

Configure SIEM Security Operations using Microsoft Sentinel (SC-5001)

Duration: 1 day

Audience: Professionnel TI

Who is this training for?

- Cybersecurity Analysts (SOC) wishing to configure and operate a SIEM solution
- System and network administrators involved in the security of IT environments
- IT security engineers or professionals
- Incident and threat management specialists
- Anyone wishing to deploy and operate Microsoft Sentinel for incident monitoring and response

Training objectives

- Create and configure a Microsoft Sentinel workspace
- Deploy solutions and connect data sources (Microsoft services, Windows events)
- Configure analytics rules to detect threats
- Automate incident responses using Sentinel's SOAR capabilities
- Leverage Microsoft Sentinel to monitor, analyze, and manage security operations
- Establish a complete threat detection and response chain

Summary

Applied Skills training courses are designed to validate specific skills by being oriented towards real-world scenarios. They offer a targeted alternative to traditional role-based certifications, with a focus on applying technical skills in real-world business situations.

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events to Microsoft Sentinel, configuring Microsoft Sentinel scanning rules, and responding to threats with automated responses.

Course outline

- Create and manage Microsoft Sentinel workspaces

- Connect Microsoft services to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Detect threats with Microsoft Sentinel analytics
- Automate in Microsoft Sentinel
- Configure SIEM security operations using Microsoft Sentinel

Approach and methodology

Practical and structured approach combining focused theory and guided workshops.

Participants gradually configure and operate SIEM security operations using Microsoft Sentinel through real-world exercises inspired by real-world scenarios, promoting immediate application of learnings. They learn how to collect, analyze, and correlate security data in order to effectively detect, investigate, and respond to incidents.

Led by a Microsoft certified trainer, the training focuses on interactivity and the development of directly transferable technical skills to strengthen the security posture of organizations in a professional context.

Prerequisites

- Fundamental understanding of Microsoft Azure or equivalent content.
- Basic understanding of Microsoft Sentinel or equivalent content.
- Experience using the Kusto Query Language (KQL) in Microsoft Sentinel or equivalent content.
- You must have your own Azure subscription. (You need an Azure subscription to complete the exercises. If you don't have an Azure subscription, [create a free account](#) and add a subscription before you begin. If you're a student, you can take advantage of the [Azure for Students](#) offer.

Recommendations

- Basics in cybersecurity (threats, monitoring, incident response)
- Knowledge of SIEM and SOC concepts Familiarity with Microsoft Azure environments
- Notions of networking and log management
-

Understanding of identity security principles (Microsoft Entra ID)