Defend Against Cyberthreats with Microsoft Defender XDR
SC 5004

Course Name	**Defend Against Cyberthreats with Microsoft Defender XDR**
Course Code	**SC-5004**
Course Duration	1 Day
Course Structure	Instructor-Led
Course Overview	SC-5004: Defend Against Cyberthreats with Microsoft Defender XDR equips delegates with the practical skills required to deploy and operate the Microsoft Defender for Endpoint environment, manage devices, perform investigations, and remediate incidents within Microsoft Defender XDR. The course also delivers comprehensive instruction on the use of Advanced Hunting with Kusto Query Language (KQL) to detect unique and emerging threats. Through structured exercises, delegates will configure the Defender for Endpoint environment, onboard devices, manage alerts and detections, configure automation, and conduct in-depth device investigations. The course concludes with practical lab exercises that consolidate end-to-end response workflows and prepare learners to operationalise extended detection and response (XDR) capabilities in their organisations.
Audience Profile	This course is intended for Security Operations Analysts and security engineers responsible for investigating, responding to, and hunting threats across endpoints and cross-domain attack surfaces. It is appropriate for professionals familiar with investigating endpoint attacks who require deeper expertise in Microsoft Defender for Endpoint and Defender XDR.
Course Prerequisites	Delegates should have experience using the Microsoft Defender portal, a basic understanding of Microsoft Defender for Endpoint and Microsoft Sentinel, and experience using Kusto Query Language (KQL). Access to a Microsoft 365 E5 tenant with a Microsoft Defender for Endpoint P2 licence is required for the exercises.
Course Outcome	Upon successful completion of this course, delegates will be equipped with the skills and knowledge required to: • Mitigate incidents using Microsoft Defender XDR • Deploy the Microsoft Defender for Endpoint environment • Configure alerts, detections, and indicators in Defender for Endpoint • Configure and manage automation in Defender for Endpoint • Perform device investigations using Defender for Endpoint

	• Use Advanced Hunting with KQL to identify unique threats
Assessment/Evaluation	This course prepares delegates for the Microsoft Applied Skills credential SC-5004: Defend Against Cyberthreats with Microsoft Defender XDR. Successful completion of the associated assessment will result in attainment of the credential and a Certificate of Attendance issued by IT-IQ Botswana.

Course Details	
Topic	**Module 1: Mitigate Incidents Using Microsoft Defender** • Unified incident view across Defender products • Triaging incidents • Coordinated response across attack surfaces **Module 2: Deploy the Microsoft Defender for Endpoint Environment** • Onboarding devices • Configuring environmental settings • Validating deployment **Module 3: Configure Alerts and Detections in Defender for Endpoint** • Managing alerts and notifications • Custom indicators • Detection rules and exclusions **Module 4: Configure and Manage Automation in Defender for Endpoint** • Automated investigation and response • Live response sessions • Automation levels and scope

	Module 5: Perform Device Investigations • Device timelines and forensic data • Investigating files, processes, and network activity • Containing and remediating compromised devices **Module 6: Defender XDR Lab Exercises** • End-to-end attack simulation and response • Threat hunting with KQL • Operationalising Defender XDR