SANS

Analyst Program

Survey

SANS 2023 CTI Survey: Keeping Up with a Changing Threat Landscape

Written by **Rebekah Brown** and **Katie Nickels**

July 2023

ANOMALI Bitdefender cisco

Silobreaker ZEROFOX

Executive Summary

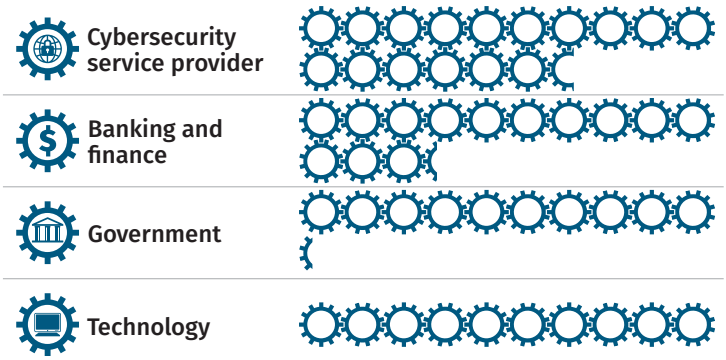
Events throughout 2022 highlighted the positive impact of cyber threat intelligence (CTI), from informing decisions about major ransomware intrusions to cyber conflict around the war in Ukraine. With this year's survey bringing in the most respondents we've ever had, the diverse feedback from CTI personnel helps highlight areas where CTI as a discipline has matured, as well as opportunities where it still must grow. Key insights from this year's survey include:

- Current events and geopolitics significantly influence what CTI personnel focus on, with most respondents reporting that the war in Ukraine has influenced their team's priorities. CTI personnel frequently rely on external news sources when deciding what to prioritize, which can prove both beneficial and challenging.
- CTI analysts continue to use a range of sources as they consume and produce intelligence, with an emphasis on external over internal sources. Although teams use multiple sources, indicators of compromise (IOCs) continue to play a key role in supporting defensive tools and teams.
- CTI is an increasingly cross-functional process in many organizations. Examples of CTI work frequently cite partnerships between CTI teams and other teams within an organization, including vulnerability management teams, security operations teams, and incident response teams. Although the importance of these partnerships is clear, they aren't without challenges—inter-team communication and trust are often identified as hurdles to overcome.
- Partnerships between CTI vendors and customers are critical, and CTI vendors play a significant role in this discipline. The majority of respondents reported using external CTI service providers in some way. We also see both an increase in the number of respondents who work for cybersecurity companies and an increase in the discussion of specific CTI vendors, products, and tools when describing CTI work. This can be a beneficial relationship to have as long as organizations continue to leverage critical internal threat-intelligence data and CTI vendors continue to help organizations know when information is relevant and actionable for them.

Survey Respondents

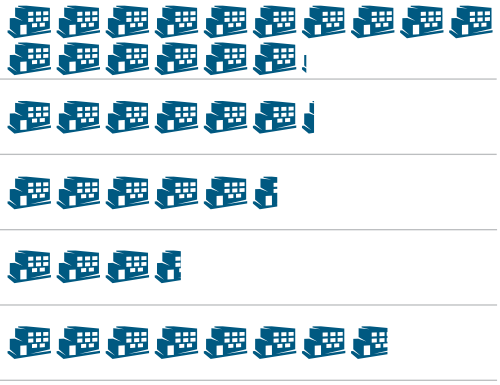
This year's survey received feedback from 984 individual respondents in more than 25 different industries. More than four times as many individuals responded to this year's survey as compared to 2022, allowing us to integrate many more perspectives. See Figure 1.

Top 4 Industries Represented



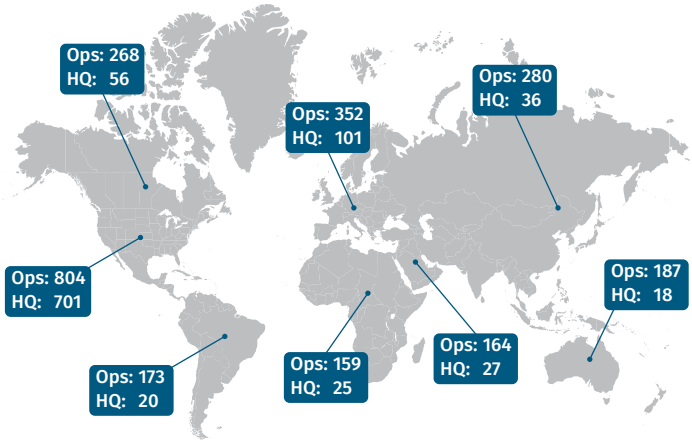
Each gear represents 10 respondents.

Organizational Size

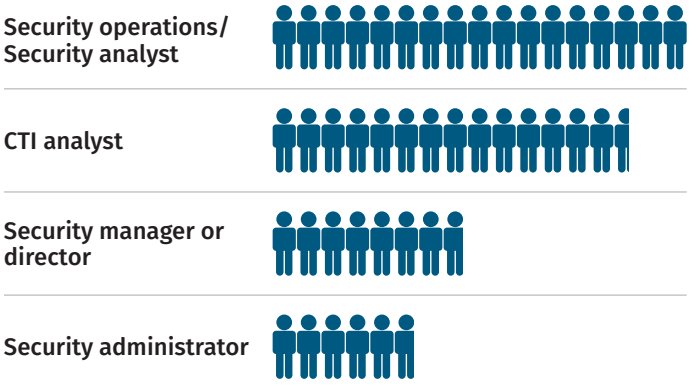


Each building represents 25 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 10 respondents.

Figure 1. Survey Demographics

This year we had several respondents from a new industry not previously included in our data collection: the water industry (including utilities and waste). In October 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released an alert on the ongoing attacks against the water sector, highlighting the critical importance of water services and the active threats that the sector faces.[1] Although we have had survey respondents in the past who identified themselves as water and wastewater sector employees, beginning this year we are including their responses as one of the 18 sectors listed in the survey. CTI work is done across many more fields than those 18, and each year we have many respondents from industry types not listed by default. This year we see a notable increase in the diversity of those fields, including agriculture, mining, civil engineering, construction, gaming, health and wellness, and law. Figure 2 illustrates some of those various industries represented by the survey respondents.

Figure 2. Industries Represented in 2023 Survey

This demonstrates that CTI continues to be a growing field and that organizations of many types can benefit from CTI. Recent attacks show that no one particular industry is being targeted; instead, attackers continue to find ways to monetize attacks in nearly every vertical. In addition to organizations in these fields benefiting from experienced CTI analysts, the CTI field itself will gain from the increased diversity of thought, experience, and perspective as analysts work against threats that can impact organizations in unique ways.

Another notable change observed in this 2023 survey is that the primary industry of respondents is cybersecurity service providers, as compared to 2022 when it was banking and finance. This notable shift suggests that CTI analysts working for cybersecurity service providers represent a substantial portion of the community. Cybersecurity service vendors often approach CTI differently than "end-user" organizations such as banks because these vendors often have visibility into many organizations while also working to balance requirements from those many stakeholders.

This year's respondents were heavily skewed toward the United States, with 71% of their organizations being primarily headquartered in the United States, up from 58.6% of last year's respondents. Although this is not surprising, it's important to note this as a limitation of the survey, because respondents are heavily influenced by their country of operations.

[1] "Ongoing Cyber Threats to U.S. Water and Wastewater Systems," www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a

People and Teams

This year's survey respondents came from a variety of team sizes and types. The organization size most commonly represented in this year's survey is 101 to 500 employees, at 17%, with another 11% representing organizations with fewer than 100 employees. This highlights the fact that organizations of all sizes utilize CTI to support their overall security operations, a far cry from the days when CTI was only thought of as useful to the top 1% of companies.

Fifty-one percent of respondents report that their organization has a formal dedicated CTI team, the highest number we have seen since 2020. See Figure 3.

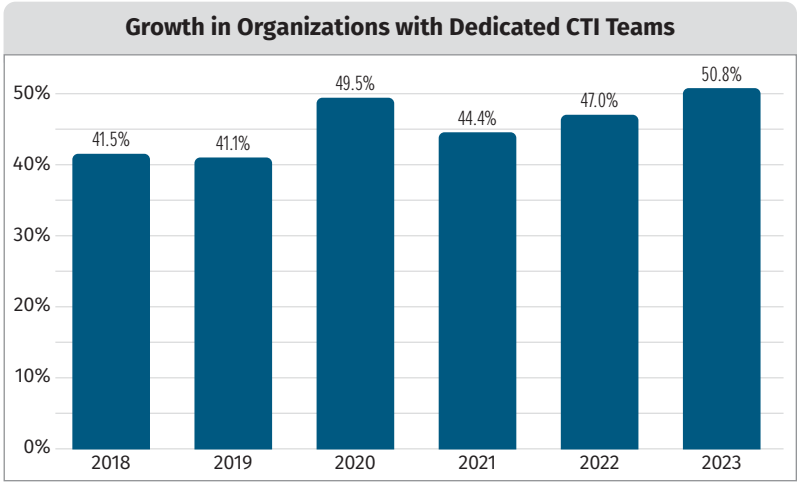


Figure 3. Growth of Formal CTI Teams

Formal dedicated teams often have more bandwidth to focus on critical CTI processes that can help streamline and optimize the work of CTI analysts, and we see reflections of this throughout the survey. Sixteen percent of respondents say they have a single dedicated person, and 21% say CTI is a shared responsibility with staff pulled from other security groups. Analysts at smaller organizations and those with a single CTI analyst face unique challenges in terms of resources, and small businesses remain at a high risk of intrusions because of this. It's encouraging to see that these organizations still recognize CTI as an important function within their security staff, because CTI can help small organizations prioritize against the most impactful threats.

One primary way organizations supplement these limited in-house CTI resources is through external CTI service providers. A majority of respondents report using external CTI service providers in some way, with 47% using a combination of in-house and service provider resources, and 17% exclusively using service providers. Using a combination of both in-house and external resources can be a wise choice for many organizations. Such an approach allows external providers to cover widespread threats that affect most organizations, while in-house personnel focus on applying that CTI to their organization and to unique threats their organization faces.

In terms of skill sets and focus areas of those working in the CTI field, the largest group of respondents identify themselves as security operations and security analysts, at 17%, followed by CTI analysts at 15%. This is a significant increase compared to the 2017 survey, in which only 6% of respondents identified themselves as dedicated CTI analysts, indicating substantial growth in this career field.

Requirements and Prioritization

The first phase of the intelligence cycle is planning and direction, which involves crucial activities to set up teams for success. A critical part of this phase is defining intelligence requirements—the questions or needs an organization has that an intelligence team can seek to support. If teams do not define requirements, they risk producing intelligence that doesn't support key decisions and that isn't used by consumers. Respondents this year clearly recognize the value of requirements, because 59% of them report that CTI requirements are clearly defined in their organization.

This represents a positive change from 2022, in which only 35% of respondents reported they had clearly defined CTI requirements. In fact, this year only 3% or respondents do not have requirements and have no plans to create them, down from 11% in 2022. Although this change is likely due, at least in part, to the maturity of respondent organizations, it suggests a promising trend: that CTI teams are thinking carefully about what they need from intelligence. See Figure 4.

