EC-Council

CSA
Certified SOC Analyst

CERTIFIED SOC ANALYST

Master Ultimate SOC Skills with Practical Expertise and AI Insights

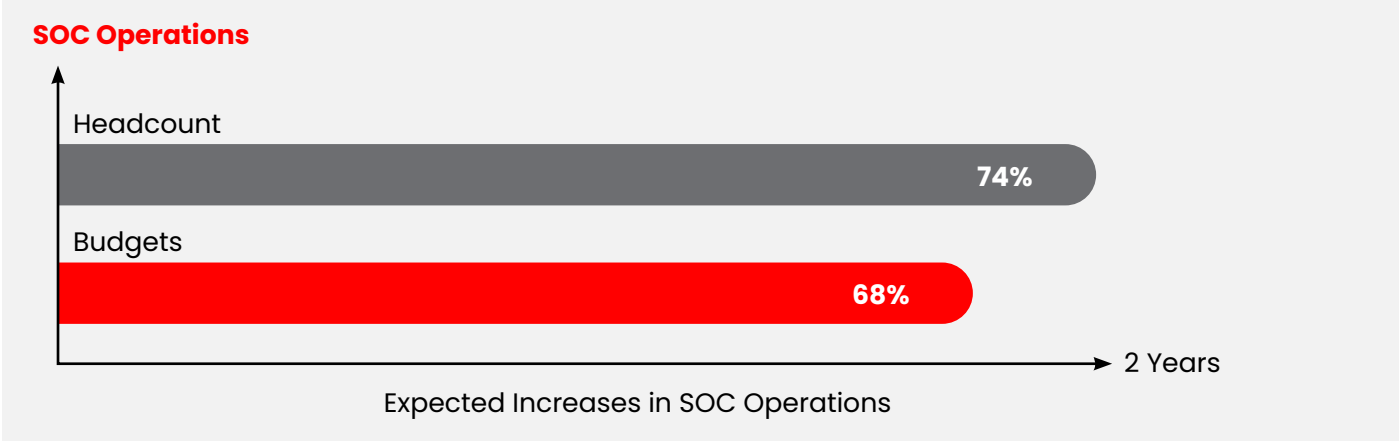
CSA
Certified SOC Analyst

Certified SOC Analyst

Why SOC Analyst Skills Are Critical in Cybersecurity

Growing Investment in SOC Operations

74% of organizations expect to increase SOC headcount over the next two years.
68% expect to increase SOC budgets over the next two years.



Expected Increases in SOC Operations

AI's Transformational Role in SOC

Areas that security leaders believe AI will revolutionize:

71%: Identity and Access Management

67%: Predictive Analytics

69%: Threat Detection and Response

68%: Perimeter Monitoring

Two-thirds of security leaders believe that AI-based automation in SOC is important now and will remain so over the next two years.

Addressing Skills and Talent Gaps

45% reported a lack of specialized skills and expertise to address rapidly evolving threats.

33% reported a shortage of talent in SOC.

23% reported a lack of internal knowledge to take advantage of AI solutions.

Source: KPMG

How C|SA Addresses These Challenges

- Equips your SOC team with cutting-edge skills to handle threats.
- Helps you develop AI-driven strategies for improved detection and response.
- Bridges the talent gap with comprehensive, hands-on SOC training.

EC-Council

Gain Mastery and Build Your Career with the Most In-Demand SOC Certification—Certified SOC Analyst

Why Join the Certified SOC Analyst Program?

The **Certified SOC Analyst** (C|SA) program is an essential stepping stone for individuals aspiring to join or advance within a Security Operations Center (SOC), focusing on its functions, development, and management.

