Threat Intelligence

Threat Intelligence

“Threat intelligence is information that an organization uses to understand the threats that are currently targeting them, or could target them in the future”.

Goals

- Provide information on more sophisticated threats (APTs, 0-day vulns
- Help the organization to understand who is (or could be) attacking them
- Why they’re doing it
- Tactics they use so they can be replicated in penetration tests and red team engagements, or defensive measures put in place to stop or slow down attackers.

Threat Intelligence Lifecycle

1. Planning & Direction
2. Collection
3. Processing
4. Analysis
5. Dissemination
6. Feedback

Types of Intelligences

Sigint - Signal Intelligence

- Comint - Communicaton Intelligence
- Elint - Electronical Intelligence

Osint - Open-source Intelligence
Open-source intelligence is information that is gathered from public sources.
Humint - Human Intelligence
This intelligence is often gathered through in-person meetings, debriefings personnel tasked with acquiring information through observation, document gathering, etc.
Geoint - Geospatial Intelligence
Satellite imaging is highly used to provide intelligence personnel with targets, landmass structures, and whether they’re manmade or natural, where our militaries are and their enemies, to better coordinate attack and defense efforts.

Types of Threat Intelligence

- Strategic Threat Intelligence
- Operational Threat Intelligence
- Tactical Threat Intelligence

Threat Actors and APTs

Threat Actor

A threat agent or threat actor in regard to cyber threat intelligence is an actor that intentionally or unintentionally generates an adverse effect on an organization, such as conducting a cyberattack or unintentionally leaking information.

Actor Categorization

- Cyber Criminals
- Nation-States
- Hacktivists
- Insider Threat

Actor Motivations

- Financial Motives
- Political Motives
- Social Motives
- Unknown Motives

APTs

APTs include a group of highly skilled attackers, who have a state backing or otherwise almost unrestricted access to a variety of resources. APTs deliver maximum, long-lasting damage and target specific organizations according to their motives. APTs typically use previously unseen malware and exploits (also known as 0-day exploits), with their own tailored software and frameworks to carry out the attacks.

Operational Intelligence

Operational intelligence typically involves collecting indicators, indicators of compromise, and precursors in order to share actionable intelligence with other entities, and work to make malicious actor’s lives harder by hitting them at different levels of the Pyramid of Pain.

Precursors

“Precursors” or “Threat Precursors” are elements of the incident identification and response process that allow both an attacker and a security researcher or professional to determine the existence of flaws and/or vulnerabilities within a system. By identifying precursors organizations can work to prevent cyber attacks before they occur.

Indicators of Compromise (IOCs)

Indicators of compromise are a core part of threat intelligence, and allow us to share information on threats in several different formats. This information is used to power intrusion detection and prevention systems, endpoint detection and response systems, firewalls, and other automated defenses. Human analysts can also use these to perform threat exposure checks against their environments to identify the early, or late, signs of a cyberattack.

Example of IOCs

- Email Addresses
- IP Addresses
- Domain Names/URLs
- File Hashes/File Names

IOC Formats

- STIX
- TAXII

MITRE ATT&CK Framework

MITRE’s Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s attack lifecycle and the platforms they are known to target.The primary use case of ATT&CK is for identifying the behavior of APTs and it explores the various ways that these APTs can compromise a computer and/or network.

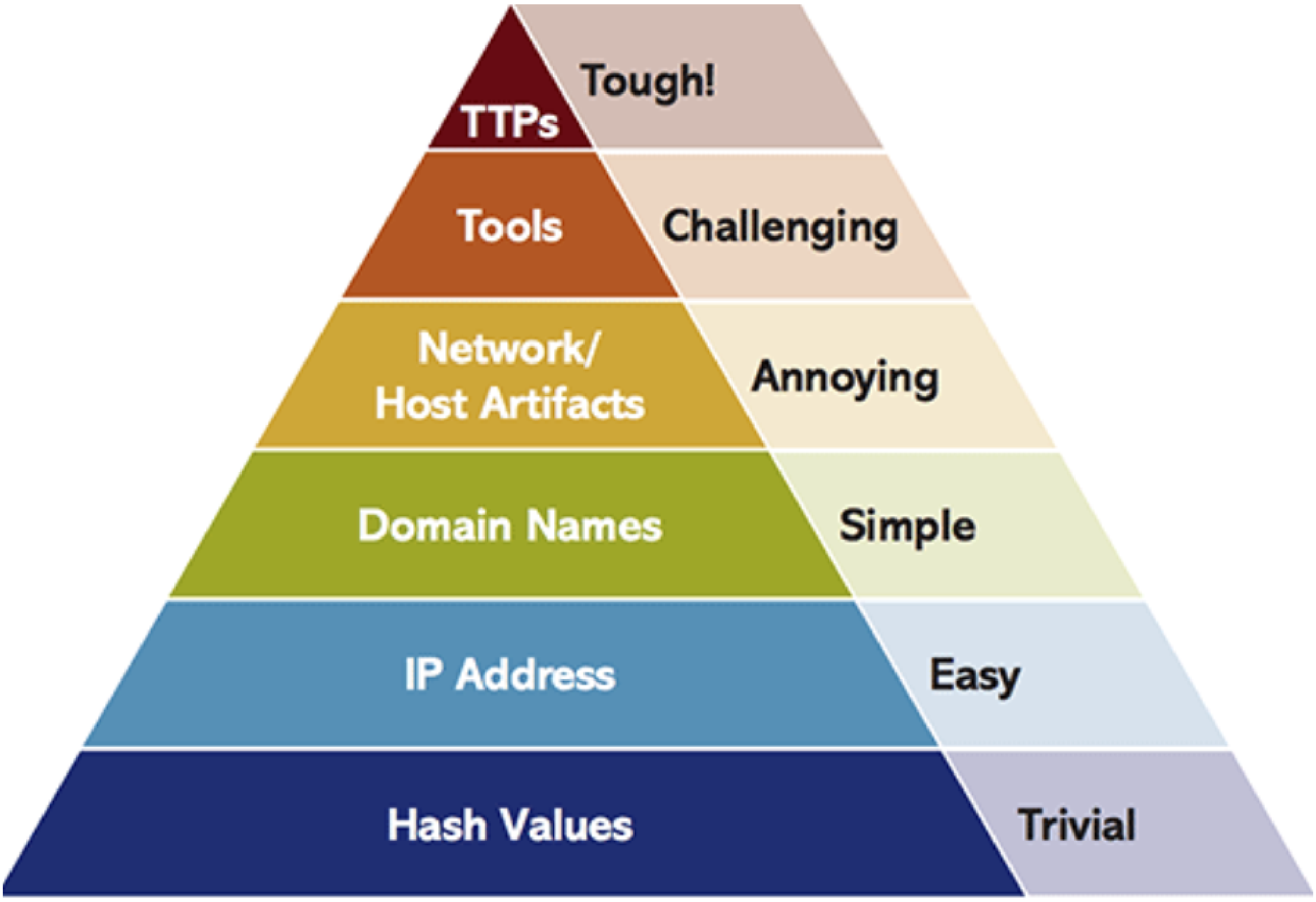
Lockheed Martin Cyber Kill Chain

It is an Intelligence Driven Defense model for the identification and prevention of cyber-attacks, specifically ones that can be classified as Advanced Persistent Threats (APTs). The CKC can help IT security teams and professionals develop strategies, products, and plans to detect and contain attacks at different stages, resulting in a more secure IT environment.

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Actions on Objectives

Pyramif of Pain

The pyramid of pain is a visual representation of the amount of pain we can cause a malicious actor in denying them certain indicators, working to disrupt their operations. Starting at the bottom are the easiest indicators that an actor can change (remember, we can change the hash of a malicious file by editing a single character! This can circumvent hash-based blocks in security tooling), and at the top is the hardest indicator to change, forcing adversaries to change their entire operations by understanding and defending against the techniques they use in attacks.



Attribution

Attribution is the determination of a cause or origin of action. In the realms of cybersecurity, we are primarily concerned about this when malicious actors are in play, and determining who, what or where a cyber breach or intrusion has occurred.

