Hacker Halted

CREEPING CYBER THREAT

Understanding the Cyber Threat Intelligence (CTI) Process

BE Rhodes @ Hacker Halted 2021

@cyber514

Outline

- WHOIS
- Introduction: A Day Without CTI
- Defining CTI
- Levels of CTI & Users
- CTI Process
- Setting your priorities
- Where do you get CTI?
- Where should you integrate CTI?
- CTI Build/Buy Decisions + Information Sharing
- CTI Use Cases
- Quick Use Case Demo
- Summary and Review
- Questions & Discussion

WHOIS

- WHOIS: Brad Rhodes
- TLDR:
  - Head of Cybersecurity at zvelo
  - COL, Cyber (17A), 76th Operational Response Command G6/CIO
  - Military Cyber Professionals Association, HammerCon Co-Lead
  - Speaker, Author, Professor, Coach
  - #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+

Feel to view/listen/grab my previous presentation/articles here:
https://github.com/cyberguy514

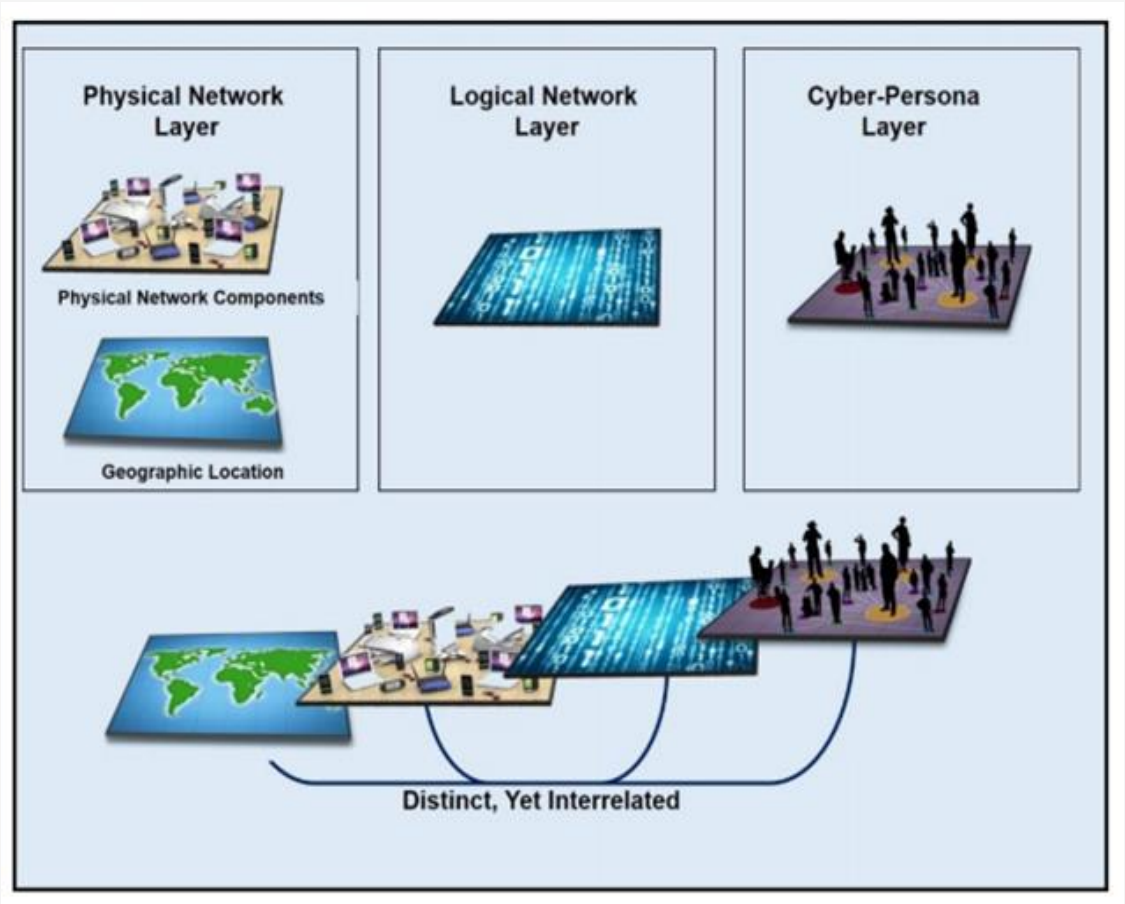
Introduction: A Day Without CTI

...you arrive at work to find your organization under **attack** from a Malicious Cyber Actor (MCA). Unfortunately, your cyber defenders do not have access to information tailored to the organization and they missed the **indicators of compromise** (IOC) that were right under their noses. In the lessons learned discussion once the bleeding had been stopped, the entire C-suite gazed in your direction and asked a simple question: what do you **need** so this never happens again?

Sound familiar? If it does, let's talk about **CTI** and why it important to organizations **GREAT** and **SMALL**!

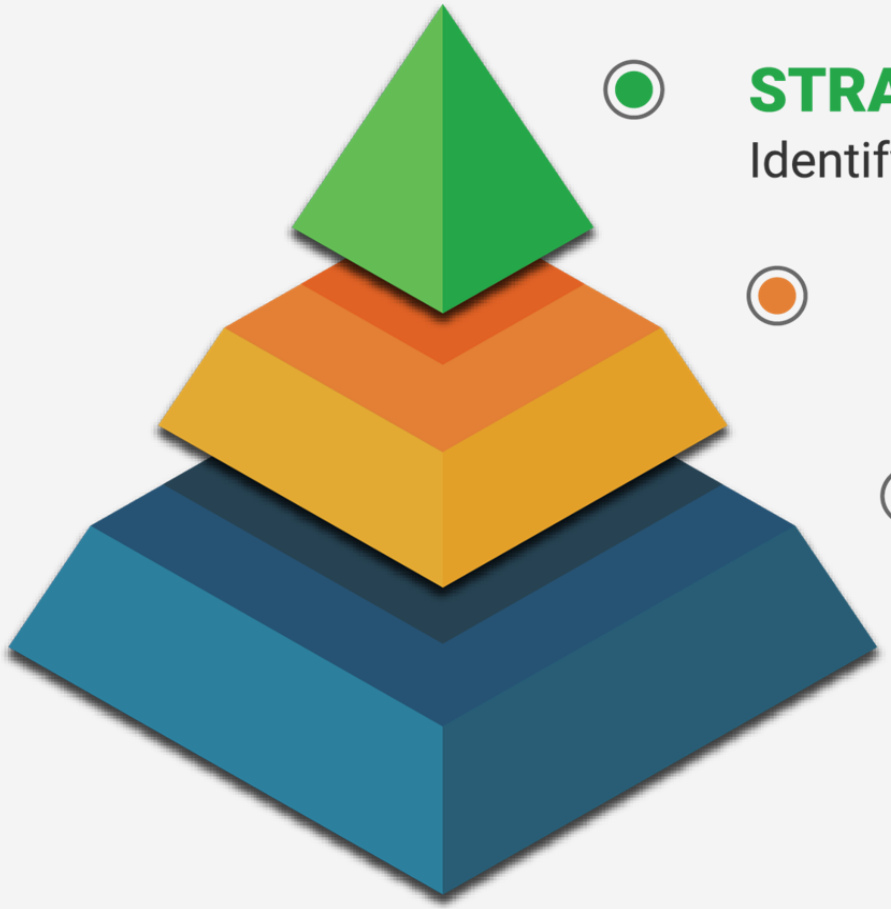
Defining CTI

- Cyber Threat Intelligence (CTI):
  - methodical process of gathering information about and analyzing cyber threats
  - data collected, processed, and analyzed based on priorities to provide relevant answers to questions
  - provides context for understanding MCA targets, attacks, and motives
  - tailored to an organization
- CTI spans the Physical, Logical, and Cyber-Persona Layers



https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf

Levels of CTI



STRATEGIC
Identify the *Who* and *Why*

OPERATIONAL
Address the *How* and *Where*

TACTICAL
Focus on the *What*

CTI Users

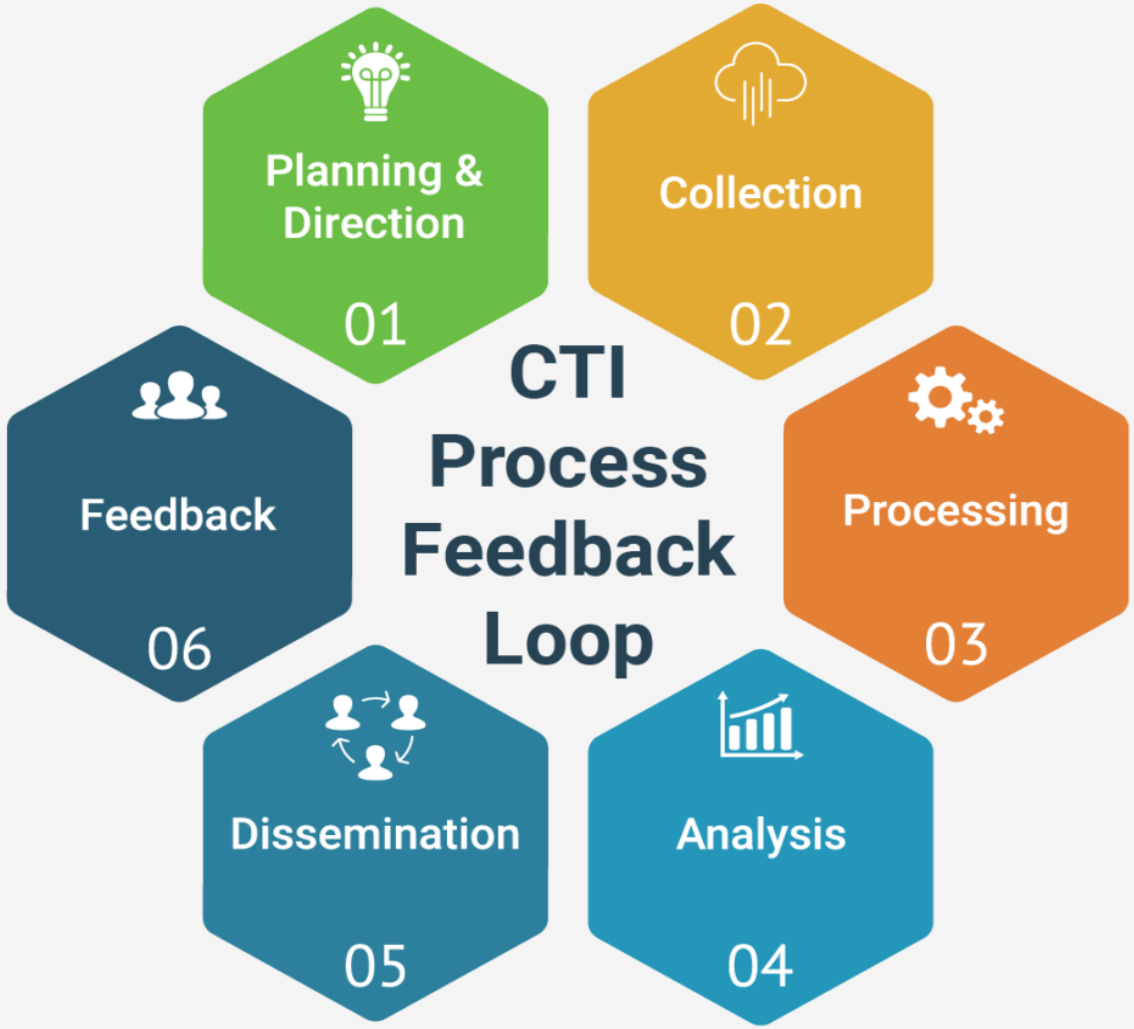
"C-Suite" — the Chief Executive Officer, Chief Financial Officer, Chief Information Officer, and so on depending on structure

