MITRE

MITRE

This room will discuss the various resources MITRE has made available for the cybersecurity community.

Task 1 Introduction to MITRE

For those that are new to the cybersecurity field, you probably never heard of MITRE. Those of us that have been around *might* only associate MITRE with CVEs (**Common Vulnerabilities and Exposures**) list, which is one resource you'll probably check when searching for an exploit for a given vulnerability. But MITRE researches in many areas, outside of cybersecurity, for the 'safety, stability, and well-being of our nation.' These areas include artificial intelligence, health informatics, space security, to name a few.

From **Mitre.org**: "*At MITRE, we solve problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.*"

In this room, we will focus on other projects/research that the US-based non-profit MITRE Corporation has created for the cybersecurity community, specifically:

- ATT&CK® (**Adversarial Tactics, Techniques, and Common Knowledge**) Framework
- CAR (**Cyber Analytics Repository**) Knowledge Base
- SHIELD (sorry, not a fancy acronym) Active Defense
- AEP (**ATT&CK Emulation Plans**)

Let's dive in, shall we...

#1	**Read the above**

No answer needed

Task 2 Basic Terminology

Before diving in, let's briefly discuss a few terms that you will often hear when dealing with the framework, threat intelligence, etc.

APT is an acronym for **Advanced Persistent Threat**. This can be considered a team/group (***threat group***), or even country (***nation-state group***), that engages in long-term attacks against organizations and/or countries. The term 'advanced' can be misleading as it will tend to cause us to believe that each APT group all have some super-weapon, e.i. a zero-day exploit, that they use. That is not the case. As we will see a bit later, the techniques these APT groups use are quite common and can be detected with the right implementations in place. You can view FireEye's current list of APT groups **here**.

TTP is an acronym for **Tactics, Techniques, and Procedures,** but what does each of these terms mean?

- The **Tactic** is the adversary's goal or objective.
- The **Technique** is how the adversary achieves the goal or objective.
- The **Procedure** is how the technique is executed.

If that is not that clear now, don't worry. Hopefully, as you progress through each section, TTPs will make more sense.

#1	**Read the above**

No answer needed

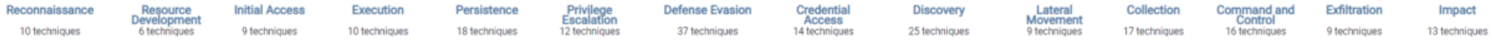
Task 3 ATT&CK® Framework

What is the ATT&CK® framework? According to the **website**, "MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations." In 2013, MITRE began to address the need to record and document common TTPs (**Tactics, Techniques, and Procedures**) that APT (**Advanced Persistent Threat**) groups used against enterprise Windows networks. This started with an internal project known as FMX (**Fort Meade Experiment**). Within this project, selected security professionals were tasked to emulated adversarial TTPs against a network, and data was collected from the attacks on this network. The gathered data helped construct the beginning pieces of what we know today as the ATT&CK® framework.

The ATT&CK® framework has grown and expanded throughout the years. One notable expansion was that the framework focused solely on the Windows platform but has expanded to cover other platforms, such as macOS and Linux. The framework is heavily contributed to by many sources, such as security researchers and threat intelligence reports. Note this is not only a tool for blue teamers. The tool is also useful for a penetration tester and/or red teamer.

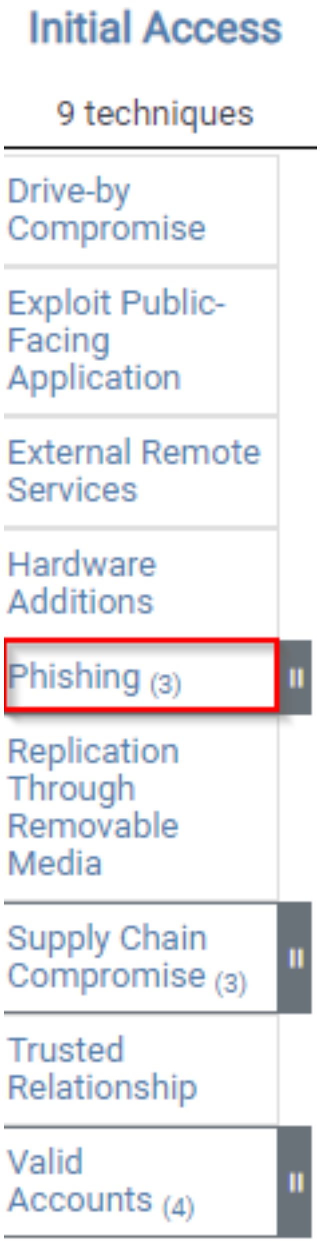
If you haven't done so, navigate to the ATT&CK® **website**.

Direct your attention to the bottom of the page to view the **ATT&CK® Matrix for Enterprise**. Across the top of the matrix, there are 14 categories. Each category contains the techniques an adversary could use to perform the tactic. The categories cover the seven-stage Cyber Attack Lifecycle (credit Lockheed Martin for the Cyber Kill Chain).

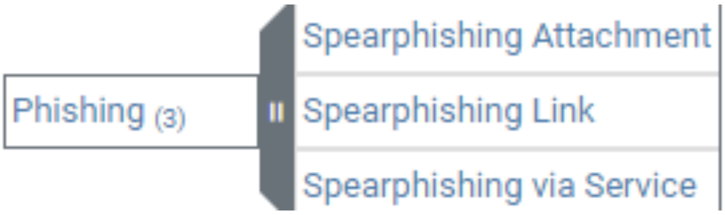


Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques

Under **Initial Access**, there are 9 techniques. Some of the techniques have sub-techniques, such as Phishing.

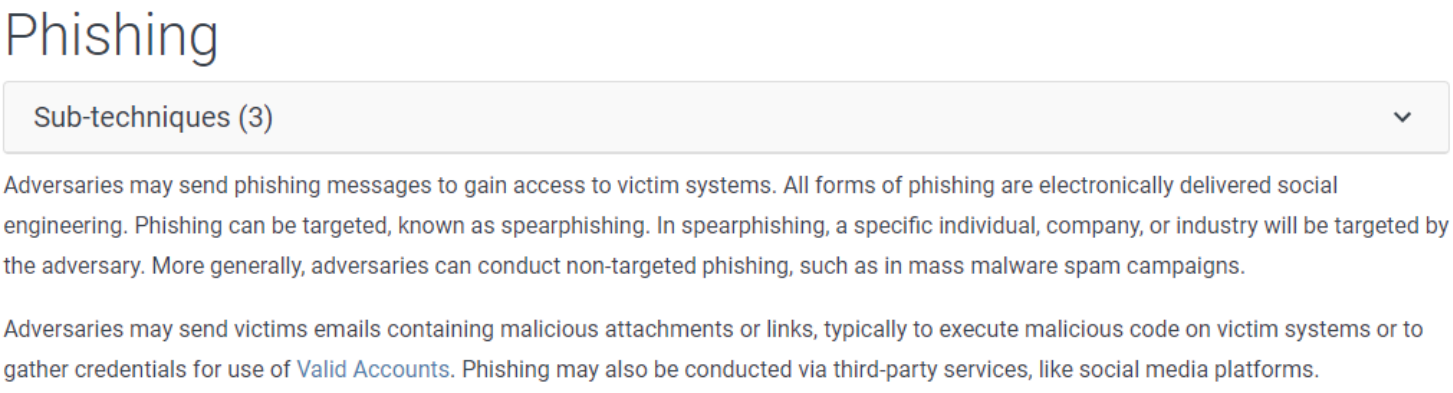


If we click on the gray bar to the right, a new layer appears listing the sub-techniques.



To get a better understanding of this technique and it's associated sub-techniques, click on Phishing.

We have been directed to a page dedicated to the technique known as Phishing and all related information regarding the technique, such as a brief description, **Procedure Examples**, and **Mitigations**.



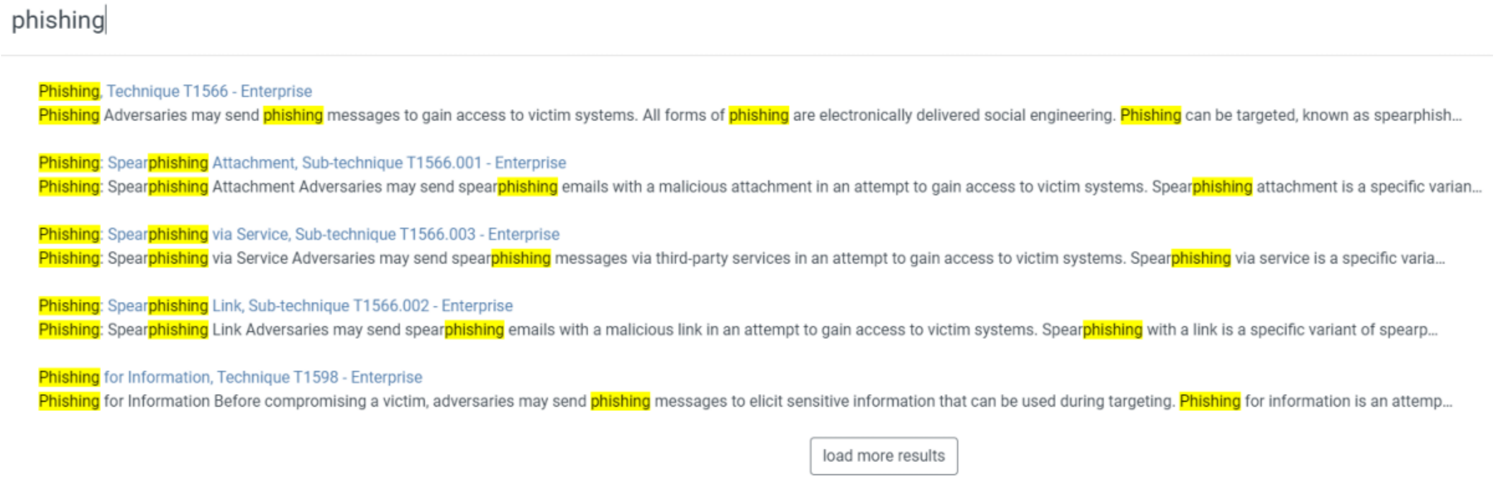
Phishing

Sub-techniques (3)

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems or to gather credentials for use of Valid Accounts. Phishing may also be conducted via third-party services, like social media platforms.

You can alternatively resort to using the Search feature to retrieve all associated information regarding a given technique, sub-technique, and/or group.



phishing

Phishing, Technique T1566 - Enterprise
Phishing Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphish...

Phishing: Spearphishing Attachment, Sub-technique T1566.001 - Enterprise
Phishing: Spearphishing Attachment Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific varian...

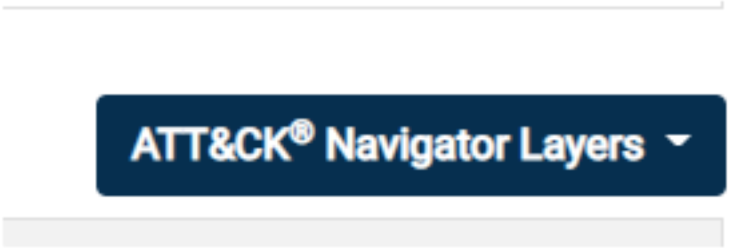
Phishing: Spearphishing via Service, Sub-technique T1566.003 - Enterprise
Phishing: Spearphishing via Service Adversaries may send spearphishing messages via third-party services in an attempt to gain access to victim systems. Spearphishing via service is a specific varia...

Phishing: Spearphishing Link, Sub-technique T1566.002 - Enterprise
Phishing: Spearphishing Link Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearp...

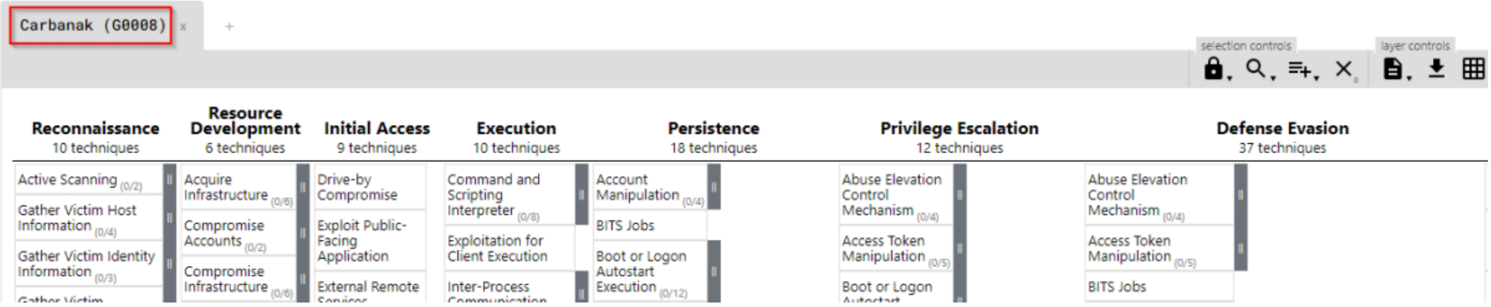
Phishing for Information, Technique T1598 - Enterprise
Phishing for Information Before compromising a victim, adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attemp...

Lastly, the same data can be viewed via the **MITRE ATT&CK® Navigator**: "*The ATT&CK® Navigator is designed to provide basic navigation and annotation of ATT&CK® matrices, something that people are already doing today in tools like Excel. We've designed it to be simple and generic - you can use the Navigator to visualize your defensive coverage, your red/blue team planning, the frequency of detected techniques, or anything else you want to do.*"

You can access the Navigator view when visiting a group or tool page. The ATT&CK® Navigator Layers button will be available.



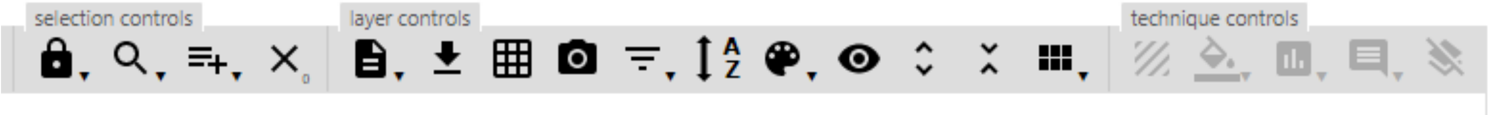
In the sub-menu select **view**.



Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote	Inter-Process	Boot or Logon Autostart Execution (0/12)	Boot or Logon	BITS Jobs
Gather Victim						

Let's get acquainted with this tool. Click **here** to view the ATT&CK® Navigator for Carbanak.

At the top left, there are 3 sets of controls: **selection controls**, **layer controls**, and **technique controls**. I encourage you to inspect each of the options under each control to get familiar with them. The question mark at the far right will provide additional information regarding the navigator.



To summarize, we can use the ATT&CK Matrix to map a threat group to their tactics and techniques. There are various methods the search can be initiated. The questions below will help you become more familiar with the ATT&CK®. It is recommended to start answering the questions from the **Phishing page**.

#1	**Only blue teamers will use the ATT&CK Matrix? (Yay/Nay)**

Nay

#2	**What is the ID for this technique?**

T1566

#3	**Based on this technique, what mitigation covers identifying social engineering techniques?**

User Training

#4	**There are other possible areas for detection for this technique, which occurs after what other technique?**

User Execution

#5	**What group has used spear phishing in their campaigns?**

Dragonfly

#6	**Based on the information for this group, what are their associated groups?**

TG-4192, Crouching Yeti, IRON LIBERTY, Energetic Bear

#7	**What tool is attributed to this group to transfer tools or files from one host to another within a compromised environment?**

PsExec

#8	**Based on the information about this tool, what group used a customized version of it?**

FIN5

#9	This group has been active since what year?

2008

#10	Instead of Mimikatz, what OS Credential Dumping tool is does this group use?

Windows Credential Editor

Task 4 CAR Knowledge Base

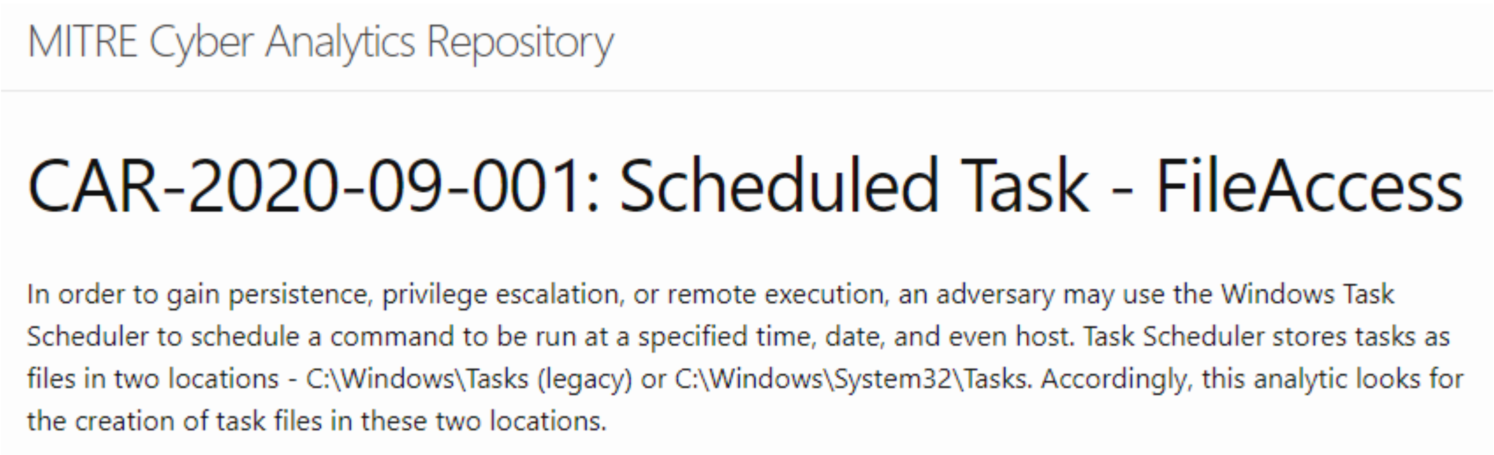
Cyber Analytics Repository

The official definition of **CAR** is "*The MITRE Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the MITRE ATT&CK® adversary model. CAR defines a data model that is leveraged in its pseudocode representations but also includes implementations directly targeted at specific tools (e.g., Splunk, EQL) in its analytics. With respect to coverage, CAR is focused on providing a set of validated and well-explained analytics, in particular with regards to their operating theory and rationale.*"

Instead of further attempting to explain what CAR is, let's dive in. With our newly acquired knowledge from the previous section, we should feel comfortable and understand the information that CAR is providing to us.

Let's begin our journey by reviewing **CAR-2020-09-001: Scheduled Task - File Access**.

