Microsoft 365 Administrator Essentials (MS-102)

Modality: Virtual Classroom

Duration: 5 Days

If you enroll in this course at the listed price, you receive a Free Official Exam Voucher for the MS-102 Exam. This course does not include Exam Voucher if enrolled within the Master Subscription, however, you can request to purchase the Official Exam Voucher separately.

About this Course:

In Microsoft 365 tenant management, you learn how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscription options, component services, user accounts and licenses, security groups, and administrative roles. You then transition to configuring Microsoft 365, with a primary focus on configuring Office client connectivity. Finally, you explore how to manage user-driven client installations of Microsoft 365 Apps for enterprise deployments.

The course then transitions to an in-depth examination of Microsoft 365 identity synchronization, with a focus on Azure Active Directory Connect and Connect Cloud Sync. You learn how to plan for and implement each of these directory synchronization options, how to manage synchronized identities, and how to implement password management in Microsoft 365 using multifactor authentication and self-service password management.

In Microsoft 365 security management, you begin examining the common types of threat vectors and data breaches facing organizations today. You then learn how Microsoft 365's security solutions address each of these threats. You are introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Safe Attachments, and Safe Links. Finally, you are introduced to the various reports that monitor an organization's security health. You then transition from security services to threat intelligence; specifically, using Microsoft 365 Defender, Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoint.

Once you have this understanding of Microsoft 365's security suite, you then examine the key components of Microsoft 365 compliance management. This begins with an overview of all key aspects of data governance, including data archiving and retention, Microsoft Purview message encryption, and data loss prevention (DLP). You then delve deeper into archiving and retention, paying particular attention to Microsoft Purview insider risk management, information barriers, and DLP policies. You then examine how to implement these compliance features by using data classification and sensitivity labels.

Course Objectives:

- Configure your company's organization profile, which is essential for setting up for your company's tenant.
- Maintain minimum subscription requirements for your company.
- Manage your services and add-ins by assigning more licenses, purchasing more storage, and so on.

- Create a checklist that enables you to confirm your Microsoft 365 tenant meets your business needs.
- Identify which user identity model best suited for your organization.
- Create user accounts from both the Microsoft 365 admin center and Windows PowerShell.
- Manage user accounts and licenses in Microsoft 365.
- Recover deleted user accounts in Microsoft 365.
- Perform bulk user maintenance in Azure Active Directory.
- Create and manage mail contacts from both the new Exchange admin center and Exchange Online PowerShell.
- Describe the various types of groups available in Microsoft 365.
- Create and manage groups using the Microsoft 365 admin center and Windows PowerShell.
- Create and manage groups in Exchange Online and SharePoint Online.
- Identify the factors that must be considered when adding a custom domain to Microsoft 365.
- Plan the DNS zones used in a custom domain.
- Plan the DNS record requirements for a custom domain.
- Add a custom domain to your Microsoft 365 deployment.
- Describe how Outlook uses Autodiscover to connect an Outlook client to Exchange Online.
- Identify the DNS records needed for Outlook and other Office-related clients to automatically locate the services in Microsoft 365 using the Autodiscover process.
- Describe the connectivity protocols that enable Outlook to connect to Microsoft 365.
- Identify the tools that can help you troubleshoot connectivity issues in Microsoft 365 deployments.
- Describe the Azure RBAC permission model used in Microsoft 365.
- Describe the most common Microsoft 365 admin roles.
- Identify the key tasks assigned to the common Microsoft 365 admin roles.
- Delegate admin roles to partners.
- Manage permissions using administrative units in Azure Active Directory.
- Elevate privileges to access admin centers by using Azure AD Privileged Identity Management.
- Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center.
- Develop an incident response plan to deal with incidents that may occur with your Microsoft 365 service.
- Request assistance from Microsoft to address technical, pre-sales, billing, and subscription support issues.
- Describe the Microsoft 365 Apps for enterprise functionality.
- Configure the Readiness Toolkit.
- Plan a deployment strategy for Microsoft 365 Apps for enterprise.
- Complete a user-driven installation of Microsoft 365 Apps for enterprise.
- Deploy Microsoft 365 Apps for enterprise with Microsoft Endpoint Configuration Manager.
- Identify the mechanisms for managing centralized deployments of Microsoft 365 Apps for enterprise.
- Deploy Microsoft 365 Apps for enterprise with the Office Deployment Toolkit.
- Describe how to manage Microsoft 365 Apps for enterprise updates.
- Determine which update channel and application method applies for your organization.
- Identify how Microsoft Viva Insights can help improve collaboration behaviors in your organization.
- Discover the sources of data used in Microsoft Viva Insights.
- Explain the high-level insights available through Microsoft Viva Insights.
- Create custom analysis with Microsoft Viva Insights.
- Summarize tasks and considerations for setting up Microsoft Viva Insights and managing privacy.
- Describe the Microsoft 365 authentication and provisioning options
- Explain the two identity models in Microsoft 365 - cloud-only identity and hybrid identity

