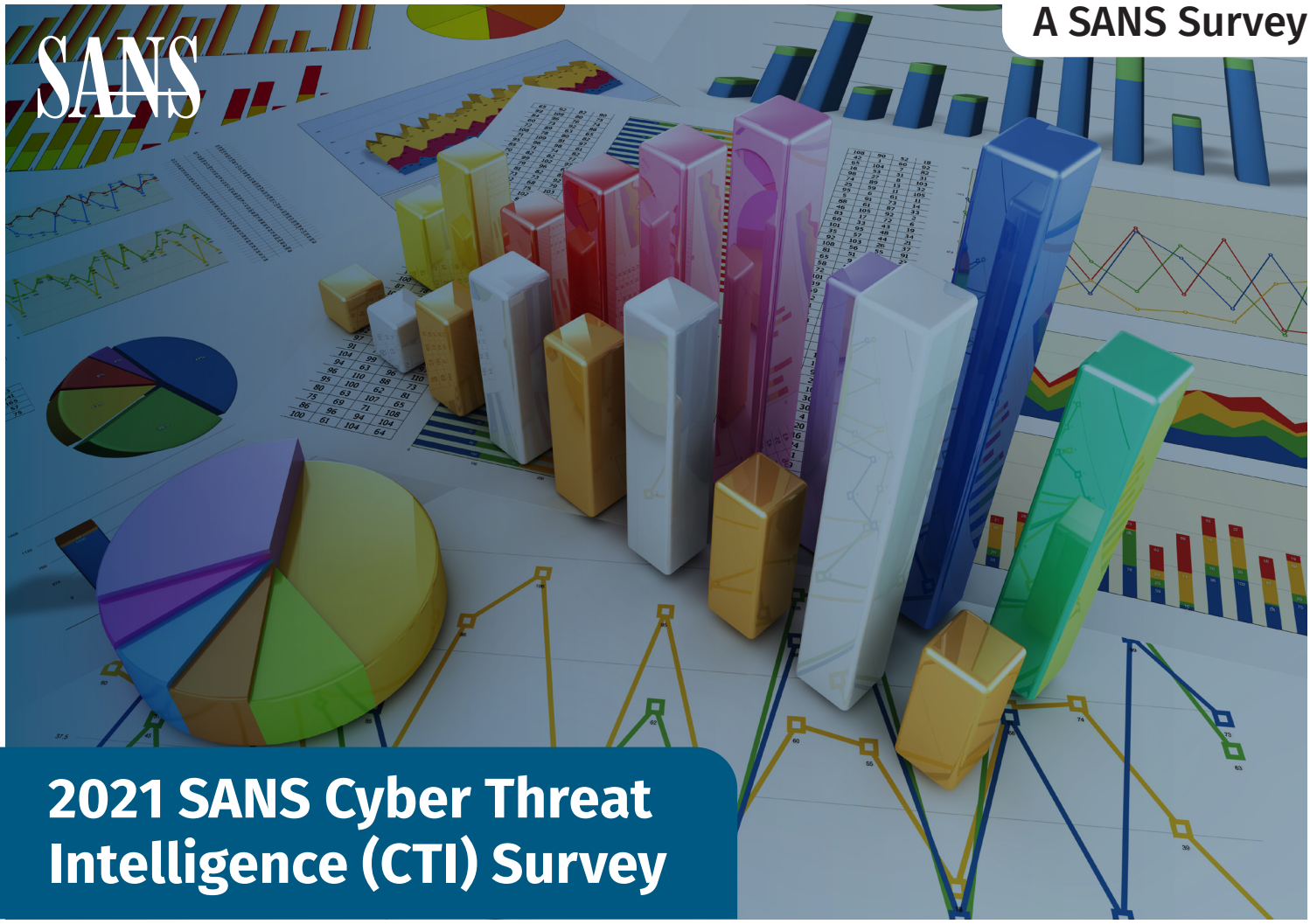
SANS | GIAC CERTIFICATIONS

WHITE PAPER

2021 SANS Cyber Threat Intelligence (CTI) Survey

Rebekah Brown and Robert M. Lee

A SANS Survey



2021 SANS Cyber Threat Intelligence (CTI) Survey

Written by **Rebekah Brown** and **Robert M. Lee**

January 2021

Sponsored by:

Anomali
Cisco Systems
DomainTools
Infoblox
Sixgill
ThreatQuotient

Executive Summary

The past year has been filled with changes to almost every aspect of daily life, and cyber threat intelligence (CTI) work did not go untouched. *CTI* is analyzed information about the capabilities, opportunities, and intent of adversaries conducting cyber operations. Adversaries tend to operate in and across digital networks and equipment that shape and impact businesses, critical infrastructure, and people's daily lives. Understanding how threat actors are targeting information, systems, people, and organizations helps organizations and individuals alike understand how to perform threat hunting and security operations, respond to incidents, design better systems, understand risk and impact, make strategic changes, and protect themselves from future harm.

While this year's survey captured some major ways in which CTI work has changed, we also noted more subtle changes across this year's responses with reversals of trends we had seen developing over the past several years. This year has also shown us how valuable time is, and we are appreciative of the practitioners who made the time to help us analyze the trends in CTI.

Even with the difficulties that 2020 brought, CTI work has continued to grow and mature. A record number of organizations reported that they have clearly communicated intelligence requirements as well as methods and processes in place to measure the effectiveness of CTI programs. These improvements continue to show the resilience of the field and the value of CTI as a resource for clarity and prioritization when complex challenges arise.

Key Takeaways

- The way CTI analysts operate has changed due in large part to the coronavirus. For example, analysts are more often disseminating information asynchronously through emails and dashboards rather than in-person briefings. Also, more analysts are back to working on their own as a sole CTI analyst, even as organizations depend more on their CTI functions for prioritization and protection of a suddenly remote workforce. And while many CTI analysts might be finding themselves working from home, they are not without tools to support them. Automation improvements in many areas of CTI collection and information processing have made parts of the increased workload more manageable.
- CTI is not just for the top 1% of organizations. This year we saw an increase in the number of small organizations that have CTI programs. While these organizations might start out with an individual analyst, or even one splitting time between other security functions, this growth shows that CTI has matured into a field where more and more organizations perceive that the benefits are worth the investment. The improved support that CTI provides for security at all levels, from tactical to strategic decision making, benefits organizations of all sizes and across all industries.

- CTI tools and processes are becoming more automated, giving analysts more time to spend on higher-level analytic activities rather than repetitive collection and processing tasks. This year we saw CTI analysts integrate more information from government security bulletins and media reporting into their analysis. This change shows a need for tools and processes that better support the inclusion of this data source to support analysis and help identify potential misinformation or disinformation that could negatively impact analysis.

Cybersecurity organizations are the top respondent industry again this year, after being overtaken by government and finance in 2020. The manufacturing sector went up this year as well. Figure 1 provides a snapshot of the demographics for the respondents to the 2021 survey.

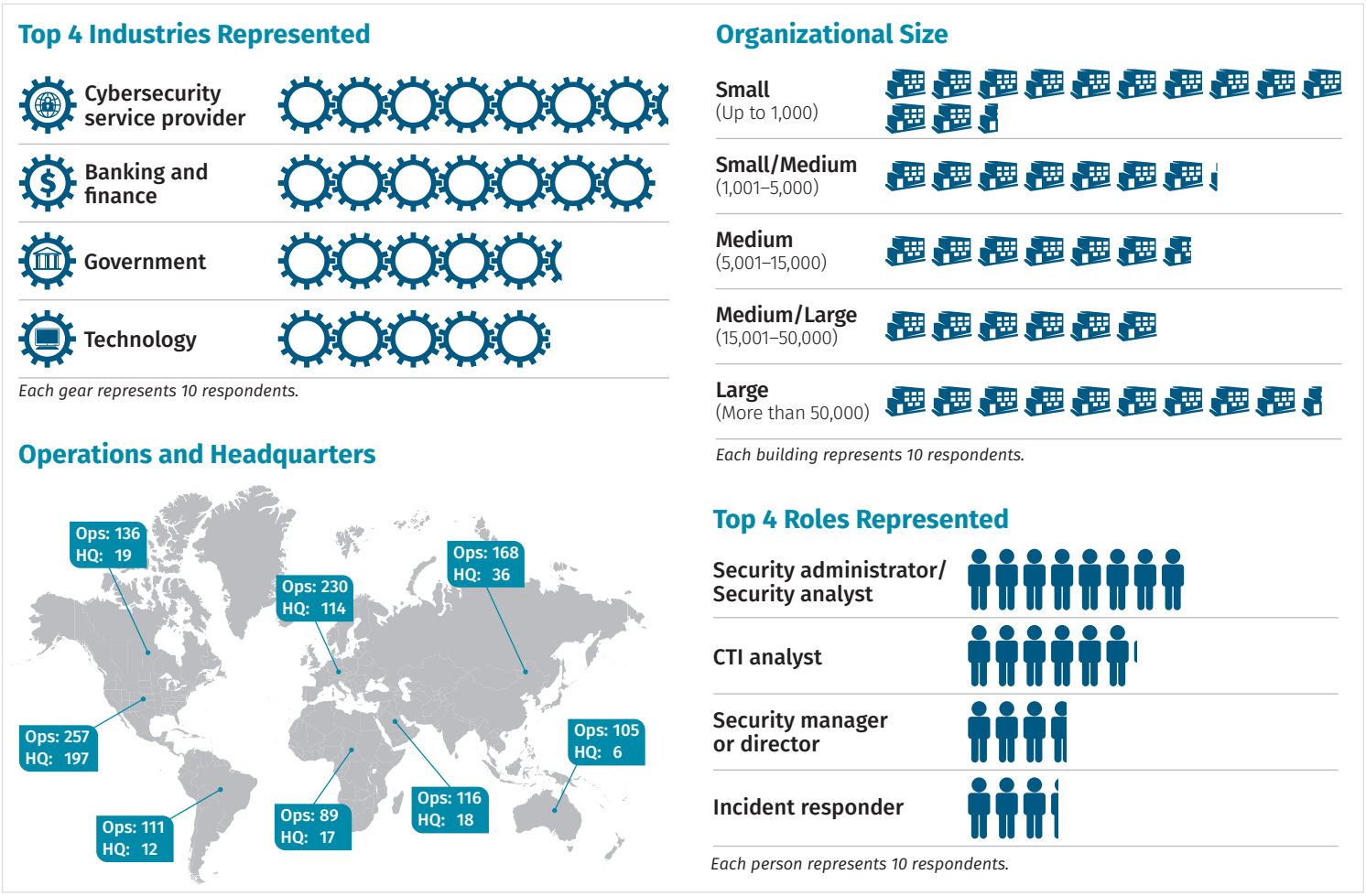


Figure 1. Survey Demographics

CTI Programs—People and Processes

An organization's CTI functions can focus on generating intelligence for others to use, consume intelligence produced by others for defensive purposes, or use a combination of intelligence production and consumption. All of these applications require a combination of people and processes that support these efforts, though the skill sets of the CTI analysts and the processes they leverage will vary based on the ways they leverage CTI. This year we saw a 7% increase in the number of respondents who reported that they produce or consume intelligence. This increase has been a consistent trend over the past several years (see Figure 2). In addition, this is the first time that the number of respondents without plans to consume or produce intelligence was 0%.

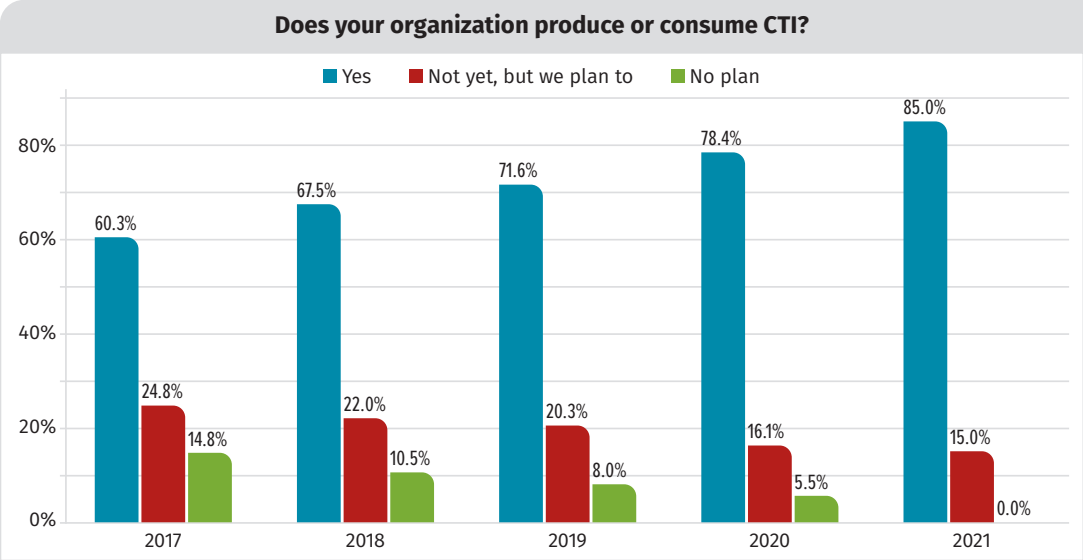


Figure 2. Trends in CTI Production and Consumption

CTI Teams

Whether an organization produces or consumes intelligence, it needs trained and capable CTI analysts. In an organization that primarily produces intelligence, analysis must drive the production process, including identifying consumer requirements, collecting relevant information, analyzing the data, and getting the findings into the right format for consumption. When an organization consumes intelligence, its analysts need to identify the right intelligence to consume—not a trivial task in the growing intelligence-production space. The analysts also need to identify how to make CTI relevant to their individual organization with its own requirements and then act on intelligence that is consumed.

The majority of CTI functions within organizations have typically focused on consumption or hybrid production/consumption activities. Because of this, historically respondents have reported that CTI teams primarily consisted of security operations center (SOC) analysts, incident response (IR) personnel, and threat intelligence analysts. Because teams' missions vary based on the particular focus of their organization, there are always specialized roles within some teams, showing the diversity in applications of CTI across organizations. This year, respondents reported specialties such as anti-fraud, threat management, cloud security, and development/integration.

Individual organizations can manage all of their CTI functions internally, or they can rely on external providers, either entirely or in a hybrid model. In the past five years, we have seen in-house-only teams slowly decrease in percentage, while hybrid-model teams have increased. This year, that trend shifted with in-house teams increasing 5% from 2020 to 37% and hybrid models decreasing 5% from 2020 to 56%. See Table 1.

Table 1. CTI Team Members Year over Year

	2021	2020	Trend
Combination of both	55.7%	60.9%	–5.2%
In-house	36.5%	31.2%	5.3%
Service provider	7.5%	7.3%	0.2%
Other	0.3%	0.5%	–0.2%

Teams with a single person dedicated to CTI as well as teams that "do not have someone assigned but plan to" both went up this year. The number of CTI functions supported by a single analyst (14% of respondents) is the highest it has been since 2017. This reversal of past trends is indicative of the way the pandemic shaped the workforce (see "The Impact of the Coronavirus on CTI Teams") and shows how CTI functions are continuing to grow in capabilities and maturity not only in larger companies, but also in smaller companies just starting to integrate CTI functions. Even with the difficulties this year brought, respondents who reported that they have no plan to assign anyone to CTI functions is down to only 4%. See Figure 3.

Figure 3. CTI Responsibilities

The Impact of the Coronavirus on CTI Teams

Roughly 20% of respondents indicated that their CTI implementation changed as a result of coronavirus. This difference is echoed across many of the sudden changes in trends that have been steady in past years, including the shift in smaller organizations responding, the increase in single analysts supporting CTI functions, and the decrease in budgets and ability to outsource support for CTI functions. Adversaries are also taking advantage of coronavirus, with an increase in coronavirus-related phishing and other social engineering lures, and increased use of ransomware targeting entities such as healthcare and schools, sparking outrage in many defenders who reported participating in working groups to counter these coronavirus-specific threats.

Although some responses focused on factors that have decreased, such as resources and staffing, many emphasized what has increased, such as attack surface and a focus on protecting communication methods, including email and videoconferencing, now that many workforces are fully remote. Consider the following examples from survey respondents:

"Due to the attack surface increase in size and complexity, additional CTI feeds are analyzed."
—Survey respondent

"[We] focus more on work-from-home (WFH) threats. Phishing, lost/stolen devices, home networking equipment malware, accidental release of sensitive information, unauthorized access to assets they shouldn't have."
—Survey respondent

Respondents also reported changes in the way communications occur, with both positive and negative impacts. Some respondents reported that the decrease in face-to-face conversations reduced sharing between teams and the need to set up a "meeting" with a 30-minute time slot and an agenda cut down impromptu conversations between CTI and IR/SOC teams.

Not all communications changes were negative, however. Several respondents reported that chat increased over text-based platforms and that more communication was occurring, not less.

"Our team has actually become more focused and collaborative with other stakeholders within the organization. This additional exposure has led to adding more individuals and teams to our product lists and additional PIRs."
—Survey respondent

Another area to highlight is the impact of coronavirus on the mental health and well-being of CTI analysts. Organizations reported an increase in awareness of how the crisis is impacting their employees and an understanding that while many are enjoying working from home, it can be difficult to "shut down" and take breaks from work when your "office" is your home. While CTI work is critical, taking care of ourselves and one another is also paramount.

CTI Processes: The Intelligence Cycle

The processes that CTI teams leverage vary from team to team; however, they tend to follow the same basic steps outlined in the traditional intelligence cycle. The intelligence cycle starts with understanding the requirements for the CTI work with which analysts are tasked (see Figure 4). With these requirements, analysts are able to focus on answering the key questions of decision makers and can tune their remaining processes to be as effective as possible.

Figure 4. Traditional Intelligence Cycle

Planning/Requirements

This year, a trend we saw beginning to form between 2019 and 2020 reversed as well. Those organizations that have formal requirements (39%) decreased by slightly less than 5%, and those that have ad hoc requirements (36%) increased by slightly more than 6%. See Table 2.

This again highlights that companies are moving through the maturation process, but are starting with ad hoc requirements rather than none, which is an improvement from years past. This may also indicate that a formal requirements process may not be a good fit for organizations just starting out and suggests a need for a more flexible process that meets the needs of the organization at any given time.

Those organizations without requirements or with no plans to generate requirements continued the trend of decreasing slightly each year.

Table 2. Year over Year Trends in CTI Requirements Definition

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

Another sign of increasing industry maturity is that executives and other business units outside of cybersecurity, such as legal and compliance, are contributing more to requirements. Security operations teams and CTI teams remained the top contributors to requirements. See Figure 5.

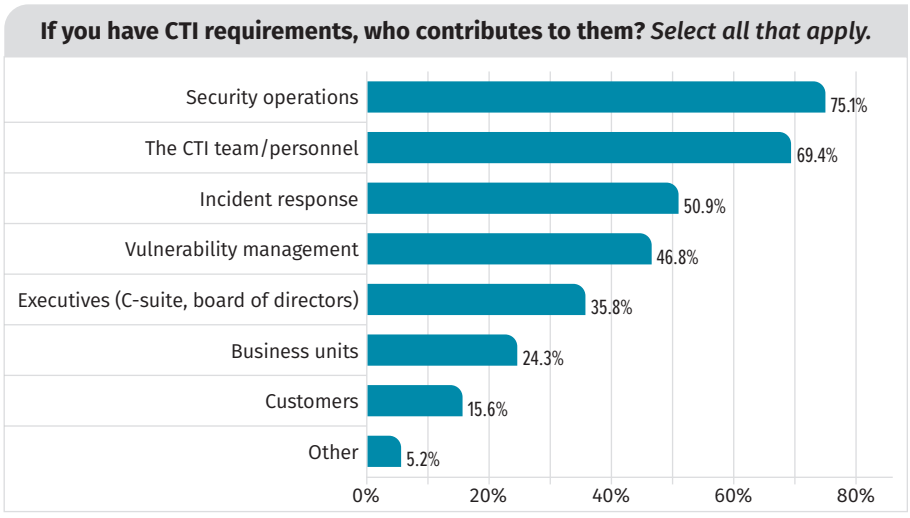


Figure 5. Contributors to CTI Requirements

Requirements are not static. As situations and threats evolve, so should requirements. This year, 38% of respondents reported that requirements are primarily updated in an ad hoc manner, which is slightly more than those reporting that they update requirements weekly, monthly, or yearly combined. However, respondents who reported that their organization never reviews and updates its CTI requirements or who just didn't know decreased from previous years, which is still promising.

We asked respondents to provide examples of their intelligence requirements, to help us gauge how organizations at different maturity levels are focusing their capabilities to best protect their organizations. If you are unsure of where your organization is, reading the following examples can help you identify where your organization currently is and what your next steps should be.

Beginning the CTI journey:

"We are still identifying what does and does not work for CTI and do not have any requirements at this time."
—Survey respondent

Next steps:

- Talk with other organizations in your industry or similar spaces to see what has worked for them in the past and get ideas of the intelligence requirements they focus on. Work with other security teams, such as the SOC or IR team (in-house or outsourced) to understand the threats the organization has faced in the past, which can also be good baselines for requirements.

Security-focused CTI efforts:

"Our main priority is to prevent and respond to Cybersecurity incidents and potential breaches by enhancing the IR processes implementing CTI."
—Survey respondent

Next steps:

- Reach out to stakeholders, including those outside of the security space, to ask them what intelligence about threats would help them make the decisions they need to in order to protect the organization.

Multifaceted CTI:

"What are the current exploitable vulnerabilities in our business that are more common? Liaise with the same sector organizations, and members of Information Security of other organizations [to understand what others see]. Support remediation action planning and change management."
—Survey respondent

Next steps:

- Set a regular cadence for reviewing and updating intelligence requirements, staying attuned to the threat landscape as well as internal changes in the organization that may lead to new requirements or retirement of requirements that are no longer needed.

Collection

After identifying requirements, analysts need to understand where to get the information that will be analyzed to provide the insight needed to help protect their organizations from threats. Information can come from many places, ranging from data in threat feeds (known as *threat data*) to reporting on events outside of cybersecurity that could potentially impact CTI. This year brought a notable increase in gathering and integration of information from "external sources such as media and news reporting," which experienced a jump of more than 10% over last year's results of 63%. Chosen by 77% of this year's respondents, it became the top source of information leveraged in CTI. See Figure 6.

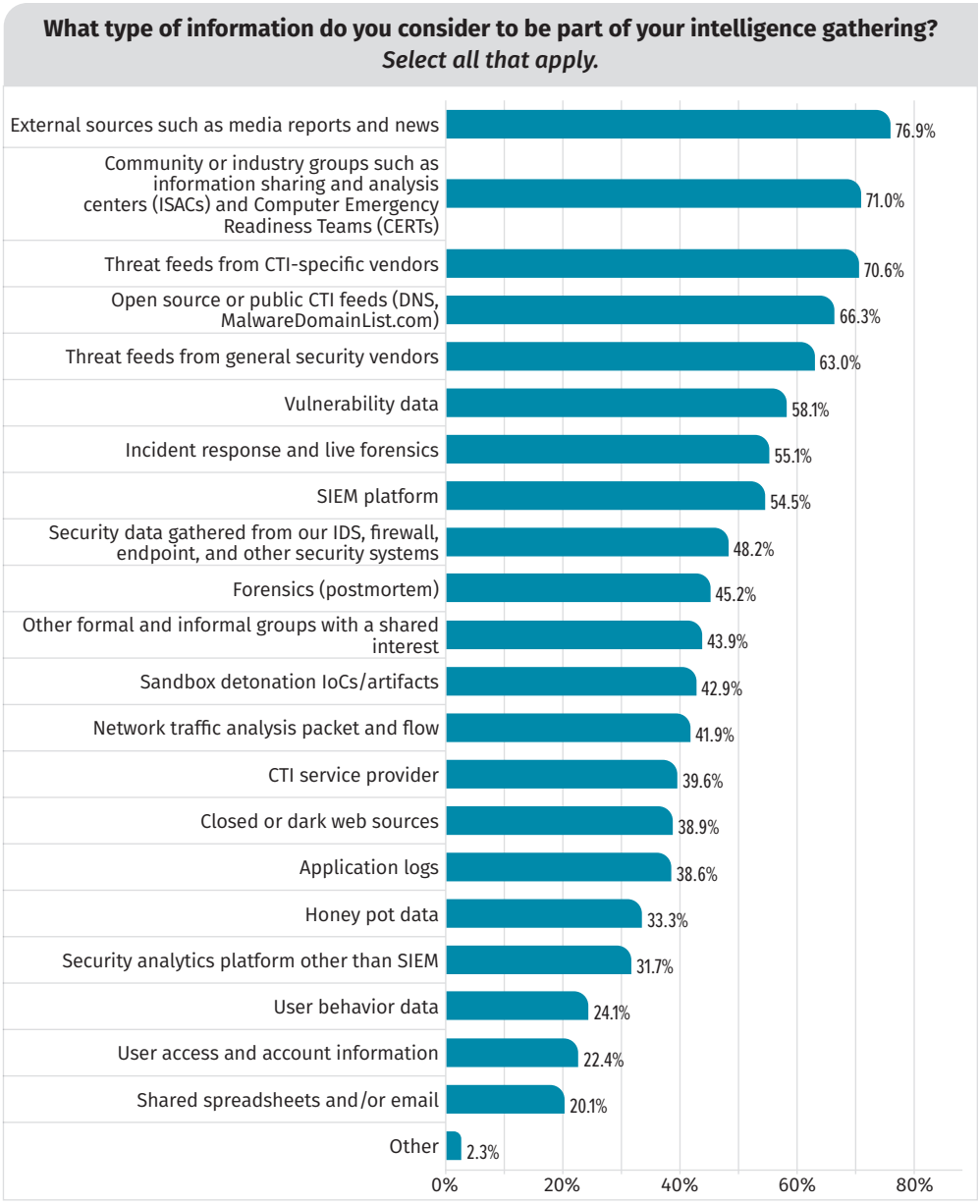


Figure 6. CTI Information Types

This trend highlights the need to understand how disinformation and misinformation make their way into the news that both individuals and CTI analysts consume. The recent emphasis in the security community on vetting analytic conclusions that are reported in the news (rather than trusting this information blindly) and using historical context around adversaries intentionally using disinformation to help identify the potential for disinformation has made this type of information more consumable for CTI purposes.[1]

Processing

Information processing puts the information that has been gathered into a format that makes it easy to leverage for analytic purposes. The most common types of processing involve data cleaning such as deduplicating information, enriching from various sources, and conducting malware analysis and reverse engineering.

[1] For more information, see "Information Anarchy: A Survival Guide for the Misinformation Age": www.youtube.com/watch?list=SRDisinformation+Guide+to&v=ixfaaVd4rlY

Processing is often viewed as the part of the intelligence cycle that is most suited to automation, because it typically involves repetitive tasks. The CTI industry has been working to automate more of these tasks in the past years, and the result is that the majority of processing tasks, with the exception of malware analysis, are moving toward being more fully or semi-automated than manual.

One interesting thing to note is that changes in other parts of the intelligence cycle impact follow-on tasks. With the move of news and media reporting as a top collection source for CTI analysts, additional processing capabilities are needed. Existing capabilities, including deduplication and enrichment, operate differently when the collection source is a threat feed in a machine-readable format and when the collection source is a news article. Several processing tools exist to help analysts integrate documents into their analysis, such as the MITRE Threat Report ATT&CK® Mapper (TRAM), and more CTI vendors are focusing on these capabilities as well. This is an area that should continue to grow if this trend carries on in a post-coronavirus world.

Analysis

Analysis, the process of breaking information down into its component parts in order to understand it better, is one of the most difficult areas of CTI to quantify. Because of that, we had not previously attempted to extract statistics on analysis. However, not everything needs to be quantified. We were able to identify trends in analysis based on open-form responses.

In CTI, analysis is necessary to understand threats, identify their relevance to a particular organization, and better position analysts to defend against or respond to them. Respondents described synthesizing information from a variety of sources, including information from their own defensive systems, information shared in public and private forums, and information reported in the media. Pulling information from multiple sources, even on the same topic, can provide a more robust understanding of a threat and help analysts assess which components are the most critical to focus on, based on their specific needs.

One area in which respondents continually described their analytic process is the assessment of how urgently their organization needs to respond to a report of a new vulnerability. Analysts can use CTI to identify whether bad actors are actively exploiting the vulnerability and what the impact of that exploitation is, which helps determine whether it is a priority.

For most organizations, the analysis component of the intelligence cycle is the area with the fewest formalized processes and tools, though many collection, processing, and management tools can support analytic endeavors. Moving forward, we hope to see an increased emphasis on measuring and supporting analytic efforts, which will move the industry forward significantly.

Dissemination

Dissemination is key to CTI—making sure that the right information gets to the right people in the format they need to utilize it. CTI can be disseminated several ways. Dissemination via tools gets information to technical partners, such as security operations and IR teams, and is useful in automated processes. Dissemination via narrative processes uses formats such as briefings, emails, reports, or presentations to get information to others who typically use it to shape their understanding of a situation and determine if any higher-level changes are needed in response to threats. See Figure 7.

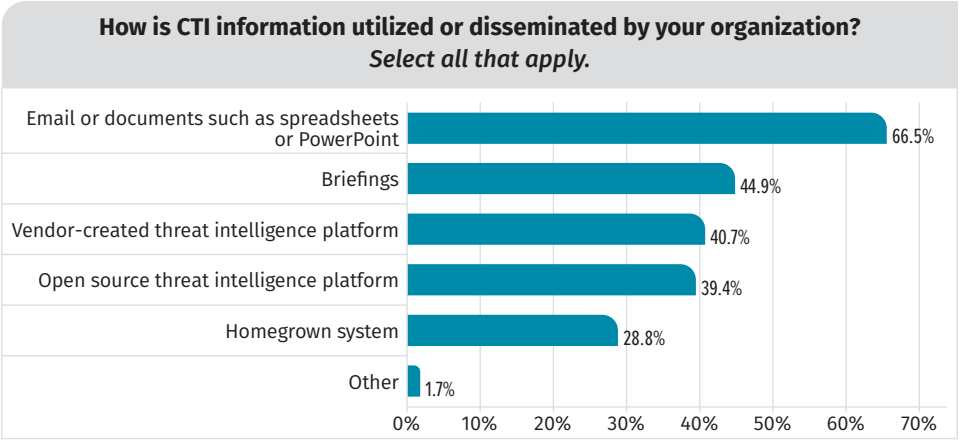


Figure 7. CTI Utilization and Dissemination

The most notable change in the dissemination of CTI this year is the sharp decrease in briefings from 53% in 2020 to 45% in 2021, which is likely due to the current remote work arrangements still in place for much of the world. Email-based reporting and both vendor-created and open source threat intelligence platforms—commonly used in a dashboard-type capacity—increased slightly, showing a shift toward asynchronous methods of disseminating relevant CTI information to stakeholders. See Table 3.

Table 3. Year over Year CTI Utilization and Dissemination

	2021	2020	Trend
Email or documents such as spreadsheets or PowerPoint	66.5%	66.3%	0.2%
Briefings	44.9%	53.0%	–8.1%
Vendor-created threat intelligence platform	40.7%	40.2%	0.5%
Open source threat intelligence platform	39.4%	37.0%	2.4%
Homegrown system	28.8%	35.5%	–6.7%
Other	1.7%	2.7%	–1.0%

CTI Tools

Analysts tend to have a love-hate relationship with their tools. But the reality is, threat intelligence analysts cannot be effective at scale and in a broader team without tools to help them maintain their knowledge, assist their analysis, provide some level of automation of their efforts, and find connections in data beyond what they can do on their first pass. This year's survey dove into the discussion of tools to see what analysts are doing and how they are operationalizing their tools and the tools around their organizations.

The first question asked was what type of management tools are being using to aggregate, analyze, or present CTI information. Unsurprisingly, spreadsheets and/or emails were one of the largest tools used consistently across organizations, but they also had one of the lowest levels of automation or unified GUI. Not everything needs to be automated and not everything needs a single GUI though. Microsoft Excel is consistently seen as a staple of the CTI community and is the one tool that is consistent in almost every CTI team on the planet.

However, automation and the ability to access everything from a single GUI, even if analysts are pivoting around, can be extremely helpful. Respondents indicated that SIEM and intrusion monitoring platforms use some level of automation (45% and 41%, respectively) for unifying analysis across tools and teams (see Figure 8).

We would expect to consistently see higher-level analysis being performed without a necessity on automation and more of the tactical-level work, including using and enriching indicators to include some levels of automation. It is interesting that the SIEM has more focus on automation than the CTI management platforms that analysts are using and might be indicative of a need in the CTI management platform market or an adoption of CTI management platform-like capabilities into the SIEM.

Further, on the topic of processing data and information specifically to include enrichment, deduplication, and standardization, respondents indicated that enrichment of information using external public data sources is semi-automated the most, at 46%. See Figure 9.

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.

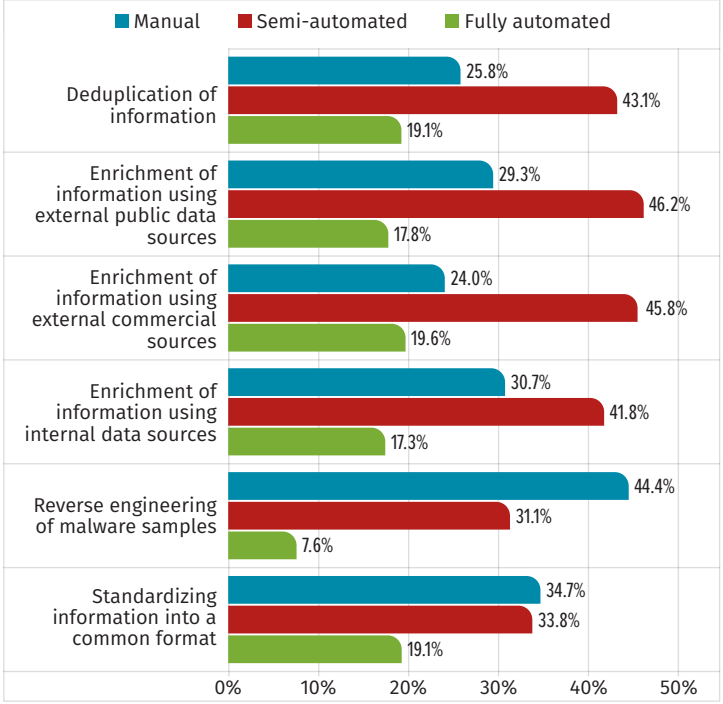


Figure 9. Information Processing

What type of management tools are you using to aggregate, analyze, and/or present CTI information?
Select all that apply and indicate whether these are used independently, utilize some level of integration/automation, or work together under a unified GUI.

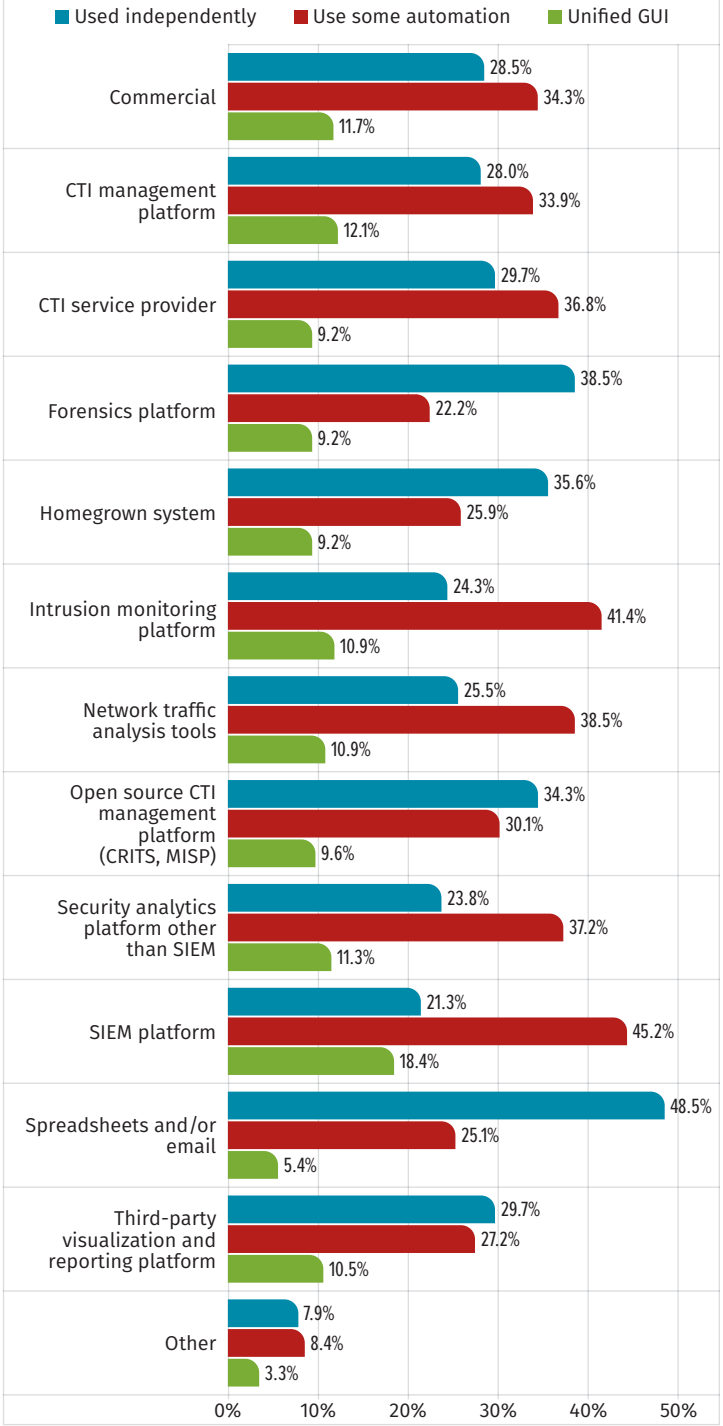


Figure 8. CTI Management Tools

However, enrichment of information using external data sources has the highest level of being fully automated, at 20%. Unsurprisingly, reverse engineering malware was the highest source of manual work, with 44% of respondents noting they do not automate those efforts, with 31% of that effort being semi-automated and only 8% being fully automated. This makes sense because most of the efforts that reverse engineers focus on are going beyond what is already available in tools and data sources to reveal new insights, often requiring a heavy focus on manual analysis.

As a recommendation, moving standardization of information into a common format is a good focus area for organizations this year. Thirty-five percent of respondents are doing this work manually, and moving to a more automated process should save time without compromising the analytical work required of analysts. See Figure 10.

More than 40% of respondents noted that CTI information is directly integrated. Across that integration, it is heavily focused on the threat intelligence platform, with 72% saying that it is their point of integration. Vendor-provided APIs are next, followed closely by intelligence service providers. Prebuilt connectors and third-party integrators have the least amount of integration, with 36% and 35% respectively (see Figure 11).

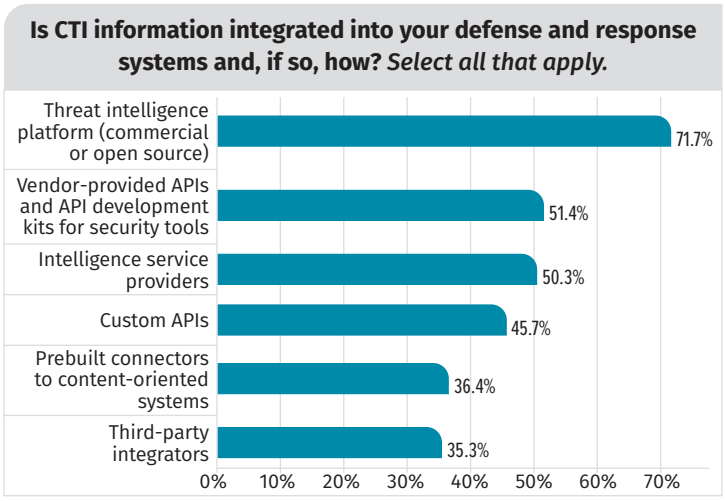


Figure 11. CTI Integration

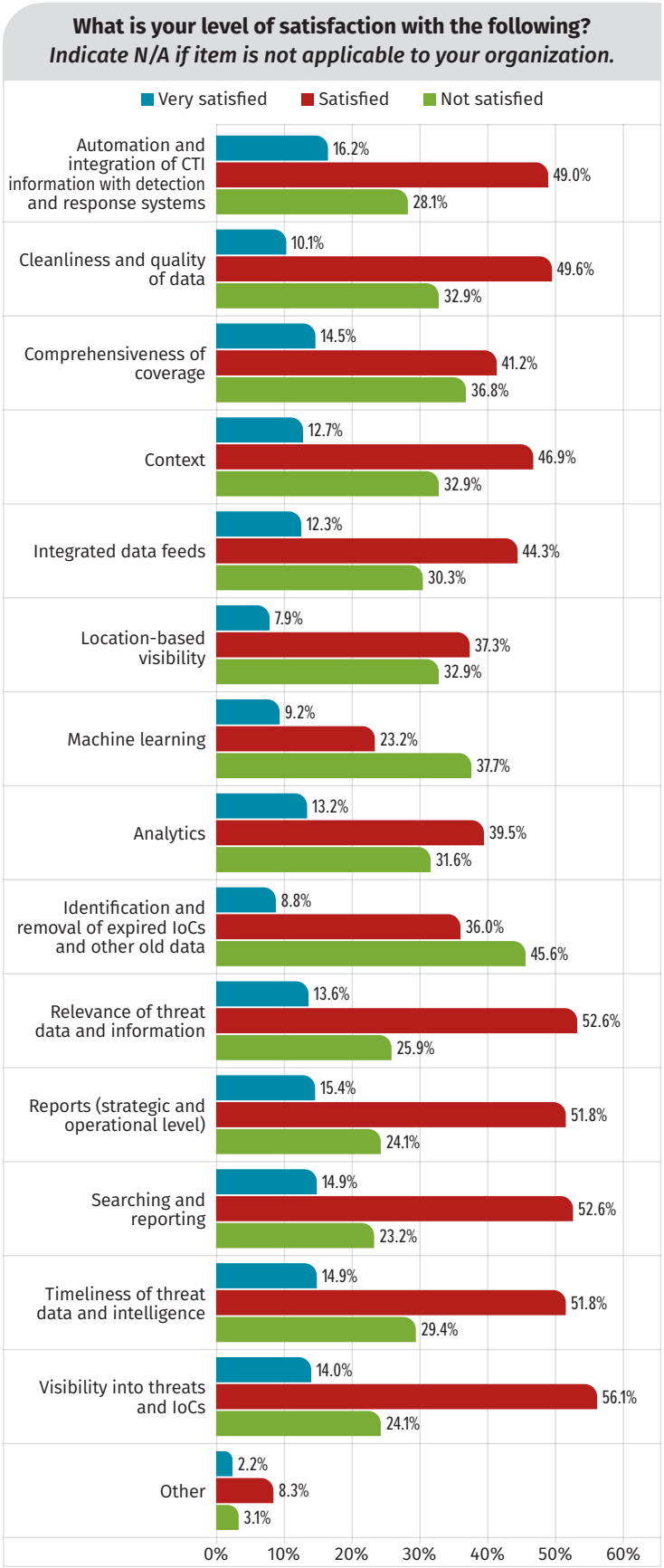


Figure 10. Information Processing Satisfaction

As we consider this finding, it is reasonable that the focus and operationalizing of threat intelligence platforms is the integration of information to defense and response systems. If anything, it is a bit surprising that only 72% of the people surveyed are using the threat intelligence platform in this way. A threat intelligence platform can be a large investment, and ensuring that it is assisting in detection and response efforts through direct integrations is a simple way to make those efforts more efficient. However, a reason for the gap could simply be the heavy reliance on automation in the SIEM for these efforts.

A significant change from last year, though, is the nearly 10% jump in vendor-supported API in this area, to 51% (up from 43% in 2020). Increased automation capabilities of processing tools could also explain this change.

Uses, Value, and Inhibitors of CTI

One of the areas that we have tracked across this survey every year is how organizations use CTI to add value to their security programs and what stands in the way of leveraging it more widely and more effectively. This year, we saw a broadening of the ways that organizations are leveraging CTI, as well as changes in the perceived value they derive from different types of CTI. We saw an increase in the number of organizations taking steps to track the effectiveness of their programs, which has a positive effect on the ability of an organization to articulate its needs and identify what is holding it back.

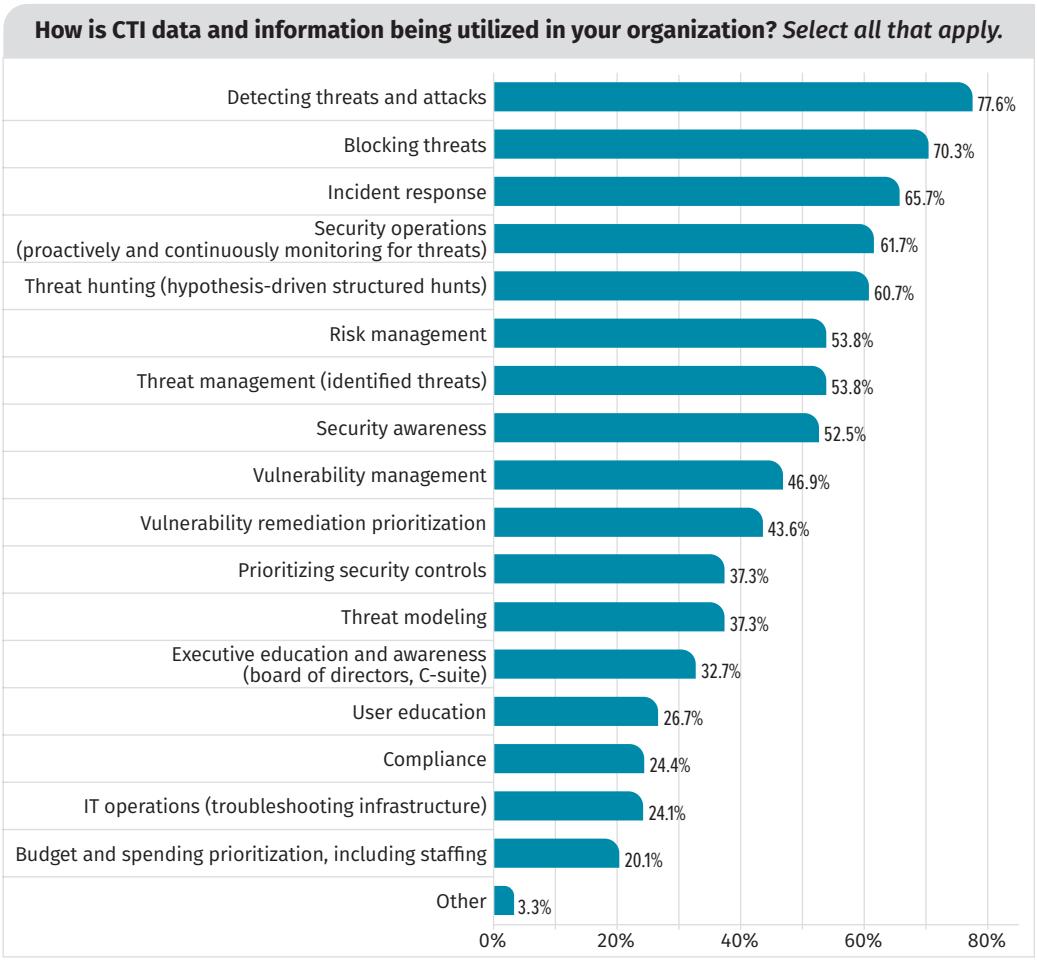


Figure 12. Data and Information Utilization

Uses

CTI has many uses in an organization, from strategic uses such as resource allocation and prioritization to tactical applications such as threat alerting and response. As in previous years, organizations continue to use CTI primarily in a technical capacity, including threat detection and blocking and incident response. However, the uses are growing in areas such as executive decision making and user awareness. The uses of CTI to support risk management and budget prioritization have both seen steady increases over the past years. See Figure 12.

When asked about types of information most useful to CTI operations, information about vulnerabilities being targeted by attackers (76%), malware being leveraged by attackers (73%) and broad information about attacker trends (72%) ranked highest (see Figure 13).

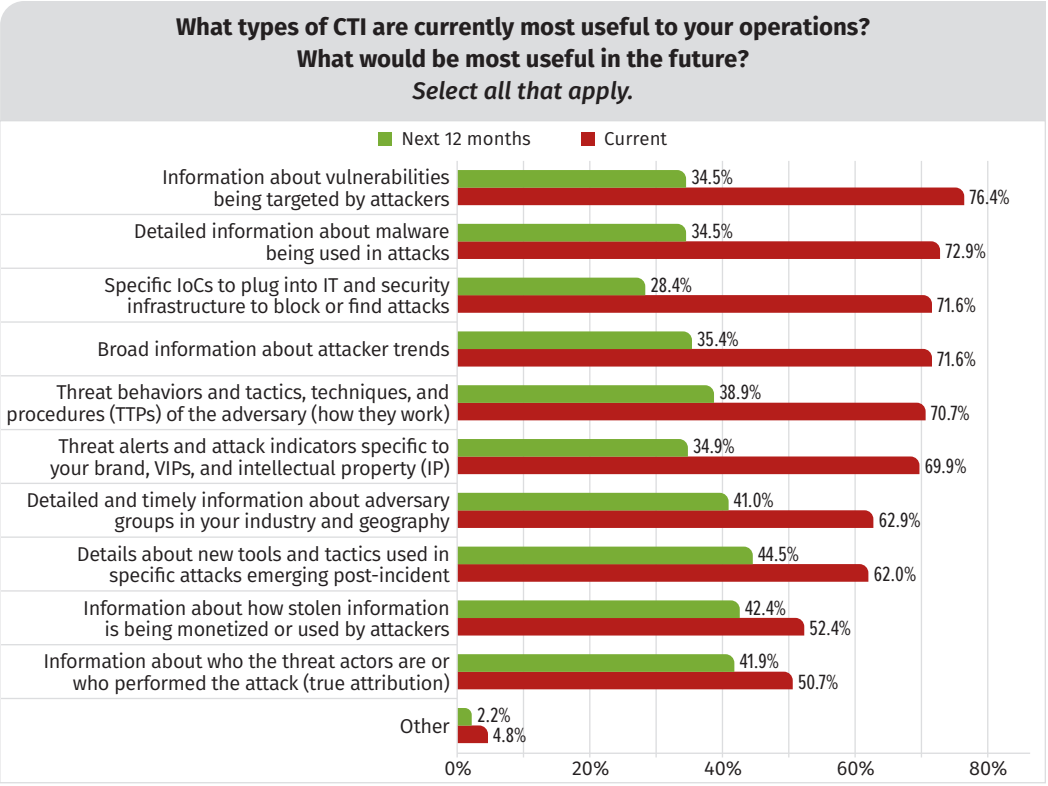


Figure 13. Usefulness of CTI Types

"Specific IoCs to plug into IT and security infrastructure to block or find attacks" is still one of the top answers from respondents when asked about current usefulness; however, it has the least respondents (28%) who anticipate IoCs being useful in the next 12 months. This demonstrates that while organizations still rely on IoCs, which are more straightforward to use with existing IT and security tools, most respondents predicted that they would use them far less in the future compared with other detection methods.

It is interesting to note that the perceived usefulness of these types of CTI decreased in 2021 from 2020, where vulnerabilities being targeted were previously used by 81% of respondents, a 5% decrease; threat behaviors and tactics were used by 73%, a 3% decrease; and detailed information about malware being used nearly 80% of the time, a 7% decrease. The usefulness of IoCs dropped from almost 76% in 2020 to 72% in 2021. See Table 4.

Table 4. Usefulness of CTI Types Year over Year

	2021	2020	Trend
Information about vulnerabilities being targeted by attackers	76.4%	81.3%	–4.9%
Detailed information about malware being used in attacks	72.9%	79.9%	–7.0%
Broad information about attacker trends	71.6%	71.7%	–0.1%
Specific IoCs to plug into IT and security infrastructure to block or find attacks	71.6%	75.7%	–4.1%
Threat behaviors and tactics, techniques, and procedures (TTPs) of the adversary (how they work)	70.7%	73.3%	–2.6%
Threat alerts and attack indicators specific to your brand, VIPs, and intellectual property (IP)	69.9%	73.9%	–4.0%
Detailed and timely information about adversary groups in your industry and geography	62.9%	70.5%	–7.6%
Details about new tools and tactics used in specific attacks emerging post-incident	62.0%	67.3%	–5.3%
Information about how stolen information is being monetized or used by attackers	52.4%	49.8%	2.6%
Information about who the threat actors are or who performed the attack (true attribution)	50.7%	48.0%	2.7%
Other	4.8%	6.4%	–1.6%

During this time, only two categories of intelligence saw their value rated higher than before: information on how stolen threat data is monetized, which increased from 50% in 2020 to 52% in 2021, and information on attribution of attackers, which increased from 48% in 2020 to 51% in 2021. These trends mirror the increase in threat data such as news and media reporting, which tend to focus on aspects such as how stolen data is used. These areas also saw a significant increase in expected usefulness in the next 12 months, reflecting the respondents who are still in the process of developing their CTI requirements and collection and who expect that their capabilities will be operationalized in the next 12 months.

Value

This year, 77% percent of respondents said that CTI had improved their detection and response capabilities. The most notable improvements were in "improving visibility into threats and attack methodologies impacting our environment," where respondents reported high numbers of both measured and significant improvements as a result of CTI. Detecting unknown threats was also seen as a significant source of value, along with prioritization efforts, which were certainly needed this year.

Measurably reducing the impact of incidents and preventing business outages were areas where respondents ranked CTI as less valuable.

Measuring Effectiveness

Last year was the first year we asked about measuring the effectiveness of CTI efforts, and this year there was a huge leap in those who reported that they measure effectiveness. In 2020, only 4% of respondents measured their programs' effectiveness, whereas this year 38% have some methods in place. Those who are tracking effectiveness capture various metrics, including number of automated or manual actions taken as a result of CTI, time it takes to respond to queries (or requests for information), and time it takes to respond to alerts generated by CTI. See Figure 14.

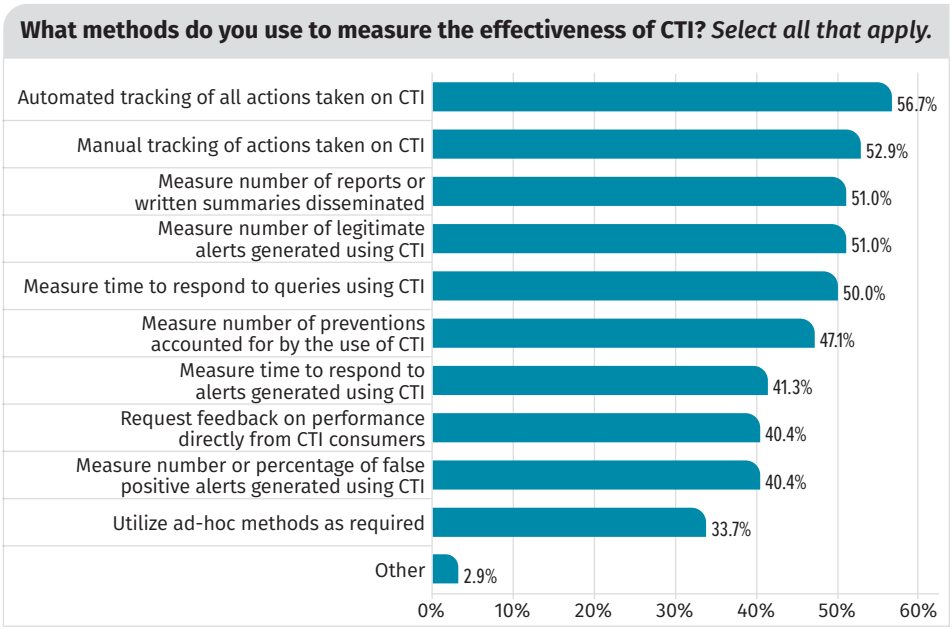


Figure 14. Measuring CTI Effectiveness

In the 2020 survey, we provided suggestions about how to begin to measure the effectiveness of a CTI program, and this year respondents have suggestions of their own. As with almost everything in CTI, measuring and reporting effectiveness should be based on each organization's requirements and its audience. Sometimes metrics and charts are needed, while at other times telling the story of how CTI supports operations will have the most impact.

"My team collects vignettes (usually PDF an email chain) when we see stakeholders discussing projects or plans in response to products we have shared. For example, we may share a warning report that a 3rd party reported a CVE being actively exploited and the number of systems we have exposed to that vulnerability. Our team may see the appropriate teams planning to prioritize patching or additional mitigations, and we will save off a copy of that email as a measure of our impact."

—Survey respondent

"We track the number of IT operations actions that result from CTI data, such as patching of high-severity CVEs to which we are particularly vulnerable."

—Survey respondent

Satisfaction with CTI

In the majority of areas, respondents are "mostly satisfied"—with the exception of removal of expired IoCs, which can commonly lead to false positives. In this area, 46% are not satisfied, 36% are somewhat satisfied, and nearly 9% are completely satisfied (see Table 5). Although this continues to be an area in which satisfaction levels are lower, they have improved over previous years.

There was a notable increase in satisfaction with automation and integration, which also aligns with respondents reporting increases in automation within CTI tools. In 2020, 62% of respondents were overall satisfied with the automation and integration of CTI information with detection and response systems, as opposed to 65% in 2021 with 16% of these current respondents very satisfied as opposed to only 9% in 2020.

Table 5. CTI Satisfaction

	Very Satisfied	Satisfied	Total Satisfied	Not Satisfied
Visibility into threats and IoCs	14.0%	56.1%	70.2%	24.1%
Searching and reporting	14.9%	52.6%	67.5%	23.2%
Reports (strategic and operational level)	15.4%	51.8%	67.1%	24.1%
Timeliness of threat data and intelligence	14.9%	51.8%	66.7%	29.4%
Relevance of threat data and information	13.6%	52.6%	66.2%	25.9%
Automation and integration of CTI information with detection and response systems	16.2%	49.0%	65.2%	28.1%
Context	12.7%	46.9%	59.6%	32.9%
Cleanliness and quality of data	10.1%	49.6%	59.6%	32.9%
Integrated data feeds	12.3%	44.3%	56.6%	30.3%
Comprehensiveness of coverage	14.5%	41.2%	55.7%	36.8%
Analytics	13.2%	39.5%	52.6%	31.6%
Location-based visibility	7.9%	37.3%	45.2%	32.9%
Identification and removal of expired IoCs and other old data	8.8%	36.0%	44.7%	45.6%
Machine learning	9.2%	23.2%	32.5%	37.7%
Other	2.2%	8.3%	10.5%	3.1%

Inhibitors

Lack of trained personnel decreased slightly from 57% to 54%; however, lack of funding increased slightly. This echoes comments from the section on impacts of the coronavirus on loss of resources for CTI tasks. See Figure 15.

An increase in the number of respondents who reported lack of automation from technical indicator to reporting value for the C-suite shows that automation increases in the CTI workflow have not been universal. This is one area where automation improvements would be beneficial.

What inhibits your organization from implementing CTI effectively?
Select all that apply.

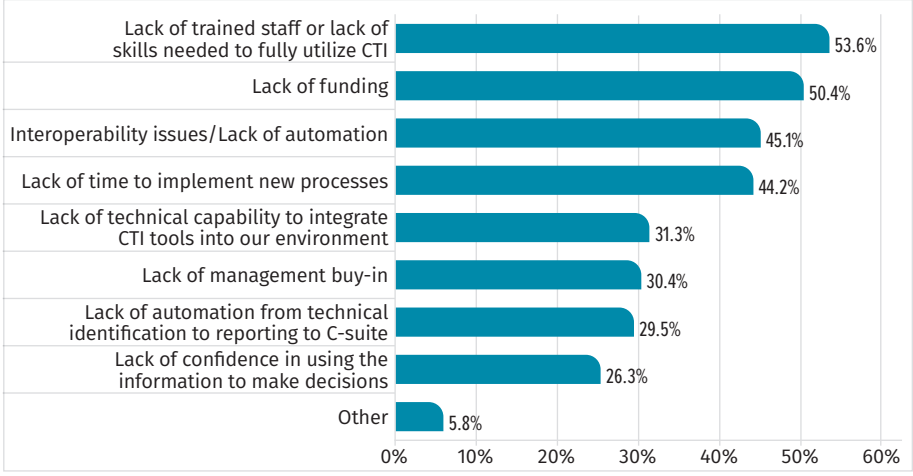


Figure 15. CTI Inhibitors

ISACs and Government Intel Sharing

When information sharing and analysis centers (ISACs) were first introduced as an industry-specific resource for information security practitioners, there were some—survey authors included—who did not expect them to provide significant value to the community. We are happy to report that this was a misjudgment because participation in ISACs and other government sharing programs and the perceived value they provide has increased year over year.

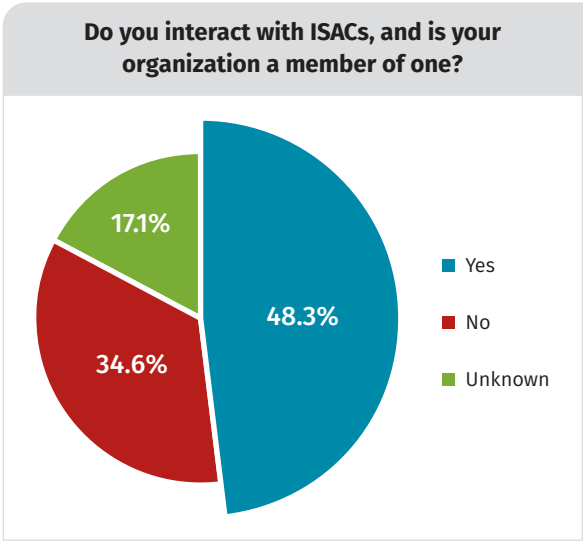


Figure 16. ISAC Participation

While the number of respondents who are part of an ISAC or other government information-sharing group increased to nearly 50%, the real change from previous years is that more people now know whether or not they are members of an ISAC. This year had the lowest number of respondents who do not know whether or not they are, at just 17%, down from 29% in 2020 (see Figure 16).

It is a common discussion point among those in the industry to highlight specific ISACs such as the Electricity ISAC and the Financial Sector ISAC. Beyond those two, there tends to be less awareness. However, anecdotally there tends to be a lot of movement from the Maritime Transportation System ISAC, Oil and Natural Gas ISAC, and Multi-State ISAC in a positive direction with community advocacy and interaction. Regardless of the CTI value of these organizations, they all represent community-focused approaches where people learn points of contact at other organizations and share insight. These efforts should be applauded, as should the ISAC members themselves.

Sixty-one percent reported utilizing government CTI, and nearly half of those respondents (49%) reported that they find this information valuable and that it provides insight they do not get from other open source or commercial sources. Considering the amount of money that gets invested into government intelligence sharing with the private sector and the process associated with getting it—which can be complicated and ambiguous—it is a bit disheartening to see only 49% of the 61% who utilize it finding significant value. The efforts of those in governments around the world can and should be lauded, but at the same time those government agencies should review the costs and benefits and look to tailor their efforts to meet intelligence consumers where they are.

When we asked respondents about the value derived from a sharing group, this year's survey results showed increases in three specific areas:

- Advocacy in the community for security
- Member meetups and events
- Training and conferences

While it initially seems counterintuitive that more value was derived from meetups and conferences in a year where everyone is working from home, the shift to virtual and remote conferences and meetups has actually made these events more accessible to many without the time or budget to travel (which were also noted as inhibitors). Hopefully, this trend of connecting people and providing support and advocacy remotely continues into the future.

Moving Forward

There is significant growth among organizations that have just started standing up CTI programs in recent years. While we have traditionally seen growth in organizations that are further along in their CTI journeys, it is very promising to see smaller organizations make progress as well—with higher numbers of small to medium businesses participating and an overall reduction in respondents who said they plan to implement programs/functions—with those numbers shifting to actual implementation across the maturity spectrum.

More organizations are integrating media reporting into their intelligence collection plans, showing the importance of knowing how to properly analyze this information for misinformation and disinformation and how to integrate it into CTI programs. Additional tool capabilities will be needed to address the increase in this type of information in CTI.

Automation of many key tasks, such as data deduplication and standardization, as well as improvements in automation of integration into detection and response systems, are all improvements that will support efficiency and scale of CTI tasks. Additional automation is still desired, though, including building automation into the process of making technical CTI data relevant to organizations' decision makers. These types of tasks are difficult to automate and will vary among different organizations, where stakeholders and decision makers have different priorities. However, with the proper insight and customization, it is possible to use automation to support CTI analysts in making these connections.

About the Authors

Rebekah Brown, co-author of FOR578: Cyber Threat Intelligence, is a cybersecurity and intelligence analysis professional specializing in threat intelligence, network warfare analysis, systems analysis, and threat modeling. Rebekah spent over a decade on active duty as a cryptologic linguist, network warfare analyst, and cyber operations chief in the United States Marine Corps before moving to the private sector, where she has developed threat intelligence programs at multiple Fortune 500 companies. She received degrees in International Relations from Hawaii Pacific University and Homeland Security with a cybersecurity focus as well as a graduate certificate in Intelligence Analysis from American Military University. She is a published author, instructor, and public speaker on intelligence-driven incident response and adversary tactics.

Robert M. Lee, a SANS certified instructor and author of ICS515: ICS Active Defense and Incident Response and FOR578: Cyber Threat Intelligence courses, is the founder and CEO of Dragos, a critical infrastructure cyber security company, where he focuses on control system traffic analysis, incident response, and threat intelligence research. He has performed defense, intelligence, and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Author of *SCADA and Me* and a nonresident National Cyber Security Fellow at New America, focusing on critical infrastructure cyber security policy issues, Robert was named EnergySec's 2015 Energy Sector Security Professional of the Year.

Sponsors

SANS would like to thank this paper's sponsors:

ANOMALI®

Infoblox® NEXT LEVEL NETWORKING

CISCO™

sixgill

DOMAINTOOLS®

THREATQUOTIENT