EC-Council

CSA
Certified SOC Analyst

CERTIFIED SOC ANALYST

Master Ultimate SOC Skills with Practical Expertise and AI Insights

CSA
Certified SOC Analyst

Certified SOC Analyst

Module	Learning Objectives
Module 01 Security Operations and Management	Learn how a SOC enhances an organization's security management to maintain a strong security posture, focusing on the critical roles of people, technology, and processes in its operations.
Module 02 Understanding Cyber Threats, IoCs, and Attack Methodology	Learn various cyberattacks, their IoCs, and the attack tactics, techniques, and procedures (TTPs) cybercriminals use.
Module 03 Log Management	Learn log management in SIEM, including how logs are generated, stored, centrally collected, normalized, and correlated across systems.
Module 04 Incident Detection and Triage	Learn SIEM fundamentals, including its capabilities, deployment strategies, use case development, and how it helps SOC analysts detect anomalies, triage alerts, and report incidents.
Module 05 Proactive Threat Detection	Learn the importance of threat intelligence and threat hunting for SOC analysts and how its integration with SIEM helps reduce false positives and enables faster, more accurate alert triage.
Module 06 Incident Response	Learn the stages of incident response and how the IRT collaborates with SOC to handle and respond to escalated incidents.
Module 07 Forensic Investigation and Malware Analysis	Learn the importance of forensic investigation and malware analysis in SOC operations to understand attack methods, identify IoCs, and enhance future defenses.
Module 08 SOC for Cloud Environments	Learn the SOC processes in cloud environments, covering monitoring, incident detection, automated response, and security in AWS, Azure, and GCP using cloud-native tools.

What You'll Learn

- 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 (IoCs) for both active and future investigations.
- Gain the ability to monitor and analyze logs and alerts from various technologies across multiple platforms, including IDS/IPS, endpoint protection, servers, and workstations.
- Understand the 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 SIEM.
- Learn how to administer SIEM solutions like 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 constantly 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 with 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.