Course content for Customized Training

Azure Multi-Tenant Architecture Model; Microsoft Defender for Endpoint & Intune

Duration: 24 hours

Lab - SC-200

Table of Contents

Module 1: Azure Multi-Tenant Architecture

1. **Introduction to Multi-Tenant Architecture in Azure**
    a. What is Multi-Tenancy?
    b. Benefits of Multi-Tenant Solutions
    c. Multi-Tenant vs. Single-Tenant
2. **Key Concepts of Multi-Tenancy in Azure**
    a. Tenant Isolation
    b. Data Partitioning Strategies
    c. Security and Compliance Considerations
    d. Scalability and Performance Optimization
3. **Multi-Tenant Deployment Models**
    a. Shared Database, Shared Schema
    b. Shared Database, Separate Schemas
    c. Dedicated Database per Tenant
    d. Dedicated Infrastructure per Tenant
4. **Azure Services for Multi-Tenant Architectures**
    a. Azure Active Directory (Azure AD) for Tenant Management
    b. Azure App Service for Hosting Multi-Tenant Applications
5. **Security and Compliance in Multi-Tenant Environments**
    a. Authentication and Authorization (Azure AD, OAuth, OpenID)
    b. Role-Based Access Control (RBAC) and Permissions
    c. Data Encryption (At-Rest and In-Transit)
    d. Compliance Standards (ISO, GDPR, HIPAA)

Module 2: Microsoft Defender for Endpoint

1. **Introduction to Microsoft Defender for Endpoint**
2. **Module 1: Protect Against Threats with Microsoft Defender for Endpoint**
    - Overview of Threat Protection
    - Threat Detection and Response
    - Real-time Threat Monitoring
3. **Module 2: Deploy the Microsoft Defender for Endpoint Environment**
    - Deployment Considerations
    - Prerequisites and Setup
    - Configuration Steps
4. **Module 3: Implement Windows Security Enhancements**
    - Security Policies and Configurations
    - Windows Defender Features
    - Endpoint Hardening Strategies
5. **Module 4: Perform Device Investigations**
    - Investigating Device Security Events
    - Log Analysis and Forensics
    - Incident Response Actions
6. **Module 5: Perform Actions on a Device**
    - Quarantine and Isolation
    - Running Remote Actions
    - Remediation Steps
7. **Module 6: Perform Evidence and Entities Investigations**
    - Analyzing Security Events
    - Investigating Suspicious Activities
    - Correlating Security Data
8. **Module 7: Configure and Manage Automation**
    - Security Automation Strategies
    - Using Playbooks for Automated Responses
    - Configuring Automated Threat Mitigation
9. **Module 8: Configure Alerts and Detections**

- Setting Up Alert Rules
- Fine-tuning Detection Mechanisms
- Customizing Alert Notifications

10. **Module 9: Utilize Vulnerability Management**
    - Vulnerability Assessment Techniques
    - Managing Security Patches and Updates
    - Risk Mitigation Strategies

Module 3: Microsoft Intune (Mobile Device Management)

1. **Introduction to Microsoft Intune**
2. **Module 1: Plan for Microsoft Intune**
    - Licensing and Product Requirements
    - Cloud vs. Hybrid MDM Strategy
    - Identity and Device Management Strategies
    - Physical Device Considerations (BYOD / CYOD)
    - Intune Portal Overview and License Assignment
3. **Module 2: Compliance**
    - Understanding Compliance Policies
    - Creating and Managing Compliance Policies
    - Enforcing Security Standards (PIN, Encryption, etc.)
4. **Module 3: Configuration**
    - Device Configuration in Intune
    - Managing Different Platforms (Android, iOS, Windows, Mac)
    - Software and Policy Management
    - Common Device Settings and Security Configurations
5. **Module 4: Managing Applications and Updates**
    - Mobile Application Management (MAM)
    - App Deployment and Distribution
    - Software Updates and Patch Management

6. **Module 5: Enrolling Devices, Alerts, Troubleshooting, and Reporting**
    - Device Enrollment Process
    - iOS Certificates and Configuration
    - Understanding and Managing Alerts
    - Reporting and Insights
    - Troubleshooting Common Issues
7. **Module 6: Monitoring and Reporting**
    - Advanced Monitoring Features
    - Generating and Analyzing Reports
    - Best Practices for Security and Compliance Monitoring
8. **Module 7: Intune as Part of the Enterprise Mobility and Security Product Suite**
    - Integration with Azure Active Directory
    - Azure Information Protection
    - Microsoft Cloud App Security
    - Microsoft Advanced Threat Analytics
    - Microsoft Identity Manager