

IS SHARING CARING?

A report on current cyber threat intelligence networking practices, results, and attitudes

JANUARY 2022



INTRODUCTION

Cyber threat intelligence (CTI) is a growing space, with an industry-wide consensus that teams cannot effectively operate in an intelligence silo. In support of improved CTI sharing, stakeholders have invested in research and development efforts around cross-boundary collaboration, technical standardization, managing trust, and reporting best practices.

Yet, there's a lack of clarity around how professionals can most effectively network **today**. To date, the conventional wisdom amongst practitioners is that CTI networking is achieved through trial & error and on an individual basis. **So, we reached out directly to practitioners to capture their CTI networking experiences.**

Objective. Benchmark CTI networking practices, results, and attitudes to provide data-driven insights around:

- How different methods stack up
- How and why individuals participate
- The role organizations play

This research serves as a starting point for more informed discussions around CTI networking. Our goal in openly sharing this knowledge is to encourage intentional, inclusive, and strategic approaches in the community. The questions we answer address lively debates currently only supported by anecdotal evidence, like:

- How do old-fashioned 1-to-1 DMs compare to invite-only Discords, paid industry memberships, and Twitter?
- What methods helped detect an attack or contributed to remediation?
- What's more valuable - raw data or finished intelligence? To whom?

Who is this report intended for?

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

By Grace Chi

With the support of Pulsedive and the CTI community

CONTENTS

Executive Summary	4
Methodology	5
Demographics	6
Insights	11
▪ How Different Methods Stack Up	11
▪ How and Why Individuals Network	20
▪ The Role Organizations Play	29
Conclusion	36
Appendix	38

EXECUTIVE SUMMARY

CTI networking is an **asset**, not an **afterthought**.

Today, CTI networking is widely encouraged and perceived as highly valuable. However, given the relative newness and growth of the field, the top CTI networks today are grassroots, free to join, and ad-hoc.

This matches the spirit of the cybersecurity community and confirms what most practitioners already suspected. However, they also result in significant manual efforts and noisiness that takes up practitioners' most precious resource (time) and potential conflicts with organizational policies (TLP, NDAs, legal liability).

KEY FINDINGS

- **Crowd favorites take the cake.** 1-to-1 Direct Messages and Peer-to-Peer Trust Groups win out – by far – as the favored methods, ranked across all levels of participation, perceived quality, and observed results.
- **Social clinches third.** Social Media and Public Forums, while controversial, should not be overlooked. Social Media outperformed on results compared to perceived quality.
- **Data? Information? Intel? All of the above.** Key advantages include access to and awareness of actionable, timely content across the entire data-information-intelligence spectrum. What kind of content is most valuable depends on whom you ask.
- **Not a matter of if you should, but how.** There is a high level of value and encouragement placed on CTI networking... at an individual level.
- **For now, it's on you.** While organizations understand the value of intelligence sharing, structures and incentives are lacking around CTI networking. It's time to acknowledge its role and the value it already brings in security programs.

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

// We are currently [CTI networking] on an ad-hoc approach... Would like to have this as part of our **long-term strategy** to mature our CTI processes as a whole..."

// [W]orking in the CTI space, having the **support of leadership** to reach out to other organizations or individuals in my network or another's network would have been the **best thing possible.**"

Anonymous respondent outlooks on the state of CTI networking

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. **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.

The survey contained ~75 questions and four open-ended prompts, and required no PII to submit a response. The link was distributed both publicly and privately through:

- Public social media posts
- Direct messages and emails
- Industry and peer-to-peer trust groups
- Newsletters

Number of quantitative respondents: 134

Number of qualitative respondents: ~120

Responses collected: November 10 – December 20, 2021

Additional analysis in this report includes segmentation by:

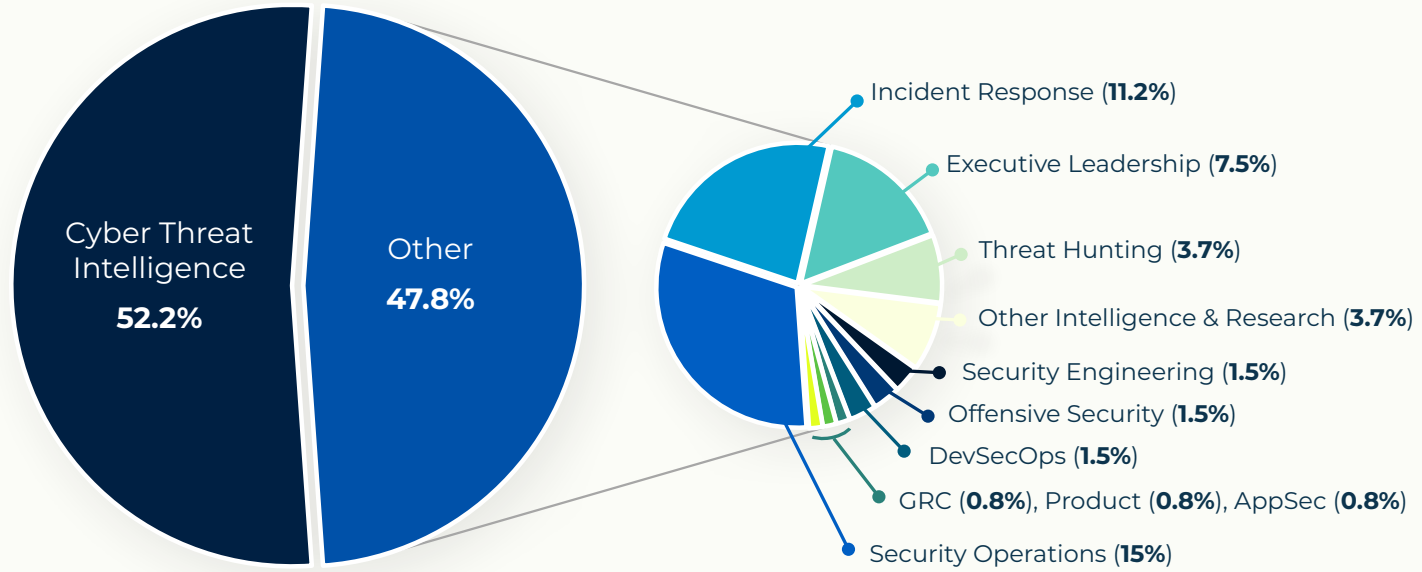
- Organization size
- Organization type
- Primary job function (CTI or other)
- Years of total work experience
- Years of CTI-related work experience

Disclaimer

- The respondents represent a small fraction of the industry. As such, results are meant to be recognized as an initial look at CTI networking, not a comprehensive study.
- By the nature of survey distribution through networking channels without compensation, respondents are biased towards general networking participation.

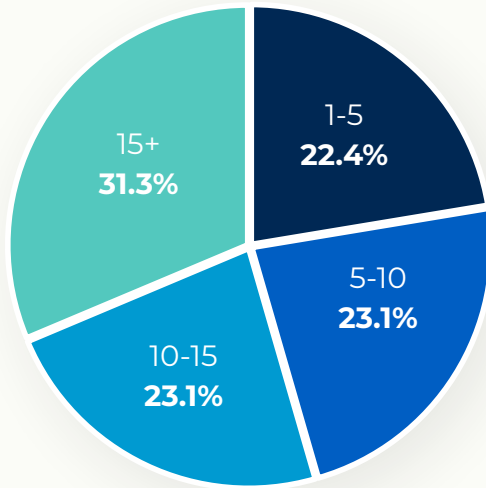
DEMOGRAPHICS

PRIMARY JOB FUNCTION

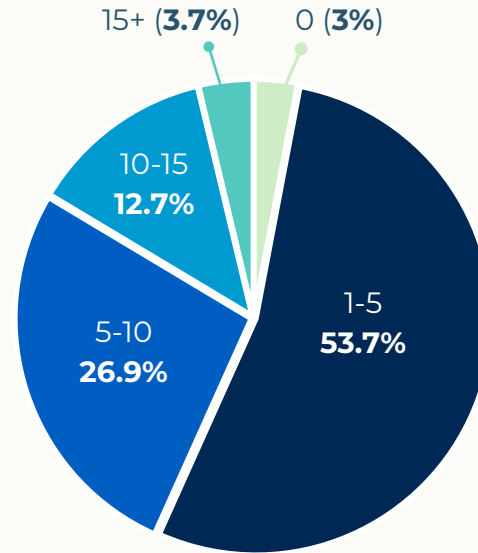


'Cyber Threat Intelligence' was the primary job function for over half of respondents, with an assortment of related roles making up the other half.

WORK EXPERIENCE



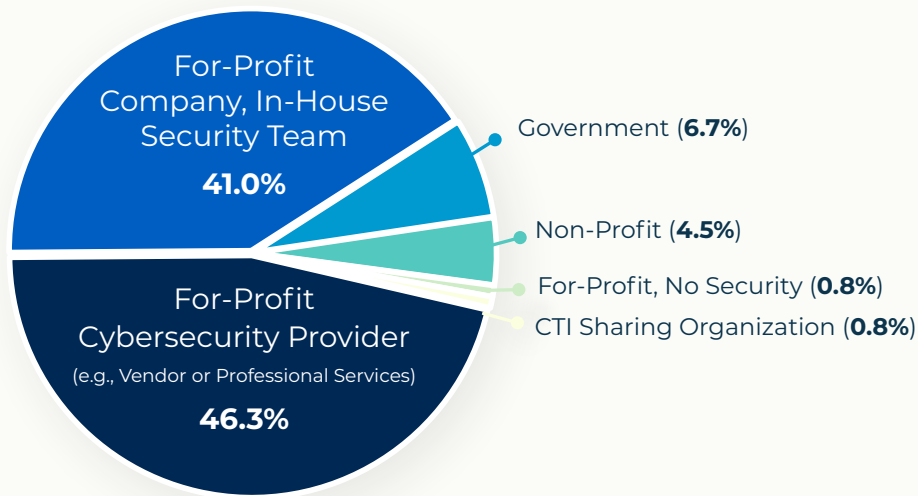
**YEARS OF TOTAL
WORK EXPERIENCE**



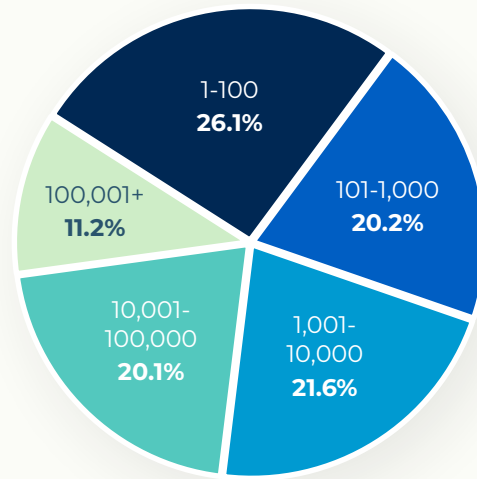
**YEARS OF CTI-RELATED
WORK EXPERIENCE**

While the years of total work experience were evenly represented, over half of respondents reported less than five years of CTI-related experience. This is consistent with the relative recency and growth of the field, drawing experienced talent from career pivots and specialization.

EMPLOYER ORGANIZATION



EMPLOYER TYPE



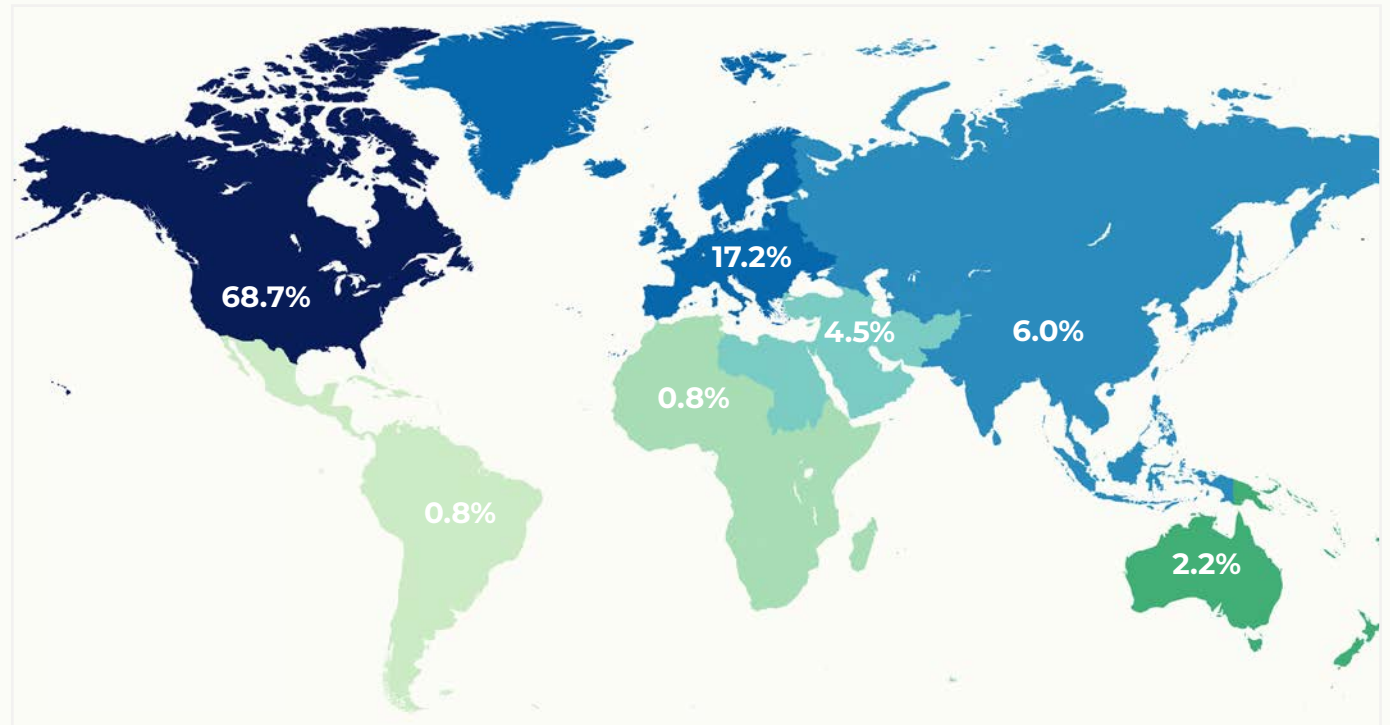
EMPLOYER SIZE
(# of employees)

The vast majority of respondents were employed by for-profit organizations, either at an in-house cybersecurity team or for a cybersecurity provider (including vendor, professional services, and consulting). Organizations of all sizes are represented.

