KQL Threat Hunting with IoCs

Tracking Indicators of Compromise (IoCs) is a crucial aspect of threat hunting, and the Microsoft Security Blog frequently provides IoC lists as examples. This summary aims to assist in tracking IoCs by leveraging the KQL column name.

In KQL threat hunting, just like with column names, it's important to consider which “String operators” to use.

e.g., ==, =~, has, in, startswith, endswith

IoCs	Advanced Hunting, Column Name
Domain	- RemoteUrl
IP address	- RemoteIP
File name	- FileName - InitiatingProcessFileName
Hash	- MD5 - SHA1 - SHA256 - InitiatingProcessMD5 - InitiatingProcessSHA1 - InitiatingProcessSHA256
File path	- FolderPath - InitiatingProcessFolderPath
Command line	- ProcessCommandLine - InitiatingProcessCommandLine
Registry key	- RegistryKey - RegistryValueType - RegistryValueName - RegistryValueData

// Monitoring C&C connection
// Analysis of cyberattack on U.S. think tanks, non-profits, public sector by unidentified attackers - Microsoft Security Blog

```
DeviceNetworkEvents
| where RemoteUrl has "pandorasong.com"

DeviceNetworkEvents
| where RemoteIP == "95.216.59.92"
```

// Monitoring SolarWinds processes launching CMD with echo
// Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers - Microsoft Security Blog

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "SolarWinds.BusinessLayerHost.exe"
| where FileName == "cmd.exe" and ProcessCommandLine has "echo"
```

// Monitoring surface potential Mercury PowerShell script backdoor initiating commands
// MERCURY and DEV-1084: Destructive attack on hybrid environment - Microsoft Security Blog

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "powershell.exe"
| where InitiatingProcessCommandLine contains_cs @"c:¥programdata¥db.ps1"
| summarize makeset(ProcessCommandLine), min(Timestamp), max(Timestamp) by DeviceId
```

// Monitoring AV setting with Tamper Protection
// KQL/02-kql-MDE-TamperProtection.md at main · LearningKijo/KQL (github.com)

```
DeviceRegistryEvents
| where Timestamp > ago(30d)
| where RegistryKey has @"HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Windows Defender"
```

Advanced Hunting schema
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-schema-tables?view=o365-worldwide