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

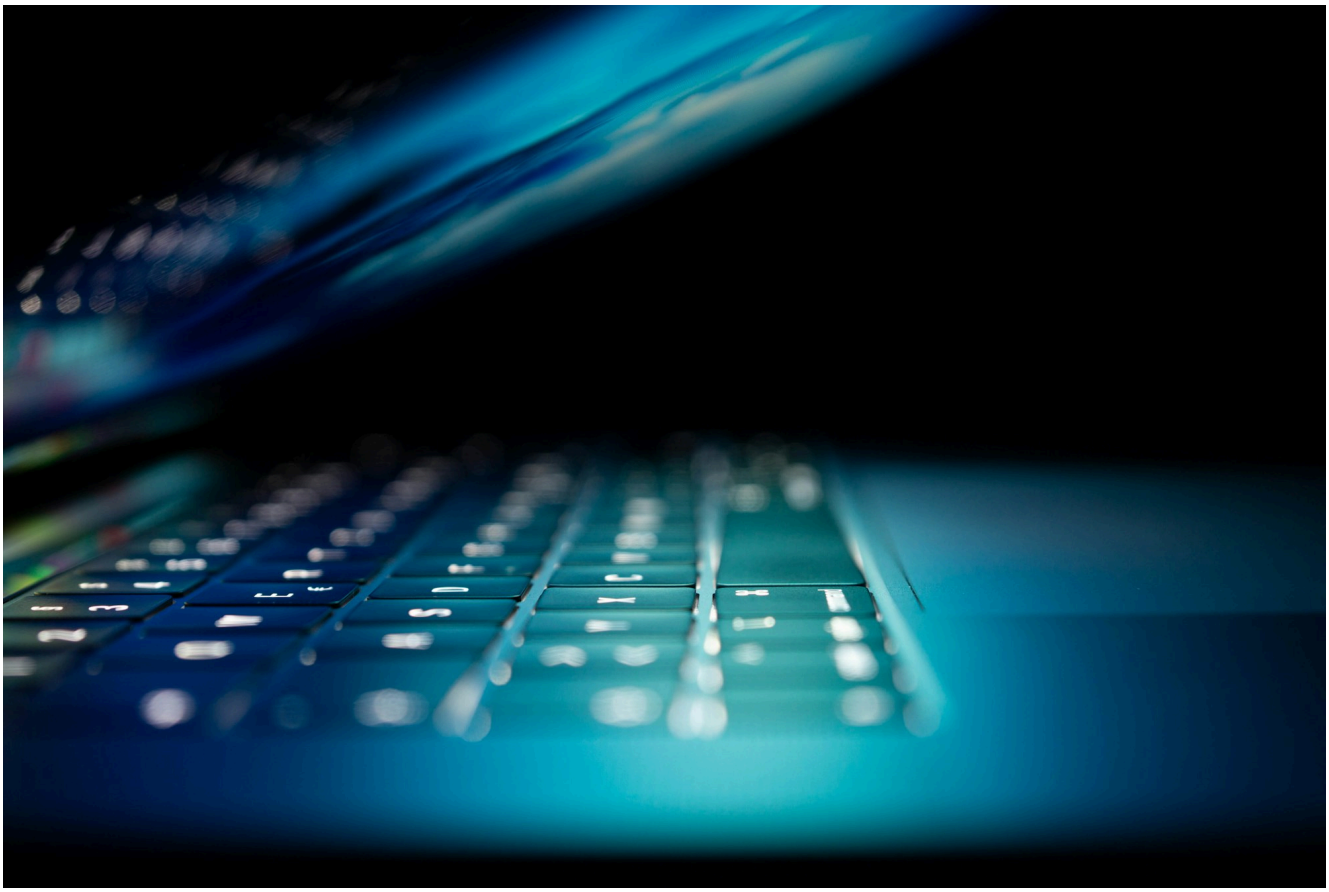


Photo by Philipp Katzenberger / Unsplash

Introduction

Why focusing on the right TTP's is important?

Focusing on the gaps in your detection mechanisms

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 known 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.

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:

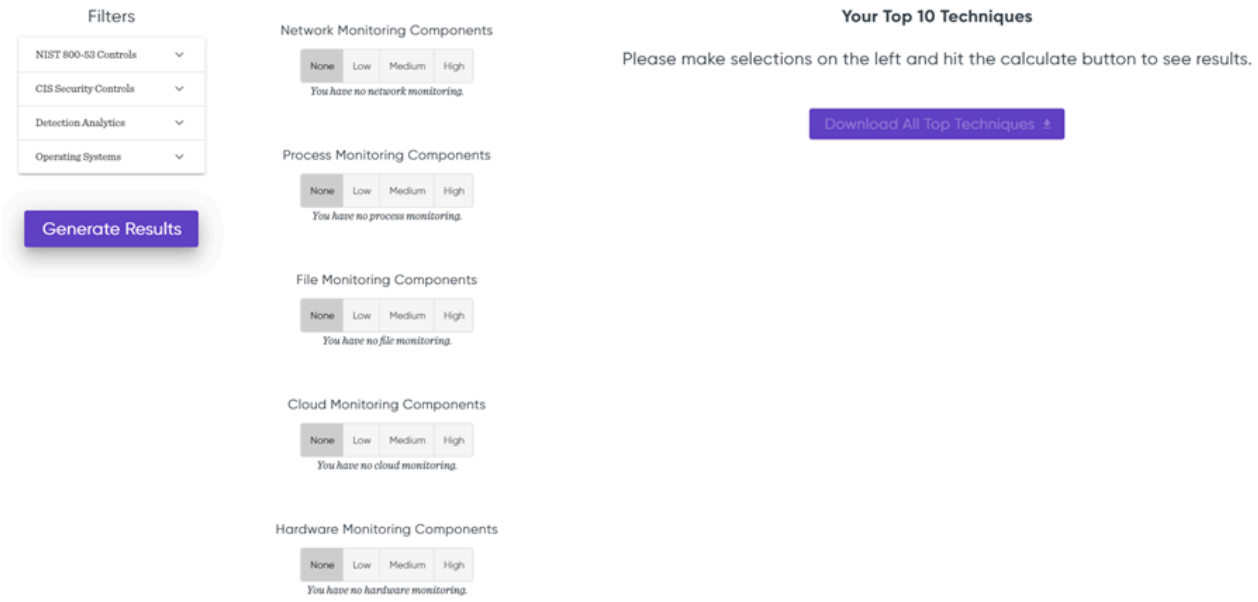
• Focusing on the techniques that are currently not well detected by your Microsoft Sentinel deployment (we will call them ‘gaps’ in your detection mechanisms) and are known to be most exploited.

• Focusing on the techniques that your enemies are known to be using.

Focusing on the gaps in your detection mechanisms

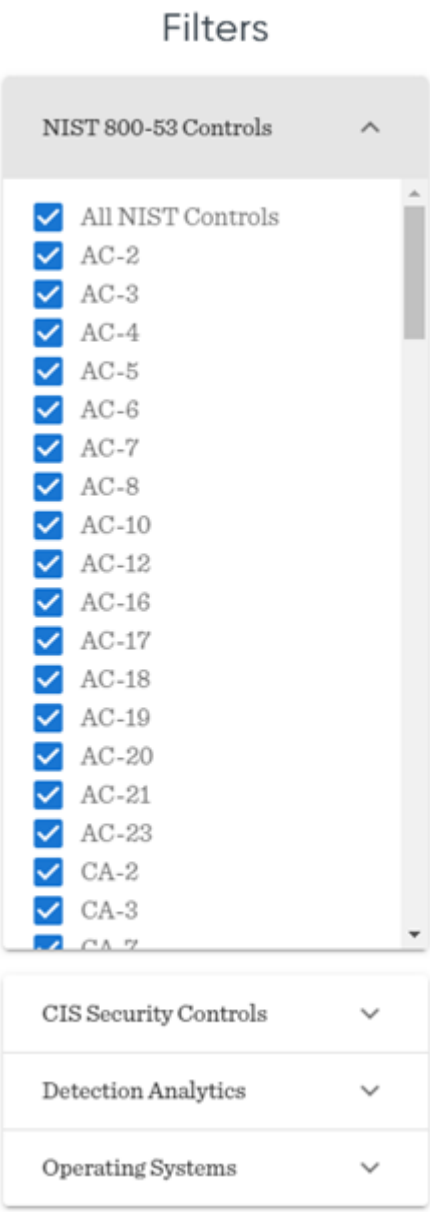
Top 10 techniques calculator

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.

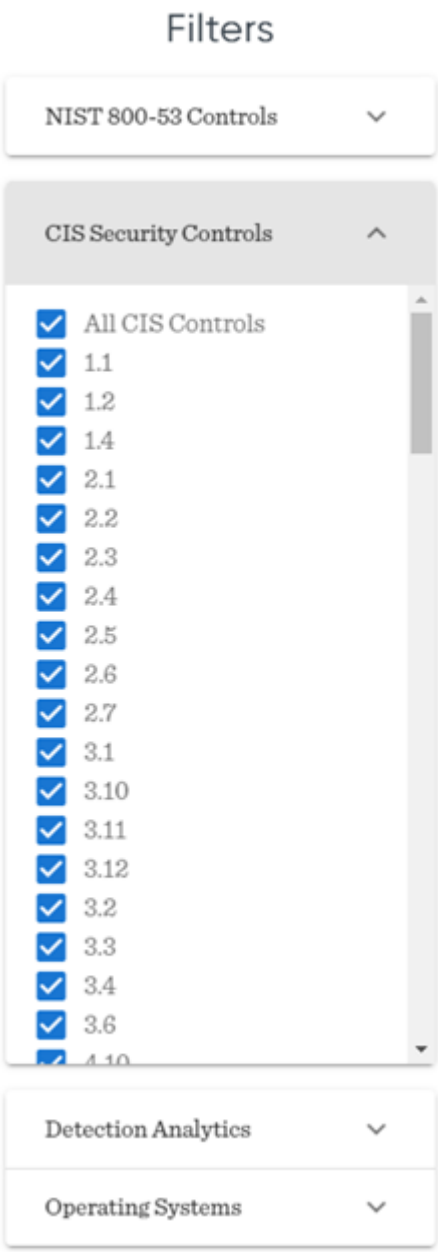


Setting up the filters

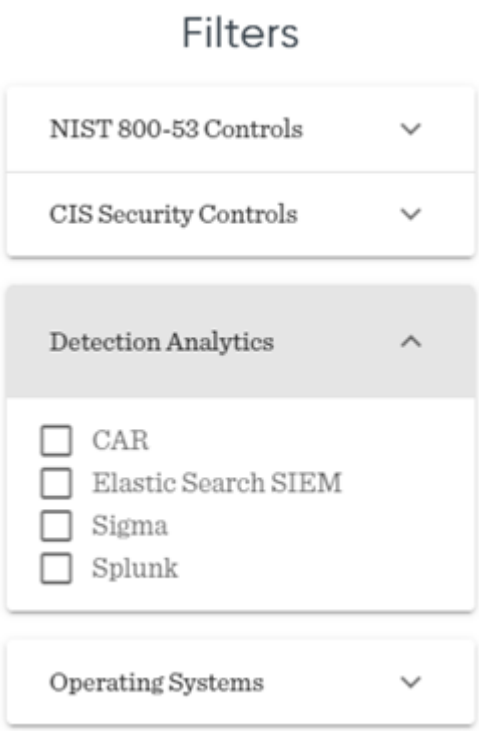
When you visit the calculator, you will see a list of filters that you can set on the left side of your screen. First is the NIST 800-53 Controls filter where you can select which NIST controls you want to focus the most on. If you want to know more about the controls that exists and the NIST 800-53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



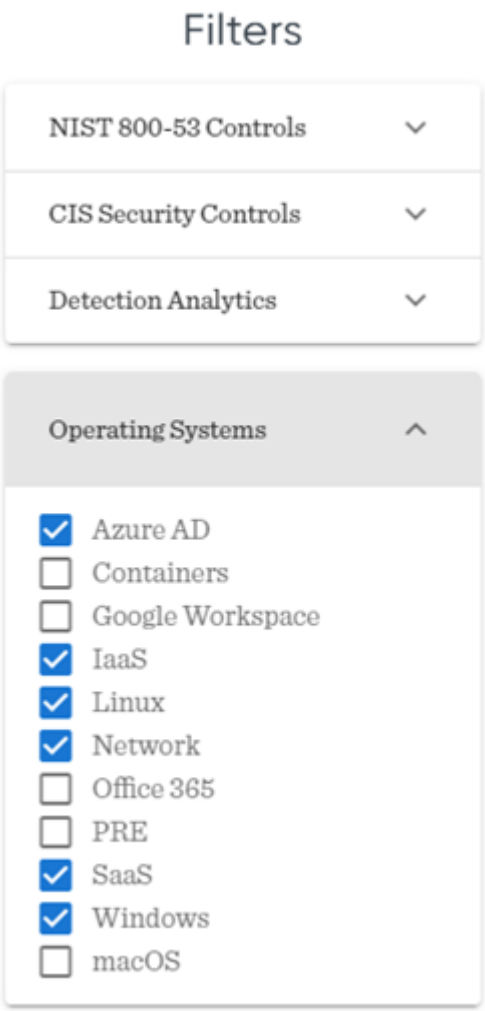
The second filter is the CIS Security Controls filter. Just like the NIST 800-53 filter, you can set this to only see the techniques related to the selected controls. We will use the 'All CIS Controls' filter for this example. If you want to know more about the CIS controls, you can take a look at this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



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.

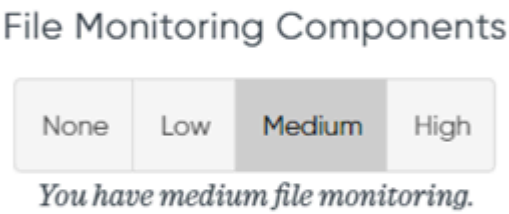


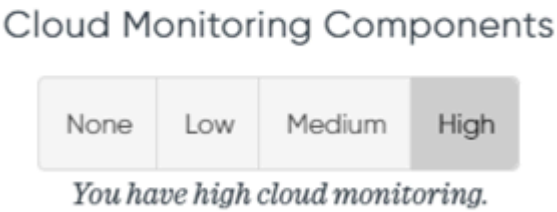
In the last filter, you can choose which technologies you are focusing on. I will choose the following settings:

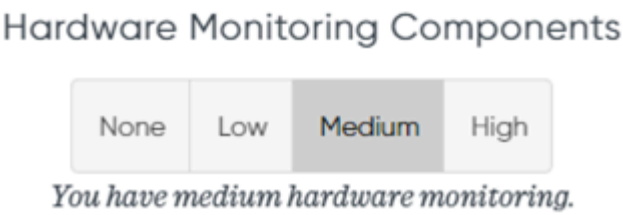


Choosing the monitoring components

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:



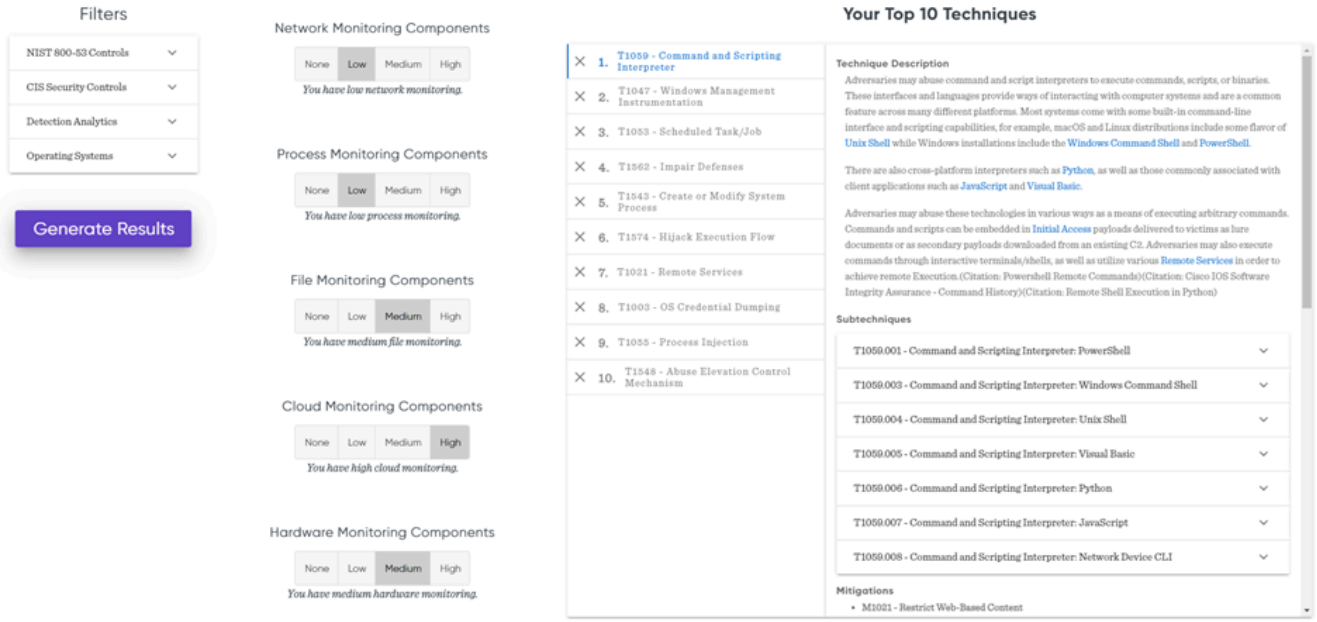




Results

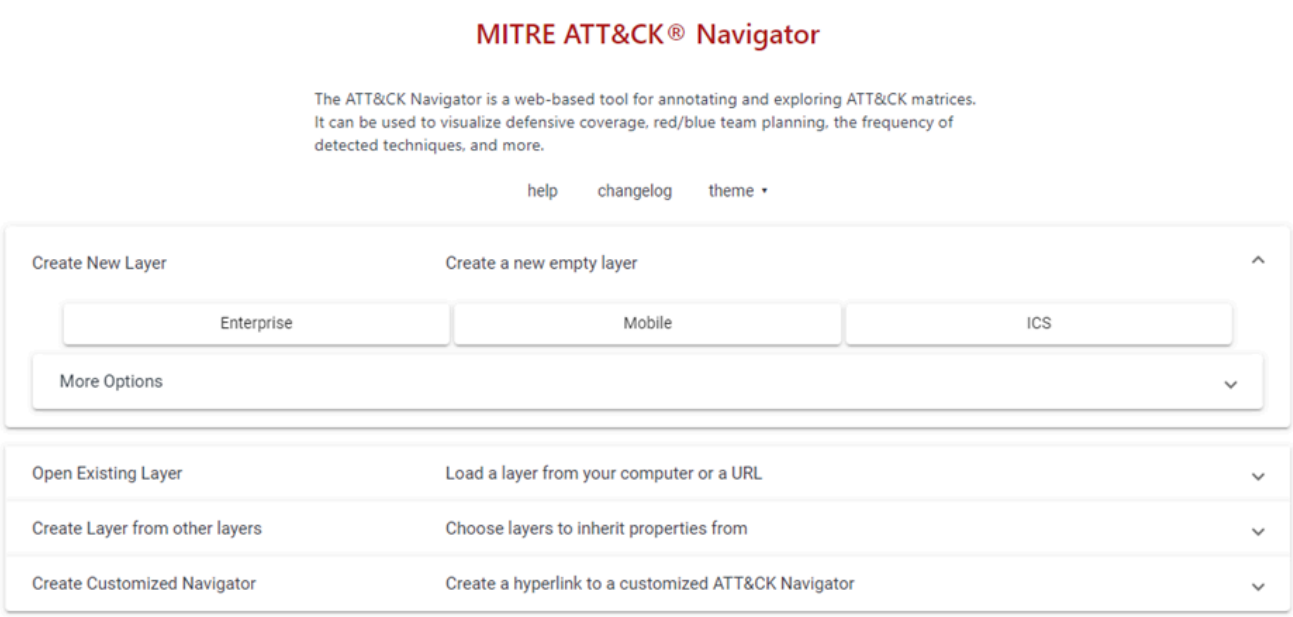
If you set everything up, you can click on the ‘Generate Results’ button to get the top 10 most important techniques you will have to focus on. You

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.



Mapping your Top 10 techniques to the MITRE Matrix

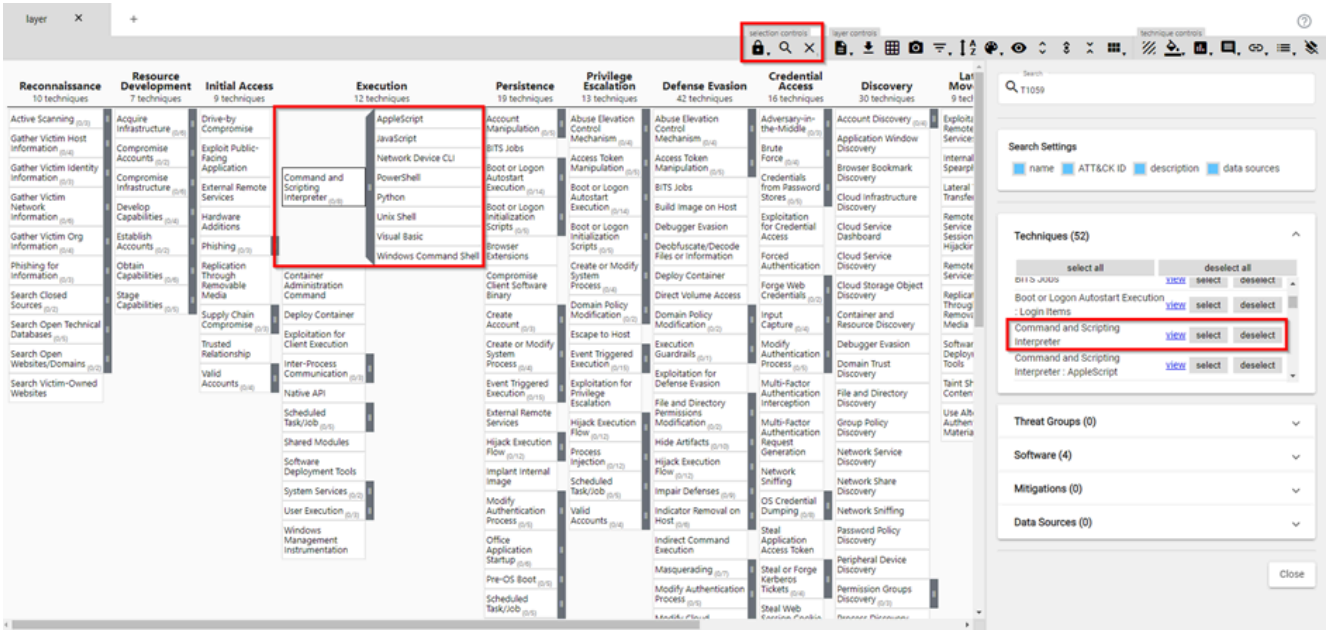
Now that you generated the 10 most important techniques to focus on, it is time to map these in one of the MITRE ATT&CK matrices that fits your organisation. When you go to the MITRE ATT&CK Navigator, you can create a new layer where you can map your techniques to. Based on your environment you can select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



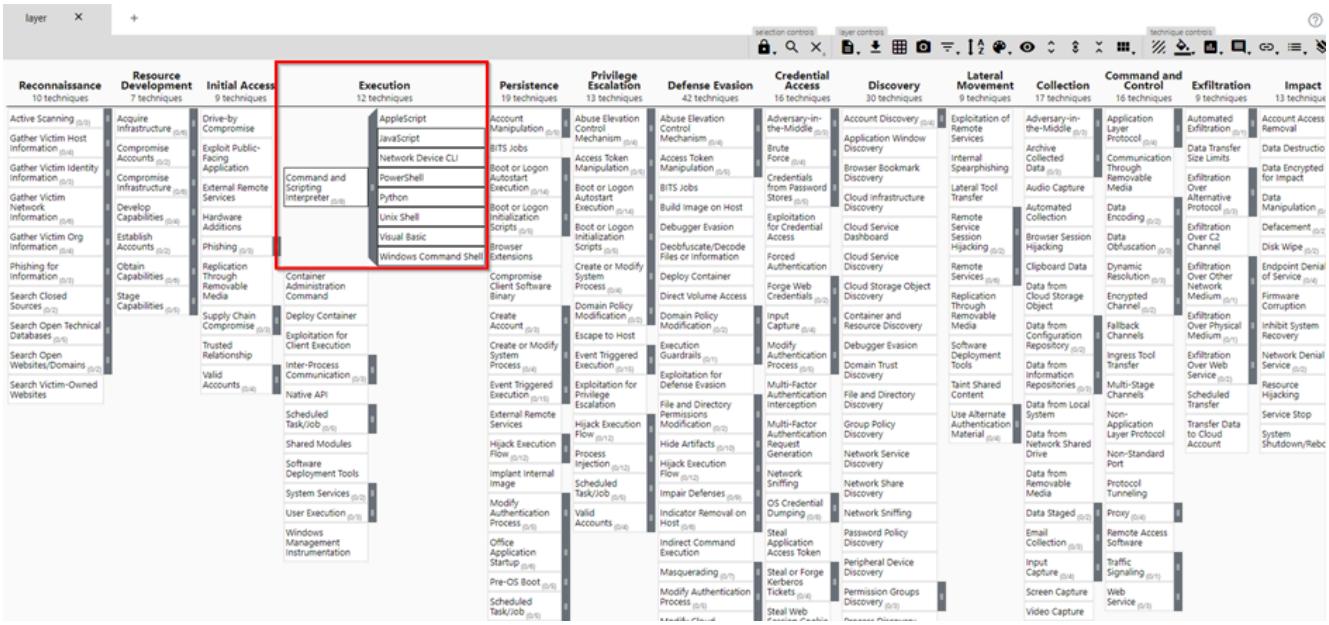
We will not discus all the capabilities the MITRE ATT&CK Navigator has to offer, since this will lead us to far from the purpose of this blog post. If you want to know everything about the MITRE ATT&CK Navigator, I highly recommend following the free courses on ATTACKIQ!

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:

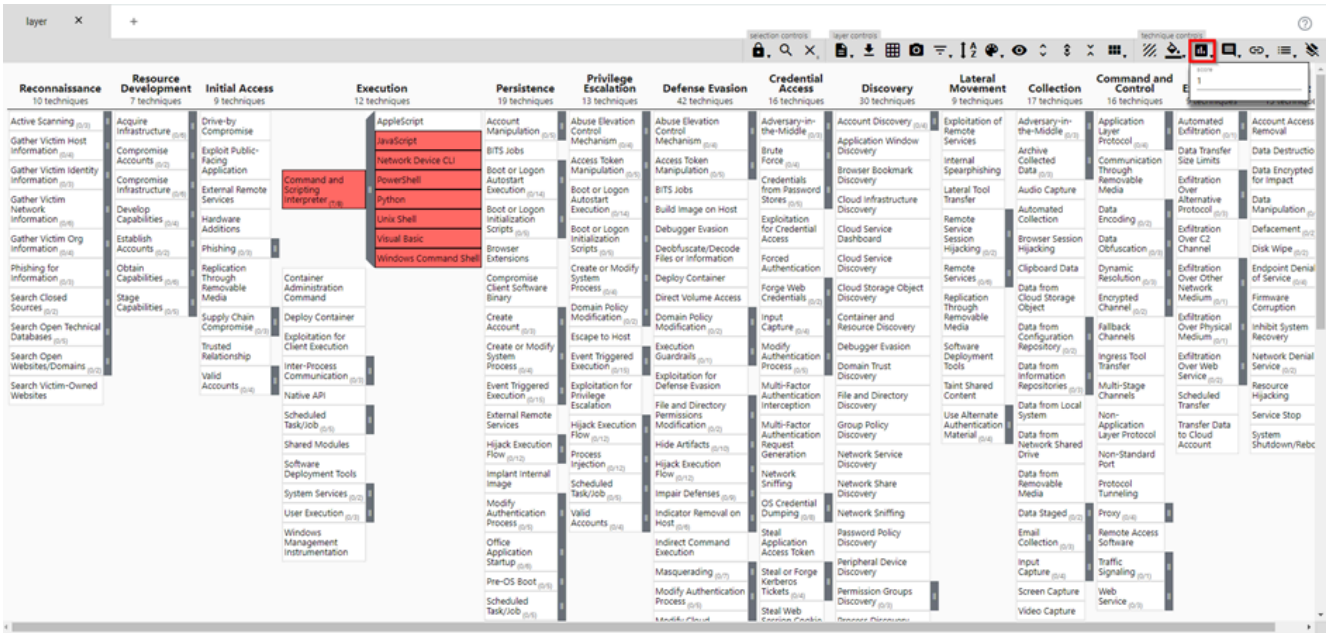


In our example, technique T1059 was our number 1 technique to look out for in the Top 10 Techniques calculator. Based on the filters we set, only these sub-techniques seemed to be important to us: T1059.001, T1059.003, T1059.004, T1059.005, T1059.006, T1059.007, T1059.008. Knowing this, we can select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



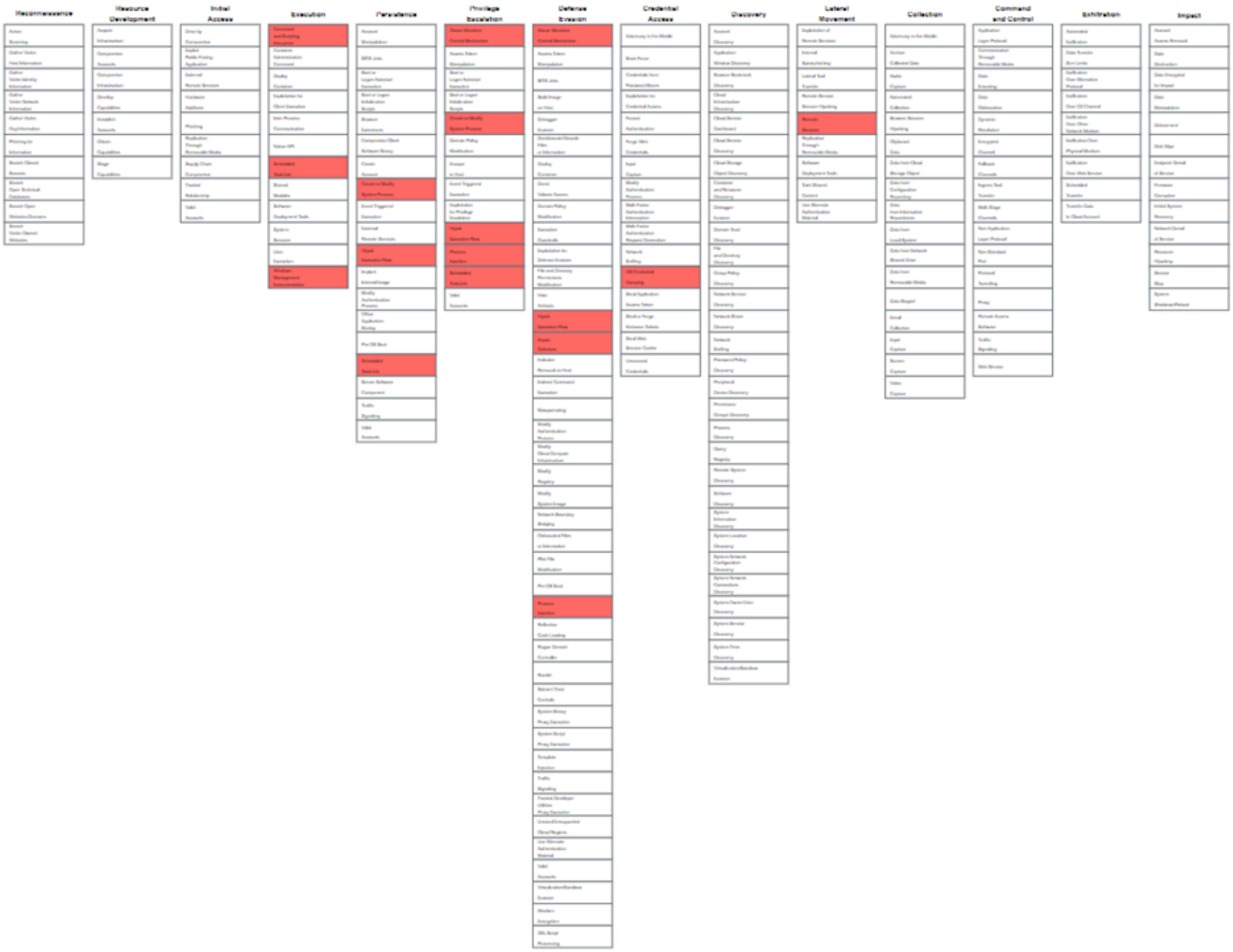
Adding scores

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:

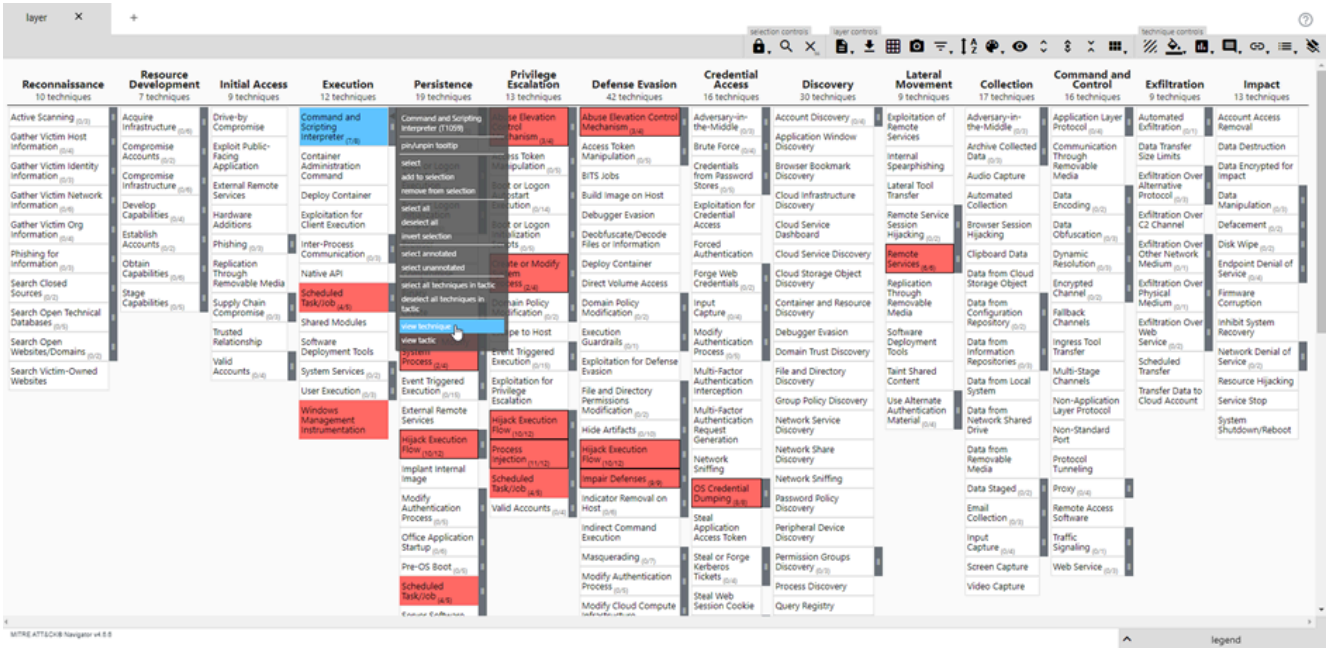


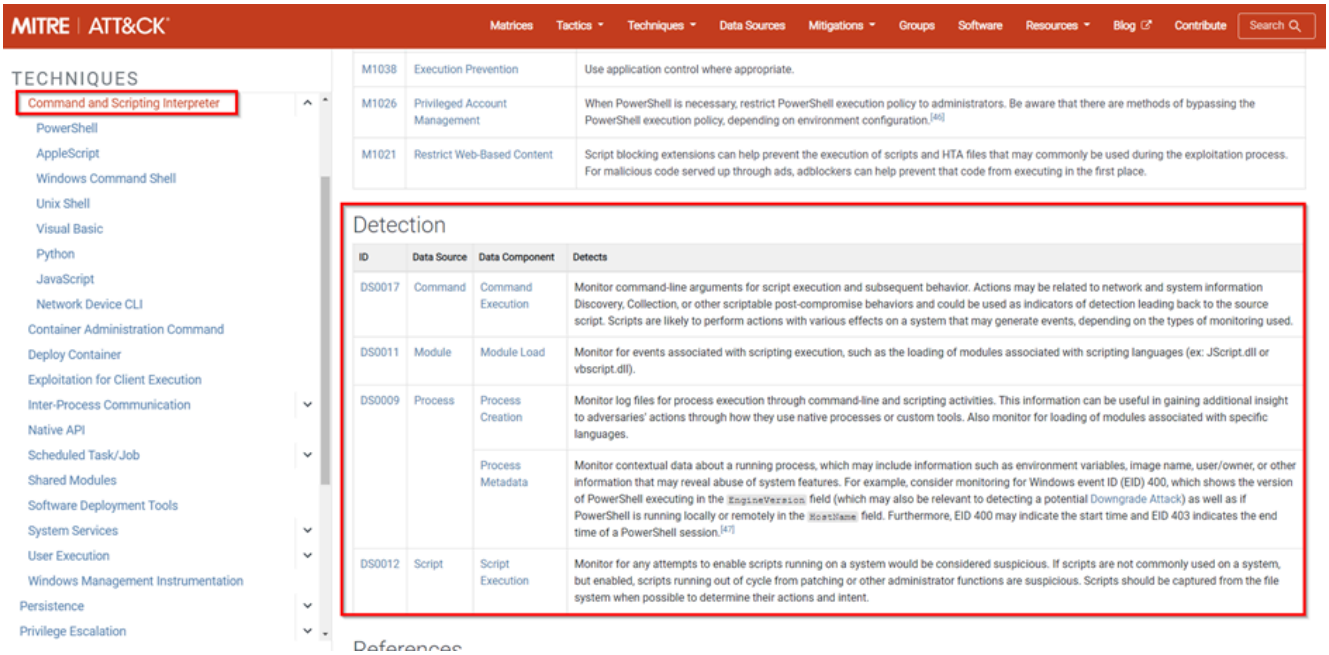
Results

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!



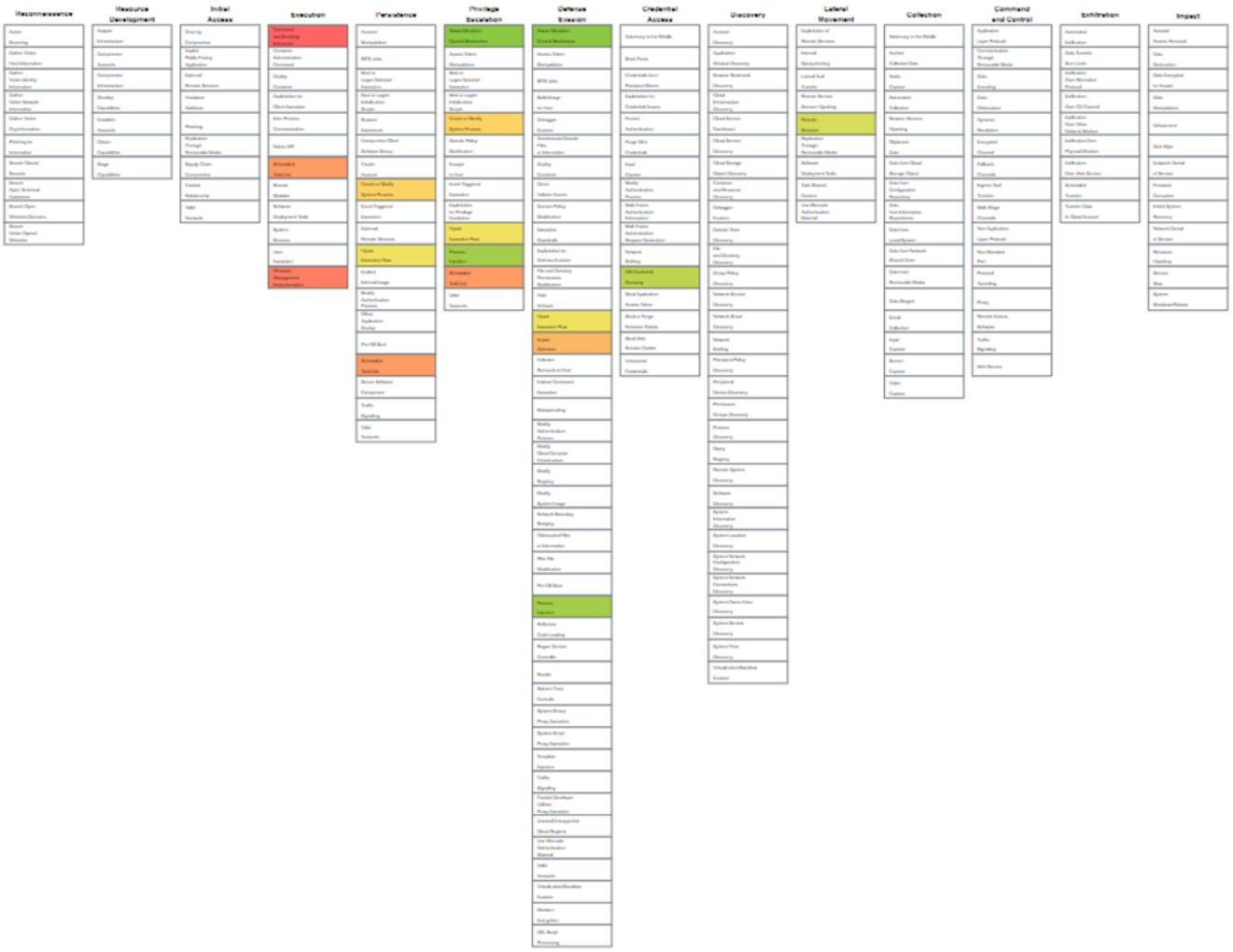


Extra

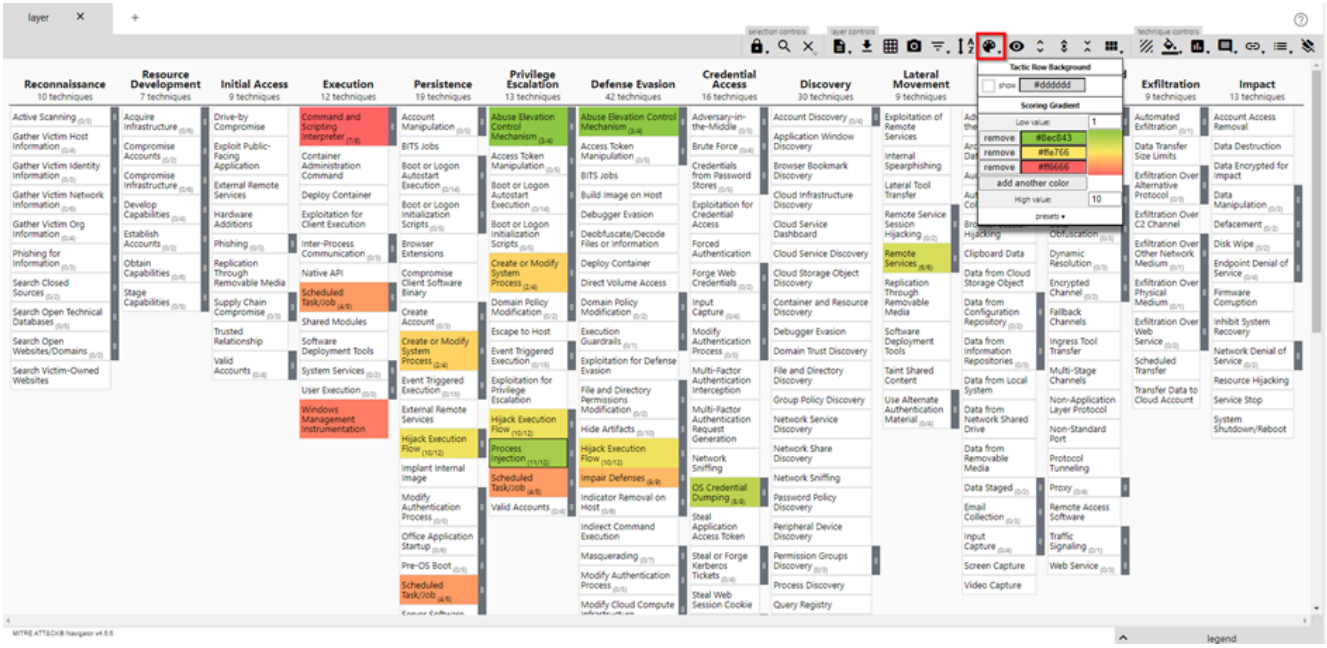
Now that you have all of this information, you can explore the techniques that seemed to be important for you, and start checking which detections you can setup in Microsoft Sentinel and which data sources you will need for those detections.

Remember when we set a score of 1 for all the techniques and sub-techniques? If you want to, you can give the techniques that were higher on the list in the Top 10 Techniques calculator more weight in comparison

to the others. This way you can **create a heatmap** with the techniques you can focus on first. I will give for this example the technique that was on number 1 in the calculator a score of 10 and make my way down to the last technique which will have a score of 1. By doing this, you will get something like this:



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

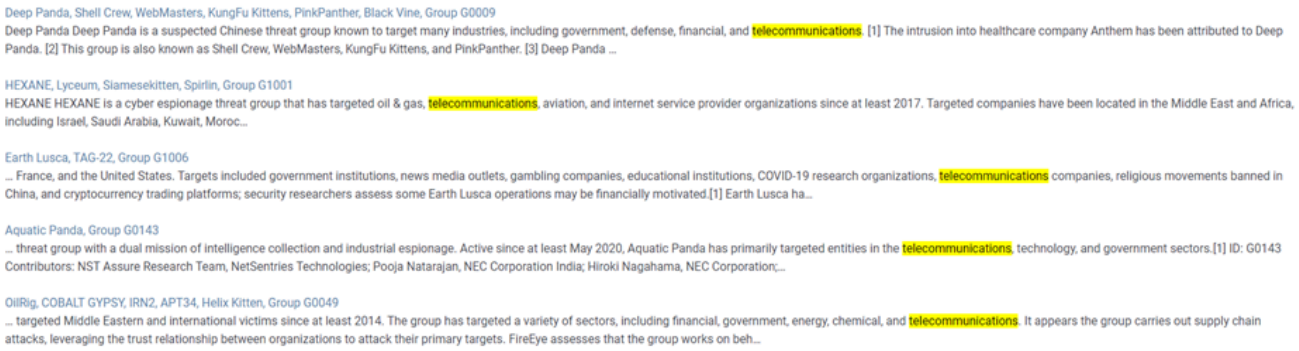


Focussing on techniques common groups are using

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

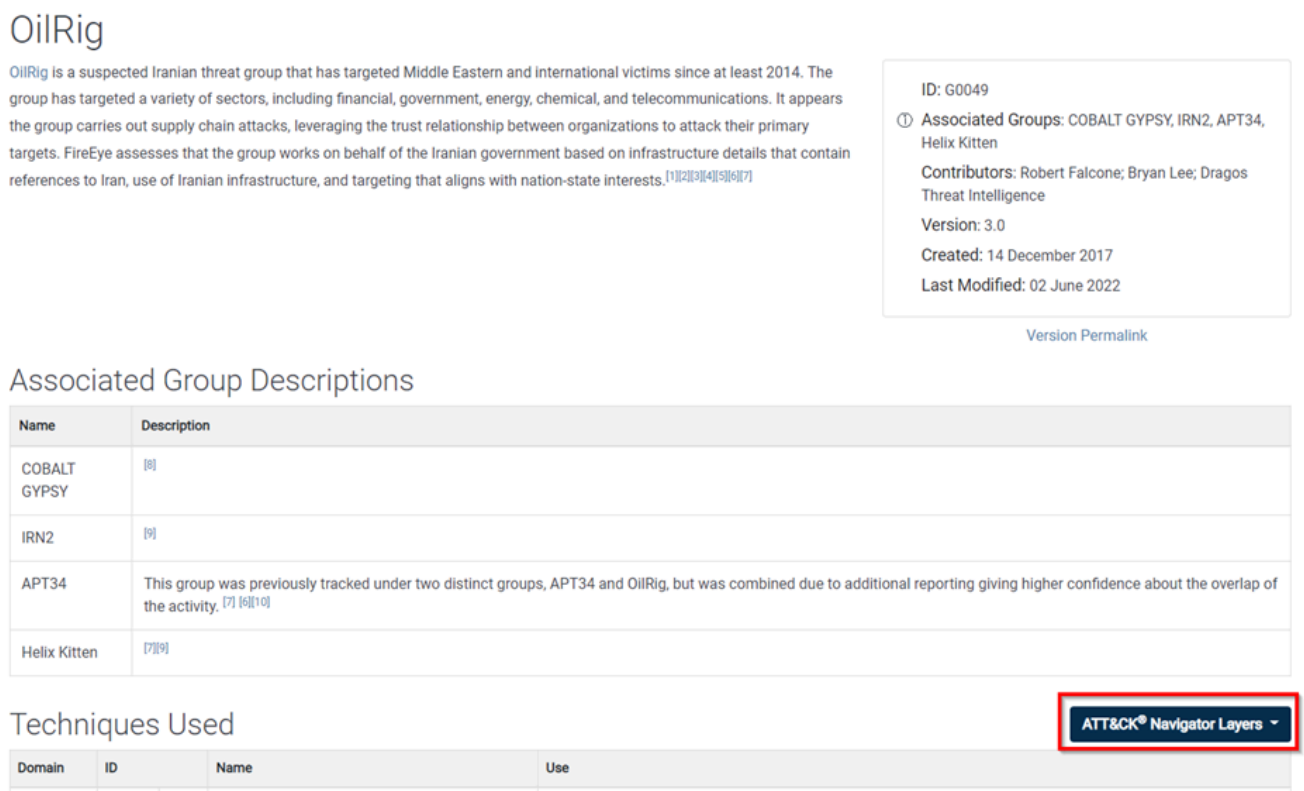
You can find industry related attack groups by simply going to the MITRE ATT&CK website and searching for the industry you work in. Let's say your company is active in telecommunications, by going to the search box in the top right corner and typing telecommunications, you will get a couple of attack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

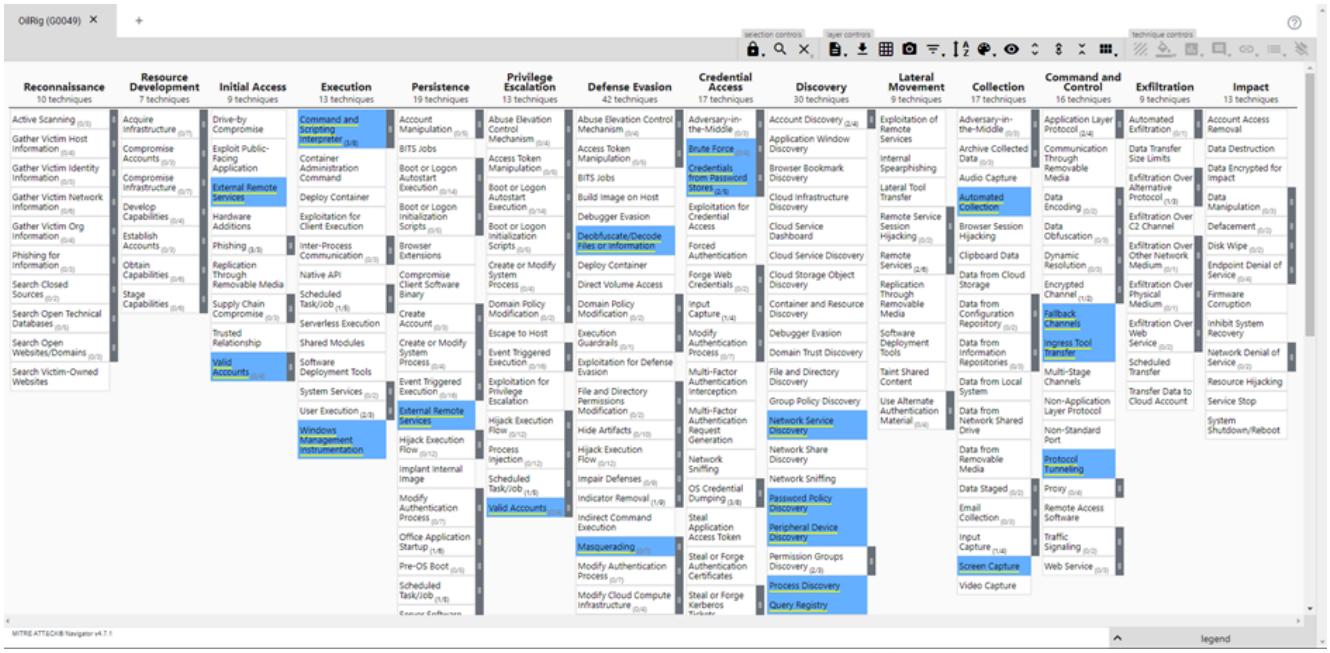


For this post, we will be using OilRig as an example to create mappings.

Creating mappings

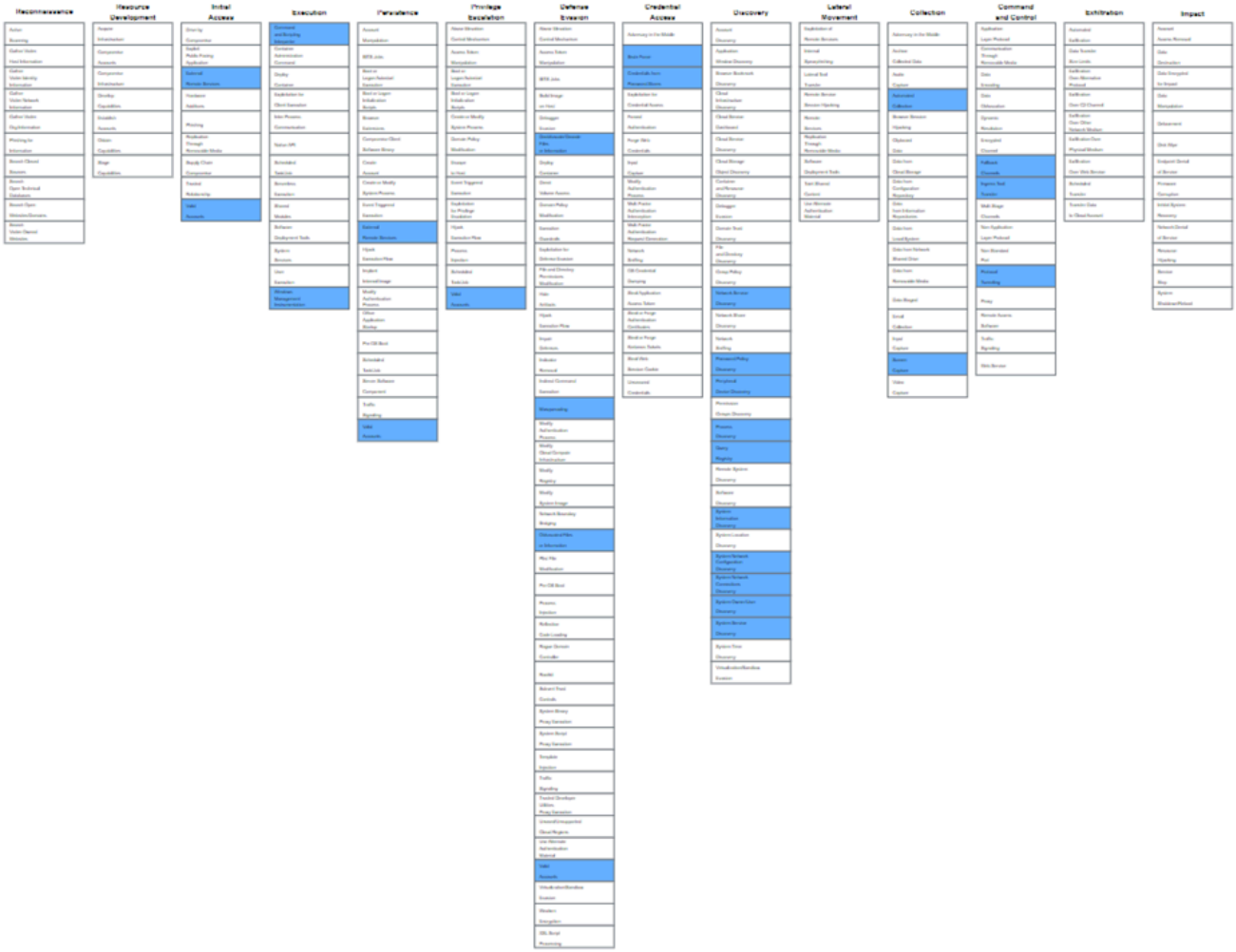
When you go to a group page in MITRE ATT&CK, you will find the 'ATT&CK Navigators Layers' button below the associated group descriptions. Mapping the techniques this group is using is just as simple as clicking this button and viewing the navigator:





Results

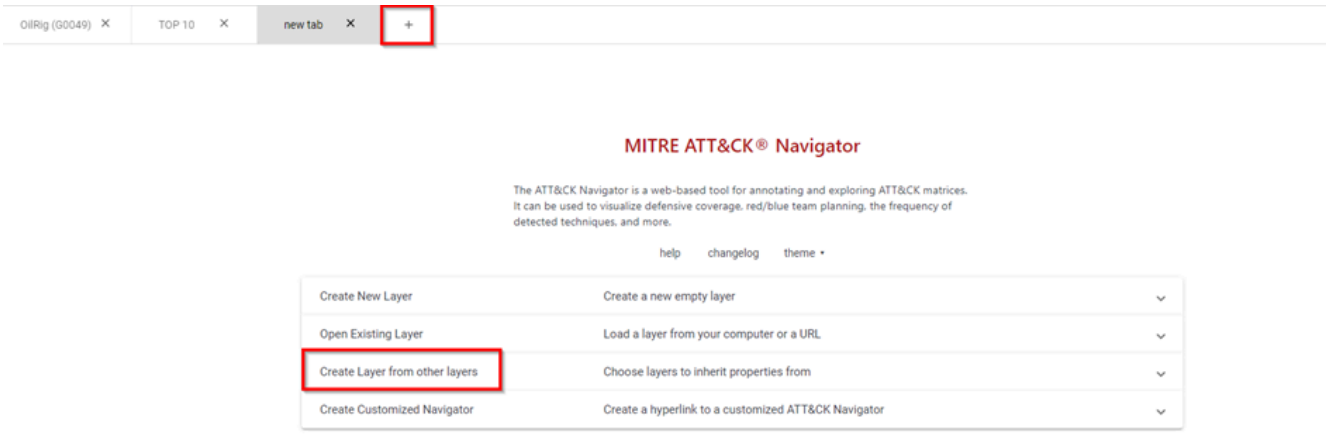
Note that all related techniques and sub-techniques have a score assigned and are given a colour. Most of the techniques also have extra comments with links to other groups that are using the same techniques.



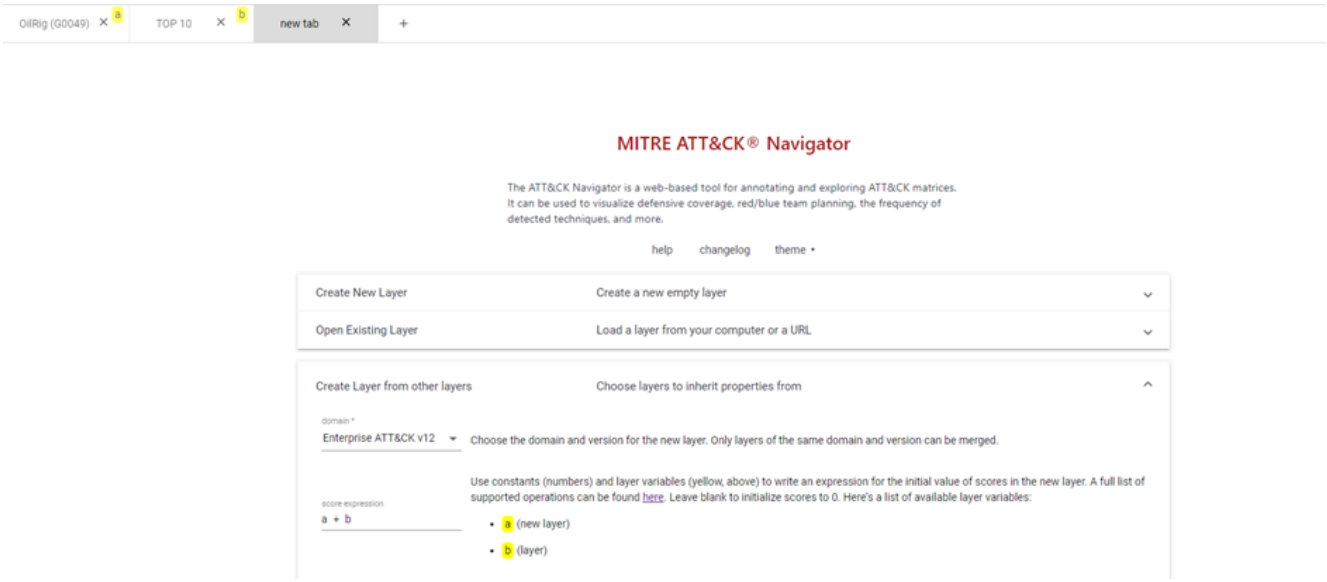
Merging the layers

Now that you have a layer of the Top 10 techniques calculator and a layer of an attack group you want to focus on, it is about time to merge these layers so you have an overview of all the important techniques. Merging the layers is done in the MITRE ATT&CK navigator and is only possible when you have the layers loaded in the navigator.

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



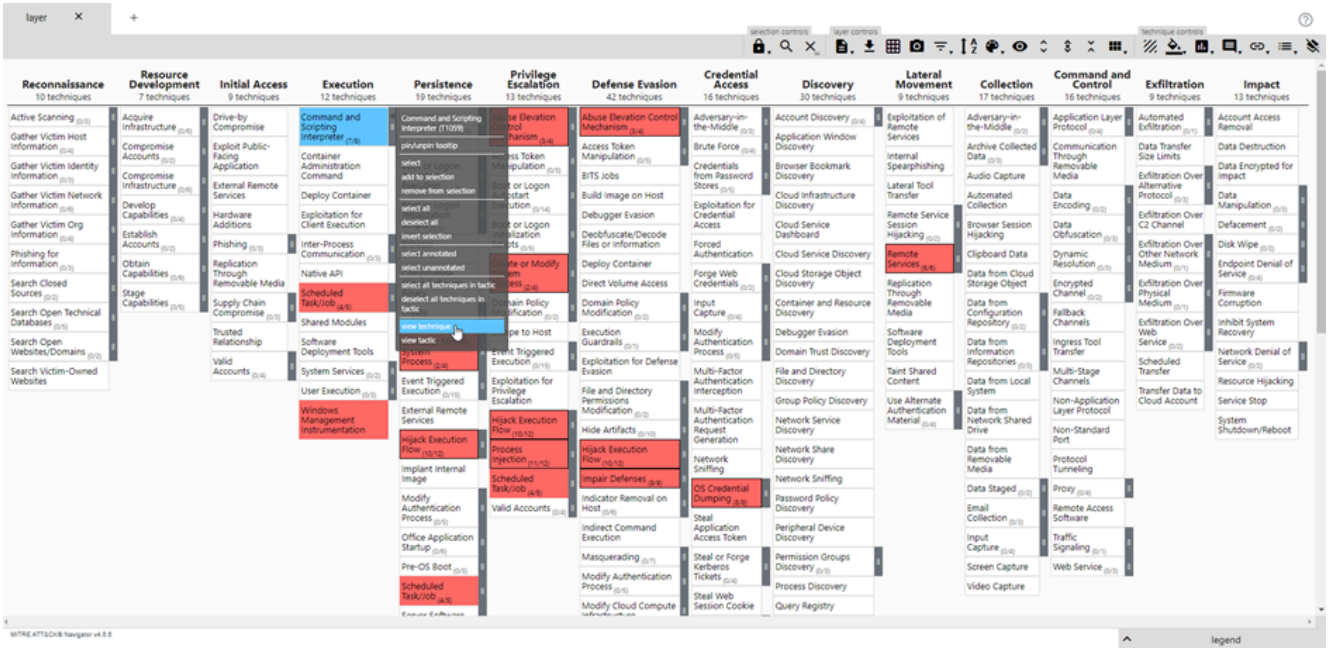
Here you will need to choose a MITRE domain (we take the latest Enterprise domain) and an expression to merge the layers. These expressions are used with the scores you added to certain techniques in your layers. When you choose an expression like a + b, the new layer will add the scores of the techniques 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

Now that we have a useable MITRE ATT&CK layer, it is time to implement this in our Microsoft Sentinel environment. When you right-click on one of the techniques in your layer, you will be able to go to the techniques page on the MITRE website by clicking “View technique”.



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

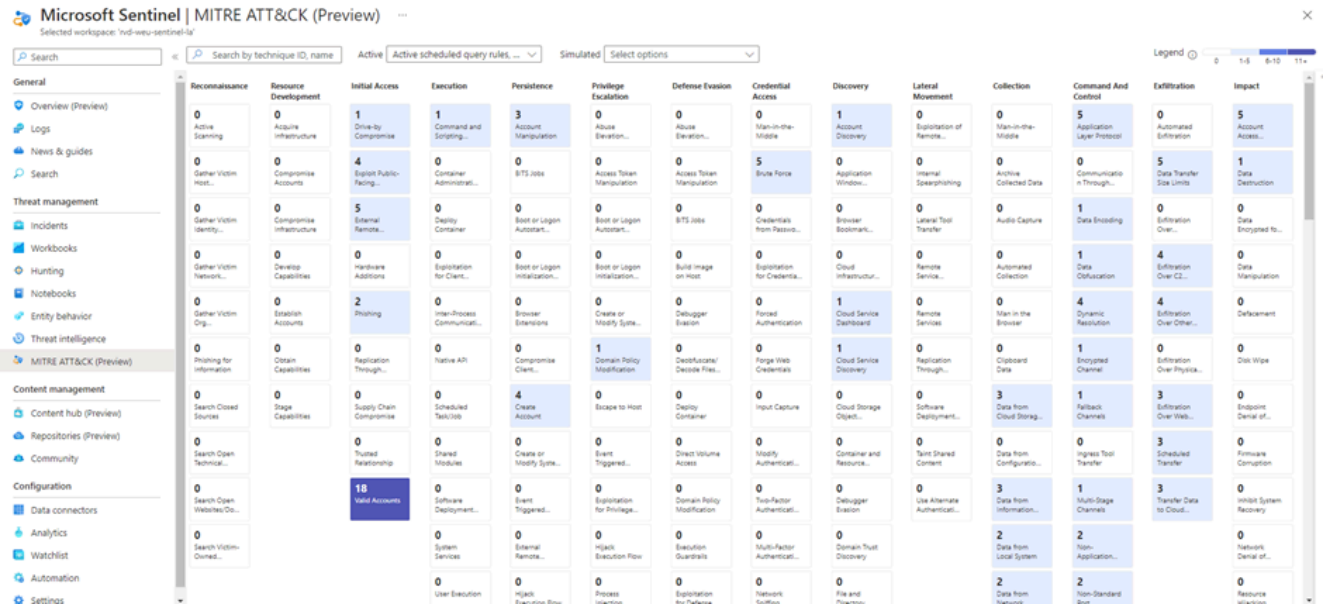
ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information Discovery, Collection, or other scriptable post-compromise behaviors and could be used as indicators 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 `EngineVersion` field (which may also be relevant to detecting a potential Downgrade Attack) as well as if PowerShell is running locally or remotely in the `HostName` 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 is 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 you Sentinel environment.

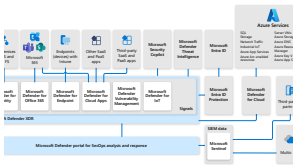


The hard part is correlating this layer to your MITRE ATT&CK Navigator layers, since there is no export feature available in the portal. Another problem is that this layer is aligned with the MITRE ATT&CK framework version 9, which is a version that is released on April 2021. Since most of

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