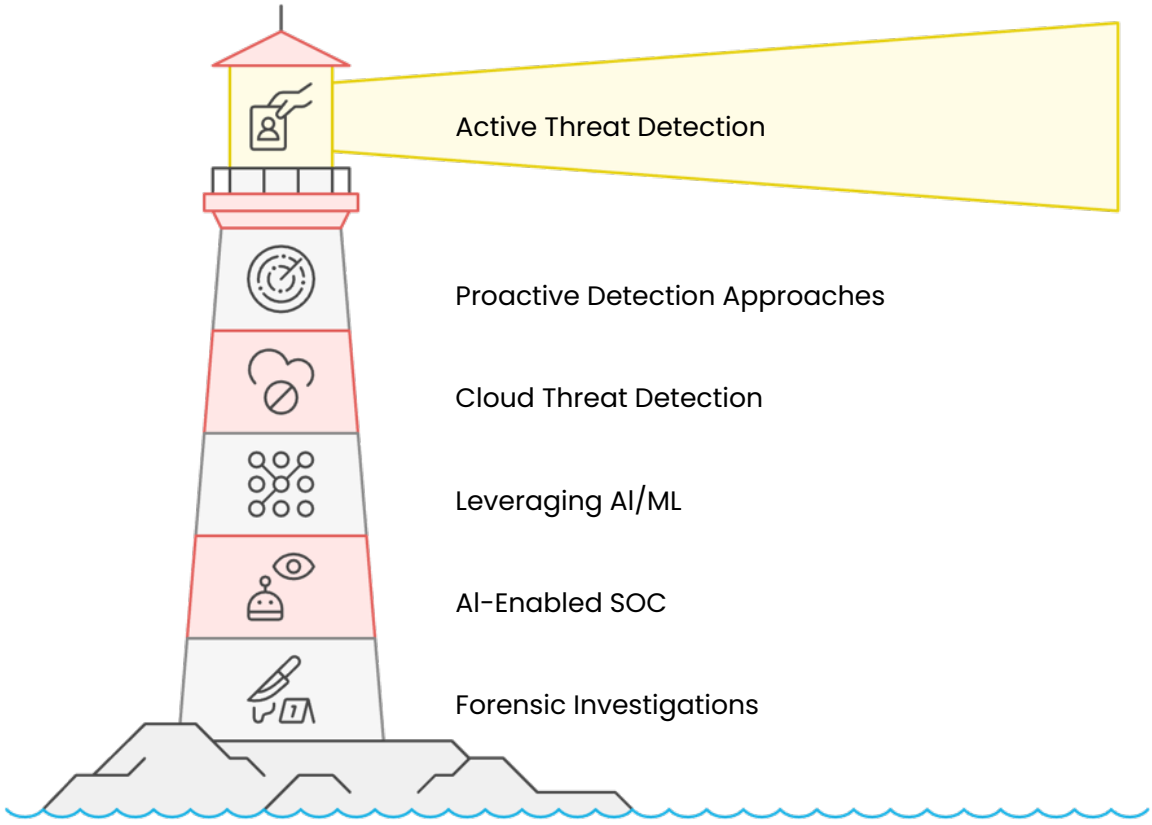
The C|SA provides training and certification in the fundamental principles and practices of security operations, threat intelligence, and incident response. It offers a deep understanding of the processes, technologies, and techniques used to detect, investigate, and respond to security threats.

The Certified SOC Analyst training program covers a range of topics, including common attack vectors, the use of security tools and technologies, security information and event management (SIEM), incident response processes, coordination, and the development of a SOC. Students gain proficiency in centralized log management (CLM), incident triaging, recognition and investigation of indicators of compromise (IoCs) and the cyber kill chain, enabling them to respond proactively to potential threats. They also gain the ability to recognize emerging threat patterns, develop correlation rules, and create effective reports that help organizations maintain a robust security posture. Students also learn to leverage AI-enabled tools and platforms to enhance SIEM capabilities, behavior analytics, and alert prioritization, and automate threat detection and threat hunting using solutions like Splunk AI, Elastic AI, Copilot, ChatGPT, and PowerShell AI.

Completing the EC-Council C|SA course will equip students with the ability to run a robust SOC with enhanced incident detection and response capabilities.

What's New in CSA Version 2

Enhancing SOC Capabilities with the Latest Complex Technologies



- Elevated topic coverage up to Level 3 (L3) SOC analysts
- Enhanced focus on active threat detection in SOC
- Inclusion of enhanced proactive detection approaches in SOC
- Inclusion of threat detection aspects in cloud environments
- Inclusion of how to leverage AI/ML capabilities for SOC
- Detailed focus on forensic investigations in SOC
  - AI-enabled SOC: Advantages of using AI in SOC
  - Leveraging AI to generate SIEM rules
  - Enhanced and automated alert triage using AI
  - Enhanced threat detection and response using AI
  - Leveraging AI for threat hunting
  - AI-enabled SIEMs such as Splunk AI, Elasticsearch AI, etc.

