EC-Council Certified SOC Analyst (CSA)

Course overview

EC-Council Certified Security Analyst Training Program will help you to master over trending and in-demand technical skills like

- Knowledge of SOC processes, procedures of these processes, technologies, and workflows.
- basic understanding and detailed knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, etc.

Through this SOC Analyst Certification Training our expert trainers offer in-depth knowledge with enhanced level capabilities for dynamic contribution to a SOC team.

- CSA Training Course has been especially designed to help you learn:
- The basics of SOC operations,
- log management and correlation,
- SIEM deployment,
- advanced incident detection, and incident response.
- This SOC Analyst course will also help you to improve your knowledge regarding performance of enhanced threat detection using the predictive capabilities of Threat Intelligence.

Why Certified SOC Analyst (CSA)?

SOC Analyst Certification acts as a launchpad for developing a security professional.

- It is very much in demand at present in the industry. This certification will not only enhance your knowledge but will also:
- Help you to demonstrate your skills and working experience for SOC Analyst job role.
- Let you secure a job in the other network security related job roles which are now one of the top paying jobs of the year.
- Make you updated with latest skillset necessary for L1/L2 SOC Analyst
- Bring you in demanded by the employers.

Target Audience

- L1/L2 SOC Analysts
- 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.

Pre-Requisite

To apply for SOC Analyst Certification one year of work experience in the Network Admin/Security domain is compulsory. If the candidate attends official training this, experience isn't required.

Course Outline

Module #	Module Topic	Description
Module 01	Introduction to Ethical Hacking	• Understand the SOC Fundamentals • Discuss the Components of SOC: People, Processes and Technology • Understand the Implementation of SOC
Module 02	Understanding Cyber Threats, IoCs, and Attack Methodology	• Describe the term Cyber Threats and Attacks • Understand the Network Level Attacks • Understand the Host Level Attacks • Understand the Application-Level Attacks • Understand the Indicators of Compromise (IoCs) • Discuss the Attacker's Hacking Methodology
Module 03	Incidents, Events, and Logging	• Understand the Fundamentals of Incidents, Events, and Logging • Explain the Concepts of Local Logging • Explain the Concepts of Centralized Logging

Module 04	Incident Detection with Security Information and Event Management (SIEM)	• Understand the Basic Concepts of Security Information and Event Management (SIEM) • Discuss the Different SIEM Solutions • Understand the SIEM Deployment • Learn Different Use Case Examples for Application-Level Incident Detection • Learn Different Use Case Examples for Insider Incident Detection • Learn Different Use Case Examples for Network Level Incident Detection • Learn Different Use Case Examples for Host Level Incident Detection • Learn Different Use Case Examples for Compliance • Understand the Concept of Handling Alert Triaging and Analysis
Module 05	Enhanced Incident Detection with Threat Intelligence	• Learn Fundamental Concepts on Threat Intelligence • Learn Different Types of Threat Intelligence • Understand How Threat Intelligence Strategy is Developed • Learn Different Threat Intelligence Sources from which Intelligence can be Obtained. • Learn Different Threat Intelligence Platform (TIP) • Understand the Need of Threat Intelligence-driven SOC
Module 06	Incident Response	• Understand the Fundamental Concepts of Incident Response • Learn Various Phases in Incident Response Process • Learn How to Respond to Network Security Incidents • Learn How to Respond to Application Security Incidents • Learn How to Respond to Email Security Incidents • Learn How to Respond to Insider Incidents • Learn How to Respond to Malware Incidents

Exam Details

Exam Details	C|SA (MCQ Exam)
Number of Questions/Practical Challenges	100
Test Duration	180 minutes
Test Format	Multiple Choice Questions
Test Delivery	ECC EXAM, VUE
Passing Score	70%