Threat Hunting: Introduction

Introduction

The purpose of this room is to introduce Threat Hunting as a structured concept focusing on its relationship to Incident Response, the Threat Hunting mindset, and the specific goals that Threat Hunting strives to achieve.

Learning Objectives:

In this room, we will strive to understand what Threat Hunting is and discuss its role in helping secure the organisation in contrast with Incident Response.

We will also explore different Threat Hunting goals and discuss how these goals help develop the organisation's security posture. By the end of the room, we will gain a baseline idea of what to look for, how to look for them, and when to decide to move on.

We will also gain an understanding that an Intelligence-driven approach to Threat Hunting, among others, is one of, if not the best way to move forward.

Room Prerequisites and Expectation Setting:

There are no hard prerequisites in order to gain value from this room; however, it would be very helpful to have a basic understanding of the concept of Threat Intelligence and consequently its role in the effectiveness of Intelligence-driven activities. Knowing the basic concept behind Incident Response, how SOCs operate, and how an organisation's Security Posture is built would also help a lot in understanding the concepts touched upon by this room.

Relevant Rooms:

The rooms listed below discuss concepts and employ techniques and approaches that are intersecting and even similar to the ones that we will be tackling throughout this room. As such, it is recommended to go through these rooms as well in order to get the most out of them

- Tactical Detection Room | Detection Engineering Module
- Preparation Room | Incident Response Module
- Introduction to Cyber Threat Intelligence
- Threat Intelligence for SOC
- OpenCTI
- MISP
- MITRE

Core Concept

Threat Hunting Introduction

Threat hunting is an approach to finding cyber security threats where there's an active effort done to look for signs of malicious activity. In its most basic form, that is the definition of Threat Hunting; however, in order for us to really understand what it entails as well as what its actual role is in the organisation, we will start by contrasting it with Incident Response.

Threat Hunting in Contrast with Incident Response

Incident Response (IR) is innately reactive. The action, or "response", is triggered by an initial notification or alert. This initial notification is first triaged, then analysed, and when enough pieces of evidence point to malicious activity, it is deemed an incident that needs to be responded to and dealt with accordingly.

More information about Incident Response, particularly the initial stages of it, is discussed in the Preparation Room of the IR Module.

Threat Hunting, on the other hand, is innately proactive. There is no actual 'trigger' that would mobilise a hunt, except for the pursuit of building the strength of the organisation's security posture, guided by Threat Intelligence.

A stark contrast can be seen here - while both are guided by the goal of ensuring the security of the organisation, the forces that drive the reactive and proactive nature of Incident Response and Threat Hunting, respectively, hardly share the same direction. This is further steered by the specific objectives that each aims to achieve.

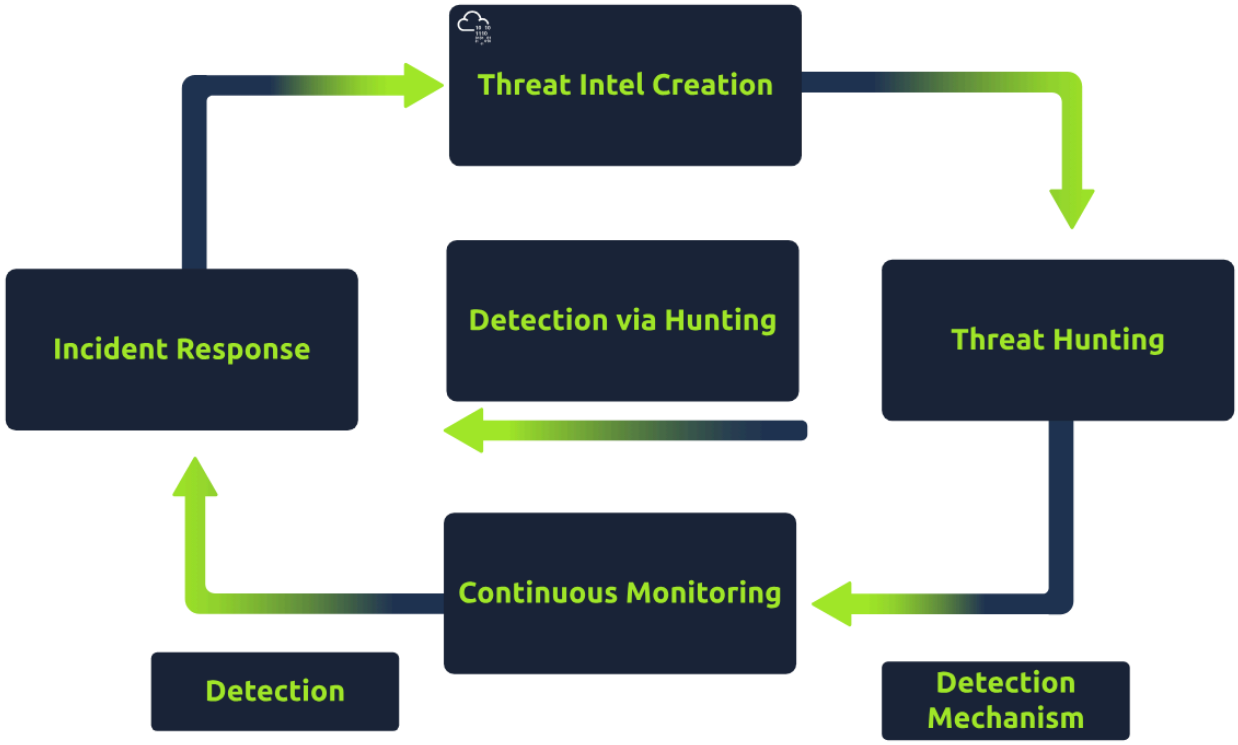
Reactive Approach	**Proactive Approach**
Incident Response	Threat Hunting
Triggered by an initial notification / alert	Active search for suspicious events that can become incidents
Guided by the initial scope of the incident	Guided by Threat Intelligence
"There's a threat that needs to be dealt with now."	"There might be a threat that we don't know yet."

Usually, organisations start doing threat hunts when there's already an established IR process as well as detection mechanisms in place, but they think that incidents aren't

being detected early enough. In the case of advanced threats, or even well-made red team exercises, there will always exist ways to go through your organisation undetected.

Threat Hunting aims to bridge this gap, constantly finding ways to add and improve the current detection mechanisms in place so that future similar bad behaviour will automatically be detected immediately. More so, during that process, detected threats go immediately to the Incident Response team. The trigger for their mobilisation are the findings from the Threat Hunt, and consequent findings from the IR process may steer the Threat Hunting team to further find bad behaviour.

This classic example shows the beauty of the synergy between two seemingly different approaches to ensuring one specific goal is met - strengthening the organisation's security posture.



****

Answer the questions below:

What do you call the approach to finding cyber security threats where there's an active effort done to look for signs of malicious activity?

Answer: Threat Hunting

In this task, what are we contrasting threat hunting with?
Answer: Incident Response

Incident response is innately reactive. What is done first thing when an initial notification or alert is received? (It is _____.)
Answer: Triaged

Threat hunting is innately proactive. What is it guided by?
Answer: Threat Intelligence

Threat Hunting and Incident Response are two different approaches that aim to ensure one specific goal is met. It is to strengthen the organisation's what?
Answer: Security posture

Threat Hunting Mindset

How you approach a task would usually dictate how successful you will be. It's easy to rely on the most cutting-edge pieces of technology being offered out there, but across the industry, people would always be the most important part of any security team. And so, while thinking of equipping ourselves with the best tools is important, investing time (and probably money) in learning the proper mindset is as significant.

What's the basis for our hunt?
It is imperative that we start our hunt with leads comprized of accurate pieces of information such as known relevant malware as well as trusted Threat Intelligence. Through leads, we give threat hunters better chances of achieving amazing things, from easy wins like looking for malicious binaries to more complex hunting projects like finding patterns of activity of certain groups that target organisations similar to us or industries we're part of.

Threat Intelligence
Since we're talking about dictating the direction of a hunt, it's essential that we arm ourselves with critical information that will let us know more about the threat(s) that we may be dealing with. Understanding the bad that we may be dealing with is akin to knowing how they might behave within our environment, possibly allowing us to narrow down our search to specific sweet spots such as specific pieces of data they might be interested in, or even knowing which groups or APTs might be particularly interested in targeting us.

Unique Threat Intelligence
Intelligence on threats that you are able to develop internally is a very valuable asset to have. Not many organisations have the kind of intrusion experience that would allow them to study and develop usable intelligence from said intrusion and even fewer have the capability of developing it internally. Furthermore, intelligence of this kind may have the characteristic of being ultimately unique to your organisation.

Indicators of Compromise (IOCs) specifically documented on previous intrusions would be the most obvious and straightforward example for this one. IOCs immediately give value not only to your threat hunters but also to your detection mechanism, as they're actual traces of an adversary. Through this, re-intrusions of that specific adversary or other adversaries that employ the same tactics would be easier to spot.

Threat Intelligence Feeds
As touched upon above, not a lot of organisations are capable of developing valuable and actionable Threat Intelligence internally. While a lot of organisations have their fair share of intrusions, not everyone has that kind of experience under their belt which allows them a front-row seat to a specific adversary's IOCs, among others. More so, it involves a lot of money, skill, and effort to be able to become an efficient Threat Intelligence producer.

It is not the end for the rest of us, as we can learn from other Threat Intelligence producers via Threat Intelligence feeds. There exist intelligence feeds that are both readily and publicly available. One of the most popular examples of this one is the MISP, an open-source Threat Intelligence and sharing platform. You may learn more about MISP here.

On the other hand, there are also paid resources that specialise in producing intelligence, some of which are capable of creating tailored intelligence for your organisation. Some examples of this are Recorded Future and ReliaQuest. These kinds of services are not cheap, and gaining a license would typically cost an arm; however, in the hands of a capable Threat Intelligence analyst, the insights that you would be able to gain would be extraordinary.

General Hunting Guide	**Examples**
Unique Threat Intelligence	Indicators of Compromise
Threat Intelligence Feeds	- MISP

	- Recorded Future - Digital Shadows

****

Answer the questions below:

What is the most obvious and straightforward example of a Unique Threat Intelligence?
Answer: Indicators of Compromise

Threat Hunting Process

What do we hunt for?
The answer to this question dictates the direction of the hunt. As the hunt progresses, the threat hunter will always go back to this question, ensuring that pieces of evidence that link to its answer are gathered.

The discussion regarding the examples below also falls under the wide-reaching topic of Threat Intelligence discussed in the previous task. However, they are valuable enough to deserve to be highlighted on their own. These highlights are more focused on the kind of intelligence where their usage would merit immediate value to the hunt. They are straightforward, specific, and immediately actionable if successfully found.

Known Relevant Malware
The internet is ripe with known malware samples, and a lot of them have publicly available published analyses. One example of leveraging this kind of intelligence is to take a closer look at your organisation, identify the relevant threat actors that might take an interest in you, and hunt for traces of the malware that they use in their toolkits within your organisation.

The example above may be a bit general. Still, once you identify what is relevant to your organisation, it would be a lot more straightforward to narrow down the samples that you want and consequently hunt for their traces within the scope of your visibility.

One example of a live malware repository is theZoo, where you may play with live malware and gain insights into how they will work within specific environmental conditions. Malware characteristics and analysis are constantly being published as well, and a good example worth exploring is Trend Micro's Threat Encyclopedia.

Attack Residues

Attack residues are a great starting point as well, especially if you think that an attack has happened already. It works particularly well with good Threat Intelligence as it would be as straightforward as ticking off a list of attack residues to check for within the environment.

The challenging part here, however, is knowing your environment well enough to be able to separate attack residues from normal behaviour. A lot of attack residues blend well with normal environmental noise. Pair this with a more advanced adversary who knows how to clean up after themselves or even worse - employ tactics that are already stealthy from the get-go, and the hunt is suddenly not as straightforward as it seems.

Overall, it's still a good way to cover our bases; remember that we only need to catch them making a mistake once while they need to constantly be perfect in their movements.

Known Vulnerabilities of Products/Applications Being Used
Threat actors are quite creative in finding vulnerabilities and misconfigurations in the products and applications that their target organisation uses. As such, at the very least, known vulnerabilities of assets should be actively hunted and patched accordingly. You might even stumble upon a threat actor actively exploiting your vulnerable assets, effectively catching 2 birds with one effort.

The organisation should be extra vigilant for announcements of zero-day vulnerabilities that may be affecting these assets. Immediate checks should be done on:

- If the current version really is vulnerable, and
- If there are traces of the vulnerability being exploited for as long as historical data may allow.

These hunts are a great way to retroactively check the exploitation of vulnerable assets while also ensuring that the assets of the organisation are all patched and up to date with the current security standards.

General Hunting Guide	**Examples**
Known Relevant Malware	- theZoo(repository) - Threat Encyclopedia
Attack Residues	- Indicators of Attack - Indicators of Compromise

Known Vulnerabilities	- Zero-day vulnerabilities - CVEs

The discussion above is a general discussion of usual threat hunt targets and is in no way an exhaustive list, albeit the list above is a good place to start. Every organisation has their own quirks and unique characteristics that must also be factored in whenever a hunting task or project is tackled.

How do we hunt for it?
Reviewing the array of information, factors, and other elements for consideration above would hopefully lead us to understand the target of our hunt. Now that we know what we want to hunt for, “How do we hunt for it?” is the sensible next question.

This section will not touch upon hunting theories and specific hunting techniques - these will be discussed in the next few rooms; rather, we will be focusing on the driving force that these theories and techniques are based on.

Attack Signatures and IOCs
Upon identifying the subject of the hunt, it’s imperative that we ensure that we characterise them into specific and actionable identifiers by which we will immediately recognize. This is done most effectively via Attack Signatures and IOCs.

By condensing the “whats” of the hunt down to Attack Signatures and IOCs, we suddenly have a set of information that we can then immediately compare to our available historical data. This makes it easier to find objects of interest such as relevant malware, attack residues, and even exploitation of known vulnerabilities. Keep in mind that we do need to know how the environment behaves and consequently, what the logs would look like when said vulnerability has been exploited.

Logical Queries
Some hunting projects are best accomplished via logical queries. A straightforward example of this one is hunting for assets that have known vulnerabilities.

Applying what we’ve discussed above - characterising the vulnerable assets via specific actionable identifiers, such as the application version, would allow us to craft logical queries that filter for these identifiers. This essentially gives us low-hanging fruits for easy pickings that, at the same time, impact the organisation’s security posture directly.

Patterns of Activity

At the end of the day, when we've already narrowed down the specific bad (e.g. relevant threat actors, etc.) that we want to focus on, the next sensible step is to characterise their behaviour through patterns of activity that they are inclined to make. In any conversation regarding this, the MITRE ATT&CK Matrix has always been a top resource, and it may as well be the star of the show here.

****

Answer the questions below:

Malware is constantly being used in the toolkits of threat actors. What is the live malware repository that we touched upon above?
Answer: theZoo

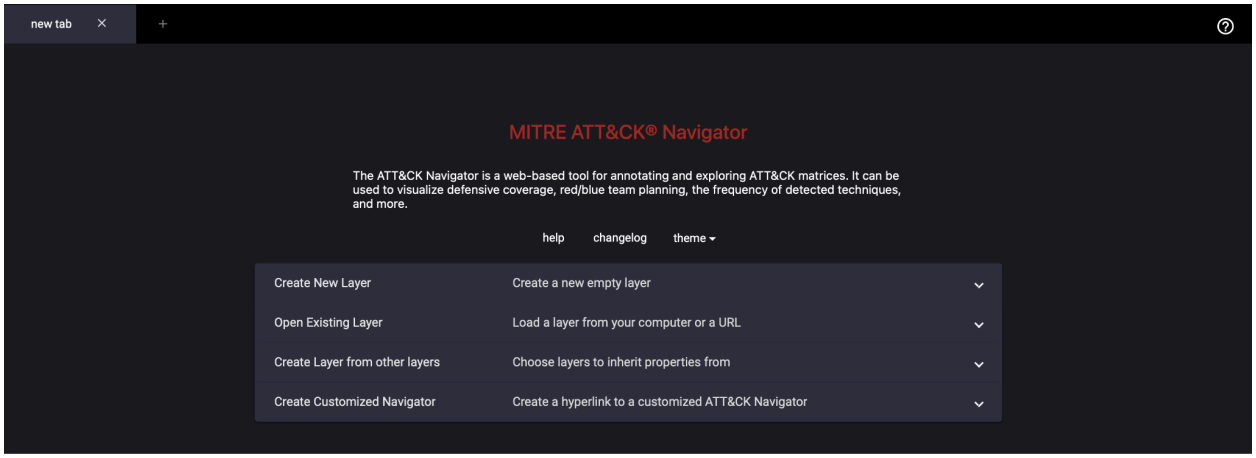
Knowing what is normal in your environment and separating them from what's not is a skill all threat hunters should have.
What example of Threat Intelligence blends well with environmental noise?
Answer: Attack Residues

Threat actors are quite creative in finding vulnerabilities and misconfigurations. What should the organisation be extra vigilant in monitoring for announcements of?
Answer: Zero-day vulnerabilities

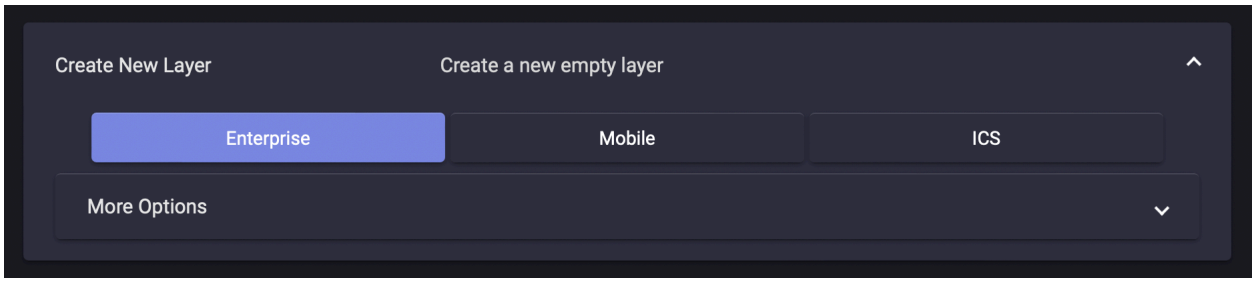
Characterisation of the subject of the hunt into specific and actionable identifiers is imperative for the hunt's success.
How is it done most effectively?
Answer: Attack Signatures and IOCs

Practical Application

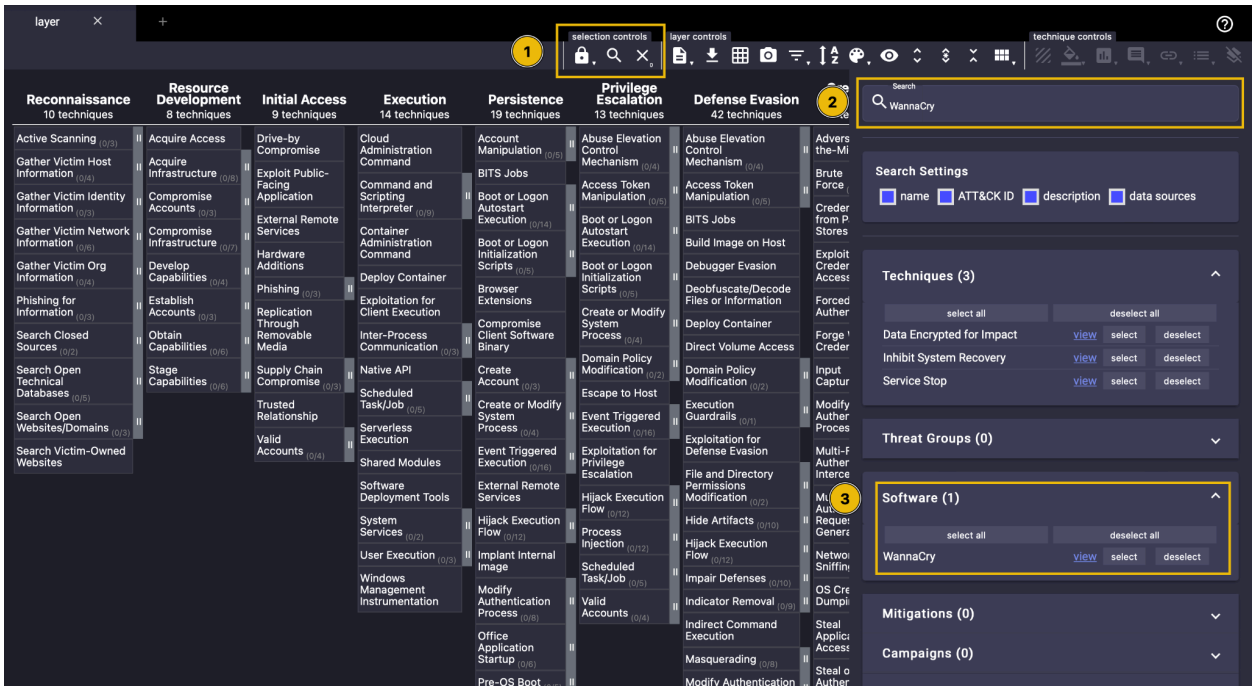
For our purposes, let's focus on the MITRE ATT&CK Navigator. The ATT&CK Navigator is a tool designed to make it easier "to visualise your defensive coverage, your red/blue team planning, the frequency of detected techniques or anything else you want to do." Not only does it show the specific attack techniques that we should look for, but it also gives an idea of how an attack flows, and it shows it in a visually appealing way. The ATT&CK Navigator will be used to answer the questions in this task. If you haven't already done so, please click on the link provided.



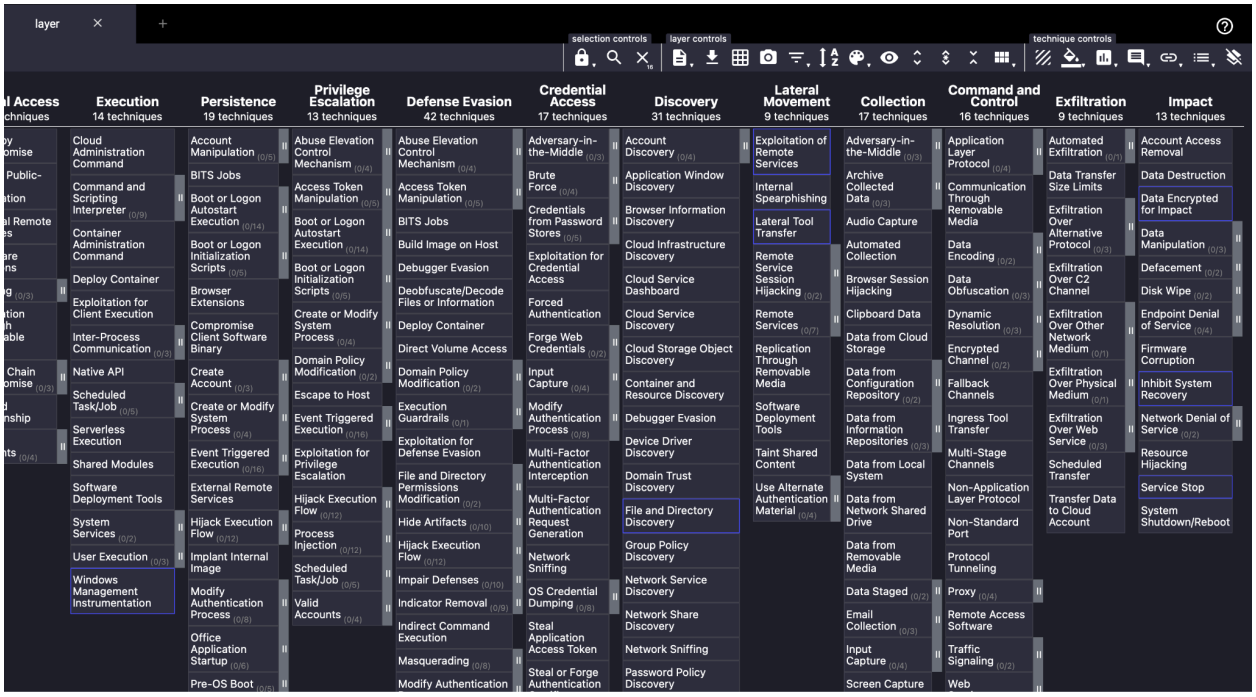
The attack navigator landing page looks like this. Let's proceed by clicking on Create New Layer → Enterprise. This should show you a blank ATT&CK Navigator page.



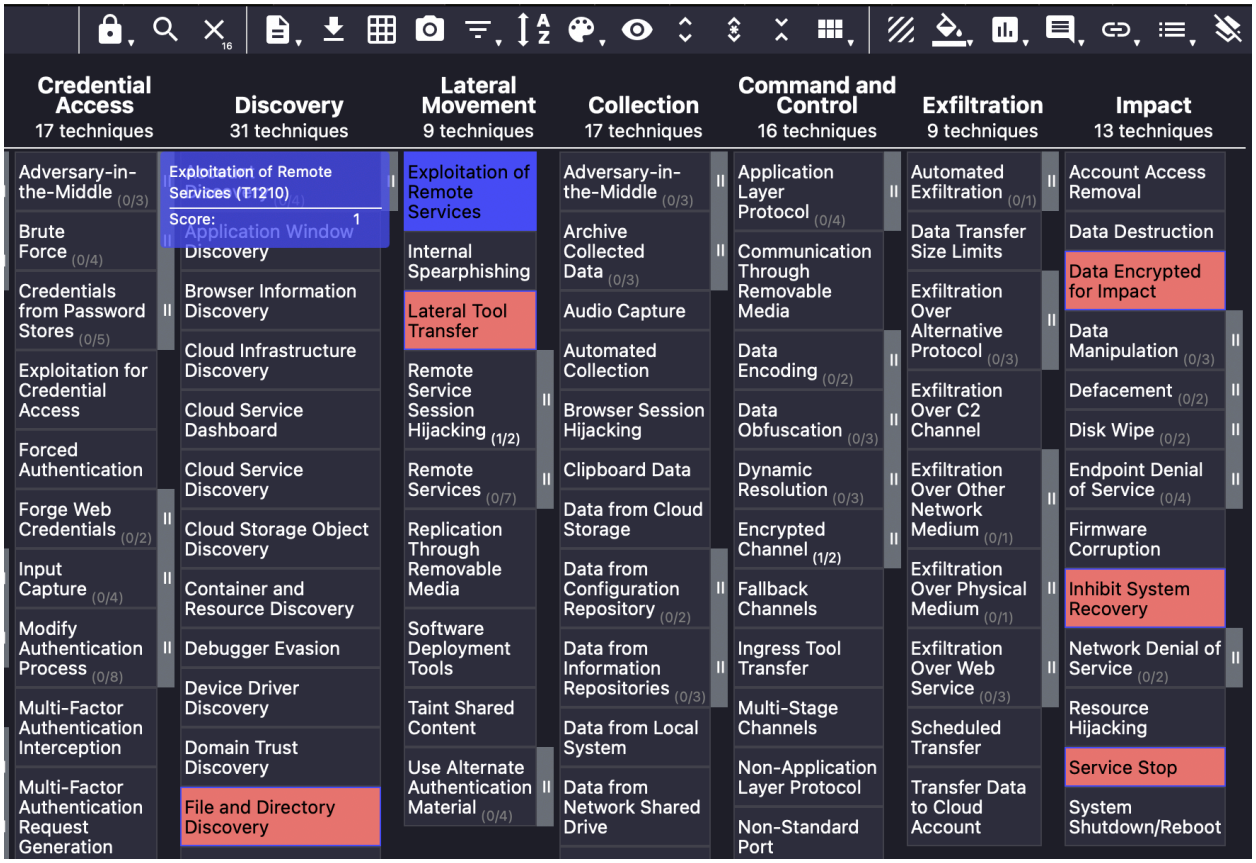
Select the magnifier glass under "selection controls", and then type "WannaCry" inside the search bar. The "Software" part of the results should show 1 result. Click on the "select" button beside the result.



It should then show something like this:

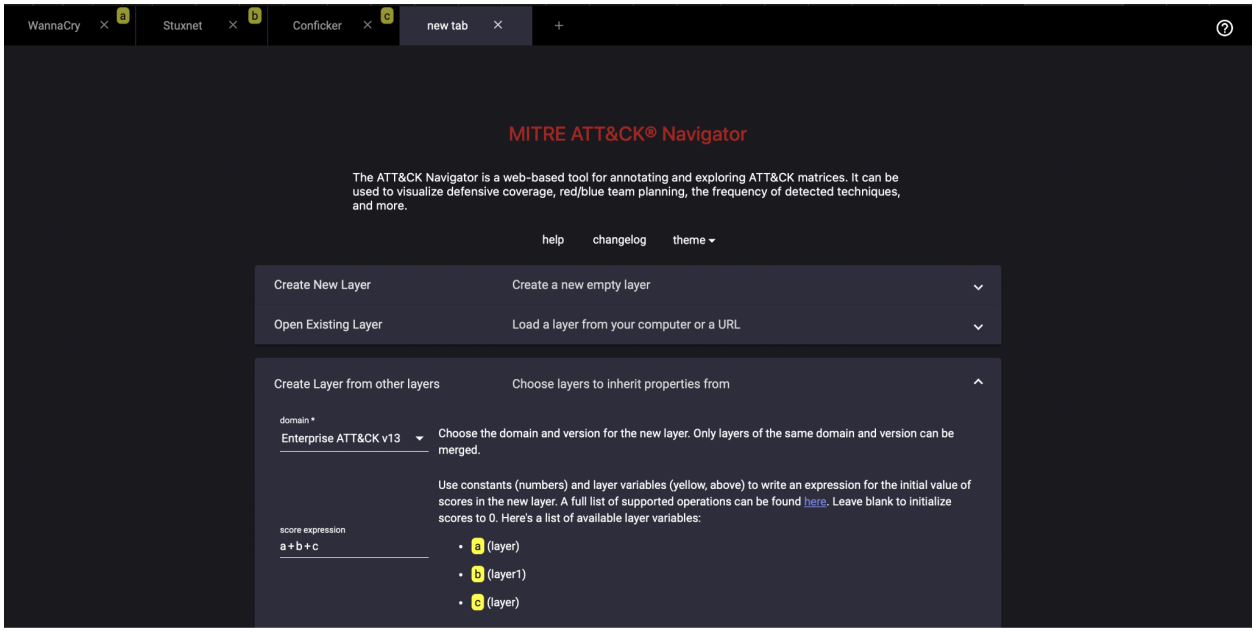


To better visualise our selection, select a background colour under “technique controls”. It will immediately fill the selected techniques with the colour of your choice. Let’s also set an arbitrary score of 1 for this layer, the control for which is beside the background colour, still under the “technique controls”. Finally, we can set a name for this layer by editing the layer information under “layer controls”. It should look something like this. Take note that hovering on the technique should show the score.



Now, in the same ATT&CK Navigator, repeat all these steps for two more threats: Stuxnet and Conficker. You can do this by simply clicking on the “+” button on top of the page and then repeating the same process we’ve outlined above. This time, set a score of 2 for Stuxnet and 4 for Conficker. This way, when we stitch all of these layers together, we’ll know exactly which threats employ the same technique by looking at the aggregate score.

Once you’ve repeated the steps above for both Stuxnet and Conficker, let’s proceed by clicking on the “+” button → “Create Layer from other layers”, choose “Enterprise ATT&CK v14” under “domain”, and then put “a+b+c” on the “score expression”. Let’s skip all of the other settings and hit Create at the bottom of the page.



This will create a new layer composed of the 3 other layers stitched into one in order to better visualise the impact of multiple threat actors that are relevant to your organisation.

By default, it would look something like this. A few changes on the colour setup under “layer controls” would transform it into something like this:

The differing colours are set to be able to immediately see which common tactics or techniques these threat actors share. A deep red colour means it's common to all of them, while the other lighter colours mean it's either one or any combination of two threat actors. The scores are arbitrary, and you can set them in terms of relevance to your organisation or just random if you just intend to play around with the tool visually. Questions at the end of this task would be related to this specific ATT&CK Navigator layer.

These tools and resources at hand would allow for a more straightforward approach to identifying patterns of activity. Once we're satisfied with the way we've characterised the relevant threats that we wanted to focus on, we can then start hunting. This intelligence-driven approach of characterising threat actor behaviour through their TTPs is one of, if not the best, way to go about hunting. It immediately gives value to the hunt, and it's sensible, straightforward, and actionable.

MITRE has done a lot, not only within the cyber security sphere but also in subjects that generally help build a "safer world". For more information on what MITRE has to offer, albeit, in the cyber security industry, you may head over to the MITRE room.

When do we decide to move on?

The single biggest challenge in Threat Hunting is knowing when to decide to move on to other things. When will you know you're done with it? Here's a Capture the Flag (CTF) analogy.

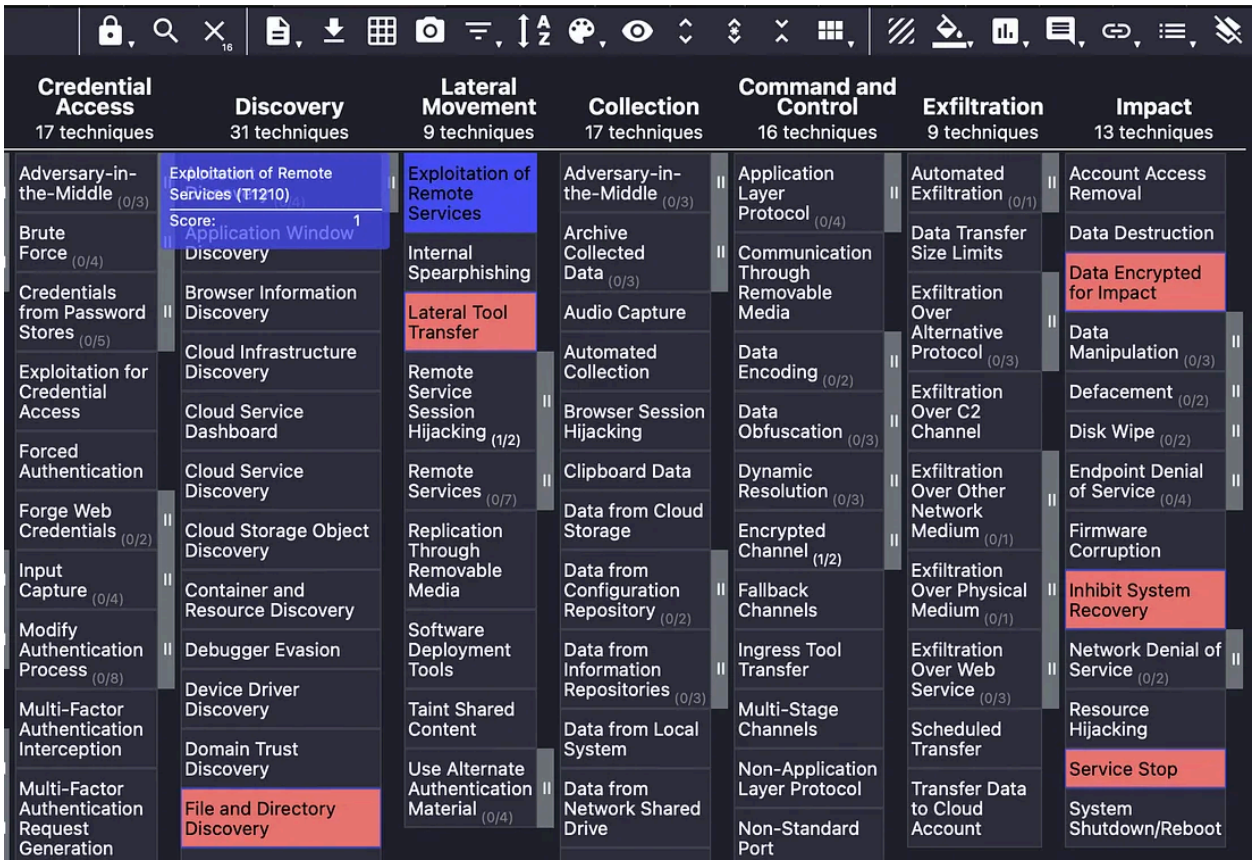
In CTFs, you immediately know before you even start that by the end of it, if you do everything right, there will be a flag waiting for you. If you aren't able to get the answer, that just means that you need to study more and further improve so that the next time you tackle a similar problem, you'll have more chances of capturing that flag. That's not necessarily the case for Threat Hunting. It's completely possible, and even more probable than not, that you do everything right and not find anything.

It will be normal to feel inadequate - there will always be internal doubt when hunting for threats. But as long as you follow your processes, especially with a hunting plan that's intelligence-driven, you should be fine.

****

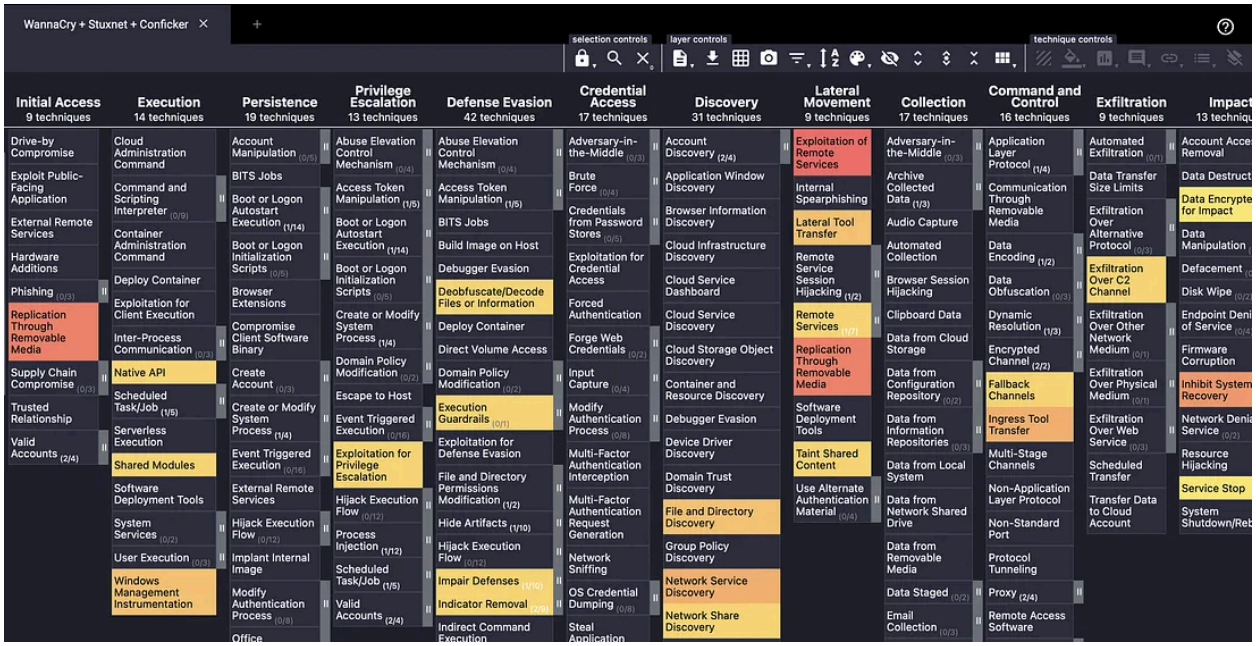
Answer the questions below:

Which tactic has the most techniques highlighted?



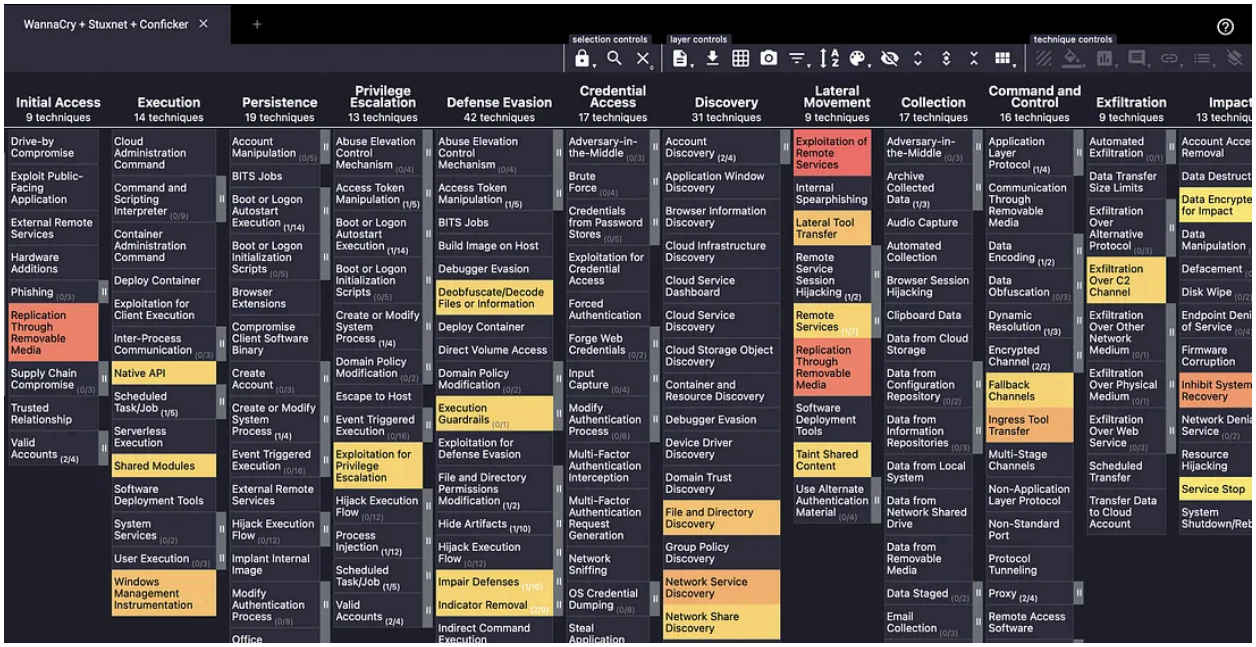
Answer: Discovery

Which technique do the three threats have in common?



Answer: Exploitation of remote services

What technique does WannaCry and Conficker have in common?



Answer: Inhibit System recovery

What's the score of techniques that Stuxnet and Conficker have in common?

Stuxnet was given an arbitrary score of 2 and Conficker was given a score of 4, so 2+4=6.

Answer: 6

Goals

So far, we have talked about the Threat Hunting concept, as well as the whats, the hows, and even the whens behind the Threat Hunting mindset; now it's time to talk about the whys.

Proactive Approach to Finding Bad

Threats are one of the constants in the world of security. There will never be a shortage of malicious actors, from Script Kiddies to well-funded Advanced Persistent Threats. There will always be someone snooping around your environment, and with that in mind, it is imperative that you find them first and you find them fast, ideally before they are able to do what they set out to do.

Discover Pre-existing Bad

Through complex and sophisticated attack chains, chance, or even mere luck, it is a reality that some activities of malicious actors may slip through an organisation's detection mechanisms. In that sense, similar kinds of activities are essentially undetectable; however, they are not invisible. It's just that detection mechanisms haven't yet been developed to automatically flag these activities.

It is through Threat Hunting that we're able to find these activities, and upon such discovery, it will consequently (and quite immediately) trigger an Incident Response. These learnings will ultimately be fed back to the continuous monitoring process of the SOC (see last section).

Minimise the Dwell Time of Attackers

Another byproduct of undetected threat actor activity is having essentially a 'free pass' to further snoop around within the environment. The longer a bad actor has access to your environment, the more opportunities they have to further learn about it. With a deeper understanding of the environment, an attacker may execute more sophisticated ways of persisting within the environment, cause bigger damage to important assets and/or information, and steal more data.

The primary goal of Threat Hunting is to minimize a threat actor's dwell time. Ultimately, security is the business of ensuring the confidentiality, integrity, and availability of the organisation's assets, and minimising dwell time also minimises the damage a threat actor might have already caused.

Develop Additional Detection Methods

In the end, we want to be able to use all of these findings as feedback to our continuous monitoring process. Security is a continuous development process, so we wouldn't want to hunt for the same threats over and over again. Instead, once we've profiled threats that were previously undetectable by current detection methods, an effort should immediately be poured into translating these profiles into detection mechanisms. In effect, future similar threats will be immediately detected and actioned upon.

****

Answer the following questions:

What is the primary goal of Threat Hunting?
Answer: Minimise a threat actor's dwell time

Feedback is important to keep the organisation secure.
Upon profiling threats through our Threat Hunting efforts, what should these profiles be translated to?
Answer: detection mechanisms