Certified SOC Analyst (CSA)

Length: 3 Days

Summary: The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

Who Should Attend: SOC Analysts (Tier I and Tier II) Network and Security Administrators, Network and Security Engineers, Network Defense Analyst, Network Defense Technicians, Network Security Specialist, Network Security Operator, and any security professional handling network security operations Cybersecurity Analyst Entry-level cybersecurity professionals Anyone who wants to become a SOC Analyst.

COURSE CONTENT

1 - Security Operations and Management

- Security Management
- Security Operations
- Security Operations Center (SOC)
- Need of SOC
- SOC Capabilities
- SOC Operations
- SOC Workflow
- Components of SOC: People, Process and Technology
- People
- Technology
- Processes
- Types of SOC Models
- SOC Maturity Models
- SOC Generations
- SOC Implementation
- SOC Key Performance Indicators (KPI) and Metrics
- Challenges in Implementation of SOC
- Best Practices for Running SOC
- SOC vs NOC

2 - Understanding Cyber Threats, IoCs, and Attack Methodology

- Cyber Threats
- Intent-Motive-Goal
- Tactics-Techniques-Procedures (TTPs)
- Opportunity-Vulnerability-Weakness
- Network Level Attacks
- Host Level Attacks
- Application Level Attacks
- Email Security Threats
- Understanding Indicators of Compromise (IoCs)
- Understanding Attacker's Hacking Methodology

3 - Incidents, Events, and Logging

- Incident
- Event
- Log
- Typical Log Sources
- Need of Log
- Logging Requirements
- Typical Log Format
- Logging Approaches

- Local Logging
- Centralized Logging

4 - Incident Detection with Security Information and Event Management (SIEM)

- Security Information and Event Management(SIEM)
- Security Analytics
- Need of SIEM
- Typical SIEM Capabilities
- SIEM Architecture and Its Components
- SIEM Solutions
- SIEM Deployment
- Incident Detection with SIEM
- Examples of commonly Used Use Cases Across all SIEM deployments
- Handling Alert Triaging and Analysis

5 - Enhanced Incident Detection with Threat Intelligence

- Understanding Cyber Threat Intelligence
- Why Threat Intelligence-driven SOC?

6 - Incident Response

- Incident Response
- Incident Response Team (IRT)
- Where Does IRT Fits in the Organization?
- SOC and IRT Collaboration
- Incident Response (IR) Process Overview
- Step 1: Preparation for Incident Response
- Step 2: Incident Recording and Assignment
- Step 3: Incident Triage
- Step 4: Notification
- Step 5: Containment
- Step 6: Evidence Gathering and Forensic Analysis
- Step 7: Eradication
- Step 8: Recovery♣ Step 9: Post-Incident Activities
- Responding to Network Security Incidents
- Responding to Application Security Incidents
- Responding to Email Security Incidents
- Responding to an Insider Incidents
- Responding to Malware incidents