Azure Security Training

Duration : 4 Days

Day 1: Azure Security Fundamentals & Identity Management

1. **Introduction to Azure Security**
    - Overview of Azure Security Architecture
    - Shared Responsibility Model in the Cloud
    - Importance of Security Posture Management
2. **Azure Identity and Access Management (IAM)**
    - Understanding Azure Active Directory (Azure AD)
    - Multi-Factor Authentication (MFA)
    - Role-Based Access Control (RBAC) for Resource Management
    - Best Practices for Managing Identities
3. **Azure Security Tools Overview**
    - Azure Security Center
    - Microsoft Defender for Cloud
    - Azure Sentinel
    - Azure Policy
4. **Hands-on Lab:**
    - Configuring Azure Security Center
    - Security Posture Assessment

Day 2: Network Security & Threat Protection

5. **Network Security in Azure**
    - Network Security Groups (NSGs)
    - Azure Firewall Configuration
    - Application Gateway and Web Application Firewall (WAF)
6. **Threat Detection and Response**
    - Microsoft Defender for Cloud Workloads
    - Integration with Microsoft Defender for Endpoint Protection
    - Using Azure Sentinel for Threat Detection and Analysis

7. **Policy Enforcement & Compliance**
    - Azure Policy for Enforcing Compliance
    - Azure Blueprints for Policy Templates
    - Continuous Compliance Monitoring
8. **Hands-on Lab:**
    - Configuring Azure Firewall and NSGs
    - Threat Detection with Microsoft Defender for Cloud

Day 3: Data Security & Encryption

9. **Data Protection in Azure**
    - Encryption at Rest and in Transit
    - Azure Key Vault for Managing Secrets
    - Azure Storage Security Settings
10. **Automated Security Workflows**
    - Automated Workflows using Logic Apps
    - Setting Up Alerts and Notifications
11. **Incident Investigation & Response**
    - Investigating Incidents with Azure Sentinel
    - Configuring Defender for Cloud
    - Setting Up an Azure Sentinel Workspace
    - Analyzing Sample Incidents and Responding
12. **Hands-on Lab:**
    - Configuring Azure Key Vault for Secrets Management
    - Incident Response with Azure Sentinel

Day 4: Cloud Data Governance & Advanced Security Measures

13. **Cloud Data Governance & Compliance**
    - Data Governance Policies in Cloud
    - Microsoft Cloud Security Benchmark
    - Microsoft CASB
14. **Key Management & Data Protection**

- Key Storage, BYOK, and HSM in Cloud
- Remote Key Management Service & Client-Side Key Management
- Data Security Lifecycle in Cloud
- Data Encryption & Key Management Interoperability Protocol (KMIP)

15. **Data Loss Prevention & Compliance Monitoring**
    - DLP Incidents Investigation on Purview Portal
    - Ensuring Compliance with Security Best Practices
16. **Hands-on Lab:**
    - Implementing Cloud Data Governance Policies
    - Investigating DLP Incidents with Purview