INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Cisco Certified CyberOps Associate 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).

Course description

There is a growing need for security professionals in the business world. As awareness of security threats grow, businesses of all sizes are beginning to understand the need for increased preparedness against these threats. Our Cisco Certified CyberOps Associate training (previously named CCNA Cyber Ops) is an excellent starting point for those interested in a career in this exciting, challenging and growing field.

This boot camp builds your foundation of cybersecurity knowledge and skills — with the goal of preparing you for the responsibilities of an entry-level security analyst working in a SOC. It also prepares you to validate your new skills by earning your Cisco Certified CyberOps Associate certification.

Who should attend

- Network engineers
- Network administrators
- Systems administrators
- System engineers
- IT managers/directors
- Anyone looking to improve their network skills

Boot camp at a glance

Certifications

- ✓ Cisco Certified CyberOps Associate

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 2-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

- Two days of expert, live instruction
- 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
- Knowledge Transfer Guarantee

Prerequisites

Prior to enrolling in our authorized Cisco Certified CyberOps Associate Boot Camp, you should have a sound working experience with basic network security and TCP/IP.

Cisco Certified CyberOps Associate overview

This boot camp prepares you to pass the new Understanding Cisco Cybersecurity Operations Fundamentals exam, which is required to become a Cisco Certified CyberOps Associate.

Topics covered in the exam include:

- Security concepts
- Security monitoring
- Host-based analysis
- Network intrusion analysis
- Security policies and procedures

Latest exam updates

On May 29, 2020, Cisco revamped its CCNA Cyber Ops certification and exam. The certification was renamed Cisco Certified CyberOps Associate, and — in line with other entry-level Cisco certifications — there is now only one exam to pass to get certified.

The new exam, Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS), replaced the previous Understanding Cisco Cybersecurity Fundamentals (210-250) and Implementing Cisco Cybersecurity Operations (210-255) exams, which were retired on May 28.

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

We had exactly what was needed to prepare us for our exams. The instructor was great. You could tell he loves teaching and was able to keep your attention and get the class to understand the material. I would recommend him as a teacher for CCNA to anyone.

Daniel Knight
Hillphoenix

An excellent instructor that obviously knows the material by heart. He was always clear and concise in his explanations and would break it down if anyone in the class didn't quite get how something worked. He is by far one of my favorite instructors ever, even though I only spent seven days with him.

Chris Soule
Rocky Gap Resort

My instructor was excellent. He made sure that I not only knew the information in order to pass my exams. He took it upon himself to teach us real-world knowledge that is necessary to do my job today.

Jeffrey McGill
TIC Gums, Inc.

My CCNA instructor has thus far been the best I've had throughout my career (being in the military, that is a LOT of training). He was extremely knowledgeable on the material and was extremely skilled at teaching it.

Shawn Tierney
United States Air Force

Cisco Certified CyberOps Associate 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	After class
Morning session	Security concepts Security monitoring	Network intrusion analysis (cont.) Security policies and procedures	Continue learning with 100s of courses included in your Infosec Skills subscription
Afternoon session	Security monitoring (cont.) Host-based analysis Network intrusion analysis	Exam prep Take 200-201 exam	
Evening session	Optional group & individual study		

Schedule may vary from class to class

Course Outline

Before your boot camp

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

Understanding Cisco Cybersecurity Operations Fundamentals (200-201)

Security concepts

- Describe the CIA triad
- Compare security deployments
  - Network, endpoint and application security systems
  - Agentless and agent-based protections
  - Legacy antivirus and antimalware
  - SIEM, SOAR and log management
- Describe security terms
  - Threat intelligence (TI)
  - Threat hunting
  - Malware analysis
  - Threat actor
  - Run book automation (RBA)
  - Reverse engineering
  - Sliding window anomaly detection
  - Principle of least privilege
  - Zero trust
  - Threat intelligence platform (TIP)
- Compare security concepts
  - Risk (risk scoring/risk weighting, risk reduction, risk assessment)
  - Threat
  - Vulnerability
  - Exploit
- Describe the principles of the defense-in-depth strategy
- Compare access control models
  - Discretionary access control
  - Mandatory access control
  - Nondiscretionary access control
  - Authentication, authorization, accounting
  - Rule-based access control
  - Time-based access control
  - Role-based access control

