SANS

A SANS Survey

CTI in Security Operations:

SANS 2018 Cyber Threat Intelligence Survey

Written by **Dave Shackleford**

February 2018

Sponsored by:
DomainTools

SANS Analyst Program

Executive Summary

As the threat landscape continues to change, and with more advanced attackers than ever, security teams need all the help they can get to more effectively prevent, detect and respond to threats. Fortunately, many organizations are sharing details about attacks and attackers, and numerous open source and commercial options exist for collecting and integrating this valuable intelligence, according to respondents to this, the fourth annual SANS survey on cyber threat intelligence (CTI).

The survey focuses on how organizations could collect security intelligence data from a variety of sources, and then recognize and act upon indicators of attack and compromise scenarios in a timely manner. For purposes of this report, CTI is defined as the "collection, classification, and exploitation of knowledge about adversaries," as it is defined in the SANS CTI Forensics course.[1] One of the course's primary authors describes CTI as "analyzed information about the intent, opportunity and capability of cyber threats."

This year's survey echoed some of the same trends we saw in our 2017 survey,[2] in which top use cases for CTI included security operations, incident response and security awareness. SIEM was the most common integration point for collecting and analyzing CTI data, and top improvements as a result of using CTI included improving visibility into threats and attack methodologies impacting our environments, improving security operations and detecting unknown threats.

Although some CTI trends continued this year, we definitely saw several differences in a number of areas, which are noted in the research.

For example, the highest area of satisfaction for CTI analysts in 2017 was relevance of threat data, but the category of searching and reporting was the top area of satisfaction this year. Threat intelligence feeds were usually integrated via APIs in 2017, and in 2018 we saw dedicated threat intelligence platforms become more common. CTI data is also becoming more embedded into the security operations center (SOC), with 53% of respondent organizations housing CTI staff in their SOC, while 32% included them as part of their enterprise security teams and another 32% included them in incident response teams.

From this year's results, it is obvious that CTI collection, integration and use within security teams are maturing. Read on for more insights!

Key Takeaways

This year's takeaways point to the growing usefulness of CTI data and the need for more integration between CTI tools and data feeds.

- CTI is becoming more useful overall, especially to security operations teams.
- CTI is becoming more integrated, with the SIEM still the most common tool for management of CTI. Standalone CTI platforms gained significant traction this year as compared to previous years, as well.
- Improvements in detection and response aligned with results from past years.
- Staffing, lack of budget and time to deploy CTI properly are still the top problems many organizations face.
- CTI tools need to be easier to configure, integrate with other systems, and use overall, allowing more junior staff to do more with less time.

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

[2] "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

Operationalizing CTI

Year-over-year results, shown in Table 1, indicate that use of CTI data has become ubiquitous over the past two years.

Taken together, these results indicate that fewer organizations are ignoring the value CTI offers. In fact, most are already using CTI for detection and response.

Table 1. Overall Use of CTI

CTI Usage Variable	2017	2018
No CTI for detection or response, with no plans to develop	15%	11%
Create or consume CTI data	60%	68%
Plan to use in the future	25%	22%

Consuming and Producing CTI

In the security and forensics communities, there has also been a subtle shift toward developing internal threat intelligence for organizations' own consumption, versus simply acquiring CTI from intelligence providers, although production of raw CTI dipped slightly this year. See Table 2.

With that said though, in 2018, the top sources of CTI threat information are from outside the organization (third-party intelligence data and media reports/news. However, internal sources of CTI data garnered just 8% fewer responses than the top response. By producing their own threat intelligence data, respondents are likely using this to supplement their third-party feeds and customize threat intel to their environments. This provides an opportunity for third-party providers to develop more customized feeds specific to their client environments.

Table 2. Production and Consumption of CTI Data

	2017	2018
Produce Raw CTI Data	7.5%	5.6%
Consume Raw CTI Data	39.6%	41.6%
Produce and Consume Raw CTI Data	46.5%	47.2%
Produce Finished CTI Reports	6.6%	9.8%
Consume Finished CTI Reports	47.4%	47.7%
Produce and Consume Finished CTI Reports	41.0%	40.7%

Mining Their Own Intel

The gathering of internal threat data is gaining traction though, especially security data from network and host controls, identified by 81% of respondents, and vulnerability data, selected by 76%. Several other internal controls were listed, such as access and user account data, user behavior data, and honeypot data (see Figure 1).

