Understanding Cisco Cybersecurity Operations Fundamentals 5 Days

Course Overview

The **Understanding Cybersecurity Operations Fundamentals (CBROPS) v1.0** course teaches an understanding of the network infrastructure devices, operations, and vulnerabilities of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. You will learn basic information about security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data used to investigate security incidents. After completing this course, you will have the basic knowledge required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center to strengthen network protocol, protect your devices and increase operational efficiency. This course prepares you for the **Cisco Certified CyberOps Associate** certification.

Who should attend

This course is designed for an associate-level cybersecurity analyst who is working in security operation centers.

Prerequisites

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

- Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA)
- 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)

After taking this course, you should be able to:

- Explain how a 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 CSIRT.
- Explain the use of VERIS to document security incidents in a standard format.
- Describe the Windows operating system features and functionality.
- Describe the Linux operating system features and functionality.

This course will help you:

- Gain the knowledge and skills to implement protocol that modernizes and tailors your network infrastructure.
- Learn hands-on training to streamline, design, and configure security measures to fortify your networks against Cybersecurity attacks.

Detailed Course Outline

- Defining the Security Operations Center Understanding Network Infrastructure and NetworkSecurity
- Monitoring Tools
- Exploring Data Type Categories Understanding Basic Cryptography Concepts Understanding
- Common TCP/IP Attacks Understanding Endpoint Security Technologies
- Understanding Incident Analysis
- in a Threat-CentricSOC
- Identifying Resources for Hunting Cyber Threats Understanding Event Correlation and Normalization
- Identifying Common Attack Vectors
- Identifying Malicious Activity
- Identifying Patterns of Suspicious Behavior Conducting Security Incident Investigations Using a Playbook
- Model to Organize SecurityMonitoring
- Understanding SOC Metrics
- Understanding SOC Workflow and AutomationDescribing Incident Response
- Understanding the Use of VERIS
- Understanding Windows Operating System BasicsUnderstanding Linux Operating System Basics
-

Lab Outline

- Configure the Initial Collaboration Lab EnvironmentUse NSM Tools to Analyze Data Categories
- Explore Cryptographic Technologies
- ExploreTC/IP Attacks Explore Endpoint Security
- Investigate Hacker MethodologyHunt Malicious Traffic
- Correlate Event Logs, PCAPs, and Alerts of an AttackInvestigate Browser-Based Attacks
- Analyze Suspicious DNS Activity Explore Security Data for Analysis
- Investigate Suspicious Activity Using Security OnionInvestigate Advanced Persistent Threats
- Explore SOC Playbooks
- Explore the Windows Operating SystemExplore the Linux Operating System
-