COURSE SYLLABUS

CompTIA Security+ Certification Training Course

Build core cybersecurity competencies in threat detection, network security, and risk management while preparing for the CompTIA Security+ (SY0-701) certification exam.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://sdfm.graduateschool.edu/courses/comptia-security-certification-training



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

Course Outline

Lesson 1: Assessing Information Security Risk

- Identify the importance of risk management
- Assess risk in computing and network environments
- Mitigate risks through various strategies
- Integrate documentation into the risk management process

Lesson 2: Analyzing Reconnaissance Threats to Computing and Network Environments

- Assess the impact of reconnaissance incidents
- Analyze the effects of social engineering attacks

Lesson 3: Analyzing Attacks on Computing and Network Environments

- Assess the impact of system hacking attacks
- Evaluate the impact of web-based attacks and malware
- Analyze hijacking and impersonation attacks
- Understand the consequences of DoS incidents
- Analyze threats to mobile and cloud security

Lesson 4: Analyzing Post-Attack Techniques

- Assess command and control techniques
- Understand persistence and lateral movement techniques
- Assess data exfiltration and anti-forensics techniques

Lesson 5: Managing Vulnerabilities in the Organization

- Implement a vulnerability management plan
- Assess common vulnerabilities and perform vulnerability scans
- Conduct penetration tests on network assets

Lesson 6: Collecting Cybersecurity Intelligence

- Deploy a security intelligence collection and analysis platform
- Collect data from network-based and host-based intelligence sources

Lesson 7: Analyzing Log Data

- Use common tools to analyze logs
- Utilize SIEM tools for analysis

Lesson 8: Performing Active Asset and Network Analysis

- Analyze incidents with Windows and Linux-based tools
- Examine malware and indicators of compromise

Lesson 9: Responding to Cybersecurity Incidents

- Deploy an incident handling and response architecture
- Mitigate incidents and prepare for forensic investigations

Lesson 10: Investigating Cybersecurity Incidents

- Apply a forensic investigation plan
- Securely collect and analyze electronic evidence
- Follow up on investigation results

Lesson 11: Addressing Security Architecture Issues

- Remediate identity and access management issues
- Implement security during the SDLC

Appendices

- Taking the Exams
- Mapping Course Content to CompTIA® Cybersecurity Analyst (CySA+®) Exam CS0-001
- Security Resources