

CS0-003: CompTIA CySA+

Detect, analyse and respond to threats like a SOC analyst — and prepare for the CompTIA CySA+ CS0-003 exam.

DURATION

5 days · 40 hours

LEVEL

Intermediate

CURRICULUM

15 modules · 8 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

Security analysts spend their days making sense of signals: alerts from a SIEM, results from a vulnerability scan, an odd process on a server or a suspicious login. The skill is in deciding quickly what matters and what to do next. This five-day course builds that analytical skill through hands-on investigation work and prepares you for the CySA+ CS0-003 exam.

Days one and two cover security operations. You will study system and network architecture from a defender's viewpoint, analyse indicators of compromise in logs, endpoint data, network traffic and email, and use threat intelligence and threat hunting techniques. You will also look at how automation and orchestration support a modern security operations centre.

Day three focuses on vulnerability management: running and tuning scans, interpreting results, prioritising with risk context and recommending controls, including for cloud and application vulnerabilities. Day four covers incident response and management, using established frameworks for detection, containment, eradication and recovery, with attack frameworks such as MITRE ATT&CK to structure analysis. Day five covers reporting and communication — metrics, stakeholder reporting and lessons learned — and an exam-readiness session.

Labs use realistic datasets so that you practise the investigation process, not just the theory. This course is aligned to the CS0-003 exam and prepares you for it; CompTIA updates its exams periodically, so confirm the current version on the CompTIA website before booking.

Highlights

- 40 hours of live, analyst-focused training
- SIEM, log and packet analysis labs
- Vulnerability scanning and prioritisation exercises
- Incident response simulations
- Mapped to the four CS0-003 domains

What's included

- Investigation labs with realistic log and packet data
- SIEM queries and alert triage
- Vulnerability scan tuning and prioritisation
- MITRE ATT&CK-based incident analysis
- Report writing exercises for stakeholders
- Performance-based question practice
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- Security and SOC analysts
- Security+ holders moving into analyst roles
- Threat intelligence and vulnerability management staff
- Incident responders
- System administrators with security responsibilities

Prerequisites

- Security+ or equivalent knowledge
- Hands-on IT or security experience (around three to four years is commonly recommended)
- Comfort with Windows and Linux command lines

Detailed curriculum — 5 days, 40 hours, 15 modules, 8 hands-on labs

Day 1 Security Operations: Architecture & Indicators

8 hours

1.1 Architecture for defenders

- Logging and log ingestion
- Identity and access in investigations
- Operating system and network concepts for analysts
- Cloud and hybrid visibility

1.2 Indicators of malicious activity

- Network indicators
- Application indicators
- Host and endpoint indicators
- Email and social engineering indicators

LAB Hunt for indicators in Windows event logs · 50 min

1.3 Packet analysis

- Reading packet captures
- Protocol anomalies
- Identifying beaconing and exfiltration

LAB Analyse a packet capture of a suspected compromise · 45 min

Day 2 Security Operations: Tools, Intelligence & Automation

8 hours

2.1 Analysis tools

- SIEM and SOAR
- Sandboxing and file analysis
- EDR and XDR
- Scripting for analysts

LAB Write SIEM queries to triage a set of alerts · 50 min

2.2 Threat intelligence and hunting

- Intelligence sources and confidence
- Hypothesis-driven threat hunting
- Threat actor profiling
- Sharing intelligence

LAB Run a threat hunt using an intelligence report · 40 min

2.3 Process improvement

- Standardising processes
- Single pane of glass
- Automation opportunities

Day 3 Vulnerability Management

8 hours

3.1 Scanning

- Asset discovery
- Agent-based and agentless scanning
- Credentialed and non-credentialed scans
- Special considerations for OT and cloud

LAB Configure and run authenticated vulnerability scans · 50 min

3.2 Analysis and prioritisation

- CVSS and context
- Common web and application vulnerabilities
- Validating findings and false positives
- Attack surface management

LAB Prioritise scan results for a remediation plan · 40 min

3.3 Controls and remediation

- Compensating controls
- Exceptions and risk acceptance
- Patching and configuration management

Day 4 Incident Response & Management

8 hours

4.1 Frameworks

- Incident response life cycle
- Cyber kill chain
- MITRE ATT&CK and the Diamond Model

4.2 Detection and analysis

- Scoping an incident
- Root cause analysis
- Evidence acquisition and chain of custody

LAB Respond to a simulated intrusion end to end · 75 min

4.3 Containment and recovery

- Containment strategies
- Post-incident activities
- Eradication and recovery

Day 5 Reporting, Communication & Exam Readiness

8 hours

5.1 Vulnerability reporting

- Reporting to technical and business audiences
- Stakeholder communication
- Metrics and key performance indicators

LAB Write an executive summary for a vulnerability assessment · 35 min

5.2 Incident reporting

- Incident declaration and escalation
- Lessons learned
- Regulatory and legal communication

5.3 Exam readiness

- Performance-based question strategy
- Domain review
- Full-length practice test

Skills and tools

Skills you will build

Security operations

Log analysis

Packet analysis

SIEM

EDR

Threat intelligence

Threat hunting

Vulnerability management

Incident response

MITRE ATT&CK

Security reporting

Tools used in class

Wireshark

Splunk

Wazuh

Nmap

OpenVAS

Sysinternals

Kali Linux

CyberChef

Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	CompTIA CySA+
Exam code	CS0-003
Questions	Maximum 85
Duration	165 minutes
Passing score	750 (on a scale of 100–900)
Format	Multiple choice, Multiple response, Performance-based / lab
Delivery	Online proctored, Test centre
Validity	3 years (renewable through CompTIA continuing education)
Official page	https://www.comptia.org/certifications/cybersecurity-analyst

Exam skill areas covered

Identify, protect, detect, respond, and recover

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

Is CS0-003 the current CySA+ exam?

The course is mapped to CS0-003. CompTIA refreshes exams periodically, so confirm the current version on the CompTIA website before booking.

Do I need Security+ first?

It is not mandatory, but Security+ level knowledge is assumed throughout the course.

Will I use a real SIEM?

Yes. Labs use open-source and trial tools with prepared datasets so that you can practise real investigations.

Is this course useful for SOC teams?

Yes. It mirrors day-to-day analyst work and can be tailored to your SOC's tooling in a private batch.

How long is CySA+ valid?

Three years, renewable through CompTIA's continuing education programme.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/cs0-003-comptia-cysa-plus · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur

New Delhi 110092

Office: 98180 12523

CompTIA, A+, Network+, Security+, CySA+, PenTest+, SecurityX, Cloud+ and Linux+ are trademarks of CompTIA, Inc. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.