



THREAT INTELLIGENCE PRACTITIONERS' SUMMIT

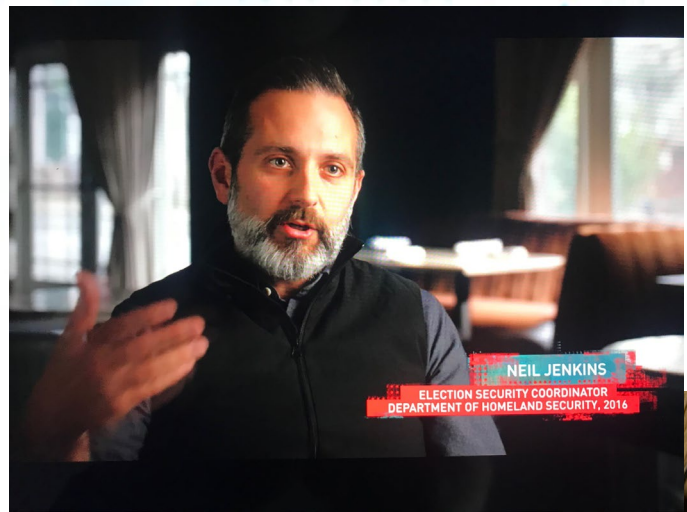
Threat intelligence Sharing in Practice – Lessons Learned from the Cyber Threat Alliance

Neil Jenkins
Chief Analytic Officer



Who Am I?

- Focus on Cyber Operations, Data Analytics and Sharing, Collaboration, Planning, Policy, and Strategy
- CTA's Chief Analytic Officer
- Institute of Security and Technology Adjunct Cyber Policy Advisor
- Former U.S. Department of Homeland Security (DHS) official
- Former support to Dept of Defense and Navy Cyber Efforts
- Ph.D. Chemist not doing Chemistry
- Owner of Maybelle
- Nerd

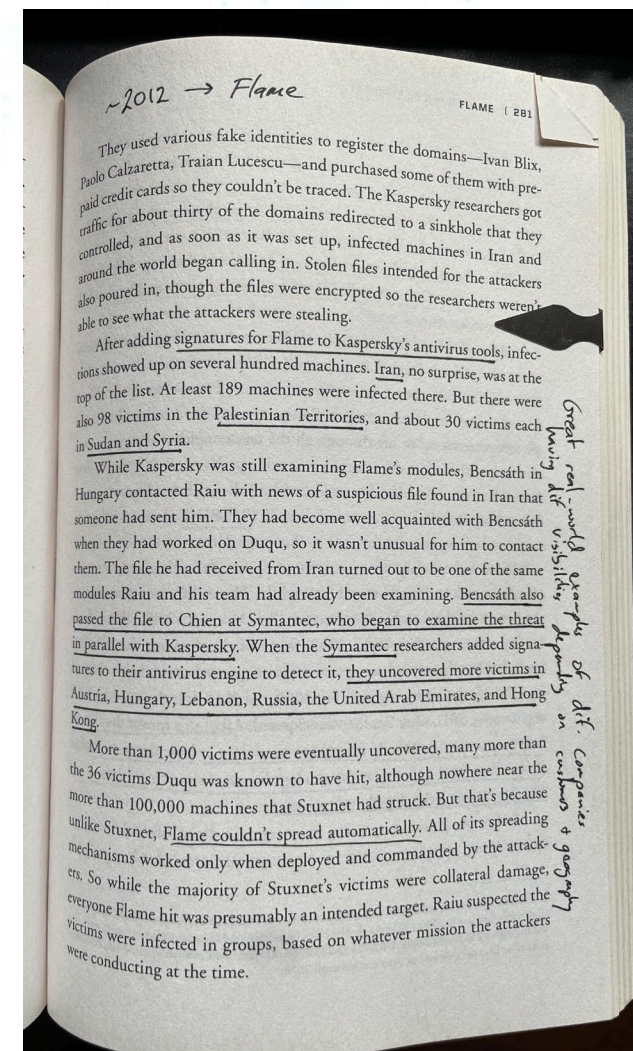


Before we begin... a reminder



Information Sharing... Still Talking After All These Years

- Practitioners and policy makers agree that increased information sharing would improve cyber defenses
- Virtually every panel, study, or review recommends more information sharing
- Technologies, frameworks, legislation (in U.S. at least), and policies all in place
- Yet information sharing often fails to live up to its promise
- The question is: Why?



Information Sharing's Faulty Assumptions



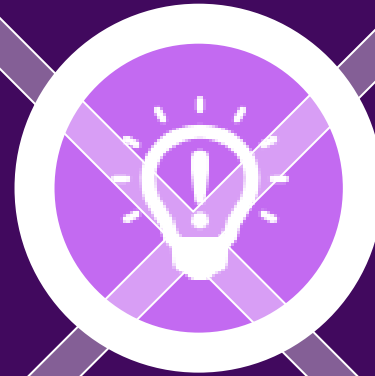
“Cyber Threat Information equals technical data”

Cyber Threat Information (CTI) consists of more than technical data



“All organizations should share that technical data”

Most organizations cannot produce or consume technical data



“Sharing is easy once connections are made”

Simply “connecting the pipes” is insufficient

Categories of Cyber Threat Information

Category of Cyber Threat Information	Examples of Information Conveyed	Intended Audience	Decision Example	Timeframe of Use
Technical	Indicators of malicious activity (e.g., malware hashes or IP addresses)	Cyber security vendors and network providers	Should the network security tool allow this packet through?	Immediate
Tactical	Details related to a specific/impending cyber attack	Network defenders (i.e., relevant staff and decision-makers)	Do we need to change a security setting today?	Short-term
Operational	Malware types; Attacker tactics, tools and procedures (TTPs)	Senior-level security personnel/managers	How often should we patch our networks?	Medium-term
Strategic	High-level information on changing cyber risk	Executives/senior decision-makers	Should we change our risk calculation because a new adversary is targeting our industry?	Long-term

Types of Cyber Threat Information

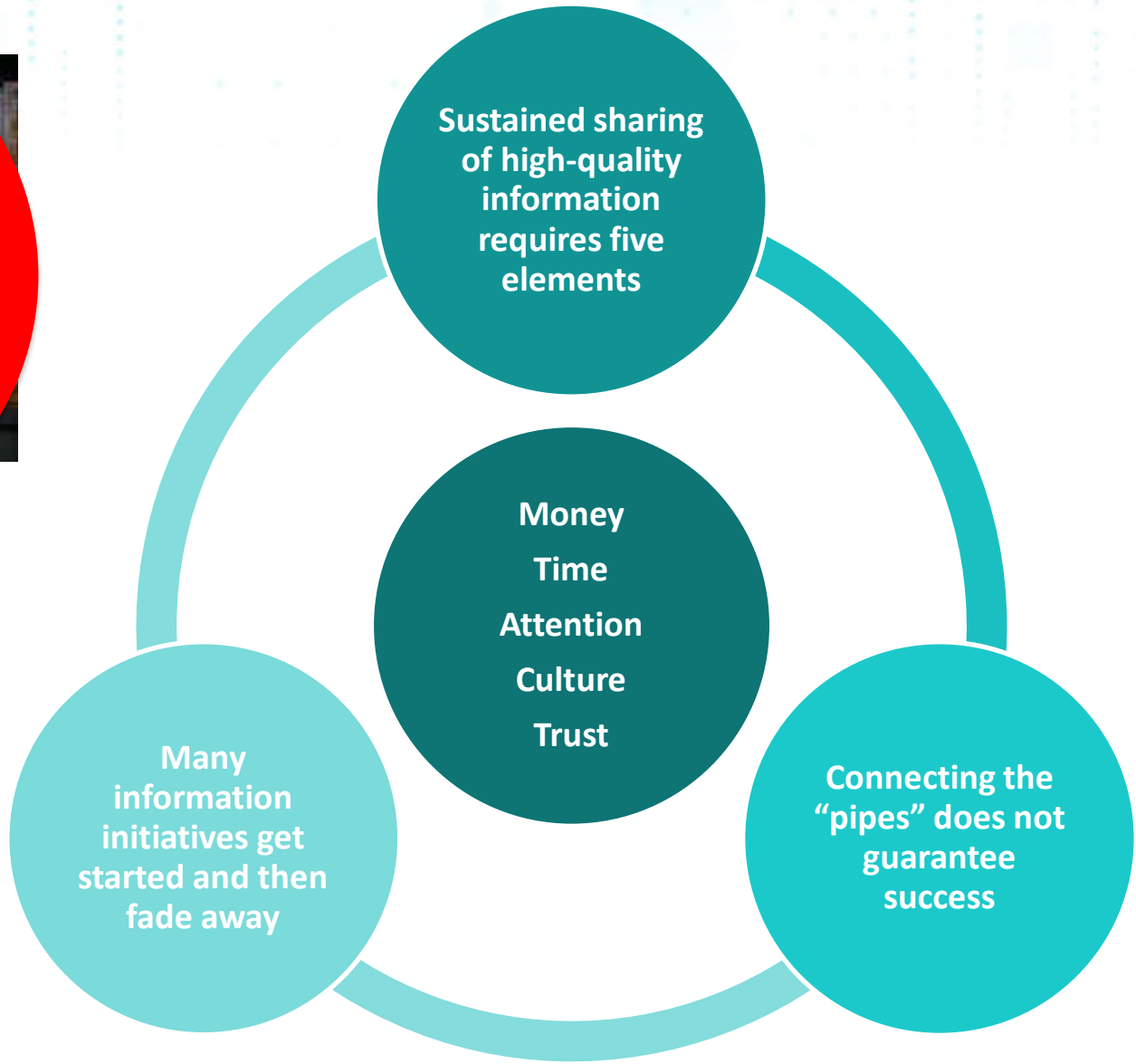
Technical Level	Tactical Level	Operational Level	Strategic Level
<p>Indicators & Sightings Hashes, binaries, IP addresses, URLs, etc.</p>	<p>Targeted Warnings Information about a malicious actor targeting an organization or type of organization in the near term</p>	<p>Vulnerabilities & Exploits Descriptions of security flaws in software and how bad actors can exploit them</p>	<p>Best Practices Methods for organizing, securing and maintaining IT networks to prevent, detect, respond and recover from cyber threats or incidents</p>
<p>Context Metainformation about technical indicators (e.g., date, time, and location of detection, type of organization targeted, etc.)</p>	<p>Situational Awareness Details of activity happening on a network and / or the broader internet at any given time</p>	<p>Defensive Measures Methods to mitigate exploits and counter adversary TTPs</p>	<p>Strategic Warnings General information about cyber threats, such as typical targets for an adversary and how they are evolving</p>
<p>Tactics, Techniques and Procedures Methods adversaries use to carry out malicious activity</p>		<p>Attribution Identifying who is responsible for specific malicious activity</p>	<p>Trends Identifying new technology, actions, or events likely to affect the digital ecosystem</p>
		<p>Ransom Information Communications, ransom demand and amount, wallet information</p>	



