CyberOps Associate (CA) v1.0
Course Overview

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 exploits and threats. CyberOps Associate prepares candidates to begin a career working as associate-level cybersecurity analysts within security operations centers.

Course Description:

The course has many features to help students understand these concepts:

- The course is comprised of twenty-eight (28) modules. Each module is comprised of topics.
- Modules emphasize critical thinking, problem solving, collaboration, and the practical application of skills.
- Rich multimedia content, including interactive activities, videos, and quizzes, addresses a variety of learning styles and helps stimulate learning and increase knowledge retention.
- Virtual environments simulate real-world cybersecurity threat scenarios and create opportunities for 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.

CyberOps Associate (CA) v1.0 Scope and Sequence

Course outline:

Module/Topics	Goals/Objectives
Module 1. The Danger	Explain why networks and data are attacked.
Module 2. Fighters in the War Against Cybercrime	Explain how to prepare for a career in cybersecurity operations.
Module 3. The Windows Operating System	Explain the security features of the Windows operating system.
Module 4. Linux Overview	Implement basic Linux security.
Module 5. Network Protocols	Explain how protocols enable network operations.
Module 6. Ethernet and Internet Protocol (IP)	Explain how the ethernet and IP protocols support network communications.
Module 7. Principles of Network Security	Connectivity Verification
Module 8. Address Resolution Protocol	Analyze address resolution protocol PDUs on a network.
Module 9. The Transport Layer	Explain how transport layer protocols support network functionality.
Module 10. Network Services	Explain how network services enable network functionality.
Module 11. Network Communication Devices	Explain how network devices enable wired and wireless network communication.
Module 12. Network Security Infrastructure	Explain how network devices and services are used to enhance network security.
Module 13. Attackers and Their Tools	Explain how networks are attacked.
Module 14. Common Threats and Attacks	Explain the various types of threats and attacks.

CyberOps Associate (CA) v1.0 Scope and Sequence

Module/Topics	Goals/Objectives
Module 15. Observing Network Operation	Explain network traffic monitoring.
Module 16. Attacking the Foundation	Explain how TCP/IP vulnerabilities enable network attacks.
Module 17. Attacking What We Do	Explain how common network applications and services are vulnerable to attack.
Module 18. Understanding Defense	Explain approaches to network security defense.
Module 19. Access Control	Explain access control as a method of protecting a network.
Module 20. Threat Intelligence	Use various intelligence sources to locate current security threats.
Module 21. Cryptography	Explain how the public key infrastructure supports network security.
Module 22. Endpoint Protection	Explain how a malware analysis website generates a malware analysis report.
Module 23. Endpoint Vulnerability Assessment	Explain how endpoint vulnerabilities are assessed and managed.
Module 24. Technologies and Protocols	Explain how security technologies affect security monitoring.
Module 25. Network Security Data	Explain the types of network security data used in security monitoring.
Module 26. Evaluating Alerts	Explain the process of evaluating alerts.
Module 27. Working with Network Security Data	Interpret data to determine the source of an alert.
Module 28. Digital Forensics and Incident Analysis and Response	Explain how the CyberOps Associate responds to cybersecurity incidents.

Happy Learning!