Office 365:Security and Compliance

WorkshopPLUS

Duration: 3 days

Focus Area: Operations and Monitoring

Difficulty: 300 - Advanced

Overview

The Office 365 Security and Compliance workshop provides attendees with in-depth knowledge and understanding of how to leverage the Security and Compliance Center to comply with their organizations Security and Compliance mandates.

Through presentations, white-board discussions, and goal-based labs, this three-day workshop covers the Security and Compliance Center tools needed for the role of an Office 365 administrator.

Each group of modules is organized by scenario and ~~is~~ designed to provide participants with this expertise, plus tools and hands-on experience to configure and implement the various Security and Compliance features in Office 365.

Objectives

After completing this training, students will be able to:

- Understand the various security features along with how they provide protection and mitigate the risk from threats like phishing, ransomware, impersonation and loss of data.
- Understand the various compliance features that will allow you to meet industry compliance requirements like GDPR and HIPPA.
- Understand how the Security and Compliance Center provides unified security and compliance in Office 365.

Key Takeaways

Course Material

Each group of modules is organized by scenario and is designed to provide participants with in-depth expertise, plus tools and hands-on experience to configure and implement the various Security and Compliance features in Office 365

Hands-on Labs

- Most of the concepts covered above will be supported by hands-on labs and demos.
- Attendees have access to resources and labs for up to 6 months after workshop completion.

Agenda

Day 1

- Permissions in the Security and Compliance Center
- Retention/Deletion Polices
- Retention Labels
- Supervision Policies

Day 2

- Data Loss Prevention
- Sensitivity Labels
- Information Rights Management and Office 365 Message Encryption
- Threat Management

Day 3

- Automated Investigation and Response (AIR)
- Content Search, eDiscovery and Advanced eDiscovery
- Audit Logs and Alerting
- Office 365 Cloud App Security
- (Optional) - Other Features

Plan for three full days. Early departure on any day is not recommended.

Microsoft

Course details

Module 1: Permissions in the Security and Compliance Center: This module demonstrates to students; which permissions are needed to perform the various activities in the Security and Compliance Center.

Module 2: Retention/Deletion Polices: This module focuses on how Retention and Deletion Polices allow administrators to effectively manage their data in Exchange Online, SharePoint Online, One Drive for Business, Skype for Business and Microsoft Teams.

Module 3: Retention Labels: In this module students learn how Retention labels classify data across your organization for governance and enforce retention rules based on that classification.

Module 4: Supervision Policies: This module instructs students on how to enable supervision policies that allow reviewers to monitor email and third-party communications as well as classify content for further review or actions.

Module 5: Data Loss Prevention: This module focuses on the configuration and implementation of Data Loss Protection in Exchange Online, SharePoint, One Drive for Business and Microsoft Teams. Default types, customized types and Exact Data Match are all covered.

Module 6: Sensitivity Labels: In this module students learn how Sensitivity Labels classify data across your organization for persistent protection, security markings, and enforce security rules based on that classification.

Module 7: Information Rights Management and Office 365 Mail Encryption: In this module you discover how to configure and implement Information Rights Management and Office 365 Mail Encryption.

Module 8: Threat Management: In this module students explore how Advanced Threat Protection increases their email delivery security using Safe Attachments, Safe Links, and Anti-Impersonation policies. You also discuss the Attack Simulator.

Module 9: Automated Investigation and Response: In this module students explore Automated investigation and response (AIR) capabilities that enable you to run automated investigation processes in response to well known threats that exist today.

Module 10: Content Search and eDiscovery Case Management: In this module students explore the Content Search feature, how to manage eDiscovery Cases and how to enhance discovery through Advanced eDiscovery using the Security and Compliance Center.

Module 11: Audit Logs and Alerting: This module introduces students to how to use Audit Logs to track both user/administrator activities and set up Alerting to monitor these activities.

Module 12: Office 365 Cloud App Security: This module introduce security and alerting features included in the Office 365 Cloud App Security feature.

Optional Module: Other Features: This module covers additional features inside and outside of the Security and Compliance Center. These are updated over time but always contain Secure Score, Compliance Manager, and File Plan manager.

Recommended Qualifications

This course is an advanced course for Office 365 Security and Compliance. It is aimed at Administrators who have already migrated to Office 365 or soon will be.

Other roles to benefit from this course are the compliance team, legal team, or security team.

The basic concepts and know-how of the product is covered in this course; however, it is expected that attendees already possess basic knowledge of Office 365.

Hardware requirements

- An Intel Core-i5-based PC
- USB port
- Microsoft/Windows Live ID to connect to the virtual environment
- 4 GB RAM
- 128 GB HDD
- Windows 7 SP1 or later
- Office 2013 Professional Plus
- Internet access with at least 1 Mbps bandwidth per student.

For more information

Contact your Microsoft Account Representative for further details.

Microsoft