The MITRE ATT&CK Framework & M365

Written By Ravi Das For KAMIND IT, Inc.

Contents

Introduction

In today's Cybersecurity world, one of the main goals for any CISO and their IT Security team is to try to model the intent, motive, and the kind of security breach that the Cyberattacker is planning on launching. True, this can be done on a real time basis primarily by using Generative AI, but there are also many times when using established models are needed as well. One such example of this is the MITRE ATT&CK framework, and is detailed in this whitepaper, along with how Microsoft uses it in its M365 subscription offerings.

An Overview

The MITRE ATT&CK framework was originally created and deployed by the MITRE Corporation all the way back in 2013, and was a culmination of the Fort Meade Experiment, also known as the "FMX". The key question that was being asked was, and continues to be:

"How well are we doing at detecting documented adversary behavior?"

(SOURCE: 1).

It is an acronym that stands for ***A***dversarial ***T***actics, ***T***echniques, ***and C***ommon ***K***nowledge. It is a knowledge base, or repository that reflects the actual behavior the Cyberattacker intends to take when they launch their specific threat variant. It demonstrates the actual thought process, or the lifecycle that they go through to plan out how they will penetrate the IT/Network Infrastructure of a business.

The Components

There are three major components to the MITRE ATT&CK framework, and they are as follows:

1) The Tactics:

   These are the short-term goals that the Cyberattacker wishes to achieve when they launch their threat variant.

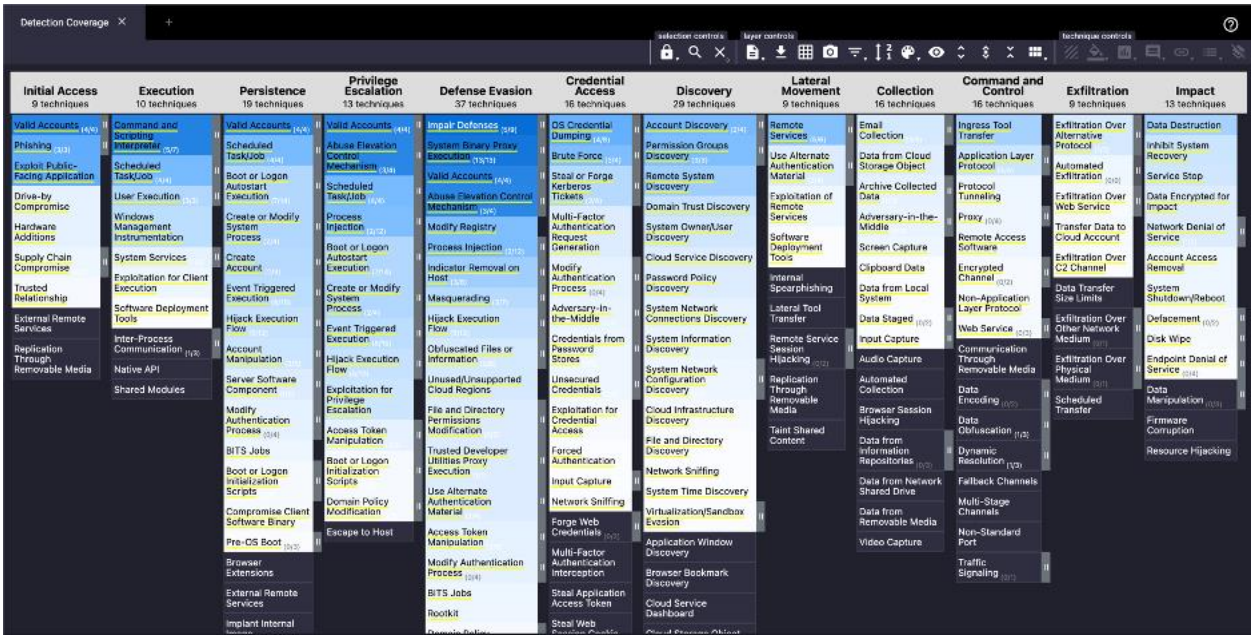
2) The Techniques:

   These are the methodologies in which the Cyberattacker will reach their objectives, through launching and deployment of their specific threat variant.

3) Documentation:

   These are the actual methodologies, or techniques that all kinds of Cyberattacker have used in the past to launch and deploy their specific threat variants.

The above components can be seen in the illustration below:



(SOURCE: 2).

It is important to note the following:

- The columns represent the Tactics.
- The techniques that the Cyberattacker uses are the individual cells in each column.
- The actual methodologies that have been used by the Cyberattacker are linked from the techniques, and they are highlighted in yellow in the above illustration.

This can also be seen at the MITRE ATT&CK framework site, and the link to it is as follows:

MITRE ATT&CK®

An Overview into The Techniques

The techniques from the illustration are detailed below:

1) Reconnaissance:

   This is where the Cyberattacker scouts out and attempts to gather intelligence about the IT/Network Infrastructure of the target.

2) Resource Development:

   This is the phase in which the Cyberattacker establishes the resources that they will need to launch their specific threat variant. For example, this could be a Command-and-Control Center, in which actions can be conducted remotely. This will also make the Cyberattacker invisible to the outside world.

3) Initial Access:

The Cyberattacker now tries to get their first foothold into the IT/Network Infrastructure of the business. This can be done by numerous ways, which include the following:

- Phishing
- Ransomware
- Social Engineering
- Source Code Exploitation
- Trojan Horses
- Any other kind or type of Malicious Payload, especially those created by Generative AI.

4) Execution:

This is where the Malicious Payload is activated by the Cyberattacker. This is very often done remotely, through the Command-and-Control Center that was created in Step #2.

5) Persistence:

In this phase, the Cyberattacker attempts to stay into the IT and Network Infrastructure of the business, without being noticed. They also make attempts to move across, in a lateral based fashion.

6) Privilege Escalation:

Once the Cyberattacker has made enough points of entry, one of their main objectives is to go after the proverbial "Crown Jewels", namely the passwords of the employees. In this regard, one of the most sought-after targets is Privileged Managed Accounts, which represent the super user passwords.

7) Defense Evasion:

The Cyberattacker tries to cover their tracks to a greater extent. This is often accomplished by deploying the malicious payload into the CPU and the memory areas of the device. These are often referred to as "Fileless Attacks".

8) Credential Access:

At this phase, once the Cyberattacker has acquired their initial "Crown Jewels", they will now make the attempt to be much more daring and try other techniques to get to other digital assets. An example here would be to deploy a Keylogger that can record the keystrokes of employees. Not only with they be able to gain additional passwords with this, but they can even build up a profile about their targeted victim.

9) Discovery:

As the Cyberattacker penetrates deeper into the IT and Network Infrastructure of the business, they will now attempt to scope out other parts of it. This will include the Servers, Databases, Intellectual Property, and even the physical assets.

10) Lateral Movement:

This was examined in Step #5. At this point, the Cyberattacker will review the lateral movements that they have used before, and further optimize them.

11) Collection:

Once the Cyberattacker has gained access to some of the "Crown Jewels", they will now make the attempt to try to gain access to other prized possessions from other sources, such as a Private Cloud, Hybrid Cloud, or even in different areas of an On Premises IT and Network Infrastructure.

12) Command And Control:

This was also reviewed in Step #2. Once the first Command and Control Center and it has proven to be successful, they will then at this point attempt to replicate more of them. This is an effort to launch multiple attacks towards the IT and Network Infrastructure of the business. A prime example of this are Distributed Denial of Service (DDoS) attacks. Multiple Command Ans Control Centers are deployed to target hundreds if not thousands of servers all at once.

13) Exfiltration:

The Cyberattacker will now attempt to hijack the Personal Identifiable Information (PII) datasets of customers, employees, and other key stakeholders. The primary goal here is not to steal them all at once, but a bit at a time, so that the business will not realize this until it is too late.

14) Impact:

This is the very last phase of the framework. At this point, once the Cyberattacker has collected all the "Crown Jewels" that they can, the final goal now is to now cause as much damage as possible towards the business. This could be launching a Ransomware Attack, selling the PII datasets on the Dark Web, or even using them to launch an Extortion Attack.

The Three Models of The Framework

At the present time, there are four different models of the MITRE ATT&CK framework. They are as follows:

1) The Enterprise Matrix:

This model focuses upon the motives, intentions, and techniques of the Cyberattacker as it relates to the Enterprise Infrastructure. This is all inclusive model that covers the following:

- Windows Platforms
- Linux Platforms
- MacOS Platforms
- Any kind of IT and Network Infrastructure
- Any kind of Cloud Platforms (such as the AWS and Microsoft Azure)
- All kinds of Containers

2) The Mobile Matrix:

   This model focuses upon the motives, intentions, and techniques of the Cyberattacker as it relates to the Mobile Infrastructure, such as those devices that make use of the iOS and Android Operating Systems.

3) The ICS Matrix:

   This model focuses upon the motives, intentions, and techniques of the Cyberattacker as it relates to the Critical Infrastructure that makes use of Industrial Control Systems. Examples of this include nuclear facilities, the national power grid, the food distribution system, oil and gas pipelines, and the water supply. There is a special emphasis here on the sensors and networks that enable automation.

4) The Cloud Matrix:

   This model focuses upon the motives, intentions, and techniques of the Cyberattacker as it relates to the Cloud Deployments, most notable of the Google Cloud Platform (GCP), the AWS, and Microsoft Azure.

Use Cases of The Framework

The question at this point often gets asked is: "How can one use the MITRE ATT&CK framework"? Here are some actual use cases:

1) Emulation:

   Along with using tools such as Generative AI, the framework can also be used accurately to predict what a Cyberattacker could potentially do in the future. From this, various "what if" scenarios can be created.

2) Penetration Testing:

   Given the breadth and scope of the framework, it can also be quite applicable to the Red Team, as they try to get into the mindset of a Cyberattacker when they do their Penetration Testing exercises.

3) Behavioral Patterns:

   Since the core of the framework is centered around understanding the intent and motives of the Cyberattacker, it can also be used to help create a profile of their behavioral patterns.

4) Risk Assessment:

   To varying degrees, the framework can also be used by the CISO and their IT Security team to gauge the degree of vulnerability of both the physical and digital assets that their business contains.

5) SOC:

This is an acronym that stands for the "Secure Operations Center". In this regard, the framework can also be used to see just how responsive the team that operates this is in detecting and responding to a threat variant.

6) Threat Hunting and Research:

   The framework can also give a wealth of information and knowledge to not only Threat Hunters, but to Threat Researchers also, as they model future attack vectors based on previous signature profiles.

The Framework and M365

As it has been highlighted throughout this whitepaper, the MITRE ATT&CK framework is a very well established and widely used methodology to map out in detail how the Cyberattacker will launch their next threat variant.

Many companies have and are continuing this framework. A great example of this is Microsoft, and how they deployed the M365 subscription. In this regard, the following offerings are mapped to the MITRE ATT&CK framework:

1) Microsoft 365 Defender, XDR, and Office 365:

   This is an all-encompassing security mechanism that does the following:

   - Detection
   - Prevention
   - Investigation
   - Response to all the identities, tenants, email, and all software applications that reside in M365 subscription.

2) Microsoft Entra ID:

   This is formerly known as Azure Active Director, or AAD for short. It is primarily available in Microsoft Azure and uses the concepts of the MITRE ATT&CK framework to provide Identity and Access Management (also known as IAM) services to manage employee profiles, and the rights, privileges, and permissions that they must access the resources from within Microsoft Azure.

3) Microsoft Exchange Online Protection:

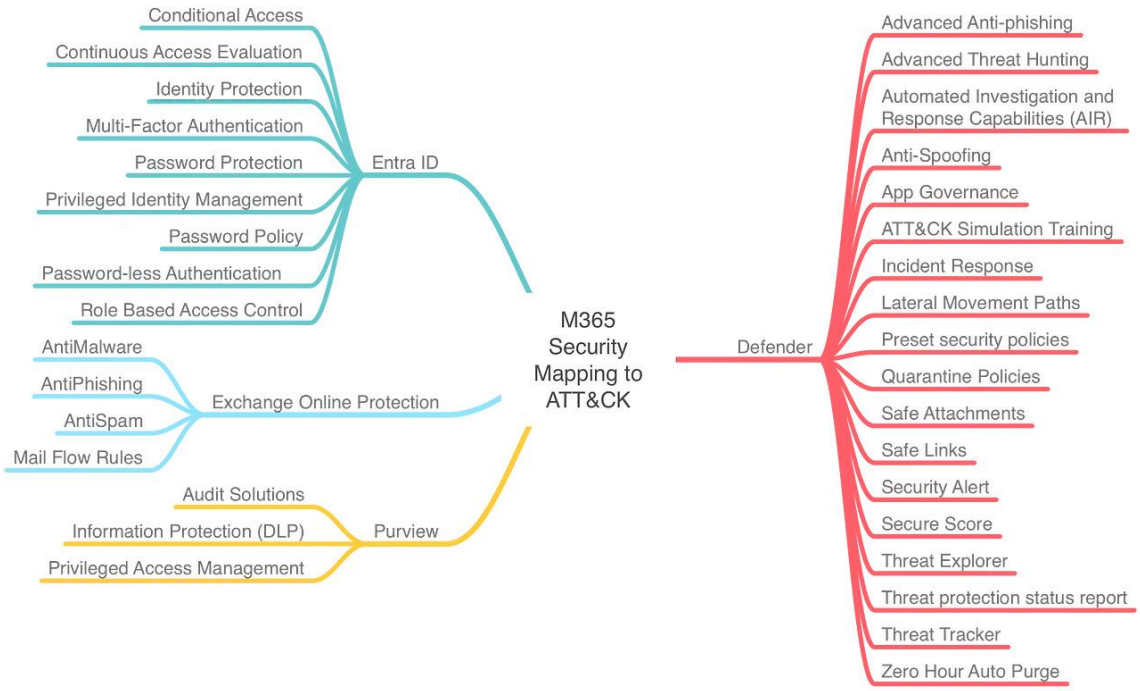
   This is a package that provides all kinds of protection from emails coming in or out of Microsoft Exchange. This includes the following:

   - Spam
   - Malware
   - Phishing
   - Other threats variants, such as rogue attachments and malicious links.

4) Microsoft Purview:

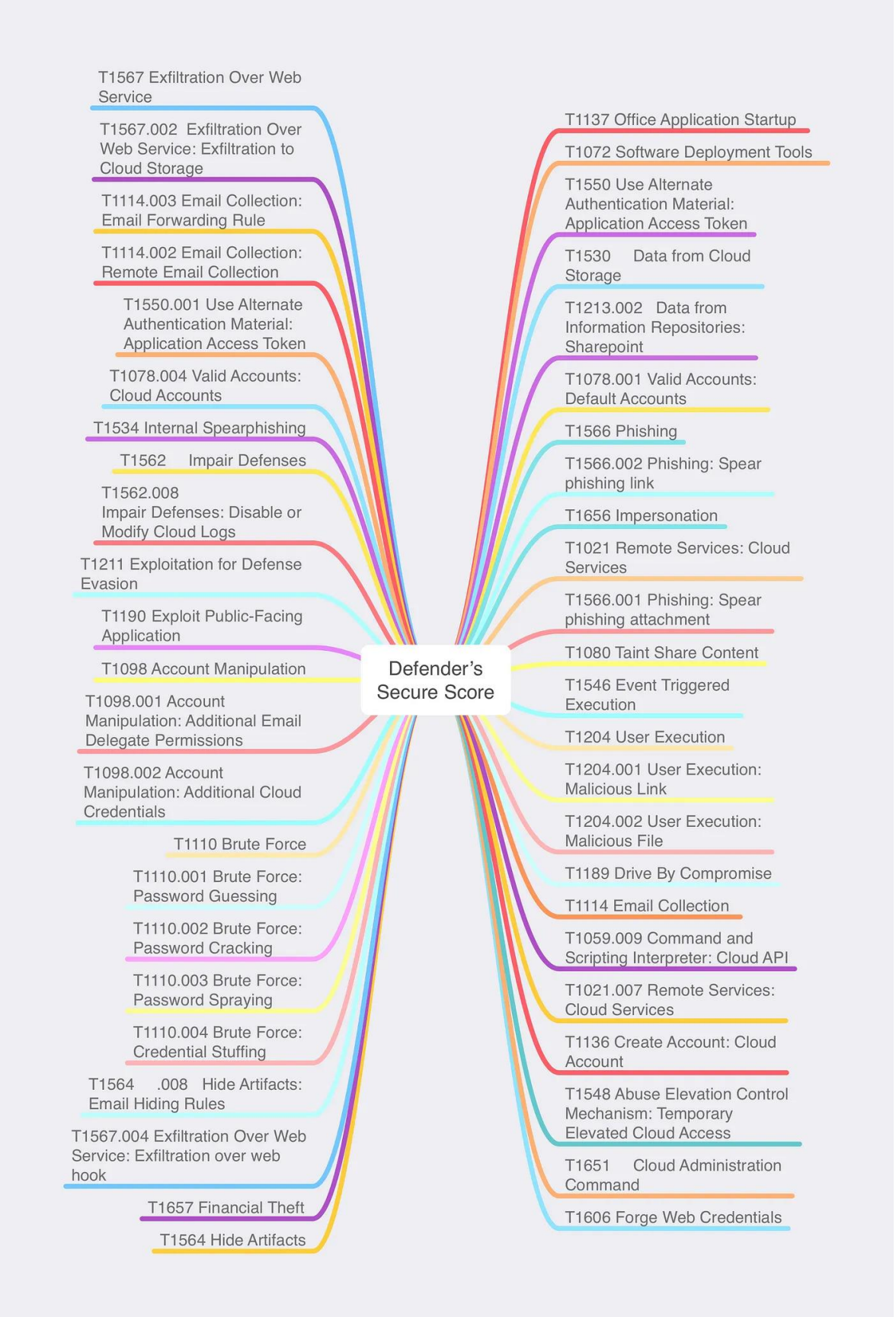
This is a governance platform that comes with most M365 subscriptions. By following the concepts of the MITRE ATT&CK framework, any business can come into compliance with the major data privacy laws of the GDRP, CCPA, HIPAA, etc.

The mappings of the Entra ID, Exchange Online Protection, and Purview platforms to the MITRE ATT&ACK framework are illustrated in the diagram below:



(SOURCE: 4).

The mappings of the Defender platform to the MITRE ATT&ACK framework are illustrated in the diagram below:


Defender's Secure Score
T1567 Exfiltration Over Web Service
T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage
T1114.003 Email Collection: Email Forwarding Rule
T1114.002 Email Collection: Remote Email Collection
T1550.001 Use Alternate Authentication Material: Application Access Token
T1078.004 Valid Accounts: Cloud Accounts
T1534 Internal Spearphishing
T1562 Impair Defenses
T1562.008 Impair Defenses: Disable or Modify Cloud Logs
T1211 Exploitation for Defense Evasion
T1190 Exploit Public-Facing Application
T1098 Account Manipulation
T1098.001 Account Manipulation: Additional Email Delegate Permissions
T1098.002 Account Manipulation: Additional Cloud Credentials
T1110 Brute Force
T1110.001 Brute Force: Password Guessing
T1110.002 Brute Force: Password Cracking
T1110.003 Brute Force: Password Spraying
T1110.004 Brute Force: Credential Stuffing
T1564 .008 Hide Artifacts: Email Hiding Rules
T1567.004 Exfiltration Over Web Service: Exfiltration over web hook
T1657 Financial Theft
T1564 Hide Artifacts
T1137 Office Application Startup
T1072 Software Deployment Tools
T1550 Use Alternate Authentication Material: Application Access Token
T1530 Data from Cloud Storage
T1213.002 Data from Information Repositories: Sharepoint
T1078.001 Valid Accounts: Default Accounts
T1566 Phishing
T1566.002 Phishing: Spear phishing link
T1656 Impersonation
T1021 Remote Services: Cloud Services
T1566.001 Phishing: Spear phishing attachment
T1080 Taint Share Content
T1546 Event Triggered Execution
T1204 User Execution
T1204.001 User Execution: Malicious Link
T1204.002 User Execution: Malicious File
T1189 Drive By Compromise
T1114 Email Collection
T1059.009 Command and Scripting Interpreter: Cloud API
T1021.007 Remote Services: Cloud Services
T1136 Create Account: Cloud Account
T1548 Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access
T1651 Cloud Administration Command
T1606 Forge Web Credentials

(SOURCE: 4).

The Framework and Microsoft Defender

In this section of the whitepaper, we do a deeper dive as to how the MITRE ATT&CK framework can be used in conjunction with Microsoft Sentinel. Although this was reviewed in the last section, it is important to provide a technical definition of what this platform is all about. It is as follows:

"Microsoft Sentinel analyzes ingested data, not only to detect threats and help you investigate, but also to visualize the nature and coverage of your organization's security status."

(SOURCE: View MITRE coverage for your organization from Microsoft Sentinel | Microsoft Learn)

But before you can do this, you first need to have the following components:

- An active instance of Microsoft Sentinel.
- Have the needed permissions to view the required content in Microsoft Sentinel. For more information on how to do this, visit the link below:

  View MITRE coverage for your organization from Microsoft Sentinel | Microsoft Learn

- The required data connectors to "ingest" information and data into Microsoft Sentinel. For more information on how to do this, visit the link below:

  Microsoft Sentinel data connectors | Microsoft Learn

- The needed rules and queries so that the required information and data can be pulled as and when needed.
- A working knowledge of the MITRE ATT&CK framework, especially how it relates to the tactics and techniques of the Cyberattacker.

