Systems & Network Training

Security+

A 5 day Hands on training course

Save on expenses. This course is also available on your premises.

Description

A hands on course aimed at getting delegates successfully through the CompTia Security+ examination.

Key outcomes

By the end of the course delegates will be able to:

- ✔ Explain general security concepts.
- ✔ Describe the security concepts in communications.
- ✔ Describe how to secure an infrastructure.
- ✔ Recognise the role of cryptography.
- ✔ Describe operational/organisational security.

Training Approach

This structured course uses Instructor Led Training to provide the best possible learning experience. Small class sizes ensure students benefit from our engaging and interactive style of teaching with delegates encouraged to ask questions throughout the course. Quizzes follow each major section allowing checking of learning. Hands on sessions are used throughout to allow delegates to consolidate their new skills.

Details

Who will benefit?
Those wishing to pass the Security+ exam.

Prerequisites
TCP/IP Foundation for engineers

Duration: 5 days

Customer rating ★★★★½

Generic Training	Small Class Sizes	Hands On Training	Our Courseware	Customise Your Course
Generic training compliments product specific courses covering the complete picture of all relevant devices including the protocols "on the wire".	We limit our maximum class size to 8 delegates; often we have less than this. This ensures optimal interactivity between delegates and instructor.	The majority of our courses use hands on sessions to reinforce the theory.	We write our own courses; courseware does not just consist of slides and our slides are diagrams not bullet point text.	Please contact us if you would like a course to be customised to meet your specific requirements. Have the course your way.
"*Friendly environment with expert teaching that teaches the why before the how.*" G.C. Fasthosts	*"Excellent course. The small class size was a great benefit..."* M.B. IBM	*"Not many courses have practice added to it. Normally just the theoretical stuff is covered."* J.W. Vodafone	*"Comprehensive materials that made the course easy to follow and will be used as a reference point."* V.B. Rockwell Collins	*"I was very impressed by the combination of practical and theory. Very informative. Friendly approachable environment, lots of hands on."* S.R. Qinetiq

Security+

Course Content

General security concepts

Non-essential services and protocols. Access control: MAC, DAC, RBAC. Security attacks: DOS, DDOS, back doors, spoofing, man in the middle, replay, hijacking, weak keys, social engineering, mathematical, password guessing, brute force, dictionary, software exploitation. Authentication: Kerberos, CHAP, certificates, usernames/ passwords, tokens, biometrics. Malicious code: Viruses, trojan horses, logic bombs, worms. Auditing, logging, scanning.

Communication security

Remote access: 802.1x, VPNs, L2TP, PPTP, IPsec, RADIUS, TACACS, SSH. Email: S/MIME, PGP, spam, hoaxes. Internet: SSL, TLS, HTTPS, IM, packet sniffing, privacy, Javascript, ActiveX, buffer overflows, cookies, signed applets, CGI, SMTP relay. LDAP. sftp, anon ftp, file sharing, sniffing, 8.3 names. Wireless: WTLS, 802.11, 802.11x, WEP/WAP.

Infrastructure security

Firewalls, routers, switches, wireless, modems, RAS, PBX, VPN, IDS, networking monitoring, workstations, servers, mobile devices. Media security: Coax, UTP, STP, fibre. Removable media. Topologies: Security zones, DMZ, Intranet, Extranet, VLANs, NAT, Tunnelling. IDS: Active/ passive, network/host based, honey pots, incident response. Security baselines: Hardening OS/NOS, networks and applications.

Cryptography basics

Integrity, confidentiality, access control, authentication, non-repudiation. Standards and protocols. Hashing, symmetric, asymmetric. PKI: Certificates, policies, practice statements, revocation, trust models. Key management and certificate lifecycles. Storage: h/w, s/w, private key protection. Escrow, expiration, revocation, suspension, recovery, destruction, key usage.

Operational/Organisation security

Physical security: Access control, social engineering, environment. Disaster recovery: Backups, secure disaster recovery plans. Business continuity: Utilities, high availability, backups. Security policies: AU, due care, privacy, separation of duties, need to know, password management, SLAs, disposal, destruction, HR policies. Incident response policy. Privilege management: Users, groups, roles, single sign on, centralised/decentralised. Auditing. Forensics: Chain of custody, preserving and collecting evidence. Identifying risks: Assets, risks, threats, vulnerabilities. Role of education/training. Security documentation.

What our customers say

"Absolutely brilliant, very knowledgeable and helpful trainer would recommend to teach anyone. Kept me interested 100% of the time which is very impressive as this does not happen often, if at all!"

O. B. Network Rail

"The best technical course I've been on!."

L. W. Fujitsu Telecoms Europe

"Very well thought out and structured course. Would recommend 100%. Lots of equipment, good quality."

A.R. Unipart

"Course content is interesting. Relevant to current systems and presented well."

S.S-T. Arqiva