Configure SIEM security operations using Microsoft Sentinel (SC-5001)

ID SC-5001 **Prix** CHF 870,– (Hors Taxe) **Durée** 1 jours

A qui s'adresse cette formation

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advise on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft Defender XDR, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Contenu

Create and manage Microsoft Sentinel workspaces

- Introduction
- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs
- Module assessment
- Summary and resources

Connect Microsoft services to Microsoft Sentinel

- Introduction
- Plan for Microsoft services connectors
- Connect the Microsoft 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector
- Module assessment
- Summary and resources

Connect Windows hosts to Microsoft Sentinel

- Introduction
- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector
- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs
- Module assessment
- Summary and resources

Threat detection with Microsoft Sentinel analytics

- Introduction
- Exercise - Detect threats with Microsoft Sentinel analytics
- What is Microsoft Sentinel Analytics?
- Types of analytics rules
- Create an analytics rule from templates
- Create an analytics rule from wizard
- Manage analytics rules
- Exercise - Detect threats with Microsoft Sentinel analytics
- Summary

Automation in Microsoft Sentinel

- Introduction
- Understand automation options
- Create automation rules
- Module assessment
- Summary and resources

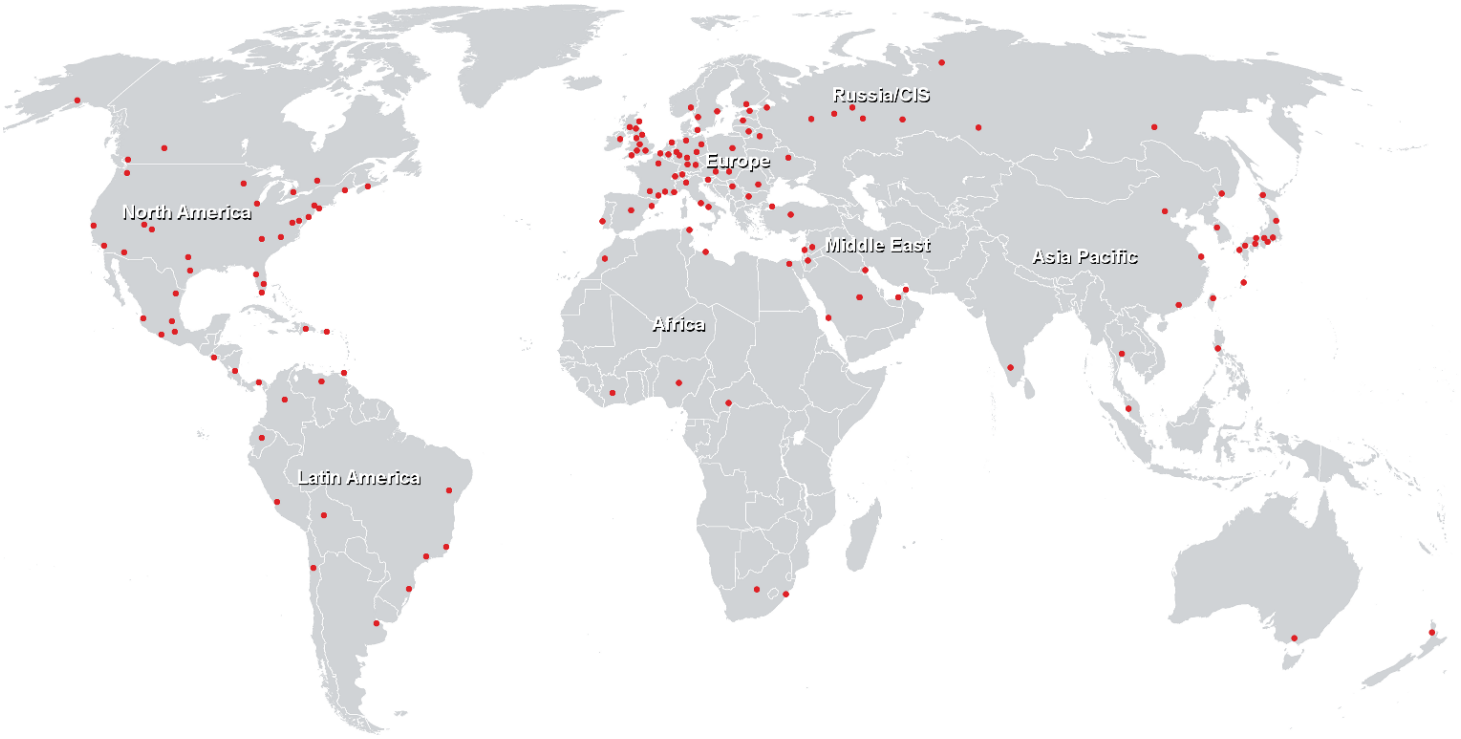
Configure SIEM security operations using Microsoft Sentinel

- Introduction
- Exercise - Configure SIEM operations using Microsoft Sentinel
- Exercise - Install Microsoft Sentinel Content Hub solutions and data connectors
- Exercise - Configure a data connector Data Collection Rule
- Exercise - Perform a simulated attack to validate the Analytic and Automation rules
- Exercise - Connect Microsoft Sentinel to Microsoft

Defender XDR
- Summary

Microsoft Solutions Partner
Microsoft Cloud Training Services

Centres de formation dans le monde entier





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch