The Definitive Guide to Sharing Threat Intelligence

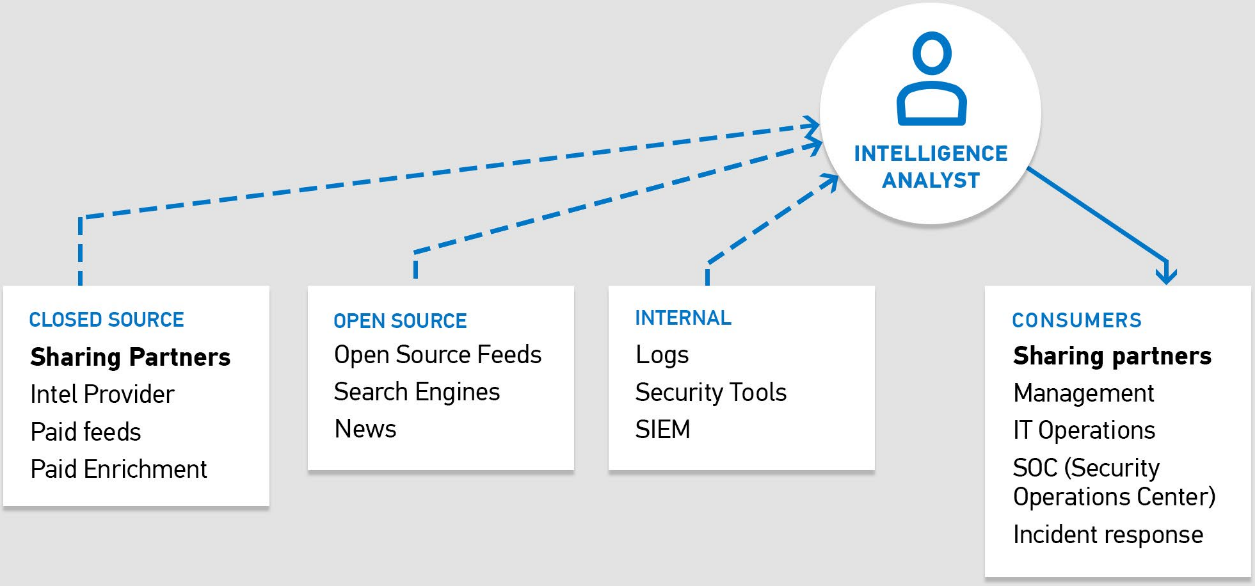
Threat intelligence is becoming a more ubiquitous feature in information security programs. Whether organizations have a full threat intelligence team, ingest threat feeds, or simply leverage threat intelligence features found in common security tools, they are now benefiting from threat intelligence in one way or another. The 2016 Ponemon Study, [The Value of Threat Intelligence](), indicates that 78% of organizations consider threat intelligence critical to achieving a strong security posture.

Commensurate with the increase in the use of threat intelligence has been an increase in sharing threat intelligence between organizations. Industry-centric sharing initiatives like Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), and other industry sharing organizations have led to a dramatic increase in the sharing of threat intelligence. Additionally, government-led initiatives from the Department of Homeland Security (DHS), like the Automated Indicator Sharing (AIS) program and the Cyber Information Sharing and Collaboration Program (CISCP), and the United Kingdom's Cyber-security Information Sharing Partnership (CiSP), have all encouraged sharing partnerships between governments and private organizations.

Despite the relative popularity of these sharing initiatives, member organizations are still mostly focused on consuming what is shared instead of adding their own contributions. There are a number of reasons for this. Not all organizations have the resources to stand up full-blown threat intelligence practices capable of producing their own intelligence. While this is not a requirement for sharing indicators or other types of intelligence, it is still a primary reason that organizations feel they have nothing of value to contribute.

Privacy concerns are another major barrier to organizations contributing to threat intelligence sharing initiatives. It's not a hard sell to consume shared data from other organizations, but there are still fears around sharing internal threat data that might be considered sensitive. These concerns are valid but not insurmountable hurdles to getting more organizations involved in sharing.

There are many quite significant benefits to sharing — perhaps some that haven't yet been realized. Included here are several points for consideration in regards to sharing threat intelligence.



Unidirectional vs. bidirectional sharing

Sharing threat intelligence comes in many flavors. The more common version is *unidirectional threat intelligence sharing,* where one entity produces and shares threat intelligence that others consume. Those consuming the intelligence do not contribute in return, often because a mechanism does not exist for "pushing" information back. Examples of unidirectional threat intelligence sharing include:

- Open-source intelligence, which might involve downloading a publicly available report covering a recent attack that contains indicators and methods used, or ingesting an open source intelligence feed.
- Closed-source reports and feeds

The other option for organizations is to engage in *bidirectional threat intelligence sharing*. For most organizations, their initial experience with this kind of sharing likely came when joining their industry ISAC or government sharing program. In these situations intelligence isn't just sent down to be consumed but can also be ingested from member organizations. Although sharing is allowed and encouraged in these programs, there is no guarantee that every organization will share anything as previously noted. They are consumers but not sharers of threat intelligence.

Concerns around sharing intelligence

The desire to consume available threat intelligence is a no-brainer. Whether or not specific sources of threat intelligence *should* be consumed by a particular organization, or if it has the *ability* to properly utilize those sources, is a separate question outside the scope of this discussion. Hint: These questions should be answered by intelligence requirements, fidelity, availability of resources, and so on. See also: Anomali ThreatStream. Overall, the decision to consume some source of intelligence is generally not a hard sell if it is deemed to be required for generating actionable intelligence in an organization.

Asking an organization to actively share indicators or produced-intelligence is another question altogether. Even contributing additional details or context to intelligence shared from other organizations can be a tall order. Below is a list of common concerns preventing organizations from engaging in sharing threat intelligence:

1. Privacy & liability concerns

- Scrubbing data for private information or sensitive corporate information before sharing is a good idea regardless of the type of sharing involved. This is most problematic with automated sharing as the scrubbing must be done before the information is shared.
- The Cybersecurity Information Sharing Act of 2015 (CISA) has provisions to address common concerns around privacy and liability. Some of these protections are contingent on certain stipulations being met. As always, proper legal advice is highly recommended to understand

how CISA may apply to specific situations[1].

- The fact that so many organizations are engaging in sharing initiatives within their industry or with the government is proof that privacy and liability concerns can be overcome — either through more accurate perception of sharing intelligence, protective clauses in legal agreements, recent legislation, or care in what is being shared. Regardless of the underlying reason, it is a promising trend for the future of shared intelligence.

2. "There is nothing of value to contribute."

Organizations with smaller information security teams and smaller budgets may feel like they don't have anything to contribute that isn't already being covered by larger organizations or those with bigger budgets. This shouldn't preclude them from stepping in where possible. There are often at least some additional details that can be added to the intelligence already shared. For example, no organization sees every possible attack or all possible variants of a particular wave of phishing emails. There are always be opportunities for organizations to get involved and share something, regardless how insignificant it may seem. These details can aid in visibility and help produce more fully sourced intelligence analysis.

3. Lack of expertise

Not having trained intelligence analysts on staff can be a hindrance to contributing to shared intelligence. While it is true that lack of trained analysts is an issue, it shouldn't curtail the notion of sharing altogether. By simply adding whatever context, observed attack details, and if possible, analysis developed by those on staff, value can still be added to the community.

4. Fear of revealing an organization has been hacked

The fear of sharing breach details more broadly than with the entities absolutely necessary is common. What if the analysis details of some interesting traffic shared in the morning turned out to be evidence of a month-long breach discovered after further analysis? Going even further, the idea of *deliberately* sharing breach details quickly with sharing partners is probably a foreign concept in most organizations. This topic is addressed more fully later in the document in the section titled, "Where to start or expand intelligence sharing" under item number six.

Sharing intelligence outside of industry verticals

Connecting to other verticals

Industry verticals are naturally a great place for organizations to share threat intelligence. The shared business understanding, (sometimes) similar cultures, and industry-specific attack surface create the perfect environment for sharing intelligence. ISACs, ISAOs, and other industry-specific information sharing organizations provide the legal frameworks to facilitate sharing intelligence among member organizations. These are probably the most likely places that active intelligence sharing occurs for most organizations.

We shouldn't stop at joining our friendly neighborhood ISAC, however. Gaining insights from organizations outside our industry echo chamber can be an important element of visibility. There are other variables to consider as well.

