



Pulsedive

The State of CTI

(Cyber Threat Intelligence)

March 25, 2021

© 2021 Pulsedive LLC

Hello!



Grace Chi
Cofounder & COO

Dan Sherry
Founder & CEO



Delivering high-fidelity cyber threat intelligence to help communities and organizations worldwide proactively improve their security posture.

Founded
2017

Located
New Jersey

Recommended by
Fortune 500
Big 4 Consulting
SANS Institute





Community-Driven Platform + Data

pulsedive.com

- Overview
- Screenshot
- Attributes
- Threats
- Feeds
- Comments

Properties

- cookies
- dns
- dom
- geo
- http
- meta
- ssl
- whois

Integrations

- VirusTotal
- Shodan
- AbuseIPDB

Linked Indicators

- DNS
- Mail Servers
- Name Servers
- Redirects
- Related URLs
- Sources

Copy Summary Seen Rescan Comment Edit Retire API

pulsedive.com

Pulsedive is a free threat intelligence platform that leverages open-source threat intelligence (OSINT) feeds and user submissions to deliver actionable intelligence.

200 OK
Very low risk
SPF record present
Registration details hidden

text/html

Redirects to: <https://pulsedive.com/>

SSL certificate found: pulsedive.com and 1 more

WHOIS privacy

hostmaster@pulsedive.com

Registrar: Google LLC

Apache, Google Analytics

Jump to integration: [VirusTotal](#) [Shodan](#) [AbuseIPDB](#)

Events

Registered	2016-11-10 00:00:00 4 years ago
Updated	2019-12-27 00:00:00 11 months ago
Cert. issued	2020-10-29 14:02:33 1 week ago
Added	2020-11-03 06:13:49 6 days ago
Scanned	2020-11-03 06:14:04 6 days ago
Updated	2020-11-03 06:14:07 6 days ago
Seen	2020-11-03 06:14:07 6 days ago
Expires	2020-11-10 00:00:00 1 day from now
Cert. expires	2021-01-27 13:02:33 2 months from now

Screenshot

2020-11-03 11:14:05

Click the image to expand and minimize.

Threat intelligence

Comment Edit Retire API

Phishing

General
Unknown risk
14648 indicators

Events

Added	2020-11-05 02:11:06 4 days ago
Seen	2020-11-09 02:38:43 16 hours ago
Updated	2020-11-09 02:39:45 16 hours ago

W Summary Source

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing, instant messaging, and text messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site. Phishing is an example of social engineering techniques used to deceive users. Users are lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, colleagues/executives, online payment processors or IT administrators. Attempts to deal with phishing incidents include legislation, user training, public awareness, and technical security measures (the latter being due to phishing attacks frequently exploiting weaknesses in current web security). The word is created as a homophone and a sensational spelling of fishing, influenced by phreaking.

github

All Images Videos News Maps Settings

All Regions Safe Search: Moderate Any Time

CI for GitHub - Build Test and Deploy

circleci.com Report

Start Building and Testing in seconds. Free Sign Up with GitHub

Create a config.yml in your project's root directory and CircleCI will read it each ...

CI for Mobile & Web Apps · Support from Engineers

The world's leading software development platform · GitHub

https://github.com

GitHub brings together the world's largest community of developers to discover, share, and build better software. From open source projects to private team repositories, we're your all-in-one platform for collaborative development.

