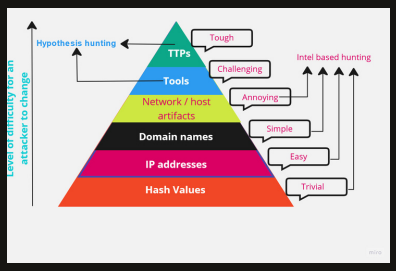
Threat hunting CheatSheet

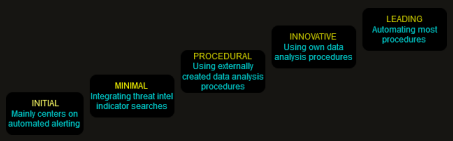
Pyramid of pain



Types of threat hunting

- Hypothesis-driven investigation
- IOC driven investigation
- Analytics and ML driven investigation

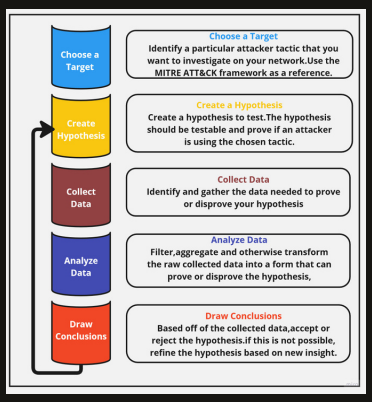
Threat hunting Maturity Model



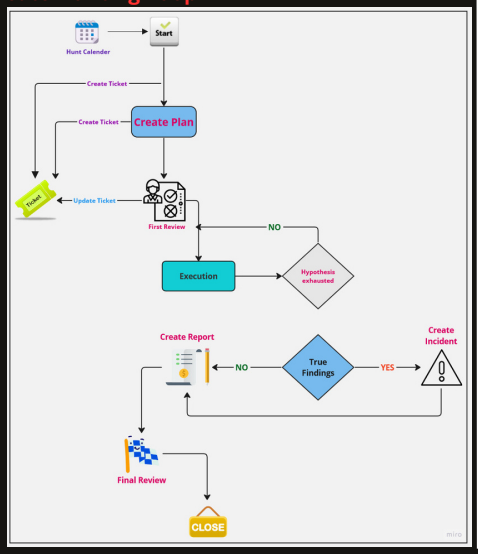
Hypothesis

- A proposed explanation for an observed behavior that may be indicative of malicious activity

How to write a Threat Hunt Plan?



Create Hunting Loop



Steps to hunt APT groups using the MITRE ATT&CK framework:

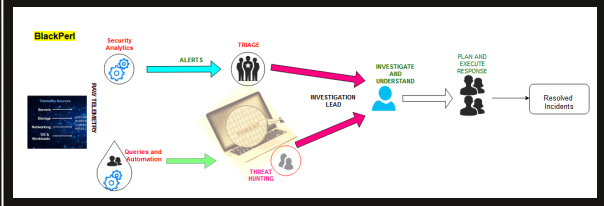
- Understand ATT&CK Framework: Study adversary techniques in the MITRE ATT&CK matrix.
- Identify Targeted APT Groups: Research relevant APT groups, considering motivations, techniques, and attack vectors.
- Analyze Public Information: Examine reports for insights into APT tactics, tools, and indicators.
- Map APT Group Tactics: Use ATT&CK framework to map frequently used tactics.
- Formulate Detection Rules: Create rules based on mapped tactics to identify indicators of malicious activity.
- Implement Threat Hunting Techniques: Use techniques like log analysis, network traffic analysis, and behavioral analytics.
- Validate Findings: Investigate and validate potential APT activity through analysis and cross-referencing.
- Mitigate and Respond: Take actions to mitigate the threat, such as isolating systems, updating controls, and sharing intelligence.
- Continuously Improve: Regularly review and update rules, techniques, and knowledge about APT groups.

WHERE DOES THREAT HUNTING FIT?

The process of threat hunting perfectly complements the standard procedures of incident detection, response, and remediation. While security technologies examine the raw data and produce alerts, threat hunting operates concurrently by employing queries and automation to uncover potential leads within the same data.

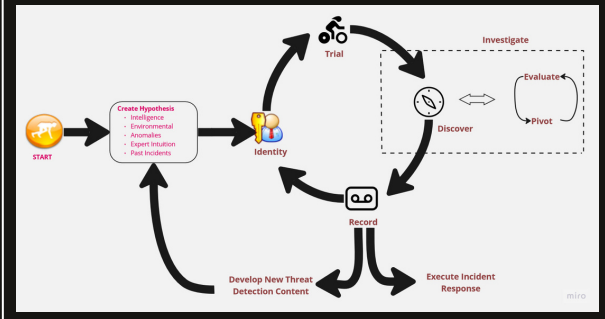
These hunting leads are subsequently scrutinized by expert human threat hunters who possess the ability to identify indicators of adversary activity. Once identified, these indicators can be managed through the existing pipeline.

The following diagram illustrates this entire process:



Threat Hunting Process

- Developing detection content
- Interpreting threat intelligence
- Assessing the impact of vulnerability exposure
- Conducting incident investigations
- Managing incident response activities



REACTIVE VS PROACTIVE

REACTIVE
Locates and corrects your system's potential vulnerabilites before they can be exploited & an attack can occur

VS

PROACTIVE
Bulks up your defenses against common attacks and defends against attacks that have already happened

Ransomware Hunt:

Detecting Ransomware Activities

- Notable Findings: A significant increase in the creation of files within a brief timeframe.
- Notable Findings: A substantial modification of file metadata within a short duration.
- Dataset: Sysmon Operational logs collected from endpoints.
- Hunting duration: 15days (Depends on Org).
- Offensive Tradecraft: Ransomware typically generates an extensive number of new files, with the existing data being encrypted. Therefore, our focus is on identifying file names that are responsible for creating a large volume of new files within a limited time period.

Security researchers have detected numerous common but discreet artifacts in numerous ransomware campaigns conducted by highly skilled intruders. These indicators primarily revolve around the utilization of system tools to make preparations for encryption, avoid detection,and eradicate forensic traces.

User friendly tools for TH

MITRE ATT&CK Navigator
HELK
EQL -Event Query Language
Security Onion
YARA
Capa

Threat Hunting techniques

Analysis: Inspect data sources, logs (e.g., DNS, firewall), network, file, and user data, review SIEM and IDS alerts for threat identification.

Searching: Define criteria, query data for anomalies.

Baselining: Establish normal threat levels, investigate deviations.

Clustering: Examine related data to isolate patterns, use ML and AI.

Grouping: Analyze suspicious data based on criteria, detect threats.

Stack Counting or Stacking: Inspect values, categorize based on characteristics, flag outliers.

Threat Hunting Tips

- Leverage programming skills
- Maximize the effectiveness of your organization's security tools.
- Use third-party tools where it makes sense.
- Write your processes and scripts down repeatability