



SHARING, COMPARED

A Study on the Changing
Landscape of CTI Networking



JANUARY 2024

GRACE CHI

INTRODUCTION

Cyber threat intelligence (CTI) is an evolving field, with an industry-wide consensus that teams cannot effectively operate in an intelligence silo. This sentiment is shared across all stakeholder segments – public, private, vendor, and academic. In support of improved CTI sharing, stakeholders have invested in efforts around cross-boundary collaboration, technical standardization, managing trust, and reporting best practices. However, understanding the time and effort spent in CTI networking (i.e. connecting human-to-human for improved business outcomes) is often overlooked.

In 2022, I published the [inaugural study on CTI networking](#) with a core hypothesis:

CTI networking is an **afterthought** in practice, in spite of its demonstrated impact as a vital asset.

Two years later, I sought to understand what's changed – and what hasn't. After making a few tweaks based on feedback, I reached out directly to practitioners to capture their CTI networking experiences. While the first survey demystified how and where professionals were spending their time collaborating, this survey aimed to build on those [initial findings](#) to:

- Revisit the perceived and demonstrated value of CTI Networking
- Highlight significant changes in behaviors and attitudes
- Dive deeper into mapping how practitioners can most effectively network today, individually and within their teams

My goal in openly sharing this knowledge is to encourage intentional, inclusive, and strategic approaches in the community. A massive thanks to all who contributed and supported this project over the years, and to everyone reading the report right now.

CTI Networking: The interaction of individuals for the purpose of CTI-related work. This excludes personal purposes (e.g. career development, sales and commercial interest).

Who is this report intended for?

- Management responsible for security program strategy to gain awareness on advantages, challenges, and best practices
- CTI practitioners looking to optimize their networking efforts and understand peer experiences
- Security and intelligence professionals in related fields seeking to expand involvement in CTI areas
- Professionals entering or pivoting into CTI careers, to demystify what it means and how to participate

By Grace Chi

With support from the CTI community and Pulsedive



CONTENTS

Executive Summary	4
Methodology	5
Demographics	6
Insights	12
▪ The Value of CTI Networking	12
▪ Execution	19
▪ Areas for Improvement	25
Where Do We Go?	33
Appendix	40
▪ Survey	41

ACKNOWLEDGMENTS

A huge thanks to all the supporters of this report, including but not limited to:

- _John_Doyle
- AaronCTI
- Apurv / @ASG_Sc0rpi0n)
- B.A.Y.O
- B4nd1t0
- Bidemi "Bid" Ologunde
- Cabve
- chonda
- Cimabue
- daguy666
- Dan Sherry
- Frans anthony
- HellOnAStick
- HGB
- James Brine
- Jason Baik <3
- jax_are_better
- Jen Kwas
- John Fokker
- Kaiden McGuire
- Kellyn Wagner Ramsdell / @bookishzinia
- Mike Moran
- Not2Day0Day
- Rebecca Ford
- rectifyq
- Riccardo Stoppani
- Stef Collart
- SwitHak
- techelek
- Thomas Roccia / @fr0gger_
- Umar Javed (CyDefOps)
- Will Baxter, SME @ Team Cymru
- Vladimir Janout
- And more who wished to remain anonymous.

EXECUTIVE SUMMARY

In the two years since the previous survey, so much has changed within the field of cybersecurity: seemingly endless vulnerabilities, high profile campaigns, threat infrastructure take-downs, and regulatory guidance/enforcement. Simultaneously, the world at large has undergone international conflict, easing pandemic restrictions, economic recession fears, social media drama, and more. In spite of these changes, our research uncovered a steadfast core of general beliefs and behaviors around CTI networking, with a few focused areas of change.

KEY FINDINGS

- **Practitioners Make an Honest Effort To Get Ahead.** The belief in CTI networking value remained persistent, and the benefits received increased over the previous survey. While responses were mixed on the ease of finding and balancing efforts, consensus remained on its importance for team members at all levels and desire to find more peers.
- **The Ultimate Goal Remains: Unlock 1-to-1 & P2P.** Survey responses demonstrated a strong preference for 1-to-1 Direct Messaging and Peer-to-Peer Trust Groups. Data suggests that engaging in Paid Membership Groups, Industry Events, Volunteer Groups and Social Media & Public Forums were complementary in nature, helping provide highly desired access for the two highest valued, but more private methods.
- **Networking Gains Visibility, But With More Restrictions.** Numerous organizational challenges came to light, like issues of legal liability, a lack of formalized processes, and gaps in measuring effectiveness. In spite of these negative forces, respondents maintained their hours spent in CTI networking efforts. They even improved visibility with leadership.
- **A New Roadmap for Success: Start, Evaluate, Optimize.** Based on trends in qualitative responses and data insights, a brand new guide introduces how to engage in more intentional, inclusive, and strategic CTI networking. The roadmap consists of three phases: 1) Start - Broaden and Build Out, 2) Evaluate - Narrow and Focus, and 3) Optimize - Validate.

“ [N]etworking helped **confirm or validate sources, processes, or information**. A couple of times, we had **just-in-time warnings** or information that helped us prepare for something bad.”

“ Due to CTI networking and building trust, we were tipped off that a third-party vendor...had been compromised and a connection into our network was also compromised.

We were able to **get ahead of the threat** as I was the direct conduit to our IR team due to that relationship I had built.”

“ Most of what I know started with a **discussion with others.**” *

*Open-ended responses from survey respondents about the results of networking, edited for anonymity.

METHODOLOGY

In order to understand the current state of CTI networking, we reached out directly to CTI professionals to share their experiences with us.

Quantitative data was collected through a Google Forms survey.¹

Qualitative data was gathered in open-ended survey questions, as well as 1-on-1 interviews conducted via chat messages, phone calls, and video calls. Several responses are included as quotes, edited for anonymity and grammar, throughout this report.

The survey contained ~75 questions and five open-ended prompts. The survey required no PII to submit a response and no material compensation or reward was offered.

Number of quantitative respondents: 90²

Number of qualitative respondents: ~75

Responses collected: September– November 2023

Additional analysis in this report includes segmentation by:

- Organization size and type
- Primary job function (CTI or other)
- Years of security-related work experience
- Years of CTI-related work experience

Survey on CTI Networking (2023 Sequel)

Context

This survey is a follow-up to my 2022 research and report benchmarking cyber threat intelligence networking practices, results, and attitudes.

Full 2022 Report: [Is Sharing Caring?](#)

SANS 2022 [CTI Summit Presentation](#)

Purpose

Security teams cannot sustain discourse around how cyber defense, collective resilience

Yet, the enormity of it all can effectively network "today", effective, and gaps. Now, we

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

Scope

This survey should be taken year of professional experience

"CTI Networking" is defined work. This definition "excludes development (e.g. get a new

Survey responses will be an current CTI networking and contact information at the end or shared with anyone else.

Methods


For clarification, here are examples of each method:

- **1-to-1** - direct messages, emails, calls, meetings
- **Peer-to-peer** - free invite-only trust groups, e.g. Discord, Slack, Telegram
- **Paid membership groups** - ISACs, committees
- **Volunteer groups & coalitions** - groups with shared non-profit objectives
- **Social media** - e.g. Reddit, Mastodon, Twitter, LinkedIn
- **Industry events** - meet-ups, seminars, conferences, expos
- **Dark web** - forums, markets
- **Community platforms** - public tools where users can share and ingest information
- **Other** - anything not included above (please explain if you choose this)

What kinds of CTI networking do you participate in? *

Note: Participation includes anything more than being present or "online" (passive lurking does not count). Participation may include contributions like planning, moderating, management, research, and automation.

	Never	Rarely	Sometimes	Frequently	N/A
1-to-1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social media	<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 trust groups	<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	<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"/>
Community platforms	<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"/>



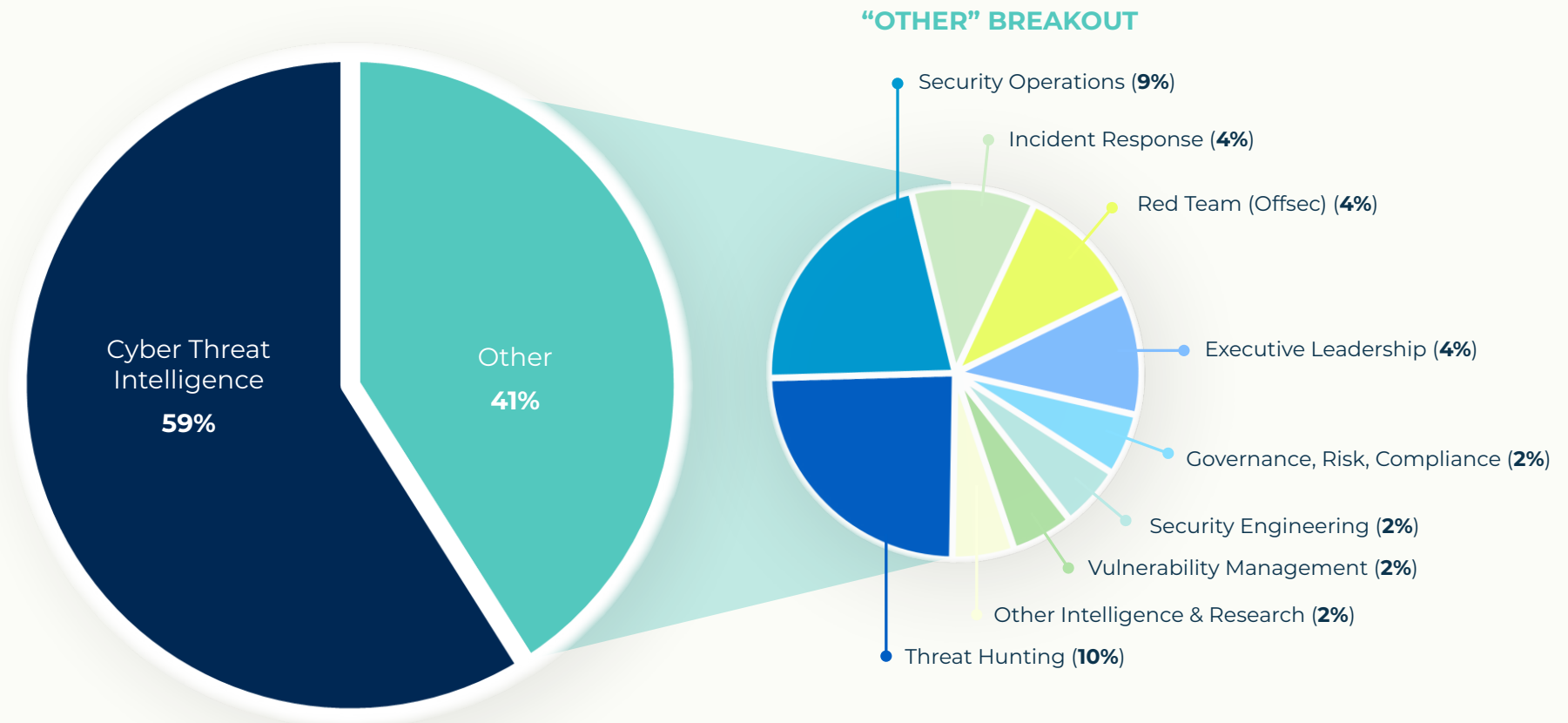
¹ A copy of the survey can be found in the **Appendix**.

² **Disclaimers:** The respondents represent a small fraction of the industry. Insights are directional and results are not statistically significant.

DEMOGRAPHICS

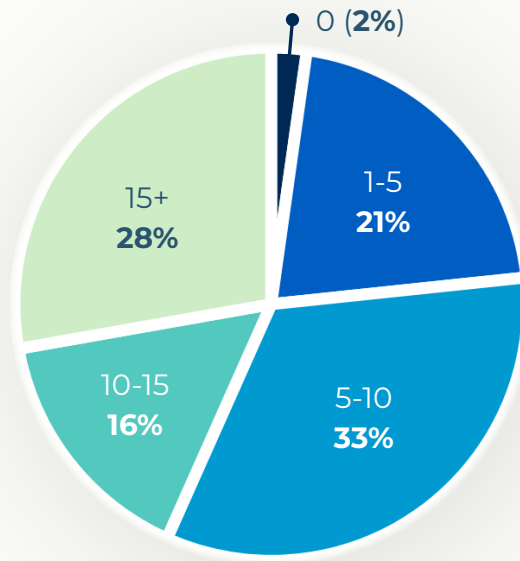
Who Responded to the Survey

PRIMARY JOB FUNCTION

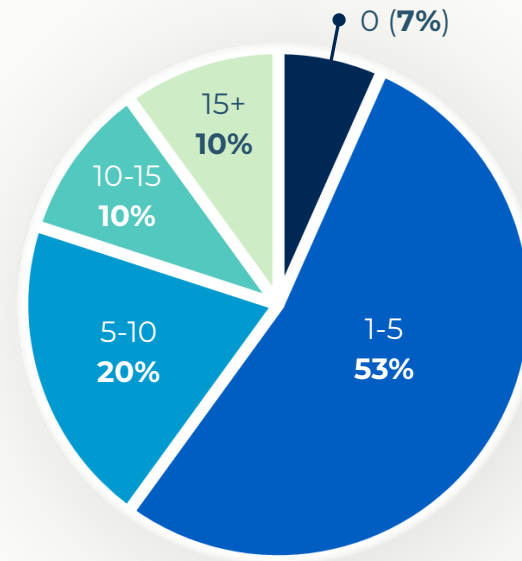


'Cyber Threat Intelligence' was the primary job function, with a variety of related functions making up the remainder.

WORK EXPERIENCE



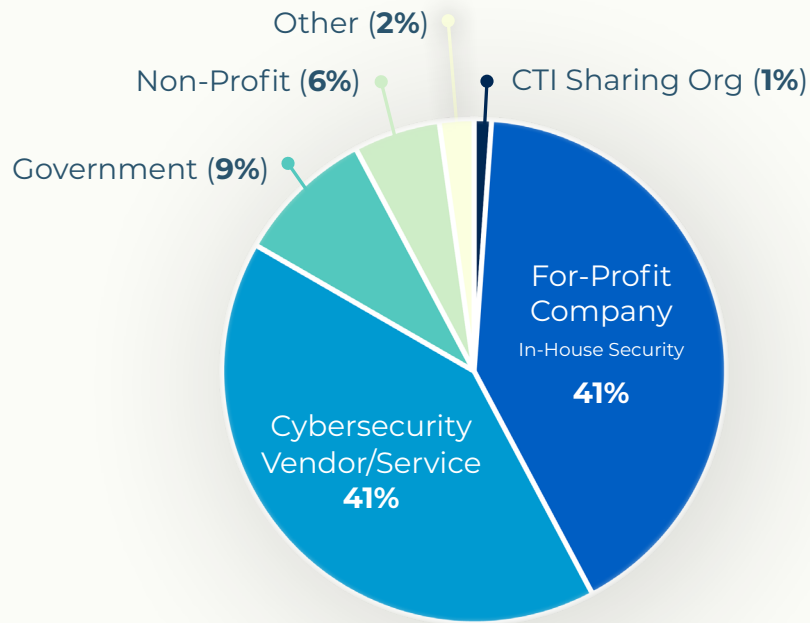
**YEARS OF SECURITY-RELATED
WORK EXPERIENCE**



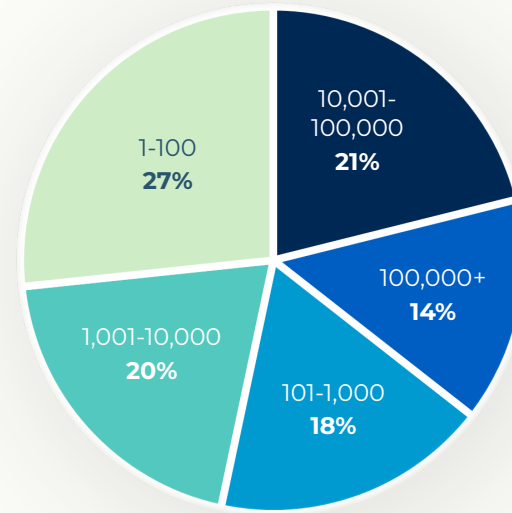
**YEARS OF CTI-RELATED
WORK EXPERIENCE**

While the years of security-related experience were evenly represented, over half of respondents reported less than five years of CTI-related experience. This is consistent with the recency and continuing growth of the field which draws experienced talent from various career paths.

ORGANIZATION



EMPLOYER TYPE



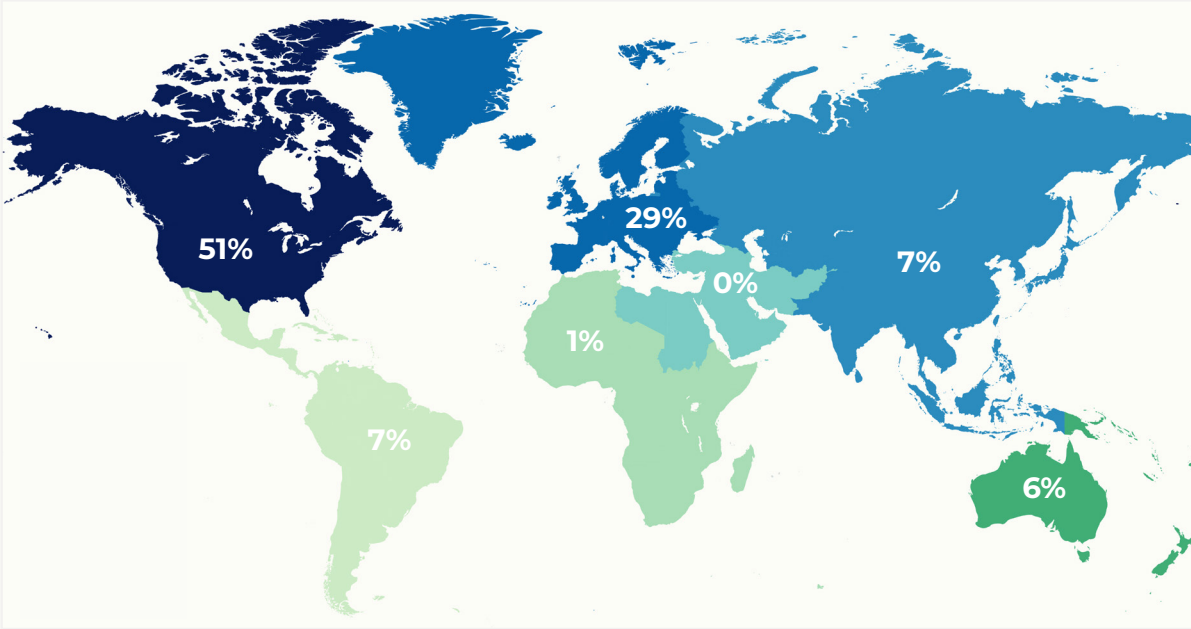
EMPLOYER SIZE
(number of employees)

The vast majority of respondents were employed by for-profit organizations, either at in-house cybersecurity teams or cybersecurity providers, with slightly improved representation of all employer types compared to the previous survey. Organizations of all sizes were evenly represented.

GEOGRAPHIC REGIONS

WHERE RESPONDENTS ARE BASED

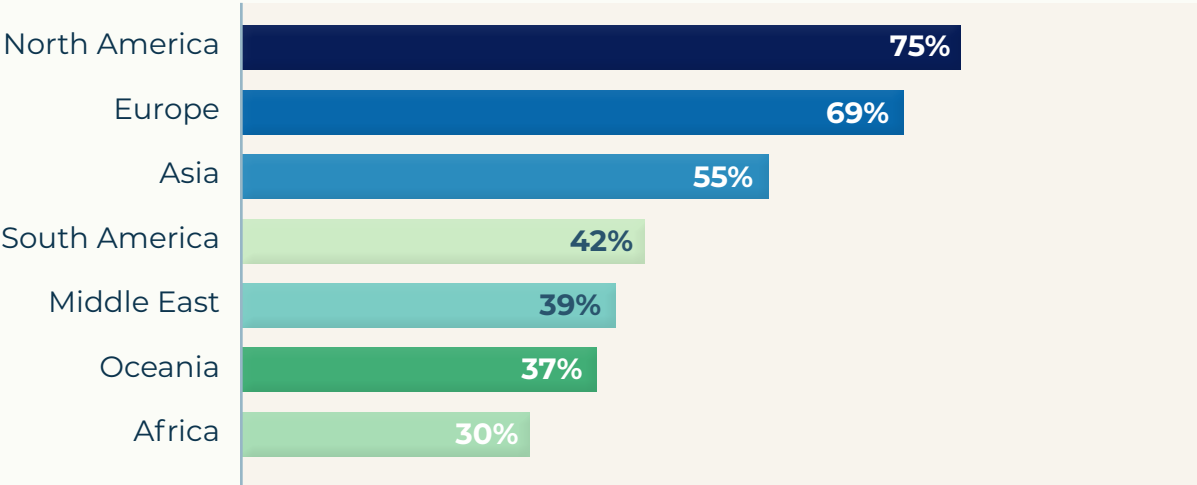
North American respondents constituted half of respondents, with an improved representation across other regions compared to the previous study.



REGIONS OF OPERATION (multiple region selections allowed)

Most respondents reported operating in multiple regions:

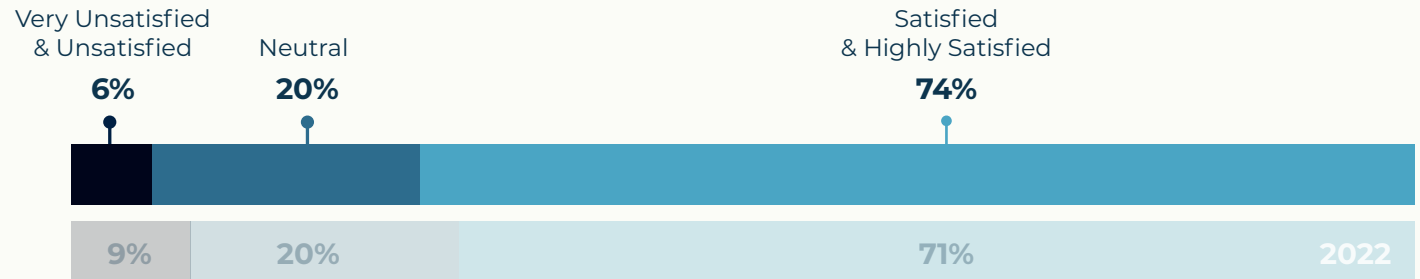
- 40% – 1 region
- 34% – 2 to 6 regions
- 24% – all 7 regions



BONUS: JOB SATISFACTION

HOW SATISFIED ARE YOU IN YOUR CURRENT JOB?

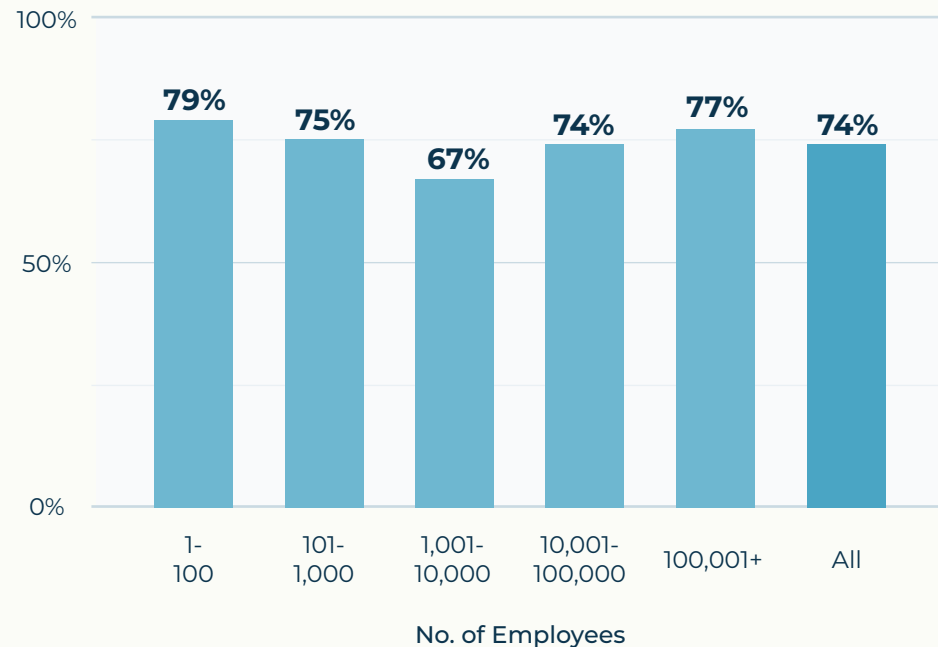
Job satisfaction was consistently high across all demographics, improving slightly compared to the previous survey.



Respondents working at cybersecurity vendor / service organizations were the most satisfied (80%) segment.

SATISFACTION BY ORGANIZATION SIZE

% Rating Satisfied & Highly Satisfied



Respondents at the smallest (<100) and largest (100,001+) organizations were more likely to rate themselves satisfied.

Respondents at organizations with 10,001-100,000 employees were the least likely to rate themselves satisfied.



THE VALUE OF CTI NETWORKING

How and Why Individuals Network

Making an Honest Effort To Get Ahead

The belief in CTI networking value remained persistent, compared to the previous survey. While responses were mixed on the ease of finding and balancing efforts (a new question added this year), consensus remained on its importance at all levels and a desire to do more.

1

BOOST IN BENEFITS

Rankings for CTI networking benefits remained similar to the previous survey, but the percentage of positive responses grew across all benefits. Respondents were most interested in networking to look ahead, ranking benefits like staying strategically aware, finding/vetting new sources, and taking proactive measures higher than operationalizing technologies and working on existing analyses.

2

DATA ON THE MIND

“Raw Data” shifted into the lead for top valued content type, beating out Contextualized Information, Processed Intelligence, Advice & Opinions, Technical Support and Emotional Support. Despite being first in value, the benefit of “getting valuable threat data” dropped from first to third – potentially highlighting a gap in what is sought after versus actually received.

3

GETTING EMOTIONAL

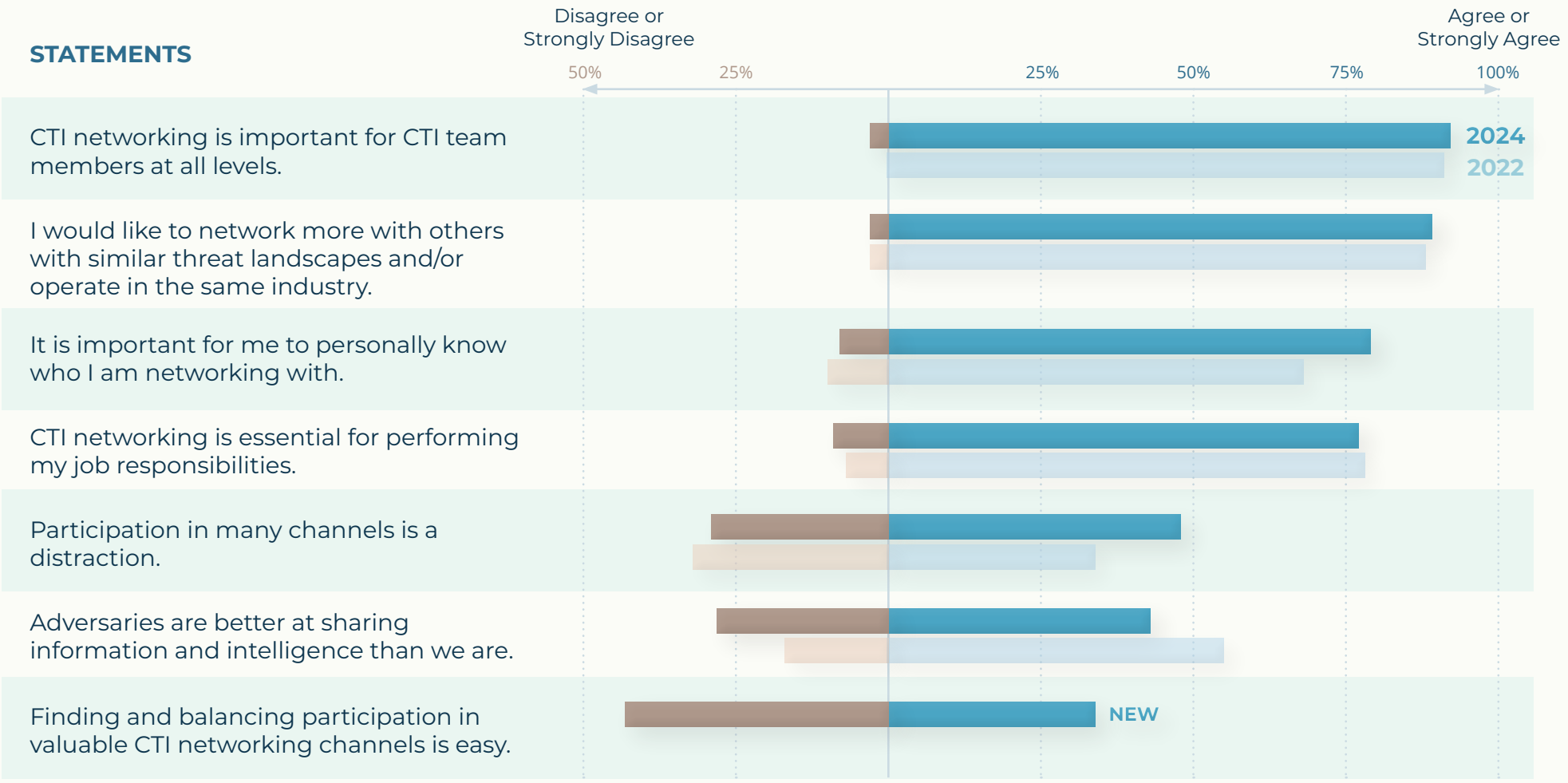
The spread of rankings for all content types (e.g. Raw Data, Contextualized Information, Processed Intelligence, etc.) decreased this year, showcasing a more equal weight of value across types. Notably breaking from previous observations and other types was “Emotional Support.” This received the most first and last place votes, creating an inverse bell curve not found anywhere else.

“ While investigating a persistent phishing campaign, CTI networking helped us find **vulnerabilities in a threat actors phishing kit** which we used to our benefit. Participants ranged from interns to team managers. **This helped gain further trust from senior management for CTI networking.**”

“ I was the first to publish details regarding [redacted] ransomware. I posted a **blog** and shared on **Twitter**. I had a few people reach out to me after my post to **share information** they had found, and to **ask for more information** that I hadn't fully shared publicly. I received a lot of additional information as a result.”

“ Sharing partnerships have led to tips that **prevented and pre-empted breaches.**”

OPINIONS & ATTITUDES



Seeking: Peers. Qualitative responses validate a strong, unfulfilled desire to network with more peers with similar interests. Responses also validated the challenges in finding and balancing participation.

- No Strong Disagreement.** No respondents “strongly disagreed” to:
- The importance of CTI networking for team members at all levels
 - The desire to network with others with shared interests

CTI NETWORKING BENEFITS

NETWORKING IN CTI HAS HELPED ME...

Ranking of respondents who answered “agree” or “strongly agree”

	2022	2024	Δ
1	Get valuable threat data	Stay aware of what's happening strategically	+1
2	Stay aware of what's happening strategically	Find, vet, or understand new sources and methods	+2
3	Take proactive measures	Get valuable threat data	-2
4	Find, vet, or understand new sources and methods	Take proactive measures	-1
5	Conduct processing and analysis during an investigation	Conduct processing and analysis during an investigation	0
6	Be less of an intelligence silo	Be less of an intelligence silo	0
7	Implement and operationalize technologies	Implement and operationalize technologies	0
8	Work with others on active projects on a day-to-day basis	Work with others on active projects on a day-to-day basis	0

Boost to Benefits. Compared to the previous survey, the percentage of agreement across all 8 statements increased.

While the ranking order of the bottom 4 statements remained the same, the percentage of “agree” and “strongly agree” responses all increased by 10%+.

“ A sharing community provided more context to ongoing events. A peer relationship has provided **attacker infrastructure** that lead to research analysis pivot.”

PARTICIPATION ACTIVITIES

HOW OFTEN DO YOU PARTICIPATE IN THE FOLLOWING?

Ranking of respondents who answered “frequently” or “sometimes”

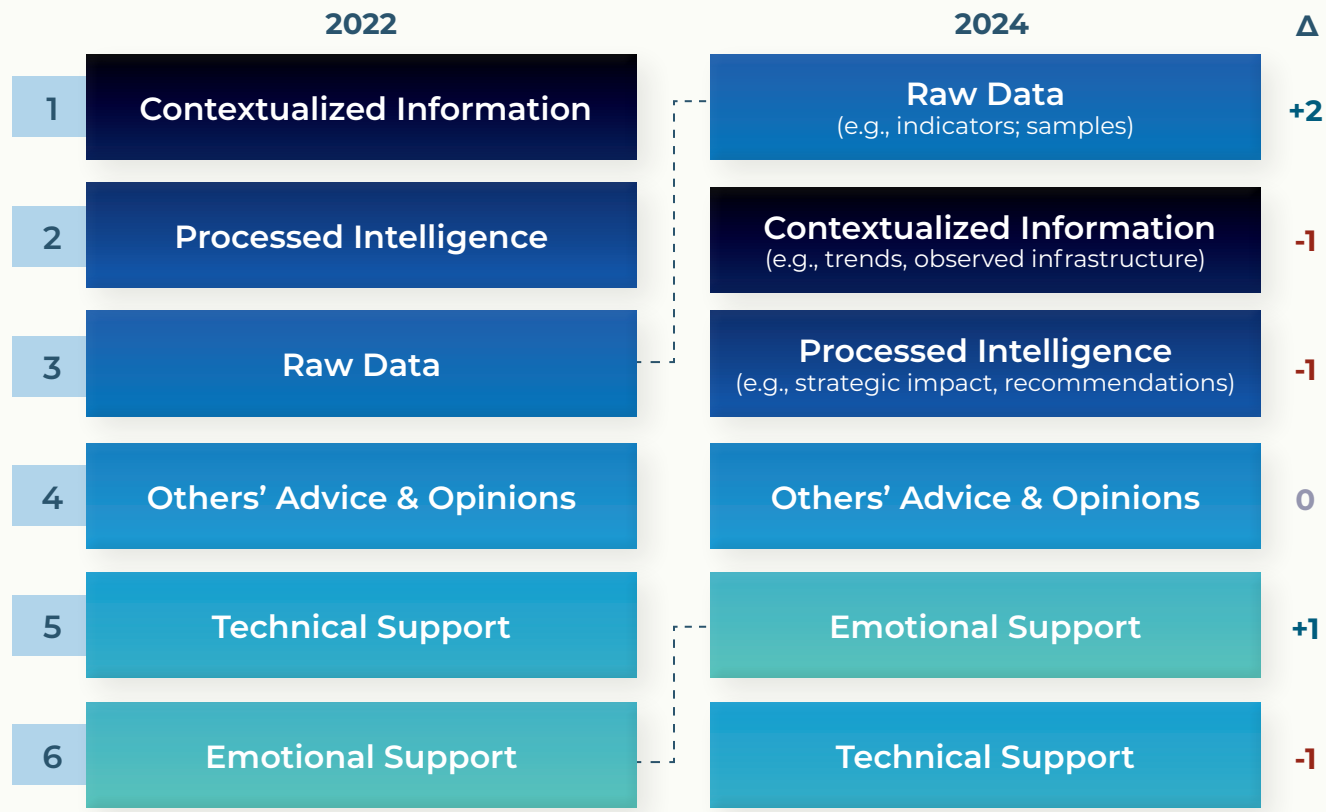
	2022	2024	Δ
1	Create and contribute to discussions	Join scheduled meetings	+3
2	Post questions and new information	Create and contribute to discussions	-1
3	Collaboratively develop or peer review reports/intelligence	Collaboratively develop or peer review reports/intelligence	0
4	Join scheduled meetings	Post questions and new information	-2
5	Automate shared enrichment/analysis	Automate shared enrichment/analysis	0
6	Create frameworks and processes	Develop content for distribution	+1
7	Develop content for distribution	Create frameworks and processes	-1

// [ISAC] meeting yesterday. Discussed threat actors attacking companies [with certain attributes]; added some **threat actors** to my list and **discussed IoCs** for those TAs which were mentioned on public resources but didn't have details... found out the different names a TA may go by. CTI sources...shared **private feeds and reports** which I don't have access to 1:1 after the meeting."

// Information from a peer group of cybersecurity professionals... resulted in **improvements to framework** used for prioritization of **vulnerability management** for enterprise customers with OT, as campaign and diamond model data was shared for attackers targeting the same industry vertical and technologies."

MVP: MOST VALUED CONTENT

WHAT PROVIDES THE MOST VALUE?



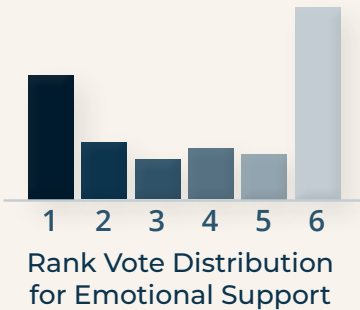
Experience Matters.

Respondents with less than 10 years of security experience and those with less than 10 years of CTI experience both preferred contextualized information.

Respondents with 10+ years of CTI experience preferred processed intelligence and the opinions of others more than those with fewer years, which may be a result of more mature networks.

// Common sharing group with trusted peers from my industry where we share on-going campaigns and associated TTPs/IOCs.

// Working with individuals who publish feeds help us build those on-the-ground relationships.... [Working with] these parties... can help fix issues which benefits the community.



Getting Emotional. While Emotional Support ranked low overall, it was unexpectedly ranked “#1” the most across all content types, resulting in a unique reverse bell curve.

Respondents at smaller companies (fewer than 1,000 employees) and at cybersecurity vendors/services organizations ranked Emotional Support higher than other segments.

MOST VALUED BREAKOUT

Rank Vote Distribution

The charts to the right represent the distribution of discrete ranking votes (#1 to #6) for each of the six content types.

