THE LEARNING CENTER
A TECHNICAL TRAINING INSTITUTION

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. CompTIA Security+ incorporates industry best practices in hands-on troubleshooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.

CompTIA Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

The new CompTIA Security+ SY0-601 exam is available as of November 12, 2020.

Our unique model follows a streamlined approach to workforce development and skills attainment

Assess: Assess each student to determine existing skill sets

Educate: Deliver goal-specific training utilizing all delivery modalities

Mentor: Expose students to instructors and mentors with front-line IT and cybersecurity experience

Certify: Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate: Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

Exam Objectives: SY0-601

Attacks, Threats, and Vulnerabilities	24%
Architecture and Design	21%
Implementation	25%
Operations and Incident Response	16%
Governance, Risk, and Compliance	14%

Course Outline:

Chapter 1: Social Engineering Techniques
Chapter 2: Type of Attack Indicators
Chapter 3: Application Attack Indicators
Chapter 4: Network Attack Indicators
Chapter 5: Threat Actors, Vectors, and Intelligence Sources
Chapter 6: Vulnerabilities
Chapter 7: Security Assessments
Chapter 8: Penetration Testing
Chapter 9: Enterprise Security Architecture
Chapter 10: Virtualization and Cloud Security
Chapter 11: Secure Application Development, Deployment, and Automation Concepts
Chapter 12: Authentication and Authorization
Chapter 13: Cybersecurity Resilience
Chapter 14: Embedded and Specialized Systems
Chapter 15: Physical Security Controls
Chapter 16: Cryptographic Concepts
Chapter 17: Secure Protocols
Chapter 18: Host and Application Security
Chapter 19: Secure Network Design
Chapter 20: Wireless Security
Chapter 21: Secure Mobile Solutions
Chapter 22: Implementing Cloud Security
Chapter 23: Identity and Account Management Controls
Chapter 24: Implement Authentication and Authorization
Chapter 25: Public Key Infrastructure
Chapter 26: Tools/Assess Organizational Security
Chapter 27: Incident Response Policies, Processes, and Procedures
Chapter 28: Investigations
Chapter 29: Mitigation Techniques and Controls
Chapter 30: Digital Forensics
Chapter 31: Security Controls
Chapter 32: Regulations, Standards, and Frameworks
Chapter 33: Organizational Policies
Chapter 34: Risk Management
Chapter 35: Privacy

Included

40 hours of instructor-led training sessions
CompTIA authorized textbook and class materials
Practice questions and exam study tips