CompTIA Security+

Course code: CTSEC

This unique five-day course serves as essential preparation for the globally recognized CompTIA Security+ SY0-701 certification exam, which has become the industry standard for IT security certification. Participants will gain a comprehensive overview of IT security solutions and will have the opportunity to practice implementing various security measures. Given the leading role of security in all corporate IT environments and the long-standing tradition of this certification exam, the CompTIA Security+ course is undoubtedly a significant advantage for IT professionals across all positions.

Who is the course for

The course is intended for advanced computer users and entry-level security administrators.

What you will learn

- Understand the fundamental concepts of identifying and addressing security risks
- Understand the fundamental concepts of cryptography and how to apply them correctly – including symmetric keys and certificates
- Gain an overview of the most vulnerable parts of TCP/IP network infrastructure and their solutions
- Understand the principles of protecting email communication, VPN remote connections, wireless networks, and other communication methods
- Understand the principles of identity authentication
- Learn how to configure user groups, their permissions, and access rights
- Implement security measures and updates
- Understand the basic concepts of security policies, from ensuring physical security to maintaining business continuity
- Create security documentation and Security Incident Handling

Prerequisite knowledge

Participants should have knowledge equivalent to the CompTIA A+ and Network+ certifications or possess practical experience in network and Microsoft operating system administration. They should also have strong experience in network configuration.

Teaching methods

Expert-led instruction with practical demonstrations and hands-on exercises on virtual machines.

Course materials

CompTIA study materials

Training participants will receive access to study materials for a period of 12 months, including access to a virtual environment where they can repeatedly go through the individual labs.

Course outline

1. Fundamentals of security
   - Information security lifecycle
   - Basics of security policies
   - Authentication methods
   - Fundamentals of cryptography
2. Security threats and vulnerabilities
   - Social engineering
   - Physical access threats
   - Network environment threats
   - Risks and vulnerabilities of wireless networks

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Risks from poorly programmed applications

3. Network security
   - Overview of network devices from a security perspective
   - Network security concept
   - Demonstrations of network attacks
   - Securing regular network traffic
   - Securing wireless network infrastructure
4. Application, data, and component security
   - Basic rules for securing workstations
   - Basic rules for securing servers
   - Data protection
   - Mobile device security
   - Application security options
5. Identity and access management
   - Types of authentication
   - Smart cards and tokens
   - Group strategies
   - Access management using ACL
   - RADIUS server and 802.1x
   - VLAN Management
   - VPN access management
   - WPA1/2 Enterprise
6. PKI and certificate management
   - PKI concept
   - Certificate usage options
   - Installation of an enterprise certification authority and template management
   - Backup and recovery of the certification authority
   - Automatic vs. manual certificate issuance
   - Management and backup of private keys
7. Security monitoring
   - OS auditing
   - Network auditing
   - IDS/IPS
   - Honeypots
   - Antivirus systems
8. Ensuring availability, business continuity, and incident response
   - Basic concepts of business continuity
   - SLA
   - High availability
   - Backup and recovery
   - Actions to take in case of a security breach

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk