Sharing is Caring:

The deeply human side to CTI networking

IS SHARING CARING?

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

JANUARY 2022

CONTACT
Grace Chi
grace@pulsedive.com

February 4, 2022 | 11AM MST

euphoricfall | Cofounder @ Pulsedive

Grace / euphoricfall

Cofounder, Pulsedive

Front row seats to CTI teams

1) Tell me your favorite board game

2) Show me your coolest art projects

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

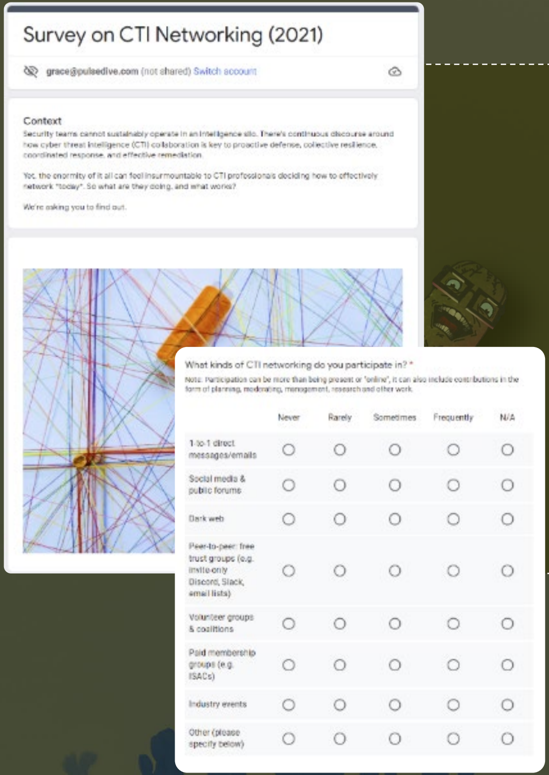
Need “more leadership and cultural buy-in - sharing not just IOCs but the context - the problems and solutions around those IOCs.”

“Sharing of technical data is very important for others to hunt, detect and prevent attacks. The lack of willingness to share this information is a huge burden to the CTI analyst who wants to share as well as collect.”

Benchmark CTI networking practices, results, and attitudes to provide data-based insights around:

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

Methodology



Survey on CTI Networking (2021)

grace@pulsedive.com (not shared) Switch account

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.

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	○	○	○	○	○
Social media & public forums	○	○	○	○	○
Dark web	○	○	○	○	○
Peer-to-peer: free trust groups (e.g. invite-only Discord, Slack, email lists)	○	○	○	○	○
Volunteer groups & coalitions	○	○	○	○	○
Paid membership groups (e.g. ISACs)	○	○	○	○	○
Industry events	○	○	○	○	○
Other (please specify below)	○	○	○	○	○

Google Form survey + interviews

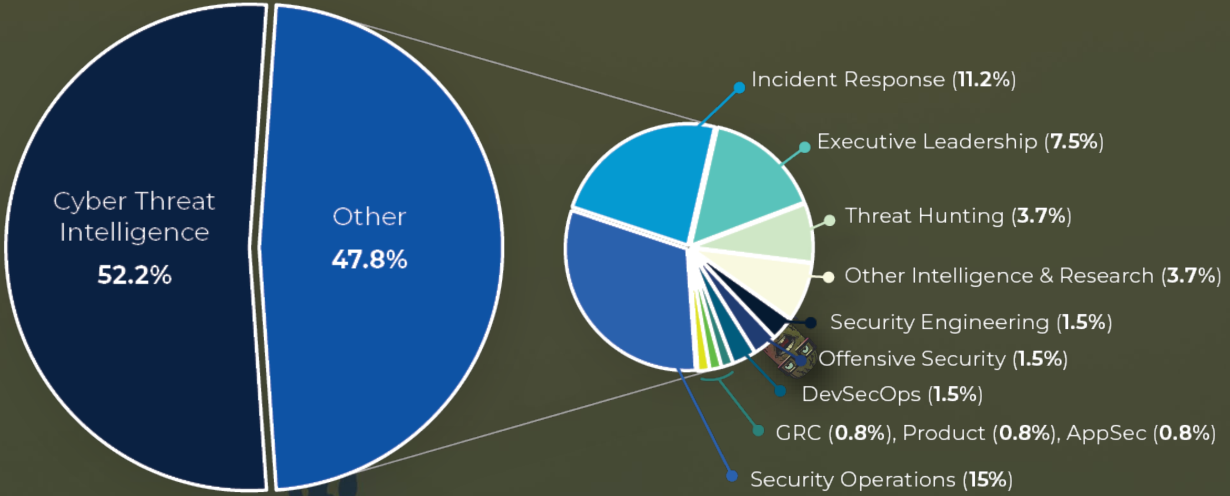
No PII, no compensation

Distributed through word of mouth

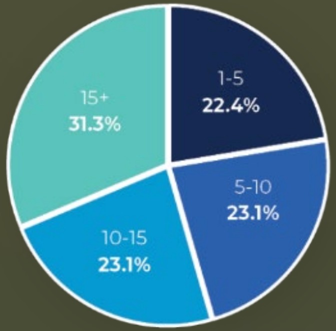
134 quantitative, 120 qualitative responses

DEMOGRAPHICS

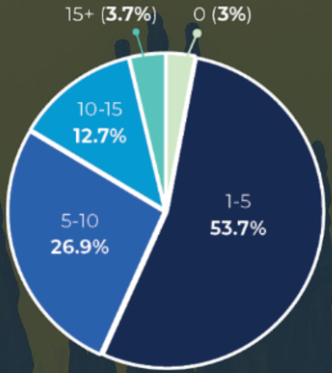
A representative spread of job functions and experience



PRIMARY JOB FUNCTION

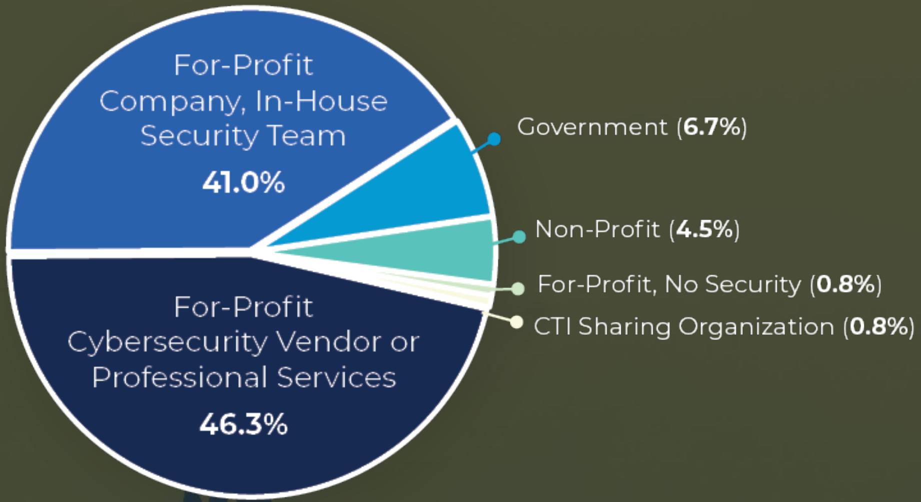


WORK EXPERIENCE

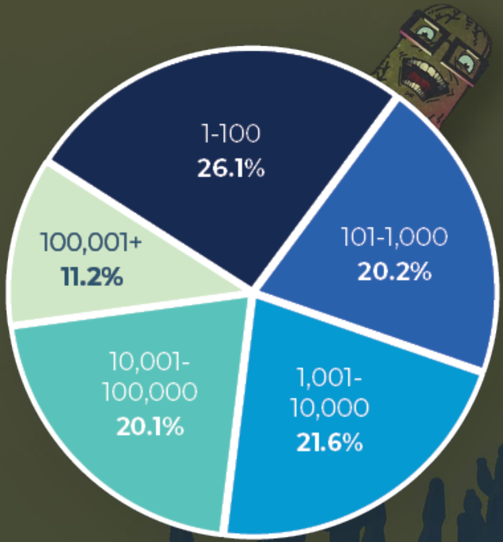


CTI EXPERIENCE

Overwhelmingly for-profit, across all organization sizes

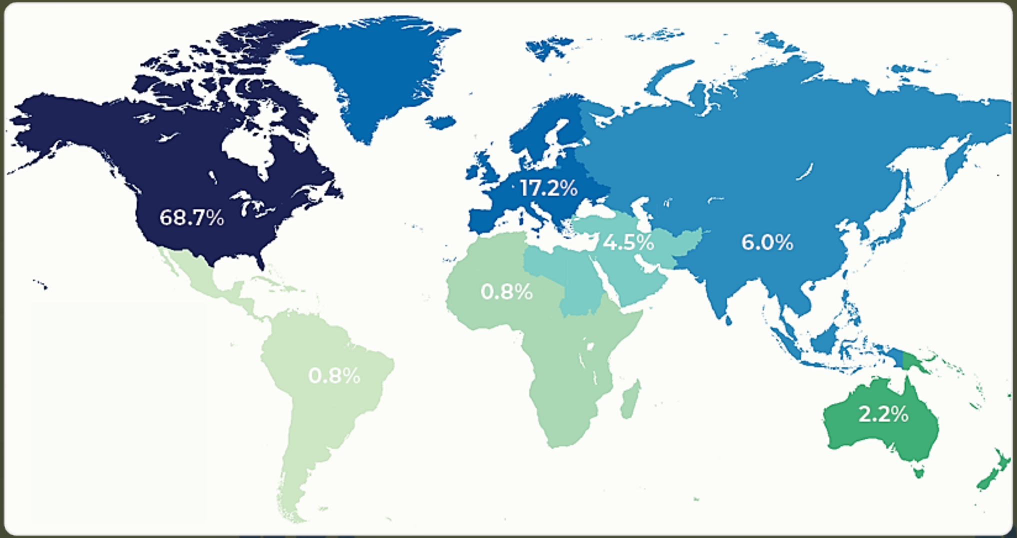


EMPLOYER TYPE



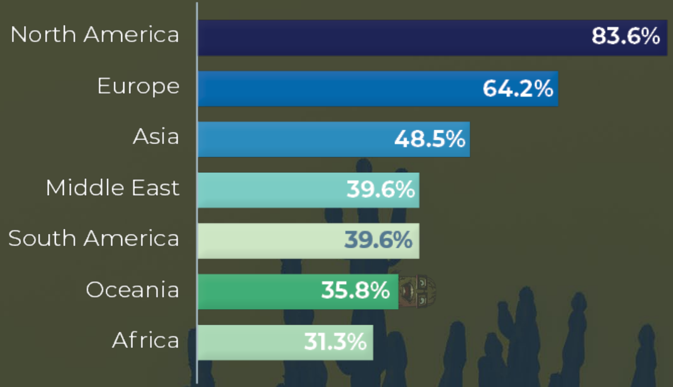
EMPLOYER SIZE

Majority NA-based, with international operations

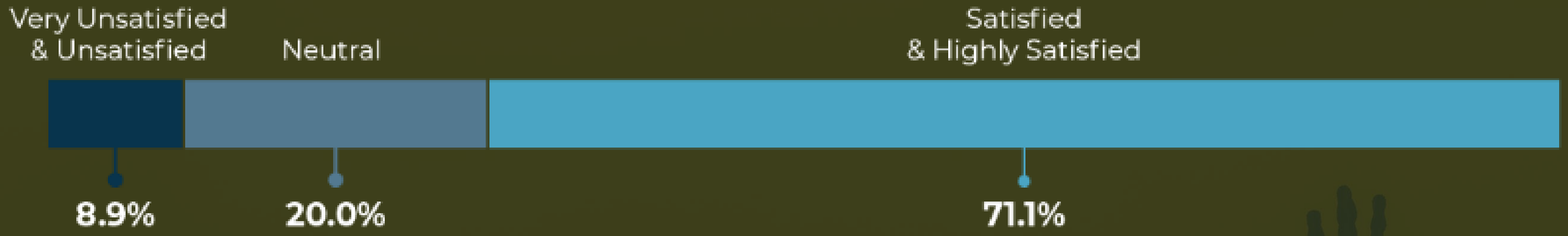


LOCATION

REGIONS OF OPERATIONS



Happy little cacti

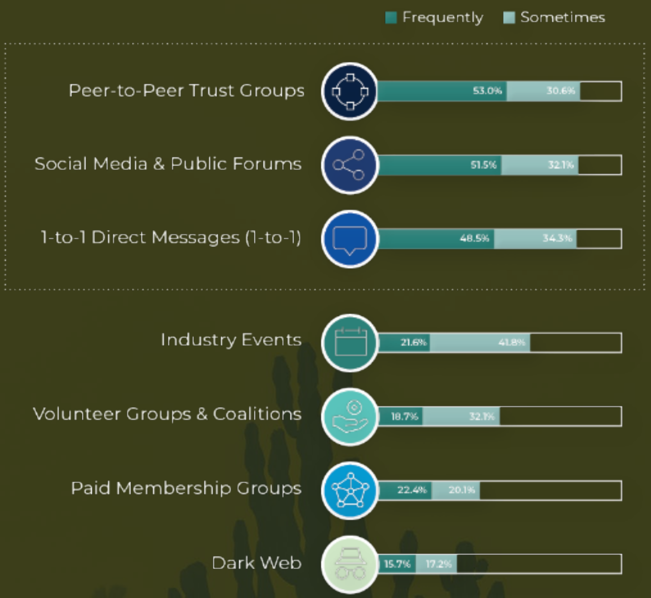


INSIGHTS

How Different Methods Stack Up

How different methods stack up

PARTICIPATION



QUALITY

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

Timely?

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

Actionable?

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

Unique?

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

RESULTS

