

# A Deep Drive on Proactive Threat Hunting

March 17, 2020 By Raj Chandel

We all know that the proactive threat hunting is need of the hour and as we have already discussed the basic requirement that highlights all generic step required for Threat Hunting Activity in our previous article “[Threat Hunting – A proactive Method to Identify Hidden Threat](#)”.

In this post, you will learn what are the main factors that should be considered before conducting a threat hunting activity in any organisation. These key factors will help an organisation to prepare a roadmap of the hunting activity before execution.

## Table of Content

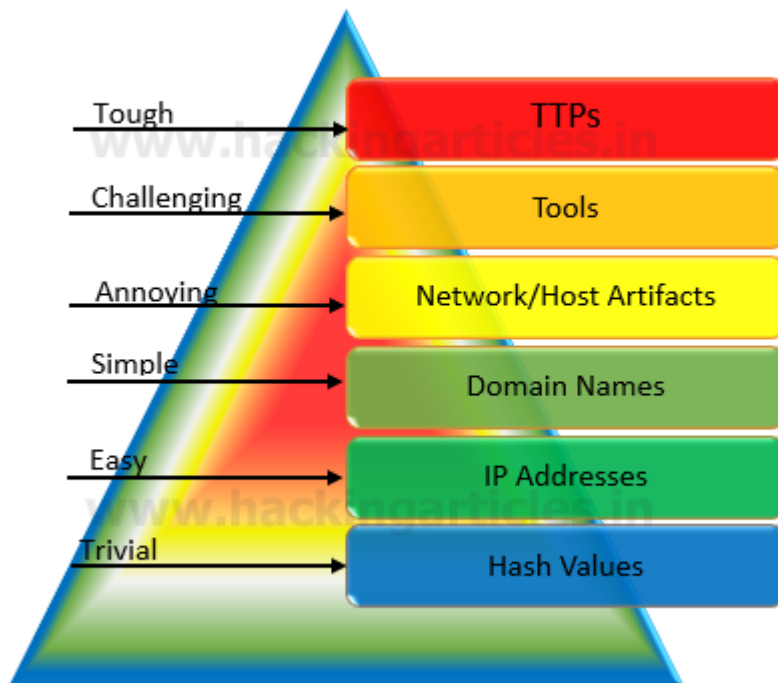
- The pyramid of Pain
- Threat Hunting Techniques
- Datasets
- Hunting Maturity Model (HMM)

## The Pyramid of Pain

The Pyramid of Pain, first proposed by security professional David J Bianco in 2013, concentrating on incident response and threat hunting in order to improve the applicability of attack indicators.

- The Pyramid measures potential usefulness of your Intel
- It also measures the difficulty of obtaining that Intel
- The higher you are, the more resources your adversaries have to expend.

**For example:** If an attacker is using malware to exploit an endpoint within their attack chain and as a defender, the security professional is using file hash values to distinguish such actions, it is trivial for them to recompile the malware illustration such that the file hash value the team are using to detect the original sample, is rendered useless.



**Hash Values:** Identifying Indicator of compromise with the help of the corresponded hash values is a most trivial step. Unfortunately, they are extremely susceptible to change (even accidentally).

**IP Addresses:** An IPv4 or IPv6 address, in most cases netblocks or CIDR ranges also fit here.

An only foolish person uses their own addresses. VPNs, Tor, open proxies all make it easy to change the IP address.

If it's hardcoded into a config, maybe adversaries have to do a little work to update it. We have found that attackers have begun to manipulate or confuse targets with malicious IP in DWORD format. The definition of a malicious URL is as follows:

*"http:// 77683606/GoogleSearch.image"*

### **IP to DWORD format**

- 1) This can be done by separating the original IP into four octets. Let's take the above IP address, which is "74.21.11.150". Split the IP address into four octets – 74, 21, 11 and 150.
- 2) Convert each octet into HEX and you will get "4a15b96" for all four octets.
- 3) Further, change HEX "4a15b96" into decimal and ultimately you will get "77683606" which is the DWORD form of the IP address.

**Domain Names:** This could be either a domain name itself (e.g., "freeinternet.net") or maybe even a sub- or sub-sub-domain (e.g., "the.new.game.freeinternet.net").

The attackers use the fast-flux or double flux to mask and safeguard their actual infrastructure. They compromised a range of easy targets like vulnerable computers or weak home routers. These routers are then used as tunnels for carrying command-control messages and data across the actual network

As per a report “**APT1: Exposing One of China’s Cyber Espionage Units | Mandiant | FireEye**” you can read how an attacker plan to get a domain registered for APT1.

*1) The first persona, “UglyGorilla”, has been active in computer network operations since October 2004. His activities include registering domains attributed to APT1 and authoring malware used in APT1 campaigns.*

*“UglyGorilla” publicly expressed his interest in China’s “cyber troops” in January 2004.*

*2) The second persona, an actor we call “DOTA”, has registered dozens of email accounts used to conduct social engineering and spear-phishing attacks in support of APT1 campaigns. “DOTA” used a Shanghai phone number while registering these accounts.*

*3) We have observed both the “UglyGorilla” persona and the “DOTA” persona using the same shared infrastructure, including FQDNs and IP ranges that we have attributed to APT1*

**Network/Host Artifacts:** It is very difficult for an adversary to conduct any useful operation without leaving any traces, which ensures that any byte flowing through the network as a result of an adversary’s involvement may be an artefact.

For example, Classify the outbound traffic with a C&C server that will be viewed as network artifacts, while on hosts, search for files & folders, registry objects, mutexes, memory strings will be considered as host artifacts.

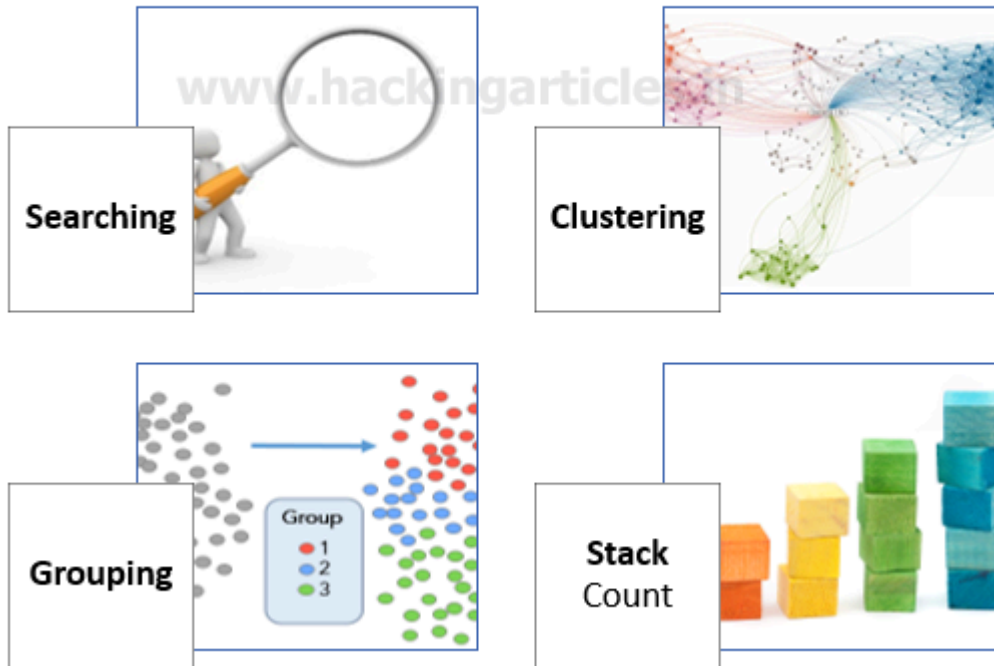
**Tools:** In this step, the hunter tries to investigate “what kind of program or command might be used by intruders to achieve their target” such as PowerShell, mimikatz, or other restriction circumvent commands for a lateral moment.

**Tactics, Techniques and Procedures (TTPs):** In this phase, the hunter attempts to examine “how the intruder achieves its target with the aid of the cyber-kill-chain” (as discussed in Part-I). They choose social engineering to target such as phishing, which is the most common TTP used to trap the user in order to gain a foothold in the network by linking a malicious object to the mail.

## **Threat Hunting Techniques**

Skilled threat hunters use a variety of techniques when reviewing data sources such as firewall logs, SIEM and IDS warnings, DNS logs, file and network data, authentication systems, and other sources in order to detect IoCs and recognize the threat.

