C-ID Descriptor
Cybersecurity Operations – CCNA CyberOps

Descriptor Details

- **Descriptor Title**: Cybersecurity Operations – CCNA CyberOps
- **C-ID Number**: 166
- **Units**: 3
- **Date of Last Revision**: 2/26/2025 07:22:06 PM GMT+0000

General Description

This course equips students with the knowledge and skills needed by today's organizations that are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. The student would be part of a team of people in Security Operations Centers (SOC’s) keeping 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.

Prerequisites

None

Corequisites

None

Advisories

ITIS 150 - Computer Network Fundamentals
ITIS 160 – Introduction to Information Systems Security

Content

1. Cybersecurity and the Security Operations Center
    a. The Danger - Explain why networks and data are attacked.
    b. Fighters in the War Against Cybercrime - Explain how to prepare for a career in Cybersecurity operations.
2. Windows Operating System
    a. Windows Overview - Explain the operation of the Windows Operating System.
    b. Windows Administration - Explain how to secure Windows endpoints.
3. Linux Operating System
    a. Using Linux - Perform basic operations in the Linux shell.
    b. Linux Administration - Perform basic Linux administration tasks.
    c. Linux Clients - Perform basic security-related tasks on a Linux host.
4. Network Protocols and Services
    a. Network Protocols - Explain how protocols enable network operations.
    b. Ethernet and Internet Protocol (IP) - Explain how the Ethernet and IP protocols support network communication.
    c. Connectivity Verification - Use common testing utilities to verify and test network connectivity.
    d. Address Resolution Protocol - Explain how the address resolution protocol enables communication on a network.
    e. The Transport Layer and Network Services - Explain how transport layer protocols and network services support network functionality.
    f. Network Services - Explain how network services enable network functionality.
5. Network Infrastructure
    a. Network Communication Devices - Explain how network devices enable wired and wireless network communication.
    b. Network Security Infrastructure - Explain how devices and services are used to enhance network security.
    c. Network Representations - Explain how networks and network topologies are represented.
6. Principles of Network Security

a. Attackers and Their Tools - Explain how networks are attacked.
b. Common Threats and Attacks - Explain the various types of threats and attacks.

7. Network Attacks: A Deeper Look
   a. Observing Network Operation - Explain network traffic monitoring.
   b. Attacking the Foundation - Explain how TCP/IP vulnerabilities enable network attacks.
   c. Attacking What We Do - Explain how common network applications and services are vulnerable to attack.
8. Protecting the Network
   a. Understanding Defense - Explain approaches to network security defense.
   b. Access Control - Explain access control as a method of protecting a network.
   c. Network Firewalls and Intrusion Prevention - Explain how firewalls and other devices prevent network intrusions.
   d. Content Filtering - Explain how content filtering prevents unwanted data from entering the network.
   e. Threat Intelligence - Use various intelligence sources to locate current security threats.
9. Cryptography and the Public Key Infrastructure
   a. Cryptography - Use tools to encrypt and decrypt data.
   b. Public Key Cryptography - Explain how the public key infrastructure (PKI) supports network security.
10. Endpoint Security and Analysis
    a. Endpoint Protection - Use a tool to generate a malware analysis report.
    b. Endpoint Vulnerability Assessment - Classify endpoint vulnerability assessment information.
11. Security Monitoring
    a. Technologies and Protocols - Explain how security technologies affect security monitoring.
    b. Log Files - Explain the types of log files used in security monitoring.
12. Intrusion Data Analysis
    a. Data Collection - Explain how security-related data is collected.
    b. Data Preparation - Arrange a variety of log files in preparation for intrusion data analysis.
    c. Data Analysis - Analyze intrusion data to determine the source of an attack.

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

Lab Activities

No information provided

Objectives

At the conclusion of this course, the student should be able to:

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

Evaluation Methods

Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.

Textbooks

- *CCNA Cybersecurity Operations NetAcad Companion Guide* and *Lab Manual*.
- Santos, O. and Muniz, J., *CCNA Cyber Ops SECOPS 210-255 Pearson uCertify Course, Labs, and Textbook Bundle*, Cisco Press.