THOMAS MORE

Lab 4.4

Enabling Microsoft Sentinel and Exploring the Workspace

Toepasbare Cloud Security voor IT-Professionals

2025 - 2026

Contents

1. Enabling Microsoft Sentinel and Exploring the Workspace

1.1. Context

Microsoft Sentinel is a SIEM/SOAR service that sits on top of Log Analytics. It adds analytics rules, hunting queries, workbooks, and automation — but it does not create a separate data store. All data lives in Log Analytics.

In this lab you will enable Sentinel, explore its workspace, generate real data by performing management operations, and investigate that data using the Logs editor.

1.2. Learning goals

By the end of this lab, you will be able to:

- Enable Sentinel on a Log Analytics workspace and understand that it adds no new storage.
- Query data from your Day 4 infrastructure (App Services, Key Vault, Storage) in the Logs editor.
- Distinguish between hunting queries (ad-hoc investigation) and analytics rules (scheduled detection).
- Enable and verify the Azure Activity Log connector by generating management plane operations.
- Browse built-in Sentinel workbooks and understand what each shows.

1.3. Estimated time

60 minutes

Suggested timing:

Time	Activity
10 minutes	Navigate to Microsoft Sentinel in the Azure portal
10 minutes	Enable Sentinel on the Log Analytics workspace
10 minutes	Enable the Azure Activity Log data connector
10 minutes	Explore the Sentinel workspace: incidents, hunting, workbooks
10 minutes	Browse built-in Sentinel workbooks
10 minutes	Reflection and discussion

1.4. Before you start

Make sure you have:

- [ ] Day 4 monitoring infrastructure is enabled (pipeline ran — Lab 4.1)
- [ ] Diagnostic settings are configured (Lab 4.2)
- [ ] Application telemetry has been generated by your requests (OpenTelemetry-based SDK, Lab 4.3)
- [ ] You have access to the Azure portal with Contributor role on the resource group

2. Navigate to Microsoft Sentinel

2.1. Open Microsoft Sentinel

1. In the Azure portal, search for **Microsoft Sentinel**
2. If you have never used Sentinel before, click **Try Microsoft Sentinel for free**
3. Select your Log Analytics workspace: `law-<your_prefix>-dev-d4`
4. Click **Enable**

2.2. Understand the Sentinel Workspace

After enabling Sentinel, you will see the Sentinel workspace with a left-hand navigation menu:

Menu Item	Purpose
Overview	Sentinel dashboard showing incidents, coverage, and recommendations
Incidents	Security incidents created by analytics rules
Hunting	Proactive threat hunting queries
Analytics	Analytics rules (scheduled KQL queries)
Data connectors	Data sources connected to Sentinel
Workbooks	Security dashboards
Automation rules	Auto-classification and alerting rules

> **Question**
>
> Sentinel uses the same Log Analytics workspace that Application Insights uses. What does this mean for data storage costs? If you enable Sentinel, do you pay extra for Sentinel itself, or only for the Log Analytics data ingestion?

3. Explore the Sentinel Overview

3.1. Review the Sentinel Overview

The Sentinel overview page shows:

Section	Content
Incidents	Number of active and closed incidents
Data connector status	Which connectors are enabled and active
Analytics rules	Number of active and inactive rules
MITRE ATT&CK coverage	Which tactics and techniques have detection rules
Security recommendations	Recommendations from Defender for Cloud

3.2. Review Data Connector Status

Look at the data connector section. You should see:

Connector	Status
Azure Monitor Logs	Enabled (automatic — all Log Analytics data)
Azure Activity Log	Not enabled (must be turned on manually)

3.3. Review MITRE ATT&CK Coverage

The MITRE ATT&CK coverage section shows which attack tactics have detection rules. Initially, this will be empty or minimal because no analytics rules have been created yet.

> **Note**
>
> MITRE ATT&CK is a knowledge base of adversary tactics and techniques. Each analytics rule is tagged with MITRE tactics (e.g., InitialAccess, LateralMovement) and techniques (e.g., T1021.004). The coverage dashboard shows how much of the MITRE framework your environment can detect.

> **Note**
>
> For more on Defender for Cloud — including SBOM generation, vulnerability scanning, and Defender for DevOps — see the theory page: Theory — Defender for Cloud (CSPM).

4. Explore Sentinel Workbooks

4.1. Browse Built-in Workbooks

1. In the left menu, click **Workbooks**
2. You will see several built-in workbooks:

Workbook	Purpose
Security operations	Overview of security operations and incident trends
Asset inventory	Which resources are monitored by Sentinel
Security recommendations	Defender for Cloud recommendations
Incident analysis	Deep dive into a specific incident
Network security	Network-related security events

4.2. Open the Security Operations Workbook

1. Find the SOC Handbook in the Content Hub
2. Install (add) it
3. Open the Security operations workbook
4. Review some of the Templates

4.3. Workspace Usage Report

1. Install the Workspace Usage Report workbook
2. Open the workbook and review the data

Your answer: In the Asset Inventory workbook, which resource types appear? Which ones are sending data, and which are not? What would cause a resource to not be sending data?

5. Explore Sentinel Hunting

5.1. Run a Hunting Query Against Your Data

Hunting queries are ad-hoc investigations — unlike analytics rules, they are not scheduled. You run them manually to search for threats that may not have triggered an alert.

1. In the left menu, click **Hunting**
2. Click on Anonymous IP address queries
3. Review the KQL query and description
4. Click **Run** to execute the query against your own data
5. Review the results — do you see any anonymous IPs querying your services?

> **Question**
>
> Did the anonymous IP hunting query return results for your environment? What does that tell you about the traffic pattern in lab 4.3? If it did return results, which endpoints were targeted?

5.2. Compare Hunting Queries to Analytics Rules

1. Click on another hunting query (e.g., **Azure Active Directory identity and access events**)
2. Review its KQL query
3. Now navigate to Analytics in the left menu and review what analytics rules are currently defined

> **Question**
>
> Compare a hunting query you just ran with an analytics rule. What is the key difference between them? When would you use a hunting query instead of creating an analytics rule?

6. Reflection Questions

Your answer:

1. You queried the Azure Activity Log in this lab. How does management plane data (Azure Activity Log) differ from application telemetry (AppRequests, AppDependencies)? Why are both needed for security investigation?
2. The Azure Activity Log connector was not enabled by default and showed 'Not connected' until you performed actions. What design principle does this reflect? When might a security team want to disable or limit such connectors?
3. You ran hunting queries against your own data. If you found a suspicious pattern, would you convert it into an analytics rule? Why or why not?
4. Sentinel adds no new storage — all data lives in Log Analytics. What does this mean for cost management when you enable multiple security services (Sentinel, Defender for Cloud, etc.)?

7. Summary

In this lab, you enabled Microsoft Sentinel on your Log Analytics workspace, explored the Sentinel workspace, enabled the Azure Activity Log data connector, and browsed built-in workbooks and hunting queries. You understand that Sentinel is a layer on top of Log Analytics that adds security-specific capabilities — analytics rules, hunting, workbooks, and automation.

8. Next Steps

- Lab 4.5: Hunt through application and infrastructure events using KQL
- Lab 4.6: Create an analytics rule and investigate a simulated incident
- Lab 4.7: Build a workbook and review monitoring coverage