SC - 5002 : Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

Course Outline

Module 1: Filter Network Traffic with a Network Security Group (NSG) Using the Azure Portal

- Understand the purpose and benefits of Network Security Groups (NSGs) for filtering network traffic
- Learn to create and configure NSGs to enforce access controls for Azure resources
- Use NSGs to allow or deny specific traffic based on source, destination, and port
- Prioritize NSG rules and leverage NSG flow logs for monitoring and troubleshooting
- Implement network security best practices with NSGs in Azure

Module 2: Create a Log Analytics Workspace for Microsoft Defender for Cloud

- Understand the role of a centralized logging solution with Azure Log Analytics workspace
- Create and configure a Log Analytics workspace in Azure
- Collect and analyze security data from Microsoft Defender for Cloud within the workspace
- Create custom queries and alerts for proactive security threat detection
- Integrate Log Analytics with other Azure services and tools for enhanced security management

Module 3: Set Up Microsoft Defender for Cloud

- Explore the features and benefits of Microsoft Defender for Cloud, including the Microsoft Security Benchmark and Security Recommendations
- Leverage Defender for Cloud Secure Score to monitor, protect, and improve cloud security
- Use the MITRE Attack Matrix to identify attack techniques and prioritize security efforts
- Understand Brute Force Attacks and implement preventive measures
- Implement Just-in-Time Virtual Machine access controls for enhanced security

Module 4: Configure and Integrate a Log Analytics Agent and Workspace in Defender for Cloud

- Learn the importance of centralized log collection and analysis in Microsoft Defender for Cloud
- Configure and deploy the Log Analytics agent in Azure
- Create and configure a Log Analytics workspace for Defender for Cloud
- Integrate the Log Analytics workspace with Defender for Cloud to collect and analyze security logs
- Leverage centralized log analytics for proactive security monitoring and threat detection

Module 5: Configure Azure Key Vault Networking Settings

- Understand the importance of securing Azure Key Vault access through networking settings
- Configure network access control using virtual network service endpoints and private endpoints
- Set up firewall rules and virtual network service endpoints to restrict Key Vault access
- Configure private endpoints for secure access from virtual networks
- Enhance overall security with properly configured networking settings for Azure Key Vault

Module 6: Connect an Azure SQL Server Using an Azure Private Endpoint

- Explore the benefits of using Azure Private Endpoint for secure connections to Azure SQL Server
- Configure and create an Azure Private Endpoint for Azure SQL Server in the Azure portal
- Understand the network architecture and components involved in setting up the Private Endpoint
- Validate and test the connection between the Azure Private Endpoint and Azure SQL Server
- Secure database connections and isolate network traffic with Azure Private Endpoint