

# Course overview

CompTIA Security+ Certification Bootcamp (H1L15s)



Prepare for and take the Security+ certification exam. CompTIA's Security+ is the premier vendor-neutral security certification, and it demonstrates your knowledge of security concepts, tools, and procedures for reacting to security incidents. It also confirms your skill in anticipating security risks and guarding against them. Our Security+ Certification Boot Camp prepares you for the Security+ certification exam based on the 2011 objectives (Exam SYO-301), and it is included in the approved list of certifications to meet DoD Directive 8570.1 requirements.

Notice: Some contents may vary according to the geographical region.

## Audience

Candidates for the Security+ certification (SYO-301)

## Prerequisites

- CompTIA A+ certification
- CompTIA Network+ certification
- Or Equivalent Experience

## Why education services from HP?

- More than 80 training locations worldwide
- Experienced and best-in-the-field HP instructors
- Online instructor-led and self-paced training at <http://www.hp.com/learn>
- Comprehensive student materials
- State-of-the-art classroom facilities
- Focus on job-specific skills

**Course title:** CompTIA Security+ Certification Bootcamp

**HP product number:** H1L15s

**Category/Subcategory:** Security

**Course length:** 5 days

**Level:** Intermediate

**Delivery language:** English \*

**To order:** You can order this course online at <http://www.hp.com/learn>. At the site, select a country, then choose "registration" or "Book a course" and fill out the online registration form.

- Customized on-site delivery

## Detailed course outline

### 1. Mitigating Threats

- System maintenance
- Application Security
- Physical security
- Malware
- Social engineering

### 2. Cryptography

- Symmetric cryptography
- Public key cryptography

### 3. Authentication

- Authentication factors and requirements
- Authentication systems
- Authentication system vulnerabilities

### 4. User- and Role-Based Security

- Baseline security policies
- Resource access

### 5. Peripheral Security

- File and disk encryption
- Peripheral and component security
- Mobile device security

### 6. Public Key Infrastructure

- Public key cryptography
- Implementing public key infrastructure (PKI)
- Web server security with PKI

### 7. Application and Messaging Security

- Application security
- E-mail security
- Social networking and messaging

### 8. Ports and Protocols

- TCP/IP basics
- Protocol-based attacks

### 9. Network Security

- Network devices
- Secure network topologies
- Secure networking
- Virtualization and cloud computing

### 10. Wireless Security

- Wireless network security
- Mobile device security

### 11. Remote Access Security

- Remote access
- Virtual private networks

### 12. Vulnerability Testing

- Risk and vulnerability assessment
- Auditing and logging
- Intrusion detection and prevention systems
- Incident response

### 13. Organizational Security

- Organizational policies
- Education and training
- Disposal and destruction

### 14. Business Continuity

- Redundancy planning
- Disaster recovery
- Environmental controls

### 15. Certification Exam (Optional)

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

\* Localized versions may be available.

To locate country contact information and to learn more about education services, please visit our worldwide web site at <http://www.hp.com/learn>.