- Explain the three authentication methods in the hybrid identity model - Password hash synchronization, Pass-through authentication, and federated authentication
- Describe how Microsoft 365 commonly uses directory synchronization
- Identify the tasks necessary to configure your Azure Active Directory environment.
- Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD.
- Identify the features of Azure AD Connect sync and Azure AD Connect Cloud Sync.
- Choose which directory synchronization best fits your environment and business needs.
- Configure Azure AD Connect and Azure AD Connect Cloud Sync prerequisites
- Set up Azure AD Connect and Azure AD Connect Cloud Sync
- Monitor synchronization services using Azure AD Connect Health
- Ensure users synchronize efficiently
- Manage groups with directory synchronization
- Use Azure AD Connect Sync Security Groups to help maintain directory synchronization
- Configure object filters for directory synchronization
- Troubleshoot directory synchronization using various troubleshooting tasks and tools
- creating and configuring password policies
- configuring self-service password management
- configuring multifactor authentication
- implementing entitlement packages
- implementing conditional access policies
- Describe techniques hackers use to compromise user accounts through email
- Describe techniques hackers use to gain control over resources
- Describe techniques hackers use to compromise data
- Mitigate an account breach
- Prevent an elevation of privilege attack
- Prevent data exfiltration, data deletion, and data spillage
- Describe the Zero Trust approach to security in Microsoft 365
- Describe the principles and components of the Zero Trust security model
- Describe the five steps to implementing a Zero Trust security model in your organization
- Explain Microsoft's story and strategy around Zero Trust networking
- Identify the features of Microsoft Defender for Office 365 that enhance email security in a Microsoft 365 deployment
- Explain how Microsoft Defender for Identity identifies, detects, and investigates advanced threats, compromised identities, and malicious insider actions directed at your organization
- Explain how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats
- Describe how Microsoft 365 Threat Intelligence can be beneficial to your organization’s security officers and administrators
- Describe how Microsoft Cloud App Security enhances visibility and control over your Microsoft 365 tenant through three core areas
- Describe the benefits of Secure Score and what kind of services can be analyzed
- Describe how to collect data using the Secure Score API
- Describe how to use the tool to identify gaps between your current state and where you would like to be regarding security
- Identify actions that increase your security by mitigating risks
- Explain where to look to determine the threats each action mitigates and the impact it has on users
- Describe how Privileged Identity Management enables you to manage, control, and monitor access

to important resources in your organization
- Configure Privileged Identity Management for use in your organization
- Describe how Privileged Identity Management audit history enables you to see all the user assignments and activations within a given time period for all privileged roles
- Explain how Microsoft Identity Manager helps organizations manage the users, credentials, policies, and access within their organizations and hybrid environments
- Explain how Privileged Access Management provides granular access control over privileged admin tasks in Microsoft 365
- Describe Azure Identity Protection (AIP) and what kind of identities can be protected
- Enable the three default protection policies in AIP
- Identify the vulnerabilities and risk events detected by AIP
- Plan your investigation in protecting cloud-based identities
- Plan how to protect your Azure Active Directory environment from security breaches
- Describe how Exchange Online Protection analyzes email to provide anti-malware pipeline protection.
- List several mechanisms used by Exchange Online Protection to filter spam and malware.
- Describe other solutions administrators may implement to provide extra protection against phishing and spoofing.
- Describe how the Safe Attachments feature in Microsoft Defender for Office 365 blocks zero-day malware in email attachments and documents.
- Describe how the Safe Links feature in Microsoft Defender for Office 365 protects users from malicious URLs embedded in email and documents that point to malicious websites.
- Create outbound spam filtering policies.
- Unblock users who violated spam filtering policies so they can resume sending emails.
- Create and modify a Safe Attachments policy using Microsoft 365 Defender
- Create a Safe Attachments policy by using PowerShell
- Configure a Safe Attachments policy
- Describe how a transport rule can disable a Safe Attachments policy
- Describe the end-user experience when an email attachment is scanned and found to be malicious
- Create and modify a Safe Links policy using Microsoft 365 Defender
- Create a Safe Links policy using PowerShell
- Configure a Safe Links policy
- Describe how a transport rule can disable a Safe Links policy
- Describe the end-user experience when Safe Links identifies a link to a malicious website embedded in email, and a link to a malicious file hosted on a website
- Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
- Create alerts that can identify malicious or suspicious events.
- Understand how the Microsoft 365 Defender's Automated investigation and response process works.
- Describe how threat hunting enables security operators to identify cybersecurity threats.
- Describe how Advanced hunting in Microsoft 365 Defender proactively inspects events in your network to locate threat indicators and entities.
- Describe how Microsoft Defender for Cloud Apps provides improved visibility into network cloud activity and increases the protection of critical data across cloud applications.
- Explain how to deploy Microsoft Defender for Cloud Apps.
- Control your cloud apps with file policies.
- Manage and respond to alerts generated by those policies.

