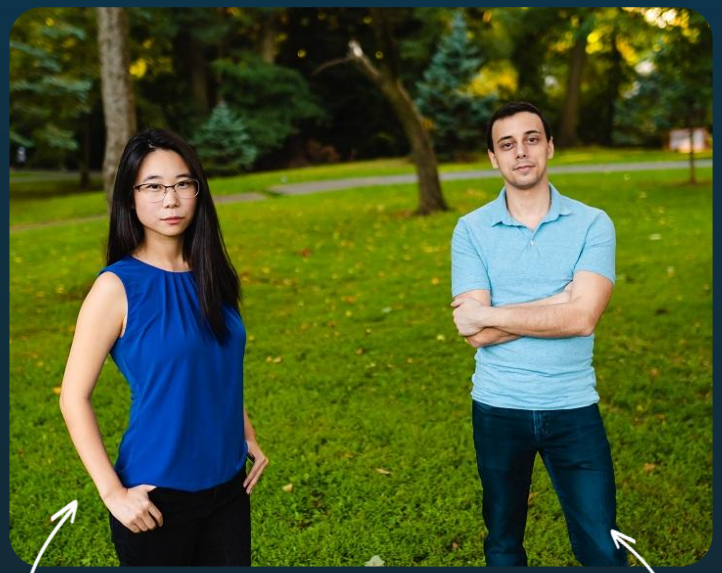
The State of CTI

(Cyber Threat Intelligence)

March 25, 2021

Hello!



Grace Chi
Cofounder & COO

Dan Sherry
Founder & CEO

Pulsedive

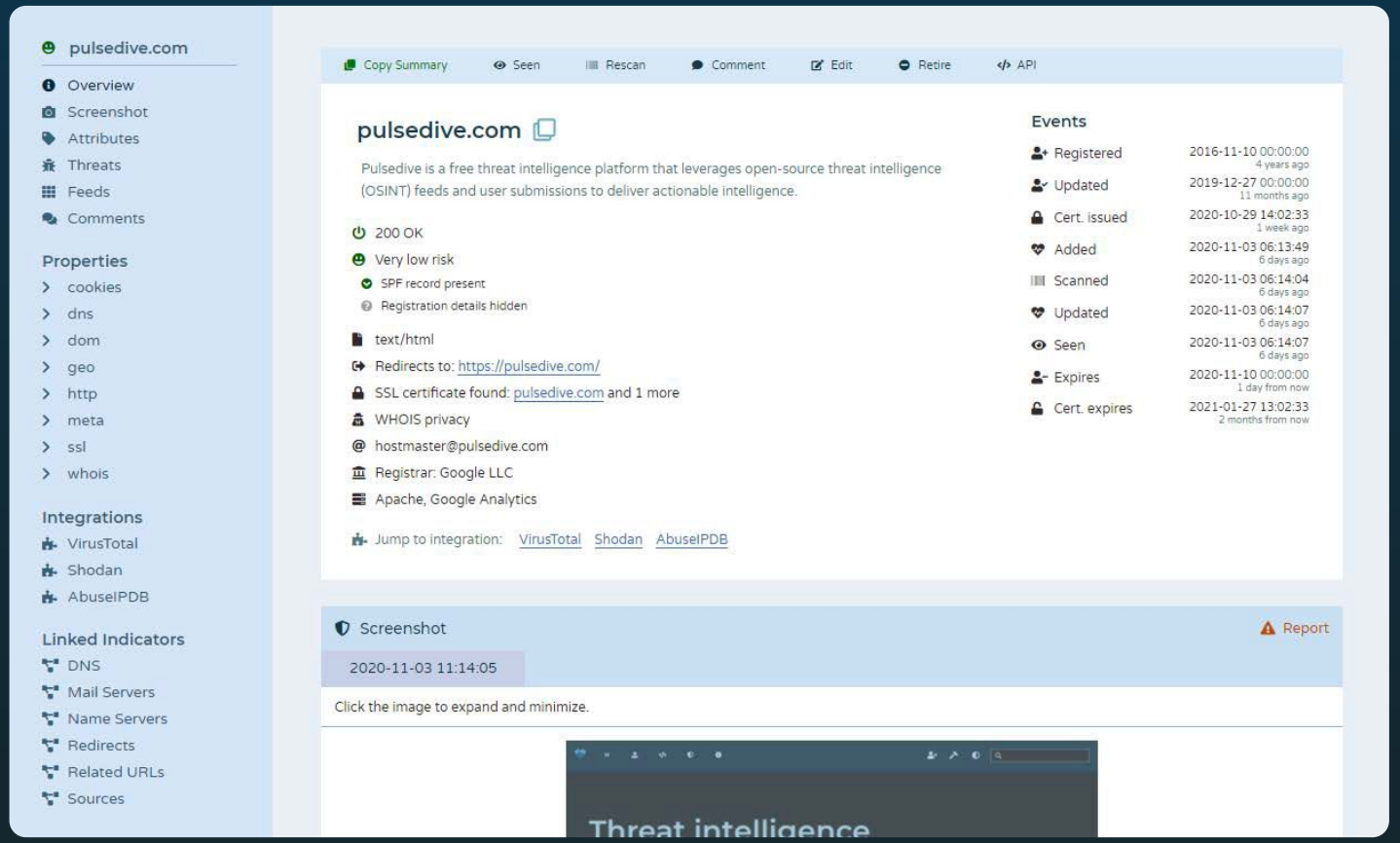
Delivering high-fidelity cyber threat intelligence to help communities and organizations worldwide proactively improve their security posture.

