Table of Contents

1. Introduction
2. Target Audience
3. Prerequisites
4. Target Certification
5. Curriculum Description
6. Curriculum Objectives
7. Virtual Machine Requirements
8. Course Outline
9. System Requirements
10. Industry certification
11. Discount Voucher
Introduction

Today’s organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOCs) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats. CCNA Cyber Ops prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers.

Target Audience

Students seeking career-oriented, entry-level security analyst skills. Target students include individuals enrolled in technology degree programs at institutions of higher education and IT professionals who wants to pursue a career in the Security Operation Centre (SOC).

Prerequisites

CCNA Cybersecurity Operations students should have the following skills and knowledge:

- PC and Internet navigation skills
- Basic Windows and Linux system concepts
- Basic Networking concepts
- Binary and Hexadecimal understanding
- Awareness of basic programming concepts
- Awareness of basic SQL queries

Target Certification

This course aligns with the CCNA Cyber Ops certification. Candidates need to pass the 210-250 SECFND exam and the 210-255 SECOPS exam to achieve the CCNA Cyber Ops certification.

Curriculum Description

The course has many features to help students understand these concepts:
• Rich multimedia content, including interactive activities, videos, games, and quizzes, addresses a variety of learning styles and help stimulate learning and increase knowledge retention.
• Virtual environments simulate real-world cybersecurity threat scenarios and create opportunities for ethical hacking, security monitoring, analysis and resolution.
• Hands-on labs help students develop critical thinking and complex problem solving skills.
• Innovative assessments provide immediate feedback to support the evaluation of knowledge and acquired skills.
• Technical concepts are explained using language that works well for learners at all levels and embedded interactive activities break up reading of the content and help reinforce understanding.
• The curriculum encourages students to consider additional IT education, but also emphasizes applied skills and hands-on experience.
• Cisco Packet Tracer activities are designed for use with Packet Tracer 7.0 or later.

CCNA Cybersecurity Operations covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC).

Upon completion of the CCNA Cybersecurity Operations course, students will be able to perform the following tasks:

• Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
• Explain the role of the Cybersecurity Operations Analyst in the enterprise.
• Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
• Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
• Explain the features and characteristics of the Linux Operating System.
• Analyze the operation of network protocols and services.
• Explain the operation of the network infrastructure.
• Classify the various types of network attacks.
• Use network-monitoring tools to identify attacks against network protocols and services.
• Use various methods to prevent malicious access to computer networks, hosts, and data.
• Explain the impacts of cryptography on network security monitoring.
• Explain how to investigate endpoint vulnerabilities and attacks.
• Evaluate network security alerts.
• Analyze network intrusion data to identify compromised hosts and vulnerabilities.
• Apply incident response models to manage network security incidents.

Virtual Machine Requirements

This course uses a single virtual machine (VM) for many of the labs through Chapter 10. Three additional VMs are added in Chapter 11. There is also a single VM option available for lab or student PCs that do not meet the following requirements:

• Host computer with at least 8 GB of RAM and 45 GB of free disk space
• Latest version of Oracle VirtualBox
• Internet connection
• Four virtual machines

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>RAM</th>
<th>Disk Space</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyberOps Workstation VM</td>
<td>1 GB</td>
<td>7 GB</td>
<td>analyst</td>
<td>cyberops</td>
</tr>
<tr>
<td>Kali</td>
<td>1 GB</td>
<td>10 GB</td>
<td>root</td>
<td>cyberops</td>
</tr>
<tr>
<td>Metasploitable</td>
<td>512 KB</td>
<td>8 GB</td>
<td>msfadmin</td>
<td>msfadmin</td>
</tr>
<tr>
<td>Security Onion</td>
<td>4 GB</td>
<td>10 GB</td>
<td>analyst</td>
<td>cyberops</td>
</tr>
<tr>
<td>Security Onion (Alternative)*</td>
<td>3 GB</td>
<td>10 GB</td>
<td>analyst</td>
<td>cyberops</td>
</tr>
</tbody>
</table>

Course Outlines

Chapter/Section/Goals/Objectives

Chapter 1. Cybersecurity and the Security Operations Center

1.1 The Danger: Explain why networks and data are attacked.

1.2 Fighters in the War Against Cybercrime: Explain how to prepare for a career in Cybersecurity operations.
### Chapter 2. Windows Operating System

2.1 Windows Overview: Explain the operation of the Windows Operating System.

2.2 Windows Administration: Explain how to secure Windows endpoints.

### Chapter 3. Linux Operating System

3.1 Using Linux: Perform basic operations in the Linux shell.

3.2 Linux Administration: Perform basic Linux administration tasks.

3.3 Linux Clients: Perform basic security-related tasks on a Linux host.

### Chapter 4. Network Protocols and Services

4.1 Network Protocols: Explain how protocols enable network operations.

4.2 Ethernet and Internet Protocol (IP): Explain how the Ethernet and IP protocols support network communication.

4.3 Connectivity Verification: Use common testing utilities to verify and test network connectivity.

4.4 Address Resolution Protocol: Explain how the address resolution protocol enables communication on a network.

4.5 The Transport Layer and Network Services: Explain how transport layer protocols and network services support network functionality.

4.6 Network Services: Explain how network services enable network functionality.

### Chapter 5. Network Infrastructure

5.1 Network Communication Devices: Explain how network devices enable wired and wireless network communication.

5.2 Network Security Infrastructure: Explain how devices and services are used to enhance network security.

5.3 Network Representations: Explain how networks and network topologies are represented.

### Chapter 6. Principles of Network Security

6.1 Attackers and Their Tools: Explain how networks are attacked.

6.2 Common Threats and Attacks: Explain the various types of threats and attacks.

### Chapter 7. Network Attacks: A Deeper Look

7.1 Observing Network Operation: Explain network traffic monitoring.

7.2 Attacking the Foundation: Explain how TCP/IP vulnerabilities enable network attacks.

7.3 Attacking What We Do: Explain how common network applications and services are vulnerable to attack.

### Chapter 8. Protecting the Network

8.1 Understanding Defense: Explain approaches to network security defense.

8.2 Access Control: Explain access control as a method of protecting a network.

8.3 Network Firewalls and Intrusion Prevention: Explain how firewalls and other devices prevent network intrusions.

8.4 Content Filtering: Explain how content filtering prevents unwanted data from entering the network.

8.5 Threat Intelligence: Use various intelligence sources to locate current security threats.

### Chapter 9. Cryptography and the Public Key Infrastructure

9.1 Cryptography: Use tools to encrypt and decrypt data.

9.2 Public Key Cryptography: Explain how the public key infrastructure (PKI) supports network security.

### Chapter 10. Endpoint Security and Analysis

10.1 Endpoint Protection: Use a tool to generate a malware analysis report.

10.2 Endpoint Vulnerability Assessment
Classify endpoint vulnerability assessment information.

Chapter 11. Security Monitoring

11.1 Technologies and Protocols: Explain how security technologies affect security monitoring.
11.2 Log Files: Explain the types of log files used in security monitoring

Chapter 12. Intrusion Data Analysis

12.1 Data Collection: Explain how security-related data is collected.
12.2 Data Preparation: Arrange a variety of log files in preparation for intrusion data analysis.
12.3 Data Analysis: Analyze intrusion data to determine the source of an attack.

Chapter 13. Incident Response and Handling

13.1 Incident Response Models: Apply incident response models to an intrusion event
13.2 CSIRTs and NIST 800-61r2: Apply standards specified in NIST 800-61r2 to a computer security incident.
13.3 Case-Based Practice: Given a set of logs, isolate a threat actor and recommend an incident response plan.

The Understanding Cisco Cybersecurity Fundamentals (SECFND) exam (210-250) is a 90-minute, 60–70 question assessment that is associated with the Cisco CCNA Cyber Ops certification. Candidates can prepare for this exam by taking the Understanding Cisco Cybersecurity Fundamentals (SECFND) v1.0 course. This exam tests a candidate's understanding of cybersecurity basic principles, foundational knowledge, and core skills needed to grasp the more associate-level materials in the second required exam, Implementing Cisco Cybersecurity Operations (SECOPS).

The Implementing Cisco Cybersecurity Operations (SECOPS) exam (210-255) is a 90-minute, 60-70 question assessment. This exam is the second of the two required exams to achieve the associate-level CCNA Cyber Ops certification and prepares candidates to begin a career within a Security Operations Center (SOC), working with Cybersecurity Analysts at the associate level. The SECOPS exam tests a candidate's knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a SOC.
60% Certification Exam discount voucher is available to qualifying students (those who receive a score of 75% or higher on the FIRST attempt of the final exam in a qualifying course and a Pass in the gradebook).