Recent News

Ask Hackaday: Why Did GitHub Ship All Our Software Off To The

Port

22	443	80
----	-----	----

Protocol

HTTP	HTTPS
SSH	

Technology

Amazon S3	Bootstrap
GitHub Pages	
Google Analytics	
Ruby on Rails	

Available in: English

Founded: February 8

Wikipedia Twitter

API Feed Settings

Used Globally by Pros,
Researchers, Hobbyists

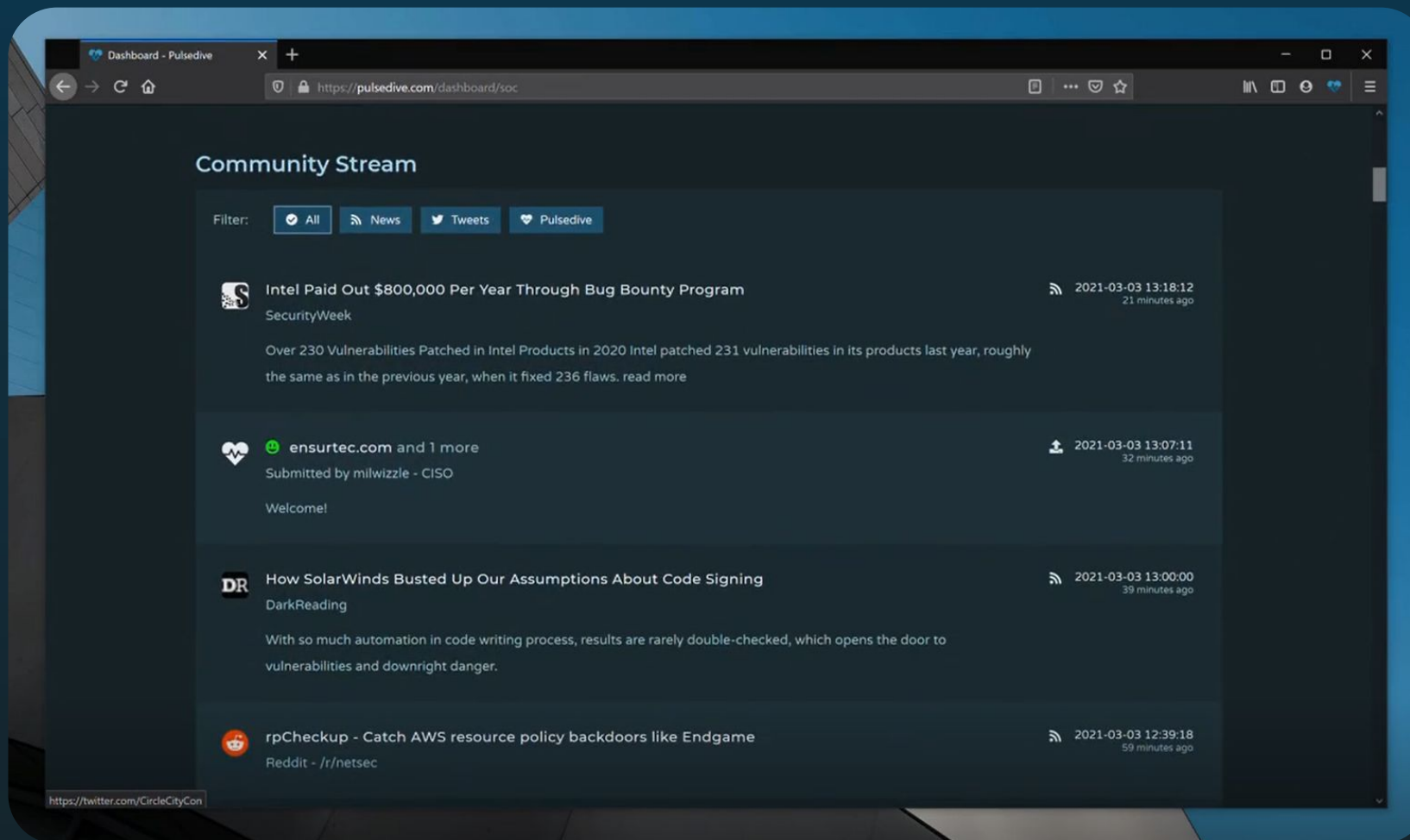




Dashboard: Latest Industry News & Events

pulsedive.com/dashboard

Free access - no account needed



Today

CYBER THREAT INTELLIGENCE (CTI) 101

CTI IN ACTION

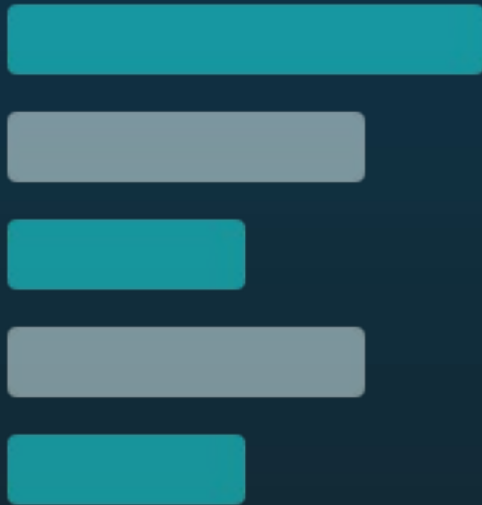
TIPS & RESOURCES



POLL

Audience Snapshot

How involved are you in cyber threat intelligence in your work?



- None
- A little (comes up)
- Moderately (monthly)
- Often (weekly)
- Very often (daily)
- It **IS** my job

Mindmeld

List some keywords related
to the definition of
cyber threat intelligence

Cyber Threat Intelligence

Many Definitions

Evidence-based knowledge, including context, mechanisms, indicators, implications, and action-oriented advice about an existing or emerging menace or hazard to assets.

This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard.

Gartner

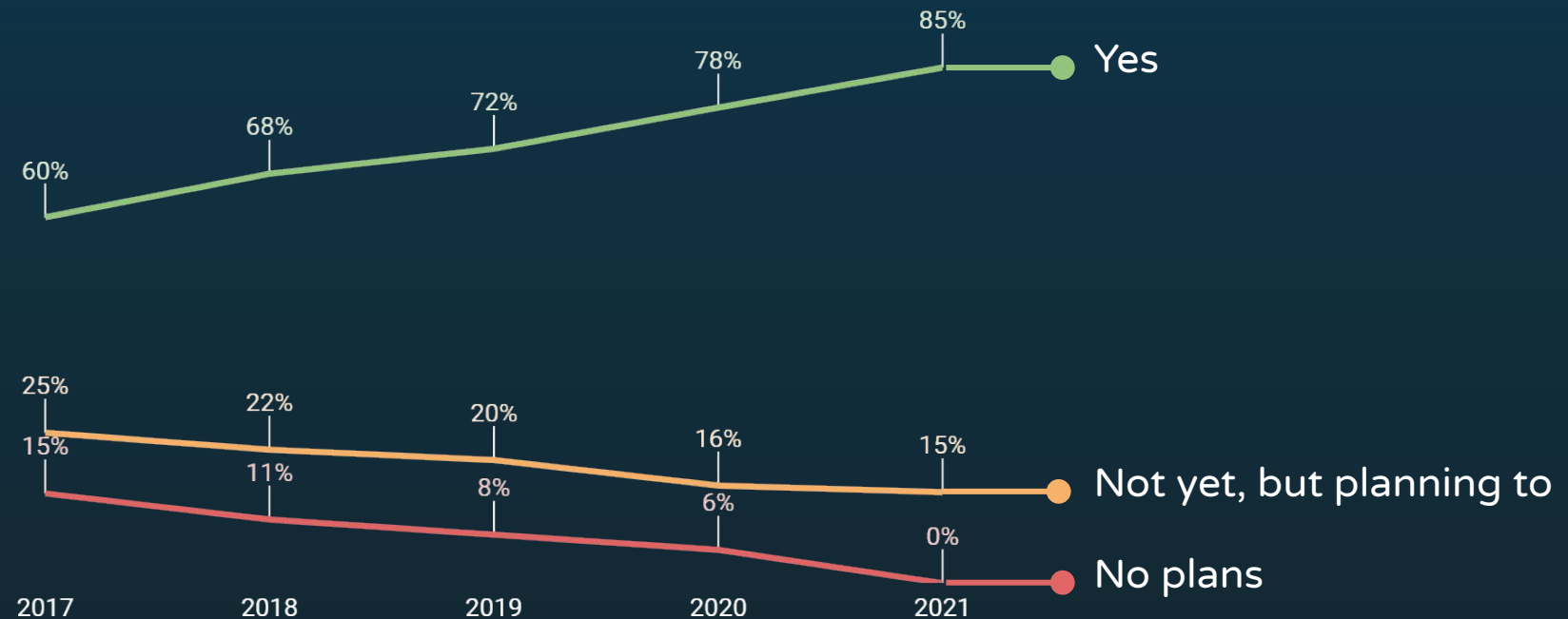
What CTI Isn't

- ✗ A notebook with every threat group or APT
- ✗ Many, expensive feeds and tools
- ✗ A dedicated team member or provider
- ✗ Ingesting every indicator you can find
- ✗ OSINT all the things
- ✗ Set it and forget it

Data. Contextualized. Informing. Action.



Does your organization produce or consume CTI?

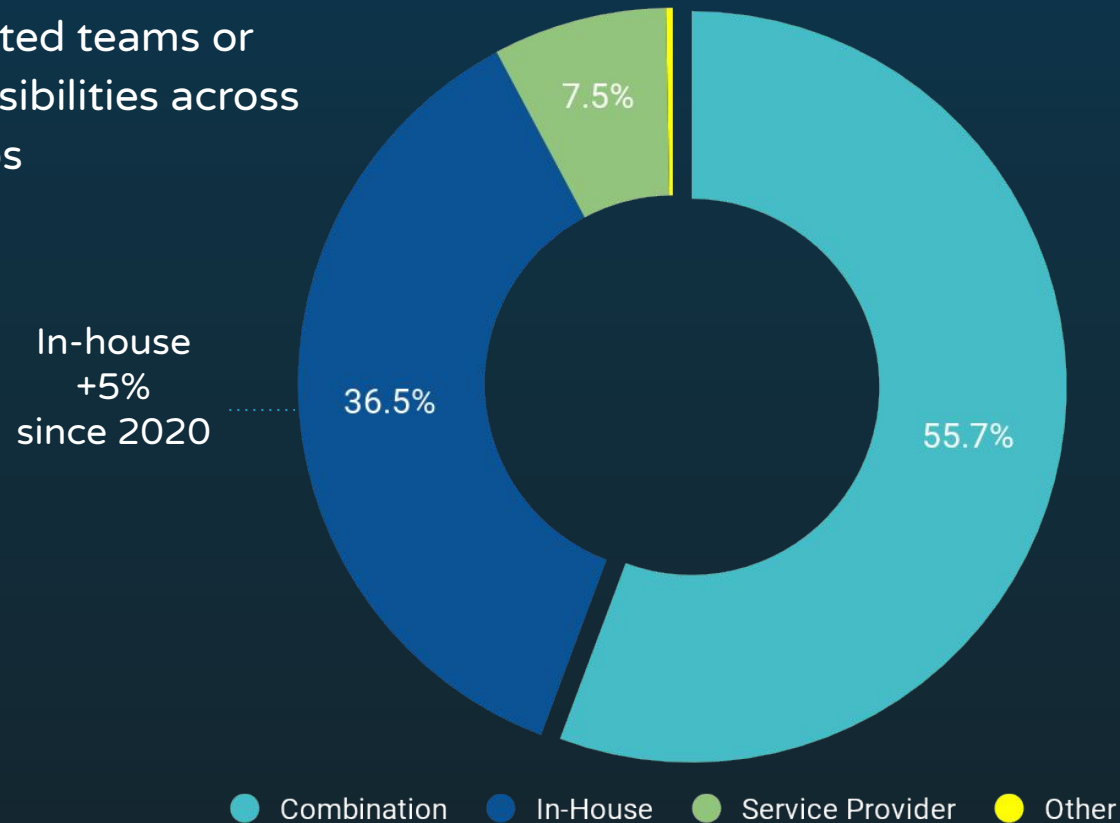


SANS Institute, 2021 CTI Survey



Who & Where?

Most organizations have formal, dedicated teams or shared responsibilities across security groups



