Networking Academy

CyberOps Associate

COURSE OUTLINE

Course Overview

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.

Target Audience

The CyberOps Associate course is designed for Cisco Networking Academy® students who are 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 want to pursue a career in the Security Operation Center (SOC). Learners in this course are exposed to all of the foundational knowledge required to detect, analyze, and escalate basic cybersecurity threats using common open-source tools.

Course Duration

It will take ***2 months*** to complete the course.

Prerequisites

CyberOps Associate students should have the following skills and knowledge:

- PC and internet navigation skills
- Basic Windows and Linux system concepts
- Basic understanding of computer networks
- Binary and Hexadecimal understanding
- Familiarity with Cisco Packet Tracer

Target Certification

This course aligns with the Cisco Certified CyberOps Associate (CBROPS) certification. Candidates need to pass the 200-201 CBROPS exam to achieve the Cisco Certified CyberOps Associate certification.

After completing the course successfully, student will get -

- One digital batch
- Course completion certificate

Course Curriculum

Module 1. The Danger

Introduction
War Stories
Threat Actors
Threat Impact
The Danger Summary

Module 2. Fighters in the War Against Cybercrime

The Modern Security Operations Center
Becoming a Defender
Fighters in the War Against Cybercrime Summary

Module 3. The Windows Operating System

Windows History
Windows Architecture and Operations
Windows Configuration and Monitoring
Windows Security
The Windows Operating System Summary

Module 4. Linux Overview

Linux Basics
Working in the Linux Shell
Linux Servers and Clients
Basic Server Administration
The Linux File System
Working with the Linux GUI
Working on a Linux Host
Linux Basics Summary

Module 5. Network Protocols

Network Communication Process
Communication Protocols
Data Encapsulation
Network Protocols Summary

Module 6. Ethernet and Internet Protocol (IP)

Ethernet
IPv4
IP Addressing Basics
Types of IPv4 Addresses
The Default Gateway
IPv6 Prefix Length
Ethernet and IP Protocol Summary

Module 7. Principles of Network Security

ICMP
Ping and Traceroute Utilities
Connectivity Verification Summary

Module 8. Address Resolution Protocol

MAC and IP
ARP
ARP Issues
Address Resolution Protocol Summary

Module 9. The Transport Layer

Transport Layer Characteristics
Transport Layer Session Establishment
Transport Layer Reliability
The Transport Layer Summary

Module 10. Network Services

DHCP
DNS
NAT
File Transfer and Sharing Services
Email
HTTP
Network Services Summary

Module 11. Network Communication Devices

Network Devices
Wireless Communications
Network Communication Devices Summary

Module 12. Network Security Infrastructure

Network Topologies
Security Devices
Security Services
Network Security Infrastructure Summary

Module 13. Attackers and Their Tools

Who is Attacking Our Network?
Threat Actor Tools
Attackers and Their Tools Summary

Module 14. Common Threats and Attacks Malware

Common Network Attacks – Reconnaissance, Access, and Social Engineering
Network Attacks – Denial of Service, Buffer Overflows, and Evasion
Common Threats and Attacks Summary

Module 15. Observing Network Operation

Introduction to Network Monitoring
Introduction to Network Monitoring Tools
Network Monitoring and Tools Summary

Module 16. Attacking the Foundation

IP PDU Details
IP Vulnerabilities
TCP and UDP Vulnerabilities
Attacking the Foundation Summary

Module 17. Attacking What We Do

IP Services
Enterprise Services
Attacking What We Do Summary

Module 18. Understanding Defense

Defense-in-Depth
Security Policies, Regulations, and Standards
Understanding Defense Summary

Module 19. Access Control

Access Control Concepts
AAA usage and operation
Access Control Summary

Module 20. Threat Intelligence

Information Sources
Threat Intelligence Services
Threat Intelligence Summary

Module 21. Cryptography

Integrity and Authenticity
Confidentiality
Public Key Cryptography
Authorities and the PKI Trust System
Applications and Impacts of Cryptography
Cryptography Summary

Module 22. Endpoint Protection

Antimalware Protection
Host-based Intrusion Prevention
Application Security
Endpoint Protection Summary

Module 23. Endpoint Vulnerability Assessment

Network and Server Profiling
Common Vulnerability Scoring System (CVSS)
Secure Device Management
Information Security Management Systems
Endpoint Vulnerability Assessment Summary

Module 24. Technologies and Protocols

Monitoring Common Protocols
Security Technologies
Technologies and Protocols Summary

Module 25. Network Security Data

Types of Security Data
End Device Logs
Network Logs
Network Security Data Summary

Module 26. Evaluating Alerts

Source of Alerts
Overview of Alert Evaluation
Evaluating Alerts Summary

Module 27. Working with Network Security Data

A Common Data Platform
Investigating Network Data
Enhancing the Work of the Cybersecurity Analyst
Working with Network Security Data Summary

Module 28. Digital Forensics and Incident Analysis and Response

Evidence Handling and Attack Attribution
The Cyber Kill Chain
The Diamond Model of Intrusion Analysis
Incident Response
Digital Forensics and Incident Analysis and Response Summary
Prepare for Your Exam and Launch Your Career!

36% DISCOUNT

Vendor Exam Fee is USD 195. After discount, the exam fee will be USD 125.

CONTACT US

☎ +880 1630 665 666

✉ ice@aiub.edu

📍 Plot 58/B, Road 21, Block B,
Kemal Ataturk Avenue, Banani, Dhaka