Securing Cisco Networks with Threat Detection and Analysis (SCYBER)

Course ID#: 1575-949-ZZ-W
Hours: 35

Course Content

Course Description:

The *Securing Cisco Networks with Threat Detection and Analysis* (SCYBER) v1.0 course is instructor-led training. This lab-intensive, five-day training course prepares students to take the Cisco Cybersecurity Specialist certification exam and enables them to function effectively as security analyst team members.

The course combines lecture materials and hands-on labs throughout to make sure that students are able to understand cybersecurity concepts and recognize specific network threats and attacks. This course is designed to teach students 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 varies from industry to industry, and private-sector roles differ from public-sector roles.

Prerequisites:

The knowledge and skills that a learner must have before attending this course are as follows:

- CCNA® equivalent knowledge is preferred
- Basic understanding of Cisco security product features
- Basic understanding of open-source and commercial network security tools
- Basic understanding of Microsoft Windows and UNIX/Linux operating systems, desktops, and servers
- Basic understanding of the Open Systems Interconnection (OSI) model and TCP/IP

Topics:

Module 1: Attacker Methodology

- Defining the Attacker Methodology
- Identifying Malware and Attacker Tools
- Understanding Attacks

Module 2: Defender Methodology

- Enumerating Threats, Vulnerabilities, and Exploits
- Defining SOC Services
- Defining SOC Procedures
- Defining the Role of a Network Security Analyst
- Identifying a Security Incident

Module 3: Defender Tools

- Collecting Network Data
- Understanding Correlation and Baselines
- Assessing Sources of Data
- Understanding Events
- Examining User Reports
- Introducing Risk Analysis and Mitigation

Securing Cisco Networks with Threat Detection and Analysis (SCYBER)

Course ID#: 1575-949-ZZ-W

Hours: 35

Module 4: Packet Analysis

- Identifying Packet Data
- Analyzing Packets Using Cisco IOS Software
- Accessing Packets in Cisco IOS Software
- Acquiring Network Traces
- Establishing a Packet Baseline
- Analyzing Packet Traces

Module 5: Network Log Analysis

- Using Log Analysis Protocols and Tools
- Exploring Log Mechanics
- Retrieving Syslog Data
- Retrieving DNS Events and Proxy Logs
- Correlating Log Files

Module 6: Baseline Network Operations

- Baselining Business Processes
- Mapping the Network Topology
- Managing Network Devices
- Baselining Monitored Networks
- Monitoring Network Health

Module 7: Incident Response Preparation

- Defining the Role of the SOC
- Establishing Effective Security Controls
- Establishing an Effective Monitoring System

Module 8: Security Incident Detection

- Correlating Events Manually
- Correlating Events Automatically
- Assessing Incidents
- Classifying Incidents
- Attributing the Incident Source

Module 9: Investigations

- Scoping the Investigation
- Investigating Through Data Correlation
- Understanding NetFlow
- Investigating Connections Using NetFlow

Module 10: Mitigations and Best Practices

- Mitigating Incidents
- Using ACLs
- Implementing Network-Layer Mitigations and Best Practices
- Implementing Link-Layer Best Practices

Module 11: Communication

- Documenting Communication
- Documenting Incident Details

Module 12: Post-Event Activity

- Conducting an Incident Post-Mortem
- Improving Security of Monitored Networks