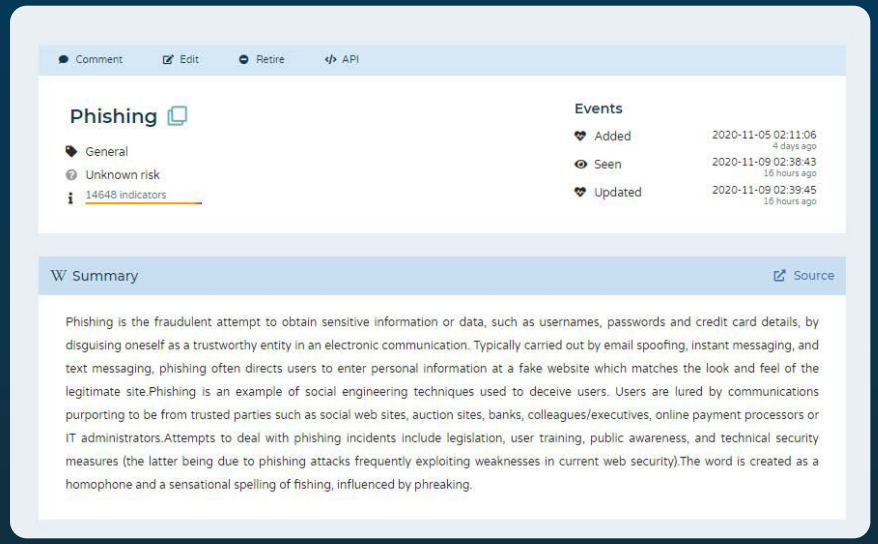
Founded
2017

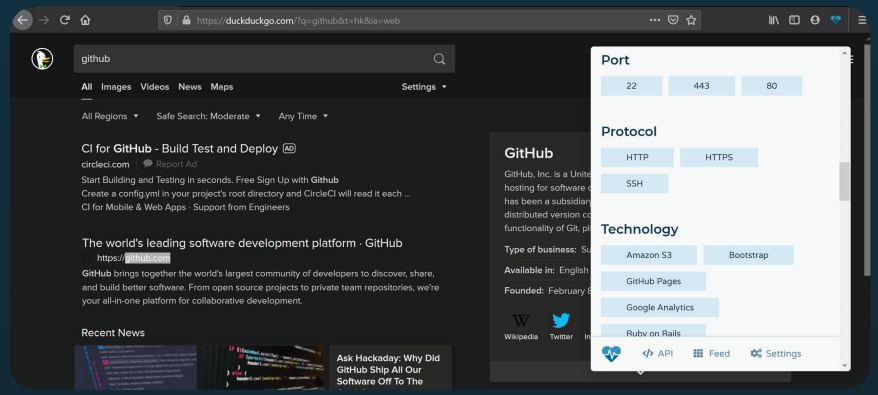
Located
New Jersey

Recommended by
Fortune 500
Big 4 Consulting
SANS Institute

Community-Driven Platform + Data



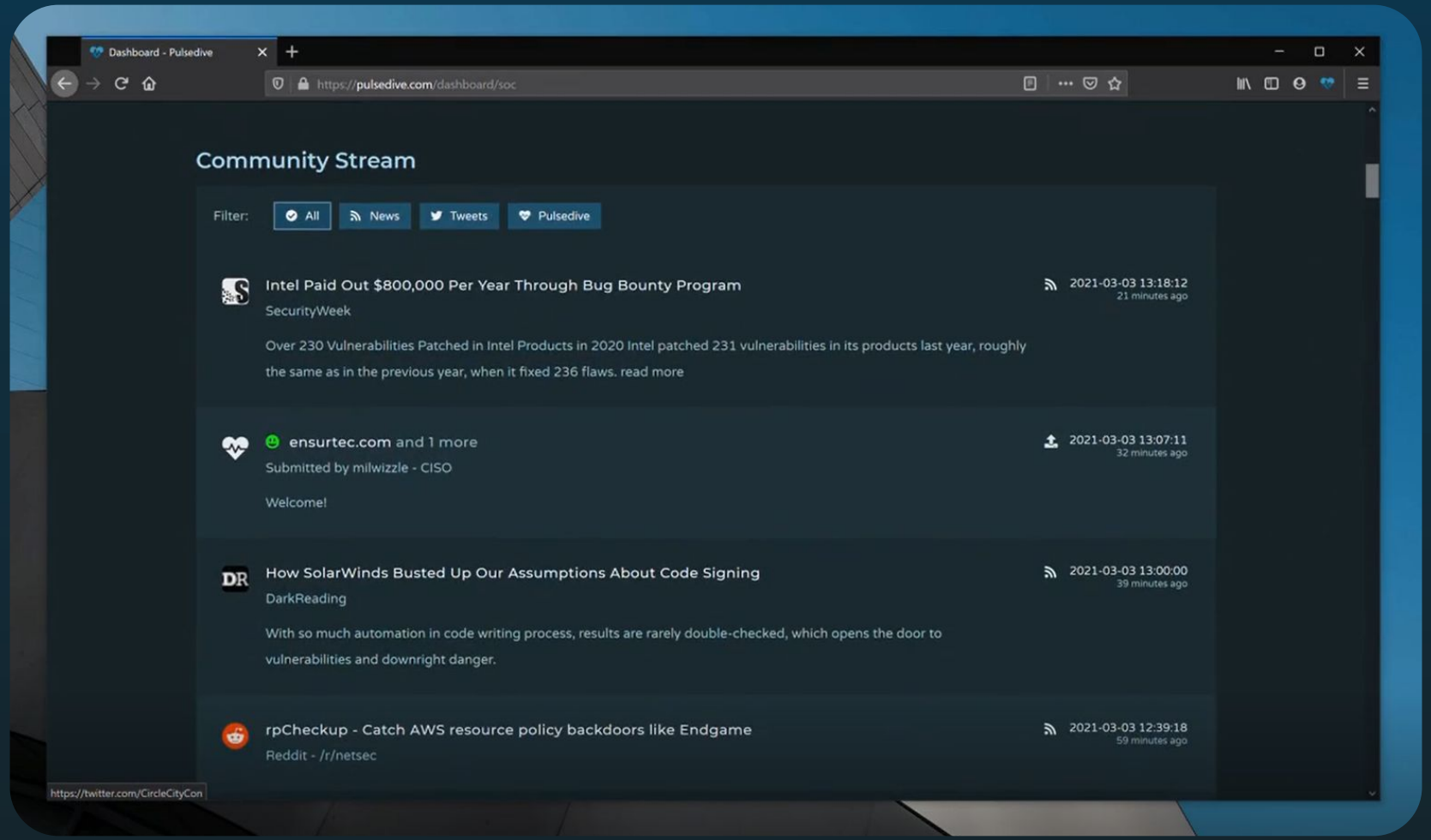




Used Globally by Pros, Researchers, Hobbyists

Dashboard: Latest Industry News & Events

pulsedive.com/dashboard Free access - no account needed



Today

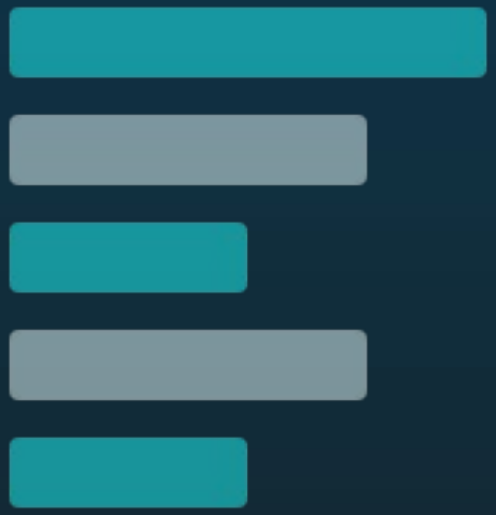
CYBER THREAT INTELLIGENCE (CTI) 101

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.

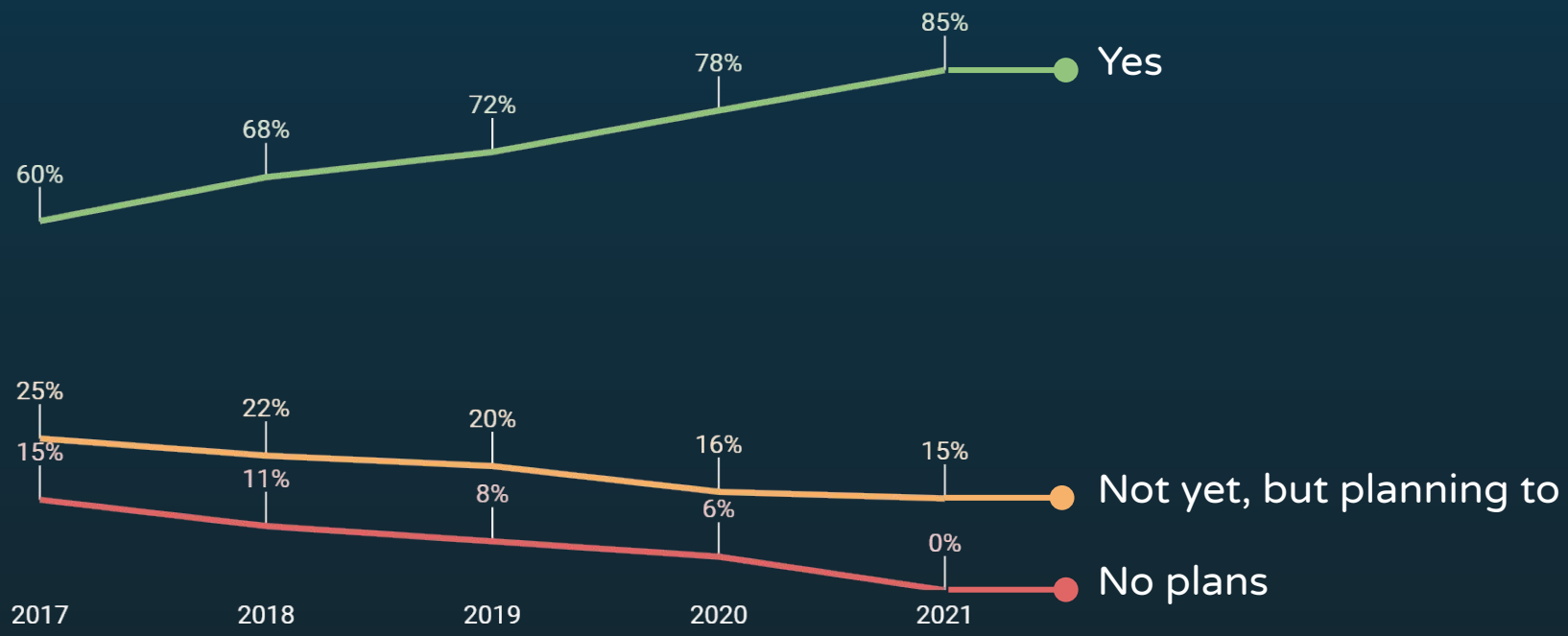
Gartner

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?

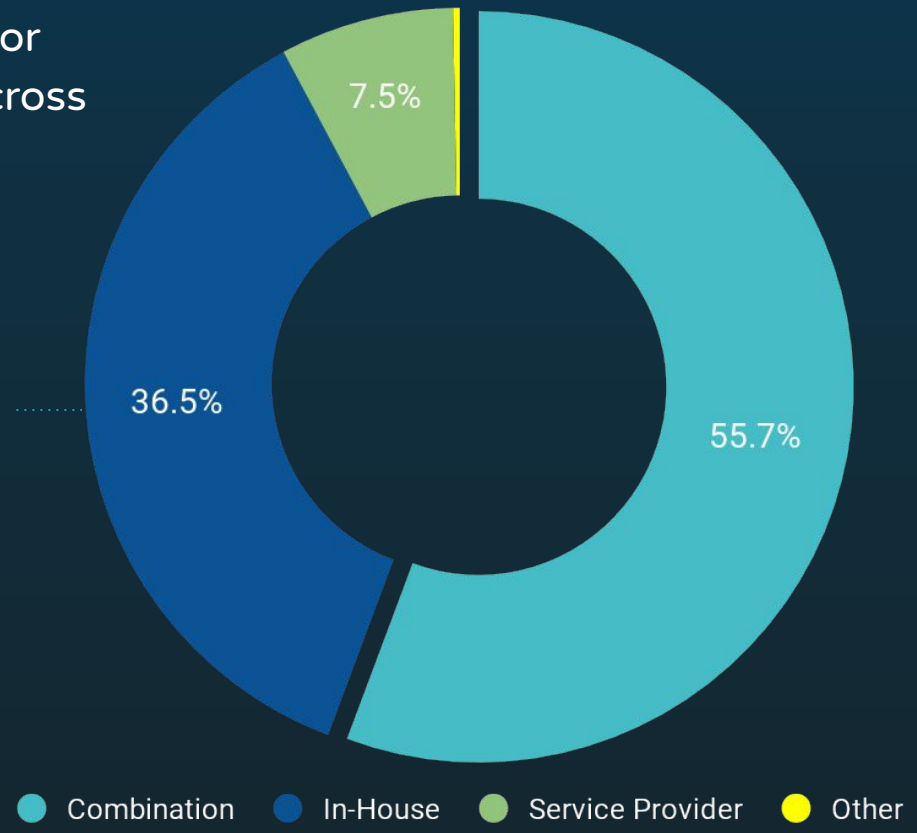


SANS Institute, 2021 CTI Survey

Who & Where?

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

In-house
+5%
since 2020



Vendors
Products, Startups

Consulting
Professional Services

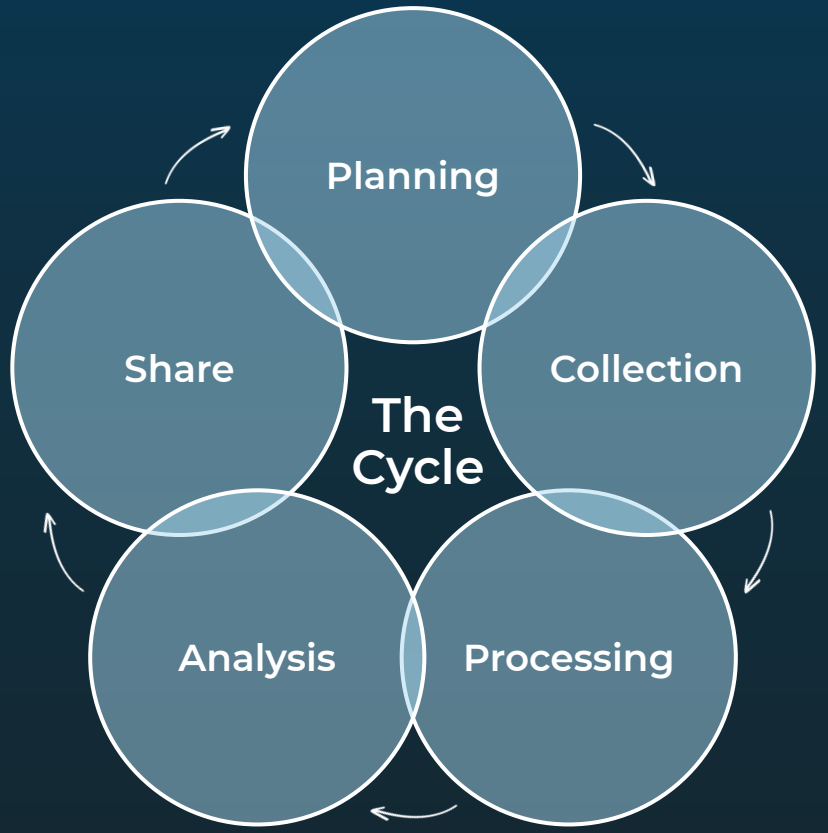
Government
Military, Federal, Local

Institutional
Academic, Healthcare

Commercial
Enterprises, Finance, Mfg

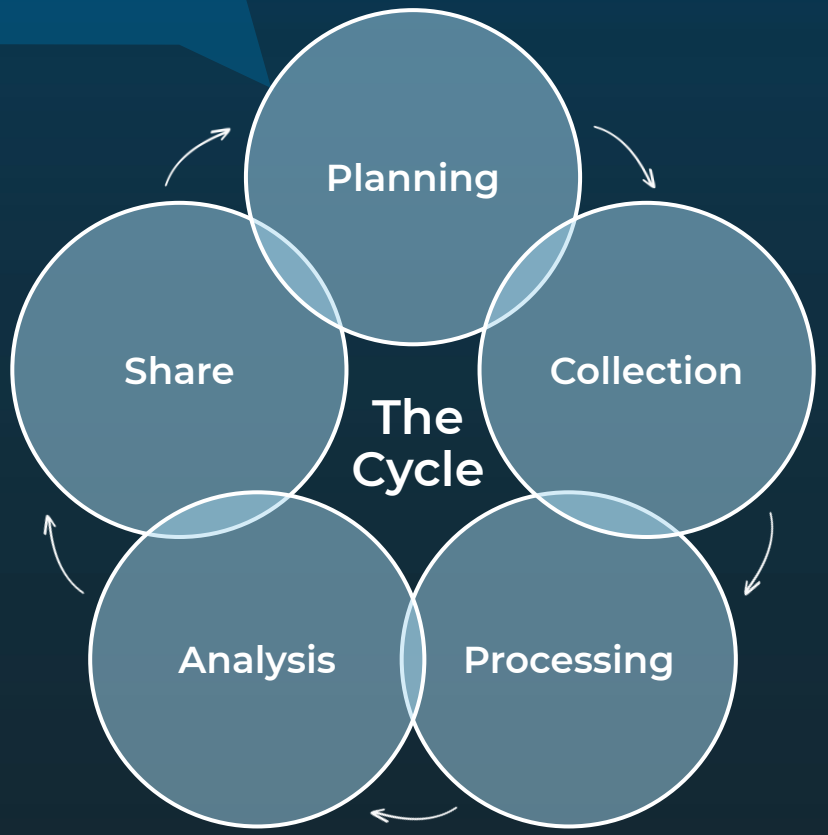
SANS Institute, 2021 CTI Survey

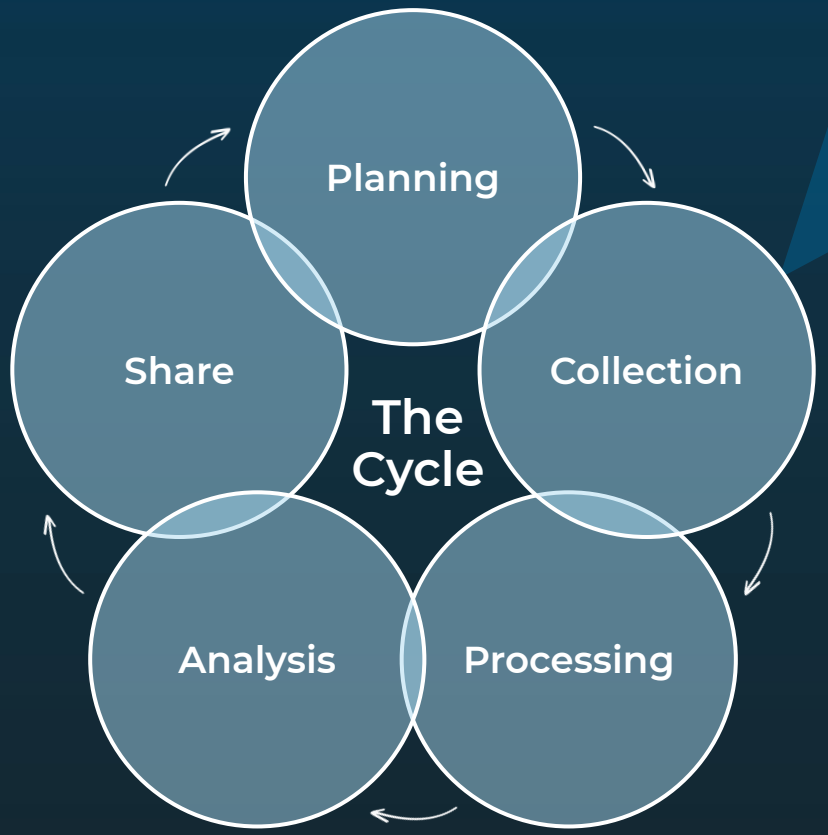
Intelligence Cycle



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

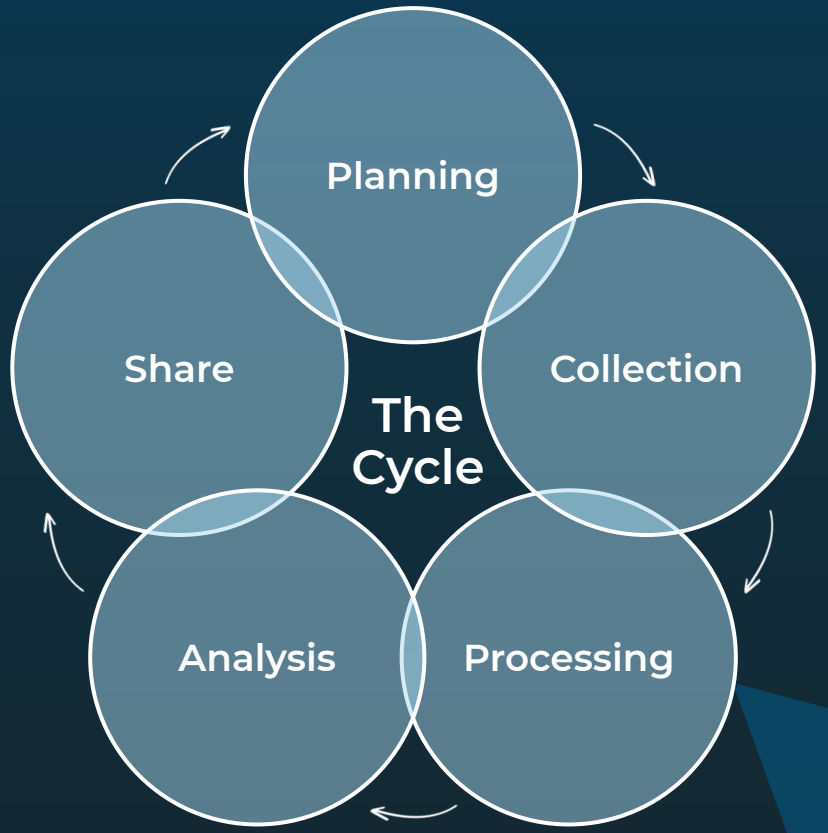




Internal & External Sources

Network logs, past incidents, risk analysis reports

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

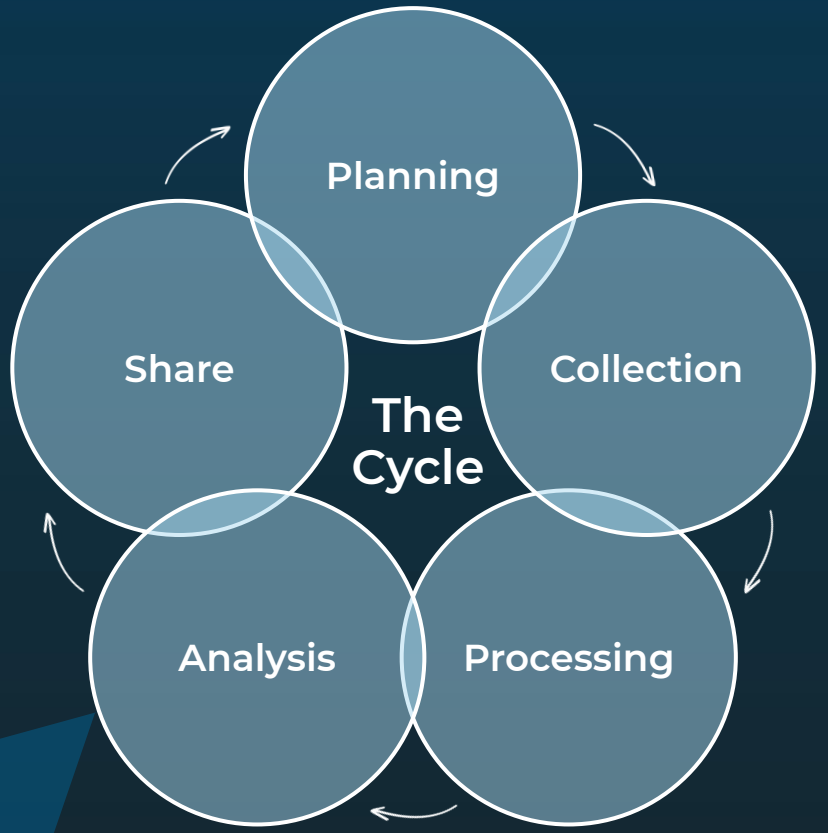


Enrichment & Contextualization

OSINT engines, scanning, lookups, web tools, footprinting

Counterintelligence, honeypots, sinkholes, YARA rules

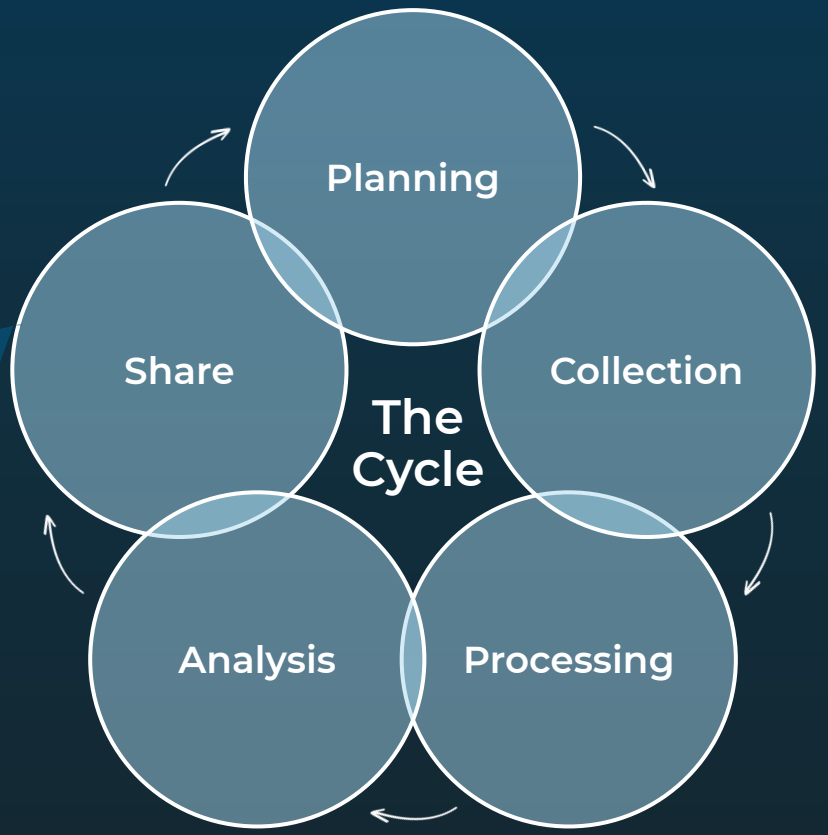
Human intelligence, social engineering



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

POLL

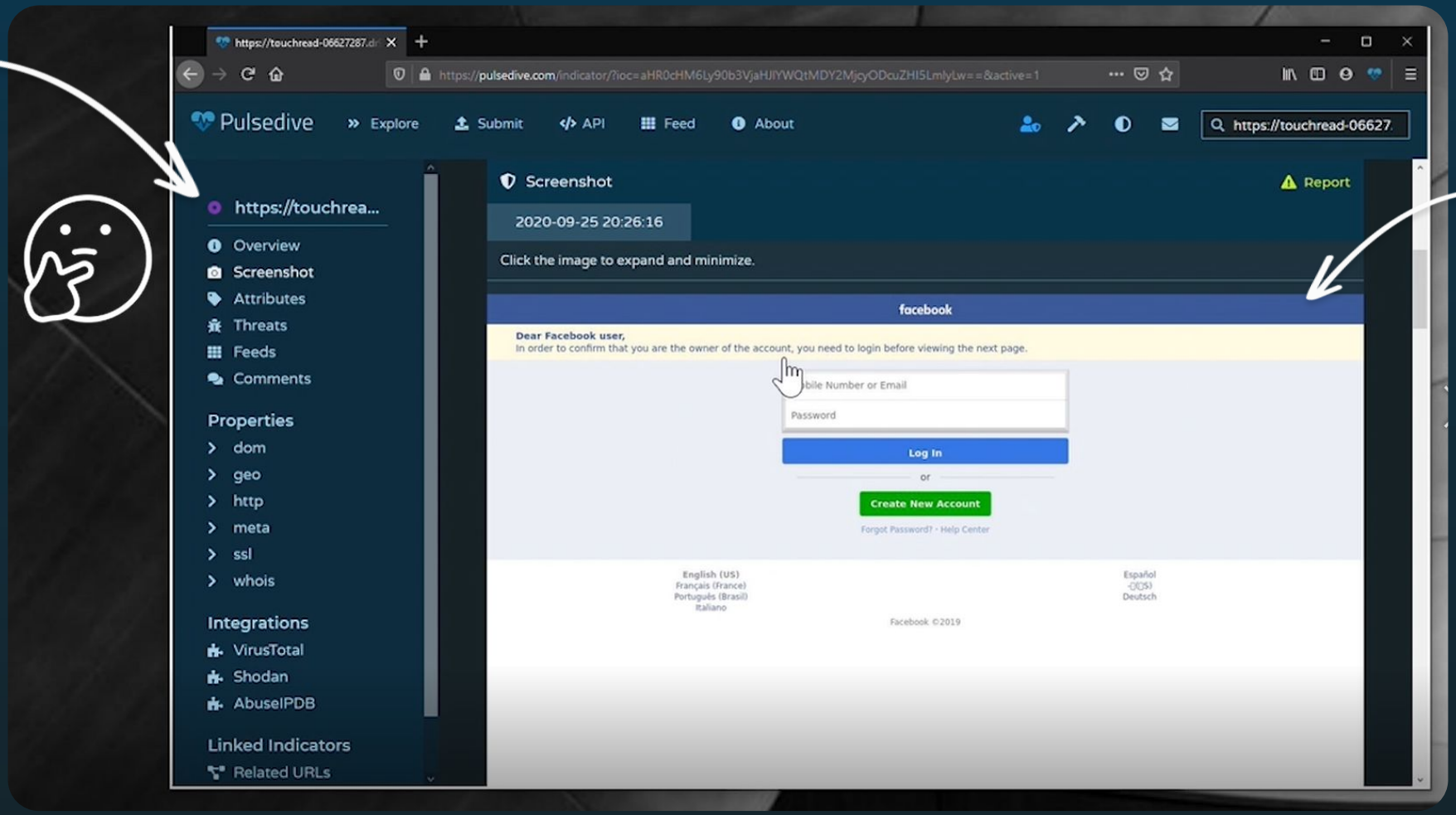
Dissemination & Feedback
Selective format, output, timeliness, and distribution of intelligence with clear actions/considerations to key stakeholders, plus feedback on deliverables i.e. reports, mailings



