Azure and Microsoft Security Services

Duration: 6 days

Module 1 : Azure Identity and Governance Services

- Intro of Azure Active Directory
- Users and Groups
- Administer hybrid identity solutions, integrating on-premises and cloud environments.
- Introduction to Identity Synchronization
- Planning for Azure AD Connect
- Implementing Azure AD Connect
- Managing Synchronized Identities
- Subscriptions and Accounts
- Azure Policy and compliance
- Role-based Access Control (RBAC)
- Conditional access policies based on compliance and security requirements.
- Configure and Deploy Azure Multi-Factor Authentication (MFA)

Module 2: Azure Network

- Establish inter site connectivity through VNet peering
- VPN Gateway connections
- ExpressRoute
- Virtual WAN.

Module 3: network security Service

- Understand cloud security
- Build a network
- Secure network
- Implement host security
- Implement platform security
- Implement subscription security
- Security Operations Lessons
- Configure security policies by using Azure Security Center
- Manage security alerts
- Create security baselines

Module 4 Azure AVD service

- Windows Virtual Desktop Architecture
- Design the WVD architecture
- Design for user identities and profiles
- Understand Windows Virtual Desktop Components
- Understand personal and pooled desktops
- Recommend an operating system for a WVD implementation

- Plan a host pools architecture
- Implement and manage networking for WVD
- Implement and manage storage for WVD
- Create and configure host pools and session hosts
- Create and manage session host image

Module 5 Azure incident detection and response tools

- Introduction to Azure Sentinel
- Create and manage Azure Sentinel workspaces
- Query logs in Azure Sentinel
- Use watchlists in Azure Sentinel
- Utilize threat intelligence in Azure Sentinel
- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment

Module 6: Implement Windows 10 security enhancements with Microsoft Defender for Endpoint

Manage alerts and incidents in Microsoft Defender for Endpoint

- Perform device investigations in Microsoft Defender for Endpoint
- Perform actions on a device using Microsoft Defender for Endpoint
- Perform evidence and entities investigations using Microsoft Defender for Endpoint
- Configure and manage automation using Microsoft Defender for Endpoint
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Utilize Threat and Vulnerability Management in Microsoft Defender for Endpoint

Module 7: Mitigate threats using Microsoft 365 Defender

- Introduction to threat protection with Microsoft 365
- Mitigate incidents using Microsoft 365 Defender
- Protect your identities with Azure AD Identity Protection
- Remediate risks with Microsoft Defender for Office 365
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Cloud App Security
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft 365
- Mitigate threats using Azure Defender
- Plan for cloud workload protections using Azure Defender
- Explain cloud workload protections in Azure Defender
- Connect Azure assets to Azure Defender
- Connect non-Azure resources to Azure Defender
- Remediate security alerts using Azure Defender

Module 8: MDM with Intune

- Plan Licensing and product requirements and capabilities
- Mobile device management strategy cloud vs hybrid
- Identity strategy – Users / Groups
- Physical device considerations BYOD / CYOD
- Use of the Intune Portals
- Compliance
- Compliance in Intune
- Create a compliance policy
- Using multiple compliance policies
- Configuration
- Configuration in Intune
- Windows
- Software
- Computer Management
- Common device settings