EC-Council Certified SOC Analyst | CSA

EC-Council – Certified SOC Analyst | CSA

The World’s No. 1 Ethical Hacking Certification for 20 Years

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. 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.

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.

Course Goals:

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).
- Understand the architecture, implementation and fine-tuning of 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.

Course Format:

Присъствен (Classroom) Курс в Учебната ни зала или В Офис на Клиент	Онлайн (Online/Virtual) Курс във виртуална зала с инструктор

Course Language Option:

Български (Bulgarian)	Английски (English)

Student Guides:

The training materials are available in electronic format. They can be used online / offline on any device. Lifetime access.

Lab Environment:

At Course Completion:

Lifetime Access - Video Archive 24/7	**Certificate of Course Completion**

Course Duration:

- 3 working days (09:00 – 17:00 / 9:00 am – 5:00 pm) UTC +2 (contact us for another Time Zone)

or

- **24 learning hours after hours (2 weeks, classes are held 2 times a week in one of the following options):**
- Sat. and Sun. 10:00 – 14:00 or 14:00 – 18:00 or 18:00 – 22:00
- Mon. and Wed. 19:00 – 23:00

- Tue. or Thu. 19:00 – 23:00

Payment:

VISA MasterCard Maestro AMERICAN EXPRESS

PayPal BANK TRANSFER

Next Class:

■

- There are no upcoming events.

For more information, use the contact format. We will contact you to confirm the data.

All EC-Council Course Schedules

■

- There are no upcoming events.

CEHv12 Brochure.cleaned