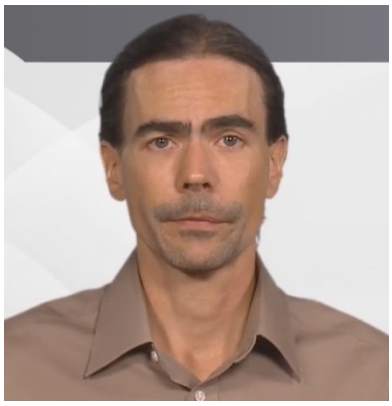
Pearson | Live Virtual Training

Train with Confidence and Advance Your Career

CompTIA Security+ (SYO-501) Certification Crash Course



Security+ is one of the most popular security certifications in the IT industry and is usually the first that IT professionals attempt. It is a three-year renewable certification that is required by the DoD and other government agencies, not to mention many corporations. The Security+ exam shows employers that a person has developed a foundation of the necessary skills needed to secure applications, computers and networks in the workplace.

This live training course will cover the SYO-501 exam. It is designed to give you the information you need to pass the exam and start your successful career as a security professional.

This Live Virtual Training is for:

- Learners who are studying for and need to pass the Security+ exam
- Professionals working in a company or organization that requires a CompTIA Security+ certification
- Professionals who want to increase their security awareness as it applies to tools, technologies, and secure design.
- Professionals who wish to bolster their resume.

You will learn:

- Explore security threats, attacks and vulnerabilities, and how to defend against and prevent these from occurring.
- Understand how security technologies and tools function. For example, firewalls, proxies, NAC, NIDS/NIPS, DLP, protocol analyzers, network scanners, and much more.
- Learn about security architecture and design, including concepts such as defense-in-depth, benchmarking, industry-standard frameworks, secure network design, and secure systems design.
- Compare and contrast various identity and access management technologies such as single sign-on and federation, and LDAP, Kerberos, MS-CHAP, NTLM, plus access control models such as MAC, DAC, ABAC, and RBAC.
- Examine risk management as it applies to security and technology. Summarize incident response and computer forensics.
- Discover cryptography and public key infrastructure (PKI).
- Explore exam-taking tips and techniques.

Prerequisites:

- There are no official prerequisites for this course. However, attendees are expected to have a basic knowledge of computers and computer networking. CompTIA does not require any pre-requisites, but they recommend a minimum of two years' experience in IT administration with a focus on security.

**Note – Live virtual training is a crash course intended to be part of a candidate's larger study & prep plan toward certification.*

Price: CAD 940 for the live virtual training course, which includes access to Pearson self-study materials (i.e. video training).

Schedule: November 12 and 13, 2019 (8 hours total, 4 hours each day)

Course times: 5 am – 9 am PST

About the Instructor:
David L. Prowse is an author, technologist, and technical trainer. He has penned a dozen books for Pearson Education, including the well-received CompTIA A+ Exam Cram and CompTIA Security+ Cert Guide. He also develops video content, including the *CompTIA A+ LiveLessons* video course. Over the past two decades he has taught CompTIA A+, Network+, and Security+ certification courses, both in the classroom and via the Internet. David has 20 years of experience in the IT field and loves to share that experience with his readers, watchers, and students. He runs the website www.davidlprowse.com in support of his books and videos.

Course Set-up:

- Attendees also need a reliable Internet connection and a web browser.
- There is no additional content needed in advance. Attendees will benefit by having access to a computer lab with multiple systems and networking gear, but this is not required for this training.

Course Outline:

Segment 1: Computer Systems Security **(60 minutes)**

- Course Introduction
- A brief introduction to security.
- Computer Systems Security
- Delivery mechanisms
- How to prevent and troubleshoot malware
- Implementing security applications
- Securing computer hardware and peripherals
- Securing mobile devices
    - Attendees will follow along with hands-on exercises.

Break – 10 minutes

Segment 2: OS Hardening, Virtualization, and Application Security **(60 minutes)**

- How to harden operating systems
- Virtualization technology
- Securing the browser
- Secure programming
    - Attendees will follow along with hands-on exercises.

Break – 10 minutes

Segment 3: Network Security **(60 minutes)**

- Network design elements
- Networking protocols and threats
- Network perimeter security
- Securing network media and devices
    - Attendees will follow along with hands-on exercises.

Break – 10 minutes

Segment 4: Physical Security, Authentication, and Access Control **(60 minutes)**

- Introduction to physical security
- Authentication models
- Access control models
- Rights, permissions, and policies
- Attendees will follow along with hands-on exercises.

Break – 10 minutes

Segment 5: Vulnerability/Risk Assessment, Monitoring, and Auditing **(60 minutes)**

- Conducting Risk Assessments
- Assessing Vulnerability with Security Tools
- Monitoring methodologies
- Using tools to monitor systems and networks
- Conducting audits
    - Attendees will follow along with hands-on exercises.

Break – 10 minutes

Segment 6: Encryption and PKI **(60 minutes)**

- Cryptography concepts
- Encryption algorithms
- Hashing basics
- Public key infrastructure
- Security Protocols
    - Attendees will follow along with hands-on exercises.

Break – 10 minutes

Segment 7: Redundancy, Disaster Recovery, and People (60 minutes)

- Redundancy planning
- Disaster recovery planning and procedures
- Social engineering methods and prevention
- User education
- Facilities security
    - Attendees will follow along with hands-on exercises.

Break – 10 minutes

Segment 8: Policies and Procedures and Exam Preparation **(60 minutes)**

- Legislative and organizational policies
- Incident response procedures
- IT security frameworks
- Exam taking tips and tricks
- Sample questions
- Q & A