DEFENDER ADVANCED THREAT HUNTING

MORE THAN MEETS THE EYE


WELCOME

AGENDA

01 Who I am

02 What Advanced Hunting/ KQL are

03 Basic KQL

04 Missing Software

05 Network Conenctions

06 The Future is YOURS!

WHO IS SHECKY?

- Senior Security Engineer
- 25+ years in IT/Infosec
- Trainiac
- Family man

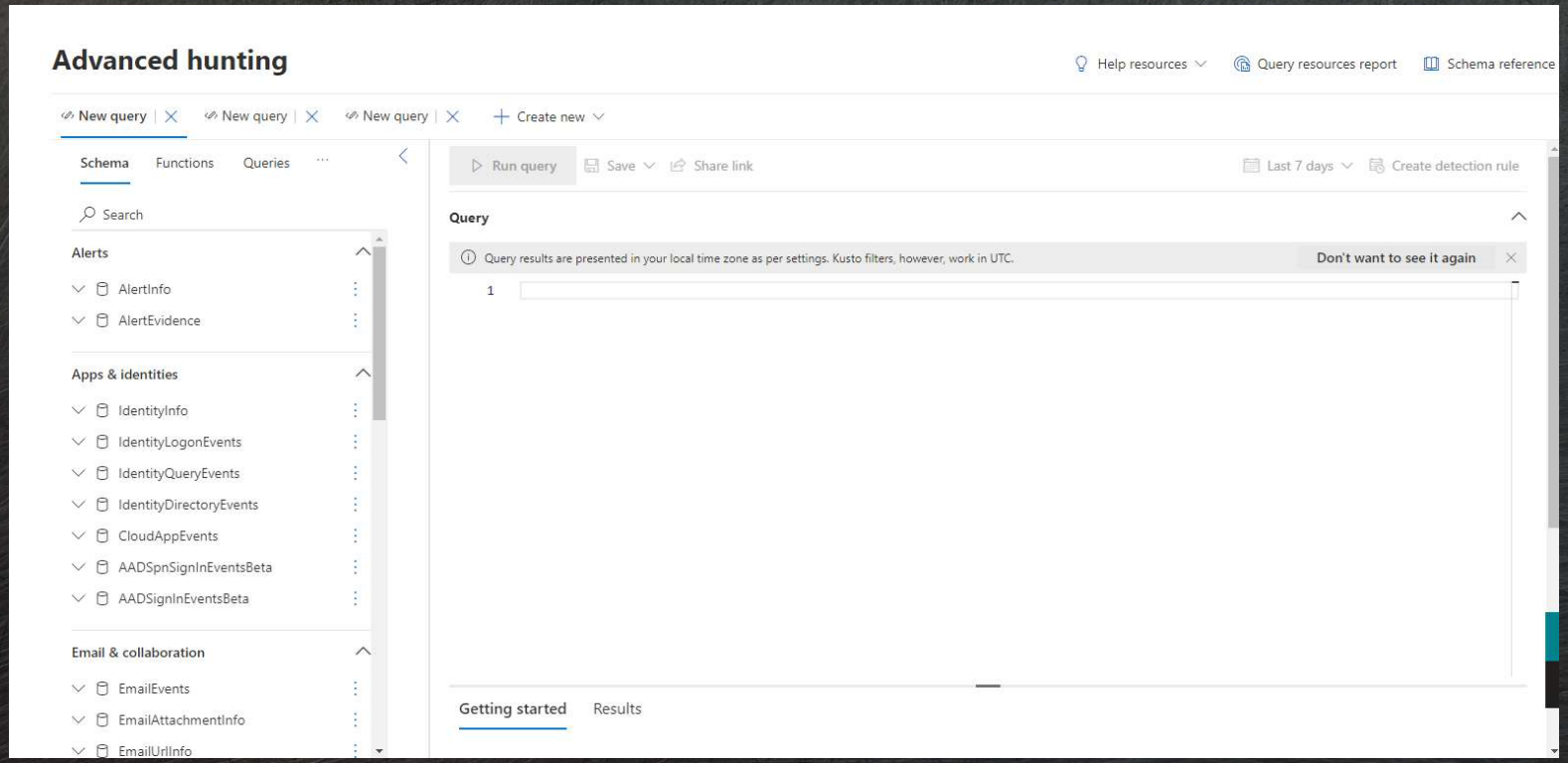
CONTACT INFO

mbkavka@siliconshecky.com
@siliconshecky
@siliconshecky@infosec.exchange
www.siliconshecky.com
github.com/siliconshecky

WHAT IS DEFENDER ADVANCED HUNTING/KQL

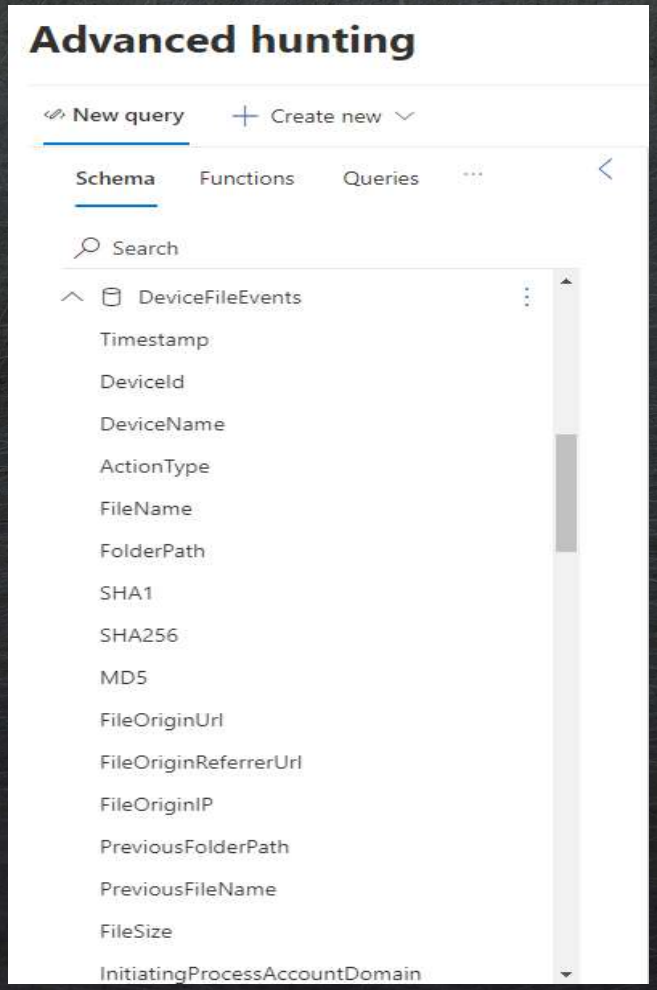
- Defender Advanced Hunting is part of the Defender Security suite
- Telemetry comes from Different Defender products including :
  - Office
  - Endpoint
  - Identity
- Tons of Data available, rivals Sysmon information: Sysmon vs Microsoft Defender for Endpoint, MDE Internals 0x01 | by Olaf Hartong | FalconForce | Medium
- All Stored in a backend Database
- KQL stands for Kusto Query Language
- Kusto is the internal Microsoft name for Azure Data Explorer
- KQL is the query language to sort through the data

THE BASICS




```
DeviceProcessEvents
    | where Timestamp > ago(1d)
    | where FileName contains "whoami"
    | where InitiatingProcessParentFileName != "Skype.exe"
    | project Timestamp, DeviceName, AccountName, InitiatingProcessFileName, FileName,
ProcessCommandLine, DeviceId, ReportId, InitiatingProcessParentFileName
```

THE BASICS


Advanced hunting
New query
Create new
Schema
Functions
Queries
Search
DeviceFileEvents
Timestamp
DeviceId
DeviceName
ActionType
FileName
FolderPath
SHA1
SHA256
MD5
FileOriginUrl
FileOriginReferrerUrl
FileOriginIP
PreviousFolderPath
PreviousFileName
FileSize
InitiatingProcessAccountDomain

QUERY LAYOUT

```
DeviceProcessEvents
    | where Timestamp > ago(1d)
    | where FileName contains "whoami"
    | where InitiatingProcessParentFileName != "Skype.exe"
    | project Timestamp, DeviceName, AccountName, InitiatingProcessFileName,
FileName, ProcessCommandLine, DeviceId, ReportId, InitiatingProcessParentFileName
```

- Table Name (i.e DeviceProcessEvents, DeviceEvents)
- Qualifiers:
- Where statement both include and exclude
- And/Or
- Multiple Where to tighten results
- Output:
- Project to select specific tables
- Comments use a double // before them and can occur anywhere

