



11 min read

Microsoft Sentinel

Operationalizing MITRE ATT&CK to support Microsoft Sentinel deployments and detections



Robbe Van den Daele

Nov 22, 2022 • 11 min read

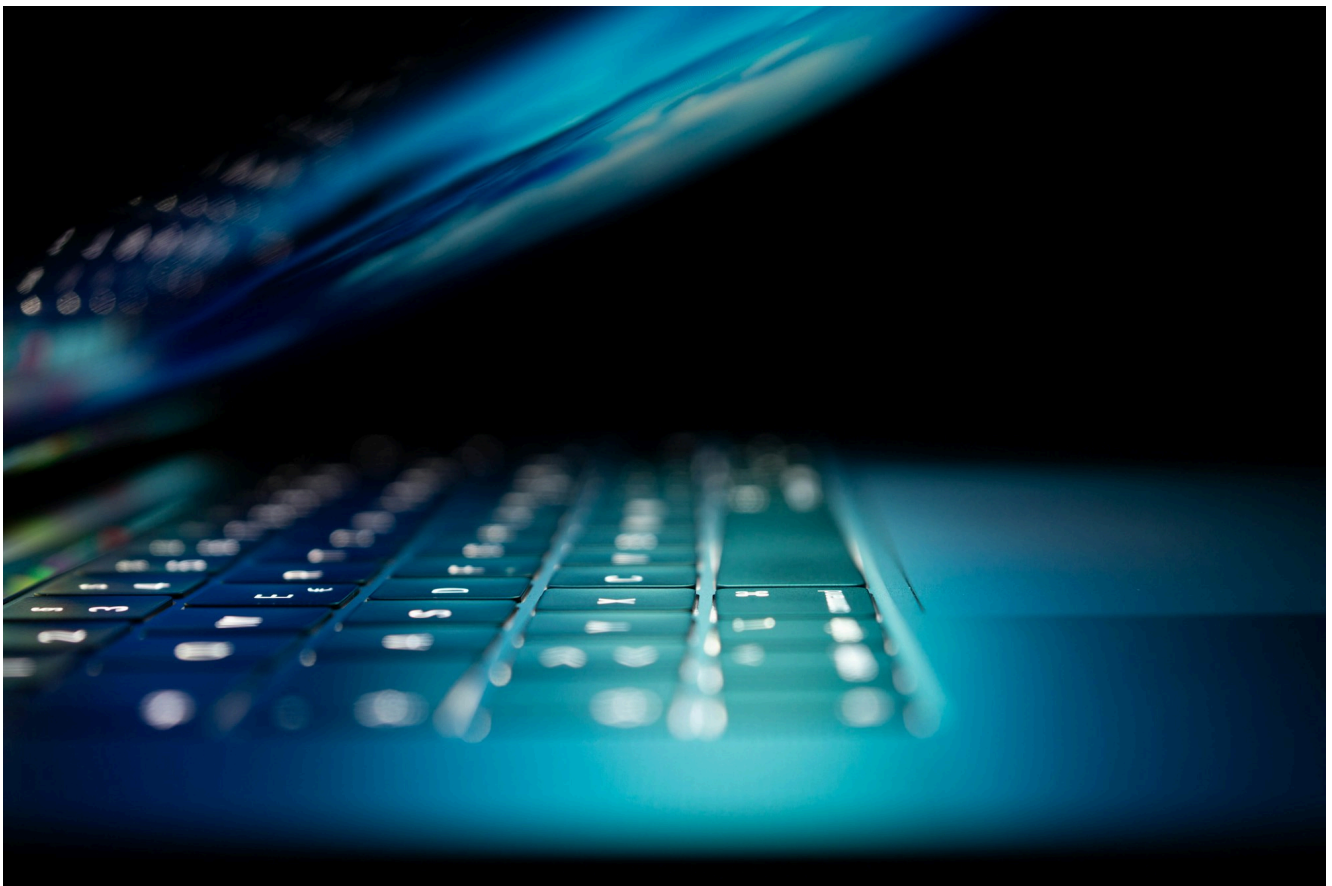


Photo by [Philipp Katzenberger](#) / [Unsplash](#)

Introduction

Why focusing on the right TTP's is important?

Focusing on the gaps in your detection mechanisms

Top 10 techniques calculator

Mapping your Top 10 techniques to the MITRE Matrix

Focussing on techniques common groups are using

Finding industry related attack groups

Creating mappings

Results

Merging the layers

Using the mappings in Sentinel

Cross mapping the MITRE blade in the Microsoft Sentinel portal with your own mappings

Conclusion

Introduction

Managing a SIEM can be a challenging task to do. When you insert too many log sources in your SIEM without enough filtering and finetuning, your SIEM can get very noisy in no time. An in-depth post about how to manage a SIEM will be available on this site at a later point in time, but one of the main things you start with is prioritizing which data sources are the most important in your SIEM.

Prioritization of your data sources can be based on how important the log source is for the company, the kind of data that is present in the log source, how natively the data source integrates with your SIEM, etc. Today we will be focussing on how you can prioritize your SIEM log sources based on Threat Informed defences. For this, we will be using the MITRE ATT&CK framework. Assuming you know what MITRE ATT&CK is, you will learn how to make Use Cases, how we can prioritize certain Techniques, and how you can check which data sources are needed for the detections you need the most.

Why focusing on the right TTP's is important?

When you use Microsoft Sentinel, one of your goals is probably to detect threats and advisory events that are happening in your environment. The real question is, what threats and advisory events do we need to detect? Is there a way to know what to focus on? And are they all the same for any organization? The answer to these questions lay in the MITRE ATT&CK framework.