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

1-to-1 & Trust Groups reign supreme (by far)

No shortcuts to the best peer-to-peer networks

Dominant across all dimensions

Private, personal reputation, reciprocal contribution

> “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% participation by employees of 100K+ orgs
46% increase by professionals with 10+ years exp compared to <10

Trust Groups
Top 2 across all dimensions of quality except uniqueness
10+ years and CTI professionals ranked Trust Groups even more positively

But don’t underestimate Social Media

Noisy. Chaotic. But popular.

Outperformed on impact

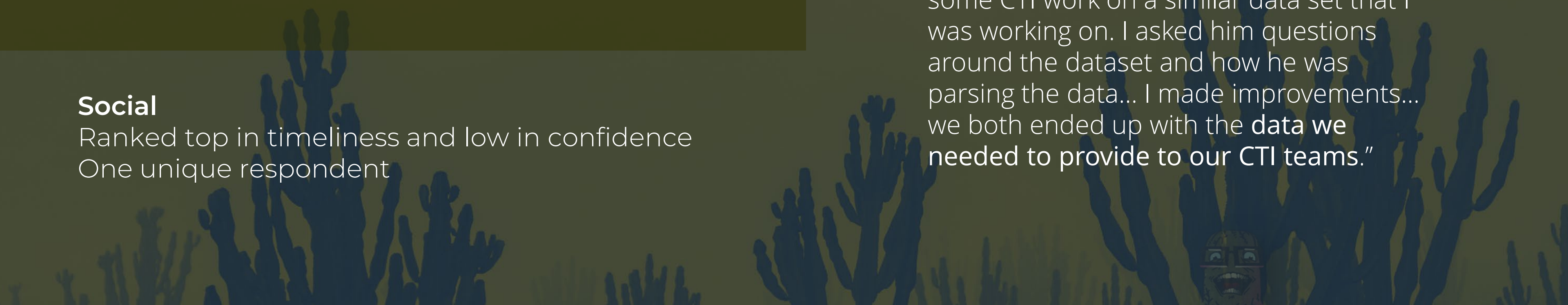
Great for short-term discovery and longer-term network building

Curate!

Social
Ranked top in timeliness and low in confidence
One unique respondent

> “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**.”



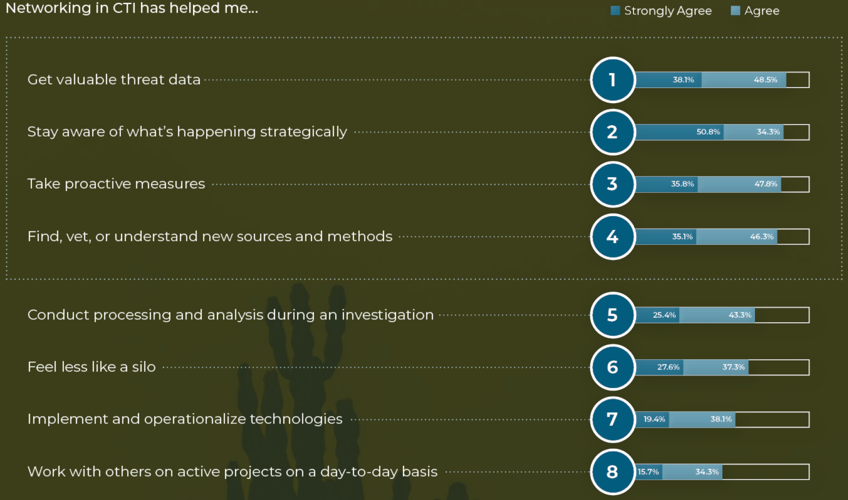
INSIGHTS

How and Why Individuals Network

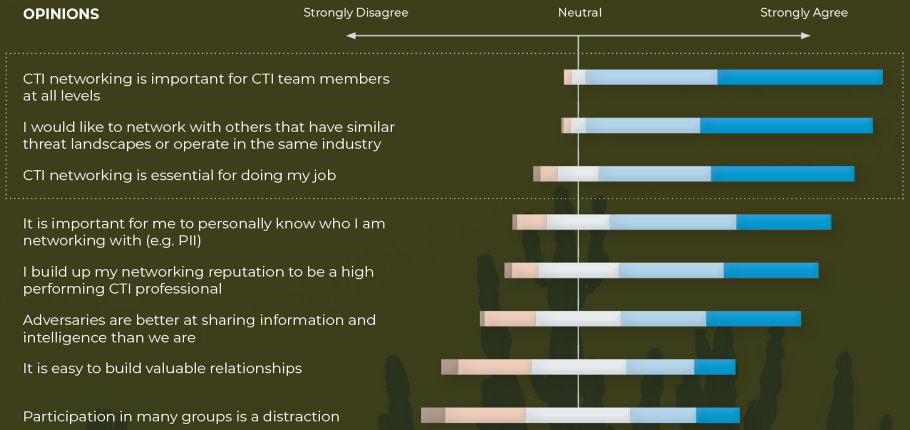
How and why individuals participate

WHAT ARE THE RESULTS OF YOUR NETWORKING EFFORTS?

Networking in CTI has helped me...



