Project Obsidian

Cyber Threat Intelligence

Module 1: Foundations of CTI

Agenda

- Objectives
- Terminology & Definitions
- CTI Overview
- Types of CTI
- CTI Lifecycle
- Collection Management Framework

Objective

Objective

This module reviews the foundations of CTI.

CTI is a nuanced topic with a variety of applications. Therefore, it is important that we share the same understanding of terminology, concepts, goals and objectives, etc.

Terminology & Definitions

Terminology & Definitions

- Cyber Threat Intelligence
- Intelligence Requirement
- Adversary/Threat
- Intrusion
- Activity Group
- Threat Actor
- Indicator of Compromise
- IOC Pivoting
- Campaign/Operation
- TLP
- Victim
- Target
- Persona
- TTP
- Tradecraft

Source: https://github.com/blueteamvillage/obsidian-cti/tree/main/module-1

Pyramid of Pain

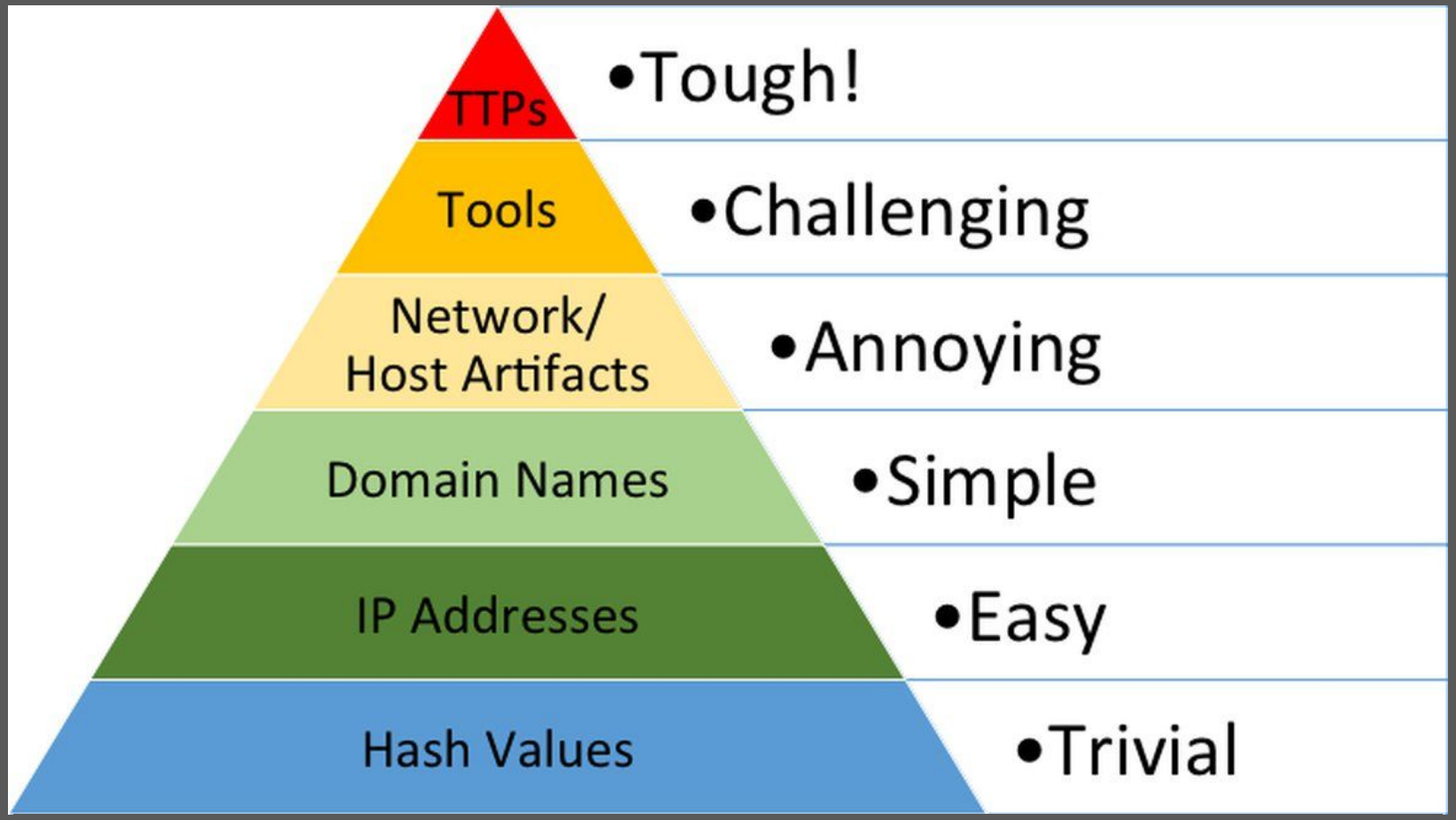


Figure: Pyramid of Pain - David Bianco

IOC Pivoting

The act of using one IOC (data point) to find more data or information, i.e. context, around an intrusion. Pivoting can be performed on host and network artifacts. IOC pivoting can generate intelligence. Outcomes include:

- Gaining insight into an adversaries infrastructure
- Revealing capabilities deployed by an adversary
- Identifying the family of malware used as part of an intrusion
- Attributing malware and/or infrastructure to an adversary
- Identifying IOCs related to a campaign

Example TTP

Tactic: high level tradecraft

-> compromise a domain controller to get passwords

Technique: manner to accomplish tactic

-> leverage exploit Y to compromise the domain controller

Procedure: specific approach to accomplish technique

-> commands used to launch exploit

Traffic Light Protocol (TLP)

TLP:RED	Not for disclosure, restricted to participants only	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER	Limited disclosure, restricted to participants' organizations	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN	Limited disclosure, restricted to the community	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.
TLP:WHITE	Disclosure is not limited	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Source: https://www.first.org/resources/papers/conf2018/MillarTom_TLP-to-IEP-Evolution-Slides-for-FIRST_20180621.pdf

CTI Overview

The goal of this section is to provide a general understanding of CTI.