When you look at one of the MITRE ATT&CK matrices, you will see the Tactics and Techniques that can be used during an attack by the attacker to accomplish their goal. Every technique in these matrices is an opportunity for you to detect advisory events to hopefully detect an ongoing attack, or an attack that may take place in the future. Although detecting all of the techniques would be great, it is not a realistic scenario. For example, an attack group will use certain tactics and techniques to attack their targets, which means that focusing on those techniques that are most being exploited is the most efficient way to create your detection mechanisms. Also, certain techniques or sub-techniques can only be used in certain environment. Using the 'Command and Scripting Interpreter' technique with an AppleScript is not affective when the attacker is targeting a Windows environment.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2.1)	Acquire Infrastructure (2.1)	Drive-by Compromise (2.1)	Command and Scripting Interpreter (2.1)	Account Manipulation (2.1)	Abuse Elevation Control Mechanism (2.1)	Abuse Elevation Control Mechanism (2.1)	Adversary-in-the-Middle (2.1)	Account Discovery (2.1)	Exploitation of Remote Services (2.1)	Adversary-in-the-Middle (2.1)	Application Layer Protocol (2.1)	Automated Exfiltration (2.1)	Account Access Removal (2.1)
Gather Victim Host Information (2.1)	Compromise Accounts (2.1)	Exploit Public-Facing Application (2.1)	Container Administration Command (2.1)	BITS Jobs (2.1)	Access Token Manipulation (2.1)	Access Token Manipulation (2.1)	Brute Force (2.1)	Application Window Discovery (2.1)	Internal Spearphishing (2.1)	Archive Collected Data (2.1)	Communication Through Removable Media (2.1)	Data Transfer Size Limits (2.1)	Data Destruction (2.1)
Gather Victim Identity Information (2.1)	Compromise Infrastructure (2.1)	External Remote Services (2.1)	Deploy Container (2.1)	Boot or Logon Autostart Execution (2.1)	Boot or Logon Autostart Execution (2.1)	Boot or Logon Autostart Execution (2.1)	Credentials from Password Stores (2.1)	Browser Bookmark Discovery (2.1)	Lateral Tool Transfer (2.1)	Audio Capture (2.1)	Automated Collection (2.1)	Exfiltration Over Alternative Protocol (2.1)	Data Encrypted for Impact (2.1)
Gather Victim Network Information (2.1)	Develop Capabilities (2.1)	Hardware Additions (2.1)	Exploitation for Client Execution (2.1)	Boot or Logon Initialization Scripts (2.1)	Boot or Logon Initialization Scripts (2.1)	Boot or Logon Initialization Scripts (2.1)	Exploitation for Credential Access (2.1)	Cloud Infrastructure Discovery (2.1)	Remote Service Session Hijacking (2.1)	Clipboard Data (2.1)	Data Encoding (2.1)	Exfiltration Over C2 Channel (2.1)	Data Manipulation (2.1)
Gather Victim Org Information (2.1)	Establish Accounts (2.1)	IT Shimming (2.1)	Inter-Process Communication (2.1)	Browser Extensions (2.1)	Create or Modify System Process (2.1)	Create or Modify System Process (2.1)	Deobfuscate/Decode Files or Information (2.1)	Cloud Service Dashboard (2.1)	Remote Services (2.1)	Browser Session Hijacking (2.1)	Data Obfuscation (2.1)	Exfiltration Over Other Network Medium (2.1)	Defacement (2.1)
Phishing for Information (2.1)	Obtain Capabilities (2.1)	Replication Through Removable Media (2.1)	Native API (2.1)	Compromise Client Software Binary (2.1)	Domain Policy Modification (2.1)	Domain Policy Modification (2.1)	Forced Authentication (2.1)	Cloud Service Discovery (2.1)	Replication Through Removable Media (2.1)	Clipboard Data (2.1)	Dynamic Resolution (2.1)	Exfiltration Over Physical Medium (2.1)	Disk Wipe (2.1)
Search Closed Sources (2.1)	Stage Capabilities (2.1)	Supply Chain Compromise (2.1)	Scheduled Task/Job (2.1)	Create Account (2.1)	Domain Policy Modification (2.1)	Domain Policy Modification (2.1)	Input Capture (2.1)	Container and Resource Discovery (2.1)	Replication Through Removable Media (2.1)	Data from Cloud Storage Object (2.1)	Encrypted Channel (2.1)	Exfiltration Over Other Network Medium (2.1)	Endpoint Denial of Service (2.1)
Search Open Technical Databases (2.1)	Trusted Relationship (2.1)	Trusted Relationship (2.1)	Software Deployment Tools (2.1)	Event Triggered Execution (2.1)	Event Triggered Execution (2.1)	Event Triggered Execution (2.1)	Modify Authentication Process (2.1)	Debugger Evasion (2.1)	Software Deployment Tools (2.1)	Data from Configuration Repository (2.1)	Fallback Channels (2.1)	Exfiltration Over Other Network Medium (2.1)	Firmware Corruption (2.1)
Search Open Websites/Domains (2.1)	Valid Accounts (2.1)	User Execution (2.1)	User Execution (2.1)	External Remote Services (2.1)	External Remote Services (2.1)	External Remote Services (2.1)	Multi-Factor Authentication Interception (2.1)	Domain Trust Discovery (2.1)	Software Deployment Tools (2.1)	Data from Local System (2.1)	Ingress Tool Transfer (2.1)	Exfiltration Over Other Network Medium (2.1)	Inhibit System Recovery (2.1)
Search Victim-Owned Websites (2.1)			Windows Management Instrumentation (2.1)	Windows Management Instrumentation (2.1)	Windows Management Instrumentation (2.1)	Windows Management Instrumentation (2.1)	Multi-Factor Authentication Request Generation (2.1)	File and Directory Permissions Modification (2.1)	Software Deployment Tools (2.1)	Data from Network Shared Drive (2.1)	Multi-Stage Channels (2.1)	Exfiltration Over Other Network Medium (2.1)	Network Denial of Service (2.1)
							Network Sniffing (2.1)	Hide Artifacts (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)	Non-Application Layer Protocol (2.1)	Exfiltration Over Other Network Medium (2.1)	Resource Hijacking (2.1)
							OS Credential Dumping (2.1)	Hijack Execution Flow (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)	Non-Standard Port (2.1)	Exfiltration Over Other Network Medium (2.1)	Service Stop (2.1)
							Password Policy Discovery (2.1)	Process Injection (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)	Protocol Tunneling (2.1)	Exfiltration Over Other Network Medium (2.1)	System Shutdown/Reboot (2.1)
							Steal Application Access Token (2.1)	Scheduled Task/Job (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)	Proxy (2.1)	Exfiltration Over Other Network Medium (2.1)	
							Steal or Forge Kerberos Tickets (2.1)	Indicator Removal on Host (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)	Remote Access Software (2.1)	Exfiltration Over Other Network Medium (2.1)	
							Steal Web Session Cookie (2.1)	Valid Accounts (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)	Traffic Signaling (2.1)	Exfiltration Over Other Network Medium (2.1)	
								Indirect Command Execution (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)	Web Service (2.1)	Exfiltration Over Other Network Medium (2.1)	
								Masquerading (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)		Exfiltration Over Other Network Medium (2.1)	
								Modify Authentication Process (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)		Exfiltration Over Other Network Medium (2.1)	
								Modify Cloud Compute Task/Job (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)		Exfiltration Over Other Network Medium (2.1)	
								Modify Cloud Compute Task/Job (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)		Exfiltration Over Other Network Medium (2.1)	
								Query Registry (2.1)	Software Deployment Tools (2.1)	Data from Removable Media (2.1)		Exfiltration Over Other Network Medium (2.1)	

