SANS

Analyst Program

Survey

SANS 2022 Cyber Threat Intelligence Survey

Written by **Rebekah Brown** and **Pasquale Stirparo**

February 2022

THREATQUOTIENT

Executive Summary

Two major cybersecurity events that showcased the role of cyber threat intelligence (CTI) in network security operations bookended this year's survey. The SolarWinds software supply chain attack[1] broke as we finished up the 2021 survey, and the Log4j vulnerability response process[2] was in full swing as we worked to wrap up the 2022 survey. Both events highlighted the need to rapidly gain situational awareness, contextualize vast amounts of shared information, and prioritize remediation of significant threats. The 2022 SANS CTI survey shows that many CTI programs can meet the challenge. While some programs are just getting started due to increased cybersecurity needs and a growing, complex threat environment brought on by the rapid shift to remote work, organizations can rely on CTI providers and information-sharing groups to fill in gaps as their programs mature.

Key takeaways:

- More organizations are beginning to develop their CTI capabilities, with an increasing number of respondents reporting that they are early on their CTI journey and still developing processes and going through the same growing pains that many robust CTI programs previously faced.
- Several promising trends from past years, such as collaboration between CTI teams and business operations groups, have been in decline since the shift to remote work in response to the COVID-19 pandemic. It takes effort to build bridges, and organizations may find coordination that was already not as intuitive or ingrained when organizations were primarily in person even more difficult now.
- Quite an important percentage of respondents, 21%, said that they could not measure whether their CTI program was indeed useful and valuable to their organizations. This result highlights the need for more and better ways to measure the effectiveness of CTI programs, the tools, and the sources, a call to action for both practitioners and vendors alike to find better and easier ways to measure CTI success.
- Threat intelligence platforms are still not the main tool used by CTI teams—not in the top four—with "spreadsheets/emails" leading the way once again, while one out of two respondents still prefers homegrown CTI platforms. Reasons behind this may differ, but vendors can certainly improve analysts' experiences by continuing to understand use cases and share more of the requirements between practitioners and vendors. However, the encouraging trend in response to this is the small increase in commercial and open source CTI management platforms with regard to automation/integration.

[1] "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack," www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

[2] "Apache Log4j Vulnerability Guidance," www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

This year we had representatives from more than 200 organizations participate in our Cyber Threat Intelligence Survey. These organizations spanned multiple sectors and were of various sizes, but we did see some interesting trends in responses this year. First, we saw a significant increase in respondents in the education sector, who made up 10% of respondents this year as opposed to 3% last year, likely due to more educational institutions working online. As with previous years, respondents came from organizations comprising fewer than 10,000 people. Last year's survey highlighted some of the impacts of the shift to remote working and schooling and the increased need for cybersecurity and threat intelligence staff at organizations that may not traditionally have had a dedicated staff. As many organizations, including many in the education sector, continue to have a remote or hybrid presence, hopefully their staff will continue to grow, and we will see reflections of the field expanding reflected in future surveys. Figure 1 provides a snapshot of the demographics for the respondents to the 2022 survey.

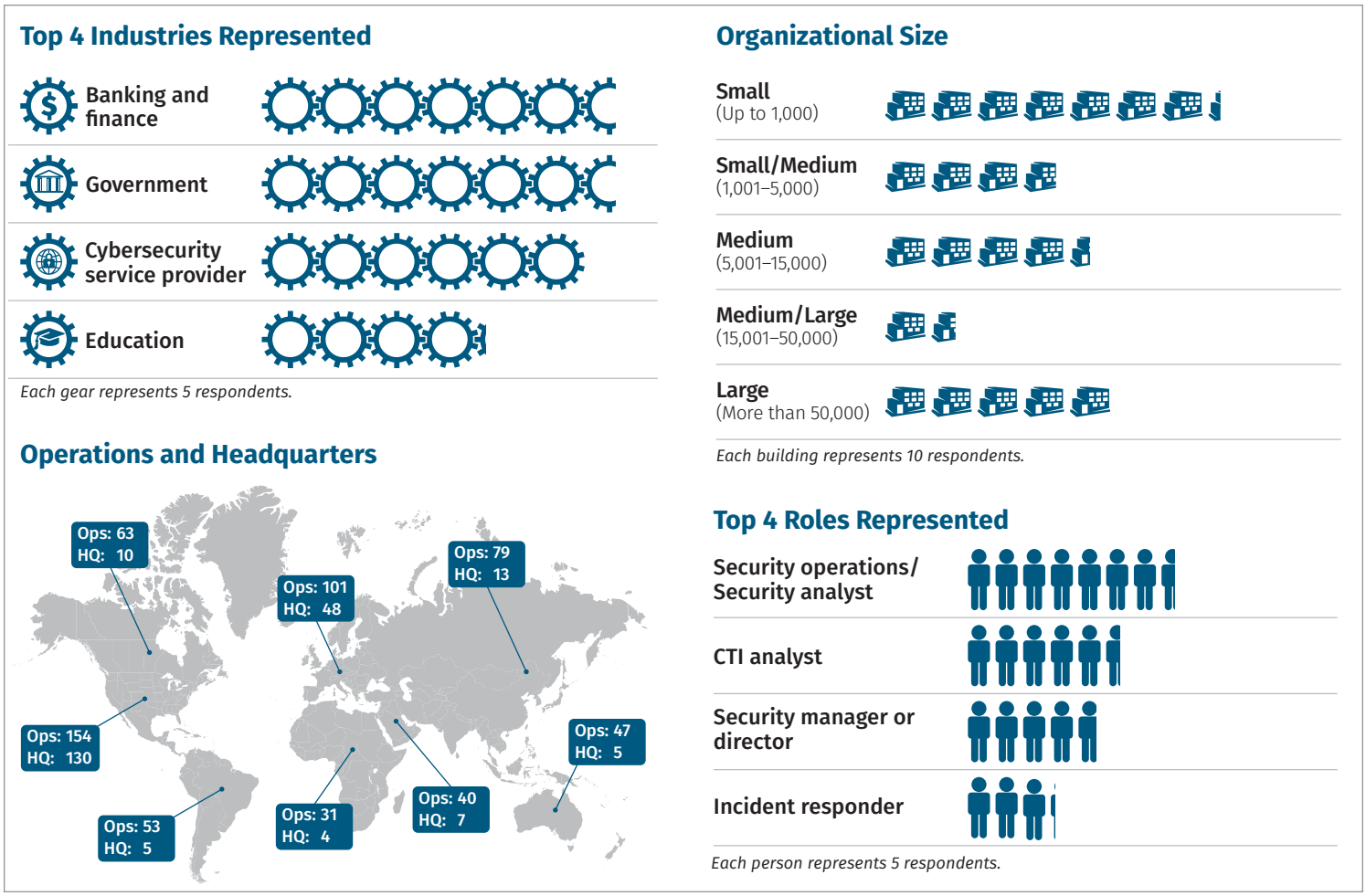

Figure 1. Demographics of Survey Respondents

CTI People and Processes

CTI is analyzed information about the intent, capabilities, and opportunities leveraged by adversaries targeting computer networks. CTI can be generated by an organization that analyzes its own data about previous data breaches or network intrusions. Organizations can also consume it based on external sources such as threat intelligence vendors or information-sharing groups. Often organizations use a combination of the two types: harnessing the power of their internal data while relying on outside expertise to provide a more robust picture of the overall threat landscape. Regardless of where the information comes from, organizations need people and processes to integrate findings and insights into their cybersecurity programs. This year's survey shows an increase in collaboration between internal threat intelligence teams and CTI vendors, with more organizations both analyzing their own threat data and utilizing external support for CTI programs.

It Takes Teamwork to Make the Dream Work

In its early days, many believed that only large organizations with existing robust cybersecurity teams in place utilized CTI. Since 2019, we have seen that more and more organizations are leveraging threat intelligence capabilities, whether or not they have a dedicated team devoted to CTI. This year, 33% of respondents work for organizations with fewer than 1,000 employees. While respondents reported a consistent trend in the presence of purely in-house capabilities, which holds steady at 36% year over year, there was an increase in reports of service-provider support for threat intelligence teams, which is the highest it has been since 2017. From 2021 to 2022, service provider support increased 5%. Although this increase indicates that many organizations are building out more robust capabilities in response to an increased online presence, it is important to note that those capabilities are not mutually exclusive. Many organizations with a CTI team on staff or with the task of CTI spread out across other teams also work with external teams for support for everything from strategic threat modeling to tactical threat detection. In fact, more than half (51%) of respondents reported that their organization uses a hybrid model with both in-house capabilities and external support. See Figure 2.

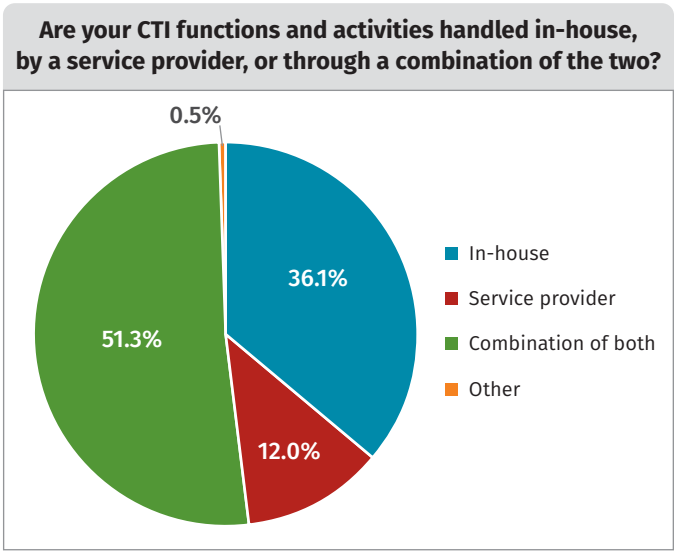

Figure 2. In-House Versus Service Provider

Team Structure and Organization

When it comes to in-house teams, organizations with formal dedicated threat intelligence teams continue to grow; it is up to 47% this year, after a brief drop in 2021 (see Figure 3).

