



Visualizing Security Data in MS Sentinel

Adrian Cortez

Overview

Visualizing data on a SIEM is important because it transforms raw security logs and events into clear, actionable insights, enabling security teams to quickly understand patterns, trends, and anomalies. Large volumes of data from multiple sources can be overwhelming, but visualizations like charts, graphs, and dashboards help analysts identify suspicious activity, prioritize threats, and monitor the overall security posture in real time. Effective visualization also supports faster decision-making during incidents, facilitates reporting to stakeholders, and helps detect patterns that might be missed in textual logs, ultimately enhancing the efficiency and effectiveness of a SOC.

Creating a Workbook in MS Sentinel

Workbooks are interactive dashboards that allow you to visualize, analyze, and explore security data from multiple sources. They combine charts, tables, and text to present insights from logs and alerts, helping SOC analysts monitor trends, investigate incidents, and make data-driven decisions in a single, customizable interface.

In this example, we will create a workbook that will help visualize frequently triggered security alerts in the past 30 days.

The screenshot displays the Microsoft Sentinel Workbooks interface. On the left is a navigation pane with a search bar and a list of categories: Home, Investigation & response, Threat intelligence, Microsoft Sentinel, Threat management, and Content management. The 'Workbooks' item under 'Threat management' is selected. The main content area is titled 'Workbooks' and features three summary cards: 'My workbooks' with a count of 0, 'Templates' with a count of 3, and 'Updates' with a count of 0. A link to 'More content at Content hub' is also present. Below these cards, there is a tabbed interface with 'My workbooks' and 'Templates' tabs. The 'My workbooks' tab is active, showing a '+ Add Workbook' button. Below this, a section titled 'Microsoft Sentinel Workbooks' includes a 'What is it?' heading and a paragraph explaining that workbooks enable instant visualization and analysis of data. It also provides two links: 'Learn more about Workbooks' and 'Learn more about OOTB content and Content hub'.

Home > **New workbook** sentinel-project-workspace

How do enterprises leverage Workbooks? Query recent Azure Monitor workbooks changes Help me create my first Azure Workbook

Done Editing Open ? Help

New workbook

Welcome to your new workbook. This area will display text formatted as markdown.

We've included a basic analytics query to get you started. Use the **Edit** button below each section to configure it or add more sections.

1 Edit ...

Metric	Value
ThreatIntelligenceIncidents	119K
ThreatIntelligenceIncidents	116K
SecurityEvent	7.84K
Heartbeat	1.22K
SecurityAlert	668
SecurityIncident	511
Usage	212
SentinelHealth	183
ThreatIntelligence	27
SentinelHealth	1

1 Edit ...

+ Add ▾

- Add text
- Add image
- Add video
- Add parameters
- Add links/tabs
- Add query**
- Add metric
- Add group

1 Editing query item: query - 2

Settings Advanced Settings Style Advanced Editor

Run Query **Samples** Data source Logs (Analy... Resource type Log Analytics Log Analytics works... sentinel-project-... Time Range Last 30 days Visualization Pie chart Size Medium **Chart Settings**

Log Analytics workspace Logs (Analytics) Query

```
SecurityAlert
| summarize AlertCount = count() by AlertName
| sort by AlertCount desc
```

Alert Name	Alert Count
Email messages containing malicious URL removed after del...	540
Email messages removed after delivery	59
Email reported by user as malware or phish	22
Other	20
Logins to Azure from a Non-IT User	13
ONU.Non-US login	7
Azure Login Activity	7

This query will summarize the amount of alerts by alert name and consolidate it in a pie chart.



Save As

sentinel-project-workspace



Title * ⓘ

Most frequently triggered security alerts in the past 30 days



Subscription * ⓘ

Azure for Students



Resource group * ⓘ

Sentinel-Project



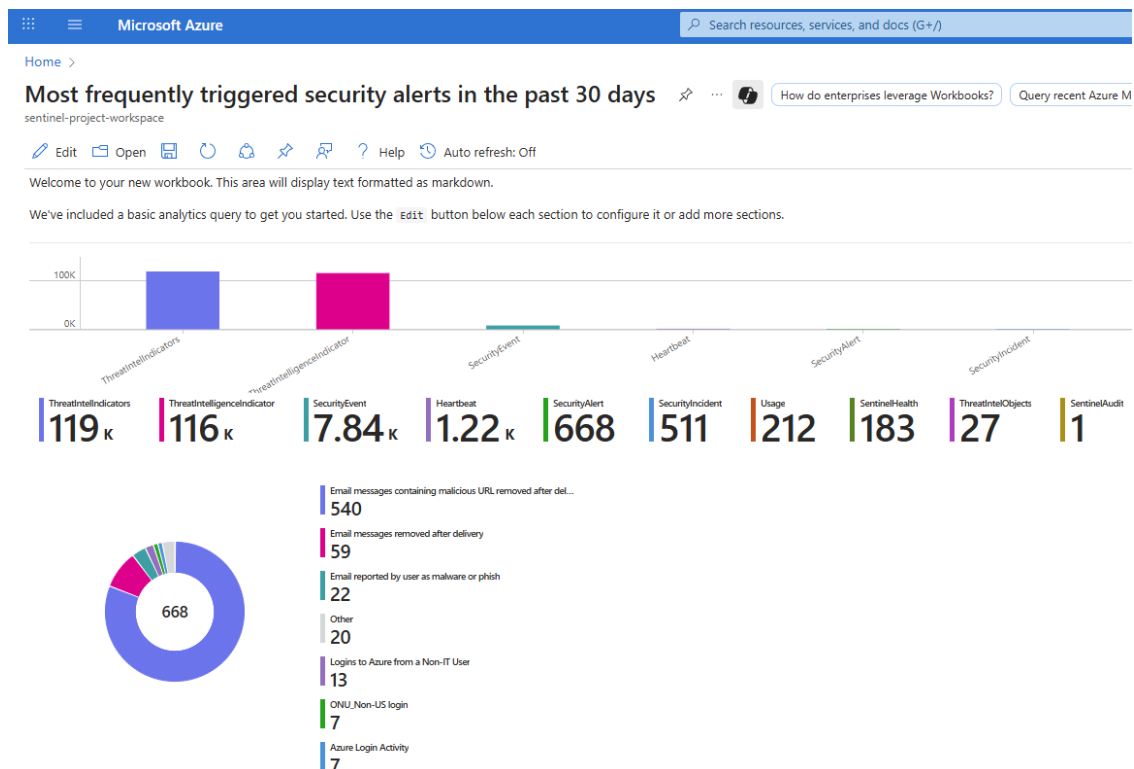
Location * ⓘ

(US) East US



☐ Save content to an Azure Storage Account. ⓘ

Final Workbook:



Create a Workbook For Security Alerts

Follow the steps from before, and use the following query. This query filters alerts that were generated in the last 30 days and groups them to show the number of alerts per day over the past 30 days.

1 Editing query item: query - 2

Settings

Advanced Settings

Style

Advanced Editor

Run Query

Samples

Data source

Logs (Analy...

Resource type

Log Analytics

Log Analytics works...

sentinel-project...

Time Range

Last 30 days

Visualization

Grid

Size

Medium

Column Settings

Log Analytics workspace Logs (Analytics) Query

```
SecurityAlert
| where TimeGenerated > ago(30d)
| summarize dailyAlerts = count() by bin(TimeGenerated, 1d)
| order by TimeGenerated asc
```

TimeGenerated	dailyAlerts
8/11/2025, 7:00:00.000 PM	463
8/12/2025, 7:00:00.000 PM	205



Save As

sentinel-project-workspace

Title *

Security Alerts (Last 24 hours)

Subscription *

Azure for Students

Resource group *

Sentinel-Project

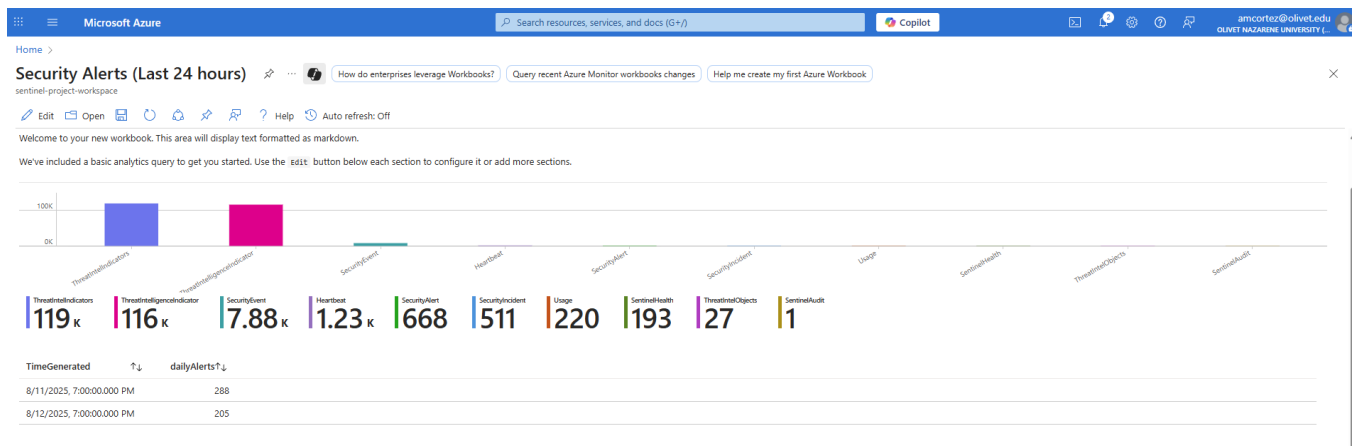
Location *

(US) East US



Save content to an Azure Storage Account.

Results



Visualize Brute Force Attempts

Here, we will create a workbook to visualize brute force events, and further practice visualization in Microsoft Sentinel. The following query finds failed logon events by ID 4625, and orders them by number of failed attempts.

1 Editing query item: query - 2

Settings Advanced Settings Style Advanced Editor

Run Query Samples Logs (Analy...) Log Analytics sentinel-project-... Last 30 days Tiles Medium Tile Settings

Log Analytics workspace Logs (Analytics) Query

```
SecurityEvent
| where TimeGenerated > ago(30d)
| where EventID == 4625
| summarize FailedAttempts = count() by Account
| top 10 by FailedAttempts
```

Save As

sentinel-project-workspace

Title *

Brute Force Attack Attempts

Subscription *

Azure for Students

Resource group *

Sentinel-Project

Location *

(US) East US

☒ Save content to an Azure Storage Account.

Result:

