Threat Intelligence and Threat Hunting from a SOC Analyst Prospective

Threat Hunting VS Threat Intelligence

- Threat Intelligence- Is the process of gathering data on emerging or existing actors or attacks using tools and techniques to generate patters on how to protect against potential risks
- Threat Hunting- Uses these data to check if any bad actors has shown on the environment
- SOC Analyst: Uses threat intelligence to perform threat hunting on their environment.

Threat Intelligence Classifications

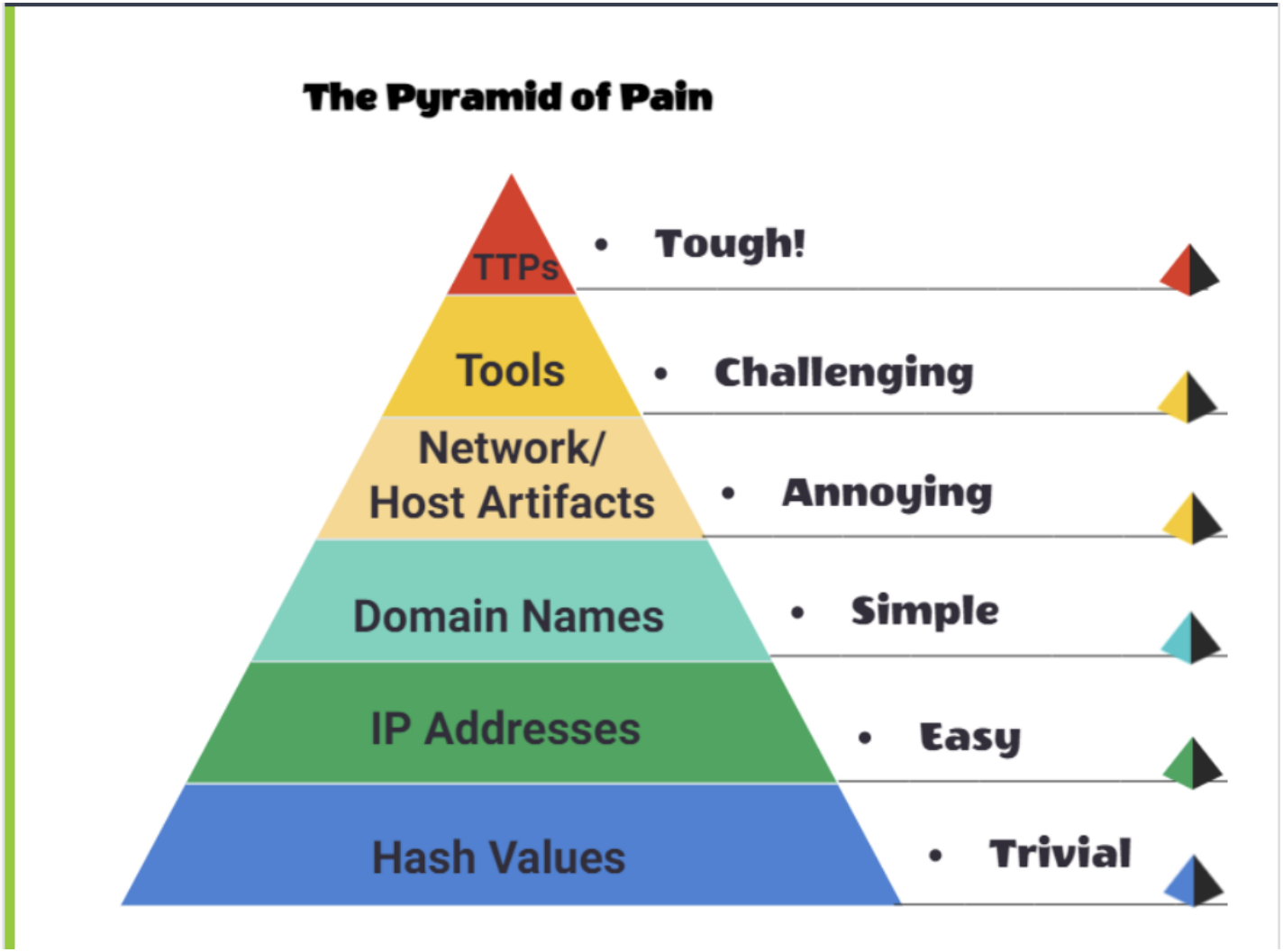
- **Strategic Intel**- Looks into an organization’s landscape and maps out the risk areas based on some trends and patterns seen
- **Technical Intel**- Looks into any evidence of attacks by an adversary
- **Tactical Intel**- Assesses TTPs which stands for Adversaries' tactics, techniques and procedures.
- **Operational Intel**- Investigates an adversary’s specific motives and intent to perform an attack. (Think like a hacker class tries to explore some of these concepts for those who are interested)

- This intel can strengthen security controls and address vulnerabilities through real-time investigations.

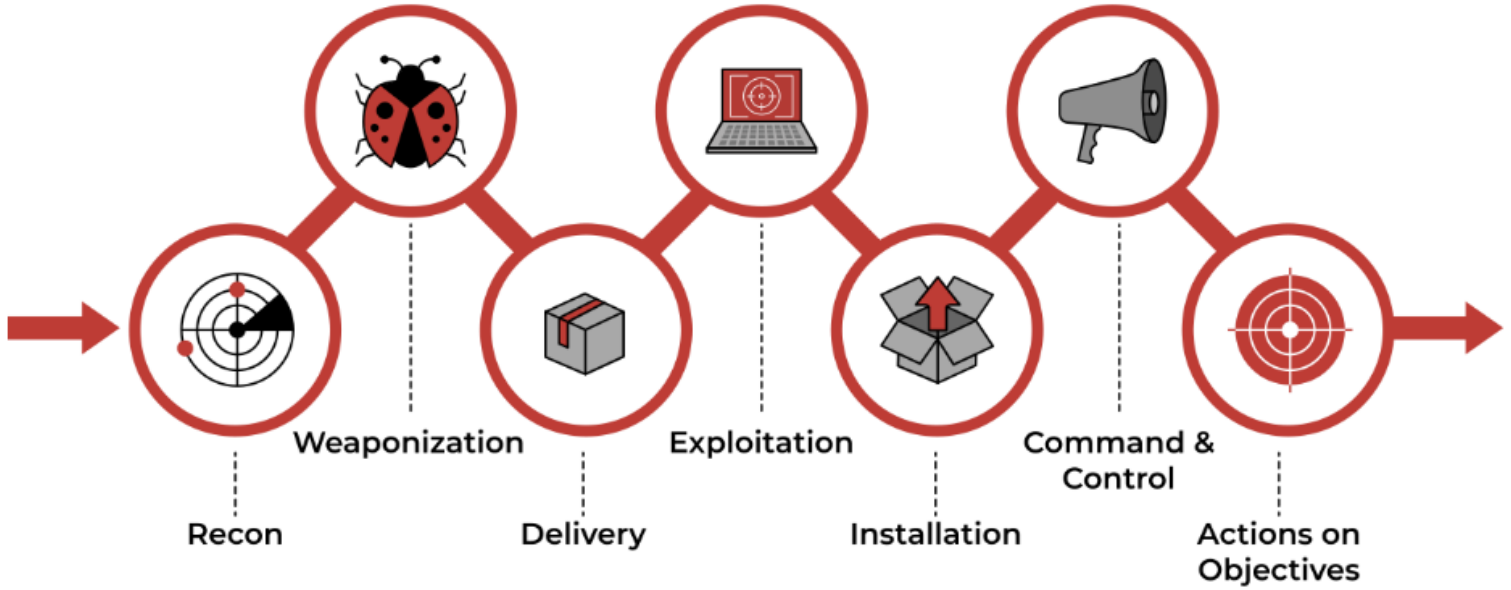
Frameworks Models Used in Threat Intelligence

- Models in Threat Intelligence are important because they are built to determine the level of difficulty that an adversary would have to go through to reach our system and what level of preparation is needed
- Some of these framework models include:
  - Pyramid of Pain
  - Cyber Kill Chain
  - Unified Kill Chain
  - Diamond Model
  - MITRE ATT&CK

Pyramid of Pain



Cyber Kill Chain

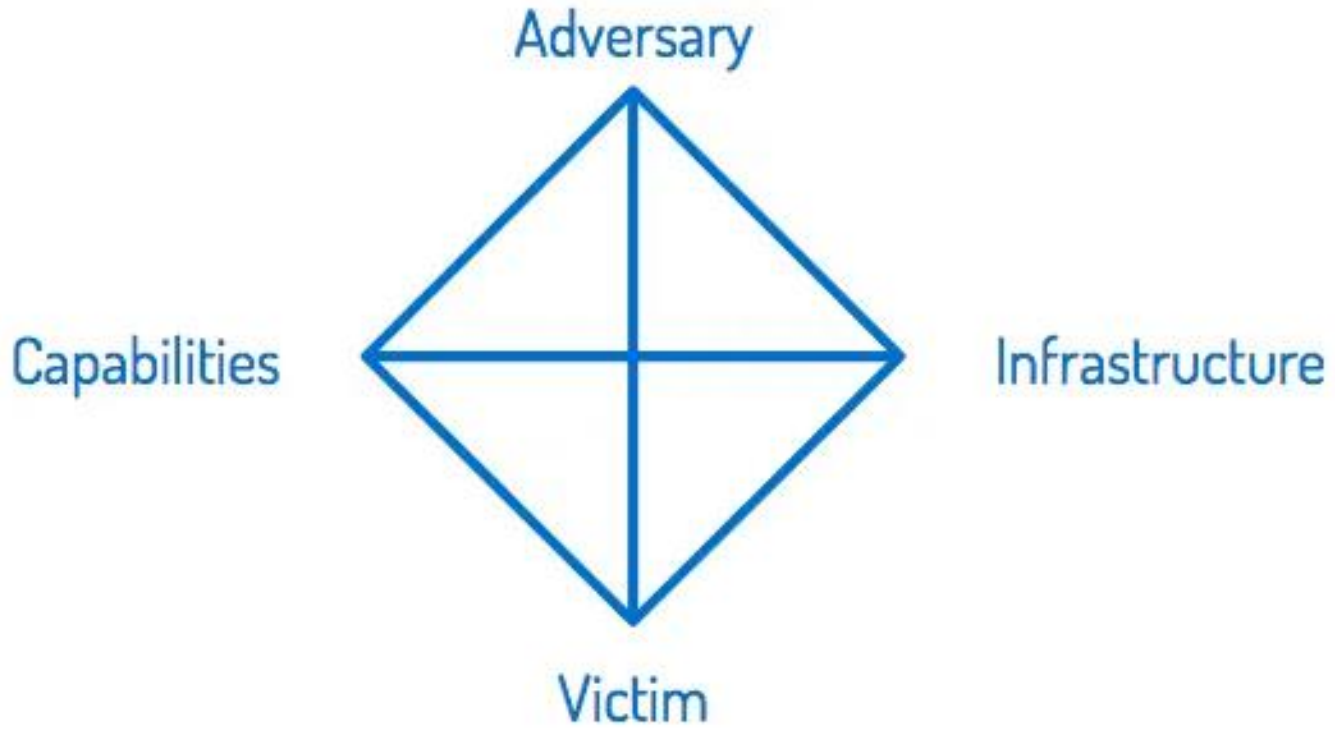


The Unified Kill Chain		
1	**Reconnaissance**	Researching, identifying and selecting targets using active or passive reconnaissance.
2	**Weaponization**	Preparatory activities aimed at setting up the infrastructure required for the attack.
3	**Delivery**	Techniques resulting in the transmission of a weaponized object to the targeted environment.
4	**Social Engineering**	Techniques aimed at the manipulation of people to perform unsafe actions.
5	**Exploitation**	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6	**Persistence**	Any access, action or change to a system that gives an attacker persistent presence on the system.
7	**Defense Evasion**	Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8	**Command & Control**	Techniques that allow attackers to communicate with controlled systems within a target network.
9	**Pivoting**	Tunneling traffic through a controlled system to other systems that are not directly accessible.
10	**Discovery**	Techniques that allow an attacker to gain knowledge about a system and its network environment.
11	**Privilege Escalation**	The result of techniques that provide an attacker with higher permissions on a system or network.
12	**Execution**	Techniques that result in execution of attacker-controlled code on a local or remote system.
13	Credential Access	Techniques resulting in the access of, or control over, system, service or domain credentials.
14	Lateral Movement	Techniques that enable an adversary to access and control other remote systems.
15	**Collection**	Techniques used to identify and gather data from a target network prior to exfiltration.
16	**Exfiltration**	Techniques that result or aid in an attacker removing data from a target network.

