A SANS Survey

# 2020 SANS Cyber Threat Intelligence (CTI) Survey

Written by **Robert M. Lee**

February 2020

*Sponsored by:*
**ThreatQuotient**

Analyst Program

# Executive Summary

*Cyber Threat Intelligence (CTI)* is analyzed information about the capabilities, opportunities and intent of adversaries that meets a specific requirement determined by a stakeholder. Organizations with CTI programs focus on understanding the threats they face and providing specific information to help defend against those threats. In the past few years, CTI has evolved from small, ad-hoc tasks performed disparately across an organization to, in many cases, robust programs with their own staff, tools and processes that support the entire organization. 2020 was a big year for the SANS CTI Survey, with a record number of respondents and the highest ever reporting of CTI programs within organizations, with 1,006 responding to the survey in 2020 and just 505 responding in 2019.[1] Some areas leveled out after years of growth—such as implementation of threat intelligence platforms and a focus on tactics, techniques and procedures (TTPs) over just indicators of compromise (IoCs)—and some areas continued to grow both in number and variety, such as the types of data being used to generate intelligence. As the field settles into its new maturity, understanding and improving the effectiveness of CTI programs will become even more critical. With that in mind, SANS asked respondents to weigh in on how their programs measure effectiveness, an area that CTI programs must continue to improve on in the coming years.

## TAKEAWAYS

- **Collaboration is key.** While the number of organizations with dedicated threat intelligence teams is growing, we continue to see an emphasis on partnering with others, whether through a paid service provider relationship or through information-sharing groups or programs. In addition, collaboration within organizations is also on the rise, with many respondents reporting that their CTI teams are part of a coordinated effort across the organization.
- **Not all processes require the same level of automation.** Semi-automation may be the gold standard when it comes to data processing, even for some tasks that are often considered redundant, such as data deduplication, because such information is sometimes useful to analysts.
- **The necessary data and tools change as CTI teams evolve.** As more organizations begin to produce their own intelligence, the nature of information that CTI analysts require is also shifting from primarily threat-feed or vendor-provided information to data from internal tools and teams. While many of the same tools and processes can be used to handle this type of information, organizations also must determine how this changes their need for tools handling this data.
- **Requirements are taking hold and are a staple of mature teams.** Requirements are a key part of the intelligence process and help to ensure a focus on collection and analysis efforts by analysts as well as proper production of intelligence. This makes the intelligence process more efficient, effective and measurable—keys to long-term success. Last year, a minority of organizations reported that they had clearly defined and documented intelligence requirements, which was highlighted as a key recommendation for organizations. This year, nearly half of respondents answered that they have defined and documented intelligence requirements. This is a fantastic jump in the data and is an encouragement to anyone who is seeking to add defined and documented intelligence requirements into their CTI program.
- **A community of consumers and producers contribute to CTI.** More organizations consume intelligence than produce it (as we would expect), but more than 40% of respondents both produce and consume intelligence. This is a great indicator of the growing maturity and professionalization of the cyber threat intelligence field. Organizations that have trouble satisfying a majority of their intelligence requirements—because they are only consuming intelligence or are missing any of their priority intelligence requirements—should consider moving to both generating and consuming intelligence. Those considering generating cyber threat intelligence should review the SANS CTI Summit videos[2] on the topic and/or attend a CTI course.[3]

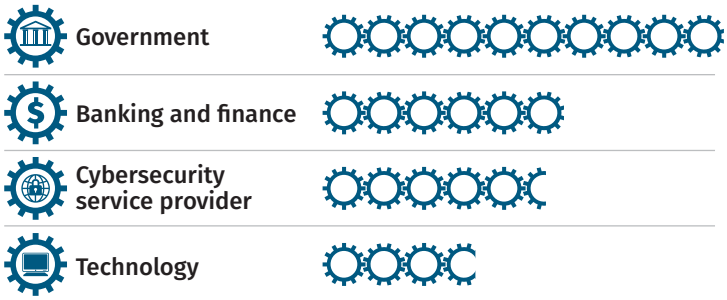
[1] "The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey," February 2019, www.sans.org/reading-room/whitepapers/analyst/evolution-cyber-threat-intelligence-cti-2019-cti-survey-38790 [Registration required.]

[2] www.youtube.com/watch?v=RwsAiz9dBEQ&list=PLfouvuAjspTrfjl_CskRxIAsMHdWusK-j

[3] www.sans.org/course/cyber-threat-intelligence

This year's survey response pool represented a wide-ranging group of security professionals from various organizations. Figure 1 provides a snapshot of those respondents.

### Top 4 Industries Represented

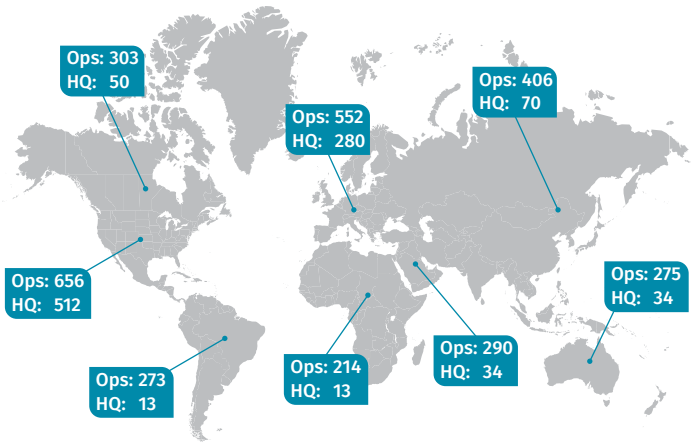



*Each gear represents 25 respondents.*

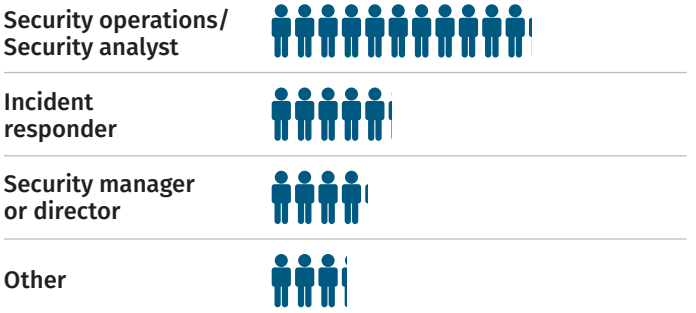
### Organizational Size


*Each building represents 25 respondents.*

### Operations and Headquarters




### Top 4 Roles Represented




*Each person represents 25 respondents.*

*Figure 1. Key Demographic Information*

## CTI Programs: The Right People and the Right Tools

Cyber Threat Intelligence involves analyzing information about threats and producing guidance to determine what steps must be taken in response to those threats. This process, which by now seems intuitive *in concept*, is incredibly complex and relies on a combination of people, processes and tools to both generate, consume and act on the intelligence. All three things are critical to a successful CTI program. Without personnel to evaluate information and make analytic judgements, there would be no CTI. Likewise, without processes and tools, even the best analysts will find themselves severely limited in the amount of data they can turn into actionable intelligence compared with the volume of threats their organizations potentially face. While the 2020 CTI Survey results show some promising improvements in these critical areas, they also highlight places where the community would benefit from continued efforts.

## People

People are often considered the core of a CTI program. Not only do they conduct the analysis that will lead to finished intelligence, but they also decide what tools and processes to use to support their efforts. A single analyst can be successful with the right tools and support from other security teams; however, respondents have historically reported the difficulty that these lone individuals face when trying to keep up with the sheer volume of tasks. In the past three years, we have seen an increase in the percentage of respondents choosing to have a dedicated team over a single individual responsible for the entire CTI program. According to the 2020 CTI Survey results, almost half of all respondents report that they have a dedicated team, which is especially encouraging because it means those single analysts now have help! See Figure 2.

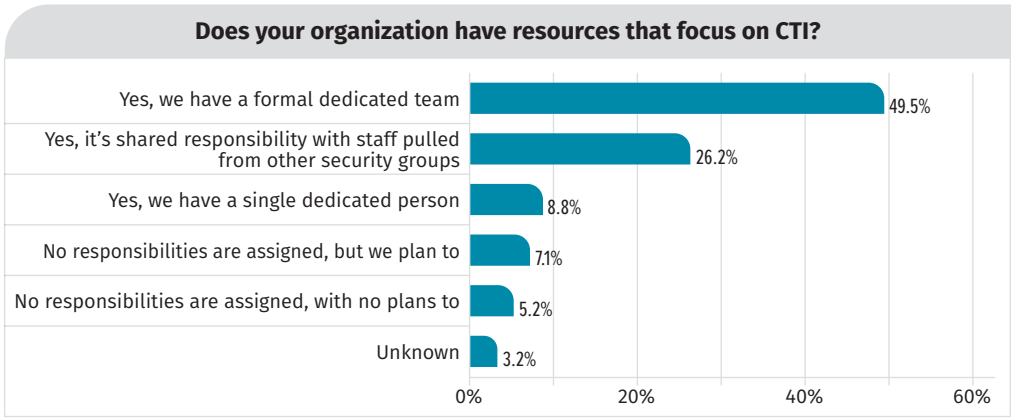



*Figure 2. Allocation of CTI Resources*

Another way to address the need for skilled analysts is to work with external partners to handle or support an organization's CTI functionality. In the past year, more organizations have chosen to partner with external resources, with 61% of respondents reporting that CTI tasks are handled by a combination of in-house and service provider teams, up from 54% in 2019.[4] The number of teams relying solely on service providers has remained relatively consistent, with 8% in 2019 and 7% in 2020.

Some respondents provided additional insight into the collaboration supporting their organization's CTI programs, for example the handling of network defense in-house, indicating that other CTI tasks such as data collection and providing threat assessments might be handled by external partners. One respondent reported that while their primary role is a threat intelligence service provider who supported other organizations, they still have relationships with external partners of their own. In some situations, an organization is limited in the amount of information it can share with external partners, such as with some government-sector respondents, but even in those cases, relationships with external partners can still be beneficial by providing insight into what other organizations are seeing or trends that may become significant down the road.

Now that we see the highest reported number of dedicated threat intelligence teams in respondent organizations, it is helpful to understand how these teams are structured. In the 2020 survey, respondents reported a mix of security operations center (SOC) and incident response (IR) personnel, as illustrated in Figure 3.

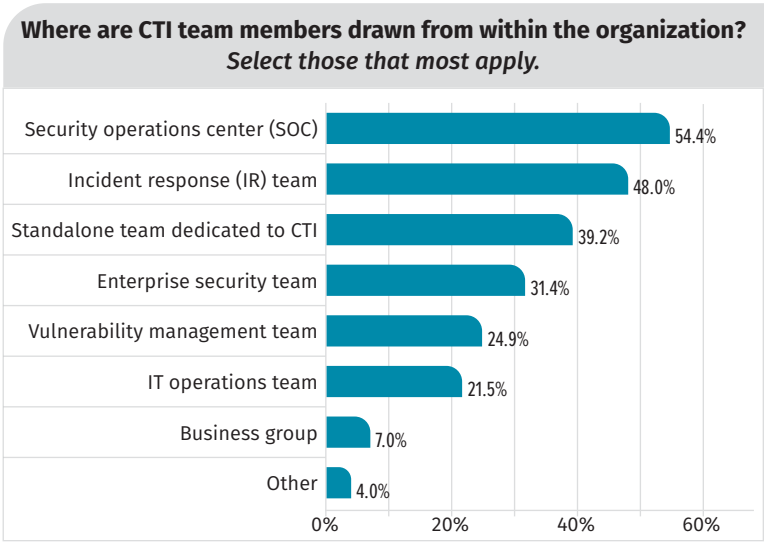



*Figure 3. CTI Team Composition*

[4] "The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey," February 2019, www.sans.org/reading-room/whitepapers/analyst/evolution-cyber-threat-intelligence-cti-2019-cti-survey-38790, p. 8. [Registration required.]

These skills are all extremely useful to an organization's threat intelligence capabilities, as both incident triage and in-depth IR of internal events are critical to understanding the threats that an organization faces. In the past, we have seen similar numbers of SOC and IR resources as part of CTI teams; however this year's respondents reported having a higher number of dedicated threat intelligence analysts as part of their teams. Respondents also indicated a high level of cross-functional collaboration between security teams in their organizations, writing that their CTI team is part of a "purple team" or a "fusion cell" focusing on security. In addition, some of the responses make it clear that there is not, and will likely never be, a one-size-fits-all approach to CTI teams, adding their own categories of personnel including finance, digital crimes and security strategy teams.

*With more people and more teams working collaboratively, it is even more important to have the right processes and tools in place to support CTI efforts.*

This year's survey responses are very promising for the continued evolution of CTI as a critical security function. Not only were there more people responding to the survey in general, but respondents are reporting more personnel dedicated to CTI functions while maintaining and even improving collaboration with both internal and external teams. With more people and more teams working collaboratively, it is even more important to have the right processes and tools in place to support CTI efforts.

## CTI Tools

Threat intelligence is the result of the aggregation and analysis of data related to the intent, opportunity and capabilities of adversaries. Getting the right data to the right places for analysis is crucial to the process. While there will always be some level of human analysis in the overall intelligence process, the goal is to allow CTI analysts to spend their time on the things requiring their expert judgment, and take the manual work out of the processes that don't. This year, we saw a small decrease in the number of respondents reporting manual efforts in some key areas, but there was still a fair amount of "sad-face emojis" in the comments when asked about manual processes.

For the survey, we have broken CTI tools into two functional groupings: tools for *processing* data and turning it into intelligence, and tools for *managing* intelligence including generating alerts based on intelligence.

### Processing Tools

Data must be processed before it can be analyzed and turned into intelligence. Processing includes repeatable tasks such as deduplication of data, data enrichment and data standardization, along with other more intensive tasks requiring analysis of their own, such as reverse engineering of malware. Most organizations report that processing is either a manual or semi-automated process. Deduplication is the most commonly automated process, with only 27% of organizations reporting manual deduplication of data. Reverse engineering of samples is the least automated process, with 48% reporting manual efforts for this task, up slightly from last year. This trend is evident with regard to management tools, where forensics platforms have the second lowest level of automation and the highest level of disparate use, meaning that when they are used in a CTI function analysts must manually initiate the transfer of data or manually input data from one system to another.

Respondents did not report a high level of change in processing capabilities between 2019 and 2020. The majority of processing tasks are done either manually or are semi-automated. One area where we saw automation improvement in is the enrichment of data. Manual enrichment of information using internal data sources is down by 5% balanced by a slight increase in semi-automated and fully automated processes. Enrichment of information using external public data sources and using semi-automated methods increased by 5% from 2019. Interestingly, reporting of fully automated processing remained the same or decreased slightly with the exception of enrichment of internal data, suggesting an interesting concept in an industry where complete automation is often the end goal. Because data processing is such a critical step in the analytic process, it appears that analysts are reluctant to trust this step entirely to automated processes, staying true to somewhat ironic phrase "trust but verify." Streamlining the verification process might result in more semi-automated processes versus fully automated processes, but may be just what analysts need to support their work.

## Management Tools

In the 2020 CTI Survey, respondents report that Security Information and Event Management (SIEM) platforms, network traffic monitoring tools and intrusion monitoring platforms are the most heavily used tools. Of this, SIEM platforms have the highest reported level of use (86.9%) as well as the highest use of automation. Most other management tools, including network traffic monitoring, intrusion analysis and forensics platforms are reported as having some automation, with the exception of spreadsheets and emails, which are mostly processed manually. Despite the lack of automated or semi-automated processes, spreadsheets and emails remain one of the top management tools for CTI analysts. See Figure 4.

**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 disparately or work together under a unified GUI.***

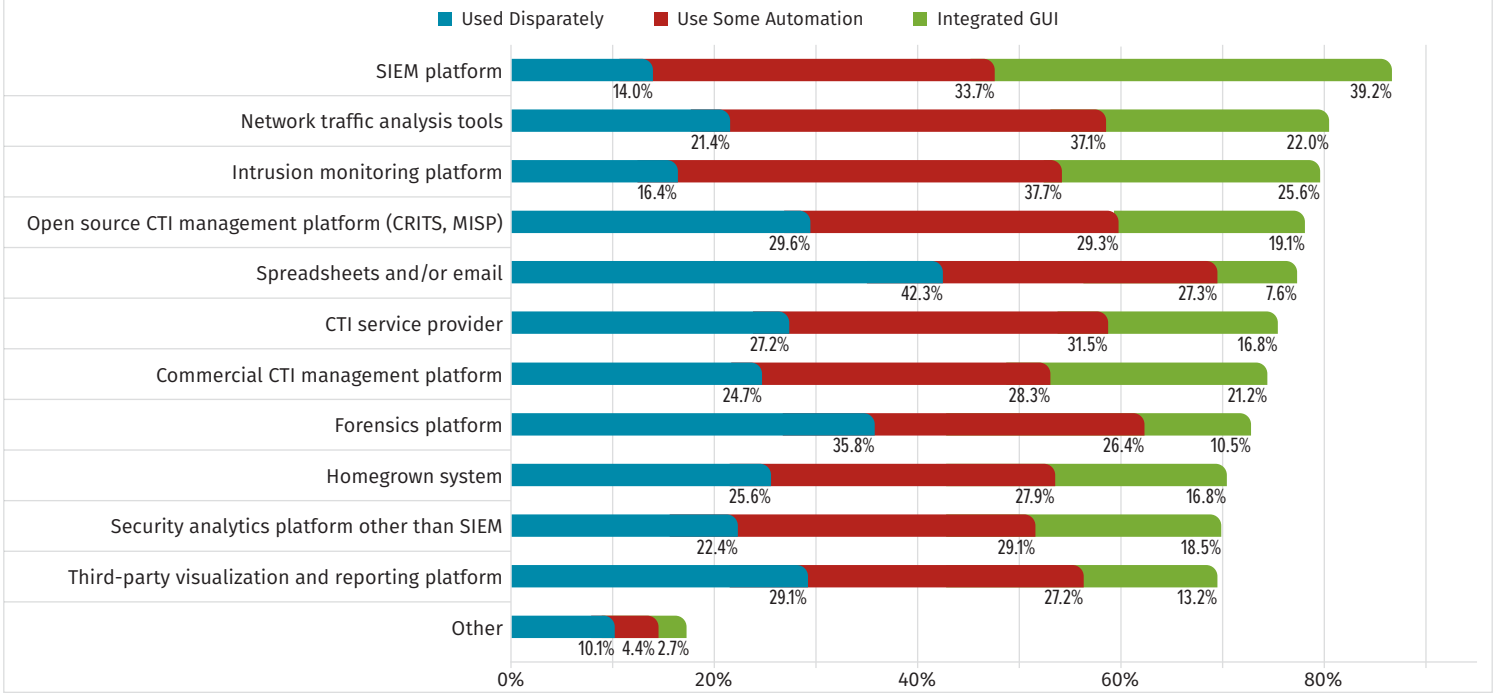



*Figure 4. CTI Management Tool Usage*

Over the years, respondents have consistently listed spreadsheets as a CTI tool for both management and processing. In addition to allowing data to be stored and shared, many spreadsheet applications have built-in functionality that supports processing such as sorting, deduplication and converting the data into various visual formats. Many dedicated CTI tool developers understand that spreadsheets are familiar and functional for analysts and have built them into their own processes. Most data in CTI tools can be exported and imported into .csv format, and some SIEM tools allow users to build automated tasks around data in spreadsheets. These additions will help overcome some of the shortcomings of working with spreadsheets, such as getting consistent data to different users within the same team, which is even more important now that there are more dedicated CTI teams as opposed to standalone analysts.

### TAKEAWAYS

- **More organizations are investing in dedicated CTI teams versus individual analysts or fully outsourced functionalities.** These teams will enable organizations to better understand and address the threats they face. Many organizations just beginning to build out their teams still need to focus not only on training of CTI skills, but also on collaboration and teamwork skills to work with internal and external partners, which are critical for a CTI team.
- **We see less full automation and more semi-automation in CTI processing tools.** While we see more automation in the management of CTI, especially when it comes to the use of tools such as SIEMs and network management tools, respondents report less full automation and more semi-automation in CTI processing tools. While manual processes are often a hindrance to analysis, semi-automation may be the most beneficial for analysts, taking away some of the most tedious aspects of a task, but still providing analysts with a level of control and transparency that gives them confidence in their processes.

## CTI Processes: The Intelligence Cycle

The CTI community and many organizations both produce and consume intelligence. Over the years, more and more organizations report that they are producing and consuming data, with a 10% increase from 2019 in those that both produce and consume raw threat data and a nearly 7% increase in those who both produce and consume alerts with contextual data as well as published threat reports. Of the three categories of CTI, we see only published threat intelligence with more sole consumers, with 55% consuming this type of intelligence without producing it (see Figure 5).

Regardless of whether an organization produces and/or consumes intelligence, a process is required to move from identification of what questions must be answered using threat intelligence to actions benefitting an organization's defenses. For many organizations, that process is a version of the classic intelligence cycle.

The intelligence cycle is a process for generating accurate, useable intelligence. It begins with a planning phase, in which the intelligence questions that must be answered (also known as "*requirements*") are generated. When the

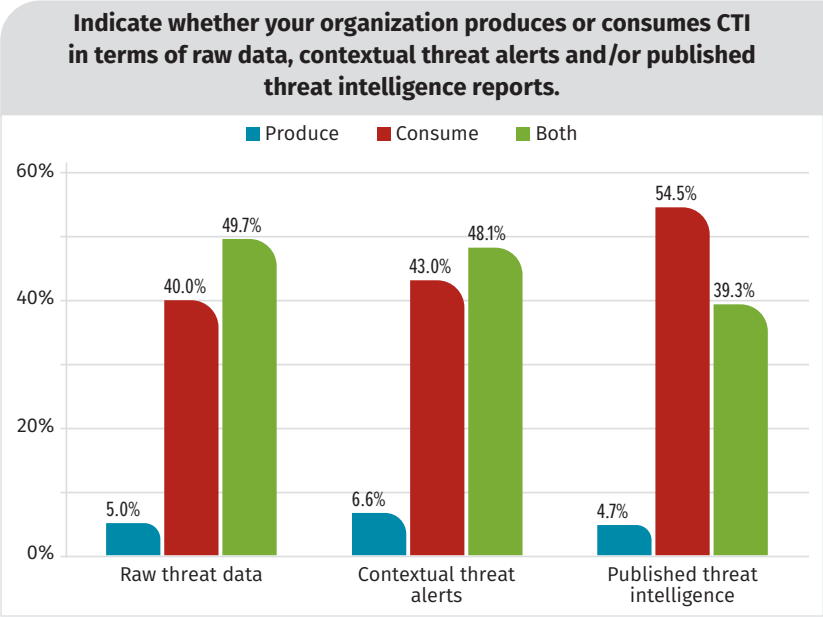



*Figure 5. CTI Production and Consumption by Type*

requirements are known, the next phase is *collection*, gathering data to help answer the questions and meet the requirements. The next phase is *processing*, where the data is put into a usable format for analysis. This leads into the fourth phase, *analysis*, in which the data is synthesized to identify the answers to the intelligence requirements. The last phase is *dissemination*, where the findings are captured in the right format to reach the intended audience outlined in the planning phase. It is important to note that while the intelligence cycle is a cyclical process, it is sometimes necessary to go backward in the process; for example if, during the analysis phase it is determined that additional information is needed or information must be processed in a different format, it is important to go back to the appropriate earlier step so that the end result is an informed, accurate analytic finding. See Figure 6.


*Figure 6. The Intelligence Cycle*

This year's survey shows that more organizations are following the steps of the intelligence cycle either intentionally or intuitively. In the 2020 survey, we covered three critical processes from the intelligence cycle: requirements, collection and dissemination.

## Requirements

The 2019 CTI Survey was the first year that we looked into the development and use of requirements to drive threat intelligence programs, an area that has seen incredible growth in the past year. Requirements seek to identify what specific questions or concerns must be addressed by a threat intelligence program. The number of organizations reporting a formal process for gathering requirements increased 13% from last year to almost 44% (see Table 1).

**Table 1. Defining CTI Requirements (Year over Year)**

| | 2020 | 2019 | Trend |
|---|---|---|---|
| Yes, we have documented intelligence requirements. | 43.8% | 30.3% | 13.5% |
| No, our requirements are ad hoc. | 29.7% | 37.0% | -7.3% |
| No, but we plan to define them. | 20.4% | 26.0% | -5.6% |
| No, we have no plans to formalize requirements. | 6.1% | 6.7% | -0.6% |

Also positive news: Those contributing to CTI requirements increased across the board, with respondents reporting more input from teams including security operations, IR and business units. In fact, security operations had more input than the CTI teams this year, indicating that operations are beginning to drive intelligence for the first time reported. See Figure 7.

**If you have CTI requirements, who contributes to them?**
***Select all that apply.***

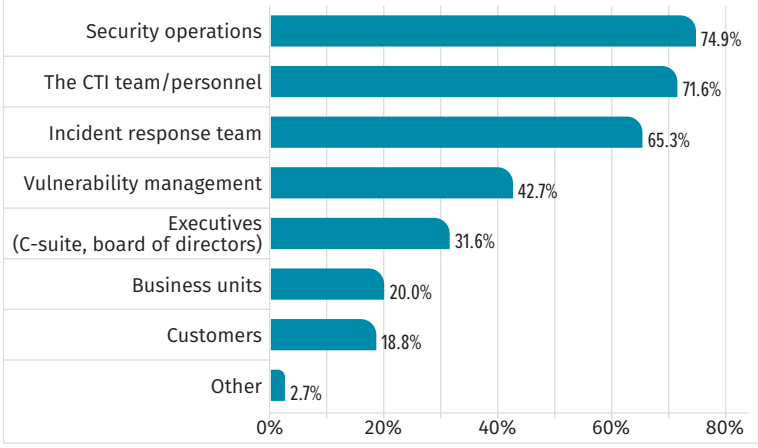



*Figure 7. CTI Requirements Contributors*

Respondents report that requirements are primarily updated in an ad hoc manner rather than on a scheduled (yearly, monthly or weekly) basis. But the good news is that only 5% of respondents say they don't update requirements at all (see Figure 8). While there are some consistent themes in requirements across the board, many are unique to a specific organization or are based on past incidents or upcoming significant events for the organization.

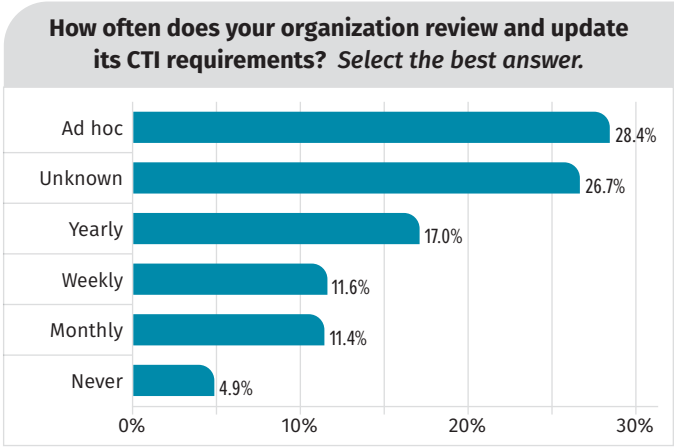



*Figure 8. Reviewing and Updating CTI Requirements*

Examples of requirements from respondents include:

- The activity of a specific adversary [with whom] we had security incidents in the past, CTI team is tasked to monitor for new reported activity as well as profile the observed TTPs of this adversary
- Consistently analyze and prioritize counter "Business email compromise" activity to protect our agent population from targeted attacks
- Brand surveillance, supply chain and partner assessments

While there was a huge jump in organizations reporting development of requirements, over half of respondents still do not have a process for identifying requirements, which will help organizations be successful whether they produce or consume intelligence. Not having requirements or not having a process for evaluating and prioritizing new requirements can become a serious roadblock for many teams.

## Collection

After identifying requirements, the next step is to identify how to get access to the information that will help answer the requirements. For respondents who consume intelligence, this means evaluating sources of intelligence that will be easy to operationalize. Nearly 70% of respondents gather some of their information from a commercial threat feed, from both CTI-specific and general security vendors, with over 45% consuming non-feed information from a CTI service provider (see Figure 9). When it

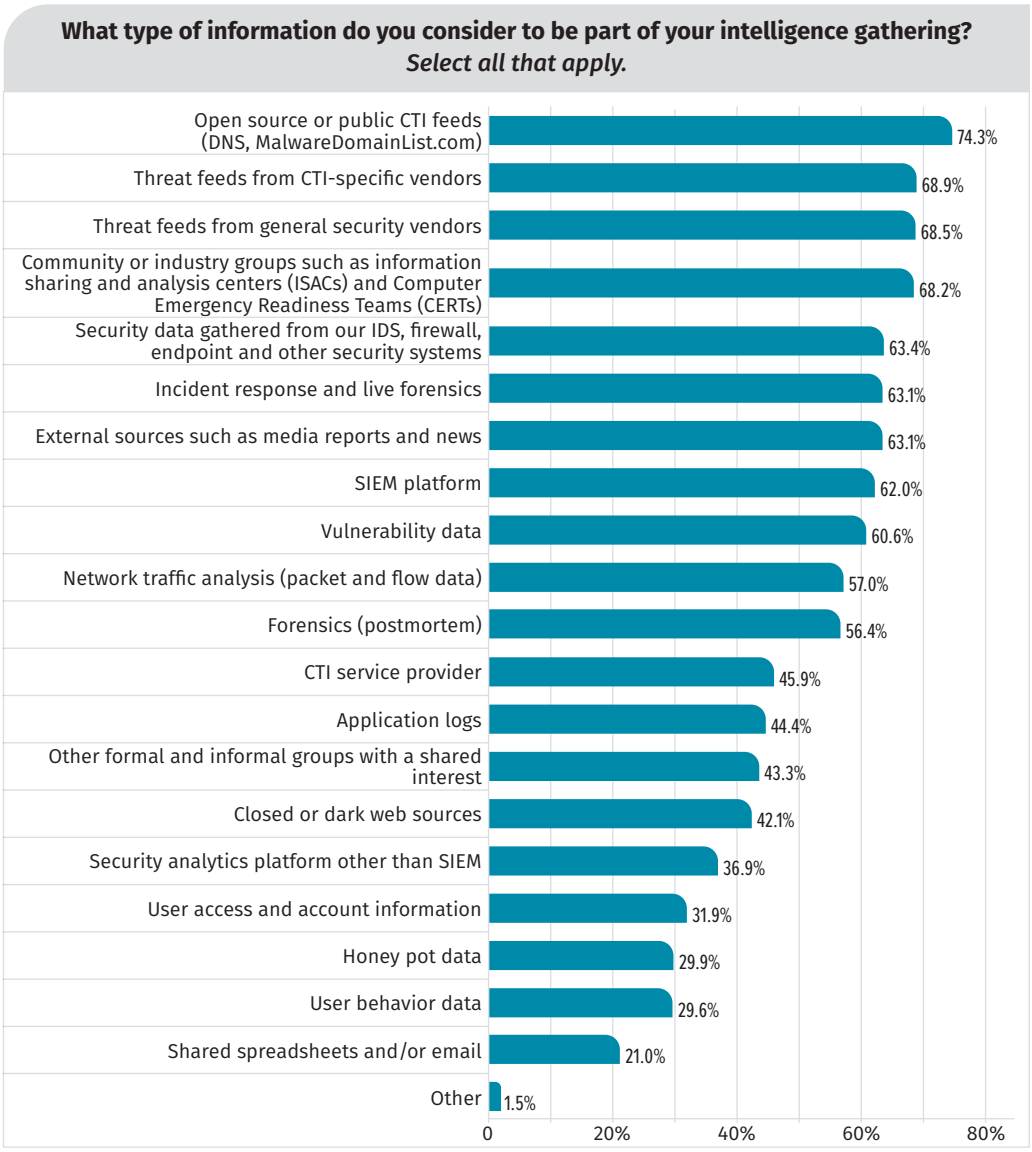



*Figure 9. Intelligence Types*

comes to consuming intelligence, timeliness and relevance are once again at the top of the list of important factors, but more and more respondents are considering how that information will be consumed as well as the content. This year, several respondents identified standardization with the Mitre's ATT&CK Matrix framework as a priority for information they consume.

Producing intelligence involves the addition of other sources of data, most of which haven't yet been processed or analyzed. These data sources include network traffic logs, vulnerability data, user behavior data and security data gathered from IDS, SIEMs and other internal security systems. A hybrid form of data also exists, for example information about a previous incident that has already been processed and analyzed in an IR context and will now be used to answer CTI requirements.

Most respondents collect data from a variety of sources. This year we saw a significant increase in several types of intelligence collection from last year, including threat feeds from CTI-specific vendors, open-source threat feeds and forensics data (see Table 2). This increase in information gathering corresponds to the increase in the number of respondents who both consume and produce intelligence.

**Table 2. Sources for Gathering Intelligence**

| | 2020 | 2019 | Trend |
|---|---|---|---|
| Open source or public CTI feeds (DNS, MalwareDomainList.com) | 74.3% | 66.2% | 8.1% |
| Threat feeds from CTI-specific vendors | 68.9% | 59.8% | 9.1% |
| Threat feeds from general security vendors | 68.5% | 63.8% | 4.7% |
| Community or industry groups such as information sharing and analysis centers (ISACs) and Computer Emergency Readiness Teams (CERTs) | 68.2% | 63.4% | 4.7% |
| Security data gathered from our IDS, firewall, endpoint and other security systems | 63.4% | 62.2% | 1.2% |
| External sources such as media reports and news | 63.1% | 63.4% | -0.3% |
| Incident response and live forensics | 63.1% | 55.3% | 7.8% |
| SIEM platform | 62.0% | 59.2% | 2.8% |
| Vulnerability data | 60.6% | 58.6% | 2.0% |
| Network traffic analysis (packet and flow data) | 57.0% | 53.2% | 3.8% |
| Forensics (postmortem) | 56.4% | 48.3% | 8.0% |
| CTI service provider | 45.9% | 42.6% | 3.3% |
| Application logs | 44.4% | 43.2% | 1.2% |
| Other formal and informal groups with a shared interest | 43.3% | 39.6% | 3.8% |
| Closed or dark web sources | 42.1% | 39.9% | 2.2% |
| Security analytics platform other than SIEM | 36.9% | 36.9% | 0.1% |
| User access and account information | 31.9% | 34.1% | -2.3% |
| Honey pot data | 29.9% | 29.3% | 0.5% |
| User behavior data | 29.6% | 30.5% | -1.0% |
| Shared spreadsheets and/or email | 21.0% | 25.1% | -4.1% |
| Other | 1.5% | 1.8% | -0.3% |

One interesting trend in the information from respondents is an increased interest in open source threat intelligence in regard to both data and tools. There was an 8% increase in respondents reporting the use of open source threat feeds as a collection source and a 14% increase in the use of open source threat intelligence management tools such as Collaborative Research Into Threats (CRITs) and Malware Information Sharing Platform (MISP). One respondent wrote that their organization is using MISP more heavily now that there is an increased emphasis on attacker TTPs rather than just IoC aggregation. Although we did not ask specifically about Mitre's ATT&CK Matrix framework in the 2020 survey, several respondents wrote in that their organizations have had success, particularly in adding contextual information to alerts and in prioritizing responses, by leveraging it.

Information gathering goes hand in hand with requirements in that requirements dictate what information the organization needs to collect. Although there are far fewer examples this year of organizations gathering information they don't need, some respondents still report their organizations spend money on data that they do not need or are unable to utilize. Just as with requirements, information should also periodically be evaluated to ensure that it is effective and usable. A data source that may have been critical in the past might no longer be needed, and new data sources might need to be identified as the organization and the threat landscape change.

## Dissemination

In order for intelligence to be effective, it must get to the right audience in a way they are able to use it. The process of getting intelligence to its intended audience is called *dissemination*. CTI is primarily disseminated in the form of reports or briefings that summarize a particular threat or is disseminated to tools used to generate alerts or inform other security teams in an automated fashion. The majority of respondents use methods meant to disseminate intelligence to people, such as email, spreadsheets or PowerPoint presentations. For many, this is done on a regular basis such as weekly threat reports, daily email-based briefs to other security teams or newsletters for general employee awareness. Briefings are also high on the list of ways to disseminate CTI, with respondents reporting regularly scheduled briefings as well as briefings for urgent issues, such as identifying when their organization has been targeted. See Figure 10.

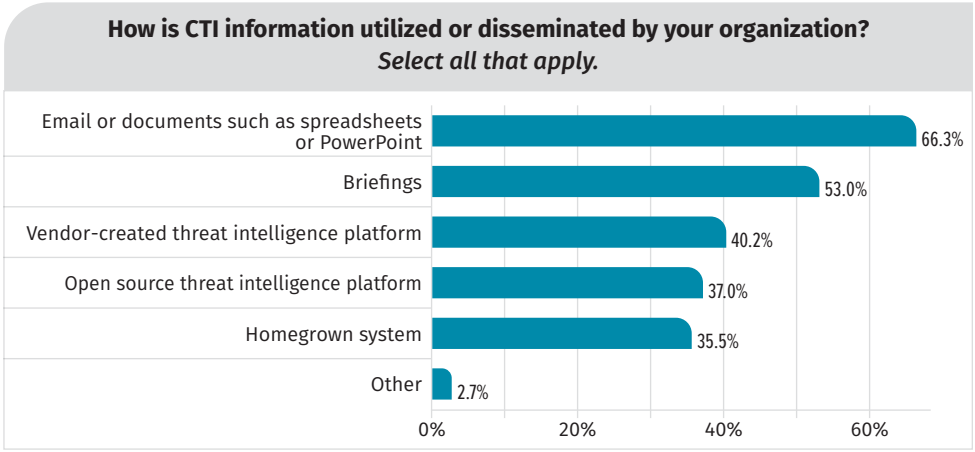



*Figure 10. Methods of Disseminating CTI Information*

When it comes to intelligence meant to be understood by others in the organization, a high degree of personalization based on the audience's preferences is needed. As one respondent put it, "Intelligence needs to be dissected before reaching different business units so it can be actionable." Finance will need a slightly different version of a brief that focuses on their specific business concerns than will the team responsible for brand protection, for example.

Intelligence is also disseminated to tools used for alerting. Most organizations rely on a threat intelligence platform for this purpose. Respondents report a similar number of organizations using open source, vendor-created or homegrown threat intelligence platforms to disseminate intelligence to other security systems. While the percentage of respondents using vendor platforms has been consistent in the past two years, the use of open source and homegrown systems has increased.

### TAKEAWAYS

- The development of CTI requirements is the first phase of the intelligence cycle and will help an organization ensure that the work being done meets the needs of their security program. More organizations are developing requirements, but the organizations that have not yet formalized this process can start by identifying the teams who leverage CTI and asking what questions they have or what problems they are consistently running into that CTI could help address.
- Although CTI data can come from a variety of sources, leveraging a framework such as Mitre's ATT&CK Matrix framework during the processing phase can help analysts identify trends and make connections between the different sources.
- Even the best-analyzed CTI products become ineffective if they don't reach the right audience in a timely manner. With more organizations producing their own intelligence, it is critical to make sure the audience—and the way they best consume intelligence—is taken into consideration before dissemination.

# Value and Inhibitors of CTI

Respondents noted they are using CTI across the spectrum of detection, response, prevention and mitigation.

## CTI Uses and Use Cases

At a high level, the leading use was for threat detection (89%), followed by threat prevention (77%), threat response (72%) and threat mitigation (59%). Organizations focusing too heavily on threat prevention often struggle with detection and response, which would otherwise be core to their ability to maintain great prevention over time. It's clear from this year's survey data that many organizations, at least where CTI is involved, have seen detection as the primary value driver. See Figure 11.

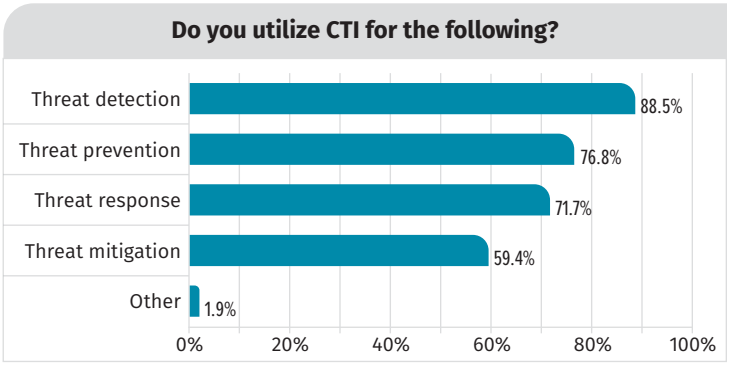



*Figure 11. CTI Detection, Response, Prevention and Mitigation*

The detection and response use cases deemed most valuable in weighted analysis order were IoCs, threat behaviors and adversary TTPs, digital footprint or attack surface identification, and strategic analysis of the adversary, respectively. Figure 12 illustrates the raw rankings of each in terms value to organizations. While IoCs still seem to reign as a major value add to programs, there has been a growing focus on TTPs in organizations. As organizations have the proper tooling to leverage TTPs more effectively, they will likely edge out IoCs as a primary detection mechanism.

Combining TTPs and IoCs can form a powerful detection and response strategy. Instead of running IoCs over every piece of data and thus increasing false positives, consider leveraging TTPs as a primary detection strategy and then running the associated IoCs against the subset of detections based off of TTPs. As an example, running indicators associated with VPNs against all network traffic would yield a higher level of false positives than running those same indicators against only network traffic that alerted against TTP-based detections associated with malicious use of VPNs. This allows analysts to have a more transposable and durable detection strategy with TTPs, but still gain the value and context associated with IoCs. Additionally, IoCs remain a highly effective mechanism for scoping environments once a threat is detected. Here, teams will excel at response when they prioritize their own IoCs observed in the detection stage.

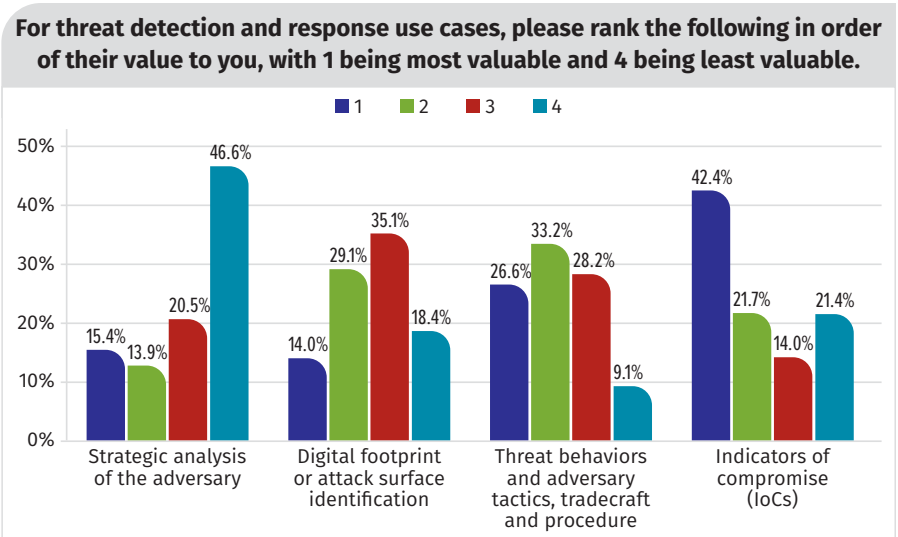



*Figure 12. Threat Detection and Response Value*

## Measuring Effectiveness and the Value of CTI

One obviously difficult area for organizations every year is measuring the effectiveness of cyber threat intelligence. The message is clear: 82% of respondents' organizations find value in it, with 17% not being sure of how to answer and fewer than 1% of respondents noting that CTI did not improve their security and response efforts. But measuring exactly what value it is bringing in a structured and defined way is understandably difficult. Only 4% of respondents had processes in place to measure effectiveness (see Figure 13). There is no one-size-fits-all strategy to measuring intelligence, but it must start with the intelligence requirements phase. Organizations with clearly defined intelligence requirements can use those requirements to set obtainable goals based on the intent behind the requirement. When looking at security and response use cases, these measurements can be mapped to overall defender-based metrics instead of simply tracking adversary metrics.

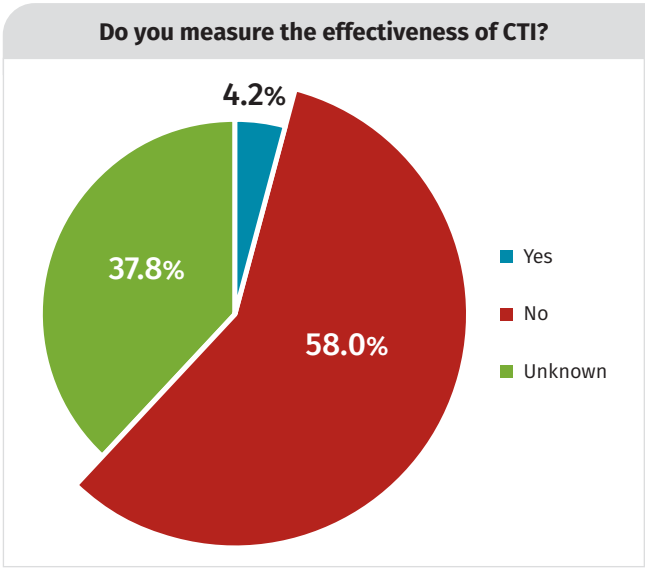



*Figure 13. Measuring CTI's Effectiveness*

Adversary metrics are those metrics that the adversary controls. As an example, if you were to track the number of intrusions you see per year, that metric would be influenced by two things: how often an adversary targets your network and how often you detect the intrusion. Of those two, the defender can only control how often they detect the intrusion. The adversary alone determines how often and how aggressively they target any given organization. Reporting only on adversary metrics can tell a misleading story that is difficult for CTI teams to understand. Instead, consider what story you can tell with defender-based metrics. For example, against the known threats that you track and your coverage against the TTPs they've shown. Historically, are you increasing the analytical breadth (coverage) and analytical depth (multiple detections for a single TTP) of your detections against the threats? How many IR playbooks has the CTI team contributed to based on their insights? How long did it previously take to scope your organization and with what level of visibility versus what you can to today based on investments in people, process and technology across the organization? These are all defender-based metrics, because you can directly influence them and use them to tell your story more than the adversary's. Measurements are not only done in metrics, but the right metrics can tell a powerful story or identify issues to correct.

## Inhibitors Holding Programs Back

There are many reasons CTI teams can struggle, including those beyond their control such as management support or company resources. Sometimes it can also just be difficult to get started. When asked about the biggest inhibitors, it was clear the focus was on people and processes. The leading issue at 57% was the lack of trained staff and skills associated with fully utilizing CTI. The next leading issue at 52% was the time to implement proper intelligence processes across the team. Interestingly, the lowest issue,

selected by 23%, was confidence in using the information to make decisions (see Figure 14). CTI practitioners and the teams using threat intelligence seem to clearly understand how to use it to support them and understand its value but are stretched thin on finding the appropriate talent. It was good to see that only a minority suffered from lack of management buy-in as well, which appears to note that the value propositions of CTI are well understood in most organizations at a variety of levels.


*Figure 14. CTI Inhibitors*

Participants were asked about their level of satisfaction with various aspects of CTI. The highest level of satisfaction for respondents was their ability to have visibility into threats (75%), search and report on those threats (73%) and have relevant threat data and information (72%). Automation and integration of CTI information through respondents' tooling still scored well (61%), but the lowest rated area was machine learning with 36% satisfaction and 58% outright dissatisfaction in the effectiveness or value of it. Tools can add a lot of value for intelligence analysis, but the process is heavily dependent on analysts.

## Sharing Is Caring

Randomly sharing IoCs by plugging in threat feeds can lead to more harm than good. The CTI community has become more regimented about how it uses intelligence, and while IoCs are still of great value, most organizations have become more thoughtful in how they source this data. This much is clear: Sharing and networking are still core components of success for the community. Information Sharing and Analysis Centers (ISACs) are not available to all respondents, although there was great global distribution in the home country of participants in the survey. And yet 45% still answered that they are members of an ISAC (see Figure 15). The biggest inhibitors based on comments was the cost of some of the ISACs' membership dues.

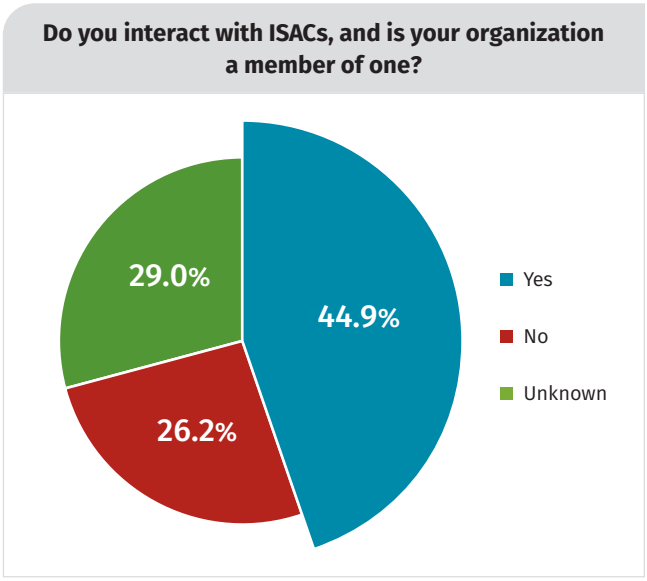



*Figure 15. ISAC Membership Rates*

Respondents belonging to an ISAC noted value across a couple of key areas: 73% noted they did get some timely and relevant threat information from ISACs. Based on the data and comments, it was clear that a major value in the ISACs was gaining points of contact at member organizations (68%), advocacy in the community (44%) and the membership meetups (43%). See Figure 16.

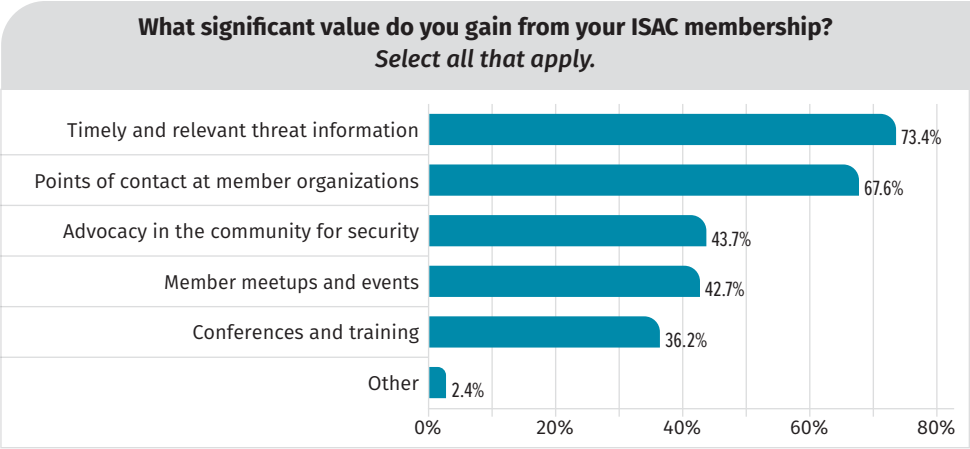



*Figure 16. Value of ISAC Membership*

As organizations mature, it is a common complaint that ISACs for threat information become less valuable. However, this simply means the organizations are outgrowing the perceived effectiveness, which is an overall good thing. In those cases, points of contact at other organizations become invaluable for going beyond the immediate sharing of available information and analysis on emerging threats and trends.

Whereas ISACs received high marks, there was a bit less consensus on the role and value of government in CTI. See Figure 17.

Written comments called out some specific organizations positively, such as the UK's NCSC. Overall though, only 47% of organizations thought government provided something significant or unique in value over what they were getting elsewhere. In many cases, the role of government is less about providing insights that differ from those emerging from the private sector (which largely has the expertise to generate those insights), but instead around the amplification of which threats the government thinks matter the most. Similar to the value propositions of the ISACs for more mature organizations, as the industry matures, the government should likely seek to take a role of empowering ISACs and adding additional amplification and context around known public threats in a wider forum.

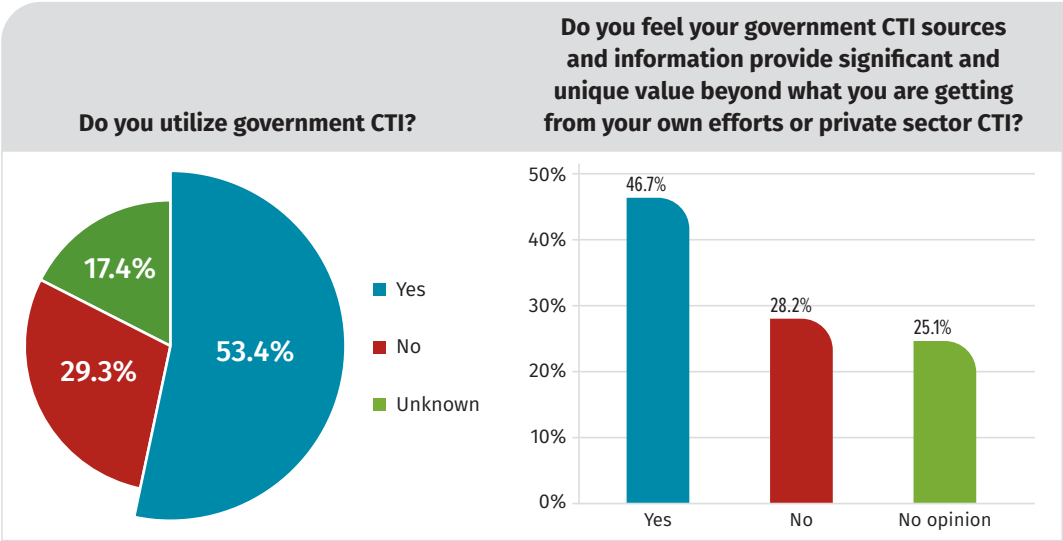



*Figure 17. Government CTI Usage*

# Conclusion: Keep Moving Forward

A lot of progress has been made in the past few years around requirements. Next steps in this area include identifying when and why to update intelligence requirements—even ad hoc adjustments can be planned for by identifying the circumstances under which they would need to be changed. It is also clear that there are numerous positive trends in the community, such as more organizations producing intelligence instead of just consuming it. But there are also many challenges, such as getting the appropriate staffing and training to conduct cyber threat intelligence. Tools and data sources are always going to be vital to the process, but the world of intelligence analysis is inherently analyst-driven and a focus is rightfully placed there.

Sharing not only IoCs and adversary TTPs, but also processes and analytic processes, will help the community continue to mature. Some processes to share include strategies for measuring the effectiveness of a CTI program. These metrics should be based on requirements and should be defender-based metrics—for example, how long did it previously take to scope your organization and with what level of visibility vs. what you can to today based on investments in people, process and technology across the organization? While the specific metrics will likely differ from organization to organization, the processes can be developed leveraging shared best practices and ideally can be built into tools in the future, both commercial and open-source, making the process timely, effective and repeatable.

### Takeaway

In the coming year, get more involved in the community and find the best practices from other organizations, especially around intelligence requirements and analyst development. With many changes in the world in the coming year, from political elections and global trade tensions, to natural disasters with unknown consequences, CTI analysts will likely be asked to focus on new and unanticipated threats. Being part of a community of intelligence analysts sharing threat data, best practices and lessons learned will help everyone adapt to rapidly changing situations and provide intelligence to protect critical networks.

## About the Author

**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.

## Sponsor

**SANS would like to thank this survey's sponsor:**