Microsoft Sentinel

Microsoft Sentinel is a cloud-native **Security Information and Event Management (SIEM)** and **Security Orchestration, Automation, and Response (SOAR)** platform available on Microsoft Azure. It is designed to help organizations proactively monitor, detect, investigate, and respond to security incidents across hybrid and multi-cloud environments. Microsoft Sentinel integrates seamlessly with various data sources, leveraging artificial intelligence (AI) and machine learning (ML) to identify threats in real-time. It provides a centralized view of an organization's security posture, making it a comprehensive solution for modern security operations centers (SOCs).

Microsoft Sentinel is a cloud-native **Security Information and Event Management (SIEM)** and **Security Orchestration, Automation, and Response (SOAR)** solution provided by Microsoft Azure. It is designed to help organizations monitor, detect, investigate, and respond to cybersecurity threats in real-time.

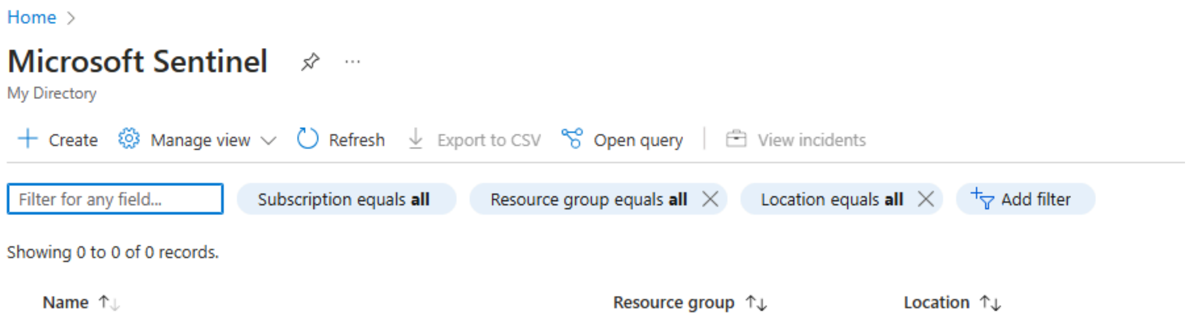
Key features of Sentinel:

1. **Data Collection**: Collects security data from various sources such as Azure, on-premises environments, third-party services, and other cloud platforms.
2. **Analytics & Threat Detection**: Uses built-in AI and machine learning to detect potential threats and suspicious activities. Customizable analytics rules for tailored detection.
3. **Incident Investigation**: Offers tools for analyzing and investigating security incidents through dashboards and visualizations.
4. **Automated Response**: Enables automated responses to detected threats using playbooks built on Azure Logic Apps.
5. **Integration with Log Analytics**: Built on top of Azure Log Analytics, enabling seamless data storage and processing.

The end goal of using Microsoft Sentinel is to enhance security operations by collecting, analyzing, and responding to data from various sources in real time. By leveraging Sentinel on top of a Log Analytics workspace, organizations gain access to advanced threat detection, incident management, and automated response capabilities. Sentinel allows security teams to proactively monitor and identify potential threats, correlate data from different systems, and apply rules to detect suspicious events. Ultimately, this streamlines security operations, reduces response times, and provides a centralized platform to protect hybrid and multi-cloud environments effectively.

