
# Visualizing Security Data in MS Sentinel

Adrian Cortez

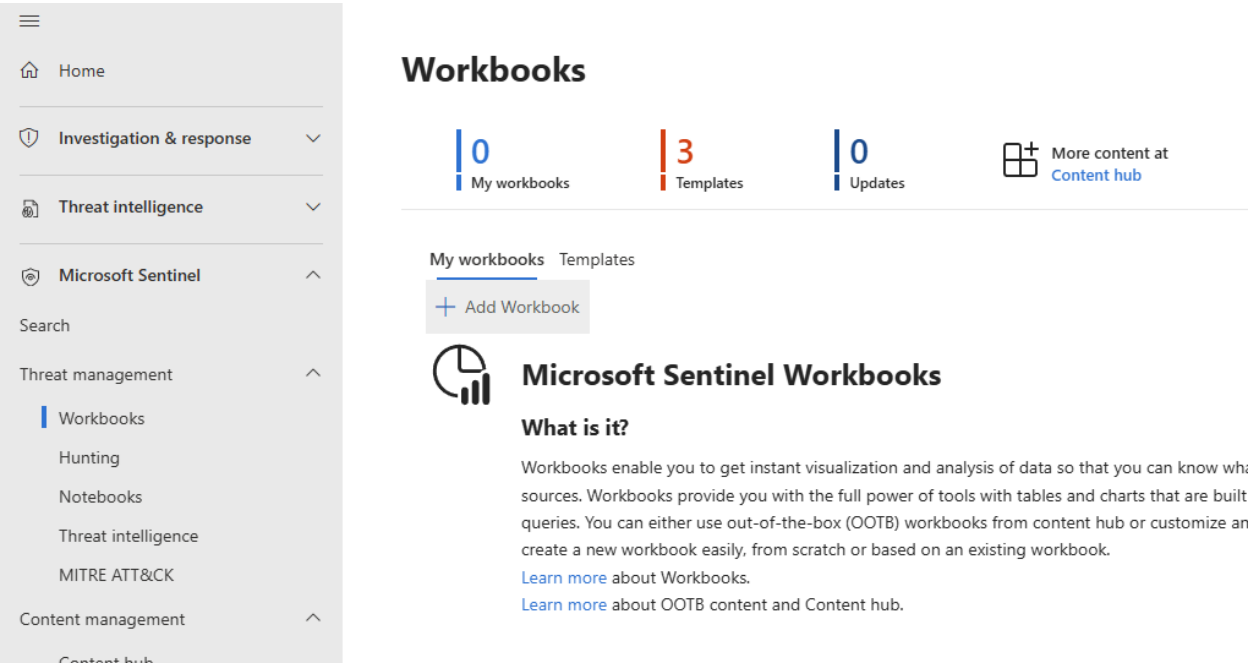
## Overview

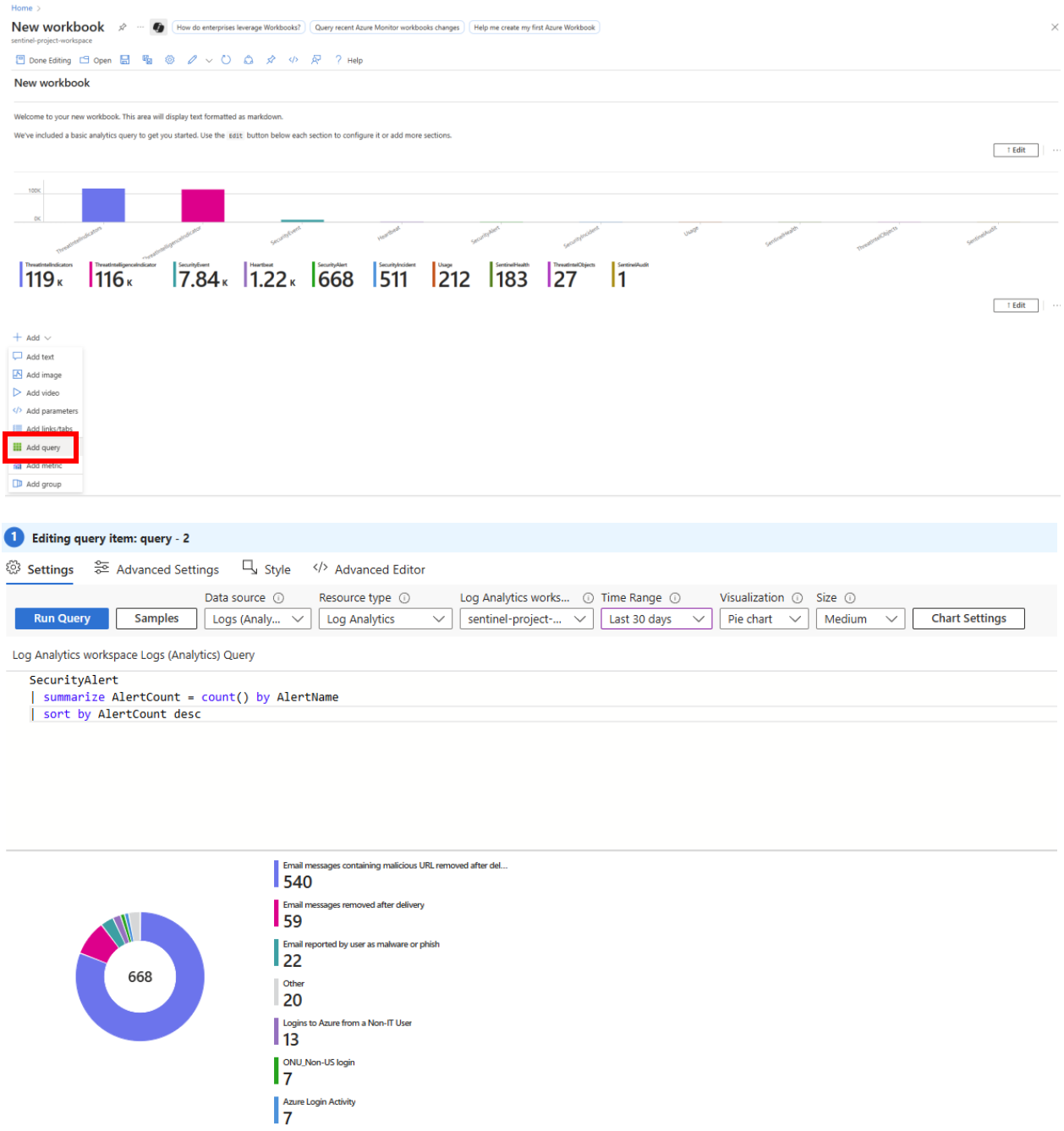
Visualizing data on a SIEM is important because it transforms raw security logs and events into clear, actionable insights, enabling security teams to quickly understand patterns, trends, and anomalies. Large volumes of data from multiple sources can be overwhelming, but visualizations like charts, graphs, 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

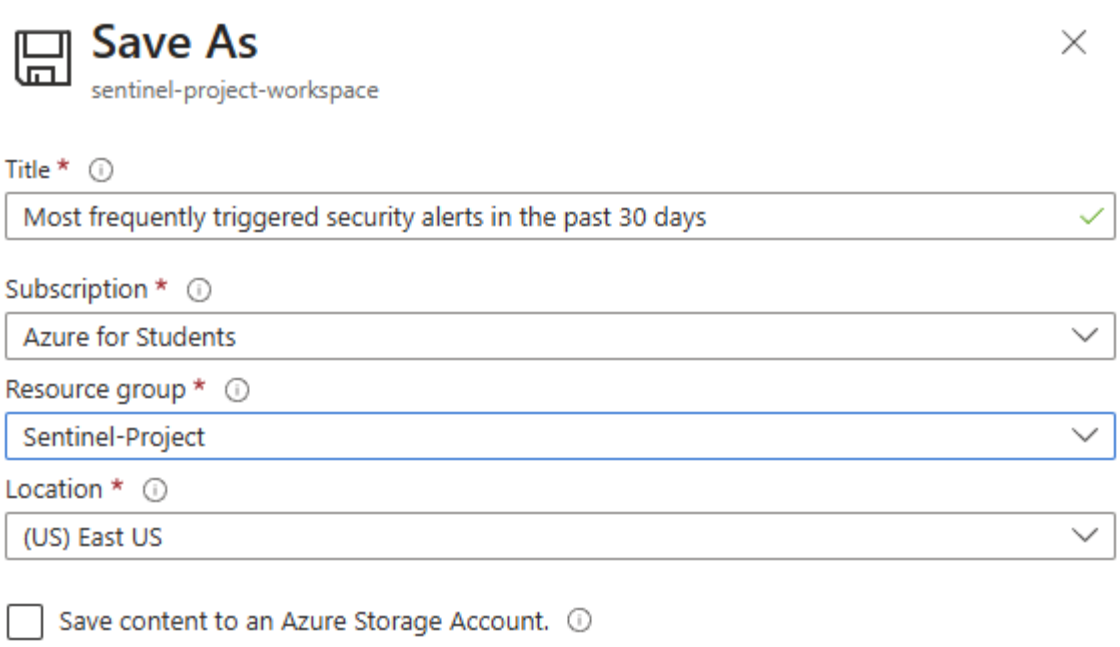
Workbooks are interactive dashboards that allow you to visualize, analyze, and explore security data from multiple sources. They combine charts, tables, and text to present insights from logs and alerts, helping SOC analysts monitor trends, investigate incidents, and make data-driven decisions in a single,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

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

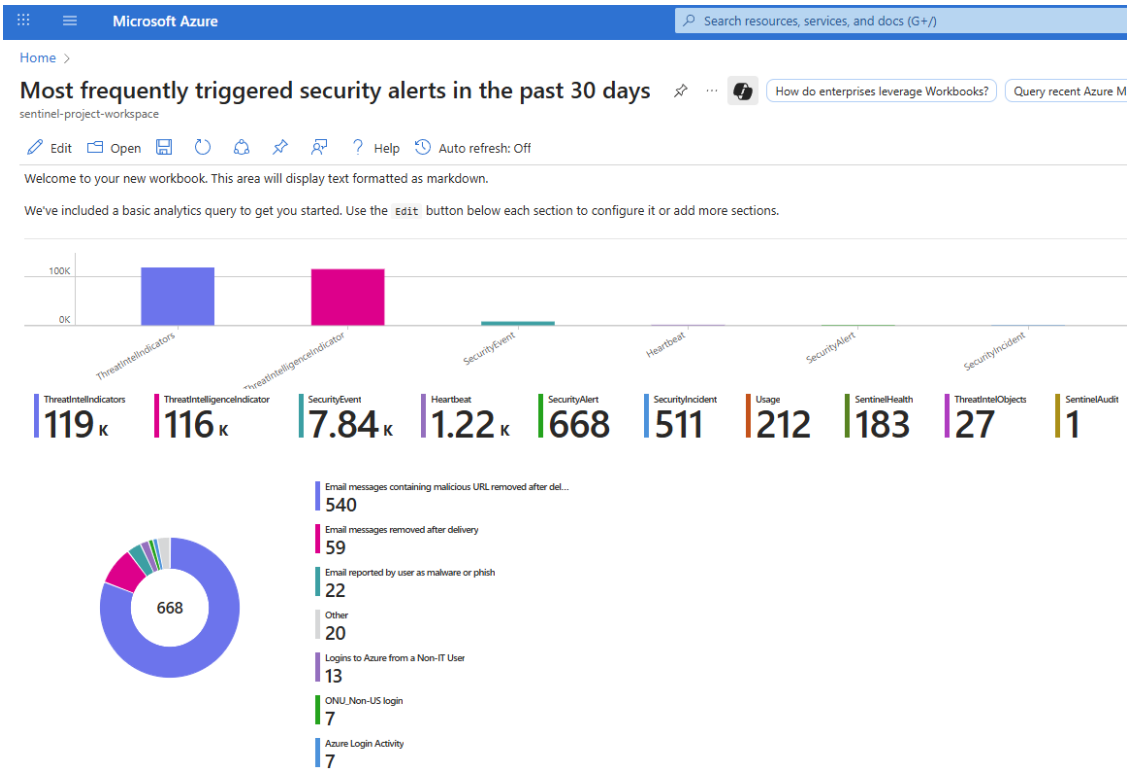





This query will summarize the amount of alerts by alert name and consolidate it in a pie chart.