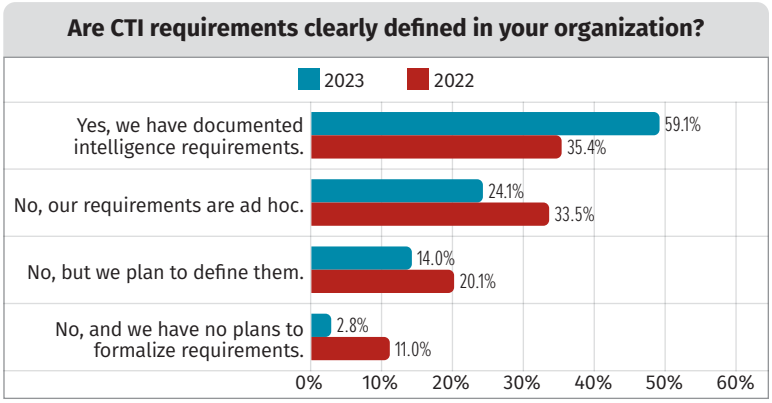


Figure 4. CTI Requirements

When it comes to who contributes to CTI requirements, however, responses show an opportunity for growth. Sixty-nine percent of respondents say the CTI team themselves contribute to requirements, compared to only 32% of respondents reporting that executives contribute. This presents an opportunity for CTI teams to potentially increase engagement with executive leadership, a group that has both a need for and a desire for CTI. Looking for additional contributions to CTI requirements beyond just the team itself presents an opportunity for teams to expand the value and impact of CTI.

Prioritizing requirements and the work the CTI team undertakes is a challenge across many teams. This year's responses reveal that the majority of CTI teams spend a significant amount of time responding to open source reporting from others, including threat reports from researchers and cybersecurity news stories. Over half of respondents note that they spend more than 40% of their time on this set of activities.

When asked how teams determine which CTI tasks to work on and how they prioritize threats, one respondent offered a clear explanation: "Whatever is trending." This response indicates that analysts and their leadership increasingly hear about cyber threats from social media, blog posts, cybersecurity news, and even mainstream news. Another noted that their requirements are often overridden when senior management panics about something and the CTI team is told to prioritize that. This trend isn't surprising given the wealth of open source information about cyber threats that constantly inundates consumers. However, this also presents an opportunity for CTI teams to try to clarify to their consumers that topics trending in the news are not always the most impactful to their organization.

Many respondents shared more structured approaches to prioritizing their work, which fell under several main categories:

- Examining assets in their organization's environment and assessing threat priority based on the risks to those assets
  - Example response: We look at known threats in the public/private domain and compare them to related software and/or vulnerabilities and prioritize these based on the prevalence of the software/system versus the actual severity of the vulnerability that may exist within our environment. What may also contribute to the order of addressing such items is the fact of any potential compensating control that may technically reduce the severity level of the vulnerability if not able to patch, etc., or haven't patched yet.
- Considering threats that others have reported as impacting the organization's industry
  - Example response: Primarily based on industry threats and trends as reported by peers/peer groups and third-party providers.
- Prioritizing threats observed in the organization's network
  - Example response: Threats from email attachments. We saw an increase in these attacks, so we decided to take action and block certain attachments.

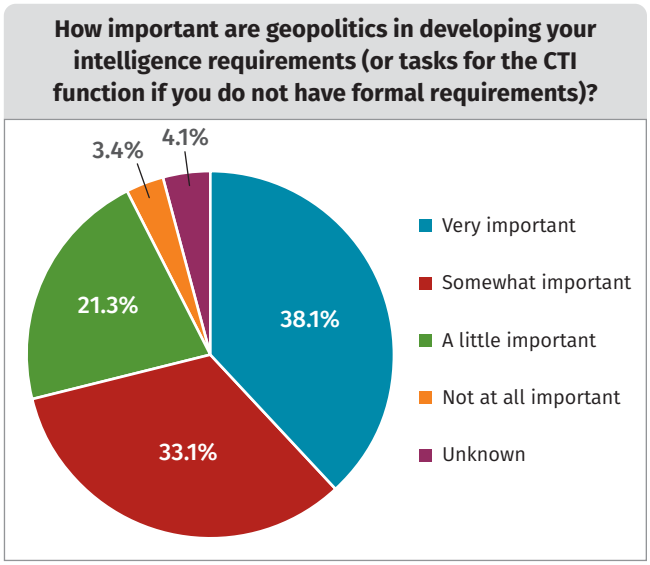


Figure 5. Geopolitics' Influence on Requirements

When it comes to deciding what to focus on, 71% of respondents report that geopolitics play a very important or somewhat important role in determining requirements. See Figure 5.

A key geopolitical event in 2022 that influenced many teams' requirements was the war in Ukraine, with 84% of respondents saying the conflict influenced their requirements in some way. See Figure 6.

This trend is understandable given the high-profile nature of the war and the anticipation by many intelligence analysts that it could lead to significant Russian targeting of US entities, particularly critical infrastructure. The effectiveness of the Department of Homeland Security (DHS) CISA Shields Up campaign, which aligned with respondents' prioritization related to the conflict, is evident.