To begin with the lab

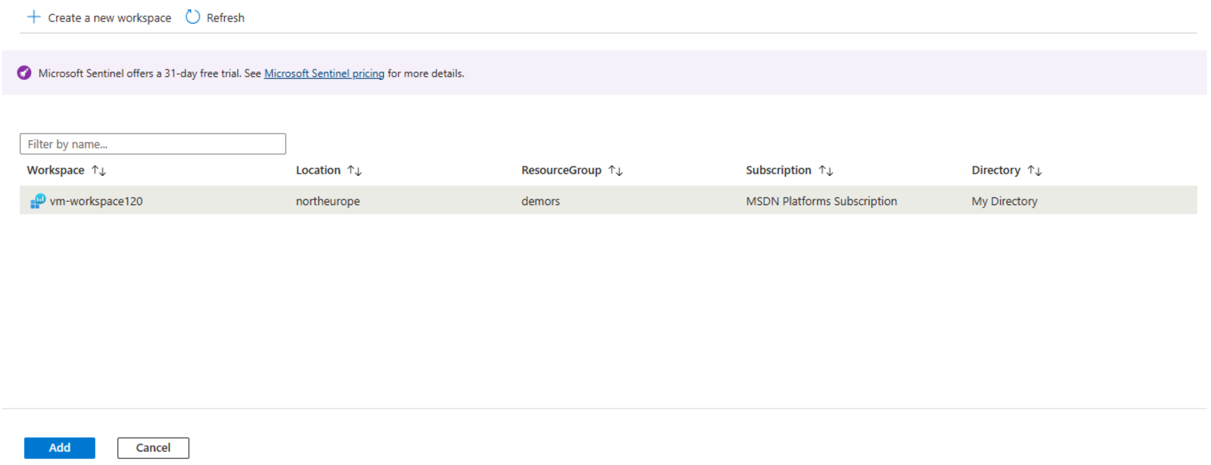
1. To move further in this lab ensure you have a Log Analytics workspace in your Azure Portal.
2. Log into your Azure portal and search the Microsoft Sentinel service in the marketplace within the Azure Portal.



Showing 0 to 0 of 0 records.

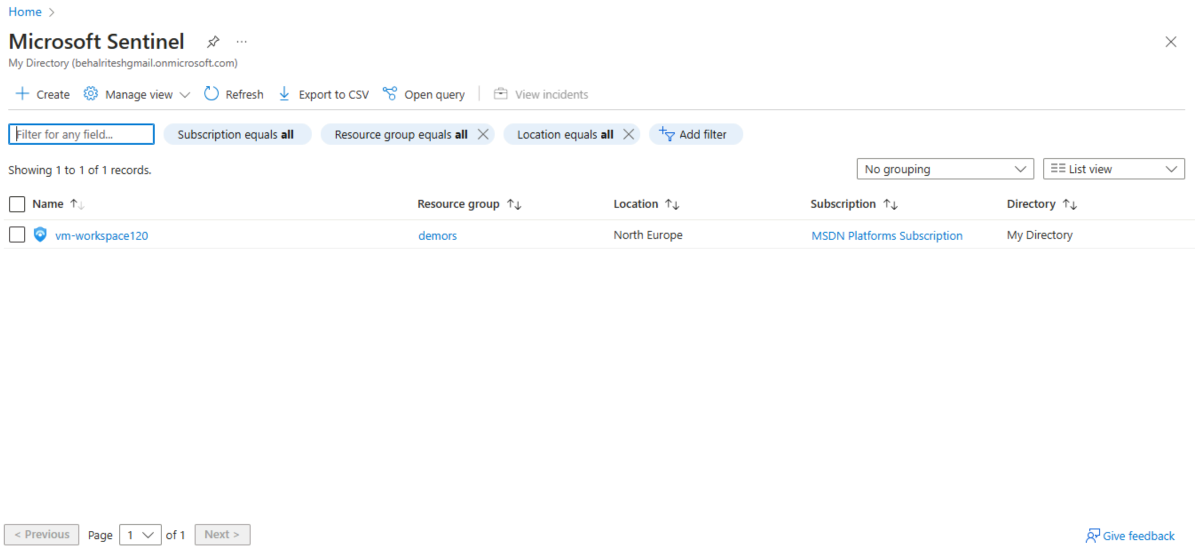
Name ↑↓	Resource group ↑↓	Location ↑↓

3. To create a new sentinel click on the Create button and choose an existing Log Analytics workspace.
4. Select Add to connect Sentinel with the workspace.



Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
vm-workspace120	northeurope	demors	MSDN Platforms Subscription	My Directory



Showing 1 to 1 of 1 records.

Name	Resource group	Location	Subscription	Directory
vm-workspace120	demors	North Europe	MSDN Platforms Subscription	My Directory

5. Go to sentinel and you will see that your SEntinel is connected over your log analytics workspace.
6. Microsoft Sentinel, once integrated, offers a range of tools to: Gather data, Develop and oversee detection rules, Observe and evaluate events recorded in the workspace.