Microsoft 365 Security

Learn how to:

- Administer user and group access in Microsoft 365
- Explain and manage Azure Identity Protection
- Plan and implement Azure AD Connect
- Manage synchronized user identities
- Explain and use conditional access
- Describe cyber-attack threat vectors
- Explain security solutions for Microsoft 365
- Use Microsoft Secure Score to evaluate and improve your security posture
- Configure various advanced threat protection services for Microsoft 365
- Plan for and deploy secure mobile devices
- Implement information rights management
- Secure messages in Office 365
- Configure Data Loss Prevention policies
- Deploy and manage Cloud App Security
- Implement Windows information protection for devices
- Plan and deploy a data archiving and retention system
- Create and manage an eDiscovery investigation

Pre-Requisites:

Delegates should have an understanding of Azure concepts, experience with Windows 10 devices and Office 365 as well as a good understanding of Active Directory and TCP/IP networking.

Duration:

4 Days

NEOS

IT Training

User and Group Management

Create and manage user accounts
Implement 365 admin roles
Plan for password policies and authentication
Understand Zero Trust security
Configure Self-service password reset (SSPR) for Azure AD
Deploy Azure AD Smart Lockout

Identity Synchronization and Protection

Plan for directory synchronization
Understand Azure AD Connect
Configure Azure AD Connect prerequisites
Manage users and groups with directory synchronization
Active Directory federation
Enable Azure Identity Protection

Identity and Access Management

Conditional access concepts
Conditional access policies
Plan for device compliance
Configure conditional users and groups
Role based access control (RBAC)
Understand identity governance
Configure and use Privileged Identity Management
Activate and deactivate PIM roles
PIM resource workflows
View audit history for Azure AD roles in PIM

Security in Microsoft 365

Identify techniques attackers use to compromise user accounts through email
Identify techniques attackers use to gain control over resources
Identify threats that can be avoided by using EOP and Microsoft Defender for Office 365
Understand Secure Score and what kind of services can be analysed.
Implement Secure Score to identify gaps in your current Microsoft 365 security posture

Threat Protection

Anti-malware Analysed in Exchange Online Protection
Safe Attachments to block zero-day malware in email attachments and documents
Safe Links to protect users from malicious URLs
Microsoft Defender for Identity
Microsoft Defender for Endpoint

Threat Management

Understand Threat Explorer
Implement Security Dashboard
Understand Advanced Thread Analytics (ATA)
Deploy ATA
Configure ATA
Use the attack simulator in Microsoft 365
Understand how Azure Sentinel can used for Microsoft 365

Microsoft Cloud Application Security

Understand Cloud App Security
Deploy Cloud App Security
Control Cloud Apps with Policies
Implement the Cloud App Catalog
Implement the Cloud Discovery dashboard
Manage cloud app permissions

Mobility

Mobile application considerations
Manage devices with MDM
Configure Domains for MDM
Manage Device Security Policies
Enrol devices to MDM
Configure a Device Enrolment Manager Role

Information Protection and Governance

Information protection concepts
Configure sensitivity labels
Configure archiving and retention
Retention policies in the Microsoft 365 Compliance Center
Retention tags and policies
Implement Records Management

Rights Management and Encryption

Microsoft 365 Encryption Options
Understand the use of S/MIME
Implement Office 365 Message Encryption

Data Loss Prevention

Understand Data Loss Prevention
Use policy templates to implement DLP policies
Configure the correct rules for protecting content
Understand how to modify existing rules of DLP policies
Configure the user override option to a DLP rule
Understand how SharePoint Online creates crawled properties from documents

Compliance Management

Understand how to use compliance score to make organizational decisions
Understand how assessments are used to determine compliance score

Insider Risk Management

Implement Insider Risk Management in Microsoft 365
Configure and approve privileged access requests for global administrators
Configure and use information barriers to conform to organizational regulations
Build ethical walls in Exchange Online
Configure Customer Lockbox

Discover and Respond

Conduct content searches in Microsoft 365
Perform an audit log investigation
Configure Microsoft 365 for audit logging
Use Advanced eDiscovery

Have any questions?

Give one of our expert staff a call.

01905 726222

Course tailoring service

Our tailoring service is a luxury you can afford, allowing you to combine elements of related courses producing a bespoke solution, designed specifically to fulfil your training needs. Is there any better way to meet all of your training objectives and maximise your training ROI?

Kit supply

Running a course at your facilities might sound like a good idea until you start thinking about the practicalities of equipment usage and the impact this could have on day to day business, so why not let us bring the necessary equipment with us?

CONTACT US

☎ 01905 726222
✉ info@neos-it-training.com
www.neos-it-training.com