



COMPTIA

# CySA+ CS0-003 — Cybersecurity 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.

INTERMEDIATE

40 HOURS

5 DAYS

## At a glance

|            |                                                  |
|------------|--------------------------------------------------|
| COURSE     | CySA+ CS0-003 — Cybersecurity Analyst            |
| TRACK      | CompTIA                                          |
| DOMAIN     | Cyber Security                                   |
| LEVEL      | Intermediate                                     |
| DURATION   | 40 hours (about 5 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 an intermediate 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

---

Four domains, mapped one-for-one to the CompTIA CySA+ CS0-003 exam objectives and taught in the same order, so nothing on the exam is left uncovered.

This course targets CS0-003, which remains a live exam. CompTIA has since published CySA+ V4 under exam code CS0-004, and lists CS0-003 as retiring on 22 December 2026 in English, later in Japanese, Portuguese and Spanish. If you intend to sit CS0-003, book it against that date. If you would rather sit V4, ask us and we will run the V4 map instead.

What defines CS0-003 is the decision to describe the analyst job as a workflow rather than a toolset. Two thirds of the exam sits in security operations and vulnerability management, and a full sixth of it is about writing and saying things clearly — the reporting domain is not a footnote here. Each domain below carries its published weighting, and we give it classroom time in proportion.

### Domain 01 — Security Operations

---

The daily work of a monitoring analyst: knowing what normal looks like well enough to spot what is not. 33% of the exam.

- System and network architecture as an analyst sees it — logging sources, operating system internals, network design, identity and access, encryption, and where the sensitive data actually sits
- Log ingestion, time synchronisation and the gaps that quietly make a timeline unreliable
- Network indicators of malicious activity: unexpected bandwidth, unknown devices, beaconing, irregular peer-to-peer traffic and scanning against your own estate
- Host indicators: processes that should not exist, unauthorised software, changed privileges, registry and filesystem anomalies, and evidence of data leaving
- Application indicators: anomalous service behaviour, unexpected outbound connections, authentication failure patterns and introduced malicious code
- Social engineering indicators, and correlating a human report against technical evidence
- Analyst tooling in practice — packet capture and protocol analysis, SIEM query and correlation, endpoint telemetry, file reputation services and sandbox output
- Email analysis: headers, sender authentication records, embedded links and attachments
- Scripting and automation with Python, PowerShell, shell and regular expressions, used to make repetitive analysis reliable rather than merely faster
- Threat intelligence and threat hunting: actor types, tactics and techniques, confidence and source reliability, intelligence sharing, and turning a hypothesis into a query
- Process improvement: standardising, streamlining and integrating tooling so the team works from one picture

### Domain 02 — Vulnerability Management

---

Finding weaknesses is straightforward. Deciding which ones matter, and getting them fixed, is the job. 30% of the exam.

- Asset discovery and scanning strategy: internal and external, credentialed and uncredentialed, agent-based and agentless, active and passive
- Static and dynamic analysis, and scanning environments where disruption is unacceptable
- Special handling for operational technology, industrial control and other fragile estates

- Reading output from network scanners, web application scanners, vulnerability scanners, debuggers, cloud posture tools and multipurpose utilities
- Prioritisation using CVSS, and why a CVSS score on its own is not a prioritisation
- Validation: confirming a finding, discarding false positives, and testing exploitability in context
- The context that changes the answer — asset value, exposure, compensating controls, zero-day risk and current threat activity in your sector
- Recommending controls for common weakness classes, including cross-site scripting, overflow conditions, broken access control and data poisoning
- The response and remediation cycle: patching, configuration management, compensating controls, maintenance windows, exceptions and risk acceptance
- Governance, service level objectives, secure development practice and threat modelling as inputs to the programme

### Domain 03 — Incident Response Management

---

What you do between the alert and the all-clear, and how you make the next one cheaper. 20% of the exam.

- Attack methodology frameworks and what each is good for: the cyber kill chain, the diamond model of intrusion analysis, MITRE ATT&CK, OSSTMM and the OWASP testing guide
- Detection and analysis: triage, validating severity, scoping the affected estate and building an evidence-backed timeline
- Containment decisions, including the trade-off between isolating quickly and preserving evidence
- Eradication and recovery, and verifying the environment is clean before restoring service
- Preparation: response plans, runbooks and playbooks, tooling, and analyst training
- Tabletop exercises and simulation, and what to change when one goes badly
- The relationship between incident response, business continuity and disaster recovery
- Forensic handling, chain of custody, and working alongside legal and regulatory obligations
- Root cause analysis, and post-incident review that produces changes rather than minutes

### Domain 04 — Reporting and Communication

---

The domain that decides whether any of the previous three produce a result. 17% of the exam.

- Vulnerability management reporting: compliance reports, action plans, prioritised remediation and risk statements a system owner will accept
- Naming the things that stop remediation — change windows, legacy dependencies, degraded function, business process interruption, and the terms of service agreements
- Metrics and key performance indicators worth reporting: time to detect, respond and remediate, recurrence rate and scan coverage
- Writing for the audience: an executive summary, a technical appendix, and the discipline to keep them separate
- Incident declaration and escalation, and knowing whose decision each step actually is
- Communication during a live incident — stakeholder updates, legal, regulators, customers, media and law enforcement
- Reporting obligations driven by regulation and contract, and the clocks attached to them
- Lessons learned and after-action reporting that changes a control, not just a document
- Handling the reports themselves, which are sensitive documents in their own right

## Who should take this

---

Security operations centre analysts, incident responders, threat hunters, vulnerability analysts, and network or system administrators moving into a defensive security role. It also suits developers and cloud engineers who are being asked to own detection and remediation for their own services.

CompTIA recommends Network+ and Security+ or equivalent knowledge, and around four years of hands-on experience as an incident response or security operations analyst. These are recommendations, not requirements — nothing gates you from sitting the exam, and we regularly teach candidates with less time served but a strong operational background.

You will need solid networking and operating system knowledge and comfort at a command line. Prior scripting experience helps but is not assumed.

## The exam

---

CySA+ is set and awarded by CompTIA.

- A maximum of 85 questions, 165 minutes
- A mix of multiple-choice and performance-based questions
- A scaled score of 750 on a scale of 100 to 900 is required to pass
- Available in English, Japanese, Portuguese and Spanish

CompTIA does not publish how much of the paper is performance-based, so plan to meet those questions anywhere in it. The exam voucher is purchased separately from CompTIA; we arrange it on your behalf and send you the code, and you book your own exam date.

## How we deliver it

---

Five days, classroom or online live, or at your office for a private group. Roughly half the time is spent in front of real telemetry — logs, captures and scan output from an estate we have compromised on purpose — rather than in slides. Domain checkpoints each day, and a full-length mock under exam conditions on the final afternoon.

Mapped to the CompTIA CySA+ CS0-003 exam objectives. Taught from Hacky Security's own curriculum and lab estate by instructors who 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](mailto:info@hackysecurity.com)

<https://hackysecurity.com/courses/cysa-plus/>

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 11 September 2026.