Cisco® Implementing Cisco® Cybersecurity Operations v1.0 (SECOPS)

Course Overview

This is a 5-day class

Learn how a Security Operations Center (SOC) functions and gain the introductory-level skills and knowledge required for success.

Who Should Attend

Security Operations Center Security Analyst
Computer Network Defense Analyst
Computer Network Defense Infrastructure Support personnel
Future Incident Responders and Security Operations Center (SOC) personnel
Students beginning a career and entering the cybersecurity field
IT personnel looking to learn more about the area of cybersecurity operations
Cisco Channel Partners

Course Objectives

The goal of the course is to teach the fundamental skills required to begin a career working as an associate-level cybersecurity analyst in a security operations center.

Course Outline

1 SOC OVERVIEW

Defining the Security Operations Center
Understanding NSM Tools and Data
Understanding Incident Analysis in a Threat-Centric SOC
Identifying Resources for Hunting Cyber Threats

2 SECURITY INCIDENT INVESTIGATIONS

Understanding Event Correlation and Normalization
Identifying Common Attack Vectors
Identifying Malicious Activity
Identifying Patterns of Suspicious Behavior
Conducting Security Incident Investigations

3 SOC OPERATIONS

Describing the SOC Playbook
Understanding the SOC Metrics
Understanding the SOC WMS and Automation
Describing the Incident Response Plan
Appendix A—Describing the Computer Security Incident Response Team
Appendix B—Understanding the use of VERIS

4 LABS

Explore Network Security Monitoring Tools