OPINIONS



CTI networking for action and awareness

87%

Get valuable threat data

85%

Stay aware of what's happening strategically

84%

Take proactive measures

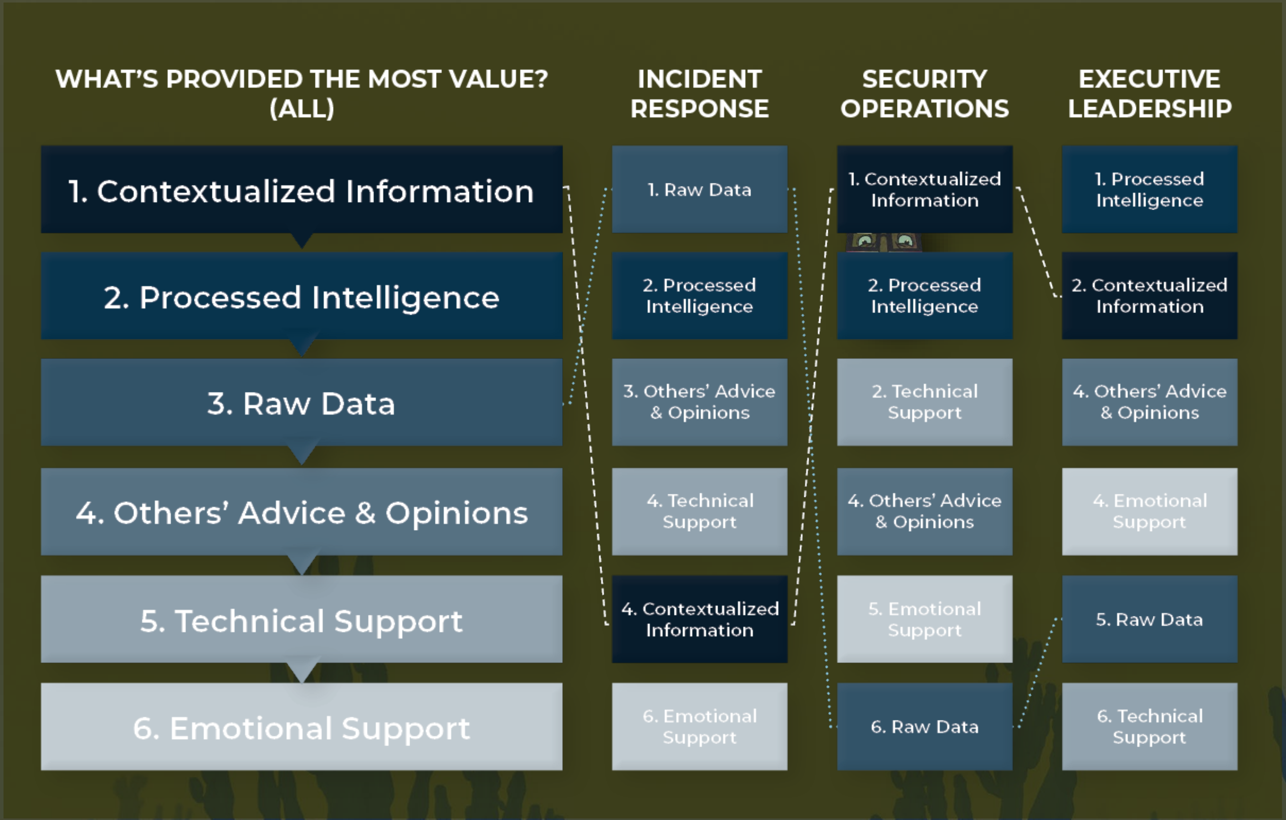
81%

Find, vet, or understand new sources & methods

> “During the [redacted APT] breach… We didn't realize it was [redacted APT] until [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.“

But what’s valued? Depends on whom you ask.



WHAT’S PROVIDED THE MOST VALUE? (ALL)	INCIDENT RESPONSE	SECURITY OPERATIONS	EXECUTIVE LEADERSHIP
1. Contextualized Information	1. Raw Data	1. Contextualized Information	1. Processed Intelligence
2. Processed Intelligence	2. Processed Intelligence	2. Processed Intelligence	2. Contextualized Information
3. Raw Data	3. Others’ Advice & Opinions	2. Technical Support	4. Others’ Advice & Opinions
4. Others’ Advice & Opinions	4. Technical Support	4. Others’ Advice & Opinions	4. Emotional Support
5. Technical Support	4. Contextualized Information	5. Emotional Support	5. Raw Data
6. Emotional Support	6. Emotional Support	6. Raw Data	6. Technical Support

Plus

Those with the least (<5) and most (15+) years experience valued advice more highly

Smaller orgs valued raw data more highly, while larger orgs placed more value on 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

An unexpected barrier: fear

Loads of advice & encouragement

> “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

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”

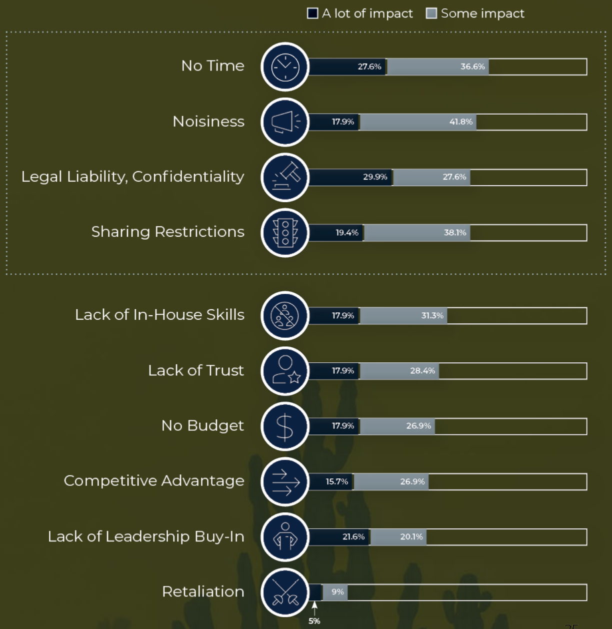
“Be skeptical with data shared, but also be generous to those that share as it can take quite a bit of courage and can often be novel”

