KQL for APIs, Logic Apps and More

KQL Café 29 April 2025

Bert-Jan Pals

C:\>whoami

Defensive Security Expert

Background:

5+ years security experience in financial sector

- SOC Lead
- Threat Hunting
- Detection Engineering
- Incident Response
- SOAR/Automation

Content:

Blogs: kqlquery.com

Tools & Queries: github.com/bert-janp

https://www.linkedin.com/in/bert-janpals/

API = Automate

APIs introduce automation potential for playbooks, enrichment, integrations, reporting, etc.

Which APIs can I use?

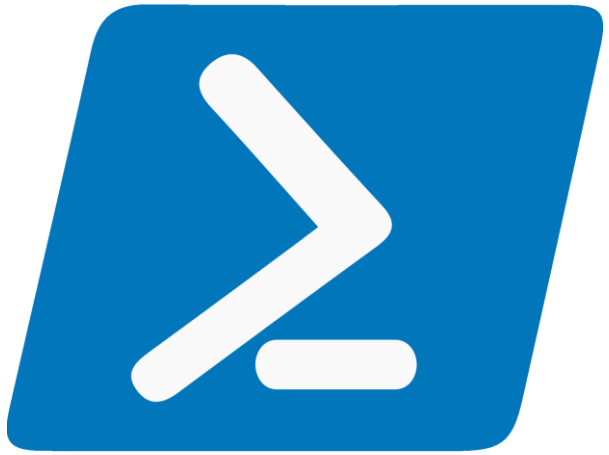
API	Defender XDR Data	Sentinel Data
Azure Monitor API	❌	✅
Graph API	✅	✅
Defender ATP API	⚠️ - MDE Data only	❌

Supported tables

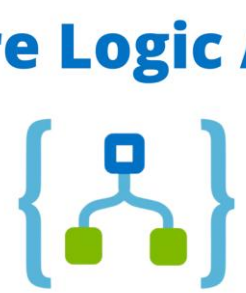
Table Category	Azure Monitor API	Graph API	Graph API (Without Unified XDR)	Defender ATP API
Alerts & behaviors	❌	✅	✅	❌
Apps & identities	❌	✅	✅	❌
Email & collaboration	❌	✅	✅	❌
Devices	❌	✅	✅	✅
Defender Vulnerability Management	❌	✅	✅	✅
Email & collaboration	❌	✅	✅	❌
Cloud Infrastructure	❌	✅	✅	❌
Sentinel - Connector Data	✅	✅	❌	❌
Sentinel - Custom Logs	✅	✅	❌	❌

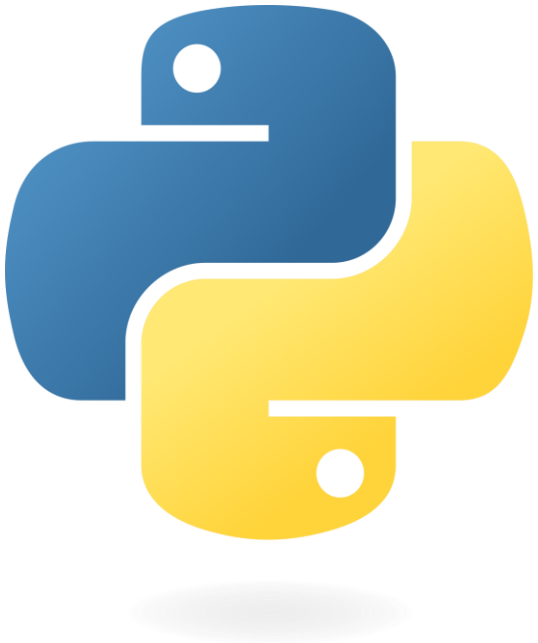
Permissions

API	Application	Permission	Admin Consent
Azure Monitor API	Log Analytics API	Data.Read	Required
Graph API	Graph	ThreatHunting.Read.AI	Required
Defender ATP API	WindowsDefenderATP	AdvancedQuery.Read.All	Required



Azure Logic Apps



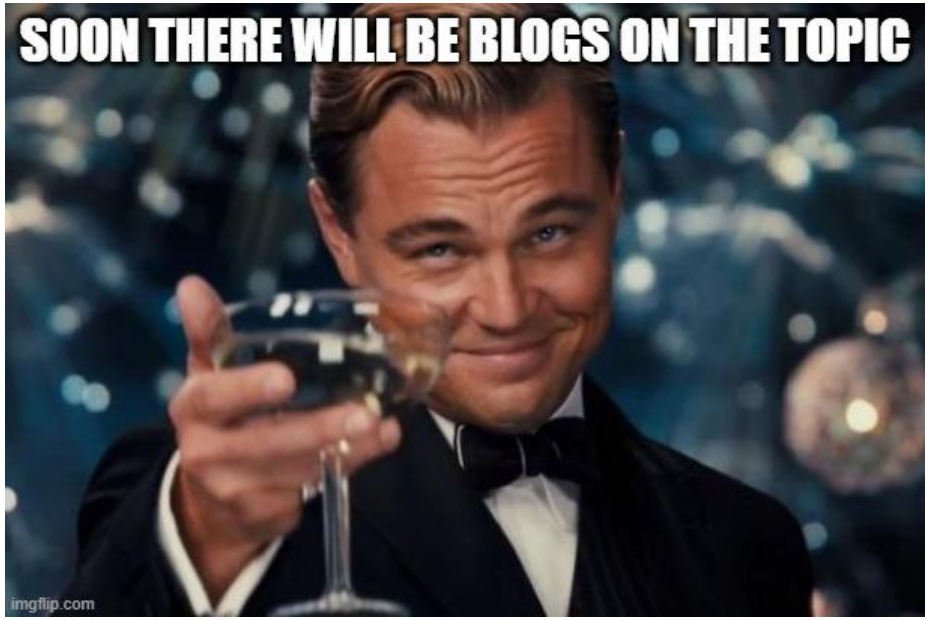


Where to use the APIs

Get started

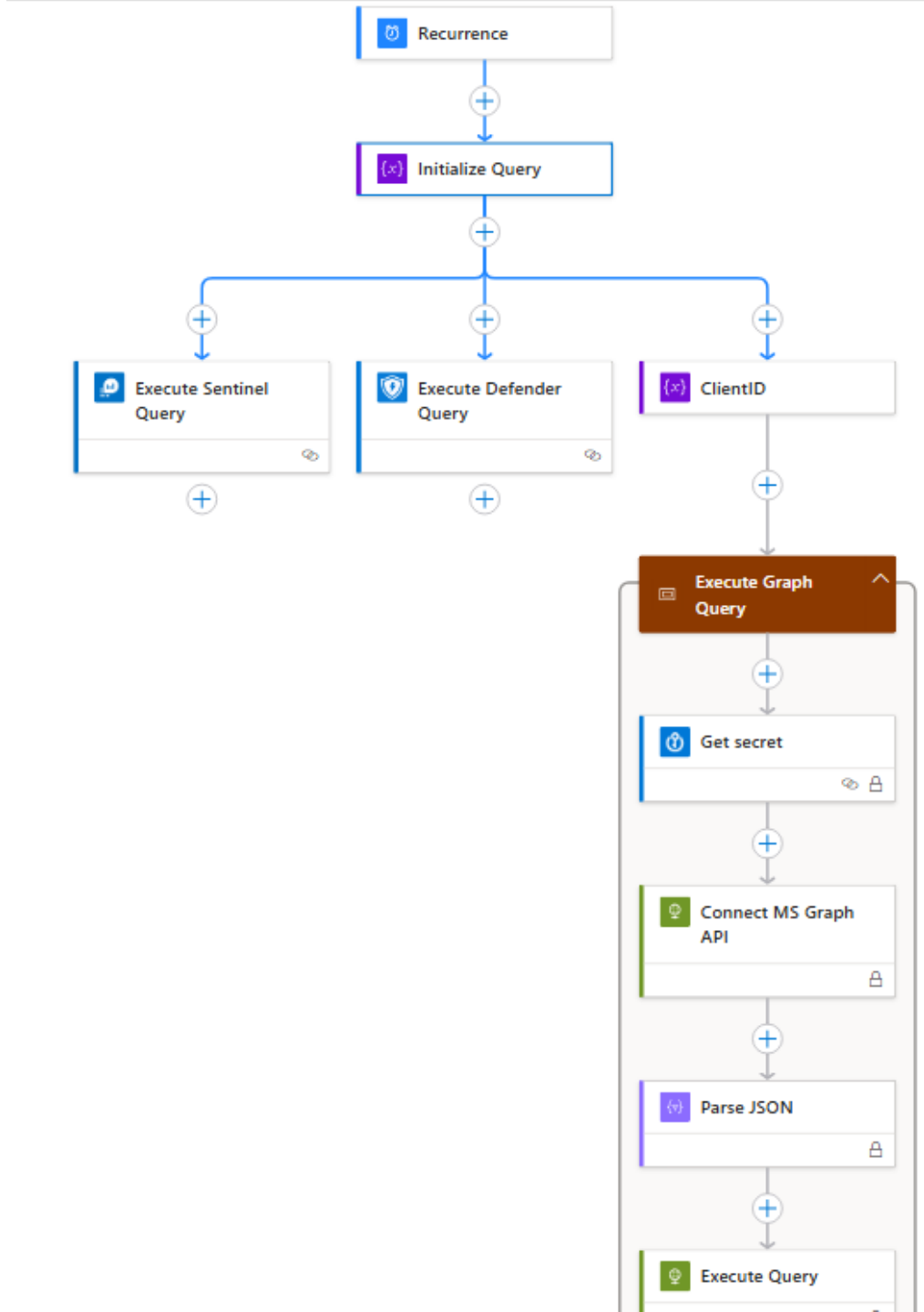
Graph - https://github.com/Bert-JanP/Incident-Response-Powershell/blob/main/Acquisition/ExecuteKQLAdvancedHunting.ps1

Graph Service Principal– https://github.com/Bert-JanP/Incident-Response-Powershell/blob/main/Acquisition/ExecuteKQLAdvancedHuntingServicePrincipal.ps1



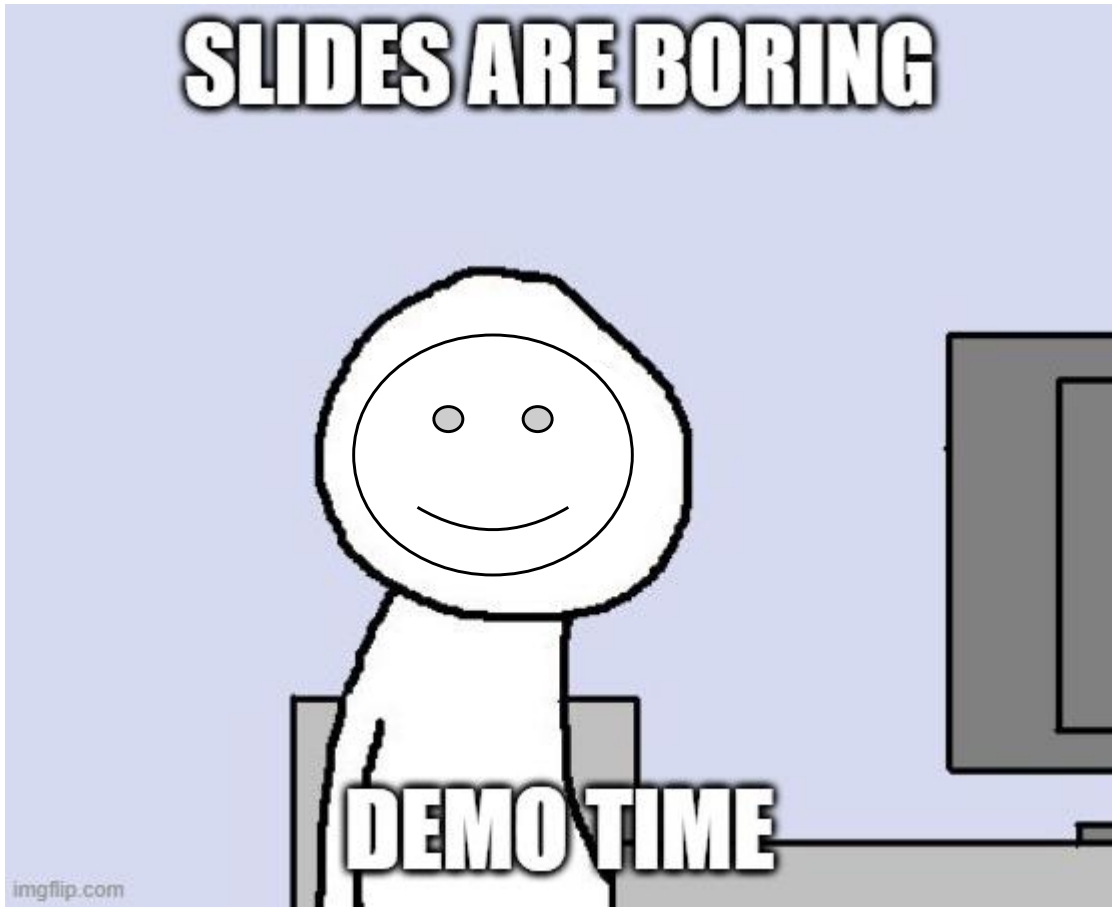
Use the API in Logic Apps

API	Connector Available	Connector Name
Azure Monitor API	✅	Azure Monitor Logs
Graph API	❌	-
Defender ATP API	✅	Microsoft Defender ATP


Recurrence
Initialize Query
Execute Sentinel Query
Execute Defender Query
ClientID
Execute Graph Query
Get secret
Connect MS Graph API
Parse JSON
Execute Query

Logic Apps

- Wrapper for the API
- Integration with Security Tools
- KQL centric solutions
  - Automate and make the results look pretty
  - Reporting
  - Enrichment


SLIDES ARE BORING
DEMO TIME
imgflip.com