

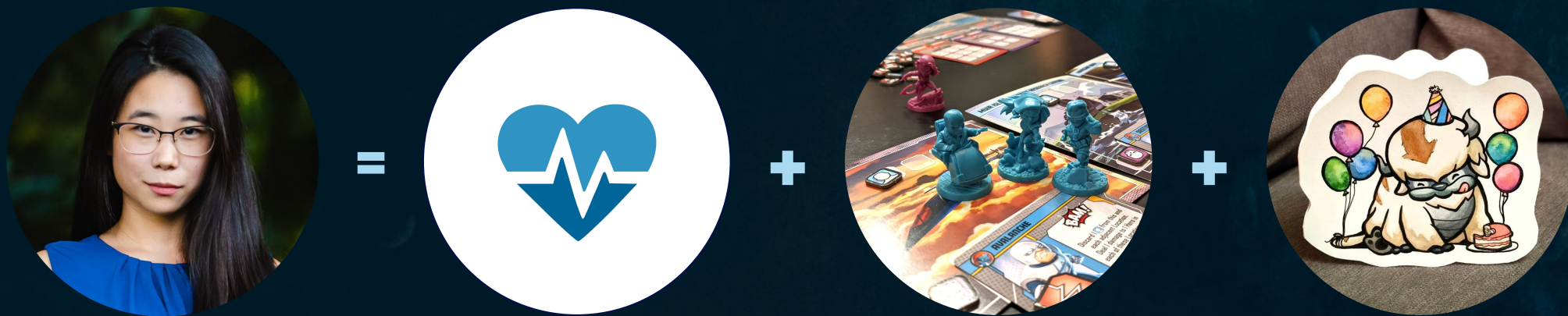


Cyber Threat Intelligence & How Sharing is Caring



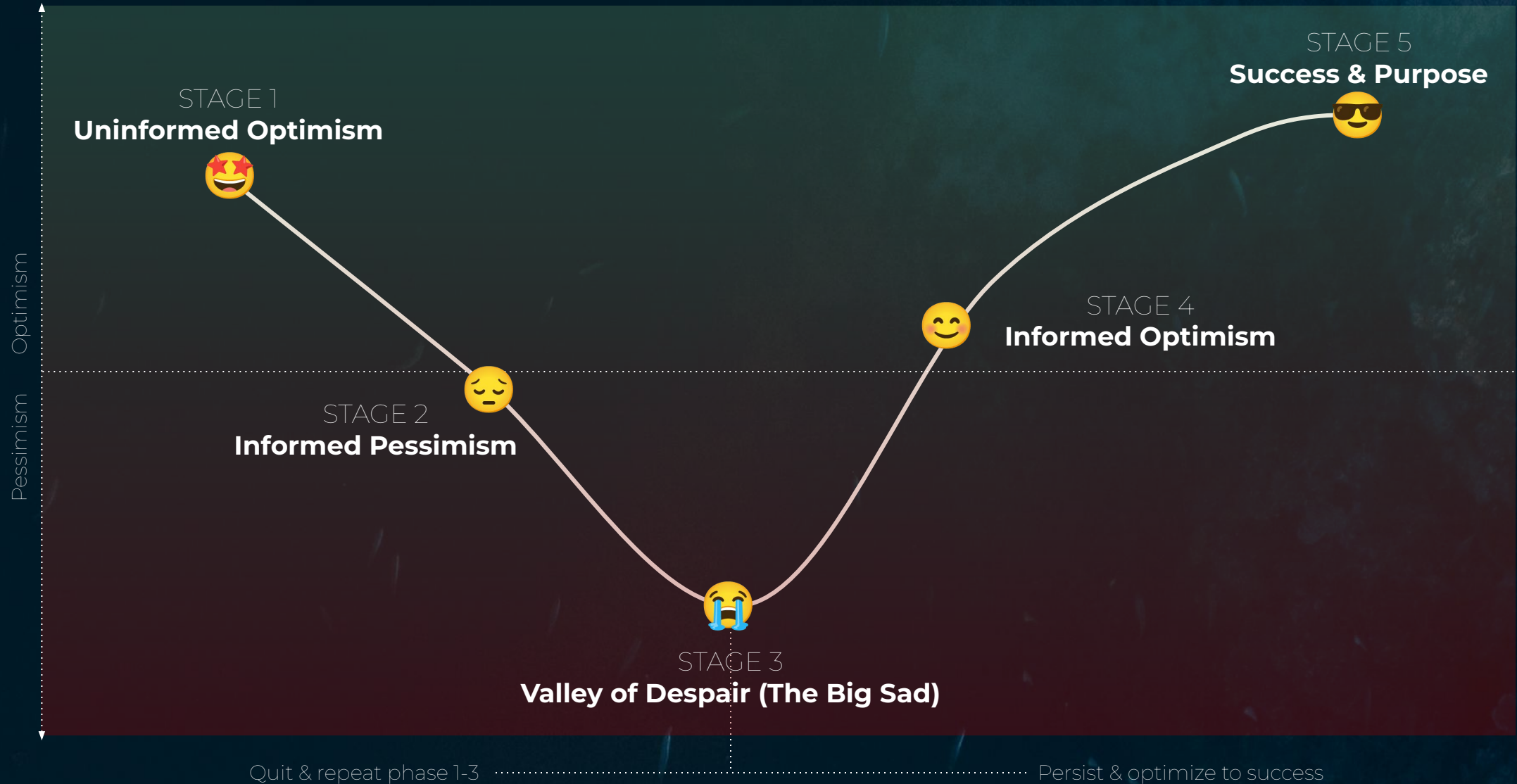
Grace Chi
June 30, 2022

👋 Introduction



BLUF: CTI networking is an asset, not an afterthought

Something We've All Been Through...





What's CTI?

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

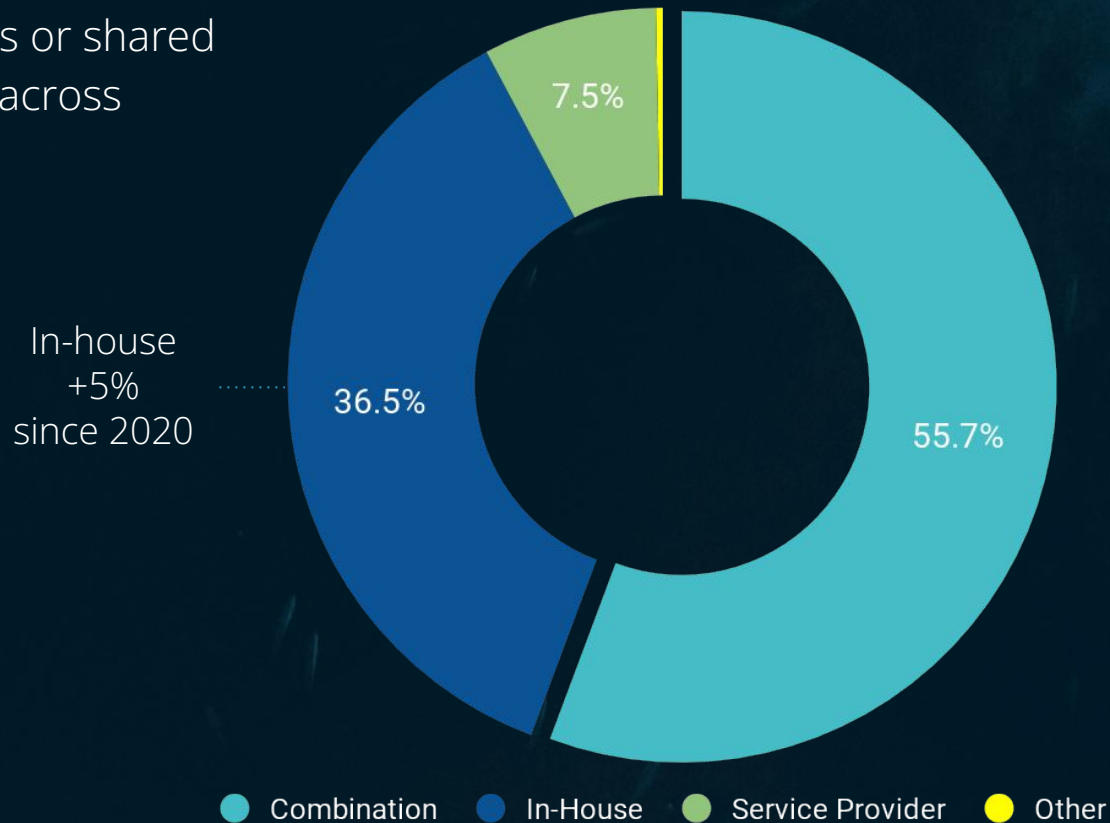
What CTI Isn't

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

Data. Contextualized. Informing. Action.

Who & Where?

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

Typical Feeder Roles & Responsibilities

Security Operations
Security Consulting
Digital Forensics/Incident Response
Detection/Security Engineer
System Administrator
Government/Military Intelligence
Technology Reporter

Writing & Reporting

Networking

Technical Research

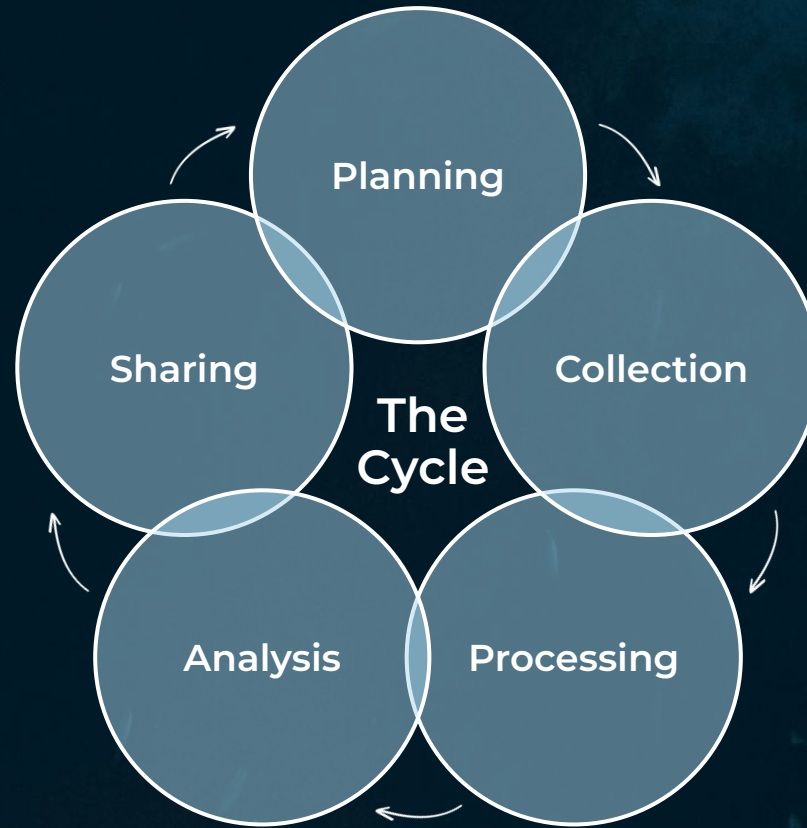
Scripting

Digital Forensics

Data Analysis



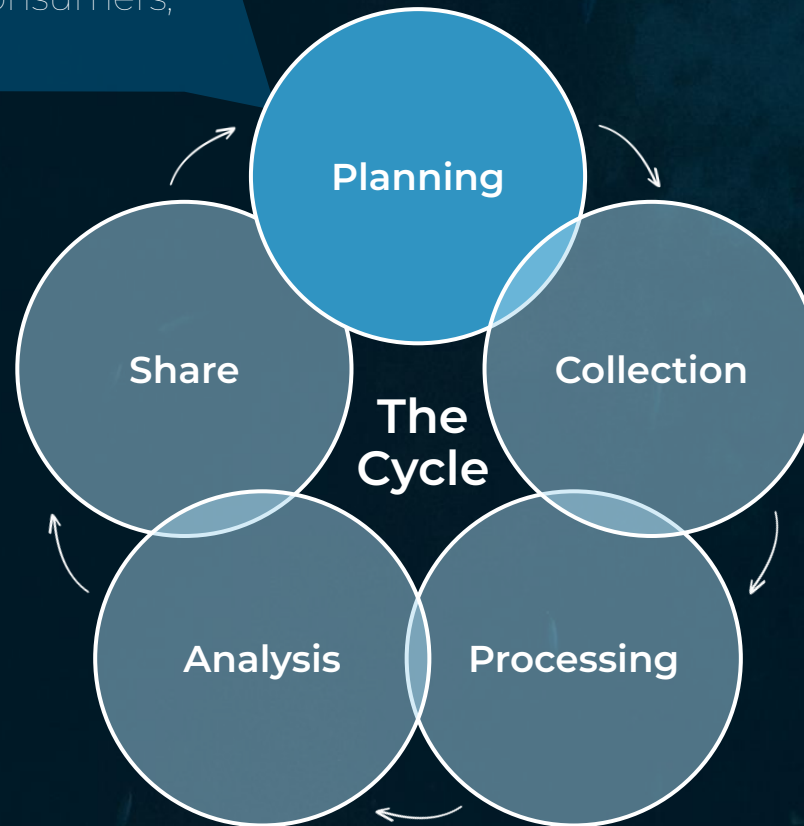
Intelligence Cycle

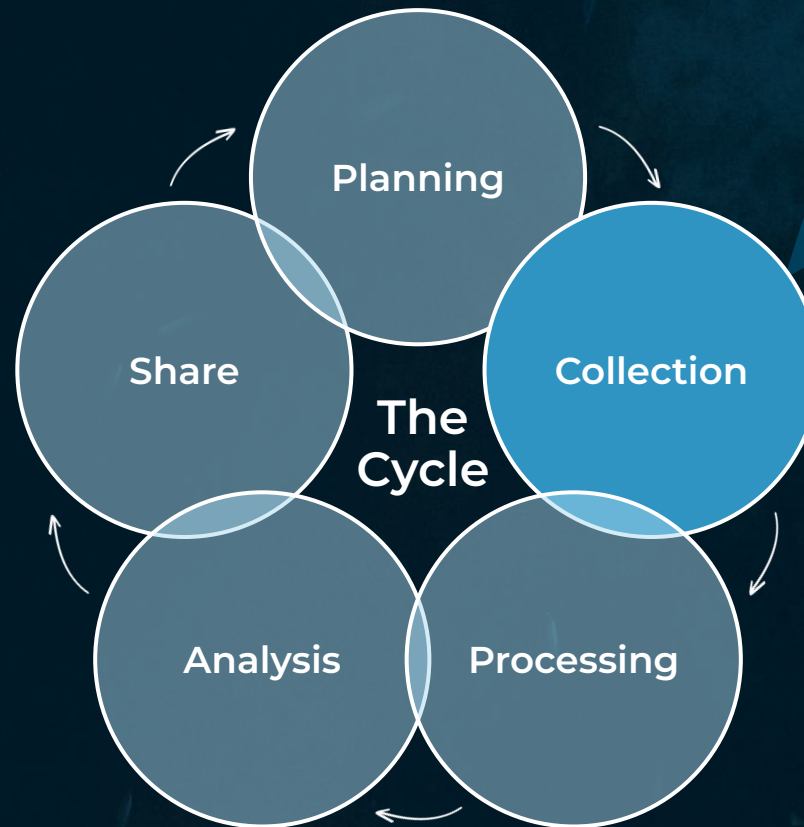


Requirements Gathering

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

👉 What do we care about? Why?



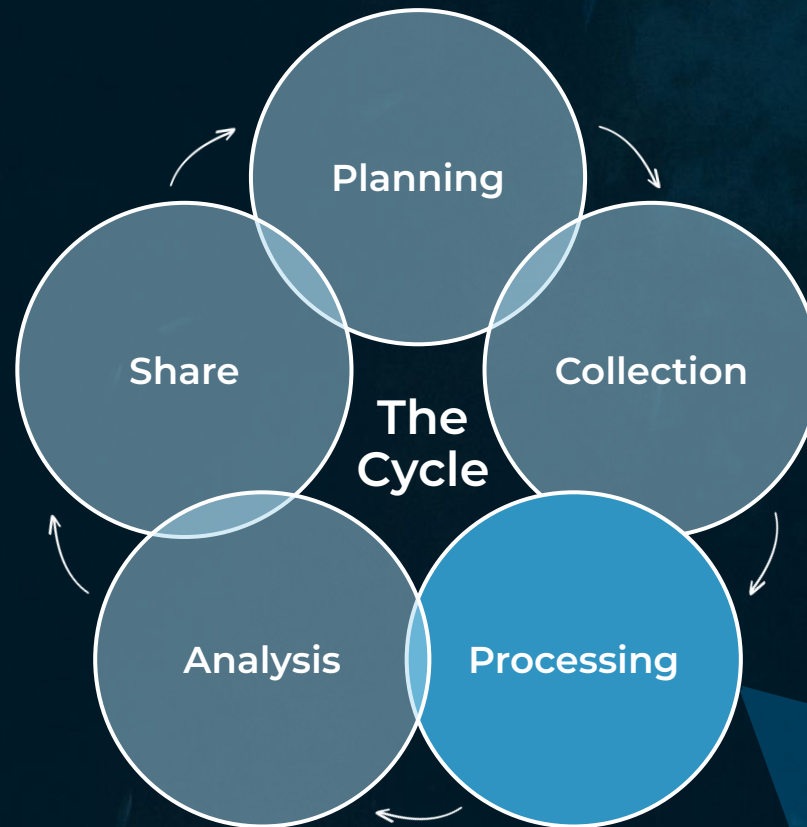


Internal & External Sources

Network logs, past incidents, risk analysis reports

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

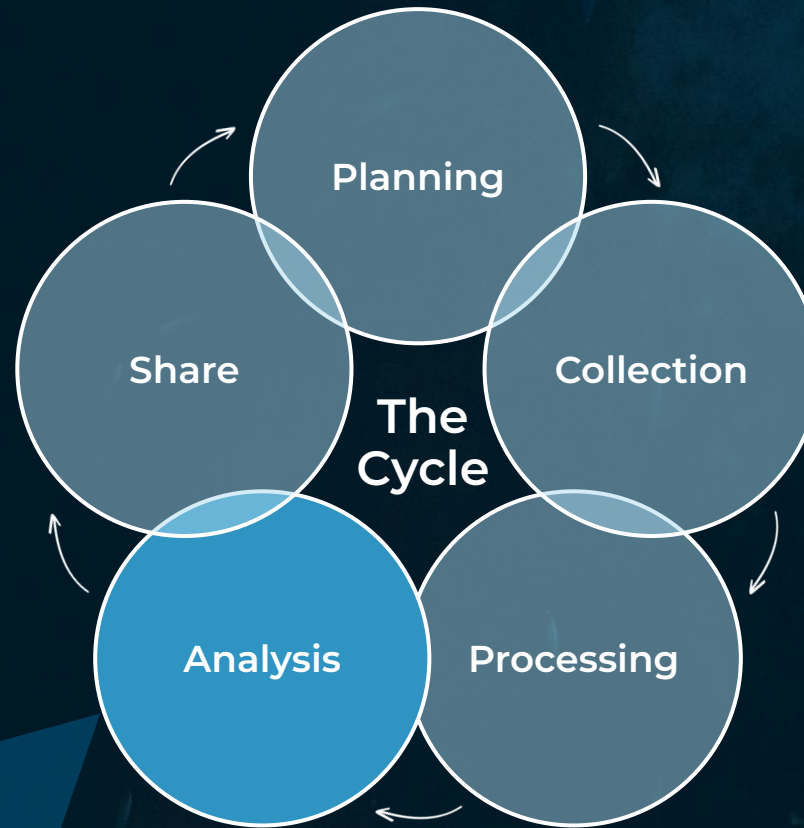
👉 What data do we need, from where?



Enrichment & Contextualization

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

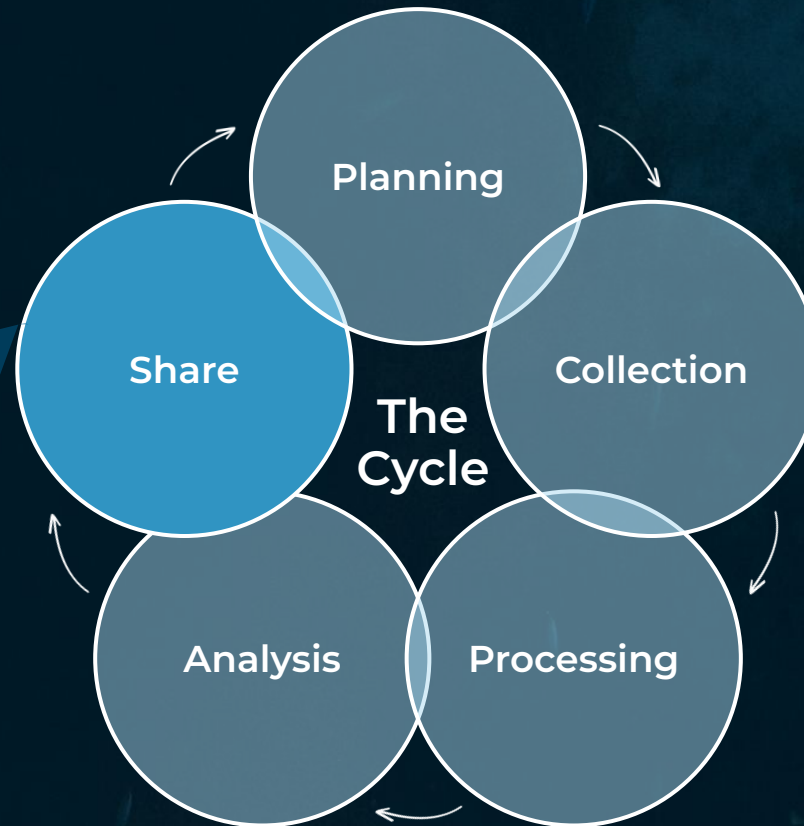
👉 What's the bigger picture here?



Analysis & Intelligence Creation

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

👉 What matters? Why and to whom?

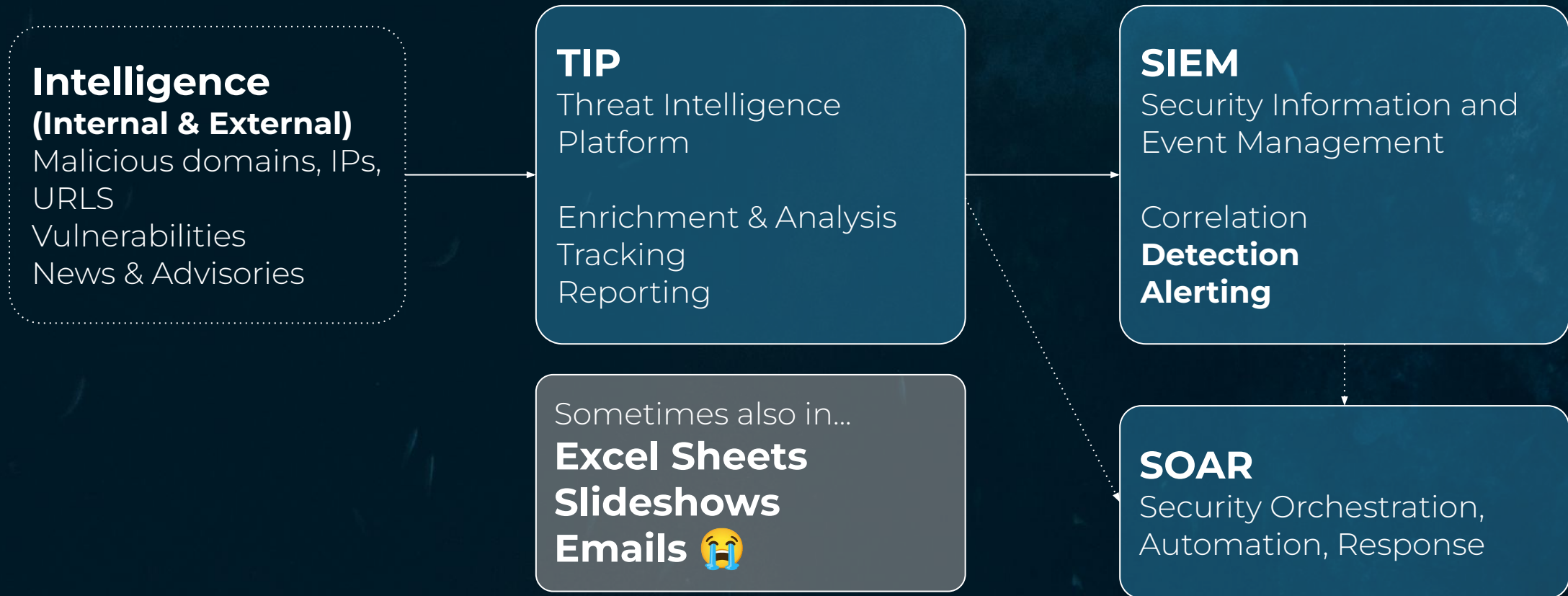


Dissemination & Feedback

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

- 👉 Who needs to know?
- 👉 What do they need to understand?

Example Flow



CTI Teams Today

CTI ON A
BUDGET



MATURE
FUSION CENTERS



Tell Me More...

Published in **Katie's Five Cents** · Feb 23, 2021

A Cyber Threat Intelligence Self-Study Plan: Part 1

There are many ways to learn. While some people prefer to have a live instructor in a course, others are great at doing self-study. I teach SANS FOR578: Cyber Threat Intelligence, which is a great course if you want to...

Intelligence 9 min read



Published in **Katie's Five Cents** · Aug 17, 2020

FAQs on Getting Started in Cyber Threat Intelligence

One of the most frequent messages I get is from people who are looking for advice on getting started in cyber threat intelligence (CTI). I thought it would be useful to compile my answers to some of the most frequently...

Cybersecurity 10 min read



CTI-fundamentals Public

A collection of papers, blogs, and resources that make up the quintessential aspects of cyber threat intelligence

☆ 241

🔗 16

CTI Theory

Author	Description	Resource URL
The US Central Intelligence Agency	The traditional Intelligence cycle describes how intelligence is ideally processed in civilian and military intelligence agencies, and law enforcement organizations.	the-intelligence-cycle.html
Recorded Future	The traditional intelligence life cycle tailored to threat intelligence embedded in modern security operations	What the 6 Phases of the Threat Intelligence Lifecycle Mean for Your Team



awesome-threat-intelligence Public

A curated list of Awesome Threat Intelligence resources

☆ 5.1k

🔗 1.1k

awesome-threat-intelligence

A curated list of awesome Threat Intelligence resources

A concise definition of Threat Intelligence: *evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.*

Feel free to contribute.

- Sources
- Formats
- Frameworks & Platforms
- Tools
- Research, Standards & Books

Katie's Five Cents: medium.com/@likethecoins

Curated Intel - CTI Fundamentals: github.com/curated-intel/CTI-fundamentals

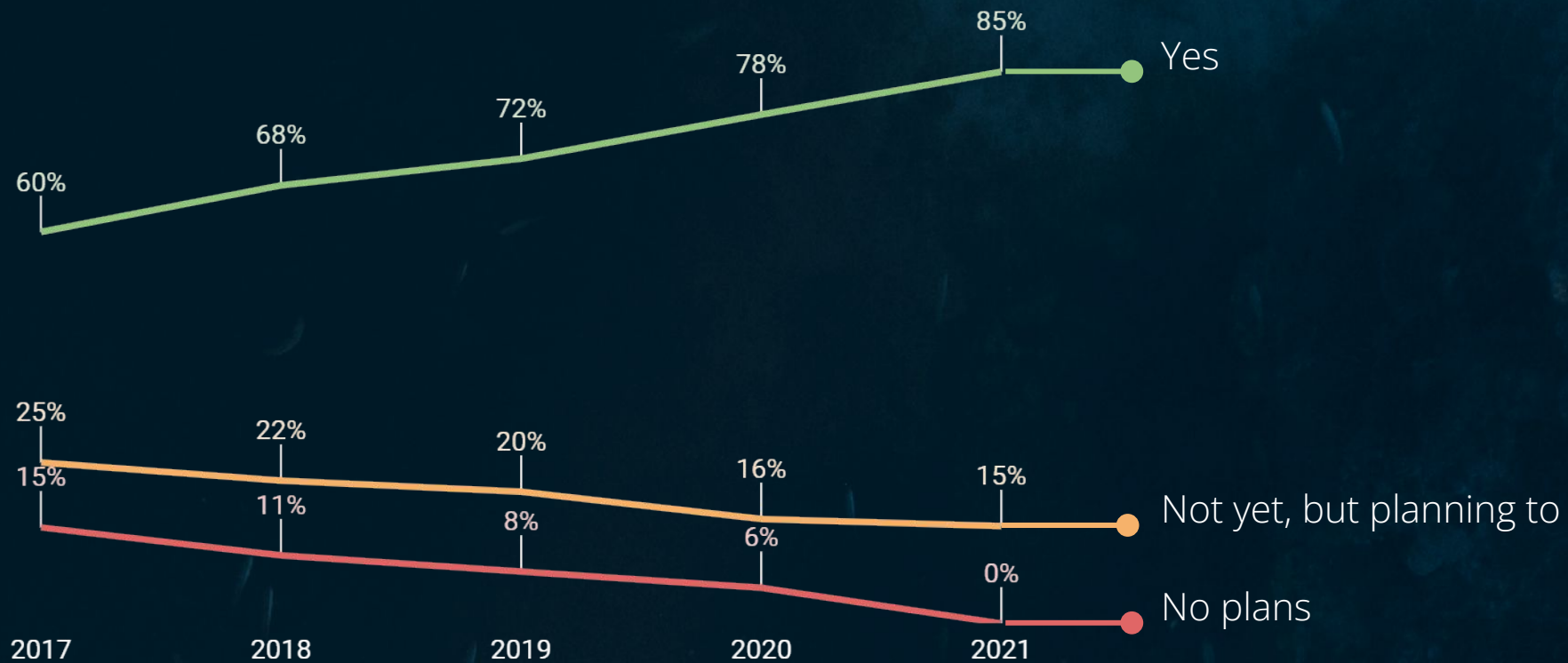
Awesome Threat Intelligence: github.com/hslatman/awesome-threat-intelligence

Mandiant CTI Analyst Core Competencies: <https://www.mandiant.com/sites/default/files/2022-05/cti-analyst-core-competencies-framework-v1.pdf>



Why bother?

Does your organization produce or consume CTI?



“[CTI Networking] is an untapped area for a lot of organizations... they are still very siloed when it comes to intelligence sharing.”

“Cross-[insert here] collaboration is essential!”

“We need better ways to share threat intelligence – safely”

“We’ll never get to our necessary level of threat intelligence awareness, landscaping, and forecasting capabilities if we’re always running around with our heads cut off AND our hands tied behind our back”



What I did

Benchmark



How different
methods stack up



How and why
individuals
participate



The role
organizations play

Method

1

Planning & Discovery

Purpose, scope, research

2

Collection

Survey distribution, word-of-mouth

3

Processing / Analysis

All the pivot tables, qualitative review

4

Dissemination

Report, blog, today's presentation

Survey on CTI Networking (2021)

[Sign in to Google](#) to save your progress. [Learn more](#)

Context

Security teams cannot sustainably operate in an intelligence silo. There's continuous discovery of how cyber threat intelligence (CTI) collaboration is key to proactive defense, collective response, and effective remediation.

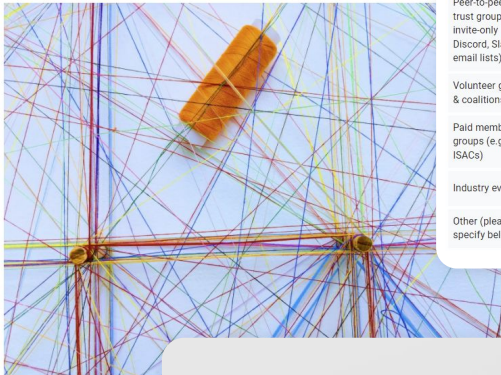
Yet, the enormity of it all can feel insurmountable to CTI professionals deciding how to effectively network "today". So what are they doing, and what works?

We're asking you to find out.

What kinds of CTI networking do you participate in? *

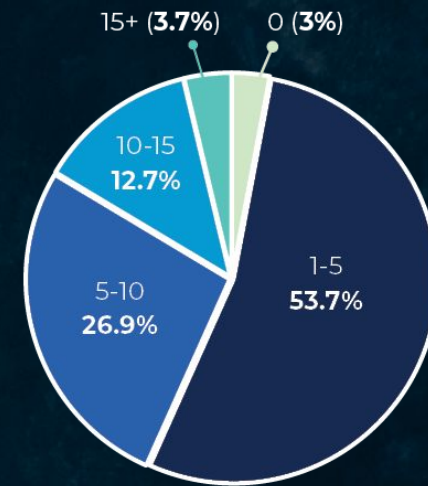
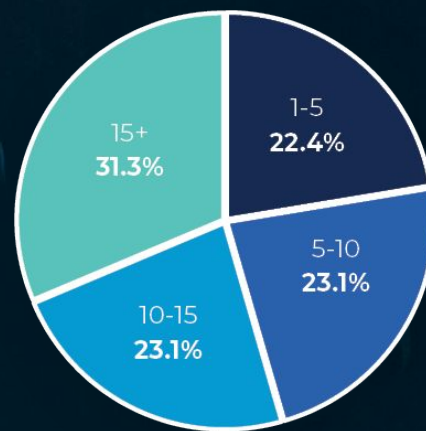
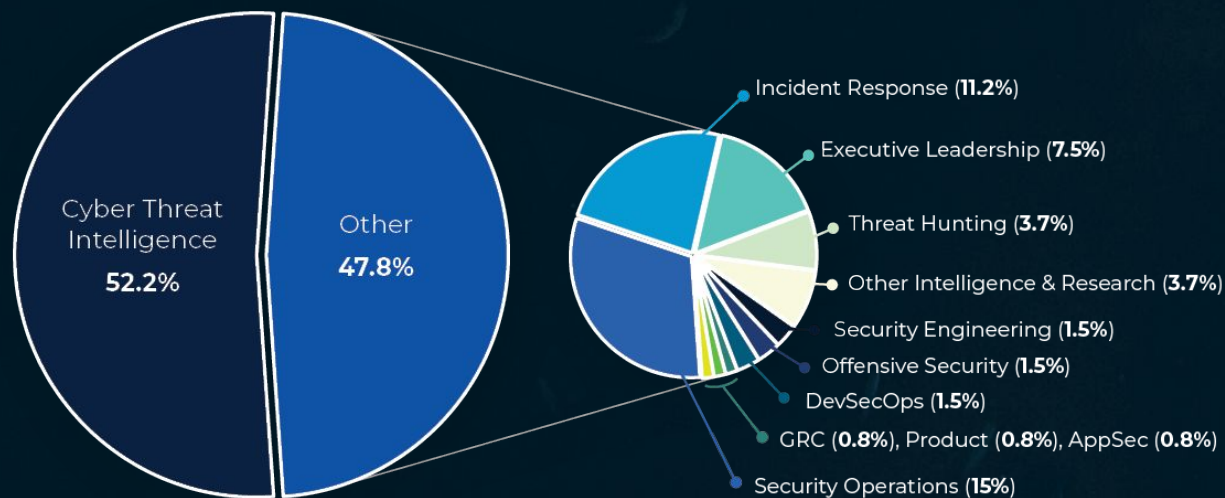
Note: Participation can be more than being present or "online", it can also include contributions in the form of planning, moderating, management, research and other work.

	Never	Rarely	Sometimes	Frequently	N/A
1-to-1 direct messages/emails	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social media & public forums	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dark web	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Peer-to-peer: free trust groups (e.g. invite-only Discord, Slack, email lists)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Volunteer groups & coalitions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Paid membership groups (e.g. ISACs)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Industry events	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other (please specify below)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Demographics

Mostly CTI and related roles
Even spread of *total* experience
Majority “newer to CTI”



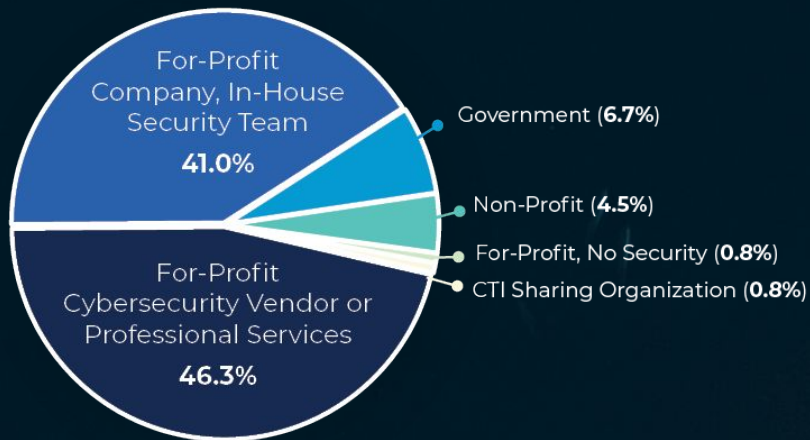
Demographics

Majority "for-profit"

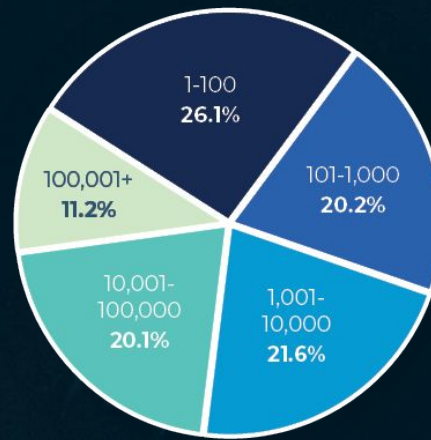
Even spread of organizational size

Strongest representation in North America and Europe

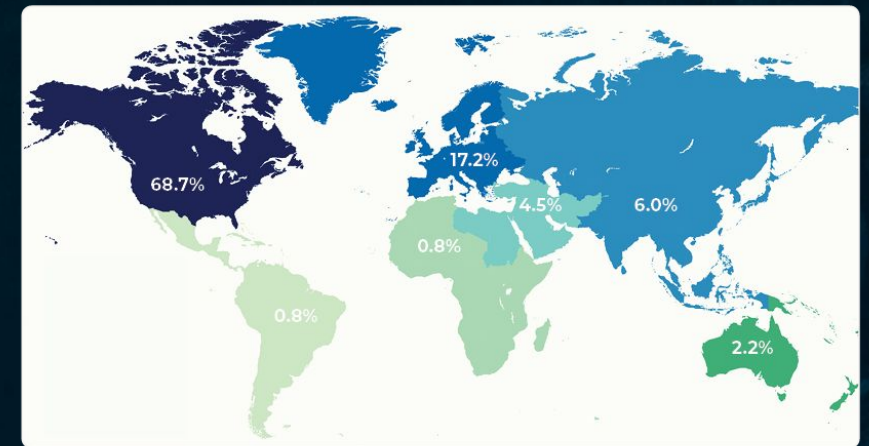
Operating in multiple regions globally



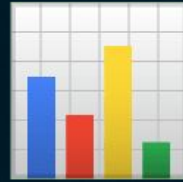
Employer Type



Org Size



Location



Findings

Satisfaction



Happy respondents

Extra boosts for smallest (<100) & largest (100K+) orgs

Dip at 10-100K size

Methods

There are no shortcuts to the strongest, most effective networks

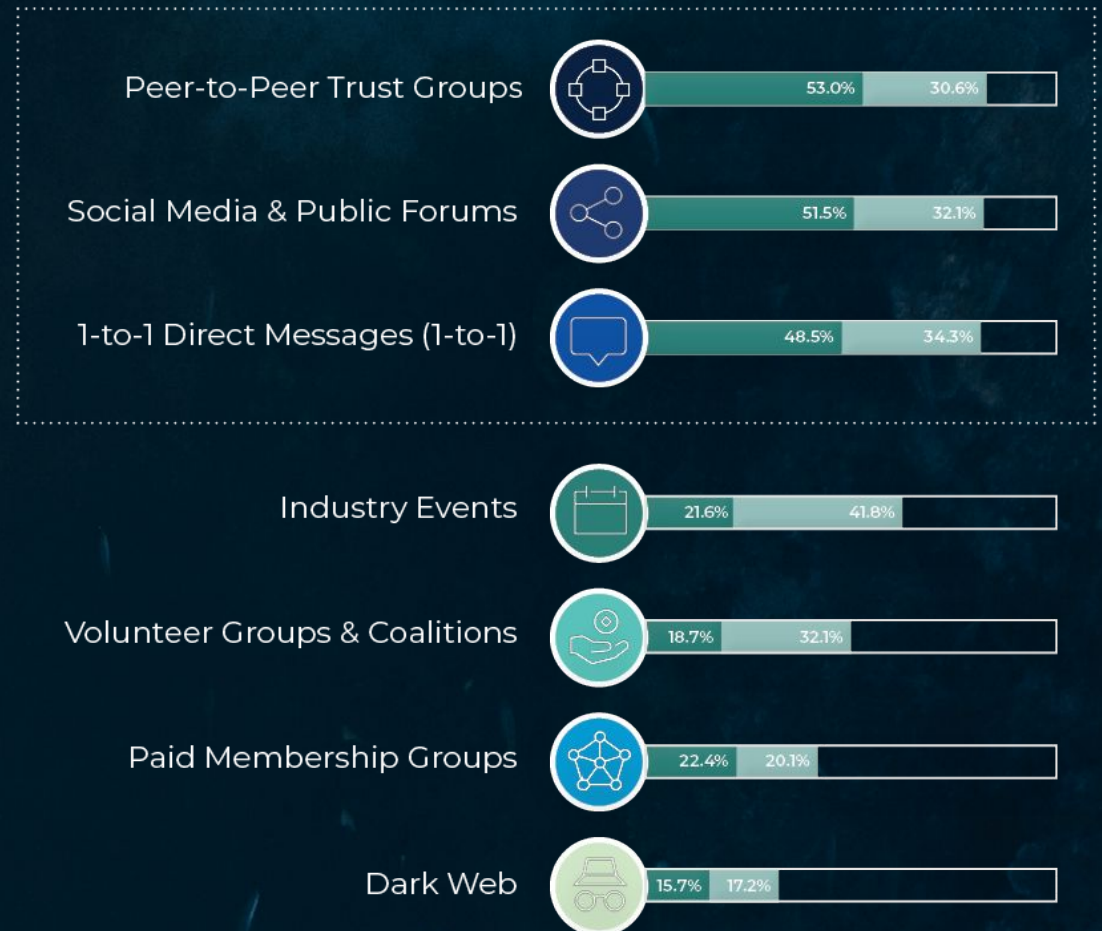
Free

Peer-to-peer

Based on personal reputation/contribution

How often do you participate in...

■ Frequently ■ Sometimes



Crowd Favorites



P2P Trust Groups, 1-to-1 DMs,
and Social Media* led the pack
across all respondent groups

Perception: valuable? high confidence?
timely? actionable?

Results: did it help prevent/detect an attack?
during? in remediation?

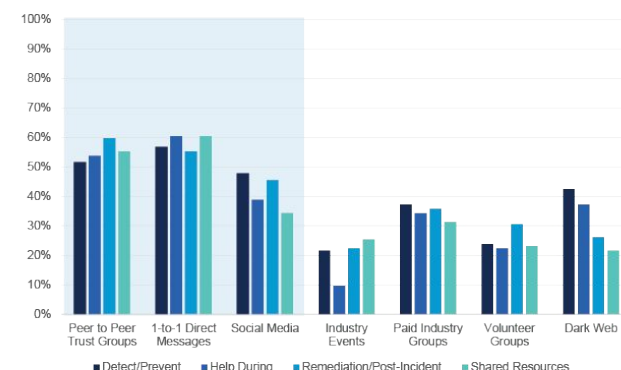
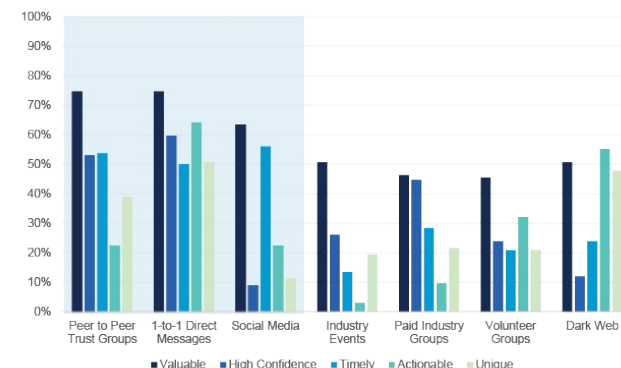
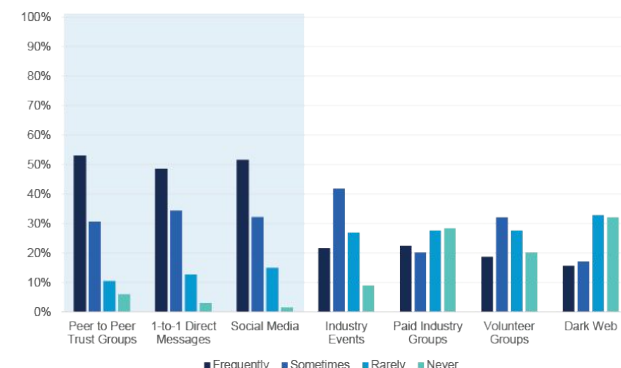
Participation



Perception



Results



Key Advantages

87%

Get valuable threat data

85%

Stay aware of what's
happening strategically

84%

Take proactive
measures

81%

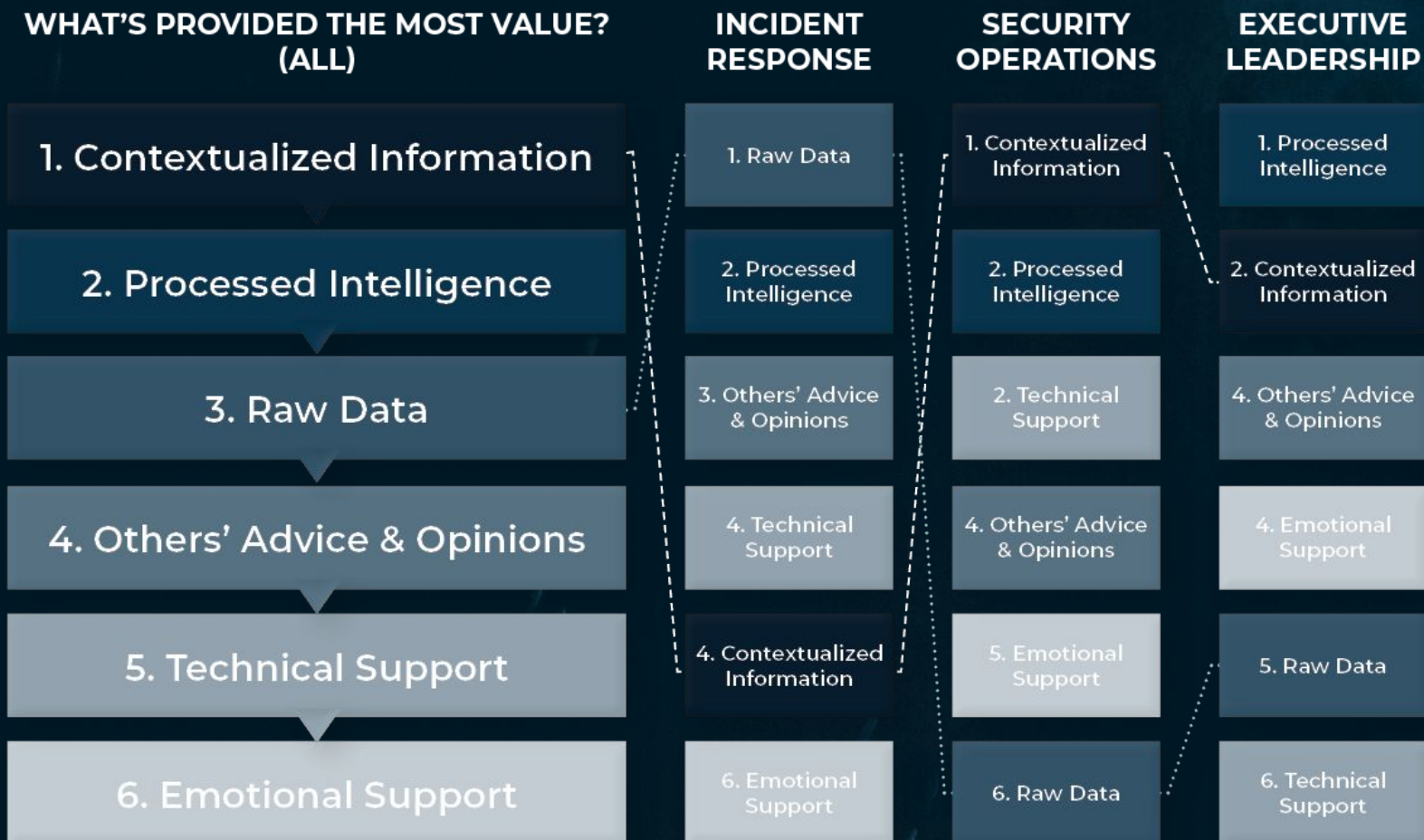
Find, vet, or understand
new sources & methods

Come for the access, stay for the awareness

Actionable, timely content

Data, information, intelligence

Highest Value



What matters most?

Depends whom you ask

- Primary function
- Years of CTI experience
- Size of organization

In Organizations

For now, it's (mostly) on you

Time and sharing restrictions

Limited reporting

Positive personal, neutral
organizational sentiments

Caveat: cyber orgs

Room to be more intentional,
inclusive, and strategic





Takeaways

**"CTI NETWORKING IS
IMPORTANT FOR TEAM
MEMBERS AT ALL LEVELS"**

91%

agreement



93%

agreement by respondents
with 10+ years of total
experience and with 5+ years
of CTI related experience

Importance

Highly recommended

Strongest consensus in survey

Don't be stopped by imposter syndrome

Take the advice of current practitioners...

- PARTICIPATE** “Start small” “Share what you can”
“Have both human (coffee, calls) and automated (IOC sharing) interactions”
“Don’t let impostor syndrome stop you from engaging”
“Get involved in a good community”
“Find and follow on social media those interested/working in your target areas”
- BUILD TRUST** “Be active, develop trust” “Don’t burn trust. Ever.”
“Get into top circles by contributing your own intel, don’t just regurgitate”
“Make sure your critical thinking and conclusions are based on sound principles!!!!”
“Provide value with a niche you’re experienced in”
“Hold yourself to the highest professional standards”
- AND ALWAYS** “Understand what your organization needs.”
STAY CAREFUL
AND STRATEGIC. “Be clear on use cases and intelligence requirements”
“Have a collection plan that includes sharing”
“Operationalize your efforts - data on the floor is useless”
“Trust, but verify” “Ensure who you network with is vetted”
“Be skeptical with data shared, but also be generous to those that share as it can take quite a bit of courage and can often be novel”
“Select trust groups based on impact” “If you’re struggling to find value early, move on”



Questions?

Closing Out



✉ grace@pulsedive.com

🐦 @euphoricfall

in /in/graceschi

<https://blog.pulsedive.com/cti-networking-report/>