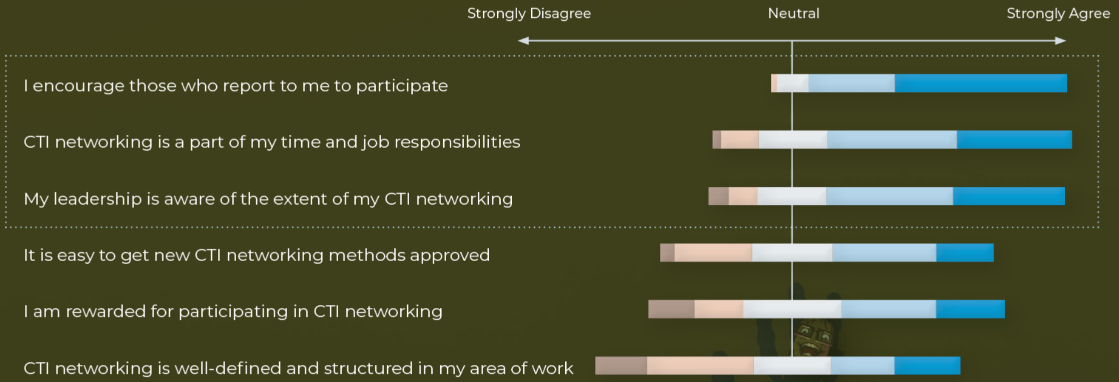
“Select trust groups based on impact” “If you’re struggling to find value early, move on”

INSIGHTS

The Role Organizations Play

The role organizations play





TLP White: there’s never enough time!

