

COMPTIA

CASP+ CAS-004 — Advanced Security Practitioner 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.

EXPERT

40 HOURS

5 DAYS

At a glance

COURSE	CASP+ CAS-004 — Advanced Security Practitioner
TRACK	CompTIA
DOMAIN	Cyber Security
LEVEL	Expert
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 a expert 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 SecurityX CAS-005 exam objectives and taught in the same order, so nothing on the exam is left uncovered.

This course targets SecurityX CAS-005. That is the current exam for this certification: CompTIA rebranded the CASP+ line to SecurityX and released CAS-005 on 17 December 2024, and it replaced the CASP+ CAS-004 exam. CAS-004 is no longer the version CompTIA lists for this certification, so a candidate starting now should plan for CAS-005. Nothing is lost if you already hold the old credential — existing CASP+ certifications carry over under the SecurityX name and run for their normal three years from the exam date.

CAS-005 is a narrower and deeper exam than CAS-004 was. The weightings moved substantially: security engineering and governance grew, security operations shrank as a proportion, and CompTIA cut the objective count to concentrate the paper. Post-quantum cryptography, automation and infrastructure as code, zero trust and generative AI now sit inside the objectives. Each domain below carries its published weighting, and we give it classroom time in proportion.

Domain 01 — Governance, Risk, and Compliance

The frame every architecture and engineering decision is judged inside. 20% of the exam.

- Security programme documentation: policies, procedures, standards and guidelines, and the differences that matter when one is challenged
- Programme management: training for phishing, security and privacy, plus communication, reporting and clear accountability through a RACI matrix
- Governance frameworks including COBIT and ITIL, and choosing one that fits the organisation rather than the auditor
- Configuration management across the asset lifecycle, configuration management databases and inventory accuracy
- Governance, risk and compliance tooling: control mapping, automation and continuous compliance tracking
- Data governance across production, development, test and quality assurance environments
- Risk management: impact analysis, quantitative against qualitative assessment, and treating rather than merely recording risk
- Third-party and supply chain risk management through the vendor lifecycle
- Threat modelling with ATT&CK, CAPEC and STRIDE, and using actor characteristics and attack patterns to drive control selection
- Attack surface analysis through architecture review, data flow analysis and trust boundary identification
- Compliance strategy against industry obligations such as PCI DSS and ISO/IEC 27000, and frameworks including NIST and the Cloud Security Alliance guidance

Domain 02 — Security Architecture

Designing an estate that holds its shape when the perimeter stops being a useful idea. 27% of the exam.

- Cloud security capabilities: cloud access security brokers in both API-based and proxy-based modes, and shadow IT discovery
- The shared responsibility model, and the gap organisations habitually leave in it

- Securing the delivery pipeline: continuous integration and deployment, and infrastructure as code with tools such as Terraform and Ansible
- Container security and orchestration, and serverless workloads with their distinct exposure
- Cloud data security: data exposure and leakage, data remanence, insecure storage and the consequences of getting key management wrong
- Control strategy in cloud environments — proactive, preventative and detective — plus customer-to-cloud connectivity, service integration and continuous authorisation
- Network architecture: segmentation and microsegmentation, virtual private networking including always-on designs, and secure API integration
- Security boundaries: asset identification and attestation, data perimeters and secured zones
- Deperimeterisation in practice with secure access service edge, software-defined wide area networking and software-defined networking
- Zero trust concepts, expressed as subject-to-object relationships rather than as a product purchase

Domain 03 — Security Engineering

The largest domain: making the architecture real, and making it maintainable. 31% of the exam.

- Automation and orchestration with scripting in PowerShell, Bash and Python
- Event-driven automation, infrastructure as code and the use of cloud APIs
- Generative AI as an engineering tool, and the risk of treating its output as verified
- Automating containerisation, patching and security workflows, including SOAR platforms
- Vulnerability management engineering: scanning, reporting and integration into the pipeline
- Security content automation protocol components — OVAL, XCCDF, CPE, CVE and CVSS — and using them for machine-readable compliance
- Advanced cryptography: post-quantum cryptography and the migration question it forces, key stretching, homomorphic encryption, forward secrecy and hardware acceleration
- Cryptographic use cases for data at rest, in transit and in use, plus secure email, blockchain applications, privacy and compliance obligations
- Certificate-based authentication and the practicalities of running a certificate estate
- Cryptographic techniques: tokenisation, code signing, digital signatures, hashing, cryptographic erase, and symmetric against asymmetric selection

Domain 04 — Security Operations

Running the estate, and finding the things that get past everything you built. 22% of the exam.

- Monitoring and data analysis: SIEM event parsing, retention decisions, and managing false positives and false negatives
- Aggregate analysis — correlation, prioritisation and trend identification across sources
- Establishing behaviour baselines for networks, systems and users, and alerting on genuine deviation
- Analysing vulnerabilities and attack surface: injection flaws, cross-site scripting, insecure configuration, outdated software and weak cipher use
- Selecting mitigations that hold: input validation, patching, encryption, configuration hardening and defence in depth
- Threat hunting with internal intelligence sources including honeypots and user behaviour analytics
- External intelligence: open-source collection, dark web monitoring, information sharing and analysis centres, and threat intelligence platforms

- Indicator sharing with STIX and TAXII, and detection engineering in rule languages such as Sigma, YARA and Snort
- Incident response and malware analysis: sandboxing, indicator extraction, code stylometry, reverse engineering and metadata analysis
- Data recovery and root cause analysis, and feeding the outcome back into architecture rather than closing the ticket

Who should take this

Security architects, security engineers, senior security operations staff, and technical leads who design and approve controls rather than only operate them. It suits people who have depth in two or three areas and now have to defend decisions across all of them, and those moving from a manager-level credential back towards hands-on technical authority.

CompTIA recommends a minimum of ten years of general hands-on IT experience including at least five years of hands-on security, along with Network+, Security+, CySA+, Cloud+ and PenTest+ or equivalent knowledge. These are recommendations, not requirements — CompTIA does not gate the exam on them. They are a fair description of the depth the questions assume, though, and we will tell you honestly if we think you should build more ground first.

This is a practitioner-level exam, not a management one. You should still be technical.

The exam

SecurityX is set and awarded by CompTIA, and forms part of its Xpert series.

- A maximum of 90 questions, a maximum of 165 minutes
- A mix of multiple-choice and performance-based questions
- Scored pass or fail, with no scaled score reported
- Available in English, with further languages to be confirmed by CompTIA

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. The certification runs for three years from the date you pass.

How we deliver it

Five days, classroom or online live, or at your office for a private group. The format is design-led: short teaching blocks, then architecture and engineering problems the group has to solve and then defend, because that is the shape the performance-based questions take. Domain checkpoints each day, and a full-length mock under exam conditions on the final afternoon.

Mapped to the CompTIA SecurityX CAS-005 exam objectives. Taught from Hacky Security's own curriculum and lab estate by instructors who design and run security architecture for a living.

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/casp-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.