SC-5004: Defend against cyberthreats with Microsoft Defender XDR

Training Details:

Course Name	Defend against cyberthreats with Microsoft Defender XDR
Level	Intermediate
Duration	1 days (8 hrs/day)
Participant background (Prerequisites)	• Familiarity with investigating • Gathering evidence about attacks on endpoints • Using Microsoft Defender for Endpoint • Using Kusto Query Language (KQL)
Project Proposed	
Expected Outcome	Equip participants with the skills to proactively detect, investigate, hunt, and respond to cyber threats using Microsoft Defender XDR and Microsoft Defender for Endpoint.

Topics	**Number of Days**
	2 days (4 hrs/day)
Total	**2 days (4 hrs/day)**

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

Defend against cyberthreats with Microsoft Defender XDR

Equips security operations analysts with the skills to effectively use Microsoft Defender XDR to protect against sophisticated cyber threats. This one-day instructor-led training covers configuring a Microsoft Defender XDR environment, managing devices and incidents, and performing advanced threat hunting using Kusto Query Language (KQL). Participants will gain hands-on experience in investigating and gathering evidence about attacks on endpoints, enhancing their ability to defend their organization's digital infrastructure

Day 1 (4 hours)

Module 1: Mitigate incidents using Microsoft Defender:

- Introduction
- Use the Microsoft Defender portal
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Microsoft Entra sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics with the Security Copilot Threat Intelligence Briefing Agent
- Analyze reports
- Configure the Microsoft Defender portal

Module 2: Deploy the Microsoft Defender for Endpoint environment

- Introduction
- Create your environment
- Understand operating systems compatibility and features
- Onboard devices
- Manage access
- Create and manage roles for role-based access control
- Configure device groups
- Configure environment advanced features

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

Module 3: Configure for alerts and detections in Microsoft Defender for Endpoint

- Introduction
- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators

Day 2 (4 hours)

Module 4: Configure and manage automation using Microsoft Defender for Endpoint

- Introduction
- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices

Module 5: Perform device investigations in Microsoft Defender for Endpoint

- Introduction
- Use the device inventory list
- Investigate the device
- Use behavioural blocking
- Detect devices with device discovery

Module 6: Defend against Cyberthreats with Microsoft Defender XDR lab exercises

- Introduction
- Configure the Microsoft Defender XDR environment
- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks with Microsoft Defender for Endpoint

Hands-On

- Configure a Microsoft Defender XDR environment
- Manage devices by using Microsoft Defender for Endpoint
- Manage incidents in Microsoft Defender XDR
- Manage investigations on an endpoint

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

- Perform Advanced Hunting with KQL to detect unique threats

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