

(CSA) Certified SOC Analyst

Modality: Virtual Classroom

Duration: 5 Days

What's Included:

- *Official EC Council Invitation to the virtual class*
- *Official EC Council Print or e-courseware. **included***
- *Official EC Council ilabs subscription (6 months)*
- *EC Council Exam Voucher with Remote Proctoring Service **included***

About this Course:

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. 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 actively detect potential cyber threats/attacks and quickly respond to security incidents. Organizations need skilled SOC Analysts who can serve as the front-line defenders, warning other professionals of emerging and present cyber threats.

The lab-intensive CSA program emphasizes the holistic approach to deliver elementary as well as advanced knowledge of how to identify 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.

Course Objectives:

- Gain Knowledge of SOC processes, procedures, technologies, and workflows.
- Gain basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, 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 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 on administering SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Understand the architecture, implementation and fine tuning of SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Gain hands-on experience on 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 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

Audience:

- 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 Outline:

Module 1:

Security Operations and Management

Module 2:

Understanding Cyber Threats, IoCs, and Attack Methodology

Module 3:

Incidents, Events, and Logging

Module 4:

Incident Detection with Security Information and Event Management (SIEM)

Module 5:

Enhanced Incident Detection with Threat Intelligence

Module 6:

Incident Response