MS-500T00 Microsoft 365 Security Administrator

Summary

Length: 32 hours Level: Experienced

In this course you will learn how to secure user access to your organization's resources. The course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to setup and use Azure AD Connect, and introduces you to conditional access in Microsoft 365. You will learn about threat protection technologies that help protect your Microsoft 365 environment. Specifically, you will learn about threat vectors and Microsoft's security solutions to mitigate threats. You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and threat management. In the course you will learn about information protection technologies that help secure your Microsoft 365 environment. The c

Learning Objectives

Administer user and group access in Microsoft 365.
Explain and manage Azure Identity Protection.
Plan and implement Azure AD Connect.
Manage synchronized user identities.
Explain and use conditional access.
Describe cyber-attack threat vectors.
Explain security solutions for Microsoft 365.
Use Microsoft Secure Score to evaluate and improve your security posture.
Configure various advanced threat protection services for Microsoft 365.
Plan for and deploy secure mobile devices.
Implement information rights management.
Secure messages in Office 365.
Configure Data Loss Prevention policies.
Deploy and manage Cloud App Security.
Implement Windows information protection for devices.
Plan and deploy a data archiving and retention system.
Create and manage an eDiscovery investigation.
Manage GDPR data subject requests.
Explain and use sensitivity labels.

Course Outline

1. User and Group Management

   Identity and Access Management concepts
   The Zero Trust model
   Plan your identity and authentication solution
   User accounts and roles
   Password Management

2. Identity Synchronization and Protection

   Plan directory synchronization
   Configure and manage synchronized identities
   Azure AD Identity Protection

3. Identity and Access Management

   Application Management
   Identity Governance

Manage device access
Role Based Access Control (RBAC)
Solutions for external access
Privileged Identity Management

4. Security in Microsoft 365

Threat vectors and data breaches
Security strategy and principles
Microsoft security solutions
Secure Score

5. Threat Protection

Exchange Online Protection (EOP)
Microsoft Defender for Office 365
Manage Safe Attachments
Manage Safe Links
Microsoft Defender for Identity

6. Threat Management

Security dashboard
Threat investigation and response
Azure Sentinel
Advanced Threat Analytics

7. Microsoft Cloud Application Security

Deploy Cloud Application Security
Use cloud application security information

8. Mobility

Mobile Application Management (MAM)
Mobile Device Management (MDM)
Deploy mobile device services
Enroll devices to Mobile Device Management

9. Information Protection and Governance

Information protection concepts
Governance and Records Management
Sensitivity labels
Archiving in Microsoft 365
Retention in Microsoft 365
Retention policies in the Microsoft 365 Compliance Center
Archiving and retention in Exchange
In-place records management in SharePoint

10. Rights Management and Encryption

Information Rights Management (IRM)
Secure Multipurpose Internet Mail Extension (S-MIME)
Office 365 Message Encryption

11. Data Loss Prevention

Data loss prevention fundamentals
Create a DLP policy
Customize a DLP policy

Create a DLP policy to protect documents
Policy tips

12. Compliance Management

    Compliance center

13. Insider Risk Management

    Insider Risk
    Privileged Access
    Information barriers
    Building ethical walls in Exchange Online

14. Discover and Respond

    Content Search
    Audit Log Investigations
    Advanced eDiscovery

Audience

The Microsoft 365 Security administrator collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and to ensures that the solutions comply with the policies and regulations of the organization. This role proactively secures Microsoft 365 enterprise environments. Responsibilities include responding to threats, implementing, managing and monitoring security and compliance solutions for the Microsoft 365 environment. They respond to incidents, investigations and enforcement of data governance. The Microsoft 365 Security administrator is familiar with Microsoft 365 workloads and hybrid environments. This role has strong skills and experience with identity protection, information protection, threat protection, security management and data governance.

Prerequisites

Learners should start this course already having the following skills: Basic conceptual understanding of Microsoft Azure. Experience with Windows 10 devices. Experience with Office 365. Basic understanding of authorization and authentication. Basic understanding of computer networks. Working knowledge of managing mobile devices.