- Machine Attribution
- Human Attribution
- Ultimately Responsible Attribution

Key Indicators to attribution

- **Tradecraft –** Frequently used behaviors such as an attacker’s techniques, tools, and procedures used to conduct cyber-attacks.

- **Infrastructure –** The physical machines or networks used in the attack; are often compromised by other means before an attack.
- **Malware –** Malware can be specific to a threat actor; it can be reused or it can be modified quickly if a compromise is suspected to avoid attribution.
- **Intent** – The intent behind the attack, the motivation, or reasoning.
- **External sources** – External reports from organizations like cyber security companies, media even students.

Tactical Intelligence

Tactical intelligence typically involves performing threat exposure checks to see if malicious indicators have been identified within the environment, conducting public exposure assessments to see how what information about the company and its employees is freely available online and if that could be exploited in any way, and collecting and using actionable intelligence to improve defenses by implementing threat feeds to power automated defenses and provide context to security investigations.

Threat Exposure Checks

A threat exposure check is when an analyst uses multiple tools such as SIEM and EDR to look for the presence of any indicators of compromise they have retrieved from intelligence vendors, information sharing partners, government alerts, or OSINT sources.

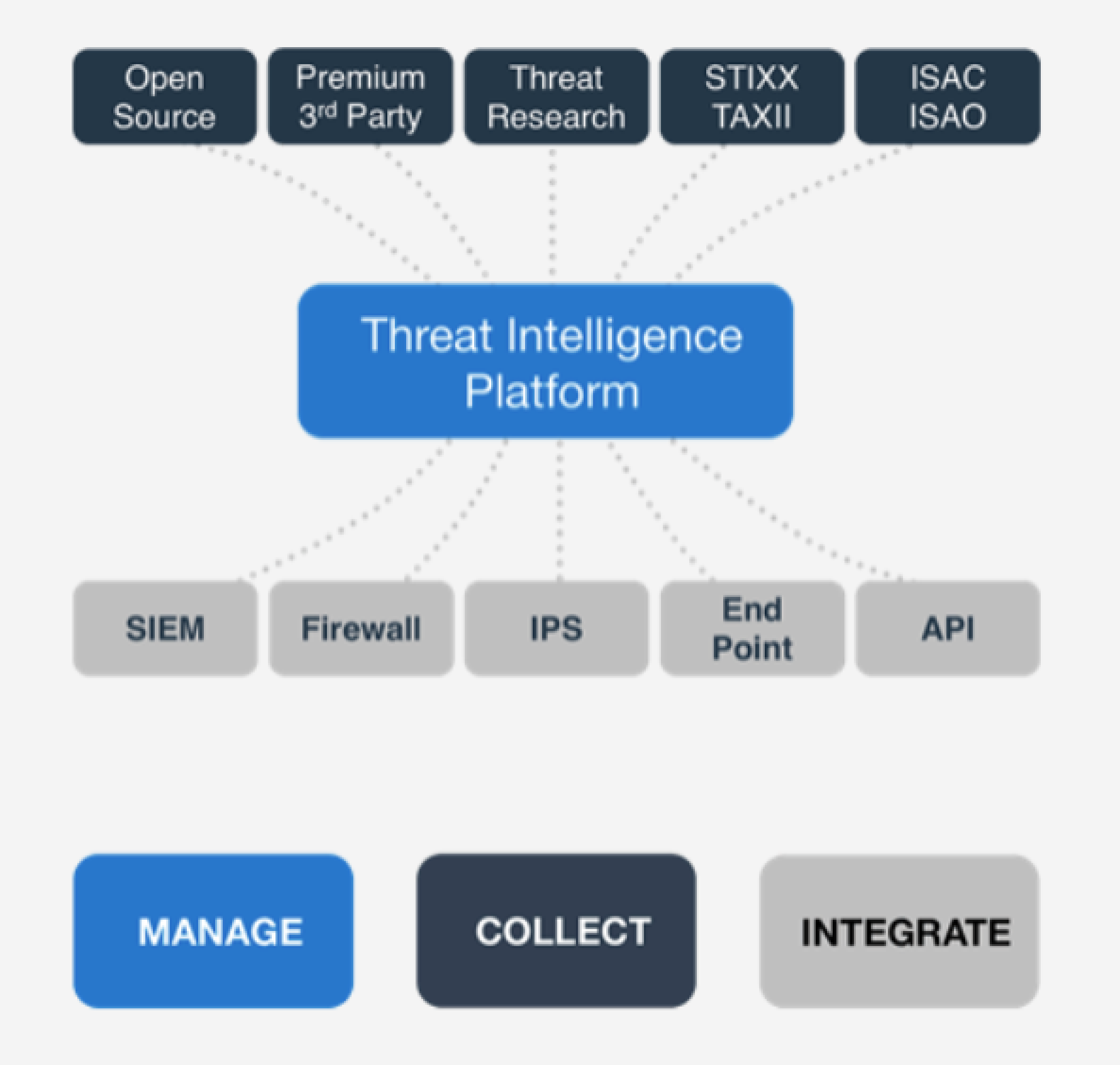
Public Exposure Checks

When we say public exposure checks, what we mean is the process a threat intelligence analyst takes to determine what information is publicly available online about their organization, and if this can be exploited in any way to cause damage. This can range from employees posting pictures of them in the office on social media to employee credentials in data breach dumps for sale on the dark web.

Threat Intelligence Platforms

Simply put, a Threat Intelligence Platform allows an organization to store everything related to threat intelligence in one single location.

- Aggregation and normalization of intelligence collected from multiple sources.
- Integrate with existing security controls such as firewalls and intrusion prevention systems.
- Analysis and sharing of threat intelligence.



TIP Products

- Malware Information Sharing Platform (MISP)
- ThreatConnect
- Anomali
- ThreatQ

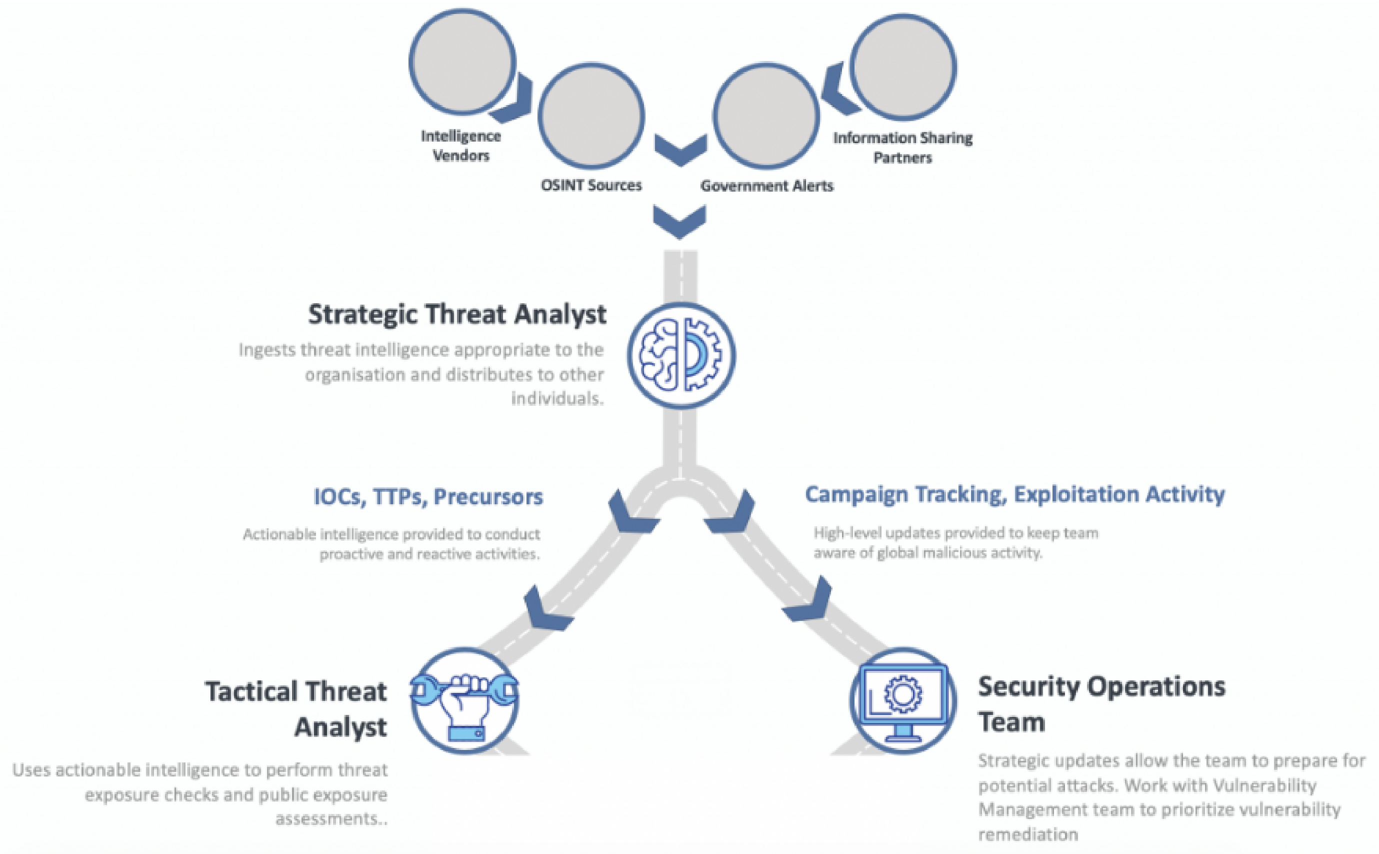
Strategic Intelligence

Strategic intelligence typically involves collecting and sharing actionable intelligence with partners and the internal security team to provide threat intelligence context, giving defenders more useful information about malicious actor activity on a global scale.Strategic Analysts tend to focus on the geopolitical activity of hostile nations, working to monitor if there is or will be an increased threat from that nation and their associated Advanced Persistent Threats (APTs) in the future.

Intelligence Sharing and Partnerships

If an organization has an established threat intelligence team, someone will likely be responsible for connecting with other organizations to join or form an Information Sharing and Analysis Center (ISAC). These are typically industry-specific groups comprised of multiple organizations in order to share actionable intelligence such as indicators of compromise, precursors, and information about attacks and threats.

IOC/TTP Gathering and Distributio


Intelligence Vendors
OSINT Sources
Government Alerts
Information Sharing Partners
Strategic Threat Analyst
Ingests threat intelligence appropriate to the organisation and distributes to other individuals.
IOCs, TTPs, Precursors
Actionable intelligence provided to conduct proactive and reactive activities.
Campaign Tracking, Exploitation Activity
High-level updates provided to keep team aware of global malicious activity.
Tactical Threat Analyst
Uses actionable intelligence to perform threat exposure checks and public exposure assessments..
Security Operations Team
Strategic updates allow the team to prepare for potential attacks. Work with Vulnerability Management team to prioritize vulnerability remediation

Traffic Light Protocol

The purpose of TLP is to allow the author of the original information to state how they want their information to be circulated, such as sharing only with specific individuals, within an organization, within trusted communities, or in the public domain.

TLP Clear

TLP CLEAR can be publicly shared, but copyright rules still apply. Reports or updates that use this TLP are distributed freely for the good of everyone.

TLP Green

TLP GREEN may be shared within communities, such as information sharing and analysis centers (ISACs), which are groups of organizations operating in the same industry or industries. This information should not be shared outside of the intended communities, such as posting it publicly on the internet.

TLP Amber

TLP AMBER may only be shared internally within an organization on a need-to-know basis to limit who has access to the information.

TLP Amber Strict

TLP:AMBER+STRICT may be used when information requires support to be effectively acted upon however still carries risk to privacy, reputation, or operations if shared outside of the organization.

TLP Red

TLP RED is extremely sensitive and could have severe consequences if it falls into the wrong hands. If an online or in-person meeting is classed as TLP RED then the information should not be shared with anyone that isn’t present in the meeting.