- Describe terms as defined in CVSS
  - Attack vector
  - Attack complexity
  - Privileges required
  - User interaction
  - Scope
- Identify the challenges of data visibility (network, host, and cloud) in detection
- Identify potential data loss from provided traffic profiles
- Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs
- Compare rule-based detection vs. behavioral and statistical detection

Security monitoring

- Compare attack surface and vulnerability
- Identify the types of data provided by these technologies
  - TCP dump
  - NetFlow
  - Next-gen firewall
  - Traditional stateful firewall
  - Application visibility and control
  - Web content filtering
  - Email content filtering
- Describe the impact of these technologies on data visibility
  - Access control list
  - NAT/PAT
  - Tunneling
  - TOR
  - Encryption
  - P2P
  - Encapsulation
  - Load balancing
- Describe the uses of these data types in security monitoring
  - Full packet capture
  - Session data
  - Transaction data
  - Statistical data
  - Metadata
  - Alert data
- Describe network attacks, such as protocolbased, denial of service, distributed denial of service and man-in-the-middle
- Describe web application attacks, such as SQL injection, command injections and crosssite scripting
- Describe social engineering attacks
- Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware and ransomware
- Describe evasion and obfuscation techniques, such as tunneling, encryption and proxies
- Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
- Identify the certificate components in a given scenario
- Cipher-suite
  - X.509 certificates
  - Key exchange
  - Protocol version
  - PKCS

Host-based analysis

- Describe the functionality of these endpoint technologies in regard to security monitoring
  - Host-based intrusion detection
  - Antimalware and antivirus
  - Host-based firewall
  - Application-level whitelisting/blacklisting
  - Systems-based sandboxing (such as Chrome, Java, Adobe Reader)
- Identify components of an operating system (such as Windows and Linux) in a given scenario
- Describe the role of attribution in an investigation
  - Assets
  - Threat actor
  - Indicators of compromise

- Indicators of attack
- Chain of custody

- Identify type of evidence used based on provided logs
  - Best evidence
  - Corroborative evidence
  - Indirect evidence
- Compare tampered and untampered disk image
- Interpret operating system, application, or command line logs to identify an event
- Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)
  - Hashes
  - URLs
  - Systems, events and networking

Network intrusion analysis

- UMap the provided events to source technologies
  - IDS/IPS
  - Firewall
  - Network application control
  - Proxy logs
  - Antivirus
  - Transaction data (NetFlow)
- Compare impact and no impact for these items
  - False positive
  - False negative
  - True positive
  - True negative
  - Benign
- Compare deep packet inspection with packet filtering and stateful firewall operation
- Compare inline traffic interrogation and taps or traffic monitoring
- Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic
- Extract files from a TCP stream when given a PCAP file and Wireshark
- Identify key elements in an intrusion from a given PCAP file
  - Source address
  - Destination address
  - Source port
  - Destination port
  - Protocols
  - Payloads
- Interpret the fields in protocol headers as related to intrusion analysis
  - Ethernet frame
  - IPv4
  - IPv6
  - TCP
  - UDP
  - ICMP
  - DNS
  - SMTP/POP3/IMAP
  - HTTP/HTTPS/HTTP2
  - ARP
- Interpret common artifact elements from an event to identify an alert
  - IP address (source / destination)
  - Client and server port identity
  - Process (file or registry)
  - System (API calls)
  - Hashes
  - URI / URL
- Interpret basic regular expressions

Security policies and procedures

- Describe management concepts
  - Asset management
  - Configuration management
  - Mobile device management
  - Patch management
  - Vulnerability management
- Describe the elements in an incident response plan as stated in NIST.SP800-61
- Apply the incident handling process (such as NIST.SP800-61) to an event
- Map elements to these steps of analysis based on the NIST.SP800-61

- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident analysis (lessons learned)

- Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800-61)
  - Preparation
  - Detection and analysis
  - Containment, eradication, and recovery
  - Post-incident analysis (lessons learned)
- Describe concepts as documented in NIST.SP800-86
  - Evidence collection order
  - Data integrity
  - Data preservation
  - Volatile data collection
- Identify these elements used for network profiling
  - Total throughput
  - Session duration
  - Ports used
  - Critical asset address space
- Identify these elements used for server profiling
  - Listening ports
  - Logged in users/service accounts
  - Running processes
  - Running tasks
  - Applications
- Identify protected data in a network
  - PII
  - PSI
  - PHI
  - Intellectual property
- Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain
  - Model and Diamond Model of Intrusion
- Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

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