In this blog post, we will be talking about two ways that can help you focus on the techniques that matters the most. These two ways are:

- Focusing on the techniques that are currently not well detected by your Microsoft Sentinel deployment (we will call them ‘gaps’ in your detection mechanisms) and are known to be most exploited.
- Focusing on the techniques that your enemies are known to be using.

Focusing on the gaps in your detection mechanisms

Top 10 techniques calculator

The MITRE Engenuity – Center for Threat Informed Defense created a great tool that helps you prioritize the techniques and sub-techniques that matters the most, called the TOP ATT&CK TECHNIQUES. These top 10 techniques are known to be exploited frequently, and reflect on your environment when you use the correct filters. The calculator can be found by using this link: <https://top-attack-techniques.mitre-engenuity.org/calculator>.

Filters

NIST 800-53 Controls ▾

CIS Security Controls ▾

Detection Analytics ▾

Operating Systems ▾

Generate Results

Network Monitoring Components

None

Low

Medium

High

You have no network monitoring.

Process Monitoring Components

None

Low

Medium

High

You have no process monitoring.

File Monitoring Components

None

Low

Medium

High

You have no file monitoring.

Cloud Monitoring Components

None

Low

Medium

High

You have no cloud monitoring.

Hardware Monitoring Components

None

Low

Medium

High

You have no hardware monitoring.

Your Top 10 Techniques

Please make selections on the left and hit the calculate button to see results.

Download All Top Techniques 🔽

Setting up the filters

When you visit the calculator, you will see a list of filters that you can set on the left side of your screen. First is the NIST 800-53 Controls filter where you can select which NIST controls you want to focus the most on. If you want to know more about the controls that exists and the NIST 800-53 Special Publication, I highly recommend to start reading the [Wikipedia page](#). For this post, we will select 'All NIST Controls'.



The second filter is the CIS Security Controls filter. Just like the NIST 800-53 filter, you can set this to only see the techniques related to the selected controls. We will use the 'All CIS Controls' filter for this example. If you want to know more about the CIS controls, you can take a look at [this website](#).

Filters

NIST 800-53 Controls

CIS Security Controls

☒ All CIS Controls

☒ 1.1

☒ 1.2

☒ 1.4

☒ 2.1

☒ 2.2

☒ 2.3

☒ 2.4

☒ 2.5

☒ 2.6

☒ 2.7

☒ 3.1

☒ 3.10

☒ 3.11

☒ 3.12

☒ 3.2

☒ 3.3

☒ 3.4

☒ 3.6

☒ 4.10

Detection Analytics

Operating Systems

In the third filter, you can select which detection rules you want to focus on based on the SIEM solution you are using. For this example, I will leave this filter blank.

Filters

NIST 800-53 Controls

▼

CIS Security Controls

▼

Detection Analytics

▲

☐ CAR

☐ Elastic Search SIEM

☐ Sigma

☐ Splunk

Operating Systems

▼

In the last filter, you can choose which technologies you are focusing on. I will choose the following settings:

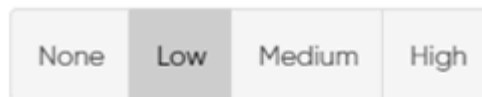
Filters

NIST 800-53 Controls	▼
CIS Security Controls	▼
Detection Analytics	▼
Operating Systems ^	
<input checked="" type="checkbox"/> Azure AD	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Google Workspace	
<input checked="" type="checkbox"/> IaaS	
<input checked="" type="checkbox"/> Linux	
<input checked="" type="checkbox"/> Network	
<input type="checkbox"/> Office 365	
<input type="checkbox"/> PRE	
<input checked="" type="checkbox"/> SaaS	
<input checked="" type="checkbox"/> Windows	
<input type="checkbox"/> macOS	

Choosing the monitoring components

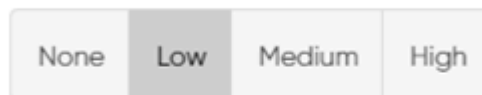
Now that the filters are configured, we will have to choose the monitoring components. Using these buttons, you can set how good your current monitoring setup is. Let's say you have already a lot of Cloud Monitoring detection in your SIEM setup, you can set the Cloud Monitoring Components filter on High. If you want to focus more on network monitoring in your SIEM, you can set the Network Monitoring Components to None or Low. By doing this you can prioritize techniques that are related to network monitoring more than techniques that are related to cloud monitoring. For this example, I used the following filter:

Network Monitoring Components



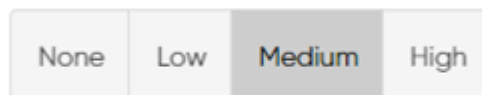
You have low network monitoring.

Process Monitoring Components



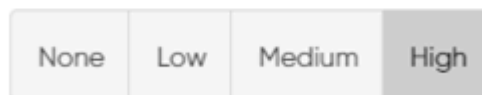
You have low process monitoring.

File Monitoring Components



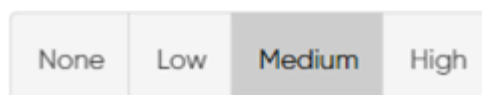
You have medium file monitoring.

Cloud Monitoring Components



You have high cloud monitoring.

Hardware Monitoring Components



You have medium hardware monitoring.

Results

If you set everything up, you can click on the 'Generate Results' button to get the top 10 most important techniques you will have to focus on. You

will see that every technique has a description, mitigation, and detection section so you can learn more about the technique. Some techniques will also have a sub-technique section, which will be filtered based on the filters you set up in the beginning.