GEOGRAPHIC REGIONS

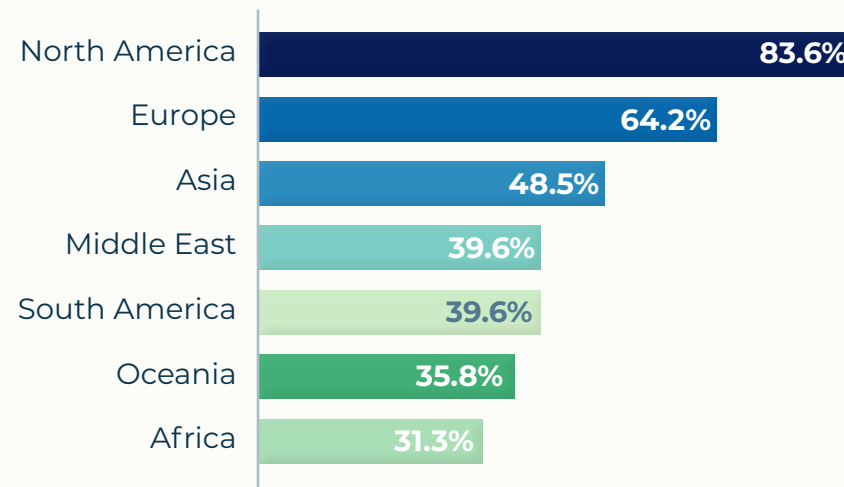
REGION WHERE RESPONDENT IS BASED

Respondents were heavily skewed towards North America, making up over two-thirds of all respondents.



REGION(S) OF OPERATION (select all that apply)

However, respondents operated in multiple regions. Half of the respondents reported working in at least three regions, and a quarter reported operating in all seven regions listed.



INSIGHTS

How Different Methods Stack Up

1-to-1 & Trust Groups Reign Supreme (By Far)



There are no shortcuts to the strongest networks.

The level of participation, perception of quality, and real-world results were consistently leading for both 1-to-1 Direct Messages and Peer-to-Peer Trust Groups. This dominance was observed across all experience levels, organization sizes, and primary job functions. In qualitative interviews, many respondents noted reliance on Trust Groups in particular, and enthusiasm for establishing more Trust communities.

As private channels that highlight the difficulty in scaling trust, both are heavily based on personal reputation and reciprocated contributions.

// I have found that collaboration platforms such as Slack or Discord are the best to share IOCs and TTPs that can have an **immediate impact** on investigation and threat hunts."

1-to-1

100% of respondents working in 100,001+ employee organizations reported regularly using 1-to-1 Direct Messages.

Professionals with 10+ years of experience rated 1-to-1 higher on all fronts than those with <10 years of experience (a 46% difference).

Trust Groups ranked high across all quality metrics, except uniqueness.

CTI professionals and those with 10+ years of experience were likely to rate Trust Groups more positively in all dimensions. This brings to light how more senior and specialized practitioners have both the access and ability to leverage these communities.

Don't Underestimate Social Media



Noisy? Chaotic? Yes. But it remains popular for a reason.

While Social Media & Public Forums fell short across multiple dimensions of quality, they ultimately outperformed when assessing impact.

Respondents shared anecdotes about the strength of channels like Twitter, Reddit, and LinkedIn for discovery - including meeting strangers around shared research topics or being contacted for their niche expertise. In addition to short-term projects, these connections led to deeper relationships outside of social.

“ Being linked with [research] in the past, an individual... reached out via social media and notified me of an additional set of [malicious research findings] that were still active... I was able to help escalate that internally... and get them **taken down within 24 hours.**”

“ Met a random guy on Twitter that was doing some CTI work on a similar data set that I was working on. I asked him questions around the dataset and how he was parsing the data... I made improvements... we both ended up with the **data we needed to provide to our CTI teams.**”

Most respondents found Social Media highly valuable and the most timely, while simultaneously ranking the lowest in confidence.

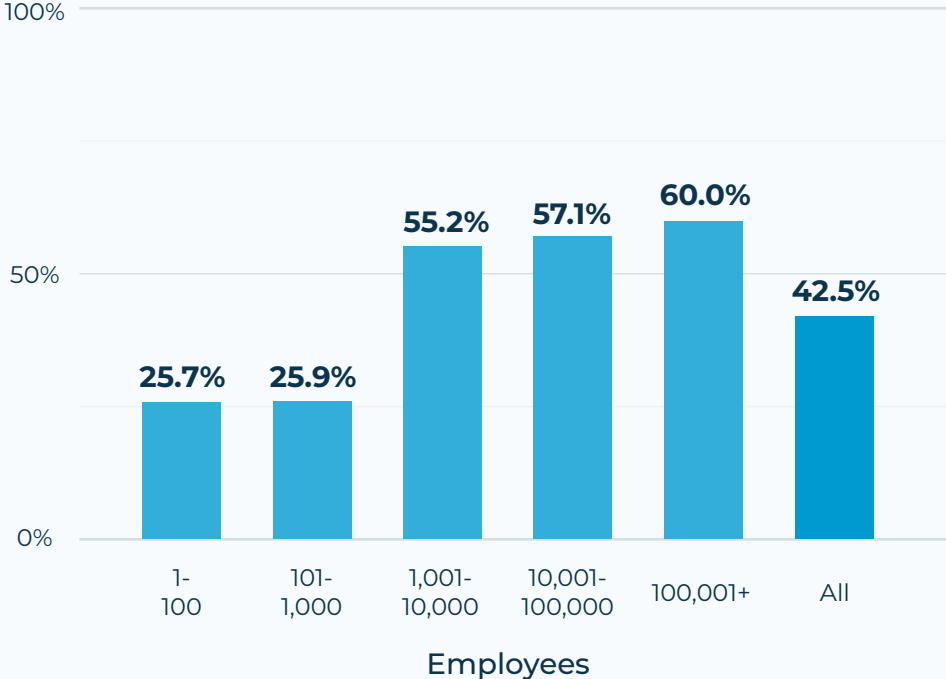
Interesting note: a single CTI professional commented in interviews that Social Media offered the highest confidence and quality data.

Paid Memberships Skew Towards Bigger Organizations



PARTICIPATION BY ORGANIZATION SIZE

% Sometimes or Frequently



Factoring in budget, resources, and sector CTI maturity.

Unsurprisingly, the larger the employer, the more likely respondents were to participate in Paid Membership Groups.

In interviews, paid members expressed interest in more engagement from CTI vendors. Yet, only a quarter of CTI vendors reported regularly engaging in these groups today.

// [ISACs] provide instant access to a trusted community and platform for sharing that is relevant to your industry."

Events & Volunteering Are Valuable, For Different Reasons



Gaining exposure for future CTI networking.

Industry Events and Volunteer Groups & Coalitions were disproportionately ranked “valuable” compared to other quality metrics like “confidence,” “uniqueness,” and “timeliness,” and generally low scoring on results.

Given the discrepancy, these methods can be viewed as offering value for other reasons, or as networking ‘enablers’ that play an adjacent role.

“CTI networking events are my go to means to **stay informed on the threat landscape** from a regional perspective... the maturity of CTI is relatively low outside the US and CTI networking with like minded individuals helps bridge the gap.”

Industry Events scored the lowest on being “actionable” at 3%. This was the lowest score across all channels and dimensions of quality. This corresponded closely with result rankings, reflecting the nature and content of events. Respondents scored events as the lowest across measures of detecting/preventing an attack, help during, and contribution to remediation/post-incident analysis.

