

M98367A - Microsoft Security Fundamentals

This course is for anyone interested enhancing their fundamental understanding of security and computer networking related skills. You might already be working in IT or Cyber Security or completely new to the industry.

Whilst knowledge of Security and Networking would be beneficial, it is not essential. This is an entry-level course so can be taken by anyone regardless of prior experience or skill level!

Course Outline

Duration: 3 days

Module 1: Understanding Security Layers

- Introducing Core Security Principles
- Understanding Physical Security as the First Line of Defence
- Performing Threat Modelling

Module 2: Understanding Authentication, Authorization and Accounting

- Starting Security with Authentication
- Introducing Directory Services with Active Directory
- Comparing Rights and Permissions
- Understanding NTFS
- Sharing Drives and Folders
- Introducing the Registry
- Using Encryption to Protect Data
- Understanding IPsec
- Introducing Smart Cards
- Configuring Biometrics, Microsoft Hello
- Using Auditing to Complete the Security Picture

Module 3: Understanding Security Policies

- Using Password Policies to Enhance Security
- Protecting Domain User Account Passwords

Module 4: Understanding Network Security

- Using Dedicated Firewalls to Protect a Network
- Using Isolation to Protect the Network
- Protecting Data with Protocol Security
- Understanding Denial-of-Service (DoS) Attacks
- Securing the Wireless Network

Module 5: Protecting the Server and Client

- Protecting the Client Computer

- Managing Client Security Using Microsoft Defender
- Protecting Your Email
- Securing & Configuring Microsoft Edge
- Protecting Your Server
- Using Security Baselines
- Locking Down Devices to Run Only Trusted Applications
- Managing Microsoft Store Apps