Microsoft Defender for Endpoint

Master Class

Trainer DI Thomas Schleich

November 2024

Module 6

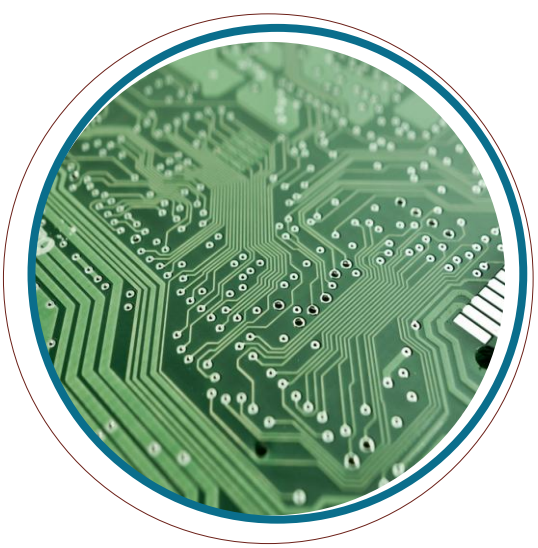
Advanced Hunting

Module 5 Contents:

- **Advanced Hunting**
- **Kusto Query Language**
  - General
  - Data flow pipeline
  - Statements

© 2023 Fast Lane

3



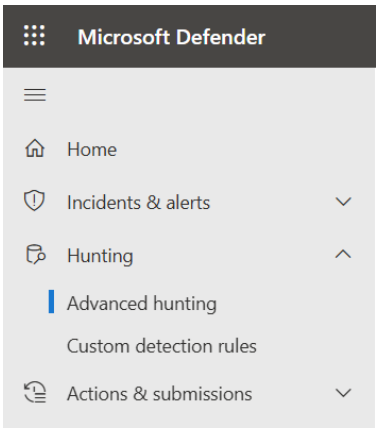
Advanced Hunting

© 2023 Fast Lane

4

Advanced Hunting

' … *is a query-based threat hunting tool …* '



- Modes
  - guided
  - advanced
- Data freshness
  - Event and activity date (alerts, security events, …)
    - immediately
  - Entity data
    - up to 24 hours

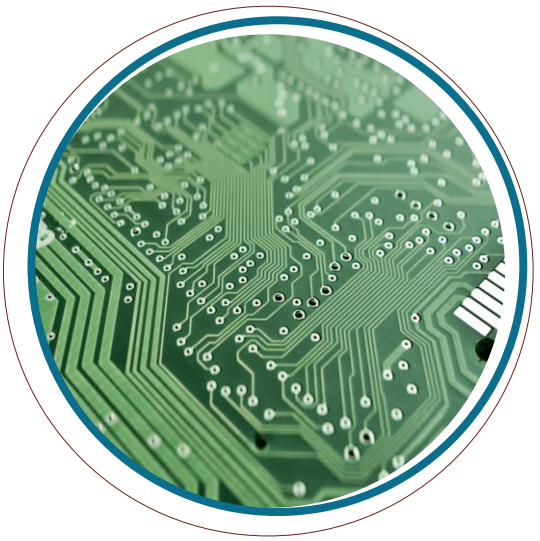
© 2023 Fast Lane

Advanced Hunting

- Schema - Tables
  - from multiple Defender Sources
  - Description in documentation
- Queries
  - could be saved query or function
  - added to schema for all administrators
- Result used
  - for investigation
  - Take actions
  - Detection rules

© 2023 Fast Lane

Source: https://learn.microsoft.com/en-us/defender-endpoint/onboard-windows-client



