SETC Training Corporate Logo

IT Security Training: Essential Concepts (SECCOPM, 4 jours)

Description

The course Essential Concepts (IT Security Training) introduces the art and science of IT security. The training begins with an overview of IT security management and its various disciplines. The course then discusses threat types & the complete Plan, Detect, Respond and Protect lifecycle. The training includes the use of firewalls, anti-virus, information security policies, user management, network management & more. If you to create, publish, implement and maintain a corporate Information Security Policy, this is the course for you.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Essential Security Concepts

Understanding the Layers: Business, Information and Access Management

About Business Security Management

The Information Security Management Discipline

The Access Management Discipline

About ISM and Change Management

The Role of the Information Security Policy

Threats and Vulnerabilities

Understanding the Topology of the Organization

IT Assets: Topology and Threats

The Anatomy of an Attack

About Privilege Escalation

Common Attack Strategies

Understanding Network Communications: The Wired World

Understanding Network Communications: The Wireless World

Protecting Network Communications: Message Verification and Validation

Overview of Common Attack Strategies

Denial of Service Attacks

Eavesdropping, Spoofing and Sniffing

Trojan Horses and Viruses

Other Attack Strategies

Understanding Cryptography

About Message Validation and Verification

The Basics of Cryptography: Keys and Algorithms

Choosing Key Lengths and Cryptographic Algorithms

Understanding Message Digests and Associated Algorithms

Understanding Public-Private Key Encryption and RSA

Working with SSL and Certificates

About the Certificate Authority: Choice and Use

About the use of a Digital Signature

Other Algorithms of Interest: BlowFish, PGP and More

Creating and Implementing a Good Information Security Policy

- The Typical Contents of an Information Security Policy
- Communication the Policy
- Creating and Implementing a Password Policy
- About Password Strength and Expiration
- Protecting against Social Engineering Attacks
- About Encrypting Passwords
- Using One Time and Tokenized Passwords
- Understanding Multi-Factor Authentication: 2, 3, 4 and More

IP Networking and Security

- Understanding IPv4 and IPv6 Network Communications
- About IP and its Vulnerabilities
- Understanding the Logical and the Physical Topology of an IP Network
- Understanding the Overall Network: the LAN and the WAN
- Understanding and Protecting against MAC Based Attacks
- Understanding and Protecting against DNS, DHCP, DFS and WINS Attacks
- Understanding and Protecting against IIS Attacks

Protecting IT Assets

- The Tools of the Trade: Finding Vulnerabilities
- Planning for Security Policy Implementation
- Identifying Vulnerabilities in the Network and the Operating System
- Restricting the Network: Rules and Firewalls
- Restricting User Accounts: Locking Down Administrator and Service Accounts
- Restricting User Accounts: The Password Policy
- Restricting User Accounts: Creating Group Policy Objects
- Locking Down Applications
- Locking Down Local and Remote Files

Preventing Against Common OS Attacks

- Operating System Vulnerabilities
- Using Firewalls and Security Policies
- Making use of Cryptography and Protection Services
- Dealing with Legacy Applications
- Dealing with Java and .NET Applications
- Preventing against Buffer Overflows
- Preventing against Denial of Service Attacks
- Making use of Event Logs
- Making use of Network Sniffers

A Complete Security Lab