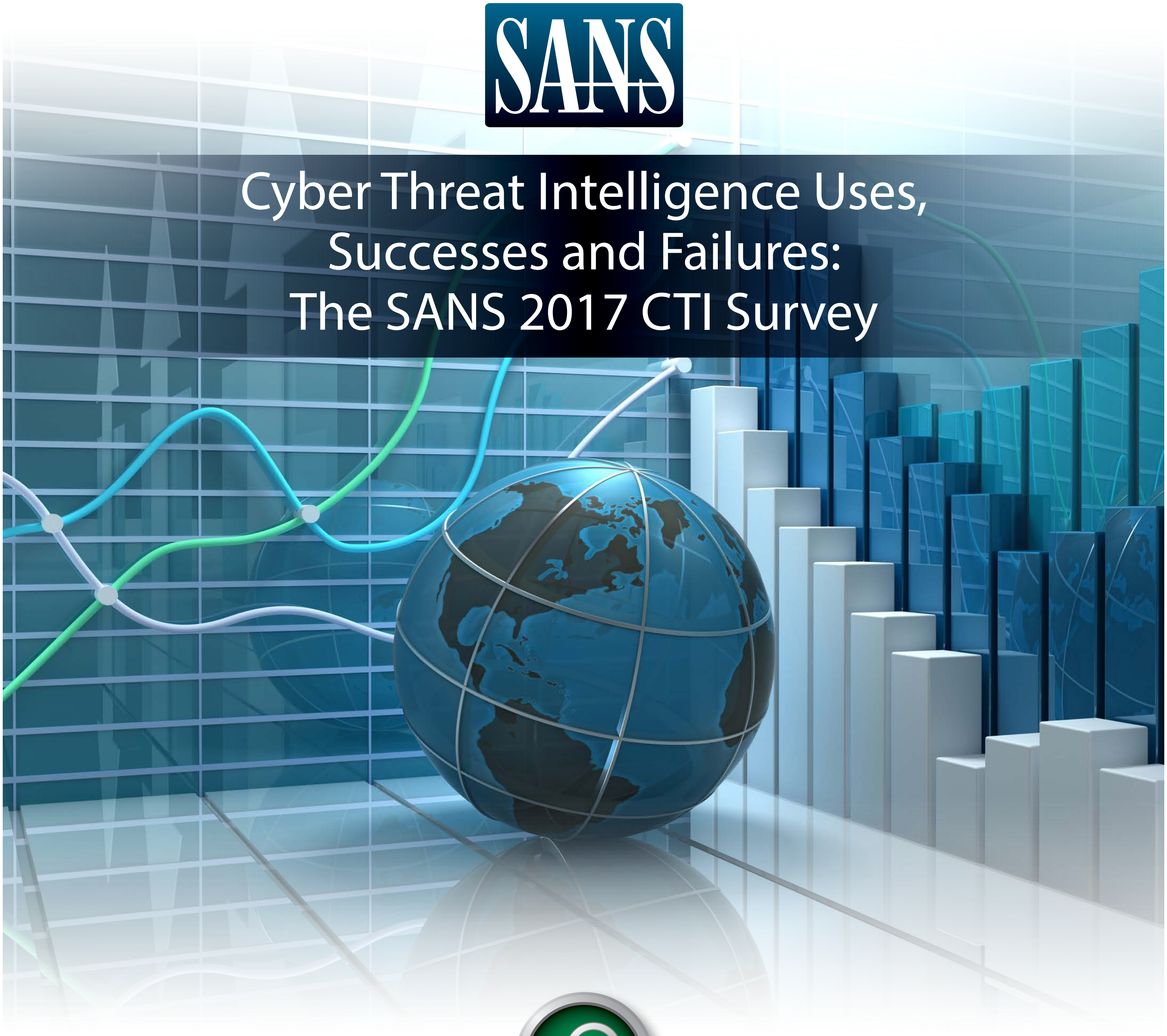
Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey

Respondents' biggest challenges to effective implementation of cyber threat intelligence (CTI) are lack of trained staff, funding, time to implement new processes, and technical capability to integrate CTI, as well as limited management support. Those challenges indicate a need for more training and easier, more intuitive tools and processes to support the use of CTI in today's networks. These and other trends and best practices are covered in this report.

Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey



A SANS Survey

Written by Dave Shackleford

Advisor: Robert M. Lee

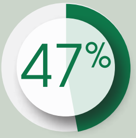
March 2017

Sponsored by
Anomali, Arbor Networks, DomainTools, LookingGlass Cyber Solutions, Rapid7, and ThreatConnect

Executive Summary

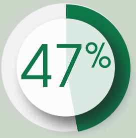
CTI Teams and Skills

actively use CTI, with another **25%** planning to

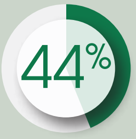


have a dedicated team that focuses on CTI

—the vast majority—operate from the cyber security teams



utilize in-house staff combined with service providers to conduct CTI



rate awareness of attack patterns and indicators of compromise (IoCs) as their most in-demand skills for leveraging CTI in detection and response

Over the past year, Yahoo revealed the largest data breaches in history,[1] and nation-state hacking activity was suspected in tampering with the U.S. presidential election.[2] More vulnerabilities are being found (and exploited) in mobile and Internet of Things (IoT) platforms, and the first true IoT botnet (Mirai) became a threat that was operationalized to take down Deutsche Telecom, KCOM and Irish telco Eir in December 2016. The attacks continue to spread through different types of IoT devices and target more businesses, types of routers, and other devices they can use to wreak havoc on the businesses they target.[3]

Malware is more sophisticated in avoiding detection, and ransomware has become the top threat affecting organizations,[4] according to the SANS 2016 Threat Landscape Survey. IT security teams are struggling just to keep up, as they have throughout Internet history, let alone get ahead of the attackers. Cyber threat intelligence (CTI) shows promise in making these types of threats easier to detect and respond to, according to our recently conducted survey on cyber threat intelligence. In this, our third survey on CTI, 60% of organizations overall are using CTI, while another 25% plan to. As we might expect, small organizations with fewer than 2,000 employees are less likely to plan to use CTI. Of those using CTI, 78% felt that it had improved their security and response capabilities, up from 64% in our 2016 CTI survey.

CTI Defined

The SANS CTI Forensics course defines CTI as the "collection, classification, and exploitation of knowledge about adversaries."[5] This includes, in particular, information about adversaries' tactics in order to detect and block them. As one of the course's primary authors describes it, "CTI is analyzed information about the intent, opportunity and capability of cyber threats."

Exploits on removable media forced us to implement controls banning their use in our info system. Without credible CTI and use cases, we would not have known to implement the control in our organization.

—2017 CTI survey respondent

CTI adopters are also facing challenges. In this survey, their biggest challenges to the effective implementation of CTI are a lack of trained staff, lack of funding, lack of time to implement new processes, and lack of technical capability to integrate CTI, as well as limited management support. Those challenges indicate a need for more training, as well as easier, more intuitive tools and processes to support the ever-growing use of CTI in today's networks.

These and other trends and best practices are covered in this report.

[1] www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0

[2] www.bbc.com/news/world-us-canada-38538002

[3] www.theregister.co.uk/2016/12/02/broadband_mirai_takedown_analysis

[4] "Exploits at the Endpoint: SANS 2016 Threat Landscape Survey," www.sans.org/reading-room/whitepapers/firewalls/exploits-endpoint-2016-threat-landscape-survey-37157

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

Who’s Using CTI

Of the 600 respondents to take this survey, 60% utilize CTI for detection and response, while another 25% plan to the future. The remaining 15% have no plans to adopt CTI practices.

Who Took This Survey

Respondents represented a broad range of industries. The top verticals included government, banking and finance, technology, and cyber security, with a mix of others that include education, healthcare, manufacturing and telecommunications. Thirty-eight percent of respondents worked in organizations with 2,000–50,000 employees, and 19% were in organizations larger than 50,000. Forty-three percent of organizations represented have 2,000 employees or fewer. See Figure 1.

