Statements:

S0174

Securing Linux/UNIX Project

HANDS-ON TRAINING

Test your understanding of securing Linux and UNIX in this project consisting of five challenges. You'll get hands-on experience using sudo, configuring OpenSSH, identifying and configuring access to TCP ports, decrypting and encrypting with GPG, and using SELinux.

Project Walkthrough

Video | 4 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

Project OVA

File | 1 file

Files you will need to complete the project.

Project Hints

Video | 5 minutes

This video provides useful hints to help you solve the project challenges.

SIEM Architecture and Process Project

HANDS-ON TRAINING

Test your SIEM skills as you progress through five challenges. We will take a use case surrounding invalid user logon attempts and standardize our username field, visualize our data with a dashboard, enrich our data with last known user information, and create an alert that triggers with the required information.

Project Overview and Challenge Documents

File | 1 file

The challenge files and other documents you will need to complete this project.

NICE Knowledge and Skill Statements:

S0173

winlogbeat

File | 1 file

Files you will need to complete this project.

NICE Knowledge and Skill Statements:

S0173

Virtual Box

File | 1 file

Files you will need to complete this project.

NICE Knowledge and Skill Statements:

S0173

Graylog

File | 1 file

Files you will need to complete this project.

NICE Knowledge and Skill Statements:

S0173

Standardizing the Username Field Hint

Video | 5 minutes

In this video you are provided hints on how to find the index field you will be required to alter, and how to navigate to a pipeline processing rule.

NICE Knowledge and Skill Statements:

S0173

Standardizing the Username Field Answer

Video | 1 minute

In this video you are provided the remaining information required to create the pipeline processing rule to begin standardizing the username field.

NICE Knowledge and Skill Statements:

S0173

Creating the Invalid User Logon Dashboard Hint

Video | 1 minute

In this video you are provided hints to search for the specific data requirements to create your dashboard for invalid user logons.

NICE Knowledge and Skill Statements:

S0173

Creating the Invalid User Logon Dashboard Answer

Video | 2 minutes

In this video you are provided with remaining information required to complete your invalid user logon dashboard.

NICE Knowledge and Skill Statements:

S0173

Lookup Table Creation Hint

Video | 2 minutes

In this video you are provided hints on creating the lookup table required to enrich last successful logons on failed logons.

NICE Knowledge and Skill Statements:

S0173

Last User Logon Search Criterion Hint

Video | 5 minutes

In this video you are provided hints to create search filter for the mapping of hostnames to last successful logons.

NICE Knowledge and Skill Statements:

S0173

Last User Logon Data Enrichment Hint

Video | 3 minutes

In this video you are provided the remaining information for the search filter and provided hints to begin mapping hostnames to last successful logged on user.

NICE Knowledge and Skill Statements:

S0173

Enriching Last User Logon to Failed Logon Hint

Video | 3 minutes

In this video you are provided the remaining information for mapping hostnames to last successful logged on user and hints on enriching failed logons with last known user information.

NICE Knowledge and Skill Statements:

S0173

Enriching Last User Logon to Failed Logon Answer

Video | 2 minutes

In this video you are provided the remaining information to create the enrichment of last known username on invalid logon attempts.

NICE Knowledge and Skill Statements:

S0173

Filtering Non-User Logons From Dashboard Hint

Video | 2 minutes

In this video you are provided hints on finding the information required to filter non-interactive and non-invalid username related activity.

NICE Knowledge and Skill Statements:

S0173

Filtering Non-User Logons From Dashboard Answer

Video | 2 minutes

In this video you are provided the remaining information required to filter the non-interact and non-invalid username related activity.

NICE Knowledge and Skill Statements:

S0173

Creating an Alert on Invalid User Logon Attempts Hint

Video | 2 minutes

In this video you are provided hints on creating an alarm to trigger when an invalid logon occurs.

NICE Knowledge and Skill Statements:

S0173

Creating an Alert on Invalid User Logon Attempts Answer

Video | 5 minutes

In this video you are provided the remaining information on creating the alarm to trigger when an invalid logon occurs.

NICE Knowledge and Skill Statements:

S0173

Vulnerability Assessment Project

HANDS-ON TRAINING

Test your skills as your progress through seven challenges leveraging free-to-use security tools and services. Set up your environment using JDK 11, Maven 3.6.3 and Git. Then use SNYK, static application security testing with Coverity Scan and a risk assessment template to discover, identify and rate the CWEs and CVEs.

Project Walkthrough

Video | 3 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:

S0001, S0137, S0174

Project Challenges

File | 1 file

Description of the challenges you need to complete as part of this project.

NICE Knowledge and Skill Statements:

S0001, S0137, S0174

Project Prerequisites

File | 1 file

Files and links you will need to complete this project.

NICE Knowledge and Skill Statements:

S0001, S0137, S0174

Risk Assessment Template

File | 1 file

The template you will need to complete this project.

NICE Knowledge and Skill Statements:

S0001, S0137, S0174

Coverity Scan Demo

Video | 17 minutes

Demonstration of Coverity Scan.

NICE Knowledge and Skill Statements:

S0001, S0137, S0174

OTX Demo

Video | 5 minutes

Demonstration of OTX.

NICE Knowledge and Skill Statements:

S0001, S0137, S0174

SNYK Demo

Video | 8 minutes

Demonstration of SNYK.

NICE Knowledge and Skill Statements:

S0001, S0137, S0174

Project Challenges Solutions

File | 1 file

This document contains solutions to the project challenges.

NICE Knowledge and Skill Statements:

S0001, S0137, S0174

Vulnerability Management Project

HANDS-ON TRAINING

Put your vulnerability management skills to the test as you progress through a series of challenges. You'll identify risky open ports, find vulnerabilities in the operating system and SMB service, verify vulnerabilities and find their CVSS score, investigate how to remediate the vulnerabilities and more.

Project Walkthrough

Video | 12 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:

S0036

Project Challenges

File | 1 file

A list of questions you will complete as part of this project.

NICE Knowledge and Skill Statements:

S0036

Vulnerability Management Metasploitable VM

File | 1 file

Files you will need to complete the project.

NICE Knowledge and Skill Statements:

S0036

Project Hints Video

Video | 2 minutes

This video provides useful hints to help you solve the project challenges.

NICE Knowledge and Skill Statements:

S0036

Project Challenges Solutions

File | 1 file

This document contains solutions to the project challenges.

NICE Knowledge and Skill Statements:

S0036

Web Application Pentesting Project

HANDS-ON TRAINING

In this project, you'll explore the most common web application security risks, including SQL injection, Cross-Site scripting (XSS), broken authentication and more. You'll need to apply all your knowledge about web application vulnerabilities and use many different tools and browser utilities to solve the challenges.

Web Application Pentesting Project - Getting Started

File | 13 challenges

This file contains information needed to get started on completing the Web Application Pentesting CTF challenge.

NICE Knowledge and Skill Statements:

S0051, S0078, S0137, S0167

Web Application Pentesting Project - Walkthrough

Video | 3 minutes

An overview of the process and tasks involved in the Web Application Pentesting project.

NICE Knowledge and Skill Statements:

S0051, S0078, S0137, S0167

Web Application Pentesting Project - Solutions

File | 1 file

Solutions to all Web Application Penetsting Project challenges.

NICE Knowledge and Skill Statements:

S0051, S0078, S0137, S0167

Web Server Protection Project

HANDS-ON TRAINING

Secure a real web server in this hands-on project. You will need to work with an Apache web server installed on a virtual machine to implement network filtering, add cookies to access log, harden the host OS, identify tampered binary files and complete other tasks to ensure that your web server is properly protected.

Project Walkthrough Video

Video | 19 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:

S0051, S0078, S0137, S0167

Project Challenges

File | 10 challenges

Description of challenges you need to complete as part of this project.

NICE Knowledge and Skill Statements:

S0051, S0078, S0137, S0167

Project Files

File | 1 file

Files you will need to complete the project.

NICE Knowledge and Skill Statements:

S0051, S0078, S0137, S0167

Project VM Keys

File | 1 file

Key files for the virtual machine used in the project.

NICE Knowledge and Skill Statements:

S0051, S0078, S0137, S0167

Project Hints Video

Video | 22 minutes

This video provides useful hints to help you solve the project challenges.

NICE Knowledge and Skill Statements:

S0051, S0078, S0137, S0167

Project Solutions

File | 1 file

This document contains solutions to all project challenges.

NICE Knowledge and Skill Statements:

S0051, S0078, S0137, S0167

Windows 10 Host Security Project

HANDS-ON TRAINING

In this project, you'll first set up a secure Hyper-V lab environment. Next, you'll practice locating and enabling the virtual trusted platform module and virtualization-based security, encrypting data with BitLocker, sharing files and modifying user permissions, verifying port security provided by Windows Firewall and more.

Project Walkthough Video

Video | 16 minutes

An overview of the process and tasks involved in the Windows 10 Host Security Project.

NICE Knowledge and Skill Statements:

S0067, S0076, S0079, S0158, S0267, S0268

Project Challenges

File | 7 challenges

This documents describes the configuration and challenges for the Windows 10 Host Security Project.

NICE Knowledge and Skill Statements:

S0067, S0076, S0079, S0158, S0267, S0268

Project Hints Video

Video | 8 minutes

Get hints to help you complete the Windows 10 Host Security Project.

NICE Knowledge and Skill Statements:

S0067, S0076, S0079, S0158, S0267, S0268

Solutions

File | 1 file

View the solutions to the Windows 10 Host Security Project.

NICE Knowledge and Skill Statements:

S0067, S0076, S0079, S0158, S0267, S0268

Windows Registry Forensics Project

HANDS-ON TRAINING

Test your Windows Registry Forensics skills by answering 25 challenges. You must first locate the registry files within the file system and export them to be examined. Then you'll use tools such as Registry Explorer, Decode and ShellBag to find the answers.

Windows Registry Forensics Project Challenges

File | 1 file

Gives a detailed explanation of the Windows Registry Forensics project.

NICE Knowledge and Skill Statements:

S0071, S0091

Windows Registry Forensics Project Walkthrough

Video | 37 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:

S0071, S0091

Windows Server Security

HANDS-ON TRAINING

You'll start with installing Active Directory. Then you'll practice creating a shared folder and calculating effective permissions, hiding shares from users, encrypting files using the Encrypting File System (EFS) and BitLocker, blocking access via IP addresses and firewall ports, and securing server traffic using certificates.

Windows Server Security Challenges

File | 1 file

This file contains directions to set up a secure Hyper-V lab on your Windows 10 host and an overview of the eight challenges in the Windows Server Security Project.

NICE Knowledge and Skill Statements:

S0136, S0158, S0367

Windows Server Security Challenges Walkthrough

Video | 8 minutes

Learn how to set up your lab environment and get a brief walkthrough of each of the eight challenges you need to solve.

NICE Knowledge and Skill Statements:

S0136, S0158, S0367

Project Walkthrough with Hints

Video | 5 minutes

Stuck on a challenge? This video provides hints to help guide you in the right direction.

NICE Knowledge and Skill Statements:

S0136, S0158, S0367

Project Solutions

File | 1 file

This file contains the solutions to the Windows Server Security Project.

NICE Knowledge and Skill Statements:

S0136, S0158, S0367

Writing Secure Code in C++ Project

HANDS-ON TRAINING

The project starts with the code of a very simple and unsafe HTTP server. This program receives requests through a TCP socket and returns the requested file or the output of executed commands. The student is guided through discovering the different security issues, describing them and fixing them.

Project Introduction

Video | 10 minutes

This video is an introduction to the project.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Receiving Requests

Video | 7 minutes

This video explores the topic of receiving requests.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Receiving Requests: The Security Flaw

Video | 3 minutes

This video takes you through the security flaws in receiving requests.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Receiving Requests: A Possible Solution

Video | 1 minute

Explore a possible solution for flaws in receiving requests.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Parsing Requests: The Flaw

Video | 1 minute

This video takes you through the security flaws in parsing requests.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Parsing Requests: A Possible Solution

Video | 4 minutes

This video explores a possible solution to the flaw in parsing requests.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Sending Files: The Flaw

Video | 4 minutes

This video takes you through the security flaws in sending files.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Sending Files: A Possible Solution

Video | 8 minutes

Take a look at the potential solution for the flaw in sending files.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Executing Programs: Flaws and Fix

Video | 6 minutes

This video will be your guide to the details of executing programs.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Executing Programs: A Possible Solution

Video | 4 minutes

This video explores a possible solution to the flaw in executing programs.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Writing Secure Code in C++ Project VM

File | 1 file

Download the VM you will need to complete the C++ project.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Writing Secure Code in Node.js

HANDS-ON TRAINING

There are seven challenges spread across three Node.js projects. Part 1 focuses on MongoDB injections and how to prevent them. Part 2 exploits event loop blocking. Part 3 is the one you need if you want to attack and fix a GraphQL API.

Writing secure code in Node.js project challenges

File | 1 file

This file describes all of the challenges

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Writing secure code in Node.js walkthrough

Video | 5 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Writing secure code in Node.js project files

File | 1 file

Contains all the files you will need to complete the challenges.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Challenge 1 hint

Video | 1 minute

This video provides useful hints to help you solve the first project challenge.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Challenge 2 hint

Video | 2 minute

This video provides useful hints to help you solve the second project challenge.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Challenge 3 hint

Video | 3 minute

This video provides useful hints to help you solve the third project challenge.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Challenge 4 hint

Video | 4 minute

This video provides useful hints to help you solve the fourth project challenge.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Challenge 5 hint

Video | 5 minute

This video provides useful hints to help you solve the fifth project challenge.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Challenge 6 hint

Video | 6 minute

This video provides useful hints to help you solve the sixth project challenge.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Challenge 7 hint

Video | 7 minute

This video provides useful hints to help you solve the seventh project challenge.

NICE Knowledge and Skill Statements:

K0004, K0016, K0024, K0068, K0069, K0070, K0140, K0236, K0372, S0060, S0257, S0266

Writing Secure Code in Java Project

HANDS-ON TRAINING

Build your Java project, then mitigate the vulnerabilities by adding validation to the inputs. You will also implement spring security on an application.

Project Walkthrough and Hints

Video | 24 minutes

This video walks you through the project, explaining what needs to be done and offering some hints.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Spring Secure File

File | 1 file

The Spring Secure file you will need for part of the project.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Northwind

File | 1 file

The Northwind file you will need to complete part of the project.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Writing Secure Code in PHP Project

HANDS-ON TRAINING

Use your secure PHP coding skills to uncover issues in a simple application. Your challenge is to go through the code and find cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, insecure secrets, lack of input sanitation/validation and lack of proper error handling.

