SC-5004: Defend against cyberthreats with Microsoft Defender XDR Course

Course Duration: 8 Hours **Course code: SC-5004**

1. Course Overview

The **SC-5004: Defend against cyberthreats with Microsoft Defender XDR** course is designed to help security professionals gain practical knowledge of Microsoft Defender XDR and its capabilities in identifying, investigating, and responding to cyberthreats. This course provides a hands-on approach to threat detection, incident response, and security operations, enabling learners to protect organizational assets and ensure a resilient security posture.

2. What You'll Learn?

By the end of this course, you will be able to:

- Understand the core functionalities of Microsoft Defender XDR.
- Detect, investigate, and respond to cyberthreats using XDR tools.
- Correlate threat data across different security services.
- Automate threat detection and response workflows.
- Strengthen organizational security with advanced threat intelligence and reporting.

3. Target Audience

This course is ideal for:

- Security Operations Analysts
- Security Engineers
- Incident Responders
- IT Professionals working in cybersecurity operations
- Microsoft Security administrators managing enterprise defense solutions

4. Pre-Requisites

Before attending this course, learners should have:

- Basic understanding of Microsoft 365 security concepts.
- Knowledge of identity, compliance, and information protection principles.
- Familiarity with general cybersecurity fundamentals and threat landscapes.

5. Course Content

Module 1: Introduction to Microsoft Defender XDR

- Overview of extended detection and response (XDR)
- Key features and capabilities of Microsoft Defender XDR

Module 2: Threat Detection and Investigation

- Configuring threat detection policies
- Investigating alerts and incidents in Defender XDR

Module 3: Responding to Cyberthreats

- Incident response lifecycle
- Automating response with Microsoft Defender XDR

Module 4: Integrating with Microsoft Security Tools

- Microsoft Sentinel and Defender XDR integration
- Enhancing investigations with threat intelligence

Module 5: Advanced Threat Hunting

- KQL queries for hunting activities
- Proactive threat detection scenarios

Module 6: Reporting and Continuous Improvement

- Security posture reporting and dashboards
- Best practices for ongoing threat defense

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com