However, organizations reporting that they have no formal CTI team and no plans to create one also increased this year—the percentage actually aligns with the increase in service provider support mentioned earlier. This indicates that organizations continue to see the value of CTI but are comfortable outsourcing it. Although we have not seen this trend in the past few years, it speaks to the evolution and accessibility of managed threat intelligence providers and their ability to support organizations of different sizes and maturity levels.

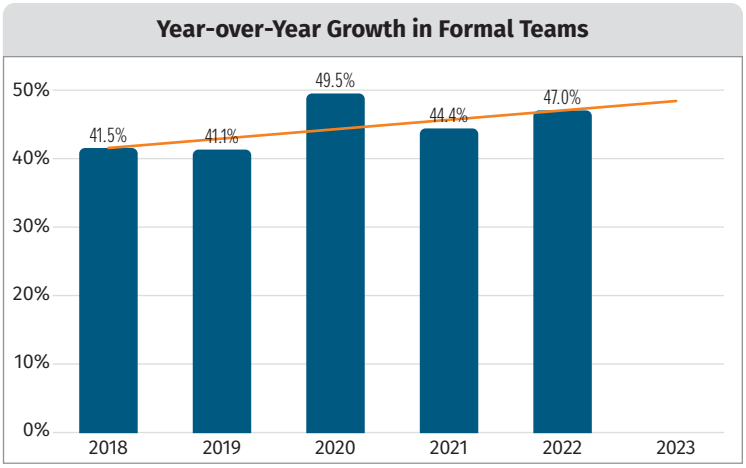

Figure 3. Organizational CTI Resources

In past years, survey respondents reported that the majority of analysts on a CTI team or handling CTI functions came from a security operations center (SOC) role. This year we see that number drop to 47%, with the difference spread across the other teams, with 1%–2% in each of the other areas (aside from business groups, which decreased). Responses to the question also indicate that organizations are hiring more analysts directly into CTI roles instead of pulling them from elsewhere on the security team, emphasizing the professionalization of the field. Several respondents also reported that they brought CTI analysts in from cybercrime and fraud teams, highlighting how a team with diverse experience across the threat landscape can help an organization respond to a wide variety of threats.

CTI Threats in 2022

In this year's survey, we heard a great deal about the types of threats that keep CTI analysts and their leadership up at night. While all organizations will have slightly different threat models and priorities, we picked up on some trends in the industry.

Email-Based Threats

Email remains a significant entry point for adversaries into a network. Several respondents reported that many of their CTI processes focus on email-based threats. Some proactively work using filters to block malicious emails, and some focus on raising awareness of employees regarding phishing campaigns. Examples from our respondents include:

> ***We have shared new variants of malicious email attachments and novel phishing email techniques in a security forum. —Survey Respondent***

> ***Constant monitoring of email and malware threats that are seen globally. Using that information to add additional protection to systems. —Survey Respondent***

Ransomware Threats

Ransomware is high on everyone's list of concerns this year, with actors targeting organizations large and small. Another concern is the interconnected nature of networks with contractors, vendors, and other dependencies that could adversely impact an organization even if it is not directly compromised. Because email introduces many ransomware threats, many of the tactics mentioned above are directly aimed at preventing ransomware from entering a system. Other ways CTI works to mitigate this threat include:

> ***Identifying third party vendors impacted by ransomware and taking action to mitigate their access to our data and infrastructure. —Survey Respondent***

Threats to Reputation or Brand

You know you have made it in this field when public relations wants to talk to the CTI team. With both ransomware and misinformation on the rise, organizations have a lot to lose with even the perception of a security breach that impacts customer data. In addition to intrusions targeting sensitive user or company data, organizations must prepare for attacks attempting to hijack the social media accounts of executives as well as the spread of misinformation about companies with the goal of damaging brand reputation.

> ***For media companies, we specifically monitor for external threat actors (action groups, hacker collectives, foreign governments) and their targeting of social media. —Survey Respondent***

CTI Processes: The Intelligence Process

For CTI teams to operate consistently among team members, it is important to have processes and frameworks in place as a scaffolding against which team members can perform analytic work. One of the foundational processes in CTI is the intelligence process, also known as the intelligence cycle. Both process and cycle are acceptable terms, although cycle often refers to a cyclical process, where when you move on to the next step you do not return to that step until the cycle has made a full rotation. In intelligence, you may move forward from one step to the next, or you may realize that you need to go backward to gain more clarity or get more information before you can proceed forward again.

For the first time, we have been able to capture insights from the 2022 CTI survey across all aspects of the intelligence process, including requirements, collection, data exploitation, analysis, and dissemination.

Defining CTI Requirements

The intelligence process starts with understanding the requirements for the CTI work that a team or individual is tasked with. Once organizations identify these requirements, analysts can focus on answering the key questions of decision makers and can optimize their remaining processes as much as possible. This year, fewer respondents reported that their organizations have formal requirements, and a there was a 5% increase in organizations without plans to develop requirements. See Table 1.

Although fewer organizations report having formalized requirements, the organizations that do have requirements are making it a priority to update them. Only 3% of respondents reported that their requirements have never been updated. Ad hoc is still the most frequent cadence for updating, with just over 40% having reported that they have no schedule or plan for updating requirements and that they are updated as needed. See Figure 4.

Although it can sometimes seem unimportant to plan a time to update requirements, having something scheduled—even just an annual review—helps keep the idea that requirements are not static top of mind.

Table 1. Intelligence Requirements Year over Year

	2019	2020	2021	2022
Yes, we have documented intelligence requirements.	30.3%	43.8%	39.0%	35.4%
No, our requirements are ad hoc.	37.0%	29.7%	36.1%	33.5%
No, but we plan to define them.	26.0%	20.4%	18.8%	20.1%
No, and we have no plans to formalize requirements.	6.7%	6.1%	6.1%	11.0%

How often does your organization review and update its CTI requirements? ***Select the best answer.***

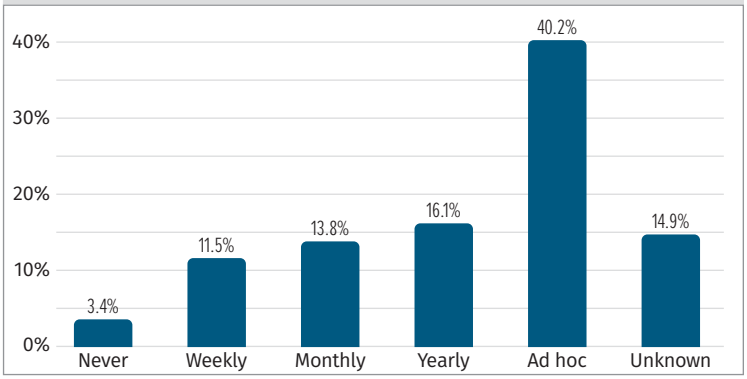

Figure 4. Reviewing and Updating CTI Requirements

In addition to having formal requirements that get updated periodically, it is also a best practice to include all CTI program stakeholders in the development of these requirements. This year, respondents reported that security operations is the team that contributes most to requirements, with 75% of respondents reporting their participation. The examples of CTI uses and analysis, covered later in this report, indicate that many organizations are directly engaged in support to security operations, and that even though they may not have formal requirements, they are working directly to support their stakeholders, which represents a great step in the right direction.

CTI Collection

Once a team has requirements it wants to address, the next step requires that they start collecting the information needed. This year, more CTI teams are leveraging external reporting sources such as media reports and news (up to 82% from 77% in 2021). With the number of major intrusions and adversary activity breaking in the news, CTI teams cannot ignore this type of reporting. See Figure 5.

What type of information do you consider to be part of your intelligence gathering? ***Select all that apply.***

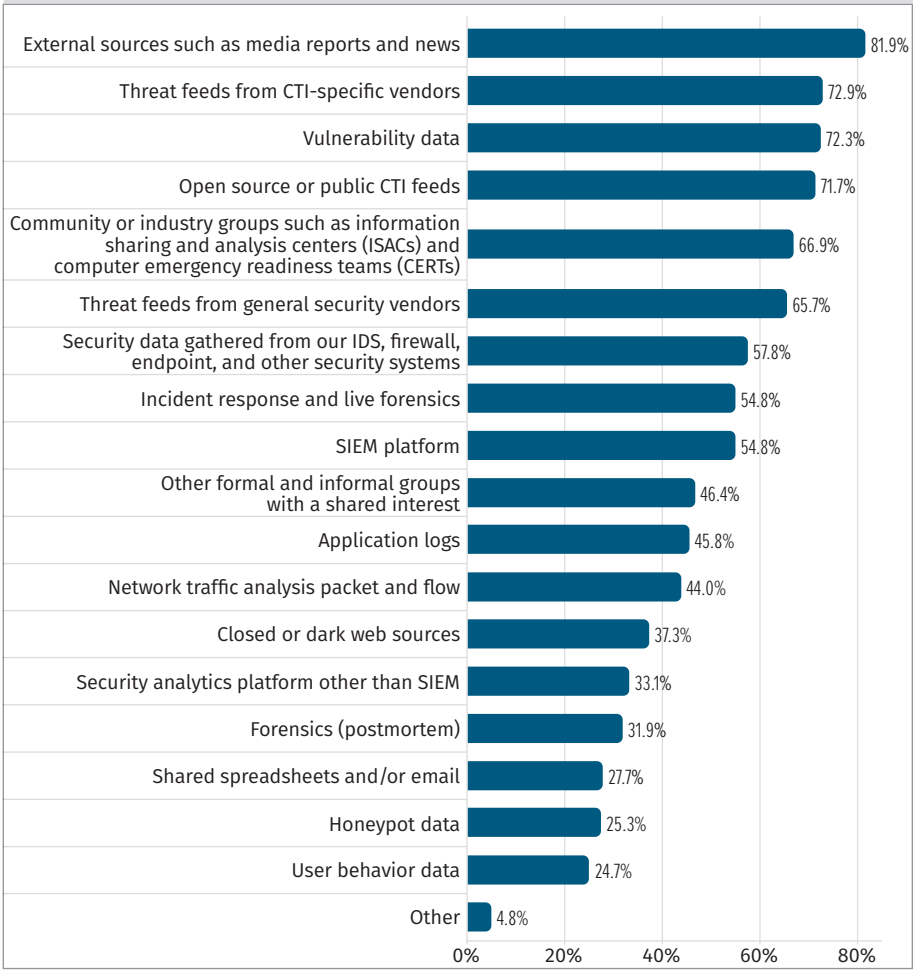

Figure 5. Sources of Intelligence Gathering

Community feeds decreased, but information from respondents' own networks (such as IDS logs and application logs) increased.

CTI Analysis

We are so excited that we could add questions about CTI analysis into this year's survey. Analysis is complicated and an often individualized process and can be difficult to capture in a survey question, but through a combination of multiple choice and write-in responses we put together a good view of how organizations conduct CTI analysis.

Coordinating with Incident Responders

This year's survey responses indicate a brief shift away from incident response (IR) and CTI collaboration. IR teams contributed less to requirements than last year, and forensics contributes less to data collection. While it is difficult to pinpoint the exact reason behind this shift, the data from this survey points at two contributors. First, many respondents this year are newer CTI organizations who are just developing their capabilities. CTI and IR coordination is a critical part of an overall cybersecurity program, but it takes some time to build both the processes and trust that facilitate robust collaboration. If you are a new CTI program just getting started, make sure to make connections with your IR team, whether in-house or external, to establish connections. You will find it much easier to establish communications before a large-scale incident hits.

The second contributor to this is likely the fact that the past year has been incredibly difficult for IR teams and CTI teams as well. We had fewer respondents this year than in past years, likely due to heavy workloads and higher-than-is-healthy levels of burnout in the field. Last year's survey touched a bit on the mental health impact of remote work and isolation, and those impacts have likely been increasing with the number and severity of significant security incidents across the profession. IR teams: Take care of yourselves and each other, and we hope to see you back in next year's survey.

The most frequently used analytic method was intuitive or experience-based judgment. In fact, only 16% said that they never leverage this method (see Figure 6). Conceptual models, such as the diamond model for intrusion and analysis (kill chain models are also frequently used), with several respondents specifically identifying the MITRE ATT&CK® framework as a model they have found significantly valuable.

Organizations use structured analytic techniques (SATs), a mainstay of traditional intelligence analysis, the least, with 33% of respondents reporting that they never use them, and only 19% reporting that they frequently use them. Organizations do not commonly use SATs because, unlike conceptual models, very few CTI analysis tools or platforms have integrated these methods into their workflows. Instead, tools more commonly directly allow an analyst to categorize or tag data by kill chain phase or diamond model axis, whereas the few productized SATs are often standalone tools, such as tools made specifically for one of the more popular SATs: analysis of competing hypothesis (ACH). SATs prove valuable for addressing biases in analysis and removing occurrences such as group think and for analysis. Increased integration of some of these techniques into tools used for CTI may make it easier for CTI teams to leverage them.

What methods are leveraged in CTI analysis?
For each of the following methods, indicate if they are used frequently, used occasionally, or not used.

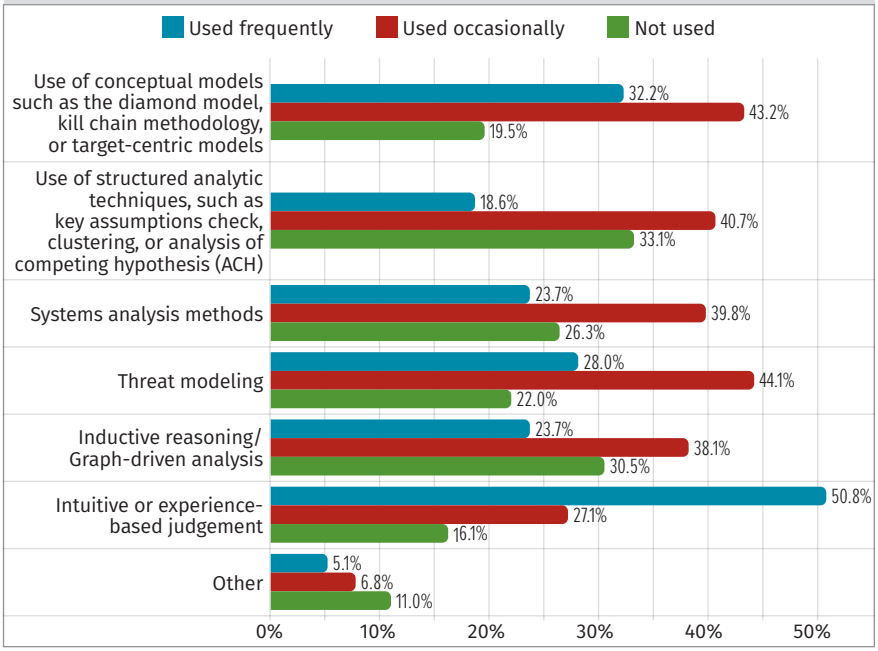

Figure 6. Leveraging Methods of CTI Analysis

CTI Dissemination

Once CTI has made it through the intelligence process all the way through analysis, the intelligence needs to get to the right audience in a timely manner. Intelligence dissemination varies depending on the type and urgency of the information. This year, respondents reported emailed documents as the most common way they disseminate CTI, followed by reports. Both of these indicate a narrative form of threat intelligence dissemination rather than just technical pieces of information such as IP addresses and domains. See Figure 7.

