



17 min read

Microsoft Sentinel

Mapping MDE and Windows Security Events overlap



Robbe Van den Daele

Mar 25, 2023 • 17 min read

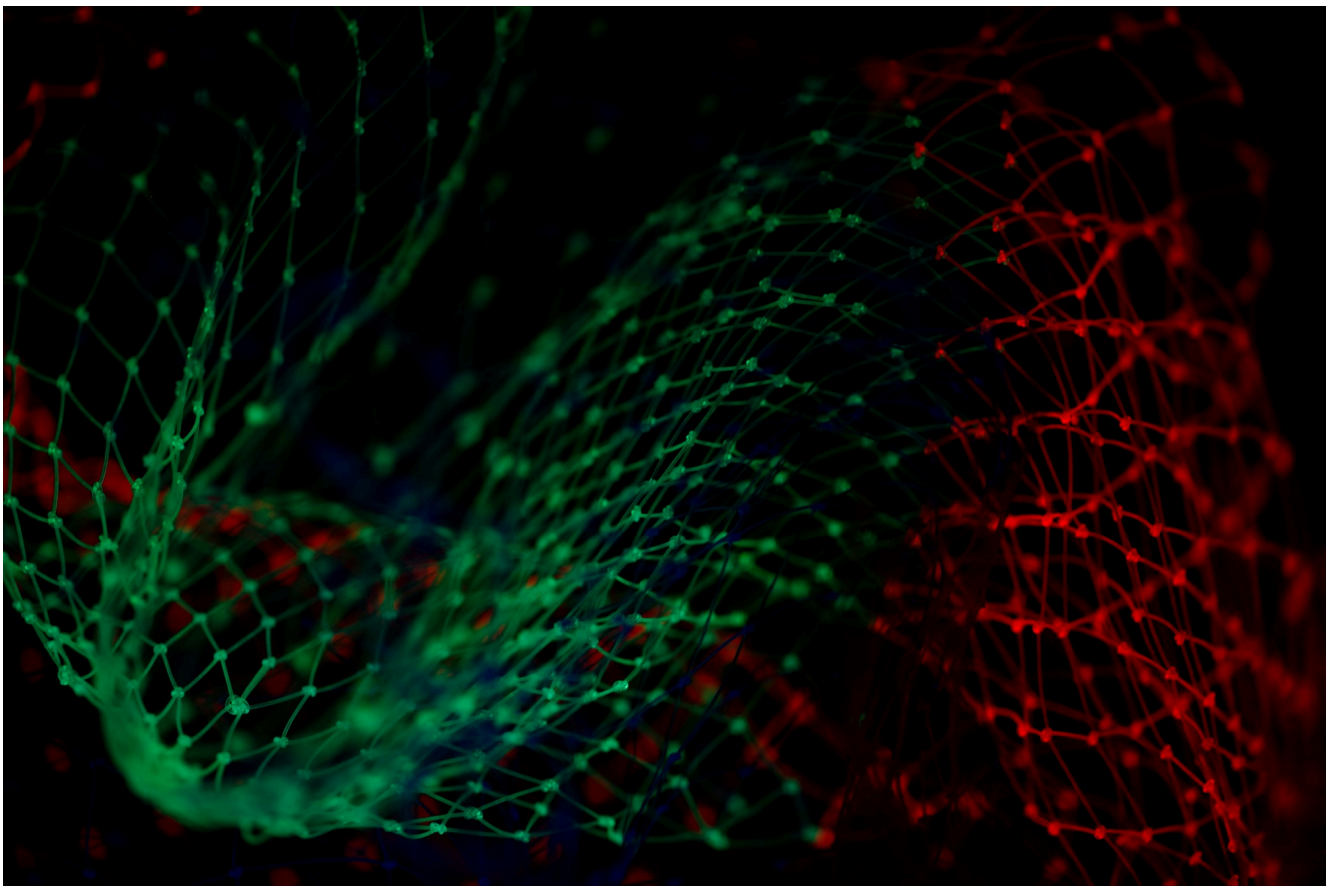


Photo by [Pietro Jeng](#) / [Unsplash](#)

Introduction

Plotting MITRE ATT&CK layers for data sources

The OSSEM data model

The yaml models

Subscribe

Importing the data

Visualizing the data

Creating MITRE layers

Comparing MITRE ATT&CK layers

MDE VS Windows Security Events

MDE VS Common Windows Security Events

Comparing and prioritizing layers

Finding MDE tables and Windows Event IDs based on MITRE layers

MDE

Windows Security Events

Conclusion, findings, and next steps

Lessons learned

What we didn't learn

Next related projects

Introduction

In my last blog post, I talked about using MITRE ATT&CK to support Microsoft Sentinel use cases. Today, I will be showing you how we can compare data coverage of data sources in Sentinel with MITRE ATT&CK and OSSEM. In this post you will find guidance about how to plot the MITRE ATT&CK data coverage of Windows Security Events and Microsoft Defender for Endpoint, so we can see the overlap between the two and hopefully can choose which data source to use.

Plotting MITRE ATT&CK layers for data sources

The reason I started this project was because I wondered what overlap there is between Microsoft Security Events data and Microsoft Defender for Endpoint data. When a customer has all endpoints and servers

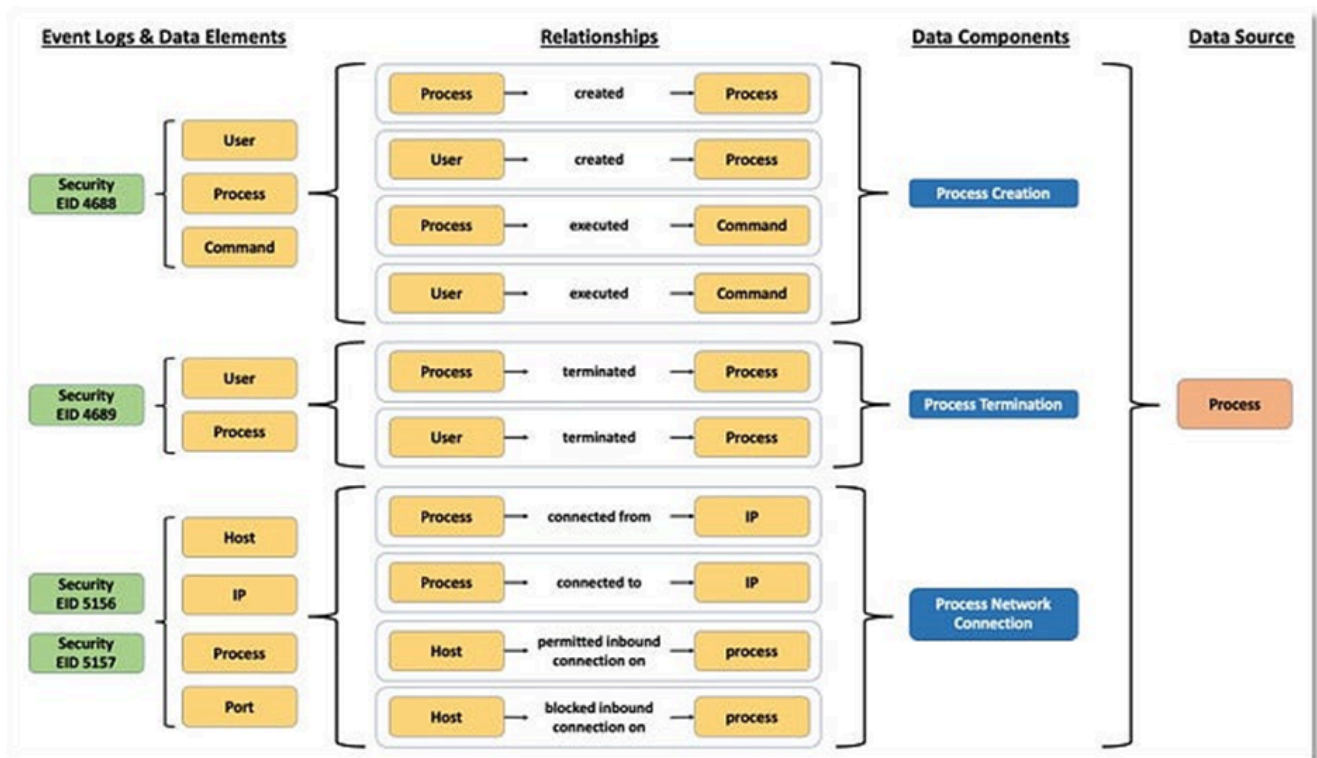
deployed in Microsoft Defender for Endpoint, is it still necessary to ingest certain Windows Security Logs in Microsoft Sentinel?

The OSSEM data model

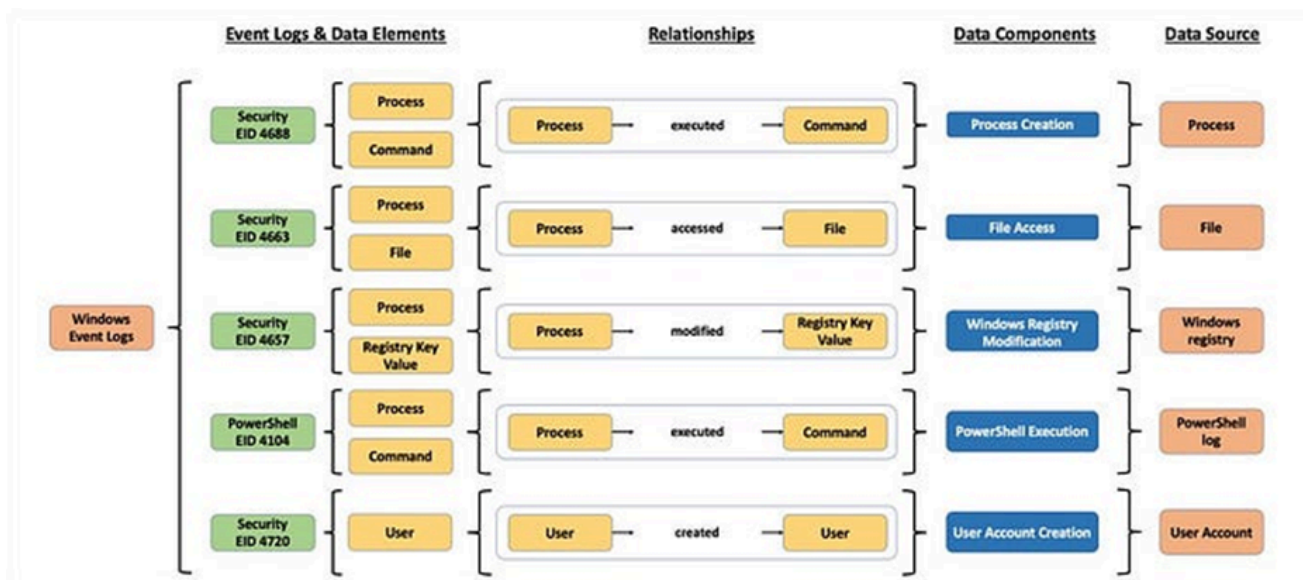
My first question was, how am I going to know which data there is available in both Windows Security Events and MDE events? After some googling, I found the awesome [OSSEM project](#) that is focusing on documenting and standardizing security event logs from diverse data sources.

In this project, you have the Detection Data Model that focuses on defining the required data in form of objects and relationships among each other, which is needed to facilitate the creation of data analytics and validate the detection of advisory techniques. On [this GitHub page](#), you can find the `techniques_to_events_mapping` that contains event types from various data sources, the relationships between them, and to which MITRE Techniques to map. And guess what, Windows Security Events and MDE events are included in the mapped data sources!

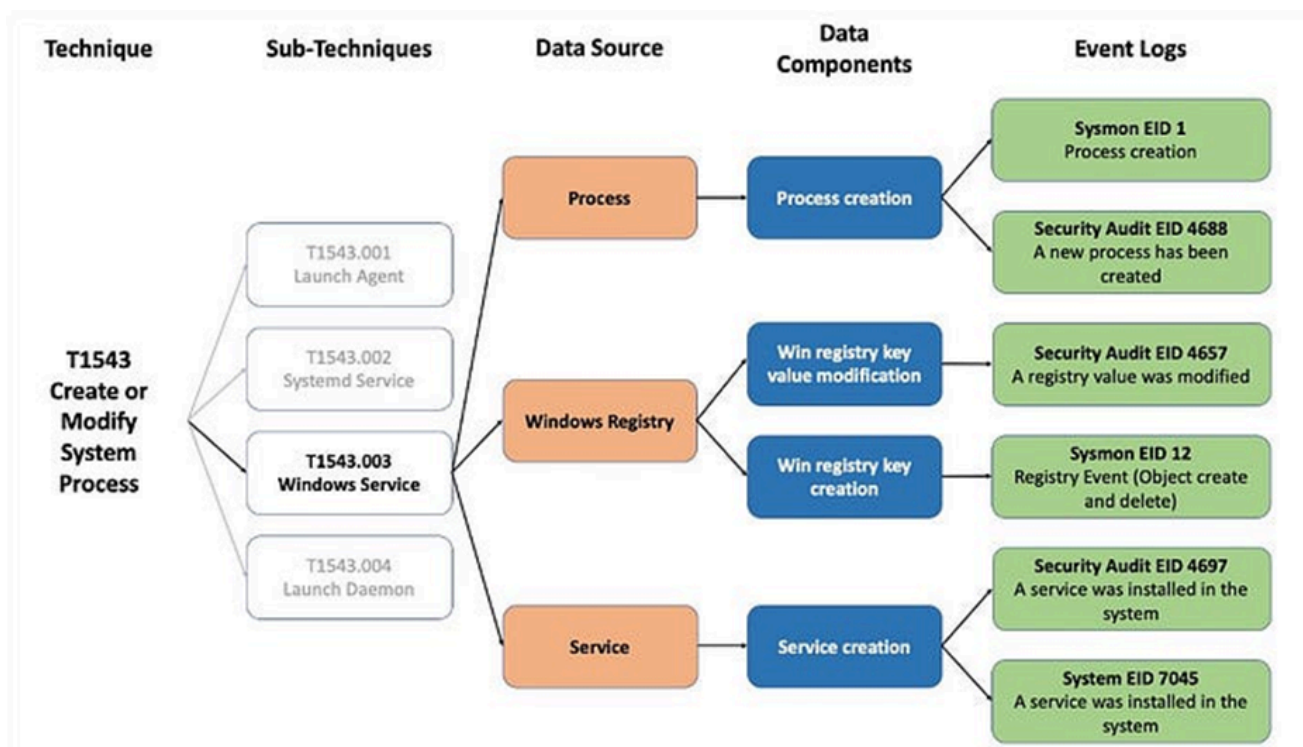
I will not go into detail about how the OSSEM model is set up and how it works, but I will cover some basics. If we use Windows Event Logs as an example, you get the following schema:



We start with the different event logs on the left side. Every event log has one or more data elements to which it relates (Processes, Commands, Files, etc.). Every data element then may have multiple relationships with each other (process created process, user created process, etc). Based on these relationships, a data component is decided (process created, process termination, etc). And finally, the data source is mapped (process, user, network, etc). Another schema of different data sources can be found below:



The data model then aligns the methodology with MITRE ATT&CK, so different sub-techniques can be mapped to the corresponding data components.



If you want to know more about the OSSEM model, make sure to check the following references:

- <https://medium.com/mitre-attack/defining-attack-data-sources-part-i-4c39e581454f>
- <https://medium.com/mitre-attack/defining-attack-data-sources-part-ii-1fc98738ba5b>
- <https://github.com/OTRF/OSSEM>
- <https://ossemproject.com/intro.html>

The yaml models

The first model I want to show is the [attack_relationships model](#) where you can find all of the events of different data sources and their relations with each other:

```

- relationship_id: REL-2022-0002
  name: User created User
  contributors:
  - Jose Rodriguez @Cyb3rPandaH
  - Roberto Rodriguez @Cyb3rWard0g
  - Olaf Hartong @olafhartong
  - Ruben Bouman @rubinatorz
  attack:
    data_source: user account
    data_component: user account creation
  behavior:
    source: user
    relationship: created
    target: user
  security_events:
  - event_id: '4720'
    name: A user account was created.
    platform: windows
    audit_category: Account Management
    audit_sub_category: User Account Management
    channel: Security
    log_source: Microsoft-Windows-Security-Auditing
    event_version:
    - '0'
  - event_id: '4741'
    name: A computer account was created.
    platform: windows
    audit_category: Account Management
    audit_sub_category: Computer Account Management
    channel: Security
    log_source: Microsoft-Windows-Security-Auditing
    event_version:
    - '0'
  - event_id: DeviceEvents
    name: DeviceEvents
    platform: windows
    log_source: Microsoft Defender for Endpoint
    filter_in:
    - ActionType: UserAccountCreated
    event_version:
    - '0'
    - '1'
  references:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4741
  notes: null

```

The second model is the model we will be using. This model is the [techniques_to_events_mapping model](#) which contains a mapping of every eventid over the different data sources to the related MITRE ATT&CK technique or sub-technique:

```
- technique_id: T1622
  is_subtechnique: false
  technique: Debugger Evasion
  tactic:
  - defense-evasion
  - discovery
  platform:
  - Windows
  - Linux
  - macOS
  data_source: process
  data_component: process creation
  relationship_id: REL-2022-0146
  name: User created Process
  source: user
  relationship: created
  target: process
  event_id: DeviceProcessEvents
  event_name: DeviceProcessEvents
  event_platform: windows
  audit_category: .nan
  audit_sub_category: .nan
  channel: .nan
  log_source: Microsoft Defender for Endpoint
  filter_in:
  - ActionType: ProcessCreated
```

In the screenshot above you see a mapping of DeviceProcessEvents of Defender for Endpoint to technique T1622. Know that the file contains an enormous number of related objects where the same and other events are mapped to one or multiple techniques and sub-techniques.

Importing the data

On [this page of the OSSEM website](#), you will find some examples of how to import the techniques to events mapping and how you can manipulate them. They are leveraging python to get the data and create insights about the mappings. In all of the examples below you will find my code that is based on the examples of the OSSEM website.

First, we have to import some libraries. These are used to get the data and transform the data into a model that is easy to manipulate and visualize.

```
# Importing library to manipulate data
import pandas as pd
# Importing library to manipulate yaml data
import yaml
# Importing library to create requests
import requests
# Import library to manipulate json data
import json
# Import library to copy objects
import copy
# Importing library for visualizations
from openhunt import visualizations as vis
```

Now that the libraries are imported, we can get the data and create the mapping to manipulate:

```
# Get OSSEM-DM techniques mapping file
yamlUrl = 'https://raw.githubusercontent.com/OTRF/OSSEM-DM/main/use-cases/mitre_atta
# Parse the data
yamlContent = requests.get(yamlUrl)
yamlMapping = yaml.safe_load(yamlContent.text)
# Map the data
mapping = pd.json_normalize(yamlMapping)
```

As you can see, we normalized the data model with the pandas library and saved the normalized mapping to the mapping variable. This variable will be used to create our visualizations and manipulations.

Visualizing the data

There are a couple of visualizations you can create to help troubleshoot and understand the data set more. The first one is the table representation of the data set. This really helps you to understand how the data set works, which properties there are per object, and more. You can filter on a value in a certain column, or you can combine multiple column filters. Below you find an example of a filter on one column:

```
mapping[(mapping['event_id']=='4724')]
```

	technique_id	is_subtechnique	technique	tactic	platform	data_source	data_component	relationship_id	name	source	relationship	target	event_id	event_name	event_platform	audit_c	
	100	T1098.005	True	Device Registration	[persistence]	[Azure AD, Windows, SaaS]	user account	user account modification	REL-2022-0133	User attempted to modify User	user	attempted to modify	user	4724	An attempt was made to reset an account's pass...	windows	Man
	6414	T1098.002	True	Additional Email Delegate Permissions	[persistence]	[Windows, Office 365, Google Workspace]	user account	user account modification	REL-2022-0133	User attempted to modify User	user	attempted to modify	user	4724	An attempt was made to reset an account's pass...	windows	Man
	7068	T1531	False	Account Access Removal	[impact]	[Linux, macOS, Windows, Office 365, SaaS]	user account	user account modification	REL-2022-0133	User attempted to modify User	user	attempted to modify	user	4724	An attempt was made to reset an account's pass...	windows	Man
	9227	T1098	False	Account Manipulation	[persistence]	[Windows, Azure AD, Office 365, IaaS, Linux, m...	user account	user account modification	REL-2022-0133	User attempted to modify User	user	attempted to modify	user	4724	An attempt was made to reset an account's pass...	windows	Man

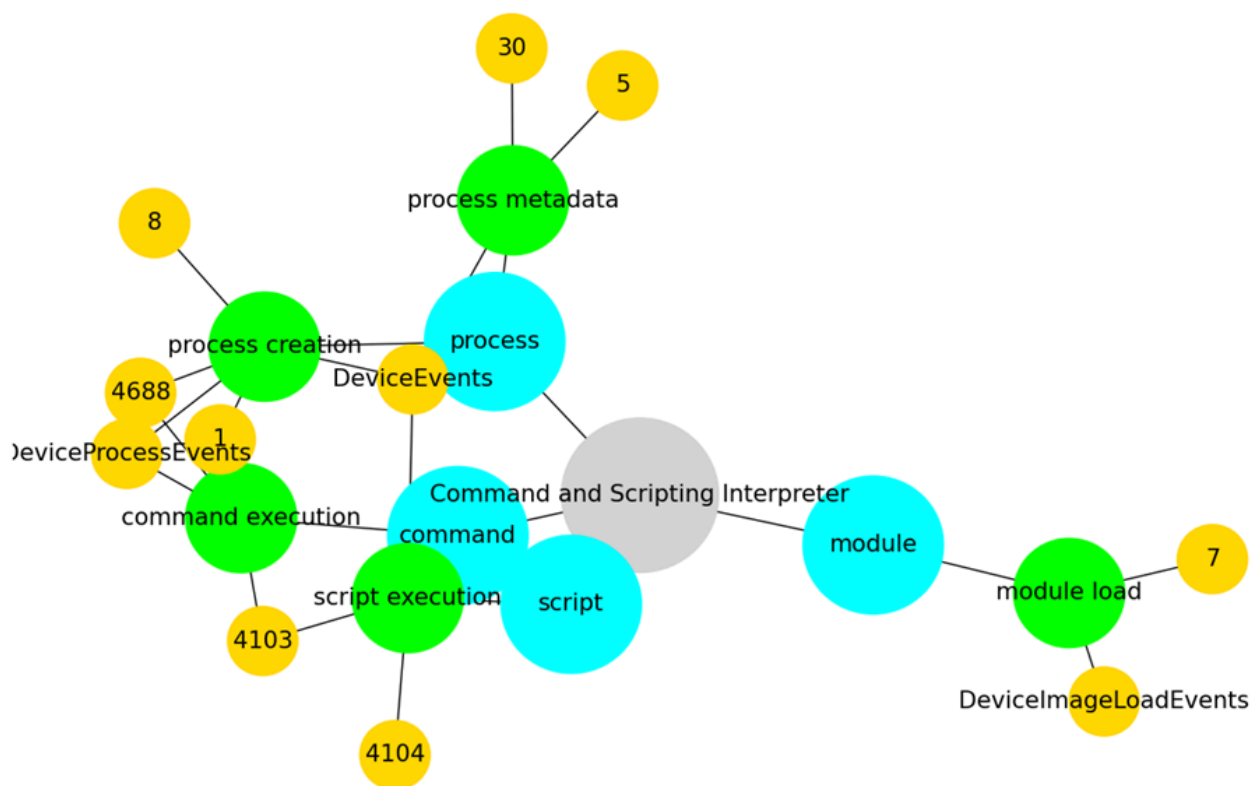
A filter on multiple columns is shown here:

```
mapping[(mapping['technique_id']=='T1448.002')][(mapping['event_id']=='5136')]
```

	technique_id	is_subtechnique	technique	tactic	platform	data_source	data_component	relationship_id	name	source	relationship	target	event_id	event_name	event_platform	audit_category
9628	T1059	False	Command and Scripting Interpreter	[execution]	[Linux, macOS, Windows, Network]	process	process creation	REL-2022-0146	User created Process	user	created	process	1	Process Creation.	windows	ProcessCreate
9629	T1059	False	Command and Scripting Interpreter	[execution]	[Linux, macOS, Windows, Network]	process	process creation	REL-2022-0146	User created Process	user	created	process	1	Process Creation.	linux	ProcessCreate
9634	T1059	False	Command and Scripting Interpreter	[execution]	[Linux, macOS, Windows, Network]	process	process creation	REL-2022-0175	Process created Process	process	created	process	1	Process Creation.	windows	ProcessCreate
9635	T1059	False	Command and Scripting Interpreter	[execution]	[Linux, macOS, Windows, Network]	process	process creation	REL-2022-0175	Process created Process	process	created	process	1	Process Creation.	linux	ProcessCreate
9638	T1059	False	Command and Scripting Interpreter	[execution]	[Linux, macOS, Windows, Network]	command	command execution	REL-2022-0018	User executed Command	user	executed	command	1	Process Creation.	windows	ProcessCreate
9642	T1059	False	Command and Scripting Interpreter	[execution]	[Linux, macOS, Windows, Network]	command	command execution	REL-2022-0131	Process executed Command	process	executed	command	1	Process Creation.	windows	ProcessCreate
9643	T1059	False	Command and Scripting Interpreter	[execution]	[Linux, macOS, Windows, Network]	command	command execution	REL-2022-0131	Process executed Command	process	executed	command	1	Process Creation.	linux	ProcessCreate

The second one is the `attack_network_graph` visualization that plots the graphical connections between the different mapping objects. The following command creates the visualization of all related nodes connected to technique T1059.


```
vis.attack_network_graph(mapping[(mapping['technique_id']=='T1059')])
```



Creating MITRE layers

Now that we have covered the basics of the OSSEM model, we can create MITRE layers for certain filters. I created a python script that can manipulate the OSSEM mappings, to create relevant MITRE layers based on chosen filters. For example, let's say we want the MITRE ATT&CK layer for all the Microsoft Defender for Endpoint Events and Microsoft Windows Security Events there are. For this, I use the code below.

```
# Microsoft Defender for Endpoint layer
techniques = get_mitre_techniques_by_filter(filterType='log_source',filterString='M:
create_mitre_mapping(techniques=techniques, template=mitre_layer, filename='Microso
# Microsoft-Windows-Security-Auditing layer
techniques = get_mitre_techniques_by_filter(filterType='log_source',filterString='M:
create_mitre_mapping(techniques=techniques, template=mitre_layer, filename='Microso
```

As you can see, I created two functions called 'get_mitre_techniques_by_filter' and 'create_mitre_mapping'. If you are interested in the code, let me know in the comments section and maybe I will share the GitHub repository later ?.

The output you get is the MITRE layer for the relevant filter that you can import in the **MITRE ATT&CK Navigator**.

```

},
"hideDisabled": false,
"techniques": [
  {
    "techniqueID": "T1622",
    "tactic": "defense-evasion",
    "score": 4,
    "color": "",
    "comment": "User created Process;Process created Process;User executed Command;Process executed Command",
    "enabled": true,
    "metadata": [],
    "links": [],
    "showSubtechniques": false
  },
  {
    "techniqueID": "T1622",
    "tactic": "discovery",
    "score": 4,
    "color": "",
    "comment": "User created Process;Process created Process;User executed Command;Process executed Command",
    "enabled": true,
    "metadata": [],
    "links": [],
    "showSubtechniques": false
  },
  {
    "techniqueID": "T1621",
    "tactic": "credential-access",
    "score": 8,
    "color": "",
    "comment": "Logon Metadata;User created logon from Ip;User created logon from Port;User created Logon;User attempted to authenticate from Port;User attempted to authentic",
    "enabled": true,
    "metadata": [],
    "links": [],
    "showSubtechniques": false
  },
  {
    "techniqueID": "T1505.005",
    "tactic": "persistence",
    "score": 8,
    "color": "",
    "comment": "User created Process;Process created Process;User executed Command;Process executed Command;User modified File;Process modified File;User modified Regist",
    "enabled": true,
    "metadata": [],
    "links": [],
    "showSubtechniques": true
  }
]

