# COURSE OVERVIEW

**Course Category:**
Security

**Course Name:**
Microsoft Security Operations Analyst
*SC-200T00*

**COURSE DURATION:** 4 Days

**Gauteng**
3rd Floor, 34 Whiteley Road,
Melrose Arch
Johannesburg
2196

**Gauteng**
192 on Bram
192 Bram Fischer Drive
Ferndale, Randburg
Johannesburg
2160

**Cape Town**
3rd Floor, Thomas Pattullo Building
19 Jan Smuts St
Cape Town
8000

**Durban**
9 Mountview Close
Broadlands
Mount Edgecombe
Durban
4302

☎ 087 941 5764

✉ sales@impactful.co.za

🌐 impactful.co.za

## COURSE OVERVIEW

Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender.

In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Azure Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting.

## TARGET AUDIENCE

The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

Delegates need to have a basic understanding of Microsoft 365 and Microsoft security, compliance and identity products as well as familiarity with Azure services.

## DELIVERY METHOD

**Our courses have flexible delivery options:**

- In-person classroom training at the Impactful training facilities in Johannesburg, Durban and Cape Town
- Virtual instructor-led training
- Nationally on-site at the client

IMPACTFUL
Powered by LRMG

## COURSE OUTLINE

**Module 1: Mitigate threats using Microsoft Defender for Endpoint**

- Define the capabilities of Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint environment settings
- Configure Attack Surface Reduction rules on Windows 10 devices
- Investigate alerts in Microsoft Defender for Endpoint
- Describe device forensics information collected by Microsoft Defender for Endpoint
- Conduct forensics data collection using Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Manage automation settings in Microsoft Defender for Endpoint
- Manage indicators in Microsoft Defender for Endpoint
- Describe Threat and Vulnerability Management in Microsoft Defender for Endpoint

**Module 2: Mitigate threats using Microsoft 365 Defender**

- Explain how the threat landscape is evolving.
- Manage incidents in Microsoft 365 Defender
- Conduct advanced hunting in Microsoft 365 Defender
- Describe the investigation and remediation features of Azure Active Directory Identity Protection.
- Define the capabilities of Microsoft Defender for Endpoint.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.
- Define the Cloud App Security framework
- Explain how Cloud Discovery helps you see what's going on in your organisation

**Module 3: Mitigate threats using Azure Defender**

- Describe Azure Defender features
- Explain Azure Security Centre features
- Explain which workloads are protected by Azure Defender
- Explain how Azure Defender protections function
- Configure auto-provisioning in Azure Defender
- Describe manual provisioning in Azure Defender
- Connect non-Azure machines to Azure Defender
- Describe alerts in Azure Defender
- Remediate alerts in Azure Defender
- Automate responses in Azure Defender

### Module 4: Create queries for Azure Sentinel using Kusto Query Language (KQL)

- Construct KQL statements
- Search log files for security events using KQL
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Summarize data using KQL statements
- Render visualizations using KQL statements
- Extract data from unstructured string fields using KQL
- Extract data from structured string data using KQL
- Create Functions using KQL

### Module 5: Configure your Azure Sentinel environment

- Identify the various components and functionality of Azure Sentinel.
- Identify use cases where Azure Sentinel would be a good solution.
- Describe Azure Sentinel workspace architecture
- Install Azure Sentinel workspace
- Manage an Azure Sentinel workspace
- Create a watchlist in Azure Sentinel
- Use KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Use KQL to access threat indicators in Azure Sentinel

### Module 6: Connect logs to Azure Sentinel

- Explain the use of data connectors in Azure Sentinel
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel
- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Azure Sentinel
- Activate the Microsoft 365 Defender connector in Azure Sentinel
- Connect Azure Windows Virtual Machines to Azure Sentinel
- Connect non-Azure Windows hosts to Azure Sentinel
- Configure Log Analytics agent to collect Sysmon events
- Explain the Common Event Format connector deployment options in Azure Sentinel
- Configure the TAXII connector in Azure Sentinel
- View threat indicators in Azure Sentinel

### Module 7: Create detections and perform investigations using Azure Sentinel

- Explain the importance of Azure Sentinel Analytics.
- Create rules from templates.
- Manage rules with modifications.
- Explain Azure Sentinel SOAR capabilities.
- Create a playbook to automate an incident response.
- Investigate and manage incident resolution.
- Explain User and Entity Behaviour Analytics in Azure Sentinel
- Explore entities in Azure Sentinel
- Visualize security data using Azure Sentinel Workbooks.

**Module 8: Perform threat hunting in Azure Sentinel**

- Describe threat hunting concepts for use with Azure Sentinel
- Define a threat hunting hypothesis for use in Azure Sentinel
- Use queries to hunt for threats.
- Observe threats over time with livestream.
- Explore API libraries for advanced threat hunting in Azure Sentinel
- Create and use notebooks in Azure Sentinel