INFOSEC Skills

LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Cyber Threat Hunting 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.

Course description

The Internet is the new digital frontier, and like any frontier, it has a hundred things waiting to attack you. But sitting quietly and waiting to be jumped isn't the style of a real professional. Sharpen your skills and learn to hunt the threat on its own turf with Infosec's Cyber Threat Hunting Boot Camp.

This immersive three-day course will teach you about the latest tactics and tools used in the fight against hackers and cyber-attackers. Taught by industry professionals who have served as penetration testers, incident responders and computer forensic investigators, the Cyber Threat Hunting Boot Camp covers security analysis, establishing a secure threat-hunting setup, successful hunt patterns and liaising with security operations center personnel to cover all angles of attack while the threat is ongoing.

Who should attend

» Penetration testers
» Red team members and other white hats
» Incident-response team members
» Security analysts
» Engineers specializing in network security or IT
» Security consultants and auditors
» Managers wanting to create threat-hunting teams within their own companies

Boot camp at a glance

Hands-on training

- ✓ Practice threat hunting in a virtualized environment
- ✓ Learn how to hunt down different types of threats
- ✓ Gather logs, capture data and search for malware activity

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 3-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

- Three days of expert, live Cyber Threat Hunting training
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Onsite proctoring of exam
- Pre-study learning path
- Knowledge Transfer Guarantee

Prerequisites

- Understanding of fundamental information security concepts
- Working knowledge of networking devices and protocols
- Exposure to pentesting and network monitoring tools and methodologies
- Basic knowledge of Linux and Windows command line

What you'll learn

After attending the Cyber Threat Hunting Boot Camp, you will have the knowledge and skills to:

» Think tactically regarding cyber threat defense
» Use threat intelligence to form your own hypotheses and begin the hunt
» Anticipate and hunt down threats in your organization's systems
» Inspect network information to identify dangerous traffic
» Understand the Hunting Maturity Model to measure your organization's hunting capability
» Learn how to find and investigate malware, phishing, lateral movement, data exfiltration and other common threats

CCTHP exam objectives

The Certified Cyber Threat Hunting Professional (CCTHP) certification is designed to certify that candidates have expert-level knowledge and skills in cyber threat identification and threat hunting.

The CCTHP body of knowledge consists of five domains covering the responsibilities of a cyber threat hunter. The certification exam is a 50-question, traditional multiple-choice test. Questions are randomly pulled from a master list and must be completed in two hours. The five CCTHP domains are:

» Cyber threat hunting definition and goals
» Cyber threat hunting methodologies and techniques
» Hunting for network-based cyber threats
» Hunting for host-based cyber threats
» Cyber threat hunting technologies and tools

Hands-on labs

Hunt cyber threats with our practical exercises that present realistic attack scenarios. Practice threat hunting on our virtualized environment that simulates a full range of servers and services used in a real company. Learn how to hunt down various network- and host-based threats, gather and analyze logs and event data, capture memory dump and search for malware activity. The after-class CTF (Capture The Flag) exercises allow you to put everything you've learned together by hunting cyber threats on your own.

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott

Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam ... but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck

EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson

Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real-world scenarios that were able to be understood.

Erik Heiss

United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell

Salient Federal Solutions

Cyber Threat Hunting Boot Camp details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3
Morning session	Introduction to cyber threat hunting	Threat hunting techniques Preparing for the hunt	Utilizing system and security event data Advanced threat hunting concepts
Afternoon session	Threat hunting process Threat hunting methodologies	The hunt is on Hunting for network-based threats Hunting for host-based threats	CCTHP exam
Evening session	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth boot camp prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Day 1

Introduction to cyber threat hunting

» What is threat hunting?
» Assumption of breach
» The concept of active defense
» Role of threat hunting in organizational security program
» Threat hunting benefits

Threat hunting process

» Preparing for the hunt: the hunter, the data, the tools
» Creating a context-based hypothesis
» Starting the hunt (confirming the hypothesis)
» Responding to the attack
» Lessons learned

Threat hunting methodologies

» The Crown Jewel Analysis (CJA)
» Cyber threat patterns and signatures
» Utilizing threat intelligence
» Threat hunting hypotheses: intelligence-driven, awareness-driven, analytics-driven

Day 2

Threat hunting techniques

- Searching
- Cluster analysis
- Grouping
- Stack counting

Preparing for the hunt

- What data do you need and how to get it?
- Host and network visibility
- Data gathering and analysis tools
- Commercial and open-source threat hunting solutions

The hunt is on

- What threats can be hunted?
- Introduction to IOCs and artifacts
- IOCs and IOAs
- Cyber kill chain

Hunting for network-based threats

- Network hunting overview (networking concepts, devices and communications, hunting tools)
- Hunting for suspicious DNS requests and geographic abnormalities
- Hunting for DDoS Activity
- Hunting for suspicious domains,

URLs and HTML responses

- Hunting for irregular traffic: misused protocols, port-application mismatches, web shells and other threats

Hunting for host-based threats

- Endpoint hunting overview (Windows and Linux processes, file systems, registry, hunting tools)
- Malware (types, common activities, AV evasion, detection and analysis tools and methods)
- Hunting for irregularities in processes
- Hunting for registry and system file changes
- Hunting for filenames and hashes
- Hunting for abnormal account activity (bruteforce attacks, privileged accounts)
- Hunting for swells in database read volume
- Hunting for unexpected patching of systems

Day 3

Utilizing system and security event data

- Event logs and IDs
- Logging on Windows and Linux
- SIEM
- Using event data during hunts

Advanced threat hunting concepts

- OODA (Observe, Orient, Decide, Act) loop
- Going beyond IOCs: hunting for advanced threats
- Chokepoint monitoring
- Deceptive technologies
- Developing an effective threat-hunting program
- Building customized threat-hunting tools
- Threat hunting best practices and resources

CCTHP exam

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC