ISF 2023 – Open-Source Threat Intelligence

How to Eat the OSINT Elephant

DIR Cybersecurity Operations

March 2023

Texas Department of Information Resources

Transforming How
Texas Government
Serves Texans

dir.texas.gov | @TexasDIR | #DIRisIT

Open-Source Threat Intelligence (OSINT)

OSINT is a process designed to gather and analyze information from public sources. For example, these sources may be government databases, websites, or brochures. The resulting intelligence is shared often in the form of a “feed”.

Challenges using Open-Source Threat Intelligence

Trust is the cornerstone of threat intelligence.

Who wants information that can't be trusted?

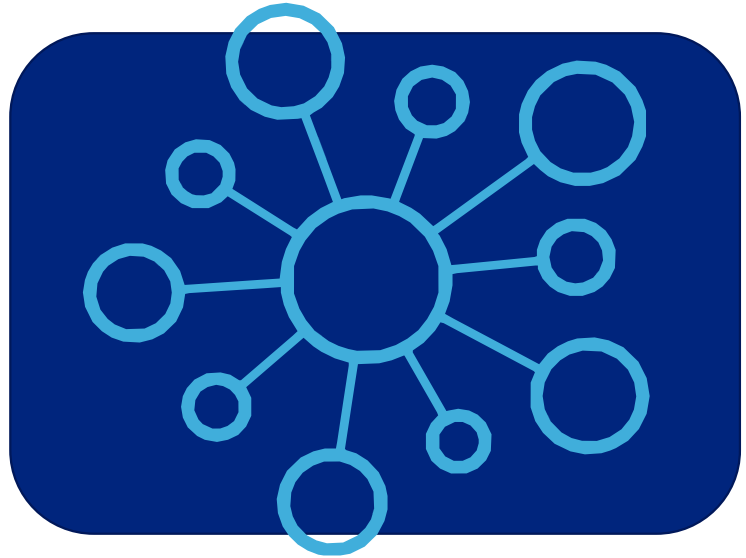
Intelligence from an untrustworthy source isn’t actionable. It is important that the producer and consumer trust each other. That trust needs to be based on transparency and verification.

DIR

Three qualities to look for in a threat intel feed:

Accuracy

Timeliness



Relevance

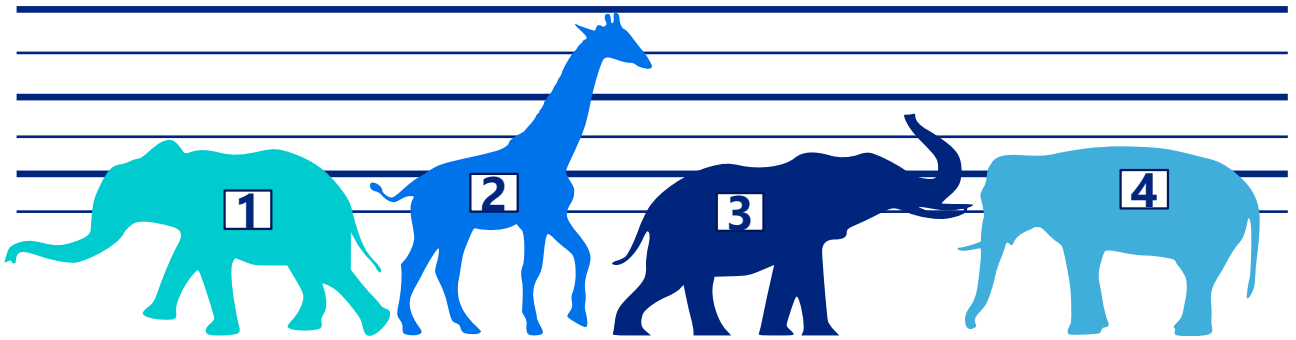
DHS Automated IOC Exchange Pilot

DIR CyberOps worked with Johns Hopkins University-Applied Physics Lab and MS-ISAC along with several other states to ingest an automated feed of analyst-vetted Indicators Of Compromise (IOCs). Metrics were kept to measure the effectiveness of the rapid exchange of IOCs.

- **CyberOps received 700 indicators over a 60-day period.**
- **CyberOps only removed one indicator for business impact.**
- **70 indicators were newly seen in our environment within 24 hours of getting the intelligence (Relevance and Timeliness).**

*Feed went down December 2020.