LOOKING PHISHY

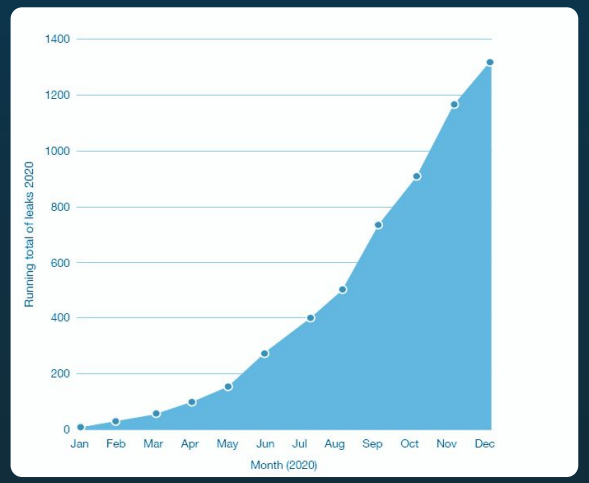
Processing & Enrichment In Action

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



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

Open Source

Dark web

Internal

External

Historical

Integrations

Enrichment

Managed CTI

Services

Finished Reports

Commercial

Management Platforms

Automation

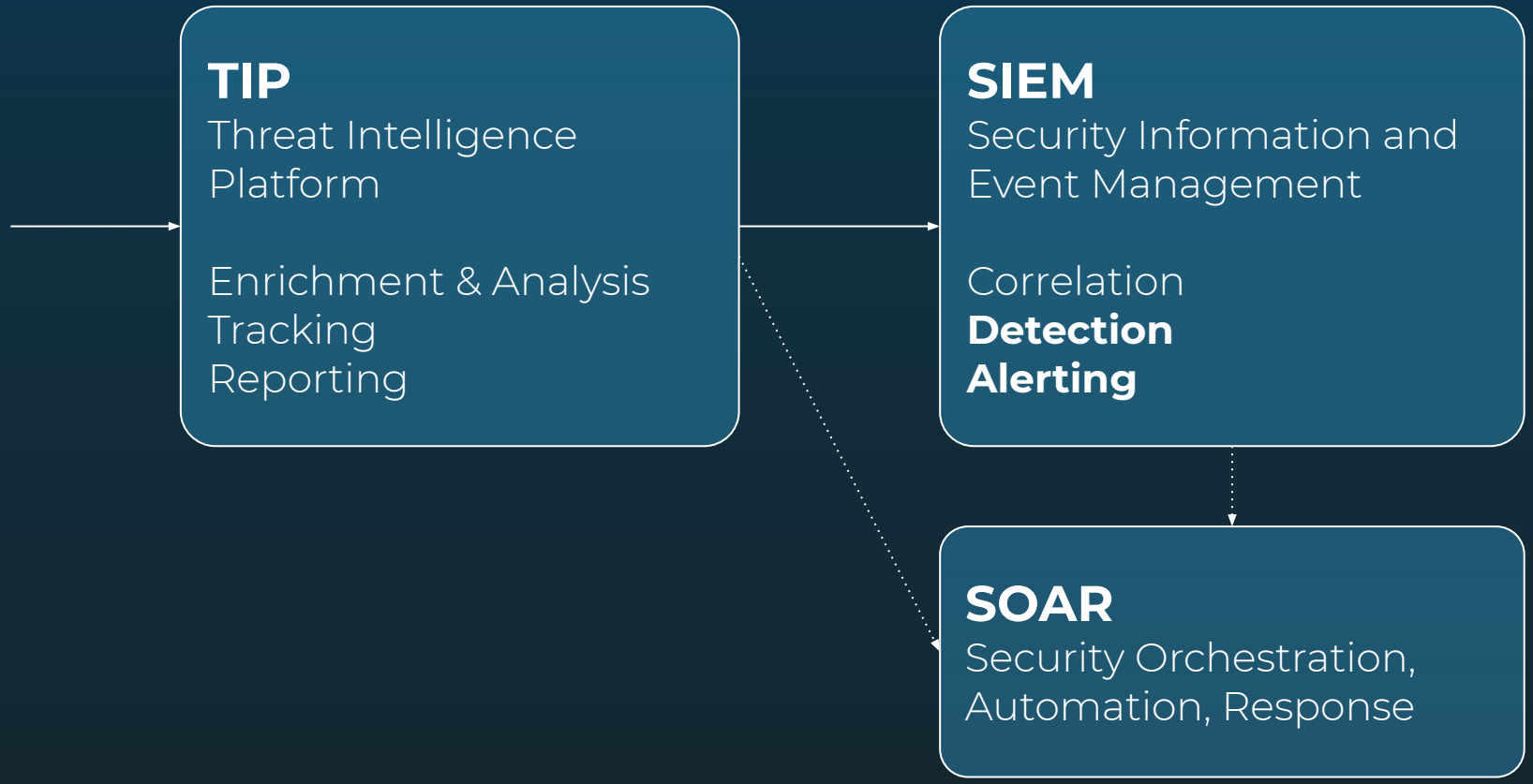
Feeds

Niche Solutions

Sector, Geography, Technology

Example Flow

Intelligence
(Internal & External)
Malicious domains,
IPs, URLS
Vulnerabilities
News & Advisories



Working with CTI Teams

ad hoc / manual

individual research

Platform + Add-On

Community

Open access to fundamental CTI research

Pro

Upgraded data collection, integration, and management capabilities

API

Team plans for custom integrations and querying of Pulsedive database

Feed

Team plans for configurable bulk download of Pulsedive's threat intelligence

team automation, processing & alerting

Enterprise

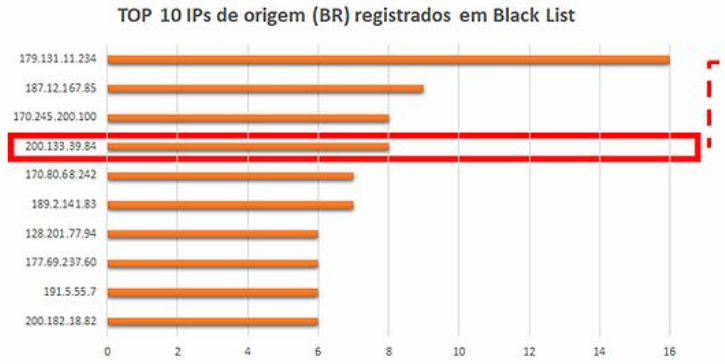
Dedicated organizational instance of Pulsedive platform, API, and Feed services

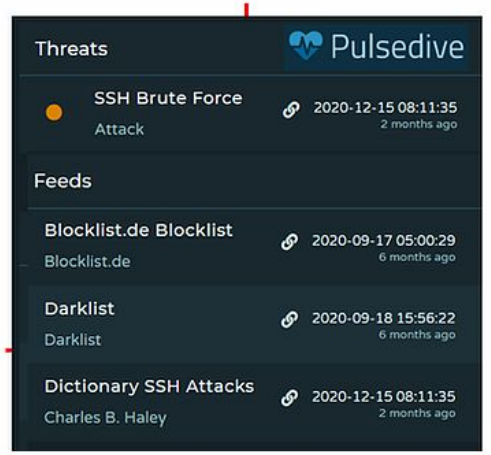
integrated threat intel program

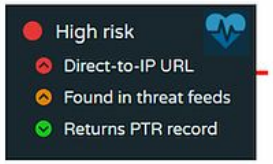
Partnership

OpenCTI

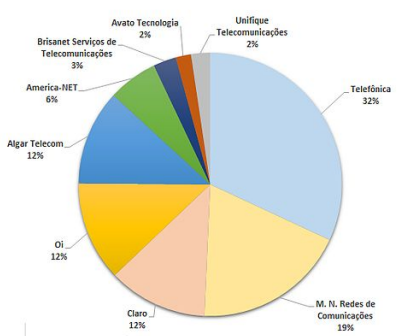
We highlight the main IPs of Brazilian origin registered in the Blacklist Dshield that communicated with our sensors. We note that the IP 200.133.39.84 that had been reported in January returned to appear in our top 10 in February.

