



Throwing KQL Like a Shuriken

Gianni Castaldi

Alex Verboon

Workplace Ninja Summit 2022



www.wpninjas.eu
#WPNinjaS

Platinum Sponsor



PATCH MY PC



**Microsoft
Security**

Gold Sponsor

glueckkanja gab

baseVISION
SECURE & MODERN WORKPLACE



RECAST SOFTWARE

LIQUIT

Lenovo



Snapdragon

Silver and Special Sponsors



LUZERN
FACEBOOK
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC  USION


SCAPPMAN

APPMANAGEVENT.COM
2022
OCTOBER 7
NETHERLANDS

dinext.



About Gianni

www.wpninjas.eu
#WPNinjaS

Focus

Microsoft Security

From

IJmuiden, Netherlands

My Blog

www.kustoking.com



Certifications

SC-200, and a lot of legacy

Hobbies

Kusto, Mountain biking and our 2 sons

Contact

gianni@kustoking.com



About Gianni Castaldi

www.wpninjas.eu
#WPNinjaS

Focus

Cyber Security

From

IJmuiden Netherlands

My Blog

www.kustoking.com



Certifications

GCFE, SC-200, and a lot of legacy

Hobbies

Our 2 sons, Kusto and mountain biking

Contact

gianni@kustoking.com



About Alex Verboon

www.wpninjas.eu
#WPNinjaS

Focus
Microsoft Security


From
Switzerland

My Blog
www.Verboon.info



Certifications
SC-200, GSEC

Hobbies
Music & Tech

Contact
 @alexverboon



Agenda

www.wpninjas.eu
#WPNinjaS

Key takeaways:

- KQL isn't that hard
- Goal 2

Why you should learn KQL

Kusto Basics

Kusto Performance

Parse & Extract

External Data

Joining Data

Scan Operator

Detections

Hunting

More KQL

Why you should learn KQL





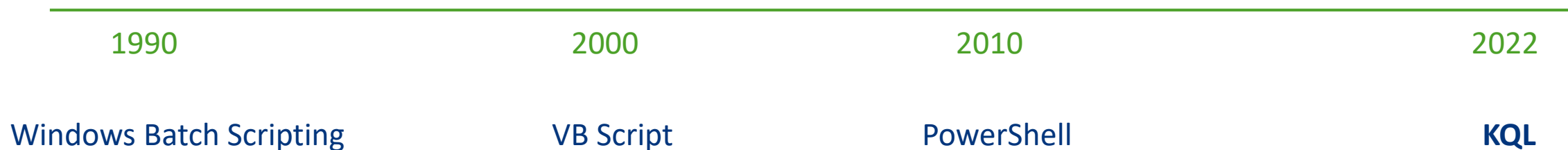
Why you should learn KQL

www.wpninjas.eu
#WPNinjaS

IT Pro Toolbox



Skills that help you mastering your daily tasks as an IT Pro





Why you should learn KQL

www.wpninjas.eu
#WPNinjaS



Developer

Developers design, build, test, and maintain cloud solutions.



Administrator

Administrators implement, monitor, and maintain Microsoft solutions.



Solution Architect

Solutions architects have expertise in compute, network, storage, security.



Data Engineer

Data engineers design and implement the management, monitoring, security, and privacy of data using the full stack of data services.



Data Scientist

Data scientists apply machine learning techniques to train, evaluate, and deploy models that solve business problems.



AI Engineer

AI engineers use Cognitive Services, Machine Learning, and Knowledge Mining to architect and implement Microsoft AI solutions.



DevOps Engineer

DevOps engineers combine people, process, and technologies to continuously deliver valuable products and services that meet end user needs and business objectives.



Security Engineer

Security engineers implement security controls and threat protection, manage identity and access, and protect data, applications, and networks.



Functional Consultant

Functional consultants leverage Microsoft Dynamics 365 and Microsoft Power Platform to anticipate and plan for customer needs.

No matter what IT career path you pursue, you'll meet **KQL**



Why you should learn KQL

www.wpninjas.eu
#WPNinjaS

You can use your KQL skills everywhere

- Azure Monitor
- Azure Log Analytics
- Azure Data Explorer
- Azure Resource Graph
- Microsoft Sentinel
- Microsoft 365 Defender
- Microsoft Endpoint Manager (Configuration Manager & Intune)
- Microsoft Purview

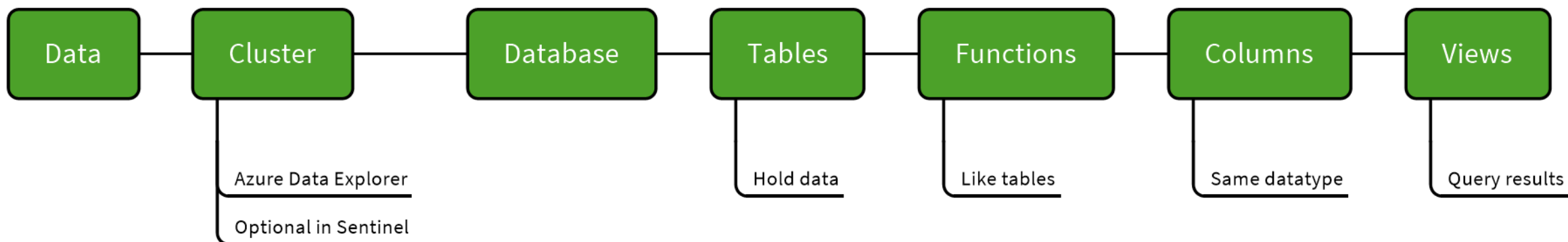
KQL Basics





KQL Basics

www.wpninjas.eu
#WPNinjaS

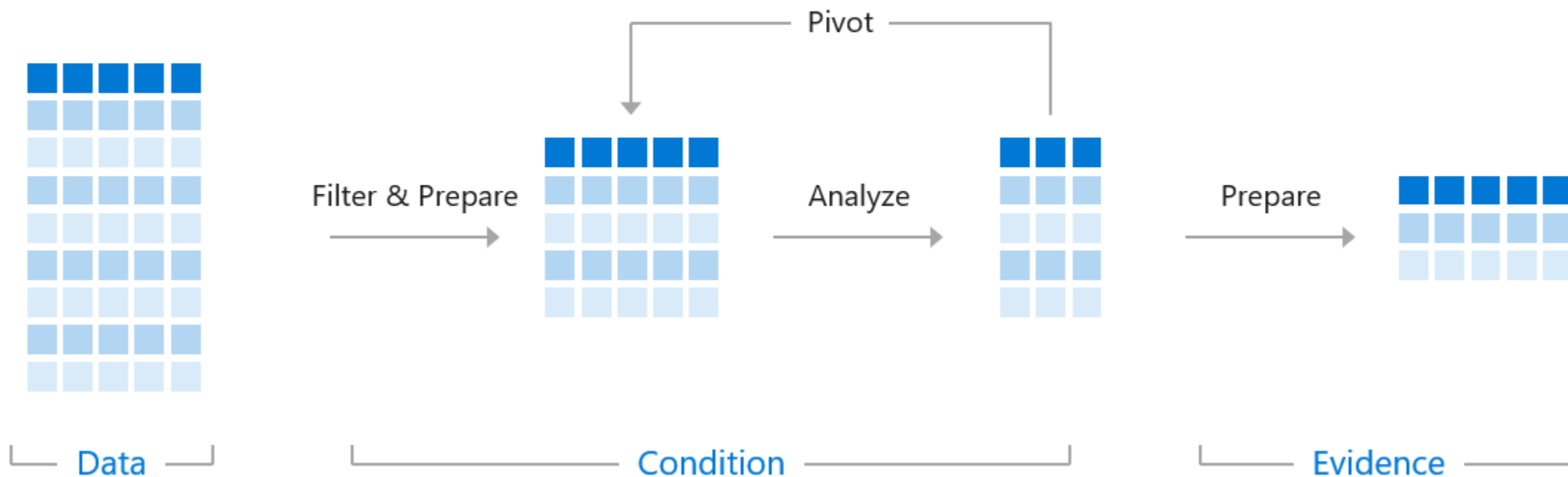




KQL Basics

www.wpninjas.eu
#WPNinjaS

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





KQL Basics

www.wpninjas.eu
#WPNinjaS

- Let
- search
- where
- extend
- order by
- Project



The **let** statement allows you to create variables that you can use within your KQL queries.

