FIREFLY

CONTACT US

Understanding Cisco Cybersecurity Operations Fundamentals

DURATION: 5 DAYS COURSE CODE: CBROPS FORMAT: LIVE/VIRTUAL

COURSE DESCRIPTION

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0 course teaches you security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This course 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 course 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.

WHO SHOULD ATTEND

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

Students pursing a technical degree

PREREQUISITES

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 course can help you gain the knowledge you need to prepare for this course:

- Implementing and Administering Cisco Solutions (CCNA®)

LEARNING OBJECTIVES

This course 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

After taking this course, 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.

COURSE OUTLINE

1. Defining the Security Operations Center
2. Understanding Network Infrastructure and Network Security Monitoring Tools
3. Exploring Data Type Categories
4. Understanding Basic Cryptography Concepts
5. Understanding Common TCP/IP Attacks
6. Understanding Endpoint Security Technologies
7. Understanding Incident Analysis in a Threat-Centric SOC
8. Identifying Resources for Hunting Cyber Threats
9. Understanding Event Correlation and Normalization
10. Identifying Common Attack Vectors
11. Identifying Malicious Activity
12. Identifying Patterns of Suspicious Behavior
13. Conducting Security Incident Investigations
14. Using a Playbook Model to Organize Security Monitoring
15. Understanding SOC Metrics
16. Understanding SOC Workflow and Automation
17. Describing Incident Response
18. Understanding the Use of VERIS
19. Understanding Windows Operating System Basics
20. Understanding Linux Operating System Basics

COURSE OUTLINE

1. Use SIEM Tools to Analyze Data Categories
2. Explore Cryptographic Technologies
3. Explore TCP/IP Attacks
4. Explore Endpoint Security
5. Investigate Hacker Methodology
6. Hunt Malicious Traffic
7. Correlate Event Logs, Packet Captures (PCAPs), and Alerts of an Attack
8. Investigate Browser-Based Attacks
9. Analyze Suspicious Domain Name System (DNS) Activity
10. Explore Security Data for Analysis
11. Investigate Suspicious Activity Using Security Onion
12. Investigate Advanced Persistent Threats
13. Explore SOC Playbooks
14. Explore the Windows Operating System
15. Explore the Linux Operating System