SETC Training Corporate Logo

IT Security Training: Cybersecurity Essentials (CYSECE, 4 jours)

Description

The course Cybersecurity Essentials (IT Security) is a full lifecycle exploration of corporate IT Security. The training starts with a review of key networking concepts including IP addressing, switches, routers, VLANs, VOIP and concludes with a comprehensive study of cybersecurity concepts such as information assurance, cryptography, authentication and legal and regulatory considerations. The course then leverages theses foundation concepts to explore the practical aspects of securing routers, switches and computers that run Windows and Linux. The training also covers intrusion detection systems (IDS) and essential policies and procedures that support IT security in an organization. The course course concludes with a detailed study of hacker attacks, including attack methods, the attack vector, incident handling and mitigation techniques.

Tarifs

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

Plan de cours

Network Fundamentals

- The OSI Reference Model and Packet Structure
- Essential IP Concepts: IP Addresses and Subnets
- Obtaining an IP Address: Static and Dynamic Addressing
- Essential IP Concepts: Transport Protocols (TCP and UDP)
- IP Behaviour: Understanding Sockets, Ports and Application Protocols
- Understanding Routers and Layer 3 Switches
- Working with and Understanding VLANs
- Exploring VOIP Technologies

IT Security: Essential Concepts

- Information Assurance Foundations
- Cryptography and Secure Communications
- Program Security: Flaws and Defenses
- Operating System Security
- Identification and Authentication
- Trusted Operating Systems and Database Management Systems
- Network Security: Threats, Controls and Technologies
- Management of Security
- Legal, privacy and ethical issues

Implementing Router Security

- Firewalls: Roles and Concepts
- Cisco IOS: The Role of Router Filters, QoS and NAT
- Cisco IOS: Implementing Classes and Class Maps
- Cisco IOS: Implementing ACLs
- Cisco IOS: Implementing Policies

Securing the Computer: Windows

- Exploring NIST Cybersecurity Guidance
- Creating an Information Security Policy
- Creating Users and Managing Permissions on Windows
- Enforcing Password Complexity and Password Aging

Managing Domain Administrators and the Administrator Account
Managing Permissions: Windows File System and Share Based Security
Creating Group Policy and Enforcing Domain Security
Securing the SAM Database

Securing the Computer: Linux

Creating Users and Managing Permissions on Linux
Using PAM Modules to Enforce Password Complexity and Age Requirements
Managing root Access
Limiting Remote Logins
Securing SSH
Managing Permissions: Linux File System and Share Based Security
Securing Key Security Files
Implementing SELinux (Optional)

Implementing Computer Security

Understanding Computer Vulnerabilities
Implementing Logging and Audit on a Computer
Disabling Vulnerable Hardware
Disabling Non-Essential Services
Designing and Implementing a Software Update Strategy
Validating the Integrity of an Update

Intrusion Detection

The role of Intrusion Detection vs Authentication and Authorization
What Intrusion Detection Can and Cannot Provide
The Types of Intrusion Detection: NIDS, NNIDS and HIDS
Where IDSs Should be Positioned
The Critical Role of Processes

Implementing an IDS

Overview of the Security Onion
Implementing Alerts
Working with Asset Data
Packet Captures and Full Content Data
Capturing and Working with Host Data
Capturing and Working with Session Data
Capturing and Working with Transaction Data
Implementation Case Study: Web Service Intrusion Detection

Policies and Procedures

Overview of Key Processes
Exploring Information Security Management
Exploring Business Continuity Management
The Risk Management Process from A to Z
Risk Identification: Creating the Risk Register
Risk Evaluation: Determining Probability and Impact
Performing SPOA Analysis and Business Impact Analysis
Risk Management: Planning for Mitigation
Risk Audits: Principles and Application
Writing a Communication Plan
Updating the IT Service Continuity Plan and the Business Continuity Plan
Designing Effective Incident Management
Providing Problem Management
The Role of Change Management and Emergency Change Management

The Importance of Service Asset Configuration Management
Exploring Methods of Attack
Understanding the Hacker's Mindset
Exploring Methods of Attack
The top 10 Security Vulnerabilities
Exploring Session Highjacking
Exploring Man in the Middle
Exploring SQL Injection
Exploring XSS
Exploring Sensitive Data Exposure
Exploring Broken Authentication
Exploring WIFI Cracks and Security Protocols
A Note on Ransomware
Where Denial of Service (DOS) fits in
Advanced Persistent Threat Management Techniques
Other Useful Concepts
Offensive and Defensive Information Warfare
Implementing Honeypots
Implementing OS and Software Service Packs
Preventing Unauthorized Devices
Providing User Education
Ensuring Regular Security Testing
Using Appropriate Cryptographic Algorithms
Exploring Stenography and Known File Formats
The Vector of Attack
The Target Scoping Stage
The Information Gathering Stage
About Target Discovery
Enumerating the Target
Vulnerability Mapping
Social Engineering
Target Exploitation
Privilege Escalation
Putting it all Together
Incident Handling
Practice makes Perfect: Training Personnel to React to an Attack Situation
How to know when you are under attack
Before you begin: Identifying the Root Cause
Identifying and Executing the Response
Limiting the Scope of the Damage
Reviewing Logs and Identifying Compromised Systems
Communicating with Affected Individuals
Preventing Future Attacks
Performing a Post-Mortem