All types showed typical distributions consistent with the previous survey, with the exception of Emotional Support, which showed a stark preference for both first and last places.

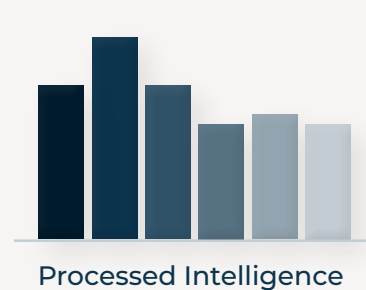
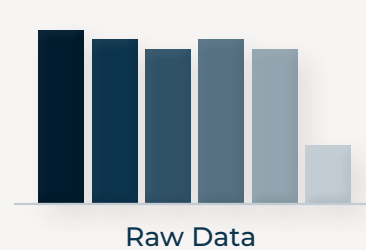
Emotional Support received the most votes for #1 and #6, and the least votes for #2-5.

Balanced Preferences. This survey showed a more balanced preference across content types. We calculated the average rank of each content type. The difference in average ranks of the highest and lowest valued type was closer than in the previous survey.

- 2022: Highest 2.87, Lowest 4.19 (Δ 1.33)
- 2024: Highest 3.16, Lowest 3.84 (Δ 0.69)

Votes for ranking

#1	#2	#3	#4	#5	#6
----	----	----	----	----	----





EXECUTION

What and Where CTI Networking Happens

Goal: Unlock 1-to-1 & P2P

Survey responses demonstrated that respondents strongly prefer 1-to-1 Direct Messaging and Peer-to-Peer Trust Groups. While participation across methods is not exclusive, this data suggests that engaging in Paid Membership Groups, Events, Volunteer Groups and Social Media & Public Forums are complementary, helping to provide highly desired access for the two top valued methods.

1

METHOD DOMINATION

Past “winners” 1-to-1 and P2P Groups pulled even further ahead compared to the previous survey to dominate across all questions about methods: 1) participation level, 2) perceived quality (with the exception of P2P Group timeliness, uniqueness), 3) positive results, and 4) where respondents disseminated produced intelligence.

2

THE RETURN OF EVENTS

With the easing of COVID and in-person meetings resuming, Industry Events showed directional boosts across participation level, perceived quality, and positive results. Several open-ended responses specifically cited a desire for budget and approval to attend events (“budget to go to events”, “budget to attend conferences or local events”, “\$\$ from the company to attend conferences”). Teams, take note.

3

EXPERTS WEIGH IN

Respondents with 10+ years of general security experience participated more in Industry Events. Those with 10+ years of CTI-specific experience reported 100% participation in 1-to-1 DMs and skewed more towards P2P Groups, Volunteer Groups, and Industry Events. Given that “access” and being able to find meaningful peers was a highly cited desire, it’s worth noting where these professionals value spending their time and effort.

“ CTI Networking has been able to contribute to high visibility situations such as MOVEit Exploitation, 3CX compromise. [H]aving **established groups**... provided **timely ability** to look in our environment before it came down from Leadership for our team to look into it. **It is better to have the answers before they even ask.**”

“ Group collaboration...my **former intel team** observed [remote access tool] used to attack a large [industry] chain across [region]. My team then was able to conceptualize and depict how attackers were escalating accounts in various locations. Being on the frontlines witnessing these escalations we were able to **relay the message to the [ISAC].**”

“ **Trusted source** confirmed activity on adversary network and infrastructure using scanning and assessment tools not available at my company or not readily available to me.”

METHODS: PARTICIPATION

1-to-1 Reigns Supreme

1-to-1 shifted up to top place, while the rankings of other methods stayed the same. The percentage of participation in Peer-to-Peer Trust Groups dropped slightly (-7%) and Social Media & Public Forums more drastically (-15%) from the previous survey. In contrast to 2022 when the top 3 methods ranked far above the rest by 20%+, this year observed a more even spread.

Social X's + Meatspace

Despite Events lagging behind Social Media by 20%+ in the previous survey, the two are now tied for 3rd place at 69% participation. This convergence may be a result of:

- Social Media Market Volatility: Once-stable spaces for news and discussion were upended with the 1) flocking to upstarts like Mastodon, Bluesky, and even Clubhouse, and 2) fleeing from 'X' formerly known and beloved as Twitter, for both personal and pricing-related reasons
- The welcome return to in-person events with easing of COVID restrictions

// [P]ost-covid the ability to meet up in-person helps foster a collaborative environment. Some of the **best collaboration and sharing** happens on the sidelines of conferences.

WHAT KINDS OF CTI NETWORKING DO YOU PARTICIPATE IN?



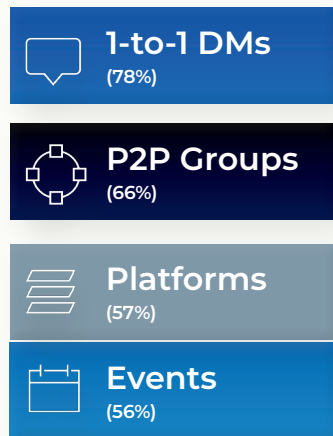
METHODS: PERCEIVED QUALITY



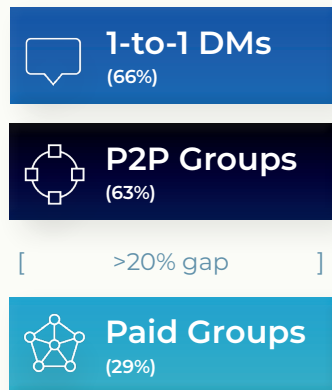
1-to-1 and P2P Trust Groups rose significantly above other methods in combined perceived quality, with the rest all roughly equal.

WHAT METHODS ARE...

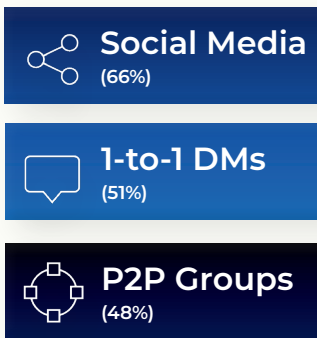
Valuable?



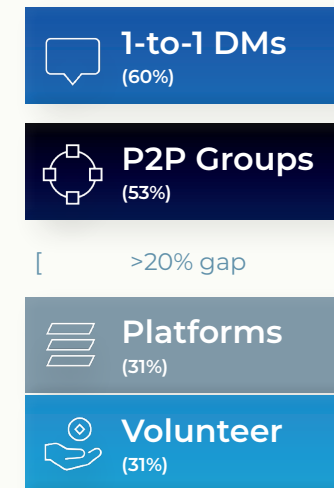
High Confidence?



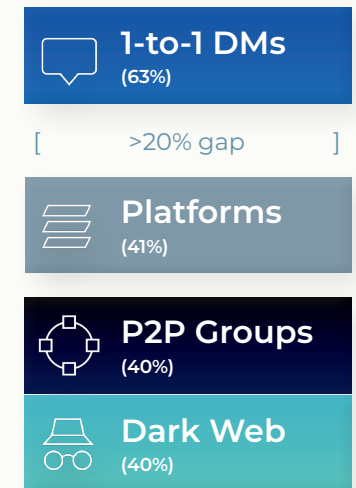
Timely?



Actionable?



Unique?



Social Controversy. Consistent with the previous survey, Social Media indexed highest on timeliness while also the lowest in confidence. Respondents working at smaller companies tended to rank Social Media more favorably.

Largest Positive Shifts

(Compared to 2022)

Volunteer Group Timeliness: +14%
 1-to-1 DMs Uniqueness: +13%
 Industry Events Actionability: +11%

Largest Negative Shifts

(Compared to 2022)

Dark Web Actionability: -32%
 Paid Groups Confidence: -16%
 Dark Web Value: -11%

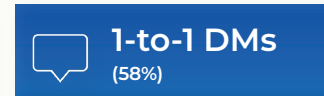
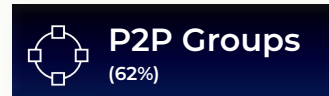
METHODS: POSITIVE RESULTS



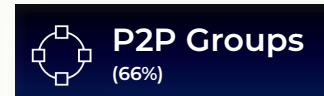
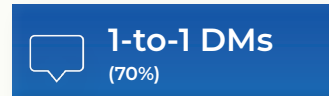
Consistent with combined perceived quality, 1-to-1 and P2P Trust Groups have provided the most positive results before, during, and after attacks.

WHAT METHOD...

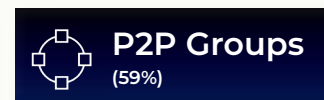
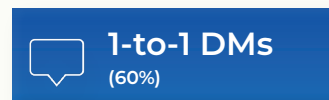
Has helped detect or prevent an attack?



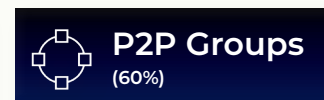
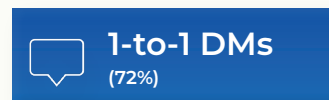
Has provided value during an attack?



Has contributed to remediation or post-incident analysis?



Has shared resources for a problem that I/the team could not address alone?



Paid Groups. Respondents who participated in Paid Groups did not report more positive results from Paid Groups compared to 1-to-1 and P2P methods.

Largest Positive Shifts
(Compared to 2022)

P2P, Prevention: +11%
P2P, During: +12%
1-to-1, During: +10%
1-to-1, Shared: +12%

Largest Negative Shifts
(Compared to 2022)

Dark Web, During: -10%
Paid Groups, Remediation: -10%

// A partner provided insight into a current investigation based on the telemetry they had visibility to. The telemetry allowed us to better respond to the event and **remediate the adversary in-house vs outsourcing...** Potentially saving the organization \$100ks in fees and lost productivity."

METHODS: DISSEMINATION

WHAT CHANNELS DO YOU PERSONALLY DISSEMINATE THE INTELLIGENCE YOU PRODUCE?



WHAT KINDS OF CTI NETWORKING DO YOU PARTICIPATE IN?



Give > Get. Compared to levels of overall participation in methods, respondents tended to disproportionately contribute in Volunteer Groups & Coalitions.

Get > Give. On the flip side, respondents tended to disproportionately under-contribute to Social Media & Public Forums and Industry Events. Given the nature of “lurking”, “following”, and “attending” for these methods, this is hardly surprising.

// Provide intelligence in easy to digest formats, and if possible publish on few well-known platforms that facilitate easy sharing.”

AREAS FOR IMPROVEMENT

Issues and Opportunities in Practice

Higher Visibility, More Restrictions

Respondents voiced numerous organizational challenges like issues of legal liability, a lack of formalized processes, and gaps in measuring effectiveness. In spite of these negative forces, respondents maintained their hours spent in CTI networking efforts while noting improved visibility with leadership.

1

"I'M NOT ALLOWED"

Legal liability and sharing restrictions rose to the top of the challenges faced. With increasing regulatory involvement, guidance, and enforcement, caution has grown around the confidentiality and consequences of disclosure – consistent with findings from the Office of the Inspector General of the Intelligence Community (US). The ranks of other challenges remained unchanged. However, an increase in the percentage of respondents concerned about retaliation may reflect growing consideration around adversary campaigns against security researchers and professionals.

2

MEASURING UP EFFORTS

75% of respondents did not measure effectiveness of CTI efforts at all, while 18% did – a negative shift that could be tied to time and resource limitations. Companies with fewer than 100 people were most likely (29%), while companies with 101-1,000 employees were least likely (6%) to measure.

3

TECHNICAL CONFUSION

Respondents disseminated produced intelligence across an average of 4 formats, with the most common being files (e.g. PDF, Word), unstructured text, CSVs, and social/blog posts. Multiple technical formats like STIX 2.x and MISP were used at <40%, showcasing challenges faced by teams to support integration without a universal industry standard.

“ Make the time. Work it into your sprint. Tell your leader that **one hour of your day** is dedicated to Slack/Discord/Telegram.”

What would improve your efforts?

“ **Legal buy-in.** There doesn't seem to be a conversation or a want to understand the benefits of CTI networking, it's only seen as a **massive liability** and that we cannot be trusted.”

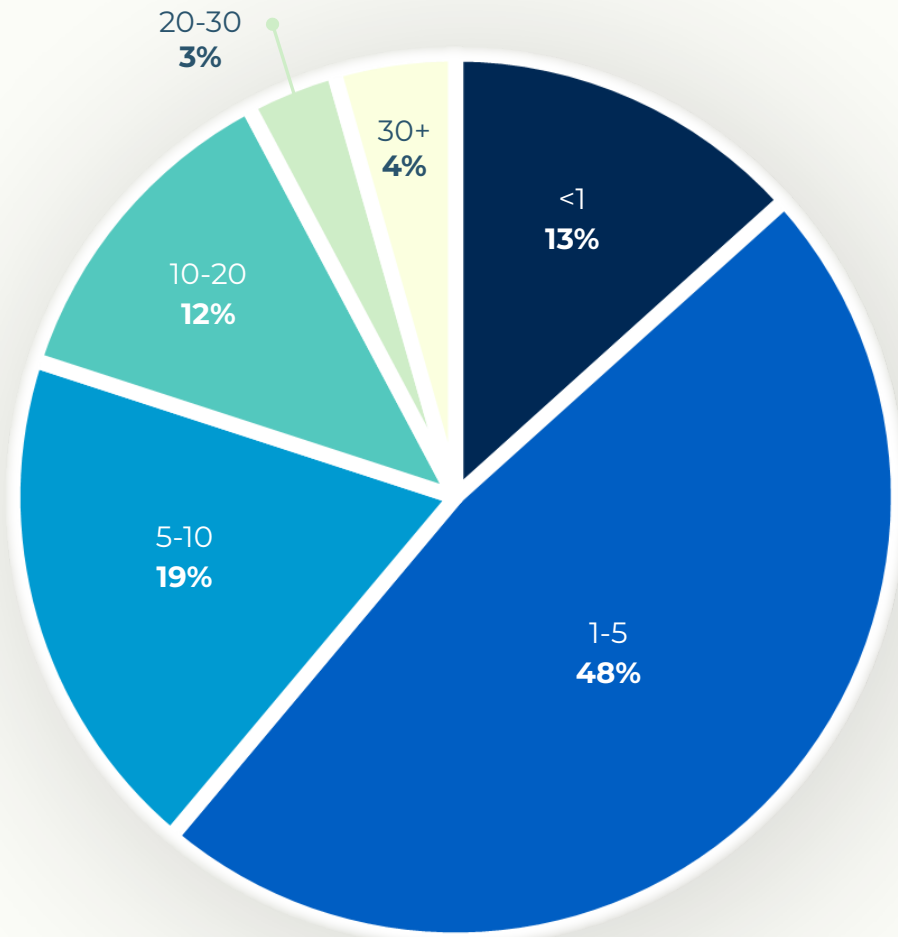
“ **Legal framework/protections** being better understood and encompassing a clearer set of data and parameters.”

“ **A centralized platform...** rather than many disparate systems interconnecting people in the know.”

“ **Use standards** in the way intelligence is described.”

TIME SPENT

TIME PARTICIPATING IN CTI NETWORKING
(hours spent per week)



Keeping Up With Time. The average time spent on CTI networking on a weekly basis remained very consistent with the previous survey, with the largest segments dedicating 1-5 or 5-10 hours each week.

A “lack of time” remained a top issue, consistent with challenges from previous and current surveys. However, individuals maintained their hours, even though in some cases it meant spending time “off-hours”. Open-ended survey responses demonstrated a desire to dedicate more time to CTI networking efforts, but respondents were limited by too many responsibilities, lack of headcount, and lack of resources to do so.

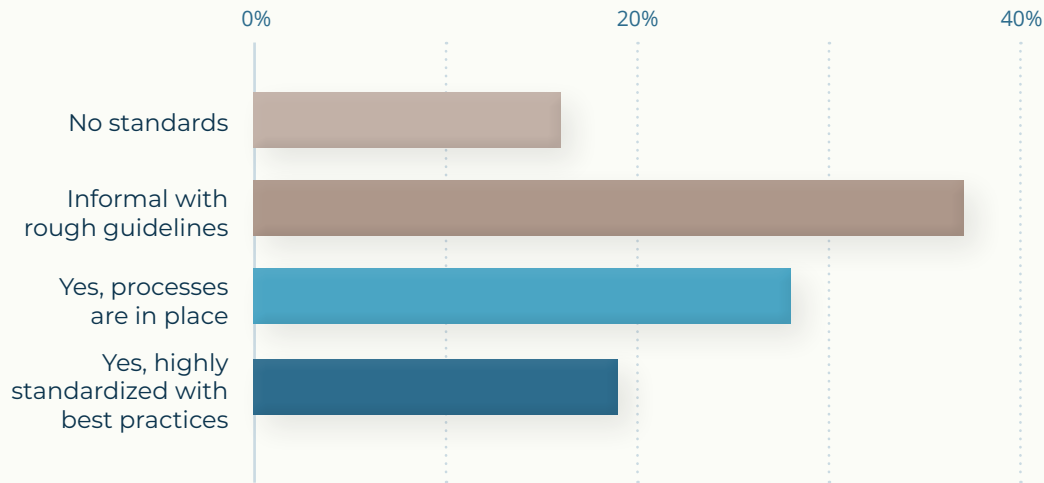
“ My job requires that I do investigations, project planning, software engineering, and security engineering work so I just don’t have enough time.”

“ I’m time poor... I make an effort to meet others in this space... but can rarely action or develop collaboratively due to my sporadic time.”

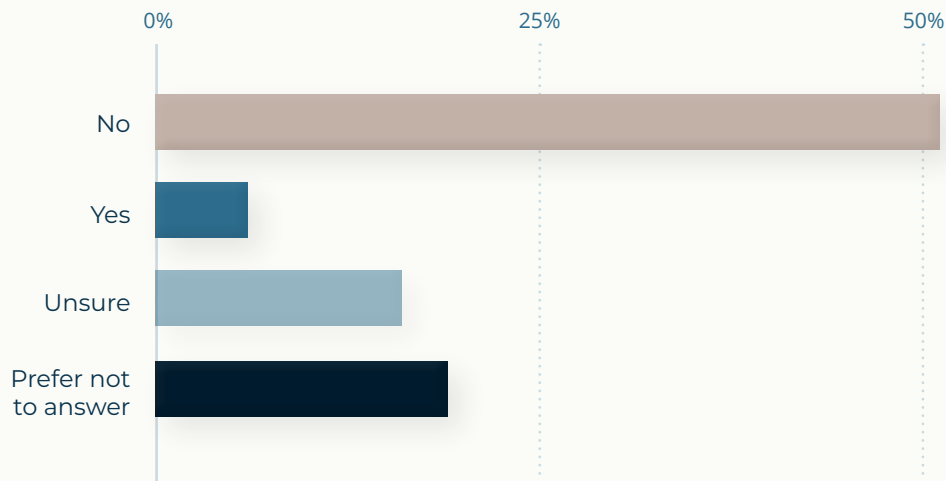
“ My biggest obstacle is finding a good community specific to my work, and **the time** to then appropriately engage with that community.”

PROCESSES

DO YOU HAVE FORMALIZED OR STANDARD WAYS TO MANAGE WHAT YOU COLLECT THROUGH CTI NETWORKING?



DO YOU BREAK ORGANIZATIONAL POLICIES / RULES DURING CTI NETWORKING?



With Great Experience Comes Great Standardization. Respondents with 10+ years of CTI experience were much more likely to have standardized collection at 72%, compared to those with less than 10 years, at 44%.

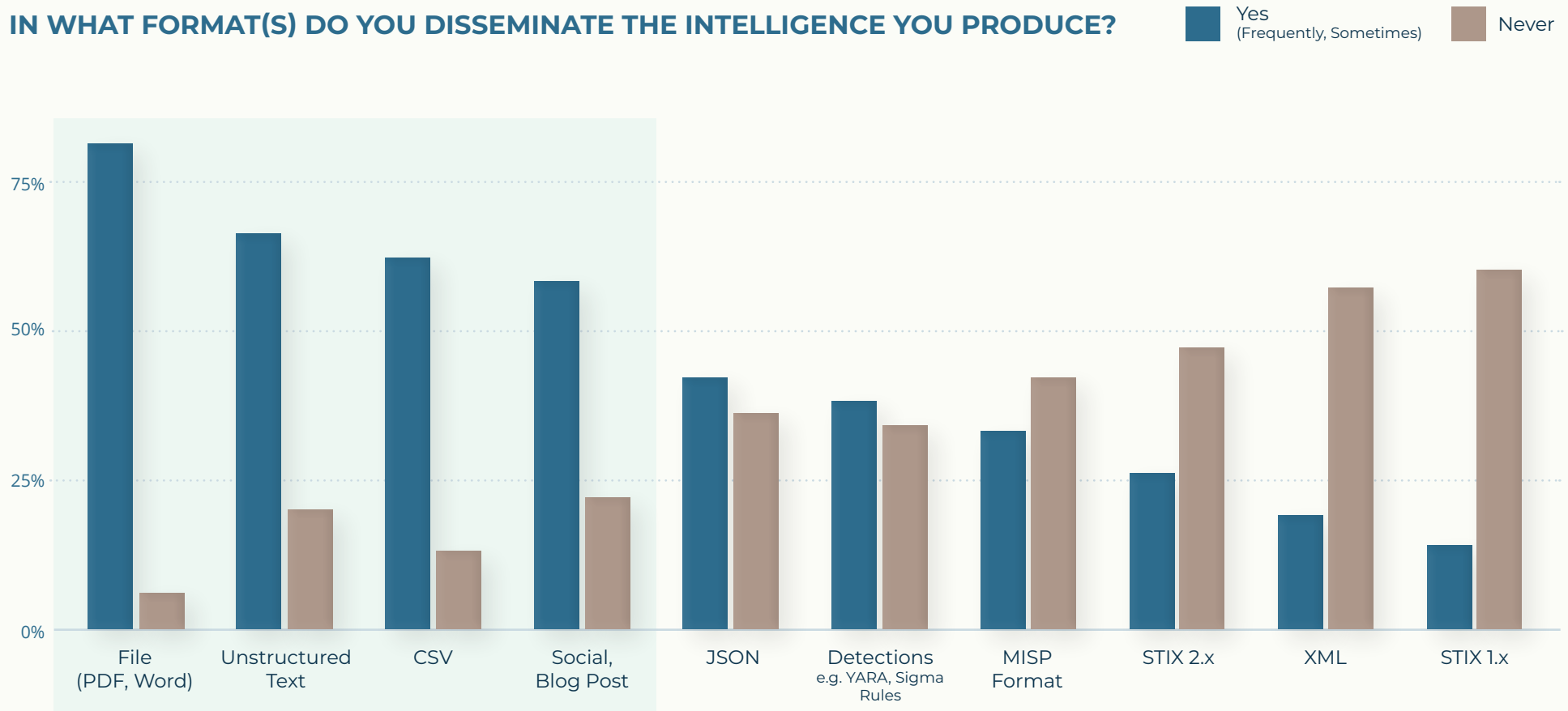
Missing Rules. While the majority of respondents did not break policies, some voiced frustrations about organizational requirements hindering CTI networking efforts.

“ I am not allowed to install encrypted messenger apps on my work laptop which **complicates collaboration** with partners using those apps.”

“ I feel like I can’t talk about or share my work... even if I wanted to share, I’d be stopped or prevented from doing so, or I would be putting my job at risk.”

FORMATS

IN WHAT FORMAT(S) DO YOU DISSEMINATE THE INTELLIGENCE YOU PRODUCE?



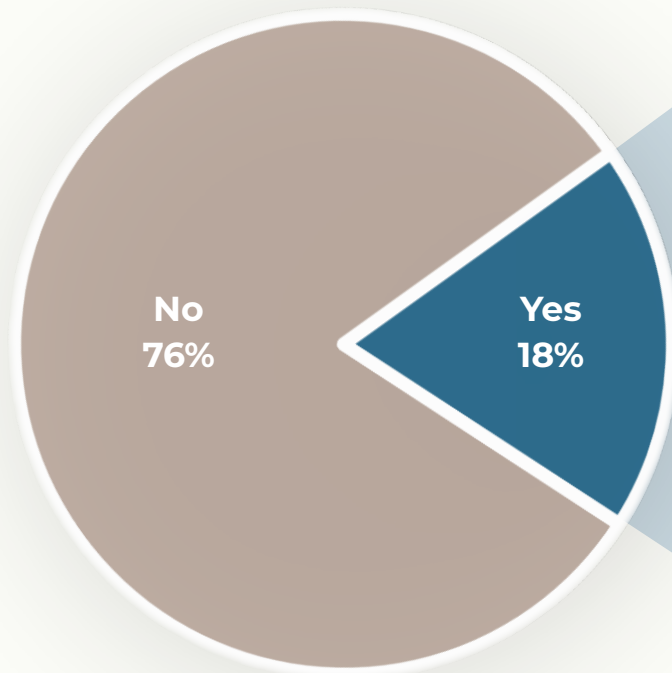
Four Formats. Respondents reported using an average of 4 formats regularly. Those who used STIX 1.x were most likely to use the most formats, with an average of 8.

Technical Complications. The multiple CTI-specific technical formats, all used at less than 40%, showcase the challenges faced by teams to support automation and integration.

61% of respondents who use STIX 2.x also use MISP; however, those who use MISP are less likely to use STIX 2.x (47%). All respondents who use XML also use CSV.

