RLearning solution private limited
PH +9342843527

AZ-500 Microsoft Azure Security Engineer (Security Technologies)

Course Overview:

The 5-Day Instructor-Led training on Microsoft Azure Security Engineer gives the In-Depth knowledge to Implement, Manage, and monitor Security for resources in Microsoft Azure, Multi-Cloud and Hybrid Microsoft Azure Infrastructure.

In this course participants will learn how to Secure End to End Azure Infrastructure with Multi-Cloud and Hybrid, Participants can Learn Deeply How to Secure Identity, Networks, Applications, and Data

The course will be delivered using the use-cases and Real-world examples this will help participants to learn concepts, using this participant can do the following:

- Managing the security posture.
- Identifying and remediating vulnerabilities.
- Performing threat modelling.
- Implementing threat protection.

Module-1: Architecture of Microsoft Azure with Microsoft Azure security Technologies

- Cloud Security Threats
- Zero Trust Security Principles
- A Big Picture with All the Azure Security Technologies (end to end Integration)

Module-2: Securing Identities in Microsoft Entra ID

- Architecture of Entra ID

- Cloud and Hybrid Identity
- Default and Custom Domain
- Authentication options
- Securing Cloud and hybrid identities
- Multifactor Authentication
- Conditional Access
- Protecting Sign-in risk
- Microsoft Entra PHS, PTA and Federation
- Password Less Authentication and password protection
- Privileged Identity Management
- Manage Service principals and Managed Identities
- App registrations and Permissions Consent
- Microsoft Entra ID Application Proxy
- Azure Role Based Access Controls
- Builtin and custom Roles
- Identity Life Cycle Management
- Life Cycle Workflows
- Access Reviews

Labs:

- Muti-factor Authentication
- Conditional Access
- Implementing Sign-in risk, User-Risk
- Implementing PHS, PTA, Federated Authentication and Security

Module -3 Securing Networking

- Securing Subnets and Virtual machines Network Security Group
- Securing Web Applications with WAF (Web Application Firewall)
- Securing the Entire VNET using Azure Firewall Appliance
- Securing the Content delivery Network with Azure Front door
- Securing Networks from DDOS Attack (DDOS protection)

Labs:

- Network Security Group
- Web Application Firewall
- Azure Firewall Appliance
- DDOS Protection

Module-4 Secure Compute, Storage, and Databases

- Securing Disk using Azure Disk Encryption
- Securing Azure Kubernetes Services and Azure Container Services
- Securing Azure Storage Accounts
  - Access control for Storage Accounts Services
  - Storage Account Keys
  - Shared Access Signature
  - Storage Firewall
- Securing database
  - Data Base Firewall
  - Data Base Always Encryption and Transparent Data Encryption
  - Apply Dynamic Mask

Labs:

- Azure Disk Encryption
- Azure Storage Encryption
- Azure storage Firewall
- Azure Shared Access Signature
- Azure Storage Endpoint
- Data base Encryption and Mask

Module-5: Manage Security Operations

- Azure Governance
- Azure Policy
- Azure key Vault
- Manage Certificates, secrets and keys
- Defender for Different Services
- Assess the incidents and Alerts
- Microsoft defender for cloud
- Assess compliance against security frameworks and Microsoft Defender for Cloud
- Microsoft sentinel and Data Connectors
- Alerts and Incidents in Sentinel

Labs:

Azure Policy
Azure Secrets and keys
Analyze the Security posture of Microsoft azure