INFOSECTRAIN

Microsoft 365 Security Administration

TRAINING & CERTIFICATION

www.infosectrain.com

Course description

Our Microsoft 365 Security Administration course is designed to provide you with the fundamental knowledge of various processes and methodologies applied to effectively secure and manage user access to an organization's resources and digital assets. This course covers a wide range of topics like user password protection, user authentication, multi-factor authentication, enabling Azure Identity Protection, introduction to conditional access in Microsoft 365 environment, setting up and using Azure AD Connect, and much more!

Dive deep into threat protection technologies that help to protect your Microsoft 365 environment in this amazing Microsoft 365 Security Administration training program. Learn about threat vectors & Microsoft's security solutions to mitigate threats. Learn about Secure score, Exchange online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and threat management. You will also be able to crack the MS-500 certification exam after completing this course as all the exam fundamentals are covered effectively in this course.

Target Audience

- Microsoft Security Administrators
- Microsoft 365 Enterprise Administrator
- Network Administrators
- Server Administrators

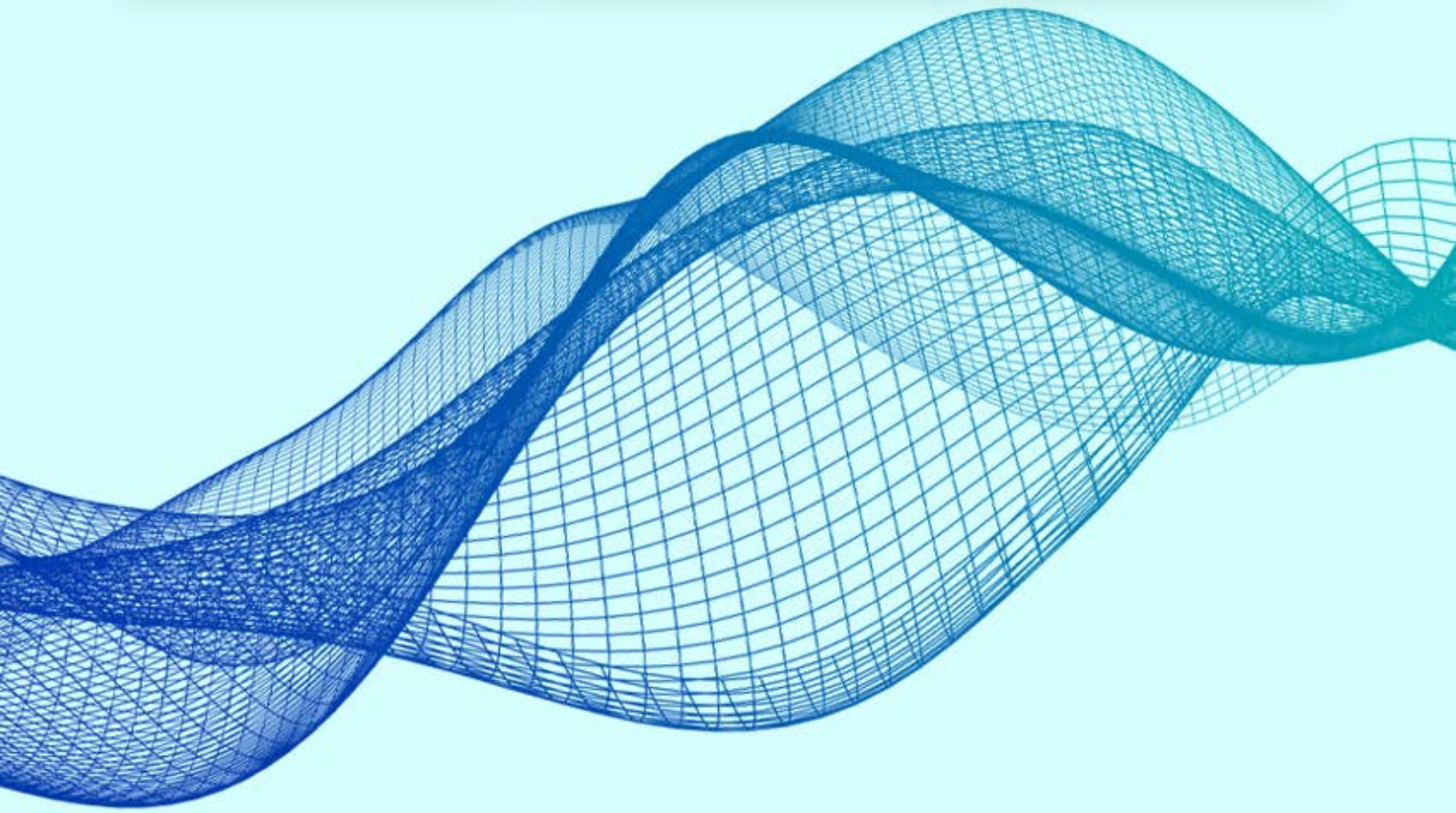
Prerequisites

- Basic Conceptual Understanding of Microsoft Azure
- Experience with Office 365
- User understanding of Windows 10 OS & devices
- Fundamental Understanding of Authorization and Authentication
- Basic Knowledge of Computer Networks
- Working experience with managing mobile devices

INFOSECTRAIN

Why Infosec Train?