MEASUREMENT

DO YOU MEASURE AND REPORT ON THE EFFECTIVENESS OF CTI NETWORKING EFFORTS?



- // Directly via **research** and **reports**. Indirectly related to dissemination value.
- // Using the **OODA Loop**, we feed our collected results back into the processes we use after networking with other peers.
- // Based on **number of threats detected**, it has been useful to help develop internal processes.
- // [T]hrough highlighting **what gap** did the information fill that we were missing, the **actions taken**, and the **result** of the actions taken. Any progress that we made from the action is considered fruitful.
- // Through **alert feedback** in the products, customer engagements, etc.
- // **Real world impact**. How intelligence **changed processes or behaviors** to reduce risk to the organization. **Direct event related activity** that was prevented or detected...

Adaptive Re-use of Processes. Using frameworks, processes, and reporting mechanisms that already exist within the CTI program prevents over-complication and unnecessary work, while encouraging continuous feedback loops.

CHALLENGES

"Sorry, but I'm not allowed to..."

Imposed rules and restrictions shot up to the top of the challenges faced by respondents.

"[I]dentifying the boundaries for relationships with CTI networking groups, especially when some elements of internal CTI are classified, is difficult."

"Biggest obstacles include TLP and sensitivity restrictions"

"Internal sharing policy/NDA/TLP"

"NDA, Laws, legal prosecutions"

"Sharing restrictions due to TLP Level"

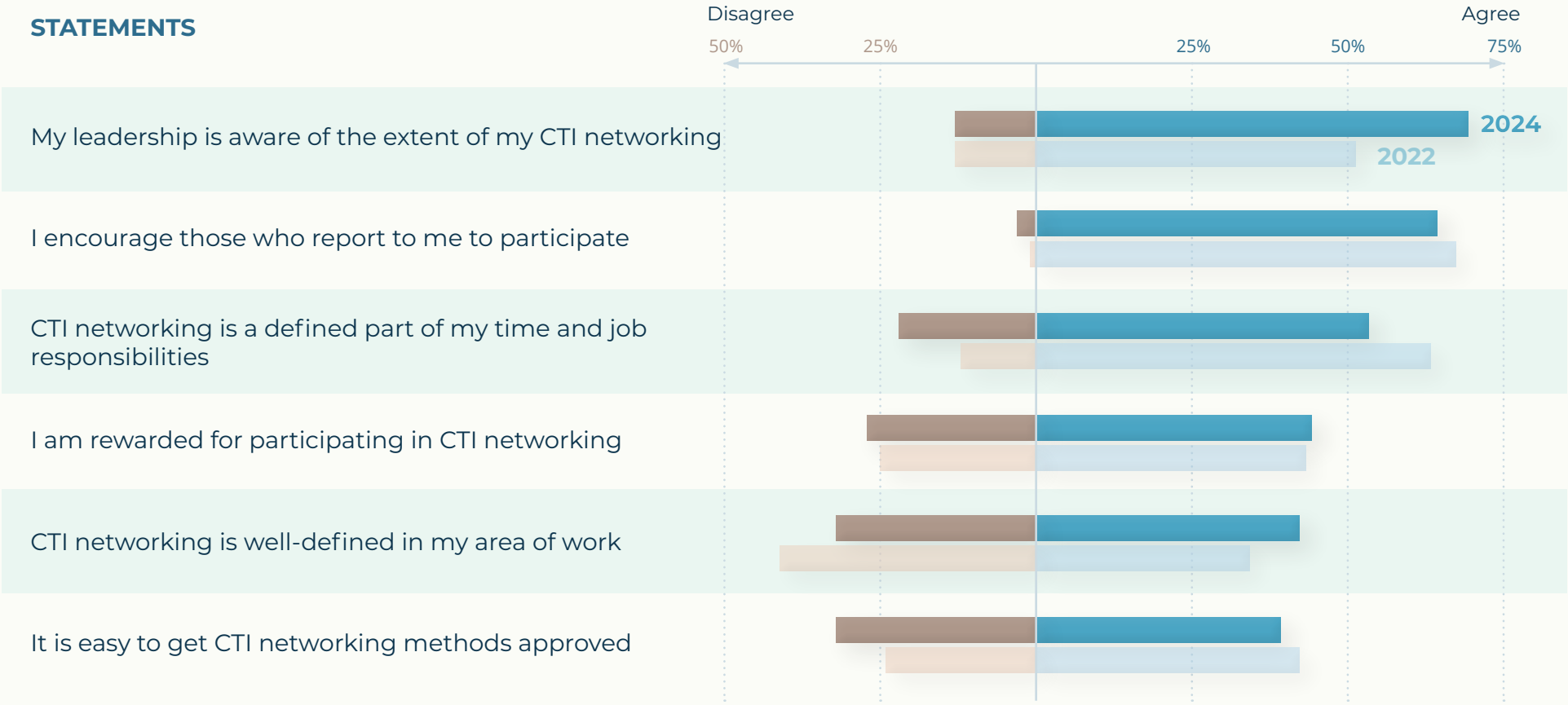
Target on Cyber Backs

While fear of retaliation (i.e., being a target of threat actors) remained in last place, the percentage of respondents noting some or a lot of impact increased by 13% compared to the previous survey. This may be a result of recent, widely covered campaigns against threat researchers, academics, and security professionals.

WHICH CHALLENGES IMPACT YOUR CTI NETWORKING?



ORGANIZATIONAL CULTURE



A Win for Visibility.

Leadership awareness of CTI networking efforts shot up by 18%, the largest percent increase in “agreement” amongst respondents.

“Defining” Shifts.

Another positive shift was the characterization of CTI networking as “well-defined”, with agreement increasing by 9% and disagreement decreasing by 9%. Conversely, the largest negative shift was in the percentage of respondents who believed that CTI networking was a defined part of their time and job responsibilities, with agreement decreasing by 10% and disagreement increasing by 10%.

WHERE DO WE GO?

Roadmap for Success

ROADMAP

Based on trends in qualitative responses and data insights, this brand new guide introduces how to engage in more intentional, inclusive, and strategic CTI networking.

Everyone starts somewhere.

With your unique requirements, security program needs, and capabilities (and limitations) in mind, try out a diversity of methods that are already in your orbit.

Build up a foundation from your existing network, organizational opportunities, reputation, and skillset.

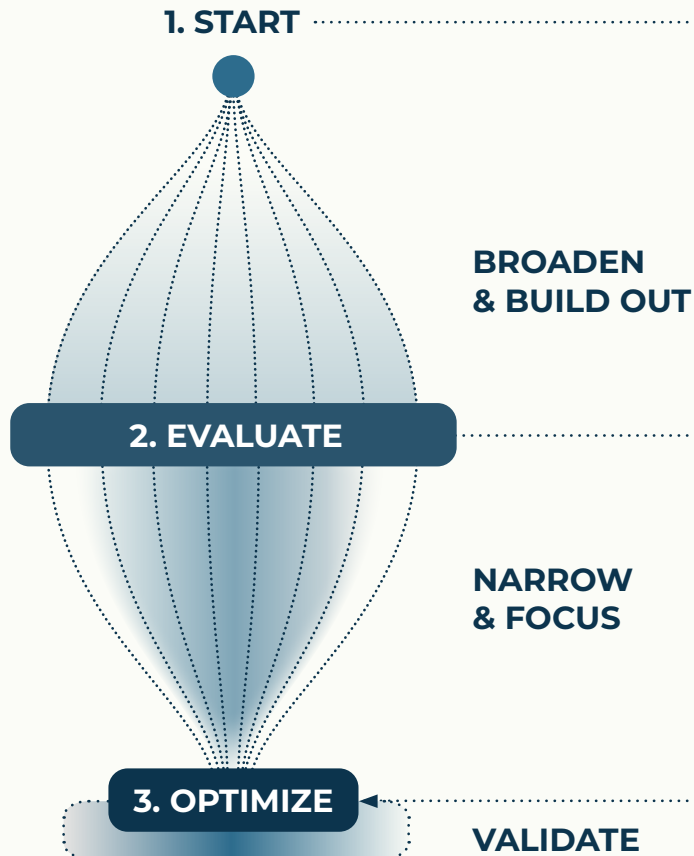
After obtaining some successes and exposure to varied CTI networking opportunities, it's time to hone in on what provides outsized value.

Examine which investments of time, energy, and budget yield outsized results. Prioritize and commit to those top three activities while maintaining limited capacity for new opportunities.

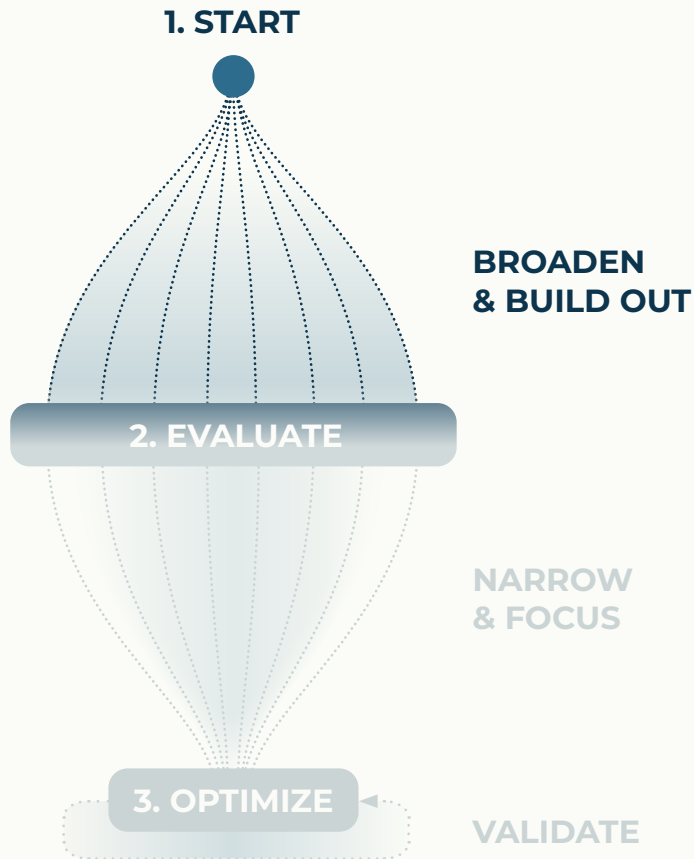
Eliminate, scale back, or delegate activities that are not providing sufficient value.

As with all things security, the process is continuous and iterative.

Periodically assess the efficacy of your efforts, attribute CTI networking in deliverables, and adapt as needs change. Validate by understanding where and how you can demonstrate results tied to CTI networking activities – both for yourself and to your organization. Doing so provides visibility into the often overlooked value of CTI networking and encourages buy-in from stakeholders for future efforts.



ROADMAP: START



Quotes on the right originate from the open-ended survey prompt: "What advice would you share with others looking to optimize their CTI networking efforts?"

There is no one-sized-fits-all path. Lower your barrier by starting with your existing circle: set up 1:1s with current or former teammates, tap into vendor relationships, and or nurture connections from events (e.g. BSides). Follow researchers publishing interesting topics on social media and provide feedback. Define what would benefit your security program, then see where your organization is active (e.g. ISAC, ERGs).

Start at 1 hour/week with a patient, experimental mindset. Initiate chats around focus areas with peers and mentors, try out a new meetup, guest-publish on a blog, or contribute to a new group. Ask thoughtful questions if you feel like a newbie, curate interesting content, and establish credibility with your unique perspective. Increase hours spent only where you see results.

// Do not be afraid to try a **new event** that **no one knows about**, they can be smaller and easier to meet people"

// Thinking outside of the box; **read, read, read**, practice curating deliverables; networking!"

// Go to security conferences, share your research online and **be patient.**"

// Start by connecting with people at your company, since that can help **lower the barrier** and point you in the right direction."

// Most importantly, don't be a d***... with a **relatively small community**, we're all Kevin Bacon degrees away..."

