Introduction to MITRE D3FEND Framework and How can you use it to Defend Your organization.

Summary

Adversaries have embraced a new vector for getting a grip on a targeted company, adding to their already extensive arsenal of skills. Unfortunately, while trying to keep their firms' networks secure, defenders have had to document and plan for practically every approach adversary could employ against them. Fortunately, many frameworks that aid in this process have emerged in the cybersecurity industry in recent years, providing defenders with valuable resources for combating cyber threats. This blog looks into the MITRE D3FEND framework and how it can be used to actively countermeasure cyber-attacks.

Introduction

MITRE D3FEND is a new framework of defensive countermeasures commissioned and supported by the National Security Agency (NSA) to assist security professionals in planning and tailoring their defences for common MITRE ATT&CK techniques. Countermeasures are included in the D3FEND matrix at every stage of an attack, assisting with prevention, mitigation, remediation, and response.

SO, what is MITRE ATT&CK Framework???

MITRE ATT&CK is an acronym for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK framework is a curated knowledge base and model for cyber adversary behaviour, representing the many stages of an adversary's attack lifecycle as well as the platforms they are known to target.

The framework is meant to be more than a collection of data: it is intended to be used as a tool to strengthen an organization's security posture. Many threat intelligence, incident detection and response, endpoint and network security platforms have aligned their observations with ATT&CK during the last few years to serve as a reference point for analysts.

Figure 1: MITRE ATT&CK Framework Snippet

https://attack.mitre.org/

Because ATT&CK is based on actual adversary behaviour, defenders may feel comfortable that these aren't just hypotheticals. However, despite its rich capabilities and global, up-to-date knowledge base, ATT&CK was not designed to provide countermeasures or defences. Defenders should also be able to defend against the techniques used by their adversaries. This is one area where this framework falls short.

How does D3FEND Help??

The D3FEND framework was created to work in collaboration with the ATT&CK framework. D3FEND focuses on standardizing the defence mechanism, while ATT&CK focuses on providing a common line of offence mechanism to identify and respond to TTP. It can aid cybersecurity professionals in the development and deployment of defence systems.

D3FEND, like MITRE ATT&CK, is organized as a matrix with high-level strategies. Harden, Detect, Isolate, Deceive, and Evict are the five basic defensive tactics currently available in D3FEND. Countermeasure method categories, such as Network Traffic Analysis and User Behaviour Analysis, sit beneath each of those tactics.

D3FEND is composed of 3 critical components:

· An examination of 20 years of earlier cybersecurity filings in the US patent database produced this knowledge graph, which outlines the defensive strategies.

· A series of user interfaces to access this data.

· A way to map these defensive measures to ATT&CK's model.

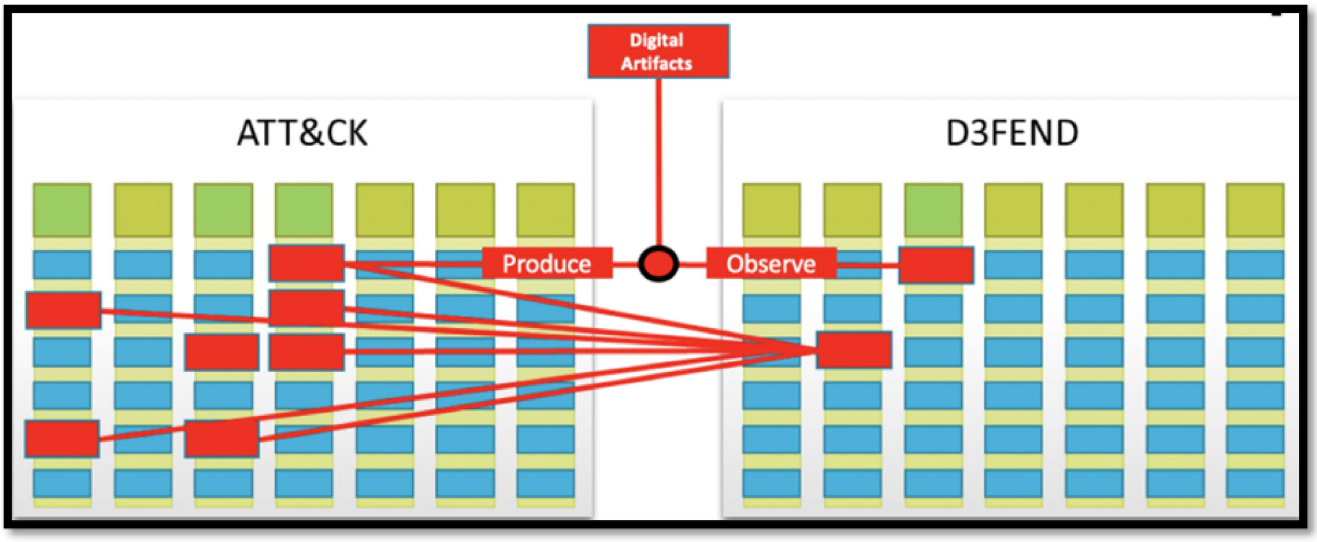

Figure 2: Mapping ATT&CK and D3DEND

How can an organization use the D3FEND framework for its benefit?

D3FEND is meant to be a perfect companion to ATT&CK, allowing defenders to apply what they've learned about an adversary's technique to applicable countermeasures right away. The benefit is obvious: security teams may discover adversary techniques, perform lookups to gather context, and find subsequent countermeasures to defeat those techniques in their environment using only these two resources.

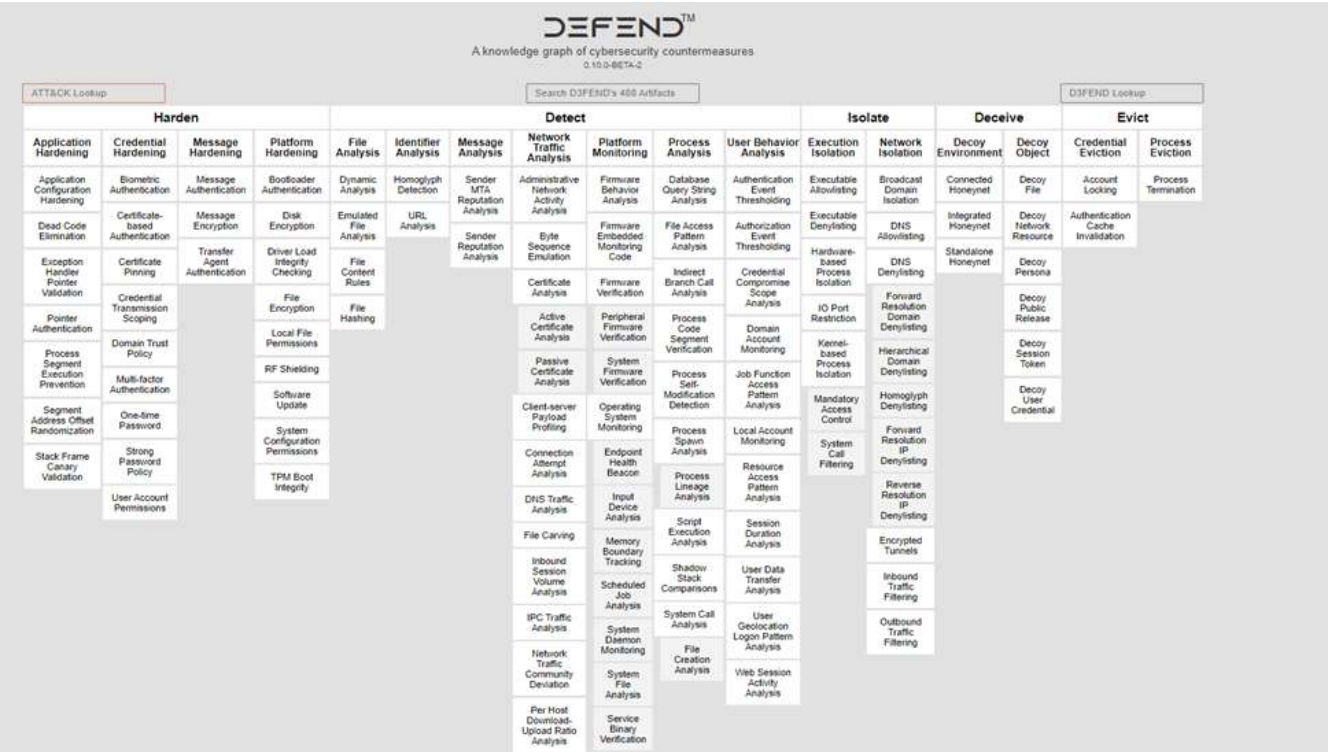

Figure 3: D3FEND Framework Snippets

The above picture is a snippet of the D3FEND framework, from their official website. At the most basic level, security teams can examine each of the countermeasures described in D3FEND and determine whether (and how) that countermeasure is currently being deployed by their company. This enables businesses to spot defensive flaws and make more strategic security equipment choices.

D3FEND is beneficial for businesses considering new security solutions to determine how much money it will take to install the countermeasure, as well as whether it will help them improve security maturity, hygiene, and posture, or minimize their attack surface. A company can receive insight into how well it might perform by comparing the functionality of a security solution to the matching ATT&CK offensive technique.

Use Case

Let's look at one small example of how a defender can use these two frameworks to strengthen their network.

One of the most frequent adversarial trends that occurs every year is an abuse of remote access mechanisms such as RDP, SSH, or a third-party tool, such as LogMeIn or TeamViewer. Adversaries love an opportunity to gain access to an environment via already established means. In February 2021, Kaspersky reported record levels of RDP attacks, highlighting as much as 10 times growth in some nations (Darkreding.com).

Let's look at how adversaries use these remote access techniques to gain unauthorized access to the system. Within ATT&CK, the technique External Remote Services (T1133) is categorized as both an Initial Access tactic and a Persistence tactic.

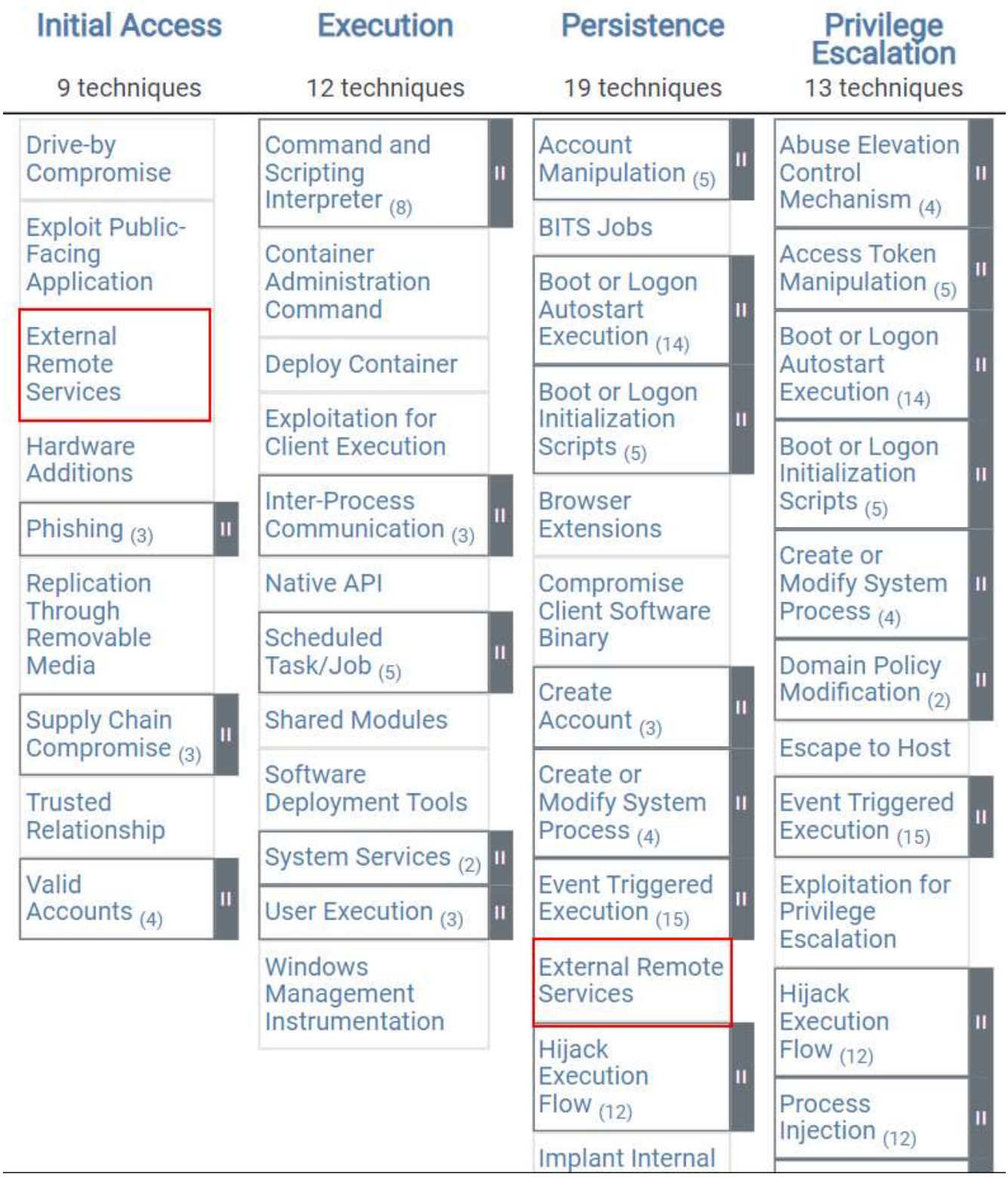

Figure 4: MITRE ATT&CK Framework

When such techniques are reflected on multiple tactics lists, it is a great cause of concern and force-multiplying mitigation for security teams. Here's why:

1. **Cause of Concern:** A technique's "flexibility" in an adversary's toolset is reflected by its appearance in multiple tactics. External remote access can be utilized to get initial access to an organization as well as sustain persistence in this situation.

o **Initial Access:** External remote services that are exposed or insecure provide an opportunity for an adversary to get a presence in an environment. As we go more into the technique, we discover that applicable services may include, VPNs, Citrix, Windows Remote Management, and Virtual Network Computing (VNC), RDP.

o **Persistence:** External remote services, on the other hand, give adversaries a great opportunity to maintain persistence inside a system. Pre-established connections make attacking and maintaining persistence in the whole network a lot easier. The attacker doesn't have to dedicate a lot of resources to exploit these services.

2. Force Multiplying Mitigation: Defenders acquire several benefits when they mitigate, just as adversaries do when they deploy multi-user techniques. When defenders gain visibility, monitoring, and/or blocking control of (or eliminating) RDP within the environment, they have minimized an adversary's ability to abuse it. Removing Initial Access and Persistence tactics from an adversary's toolkit can deal a big blow to their capabilities and attack plan.

Mitigations

ID	Mitigation	Description
M1042	Disable or Remove Feature or Program	Disable or block remotely available services that may be unnecessary.
M1035	Limit Access to Resource Over Network	Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems.
M1032	Multi-factor Authentication	Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of Multi-Factor Authentication Interception techniques for some two-factor authentication implementations.
M1030	Network Segmentation	Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls.

Figure 5: Mitigation for External Remote Services

In the above picture, we can see that access to a Valid account is the requirement for remote service abuse. We can see how locking down external remote services also provides a chance to implement strong account procedures, such as strong and rotating passwords, least privileges, and other recommendations. ATT&CK provides mitigation methodologies of these techniques too as seen in the above Figure. But Mitigating and Counter Measures are not the same thing.

After all, a security team may wish to quickly minimize a growing threat while also deploying long-term remedies to monitor and/or defend against future attacks. D3FEND contains all of these answers and more. We can observe the relationships drawn by various countermeasures and this technique by searching up ATT&CK technique T1133, External Remote Services.

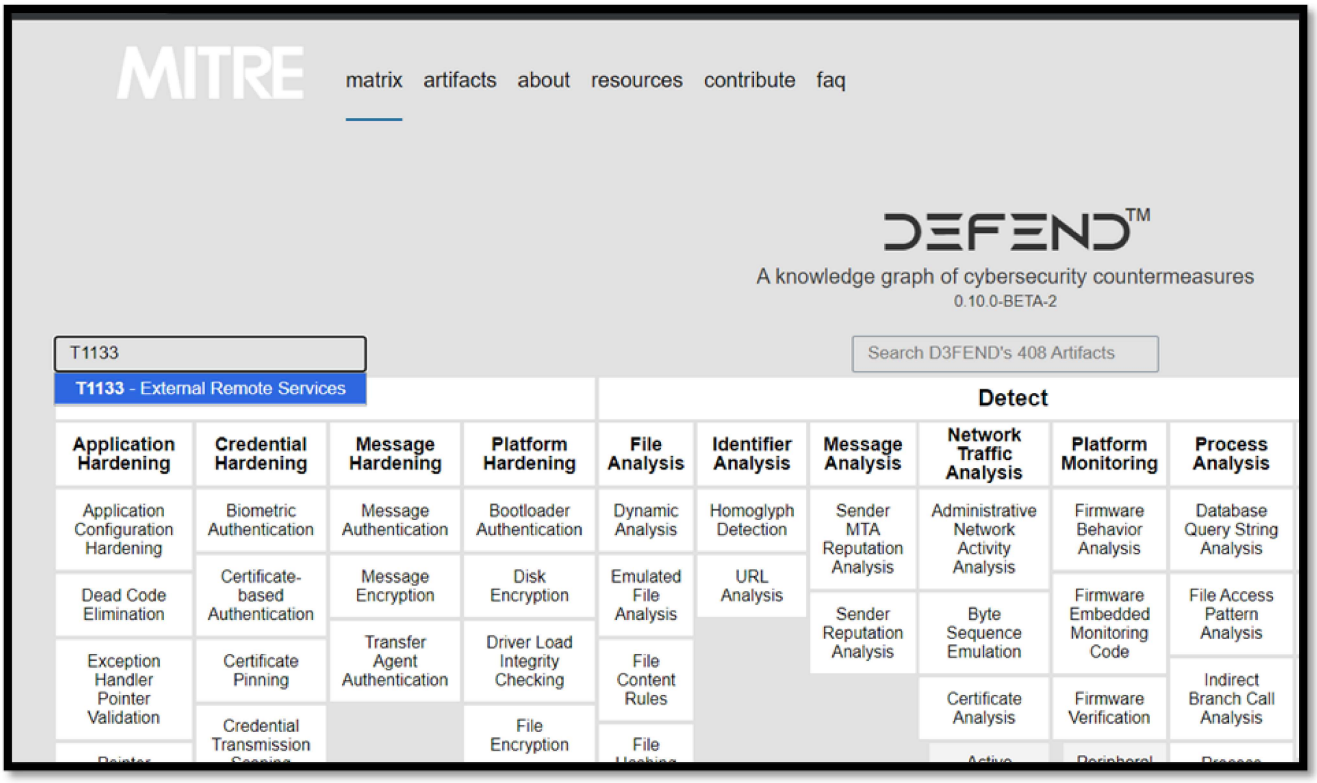

Figure 6: ATT&CK Search on D3FEND

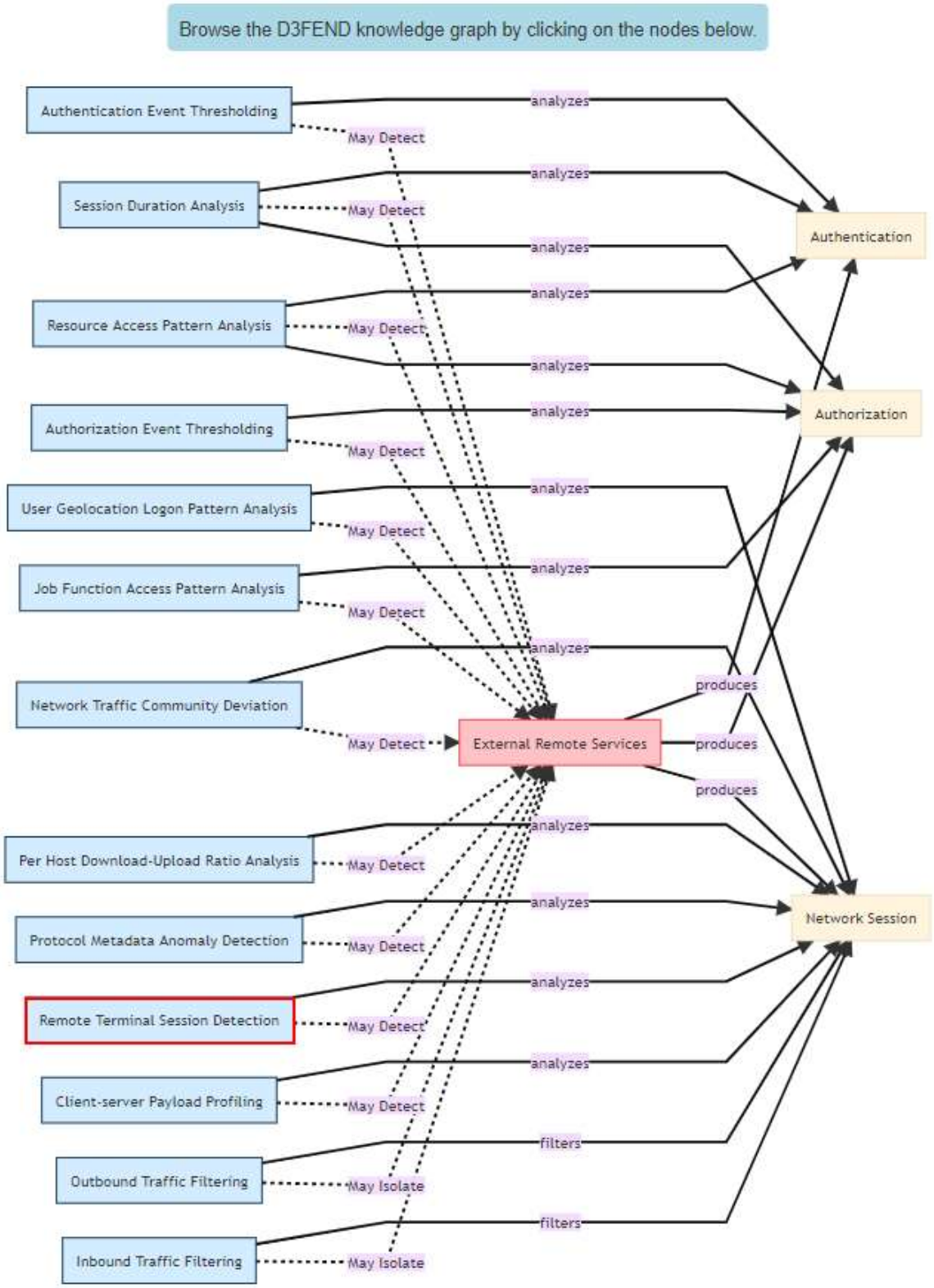

Figure 7: Relationship between ATT&CK and D3FEND

Above figure, shows various countermeasures within D3FEND and how they can be used to counteract External Remote Services. This is a great place for defenders to start researching and implementing effective countermeasures.

For this case, We'll Focus on the Remote Terminal Session Detection countermeasure as shown in figure 7.

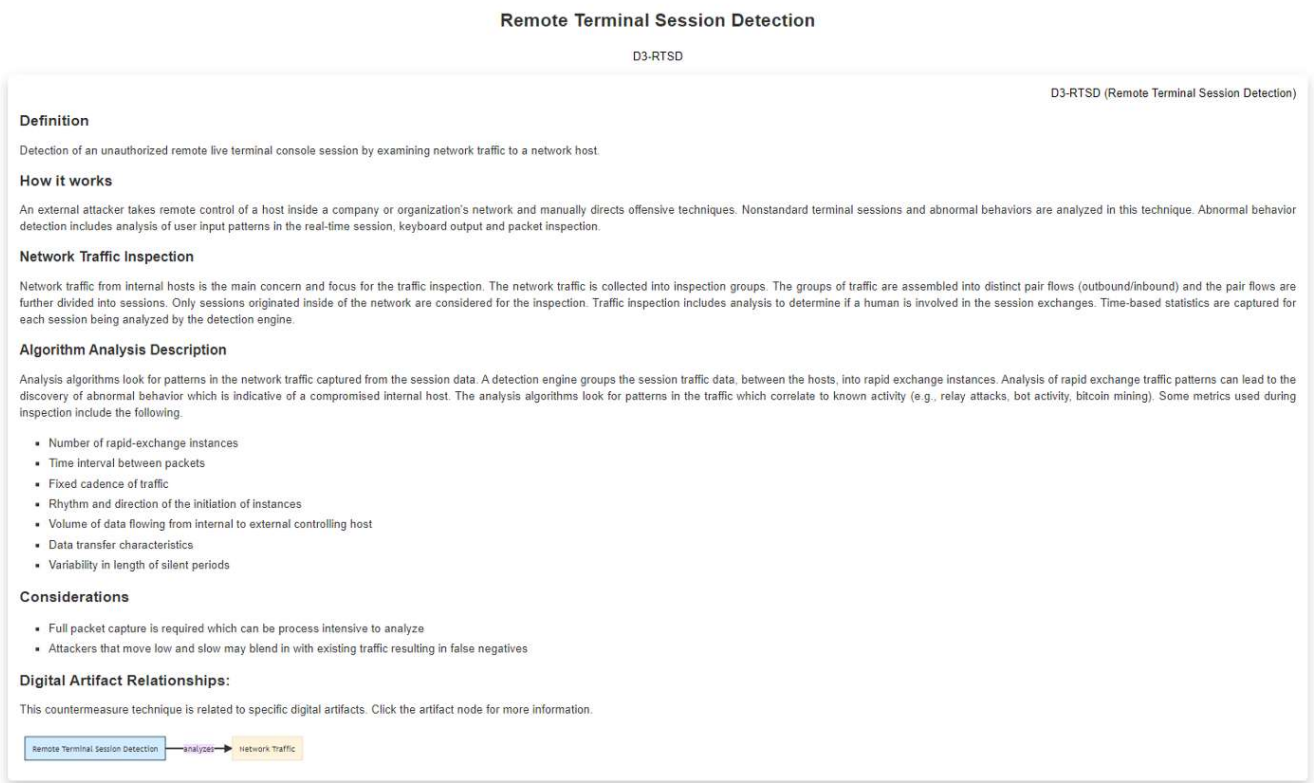

Figure 8: Explanation of Remote Terminal Session Detection in D3FEND

We can see a detailed explanation of how countermeasures like network traffic inspection and algorithm analysis can be used to detect remote terminal sessions. For defenders trying to fine-tune their controls or create custom detections, this is incredibly useful information.

However, D3FEND goes a step farther by providing mappings to other ATT&CK techniques that these countermeasures may be effective against. As shown below figure.

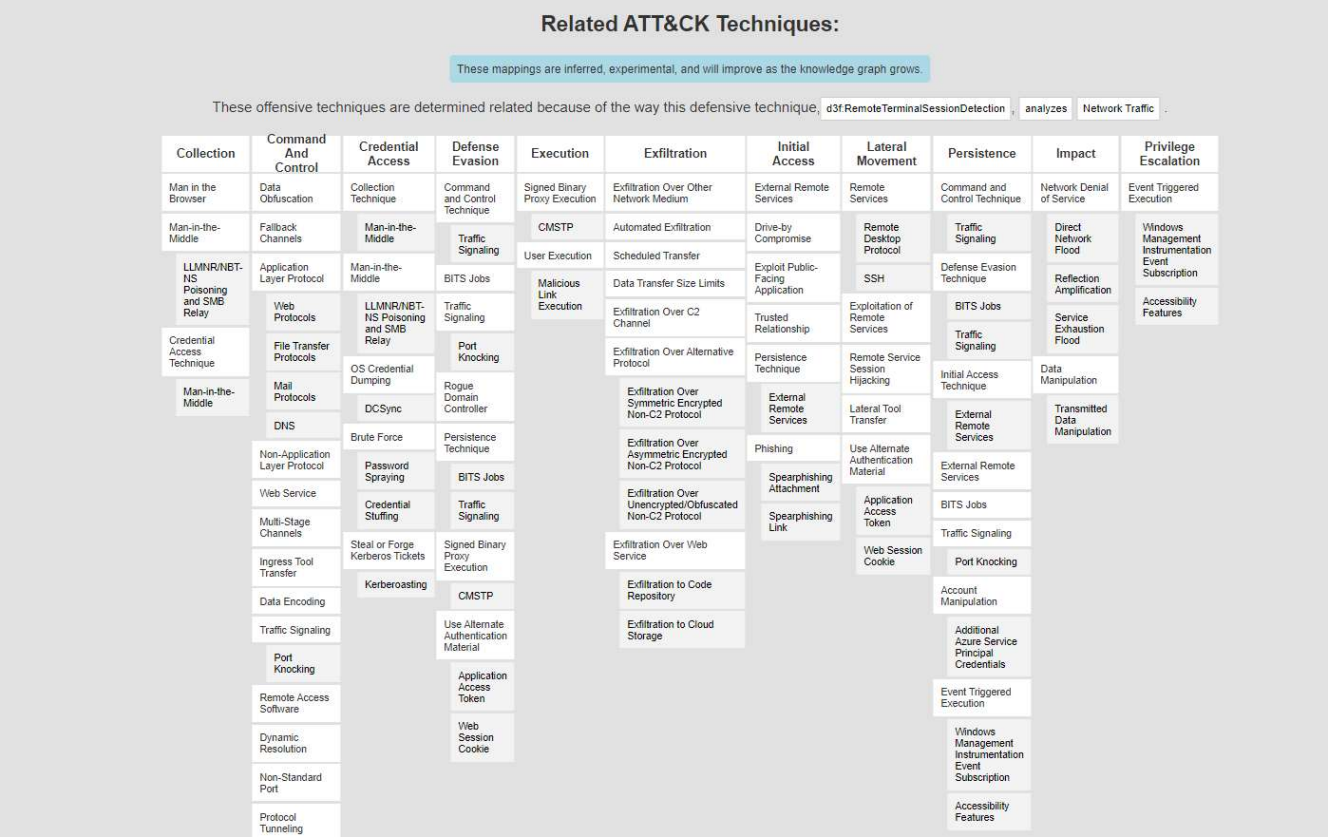

Figure 8: ATT&CK and D3FEND Mapping

This is where defenders can obtain a true advantage over an adversary by combining the two matrices. Defenders can start with a single adversary tactic, such as External Remote Services, and combine their knowledge to create countermeasures against that strategy.

Conclusion

In the above scenario, we solved the problem of External Remote services by merging the well-known ATT&CK matrix with D3FEND, a framework developed by MITRE and the NSA. D3FEND gives defenders a knowledge network of cybersecurity countermeasures in the form of a matrix, allowing them to compare tactics to protection mechanisms. Defenders can strike a major blow to enemy success rates when these two matrices are combined. Such frameworks could be extremely helpful for defence personnel and organizations to protect their assets and network.

Reference:

RDP Attacks Persist Near Record Levels in 2021 (darkreading.com)

https://d3fend.mitre.org/

https://www.csoonline.com/article/3625470/mitre-d3fend-explained-a-new-knowledge-graph-for-cybersecurity-defenders.html

https://www.uptycs.com/blog/what-is-mitre-d3fend-and-how-should-my-organization-use-it

https://www.extrahop.com/company/blog/2021/what-is-mitre-d3fend/#:~:text=Commissioned%20and%20funded%20by%20the,mitigate%2C%20remediate%2C%20and%20respond.

https://www.linkedin.com/pulse/know-your-enemy-yourself-mitre-attck-d3fend-massey-gdl-msc-cissp-fip?trk=pulse-article_more-articles_related-content-card

https://sharkstriker.com/mitre-releases-d3fend-to-add-defensive-countermeasures-to-its-attck-framework/

https://attack.mitre.org/

https://d3fend.mitre.org/resources/D3FEND.pdf

https://medium.com/@akashnadar24/mitre-att-ck-d3fend-framework-b7927498e60d

https://sansorg.egnyte.com/dl/2AJkXYgE8Q