CSA – Certified SOC Analyst

EC-Council

Com certificação

- **Nível:** Intermédio
- **Duração:** 24h

Sobre o curso

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.

Learning Objectives of CSA

- 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.

Certification

After the completion of the CSA training, candidates will be ready to attempt the **Certified SOC Analyst** exam. Upon successful completion of the exam, with a score of at least 70%, the candidate will be entitled to the CSA certificate and membership privileges. Members are expected to adhere to recertification requirements through EC-Council's Continuing Education Requirements.

Destinatários

- 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.

Pré-requisitos

Exam Eligibility Requirement

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.

Programa

- Security Operations and Management
- Understanding Cyber Threats, IoCs, and Attack Methodology
- Incidents, Events, and Logging
- Incident Detection with Security Information and Event Management (SIEM)
- Enhanced Incident Detection with Threat Intelligence
- Incident Response