DATA DEEP DIVE

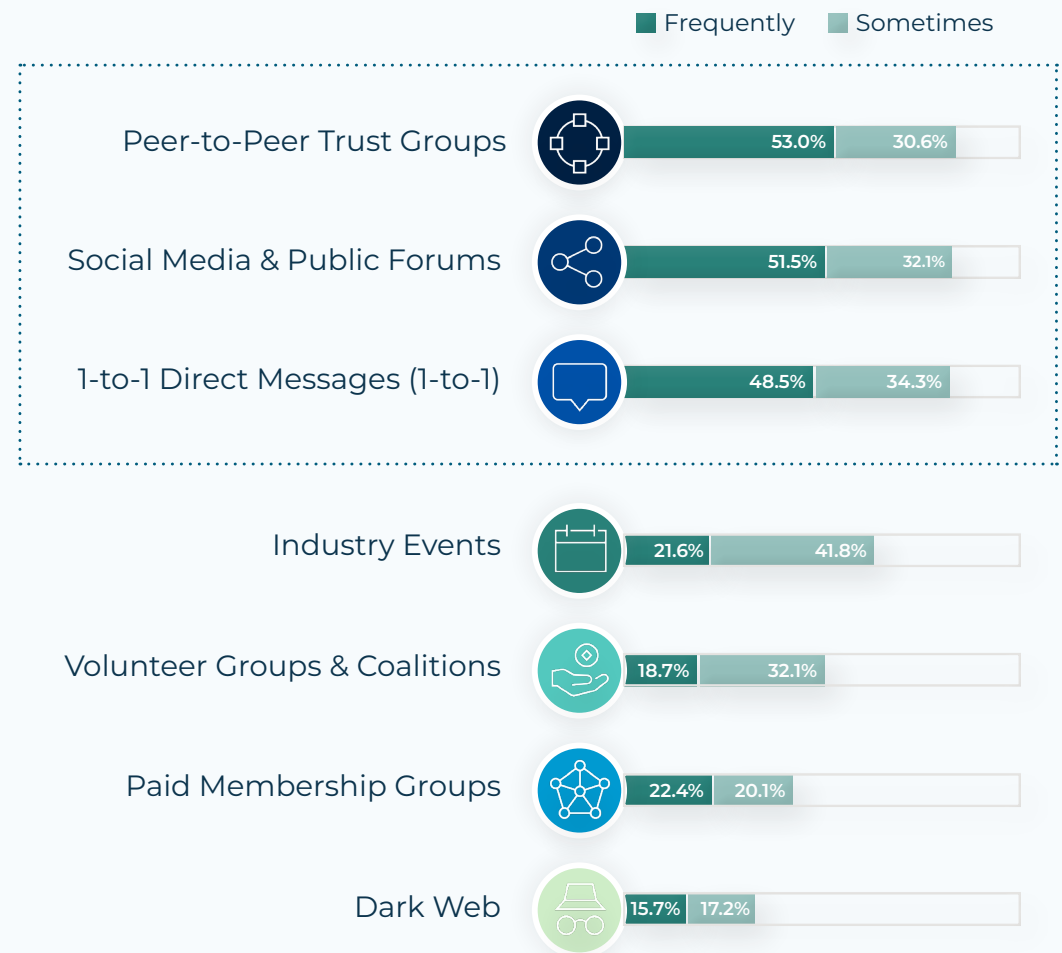
Participation

Trust Groups, Social Media, and 1-to-1 have the most participation across the seven methods presented. The top methods showcase an interesting spread: from the most accessible and public, to harder-to-access private groups, to the most exclusive (and manual) form of 1-on-1 networking.

Free & Free-Form

Staying active in these three free methods is mostly ad hoc, based on individual contributions and relationships, versus organizational and institutional ties.

WHAT KINDS OF CTI NETWORKING DO YOU PARTICIPATE IN?



DATA DEEP DIVE




Quality

1-to-1 and Trust Groups made top three across all factors for perceived quality.

Social Media ranked first in “timeliness,” third in “value,” and third in “actionable,” while Dark Web ranked second “uniqueness.”




However, when combining all votes of quality, Paid Membership Groups ranked third overall.

Combined Quality Ranking




-  1-to-1 Direct Messages
-  Peer-to-Peer Trust Groups
-  Paid Membership Groups

WHAT METHODS ARE...




Valuable?

-  1-to-1 Direct Messages
-  Peer-to-Peer Trust Groups
-  Social Media & Public Forums




High Confidence?

-  1-to-1 Direct Messages
-  Peer-to-Peer Trust Groups
-  Paid Membership Groups


Actionable?

-  1-to-1 Direct Messages
-  Peer-to-Peer Trust Groups
-  Social Media & Public Forums

Timely?

-  Social Media & Public Forums
-  Peer-to-Peer Trust Groups
-  1-to-1 Direct Messages

Unique?

-  1-to-1 Direct Messages
-  Dark Web
-  Peer-to-Peer Trust Groups

DATA DEEP DIVE




Results

1-to-1, Trust Groups, and Social Media consistently beat out other methods when assessing which methods played a role before, during, and post attacks.

An Indicator of Impact




While these results aren't the only benefits of CTI networking, they can indicate real-world, on-the-job impact.

Combined Results Ranking




-  1-to-1 Direct Messages
-  Peer-to-Peer Trust Groups
-  Social Media & Public Forums

WHAT METHODS...




Helped detect or prevent an attack?

-  1-to-1 Direct Messages
-  Peer-to-Peer Trust Groups
-  Social Media & Public Forums

Provided value during an attack?

-  1-to-1 Direct Messages
-  Peer-to-Peer Trust Groups
-  Social Media & Public Forums

Contributed to remediation or post-incident analysis?

-  Peer-to-Peer Trust Groups
-  1-to-1 Direct Messages
-  Social Media & Public Forums

DATA DEEP DIVE

Comparison

The charts along the right showcase levels of respondent participation, perceived value, and results of each method.



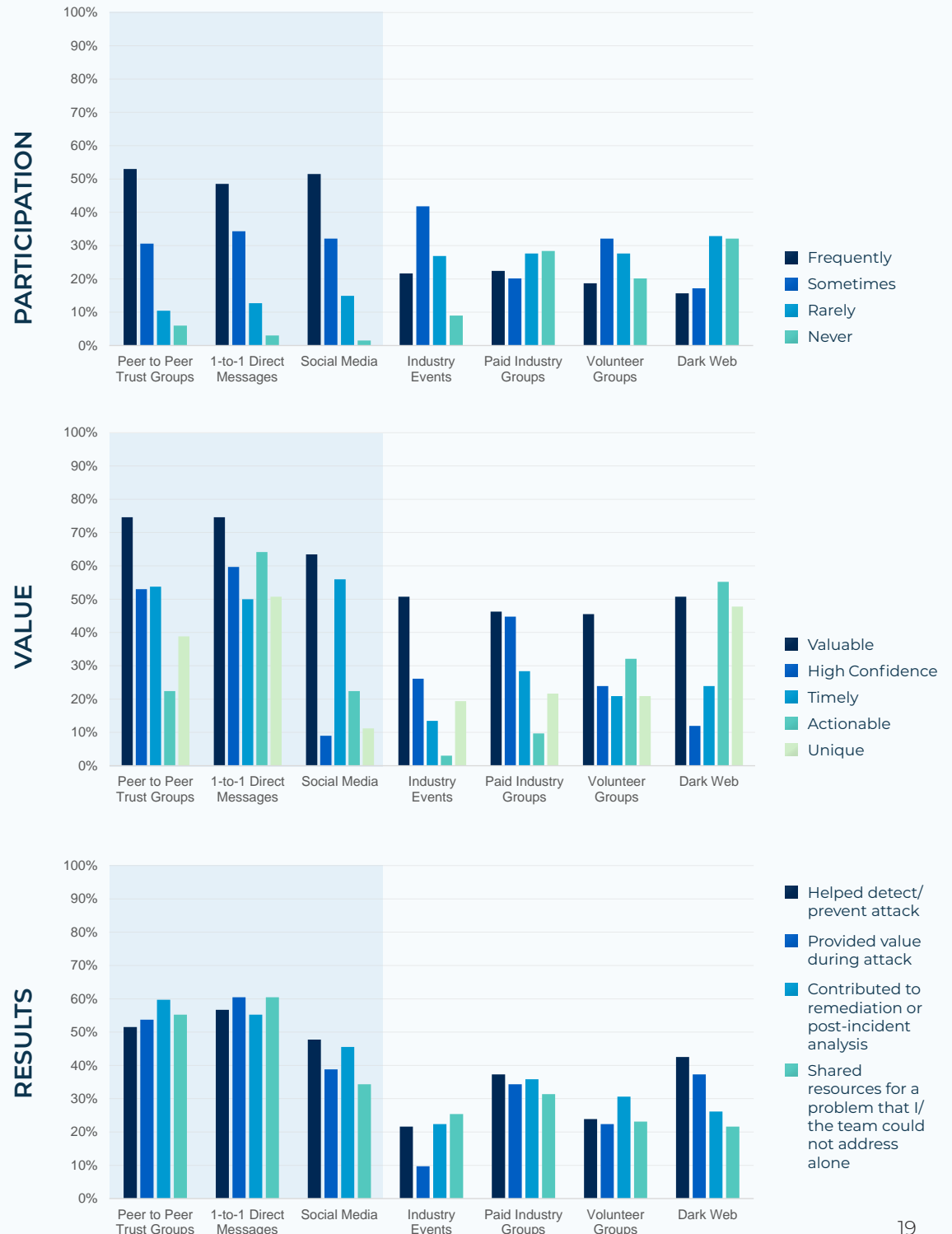
1-to-1 and Trust Groups Win Out

1-to-1 Direct Messages and Peer-to-Peer Trust Groups were consistently high-scoring across all three measures.



Don't Underestimate Social

While perceptions of Social Media & Public Forums were lower on key factors like confidence, actionability, and uniqueness of data, it made an outsize impact on results compared to other methods.



INSIGHTS

How and Why Individuals Network

CTI Networking Offers Key Advantages

“Networking in CTI helped me...”

(Agree & Strongly Agree)

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

Sources for action and awareness.

Respondents reported high levels of agreement in ingesting and acting on various types of CTI content. Statements regarding working with others (50%) and feeling less siloed (65%) had moderate levels of agreement, demonstrating the success found from actionable and timely networking.

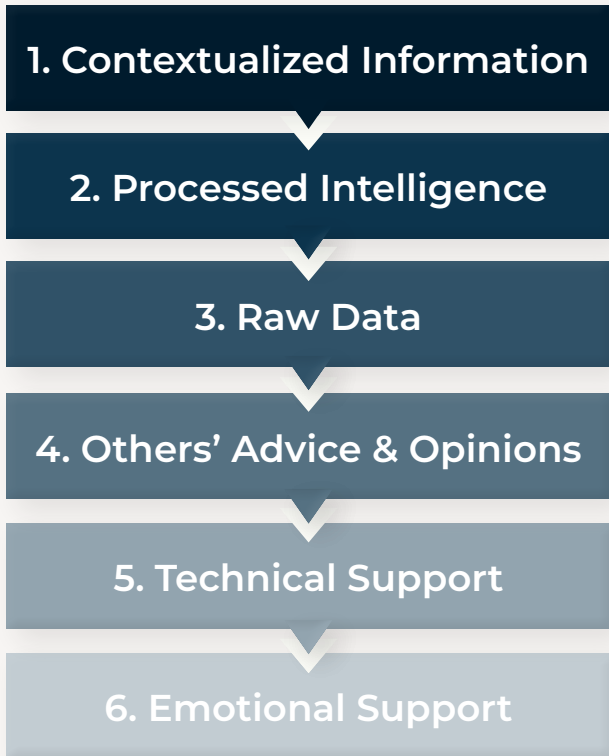
“ There have... been multiple times where simply understanding the scope of some activity, quickly and via the input from trusted individuals, has **directly led to detecting and mitigating malicious activity.**”

“ During the [redacted APT] breach... We didn't realize it was [redacted APT] until [reaching out to Trust Groups] **helped connect the dots for us.** That made a MAJOR change in the investigation and helped kick our IR into gear... the event was over 3,000 human work hours. Much of what we did for remediation was based on **what we learned in speaking to others.**”

“ **[Building] a bigger picture** due to multiple vantage points of threat actors... We've been able to confirm overlap [with trusted CTI parties] and assess their collection and analysis methodologies that matched ours and use that to build a more complete picture.”

What's Valued Most Differs By Job Function

WHAT'S PROVIDED THE MOST VALUE? (ALL)



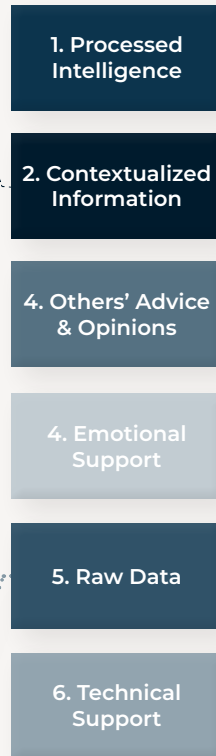
INCIDENT RESPONSE



SECURITY OPERATIONS



EXECUTIVE LEADERSHIP



All ranges of the data-info-intel spectrum ended up on top.

Which level? That depends on who you ask.

Raw data was particularly controversial: #1 for Incident Response and #6 for Security Operations. Unsurprisingly, Executive Leadership most preferred Processed Intelligence and Contextualized Information.

Those with both the least (<5) and most (15+) years of experience valued the advice of others more highly, reflecting different reasons between starting off and relying on a trusted network.

As years of direct CTI experience increase, the value of contextualized information correspondingly increases.

The smaller the organization, the more value is placed on raw data.

The larger the organization, the more value is placed on the advice & opinions of others.

Highly Recommended For All Levels

“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

The survey’s strongest consensus.

Out of all questions asked, this statement had the highest level of agreement (only 2% disagreed). This tied to an unexpected challenge revealed in qualitative responses.

A handful noted their **biggest barrier** was related to personal fear: impostor syndrome, feeling too new or unknowledgeable, or not being able to contribute ‘more.’

Meanwhile, about 50% of those who shared **advice** directly addressed this by encouraging others to participate, share what they can, and not be hampered by personal fears.

The following page summarizes themes of key advice: **be active, trustworthy, careful, and strategic.**

“ Do not be afraid to bring new ideas to the table. I think we are afraid of **being wrong or looking incompetent**. Discussing new ideas, brainstorming, and sharing only **makes us stronger.**”

ADVICE BY AND FOR THE CTI COMMUNITY

“What advice would you share with others?” (Edited for grammar and clarity)

- 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”

DATA DEEP DIVE

WHAT ARE THE RESULTS OF YOUR NETWORKING EFFORTS?

Networking in CTI has helped me...

■ Strongly Agree ■ Agree



DATA DEEP DIVE

HOW OFTEN DO YOU PARTICIPATE IN THE FOLLOWING?

■ Frequently ■ Sometimes



Both respondent groups that had CTI as their primary job function and those with 10+ years of experience were more likely to create frameworks and participate in peer reviews.

DATA DEEP DIVE

WHAT HAS PROVIDED YOU THE MOST VALUE?



The ranking above shows the combined average of all respondents. This rank holds true for those with CTI as their primary job function.

The right showcases interesting differences in rankings, observed with other job functions and years of total work experience.

INCIDENT RESPONSE	SECURITY OPERATIONS	EXECUTIVE LEADERSHIP
1. Raw Data	1. Contextualized Information	1. Processed Intelligence
2. Processed Intelligence	2. Processed Intelligence	2. Contextualized Information
3. Others' Advice & Opinions	2. Technical Support	3. Others' Advice & Opinions
4. Technical Support	4. Others' Advice & Opinions	4. Emotional Support
4. Contextualized Information	5. Emotional Support	5. Raw Data
6. Emotional Support	6. Raw Data	6. Technical Support

1-5 YEARS EXPERIENCE	15+ YEARS EXPERIENCE
1. Contextualized Information	1. Processed Intelligence
2. Others' Advice & Opinions	2. Contextualized Information
3. Raw Data	3. Others' Advice & Opinions
4. Technical Support	4. Raw Data
5. Processed Intelligence	5. Technical Support
6. Emotional Support	6. Emotional Support

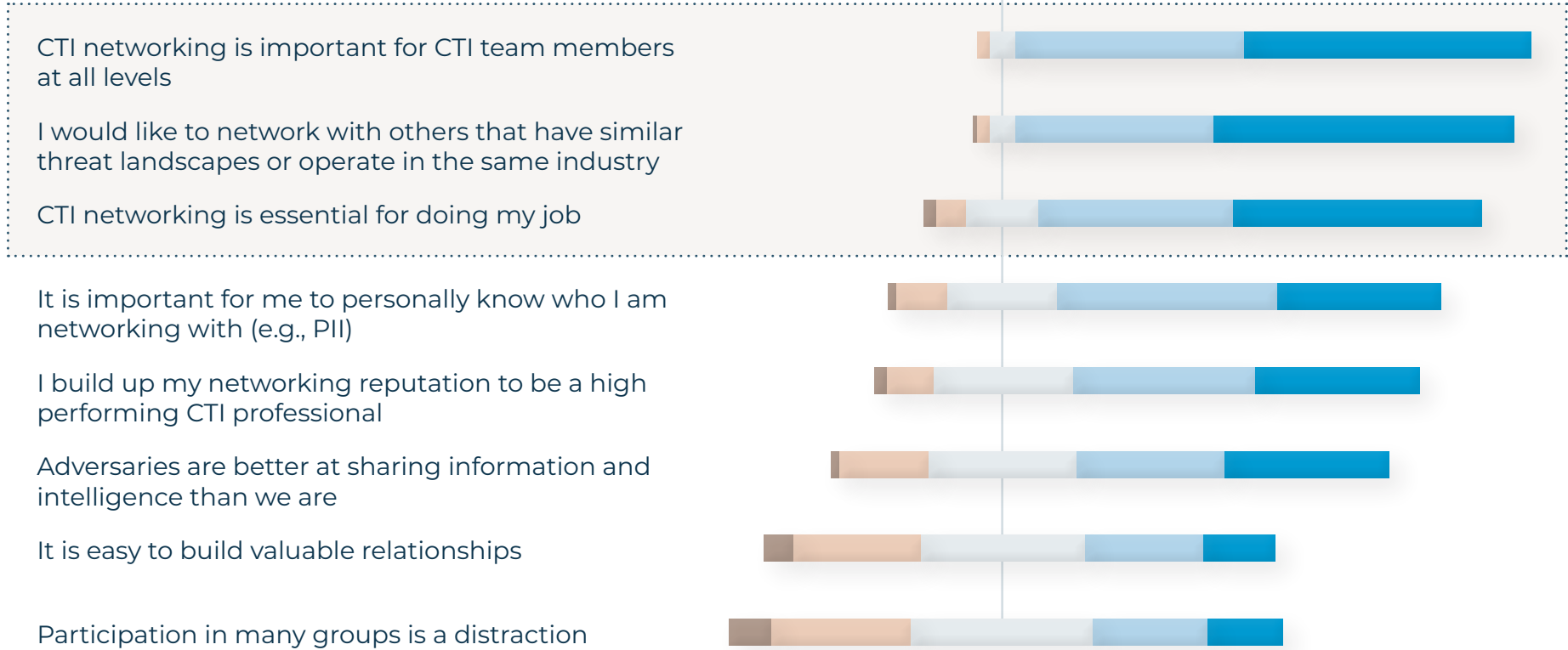
DATA DEEP DIVE

OPINIONS

Strongly Disagree

Neutral

Strongly Agree



Qualitative responses validated a strong, unfulfilled desire to network with more peers in the same industry, region, and areas of specialization.

No respondents “strongly disagreed” and very few “disagreed” that CTI networking was important for team members of all levels, highlighting a shared belief that all CTI roles have perceived benefits from networking.

INSIGHTS

The Role Organizations Play

Most Respondents Are (Very) Happy

Job satisfaction was consistently high across all demographics.

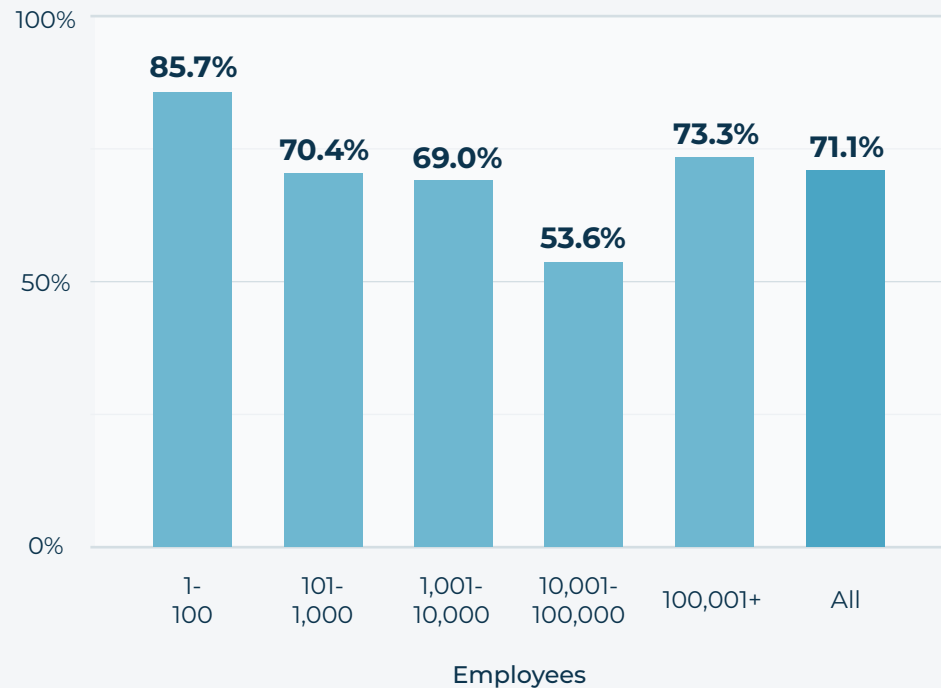


Respondents at the smallest and largest organizations were most likely to rate themselves satisfied or highly satisfied.

Those at organizations with 10K-100K employees were the least likely to rate themselves satisfied.