- Variable with a single value
- Variable with multiple values
- Variable with data from watchlists
- Variable with data from a KQL query



KQL Basics - let

www.wpninjas.eu
#WPNinjaS

Assign value to a
variable

The screenshot shows the Microsoft Sentinel KQL query editor. The top bar includes a 'New Query 1*' tab, a 'Run' button, and a 'Time range: Last 7 days' selector. The query editor contains the following KQL code:

```
1 // define computername
2 let xComputerName = "testmachine65";
3 DeviceEvents
4 | where DeviceName has (xComputerName)
5 | project TimeGenerated, DeviceName, ActionType
```

Below the query editor, the 'Results' tab is selected, showing a message: 'No results found from the last 24 hours. Try [selecting another time range](#)'.

On the left side of the interface, there is a vertical sidebar labeled 'Schema and Filter'.



Assign multiple
values to a
variable

KQL Basics - let

www.wpninjas.eu
#WPNinjaS

The screenshot shows the Microsoft Sentinel KQL query editor. At the top, there are tabs for 'New Query 1*' and 'New Query 2*'. The active query is named 'MTPLabSentinel01'. A 'Run' button is visible, along with a 'Time range' dropdown set to 'Last 7 days'. The query text is as follows:

```
1 // define computername
2 let xComputerName = dynamic(["testmachine65","testserver66"]);
3 DeviceEvents
4 | where DeviceName has_any (xComputerName)
5 | project TimeGenerated, DeviceName, ActionType
6 | summarize arg_max(TimeGenerated,*) by DeviceName
```

Below the query editor, there are tabs for 'Results' and 'Chart'. The 'Results' tab is active, showing a message: 'No results found from the last 24 hours. Try [selecting another time range](#)'.

On the left side of the interface, there is a vertical sidebar labeled 'Schema and Filter'.



KQL Basics - let

www.wpninjas.eu
#WPNinjaS

Reference values
from a Sentinel
watchlist

Selected workspace: mtlabsentinel01

New Query 1* New Query 2* New Query 3* x New Query 4* + Feedback Queries

MTPLabSentinel01 Run Time range: Set in query Save Share + New alert rule Export Pin to

```
1 _GetWatchlist('HighValueAssets')
2
3
4 let xComputerName = _GetWatchlist('HighValueAssets')
5 | extend xComputerName = ["Asset Name"]
6 | project xComputerName;
7 DeviceEvents
8 | where DeviceName has_any (xComputerName)
9 | project TimeGenerated, DeviceName, ActionType
10 | summarize arg_max(TimeGenerated,*) by DeviceName
```

Schema and Filter

Results Chart Add bookmark

<input type="checkbox"/> DeviceName	TimeGenerated [UTC]	ActionType
<input type="checkbox"/> > testmachine67	9/11/2022, 10:55:44.210 AM	DpapiAccessed
<input type="checkbox"/> > client01.corp.net	8/22/2022, 8:59:22.541 PM	DpapiAccessed



KQL Basics - let

www.wpninjas.eu
#WPNinjaS

Reference values
from a kql query

New Query 1*New Query 2*New Query 3*New Query 4*+FeedbackQueriesSettingsBookmarks

MTPLabSentinel01

IdentityInfo: (AccountCloudSID, AccountCreationTime, AccountDisplayName, AccountDomain, AccountName, AccountObjectId, AccountSID, ...)

```
1 // domain accounts
2 let xIdentityInfo = IdentityInfo
3 | summarize arg_max(TimeGenerated,*) by AccountName
4 | where AccountDomain == "corp.net";
5 xIdentityInfo
6 | join kind=leftouter DeviceLogonEvents
7 on $left.AccountName == $right.AccountName
8 | project TimeGenerated, DeviceName, AccountName, OnPremisesDistinguishedName, GroupMembership, AssignedRoles
```

Queries History

Schema and Filter

No queries history

You haven't run any queries yet. To start, go to Queries on the side pane or type a query in the query editor.



KQL Basics - search

www.wpninjas.eu
#WPNinjaS

KQL Performance





KQL Performance

www.wpninjas.eu
#WPNinjaS

Query

```
1 DeviceFileEvents
2 | where Timestamp > ago(30d)
3 | project FileName, SHA1, DeviceId, DeviceName
4 | join kind=inner
5 (
6   DeviceProcessEvents
7   | where Timestamp > ago(30d)
8   | project FileName, FileSha1 = SHA1, DeviceId, DeviceName
```

Query Performance in Defender

Getting Started Results

Export 1000 items Search 0:0.188 Low Chart Type Customize column

FileName	SHA1	DeviceId	DeviceName	FileName1	FileSha1	DeviceId1	DeviceName1
Microsoft Relauncher	6b5638b1c5969da...	723754205638b7d...	x1-2	xpcproxy	a14c220d242e497cba9e...	723754205638b7d9e6d...	x1-2

Query that utilizes more than 100 seconds of CPU is considered a query that consumes excessive resources. Query that utilizes more than 1,000 seconds of CPU is considered an abusive query and might be throttled.

Home > Logs Demo

New Query 1* New Query 2* +

Your query is consuming excessive resources. [Learn more](#)

Demo Run Time range: Set in query Save Share New alert rule Export Pin to Format query

```
8 | where TimeGenerated > ago(720d)
9
10 union withsource=SourceTable *
11 | summarize arg_max(TimeGenerated,*) by SourceTable
12 | where TimeGenerated > ago(720d)
```

Query Performance in Log Analytics

Results Chart

SourceTable	TimeGenerated [UTC] ↑↓	Computer	Origin	Namespace	Name	Val
SecurityEvent	9/4/2022, 10:19:11.053 AM	DC01.na.contosonoteis.com				
Heartbeat	9/4/2022, 10:19:06.360 AM	CH1-AVSMGMTVM				

Query Details

Total CPU 447515 Milliseconds

Data used for processed query 0 KB

Time span of the processed query 128.2 days

Age of processed data 128.2 days

Number of workspaces 1

Number of regions 1

Parallelism Medium

Request ID 151f9064-016a-4b9b-8d37-58346c111b...



KQL Performance

www.wpninjas.eu
#WPNinjaS

Use Time Filters

The time range specifies the set of records that are evaluated for the query based on when the record was created.

