# Introduction

The **Microsoft Securing Windows Server 2016** course is designed to provide IT professionals with the essential knowledge and skills required to secure and protect Windows Server 2016 environments. This comprehensive training focuses on the implementation of robust security measures, with the understanding that network breaches are already prevalent. Participants will learn how to safeguard their IT infrastructure by configuring administrative credentials, mitigating security threats, employing advanced threat analysis features, and applying encryption techniques to control data access.

The course also delves into advanced security concepts such as **Dynamic Access Control (DAC)** and securing network traffic. By the end of the training, participants will be equipped to apply best practices to ensure the security of their **Windows Server 2016** environments.

# Targeted Groups

This course is designed for:

- **IT Professionals** responsible for administering and securing **Windows Server 2016** networks.
- Professionals working in **domain-based environments**, with managed Internet access and **cloud services**.
- Individuals seeking to advance their security management skills within Windows Server environments.

# Course Objectives

Upon completing this course, participants will be able to:

- Implement **Windows Server 2016 security best practices**.
- **Restrict administrator rights** using **Just Enough Administration (JEA)**.
- Secure **privileged access** and effectively mitigate malware and security threats.
- Utilize **advanced auditing and log analytics** to detect and analyze security activity.
- Deploy and configure **Advanced Threat Analytics (ATA)** and **Microsoft Operations Management Suite (OMS)** for enhanced security.
- Configure **Guarded Fabric VMs** and apply **Security Compliance Toolkit (SCT)**.
- Protect data using **encryption**, **BitLocker**, and **DAC** for data access restrictions.
- Secure **file services**, network traffic, and DNS configurations.

# Targeted Competencies

By the end of the course, participants will develop expertise in:

- **Implementing User Rights**, **Security Options**, and **Group-Managed Service Accounts**.

- Limiting **Administrator Privileges** with **JEA**.
- Securing applications using **Windows Defender** and **AppLocker**.
- **Configuring Advanced Auditing** and utilizing **PowerShell** for logging.
- Protecting data through **encryption** and **BitLocker**.
- Implementing **DAC** to ensure secure data access.
- Securing **DNS** and configuring **firewalls** to protect network traffic.

# Course Content

## Unit 1: Attacks, Breach Detection, and Sysinternals Tools

- Understanding cyber-attacks and how to identify security breaches.
- Utilizing **Sysinternals tools** for system activity analysis.

## Unit 2: Protecting Credentials and Privileged Access

- Securing **User Rights**, **Computer**, and **Service Accounts**.
- Protecting credentials and deploying **Privileged Access Workstations** and **jump servers**.
- Integrating **Local Administrator Password Solutions (LAPS)**.

## Unit 3: Limiting Administrator Rights with Just Enough Administration (JEA)

- Understanding and implementing **JEA**.
- Procedures for verifying and deploying **JEA**.

## Unit 4: Privileged Access Management and Administrative Forest

- Exploring **Enhanced Security Administrative Environment (ESAE)** forests.
- Introduction to **Microsoft Identity Manager (MIM)**, **Just In Time (JIT)** administration, and **Privileged Access Management (PAM)**.

## Unit 5: Mitigating Malware and Threats

- Configuring and managing **Windows Defender**.
- Using **Device Guard** and **Software Restriction** policies to mitigate threats.

## Unit 6: Analyzing Activity with Advanced Auditing and Log Analytics

- Fundamentals and configuration of **Advanced Auditing**.
- Using **Windows PowerShell** for auditing and logging activities.

## Unit 7: Deploying and Configuring Advanced Threat Analytics (ATA) and Operations Management Suite (OMS)

- Steps to deploy and configure **ATA**.
- Integration with **Microsoft Operations Management Suite** and the **Azure Security Center**.

### Unit 8: Securing Virtualization Infrastructure

- Provisioning **Shielded VMs** and utilizing **Guarded Fabric** for secure virtualization.

### Unit 9: Securing Application Development and Server-Workload Infrastructure

- Implementing the **Security Compliance Manager** for application and server security.
- The role of **Containers** in securing applications.

### Unit 10: Planning and Protecting Data

- Formulating and implementing **encryption strategies**.
- Utilizing **BitLocker** and **Azure Information Protection** to safeguard data.

### Unit 11: Optimizing and Securing File Services

- Using **File Server Resource Manager (FSRM)** to manage files and security.
- Implementing **DAC** for secure access to files and data.

### Unit 12: Securing Network Traffic with Firewalls and Encryption

- Mastering **Windows Firewall** configurations and **IPsec** to protect network traffic.
- Implementing **Datacenter Firewall** for advanced protection.

### Unit 13: Securing Network Traffic

- **DNSSEC** and advanced DNS security configurations.
- Using **Microsoft Message Analyzer** to analyze and secure network traffic.
- Ensuring server and **SMB traffic** security.

## Conclusion

The **Microsoft Securing Windows Server 2016** course provides participants with essential tools and techniques to effectively secure their Windows Server 2016 environment. This comprehensive training will help professionals mitigate security threats, protect data, and ensure the ongoing security and integrity of their server infrastructure.