Unified Kill Chain

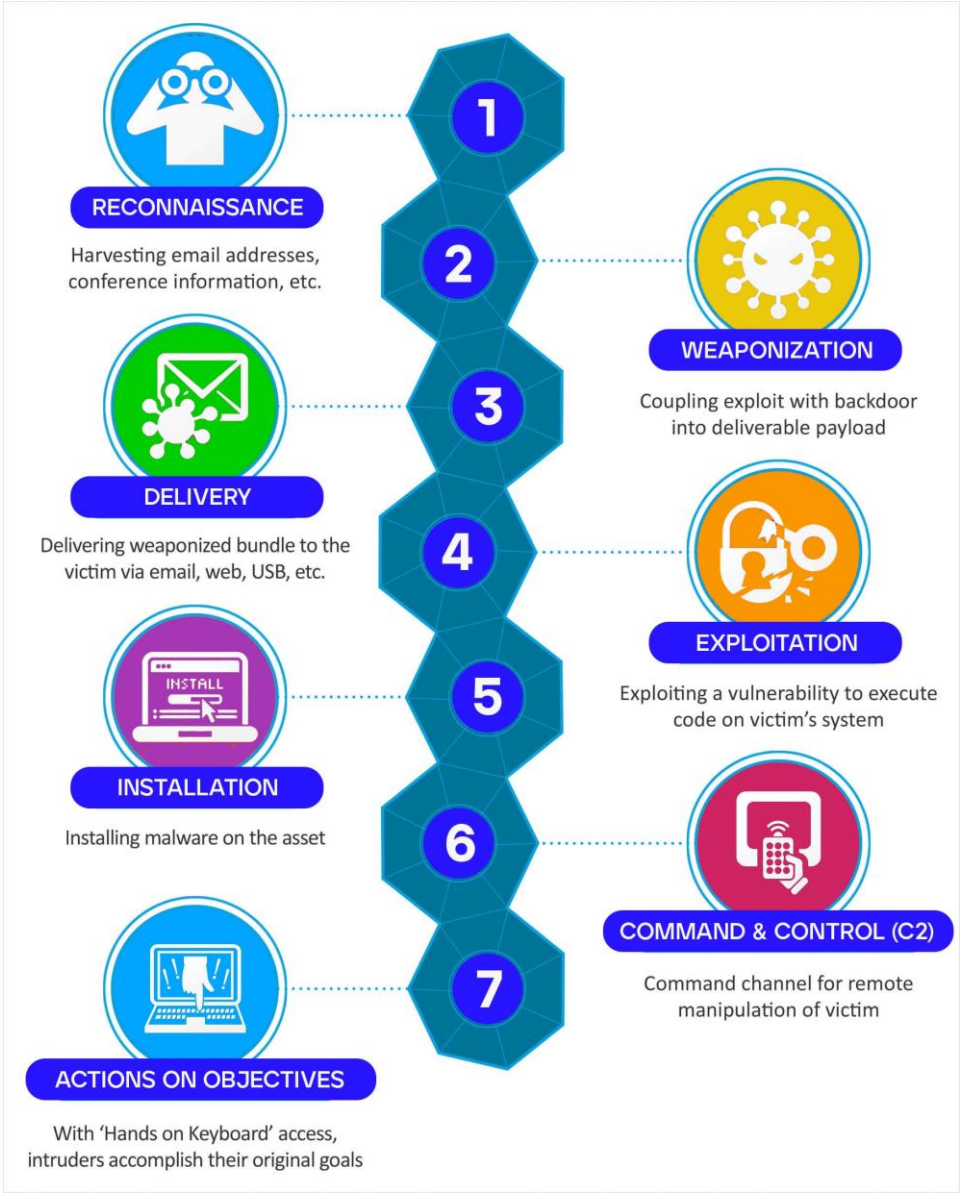
Diamond Model

Luke Skywalker!



Kill-Chain Examples

Playbook Examples



MITRE

"At MITRE, we solve problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation."

MITRE is used by organizations to understand their security readiness and uncover vulnerabilities in their defenses.

MITRE Terminology

APT- Advanced Persistent Threat- can be considered a team/group (threat group), or even country (nation-state group), that engages in long-term attacks against organizations and/or countries.

TTP- Tactics, Technique, and Procedures-
- o The Tactic is the adversary's goal or objective.
- o The Technique is how the adversary achieves the goal or objective.
- o The Procedure is how the technique is executed.

MITRE ATT&CK®- is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

CAR- Cyber Analytics Repository- is a knowledge base of analytics developed by MITRE based on the MITRE ATT&CK® adversary model.

MITRE Engage- is a framework for planning and discussing adversary engagement operations that empowers you to engage your adversaries and achieve your cybersecurity goals.

MITRE D3FEND- Detection, Denial, and Disruption Framework Empowering Network Defense. A knowledge graph of cybersecurity countermeasures.

MITRE ATT&CK Github link

- https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0008%2FG0008-enterprise-layer.json

- https://mitre-attack.github.io/attack-navigator/

MITRE TryHackMe Room

https://tryhackme.com/room/mitre

TOOLS USED IN THREAT HUNTING BY A SOC ANALYST