What is the size of the workforce at your organization, including employees, contractors and consultants?

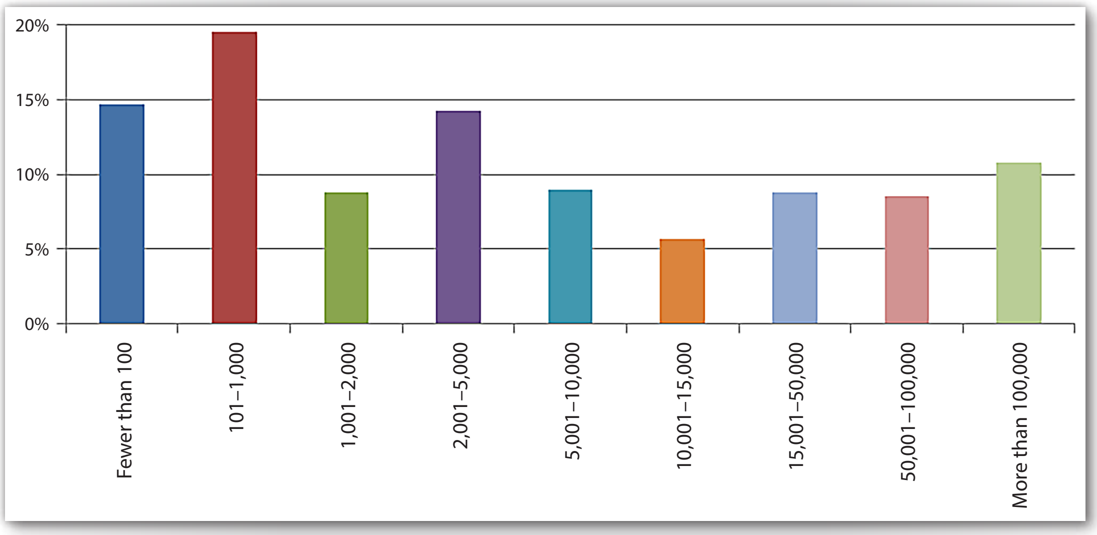


Figure 1. Workforce Size

The majority of organizations have operations in the United States (over 75%), with 40% operating in Europe and 34% in Asia. A mix of organizations has operations in Canada, Australia/New Zealand, the Middle East, South America and Africa, too. The U.S. housed the headquarters of 67%, with 13% based in Europe and 7% headquartered in Asia.

The roles of respondents also varied widely. Security administrators or analysts made up 25% of the sample (far fewer than last year), with another 13% 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. This year, 6% of respondents carry the title of “cyber threat intelligence analyst” or a similar title, compared to 1% who held such a role in 2016.[6]

[6] ”The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing,” www.sans.org/reading-room/whitepapers/analyst/state-cyber-threat-intelligence-survey-cti-important-maturing-37177

Raw Threat Intelligence

Indicators of compromise and other potential identifiers of malicious behavior that can be used to look for threats or apply preventive, detective or responsive actions

Finished Intelligence Report

Threat intelligence data that has been analyzed in context with other information and applied specifically to the organization and its use cases

Using Threat Intelligence

As security teams become more comfortable with leveraging CTI, many are constantly seeking new and varied sources of threat data. This year's survey reveals a significant shift toward developing internal threat intelligence, as well. Currently, 8% of teams are producing raw threat intelligence, with another 7% producing finished reports on their own.

The majority are still consuming data from elsewhere, though, with roughly 40% consuming raw data and 47% consuming finished intelligence reports from vendors and other sources. Many are also producing and consuming both, as shown in Figure 2.

Indicate whether your organization produces or consumes cyber threat intelligence (CTI) in terms of raw data and/or finished threat intelligence reports.

