IMPLEMENTING CISCO CYBERSECURITY OPERATIONS

DURATION: 5 DAYS

COURSE OVERVIEW

This is the second course in Cisco's CCNA Cyber Ops Curriculum and is designed to provide students with an understanding of how a Security Operations Center (SOC) functions and the knowledge required in this environment. This course focuses on the introductory-level skills needed for a SOC Analyst at the associate level. Specifically, understanding basic threat analysis, event correlation, identifying malicious activity and how to use a playbook for incident response.

TARGET AUDIENCE

Individuals interested in a career in cyber security, or looking to understand more about cybersecurity operations, or working towards their CCNA Cyber OPs certification.

COURSE OBJECTIVES

After completing this course you should be able to:

1. Define a SOC and the various job roles in a SOC
2. Understand SOC infrastructure tools and systems
3. Learn basic incident analysis for a threat centric SOC
4. Explore resources available to assist with an investigation
5. Explain basic event correlation and normalization
6. Describe common attack vectors
7. Learn how to identifying malicious activity
8. Understand the concept of a playbook
9. Describe and explain an incident respond handbook
10. Define types of SOC Metrics
11. Understand SOC Workflow Management system and automation

COURSE CONTENT

SOC Overview

1. Defining the Security Operations Center
2. Understanding NSM Tools and Data
3. Understanding Incident Analysis in a Threat-Centric SOC
4. Identifying Resources for Hunting Cyber Threats

Security Incident Investigations

1. Understanding Event Correlation and Normalization
2. Identifying Common Attack Vectors
3. Identifying Malicious Activity
4. Identifying Patterns of Suspicious Behavior
5. Conducting Security Incident Investigations

SOC Operations

1. Describing the SOC Playbook
2. Understanding the SOC Metrics
3. Understanding the SOC WMS and Automation
4. Describing the Incident Response Plan
5. Appendix A - Describing the Computer Security Incident Response Team
6. Appendix B - Understanding the use of VERIS

Labs

1. Guided Lab 1: Explore Network Security Monitoring Tools
2. Discovery 1: Investigate Hacker Methodology
3. Discovery 2: Hunt Malicious Traffic
4. Discovery 3: Correlate Event Logs, PCAPs, and Alerts of an Attack
5. Discovery 4: Investigate Browser-Based Attacks
6. Discovery 5: Analyze Suspicious DNS Activity
7. Discovery 6: Investigate Suspicious Activity Using Security Onion
8. Discovery 7: Investigate Advanced Persistent Threats
9. Discovery 8: Explore SOC Playbooks

COURSE PREREQUISITES

Attendees should ideally meet the following prerequisites:

1. Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (**ICND1**)
2. Skills and knowledge equivalent to those learned in Security Fundamentals (**SECFND**)
3. Working knowledge of the Windows operating system
4. Working knowledge of Cisco IOS networking and concepts

TEST CERTIFICATION

Recommended as preparation for the following exam(s):

210-255 - SECOPS

This is one of two exams required to achieve the CCNA Cyber Ops Certification