Understanding Cisco Cybersecurity Operations - On Demand (SECOPS 1.0)

Modality: On Demand

Duration: 40 Hours

CLC: 15 Units

About the course:

The course “Understanding Cisco Cybersecurity Operations - On Demand” is created to help improve your knowledge of Cisco technology and its products. This online Cisco training course focuses on the Cisco technologies and valuable knowledge to help you prepare for the Cisco exams. Through this course, you will get all the significant information about Cisco and Cisco products. The self-paced interactive is designed as such which will keep you interested till the end of the course.

In addition to that, the course comes with an array of hands on exercises to help the student practice on Cisco systems for troubleshooting and configuration.

Course Outline:

Module 1: SOC Overview
Objective: Describe the three common Security Operations Center types, the different tools used by the SOC analysts, the different job roles within the Security Operations Center, and incident analysis within a threat-centric Security Operations Center.

Lesson 1: Defining the Security Operations Center
Objective: Explain how a SOC operates and describes the different types of services that are performed from a Tier 1 SOC analyst’s perspective.

- Types of Security Operations Centers
- Objective: Explain the different types of SOCs (Threat-Centric, Compliance-Based, Operational-Based).
- SOC Analyst Tools
- Objective: Describe at a high-level, the types of network security monitoring tools typically used within a SOC.
- Data Analytics
- Objective: Explain the purpose of data analytics, and using log mining, packet captures, and rule-based alerts for incident investigations.
- Hybrid Installations: Automated Reports, Anomaly Alerts
- Objective: Describe at a high level, the use of automation within the SOC.
- Proper Staffing Necessary for an Effective Incident Response Team
- Objective: Describe the proper staffing necessary for implementing an effective incident response team.
- Roles in a Security Operations Center
- Objective: Describe the different job roles within a typical SOC.

- Develop Key Relationships with External Resources
- Objective: List the external resources a typical SOC needs to establish a relationship with.
- Challenge

Lesson 2: Understanding NSM Tools and Data
Objective: Explain the network security monitoring tools and data available to the network security analyst.

- Introduction
- NSM Tools
- Objective: Describe the three types of network security monitoring tools used within the SOC (commercial, open source, or homegrown).
- NSM Data
- Objective: Describe the different types of network security monitoring data (session data, full packet capture, transaction data, alert data, and statistical data).
- Security Onion
- Objective: Explain at a high level, the use of Security Onion as a network security monitoring tool.
- Full Packet Capture
- Objective: Explain packet capture data is stored in the PCAP format, and the storage requirements for full packet capture.
- Session Data
- Objective: Describe session data content, and provide an example of session data.
- Transaction Data
- Objective: Describe transaction data content, and provide an example of transaction data.
- Alert Data
- Objective: Describe alert data content, and provide an example of alert data.
- Other NSM Data Types
- Objective: Describe the other types of network security monitoring data (extracted content, statistical data, and metadata).
- Correlating NSM Data
- Objective: Explain the need to correlate network security monitoring data, and provide an example.

Lesson 3: Understanding Incident Analysis in a Threat-Centric SOC
Objective: Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by the threat actors.

- Classic Kill Chain Model Overview
- Objective: Describe using the classic kill chain model to perform network security incident analysis.
- Kill Chain Phase 1: Reconnaissance
- Objective: Describe the reconnaissance phase of the classic kill chain model.
- Kill Chain Phase 2: Weaponization
- Objective: Describe the weaponization phase of the classic kill chain model.
- Kill Chain Phase 3: Delivery
- Objective: Describe the delivery phase of the classic kill chain model.
- Kill Chain Phase 4: Exploitation

- Objective: Describe the exploitation phase of the classic kill chain model.
- Kill Chain Phase 5: Installation
- Objective: Describe the installation phase of the classic kill chain model.
- Kill Chain Phase 6: Command-and-Control
- Objective: Describe the command-and-control phase of the classic kill chain model.
- Kill Chain Phase 7: Actions on Objectives
- Objective: Describe the actions on objectives phase of the classic kill chain model.
- Applying the Kill Chain Model
- Objective: Describe how the kill chain model can be applied to detect and prevent ransomware.
- Diamond Model Overview
- Objective: Describe using the diamond model to perform network security incident analysis.
- Applying the Diamond Model
- Objective: Describe how to apply the diamond model to perform network security incident analysis using a threat intelligence platform such as ThreatConnect.
- Exploit Kits
- Objective: Describe the use of exploit kits by the threat actors.

