SC-5009: Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra

Training Details:

Course Name	Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra
Level	Intermediate
Duration	1day(8hrs)
Participant background (Prerequisites)	• Basic understanding of Microsoft Azure services, resource management, and cloud computing concepts. • Familiarity with cybersecurity fundamentals, including threat protection, security monitoring, and governance principles. • Working knowledge of Microsoft Entra ID, authentication, authorization, and Role-Based Access Control (RBAC). • Basic awareness of AI services, generative AI concepts, and AI workloads in Azure environments. • Experience navigating the Azure portal and interpreting security dashboards, alerts, and recommendations.
Project Proposed	Labs
Expected Outcome	• Secure AI workloads and Microsoft Foundry environments using Microsoft Defender for Cloud. • Implement AI governance, guardrails, and runtime threat protection for AI applications. • Manage AI identities and access using Microsoft Entra, managed identities, and RBAC. • Configure Conditional Access and Identity Protection policies to reduce identity-based risks. • Monitor, investigate, and respond to AI and identity security threats using Microsoft Defender XDR and Microsoft Entra security capabilities. • Apply security best practices to build and operate secure AI solutions in Azure.

Topics	**Number of Days**
Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra	1 day(8hrs)
Total	**1 day(8hrs)**

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

Learning Path 1: Protect Microsoft Foundry solutions by using Microsoft Defender for Cloud

Module1: Understand how Microsoft defender for Cloud support AI security and governance in Azure

- Understand AI services in Azure
- Understand AI security risks in Azure
- AI guardrails and protections in Azure
- How Azure security and governance tools support AI workloads

Module 2: Protect AI workloads with Microsoft Defender for Cloud

- Enable the AI workloads plan
- Review insights in the Data and AI security dashboard
- Assess and improve Ai security posture with Cloud security posture Management(CSPM)
- Detect AI threats at runtime with Cloud Workload Protection(CWP)
- Investigate AI security alerts with prompt evidence in Microsoft Defender XDR

Module 3: Configure and manage guardrails in Microsoft Foundry

- Understand guardrails and Microsoft Content safety
- Understand safety controls in Microsoft Foundry
- Try out built-in guardrails
- Create and manage blocklists in Microsoft Foundry
- Configure and apply guardrails in Microsoft Foundry
- Choose and refine the right guardrails for your AI workloads

Module 4: Secure Microsoft Foundry environment

- Control access to Microsoft Foundry with Microsoft Entra ID
- Manage access within Microsoft Foundry projects
- Secure Microsoft Foundry secrets with Aure Key Vault
- Isolate networks with managed virtual network and private link
- Enable diagnostic logging in Microsoft Foundry

Learning Path 2: Secure AI identity infrastructure with Microsoft Entra

Module 1: Understand identity architecture for AI workloads

- Identity as the control layer for AI solutions
- Management plane and data plane access in AI workloads
- Authentication flows for AI endpoints in Microsoft Foundry
- Human and workload identities in AI workloads
- Role assignments and scope in AI environments
- Common identity misconfigurations in AI deployments

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

Module 2: Implement access management for Azure resources

- Assign Azure roles
- Configure custom Azure roles
- Create and configure managed identities
- Access Azure resources with managed identities
- Analyze Azure role permissions
- Configure Azure Key Vault RBAC policies
- Retrieve objects from Azure Key Vault

Module 3: Plan, implement, and administer Conditional Access

- Plan security defaults
- Exercise - Work with security defaults
- Plan Conditional Access policies
- Implement Conditional Access policy controls and assignments
- Exercise - Implement Conditional Access policies roles and assignments
- Test and troubleshoot Conditional Access policies
- Implement application controls
- Implement session management and continuous access evaluation
- Exercise - Configure authentication session controls
- Microsoft Entra Conditional Access Optimization agent

Module 4: Manage Microsoft Entra Identity Protection

- Review identity protection basics
- Implement and manage user risk policy
- Exercise enable sign-in risk policy
- Exercise configure Microsoft Entra multifactor authentication registration policy
- Monitor, investigate, and remediate elevated risky users
- Implement security for workload identities
- Explore Microsoft Defender for Identity
- Explore the Identity Risk Management Agent

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