Global Horizon
TRAINING CENTER

Training Course:
Microsoft Sentinel (SIEM & SOAR)

27 September - 1 October 2026
Manama (Bahrain)

Training Course:
Microsoft Sentinel (SIEM & SOAR)

Training Course code: IT236608 From: 27 September - 1 October 2026 Venue: Manama (Bahrain) - Training Course Fees: 5150 Euro

Introduction

Microsoft Sentinel is Microsoft's cloud-native Security Information and Event Management SIEM and Security Orchestration, Automation, and Response SOAR platform. It enables organizations to collect, analyze, detect, investigate, and respond to cyber threats across hybrid and multi-cloud environments through AI-driven analytics, threat intelligence, automation, and integrated incident management. This course provides participants with the practical knowledge required to deploy, configure, monitor, and optimize Microsoft Sentinel to strengthen an organization's Security Operations Center SOC.

Objectives

By the end of this training program, participants will be able to:

- Understand the architecture and capabilities of Microsoft Sentinel.
- Deploy and configure Microsoft Sentinel within Microsoft Azure.
- Connect and manage multiple security data sources.
- Configure data connectors and data ingestion.
- Utilize Log Analytics Workspace effectively.
- Write and optimize Kusto Query Language KQL queries.
- Create analytics rules for threat detection.
- Investigate security incidents using Microsoft Sentinel.
- Perform threat hunting using advanced hunting techniques.
- Automate incident response using Playbooks and Logic Apps.
- Integrate threat intelligence feeds.
- Monitor security posture using Workbooks and Dashboards.
- Implement security best practices and operational procedures.

Target Audience

This course is designed for:

- Security Operations Center SOC Analysts
- Cybersecurity Engineers
- Security Administrators
- Cloud Security Engineers
- Azure Administrators
- Incident Response Teams
- Threat Hunters
- IT Security Professionals

- Security Architects

Outlines

Day 1: Introduction to Microsoft Sentinel

- Overview of SIEM and SOAR Concepts
- Microsoft Security Ecosystem
- Microsoft Sentinel Architecture
- Azure Prerequisites
- Creating Log Analytics Workspace
- Deploying Microsoft Sentinel
- Microsoft Defender Integration
- Licensing and Cost Management
- Security Data Collection Overview

Day 2: Data Collection and Log Management

- Data Connectors
- Azure Native Connectors
- Microsoft 365 Integration
- Microsoft Defender XDR Integration
- Windows Security Events
- Linux Syslog Collection
- Azure Activity Logs
- Custom Log Ingestion
- Common Event Format CEF
- Syslog Configuration
- Data Normalization
- Data Retention Policies

Day 3: Kusto Query Language KQL & Analytics Rules

- Introduction to KQL
- Query Operators
- Filtering and Searching Logs
- Aggregations and Summaries
- Time Series Analysis
- Parsing Security Logs
- Building Custom Queries
- Scheduled Analytics Rules
- Near Real-Time Detection Rules
- Fusion Detection
- Alert Tuning
- Reducing False Positives

Day 4: Incident Investigation & Threat Hunting

- Incident Lifecycle

- Incident Queue Management
- Entity Mapping
- Investigation Graph
- Threat Hunting Methodology
- Hunting Queries
- Bookmarks
- MITRE ATT&CK Framework Mapping
- UEBA User and Entity Behavior Analytics
- Threat Intelligence Integration
- IOC Management
- Case Management Best Practices

Day 5: Automation, SOAR & Best Practices

- Introduction to SOAR
- Microsoft Logic Apps
- Playbook Creation
- Automated Incident Response
- Security Automation Rules
- Approval Workflows
- Ticketing System Integration
- Workbooks and Dashboards
- Security Reporting
- Performance Optimization
- Governance and Compliance
- Microsoft Sentinel Best Practices
- Final Hands-on Lab
- Course Review and Q&A

Registration form on the Training Course: Microsoft Sentinel (SIEM & SOAR)

Training Course code: IT236608 From: 27 September - 1 October 2026 Venue: Manama (Bahrain) - Training Course Fees: 5150 Euro

Complete & Mail or fax to Global Horizon Training Center (GHTC) at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Company Information

Company Name: .....
Address: .....
City / Country: .....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng): .....
Position: .....
Telephone / Mobile: .....
Personal E-Mail: .....
Official E-Mail: .....

Payment Method

- ☐ Please find enclosed a cheque made payable to Global Horizon
- ☐ Please invoice me
- ☐ Please invoice my company

Easy Ways To Register

Telephone: +201095004484 to provisionally reserve your place.	Fax your completed registration form to: +20233379764	E-mail to us : info@gh4t.com or training@gh4t.com	Complete & return the booking form with cheque to:Global Horizon 3 Oudai street, Aldouki, Giza, Giza Governorate, Egypt.