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

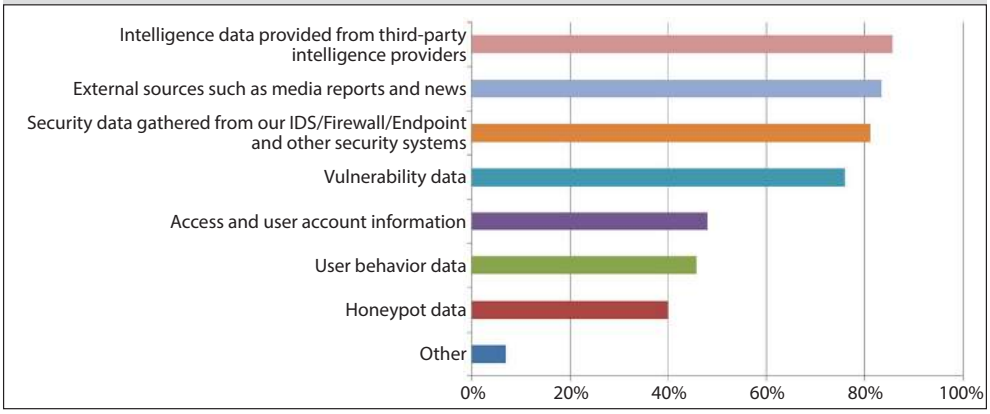

Figure 1. Intelligence Information Sources

Embedding CTI in Security Operations

In 2017, the majority of respondents indicated they were focused on using CTI for security operations (locating sources and/or blocking malicious activities or threats), followed by incident response and informing security awareness activities). Threat management, vulnerability management and threat hunting were also very popular use cases.

Responses to the 2018 survey reveal a drop in the use of CTI for security awareness, with more emphasis on security operations tasks: detecting threats (79%), incident response (71%), blocking threats (70%) and threat hunting (a little further down the

list at 62%). The use of threat hunting is growing, according to the SANS 2017 Threat Hunting Survey. Figure 2 shows the full breakdown of how respondents' organizations use CTI data.

The increasing emphasis on CTI use in security operations is not surprising. In fact, we asked respondents for real-life use cases and examples this year, and got a number of responses that align closely with operations.

Numerous responses indicated that threat intelligence was key in augmenting and improving firewall rules, network access control lists and reputation lists. Known sites and indicators associated with ransomware were shared through threat intelligence, allowing operations teams to quickly search for existing compromise and proactively block access from internal clients.

How are CTI data and information being utilized in your organization?
Select all that apply.

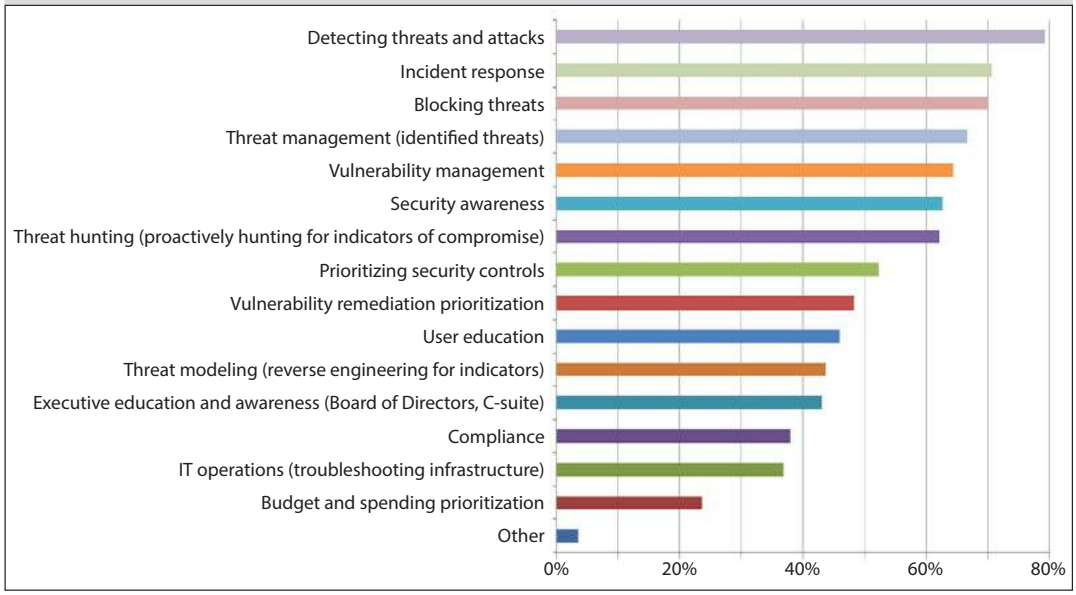

Figure 2. Top Use Cases for CTI Feed Data

Staffing and Teams

Whether producing or consuming CTI, almost 42% of respondents have a formal team dedicated to CTI (down from 47% in 2017), another 12% have a single team member dedicated to CTI (an increase from the 9% in 2017), and close to 31% stated they don't currently have a person or team dedicated to CTI, but treat it as a shared responsibility between security groups (up from 26% in 2017). See Figure 3.

Overall, we don't feel these numbers represent a significant shift or trend. While the composition of the teams or staff using CTI may differ, roughly the same general percentage of organizations is dedicating *some* resources to CTI, which may simply be a measure of organizational size, industry or both.

CTI in Real Life

In one write-in example, security operations discovered an admin who had posted internal device configurations in a forum without obscuring passwords and other internal details while seeking technical assistance. CTI discovered related keywords through open source intelligence gathering.

Supplementing Staff

Similar to what we saw in 2017, this year in-house and in-house/outsourced CTI is almost evenly split. Most organizations employ an in-house team (43%), while another 51% outsource some aspects of this function. Only 6% outsource CTI entirely.

Does your organization have resources that focus on CTI?

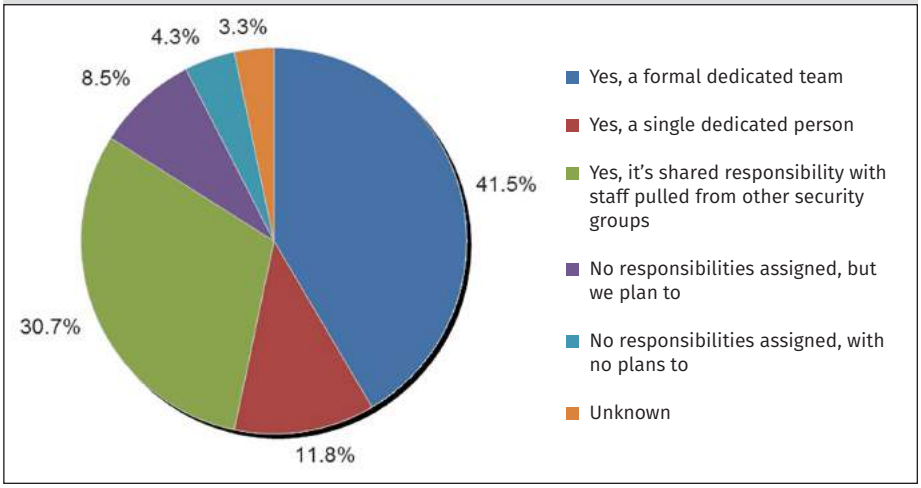

Figure 3. Staff and Team Allocation for CTI

Outsourcing CTI gives organizations different intelligence (and perhaps different expertise and experience) than they can get on their own, which may be attractive for organizations struggling to find time and internal talent for CTI programs. However, as has been true for the past several years, we continue to see the gradual upward trend of organizations gathering and building internal threat intelligence sources and output in addition to utilizing data provided from CTI vendors.

TAKEAWAY

Current and past CTI surveys reveal a gradual upward trend of organizations gathering and building internal threat intelligence sources and output to augment and work with the data they are also receiving from their CTI providers.

Defining Survey Respondents

This year's survey respondents represented a broad range of industries, as in past years. The top four verticals, included in Table 3, were the exact same as in 2017.

Along with these industries, respondents come from a mix of other industries, including education, healthcare, manufacturing and telecommunications.

Table 3. Top Four Industries Represented in the Survey

Industry	2017	2018
Cyber security	11.3%	16.1%
Banking and finance	15.0%	14.2%
Government	15.3%	12.4%
Technology	12.8%	11.2%

Roughly 27% of respondents worked in organizations with 5,000–50,000 employees, and over 16% were in organizations larger than 50,000. Forty-four percent of the organizations represented have 2,000 employees or fewer. The majority of organizations have operations in the United States (over 70%), with 42% in Europe and 33% in Asia. A mix of organizations has operations in many other countries and regions, too. The U.S. is headquarters for 62%, with 16% based in Europe, while just fewer than 7% are headquartered in Asia and 6% in Canada.

Roles and Responsibilities

The roles of respondents also varied widely. Roughly 22% identified themselves as security administrators or analysts, with another 10% in security management and executive roles (CSO and CISO). Over 16% were in IT operations or IT management, and many other roles were listed, including security architects, security researchers, CTI analysts and more. A small number also identified as threat hunters, threat research analysts and other related job functions that might create or use CTI.

Birth of a New Job Title

A full 12% of respondents carry the title of "Cyber Threat Intelligence Analyst" or similar, which doubled from 2017. This may signal growth in specialized CTI-related jobs.

Finding skilled staff to staff the CTI consoles is getting more difficult, according to this year's responses. We'll look at barriers to successful CTI program implementation a bit later in the report, but one statistic stands out as relevant here. In this year's survey, 62% of respondents cited a lack of trained CTI professionals and skills as a major roadblock, an increase of nearly 10 percentage points over 2017 (53%). This indicates that the more CTI is used and consumed, the more this skill set is in demand. It may be much more difficult to find staff members who are experienced in setting up and operating CTI programs. Similarly, 39% cited a lack of technical ability to integrate CTI tools into the organizational environment.

Back to the SOC

The majority (53%) of respondents indicated that CTI staff and teams were associated with the SOC. Enterprise security teams were second (32%), with incident response teams a close third. IT operations teams are the fourth option, while standalone CTI teams came in fifth with just over 26%. See Figure 4.