Industries develop muscle memory around specific threats that are commonly seen, and attacks from certain actors or groups become easily recognizable. What happens when one of these groups or actors suddenly moves into a new industry, though? Chances are that little may be known about them in that new industry. Some information can be carried forward through third party threat intelligence services but likely not the full breadth of knowledge that the previous industry has built around that actor or group (this touches on the need for sharing with vendors but we'll table that discussion until later in the document). The result is that the new industry is caught with little knowledge of the adversary and insufficient means of protecting themselves.

Here is a theoretical example that hopefully clarifies

[1] For more information on CISA: corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

this point. In 2015, it became public that giant healthcare provider, Anthem, had been breached and a massive amount of patient data was suspected to have been stolen[2]. It was later surmised that a group known as Deep Panda (using Crowdstrike's vernacular) was likely behind the attack. Supposing this attribution was accurate, and supposing other attacks associated with this group were also accurate, it's likely that Anthem had no reason to believe that this group would target them. Prior to the attack, public reporting about this group noted that they had been involved in several sectors such as defense, financial institutions, and government agencies — nothing relating to healthcare[3]. Had entities within the defense and healthcare industries shared intelligence, there might have been some transfer of knowledge about these actors that could have bolstered Anthem's defenses, potentially leading to an earlier detection or prevention of the breach.

This is obviously heavy speculation, as Anthem still would not have had any reason to assume this group was shifting to healthcare. Regardless, intelligence sharing between these industries certainly wouldn't have hurt. The benefits go both ways as actors and groups shift tools and tactics between and across industries.

Localized intelligence sharing

Finding partners local to your organization's physical location also has benefits. Not all attacks are remote in nature. Physical breaches, WiFi attacks, USB drive drops, and hybrid trespassing/information security attacks may indicate local actors with physical access to entities in the local area. Additionally, localized events such as weather, terrorist attacks, accidents, etc. would benefit from localized sharing of intelligence that is not dependant upon an industry vertical. In the United States, DHS Fusion Centers are a great place to start with localized, cross-industry sharing. Networking at local security events is a great place to find good intelligence sharing partners as well.

Sharing intelligence with smaller organizations

Sharing with smaller organizations can also be beneficial because they see tactics that bigger organizations may not. They can represent low-hanging fruit to attackers because they often don't have the budget for the comprehensive security tools and security staff that larger organizations have. Sharing with smaller organizations has benefits that can go both ways — smaller firms can benefit from the deeper expertise of the larger ones and larger organizations benefit from the broader visibility smaller firms can provide into current threat tactics. This encourages both organizations to impart knowledge of intelligence practices and other important skills. Resources in these smaller organizations will hopefully become regular contributors to intelligence sharing and become just as valuable as resources from larger organizations.

Targeted or not

Sharing intelligence about specific campaigns or attacks can bring additional context back in return. Knowing whether or not other organizations were affected by a specific campaign is enough to indicate that it wasn't targeted only to your organization. Granted there are often a variety of ways to gain visibility into whether or not an attack was targeted only to your organization, such as a quick check on VirusTotal. But what about those times when there are no signs of the attack across those resources, how can you tell for sure? Broadly sharing intelligence with numerous partners can help add some visibility to this question. Such sharing is beneficial because it provides additional context about attacks from organizations that actually experienced it. Knowing the attack was aimed specifically at your industry or perhaps aimed at businesses sponsoring a specific event is valuable information.

But what if it was targeted only to my organization, and and I've just informed the other organizations of the details? They could accidentally share that information with an antivirus vendor and discern that you are tracking the attack when their malware is caught. This is a legitimate concern that highlights the need for all of us to be good sharing partners. We all need to be very cautious with information shared in confidence. Honoring the Traffic Light Protocol (TLP) or any other guidelines agreed to when we enter into sharing agreements with other organizations is paramount

[2] krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/

[3] www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks

to successful intelligence sharing. Holding others accountable in these agreements is also important to maintain a culture of integrity and help ensure proper stewardship of shared intelligence amongst all parties involved. Ultimately, the rewards still far outweigh the risks in sharing even sensitive information about attacks, campaigns, attackers, or other intelligence.

