MS-500

Microsoft 365 security

Description:

In this four-day course you will learn how to secure user access to your organization’s resources, about threat protection technologies that help protect your Microsoft 365 environment, about information protection technologies that help secure your Microsoft 365 environment and about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations.

Students will be able to:

- Conduct an audit log investigation.
- Create and manage an eDiscovery investigation.
- Configure various advanced threat protection services for Microsoft 365.
- Configure Advanced Threat Analytics.
- Configure Data Loss Prevention policies.
- Describe cyber-attack threat vectors.
- Describe security solutions for Microsoft 365
- Deploy and manage Cloud App Security.
- Manage email retention through Exchange.
- Manage GDPR data subject requests.
- Plan and deploy a data archiving and retention system.
- Perform assessments in Compliance Manager.
- Plan and deploy Mobile Device Management.
- Secure messages in Office 365.
- Implement information rights management.
- Implement Azure information protection for Microsoft 365.
- Implement Windows information protection for devices.
- Use Microsoft Secure Score to evaluate your security posture.
- Use the Security Dashboard in the Microsoft Security & Compliance center.

Course requirements:

- Basic conceptual understanding of Microsoft Azure.
- Experience with Windows 10 devices.
- Experience with Office 365.
- Basic understanding of authorization and authentication.
- Basic understanding of computer networks.
- Working knowledge of managing mobile devices.

This course is intended for:

Security administrator who want to plan and implement security strategies and ensures that the solutions comply with the policies and regulations of the organization.

Literature:

All participants will get original Microsoft student materials.

Hardware:

Classrooms are equipped with high-performance computers with Internet access and the possibility of wireless connection.

Syllabus:

Module 1: User and Group Security

- Lesson: User Accounts in Microsoft 365
- Lesson: Administrator Roles and Security Groups in Microsoft 365
- Lesson: Password Management in Microsoft 365
- Lesson: Azure AD Identity Protection
- Lab: Managing your Microsoft 365 Identity environment

Module 2: Identity Synchronization

- Lesson: Introduction to Identity Synchronization
- Lesson: Planning for Azure AD Connect
- Lesson: Implementing Azure AD Connect
- Lesson: Managing Synchronized Identities
- Lab: Implementing Identity Synchronization

Module 3: Federated Identities

- Lesson: Introduction to Federated Identities
- Lesson: Planning an AD FS Deployment
- Lesson: Implementing AD FS

Module 4: Access Management

- Lesson: Conditional Access
- Lesson: Managing Device Access
- Lesson: Role Based Access Control (RBAC)
- Lesson: Solutions for External Access

Module 5: Security in Microsoft 365

- Lesson: Threat Vectors and Data Breaches
- Lesson: Security Solutions for Microsoft 365
- Lesson: Microsoft Secure Score

Module 6: Advanced Threat Protection

- Lesson: Exchange Online Protection
- Lesson: Office 365 Advanced Threat Protection
- Lesson: Managing Safe Attachments
- Lesson: Managing Safe Links

- Lesson: Azure Advanced Threat Protection
- Lesson: Windows Defender Advanced Threat Protection
- Lab: Advanced Threat Protection

Module 7: Threat Intelligence

- Lesson: Microsoft 365 Threat Intelligence
- Lesson: Using the Security Dashboard
- Lesson: Configuring Advanced Threat Analytics
- Lab: Advanced Threat Analytics

Module 8: Mobility

- Lesson: Plan for Mobile Application Management
- Lesson: Plan for Mobile Device Management
- Lesson: Deploy Mobile Device Management
- Lesson: Enroll Devices to Mobile Device Management

Module 9: Information Protection

- Lesson: Information Rights Management
- Lesson: Secure Multipurpose Internet Mail Extension
- Lesson: Office 365 Message Encryption
- Lesson: Azure Information Protection
- Lesson: Advanced Information Protection
- Lesson: Windows Information Protection
- Lab: Data Loss Prevention

Module 10: Data Loss Prevention

- Lesson: Data Loss Prevention Explained
- Lesson: Data Loss Prevention Policies
- Lesson: Custom DLP Policies
- Lesson: Creating a DLP Policy to Protect Documents
- Lesson: Policy Tips
- Lab: Data Loss Prevention

Module 11: Cloud Application Security

- Lesson: Cloud Application Security Explained
- Lesson: Using Cloud Application Security Information
- Lesson: Office 365 Cloud App Security

Module 12: Archiving and Retention

- Lesson: Archiving in Microsoft 365
- Lesson: Retention in Microsoft 365
- Lesson: Retention Policies in the Security and Compliance Center
- Lesson: Archiving and Retention in Exchange
- Lesson: In-place Records Management in SharePoint
- Lab: Archiving and Retention

Module 13: Data Governance in Microsoft 365

- Lesson: Planning Security and Compliance Needs
- Lesson: Building Ethical Walls in Exchange Online
- Lesson: Manage Retention in Email
- Lesson: Troubleshooting Data Governance
- Lesson: Analytics and Telemetry

Module 14: Managing Search and Investigations

- Lesson: Searching for Content in the Security and Compliance Center
- Lesson: Audit Log Investigations
- Lesson: Advanced eDiscovery
- Lab: eDiscovery

Contact us
OKsystem a.s., Na Pankráci 1690/125, 140 00 Prague 4
(+420) 236 072 111 skoleni@oksystem.cz www.okskoleni.cz