Azure Sentinel Level 400
Hunting and using notebooks

Ofer Shezaf
About module #6: Rule writing

Overview

• In this module you will learn how to hunt using Azure Sentinel.

Pre-requisites

• Azure Sentinel Overview module.
• KQL workshop.
Hunting
Visualize data sets

Automatically detect and plot anomalies in data

```javascript
// Visualizing Time Series anomalies
TimeSeriesData
| extend (anomalies, score, baseline) = 
|     series_decompose_anomalies(TotalCount, 3, -1) // 'linefit'
| render timechart with (title="Trend Micro Time Series anomalies")
```
extend Week = iff(TimeGenerated>ago(7d), "This Week", "Last Week"), TimeGenerated = iff(TimeGenerated>ago(7d), TimeGenerated, TimeGenerated + 7d)

SigninLogs
| summarize count() by bin(TimeGenerated, 1h) |

Completed: Showing results from the last 48 hours.

For Smart Diagnostics click on a highlighted data variation

Analyze Root cause
The following pattern may explain the data discrepancy:

DeviceDetail['browser'] == "Chrome 76.0.3782"
Bookmarks

- Bookmark any event in search results
- Use as incident artifacts
- Map to entities to enable bookmark (and event) investigation

Hunting bookmarks enable Azure Sentinel users to save, tag, annotate, share and investigate results from a Log Analytics query. You can view and manage Hunting Bookmarks in Azure Sentinel - Hunting. Click here to learn more.
Notebooks
Understanding notebooks

- A web app for creating and running interactive documents.
- Documents contain:
  - live code,
  - Visualizations
  - Narrative text
- App Server can be:
  - Free MS service
  - Azure VM, Local Docker
Why Jupyter?

- Data persistency
- Full scripting/programming environment (vs. declarative query)
- Sharing, Knowledge base
- Access to a wide variety of libraries:
  - Machine learning
  - Advanced data manipulation and analysis
  - Visualization

Also read Why Use Jupyter for Security Investigations
Use cases

• Building notebooks on the fly
  • Tier 3 Analysts requiring deep investigation capability
  • Hunters/Threat Intel analysts

• Authoring reusable notebooks
  • By Tier 3 analysts and SOC Engineering
  • For use as template notebooks by Tier 1+
Sentinel Integration

- KQL Magic
- MSTICPY
Where to go from here?

Tools

- Notebooks lab
- Kqlmagic - Microsoft Azure Monitor magic extension to Jupyter notebook
- Msticpy – MSTIC Jupyter and Python Security Tools

Blogs:

- Why Use Jupyter for Security Investigations