Lesson 4: Identifying Resources for Hunting Cyber Threats

- Cyber-Threat Hunting Concepts
- Objective: Describe at a high level, the cyber-threat hunting concepts.
- Hunting Maturity Model
- Objective: Explain the five hunting maturity levels (HM0 to HM4).
- Cyber-Threat Hunting Cycle
- Objective: Explain the hunting cycle four-stage loop.
- Common Vulnerability Scoring System
- Objective: Describe at a high level, the use of the Common Vulnerability Scoring System, and list the v3.0 base metrics.
- CVSS v3.0 Scoring
- Objective: Describe the Common Vulnerability Scoring System v3.0 scoring components (base, temporal, and environmental).
- CVSS v3.0 Example
- Objective: Provide an example of Common Vulnerability Scoring System v3.0 scoring.
- Hot Threat Dashboard
- Objective: Describe the use of a hot threat dashboard within a SOC.
- Publicly Available Threat Awareness Resources
- Objective: Provide examples of some of the publicly available threat awareness resources.
- Other External Threat Intelligence Sources and Feeds Reference
- Objective: Provide examples of some of the publicly available external threat intelligence sources and feeds.

Module 2: Security Incident Investigations
Objective: Explain the concepts of security incident investigations, including events correlation and normalization, common attack vectors, and able to identify malicious and suspicious activities.

Lesson 1: Understanding Event Correlation and Normalization

- Event Sources
- Objective: Describe some of the network security monitoring event sources (IPS, Firewall, NetFlow, Proxy Server, IAM, AV, Application Logs).
- Evidence
- Objective: Describe direct evidence and circumstantial evidence.
- Security Data Normalization
- Objective: Provide an example of security data normalization.
- Event Correlation
- Objective: Provide an example of security events correlation.
- Other Security Data Manipulation
- Objective: Explain the basic concepts of security data aggregation, summarization, and deduplication.

Lesson 2: Identifying Common Attack Vectors

- Objective: Identify the common attack vectors.
- Obfuscated JavaScript
- Objective: Explain the use of obfuscated JavaScript by the threat actors.
- Shellcode and Exploits
- Objective: Explain the use of shellcode and exploits by the threat actors.
- Common Metasploit Payloads
- Objective: Explain the three basic types of payloads within the Metasploit framework (single, stager, stage).
- Directory Traversal
- Objective: Explain the use of directory traversal by the threat actors.
- SQL Injection
- Objective: Explain the basic concepts of SQL injection attacks.
- Cross-Site Scripting
- Objective: Explain the basic concepts of cross-site scripting attacks.
- Punycode
- Objective: Explain the use of punycode by the threat actors.
- DNS Tunneling
- Objective: Explain the use of DNS tunneling by the threat actors.
- Pivoting
- Objective: Explain the use of pivoting by the threat actors.

Lesson 3: Identifying Malicious Activity

- Objective: Explain how to identify malicious activities.
- Understanding the Network Design
- Objective: Explain the needs for the security analysts to have an understanding of the network design which they are protecting.
- Identifying Possible Threat Actors
- Objective: Describe the different threat actor types.
- Log Data Search
- Objective: Provide an example of log data search using ELSA.
- NetFlow as a Security Tool
- Objective: Explain using NetFlow as a security tool.

- DNS Risk and Mitigation Tool
- Objective: Explain how DNS can be used by the threat actors to perform attacks.

Lesson 4: Identifying Patterns of Suspicious Behavior

- Objective: Explain how to identify patterns of suspicious behaviors.
- Network Baselining
- Objective: Explain the purpose of baselining the network activities.
- Identify Anomalies and Suspicious Behaviors
- Objective: Explain using the established baseline to identify anomalies and suspicious behaviors.
- PCAP Analysis
- Objective: Explain the basic concepts of performing PCAP analysis.
- Delivery
- Objective: Explain the use of a sandbox to perform file analysis.

