Configure SIEM Security Operations Using Microsoft Sentinel
SC-5001

Course Name	**Configure SIEM Security Operations Using Microsoft Sentinel**
Course Code	**SC-5001**
Course Duration	1 Day
Course Structure	Instructor-Led
Course Overview	SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel introduces delegates to the configuration and operation of Microsoft Sentinel as an enterprise security information and event management (SIEM) solution. The course provides comprehensive guidance on configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events, configuring analytics rules, and responding to threats through automated playbooks. Upon completion, delegates will be equipped to deploy Microsoft Sentinel content hub solutions, integrate critical telemetry sources, build effective detection logic, and orchestrate automated response workflows. The course is purposefully aligned to the responsibilities of the Microsoft Security Operations Analyst, with hands-on exercises that reinforce real-world investigation, monitoring, and response practices.
Audience Profile	This course is designed for the Microsoft Security Operations Analyst, who collaborates with organizational stakeholders to secure information technology systems. The role focuses on rapidly remediate active attacks, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. The course is also suitable for security engineers and administrators who participate in the configuration and deployment of Microsoft Sentinel.
Course Prerequisites	Delegates should have a basic understanding of Microsoft 365, Microsoft Azure services, Windows server and client administration, and an introductory understanding of cybersecurity concepts. Familiarity with Kusto Query Language (KQL) is advantageous.
Course Outcome	Upon successful completion of this course, delegates will be equipped with the skills and knowledge required to: • Create and configure a Microsoft Sentinel workspace • Deploy a Microsoft Sentinel content hub solution • Connect Windows hosts and Microsoft services to Microsoft Sentinel

	• Configure analytics rules to detect threats • Configure automation and playbooks for incident response • Operate and tune a Microsoft Sentinel deployment
Assessment/Evaluation	This course prepares delegates for the Microsoft Applied Skills credential: Configure SIEM Operations with Microsoft Sentinel. 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: Configure the Microsoft Sentinel Workspace** • Creating a Log Analytics workspace • Enabling Microsoft Sentinel • Configuring workspace permissions **Module 2: Deploy Sentinel Content Hub Solutions** • Exploring the content hub • Installing solutions and connectors • Managing solution updates **Module 3: Connect Windows Hosts to Microsoft Sentinel** • Configuring data collection rules • Onboarding Windows servers and endpoints • Validating data ingestion **Module 4: Configure Analytics Rules** • Built-in versus custom analytics rules • Scheduled, NRT, and Microsoft security rules • Tuning detections to reduce false positives

	Module 5: Configure Automation in Microsoft Sentinel • Automation rules and playbooks • Integrating Logic Apps • Automating incident enrichment and response **Module 6: Operate Microsoft Sentinel** • Investigating incidents • Hunting for threats • Maintaining and optimising the workspace