Writing Secure Code in PHP Project Walkthrough

Video | 5 minutes

This video walks you through the project, explaining what needs to be done in each of the challenges.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Writing Secure Code in PHP Project Files

File | 1 file

This zip contains files you will need to complete the project.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Writing Secure Code in PHP Project Hints

File | 5 minutes

This video provides useful hints to help you solve the project challenges.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

Writing Secure Code in PHP Project Solutions

File | 1 file

This document contains solutions to the project challenges.

NICE Knowledge and Skill Statements:

S0060, S0172, S0239, S0266

x86 Disassembly Project

HANDS-ON TRAINING

Practice your x86 skills by using tools like NASM, Makefiles, objdump, gdp and more to complete three projects. You'll create the quintessential Hello World program, debug an x86 program and tie everything together with a project that leverages input, output and logic flows.

x86 Project VM

File | 1 file

Use this virtual machine (VM) to complete the three labs in the Introduction to x86 Disassembly Learning Path.

LAB: Hello World! Creating the Usual Hello World in x86

Video | 20 minutes

This project will guide you through building an application written entirely in x86 Assembly.

LAB: x86 Debugging: Lab to Debug an x86 Program

Video | 7 minutes

This project will guide you through debugging at the x86 level, plus techniques for locating and fixing bugs.

LAB: x86 Program with Input, Output and Logic Flows

Video | 15 minutes

This project will tie together all of the x86 concepts learned so far into a lab that leverages i/o, strings, conditional codes and logic structures.

Training mapped to the NICE Workforce Framework for Cybersecurity

Infosec Skills connects employee job descriptions to an established workforce development framework. Your organization can take a bottoms-up approach to any training initiative by mapping development plans to specific NICE knowledge and skills, work roles or even the competencies deemed most critical to employee success.

How Infosec Skills content is mapped to the framework

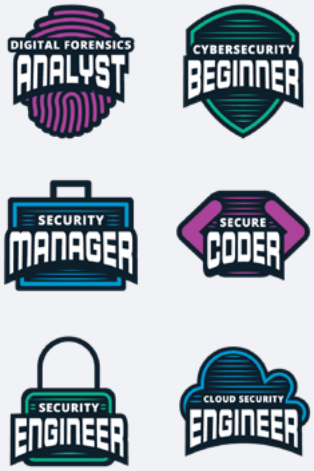
Every Infosec Skills course, cyber range or project is audited and mapped to relevant NICE knowledge and skill statements. For example, some of the statements mapped to our “Common malware behavior” course include:

- K0259: Knowledge of malware analysis concepts and methodologies
- K0392: Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.)
- S0131: Skill in analyzing malware
- S0087: Skill in deep analysis of captured malicious code (e.g., malware forensics)

Not using the NICE Framework? Don’t worry — we’ve got you covered!

Infosec Skills Roles provide training recommendations for 12 of the most common cybersecurity positions, from beginner to advanced. Use these Roles to quickly build employee development plans and maximize training relevancy.

Explore Roles



Authorizing Official (SP-RSK-001)

Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations and the Nation (CNSSI 4009).

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0028, K0037, K0044, K0048, K0049, K0070, K0146, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0295, K0322, K0342, K0622, K0624	S0034
ISACA CRISC	K0002, K0003, K0004, K0005, K0013, K0019, K0048, K0054, K0059, K0070, K0101, K0168, K0169, K0199, K0260, K0261, K0262, K0267, K0342	
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0038, K0048, K0049, K0059, K0070, K0101, K0146, K0169, K0170, K0179, K0199, K0260, K0261, K0262, K0267, K0342, K0622, K0624	
ISACA CISA	K0002, K0003, K0004, K0005, K0019, K0027, K0044, K0101, K0146, K0261, K0262, K0267, K0322, K0622	S0034
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0013, K0048, K0070, K0084, K0101, K0146, K0169, K0260, K0261, K0262, K0267, K0342	
Other learning paths	K0040, K0089, K0126	S0367

Security Control Assessor (SP-RSK-002)

Conducts independent comprehensive assessments of the management, operational and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST 800-37).

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0010, K0013, K0018, K0019, K0021, K0024, K0026, K0028, K0037, K0044, K0048, K0049, K0056, K0070, K0146, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0287, K0322, K0342, K0622, K0624	S0034, S0236
ISACA CISA	K0002, K0003, K0004, K0005, K0007, K0010, K0018, K0019, K0021, K0026, K0027, K0044, K0056, K0101, K0146, K0261, K0262, K0267, K0287, K0322, K0622	S0027, S0034, S0147, S0171, S0273
ISC2 CGRC (previously - CAP)	K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0019, K0040, K0048, K0054, K0070, K0101, K0168, K0179, K0199, K0260, K0261, K0262, K0267, K0342	S0034, S0078, S0097, S0136, S0137, S0147
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0007, K0011, K0013, K0018, K0019, K0021, K0026, K0038, K0048, K0049, K0056, K0059, K0070, K0101, K0146, K0169, K0170, K0179, K0199, K0260, K0261, K0262, K0267, K0342, K0622, K0624	
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0013, K0021, K0026, K0048, K0070, K0084, K0101, K0146, K0169, K0260, K0261, K0262, K0267, K0342	S0001, S0038, S0171, S0175, S0242
Other learning paths	K0009, K0029, K0089, K0100, K0126	S0073, S0110, S0115, S0120, S0124, S0135, S0138, S0141, S0145, S0172, S0173, S0174, S0184, S0239, S0241, S0252, S0278, S0280, S0296, S0367, S0374

Software Developer (SP-DEV-001)

Develops, creates, maintains and writes/codes new (or modifies existing) computer applications, software or specialized utility programs.

Core path name	Knowledge statements	Skill statements
CertNexus Cyber Secure Coder	K0001, K0003, K0004, K0005, K0006, K0028, K0039, K0044, K0068, K0070, K0079, K0080, K0081, K0082, K0084, K0105, K0139, K0140, K0153, K0260, K0261, K0262, K0624	S0014, S0022, S0031, S0034, S0135, S0138, S0149, S0174, S0367
Certified Mobile and Web App Penetration Tester	K0004, K0060, K0070, K0105, K0140, K0342, K0624	S0001, S0022, S0174
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0028, K0039, K0044, K0050, K0070, K0073, K0081, K0082, K0153, K0170, K0179, K0199, K0260, K0261, K0262, K0322, K0332, K0342, K0624	S0031, S0034
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0070, K0081, K0084, K0154, K0260, K0261, K0262, K0263, K0342, K0343	S0001, S0175
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0028, K0039, K0044, K0070, K0073, K0079, K0081, K0082, K0084, K0086, K0153, K0154, K0170, K0179, K0199, K0624	
Other learning paths	K0016, K0027, K0051, K0066, K0202	S0019, S0060

Secure Software Assessor (SP-DEV-002)

Analyzes the security of new or existing computer applications, software or specialized utility programs and provides actionable results.

Core path name	Knowledge statements	Skill statements
Secure SDLC	K0005, K0028, K0039, K0044, K0153, K0178, K0263, K0624	S0174
CertNexus Cyber Secure Coder	K0001, K0003, K0004, K0005, K0006, K0028, K0039, K0044, K0068, K0070, K0079, K0080, K0081, K0082, K0084, K0105, K0139, K0140, K0153, K0178, K0260, K0261, K0262, K0624	S0022, S0031, S0034, S0135, S0138, S0174, S0367
CompTIA Security+	K0002, K0005, K0006, K0044, K0070, K0081, K0154, K0178, K0179, K0263, K0322, K0342, K0624	S0031, S0138
CompTIA CySA+	K0002, K0003, K0004, K0005, K0039, K0044, K0070, K0079, K0080, K0081, K0082, K0153, K0178, K0179, K0199, K0342, K0624	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0028, K0039, K0044, K0070, K0073, K0079, K0081, K0082, K0084, K0086, K0153, K0154, K0170, K0178, K0179, K0199, K0624	
Other learning paths	K0016, K0027, K0050, K0051, K0060, K0066, K0202, K0343	S0001, S0175

Enterprise Architect (SP-ARC-001)

Develops and maintains business, systems and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

Core path name	Knowledge statements	Skill statements
ISACA CISA	K0002, K0003, K0004, K0005, K0027, K0044, K0056, K0061, K0074, K0091, K0198, K0264, K0275, K0286, K0287, K0322	S0027
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0024, K0028, K0037, K0044, K0056, K0061, K0063, K0074, K0075, K0082, K0091, K0093, K0170, K0179, K0180, K0198, K0200, K0203, K0211, K0214, K0240, K0264, K0275, K0287, K0291, K0322, K0326, K0332, K0333, K0487, K0516	
ISC2 CISSP-ISSAP	K0001, K0002, K0004, K0005, K0006, K0024, K0027, K0056, K0061, K0075, K0082, K0093, K0170, K0203, K0291, K0299, K0332, K0333, K0516	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0028, K0035, K0044, K0074, K0075, K0082, K0091, K0102, K0170, K0179, K0180, K0198, K0203, K0211, K0214, K0240, K0264, K0287, K0291, K0299, K0323, K0333	S0027
Security Architecture	K0004, K0005, K0027, K0044, K0075, K0170, K0179, K0211, K0287, K0291, K0293	S0122, S0367
Other learning paths	K0030, K0043, K0060, K0227	S0005, S0060, S0374

Security Architect (SP-ARC-002)

Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.

Core path name	Knowledge statements	Skill statements
ISACA CISA	K0002, K0003, K0004, K0005, K0007, K0010, K0018, K0019, K0026, K0027, K0044, K0056, K0061, K0074, K0091, K0198, K0261, K0262, K0264, K0275, K0286, K0287, K0322	S0027
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0010, K0013, K0018, K0019, K0024, K0026, K0037, K0044, K0056, K0057, K0061, K0063, K0071, K0074, K0082, K0091, K0093, K0170, K0180, K0198, K0200, K0211, K0214, K0240, K0260, K0261, K0262, K0264, K0275, K0287, K0291, K0320, K0322, K0326, K0332, K0333, K0336, K0565	
ISC2 CISSP-ISSAP	K0001, K0002, K0004, K0005, K0006, K0007, K0009, K0018, K0019, K0024, K0026, K0027, K0056, K0057, K0061, K0071, K0082, K0093, K0170, K0202, K0260, K0261, K0262, K0291, K0332, K0333, K0336, K0565	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0013, K0026, K0035, K0044, K0074, K0082, K0091, K0102, K0170, K0180, K0198, K0211, K0214, K0240, K0264, K0287, K0291, K0323, K0333	S0027, S0076
Security Architecture	K0004, K0005, K0027, K0044, K0170, K0211, K0287, K0291, K0293	S0022, S0122, S0367
Other learning paths	K0011, K0015, K0030, K0036, K0043, K0059, K0060, K0092, K0227, K0277	S0005, S0059, S0061, S0138, S0152, S0168, S0170, S0374

Research and Development Specialist (SP-TRD-001)

Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

Core path name	Knowledge statements	Skill statements
ISACA CISA	K0002, K0003, K0004, K0005, K0007, K0010, K0018, K0019, K0026, K0027, K0044, K0056, K0061, K0074, K0091, K0198, K0261, K0262, K0264, K0275, K0286, K0287, K0322	S0027
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0010, K0013, K0018, K0019, K0024, K0026, K0037, K0044, K0056, K0057, K0061, K0063, K0071, K0074, K0082, K0091, K0093, K0170, K0180, K0198, K0200, K0211, K0214, K0240, K0260, K0261, K0262, K0264, K0275, K0287, K0291, K0320, K0322, K0326, K0332, K0333, K0336, K0565	
ISC2 CISSP-ISSAP	K0001, K0002, K0004, K0005, K0006, K0007, K0009, K0018, K0019, K0024, K0026, K0027, K0056, K0057, K0061, K0071, K0082, K0093, K0170, K0202, K0260, K0261, K0262, K0291, K0332, K0333, K0336, K0565	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0013, K0026, K0035, K0044, K0074, K0082, K0091, K0102, K0170, K0180, K0198, K0211, K0214, K0240, K0264, K0287, K0291, K0323, K0333	S0027, S0076
Security Architecture	K0004, K0005, K0027, K0044, K0170, K0211, K0287, K0291, K0293	S0022, S0122, S0367
Other learning paths	K0011, K0015, K0030, K0036, K0043, K0059, K0060, K0092, K0227, K0277	S0005, S0059, S0061, S0138, S0152, S0168, S0170, S0374

Systems Requirements Planner (SP-SRP-001)

Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0019, K0032, K0044, K0047, K0056, K0061, K0063, K0073, K0074, K0090, K0091, K0093, K0169, K0170, K0180, K0200, K0287, K0332, K0333, K0622	
ISACA CISA	K0002, K0003, K0004, K0005, K0018, K0019, K0032, K0044, K0047, K0056, K0061, K0074, K0090, K0091, K0101, K0267, K0287, K0622	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0032, K0035, K0044, K0047, K0073, K0074, K0086, K0087, K0090, K0091, K0102, K0164, K0169, K0170, K0180, K0267, K0287, K0333	
ISACA CRISC	K0002, K0003, K0004, K0005, K0018, K0019, K0059, K0066, K0073, K0101, K0168, K0169, K0267	
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0018, K0019, K0035, K0038, K0056, K0059, K0087, K0101, K0169, K0170, K0267, K0332, K0622	
Other learning paths	K0043, K0060, K0126	S0005, S0367

System Test & Evaluation Specialist (SP-TST-001)

Plans, prepares and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0028, K0037, K0044, K0057, K0091, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0287, K0332	
ISC2 CISSP-ISSAP	K0001, K0002, K0004, K0005, K0006, K0027, K0057, K0170, K0199, K0203, K0260, K0261, K0262, K0332	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0028, K0044, K0091, K0102, K0169, K0170, K0179, K0199, K0203, K0287	S0110
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0169, K0170, K0179, K0199, K0260, K0261, K0262, K0332	
Incident Response	K0003, K0004, K0005, K0287	
Other learning paths	K0088, K0126, K0139	S0060, S0061, S0367

Information Systems Security Developer (SP-SYS-001)

Designs, develops, tests and evaluates information system security throughout the systems development life cycle.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0024, K0028, K0032, K0044, K0049, K0050, K0056, K0061, K0063, K0065, K0073, K0081, K0082, K0090, K0091, K0093, K0169, K0170, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0276, K0287, K0308, K0322, K0332, K0333, K0336	S0023, S0031, S0034
ISC2 CISSP-ISSAP	K0001, K0002, K0004, K0005, K0006, K0018, K0024, K0027, K0050, K0056, K0061, K0065, K0081, K0082, K0093, K0170, K0203, K0260, K0261, K0262, K0308, K0332, K0333, K0336	S0031, S0145
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0028, K0032, K0035, K0044, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0102, K0169, K0170, K0179, K0180, K0203, K0276, K0287, K0333	S0023, S0036
ISACA CISA	K0002, K0003, K0004, K0005, K0018, K0027, K0032, K0044, K0056, K0061, K0065, K0081, K0090, K0091, K0261, K0262, K0287, K0322	S0034, S0085
CompTIA A+	K0001, K0030, K0032, K0035, K0036, K0050, K0060, K0061, K0260, K0261, K0262, K0332	
Other learning paths	K0015, K0066, K0126, K0139, K0297	S0001, S0022, S0367

Systems Developer (SP-SYS-002)

Designs, develops, tests and evaluates information systems throughout the systems development life cycle.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0024, K0028, K0032, K0044, K0049, K0050, K0056, K0061, K0063, K0065, K0073, K0081, K0082, K0090, K0091, K0093, K0169, K0170, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0276, K0287, K0308, K0322, K0332, K0333, K0336	S0023, S0031, S0034
ISC2 CISSP-ISSAP	K0001, K0002, K0004, K0005, K0006, K0018, K0024, K0027, K0050, K0056, K0061, K0065, K0081, K0082, K0093, K0170, K0203, K0260, K0261, K0262, K0308, K0332, K0333, K0336	S0031, S0145
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0028, K0032, K0035, K0044, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0102, K0169, K0170, K0179, K0180, K0203, K0276, K0287, K0333	S0023, S0036
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0018, K0035, K0049, K0056, K0065, K0081, K0087, K0169, K0170, K0179, K0260, K0261, K0262, K0308, K0332	
Security Architecture	K0004, K0005, K0027, K0044, K0170, K0179, K0287, K0297	S0022, S0023, S0036, S0367
Other learning paths	K0015, K0030, K0036, K0060, K0066, K0126, K0139, K0227	S0025, S0060, S0085, S0097, S0136, S0146

Database Administrator (OM-DTA-001)

Administers databases and/or data management systems that allow for the secure storage, query and utilization of data.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0022, K0023, K0056, K0065, K0069, K0083, K0260, K0261, K0262, K0287	
ISC2 CISSP-ISSAP	K0001, K0002, K0004, K0005, K0006, K0021, K0056, K0065, K0260, K0261, K0262	
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0021, K0025, K0056, K0065, K0097, K0260, K0261, K0262, K0277	
ISC2 CCSP	K0002, K0003, K0004, K0005, K0006, K0021, K0025, K0065, K0097, K0277, K0287	
Linux Fundamentals	K0001, K0021, K0056, K0060, K0065, K0069	S0002
Other learning paths	K0420	

Data Analyst (OM-DTA-002)

Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining and research purposes.

Core path name	Knowledge statements	Skill statements
CompTIA IT Fundamentals (ITF+)	K0004, K0016, K0060, K0068, K0229, K0420	S0060
Cybersecurity Data Science	K0238	S0089
Information Security Fundamentals	K0001, K0002, K0005, K0006, K0056, K0060, K0065, K0129	
Linux Fundamentals	K0001, K0056, K0060, K0065, K0069, K0129, K0229, K0236	S0130
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0022, K0023, K0056, K0065, K0069, K0083, K0095	
Other learning paths	K0015, K0025, K0051, K0139, K0140	S0094, S0095

Knowledge Manager (OM-KMG-001)

Responsible for the management and administration of processes and tools that enable the organization to identify, document and access intellectual capital and information content.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0095, K0146, K0195, K0260, K0261, K0262, K0287	
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0013, K0146, K0194, K0260, K0261, K0262	
Cybersecurity Management	K0002, K0003, K0004, K0005, K0006, K0013, K0146, K0194, K0195, K0260, K0261, K0262, K0287	
Enterprise Security Risk Management	K0002, K0003, K0004, K0005, K0006, K0013, K0146, K0194, K0195, K0260, K0261, K0262, K0287	
ISC2 CGRC (previously - CAP)	K0002, K0003, K0004, K0005, K0006, K0013, K0260, K0261, K0262	
Other learning paths	K0283, K0315, K0420	

Technical Support Specialist (OM-STS-001)

Provides technical support to customers who need assistance utilizing client level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable).

Core path name	Knowledge statements	Skill statements
CompTIA A+	K0001, K0088, K0109, K0114, K0116, K0224, K0260, K0261, K0262, K0302	S0142
CompTIA Network+	K0001, K0002, K0004, K0109, K0194, K0260, K0261, K0262	S0142
Linux Fundamentals	K0001, K0114, K0116, K0247, K0294	S0142
CompTIA Security+	K0002, K0005, K0006, K0109	
CompTIA CySA+	K0002, K0003, K0004, K0005, K0242, K0292, K0317	
Other learning paths	K0053, K0287	S0365

Network Operations Specialist (OM-NET-001)

Plans, implements and operates network services/systems, to include hardware and virtual environments.

Core path name	Knowledge statements	Skill statements
CompTIA Network+	K0001, K0002, K0004, K0011, K0038, K0049, K0061, K0071, K0104, K0108, K0111, K0113, K0137, K0159, K0179, K0180, K0260, K0261, K0262, K0274, K0332	S0041, S0162
CompTIA Security+	K0002, K0005, K0006, K0011, K0049, K0104, K0108, K0160, K0179, K0201	
JNCIA-Junos	K0001, K0004, K0005, K0011, K0049, K0061	S0041, S0084, S0170
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0010, K0049, K0050, K0061, K0071, K0093, K0104, K0113, K0136, K0138, K0159, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0274, K0287, K0332, K0622	
CCNA	K0001, K0004, K0011, K0049, K0061, K0071, K0108, K0111, K0113, K0332	S0004, S0041, S0077
Other learning paths	K0029, K0053, K0135	S0079

System Administrator (OM-ADM-001)

Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).

Core path name	Knowledge statements	Skill statements
CompTIA A+	K0001, K0050, K0088, K0104, K0117, K0130, K0158, K0260, K0261, K0262, K0274, K0318, K0332	S0073, S0076, S0151
Linux Fundamentals	K0001, K0049, K0100, K0117, K0318, K0332	S0076, S0143, S0151, S0158
CompTIA Network+	K0001, K0002, K0004, K0049, K0104, K0130, K0167, K0179, K0260, K0261, K0262, K0274, K0332	S0151
CompTIA Security+	K0002, K0005, K0006, K0049, K0104, K0130, K0158, K0167, K0179, K0318	S0158
ISC2 CGRC (previously - CAP)	K0002, K0003, K0004, K0005, K0006, K0053, K0064, K0179, K0260, K0261, K0262	S0153, S0155
Other learning paths	K0077	S0033, S0043

Systems Security Analyst (OM-ANA-001)

Responsible for the analysis and development of the integration, testing, operations and maintenance of systems security.

Core path name	Knowledge statements	Skill statements
CompTIA A+	K0001, K0035, K0036, K0060, K0061, K0260, K0261, K0262	
CompTIA CySA+	K0002, K0003, K0004, K0005, K0040, K0044, K0049, K0056, K0082, K0179, K0333, K0339	S0167
ISACA CISA	K0002, K0003, K0004, K0005, K0018, K0019, K0044, K0056, K0061, K0261, K0262, K0263, K0267, K0275, K0287, K0290, K0322	S0027, S0147
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0019, K0024, K0044, K0049, K0056, K0061, K0063, K0075, K0082, K0093, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0275, K0276, K0285, K0287, K0322, K0333	S0031
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0035, K0040, K0044, K0075, K0082, K0102, K0179, K0180, K0203, K0267, K0276, K0287, K0333, K0339	S0027, S0036
Other learning paths	K0015, K0227, K0266, K0297	S0060, S0141, S0367

Cyber Legal Advisor (OV-LGA-001)

Provides legal advice and recommendations on relevant topics related to cyber law.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0146, K0165, K0169	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0048, K0154, K0165, K0169, K0257, K0270	
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0048, K0072, K0146, K0154, K0165, K0169	
ISACA CRISC	K0002, K0003, K0004, K0005, K0048, K0072, K0165, K0169	
PMI Project Management Professional (PMP)	K0002, K0072, K0270	
Other learning paths	K0126	S0372

Privacy Officer/Privacy Compliance Manager (OV-LGA-002)

Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy and incident response needs of privacy and security executives and their teams.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0612, K0615	
ISACA CRISC	K0002, K0003, K0004, K0005, K0066, K0168, K0615	
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0615	S0356
ISC2 CGRC (previously - CAP)	K0002, K0003, K0004, K0005, K0006, K0168, K0612	
Threat Modeling	K0002, K0004, K0005, K0612	
Other learning paths	K0614	S0354

Cyber Instructional Curriculum Developer (OV-TEA-001)

Develops, plans, coordinates and evaluates cyber training/education courses, methods and techniques based on instructional needs.

Core path name	Knowledge statements	Skill statements
Training and Awareness Basics	K0003, K0004, K0005, K0146, K0243, K0245, K0252	
ISACA CRISC	K0002, K0003, K0004, K0005, K0059, K0147	
Enterprise Security Risk Management	K0002, K0003, K0004, K0005, K0006, K0059, K0146, K0147, K0243, K0287	S0070
Cybersecurity Management	K0002, K0003, K0004, K0005, K0006, K0146, K0243, K0287	
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0146, K0243, K0287	
Other learning paths		S0296

Cyber Instructor (OV-TEA-002)

Develops and conducts training or education of personnel within cyber domain.

Core path name	Knowledge statements	Skill statements
Training and Awareness Basics	K0003, K0004, K0005, K0007, K0146, K0245, K0252, K0313	
ISACA CRISC	K0002, K0003, K0004, K0005, K0007, K0059, K0147	S0070
EC-Council CEH	K0002, K0115, K0147	S0001, S0051, S0052, S0081, S0156, S0293
Web Server Protection	K0005, K0006	S0051, S0084, S0121
CompTIA Security+	K0002, K0005, K0006, K0007, K0130, K0147	S0081
Other learning paths	K0001, K0215, K0287	S0004, S0057, S0060, S0073, S0075, S0076, S0097, S0131, S0184, S0270, S0356, S0358

Information Systems Security Manager (OV-MGT-001)

Responsible for the cybersecurity of a program, organization, system or enclave.

Core path name	Knowledge statements	Skill statements
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0026, K0033, K0038, K0042, K0048, K0059, K0070, K0087, K0092, K0101, K0106, K0150, K0151, K0167, K0169, K0170, K0179, K0199, K0260, K0261, K0262, K0267, K0332, K0342, K0622, K0624	
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0026, K0033, K0042, K0048, K0061, K0070, K0077, K0090, K0150, K0167, K0169, K0170, K0179, K0180, K0199, K0260, K0261, K0262, K0287, K0332, K0342, K0622, K0624	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0026, K0040, K0042, K0048, K0070, K0087, K0090, K0106, K0150, K0167, K0169, K0170, K0179, K0180, K0199, K0267, K0287, K0624	S0027
ISACA CISM	K0002, K0006, K0021, K0026, K0042, K0054, K0072, K0087, K0090, K0101, K0121, K0149, K0150, K0199, K0267, K0287, K0622	
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0021, K0026, K0042, K0046, K0048, K0070, K0072, K0101, K0121, K0149, K0150, K0169, K0260, K0261, K0262, K0267, K0342	
Other learning paths	K0043, K0053, K0058, K0126, K0168	

Communications Security (COMSEC) Manager (OV-MGT-002)

Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).

Core path name	Knowledge statements	Skill statements
ISACA CISA	K0002, K0003, K0004, K0005, K0018, K0026, K0042, K0090, K0101, K0121, K0267, K0287, K0622	S0027
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0026, K0042, K0090, K0285, K0287, K0622	
Security Engineering	K0001, K0002, K0004, K0005, K0006, K0026, K0038, K0042, K0090, K0267, K0287, K0622	S0027
Introduction to Applied Cryptography and Cryptanalysis	K0004, K0005, K0018, K0038, K0622	S0059
CompTIA Security+	K0002, K0005, K0006, K0018, K0026, K0042	S0138
Other learning paths	K0126	

Cyber Workforce Developer and Manager (OV-SPP-001)

Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0146, K0169, K0215, K0243	
Cybersecurity Audit Fundamentals	K0004, K0005, K0006, K0127, K0233	
Training and Awareness Basics	K0003, K0004, K0005, K0146, K0243, K0313	
EC-Council CEH	K0002, K0147, K0309	
ISACA CRISC	K0002, K0003, K0004, K0005, K0072, K0101, K0147, K0168, K0169, K0335	
Other learning paths	K0234	

Cyber Policy and Strategy Planner (OV-SPP-002)

Develops and maintains cybersecurity plans, strategy and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0146, K0624	
EC-Council CEH	K0002, K0070, K0309, K0624	
CompTIA PenTest+	K0003, K0004, K0005, K0070, K0234, K0624	
Cybersecurity Audit Fundamentals	K0004, K0005, K0006, K0070, K0127, K0624	
ISACA CRISC	K0002, K0003, K0004, K0005, K0070, K0168, K0335	
Other learning paths	K0313	

Executive Cyber Leadership (OV-EXL-001)

Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

Core path name	Knowledge statements	Skill statements
CompTIA PenTest+	K0003, K0004, K0005, K0009, K0070, K0106, K0147, K0314, K0624	
Security Engineering	K0001, K0002, K0004, K0005, K0006, K0070, K0106, K0147, K0296, K0624	S0358
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0624	
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0070, K0296	S0356
ISC2 CISSP-ISSAP	K0001, K0002, K0004, K0005, K0006, K0009, K0070, K0624	
Other learning paths		

Program Manager (OV-PMA-001)

Leads, coordinates, communicates, integrates and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0090, K0146, K0165, K0169, K0196, K0198, K0200	
Cybersecurity Management	K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0146, K0148, K0154, K0165, K0169, K0194, K0198, K0200, K0270	
NIST Cybersecurity Framework	K0002, K0004, K0048, K0165	S0372
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0047, K0048, K0090, K0154, K0164, K0165, K0169, K0198, K0257, K0270	
Enterprise Security Risk Management	K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0146, K0148, K0154, K0165, K0169, K0194, K0196, K0270	S0038
Other learning paths	K0126	

Information Technology (IT) Project Manager (OV-PMA-002)

Directly manages information technology .

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0090, K0146, K0165, K0169, K0196, K0198, K0200	
ISACA CRISC	K0002, K0003, K0004, K0005, K0048, K0059, K0072, K0101, K0165, K0169	S0038
Enterprise Security Risk Management	K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0059, K0072, K0090, K0101, K0146, K0148, K0154, K0165, K0169, K0194, K0196, K0270	S0038
NIST Cybersecurity Framework	K0002, K0004, K0048, K0165	S0372
ISACA CISA	K0002, K0003, K0004, K0005, K0047, K0090, K0101, K0146, K0154, K0198, K0257, K0270	
Other learning paths	K0043, K0126, K0164	

Product Support Manager (OV-PMA-003)

Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0090, K0150, K0165, K0169, K0196, K0198, K0200	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0048, K0090, K0150, K0154, K0164, K0165, K0169, K0198, K0257, K0270	
PMI Project Management Professional (PMP)	K0002, K0072, K0249, K0270	
Enterprise Security Risk Management	K0002, K0003, K0004, K0005, K0006, K0048, K0059, K0072, K0090, K0148, K0154, K0165, K0169, K0194, K0196, K0270	S0038
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0048, K0072, K0150, K0154, K0165, K0169, K0196, K0198	S0038
Other learning paths	K0043, K0126	S0372

IT Investment/Portfolio Manager (OV-PMA-004)

Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0146, K0165, K0169	
ISC2 CISSP-ISSEP	K0002, K0004, K0005, K0006, K0048, K0154, K0165, K0169, K0257, K0270	
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0048, K0072, K0146, K0154, K0165, K0169	
ISACA CRISC	K0002, K0003, K0004, K0005, K0048, K0072, K0165, K0169	
PMI Project Management Professional (PMP)	K0002, K0072, K0270	
Other learning paths	K0126	S0372

IT Program Auditor (OV-PMA-005)

Conducts evaluations of an IT program or its individual components, to determine compliance with published standards.

Core path name	Knowledge statements	Skill statements
Cybersecurity Audit Fundamentals	K0004, K0005, K0006, K0043, K0126, K0200, K0270	S0085
ISC2 CGRC (previously - CAP)	K0002, K0003, K0004, K0005, K0006, K0048, K0165	
ISC2 CISSP-ISSMP	K0002, K0003, K0004, K0048, K0072, K0154, K0165, K0169, K0198	S0038
Cybersecurity Administration	K0001, K0002, K0004, K0005, K0006, K0048, K0148, K0165, K0169	
ISACA CISA	K0002, K0003, K0004, K0005, K0047, K0090, K0154, K0198, K0257, K0270	S0085
Other learning paths		S0372

Cyber Defense Analyst (PR-CDA-001)

Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Core path name	Knowledge statements	Skill statements
CompTIA CySA+	K0002, K0003, K0004, K0005, K0007, K0013, K0033, K0040, K0042, K0044, K0049, K0056, K0065, K0070, K0106, K0112, K0161, K0162, K0167, K0177, K0179, K0191, K0192, K0301, K0339, K0342, K0624	S0167
Cisco Certified CyberOps Associate	K0001, K0042, K0046, K0058, K0061, K0070, K0106, K0143, K0160, K0190, K0191, K0221, K0222, K0301, K0324, K0332, K0342	
EC-Council CEH	K0002, K0013, K0018, K0019, K0061, K0070, K0106, K0160, K0161, K0177, K0191, K0192, K0261, K0297, K0300, K0301, K0324, K0332, K0339, K0624	S0025, S0078, S0156, S0167
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0007, K0018, K0019, K0042, K0056, K0060, K0061, K0065, K0070, K0093, K0106, K0111, K0113, K0160, K0161, K0162, K0177, K0179, K0180, K0192, K0221, K0301, K0318, K0324, K0332	S0156
Security Engineering	K0001, K0002, K0004, K0005, K0006, K0007, K0013, K0033, K0040, K0042, K0044, K0049, K0065, K0070, K0074, K0075, K0104, K0106, K0112, K0113, K0157, K0167, K0179, K0180, K0190, K0203, K0322, K0324, K0339, K0624	S0027, S0036, S0078
Other learning paths	K0015, K0024, K0059, K0107, K0110, K0116, K0139, K0168, K0260, K0262, K0290, K0303	S0054, S0057, S0147, S0367

Cyber Defense Infrastructure Support Specialist (PR-INF-001)

Tests, implements, deploys, maintains and administers the infrastructure hardware and software.

Core path name	Knowledge statements	Skill statements
CompTIA Security+	K0002, K0005, K0006, K0021, K0033, K0042, K0044, K0104, K0106, K0179, K0205, K0324	
NIST DoD RMF	K0002, K0003, K0004, K0157	
CCNA	K0001, K0004, K0033, K0061, K0324, K0332, K0334	S0007, S0077
CompTIA IT Fundamentals (ITF+)	K0004, K0021	S0121, S0124
CompTIA Network+	K0001, K0002, K0004, K0021, K0033, K0044, K0061, K0062, K0104, K0179, K0205, K0274, K0324, K0332	
Other learning paths	K0058, K0135, K0258	S0054, S0059, S0079, S0367

Cyber Defense Incident Responder (PR-CIR-001)

Investigates, analyzes and responds to cyber incidents within the network environment or enclave.

Core path name	Knowledge statements	Skill statements
CompTIA Security+	K0002, K0005, K0006, K0021, K0026, K0033, K0041, K0042, K0046, K0070, K0106, K0167, K0177, K0179, K0221, K0230, K0624	
Incident Response	K0003, K0004, K0005, K0026, K0041, K0042, K0046, K0058, K0062, K0106, K0162, K0287	S0003
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0034, K0042, K0070, K0106, K0161, K0162, K0177, K0179, K0221, K0332, K0565	S0173, S0365
EC-Council CEH	K0002, K0070, K0106, K0161, K0177, K0259, K0332, K0565, K0624	S0078
Certified Computer Forensics Examiner (CCFE)	K0001	S0047
Other learning paths	K0157	S0077, S0079, S0080

Vulnerability Assessment Analyst (PR-VAM-001)

Performs assessments of systems and networks within the NE or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Core path name	Knowledge statements	Skill statements
CompTIA Security+	K0002, K0005, K0006, K0019, K0021, K0033, K0044, K0056, K0070, K0106, K0167, K0177, K0179, K0210, K0301, K0308, K0342, K0624	S0081
Vulnerability Assessment	K0002, K0005, K0006, K0033, K0344	S0001, S0137
CompTIA PenTest+	K0003, K0004, K0005, K0009, K0068, K0070, K0106, K0177, K0206, K0301, K0342, K0624	S0001, S0051, S0052, S0081
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0019, K0021, K0033, K0044, K0056, K0061, K0070, K0162, K0167, K0177, K0179, K0203, K0210, K0265, K0287, K0308, K0332, K0342, K0624	
EC-Council CEH	K0002, K0009, K0019, K0061, K0070, K0106, K0161, K0177, K0301, K0308, K0332, K0344, K0624	S0001, S0025, S0051, S0052, S0081, S0137
Other learning paths	K0089, K0139, K0224	S0044, S0120, S0171, S0364, S0367

Threat/Warning Analyst (AN-TWA-001)

Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes and disseminates cyber threat/warning assessments.

Core path name	Knowledge statements	Skill statements
CompTIA Network+	K0001, K0002, K0004, K0108, K0109, K0177, K0362, K0395, K0417, K0427, K0437, K0446, K0471, K0480, K0516, K0560, K0565, K0604, K0610, K0612, K0614	
Threat Modeling	K0002, K0004, K0005, K0177, K0405, K0440, K0604, K0612	S0218, S0229
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0108, K0177, K0362, K0395, K0427, K0436, K0444, K0445, K0446, K0449, K0471, K0480, K0516, K0556, K0560, K0565, K0603, K0604, K0614	
EC-Council CEH	K0004, K0058, K0108, K0177, K0362, K0409, K0446, K0471, K0480, K0565, K0604	
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0362, K0377, K0392, K0395, K0417, K0427, K0437, K0471, K0480, K0511, K0516, K0561, K0565, K0610, K0612	
Other learning paths	K0036, K0349, K0431, K0460, K0469	S0228, S0278, S0296

Exploitation Analyst (AN-EXP-001)

Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0362, K0417, K0470, K0471, K0487, K0489	S0236
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0108, K0177, K0362, K0444, K0447, K0471, K0489, K0560	S0199, S0258
Linux Fundamentals	K0001, K0349, K0397, K0444, K0471, K0487, K0529, K0608	
Network Traffic Analysis Cyber Range	K0004, K0005, K0143, K0177, K0362, K0471	S0199, S0258, S0269
CompTIA Security+	K0002, K0005, K0006, K0108, K0109, K0177, K0362, K0376, K0379, K0397, K0451	S0294
Other learning paths	K0131, K0224, K0351, K0354, K0371, K0393, K0394, K0430, K0523, K0535, K0544, K0559	S0184, S0207, S0239

All-Source Analyst (AN-ASA-001)

Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Core path name	Knowledge statements	Skill statements
CompTIA Security+	K0002, K0005, K0006, K0108, K0109, K0177, K0221, K0362, K0427, K0480, K0561, K0603, K0610	
ISACA CISA	K0002, K0003, K0004, K0005, K0108, K0109, K0221, K0427, K0556, K0560, K0561, K0598, K0603	
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0108, K0177, K0221, K0362, K0395, K0427, K0436, K0444, K0445, K0446, K0449, K0471, K0480, K0516, K0556, K0560, K0565, K0603, K0604, K0614	
Threat Modeling	K0002, K0004, K0005, K0177, K0405, K0440, K0604, K0612	S0218, S0229
CompTIA Network+	K0001, K0002, K0004, K0108, K0109, K0177, K0221, K0362, K0395, K0427, K0437, K0446, K0471, K0480, K0516, K0560, K0565, K0604, K0610, K0612, K0614	
Other learning paths	K0036, K0058, K0349, K0377, K0392, K0409, K0410, K0431, K0460, K0469, K0511	S0278

Mission Assessment Specialist (AN-ASA-002)

Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0362, K0377, K0392, K0395, K0410, K0417, K0427, K0437, K0471, K0480, K0511, K0516, K0561, K0565, K0610, K0612	
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0108, K0177, K0362, K0395, K0427, K0436, K0444, K0445, K0446, K0449, K0471, K0480, K0516, K0556, K0560, K0565, K0603, K0604, K0614	
Threat Modeling	K0002, K0004, K0005, K0177, K0405, K0440, K0604, K0612	S0218, S0229
Linux Fundamentals	K0001, K0036, K0349, K0444, K0471, K0516, K0561, K0565	
CompTIA Network+	K0001, K0002, K0004, K0108, K0109, K0177, K0362, K0395, K0417, K0427, K0437, K0446, K0471, K0480, K0516, K0560, K0565, K0604, K0610, K0612, K0614	
Other learning paths	K0058, K0409, K0431, K0460, K0469, K0598	S0228, S0278, S0296

Target Developer (AN-TGT-001)

Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Core path name	Knowledge statements	Skill statements
Cisco Certified CyberOps Associate	K0001, K0058, K0362, K0402, K0440, K0516, K0565, K0603	
CompTIA PenTest+	K0003, K0004, K0005, K0177, K0362, K0392, K0409, K0437, K0565	S0278
ITIL 4 Foundation	K0004	S0296
CompTIA Security+	K0002, K0005, K0006, K0108, K0109, K0177, K0362, K0379, K0427, K0561, K0603	
CompTIA CySA+	K0002, K0003, K0004, K0005, K0177, K0362, K0381, K0409, K0460, K0561, K0565, K0603, K0604	
Other learning paths	K0036, K0349, K0351, K0395, K0417, K0431, K0436, K0444, K0445, K0446, K0449, K0471, K0479, K0543, K0555, K0556, K0560, K0598, K0614	S0218, S0228, S0229

Target Network Analyst (AN-TGT-002)

Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0362, K0392, K0395, K0403, K0471, K0487, K0516	
EC-Council CEH	K0002, K0177, K0362, K0392, K0479, K0544	S0291
CompTIA A+	K0001, K0108, K0109, K0349, K0392, K0395, K0440, K0444, K0471, K0516, K0600	
CompTIA CySA+	K0002, K0003, K0004, K0005, K0177, K0362, K0487, K0567	
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0108, K0177, K0362, K0395, K0436, K0444, K0445, K0449, K0471, K0516	
Other learning paths	K0379, K0424, K0431, K0472, K0559, K0599	S0219, S0228, S0229, S0261, S0268, S0280

Multi-Disciplined Language Analyst (AN-LNG-001)

Applies language and culture expertise with target/threat and technical knowledge to process, analyze and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign languageintensive or interdisciplinary .

Core path name	Knowledge statements	Skill statements
CompTIA Security+	K0002, K0005, K0006, K0108, K0177, K0488, K0548, K0600	S0241
CompTIA CySA+	K0002, K0003, K0004, K0005, K0177, K0487, K0488, K0548, K0567	
CompTIA A+	K0001, K0108, K0417, K0491, K0600	
Cisco Certified CyberOps Associate	K0001, K0143, K0493	S0184
Cybersecurity Data Science	K0177, K0476, K0493	
Other learning paths	K0377, K0396, K0398, K0431, K0449, K0524, K0579, K0599	S0218

All Source-Collection Manager (CO-CLO-001)

Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Core path name	Knowledge statements	Skill statements
CompTIA Security+	K0002, K0005, K0006, K0109, K0177, K0427, K0474, K0480, K0527, K0561, K0610	
CompTIA A+	K0001, K0036, K0109, K0392, K0395, K0412, K0417, K0440, K0444, K0446, K0471, K0480, K0516, K0610, K0612	
ISACA CISA	K0002, K0003, K0004, K0005, K0109, K0361, K0417, K0419, K0427, K0474, K0503, K0560, K0561	
CompTIA Network+	K0001, K0002, K0004, K0109, K0177, K0395, K0417, K0427, K0446, K0471, K0474, K0475, K0480, K0516, K0560, K0565, K0610, K0612	
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0392, K0395, K0417, K0419, K0427, K0471, K0480, K0516, K0527, K0561, K0565, K0579, K0610, K0612	
Other learning paths	K0058, K0353, K0364, K0405, K0425, K0431, K0435, K0445, K0449, K0477, K0496, K0584	

All Source-Collection Requirements Manager (CO-CLO-002)

Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0395, K0417, K0419, K0427, K0480, K0516, K0527, K0561, K0565, K0579, K0610, K0612	
CompTIA Network+	K0001, K0002, K0004, K0109, K0177, K0395, K0417, K0427, K0446, K0474, K0475, K0480, K0516, K0560, K0565, K0610, K0612	
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0109, K0177, K0427, K0431, K0445, K0446, K0527, K0561, K0565, K0610	
Cybersecurity Administration	K0001, K0002, K0004, K0005, K0006, K0177, K0395, K0417, K0427, K0445, K0446, K0516, K0527, K0561, K0565, K0610, K0612	
Security Engineering	K0001, K0002, K0004, K0005, K0006, K0109, K0395, K0417, K0419, K0427, K0475, K0480, K0527, K0561, K0568, K0584, K0610	
Other learning paths	K0036, K0058, K0353, K0361, K0364, K0412, K0425, K0435, K0444, K0477, K0496	

Cyber Intel Planner (CO-OPL-001)

Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0362, K0377, K0392, K0395, K0399, K0403, K0417, K0427, K0455, K0471, K0480, K0511, K0519, K0561, K0565, K0610, K0612	
Cybersecurity Administration	K0001, K0002, K0004, K0005, K0006, K0362, K0377, K0395, K0403, K0417, K0427, K0445, K0446, K0471, K0556, K0561, K0565, K0610, K0612	
CompTIA Network+	K0001, K0002, K0004, K0108, K0109, K0362, K0395, K0417, K0427, K0446, K0471, K0480, K0560, K0565, K0599, K0610, K0612, K0614	
CompTIA CySA+	K0002, K0003, K0004, K0005, K0362, K0432, K0460, K0504, K0561, K0565, K0603, K0612	
ISACA CISA	K0002, K0003, K0004, K0005, K0108, K0109, K0417, K0427, K0432, K0501, K0504, K0556, K0560, K0561, K0589, K0598, K0603	S0273
Other learning paths	K0036, K0349, K0379, K0405, K0408, K0411, K0431, K0435, K0436, K0440, K0444, K0506, K0512, K0518, K0586	S0186, S0218, S0278, S0296

Cyber Ops Planner (CO-OPL-002)

Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization and enables integration during the execution of cyber actions.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0362, K0377, K0392, K0395, K0399, K0403, K0417, K0455, K0471, K0480, K0511, K0516, K0519, K0561, K0565, K0610, K0612	
CompTIA Network+	K0001, K0002, K0004, K0108, K0109, K0362, K0395, K0417, K0446, K0471, K0480, K0516, K0560, K0565, K0599, K0610, K0612, K0614	
ISACA CISA	K0002, K0003, K0004, K0005, K0108, K0109, K0417, K0432, K0501, K0504, K0556, K0560, K0561, K0589, K0598, K0603	S0273
PMI Project Management Professional (PMP)	K0002, K0379, K0506, K0512	
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0108, K0362, K0395, K0399, K0436, K0444, K0445, K0446, K0471, K0480, K0516, K0556, K0560, K0565, K0603, K0614	
Other learning paths	K0036, K0349, K0408, K0411, K0431, K0435, K0518, K0586	S0186, S0218, S0296

Partner Integration Planner (CO-OPL-003)

Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0109, K0362, K0377, K0392, K0395, K0403, K0417, K0455, K0511	
CompTIA Network+	K0001, K0002, K0004, K0108, K0109, K0362, K0395, K0417, K0599	
ISC2 CISSP-ISSAP	K0001, K0002, K0004, K0005, K0006, K0395, K0403, K0417, K0432, K0455	
ISACA CISA	K0002, K0003, K0004, K0005, K0108, K0109, K0417, K0432, K0501, K0504, K0598	
Threat Modeling	K0002, K0004, K0005	S0218
Other learning paths	K0379, K0408, K0411, K0431, K0435, K0436, K0444, K0506, K0512	S0186, S0296

Cyber Operator (CO-OPS-001)

Conducts collection, processing and/or geolocation of systems to exploit, locate and/or track targets of interest. Performs network navigation, tactical forensic analysis and, when directed, executing on-net operations.

Core path name	Knowledge statements	Skill statements
CompTIA Security+	K0002, K0005, K0006, K0021, K0109, K0363, K0379, K0403, K0427, K0428, K0433, K0452, K0480, K0530, K0536, K0573, K0609	S0267
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0109, K0373, K0403, K0427, K0433, K0438, K0452, K0480, K0516, K0565	S0236
Cisco Certified CyberOps Associate	K0001, K0430, K0440, K0516, K0565, K0608	S0221
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0363, K0375, K0427, K0428, K0433, K0438, K0452, K0480, K0486, K0516, K0560, K0565, K0573	S0062, S0192, S0221, S0267, S0270, S0298
EC-Council CEH	K0002, K0009, K0373, K0375, K0427, K0428, K0430, K0480, K0536, K0565	S0221, S0242, S0267, S0293, S0295
Other learning paths	K0051, K0224, K0372, K0406, K0420, K0429, K0481, K0531	S0206, S0252, S0257, S0266, S0275, S0282

Cyber Crime Investigator (IN-INV-001)

Identifies, collects, examines and preserves evidence using controlled and documented analytical and investigative techniques.

Core path name	Knowledge statements	Skill statements
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0118, K0123, K0125, K0128, K0155, K0156, K0209, K0244, K0251, K0624	
CompTIA CASP+	K0002, K0003, K0004, K0005, K0006, K0070, K0118, K0125, K0128, K0624	
Linux Fundamentals	K0001, K0070, K0114	
Incident Response	K0003, K0004, K0005, K0046, K0110	
Certified Computer Forensics Examiner (CCFE)	K0001, K0107, K0118, K0123, K0125, K0128, K0156, K0168	S0047, S0068
Other learning paths	K0231, K0351	

Law Enforcement/Counterintelligence Forensics Analyst (IN-FOR-001)

Conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

Core path name	Knowledge statements	Skill statements
Certified Computer Forensics Examiner (CCFE)	K0001, K0017, K0107, K0117, K0118, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0156, K0168, K0182, K0184, K0185, K0305	S0047, S0062, S0065, S0068, S0071, S0075, S0090, S0091, S0092
Certified Mobile Forensics Examiner (CMFE)	K0017, K0060, K0118, K0122, K0128, K0133, K0134	S0047, S0065, S0071, S0091
ISC2 CISSP	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0021, K0042, K0070, K0077, K0109, K0118, K0122, K0123, K0125, K0128, K0132, K0133, K0145, K0155, K0156, K0167, K0179, K0184, K0305, K0624	
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0017, K0042, K0060, K0070, K0117, K0118, K0122, K0128, K0132, K0133, K0145, K0179, K0185	S0046, S0062, S0067, S0071, S0075, S0090, S0091
Certified Reverse Engineering Analyst (CREA)	K0183, K0186, K0188, K0189	S0087, S0092, S0093
Other learning paths	K0119, K0187	S0032, S0069, S0073, S0074, S0089

Cyber Defense Forensics Analyst (IN-FOR-002)

Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Core path name	Knowledge statements	Skill statements
CompTIA Security+	K0002, K0005, K0006, K0018, K0021, K0042, K0070, K0109, K0118, K0145, K0167, K0179, K0255, K0301, K0624	S0089
Certified Computer Forensics Examiner (CCFE)	K0001, K0117, K0118, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0156, K0168, K0182, K0184, K0185, K0304	S0047, S0062, S0065, S0068, S0071, S0075, S0090, S0091, S0092
Certified Reverse Engineering Analyst (CREA)	K0183, K0186, K0188, K0189	S0087, S0092, S0093, S0131
CERT-Certified Computer Security Incident Handler (CSIH)	K0001, K0004, K0018, K0042, K0060, K0070, K0117, K0118, K0122, K0128, K0132, K0133, K0145, K0179, K0185, K0255, K0301, K0304	S0062, S0067, S0071, S0075, S0090, S0091, S0156
CompTIA CySA+	K0002, K0003, K0004, K0005, K0042, K0070, K0118, K0122, K0128, K0132, K0133, K0134, K0145, K0167, K0179, K0183, K0186, K0301, K0304, K0624	
Other learning paths	K0077, K0119, K0155, K0187, K0224	S0032, S0069, S0073, S0074

Appendix: NICE knowledge and skill statements

The following table contains the knowledge and skill statements found in the NICE Workforce Framework for Cybersecurity. The first six knowledge statements are common to all 52 of the cybersecurity work roles in the framework.

Knowledge ID	Description
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004	Knowledge of cybersecurity and privacy principles.
K0005	Knowledge of cyber threats and vulnerabilities.
K0006	Knowledge of specific operational impacts of cybersecurity lapses.
K0007	Knowledge of authentication, authorization, and access control methods.
K0008	Knowledge of applicable business processes and operations of customer organizations.
K0009	Knowledge of application vulnerabilities.
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.
K0012	Knowledge of capabilities and requirements analysis.
K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K0014	Knowledge of complex data structures.
K0015	Knowledge of computer algorithms.
K0016	Knowledge of computer programming principles
K0017	Knowledge of concepts and practices of processing digital forensic data.
K0018	Knowledge of encryption algorithms
K0019	Knowledge of cryptography and cryptographic key management concepts
K0020	Knowledge of data administration and data standardization policies.
K0021	Knowledge of data backup and recovery.
K0022	Knowledge of data mining and data warehousing principles.
K0023	Knowledge of database management systems, query languages, table relationships, and views.
K0024	Knowledge of database systems.
K0025	Knowledge of digital rights management.
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.
K0027	Knowledge of organization’s enterprise information security architecture.
K0028	Knowledge of organization’s evaluation and validation requirements.
K0029	Knowledge of organization’s Local and Wide Area Network connections.
K0030	Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).
K0031	Knowledge of enterprise messaging systems and associated software.
K0032	Knowledge of resiliency and redundancy.
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).

Knowledge ID	Description
K0034	Knowledge of network services and protocols interactions that provide network communications.
K0035	Knowledge of installation, integration, and optimization of system components.
K0036	Knowledge of human-computer interaction principles.
K0037	Knowledge of Security Assessment and Authorization process.
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
K0041	Knowledge of incident categories, incident responses, and timelines for responses.
K0042	Knowledge of incident response and handling methodologies.
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.
K0048	Knowledge of Risk Management Framework (RMF) requirements.
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.
K0051	Knowledge of low-level computer languages (e.g., assembly languages).
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).
K0053	Knowledge of measures or indicators of system performance and availability.
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.
K0055	Knowledge of microprocessors.
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
K0057	Knowledge of network hardware devices and functions.
K0058	Knowledge of network traffic analysis methods.
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
K0060	Knowledge of operating systems.
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
K0062	Knowledge of packet-level analysis.
K0063	Knowledge of parallel and distributed computing concepts.
K0064	Knowledge of performance tuning tools and techniques.
K0065	Knowledge of policy-based and risk adaptive access controls.
K0066	Knowledge of Privacy Impact Assessments.
K0067	Knowledge of process engineering concepts.
K0068	Knowledge of programming language structures and logic.
K0069	Knowledge of query languages such as SQL (structured query language).
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).

Knowledge ID	Description
K0071	Knowledge of remote access technology concepts.
K0072	Knowledge of resource management principles and techniques.
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
K0075	Knowledge of security system design tools, methods, and techniques.
K0076	Knowledge of server administration and systems engineering theories, concepts, and methods.
K0077	Knowledge of server and client operating systems.
K0078	Knowledge of server diagnostic tools and fault identification techniques.
K0079	Knowledge of software debugging principles.
K0080	Knowledge of software design tools, methods, and techniques.
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).
K0082	Knowledge of software engineering.
K0083	Knowledge of sources, characteristics, and uses of the organization’s data assets.
K0084	Knowledge of structured analysis principles and methods.
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.
K0088	Knowledge of systems administration concepts.
K0089	Knowledge of systems diagnostic tools and fault identification techniques.
K0090	Knowledge of system life cycle management principles, including software security and usability.
K0091	Knowledge of systems testing and evaluation methods.
K0092	Knowledge of technology integration processes.
K0093	Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).
K0094	Knowledge of the capabilities and functionality associated with content creation technologies (e.g., wikis, social networking, content management systems, blogs).
K0095	Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines).
K0096	Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint).
K0097	Knowledge of the characteristics of physical and virtual data storage media.
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one’s own organization.
K0100	Knowledge of the enterprise information technology (IT) architecture.
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.
K0102	Knowledge of the systems engineering process.
K0103	Knowledge of the type and frequency of routine hardware maintenance.
K0104	Knowledge of Virtual Private Network (VPN) security.
K0105	Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web service description language).
K0106	Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities.
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
K0108	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).
K0109	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).
K0110	Knowledge of adversarial tactics, techniques, and procedures.

Knowledge ID	Description
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)
K0112	Knowledge of defense-in-depth principles and network security architecture.
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).
K0115	Knowledge that technology that can be exploited.
K0116	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
K0118	Knowledge of processes for seizing and preserving digital evidence.
K0119	Knowledge of hacking methodologies.
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.
K0121	Knowledge of information security program management and project management principles and techniques.
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).
K0124	Knowledge of multiple cognitive domains and tools and methods applicable for learning in each domain.
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).
K0128	Knowledge of types and collection of persistent data.
K0129	Knowledge of command-line tools (e.g., mkdir, mv, ls, passwd, grep).
K0130	Knowledge of virtualization technologies and virtual machine development and maintenance.
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
K0133	Knowledge of types of digital forensics data and how to recognize them.
K0134	Knowledge of deployable forensics.
K0135	Knowledge of web filtering technologies.
K0136	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
K0137	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).
K0138	Knowledge of Wi-Fi.
K0139	Knowledge of interpreted and compiled computer languages.
K0140	Knowledge of secure coding techniques.
K0142	Knowledge of collection management processes, capabilities, and limitations.
K0143	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.
K0144	Knowledge of social dynamics of computer attackers in a global context.
K0145	Knowledge of security event correlation tools.
K0146	Knowledge of the organization's core business/mission processes.
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.
K0149	Knowledge of organization's risk tolerance and/or risk management approach.

Knowledge ID	Description
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.
K0151	Knowledge of current and emerging threats/threat vectors.
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).
K0153	Knowledge of software quality assurance process.
K0154	Knowledge of supply chain risk management standards, processes, and practices.
K0155	Knowledge of electronic evidence law.
K0156	Knowledge of legal rules of evidence and court procedure.
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.
K0158	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
K0159	Knowledge of Voice over IP (VoIP).
K0160	Knowledge of the common attack vectors on the network layer.
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
K0162	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
K0163	Knowledge of critical information technology (IT) procurement requirements.
K0164	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).
K0165	Knowledge of risk/threat assessment.
K0167	Knowledge of system administration, network, and operating system hardening techniques.
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.
K0171	Knowledge of hardware reverse engineering techniques.
K0172	Knowledge of middleware (e.g., enterprise service bus and message queuing).
K0174	Knowledge of networking protocols.
K0175	Knowledge of software reverse engineering techniques.
K0176	Knowledge of Extensible Markup Language (XML) schemas.
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0178	Knowledge of secure software deployment methodologies, tools, and practices.
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).
K0183	Knowledge of reverse engineering concepts.
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).
K0186	Knowledge of debugging procedures and tools.
K0187	Knowledge of file type abuse by adversaries for anomalous behavior.
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).
K0189	Knowledge of malware with virtual machine detection (e.g. virtual aware malware, debugger aware malware, and unpacked malware that looks for VM-related strings in your computer's display device).

Knowledge ID	Description
K0190	Knowledge of encryption methodologies.
K0191	Knowledge of signature implementation impact for viruses, malware, and attacks.
K0192	Knowledge of Windows/Unix ports and services.
K0193	Knowledge of advanced data remediation security features in databases.
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.
K0195	Knowledge of data classification standards and methodologies based on sensitivity and other risk factors.
K0196	Knowledge of Import/Export Regulations related to cryptography and other security technologies.
K0197	Knowledge of database access application programming interfaces (e.g., Java Database Connectivity [JDBC]).
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).
K0201	Knowledge of symmetric key rotation techniques and concepts.
K0202	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
K0204	Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes).
K0205	Knowledge of basic system, network, and OS hardening techniques.
K0206	Knowledge of ethical hacking principles and techniques.
K0207	Knowledge of circuit analysis.
K0208	Knowledge of computer based training and e-learning services.
K0209	Knowledge of covert communication techniques.
K0210	Knowledge of data backup and restoration concepts.
K0211	Knowledge of confidentiality, integrity, and availability requirements.
K0212	Knowledge of cybersecurity-enabled software products.
K0213	Knowledge of instructional design and evaluation models (e.g., ADDIE, Smith/Ragan model, Gagne's Events of Instruction, Kirkpatrick's model of evaluation).
K0214	Knowledge of the Risk Management Framework Assessment Methodology.
K0215	Knowledge of organizational training policies.
K0216	Knowledge of learning levels (i.e., Bloom's Taxonomy of learning).
K0217	Knowledge of Learning Management Systems and their use in managing learning.
K0218	Knowledge of learning styles (e.g., assimilator, auditory, kinesthetic).
K0220	Knowledge of modes of learning (e.g., rote learning, observation).
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K0222	Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.
K0226	Knowledge of organizational training systems.
K0227	Knowledge of various types of computer architectures.
K0228	Knowledge of taxonomy and semantic ontology theory.
K0229	Knowledge of applications that can log errors, exceptions, and application faults and logging.
K0230	Knowledge of cloud service models and how those models can limit incident response.

Knowledge ID	Description
K0231	Knowledge of crisis management protocols, processes, and techniques.
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.
K0234	Knowledge of full spectrum cyber capabilities (e.g., defense, attack, exploitation).
K0235	Knowledge of how to leverage research and development centers, think tanks, academic research, and industry systems.
K0236	Knowledge of how to utilize Hadoop, Java, Python, SQL, Hive, and Pig to explore data.
K0237	Knowledge of industry best practices for service desk.
K0238	Knowledge of machine learning theory and principles.
K0239	Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.
K0240	Knowledge of multi-level security systems and cross domain solutions.
K0241	Knowledge of organizational human resource policies, processes, and procedures.
K0242	Knowledge of organizational security policies.
K0243	Knowledge of organizational training and education policies, processes, and procedures.
K0244	Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.
K0245	Knowledge of principles and processes for conducting training and education needs assessment.
K0246	Knowledge of relevant concepts, procedures, software, equipment, and technology applications.
K0247	Knowledge of remote access processes, tools, and capabilities related to customer support.
K0248	Knowledge of strategic theory and practice.
K0249	Knowledge of sustainment technologies, processes and strategies.
K0250	Knowledge of Test & Evaluation processes for learners.
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.
K0252	Knowledge of training and education principles and methods for curriculum design, teaching and instruction for individuals and groups, and the measurement of training and education effects.
K0254	Knowledge of binary analysis.
K0255	Knowledge of network architecture concepts including topology, protocols, and components.
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).
K0259	Knowledge of malware analysis concepts and methodologies.
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.
K0261	Knowledge of Payment Card Industry (PCI) data security standards.
K0262	Knowledge of Personal Health Information (PHI) data security standards.
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.
K0264	Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements).
K0265	Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.
K0266	Knowledge of how to evaluate the trustworthiness of the supplier and/or product.
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
K0268	Knowledge of forensic footprint identification.
K0269	Knowledge of mobile communications architecture.
K0270	Knowledge of the acquisition/procurement life cycle process.
K0271	Knowledge of operating system structures and internals (e.g., process management, directory structure, installed applications).
K0272	Knowledge of network analysis tools used to identify software communications vulnerabilities.

Knowledge ID	Description
K0274	Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.
K0275	Knowledge of configuration management techniques.
K0276	Knowledge of security management.
K0277	Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features).
K0278	Knowledge of current and emerging data remediation security features in databases.
K0280	Knowledge of systems engineering theories, concepts, and methods.
K0281	Knowledge of information technology (IT) service catalogues.
K0283	Knowledge of use cases related to collaboration and content synchronization across platforms (e.g., Mobile, PC, Cloud).
K0284	Knowledge of developing and applying user credential management system.
K0285	Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.
K0286	Knowledge of N-tiered typologies (e.g. including server and client operating systems).
K0287	Knowledge of an organization’s information classification program and procedures for information compromise.
K0288	Knowledge of industry standard security models.
K0289	Knowledge of system/server diagnostic tools and fault identification techniques.
K0290	Knowledge of systems security testing and evaluation methods.
K0291	Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)
K0292	Knowledge of the operations and processes for incident, problem, and event management.
K0293	Knowledge of integrating the organization’s goals and objectives into the architecture.
K0294	Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.
K0295	Knowledge of confidentiality, integrity, and availability principles.
K0296	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.
K0297	Knowledge of countermeasure design for identified security risks.
K0299	Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
K0300	Knowledge of network mapping and recreating network topologies.
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
K0302	Knowledge of the basic operation of computers.
K0303	Knowledge of the use of sub-netting tools.
K0304	Knowledge of concepts and practices of processing digital forensic data.
K0305	Knowledge of data concealment (e.g. encryption algorithms and steganography).
K0308	Knowledge of cryptology.
K0309	Knowledge of emerging technologies that have potential for exploitation.
K0310	Knowledge of hacking methodologies.
K0311	Knowledge of industry indicators useful for identifying technology trends.
K0312	Knowledge of intelligence gathering principles, policies, and procedures including legal authorities and restrictions.
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).
K0314	Knowledge of industry technologies’ potential cybersecurity vulnerabilities.
K0315	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing information.
K0316	Knowledge of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.

Knowledge ID	Description
K0317	Knowledge of procedures used for documenting and querying reported incidents, problems, and events.
K0318	Knowledge of operating system command-line tools.
K0319	Knowledge of technical delivery capabilities and their limitations.
K0320	Knowledge of organization's evaluation and validation criteria.
K0321	Knowledge of engineering concepts as applied to computer architecture and associated computer hardware/software.
K0322	Knowledge of embedded systems.
K0323	Knowledge of system fault tolerance methodologies.
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).
K0326	Knowledge of demilitarized zones.
K0330	Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).
K0335	Knowledge of current and emerging cyber technologies.
K0336	Knowledge of access authentication methods.
K0338	Knowledge of data mining techniques.
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.
K0341	Knowledge of foreign disclosure policies and import/export control regulations as related to cybersecurity.
K0342	Knowledge of penetration testing principles, tools, and techniques.
K0343	Knowledge of root cause analysis techniques.
K0344	Knowledge of an organization's threat environment.
K0346	Knowledge of principles and methods for integrating system components.
K0347	Knowledge and understanding of operational design.
K0349	Knowledge of website types, administration, functions, and content management system (CMS).
K0350	Knowledge of accepted organization planning systems.
K0351	Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.
K0352	Knowledge of forms of intelligence support needs, topics, and focus areas.
K0353	Knowledge of possible circumstances that would result in changing collection management authorities.
K0354	Knowledge of relevant reporting and dissemination procedures.
K0355	Knowledge of all-source reporting and dissemination procedures.
K0356	Knowledge of analytic tools and techniques for language, voice and/or graphic material.
K0357	WITHDRAWN: Knowledge of analytical constructs and their use in assessing the operational environment. (See K0224)
K0358	Knowledge of analytical standards and the purpose of intelligence confidence levels.
K0359	Knowledge of approved intelligence dissemination processes.
K0361	Knowledge of asset availability, capabilities and limitations.
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).
K0363	Knowledge of auditing and logging procedures (including server-based logging).
K0364	Knowledge of available databases and tools necessary to assess appropriate collection tasking.
K0368	Knowledge of implants that enable cyber collection and/or preparation activities.

Knowledge ID	Description
K0371	Knowledge of principles of the collection development processes (e.g., Dialed Number Recognition, Social Network Analysis).
K0372	Knowledge of programming concepts (e.g., levels, structures, compiled vs. interpreted languages).
K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
K0374	WITHDRAWN: Knowledge of basic structure, architecture, and design of modern digital and telephony networks. (See K0599)
K0375	Knowledge of wireless applications vulnerabilities.
K0376	Knowledge of internal and external customers and partner organizations, including information needs, objectives, structure, capabilities, etc.
K0377	Knowledge of classification and control markings standards, policies and procedures.
K0379	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.
K0380	Knowledge of collaborative tools and environments.
K0381	Knowledge of collateral damage and estimating impact(s).
K0382	Knowledge of collection capabilities and limitations.
K0383	Knowledge of collection capabilities, accesses, performance specifications, and constraints utilized to satisfy collection plan.
K0384	Knowledge of collection management functionality (e.g., positions, functions, responsibilities, products, reporting requirements).
K0386	Knowledge of collection management tools.
K0387	Knowledge of collection planning process and collection plan.
K0388	Knowledge of collection searching/analyzing techniques and tools for chat/buddy list, emerging technologies, VOIP, Media Over IP, VPN, VSAT/wireless, web mail and cookies.
K0389	Knowledge of collection sources including conventional and non-conventional sources.
K0390	Knowledge of collection strategies.
K0391	Knowledge of collection systems, capabilities, and processes.
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
K0393	Knowledge of common networking devices and their configurations.
K0394	Knowledge of common reporting databases and tools.
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).
K0396	Knowledge of computer programming concepts, including computer languages, programming, testing, debugging, and file types.
K0397	Knowledge of security concepts in operating systems (e.g., Linux, Unix.)
K0398	Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).
K0399	Knowledge of crisis action planning and time sensitive planning procedures.
K0400	Knowledge of crisis action planning for cyber operations.
K0401	Knowledge of criteria for evaluating collection products.
K0402	Knowledge of criticality and vulnerability factors (e.g., value, recuperation, cushion, countermeasures) for target selection and applicability to the cyber domain.
K0403	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.
K0404	Knowledge of current collection requirements.
K0405	Knowledge of current computer-based intrusion sets.
K0406	Knowledge of current software and methodologies for active defense and system hardening.
K0407	Knowledge of customer information needs.

Knowledge ID	Description
K0408	Knowledge of cyber actions (i.e. cyber defense, information gathering, environment preparation, cyber-attack) principles, capabilities, limitations, and effects.
K0409	Knowledge of cyber intelligence/information collection capabilities and repositories.
K0410	Knowledge of cyber laws and their effect on Cyber planning.
K0411	Knowledge of cyber laws and legal considerations and their effect on cyber planning.
K0412	Knowledge of cyber lexicon/terminology
K0413	Knowledge of cyber operation objectives, policies, and legalities.
K0414	Knowledge of cyber operations support or enabling processes.
K0415	Knowledge of cyber operations terminology/lexicon.
K0416	Knowledge of cyber operations.
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).
K0418	Knowledge of data flow process for terminal or environment collection.
K0419	Knowledge of database administration and maintenance.
K0420	Knowledge of database theory.
K0421	Knowledge of databases, portals and associated dissemination vehicles.
K0422	Knowledge of deconfliction processes and procedures.
K0423	Knowledge of deconfliction reporting to include external organization interaction.
K0424	Knowledge of denial and deception techniques.
K0425	Knowledge of different organization objectives at all levels, including subordinate, lateral and higher.
K0426	Knowledge of dynamic and deliberate targeting.
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).
K0428	Knowledge of encryption algorithms and tools for wireless local area networks (WLANs).
K0429	Knowledge of enterprise-wide information management.
K0430	Knowledge of evasion strategies and techniques.
K0431	Knowledge of evolving/emerging communications technologies.
K0432	Knowledge of existing, emerging, and long-range issues related to cyber operations strategy, policy, and organization.
K0433	Knowledge of forensic implications of operating system structure and operations.
K0435	Knowledge of fundamental cyber concepts, principles, limitations, and effects.
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber-attack, cyber defense), principles, capabilities, limitations, and effects.
K0437	Knowledge of general Supervisory control and data acquisition (SCADA) system components.
K0438	Knowledge of mobile cellular communications architecture (e.g., LTE, CDMA, GSM/EDGE and UMTS/HSPA).
K0439	Knowledge of governing authorities for targeting.
K0440	Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability.
K0442	Knowledge of how converged technologies impact cyber operations (e.g., digital, telephony, wireless).
K0443	WITHDRAWN: Knowledge of how hubs, switches, routers work together in the design of a network. (See K0143)
K0444	Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.
K0446	Knowledge of how modern wireless communications systems impact cyber operations.
K0447	Knowledge of how to collect, view, and identify essential information on targets of interest from metadata (e.g., email, http).
K0448	Knowledge of how to establish priorities for resources.
K0449	Knowledge of how to extract, analyze, and use metadata.

Knowledge ID	Description
K0451	Knowledge of identification and reporting processes.
K0452	Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.
K0453	Knowledge of indications and warning.
K0454	Knowledge of information needs.
K0455	Knowledge of information security concepts, facilitating technologies and methods.
K0456	Knowledge of intelligence capabilities and limitations.
K0457	Knowledge of intelligence confidence levels.
K0458	Knowledge of intelligence disciplines.
K0459	Knowledge of intelligence employment requirements (i.e., logistical, communications support, maneuverability, legal restrictions, etc.).
K0460	Knowledge of intelligence preparation of the environment and similar processes.
K0461	Knowledge of intelligence production processes.
K0462	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.
K0463	Knowledge of intelligence requirements tasking systems.
K0464	Knowledge of intelligence support to planning, execution, and assessment.
K0465	Knowledge of internal and external partner cyber operations capabilities and tools.
K0466	Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information.
K0467	Knowledge of internal and external partner organization capabilities and limitations (those with tasking, collection, processing, exploitation and dissemination responsibilities).
K0468	Knowledge of internal and external partner reporting.
K0469	Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.
K0470	Knowledge of Internet and routing protocols.
K0471	Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).
K0472	Knowledge of intrusion detection systems and signature development.
K0473	Knowledge of intrusion sets.
K0474	Knowledge of key cyber threat actors and their equities.
K0475	Knowledge of key factors of the operational environment and threat.
K0476	Knowledge of language processing tools and techniques.
K0477	Knowledge of leadership's Intent and objectives.
K0478	Knowledge of legal considerations in targeting.
K0479	Knowledge of malware analysis and characteristics.
K0480	Knowledge of malware.
K0481	Knowledge of methods and techniques used to detect various exploitation activities.
K0482	Knowledge of methods for ascertaining collection asset posture and availability.
K0483	Knowledge of methods to integrate and summarize information from any potential sources.
K0484	Knowledge of midpoint collection (process, objectives, organization, targets, etc.).
K0485	Knowledge of network administration.
K0486	Knowledge of network construction and topology.
K0487	Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
K0488	Knowledge of network security implementations (e.g., host-based IDS, IPS, access control lists), including their function and placement in a network.
K0489	Knowledge of network topology.

