Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.2

Duration: 40 Hours (5 Days)

Overview

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) training teaches you security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This training teaches you how to monitor alerts and breaches, and how to understand and follow established procedures for response to alerts converted to incidents. Through a combination of lecture, hands-on labs, and self-study, you will learn the essential skills, concepts, and technologies to be a contributing member of a Cybersecurity Operations Center (SOC) including understanding the IT infrastructure, operations, and vulnerabilities. This training helps you prepare for the Cisco Certified CyberOps Associate certification and the role of a Junior or Entry-level cybersecurity operations analyst in a SOC. This training also earns you 30 Continuing Education (CE) credits towards recertification.

This training also earns you 30 Continuing Education (CE) credits towards recertification and prepares you for the 300-201 CBRCOR core exam.

Audience Profile

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

This course prepares you to take the exam:

300-201 CBROPS

How You'll Benefit

This training will help you:

- Learn the fundamental skills, techniques, technologies, and the hands-on practice necessary to prevent and defend against cyberattacks as part of a SOC team
- Prepare for the 200-201 Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) exam which earns the Cisco Certified CyberOps Associate certification
- This training also earns you 30 Continuing Education (CE) credits

Who Should Enroll

This training is designed for individuals seeking a role as an associate-level cybersecurity analyst and IT professionals desiring knowledge in Cybersecurity operations or those in pursuit of the Cisco Certified CyberOps Associate certification including:

- Students pursuing a technical degree
- Current IT professionals
- Recent college graduates with a technical degree

- Network engineers
- Systems engineers
- Network Security engineers
- Technical solutions architects
- SOC Engineer

What to Expect in the Exam

- Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) v1.2 is a 120-minute exam that certifies a candidate’s knowledge and skills related to security concepts, security monitoring, host based analysis, network intrusion analysis, and security policies and procedures.

Course Prerequisites

Before taking this training, you should have the following knowledge and skills:

- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with basics of networking security concepts

The following Cisco training can help you gain the knowledge you need to prepare for this training:

- Implementing and Administering Cisco Solutions (CCNA®)

Course Outline

After taking this training, you should be able to:

- Explain how a Security Operations Center (SOC) operates and describe the different types of services that are performed from a Tier 1 SOC analyst’s perspective.
- Explain Network Security Monitoring (NSM) tools that are available to the network security analyst.
- Explain the data that is available to the network security analyst.
- Describe the basic concepts and uses of cryptography.
- Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts.
- Understand common endpoint security technologies.
- Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors.
- Identify resources for hunting cyber threats.
- Explain the need for event data normalization and event correlation.
- Identify the common attack vectors.
- Identify malicious activities.
- Identify patterns of suspicious behaviors.
- Conduct security incident investigations.
- Explain the use of a typical playbook in the SOC.
- Explain the use of SOC metrics to measure the effectiveness of the SOC.
- Explain the use of a workflow management system and automation to improve the effectiveness of the SOC.

- Describe a typical incident response plan and the functions of a typical Computer Security Incident Response Team (CSIRT).
- Explain the use of Vocabulary for Event Recording and Incident Sharing (VERIS) to document security incidents in a standard format.

Lab Outline

- Use NSM Tools to Analyze Data Categories
- Explore Cryptographic Technologies
- Explore TCP/IP Attacks
- Explore Endpoint Security
- Investigate Hacker Methodology
- Hunt Malicious Traffic
- Correlate Event Logs, Packet Captures (PCAPs), and Alerts of an Attack
- Investigate Browser-Based Attacks
- Analyze Suspicious Domain Name System (DNS) Activity
- Explore Security Data for Analysis
- Investigate Suspicious Activity Using Security Onion
- Investigate Advanced Persistent Threats
- Explore SOC Playbooks
- Explore the Windows Operating System
- Explore the Linux Operating System