

# Implementing Cisco Cybersecurity Operations (SECOPS) v1.0

## What you'll learn in this course

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 course prepares you for the 210-255 SECOPS exam, one of the two exams for the current Cisco Certified CyberOps Associate\* 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 (now called Cisco Certified CyberOps Associate) certification as an approved baseline certification in the Information Assurance (IA) Workforce CCSP Incident Responder and CCSP Analyst job categories. Please see [Cisco CCNA Cyber Ops and the DoD Approved 8570 Baseline Certifications](#) for more information.

## Course duration

- Instructor-led training: 5 days in the classroom with hands-on lab practice
- Virtual instructor-led training: 5 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 5 days of instruction with hands-on lab practice, videos, and challenges

## How you'll benefit

This course will help you:

- Learn the fundamental skills that a cybersecurity analyst in a security operations center uses, including threat analysis, event correlation, identifying malicious activity, and how to use a playbook for incident response
- Prepare for the Cisco Certified CyberOps Associate certification with hands-on practice using real-life security analysis tools, such as those found in a Linux distribution
- Qualify for entry-level job roles in the high-demand area of cybersecurity



## Who should enroll

- 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

## How to enroll

- For instructor-led training, visit the [Cisco Learning Locator](#).
- For private group training, visit [Cisco Private Group Training](#).

## Technology areas

- Security
- Cybersecurity operations

## Course details

### Objectives

After taking this course, you should be able to:

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



## 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**, by Omar Santos, Joseph Muniz, and Stefano De Crescenzo

## Outline

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



## Lab outline

- Explore Network Security Monitoring Tools
- Investigate Hacker Methodology
- Hunt Malicious Traffic
- Correlate Event Logs, PCAPs, and Alerts of an Attack
- Investigate Browser-Based Attacks
- Analyze Suspicious DNS Activity
- Investigate Suspicious Activity Using Security Onion
- Investigate Advanced Persistent Threats
- Explore SOC Playbooks

\* Cisco CCNA Cyber Ops has been renamed to Cisco Certified CyberOps Associate