There's more to it than just pipes

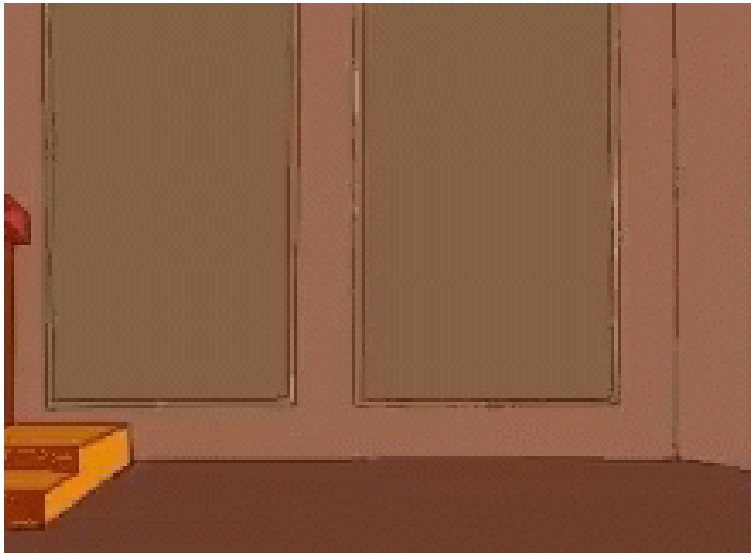


There's more to it than just pipes



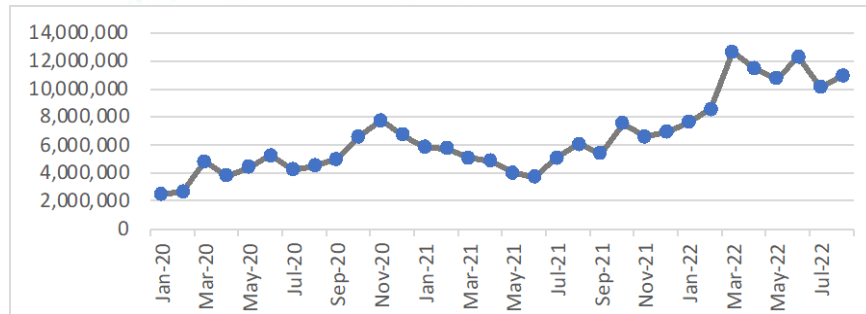
Review of Information Sharing Blockers

- Technology
- Lack of Frameworks
- Legal
- Policies
- Resources and Money
- Time and Attention
- Culture
- Trust