Incident responders and teams, network defenders, host analysts, malware analysts, forensic analysts, and more

SOC personnel, Cyber-systems operators, MSSPs, and others

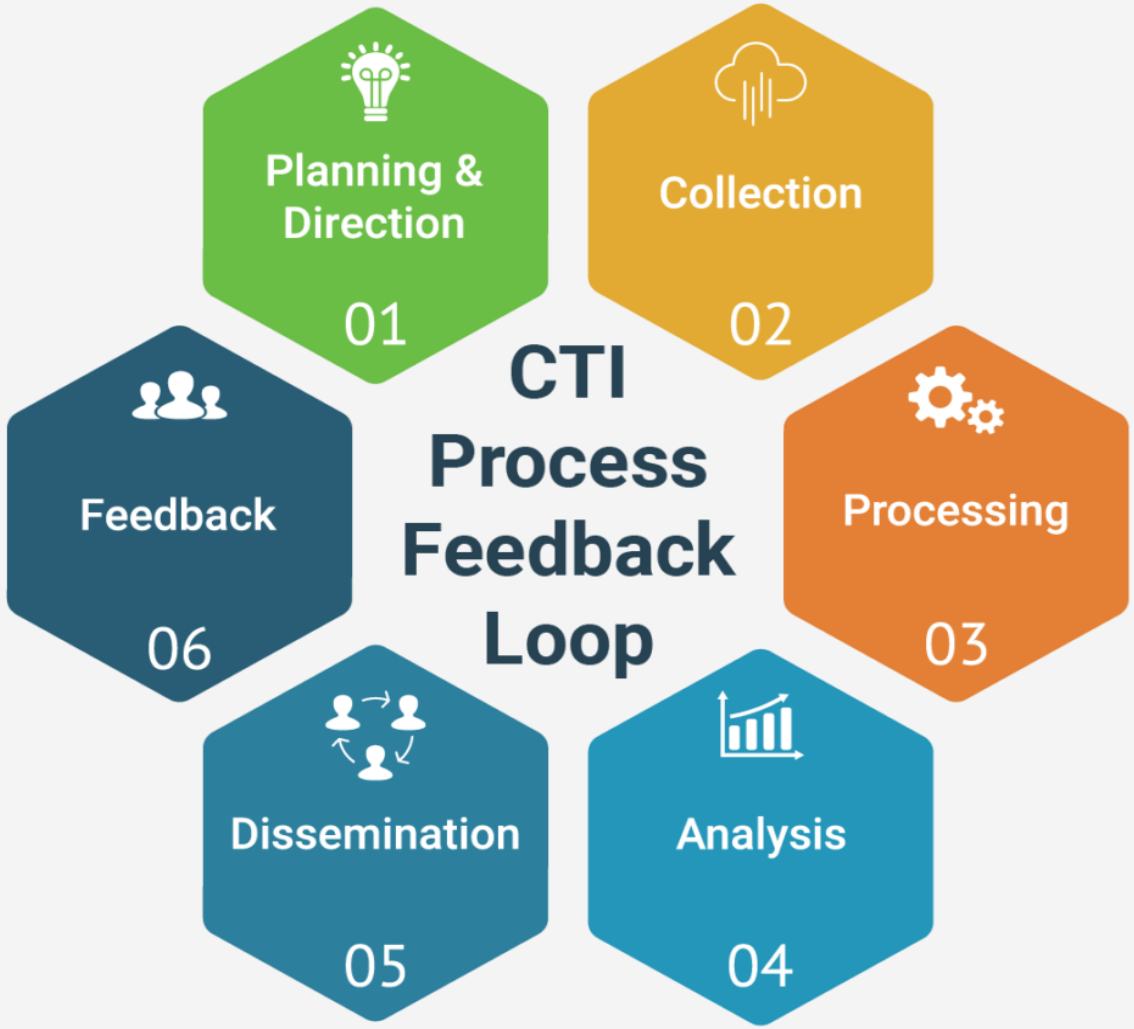
Other users: stakeholders, auditors, legal, HR, **third-parties**, and additional functional areas

CTI Process (1 of 2)



- **Planning and Direction**
  - Based on organization requirements & priorities
  - Requirements & priorities should be reassessed regularly
  - Focused on **actionable** outcomes that support **decisions**
- **Collection**
  - "The" Big Data problem
  - Gathers *raw data*
  - **Volume**, **Visibility**, & **Location**
- **Processing**
  - Methods: Rules-Based, Artificial Intelligence/Machine Learning (AI/ML), Manual Analysis
  - Raw data to *information*
  - Data Validation: **verify then trust (maybe)**

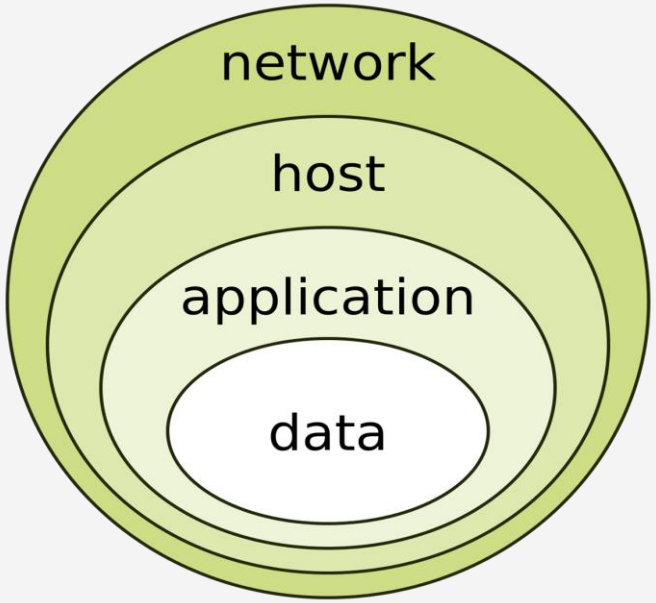
CTI Process (2 of 2)



- **Analysis**
  - Focused on created **relevant** answers for **decisions makers**
  - Information to *intelligence*
  - Methods: Manual, Fully-Automate, Hybrid
- **Dissemination**
  - Flat files, Application Programming Interface (API), Feeds (automatic pushes), analytic reports
  - Need **real-time**? Infrastructure must support it!
- **Feedback**
  - Must be a **dialogue** between consumers and producers
  - Measure of Performance (MOP): **Quantitative**
  - Measure of Effectiveness (MOE): **Qualitative**

Setting YOUR priorities

https://transformingops.com/2016/04/24/people-process-technology/



https://simple.wikipedia.org/wiki/Defense_in_depth_(computing)

