Defining CTI

By Wade Wells
WadingThruLogs

Section Goal

- Defining Threat intel/Cyber threat intel and its attributes
- What it can be used for
- Tell a story
- Types of intel

Quick Overview

1. What is intel?
2. Types of intel
3. Intelligence life cycle
4. Priority intel Requirements
5. Knowing your consumer
6. CTI for different departments.

What is Intelligence?

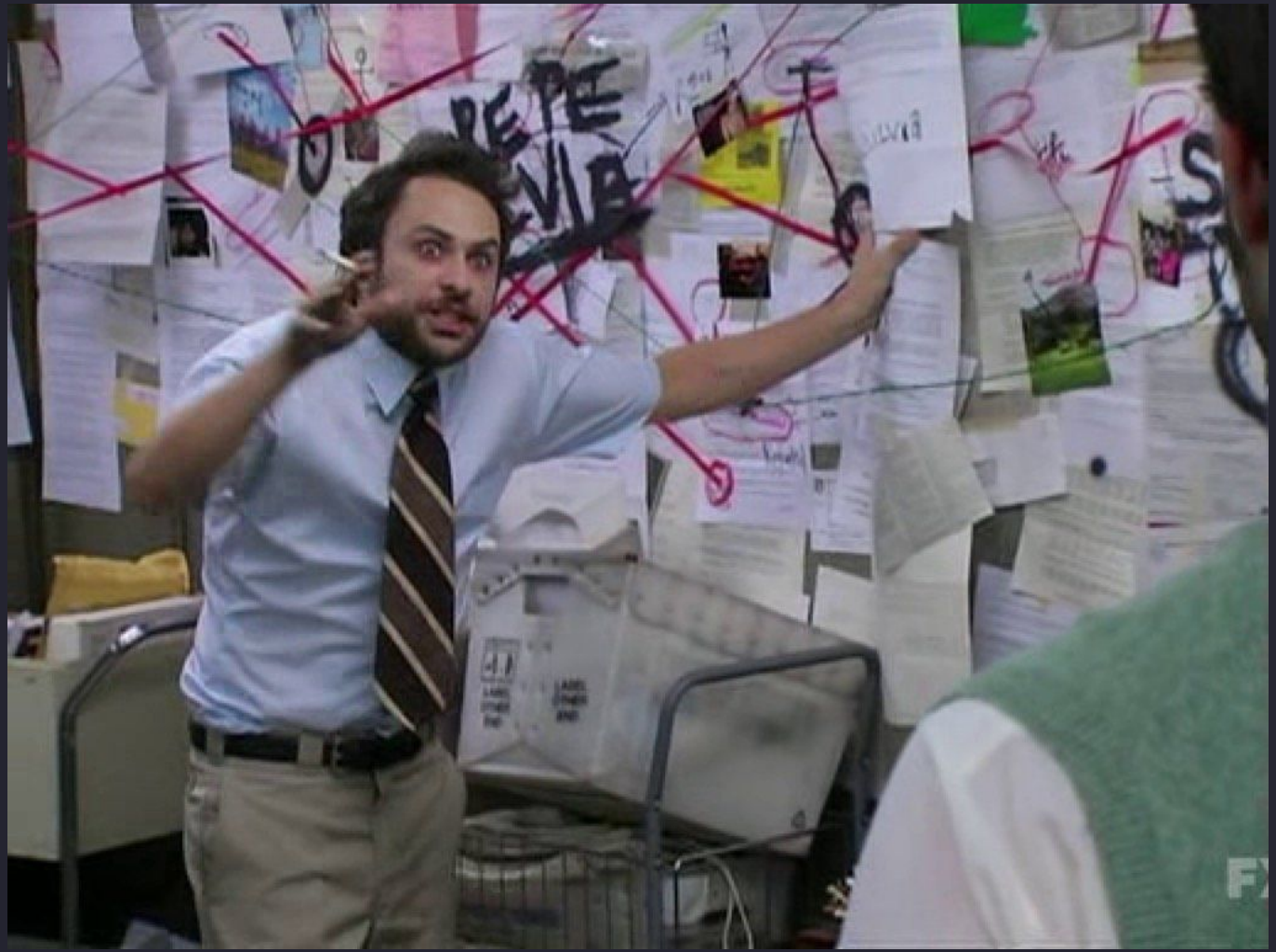
1. " It is data and information that is collected, processed, and analyzed in order to determine a threat actor's motives, intents, and capabilities; all with the objective of focusing on an event or trends to better inform and create an advantage for defenders.” - Kyle Wilhoit | joseph Opacki