CTI Overview – From Data to Action

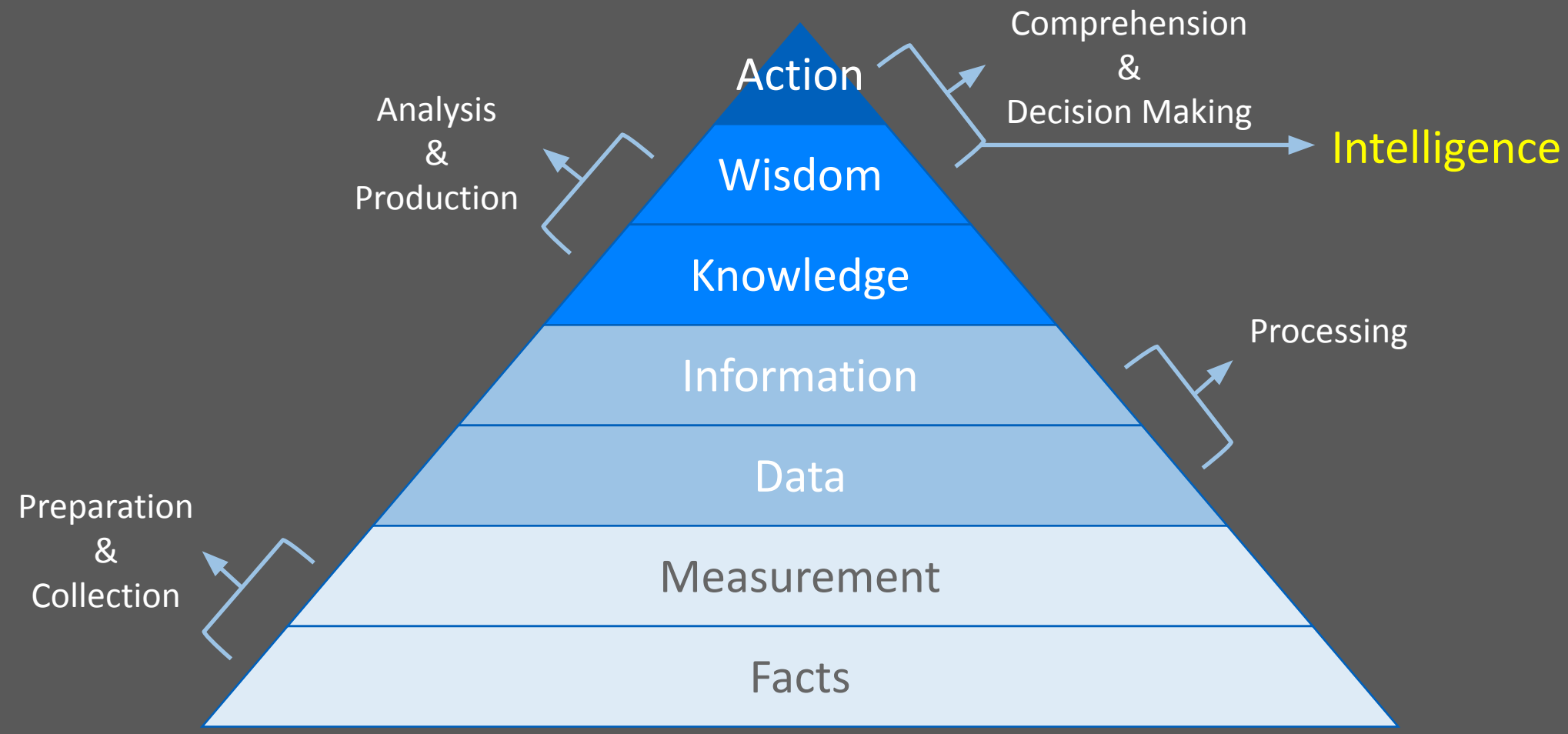


Figure: DIKW pyramid
Practical Threat Intelligence and Data-Driven Threat Hunting, Valentina Costa-Gazcon

Additional CTI Topics

Sherman Kent and the Profession of Intelligence Analysis

https://apps.dtic.mil/sti/pdfs/ADA526587.pdf

- Kent's Analytic Doctrine

Psychology of Intelligence Analysis by Richards J. Heuer, Jr.

https://www.ialeia.org/docs/Psychology_of_Intelligence_Analysis.pdf

- Tools for Thinking
- Cognitive Biases
- Improving Intelligence Analysis

Additional CTI Topics (cont)

Bias...

Cognitive Biases in Cyber Threat Intelligence

https://warnerchad.medium.com/cognitive-biases-in-cti-ac05091a903a

List of Cognitive Biases

https://en.wikipedia.org/wiki/List_of_cognitive_biases

Additional CTI Topics (cont)

Mental Models for Learning Design
https://www.litmos.com/blog/articles/mental-models-learning-design

The Diamond Model of Intrusion Analysis
https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Lockhead Martin Cyber Kill Chain
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

MITRE ATT&CK
https://attack.mitre.org/

Types of CTI

Threat intel has 3 distinct categories for audience & objectives.

Source: https://zvelo.com/strategic-operational-tactical-cyber-threat-intelligence/

Tactical Intelligence

Objective: Get technical details of threats to detect & prevent attacks

Audience: SOC Analysts, SIEM, Firewall, Endpoints, IDS/IPS

- Focuses on the immediate future
- Technical in nature
- Identifies simple indicators of compromise (IOCs)
- Provides info about TTPs used by adversaries to achieve their goals
- Easiest type of intelligence to consume
- Should be automated
- Open source and free data feeds can be used
- Has a limited lifespan

Operational Intelligence

Objective: Campaign tracking & threat actor profiling to gain a better understanding of the adversaries

Audience: SOC Analysts, Threat Hunter, Vuln Mgmt, Incident Responders, Security Management

Behind every attack is a “who,” “why,” and “how.”

- “Who” is called attribution
- “Why” is called motivation or intent
- “How” is made up of the TTPs the threat actor employs.

Strategic Intelligence

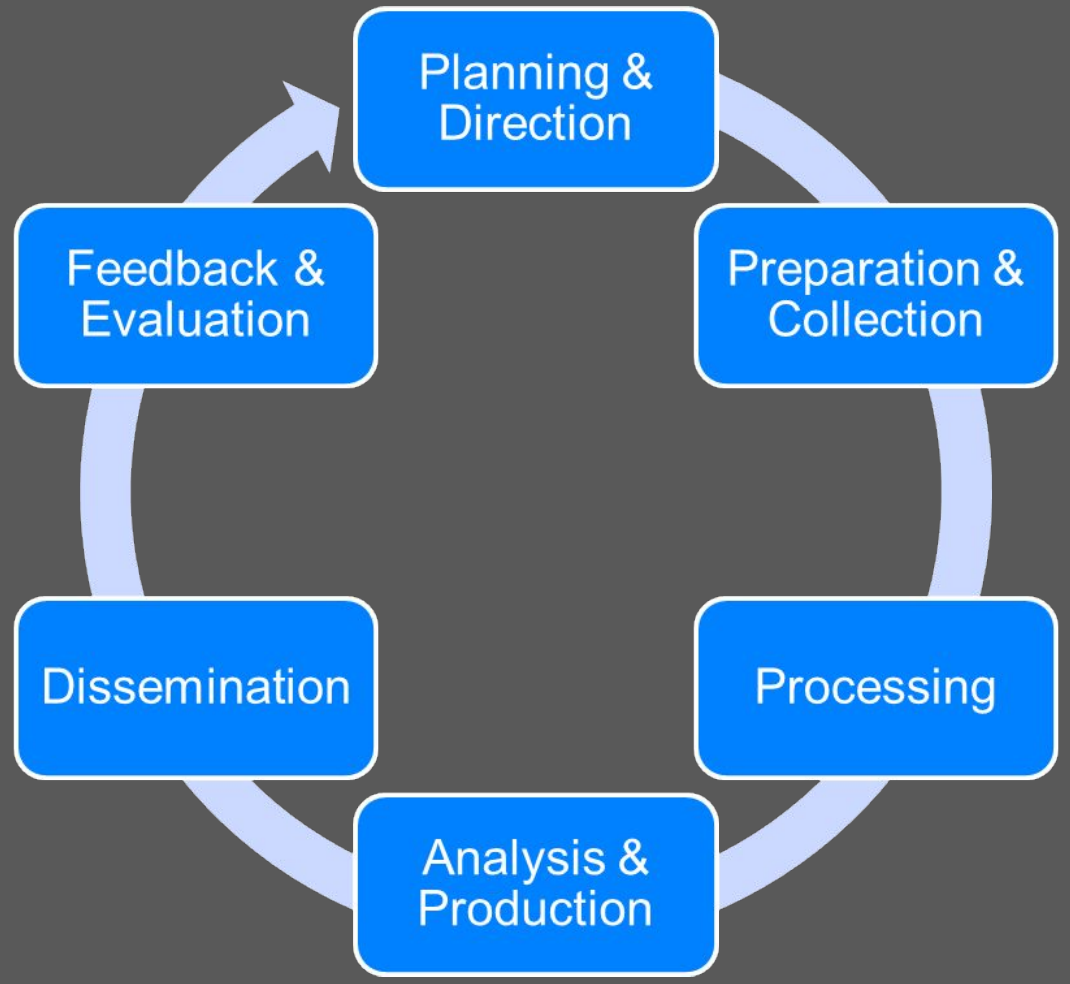
Objective: Inform business decisions and the processes behind them

Audience: C-Suite, Executive Board, Security Management

Strategic intelligence pieces together the impact of high level factors such as:

- Foreign policy
- Global events
- International movements

CTI Lifecycle



CTI Lifecycle - Planning & Direction

The planning and direction phase is when CTI goals and objectives are set. At a minimum this phase should:

- Identify critical assets and business processes
- Determine why and how the organization might be a targeted
- Establish stakeholder requirements, e.g. what are their security concerns
- Identify potential threats, i.e. adversaries, to the organization
- Select and prioritize mitigations based on potential threats to the organization

CTI Lifecycle - Preparing and Collection

Preparation and collection is the process of gathering information to satisfy an organization's intelligence requirements. Collection occurs through a variety of means, including:

- Pulling metadata and logs from internal networks and security devices
- Subscribing to threat data feeds from industry organizations and cybersecurity vendors
- Holding conversations and targeted interviews with knowledgeable sources
- Scanning open source news and blogs
- Scraping and harvesting information from websites and forums
- Infiltrating closed sources such as dark web forums

CTI Lifecycle - Processing

Processing is the transformation of collected data into a format usable by the organization. Data and information may need to be:

- Correlated
- Ranked
- Deduplicated
- Verified

Almost all raw data collected needs to be processed in some manner, whether by humans or machines or both.

CTI Lifecycle - Analysis and Production

Analysis is a human process that turns information into intelligence that can operationalized by all stakeholders. if the goal is to communicate with non-technical leaders, your report must:

- Be concise
- Avoid confusing and overly technical terms and jargon
- Articulate the issues in business terms (such as direct and indirect costs and impact on reputation)
- Include a recommended course of action

CTI Lifecycle - Dissemination

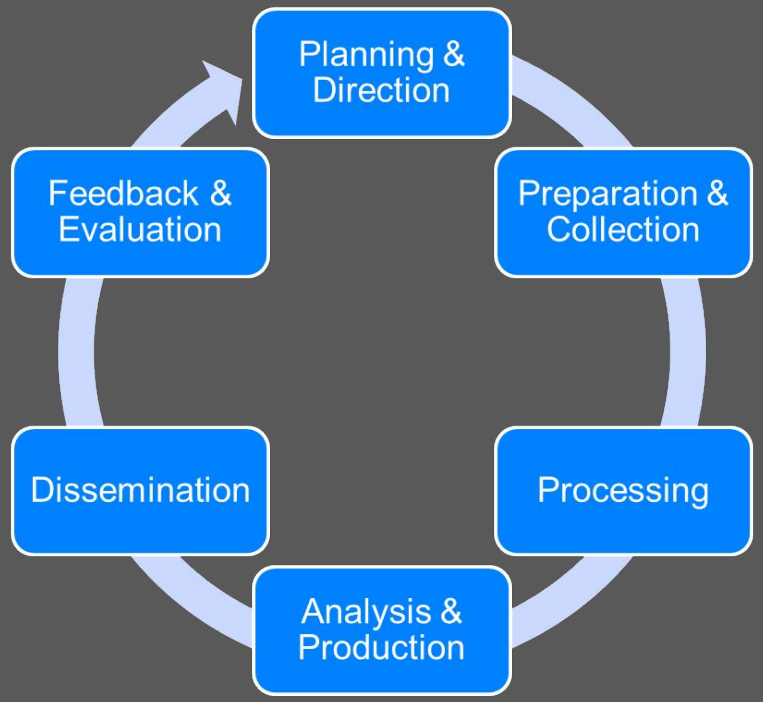
During this phase intelligence is delivered to and used by stakeholders. For each stakeholder, you need to ask:

- What threat intelligence do they need, and how can external information support their activities?
- How should the intelligence be presented to make it understandable and actionable for each stakeholder?
- How often should we provide updates and other information?
- Through what media should the intelligence be disseminated?
- How should we follow-up if they have questions?

CTI Lifecycle - Feedback and Evaluation

Feedback is challenging and critical to the success of any CTI program

- Establish processes for receiving feedback from stakeholders
- Enable the CTI team to evaluate the effectiveness of outcomes



CTI Lifecycle - Maturity Matrix

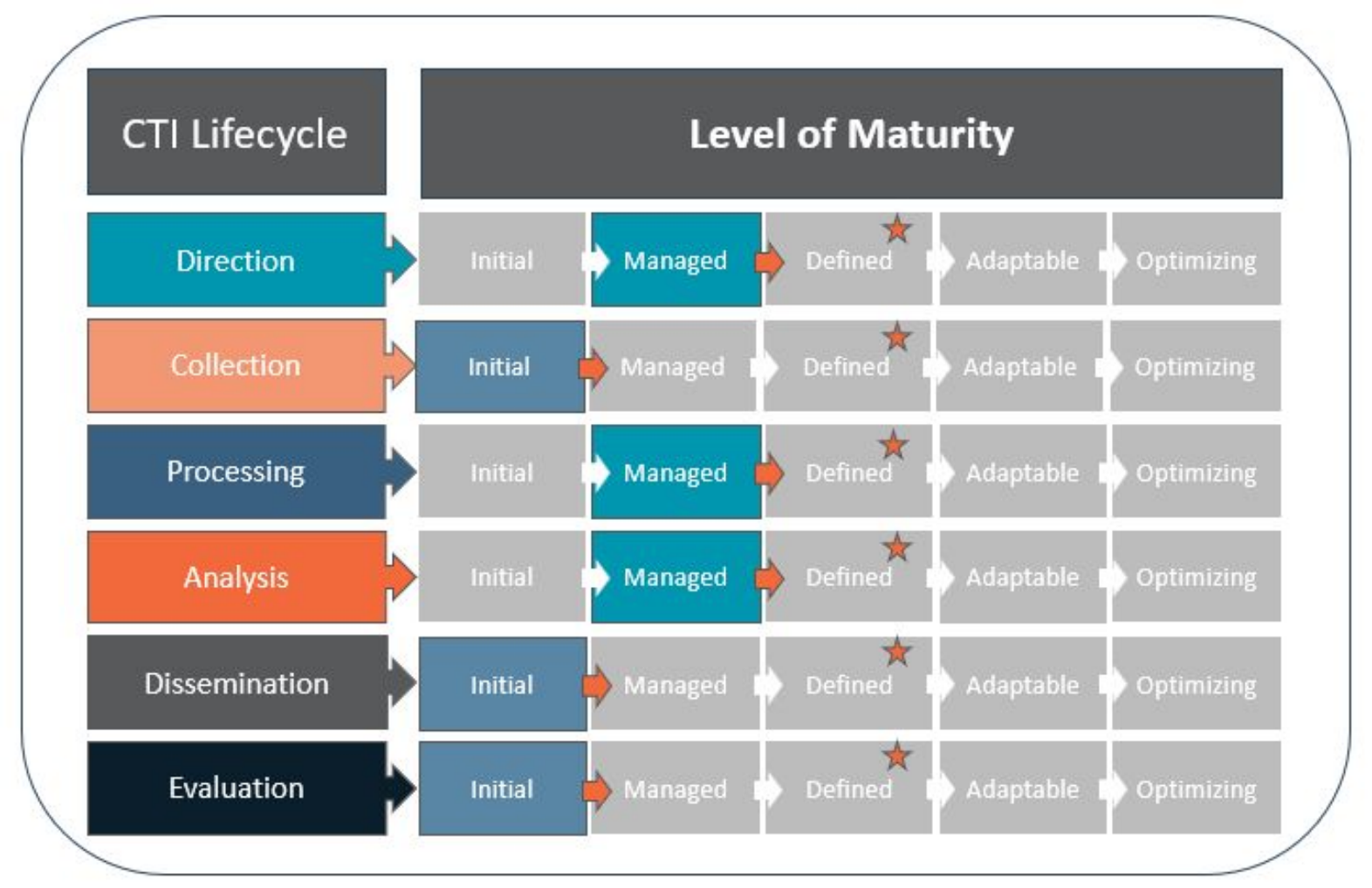


Figure: CTI Maturity Matrix, Clay Wells, Security Risk Advisors

Collection Management Framework

Collection Management Framework

Malware Data Sources - External

Source	First Seen	Last Seen	IPs	Domains	RDNS	SHA256
VirusTotal	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
Hybrid Analysis	**Y**	**Y**	**Y**	**Y**	**-**	**Y**
Any.run	**-**	**-**	**Y**	**Y**	**-**	**Y**
Joes	**-**	**-**	**Y**	**Y**	**-**	**Y**
Count	*2 of 4*	*2 of 4*	*4 of 4*	*4 of 4*	*1 of 4*	*4 of 4*

Collection Management Framework

Malware Data Sources - Internal

	Endpoint Protection	Windows System	Network	Firewall
Data Type	System Alert	Host-based Logs	Netflow	System Alert
Killchain Coverage	Exploitation and Installation	Exploitation, Installation, Actions on Objectives	Internal Recon, Delivery, C2	Internal Recon, Delivery, C2
Follow on Collection	Malware Sample	Files and Timelines	Packet Capture	Netflow
Storage (Days)	30	90	30	60

Thank you

Join the conversation

https://discord.blueteamvillage.org