Performing Cybersecurity Using Cisco Technologies

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Exam delivery in the classroom, with a **98% success rate**
- Course-specific thinQtank® Learning publications to make the learning fun and engaging
- Extended hours of training, including immersive hands-on exercises
- **We do not teach the test.** We always deliver valuable hands-on experience
- All reading material and study guides sent to you when you register
- Every course taught by CCIE expert instructors

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an **instructor-led training camp**, with the exam sat in the classroom as part of the camp. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and practical lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

RECOMMENDED KNOWLEDGE

- Familiarity with the Splunk search and navigation functions
- A basic understanding of scripting in one or more of Python, JavaScript or PHP
- Familiarity with UNIX and Linux shells (bash, csh) and shell commands

Cisco sets **no prerequisites** for this training. The above is what Cisco recommends you already have.

TARGET AUDIENCE

- Cybersecurity engineers and investigators
- Incident managers and incident responders
- Network engineers and SOC analysts at entry level with at least a year of experience
- Anyone working toward **CCNP Cybersecurity** certification

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

WHERE IT SITS

CCNP Cybersecurity takes two exams: this core, plus one concentration. Both concentrations were renamed in February 2026.

CBRCOR 350-201 CORE + **CBRFIR 300-215** or **CBRTHD 300-220** CONCENTRATION → **CCNP Cybersecurity**

CBRFIR is forensic analysis and incident response; CBRTHD is threat hunting and defending. Both titles now end “for Cybersecurity”.

COURSE OVERVIEW

thinQtank® Learning offers a unique instructor-led training camp for **Performing Cybersecurity Using Cisco Security Technologies**. As with all our Cisco training experiences, the exam is delivered in the classroom.

The course gives you the knowledge and skills to run security operations using cloud platforms and a **SecDevOps** methodology. You will learn the techniques for detecting cyberattacks, analyzing threats, and making the recommendations that improve an organization's security posture.

Coverage runs from governance, risk and SOC service models through analytics and playbooks, cloud responsibility models, asset management and zero trust, APIs and automation, packet and log investigation, threat tuning, threat intelligence, malware forensics, threat hunting and incident response.

350-201 is the **core exam** for CCNP Cybersecurity — the certification Cisco renamed from CyberOps Professional in February 2026. Passing it also earns **Cisco Certified Specialist — Cybersecurity Core**.

EXAM

350-201 CBRCOR — Performing Cybersecurity Using Cisco Security Technologies

120 minutes · course version v1.1. Cisco does not publish a question count or a pass mark for this exam, so this sheet does not state one.

The **core exam** for CCNP Cybersecurity. Pair it with one concentration exam to complete the certification. It also earns **Cisco Certified Specialist — Cybersecurity Core**, and carries **80 Continuing Education credits**.

Cisco renamed CyberOps Professional to **CCNP Cybersecurity** on 3 February 2026. The code and the CBRCOR alias are unchanged; the exam title moved from “Performing CyberOps” to “Performing Cybersecurity”. Verified on cisco.com, 31 August 2026.

EXCLUSIVE LEARNING PACKAGE

- Comprehensive video training package
- Virtual builds of every lab and hands-on learning objective, so you can keep practicing after the course ends
- Post-class **Office Hours** — interactive events giving you access to top instructors long after the class ends
- A Cisco acronym list to help you keep the key terms straight
- Tips and tricks for preparing, attending and reviewing
- Exam voucher included, and the exam delivered in the classroom

Performing Cybersecurity Using Cisco Technologies

COURSE OBJECTIVES

On completing this course you will be able to:

- Describe the types of service coverage within a SOC, and the operational responsibilities associated with each
- Compare the security operations considerations of cloud platforms
- Describe the general methodologies of SOC platform development, management and automation
- Describe asset segmentation, segregation, network segmentation and microsegmentation, and the approaches to each, as part of asset controls and protections
- Describe zero trust and its associated approaches, as part of asset controls and protections
- Perform incident investigations using SIEM and security orchestration and automation (SOAR)
- Use core security technology platforms for security monitoring, investigation and response
- Describe the DevOps and SecDevOps processes
- Describe the common data formats — JSON, HTML, XML and CSV
- Describe API authentication mechanisms
- Determine known indicators of compromise (IoCs) and indicators of attack (IoAs)
- Interpret events during an attack based on analysis of traffic patterns
- Describe the different security tools available for network analysis, and their limitations — packet capture, traffic analysis and network log analysis
- Analyze anomalous user and entity behavior (UEBA)
- Perform proactive threat hunting following best practice

COURSE OUTLINE

01 Understanding Risk Management and SOC Operations

- Governance, Risk and Compliance
- Security Regulatory Requirements
- Security Policy
- Protected Information
- Risk Analysis and Insurance
- SOC Services, Operations and Automation
- SOC Service Models

02 Understanding Analytical Processes and Playbooks

- Security Analytics
- SOC Playbook
- SOC Automation and Workflow
- Incident Response Concepts, Metrics and Workflow
- Documenting Security Incidents in Cases
- Security Orchestration, Automation and Response
- Cisco XDR
- Splunk Enterprise and Phantom Overview

