Certified SOC Analyst v1 (CSA)

Duration 3 Days

COURSE DESCRIPTION

The Certified SOC Analyst (CISA) 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.

C|SA 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.

COURSE OBJECTIVE

- Gain Knowledge Of SOC Processes, Procedures, Technologies, And Workflows.
- 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 (IOCs) 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/AlienVault/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.

COURSE OUTLINE

Module 01: Security Operations and Management
Module 02: Understanding Cyber Threats, loCs, and Attack Methodology
Module 03: Incidents, Events, and Logging
Module 04: Incident Detection with Security Information and Event Management (SIEM)
Module 05: Enhanced Incident Detection with Threat Intelligence
Module 06: Incident Response

WHO SHOULD ATTEND

- SOC Analysts (Tier I and Tier ll)
- 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.

PREREQUISITES

To ensure that participants can successfully engage with and benefit from the Certified SOC Analyst (CSA) course, the following minimum prerequisites are recommended:

- Basic understanding of networking concepts, including TCP/IP protocols and network topology.
- Familiarity with operating systems, particularly Windows and Linux, and their command line interfaces.
- Knowledge of information security principles, including confidentiality, integrity, and availability.
- An introductory level of understanding of various types of cyber threats and common attack vectors.
- Awareness of security devices such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).
- Some experience with or exposure to security information and event management (SIEM) systems is beneficial but not mandatory.
- Problem-solving skills and analytical thinking to effectively participate in incident detection and response activities.

These prerequisites are designed to provide a foundation upon which the CSA course content can build. They are not meant to be barriers but rather to ensure a productive and enriching learning experience. Individuals with a keen interest in cybersecurity and a willingness to learn will find that the course offers the necessary guidance to develop their skills as a SOC analyst.

EXAM

The CISA exam is designed to test and validate a candidate's comprehensive understanding of the job tasks required as a SOC analyst. Thereby, validating their comprehensive understanding of a complete SOC workflow.

Exam Eligibility Requirement

The CISA 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.

Exam Code: 312-39
Number of Questions: 100
Exam Title: Certified SOC Analyst
Test Duration: 3 Hours
Test Format: Multiple Choice
Availability: EC-Council Exam Portal