```

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2/3)	Acquire Infrastructure (2/7)	Drive-by Compromise (2/9)	Command and Scripting Interpreter (2/13)	Account Manipulation (2/19)	Abuse Elevation Control Mechanism (2/13)	Abuse Elevation Control Mechanism (2/42)	Adversary-in-the-Middle (2/17)	Account Discovery (2/30)	Exploitation of Remote Services (2/9)	Adversary-in-the-Middle (2/17)	Application Layer Protocol (2/16)	Automated Exfiltration (2/9)	Account Access Removal (2/13)
Gather Victim Host Information (2/10)	Compromise Accounts (2/7)	Exploit Public-Facing Application (2/9)	Container Administration Command (2/13)	BITS Jobs (2/19)	Access Token Manipulation (2/13)	Access Token Manipulation (2/42)	Brute Force (2/17)	Application Window Discovery (2/30)	Archive Collected Data (2/9)	Internal Spearphishing (2/17)	Communication Through Removable Media (2/16)	Data Transfer Size Limits (2/9)	Data Destruction (2/13)
Gather Victim Identity Information (2/10)	Compromise Infrastructure (2/7)	External Remote Services (2/9)	Deployment Container (2/13)	Boot or Logon Autostart Execution (2/19)	Boot or Logon Autostart Execution (2/13)	Boot or Logon Autostart Execution (2/42)	Credentials from Password Stores (2/17)	Browser Bookmark Discovery (2/30)	Internal Tool Transfer (2/9)	Audio Capture (2/17)	Exfiltration Over Alternative Protocol (2/16)	Data Encrypted for Impact (2/9)	Data Encrypted for Impact (2/13)
Gather Victim Network Information (2/10)	Develop Capabilities (2/7)	Hardware Additions (2/9)	Exploitation for Client Execution (2/13)	Boot or Logon Initialization Scripts (2/19)	Boot or Logon Initialization Scripts (2/13)	Boot or Logon Initialization Scripts (2/42)	Debugger Evasion (2/17)	Cloud Infrastructure Discovery (2/30)	Remote Service Hijacking (2/9)	Automated Collection (2/17)	Data Encoding (2/16)	Exfiltration Over C2 Channel (2/9)	Data Manipulation (2/13)
Gather Victim Org Information (2/10)	Establish Accounts (2/7)	Rhishing (2/9)	Inter-Process Communication (2/13)	Browser Extensions (2/19)	Desktop/Script/Decode Files or Information (2/13)	Desktop/Script/Decode Files or Information (2/42)	Forced Authentication (2/17)	Cloud Service Dashboard (2/30)	Session Hijacking (2/9)	Browser Session Hijacking (2/17)	Data Obfuscation (2/16)	Exfiltration Over Other Network Medium (2/9)	Defacement (2/13)
Phishing for Information (2/10)	Obtain Capabilities (2/7)	Replication Through Removable Media (2/9)	Native API (2/13)	Compromise Client Software Binary (2/19)	Create or Modify System Process (2/13)	Create or Modify System Process (2/42)	Forge Web Credentials (2/17)	Cloud Service Discovery (2/30)	Remote Services (2/9)	Clipboard Data (2/17)	Dynamic Resolution (2/16)	Endpoint Denial of Service (2/9)	Endpoint Denial of Service (2/13)
Search Closed Sources (2/10)	Stage Capabilities (2/7)	Supply Chain Compromise (2/9)	Scheduled Task/Job (2/13)	Create Account (2/19)	Domain Policy Modification (2/13)	Domain Policy Modification (2/42)	Input Capture (2/17)	Cloud Storage Object Discovery (2/30)	Application Through Removable Media (2/9)	Data from Cloud Storage (2/17)	Encrypted Channel (2/16)	Exfiltration Over Physical Medium (2/9)	Firmware Corruption (2/13)
Search Open Technical Databases (2/10)	Trusted Relationship (2/7)	Shared Modules (2/9)	Serverless Execution (2/13)	Event Triggered Execution (2/19)	Event Triggered Execution (2/13)	Event Triggered Execution (2/42)	Modify Authentication Process (2/17)	Container and Resource Discovery (2/30)	Debugger Evasion (2/9)	Data from Configuration Repository (2/17)	Fallback Channels (2/16)	Exfiltration Over Web Service (2/9)	Inhibit System Recovery (2/13)
Search Open Websites/Domains (2/10)	Valid Accounts (2/7)	Software Deployment Tools (2/9)	System Services (2/13)	External Remote Services (2/19)	Hijack Execution Flow (2/13)	Hijack Execution Flow (2/42)	Multi-Factor Authentication Interception (2/17)	File and Directory Discovery (2/30)	Software Deployment Tools (2/9)	Data from Information Repositories (2/17)	Ingress Tool Transfer (2/16)	Scheduled Transfer (2/9)	Network Denial of Service (2/13)
Search Victim-Owned Websites (2/10)	Windows Management Instrumentation (2/7)	User Execution (2/9)	Windows Management Instrumentation (2/13)	Implant Internal Image (2/19)	Scheduled Task/Job (2/13)	Scheduled Task/Job (2/42)	Request Generation (2/17)	Group Policy Discovery (2/30)	File and Directory Discovery (2/9)	Data from Local System (2/17)	Non-Application Layer Protocol (2/16)	Transfer Data to Cloud Account (2/9)	Resource Hijacking (2/13)
					Indicator Removal (2/13)	Indicator Removal (2/42)	Network Sniffing (2/17)	Network Service Discovery (2/30)	File and Directory Discovery (2/9)	Data from Network Shared Drive (2/17)	Non-Standard Port (2/16)	Service Stop (2/9)	System Shutdown/Reboot (2/13)
					Impair Defenses (2/13)	Impair Defenses (2/42)	OS Credential Dumping (2/17)	Network Sniffing (2/30)	File and Directory Discovery (2/9)	Data from Removable Media (2/17)	Protocol Tunneling (2/16)	System Shutdown/Reboot (2/9)	
					Indirect Command Execution (2/13)	Indirect Command Execution (2/42)	Steal or Forge Authentication Certificates (2/17)	Password Policy Discovery (2/30)	File and Directory Discovery (2/9)	Data Staged (2/17)	Proxy (2/16)	System Shutdown/Reboot (2/9)	
					Malicious File (2/13)	Malicious File (2/42)	Steal or Forge Authentication Certificates (2/17)	Peripheral Device Discovery (2/30)	File and Directory Discovery (2/9)	Input Capture (2/17)	Remote Access Software (2/16)	System Shutdown/Reboot (2/9)	
					Modify Authentication Process (2/13)	Modify Authentication Process (2/42)	Steal or Forge Kerberos (2/17)	Permission Groups Discovery (2/30)	File and Directory Discovery (2/9)	Screen Capture (2/17)	Traffic Signaling (2/16)	System Shutdown/Reboot (2/9)	
					Modify Cloud Compute Infrastructure (2/13)	Modify Cloud Compute Infrastructure (2/42)		Query Registry (2/30)	File and Directory Discovery (2/9)	Video Capture (2/17)	Web Service (2/16)	System Shutdown/Reboot (2/9)	

An explanation of the different parameters you can set in the `get_mitre_techniques_by_filter` function can be found below:

- `filterType` – This parameter lets you choose on which column you want to filter.
- `filterString`– This parameter is the string you will be searching for in the column you set in the `FilterType` parameter
- `techniquesArray` – The techniques array is an array you can provide if you already have a technique by filter array you want to reuse. This is typically empty or is an array that was created by the `get_mitre_techniques_by_filter` function itself.
- `commentProperty` – This is the column you want to include in the comments section of the techniques and will be the column that will be counted for the score of the layer

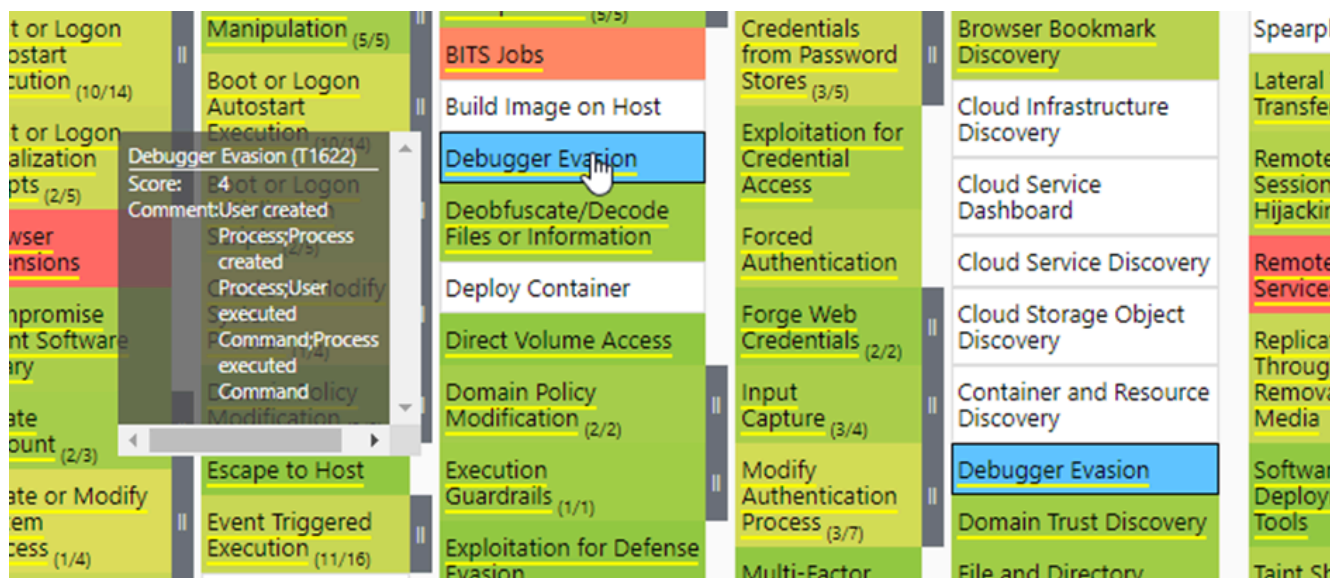
The score

Every technique that is present in the mapping layer gets a score. The score is the number of occurrences where the string in the `commentProperty` parameter maps to the relevant technique. For example, in the below command, we will count how many values in the 'name' column maps to the techniques that are included in the Microsoft Defender for Endpoint log source:

```
# Microsoft-Windows-Security-Auditing layer
techniques = get_mitre_techniques_by_filter(filterType='log_source',filterString='M:
create_mitre_mapping(techniques=techniques, template=mitre_layer, filename='Microso-
```

In the layer, we see that T1622 under Defender Evasion has a score of 4. This is because there are 4 occurrences in the 'name' column of the

mapping that relates to this technique:



When we plot this in the table form with Python, we see this is correct:

```
mapping[(mapping['technique_id']=='T1622')][(mapping['log_source']=='Microsoft-Windows-Security-Auditing')]
```

technique_id	is_subtechnique	technique	tactic	platform	data_source	data_component	relationship_id	name	source	relationship	target	event_id	event_name	event_platform	audit_category	as
2	T1622	False	Debugger Evasion	[defense-evasion, discovery]	[Windows, Linux, macOS]	process	process creation	REL-2022-0146	User created Process	user	created	process	4688	A new process has been created.	windows	Detailed Tracking
8	T1622	False	Debugger Evasion	[defense-evasion, discovery]	[Windows, Linux, macOS]	process	process creation	REL-2022-0175	Process created Process	process	created	process	4688	A new process has been created.	windows	Detailed Tracking
12	T1622	False	Debugger Evasion	[defense-evasion, discovery]	[Windows, Linux, macOS]	command	command execution	REL-2022-0018	User executed Command	user	executed	command	4688	A new process has been created.	windows	Detailed Tracking
16	T1622	False	Debugger Evasion	[defense-evasion, discovery]	[Windows, Linux, macOS]	command	command execution	REL-2022-0131	Process executed Command	process	executed	command	4688	A new process has been created.	windows	Detailed Tracking

The comments

As explained in the Score section, the comments contain the values of the column that was set in the commentProperty parameter. You can choose any column you like to be included in the comments section of the techniques. However, if you would like to compare layers with each other, it makes more sense to compare them with the 'name' column since these tell what is being detected

Comparing MITRE ATT&CK layers

Now that you have a basic understanding of how I can create MITRE layers with OSSEM, it is time to gather some insights by comparing layers.

MDE VS Windows Security Events

The first layers we are going to compare is the MDE and Windows Security Events layer. These layers are representations of **all the data you can log with the two data connectors, and how they are mapped to MITRE**. This does not mean that when you enable these data connectors in Sentinel, this will be your data coverage mapping. **It only shows what the potential is of both connectors.**

MDE mapping

To create the MDE mapping, I use the following commands:

```
# Microsoft Defender for Endpoint layer
techniques = get_mitre_techniques_by_filter('log_source','Microsoft Defender for Endp
create_mitre_mapping(techniques=techniques, template=mitre_layer, filename='Microso
```

You can download the JSON mapping below, so you can import the mapping yourself in the MITRE ATT&CK Navigator. When you open the navigator, you will see the following layer:

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning (3.0)	Acquire Infrastructure (3.0)	Drive-by Compromise (3.0)	Command and Control (3.0)	Account Manipulation (3.0)	Abuse Elevation Control Mechanism (3.0)	Abuse Elevation Control Mechanism (3.0)	Adversary in the Middle (3.0)	Account Discovery (3.0)	Exploitation of Remote Services (3.0)	Adversary in the Middle (3.0)	Application Layer Protocol (3.0)	Automated Exfiltration (3.0)	Account Access Removal (3.0)
Gather Victim Host Information (3.0)	Compromise Accounts (3.0)	Exploit Public-Facing Application (3.0)	Container Administration Command (3.0)	BITS Jobs (3.0)	Access Token Manipulation (3.0)	Access Token Manipulation (3.0)	Brute Force (3.0)	Application Window Discovery (3.0)	Internal Spearphishing (3.0)	Archive Collected Data (3.0)	Communication Through Removable Media (3.0)	Data Transfer Size Limits (3.0)	Data Destruction (3.0)
Gather Victim Identity Information (3.0)	Compromise Infrastructure (3.0)	External Remote Services (3.0)	Deploy Container (3.0)	Boot or Logon Autostart Execution (3.0)	Boot or Logon Autostart Execution (3.0)	Boot or Logon Autostart Execution (3.0)	Credentials from Browser Stores (3.0)	Browser Bookmark Discovery (3.0)	Remote Service Session Hijacking (3.0)	Audio Capture (3.0)	Data Encoding (3.0)	Exfiltration Over Alternative Protocol (3.0)	Data Encrypted for Impact (3.0)
Gather Victim Network Information (3.0)	Develop Capabilities (3.0)	Hardware Additions (3.0)	Exploitation for Client Execution (3.0)	Boot or Logon Initialization Scripts (3.0)	Boot or Logon Initialization Scripts (3.0)	Boot or Logon Initialization Scripts (3.0)	Build Image on Host (3.0)	Cloud Infrastructure Discovery (3.0)	Cloud Service Dashboard (3.0)	Automated Collection (3.0)	Data Obfuscation (3.0)	Defacement (3.0)	Data Manipulation (3.0)
Gather Victim Org Information (3.0)	Establish Accounts (3.0)	Phishing (3.0)	Inter-Process Communication (3.0)	Browser Extensions (3.0)	Create or Modify System Process (3.0)	Create or Modify System Process (3.0)	Debugger Evasion (3.0)	Cloud Storage Object Discovery (3.0)	Exploitation of Remote Services (3.0)	Remote Service Session Hijacking (3.0)	Dynamic Resolution (3.0)	Exfiltration Over C2 Channel (3.0)	Endpoint Denial of Service (3.0)
Phishing for Information (3.0)	Obtain Capabilities (3.0)	Replication Through Removable Media (3.0)	Native API (3.0)	Compromise Client Software Binary (3.0)	Domain Policy Modification (3.0)	Domain Policy Modification (3.0)	Forge Web Credentials (3.0)	Container and Resource Discovery (3.0)	Exploitation of Remote Services (3.0)	Clipboard Data (3.0)	Encrypted Channel (3.0)	Exfiltration Over Physical Medium (3.0)	Firmware Corruption (3.0)
Search Closed Sources (3.0)	Stage Capabilities (3.0)	Supply Chain Compromise (3.0)	Scheduled Task/Job (3.0)	Create Account (3.0)	Event Triggered Execution (3.0)	Event Triggered Execution (3.0)	Input Capture (3.0)	Debugger Evasion (3.0)	Exploitation of Remote Services (3.0)	Data from Cloud Storage (3.0)	Exfiltration Over Physical Medium (3.0)	Exfiltration Over Web Service (3.0)	Inhibit System Recovery (3.0)
Search Open Technical Databases (3.0)	Trusted Relationship (3.0)	Shared Modules (3.0)	Software Deployment Tools (3.0)	Event Triggered Execution (3.0)	Exploitation for Privilege Escalation (3.0)	Exploitation for Privilege Escalation (3.0)	Multi-Factor Authentication Request Generation (3.0)	File and Directory Discovery (3.0)	Exploitation of Remote Services (3.0)	Data from Configuration Repository (3.0)	Exfiltration Over Physical Medium (3.0)	Exfiltration Over Web Service (3.0)	Network Denial of Service (3.0)
Search Victim-Owned Websites (3.0)	Valid Accounts (3.0)	System Services (3.0)	User Execution (3.0)	External Remote Services (3.0)	Hijack Execution Flow (3.0)	Hijack Execution Flow (3.0)	Network Sniffing (3.0)	Group Policy Discovery (3.0)	Exploitation of Remote Services (3.0)	Data from Local System (3.0)	Exfiltration Over Physical Medium (3.0)	Exfiltration Over Web Service (3.0)	Resource Hijacking (3.0)
		Windows Management Instrumentation (3.0)	Implant Internal Image (3.0)	Modify Authentication Process (3.0)	Scheduled Task/Job (3.0)	Scheduled Task/Job (3.0)	OS Credential Dumping (3.0)	Network Share Discovery (3.0)	Exploitation of Remote Services (3.0)	Data from Removable Media (3.0)	Exfiltration Over Physical Medium (3.0)	Exfiltration Over Web Service (3.0)	Service Stop (3.0)
			Office Application Startup (3.0)	Office Application Startup (3.0)	Office Application Startup (3.0)	Office Application Startup (3.0)	Steal Application Access Token (3.0)	Peripheral Device Discovery (3.0)	Exploitation of Remote Services (3.0)	Data from Removable Media (3.0)	Exfiltration Over Physical Medium (3.0)	Exfiltration Over Web Service (3.0)	System Shutdown/Reboot (3.0)
			Pre-OS Boot (3.0)	Pre-OS Boot (3.0)	Pre-OS Boot (3.0)	Pre-OS Boot (3.0)	Steal or Forge Authentication Certificates (3.0)	Permission Groups Discovery (3.0)	Exploitation of Remote Services (3.0)	Data from Removable Media (3.0)	Exfiltration Over Physical Medium (3.0)	Exfiltration Over Web Service (3.0)	
			Scheduled Task/Job (3.0)	Scheduled Task/Job (3.0)	Scheduled Task/Job (3.0)	Scheduled Task/Job (3.0)	Steal or Forge Hardwares (3.0)	Process Discovery (3.0)	Exploitation of Remote Services (3.0)	Data from Removable Media (3.0)	Exfiltration Over Physical Medium (3.0)	Exfiltration Over Web Service (3.0)	
								Query Registry (3.0)	Exploitation of Remote Services (3.0)	Data from Removable Media (3.0)	Exfiltration Over Physical Medium (3.0)	Exfiltration Over Web Service (3.0)	

Mde name

mde-name.json • 237 KB



Windows Security Events mapping

To create the Windows Security Events mapping, I use the following commands:

```
# Microsoft-Windows-Security-Auditing layer
techniques = get_mitre_techniques_by_filter('log_source', 'Microsoft-Windows-Security-Auditing')
create_mitre_mapping(techniques=techniques, template=mitre_layer, filename='Microsoft-Windows-Security-Auditing-mapping.json')
```

You can download the JSON mapping below, so you can import the mapping yourself in the MITRE ATT&CK Navigator. When you open the navigator, you will see the following layer:

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning (10)	Acquire Infrastructure (17)	Drive-by Compromise (9)	Command and Scripting Interpreter (14)	Account Manipulation (14)	Abuse Elevation Control Mechanism (14)	Abuse Elevation Control Mechanism (14)	Adversary in-the-Middle (14)	Account Discovery (14)	Exploitation of Remote Services (14)	Adversary in-the-Middle (14)	Application Layer Protocol (14)	Automated Exfiltration (14)	Account Access Removal (14)
Gather Victim Host Information (14)	Compromise Accounts (14)	Exploit Public-Facing Application (14)	Container Administration Command (14)	BITS Jobs (14)	Access Token Manipulation (14)	Access Token Manipulation (14)	Brute Force (14)	Application Window Discovery (14)	Internal Spearphishing (14)	Archive Collected Data (14)	Communication Through Removable Media (14)	Data Transfer Size Limits (14)	Data Destruction (14)
Gather Victim Identity Information (14)	Compromise Infrastructure (17)	External Remote Services (14)	Deploy Container (14)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Credentials from Password Stores (14)	Browser Bookmark Discovery (14)	Remote Service Session Hijacking (14)	Audio Capture (14)	Automated Collection (14)	Exfiltration Over Alternative Protocol (14)	Data Encrypted for Impact (14)
Gather Victim Network Information (14)	Develop Capabilities (14)	Hardware Additions (14)	Exploitation for Client Execution (14)	Boot or Logon Initialization Scripts (14)	Boot or Logon Initialization Scripts (14)	Boot or Logon Initialization Scripts (14)	Exploitation for Credential Access (14)	Cloud Infrastructure Discovery (14)	Cloud Service Dashboard (14)	Remote Service Session Hijacking (14)	Browser Session Hijacking (14)	Exfiltration Over C2 Channel (14)	Data Manipulation (14)
Gather Victim Org Information (14)	Establish Accounts (14)	Phishing (14)	Inter-Process Communication (14)	Browser Extensions (14)	Create or Modify System Process (14)	Create or Modify System Process (14)	Forced Authentication (14)	Cloud Service Discovery (14)	Cloud Service Discovery (14)	Remote Services (14)	Clipboard Data (14)	Dynamic Resolution (14)	Defacement (14)
Phishing for Information (14)	Obtain Accounts (14)	Replication Through Removable Media (14)	Native API (14)	Compromise Client Software Binary (14)	Domain Policy Modification (14)	Domain Policy Modification (14)	Range Web Credentials (14)	Cloud Storage Object Discovery (14)	Application Through Removable Media (14)	Data from Cloud Storage (14)	Encrypted Channel (14)	Exfiltration Over Physical Medium (14)	Disk Wipe (14)
Search Closed Sources (14)	Stage Capabilities (14)	Supply Chain Compromise (14)	Scheduled Task/Job (14)	Create Account (14)	Escape to Host (14)	Escape to Host (14)	Input Capture (14)	Container and Resource Discovery (14)	Debugger Evasion (14)	Data from Configuration Repository (14)	Failback Channels (14)	Exfiltration Over Web Service (14)	Endpoint Denial of Service (14)
Search Open Technical Databases (14)	Search Open Websites/Domaines (14)	Trusted Relationship (14)	Shared Modules (14)	Create or Modify System Process (14)	Event Triggered Execution (14)	Event Triggered Execution (14)	Modify Authentication Process (14)	File and Directory Discovery (14)	Domain Trust Discovery (14)	Data from Local System (14)	Ingress Tool Transfer (14)	Scheduled Transfer (14)	Firmware Corruption (14)
Search Victim-Owned Websites (14)		Valid Accounts (14)	Software Deployment Tools (14)	System Services (14)	Event Triggered Execution (14)	Event Triggered Execution (14)	Multi-Factor Authentication Request Generation (14)	Network Service Discovery (14)	File and Directory Discovery (14)	Data from Network Shared Drive (14)	Non-Application Layer Protocol (14)	Transfer Data to Cloud Account (14)	Inhibit System Recovery (14)
			User Execution (14)	Windows Management Instrumentation (14)	Hijack Execution Flow (14)	Hijack Execution Flow (14)	Network Authentication Interception (14)	Network Service Discovery (14)	Group Policy Discovery (14)	Use Alternate Authentication Material (14)	Non-Standard Port (14)	Resource Hijacking (14)	Service Stop (14)
					Implant Internal Image (14)	Implant Internal Image (14)	OS Credential Dumping (14)	Network Sniffing (14)	Network Service Discovery (14)	Network Service Discovery (14)	Protocol Tunneling (14)	System Shutdown/Reboot (14)	
					Modify Authentication Process (14)	Modify Authentication Process (14)	Steal Application Access Token (14)	Peripheral Device Discovery (14)	Peripheral Device Discovery (14)	Peripheral Device Discovery (14)	Remote Access Software (14)		
					Office Application Startup (14)	Office Application Startup (14)	Steal or Forge Authentication Certificates (14)	Permission Groups Discovery (14)	Permission Groups Discovery (14)	Permission Groups Discovery (14)	Traffic Signaling (14)		
					Pre-OS Boot (14)	Pre-OS Boot (14)	Steal or Forge Certificates (14)	Process Discovery (14)	Process Discovery (14)	Process Discovery (14)	Web Service (14)		
					Scheduled Task/Job (14)	Scheduled Task/Job (14)	Steal or Forge Kerberos (14)	Query Registry (14)	Query Registry (14)	Query Registry (14)	Video Capture (14)		

Microsoft windows security auditing name

microsoft-windows-security-auditing-name.json • 247 KB



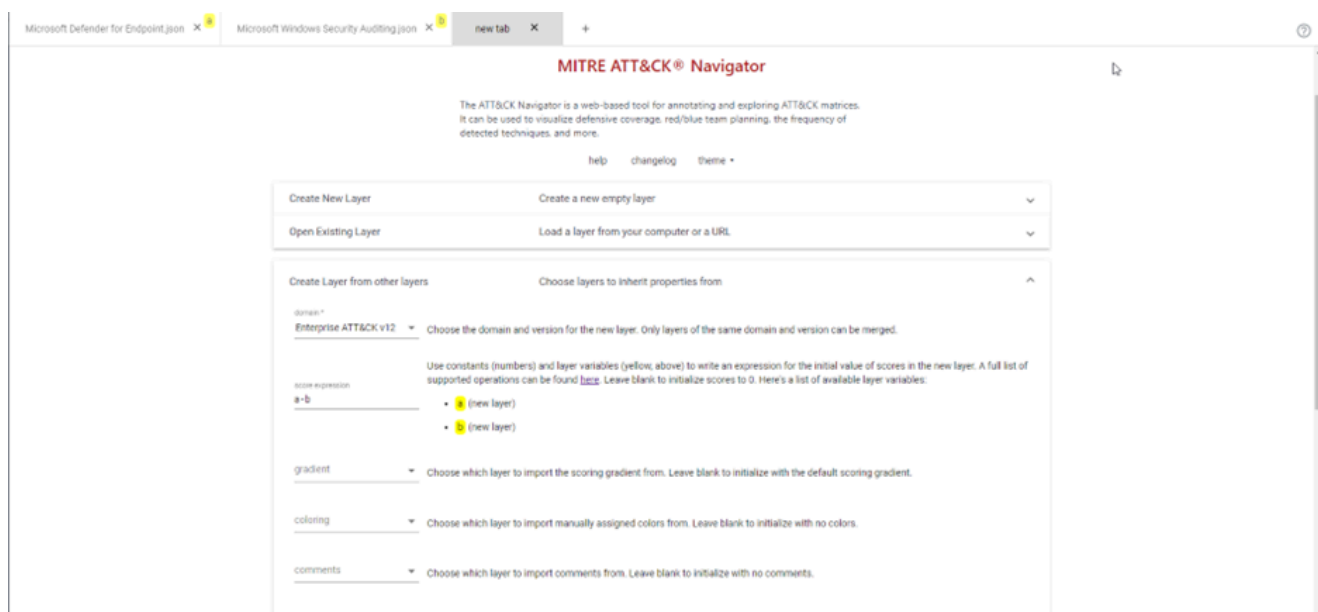
Comparing the layers

Before I start to compare the layers, I like to set the **scale in both layers to the same maximum value**. This way the colors of the techniques are comparable when you want to manually switch between the two layers. I always change the scale to the value of the layer that has the highest score. In this example, Microsoft Windows Security Logs has the highest score of 36, which means I also change the scale of the MDE layer to 36.



Now that the scales are the same, you can manually pivot between the two layers to compare which data source can map data to which techniques and compare which data source have most of the mappings to certain techniques. This can be very insightful information when you combine this with the most important techniques for your organization as described in my [first MITRE ATT&CK blog post](#).

When you quickly want to find out which data source is the best for you, this process is not ideal since it can take some time. To speed things up, you can create a comparison layer between the two. To do this, create a new layer from the two other layers by choosing the v12 Enterprise layer, and create a score expression where you subtract the Windows Security Events layer from the MDE layer:



After that, you get a new layer that tells you nothing.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	17 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (A1.1)	Acquire Infrastructure (A2.1)	Drive-by Compromise (A3.1)	Command and Scripting Interpreter (A4.1)	Account Manipulation (A5.1)	Abuse Elevation Control Mechanism (A6.1)	Abuse Elevation Control Mechanism (A6.1)	Adversary in-the-Middle (A7.1)	Account Discovery (A8.1)	Exploitation of Remote Services (A9.1)	Adversary in-the-Middle (A10.1)	Application Layer Protocol (A11.1)	Automated Exfiltration (A12.1)	Account Access Removal (A13.1)
Gather Victim Host Information (A1.2)	Compromise Accounts (A2.2)	Exploit Public-Facing Application (A3.2)	Container Administration Command (A4.2)	BITS Jobs (A5.2)	Access Token Manipulation (A6.2)	Access Token Manipulation (A6.2)	Brute Force (A7.2)	Application Window Discovery (A8.2)	Internal Spearphishing (A9.2)	Archive Collected Data (A10.2)	Communication Through Removable Media (A11.2)	Data Transfer Size Limits (A12.2)	Data Destruction (A13.2)
Gather Victim Identity Information (A1.3)	Compromise Infrastructure (A2.3)	External Remote Services (A3.3)	Deploy Container (A4.3)	Boot or Logon Autostart Execution (A5.3)	Boot or Logon Autostart Execution (A6.3)	Boot or Logon Autostart Execution (A6.3)	Credentials from Password Stores (A7.3)	Browser Bookmark Discovery (A8.3)	Remote Service Session Hijacking (A9.3)	Audio Capture (A10.3)	Data Encoding (A11.3)	Exfiltration Over Alternative Protocol (A12.3)	Data Encrypted for Impact (A13.3)
Gather Victim Network Information (A1.4)	Develop Capabilities (A2.4)	Hardware Additions (A3.4)	Exploitation for Client Execution (A4.4)	Boot or Logon Initialization Scripts (A5.4)	Boot or Logon Initialization Scripts (A6.4)	Boot or Logon Initialization Scripts (A6.4)	Debugger Evasion (A7.4)	Cloud Infrastructure Discovery (A8.4)	Remote Service Session Hijacking (A9.4)	Automated Collection (A10.4)	Data Obfuscation (A11.4)	Exfiltration Over Other Network Medium (A12.4)	Data Manipulation (A13.4)
Gather Victim Org Information (A1.5)	Establish Accounts (A2.5)	Phishing (A3.5)	Inter-Process Communication (A4.5)	Browser Extensions (A5.5)	Create or Modify System Process (A6.5)	Create or Modify System Process (A6.5)	Decompilate/Decode Files or Information (A7.5)	Cloud Service Dashboard (A8.5)	Remote Services (A9.5)	Browser Session Hijacking (A10.5)	Dynamic Resolution (A11.5)	Exfiltration Over Physical Medium (A12.5)	Defacement (A13.5)
Phishing for Information (A1.6)	Obtain Capabilities (A2.6)	Replication Through Removable Media (A3.6)	Native API (A4.6)	Compress Client Software Binary (A5.6)	Domain Policy Modification (A6.6)	Domain Policy Modification (A6.6)	Force Authentication (A7.6)	Cloud Service Discovery (A8.6)	Remote Services (A9.6)	Clipboard Data (A10.6)	Encrypted Channel (A11.6)	Exfiltration Over Other Network Medium (A12.6)	Disk Wipe (A13.6)
Search Closed Sources (A1.7)	Stage Capabilities (A2.7)	Supply Chain Compromise (A3.7)	Scheduled Task/Job (A4.7)	Create Account (A5.7)	Domain Policy Modification (A6.7)	Domain Policy Modification (A6.7)	Forge Web Credentials (A7.7)	Cloud Storage Object Discovery (A8.7)	Remote Services (A9.7)	Data from Cloud Storage (A10.7)	Encrypted Channel (A11.7)	Exfiltration Over Other Network Medium (A12.7)	Endpoint Denial of Service (A13.7)
Search Open Technical Databases (A1.8)	Trusted Relationship (A2.8)	Trusted Relationship (A3.8)	Serverless Execution (A4.8)	Create or Modify System Process (A5.8)	Domain Policy Modification (A6.8)	Domain Policy Modification (A6.8)	Input Capture (A7.8)	Container and Resource Discovery (A8.8)	Remote Services (A9.8)	Data from Configuration Repository (A10.8)	Encrypted Channel (A11.8)	Exfiltration Over Other Network Medium (A12.8)	Firmware Corruption (A13.8)
Search Open Websites/Domains (A1.9)	Valid Accounts (A2.9)	Valid Accounts (A3.9)	Shared Modules (A4.9)	Create or Modify System Process (A5.9)	Event Triggered Execution (A6.9)	Event Triggered Execution (A6.9)	Modify Authentication Process (A7.9)	Debugger Evasion (A8.9)	Software Deployment Tools (A9.9)	Data from Information Repositories (A10.9)	Encrypted Channel (A11.9)	Exfiltration Over Web Service (A12.9)	Inhibit System Recovery (A13.9)
Search Victim-Owned Websites (A1.10)			System Services (A4.10)	Event Triggered Execution (A5.10)	Exploitation for Privilege Escalation (A6.10)	Exploitation for Privilege Escalation (A6.10)	Multi-Factor Authentication Request Generation (A7.10)	File and Directory Discovery (A8.10)	Domain Trust Discovery (A9.10)	Data from Local System (A10.10)	Encrypted Channel (A11.10)	Exfiltration Over Web Service (A12.10)	Network Denial of Service (A13.10)
			User Execution (A4.11)	External Remote Services (A5.11)	Exploitation for Privilege Escalation (A6.11)	Exploitation for Privilege Escalation (A6.11)	Multi-Factor Authentication Request Generation (A7.11)	Group Policy Discovery (A8.11)	Use Alternate Authentication Material (A9.11)	Data from Network Shared Drive (A10.11)	Encrypted Channel (A11.11)	Exfiltration Over Web Service (A12.11)	Resource Hijacking (A13.11)
			Windows Management Instrumentation (A4.12)	Hijack Execution Flow (A5.12)	Process Injection (A6.12)	Process Injection (A6.12)	Multi-Factor Authentication Request Generation (A7.12)	Network Service Discovery (A8.12)	Use Alternate Authentication Material (A9.12)	Data from Removable Media (A10.12)	Encrypted Channel (A11.12)	Exfiltration Over Web Service (A12.12)	Service Stop (A13.12)
			Implement Internal Image (A4.13)	Scheduled Task/Job (A5.13)	Scheduled Task/Job (A6.13)	Scheduled Task/Job (A6.13)	Multi-Factor Authentication Request Generation (A7.13)	Network Sniffing (A8.13)	Use Alternate Authentication Material (A9.13)	Data from Removable Media (A10.13)	Encrypted Channel (A11.13)	Exfiltration Over Web Service (A12.13)	System Shutdown/Reboot (A13.13)
			Modify Authentication Process (A4.14)	Valid Accounts (A5.14)	Valid Accounts (A6.14)	Valid Accounts (A6.14)	Multi-Factor Authentication Request Generation (A7.14)	Network Sniffing (A8.14)	Use Alternate Authentication Material (A9.14)	Data from Removable Media (A10.14)	Encrypted Channel (A11.14)	Exfiltration Over Web Service (A12.14)	
			Office Application Start-Up (A4.15)				Multi-Factor Authentication Request Generation (A7.15)	Network Sniffing (A8.15)	Use Alternate Authentication Material (A9.15)	Data from Removable Media (A10.15)	Encrypted Channel (A11.15)	Exfiltration Over Web Service (A12.15)	
			Pre-OS Boot (A4.16)				Multi-Factor Authentication Request Generation (A7.16)	Network Sniffing (A8.16)	Use Alternate Authentication Material (A9.16)	Data from Removable Media (A10.16)	Encrypted Channel (A11.16)	Exfiltration Over Web Service (A12.16)	
			Scheduled Task/Job (A4.17)				Multi-Factor Authentication Request Generation (A7.17)	Network Sniffing (A8.17)	Use Alternate Authentication Material (A9.17)	Data from Removable Media (A10.17)	Encrypted Channel (A11.17)	Exfiltration Over Web Service (A12.17)	

But we can fix this! Simply go to the score settings and change the maximal value to the positive value of the minimal (-9 and +5 become -9 and +9). Then set the -9 score to green, the middle score to white, and the +9 score to red. Fyi, if you ever create another comparison layer, just make sure both the minimal and maximal scores reflect the score of the highest absolute number.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration	Impact
Active Scanning (10)	Acquire Infrastructure (20)	Drive-by Compromise (10)	Command and Scripting Interpreter (10)	Account Manipulation (10)	Abuse Elevation Control Mechanism (10)	Abuse Elevation Control Mechanism (10)	Adversary in-the-Middle (10)	Account Discovery (10)	Exploitation of Remote Services (10)	Automated Exfiltration (10)	Account Access Removal (10)
Gather Victim Host Information (10)	Compromise Accounts (10)	Exploit Public-Facing Application (10)	Container Administration Command (10)	BITS Jobs (10)	Access Token Manipulation (10)	Access Token Manipulation (10)	Brute Force (10)	Application Window Discovery (10)	Internal Spearphishing (10)	Data Transfer Size Limits (10)	Data Destruction (10)
Gather Victim Identity Information (10)	Compromise Infrastructure (10)	External Remote Services (10)	Deploy Container (10)	Boot or Logon Autostart Execution (10)	Boot or Logon Autostart Execution (10)	Build Image on Host (10)	Credentials from Password Stores (10)	Browser Bookmark Discovery (10)	Remote Service Session Hijacking (10)	Data Encrypted for Impact (10)	Data Manipulation (10)
Gather Victim Network Information (10)	Develop Capabilities (10)	Hardware Additions (10)	Exploitation for Client Execution (10)	Boot or Logon Initialization Scripts (10)	Boot or Logon Initialization Scripts (10)	Debugger Evasion (10)	Exploitation for Credential Access (10)	Cloud Infrastructure Discovery (10)	Cloud Service Hijacking (10)	Exfiltration Over Alternative Protocol (10)	Data Manipulation (10)
Gather Victim Org Information (10)	Establish Accounts (10)	Phishing (10)	Inter-Process Communication (10)	Browser Extensions (10)	Create or Modify System Process (10)	Deobfuscate/Decode Files or Information (10)	Forced Authentication (10)	Cloud Service Dashboard (10)	Remote Services (10)	Exfiltration Over C2 Channels (10)	Defacement (10)
Phishing for Information (10)	Obtain Capabilities (10)	Replication Through Removable Media (10)	Native API (10)	Compromise Client Software Binary (10)	Domain Policy Modification (10)	Direct Volume Access (10)	Forge Web Credentials (10)	Cloud Storage Object Discovery (10)	Clipboard Data (10)	Exfiltration Over Other Network Medium (10)	Disk Wipe (10)
Search Closed Sources (10)	Stage Capabilities (10)	Supply Chain Compromise (10)	Scheduled Task/Job (10)	Domain Policy Modification (10)	Event Triggered Execution (10)	Domain Policy Modification (10)	Input Capture (10)	Container and Resource Discovery (10)	Data from Cloud Storage (10)	Exfiltration Over Physical Medium (10)	Endpoint Denial of Service (10)
Search Open Technical Databases (10)	Trusted Relationship (10)	Shared Modules (10)	System Services (10)	Create Account (10)	Event Triggered Execution (10)	Execution Guardrails (10)	Modify Authentication Process (10)	Debugger Evasion (10)	Data from Configuration Repository (10)	Exfiltration Over Web Service (10)	Firmware Corruption (10)
Search Open Websites/Domains (10)	Valid Accounts (10)	Software Deployment Tools (10)	User Execution (10)	Create or Modify System Process (10)	Exploitation for Privilege Escalation (10)	Exploitation for Defense Evasion (10)	Multi-Factor Authentication Request Interception (10)	Domain Trust Discovery (10)	Data from Information Repositories (10)	Exfiltration Over Ingress Tool Transfer (10)	Network Denial of Service (10)
Search Victim-Owned Websites (10)			Windows Management Instrumentation (10)	Event Triggered Execution (10)	Exploitation for Privilege Escalation (10)	File and Directory Permissions Modification (10)	Multi-Factor Authentication Request Generation (10)	File and Directory Discovery (10)	Data from Local System (10)	Scheduled Transfer (10)	Resource Hijacking (10)
				Implant Internal Image (10)	Process Injection (10)	Hide Artifacts (10)	Network Sniffing (10)	Group Policy Discovery (10)	Data from Network Shared Drive (10)	Transfer Data to Cloud Account (10)	Service Stop (10)
				Scheduled Task/Job (10)	Scheduled Task/Job (10)	Impair Defenses (10)	OS Credential Dumping (10)	Network Service Discovery (10)	Non-Application Layer Protocol (10)	System Shutdown/Reboot (10)	
				Modify Authentication Process (10)	Valid Accounts (10)	Indicator Removal (10)	Stall or Forge Authentication Certificate (10)	Network Share Discovery (10)	Non-Standard Port (10)		
				Office Application Startup (10)		Indirect Command Execution (10)	Stall or Forge Authentication Certificate (10)	Peripheral Device Discovery (10)	Protocol Tunneling (10)		
				Pre-OS Boot (10)		Modify Cloud Compute Infrastructure (10)	Stall or Forge Authentication Certificate (10)	Permission Groups Discovery (10)	Proxy (10)		
				Scheduled Task/Job (10)				Process Discovery (10)	Small Collection (10)		
								Query Registry (10)	Screen Capture (10)		
									Video Capture (10)		

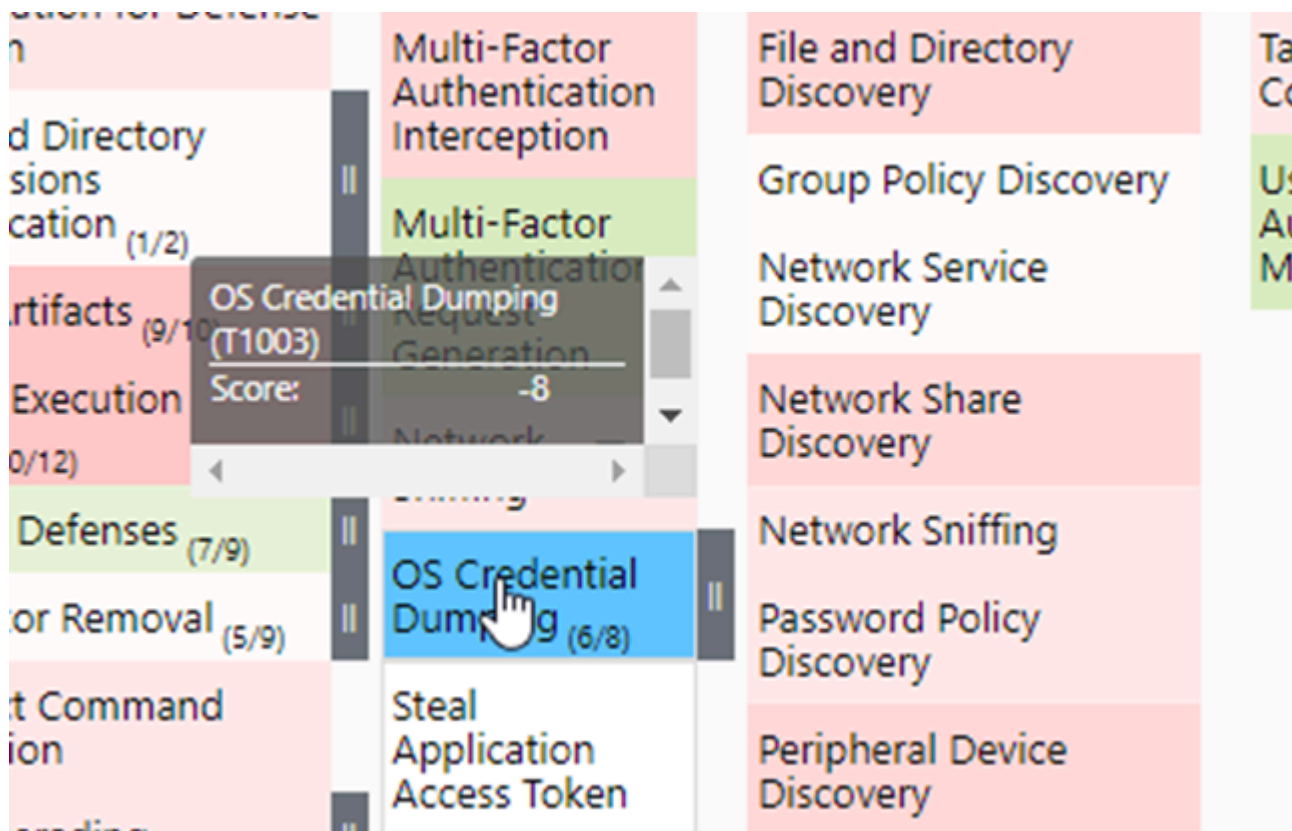
We now created a layer where **techniques that have a green color are techniques where Microsoft Security Logs have more mappings**, and **techniques that have a red color are techniques where MDE has more mappings**. This might be more useful when you try to decide which data source to use based on the techniques that matter the most to you. You can download this layer [here](#).

Mde vs security logs name

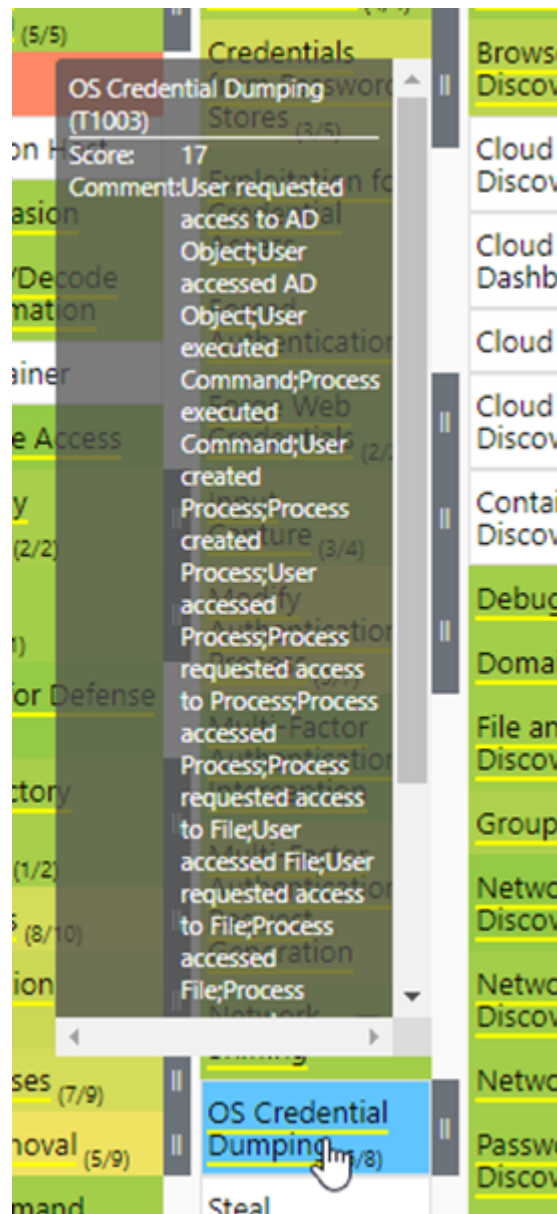
mde-vs-security-logs-name.json • 103 KB

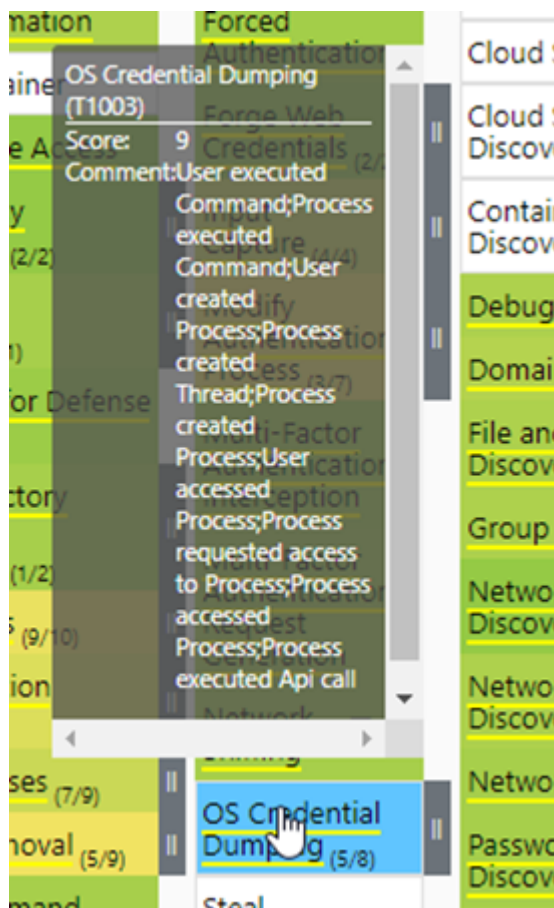


Be careful! A technique that has a dark color does not mean that the technique does not have any mappings of the other data source. It is more like a scale representation of the differences between the data sources. Let's say you are interested in OS Credential dumping, from the comparison layer you will learn the Microsoft Security Logs have more data mapped to this technique:



If you check this out in the Windows Security Logs layer and MDE layer, you will indeed see that Windows Security Logs have 8 more mappings than MDE has:





However, this does not necessarily mean that you must choose Windows Security Logs over MDE logs. When you check what MDE can map to this technique in the comments, this might be enough for your needs.

MDE VS Common Windows Security Events

If you have some experience with ingesting Windows Security Events in Microsoft Sentinel, you know that you have the option to choose between ingesting all, common, minimal, or customer Windows events. I think we can all agree that ingesting all Windows Security events is for a lot of organizations too expensive, which is why comparing the MDE VS Windows Security Events mapping might be less useful for some organizations. To solve this, I created a mapping for the common Windows Security events.

MDE mapping

I will not go into how the MDE layer is created, since we already covered that in the MDE VS Windows Security Events section. You can download

the MDE layer below.

Mde name



mde-name.json • 237 KB

Common Windows Security Events mapping

To be able to map the common events, we first need to know which events are included in the Common mapping. You can find the included events for common at this [Microsoft learn page](#). To create the MITRE layer I used the following code:

```
# Event IDs in Sentinel 'Common' Security Events
commonEvents = [1, 299, 300, 324, 340, 403, 404, 410, 411, 412, 413, 431, 500, 501,
                4647, 4648, 4649, 4657, 4661, 4662, 4663, 4665, 4666, 4667, 4688, 4689,
                4718, 4719, 4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730,
                4752, 4754, 4755, 4756, 4757, 4760, 4761, 4762, 4764, 4767, 4768, 4770,
                4825, 4826, 4870, 4886, 4887, 4888, 4893, 4898, 4902, 4904, 4905, 4906,
                5140, 5145, 5632, 6144, 6145, 6272, 6273, 6278, 6416, 6423, 6424, 8000]

# Common events layer
techniques_local = []
for event in commonEvents:
    techniques_local = get_mitre_techniques_by_filter('event_id',str(event), technique_id_list=techniques_local)
create_mitre_mapping(techniques=techniques_local, template=mitre_layer, filename='CommonEvents.json')
```

You can download the JSON mapping here, so you can import the mapping yourself in the MITRE ATT&CK Navigator. When you open the navigator, you will see the following layer:

Common security events name



common-security-events-name.json • 199 KB

Microsoft Defender for Endpoint.json x Common Security Events.json x +

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3/3)	Acquire Infrastructure (3/7)	Drive-by Compromise (3/9)	Command and Scripting Interpreter (3/13)	Account Manipulation (3/19)	Abuse Elevation Control Mechanism (3/13)	Abuse Elevation Control Mechanism (3/42)	Adversary-in-the-Middle (3/17)	Account Discovery (3/30)	Exploitation of Remote Services (3/9)	Adversary-in-the-Middle (3/16)	Automated Exfiltration (3/9)	Account Access Removal (3/13)
Gather Victim Host Information (3/10)	Compromise Accounts (3/7)	Exploit Public-Facing Application (3/9)	Container Administration Command (3/13)	BITS Jobs (3/19)	Access Token Manipulation (3/13)	Access Token Manipulation (3/42)	Brute Force (3/17)	Application Window Discovery (3/30)	Internal Spearphishing (3/9)	Communication Through Removable Media (3/16)	Data Transfer Size Limits (3/9)	Data Destruction (3/13)
Gather Victim Identity Information (3/10)	Compromise Infrastructure (3/7)	External Remote Services (3/9)	Deploy Container (3/13)	Boot or Logon Autostart Execution (3/19)	Access Token Manipulation (3/13)	Access Token Manipulation (3/42)	Credentials from Password Stores (3/17)	Browser Bookmark Discovery (3/30)	Automated Collection (3/9)	Audio Capture (3/16)	Exfiltration Over Alternative Protocol (3/9)	Data Encrypted for Impact (3/13)
Gather Victim Network Information (3/10)	Develop Capabilities (3/7)	Hardware Additions (3/9)	Exploitation for Client Execution (3/13)	Boot or Logon Autostart Execution (3/19)	Boot or Logon Autostart Execution (3/13)	Boot or Logon Autostart Execution (3/42)	Build Image on Host (3/17)	Cloud Infrastructure Discovery (3/30)	Remote Service Session Hijacking (3/9)	Data Encoding (3/16)	Exfiltration Over C2 Channel (3/9)	Data Manipulation (3/13)
Gather Victim Org Information (3/10)	Establish Accounts (3/7)	Phishing (3/9)	Inter-Process Communication (3/13)	Browser Extensions (3/19)	Boot or Logon Initialization Scripts (3/13)	Boot or Logon Initialization Scripts (3/42)	Debugger Evasion (3/17)	Cloud Service Dashboard (3/30)	Remote Service Session Hijacking (3/9)	Data Obfuscation (3/16)	Exfiltration Over Other Network Medium (3/9)	Defacement (3/13)
Phishing for Information (3/10)	Obtain Capabilities (3/7)	Replication Through Removable Media (3/9)	Native API (3/13)	Browser Extensions (3/19)	Boot or Logon Initialization Scripts (3/13)	Boot or Logon Initialization Scripts (3/42)	Deobfuscate/Decode Files or Information (3/17)	Cloud Service Discovery (3/30)	Remote Services (3/9)	Dynamic Resolution (3/16)	Exfiltration Over Endpoint Denial of Service (3/9)	Disk Wipe (3/13)
Search Closed Sources (3/10)	Stage Capabilities (3/7)	Supply Chain Compromise (3/9)	Scheduled Task/job (3/13)	Compromise Client Software Binary (3/19)	Create or Modify System Process (3/13)	Create or Modify System Process (3/42)	Direct Volume Access (3/17)	Cloud Storage Object Discovery (3/30)	Replication Through Removable Media (3/9)	Encrypted Channel (3/16)	Exfiltration Over Physical Medium (3/9)	Firmware Corruption (3/13)
Search Open Technical Databases (3/10)		Trusted Relationship (3/9)	Software Deployment Tools (3/13)	Domain Policy Modification (3/19)	Escape to Host (3/13)	Escape to Host (3/42)	Deploy Container (3/17)	Container and Resource Discovery (3/30)	Software Deployment Tools (3/9)	Failback Channels (3/16)	Exfiltration Over Web Service (3/9)	Inhibit System Recovery (3/13)
Search Open Websites/Domains (3/10)		Valid Accounts (3/9)	System Services (3/13)	Event Triggered Execution (3/19)	Event Triggered Execution (3/13)	Event Triggered Execution (3/42)	Domain Policy Modification (3/17)	Debugger Evasion (3/30)	Taint Shared Content (3/9)	Multi-Stage Channels (3/16)	Network Denial of Service (3/9)	Resource Hijacking (3/13)
Search Victim-Owned Websites (3/10)			User Execution (3/13)	External Remote Services (3/19)	External Remote Services (3/13)	External Remote Services (3/42)	File and Directory Permissions Modification (3/17)	Domain Trust Discovery (3/30)	Use Alternate Authentication Material (3/9)	Non-Application Layer Protocol (3/16)	Transfer Data to Cloud Account (3/9)	System Shutdown/Reboot (3/13)
			Windows Management Instrumentation (3/13)	Hijack Execution Flow (3/19)	Hijack Execution Flow (3/13)	Hijack Execution Flow (3/42)	Hide Artifacts (3/17)	Network Service Discovery (3/30)	Non-Standard Port (3/9)	Protocol Tunneling (3/16)		
				Implant Internal Image (3/19)	Implant Internal Image (3/13)	Implant Internal Image (3/42)	Impair Defenses (3/17)	Network Share Discovery (3/30)				
				Scheduled Task/job (3/19)	Scheduled Task/job (3/13)	Scheduled Task/job (3/42)	Indicator Removal (3/17)	Network Sniffing (3/30)				
				Modify Authentication Process (3/19)	Valid Accounts (3/13)	Valid Accounts (3/42)	Indirect Command Execution (3/17)	OS Credential Dumping (3/30)				
				Office Application Startup (3/19)			Input Capture (3/17)	Password Policy Discovery (3/30)				
				Pre-OS Boot (3/19)			Stall Application Access Token (3/17)	Peripheral Device Discovery (3/30)				
				Scheduled Task/job (3/19)			Stall or Forge Authentication Certificates (3/17)	Permission Groups Discovery (3/30)				
							Stall or Forge Kerberos Tickets (3/17)	Process Discovery (3/30)				
								Query Registry (3/30)				

Comparing the layers

I will not go into detail about how to set up the layers for comparing them with each other, since I already cover this in the MDE VS Windows Security Events section. If you create a comparison layer for both, you will now see that in general MDE has more data mappings than the Common Windows Security Events does:

Microsoft Defender for Endpoint.json x Common Security Events.json x MDE VS Common Security Log x +

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3/3)	Acquire Infrastructure (3/7)	Drive-by Compromise (3/9)	Command and Scripting Interpreter (3/13)	Account Manipulation (3/19)	Abuse Elevation Control Mechanism (3/13)	Abuse Elevation Control Mechanism (3/42)	Adversary-in-the-Middle (3/17)	Account Discovery (3/30)	Exploitation of Remote Services (3/9)	Adversary-in-the-Middle (3/16)	Automated Exfiltration (3/9)	Account Access Removal (3/13)
Gather Victim Host Information (3/10)	Compromise Accounts (3/7)	Exploit Public-Facing Application (3/9)	Container Administration Command (3/13)	BITS Jobs (3/19)	Access Token Manipulation (3/13)	Access Token Manipulation (3/42)	Brute Force (3/17)	Application Window Discovery (3/30)	Internal Spearphishing (3/9)	Communication Through Removable Media (3/16)	Data Transfer Size Limits (3/9)	Data Destruction (3/13)
Gather Victim Identity Information (3/10)	Compromise Infrastructure (3/7)	External Remote Services (3/9)	Deploy Container (3/13)	Boot or Logon Autostart Execution (3/19)	Access Token Manipulation (3/13)	Access Token Manipulation (3/42)	Credentials from Password Stores (3/17)	Browser Bookmark Discovery (3/30)	Automated Collection (3/9)	Audio Capture (3/16)	Exfiltration Over Alternative Protocol (3/9)	Data Encrypted for Impact (3/13)
Gather Victim Network Information (3/10)	Develop Capabilities (3/7)	Hardware Additions (3/9)	Exploitation for Client Execution (3/13)	Boot or Logon Autostart Execution (3/19)	Boot or Logon Autostart Execution (3/13)	Boot or Logon Autostart Execution (3/42)	Build Image on Host (3/17)	Cloud Infrastructure Discovery (3/30)	Remote Service Session Hijacking (3/9)	Data Encoding (3/16)	Exfiltration Over C2 Channel (3/9)	Data Manipulation (3/13)
Gather Victim Org Information (3/10)	Establish Accounts (3/7)	Phishing (3/9)	Inter-Process Communication (3/13)	Browser Extensions (3/19)	Boot or Logon Initialization Scripts (3/13)	Boot or Logon Initialization Scripts (3/42)	Debugger Evasion (3/17)	Cloud Service Dashboard (3/30)	Remote Service Session Hijacking (3/9)	Data Obfuscation (3/16)	Exfiltration Over Other Network Medium (3/9)	Defacement (3/13)
Phishing for Information (3/10)	Obtain Capabilities (3/7)	Replication Through Removable Media (3/9)	Native API (3/13)	Browser Extensions (3/19)	Boot or Logon Initialization Scripts (3/13)	Boot or Logon Initialization Scripts (3/42)	Deobfuscate/Decode Files or Information (3/17)	Cloud Service Discovery (3/30)	Remote Services (3/9)	Dynamic Resolution (3/16)	Exfiltration Over Endpoint Denial of Service (3/9)	Disk Wipe (3/13)
Search Closed Sources (3/10)	Stage Capabilities (3/7)	Supply Chain Compromise (3/9)	Scheduled Task/job (3/13)	Compromise Client Software Binary (3/19)	Create or Modify System Process (3/13)	Create or Modify System Process (3/42)	Direct Volume Access (3/17)	Cloud Storage Object Discovery (3/30)	Replication Through Removable Media (3/9)	Encrypted Channel (3/16)	Exfiltration Over Physical Medium (3/9)	Firmware Corruption (3/13)
Search Open Technical Databases (3/10)		Trusted Relationship (3/9)	Software Deployment Tools (3/13)	Domain Policy Modification (3/19)	Escape to Host (3/13)	Escape to Host (3/42)	Deploy Container (3/17)	Container and Resource Discovery (3/30)	Software Deployment Tools (3/9)	Failback Channels (3/16)	Exfiltration Over Web Service (3/9)	Inhibit System Recovery (3/13)
Search Open Websites/Domains (3/10)		Valid Accounts (3/9)	System Services (3/13)	Event Triggered Execution (3/19)	Event Triggered Execution (3/13)	Event Triggered Execution (3/42)	Domain Policy Modification (3/17)	Debugger Evasion (3/30)	Taint Shared Content (3/9)	Multi-Stage Channels (3/16)	Network Denial of Service (3/9)	Resource Hijacking (3/13)
Search Victim-Owned Websites (3/10)			User Execution (3/13)	External Remote Services (3/19)	External Remote Services (3/13)	External Remote Services (3/42)	File and Directory Permissions Modification (3/17)	Domain Trust Discovery (3/30)	Use Alternate Authentication Material (3/9)	Non-Application Layer Protocol (3/16)	Transfer Data to Cloud Account (3/9)	System Shutdown/Reboot (3/13)
			Windows Management Instrumentation (3/13)	Hijack Execution Flow (3/19)	Hijack Execution Flow (3/13)	Hijack Execution Flow (3/42)	Hide Artifacts (3/17)	Network Service Discovery (3/30)	Non-Standard Port (3/9)	Protocol Tunneling (3/16)		
				Implant Internal Image (3/19)	Implant Internal Image (3/13)	Implant Internal Image (3/42)	Impair Defenses (3/17)	Network Share Discovery (3/30)				
				Scheduled Task/job (3/19)	Scheduled Task/job (3/13)	Scheduled Task/job (3/42)	Indicator Removal (3/17)	Network Sniffing (3/30)				
				Modify Authentication Process (3/19)	Valid Accounts (3/13)	Valid Accounts (3/42)	Indirect Command Execution (3/17)	OS Credential Dumping (3/30)				
				Office Application Startup (3/19)			Input Capture (3/17)	Password Policy Discovery (3/30)				
				Pre-OS Boot (3/19)			Stall Application Access Token (3/17)	Peripheral Device Discovery (3/30)				
				Scheduled Task/job (3/19)			Stall or Forge Authentication Certificates (3/17)	Permission Groups Discovery (3/30)				
							Stall or Forge Kerberos Tickets (3/17)	Process Discovery (3/30)				
								Query Registry (3/30)				

You can download this layer here.

mde-vs-common-security-log-name.json • 110 KB

When you compare layers and create new ones as we did in the previous chapters, it might be interesting to weigh these layers with the techniques you are interested in. If you want to learn how to decide which techniques are the most important for your organization, make sure to read the [first MITRE ATT&CK blog post](#) of HybridBrothers.

Let's say you have a simple MITRE layer where every relevant technique for your organization has a score of 1, and all other techniques that are not relevant are disabled.

MITRE ATT&CK Framework													
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	10 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning g0l	Acquire Infrastructure g0l	Drive-by Compromise	Command and Scripting Interpreter g0l	Account Manipulation g0l	Abuse Elevation Control Mechanism g0l	Abuse Elevation Control Mechanism g0l	Adversary in-the-Middle g0l	Account Discovery g0l	Exploitation of Remote Services g0l	Adversary in-the-Middle g0l	Application Layer Protocol g0l	Automated Lateralization g0l	Account Access Removal
Gather Victim Host Information g0l	Compromise Accounts g0l	Exploit Public-Facing Application g0l	Container Administration Command g0l	RITS Jobs g0l	Access Token Manipulation g0l	Access Token Manipulation g0l	Brute Force g0l	Application Window Discovery g0l	Internal Spearphishing g0l	Archive Collected Data g0l	Communication Channel Removable Media g0l	Data Transfer Size Limits g0l	Data Destruction
Gather Victim Identity Information g0l	Compromise Infrastructure g0l	External Remote Services g0l	Deploy Container Executables g0l	Boot or Logon Autostart Execution g0l	Boot or Logon Autostart Execution g0l	RITS Jobs g0l	Credentials from Password Stores g0l	Browser Bookmark Discovery g0l	Remote Service Session Hijacking g0l	Automated Collection g0l	Data Encoding g0l	Data Encrypted for Impact g0l	Data Encrypted for Impact
Gather Victim Network Information g0l	Develop Capabilities g0l	Hardware Additions g0l	Exploitation for Client Execution g0l	Browser Extensions g0l	Build Image on Host g0l	Debugger Execution g0l	Exploitation for Credential Access g0l	Cloud Infrastructure Discovery g0l	Remote Service Session Hijacking g0l	Multi-Stage Channel g0l	Dynamic Resolution g0l	Exfiltration Over Other Network g0l	Exfiltration Over Other Network
Gather Victim Org Information g0l	Establish Accounts g0l	Obtain Capabilities g0l	Inter-Process Communication g0l	Compromise Client Software Binary g0l	Boot or Logon Indicators g0l	Debugger Execution g0l	Forced Authentication g0l	Cloud Service Checkpoint g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
Hijacking for Information g0l	Obtain Capabilities g0l	Application Through Removable Media g0l	Native API g0l	Compromise Client Software Binary g0l	Create or Modify System Registry g0l	Deploy Container Direct Volume Access g0l	Forge Web Cookies g0l	Cloud Service Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
Search Cloud Sources g0l	Stage Capabilities g0l	Supply Chain Compromise g0l	Scheduled Task/Job g0l	Create Account g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
Search Open Technical Databases g0l	Trusted Relationship g0l	Shared Modules g0l	Serverless Execution g0l	Event to Host g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
Search Open Websites/Domains g0l	Valid Accounts g0l	Software Deployment Tools g0l	System Services g0l	Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
Search Victim-Owned Websites g0l	Valid Accounts g0l	System Services g0l	System Services g0l	Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
		User Execution g0l	User Execution g0l	Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
		Windows Management Instrumentation g0l	Windows Management Instrumentation g0l	Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification g0l	Input Capture g0l	Container and Resource Discovery g0l	Remote Services g0l	Clipboard Data g0l	Dynamic Resolution g0l	Exfiltration Over Physical Medium g0l	Exfiltration Over Physical Medium
				Event Triggered Execution g0l	Domain Policy Modification g0l	Domain Policy Modification							

In this example we will be using the comparison layer of MDE and Windows Security Event logs:

To create a new layer of a comparison layer that has the weighting of the above prioritization layer, you need the following settings:

By doing this, we will reuse the score of the techniques in the comparison layer if the prioritization layer also has a score of 1 (since we multiply the two layers). When a technique does not have a score of 1 in the prioritization layer, the technique will get an empty score regardless of the score in the comparison layer. We reuse the gradient and colors of the comparison layer, so we get the same look and feel. Finally, we take the

The screenshot displays the MITRE ATT&CK framework interface, showing a grid of attack techniques categorized by phase and platform. The top navigation bar includes tabs for different platforms: Microsoft Defender for Endpoint, Microsoft Windows Security Auditing, MDE VS Security Logs, Important Techniques, MDE VS Security Logs X Pro Techniques, and Technique Controls. The main grid is organized into columns representing different phases of an attack, with techniques listed in rows. Each technique entry includes an icon, a name, and a brief description. The interface also features a search bar and various filters on the right side.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0.1)	Acquire Infrastructure (0.1)	Drive-by Compromise (0.1)	Command and Scripting Interface (0.1)	Account Manipulation (0.1)	Abuse Elevation Control Mechanism (0.1)	Abuse Elevation Control Mechanism (0.1)	Adversary in the Middle (0.1)	Account Discovery (0.1)	Exploitation of Remote Services (0.1)	Adversary in the Middle (0.1)	Application Layer Protocol (0.1)	Automated Exfiltration (0.1)	Account Access Removal (0.1)
Gather Victim Host Information (0.1)	Compromise Accounts (0.1)	Exploit Public-Facing Application (0.1)	Container Administration Command (0.1)	BITS Jobs (0.1)	Access Token Manipulation (0.1)	Access Token Manipulation (0.1)	Brute Force (0.1)	Application Window Discovery (0.1)	Internal Spearphishing (0.1)	Archive Collected Data (0.1)	Communication (0.1)	Data Transfer Size Limits (0.1)	Data Destruction (0.1)
Gather Victim Identity Information (0.1)	Compromise Infrastructure (0.1)	External Remote Services (0.1)	Deploy Container (0.1)	Boot or Logon Automation (0.1)	Boot or Logon Manipulation (0.1)	BITS Jobs (0.1)	Credentials from Password Store (0.1)	Browser Bookmark Discovery (0.1)	Lateral Tool Transfer (0.1)	Audio Capture (0.1)	Removable (0.1)	Data Encrypted for Impact (0.1)	Data Encrypted for Impact (0.1)
Gather Victim Network Information (0.1)	Develop Capabilities (0.1)	Hardware Additions (0.1)	Exploitation for Client Execution (0.1)	Boot or Logon Initialization Scripts (0.1)	Boot or Logon Initialization Scripts (0.1)	Build Image on Host (0.1)	Exploitation for Credential Access (0.1)	Cloud Infrastructure Discovery (0.1)	Remote Service Session Hijacking (0.1)	Automated Collection (0.1)	Data Encoding (0.1)	Exfiltration Over Alternative Protocol (0.1)	Data Manipulation (0.1)
Gather Victim Org Information (0.1)	Establish Accounts (0.1)	Phishing (0.1)	Inter-Process Communication (0.1)	Browser Extensions (0.1)	Boot or Logon Initialization Scripts (0.1)	Debugger Evasion (0.1)	Exploitation for Lateral Movement (0.1)	Cloud Service Dashboard Access (0.1)	Service Hijacking (0.1)	Browser Session Hijacking (0.1)	Data Obfuscation (0.1)	Exfiltration Over C2 Channel (0.1)	Defacement (0.1)
Phishing for Information (0.1)	Obtain Capabilities (0.1)	Obtain Capabilities (0.1)	Application Through Removable Media (0.1)	Create or Modify System Processes (0.1)	Create or Modify System Processes (0.1)	Desktop/Account/Device Files or Information (0.1)	Forceful Authentication (0.1)	Cloud Service Discovery (0.1)	Remote Services (0.1)	Clipboard Data (0.1)	Dynamic Exfiltration (0.1)	Exfiltration Over Other Network Medium (0.1)	Disk Wipe (0.1)
Search Cloud Sources (0.1)	Stage Capabilities (0.1)	Supply Chain Compromise (0.1)	Native API (0.1)	Compromise Client Software Binary (0.1)	Compromise Client Software Binary (0.1)	Deploy Container (0.1)	Forge Web Storage (0.1)	Cloud Storage Object Storage (0.1)	Service Hijacking (0.1)	Data from Cloud Storage (0.1)	Encrypted Channel (0.1)	Exfiltration Over Physical Medium (0.1)	Endpoint Denial of Service (0.1)
Search Open Technical Databases (0.1)	Trusted Relationship (0.1)	Valid Accounts (0.1)	Shared Modules (0.1)	Create Account (0.1)	Create Account (0.1)	Domain Policy Modification (0.1)	Input Capture (0.1)	Container and Resource Discovery (0.1)	Software Deployment Tools (0.1)	Data from Configuration Repository (0.1)	Fallback Channels (0.1)	Exfiltration Over Web Service (0.1)	Firmware Corruption (0.1)
Search Open Websites/Domain (0.1)	Valid Accounts (0.1)	Valid Accounts (0.1)	Software Deployment Tools (0.1)	Event Triggered Execution (0.1)	Event Triggered Execution (0.1)	Exploitation for Defense Evasion (0.1)	Modify Authentication Process (0.1)	Domain Trust Discovery (0.1)	Domain Trust Discovery (0.1)	Data from Information Repository (0.1)	Ingress Tool Transfer (0.1)	Exfiltration Over Web Service (0.1)	Inhibit System Recovery (0.1)
Search Victim-Owned Websites (0.1)	Windows Management Instrumentation (0.1)	Windows Management Instrumentation (0.1)	User Execution (0.1)	External Remote Services (0.1)	Hijack Execution Flow (0.1)	Hijack Execution Flow (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial of Service (0.1)	Resource Hijacking (0.1)
			System Services (0.1)	System Services (0.1)	System Services (0.1)	System Services (0.1)	Multi-Factor Authentication Interception (0.1)	File and Directory Permissions Manipulation (0.1)	Multi-Factor Authentication Interception (0.1)	Task Shared Context (0.1)	Multi-Stage Channel (0.1)	Network Denial	

