KQL<externaldata> Threat Hunting with IoCs

One effective method of tracking security breaches with IoCs is by utilizing KQL in Microsoft 365 Defender or Microsoft Sentinel. This summary is intended to provide guidance on how to leverage "externaldata" in KQL for hunting activities.

KQL / operator	Description
externaldata	externaldata() is a function in KQL that allows you to load external data from sources such as Azure Blob Storage, Azure Data Lake Storage, Azure Synapse Analytics, and even from publicly accessible URLs. The loaded data can be queried and analyzed along with the data in your Kusto cluster. MS docs : externaldata operator - Azure Data Explorer | Microsoft Learn

In 3 steps

Step 1
Collect insights on IoCs from sources such as the MSTIC blog, NIST, cybersecurity vendors and so on.

Step 2
Import the IoCs into a csv file and upload it to an external storage such as GitHub.

Step 3
Use the 'externaldata' operator to hunt suspicious activities in M365 Defender or Microsoft Sentinel.

e.g. Mango Sandstorm with Storm-1084

```
// IoCs C2C - MERCURY and DEV-1084: Destructive attack on hybrid environment
// KQL/MangoSandstorm-Storm-1084.md at main · LearningKijo/KQL · GitHub

let MangoSandstorm = externaldata(Indicator:string, Type:string, Description:string)
[@'https://raw.githubusercontent.com/LearningKijo/KQL/main/KQL-XDR-Hunting/ThreatHunting/IOCs-
Folder/MangoSandstorm-Storm-1084-IOCs-042023.csv'] with (format='csv', ignorefirstrecord = true);
let Domains = (MangoSandstorm | where Type == "Domain"| project Indicator);
let IPaddress = (MangoSandstorm | where Type == "IP address"| project Indicator);
DeviceNetworkEvents
| where Timestamp > ago(7d)
| where RemoteUrl has_any (Domains) or RemoteIP in (IPaddress)
| project-reorder Timestamp, DeviceId, DeviceName, RemoteUrl, RemoteIP, ActionType
```

Timestamp	DeviceId	DeviceName	RemoteUrl	RemoteIP	ActionType	RemotePort	LocalIP
May 1, 2023 12:33:25 PM	62525	win11a		141.95.22.153	ConnectionSuccess	443	10.160.99.6
May 1, 2023 12:33:28 PM	62525	win11a	https://vatacloud.com	141.95.22.153	ConnectionSuccess	443	10.160.99.6
May 1, 2023 12:33:28 PM	62525	win11a		141.95.22.153	ConnectionSuccess	80	10.160.99.6
May 1, 2023 12:33:28 PM	62525	win11a	http://vatacloud.com/	141.95.22.153	ConnectionSuccess	80	10.160.99.6
May 1, 2023 12:33:30 PM	62525	win11a		141.95.22.153	HttpConnectionInspected	80	10.160.99.6
May 1, 2023 12:34:24 PM	62525	win11a	https://pairing.rport.io	49.12.228.207	ConnectionSuccess	443	10.160.99.6
May 1, 2023 12:35:32 PM	62525	win11a	https://pairing.rport.io	49.12.228.207	ConnectionSuccess	443	10.160.99.6
May 2, 2023 9:13:13 AM	ce25a	vm1cyberlab		141.95.22.153	ConnectionSuccess	443	10.0.0.4

GitHub : 11-kql-externaldata-IoCs-threathunting.md
https://github.com/LearningKijo/KQL/blob/main/KQL-Effective-Use/11-kql-externaldata-IoCs-threathunting.md