Diversified security and expertise

Organizations all have varied security tools and different expertise in their security programs. This is a bit of a common sense point to make that is generally understood without having to point it out. However, this fact has implications in the world of threat intelligence. The collective set of security tools, intelligence collection mechanisms, and available expertise an organization has represents its threat intelligence visibility. This gives the organization a unique point-of-view when it comes to knowledge gleaned about particular pieces of malware, campaigns, and depending on the maturity of their threat intelligence program, even of threat actors and the like. In a sharing collective, having access to organizations with different security tools and experts with different backgrounds can mean different insights applied to threat intelligence questions. This translates into broader collective knowledge when all these resources are brought to bear on a particular topic, campaign, or other intelligence question. Organizations going it alone don't get this expanded view into threats or other topics of interest. Of course, these benefits are also contingent on participation from the various organizations involved as well.

Sharing with... <gasp> vendors

Vendors engaged in collecting threat intelligence have several benefits to offer that can augment threat intelligence programs. They often employ human intelligence collection (HUMINT) as well as technical collection methods not performed by most organizations (crawlers, specialized honeypots, etc.). This results in broader visibility and enrichment to existing intelligence collection mechanisms inside organizations. These intelligence vendors often do not have much visibility into what is actually seen inside organizations unless they happen to have a part of their business that deals with incident response. Post breach forensic details provide a rich connector to externally collected intelligence with what is seen inside an organization after a breach. Intelligence created on a day-to-day basis from inside organizations is often not something intelligence vendors have access to. The result is that organizations themselves have to be the connector between externally gathered intelligence and what they collect from their own networks. This works — but further value might be gained if certain intel were shared back to these vendors so their analysts could correlate what they know with observed intelligence from inside organizations.

This is usually a contentious suggestion. Generally speaking, organizations aren't keen on letting third party vendors have access to internally generated intelligence. Especially if those vendors are viewed as "turning a profit" on freely divulged information.

These concerns aren't off-base but when I was at my previous job, I had a different perspective on this matter. I realized that there was a problem with visibility on both sides of the equation. Working inside a corporate security program, I didn't have the resources to staff up and start doing human intelligence collection everywhere I had adversaries. I didn't have the resources to try and stand up all the technical collection apparatus I wanted to either. Paying for third-party intelligence was a way to fill-in these gaps. This helped in my opinion but I realized the intelligence providers didn't always have the data curated in a way that was contextualized specifically to my environment. Outside of looking for intelligence relevant to my industry or my company's name, how would they even know what I was seeing on a daily basis to give me relevant intelligence on that level? It was up to me or my analysts to sift through what they had available and find connections to stuff we observed or had interest in. Even then, sometimes it was difficult to find substantially useful intelligence to what we were seeing. Sometimes it was and sometimes it wasn't. Requests for Information (RFIs) certainly help fill this gap but I didn't want to rely on these on a daily basis.

There had to be a more efficient way to collaborate with them. If they could see what we were seeing internally, in theory they could direct their collection efforts more accurately to my observed threats and augment my intelligence in a much more meaningful manner. Wishful thinking perhaps, but probably not outside the realm of reason.

In a previous role, I reached out to two of our vendors where I felt we had a strong enough relationship with to test this out. Interestingly, one was a traditional threat intelligence vendor and the other was in a slightly different space in information security. I trusted their researchers and the overall integrity of their leadership and I felt they would be able to turn our internally-generated intelligence into something useful back. I changed positions not long after these discussions so I was never able to see these efforts fulfilled. It's hard to say what would have happened. Despite that, I'm still a firm believer that some sharing back to vendors could be a very beneficial effort.

General thoughts on this:

1. **Careful selection of vendors to partner with in this manner**
   - What will I get back for sharing with them?
   - Who inside their organization will see the data? What are their roles?
   - What will they do with the data?
   - Do I trust them?
2. **Carefully scrub anything shared with them**
   - What is the minimum amount of information I can provide to see results?
   - No private info or sensitive company info
3. **Ensure a legal framework is in place to protect both sides**
   - Ensure the data is used as expected and not sold to other parties, etc.
   - Work with lawyers to make sure proper protections are in place
4. **Shouldn't be limited to just "threat intelligence" vendors**
   - Who does my organization have a relationship with that might benefit from this data and help better protect my org as a result?