The screenshot displays the MITRE ATT&CK Navigator interface. On the left, a 'Filters' panel includes dropdowns for 'NIST 800-53 Controls', 'CIS Security Controls', 'Detection Analytics', and 'Operating Systems', along with a 'Generate Results' button. The main area shows five monitoring components with their respective levels:

- Network Monitoring Components:** None, Low (selected), Medium, High. Status: *You have low network monitoring.*
- Process Monitoring Components:** None, Low, Medium, High (selected). Status: *You have low process monitoring.*
- File Monitoring Components:** None, Low, Medium, High (selected). Status: *You have medium file monitoring.*
- Cloud Monitoring Components:** None, Low, Medium, High (selected). Status: *You have high cloud monitoring.*
- Hardware Monitoring Components:** None, Low, Medium, High (selected). Status: *You have medium hardware monitoring.*

On the right, the 'Your Top 10 Techniques' panel lists the following techniques:

1. T1059 - Command and Scripting Interpreter
2. T1047 - Windows Management Instrumentation
3. T1053 - Scheduled Task/Job
4. T1562 - Impair Defenses
5. T1543 - Create or Modify System Process
6. T1574 - Hijack Execution Flow
7. T1021 - Remote Services
8. T1003 - OS Credential Dumping
9. T1055 - Process Injection
10. T1548 - Abuse Elevation Control Mechanism

The details for the first technique, T1059 - Command and Scripting Interpreter, are shown on the right, including a description, subtechniques (e.g., T1059.001 - Command and Scripting Interpreter: PowerShell), and mitigations (e.g., M1021 - Restrict Web-Based Content).

Mapping your Top 10 techniques to the MITRE Matrix

Now that you generated the 10 most important techniques to focus on, it is time to map these in one of the MITRE ATT&CK matrices that fits your organisation. When you go to the [MITRE ATT&CK Navigator](#), you can create a new layer where you can map your techniques to. Based on your environment you can select the Enterprise, Mobile, or ICS matrix. In most cases the enterprise matrix will be used, so for this post we will choose enterprise:

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

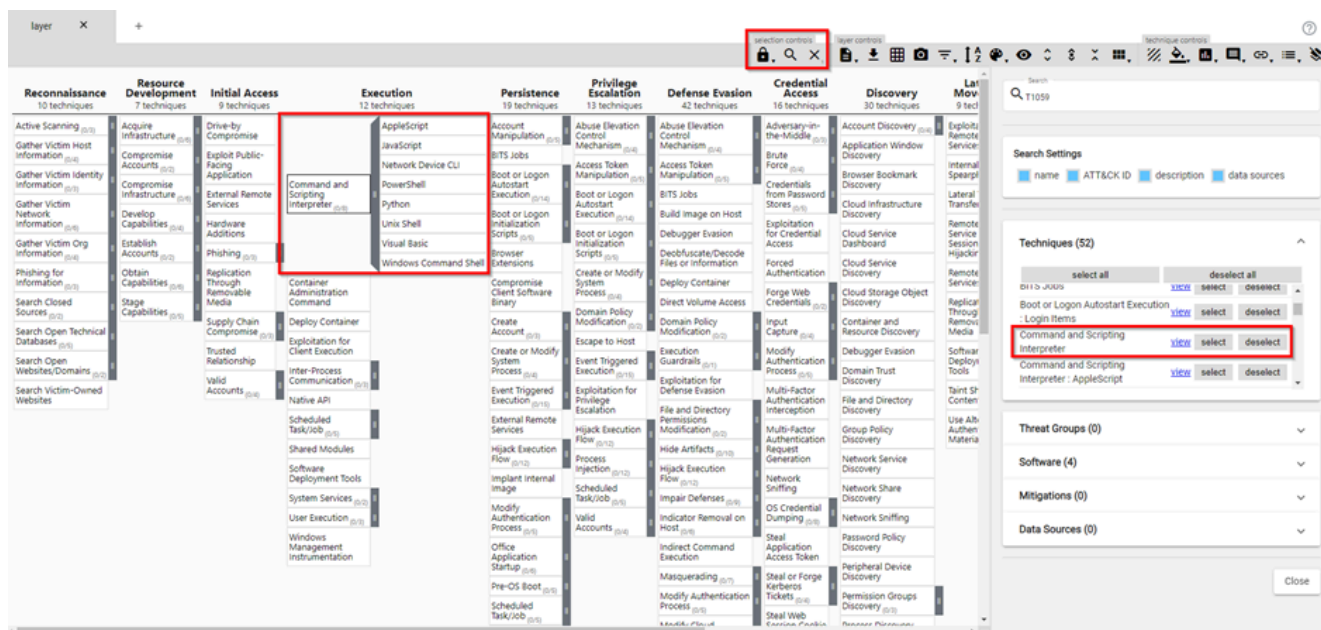
[help](#) [changelog](#) [theme ▾](#)

Create New Layer	Create a new empty layer	^
Enterprise	Mobile	ICS
More Options ▾		
Open Existing Layer	Load a layer from your computer or a URL	▾
Create Layer from other layers	Choose layers to inherit properties from	▾
Create Customized Navigator	Create a hyperlink to a customized ATT&CK Navigator	▾

