CSNP

LEARN // INNOVATE // SECURE

Cyber Threat Intelligence & How Sharing is Caring

Grace Chi

June 30, 2022

👋 Introduction

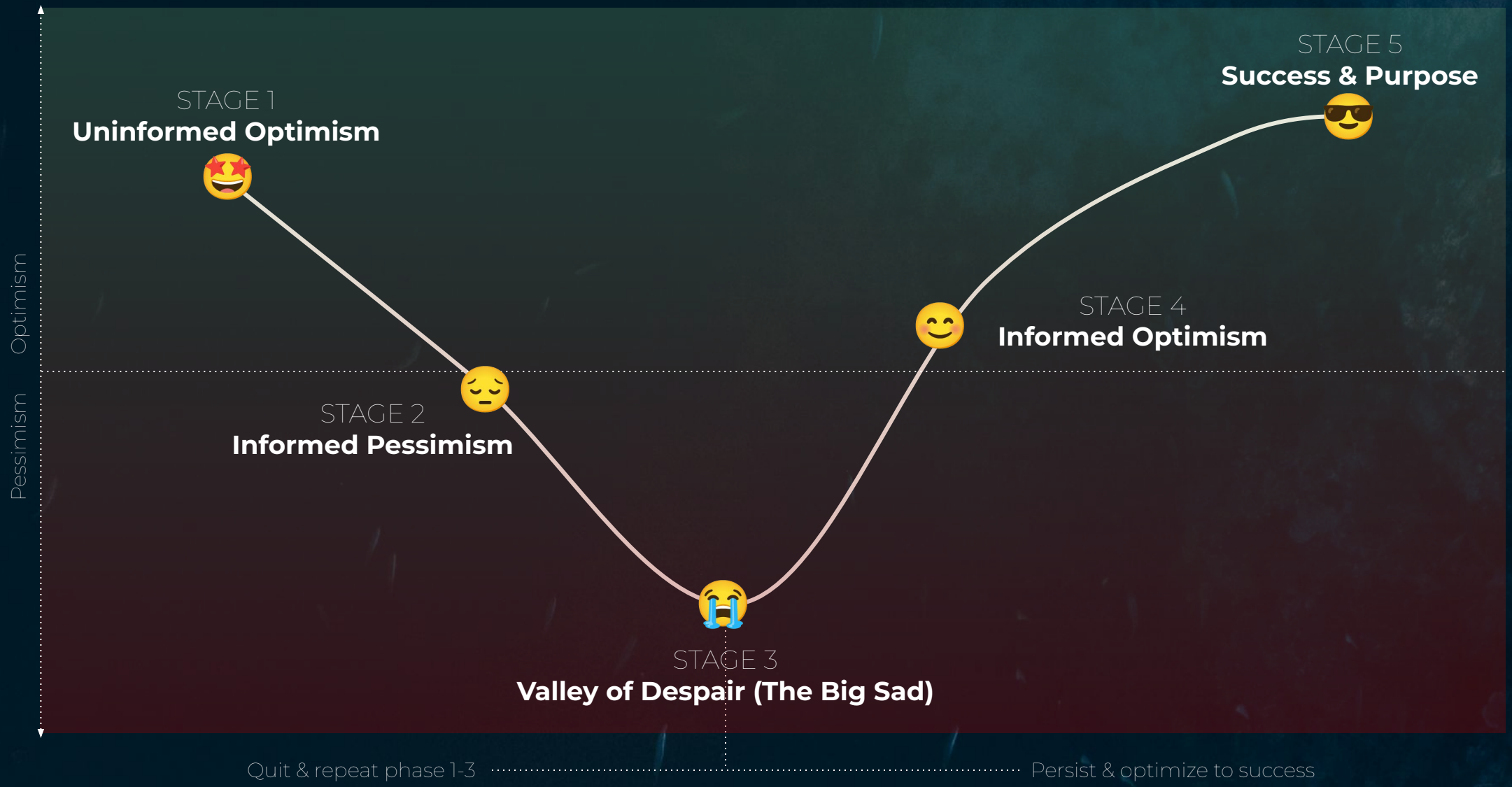

=

+

+


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

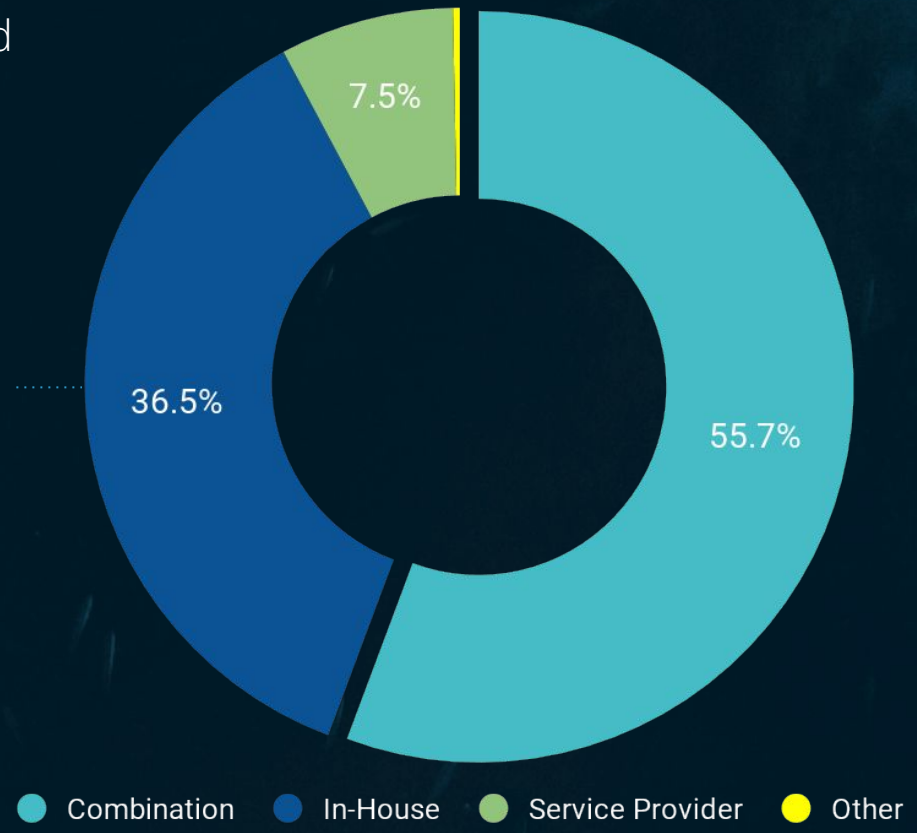
- ❌ A notebook with every threat group or APT
- ❌ Many, expensive feeds and tools
- ❌ Ingesting every indicator you can find
- ❌ OSINT all the things
- ❌ A dedicated team member or provider
- ❌ Set it and forget it

Data. Contextualized. Informing. Action.

Who & Where?

Organizations have formal, dedicated teams or shared responsibilities across security groups

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

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

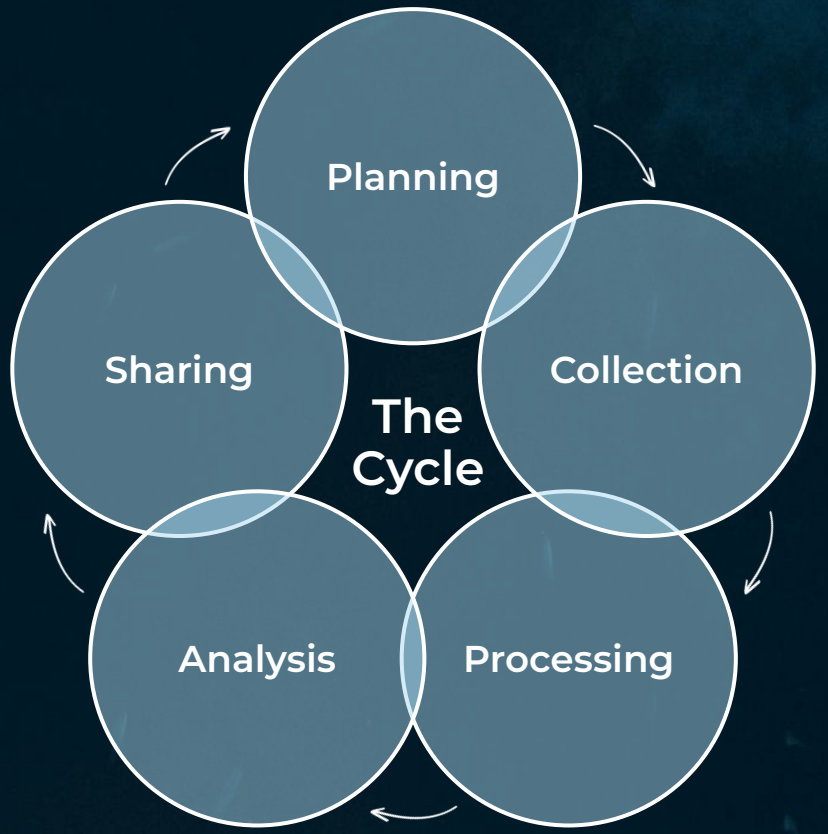
Technical Research

Scripting

Digital Forensics

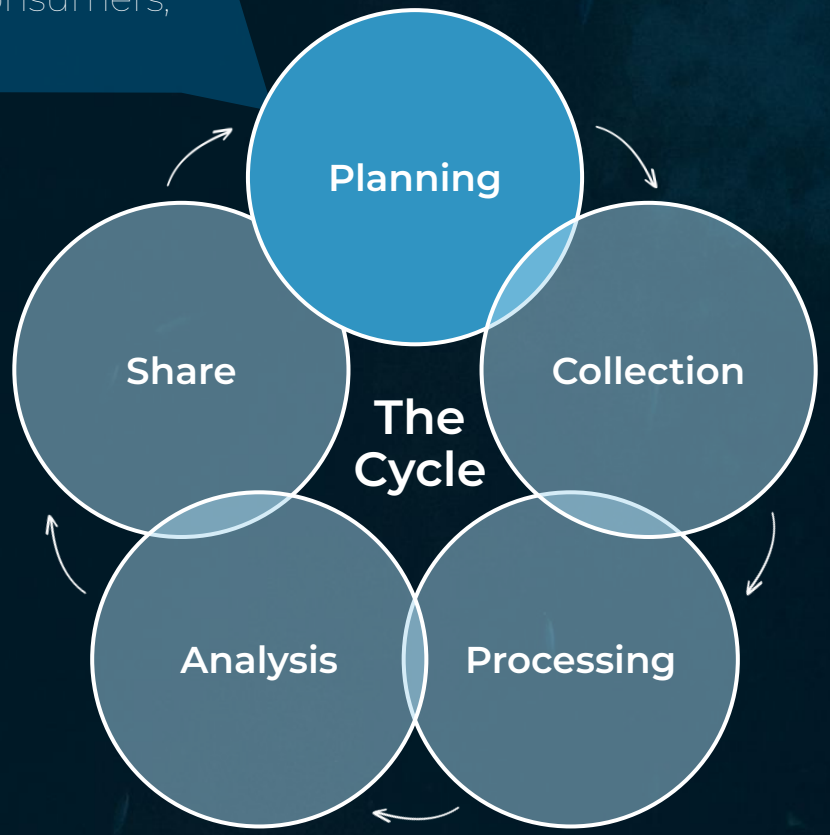
Data Analysis

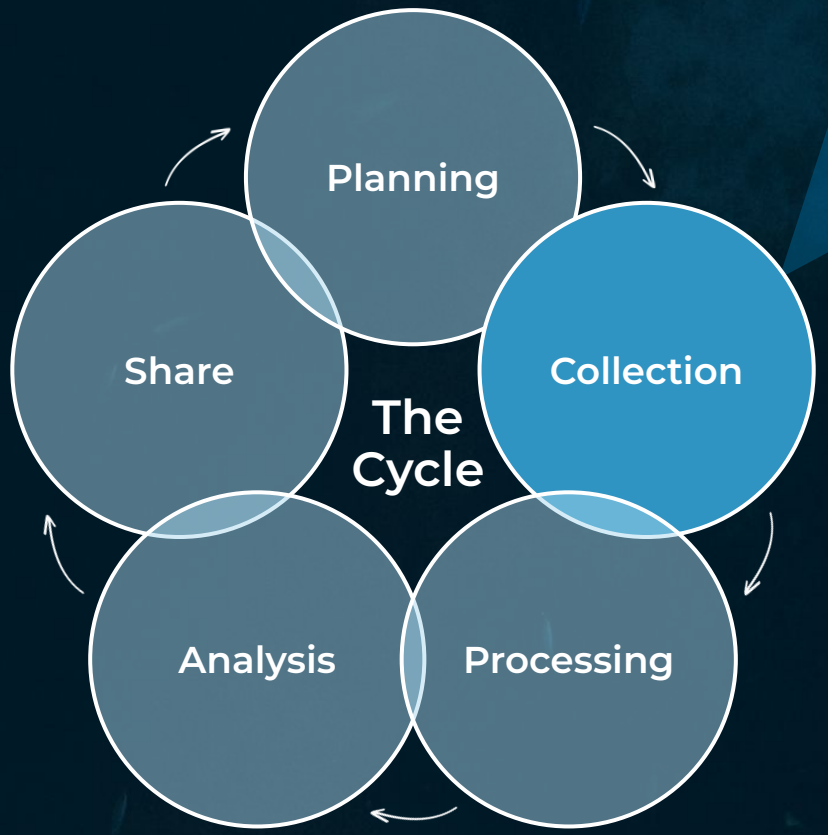
Intelligence Cycle



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?



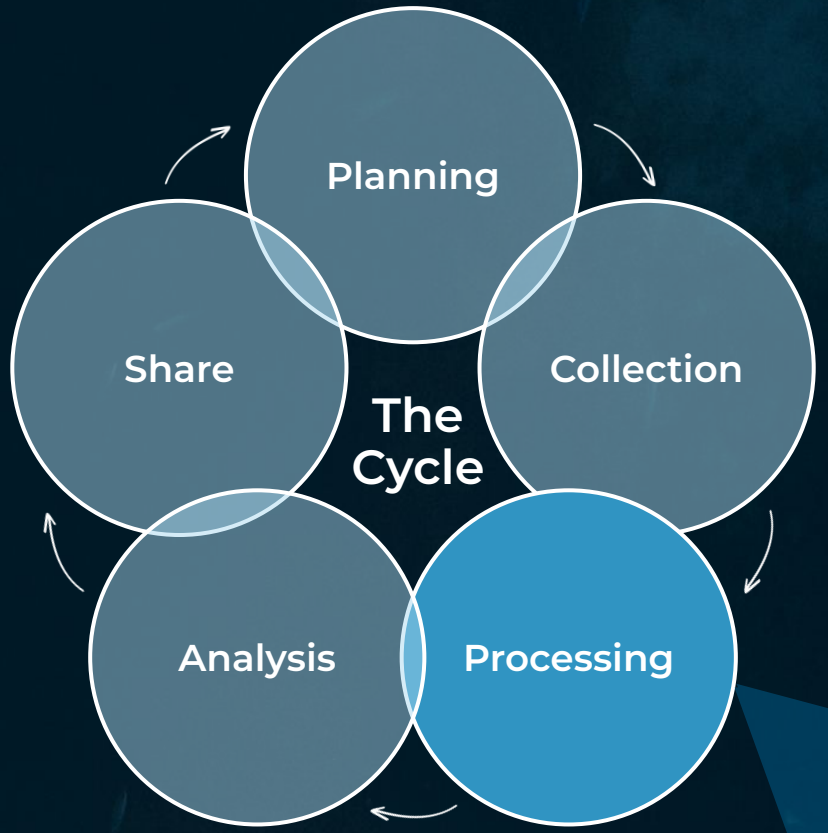


Internal & External Sources

Network logs, past incidents, risk analysis reports

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

👉 What data do we need, from where?



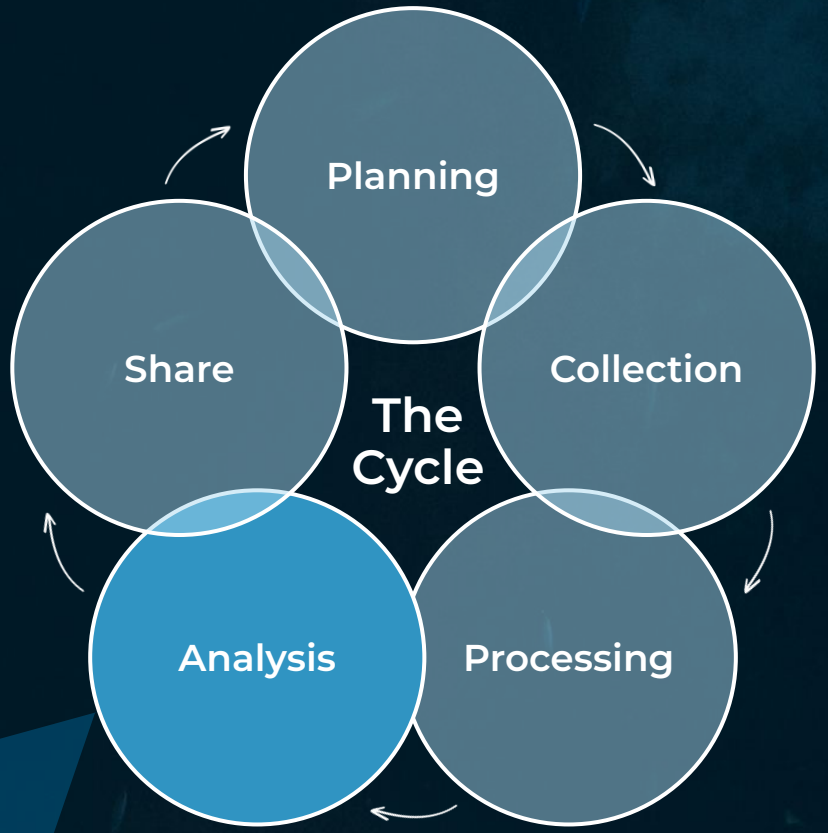
Enrichment & Contextualization

OSINT engines, scanning, lookups, web tools, footprinting

Counterintelligence, honeypots, sinkholes, YARA rules

Human intelligence, social engineering

👉 What's the bigger picture here?

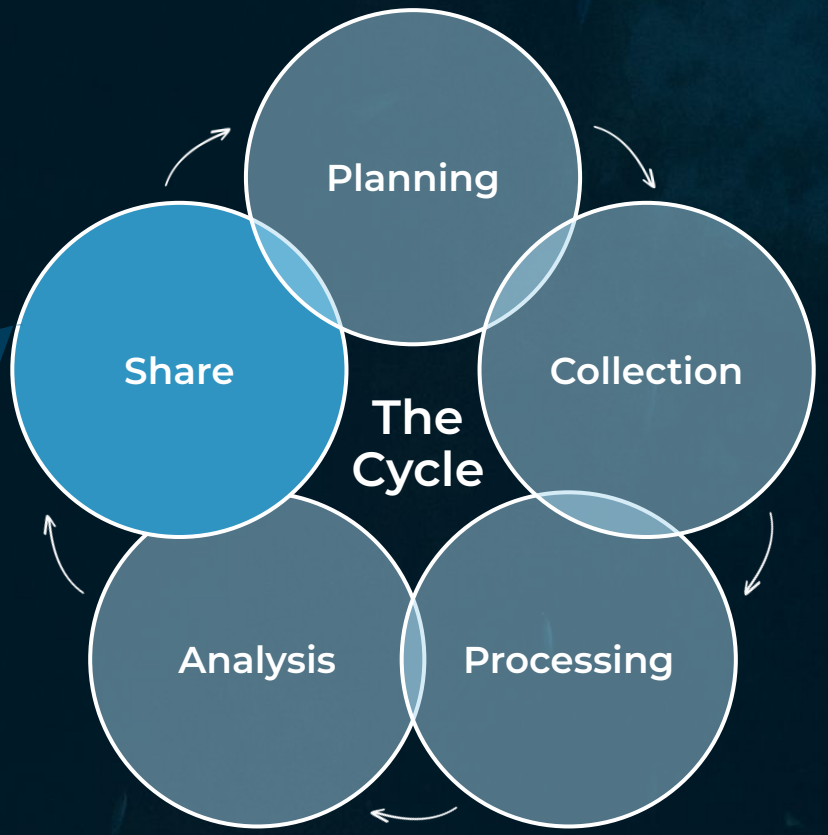


Analysis & Intelligence Creation
Motives, targets, behavior, impact
Actionable reports and informed narratives to protect orgs, inform decision-making and next steps

👉 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

Open Source

Dark web

Internal

External

Historical

Integrations

Enrichment

Managed CTI

Services

Finished Reports

Commercial

Management Platforms

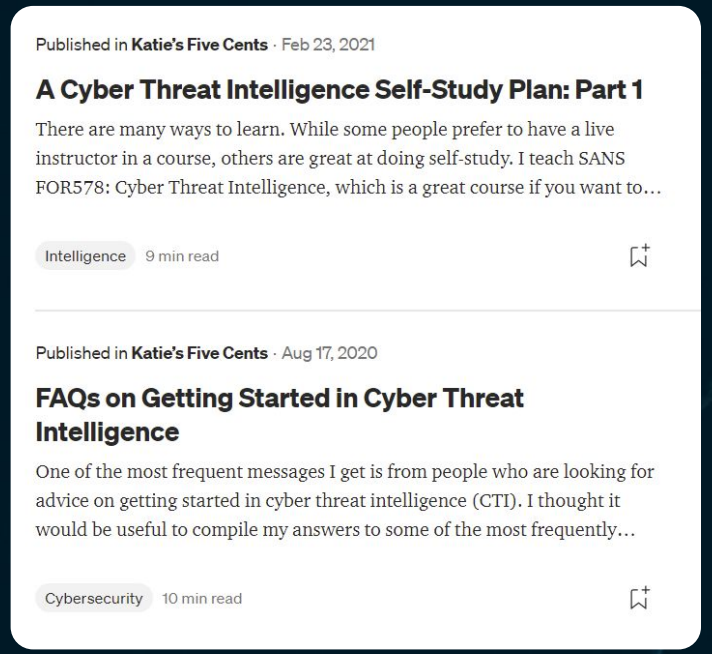
Automation

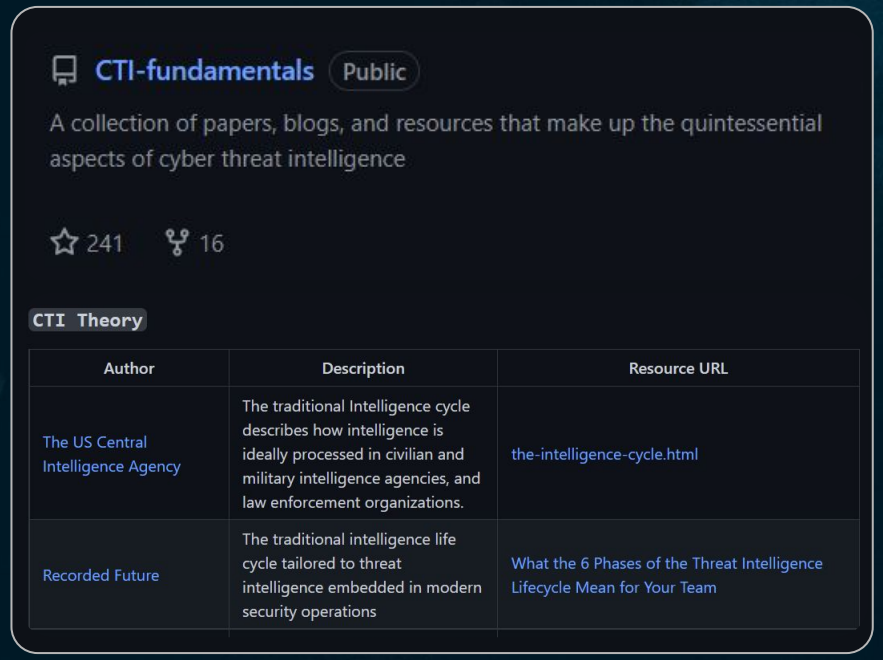
Feeds

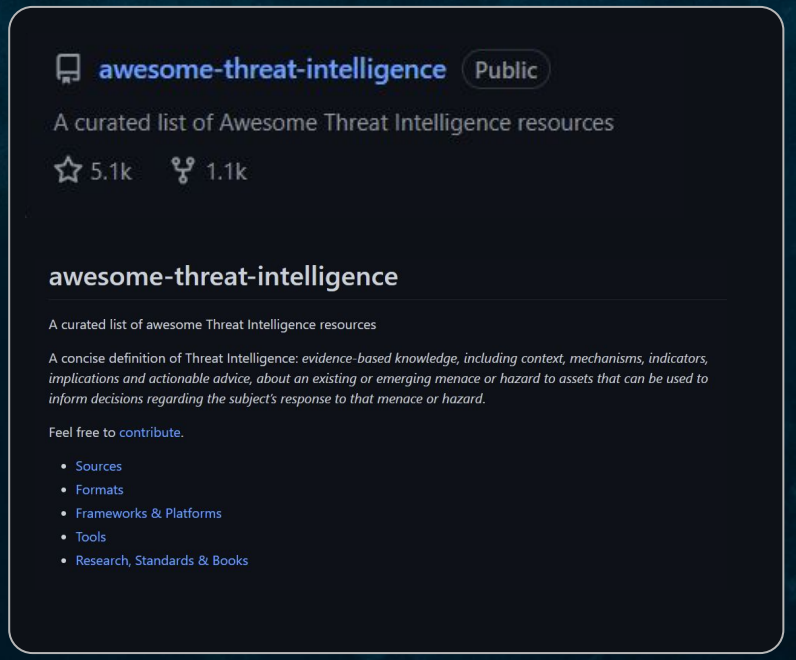
Niche Solutions

Sector, Geography, Technology

Tell Me More...



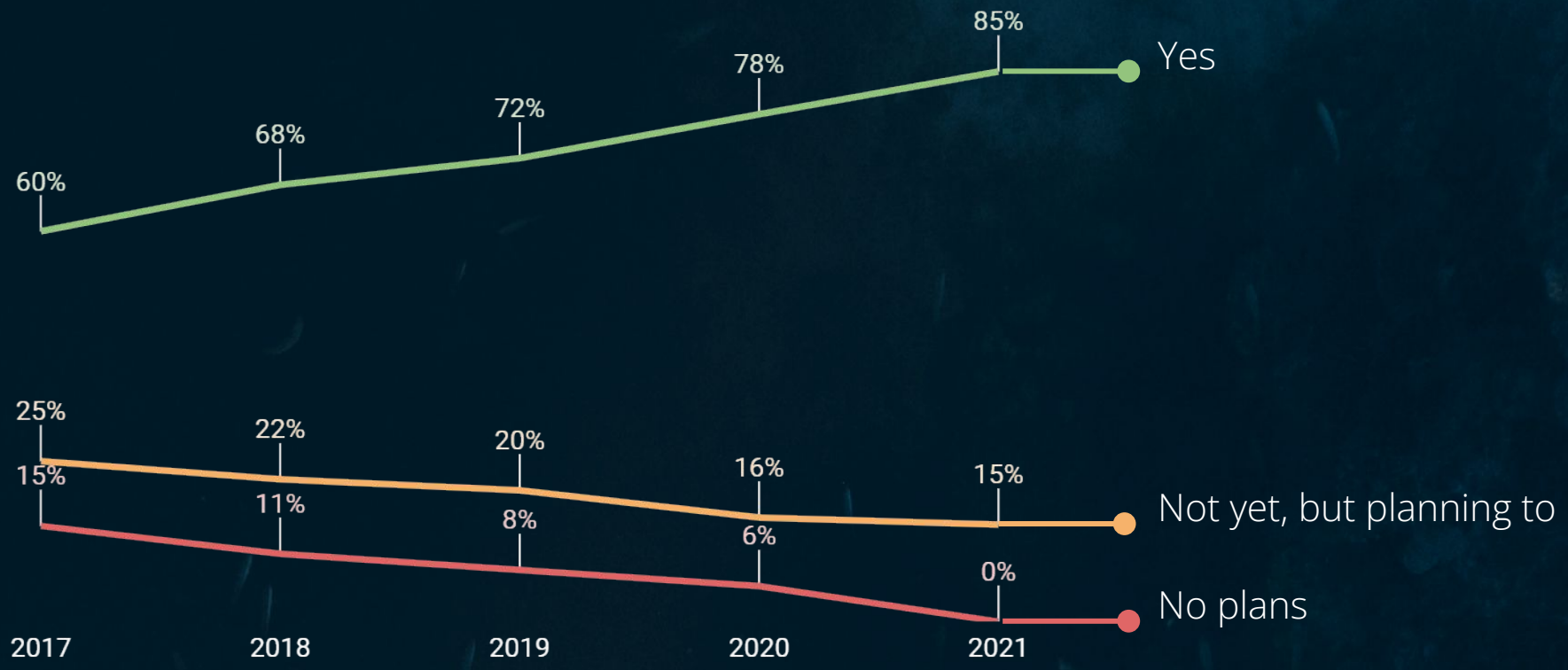




Katie's Five Cents: medium.com/@likethecoins
Curated Intel - CTI Fundamentals: github.com/curated-intel/CTI-fundamentals
Awesome Threat Intelligence: github.com/hslatman/awesome-threat-intelligence
Mandiant CTI Analyst Core Competencies: https://www.mandiant.com/sites/default/files/2022-05/cti-analyst-core-competencies-framework-v1.pdf

Why bother?

Does your organization produce or consume CTI?



SANS Institute, 2021 CTI Survey

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

"We need better ways to share threat intelligence – safely"

"Cross-[insert here] collaboration is essential!"

"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"

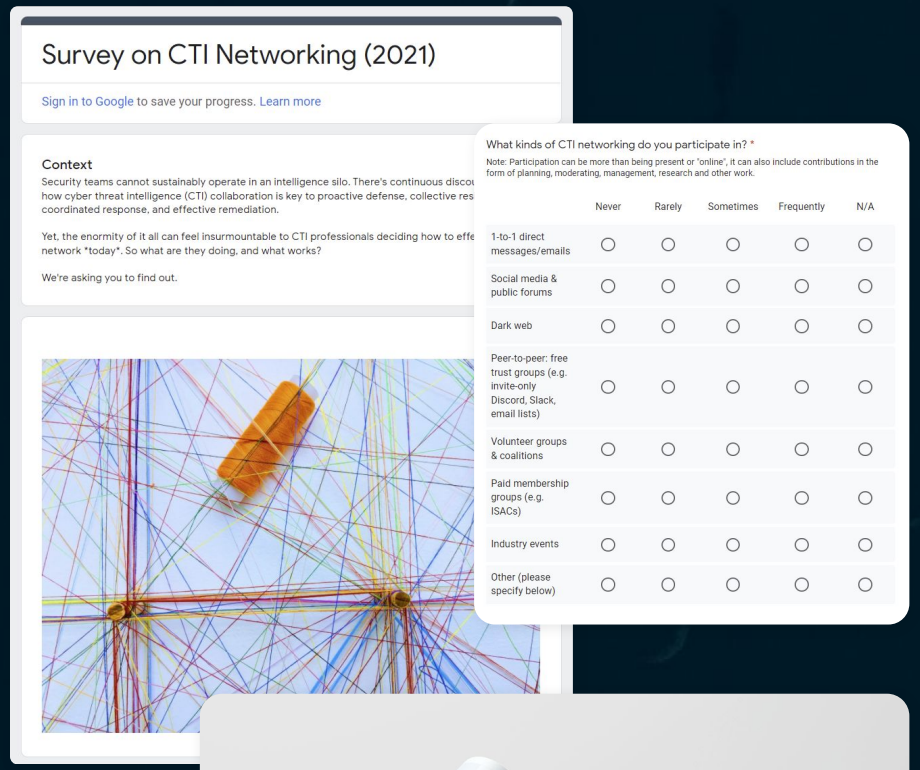
What I did

Benchmark

How different methods stack up

How and why individuals participate

The role organizations play



Method

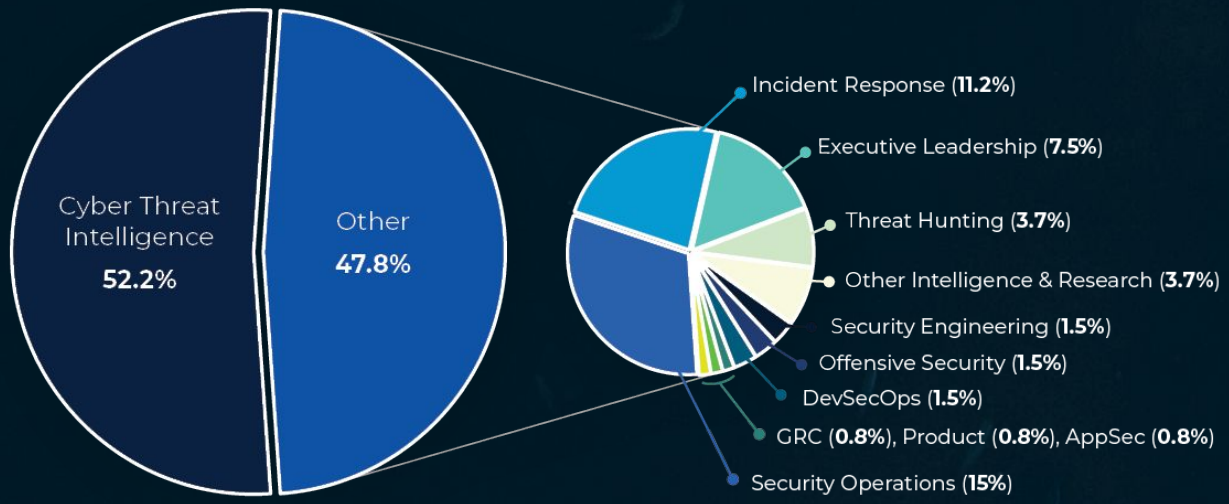
1. **Planning & Discovery**
   Purpose, scope, research
2. **Collection**
   Survey distribution, word-of-mouth
3. **Processing / Analysis**
   All the pivot tables, qualitative review
4. **Dissemination**
   Report, blog, today's presentation

Demographics

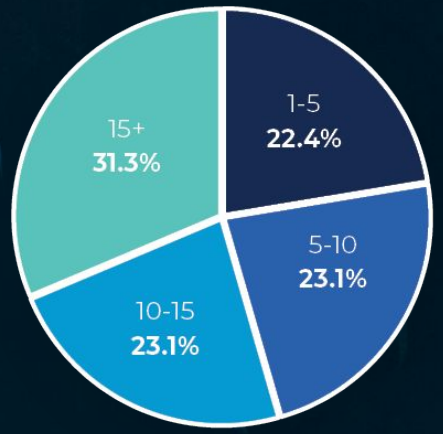
Mostly CTI and related roles

Even spread of *total* experience

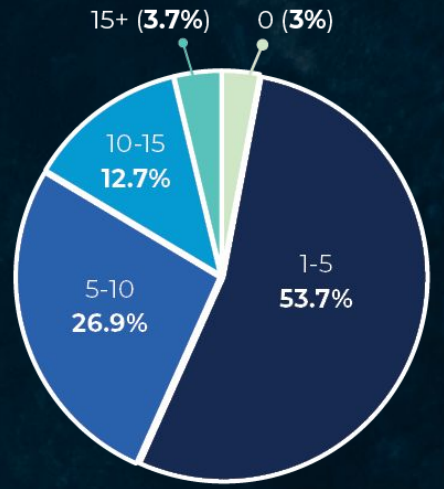
Majority "newer to CTI"



Primary Role



Years Experience



Years CTI Experience

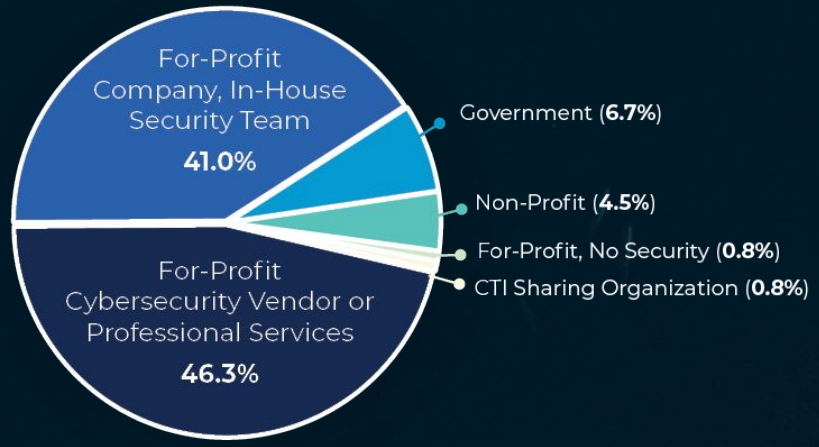
Demographics

Majority “for-profit”

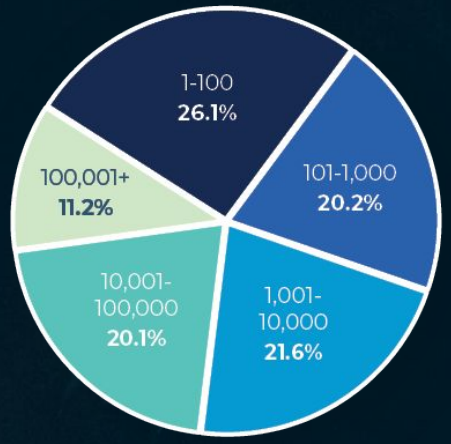
Even spread of organizational size

Strongest representation in North America and Europe

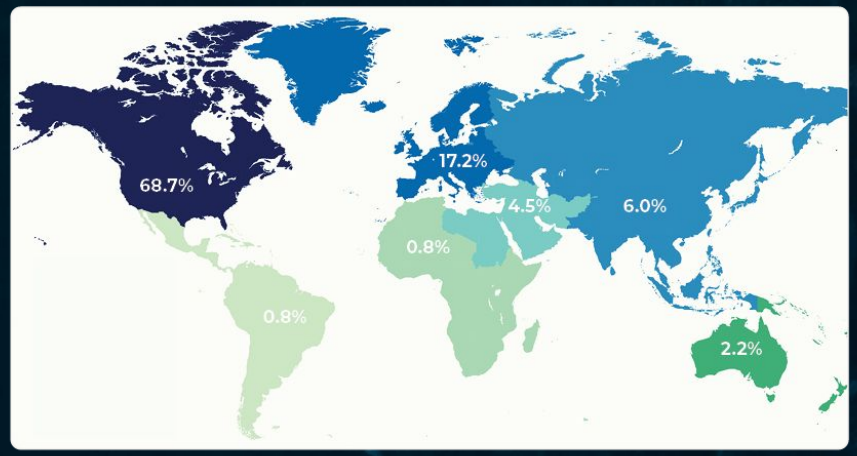
Operating in multiple regions globally



Employer Type



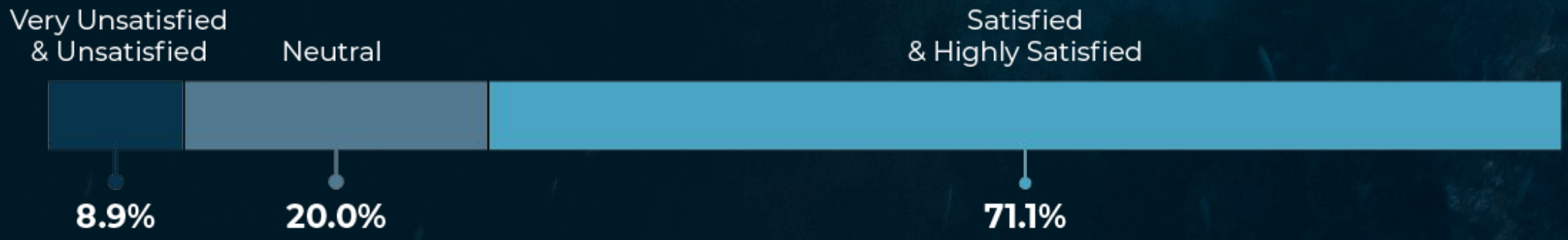
Org Size



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

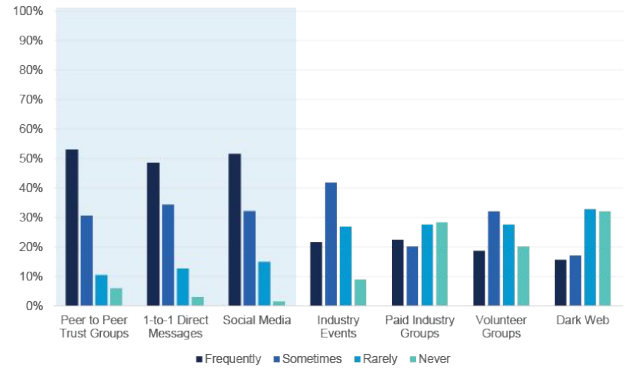
Crowd Favorites

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

Perception: valuable? high confidence? timely? actionable?

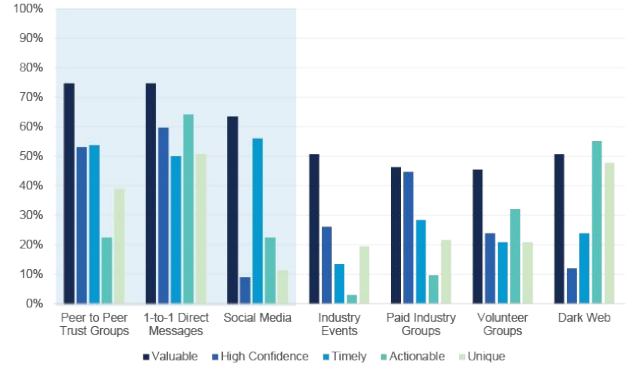
Results: did it help prevent/detect an attack? during? in remediation?

Participation



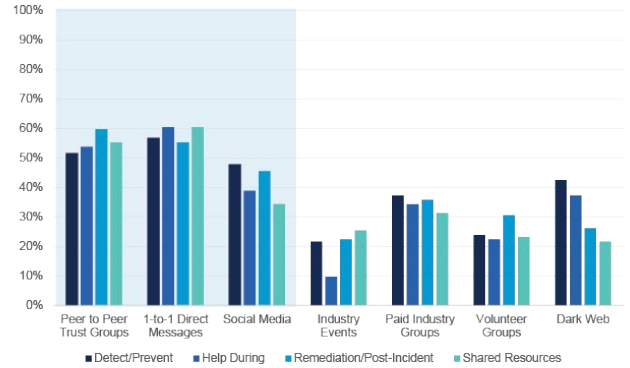
×

Perception



×

Results



Key Advantages

87% Get valuable threat data

85% Stay aware of what's happening strategically

84% Take proactive measures

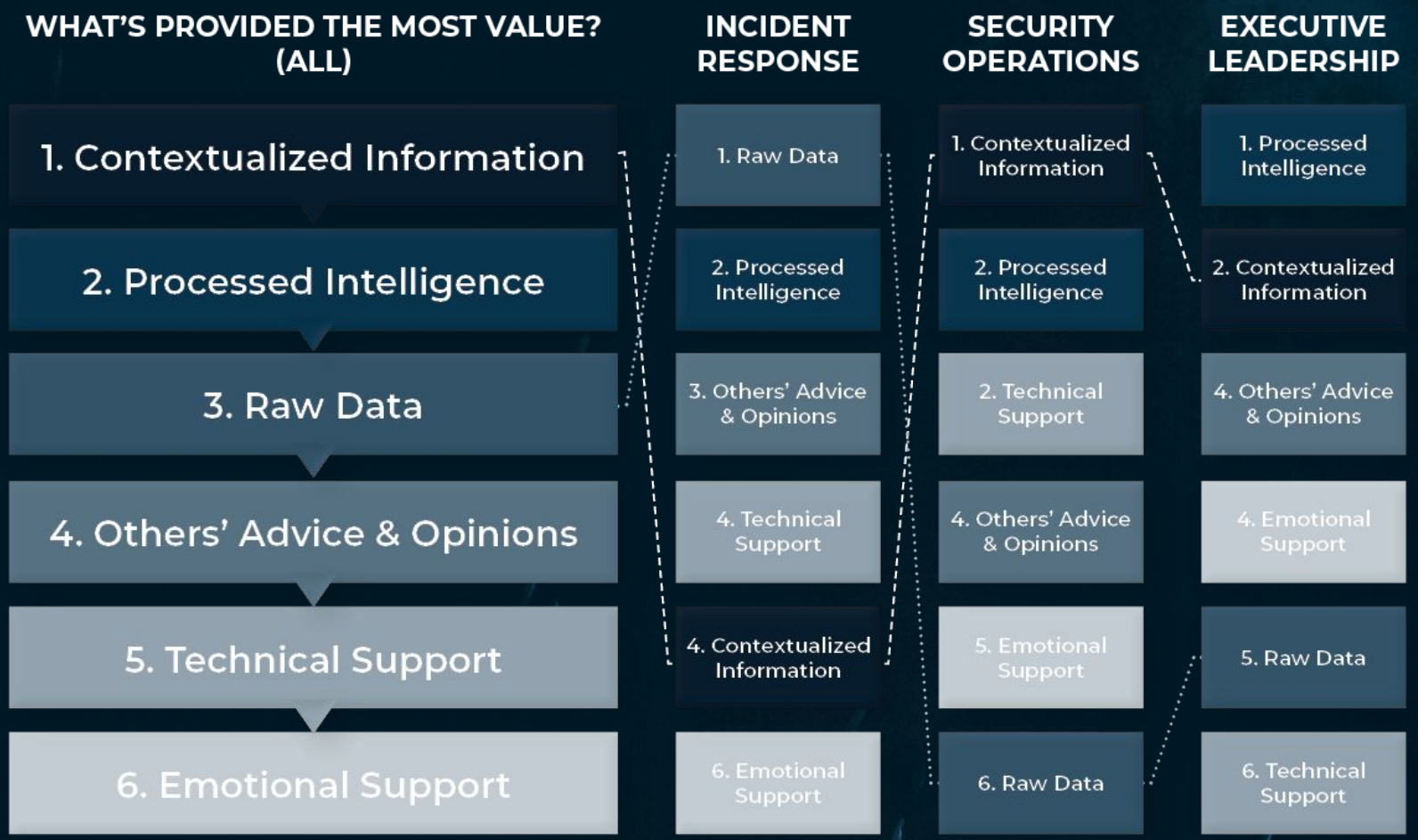
81% Find, vet, or understand new sources & methods

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 STAY CAREFUL AND STRATEGIC.

"Understand what your organization needs."

"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

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

grace@pulsedive.com
@euphoricfall
/in/graceschi