Copilot für Microsoft 365 für Administratoren (MS-4006)

Dieser Kurs beginnt mit der Überprüfung des Microsoft Copilot für Microsoft 365-Designs. Das Hauptaugenmerk liegt jedoch auf den Sicherheits- und Compliancefunktionen, die Administratoren im Microsoft 365-Mandanten konfigurieren müssen, um die Organisationsdaten ihres Unternehmens zu schützen, bevor sie Copilot für Microsoft 365 implementieren.

INHALTE

Examine the Copilot for Microsoft 365 design

- Examine the Copilot for Microsoft 365 logical architecture
- Examine the key components of Copilot for Microsoft 365
- Explore the Copilot for Microsoft 365 service and tenant architecture
- Extend Copilot for Microsoft 365 with Microsoft Graph connectors

Implement Copilot for Microsoft 365

- Get ready for Copilot for Microsoft 365
- Prepare your data for searches in Copilot for Microsoft 365
- Protect your Copilot for Microsoft 365 data with Microsoft 365 security tools
- Assign your Copilot for Microsoft 365 licenses
- Drive Copilot for Microsoft 365 adoption with a Copilot Center of Excellence

Examine data security and compliance in Copilot for Microsoft 365

- Examine how Copilot for Microsoft 365 uses your proprietary business data
- Examine how Copilot for Microsoft 365 protects sensitive business data
- Examine how Copilot for Microsoft 365 uses Microsoft 365 isolation and access controls
- Examine how Copilot for Microsoft 365 meets regulatory compliance mandates

Manage secure user access in Microsoft 365

- Examine the identity and access tools used in Microsoft 365
- Manage user passwords

PREIS P. P.

€ 690,- (zzgl. MwSt.)

DAUER

1 Tag (09:00 - 17:00 Uhr)

SIE HABEN FRAGEN?

+43 50 4510-0

E-Mail Anfrage: office@tectrain.at

https://www.tectrain.at/seminare/microsoft-technisch/microsoft-copilot/copilot-fuer-microsoft-365-fuer-administratoren

- Implement Conditional Access policies
- Enable pass-through authentication
- Implement multifactor authentication
- Enable passwordless sign-in with Microsoft Authenticator
- Explore self-service password management
- Explore Windows Hello for Business
- Implement Microsoft Entra Smart Lockout
- Explore Security Defaults in Microsoft Entra ID
- Investigate authentication issues using sign-in logs

Explore threat intelligence in Microsoft Defender XDR

- Explore Microsoft Intelligent Security Graph
- Explore alert policies in Microsoft 365
- Run automated investigations and responses
- Explore threat hunting with Microsoft Threat Protection
- Explore advanced threat hunting in Microsoft Defender XDR
- Explore threat analytics in Microsoft 365
- Identify threat issues using Microsoft Defender reports

Implement data classification of sensitive information

- Explore data classification
- Implement data classification in Microsoft 365
- Explore trainable classifiers
- Create and retrain a trainable classifier
- View sensitive data using Content explorer and Activity explorer
- Detect sensitive information documents using Document Fingerprinting

Explore sensitivity labels

- Manage data protection using sensitivity labels
- Explore what sensitivity labels can do
- Determine a sensitivity label's scope
- Apply sensitivity labels automatically
- Explore sensitivity label policies

Implement sensitivity labels

- Plan your deployment strategy for sensitivity labels
- Examine the requirements to create a sensitivity label
- Create sensitivity labels
- Publish sensitivity labels
- Remove and delete sensitivity labels

ZIELGRUPPE

Administratoren, Microsoft 365-Administratoren oder Personen, die die Microsoft 365-Administratorrolle anstreben und mindestens einen der rollenbasierten Microsoft 365-Zertifizierungspfade für Administratoren abgeschlossen haben.

ABSCHLUSS

Nach Seminarabschluss erhalten Sie ein tecTrain-Teilnahmezertifikat.