2. "Intel [is] threat indicators that have been determined to have value by being relevant and useful to the consuming organization." - Bimfort, 1995

3. “Analyzed information that supports a decision.” - Katie Nickles, 2022

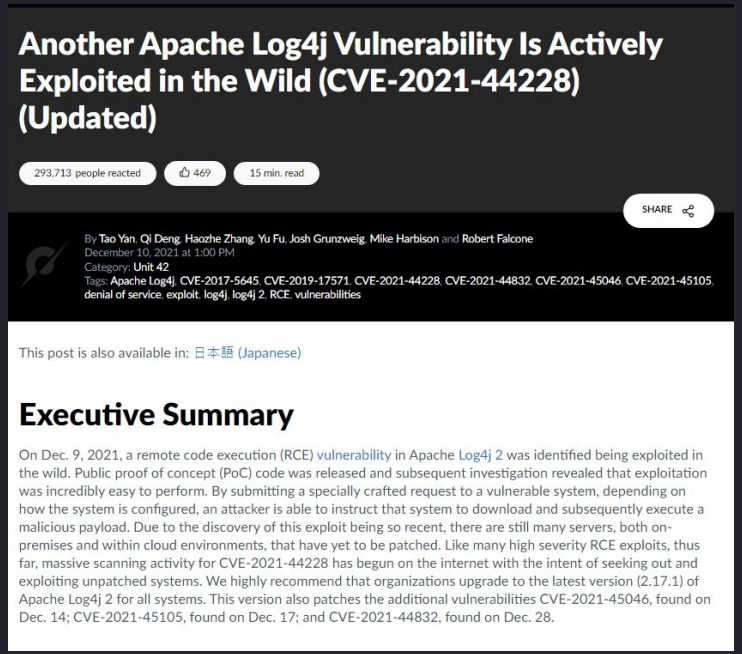
4. Threat Intelligence is actionable knowledge and insight(as well as the process of doing it) on adversaries and their malicious activities enabling defenders and their organizations to reduce harm through better security decision-making - Sergio Caltagirone

https://www.cia.gov/static/554d7d05a62d7d6de84b5b84ae6702ae/A-Definition-Of-Intelligence.pdf


FX

How CTI can help

NEWS



Another Apache Log4j Vulnerability Is Actively Exploited in the Wild (CVE-2021-44228) (Updated)

293,713 people reacted | 469 | 15 min. read

SHARE

By Tao Yan, Qi Deng, Haozhe Zhang, Yu Fu, Josh Grunzweig, Mike Harbison and Robert Falcone
December 10, 2021 at 1:00 PM
Category: Unit 42
Tags: Apache Log4j, CVE-2017-5645, CVE-2019-17571, CVE-2021-44228, CVE-2021-44832, CVE-2021-45046, CVE-2021-45105, denial of service, exploit, log4j, log4j 2, RCE, vulnerabilities

This post is also available in: 日本語 (Japanese)

Executive Summary

On Dec. 9, 2021, a remote code execution (RCE) vulnerability in Apache Log4j 2 was identified being exploited in the wild. Public proof of concept (PoC) code was released and subsequent investigation revealed that exploitation was incredibly easy to perform. By submitting a specially crafted request to a vulnerable system, depending on how the system is configured, an attacker is able to instruct that system to download and subsequently execute a malicious payload. Due to the discovery of this exploit being so recent, there are still many servers, both on-premises and within cloud environments, that have yet to be patched. Like many high severity RCE exploits, thus far, massive scanning activity for CVE-2021-44228 has begun on the internet with the intent of seeking out and exploiting unpatched systems. We highly recommend that organizations upgrade to the latest version (2.17.1) of Apache Log4j 2 for all systems. This version also patches the additional vulnerabilities CVE-2021-45046, found on Dec. 14; CVE-2021-45105, found on Dec. 17; and CVE-2021-44832, found on Dec. 28.

THREAT RESEARCH

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

FIREEYE

DEC 13, 2020 | 17 MIN READ | LAST UPDATED: MAY 10, 2022

#THREAT RESEARCH

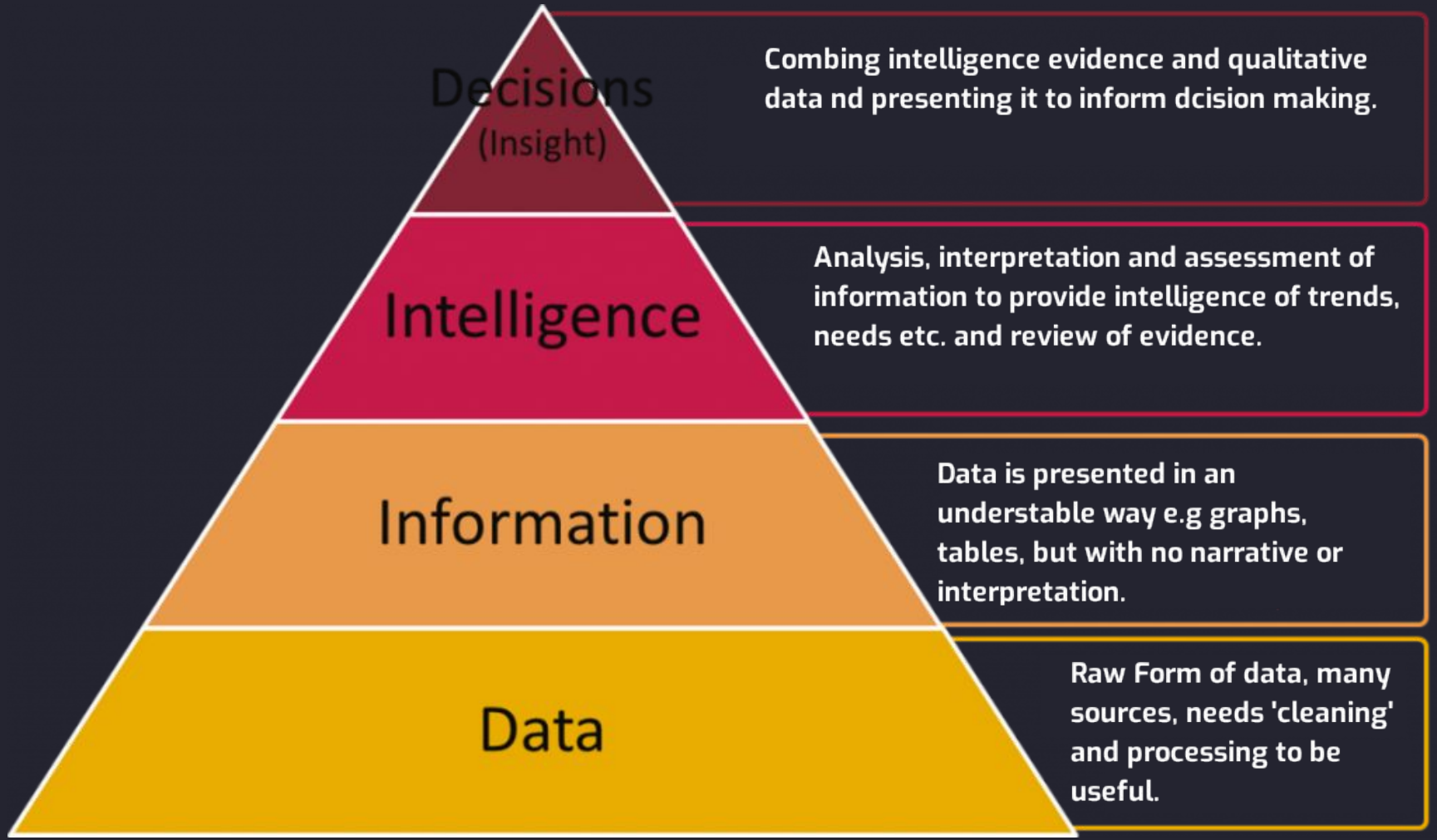
A.R.T.

