Szkolenie: Microsoft
MS-101T00 Microsoft 365 Mobility and Security

FORMA SZKOLENIA  MATERIAŁY SZKOLENIOWE  CENA  CZAS TRWANIA
Stacjonarne  Cyfrowe  3600 PLN NETTO*  5 dni
Stacjonarne  Tablet CTAB  4000 PLN NETTO*  5 dni

* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

LOKALIZACJE
Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00
Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

DOSTĘPNE TERMINY
2020-02-03  |  5 dni  |  Warszawa
2020-03-02  |  5 dni  |  Kraków
2020-05-11  |  5 dni  |  Warszawa

Cel szkolenia:
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.

Audience profile
This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

At course completion:
By actively participating in this course, you will learn about the following:

- 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

Plan szkolenia:

- Introduction to Microsoft 365 Security Metrics Lessons
  - Threat Vectors and Data Breaches
  - Security Solutions in Microsoft 365
  - Introduction to the Secure Score
  - Introduction to Azure Active Directory Identity Protection

- Managing Your Microsoft 365 Security Services Lessons
  - Introduction to Exchange Online Protection
  - Introduction to Advanced Threat Protection
  - Managing Safe Attachments
Managing Safe Links
Monitoring and Reports

Lab 1 - Manage Microsoft 365 Security Services
- Exercise 1 - Set up a Microsoft 365 Trial Tenant
- Exercise 2 - Implement an ATP Safe Links policy and Safe Attachment policy

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

Lab 2 - Implement Alert Notifications Using the Security Dashboard
- Exercise 1 - Prepare for implementing Alert Policies
- Exercise 2 - Implement Security Alert Notifications
- Exercise 3 - Implement Group Alerts
- Exercise 4 - Implement eDiscovery Alerts

Introduction to Data Governance in Microsoft 365
- 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

Archiving and Retention in Office 365
- In-Place Records Management in SharePoint
- Archiving and Retention in Exchange
- Retention Policies in the SCC

Lab 3 - Implement Archiving and Retention
- Exercise 1 - Initialize Compliance in Your Organization
- Exercise 2 - Configure Retention Tags and Policies
- Exercise 3 - Implement Retention Policies

Implementing Data Governance in Microsoft 365
- Planning Your Security and Complaince Needs
- 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

Lab 4 - Implement DLP Policies
  Exercise 1 - Manage DLP Policies
  Exercise 2 - Test MRM and DLP Policies

Managing Data Governance in Microsoft 365 Lessons
  Managing Retention in Email
  Troubleshooting Data Governance
  Implementing Azure Information Protection
  Implementing Advanced Features of AIP
  Implementing Windows Information Protection

Lab 5 - Implement AIP and WIP
  Exercise 1 - Implement Azure Information Protection
  Exercise 2 - Implement Windows Information Protection

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

Lab 6 - Manage Search and Investigations
  Exercise 1 - Investigate Your Microsoft 365 Data
  Exercise 2 - Configure and Deploy a Data Subject Request

Planning for Device 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

Lab 7 - Implement the Microsoft Store for Business
  Exercise 1 - Configure the Microsoft Store for Business
  Exercise 2 - Manage the Microsoft Store for Business

Planning Your Windows 10 Deployment Strategy Lessons
  Windows 10 Deployment Scenarios
  Implementing Windows Autopilot
  Planning Your Windows 10 Subscription Activation Strategy
  Resolving Windows 10 Upgrade Errors
Introduction to Windows Analytics

- Implementing Mobile Device Management Lessons
  - Planning Mobile Device Management
  - Deploying Mobile Device Management
  - Enrolling Devices to MDM
  - Managing Device Compliance
- Lab 8 - Manage Devices with IntuneLab: Manage Devices with Intune
  - Exercise 1 - Enable Device Management
  - Exercise 2 - Configure Azure AD for Intune
  - Exercise 3 - Create Intune Policies
  - Exercise 4 - Enroll a Windows 10 Device
  - Exercise 5 - Manage and Monitor a Device in Intune

Wymagania:

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

Poziom trudności

Certyfikaty:

Uczestnicy szkolenia MS-101T00 Microsoft 365 Mobility and Security otrzymują certyfikat ukończenia autoryzowanego kursu Microsoft.

Prowadzący:

Microsoft Certified Trainer.

Informacje dodatkowe:

Zajęcia prowadzone są w języku polskim, materiały źródłowe oraz oprogramowanie są w języku angielskim.