COURSE SYLLABUS

CompTIA Security+ Exam Preparation Course (Self-Paced)

Prepare to sit the CompTIA Security+ exam and build the security fundamentals employers and agencies look for.

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



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

Course Outline

Module 1: Security Controls and Foundational Concepts

- Lessons:
  - Categories and Types of Security Controls
  - The CIA Triad and Non-Repudiation
  - Authentication, Authorization, and Accounting
  - Zero Trust, Deception, and Disruption Technology
- Applied activity: Given a short scenario describing an organization's security posture, learners categorize five described controls by type and category and justify each classification.

Module 2: Change Management and Cryptographic Solutions

- Lessons:
  - Business Processes Tied to Change Management
  - Technical Change Management Implications
  - Symmetric and Asymmetric Encryption
  - Hashing, Digital Signatures, and Public Key Infrastructure
- Applied activity: Learners walk through a simplified PKI certificate request and validation scenario, identifying which cryptographic solution addresses confidentiality, integrity, or authenticity at each step. Note for the builder: align this module's content with the standalone Cryptography Essentials course so learners who take both do not see contradictory explanations.

Module 3: Threat Actors and Motivations

- Lessons:
  - Types of Threat Actors: Nation-State, Organized Crime, Hacktivist, Insider
  - Threat Actor Attributes: Resources, Sophistication, Funding
  - Motivations: Financial, Political, Ethical, Espionage
- Applied activity: Given four short incident summaries, learners identify the most likely threat actor type and motivation for each and

explain their reasoning.

Module 4: Threat Vectors, Attack Surfaces, and Vulnerability Types

- Lessons:
  - Message-Based and Image-Based Threat Vectors
  - Network, Removable Media, and Supply Chain Vectors
  - Human Vectors and Social Engineering
  - Application, Operating System, and Hardware Vulnerabilities
  - Zero-Day and Misconfiguration Vulnerabilities
- Applied activity: Learners review five short scenarios, including an email, a phone call, a USB drive found in a parking lot, an unpatched server, and a vendor breach, and identify the vector and the social engineering principle involved where applicable.

Module 5: Indicators of Malicious Activity and Mitigation Techniques

- Lessons:
  - Malware Indicators: Ransomware, Trojans, Worms, Spyware
  - Physical and Network Attack Indicators
  - Application Attack Indicators: Injection, Cross-Site Scripting, Buffer Overflow
  - Segmentation, Access Control, and Hardening as Mitigations
  - Patching, Monitoring, and Least Privilege as Mitigations
- Applied activity: Learners triage a short simulated alert log based on described symptoms, select the matching malware or attack type, and propose one mitigation for each.

Module 6: Security Architecture Models

- Lessons:
  - Cloud, On-Premises, and Hybrid Models
  - Infrastructure as Code and Virtualization
  - IoT, Industrial Control Systems, and Embedded System Considerations
  - Considerations for Availability, Resilience, and Cost
- Applied activity: Learners map security responsibilities for a described hybrid deployment, dividing them between cloud provider and customer using a shared responsibility framing.

Module 7: Enterprise Infrastructure Security

- Lessons:
  - Network Appliances: Firewalls, Load Balancers, Proxies
  - VPNs and Secure Communication
  - Zero Trust Network Architecture
  - Port Security and Network Segmentation Techniques
- Applied activity: Learners annotate a simple network diagram description with the placement of a firewall, a VPN concentrator, and a segmentation boundary to meet a stated security requirement.

Module 8: Data Protection, Resilience, and Recovery

- Lessons:
  - Data Types, Classification, and Ownership
  - Data States and Protection Techniques: At Rest, In Transit, In Use
  - Resilience Concepts: Redundancy, High Availability
  - Recovery Concepts: Backups, Recovery Time and Recovery Point Objectives

- Testing Recovery: Tabletop Exercises and Failover Tests

- Applied activity: Given a described outage scenario, learners calculate whether a stated backup schedule meets a target recovery point objective and propose one resilience improvement.

Module 9: Hardening Techniques and Asset Management

- Lessons:
  - Baselines and Secure Configuration
  - Hardening Targets: Endpoints, Servers, Mobile, Wireless
  - Asset Inventory and Classification
  - Asset Lifecycle: Acquisition, Disposal, and Sanitization
- Applied activity: Learners review a short asset list with mixed device types and propose one hardening action and one lifecycle consideration for each.

Module 10: Vulnerability Management

- Lessons:
  - Vulnerability Identification: Scanning and Feeds
  - Analysis: Scoring and Prioritization
  - Vulnerability Response and Remediation
  - Validation and Reporting
- Applied activity: Given four described vulnerabilities with different severity and exploitability, learners rank them for remediation priority and justify the order.

Module 11: Monitoring, Alerting, and Enterprise Security Capabilities

- Lessons:
  - Monitoring Concepts: Logs, Baselines, Anomalies
  - SIEM and Security Data Aggregation
  - Firewalls, Intrusion Detection, and Intrusion Prevention
  - Data Loss Prevention and Endpoint Detection and Response
- Applied activity: Learners review a short set of described log entries, identify which would trigger a SIEM alert and why, then select the enterprise capability best suited to prevent recurrence.

Module 12: Identity and Access Management, Automation, and Orchestration

- Lessons:
  - Identity Concepts: Provisioning, Federation, Single Sign-On
  - Access Control Models: Role-Based, Attribute-Based, Least Privilege
  - Multifactor Authentication and Privileged Access Management
  - Automation and Orchestration Use Cases and Benefits
  - Automation Risks and Considerations
- Applied activity: Learners design a basic access model of roles and permissions for a described small organization and identify one process suitable for automation.

Module 13: Incident Response and Investigation Data Sources

- Lessons:
  - Incident Response Process and Roles
  - Preparation, Detection, and Analysis Phases
  - Containment, Eradication, and Recovery Phases

- Log and Data Sources for Investigation
- Lessons Learned and Reporting

- Applied activity: Given a short simulated incident narrative, learners sequence the response phases taken and identify which log or data source would confirm each phase's findings.

Module 14: Security Governance and Risk Management

- Lessons:
  - Governance Structures: Policies, Standards, Procedures, Guidelines
  - Roles and Responsibilities in Security Governance
  - Risk Identification and Assessment
  - Risk Treatment: Accept, Avoid, Transfer, Mitigate
  - Risk Registers and Reporting
- Applied activity: Learners assess a described organizational risk, assign a qualitative rating, and select a risk treatment option with justification.

Module 15: Third-Party Risk and Compliance

- Lessons:
  - Vendor Assessment and Due Diligence
  - Contractual and Supply Chain Risk Considerations
  - Compliance Concepts: Regulations, Standards, Frameworks
  - Consequences of Non-Compliance
  - Privacy Considerations in Compliance
- Applied activity: Learners review a short vendor profile and identify two due diligence questions they would ask before onboarding the vendor, tied to a named framework or regulation category.

Module 16: Audits, Assessments, and Security Awareness

- Lessons:
  - Attestation and Internal versus External Audits
  - Vulnerability Assessments and Penetration Testing Basics
  - Security Awareness Program Design
  - Phishing Simulations and Reporting Culture
- Applied activity: Learners outline a basic annual security awareness plan for a described small organization, including one phishing simulation and one reporting mechanism.