training code: MS-500 / ENG DL 4d / EN

Microsoft 365 Security Administrator

Purpose of the training

Training addressed to persons responsible for managing identity and access security, protection against threats in the Microsoft 365 environment, information protection as well as internal rules and external data storage requirements and conducting investigations.
The course includes the following topics:

- Secure user access to organization resources, password protection, multifactor authentication, identity protection in Azure, configuration of Active Directory federation services, Azure AD Connect configuration and conditional access and solutions for external access to Microsoft 365
- Threat vectors and security solutions to protect against this type of attack, such as: Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection and how to use Microsoft 365 Threat Intelligence to configure the system to achieve the right level of security, this also includes issues related to mobile devices and application management
- Information protection as a concept of locating and classifying data anywhere, including information protection technologies that help protect the Microsoft 365 environment, i.e. content management with information permissions, message encryption, as well as labels, policies and rules to prevent data loss, information protection, and implementation of the Microsoft Cloud App Security
- Internal policies and external requirements for data storage and investigation, including archiving and storage in Microsoft 365, data management and search by content, i.e. rules and tags for data storage, records management in place for SharePoint, storage of emails and ways to search for content that supports eDiscovery investigations and how to prepare for the Global Data Protection Regulation (GDPR)

Benefits of completing the training

Obtaining knowledge and practical skills in the security of Office 365. Including getting acquainted with:

- User and group security management and password management in Microsoft 365, Azure Identity Protection, Azure AD Connect planning and deployment, synchronized identity management, federated identity implementation planning, and use of conditional access

- Issues describing risk vectors for cyberattacks, security solutions for Microsoft 365, using Microsoft Secure Score to assess security, using the security panel in the Microsoft Security & Compliance Center, configuring various advanced threat protection services for Microsoft 365 services, configuring advanced threat analysis and planning and implementation management of mobile devices
- Implementation of information rights management, secure messages in Office 365, configuration of data loss prevention policies, implementation of Cloud App Security management, implementation of Azure information protection for Microsoft 365, implementation of protection of Windows information for devices
- Planning and implementation of the data archiving and storage system, assessment in the Compliance Manager, e-mail retention management via Exchange, conducting investigations in the audit log, creating an investigation into the eDiscovery case, managing the requests of entities on GDPR data

Expected Listener Preparation

Basic information about Microsoft Azure, experience in working with Windows 10 and Office 365 devices, basics in the field of authorization and authentication, basics of computer networks and knowledge in the field of mobile device management. Ability to use English-language materials.

Training Language

- Training: English
- Materials: English

Duration

4 days / 28 hours

Training agenda

1. User and group security
   - User accounts in Microsoft 365
   - Administrative roles and security groups in Microsoft 365
   - Managing passwords in Microsoft 365
   - Identity protection in Azure AD
2. Identity synchronization
   - Introduction to identity synchronization
   - Planning Azure AD Connect
   - Implementing Azure AD Connect
   - Managing synchronized identities
3. Federation identity
   - Introduction to federal identity
   - Planning the implementation of AD FS
   - AD FS implementation
4. Access management
   - Conditional access
   - Device access management
   - Role-based access control (RBAC)
   - Solutions for external access
5. Security in Microsoft 365
   - Threat vectors and data breach
   - Security solutions for Microsoft 365
   - Microsoft security indicator
6. Advanced protection against threats
   - Exchange Online Protection
   - Office 365 Advanced Threat Protection
   - Managing secure attachments
   - Managing secure links
   - Azure Advanced Threat Protection
   - Windows Defender Advanced Threat Protection
7. Threat analysis
   - Analysis of threats in Microsoft 365
   - Use of the security dashboard
   - Configuration of advanced threat analysis
8. Mobility
   - Planning the management of mobile applications
   - Planning mobile devices management
   - Implementation of mobile device management
   - Device registration in Mobile Device Management
9. Information protection

- Information rights management
- Safe, universal extension of e-mail
- Encrypting Office 365 messages
- Azure Information Protection
- Advanced information protection
- Protecting Windows information

10. Preventing data loss
    - Guide to preventing data loss
    - Data loss prevention rules
    - Custom DLP rules
    - Creating a DLP policy to protect documents
    - Policy instructions
11. Cloud Application Security
    - Explanation of the security of applications in the cloud
    - Using the application security information in the cloud
    - Office 365 Cloud App Security
12. Archiving and storage
    - Archiving in Microsoft 365
    - Storage in Microsoft 365
    - Storage policy in the Security and Compliance Center
    - Archiving and storage in Exchange
    - Manage records in place in SharePoint
13. Data management in Microsoft 365
    - Planning needs in terms of security and compliance
    - Building ethical walls in Exchange Online
    - Managing storage in e-mail
    - Solving problems with data management
    - Analytics and telemetry
14. Managing search and investigations
    - Search content in the Security and Compliance Center
    - Audit investigations
    - Advanced eDiscovery