Knowledge ID	Description
K0491	Knowledge of networking and Internet communications fundamentals (i.e. devices, device configuration, hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.).
K0492	Knowledge of non-traditional collection methodologies.
K0493	Knowledge of obfuscation techniques (e.g., TOR/Onion/anonymizers, VPN/VPS, encryption).
K0494	Knowledge of objectives, situation, operational environment, and the status and disposition of internal and external partner collection capabilities available to support planning.
K0495	Knowledge of ongoing and future operations.
K0496	Knowledge of operational asset constraints.
K0497	Knowledge of operational effectiveness assessment.
K0498	Knowledge of operational planning processes.
K0499	Knowledge of operations security.
K0500	Knowledge of organization and/or partner collection systems, capabilities, and processes (e.g., collection and protocol processors).
K0501	Knowledge of organization cyber operations programs, strategies, and resources.
K0502	Knowledge of organization decision support tools and/or methods.
K0503	Knowledge of organization formats of resource and asset readiness reporting, its operational relevance and intelligence collection impact.
K0504	Knowledge of organization issues, objectives, and operations in cyber as well as regulations and policy directives governing cyber operations.
K0505	Knowledge of organization objectives and associated demand on collection management.
K0506	Knowledge of organization objectives, leadership priorities, and decision-making risks.
K0507	Knowledge of organization or partner exploitation of digital networks.
K0508	Knowledge of organization policies and planning concepts for partnering with internal and/or external organizations.
K0509	Knowledge of organizational and partner authorities, responsibilities, and contributions to achieving objectives.
K0510	Knowledge of organizational and partner policies, tools, capabilities, and procedures.
K0511	Knowledge of organizational hierarchy and cyber decision-making processes.
K0512	Knowledge of organizational planning concepts.
K0513	Knowledge of organizational priorities, legal authorities and requirements submission processes.
K0514	Knowledge of organizational structures and associated intelligence capabilities.
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.
K0517	Knowledge of post implementation review (PIR) approval process.
K0518	Knowledge of planning activity initiation.
K0519	Knowledge of planning timelines adaptive, crisis action, and time-sensitive planning.
K0520	Knowledge of principles and practices related to target development such as target knowledge, associations, communication systems, and infrastructure.
K0521	Knowledge of priority information, how it is derived, where it is published, how to access, etc.
K0522	Knowledge of production exploitation and dissemination needs and architectures.
K0523	Knowledge of products and nomenclature of major vendors (e.g., security suites - Trend Micro, Symantec, McAfee, Outpost, and Panda) and how those products affect exploitation and reduce vulnerabilities.
K0524	Knowledge of relevant laws, regulations, and policies.
K0525	Knowledge of required intelligence planning products associated with cyber operational planning.
K0526	Knowledge of research strategies and knowledge management.
K0527	Knowledge of risk management and mitigation strategies.
K0528	Knowledge of satellite-based communication systems.
K0529	Knowledge of scripting

Knowledge ID	Description
K0530	Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation.
K0531	Knowledge of security implications of software configurations.
K0532	Knowledge of specialized target language (e.g., acronyms, jargon, technical terminology, code words).
K0533	Knowledge of specific target identifiers, and their usage.
K0534	Knowledge of staff management, assignment, and allocation processes.
K0535	Knowledge of strategies and tools for target research.
K0536	Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).
K0538	Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities
K0539	Knowledge of target communication profiles and their key elements (e.g., target associations, activities, communication infrastructure).
K0540	Knowledge of target communication tools and techniques.
K0541	Knowledge of target cultural references, dialects, expressions, idioms, and abbreviations.
K0542	Knowledge of target development (i.e., concepts, roles, responsibilities, products, etc.).
K0543	Knowledge of target estimated repair and recuperation times.
K0544	Knowledge of target intelligence gathering and operational preparation techniques and life cycles.
K0545	Knowledge of target language(s).
K0546	Knowledge of target list development (i.e. Restricted, Joint, Candidate, etc.).
K0547	Knowledge of target methods and procedures.
K0548	Knowledge of target or threat cyber actors and procedures.
K0549	Knowledge of target vetting and validation procedures.
K0550	Knowledge of target, including related current events, communication profile, actors, and history (language, culture) and/or frame of reference.
K0551	Knowledge of targeting cycles.
K0552	Knowledge of tasking mechanisms.
K0553	Knowledge of tasking processes for organic and subordinate collection assets.
K0554	Knowledge of tasking, collection, processing, exploitation and dissemination.
K0555	Knowledge of TCP/IP networking protocols.
K0556	Knowledge of telecommunications fundamentals.
K0557	Knowledge of terminal or environmental collection (process, objectives, organization, targets, etc.).
K0558	Knowledge of the available tools and applications associated with collection requirements and collection management.
K0559	Knowledge of the basic structure, architecture, and design of converged applications.
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
K0562	Knowledge of the capabilities and limitations of new and emerging collection capabilities, accesses and/or processes.
K0563	Knowledge of the capabilities, limitations and tasking methodologies of internal and external collections as they apply to planned cyber activities.
K0564	Knowledge of the characteristics of targeted communication networks (e.g., capacity, functionality, paths, critical nodes).
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.
K0566	Knowledge of the critical information requirements and how they're used in planning.
K0567	Knowledge of the data flow from collection origin to repositories and tools.
K0568	Knowledge of the definition of collection management and collection management authority.
K0569	Knowledge of the existent tasking, collection, processing, exploitation and dissemination architecture.

Knowledge ID	Description
K0570	Knowledge of the factors of threat that could impact collection operations.
K0571	Knowledge of the feedback cycle in collection processes.
K0572	Knowledge of the functions and capabilities of internal teams that emulate threat activities to benefit the organization.
K0573	Knowledge of the fundamentals of digital forensics to extract actionable intelligence.
K0574	Knowledge of the impact of language analysis on on-net operator functions.
K0575	Knowledge of the impacts of internal and external partner staffing estimates.
K0576	Knowledge of the information environment.
K0577	Knowledge of the intelligence frameworks, processes, and related systems.
K0578	Knowledge of the intelligence requirements development and request for information processes.
K0579	Knowledge of the organization, roles and responsibilities of higher, lower and adjacent sub-elements.
K0580	Knowledge of the organization’s established format for collection plan.
K0581	Knowledge of the organization’s planning, operations and targeting cycles.
K0582	Knowledge of the organizational planning and staffing process.
K0583	Knowledge of the organizational plans/directives/guidance that describe objectives.
K0584	Knowledge of the organizational policies/procedures for temporary transfer of collection authority.
K0585	Knowledge of the organizational structure as it pertains to full spectrum cyber operations, including the functions, responsibilities, and interrelationships among distinct internal elements.
K0586	Knowledge of the outputs of course of action and exercise analysis.
K0587	Knowledge of the POC’s, databases, tools and applications necessary to establish environment preparation and surveillance products.
K0588	Knowledge of the priority information requirements from subordinate, lateral and higher levels of the organization.
K0589	Knowledge of the process used to assess the performance and impact of operations.
K0590	Knowledge of the processes to synchronize operational assessment procedures with the critical information requirement process.
K0591	Knowledge of the production responsibilities and organic analysis and production capabilities.
K0592	Knowledge of the purpose and contribution of target templates.
K0593	Knowledge of the range of cyber operations and their underlying intelligence support needs, topics, and focus areas.
K0594	Knowledge of the relationships between end states, objectives, effects, lines of operation, etc.
K0595	Knowledge of the relationships of operational objectives, intelligence requirements, and intelligence production tasks.
K0596	Knowledge of the request for information process.
K0597	Knowledge of the role of network operations in supporting and facilitating other organization operations.
K0598	Knowledge of the structure and intent of organization specific plans, guidance and authorizations.
K0599	Knowledge of the structure, architecture, and design of modern digital and telephony networks.
K0600	Knowledge of the structure, architecture, and design of modern wireless communications systems.
K0601	Knowledge of the systems/architecture/communications used for coordination.
K0602	Knowledge of collection disciplines and capabilities.
K0603	Knowledge of the ways in which targets or threats use the Internet.
K0604	Knowledge of threat and/or target systems.
K0605	Knowledge of tipping, cueing, mixing, and redundancy.
K0606	Knowledge of transcript development processes and techniques (e.g., verbatim, gist, summaries).
K0607	Knowledge of translation processes and techniques.
K0608	Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).

Knowledge ID	Description
K0609	Knowledge of virtual machine technologies.
K0610	Knowledge of virtualization products (VMware, Virtual PC).
K0612	Knowledge of what constitutes a "threat" to a network.
K0613	Knowledge of who the organization's operational planners are, how and where they can be contacted, and what are their expectations.
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.
K0615	Knowledge of privacy disclosure statements based on current laws.
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
K0628	Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.

Skill ID	Description
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
S0002	Skill in allocating storage capacity in the design of data management systems.
S0003	Skill of identifying, capturing, containing, and reporting malware.
S0004	Skill in analyzing network traffic capacity and performance characteristics.
S0005	Skill in applying and incorporating information technologies into proposed solutions.
S0006	Skill in applying confidentiality, integrity, and availability principles.
S0007	Skill in applying host/network access controls (e.g., access control list).
S0008	Skill in applying organization-specific systems analysis principles and techniques.
S0009	WITHDRAWN: Skill in assessing the robustness of security systems and designs. (See S0027)
S0010	Skill in conducting capabilities and requirements analysis.
S0011	Skill in conducting information searches.
S0012	Skill in conducting knowledge mapping (e.g., map of knowledge repositories).
S0013	Skill in conducting queries and developing algorithms to analyze data structures.
S0014	Skill in conducting software debugging.
S0015	Skill in conducting test events.
S0016	Skill in configuring and optimizing software.
S0017	Skill in creating and utilizing mathematical or statistical models.
S0018	Skill in creating policies that reflect system security objectives.
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.
S0020	Skill in developing and deploying signatures.
S0021	Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data).
S0022	Skill in designing countermeasures to identified security risks.
S0023	Skill in designing security controls based on cybersecurity principles and tenets.
S0024	Skill in designing the integration of hardware and software solutions.
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
S0026	Skill in determining an appropriate level of test rigor for a given system.
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
S0028	Skill in developing data dictionaries.

Skill ID	Description
S0029	Skill in developing data models.
S0030	Skill in developing operations-based testing scenarios.
S0031	Skill in developing and applying security system access controls.
S0032	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.
S0033	Skill in diagnosing connectivity problems.
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
S0035	Skill in establishing a routing schema.
S0036	Skill in evaluating the adequacy of security designs.
S0037	Skill in generating queries and reports.
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.
S0039	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.
S0040	Skill in implementing, maintaining, and improving established network security practices.
S0041	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.
S0042	Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.).
S0043	Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.).
S0044	Skill in mimicking threat behaviors.
S0045	Skill in optimizing database performance.
S0046	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.
S0048	Skill in systems integration testing.
S0049	Skill in the measuring and reporting of intellectual capital.
S0050	Skill in design modeling and building use cases (e.g., unified modeling language).
S0051	Skill in the use of penetration testing tools and techniques.
S0052	Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
S0053	Skill in tuning sensors.
S0054	Skill in using incident handling methodologies.
S0055	Skill in using knowledge management technologies.
S0056	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).
S0057	Skill in using protocol analyzers.
S0058	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).
S0061	Skill in writing test plans.
S0062	Skill in analyzing memory dumps to extract information.
S0063	Skill in collecting data from a variety of cyber defense resources.
S0064	Skill in developing and executing technical training programs and curricula.
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).
S0066	Skill in identifying gaps in technical capabilities.
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.

Skill ID	Description
S0069	Skill in setting up a forensic workstation.
S0070	Skill in talking to others to convey information effectively.
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).
S0072	Skill in using scientific rules and methods to solve problems.
S0073	Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
S0074	Skill in physically disassembling PCs.
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).
S0076	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
S0077	Skill in securing network communications.
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
S0080	Skill in performing damage assessments.
S0081	Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).
S0082	Skill in evaluating test plans for applicability and completeness.
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.
S0084	Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).
S0085	Skill in conducting audits or reviews of technical systems.
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).
S0090	Skill in analyzing anomalous code as malicious or benign.
S0091	Skill in analyzing volatile data.
S0092	Skill in identifying obfuscation techniques.
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.
S0094	Skill in reading Hexadecimal data.
S0095	Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode).
S0096	Skill in reading and interpreting signatures (e.g., snort).
S0097	Skill in applying security controls.
S0098	WITHDRAWN: Skill in detecting host and network based intrusions via intrusion detection technologies. (See S0025)
S0100	Skill in utilizing or developing learning activities (e.g., scenarios, instructional games, interactive exercises).
S0101	Skill in utilizing technologies (e.g., SmartBoards, websites, computers, projectors) for instructional purposes.
S0102	Skill in applying technical delivery capabilities.
S0103	Skill in assessing the predictive power and subsequent generalizability of a model.
S0104	Skill in conducting Test Readiness Reviews.
S0106	Skill in data pre-processing (e.g., imputation, dimensionality reduction, normalization, transformation, extraction, filtering, smoothing).
S0107	Skill in designing and documenting overall program Test & Evaluation strategies.
S0108	Skill in developing workforce and position qualification standards.
S0109	Skill in identifying hidden patterns or relationships.
S0110	Skill in identifying Test & Evaluation infrastructure (people, ranges, tools, instrumentation) requirements.

Skill ID	Description
S0111	Skill in interfacing with customers.
S0112	Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events.
S0113	Skill in performing format conversions to create a standard representation of the data.
S0114	Skill in performing sensitivity analysis.
S0115	Skill in preparing Test & Evaluation reports.
S0116	Skill in designing multi-level security/cross domain solutions.
S0117	Skill in providing Test & Evaluation resource estimate.
S0118	Skill in developing machine understandable semantic ontologies.
S0119	Skill in Regression Analysis (e.g., Hierarchical Stepwise, Generalized Linear Model, Ordinary Least Squares, Tree-Based Methods, Logistic).
S0120	Skill in reviewing logs to identify evidence of past intrusions.
S0121	Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).
S0122	Skill in the use of design methods.
S0123	Skill in transformation analytics (e.g., aggregation, enrichment, processing).
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.
S0125	Skill in using basic descriptive statistics and techniques (e.g., normality, model distribution, scatter plots).
S0126	Skill in using data analysis tools (e.g., Excel, STATA SAS, SPSS).
S0127	Skill in using data mapping tools.
S0128	Skill in using manpower and personnel IT systems.
S0129	Skill in using outlier identification and removal techniques.
S0130	Skill in writing scripts using R, Python, PIG, HIVE, SQL, etc.
S0131	Skill in analyzing malware.
S0132	Skill in conducting bit-level analysis.
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.
S0134	Skill in conducting reviews of systems.
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).
S0136	Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
S0137	Skill in conducting application vulnerability assessments.
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).
S0139	Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
S0140	Skill in applying the systems engineering process.
S0141	Skill in assessing security systems designs.
S0142	Skill in conducting research for troubleshooting novel client-level problems.
S0143	Skill in conducting system/server planning, management, and maintenance.
S0144	Skill in correcting physical and technical problems that impact system/server performance.
S0145	Skill in integrating and applying policies that meet system security objectives.
S0146	Skill in creating policies that enable systems to meet performance objectives (e.g. traffic routing, SLA's, CPU specifications).
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
S0148	Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.

Skill ID	Description
S0150	Skill in implementing and testing network infrastructure contingency and recovery plans.
S0151	Skill in troubleshooting failed system components (i.e., servers)
S0152	Skill in translating operational requirements into protection needs (i.e., security controls).
S0153	Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.
S0154	Skill in installing system and component upgrades. (i.e., servers, appliances, network devices).
S0155	Skill in monitoring and optimizing system/server performance.
S0156	Skill in performing packet-level analysis.
S0157	Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.).
S0158	Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software).
S0159	Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.
S0160	Skill in the use of design modeling (e.g., unified modeling language).
S0162	Skill in applying various subnet techniques (e.g., CIDR)
S0166	Skill in identifying gaps in technical delivery capabilities.
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
S0168	Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks.
S0169	Skill in conducting trend analysis.
S0170	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).
S0171	Skill in performing impact/risk assessments.
S0172	Skill in applying secure coding techniques.
S0173	Skill in using security event correlation tools.
S0174	Skill in using code analysis tools.
S0175	Skill in performing root cause analysis.
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.
S0177	Skill in analyzing a target's communication networks.
S0178	Skill in analyzing essential network data (e.g., router configuration files, routing protocols).
S0179	Skill in analyzing language processing tools to provide feedback to enhance tool development.
S0181	Skill in analyzing midpoint collection data.
S0182	Skill in analyzing target communications internals and externals collected from wireless LANs.
S0183	Skill in analyzing terminal or environment collection data.
S0184	Skill in analyzing traffic to identify network devices.
S0185	Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.
S0186	Skill in applying crisis planning procedures.
S0187	Skill in applying various analytical methods, tools, and techniques (e.g., competing hypotheses; chain of reasoning; scenario methods; denial and deception detection; high impact-low probability; network/association or link analysis; Bayesian, Delphi, and Pattern analyses).
S0188	Skill in assessing a target's frame of reference (e.g., motivation, technical capability, organizational structure, sensitivities).
S0189	Skill in assessing and/or estimating effects generated during and after cyber operations.
S0190	Skill in assessing current tools to identify needed improvements.
S0191	Skill in assessing the applicability of available analytical tools to various situations.
S0192	Skill in auditing firewalls, perimeters, routers, and intrusion detection systems.

Skill ID	Description
S0193	Skill in complying with the legal restrictions for targeted information.
S0194	Skill in conducting non-attributable research.
S0195	Skill in conducting research using all available sources.
S0196	Skill in conducting research using deep web.
S0197	Skill in conducting social network analysis, buddy list analysis, and/or cookie analysis.
S0198	Skill in conducting social network analysis.
S0199	Skill in creating and extracting important information from packet captures.
S0200	Skill in creating collection requirements in support of data acquisition activities.
S0201	Skill in creating plans in support of remote operations. (i.e., hot/warm/cold/alternative sites, disaster recovery).
S0202	Skill in data mining techniques (e.g., searching file systems) and analysis.
S0203	Skill in defining and characterizing all pertinent aspects of the operational environment.
S0204	Skill in depicting source or collateral data on a network map.
S0205	Skill in determining appropriate targeting options through the evaluation of available capabilities against desired effects.
S0206	Skill in determining installed patches on various operating systems and identifying patch signatures.
S0207	Skill in determining the effect of various router and firewall configurations on traffic patterns and network performance in both LAN and WAN environments.
S0208	Skill in determining the physical location of network devices.
S0209	Skill in developing and executing comprehensive cyber operations assessment programs for assessing and validating operational performance characteristics.
S0210	Skill in developing intelligence reports.
S0211	Skill in developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
S0212	Skill in disseminating items of highest intelligence value in a timely manner.
S0213	Skill in documenting and communicating complex technical and programmatic information.
S0214	Skill in evaluating accesses for intelligence value.
S0215	Skill in evaluating and interpreting metadata.
S0216	Skill in evaluating available capabilities against desired effects to provide effective courses of action.
S0217	Skill in evaluating data sources for relevance, reliability, and objectivity.
S0218	Skill in evaluating information for reliability, validity, and relevance.
S0219	Skill in evaluating information to recognize relevance, priority, etc.
S0220	Skill in exploiting/querying organizational and/or partner collection databases.
S0221	Skill in extracting information from packet captures.
S0222	Skill in fusion analysis
S0223	Skill in generating operation plans in support of mission and target requirements.
S0224	Skill in gisting target communications.
S0225	Skill in identifying a target’s communications networks.
S0226	Skill in identifying a target’s network characteristics.
S0227	Skill in identifying alternative analytical interpretations to minimize unanticipated outcomes.
S0228	Skill in identifying critical target elements, to include critical target elements for the cyber domain.
S0229	Skill in identifying cyber threats which may jeopardize organization and/or partner interests.
S0231	Skill in identifying how a target communicates.
S0232	Skill in identifying intelligence gaps and limitations.
S0233	Skill in identifying language issues that may have an impact on organization objectives.
S0234	Skill in identifying leads for target development.

Skill ID	Description
S0235	Skill in identifying non-target regional languages and dialects
S0236	Skill in identifying the devices that work at each level of protocol models.
S0237	Skill in identifying, locating, and tracking targets via geospatial analysis techniques
S0238	Skill in information prioritization as it relates to operations.
S0239	Skill in interpreting compiled and interpretive programming languages.
S0240	Skill in interpreting metadata and content as applied by collection systems.
S0241	Skill in interpreting traceroute results, as they apply to network analysis and reconstruction.
S0242	Skill in interpreting vulnerability scanner results to identify vulnerabilities.
S0243	Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).
S0244	Skill in managing client relationships, including determining client needs/requirements, managing client expectations, and demonstrating commitment to delivering quality results.
S0245	Skill in navigating network visualization software.
S0246	Skill in number normalization.
S0247	Skill in performing data fusion from existing intelligence for enabling new and continued collection.
S0248	Skill in performing target system analysis.
S0249	Skill in preparing and presenting briefings.
S0250	Skill in preparing plans and related correspondence.
S0251	Skill in prioritizing target language material.
S0252	Skill in processing collected data for follow-on analysis.
S0253	Skill in providing analysis on target-related matters (e.g., language, cultural, communications).
S0254	Skill in providing analysis to aid writing phased after action reports.
S0255	Skill in providing real-time, actionable geolocation information utilizing target infrastructures.
S0256	Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.
S0257	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data).
S0258	Skill in recognizing and interpreting malicious network activity in traffic.
S0259	Skill in recognizing denial and deception techniques of the target.
S0260	Skill in recognizing midpoint opportunities and essential information.
S0261	Skill in recognizing relevance of information.
S0262	Skill in recognizing significant changes in a target’s communication patterns.
S0263	Skill in recognizing technical information that may be used for leads for metadata analysis.
S0264	Skill in recognizing technical information that may be used for leads to enable remote operations (data includes users, passwords, email addresses, IP ranges of the target, frequency in DNI behavior, mail servers, domain servers, SMTP header information).
S0265	Skill in recognizing technical information that may be used for target development including intelligence development.
S0266	Skill in relevant programming languages (e.g., C++, Python, etc.).
S0267	Skill in remote command line and Graphic User Interface (GUI) tool usage.
S0268	Skill in researching essential information.
S0269	Skill in researching vulnerabilities and exploits utilized in traffic.
S0270	Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools.
S0271	Skill in reviewing and editing assessment products.
S0272	Skill in reviewing and editing intelligence products from various sources for cyber operations.
S0273	Skill in reviewing and editing plans.

Skill ID	Description
S0274	Skill in reviewing and editing target materials.
S0275	Skill in server administration.
S0276	Skill in survey, collection, and analysis of wireless LAN metadata.
S0277	Skill in synthesizing, analyzing, and prioritizing meaning across data sets.
S0278	Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).
S0279	Skill in target development in direct support of collection operations.
S0280	Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementation of new technologies).
S0281	Skill in technical writing.
S0282	Skill in testing and evaluating tools for implementation.
S0283	Skill in transcribing target language communications.
S0284	Skill in translating target graphic and/or voice language materials.
S0285	Skill in using Boolean operators to construct simple and complex queries.
S0286	Skill in using databases to identify target-relevant information.
S0287	Skill in using geospatial data and applying geospatial resources.
S0288	Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).
S0289	Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.
S0290	Skill in using non-attributable networks.
S0291	Skill in using research methods including multiple, different sources to reconstruct a target network.
S0292	Skill in using targeting databases and software packages.
S0293	Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.
S0294	Skill in using trace route tools and interpreting the results as they apply to network analysis and reconstruction.
S0295	Skill in using various open source data collection tools (online trade, DNS, mail, etc.).
S0296	Skill in utilizing feedback to improve processes, products, and services.
S0297	Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
S0298	Skill in verifying the integrity of all files. (e.g., checksums, Exclusive OR, secure hashes, check constraints, etc.).
S0299	Skill in wireless network target analysis, templating, and geolocation.
S0300	Skill in writing (and submitting) requirements to meet gaps in technical capabilities.
S0301	Skill in writing about facts and ideas in a clear, convincing, and organized manner.
S0302	Skill in writing effectiveness reports.
S0303	Skill in writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.
S0304	Skill to access information on current assets available, usage.
S0305	Skill to access the databases where plans/directives/guidance are maintained.
S0306	Skill to analyze strategic guidance for issues requiring clarification and/or additional guidance.
S0307	Skill to analyze target or threat sources of strength and morale.
S0308	Skill to anticipate intelligence capability employment requirements.
S0309	Skill to anticipate key target or threat activities which are likely to prompt a leadership decision.
S0310	Skill to apply analytical standards to evaluate intelligence products.
S0311	Skill to apply the capabilities, limitations and tasking methodologies of available platforms, sensors, architectures and apparatus as they apply to organization objectives.
S0312	Skill to apply the process used to assess the performance and impact of cyber operations.
S0313	Skill to articulate a needs statement/requirement and integrate new and emerging collection capabilities, accesses and/or processes into collection operations.

Skill ID	Description
S0314	Skill to articulate intelligence capabilities available to support execution of the plan.
S0315	Skill to articulate the needs of joint planners to all-source analysts.
S0316	Skill to associate Intelligence gaps to priority information requirements and observables.
S0317	Skill to compare indicators/observables with requirements.
S0318	Skill to conceptualize the entirety of the intelligence process in the multiple domains and dimensions.
S0319	Skill to convert intelligence requirements into intelligence production tasks.
S0320	Skill to coordinate the development of tailored intelligence products.
S0321	Skill to correlate intelligence priorities to the allocation of intelligence resources/assets.
S0322	Skill to craft indicators of operational progress/success.
S0323	Skill to create and maintain up-to-date planning documents and tracking of services/production.
S0324	Skill to determine feasibility of collection.
S0325	Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information needed.
S0326	Skill to distinguish between notional and actual resources and their applicability to the plan under development.
S0327	Skill to ensure that the collection strategy leverages all available resources.
S0328	Skill to evaluate factors of the operational environment to objectives, and information requirements.
S0329	Skill to evaluate requests for information to determine if response information exists.
S0330	Skill to evaluate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.
S0331	Skill to express orally and in writing the relationship between intelligence capability limitations and decision-making risk and impacts on the overall operation.
S0332	Skill to extract information from available tools and applications associated with collection requirements and collection operations management.
S0333	Skill to graphically depict decision support materials containing intelligence and partner capability estimates.
S0334	Skill to identify and apply tasking, collection, processing, exploitation and dissemination to associated collection disciplines.
S0335	Skill to identify Intelligence gaps.
S0336	Skill to identify when priority information requirements are satisfied.
S0337	Skill to implement established procedures for evaluating collection management and operations activities.
S0338	Skill to interpret planning guidance to discern level of analytical support required.
S0339	Skill to interpret readiness reporting, its operational relevance and intelligence collection impact.
S0340	Skill to monitor target or threat situation and environmental factors.
S0341	Skill to monitor threat effects to partner capabilities and maintain a running estimate.
S0342	Skill to optimize collection system performance through repeated adjustment, testing, and re-adjustment.
S0343	Skill to orchestrate intelligence planning teams, coordinate collection and production support, and monitor status.
S0344	Skill to prepare and deliver reports, presentations and briefings, to include using visual aids or presentation technology.
S0345	Skill to relate intelligence resources/assets to anticipated intelligence requirements.
S0346	Skill to resolve conflicting collection requirements.
S0347	Skill to review performance specifications and historical information about collection assets.
S0348	Skill to specify collections and/or taskings that must be conducted in the near term.
S0349	Skill to synchronize operational assessment procedures with the critical information requirement process.
S0350	Skill to synchronize planning activities and required intelligence support.
S0351	Skill to translate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.
S0352	Skill to use collaborative tools and environments for collection operations.
S0353	Skill to use systems and/or tools to track collection requirements and determine if they are satisfied.

Skill ID	Description
S0354	Skill in creating policies that reflect the business's core privacy objectives.
S0355	Skill in negotiating vendor agreements and evaluating vendor privacy practices.
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
S0357	Skill to anticipate new security threats.
S0358	Skill to remain aware of evolving technical infrastructures.
S0359	Skill to use critical thinking to analyze organizational patterns and relationships.
S0360	Skill to analyze and assess internal and external partner cyber operations capabilities and tools.
S0361	Skill to analyze and assess internal and external partner intelligence processes and the development of information requirements and essential information.
S0362	Skill to analyze and assess internal and external partner organization capabilities and limitations (those with tasking, collection, processing, exploitation and dissemination responsibilities).
S0363	Skill to analyze and assess internal and external partner reporting.
S0364	Skill to develop insights about the context of an organization's threat environment
S0365	Skill to design incident response for cloud service models.
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
S0369	Skill to identify sources, characteristics, and uses of the organization's data assets.
S0370	Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.
S0372	Skill to translate, track, and prioritize information needs and intelligence collection requirements across the extended enterprise.
S0374	Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations.