CompTIA SecurityX

Course code: CTSX

This four-day course prepares you for the CompTIA SecurityX (CAS-005) certification exam, which is aimed at security architects and senior security engineers.SecurityX focuses on designing security for the enterprise environment, whether on-premises, in the cloud or in a hybrid model. The course is therefore built around scenarios and decision-making: which control to choose and how to align it with regulatory requirements and the organisation's risks.The course covers the four exam domains: Governance, Risk, and Compliance; Security Architecture; Security Engineering; and Security Operations. The outline below follows the modules of the official CompTIA course, whose structure differs slightly from the exam domains.

Who is the course for

This course is intended for professionals who design and are accountable for security, not just operate it.

- Security architects and senior security engineers
- Security auditors who assess the effectiveness of controls
- Technical leads of SOC and incident response teams
- Cloud and infrastructure architects responsible for the security of hybrid environments
- GRC specialists who need a technical foundation for risk-based decision-making

What we teach you

After completing the course, you will be able to do the following in a given scenario:

- Set up governance for a security program: policies, frameworks, change management, and rules for the use of AI in the organization
- Assess the impact of regulations and standards on security strategy
- Manage risks, including third-party and AI risks, and prepare the organization for a crisis situation and a data breach
- Model threats and determine which of them apply to your attack surface
- Design a resilient and secure architecture for on-premises, cloud, and hybrid environments and incorporate Zero Trust principles into it
- Secure the software lifecycle, from requirements through CI/CD and the supply chain to system decommissioning
- Design and troubleshoot IAM: federation, conditional access, privileged access, and PKI
- Harden endpoints, networks, and specialized systems, including ICS/OT and legacy environments, make use of hardware security (TPM, HSM, secure and measured boot), and resolve complex network issues
- Choose the right cryptography for a given use case and prepare for the transition to post-quantum algorithms
- Automate security using scripts, SOAR, and generative AI
- Analyze monitoring data, perform threat hunting using threat intelligence, and recommend vulnerability mitigations
- Lead incident analysis from detection through forensic analysis and malware analysis to lessons learned

Required skills

Knowledge at the level of Security+ and CySA+ or PenTest+ is recommended; Network+ and Cloud+ are an advantage.

The course does not cover the fundamentals (what a firewall, PKI, or SIEM is) and goes straight to design and decision-making for each topic.

Teaching materials

Participants will receive the official CompTIA study materials and access to hands-on labs, valid for 12 months.

Course outline

Governance, Risk, and Compliance

- Governance components – security documentation and security program management, governance frameworks, change and configuration management, GRC tools, data governance in staging environments, legal and privacy

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

implications of using AI
- Compliance – industry regulations and standards, security and reporting frameworks, audit vs. assessment vs. certification, privacy protection (GDPR and others), compliance across jurisdictions
- Risk management – impact analysis, risk assessment and risk management, third-party risk, risks to availability, confidentiality, integrity, and privacy, risks of using AI, crisis management and breach response

Architecture and Design

- Secure software development – security requirements, software and hardware assurance, CI/CD, supply chain risk management, end-of-life systems
- Secure architecture – attack surface management, supporting detection and threat hunting in the design, data protection and DLP design, hybrid infrastructure, third-party integrations, control effectiveness
- Operational resilience – availability and integrity by design, network traffic inspection, NAC and VPN, proxies, specialized components
- Cloud infrastructure – CASB and shadow IT detection, shared responsibility model, CI/CD pipelines, infrastructure as code and configuration management (Terraform, Ansible), container and orchestration security, serverless, API security, data protection in the cloud, provider-managed vs. customer-managed encryption keys, cloud control strategies, connectivity and integration of cloud services
- Zero Trust – continuous authorization and context-based reauthentication, network architecture, API validation, asset identification and attestation, security boundaries and deperimeterization, subject-object relationships
- AAA and IAM – provisioning and deprovisioning, federation, conditional access, identity and service providers, policy decision and enforcement points, access control models, PKI architecture, biometrics, secrets management, cloud IAM policies, privileged identity management, IAM troubleshooting

Security Engineering

- Endpoint security – EDR, endpoint privilege management, endpoint protection tools, MDM, attacker TTPs, specialized, embedded, and legacy systems (ICS/OT) and their industry-specific characteristics
- Network infrastructure – troubleshooting complex issues: network misconfigurations, IDS/IPS, observability, DNS security, email security, cryptographic issues, resource exhaustion
- Hardware security and automation – hardware security technologies and features, attacks on hardware and firmware (firmware tampering, BIOS/UEFI, USB), scripting, scheduling and event triggers, generative AI in security, SOAR and workflow automation
- Advanced cryptography – post-quantum cryptography, key stretching, key splitting and envelope encryption, homomorphic encryption and secure multiparty computation, forward secrecy and AEAD, performance vs. security, data protection in different states, blockchain, software integrity and provenance

Security Operations and Incident Response

- Threat modeling – threat profiling, structured threat assessment, attack surface identification, applicability of threats to the organization, threats to AI models (prompt injection, data poisoning, model theft, and model inversion), AI-enabled attacks (deepfakes), and secure deployment of AI assistants
- Security monitoring – data collection and integration in SIEM, data processing and behavioral baselining, alerting, reporting, and metrics
- Attacks and mitigations – vulnerabilities in input and output handling, memory and code execution, cryptography, configuration, and supply chain, along with corresponding mitigations and secure coding
- Threat hunting and threat intelligence – internal and external intelligence sources, counterintelligence and OPSEC, threat intelligence platforms, IoC sharing, rule languages (YARA, Sigma, Snort)
- Incident analysis and response – malware analysis, forensic analysis, detection and initial analysis, prevention and preparedness, continuous improvement

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved