Implement end-to-end security controls for cloud and AI workloads

Training Details:

Course Name	Implement end-to-end security controls for cloud and AI workloads
Level	Intermediate
Duration	4 days(8 hrs/day)
Participant background (Prerequisites)	1. Basic understanding of cloud computing and Azure fundamentals (VMs, storage, networking) 2. Knowledge of identity and access concepts (authentication, authorization, RBAC, MFA) 3. Familiarity with core cybersecurity principles (Zero Trust, least privilege, defense-in-depth) 4. Understanding of networking basics (IP, firewalls, VPNs, public vs private access) 5. Some hands-on experience with Azure Portal or security tools
Project Proposed	Labs
Expected Outcome	1. Ability to implement and manage identity and secure access using Microsoft Entra (authentication, PIM, Conditional Access) 2. Skills to secure sensitive data and secrets using Azure Key Vault, storage, and databases 3. Capability to enforce governance, compliance, and least-privilege access using Azure Policy, RBAC, and Defender for Cloud 4. Proficiency in designing and implementing network and infrastructure security controls (Firewall, private endpoints, VM security) 5. Ability to monitor, detect, and respond to threats using Microsoft Defender, Sentinel, and Security Copilot, including emerging AI security practices

Topics	**Number of Days**
Implement end-to-end security controls for cloud and AI workloads	4 days(8hrs/day)
Total	**4 days(8hrs/day)**

www.cloudthat.com
+91-888-000-2200
102, 4th B cross, 5th Block, Koramangala, Industrial Area, Bengaluru, Karnataka 560095.

Module 1: Secure access to resources by using Microsoft Entra

- Manage and implement authentication methods in Microsoft Entra ID
- Implement and configure Privileged Identity Management (PIM)
- Authenticate your API plugin for declarative agents with secured APIs

Module 2: Secure Azure Key Vault with defense in depth for the cloud and AI workloads

- Configure and secure Azure Key Vault
- Manage keys and secrets in Azure Key Vault
- Manage certificates and monitor Azure Key Vault
- Protect Azure Key Vault with Microsoft Defender for Cloud

Module 3: Enforce security governance and regulatory compliance

- Enforce governance with Azure Policy and resource locks
- Configure security controls and remediate recommendations in Defender for Cloud
- Evaluate regulatory compliance in Defender for Cloud
- Manage and right-size RBAC role assignments for least privilege
- Protect backup data with Azure Backup security features
- Implement security controls in infrastructure as code

Module 4: Implement security for Azure Storage for the cloud and AI security engineer

- Describe Azure storage services
- Implement security and manage access for Azure Storage
- Configure network security for Azure Storage
- Implement Microsoft Defender for Storage

Module 5: Implement security for Azure SQL databases

- Configure platform-level security for Azure SQL
- Configure auditing for Azure SQL Database and SQL Managed Instance
- Implement Microsoft Defender for Databases

Module 6: Implement network security controls in Azure

- Segment and isolate Azure workloads using network security controls
- Centralize and enforce traffic inspection using Azure Firewall
- Secure remote and hybrid connectivity using VPN gateways and Microsoft Entra Private Access
- Eliminate public network exposure of Azure PaaS services

Module 7: Implement security for AI

- Secure access for Microsoft Entra Agent Identity
- Analyze AI identity risks using Microsoft Defender XDR

www.cloudthat.com
+91-888-000-2200
102, 4th B cross, 5th Block, Koramangala, Industrial Area, Bengaluru, Karnataka 560095.

- Enable real-time protection for Copilot Studio agents
- Configure AI Gateway security in Microsoft Foundry
- Configure and manage guardrails in Microsoft Foundry
- Protect AI workloads with Microsoft Defender for Cloud
- Enable Defender for AI Services workload protection in Microsoft Defender for Cloud
- Manage agents using Microsoft Agent 365
- Identify AI data risks using Microsoft Purview Data Security Posture Management

Module 8: Implement security for servers and virtual machines

- Implement disk encryption for Azure virtual machines
- Configure trusted launch security features for Azure virtual machines
- Plan and implement Azure Bastion
- Manage security for Arc-enabled hybrid servers
- Implement Microsoft Defender for Servers
- Enable and enforce just-in-time VM access
- Enforce VM security configuration with Azure Machine Configuration

Module 9: Secure Azure application platform services for the cloud and AI security engineer

- Detect container risks using Microsoft Defender for Containers
- Implement security controls for Azure Kubernetes Service
- Implement security controls for Azure Container Registry, Container Instances, and Container Apps
- Implement security controls for Azure Function apps and Logic apps
- Implement security controls for Azure App Services and Web Application Firewall
- Implement API backend security using Azure API Management

Module 10: Manage security posture by using Microsoft Defender for Cloud

- Connect hybrid and multicloud environments to Microsoft Defender for Cloud
- Identify security risks by using Cloud Security Posture Management
- Discover unprotected assets and vulnerabilities by using Microsoft Defender External Attack Surface Management
- Evaluate regulatory compliance in Defender for Cloud
- Enable and configure workload protection plans in Microsoft Defender for Cloud
- Configure Microsoft Defender Vulnerability Management settings for Azure VMs

Module 11: Implement activity and event collection in Microsoft Sentinel

- Create and manage Microsoft Sentinel workspaces
- Manage content in Microsoft Sentinel
- Connect Microsoft services to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel

www.cloudthat.com
+91-888-000-2200
102, 4th B cross, 5th Block, Koramangala, Industrial Area, Bengaluru, Karnataka 560095.

- Implement automation rules and playbooks in Microsoft Sentinel
- Manage data storage and query audit logs in Microsoft Sentinel

Module 12: Deploy and operate Microsoft Security Copilot

- Describe Microsoft Security Copilot
- Configure workspaces for Microsoft Security Copilot
- Manage plugins and agents in Microsoft Security Copilot

www.cloudthat.com
+91-888-000-2200
102, 4th B cross, 5th Block, Koramangala, Industrial Area, Bengaluru, Karnataka 560095.