Although the conflict may not have resulted in all-out "cyberwar" as some analysts anticipated, the focus on defending against Russian threats may have resulted in improved defenses that thwarted many attacks.[2]

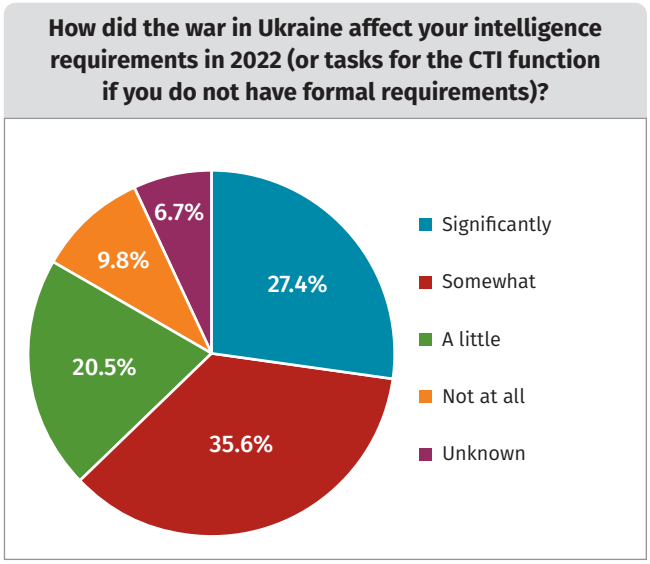


Figure 6. Effect of the War in Ukraine

[2] "Defending Ukraine: Early Lessons from the Cyber War," https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Sources

Just as requirements are key to focusing on the right questions or problem areas for an organization, information sources are vital to the quality, accuracy, and actionability of CTI. When it comes to sources of information gathered by CTI personnel, external sources such as commercial or open source threat feeds, news, and social media continue to be more commonly used than internal sources such as security event logging and forensics data. Consistent with the pattern that trending news is key in prioritizing intelligence requirements, 69% of respondents report external sources such as media reports and news as their primary information source. The most commonly used internal source they report is incident response and forensics data, used by 52% of respondents. See Figure 7.

This finding presents an opportunity for CTI personnel to remind themselves of the value of internal information, particularly from intrusions. This information can provide valuable insight, in particular because it specifically targeted that organization, meaning the threats are guaranteed to be relevant. Despite the value of internal intrusion analysis, there are many obstacles to getting this information, including that teams may not want to share it or may not have the resources to fully document findings from an intrusion.

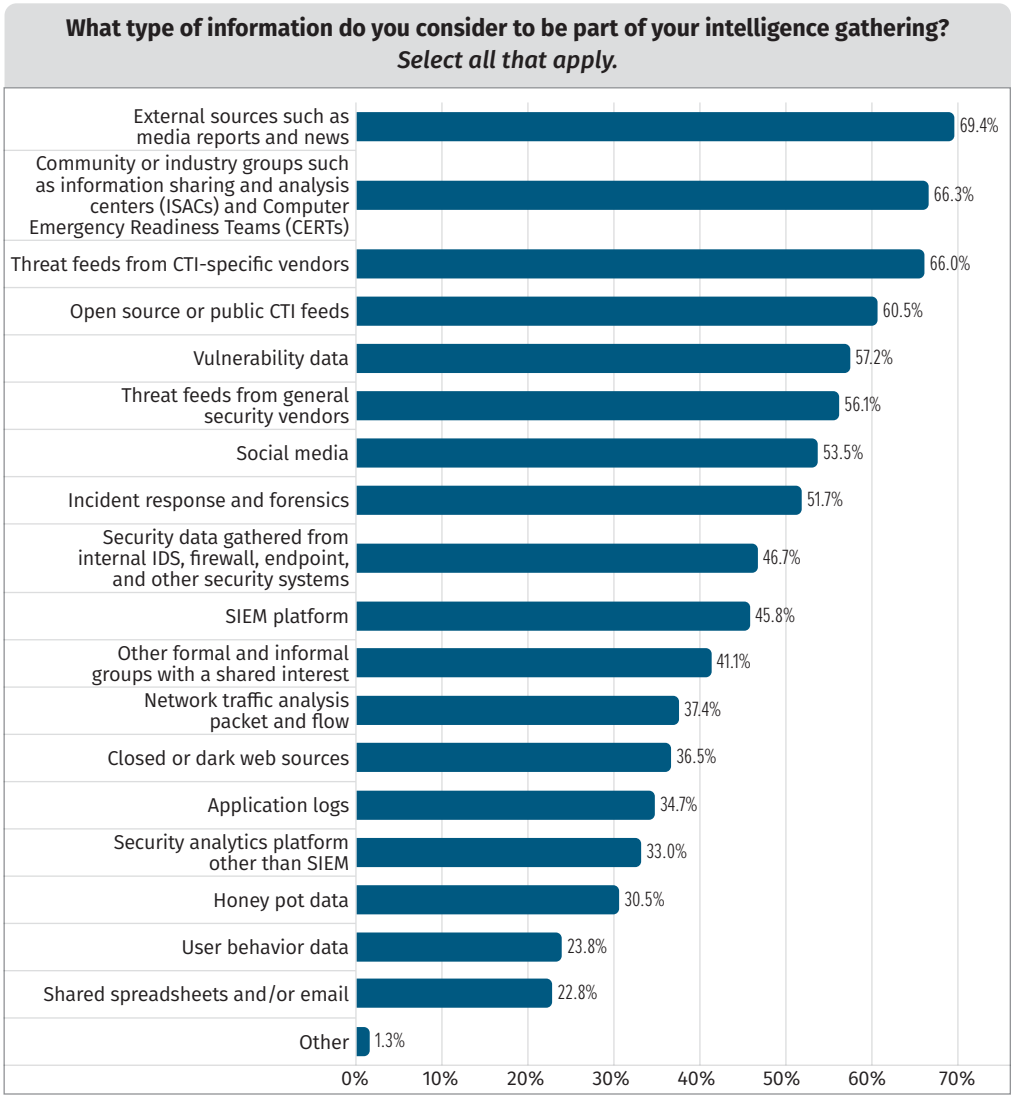


Figure 7. Information Sources

Following external news sources, the second most commonly used source among respondents is community or industry groups, such as information sharing and analysis centers (ISACs) and Computer Emergency Readiness Teams (CERTs), with 66% of respondents reporting use of these sources. This finding suggests that these formal groups have a key role in disseminating information to CTI teams, because this source was more popular than other formal and informal groups used by 41% of respondents.

Other top sources include threat feeds, including from CTI vendors (used by 66% of respondents), open source (61%), and general security vendors (56%). These threat feeds are often made up of IOCs such as hash values, domain names, and IP addresses.

One of the most common responses to the open-ended question about examples of CTI in action involves indicator use cases. Multiple respondents report that they use commercial or freely available IOCs to ingest into tools such as security information and event management (SIEM) and endpoint detection and response (EDR) to determine whether they are present on their network. This finding shows that even with the rise of tracking tactics, techniques, and procedures (TTPs), including with MITRE ATT&CK®, CTI personnel still find value in indicators as a key source. This is likely in part due to the ease of applying indicators in tools. Although indicators can play a role in CTI, organizations should consider, as their CTI function matures, how they can produce or consume beyond feeds of IOCs.

Producing Intelligence

After CTI teams have identified appropriate personnel, established requirements, and collected information from many sources, they must analyze that information to produce intelligence outputs. Thoughtfully leveraged tools and processes help enable analysts to be efficient and thorough as they do this. Once intelligence outputs are produced, their work isn't done yet; they still need to disseminate those outputs in an accessible way and obtain feedback to refine and improve future products.

Production and Consumption

It is often said that intelligence is both a process and a product, and CTI is no different. CTI is both produced by following intelligence processes and is also consumed using a different set of processes. Some organizations analyze their own data about previous data breaches or network intrusions and generate intelligence products (or reports) based on that information. They may also generate raw data such as lists of IOCs that they can use internally and also share externally. CTI can also be consumed by organizations that take intelligence provided by external sources such as threat-intelligence vendors or information-sharing groups and apply it to their own internal processes. Many organizations use a combination of the two types, leveraging their own internal information, as discussed earlier, and also incorporating intelligence generated by others into their security processes. A few organizations—primarily threat-intelligence providers—only produce intelligence that is meant to be used by other organizations without consuming other sources of intelligence. See Figure 8.

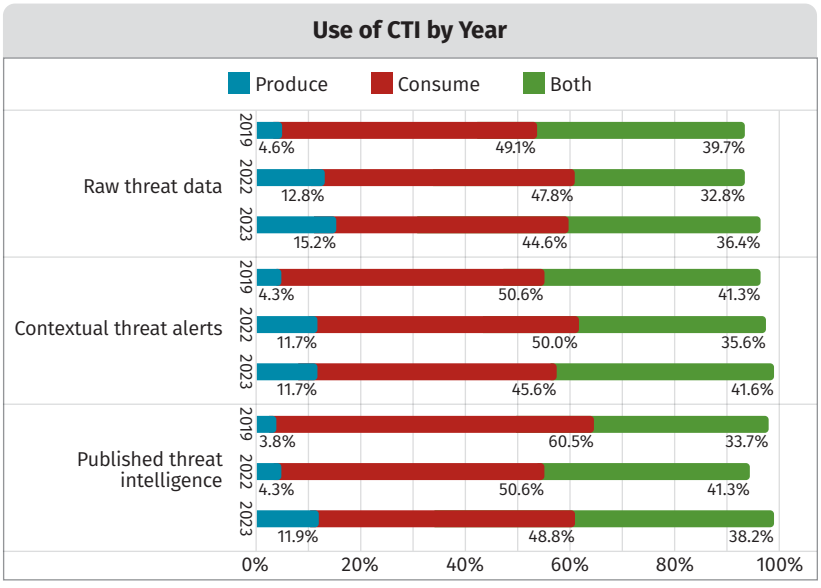


Figure 8. Year-over-Year CTI Usage

This year's survey shows that the highest number of respondents consume intelligence and that the numbers are rather consistent across the types of information that they consume: raw threat data, contextual alerts, and published threat intelligence. Of those who produce intelligence, their most common output is raw threat data consumed by other organizations, with 15% of respondents producing this output. This indicates how the field of threat-intelligence production has grown over the past few years. In 2019, only 5% of respondents exclusively produced raw threat data, and 3% produced published threat intelligence. The doubling (and even tripling) of respondents in this space demonstrates the growing market for threat intelligence and the growing ability of vendors in this space to produce intelligence for consumption. Interestingly, aside from the increase in production, the balance of those consuming and both consuming and producing has remained relatively consistent over the past few years with one exception: Nearly 10% fewer organizations exclusively consume published intelligence reports, whereas the number of organizations producing and the number of organizations both producing and consuming intelligence reports have both increased, indicating an overall higher level of reporting available. Not only are there more reports by volume, but they are being produced by a greater number of organizations, which likely leads to an increase in the diversity of reporting perspectives and approaches.

When we asked respondents to share examples of CTI at work, we can see some of the unique ways that organizations both consume and produce intelligence.

Consume

- "We consume threat-intel data from other third parties in order to evaluate [our] overall security posture and also used by our threat-intel and incident-response teams to act on potential security breaches."
- "IoCs gathered from events on peer/similar/same region companies shared through a closed group."
- "External threat intel is used to support the prioritization of vulnerability management and remediation, primarily as an 'escalator' in cases where intel aligns with vulnerabilities aligns with exposure."

Produce

- "We produce threat intelligence from our IR practice; we share those findings publicly."
- "We produce internal intelligence reports from synthesis of external reports, identifying specific areas that are usable for our security operations, such as threat detection and threat-hunting opportunities."

Tools

As teams are producing and consuming CTI, various categories of tools can help them be successful and efficient. As they have for several years, spreadsheets reign supreme when it comes to tools used to aggregate and analyze CTI information, with 71% of respondents using them. This highlights that a simple spreadsheet remains a powerful and cost-effective way to help analysts organize information, even with the availability of CTI-specific tools. The second-ranked tool (59%) behind spreadsheets was a SIEM or other security analytics platform, demonstrating that CTI personnel are making use of tools that are likely already in their environment for use by other security operations teams. Open source threat-intelligence platforms (TIPs) ranked third, with 48% of respondents using these TIPs.

Analytic Processes

With an increase in production of intelligence, it is important to pay attention to both the sources being used, as discussed earlier, and the analytic processes being used. This is the second year that we have asked survey respondents to share some information about the processes and techniques that they use when conducting analysis. We asked respondents about five different methods they commonly use in intelligence analysis and asked whether they use those methods frequently, occasionally, or never. The most commonly used method is intuitive or judgment-based analysis, followed very closely by threat modeling, and then the use of conceptual models such as the Diamond Model or Kill Chain. See Figure 9.

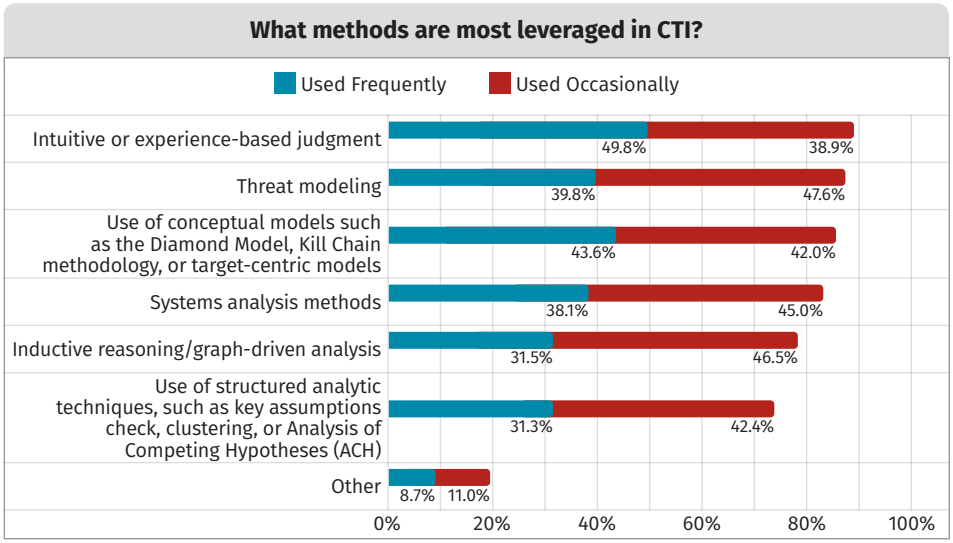


Figure 9. CTI Methodologies

In both 2022 and 2023, respondents indicated that they use intuitive analysis and experience-based judgment most heavily, with nearly half of respondents using this method frequently. Experience and intuition can both be useful to analysts as they work to interpret threat data and synthesize insights, but because cognitive biases can lead to flawed analysis, it is important that analysts do not rely solely on them. The good thing is that most analysts do not exclusively rely on experience; they pair that beneficial experience with other methods of analysis to counter biases and use their intuition as a starting point rather than the entire process. In the past year, we have seen significant jumps in the number of people reporting that in addition to experience-based judgments they also frequently use conceptual models, structured analytic techniques (SATs), and inductive reasoning/graph-driven analysis.[3] Most notable is the increase in those who frequently leverage SATs, which are methods specifically designed to counteract cognitive bias in analysis. In 2022, only 19% reported that they frequently use SATs in analysis. In 2023, that number has jumped to over 30%!

[3] "There Is MOAR To Structured Analytic Techniques Than Just ACH! – SANS CTI Summit 2018," https://www.youtube.com/watch?v=PtYWVzY2Ves

Dissemination and Feedback

Once CTI has been produced—whether this production was done by a third-party partner, a vendor, or the CTI team itself—it needs to get to the right people or systems at the right time to enable them to make the best use of the intelligence. Another critical component of the dissemination process is gathering feedback to make sure that the intelligence benefited the organization. If it is not helping improve security or helping defenders make more insightful decisions, then something about the CTI process needs to be adjusted. Organizations should approach dissemination and feedback intentionally as a critical part of the intelligence process.

Dissemination Methods

All the methods we asked about in the survey—emails, integrations with threat intelligence platforms, reports, and briefings—are each used by over 50% of respondents. This indicates that CTI personnel have to be prepared to disseminate information in different formats based on the goals and the audience. Several respondents described using both written reports and in-person or remote briefings for security-education and security-awareness purposes. The same content that organizations can use for security-awareness briefings—for example, a change in tactics in phishing campaigns—likely also has indicators that they can disseminate to security tools via a threat-intelligence platform, doubling the impact of the same threat-intelligence content.

A Note on RFIs

This year some respondents pointed out that it isn't always the threat-intelligence team pushing information out to others. Sometimes other groups within an organization reach out to CTI teams with requests for information (RFIs). Responding to RFIs is a great way not only to provide information to the organization, but also for CTI teams to learn more about which types of information are helpful to others in the organization, which they can then use to generate future intelligence requirements. In fact, RFIs represent a type of feedback on what organizations find valuable.

Impact of CTI

As previously mentioned, gathering feedback is one of the best ways to ensure that CTI is benefiting an organization. This holds true whether you are an in-house CTI team or individual or are part of a CTI team in a cybersecurity organization that provides intelligence to multiple partners. This year, 50% of respondents indicate that they measure the effectiveness of their CTI programs, and 87% report that CTI has helped to improve security prevention, detection, and response. Of those who measure the effectiveness of their programs, the most common methods of measurement are first automated and then manual tracking of actions that they take based off of CTI. Many also use the time it takes to respond to an alert or incident as a measure of impact. Although CTI might not be able to prevent all incidents, it can help reduce the time it takes to respond to an issue. Interestingly, only 23% get feedback directly from customers as a method of measuring impact. See Figure 10.

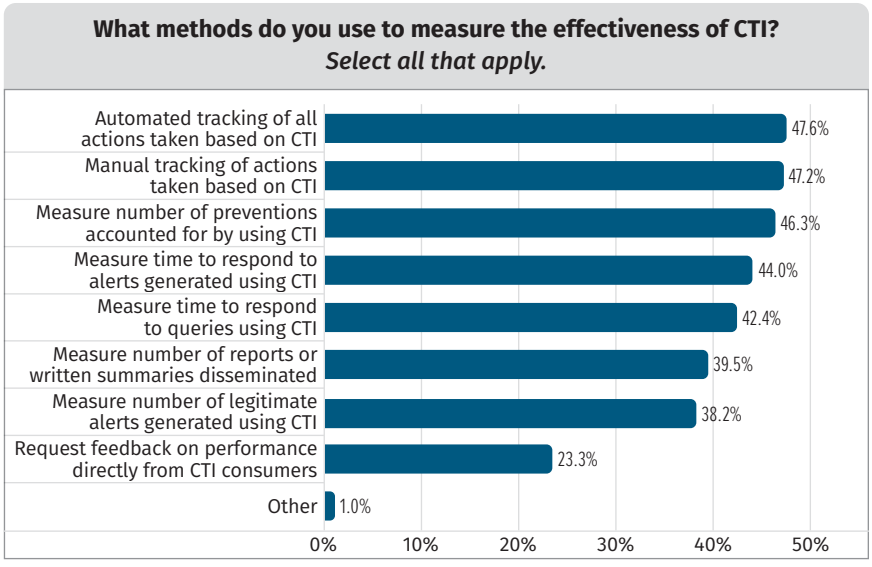


Figure 10. Measuring CTI Effectiveness

Although we saw a lower number of respondents who directly solicit feedback, when we asked for examples of how they measure CTI impact, we received several responses that spoke to the importance of this type of feedback:

- "We capture key success stories with our customers. How did our notification/report result in actions taken to improve security and reduce risk for our customers? How did our actionable information result in timely actions and decisions?"
- "[We] meet regularly with consumers to discuss feedback from CT intel and collaborate on what is working, what needs improvement, what they would like to see."
- "Feedback from customers about effectiveness of defensive measures taken on the basis of [CTI]."

Gathering feedback, directly or indirectly, provides a great way to understand the impact of CTI and identify ways to improve or optimize the support being provided to other teams.

Challenges and Limitations

This year's survey highlights many ways that the CTI field continues to grow in maturity and capabilities, which we see from things such as an increase in the number of organizations with formal and documented intelligence requirements, the number of organizations with dedicated CTI teams, and an increase in the analytic methods organizations use to generate CTI. When it comes to challenges, we also see a decrease in challenges reported across the board. Although all these indications are promising, many organizations still face significant challenges when it comes to CTI. Survey respondents cite a number of areas that currently hold them back, including a lack of training, lack of staff, lack of time, and lack of automation. See Figure 11.

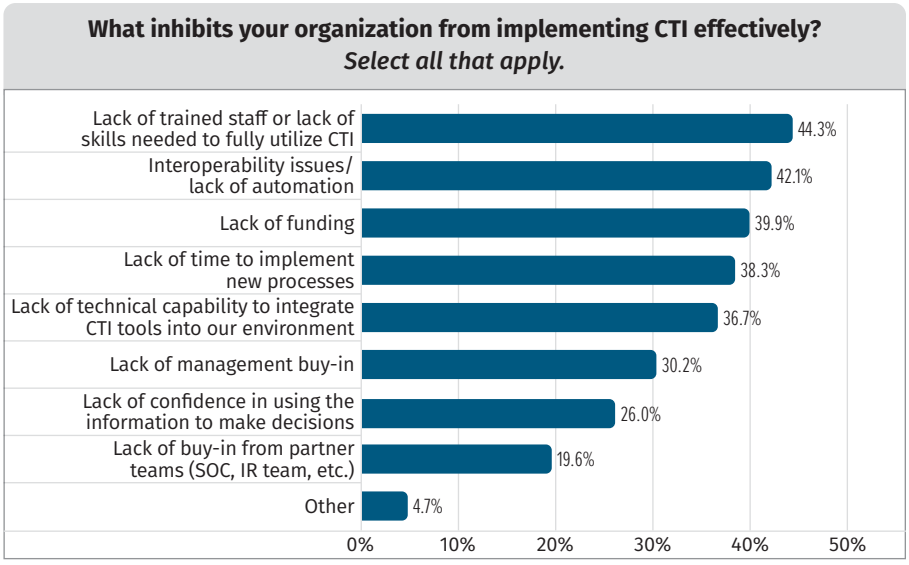


Figure 11. CTI Challenges

Lack of trained staff is a commonly cited challenge in the CTI space. Although we see many signs that the CTI field continues to mature, it is still a relatively new field in cybersecurity, and the growth of CTI teams can often outpace the training pipeline. In 2022, 57% of organizations listed lack of trained staff as their number one challenge. This year, although staffing still remains the top challenge, that number has dropped down to 44% of organizations. Many great resources are available for those looking to get into the CTI field or those in other cybersecurity jobs who are interested in learning more about CTI. To get started, check out these blogs:

- Cyber Threat Intelligence Self-Study Plan—Part I[4]
- Cyber Threat Intelligence Self-Study Plan—Part II[5]
- CTI Reading List[6]
- SANS CTI Summit Presentations[7]

Despite the reduction in the number of challenges CTI teams face, lack of automation remains a hurdle to many and is the second most prevalent challenge experienced by CTI personnel. This area has grown steadily since 2017 and peaked in 2022. We can attribute the decrease of more than 10% to the rise in cybersecurity vendors providing threat-intelligence support, with many using their own platforms and tools as part of their processes. An improvement in these tools would have a significant impact on the overall industry, and many teams who struggle to optimize their workflows would welcome the change. See Figure 12.

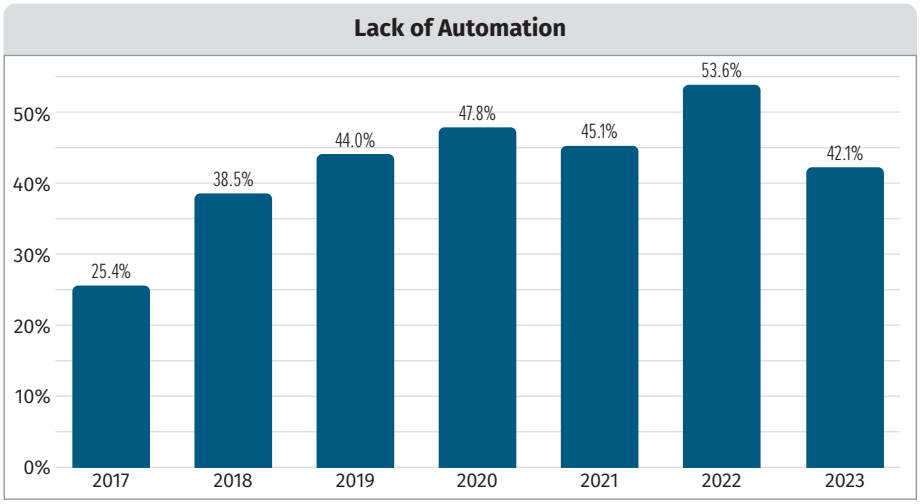


Figure 12. Year-over-Year Automation

Many of these challenges are ones we have been tracking through this survey for years, but we are always on the lookout for new challenges and limitations facing CTI personnel. Challenges identified by respondents include:

- Lack of communication and sharing between teams
- Lack of trust between teams, such as hesitancy to share incident data or lack of confidence in the accuracy of information
- Lack of awareness of CTI functions and their value

One big way to build trust, increase awareness, and improve communications between teams is to seek out and act on feedback from other teams within an organization. You read about the importance of feedback in earlier sections as it relates to developing requirements and measuring impact, but it can also prove helpful for establishing trust relationships and showing the value of increased collaboration.

[4] https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-1-968b5a8daf9a

[5] https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-2-d04b7a529d36

[6] https://sroberts.medium.com/cti-reading-list-a93ccdd7469c

[7] https://www.sans.org/presentations/

In coming years, as CTI continues to evolve and as threat actors and technologies advance, we will continue to look for challenges facing CTI teams. One challenge that became apparent, beyond the survey questions addressing challenges themselves, is the increasing difficulty CTI analysts face because of the growing volume of open source reporting. Over 60% of survey respondents wrote that they spend more than half of their time responding to open source reporting, including threat reports from researchers and cybersecurity news stories. In addition, in the past few years, media reporting has become one of the top sources of information that CTI personnel consume. This focus on reports and the subsequent need to respond to the many questions they raise is an area where the CTI field could benefit from additional best practices and processes, especially when it comes to the potential risks of disinformation.

Moving Forward

CTI analysts will continue to face demands from various stakeholders, whether those are leaders asking about the latest cybersecurity news or incident responders requesting help to understand a threat's lateral movement. Organizations can use many of the responses from this year's survey to help them prioritize requirements as they move forward. Recommendations to aid with the challenging task of prioritization include:

- Understand the organization's assets, software, infrastructure, and information to help focus on threats most likely to affect those.
- Include multiple stakeholders in the CTI requirement prioritization process to ensure the team doesn't focus solely on what the CTI team thinks is important.
- Recognize that CTI analysts cannot address all needs and limit prioritized requirements based on the number of personnel allocated. For many teams, limiting core requirements to no more than 3–10 requirements may be appropriate.

Developments around the world will continue to influence CTI, whether in the form of geopolitical conflict or new malware. As this year's survey reveals, world events sometimes consume a significant portion of CTI resources, which could result in organizations deprioritizing other valuable sources. CTI teams should strive to strike a balance between using external news as a source and incorporating internal intrusion analysis as well. Although finding the right role for so-called current intelligence isn't easy, CTI personnel might consider providing a single product line focused on external news as one approach while ensuring that other products focus on a broader range of sources than just external ones.

CTI will remain a potent force to help teams combat cyber threats and to empower stakeholders of all types in their decision making. As the field continues to grow and evolve, we expect to witness even more maturity in people, processes, and technology as CTI personnel tackle fresh challenges and address new areas of need.

Sponsors

SANS would like to thank this survey's sponsors: