Microsoft 365 Security Administrator (MS-500)

Course: **00095**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Software Application Security**
Price: **3895,00 €**

About Course

This Microsoft 365 Security Administrator course will teach you how to secure user access to your organization's resources. First, the course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to set up and use Azure AD (Active Directory) Connect, and introduces you to conditional access in Microsoft 365. Second, you will learn about threat protection technologies that help protect your Microsoft 365 environment. Specifically, you will learn about threat vectors and Microsoft's security solutions to mitigate threats. You will learn about Secure Score, Exchange Online Protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and threat management. Third, the course will teach you about information protection technologies that help secure your Microsoft 365 environment. For example, the course discusses information rights-managed content, message encryption, labels, policies, and rules that support data loss prevention and information protection. Lastly, you will learn about archiving and retention in Microsoft 365, data governance, and how to conduct content searches and investigations. This course covers data retention policies and tags, in-place records management for SharePoint, email retention, and how to conduct content searches that support eDiscovery investigations

What you'll learn

- 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.
- Manage GDPR (General Data Protection Regulation) data subject requests.
- Explain and use sensitivity labels.
- Continue learning and face new challenges with after-course one-on-one instructor coaching.

Pre-requisites

- Basic conceptual understanding of Microsoft Azure
- Experience with Windows 10 devices
- 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

Curriculum

Module 1: User and Group Management

- Identity and Access Management concepts
- The Zero Trust model

- Plan your identity and authentication solution
- User accounts and roles
- Password Management

Module 2: Identity Synchronization and Protection

- Plan directory synchronization
- Configure and manage synchronized identities
- Azure AD Identity Protection

Module 3: Identity and Access Management

- Application Management
- Identity Governance
- Manage device access
- Role-Based Access Control (RBAC)
- Solutions for external access
- Privileged Identity Management

Module 4: Security in Microsoft 365

- Threat vectors and data breaches
- Security strategy and principles
- Microsoft security solutions
- Secure Score

Module 5: Threat Protection

- Exchange Online Protection
- Manage Safe Attachments
- Manage Safe Links
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint

Module 6: Threat Management

- Security dashboard
- Threat investigation and response
- Azure Sentinel
- Advanced Threat Analytics

Module 7: Microsoft Cloud Application Security

- Deploy Cloud Application Security
- Use cloud application security information

Module 8: Mobility

- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Deploy mobile device services
- Enroll devices in Mobile Device Management

Module 9: Information Protection and Governance

- Information protection concepts
- Governance and Records Management
- Sensitivity labels
- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention policies in the Microsoft 365 Compliance Center
- Archiving and retention in Exchange
- In-place records management in SharePoint

Module 10: Rights Management and Encryption

- Information Rights Management (IRM)
- Secure Multipurpose Internet Mail Extension (S-MIME)
- Office 365 Message Encryption

Module 11: Data Loss Prevention

- Data loss prevention fundamentals

- Create a DLP (Data Loss Prevention) policy
- Customize a DLP policy
- Create a DLP policy to protect documents

Module 12: Compliance Management

- Compliance center

Module 13: Insider Risk Management

- Insider Risk
- Privileged Access
- Information barriers
- Building ethical walls in Exchange Online

Module 14: Discover and Respond

- Content Search
- Audit Log Investigations
- Advanced eDiscovery