

## Learning Services

# Implementing Cisco Cybersecurity Operations (SECOPS) v1.0



### Overview

The Implementing Cisco Cybersecurity Operations (SECOPS) version 1.0 Cisco® Training on Demand course teaches you to understand how a Security Operations Center (SOC) functions and gives you the introductory-level skills and knowledge needed in this environment. You learn core skills for an SOC analyst at the associate level, understanding basic threat analysis and event correlation, identifying malicious activity, and using a playbook for incident response.

In addition, you gain knowledge on identifying resources for hunting cyber threats, common attack vectors, malicious activity, and patterns of suspicious behavior, and on conducting security incident investigations.

### Duration

The SECOPS v1.0 Training on Demand course is a self-paced course that consists of 15 sections of instructor video and text along with interactive activities, 9 hands-on lab exercises, content review questions, and challenge questions.

### Target Audience

This course is designed for SOC security analysts and personnel, computer network defense analysts and infrastructure support personnel, future incident responders, Cisco channel partners, and those preparing for the 210-255 SECOPS exam.

## Objectives

Upon completion of this course, you should be able to:

- Define an SOC and the various job roles in an 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 identify malicious activity
- Understand the concept of a playbook
- Describe and explain an incident response handbook
- Define types of SOC metrics
- Understand the SOC workflow management system (WMS) and automation

## Course Prerequisites

The knowledge and skills necessary before attending this course are:

- Interconnecting Cisco Networking Devices, Part 1 (ICND1), Understanding Cisco Cybersecurity Fundamentals (SECFND), Windows operating system, and Cisco IOS® networking and concepts

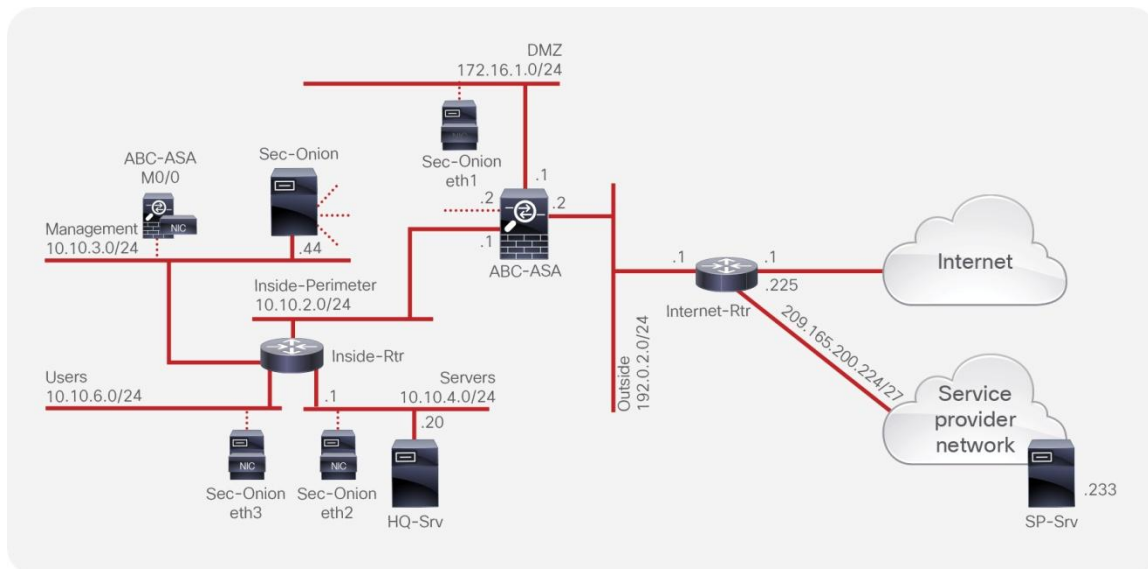
## Course Outline

- Section 1: Defining the Security Operations Center
- Section 2: Understanding NSM Tools and Data
- Section 3: Understanding Incident Analysis in a Threat-Centric SOC
- Section 4: Identifying Resources for Hunting Cyber Threats
- Section 5: Understanding Event Correlation and Normalization
- Section 6: Identifying Common Attack Vectors
- Section 7: Identifying Malicious Activity
- Section 8: Identifying Patterns of Suspicious Behavior
- Section 9: Conducting Security Incident Investigations
- Section 10: Describing the SOC Playbook
- Section 11: Understanding the SOC Metrics
- Section 12: Understanding the SOC WMS and Automation
- Section 13: Describing the Incident Response Plan
- Section 14: Appendix A – Describing the Computer Security Incident Response Team
- Section 15: Appendix B – Understanding the use of VERIS

## Lab Outline

This course contains nine hands-on lab exercises.

### Representative topology for all labs in the course:



The labs included in this course are:

- Discovery Lab 2.11: Explore Network Security Monitoring Tools
- Discovery Lab 3.14: Investigate Hacker Methodology
- Discovery Lab 4.11: Hunt Malicious Traffic
- Discovery Lab 5.7: Correlate Event Logs, PCAPs, and Alerts of an Attack
- Discovery Lab 6.11: Investigate Browser-Based Attacks
- Discovery Lab 7.7: Analyze Suspicious DNS Activity
- Discovery Lab 8.6: Investigate Suspicious Activity Using Security Onion
- Discovery Lab 9.4: Investigate Advanced Persistent Threats
- Discovery Lab 10.6 Explore SOC Playbooks

## Cisco Capital

### Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.](#)




---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)