Open Threat Hunting Framework Operational

# Operational

Threat Hunting requires a methodical approach. However, it is important to remember that -Threat Hunting is not a project (time bound activity). As attackers keep evolving, threat hunters should create new detection mechanisms and continuously refine existing ones to improve detections (i.e. reduce false positives and automate). With the OTHF, threat hunt teams can have a continuous improvement driven framework for threat hunting that is designed to scale to support even the largest organizations by acting as the driving force behind automated detections. This isn't the art of fiction. Over the years, the OTHF team has worked rigorously to create a platform agnostic threat hunting process and this framework and processes is the result of zeal for effective and efficient threat hunting that will integrate with automated detection processes such as Palantir' Automated Detection Strategy (ADS)[[1]](#footnote-1) and applying lessons learned during incidents responded.

Diagram

Description automatically generated

Figure 1: IBM X-Force Threat Hunting Framework

At its core, the framework lays out simple steps:

1. Know the threats as applicable to your company and industry
2. Understand TTPs for applicable threats
3. Develop the Threat Hunt per unique TTP
4. Automate developed Hunts
5. Periodically revalidate the work – Threats, TTPs and Hunts.

Details below explain how Threat Hunter could benefit from those building blocks and elaborates the process of Threat Hunting.

## Identifying Hunts

Every organization faces security risks, but the risks aren’t the same for everyone. An attacker specifically targeting a hospitality organization, for example, will likely go after different assets than an attacker specifically targeting an electricity utilities company. Within the organization, targets may vary. An attack on the accounting department might target financial data or employees’ personal information, while an attack on the engineering department might target intellectual property. Additionally, there are also threats that are opportunistic in nature that are not targeting a specific industry or organization but can pose as a significant risk.

This section of the OTHF is designed to help organizations identify and prioritize hunts to maximize the value of the threat hunting program.

### Intelligence Driven

Much like with threat hunting, the OTHF is not meant to be a definite guide on cyber threat intelligence (CTI), but it is important for a threat hunting program to understand that CTI can be a major asset to identify and prioritize threat hunts.

CTI provides crucial support by providing detailed information on characteristics of previous attacks, common access vectors, and the techniques and procedures that adversaries employ. Threats are characterized by types of attackers, common points where an infection might occur, and the procedures attackers are likely to employ. Understanding the steps attacker may take, allows the threat hunter to define the potential clues of malicious behavior aligned with the attack stages.

While having a dedicated CTI team to help identify and prioritize activities for the threat hunting program is ideal, the OTHF will cover approaches that can be adapted by organizations of varying levels of maturity.

The OTHF focuses mostly on two types of threat intelligence:

* Strategic Threat Intelligence (STI) – High level analysis of adversary motivations, abilities, and associated targets. STI is not focused on the technical details of how an attack will happen but rather this intelligence will shed light on why adversaries attack and who they may target.
* Tactical Threat Intelligence (TTI) – Detailed analysis of the TTPs associated with an adversary or malware family. TTI analysis may include multiple reports for adversary groups or malware families which describe the how an attack will happen through each of its various stages.

#### Strategic Threat Intelligence Sources

In more mature organizations, an internal or third-party CTI team should be leveraged for the latest intelligence on which adversaries are actively targeting or most likely to target an organization and would be the underlying motivation for the attack.

If the threat hunting team has access to a dedicated CTI team, the threat hunt program should coordinate with the CTI team to receive regular updates on adversary activities and motivations. The threat hunting program should be able to identify the top threats to the organization at any given time through a relationship with the CTI team.

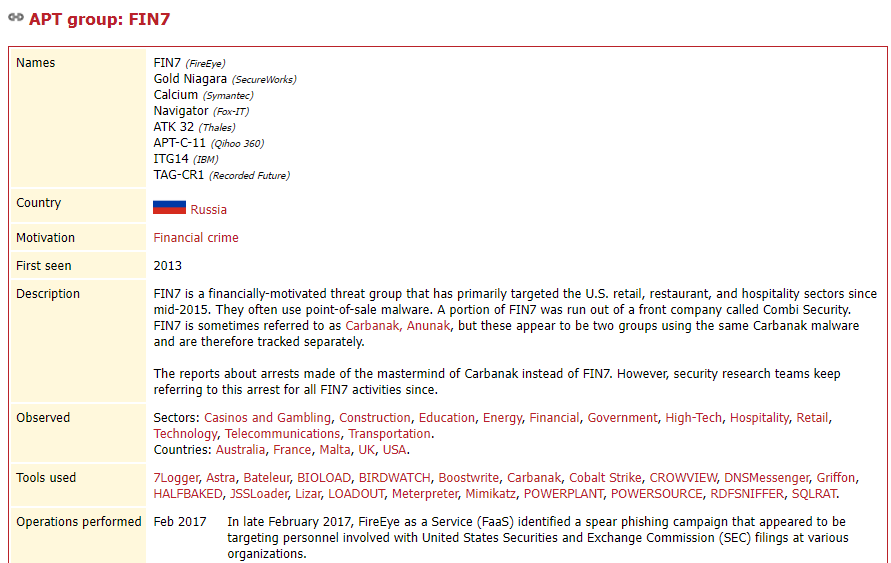
If an organization does not have a dedicated CTI team, threat hunting programs can leverage several free sources to gather STI data including a mapping adversary groups to targeted industries and motivations.

##### Electronic Transactions Development Agency

The Electronic Transactions Development Agency (ETDA) maintains a Threat Actor Encyclopedia containing numerous threat actor groups. Within each entry, users can find a description of the adversary, suspected country of origin, targeted sectors and countries, and motivation. Additionally, where applicable the ETDA populates a “Operations Performed” section detailing attacks that have been attributed to the adversary.

Every threat actor “card” can be downloaded as a PDF or JSON object.

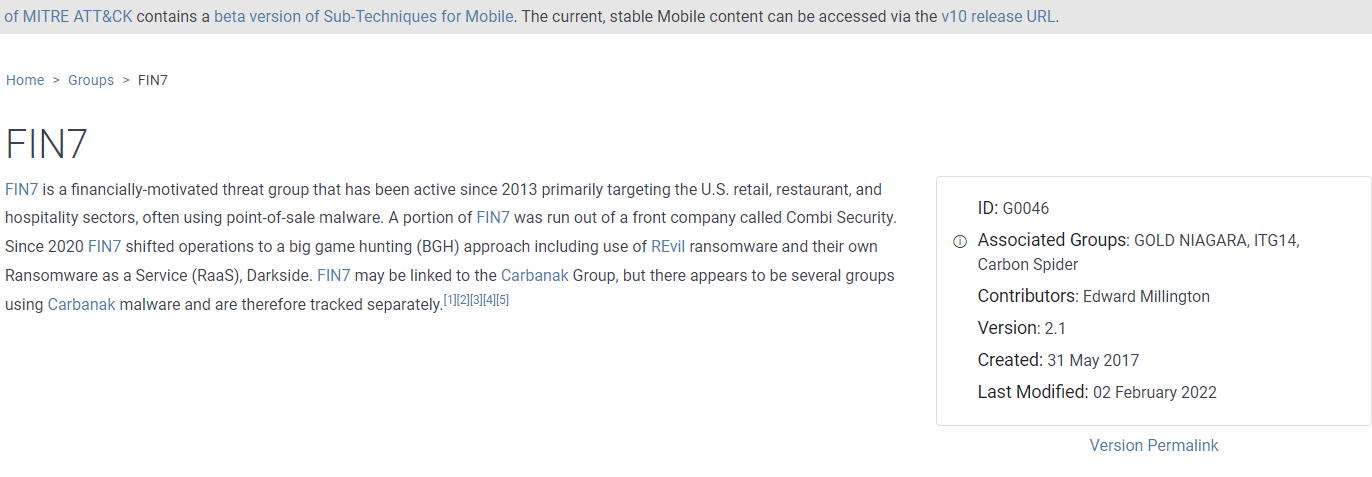
ETDA Threat Actor Encyclopedia: <https://apt.etda.or.th/cgi-bin/listgroups.cgi>



##### MITRE ATT&CK Groups

MITRE maintains a Groups page within the ATT&CK framework that provides an overview of adversary groups and the industries they frequently target. MITRE classifies a group as “sets of related intrusion activity that are tracked by a common name in the security community”[[2]](#footnote-2). While the level of STI gathered from MITRE Groups may not be as detailed or targeted as what a dedicated CTI team will produce, threat hunters can leverage the resources within MITRE Groups to identify which adversaries are associated with their organization’s industry and check the references for attributed attacks against parent companies, subsidiaries, or geolocations.

MITRE ATT&CK Groups: <https://attack.mitre.org/groups/>



##### Other STI Sources

Secureworks Threat Profiles: <https://www.secureworks.com/research/threat-profiles>

Mandiant Advanced Persistent Threat Groups: <https://www.mandiant.com/resources/apt-groups>

#### Tactical Threat Intelligence Sources

In more mature organizations, an internal or third-party CTI team should be leveraged for the latest intelligence on mapping adversaries and malware to specific tools, tactics, and procedures. If a dedicated CTI team is available to the threat hunting program, the CTI team should be consistently maintaining a TII resource and make it available to all threat hunters.

If an organization does not have a dedicated CTI team, threat hunting programs can leverage several free sources to gather TII to gather intelligence on the TTPs leveraged by various adversaries and malware.

##### The MITRE ATT&CK Tactics and Techniques

MITRE provides a comprehensive library of adversarial tactics and techniques. A globally accessible open-source knowledge base, it incorporates a detailed list of offensive tools and techniques that hunt teams can draw from when constructing hypotheses. The framework also includes a detailed list of which data sources should be examined a specific technique in an environment.

For the techniques defined in MITRE ATT&CK framework has a “Data Sources” field in the reference box to the right which explains what Data Sources are recommended for the detection of the specific technique.

Graphical user interface, text, application, email

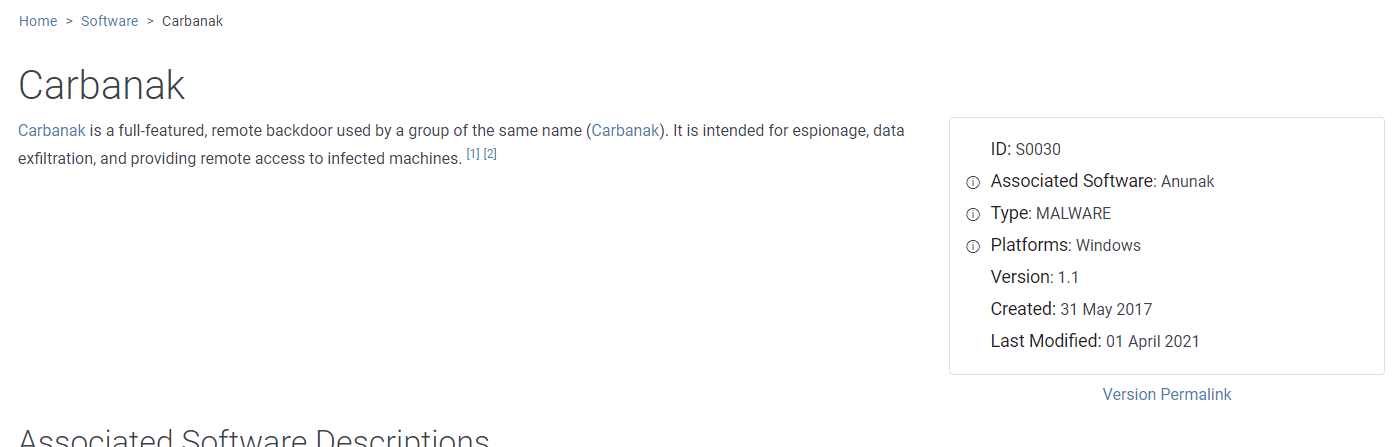
Description automatically generated

Figure : MITRE ATT&CK Framework Technique and Data Sources

MITRE also maintains an ATT&CK Software repository which details malware and tools used

MITRE provides a comprehensive library of adversarial tactics and techniques. A globally accessible open-source knowledge base, it incorporates a detailed list of offensive tools and techniques that hunt teams can draw from when constructing hypotheses. The framework also includes a detailed list of which data sources should be examined a specific technique in an environment.

For the techniques defined in MITRE ATT&CK framework has a “Data Sources” field in the reference box to the right which explains what Data Sources are recommended for the detection of the specific technique.

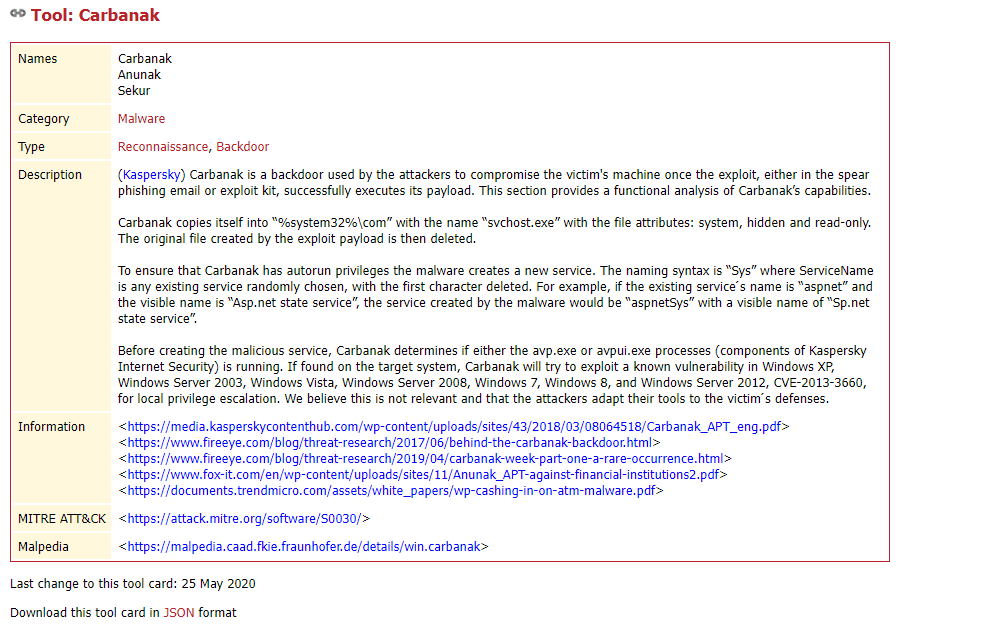


##### Electronic Transactions Development Agency

The Electronic Transactions Development Agency (ETDA) maintains a Threat Actor Encyclopedia containing numerous threat actor groups. Within each entry, a “Tools used” section is populated with tools that have been associated with the adversary. Each tool within the ETDA encyclopedia contains information describing tools capabilities, uses, and links to other reports associated with the tool.

Every tool “card” can be downloaded as a JSON object.

ETDA Threat Actor Encyclopedia: <https://apt.etda.or.th/cgi-bin/listgroups.cgi>



#### Threat Assessment

Threat assessment is a proactive activity to help an organization understand their specific risks by gaining insight into what adversaries may be targeting them and how the attack may happen. Threat assessments, blend together data from STI and TTI and through this exercise a threat hunting program can identifying hunts that are relevant to an organization and can have a positive impact on the organization’s level of risk.

Threat assessments should take a methodical approach and depending the resources available to the threat hunting program, portions of a threat assessment may be based on assumptions or best guesses. As a threat hunting program matures, the accuracy of the threat assessment should improve based on improved STI, TTI, and understanding of the organization.

* First step is to use the available resources to gather STI to identify threats that are applicable to your organization. Understand these adversaries and their evolving methodologies.
* Research and understand the identified adversaries. Analyze the threat groups’ motivations, to assist you in crafting a narrative of threats to your organization
* Based on the motivations and methodologies of the adversaries, understand the basic level of potential impact to the organization. This section is not meant to include a full impact assessment but rather gives hunters and opportunity to prioritize hunts based the severity of different style of attacks.
* Research and understand the tools, techniques, and procedures associated with the adversary to build a narrative about how each adversary carries out an attack
* Based on the capabilities and tools/techniques of adversaries, combined with your knowledge of security controls determine the likelihood of the attack.

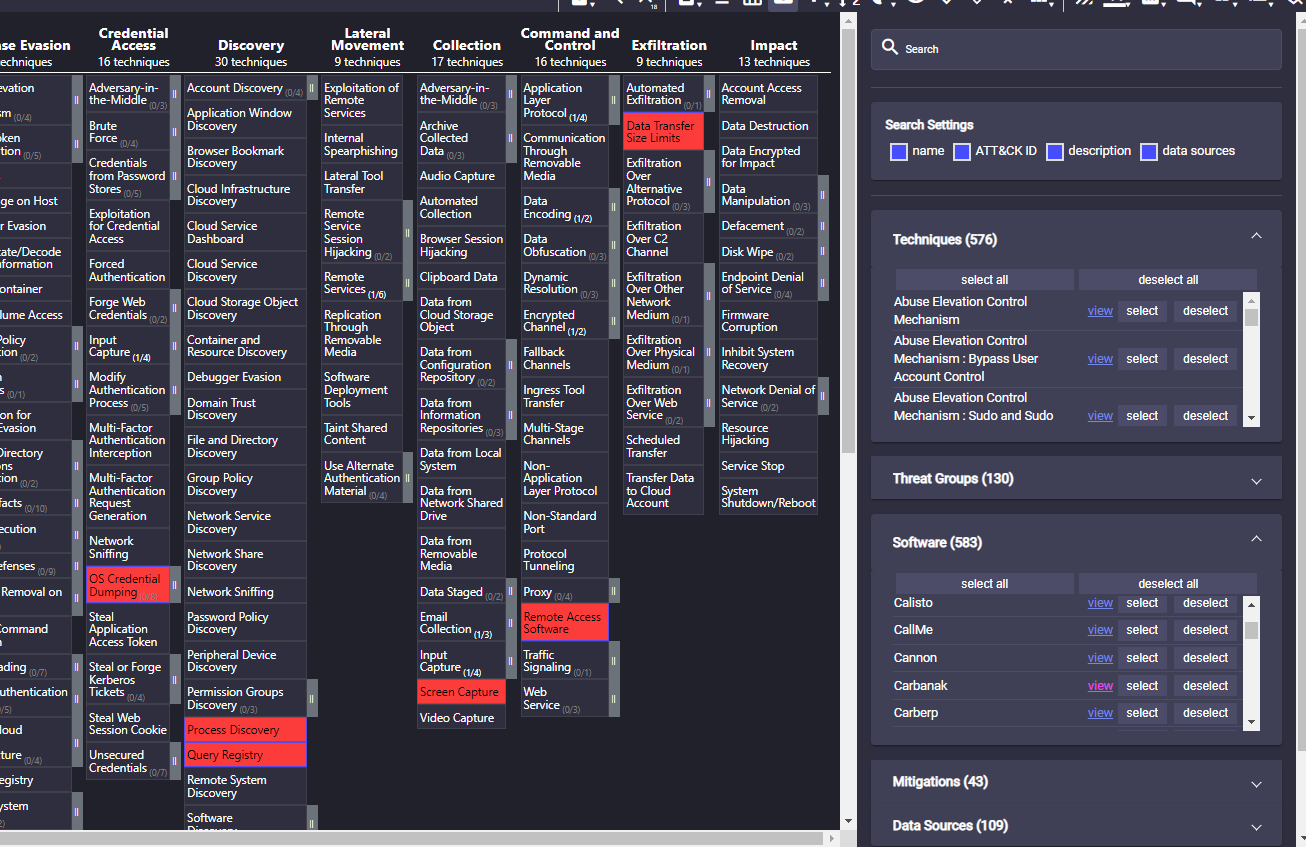
Most organizations have finite resources and budget. It may be practically impossible to address every identified threat group based on available resources. Prioritization is key. Threat hunting programs can leverage the threat assessment process to identify hunts that will provide the most value to the organization.

Figure 3: Threat Assessment Process

##### MITRE Navigator

MITRE Navigator is a free tool that enables users to efficiently use the data within the ATT&CK framework. Navigator enables users to create layers upon the ATT&CK matrix and automatically annotate techniques that are applicable to the defined layer.

Navigator allows threat hunters to quickly query the ATT&CK data set to highlight associated tactics and techniques associated with group, software, data sources, and mitigations.

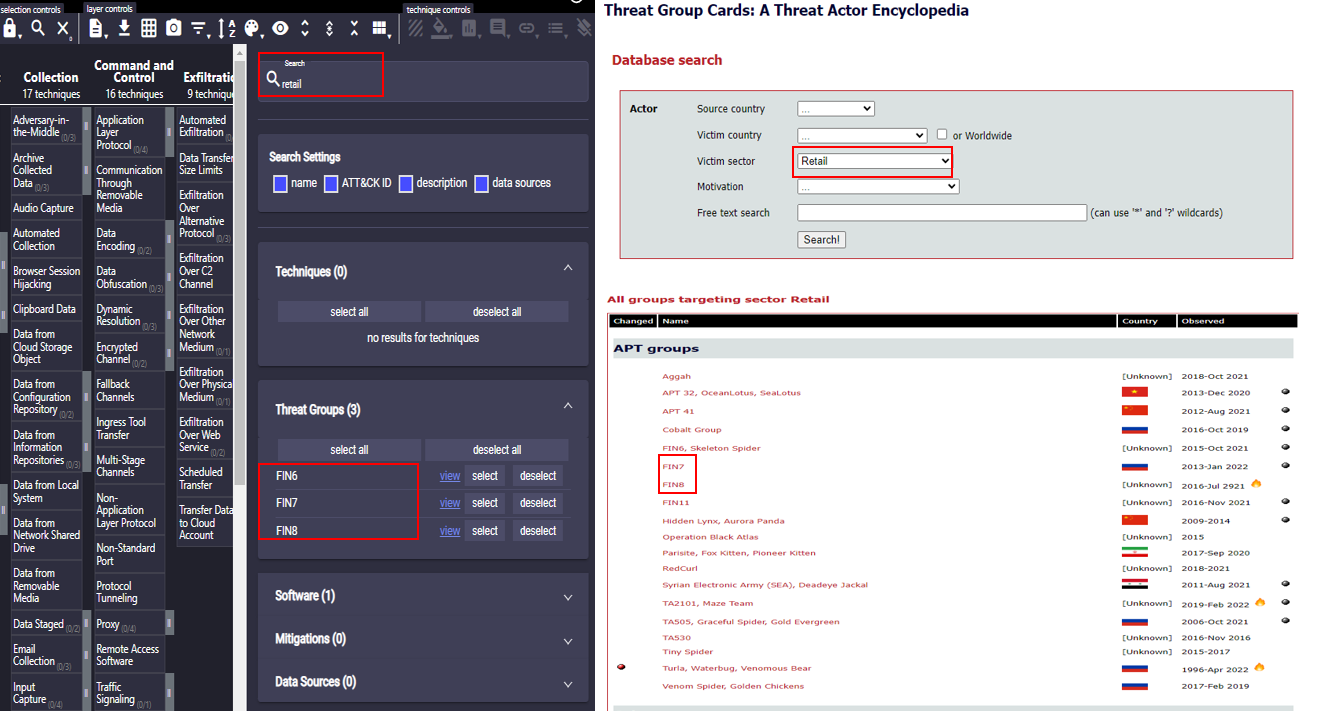


##### Example Threat Assessment

In this example a threat hunter from a mid-sized retail organization will execute a threat assessment using MITRE and ETDA.

**Who is targeting?**

Using MITRE Navigator and ETDA, the hunter can simply search for the word “retail” as it applies to Groups and Threat Groups. Cross referencing the results, the only adversaries that are listed in both MITRE and ETDA are FIN7 and FIN8. While all of the groups listed as targeting “retail” in either MITRE or EDTA should be assessed, the threat hunter should prioritize the groups that exist within both data sources first.



**What are they after?**

MITRE and ETDA have both FIN7 and FIN8 listed as financially motivated adversaries.

**How bad would it be?**

Based on the data within ETDA and MITRE (at the time of writing), FIN7 attacks have centered around payment card theft and ransomware both of which could result in serious operational, financial, and reputational damages. Assessing the timestamp data (at the time of writing) of the reference materials listed in MITRE and ETDA, FIN7 has shifted their operations towards large scale ransomware attacks.

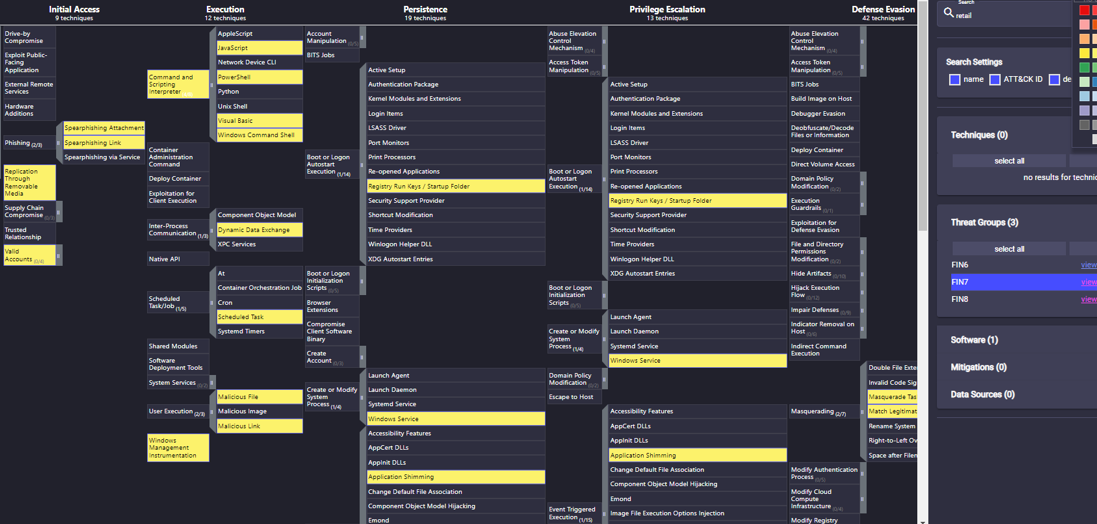
Based on the data within ETDA and MITRE (at the time of writing), FIN8 attacks have centered around payment card theft through point of sale (POS) malware which could result in serious financial and reputational damages.

Assessing the timestamp data (at the time of writing) of the reference materials listed in MITRE and ETDA, FIN7 has been more active than FIN8 and ransomware has the potential impact to shut down business operations.

Based on the data available to the threat hunter, FIN7 should be prioritized.

**How would they do it?**

With a particular threat actor in mind, threat hunter can use MITRE Navigator to visualize the techniques associated with FIN7 and can visualize the techniques as they are used throughout the MITRE Tactics.



Determining which technique to evaluate first may be determined by the size of the threat hunting program. While there is value in prioritizing techniques which present the most risk to the organization, it can develop into a long-time assessment delaying the hunter from executing a hunt. Prioritizing based on the sequential or reverse order of techniques based on the Tactic flow is a reasonable option, but the threat hunting leaders should decide definitively how hunters prioritize techniques.

In this example, the hunter will prioritize the techniques in sequential order as the are laid out in the MITRE Tactic lifecycle.

Starting with Initial Access, FIN7 is associated with Phishing, Replication Through Removable Media, and Valid Accounts

**Likelihood of Success**

While having a mapping of a relevant adversary to techniques and tactics is valuable, there may be multiple ways a technique can be used in an attack, or the associated technique may not be applicable to every organization. Hunters can focus their efforts even further by using the resources within MITRE to research specifically how FIN7 uses the associated technique.

The hunter assesses the three techniques and learns that their organization disables the USB port on all of the workstations within the enterprise. While not an undefeatable control, it does reduce the likelihood that FIN7 will gain initial access through removable media. Next, the hunter checks the MITRE technique mapping for FIN7 to determine how they are utilizing Valid Accounts. Based on MITRE, FIN7 leverages Valid Accounts for lateral movement and not initial access. This does not mean that FIN7 does not ever or will never leverage Valid Accounts for initial access, but this allows the hunter to de-prioritize this technique for FIN7 based on the intelligence available.



Within Phishing, FIN7 has associations with Spearphishing Attachment and Spearphishing Link. Based on the hunter’s understanding of the organization’s security controls, they feel that both techniques are equally likelihood to succeed however based on the reference material within MITRE, FIN7 has been most recently (at the time of writing) attributed to carrying out an attack using Spearphishing Link.

Based on the threat assessment, the hunter has been able to identify which adversary is most likely to be associated with an attack against their organization, what their goals will be, and what techniques they should hunt for first.

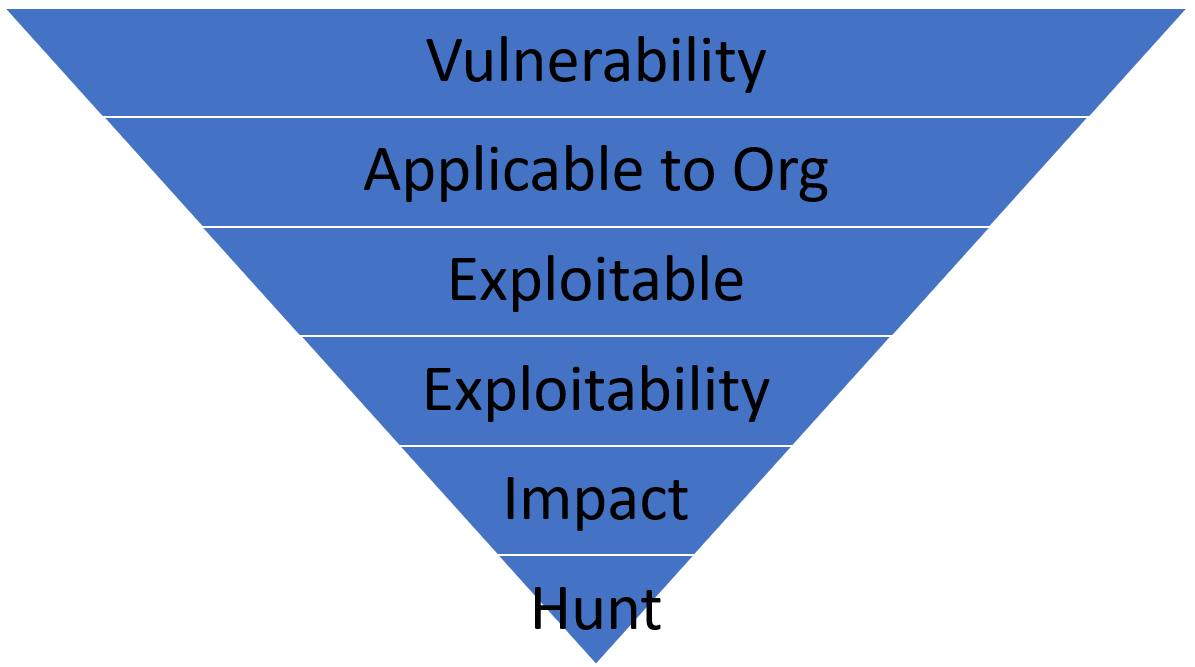
### Vulnerablity and Exploit Data

According to NIST, a vulnerability is a weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat[[3]](#footnote-3).

Vulnerabilities are just a reality that all security teams must accept. Every year, a vast number of new vulnerabilities are discovered and made public, and organizations must constantly assess and patch vulnerabilities. Patch management has continually been a challenge for organizations and within the time where a vulnerability is released and a patch is successfully applied, organizations are at risk from additional threats. During this window of vulnerability, threat hunting teams can provide some risk mitigation coverage by executing threat hunts for evidence that the vulnerability has been used as part of an attack.

Typically, a vulnerability disclosure does not contain enough information for threat hunters to successfully execute a hunt for an associated attack. There is a significant difference between something being vulnerable and something being exploitable. Exploits are pieces of code or sequences of instructions that take advantage of a vulnerability to cause an unintended behavior, gain unauthorized access, or execute arbitrary additional commands.

While a vulnerability details a theoretical way to execute an attack against exploits provide a direct path for an adversary to take advantage of a vulnerability in an attack. To help threat hunting teams identify and prioritize threat hunts associated with vulnerabilities, the OTHF encourages threat hunting programs to implement a similar triage process:



* Vulnerability – A vulnerability is released
* Applicable to Org – Is the vulnerability associated with software, hardware, or other system that is used within the organization?
* Exploitable – Has there been an exploit released or has it been exploited by an adversary in the wild?
* Exploitability – How difficult is exploitation?
  + Is the vulnerability associated with software or systems that are publicly available?
  + Does it require preexisting physical, network, or authentication access to be successful?
  + Are there existing security controls that mitigate the exploit?
* Impact – What is the level of impact to the organization if an attacker successfully exploits the vulnerability?
* Hunt

#### Vulnerablity and Exploit Data Sources

Exploit DB - project maintained by Offensive Security which is a collection of public exploits and vulnerable software.

<https://www.exploit-db.com/>

Rapid7 Vulnerability and Exploit Database – Repository of vetted software exploits and exploitable vulnerabilities.

<https://www.rapid7.com/db/>

CXSecurity – web-based application containing the latest exploits for local and remote vulnerabilities.

<https://cxsecurity.com/exploit/>

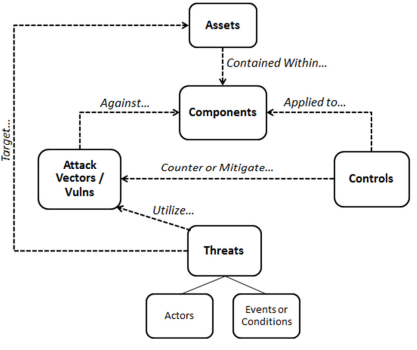
### Attack Surface Driven

NIST defines an attack surface as “The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.”[[4]](#footnote-4). Attack surface discovery (ASD) is a continuous process aimed towards discovering, categorizing, and evaluating the security of an organization’s cyber assets. Where ASD differs from asset or vulnerability management is that ASD can be considered the aggregate of assets, vulnerabilities, mitigations, and controls to present an organization with a contextualized view of how areas within the network that an attacker could be successful.

Threat hunters can leverage ADS to identify and prioritize hunts for threats that are directly associated with the available attack surface of an organization. Leveraging ASD data to identify hunts, ensures that hunters are focused on threats that are most likely to be successful against their organization.

In the paper, “A Threat-Driven Approach to Cyber Security” [[5]](#footnote-5) M. Muckin and S. Fitch propose a relational model between threats, assets, and controls. Through this model, Muckin and Fitch demonstrate that adversaries rarely directly access targeted cyber assets, instead they interact with and circumvent other components of a system to obtain their objectives. Muckin and Fitch go onto state that given an indirect relationship between adversaries and targeted assets, “controls must be selected and implemented to address threats and attack vectors” where a control is a direct response against relevant threats and attack vectors that exist within a given system or application.

Threat hunters can leverage threat intelligence as an input into a Threats-Assets-Controls Relational Model to identify potential areas of exposure and attack vectors are highlighted which can drive identification of relevant hunts for a particular system or application.



Muckin, Fitch Threats, Assets and Controls Relationship Model

### Mission Driven

The delivery of the core operations while maintaining data security of those operations can be considered the missions of the organization. Outside of using threat intelligence to identify threat hunts, threat hunt programs may also choose to perform threat hunts based on ensuring mission assurance by focusing threat hunting efforts to detecting adversaries as they attempt to compromise mission relevant systems, services, users, protocols, devices, networks, processes, or data (cyber assets).

To fully understand and reduce the risk of impacting core missions, threat hunters must execute mission mapping and threat modeling exercises to identifying underlying cyber assets that enable the organization’s missions.

The idea behind mission driven threat hunting is based upon K. Jabbour and S. Muccio, “The Science of Mission Assurance,[[6]](#footnote-6)” where a four-step process is outlined for cyber mission assurance.

1. Develop and prioritize a list of mission essential functions
2. Mission mapping to identifying all dependencies a mission has on cyberspace
3. Identify vulnerable assets
4. Analyze risks and mitigate.

For mission driven threat hunting, hunters should take a similar approach:

1. Identify and prioritize core operations
2. Perform mission mapping to identify all mission dependent systems, services, and data
3. Perform a threat model of dependent systems, services, and data
4. Identify and prioritize hunts to detect identified threats for identified mission dependent systems, services, and data

The value of mission driven threat hunting is that hunters are prioritizing hunts based on a deeper understanding of what cyber assets are supporting missions and how an attack on them impacts the overall risk to the organization.

#### Mission Mapping

It is not uncommon for threat hunters or even the IT administrators to not fully understand all of the dependencies and interconnections of cyber assets that enable missions. Mission mapping aims to address this issue by actively building understanding of all of the complex relationships between cyber assets and their relation to missions.

There are various methods to perform mission mapping, but the methods drawn from J. Guion and M. Reith’s “Cyber Terrain Mission Mapping: Tools and Methodologies” including Functional Mission Analysis, Crown Jewels Analysis, Ontology Modeling, and Impact Dependency Graph were all specifically designed for use by cybersecurity personnel to identify cyber key terrain.

It should be noted that some of the aforementioned mission mapping methodologies are highly effective but require a significant amount of effort and supporting software to build out and maintain. As threat hunting organizations mature, they may opt to implement one of the methods from “Cyber Terrain Mission Mapping: Tools and Methodologies” that factor in quantitative data.

For the purposes of the OTHF, the framework will focus on Ontology Modeling which leverages an entity-relationship-attribute (ERA) diagram to create an easy-to-understand mission map modeling the relationships between missions, users, capabilities, and assets.

It is not a requirement for any threat hunting program to implement a defined mission mapping standard, some organizations may opt to identify key missions and model their cyber asset dependencies through a tree graph, with the mission at the top and connecting dependent systems, software, users, networks, and physical infrastructure in a hierarchal manner.

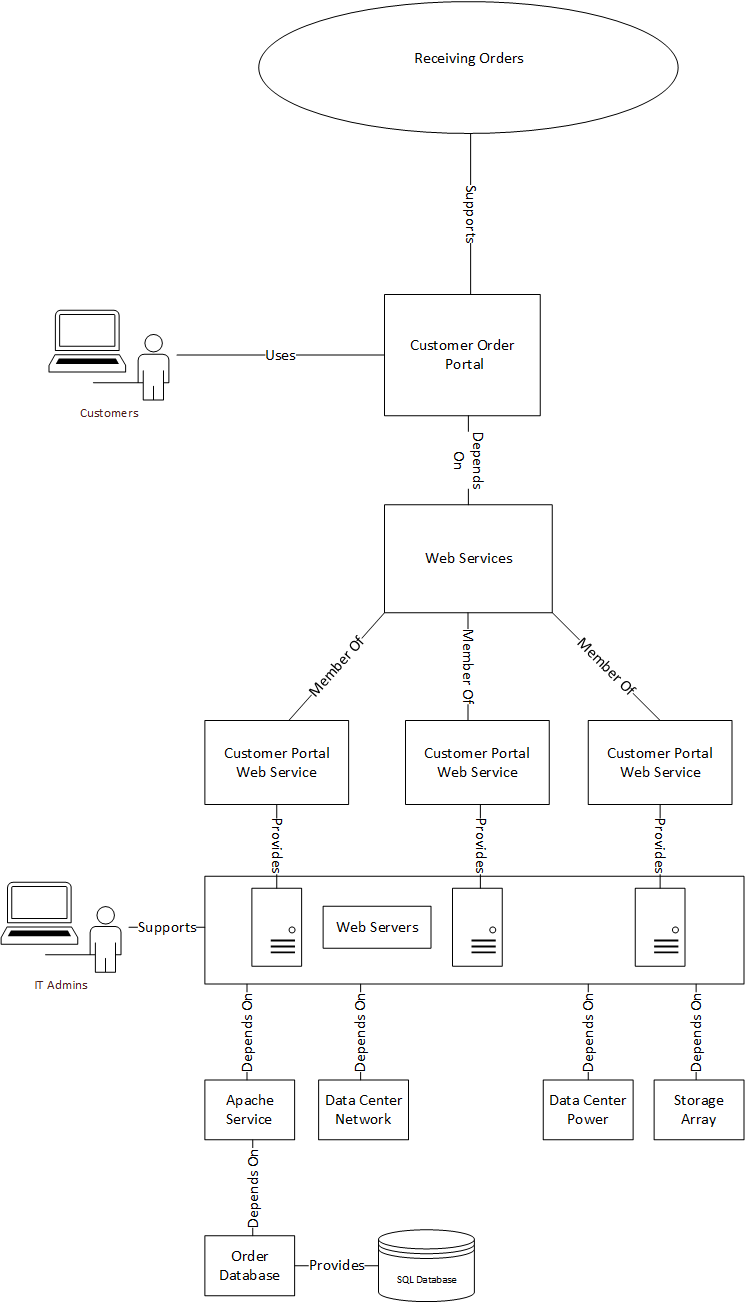
##### Ontology Modeling

In the paper, “CAMUS: Automatically Mapping Cyber Assets to Missions and Users”[[7]](#footnote-7), Goodall, D’Amico, and Kopylec from Applied Visions Inc outline how they translated ERAs into a ontology models for automated mission mapping using a custom tool named CAMUS.

The resulting mission mapping models leveraging the ERA approach results in a nodal graph where relationships are defined as “uses”, “depends on”, and “requires”. Through this approach threat hunters are able to traverse the graph and ask, “What cyber assets are needed to execute my mission”, or the bottom-up, “what missions are impacted by the loss of this system”[[8]](#footnote-8).

##### Example Ontology Model

In this simple example, we demonstrate an organization who has a core business component (mission) of “Receiving Orders”. User the ERA approach, threat hunters can identify and build threat hunts around proactively identify threats that would impact the cyber assets that the support Receiving Orders mission. Threat hunters may need to fuse vulnerability and attack service data with the ontology model to design a threat hunt for applicable threats for the identified cyber asset.



## Observation Driven

As hunters get access to data, they may observe new trends, patterns in user or system behavior, or identify pieces of data that seem like anomalies compared to current and historical knowledge of the datasets. These observations can be a valuable driver in developing new threat hunts and provide an opportunity for threat hunters to leverage their unique understanding of the environment along with their creativity to identify threat hunts unique to their organization.

While observations may be obtained through unstructured mechanisms, hunters should use their observations to formulate a structure hunt.

The following process is meant to demonstrate how observations can drive a threat hunt.

1. While performing research within the network connected process data set, a member of the hunt team notices a process named “certutil.exe” making a network connection to an IP address 192.168.1.1
2. The hunter has never observed “certutil.exe” within the network connected processes data set.
3. The hunter performs a historical search for “certutil.exe” within the network connected process data and determines that this event is not an anomaly and occurs regularly within the environment.
4. The hunter does some research about why certutil.exe would establish a network connection for legitimate and malicious reasons.
5. Triaging the current and historical events, the hunter determines that this certutil.exe activity is legitimate
6. Hunter creates a hypothesis to hunt for malicious network connected certutil.exe events

## Threat Hunting Process

One of the most important elements to implement when operationalizing a threat hunting program is structure. Structure ensure that hunters remain task-driven, adhere to well-defined standards, and focused on activities that bring value to the organization. Without structure, hunt teams’ risk executing hunts within a disorganized and disjointed environment which creates an extremely difficult situation to demonstrate the value of threat hunting or track improvements.

In terms of threat hunting structure, a well-defined threat hunting process is critical for setting up the threat hunting program for success and can prevent inefficient or ineffective hunts from devaluing the threat hunting program. The threat hunt process should be considered the authoritative resource for design, documentation, and quality standards for threat hunts.

Figure 4: OTHF Hunting Process

The OTHF process shows the high-level building blocks of Threat Hunting. The process should be applied for each unique threat and TTP identified. Each Threat Hunt should be defined and executed as a project with clear scope in mind aka Threat Hunting goal.

Figure 5: Detailed Threat Hunting Process - provides a detailed project overview and workflow. We explain the process in the text below.

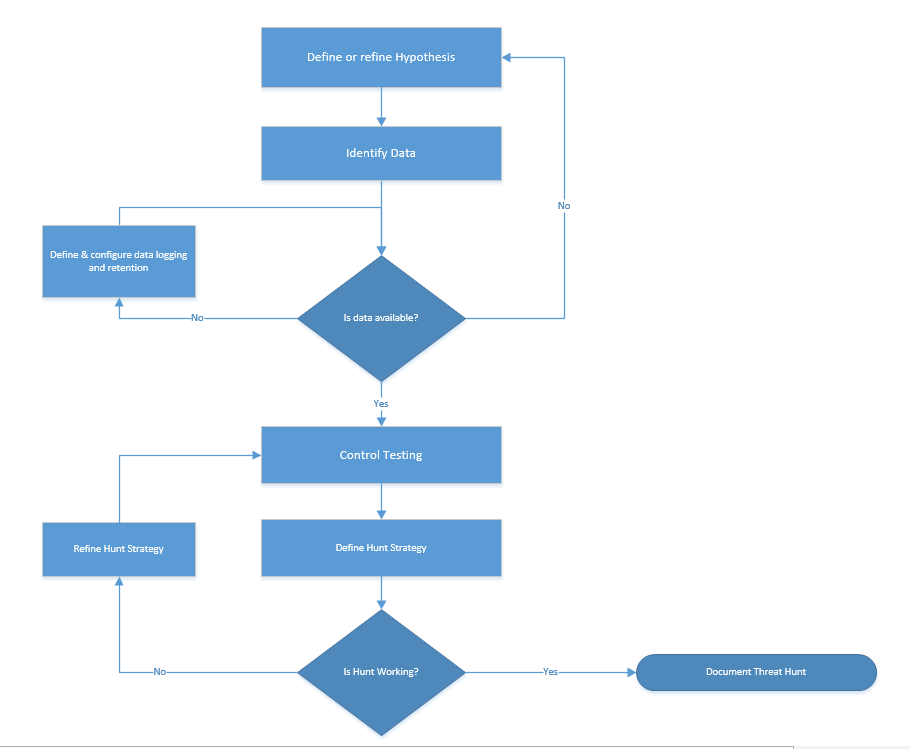


Figure 5: Detailed Threat Hunting Process

### Define a threat hunt goal

“If you don’t know where you’re going, any road will get you there.”[[9]](#footnote-9)

Having direction is very important in threat hunting. Not having direction, a goal, or not knowing where your hunt is going, it’s all the same. You go nowhere. You can never get “there,” because you don’t really have a destination. Without direction, without a goal, threat hunts will suffer to determine success and risk being ineffective.

Rather than generally searching for various types of threats, threat hunter should start by defining a specific, narrowly focused goal. The goal can be created based on any hunt identification methods listed in the Identifying Hunts section of the OTHF as well as any additional methods not listed however, threat hunting programs should define standards and best practices for goal development.

#### SMART Goals

SMART is a widely accepted criteria for individuals and organizations to set goals and objectives. SMART is an acronym that stands for specific, measurable, achievable, relevant and time-based.

**Specific** - Goal should be well-defined, clear, with unambiguous intentions

Goals that are specific have a significantly greater likelihood of being accomplished and a popular approach to designing a specific goal is to incorporate answers to the popular “W” questions.

Who – Consider who is required to accomplish the goal? Who will be responsible for executing and a dependency for success?

What – What exactly are you trying to accomplish? Details matter and it pays to be hyper focused when goal setting.

Where – Location specific details may not always be relevant to a goal but if there is a location or trigger that is relevant to the goal, it should be stated.

Why – Why are you trying to accomplish this goal? Why is it relevant to the organization? How does it incorporate with the organizations overall mission statement, goals, and objectives?

**Measurable** – Progress towards accomplishing the goal should be easily determined through defining specific criteria for measuring success.

Goals should have criteria for measuring progress and success. If there are no metrics defined than how will you determine if you’ve accomplished your goal or how close to completion are you?

**Achievable** – The goal should be attainable and not impossible to accomplish.

Goals are meant to enable progress not to discourage it. When setting goals, ensure that they are attainable and there are no major roadblocks like the lack of skills or tools to accomplish the goals.

**Relevant** – The goal should align with the broader goals and mission statement of the organization

Goal relevance refers focusing on something that makes sense within the scope of the organization’s vision and mission. A goal that is designed to address an issue that is not relevant to the organization is not adding value.

**Time-Based** – The goal should be bound by a timeframe including a target date for completion.

The best goals in the world can be ruined through inaction therefore including time elements such as deadlines or intervals adds layers of accountability and urgency increasing the likelihood of success. Additionally, including Time-Based along with Measurable criteria within a goal can help you define what should be achieved at throughout the goal’s lifespan.

##### SMART Threat Hunting Goals

Leveraging SMART to build threat hunting goals is not a requirement but it does provide easy to understand criteria to ensure that hunts are effective, efficient, and easy to operationalize.

Consider the following example in building a SMART goal from a weak goal.

Goal: Detect evidence of ProxyLogon

Assessment: ProxyLogon is the generic name for CVE-2021-26855, the vulnerability that enables attackers to bypass authentication. ProxyLogon is often chained together with CVE-2021-26857, CVE-2021-26858, CVE-2021-27065 which were initially used by the HAFNIUM group to compromise Exchange servers. At its core CVE-2021-26855 enables a remote adversary to bypass the authentication mechanisms within Exchange and perform actions packed within a specially crafted HTTP request with the highest privileges. Given the versatility of the vulnerability adversaries are able to execute requests against various services with Exchange however, threat intelligence shows that adversaries have leveraged the vulnerability to access user mailboxes and upload web shells.

Based on the understanding of ProxyLogon, depending on which component of the exploit or variation of the exploit the hunter is targeting, the required data sources and hunt strategy may vary adding ambiguity to the hunt.

The hunter can strengthen this goal by adding criteria to make it more specific to a specific component of the vulnerability or behaviors resident within different implementations of the exploit.

**Specific**: Detect successful exploitation of CVE-2021-26855 & CVE-2021-27065 via the Metasploit ProxyLogon RCE resulting in the introduction of a web shell on a Exchange server.

Assessment: While the hunter has added adequate specificity to ensure the hunt remains hyper focused on a specific activity, there are no metrics specified to determine when the goal is complete.

The hunt can strengthen this goal by adding criteria that would clearly define when the goal of the hunt has been accomplished.

**Measurable**: Detect successful exploitation of CVE-2021-26855 & CVE-2021-27065 via the Metasploit ProxyLogon RCE resulting in the introduction of a web shell through analysis of at least 7 days of file activity data of all Exchange servers in the XYZ North American domain.

Assessment: When setting this goal, the hunter must consider the likelihood of success based upon the measurements of success outlined in the goal. If the criteria listed in the goal creates an impossible situation for success, the hunter should revise the goal.

**Achievable**: Does the threat hunt team have access to 7 days’ worth of file activity data for Exchange servers in the XYZ North American domain?

Assessment: The hunter now has an achievable goal that is measurable and using specific criteria however the threat hunter must still consider whether the goal is relevant to the organization and the threat hunting program’s mission statement.

**Relevant**: Does the organization use Microsoft Exchange for email? Is the Exchange deployment on premises or in the cloud? If the organization uses Microsoft Exchange, are the servers patched? Are there existing automated detections designed to alert on the same behaviors specified in the goal? Is the threat hunting program responsible for hunting in the XYZ north American domain?

Assessment: Confirming the relevancy the hunter now possesses a well-structured goal however without including a time component, the goal risks losing any sort of urgency for completion.

**Time-Based:** By June 23, 2022 assess at least 7 days of file activity data of all Exchange servers in the XYZ North American domain for evidence of successful exploitation of CVE-2021-26855 & CVE-2021-27065 via the Metasploit ProxyLogon RCE resulting in the introduction of a web shell.

### Develop Hypothesis

Hypothesis is a testable statement about the proposed explanation for some observed phenomenon[[10]](#footnote-10). The foundations of a strong threat hunt hypothesis are relevance and testability. Relevance has been already explained above, it means how does the hypothesis relate to organizational needs, current industry trends, and available data sources. Testability means that the data and tools available would provide some chance of finding what the threat hunter is looking for within the hypothesis. That means, a good hypothesis is a question that helps you identify threats, gain information about your environment, or prove your hypothesis wrong or right. Not all these goals need to be met, however, hypothesis should always have a conclusion, whether it is proven right or wrong[[11]](#footnote-11).

As Paul C. Price, Rajiv Jhangiani, I-Chant A. Chiang, Dana C. Leighton, and Carrie Cuttler detail in their work “Developing a Hypothesis”, hypotheses always have an if-then relationship so threat hunters can structure their hypothesis with an if-then format to ensure they are crafting a craft a testable and measurable hypothesis.

Additionally, threat hunters can implement a “If..then” or “Given, When, Then” notation to their hypothesis to help ensure that it contains the core components of a strong hypothesis.

#### Given When Then

Developed by Daniel Terhorst-North and Chris Matts as part of Behavior-Driven Development (BDD)[[12]](#footnote-12), Given-When-Then is a notation style of representing unit tests.

Given-When-Then instructs users to break tests down to three sections:

* Given is meant to describe the context of the scenario or pre-conditions of the test.
* When is the triggering event or condition to test
* Then describes the resulting outcomes or changes you expect due to the specified behavior.

Within threat hunting, the given-when-then framework ensures that hunts are designed with testability and context to drive specifics.

Example

**Given** a Microsoft Exchange CAS is vulnerable to CVE-2021-26855 & CVE-2021-27065, **when** a remote adversary leverages the ProxyLogon RCE module within Metasploit to establish interactive access to the system, **then** a malicious ASPX file will be written to C:\Program Files\Microsoft\V15\Front End\HttpProxy\owa\auth\ or c:\inetpub\wwwroot.

### Validate Data

Leveraging the knowledge gained through generating signal data, threat hunter should validate that the requisite data is available (logged and retained) and accessible to the threat hunt team to conduct searches. Better data quality leads to better decision making. Therefore, Threat Hunter should:

1. Document what data is needed: Identify what data is required to test the hypothesis. If you don’t know where to start, as explained above, MITRE ATT&CK Framework provides a starting point by identifying data sources relevant to the techniques. Your Threat Intelligence team may offer you greater depth of details on techniques and data sources required based on their analysis and research.
2. Identify what is available: The data availability really means that quality data is available. Quality of data is essential in getting good and consistent results. The quality of the data should be validated based on following criteria:
   1. Availability: The environment may not be setup to provide you the data you need to conduct the hunt. If the data is not captured or logged and retained, Threat Hunt team should coordinate to get the data required for analysis.
   2. Completeness: The systems and tools may be configured to capture the data needed for threat hunt. However, the environment may not be configured consistently to provide required data e.g. data may be available on 50% of the end points – would hamper the quality of analysis and decision derived. Therefore, Threat Hunter must determine the minimum criteria to proceed and adjust.
   3. Consistency: A data item(s) should be consistent in its content and format. If data isn’t consistent, different groups may operate under different assumptions and skew the decisions.
   4. Retention: Also referred as timeliness of the data. Data should get recorded as soon after the real-world event as possible. Data that reflects events that happened more recently are more likely to reflect the current reality. Data retention rules established in the organization can severely impact the ability to conduct effective hunts.

If Threat Hunt team identifies any quality gaps explained above, the project has already identified security gap. Threat Hunter can report these findings to fix data availability or refine the hypothesis to work with available datasets.

Roberto Rodriguez provides a fantastic overview of the importance of data validation in terms of threat hunting operations in his blog, “Ready to hunt, First, Show me your data!” [[13]](#footnote-13). In his blogpost, Rodriguez states “if data needed for a hunting engagement does not meet specific requirements defined by the hunt team, then the data is not considered quality data” meaning that all the data in the world will not necessarily advance threat hunting operations if it is not properly curated to ensure the highest data quality.

Before an organization can begin an effort to ensure that that threat hunting is using high quality data, organizations must first define a mechanism to measure data quality. Organizations have various options when choosing a strategy to measure data quality one example of a well-define data quality management solution is the [DoD Total Data Quality Management](http://mitiq.mit.edu/ICIQ/Documents/IQ%20Conference%201996/Papers/DODGuidelinesonDataQualityManagement.pdf).

Once an organization has established criteria and a measurement function to evaluate the quality of their data, they should implement a well-define data modeling strategy to provide specific guidelines regarding data modeling so as new data is created, it adheres to a standard which produces high quality data. One such approach is the [Common Information Model (CIM)](https://www.dmtf.org/standards/cim).

#### DoD Total Data quality Management (TQDM)

Built upon existing total quality management approaches, DoD’s TQDM process was designed as a process to support database migrations and promote the adoption of data standards amongst databases throughout the DoD. Through the TQDM process, the DoD has created a list of characteristics that threat hunt teams can use to quantify the quality of their data.

|  |  |  |
| --- | --- | --- |
| Characteristic | Description | Example Metric |
| Accuracy | Accurate data is free of errors and that can be used as a reliable source of information. Additionally, a qualitative assessment exists where fewer errors results in a higher assessment. | Percent of stored values that are correct when evaluated against the actual value.  Example, Species=Cat when the subject is a cat. |
| Completeness | The degree to which values present in the expected fields. | Measurement of the number of fields that contain data vs the total number of fields. |
| Consistency | The measurement of variance a set of data adheres to a defined set of constraints | Percentage of values that match in type and structure across tables, files, and records. |
| Timeliness | The speed in which values are up to date within a data set. | Percentage of entire data set that is available within a specified time frame. |
| Uniqueness | The measure of the variance within the records of a dataset. | Perfect of database records having a unique primary key |
| Validity | The level of to which values are aligned with a defined classification and domain. | Percentage of values within a dataset that adhere to their allowed values specified by their domain/classification. |

DoD Core Set of Data Quality[[14]](#footnote-14)

#### Common Information Model

Common Information Model (CIM) standard is a project maintained by [DMTF](https://www.dmtf.org/) that defines how information systems, networks, applications, and services are managed while allowing for extensions through third party vendors.

The CIM standard includes a management schema, a specification, and a metamodel.

Management Schema – Structured into the distinct components: core model, common model, and extension schemas, the management schema supplies a well-defined framework of interrelated systems and their properties and associations.

Specification – Enables integrations with other management systems by providing definitions and syntax specifications for various systems to communication using a common domain.

Metamodel – Defines expressions for common elements that must be clearly presented to management applications (for example, classes, properties, methods, and associations).

A practical application of a common information model for threat hunting can be found with Splunk’s [Common Information Model](https://docs.splunk.com/Documentation/CIM/5.0.1/User/Overview). While Splunk’s CIM is designing within the Splunk platform, the underlying concepts to implement data normalization and validation can be applied across various data types and platforms.

### Create Test Data

This step refers to the process of creating test data based on the techniques adopted by the adversaries. Generating test data that is a direct result of the targeted technique used by adversaries is a critical step in validating that the hypothesis is accurate and requisite data is available. It is recommended to spin up a lab environment before to test these configurations, scripts, or subscriptions before finalizing the hunt for production deployment.

While recreating adversary operations with full featured offensive toolsets and command control infrastructure would be ideal for creating test data, several open-source tools exist that can help threat hunters generate signal data through actions associated with adversary techniques.

As the threat hunting team gains efficiency, team may lose valuable time orchestrating the test data. To overcome this inefficiency, organizations must expand the charter of management and development of test data to improve automation. This concept is well known as data-driven testing. The Red Canary team has maintained an open-source detection testing framework called Atomic Red Team[[15]](#footnote-15). It is a library of tests mapped to the MITRE ATT&CK® framework. Security teams can use it to reproducibly test the environments. As explained above, MITRE ATT&CK framework is a taxonomy of threats that attempts to describe the many techniques that an adversary might use when attacking an organization. In that context, Atomic Red Team can be referred as a collection of tests for emulating those adversary techniques.

As threat hunting and detection methods mature, organization should consider leveraging red team services to generate signal data for more advance TTPs.

Threat hunters need to analyze the data sources to prove or disprove a given hypothesis using multiple forms of evidence. Hunters should also document where the data comes from, ensuring that sources are both contextualized and consistent.

### Define Hunt Strategy

In this stage threat hunters should design the conditions to target within the identified data source to identify adversary activity quickly and accurately. Threat hunters should use this stage to establish a baseline of what is normal for the given activities they are analyzing within the environment and should have a good understanding of what data patterns are present within the targeted data sources. Threat hunters should compare benign entries versus the signal data to understand the differences to target, so the hunt activity is hyper focused on only on adversary activity. A well-designed strategy can reduce false-positives and increase the hunt efficiency.

### Validate Hunt

The validation stage of the framework is a chance for the hunter to test their hunt strategy across a large set of data and may require a iterative process to ensure a threat hunt is ready for production.

Hunt validation requires the hunter to execute the hunt against data over time incorporating as much historical data as possible to test the hunt’s signal-to-noise ratio[[16]](#footnote-16). As results of the hunt are received the hunter should evaluate the data and tune the conditions of the hunt to eliminate false positives or modify the hunt strategy as needed.

ü

**X**

**Tune Hunt**

**False Positive Identified**

Figure 6: Iterative process of Hunt Validation over range of historical data

### Document Findings

The final step is to ensure the goal, hypothesis, TTPs, and searches are methodically documented.

“If it isn't written down, then there is no evidence that it did or did not occur.”

Documentation encourages knowledge sharing, which empowers your hunt team to understand the fundamentals of what data a hunt returned and whether it was successful. Without documentation, threat hunting organizations will lack cohesion, become inefficient, and ineffective.

At the conclusion of every hunt, the hunter should document the date and time of the hunt and any all findings. Findings can be interesting observations, missing data, false positives, true positives, policy violations, or other data that helps hunters better understand their environments.

### Example hunt

Remote Transfers using BITSAdmin

In Context of APT10

#### Document Control

|  |  |
| --- | --- |
| Title | Remote Transfers using BITSAdmin |
| Created | 2022-02-17 |
| Document Version | 0.1 |
| Last Updated |  |
| Document Owner |  |
| Change Reviewers |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Name | Changes |
|  |  |  |  |

#### Goal

Detect malicious transfers associated with bitsadmins.exe being used to download content from a remote host residing outside of the <clients> network.

#### Hypothesis

Given an adversary leverages BITS to send or receive data with a local or remote host. When the bits job executes, a windows event log entry using EID 59/60 will be written containing the URL to the host.

#### Validate Data

* The detection of BITSAdmin requires the ingestion of WEL 59/60 in the BITS event log
  + EventID 59 - BITS started the <jobname> transfer job that is associated with http://example.com URL.
  + EventID 60 - BITS stopped transferring the <jobname> transfer job that is associated with the http://example.com URL. The status code is 0xxxx.
* 2021-12-14 BITS Windows event logs are currently not being ingested into the centralized SIEM. Threat Hunting team working with the security team to enable data logging and storage. Ticket Number 1234 has been created
* 2021-12-15 Ticket Number 1234 resolved. BITS Windows event log 59 and 60 is currently ingested into the centralized SIEM. Potential blind spots may occur within the organization that are related BITSAdmin process due to events only being ingested from the North American domain not the European.

#### Create Test Data

Validation for the BitsAdmin condition can occur by performing the following execution on a Windows system:

Bitsadmin.exe /create 1 bitsadmin.exe /addfile 1 https://live.sysinternals.com/autoruns.exe c:\data\playfolder\autoruns.exe bitsadmin.exe /RESUME 1 bitsadmin /complete 1

#### Define Hunt Strategy

Look for transfer jobs within the Microsoft-Windows-Bits-Client EventID 59. Identify URL that fall outside normal operation such as Google, Microsoft, Adobe, and WindowsLive. Additionally look for stopped transfer jobs within EventID 60, which also contains the URL and the object being transferred.

BITS stopped transferring the evil.png transfer job that is associated with the <https://i.imgur.com/evil.png> URL. The status code is 0x0.

#### Validate Hunt

* 2021-12-15 – Hunt has been tested against a small subset of data and test data has been found. 200 False positives discovered related to third party programs such as browsers. Baseline has been adjusted to filter unrelated data.
* 2021-12-15 Hunt has been tested against a small subset of data and test data has been found .50 False positives discovered related to known good processes. Baseline has been adjusted to filter unrelated data.
* 2021-12-22 – Hunt has been tested against a small test environment and test data has been found. False positives have not been discovered nor any hits for malicious activities
* 2022-01-22 – Hunt has been tested against a large test environment and test data has been found. 15 False positives discovered relating to program setup. Baseline has been adjusted to filter unrelated data
* 2022-02-22 – Hunt has been tested against a large subset of data in the environment and test data has been found. No false positives discovered, only test data remains. Able to be pushed to production.

#### Document Findings

* 2021-12-14 BITS Windows event logs are currently not being ingested into the centralized SIEM. Threat Hunting team working with the security team to enable data logging and storage. Ticket Number 1234 has been created
* 2021-12-15 Ticket Number 1234 resolved. BITS Windows event log 59 and 60 is currently ingested into the centralized SIEM. Potential blind spots may occur within the organization that are related BITSAdmin process due to events only being ingested from the North American domain not the European
* 2021-12-15 – Detection of possible malicious transfers identified on the hosts XFIR\_Banshee
  + Ticket 778 has been created to research URL and consult with Admins to determine if the transfers are legitimate. bitsadmin /transfer myDownloadJob /download /priority normal https://downloadsrv/10mb.zip c:\\10mb.zip
  + Ticket 778 has been resolved. Determined as a false positive due to administrative activities.
  + Baseline has been tuned to adjust hunt. False positive has been documented.
* .
* 2021-12-15 – Ticket 123 has been submitted to SOC to convert this hunt into an automated detection.
* 2021-12-18 SOC has updated Ticket 123 with their ADS documentation for approval
* 2021-12-20 Hunt team approves SOC ADS
* 2021-12- 20 Hunt successfully converted to ADS on this date, with ticket 123. Hunt closed.

#### References

Phishing Campaign Leveraging BitsAdmin: https://unit42.paloaltonetworks.com/unit42-unique-office-loader-deploying-multiple-malware-families/

BITS used to download malware: https://www.secureworks.com/blog/malware-lingers-with-bits

https://isc.sans.edu/forums/diary/Microsoft+BITS+Used+to+Download+Payloads/21027/

https://marcoramilli.com/2018/08/31/hacking-the-hacker-stopping-a-big-botnet-targeting-usa-canada-and-italy/

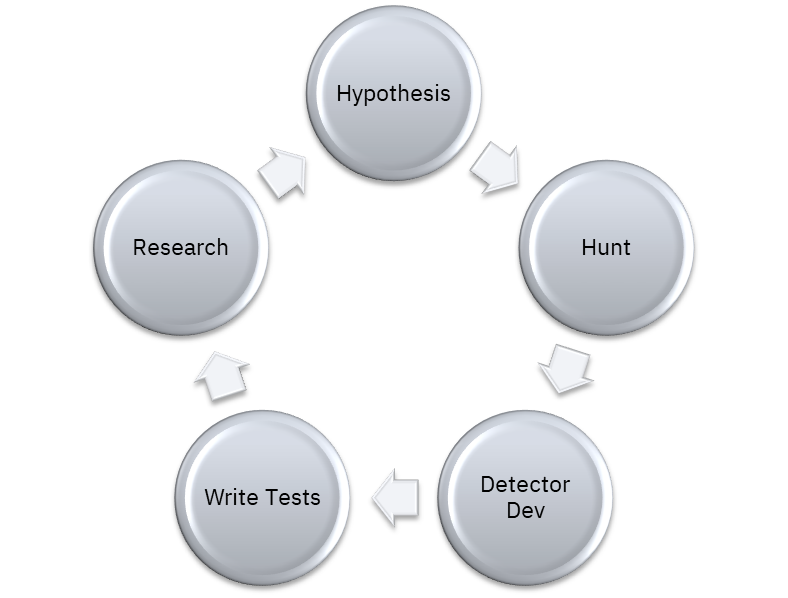
## Automation

Pioneered by Google through their “Hunt Once” approach which asks hunt teams to design and execute a threat hunt one time and then build an automated hunt that can run continuously as a detection. Automation is a fantastic way to scale threat hunting operations so a small team of hunters can execute effective hunts against large environments. Additionally, automation enables hunters to dedicate valuable time to developing new and interesting hunts using complex datasets and analysis techniques rather than executing the same hunts on a regular interval.

Not every organization will have the people, processes, or technology to implement automation however, given the benefits of automation all threat hunting organizations should consider building a roadmap leading towards automation.

Core requirements to transition threat hunts to automated detections

* Accurate, Complete, Consistent, Timely, Unique, and Valid datasets within high availability tools that can maintain a continuous search and trigger a notification when the hunt conditions are met.
* Well-defined and validated hunt that is highly tuned on hunt signal that will not decay
* Defined criteria to identify and approve hunts for automation
* A defined process to migrate a hunt from the threat hunt team to the security operations team or the technical capabilities to create custom software or tools through a defined automation standard such as Robotic Process Automation
* A documentation standard for all automated detections



Google Hunt Once Process

### Identification

The first step in building an automation identification process is to understand the strengths of humans vs computers.

Humans are exceptional at dealing with:

* Uncertainty
* Ambiguity
* Pattern recognition
* Decision making
* Judgement calls when circumstances change

Computers shine when:

* Consistent execution of the same process is required
* When a process or activity is required to scale rapidly
* When a process requires fast computational processing or complex condition matching

The hunts that are most likely going to contain characteristics that are more suited for automation are:

* Time-consuming and time critical hunts with high transaction volumes. These hunts hinder human performance but not computers.
* Repetitive hunts that require constant execution will have a bigger positive impact than the ones that are executed occasionally.
* Hunts that are prone to human error due to their computational and conditional complexity
* Hunts that require data fusion or from disintegrated systems can result in human error, so such processes are well suited for computers.

### Automation through Security Operations

Hunter hunt, they should not triage alerts. Clear roles and responsibilities should be created between threat hunt and SOC teams when considering threat hunt automation. The expectation of the threat hunt team is that any hunt that is going to be automated should be so well designed and documented, that the SOC team should not need to deal with any of common issues with weak detections such as false positives and constant tuning. Conversely, the SOC should be expected to take responsibility for transitioning the hunt to an automated detection and apply internal documentation and testing standards.

One of the best frameworks for creating and managing automated detections is Palantir’s ADS Framework[[17]](#footnote-17). The ADS is a well-designed detection documentation and management framework which implements detection documentation in the following manner. This natural language template ensures that any given alert will have sufficient documentation, will be validated for durability, and reviewed prior to production deployment.

* Goal
* Categorization – MITRE framework mapping
* Detection Strategy
  + Data Sources – what data sources to consider/needed for searches
  + Suppression – what is known good state to filter (processes and network based)
  + Action
* Technical context: details of TTPs, related data sources and how it is an evidence of adversary presence
* Blind spots and assumptions:
  + Blind spots occur when assumptions are violated.
* False positives: what false positives are feasible based on known good and search criteria
* Response: how organization should response if threat hunt provides a positive result, i.e. detects the presence of adversary in the environment.
* Other relevant resources

For more information regarding the ADS, reference the ADS GitHub project[[18]](#footnote-18) here:

<https://github.com/palantir/alerting-detection-strategy-framework>

https://blog.palantir.com/alerting-and-detection-strategy-framework-52dc33722df2

### Robotic Process Automation (RPA)

For organizations that have the technical capabilities to design custom solutions for automated threat hunting, the Robotic Process Automation (RPA) can be used as a framework to ensure that any automations are well-designed, effective, and well documented. RPA is a form of business process automation that allows organizations to define sets of instructions for a “bot” to perform. RPA bots are any technical mechanism that replicate human-computer operations to carry out a ton of error-free tasks, at high volume and speed. RPA software utilizes RPA bots to automate routine tasks within software applications normally performed by a human. These bots are designed to eliminate the need for humans to conduct time-consuming, repetitive, and tedious tasks. Threat hunting operations can leverage RPA software to develop custom bots to execute threat hunts that have been identified as good candidates for automation. There are many RPA software vendors available. Organizations will need to find the right vendor or product to suit their budget and operational needs.

<https://en.wikipedia.org/wiki/Robotic_process_automation>

<https://www.techtarget.com/searchcio/definition/RPA>

1. https://github.com/palantir/alerting-detection-strategy-framework [↑](#footnote-ref-1)
2. https://attack.mitre.org/groups/ [↑](#footnote-ref-2)
3. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf [↑](#footnote-ref-3)
4. https://doi.org/10.6028/NIST.SP.800-171r2 [↑](#footnote-ref-4)
5. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf [↑](#footnote-ref-5)
6. K. Jabbour and S. Muccio, “The Science of Mission Assurance,” Journal of Strategic Security, vol. 4, no. 2, pp. 61–74, 2011. [↑](#footnote-ref-6)
7. https://securedecisions.com/wp-content/uploads/2011/06/Camus-Automatically-Mapping-Cyber-Assets-to-Missions-and-Users.pdf [↑](#footnote-ref-7)
8. L. Buchanan, M. Larkin, and A. D’Amico, “Mission Assurance Proof-of-Concept: Mapping Dependencies

   among Cyber Assets, Missions, and Users,” in IEEE International Conference on Technologies for Homeland Security (HST), 2012, pp. 298–304. [↑](#footnote-ref-8)
9. Quote by Lewis Carroll [↑](#footnote-ref-9)
10. https://whatis.techtarget.com/definition/hypothesis [↑](#footnote-ref-10)
11. https://www.cybereason.com/blog/how-to-generate-a-hypothesis-for-a-threat-hunt-techniques [↑](#footnote-ref-11)
12. https://martinfowler.com/bliki/GivenWhenThen.html#footnote-ivan [↑](#footnote-ref-12)
13. Ready to hunt? First, Show me your data! - <https://posts.specterops.io/ready-to-hunt-first-show-me-your-data-a642c6b170d6> [↑](#footnote-ref-13)
14. http://mitiq.mit.edu/ICIQ/Documents/IQ%20Conference%201996/Papers/DODGuidelinesonDataQualityManagement.pdf [↑](#footnote-ref-14)
15. Atomic Red Team - <https://github.com/redcanaryco/atomic-red-team> [↑](#footnote-ref-15)
16. https://en.wikipedia.org/wiki/Signal-to-noise\_ratio [↑](#footnote-ref-16)
17. https://blog.palantir.com/alerting-and-detection-strategy-framework-52dc33722df2 [↑](#footnote-ref-17)
18. https://github.com/palantir/alerting-detection-strategy-framework [↑](#footnote-ref-18)