Where do CTI team member reside (or where are team members drawn from) within the organization? *Select those that most apply.*

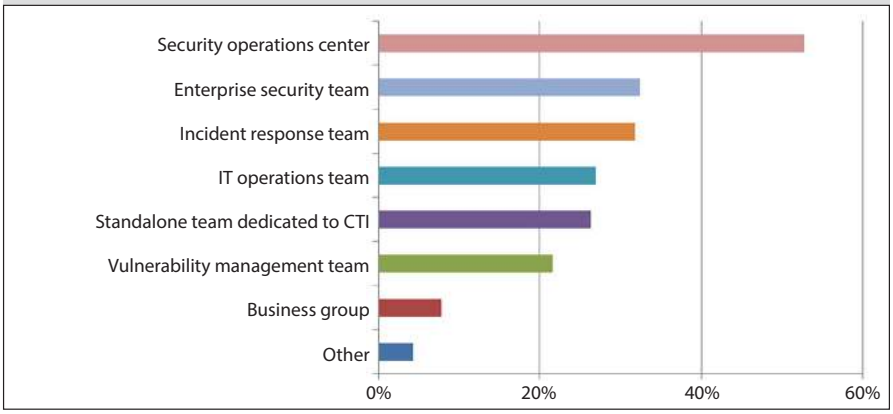

Figure 4. Where CTI Team Members Reside

Organizations have been struggling for some time to find well-trained and experienced security operations staff, as well as incident responders. Aligning CTI analysts with SOC activities makes sense, because CTI can feed and inform many day-to-day security operations practices in detection and response (more on this in a bit). However, the problem of finding good people seems to have bled over from security operations to CTI as well. This trend is likely to continue for some time.

TAKEAWAY

Embedding CTI into SOC activities demonstrates maturity of programs and provides organizations with the ability to use data feeds to support multiple SOC functions.

Acquiring and Using Threat Intel

As in last year's survey, organizations are leveraging a wide variety of external CTI sources. For example, 82% utilize CERTs and ISACs for CTI, while use of internal sources has dropped to fourth place since our 2017 survey, in which this answer option took second place. A larger percentage—62% as opposed to 54%—are still using internal feed sources, as illustrated in Figure 5.

Where is your CTI information derived from? *Select those that most apply.*

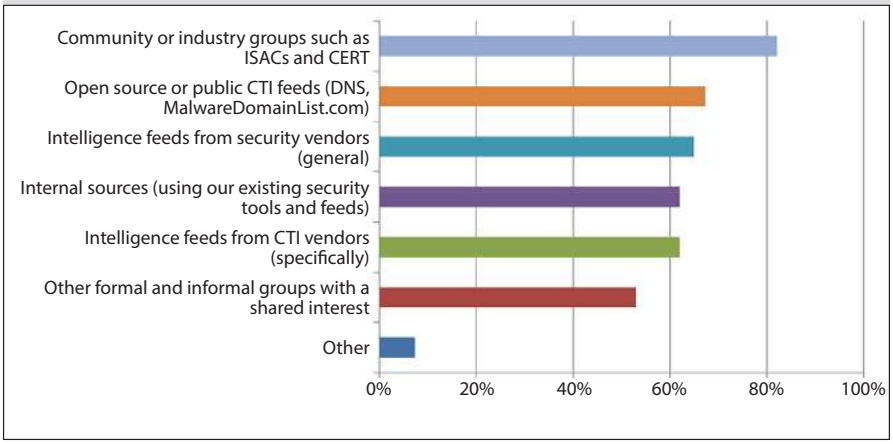

Figure 5. CTI Data Sources

Open source feeds, such as MalwareDomainList.com, came in second at 67%, and vendor feeds were third at 65%. We don't think the numbers really mean there's a major shift happening. In fact, the percentage of respondents gathering internal CTI data went up significantly, as did those gathering data from other formal and informal groups with a shared interest! What is obvious is that respondents' organizations are utilizing data from multiple data sources.

With the shortage of skills respondents reported, gathering, normalizing and analyzing open source CTI with vendor-provided and internally collected CTI, the task of connecting the dots between these data sources is most likely being done manually. For example, in one question on satisfaction—discussed later in this section—39% cite lack of interoperability and automation as a key inhibitor to fully implementing and utilizing CTI. In another question, we see that manual spreadsheets and email are often used for integrating CTI feeds. While other results show this is an area that vendors are improving upon, SIEM and other integration vendors should continue to improve organizations' abilities to reap the benefits of threat intelligence through better integration and automation.

Usefulness of CTI

The two most useful types of intelligence cited by respondents include detailed malware indicators used in attacks (81%), followed closely by information on the vulnerabilities that are targeted by attackers (79%). Respondents were able to select multiple choices, so they indicated that broad attacker trends (76%) and specific indicators of compromise (IOCs; 67%) were also very useful. See Figure 6.

During investigations, tracking vulnerabilities as they apply to IOCs is critical in preventing other attacks on those vulnerabilities and represents another growth point over our 2017 survey. Several write-in answers explained how respondents use CTI to prioritize vulnerability management:

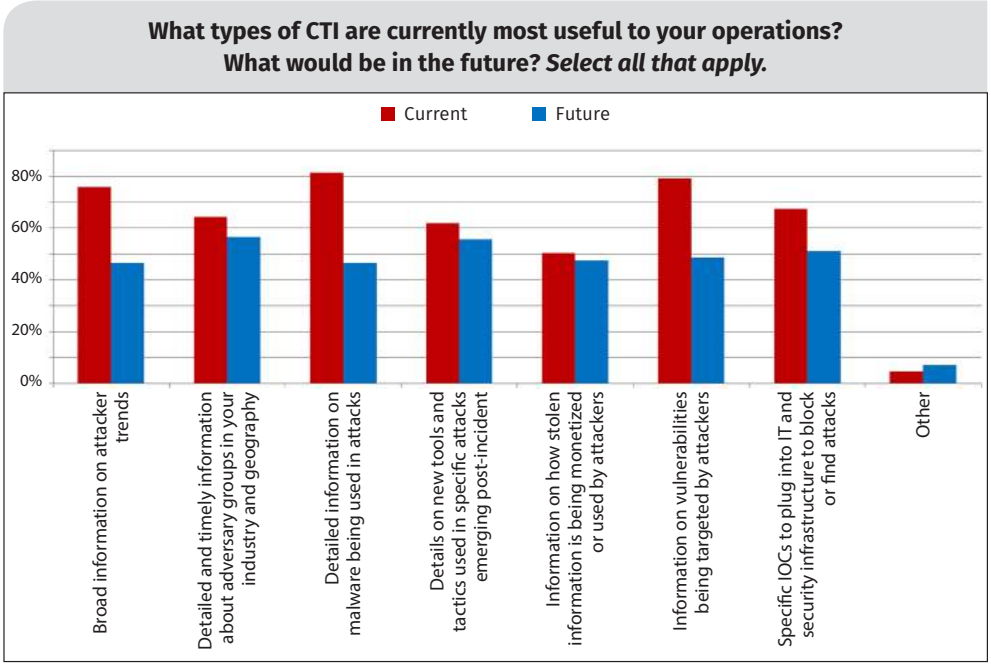

Figure 6. Most Useful CTI Data Today and in the Future

- "A new vulnerability comes out. Details are passed to Vulnerability Management for prioritization. If a known campaign/adversary is using it, that information is also passed for consideration and prioritization purposes."
- "Watching news or reading CTI provided by our [ISAC] will give us information [related] to current threats [and malware] that we have to patch/block/mitigate against. For example, proactively patching [the vulnerabilities related to] NotPetya as soon as our sources provided information on it."
- "CTI enables our organization to keep track of offenses that eventually guide the objectives in our defense strategies (deployment of better controls ... etc.) and risk management strategies."

Integrative Uses

The most obvious takeaway here is that organizations are looking for increasingly specific information about attackers, tools and IOCs. This big-picture information is interesting and useful, but technicians and operators also need specific data they can apply to detection and response scenarios immediately. Other write-in responses highlight the types of data respondents are drilling down into during investigations and how they're analyzing it:

- "We will monitor threat feeds and escalate [a] certain vulnerability remediation priority based on active exploitation campaigns in the wild. These feeds include vendor threat feeds or just security news."
- "We utilize several intelligence feeds to augment our perimeter firewall capabilities."

- "Pulled info on threat actors, source IPs, domains and [fed] them into EDR [endpoint detection and response] for [blacklists] and traffic reports from them."
- "We have alerting set up in our SIEM that correlates event searches against our subscribed threat intelligence feeds. From there we conduct our investigations and take whatever actions [are] deemed an appropriate response. The response is typically blocking malicious activities and hunting for further indicators of compromise across the enterprise environment."

TAKEAWAY

Most analysts want highly specific information where they can get it, but other consumers of this intelligence may also want the "big picture" information about attacks.

One answer, in particular, shows how CTI is collected and used during investigations and responses. It reads, "As CTI raw data, we gathered ransomware IPs, domain names, file hashes from CTI providers as a service and integrated those valuable data [points into] our SIEM, malware analysis appliance, firewall and IPS. Then, when traffic occurs from our [network] to those blacklisted IPs or when an email is received with a file attached with a hash of `Wcry` files, alarms are sent to related security teams. If the system is in blocking mode, we block that traffic."

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.*

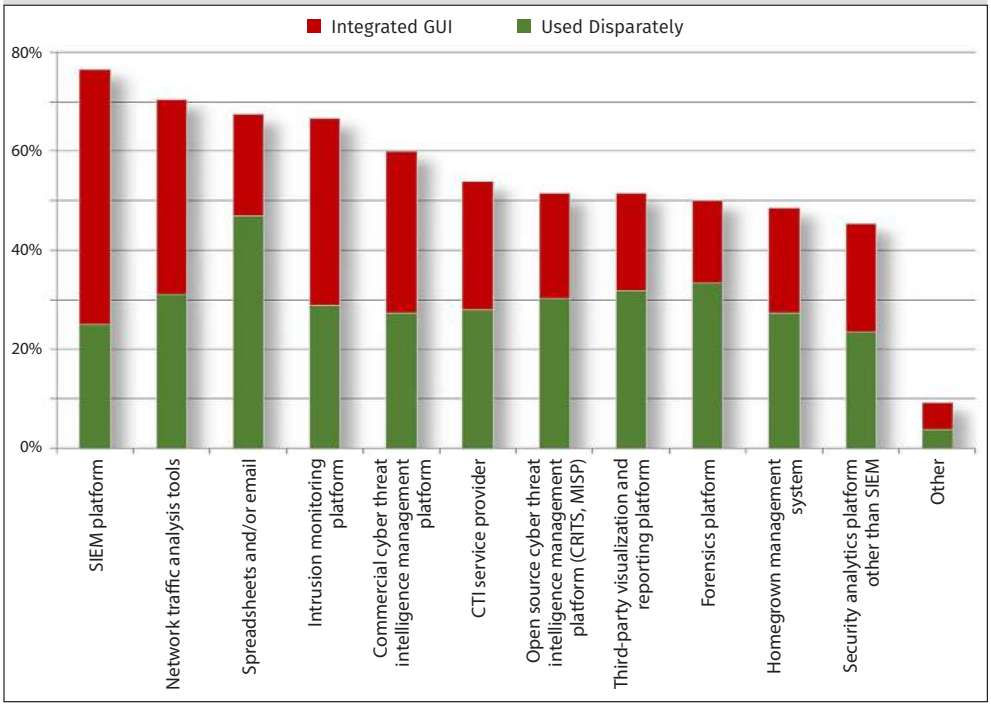

Figure 7. CTI Integration and Analysis Tools

Aggregation of CTI Feeds

Security teams are using a broad variety of tools to aggregate, analyze and present CTI in their environments, the top tool being their SIEMs, followed by network traffic analysis tools and spreadsheets and email. These results are similar to 2017, with the (somewhat dismaying) exception of spreadsheets and email coming in third with 67%, pushing intrusion monitoring to fourth. (In 2017, intrusion monitoring tools were third, behind network traffic analysis tools, followed by spreadsheets and email.)

See Figure 7 for the complete breakdown of integration and analysis tools.

Seeing a rise in manual methods is not encouraging. This trend is something we'll be tracking in future research.

TAKEAWAY

Organizations are obviously struggling with CTI data in disparate formats and are likely having even more trouble reconciling the data with numerous other critical sources of logs and events.

Dedicated Platforms on the Rise

Most security teams are integrating CTI feeds into the environment using dedicated threat intelligence platforms (57%), followed by APIs (vendor-provided at 48%, followed closely by custom APIs at 46%). In our 2017 survey, most were using APIs, with only 41% using dedicated threat intelligence platforms (both commercial and open source). See Figure 8.

This shows a significant amount of growth in the use of dedicated tools and platforms, which may also align with the current lack of skills in CTI.

Percentage using CTI platforms for aggregation, up from **41%** in 2017

Are these intelligence feeds integrated into your defense and response systems and, if so, how? *Select all that apply.*

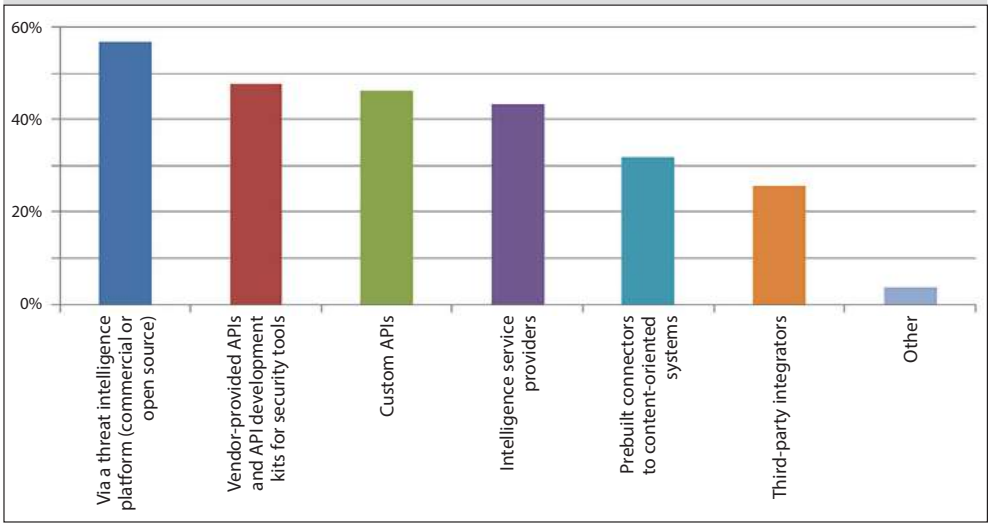

Figure 8. CTI Feed Integration

Improving Detection and Response

Are organizations satisfied with CTI? This is a complex question, and we chose to break down the responses into different categories. In general, 76% (the largest response group) say their teams are most satisfied with searching and reporting, 71% are satisfied with visibility into threats and IOCs, as well as the strategic and operational reports they receive. In addition, 70% are happy with the timeliness of their CTI, while 69% are satisfied with the relevance of their threat data, as well as the cleanliness and quality of data, and 65% were satisfied with comprehensiveness of coverage, with the same percentage being satisfied with context.

Respondents are least satisfied with machine learning and analytics, and with the removal of expired IOCs and other CTI data. The full breakdown of responses is provided in Table 4 (on the next page).

TAKEAWAY

Cleanliness and maintenance of CTI systems are important maintenance functions that should not be overlooked. If we build patterns and trends based on the wrong data, or incorrect data, it's very easy to focus on or prioritize the wrong threats!

Overall, in fact, respondents were less satisfied in most categories compared to 2017. Searching and reporting satisfaction increased slightly, which may indicate that integration and event management tools are improving in speed and efficiency.

Table 4. CTI Satisfaction

CTI Element	Overall Satisfaction	Not Satisfied
Automation and integration of threat intelligence with detection and response systems	63.0%	35.43%
Cleanliness and quality of data	68.5%	29.13%
Comprehensiveness of coverage	65.4%	32.28%
Context	65.4%	33.07%
Integrated data feeds	63.8%	33.07%
Location-based visibility	52.0%	43.31%
Machine learning/Analytics	39.4%	55.91%
Identification and removal of expired IOCs and other old data	37.8%	57.48%
Relevance of threat data and information	69.3%	26.77%
Reports (strategic and operational level)	70.9%	25.20%
Searching and reporting	76.4%	20.47%
Timeliness of threat data and intelligence	70.1%	28.35%
Visibility into threats and IOCs	70.9%	25.98%
Other	14.2%	6.30%

CTI Is Helping

Is CTI helping organizations do a better job of detecting threats, or ideally preventing those threats from manifesting altogether? In a nutshell: Yes. In one of the clearest trends we've seen over the past three years, respondents have increasingly stated that CTI is improving their prevention, detection and response capabilities. In 2018, 81% affirmed that CTI is helping, compared to 78% in 2017 and 64% in 2016. In addition, the number of respondents who answered "unknown" (in other words, they didn't feel they could answer the question confidently) has steadily decreased from 34% in 2016 to 21% in 2017, and now to only 15% in 2018.

This is definite proof that CTI is helping more organizations, and we're more comfortable measuring that improvement. That's not to say we aren't still experiencing some uncertainty in how best to quantify improvements. For example:

- For improvements in prevention, many (29%) are still uncertain, but 19% feel that CTI has improved prevention by as much as 51–75%.
- The highest percentage improvement in detection (25%) is in the 26–50% range, and that same range is the highest for response (19%).
- However, 28% are still uncertain about improvement in detection, and another 25% feel this way about response improvements.

See the full breakdown in Table 5.

Table 5. CTI Improvement Metrics

	Unknown	No Improvement	1–5%	6–10%	11–25%	26–50%	51–75%	76–100%
Prevention	29.3%	0.0%	2.4%	11.4%	18.7%	16.3%	18.7%	3.3%
Detection	27.6%	0.8%	0.8%	10.6%	9.8%	25.2%	15.4%	8.1%
Response	25.2%	0.8%	4.1%	10.6%	10.6%	18.7%	8.9%	8.9%

Of those who felt their security and response capabilities had improved with CTI, the majority felt they had better visibility into threats and attack methodologies, which increased slightly from 2017 but was still the top improvement overall. Additional improvements were noted in security operations (a close second), which was tied with detecting unknown threats in 2017.

The largest improvements from last year were in improving security operations (increased from 63% to 70%), preventing damage to business systems or data (increased from 36% to 45%), reducing time to identify and respond to incidents (increased from 50% to 59%), and revealing vulnerabilities where we could implement new controls (increased from 48% to 59%). See Figure 9 for the entire list of CTI security improvements in 2018.

As stated earlier, the highest degree of CTI satisfaction came through visibility into threats and indicators of compromise (71% indicated overall satisfaction, of which 20% were very satisfied). This reinforces the trends we're seeing that indicate CTI is being primarily aligned with the SOC, and tying into operational activities such as security monitoring, threat hunting and incident response.

How has the use of CTI improved your security and response? *Select all that apply.*

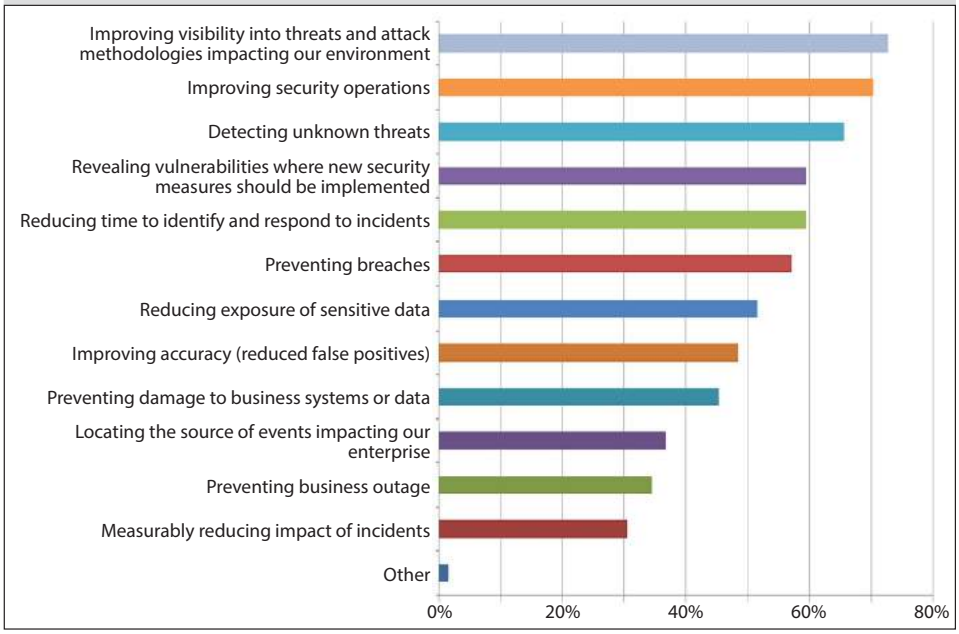

Figure 9. CTI Security and Response Improvements

Challenges and Barriers

As in years past, the top roadblock to successfully implementing CTI programs is a lack of trained and experienced staff. This is even more prominent in 2018 (62%) versus 2017 (53%), which likely coincides with CTI's growing prominence in the SOC. Budget is still an issue, which coincides with 2017 as well. In fact, the top four inhibitors from 2018 were the same as 2017 (lack of trained and experienced staff, budget, lack of time, and lack of technical ability to integrate CTI). In 2017, lack of management buy-in was a bigger issue than in 2018, however. See Figure 10.

What inhibitors are holding your organization back from implementing CTI effectively? *Select all that apply.*

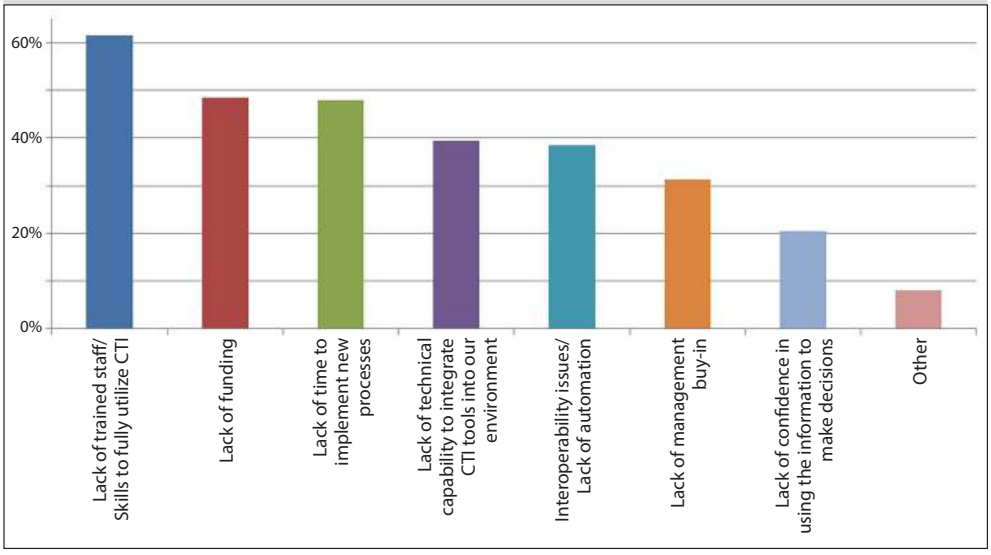

Figure 10. Challenges with CTI

While the tools and data seem to be improving in general, we are still struggling to find the right people and skills (and sadly, budget) to properly implement CTI as we'd need and like. According to John Pescatore, SANS' director of emerging technologies, increasing automation and adding more staff are not the approaches organizations should take. He says, "The real successes in cyber security have been where skills are continually upgraded, staff growth is moderate and next-generation cyber security tools are used to act as 'force multipliers' that enable limited staff to keep up with the speed of both threats and business demands."[3]

[3] "SANS Cybersecurity Trends and Predictions for 2018," December 2018, www.informationsecuritybuzz.com/expert-comments/sans-cybersecurity-trends-predictions-2018

Given the growing usefulness of CTI in helping with security operations and response, the lack of people and tools is surprising to see again in this year's survey. Some respondents suggested that improvement of "plug and play" tools, integration capabilities and ease of use could help organizations overcome skills gaps. Unfortunately, CTI will still require some commitment of resources, which still seems to be a struggle. While SANS does offer a course on CTI (noted in the "Executive Summary" of this paper), there seems to be very little substitute for experience.

Conclusion

Based on the responses to this year's survey, we're definitely seeing several trends emerge. CTI seems to be most practically useful to operations teams who are monitoring events in the environment, looking actively for threats and responding to incidents.

This year, we saw an emphasis on highly specific areas of focus, including detailed information on malware, vulnerabilities that attackers target, and specific indicators teams can use in threat hunting and response activities. Broad attacker trends are still highly useful, too, but more and more, the usefulness of CTI comes down to rapid detection and response, managing discovered vulnerabilities, as well as prevention when possible. This calls for continued integration and interoperability on the part of CTI vendors, plus detection and response tools.

CTI is becoming more common and useful for security operations teams, and likely others as well. Training for security staff and acquiring budget for CTI programs continue to plague many organizations, even though the trends easily show that CTI is providing value currently and will likely continue to do so in the future. As products mature and become easier to use, this may help to some degree by allowing more junior security staff to "level up" and make practical use of CTI in more ways.

About the Author

Dave Shackleford, a SANS analyst, instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this survey's sponsor:

DOMAINTOOLS®