Threat Intelligence Platform (TIP)



A TIP is an automated tool that is used to ingest and analyze intelligence, share intelligence with others, and usually, push the trusted intelligence directly to security tools. This is the tool CyberOps uses to eat our elephant.

Two key factors to a successful TIP operation:

- **High confidence.**
- **Low regret.**

TIP Ingests Multiple OSINT Data Sources

- Previous reports of malicious behavior
- ASN
- Geolocation
- Open ports
- Number of domains that resolve to the address
- Previous reports of malicious behavior
- Protocol (http/https)
- Entropy of domain/URL
- SSL certificates
- Domain registration date
- Domain popularity and ranking
- Domain DNS activity

DIR

Identifying confident threat feeds:

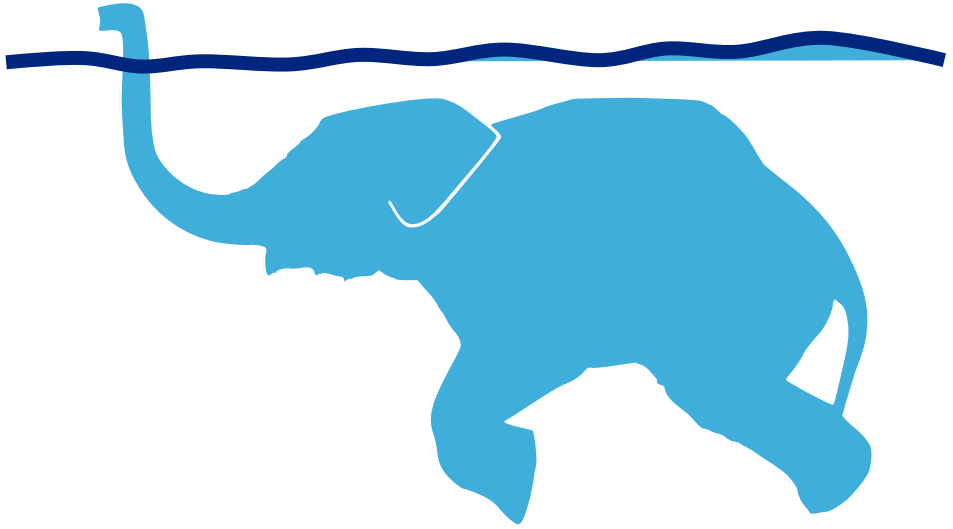
- Evaluate the feed reputation using TIP and OSINT.
- Compare false positive rating from the TIP.
- Evaluate the false positive percent. Preferably below 9%.
- Monitor the false positive rating over the last three months, comparing month to month.
- Monitor overlap with other feeds.
  - Which feed gets the info first?
  - How many of the IOCs are unique to that feed?
  - How many blocks or detections do they generate and are they of value?

    Should it generate blocks? For example, a feed of ransomware delivery servers would hopefully have a very few blocks compared to a feed of recon scanners.

Deeper into false positive

Indicators from the same feed from different months:

42,727 indicators.
5,470 false positive.
13% false positive percent.



342,027 indicators.
4,187 false positive count.
1% false positive percent.

It is important to note that a high false positive percent doesn't mean there's not value in the list. We are initially identifying feeds that have a low false positive count.

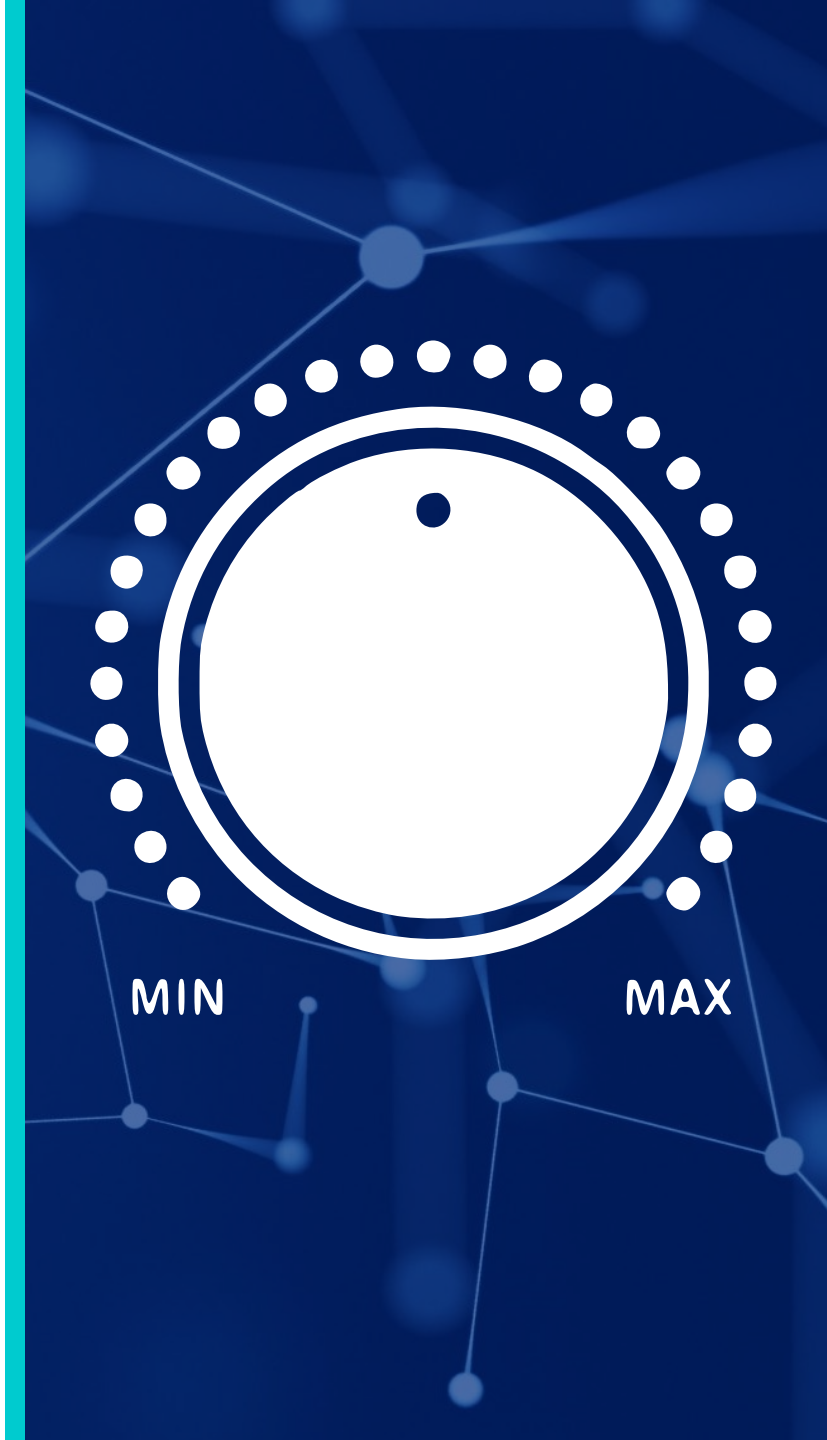
DIR

Tuning based on confidence.

As the confidence is adjusted, you'll see the indicator count change. 100% confidence indicates soaring probability of maliciousness.

16,235 indicators at 100%
42,020 indicators at 90%
55,353 indicators at 75%
76,307 indicators at 50%
86,240 indicators at 25%
92,708 indicators at 0%

Lower confidence blocks can result in business impact or regret.



Low Regret versus High Regret Blocks

Low regret:

- Single IP that shows bad
- Small domain/URL
- Small Classless Inter-Domain Routing (CIDR)
- Single Point Content Delivery Networks (CDN) – This is a very small CDN used for marketing.

High regret:

- Whole CDNs
- Geolocations
- Large IP address ranges/CIDRs
- Microsoft/Google/AWS, any of the large hosting organizations.
- Any State of Texas-owned network address, or cloud domains.

Identifying confident threat feeds:

The amount of Content Delivery Network (CDN) traffic coming to/from state agencies is skyrocketing, so blocking these can have unintended consequences.

Often the approach is to block access to an IP address where the malicious domain is located, but this IP address is shared with many legitimate domains. Blocking access to this CND IP address blocks access to all the businesses there.

For example, with US Postal mail delivery, if that address is a skyscraper with its many unrelated and independent occupants, halting the delivery of mail to the address of the skyscraper causes collateral damage affecting all the parties at that address.

DIR

Manual vetting process

This is the longest part of the process:

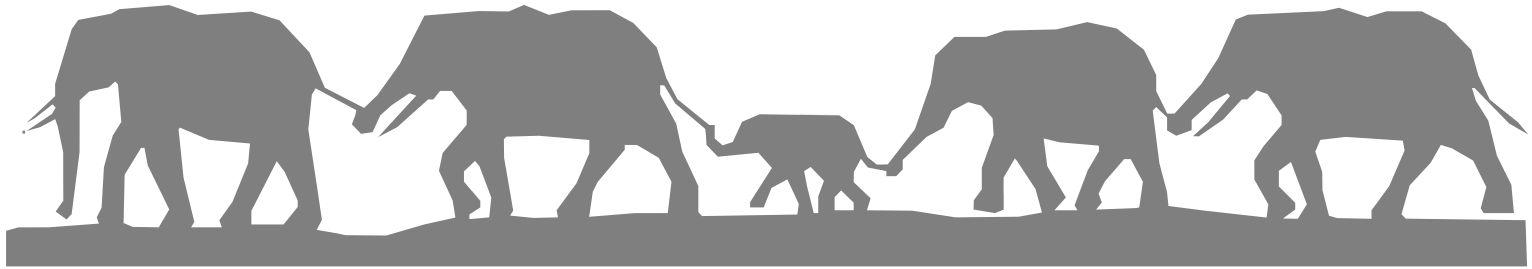
- We manually sample 1-2% of the indicators.
- Once vetted, we begin pushing a subset of indicators to our toolset.
- The first push: all indicators with 24 hours that have over a 50% confidence rating are tested for seven days before we move to automation.
- Scrutinize indicators that have a confidence below 50%.
- Tuning: we push indicators 50%-25% for a week looking for regret.
- Most indicators have a Time to Live of 90 days.

DIR

Curating feeds for agency's needs

Choose feeds based on what you are doing. Focus on threat feeds that represent your entity's relevant business sector.

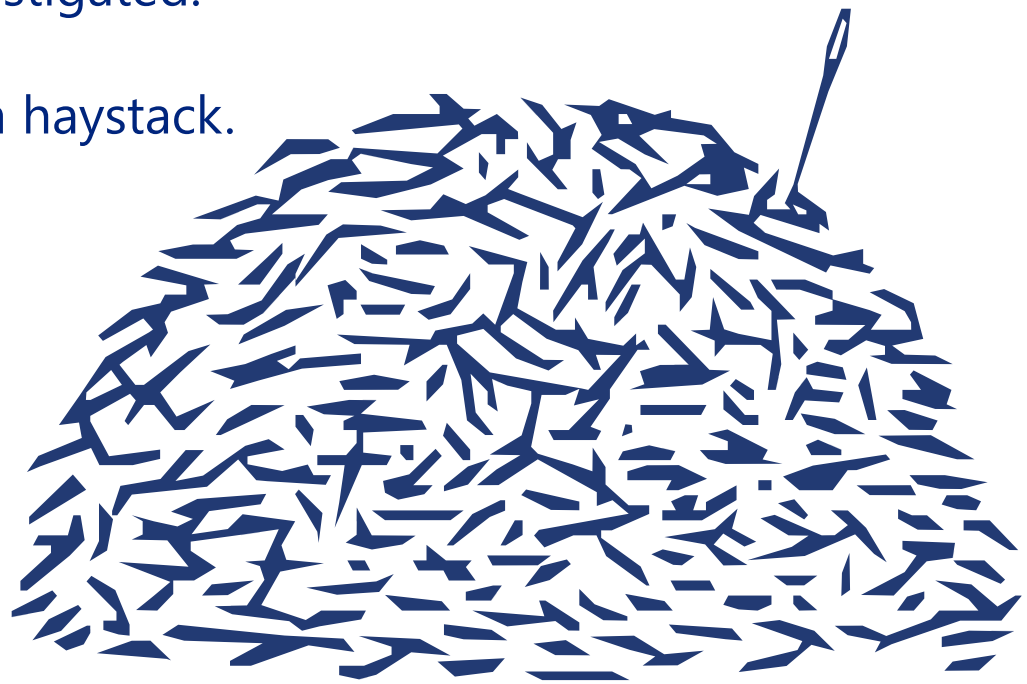
- Technology
- Government
- Education
- Health
- Energy
- Transportation
- Finance/Banking



