CERTIFIED SOC ANALYST (CSA)

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.
Recent years have witnessed the evolution of cyber risks, creating an unsafe environment for the players of various sectors.
To handle these sophisticated threats, enterprises need advanced cybersecurity solutions along with traditional methods of defense. Practicing good cybersecurity hygiene and implementing an appropriate line of defense, and incorporating a security operations center (SOC) have become reasonable solutions. The team pursues twenty-four-hour and “follow-the-sun” coverage for performing security monitoring, security incident management, vulnerability management, security device management, and network flow monitoring.
A SOC Analyst continuously monitors and detects potential threats, triages the alerts, and appropriately escalates them. Without a SOC analyst, processes such as monitoring, detection, analysis, and triaging will lose their effectiveness, ultimately negatively affecting the organization.
- EY Global Information Security Survey 2018–19

Nearly 6 in 10 financial service providers own a Security Operations Center (SOC).

Target Audience

Suggested Duration

• 3 days (9 am – 5 pm)
• Minimum of 24 hours

Certification

After the completion of the CSA training, candidates will be **CERTIFIED SOC ANALYST (CSA)**

Course Description

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.

NASCIO Representing Chief Information Office of the States revealed in over a year-long survey (July 2016 – December 2017), “since the creation of the SOC, the security division has seen an overall 64 percent decrease in incident response time.”

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.
Recent years have witnessed the evolution of cyber risks, creating an unsafe environment for the players of various sectors.
To handle these sophisticated threats, enterprises need advanced cybersecurity solutions along with traditional methods of defense. Practicing good cybersecurity hygiene and implementing an appropriate line of defense, and incorporating a security operations center (SOC) have become reasonable solutions. The team pursues twenty-four-hour and "follow-the-sun" coverage for performing security monitoring, security incident management, vulnerability management, security device management, and network flow monitoring.
A SOC Analyst continuously monitors and detects potential threats, triages the alerts, and appropriately escalates them. Without a SOC analyst, processes such as monitoring, detection, analysis, and triaging will lose their effectiveness, ultimately negatively affecting the organization.
- EY Global Information Security Survey 2018–19
Nearly 6 in 10 financial service providers own a Security Operations Center (SOC).
Target Audience
Suggested Duration
• 3 days (9 am – 5 pm)
• Minimum of 24 hours
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.
• *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.
The CSA exam is designed to test and validate a candidate's comprehensive understanding of the jobs tasks required as a SOC analyst. Thereby validating their comprehensive understanding of a complete SOC workflow
The CSA program requires a candidate to have 1 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 Title	Certified SOC Analyst
Exam Code	312-39
Number of Questions	100
Duration	3 hours
Availability	EC-Council Exam Portal (please visit https://www. eccexam.com)
Test Format	Multiple Choice
Passing Score	70%

Exam Details
Exam Eligibility Requirement
8 Critical Components of CSA
1. 100% Compliance to NICE 2.0 Framework
CSA maps 100 percent to the National Initiative for Cybersecurity Education (NICE) framework under the "Protect and Defend (PR)" category for the role of Cyber Defense Analysis (CDA). It is designed as per the realtime job roles and responsibilities of a SOC analyst.
The CSA course trains the candidate to use various defensive measures and data collected from multiple sources to identify, analyze, and report events that might occur or are already present in the network to protect data, systems, and networks from threats.
2. Emphasizes on End-to-End SOC workflow
CSA offers an insightful understanding of end-to-end SOC overflow. It includes all SOC procedures, technologies, and processes to collect, triage, report, respond, and document the incident.
3. Learn Incident Detection with SIEM
Training on various use cases of SIEM (Security

Information and Event Management) solutions to detect incidents through signature and anomaly-based detection technologies. Candidates will learn incident detection on different levels - Application level, Insider level, Network level, and Host level.

4. Enhanced Incident Detection with Threat Intelligence

CSA covers a module dedicated to rapid incident detection with Threat Intelligence. The module also imparts knowledge on integrating Threat Intelligence feeds into SIEM for enhanced threat detection.

5. Elaborate Understanding of SIEM Deployment

It covers 45 elaborated use cases which are widely used across all the SIEM deployments.

6. Promotes Hands-On Learning

CSA being a practically-driven program, offers hands-on experience on incident monitoring, detection, triaging, and analysis. It also covers containment, eradication, recovery, and reporting of the security incidents. To that end, there are 80 tools incorporated into the training.

7. Lab Environment Simulates a Realtime Environment

There are 22 labs in total in the CSA program, which demonstrates processes aligned to the SOC Workflow. These include, but are not restricted to, activites such as:

- Modus operandi of different type of attacks at application, network and host level to understand thier IOCs
- Working of local and centralized logging concepts which demonstrates how logs are pulled from the different devices on the network to facilitate incident monitoring, detection, and analysis
- Examples of SIEM use case development for detecting application, network and host level incidents using various SIEM tools
- Triaging of alerts to provide rapid incident detection and response
- Prioritization and escalation of incidents by generating incident ticket
- The containment of incidents
- The eradication of incidents
- The recovery from the incidents
- Creating report of the incidents

8. Learn More with Additional Reference Material

The CSA program comes with additional reference material, including a list of 291 common and specific use cases for ArcSight,

Qradar, LogRhythm, and Splunk's SIEM deployments.

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

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.

I strongly feel that this program provides necessary skills for a SOC Analyst job role at level L1 and L2. I also believe this program will help us in upskilling our SOC team. This course certainly benefits Network Security Admins/Other Network Sec Job roles and equips them with the knowledge to become a SOC Analyst.
The program provides an In depth training of SOC skills and tools and is also beneficial to all aspects of security program (GRC, IAM), and people in help desk and networking teams.
- Dan Bowden,
CISO, Sentara Healthcare, USA

I see this as the first structured programme devoted to the skills required for a SOC Analyst with specific focus on the job requirements. This is a well designed course and would benefit the SOC professionals/ aspirants in acquiring the overall understanding of the skills required.
As a subset of the skills required in the SOC Analyst job, this program will also benefit other Network Security related job roles.
- Prabir Panda,
Enterprise Architect Security,
Election Commission of India

This program provides the necessary academic background provide necessary skill set for a SOC Analyst job role at level L1 and L2. A virtual environment with various scenarios with playbook & runbooks examples further enhances practical skills. The program will benefit our SOC team and act as valuable reference material.
According to me, the major strength of this program is the academic research conducted behind the creation of this program. The Digital Forensic team, Resilience, Incident Response and Threat Intelligence teams can also greatly benefit from this program.

- Dawie Wentzel,
Head of Cyber Forensics,
Absa Group, South Africa

I see this program as a logical step an Analyst could use to progress to the next/a higher level certification, or open the opportunity to move laterally to new certifications. A major strength I see is the program covers all areas/skills for individuals in sufficient depth to successfully operate as SOC Analysts, and/or use the program as a launchpad to develop as a security professional. I am confident that this program will provide the skill set necessary for L1/L2 SOC Analysts.
- Miki Calero,
Founder,
Urbis Global LLC (Ex-US Army)
e 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.

- *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.*

8 Critical Components of CSA

1. 100% Compliance to NICE 2.0 Framework

CSA maps 100 percent to the National Initiative for Cybersecurity Education (NICE) framework under the “Protect and Defend (PR)” category for the role of Cyber Defense Analysis (CDA). It is designed as per the realtime job roles and responsibilities of a SOC analyst.

The CSA course trains the candidate to use various defensive measures and data collected from multiple sources to identify, analyze, and report events that might occur or are already present in the network to protect data, systems, and networks from threats.

2. Emphasizes on End-to-End SOC workflow

CSA offers an insightful understanding of end-to-end SOC overflow. It includes all SOC procedures, technologies, and processes to collect, triage, report, respond, and document the incident.

3. Learn Incident Detection with SIEM

Training on various use cases of SIEM (Security Information and Event Management) solutions to detect incidents through signature and anomaly-based detection technologies. Candidates will learn incident detection on different levels - Application level, Insider level, Network level, and Host level.

4. Enhanced Incident Detection with Threat Intelligence

CSA covers a module dedicated to rapid incident detection with Threat Intelligence. The module also imparts knowledge on integrating Threat Intelligence feeds into SIEM for enhanced threat detection.

5. Elaborate Understanding of SIEM Deployment

It covers 45 elaborated use cases which are widely used across all the SIEM deployments.

6. Promotes Hands-On Learning

CSA being a practically-driven program, offers hands-on experience on incident monitoring, detection, triaging, and analysis. It also covers containment, eradication, recovery, and reporting of the security incidents. To that end, there are 80 tools incorporated into the training.

7. Lab Environment Simulates a Realtime Environment

There are 22 labs in total in the CSA program, which demonstrates processes aligned to the SOC Workflow. These include, but are not restricted to, activites such as:

- Modus operandi of different type of attacks at application, network and host level to understand thier IOCs
- Working of local and centralized logging concepts which demonstrates how logs are pulled from the different devices on the network to facilitate incident monitoring, detection, and analysis
- Examples of SIEM use case development for detecting application, network and host level incidents using various SIEM tools
- Triaging of alerts to provide rapid incident detection and response
- Prioritization and escalation of incidents by generating incident ticket
- The containment of incidents
- The eradication of incidents
- The recovery from the incidents
- Creating report of the incidents

8. Learn More with Additional Reference Material

The CSA program comes with additional reference material, including a list of 291 common and specific use cases for ArcSight, Qradar, LogRhythm, and Splunk's SIEM deployments.

I strongly feel that this program provides necessary skills for a SOC Analyst job role at level L1 and L2. I also believe this program will help us in

upskilling our SOC team. This course certainly benefits Network Security Admins/Other Network Sec Job roles and equips them with the knowledge to become a SOC Analyst.
The program provides an In depth training of SOC skills and tools and is also beneficial to all aspects of security program (GRC, IAM), and people in help desk and networking teams.
- Dan Bowden,
CISO, Sentara Healthcare, USA

I see this as the first structured programme devoted to the skills required for a SOC Analyst with specific focus on the job requirements. This is a well designed course and would benefit the SOC professionals/ aspirants in acquiring the overall understanding of the skills required. As a subset of the skills required in the SOC Analyst job, this program will also benefit other Network Security related job roles.
- Prabir Panda,
Enterprise Architect Security,
Election Commission of India

This program provides the necessary academic background provide necessary skill set for a SOC Analyst job role at level L1 and L2. A virtual environment with various scenarios with playbook & runbooks examples further enhances practical skills. The program will benefit our SOC team and act as valuable reference material. According to me, the major strength of this program is the academic research conducted behind the creation of this program. The Digital Forensic team, Resilience, Incident Response and Threat Intelligence teams can also greatly benefit from this program.
- Dawie Wentzel,
Head of Cyber Forensics,
Absa Group, South Africa

I see this program as a logical step

an Analyst could use to progress to the next/a higher level certification, or open the opportunity to move laterally to new certifications. A major strength I see is the program covers all areas/skills for individuals in sufficient depth to successfully operate as SOC Analysts, and/or use the program as a launchpad to develop as a security professional. I am confident that this program will provide the skill set necessary for L1/L2 SOC Analysts.
- Miki Calero,
Founder,
Urbis Global LLC (Ex-US Army)