

Securing Cisco Networks with Threat Detection and Analysis (SCYBER)

Duration 5 Days

COURSE OVERVIEW

This course is designed to teach you how a network security operations center (SOC) works and how to begin to monitor, analyze, and respond to security threats within the network. The course combines lecture materials and hands-on labs throughout to make sure that you are able to successfully understand cyber security concepts and to recognize specific threats and attacks on your network.

COURSE OBJECTIVES

Upon completion of this course, you should have obtained four major areas of competency:

- Monitor security events
- Configure and tune security event detection and alarming
- Analyze traffic for security threats
- Respond appropriately to security incidents

WHO SHOULD ATTEND

This course is designed for technical professionals who need to know how to monitor, analyze, and respond to network security threats and attacks, CCNA individuals, network analysts, large private sector, and DoD

COURSE PREREQUISITES

None. However, standard CCNA knowledge and Basic Cisco IOS® skills are recommended for candidates who prepare to take the exam for Cisco Cyber security Specialist certification

COURSE OUTLINE

The course outline is as follows:

- **Module 1:** Course Introduction: Overview of Network Security and Operations
- **Module 2:** Network and Security Operations Data Analysis
- **Module 3:** Packet Analysis
- **Module 4:** Network Log Analysis
- **Module 5:** Baseline Network Operations
- **Module 6:** Preparing for Security Incidents
- **Module 7:** Detecting Security Incidents
- **Module 8:** Investigating Security Incidents
- **Module 9:** Reacting to an Incident
- **Module 10:** Communicating Incidents Effectively
- **Module 11:** Postevent Activity

Lab

The lab outline is as follows:

- Lab 1: Assess Understanding of Network and Security Operations
- Lab 2: Assess Understanding of Network and Security Data Analysis
- Lab 3: Network and Security Data Analysis Team-Building Activity
- Lab 4: Packet Capture Exercise 1
- Lab 5: Packet Capture Exercise 2
- Lab 6: Packet Capture Exercise 3
- Lab 7: Understanding Log Data
- Lab 8: Correlation Lab
- Lab 9: Assessing Understanding
- Lab 10: Mapping a Monitored Network Topology
- Lab 11: Assessing Normal Behaviors of a Monitored Network
- Lab 12: Assessing Current Security Controls
- Lab 13: Assessing Current Monitoring System
- Lab 14: Manually Correlating Events
- Lab 15: Automatically Correlating Events
- Lab 16: Identifying a Security Incident
- Lab 17: Understanding NetFlow
- Lab 18: NetFlow Practical Activity
- Lab 19: Assessing Understanding
- Lab 20: Selecting Mitigations
- Lab 21: Developing Mitigations
- Lab 22: Documenting Incidents
- Lab 23: Recommending Remediation
- Lab 24: Improving Security
- Lab 25: Incident Response Challenge Lab

Lab Infrastructure and Topology

This lab infrastructure is designed to walk you through the process of understanding how a network SOC works and then proceeds into the data security threat analysis and response process.

The course uses software such as Lancope, Splunk, OSSIM, and Observium to simulate some of the most current cyber security threats on the lab equipment. For example, in the module “Investigating Security Threats,” you will perform the initial configuration of NetFlow, followed by interpreting the traffic in the NetFlow environment. Similarly, you will configure SNMP monitoring to work with the Observium software.

Figure 1 shows the high-level lab topology for this course.

Figure 1. Lab Topology