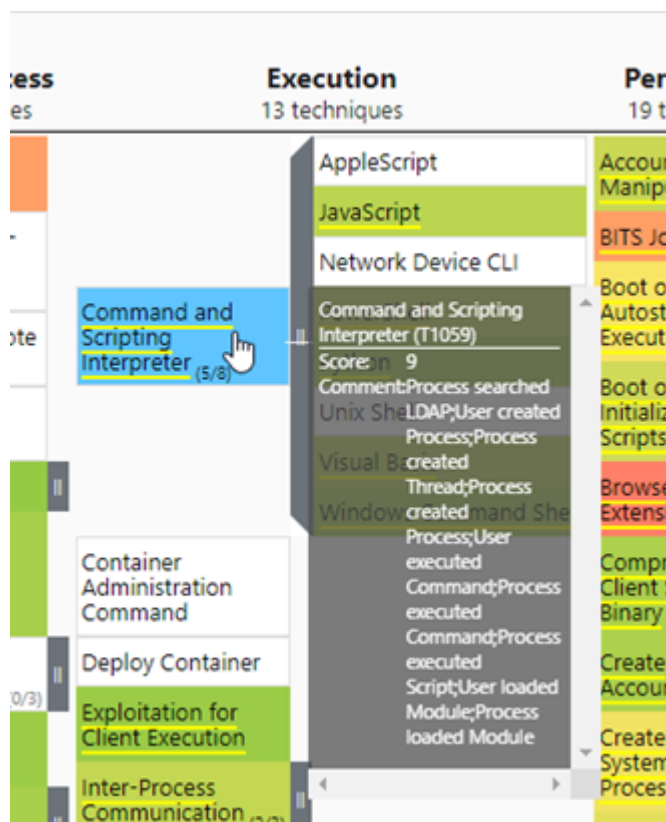
Finding MDE tables and Windows Event IDs based on MITRE layers

<https://hybridbrothers.com/mapping-mde-and-windows-security-events-overlap/>

data related to 'Command and Scripting Interpreter' or detecting misuse of it is very important for your organization. By using the python script as explained in the 'Visualizing data' section of this post, you can find out in which table of MDE this data resides, or which event ids in Windows Security Logs relate to this data.

MDE

MITRE Layer:



Mapping query in Python:

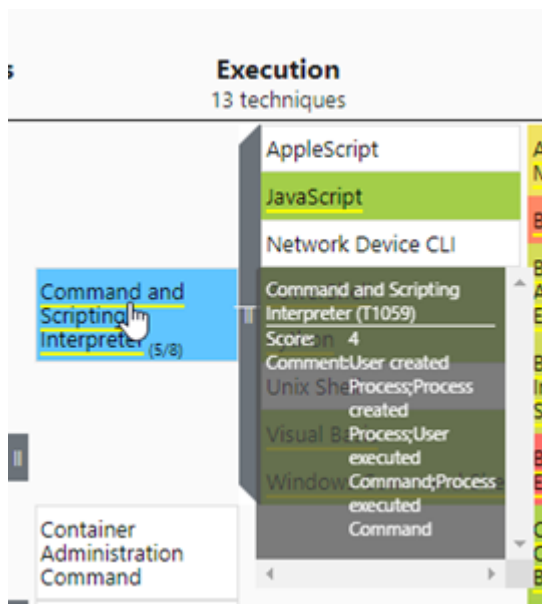
```
mapping[(mapping['log_source']=='Microsoft Defender for Endpoint')][(mapping['technique']
```

Output:

technique_id	is_subtechnique	technique	tactic	platform	data_source	data_component	relationship_id	name	source	relationship	target	event_id	event_name	event_p
9626	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	process	process metadata	REL-2022-0073	Process searched LDAP	process	searched	ldap	DeviceEvents	DeviceEvents	v
9630	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	process	process creation	REL-2022-0146	User created Process	user	created	process	DeviceProcessEvents	DeviceProcessEvents	v
9632	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	process	process creation	REL-2022-0153	Process created Thread	process	created	thread	DeviceEvents	DeviceEvents	v
9636	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	process	process creation	REL-2022-0175	Process created Process	process	created	process	DeviceProcessEvents	DeviceProcessEvents	v
9640	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	command	command execution	REL-2022-0018	User executed Command	user	executed	command	DeviceProcessEvents	DeviceProcessEvents	v
9645	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	command	command execution	REL-2022-0131	Process executed Command	process	executed	command	DeviceProcessEvents	DeviceProcessEvents	v
9648	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	script	script execution	REL-2022-0066	Process executed Script	process	executed	script	DeviceEvents	DeviceEvents	v
9649	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	script	script execution	REL-2022-0066	Process executed Script	process	executed	script	DeviceEvents	DeviceEvents	v
9650	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	script	script execution	REL-2022-0066	Process executed Script	process	executed	script	DeviceEvents	DeviceEvents	v
9652	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	module	module load	REL-2022-0014	User loaded Module	user	loaded	module	DeviceImageLoadEvents	DeviceImageLoadEvents	v

Windows Security Events

MITRE layer:



Mapping query in Python:

```
mapping[(mapping['log_source']=='Microsoft-Windows-Security-Auditing')][(mapping['t
```

Output:

technique_id	is_subtechnique	technique	tactic	platform	data_source	data_component	relationship_id	name	source	relationship	target	event_id	event_name	event_platform	audit_category
9627	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	process	process creation	REL-2022-0146	User created Process	user	created	process	4688	A new process has been created.	windows	Detailed Tracking
9633	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	process	process creation	REL-2022-0175	Process created Process	process	created	process	4688	A new process has been created.	windows	Detailed Tracking
9637	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	command	command execution	REL-2022-0018	User executed Command	user	executed	command	4688	A new process has been created.	windows	Detailed Tracking
9641	T1059	False	Command and Scripting Interpreter	[Linux, macOS, Windows, Network]	command	command execution	REL-2022-0131	Process executed Command	process	executed	command	4688	A new process has been created.	windows	Detailed Tracking

Conclusion, findings, and next steps

By following this blog post, you should have an understanding of how I was able to create MITRE mappings of the data coverage for both Microsoft Defender for Endpoints data and all or specific Microsoft Security Events using the OSSEM model.

Lessons learned

What we have learned during this post is that there are some overlaps of data in both MDE and Windows Security Events. This means that **enabling both MDE raw logs and Windows Security Events logs in Microsoft Sentinel might not be a good idea** without a proper reason to do so, since you will have **duplicate data**.

Another thing we learned is which **data source has the most mappings to a certain technique**. This might help in deciding which

data source you will be using in your Sentinel environment, considering the types of events you will find in the data sources.

Once you correlate a comparison layer (for example, MDE VS Windows Security Events) and your prioritization layer with techniques that are important to you, you will have a **better understanding of which data source to choose for the techniques that matter** to you. You can also pivot back to the MITRE layers of the data sources themselves to find which data types are logged in the comments section of the technique, and you can use the table or graph mapping in the python script to find which event ids or tables you need to ingest the data you want.

Another valuable insight you might learn is **which extra event ids you need to enable** if you for example choose to rely on MDE data and want to fill gaps with Microsoft Security Events. You can use your prioritization layer and python graph or table mapping to find the needed event ids.

What we didn't learn

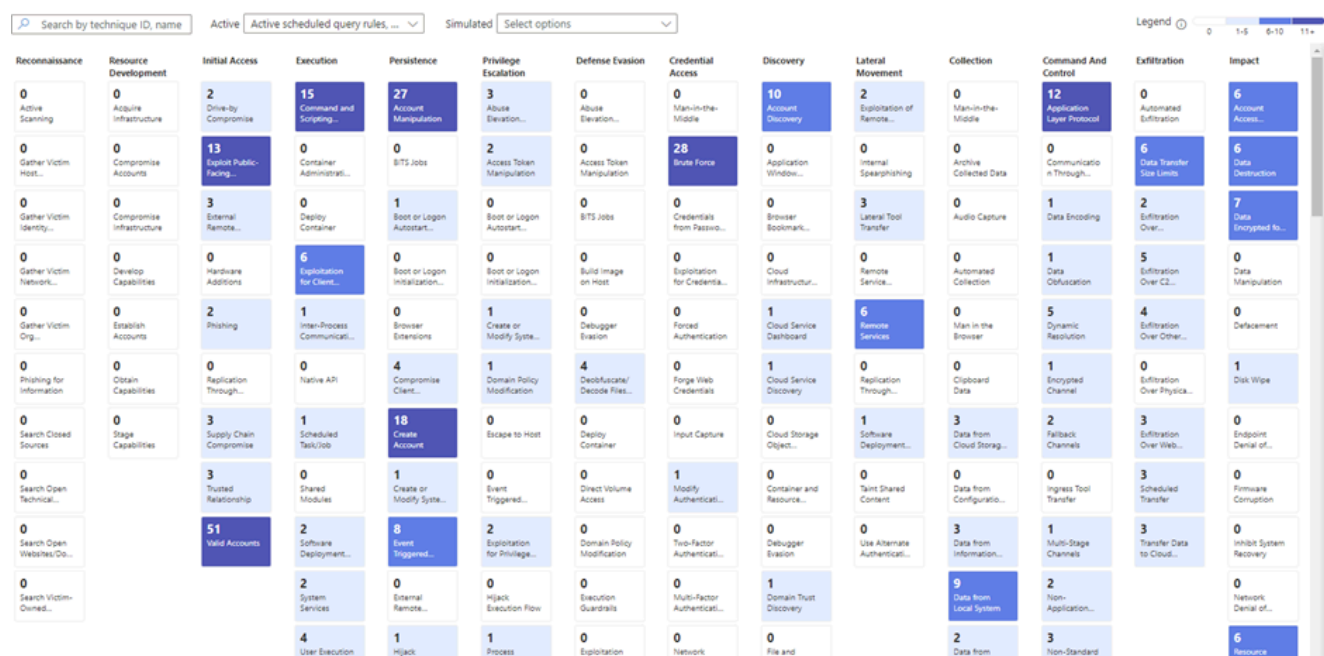
The most important one I want you to keep in mind is that we have **mapped the RAW data capabilities** of both data sources to the MITRE layer, which means we **did not map the available detections in Microsoft Sentinel** for each data source.

There might be **reasons other than data coverage to choose a certain data source**. Examples are the **cost price of data ingestion** and **detection coverage of the data source**. When you want to ingest MDE logs in Microsoft Sentinel, you are not able to choose for which devices you want to ingest the logs. This might lead to high costs when you for example only want to ingest MDE logs of servers but also have MDE deployed on client devices. When there are more analytic rules for Windows Security Events than MDE logs, the data coverage of MDE logs

might be less relevant if it were to be that MDE has better data coverage, but Windows Security Events data coverage is acceptable for you.

Next related projects

As mentioned before, there are other reasons to choose a certain data source. One of them is the detection coverage of the data source. In Microsoft Sentinel, there is a MITRE blade that shows you the MITRE coverage of your current active analytic rules and the template analytics rules.

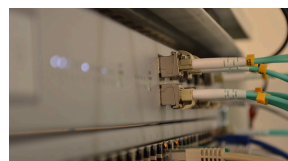
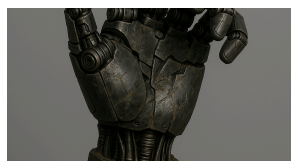
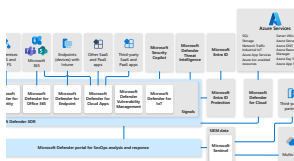


The thing I am missing in this blade is the possibility to filter on certain data connectors. To solve this issue, we are developing a script that is able to create the **MITRE ATT&CK coverage for the template rules of specific data connectors**. Once we have this, we will be able to create a much better decision on whether to use the MDE log in Sentinel, the Windows Security Events logs, or a combination of both.

If you are interested in the complete python code to create MITRE ATT&CK mappings based on the OSSEM model, let me know in the

comment section below! If there is enough interest, I might share the GitHub repository where you can find:

- A Jupyter notebook with all the examples and code to map OSSEM to MITRE layers
- The MITRE layers discussed in this blog posts
- MITRE layers for Minimal Windows Security events in Windows Security events that are used in current out-of-the-box analytic rules
- A script that checks if you are ingesting all of the Windows Security Events that are used in out-of-the-box or custom-created analytic rules



Transition from Microsoft Sentinel to Defender XDR - Practical challenges

Detecting non-privileged Windows Hello abuse

MDE Device Discovery - Improving the monitored network page

Introduction
Microsoft
announced on the...

Jul 4, 2025 12 min read

Introduction I
recently followed a
live session of Dirk...

Apr 26,
2025 16 min
read

Introduction This
blogpost is
probably the first ...

Mar 19,
2025 6 min
read

Hybrid Brothers © 2025

[Sign up](#) [Privacy policy](#)

Powered by Ghost