Vendors

Products, Startups

Consulting

Professional Services

Government

Military, Federal, Local

Institutional

Academic, Healthcare

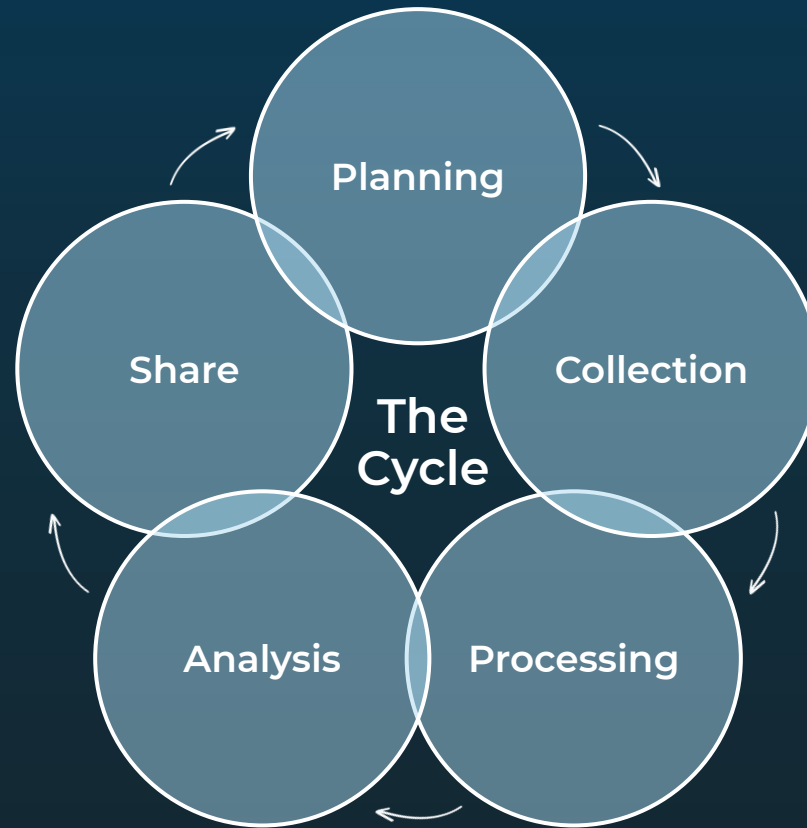
Commercial

Enterprises, Finance, Mfg

SANS Institute, 2021 CTI Survey

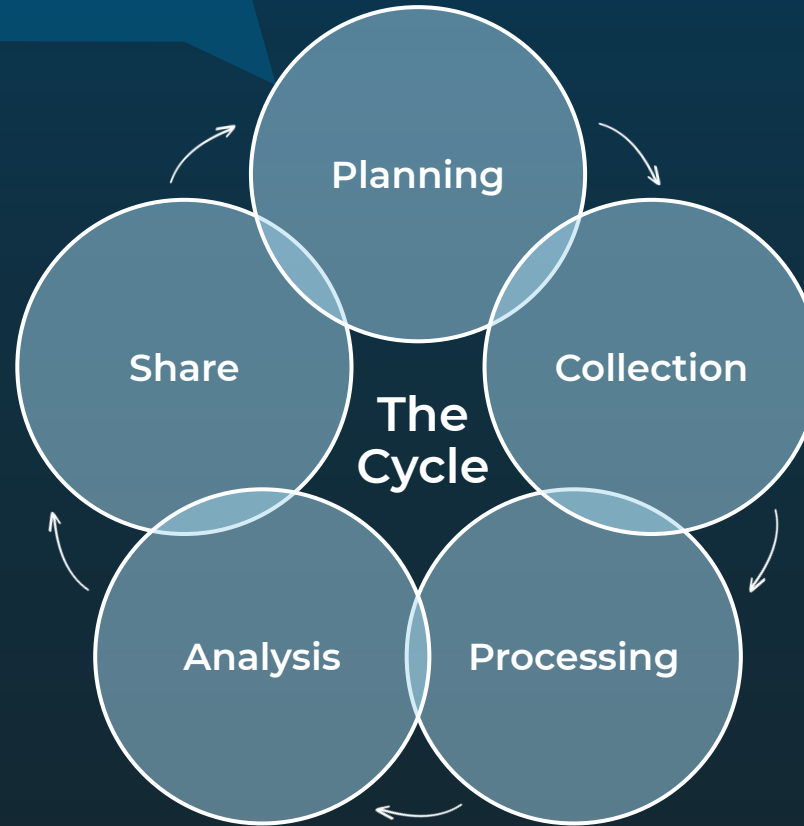


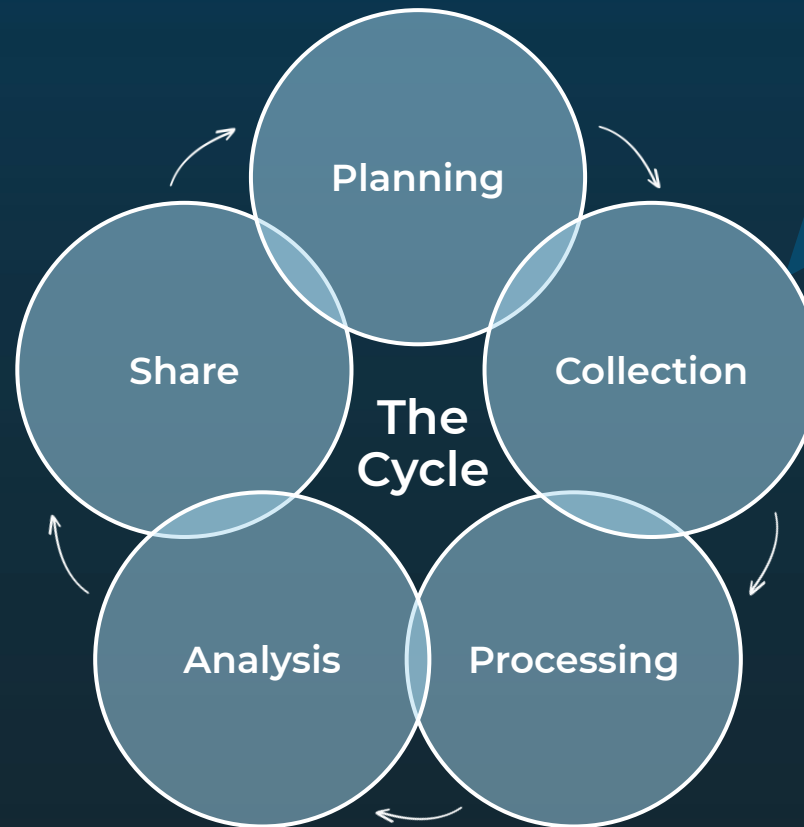
Intelligence Cycle



Requirements Gathering

Set purpose, scope, and priorities
Stakeholder interviews, core objectives,
goals and tasks with defined KPIs
Understand risks, end users/consumers,
operations and capabilities

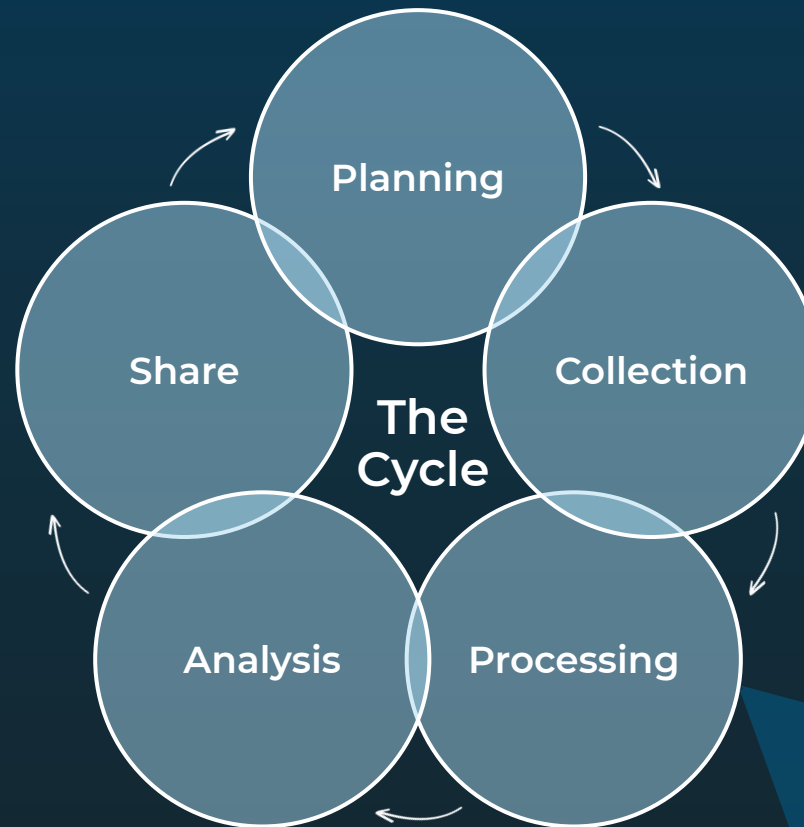




Internal & External Sources

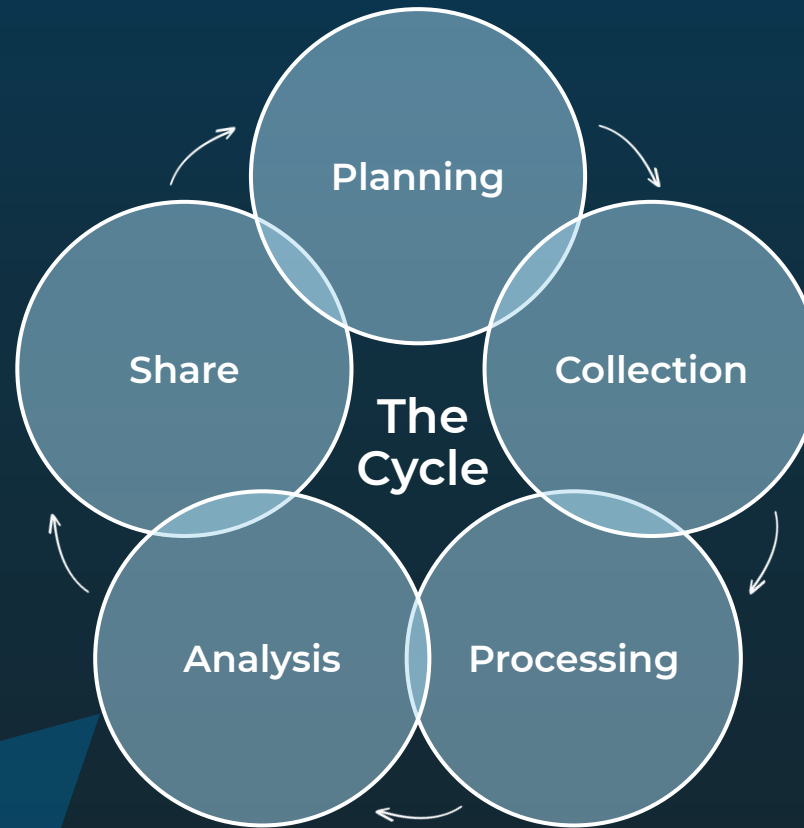
Network logs, past incidents, risk analysis reports

Threat feeds & research, IOCs & TTPs, open and dark web



Enrichment & Contextualization

OSINT engines, scanning, lookups, web tools, footprinting
Counterintelligence, honeypots, sinkholes, YARA rules
Human intelligence, social engineering



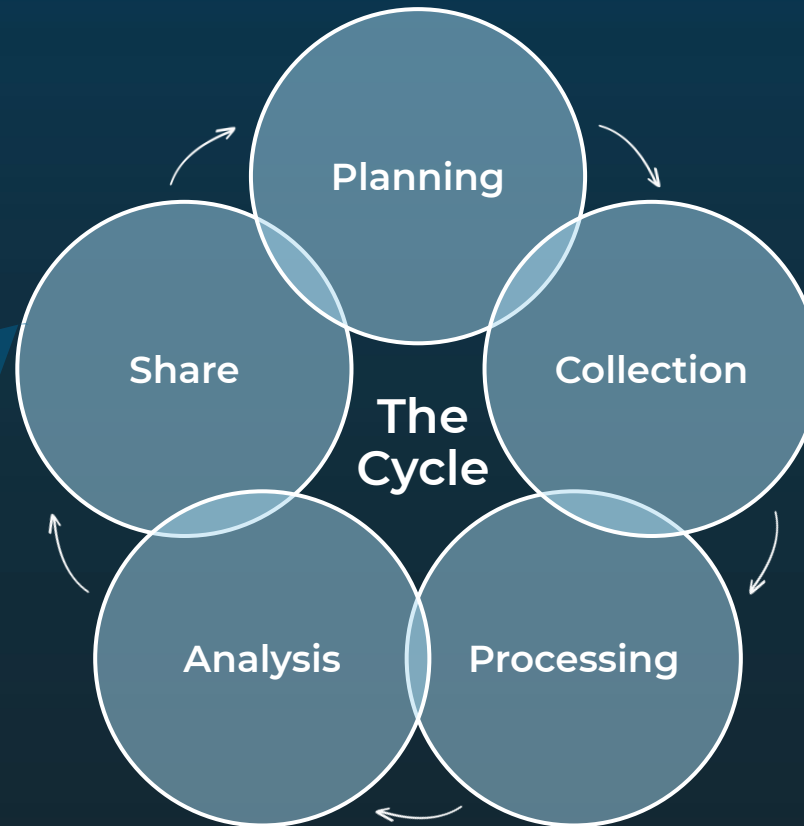
Analysis & Intelligence Creation

Motives, targets, behavior, impact
Actionable reports and informed
narratives to protect orgs, inform
decision-making and next steps

POLL

Dissemination & Feedback

Selective format, output, timeliness, and distribution of intelligence with clear actions/considerations to key stakeholders, plus feedback on deliverables i.e. reports, mailings