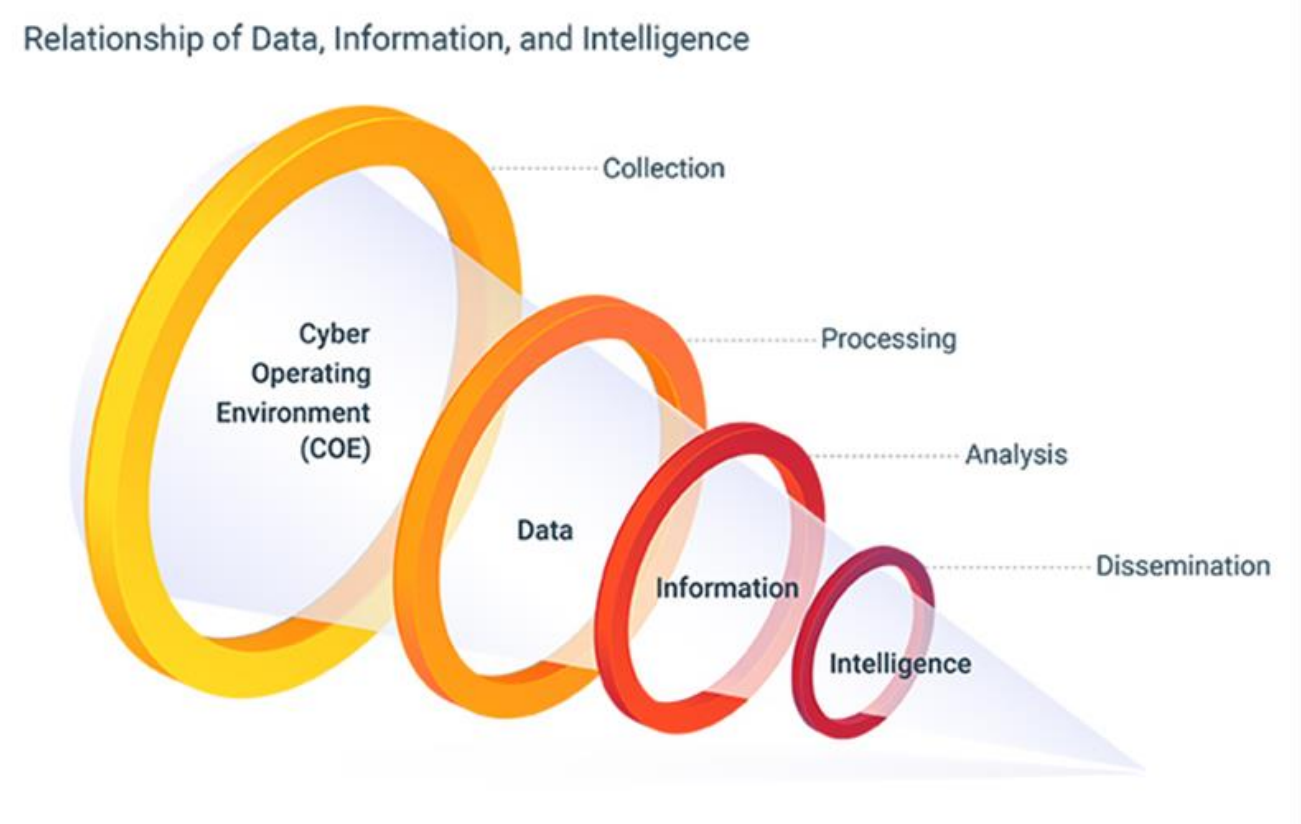
- **Priority Cyber Intelligence Requirements (PCIR):** What are the potential Cyber Threats to your organization? Be sure to include **MCAs** intent to cause harm.
- **Friendly Cyber Information Requirements (FCIR):** What do you need to know about your organization's Cyber Operating Environment (COE)? From a **Defense-in-Depth (DID)** perspective — Perimeter, Networks, Endpoints, and Data — including related vulnerabilities.
- **C-Suite Critical Cyber Information Requirements (C3IR):** What is the key information executive leadership must have to make decisions? For example, if you have a system with a critical vulnerability, is there a threat with intent to exploit it? And how will you know if, or when, a breach actually occurs?

Where do you get CTI?

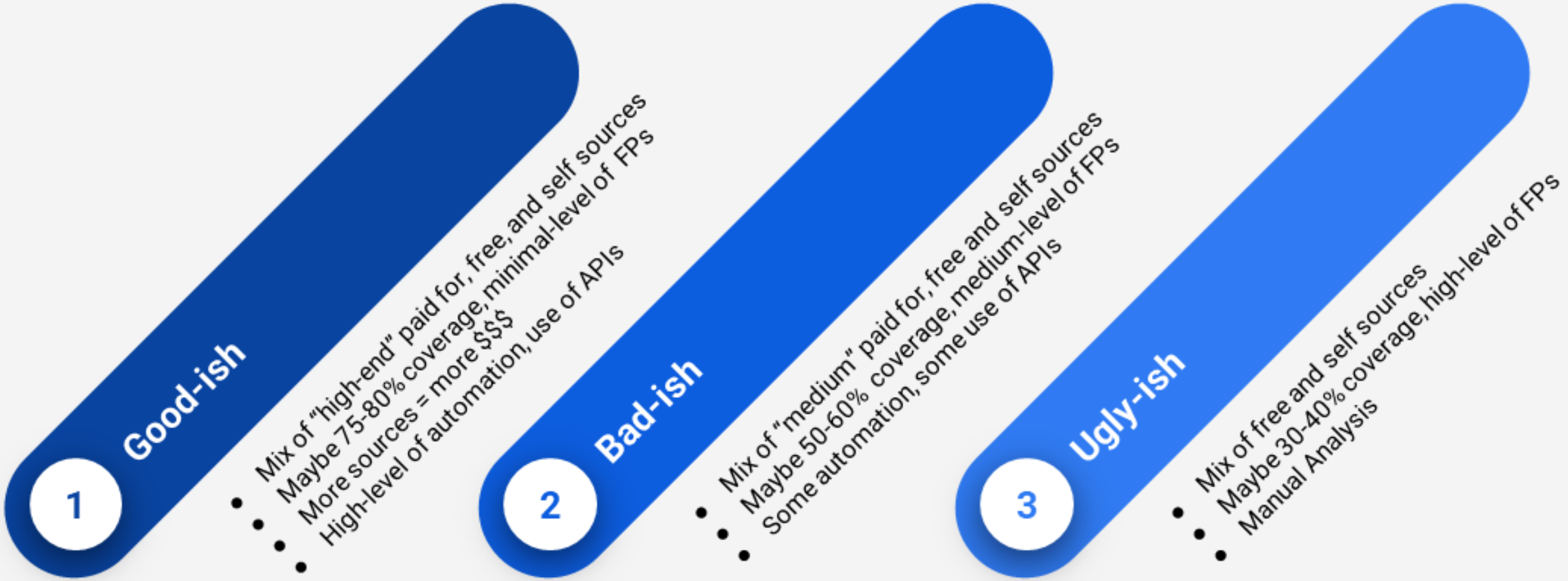
- **Third-Party Data.** Organizations can procure third party data feeds and information. These feeds can be open source or free but may come with the risk of higher **False Positives (FPs)**. Alternatively, when accuracy is critical, third party data may be purchased from a trusted vendor for a premium. List: https://github.com/hslatman/awesome-threat-intelligence
- **Self-Sourced Data.** Organizations often decide to gather data on their own from various internal sources, sensors, honeypots/nets, crowdsourcing, etc. The downside of this method is that the data collected must be stored, which can be costly.
- **Combination of Third-Party and Self-Sourced Data.** Many organizations employ a mix of feeds *plus* their own proprietary data. In theory, this may be the most effective approach to maximize CTI coverage. Research shows both gaps and differences across the unique third-party feeds available. And, while combining data sources is unlikely to result in 100% CTI coverage, organizations should maximize sources as much as possible.

Where should you integrate CTI?

- **Everywhere!**
  - People: get CTI into the hands of your analysts!
  - Process: leverage CTI to support cyber defense related decisions
  - Technology: plug CTI into your SIEMs, SOARs, IDS/IPS, Firewalls, UTMs, etc…
- Tailor CTI to what your organization needs



Where do you get CTI?: Good-ish, Bad-ish, Ugly-ish



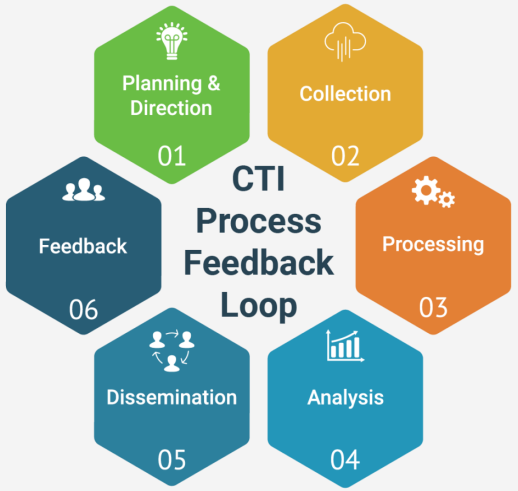
CTI Build/Buy Decisions + Information Sharing

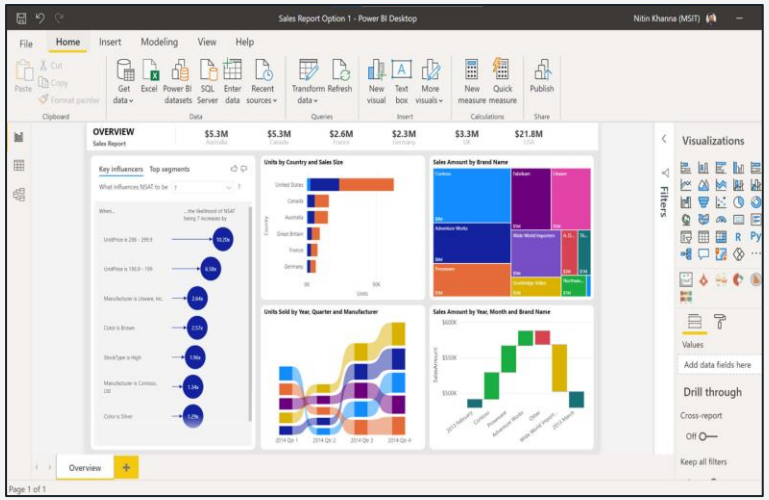
- Build? Maybe if you have extensive resources (time, money, personnel) so you can consume multiple external feeds (for coverage) & you create your own CTI from internal networks/systems
- Buy? Potentially a better decision if you don't have extensive resources; be sure to procure from a vendor who already consumes multiple external feeds (so you don't have to) - you'll still need to create CTI from your internal networks (platform: https://www.opencti.io/en/)
- Information Sharing - we've got to do it!
  - Structured Threat Information Expression (STIX): https://oasis-open.github.io/cti-documentation/stix/intro.html
  - MISP: https://www.misp-project.org/
  - Information Sharing & Analysis Centers: https://www.nationalisacs.org/
  - Information Sharing & Analysis Organizations: https://www.isao.org/

CTI Use Cases

- **Strategic Cyber Threat Intelligence Use Case: Brand Exposure Intelligence.** There are multiple data points to consider here including cybersquatting (also known as domain or subdomain squatting), domain or subdomain hijacking, phishing campaigns, and exploited web-pages/parts. Assessing exposures in each of these areas helps strategic users understand how their brand is being co-opted by MCAs to exploit their customers.
- **Operational Cyber Threat Intelligence Use Case: Threat Hunting.** Threat Hunting pulls from multiple sources, including CTI, to leverage all available IOCs that are applicable to an environment and proactively look for evidence of MCA activities.
- **Tactical Cyber Threat Intelligence Use Case: Triage.** In a triage case, tactical users first check their local CTI store, or call the APIs of their CTI sources. If there is an IOC match, they move forward with their incident handling process. If there is no match, they move onto the next alert. Utilizing CTI in a "verify, then trust" construct can significantly reduce the amount of time analysts at the tactical level must spend to differentiate between good and bad.

Quick Use Case Demo: Blocklist (Tactical)





https://powerbi.microsoft.com/en-us/

- **Planning and Direction**
  - Utilizing open source(s), generate a URL blocklist to protect our enterprise
- **Collection**
  - Choose source(s)
  - Download source file (URLHaus)
- **Processing**
  - File clean-up
- **Analysis**
  - Tooling: Power BI
  - Enrichment
- **Dissemination**
  - URL Blocklist (full-path)
- **Feedback**
  - Measure of Performance (MOP)
  - Measure of Effectiveness (MOE)

Summary and Review

- CTI…
  - has multiple levels: strategic, operational, tactical
  - is different for every organization
  - must be prioritized
  - can support people, processes, and technologies
  - may be built internal or procured as an external commodity
  - has multiple use cases
- Ultimately, properly leveraging CTI is critical to mission success into today's increasingly complex and competitive cyber operating environment!

Questions & Discussions

- Thank you to Hacker Halted for this amazing opportunity!
- Feel free to reach to me via email: brhodes@zvelo.com
- Or connect with me on LinkedIn: https://www.linkedin.com/in/brad-rhodes-1951ba7/