Microsoft® Windows® Security

Objetivos Gerais

Este curso é dirigido a todos os profissionais envolvidos na gestão, implementação e manutenção da Segurança dos Sistemas Windows.

Objetivos Específicos:

No final do curso os formandos ficaram aptos:

- A dominar o básico de segurança em um ambiente Microsoft;
- Dominar os objetivos da certificação de fundamentos de segurança do Microsoft tecnologia Associate (MTA);
- Compreender as camadas de segurança;
- Entender a segurança do sistema operacional;
- Entender a segurança da rede;
- Entender o software de segurança;
- Dominar todos os objetivos do Microsoft Technology Associate Security Fundamentals exam (exam 98-367).

Destinatários:

A todos os profissionais que necessitem dos fundamentos da segurança num ambiente Microsoft. O objetivo é fornecer uma cobertura rápida e focada dos Skills fundamentais de segurança.

Carga Horária: 40 horas

CONTEÚDO:

Módulo 1 – Understanding Core Security Principles

1.1 Understanding Risk

1.2 Exploring the Security Triad

1.3 Implementing a Defense-in-Depth Security Strategy

1.4 Enforcing the Principle of Least Privilege

1.5 Hardening a Server

Módulo 2 – Understanding Malware and Social Engineering

2.1 Comparing Malware
2.2 Protecting Against Malware
2.3 Thwarting Social-Engineering Attacks
2.4 Protecting Email

Módulo 3- Understanding User Authentication

3.1 Comparing the Three Factors of Authentication
3.2 Using Passwords for Authentication
3.3 Using Smart Cards and Token Devices for Authentication
3.4 Using Biometrics for Authentication
3.5 Starting Applications with Run As Administrator
3.6 Preventing Time Skew with Kerberos
3.7 Identifying RADIUS Capabilities
3.8 Identifying Unsecure Authentication Protocols

Módulo 4- Securing Access with Permissions

4.1 Comparing NTFS Permissions
4.2 Exploring Share Permissions
4.3 Identifying Active Directory Permissions
4.4 Assigning Registry Permissions

Módulo 5 - Using Audit Policies and Network Auditing

5.1 Exploring Audit Policies
5.2 Enabling Auditing
5.3 Viewing Audit Information
5.4 Managing Security Logs
5.5 Auditing a Network with MBSA

Módulo 6 - Protecting Clients and Servers

6.1 Understanding User Account Control
6.2 Keeping Systems Updated
6.3 Protecting Clients
6.4 Protecting Servers
6.5 Exploring DNS Security Issues

Módulo 7 - Protecting a Network

7.1 Identifying Common Attack Methods
7.2 Exploring Firewalls
7.3Exploring Network Access Protection
7.4 Identifying Protocol Security Methods

Módulo 8 - Understanding Wireless Security

8.1 Comparing Wireless Devices

8.2 Comparing Wireless Security Methods

8.3 Configuring Wireless Routers

8.4 Configuring Windows 7 for Wireless

Módulo 9 - Understanding Physical Security

9.1 Comparing Site Security and Computer Security

9.2 Using Group Policy to Enhance Computer Security

9.3 Exploring Mobile Device Security

Módulo 10 - Enforcing Confidentiality with Encryption

10.1 Comparing Encryption Methods

10.2 Securing Email

10.3 Understanding EFS

10.4 Exploring BitLocker Drive Encryption

Módulo 11 Understanding Certificates and a PKI

11.1 Understanding a Certificate

11.2 Exploring the Components of a PKI

Módulo 12 - Understanding Internet Explorer Security

12.1 Exploring Browser Settings

12.2 Comparing Security Zones

12.3 Using IE Tools to Identify Malicious Websites