CSA: EC-Council Certified SOC Analyst

Course Code: CSA
Duration: 3 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

The Certified 90C 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 certification 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.

As the security landscape is expanding, a SOC team offers high-quality IT-security services to detect potential cyber threats/attacks actively and quickly respond to security incidents. Organizations need skilled SOC Analyst who can serve as the front-line defenders, warning other professionals of emerging and present cyber threats.

The lab-intensive SOC analyst certification program emphasizes the holistic approach to deliver elementary as well as advanced knowledge of how to identity and validate intrusion attempts. Through this, the candidate will learn to use SIEM solutions and predictive capabilities using threat intelligence. The program also introduces the practical aspect of SIEM using advanced and the most frequently used tools. The candidate will learn to perform enhanced threat detection using the predictive capabilities of Threat Intelligence.

Recent years have witnessed the evolution of cyber risks, creating an unsafe environment for the players of various sectors. To handle these sophisticated threats, enterprises need advanced cybersecurity solutions along with traditional methods of defense. Practicing good cybersecurity hygiene and implementing an appropriate line of defense, and incorporating a security operations center (SOC) has become reasonable solutions. The team pursues twenty-four-hour and "follow-the-sun" coverage for performing security monitoring, security incident management, vulnerability management, security device management, and network flow monitoring. Read more about the functions of SOC here.

A SOC Analyst continuously monitors and detects potential threats, triages the alerts, and appropriately escalates them. Without a SOC analyst, processes such as monitoring, detection, analysis, and triaging will lose their effectiveness, ultimately negatively affecting the organization.

SKILLS COVERED

- Gain Knowledge of SOC Processes, Procedures, Technologies, And Workflows Is
- Gain A Basic Understanding and In-Depth Knowledge Of Security Threats, Attacks, Vulnerabilities, Attacker's Behaviors, Cyber Killchain, Etc.

- Able To Recognize Attacker Tools, Tactics, And Procedures to Identify Indicators of Compromise (10Cs) That Can Be Utilized During Active and Future Investigations
- Able To Monitor and analyze Logs and Alerts from A Variety of Different Technologies Across Multiple Platforms (IDS/IPS, End-Point Protection, Servers, And Workstations).
- Gain Knowledge of The Centralized Log Management (CLM) Process.
- Able To Perform Security Events and Log Collection, Monitoring, And Analysis.
- Gain Experience and Extensive Knowledge of Security Information and Event Management.
- Gain Knowledge of Administering SIEM Solutions (Splunk/AlienVault/OSSIM/ELK)
- Gain Knowledge of Administering SIEM Solutions (Splunk/Alien/ault/OSSIM/ELK),
- Gain Hands-On Experience in SIEM Use Case Development Process.
- Able To Develop Threat Cases (Correlation Rules), Create Reports, Etc.
- Learn Use Cases That Are Widely Used Across the SIEM Deployment.
- Plan, Organize, And Perform Threat Monitoring and Analysis in The Enterprise.
- Able To Monitor Emerging Threat Patterns and Perform Security Threat Analysis.
- Gain Hands-On Experience In The Alert Triaging Process.
- Able To Escalate Incidents to Appropriate Teams for Additional Assistance.
- Able To Use a Service Desk Ticketing System.
- Able To Prepare Briefings and Reports Of Analysis Methodology And Results.
- Gain Knowledge of Integrating Threat Intelligence into SIEM For Enhanced Incident Detection and Response.
- Able To Make Use of Varied, Disparate, Constantly Changing Threat Information.
- Gain Knowledge of Incident Response Process.
- Gain Understating of SOC And IRT Collaboration for Better Incident Response.

WHO SHOULD ATTEND?

- Individual contributors, managers, directors and other leaders who need strategic thinking skills to gain better business insights and identify trends that can contribute to a more successful business strategy

PREREQUISITES

There are no prerequisites required to attend this course.

MODULES

Module 00: 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

Module 01: 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

Module 02: 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
- Exercise 1: Application Level Threats: Understanding the Working of SQL Injection
  Attacks
- Exercise 2: Application Level Threats: Understanding the Working of XSS Attacks
- Exercise 3: Network Level Threats: Understanding the Working of Network Scanning Attacks
- Exercise 4: Host Level Threats: Understanding the Working of Brute Force Attacks

Module 03: Incidents, Events, and Logging

- Incident
- Event
- Log
- Typical Log Sources
- Need of Log
- Logging Requirements
- Typical Log Format
- Logging Approaches
- Local Logging
- Centralized Logging
- Exercise 1: Local Logging: Configuring, Monitoring, and Analyzing Windows Logs
- Exercise 2: Local Logging: Configuring, Monitoring, and Analyzing IIS Logs
- Exercise 3: Local Logging: Configuring, Monitoring, and Analyzing Snort IDS Logs
- Exercise 4: Centralized Logging: Collecting Logs from Different Devices into
  Centralized Location

Module 04: 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
- Exercise 1: Creating Splunk Use Case and Generating Alerts for Brute-force Attempts
- Exercise 2: Creating Splunk Use Case and Generating Alerts for SQL Injection Attempts
- Exercise 3: Creating Splunk Use Case and Generating Alerts for XSS Attempts
- Exercise 4: Creating Splunk Use Case and Generating Alerts for Network Scanning Attempts
- Exercise 5: Creating Splunk Use Case for Registry Monitoring
- Exercise 6: Creating Splunk Use Case for Monitoring Insecure Ports and Services

Module 05: Enhanced Incident Detection with Threat Intelligence

- Understanding Cyber Threat Intelligence
- Why Threat Intelligence-driven SOC?
- Exercise 1: Integrating IoCs into ELK Stack
- Exercise 2: Integrating OTX Threat Data in OSSIM
- Exercise 3: Integrating Threat Intelligence Capability of OSSIM

Module 06: 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
- Exercise 1: Generating Tickets for Incidents
- Exercise 2: Containing Data Loss Incidents
- Exercise 3: Eradicating SQL injection and XSS Incidents
- Exercise 4: Recovering from Data Loss Incidents
- Exercise 5: Reporting an Incident

END OF PAGE