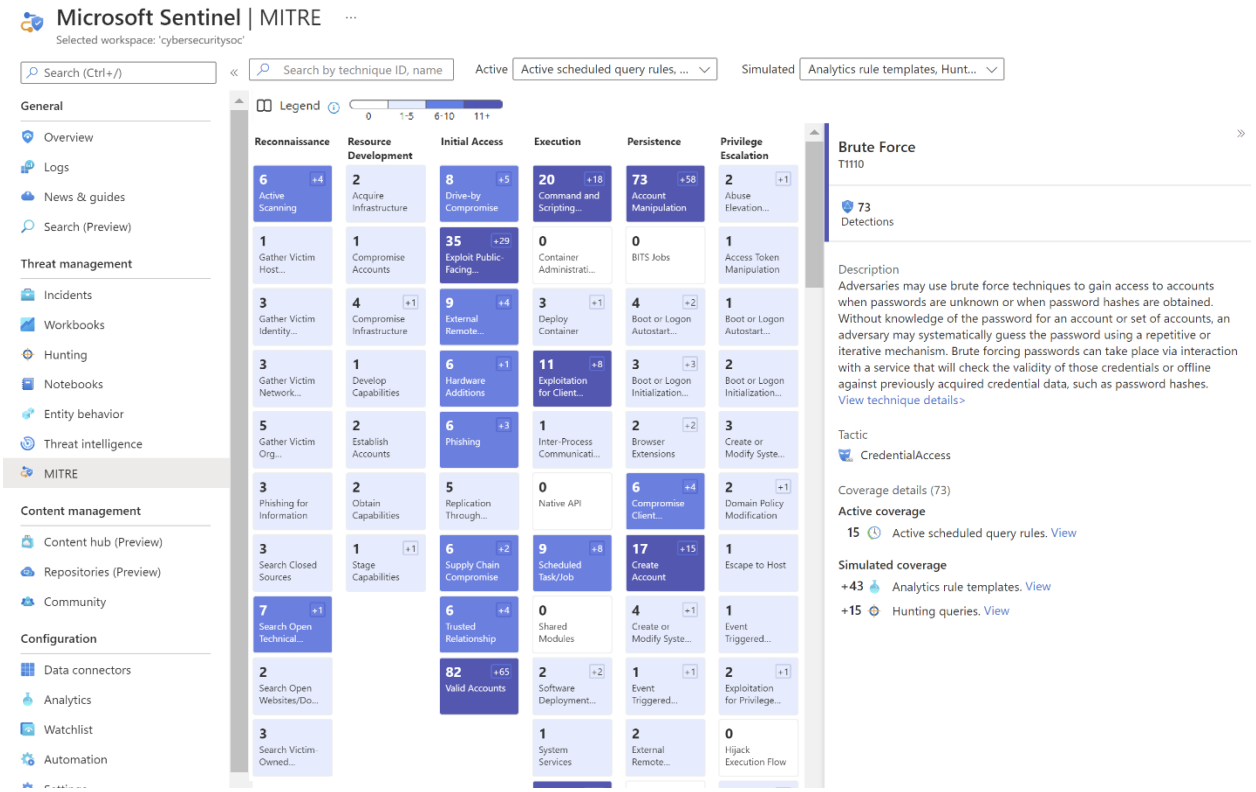
How To Access the Framework

To access the framework in Microsoft Sentinel, follow these steps:

1) To access Microsoft Sentinel, log into your Azure Portal at:

   portal.azure.com

2) Hover to "Threat Management", and from there select "MITRE ATTA&CK (Preview)". This is illustrated in the diagram below:



(SOURCE: 5).

3) Once the last step has been accomplished, there are several things you can do, which include the following:

- <u>The Legend</u>:

  Use this to see how many threat variants are being detected.

- <u>The Search Bar</u>:

  Use this to find a certain technique in the MITRE ATT&CK framework. You can query for this by either the name of the technique, its ID number, or even both.

- <u>The Specific Technique</u>:

  Use this to get all the details about what you just queried for in the last step. You can even click on any of the links to see how this specific is accessible in Microsoft Sentinel.

The Use of Simulated Coverage

Simulated Coverage is technically defined as follows:

"Simulated Coverage refers to detections that are available, but not currently configured in your Microsoft Sentinel workspace."

(SOURCE: 5).

With this functionality, you can get a firsthand view as to the security posture of your business. To accomplish this task, follow these steps:

1) To access Microsoft Sentinel, log into your Azure Portal at:

   portal.azure.com

2) Go to "Threat Management".

3) Select "MITRE ATTA&CK (Preview)".

4) Select the Simulated Coverages that you want to view by selecting "Simulated Rules".

5) Select the elements that you want to incorporate into your Simulated Coverages.

Creating Rules

From Microsoft Sentinel, you can also create rules to further customize the security posture for your organization. The following rules can be created:

1) Analytics Rules:

   You can create all sorts of data to see how your business is faring on the Cybersecurity Threat Landscape. For more information on how to do this, access the link below:

   Create scheduled analytics rules in Microsoft Sentinel | Microsoft Learn

2) Incidents:

   You can create various kinds and types of alerts and warnings for any impending threat variants that are inbound to your business, which utilizes the MITRE ATT&CK framework. For more information on how to do this, access the links below:

   Investigate incidents with Microsoft Sentinel (legacy) | Microsoft Learn

   Investigate incidents in the Microsoft Defender portal - Microsoft Defender XDR | Microsoft Learn

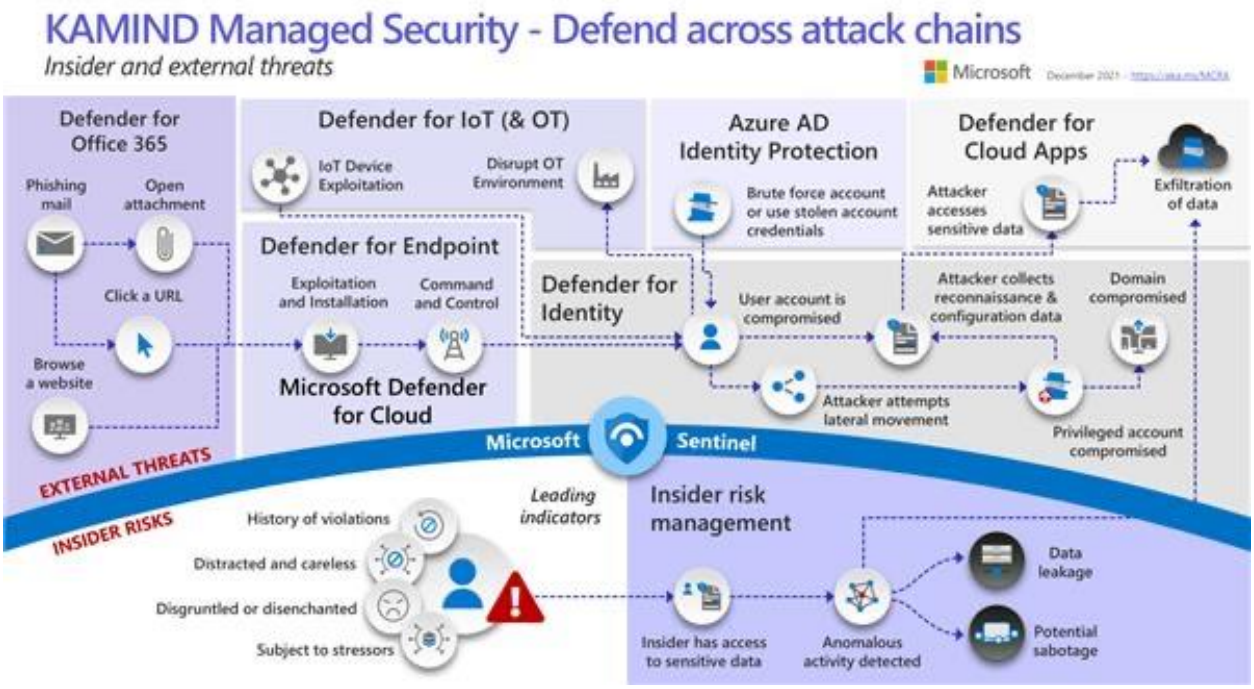
3) Threat Hunting:

   Before you launch a Threat Hunting exercise, you can also create distinct kinds of rules to determine which specific threat variant that you need to focus on, using the information that is already provided by the MITRE ATT&CK framework. For more information on how to do this, access the links below:

   Hunting capabilities in Microsoft Sentinel | Microsoft Learn

   Hunt with bookmarks in Microsoft Sentinel | Microsoft Learn

At KAMIND IT, Inc., we have specially configured the deployment of the MITRE ATT&CK framework into Microsoft Sentinel. This is illustrated in the diagram below:



(SOURCE: 6).

Conclusions

At KAMIND IT, Inc., when we have discussions about the MITRE ATT&CK framework with our customers, we believe in taking what is known as “End to End Approach”. This simply means that all points in their entire IT and Network Infrastructure are protected, ranging from whether it is On Premises or in Microsoft Azure, to all the servers and devices which serve as the endpoints.

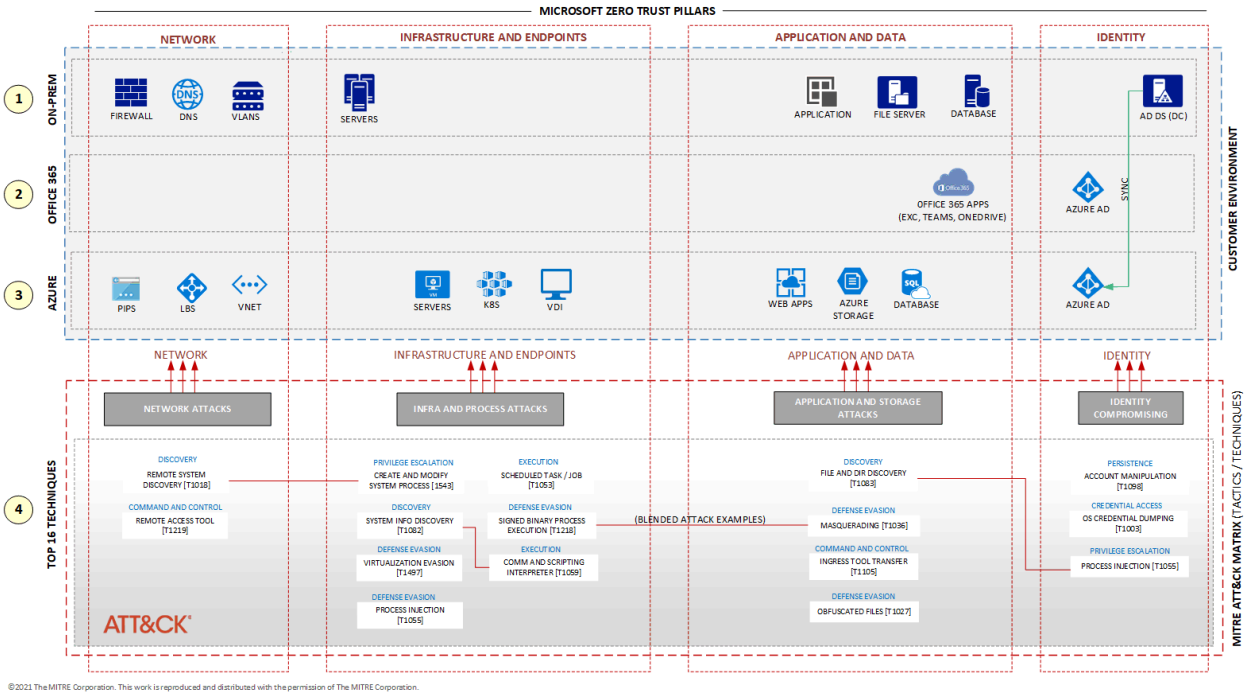
To accomplish this task, we utilize what is known as the Zero Trust Approach. This involves segmenting out the entire IT and Network Infrastructure into different zones, each protected by Multifactor Authentication (MFA). There are two primary objectives with this kind of approach:

- The identity of all end users is confirmed by at least three or more differing authenticating mechanisms. This is in observation for this cardinal rule in Cybersecurity:

  “Never Trust, Always Verify”

- By having different zones, many additional layers of security are added, so that the statistical chances of the Cyberattacker breaking through all of them is almost 0%.

This approach is illustrated in the diagram below:



(SOURCE: 7).

Finally, if you have any questions or need help in deploying the MITRE&CK framework into your security posture, contact us today.

Sources

1) What Is the MITRE ATT&CK Framework? | Get the 101 Guide | Trellix
2) Assessing and expanding MITRE ATT&CK coverage in Splunk Enterprise Security - Splunk Lantern
3) What is the MITRE ATT&CK Framework? | IBM
4) M365 security capabilities mapped to MITRE ATT&CK | Center for Threat-Informed Defense
5) View MITRE coverage for your organization from Microsoft Sentinel | Microsoft Learn
6) Portland Managed Cybersecurity Services | KAMIND IT
7) Map threats to your IT environment - Azure Architecture Center | Microsoft Learn