INFOSECTRAIN
Educate. Excel. Empower.

EC-Council Accredited Training Center

Certified SOC ANALYST (CSA)

(Security Operations Center)

Certification Training

INFOSECTRAIN

Course Highlights

- 24-Hour of Instructor-led Training
- Learn from Certified SOC, DFIR & Threat Intelligence
- Real-time SIEM Labs using tools like Splunk, ELK, & QRadar
- Hands-on Log Analysis, Alert Triage & Threat Detection Exercises
- MITRE ATT&CK, Cyber Kill Chain & Use Case Mapping
- SOC Reporting, Ticketing & Investigation Documentation
- Interview Preparation for SOC Analyst Jobs (L1–L2)
- Post-training Doubt Clearing & Mentorship Support
- Access to Recorded Sessions

About Course

The Certified SOC Analyst (CSA V2) Training from InfosecTrain is structured to help newcomers and early-career security professionals build the exact skills demanded by modern SOC teams. Based on the updated EC-Council CSA V2 syllabus, the course begins with foundational concepts such as SOC architecture, roles, processes, attacker behaviors, and threat landscapes, intensifies with attacker TTP analysis using MITRE ATT&CK, IoC identification, threat-intelligence integration, and real alert triage simulations. It concludes with full-scale incident response workflows, documentation requirements, escalation procedures, and AI-assisted detection models used in 2026 SOC environments.

A strategic blend of theory, guided labs, real-world datasets, and case-based scenarios ensures students gain practical SOC readiness and confidently support incident detection and response functions in a live SOC.

Course Objectives

- Build a strong foundation in SOC operations, security monitoring, log management, SIEM workflows, and threat detection concepts.
- Develop hands-on SOC skills including log correlation, alert triage, IoC analysis, threat intelligence integration, and MITRE ATT&CK mapping.
- Train participants to detect, investigate, escalate, and document security incidents in alignment with modern SOC L1-L2 practices.
- Prepare learners to confidently clear the EC-Council Certified SOC Analyst (CSA V2) certification exam and step into SOC Analyst roles.

INFOSECTRAIN

Target Audience

This course is ideal for:

- Tier I and Tier II SOC Analysts (entry- to intermediate-level)
- Cybersecurity Analysts, Network Security Engineers/Administrators,
- Network Defense Analysts, Network & Security
- Technicians/Operators/Specialists
- Entry-level cybersecurity professionals seeking to build core SOC skills
- IT/Network/System Administrators or Engineers wanting to transition into SOC/security monitoring roles
- Anyone aiming to become a SOC Analyst, aspiring professionals, career switchers, or freshers with interest in SOC operations

Pre-requisites

There are no formal prerequisites mandated by EC-Council to take CSA V2 ; it is open to beginners/entry-level candidates.

INFOSECTRAIN

Exam Information

Exam Code	312-39
Exam Duration	180 Minutes
Number of Questions	100
Exam Format	Multiple-choice Questions
Passing Score	70%
Exam Language	English

INFOSECTRAIN

Course Content

Module 1 Security Operations and Management

Key topics covered:

SOC, SOC Capabilities, SOC Operations, SOC Workflow, Components of SOC, SOC Models, SOC Maturity Models, SOC Generations, SOC KPIs and Metrics, SOC Challenges

Module 2 Understanding Cyber Threats, IoCs, and Attack Methodology

Key topics covered:

Cyber Threats, TTPs, Reconnaissance Attacks, Man-in-the-Middle Attacks, Password Attack Techniques, Malware Attacks, Advanced Persistent Threat Lifecycle, Host-Based DoS Attacks, Ransomware Attacks, SQL Injection Attacks, XSS Attacks, Cross-Site Request Forgery (CSRF) Attack, Session Attacks, Social Engineering Attacks, Email Attacks, Insider Attacks, IoCs, Attacker's Hacking Methodology, MITRE D3FEND Framework, Diamond Model of Intrusion Analysis

HANDS-ON LABS:

- ✔ Perform SQL Injection Attack, Cross-Site Scripting (XSS)
- ✔ Attack, Network Scanning Attack, DoS Attack, and Brute Force Attack to understand their TTPs and IoCs.
- ✔ Detect and analyze IoCs using Wireshark.

Module 3 Log Management

Key topics covered:

Incident, Event, Log, Log Sources, Log Format, Local Logging, Windows Event Log, Linux Logs, Mac Logs, Firewall Logs, IP tables, Router Logs, IIS Logs, Apache Logs, Database Logs, Centralized Logging, Log Collection, Log Transmission, Log Storage, AI-Powered Script for Log Storage, Log Normalization, Log Parsing, Log Correlation, Log Analysis, Alerting and Reporting

HANDS-ON LABS:

- ✔ Configure, monitor, and analyze various logs.
- ✔ Collect logs from different devices into a centralized location using Splunk.