Certified & Experienced Instructor	Flexible Schedule	Access to the recorded sessions
Post Training Support	Tailor Made Training	4 hrs/day in Weekend/ Weekday



Course Content

INFOSECTRAIN

Module 1: User & Group Protection

- Identity & Access Management Concepts
- Zero Trust Security
- User Accounts in Microsoft 365
- Administrator Roles and Security Groups in Microsoft 365
- Password Management in Microsoft 365
- Azure AD Identity Protection
- Lab : Initialize your trial tenant
- Set up your Microsoft 365 tenant
- Lab : Configure Privileged Identity Management
- Discover and Manage Azure Resources
- Assign Directory Roles
- Activate and Deactivate PIM Roles
- Directory Roles (General)
- PIM Resource Workflows
- View audit history for Azure AD roles in PIM

Module 2: Identity Synchronization

- Introduction to Identity Synchronization
- Planning for Azure AD Connect
- Implementing Azure AD Connect
- Managing Synchronized Identities
- Introduction to Federated Identities
- Lab : Implement Identity Synchronization
- Set up your organization for identity synchronization

Module 3: Access Management

- Conditional access
- Manage device access
- Role Based Access Control (RBAC)
- Solutions for external access
- Lab: Use Conditional Access to enable MFA
- MFA Authentication Pilot (require MFA for specific apps)
- MFA Conditional Access (complete an MFA roll out)

Module 4: Security in Microsoft 365

- Threat vectors and data breaches
- Security strategy and principles
- Security solutions in Microsoft 365
- Microsoft Secure Score
- Lab: Use Microsoft Secure Score
- Improve your secure score in the Microsoft 365 Security Center

Module 5: Advanced Threat Protection

- Exchange Online Protection
- Office 365 Advanced Threat Protection
- Manage Safe Attachments
- Manage Safe Links
- Azure Advanced Threat Protection
- Microsoft Defender Advanced Threat Protection
- Lab: Manage Microsoft 365 Security Services
- Implement ATP Policies

Module 6: Threat Management

- Use the Security dashboard
- Microsoft 365 threat investigation and response
- Azure Sentinel for Microsoft 365
- Configuring Advanced Threat Analytics
- Lab: Using Attack Simulator
- Conduct a simulated Spear phishing attack
- Conduct simulated password attacks

Module 7: Mobility

- Plan for Mobile Application Management
- Plan for Mobile Device Management
- Deploy Mobile Device Management
- Enroll Devices to Mobile Device Management
- Lab: Configure Azure AD for Intune
- Enable Device Management
- Configure Azure AD for Intune
- Create Intune Policies

Module 8: Information Protection

- Information Protection Concepts
- Azure Information Protection
- Advanced Information Protection
- Windows Information Protection
- Lab: Implement Azure Information Protection and Windows Information Protection
- Implement Azure Information Protection
- Implement Windows Information Protection

Module 9: Rights Management & Encryption

- Information Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption
- Lab: Configure Office 365 Message Encryption
- Configure Office 365 Message Encryption
- Validate Information Rights Management

Module 10: Data Loss Prevention

- Data Loss Prevention Explained
- Data Loss Prevention Policies
- Custom DLP Policies
- Creating a DLP Policy to Protect Documents
- Policy Tips
- Lab: Implement Data Loss Prevention policies
- Manage DLP Policies
- Test MRM and DLP Policies

Module 11: Cloud Application Security

- Cloud App Security Explained
- Using Cloud Application Security Information

Module 12: Compliance in Microsoft 365

- Plan for compliance requirements
- Build ethical walls in Exchange Online
- Manage Retention in Email
- Troubleshoot Data Governance

Module 13: Archiving & Retention

- 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
- Lab: Compliance and Retention
- Initialize Compliance
- Configure retention tags and policies

Module 14: Content Search and Investigation

- Content Search
- Audit Log Investigations
- Advanced eDiscovery
- Lab: Manage Search and Investigation
- Investigate your Microsoft 365 Data
- Conduct a Data Subject Request

www.infosectrain.com | sales@infosectrain.com