## Threat Hunting Techniques



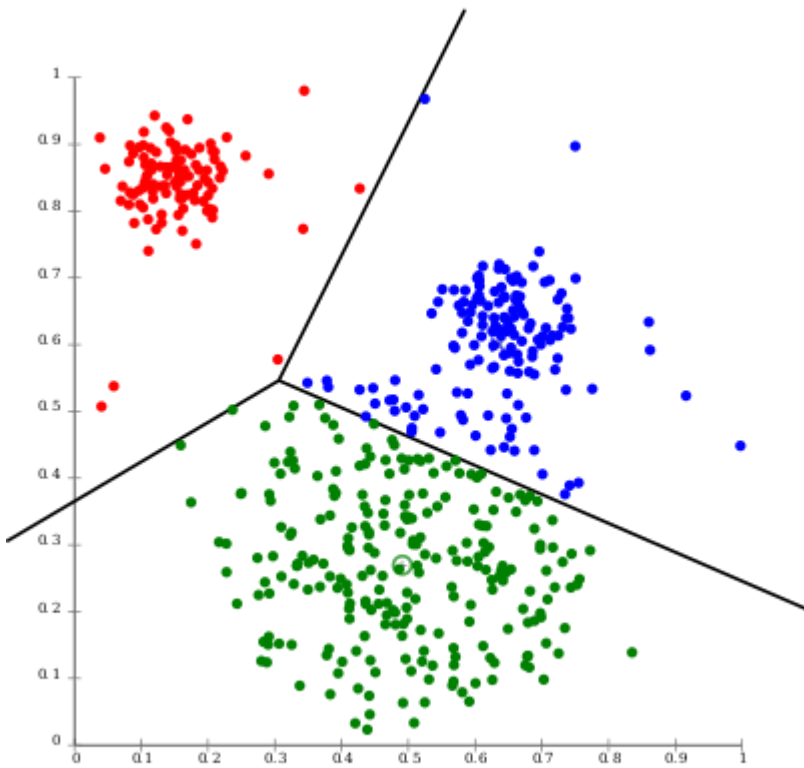
### **SEARCHING**

This is the simplest and least difficult technique used in threat hunting. It is the process for querying data for specific artifacts using defined search criteria and tools. It involves environmental data to analyze like logs, alerts, memory dumps, system events etc. As a security professional who involves in threat hunt need to analyze more data so in starting of threat searching, it's not possible to know exactly what you are looking for. So, there are two important factors need to keep in mind while doing a search:

- Too wide hunting for common artifacts that can produce unnecessarily various results of very little use.
- Focusing too specifically will lead to very few findings and prevent it from being concluded.

### **CLUSTERING**

Clustering is an analytical process, typically performed using machine learning, involving the classification of related classes (or clusters) of data points based on certain behaviors from a wider range of data. In actual fact, the technique is popular in various fields such as machine learning, pattern recognition, retrieval of information, data compression and computer graphics, for statistical data analytics.



source: [https://en.wikipedia.org/wiki/Cluster\\_analysis](https://en.wikipedia.org/wiki/Cluster_analysis)

A statistical technique in which groups of like data points established on specific aspects of a large data set are separated into groups. This is most effective when acting upon a broad group of data points that do not share behavioral characteristics. Clustering finds precise cumulative behaviors, like an unusual number of instances of a common occurrence through various applications such as outlier detection.

Read more from here: [https://en.wikipedia.org/wiki/Cluster\\_analysis](https://en.wikipedia.org/wiki/Cluster_analysis)

## **GROUPING**

The grouping includes taking a variety of different objects and determining when multiple objects come together based on common criteria. This consists of identifying common criteria that are used to group objects, such as incidents that occur within a given time period. It is best used when hunting for other artifacts which are equally or unusual.

The grouping is different from clustering as it is performed after clustering by looking at unusual data sets and of the researcher's concern in order to see the root cause whereas clustering uses enormous quantities of data to classify data sets which require more analysis using the grouping technique.

## **STACKING**

The stack counting is an analysis method used in a simulated haystack to find the needle. It is the most popular practice conducted by hunters to examine a hypothesis.

“You are familiar with the term, if you ever used the pivot tables of Microsoft Office, the stats command of Splunk or the “top” command of Arcsight”.

Data stacking is used to isolate and classify patterns by using frequency analyses in mass quantities of related data. It requires an algorithmic method of reducing vast volumes of data that can be processed and analyzed into manageable chunks.

In the context of a large data set, the investigator identifies the characteristics that differentiate the odd data rows and may prove that they are malicious. Instead, these attributes are the grouping parameters used to build estimates for the frequency analysis.