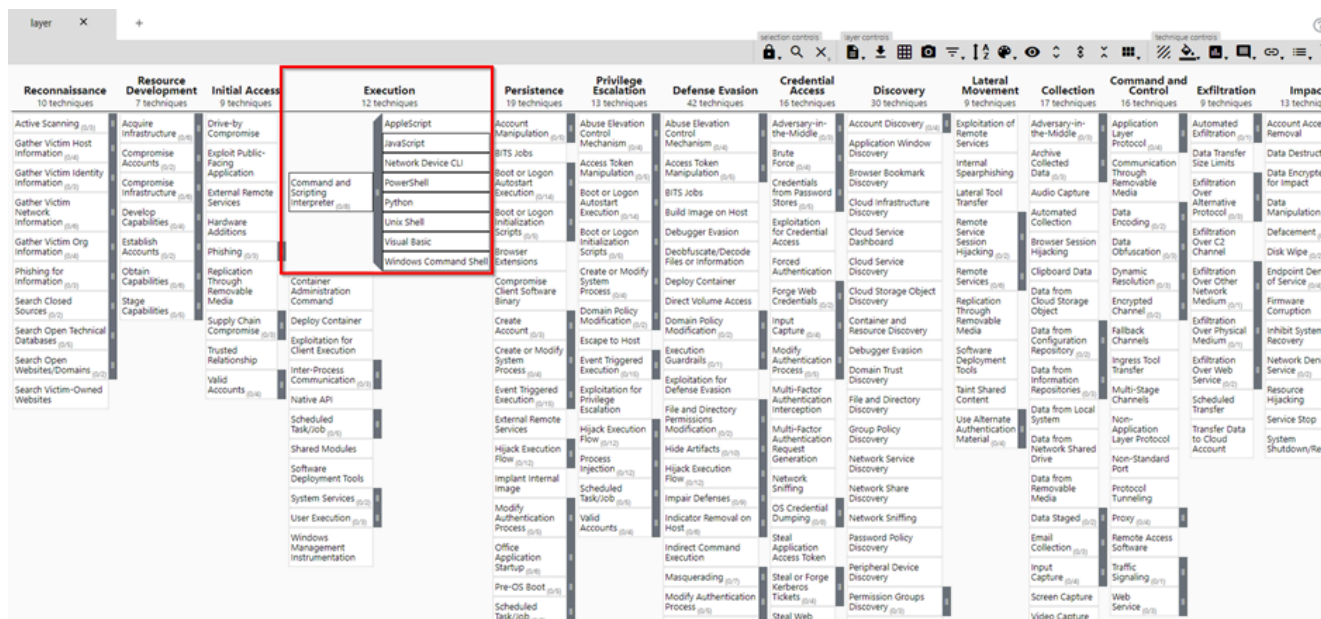
We will not discuss all the capabilities the MITRE ATT&CK Navigator has to offer, since this will lead us too far from the purpose of this blog post. If you want to know everything about the MITRE ATT&CK Navigator, I highly recommend following the free courses on [ATTACKIQ!](#)

Selecting relevant techniques and sub-techniques

When you click on the search glass in the navigator, you will be able to search for the techniques you generated in the Top 10 Techniques calculator. When a certain technique has sub-techniques, you can also view these by clicking on the grey bar at the right of the technique:

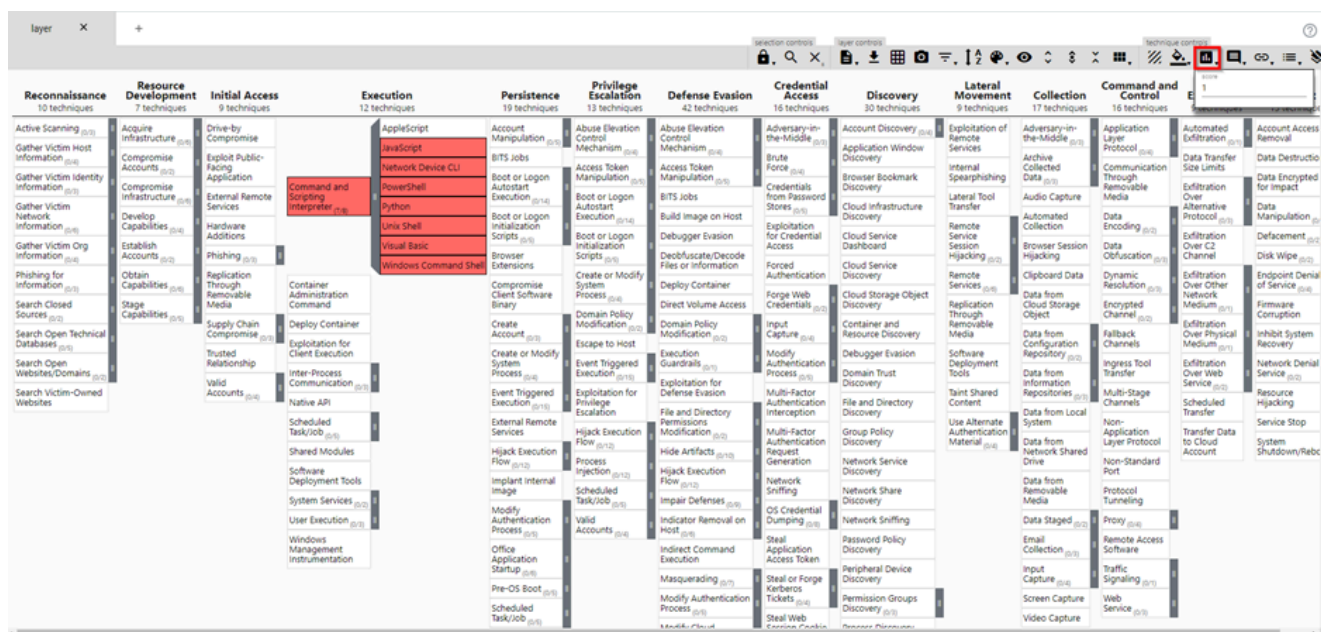


In our example, technique T1059 was our number 1 technique to look out for in the Top 10 Techniques calculator. Based on the filters we set, only these sub-techniques seemed to be important to us: T1059.001, T1059.003, T1059.004, T1059.005, T1059.006, T1059.007, T1059.008. Knowing this, we can select this technique in the MITRE ATT&CK Navigator, along with the sub-techniques:



Adding scores

Now that we have a technique and the relevant sub-techniques selected, we can add a score so these will get color. You can add a score by clicking the score button at the top right of the navigator. We will start with setting a score of one:



Results

If we repeat this process for all techniques and sub-techniques that were generated by the Top 10 calculator, we will have a layer like this:

By using this method, you will get a graphical overview of which techniques in the complete possible attack chain you will have to focus the most on. Even better, when you **right click on a technique and click on view technique**, you will be redirected to the **attack.mitre.org** website where you can view all the details about the technique and sub-techniques such as, descriptions, groups that are using this technique, mitigations, detections, and references!

Mitre | ATT&CK

- Matrices
- Tactics
- Techniques
- Data Sources
- Mitigations
- Groups
- Software
- Resources
- Blog
- Contribute
- Search

TECHNIQUES

Command and Scripting Interpreter

- PowerShell
- AppleScript
- Windows Command Shell
- Unix Shell
- Visual Basic
- Python
- JavaScript
- Network Device CLI
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation
- Persistence
- Privilege Escalation

M1038	Execution Prevention	Use application control where appropriate.
M1026	Privileged Account Management	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration. ^[46]
M1021	Restrict Web-Based Content	Script blocking extensions can help prevent the execution of scripts and HTA files that may commonly be used during the exploitation process. For malicious code served up through ads, adblockers can help prevent that code from executing in the first place.

Detection

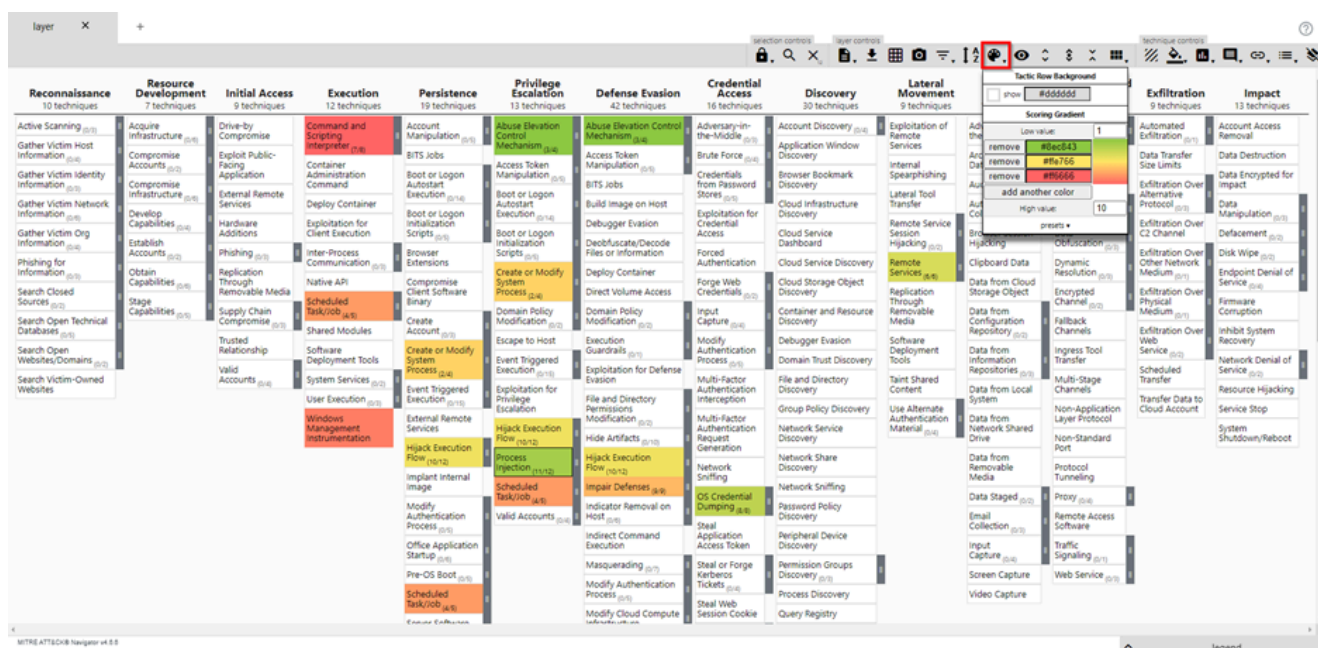
ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information Discovery, Collection, or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script. Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used.
DS0011	Module	Module Load	Monitor for events associated with scripting execution, such as the loading of modules associated with scripting languages (ex: JScript.dll or vbscript.dll).
DS0009	Process	Process Creation	Monitor log files for process execution through command-line and scripting activities. This information can be useful in gaining additional insight to adversaries' actions through how they use native processes or custom tools. Also monitor for loading of modules associated with specific languages.
		Process Metadata	Monitor contextual data about a running process, which may include information such as environment variables, image name, user/owner, or other information that may reveal abuse of system features. For example, consider monitoring for Windows event ID (EID) 400, which shows the version of PowerShell executing in the <code>\$scriptversion</code> field (which may also be relevant to detecting a potential Downgrade Attack) as well as if PowerShell is running locally or remotely in the <code>\$scriptfile</code> field. Furthermore, EID 400 may indicate the start time and EID 403 indicates the end time of a PowerShell session. ^[47]
DS0012	Script	Script Execution	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

Now that you have all of this information, you can explore the techniques that seemed to be important for you, and start checking which detections you can setup in Microsoft Sentinel and which data sources you will need for those detections.

16/27

You can change the colors by using the Color Setup button:

[illegible]



Focussing on techniques common groups are using

Besides focussing on the gaps in your detection systems, it is also interesting to focus on TTP's that attack groups are using to infiltrate in companies that match your industry. By doing this, detections can be setup against a real-world scenario of an attack.

Finding industry related attack groups

You can find industry related attack groups by simply going to the [MITRE ATT&CK website](https://mitre-attack.com/) and searching for the industry you work in. Let's say your company is active in telecommunications, by going to the search box in the top right corner and typing telecommunications, you will get a couple of attack groups that are known to exploit telecommunication companies:

Deep Panda, Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine, Group G0009

Deep Panda Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. [1] The intrusion into healthcare company Anthem has been attributed to Deep Panda. [2] This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. [3] Deep Panda ...

HEXANE, Lyceum, Slamesekitten, Spirlin, Group G1001

HEXANE HEXANE is a cyber espionage threat group that has targeted oil & gas, telecommunications, aviation, and internet service provider organizations since at least 2017. Targeted companies have been located in the Middle East and Africa, including Israel, Saudi Arabia, Kuwait, Moroc...

Earth Lusca, TAG-22, Group G1006

... France, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations, telecommunications companies, religious movements banned in China, and cryptocurrency trading platforms; security researchers assess some Earth Lusca operations may be financially motivated.[1] Earth Lusca ha...

Aquatic Panda, Group G0143

... threat group with a dual mission of intelligence collection and industrial espionage. Active since at least May 2020, Aquatic Panda has primarily targeted entities in the telecommunications, technology, and government sectors.[1] ID: G0143 Contributors: NST Assure Research Team, NetSentries Technologies; Pooja Natarajan, NEC Corporation India; Hiroki Nagahama, NEC Corporation...

OilRig, COBALT GYPSY, IRN2, APT34, Helix Kitten, Group G0049

... targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on beh...

For this post, we will be using OilRig as an example to create mappings.

Creating mappings

When you go to a group page in MITRE ATT&CK, you will find the ‘ATT&CK Navigators Layers’ button below the associated group descriptions. Mapping the techniques this group is using is just as simple as clicking this button and viewing the navigator:

OilRig

OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.^{[1][2][3][4][5][6][7]}

ID: G0049

① Associated Groups: COBALT GYPSY, IRN2, APT34, Helix Kitten

Contributors: Robert Falcone; Bryan Lee; Dragos Threat Intelligence

Version: 3.0

Created: 14 December 2017

Last Modified: 02 June 2022

[Version Permalink](#)

Associated Group Descriptions

Name	Description
COBALT GYPSY	[8]
IRN2	[9]
APT34	This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity. [7] [6][10]
Helix Kitten	[7][9]

Techniques Used

ATT&CK® Navigator Layers ▾

Domain	ID	Name	Use
--------	----	------	-----

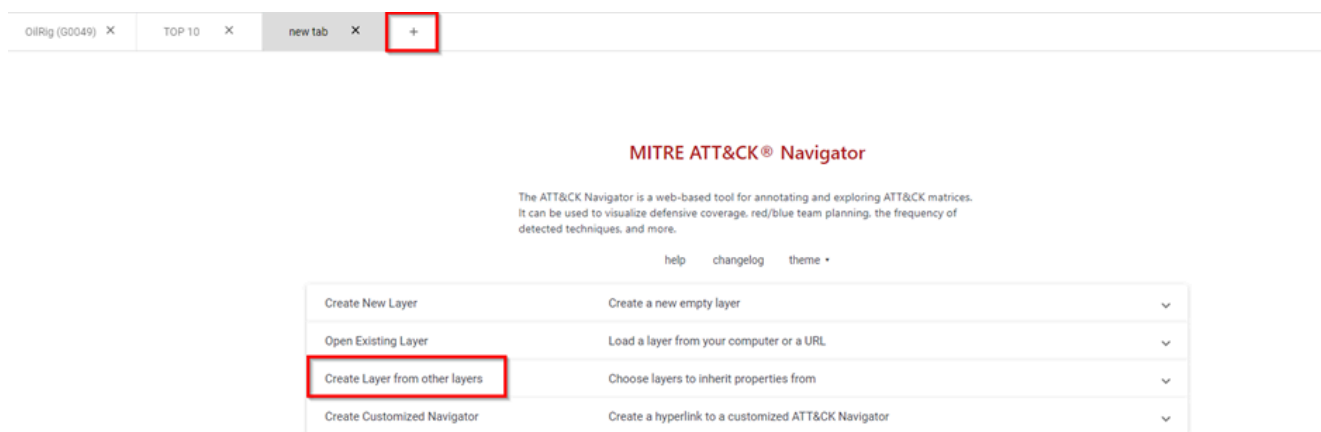
The image shows the MITRE ATT&CK Navigator v4.7.1 interface. It displays a grid of attack techniques organized into columns representing different stages of an attack: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. Each technique is listed with its name, a score (e.g., 0.7, 1.0, 1.5), and a color-coded background. Some techniques have links to other groups that use the same technique, indicated by a small icon. The interface includes a search bar at the top and a legend at the bottom right.

Results

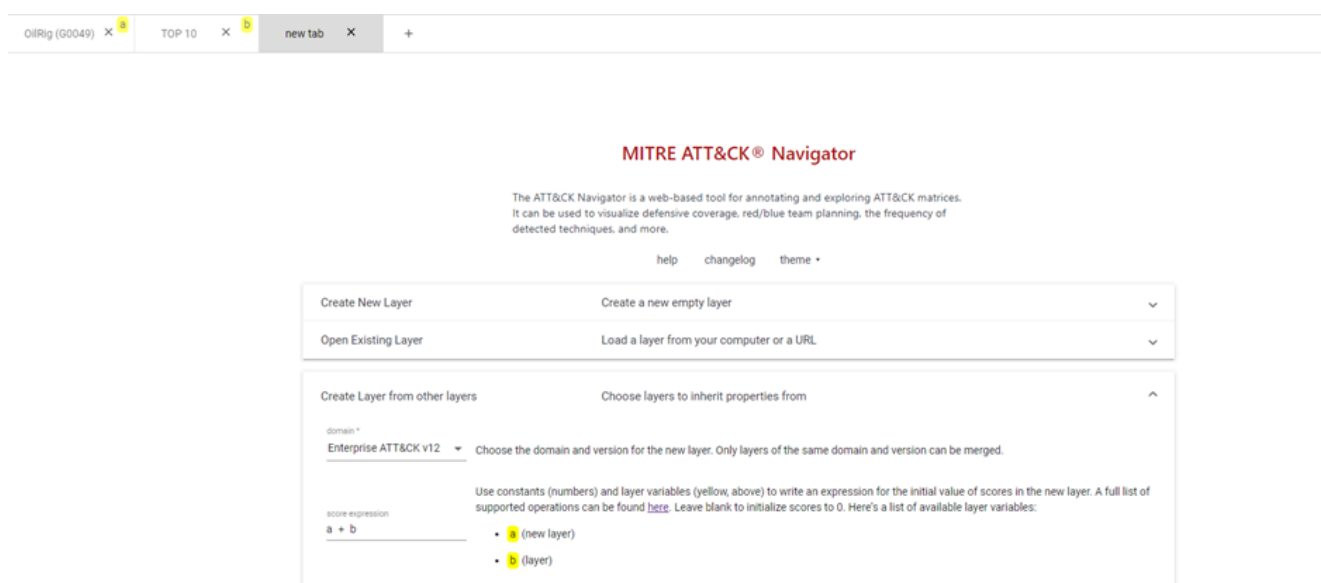
Note that all related techniques and sub-techniques have a score assigned and are given a colour. Most of the techniques also have extra comments with links to other groups that are using the same techniques.

Merging the layers

Create a new layer by clicking on the Add icon, and go to the ‘Create layers from other layers’ tab:



Here you will need to choose a MITRE domain (we take the latest Enterprise domain) and an expression to merge the layers. These expressions are used with the scores you added to certain techniques in your layers. When you choose an expression like $a + b$, the new layer will add the scores of the techniques in layer a to the scores of the techniques in layer b. All the possible expression can be found on [this page](#). For this example, we use the simple $a + b$ expression.



Once you click on the create button, the new layer will be created for you.

