

Certified Cybersecurity Operations Analyst (CCOA)

Course Duration : 40 Hours

Course code : CCOA

1. Course Overview

The Certified Cybersecurity Operations Analyst™ (CCOA) course is designed for professionals responsible for monitoring, detecting, analyzing, and responding to cybersecurity threats in real-time environments. This course focuses on security operations center (SOC) functions, threat intelligence, incident response, and continuous monitoring. Learners gain hands-on knowledge of operational security tools and techniques used to protect enterprise systems and networks.

2. What you'll learn?

- Security operations center (SOC) roles and workflows
- Threat detection and incident analysis
- Log monitoring and security event correlation
- Incident response and remediation processes
- Cyber threat intelligence and attack lifecycle
- Continuous monitoring and reporting

3. Target Audience

- SOC Analysts (Tier 1 and Tier 2)
- Cybersecurity Operations Professionals
- IT Security and Network Security Engineers
- Incident Response Team Members
- Entry-level professionals pursuing a cybersecurity career

4. Pre-Requisites

- Basic knowledge of networking and operating systems
- Understanding of fundamental cybersecurity concepts is recommended
- No mandatory certification prerequisites

5. Course Content (Modules)

Module 1: Introduction to Cybersecurity Operations

- Cybersecurity operations fundamentals
- SOC structure and responsibilities

Module 2: Threat Detection and Monitoring

- Security logs and event analysis
- SIEM tools and alert handling

Module 3: Incident Response and Analysis

- Incident classification and escalation
- Containment, eradication, and recovery

Module 4: Threat Intelligence and Attack Techniques

- Threat actors and attack vectors
- MITRE ATT&CK framework

Module 5: Security Operations Tools and Reporting

- SOC tools and technologies
- Incident documentation and reporting