Azure Sentinel (Microsoft Sentinel) Deployment & Management Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution that fundamentally changes how modern enterprises approach their security operations. In today's volatile digital landscape, where the attack surface spans across on-premises, multicloud, and hybrid environments, traditional SIEM systems are often too slow, complex, and costly. Sentinel's serverless architecture, powered by Artificial Intelligence (AI) and Machine Learning (ML), provides scalable threat detection and automated incident response, enabling Security Operations Center (SOC) teams to cut through the noise and focus on genuine threats. Azure Sentinel (Microsoft Sentinel) Deployment & Management Training Course is engineered to equip Security Analysts, Engineers, and Architects with the practical, hands-on expertise required to successfully deploy, configure, and manage Sentinel, ensuring a robust cloud security posture and maximizing the efficiency of their security workflows.

This course serves as the definitive guide to mastering the entire threat management lifecycle within Microsoft Sentinel. Participants will gain proficiency in data ingestion across diverse sources, writing powerful Kusto Query Language (KQL) queries for proactive threat hunting, configuring analytics rules for high-fidelity alert generation, and deploying security playbooks via Azure Logic Apps for SOAR implementation. The curriculum places a strong emphasis on real-world cloud use cases and MITRE ATT&CK framework mapping, culminating in the ability to design a cost-optimized, enterprise-grade Sentinel solution that delivers unified security visibility and rapid incident response across the organization's entire digital estate.

Programme Curriculum

Azure Sentinel (Microsoft Sentinel) Deployment & Management Training Course

Introduction

Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution that fundamentally changes how modern enterprises approach their security operations. In today's volatile digital landscape, where the attack surface spans across on-premises, multicloud, and hybrid environments, traditional SIEM systems are often too slow, complex, and costly. Sentinel's serverless architecture, powered by Artificial Intelligence (AI) and Machine Learning (ML), provides scalable threat detection and automated incident response, enabling Security Operations Center (SOC) teams to cut through the noise and focus on genuine threats. Azure Sentinel (Microsoft Sentinel) Deployment & Management Training Course is engineered to equip Security Analysts, Engineers, and Architects with the practical, hands-on expertise required to successfully deploy, configure, and manage Sentinel, ensuring a robust cloud security posture and maximizing the efficiency of their security workflows.

This course serves as the definitive guide to mastering the entire threat management lifecycle within Microsoft Sentinel. Participants will gain proficiency in data ingestion across diverse sources, writing powerful Kusto Query Language (KQL) queries for proactive threat hunting, configuring analytics rules for high-fidelity alert generation, and deploying security playbooks via Azure Logic Apps for SOAR implementation. The curriculum places a strong emphasis on real-world cloud use cases and MITRE ATT&CK framework mapping, culminating in the ability to design a cost-optimized, enterprise-grade Sentinel solution that delivers unified security visibility and rapid incident response across the organization's entire digital estate.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Deploy & Configure a resilient and cost-optimized Microsoft Sentinel workspace and Log Analytics environment.
2. Master Data Ingestion by connecting diverse sources using various data connectors.
3. Utilize the Kusto Query Language to perform complex log analysis and advanced proactive threat hunting.
4. Design and implement high-fidelity Analytics Rules and custom detection logic to minimize false positives.
5. Perform effective Incident Management, investigation, and deep-dive analysis using the Investigation Graph and UEBA features.
6. Develop and automate security workflows using SOAR capabilities by creating Logic App Playbooks.
7. Leverage the Content Hub and Solution Templates for rapid deployment of pre-built security content and best practices.
8. Apply MITRE ATT&CK techniques for mapping detections and improving overall security coverage.
9. Integrate Threat Intelligence (TI) feeds to enrich data and enhance the detection of known malicious indicators.
10. Customize and build interactive Workbooks and Dashboards for Security Visualization and operational reporting.
11. Manage and optimize User and Entity Behavior Analytics for detecting insider threats and compromised accounts.
12. Implement Azure Lighthouse for MSSP multi-tenant management and cross-workspace visibility.

13. Configure Watchlists and Parsers for data normalization and query efficiency in the SIEM platform.

Target Audience

1. Security Analysts
2. Security Engineers
3. Cloud Security Architects
4. Incident Responders
5. IT System Administrators
6. Cybersecurity Consultants
7. DevOps/DevSecOps Engineers
8. IT Managers/Directors overseeing security strategy

Course Modules

Module 1: Introduction and Core Architecture

- Microsoft Sentinel, Traditional SIEM and XDR
- Planning the Log Analytics Workspace and data retention/tiering strategy.
- Understanding the Content Hub for content discovery and deployment.
- Cost Management and optimization strategies for large-scale data ingestion.
- Case Study: Analyzing the cost-benefit of migrating from an on-premises SIEM to a cloud-native Sentinel architecture.

Module 2: Data Ingestion and KQL Mastery

- Connecting Microsoft 365 and Azure Services data sources.
- Implementing non-Azure Data Connectors and Agent deployment.
- Advanced Kusto Query Language for data manipulation and log filtering.
- Normalization with Azure Sentinel Information Model Parsers.
- Case Study: Troubleshooting a multi-stage attack by correlating logs from an on-premises firewall and Azure Activity logs using KQL.

Module 3: Threat Detection with Analytics Rules

- Designing and deploying Scheduled Query Rules for custom detection.
- Configuring Fusion and ML Behavior Analytics rules for high-fidelity incidents.
- Leveraging Watchlists and Reference Data to refine detection logic.
- Mapping analytic rules to the MITRE ATT&CK Framework for coverage gaps.
- Case Study: Developing a custom detection rule to identify a specific Ransomware strain's lateral movement technique that bypasses standard anti-virus software.

Module 4: Incident Management and Investigation

- Understanding the Incident Lifecycle from creation to closure.
- Utilizing the Investigation Graph for visual threat analysis and entity relationships.
- Applying User and Entity Behavior Analytics for detecting risky users.
- Managing and integrating Threat Intelligence (TI) feeds for incident enrichment.
- Case Study: Investigating an 'Impossible Travel' incident, utilizing the Investigation Graph to trace the user's activities and determine if a compromised credential was involved.

Module 5: Proactive Threat Hunting

- Developing Proactive Hunting Queries using KQL and the Hunting Dashboard.
- Integrating Jupyter Notebooks for advanced data science-driven threat hunting.
- Utilizing built-in hunting queries and adapting them for a specific environment.
- Identifying "Living off the Land" techniques through log analysis.
- Case Study: Performing a forensic-style hunt for a potential Insider Threat using advanced KQL queries to search for anomalous data exfiltration patterns.

Module 6: Security Orchestration and Automation (SOAR)

- Introduction to Azure Logic Apps and the SOAR concept in Sentinel.
- Building Automation Rules to streamline incident response and assignment.
- Designing and implementing Security Playbooks for common security tasks
- Integrating playbooks with third-party tools
- Case Study: Automating the full response to a phishing campaign alert, from email quarantine to user account disabling and SOC notification.

Module 7: Reporting, Workbooks, and Monitoring

- Creating custom and interactive Workbooks for tailored security reporting.
- Monitoring Health and Performance of the Sentinel workspace and data connectors.
- Building executive-level and operational Security Dashboards.
- Using Time-Series and visualization techniques to spot security trends.
- Case Study: Developing a C-Suite Workbook that provides a real-time overview of the organization's top 5 security risks and the efficacy of automated responses.

Module 8: Deployment & Management Best Practices

- Implementing Security Best Practices for access control and governance.
- Managing Sentinel across multiple customers or tenants using Azure Lighthouse.
- Utilizing Sentinel as Code with Azure DevOps/GitHub for deployment consistency.
- Disaster Recovery and business continuity planning for the SIEM environment.
- Case Study: Designing a Managed Security Service Provider strategy to deploy and manage Sentinel for ten different clients with segregated access and reporting.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now