How is CTI information utilized or disseminated by your organization?
Select all that apply.

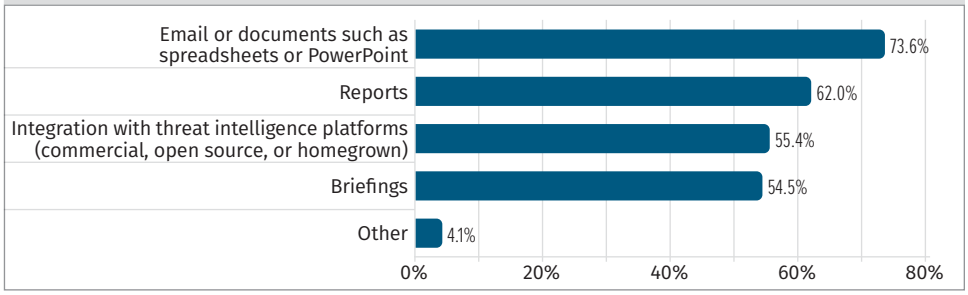

Figure 7. Utilization and Dissemination of CTI

A high demand still exists for this type of technical-level dissemination, with 55% of respondents indicating that they integrate directly with threat intelligence platforms to facilitate tasks such as threat hunting, email filtering, and malware detection.

As with many things in the CTI space, dissemination depends on several factors, including the situation itself. One respondent articulated this point very well, identifying that there are standard processes and then processes to escalate to a wider audience when needed:

> *Post-analysis intelligence is disseminated to team leads to further dissemination as required to their teams. In the event it is determined a wider audience is required, department heads are brought in. During large-scale events that have the potential to affect the organization as a whole, briefings are created for the C-staff and/or board. —Survey Respondent*

This year's survey showed a promising trend when it comes to people and processes: More organizations are beginning to implement threat intelligence capabilities in their organizations. Although those organizations are in the early stages of development, the field of CTI has come a long way since SANS first began surveying CTI professionals, and these organizations will have a wealth of information to help them on their way to successful programs.

Uses and Value of CTI

Threat intelligence has many different uses within an organization, from tactical to strategic, from supporting the risk-assessment team to helping prioritize patching. Also, depending on the maturity level of each organization, one can go from simply consuming intelligence to full production.

As expected, and as it normally should be, most organizations are consumers of intelligence. From our respondents, the types of intelligence consumed are mostly published threat intelligence (58%) and contextual threat alerts (50%), but a significant number also consume raw threat data (48%). We could expect this, because the number of organizations with a higher maturity level and with the need to produce intelligence should indeed be lower. See Figure 8.

Figure 8. Production Versus Consumption of CTI

What is interesting though, and a sign that CTI as a discipline is growing and maturing, is the number of organizations that both consume and produce intelligence, with answers between 33%–36% across the three types of intelligence proposed.

With regard to consumption, it is always interesting to see the variety of uses of CTI across organizations. Mitigation is one of the most frequent use cases, with several respondents crediting CTI with helping assess and prioritize patching when new vulnerabilities are announced (as well as detection and threat hunting based on published reports and IoCs). Finally, security awareness for staff, including training and ongoing situational awareness for the C-suite, is a very common use case. All these answers reinforce the notion of relevance and applicability of CTI to the specificity of an organization, as well as the need to be able, for those who do, to produce different types of threat intelligence products/outputs.

Value and Usefulness of CTI Types

One of the main reasons to have a threat intelligence program in a company is to improve the overall security posture of the company and to help other teams make better decisions (whether about responding to an incident or about assessing the risk exposure of the organization).

When asked whether CTI has improved the security prevention, detection, and response of their organization, 75% of respondents confirmed this was the case, and this result aligns with previous years as well. However, aside from this positive trend, 21% of respondents said that they do not know. This is an important result to note because it may highlight the need for more and better ways to measure the effectiveness of CTI programs, the tools, and the sources. Not being able to measure the value of something is what could eventually be the end of it, as teams won't be able to justify the need for more resources, new people, new tools, etc. This is a call to action for both practitioners and vendors alike, to find better and easier ways to measure success in CTI.

We have already said that CTI has multiple types and formats, and we wanted to understand what type of threat intelligence respondents find most useful now as well as what they might find helpful in the next 12 months.

According to our respondents, technical information about malware attackers use (81%) and information about current targeted vulnerabilities (80%) represent the two most useful types of CTI currently. This is consistent with 2021 results, except the two positions have switched. When considering the future, 52% of respondents think that more detailed and timely information about adversary groups in their industry and geography will prove most useful. Timeliness and relevance are indeed key to intelligence, and while respondents are asking for more of it, which is good, a positive sign is that the satisfaction with context (from 59% to 61%), analytics (from 52% to 55%), and relevance (from 66% to 67%) of CTI data has increased from last year. These represent small improvements but are a positive sign nevertheless. See Figure 9.

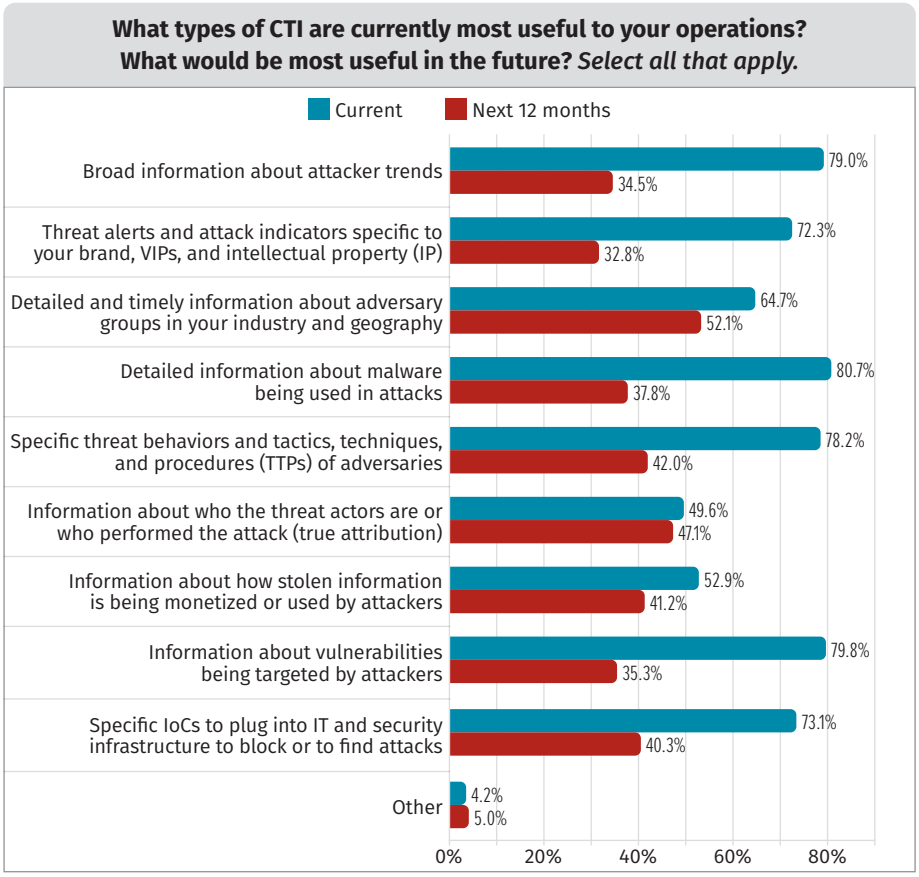

Figure 9. Most Useful CTI

Two things have slightly decreased in terms of satisfaction: strategic reporting and searching and reporting.

Finally, confirming the trend from the previous year, respondents were still mostly not satisfied with the removal of expired IOC, a common problem that can lead to numerous false positives.

CTI Tools

Analysts always find the tools topic contentious, with threat intelligence platforms (TIPs) representing both the instrument to accelerate and enhance the intelligence cycle as well as sometimes a source of pain and frustration for the analysts. The tools should support automation and scaling. After all, with the amount of data to correlate and analyze daily, it would be unthinkable not to have such features integrated. It is important to serve different type of customers (including internal ones, like SOC, IR teams, etc.) but also allow enough room for the analysis itself, the human aspect that cannot be taken out of the loop completely (no matter what).

First we asked what type of management tools our respondents use to aggregate, analyze, or present CTI information. Unsurprisingly, spreadsheets/emails held No. 1 place again, with 44% of respondents saying they use these forms manually/independently. However, if we look at what tools organizations use the most to support some level of automation/integration, SIEM (40%) and network traffic analysis tools (38%) are the favorite technologies. These results seem to remain consistent across the years.

We want to note a couple of interesting points about this specific topic. The first is that TIPs are not the main tool used by CTI teams yet; among the top four tools used, none is a CTI platform. The second striking result is that more than one in two CTI practitioners (56%) uses a homegrown CTI platform, which is a sign that should not be underestimated. Vendors can certainly improve the analyst's experience in this area by continuing to understand use cases and share more of the requirements between practitioners and vendors. In addition, CTI teams should really focus on what their core requirements are to confirm whether a custom homegrown CTI platform is really the answer.

However, consider this encouraging trend regarding the point above: Since 2021, the use of commercial and open source CTI management platforms with some automation/integration has grown from 35% and 30%, respectively, to 37% for both. This increase in adoption is a good sign that the development of such platforms is recognizing analyst needs and requirements more and more. Although much work remains to be done, the industry seems headed in the right direction.

What processing is done to CTI information to make it more usable?
Select all that apply and indicate if the process is manual, semi-automated, or fully automated.

