EC-COUNCIL CERTIFIED SOC ANALYST (CSA)

DURATION: 3 DAYS

COURSE OVERVIEW

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.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. 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.

This is the recommended training for those students looking to achieve the EC-Council Certified SOC Analyst Certification

TARGET AUDIENCE

SOC Analysts (Tier I and Tier II), Cybersecurity Analysts, Entry-level cybersecurity professionals. Network and Security Administrators

COURSE OBJECTIVES

After completing this course you should be able to:

1. Articulate SOC processes, procedures, technologies, and workflows.
2. Understand and security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, etc.
3. Recognize attacker tools, tactics, and procedures to identify indicators of compromise (IOCs) that can be utilized during active and future investigations.
4. Monitor and analyze logs and alerts from a variety of different technologies across multiple platforms (IDS/IPS, end-point protection, servers and workstations).
5. Apply Centralized Log Management (CLM) processes.
6. Perform Security events and log collection, monitoring, and analysis.
7. Understand Security Information and Event Management.

8. Administer SIEM solutions (Splunk /Alien Vault/OSSIM/ELK).
9. Understand the architecture, implementation and fine tuning of SIEM solutions (Splunk/ Alien Vault/OSSIM/ELK).
10. Gain hands-on experience on SIEM use case development process.
11. Develop threat cases (correlation rules), create reports, etc.
12. Recognize use cases that are widely used across the SIEM deployment.
13. Plan, organize, and perform threat monitoring and analysis in the enterprise.
14. Monitor emerging threat patterns and perform security threat analysis.
15. Gain hands-on experience in alert triaging process.
16. Escalate incidents to appropriate teams for additional assistance.
17. Use a Service Desk ticketing system.
18. Prepare briefings and reports of analysis methodology and results.
19. Integrate threat intelligence into SIEM for enhanced incident detection and response.
20. Make use of varied, disparate, constantly changing threat information.
21. Articulate knowledge of Incident Response Process.
22. Understand SOC and IRT collaboration for better incident response.

COURSE CONTENT

SOC Essential Concepts

Computer Network Fundamentals

TCP/IP Protocol Suite

Application Layer Protocols

Transport Layer Protocols

Internet Layer Protocols

Link Layer Protocols

IP Addressing and Port Numbers

Network Security Controls

Network Security Devices

Windows Security

Unix/Linux Security

Web Application Fundamentals

Information Security Standards, Laws and Acts

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

Challenges in Implementation of SOC

Best Practices for Running SOC

SOC vs NOC

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

Understanding Attacker's Hacking Methodology

Incidents, Events and Logging

Incident

Event

Log

Typical Log Sources

Need of Log

Logging Requirements

Typical Log Format

Logging Approaches

Local Logging

Centralized Logging

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

Enhanced Incident Detection with Threat Intelligence

Understanding Cyber Threat Intelligence

Why-Threat Intelligence-driven SOC?

Incident Response

Incident Response

Incident Response Team (IRT)

Where does IRT Fit 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 Insider Incidents

Responding to Malware Incidents

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

Network Administration or Security Domain experience

TEST CERTIFICATION

Recommended as preparation for the following exam:

312-39 - Certified SOC Analyst

The CSA program requires a candidate to have one year of work experience in the Network Admin/Security domain and should be able to provide proof of the same as validated through the application process unless the candidate attends official training.