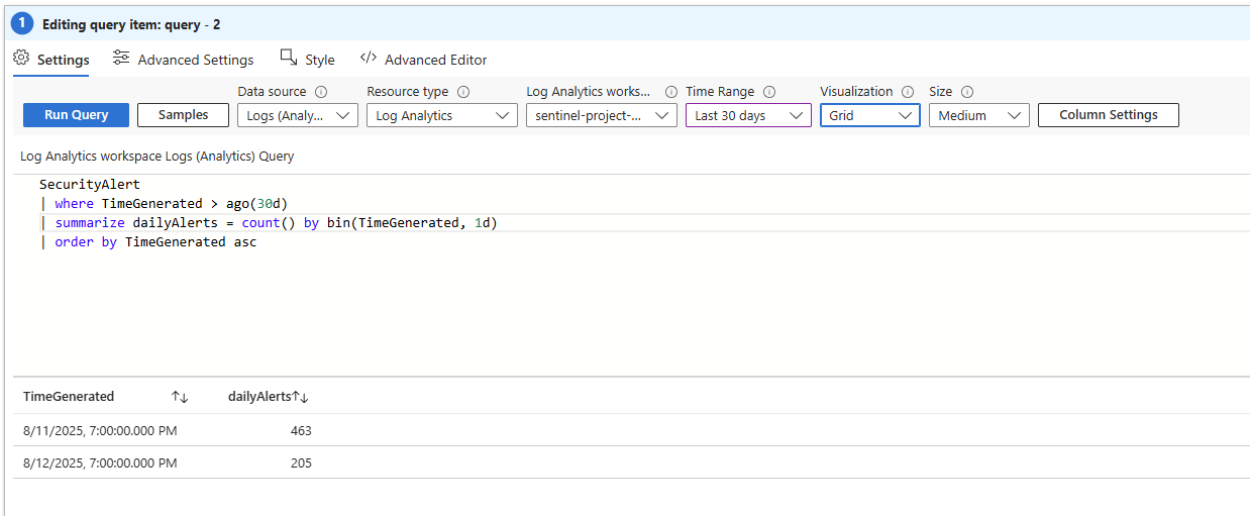


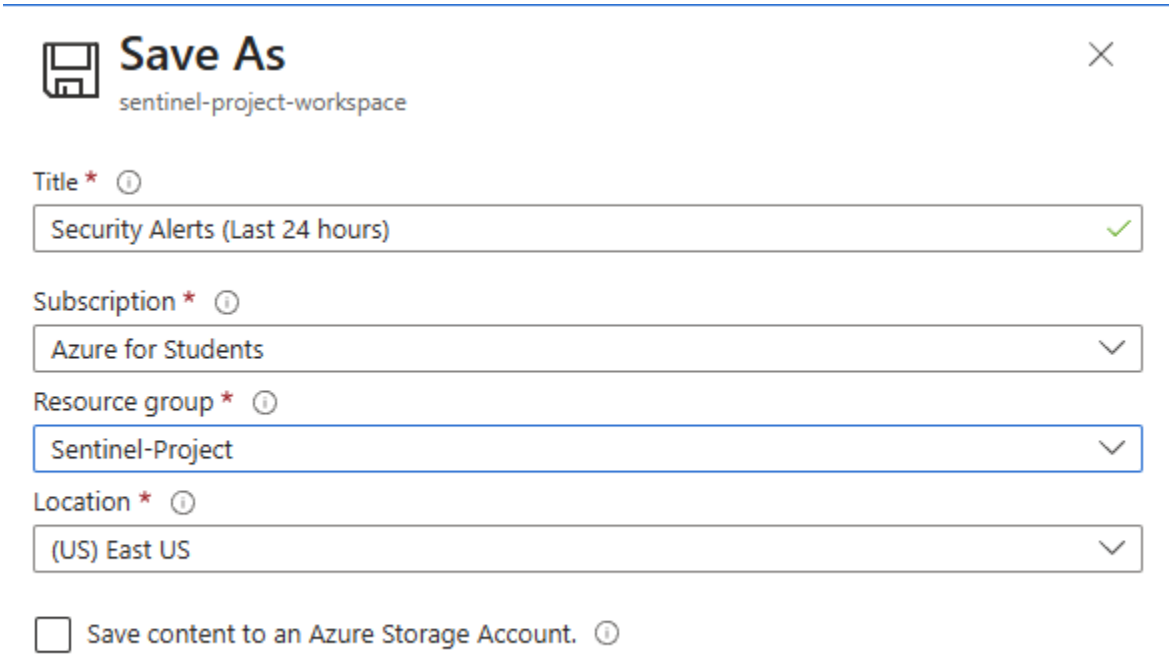

## Final Workbook:



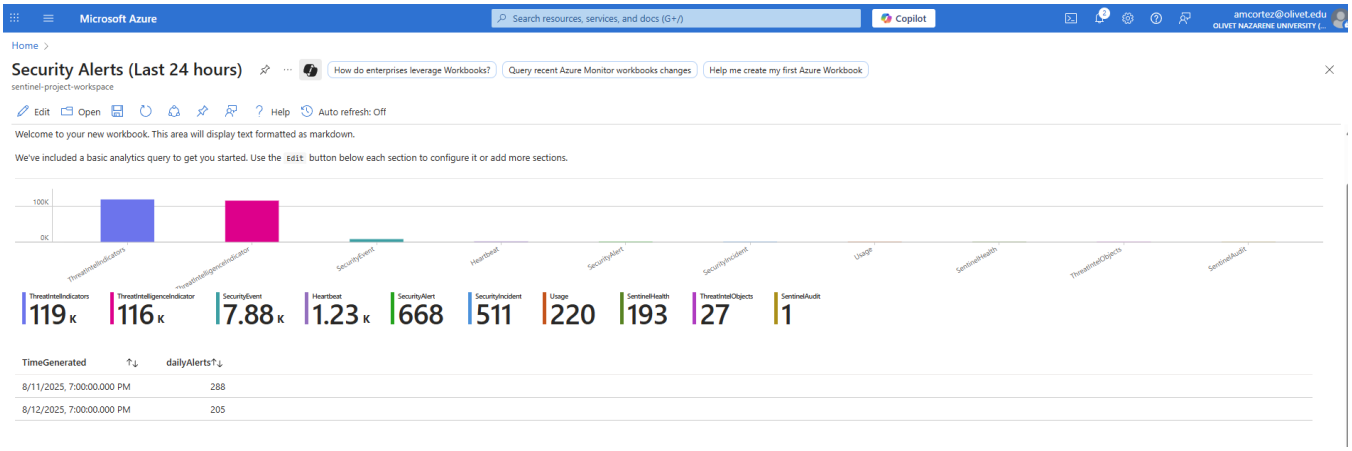
## Create a Workbook For Security Alerts

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.



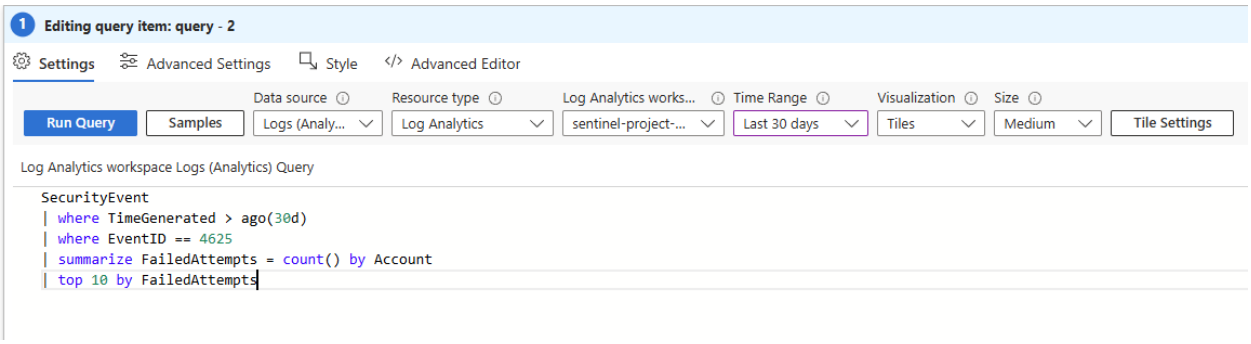



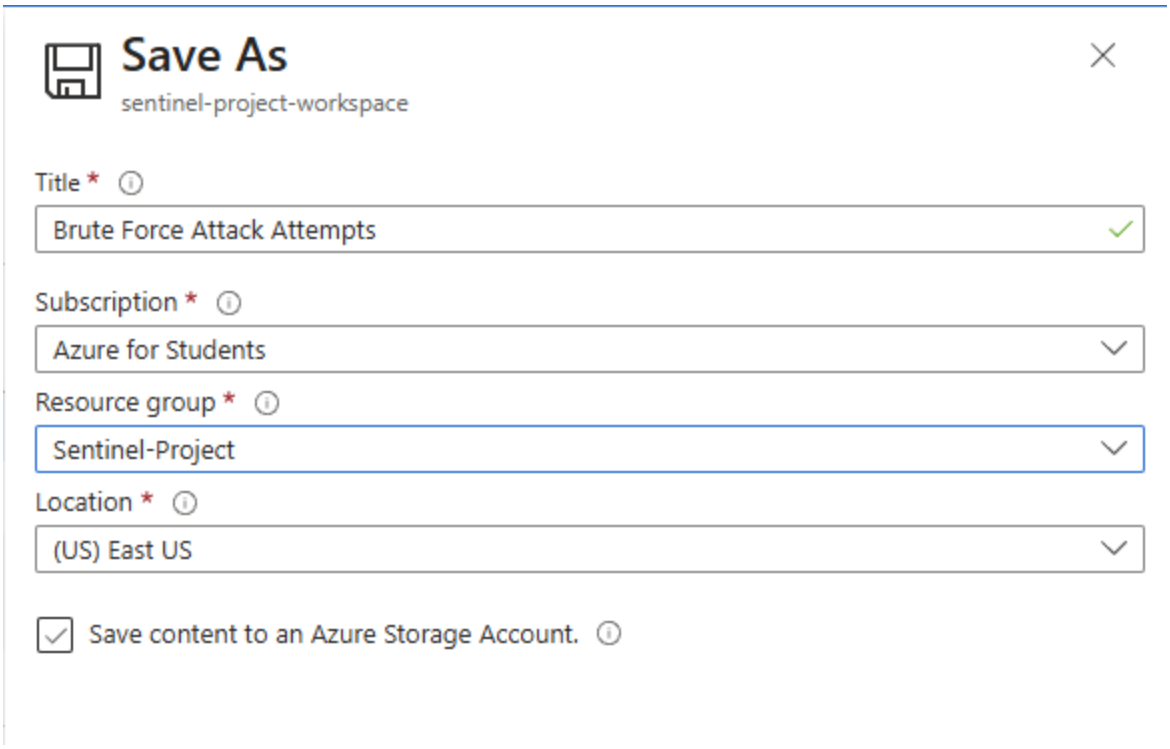

Results



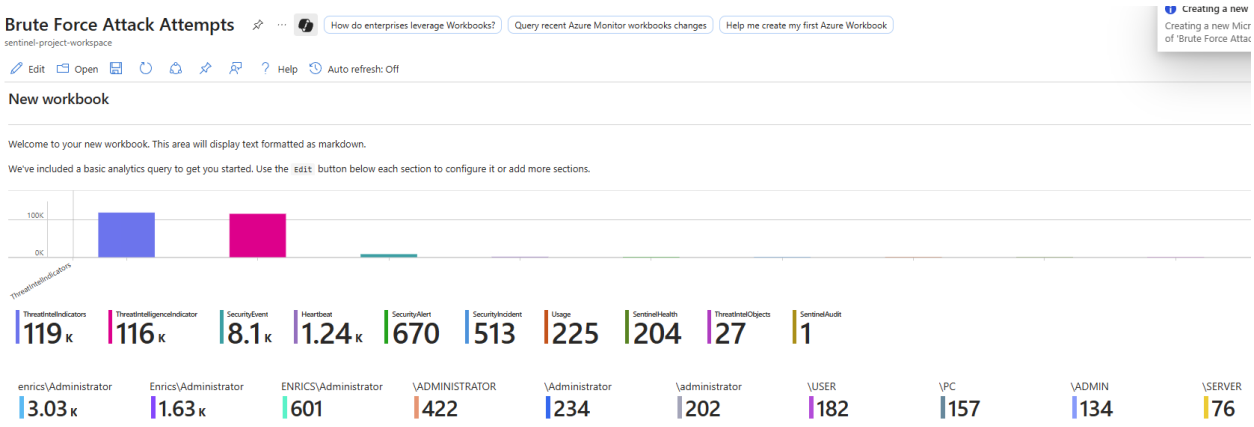

## Visualize Brute Force Attempts

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.




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:


Brute Force Attack Attempts
sentinel-project-workspace
How do enterprises leverage Workbooks?
Query recent Azure Monitor workbooks changes
Help me create my first Azure Workbook
Edit
Open
Help
Auto refresh: Off
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.
ThreatIntelIndicators 119K
ThreatIntelligenceIndicator 116K
SecurityEvent 8.1K
Heartbeat 1.24K
SecurityAlert 670
SecurityIncident 513
Usage 225
SentinelHealth 204
ThreatIntelObjects 27
SentinelAudit 1
enrics\Administrator 3.03K
Enrics\Administrator 1.63K
ENRICS\Administrator 601
\ADMINISTRATOR 422
\Administrator 234
\administrator 202
\USER 182
\PC 157
\ADMIN 134
\SERVER 76