

CompTIA SecurityX Certification Prep Course

Durée: 5 Jours Réf de cours: GK2951 Version: CAS-005

Résumé:

Learn advanced security administration tools and techniques while preparing for the CompTIA SecurityX exam (CAS-005) in this hands-on course.

The CompTIA SecurityX (CAS-005) Certification Prep Course is designed for experienced cybersecurity professionals ready to take their expertise to the next level. As the newly rebranded successor to CASP+, SecurityX is part of CompTIA's Xpert series and focuses on the skills required of senior security engineers and architects who lead enterprise-level cybersecurity initiatives. This course equips learners with the advanced knowledge needed to design and implement secure solutions across complex environments, preparing them to meet today's evolving threat landscape head-on.

Throughout the course, students will engage with real-world scenarios and hands-on labs that mirror the challenges faced by professionals in high-stakes cybersecurity roles. Topics include digital security architecture, enterprise risk management, governance, and advanced threat mitigation strategies. Whether you're aiming to validate your skills or step into a leadership role in cybersecurity, this course offers the depth and rigor needed to succeed on the SecurityX (CAS-005) exam and beyond.

Public visé:

This course is designed for IT professionals in the cybersecurity industry whose primary job responsibility is to secure complex enterprise environments. The target student should have real-world experience with the technical administration of these enterprise environments. This course is also designed for students who are seeking the CompTIA SecurityX certification and who want to prepare for Exam CAS-005. Students seeking SecurityX certification should have at least 10 years of experience in IT management, with at least 5 years of hands-on technical security experience.

Objectifs pédagogiques:

- Design, implement, and integrate secure solutions across complex environments to support a resilient enterprise in security architecture and engineering.
- Utilize cryptographic technologies and techniques while evaluating the impact of emerging trends, such as artificial intelligence, on information security.
- Use automation, monitoring, detection, and incident response to proactively support ongoing security operations.
- Implement governance, compliance, risk management, and threat modeling strategies across the enterprise.
- Apply security practices to cloud, on-premises, and hybrid environments to ensure enterprise-wide protection.
- Validate advanced, hands-on skills in security architecture and senior security engineering within live environments.

Pré-requis:

To be fit for this advanced course, you should have at least a foundational knowledge of information security. This includes, but is not limited to:

- Knowledge of identity and access management (IAM) concepts and common implementations, such as authentication factors and directory services.
- Knowledge of cryptographic concepts and common implementations, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) and public key infrastructure (PKI).
- Knowledge of computer networking concepts and implementations, such as the TCP/IP model and configuration of routers and switches.
- Knowledge of common security technologies used to safeguard the enterprise, such as anti-malware solutions, firewalls, and VPNs
- G013 - Formation CompTIA Security+

Contenu:

Module 1: Introduction

- Preassessment

Module 2: Summarizing Governance Risk and Compliance

- Implement Appropriate Governance Components
- Explain Legal Compliance
- Apply Risk Management Strategies

Module 3: Implementing Architecture and Design

- Apply Software Development
- Integrate Software Architecture
- Support Operational Resilience
- Implement Cloud Infrastructure
- Integrate Zero Trust Concepts
- Troubleshoot using AAA and IAM

Module 4: Understanding Security Engineering

- Enhance Endpoint Security
- Configure Network Infrastructure
- Initiate Security Automation
- Apply Cryptography Concepts

Module 5: Applying Security Operations and Incident Response

- Perform Threat Modeling
 - Examine Security Monitoring
 - Analyze Known Attack Methods and Associated Mitigations
 - Apply Threat Hunting Tools and Technologies
 - Evaluate Incident Analysis and Response
-

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "*****booking form*****" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur globalknowledge.fr/handicap
- Le Règlement intérieur est disponible sur globalknowledge.fr/reglement