Open Threat Hunting Framework

V0.1

Table of Content

Table of Figures

1 Introduction

Establishing or maturing an effective threat hunting program is a challenging task compared to approaching threat hunting from an unofficial perspective where existing security resources execute ad-hoc hunts in their spare time however, a well-designed and dedicated threat hunting program can be a major driver in changing the security culture of an entire organization.
The purpose of this document is to provide foundational understanding of Threat Hunting and introduce the Open Threat Hunt Framework (OTHF) which are practical guidelines to developing and maturing an effective threat hunting program.

The goal of the OTHF is to provide organizations with a framework which provides guidance on implementing core organizational, operational, and technical components to launch and mature threat hunting operation. The OTHF is completely vendor and tool agnostic and not meant to be an exhaustive resource on threat hunting techniques or analysis but instead designed to present organizations with often overlooked pieces of threat hunting that have a massive impact on the success of the program.

While the overall OTHF is designed for organizations attempting to launch and mature a dedicated threat hunting program staffed with dedicated resources, the OTHF is modular by design to accommodate organizations who are unable to staff a dedicated team but can still leverage the operational components to begin or improve threat hunting within their organization.

2 Foundational

2.1 Organizational Support

"Going it alone, you won't last a day out there" – Sandor Clegane, Game of Thrones
To launch and mature an effective threat hunting program, it is critical to have buy-in for executive leadership and sometimes that can be a difficult conversation to heave with leadership. A major security benefit form threat hunting is that is offers the ability to verify assumptions about the design, controls, and behaviors of a network but it also operates within a space that assumes that existing security protections have failed. Security investments continue to increase year over year so when approaching leadership to support investing in a threat hunting team, consider the following guidelines.

Gaining the support of the chief security officer (CSO) or chief information security officer (CISO) is critically important, and efforts should be made to gain executive support beyond the security organizational boundaries. The more executive support a threat hunting program can get the better. If a threat hunting program does not gain executive support, the effectiveness and growth of the program will be limited.

Depending on the organization, obtaining long term support from executives can be challenging but demonstrating the value of threat hunting by showing how threat hunting can help reduce risk, reduce dwell time, and enhance existing security teams within the organization can help leadership understand the value add and buy into the effort.

The following are some data points which can be used to gaining leadership support:

- If your organization has experienced any breaches, present dwell time, impact, and cost data associated with the breaches
- Present third-party evidence related to the cost of data breaches
- Present dwell time data from third-party resources
- Compare recent penetration testing or red team exercise activities against existing security tooling highlighting the gaps in detections
- Consider scheduling a compromise assessment and using the results as data point to highlight identified risks, threats, or lack of visibility

The following are some talking points to discuss with leadership regarding the value-add of threat hunting:

- Reduce the average time to detect threats
- Increase the quality of automated detections to reduce alert fatigue and improve security operations
- Ensure security controls are adequate
- Reduce costly incident response activities
- Protect intellectual property and brand reputation

Be prepared to submit an official proposal to start a threat hunting program including an executive summary, justification, cost schedule and deliverables. The following sections within this framework will be valuable resources in developing the proposal:

- Resources and Staffing

- Data and Technology Audit
- Metrics

It is quite ok to start small, demonstrate value, and then expand threat hunting operations as the team provides value to the organization. Details regarding short- and long-term goals and milestones should be included within the proposal.

2.2 Organizational Placement

While not a critical component to begin or run an effective threat hunting program at an organization, the placement of the threat hunting team within an organization can directly impact how well the value threat hunting is bringing to the organization is communicated to leadership.
The placement of the threat hunting team may depend on the staffing model of the threat hunting program. If threat hunting is going to be executed as a part time function within an existing team obviously, changing the organizational layout will be challenge however to maximize the effectiveness and growth opportunities for a threat hunting program, it is best if the threat hunting team directly informs security leadership such as the CISO or CSO. Directly communication lines between threat hunters provides leadership direct, unfiltered input into the state of security within the organization.

2.3 Threat Hunting Definition

"Ask 10 security professionals for the definition of threat hunting and you'll get 11 answers"
Each organization that wants to launch or has a threat hunting program must define what threat hunting means to the organization and that definition should be driven by the mission statement of the threat hunting program. The OTHF is not designed to act as the authority of what is or isn't threat hunting because threat hunting means a lot of different things to a lot of different people and that's ok. The only requirements regarding the definition of threat hunting that the OTHF includes is:

1. The organization should decide on and document the definition of threat hunting
2. The definition of threat hunting should be driven by the mission statement of the threating hunting program

Considerations organizations should include when defining threat hunting:

- Avoid hunting for activities that are already being detected by differentiating between proactive from reactive efforts
    - If you define threat hunting as an activity that involves purposefully seeking out evidence of malicious activities within the environment that did not generate security alerts, the organization can avoid duplications of effort and maximize value add to the organization. Additionally, if an organization specifically calls out how threat hunting is a proactive approach to cybersecurity, it can eliminate confusion as to how threat hunting differs from incident response or security operations responding to an alert.

- Describe threat hunting as a dedicated, repeatable process
    - Threat hunting benefits from a methodical approach. From the threat hunters perspective, hunters will benefit from a disciplined approach to understand the threats applicable to the target environment, understand their respective techniques, tactics, and procedures, and then use that information to determine what clues to look for that

might indicate an attack underway. Additionally, a well-defined process makes it easier to track improvements, increase collaboration, and provide quality control.

- The value of including language to ensure threat hunting is based upon a hypothesis
    - The main advantage of leveraging a hypothesis-based threat hunting model is that it ensures that a threat hunt is testable and provides guidelines to determine success or failure. Additionally, a hypothesis provides a clear statement of the question that the hunter intends to investigate. Without a hypothesis, a threat hunting can become unfocused and difficult to conclude any sort of concrete findings. There are activities within threat hunting that may not have a formal hypothesis such as generation observations on the behavioral data of systems or users within the network such as "I wonder how many users actually use PowerShell on a day-to-day basis?" however such observational research should be used to create a hypothesis-based threat hunt.

Example definitions of threat hunting:

- Threat Hunting is a dedicated, continuous, hypothesis-based search methodology to reduce the time to detect adversaries operating within an environment that have yet to be detected.
- "Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network".[1]
- "Cyber threat hunting is a proactive security search through networks, endpoints, and datasets to hunt malicious, suspicious, or risky activities that have evaded detection by existing tools."[2]
- "Threat hunting is the practice of searching for cyber threats that might otherwise remain undetected in your network."[3]
- ""a focused and iterative approach to searching out, identifying, and understanding adversaries internal to the defender's networks."[4]

2.4 Mission Statement

It is essential that organizations set the clear expectations, principles, and a vision for the Threat Hunting Team. A mission statement is a critical component to help communicate the purpose and direct the threat hunting program in the right direction. The growth and success of the threat hunting program will be dependent on short-, medium-, and long-term goals and the mission statement provides an invaluable navigation tool to define and obtain goals. It is important to note that a mission statement is not meant to be something used during just the launch of the threat program but a navigational beacon that provides direction as the program grows and matures. Additionally, a well-constructed mission statement will help the team see the meaning and purpose of their work by giving them clear reasons their job benefits a larger goal. The best part about mission statements is that they can always been changed. Do not be afraid to replace or revise your mission statement as your threat hunting program grows and matures.

---

[1] https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

[2] https://www.trellix.com/en-us/security-awareness/operations/what-is-cyber-threat-hunting.html

[3] https://www.checkpoint.com/cyber-hub/cloud-security/what-is-threat-hunting/

[4] https://www.sans.org/white-papers/who-what-where-when-why-how-effective-threat-hunting/

Consider the following example mission statement:
To be the driving force in custom automated adversary detection targeting XYZ .
From this mission statement, the reader immediately understands that this threat hunting program is focused on hunting for adversary activities and creating automated detections specific to the organization so it's reasonable to assume that a big focus of this threat hunting program would be identifying and understanding relevant adversaries and developing threat hunts that would transition well to custom automated detections.
Here are some recommendations for building a mission statement for threat hunting:

- Keep it concise and do not exceed more than one or two sentences and
- Consider including language to ensure that threat hunting is meant to compliment existing security teams, not replace them
- Get feedback and include the team members in its development
- It's not important to include details into how goals will be achieved
- Attempt to include components that align with the mission statement and core values of the overall organization

2.5 Strategy

The strategy of a threat hunting program is a thoughtfully constructed plan or approach that outlines how the program will achieve the mission. It's worth nothing that strategies play a role in how goals and objectives are accomplished as well but for the purposes of this section, we will focus on strategy as it relates to the program's mission.

A well-crafted strategy provides a clear roadmap sets the tone of the actions people in the organization should take and identify the priorities to achieve the desired goals. It is important to note that a strategy is not a mission statement. When applied properly a strategy will dictate how resources will be allocated to accomplish the mission. Therefore, threat hunting organizations should develop a mission statement first before developing a strategy for the threat hunting program.

It is worth noting that an organization's strategy is dynamic as it will continue to change as it adapts to new goals and objectives. Strategies are critical to the success of a threat hunting program because they are the driving force behind creating the plans and actions to accomplish goals.

