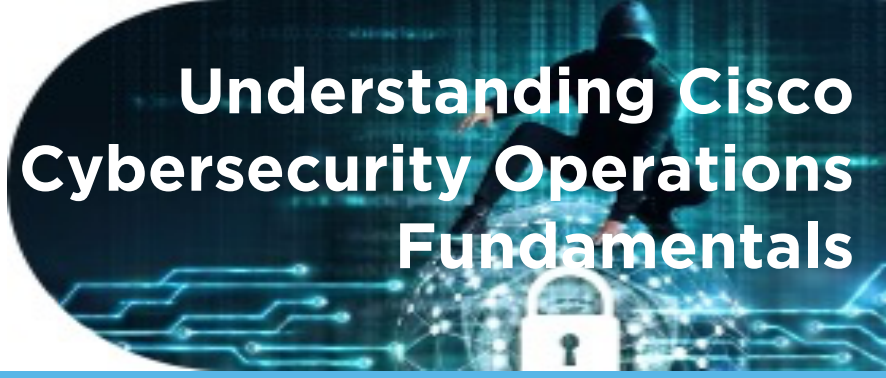
Platinum Learning Partner

Business Learning Partner

Understanding Cisco Cybersecurity Operations Fundamentals



CBROPS: 200-201

Course Overview

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 centre (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.

Prerequisite Knowledge

To fully benefit from this course, 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 course can help you gain the knowledge you need to prepare for this course:

- Implementing and Administering Cisco Solutions (CCNA®)

Real skills for real engineers

Understanding Cisco Cybersecurity Operations Fundamentals

Objectives

Upon completing this course, the learner will be able to meet these overall objectives:

- Explain how a Security Operations Centre (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 behaviours.
- 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.