# SOC Analyst (CSA Exam Prep)

Detect, triage and respond to security incidents in a SOC using SIEM and threat intelligence.

| DURATION | FORMAT | LEVEL | LABS |
| --- | --- | --- | --- |
| 45 hours | Onsite, online or hybrid | Intermediate | Cloud sandbox included |

## About this programme

Prepares analysts for day-to-day work in a security operations centre: SOC processes, attacker TTPs and IoCs, centralised logging, SIEM detection with Splunk, ELK and Microsoft Sentinel, threat intelligence and incident response, aligned to the EC-Council Certified SOC Analyst (CSA) programme.

Who it is for: Tier 1 and Tier 2 SOC analysts, and network and security administrators

## What your team will be able to do

- Explain SOC roles, processes and technology
- Recognise attacker TTPs and indicators of compromise
- Build centralised logging and SIEM detection use cases
- Enrich detections with threat intelligence
- Triage, contain, eradicate and report on incidents

## Before you start

- Networking fundamentals
- Basic security concepts (Security+ level)

## Course outline

### 1. SOC operations and current threats

- People, processes and technology in a SOC
- Implementing a SOC
- Cyber threats, IoCs and attacker TTPs

### 2. Logging and SIEM

- Incidents, events and logging
- Local and centralised logging best practice
- SIEM fundamentals and deployment
- Detection use cases: application, insider, network, host and compliance
- Labs: detection use cases in Splunk and ELK

### 3. Threat intelligence

- Threat intelligence types, sources and platforms
- Integrating threat intelligence and IoCs into the SIEM

### 4. Incident response

- The incident response process
- Responding to network, application, email, insider and malware incidents
- Triage, prioritisation and ticketing
- Containment, eradication, recovery and incident reporting

### 5. Forensics and cloud SOC

- Forensic investigation and malware analysis
- SOC processes for AWS, Azure and GCP
- Cloud monitoring and automated response with Microsoft Sentinel

## Sample schedule

6 days onsite, or 12 half-day sessions online. We fit days and session lengths to your team's calendar.

| | | |
|---|---|---|
| Day 1 | 8 h | SOC operations and current threats |
| Day 2 | 8 h | Logging and SIEM |
| Day 3 | 8 h | Logging and SIEM (continued); Threat intelligence |
| Day 4 | 8 h | Threat intelligence (continued); Incident response |
| Day 5 | 8 h | Incident response (continued); Forensics and cloud SOC |
| Day 6 | 5 h | Forensics and cloud SOC (continued) |

## Assessment and certification

### How learning is checked

- A short knowledge check on day one and again at the end, so you can see each person's progress
- Graded hands-on labs in every module, reviewed by the trainer
- A final exercise that applies the programme to a problem like your team's own
- A timed practice exam in the format of the real one, with a review of every answer

### Certificate and exams

- Participants who complete the programme receive a Cognitive Networks AI certificate of completion.
- Prepares your team for the Certified SOC Analyst exam. Exam vouchers are not included: each participant books the exam with EC-Council.

## Formats and cohort size

- Onsite: At your office or a venue you choose, in full days.
- Online, live: Instructor-led over video, usually in half-day sessions so people can keep up with work.
- Hybrid: Some days in a room together, the rest online. Useful when a team works across cities.

Cohort size: 15 to 25 people per trainer. Larger teams run as parallel cohorts on the same outline, so everyone learns the same thing.

Pricing: We quote per cohort, based on duration, format and number of cohorts. There is no per-seat price list: tell us your team and we send a proposal within one business day.

### Bring this programme to your team

Request a proposal at cognitivenetworks.ai/contact?programme=soc-analyst

reachus@cognitivenetworks.ai · Bangalore +91 72043 05303 · Dallas +1 (303) 827-7415

> CSA and Certified SOC Analyst are trademarks of EC-Council. Cognitive Networks AI is not affiliated with EC-Council. This programme prepares your team for the exam. It is not an official course of EC-Council, and the exam is booked separately.