Figure 1: Setting up Threat Hunting Mission, Strategy, Goals and Objectives

3 Structure

3.1 Roles and Responsibilities

3.2 Resources and Staffing

3.3 Skills Matrix

3.4 Maturity

3.4.1 OTHF Maturity Model

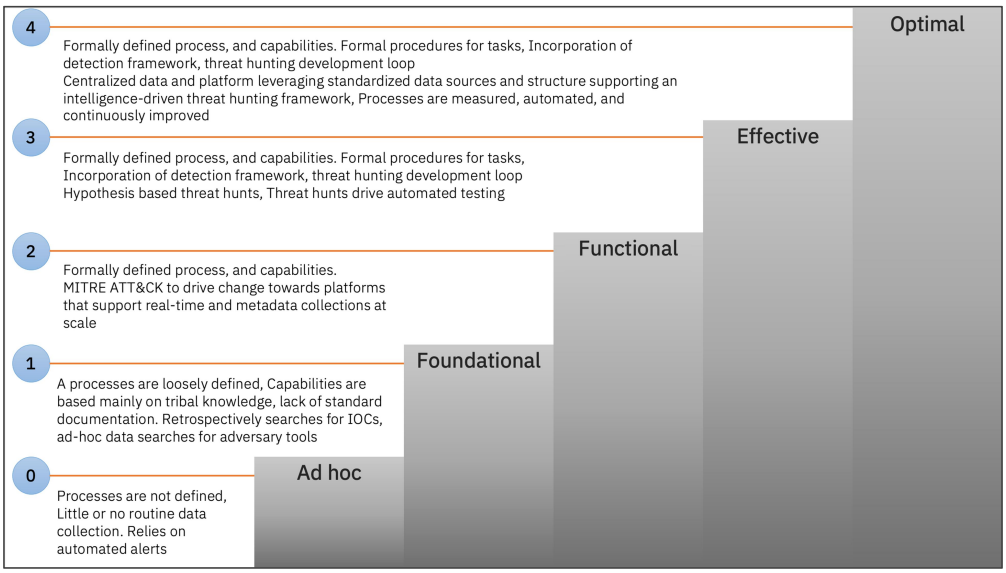


Figure 2: OTHF Maturity Model

4 Preparation

"Data" is everything. Without data, there is nothing to investigate, nothing to hunt for. Reliability of the data determines how productive and efficient will be your hunt team. It won't be wrong to say Data Science is a key element of Threat Hunting. Therefore, it is important to discuss data, data reliability and data dictionary.

4.1 The Data

Threat hunting involves analyzing data from variety of sources to recognize unusual patterns. There is no standard on how much data will be needed or what data sources will be needed for specific threat hunt.

These logs would come from network activity and the data from operating systems of endpoints and applications. First, it is important to understand, based on the operational environment, what fundamental data sources are available at your disposal. The data sources can be categorized as network, end points or security relevant. The security event data would come from:

1) Physically controlled areas: Data centers, Server Racks / Cabinets, or Control Centers have gates for access control, CCTV cameras, or heat sensors.
2) Networking devices: this would include network access control devices such as web proxies, firewalls and intrusion prevention systems, detective controls such as intrusion prevention systems.
3) Network traffic: packet capture
4) Operating system on End Points: Different end points such as servers, workstations, or Human Machine Interaces (HMIs) provide system events (operations performed by OS) and audit events.
5) Applications and Services: Customized or Commercial Off The Shelf (COTS) applications, services, Application Programming Interfaces (APIs) will provide data request and responses, usage information and other significant events.
6) Security software: Data from Antimalware software, and vulnerabilities management software

The information should be documented in detail with standardized metadata in a central repository. This metadata repository is also called as event data dictionary. It is important because different fields / attributes available in the event data could provide contextual information for data analysis and correlation.

4.2 Developing and Maintaining Data Dictionary

Threat hunting requires a thorough understanding of normal operations. That means, it is essential to know every single data source logged and collected for development of analytics
e.g. Security, Sysmon or PowerShell logs. Beyond log sources, team should also know the attributes behind every log data collected. Why?, data scientists or analysts spend 80% of their time just finding, cleaning and organizing data. Threat hunting effort is no different. The threat hunter must have an easy way to discover, access and share the data.

"Data Dictionary" solves this problem. The Data Dictionary is a collection of names, definitions, and attributes about data elements that are being used or captured. Data dictionary helps avoides data inconsistencies, provides consistency in the collection and use of data, and enforces the use of data standardization. A data dictionary should become the go-to tool to understand everything about a data set and check data quality at a glance.
If you have recently initiated or kicked-off the Threat Hunting program or have no data governance team, it is likely that Data Dictionary doesn't exist within your organization. Creating Data Dictionary is not a small

endeavor. Effort required to develop the data dictionary largely depends on the technology landscape of the organization, organizational processes and available human resources. Organizations may choose to develop it all at once (focused project) or gradually develop and improve this library during different security initiatives.
Specific contents in a data dictionary can vary. In general, these components are various types of metadata, providing information about data. When planning to create a data dictionary, it is important to consider all available data management resources, including databases and spreadsheets. Online templates are useful for creating this type of data dictionary . Dragos introduced "Collection Management Framework"[5] that provides guidance on keeping track of tools used and data being collected.
Initiate the development by assessing and documenting the tools implemented and configured in your organization. Start by listing the data sources at high-level and then collect more detailed information from each data source Following resources could be useful for development.

- Existing commercial security tools within your ecosystem (i.e EDR solutions) that collect data for you, your vendor should be providing data dictionaries for every security event.
- Open-Source Security Events Metadata (OSSEM)[6]. OSSEM defines and share a common data model to improve the data standardization and transformation of security event logs. It also allows you to define and share data structures and relationships identified in security events logs.
- MITRE CAR[7] provides the dictionary of data objects that may be monitored based on MITRE ATT&CK framework

4.3 Data Reliability

Let us focus on the use of data now. Threat hunter will use scientific methods, processes, algorithms and systems to extract knowledge and insights from noisy, structured and unstructured data, and apply knowledge from data across a broad range of application domains. Therefore, data reliability crucial. It is an aspect of data quality that defines how much data is complete and accurate. This improves the data trust. It eliminates the guesswork, gives accurate analysis and insights.

Reliable data is:

- Complete – datasets must contain all required information. It should not be limited to high value assets.
- Accurate – data must conform with reality.
- Timely – data must be accurate in a specific period.
- Validated – data must have right values for the attributes.
- Consistent – data may get stored and transported to different applications, quality of data must be maintained.
- Unique – the data set shouldn't be recorded more than once.

Low reliability of the data can result in aggregations of incorrect data that can lead to wrong decisions that is, incomplete or incorrect hunt results.
Therefore, investing in data reliability consistently will yield faster and reliable threat hunts. It will allow the automation of detection, essential for effective security monitoring.
Mature security organizations likely have security data governance team to improve the reliability of the data required for security monitoring. However, that does not guarantee the data reliability. It is feasible

[5] Collection Management Frameworks – Looking Beyond Asset Inventories in Preparation for and Response to Cyber Threats
[6] https://github.com/OTRF/OSSEM
[7] https://car.mitre.org/

that team runs into the issues such as coverage, missing data, missing standard naming conventions, parsing issues, and timestamp.
Therefore, it is essential that Data Governance and Threat Hunt teams work side by side, share the hunt objectives and findings. This feedback process will ensure the continuous improvement needed for improving data reliability.
In the absence of data governance team, Threat Hunt team should assess and improve data reliability.

4.4 Technology Stack

The event data generated by different data sources within the organization is continuous. The Size of an organization greatly influences the volume of data it generates. On any given day, a large organization can generate hundreds of gigabytes of log data. When dealing with that much data, there are some common issues. The automated data collection, storage and analytic tools is ideal while analyzing the large volume of data and correlating multiple data sources.

Log management systems allow log data collection, data retention, log indexing, reporting, and searching capabilities. Whereas, Security Incident and Event Management (SIEM) system is characterized by Security Event Management (SEM), Eecurity Information Management (SIM), and Security Event Correlation (SEC). SIEM automatically correlates, including all your log data, better than what humans can do alone. SIEM approaches log analysis with a security focus.
Organizations have finite resources. Therefore, organizations prioritize the log sources and data management. Threat hunter must be aware of what data has been automated and is made available at a centralized location (log management system) and what data must be collected and extracted manually.
Threat hunters use a variety of tools to support their methodologies. Tools can include the following:

- Log management system: this allows threat hunter to query, analyze and correlate large volume of data. Allows data analysis and correlation at scale.
- Advanced analytics and statistical analytics tools: If organization has not implemented log management or SIEM, open-source tools such as MongoDB or Redis tools could support ingestion and analysis of large volume of data. Although, feasible, this manual process would require the team to collect and load the data manually. This could be very time consuming as, the team must:
    - develop custom parsers for different log sources for data ingestion
    - develop custom queries for search and correlation of data
- Spreadsheets: This is well known and universally adopted tool for data analysis and statistical analysis. However, it is not optimal while handling large volume of data and correlation.

5 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)[8] and applying lessons learned during incidents responded.

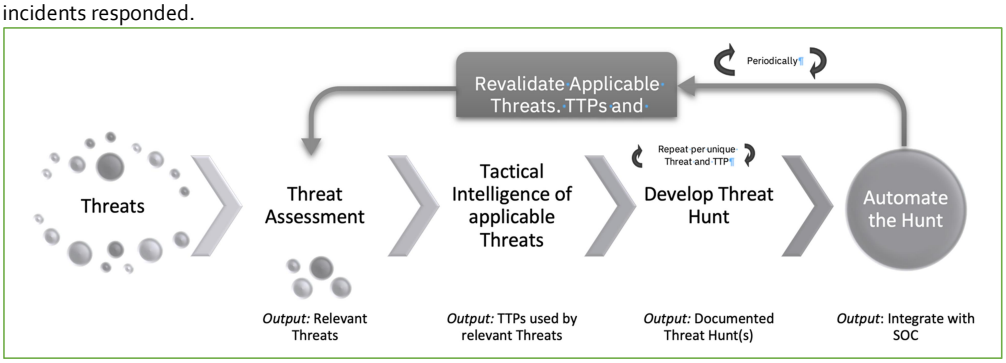


Figure 3: Threat Hunting Framework

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.

5.1 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.

[8] https://github.com/palantir/alerting-detection-strategy-framework

5.1.1 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.

5.1.2 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.

5.1.2.1 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

APT group: FIN7

Names	FIN7 *(FireEye)* Gold Niagara *(SecureWorks)* Calcium *(Symantec)* Navigator *(Fox-IT)* ATK 32 *(Thales)* APT-C-11 *(Qihoo 360)* ITG14 *(IBM)* TAG-CR1 *(Recorded Future)*
Country	Russia
Motivation	Financial crime
First seen	2013
Description	FIN7 is a financially-motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. FIN7 is sometimes referred to as Carbanak, Anunak, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. The reports about arrests made of the mastermind of Carbanak instead of FIN7. However, security research teams keep referring to this arrest for all FIN7 activities since.
Observed	Sectors: Casinos and Gambling, Construction, Education, Energy, Financial, Government, High-Tech, Hospitality, Retail, Technology, Telecommunications, Transportation. Countries: Australia, France, Malta, UK, USA.
Tools used	7Logger, Astra, Bateleur, BIOLOAD, BIRDWATCH, Boostwrite, Carbanak, Cobalt Strike, CROWVIEW, DNSMessenger, Griffon, HALFBAKED, JSSLoader, Lizar, LOADOUT, Meterpreter, Mimikatz, POWERPLANT, POWERSOURCE, RDFSNIFFER, SQLRAT.
Operations performed	Feb 2017 In late February 2017, FireEye as a Service (FaaS) identified a spear phishing campaign that appeared to be targeting personnel involved with United States Securities and Exchange Commission (SEC) filings at various organizations.

Figure 4: ETDA Threat Intelligence on FIN7

5.1.2.2 The 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"[9]. 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/

[9] https://attack.mitre.org/groups/

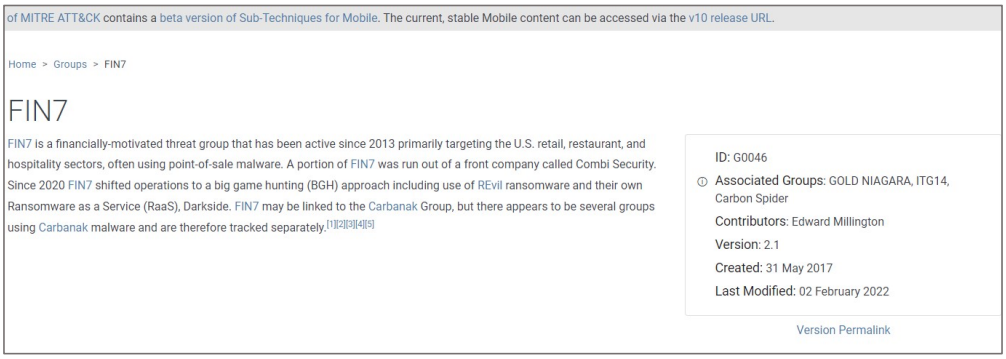


Figure 5: MITRE ATT&CK Threat information on FIN7

5.1.2.3 Other Sources

Secureworks Threat Profiles: https://www.secureworks.com/research/threat-profiles
Mandiant Advanced Persistent Threat Groups: https://www.mandiant.com/resources/apt-groups

5.1.3 Tactical Threat Intelligence

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.

5.1.3.1 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.

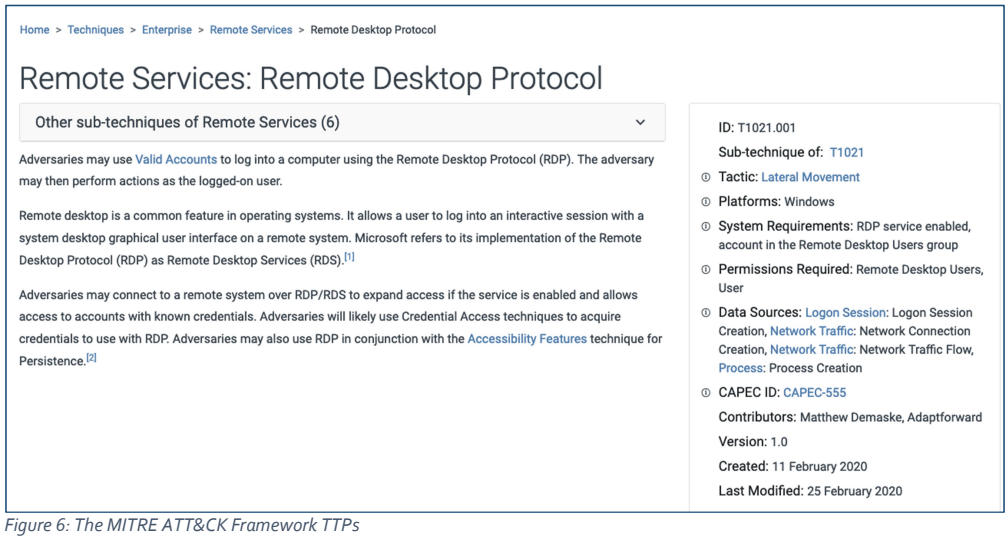
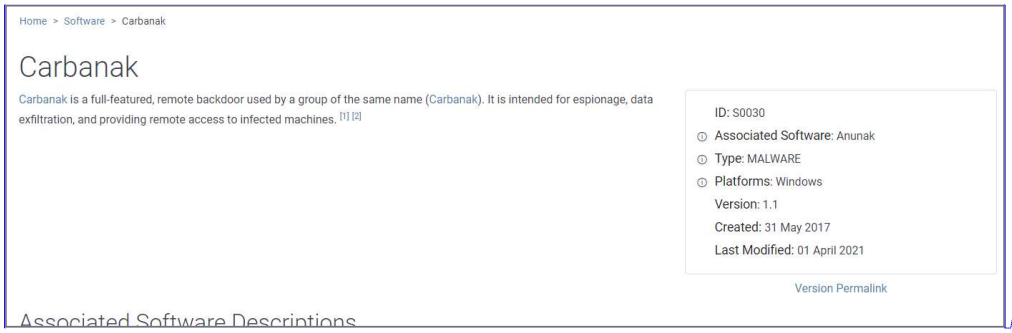


Figure 6: The MITRE ATT&CK Framework TTPs

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.

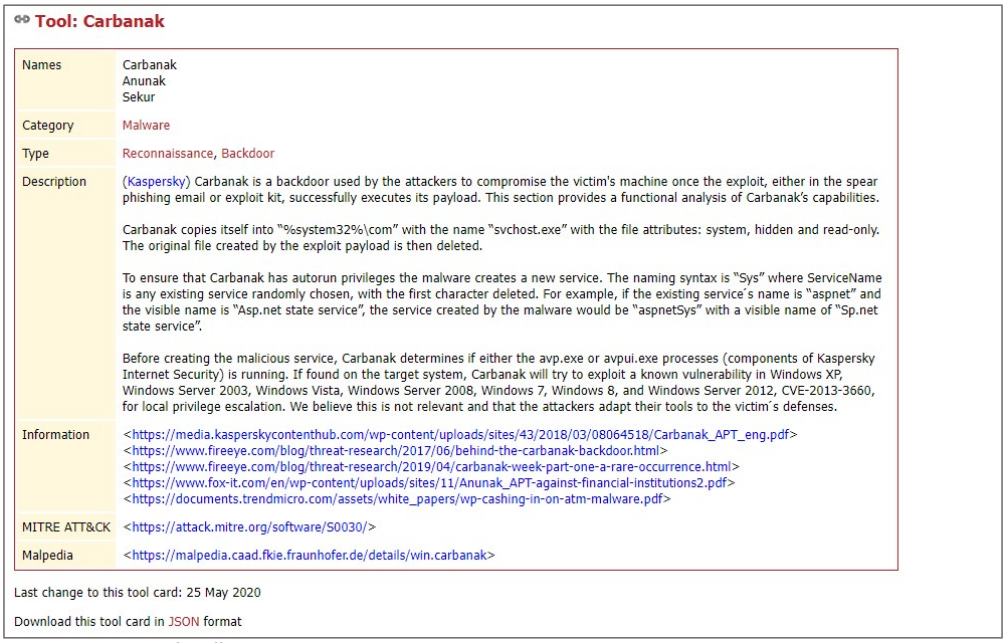


Comment [SSK1]: Is this correctly placed? Needs Caption

5.1.3.2 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



Tool: Carbanak

Names	Carbanak Anunak Sekur
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Kaspersky) Carbanak is a backdoor used by the attackers to compromise the victim's machine once the exploit, either in the spear phishing email or exploit kit, successfully executes its payload. This section provides a functional analysis of Carbanak's capabilities. Carbanak copies itself into "%system32%\com" with the name "svchost.exe" with the file attributes: system, hidden and read-only. The original file created by the exploit payload is then deleted. To ensure that Carbanak has autorun privileges the malware creates a new service. The naming syntax is "Sys" where ServiceName is any existing service randomly chosen, with the first character deleted. For example, if the existing service´s name is "aspnet" and the visible name is "Asp.net state service", the service created by the malware would be "aspnetSys" with a visible name of "Sp.net state service". Before creating the malicious service, Carbanak determines if either the avp.exe or avpui.exe processes (components of Kaspersky Internet Security) is running. If found on the target system, Carbanak will try to exploit a known vulnerability in Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8, and Windows Server 2012, CVE-2013-3660, for local privilege escalation. We believe this is not relevant and that the attackers adapt their tools to the victim´s defenses.
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf> <https://www.fireeye.com/blog/threat-research/2017/06/behind-the-carbanak-backdoor.html> <https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-one-a-rare-occurrence.html> <https://www.fox-it.com/en/wp-content/uploads/sites/11/Anunak_APT-against-financial-institutions2.pdf> <https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0030/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.carbanak>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

Figure 7: ETDA Tactical Intelligence

5.1.4 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 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.

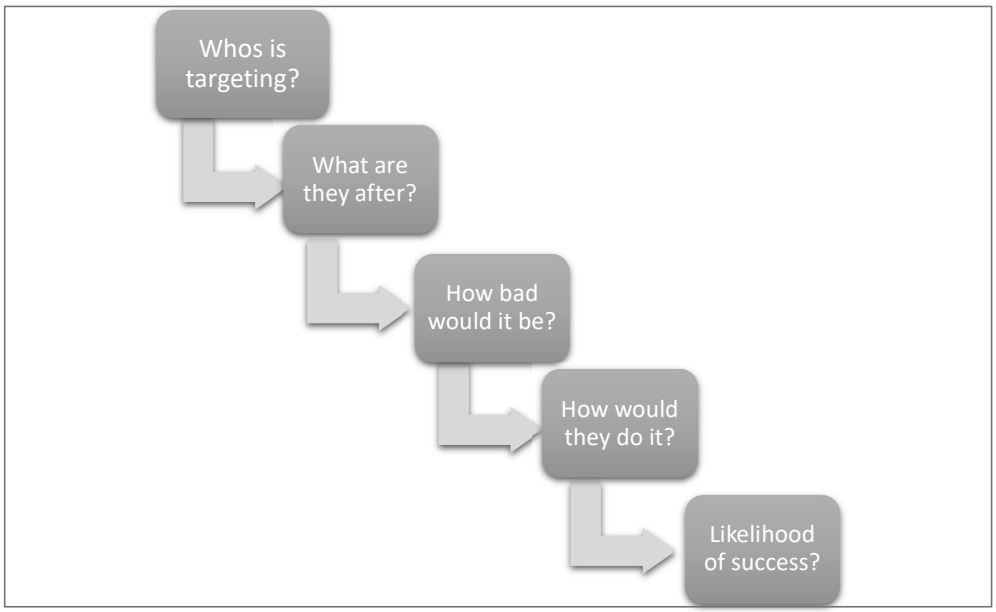


Figure 8: Threat Assessment Process

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.

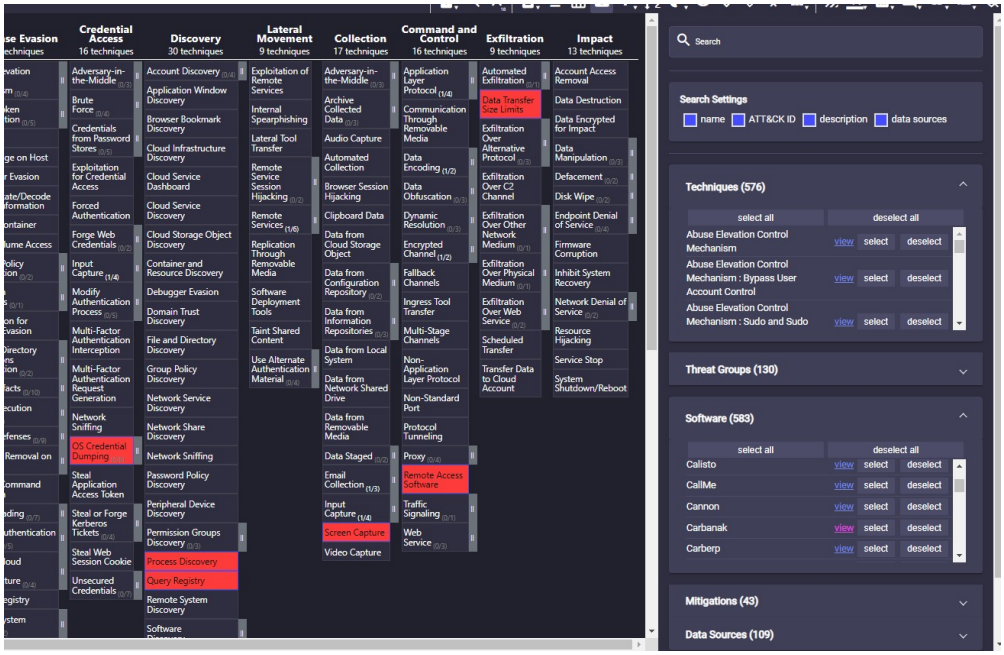


Figure 9: Threat Assessment using MITRE Navigator

5.1.4.1 Vulnerability and Exploit Data Driven

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[10].

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:

[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf

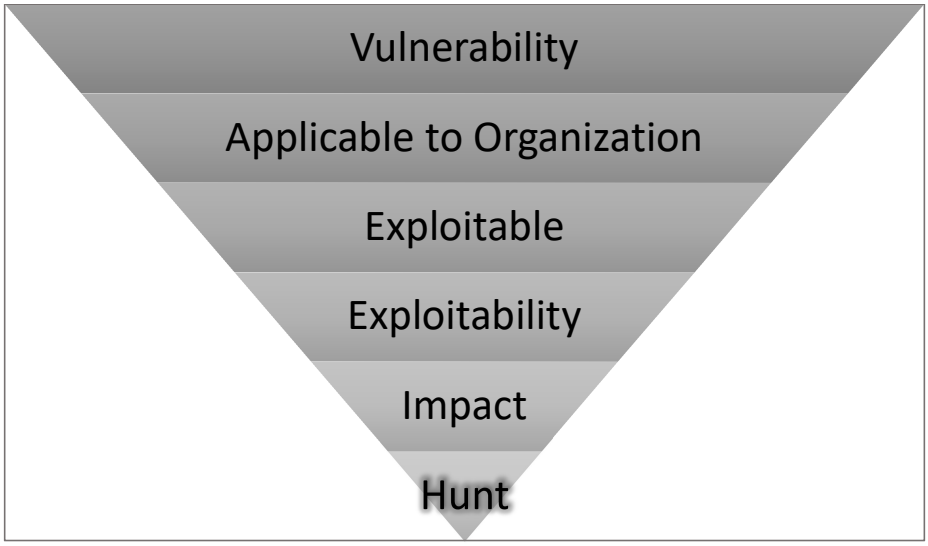


Figure 10: Vulnerabilities and Exploits Driven Hunts

- 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

Vulnerability 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/

5.1.4.2 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."[11]. 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"[12] 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.

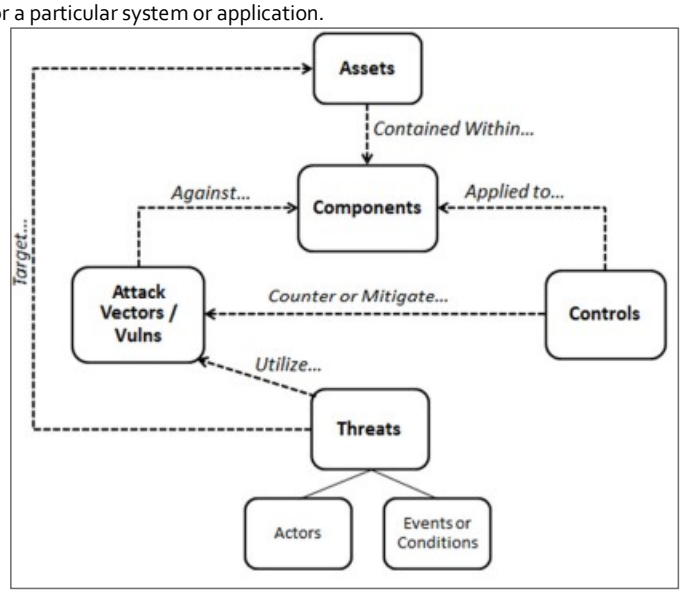


Figure 11: Muckin, Fitch Threats, Assets and Controls Relationship Model

[11] https://doi.org/10.6028/NIST.SP.800-171r2
[12] https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf

5.1.4.3 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,[13]" 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.

[13] K. Jabbour and S. Muccio, "The Science of Mission Assurance," Journal of Strategic Security, vol. 4, no. 2, pp. 61–74, 2011.

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"[14], 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"[15].

Example of 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.

[14] https://securedecisions.com/wp-content/uploads/2011/06/Camus-Automatically-Mapping-Cyber-Assets-to-Missions-and-Users.pdf

[15] 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.

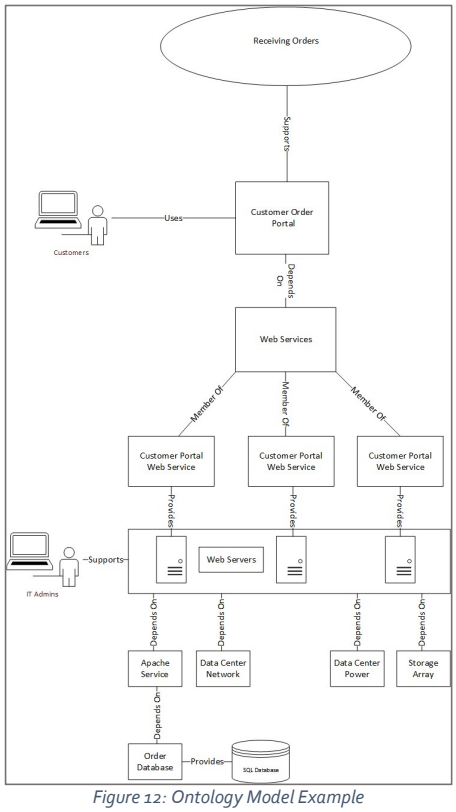


Figure 12: Ontology Model Example

5.1.4.4 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

Hunter creates a hypothesis to hunt for malicious network connected certutil.exe events.

5.2 The 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.

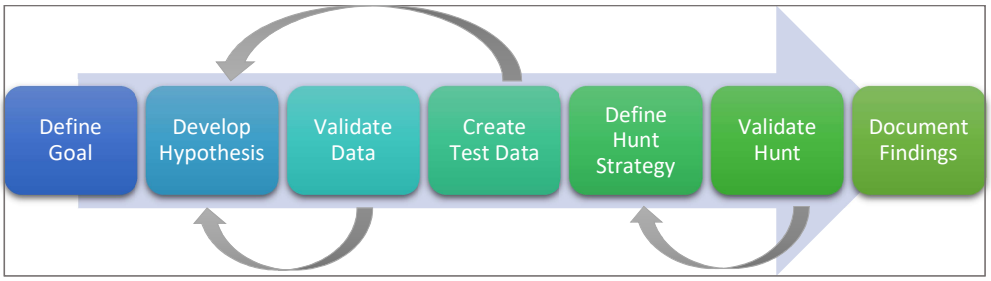


Figure 13: OTHF - Threat Hunting Process

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 14: Detailed Threat Hunting Process~~Figure 11: Detailed Threat Hunting Process~~ provides a detailed project overview and workflow. We explain the process in the text below.

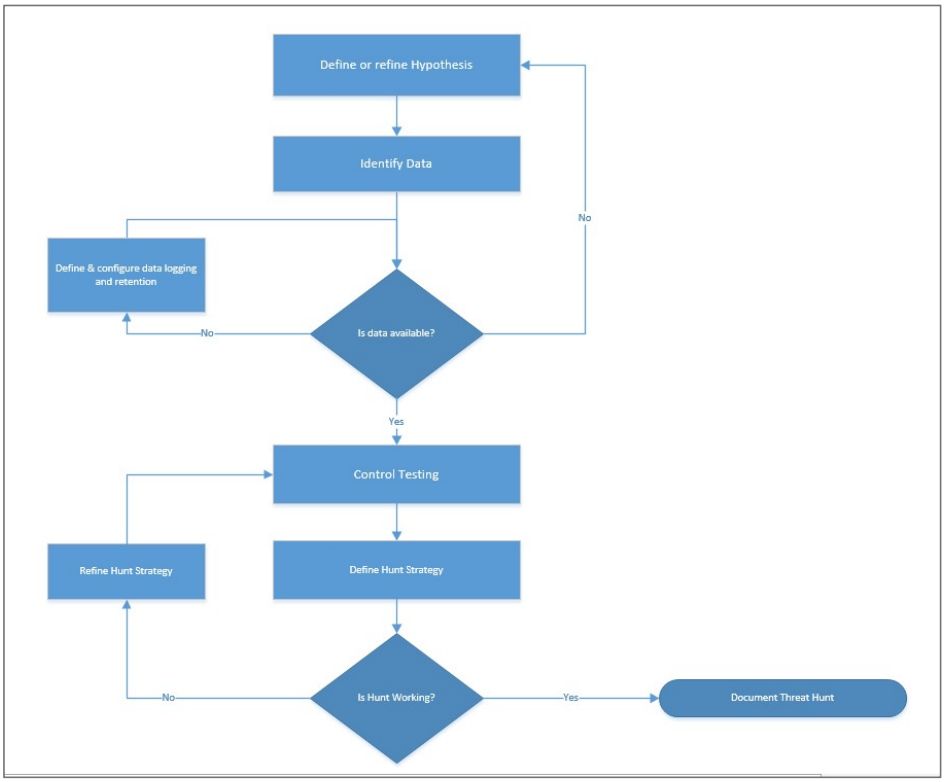


Figure 14: Detailed Threat Hunting Process

5.2.1 Define a Threat Hunt Goal

"If you don't know where you're going, any road will get you there."[16]

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

[16] Quote by Lewis Carroll

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.

5.2.2 Develop Hypothesis

Hypothesis is a testable statement about the proposed explanation for some observed phenomenon[17]. 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

[17] https://whatis.techtarget.com/definition/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[18].

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)[19], 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

5.2.3 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:
    a. 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.
    b. 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

[18] https://www.cybereason.com/blog/how-to-generate-a-hypothesis-for-a-threat-hunt-techniques
[19] https://martinfowler.com/bliki/GivenWhenThen.html#footnote-ivan

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.

c. 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.

d. 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!" [20]. 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.

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).

DOD Total Data Quality Management (TDQM)

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	Percentage of entire data set that is

[20] Ready to hunt? First, Show me your data! - https://posts.specterops.io/ready-to-hunt-first-show-me-your-data-a642c6b170d6

	within a data set.	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.

Table 1: DoD Core Set of Data Quality[21]

Common Information Model
Common Information Model (CIM) standard is a project maintained by DMTF 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. 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.

5.2.4 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[22]. 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

[21] http://mitiq.mit.edu/ICIQ/Documents/IQ%20Conference%201996/Papers/DODGuidelinesonDataQualityManagement.pdf

[22] Atomic Red Team - https://github.com/redcanaryco/atomic-red-team

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.

5.2.5 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.

5.2.6 Validate the 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[23]. 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.

[23] https://en.wikipedia.org/wiki/Signal-to-noise_ratio

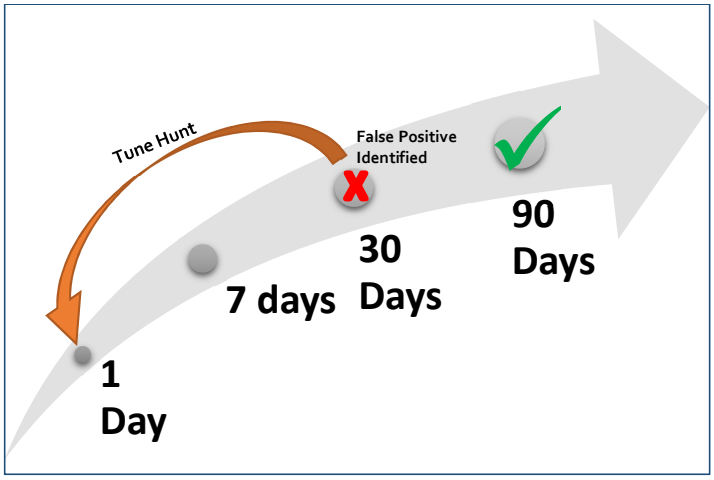


Figure 15: Iterative process of Hunt Validation over range of historical data

5.2.7 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.

5.3 Hunt Tempo

Threat hunts could be triggered by different security initiatives such as:

- New threat intelligence data – e.g. new threat actor, updates to the TTPs from known threat actor(s).
- Cybersecurity Incidents: findings from cybersecurity incidents or lessons learned
- Vulnerabilities reported after red team exercises / penetration testing
- Findings from tabletop exercises: tabletop exercises are excellent way to explore some process and data deficiencies for cybersecurity incident investigations.
- Other threat hunts: Threat hunt may result in findings that may trigger additional hunting projects.
- Identification and analysis of Crown jewels: The crown jewels could be critical processes, assets, or data, if compromised; may result in severe consequences.
- Threat modeling: Threat modeling is process that allows organizations to identify, enumerate and prioritize the threats based on the absence of security controls for the system.
- Regulatory requirements: new or changes in regulatory requirements may influence the need for new hunts. E.g. Changes in detection and reporting regulatory requirements could provide feed in hunt backlog.

It is important to keep the backlog of threat hunt ideas so that team can prioritize and schedule.

5.3.1 Prioritization

With finite resources within the team, it is essential to prioritize the hunts. The prioritization should depend combination on factors as :

1) The TaHiTI[24] (**T**argeted **H**unting **i**ntegrating **T**hreat **I**ntelligence) is a threat hunting methodology that focuses on the top 3 layers of the pyramid of pain – TTPs, Tools, and Network / Host Artifacts. The hunts based on the lower three layers are based on the information received from the past attacks and campaigns – e.g. known bad domain names, IP addresses and hashes. Although important, the targeted attacks with same IOCs may not be a best use of the threat hunt team. Therefore, as team gains maturity, should focus on (or prioritize) top three layers of the pyramid as it can yield high value.
2) Other factors: Apart from general prioritization addressed above as per TaHiTI, following factors should be used for prioritization based on its importance.
    a. Regulatory Requirements: these could allow organizations to maintain their license to operate. Therefore, organizations must prioritize these if requirements change or new requirements for detection and reporting are imposed.
    b. Historical Security Incidents: Historical incidents provide important data points for hunts because those are successful violations of security controls and policies.
    c. Vulnerabilities reported after red team exercises / penetration testing: like historical security incidents, the pen tests or red team exercises provide the TTPs that have been successful.
    d. Risk evaluations of threat hunt ideas: Each threat hunt idea should be evaluated for the risks to the business. If risk to the operational continuity, safety of employees or community, financial or reputational status of the organization is sever, team must prioritize
    e. New Threat Intelligence data: Threats may go dormant or may choose to hibernate for a period. New Threats may emerge or dormant threats may suddenly become active again. The prioritization of threat hunts may get influenced due to this.
        i. A potential threat is more likely to have more impact if it involves observations supporting many different hunting hypotheses. These threats and TTPs should be prioritized above other hunts.
        ii. The absence or downward trend of threat activities does not guarantee that organization won't find it in their environment. Organizations may tend to deprioritize those hunt ideas. Reprioritization of those hunts could be considered. However, those should not be removed from backlog.

5.3.2 Scheduling

Within any organization scheduling is a major pain point, simply because amount of time needed to build the schedule, manage employee availability and other organizational constraints. In the threat hunt

[24] https://www.betaalvereniging.nl/en/safety/tahiti/

organization, team would need two different types of scheduling focus as detailed below. In any case, team should remember, scheduling is not a one-time activity. It is continuous and on-going effort. Regular status reporting, updating of the schedule and the management of schedule changes on a regular basis ensures the schedule is "useful".

5.3.2.1 Resources Scheduling:

Resource scheduling is very important for the Threat Hunting group to schedule threat hunts by using organizational resources in most effective and efficient manner. Resources are the are primary sources of productivity and profitability upon which organizational strategies are frames. Organization has finite resources; therefore, resource scheduling methods must incorporate time and resource capacity into the scheduling process. There are predominantly two methods of resource scheduling[25]:

1. Time-constrained scheduling: assumes that time constraints are fixed and activities must be undertaken within defined time constraints. This method assumes
2. Resource-constrained scheduling: assumes that the resources are finite. Therefore, it emphasizes that task activities must be conducted primarily within resource constraints.

Team should remember, no one technique is perfect. The managers should combine these techniques to effectively plan and schedule the hunts.

Here are few scheduling techniques that will help speed up your threat hunt scheduling process:

1. Maintain Threat Hunt Backlog: Within agile project management, product backlog term is referred often. It refers to a prioritized list of functionality which a product should contain. It is sometimes referred to as a to-do list, and is considered an 'artifact' within Agile Scrum framework. Threat hunt team should use this concept to maintain the list hunt requirements and ideas collected by the team. Establishing an appropriate backlog is very important. When teams have too little work in the backlog, there is a risk of sitting idle. That wastes time and money. On the other hand, when teams have extensive backlogs with excessive detail, the business runs the risk of having over-invested in the plans that can change. That also wastes time and money. Therefore, a middle ground is essential. The entire backbone of planning depends on the goals and resources required for the hunt. Therefore, team should maintain these requirements in the backlog.
2. Ensure staff and resources availability: Team should manage general availability by having employees mark what times and days they are not available. General availability consists of days or times when a person is normally unable to work. The availability management should be extended to other required resources as well. It is possible that organization has finite hardware and software resources needed for the.
3. Use a template: Find a template that you are comfortable using that helps you get your job done faster. A lot of companies use Excel for this, which can be kind of difficult to manage, but pick something that works well for you.
4. Create a schedule based on the employee's skills and resources available: It is important to create a schedule that matches the right team member to the job at hand. E.g. Hunts that focus on collecting and analyzing network telemetry should be managed by networking subject matter experts. Hardware and software resources required for hunts may constrain your ability to freely schedule hunts. Therefore, scheduling process should include employees and other resources needed for hunts.

[25] https://www.pmi.org/learning/library/resource-scheduling-capacity-schedule-construction-5376

5. Evaluate the scheduling process: monitor and evaluate your schedule in real time. Use visual way to spot the gaps, overlaps, and potential errors in your scheduling process.
6. Effectively communicate: All organizations know the importance of communication, and no more important is effective communication than where employee schedules are concerned.

5.3.2.2 Threat Hunt Project:

Above, we discussed scheduling constraints and best practices for the operational threat hunt organization. Now let us look into project management, i.e. managing threat hunt. Each threat hunt is a time bound activity with specific inputs and expected results. Therefore, threat hunts are like projects. Breaking down hunt in manageable tasks is essential. It allows the team to schedule (determine the timeline), and reality of the delivery of the hunt. Scheduling is an integral part of project management; therefore, it has been a key knowledge area in Project Management Institute[26]'s (PMI) core publication - Project Management Body of Knowledge (PMBOK® Guide). Here is a simple guidance for threat hunt project scheduling:

3. Develop a reusable Work Breakdown Structure and Work Packages: A reusable work breakdown structure should be maintained. This can be optimized for specific hunts as needed. The work breakdown allows the team to refine work packages (tasks) needed during the hunt.
4. Schedule: Work packages can be used to assign duration, identify task interdependencies and resources needed to complete specific task.

Use a template for Project Plan: Project planning templates or software tools allow you to create and maintain the detailed project timeline effectively. Microsoft Project tool is widely used. However, Microsoft Excel can be used as well. PMI has several ready to use templates [27]that can be used for this.

5.4 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

[26] https://www.pmi.org/
[27] Project Management Templates

- 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

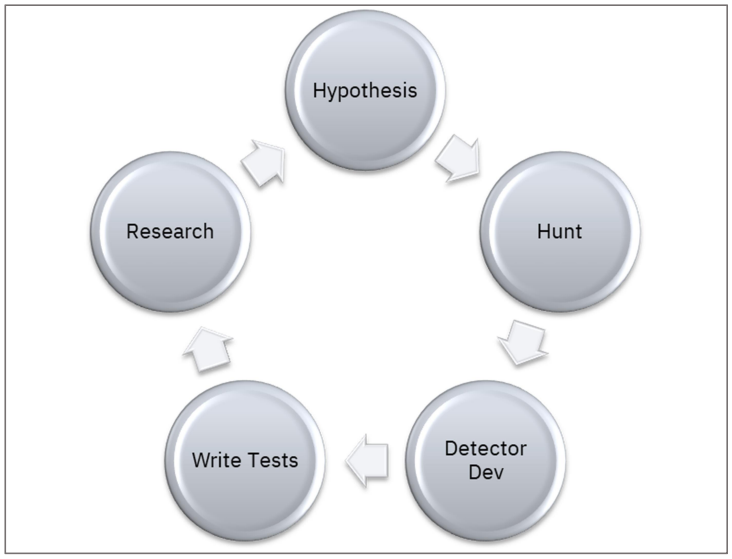


Figure 16: Google Hunt Once Process

5.4.1.1 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.

5.4.1.2 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[28]. 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[29] here:

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

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

[29] https://github.com/palantir/alerting-detection-strategy-framework

5.4.1.3 Robotic Process Automation (RPA)

For organizations that have the technical capabilities to design custom solutions for automated threat hunting, the Robotic Process Automation[30][31] (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.

5.5 Continuous Improvement

5.5.1 Goals and Objectives

Every threat hunt program, in fact every hunter, must have a goal in order to succeed. A goal is the desired result that a program or hunter plans to accomplish. Goals should be specific, realistic, and attainable and usually have a deadline. Goals can either be short term or long term and can be any of these types:

Long-term goals:
Big picture goals that often stretch over a significant amount of time and require accomplishing short term goals to complete.
Example: Make the threat hunting program a leader within the security organization

Short-term goals:
How long-term goals are broken down into manageable pieces. Short-term goals tend to be easily measured and associated with a specific time period.
Example: Increase awareness of the value threat hunting will bring to the organization

Performance-based goals:
Performance-based goals are associated with specific tasks or objectives that are easy to measure or evaluate. Performance-based goals are often associated with a specific time period.
Example: Migrate 100 threat hunts to automated detections by the end of Q1.

Quantitative goals:
Quantitative goals are directly associated on hard data such as percentages, numbers, or statistics.
Example: Reduce SOC false positive triage efforts by 25% by redesigning existing automated detections through threat hunting process.

Qualitative goals:
Qualitative goals are ones that are felt more than measured. The achievement of qualitative goals are not based on hard data but on the impact on the satisfaction and worth of the person or program.
Example: Improve relations between SOC and threat hunting team.

---

[30] https://en.wikipedia.org/wiki/Robotic_process_automation

[31] https://www.techtarget.com/searchcio/definition/RPA

Outcome-oriented goals:
Outcome goals are centered on the end-results specifically stating what the goal is designed achieve. Outcome goals do not detail how the end-result will be achieved but rather states clearly what is to be achieved.
Example: Establish and implement a threat hunting process

Process-oriented goals:
Process goals are detailed plans of action and track the progress of steps taken to advance. Process goals are about the way the threat hunt team does things, not about the results.

5.5.1.1 GOST Framework

The Harvard Business Review's Robert Kaplan 95% of employees are unaware of or do not understand their company's strategy[32] indicating that there is clear disconnect between a company's overarching strategic management plan and the people who are meant to execute it. The GOST framework stands for Goals Objectives Strategy and Tactics and provides a way to bring visibility and clarity to what an organization is trying to do and how they are going to do it.
On a smaller scale, threat hunters should be aware of the overall strategy of the threat hunting organization. When threat hunt teams do not understand what the team is trying to accomplish, why it is important, and what is expected of them it can result in confusion, decreased morale, and a lack confidence in leadership.

Breaking down the GOST framework, you can see that there is a clear distinction between the components of the framework in terms of what the team is trying to accomplish and how they are meant to accomplish it.

Goals are what you want to achieve broadly, and they are qualitative. Objectives are quantitative measurements or numeric targets that describe the specific outcomes that define your goal such as marketing penetration, profit, and revenue. Strategy is the high-level plan you will follow to achieve your goals and tactics are specific actions you will take to achieve your goals.

Figure 17: GOST Framework[33]

[32] https://pubmed.ncbi.nlm.nih.gov/16250626/

[33] https://ebrary.net/116529/management/gost_framework

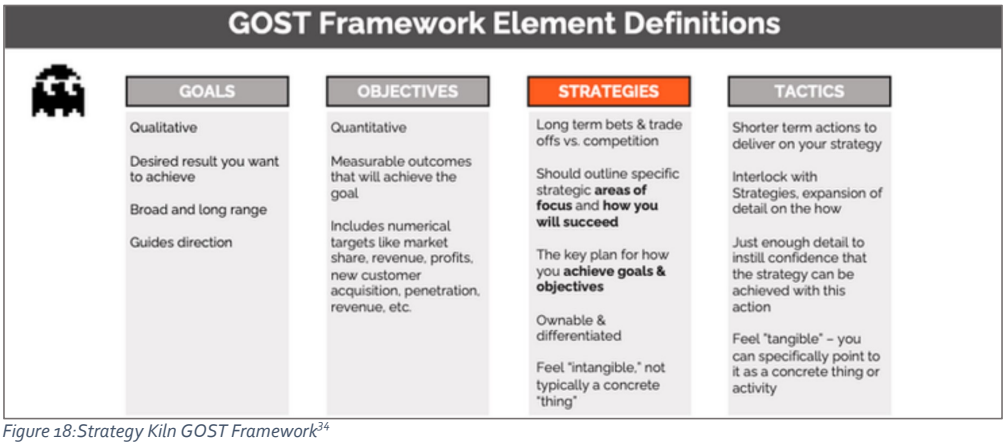


Figure 18:Strategy Kiln GOST Framework[34]

Example GOST for Threat Hunting

Goal:

- To be the driving force in high quality automated detections for indicators of attack (IoA) and tactics, techniques, and procedures (TTPs) of an attacker.

Objectives:

- Increase endpoint visibility by deploying a EDR solution to 75% of the entire workstation and server fleet over the next 12 months.
- Identify the top 5 threats to the organization and map those threats to data sources and centralize 100% of those data sources within 6 months.
- Average migration of 1 threat hunt to an automated detection per week over the next year.

Strategy:

- Focus efforts on identifying and developing threat hunts that are relevant to the organization and good candidates for automation.

Tactics:

- Establish and nurture a relationship with the SOC to build a threat hunt to automated detection pipeline.
- Develop and implement a process to migrate a threat hunt to an automated detection to be managed by the SOC
- Develop and implement a threat hunting process that has includes quality control and documentation standards

5.5.2 Continuous Improvement

Continuous improvement is any strategy, framework, or process that organizations implement to provide sustained and structured efforts towards improving business functions. Threat hunt teams that implement a continuous improvement strategy and actively seek improvement opportunities will have a much better chance at generating value over time for both the organization and for hunters. Value comes in the form of improved analysis capabilities, data quality, metrics, and reduced risk due to threats.

[34] https://www.strategykiln.com/post/gost-busters-goals-objectives-strategies-and-tactics-explained-with-an-amazon-example

Kaizen, a continuous and never-ending quest for improvements is essential for Threat Hunting program. Threat Hunt program cannot exist in vacuum. First and foremost, hunting is an essential component of security program continuous improvement. This section, however, aims to focus on improving the efficiency, effectiveness, and quality of each component of hunting process.

5.5.2.1 Continual Improvement Model

The lessons learned activity must be carried out after each hunt. Lessons learned feedback and documentation should ensure that the team retrospectively reviews and analyzes all process areas of threat hunting. The analysis should provide the details: if objectives of threat hunt were met such as quality of threat intelligence data, workflow applicability, organizational environment, the data reliability gaps, if the team was adequately staffed with skilled resources, and if the time allocated was adequate.

The purpose of continual improvement is to ensure the service, offering, or product remains aligned to the organization's goals. As it applies to threat hunting, this requires visibility into the operation in entirety, as the overall improvement of the operations is the result of improvement realized at all levels. This includes people, processes, and technology all are expected to perform at the requisite level to facilitate value.[35]

One of the more important aspects of a successful threat hunting operation is the ability to effectively demonstrate the value threat hunting brings to the organization. The Continual Improvement Model (CIM) is a highly effective way for threat hunt teams to implement a culture of improvement and establish a pipeline of data points that can be expressed to senior management to show how threat hunting is improving and bringing value to the organization.

QPR International describes implementation recommendations for the ITIL Continuous Improvement Model through the following steps[36]:
What is the vision?

- The improvement should always support the organization's goals and objectives.
- It should also link individual actions to the future vision, in order that it really can be seen as an improvement.

[35] https://www.knowledgehut.com/tutorials/itil4-tutorial/itil-continual-improvement-model
[36] https://www.qrpinternational.be/blog/it-governance-and-service-management/itil-4-continual-improvement/#:~:text=The%20ITIL%204%20continual%20improvement,Service%20Value%20System%20(SVS).

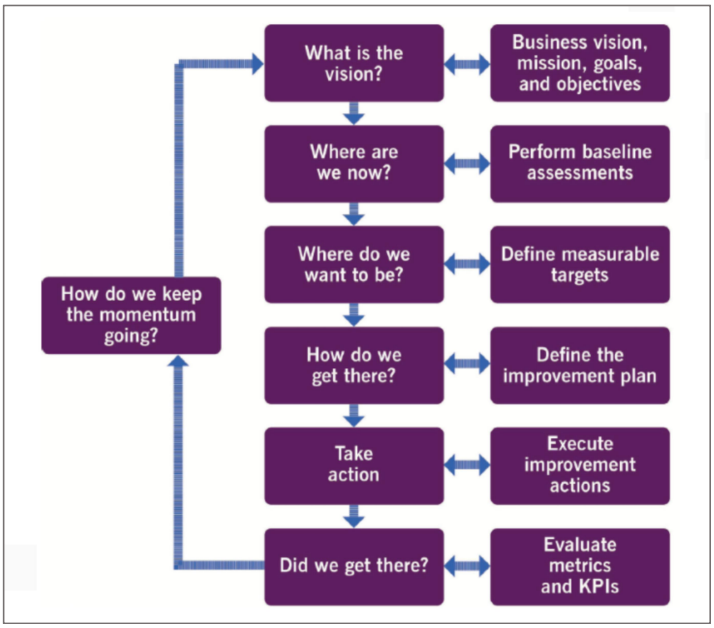


Figure 19: ITIL Continuous Improvement Model

Where are we now?

- For an improvement to really impact, it should have a clear starting point. The step 'where are we now' helps you to assess your current situation, from a technical, human resource and user's perception perspective.

Where do we want to be?

- This step helps you visualize your improvement initiative.
- Here you set your Key Performance Indicators (KPI's) and the objectives of the improvement initiative.

How do we get there?

- The fourth step helps you plan. The continual improvement model advises to work iteratively, however with some initiatives this might not be needed, and another approach will suffice.

Take action!

- Execute the plan that you created in the fourth step. A measurement process is key in this step as it will help you stay on track. To execute the plan, you can use any type of approach that you think fits best (waterfall, big bang or small iterations).

Did we get there?

- Check and confirm the progress and the value of the improvement initiative.
- If the desired result has not been achieved, additional actions need to be taken (often in a new iteration).

How do we keep the momentum going?

- If the initiative is a success, use it to build support and momentum for the next improvement initiatives.
- To do so, share the success both internally and externally. If the initiative failed to achieve success, make sure to use it for your 'lessons learned'. This way the initiative did create value, even though it was not a success.

5.5.3 Maturity Models and OTHF Maturity Assessment Criteria

The Open Group information security management maturity model (O-ISM3) describes a maturity as the measurement of an organization's ability implement continuous improvement practices within a particular discipline. With a focus on continuous improvement, maturity models are well suited for assessing threat hunting operations.

Why maturity models are important for threat hunt teams:

- Benchmarking – Determine where the threat hunt team is in terms of current state and compare against goals and objectives for performance improvement.
- Performance Improvement – With a model a threat hunt team can directly track their operations against the best practices defined by the model. Maturity models can help organizations identify gaps which a plan that addresses specific issues.
- Unified improvement language – Implementing a maturity model ensures that the entire threat hunting organization is aligned on future goals and using the same language to discuss capabilities that would enable the organization to increase their maturity with respect to the model.

The SQRRL "A Framework for Cyber Threat Hunting"[37] white paper is one of the most important papers released to the world of threat hunting and serves as a foundational part of the OTHF. Within SQRRL's works, they introduce the concept of threat hunting specific maturity model and a set of criteria in which a threat hunting program can be evaluated against.

Through the introduction of a maturity model, SQRRL created a way for threat hunt teams to build short-, medium-, and long-term goals through some high-level characteristics associated with the varying levels of maturity. Depending on the organization, they may want to have more specific requirements and assessment criteria laid out within the model and so the OTHF has created a maturity model that organizations can use to assess their maturity against.

Following table outlines the OTHF assessment criteria for each process area in scope:

[37] https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf

	LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL4
PEOPLE	- A threat hunting role does not exist or is informal - A skills catalog does not exist. No hunter training program is available	A threat hunting team exists but role description and expectations are informal documented and communicated. - A rudimentary skills catalog exists, with no defined criteria, requirements, or a plan. No hunter training program is available.	A threat hunting team exists with dedicated roles and expectations are formally documented and communicated. - A functional skills catalog exists, with defined criteria, requirements, or a plan. However, the skillset is assessed by the TH program leadership on an ad hoc basis. There is no formalized plan for addressing gaps. No hunter training program a	- A effective skills catalog exists, with defined criteria, requirements, or a plan. However, skillset is assessed by the TH program leadership on a ad hoc basis. Criteria and requirements are defined, and a formalized mentoring program is in place for bridging the skills gaps - A formalized training program is established for all levels of hunters. - A formal recruiting plan is in place.	- A robust skills catalogue exists, with a defined criteria, requirements, or a plan. However skillset is assessed by the TH program leadership as well as through self-assessment on a regular basis. Criteria and requirements are well defined, and a formalized mentoring program is in place for bridging the skills gaps. -A cross training program is in place for inter-departmental training - A formal recruiting plan is in place.

PROCESS	- A hunting framework does not exist or is in its infancy - Threat hunting does not exist	- A hunting framework is informally documented - Threat hunting is mainly a reactive service when incident response activity arises - The process area covers less than 50% of the organization	- A hunting framework is formalized and documented - Threat hunting is proactively continued regardless of incident response activities - No automated detection framework in place. - The process area covers 50% to 75% of the organization	- A formalized hunting framework is regularly executed. Outcomes are consistently discussed with impacted stakeholders. - A Threat Hunting mission statement has not been defined. - Hunts are constantly documented and reviewed with the ability to be turned into automated detection - The process area covers 75% to 90% of the organization	- The threat hunting frameworks is regularly reviewed and validated for efficiency. - A clear Threat Hunting mission statement has been defined and understood by the team. - Stakeholder feedback validates that the hunt outcome meets or exceeds expectations. - Newly developed are shared with the threat hunting community. - Hunts are constantly documented and reviewed and turned into automated detection - The process area covers 90% to 100% of the organization

DATA SOURCE	- Visibility on data sources is unknown - Quality of data sources is unknown - No tools or processes to passively collect data	- Visibility on data sources is partially understood - Data sources are informally documented - Tools are present to passively collect data - The data sources covers less than 50% of the organization	- Visibility and quality of data sources are informally measured - Available hunting data sources are formally documented - Collection tools are part of the threat hunt program too actively collect data - The data sources covers 50% to 75% of the organization	- Visibility and quality on data sources is formally measured and in place - Data collection is executed consistently - Hunting techniques include data science - The data sources covers 75% to 90% of the organization including critical assets	- A standard exists for enterprise wide logging and documentation - Standardization of hunting data sources is fully automated - Hunt operations include data science techniques - The data sources cover 90% to 100% of the organization across network and endpoint.
THREAT INTEL	- Threat intelligence is not a function within the organization or is still in its infancy - Threat intelligence is never or rarely collected - No CTI technology - No technology integration or Data is raw and unformatted.	- Threat intelligence sharing is reported on an ad hoc basis. Expectations are informal documented and communicated. - Threat intelligence scope is global and org specific - Threat Intelligence platform exists with updated feeds - Technology Integration: SIEM, Firewall/Proxy, or IDS/IPS	- Threat intelligence sharing is a separate function within the organization and expectations are formally documented and communicated. -Threat intelligence scope is global, org specific, and industry specific. -Teams take external and internal data input to shift from a reactive to a proactive posture. - Threat intelligence platform exists alongside an IOC tool	- Threat intelligence sharing is a separate function within the organization and expectations are formally documented and communicated. - Region-specific, global, industry-specific, org specific - Contributors and members of organizations such as Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) - Automation of some	- Threat Intelligence is a key function that allows the business to make operationally and strategically aligned decisions. - Create tactical an strategic TI - Team has the capability to build custom applications and processes - Majority of TI is automated - Advanced analytics and orchestration capabilities - Region-specific, global, industry-specific, org specific

			- Technology Integration: TIP, SIEM, Firewall/Proxy, or IDS/IPS is being integrated within threat intel	threat intelligence analysis tasks - Technology Integration: TIP, SIEM, defensive tools, incident response system, and all security data is being integrated within threat intel - Supports IR engagements based on knowledge of the adversaries involved	- Contributors and members of organizations such as Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) - A sophisticated threat intelligence platform exists that allows the team to build out a SOAPA
METRICS	- Few or no metrics are identified, tracked, or reported	- Key metrics are reported on an ad hoc basis - Key metrics are identified and measurement elements are accurate	- Performance targets such as operational metrics and key performance indicators is accurate and communicated to management	- Metrics are formally tracked and reviewed. Output is communicated and reported to management on a regular schedule. - Improvements are discussed but not a critical priority	- Improvements are prioritized for areas where performance is not meeting target goals. - Operational metrics are updated in real-time via automation - Hunt outcomes included in risk assessments

6 Metrics

6.1 Defining Success

6.2 Measuring Success

6.3 Defining Metrics

6.4 Publication

7 Appendix

7.1 Example Threat Hunting Program Proposal

Comment [SSK2]: Add

TBD

7.2 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.

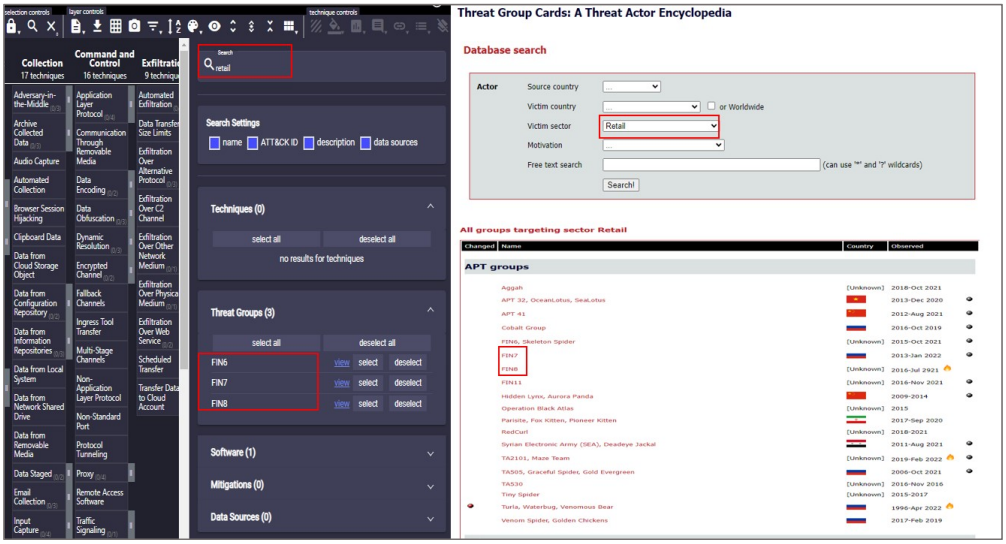


Figure 20: Example Threat Assessment - MITRE Navigator for Retail Sector

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.

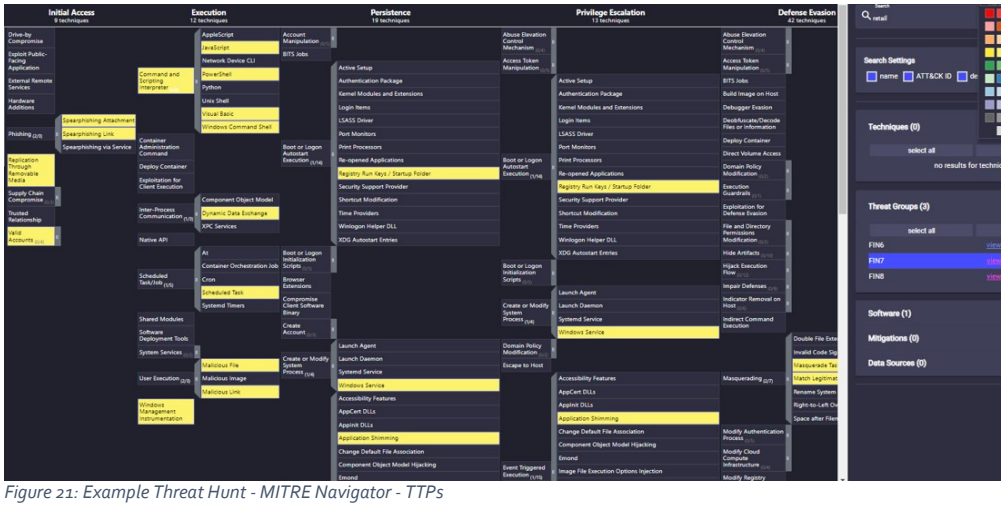


Figure 21: Example Threat Hunt - MITRE Navigator - TTPs

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.

Figure 22: Example Threat Assessment - assessing likelihood

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.

7.3 Example Threat Hunt Goal

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.

7.4 Example Threat Hunt

Remote Transfers using BITSAdmin

In Context of APT10

7.4.1 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

7.4.2 Goal

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

7.4.3 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.

7.4.4 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.

7.4.5 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
```

7.4.6 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 oxo.

7.4.7 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.

7.4.8 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.

7.4.9 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/