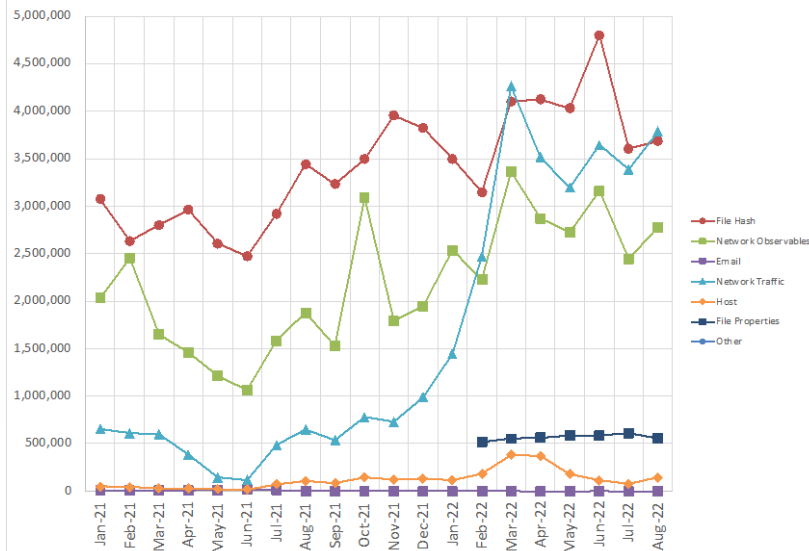
CTA's Model – Automated Sharing

Observable Sharing

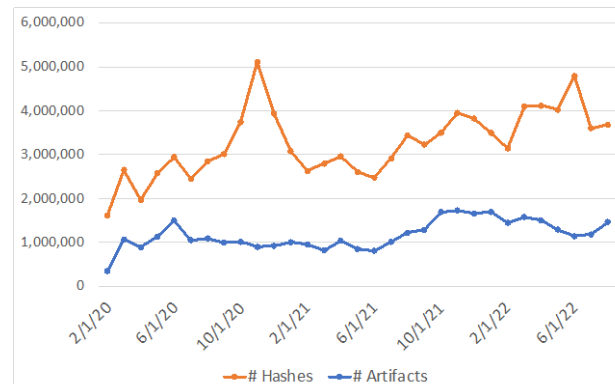


- CTA's Goal: Improve information sharing and collaboration between cybersecurity providers, enabling them to better protect their customers
 - Increase defensive leverage*
- Automated sharing of observables and context is required and enforced through a scoring algorithm
- Members that share above threshold have access to all the shared data
- No anonymous submissions
- We regularly review data quality and analyze the shared data to highlight successes and raise awareness of issues
- Nearly 300 million IOCs shared since Feb 2017

Observable Count by Type



File Artifact and Hash Sharing



*https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF



Automated information sharing needs occasional tweaks



VS



Update context, evaluate new data sources, find new IOCs, review confidence levels, etc.

Even with automation, not everything will be shared

- Members maintain customer and victim confidentiality
 - Some choose to only share indicators they see in multiple customers
 - Sharing ransomware samples or incident response data can be very difficult
- Members make sharing decisions based on customer agreements or tooling
 - Customers may not allow sharing of malware samples from their networks
 - Some vendors may not have access to data in security products in customer environments
- Some incidents may not have useful IOCs available to share

Bottom Line: No CTA member shares everything they have, and we certainly don't expect them to



Additional Lessons Learned from Automated Sharing

- “Just because you have an indicator, it doesn’t guarantee you can do something with it”
- Bureaucracies aren’t just for government anymore – siloed information and operations exist everywhere
 - If your automation is connected to Team A’s data, are you going to be able to get data from Team B, too?
- Sharing context is important, but can slow down sharing
 - Attribution is key example here: “Everyone wants attribution, but attribution is hard and that’s why everyone wants it.”
 - “Context does help narrow down the data to review, which is important when there is so much data shared”
 - However... context that is shared is often not used in automated processes

