Understanding Cisco Cybersecurity Operations

thinQtank® LEARNING

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 expert, certified instructors

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an intensive, **extended-hours instructor-led boot camp**, with the exam sat in the classroom as part of the camp. The extended days are **entirely instructor-led** and cover the self-study content as well as the standard delivery — you are not sent away to work through it alone. That self-study material also arrives as part of the digital courseware on day one and should form part of your exam preparation. 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.

PREREQUISITES

- Basic familiarity with networking and the TCP/IP protocol suite
- Basic Windows and Linux operating system navigation
- Basic understanding of networking security concepts
- CCNA-level networking knowledge recommended (no formal prerequisite)

COURSE OBJECTIVES

On completing this course you will be able to:

- Explain how a security operations center (SOC) operates and the analyst's role
- Describe core security concepts including the CIA triad, defense in depth, and access control
- Interpret network telemetry, logs, events, and alerts from monitoring tools
- Perform host-based analysis on Windows and Linux endpoints
- Analyze packet captures, protocol headers, and network intrusion evidence
- Identify common attack vectors, reconnaissance, and malicious activity
- Recognize attack sequences across correlated security events
- Apply data normalization and event correlation to monitoring data
- Investigate suspicious traffic using the 5-tuple and NetFlow
- Handle digital evidence and maintain chain of custody
- Apply the incident response process, playbooks, and escalation
- Classify incidents by severity and triage alerts effectively
- Describe SOC metrics, workflow, and automation (SOAR)

COURSE OVERVIEW

thinQtank® Learning offers an industry-unique training camp in which students earn the **CCNA Cybersecurity certification** — formerly the Cisco Certified CyberOps Associate. As with all our Cisco training experiences, the exam is delivered in the classroom.

Understanding Cisco Cybersecurity Operations Fundamentals prepares you to work as an associate-level analyst in a threat-centric **security operations center (SOC)** — monitoring network telemetry, analyzing host and network intrusions, and responding to security incidents.

You will learn security concepts, security monitoring, host-based analysis, network intrusion analysis, and the security policies and procedures that govern incident response, with heavy hands-on work reading logs, packets, and endpoint evidence.

CCNA Cybersecurity is the associate-level foundation for a career in cybersecurity operations, and the single exam — **200-201** — is where that track begins.

EXAM

200-201 CCNACYBR — Understanding Cisco Cybersecurity Operations Fundamentals

This outline follows blueprint version 1.2.

One exam earns the **CCNA Cybersecurity certification** — the associate-level foundation for a threat-centric security operations (SOC) analyst role.

Cisco does not publish a fixed question count or passing score for this exam.

TARGET AUDIENCE

- Anyone looking to earn their CCNA Cybersecurity certification
- Aspiring and junior security operations center (SOC) analysts
- Cybersecurity analysts and incident responders
- Network engineers moving into security operations
- IT staff supporting security monitoring and response

DELIVERY METHODS

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

EXCLUSIVE LEARNING PACKAGE

- Comprehensive video training package
- Hundreds of pre-built labs for continued practice and learning
- Custom Linux builds for hands-on security analysis
- After-course instructor coaching benefits
- Exam voucher included, and the exam delivered in the classroom

Understanding Cisco Cybersecurity Operations

COURSE OUTLINE

01 Defining the Security Operations Center

- Types of Security Operations Centers
- SOC Analyst Tools and Responsibilities
- Data Analytics in a SOC
- Interacting with a SOC

02 Understanding Network Infrastructure and Monitoring Tools

- Network Fundamentals for Security
- Firewalls, IPS and Content Filtering
- Network Security Monitoring Tools
- Full Packet Capture and Session Data

03 Exploring Data Type Categories

- Network Telemetry and Data Types
- NetFlow and Session Data
- Transaction Data and Alert Data
- Statistical and Extracted Content Data

04 Understanding Basic Cryptography Concepts

- Cryptography Overview
- Hashing and Integrity
- Symmetric and Asymmetric Encryption
- Public Key Infrastructure and Certificates

05 Understanding Common TCP/IP Attacks

- Legacy TCP/IP Vulnerabilities
- IP and ICMP Vulnerabilities
- TCP and UDP Vulnerabilities
- Attack Surfaces and Attack Vectors