- Configure and troubleshoot Cloud Discovery.
- Describe how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats.
- Onboard supported devices to Microsoft Defender for Endpoint.
- Implement the Threat and Vulnerability Management module to effectively identify, assess, and remediate endpoint weaknesses.
- Configure device discovery to help find unmanaged devices connected to your corporate network.
- Lower your organization's threat and vulnerability exposure by remediating issues based on prioritized security recommendations.
- Describe the protection stack provided by Microsoft Defender for Office 365.
- Understand how Threat Explorer can be used to investigate threats and help to protect your tenant.
- Describe the Threat Tracker widgets and views that provide you with intelligence on different cybersecurity issues that might affect your company.
- Run realistic attack scenarios using Attack Simulator to help identify vulnerable users before a real attack impacts your organization.

Audience:

This course is designed for persons aspiring to the Microsoft 365 Administrator role and have completed at least one of the Microsoft 365 role-based administrator certification paths.

Prerequisites:

Before attending this course, students must have:

- Completed a role-based administrator course such as Messaging, Teamwork, Security, Compliance, or Collaboration.
- A proficient understanding of DNS and basic functional experience with Microsoft 365 services.
- A proficient understanding of general IT practices.
- A working knowledge of PowerShell.

Course Outline:

Module 1- Configure your Microsoft 365 experience

This module examines each of the tasks that an organization must complete to successfully configure its Microsoft 365 experience.

Learning Objectives:

- Configure your company’s organization profile, which is essential for setting up for your company’s tenant.

- Maintain minimum subscription requirements for your company.
- Manage your services and add-ins by assigning more licenses, purchasing more storage, and so on.
- Create a checklist that enables you to confirm your Microsoft 365 tenant meets your business needs.

Lessons:

- Introduction
- Configure your Microsoft 365 experience
- Manage your tenant subscriptions in Microsoft 365
- Integrate Microsoft 365 with customer engagement apps
- Complete your tenant configuration in Microsoft 365
- Knowledge check
- Summary

Module 2- Manage users, contacts, and licenses in Microsoft 365

This module provides instruction on how to create and manage user accounts, assign Microsoft 365 licenses to users, recover deleted user accounts, and create and manage mail contacts.

Learning Objectives:

- Identify which user identity model best suited for your organization.
- Create user accounts from both the Microsoft 365 admin center and Windows PowerShell.
- Manage user accounts and licenses in Microsoft 365.
- Recover deleted user accounts in Microsoft 365.
- Perform bulk user maintenance in Azure Active Directory.
- Create and manage mail contacts from both the new Exchange admin center and Exchange Online PowerShell.

Lessons:

- Introduction
- Determine the user identity model for your organization
- Create user accounts in Microsoft 365
- Manage user account settings in Microsoft 365
- Manage user licenses in Microsoft 365
- Recover deleted user accounts in Microsoft 365
- Perform bulk user maintenance in Azure Active Directory
- Create and manage guest users
- Create and manage contacts
- Summary

Module 3- Manage groups in Microsoft 365

This module provides instruction on how to create groups for distributing email to multiple users within Exchange Online. It also explains how to create groups to support collaboration in SharePoint

Online.

Learning Objectives:

- Describe the various types of groups available in Microsoft 365.
- Create and manage groups using the Microsoft 365 admin center and Windows PowerShell.
- Create and manage groups in Exchange Online and SharePoint Online.

Lessons:

- Introduction
- Examine groups in Microsoft 365
- Create and manage groups in Microsoft 365
- Create groups in Exchange Online and SharePoint Online
- Knowledge check
- Summary

Module 4- Add a custom domain in Microsoft 365

This module provides instruction on how to add a custom domain to your Microsoft 365 deployment. It also examines the DNS requirements that are necessary to support a new domain.

Learning Objectives:

- Identify the factors that must be considered when adding a custom domain to Microsoft 365.
- Plan the DNS zones used in a custom domain.
- Plan the DNS record requirements for a custom domain.
- Add a custom domain to your Microsoft 365 deployment.

Lessons:

- Introduction
- Plan a custom domain for your Microsoft 365 deployment
- Plan the DNS zones for a custom domain
- Plan the DNS record requirements for a custom domain
- Create a custom domain in Microsoft 365
- Knowledge check
- Summary

Module 5- Configure client connectivity to Microsoft 365

This module examines how clients connect to Microsoft 365. It also provides instruction on how to configure name resolution and Outlook clients, and how to troubleshoot client connectivity.

Learning Objectives:

- Describe how Outlook uses Autodiscover to connect an Outlook client to Exchange Online.
- Identify the DNS records needed for Outlook and other Office-related clients to automatically

locate the services in Microsoft 365 using the Autodiscover process.
- Describe the connectivity protocols that enable Outlook to connect to Microsoft 365.
- Identify the tools that can help you troubleshoot connectivity issues in Microsoft 365 deployments.

Lessons:

- Introduction
- Examine how automatic client configuration works
- Explore the DNS records required for client configuration
- Configure Outlook clients
- Troubleshoot client connectivity
- Knowledge check
- Summary

Module 6- Configure administrative roles in Microsoft 365

This module examines the key functionality that's available in the more commonly used Microsoft 365 admin roles. It also provides instruction on how to configure these roles.

Learning Objectives:

- Describe the Azure RBAC permission model used in Microsoft 365.
- Describe the most common Microsoft 365 admin roles.
- Identify the key tasks assigned to the common Microsoft 365 admin roles.
- Delegate admin roles to partners.
- Manage permissions using administrative units in Azure Active Directory.
- Elevate privileges to access admin centers by using Azure AD Privileged Identity Management.

Lessons:

- Introduction
- Explore the Microsoft 365 permission model
- Explore the Microsoft 365 admin roles
- Assign admin roles to users in Microsoft 365
- Delegate admin roles to partners
- Manage permissions using administrative units in Azure Active Directory
- Elevate privileges using Azure AD Privileged Identity Management
- Knowledge check
- Summary

Module 7- Manage tenant health and services in Microsoft 365

This module examines how to monitor your organization's transition to Microsoft 365 using Microsoft 365 tools. It also examines how to develop an incident response plan and request assistance from Microsoft.

Learning Objectives:

- Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center.
- Develop an incident response plan to deal with incidents that may occur with your Microsoft 365 service.
- Request assistance from Microsoft to address technical, pre-sales, billing, and subscription support issues.

Lessons:

- Introduction
- Monitor the health of your Microsoft 365 services
- Monitor tenant health using Microsoft 365 Adoption Score
- Monitor tenant health using Microsoft 365 usage analytics
- Develop an incident response plan
- Request assistance from Microsoft
- Knowledge check
- Summary

Module 8- Deploy Microsoft 365 Apps for enterprise

This module examines how to implement the Microsoft 365 Apps for enterprise productivity suite in both user-driven and centralized deployments.

Learning Objectives:

- Describe the Microsoft 365 Apps for enterprise functionality.
- Configure the Readiness Toolkit.
- Plan a deployment strategy for Microsoft 365 Apps for enterprise.
- Complete a user-driven installation of Microsoft 365 Apps for enterprise.
- Deploy Microsoft 365 Apps for enterprise with Microsoft Endpoint Configuration Manager.
- Identify the mechanisms for managing centralized deployments of Microsoft 365 Apps for enterprise.
- Deploy Microsoft 365 Apps for enterprise with the Office Deployment Toolkit.
- Describe how to manage Microsoft 365 Apps for enterprise updates.
- Determine which update channel and application method applies for your organization.

Lessons:

- Introduction
- Explore Microsoft 365 Apps for enterprise functionality
- Explore your app compatibility by using the Readiness Toolkit
- Complete a self-service installation of Microsoft 365 Apps for enterprise
- Deploy Microsoft 365 Apps for enterprise with Microsoft Endpoint Configuration Manager
- Deploy Microsoft 365 Apps for enterprise from the cloud
- Deploy Microsoft 365 Apps for enterprise from a local source
- Manage updates to Microsoft 365 Apps for enterprise

- Explore the update channels for Microsoft 365 Apps for enterprise
- Manage your cloud apps using the Microsoft 365 Apps admin center
- Knowledge check
- Summary

Module 9- Analyze your Microsoft 365 workplace data using Microsoft Viva Insights

This module examines the workplace analytical features of Microsoft Viva Insights, including how it works, and how it generates insights and improves collaboration within an organization.

Learning Objectives:

- Identify how Microsoft Viva Insights can help improve collaboration behaviors in your organization.
- Discover the sources of data used in Microsoft Viva Insights.
- Explain the high-level insights available through Microsoft Viva Insights.
- Create custom analysis with Microsoft Viva Insights.
- Summarize tasks and considerations for setting up Microsoft Viva Insights and managing privacy.

Lessons:

- Introduction
- Examine the analytical features of Microsoft Viva Insights
- Create custom analysis with Microsoft Viva Insights
- Configure Microsoft Viva Insights
- Examine Microsoft 365 data sources used in Microsoft Viva Insights
- Prepare organizational data in Microsoft Viva Insights
- Knowledge check
- Summary

Module 10- Explore identity synchronization

This module examines identity synchronization and explores the authentication and provisioning options that can be used, and the inner-workings of directory synchronization.

Learning Objectives:

- Describe the Microsoft 365 authentication and provisioning options
- Explain the two identity models in Microsoft 365 - cloud-only identity and hybrid identity
- Explain the three authentication methods in the hybrid identity model - Password hash synchronization, Pass-through authentication, and federated authentication
- Describe how Microsoft 365 commonly uses directory synchronization

Lessons:

- Introduction
- Examine authentication options in Microsoft 365

- Examine provisioning options in Microsoft 365
- Explore directory synchronization
- Explore Azure AD Connect
- Knowledge check
- Summary

Module 11- Prepare for identity synchronization to Microsoft 365

This module examines all the planning aspects that must be considered when implementing directory synchronization between on-premises Active Directory and Microsoft 365.

Learning Objectives:

- Identify the tasks necessary to configure your Azure Active Directory environment.
- Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD.
- Identify the features of Azure AD Connect sync and Azure AD Connect Cloud Sync.
- Choose which directory synchronization best fits your environment and business needs.

Lessons:

- Introduction
- Plan your Azure Active Directory deployment
- Prepare for directory synchronization
- Choose your directory synchronization tool
- Plan for directory synchronization using Azure AD Connect
- Plan for directory synchronization using Azure AD Connect Cloud Sync
- Knowledge check
- Summary

Module 12- Implement directory synchronization tools

This module examines the Azure AD Connect and Azure AD Connect Cloud Sync installation requirements, the options for installing and configuring the tools, and how to monitor synchronization services using Azure AD Connect Health.

Learning Objectives:

- Configure Azure AD Connect and Azure AD Connect Cloud Sync prerequisites
- Set up Azure AD Connect and Azure AD Connect Cloud Sync
- Monitor synchronization services using Azure AD Connect Health

Lessons:

- Introduction
- Configure Azure AD Connect prerequisites
- Configure Azure AD Connect
- Monitor synchronization services using Azure AD Connect Health

- Configure Azure AD Connect Cloud Sync prerequisites
- Configure Azure AD Connect Cloud Sync
- Knowledge check
- Summary

Module 13- Manage synchronized identities

This module examines how to manage user identities when Azure AD Connect is configured, how to manage users and groups in Microsoft 365 with Azure AD Connect, and how to maintain directory synchronization.

Learning Objectives:

- Ensure users synchronize efficiently
- Manage groups with directory synchronization
- Use Azure AD Connect Sync Security Groups to help maintain directory synchronization
- Configure object filters for directory synchronization
- Troubleshoot directory synchronization using various troubleshooting tasks and tools

Lessons:

- Introduction
- Manage users with directory synchronization
- Manage groups with directory synchronization
- Use Azure AD Connect Sync Security Groups to help maintain directory synchronization
- Configure object filters for directory synchronization
- Troubleshoot directory synchronization
- Knowledge check
- Summary

Module 14- Manage secure user access in Microsoft 365

This module examines various password-related tasks for users and administrators, including:

- creating and configuring password policies
- configuring self-service password management
- configuring multifactor authentication
- implementing entitlement packages
- implementing conditional access policies

Learning Objectives:

- Manage user passwords
- Describe pass-through authentication
- Enable multifactor authentication
- Describe self-service password management
- Implement Azure AD Smart Lockout
- Implement entitlement packages in Azure AD Identity Governance

- Implement conditional access policies
- Create and perform an access review

Lessons:

- Introduction
- Manage user passwords
- Enable pass-through authentication
- Enable multi-factor authentication
- Explore self-service password management
- Implement Azure AD Smart Lockout
- Implement entitlement packages in Azure AD Identity Governance
- Implement conditional access policies
- Create and run an access review
- Investigate authentication issues using sign-in logs
- Knowledge check
- Summary

Module 15- Examine threat vectors and data breaches

This module examines the types of threat vectors and their potential outcomes that organizations must deal with on a daily basis and how users can enable hackers to access targets by unwittingly executing malicious content.

Learning Objectives:

- Describe techniques hackers use to compromise user accounts through email
- Describe techniques hackers use to gain control over resources
- Describe techniques hackers use to compromise data
- Mitigate an account breach
- Prevent an elevation of privilege attack
- Prevent data exfiltration, data deletion, and data spillage

Lessons:

- Explore today's work and threat landscape
- Examine how phishing retrieves sensitive information
- Examine how spoofing deceives users and compromises data security
- Compare spam and malware
- Examine how an account breach compromises a user account
- Examine elevation of privilege attacks
- Examine how data exfiltration moves data out of your tenant
- Examine how attackers delete data from your tenant
- Examine how data spillage exposes data outside your tenant
- Examine other types of attacks
- Knowledge check
- Summary

Module 16- Explore the Zero Trust security model

This module examines the concepts and principles of the Zero Trust security model, as well as how Microsoft 365 supports it, and how your organization can implement it.

Learning Objectives:

- Describe the Zero Trust approach to security in Microsoft 365
- Describe the principles and components of the Zero Trust security model
- Describe the five steps to implementing a Zero Trust security model in your organization
- Explain Microsoft's story and strategy around Zero Trust networking

Lessons:

- Introduction
- Examine the principles and components of the Zero Trust model
- Plan for a Zero Trust security model in your organization
- Examine Microsoft's strategy for Zero Trust networking
- Adopt a Zero Trust approach
- Knowledge check
- Summary

Module 17- Explore security solutions in Microsoft 365 Defender

This module introduces you to several features in Microsoft 365 that can help protect your organization against cyberthreats, detect when a user or computer has been compromised, and monitor your organization for suspicious activities.

Learning Objectives:

- Identify the features of Microsoft Defender for Office 365 that enhance email security in a Microsoft 365 deployment
- Explain how Microsoft Defender for Identity identifies, detects, and investigates advanced threats, compromised identities, and malicious insider actions directed at your organization
- Explain how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats
- Describe how Microsoft 365 Threat Intelligence can be beneficial to your organization’s security officers and administrators
- Describe how Microsoft Cloud App Security enhances visibility and control over your Microsoft 365 tenant through three core areas

Lessons:

- Introduction
- Enhance your email security using Exchange Online Protection and Microsoft Defender for Office 365
- Protect your organization's identities using Microsoft Defender for Identity
- Protect your enterprise network against advanced threats using Microsoft Defender for

Endpoint
- Protect against cyber attacks using Microsoft 365 Threat Intelligence
- Provide insight into suspicious activity using Microsoft Cloud App Security
- Review the security reports in Microsoft 365 Defender
- Knowledge check
- Summary

Module 18- Examine Microsoft Secure Score

This module examines how Microsoft Secure Score helps organizations understand what they've done to reduce the risk to their data and show them what they can do to further reduce that risk.

Learning Objectives:

- Describe the benefits of Secure Score and what kind of services can be analyzed
- Describe how to collect data using the Secure Score API
- Describe how to use the tool to identify gaps between your current state and where you would like to be regarding security
- Identify actions that increase your security by mitigating risks
- Explain where to look to determine the threats each action mitigates and the impact it has on users

Lessons:

- Introduction
- Explore Microsoft Secure Score
- Assess your security posture with Microsoft Secure Score
- Improve your secure score
- Track your Microsoft Secure Score history and meet your goals
- Knowledge check
- Summary

Module 19- Examine Privileged Identity Management

This module examines how Privileged Identity Management ensures users in your organization have just the right privileges to perform the tasks they need to accomplish.

Learning Objectives:

- Describe how Privileged Identity Management enables you to manage, control, and monitor access to important resources in your organization
- Configure Privileged Identity Management for use in your organization
- Describe how Privileged Identity Management audit history enables you to see all the user assignments and activations within a given time period for all privileged roles
- Explain how Microsoft Identity Manager helps organizations manage the users, credentials, policies, and access within their organizations and hybrid environments
- Explain how Privileged Access Management provides granular access control over privileged admin tasks in Microsoft 365

Lessons:

- Introduction
- Explore Privileged Identity Management in Azure AD
- Configure Privileged Identity Management
- Audit Privileged Identity Management
- Explore Microsoft Identity Manager
- Control privileged admin tasks using Privileged Access Management
- Knowledge check
- Summary

Module 20- Examine Azure Identity Protection

This module examines how Azure Identity Protection provides organizations the same protection systems used by Microsoft to secure identities.

Learning Objectives:

- Describe Azure Identity Protection (AIP) and what kind of identities can be protected
- Enable the three default protection policies in AIP
- Identify the vulnerabilities and risk events detected by AIP
- Plan your investigation in protecting cloud-based identities
- Plan how to protect your Azure Active Directory environment from security breaches

Lessons:

- Introduction
- Explore Azure Identity Protection
- Enable the default protection policies in Azure Identity Protection
- Explore the vulnerabilities and risk events detected by Azure Identity Protection
- Plan your identity investigation
- Knowledge check
- Summary

Module 21- Examine Exchange Online Protection

This module examines how Exchange Online Protection (EOP) protects organizations from phishing and spoofing. It also explores how EOP blocks spam, bulk email, and malware before they arrive in users' mailboxes.

Learning Objectives:

- Describe how Exchange Online Protection analyzes email to provide anti-malware pipeline protection.
- List several mechanisms used by Exchange Online Protection to filter spam and malware.
- Describe other solutions administrators may implement to provide extra protection against phishing and spoofing.
- Understand how EOP provides protection against outbound spam.

Lessons:

- Introduction
- Examine the anti-malware pipeline
- Detect messages with spam or malware using Zero-hour auto purge
- Explore anti-spoofing protection provided by Exchange Online Protection
- Explore other anti-spoofing protection
- Examine outbound spam filtering
- Knowledge check
- Summary

Module 22- Examine Microsoft Defender for Office 365

This module examines how Microsoft Defender for Office 365 extends EOP protection by filtering targeted attacks such as zero-day attacks in email attachments and Office documents, and time-of-click protection against malicious URLs.

Learning Objectives:

- Describe how the Safe Attachments feature in Microsoft Defender for Office 365 blocks zero-day malware in email attachments and documents.
- Describe how the Safe Links feature in Microsoft Defender for Office 365 protects users from malicious URLs embedded in email and documents that point to malicious websites.
- Create outbound spam filtering policies.
- Unblock users who violated spam filtering policies so they can resume sending emails.

Lessons:

- Introduction
- Climb the security ladder from EOP to Microsoft Defender for Office 365
- Expand EOP protections by using Safe Attachments and Safe Links
- Manage spoofed intelligence
- Configure outbound spam filtering policies
- Unblock users from sending email
- Knowledge check
- Summary

Module 23- Manage Safe Attachments

This module examines how to manage Safe Attachments in your Microsoft 365 tenant by creating and configuring policies and using transport rules to disable a policy from taking effect in certain scenarios.

Learning Objectives:

- Create and modify a Safe Attachments policy using Microsoft 365 Defender
- Create a Safe Attachments policy by using PowerShell
- Configure a Safe Attachments policy

- Describe how a transport rule can disable a Safe Attachments policy
- Describe the end-user experience when an email attachment is scanned and found to be malicious

Lessons:

- Introduction
- Protect users from malicious attachments by using Safe Attachments
- Create Safe Attachment policies using Microsoft Defender for Office 365
- Create Safe Attachments policies using PowerShell
- Modify an existing Safe Attachments policy
- Create a transport rule to bypass a Safe Attachments policy
- Examine the end-user experience with Safe Attachments
- Knowledge check
- Summary

Module 24- Manage Safe Links

This module examines how to manage Safe Links in your tenant by creating and configuring policies and using transport rules to disable a policy from taking effect in certain scenarios.

Learning Objectives

- Create and modify a Safe Links policy using Microsoft 365 Defender
- Create a Safe Links policy using PowerShell
- Configure a Safe Links policy
- Describe how a transport rule can disable a Safe Links policy
- Describe the end-user experience when Safe Links identifies a link to a malicious website embedded in email, and a link to a malicious file hosted on a website

Lessons:

- Introduction
- Protect users from malicious URLs by using Safe Links
- Create Safe Links policies using Microsoft 365 Defender
- Create Safe Links policies using PowerShell
- Modify an existing Safe Links policy
- Create a transport rule to bypass a Safe Links policy
- Examine the end-user experience with Safe Links
- Knowledge check
- Summary

Module 25- Explore threat intelligence in Microsoft 365 Defender

This module examines how Microsoft 365 Threat Intelligence provides admins with evidence-based knowledge and actionable advice that can be used to make informed decisions about protecting and responding to cyber-attacks against their tenants.

Learning Objectives:

- Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
- Create alerts that can identify malicious or suspicious events.
- Understand how the Microsoft 365 Defender's Automated investigation and response process works.
- Describe how threat hunting enables security operators to identify cybersecurity threats.
- Describe how Advanced hunting in Microsoft 365 Defender proactively inspects events in your network to locate threat indicators and entities.

Lessons:

- Introduction
- Explore Microsoft Intelligent Security Graph
- Explore alert policies in Microsoft 365
- Run automated investigations and responses
- Explore threat hunting with Microsoft Threat Protection
- Explore advanced threat hunting in Microsoft 365 Defender
- Explore threat analytics in Microsoft 365
- Identify threat issues using Microsoft Defender reports
- Knowledge check
- Summary

Module 26- Implement app protection by using Microsoft Defender for Cloud Apps

This module examines how to implement Microsoft Defender for Cloud Apps, which identifies and combats cyberthreats across all your Microsoft and third-party cloud services.

Learning Objectives:

- Describe how Microsoft Defender for Cloud Apps provides improved visibility into network cloud activity and increases the protection of critical data across cloud applications.
- Explain how to deploy Microsoft Defender for Cloud Apps.
- Control your cloud apps with file policies.
- Manage and respond to alerts generated by those policies.
- Configure and troubleshoot Cloud Discovery.

Lessons:

- Introduction
- Explore Microsoft Defender Cloud Apps
- Deploy Microsoft Defender for Cloud Apps
- Configure file policies in Microsoft Defender for Cloud Apps
- Manage and respond to alerts in Microsoft Defender for Cloud Apps
- Configure Cloud Discovery in Microsoft Defender for Cloud Apps
- Troubleshoot Cloud Discovery in Microsoft Defender for Cloud Apps
- Knowledge check

- Summary

Module 27- Implement endpoint protection by using Microsoft Defender for Endpoint

This module examines how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats by using endpoint behavioral sensors, cloud security analytics, and threat intelligence.

Learning Objectives:

- Describe how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats.
- Onboard supported devices to Microsoft Defender for Endpoint.
- Implement the Threat and Vulnerability Management module to effectively identify, assess, and remediate endpoint weaknesses.
- Configure device discovery to help find unmanaged devices connected to your corporate network.
- Lower your organization's threat and vulnerability exposure by remediating issues based on prioritized security recommendations.

Lessons:

- Introduction
- Explore Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint in Microsoft Intune
- Onboard devices in Microsoft Defender for Endpoint
- Manage endpoint vulnerabilities with Microsoft Defender Vulnerability Management
- Manage device discovery and vulnerability assessment
- Reduce your threat and vulnerability exposure
- Knowledge check
- Summary

Module 28- Implement threat protection by using Microsoft Defender for Office 365

This module examines the Microsoft Defender for Office 365 protection stack and its corresponding threat intelligence features, including Threat Explorer, Threat Trackers, and Attack simulation training.

Learning Objectives:

- Describe the protection stack provided by Microsoft Defender for Office 365.
- Understand how Threat Explorer can be used to investigate threats and help to protect your tenant.
- Describe the Threat Tracker widgets and views that provide you with intelligence on different cybersecurity issues that might affect your company.
- Run realistic attack scenarios using Attack Simulator to help identify vulnerable users before a real attack impacts your organization.

Lessons:

- Introduction
- Explore the Microsoft Defender for Office 365 protection stack
- Investigate security attacks by using Threat Explorer
- Identify cybersecurity issues by using Threat Trackers
- Prepare for attacks with Attack simulation training
- Knowledge check
- Summary