LOOKING PHISHY

Processing & Enrichment In Action

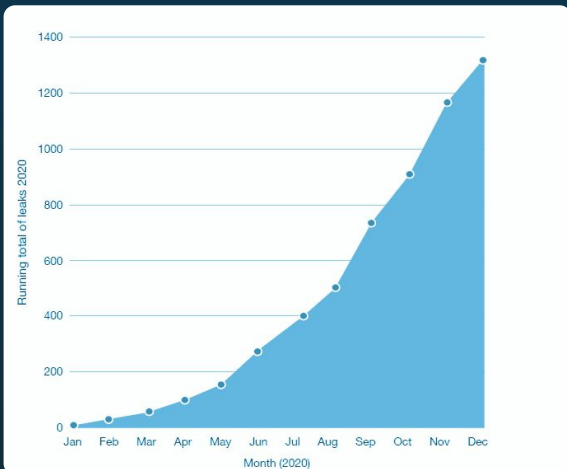
URL
hxxps://touchread-06627287[.]dr9[.]ir/

The screenshot displays the Pulsedive web interface. On the left, a sidebar contains navigation links: Overview, Screenshot, Attributes, Threats, Feeds, and Comments. Below these are sections for Properties (dom, geo, http, meta, ssl, whois), Integrations (VirusTotal, Shodan, AbuseIPDB), and Linked Indicators (Related URLs). The main content area is titled 'Screenshot' and shows a timestamp of '2020-09-25 20:26:16'. It features a 'Report' button and a message: 'Click the image to expand and minimize.' The central image is a screenshot of a Facebook login page. The page has a blue header with the 'facebook' logo. Below the header, a yellow banner reads: 'Dear Facebook user, In order to confirm that you are the owner of the account, you need to login before viewing the next page.' The login form includes fields for 'Mobile Number or Email' and 'Password', a 'Log In' button, and a 'Create New Account' button. At the bottom, there are language options (English (US), Français (France), Português (Brasil), Italiano, Español (ES), Deutsch) and a copyright notice 'Facebook ©2019'. A white arrow points from the URL text to the 'Screenshot' link in the sidebar. Another white arrow points from the 'SCREENSHOT' text to the Facebook login page image.

SCREENSHOT
Facebook
phishing



Trends



Effective campaigns
Double extortion
Hackers for hire
Massive growth

PwC, Cyber Threats 2020: A Year in Retrospect, 2021
ENISA, Threat Landscape Reports, 2020



Why?

The Bottom Line

Understand.
Context & Strategy

Do.
Mitigate, Detect, Protect

Optimize.
Resources, Priorities



Users and Contributors

Ideally across the entire org

Security Operations
CTI Teams
Incident Response
Vulnerability Management
Risk & Compliance
Executives / Leadership
Business Units
Customers and/or End Users
Red Teams
Abuse Research

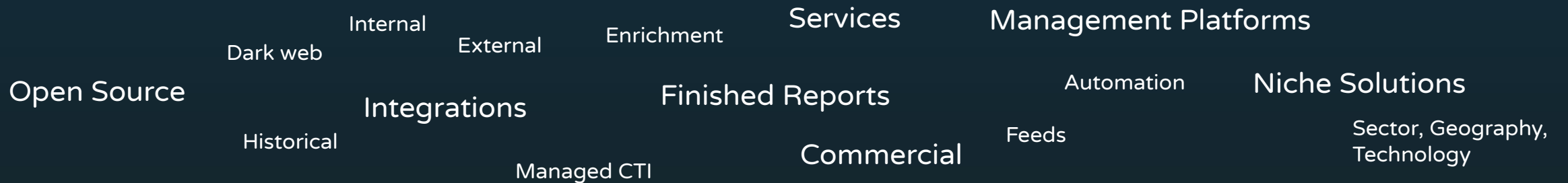


CTI Teams Today

CTI ON A BUDGET



MATURE FUSION CENTERS



Example Flow

Intelligence (Internal & External)