Using the mappings in Sentinel

23/27

The screenshot displays the MITRE ATT&CK Navigator v4.5.0 interface. It features a sidebar on the left with a search bar and a list of techniques. The main area is a grid of technique cards, each representing a specific attack technique. The cards are organized into columns based on the MITRE ATT&CK framework stages: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. A technique card titled 'Use Technique' is highlighted in the Persistence stage. The interface includes various navigation and search tools at the top.

When you scroll down in the technique page, you will find a table of detections you can create to detect this technique. You get the Data Source and Data Component you need to check, along with tips on what things to look out for in the Detects column.

Detection

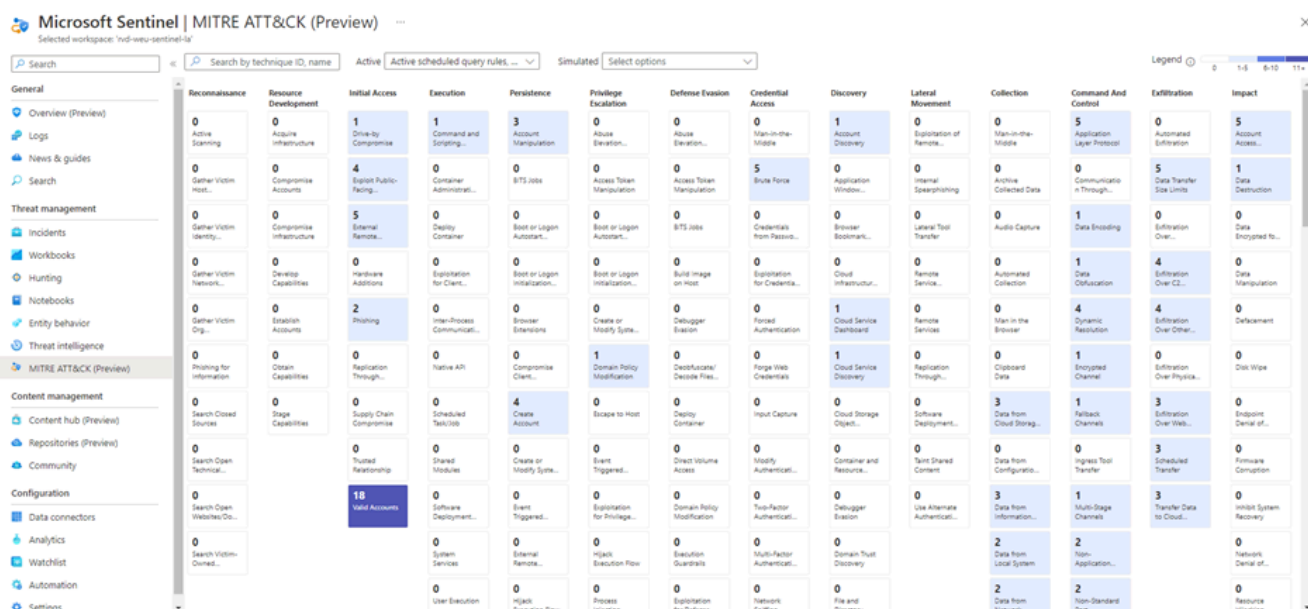
ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information Discovery, Collection, or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script. Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used.
DS0011	Module	Module Load	Monitor for events associated with scripting execution, such as the loading of modules associated with scripting languages (ex: JScript.dll or vbscript.dll).
DS0009	Process	Process Creation	Monitor log files for process execution through command-line and scripting activities. This information can be useful in gaining additional insight to adversaries' actions through how they use native processes or custom tools. Also monitor for loading of modules associated with specific languages.
		Process Metadata	Monitor contextual data about a running process, which may include information such as environment variables, image name, user/owner, or other information that may reveal abuse of system features. For example, consider monitoring for Windows Event ID (EID) 400, which shows the version of PowerShell executing in the <code>EngineVersion</code> field (which may also be relevant to detecting a potential Downgrade Attack) as well as if PowerShell is running locally or remotely in the <code>HostName</code> field. Furthermore, EID 400 may indicate the start time and EID 403 indicates the end time of a PowerShell session. ^[48]
DS0012	Script	Script Execution	Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

In this stage, you will have to figure out which Microsoft Sentinel data sources are equal to the MITRE ATT&CK data sources. For example, network traffic logs can be found in the Fortigate, Palo Alto, Baracuda, etc data sources in Microsoft Sentinel. Whereas process logs can be ingested

using the log analytics or azure monitoring agent. Once you figured this out, you will need to create analytic rules based on the tips you find in the Detects column.

Cross mapping the MITRE blade in the Microsoft Sentinel portal with your own mappings

Microsoft Sentinel has a MITRE ATT&CK blade present, where you can see for which techniques you have coverage in Microsoft Sentinel. This helps a lot when you want to check whether certain techniques you find to be important are implemented in your Sentinel environment.

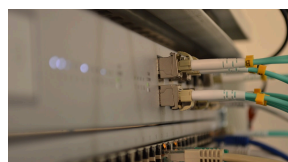
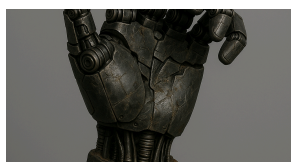
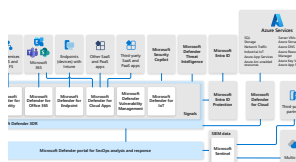


The hard part is correlating this layer to your MITRE ATT&CK Navigator layers, since there is no export feature available in the portal. Another problem is that this layer is aligned with the MITRE ATT&CK framework version 9, which is a version that is released on April 2021. Since most of

the organizations use the latest version (currently version 12), correlating these can get pretty hard and will involve some manual work.

Conclusion

In this post you mainly learned how you can prioritize certain data sources in Microsoft Sentinel using the MITRE ATT&CK framework. We did not talk about how to actually implement these in Microsoft Sentinel in depth, since it is very environment specific. We are currently investigating other tools that may help to implement these in Sentinel and are planning to create some new tools our own. **Once we have more information about these tools, we will create a new post explaining how to use them to implement the threat informed use cases you created in Microsoft Sentinel more easily.**



**Transition
from
Microsoft
Sentinel to
Defender
XDR -**

**Detecting
non-
privileged
Windows
Hello
abuse**

**MDE
Device
Discovery -
Improving
the
monitored**

Practical challenges

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

network page

Introduction This
blogpost is
probably the first ...

Mar 19, 2025 6 min read

Hybrid Brothers © 2025

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

Powered by Ghost