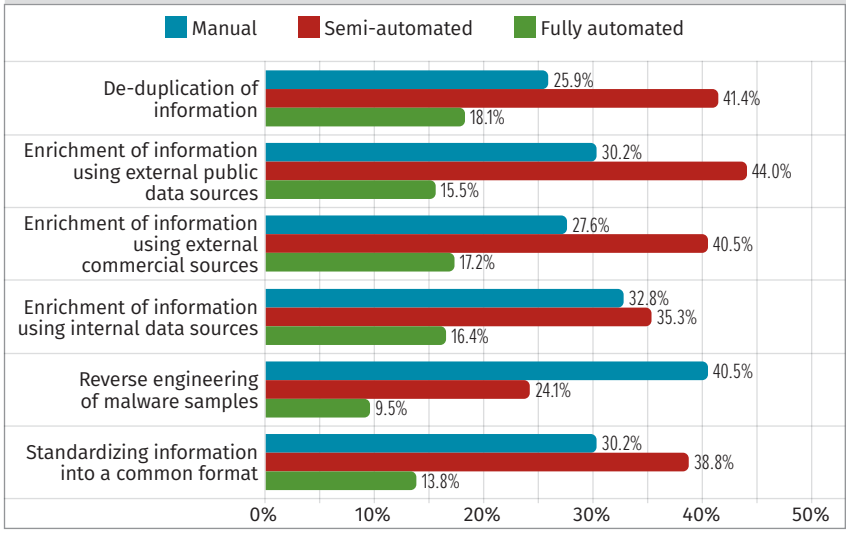

Figure 10. CTI Processing

With regard to processing of information—with the expected exception for reversing engineering of malware samples, for which the majority of respondents indicating manual processing (41%)—every other type of processing has a low percentage of responses towards full automation (15% on average across all responses). All other responses have been toward semi-automation, with manual processing still getting very high numbers (roughly 30% on average). See Figure 10.

Even though correlation does not imply causation, if we look at this data in light of the previous point, we can see that the need exists for more automation. So, CTI platforms that offer more automation may help their adoption rates, and increased automation may help CTI teams reduce the amount of manual and semi-manual processing (which is still high).

Finally, the importance of integrating the many different tools used—not only the tools used by the CTI teams themselves but also by the others like SOC, IR, vulnerability team, etc.—is paramount today. In this regard, the first result is that only 46% of respondents integrate their threat intelligence within their defense and response systems. This is not great, as we would all hope to see a much higher number, but the good news is that this represents a significant increase from the 41% of last year. Indeed, this positive trend reinforces all responses received about tools: We still have a long way to go, but the direction seems to be right.

Organizations integrate CTI information into defense and response systems most commonly via CTI platform (67% of respondents), followed by intelligence service providers (59%) and vendor APIs (45%). Again, this shows that vendors currently play an important role in making such integration happen.

Moving Forward

CTI *requires* both collaboration and communication. Although it appears that the shift to remote work, increased threats, and high workloads impacted some key components of collaboration over the past two years, organizations *can* address these factors by both processes and tools. Organizations should assess whether they have lost communication channels with key stakeholders and should identify ways to build up those channels again. In some cases, organizations may need additional tools to facilitate collaboration. Many CTI tools, such as TIPs, have built-in collaboration functionalities that teams can explore to see if they fit with existing processes and workflows—and don't be afraid to make new processes. Many CTI teams have gone through a lot of changes, and it is natural to adjust to what will work in current situations.

This year's survey dove into specifics of analysis, finding that many analysts leverage the analytic models and frameworks such as the diamond model and ATT&CK. Models and frameworks are easiest to use when directly integrated into the tools that analysts use every day. That's not to say that a diamond model markup on a whiteboard isn't a solid way to conduct analysis, but it is much easier to capture, share, and replicate findings when they are easily captured. If your organization is one of the 55% using a homegrown CTI platform, consider integrating the models you use most often, or the ones you would like the teams to begin to use more. Those building and maintaining commercial platforms should continue to identify models that customers find useful and provide resources for those (while remembering that analysis is rarely one-size-fits-all). Having more than one option for models will allow analysts to apply the right frameworks to the right situations. And while we're at it, let's integrate some structured analytic techniques as well!

Discussions about tooling are always a hot topic in InfoSec, and CTI is no exception. The discourse around TIPs has been going on for a while, as on one side practitioners develop new and better requirements, and on the other side vendors come up with new functionalities to meet them. As we saw from the survey, TIPs are still not in the top three tools used by CTI teams, and half of the respondents use some sort of homegrown CTI platform. Moreover, most of the processing is still done manually, with a low percentage being able to go full automation. Even though the use of automation and integration in commercial and open source CTI management platforms has increased, representing a positive trend with the development of such platforms, this is a strong signal that should not be underestimated. This is an area where CTI vendors can improve the experience of analysts by continuing to better understand their use cases and requirements and, mostly drastically, by increasing automation. Considering the number of different data formats and the increasing volume of such data the industry is dealing with, higher automation in processing and correlation is the way to go.

If you can't measure something, you can't improve it. One interesting takeaway came from asking our respondents if CTI has improved their security (prevention/detection/response). Even though in a descending trend, a high percentage of organizations still cannot measure the effectiveness of CTI programs, the tools, and the sources. Measuring the value of an intelligence program means that teams will be able to justify the need for more resources, new people, new tools, etc., ideally moving organizations, and in turn the industry, toward a higher maturity level. This represents a call to action for both practitioners and vendors alike to find better and easier ways to measure success in CTI.

Sponsor

SANS would like to thank this survey's sponsor: