The Learning Center
Las Vegas

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. Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.

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+ SY0-501 exam is available as of October 4, 2017.

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

Assess: Assess each individual 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

The Learning Center
Las Vegas

Course Outline:

Chapter 1: Security Fundamentals
- Module A: Security concepts
- Module B: Risk management
- Module C: Vulnerability assessment

Chapter 2: Understanding attacks
- Module A: Understanding attackers
- Module B: Social engineering
- Module C: Malware
- Module D: Network attacks
- Module E: Application attacks

Chapter 3: Cryptography
- Module A: Cryptography concepts
- Module B: Public key infrastructure

Chapter 4: Network fundamentals
- Module A: Network components
- Module B: Network addressing
- Module C: Network ports and applications

Chapter 5: Securing networks
- Module B: Transport encryption
- Module C: Hardening networks
- Module D: Monitoring and detection

Chapter 6: Securing hosts and data
- Module A: Securing hosts
- Module B: Securing data
- Module C: Mobile device security

Chapter 7: Securing network services
- Module A: Securing applications
- Module B: Virtual and cloud systems

Chapter 8: Authentication
- Module A: Authentication factors
- Module B: Authentication protocols

Chapter 9: Access control
- Module A: Access control principles
- Module B: Account management

Chapter 10: Organizational security
- Module A: Security policies
- Module B: User training

Module C: Physical security and safety

Chapter 11: Disaster planning and recovery

Included

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

Sessions

2018 Dates:
Session 5: 5/12118-5/25/18 8am-5pm PST
Session 6: 7/16/18-7/20/18 8am-5pm PST
Session 7: 8/20/18-8/24/18
Session 8: 10/1/18-10/5/18
Session 9: 11/12/18-11/16/18

www.tlclasvegas.com