06 Understanding Endpoint Security Technologies

- Host-Based Firewalls and Antivirus
- Host-Based Intrusion Prevention
- Application Allow and Block Listing
- Sandboxing and Endpoint Detection and Response

07 Understanding Windows Operating System Basics

- Windows Processes, Threads and Services
- The Windows Registry and Event Logs
- Windows Management Tools
- Windows Networking and Security

08 Understanding Linux Operating System Basics

- Linux Processes, Forks and Daemons
- The Linux File System and Permissions
- Linux Logs, syslog and cron
- Linux Networking and Security

09 Understanding Incident Analysis in a Threat-Centric SOC

- The Cyber Kill Chain Model
- The Diamond Model of Intrusion
- MITRE ATT&CK and Threat Modeling
- Applying Models to Analysis

10 Identifying Resources for Hunting Cyber Threats

- Threat Intelligence Sources
- CVSS and Vulnerability Scoring
- Indicators of Compromise and Attack
- Security Data Analysis Resources

COURSE OUTLINE CONTINUED

11 Understanding Event Correlation and Normalization

- Data Normalization
- 5-Tuple Correlation
- Retrospective Analysis
- Deterministic vs Probabilistic Analysis

12 Identifying Common Attack Vectors

- Reconnaissance and Scanning
- Social Engineering and Phishing
- Web Application and DNS Attacks
- Command-and-Control and Exfiltration

13 Identifying Malicious Activity

- Interpreting Packet Captures
- Reading Protocol Headers
- IDS/IPS Alerts and Signatures
- Recognizing Traffic Anomalies

14 Identifying Patterns of Suspicious Behavior

- Baselines and Anomaly Detection
- Brute Force and Credential Attacks
- Lateral Movement and Persistence
- Beaconing and Encrypted Channels

15 Conducting Security Incident Investigations

- Evidence Collection and Handling
- Chain of Custody
- Order of Volatility
- Digital Forensics Fundamentals

16 Using a Playbook Model to Organize Security Monitoring

- Playbooks and Runbooks
- Analytic Processes
- Security Monitoring Workflow
- Escalation Procedures

17 Understanding SOC Metrics

- Security Data Aggregation
- Time to Detect and Time to Respond
- SOC Metrics and Key Performance Indicators
- Continuous Monitoring

18 Understanding SOC Workflow and Automation

- SOC Workflow Management and Case Management
- SOAR and Orchestration
- Automating Response Actions
- Continuous Improvement

19 Describing Incident Response

- The Incident Response Plan and Team
- The NIST Incident Response Lifecycle
- Containment, Eradication and Recovery
- Post-Incident Handling and Lessons Learned

20 Understanding Compliance and the Use of VERIS

- The VERIS Framework
- Data Retention and Compliance
- Regulatory Requirements
- Business Continuity Fundamentals

Understanding Cisco Cybersecurity Operations

LABS OUTLINE

01 Explore the Security Operations Center
02 Investigate Network Data with Security Tools
03 Categorize and Interpret Data Types
04 Apply Cryptographic Hashing and Verification
05 Analyze Common TCP/IP Attacks in a Capture
06 Examine Endpoint Security Technologies
07 Investigate Windows Endpoint Artifacts
08 Investigate Linux Endpoint Artifacts
09 Map an Intrusion to the Kill Chain and Diamond Model
10 Use Threat Intelligence and CVSS Scoring
11 Normalize and Correlate Security Events
12 Analyze NetFlow and Session Data
13 Identify Reconnaissance and Scanning Activity
14 Analyze a Packet Capture for Malicious Activity
15 Read IDS/IPS Alerts and Signatures
16 Investigate DNS and Web-Based Attacks
17 Detect Brute Force and Lateral Movement
18 Investigate a Security Incident End to End
19 Preserve Evidence and Maintain Chain of Custody
20 Build and Follow a Security Monitoring Playbook
21 Triage and Classify Alerts by Severity
22 Automate a Response with a SOAR Workflow
23 Apply the NIST Incident Response Lifecycle
24 Document an Incident Using VERIS

TERMS

thinQtank® LEARNING