- **urlscan.io** - A great tool when scanning and analyzing websites. It records activities and interactions of one website to other websites, kind of like where goes websites or Virus Total
- **Yara** - is a language that you can use to write rules to detect malware and malicious files.
- **Abuse.ch** is a research project from Bern University that has created some interesting tools when it comes to Threat Hunting such as:
- **Malware Bazaar:** A resource for sharing malware samples- https://bazaar.abuse.ch/ You can search there if something has been reported as malware
- **Feodo Tracker:** A resource used to track botnet command and control (C2) infrastructure linked with Emotet, Dridex and TrickBot. https://feodotracker.abuse.ch/browse/
- **SSL Blacklist:** A resource for collecting and providing a blocklist for malicious SSL certificates and JA3/JA3s fingerprints. https://sslbl.abuse.ch/
- **URL Haus:** A resource for sharing malware distribution sites. https://urlhaus.abuse.ch/
- **Threat Fox**: A resource for sharing indicators of compromise (IOCs). https://threatfox.abuse.ch/

Threat Intel Resources and Guides

- Katie Nickels (SANS Instructor, Industry Leader)
  - https://medium.com/katies-five-cents/faqs-on-getting-started-in-cyber-threat-intelligence-f567f267348e
  - https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-1-968b5a8daf9a
  - https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-2-d04b7a529d36
- https://www.threatintel.academy/
- https://chrissanders.org/training/cuckoosegg/
- https://unprotect.it/map/