03 Understanding Cloud Service Model Security Responsibilities

- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in the IaaS Service Model
- Security Responsibilities in the PaaS Service Model
- Security Responsibilities in the SaaS Service Model
- Cloud Deployment Models
- Key Security Controls in SaaS
- Cloud Access Security Broker
- Cisco Cloudlock
- Cloud Security Regulations and References

04 Understanding Enterprise Environment Assets

- Asset Management
- Remediating Vulnerabilities and the SOC
- Assessing Vulnerabilities
- Patch Management
- Data Storage and Protecting Data Privacy
- Multi-Factor Authentication
- Zero Trust Model

05 Understanding APIs

- API Overview
- CSV, HTML and XML Data Encoding
- JSON Data Encoding
- YAML Data Serialization Standard
- HTTP-Based APIs
- RESTful vs. Non-RESTful APIs
- Cisco pxGrid
- HTTP-Based Authentication
- Postman
- NETCONF
- Data Modeling with YANG
- RESTCONF
- gRPC
- STIX and TAXII Specifications
- Role of APIs in Cisco Security Solutions
- Python Fundamentals
- Python Virtual Environments

06 Understanding SOC Development and Deployment Models

- Agile Methodology
- DevOps Practices and Principles
- Components of a CI/CD Pipeline
- Essential Windows and Linux CLI for Development and Operations
- Infrastructure as Code
- SOC Platform Development, Engineering, Operation and Maintenance

Performing Cybersecurity Using Cisco Technologies

COURSE OUTLINE CONTINUED

07 Investigating Packet Captures, Logs and Traffic Analysis

- Identity Access Management Logs
- Artifacts and Traffic Streams in a Packet Capture
- Next-Generation Firewall and IPS Logs
- Dissecting Suspicious Requests
- Network Traffic Analysis Using NetFlow Analytics
- Detecting and Enforcing DLP On-the-Wire
- Cisco Secure Endpoint Architecture
- Cisco Secure Web Appliance
- Network DNS Logs
- Cisco Secure Email
- Email Security Logs (Not Detection-Based)
- Cisco Umbrella

08 Investigating Endpoint and Appliance Logs

- Cisco ISE Monitoring, Reporting and Alerting
- Cisco Secure Endpoint
- Cisco Secure Malware Analytics
- Endpoint Logs from Non-Detection Sources
- Server DNS Logs
- Internet of Things
- Web Security Logs
- Endpoint Data Loss Prevention

09 Implementing Threat Tuning

- Security Tuning Governance Policy
- Tuning Security Controls, Rules, Filters and Policies
- Determining If a Rule Is Defective
- Anatomy of a Snort Rule
- Troubleshooting Detection Rules
- Recommending Scenarios for Tuning

10 Threat Research and Threat Intelligence Practices

- Cyber Threat Intelligence Overview
- Cyber Threat Intelligence Lifecycle
- Cyber Threat Intelligence Data Sources
- Indicators of Compromise and Indicators of Attack
- Security Intelligence Reports
- Cyber Attribution
- Cyber Threat Intelligence Tools
- Security Intelligence in a TIP Platform
- Using Indicator Analysis to Reveal Hidden Infections

11 Performing Security Analytics and Reports in a SOC

- Security Data and Log Analytic Techniques
- Security Data Management Users
- Security Data with Log Management and Retention
- Security Data and Log Aggregation
- Security Information and Event Management
- Security Data and Log Analytics Automation
- Dashboards and Reports

12 Malware Forensics Basics

- Malware Detection Tools
- Static Malware Analysis from Detection Tools
- Dynamic Malware Analysis from Sandbox Logs
- File Fingerprinting for Attribution
- Evading Detection
- File Forensics

13 Threat Hunting Basics

- Proactive Threat Hunting Concepts
- Using the MITRE ATT&CK Framework for Threat Hunting
- Using CAPEC to Hunt for Weaknesses in Applications
- Evaluating Security Posture and Gaps in Controls Using MITRE ATT&CK
- Threat Hunting Case Study

14 Performing Incident Investigation and Response

- Threat Modeling
- Attack Campaigns, Tactics, Techniques and Procedures
- Steps to Investigate Potential Data Loss

LABS OUTLINE

01 Explore Cisco XDR
02 Explore Splunk Phantom Playbooks
03 Evaluate Assets in a Typical Enterprise Environment
04 Fix a Python API Script
05 Create Basic Bash Scripts
06 Examine Cisco Secure Firewall Packet Captures and PCAP Analysis
07 Validate an Attack and Determine the Incident Response
08 Submit a Sample to Cisco Secure Malware Analytics for Analysis
09 Endpoint-Based Attack Scenario Referencing MITRE ATT&CK
10 Explore Cisco Secure Firewall Access Control Policy and Snort Rules
11 Investigate IoCs Using Cisco XDR
12 Explore the ThreatConnect Threat Intelligence Platform
13 Track the TTPs of a Successful Attack Using a TIP
14 Reverse Engineer Malware
15 Perform Threat Hunting
16 Conduct an Incident Response