Certified SOC Analyst (CSA)

Duration: 3 Days

Course Description:

The EC-Council Certified SOC Analyst (CSA) program equips learners with essential skills in security operations, threat intelligence, and incident response. It covers the processes, technologies, and techniques used to detect, investigate, and respond to threats while covering attack vectors, SIEM deployment (with 350 use cases), and SOC development. Students gain proficiency in Centralized Log Management, incident triaging, investigating loCs, and applying the cyber kill chain. They also learn to create effective reports and leverage AI-enabled tools and platforms to enhance SIEM capabilities, automate threat detection, prioritize alerts, and support threat hunting— critical skills for building a successful SOC analyst career.

Course Objectives:

- Acquire a comprehensive knowledge of SOC processes, procedures, technologies, and workflows.
- Develop a foundational and advanced understanding of security threats, attacks, vulnerabilities, attacker behavior, and the cyber kill chain.
- Learn to identify attacker tools, tactics, and procedures to recognize indicators of compromise (loCs) for both active and future investigations.
- Gain the ability to monitor and analyze logs and alerts from various technologies across multiple platforms, including DS/PS, endpoint protection, servers, and workstations.
- Understand the centralized log management (CLM) process and its significance in security operations.
- Acquire skills in collecting, monitoring, and analyzing security events and logs.
- Attain extensive knowledge and hands-on experience in security information and event management (SIEM).
- Learn how to administer SIEM solutions such Splunk, AlienVault, OSSIM, and the ELK Stack.
- Understand the architecture, implementation, and fine-tuning of SIEM solutions for optimal performance.
- Gain practical experience in the SIEM use case development process.
- Develop threat detection cases (correlation rules) and create comprehensive reports.
- Learn about widely used SIEM use cases across different deployments.
- Plan, organize, and execute threat monitoring and analysis within an enterprise environment.
- Acquire skills to monitor emerging threat patterns and perform security threat analysis.
- Gain hands-on experience in the alert triaging process for effective threat management
- Learn how to escalate incidents to the appropriate teams for further investigation and remediation.
- Use service desk ticketing systems for efficient incident tracking and resolution.
- Develop the ability to prepare detailed briefings and reports outlining analysis methodologies and results.
- Learn how to integrate threat intelligence into SIEM systems for enhanced incident detection and response.
- Understand how to leverage diverse and continually evolving sources of threat intelligence.
- Gain knowledge of the incident response process and best practices for managing security incidents.
- Develop a solid understanding of SOC and incident response team (IRT) collaboration for improved incident management and response.
- Assist in responding to and investigating security incidents using forensic analysis techniques.
- Gain specialized knowledge in cloud-based threat detection and how to adapt techniques for cloud environments
- Engage in proactive threat detection by participating in threat-hunting exercises.
- Develop skills in creating SIEM dashboards, generating SOC reports, and building effective correlation rules for advanced threat detection.
- Acquire hands-on experience in malware analysis techniques.
- Explore how AI/ML technologies can be leveraged to improve threat detection and response in SOC operations

Course Outlines:

- Module 01: Security Operations and Management
- Module 02: Understanding Cyber Threats, loCs, and Attack Methodology
- Module 03: Log Management
- Module 04: Incident Detection and Triage
- Module 05: Proactive Threat Detection
- Module 06: Incident Response
- Module 07: Forensic Investigation and Malware Analysis
- Module 08: SOC for Cloud Environments