HDTC Training Center

Provide

Technical proposal of the Training program

Certified security operations center Analyst

Course Overview:

The Certified Security Operations Center Analyst (CSOSA) program is designed to equip cybersecurity professionals with the foundational skills and technical capabilities required to work effectively in a modern Security Operations Center (SOC).

It covers real-world techniques in monitoring, detecting, analyzing, responding to, and recovering from cybersecurity threats using industry-leading tools and frameworks.

The course blends theoretical knowledge with hands-on labs to prepare participants for real-time incident response and security event monitoring roles.

General Objective:

To prepare participants to take on entry-to-mid-level roles within a Security Operations Center (SOC) and become effective cybersecurity analysts capable of identifying and responding to evolving cyber threats.

Program Objectives:

By the end of this program, participants will be able to:

- Understand the structure, roles, and responsibilities within a SOC.
- Identify and analyze various types of cyber threats, attack vectors, and indicators of compromise (IoCs).
- Utilize SIEM (Security Information and Event Management) tools for log collection and threat detection.
- Apply threat intelligence in proactive defense strategies.
- Perform real-time monitoring, triage, and incident analysis.
- Follow incident response procedures and escalation protocols.
- Document and report on incidents following best practices.
- Understand compliance frameworks and how SOC supports regulations like ISO 27001, GDPR, and NIST.

Program Outlines:

Day 1: Introduction to Security Operations Centers

- What is a SOC? Roles, responsibilities, structure
- SOC maturity models (MSSP, in-house, hybrid)
- Common tools used in a SOC (SIEM, SOAR, EDR, IDS/IPS)
- SOC Tiers (Tier 1, 2, 3 Analysts and responsibilities)

Day 2: Cyber Threat Landscape and Threat Intelligence

- Common cyber threats: malware, phishing, ransomware, APTs
- MITRE ATT&CK framework
- Threat intelligence lifecycle
- Open-source threat intel platforms (e.g., MISP, VirusTotal)

Day 3: SIEM and Log Management

- Introduction to SIEM tools (e.g., Splunk, IBM QRadar, Elastic SIEM)
- Log collection, normalization, correlation
- Creating alerts, use cases, and dashboards
- Lab: Simulated attack detection with SIEM

Day 4: Incident Detection and Response

- Cyber Kill Chain and incident handling process
- Triage and prioritization of security alerts
- Digital forensics basics: packet capture, log analysis
- Case study: Analyzing a real-world incident

Day 5: Reporting, Escalation, and Compliance

- Incident documentation and reporting
- Escalation matrix and playbooks
- SOC's role in regulatory compliance (ISO 27001, NIST, GDPR)
- Final simulation: Live incident response exercise
- Review and exam preparation (optional)

Target Audience:

- Entry-level cybersecurity professionals
- SOC Tier 1 & Tier 2 analysts
- IT and network administrators transitioning into security roles
- Incident response team members
- Recent graduates seeking a SOC analyst career
- Security enthusiasts looking for hands-on experience

Training methods:

- Technology-Based Learning.
- Simulation in Training.
- On-the-job guidance.
- Trainer-Led Training.
- Work Teams and Roles.
- Films and Videos.
- Case Studies and Workshops.