SC-200 Practice Test Questions and Answers

1. What is the primary focus of the Microsoft SC-200 certification?

A) Azure infrastructure management

B) Security operations and threat detection using Microsoft security tools

C) Software development practices

D) Database administration

2. Which Microsoft tool is primarily used for security information and event management (SIEM)?

A) Microsoft Defender for Office 365

B) Microsoft Sentinel

C) Azure Active Directory

D) Microsoft Intune

3. In Microsoft Sentinel, what is a playbook used for?

A) Creating user accounts

B) Automating response actions to security incidents

C) Managing network configurations

D) Backing up data

4. What type of queries are used in Microsoft Sentinel for threat hunting?

A) SQL queries

B) KQL (Kusto Query Language) queries

C) PowerShell scripts

D) Python scripts

Answers: 1-B 2-B 3-B 4-B