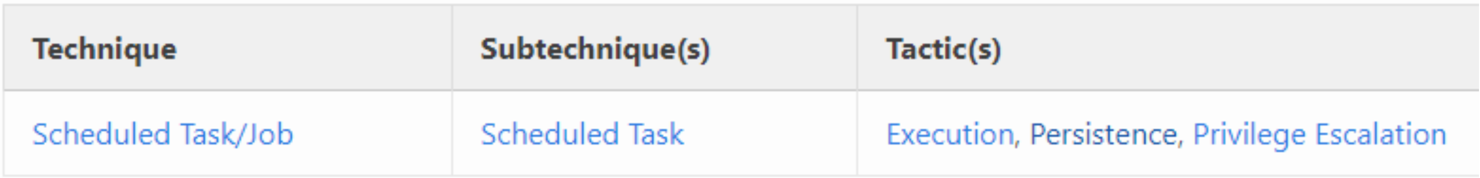
Upon visiting the page, we're given a brief description of the analytic and references to ATT&CK (**technique**, **sub-technique**, and **tactic**).



MITRE Cyber Analytics Repository

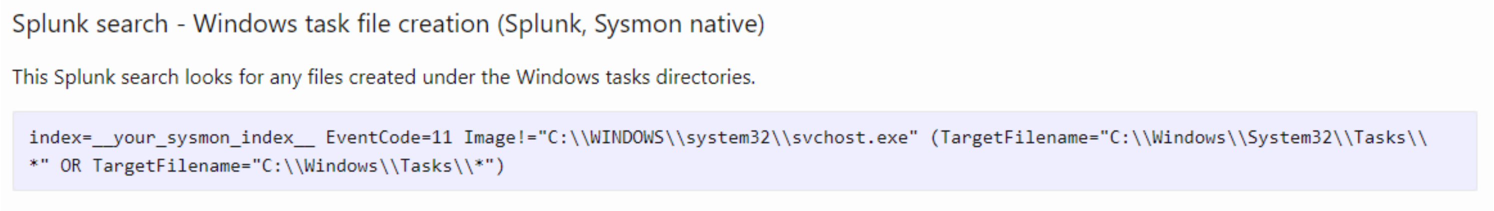
CAR-2020-09-001: Scheduled Task - FileAccess

In order to gain persistence, privilege escalation, or remote execution, an adversary may use the Windows Task Scheduler to schedule a command to be run at a specified time, date, and even host. Task Scheduler stores tasks as files in two locations - C:\Windows\Tasks (legacy) or C:\Windows\System32\Tasks. Accordingly, this analytic looks for the creation of task files in these two locations.



Technique	Subtechnique(s)	Tactic(s)
Scheduled Task/Job	Scheduled Task	Execution, Persistence, Privilege Escalation

We're also provided with Pseudocode and a query on how to search for this specific analytic within Splunk. A pseudocode is a plain, human-readable way to describe a set of instructions or algorithms that a program or system will perform.



Splunk search - Windows task file creation (Splunk, Sysmon native)

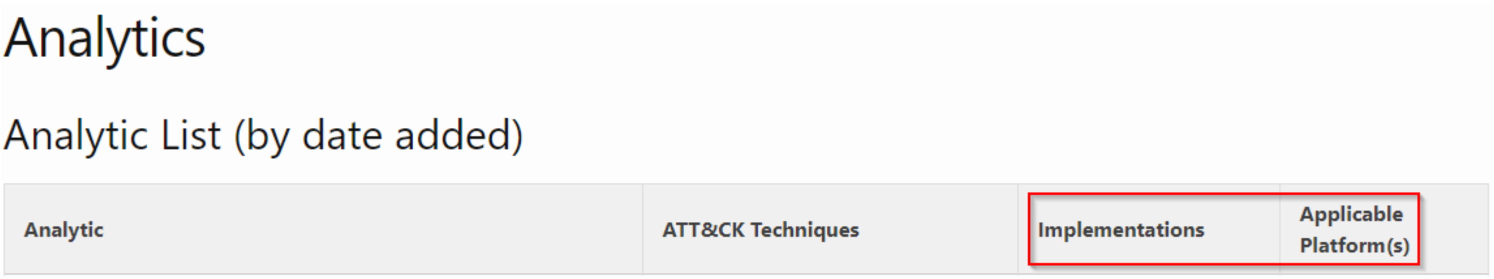
This Splunk search looks for any files created under the Windows tasks directories.

```
index=__your_sysmon_index__ EventCode=11 Image!="C:\\WINDOWS\\system32\\svchost.exe" (TargetFilename="C:\\Windows\\System32\\Tasks\\
*" OR TargetFilename="C:\\Windows\\Tasks\\*")
```

Note the reference to Sysmon. We have not covered Sysmon as of yet, but you can read more about this tool **here**.

To take full advantage of CAR, we can view the **Full Analytic List** or the **CAR ATT&CK® Navigator layer** to view all the analytics.

Full Analytic List



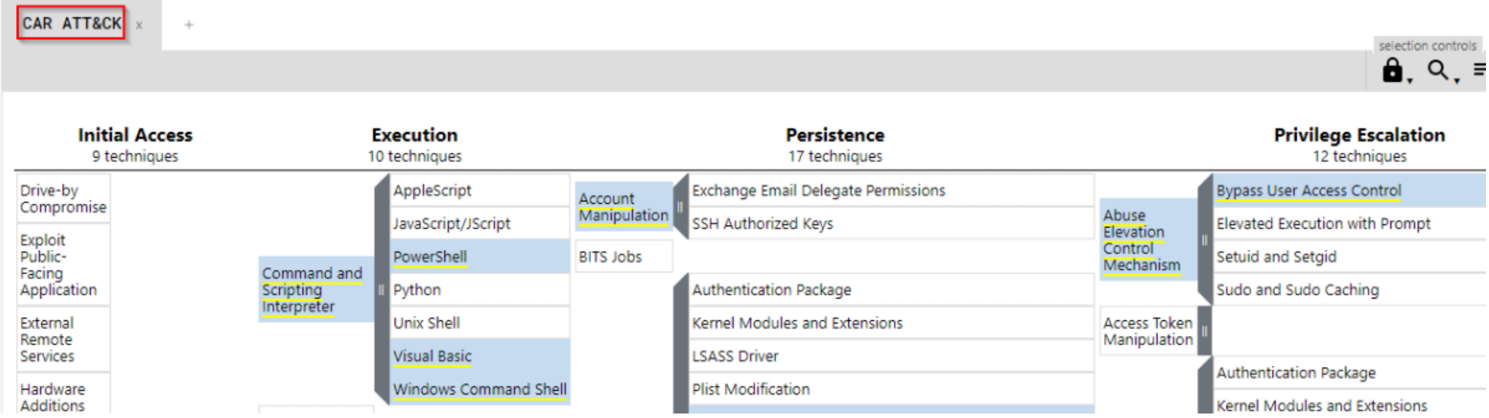
Analytics

Analytic List (by date added)

Analytic	ATT&CK Techniques	Implementations	Applicable Platform(s)

In the Full Analytic List view, we can see what implementations are available for any given analytic at a single glance, along with what OS platform it applies to.

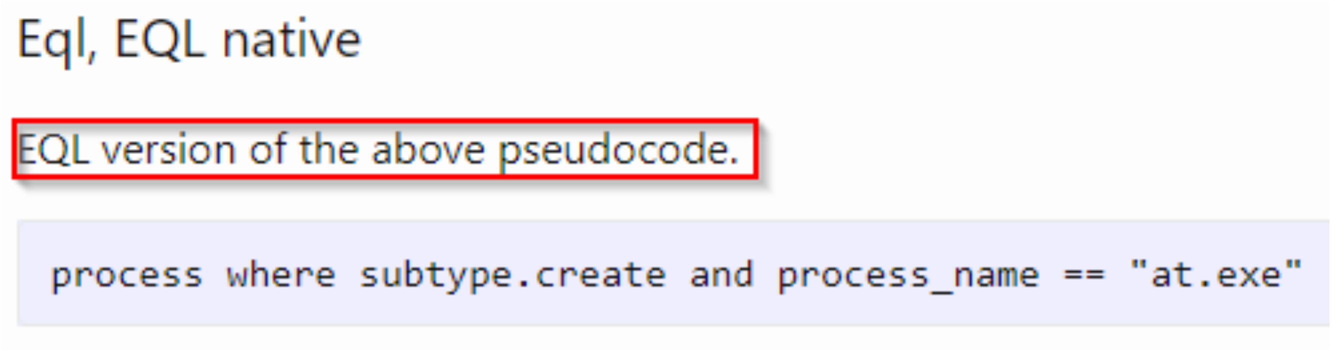
CAR ATTACK Navigator



(The techniques highlighted in blue are the analytics currently in CAR)

Let's look at another analytic to see a different implementation, **CAR-2014-11-004: Remote PowerShell Sessions**.

Under Implementations, pseudocode is provided and an EQL version of the pseudocode. EQL (pronounced as 'equal'), and it's an acronym for Event Query Language. EQL can be utilized to query, parse, and organize Sysmon event data. You can read more about this **here**.



Eql, EQL native

EQL version of the above pseudocode.

```
process where subtype.create and process_name == "at.exe"
```

To summarize, CAR is a great place for finding analytics that takes us further than the Mitigation and Detection summaries in the ATT&CK® framework. This tool is not a replacement for ATT&CK® but an added resource.

#1	**For the above analytic, what is the pseudocode a representati-on of?**

splunk search

#2	**What tactic has an ID of TA0003?**

persistence

#3	What is the name of the library that is a collection of Zeek (BRO) scripts?

BZAR

#4	What is the name of the technique for running executables with the same hash and different names?

Masquerading

#5	Examine CAR-2013-05-004, what additional information is provided to analysts to ensure coverage for this technique?

Unit Tests

Task 5 Shield Active Defense

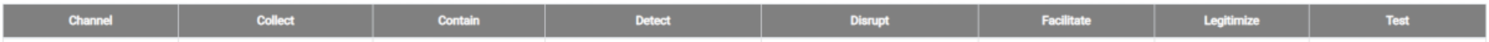
MITRE | SHIELD

Per the website, "*Shield is an active defense knowledge base MITRE is developing to capture and organize what we are learning about active defense and adversary engagement. Derived from over 10 years of adversary engagement experience, it spans the range from high level, CISO ready considerations of opportunities and objectives, to practitioner friendly discussions of the TTPs available to defenders.*"

The U.S. Department of Defense defines **active defense** as "*The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.*"

Shield Active Defense is similar to the ATT&CK® Matrix, but the tactics and techniques provided to us enable us to trap and/or engage (with) an adversary active within the network. For example, we can plant decoy credentials on a resource and monitor if/when the account's credentials are used elsewhere within the network. By doing this, we are alerted to the adversary's presence and provides the opportunity to learn about their tools and tactics. The information that is gathered can be classified as **threat intelligence**.

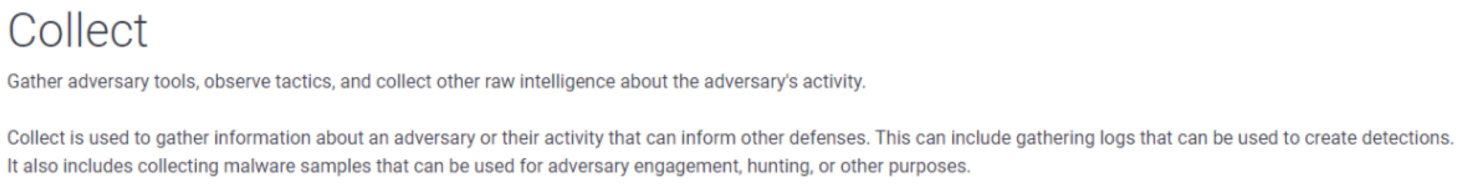
If you haven't done so, navigate to the Shield **website**. Across the Shield (Active Defense Matrix) top are the tactics, similar to the ATT&CK® Matrix.



Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	Test

Each column will list the techniques associated with each tactic (again, as the ATT&CK® Matrix). By clicking on any column headers, we will be redirected to a page providing more information.

Let's click on **Collect**. At this point, we should already be familiar with how MITRE displays the information to us. Here we see a brief definition of tactic, Collect, and associated ID along with the list of techniques, each with a brief description.

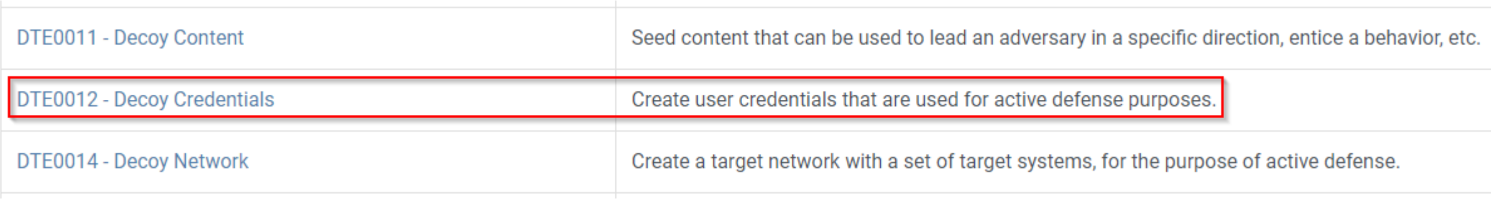


Collect

Gather adversary tools, observe tactics, and collect other raw intelligence about the adversary's activity.

Collect is used to gather information about an adversary or their activity that can inform other defenses. This can include gathering logs that can be used to create detections. It also includes collecting malware samples that can be used for adversary engagement, hunting, or other purposes.

Click on **DTE0012 - Decoy Credentials**.



DTE0011 - Decoy Content	Seed content that can be used to lead an adversary in a specific direction, entice a behavior, etc.
DTE0012 - Decoy Credentials	Create user credentials that are used for active defense purposes.
DTE0014 - Decoy Network	Create a target network with a set of target systems, for the purpose of active defense.

Aside from the summary, we are provided with **Opportunities**, **Use Cases**, and **Procedures** to perform this technique. Also, note that this technique maps to other Shield tactics (*yes, I will repeat it - this is also the case with the ATT&CK® Matrix*). Finally, at the bottom is listed the **ATT&CK® Techniques** associated with this Shield Technique.

Exploring the navigation options across the top links are provided to us to view the Shield Tactics and Techniques as individual pages. This view is good if you want a summary of each at a glance.

Under **ATT&CK® Mapping Overview** (in our case) for Initial Access [TA0001], the table lists the ATT&CK® Techniques and hints (**opportunities**) on how to use the suggestive Active Defense Technique in our environment.
That should be enough of an overview. Now to practice using this tool by answering the questions below.

#1	**Which Shield tactic has the most techniques?**

detect

#2	**Is the technique 'Decoy Credentials' listed under the tactic from question #1? (Yay/-Nay)**

Yay

#3	**Explore DTE0011, what is the ID for the use case where a defender can plant artifacts on a system to make it look like a virtual machine to the adversary?**

DUC0234

#4	**Based on the above use case, what is its ATT&CK® Technique mapping?**

T1497

#5	**Continuing from the previous question, look at the information for this ATT&CK® Technique, what 2 programs are listed that adversary's will check for?**

Sysinternals and Wireshark

Task 6 ATT&CK® Emulation Plans

If these tools provided to us by MITRE are not enough, under **MITRE ENGENUITY**, we have **CTID**, the **Adversary Emulation Library**, and **ATT&CK® Emulation Plans**.

CITD
MITRE formed an organization named The **Center of Threat-Informed Defense** (**CTID**). This organization consists of various companies and vendors from around the globe. Their objective is to conduct research on cyber threats and their TTPs and share this research to improve cyber defense for all.
Some of the companies and vendors who are participants of CTID:

- AttackIQ
- Verizon
- Microsoft
- Red Canary
- Splunk

Per the website, "*Our goal is to change the game on adversaries by relentlessly improving our collective ability to prevent, detect, and respond to cyber attacks.*"

Adversary Emulation Library & ATT&CK® Emulations Plans
The **Adversary Emulation Library** is a public library making adversary emulation plans a free resource for blue/red teamers. The library and the emulations are a contribution from CTID. There are 3 **ATT&CK® Emulation Plans** currently available: **APT3**, **APT29**, and **FIN6**. The next ATT&CK® Emulation in the pipeline is **FIN7**. The emulation plans are a step-by-step guide on how to mimic the specific threat group. If any of the C-Suite were to ask, "how would we fare if APT29 hits us?" This can easily be answered by referring to the results of the execution of the emulation plan.

Review the emulation plans to answer the questions below.

#1	**How many phases does APT3 Emulation Plan consists of?**

3

#2	**Under Persistence, what binary was replaced with cmd.exe?**

sethc.exe

#3	**Examining APT29, what 2 tools were used to execute the first scenario?**

pupy and meterpreter

#4	**What tool was used to execute the second scenario?**

poshc2

#5	**Where can you find step-by-step instructions to execute both scenarios?**

ATT&CK Arsenal

Task 7 ATT&CK® and Threat Intelligence

Threat Intelligence (TI) or **Cyber Threat Intelligence (CTI)** is the information, or TTPs, attributed to the adversary. By using threat intelligence, as defenders, we can make better decisions regarding the defensive strategy. Large corporations might have an in-house team whose primary objective is to gather threat intelligence for other teams within the organization, aside from using threat intel already readily available. Some of this threat intel can be open source or through a subscription with a vendor, such as **CrowdStrike**. In contrast, many defenders wear multiple hats (roles) within some organizations, and they need to take time from their other tasks to focus on threat intelligence. To cater to the latter, we'll work on a scenario of using ATT&CK® for threat intelligence. The goal of threat intelligence is to make the information actionable.

Scenario: You are a security analyst who works in the aviation sector. Your organization is moving their infrastructure to the cloud. Your goal is to use the ATT&CK® Matrix to gather threat intelligence on APT groups who might target this particular sector and use techniques affecting your areas of concern. You are checking to see if there are any gaps in coverage. After selecting a group, look over the selected group's information and their tactics, techniques, etc.

#1	**What is a group that targets your sector who has been in operation since at least 2013?**

APT33

#2	**Does this group use Stuxnet? (Yay/Nay)**

nay

#3	**As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it?**

cloud accounts

#4	**What tool is associated with this technique?**

ruler

#5	**Per the detection tip, what should you be detecting?**

abnormal or malicious behavior

#6	**What platforms does this affect?**

AWS, Azure, Azure AD, GCP, Office 365, SaaS

Task 8 Conclusion

In this room, we explored tools/resources that MITRE has provided to the security community. The room's goal was to expose you to these resources and give you a foundational knowledge of their uses. Many vendors of security products and security teams across the globe consider these contributions from MITRE invaluable in the day-to-day efforts to thwart evil. The more information we have as defenders, the better we are equipped to fight back. Some of you might be looking to transition to become a SOC analyst, detection engineer, cyber threat analyst, etc. these tools/resources are a must to know.

As mentioned before, though, this is not only for defenders. As red teamers, these tools/resources are useful as well. Your objective is to mimic the adversary and attempt to bypass all the controls in place within the environment. With these resources, as the red teamer, you can effectively mimic a true adversary and communicate your findings in a common language that both sides can understand. In a nutshell, this is known as **purple teaming**.

#1	**Read the above**

No answer needed