CA302: Operational Cyber Defense

26 Instructional Hours 46 CPEs 20 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical exploration of Blue Team operations within modern cybersecurity environments. It covers the structure, roles, and responsibilities of defensive teams, along with the operational frameworks of Security Operations Centers (SOCs). Learners are introduced to core defensive disciplines such as network monitoring, endpoint security, threat intelligence, detection engineering, incident response, and vulnerability management. The material emphasizes real-world application through structured workflows, tools (SIEM, EDR/XDR), and industry frameworks like MITRE ATT&CK, enabling learners to build, operate, and improve defensive security capabilities in organizational settings.

You Will Be Able To

- Monitor and analyze security events using SOC processes and tools such as SIEM and EDR
- Detect, triage, and respond to security incidents using structured playbooks and workflows
- Implement network and endpoint security controls to defend against common attack vectors
- Perform vulnerability management and prioritize remediation based on risk

Who Should Attend

This course is designed for individuals seeking to build or strengthen defensive cybersecurity skills, particularly those interested in Security Operations Center (SOC) roles. It is suitable for beginners to intermediate learners, including IT professionals, system administrators, and aspiring cybersecurity analysts who want hands-on knowledge of monitoring, detection, and incident response. It is also valuable for professionals transitioning from general IT into specialized security roles or aiming to understand real-world Blue Team operations.

Relevant Combat Roles

- SOC Analyst
- Incident Responder / Incident Handler
- Threat Hunter / Threat Intelligence Analyst
- Security Operations Engineer
- Vulnerability Management Analyst

Topics Covered

Blue Team Operations & SOC Fundamentals
(defensive principles, SOC architecture, governance, and metrics)

Threat Intelligence & Detection Engineering
(IOC vs IOA, intel-to-action workflows, detection engineering, alert triage)

Monitoring, Logging & Security Automation
(network security monitoring, SIEM, SOAR, logging, traffic analysis)

Endpoint & Network Security
(EDR/XDR capabilities, segmentation, response playbooks)

Vulnerability Management & Threat Hunting
(exposure management, risk prioritization, threat hunting, MITRE ATT&CK)

Labs

SOC Operations & Incident Response
(SOC alert triage, incident classification, and response playbooks using SIEM tools such as Splunk/ELK)

Network Security Monitoring & Traffic Analysis
(Wireshark traffic analysis, DNS/HTTP(S) attack investigation, network architecture, and access control with IPTables)

Detection Engineering & IDS/IPS
(Snort and Suricata setup, rule creation, and YARA-based detection)

Endpoint Detection & Response (EDR)
(endpoint investigation, host isolation, process termination, and forensic data collection)

SIEM, Logging & Security Analytics
(Splunk, ELK stack setup, log analysis, and security monitoring)