Kuste Query Language

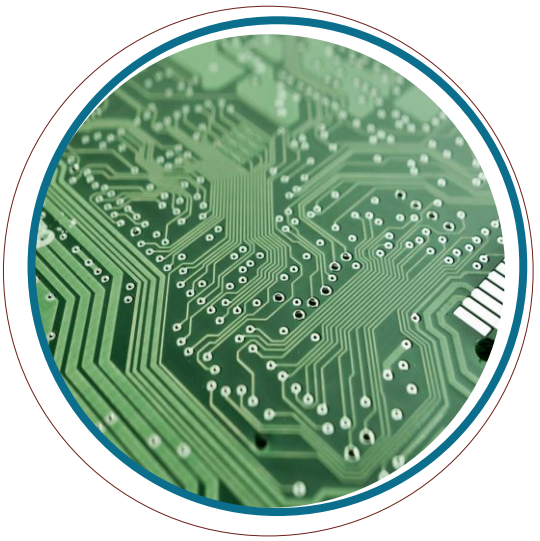
General

General

Some rules for KQL

- Case sensitivity
  - Tablenames
  - Fieldnames
  - Operators
  - Functions
- Comments: //
- Line breaks: before |
- Time: always saved as UTC

Source: https://learn.microsoft.com/en-us/defender-endpoint/onboard-windows-client



Data Flow pipeline

Source: https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction

Data Flow Pipeline

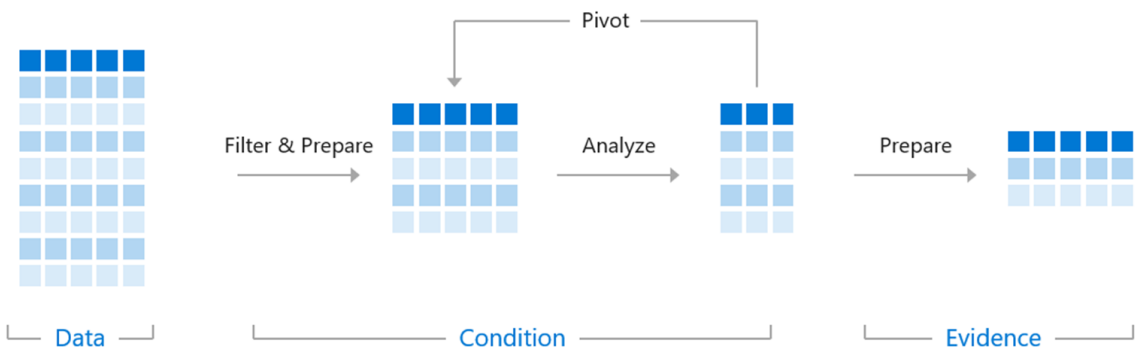
Overview

- Each statement starts with either a
  - Table
  - Variable(s) declaration(s)
  - Functions with result type table
- Variable declaration must end with ;
- Use | to pass data from table to operator
  - Multiple | are possible

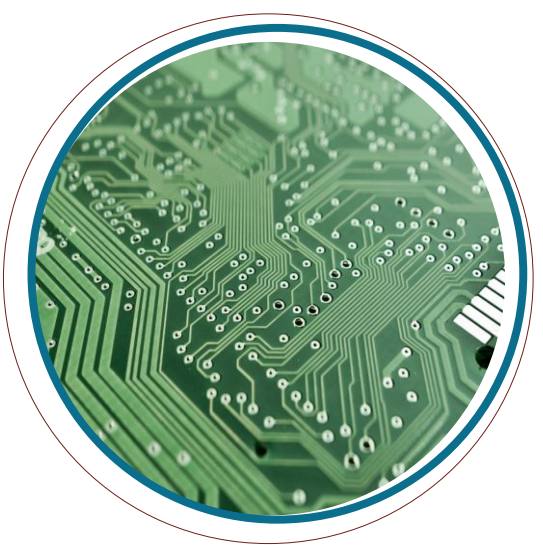
Source: https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction

Data Flow Pipeline

```
SecurityEvent | where EventID == "4626" | summarize count() by Account | limit 10
```



© 2023 Fast Lane



Basic statements

© 2023 Fast Lane

Basic statements

- Getting table data

```
DeviceInfo
// Case-sensitivity
```

- Using Pipeline

```
DeviceInfo
| limit 5
// limit doesn't sort the records.
// Alias for limit: take

DeviceInfo
| top 5 by DeviceName desc
// Records sorted first
```

© 2023 Fast Lane

Basic statements

- Sorting results

```
DeviceInfo
| sort by DeviceName asc
DeviceInfo
| sort by DeviceName asc, PublicIP desc
// Alias for sort: order
```

© 2023 Fast Lane

Basic statements

- Variables

```
let lmt = 3;
DeviceInfo
| sort by DeviceName asc , Timestamp desc
| limit lmt;
// let creates a variable.

let myTable =
DeviceInfo
| limit 10;
myTable
// A variable could also contain a table.
```

© 2023 Fast Lane

Basic statements

- design result

```
DeviceInfo
| project DeviceName,DeviceType,PublicIP
// only this columns appear in the result

DeviceInfo
| project-away DeviceType,PublicIP
// all columns of DeviceInfo except DeviceType,PublicIP apppear in the result

DeviceInfo
| project-keep Device*,Device*,PublicIP
// project-keep has the same result as project but you could use *
```

© 2023 Fast Lane

Basic statements

- design result

```
DeviceInfo
| project DeviceName,DeviceType,PublicIP
// only this columns appear in the result

DeviceInfo
| project-away DeviceType,PublicIP
// all columns of DeviceInfo except DeviceType,PublicIP apppear in the result

DeviceInfo
| project-keep Device*,Device*,PublicIP
// project-keep has the same result as project but you could use *
```

© 2023 Fast Lane

Basic statements

- Filter records

```
DeviceInfo
| where DeviceName =~ 'Client1'
// =~ case-insensitive

DeviceInfo
| where DeviceName startswith "server" // server*

DeviceInfo
| where DeviceName endswith ".local" // *.local

DeviceInfo
| where DeviceName contains "aztrg2112" // *aztrg2112*
```

© 2023 Fast Lane

Basic statements

- Extends result

```
AlertEvidence
| where EntityType == 'File'
| extend FileSizeKB = FileSize / 1024
| project FileName,FileSize,FileSizeKB

AlertEvidence
| where EntityType == 'File'
| extend FileSizeKB = FileSize / 1024,
         FileSizeMB = FileSize / 1024 / 1024
| project FileName,FileSize,FileSizeKB,FileSizeMB
```

© 2023 Fast Lane

Basic statements

- Remove duplicates

```
DeviceInfo
| project DeviceName
| distinct DeviceName

DeviceInfo
| project DeviceName,PublicIP
| distinct DeviceName,PublicIP

DeviceInfo
| summarize by DeviceName,PublicIP
```

© 2023 Fast Lane

Basic statements

- Group records

```
DeviceInfo
| summarize count() by DeviceName

DeviceInfo
| summarize count() by DeviceName,PublicIP

DeviceInfo
| summarize Qty = count() by DeviceName,PublicIP
| sort by DeviceName asc, Qty desc
```

© 2023 Fast Lane

Basic statements

- Group records
- some aggregate functions

sum()	make_list()	arg_max()
avg()	make_set()	arg_min()
min()	make_bag()	
max()		

© 2023 Fast Lane

Basic statements

Join tables

- union
  - 'concatenates' two or more tables
- join
  - 'joins' two tables using key properties

© 2023 Fast Lane

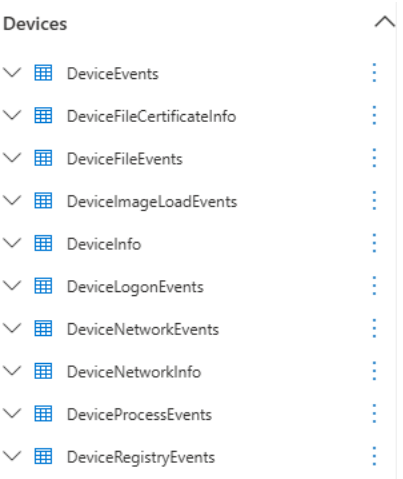
Basic statements

- extracting text
  - extract() function - use regular expression
  - parse operator
- expanding arrays
  - mv-expand operator
- expanding json objects
  - parse_json() function to convert string to json object
  - evaluate operator + bag_unpack() function

