EC-Council Certified SOC Analyst (CCSA) + Voucher d'examen

Durée: 3 Jours **Réf de cours: EC-CSA** **Version: 2.0** **Méthodes d'apprentissage: Virtual Learning**

Résumé:

The EC-Council C|SA program provides training and certification in the fundamental principles and practices of security operations, threat intelligence, and incident response. It delivers a comprehensive understanding of the processes, technologies, and techniques used to detect, investigate, and respond to cybersecurity threats.
The Certified SOC Analyst (C|SA) training program covers a broad range of topics, including common attack vectors, security tools and technologies, Security Information and Event Management (SIEM), incident response procedures, SOC coordination, and SOC development. Participants gain hands-on proficiency in centralized log management (CLM), incident triaging, and the identification and investigation of indicators of compromise (IoCs) and the cyber kill chain, enabling proactive threat detection and response.
The program also equips learners with the skills to identify emerging threat patterns, develop correlation rules, and create effective reporting mechanisms that support a strong organizational security posture. In addition, students learn how to leverage AI-enabled tools and platforms to enhance SIEM capabilities, behavior analytics, alert prioritization, and automated threat detection and threat hunting using solutions such as Splunk AI, Elastic AI, Copilot, ChatGPT, and PowerShell AI.
Upon completing the EC-Council C|SA course, participants will be equipped with the practical knowledge and technical capabilities required to operate and support a robust Security Operations Center (SOC) with enhanced incident detection and response capabilities.
Updated 19/05/2026

Public visé:

Junior SOC Security Analysts SOC Analysts (Tier I, II, and III) Security Incident Response Analysts SOC Threat Analysts Information Security Analysts Entry-level cybersecurity professionals Network and Security Administrators Cybersecurity Analysts

Objectifs pédagogiques:

- **What You'll Learn**
- Acquire comprehensive knowledge of SOC processes, procedures, technologies, and workflows.
- Develop foundational and advanced understanding of security threats, attacks, vulnerabilities, attacker behavior, and the cyber kill chain.
- Learn to identify attacker tools, tactics, and procedures (TTPs) and recognize Indicators of Compromise (IoCs) for active and future investigations.
- Gain the ability to monitor and analyze logs and alerts from multiple technologies and platforms, including IDS/IPS, endpoint protection systems, servers, and workstations.
- Understand the Centralized Log Management (CLM) process and its importance in security operations.
- Acquire skills in collecting, monitoring, and analyzing security events and logs.
- Gain extensive knowledge and hands-on experience with SIEM technologies.
- Learn how to administer SIEM solutions such as Splunk, AlienVault, OSSIM, and the ELK Stack.
- Understand the architecture, implementation, and optimization of SIEM solutions for enhanced performance.
- Gain hands-on experience in alert triaging for effective threat management.
- Learn how to escalate incidents to appropriate teams for further investigation and remediation.
- Use service desk ticketing systems for efficient incident tracking and resolution.
- Develop the ability to prepare detailed reports and briefings outlining analysis methodologies and findings.
- Learn how to integrate threat intelligence into SIEM systems to enhance incident detection and response.
- Understand how to leverage continuously evolving sources of threat intelligence.
- Gain knowledge of incident response processes and best practices for managing security incidents.
- Develop a strong understanding of SOC and Incident Response Team (IRT) collaboration for effective incident management and response.
- Assist in investigating and responding to security incidents using forensic analysis techniques.
- Gain specialized knowledge in cloud-based threat detection and adapting SOC techniques for cloud environments.
- Participate in proactive threat-hunting exercises to strengthen

- Gain practical experience in SIEM use case development.
- Develop threat detection use cases, correlation rules, and comprehensive reporting capabilities.
- Learn commonly used SIEM use cases across various deployment environments.
- Plan, organize, and execute enterprise-level threat monitoring and security analysis activities.
- Acquire skills to identify emerging threat patterns and conduct security threat analysis.
- detection capabilities.
- Develop skills in building SIEM dashboards, generating SOC reports, and creating advanced correlation rules for threat detection.
- Acquire hands-on experience in malware analysis techniques.
- Explore how AI and machine learning technologies can enhance threat detection and response within SOC operations.

Pré-requis:

- Basic knowledge or experience in network administration or security domains
- Basic understanding of IT and cybersecurity fundamentals is recommended

Test et certification

- **Exam Code:** 312-39
- **Number of Questions:** 100
- **Duration:** 3 Hours
- **Availability:** EC-Council Exam Portal
- **Test Format:** Multiple Choice

Contenu:

Module 01 – Security Operations and Management

Learn how a Security Operations Center (SOC) enhances an organization's overall security management and helps maintain a strong security posture. This module focuses on the critical roles of people, technology, and processes in effective SOC operations.

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

Explore various cyberattacks, their Indicators of Compromise (IoCs), and the tactics, techniques, and procedures (TTPs) commonly used by cybercriminals.

Module 03 – Log Management

Understand log management within SIEM environments, including how logs are generated, stored, centrally collected, normalized, and correlated across multiple systems.

Module 04 – Incident Detection and Triage

Learn SIEM fundamentals, including deployment strategies, use case development, and how SOC analysts use SIEM platforms to detect anomalies, triage alerts, and report security incidents.

Module 05 – Proactive Threat Detection

Learn the importance of threat intelligence and threat hunting for SOC analysts, and how integrating these capabilities with SIEM reduces false positives and enables faster, more accurate alert triage.

Module 06 – Incident Response

Understand the stages of incident response and how Incident Response Teams (IRT) collaborate with SOC teams to investigate, manage, and respond to escalated security incidents.

Module 07 – Forensic Investigation and Malware Analysis

Learn the role of forensic investigation and malware analysis in SOC operations to better understand attack methodologies, identify IoCs, and strengthen future security defenses.

Module 08 – SOC for Cloud Environments

Explore SOC operations in cloud environments, including monitoring, incident detection, automated response, and cloud security practices across AWS, Azure, and GCP using cloud-native security tools.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.