Global Horizon
TRAINING CENTER

Training Course:
Microsoft Intune, Defender & Sentinel Administration

30 August - 10 September 2026
Cairo (Egypt)

Training Course:
Microsoft Intune, Defender & Sentinel Administration

Training Course code: IT236599 From: 30 August - 10 September 2026 Venue: Cairo (Egypt) - Training Course Fees: 6300 Euro

Introduction

As organizations continue to embrace digital transformation, hybrid work, and cloud-based services, securing endpoints, identities, applications, and organizational data has become a strategic priority. Microsoft Intune, Microsoft Defender, and Microsoft Sentinel provide a unified security ecosystem that enables organizations to manage devices, enforce compliance, protect against cyber threats, monitor security events, and automate incident response across enterprise environments.

This comprehensive 10-day training program, developed by Global Horizon Training Center, equips IT professionals with the knowledge and hands-on skills required to deploy, configure, administer, secure, monitor, and optimize enterprise environments using Microsoft Intune, Microsoft Defender, and Microsoft Sentinel. Participants will gain practical experience in modern endpoint management, identity protection, application deployment, device compliance, endpoint security, threat detection, security monitoring, incident investigation, and automated response using Microsoft's integrated security platform.

Objectives

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

- Understand Microsoft Intune architecture and modern endpoint management concepts.
- Configure and manage Microsoft Intune tenant settings and administrative roles.
- Integrate Microsoft Entra ID with Microsoft Intune for identity-based device management.
- Deploy Windows devices using Windows Autopilot.
- Configure device enrollment, configuration profiles, and compliance policies.
- Implement Conditional Access policies based on Zero Trust principles.
- Integrate Microsoft Defender for Endpoint with Microsoft Intune.
- Deploy endpoint security policies including Microsoft Defender Antivirus, Firewall, Attack Surface Reduction ASR, and Endpoint Detection and Response EDR.
- Deploy and manage enterprise applications using Microsoft Intune.
- Implement Microsoft Purview Sensitivity Labels and Endpoint Data Loss Prevention DLP.
- Monitor endpoint health, analyze reports, and troubleshoot deployment issues.
- Deploy and configure Microsoft Sentinel as a cloud-native SIEM and SOAR platform.
- Investigate security incidents, perform threat hunting using Kusto Query Language KQL, and automate incident response using Logic Apps and Playbooks.

Target Audience

This training program is designed for:

- Microsoft Intune Administrators
- Microsoft 365 Administrators
- Security Administrators
- Endpoint Management Engineers
- Infrastructure Engineers
- System Administrators
- Cloud Administrators
- Cybersecurity Engineers
- Security Operations Center SOC Analysts
- IT Professionals responsible for enterprise endpoint management and security operations

Training Program Outline

Day 1: Microsoft Intune Fundamentals & Tenant Setup

- Introduction to Microsoft Intune and Endpoint Management Architecture
- Understanding Mobile Device Management MDM vs. Mobile Application Management MAM
- Microsoft Intune Licensing and Prerequisites
- Navigating the Microsoft Intune Admin Center
- Configuring Tenant Settings and Validating Readiness
- Exploring Administrative Roles and Permissions
- Implementing Role-Based Access Control RBAC
- Assigning and Testing Administrative Access

Day 2: Microsoft Entra ID, Device Enrollment & Windows Autopilot

- Microsoft Entra ID Fundamentals and Identity Integration with Intune
- Understanding Device Identity Types: Entra Joined, Registered, and Hybrid Joined
- Enrollment Prerequisites and Supported Device Scenarios
- Configuring Enrollment Restrictions
- Creating Device and User Groups
- Building Dynamic Membership Rules
- Automating Device Targeting and Testing Registration Workflows
- Windows Autopilot Deployment Concepts and Lifecycle
- Understanding Hardware Hashes and Deployment Preparation
- Creating Deployment Profiles
- Configuring Enrollment Status Page ESP
- Assigning Devices to Autopilot Groups
- Uploading Hardware IDs
- Performing Clean Device Provisioning and Enrollment Validation

Day 3: Device Configuration Profiles & Compliance Policies

- Introduction to Configuration Profiles
- Comparing Settings Catalog and Administrative Templates
- Creating Device Restriction Policies
- Configuring Wi-Fi Deployment Profiles
- Applying User Interface Customization Settings
- Understanding Profile Assignment Logic

- Managing Policy Conflicts and Validation Testing
- Understanding Compliance States and Evaluation Flow
- Creating Compliance Policies for Password Security
- Configuring BitLocker Encryption Validation
- Setting Operating System Version Compliance Requirements
- Compliance Monitoring and Reporting

Day 4: Conditional Access & Microsoft Defender Integration

- Introduction to Conditional Access Architecture
- Applying Zero Trust Access Controls
- Creating Conditional Access Policies Requiring Compliant Devices
- Conditional Access Signals and Decision Engine Processing
- Grant Controls and Session Controls
- Integrating Multi-Factor Authentication MFA
- Building Advanced Access Restriction Scenarios
- Configuring Location-Based Access Rules
- Restricting Unmanaged Device Access
- Testing Conditional Access Behavior
- Troubleshooting Policy Evaluation Results
- Integrating Microsoft Defender for Endpoint with Intune
- Understanding Unified Endpoint Security Management
- Enabling Service-to-Service Connector Integration
- Configuring Endpoint Onboarding Packages
- Deploying Antivirus Security Baselines
- Configuring Firewall Policies
- Validating Device Protection Posture
- Reviewing Endpoint Security Status Reports

Day 5: Application Management, Endpoint Hardening & Data Protection

- Microsoft Store Application Integration
- Understanding Win32 Application Packaging and Deployment
- Creating Application Deployment Assignments
- Configuring Install and Uninstall Commands
- Deploying Applications to Target Groups
- Configuring Attack Surface Reduction ASR Rules
- Introduction to Endpoint Detection and Response EDR
- Validating Application Deployment and Endpoint Hardening Enforcement
- Introduction to Microsoft Purview
- Understanding Data Classification Concepts
- Sensitivity Labels Fundamentals
- Creating and Configuring Sensitivity Labels
- Publishing Label Policies to Users and Groups
- Applying and Testing Label Enforcement
- Understanding Endpoint Data Loss Prevention DLP
- Configuring Basic Endpoint DLP Policies
- Validating Protection and Data Governance Scenarios

Day 6: Monitoring, Reporting & Advanced Troubleshooting

- Navigating Intune Reporting Dashboards

- Understanding Intune Management Extension Logs
- Collecting and Analyzing Device Diagnostics
- Identifying Common Deployment Failures
- Reviewing Microsoft Defender Security Alerts
- Investigating Compliance and Policy Deployment Issues
- Validating Conditional Access Reporting Results
- Performing End-to-End Troubleshooting Exercises
- Reviewing Endpoint Security Best Practices
- Final Practical Lab for Microsoft Intune and Microsoft Defender

Day 7: Microsoft Sentinel Fundamentals

- Introduction to Microsoft Sentinel
- Understanding SIEM and SOAR Concepts
- Microsoft Sentinel Architecture
- Log Analytics Workspace Fundamentals
- Creating and Configuring Sentinel Workspaces
- Connecting Data Sources using Data Connectors
- Integrating Microsoft Defender with Microsoft Sentinel
- Integrating Microsoft 365 Security Services
- Azure Resource Integration
- Third-Party Data Source Integration
- Configuring Data Collection Rules
- Content Hub Overview
- Microsoft Sentinel Workbooks
- Security Dashboards
- Security Monitoring Best Practices

Day 8: Microsoft Sentinel - Threat Detection, Investigation & Threat Hunting

- Understanding Analytics Rules
- Creating Scheduled and Near Real-Time Analytics Rules
- Alert Generation and Correlation
- Incident Management
- Incident Investigation Process
- Entity Mapping
- Investigation Graph
- Threat Intelligence Integration
- Managing Watchlists
- Introduction to Kusto Query Language KQL
- Creating Hunting Queries
- Advanced Threat Hunting Techniques
- MITRE ATT&CK Framework Mapping
- Investigating Advanced Security Threats
- Security Dashboards and Reporting

Day 9: Microsoft Sentinel - Security Automation & Incident Response

- Automation Rules
- Microsoft Logic Apps Integration
- Creating Security Playbooks
- Automated Incident Response

- Security Orchestration SOAR Workflows
- Managing the Incident Lifecycle
- Security Operations Best Practices
- Compliance Reporting
- Performance Optimization
- Advanced Troubleshooting Techniques
- Continuous Security Monitoring
- Threat Response Validation Exercises

Day 10: Microsoft Sentinel - Advanced Operations & Capstone Project

- Advanced Threat Hunting Scenarios
- Threat Intelligence Management
- Security Posture Assessment
- Cross-Platform Security Monitoring
- End-to-End Integration of Microsoft Intune, Microsoft Defender, and Microsoft Sentinel
- Incident Investigation Across the Microsoft Security Ecosystem
- End-to-End Security Monitoring and Response
- Operational Best Practices for Enterprise Security
- Final Hands-on Capstone Lab
- Final Knowledge Assessment
- Course Review and Q&A

Registration form on the Training Course: Microsoft Intune, Defender & Sentinel Administration

Training Course code: IT236599 From: 30 August - 10 September 2026 Venue: Cairo (Egypt) - Training Course Fees: 6300 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.