FIREFLY

CONTACT US

Implementing Cisco Cybersecurity Operations

DURATION: 5 DAYS COURSE CODE: SECOPS FORMAT: LIVE/VIRTUAL

COURSE DESCRIPTION

The Implementing Cisco Cybersecurity Operations (SECOPS) v1.0 course gives you foundation-level knowledge of security incident analysis techniques used in a Security Operations Center (SOC). You will learn how to identify and analyze threats and malicious activity, correlate events, conduct security investigations, use incident playbooks, and learn SOC operations and procedures. This is the second of two courses that prepare you for the Cisco® CCNA® Cyber Ops certification. This certification validates your knowledge and hands-on skills to help handle cybersecurity events as an associate-level member of an SOC team.

Today's cybersecurity professionals need to detect, investigate, and respond to a wide variety of security events. This course will help you gain the skills to play a role in your organization's SOC detecting and responding to security events.

The United States Department of Defense recognizes Cisco CCNA CyberOps certification as an approved baseline certification in the Information Assurance (IA) Workforce CCSP Incident Responder and CCSP Analyst job categories. Please see Cisco CCNA CyberOps and the DoD Approved 8570 Baseline Certifications for more information.

WHO SHOULD ATTEND

IT professionals

Any learner interested in entering associate-level cybersecurity roles such as:

- SOC cybersecurity analysts
- Computer or network defense analysts
- Computer network defense infrastructure support personnel
- Future incident responders and SOC personnel
- Cisco integrators or partners

PREREQUISITES

To fully benefit from this course, you should first complete the following course or obtain the equivalent knowledge and skills:

- Understanding Cisco Cybersecurity Fundamentals (SECFND)

The following Cisco learning offering can help you meet this prerequisite:

CCNA Cyber Ops SECFND #210-250 Official Cert Guide

LEARNING OBJECTIVES

Describe the three common SOC types, tools used by SOC analysts, job roles within the SOC, and incident analysis within a threat-centric SOC

Explain security incident investigations, including event correlation and normalization and common attack vectors, and be able to identify malicious and suspicious activities

Explain the use of a SOC playbook to assist with investigations, the use of metrics to measure the effectiveness of the SOC, the use of a SOC workflow management system and automation to improve SOC efficiency, and the concepts of an incident response plan

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

DISCOVERY LABS

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