Reference: sm/SC-5001

Microsoft Sentinel SC-5001 Training: SIEM and Advanced Security Operations

Configure, Operate and Monitor a Modern Cloud SIEM/SOAR

Duration: 1 Day | Hours: 6 h

Remote · Sessions guaranteed from 1 registrant · 60% hands-on practice

Description

This Microsoft Sentinel – SIEM and Advanced Security Operations training teaches you to configure, operate and monitor a modern SIEM/SOAR security platform in Azure. You will learn to collect, analyse and correlate security events from a variety of sources, to write KQL queries to extract insights and to create effective detection rules. The course also includes the creation of custom dashboards, automation via Azure Logic Apps playbooks, and the workflows of an operational SOC. Hands-on workshops based on real-world scenarios will enable you to identify and respond to cybersecurity threats. By the end, you will be able to drive advanced security operations with Microsoft Sentinel.

Learning Objectives

By the end of the training, the participant will be able to:

- Understand the fundamentals of SIEM/SOAR cybersecurity in a cloud environment
- Master the configuration, administration and monitoring of Azure Sentinel for threat detection and incident response
- Collect, normalise and analyse security data from a variety of sources (logs, events, cloud/on-premises solutions)
- Implement detection rules, behavioural analytics and automation playbooks for incident response
- Develop actionable dashboards and reports for operational cyber threat intelligence
- Apply best practices to operate a modern SIEM/SOAR Security Operations Centre (SOC)

Prerequisites

Because every participant is unique, a personalised interview with our expert allows us to design a training course perfectly aligned with their objectives, level and professional challenges.

- Basic knowledge of cybersecurity, networking and threat models
- Notions of logs, system events and KQL syntax (an introduction is a plus)
- Familiarity with Microsoft Azure (portal, resources, RBAC)

Target Audience

- Security engineers, SOC analysts, SIEM managers
- Cloud administrators and DevOps involved in security monitoring
- Security architects or cybersecurity consultants who want to master Microsoft Sentinel for advanced security operations

Detailed Programme

The training alternates between theoretical input and hands-on practice (approximately 60% of the time). Modules are built around practical exercises based on real-world business use cases.

Module 1 – Introduction to SIEM and SOAR

- Key concepts of SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response)
- Overview of the features of Azure Sentinel

Module 2 – Architecture and Data Collection

- Sentinel architecture, Log Analytics workspaces
- Data connectors: Azure, Windows, Linux, firewalls, Microsoft 365, and third-party sources
- Log normalisation and formats

Module 3 – Kusto Query Language (KQL)

- KQL fundamentals
- Search queries, aggregations and trend visualisation
- Query optimisation for performance

Module 4 – Analytics Rules and Intelligent Detections

- Creating analytics rules based on conditions, trends and behaviours
- Using Machine Learning & predefined templates
- Testing false positives / negatives

Module 5 – Incidents and Investigations

- Designing investigations: trigrams, indicators and pivoting
- Exploring entities and correlations between alerts
- Tracing attacks using investigation graphs

Module 6 – Playbooks and Automation

- Overview of Azure Logic Apps playbooks for automated response
- Playbook examples for quarantine, IP blocking, notifications
- Integration with Teams, email, ticketing

Module 7 – Dashboards and Reporting

- Creating custom dashboards
- Publishing reports for compliance and management
- Real-time dashboards

Module 8 – Hands-on Scenarios and SOC Workflows

- Demonstrations of real detections: phishing, lateral movement, brute force, exfiltration
- Setting up a structured SOC alerting and response process

Module 9 – Best Practices and Continuous Security

- Cost management, log retention, data protection
- Periodic rule updates, playbook tuning

Course Highlights

- Focuses on operating a cloud SIEM with Microsoft Sentinel
- Covers detection, investigation and automated response to incidents
- Emphasises real-world SOC cases and continuous security best practices
- Prepares you for the Microsoft SC-5001 exam

Teaching Methods

Format and Delivery

The training is delivered remotely via an interactive virtual classroom. It can also be delivered on-site, with content customised to match the needs of your professional project. The theory/practice split is approximately 40%/60%.

MFE-IT Ultra-Personalised Format

Each session accommodates between 1 and 3 participants, ensuring highly individualised support. A preliminary interview allows us to tailor the content to each participant's profile. Inter-company sessions are guaranteed from just 1 registrant (except in cases of force majeure).

Skills Assessment

Throughout the training, the trainer assesses participant progress through multiple-choice questions, role-playing exercises and hands-on work. At the end, a certificate of achievement is issued to each participant.

Post-Training Support

For one month following the training, each participant can contact MFE-IT trainers with questions about implementing acquired knowledge. A response is provided by email or telephone within 48 working hours.

Accessibility

MFE-IT is committed to welcoming people with disabilities. Contact: contact@mfe-it.com.

Practical Information

Trainer Resources

- Structured demonstrations aligned with the detailed programme
- Exercise briefs and solutions throughout the training
- A ready-to-use technical environment for practical workshops
- Trainer validation of acquired knowledge at the end of each workshop
- Digital reference documents

Certification and Validation

At the end of the training, a certificate is sent by email specifying the objectives, nature, duration and assessment results. A completion certificate can also be provided on request.

Benefits for Participants

- Train from your workplace or home, with no travel required
- Benefit from an expert trainer-consultant on the subject
- Enjoy an ultra-personalised format (1 to 3 participants)
- Continue training even in the event of unforeseen circumstances

Benefits for the Organisation

- Optimise the training budget by reducing travel and accommodation costs
- Offer quality training to all employees, regardless of location
- Reduce absence time linked to travel
- Support team upskilling in all contexts