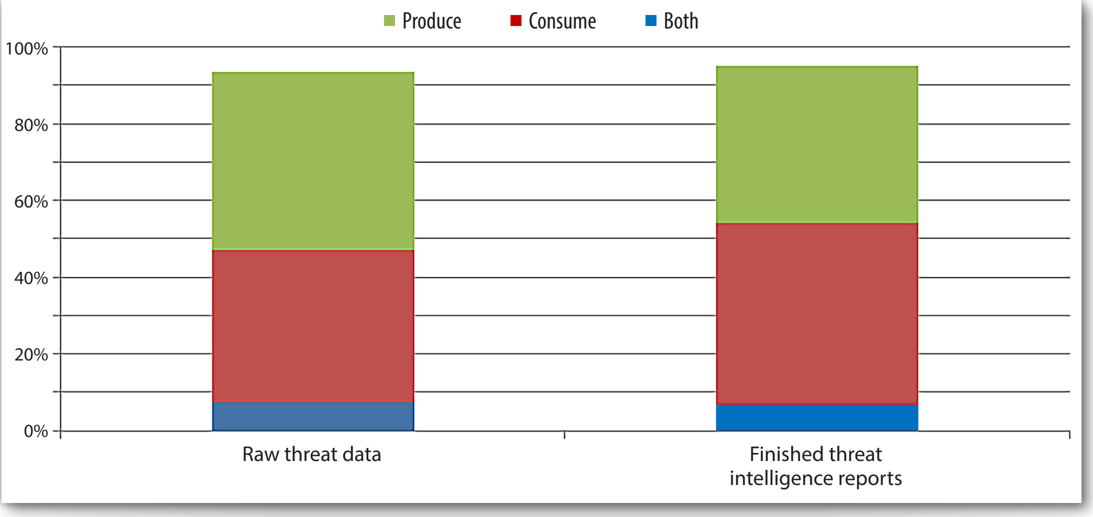


Figure 2. CTI Production/Consumption

Raw CTI data creation and consumption are critical for organizations to cultivate, as these data are the most usable in correlation and analysis. This can be incredibly time-consuming, however. Consuming "finished" threat intelligence reports from outside sources is most definitely the easiest way to obtain this threat data and potentially put it to use.

CTI Data Sources

On that note, we saw organizations leveraging a wide variety of external CTI sources in 2017. The top source by a significant margin included industry and community groups such as computer emergency readiness teams (CERTs) and information sharing and analysis centers (ISACs; 73%). This was largely the same as 2016 (74%). The second most-utilized source of CTI changed radically from 2016, however. In 2017, 54% gathered CTI from a variety of internal sources, including security and operations tools. In 2016, internal sources were fourth (46%), with the second and third most popular sources being security vendor feeds and open source/public feeds. Vendor feeds and open source/public feeds came in third (52%) and fourth (50%), respectively, in 2017. See the full 2017 results in Figure 3.

