MS 365 Mobility and Security

Length: 5 days
Format: Bootcamp
Time: Day

About This Course

This course covers three central elements of Microsoft 365 enterprise administration - Microsoft 365 security management, Microsoft 365 compliance management, and Microsoft 365 device management. In Microsoft 365 security management, you will examine all the common types of threat vectors and data breaches facing organizations today, and you will learn how Microsoft 365's security solutions address these security threats. You will be introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You will then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Advanced Threat Protection, Safe Attachments, and Safe Links. Finally, you will be introduced to the various reports that monitor your security health. You will then transition from security services to threat intelligence; specifically, using the Security Dashboard and Advanced Threat Analytics to stay ahead of potential security breaches.

With your Microsoft 365 security components now firmly in place, you will 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, Information Rights Management, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365 message encryption, and data loss prevention (DLP). You will then delve deeper into archiving and retention, paying particular attention to in-place records management in SharePoint, archiving and retention in Exchange, and Retention policies in the Security and Compliance Center.

Now that you understand the key aspects of data governance, you will examine how to implement them, including the building of ethical walls in Exchange Online, creating DLP policies from built-in templates, creating custom DLP policies, creating DLP policies to protect documents, and creating policy tips. You will then focus on managing data governance in Microsoft 365, including managing retention in email, troubleshooting retention policies and policy tips that fail, as well as troubleshooting sensitive data. You will then learn how to implement Azure Information Protection and Windows Information Protection. You will conclude this section by learning how to manage search and investigation, including searching for content in the Security and Compliance Center, auditing log investigations, and managing advanced eDiscovery.

The course concludes with an in-depth examination of Microsoft 365 device management. You will begin by planning for various aspects of device management, including preparing your Windows 10 devices for co-management. You will learn how to transition from Configuration Manager to Intune, and you will be introduced to the Microsoft Store for Business and Mobile Application Management. At this point, you will transition from planning to implementing device management; specifically, your Windows 10 deployment strategy. This includes learning how to implement Windows Autopilot, Windows Analytics, and Mobile Device Management (MDM). When examining MDM, you will learn how to deploy it, how to enroll devices to MDM, and how to manage device compliance.

Required Exams

Audience Profile

This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role.

Course Objectives

By completing this course, students will learn how to:

* Microsoft 365 Security Metrics
* Microsoft 365 Security Services
* Microsoft 365 Threat Intelligence
* Data Governance in Microsoft 365
* Archiving and Retention in Office 365
* Data Governance in Microsoft 365 Intelligence
* Search and Investigations
* Device Management
* Windows 10 Deployment Strategies
* Mobile Device Management

Outline

Module 1: Introduction to Microsoft 365 Security Metrics

In this module, you will examine all the common types of threat vectors and data breaches facing organizations today, and you will learn how Microsoft 365's security solutions address these security threats, including the Zero Trust approach. You will be introduced to the Microsoft Secure Score, Privileged Identity Management, as well as to Azure Active Directory Identity Protection.

Lessons

* Threat Vectors and Data Breaches
* The Zero Trust Model
* Security Solutions in Microsoft 365
* Introduction to Microsoft Secure Score
* Privileged Identity Management
* Introduction to Azure Active Directory Identity Protection

Module 2: Managing Your Microsoft 365 Security Services

This module examines how to manage the Microsoft 365 security services, including Exchange Online Protection, Advanced Threat Protection, Safe Attachments, and Safe Links. You will be introduced to the various reports that monitor your security health.

Lessons

* Introduction to Exchange Online Protection
* Introduction to Advanced Threat Protection
* Managing Safe Attachments
* Managing Safe Links
* Monitoring and Reports

Module 3: Microsoft 365 Threat Intelligence

In this module, you will then transition from security services to threat intelligence; specifically, using the Security Dashboard and Advanced Threat Analytics to stay ahead of potential security breaches.

Lessons

* Overview of Microsoft 365 Threat Intelligence
* Using the Security Dashboard
* Configuring Advanced Threat Analytics
* Implementing Your Cloud Application Security

Module 4: Introduction to Data Governance in Microsoft 365

This module examines 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, Information Rights Management, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365 message encryption, and data loss prevention (DLP).

Lessons

* Introduction to Archiving in Microsoft 365
* Introduction to Retention in Microsoft 365
* Introduction to Information Rights Management
* Introduction to Secure Multipurpose Internet Mail Extension
* Introduction to Office 365 Message Encryption
* Introduction to Data Loss Prevention

Module 5: Archiving and Retention in Microsoft 365

This module delves deeper into archiving and retention, paying particular attention to in-place records management in SharePoint, archiving and retention in Exchange, and Retention policies in the Security and Compliance Center.

Lessons

* In-Place Records Management in SharePoint
* Archiving and Retention in Exchange
* Retention Policies in the SCC

Module 6: Implementing Data Governance in Microsoft 365 Intelligence

This module examines how to implement the key aspects of data governance, including the building of ethical walls in Exchange Online, creating DLP policies from built-in templates, creating custom DLP policies, creating DLP policies to protect documents, and creating policy tips.

Lessons

* Evaluating Your Compliance Readiness
* Implementing Compliance Center Solutions
* Building Ethical Walls in Exchange Online
* Creating a Simple DLP Policy from a Built-in Template
* Creating a Custom DLP Policy
* Creating a DLP Policy to Protect Documents
* Working with Policy Tips

Module 7: Managing Data Governance in Microsoft 365

This module focuses on managing data governance in Microsoft 365, including managing retention in email, troubleshooting retention policies and policy tips that fail, as well as troubleshooting sensitive data. You will then learn how to implement Azure Information Protection and Windows Information Protection.

Lessons

* Managing Retention in Email
* Troubleshooting Data Governance
* Implementing Azure Information Protection
* Implementing Advanced Features of AIP

* Implementing Windows Information Protection

Module 8: Managing Search and Investigations

This module conclude this section on data governance by examining how to manage search and investigation, including searching for content in the Security and Compliance Center, auditing log investigations, and managing advanced eDiscovery.

Lessons

* Searching for Content in the Security and Compliance Center
* Auditing Log Investigations
* Managing Advanced eDiscovery

Module 9: Planning for Device Management

This module provides an in-depth examination of Microsoft 365 Device management. You will begin by planning for various aspects of device management, including preparing your Windows 10 devices for co-management. You will learn how to transition from Configuration Manager to Microsoft Intune, and you will be introduced to the Microsoft Store for Business and Mobile Application Management.

Lessons

* Introduction to Co-management
* Preparing Your Windows 10 Devices for Co-management
* Transitioning from Configuration Manager to Intune
* Introduction to Microsoft Store for Business
* Planning for Mobile Application Management

Module 10: Planning Your Windows 10 Deployment Strategy

This module focuses on planning your Windows 10 deployment strategy, including how to implement Windows Autopilot and Windows Analytics, and planning your Windows 10 subscription activation service.,

Lessons

* Windows 10 Deployment Scenarios
* Implementing and Managing Windows Autopilot
* Planning Your Windows 10 Subscription Activation Strategy
* Resolving Windows 10 Upgrade Errors

* Introduction to Windows Analytics

Module 11: Implementing Mobile Device Management

This module focuses on Mobile Device Management (MDM). You will learn how to deploy it, how to enroll devices to MDM, and how to manage device compliance.

Lessons

* Planning Mobile Device Management
* Deploying Mobile Device Management
* Enrolling Devices to MDM
* Managing Device Compliance