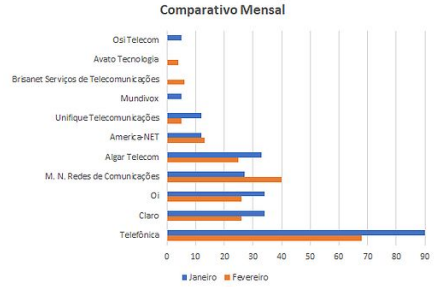






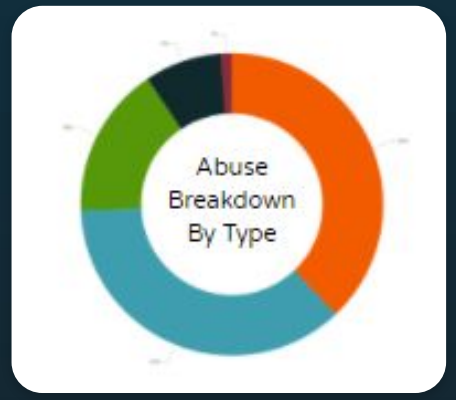
Finally, when analyzing the volume of attacks coming from registered IPs in Brazil, we list the ISPs most involved. The operators Telefônica, MN Redes de Comunicações, Claro, OI and Algar Telecom are highlighted.

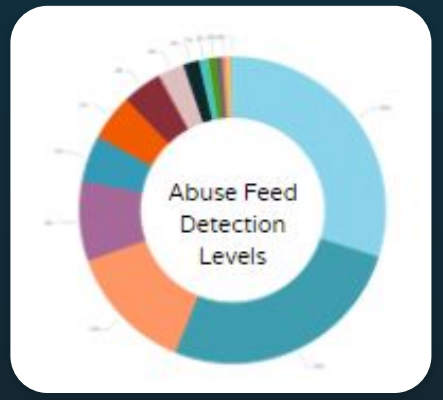


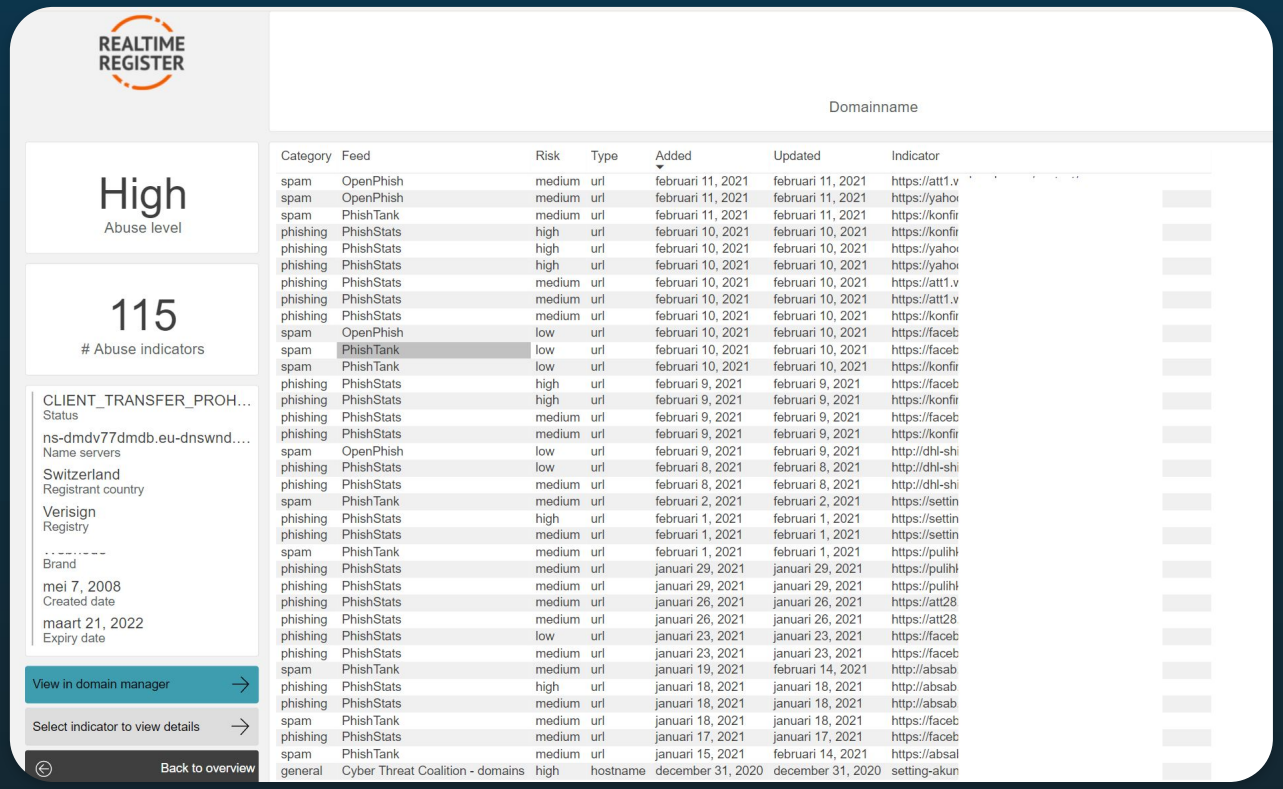


It is also possible to observe that these same operators stand out in the monthly comparison.

Partnership







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=PLfouvuAjspToL98Xfq57bnRayEFl0XZwE
https://www.youtube.com/playlist?list=PLfouvuAjspToG7_FMUOqS0JPq69sn5DBe

The Intelligence EASY Button
Chris Cochran

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_qppc

Thank You!


@pulsedive


/company/pulsedive

pulsedive.com