CompTIA Security+

LEARNING OBJECTIVES

Technology is complicated. It moves fast. It's always evolving. And it's essential to the success of any business—big or small. That means there's plenty of opportunity for professionals with a knack for IT security, OS installation, and firewall maintenance.

But quality online IT certificate programs are few and far between. With our training, you'll gain the knowledge and skills you need to secure a corporate network using a layered security model. And, we prepare learners to take the **TestOut Security Pro** and **Security+ SY0-501** exams—1 free voucher included with the course.

Program Orientation (1 hour)

- Get an overview of the course and set expectations.

Introduction (1 hour)

- Get a security overview.
- Use the simulator.

Security Basics (4 hours)

- Understand attacks and defense planning.
- Review cryptography basics, network monitoring, and incident response.

Policies, Procedures, and Awareness (5 hours)

- Discuss security policies, risk management, business continuity, social engineering, app development, app deployment, and third-party integration.

Physical (2 hours)

- Discuss physical threats.
- Understand device protection.
- Review network infrastructure protection and environmental controls.

Perimeter (9 hours)

- Learn about firewalls, network address translation (nat), virtual private networks (vpn), web threat protection, network access protection, and wireless attacks.

Network (10 hours)

- Review network threats, network device vulnerabilities, network applications, switch attacks, and switch security.
- Use VLANs.
- Understand router security.
- Discuss intrusion detection and prevention, protocol analyzers, remote access, network authentication, penetration testing, virtual networking, software-defined networking (SDN), and cloud services.

Host (10 hours)

- Learn about malware, password attacks, windows system hardening, hardening enforcement, BYOD security, and more.

Application (12 hours)

- Comprehend access control models, authentication, authorization, web application attacks, internet browsers, application development, and more.

Data (9 hours)

- Discuss data management, advanced cryptography, symmetric encryption, asymmetric encryption, file encryption, public key infrastructure (PKI), data loss prevention (DLP), and cloud storage.

Security Pro Practice (43 hours)

- Prepare for certification.

Security+ Security Practice Certification Exams (17 hours)

- Prepare for certification.

Security Pro Certification—Optional, Single Attempt Only (2 hours)

- Prepare for certification.

Total Hours = 125