Reference: sm/SC-5001

Microsoft Sentinel SC-5001 Training Course

SIEM and Advanced Security Operations

Duration: 1 day (6 h)

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

DESCRIPTION

This Microsoft Sentinel – SIEM and Advanced Security Operations training course 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, write KQL queries to extract insights, and build effective detection rules.

The course also covers the creation of custom dashboards, automation through Azure Logic Apps playbooks, and the workflows of an operational SOC. Hands-on labs based on real-world scenarios will enable you to identify and respond to cybersecurity threats. By the end, you will be able to run advanced security operations with Microsoft Sentinel.

LEARNING OBJECTIVES

By the end of this training course, participants 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 threat intelligence.
- Apply best practices to operate a modern SIEM/SOAR Security Operations Centre (SOC).

PREREQUISITES

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

Because each participant is unique, a personalised interview is systematically organised in advance with our expert to design a course perfectly aligned with their objectives, level and professional challenges.

TARGET AUDIENCE

- Security engineers, SOC analysts and 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.

Introduction to SIEM and SOAR

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

Architecture and data collection

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

Kusto Query Language (KQL)

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

Analytics rules and intelligent detections

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

Incidents and investigations

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

Playbooks and automation

- Introduction to Azure Logic Apps playbooks for automated response.
- Example playbooks for quarantine, IP blocking and notifications.
- Integration with Teams, email and ticketing.

Dashboards and reporting

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

Practical scenarios and SOC workflows

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

Best practices and continuous security

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

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%, with extensive hands-on work on concrete business use cases.

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: level, objectives, professional context and challenges. 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-play and hands-on work. The small group size makes individual validation possible at the end of each workshop. At the end of the training, a certificate of validated skills 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. For any accommodation request, a discussion with our disability officer helps identify specific needs and adapt the training. Contact: contact@mfe-it.com.

PRACTICAL INFORMATION

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.

Type of Training

Professionalising training action, aimed at improving and broadening participants' skills.

Monitoring and Assessment

Participant attendance is verified by signing an attendance sheet per half-day, countersigned by the trainer. Participants put the course material into practice through hands-on work on individual workstations; skills are validated by the trainer at the end of each workshop.

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) that encourages interaction and practice.
- 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.