Securing Cisco Networks with Threat Detection and Analysis (SCYBER)

The Securing Cisco® Networks with Threat Detection Analysis (SCYBER) course, version 1.0 is an instructor-led course offered by Learning Services High-Touch Delivery. This lab-intensive training course prepares you to take the Cyber Security Specialist Certification exam (exam ID = 600-199) and to hit the ground running as a security analyst team member.

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. 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 job role for a security analyst will vary from industry to industry and differ in the private sector versus the public sector.

**Duration**

Five days.

**Target Audience**

This course is designed for technical professionals who need to know how to monitor, analyze, and respond to network security threats and attacks.

**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
Course Prerequisites
Following is the recommended prerequisite training for this course:
- Standard CCNA® certification as a minimum with CCNA Security a plus
- Basic Cisco IOS® Software switch and router configuration skills

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 Outline
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.
Registration Email
For more information about schedules and registration for this course, contact
aeskt_registration@external.cisco.com.

Website Addresses for More Information
For more information on Learning Services for Cisco classic products and technologies, visit
www.cisco.com/go/ase.

For information on Cisco TelePresence® training, visit www.cisco.com/go/telepresentetraining/.

For information on broadband video training for service providers, visit

For information on Cisco WebEx® technology training, visit www.cisco.com/go/webextraining.

For information on mobile Internet technology training, visit www.cisco.com/go/mitg.