Certified Cybersecurity Operations Analyst Course Curriculum

Module 1: Introduction to Cybersecurity Operations

- Overview of Cybersecurity and SOC
- Understanding the Cybersecurity Landscape
- Key Roles in a Security Operations Center (SOC)
- Cybersecurity Frameworks and Standards

Module 2: Threats, Vulnerabilities, and Attack Vectors

- Types of Cyber Threats (Malware, Phishing, Ransomware, etc.)
- Common Vulnerabilities in IT Systems
- Anatomy of Cyber Attacks and Kill Chain Model
- Case Studies on Real-World Attacks

Module 3: Network Security Fundamentals

- TCP/IP Protocol Suite and OSI Model Overview
- Firewalls, VPNs, and Proxy Servers
- Intrusion Detection and Prevention Systems (IDS/IPS)
- Network Traffic Monitoring and Analysis

Module 4: Security Monitoring Tools and Technologies

- Introduction to SIEM Tools (e.g., Splunk, IBM QRadar)
- Endpoint Detection and Response (EDR) Solutions
- Log Management and Analysis
- Network and Host-based Monitoring

Module 5: Incident Detection and Threat Intelligence

- Identifying Indicators of Compromise (IoCs)
- Gathering and Analyzing Threat Intelligence
- Threat Hunting Techniques
- Malware Analysis Basics

Module 6: Incident Response and Management

- Incident Response Lifecycle
- Developing and Implementing Incident Response Plans
- Containment, Eradication, and Recovery Steps
- Post-Incident Analysis and Reporting

Module 7: Cybersecurity Forensics

- Introduction to Digital Forensics
- Evidence Collection and Preservation
- Disk and Memory Forensics
- Tools for Forensic Analysis (e.g., FTK, Autopsy)

Module 8: Proactive Defense Strategies

- Security Awareness and Best Practices
- Vulnerability Scanning and Patch Management
- Implementing Defense-in-Depth Strategies
- Cybersecurity Policy Development

Module 9: Compliance and Regulations

- Understanding GDPR, CCPA, HIPAA, and PCI DSS
- Ensuring Compliance in Security Operations
- Audit Readiness and Reporting

Module 10: Preparation for Certification Exams

- Overview of Relevant Certifications (CompTIA CySA+, Cisco CyberOps, etc.)
- Exam Preparation Tips and Strategies
- Practice Questions and Mock Tests

Key Features of the Curriculum

- **Hands-On Labs**: Practical exercises with industry-standard tools.
- **Case Studies**: Real-world scenarios to enhance analytical skills.
- **Capstone Project**: End-of-course project to apply acquired knowledge.