

Implementing Cisco Cybersecurity Operations (SECOPS) v1.0

Duración: 5 días, 35 horas.

Overview:

Today's organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOC's) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats. CCNA Cyber Ops prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers..

Course Prerequisites

It is recommended, but not required, to have the following skills and knowledge before attending this course:

- Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1)
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts

Course Description

This course allows learners to understand how a Security Operations Center (SOC) functions and the introductory-level skills and knowledge needed in this environment. It focuses on the introductory-level skills needed for a SOC Analyst at the associate level. Specifically, understanding basic threat analysis, event correlation, identifying malicious activity, and how to use a playbook for incident response.

Course Objectives

- Upon completion of this course, you will be able to:
- Define a SOC and the various job roles in a SOC
- Understand SOC infrastructure tools and systems
- Learn basic incident analysis for a threat centric SOC
- Explore resources available to assist with an investigation
- Explain basic event correlation and normalization
- Describe common attack vectors
- Learn how to identifying malicious activity
- Understand the concept of a playbook
- Describe and explain an incident respond handbook
- Define types of SOC Metrics
- Understand SOC Workflow Management system and automation

Job Roles

- Security Operations Center – Security Analyst
- Computer/Network Defense Analysts
- Computer Network Defense Infrastructure Support Personnel
- Future Incident Responders and Security Operations Center (SOC) personnel.
- Students beginning a career, entering the cybersecurity field.
- Cisco Channel Partners

Course Outline

- Module 1: SOC Overview
 - Lesson 1: Defining the Security Operations Center
 - Lesson 2: Understanding NSM Tools and Data
 - Lesson 3: Understanding Incident Analysis in a Threat-Centric SOC
 - Lesson 4: Identifying Resources for Hunting Cyber Threats

Module 2: Security Incident Investigations

- Lesson 1: Understanding Event Correlation and Normalization
- Lesson 2: Identifying Common Attack Vectors
- Lesson 3: Identifying Malicious Activity
- Lesson 4: Identifying Patterns of Suspicious Behavior
- Lesson 5: Conducting Security Incident Investigations

Module 3: SOC Operations

- Lesson 1: Describing the SOC Playbook
- Lesson 2: Understanding the SOC Metrics
- Lesson 3: Understanding the SOC WMS and Automation
- Lesson 4: Describing the Incident Response Plan
- Lesson 5: Appendix A—Describing the Computer Security Incident Response Team
- Lesson 6: Appendix B—Understanding the use of VERIS

Lab Outline

Guided Lab 1: Explore Network Security Monitoring Tools

- Discovery 1: Investigate Hacker Methodology
- Discovery 2: Hunt Malicious Traffic
- Discovery 3: Correlate Event Logs, PCAPs, and Alerts of an Attack
- Discovery 4: Investigate Browser-Based Attacks
- Discovery 5: Analyze Suspicious DNS Activity
- Discovery 6: Investigate Suspicious Activity Using Security Onion
- Discovery 7: Investigate Advanced Persistent Threats
- Discovery 8: Explore SOC Playbooks

Exam Description

This exam is the second of the two required exams in achieving the associate-level CCNA Cyber Ops certification and prepares candidates to begin a career within a Security Operations Center (SOC), working with Cybersecurity Analysts at the associate level. The SECFND exam tests a candidate's knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a SOC.