Introduction

The ability to block sophisticated threats improves each year, but we face determined and creative adversaries whose techniques evolve just as quickly . therefore organizations need to deploy another layer of defense to proactively detect threat actors before they can actually do any damage to their environment .

What is threat hunting ?

Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network **unknown** threat that aren't detected by current automated methods of prevention and detection .

we assume that an adversary is already present in the network

Why threat hunting ?

- Threat hunting help organization reduce the **dwell time**
- Threat hunting help in identifying the threat within the organization's asset **before any damage can be done**

Threat Hunting Maturity Model-1

Threat Hunting Maturity Model can help organizations measure their current maturity and provide a roadmap for improvement. The maturity levels start from a **non-existing** (initial) stage to a **fully** matured level (leading).

Threat Hunting Maturity Model-2

Initial ***(Level 0)***	At this level the organization cover only the basics , they rely on detection (*example : SIEM*). They are not considered hunting because they don't collect much data from their environment.
Minimal ***(Level 1)***	They still rely on detection and they track the latest threat report and collect the data from their environment into central location , so one there is new threat report they can extract key indicator and search if they have been seen before in the recent past in their environment (*they don't have regular threat hunting routine*)

Threat Hunting Maturity Model-2 (cont)

Procedural ***(Level 2)***	They usually collect large amount of data , the organization at this level uses procedures available on the internet created by others (*they have regular threat hunting routine*)
Innovative ***(Level 3)***	The organization instead of relying on available procedures , they are the ones who creates the procedures (*it's aided by data visualization and machine learning*)
Leading ***(Level 4)***	They automate the majority of procedures (*instead of repeating the same process over and over again they can focus on creating new ones*)

NOTE : The Hunting Maturity Model is just a prescriptive model, the organizations does not have to fit into one level , sometimes they are at varying levels of capabilities

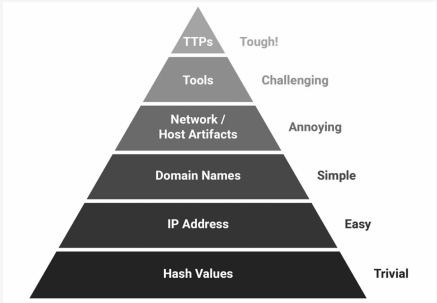
Threat Hunting Frameworks

Frameworks can be a foundation for the threat hunters when starting their hunting process.

Cyber Attack Life Cycle

The process by which sophisticated cyber attacks are conducted *(help in understand how a cyber attack happens from the perspective of an adversary)*

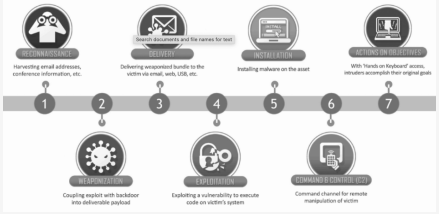
Pyramid Of Pain



The relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them *(help in Measuring the effectiveness of indicators we use in threat hunting)*

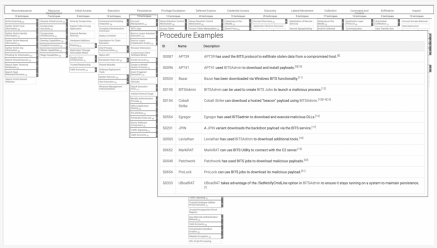
Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

Cyber kill Chain



The steps that an attacker needs to take in order achieve their objective

Mitre Attack



Knowledge base for attackers tactics technique and procedures *(It is alternative for cyber kill chain with more details)*

Threat Hunting Methodologies

IOCS based threat hunting	The threat hunter use IOCs from threat intel feeds ,It is performed once the SIEM has an alert based on IOCs in the system , they investigate the activity before and after the alert to identify any compromise in the environment *(This hunting requires someone in the community to identify the IOC and share it)*

Threat Hunting Methodologies (cont)

Hypothesis based threat hunting	Threat hunters Create hypotheses , they monitor activities for any patterns in order to detect the threat . In this way, the hunter is able to proactively detect threat actors before they can actually do any damage to the environment . To create the hypothesis , the hunter can base on : *1- Create hypothesis base on new shared threat report of new information about a new threat , so they create a hypothesis and hunt based on it to make sure that the new threat is not infected their organization in particular. 2- Threat hunter learn about an attack and try to hunt for any indicator of the attack in their environment. 3 - Threat hunter start directly from the data and try to find anything malicious.*
Anomaly based threat hunting	Leveraging machine learning to detect abnormal behavior and uncover new threat patterns
Situational based threat hunting	Start the hunt based on enterprise's internal risk assessment and vulnerabilities analysis of the environment *(this methodology is impacted by situational awareness)*

What Threat Hunter Needs

Data	Every single spot on the organization need to be monitored because the hunt effectiveness depend on how imporatnt the data is.
Threat Intel	Threat hunters base their hunt on IOAs and IOCs

By **Nourelhouda Bensiali** (Nourelhouda)

cheatography.com/nourelhouda/

Published 28th February, 2024.
Last updated 28th February, 2024.

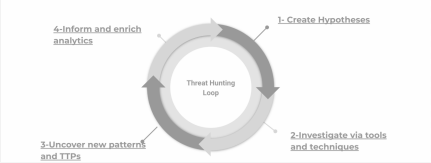
Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

What Threat Hunter Needs (cont)

Baseline in order to detect abnormalities threat hunter needs to understand the normalities ,so baseline will define the events that are authorized and expected making it easier to spot anomalies

The more you know about your own network, the more effectively you can protect it.

Threat Hunting Process-1



Threat Hunting Process-2

Create hypothesis	The key to get started in threat hunting is knowing what to ask *Example :* Who are threat actor that likely to target my organization? what they are targeting ? what is there motives ?
Investigate via tools and techniques	After generating the hypothesis , this hypothesis need to be tested by using relevant tools and techniques
Uncover new patterns and TTPs	This step is aims to uncover new patterns and TTPs found on investigation ,in this step the hypothesis can be proved or disproved *(The disproved hypothesis can be refined and retested)*
Inform and enrich Analytics	Successful hunts form the basis for informing and enriching automated analytics *(information from hunts can be used to improve existing detection mechanisms, which might include updating SIEM rules or detection signatures)*

Threat Hunting Metrics

Number of incidents that are detected by severity
Number of compromised hosts
Dwell Time of any incidents discovered
Number of detection gaps filled
Any new visibility gained during the exercise.
False positive rate
Vulnerabilities identified
Number of hunts transitioned to new analytics

These metrics can be used to measure the hunt success

Resources

The Cyber Hunting Maturity Model
A Framework forCyber Threat Hunting
Why threat hunting is important
Elastic Guide to threat hunting
What Is Cyber Threat Hunting?
CROWDSTRIKE
INFOSEC
Keynote: Threat Hunting as a Culture (HaaC)
Threat Hunting
NetworkChuck
SANS Digital Forensics and Incident Response
Cyborg Security
The Hacker News
Mitre Attack
Cyber Kill Chain
Attack Life Cycle
Pyramid of Pain
BLEEPINCOMPUTER

I used These resources to learn and then apply this knowledge to my day job as well as to create this cheatsheet

By **Nourelhouda Bensiali** (Nourelhouda)

cheatography.com/nourelhouda/

Published 28th February, 2024.
Last updated 28th February, 2024.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com