THINQTANK® LEARNING

CISCO CCNP CYBERSECURITY
Performing Cybersecurity Using Cisco Security Technologies (CBRCOR)

Our Learning Exclusive

- Custom exam prep software and materials
- Exam delivery in classroom with 98% success
- Course specific thinQtank® Learning publications to promote fun exciting learning
- Extended hours of training including immersive hands-on exercises
- WE DO NOT "TEACH THE TEST" We always deliver valuable hands-on experience
- Receive all reading material and study guides when you register
- All courses taught by CCIE expert instructors

Course Duration

- Five days of instructor-led learning
- 60% lecture, 40% hands-on labs

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

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

Target Audience

- Cybersecurity Engineers/Investigators
- Incident Managers/Responders
- Network Engineers and SOC Analysts currently functioning at entry level with a minimum of 1 year of experience

Exam Information

- 350-201 – Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Delivery Methods

- Instructor-Led Training
- Immersive Live-Online Training
- On-Site and Custom Delivery

Exclusive Tools and Learning Package

- Comprehensive video training package
- Virtual builds of all labs and hands-on learning objectives to continue hands-on experience after course completion
- Industry-unique training course to achieve multiple certifications in one training camp
- Post-class ongoing "Office Hours" events: Interactive events grant you access to top instructors long after your class is completed to ensure that you successfully utilize what you've learned.
- Cisco-related Acronym List to help you understand key terms
- Tips & Tricks: From preparing for your course through post-class review, these tips will help you to apply your new knowledge

Course Overview

thinQtank® Learning is offering a unique five-day training camp comprised of five days of instructor-led learning that gives students the knowledge and skills needed to implement cybersecurity using Cisco technologies. The Performing Cybersecurity Using Cisco Security Technologies (CBRCOR) course guides you through the fundamentals, methods, and automation of cybersecurity operations. The knowledge you gain in this training will prepare you for the role of Information Security Analyst on a Security Operations Center (SOC) team. You will learn foundational concepts and their application in real-world scenarios, as well as how to leverage playbooks to formulate an Incident Response (IR). The training teaches you how to use automation for security using cloud platforms and a SecDevOps methodology. You will learn the techniques for detecting cyberattacks, analyzing threats, and making appropriate recommendations to improve cybersecurity.

Course Objectives

Upon successful completion of this course, you should be able to:

- Describe the types of service coverage within a SOC and operational responsibilities associated with each
- Compare security operations considerations of cloud platforms
- Describe the general methodologies of SOC platforms development, management, and automation
- Describe asset segmentation, segregation, network segmentation, microsegmentation, and approaches to each, as part of asset controls and protections
- Describe Zero Trust and associated approaches, as part of asset controls and protections
- Perform incident investigations, Security Information and Event Management (SIEM), security orchestration and automation (SOAR)
- Use different types of core security technology platforms for security monitoring, investigation, and response
- Describe the DevOps and SecDevOps processes
- Describe the common data formats (e.g., JavaScript Object Notation (JSON), HTML, XML, and Comma-Separated Values (CSV))
- Describe API authentication mechanisms
- Analyze the approach and strategies of threat detection during monitoring, investigation, and response
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs)
- Interpret events during an attack based on analysis of traffic patterns
- Describe different security tools and limitations for network analysis (e.g., packet capture, traffic analysis, and network log analysis tools)
- Analyze anomalous user and entity behavior (UEBA)
- Perform proactive threat hunting following best practices

THINQTANK® LEARNING

CISCO CCNP CYBERSECURITY
Performing Cybersecurity Using Cisco Security Technologies (CBRCOR)

Course Outline

1 Section 1: 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

2 Section 2: 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

3 Section 3: Understanding Cloud Service Model Security Responsibilities
- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in the laaS 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

4 Section 4: 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

5 Section 5: Understanding APIs
- API Overview
- CSV, HTML, and XML Data Encoding
- JSON Data Encoding
- YAML Data Serialization Standard
- HTTP-Based APIs
- RESTful APIs vs. Non-RESTful APIs
- Cisco pxGrid
- HTTP-Based Authentication
- Postman
- NETCONF
- Data Modeling with YANG
- RESTCONF
- Google RPC
- STIX and TAXII Specifications
- Role of APIs in Cisco Security Solutions
- Python Fundamentals
- Python Virtual Elements

6 Section 6: 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

7 Section 7: Investigating Packet Captures, Logs, and Traffic Analysis
- Identity Access Management Logs
- Artifacts and Traffic Streams in a Packet Capture
- Nextgen Firewall and IPS Logs
- Dissecting Suspicious Requests
- Network Traffic Analysis Using NetFlow Analytics
- Detecting and Enforcing DLP On-the-Wire
- Cisco AMP Architecture
- Cisco Web Security Appliance
- Network DNS Logs
- Cisco Email Security Appliance
- Email Security Logs (Not Detection-Based)
- Cisco Umbrella

8 Section 8: Investigating Endpoint and Appliance Logs
- Cisco ISE Monitoring, Reporting, and Alerting
- Cisco Advanced Malware Protection
- Cisco Threat Grid
- Endpoint Logs from Non-Detection Sources
- Server DNS Logs
- Internet of Things
- Web Security Logs
- Endpoint Data Loss Prevention

CISCO CCNP CYBERSECURITY
Performing Cybersecurity Using Cisco Security Technologies (CBRCOR)

Course Outline Continued

9 Section 9: 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 Section 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 Section 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 Aggregations
- Security Information and Event Management
- Security Data and Log Analytics Automation
- Dashboards and Reports

12 Section 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 Section 13: Threat Hunting Basics
- Proactive Threat Hunting Concepts
- Using MITRE ATTACK@ Framework for Threat Hunting
- Using CAPEC to Hunt for Weaknesses in Applications
- Evaluating Security Posture and Gaps in Controls Using MITRE ATTACK®
- Threat Hunting Case Study

14 Section 14: Performing Incident Investigation and Response
- Threat Modeling
- Attack Campaigns, Tactics, Techniques, and Procedures
- Steps to Investigate Potential Data Loss

Labs Outline

- Explore Cisco XDR
- Explore Splunk Phantom Playbooks
- Evaluate Assets in a Typical Enterprise Environment
- Fix a Python API Script
- Create Bash Basic Scripts
- Examine Cisco Firepower Packet Captures and PCAP Analysis
- Validate an Attack and Determine the Incident Response
- Submit a Sample to Cisco Secure Malware Analytics for Analysis
- Endpoint-Based Attack Scenario Referencing MITRE ATTACK®
- Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
- Investigate IOCs using Cisco XDR
- Explore the ThreatConnect Threat Intelligence Platform
- Track the TTPs of a Successful Attack Using a TIP
- Reverse Engineer Malware
- Perform Threat Hunting
- Conduct an Incident Response

CISCO CCNP CYBERSECURITY
Performing Cybersecurity Using Cisco Security Technologies (CBRCOR)

thinQtank® Global, Inc. dba thinQtank® Learning P.O. Box 803215, Valencia, CA 91380 USA
Tel 855-TO-THINQ Fax 208-979-0668 www.thinqtanklearning.com