COURSE SYLLABUS

CompTIA SecurityX Exam Preparation Course (Self-Paced)

Build the advanced governance, architecture, engineering, and operations skills the CompTIA SecurityX exam demands.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/securityx-exam-preparation-course-self-paced

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Course and Exam Orientation

- Lessons:
  - Exam format and domain weighting
  - How this course maps to the CAS-005 objectives
  - Building a personal study and practice plan
- Applied activity: Learners map their own job responsibilities against the four domains and identify their two weakest areas.

Module 2 (Objective 1.1): Implementing Governance Components

- Lessons:
  - Security program documentation and management
  - Governance frameworks and change management
  - GRC tools and data governance
- Applied activity: Learners build a RACI matrix for a new security policy rollout and identify a GRC tool to track its compliance status.

Module 3 (Objective 1.2): Performing Risk Management Activities

- Lessons:
  - Impact analysis and risk assessment
  - Third-party risk and availability/confidentiality risk
  - Integrity, privacy risk, and crisis management
- Applied activity: Learners score a scenario involving a subprocessor data breach and select the correct availability, confidentiality, and privacy risk responses.

Module 4 (Objective 1.3): Compliance and Information Security Strategy

- Lessons:
  - Industry-specific compliance and standards

- Security and reporting frameworks and audits
- Privacy regulation and cross-jurisdictional compliance

- Applied activity: Learners review a scenario describing a multinational data transfer and identify which privacy regulations and cross-jurisdictional obligations apply.

Module 5 (Objective 1.4): Threat Modeling

- Lessons:
  - Threat actor characteristics and attack patterns
  - Threat modeling frameworks
  - Attack surface determination and modeling methods
- Applied activity: Learners apply STRIDE to a sample application architecture diagram and identify the attack surface introduced by a described organizational change, such as a merger.

Module 6 (Objective 1.5): AI Adoption and Information Security Challenges

- Lessons:
  - Legal, privacy, and model-level threats
  - AI-enabled attacks and usage risk
  - Governing AI-enabled assistants and digital workers
- Applied activity: Learners review a proposed AI assistant deployment and design the access permissions, guardrails, and usage disclosure it needs before approval.

Module 7 (Objective 2.1): Designing Resilient Systems

- Lessons:
  - Security component placement
  - Availability and integrity design considerations
  - Applying resilient design to a scenario
- Applied activity: Learners place a set of security components onto a blank architecture diagram for a described resilient system requirement.

Module 8 (Objective 2.2): Security Throughout the Systems Life Cycle

- Lessons:
  - Security requirements and software assurance
  - CI/CD and supply chain risk
  - Hardware assurance and end-of-life considerations
- Applied activity: Learners select the correct software assurance technique for each stage of a described CI/CD pipeline and flag a missing SBOM step.

Module 9 (Objective 2.3): Integrating Controls into Secure Architecture

- Lessons:
  - Attack surface management and detection enablers
  - Information and data security design
  - Hybrid infrastructure, third-party integration, and control effectiveness
- Applied activity: Learners recommend sensor placement and a DLP control for a described hybrid infrastructure with a third-party integration.

Module 10 (Objective 2.4): Access, Authentication, and Authorization System Design

- Lessons:

- Provisioning, federation, and policy points
- Access control models and logging
- PKI architecture and access control systems

- Applied activity: Learners select the correct access control model for three described scenarios and design a certificate template for a new PKI use case.

Module 11 (Objective 2.5): Securely Implementing Cloud Capabilities

- Lessons:
  - CASB, shared responsibility, and CI/CD in the cloud
  - Container, serverless, and API security
  - Cloud data security and control strategies

- Applied activity: Learners review a cloud workload diagram and assign a CASB, container, and API control to close a described shadow IT and data exposure gap.

Module 12 (Objective 2.6): Integrating Zero Trust into System Architecture Design

- Lessons:
  - Continuous authorization and network architecture
  - API integration and asset identification
  - Security boundaries and deperimeterization

- Applied activity: Learners redesign a perimeter-based network into a zero trust architecture, defining security boundaries and selecting a deperimeterization technology.

Module 13 (Objective 3.1): Troubleshooting Identity and Access Management

- Lessons:
  - Subject access control and secrets management
  - Conditional access and privileged identity management
  - Authentication and authorization protocols

- Applied activity: Learners diagnose a described SSO failure and identify whether the root cause lies in the SAML assertion, the conditional access policy, or key rotation.

Module 14 (Objective 3.2): Enhancing Endpoint and Server Security

- Lessons:
  - Endpoint control and monitoring
  - Host-based protection technologies
  - Threat-actor tactics, techniques, and procedures against endpoints

- Applied activity: Learners review a sequence of endpoint events and identify which threat-actor TTP each step represents.

Module 15 (Objective 3.3): Troubleshooting Network Infrastructure Security

- Lessons:
  - Network misconfigurations and IPS/IDS issues
  - DNS and email security
  - TLS, PKI, and denial-of-service issues

- Applied activity: Learners review a network capture and email header showing a spoofed message, and identify which of DKIM, SPF, or DMARC failed to catch it.

Module 16 (Objective 3.4): Implementing Hardware Security Technologies

- Lessons:

- Roots of trust and coprocessors
- Boot integrity and tamper resistance
- Hardware-level threat-actor tactics

- Applied activity: Learners select the correct hardware root of trust and boot integrity control for a device that must resist firmware tampering.

Module 17 (Objective 3.5): Securing Specialized and Legacy Systems

- Lessons:
  - Operational technology and embedded systems
  - Security and privacy considerations for specialized systems
  - Industry-specific challenges and legacy system characteristics
- Applied activity: Learners design a segmentation approach for a described SCADA environment that cannot be patched, citing the safety constraint that rules out a standard patching approach.

Module 18 (Objective 3.6): Using Automation to Secure the Enterprise

- Lessons:
  - Scripting and infrastructure as code
  - Automated response and containment
  - Vulnerability scanning and workflow automation
- Applied activity: Learners draft a SOAR playbook step that automatically contains a host flagged by a CVSS-scored vulnerability scan.

Module 19 (Objective 3.7): Advanced Cryptographic Concepts

- Lessons:
  - Post-quantum cryptography
  - Key management and computation techniques
  - Performance, secrecy, and authentication trade-offs
- Applied activity: Learners evaluate a proposed cryptographic architecture for a long-lived data set and recommend whether post-quantum algorithms or envelope encryption better fit the retention requirement.

Module 20 (Objective 3.8): Applying Cryptographic Use Cases and Techniques

- Lessons:
  - Cryptographic use cases across data states
  - Provenance, authentication, and key management use cases
  - Cryptographic techniques
- Applied activity: Learners select the cryptographic use case and technique that best fit a described mobile payment scenario, justifying the choice against data-in-use and non-repudiation requirements.

Module 21 (Objective 4.1): Analyzing Data for Monitoring and Response

- Lessons:
  - SIEM and aggregate data analysis
  - Behavior baselines and diverse data sources
  - Alerting and reporting
- Applied activity: Learners triage a batch of SIEM alerts and rank them using the prioritization factors, then propose one SIEM tuning change to reduce noise.

Module 22 (Objective 4.2): Analyzing Vulnerabilities and Attacks to Reduce Attack Surface

- Lessons:
  - Injection, memory, and request-forgery vulnerabilities
  - Configuration, software, and cryptographic weaknesses
  - Mitigations
- Applied activity: Learners review a short code and traffic sample set, identify the vulnerability class present in each, and select a matching mitigation for each.

Module 23 (Objective 4.3): Threat-Hunting and Threat Intelligence

- Lessons:
  - Internal and external intelligence sources
  - Counterintelligence and threat intelligence platforms
  - Rule-based detection languages and indicators of attack
- Applied activity: Learners draft a hypothesis-based hunt using a described threat intelligence feed and translate one indicator of compromise into a Sigma rule.

Module 24 (Objective 4.4): Incident Response Data and Artifact Analysis

- Lessons:
  - Malware and reverse-engineering analysis
  - Storage, network, host, and metadata analysis
  - Response, recovery, and root cause
- Applied activity: Learners reconstruct a simulated incident timeline from a set of host, network, and metadata artifacts, then identify the root cause.

Module 25: Exam Strategy, Practice Scenarios, and Review

- Lessons:
  - Performance-based question strategy
  - Full-length practice scenarios across all four domains
  - Reviewing weak domains and final readiness
- Applied activity: Learners complete a timed practice scenario set spanning all four domains and self-score against the domain weighting.