© 2023 Fast Lane

Source: https://learn.microsoft.com/en-gb/defender-xdr/advanced-hunting-schema-tables

Device Tables



© 2023 Fast Lane

Device Tables

DeviceInfo

Machine information, including OS information

DeviceId, DeviceName, PublicIP, OSPlatform, IsExcluded, DeviceType, JoinType, LoggedOnUsers, …

DeviceEvents

Multiple event types, including events triggered by security controls such as Windows Defender Antivirus and exploit protection

ActionType, FileName, ProcessID, ProcessCommandLine, Registry*, …

© 2023 Fast Lane

Device Tables

DeviceFileEvents

File creation, modification, and other file system events

DeviceId, DeviceName, ActionType, FileName, FolderPath, InitiatingAccount*, InitiatingProcess* …

DeviceLogonEvents

Sign-ins and other authentication events

ActionType, DeviceName, LogonType, Account*, Remote*, AdditionalFields, …

© 2023 Fast Lane

Device Tables

DeviceNetworkInfo

Network properties of machines, including adapters, IP and MAC addresses, as well as connected networks and domains

DeviceNetworkEvents

Network connection and related events

Remote*, Local*, …

© 2023 Fast Lane

Device Tables

DeviceProcessEvents

Process creation and related events

DeviceRegistryEvents

Creation and modification of registry entries

DeviceImageLoadEvents

DLL loading events

RegistryKeyCreated,
RegistryKeyDeleted,
RegistryKeyRenamed,
RegistryValueDeleted,
RegistryValueSet

© 2023 Fast Lane

Some Examples

© 2023 Fast Lane

Try to read the query

- Start PowerShell without profile

```
DeviceProcessEvents
| where ProcessCommandLine has_all ("-nop", "powershell.exe")
| summarize TotalCommands = dcount(ProcessCommandLine),
            ExecutedCommands = make_set(ProcessCommandLine) by DeviceName
```

- Disable Defender

```
DeviceProcessEvents
| where FileName =~ "powershell.exe"
| where ProcessCommandLine has_any ("Add-MpPreference","Set-MpPreference")
| where ProcessCommandLine has_any ("ExclusionProcess","ExclusionPath")
```

© 2023 Fast Lane

Try to read the query

- Last information of devices by name

```
DeviceInfo
| where isnotempty(DeviceName) and isnotempty(OSPlatform)
| summarize arg_max(Timestamp, *) by DeviceName
```

- Last network information of non-excluded devices by DeviceID

```
DeviceNetworkInfo
| join DeviceInfo on DeviceId
| where not(IsExcluded)
| summarize arg_max(Timestamp,*) by DeviceId
```

© 2023 Fast Lane

Try to read the query

- Webrequests by PS

```
DeviceEvents
| extend _tmp = parse_json(AdditionalFields)
| where _tmp.Command contains 'Invoke-WebRequest'
| order by Timestamp
```

- Open service ports

```
let RemoteServices = dynamic([22, 139, 445, 3389, 5900, 5985, 5986]);
DeviceNetworkEvents
| where ActionType == "ListeningConnectionCreated"
| where LocalPort in (RemoteServices)
| summarize OpenPorts = make_set(LocalPort),
            TotalOpenRemoteServicesPorts = dcount(LocalPort) by DeviceName
| sort by TotalOpenRemoteServicesPorts
```

© 2023 Fast Lane

More queries and hints for hunting

- https://github.com/Bert-JanP/Hunting-Queries-Detection-Rules/tree/main/Defender%20For%20Endpoint
- https://github.com/Bert-JanP/Hunting-Queries-Detection-Rules

© 2023 Fast Lane

End of Module 6

© 2023 Fast Lane

35