

CAS-005: CompTIA SecurityX (formerly CASP+)

Design and lead enterprise security at expert level — and prepare for CompTIA SecurityX (formerly CASP+), exam CAS-005.

DURATION

5 days · 40 hours

LEVEL

Expert

CURRICULUM

14 modules · 7 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

SecurityX, previously known as CASP+, is CompTIA's expert-level certification for practitioners who design and implement security solutions rather than only operate them. It expects you to balance technical depth with governance, risk and business requirements across complex, hybrid environments. This five-day course is built for experienced professionals preparing for that step.

Day one covers governance, risk and compliance: security programme governance, risk management strategies, compliance and legal frameworks, and the security implications of emerging technologies such as artificial intelligence. Day two moves to security architecture, including resilient system design, zero trust, secure cloud and hybrid architectures, and integrating security into the software development life cycle.

Day three focuses on security engineering: identity and access management at scale, endpoint and server hardening, specialised systems, cryptographic solutions and PKI design. Day four addresses security operations, including threat modelling, threat hunting, vulnerability analysis, monitoring and response, and automation. Day five consolidates the domains through cross-domain case scenarios and an exam-readiness session focused on the performance-based items the exam is known for.

Labs and scenarios are written at an architect level: you will evaluate designs, choose controls under constraints and justify your decisions. This course is aligned to the CAS-005 exam and prepares you for it; confirm the current exam details on the CompTIA website before booking.

Highlights

- 40 hours of expert-level, scenario-driven training
- Governance, architecture, engineering and operations
- Advanced labs on zero trust, PKI and threat hunting
- Mapped to the four CAS-005 domains
- Performance-based scenario practice

What's included

- Expert-level scenarios with design trade-offs
- Zero trust and hybrid architecture workshops
- PKI and cryptographic solution design lab
- Threat hunting and detection engineering exercises
- AI security and emerging technology coverage
- Performance-based scenario practice
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- Senior security engineers and architects
- Security team leads
- Experienced analysts moving into architecture
- Holders of Security+, CySA+ or PenTest+ seeking an expert credential

Prerequisites

- Significant hands-on IT security experience (CompTIA recommends around ten years in IT, including five in security)
- Security+, CySA+ or equivalent knowledge
- Familiarity with cloud, networking and identity concepts

Detailed curriculum — 5 days, 40 hours, 14 modules, 7 hands-on labs

Day 1 Governance, Risk & Compliance

8 hours

1.1 Security programme governance

- Governance frameworks and documentation
- Awareness and training programmes
- Security programme management
- Governance for AI adoption

1.2 Risk management

- Risk assessment approaches
- Crisis management and business continuity
- Third-party and supply chain risk
- Risk reporting

LAB Build a risk register and treatment plan for a case organisation · 45 min

1.3 Compliance and privacy

- Regulatory and industry frameworks
- Audit and assurance considerations
- Privacy obligations including data residency

Day 2 Security Architecture

8 hours

2.1 Resilient design

- Availability and integrity design considerations
- Attack surface reduction
- Component placement and segmentation

2.2 Zero trust and hybrid architecture

- Zero trust principles and implementation
- Software-defined networking
- Secure cloud and hybrid patterns
- Secure access service edge (SASE)

LAB Design a zero trust architecture for a hybrid enterprise · 60 min

2.3 Secure development

- Security in the SDLC
- Data security architecture
- Software supply chain security

LAB Threat model an application design · 40 min

Day 3 Security Engineering

8 hours

3.1 Identity and access at scale

- Federation and conditional access
- Troubleshooting IAM
- Privileged access management

3.2 Endpoint, server and specialised systems

- Host hardening and attestation
- OT, ICS and embedded systems security
- Mobile and endpoint management

LAB Harden a server and verify against a benchmark · 45 min

3.3 Cryptography and PKI

- Choosing cryptographic solutions
- Post-quantum considerations
- PKI design and certificate life cycle
- Key management

LAB Build a two-tier PKI and troubleshoot certificate errors · 50 min

Day 4 Security Operations

8 hours

4.1 Threat management

- Threat modelling methods
- Threat hunting
- Threat intelligence integration

LAB Hunt for an adversary using detection data · 60 min

4.2 Monitoring and response

- Detection engineering
- Incident response at enterprise scale
- Vulnerability and attack analysis
- Forensics considerations

4.3 Automation

- Security orchestration and automation
- AI-assisted operations
- Scripting for security tasks

LAB Automate an alert enrichment workflow · 40 min

Day 5 Cross-Domain Scenarios & Exam Readiness

8 hours

5.1 Integrated case scenarios

- Merger and acquisition security integration
- Responding to a major incident
- Cloud migration security design

5.2 Exam readiness

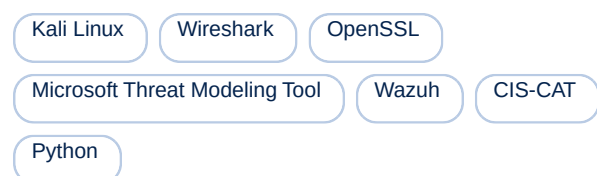
- Performance-based item strategy
- Final domain recap
- Practice test and review

Skills and tools

Skills you will build



Tools used in class



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 SecurityX

Exam code	CAS-005
Questions	Maximum 90
Duration	165 minutes
Passing score	Pass/fail only (no scaled score)
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/securityx

Exam skill areas covered

Security Fundamentals

Security Operations and Compliance

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

Frequently asked questions

Is SecurityX the same as CASP+?

Yes. CompTIA renamed CASP+ to SecurityX, and the current exam is CAS-005.

How is SecurityX different from CISSP?

CISSP is broader and more managerial, while SecurityX focuses on hands-on design and engineering for senior practitioners.

Why is there no scaled score?

SecurityX is reported as pass or fail only, so preparation focuses on consistent competence across all domains.

Do I need prior CompTIA certifications?

They are not required, but the course assumes Security+ and CySA+ level knowledge plus substantial experience.

Can you run this for a senior security team?

Yes. Private batches can use your architecture challenges as scenario material.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/cas-005-comp-tia-securityx · 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.