SATISFACTION BY ORGANIZATION SIZE

% Rating Satisfied & Highly Satisfied



When Individual Enthusiasm Meets Blockers

86%

Spend at least an hour every week networking

61%

Have some or highly standardized processes

25%

Measure or report on effectiveness of efforts

TOP CHALLENGES



No Time



Noisiness



Legal Liability, Confidentiality

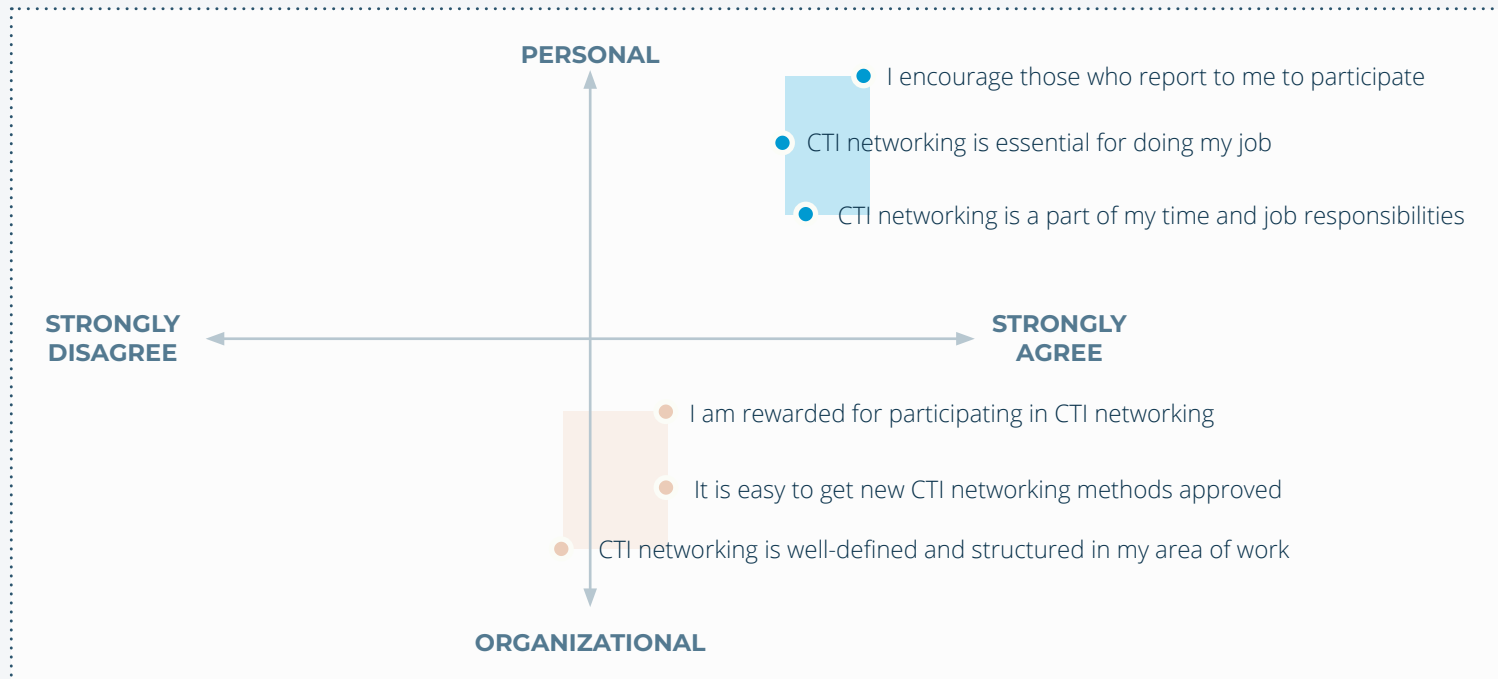


Sharing Restrictions

Respondents dedicate time each week to CTI networking, and over half had at least some standards in place for what is collected. Despite this, only a quarter of respondents actually measure or report on the effectiveness of their efforts, and 64% stated that the biggest challenge they faced was having no time. Two other top challenges addressed externally imposed limitations to sharing.

- // **Time.** I wish I had more of it during the workday to focus on networking."
- // **Fear.** Fear of **sharing**, fear of **legal/administrative retribution** from the organization you support."
- // **Legal restrictions** or legal being slow to allow sharing and completely **watering down** what is shared."

There's Room for Development at Organizational Levels



CTI networking directly supports items like information sharing and strategic awareness found in cybersecurity maturity assessment models.

Yet, there is a significant contrast between **highly positive individual** and **more neutral organizational** sentiments around CTI networking.

For now, it's on the individual.

Given the direct impact on security posture and programs resulting from individual CTI networking participation, this is a key area for organizational development.

Organizational maturity, strategic, and operational planning would benefit from 1) acknowledging the role that CTI networking is **already playing** and 2) **incorporating efforts** within the program. From there, organizations can create structure, help remove barriers (within reason), and duly reward efforts.

DATA DEEP DIVE

Time Is of the Essence

Overall, respondents were most likely to spend at least 1-5 hours networking per week.

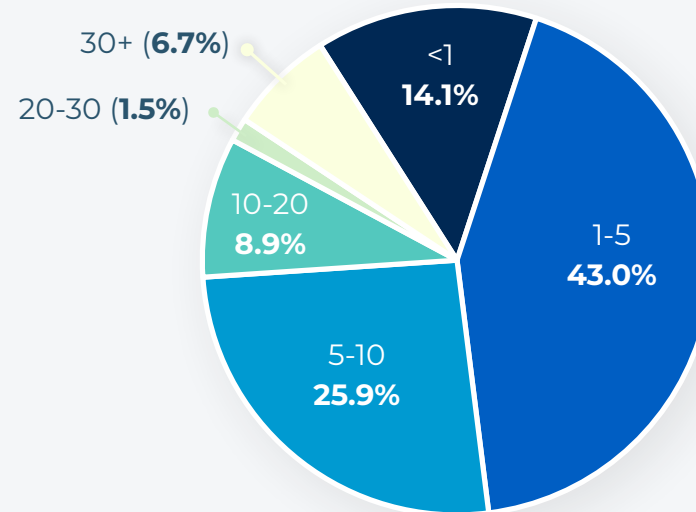
Respondents outside of North America spent the least amount of time networking (24% chose "less than 1 hour").

The More CTI, The More Structure

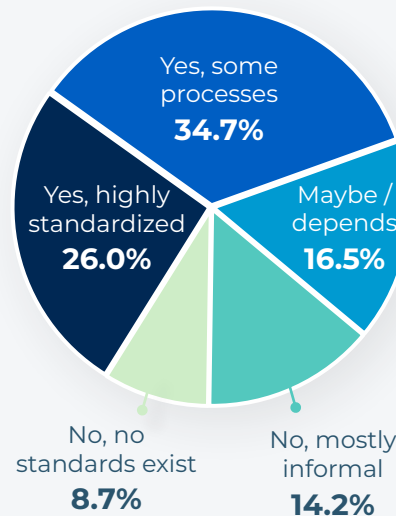
Respondents with CTI as their primary job function were more likely to have highly standardized processes (31%) and measure effectiveness (30%).

Similarly, respondents with >5 years in CTI related work revealed similar increases in the likelihood of having highly standardized processes (42%) and measuring effectiveness (33%).

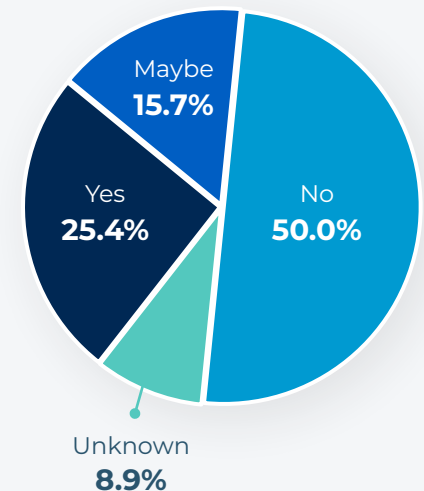
TIME PARTICIPATING IN CTI NETWORKING
(hours spent per week)



DO YOU HAVE FORMALIZED OR STANDARDIZED WAYS TO MANAGE WHAT YOU COLLECT?



DO YOU MEASURE EFFECTIVENESS?



DATA DEEP DIVE

Different Blockers

Lack of budget and skills are common challenges impacting security and CTI teams.

However, for CTI networking, which is primarily seen as an individual undertaking, those specific issues fell lower in the ranks. Instead, lack of time, noisiness, and sharing restrictions/policies took the top ranks.

(SANS Institute, 2021 CTI Survey)

There was no shortage of open-ended responses validating lack of time as a leading obstacle

Time. I wish I had more of it during the workday to focus on networking.
 Time
 Time and oversubscription.
 Time
 Too busy
 Time
 Time.
 Time
 Lack of time.
 Not enough time in the day.
 Not enough people or hours in the day.
 The number of hours in a day
 Personally, I don't have the time to commit to long-form sharing projects
 Time (small team with limited bandwidth)
 TIME. One-on-one communications are strong, but the time this takes is just ridiculous.
 Trust groups are fantastic, but again, the more threads you have to monitor, take part in, etc., the more TIME it all takes.
 I would think it's the time right now in my current role.
 No time for networking, frankly.
 Time and money
 Time to label CTI to apply to security incidents
 Not enough time/return of investment shown

WHICH CHALLENGES IMPACT YOUR CTI NETWORKING?



CONCLUSION

Where do we go from here?

CONCLUSION

The end of the beginning.

This research served as a starting look into the nebulous, even secretive, world of CTI networking and its impact.

The results shared 1) how different methods stack up, 2) how and why individuals participate, and 3) the role organizations play in CTI networking.

While the survey had significant limitations (small sample size, over-representation of North American and for-profit CTI respondents), the findings validated industry “hunches” with data.

What we found is that while CTI networking participation is **deemed beneficial** to professionals of all levels and relevant roles, it is contained to individual efforts and treated as an **afterthought** in the organization.

With this initial benchmark of current behaviors, opinions, and results, we hope to push the field towards more effective, inclusive, and strategic CTI networking efforts – both to help practitioners achieve greater success and for organizational decision-makers to best leverage its value in developing security programs.

Areas for Further Research



LARGER SURVEY

Gather a significantly larger respondent set with improved representation from diverse employer types and international regions.



IN- AND EX-CLUSIONARY CULTURE

Explore the impact of biases, groupthink, and other prejudices that hinder networks and create barriers to representation.



GUIDANCE BY CAREER LEVELS

Dig deeper into how individuals in entry, mid, and senior stages in their CTI career can participate in and leverage networking.



COMPANY CASE STUDIES

Research “success stories” of specific organizational strategies tying CTI networking to security program maturity.

INTERESTED IN PARTICIPATING IN FUTURE RESEARCH?

Contact Grace Chi at grace@pulsedive.com

APPENDIX

APPENDIX

Survey on CTI Networking (2021)

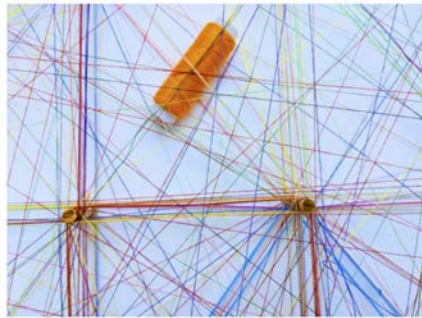
Sign in to Google to save your progress. [Learn more](#)

Context

Security teams cannot sustainably operate in an intelligence silo. There's continuous 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". So what are they doing, and what works?

We're asking you to find out.



Survey Form

All respondents filled out an online Google Forms survey between November 10 and December 20, 2021. PII was not required to submit responses.

The form consisted of 7 parts:

- Introduction (pictured above)
- Demographics
- Methods
- Behaviors
- Opinions & Attitudes
- Open-Ended Questions
- Submit

SURVEY QUESTIONS: DEMOGRAPHICS

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 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 QUESTIONS: METHODS

What kinds of CTI networking do you participate in? *

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

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

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 direct messages/emails	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social media & public forums	<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: free trust groups (e.g. invite-only Discord, Slack, email lists)	<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 (e.g. ISACs)	<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"/>
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 direct messages/emails	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Social media & public forums	<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: free trust groups (e.g. invite-only Discord, Slack, email lists)	<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"/>
Paid membership groups (e.g. ISACs)	<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"/>
Other (if answered above)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

APPENDIX

SURVEY QUESTIONS: 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 follow discussion channels	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Develop mailers, distribution lists	<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 processes with best practices
- Yes, I follow some processes
- Maybe / it depends
- No, mostly informal with some guidelines
- No, no standards exist
- N/A

Do you measure or report on the effectiveness of CTI networking efforts? *

- Yes
- No
- Maybe
- Unknown

Please rank (each number may only be used once) the following by what has provided you the most value: *

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

	1	2	3	4	5	6
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"/>
Emotional support	<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"/>
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"/>
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"/>

Do you break organizational policy/rules during CTI networking? *

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

APPENDIX

SURVEY QUESTIONS: OPINIONS & ATTITUDES

How satisfied are you in your current job? *

	1	2	3	4	5	
Very unsatisfied	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Highly satisfied

What is your organizational culture for CTI networking? *

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	N/A
It is easy to get new CTI networking methods approved	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CTI networking is well-defined and structured in my area of work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CTI networking is a part of my time and job responsibilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I encourage those who report to me to participate	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am rewarded for participating in CTI networking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My leadership is aware of the extent of my CTI networking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	N/A
I build up my networking reputation in order to be a high performing CTI professional	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CTI networking is essential for doing my job	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is easy to build valuable relationships	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Participation in many groups is a distraction	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CTI networking is important for CTI team members at all levels	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I would like to network with others that have similar threat landscapes or operate in the same industry	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Adversaries are better at sharing information and intelligence than we are	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is important for me to personally know who I am networking with (e.g. PII)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	N/A
Feel less like a silo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Get valuable threat data	<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 day-to-day basis	<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"/>
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"/>
Take proactive measures	<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"/>
Implement and operationalize technologies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

APPENDIX

OPINIONS & ATTITUDES, CON'T.

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

	No impact at all	Not much impact	Neutral	Some impact	A lot of impact	N/A
Sharing restrictions (e.g. TLP)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legal liability or confidentiality (e.g. NDA)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Noisiness (e.g. false positives)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Competitive advantage (e.g. IP)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of in-house skills to take action	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
No time	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of leadership buy-in	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Retaliation (e.g. targeted by attacker)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lack of trust	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
No budget	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reputational fear	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

SURVEY QUESTIONS: OPEN-ENDED

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

Your answer

What is your biggest current obstacle in CTI networking?
Specific examples and impact are helpful.

Your answer

What changes would vastly improve the value of your CTI networking efforts?

Your answer

Describe a past experience where CTI networking yielded interesting results.
Describe the context, methods, participant types, and consequences.

Your answer

Conclusion

If you are interested in being contacted for follow-up research or to receive results, please provide your information below.
If not, submit the form. 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

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.

APPENDIX

Sources

- Al-Ibrahim, O., Mohaisen, A., Kamhoua, C.A., Kwiat, K.A., & Njilla, L.L. (2017). *Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligence*. ArXiv, abs/1702.00552. Retrieved 2021, from <https://arxiv.org/pdf/1702.00552.pdf>.
- 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>.
- 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>.
- Garrido-Pelaz, R., González-Manzano, L., & Pastrana, S. (2016). *Shall We Collaborate?: A Model to Analyse the Benefits of Information Sharing*. Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. Retrieved 2021, from <https://arxiv.org/pdf/1607.08774.pdf>.
- 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/>.
- 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>.
- Office of the Director of National Intelligence. (2018). *A White Paper on the Key Challenges in Cyber Threat Intelligence: Explaining the "See it, Sense it, Share it, Use it" approach to thinking about Cyber Intelligence*. Retrieved 2021, from https://www.dni.gov/files/CTIIC/documents/White_paper_on_Cyber_Threat_Intelligence_ODNI_banner_10_30_2018.pdf.
- 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.

IS SHARING CARING?

A report on current cyber threat intelligence networking practices, results, and attitudes

CONTACT

Grace Chi

grace@pulsedive.com

