CompTIA SecurityX

Duration: 5 Days

COURSE DESCRIPTION

Designed for experienced cybersecurity professionals, the CompTIA SecurityX Certification Prep (Exam CAS-005) course focuses on advanced security concepts essential for managing and securing complex enterprise environments also covering governance, risk management, security architecture and security operations. implementation of secure solutions across diverse infrastructures. Participants will gain expertise in automation, threat modeling, and cryptographic technologies, ensuring proactive detection and response to cybersecurity threats.

COURSE OBJECTIVES

In this course, you will analyze and apply advanced security concepts, principles, and implementations that contribute to enterprise-level security. You will:

- Architect and implement secure solutions across complex environments
- Manage governance, risk, compliance, and threat modeling strategies
- Secure cloud, on-premises, and hybrid infrastructures
- Use automation and incident response techniques for proactive security
- Apply advanced cryptographic technologies and assess emerging AI-related risks

COURSE OUTLINE

Module 1: Governance, Risk, and Compliance

Organizational security requirements, implementing the appropriate governance components.

- Security program documentation
- Security program management
- Governance frameworks
- Change/configuration management
- Governance risk and compliance (GRC) tools
- Data governance in staging environments

Organizational security requirements, perform risk management activities.

- Impact analysis
- Risk assessment and management
- Third-party risk management
- Availability risk considerations
- Confidentiality risk considerations
- Integrity risk considerations
- Privacy risk considerations
- Crisis management
- Breach response

Explain how compliance affects information security strategies.

- Awareness of industry-specific
- Industry standards
- Security and reporting frameworks

- Audits vs. assessments vs. certifications
- Privacy regulations
- Awareness of cross-jurisdictional compliance requirements

Perform threat-modeling activities.

- Actor characteristics
- Attack patterns
- Frameworks
- Attack surface determination
- Methods
- Modeling applicability of threats to the organization/environment

Summarize the information security challenges associated with artificial intelligence (AI) adoption.

- Legal and privacy implications
- Threats to the model
- AI-enabled attacks
- Risks of AI usage
- AI-enabled assistants/digital workers

Module 2: Security Architecture

Analyze requirements to design resilient systems.

- Component placement and configuration
- Availability and integrity design considerations

Implement security in the early stages of the systems life cycle and throughout subsequent stages.

- Security requirements definition
- Software assurance
- Continuous integration/continuous deployment (CI/CD)
- Supply chain risk management
- Hardware assurance
- End-of-life (EOL) considerations

Integrate appropriate controls in the design of secure architecture.

- Attack surface management and reduction
- Detection and threat-hunting enablers
- Information and data security design
- DLP
- Hybrid infrastructures
- Third-party integrations
- Control effectiveness

Apply security concepts to the design of access, authentication, and authorization systems.

- Provisioning/deprovisioning
- Federation
- Single sign-on (SSO)
- Conditional access
- Identity provider
- Service provider
- Attestations
- Policy decision and enforcement points
- Access control models
- Logging and auditing

- Public key infrastructure (PKI) architecture
- Access control systems

Securely implement cloud capabilities in an enterprise environment.

- Cloud access security broker (CASB)
- Shadow IT detection
- Shared responsibility model
- CI/CD pipeline
- Terraform
- Ansible
- Package monitoring
- Container security
- Container orchestration
- Serverless
- API security
- Cloud vs. customer-managed
- Cloud data security considerations
- Cloud control strategies
- Customer-to-cloud connectivity
- Cloud service integration
- Cloud service adoption

Integrate Zero Trust concepts into system architecture design.

- Continuous authorization
- Context-based reauthentication
- Network architecture
- API integration and validation
- Asset identification, management, and attestation
- Security boundaries
- Deperimeterization
- Defining subject-object relationships

Module 3: Security Engineering

Troubleshoot common issues with identity and access management (IAM) components in an enterprise environment.

- Subject access control
- Biometrics
- Secrets management
- Conditional access
- Attestation
- Cloud IAM access and trust policies
- Logging and monitoring
- Privilege identity management
- Authentication and authorization

Analyze requirements to enhance the security of endpoints and servers.

- Application control
- Endpoint detection response (EDR)
- Event logging and monitoring
- Endpoint privilege management
- Attack surface monitoring and reduction
- Host-based intrusion protection system / host-based detection system (HIPS/ HIDS)

- Anti-malware
- SELinux
- Host-based firewall
- Browser isolation
- Configuration management
- Mobile device management (MDM) technologies
- Threat-actor tactics, techniques, and procedures (TTPs)

Troubleshoot complex network infrastructure security issues.

- Network misconfigurations
- IPS/IDS issues
- Observability
- Domain Name System (DNS) security
- Email security
- Transport Layer Security (TLS) errors
- Cipher mismatch
- PKI issues
- Issues with cryptographic implementations
- DoS/distributed denial of service (DDoS)
- Resource exhaustion
- Network access control list (ACL) issues

Implement hardware security technologies and techniques.

- Roots of trust
- Security coprocessors
- Virtual hardware
- Host-based encryption
- Self-encrypting drive (SED)
- Secure Boot
- Measured boot
- Self-healing hardware
- Tamper detection and countermeasures
- Threat-actor TTPs

Secure specialized and legacy systems against threats.

- Operational technology (OT)
- Internet of Things (IoT)
- System-on-chip (SoC)
- Embedded systems
- Wireless technologies/radio frequency (RF)
- Security and privacy considerations
- Industry-specific challenges
- Characteristics of specialized/legacy systems

Use automation to secure the enterprise.

- Scripting
- Cron/scheduled tasks
- Event-based triggers
- Infrastructure as code (IaC)
- Configuration files
- Cloud APIs/software development kits (SDKs)
- Generative AI

- Containerization
- Automated patching
- Auto-containment
- Security orchestration, automation, and response (SOAR)
- Vulnerability scanning and reporting
- Security Content Automation Protocol (SCAP)
- Workflow automation

Explain the importance of advanced cryptographic concepts.

- Post-quantum cryptography (PQC)
- Key stretching
- Key splitting
- Homomorphic encryption
- Forward secrecy
- Hardware acceleration
- Envelope encryption
- Performance vs. security
- Secure multiparty computation
- Authenticated encryption with associated data (AEAD)
- Mutual authentication

Apply the appropriate cryptographic use case and/or technique.

- Use cases
- Techniques

Module 4: Security Operations

Analyze data to enable monitoring and response activities.

- Security information event management (SIEM)
- Aggregate data analysis
- Behavior baselines and analytics
- Incorporating diverse data sources
- Alerting
- Reporting and metrics

Analyze vulnerabilities and attacks and recommend solutions to reduce the attack surface.

- Vulnerabilities and attacks
- Mitigations

Apply threat-hunting and threat intelligence concepts.

- Internal intelligence sources
- External intelligence sources
- Counterintelligence and operational security
- Threat intelligence platforms (TIPs)
- Indicator of compromise (IoC) sharing
- Rule-based languages
- Indicators of attack

Analyze data and artifacts in support of incident response activities.

- Malware analysis
- Reverse engineering
- Volatile/non-volatile storage analysis
- Network analysis

- Host analysis
- Metadata analysis
- Hardware analysis
- Data recovery and extraction
- Threat response
- Preparedness exercises
- Timeline reconstruction
- Root cause analysis
- Cloud workload protection platform (CWPP)
- Insider threat

PREREQUISITES

Minimum of 10 years of general, hands-on IT experience that includes at least 5 years of broad, hands-on IT security experience.

WHO SHOULD ATTEND

- Cybersecurity Specialist
- Network Security Analyst
- Security Architect
- Senior Security Engineer
- SOC Manager
- Security Analyst
- IT Cybersecurity Specialist / INFOSEC Specialist
- Cyber Risk Analyst