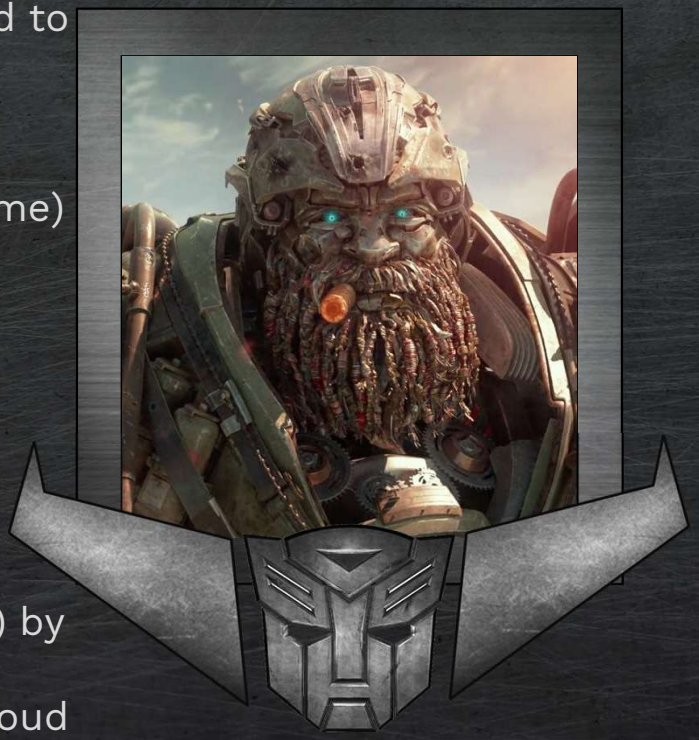
ADVANCED ITEMS

- Use Variables
- If Statements
- Distinct Output Based on Data Name(i.e DeviceName)
- Summarize sets
- Output based on set containing or not containing data
- Join Multiple Tables on specific items (i.e. DeviceName)

SOFTWARE QUERIES

DEFENDER HUNTING QUERY

```
DeviceTvmSoftwareInventory
        | where DeviceName !contains "<computer name not wanted to search on like VDIs>"
        | where OSPlatform !contains "server"
        | where OSPlatform !contains "linux"
        | summarize all_software_installed = make_set(SoftwareName) by DeviceName
        | where set_has_element( all_software_installed, "qualys_cloud_security_agent") == 0
```



AZURE LOG ANALYTICS

```
AppInventory_CL
        | where TimeGenerated > ago(120d)
        | summarize all_software_installed = make_set(AppName_s) by ComputerName_s
        | where set_has_element( all_software_installed, "Qualys Cloud Security Agent") == 0
```

REMOTE DESKTOP CONNECTION QUERY

```
DeviceNetworkEvents
| where Timestamp > ago(7d)
| where ActionType == "ConnectionSuccess"
| where RemotePort == 3389
| where InitiatingProcessFileName == "mstsc.exe"
| join DeviceLogonEvents on DeviceName
//| where IsLocalAdmin != 1
| where AccountName !contains "<service account name>"
| where AccountName !contains "<SCCM Server Name>"
| where AccountName !endswith "$"
| where InitiatingProcessAccountName1 != "system"
| where LogonType contains "Interactive"
| summarize any(AccountName, InitiatingProcessAccountName,
LogonType, IsLocalAdmin, RemoteUrl, RemotePort,
InitiatingProcessFileName,  InitiatingProcessCommandLine) by
DeviceName
//| project DeviceName, InitiatingProcessAccountName, LogonType,
IsLocalAdmin, RemoteUrl, RemotePort, InitiatingProcessFileName,
InitiatingProcessCommandLine, Timestamp
```

POTENTIAL TROUBLES

- Pulling Data Into SIEM is limited
- Ingesting the data into Sentinel is not free
- Queries only go back 30 days
- Data from the endpoint can take 20 minutes to see in Defender
- For real Advanced Items you potentially have to go through JSON
- Not everything that the defender agent sees is available
- API usage can get goofy
- Finally, many new features are Ala-Carte

LINKS

Must Learn KQL:
https://github.com/rod-trent/MustLearnKQL -

Defender Ninja Training:
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/become-a-microsoft-defender-for-endpoint-ninja/ba-p/1515647 -

Microsoft KQL Repository:
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries -

- Advanced Hunting using KQL can be very powerful
- The data inside of Defender is very fruitful
- Looking for things like RDP or Software missing (or installed) helps security overall
- You can create custom detections from these queries provided you have DeviceIds, ReportIds, and Timestamps projected


THANK YOU