EC-Council

C|S|A
Certified SOC Analyst

CERTIFIED SOC ANALYST (CSA)

Security Origin

Index:

CERTIFIED SOC ANALYST

Transition into a role as a cyber emergency responder!

A security operations center (SOC) analyst certification program is a stepping stone to a career in a security operations center (SOC). These programs are designed to equip current and aspiring SOC analysts with the skills to perform basic and intermediate tasks.

Elevate your cybersecurity expertise with CSA: The premier training program empowering SOC professionals for dynamic threat response

The Certified SOC Analyst (CSA) program is a fast-paced training course designed to equip you with the latest and most sought-after technical skills for a successful SOC career. Led by industry veterans, the program provides in-depth knowledge to empower you to excel within a SOC team. This intensive 30-40 hours program delves into the core principles of SOC operations, followed by practical training in log management and analysis, SIEM system implementation, advanced techniques for identifying security incidents, and effective incident response strategies. You'll also gain proficiency in managing various SOC workflows and collaborating seamlessly with CSIRT teams during security events.

Overview:

The CSA program is designed to equip you with the knowledge and skills necessary to thrive in a Security Operations Center (SOC) environment. It is meticulously crafted to align 100% with the National Initiative for Cybersecurity Education (NICE) framework under the "Protect and Defend (PR)" category for the role of Cyber Defense Analyst (CDA).

The curriculum dives deep into Security Information and Event Management (SIEM) solutions, equipping you with the expertise to detect incidents through advanced techniques like signature and anomaly-based detection. You'll gain proficiency in identifying threats across various levels, including application, network, host, and insider threats. Additionally, a dedicated module on Threat Intelligence empowers you to leverage this knowledge to enhance your incident detection capabilities and integrate threat intelligence feeds seamlessly into your SIEM for superior threat protection.

The program prioritizes hands-on learning through practical exercises in incident monitoring, detection, triaging, and analysis. You'll gain valuable experience in containment, eradication, recovery, and reporting of security incidents. To solidify your learning, the program incorporates 80 different tools and utilizes 22 lab simulations that mirror real-world SOC environments. These labs provide practical experience in various areas, such as understanding attacker behaviors across application, network, and host levels, exploring local and centralized logging concepts, developing SIEM use cases, effectively triaging alerts, prioritizing and escalating incidents, and crafting comprehensive incident reports.

For further exploration, the CSA program offers extensive reference materials, including a comprehensive list of 291 use cases specific to popular SIEM solutions like ArcSight, Qradar, LogRhythm, and Splunk. This additional resource empowers you to delve deeper into the practical applications of your newfound knowledge.

Why you should choose CSA:

Addresses the Growing Threat Landscape: The passage highlights the increasing complexity of cyber threats. The CSA program equips you with the skills to actively detect and respond to these evolving threats.

Fills the Need for Skilled SOC Analysts: Organizations are seeking skilled SOC analysts to defend against cyberattacks. The CSA program positions you as a front-line defender with the expertise to identify and validate intrusion attempts.

Holistic Approach with Hands-on Learning: The program offers a comprehensive curriculum that covers both fundamental and advanced concepts. It emphasizes practical skills through lab exercises, allowing you to gain real-world experience with SIEM solutions, threat intelligence, and various security tools.

Focuses on Enhanced Threat Detection: The program teaches you to leverage threat intelligence and advanced techniques for superior detection of potential cyber threats.

Prepares You for Real-World SOC Environments: With its focus on practical applications and simulated SOC workflows, the CSA program equips you with the necessary skills to excel in a real-world SOC environment.

In essence, the CSA program provides a comprehensive and practical training experience that prepares you to be a valuable asset in today's demanding cybersecurity landscape.

Target Audience:

The Certified SOC Analyst (CSA) certification targets individuals seeking to validate their knowledge and skills in network security, particularly those in the following categories:

- **Entry-level cybersecurity professionals:** Individuals new to the cybersecurity field seeking to gain foundational knowledge and skills in protecting systems and networks from cyber threats.
- **SOC Analysts (Tier I and Tier II):** Front-line defenders responsible for monitoring, detecting, and responding to potential cyber threats within an organization's network.
- **Cybersecurity Analysts:** Experts tasked with analyzing and mitigating cyber risks and vulnerabilities to safeguard digital assets and infrastructure.
- **Network and Security Administrators, Network and Security Engineers, Network Defense Analysts, Network Defense Technicians, Network Security Specialists, Network Security Operators:** Professionals overseeing the design, implementation, and maintenance of network security measures to protect against cyber threats.
- **Anyone who wants to become a SOC Analyst:** Individuals interested in pursuing a career in security operations, focusing on monitoring, detecting, and responding to cybersecurity incidents.

The CSA caters to a broad audience within the cybersecurity domain, offering a comprehensive understanding of network security fundamentals and emerging technologies.

Pre-requisites:

The CSA program seeks candidates with one year of verifiable experience in network administration or security. This experience can be demonstrated during the application process. However, if you lack this experience, consider attending the official training program offered by the CSA to qualify for the certification.

Exam Information:

Number of Questions: 100	Test Duration: 3 Hours
Test Format: Multiples Choice	Test Delivery: Online Proctored
Exam Prefix: 312-39	Passing Score: 70%

Course Objectives:

Module 01: Security Operations and Management

Learn the principles and practices of security operations, including management strategies for effective cyber defense.

Module 02: Understanding Cyber Threats, IoCs, and Attack Methodology

Gain insight into various cyber threats, indicators of compromise (IoCs), and attack techniques to enhance threat awareness and response capability.

Module 03: Incidents, Events, and Logging

Explore incident and event management processes, focusing on effective logging practices for accurate threat detection and response.

Module 04: **Incident Detection with Security Information and Event Management (SIEM)**

Understand the role of SIEM systems in detecting and analyzing security incidents, leveraging log data for proactive threat detection.

Module 05: **Enhanced Incident Detection with Threat Intelligence**

Enhance incident detection capabilities through the integration of threat intelligence feeds, enabling proactive identification of emerging threats.

Module 06: **Incident Response**

Develop the skills and processes necessary to effectively respond to security incidents, minimizing impact and restoring normal operations efficiently.

Module 07: **Endpoint Security - Mobile Devices**

-Addresses security considerations and measures for mobile devices, covering both Android and iOS platforms.

Module 08: **Endpoint Security - IoT Devices**

-Discusses security concerns and strategies for Internet of Things (IoT) devices, which are increasingly connected to networks.

Module 09: **Administrative Application Security**

-Focuses on securing applications from an administrative standpoint, covering best practices and policies to ensure application security.

Module 10: **Data Security**

-Addresses strategies and technologies to secure sensitive data, including encryption, access controls, and data loss prevention measures.

Module 11: Enterprise Virtual Network Security

-Covers security considerations for virtualized environments, including virtual networks and virtual machines.

Module 12: Enterprise Cloud Security

-Explores security challenges and solutions related to cloud computing, focusing on securing data and applications in the cloud.

Module 13: Enterprise Wireless Network Security

-Addresses security concerns specific to wireless networks, including encryption protocols and access controls.

Module 14: Network Traffic Monitoring and Analysis

-Discusses techniques and tools for monitoring and analyzing network traffic to identify potential security threats.

Module 15: Network Logs Monitoring and Analysis

-Focuses on the monitoring and analysis of logs generated by network devices to detect and respond to security incidents.

Module 16: Incident Response and Forensics Investigation

-Covers the process of responding to security incidents and conducting forensic investigations to identify the root cause.

Module 17: Business Continuity and Disaster Recovery

-Addresses strategies for ensuring business continuity and recovery from disasters, including the development of contingency plans.

Module 18: Risk Anticipation with Risk Management

-Discusses risk management principles and practices, including risk assessment, mitigation strategies, and risk monitoring.

Module 19: Threat Assessment with Attack Surface Analysis

-Explores methods for assessing and analyzing threats, including understanding the attack surface and potential vulnerabilities.

These modules collectively provide a comprehensive overview of network and cybersecurity, covering a wide range of topics to prepare professionals for securing diverse IT environments.

What you will learn:

- 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.

C|S A
CERTIFIED
SOC ANALYST
www.Securityorigin.com