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.

What AI Knowledge Do You Gain with CSA?

AI-driven capabilities are seamlessly embedded within SIEM's architecture, automating processes like threat detection, correlation, and prioritization without requiring separate configurations.

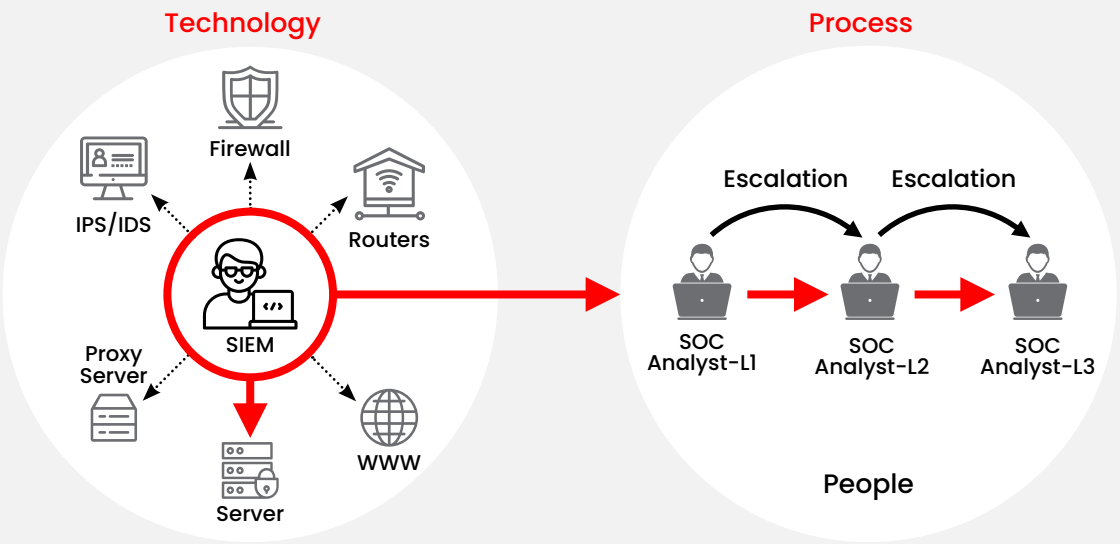
Students will learn the following knowledge related to AI:

- How AI transforms traditional SOC operations
- Leveraging AI-powered tools' natural language inputs for creating detection rules
- Leveraging AI-enabled tools for enhanced behavioral analytics
- How AI-enabled SIEM improves the capabilities of traditional SIEM systems
- How AI enhances the process of identifying, categorizing, and prioritizing security alerts
- Integrating Splunk AI and Elasticsearch AI with SIEM
- Leveraging AI-driven platforms (e.g., Copilot, ChatGPT, PowerShell AI Module) to generate PowerShell scripts for threat hunting

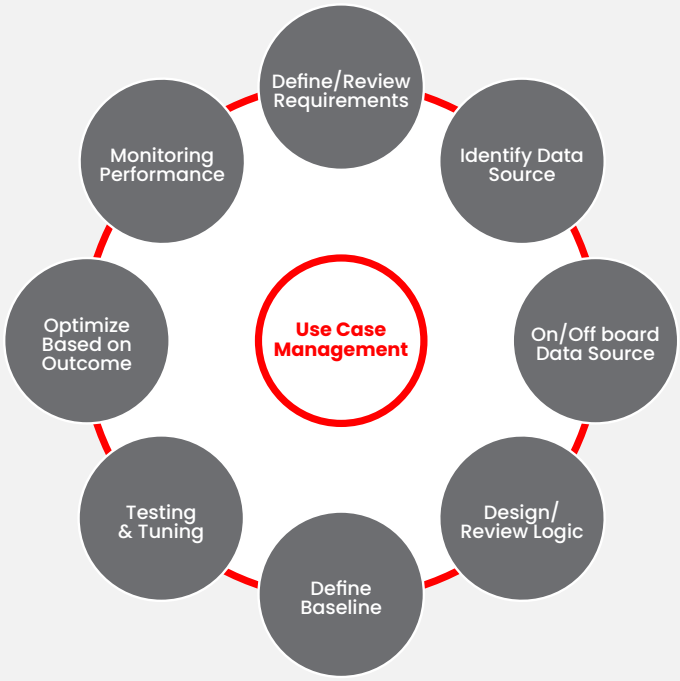
Future Proof Your SOC Analyst Career and Skills with CSA

Key Features:

1. **End-to-End Workflow, Procedures, and Technologies:**
   A strong focus on the end-to-end workflow, procedures, technologies, processes, and day-to-day operations as carried out by a SOC analyst (L1, L2, L3) in the SOC.



2. **Deep Focus on SIEM Use Case Development, Management, and Alert Triaging:**
   The course provides a comprehensive understanding of the development, fine-tuning, and management of SIEM use cases, which are at the core of SOC analyst job roles.



3. **Reactive and Proactive Threat Detection Approaches**

   Reactive Threat Detection: This refers to real-time monitoring and immediate responses to threats. It involves detecting ongoing attacks or suspicious behaviors as they happen.

   Proactive Threat Detection: This approach emphasizes the importance of anticipating potential threats before they happen. It includes using methods like threat hunting and threat intelligence to stay updated on current threat trends, as well as identifying weaknesses that attackers could exploit.

4. **Mapped with NICE 2.0 Framework**

NICE Category	NICE Specialty Area	NICE Work Role
Protect and Defend (PR)	Cybersecurity Defense Analysis (CDA)	Cyber Defense Analyst

5. **Use Cases to Optimize Threat Detection and Response:**
   350 common and specific use cases for ArcSight, QRadar, LogRhythm, and Splunk's SIEM deployments.
6. **Elaborate Understanding of SIEM Deployment:**
   65 elaborate use cases widely applied across all SIEM deployments.
7. **Hands-On Training:**
   50+ hands-on labs and 120+ tools, with more than 50% of the training dedicated to labs.
8. **Job-Ready Skills:**
   Aligned with real-world SOC analyst roles through SME input and collaboration with industry experts.
9. **AI Tools and Techniques:**
   Leverage AI/ML capabilities for SOC.

Job Roles Mapped to C|SA Certification

The C|SA certification aligns with real-world job functions to ensure learners are prepared for key roles within a modern SOC environment. These roles reflect responsibilities across multiple levels of security operations:

- **Junior SOC Security Analyst**
- **SOC Analyst**
- **Security Incident Response Analyst**
- **SOC Threat Analyst**
- **SOC Analysts (L1, L2, and L3)**
- **Info Security Analyst 3**

C|SA Exam and Training

Exam Details

Exam Code : **312-39**

Number of Questions : **100**

Duration : **3 hours**

Availability : **EC-Council Exam Portal**

Test Format : **Multiple Choice**

Training Details

Training: 3 days

Training Options:

iLearn (Self-Study)
This option is an asynchronous, self-study environment delivered in a video-streaming format.

iWeek (Live Online)
This option is an online, live training course led by an instructor.

Training Partner (In Person)
This option offers in-person training so that you can benefit from collaborating with your peers.

Why Do Top Cybersecurity Professionals Love C|SA?

JACOB SILVA

The C|SA certification helped me strengthen my background knowledge and improve my confidence. It helped me a lot within SOC proof concepts. So, I created a security operations center proof of concept using different technologies. I am now in the process of setting up my own security operations center for monitoring.

JIMMY KINYONYI BAGONZA

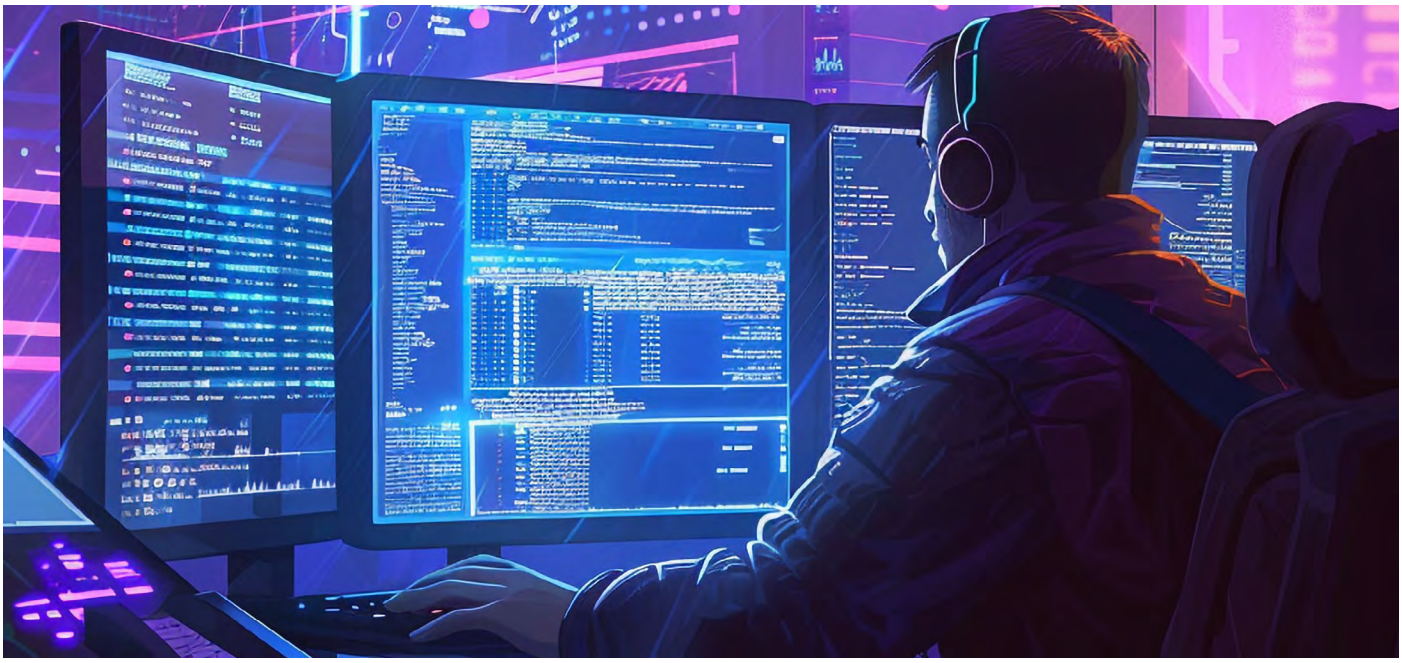
Today, organizations need to shift from prevention to rapid detection of cybersecurity threats. So, the C|SA training comes in very handy. This course has given me a solid foundation in SOC operations and a competitive advantage in the job market.

OMID NOORY

The C|SA program is much more than a training for career advancement. With the C|SA training, you become an incident responder and forensic investigator, so this course is essential for everyone in this industry.

EC-Council Recognition, Endorsement, and Mapping

About EC-Council



We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifications. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the U.S. Department of Defense, the intelligence community, NATO, and over 2,000 of the best universities, colleges, and training companies, our programs have certified people in over 150 countries, and set the bar in the field of cybersecurity education. Best known for the Certified Ethical Hacker (C|EH) program, we are dedicated to equipping over 380,000 information-age soldiers with the knowledge, skills, and abilities required to fight and win against cyber adversaries. EC-Council builds individual and organization-wide cyber capabilities through our other programs as well, including Certified Secure Computer User (C|SCU), Computer Hacking Forensic Investigator (C|HFI), Certified Network Defender (C|ND), Certified SOC Analyst (C|SA), Certified Threat Intelligence Analyst (C|TIA), Certified Incident Handler (E|CIH), and the Certified Chief Information Security Officer (C|CISO). We are an ANAB ISO/IEC 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570, in the UK by the GCHQ, CREST, and various other authoritative bodies. Founded in 2001, EC-Council employs over 400 individuals worldwide, with 10 global offices in the U.S., UK, Malaysia, Singapore, India, and Indonesia. Our U.S. offices are in Albuquerque, NM, and Tampa, FL. Learn more at **www.eccouncil.org.**

EC-Council

C|SA

Certified SOC Analyst

CERTIFIED SOC ANALYST

WE DON'T JUST TEACH

SOC ANALYST SKILLS

WE BUILD	PRACTICAL EXPERTISE WITH AI SOLUTIONS
	ENHANCED DETECTION & RESPONSE CAPABILITIES