Where to start or expand intelligence sharing

Whether your organization is already actively sharing intelligence or hasn't begun doing so yet, here are some tips on where to get started or ways to enhance sharing that is already happening:

1. Tools and communities

Begin with choosing appropriate tools to share threat intelligence. Email is the easiest place to start but focus on moving into more formal methods of sharing through available tools possibly leveraging standards such as STIX and TAXII. ISACs and other industry organizations are perfect communities to get started with intelligence sharing and normally have mechanisms in place for doing so. Ad hoc sharing with local entities or partners in other industries may start out less formal at first but work to leverage standard tools and sharing mechanisms with these as well. From a tools perspective Anomali STAXX is a free solution offered by Anomali that supports sharing indicators through STIX and TAXII. Anomali ThreatStream users already have a very robust solution to share indicators and other intelligence with other organizations or create their own sharing communities.

2. Share and contribute

Make sure to contribute to sharing once sharing partnerships are in place. Also contribute where your team can add additional context to intelligence shared from other parties. Sharing observed adversary behaviors, attacks seen, or details from incident response are great places to start. Don't worry if there isn't much in the way of analysis added to what is shared initially. Watch for sharing things that have already been shared. If the phishing attack you were about to share has already been shared by someone else, look through what they provided and see if there is additional context you or your team can add. Try to gauge the value of what is being shared in your community and tune what gets shared out accordingly. Don't forget about historical context. Being able to tie this morning's phishing barrage to a similar barrage 3 days or a week ago helps to identify a specific actor's activities. Being able to eventually identify several attack campaigns that seem to be associated with the same actor or group helps to build a profile of what that actor likes to do and how they like to do it. This process is much easier when looking at actor activities broadly across several organizations and tying them together along with historical details and other contextual enrichments.

3. Share outside your vertical

Look for opportunities to share with organizations outside of your vertical. This includes localized entities such as Fusion Centers as well as other organizations deemed to be a good fit for sharing intelligence. The idea of sharing with outside entities is becoming more accepted in organizations thanks to ISACs, legislation, and government initiatives around this subject. Leveraging this acceptance to build trust and sharing relationships with entities outside of the industry vertical and government should garner some success. As always, working closely with legal teams/lawyers to draw up appropriate agreements to facilitate sharing between the entities is really a requirement.

4. Consider sharing with vendors

This suggestion probably isn't for everybody, but if the section on sharing with vendors resonated with you, consider some potential vendors who might be beneficial to share intelligence with and reach out to them. Chances are they will not necessarily have a mechanism in place to ingest intelligence from your organization but see what makes sense to start with if a sharing agreement can be reached.

5. Share hunting & defense techniques

While the focus of this document has centered around sharing intelligence, consider other items to share as well. Threat hunting details such as searches that have proved valuable, specific log entries that are useful, and other related details can turn into shortcuts in other organizations' hunting efforts. Hopefully they return the favor and it becomes a force multiplier in threat hunting. Also, sharing any successful defense techniques or rules such as YARA rules, snort signatures, Bro rules, scripts, and anything else that can easily be replicated between organizations. The more we share with each other, the harder it will become for the bad guys.

6. Share breach details

Breaches can be sticky subjects inside organizations. The usual reaction to a full-blown information security breach is to engage the authorities, employ a third-party incident response organization to help clean things up, notify whoever is required to notify, and release as little detail outside of those efforts as possible. While this strategy works in some ways, it falls short of what is truly possible in providing a better response. Depending on the legal framework in place that facilitates intelligence sharing, ample protections around disclosure could already exist to ensure protection for sharing breach details with sharing partners (consult legal advice pertinent to your specific agreements to be sure). What this brings is a variety of potential benefits for all parties involved. Pushing out breach details quickly could mean the difference in someone else being breached and being able to stop it quickly. Also, it could bring lots of assistance in terms of additional intelligence and quicker answers to incident response challenges thanks to the additional resources from other organizations adding their skills and expertise to the event. The other organizations are going to find out about the event one way or another, why not leverage their help while it's still going on?

Conclusion

Sharing threat intelligence is gradually becoming an accepted component in information security defense. There are still a number of ways we can gain more through sharing threat intelligence, however. By engaging more actively and more broadly in sharing, we pass information more quickly; we can make better judgements; and we can deliver more insightful analysis to stakeholders and intelligence consumers. Changes to malware, infrastructure, new tools, new techniques, actor behaviors, campaigns, and other intelligence-related details can all become quickly known across a multitude of organizations. Ultimately, the bad guys may be trying to compromise single organizations but are battling a collective in the process.

Travis Farral, Director of Security Strategy at Anomali
travis@anomali.com