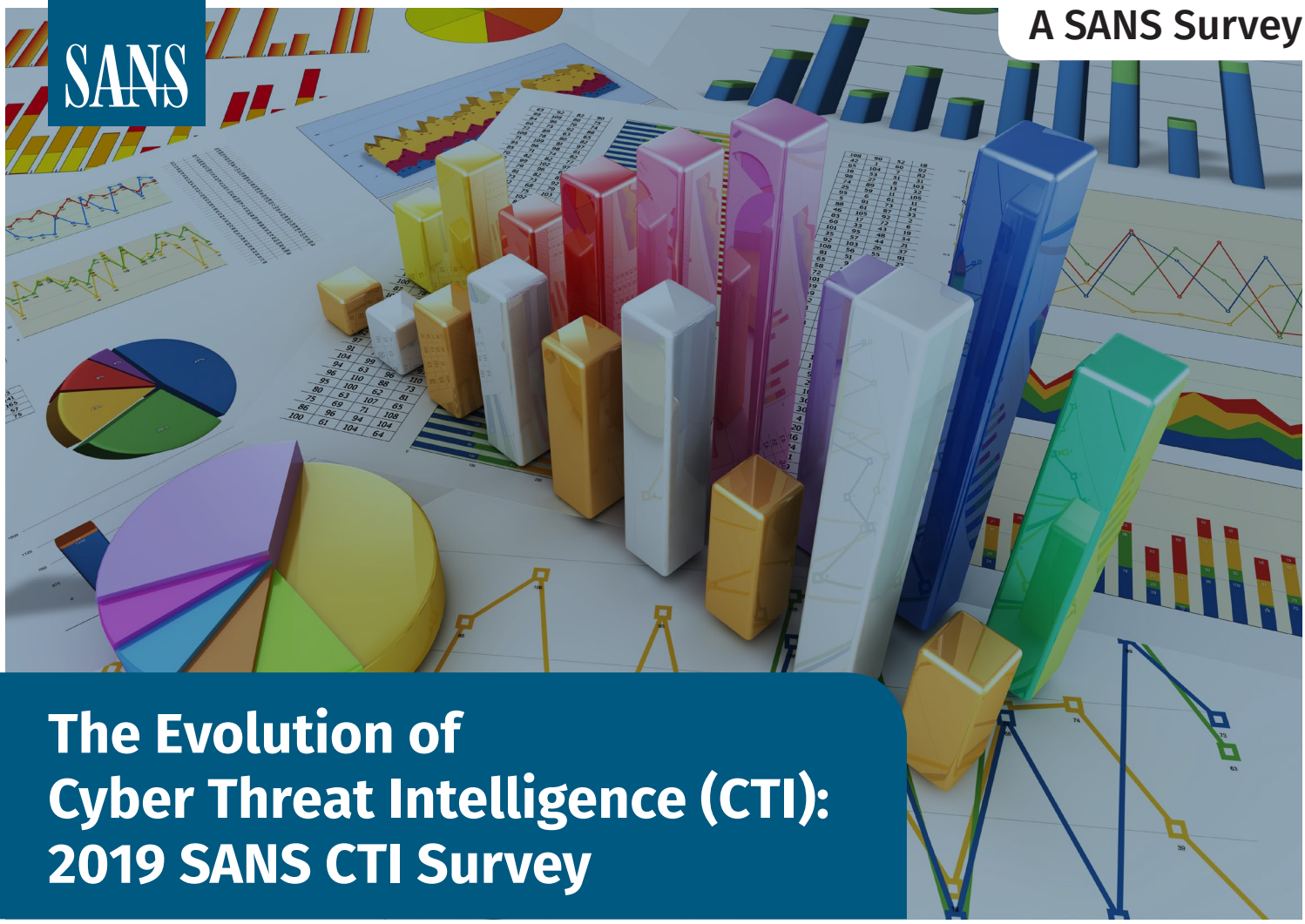
SANS

A SANS Survey



The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey

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

February 2019

Sponsored by:
Anomali

SANS Analyst Program

Executive Summary

Cyber threat intelligence (CTI) analyzes information about the intent, capabilities and opportunities of adversaries in cyberspace, making it a valuable resource for organizations as well as individuals serving in roles such as network architects, security operations team members, incident responders and high-level decision makers, all of whom must be prepared for the wide range of threats challenging their organizations. SANS has been tracking the evolution of CTI as a mechanism for prevention, detection and response through seven CTI summits and five surveys, and has seen a gradual maturation of the field and its applications in information security.

This year's survey saw an increase in usage and interest in CTI, along with a diversification in how the intelligence is being used by organizations. While the use of CTI continues to grow, there is no one-size-fits-all approach. Organizations leverage different types of CTI to meet different needs. This survey focuses on how and why CTI is being used, how it is helping defenders, what data sources are being leveraged, and how data is converted into usable intelligence.

Key Takeaways

The use of CTI as a resource for network defense is growing, with 72% of respondents' organizations producing or consuming CTI, compared with 60% in 2017.[1] **A diversification in use cases for CTI, along with a better understanding of how it's used to benefit an organization's security posture, means that CTI is being more widely utilized by both large and small organizations.**

More organizations are consuming CTI, especially in the form of finalized intelligence reports, and integrating them into their defensive mechanisms. **Operationalizing narrative-based intelligence reports—reports that describe in detail a series of events related to an intrusion or incident—is time-consuming for CTI analysts. A lack of automation for these reports makes them especially time-consuming. CTI teams need to ensure that they are properly staffed and allocating enough time to make the best use of this type of reporting.**

The more specific intelligence is, the better. Respondents report that intelligence on the general threat landscape is useful, but not as useful as intelligence specific to their industry, their brand and even their executives. **While it is important to track and defend against widespread, nontargeted threats, much of CTI's value comes from its capability to provide an awareness of and mitigation for organization-specific threats.**

Information-sharing programs have value beyond just the information that is being shared. Benefits such as point-of-contacts, advocacy for security and best practices are also tangible benefits of participation in an information-sharing group. **With the number of options available for collaborating and sharing, including government-sponsored groups, private sector groups and industry-focused groups (both formal**

[1] "Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey," March 2017, www.sans.org/reading-room/whitepapers/analyst/cyber-threat-intelligence-uses-successes-failures-2017-cti-survey-37677, p. 1. [Registration required.]

and informal), it should not be difficult to find a sharing partnership that will benefit your organization.

While progress has been made on system integration and interoperability, more automation and machine learning capabilities would be useful, **which would allow organizations to better allocate resources and give analysts more time to focus on analysis and dissemination of intelligence, rather than on collection and processing of data.**

Survey Respondents and Demographics

This year's survey received 585 responses across a wide variety of industries. The first important takeaway is that the CTI community is growing and diversifying, which will yield new insights into different types of threats and their behaviors. The largest portion of respondents came from cybersecurity service providers (16%), banking and finance (15%), government (14%) and technology (11%). These are some of the normal respondents seen in these surveys, but there was an uptick in healthcare, manufacturing and electric industry participation this year. Least-represented were the media, pharmaceutical and water industries. Identifying and analyzing intrusions to uncover threats is important to understanding the security needs in industries and informing decision makers about what adversary-based risks matter to their organization; the underrepresentation in some industries might be a sampling bias, but also could represent a gap in insights in those industries.

In 2019, SANS finds that the CTI community is growing and diversifying, which will yield new insights into different types of threats and their behaviors.

When survey participants were asked about the size of their organizations (from less than 100 to more than 100,000), there was a fairly even distribution, potentially hinting at the perceived importance of CTI across companies of all sizes. Surprisingly, security operations analysts were the most common respondents (23%), followed by CTI analysts (10%). The rest of the respondents were distributed across roles such as incident response (IR) teams, security architects, threat hunters and security administrators.

Value of CTI

One of the most important tasks that analysts have is being honest with themselves and their organizations about the value they are delivering. Security can be hard to measure objectively, but even subjectively measuring value can offer some insight into an organization's culture around security. The survey asked respondents whether their use of CTI had improved their security and response; 81% of respondents answered positively, while 17% said they did not know. Only 2% of respondents found that CTI was not helpful. See Figure 1.

The 17% who were unsure of CTI's value to their organization, and those who find themselves relating to the unknown nature of its value, should challenge themselves to set forth a set of clear requirements to measure the value for the next year. One recommendation is to consider and measure the average resolution time of security incidents when CTI analysts participate to enrich the understanding of the incident for security operations and incident responders. Another recommendation is building a threat model for the organization, based on active threats in the organization's industry and what types of threat behaviors—tracked using a framework such as MITRE's ATT&CK—have been observed by those threats.[2] Those behaviors, if not currently prevented or detected, can be prioritized across architecture, security operation and response functions.

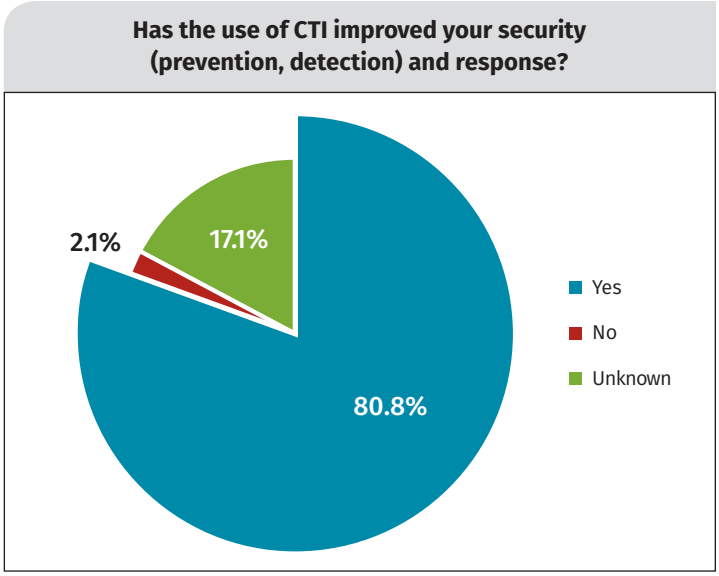


Figure 1. CTI Efficacy

We also wondered about how respondents perceive the value of CTI that comes explicitly from governments and information sharing and analysis centers (ISACs). Only 40% of respondents were participating in their industry's ISAC. Of those who did participate, though, only 5% said they did not gain value, although the ones who did not gain value may significantly make up the portion of respondents who were no longer participating. We asked those who responded positively what the biggest value propositions of the ISACs were. Timely and relevant threat information (69%), points of contact at member organizations (63%), and advocacy in the community for security (49%) were the top three choices of the respondents. ISACs vary widely in their maturity and community engagement across different industries. Often, the financial services ISAC and the electrical ISAC are highlighted positively. Both ISACs are well-known for hosting member meetups, advocating for their members and sharing information widely throughout the groups. These may serve as good models for other ISACs as they continue to grow and engage their communities.

In relation to government CTI, 51% of the participants noted they took advantage of this data source. Given the proliferation and easy access to many sources of government CTI, it is interesting that only 51% of the community is taking advantage of it. The 51% who did take advantage of it revealed though that only 41% of those participants felt they gained significant or unique value beyond what they were getting themselves or from the private sector. This lack of significant value may contribute to the lower-than-anticipated adoption rate across the participants. This was also one of the questions with the most write-in comments from participants (see the "Respondents Speak Out" sidebar).

SANS Recommends

For those who are unsure of CTI's value, create a set of clear requirements for your organization to measure its value against. Consider measuring the average resolution time of security incidents when CTI analysts participate to enrich the understanding of the incident for security operations and incident responders against the average resolution time when CTI analysts do not participate.

[2] https://attack.mitre.org

As the government matures its own understanding of private sector cyber threats, it can better approach the problem by giving additional context and focusing on adversaries' behaviors such as their TTPs, instead of simply relying on indicators of compromise (IoCs), which the private sector has traditionally dominated.

The view on government-provided CTI is mixed, with only a portion of all the respondents participating and finding value. However, as the government matures its own understanding of private sector cyber threats, it can better approach the problem by giving additional context and focusing on adversary behaviors such as their tactics, techniques and procedures (TTPs) instead of simply relying on indicators of compromise (IoCs), which the private sector has traditionally dominated. Particularly important insights to which the government has access often remain classified, whereas most of the incidents that occur (and most of the teams dealing with them) are in the private sector.

Most of the threat intelligence and the expertise developing around it are private sector skills; therefore the results of the respondents should come as no surprise. Yet governments around the world are in a unique position to bring the community together and collaborate across industries to provide value propositions similar to that of the ISACs.

Respondents Speak Out

Some comments specifically about government-distributed CTI information include:

- "FBI alerts are some of the most detailed and reliable reports on adversary groups and their TTPs [tactics, techniques and procedures]."
- "Private sector CTI always comes with a cost, whereas when the government shares CTI, it's free."
- "They [the government] are getting better [at] collaborating with industry."

However, some of the comments indicate that work still needs to be done to improve the nature of government-distributed CTI information:

- "The information is usually very old by the time it's distributed."
- "Government-sourced CTI often fails at being timely and accurate."
- "It took significant time and effort to set up government CTI ingest. But data delivered is the same as with the ISAC. ISAC also delivers additional information on top of government. My preference is to maintain direct government integration with hope that in the future better and unique data will be available."

Indicators, Behaviors, Attack Surface and Strategic Analysis Value

Out of all of the respondents, 86% utilized CTI for threat detection or response in their organizations. The respondents were provided different types of CTI to determine which they leveraged in ranked order. See Figure 2.

As expected, IoCs were the most highly ranked, with 41% of the participants selecting them as the most valuable. It is incredibly common for security organizations to mostly consider intelligence as an indicator feed, although CTI ranges much further than that. Additionally, most of the participants in the survey were security operations analysts, who often view the CTI value proposition as enriching alerts with technical details. The second choice was threat behaviors and adversary TTPs, which 27% of respondents chose as the most valuable. Next was digital footprint or attack surface identification, with 18% selecting it as the most valuable, followed by strategic analysis of the adversary, with 13% selecting it as the most valuable.

For threat detection and response use cases, what is more valuable to you in ranked order: strategic analysis of the adversary; digital footprint or attack surface identification; threat behaviors and adversary tactics, tradecraft and procedure; indicators of compromise?

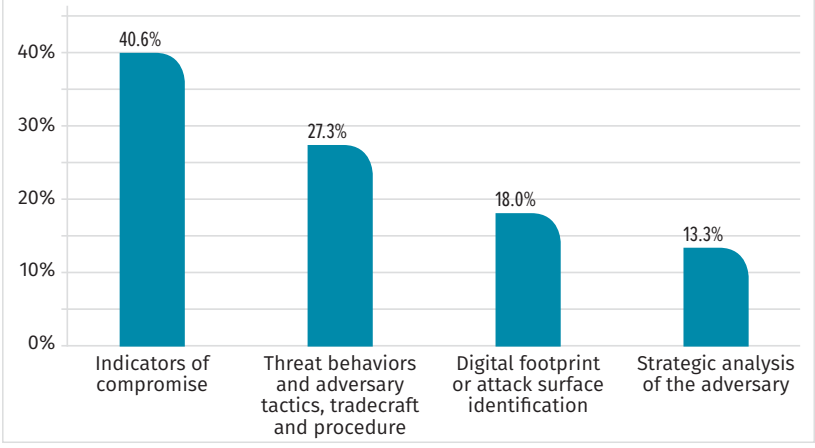


Figure 2. How Organizations Are Leveraging CTI

Although IoCs have gained the most market attention, it is likely that threat behaviors and adversary TTPs will continue to rise as organizations become more familiar with them and learn how to leverage them easily.

We will continue to monitor the use of different types of CTI in the coming years. Although IoCs have gained the most market attention, they are often too generic to provide long-term, strategic intelligence value. It is likely that threat behaviors and adversary TTPs will continue to rise as organizations become more familiar with them and learn how to leverage them easily. There has been considerable market focus on this area recently, including a significant uptick in discussions and highlights of MITRE's ATT&CK framework, which aims to classify adversary behaviors for easier sharing and classification across organizations.

CTI Requirements

Arguably the most important part of the CTI process is identifying and defining good requirements. Requirements guide the entire intelligence life cycle and make the collection, analysis, processing and dissemination of intelligence much more focused, enabling organizations to properly operationalize intelligence work. Shockingly, only 30% of organizations noted that the requirements had been documented. Another 26% did note that they planned to define them, but 37% said the requirements were ad hoc, and 7% indicated they had no plans to formalize requirements. See Figure 3.

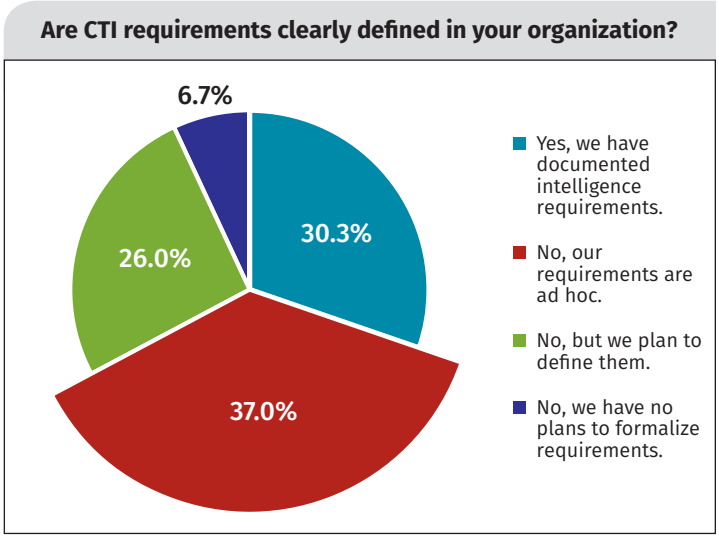


Figure 3. Defining CTI Requirements

SANS strongly recommends that organizations clearly document requirements for their CTI teams to establish a clear focus. Requirements that come up on short notice are still perfectly fine and can be treated as priority intelligence requirements that are important and time-sensitive.

Defining good intelligence requirements requires input from a wide variety of people at an organization. It is common for CTI to support security operations and IR, but good CTI is capable of supporting a wide range of functions that deal with risk across the organization. Respondents seem to get input

Best Practice for Defining Requirements

A best practice for defining requirements is to identify a knowledge gap or pain point for the organization as it relates to threats and set forth a simply stated question or statement to be satisfied. A few common intelligence requirements would be:

- What threats are active in our industry?
- What adversary capabilities do we not prepare for currently?
- Of our vulnerabilities, which are being actively exploited in the wild?

A few common requirements that could be priority requirements and time-sensitive would be:

- What intelligence exists to support this current IR case?
- How does our threat model change by doing business with a partner company?

from a variety of sources: 66% of respondents noted that the CTI team contributed, with 65% indicating that security operations contributed, followed by 49% in IR. These are strong values and represent expected contributions. See Figure 4.

Vulnerability management contributed for 33% of respondents. Fortunately, another 33% of respondents noted that executives (C-suite or board members) contributed directly to the intelligence requirements process. Gaining senior level buy-in for intelligence requirements can often be a hallmark of maturity for a CTI team, and the number of participants who have that level of engagement surpassed expectations.

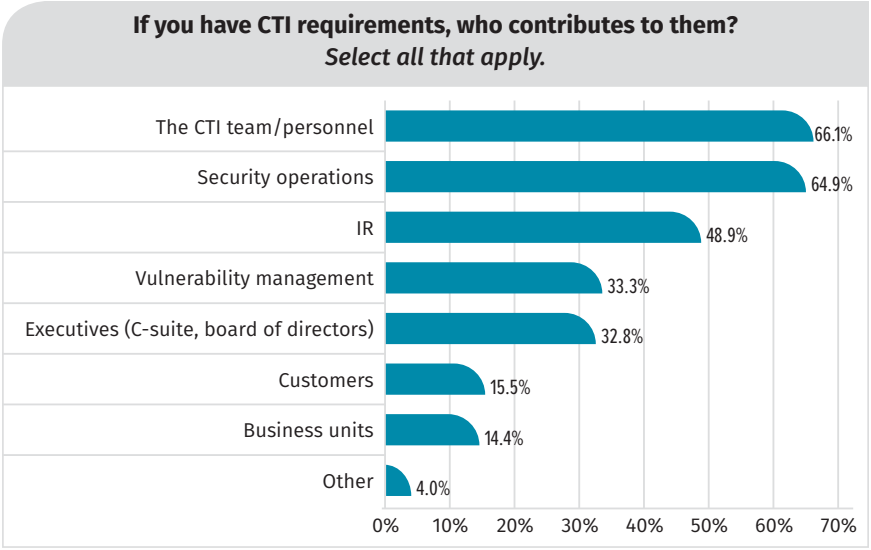


Figure 4. CTI Requirement Sources

Collection Sources

After defining requirements, an important part of CTI is determining where you have intelligence collection. Most organizations struggle to understand their collection both internally and externally. External collection can be easier to document, such as sources of feeds and reports or malware repositories and tools, but it can be particularly challenging to determine what internal collection exists and whether it is consistent across the organization. As an example, an organization may get host-based logs from systems, but be unsure of where gaps in collection exist across all the hosts.

Figure 5 presents respondents' perceptions of the external and internal data sources that are part of their intelligence-gathering efforts.

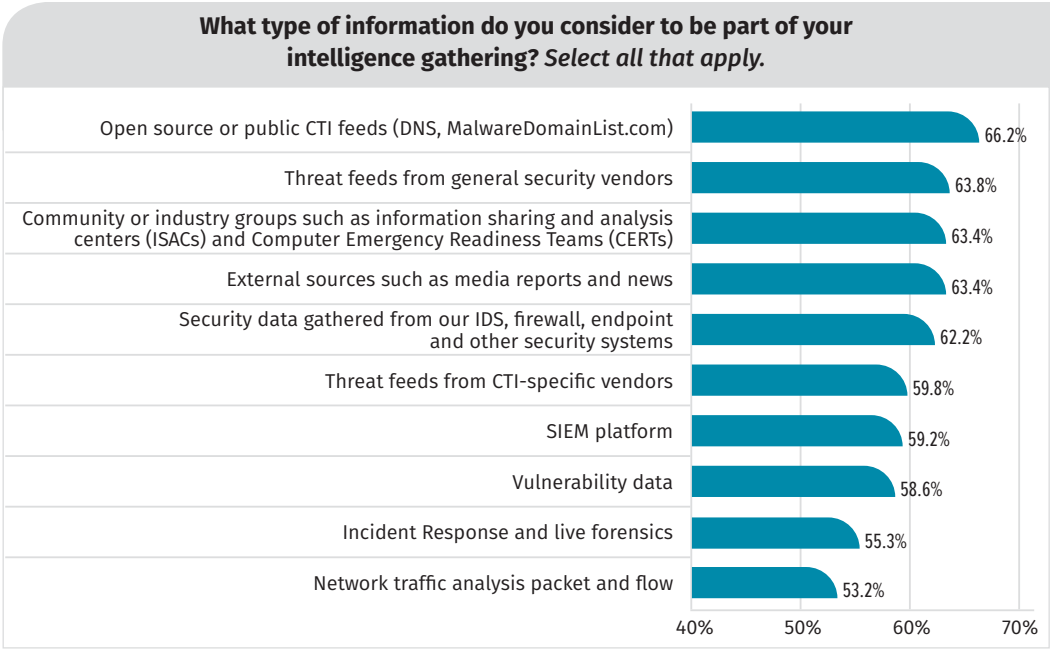


Figure 5. Internal and External Data Sources

The top choices are very close in distribution. The greatest percentage of respondents (66%) took advantage of open source or public CTI threat feeds, followed closely by threat feeds from security vendors (64%), community or industry groups (63%), and external sources such as media and news (63%). The fifth most popular was security data such as alerts gathered from the IDS, firewall, endpoints and other security systems at 62%.

Although the choices were very close in their distribution, it still seems that external sources are often favored over internal sources for gathering CTI. This could be a result of the ease of obtaining external sources compared with how difficult it can be to get the right collection within the organization. It is a common complaint of CTI teams that there are breakdowns in communication in organizations among security operations, security architects and incident responders, leaving incomplete access to intrusions that must be analyzed.

None of the sources presented had less than 25% adoption across the participants, with the lowest being shared spreadsheets, honey pot data and user behavior data. IR and live forensics, as well as network traffic analysis, vulnerability data and SIEM platforms, all had more than 50% of respondents note that they were part of their collection.

The best way to ensure that collection sources are understood and properly leveraged is to develop a collection management framework (CMF), which details data sources (both internal and external), what data they contain and how they are being utilized. A CMF not only reduces silos between teams, but also helps to identify high-value sources as well as gaps in collection that need to be addressed for full coverage.

Best Practices for CTI Team Makeup

Requirements drive the value of different makeups of CTI teams, but it is generally a best practice to have a wide range of skills and backgrounds represented. Such a combination helps to defeat biases and deliver intelligence against a wide range of intelligence requirements instead of only security operations and IR.

Identifying the Right Staffing for CTI

There are many opportunities to staff a CTI function, whether it's in-house or outsourced, and whether it's a dedicated team or an element of an existing security team. Across the participants, 37% handled CTI as an in-house-only function; 54% handled it as a combined in-house and service provider function. With more than 90% of respondents having dedicated or combined CTI functions, it appears that an in-house CTI function is core to organizations. Only 8% completely handed that responsibility over to a service provider.

Digging into the metrics a bit more, SANS wanted to know whether the in-house function was dedicated or had some other makeup. The survey found that 41% of respondents had a formal dedicated CTI team. Further, 28% of respondents had a shared-responsibility team with staff pulled across security, and 13% had a single dedicated CTI analyst.

Of those respondents reporting having an in-house CTI function, team members came from a variety of sources. The largest concentration (49%) was from the security operations center (SOC), followed closely by IR with 44%, as illustrated in Figure 6.

Where are CTI team members drawn from within the organization?
Select those that most apply.

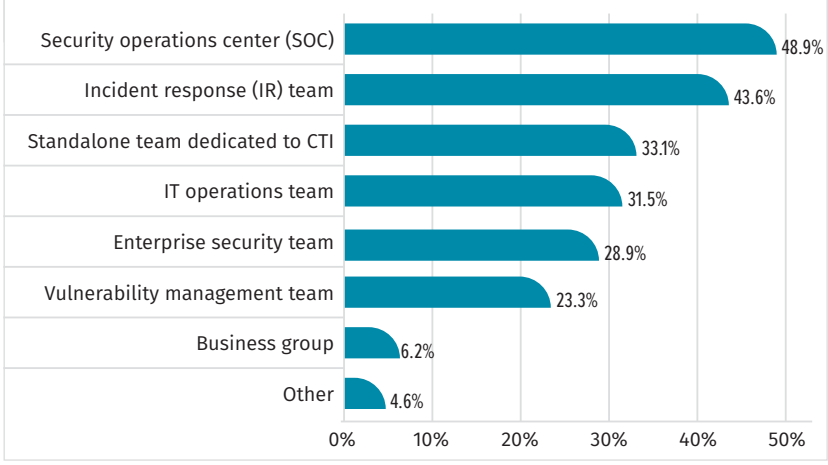


Figure 6. CTI Team Composition

What is interesting is that the respondents indicated that they pulled from across the organization pretty consistently, including involving staff from vulnerability management, IT operations, the enterprise security team, and even business groups. Including members from a range of backgrounds helps improve the quality of the intelligence delivered.

CTI Usage

This year's survey painted a picture of a maturing and diversifying definition of CTI, and these changes are evident in the way that CTI is being produced and used across the industry. The majority of organizations involved with CTI fall into one of three primary categories: those who produce intelligence, those who consume intelligence that has been produced by someone else, and those who both produce their own intelligence and consume intelligence that others have produced. In the 2019 survey, we found that 72% of organizations reported that they either produce or consume CTI, a steady increase from 60% in 2017 and 68% in 2018, as illustrated in Figure 7,[3] with a corresponding decrease in those reporting that they neither produce nor consume. In 2019, only 8% of respondents reported no plans to consume or produce intelligence at all, indicating that more and more organizations plan to leverage CTI as a part of their overall information security strategy.

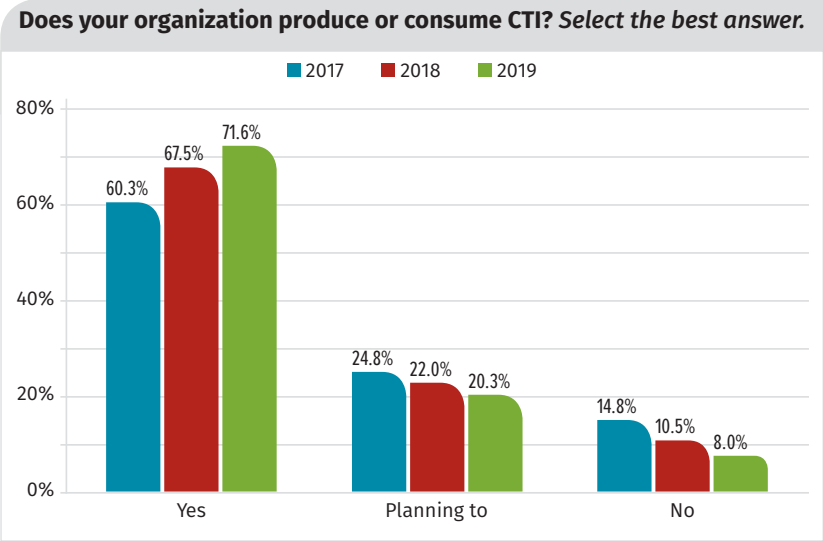


Figure 7. CTI Producer vs. Consumer

Intelligence Production and Consumption

A small percentage reported that they only produce intelligence, which includes both raw threat data (5%), analyzed indicators for alerting (4%) and finalized reports (4%). See Figure 8.

The number only producing CTI has decreased since the 2018 results, where 6% reported producing raw threat data, and 10% reported producing finalized reports.[4] Although there was a decrease in the percentage of respondents reporting that they produce finalized intelligence, the highest number of respondents reported consuming finalized intelligence. What this tells us is not necessarily that there is a decrease in the overall number of organizations producing intelligence for general consumption, but that the number of organizations leveraging intelligence is increasing, making the percentage of producers lower by comparison.

Figure 8. Intelligence Types

[3] "CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey," February 2018, www.sans.org/reading-room/whitepapers/analyst/cti-security-operations-2018-cyber-threat-intelligence-survey-38285, p. 3, Table 1. [Registration required.]

[4] "CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey," February 2018, www.sans.org/reading-room/whitepapers/analyst/cti-security-operations-2018-cyber-threat-intelligence-survey-38285, p. 3, Table 2. [Registration required.]

What does that mean for the intelligence world? It means there is an increased demand for CTI, especially finalized, long-form reports that give a complete overview of the threat. This demand will either need to be met by the existing intelligence producers, who may have to diversify as they build a broader customer base, or organizations will need to transition to both consuming and producing their own intelligence reporting to ensure that it is applicable and actionable within their specific organizations.

Leveraging CTI

Whether it is production, consumption or both, 72% of organizations participating in the 2019 survey reported utilizing CTI, with another 20% planning to do so. However, the ways that CTI is being used varies across organizations. This year's survey shows that the uses of CTI have broadened to the point that there is not one clear leading use case, as we saw in previous years. The top responses, separated often by less than a percentage point, include security operations, detecting threats and attacks, blocking threats and security awareness. One interesting trend in this year's survey is the that the use of threat intelligence for detecting threats and attacks decreased significantly from the 2018 survey, from 79% in 2018 to 66% in 2019, as shown in Table 1.[5]

Table 1. Year-Over-Year Comparison of Uses of CTI[6]

	2019		2018	
How is CTI data and information being utilized in your organization?	**%**	**Rank**	**%**	**Rank**
Security operations (proactively and continuously monitoring for threats)	66.2%	1	N/A	N/A
Detecting threats and attacks	65.6%	2	79.3%	1
Blocking threats	64.3%	3	70.1%	3
Security awareness	59.5%	4	62.6%	6
Threat management (identified threats)	57.3%	5	66.7%	4
Vulnerability management	53.7%	6	64.4%	5
Incident response	49.7%	7	70.7%	2
Threat hunting (hypothesis-driven structured hunts)	47.3%	8	62.1%	7
Risk management	45.7%	9	N/A	N/A
Prioritizing security controls	41.8%	10	52.3%	8
User education	41.8%	10	46.0%	10
Vulnerability remediation prioritization	39.3%	12	48.3%	9
Threat modeling	37.8%	13	43.7%	11
IT operations (troubleshooting infrastructure)	33.5%	14	36.8%	14
Executive education and awareness (board of directors, C-suite)	31.4%	15	43.1%	12
Compliance	28.1%	16	37.9%	13
Budget and spending prioritization	14.3%	17	23.6%	15
Other	1.5%	18	3.5%	16

[5] "CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey," February 2018, www.sans.org/reading-room/whitepapers/analyst/cti-security-operations-2018-cyber-threat-intelligence-survey-38285, p. 3. [Registration required.]

[6] Where an option was not offered, we have inserted an N/A.

Threat detection and threat blocking were some of the earliest usages of threat intelligence, due in large part to the fact that existing technologies easily supported these use cases. In the past few years, the threat intelligence industry has matured, and new applications and methods for utilizing CTI have been introduced, so we are seeing more and more use cases. Some innovative applications reported by survey respondents include:

- "[We are] currently using a tipper format to the SOC for ad hoc/intelligence-driven hunting, based on customer industry/profile, installed software/hardware, vulnerability scan results, or other factors based on recent news or emerging threats."
- "During a recent ransomware outbreak, [we were] able to trade and analyze samples with fellow analysts, and by identifying shared infrastructure, proactively blocked threat traffic from infrastructure that these actors began to leverage months later."
- "Utilize CTI to tune defenses and provide roadmap for user education and scenarios for training"

In this year's survey, respondents indicate that they currently get the most value out of CTI that includes details about the threat landscape in general and their organization/brand specifically. This type of intelligence can be used broadly across organizations. Attribution data on "who" was carrying out attacks ranked lowest in current value, but ranked highest in the type of intelligence that an organization would like to begin to leverage in the next 12 months. See Figure 9.

SANS Recommends

Whether your organization has been leveraging CTI for years or you are just getting started, it is important to note that CTI can be used in many different ways, and the best applications are going to depend on your organization and its needs. Understanding your requirements, key use cases, existing capabilities and maturity will help you get on the right track.

What types of CTI are currently most useful to your operations? What would be most useful in the future?
Select all that apply.

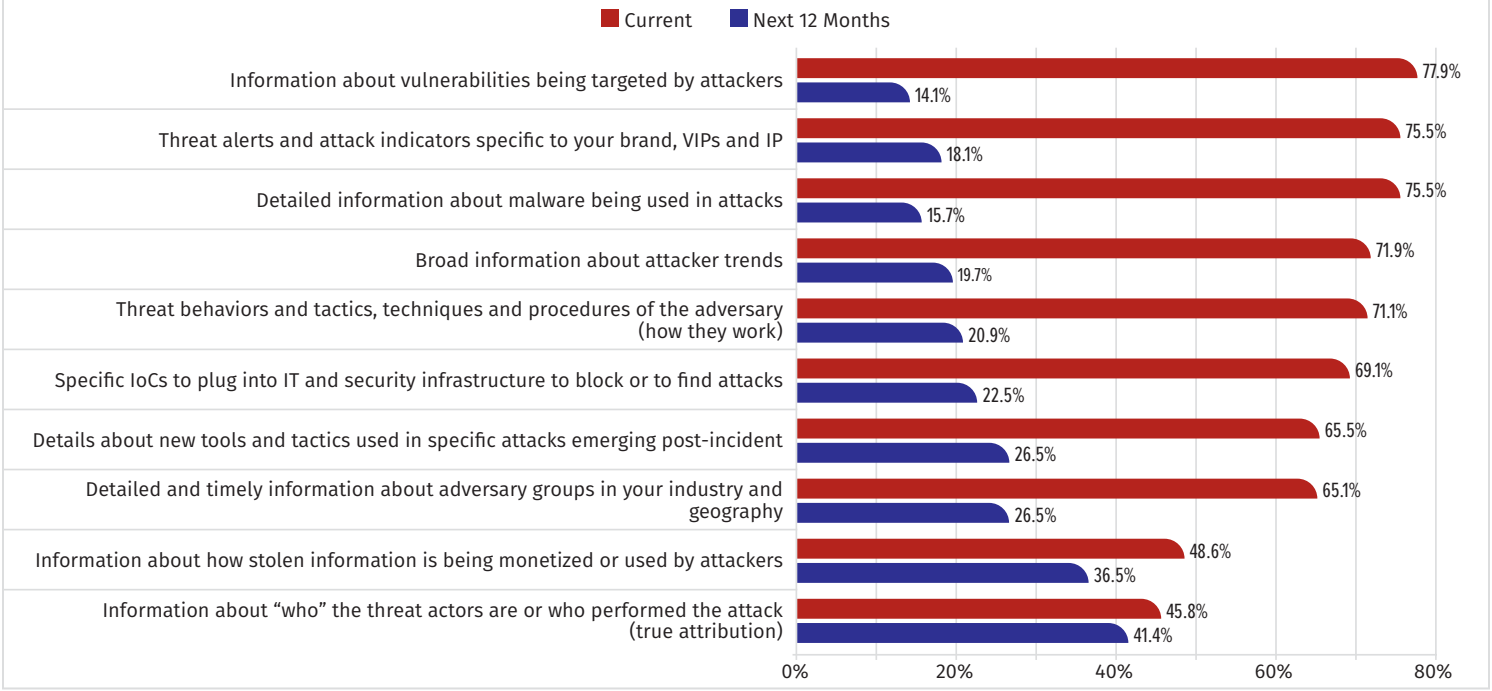


Figure 9. Current and Future Usefulness

What Has CTI Done for You?

When asked to rate how CTI is supporting and improving existing security programs, respondents indicated that the most significant and measurable improvements were in improving visibility into threats and attack methodologies affecting our environment, revealing vulnerabilities where new security measures should be implemented, prioritization of efforts and resource utilization, and more accurate risk analysis. These areas directly line up with the definition of CTI: analyzed information about the intent, capabilities and opportunities of adversaries. Applications falling outside of areas that would depend on CTI, such as preventing business outages, are ranked as the least useful. See Table 2.

Table 2. Usefulness of CTI

	Level of Improvement Noted			
Area of Improvement	**None**	**Measureable**	**Significant**	**Overall**
Improving visibility into threats and attack methodologies impacting our environment	3.3%	47.3%	43.3%	90.6%
Revealing vulnerabilities where new security measures should be implemented	8.2%	51.4%	32.7%	84.1%
More accurate risk analysis	6.9%	49.0%	31.8%	80.8%
Reducing time to identify and respond to incidents	6.5%	52.7%	27.8%	80.4%
Prioritization of efforts and resource utilization	9.8%	48.2%	31.0%	79.2%
Detecting unknown threats	12.2%	47.8%	29.8%	77.6%
Improving accuracy (fewer false positives)	11.0%	51.8%	24.9%	76.7%
Locating the source of events impacting our enterprise	10.6%	53.5%	22.0%	75.5%
Measurably reducing the impact of incidents	11.8%	54.3%	19.6%	73.9%
Reducing exposure of sensitive data	10.6%	53.1%	20.8%	73.9%
Preventing breaches	13.5%	44.5%	25.3%	69.8%
Preventing business outage	23.7%	37.6%	13.9%	51.4%

When rating overall satisfaction with CTI, the majority of organizations are satisfied or somewhat satisfied with CTI data, with the most satisfaction coming from relevance and timeliness of strategic reports and threat awareness. The areas with the least satisfaction include automation of CTI data and machine learning, indicating that the majority of organizations rely heavily on manual processes and human analysis for the parts of CTI that they think are most useful. See Table 3.

Table 3. Satisfaction with CTI

	Very Satisfied	Satisfied	Combined Satisfaction	Not Satisfied
Timeliness of threat data and intelligence	8.3%	61.8%	70.1%	24.0%
Visibility into threats and IoCs	12.2%	57.1%	69.3%	24.8%
Searching and reporting	9.8%	58.7%	68.5%	24.8%
Relevance of threat data and information	10.6%	56.3%	66.9%	26.4%
Integrated data feeds	6.3%	57.5%	63.8%	29.9%
Reports (strategic and operational level)	12.6%	51.2%	63.8%	30.3%
Analytics	7.9%	51.6%	59.4%	34.3%
Cleanliness and quality of data	7.5%	51.6%	59.1%	37.4%
Context	9.1%	50.0%	59.1%	35.4%
Comprehensiveness of coverage	5.5%	51.6%	57.1%	37.4%
Automation and integration of CTI information with detection and response systems	8.7%	47.6%	56.3%	39.4%
Location-based visibility	5.5%	45.3%	50.8%	42.5%
Identification and removal of expired indicators of compromise (IoCs) and other old data	8.3%	38.2%	46.5%	47.6%
Machine learning	5.5%	29.1%	34.6%	55.9%
Other	1.2%	9.8%	11.0%	4.7%

The areas of least satisfaction provide clear guidance on areas with the potential for the most improvement. Previous years' surveys indicated a desire for more accurate and timely intelligence with more context, and over time the quality and usability of intelligence have improved significantly to the point where the majority of respondents are very satisfied or satisfied with these aspects of CTI. In the future, overall satisfaction can be improved by focusing on improving automation and integration of quality information.

SANS Recommends

You can improve your overall satisfaction with CTI by focusing on improving automation and integration of quality information.

Putting CTI to Work

Even with higher quality and more timely data, CTI must be integrated into the systems that defenders use to leverage this data, and—as previously mentioned—respondents are hoping to see improvements in integration and automation in the future. Beyond offering general awareness of threats, which survey respondents do value, CTI must be managed, processed and integrated into prevention, detection and response systems.

Processing Intelligence

Most types of threat data must be processed prior to being usable. Some of these processes include deduplication of data; enrichment of data using public, commercial or internal data; reverse engineering of malware; and data standardization. Most organizations report that processing is either a manual or semi-automated process, although a notable percentage report fully automated processes for these tasks. In general, the trend is that processing tasks are primarily semi-automated, followed by manual and then fully automated.

The outliers for this trend are reverse engineering of malware and standardization of data into a common format. Reverse engineering of malware samples requires manual analysis for 46% of respondents, is semi-automated for 29%, and fully automated for only 8%—much lower than other processing methods. Standardization of data is reported as being almost equally manual and semi-automated, also with a lower percentage of fully automated processes, as shown in Figure 10.

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

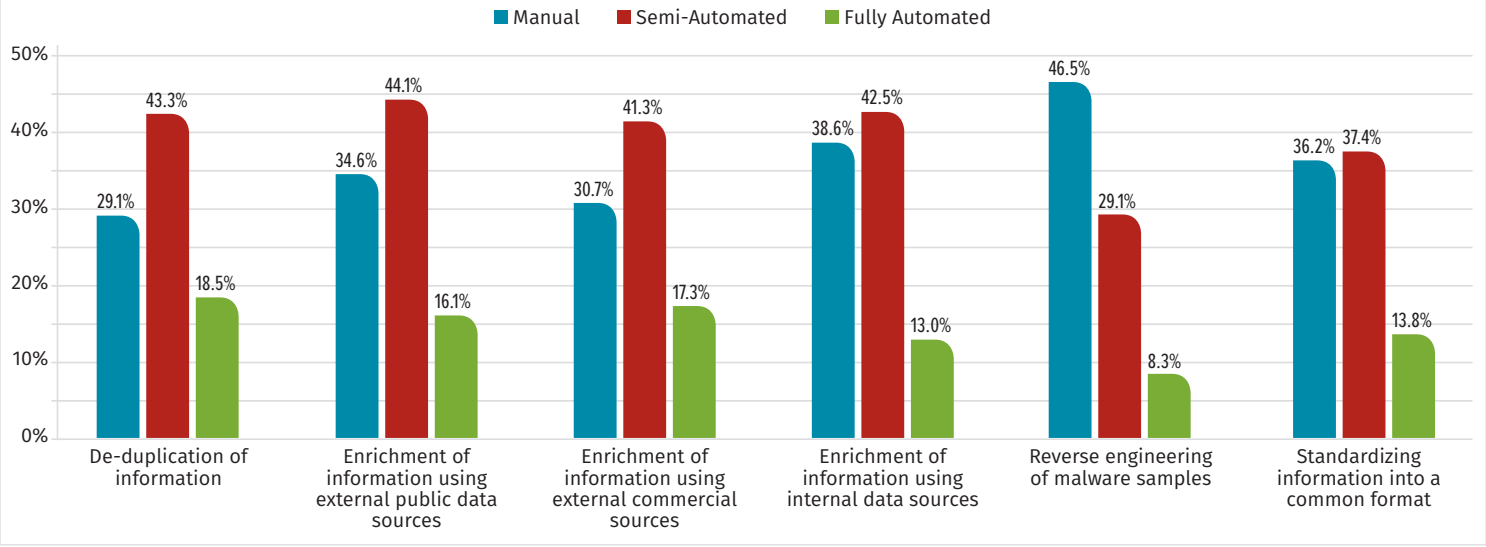


Figure 10. CTI Processing

Managing and Integrating Intelligence

In this survey we found that when it comes to managing CTI, SIEM platforms still reign supreme, with 82% responding that they use a SIEM for intelligence management (54% of those respondents use an integrated GUI); network traffic analysis tools come in a close second, leveraged by 77% of respondents. A large number of respondents, 66% and 64% respectively, leverage a commercial or open source CTI management platform, often referred to as a threat intelligence platform, or TIP. Many organizations use multiple methods to manage data, without a single platform or source to handle all aspects of CTI.

One trend that has continued to grow is the use of spreadsheets and/or emails for managing intelligence, which are being leveraged by 76% of respondents, up from 67% in 2018 and 61% in 2017. This method is most often used disparately, rather than through an integrated GUI. While some think this trend is alarming and that there must be a better way to gather and manage intelligence, the continued usage—and even increase in usage—shows that these methods are often the default or preferred method for many intelligence analysts.

SANS Recommends

Because they are used so frequently, rather than trying to get rid of such management tools as spreadsheets and/or emails for managing intelligence, analysts should focus on how to properly leverage and manage them. It would be ideal to integrate them more fully with other management methods.

While SIEMs are used for management, more than half of respondents (56%) said that they use a threat intelligence platform or other intelligence service provider (53%) for integration into response. Many organizations (46%) rely on specific vendor integrations to support response operations, primarily through APIs or prebuilt connectors. In fact, 43% leverage custom APIs, indicating that even with intelligence-specific platforms and integrations, there is rarely a one-size-fits-all solution. As one respondent put it, integrating threat intelligence into response is a "work in progress"—even when there is a system in place, it often requires customization, modification and improvements as intelligence sources and processes change.

The Way Ahead

CTI has changed immensely in a few short years and is no longer synonymous with IoCs, but is growing to include TTPs, threat behaviors, attack surface awareness and strategic assessments. In addition, SANS has seen a maturation of the CTI process itself as more organizations are developing intelligence requirements, producing and consuming intelligence across the spectrum, and leveraging it in ways that are specific and unique. Information sharing—with an emphasis on sharing best practices, use cases and lessons learned as well as timely, actionable and relevant intelligence—remains a key way to move forward as a community.

The trends we have seen in 2019 show there is less emphasis on raw threat data and more emphasis on strategic-level reports, especially ones that are specifically relevant to an organization. With a growing number of organizations both producing and consuming intelligence, and an increasing number of analysts dedicated exclusively to CTI functions, this is an area in which we expect to see more organizations handle themselves or create in partnership with intelligence providers, rather than outsourcing completely. Efforts such as this will directly benefit from a diverse CTI team with members from different organizational disciplines and backgrounds.

Automation is a growing area of interest, specifically for collecting and processing tasks such as deduplication and enrichment of data. For teams to focus on the increasing use cases for CTI, including attack surface awareness and strategic analysis, they will first have to find ways to automate or streamline aspects such as collecting and processing, which often take up the majority of an analyst's time. Continued growth and development in this area will likely increase organizations' abilities to operationalize intelligence and result in greater satisfaction with CTI.

The 2019 survey shows a discipline that is evolving in many positive ways and is becoming more diverse in use cases, collection sources and output. CTI is used to determine where to focus security efforts, track adversary trends, detect adversary activity, and make networks more secure and resilient against threats. While there are still many improvements that can be made to support analysis efforts, this survey has shown just how much CTI has evolved.

About the Authors

Rebekah Brown, SANS instructor and co-author of the SANS FOR578: "Cyber Threat Intelligence" course, the SANS "Cyber Threat Intelligence Consumption" poster, and Intelligence-Driven Incident Response, excels at educating students and professionals about threat intelligence. Rebekah has helped develop threat intelligence programs at the highest levels of government, including providing a briefing at the White House on the future of cyber warfare and coordinated defensive and offensive cyber operations. Today, she focuses on understanding intelligence sources, conducting multiple levels of analysis, and explaining what intelligence means and how it can be used to a variety of audiences as the threat intelligence lead for Rapid7.

Robert M. Lee, a SANS certified instructor and author of the "ICS Active Defense and Incident Response" and "Cyber Threat Intelligence" courses, is the founder and CEO of Dragos, a critical infrastructure cybersecurity 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 cybersecurity 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:

ANOMALI®