Logs

Demo

New Query 1*

Run

Time range: Set in query

Save

Share

New alert rule

Export

Pin to

Format query

```
1 SigninLogs
2 | where TimeGenerated > ago(1d)
3
4 SigninLogs
5 | where TimeGenerated between (datetime(2022-09-01) .. datetime(2022-09-04))
6
7 let startdate=3d;
8 let enddate=1d;
9 SigninLogs
10 | where TimeGenerated between (startofday(ago(startdate))..startofday(ago(enddate)))
11
12
13
```

Results

Chart

TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category	ResultType	Result
> 9/2/2022, 5:24:22.972 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs	50140	None
> 9/2/2022, 5:24:37.044 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs	0	None
> 9/2/2022, 5:24:49.059 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs	0	None
> 9/2/2022, 5:25:00.831 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs	0	None
> 9/2/2022, 5:53:23.898 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs	0	None
> 9/2/2022, 5:30:59.478 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs	50125	None
> 9/2/2022, 5:06:44.839 PM	/tenants/4b2462a4-bbee-495a-...	Sign-in activity	1.0	SignInLogs	50140	None



KQL Performance

www.wpninjas.eu
#WPNinjaS

From search to....

Use **search** to
'**explore**', then
narrow down
using **has** and **==**

The screenshot shows the KQL editor interface with a query being refined in five steps:

```
1 search 'sam'
2
3 search in (SigninLogs) 'sam'
4
5 SigninLogs
6 | search UserPrincipalName:'sam'
7
8 SigninLogs
9 | where UserPrincipalName contains "sam"
10
11 SigninLogs
12 | where UserPrincipalName has "sam"
13
14 SigninLogs
15 | where UserPrincipalName == "sam@verboon.online"
16
17
```

The interface includes a top bar with 'New Query 1*', 'MTPLabSentinel01', a 'Run' button, and a 'Time range : Last 7 days' selector. On the left, a 'Schema and Filter' sidebar shows a tree with 'print_0' and 'searching and filtering'. The bottom of the editor has tabs for 'Results' and 'Chart', and an 'Add bookmark' button.



KQL Performance

www.wpninjas.eu

#WPNinjaS

KQL Performance matters, learn more

- Advanced hunting query best practices
<https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-best-practices?view=o365-worldwide>
- Advanced hunting quotas and usage parameters
<https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-limits?view=o365-worldwide>
- Log query scope and time range in Azure Monitor Log Analytics
<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/scope#query-scope-limits>
- Query best practices
<https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/best-practices>

KQL Parse & Extract





KQL Parse & Extract

www.wpninjas.eu

#WPNinjaS

```
1 // Oldschool extract with regex
2 let Table = datatable(ParseMe:string)
3 [
4   'fruit="Apples", color="Orange", packing="Bottle"',
5   'fruit="Bananas", color="Red", packing="Crate"',
6   'fruit="Pears", color="Green", packing="Box"',
7   'fruit="Cherries", color="Yellow", packing="Envelope"',
8   'fruit="Oranges", color="Blue", packing="Tube"'
9 ];
10 Table
```

Results

Chart



Add bookmark



ParseMe



>

fruit="Apples", color="Orange", packing="Bottle"



>

fruit="Bananas", color="Red", packing="Crate"



>

fruit="Pears", color="Green", packing="Box"



>

fruit="Cherries", color="Yellow", packing="Envelope"



>

fruit="Oranges", color="Blue", packing="Tube"



```
1 // Oldschool extract with regex
2 let Table = datatable(ParseMe:string)
3 [
4   'fruit="Apples", color="Orange", packing="Bottle"',
5   'fruit="Bananas", color="Red", packing="Crate"',
6   'fruit="Pears", color="Green", packing="Box"',
7   'fruit="Cherries", color="Yellow", packing="Envelope"',
8   'fruit="Oranges", color="Blue", packing="Tube"'
9 ];
10 Table
11 | extend fruit = extract('fruit="(\w+)"',1,ParseMe)
12           , color = extract('color="(\w+)"',1,ParseMe)
13           , packing = extract('packing="(\w+)"',1,ParseMe)
```

Results

Chart



Add bookmark



fruit

color

packing

ParseMe



>

Apples

Orange

Bottle

fruit="Apples", color="Orange", packing="Bottle"



>

Bananas

Red

Crate

fruit="Bananas", color="Red", packing="Crate"



>

Pears

Green

Box

fruit="Pears", color="Green", packing="Box"



>

Cherries

Yellow

Envelope

fruit="Cherries", color="Yellow", packing="Envelope"



>

Oranges

Blue

Tube

fruit="Oranges", color="Blue", packing="Tube"



```
1 // But extract is slow and regex is hard
2 let Table = datatable(ParseMe:string)
3 [
4   'fruit="Apples", color="Orange", packing="Bottle"',
5   'fruit="Bananas", color="Red", packing="Crate"',
6   'fruit="Pears", color="Green", packing="Box"',
7   'fruit="Cherries", color="Yellow", packing="Envelope"',
8   'fruit="Oranges", color="Blue", packing="Tube"'
9 ];
10 Table
11 | parse ParseMe with 'fruit="' fruit '"', color="'" color '"', packing="'" packing
```

Results

Chart

 Add bookmark

<input type="checkbox"/> ParseMe	fruit	color	packing
<input type="checkbox"/> > fruit="Apples", color="Orange", packing="Bottle"	Apples	Orange	Bottle"
<input type="checkbox"/> > fruit="Bananas", color="Red", packing="Crate"	Bananas	Red	Crate"
<input type="checkbox"/> > fruit="Pears", color="Green", packing="Box"	Pears	Green	Box"
<input type="checkbox"/> > fruit="Cherries", color="Yellow", packing="Envelope"	Cherries	Yellow	Envelope"
<input type="checkbox"/> > fruit="Oranges", color="Blue", packing="Tube"	Oranges	Blue	Tube"



```
1 // So parse needs to be in the same order
2 let Table = datatable(ParseMe:string)
3 [
4   'fruit="Apples", color="Orange", packing="Bottle",
5   'fruit="Bananas", color="Red", packing="Crate",
6   'fruit="Pears", color="Green", packing="Box",
7   'fruit="Cherries", color="Yellow", packing="Envelope",
8   'fruit="Oranges", color="Blue", packing="Tube"
9 ];
10 Table
11 | parse-ky ParseMe as (
12   fruit:string
13   , color:string
14   , packing:string
15 ) with (pair_delimiter=',', kv_delimiter='=', quote='')
16
```

Results

Chart



Add bookmark

<input type="checkbox"/> ParseMe	fruit	color	packing
<input type="checkbox"/> > fruit="Apples", color="Orange", packing="Bottle"	Apples	Orange	Bottle
<input type="checkbox"/> > fruit="Bananas", color="Red", packing="Crate"	Bananas	Red	Crate
<input type="checkbox"/> > fruit="Pears", color="Green", packing="Box"	Pears	Green	Box
<input type="checkbox"/> > fruit="Cherries", color="Yellow", packing="Envelope"	Cherries	Yellow	Envelope
<input type="checkbox"/> > fruit="Oranges", color="Blue", packing="Tube"	Oranges	Blue	Tube



Will it Run?

www.wpninjas.eu
#WPNinjaS

```
1 // Now what if we mixup the keys?
2 let Table = datatable(ParseMe:string)
3 [
4   'fruit="Apples", color="Orange", packing="Bottle"',
5   'fruit="Bananas", color="Red", packing="Crate"',
6   'fruit="Pears", color="Green", packing="Box"',
7   'fruit="Cherries", color="Yellow", packing="Envelope"',
8   'fruit="Oranges", color="Blue", packing="Tube"'
9 ];
10 Table
11 | parse-ky ParseMe as (
12     packing:string
13     , color:string
14     , fruit:string
15 ) with (pair_delimiter=',', kv_delimiter='=', quote='"')
```



Will it Run?

www.wpninjas.eu

#WPNinjaS

```
1 // Now what if we mixup the keys?
2 let Table = datatable(ParseMe:string)
3 [
4   'fruit="Apples", color="Orange", packing="Bottle",
5   'fruit="Bananas", color="Red", packing="Crate",
6   'fruit="Pears", color="Green", packing="Box",
7   'fruit="Cherries", color="Yellow", packing="Envelope",
8   'fruit="Oranges", color="Blue", packing="Tube"
9 ];
10 Table
11 | parse-kv ParseMe as (
12     packing:string
13     , color:string
14     , fruit:string
15 ) with (pair_delimiter=',', kv_delimiter='=', quote='')
```

Results

Chart



Add bookmark

<input type="checkbox"/> ParseMe		packing	color	fruit
<input type="checkbox"/> >	fruit="Apples", color="Orange", packing="Bottle"	Bottle	Orange	Apples
<input type="checkbox"/> >	fruit="Bananas", color="Red", packing="Crate"	Crate	Red	Bananas
<input type="checkbox"/> >	fruit="Pears", color="Green", packing="Box"	Box	Green	Pears
<input type="checkbox"/> >	fruit="Cherries", color="Yellow", packing="Envelope"	Envelope	Yellow	Cherries
<input type="checkbox"/> >	fruit="Oranges", color="Blue", packing="Tube"	Tube	Blue	Oranges

Bonus!





```
1 // Tabular Function
2 let TableParser = (Table:(ParseMe:string)) {
3     Table
4     | parse-kv ParseMe as (
5         fruit:string
6         , color:string
7         , packing:string
8     ) with (pair_delimiter=',', kv_delimiter='=', quote='')
9     | project-away ParseMe
10 };
11 // Table
12 let Table = datatable(ParseMe:string)
13 [
14 'fruit="Apples", color="Orange", packing="Bottle"',
15 'fruit="Bananas", color="Red", packing="Crate"',
16 'fruit="Pears", color="Green", packing="Box"',
17 'fruit="Cherries", color="Yellow", packing="Envelope"',
18 'fruit="Oranges", color="Blue", packing="Tube"'
19 ];
20 TableParser(Table)
```

Results

Chart

☆ Add bookmark

<input type="checkbox"/> fruit	color	packing
<input type="checkbox"/> > Apples	Orange	Bottle
<input type="checkbox"/> > Bananas	Red	Crate
<input type="checkbox"/> > Pears	Green	Box
<input type="checkbox"/> > Cherries	Yellow	Envelope
<input type="checkbox"/> > Oranges	Blue	Tube

KQL External Data





KQL External Data

www.wpninjas.eu

#WPNinjaS

The **externaldata** operator returns a table whose schema is defined in the query itself, and whose data is read from an external storage artifact, such as a blob in Azure Blob Storage or a file hosted in GitHub.

Use cases

- IOCs – Indicators of compromise
- IP Address Data
- Data enrichment

Syntax

```
externaldata ( ColumnName : ColumnType [, ...] )  
[ StorageConnectionString [, ...] ]  
[ with ( PropertyName = PropertyValue [, ...] ) ]
```

KQL External Data

www.wpninjas.eu
#WPNinjaS

Property	Type	Description
format	string	Data format. If not specified, an attempt is made to detect the data format from file extension (defaults to <code>csv</code>). Any of the ingestion data formats are supported.
ignoreFirstRecord	bool	If set to true, indicates that the first record in every file is ignored. This property is useful when querying CSV files with headers.
ingestionMapping	string	A string value that indicates how to map data from the source file to the actual columns in the operator result set. See data mappings .

Format	Extension	Description
CSV	<code>.csv</code>	A text file with comma-separated values (,). See RFC 4180: Common Format and MIME Type for Comma-Separated Values (CSV) Files .
JSON	<code>.json</code>	A text file with JSON objects delimited by <code>\n</code> or <code>\r\n</code> . See JSON Lines (JSONL) .
MultiJSON	<code>.multijson</code>	A text file with a JSON array of property bags (each representing a record), or any number of property bags delimited by whitespace, <code>\n</code> or <code>\r\n</code> . Each property bag can be spread on multiple lines. This format is preferred over <code>JSON</code> , unless the data is non-property bags.
TXT	<code>.txt</code>	A text file with lines delimited by <code>\n</code> . Empty lines are skipped.

More ingestion formats

<https://docs.microsoft.com/en-us/azure/data-explorer/ingestion-supported-formats>



KQL External Data

www.wpninjas.eu
#WPNinjaS

IOCs – Indicators of compromise

```
http://59.92.170.52:52121/bin.sh
http://117.207.225.131:46120/i
http://220.135.243.213:14620/.i
http://59.93.19.89:47197/bin.sh
http://121.237.15.24:4971/bin.sh
http://114.42.50.18:54455/i
```

New Query 1* x + Feedback Queries

Demo Run Time range : Last 24 hours Save Share + New alert rule Export

```
>> 1 // retrieve URLs only that are online from URLhaus
2 // https://urlhaus.abuse.ch/downloads/text_online/
3 let urlhaus_online = (externaldata(url_online: string ) [@"https://urlhaus.abuse.ch/downloads/text_online/"]
4 with (format="txt"))
5 | project url_online;
6 urlhaus_online
```

There's only one attribute, the URL



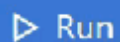
New Query 2*



Feedback



Demo



Run

Time range: Last 24 hours



Save



Share



New alert rule



Ex



```
1 // retrieve URLs only that are online from URLhaus
2 // https://urlhaus.abuse.ch/downloads/text_online/
3 let urlhaus_online = (externaldata(url_online: string ) [@"https://urlhaus.abuse.ch/downloads/text_online/"]
4 with (format="txt"))
5 | project url_online;
6 urlhaus_online
```

Schema and Filter



No queries history



KQL External Data

www.wpninjas.eu
#WPNinjaS

```
← → ↺ Added security | https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt

#Proactive Hunt C2 Threat Intelligence Feeds Generated on Threatview[.]io on 06-September-2022. Machine
https://threatview[.]io/Downloads/High-Confidence-CobaltstrikeC2_IP_feed.txt
#IP,Date of Detection,Host,Protocol,Beacon Config,Comment
139.60.161.47,06 September 2022 05:45 PM UTC,alojun.com,https,"alojun.com,/jquery-3.3.1.min.js",Genera
139.60.161.162,06 September 2022 05:45 PM UTC,asdder.com,https,"asdder.com,/jquery-3.3.1.min.js",Gener
213.227.154.100,06 September 2022 05:45 PM UTC,senebuvuyi.com,https,"senebuvuyi.com,/lu.css",Generated
137.184.139.189,06 September 2022 05:45 PM
UTC,shrekf.art,https,"d15oagcddncz2r.cloudfront.net,/safebrowsing/TzVkLdp/W7W6Kg8vt0mpodyuRjehPJihI",G
Hunter
```

```

▶ Run Time range : Last 24 hours Save Share + New alert rule Export Pin to Format query

1 // C2 Hunt Feed - Infrastructure hosting Command & Control Servers found during Proactive Hunt by Threatview.io
2 let C2Hunt = (externaldata(IPAddress:string,Date:string,Host:string,Protocol:string,BeaconConfig:string,
3   Comment:string ) [@"https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt"]
4   with (format="csv",ignoreFirstRecord=true))
5   | where IPAddress !startswith "#";
6   C2Hunt|
```

Here we have multiple attributes to declare

New Query 2*New Query 1*New Query 3*New Query 4*×

FeedbackQueries

Demo▶ RunTime range : Last 24 hoursSaveShare+ New alert ruleExportPin toFormat query

1 // C2 Hunt Feed - Infrastructure hosting Command & Control Servers found during Proactive Hunt by Threatview.io

2 let C2Hunt = (externaldata(IPAddress:string,Date:string,Host:string,Protocol:string,BeaconConfig:string,

3 Comment:string) [@"https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt"]

4 | where IPAddress !startswith "#";

5 C2Hunt

No queries history

To start, go to Queries on the side pane or type a query in the query

Search (Ctrl+/)

Upload

Change access level

Refresh

Delete

Change tier

Acquire lease

Break lease

View snapshots

Create snapshot

Overview

Diagnose and solve problems

Access Control (IAM)

Settings

Shared access tokens

Access policy

Properties

Metadata

Authentication method: Azure AD User Account (Switch to Access key)

Location: tidata

Search blobs by prefix (case-sensitive)

Show deleted blobs

Add filter

Name

ci-badguys.txt

We can also access data that is stored in Azure storage blobs

ci-badguys.txt

Blob

Save

Discard

Download

Refresh

Delete

Overview

Versions

Snapshots

Edit

Generate SAS

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage blob. Use it when you want to grant access to storage account resources

Learn more about creating an account SAS

Signing method

☒ Account key
 ☐ User delegation key

Start and expiry date/time

Start

09/06/2022 8:20:51 PM

Allowed protocols

☒ HTTPS only
 ☐ HTTPS and HTTP

Generate SAS token and URL

Blob SAS token

sp=r&st=2022-09-06T18:20:51Z&se=2022-09-07T02:20:51Z&spr=https&sv=2021-06-08&sr=b&sig=a0jTurtjW4dU2RikgzMBbeL8l82gl9U9WSwO%2FoKqFuM%3

Blob SAS URL

https://tfiles.blob.core.windows.net/tidata/ci-badguys.txt?sp=r&st=2022-09-06T18:20:51Z&se=2022-09-07T02:20:51Z&spr=https&sv=2021-06-08&sr=b&sig=a



New Query 2*



New Query 1*



New Query 3*



New Query 4*



New Query 5*



Feedback



Queries



Demo



Run

Time range: Last 24 hours



Save



Share



New alert rule



Export



Pin to



Format q



```
1 let cinsarmylist = (externaldata(ip:string)
2 [h@"https://tfiles.blob.core.windows.net/tidata/ci-badguys.txt?sp=r&st=2022-03-20T15:44:46Z&
se=2023-08-04T22:44:46Z&spr=https&sv=2020-08-04&sr=b&sig=xGTnzyeXGC0mn32pihGuIF%2FiVyHLBoVRi3aZg9u5FXg%3D"]
3 with (format="txt",IgnoreFirstRecord=true));
4 cinsarmylist
```

Schema and Filter



No queries history

To start, go to Queries on the side

KQL Joining Data



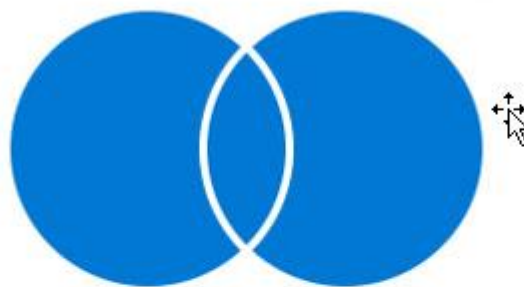


KQL Joining Data

LEFT JOIN



FULL OUTER JOIN



**LEFT JOIN
(if NULL)**



INNER JOIN



RIGHT JOIN



**RIGHT JOIN
(if NULL)**





KQL Joining Data

www.wpninjas.eu
#WPNinjaS

Join Flavor	Output Records
kind=leftanti, kind=leftantisemi	Returns all the records from the left side that don't have matches from the right
kind=rightanti, kind=rightantisemi	Returns all the records from the right side that don't have matches from the left.
kind unspecified, kind=innerunique	Only one row from the left side is matched for each value of the on key. The output contains a row for each match of this row with rows from the right
kind=leftsemi	Returns all the records from the left side that have matches from the right.
kind=rightsemi	Returns all the records from the right side that have matches from the left.
kind=inner	Contains a row in the output for every combination of matching rows from left and right.
kind=leftouter (or kind=rightouter or kind=fullouter)	Contains a row for every row on the left and right, even if it has no match. The unmatched output cells contain nulls.



KQL Joining Data

www.wpninjas.eu
#WPNinjaS

KQL Scan Operator





C:\ Administrator: C:\Windows\system32\cmd.exe

```
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: create full C:\export
Creating snapshot...
Snapshot set {cebd4bdb-6e6d-4346-84ce-0162b1e7f51c} generated successfully.
Snapshot {0cdff09a-9a95-40e3-877f-807a45eb112e} mounted as C:\$SNAP_202209131724_VOLUMEC$\
Snapshot {0cdff09a-9a95-40e3-877f-807a45eb112e} is already mounted.
Initiating DEFRAGMENTATION mode...
    Source Database: C:\$SNAP_202209131724_VOLUMEC$\Windows\NTDS\ntds.dit
    Target Database: C:\export\Active Directory\ntds.dit

          Defragmentation  Status ( omplete)

      0    10    20    30    40    50    60    70    80    90   100
      |----|----|----|----|----|----|----|----|----|----|
      .....

Copying registry files...
Copying C:\export\registry\SYSTEM
Copying C:\export\registry\SECURITY
Snapshot {0cdff09a-9a95-40e3-877f-807a45eb112e} unmounted.
IFM media created successfully in C:\export
ifm: quit
ntdsutil: quit

C:\Users\Administrator>
```



Advanced Hunting

New query | X Test | X N



Run query

Save

Query

1 search "ntdsutil"

Getting Started

Results



1 of 5



\$table



DeviceProcessEvents



DeviceNetworkEvents



DeviceNetworkEvents



DeviceImageLoadEvents

Inspect record

Assets

Devices (1)

Risk Score

dc01

None

Users (1)

administrator

Process tree

Expand all



[8220] cmd.exe



[9120] ntdsutil.exe ntdsutil

loaded module



samlib.dll

All details

\$table

DeviceImageLoadEvents

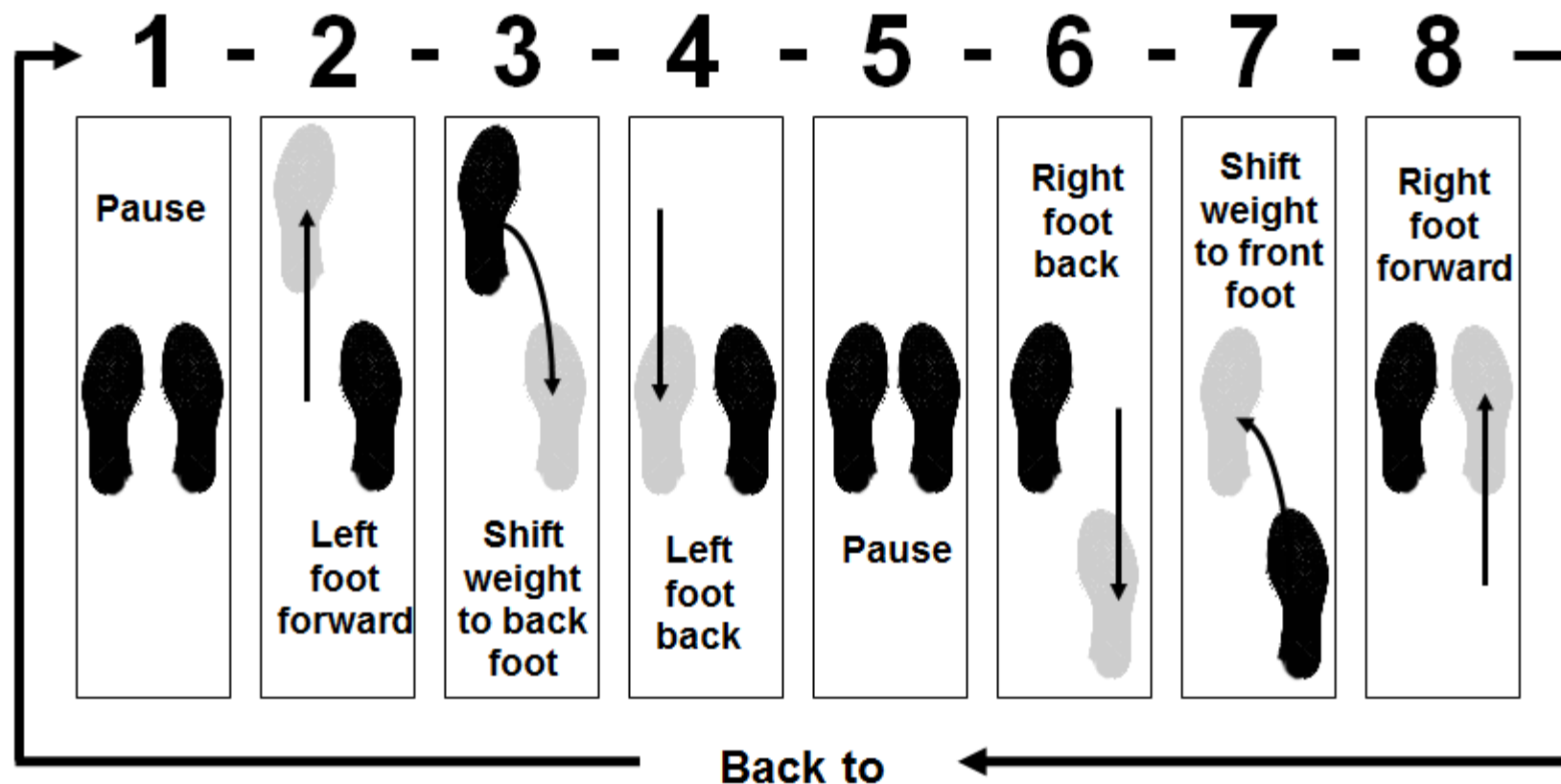
www.wpninjas.eu
#WPNinjaS



KQL Scan Operator

www.wpninjas.eu
#WPNinjaS

Basic Salsa Steps





Query

```
1 DeviceImageLoadEvents
2 | where InitiatingProcessFileName =~ "ntdsutil.exe"
3
4
5
6
7
8
9
```

Getting Started

Results

↓ Export

3 items

🔍 Search

🕒 0:0.47

■ ■ ■ Low ⓘ

📈 Change

<input type="checkbox"/>	Timestamp ↓	DeviceId	DeviceName	ActionType	FileName
<input type="checkbox"/>	Sep 13, 2022 5:23:58 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ImageLoaded	ntdsutil.exe
<input type="checkbox"/>	Sep 13, 2022 5:22:26 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ImageLoaded	vss_ps.dll
<input type="checkbox"/>	Sep 13, 2022 5:22:05 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ImageLoaded	samlib.dll



Step 1

Query

```
1 DeviceImageLoadEvents
2 | where InitiatingProcessFileName =~ "ntdsutil.exe"
3 | sort by Timestamp asc
4 | scan with_match_id=funnel_id declare(Step:string, Delta:timespan) with
5 | (
6 |     step Authentication: InitiatingProcessFileName =~ "ntdsutil.exe"
7 |     and FileName =~ "samlib.dll"
8 |     => Step = "Authenticated";
9 | )
```

Getting Started

Results

[↓](#) Export

1 item

🕒 0:1.422

■ ■ ■ Low ⓘ

<input type="checkbox"/>	Timestamp	DeviceId	DeviceName	ActionType	FileName
<input type="checkbox"/>	Sep 13, 2022 5:22:05 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ImageLoaded	samlib.dll



Step 2

```
6 step Authentication: InitiatingProcessFileName =~ "ntdsutil.exe"
7   and FileName =~ "samlib.dll"
8   => Step = "Authenticated";
9 step NTDSExport: InitiatingProcessFileName =~ "ntdsutil.exe"
10  and FileName =~ "vss_ps.dll"
11  and Authentication.Timestamp > 10m
12  => Step = "NTDS export"
13  , Delta = Timestamp - Authentication.Timestamp;
```

Getting Started Results

[Export](#)

2 items

🕒 0:3.125 Low ⓘ

[Chart Type](#) [Customize](#)

<input type="checkbox"/>	Timestamp	DeviceId	DeviceName	funnel_id	FileName	Step
<input type="checkbox"/>	Sep 13, 2022 5:22:05 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	0	samlib.dll	Authenticated
<input type="checkbox"/>	Sep 13, 2022 5:22:26 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	0	vss_ps.dll	NTDS export



Final

www.wpninjas.eu
#WPNinjaS

```
1 DeviceImageLoadEvents
2 | where InitiatingProcessFileName =~ "ntdsutil.exe"
3 | sort by Timestamp asc
4 | scan with_match_id=funnel_id declare(Step:string, Delta:timespan) with
5 (
6     step Authentication: InitiatingProcessFileName =~ "ntdsutil.exe"
7     and FileName =~ "samlib.dll"
8     => Step = "Authenticated";
9     step NTDSExport: InitiatingProcessFileName =~ "ntdsutil.exe"
10    and FileName =~ "vss_ps.dll"
11    and Authentication.Timestamp > 10m
12    => Step = "NTDS export"
13    , Delta = Timestamp - Authentication.Timestamp;
14 )
15 | where Step == "NTDS export"
```

Getting Started

Results

↓ Export

1 item

🔍 Search

🕒 0:3.735

📊 Low ^①

📈 Chart Ty



Timestamp

DeviceId

DeviceName

ActionType

FileName



Sep 13, 2022 5:22:26 PM

📁 bb6e4c052ee6f2c...



📁 dc01.kustoworks.c...



ImageLoaded

vss_ps.dll

KQL Detections

Detection - the fact of noticing or discovering something



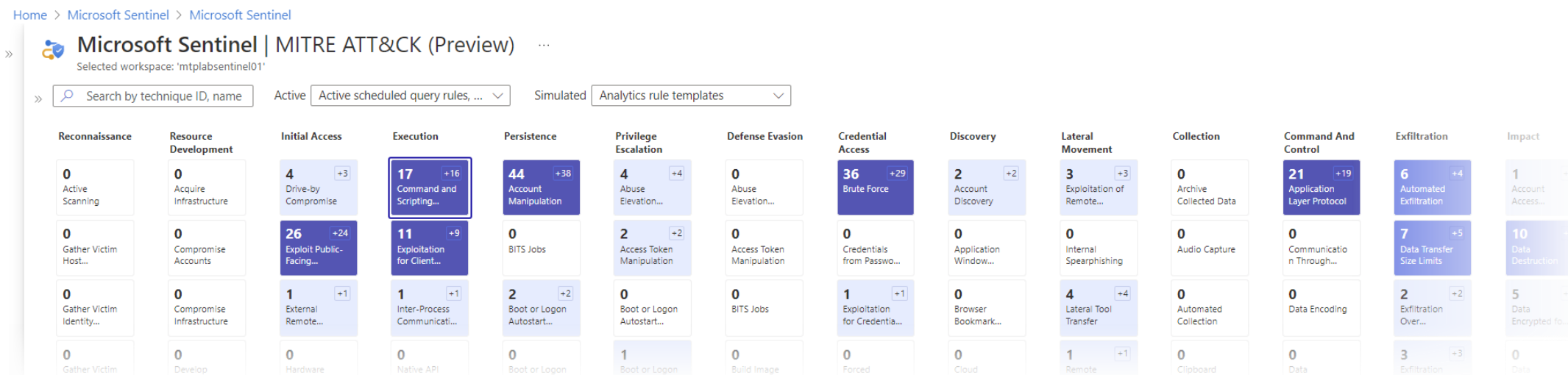


KQL Detections

www.wpninjas.eu
#WPNinjaS

Detection the fact of noticing or discovering something

The term **Detections** and KQL is often related to **Security** but not limited to. When creating detections in KQL we want to identify a specific user, device, object, activity or a sequence of events.





Use of Remote Desktop Protocol (RDP)

Scenario

We want to detect when an RDP session is established on a device that originates from a public IP Address



Detections

www.wpninjas.eu
#WPNinjaS

Commonly used Ports

Scenario

We want to detect when specific ports are used



Creation of local User Accounts / Modification of Local Administrator Group Membership

Scenario

We want to detect when a local user account is created on a device and/or when the Local Administrators group membership is changed.

KQL Hunting

the process of proactively and iteratively searching through logs to detect and isolate advanced threats that evade existing security solutions





Begin

www.wpninjas.eu
#WPNinjaS





Result

www.wpninjas.eu
#WPNinjaS





```
1 let SuspiciousFiles = dynamic(["dir.exe"  
2 , "ipconfig.exe"  
3 , "systeminfo.exe"  
4 , "ping.exe"  
5 , "type.exe"  
6 , "net.exe"  
7 , "dsquery.exe"  
8 , "csvde.exe"  
9 , "nbtstat.exe"  
10 , "nltest.exe"  
11 , "ntdsutil.exe"  
12 , "adfind.exe"  
13 , "nslookup.exe"  
14 , "procdump.exe"  
15 , "whoami.exe"  
16 , "wmic.exe"  
17 , "mimikatz.exe"  
18 , "tasklist.exe"  
19 , "rubeus.exe"  
20 ]);
```




Hunt 1

www.wpninjas.eu
#WPNinjaS

```
1 let SuspiciousFiles = dynamic(["dir.exe", "ipconfig.exe", "systeminfo.exe", "ping.exe", "type.exe", "net.exe"  
2   , "dsquery.exe", "csvde.exe", "nbtstat.exe", "nltest.exe", "ntdsutil.exe", "adfind.exe", "nslookup.exe"  
3   , "procdump.exe", "whoami.exe", "wmic.exe", "mimikatz.exe", "tasklist.exe", "rubeus.exe"]);  
4 DeviceProcessEvents  
5 | where FileName has_any(SuspiciousFiles)  
6  
7
```

Getting Started Results

Export	1006 items	<input type="text" value="Search"/>	0:0.156	Low	Chart Type	Custo
<input type="checkbox"/> Timestamp	DeviceId	DeviceName	ActionType	FileName	FolderPath	
<input type="checkbox"/> Sep 13, 2022 5:41:13 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ProcessCreated	ipconfig.exe	C:\Windows	
<input type="checkbox"/> Sep 13, 2022 5:22:57 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ProcessCreated	ntdsutil.exe	C:\Windows	



Hunt 1

www.wpninjas.eu
#WPNinjaS

```
8 | scan with_match_id=funnel_id declare(Step:int, Delta:timespan, Duration:timespan, Files:dynamic, CommandLines:dynamic) with
9 | (
10 |     step s1: FileName in(SuspiciousFiles)
11 |     => Step = 1, Delta = timespan(0)
12 |     , Duration = timespan(0)
13 |     , Files = pack_array(FileName)
14 |     , CommandLines = pack_array(ProcessCommandLine);
15 | )
16 | summarize arg_max(Timestamp, ReportId, *) by funnel_id, DeviceId, Step
```

Getting Started Results

↓ Export

4 items

Search

⌚ 0:0.172 ■ ■ ■ Low ^①

📊 Chart Type ▾

⚙️ Customize columns

<input type="checkbox"/> funnel_id	DeviceId ↑	Step	Timestamp	ReportId	FileName	Pro
<input type="checkbox"/> 0	📁 3246791d68c8e57... ↗	1	Sep 11, 2022 11:02:15 AM	43815	net.exe	"n
<input type="checkbox"/> 0	📁 91ec3a4f51a545dc... ↗	1	Sep 12, 2022 7:36:31 AM	22680	tasklist.exe	ta:
<input type="checkbox"/> 0	📁 b8706ac239a7350... ↗	1	Aug 17, 2022 7:53:51 PM	554	ipconfig.exe	ip:
<input type="checkbox"/> 0	📁 bb6e4c052ee6f2c... ↗	1	Sep 13, 2022 5:41:13 PM	9738	ipconfig.exe	"ip



Hunt 1

```
15 , Files = pack_array(FileName)
16 , CommandLines = pack_array(ProcessCommandLine);
17 step s2: FileName in(SuspiciousFiles)
18 and Timestamp - s1.Timestamp <= TimePeriod
19 and DeviceId == s1.DeviceId
20 and ProcessCommandLine != s1.ProcessCommandLine => Step = 2
21 , Delta = Timestamp - s1.Timestamp
22 , Duration = Timestamp - s1.Timestamp
23 , Files = pack_array(s1.FileName, FileName)
24 , CommandLines = pack_array(s1.ProcessCommandLine, ProcessCommandLine);
25 step s3: FileName in(SuspiciousFiles) and Timestamp - s2.Timestamp <= TimePeriod and DeviceId == s2.DeviceId and ProcessComm
26 step s4: FileName in(SuspiciousFiles) and Timestamp - s3.Timestamp <= TimePeriod and DeviceId == s3.DeviceId and ProcessComm
27 step s5: FileName in(SuspiciousFiles) and Timestamp - s4.Timestamp <= TimePeriod and DeviceId == s4.DeviceId and ProcessComm
```

Getting Started

Results

↓ Export

59 items

🔍 Search

🕒 0:2.828

🟡 Low ⓘ

📊 Chart Type ▾

🛠️ Customize columns

<input type="checkbox"/> funnel_id	DeviceId	Step	Timestamp	ReportId	FileName	Pr
<input type="checkbox"/> 0	📁 3246791d68c8e57... ➡	1	Sep 11, 2022 11:02:15 AM	43815	net.exe	"r
<input type="checkbox"/> 0	📁 91ec3a4f51a545dc... ➡	1	Aug 30, 2022 7:39:47 PM	15952	systeminfo.exe	sy
<input type="checkbox"/> 0	📁 91ec3a4f51a545dc... ➡	2	Aug 30, 2022 7:39:57 PM	15958	ipconfig.exe	ip



Hunt 1

```
40 | summarize arg_max(Timestamp, ReportId, *) by funnel_id, DeviceId, Step
41 | where Step >= Threshold
```

Getting Started Results

↓ Export

23 items

🕒 0:2.422

■ ■ ■ Low ⓘ

Chart Type ▾

Customize columns

<input type="checkbox"/>	funnel_id	DeviceId	Step	Timestamp	ReportId	FileName	Pr
<input type="checkbox"/>	0	91ec3a4f51a545dc...	3	Aug 30, 2022 7:40:04 PM	15963	nltest.exe	nl
<input type="checkbox"/>	0	91ec3a4f51a545dc...	4	Aug 30, 2022 7:40:08 PM	15967	ipconfig.exe	ip
<input type="checkbox"/>	1	91ec3a4f51a545dc...	3	Aug 30, 2022 7:40:08 PM	15967	ipconfig.exe	ip
<input type="checkbox"/>	1	91ec3a4f51a545dc...	4	Aug 30, 2022 7:42:06 PM	16027	systeminfo.exe	sy
<input type="checkbox"/>	2	91ec3a4f51a545dc...	3	Aug 30, 2022 7:42:06 PM	16027	systeminfo.exe	sy
<input type="checkbox"/>	1	91ec3a4f51a545dc...	5	Aug 30, 2022 7:42:19 PM	16035	nltest.exe	nl
<input type="checkbox"/>	2	91ec3a4f51a545dc...	4	Aug 30, 2022 7:42:19 PM	16035	nltest.exe	nl
<input type="checkbox"/>



Hunt 2

www.wpninjas.eu
#WPNinjaS

```
1 DeviceProcessEvents
2 | extend EncodedString = extract(@" -[eE][^xXrR]\S* ([a-zA-Z0-9]*={0,2})", 1, ProcessCommandLine)
3 | where isnotempty(EncodedString)
```

Getting Started Results

↓ Export

9 items



<input type="checkbox"/>	Timestamp	DeviceId	DeviceName	ActionType	FileName
<input type="checkbox"/>	Sep 13, 2022 5:28:58 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ProcessCreated	powershell.exe
<input type="checkbox"/>	Sep 13, 2022 5:29:32 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ProcessCreated	powershell.exe
<input type="checkbox"/>	Sep 13, 2022 6:26:05 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ProcessCreated	powershell.exe
<input type="checkbox"/>	Sep 13, 2022 6:26:14 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ProcessCreated	powershell.exe
<input type="checkbox"/>	Sep 13, 2022 5:18:48 PM	bb6e4c052ee6f2c...	dc01.kustoworks.c...	ProcessCreated	sqlservr.exe
<input type="checkbox"/>	Sep 7, 2022 2:03:48 PM	91ec3a4f51a545dc...	novogons	ProcessCreated	cmd.exe



Hunt 2

EncodedString ↑

IAANAAoAIAAgACAAIAAgACAAIAAgACQAUgBhAG4AZABvAG0ARgBvAGwAZABIAHIATgBhAG0AZQAgAD0AIAAtAGoAbwBpAG4AIAAoACgANgA1AC4ALgA5ADA AKQAgA

IAANAAoAIAAgACAAIAAgACAAIAAgACQAUgBhAG4AZABvAG0ARgBvAGwAZABIAHIATgBhAG0AZQAgAD0AIAAtAGoAbwBpAG4AIAAoACgANgA1AC4ALgA5ADA AKQAgA

IAANAAoAIAAgACAAIAAgACAAIAAgACQAUgBhAG4AZABvAG0ARgBvAGwAZABIAHIATgBhAG0AZQAgAD0AIAAtAGoAbwBpAG4AIAAoACgANgA1AC4ALgA5ADA AKQAgA

IAANAAoAIAAgACAAIAAgACAAIAAgACQAUgBhAG4AZABvAG0ARgBvAGwAZABIAHIATgBhAG0AZQAgAD0AIAAtAGoAbwBpAG4AIAAoACgANgA1AC4ALgA5ADA AKQAgA

IABbAEUAbgB2AGkAcgBvAG4AbQBIAg4AdABdADoAOgBPAFMAVgBIAHIAcwBpAG8AbgAuAFYAZQByAHMAaQBvAG4AIAA=

IABbAEUAbgB2AGkAcgBvAG4AbQBIAg4AdABdADoAOgBPAFMAVgBIAHIAcwBpAG8AbgAuAFYAZQByAHMAaQBvAG4AIAA=

IABbAEUAbgB2AGkAcgBvAG4AbQBIAg4AdABdADoAOgBPAFMAVgBIAHIAcwBpAG8AbgAuAFYAZQByAHMAaQBvAG4AIAA=

IABbAEUAbgB2AGkAcgBvAG4AbQBIAg4AdABdADoAOgBPAFMAVgBIAHIAcwBpAG8AbgAuAFYAZQByAHMAaQBvAG4AIAA=

SQL



Hunt 2

www.wpninjas.eu

#WPNinjaS

```
1 DeviceProcessEvents
2 | extend EncodedString = extract(@" -[eE][^xXrR]\S* ([a-zA-Z0-9]*={0,2})", 1, ProcessCommandLine)
3 | where isnotempty(EncodedString)
4 | where strlen(EncodedString) >= 4
5 | extend DecodedString = base64_decode_tostring(EncodedString)
6 | where isnotempty(DecodedString)
7 | extend DecodedString = replace_string(DecodedString, "\x00", "")
8 | project-reorder Timestamp, DecodedString
```



Hunt 2

<input type="checkbox"/>	Timestamp	DecodedString
<input type="checkbox"/>	Sep 13, 2022 5:28:58 PM	[Environment]::OSVersion.Version
<input type="checkbox"/>	Sep 13, 2022 5:29:32 PM	[Environment]::OSVersion.Version
<input type="checkbox"/>	Sep 13, 2022 6:26:05 PM	[Environment]::OSVersion.Version
<input type="checkbox"/>	Sep 13, 2022 6:26:14 PM	[Environment]::OSVersion.Version
<input type="checkbox"/>	Sep 7, 2022 2:03:48 PM	\$RandomFolderName = -join ((65..90) + (97..122) Get-Random -Count 8 % {[char]\$_});
<input type="checkbox"/>	Sep 7, 2022 2:03:48 PM	\$RandomFolderName = -join ((65..90) + (97..122) Get-Random -Count 8 % {[char]\$_});
<input type="checkbox"/>	Sep 7, 2022 2:04:05 PM	\$RandomFolderName = -join ((65..90) + (97..122) Get-Random -Count 8 % {[char]\$_}); \$RandomFileName = [System.IO.Path]::GetRandomFileNam...
<input type="checkbox"/>	Sep 7, 2022 2:04:05 PM	\$RandomFolderName = -join ((65..90) + (97..122) Get-Random -Count 8 % {[char]\$_}); \$RandomFileName = [System.IO.Path]::GetRandomFileNam...

More KQL





Learning KQL

www.wpninjas.eu
#WPNinjaS

- Must Learn KQL
- KQL Café
- Microsoft Learn
- GitHub
 - [reprise99/Sentinel-Queries: Collection of KQL queries \(github.com\)](https://github.com/reprise99/Sentinel-Queries)
 - [ugurkocde/KQL Intune \(github.com\)](https://github.com/ugurkocde/KQL_Intune)
 - There's many more <https://github.com/topics/kql>



<https://aka.ms/MustLearnKQL>



<https://kqlcafe.com/>



More KQL

www.wpninjas.eu
#WPNinjaS

KQL quick reference

<https://docs.microsoft.com/en-us/azure/data-explorer/kql-quick-reference>

KQL Demo Environment

https://portal.azure.com/#view/Microsoft_Azure_Monitoring_Logs/DemoLogsBlade

Microsoft Intune and Azure Log Analytics

<https://techcommunity.microsoft.com/t5/device-management-in-microsoft/microsoft-intune-and-azure-log-analytics/ba-p/463145>

Using external data sources to enrich network logs using Azure storage and KQL

<https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/using-external-data-sources-to-enrich-network-logs-using-azure/ba-p/1450345>