

Episode Title: Use Microsoft Sentinel to monitor on-prem servers and VMs

Objectives:

At the end of this episode, I will be able to:

1. Deploy a Log Analytics and Microsoft Sentinel workspace
2. Configure data sources and connectors
3. Create Microsoft Sentinel analytics rules

Key Points:

Key Point 1

Microsoft Sentinel builds on top of a Log Analytics workspace in Azure. You will need Log Analytics before being able to deploy Sentinel.

Key Point 2

The various Azure and on-premises resources that can send log or event data should be configured as data sources. These can either use built-in connectors or have an agent installed on the resource.

Key Point 3

After the workspace is ingesting log and event data, use analytic rules to query the data and build automation for incidents and investigation.

- If additional resources are used during the episode, they can be obtained using the download link on the overview episode (e.g. diagrams, no powerpoints)

External Resources:

If external resources were used during this episode, you can reference the following external resources for supplementary tools and information, if none were used, then this section will be blank:

- What is Microsoft Sentinel?
: <https://learn.microsoft.com/en-us/azure/sentinel/overview>