Performing CyberOps Using Cisco Security Technologies (CBRCOR) v.1.2

Duration: 40 Hours (5 Days)

Overview

The Performing CyberOps Using Cisco Security Technologies (CBRCOR) training guides you through cybersecurity operations fundamentals, methods, and automation. 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, and how to leverage playbooks in formulating 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.

This training also earns you 40 Continuing Education (CE) credits towards recertification and prepares you for the 350-201 CBRCOR core exam.

Audience Profile

- Cybersecurity engineer
- Cybersecurity investigator
- Incident manager
- Incident responder
- Network engineer

This course prepares you to take the exam:

350-201 CBRCOR core exam

How You'll Benefit

- Gain an advanced understanding of the tasks involved for senior-level roles in a security operations center
- Configure common tools and platforms used by security operation teams via practical application
- Prepare you to respond like a hacker in real-life attack scenarios and submit recommendations to senior management
- Prepare for the 350-201 CBRCOR core exam
- Earns you 40 Continuing Education (CE) credits towards recertification

Who Should Enroll

- Network engineers
- Systems engineers
- Network Security engineers
- Consulting systems engineers
- Technical solutions architects
- Field engineers
- Cisco integrators and partners
- Server administrator
- SOC Engineer

What to Expect in the Exam

350-201 Performing CyberOps Using Cisco Security Technologies (CBRCOR) is a 120-minute exam associated with the Cisco CyberOps Professional Certification. The multiple-choice format tests knowledge of core cybersecurity operations including cybersecurity fundamentals, techniques, policies, processes, and automation. The exam will test for knowledge in the following areas:

- Monitoring for cyberattacks
- Analyzing high volume of data using automation tools and platforms—both open source and commercial
- Accurately identifying the nature of attack and formulate a mitigation plan
- Scenario-based questions; for example, using a screenshot of output from a tool, you may be asked to interpret portions of output and establish conclusions

Course Prerequisites

Although there are no mandatory prerequisites, to fully benefit from this training, you should have the following knowledge:

- Familiarity with UNIX/Linux shells (bash, csh) and shell commands.
- Familiarity with the Splunk search and navigation functions

- Basic understanding of scripting using one or more of Python, JavaScript, PHP or similar.

Recommended Cisco offering that may help you prepare for this training:

- Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)
- Implementing and Administering Cisco Solutions (CCNA)

Recommended third-party resources:

- Splunk Fundamentals 1
- Blue Team Handbook: Incident Response Edition by Don Murdoch
- Threat Modeling- Designing for Security y Adam Shostack
- Red Team Field Manual by Ben Clark
- Blue Team Field Manual by Alan J White
- Purple Team Field Manual by Tim Bryant
- Applied Network Security and Monitoring by Chris Sanders and Jason Smith

)

Course Outline

After taking this training, 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.
- Explain asset segmentation, segregation, network segmentation, micro-segmentation, 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 using Security Information and Event Management (SIEM) and/or security orchestration and automation (SOAR) in the SOC.
- Use different types of core security technology platforms for security monitoring, investigation, and response.
- Describe the DevOps and SecDevOps processes.
- Explain the common data formats, for example, JavaScript Object Notation (JSON), HTML, XML, 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 the sequence of events during an attack based on analysis of traffic patterns.
- Describe the different security tools and their limitations for network analysis (for example, packet capture tools, traffic analysis tools, network log analysis tools).
- Analyze anomalous user and entity behavior (UEBA).
- Perform proactive threat hunting following best practices.

Lab Outline

- Explore Cisco SecureX Orchestration
- Explore Splunk Phantom Playbooks
- Examine Cisco Firepower Packet Captures and PCAP Analysis
- Validate an Attack and Determine the Incident Response
- Submit a Malicious File to Cisco Threat Grid for Analysis
- Endpoint-Based Attack Scenario Referencing MITRE ATTACK
- Evaluate Assets in a Typical Enterprise Environment
- Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
- Investigate IOCs from Cisco Talos Blog Using Cisco SecureX
- Explore the ThreatConnect Threat Intelligence Platform
- Track the TTPs of a Successful Attack Using a TIP
- Query Cisco Umbrella Using Postman API Client
- Fix a Python API Script
- Create Bash Basic Scripts
- Reverse Engineer Malware
- Perform Threat Hunting
- Conduct an Incident Response