Implementing Cisco Cybersecurity Operations - (SECOPS)

Course Details

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

Labs:

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