

EC-COUNCIL

CSA — Certified SOC Analyst Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

BEGINNER

32 HOURS

4 DAYS

At a glance

COURSE	CSA — Certified SOC Analyst
TRACK	EC-Council
DOMAIN	Cyber Security
LEVEL	Beginner
DURATION	32 hours (about 4 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is a beginner course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Eight modules, mapped one-for-one to EC-Council's Certified SOC Analyst outline and taught in the same order, so nothing on the 312-39 exam is left uncovered.

Each module below carries the weighting published in EC-Council's CSA exam blueprint, and we give it classroom time in proportion. Two modules — incident detection and triage, and incident response — carry a quarter of the exam each. That is half the paper between them, and it is where most of our classroom time goes.

This is a console course. A SOC analyst is judged on what they do with an alert in the first ten minutes, so the teaching is built around queue work: ingest real log sources, write the rule, watch it fire, triage what comes back, and decide whether to escalate.

Module 01 — Security Operations and Management

What a security operations centre is for, how one is structured, and what makes it work or fail as an organisation rather than a tool. 5% of the exam.

- SOC purpose, capabilities and the operations it is accountable for
- SOC workflow from alert ingestion to closure, and the tier model behind it
- Components of a SOC: people, process, technology and the facility itself
- SOC operating models, including in-house, managed, hybrid and virtual
- SOC maturity models and assessing where a given SOC actually sits
- The generations of SOC design and what each one was built to solve
- Key performance indicators and metrics, and the ones that distort behaviour
- Common SOC challenges: alert volume, analyst burnout, tuning debt and staff turnover

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

The attacker's side of the console, described precisely enough that you recognise it in a log line. 8% of the exam.

- Cyber threats, threat actor categories, and tactics, techniques and procedures
- Reconnaissance attacks and man-in-the-middle techniques
- Password attack techniques and credential abuse
- Malware attacks and the ransomware lifecycle
- The advanced persistent threat lifecycle and what long-dwell intrusion looks like in logs
- Application-layer attacks: SQL injection, cross-site scripting, cross-site request forgery and session attacks
- Host-based denial-of-service attacks
- Social engineering, email-borne attacks and insider activity
- Indicators of compromise, and the difference between an indicator and an alert
- Attack methodology as a model, using the MITRE D3FEND framework and the Diamond Model of Intrusion Analysis

Module 03 — Log Management

Everything downstream depends on whether the right logs arrived, parsed, in time. 15% of the exam.

- Events, incidents and logs, and keeping the three distinct
- Log sources and formats across the estate, and what each one can and cannot tell you
- Local logging: Windows Event Log, Linux logs and macOS logs
- Network and infrastructure logs: firewall, iptables and router logging
- Application and service logs, including IIS, Apache and database logs
- Centralised logging: collection, transmission and storage, and the integrity of each step
- Log normalisation and parsing, and what is lost when a parser is wrong

- Log correlation and analysis across sources to reconstruct a sequence
- Alerting and reporting built on log data rather than assumption

Module 04 – Incident Detection and Triage

A quarter of the exam, and the core of the Tier 1 job: making a SIEM produce alerts worth acting on. 25% of the exam.

- SIEM concepts, architecture and components, the types of SIEM solution, and the deployment architectures they support
- SIEM deployment, data onboarding and the tuning that follows
- AI-assisted SIEM capabilities, including rule generation, and checking what they produce
- Use case development and the use case lifecycle, from requirement to retirement
- Application-level incident detection and the signals that surface it
- Network-level incident detection across perimeter, internal and egress traffic
- Insider incident detection, and the behavioural signals that distinguish it
- Compliance-driven use cases and the reporting they require
- Alert triage: validating, prioritising, correlating and deciding what escalates
- SOC dashboards and reports that tell a reader something they can act on

Module 05 – Proactive Threat Detection

Looking for what the alerts did not catch. 12% of the exam.

- Cyber threat intelligence concepts and the intelligence lifecycle
- Strategic, tactical, operational and technical intelligence, and who each one serves
- Threat intelligence strategy, sources and source reliability
- Threat intelligence platforms and feeding intelligence into detection content
- Intelligence-driven SOC operation and practical intelligence use cases
- AI-supported threat detection, and validating machine-suggested leads
- Threat hunting concepts, the hunting process and hunting frameworks
- Hypothesis-driven hunting with PowerShell and with YARA rules
- Threat hunting tooling, and turning a successful hunt into a permanent detection

Module 06 – Incident Response

The other quarter of the exam: what happens after triage decides this one is real. 25% of the exam.

- Incident response concepts, the incident response team and its collaboration with the SOC
- The incident response process end to end
- Ticketing systems, incident triage and notification, and the handover records that hold up later
- Containment, eradication and recovery, and the trade-offs between speed and evidence
- Responding to network security incidents and to application security incidents
- Responding to email security incidents
- Responding to insider threats and to malware incidents
- SOC playbooks: writing one that a tired analyst can follow at three in the morning
- Endpoint detection and response, extended detection and response, and where each fits
- Security orchestration, automation and response, and building a SOAR playbook

Module 07 — Forensic Investigation and Malware Analysis

Enough forensic and analytical discipline to hand over findings that survive scrutiny. 5% of the exam.

- Forensic investigation concepts, methodology and process
- Evidence handling, chain of custody and order of volatility
- Forensic investigation of network security incidents
- Forensic investigation of application security incidents
- Forensic investigation of email security incidents and insider incidents
- Malware analysis concepts and the types of analysis available
- Static malware analysis in a contained environment
- Dynamic malware analysis and behavioural observation
- Malware analysis tooling, and converting findings into detection content

Module 08 — SOC for Cloud Environments

The same job, in estates where you do not own the infrastructure and the telemetry arrives differently. 5% of the exam.

- Cloud SOC concepts, and what changes when logs come from a provider's control plane
- Azure SOC architecture and Microsoft Sentinel
- AWS SOC architecture and AWS Security Hub
- Centralised cloud logging, including OpenSearch-based collection
- Google Cloud Platform security operations, Security Command Center and Chronicle
- Cloud-specific detection use cases: identity abuse, misconfiguration and data exposure
- Responding to an incident across cloud and on-premises boundaries at once

Who should take this

Tier 1 and Tier 2 SOC analysts, and people moving into a SOC from network or system administration, service desk or IT support. It also suits security engineers who build detection content and want to understand how it is consumed, and incident responders who inherited the queue without formal grounding in it.

You will need working knowledge of networking, and enough Windows and Linux to read a log and know what generated it. Familiarity with a command line helps. You do not need prior SOC experience.

The exam

The Certified SOC Analyst exam is set and awarded by EC-Council and delivered through the EC-Council exam portal.

- Exam code 312-39
- 100 multiple-choice questions
- Three hours
- A passing score of 70% is published by EC-Council

The exam voucher is purchased separately from the certification body; we arrange it on your behalf and send you the code, and you book your own exam date. EC-Council sets its own exam eligibility policy, so confirm your route before you book.

How we deliver it

Four days, classroom or online live, or at your office for a private group. Most of the time is spent on a console rather than on slides: you onboard log sources, write and tune detection rules, work a live alert queue, and run an incident end to end against a scripted intrusion. Small cohorts, so everyone works the queue rather than watching someone else work it.

Mapped to EC-Council's Certified SOC Analyst outline and the published 312-39 exam blueprint. Taught from Hacky Security's own curriculum and lab estate by instructors who also work our security operations centre.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 · info@hackysecurity.com

<https://hackysecurity.com/courses/csa/>

CHANDIGARH · SHIMLA · DELHI · DUBAI · LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 12 September 2026.