86%

Spend at least an hour every week networking

61%

Have some or highly standardized processes

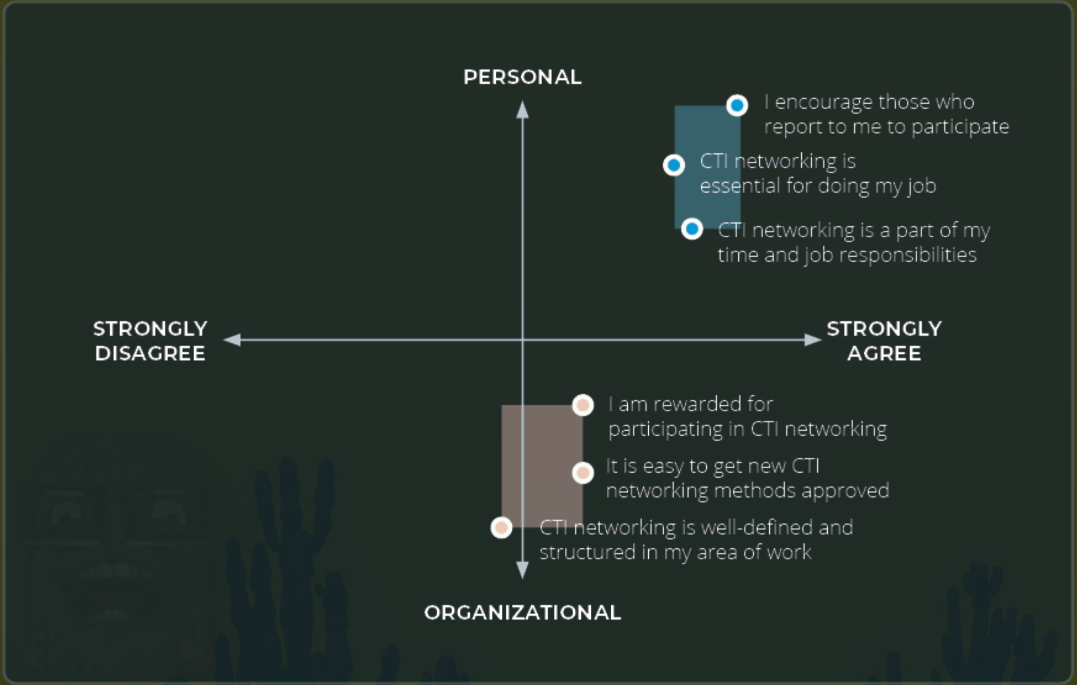
25%

Measure or report on effectiveness of efforts

TOP CHALLENGES

- No Time
- Noisiness
- Legal Liability, Confidentiality
- Sharing Restrictions

There’s room for development at organizations



> “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**.”

CONCLUSION

Where do we go from here?

What we found

How different methods stack up

Crowd favorites, DMs & Trust Groups, take the cake.

Social clinches third.

How and why individuals participate

Data? Information? Intel? All of the above.

Not a matter of *if* you should, but *how*.

The role organizations play

For now, it’s on you.

It’s time to acknowledge the impact CTI networking is already making.

The end of the beginning

- **Larger Survey**
- **In- and Ex-clusionary Culture**
- **Guidance By Career Levels**
- **Company Case Studies**

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.

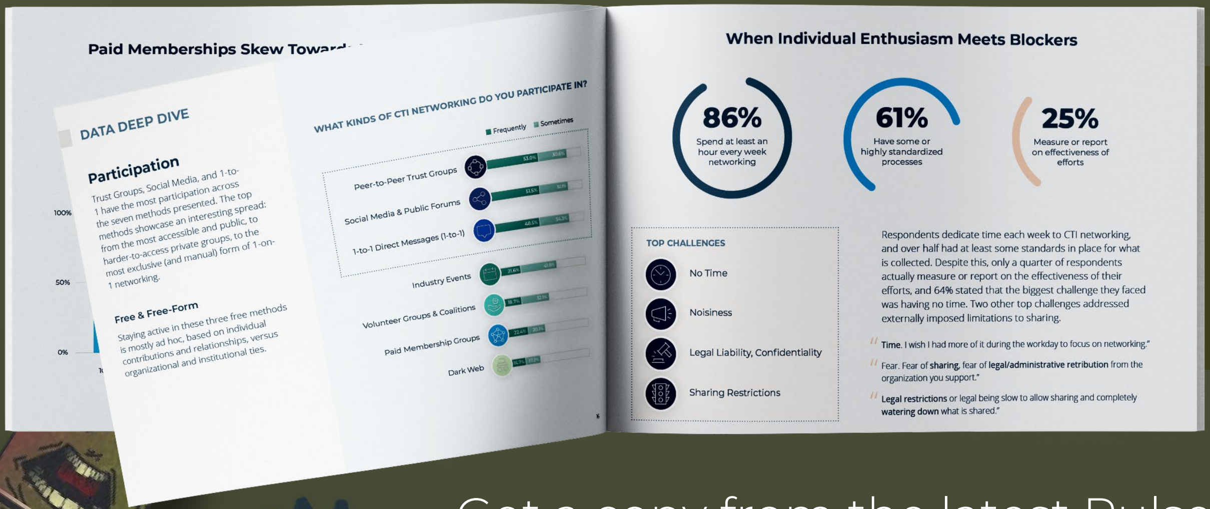
Office of the Director of National Intelligence. (2018). *A White Paper on the Key Challenges in Cyber Threat Intelligence: Explaining the "See it, Sense it, Share it, Use it" approach to thinking about Cyber Intelligence*. Retrieved 2021, from https://www.dni.gov/files/CTIIC/documents/White_paper_on_Cyber_Threat_Intelligence_ODNI_banner_10_30_2018.pdf.

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.

Get the whole report



Paid Memberships Skew Towar…

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 the 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?

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."

Contact

✉ grace@pulsedive.com

@euphoricfall

/in/graceschi

Did you find me on every slide?

Get a copy from the latest Pulsedive blog, or direct url:
pulsedive.com/downloads/ctinetworkingreport2022.pdf

(no, you won't need to enter your email, phone, soul, or anything else)