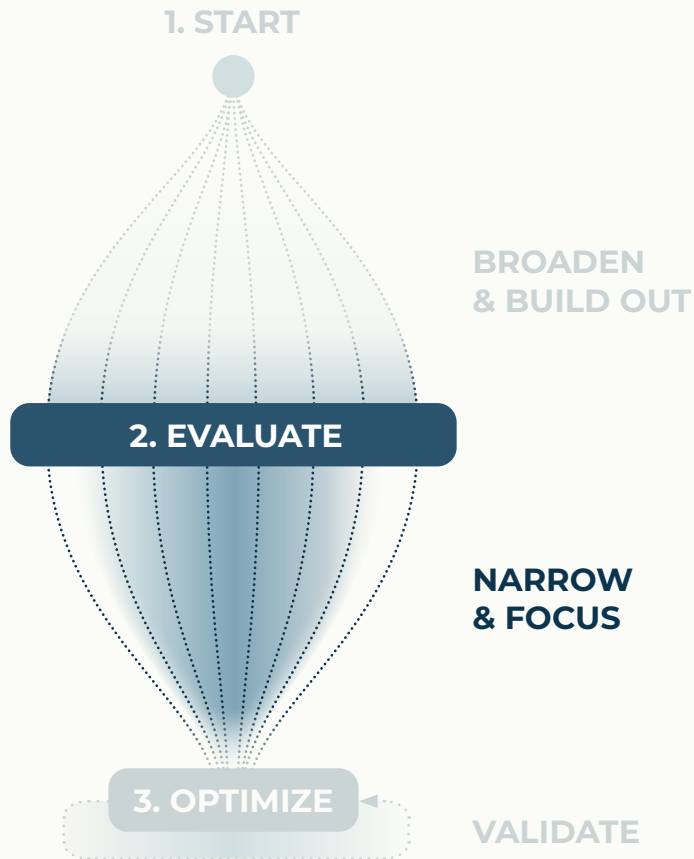
// One place I recommend starting if you really don't know anyone, are **your security vendors**. I've found GREAT collaboration partners by asking my intel vendors if there are other analysts like me who they can make an introduction to."

// Ask questions! Contributing to a discussion doesn't **have to mean sharing information**, it could be asking **clarifying questions** or **encouraging others** to elaborate..."

// Connect with others who are well established in the industry, learn to engage and **contribute to platforms** and always ask questions relevant to your **intelligence needs.**"

// **Be skeptical. Be curious.** Ask questions and do your own research to validate. Expect to be a lone wolf but if you find a pack, ensure **you bring in others to grow the pack in a positive manner.**"

ROADMAP: EVALUATE



Quotes on the right originate from the open-ended survey prompt: "What advice would you share with others looking to optimize their CTI networking efforts?"

After some opportunities and exposure, you may feel you're being stretched too thin. **It's time to hone in on what provides real value.**

Think critically and commit to around three core channels that show serious promise or have proven results. Now that you've seen what works and what doesn't, be selective and scale back time evaluating new opportunities. Consider structuring and scheduling your own 1:1's or breakouts if you've found key peers from larger methods. Where possible, pass on introductions, embrace mentorship, and share invites to qualified peers. Don't be afraid to (politely) bow out of commitments that lack ROI – the key here is quality, not quantity.

// Shortlist a few [methods] like a **closed group** or a 1-1 contact and stick to it... if focusing on more sources, try to **create a workflow** that make it easy to go through all the information"

// Focus on **what you're good at**, share that information with partners **who share back**...limit the effort you exert with those who betray trust, only consume, or share [low-value] things."

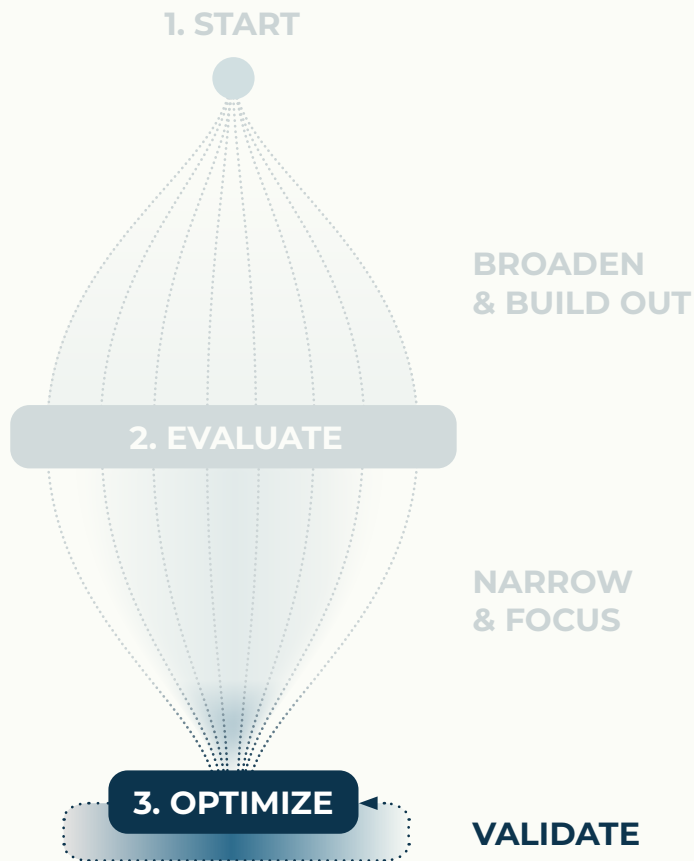
// I have gotten much more value out of **quiet, TLP-Red high trust groups**. [I]nformation shared in these groups is significantly better, they are smaller so you can get to know individuals, and there is a standing expectation that the information can be **properly protected**."

// [I]nvest in **low number of high value networking opportunities** and try to build and contribute to **long-lasting relationships**, rather than trying to be all over the place with everyone since that is much more time consuming and the ROI is usually bad.

// Optimize and schedule your study... Don't allow the sheer volume of threats and vulnerabilities to **take over your life**, force the company to set realistic guidelines and when you clock out, that means you're OFF WORK, not studying threat feeds and IOC's until 2am... Create a good working strategy and stick to it when threats arrive, **seeking help through your delegates when you need new ideas**, as you continue to isolate and limit the other areas that you can still contain. Above all, stay on top of emerging threats and **meet weekly with your counterparts**..."

// Focus on the **relevant stuff to you** as there's a sh**load of material every day and it's overwhelming at times."

ROADMAP: OPTIMIZE



Quotes on the right originate from the open-ended survey prompts: "What advice would you share with others looking to optimize their CTI networking efforts?" and "Describe a past experience where CTI networking yielded interesting results"

The process to maximize results with CTI networking is an iterative and continuous cycle. Building workflows, attributions, and measurements that truthfully recognize time and effort spent not only helps validate where and why you invest to yourself, but also to your team... and skeptical stakeholders.

Data showed an increase in transparency to leadership, but that is merely the first step to more meaningful change. To be viewed as more than a "liability" and receive the buy-in to even begin considering approvals, there must be significant and demonstrated business benefits (i.e. the risks must be understood and accepted). Additionally, as roles, companies, and the threat landscape inevitably change, you must also be able to understand and align those to your methods and sources. As always, it's never "set it and forget it."

// Focus on areas that **provide a measurable return** and tout those successes internally. Managing up and illustrating the value of spending time and resources in this area is the best way to **get buy-in from leadership.**"

// [N]etworking helped **confirm or validate sources, processes, or information.** A couple of times, we had **just-in-time warnings** or information that helped us prepare for something bad."

// Most of what I know started with a **discussion with others.**"

// Fruitful partnerships, open lines of communication, **getting ahead of the adversary** to stop ransomware deployment and get APTs kicked off networks."

// Private intelligence between trusted groups is...the most valuable data for me. In many cases during investigation it is possible to **correlate data** with other researchers... **confirming or completing analysis,** or getting additional data to pivot."

// Several engagements, I've needed help looking at something for a different opinion or fresh set of eyes and **got significant value in return.**"

// CTI networking on social media has revealed a **previously unknown malware** communicating with a C2 node in a victim environment, and I was able to use that information to **guide the response.**"

The following page compiles respondent stories where CTI networking resulted in specific successes for the organization.

STORIES OF SUCCESS

Quotes originate from the open-ended survey prompt: "Describe a past experience where CTI networking yielded interesting results"

- // While investigating a persistent phishing campaign, CTI networking helped us find **vulnerabilities in a threat actors phishing kit** which we used to our benefit. Participants ranged from interns to team managers. This helped gain **further trust from senior management** for CTI networking."
- // CTI networking has allowed the team to **respond to active attacks** attempting to leverage a **0 day vulnerability** within our environment."
- // A phishing wave hit a peer company, they posted their detection rule to a peer-to-peer sharing group, we implemented it and were **able to detect the campaign** when it hit us a few days later."
- // An organization provided IOCs for a nation-state cyber attack which led to the **identification of patient zero**."
- // Due to CTI networking and building trust, we were tipped off that a third-party vendor... had been compromised and a connection into our network was also compromised. We were able to **get ahead of the threat...** due to **the relationship I had built**."
- // I was notified on a **discord trust group** by another CTI professional of a post on a forum about databases of a major [organization] being sold...
 1. It was early in the morning when the post had been released
 2. It was the weekend
 3. I was away from my laptop as I was about to go to conference.By notifying me... I was able to **pass on the intelligence to my higher ups** which resulted in the [organization] **being alerted in a matter of hours** about the post. The [organization] and other government officials hadn't heard anything about the post and were able to investigate. "
- // Ransomware get requests isolated through [community platforms] mere days before actual attacks proliferated, likely the first time the team was **ahead of the curve** and modified search metrics to allow for the new threat logic. Info brought to the table by a **team member working off the clock** to expand their threat vocabulary, **saved a valuable client from loss** due to a new mobile threat."
- // Took my team to a local CTI conference, where we listened to several talks around new methods of intelligence gathering and dissemination. We **spoke to the presenters** at the conference to share our perspective. Then the team was able to incorporate what we learned into **new processes for identifying novel threat actor activity in our client environments**."
- // Sharing of indicators in a peer group **immediately identified the threat actor** based on high confidence information from a member of the group."
- // A vendor published a report describing a new intrusion by a well known actor that didn't align with previous observations from that actor.
Through CTI network I was able to identify that the described activity was researcher testing and **not from the threat actor**."
- // Caught a threat actor by helping smaller organization do IR, purple teamed it internally, caught threat actor, **worked with law, caught [the threat actor]**."
- // Investigating a TA in order to make attribution. C2 was traced across multiple countries by other [government organization] in the working group. At the end we were able to **find out the entire infrastructure** across [continent]."
- // A colleague at another organization shared some infrastructure I used...to **develop a detection** that the colleague plug[ged] into their defensive tools to help protect their organization long term from a particular actor. I was able to... find additional clusters of adversary activity including malware and work collaboratively across industries to **contribute to an indictment**."

CONCLUSION

Since 2022, the CTI community has continued to tirelessly investigate emerging threats, mitigate new vulnerabilities, adopt new tools, enhance frameworks, and improve business outcomes through collaboration. Externally, physical meetings resumed, the social media landscape evolved, regulatory agencies deepened engagement, international conflicts dominated headlines, and hiring slowed (if not froze) while budgets were slashed. Despite these changes, our research found that the general behaviors and beliefs of practitioners regarding CTI networking has not drastically changed. Respondents were:

- Highly satisfied in their roles (74%)
- Engaged in CTI networking to “get ahead” and “stay in the know”
- Staunch believers in its importance to perform job responsibilities, at all levels (92%)
- Skewed heavily towards 1) 1-to-1 direct messages and 2) free, focused P2P trust groups
- Dedicated to an average of 1-10 hours a week of CTI networking (67%)
- Limited by challenges in external restrictions, lack of time, and noisiness
- Operating in a more ad hoc vs. formalized and measured capacity

In notable shifts from the previous survey, respondents:

- Received more benefits from CTI networking efforts overall
- Increased value placed on raw data and emotional support
- Experienced a resurgence in the participation and value of events
- Found more issues and lack of buy-in around legal liability and sharing restrictions
- Grew leadership visibility around existing CTI networking efforts

This report offers insights into the perceived and demonstrated value of CTI networking, highlighting what’s changed, and what hasn’t, since the previous survey. The data validated that CTI networking is still treated as an afterthought in the organization, in spite of demonstrated impact. With this benchmark and newly created “roadmap”, I hope to push the field towards more effective, inclusive, and strategic efforts – both for practitioners to achieve greater success and for organizational stakeholders to develop security programs.

INTERESTED IN PARTICIPATING IN FUTURE RESEARCH?

Contact Grace Chi at
grace@pulsedive.com



APPENDIX

Survey and References

APPENDIX

Survey Form

All respondents completed a Google Forms survey consisting of 7 sections:

- Introduction
- Demographics
- Methods
- Behaviors
- Opinions & Attitudes
- Open-Ended Questions
- Conclusion

Personally identifiable information (PII) was not required to submit a response.

Survey on CTI Networking (2023 Sequel)

Context

This survey is a follow-up to my 2022 research and report benchmarking cyber threat intelligence networking practices, results, and attitudes.

Full 2022 Report: [Is Sharing Caring?](#)
SANS 2022 CTI Summit Presentation

Purpose

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

Yet, the enormity of it all can feel insurmountable to CTI professionals deciding how to effectively network *today*. In 2022, we discovered what practitioners are doing, what's effective, and gaps. Now, we're asking again to find out what's changed and how.

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

Scope

This survey should be taken by professionals that work in or closely with CTI with at least 1 year of professional experience.

"CTI Networking" is defined as the interaction of individuals for the purpose of CTI-related work. This definition *excludes* personal networking purposes purely for career development (e.g. get a new job, close a customer deal).

Survey responses will be anonymized and analyzed to inform not-for-profit research on current CTI networking and sharing behaviors. You will be given the opportunity to provide contact information at the end, and this information will not be used for any other purpose or shared with anyone else.



Instructions

It is strongly recommended to use a computer while completing this survey.

There are 6 sections with multiple choice and optional short answers questions. The survey will take 5-15 minutes to complete.

Hit "Next" to begin and make sure to hit "Submit" to record your responses.

Questions? Contact: grace@pulsedive.com.

Demographics

Please share a little about yourself.

Current Job Title *

Your answer _____

Role (Primary Function) *

- ☐ Cyber Threat Intelligence
- ☐ Security Operations
- ☐ Vulnerability Management
- ☐ Incident Response
- ☐ Digital Forensics
- ☐ Threat Hunting
- ☐ Red Team (Offensive Security)
- ☐ Governance, Risk, and Compliance (GRC)
- ☐ Executive Leadership
- ☐ Other: _____

Total Years of Security-Related Work Experience *

- ☐ 0 (none)
- ☐ 1-5
- ☐ 5-10
- ☐ 10-15
- ☐ 15+

Years of CTI-Related Experience *

- ☐ 0 (none)
- ☐ 1-5
- ☐ 5-10
- ☐ 10-15
- ☐ 15+

Current Employer Type *

- ☐ For-Profit Cybersecurity Vendor or Professional Service (e.g. Products, MSSPs, Consulting)
- ☐ For-Profit Company, In-House Security Team
- ☐ Cyber Intelligence Sharing Organization (e.g. ISACs)
- ☐ Government
- ☐ Non-Profit
- ☐ Other: _____

Size of Organization (Employees) *

- ☐ 1-100
- ☐ 101-1,000
- ☐ 1,001-10,000
- ☐ 10,001-100,000
- ☐ 100,001+

In what region are you based? *

- ☐ North America
- ☐ Africa
- ☐ Asia
- ☐ Europe
- ☐ Latin & South America
- ☐ Middle East
- ☐ Oceania

In what regions do you operate? *

- ☐ North America
- ☐ Africa
- ☐ Asia
- ☐ Europe
- ☐ Latin & South America
- ☐ Middle East
- ☐ Oceania

APPENDIX

Survey Form

Methods

For clarification, here are examples of each method:

- **1-to-1** - direct messages, emails, calls, meetings
- **Peer-to-peer** - free invite-only trust groups, e.g. Discord, Slack, Telegram
- **Paid membership groups** - ISACs, committees
- **Volunteer groups & coalitions** - groups with shared non-profit objectives
- **Social media** - e.g. Reddit, Mastodon, Twitter, LinkedIn
- **Industry events** - meet-ups, seminars, conferences, expos
- **Dark web** - forums, markets
- **Community platforms** - public tools where users can share and ingest information
- **Other** - anything not included above (please explain if you choose this)

What kinds of CTI networking do you participate in? *

Note: Participation includes anything more than being present or "online" (passive lurking does not count). Participation may include contributions like planning, moderating, management, research, and automation.

	Never	Rarely	Sometimes	Frequently	N/A
1-to-1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social media	<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 trust groups	<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	<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"/>
Community platforms	<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"/>

If you answered "Other" above, please describe

Your answer

Networking Method Breakdown

Now, we'll dive into each type of networking.

Networking Method Breakdown

Now, we'll dive into each type of networking.

Indicate which descriptions are true for each of the following methods. Check all that apply.

	Is valuable	Is high confidence	Is timely	Is highly actionable	Is unique
1-to-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social media	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dark web	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Peer-to-peer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Volunteer groups & coalitions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Paid membership groups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Industry events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Community platforms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (if answered above)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Indicate which statements are true for each of the following methods. Check all that apply.

	Has helped detect or prevent an attack	Has provided value during an attack	Has contributed to remediation or post-incident analysis	Has shared resources for a problem that I/the team could not address alone
1-to-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social media	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dark web	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Peer-to-peer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Volunteer groups & coalitions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

What channels do you personally disseminate the intelligence you produce? *

	Never	Rarely	Sometimes	Frequently	N/A
1-to-1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social media	<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 trust groups	<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	<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"/>
Community platforms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

In what format(s) do you disseminate the intelligence you produce? *

	Never	Rarely	Sometimes	Frequently	N/A
Unstructured text	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Files (PDF, Word, images)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
STIX 1.x	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
STIX 2.x	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
MISP format	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CSV	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
JSON (non-STIX or MISP)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
XML (non-STIX)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Finished detections (YARA, Sigma)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Survey Form

Behaviors

How many hours do you spend weekly, on average, participating in CTI networking? *

- ☐ Less than 1 hour
- ☐ 1-5 hours
- ☐ 5-10 hours
- ☐ 10-20 hours
- ☐ 20-30 hours
- ☐ 30+ hours - it is a main responsibility

How often do you participate in the following? *

	Never	Rarely	Sometimes	Frequently	N/A
Post questions and new information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Create and contribute to discussions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Develop content distribution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Join scheduled meetings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automate shared enrichment/analysis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Collaboratively develop or peer review reports/intelligence	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Create frameworks and processes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Do you have formalized or standardized ways to manage what you collect through CTI networking? *

- ☐ Yes, highly standardized with best practices
- ☐ Yes, processes are in place
- ☐ No, informal with rough guidelines
- ☐ No, no standards exist
- ☐ N/A

If you answered "Yes" above, please explain how you measure and report on effectiveness.

Your answer

Do you break organization policies/rules during CTI networking? *

- ☐ Yes
- ☐ No
- ☐ Unsure
- ☐ Prefer not to answer
- ☐ N/A

What are the results of your networking efforts? *
Networking in CTI has helped me...

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	N/A
Get valuable threat data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Take proactive measures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Work with others on active projects on a regular basis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Conduct processing and analysis during an investigation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Be less of an intelligence silo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Find, vet, or understand new sources and methods	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Implement and operationalize technologies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Stay aware of what's happening strategically	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please rank the following by what's provided you the most value. Each number may only be used once. *

1: most valuable to 6: least valuable. Note: not a ranking of value in theory, but what has provided the most value in practice.

	1	2	3	4	5	6
Raw data (i.e. indicators; samples)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Advice & opinions of others	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Emotional support	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Processed Intelligence (i.e. reports with impact, recommendations)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Contextualized information (i.e. trends, observed infrastructure)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Technical support	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Survey Form

Opinions & Attitudes

How satisfied are you in your current job? *

12345

Very unsatisfiedHighly satisfied

Tell us about your organizational culture regarding CTI networking? *

Strongly disagreeDisagreeNeutralAgreeStrongly AgreeN/A

I am rewarded for participating in CTI networking

CTI networking is a defined part of my time and job responsibilities

It is easy to get CTI networking methods approved

CTI networking is well-defined in my area of work

I encourage those who report to me to participate

My leadership is aware of the extent of my CTI networking

What are your opinions regarding CTI networking? I believe... *

Strongly disagreeDisagreeNeutralAgreeStrongly agreeN/A

It is important for CTI team members at all levels

Adversaries are better at sharing information and intelligence than we are

I would like to network more with others with similar threat landscapes and/or operate in the same industry

Participation in many channels is a distraction

It is essential for performing my job responsibilities

It is important for me to personally know who I am networking with

Finding and balancing participation in valuable CTI networking channels is easy

How much do the following challenges impact your CTI networking? *

No impact at allNot much impactNeutralSome impactA lot of impactN/A

Noisiness (e.g. false positives)

Legal liability or confidentiality (e.g. NDA)

No budget

Lack of leadership buy-in

Retaliation (e.g. target by attacker)

Reputational fear

No time

Lack of in-house skills to act

Sharing restrictions (e.g. TLP)

Lack of trust

Competitive advantage (e.g. IP)

44

Survey Form

Open-Ended Questions

Describe a past experience where CTI networking yielded interesting results.

Provide as much detail as you can, including context, methods, participant types, and consequences.

Your answer

What changes would vastly improve your CTI networking efforts?

Your answer

Describe in detail your biggest current obstacle in CTI networking.

Specific examples and impact are helpful.

Your answer

What advice would you share with others looking to optimize their CTI networking efforts?

Your answer

If you took this survey in 2021, what's changed in your CTI networking experience since your last response?

Your answer

Conclusion

If you are interested in being contacted for follow-up research or to receive the results, please provide your information below.

If not, hit the submit button below.

Thank you for participating in this survey.



What is your name?

If we reach out, this is how we will address you. Feel free to use a pseudonym.

Your answer

What is your email?

Your answer

If you'd like to be included in acknowledgements, please write the name/handle you'd like to be credited as here.

This may appear in reports, presentations, blogs.

Your answer

For what reasons can we contact you?

- ☐ You may contact me for further research on this topic.
- ☐ I would like to receive a copy of the survey results.

Back

Submit

Page 7 of 7

Clear form

Form Submission

Respondents could opt into being contacted for further research or to receive a copy of the results.

No responses were collected until respondents hit submit on the final page.

SOURCES

- Bouwman, X., Le Pochat, V., Foremski, P., Van Goethem, T., Gañán, C., Moura, G., Tajalizadehkhoob, S., Joosen, W., and van Eeten, M. (2022). *Helping hands: Measuring the impact of a large threat intelligence sharing community*. Retrieved 2021, from <https://www.usenix.org/conference/usenixsecurity22/presentation/bouwman>.
- Brown, R., and Nickels, K. (2023). *SANS 2023 CTI Survey: Keeping Up with a Changing Threat Landscape*. Retrieved 2023, from <https://www.sans.org/white-papers/2023-cti-survey-keeping-up-changing-threat-landscape/>.
- Chi, G. (2022). *Is Sharing Caring? A report on current cyber threat intelligence networking practices, results, and attitudes*. Retrieved 2023, from <https://blog.pulsedive.com/cti-networking-report/>.
- Ettinger, J. (2019). (rep.). *Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States*. Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University. Retrieved 2021, from <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=546578>.
- Infoblox (2021). *Fourth Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way*. Retrieved 2021, from <https://info.infoblox.com/resources-whitepapers-ponemon-fourth-annual-study-on-exchanging-cyber-threat-intelligence>.
- Johnson C., Badger L., Waltermire D., Snyder J., and Skorupka C. (2016). *Guide to Cyber Threat Information Sharing, Special Publication (NIST SP)*. National Institute of Standards and Technology. Retrieved 2021, from <https://doi.org/10.6028/NIST.SP.800-150>.
- Lee, R. and Brown, R. (2021). *2021 SANS Cyber Threat Intelligence (CTI) Survey*. Sponsored by Anomali, Cisco Systems, DomainTools, Infoblox, Sixgill, and ThreatQuotient with SANS Institute. Retrieved 2021, from <https://www.sans.org/white-papers/40080/>.
- Maleh, Y., Mamoun Alazab, L., and Romdhani, I. (2023). *Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*. River Publishers eBooks. Retrieved 2023, from <https://doi.org/10.1201/9781003373384>.
- Office of the Inspector General of the Intelligence Community, Audit Division (2023). *Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015* (Publication No. AUD-2023-002). Retrieved from <https://www.oversight.gov/sites/default/files/oig-reports/ICIG/Joint-Report-Implementation-Cybersecurity-Information-Sharing-Act-2015AUD-2023-002Unclassified.pdf>
- Skopik, F., Settanni, G., and Fiedler, R. (2016). *A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing* Computers & Security, Volume 60. Retrieved 2021, from <https://doi.org/10.1016/j.cose.2016.04.003>.
- Skopik, F. (2017). *Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level*. Auerbach Publications.
- Straight, J. (2018). "Legal Implications of Threat Intelligence Sharing." Conference Presentation, SANS Institute, January 2018.
- Sundar, S. and Mann, D. (2017). *Effective Regional Cyber Threat Information Sharing*. Retrieved 2021, from <https://www.mitre.org/publications/technical-papers/effective-regional-cyber-threat-information-sharing>.
- Wagner, T., Mahbub, K., Palomar, E. and Abdallah, A. (2019). *Cyber threat intelligence sharing: Survey and research directions*. Computers & Security, 87. Retrieved 2021, from <https://doi.org/10.1016/j.cose.2019.101589>.
- Wagner, T., Palomar, E., Mahbub, K., and Abdallah, A. (2018). *A Novel Trust Taxonomy for Shared Cyber Threat Intelligence*. Security and Communication Networks, 2018. Retrieved 2021, from <https://www.hindawi.com/journals/scn/2018/9634507/>.
- U.S. Department of Defense. (2021). *Cybersecurity Maturity Model Certification (CMMC) Assessment Guide, Level 2, Version 2.0*. Retrieved 2021, from https://www.acq.osd.mil/cmmc/docs/AG_Level2_MasterV2.0_FINAL_202112016.pdf.



SHARING, COMPARED

A Study on the Changing Landscape of CTI Networking

CONTACT

Grace Chi

grace@pulsedive.com