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

By the end of this course, students will be able to:

- 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

Learning Path: Configure SIEM security operations in Microsoft Sentinel

- Module 1 — Create and manage Microsoft Sentinel workspaces

  Configure and manage Microsoft Sentinel workspaces
- Module 2 — Connect Microsoft services to Microsoft Sentinel

  Connect Microsoft services to Microsoft Sentinel
- Module 3 — Connect Windows hosts to Microsoft Sentinel

  Connect Windows hosts to Microsoft Sentinel
- Module 4 — Threat detection with Microsoft Sentinel analytics

  Threat detection with Microsoft Sentinel analytics
- Module 5 — Automation in Microsoft Sentinel

  Automation in Microsoft Sentinel
- Module 6 — 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

Students should have the Following knowledge and experience before attending this course:

- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Microsoft Windows

- Familiarity with Azure services, specifically Azure Virtual Machines
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts

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)