*Course **2011** Overview*

Endpoint Security and Network Access Control - 4 Days

You Will Learn How To

- • Enforce security policies to protect sensitive data from internal and external threats
- • Deploy Network Access Control to prevent malware contamination
- • Implement Data Loss Prevention (DLP) through host-based IDS/IPS and endpoint encryption
- • Regulate USB devices and optimise anti-malware
-

Who Should Attend

Security professionals seeking to enforce security policies for the protection of sensitive data and assets from internal and external threats. Knowledge at the level of Course 468, "System and Network Security Introduction," is assumed.

Hands-On Experience Includes:

- • Implementing port security
- • Deploying agent software to manage endpoints
- • Assigning endpoints dynamically to VLANs
- • Enforcing anti-malware policies
- • Controlling peripheral device access
- • Requiring encryption on attached network devices

*Course **2011** Outline*

Endpoint Security and Network Access Control - 4 Days

Introduction to Endpoint Security

Internal defences vs. perimeter defences

- Defining a holistic security posture
- Assessing threats from client-side and internal attacks
- Shifting the paradigm from a fortress mentality

Establishing a secure internal architecture

- Instituting a risk-based access control policy
- Choosing guest access strategies
- Regulating, monitoring and controlling network traffic

Establishing VLANs to Isolate Traffic

Developing a VLAN strategy

- Deciding on the number and types of VLANs
- Configuring VLAN trunking
- Managing VLAN access centrally

Segregating and isolating traffic

- Restricting access with port security
- Setting up quarantine and guest VLANs
- Managing port security violations

Implementing Network Access Control (NAC)

Installing a NAC server

- Implementing and authenticating with EAP
- Leveraging VLAN infrastructure

Securing access with 802.1X

- Configuring authentication agents
- Deploying certificates and RADIUS servers
- Denying rogue devices

Establishing Policy Servers and Repositories

Implementing policy-based access control

- Configuring system health requirements
- Creating a Bring Your Own Devices (BYODs) policy

Managing patches and anti-malware updates

- Establishing software repositories
- Pushing OS and application patches to clients

Monitoring and enforcing endpoint security

- Checking system health against policy
- Validating pre-connect and post-connect profiles
- Quarantining and remediating noncompliant devices

Managing Confidentiality for Data at Rest

Establishing an encryption policy

- Handling mobile devices and removable media
- Integrating encryption with Data Loss Prevention (DLP)

Implementing encryption

- Leveraging PKI to generate corporate recovery keys
- Enforcing full and partial disk encryption for endpoints

Preventing and Detecting Data Exfiltration

Developing a data loss strategy

- Permitting required traffic and denying dangerous traffic
- Configuring enterprise host firewalls
- Regulating attached USB and portable devices

Monitoring and detecting data leakage

- Preventing covert tunnels within DNS and HTTP(S) traffic
- Preventing Personally Identifiable Information (PII) leaks
- Identifying attempts to steal data

Implementing Anti-Malware Defences

Deploying anti-malware

- Pushing defensive software to endpoints
- Establishing internal anti-malware signature update servers
- Managing mobile and remote users

Managing enterprise anti-malware configuration

- Configuring scanning policies
- Determining responses to infection alerts
- Securing anti-malware configurations

Deploying host-based IDS/IPS

- Monitoring host processes
- Deciding among deployment options

Reporting and Compliance Checking

Responding to and mitigating attacks

- Assessing incidence response strategies
- Developing mitigation and containment strategies

Demonstrating organisational compliance

- Generating reports for compliant and noncompliant systems
- Complying with government regulations
- Tracking policy effectiveness
- Producing policy violation reports