Module 4 Incident Detection and Triage

Key topics covered:

SIEM, SIEM Architecture and its Components, AI-Enabled SIEM, Types of SIEM Solutions, SIEM Deployment, SIEM Use Cases, SIEM Deployment Architecture, SIEM Use Case Lifecycle, Application-Level Incident Detection SIEM Use Cases, Insider Incident Detection SIEM Use Cases, Examples of Network Level Incident Detection SIEM Use Cases, Examples of Compliance Use Cases, SIEM Rules Generation with AI, Alert Triage, Splunk AI, Elasticsearch AI, Alert Triage with AI, Dashboards in SOC, SOC Reports

HANDS-ON LABS:

- ✔ Develop Splunk use cases to detect and generate alerts for brute-force attempts, ransomware attacks, SQL injection attempts, XSS attempts, Broken Access Control attempts, application crashes using Remote Code Execution, scanning attempts, monitoring insecure ports and services, HTTP flood/denial of service (DoS) attacks, monitoring Windows audit log tampering, and malicious PowerShell script execution.
- ✔ Enhance alert triage using the SIGMA rules for Splunk queries.
- ✔ Create dashboards in Splunk.
- ✔ Create ELK use cases for monitoring trusted binaries connecting to the internet, credential dumping using Mimikatz, and monitoring malware activity in the system.
- ✔ Create dashboards in ELK.
- ✔ Detect brute-force attack patterns using correlation rules in ManageEngine Log 360.

Module 5 Proactive Threat Detection

Key topics covered:

Cyber Threat Intelligence (CTI), Threat Intelligence Lifecycle, Types of Threat Intelligence, Threat Intelligence Strategy, Threat Intelligence Sources, Threat Intelligence Platform (TIP), Threat Intelligence-Driven SOC, Threat Intelligence Use Cases for Enhanced Incident Response, Enhanced Threat Detection with AI, Threat Hunting, Threat Hunting Process, Threat Hunting Frameworks, Threat Hunting with PowerShell Script, PowerShell AI Module, Threat Hunting with AI, Threat Hunting with YARA, Threat Hunting Tools

HANDS-ON LABS:

- Integrate IoCs into the ELK Stack.
- Integrate OTX threat data into OSSIM.
- Detects incidents in Windows Server using YARA.
- Conduct threat hunting using Windows PowerShell scripts, Hunt Manager in Velociraptor, Log360 UEBA, and Sophos Central.

INFOSECTRAIN

Module 6 Incident Response

Key topics covered:

Incident Response (IR), IRT, SOC and IRT Collaboration, IR Process, Ticketing System, Incident Triage, Notification, Containment, Eradication, Recovery, Network Security Incident Response, Application Security Incident Response, Email Security Incident Response, Insider Threats and Incident Response, Malware Threats and Incident Response, SOC Playbook, Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), SOAR, SOAR Playbook

HANDS-ON LABS:

- Generate tickets for incidents.
- Contain data loss incidents.
- Eradicate SQL injection and XSS incidents.
- Perform recovery from data loss incidents.
- Create incident reports using OSSIM.
- Perform automated threat detection and response using Wazuh.
- Detects threats using Sophos Central XDR.
- Integrate Sophos Central XDR with Splunk.

Module 7 Forensic Investigation and Malware Analysis

Key topics covered:

Forensics Investigation, Forensics Investigation Methodology, Forensics Investigation Process, Forensics Investigation of Network Security Incidents, Forensics Investigation of Application Security Incidents, Forensics Investigation of Email Security Incidents, Forensics Investigation of Insider Incidents, Malware Analysis, Types of Malware Analysis, Malware Analysis Tools, Static Malware Analysis, Dynamic Malware Analysis

HANDS-ON LABS:

- ✔ Perform forensic investigation of application security incidents: SQL Injection Attacks.
- ✔ Perform forensic investigation of a compromised system incident using Velociraptor.
- ✔ Analyze RAM for suspicious activities using Redline.
- ✔ Perform static analysis on a suspicious file using PeStudio.
- ✔ Examine a suspicious file using VirusTotal.
- ✔ Perform dynamic malware analysis in Windows using Process Hacker.

Module 8 SOC for Cloud Environments

Key topics covered:

Cloud SOC, Azure SOC Architecture, Microsoft Sentinel, AWS SOC Architecture, AWS Security Hub, Centralized Logging with OpenSearch, Google Cloud Platform (GCP) Security Operation Center, Security Command Center, Chronicle

HANDS-ON LABS:

- ✓ Implement Microsoft Sentinel in Azure

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on