Threat Hunting – A proactive Method to Identify Hidden Threat

February 23, 2020 By Raj Chandel

According to ISO 27005, a threat is defined as a potential cause of an incident that may cause harm to systems and organization. Software attacks, theft of intellectual property, identity theft, sabotage, and information extortion are examples of information security threats. As a result, most of the organization chose active threat hunting practice to defend their organization from the network's unknown threat.

Table of Content

What is threat hunting?

Threat hunting is a proactive offense approach that security professionals use with the aid of Intel Threat. It consists of iteratively scanning through networks to detect compromise indicators (IoCs) and threats such as Advanced Persistent Threats (APTs) which bypass your existing security framework.

Analysts monitor, detect and delete active opponents in a network. They do this as early as possible in order to minimize damage and to reduce the time needed to identify a suspected threat.

Threat hunting tools and techniques are used by researchers to monitor and detect hidden activities. An example of a threat hunting Framework is, implemented N-SOC as part of a next-generation SIEM framework.

The SANS Institute authors expand on the cyber threat hunting process, calling it an active defense strategy consisting of:

Intelligence: The process of collecting data, turning the data into usable information, analyzing the potentially competing sources of that information to produce a tactical defense strategy.

Offense: The countermeasures organizations may take to defend against cyberattacks, in particular Advanced Persistent Threats (APT).

Why threat hunting is Important?

Threat hunting's main purpose is to reduce the time needed to find signs of threats who have already breached the IT infrastructure. Since zero-day and Advanced Persistent Threats (APT) continue to challenge security staff, researchers are implementing threat analysis tools and approach to discover threats more efficiently. Through discovering these imprints as soon as possible, the risk of breaches can be reduced on the enterprise.

Other benefits of threat hunting include:

- Identification of gaps in visibility necessary to detect and respond to a specific attacker TTP.
- Classification of gaps in finding.
- Advancement of new monitoring use cases and detection analytics.
- Exposing new threats and TTPs that response to the threat intelligence process.
- Recommendations for new preventive measures.

Who is threat hunter?

A threat hunter is a security professional who is skilled to recognize, isolate and defuse APTs by using manual or AI-based techniques because such threats can not be detected by network monitoring tools. He may hunt for insider provocations or outside intruders to uncover risks posed by malicious actor typically employees, or outsiders, including a criminal organization.

Threat hunting activity is mainly related to the NSOC, which represents the Next-Generation Security Operations Center because the threat hunter reports to the threat hunting team manager for hidden threats, who reports to the Chief Information Security Officer (CISO) and is further reported to the SOC manager for integration with the Security Operations Center (SOC)

What Are the IOCs?

Threat Intelligence feeds can aid in this phase by defining specific vulnerability identifying common **indicators of Compromise** (IOCs) and suggesting measures necessary to prevent threat or breach.

Some of the most common indicators of compromise include:

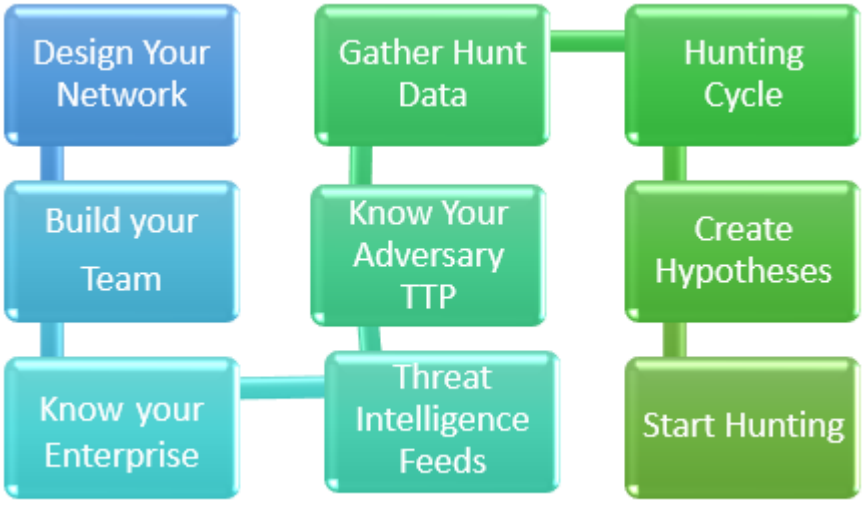
- A case would be when the intrusion that attacks an organizational host that established a connection with attackers such as IP addresses, URLs and Domain names
- An example will be a phishing campaign based on an unwilling user clicking on a connection or attachment and a harmful instruction being activated such as Email addresses, email subject, links and attachments.
- An instance would be an attempt by an external host that has already been detected for malicious behaviours such as Registry keys, filenames and file hashes and DLLs.

Threat Hunting Plan

The cyber threat hunting team should be answerable to these questions before planning for the operation.

1. *What is it that you hunt? You have to select exactly which adversaries you're chasing for.*
    - Exploitation?
    - Lateral movement?
    - Exfiltration?
2. *Where are you going to find the opponent/adversaries/IOC?*
3. *How would you consider an opponent/adversaries/IOC?*
4. *When will you find it?*

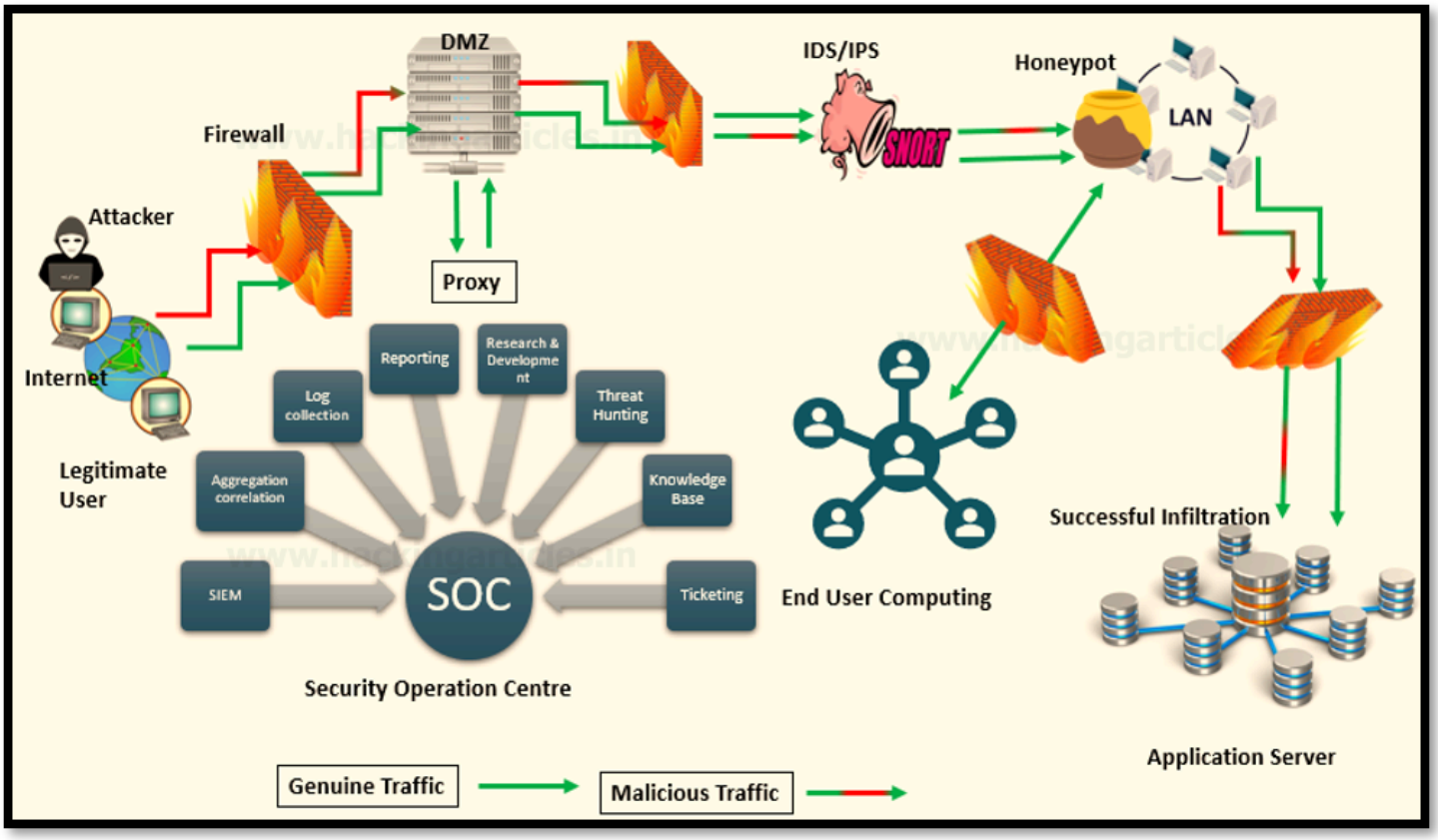
The Chief Information Security Officer (CISO) should prepare a complete checklist that would be required for effective threat hunting before beginning the threat hunting operation within the company. This helps the team define the resources and tools used in the project and create a parallel strategy as the backup plan if the primary process fails.



1. Design Your Network for Hunting

It is important to consider that the proactive threat hunting should be conduct in a well secure environment where Chief information Security Office arrange all network essential equipment required in the activity, such as given below.

- Segmentation : Security Zones
- NTP : Network Time Protocol
- Protection/Detection : FW/IDS/IPS/DLP/Proxy
- Tapping : Dump PCAP Data
- Visibility : Enable Logging as required



2. Get your Team Ready

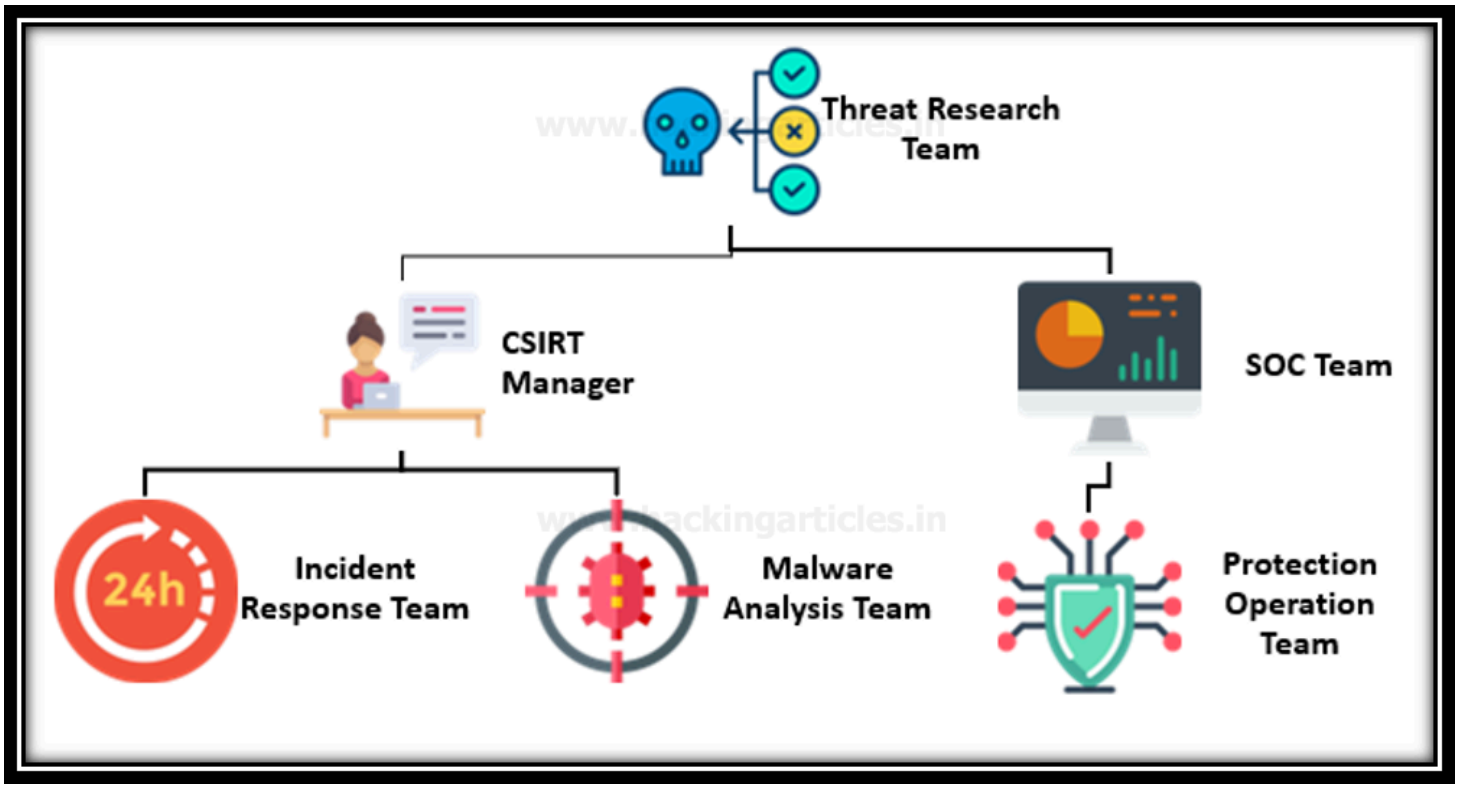
The officer should build a team of professionals that are spontaneous in doing their job as per the situation requirements and know the situational awareness.

The skill of a threat hunter:

Proactively hunts for known adversaries—He is capable to identify the pattern of malicious code used by famous attackers that match to threat intel feeds or blacklist of known program.

Prevent the attack by identifying unknown threats— Threat hunters evaluate the computer system by means of constant surveillance. They choose behavioural analysis to identify abnormalities that indicate a threat.

Implements the incident response proposal—Hunters collect as much information as possible when they identify a threat before conducting an incident response strategy to nullify it. This could be used to refine the response plan and prevent future attacks.



3. Know your Enterprise

Group members should be mindful of the organization's jewel crown by knowing the valuable assets and recognizing threat carriers that might affect the company. They should be able to calculate the effect of risk by prioritizing the unknown threat within the network.

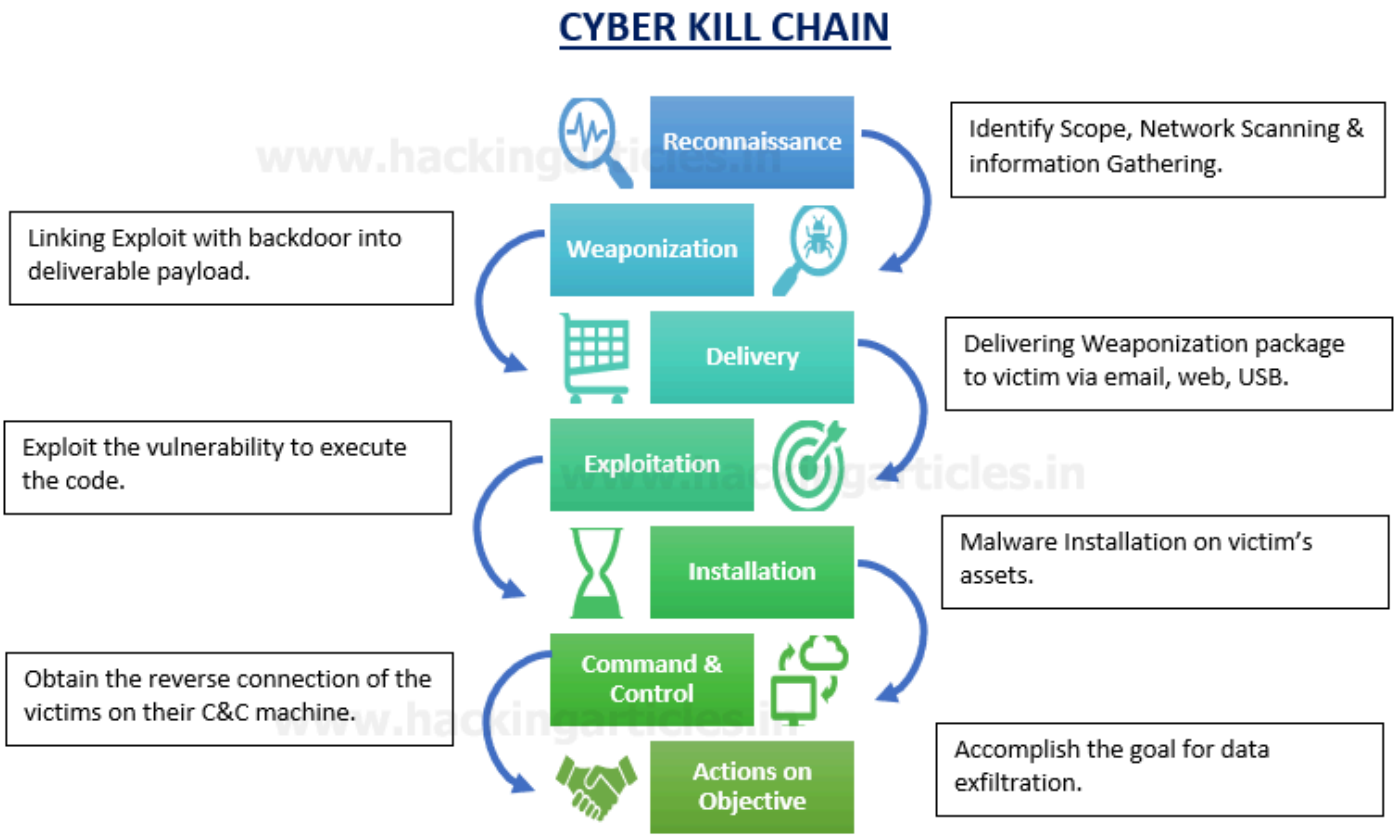
Hence, they should be able to classify the following checklist for their organization:

- Identify Assets
- Know Threats to Your Assets
- Prioritize (High Value / Critical Assets First)
- Baselining – Know what is normal ?

4. Know Your Adversary TTP

The Threat Hunters team aims to evaluate Tactics, Techniques, and Procedures (TTPs) that are learned from the indicators with the help of a process known as "**Attack Tree Analysis**" that includes defining certain measures an attacker can take to break the networks of an organization (Schneier, 1999). "The Lockheed Martin **Cyber Kill Chain**," which describes one way of determining where an adversary's actions occurred in the attack chain. Intruders also follow these steps on the Cyber Kill Chain while striving to get into a network or web server.

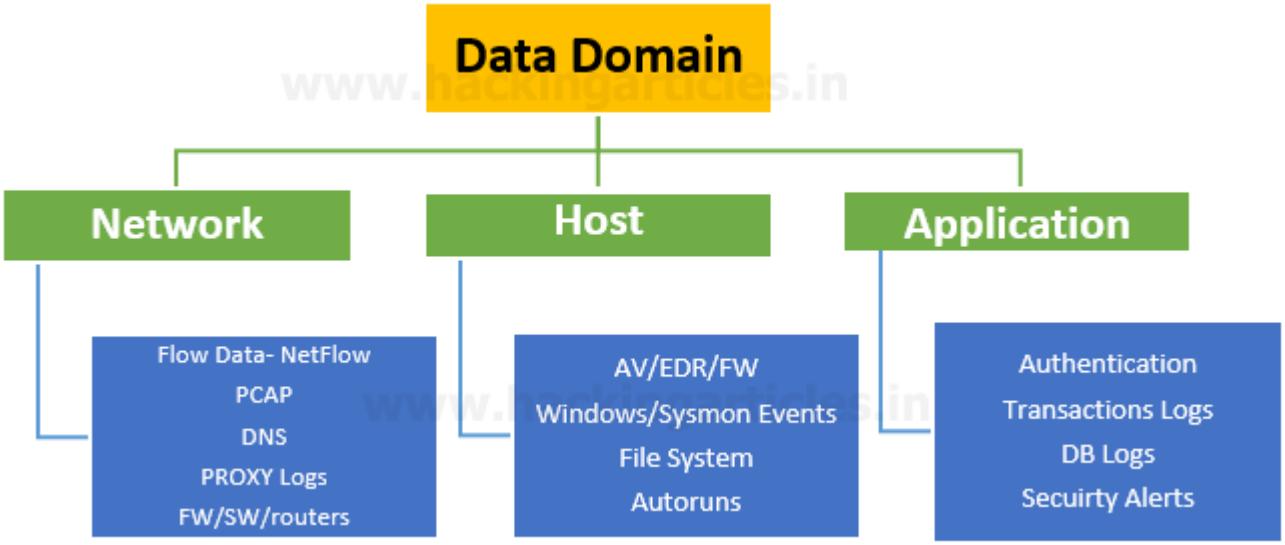
A cyber kill chain is a 'Lockheed Martin' model that uncovers the phases of a cyber-attack from early reconnaissance to the objective of data exfiltration: Flow Data NetFlow PCAP DNS Proxy Logs FW/SW/Routers.



5. Collect Hunt Data

When conducting the threat hunting task, the collection of hunting data is a very valuable phase in which one must collect the malicious data from the logs created in the network by monitoring the security equipment installed in the network in order to filter packets. Indeed, this phase is the big contribution in providing threat Intel feeds.

Through analyzing logs at each grade, the specialist may recognize the unknown threat carriers that would be active over a long period of time in the network and may constitute a threat of **zero-day.**



6. Threat Intelligence Feeds

CTI is focused on data collection and analysis to identify potential or current threats to an IT infrastructure. This helps organizations to proactively defend critical infrastructure or intellectual property of an entity from cyber-attacks by using open-source intelligence (OSINT), social media intelligence (SOCMINT), human intelligence (HUMINT), deep and dark web technological intelligence or intelligence Security teams look for Indicators of Compromise (IoCs) for persistent threats and zero-day (recently discovered) exploits.

The cyber threat intel Feeds can be categorized in two broad categories:

Free Available: Open Source, OSINT, Social Listing

Paid: Private, Government, commercial vender

The intelligence feeds are continual streams of credible information about existing or potential threats and bad actors. The researchers are collecting security data from several sources on IoCs such as abnormal behaviour and suspicious domains and IP addresses. They can then correlate the information and process it to generate reports of threat intelligence and management.

7. Create a Hypothesis

What to hunt ?	Where to hunt ?	What to considered ?
• Exfiltration • Lateral Movement • Fileless Malware • Command & Control	• PCAPS, NetFlow • PCAPS, Logs • HTTP, BRO/Snort Logs	• Compress Files • PSEXEC, Powershell • Powershell, WMI • Malicious URLs/Domains/User Agent/DNS

8. Hunting cycle

The team should follow a common framework at the time of threat hunting which defines the threat hunting cycle process. It is a closed-loop that forms a model process for effective hunting which defines four vital stages.

Hypothesis: – Cyber threat hunting is started by making informative beliefs, about the different types of adversarial effects or behaviours that exist in your business network.

Investigate via tools & technique: – Hypotheses are examined via multiple tools and techniques in Identifying the relationship between different data sets. An analyst can use these to discover new malicious patterns in their data and reconstruct complex attack paths to reveal an attacker's Tactics, Techniques, and Procedures (TTPs).

Uncover new pattern & TTP: – A hunter often uses manual methods, tool-based workflows or analytics to discover the specific patterns or anomalies that may be detected in an investigation. What you will find in this

phase is a critical part of a hunt's success criteria. Even if an anomaly or intruder is not detected, you want to be able to rule out the existence of a particular strategy or compromise. Essentially, this step acts as the step of "proving or disproving the hypothesis."

Inform Enrich & Analytic: – Lastly, effective hunts form the basis for guiding and empowering predictive analytics. Do not waste time doing the same hunts over and over with your squad. If you discover an indicator or pattern that may reoccur in your system, automate its monitoring to keep your team focused on the next new hunt. Hunting information can be used to upgrade existing monitoring systems, which could include modifying SIEM rules or signatures for analysis.

9. Measuring Success

Once the hunting operation cycle has been completed, it is important to evaluate the finding and the assign task KRA to measure the success matrix.

- Number of Incidents by severity
- Number of Compromised Hosts
- Dwell Time of Incidents Discovered.
- Logging Gaps Identified and Corrected
- Vulnerabilities Identified
- Insecure Practices Identified and Corrected
- Hunts Transitioned to Analytics
- New Visibilities Gained

Resources:

TaHiTI-Threat-Hunting-Methodology-whitepaper.pdf

D2 BSIDES – Hunting Threats in Your Enterprise

Sqrrl: A Framework for Cyber Threat Hunting