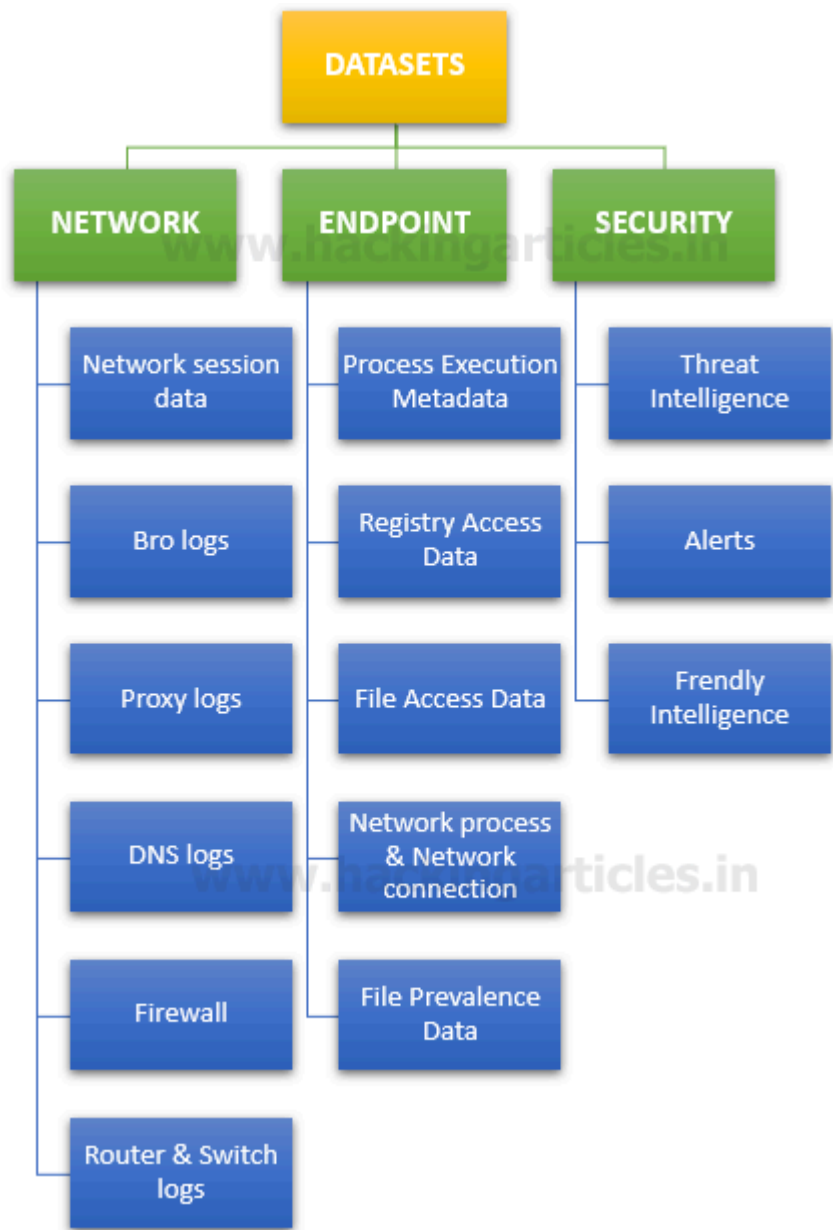
*For example: To identify a thread count with the help of Process Explorer.*

The screenshot displays the 'chrome.exe:5220 Properties' dialog box in Windows. The 'Threads' tab is selected, showing a list of threads. Thread 6540 is highlighted, with a CPU usage of 0.01 and Cycles Delta of 15,18,499. A red arrow points from this thread to the 'Stack for thread 6540' window. The 'Stack' window shows the following stack frames:

| Index | Module Name        | Offset                      |
|-------|--------------------|-----------------------------|
| 0     | 0x0000000000000000 |                             |
| 1     | ntdll.dll          | NtWaitForSingleObject+0x14  |
| 2     | KERNELBASE.dll     | WaitForSingleObjectEx+0x93  |
| 3     | chrome.dll         | ChromeMain+0x1dcc8          |
| 4     | chrome.dll         | ChromeMain+0x10ff2          |
| 5     | chrome.dll         | ChromeMain+0x10f20          |
| 6     | chrome.dll         | ChromeMain+0x10876          |
| 7     | chrome.dll         | IsSandboxedProcess+0x2c3516 |
| 8     | chrome.dll         | ChromeMain+0x260a5          |
| 9     | chrome.dll         | ChromeMain+0xc337           |
| 10    | chrome.dll         | ChromeMain+0xbdaf           |
| 11    | chrome.dll         | ChromeMain+0x125            |
| 12    | chrome.exe         | Ordinal0+0x2c27             |
| 13    | chrome.exe         | Ordinal0+0x1947             |