Lesson 5: Conducting Security Incident Investigations

- Security Incident Investigation Procedures
- Objective: Explain the objective of security incident investigation to discover the who, what, when, where, why, and how about the security incident.
- Threat Investigation Example: China Chopper Remote Access Trojan
- Objective: Describe at a high level, the China Chopper Remote Access Trojan.

Module 3: SOC Operations
Objective: Explain using a SOC playbook to assist with investigations, using metrics to measure the SOC's effectiveness, using a SOC workflow management system and automation to improve the SOC's efficiency, and the concepts of an incident response plan.

Lesson 1: Describing the SOC Playbook

- Objective: Explain the use of a typical playbook in the SOC.
- Security Analytics
- Objective: Describe the security analytics process,
- Playbook Definition
- Objective: Describe the use of a playbook in a SOC.
- What Is in a Play?
- Objective: Describe the components of a play in a typical SOC playbook.
- Playbook Management System
- Objective: Describe the use of a playbook management system in the SOC.

Lesson 2: Understanding the SOC Metrics

- Objective: Explain the use of SOC metrics to measure the SOC's effectiveness.
- Security Data Aggregation
- Objective: Explain using a SIEM to provide security data aggregation, real-time reporting, and analysis of security events.
- Time to Detection

- Objective: Explain what is the time to detection.
- Security Controls Detection Effectiveness
- Objective: Explain measuring the security controls effectiveness in terms of true positive/negative events, false positive/negative events.
- SOC Metrics
- Objective: Explain using different metrics to measure the SOC effectiveness.
- Challenge

Lesson 3: Understanding the SOC WMS and Automation

- Objective: Explain the use of a workflow management system and automation to improve the SOC's effectiveness.
- SOC WMS Concepts
- Objective: Explain the basic concepts and benefits of using a workflow management system within a SOC.
- Incident Response Workflow
- Objective: Describe a typical incident response workflow.
- SOC WMS Integration
- Objective: Describe how a typical workflow management system is integrated within a SOC.
- SOC Workflow Automation Example
- Objective: Provide an example of a SOC workflow automation system (Cybersponse).
- Challenge

Lesson 4: Describing the Incident Response Plan

- Incident Response Planning
- Objective: Explain the purpose for incident response planning.
- Incident Response Life Cycle
- Objective: Describe the typical incident response life cycle.
- Incident Response Policy Elements
- Objective: Describe the typical elements within an incident response policy.
- Incident Attack Categories
- Objective: Describe how incidents can be classified.
- Reference: US-CERT Incident Categories
- Objective: Describe the different US-CERT incident categories (CAT 0 to CAT 6).
- Regulatory Compliance Incident Response Requirements
- Objective: Describe compliance regulations which contain an incident response requirements.
- Challenge

Lesson 5: Appendix A—Describing the Computer Security Incident Response Team

- Objective: Explain the functions of a typical Computer Security Incident Response Team.
- CSIRT Categories
- Objective: Describe the different general CSIRT categories.
- CSIRT Framework
- Objective: Describe the basic framework that defines a CSIRT.
- CSIRT Incident Handling Services
- Objective: Describe the different CSIRT incident handling services (triage, handling,

feedback, optional announcement).
- Challenge

Lesson 6: Appendix B—Understanding the use of VERIS

- Objective: Explain the use of VERIS to document security incidents in a standard format.
- VERIS Overview
- Objective: Explain what is VERIS.
- VERIS Incidents Structure
- Objective: Explain the VERIS incident structure.
- VERIS 4 As
- Objective: Explain the VERIS 4 As.
- VERIS Records
- Objective: Describe a typical VERIS record.
- VERIS Community Database
- Objective: Describe the VERIS Community Database.
- Verizon Data Breach Investigations Report and Cisco Annual Security Report
- Objective: Describe the Verizon Data Breach Investigations Report, and the Cisco Annual Security Report.
- Challenge