Hunting Using KQL

By Grant Knoetze

Create Queries for Hunting in KQL

Kusto Query Language (KQL) is the query language used to perform analysis on data to create Analytics, Workbooks, and perform Hunting in Microsoft Sentinel and Microsoft Defender XDR. Understanding how to summarize and visualize data with a KQL statement provides the foundation to build efficient threat detections.

Create Queries for Hunting in KQL

- As a security operations analyst or threat hunter, you will have to search using a query language, in Microsoft it is Kusto Query Language (KQL).
- You can query log data using KQL.
- The data is aggregated and correlated for you.
- This allows for pattern detection.

Create Queries for Hunting in KQL

- One such aggregation might be the number of failed logons. This information, combined with a predetermined threshold, can be used to generate an alert for "Account with over 10 failed logons in the past hour" as an example.

Summarize and Render

- The KQL summarize operator performs the calculations. To quickly see a pattern, an analyst can visualize the results in a graph. The KQL render operator performs the visualization. Combining the summarize and render operators provides the foundation for advanced visualizations, including time bucketing and time slicing.

Use the summarize operator

- The count operator with its variations creates a new column with the calculated result for the specified fields.
- The first statement below returns one column that is a unique list of Activity column values.
- The second statement returns a count of SecurityEvent rows where EventID equals 4618, and the count is grouped by Process and Computer. Because of the by clause, the result set contains three columns: Process, Computer, Count.
- Run each Query separately to see the results.

Search for Created Scheduled Tasks

```
SecurityEvent
| where EventID == 4688 // Process creation events
| where NewProcessName contains "schtasks.exe"
| where CommandLine contains "/create" and AccountName != "SYSTEM"
| where TimeGenerated > ago(7d)
| project TimeGenerated, Computer, Account, CommandLine, NewProcessName
```

Search for Malicious Documents with Macros Connecting to a Suspicious Domain

```
SecurityEvent
| where EventID == 4688
| where NewProcessName in ("winword.exe", "excel.exe", "powerpnt.exe")
| where not (CommandLine contains ".microsoft.com" or CommandLine contains ".live.com" or CommandLine contains ".office.com")
| project TimeGenerated, Computer, Account, CommandLine, NewProcessName
```

Search for PowerShell Execution Events That Could Involve a Download

```
SecurityEvent
| where EventID == 4688
| where NewProcessName contains "powershell.exe"
| where CommandLine has_any ("WebClient", "DownloadFile", "http", "https")
| project TimeGenerated, Computer, Account, CommandLine, NewProcessName
```

Search for a Program Attempting to Dump lsass.exe

SecurityEvent

| where EventID == 4656 // Handle to process requested

| where ObjectName contains "lsass.exe“

| where ProcessCommandLine contains "dbgcore.dll" or ProcessCommandLine contains "dbghelp.dll“

| project TimeGenerated, Computer, Account, ProcessName, CommandLine

Search for Malicious Documents with Macros Connecting to Suspicious Domains

```
SecurityEvent
| where EventID == 4688
|where FileName_s in~ ("winword.exe", "excel.exe", "powerpnt.exe“
|where not (CommandLine contains ".microsoft.com" or CommandLine contains ".live.com" or CommandLine contains ".office.com")
|project TimeGenerated, Computer, AccountName_s, FileName_s, CommandLine
```

Search for a Malicious Document that Executed Another Program

```
SecurityEvent
| where EventID == 4688
| where FileName_s in~ ("winword.exe", "excel.exe", "powerpnt.exe")
| where not (    (FileName_s in~ ("splwow64.exe", "msoia.exe", "officeclicktorun.exe")) and    (FolderPath_s startswith "C:\\Windows" or FolderPath_s startswith "C:\\Program Files"))| project TimeGenerated, Computer, FileName_s, FolderPath_s, CommandLine
```

Search for Domains Contacted by a Process Name or PID

```
let processId = "<PID>";AzureNetworkAnalytics_CL
| where InitiatingProcessId_d == processId
| project TimeGenerated, Computer, InitiatingProcessFileName_s, InitiatingProcessId_d, RemoteUrl_s, RemoteIP_s, RemotePort_d, Protocol_s
```

Search for Processes Executed Based on Hash, Name, or Path

```
let fileHash = "806b5269e7aa9c2c82ce247b30a3e92a4f7285b21e2bcf54c8ffad86bd92ea68";SecurityEvent
| where Hash_SHA256_s == fileHash
| project TimeGenerated, Computer, Account_s, ParentProcessName_s, FileName_s, FolderPath_s, Hash_SHA256_s, Hash_MD5_s
```

Query by File Path (Sentinel):

```
let filePath = "<file path>"; SecurityEvent
| where FolderPath_s contains filePath
| project TimeGenerated, Computer, Account_s, ParentProcessName_s, FileName_s, FolderPath_s, Hash_SHA256_s, Hash_MD5_s
```

Find Commands Executed on the System

```
SecurityEvent
| where EventID == 4688
| where FileName_s == "cmd.exe" and (CommandLine_s contains "/c")
| project TimeGenerated, Computer, Account_s, ParentProcessName_s, CommandLine_s, FileName_s, FolderPath_s
```

List All Processes Executed by a Malicious Program

```
let parentProcessId = "<PID>";SecurityEvent
| where ParentProcessId_d == parentProcessId
| project TimeGenerated, Computer, Account_s, ParentProcessName_s, ParentProcessId_d, FileName_s, CommandLine_s, FolderPath_s, Hash_SHA256_s
```

List Domains That Resolved to a Specific IP

```
let givenIP = "<given ip>"; AzureNetworkAnalytics_CL
| where RemoteIP_s == givenIP
| project TimeGenerated, Computer, RemoteIP_s, RemoteUrl_s, InitiatingProcessFileName_s, CommandLine_s
```

Find Processes Created by a Specific User

```
let username = "<username>"; SecurityEvent
| where Account_s == username
| project TimeGenerated, Computer, Account_s, ParentProcessName_s, ParentProcessId_d, FileName_s, CommandLine_s, FolderPath_s, Hash_SHA256_s
```

Find Dropped/Downloaded Script Files

```
SecurityEvent
| where EventID == 4663 // File creation/modification event
| where FileName_s endswith ".js" or FileName_s endswith ".vbs" or FileName_s endswith ".ps1"
| where FolderPath_s startswith "C:\\Users" and (FolderPath_s contains "AppData\\Local\\Temp" or FolderPath_s startswith "C:\\Users\\Public")
| project TimeGenerated, Computer, Account_s, ParentProcessName_s, CommandLine_s, FileName_s, FolderPath_s, Hash_SHA256_s
```

Detect the Mounting of .iso or .img Images

```
SecurityEvent
| where EventID == 4663  // File access event
| where FileName_s endswith ".iso.lnk" or FileName_s endswith ".img.lnk“
| project TimeGenerated, Computer, Account_s, ParentProcessName_s, CommandLine_s, FileName_s, FolderPath_s, Hash_SHA256_s
```