training code: MS-101 / ENG DL 5d / EN

Microsoft 365 Mobility and Security

Purpose of the training

The training is aimed at the people responsible for Office 365 management. The course is particularly intended for the people who aspire for the role of Microsoft 365 Enterprise service administrator and completed one of the role-based Microsoft 365 paths. The training consists of three main elements of administering Microsoft 365 Enterprise – Microsoft 365 security management, managing compliance with Microsoft 365 and Microsoft 365 device management. The course includes such topics:
Microsoft 365 security management:

- types of threat and data violation vectors, as well as Microsoft 365 security solutions solve these threats.
- Microsoft Secure Score
- Azure Active Directory Identity Protection
- managing Microsoft 365 threat services, including Exchange Online Protection, Advanced Threat Protection, Safe Attachments and Safe Links
- reports monitoring condition status
- using security dashboard and advanced threat analysis to be ahead of the potential security threats.

Managing compliance with Microsoft 365:

- key apects of data management – archivization and data storage, managing rights to information, secure universal Internet e-mail extension (S/MIME), Office 365 message encryption and Data Loss Prevention (DLP)
- archiving and storing including managing records in place in SharePoint, archiving and storing in Exchange application as well as the rules of storage in the Security and Compliance Center
- implementing key aspects of data management, including building ethical walls in Exchange Online, formulating DLP rules from embedded templates, creating non-standard DLP rules , formulating DLP rules to protect documents and guidelines related to the rules
- coordinating data management in Microsoft 365, including managing storage in e-mail mailbox, solving problems with the rules of storage and guidelines, as well as solving problems with sensitive personal information, implementing Azure Information Protection service and Windows Information Protection
- manging search and investigation, including looking for content in Security and Compliance Center,

auditing diary research and eDiscovery advanced management.

Microsoft 365 device management:

- device management, including preparing devices with Windows 10 system
- transition from Configuration Manager to Intune service
- Microsoft Store for companies
- mobile application management
- a strategy of implementing Windows 10 system, including implementing Windows Autopilot, Windows Analytics and Mobile Devices Management (MDM)
- registering a device in MDM
- managing device compliance.

Benefits of completing the training

Acquiring knowledge and practical skills in Office 365, including acquaintance with:

- Microsoft 365 security metrics
- Microsoft 365 security services
- Microsoft 365 threat analysis
- Data management in Microsoft 365
- Archivization and storage in Office 365
- Data management in Microsoft 365
- Searching and investigation
- Device management
- Strategies of implementing Windows 10 system
- Mobile device management.

Expected Listener Preparation

A completed role-based administrator course, such as Messaging, Teamwork, Security and Compliance, Collaboration or equivalent knowledge, a knowledge of DNS functioning and basic knowledge of Microsoft 365 services, a knowledge of general IT practices, as well as knowledge about using PowerShell.
An ability to use materials in English language

Training Language

- Training: English

- Materials: English

Training Includes

- manual in electronic form available on the platform:
- https://learn.microsoft.com/pl-pl/training/
- access to Altkom Akademia's student portal

Duration

5 days / 35 hours

Training agenda

1. Introduction to Microsoft 365 security indicators
    1. Threat and data violation vectors
    2. Security solutions in Microsoft 365
    3. Introduction to secure result
    4. Introduction to Azure Active Directory Identity Protection service
2. Microsoft 365 security services management
    1. Introduction to Exchange Online Protection
    2. Introduction to advanced anti-threat protection
    3. Secure appendices management
    4. Secure link management
    5. Monitoring and reports
3. Lab 1 – Manage Microsoft 365 security services
4. Microsoft 365 threat analysis
    1. Discussing Microsoft 365 threat analysis
    2. Using the security desktop
    3. Configuring advanced threat analysis
    4. Application security implementation in Cloud
5. Lab 2 – Implementing alert notifications using security desktop

6. Introduction to data management in Microsoft 365
    1. Introduction to archivization in Microsoft 365
    2. Introduction to storage in Microsoft 365
    3. Introduction to managing rights to information
    4. Introduction to secure universal Internet mailbox extension
    5. Introduction to Office 365 message encryption
    6. Introduction to Data Loss Prevention
7. Archivization and storage in Office 365
    1. Managing records in place in SharePoint
    2. Archivization and storage in Exchange
    3. Storage rules in SCC
8. Lab 3 – Implementing archivization and storage
9. Implementing data management in Microsoft 365
    1. Planning security and need satisfaction
    2. Building ethical walls in Exchange Online
    3. Formulating simple DLP rules based on embedded template
    4. Formulating non-standard DLP rules
    5. Formulating DLP rules in order to secure documents
    6. Working with guidelines related to rules
10. Lab 4 – Implementing DLP rules
11. Coordinating data management in Microsoft 365
    1. Managing storage in e-mail message
    2. Solving problems with data management
    3. Implementing Azure Information Protection service
    4. Implementing AIP advanced functions
    5. Implementing information security in Windows system
12. Lab 5 – Implementing AIP and WIP
13. Managing search and investigation
    1. Searching content in Security and Compliance Center
    2. Studying control diary
    3. Advanced eDiscovery management
14. Lab 6 – Managing search and investigation
15. Planning device management
    1. Introduction to co-management
    2. Preparing devices with Windows 10 system to co-management
    3. Transition from Configuration Manager application toIntune service
    4. Introduction to Microsoft Store for Companies
    5. Planning mobile application management

16. Lab 7 – Implementing Microsoft Store for companies
17. Planning strategy of implementing Windows 10 system
    1. Scenarios of implementing Windows 10 system
    2. Implementing Windows Autopilot
    3. Planning the strategy of activating Windows 10 subscription
    4. Solving problems with Windows 10 system update
    5. Introduction to Windows Analytics
18. Implementing mobile device management
    1. Planning mobile device management
    2. Implementing mobile device management
    3. Registering devices in MDM
    4. Managing Device Compliance
19. Lab 8 -Managing devices using Intune service