Certified SOC Analyst (C|SA) Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Certified SOC Analyst (C|SA) Training Course is meticulously engineered to bridge the critical cybersecurity skills gap by imparting cutting-edge, hands-on expertise in the entire SOC workflow. Participants will master core competencies like Security Information and Event Management operations, log analysis, and incident triaging to effectively monitor, detect, and respond to the most sophisticated Advanced Persistent Threats and emerging cyber threats. This certification is fundamentally focused on a practical, NICE Framework-aligned curriculum that transforms theoretical knowledge into immediate, actionable defense skills, ensuring graduates can dynamically contribute to their organization's robust security posture.

The course's unique strength lies in its lab-intensive methodology, designed to simulate real-world security incidents and complex enterprise environments. Beyond foundational concepts, the C|SA curriculum delves into advanced areas like threat intelligence integration, proactive threat hunting, and basic digital forensics and malware analysis. By focusing on the attacker's perspective, including Tactics, Techniques, and Procedures and the Cyber Kill Chain, analysts gain a predictive edge. Completing this program certifies a candidate's proficiency in using leading SOC tools and prepares them not just for the exam, but to excel as Tier I and Tier II SOC Analysts, making them invaluable assets in the ongoing fight against cybercrime and protecting critical business data.

Programme Curriculum

Certified SOC Analyst (C|SA) Training Course

Introduction

Certified SOC Analyst (C|SA) Training Course is meticulously engineered to bridge the critical cybersecurity skills gap by imparting cutting-edge, hands-on expertise in the entire SOC workflow. Participants will master core competencies like Security Information and Event Management operations, log analysis, and incident triaging to effectively monitor, detect, and respond to the most sophisticated Advanced Persistent Threats and

emerging cyber threats. This certification is fundamentally focused on a practical, NICE Framework-aligned curriculum that transforms theoretical knowledge into immediate, actionable defense skills, ensuring graduates can dynamically contribute to their organization's robust security posture.

The course's unique strength lies in its lab-intensive methodology, designed to simulate real-world security incidents and complex enterprise environments. Beyond foundational concepts, the C|SA curriculum delves into advanced areas like threat intelligence integration, proactive threat hunting, and basic digital forensics and malware analysis. By focusing on the attacker's perspective, including Tactics, Techniques, and Procedures and the Cyber Kill Chain, analysts gain a predictive edge. Completing this program certifies a candidate's proficiency in using leading SOC tools and prepares them not just for the exam, but to excel as Tier I and Tier II SOC Analysts, making them invaluable assets in the ongoing fight against cybercrime and protecting critical business data.

Course Duration

5 days

Course Objectives

1. Master end-to-end SOC Workflow and operational procedures, ensuring effective team collaboration.
2. Acquire practical proficiency in Security Information and Event Management (SIEM) tool administration and deployment
3. Perform in-depth Log Analysis and Event Correlation from diverse log sources for rapid anomaly detection.
4. Utilize the MITRE ATT&CK Framework and Cyber Kill Chain to analyze and contextualize attacker TTPs.
5. Develop skills for effective Incident Triage, prioritization, and accurate escalation using ticketing systems.
6. Integrate and operationalize Cyber Threat Intelligence (CTI) platforms to enrich alerts and improve threat detection.
7. Execute Proactive Threat Hunting techniques to uncover hidden threats and reduce attack dwell time.
8. Formulate robust Incident Response (IR) plans, focusing on containment, eradication, and recovery phases.
9. Conduct foundational Digital Forensics and Malware Analysis to support incident investigation.
10. Apply security monitoring techniques across Cloud Environments and hybrid infrastructures.
11. Understand and report on Vulnerability Assessment and management processes within the SOC.
12. Leverage Security Orchestration, Automation, and Response concepts to enhance SOC efficiency.
13. Generate comprehensive and impactful Security Reports and post-incident analysis documents.

Target Audience

1. Aspiring and Current Tier I/Tier II SOC Analysts
2. Cybersecurity Specialists and Consultants
3. Network and Security Administrators/Engineers
4. Incident Response Team Members
5. IT Professionals looking to transition into security operations
6. Security Auditors and Compliance Officers
7. Federal/Government Cyber Defense Staff
8. Recent Graduates in Cybersecurity or Information Technology

Course Modules

Module 1: Security Operations Center (SOC) Fundamentals

- SOC models, capabilities, maturity models, and the roles.
- End-to-end SOC processes, including monitoring, detection, and analysis.
- Alignment with standards like the NICE Framework and industry best practices.
- Overview of core SOC tools
- Key Performance Indicators like MTTD (Mean Time to Detect) and MTTR (Mean Time to Respond).
- Case Study: Analyzing a company's transition from a basic security team to a full-fledged, multi-tier SOC model, highlighting initial setup challenges and KPI improvements.

Module 2: Understanding Cyber Threats and Attack Methodology

- Threat Landscape.
- Deep dive into the Cyber Kill Chain and MITRE ATT&CK Framework for threat categorization.
- Indicators of Compromise
- Understanding attacker techniques like network scanning and vulnerability discovery.
- Analyzing network, host, and application-level attacks
- Case Study: Mapping a recent, major supply chain attack to the phases of the Cyber Kill Chain and corresponding MITRE ATT&CK techniques.

Module 3: Centralized Log Management and Analysis

- Identifying and configuring logging from diverse sources
- Understanding protocols and the data normalization process.
- Writing correlation rules in a SIEM to link disparate events into a single incident.
- Advanced techniques for reducing noise and focusing on high-fidelity security events.
- Writing custom decoders/parsers for non-standard log formats.
- Case Study: Investigating a mass user lockout scenario by analyzing correlated Active Directory, VPN, and Firewall logs to pinpoint a Brute Force attack.

Module 4: Incident Detection with SIEM Solutions

- Components, deployment models, and scaling considerations.
- Creating and tuning SIEM detection rules for specific threats
- The process of validating, enriching, and prioritizing alerts to filter out false positives.
- Applying behavioral analytics and anomaly detection techniques within the SIEM.
- Designing operational and executive-level dashboards for real-time visibility and compliance.
- Case Study: A hands-on lab using Splunk or Elastic Stack to detect signs of lateral movement after an initial compromise alert from an EDR system.

Module 5: Enhanced Detection with Threat Intelligence (CTI)

- Understanding the process from requirements to feedback and intelligence sharing.
- Integrating CTI feeds with the SIEM.
- Utilizing threat data for proactive blocking and retrospective analysis
- Basic concepts of attributing attacks to specific threat actors or groups.
- Merging CTI with vulnerability data to focus on critical, actively exploited flaws.
- Case Study: Using a TIP to ingest a new IOC list for a zero-day exploit and immediately checking historical logs for prior network presence.

Module 6: Incident Response (IR) Fundamentals

- Detailed breakdown of the six phases.

- Developing and executing structured response procedures for common incident types
- Implementing technical controls immediate threat mitigation.
- Working effectively with cross-functional teams during a breach.
- Creating post-incident reports documenting the timeline, impact, and remediation steps.
- Case Study: Executing an IR playbook simulation for a major ransomware incident, focusing on the critical containment and eradication steps.

Module 7: Proactive Threat Hunting

- Developing and validating a threat hypothesis based on known TTPs and organizational assets.
- Utilizing tools like YARA for malware signature matching and network monitoring utilities
- Leveraging raw data beyond standard logs for deep analysis.
- Starting the hunt from external threat reports or internal environmental anomalies.
- Techniques for iteratively refining search queries and expanding the scope of an investigation.
- Case Study: A practical exercise to hunt for signs of a specific PowerShell attack technique across endpoint logs using a hypothesis driven by a recent CTI report.

Module 8: Digital Forensics and Malware Analysis

- The Chain of Custody, evidence preservation, and data acquisition from endpoints/memory.
- Differentiation between Static and Dynamic Analysis techniques.
- Using memory forensics tools and disk imaging utilities
- Analyzing Packet Capture files to extract malicious command-and-control traffic.
- Identifying common attacker techniques used to hide their tracks.
- Case Study: Analyzing a suspicious attachment from a phishing email in a sandboxed environment to determine its function and extract new IoCs.

Training Methodology

The Certified SOC Analyst training adopts a High-Impact Blended Learning approach, ensuring both deep theoretical understanding and practical skill mastery.

1. Instructor-Led Training / Live Online.
2. Hands-On Virtual Labs.
3. Scenario-Based Exercises.
4. Case Study Analysis.
5. Assessment.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com