## Datasets

The methods you use are all part of the strategy and experience of what you will do. If you don't have sufficient details, but what is the right details, you can't hunt? The response to that question is dependent on what you are aiming for, but the following is a broad list of datasets that are well suited for hunting and security:



## Hunting Maturity Model (HMM)

The Hunting Maturity Model is developed by Sqrrl's security architect and DavidJBianco. It measures the current maturity level of hunting of any organization based on the data collection, creates data analysis procedures, incident responses and hunting automation.

There are five levels of Hunting Maturity Model (HMM)

The increasing level of maturity is focused on how an organization has the ability to track and establish data analysis procedures (DAP) on the basis of the data it collects and its hunting automation. Analysts and managers will use the HMM to assess the current maturity and to build a roadmap.

**HM0 – INITIAL:** HM0 uses automated alerting tools, such as IDS, SIEM or antiviruses, mainly to identify malicious activities across the organization. They may provide signature update feeds or indicators of threats and even build their signatures or indicators, but these are fed directly into the monitoring system.

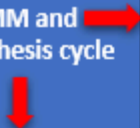




**HM1-Minimal:** An organization in HM1 still relies mainly on automatic warnings, but at least some routine IT data collection is carried out by them. They also utilize threat intelligence to drive detection.

**HM2-Procedural:** At Level 2 maturity, an organization follows analysis procedures created by others. It has a high or very high level of routine data collection. They may periodically practice and adapt procedures developed by others and can make minor improvements but are not yet able to establish entirely new guidelines themselves.

**HM3-Innovative:** At least a few hunters are present in HM3 organizations who understand different forms of data analysis techniques and are able to use these approaches to detect malicious activities. Such organizations are typically those which establish and publish procedures rather than depend upon procedures established by other parties (as in the HM2 case).

**HM4-Leading:** HM4 is exactly the same as HM3, with a significant difference: automation. Every effective hunting process at HM4 will be introduced and translated into automatic detection. This liberates analysts from the pressure of continued implementation of the same processes and encourages them than to focus on developing current or new processes.



| Relation between HMM and Hypothesis cycle<br>     | HM0 – INITIAL  | HM1-Minimal  | HM2- Procedural  | HM3-Innovative   | HM4-Leading   |
|--|--|--|--|--|---|
| <b>Data-Collection</b><br>                        | Little or no data collection.                              | Moderate collection some types of data from a key point of infrastructure.                       | High collection of a specific types of data throughout IT environment.                           | High collection of a specific types of data throughout IT environment.   | High collection of many types of data throughout IT environment.  |
| <b>Hypothesis-Creation</b><br>                    | Respond to automatic alert from SIEM, IDS, Firewall, etc.  | Review threat intel to create a new hypothesis.  | Review threat intelligence & friendly intelligence to create a new hypothesis.                   | Review threat intelligence & friendly intelligence and manual cyber risk scoring (i.e. <b>crown jewel analysis</b> ) to create a new hypothesis. | Review threat intelligence & friendly intelligence and automated cyber risk scoring to create a new hypothesis. |
| <b>Tools &amp; Techniques for Hypothesis</b><br> | Alert Consoles, SIEM searches, no proactive investigation. | Utilized SIEM or log analysis tools to conduct basic search via full text or SQL - like queries. | Use simple tools and histogram to search and analysis data based on existing hunting procedures. | Leverage virtualization and graph search. Build new hunting procedure.   | Advance virtualization and graph search. Published and automate new hunting procedure.                          |
| <b>Pattern &amp; TTP Detection</b><br>          | None   | Integrate threat intel feed into automated alerting for basic match.                             | Build a library of effective hunting procedures and perform them on a regular schedule.          | Build a library of effective hunting procedures and perform them frequently, data science (Machine learning).                                    | Automated effective hunting procedure to continuously improve alerting capabilities & advance data science.     |

**Keywords:** Crown jewels analysis: Crown Jewels Analysis (CJA) is a process for identifying those cyber assets that are most critical to the accomplishment of an organization’s mission.

Reference:

<https://www.threathunting.net/files/hunt-evil-practical-guide-threat-hunting.pdf>

<https://www.threathunting.net/files/huntpedia.pdf>