Reducing Noise – A huge benefit

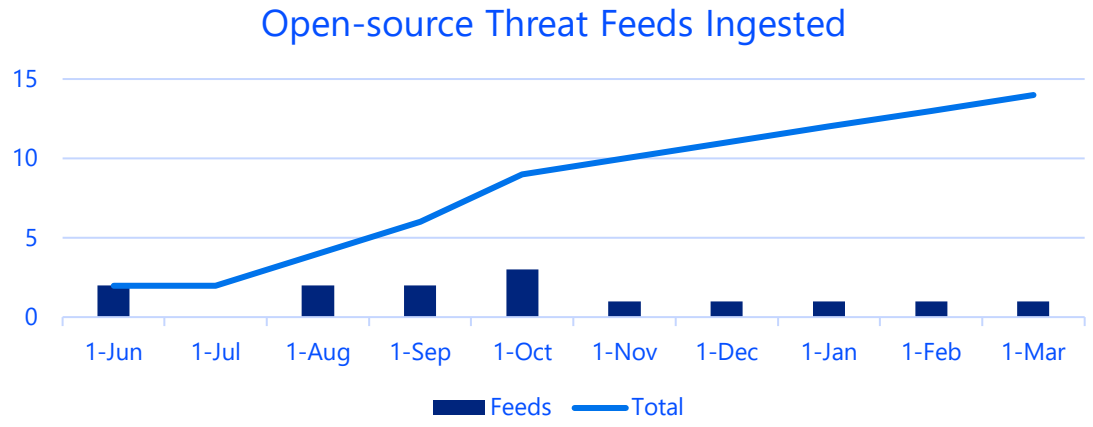
By properly using the intelligence in your threat feeds and your TIP, you will start to block a lot of the noise that is in your security tools.

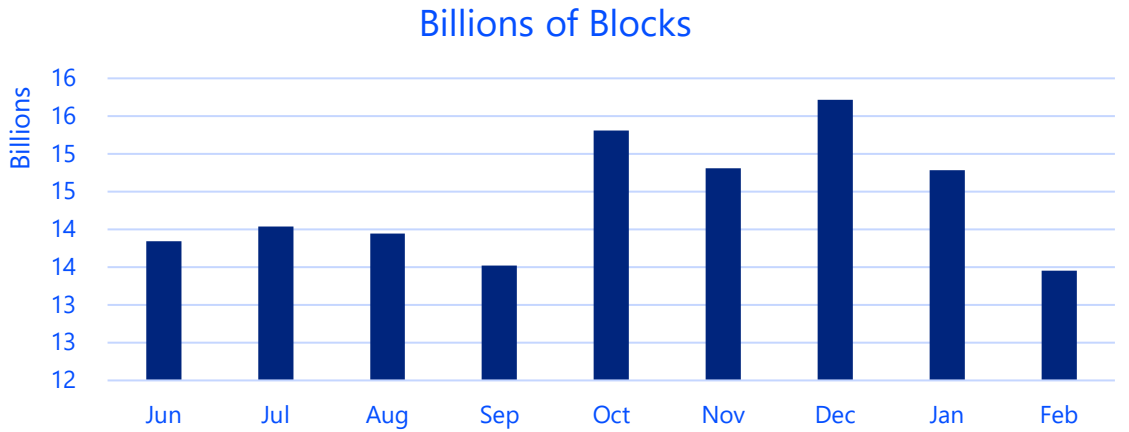
- A trusted feed will reduce alerts that must be investigated.
- Known scanners are blocked, reducing alerts.
- Miscreants want their activities to be a needle in a haystack.
- So, they throw a lot of hay on the haystack.
- Use OSINT and a TIP to reduce their hay

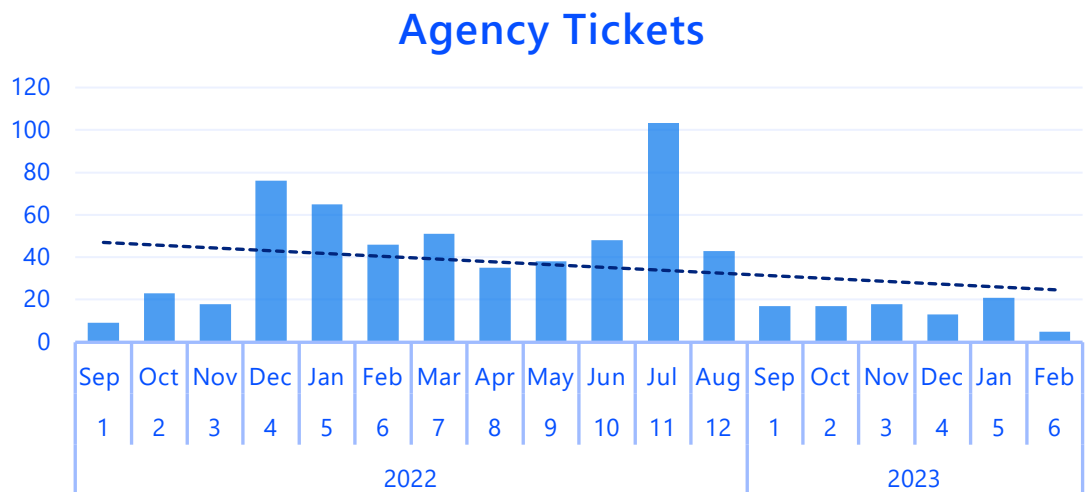


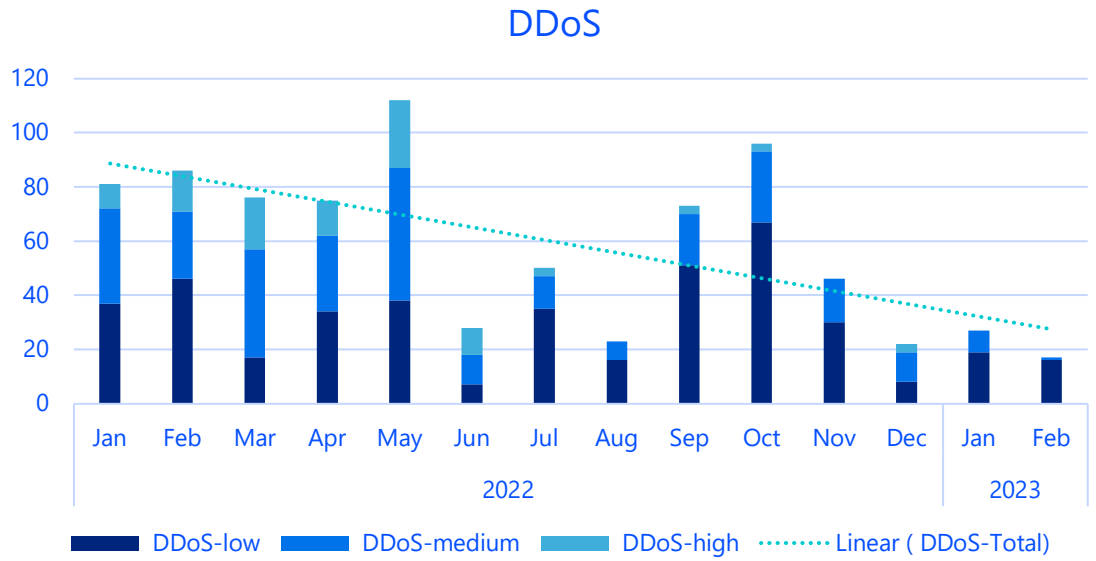
DIR

Difficult to measure effectiveness / Trends







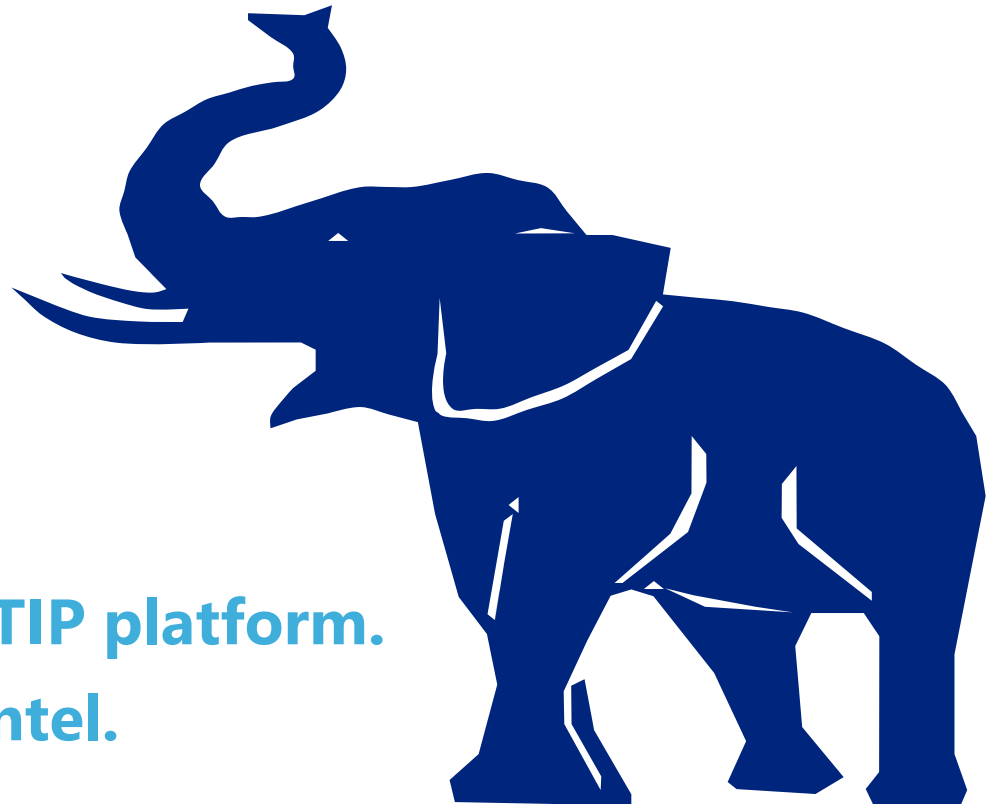


CyberOps is eating our elephant

DIR CyberOps has ingested over three million indicators since June with **NO** block removal or whitelist requests for any OSINT threat feed indicator ingested at our confidence level.

CyberOps TIP/OSINT Roadmap

- More automation.
- Fine TUNING existing feeds.
- Track the count of blocks per feed.
- Visibility into duplication rate in feeds.
- Ingest additional OSINT feeds outside TIP platform.
- Increase depth and breadth of OSINT Intel.



DIR

Resources

NIXSPAM – blocklist used to protect mailservers against spam.
https://www.nixspam.net/download/nixspam-ip.dump.gz
URLhaus – Sharing malicious URLS that are being used for malware distribution.
https://urlhaus.abuse.ch/downloads/
Malware Bazaar Database – collect of malware hashes
https://bazaar.abuse.ch/verify-ua/
Open Phish Feed –threat intelligence feeds make up a constantly updated database of patterns that match the URLs and email addresses recorded by Netcraft.
https://openphish.com/feed.txt
CINS Score –reputation data from CINS threat intelligence gateways.
http://cinsscore.com/list/ci-badguys.txt
Blocklist Apache Attacks - free service provided by a Fraud/Abuse-specialist.
http://www.blocklist.de/lists/apache.txt
TOR Exit Nodes - last Tor node before exiting onto the internet.
https://www.dan.me.uk/torlist/

Resources

Openphish
https://openphish.com/feed.txt
Snort IP BlockList -Snort Labs IP Reputation
https://snort.org/downloads/ip-block-list
Greensnow
https://blocklist.greensnow.co/greensnow.txt
SANS Internet Storm Center
https://www.dshield.org/api/
Proofpoint Emerging Threats
https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Ant-Bot List
https://www.botvrij.eu/
PhishStats – Phishscore
https://phishstats.info/phish_score.csv

Thank You

DIR Cybersecurity Operations

Email: security-alerts@dir.texas.gov

After Hours On-Call Analysts:

DIR Cyber Operations (24/7) 800.969.6470

DIR Escalation (24/7) 512.701.7152

Texas Department of Information Resources

Transforming How Texas Government Serves Texans