Malicious domains,
IPs, URLs
Vulnerabilities
News & Advisories

TIP

Threat Intelligence
Platform

Enrichment & Analysis
Tracking
Reporting

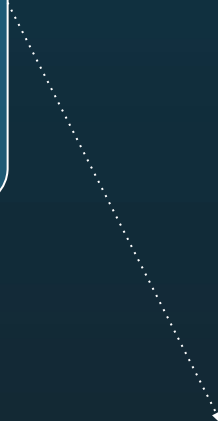
SIEM

Security Information and
Event Management

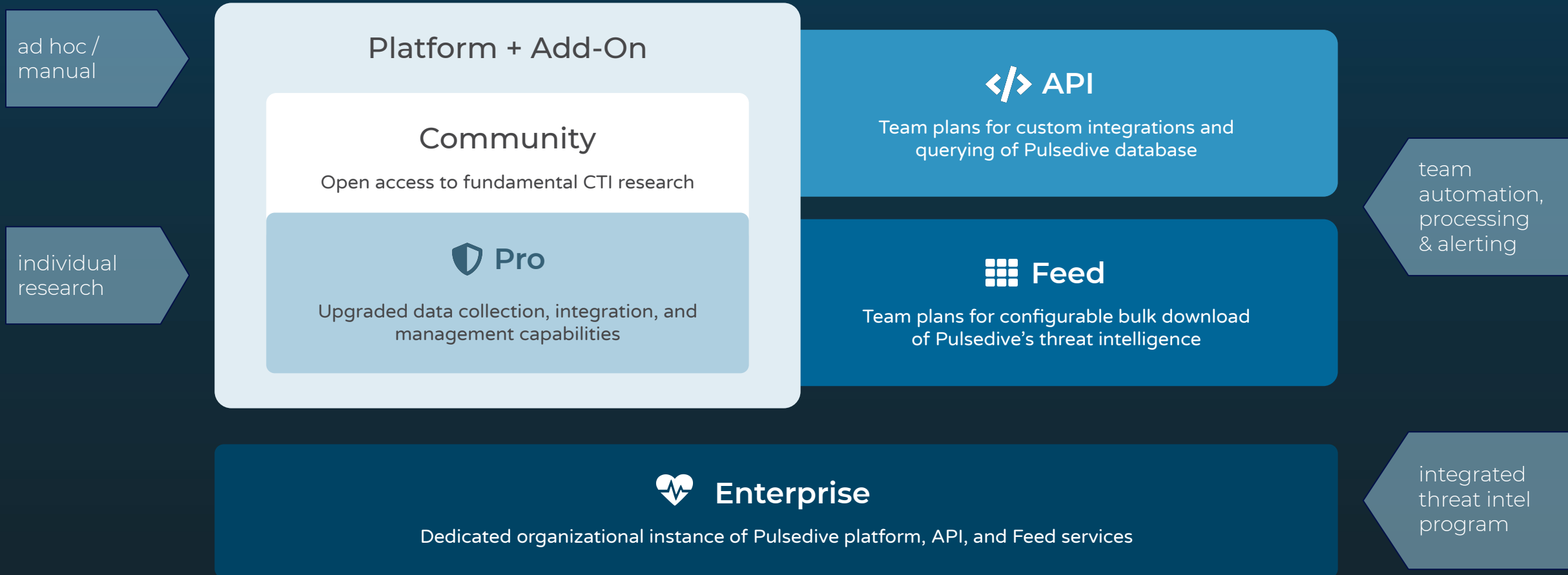
Correlation
Detection
Alerting

SOAR

Security Orchestration,
Automation, Response



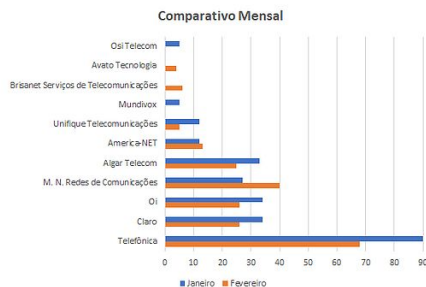
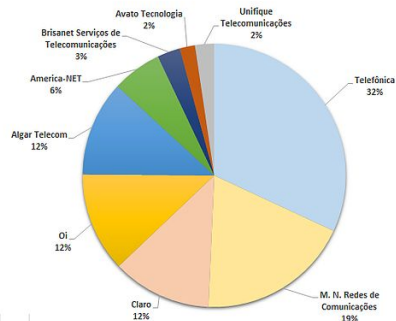
Working with CTI Teams



Partnership

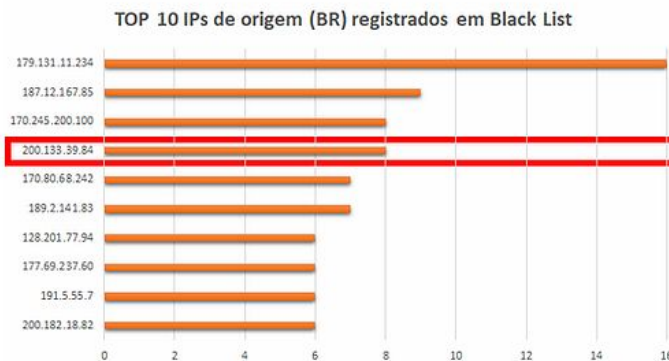


Finally, when analyzing the volume of attacks coming from registered IPs in Brazil, we list the ISPs most involved. The operators Telefônica, MN Redes de Comunicações, Claro, Oi and Algar Telecom are highlighted.



It is also possible to observe that these same operators stand out in the monthly comparison.

We highlight the main IPs of Brazilian origin registered in the Blacklist Dshield that communicated with our sensors. We note that the IP 200.133.39.84 that had been reported in January returned to appear in our top 10 in February.

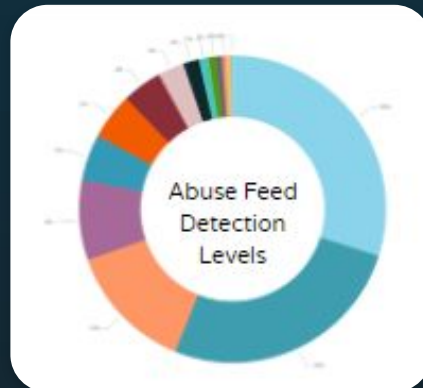
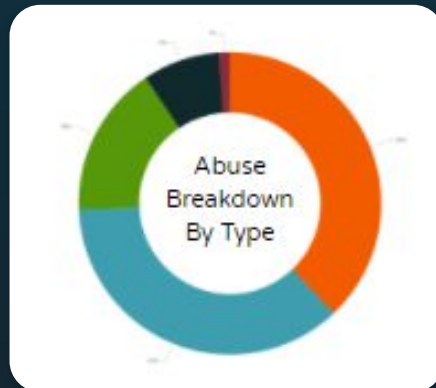


200.133.39.84 was found in our database!
This IP was reported 1,391 times. Confidence of Abuse is 100%: ?
100%

- High risk
- Direct-to-IP URL
- Found in threat feeds
- Returns PTR record

A screenshot of the Pulsedive interface. The top section is titled "Threats" and shows a threat named "SSH Brute Force Attack" with a timestamp of "2020-12-15 08:11:35" and a status of "2 months ago". Below this is a section titled "Feeds" which lists several threat feeds: "Blocklist.de Blocklist" (2020-09-17 05:00:29, 6 months ago), "Darklist" (2020-09-18 15:56:22, 6 months ago), and "Dictionary SSH Attacks" (2020-12-15 08:11:35, 2 months ago). The interface is dark-themed with blue and orange accents.

Partnership



REALTIME REGISTER							Domainname	
High Abuse level								
115 # Abuse indicators								
CLIENT_TRANSFER_PROH... Status ns-dmdv77dmdb.eu-dnswnd.... Name servers Switzerland Registrant country Verisign Registry ----- Brand mei 7, 2008 Created date maart 21, 2022 Expiry date								
View in domain manager →								
Select indicator to view details →								
Back to overview ↶								
Category	Feed	Risk	Type	Added	Updated	Indicator		
spam	OpenPhish	medium	url	februari 11, 2021	februari 11, 2021	https://att1.v		
spam	OpenPhish	medium	url	februari 11, 2021	februari 11, 2021	https://yahoi		
spam	PhishTank	medium	url	februari 11, 2021	februari 11, 2021	https://konfir		
phishing	PhishStats	high	url	februari 10, 2021	februari 10, 2021	https://konfir		
phishing	PhishStats	high	url	februari 10, 2021	februari 10, 2021	https://yahoi		
phishing	PhishStats	high	url	februari 10, 2021	februari 10, 2021	https://yahoi		
phishing	PhishStats	medium	url	februari 10, 2021	februari 10, 2021	https://att1.v		
phishing	PhishStats	medium	url	februari 10, 2021	februari 10, 2021	https://att1.v		
phishing	PhishStats	medium	url	februari 10, 2021	februari 10, 2021	https://konfir		
spam	OpenPhish	low	url	februari 10, 2021	februari 10, 2021	https://faceb		
spam	PhishTank	low	url	februari 10, 2021	februari 10, 2021	https://faceb		
spam	PhishTank	low	url	februari 10, 2021	februari 10, 2021	https://konfir		
phishing	PhishStats	high	url	februari 9, 2021	februari 9, 2021	https://faceb		
phishing	PhishStats	high	url	februari 9, 2021	februari 9, 2021	https://konfir		
phishing	PhishStats	medium	url	februari 9, 2021	februari 9, 2021	https://faceb		
phishing	PhishStats	medium	url	februari 9, 2021	februari 9, 2021	https://konfir		
spam	OpenPhish	low	url	februari 9, 2021	februari 9, 2021	http://dhl-shi		
phishing	PhishStats	low	url	februari 8, 2021	februari 8, 2021	http://dhl-shi		
phishing	PhishStats	medium	url	februari 8, 2021	februari 8, 2021	http://dhl-shi		
spam	PhishTank	medium	url	februari 2, 2021	februari 2, 2021	https://settin		
phishing	PhishStats	high	url	februari 1, 2021	februari 1, 2021	https://settin		
phishing	PhishStats	medium	url	februari 1, 2021	februari 1, 2021	https://settin		
spam	PhishTank	medium	url	februari 1, 2021	februari 1, 2021	https://pulihl		
phishing	PhishStats	medium	url	januari 29, 2021	januari 29, 2021	https://pulihl		
phishing	PhishStats	medium	url	januari 29, 2021	januari 29, 2021	https://pulihl		
phishing	PhishStats	medium	url	januari 26, 2021	januari 26, 2021	https://att28		
phishing	PhishStats	medium	url	januari 26, 2021	januari 26, 2021	https://att28		
phishing	PhishStats	low	url	januari 23, 2021	januari 23, 2021	https://faceb		
phishing	PhishStats	medium	url	januari 23, 2021	januari 23, 2021	https://faceb		
spam	PhishTank	medium	url	januari 19, 2021	februari 14, 2021	http://absab		
phishing	PhishStats	high	url	januari 18, 2021	januari 18, 2021	http://absab		
phishing	PhishStats	medium	url	januari 18, 2021	januari 18, 2021	http://absab		
spam	PhishTank	medium	url	januari 18, 2021	januari 18, 2021	https://faceb		
phishing	PhishStats	medium	url	januari 17, 2021	januari 17, 2021	https://faceb		
spam	PhishTank	medium	url	januari 15, 2021	februari 14, 2021	https://absal		
general	Cyber Threat Coalition - domains	high	hostname	december 31, 2020	december 31, 2020	setting-akun		

Many Ways In + Boosters



Related Work Experience

Bootcamps & Courses

Social Media

Certifications

Personal Research/Lab

Groups/Networking!!

Diploma/Degree

Events & Volunteering

Follow & Learn

My First Year In Cyber Threat Intel

<https://blog.bushidotoken.net/2020/08/my-first-year-in-cyber-threat.html>

FAQs on Getting Started in CTI

<https://medium.com/katies-five-cents/faqs-on-getting-started-in-cyber-threat-intelligence-f567f267348e>

Top 10 Reading List for CTI

<https://medium.com/katies-five-cents/a-top-10-reading-list-if-youre-getting-started-in-cyber-threat-intelligence-c11a18fc9798>

Discover Your Pathway to Cyber

<https://www.cyber.nj.gov/news-events/alice-in-cyberspace/>

How I Moved from Journalism to CTI

<https://www.selenalarson.com/blog/2021/3/11/how-i-moved-from-journalism-to-cyber-threat-intelligence>

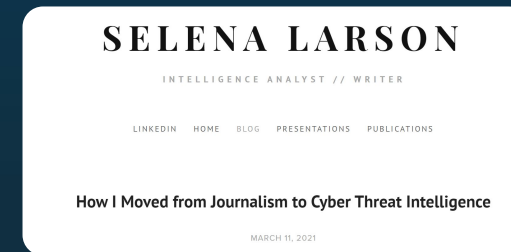
Herman Slatman, Awesome Threat Intelligence

<https://github.com/hslatman/awesome-threat-intelligence>

SANS CTI Summit 2020 & 2021 Playlists

<https://youtube.com/playlist?list=PLfouvuaJispToL98Xfq57bnRayEFI0XZwE>

https://www.youtube.com/playlist?list=PLfouvuaJispToG7_FMUOqS0JPq69sn5DBe



The Intelligence EASY Button
Chris Cochran

FAQs on Getting Started in Cyber Threat Intelligence



Katie Nickels [Follow](#)

Aug 17, 2020 · 10 min read



References



Gartner, Threat Intelligence Definition

<https://www.gartner.com/reviews/market/security-threat-intelligence-services>

PwC, Cyber Threats 2020: A Year in Retrospect, 2021

<https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf>



Robert M. Lee, SANS Institute, 2021

2021 SANS Cyber Threat Intelligence (CTI) Survey Results

<https://www.sans.org/webcasts/2021-cyber-threat-intelligence-cti-survey-results-116475>

ENISA, Various Threat Landscape and Threat Intelligence Reports

<https://www.enisa.europa.eu/publications>



Chris Cochran, The Threat Intelligence EASY Button, SANS CTI Summit 2020

https://youtu.be/ecY5WW_gppc



Thank You!



@pulsedive



/company/pulsedive

pulsedive.com

© 2021 Pulsedive LLC