- **Accuracy:** Is the intelligence reliable and detailed?
- **Relevance:** Does intelligence apply to your business or industry?
- **Timeliness:** Is the intelligence being received with enough time to do something?

Data > Information > Intelligence

- **Data** consists of discrete facts and statistics gather as the basis for further analysis
- **Information** is comprised of multiple data points that are combined to answer specific questions
- **Intelligence** is the output of an analysis of data and information that uncovers patterns and provides vital contact to information decision-making.

- *Data Example*: Domain
- *Information Example:* Domain hosting malware
- *Intelligence Example:* Domain hosting malware that your organization visits frequently.



https://ukhsa.blog.gov.uk/2018/12/05/from-data-to-decisions-building-blocks-for-population-health-intelligence-systems/

Tell a Story

- Not always viable
- Narratives and Hooks
- Know your audience
- Stay away from FUD

Types of intel

Strategic

Operational

Technical

Tactical

Strategic

Intel related to the risk of the organization. Given to or used by decision-makers and usually less technical.

Examples:

- Intel Reports
- Threat Briefings
- Executive Summaries

Made From:

- Government policy
- Local or national news sources
- Industry reporting
- Social media

Operational

Focuses mainly on how and when a threat actor is going to attack a company. Information on the intent behind the attack.

Examples:

- Possible CISA reports

Made From Scraping :

- Forums
- Chats
- Message board
- Darkwebs
- Agencies...

Technical

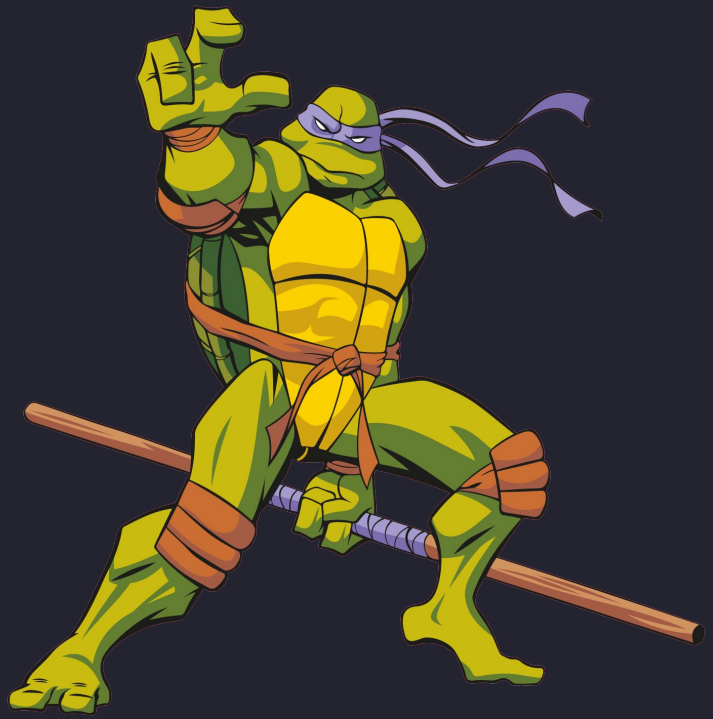
Relies on atomic indicators or IoC not TTPs.
Looking for C2, email address or artifacts.
Should be mostly automated.

Example Data:

- IPs
- Hashs
- Domains
- Emails:

Made with:

- Threat Feeds
- Badly written reports



Tactical

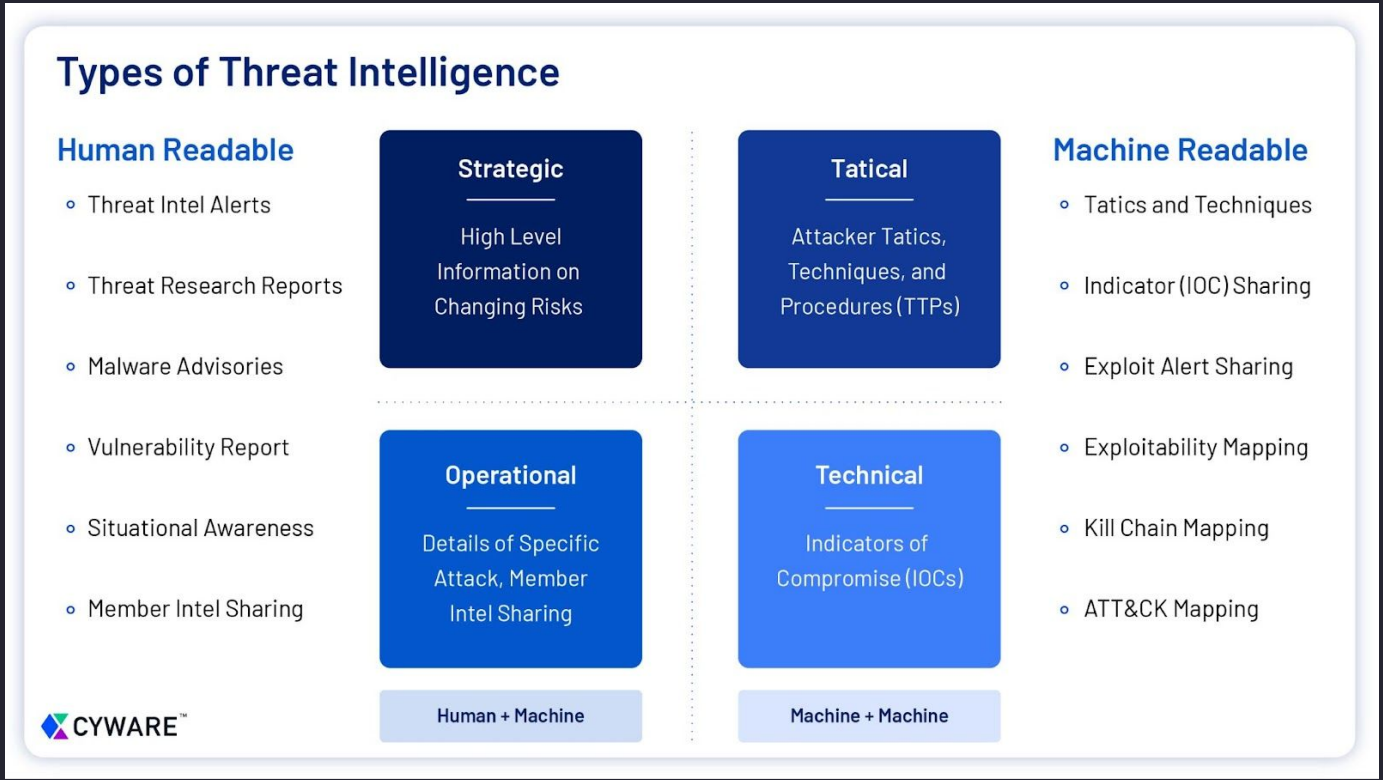
Info related to that tactics, techniques and procedures used by threat actors to achieve their objectives. Usually used by Defense teams to build detections and preventions.

Examples:

- Threat reports,
- campaign activity
- infection vector
- Infrastructure used by attacker
- TTP of Threat actor.

Made From:

- Malware analysis
- Intel companies
- Cyber Vendors



https://cyware.com/educational-guides/cyber-threat-intelligence