Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

SecurityX Training and Certification

Course Description & Overview

SecureNinja's CompTIA SecurityX (CAS-005) certification training is designed for experienced cybersecurity professionals who specialize in securing enterprise environments. This course focuses on advanced security architecture, engineering, governance, compliance, and security operations, ensuring candidates can design, implement, and manage secure solutions across cloud, on-premises, and hybrid infrastructures.

SecurityX is the next evolution of CompTIA's CASP+, integrating modern security practices such as Zero Trust architecture, AI-based threat analysis, automation, and compliance frameworks. With hands-on scenarios and real-world applications, participants will learn to protect enterprise systems, mitigate risks, respond to threats, and ensure compliance with global security standards.

Why Choose CompTIA SecurityX

- Industry-Leading Certification – Validates expert-level cybersecurity skills required for enterprise security leadership roles
- Advanced Security Focus – Covers risk management, threat intelligence, security architecture, and cryptographic solutions
- Cloud & AI Security Integration – Includes cloud security, AI-enabled threats, and emerging attack techniques
- Vendor-Neutral Approach – Provides expertise applicable across multiple security technologies and enterprise environments
- Performance-Based Learning – Includes real-world simulations and hands-on exercises to reinforce security best practices

Topics Covered

- Governance, Risk, and Compliance – Implementing GRC strategies, security frameworks, and compliance policies
- Security Architecture – Designing and deploying resilient security infrastructures and Zero Trust models
- Security Engineering – Implementing advanced cryptographic solutions, endpoint protection, and threat detection
- Security Operations – Managing incident response, automation, monitoring, and forensic analysis
- Threat Intelligence & AI-Based Security – Detecting and mitigating emerging cyber threats using AI-driven security tools
- Cloud & Hybrid Security – Securing multi-cloud, on-premises, and hybrid environments
- Zero Trust & Identity Management – Implementing multi-factor authentication, access control models, and federated identity solutions

Who is it for

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Cybersecurity Architects – Designing and integrating security solutions across complex enterprise infrastructures
- Security Engineers – Developing automated threat detection and response mechanisms
- Incident Response & Threat Intelligence Analysts – Monitoring security incidents and analyzing cyber threats
- Risk & Compliance Managers – Ensuring adherence to regulatory standards and security frameworks
- Enterprise Security Leaders – Managing enterprise-wide cybersecurity initiatives and strategy

Who Would Benefit

- Experienced cybersecurity professionals seeking expert-level certification
- CISOs, security architects, and engineers responsible for enterprise security
- IT professionals transitioning to cybersecurity leadership roles
- Organizations looking to build a resilient security posture against evolving cyber threats

Prerequisites

- No formal prerequisites, but CompTIA Security+, CySA+, CASP+, CISSP, or equivalent experience is recommended
- Recommended Experience: Minimum 10 years of hands-on IT experience, with at least 5 years in cybersecurity
- Prior knowledge of networking, security frameworks, and risk management is beneficial

Course Outline

Module 1: Governance, Risk, and Compliance

- Implementing security frameworks (ISO 27001, NIST, PCI-DSS)
- Risk assessment, compliance tracing, and regulatory requirements
- Privacy considerations, breach response, and security program management

Module 2: Security Architecture

- Designing resilient system architectures with Zero Trust principles
- Implementing network segmentation, microsegmentation, and secure cloud strategies
- Integrating multi-cloud security and hybrid infrastructure protections

Module 3: Security Engineering

- Implementing advanced cryptographic techniques and post-quantum cryptography
- Securing endpoints, mobile devices, IoT, and industrial control systems
- Troubleshooting network infrastructure security issues

Module 4: Security Operations & Threat Intelligence

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Threat intelligence gathering and real-time threat-hunting strategies
- AI-enabled attacks and machine learning defense techniques
- Incident response, forensic analysis, and log correlation

Module 5: Identity & Access Management and Zero Trust

- Configuring federated identity management, SSO, MFA, and conditional access
- Zero Trust implementation strategies and continuous authentication
- Managing authentication, authorization, and IAM frameworks

Module 6: Security Automation & AI Threat Analysis

- Implementing AI-driven security tools for automated threat detection
- Security orchestration, automation, and response (SOAR) systems
- Integrating machine learning models for advanced cybersecurity applications

Exam Details

- Number of Questions: Up to 90
- Question Types: Multiple-choice & performance-based
- Duration: 165 minutes
- Passing Score: Pass/Fail (no scaled score)

The CompTIA SecurityX (CAS-005) certification is an advanced cybersecurity credential designed for professionals securing enterprise environments with modern security solutions. It focuses on governance, compliance, security operations, architecture, and emerging cyber threats. With hands-on labs and real-world scenarios, this course prepares cybersecurity leaders to develop, manage, and maintain resilient security systems in today’s evolving threat landscape.