Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Description

Understanding Cisco’s Cybersecurity Operations Fundamentals

The Understanding Cisco’s Cybersecurity Operations Fundamentals (CBROPS) course is designed to provide you with essential skills in network security. By diving into threat analysis, you will learn to identify, investigate, and respond effectively to cyberattacks. Through hands-on exercises and comprehensive training, you will master key tools and concepts to ensure the security of critical infrastructures.

Intended for cybersecurity analysts working in a Security Operations Center (SOC), this course will equip you with the foundational knowledge necessary to understand and manage cyber threats. You will also explore incident analysis techniques, event correlation methods, and data normalization processes. This course is a crucial step for those looking to specialize in cybersecurity and pursue the Cisco Certified CyberOps Associate certification.

Niveau
Intermédiaire
Course Content
Module 1: Defining the Security Operations Center

- Understand the roles and responsibilities of a SOC
- Identify different types of SOCs

Module 2: Understanding Network Infrastructure and Security Monitoring Tools

- Use NSM tools
- Analyze network data

Module 3: Exploring Data Categories

- Classify the types of data used in a SOC

Module 4: Understanding Cryptography Basics

- Utilize cryptography techniques

Module 5: Understanding Common TCP/IP Attacks

- Identify security vulnerabilities

Module 6: Understanding Endpoint Security Technologies

- Protect endpoints

Module 7: Understanding Incident Analysis in a Threat-Centric SOC

- Analyze security incidents

Module 8: Identifying Resources for Threat Hunting

- Hunt for cyber threats

Module 9: Understanding Event Correlation and Normalization

- Correlate and normalize security data

Module 10: Identifying Common Attack Vectors

- Understand cyberattack behavior patterns

Module 11: Conducting Security Incident Investigations

- Explore SOC Playbooks

Module 12: Understanding Windows and Linux Operating System Basics

- Explore Windows and Linux systems in a SOC

Lab / Exercises

- Set up the initial collaboration lab environment
- Use NSM tools to analyze data categories
- Explore cryptographic technologies
- Explore TCP/IP attacks
- Explore endpoint security
- Study hacker methodology
- Hunt for malicious traffic
- Correlate event logs, PCAPs, and attack alerts
- Investigate browser-based attacks
- Analyze suspicious DNS activities
- Explore security data for analysis
- Investigate suspicious activities using Security Onion
- Investigate advanced persistent threats
- Explore SOC Playbooks
- Explore the Windows operating system
- Explore the Linux operating system

Documentation

- Digital course materials included

Participant profiles

- Cybersecurity analysts
- Network and security technicians
- System administrators
- IT professionals seeking cybersecurity specialization

Prerequisites

- Knowledge of TCP/IP networks
- Skills in Windows and Linux operating systems
- Basic understanding of network security
- Familiarity with network monitoring tools

Objectives

- Define the role of a SOC
- Use network monitoring tools
- Analyze network data to detect threats
- Understand cryptography basics
- Identify and correlate security events
- Conduct investigations on cyberattacks

Description
Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) training
Classroom Registration Price (CHF)
4350
Virtual Classroom Registration Price (CHF)
4350
Duration (in Days)
5
Reference
CBROPS