Addressing the gaps: Building Trust and Collaboration

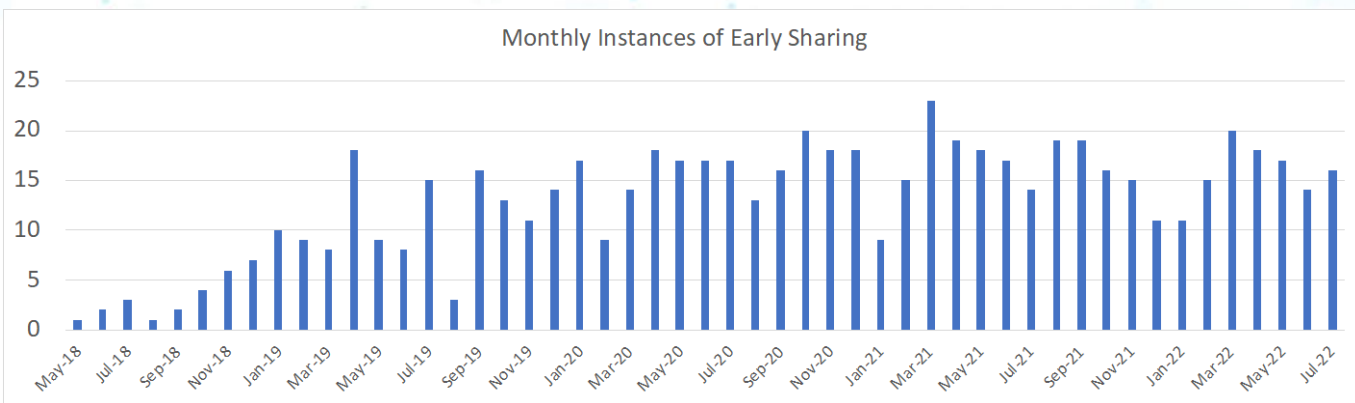


- How do we create an environment where more sensitive information can be shared? Look to Trust Groups
 - Pulsedive CTI Survey: “1-to-1 Direct Messages and Peer-to-Peer Trust Groups win out – by far – as the favored methods” of sharing CTI*
- Trust is a key requirement for sharing and (eventually) collaboration
 - With trust, people sometimes find ways around the blockers
- How do we build and foster trust?***
 - Competence trust – believing in the capability of others to do their jobs and act when the time is right
 - Interpersonal trust – believing that others will behave in ways you expect them to

*Grace Chi, Pulsedive; <https://blog.pulsedive.com/cti-networking-report/>

**Heidi K. Gardner, Harvard; <https://hbr.org/product/smart-collaboration-how-professionals-and-their-firms-succeed-by-breaking-down-silos/10001-HBK-ENG>

CTA's Model – Analytic Sharing and Collaboration




UNITED WE DISRUPT: VPN FILTER

Case Study: Not every cybersecurity provider has the same visibility into a threat. The only way we can expand our knowledge base is to share with one another and then act together to protect our customers.

 Cisco shared malware samples and analytic findings with CTA members

 CTA members used this information to develop protections

 CTA members published their own findings and analysis, amplifying Cisco's messaging

CTA Working Groups

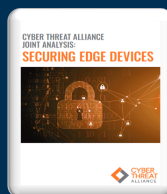
Election
Cybersecurity
Working Group



Olympic
Cybersecurity
Working Group

These working groups:

- Share information and shape future collection and sharing based on member needs.
- Work with the system owners / operators and experts to create partnerships in advance.
- Plan for any incidents and disruptions that may occur.



- Foster an environment that builds trust between CTA members
- Provide opportunities to display competence trust and build interpersonal trust
 - Ask questions, provide feedback, identify common interests
 - What you think is unimportant might be key information to someone else
 - Not everyone knows what you think they know
- Goal: Move from information sharing to operational collaboration
 - Information sharing → Operational planning → Synchronized action

Conclusions

- Why has information sharing failed to live up to its promises?
 - Unreasonable expectations that information sharing alone will solve our problems
 - Must supplement automation with trust and collaboration, which is difficult to scale
 - Information sharing is not an end in-and-of itself
 - Operational collaboration is the true goal
- Organizations must address the various blockers that can hinder sharing
 - Technologies, frameworks, legal, policies, resources, time, attention, culture, and trust
- CTA, ISACs, and governments must learn to thread the needle, working at scale and building trust