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

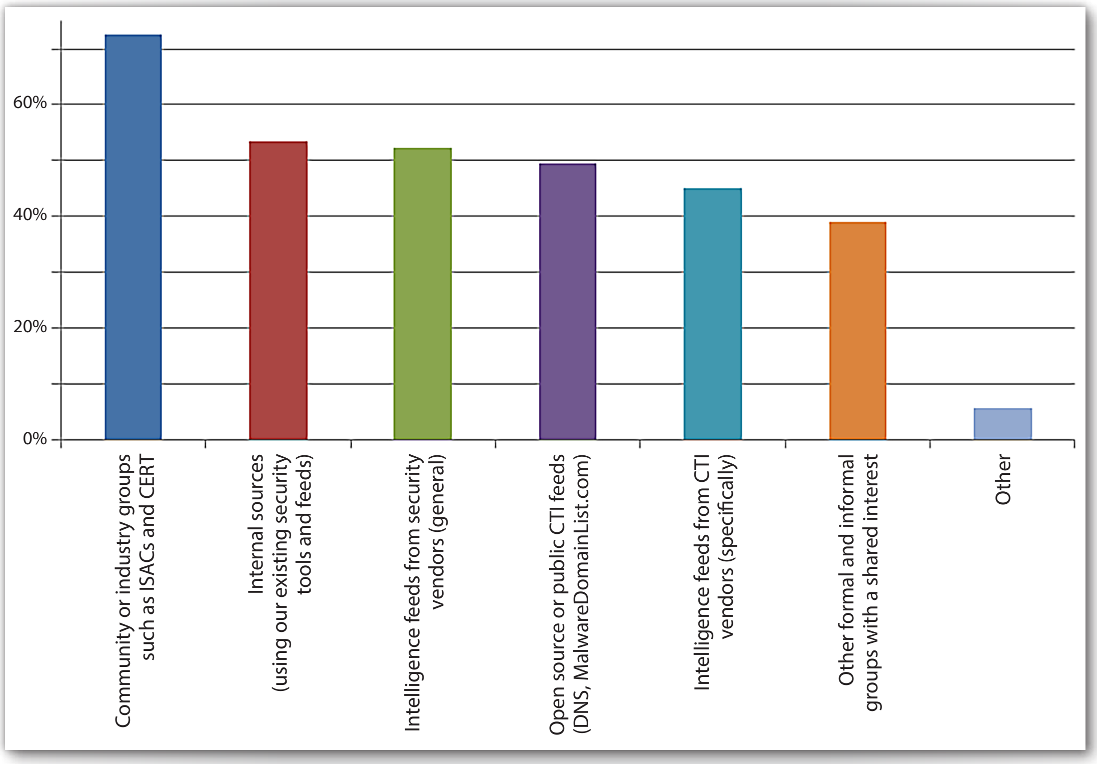


Figure 3. CTI Sources

Looking at the data in Figure 3, this seems to suggest that more and more organizations are choosing a hybrid model of CTI data collection, with a mix of external and internal sources.

Managing CTI Data

Of those who knew how many threat indicators their systems could successfully integrate into their workloads, 19% (the largest group) said they can handle roughly 11–100 indicators coming in, while 22% can effectively utilize 1–10 per week. The full breakdown of responses is shown in Table 1.

TAKEAWAY

As more vendors and sources of data enter the CTI ecosystem, the need to scale and, more importantly, to refine data to make it relevant, will become more critical for CTI collection and analytics.

Table 1. Volume of CTI Data

Number of Threat Indicators/Week	Receive	Effectively Utilize
Unknown	35.0%	43.6%
None	0.4%	0.4%
1–10	12.0%	22.2%
11–100	19.2%	12.8%
101–250	7.3%	7.3%
251–500	3.0%	2.1%
501–1,000	7.7%	2.6%
1,001–5,000	2.6%	3.8%
5,001–10,000	1.3%	1.7%
10,001–100,000	4.7%	1.7%
100,001–1,000,000	3.0%	0.4%
1,000,001–10,000,000	2.1%	1.3%
Greater than 10,000,000	1.7%	0.0%

These results differ from our 2016 survey, in which larger percentages of respondents said their organizations effectively utilize between 1 and 100 indicators on a weekly basis. In 2017, respondents report that their organizations can effectively utilize more than 100 indicators effectively.

However, these numbers are estimates on the part of respondents. The vast majority stated that they just didn't know how many indicators they received or could use. And, given the relative immaturity of CTI, this may be the case for some time to come. Of course, this could also signal a gap in what vendors and customers understand about threat intelligence, with vendors providing information about how organizations can consume intelligence efficiently that customers may not yet understand.

Threat Intel Teams

Whether producing or consuming CTI, almost 47% of respondents indicated that they have a formal team dedicated to CTI currently, which is up significantly from 2016 (28%). Another 9% have a single team member dedicated to CTI (a decrease from the 18% in 2016), which indicates that the size of CTI teams is growing. Another 26% of respondents stated they don’t currently have a person or team dedicated to CTI, but treat it as a shared responsibility between security groups (see Figure 4).

Does your organization have resources that focus on CTI?

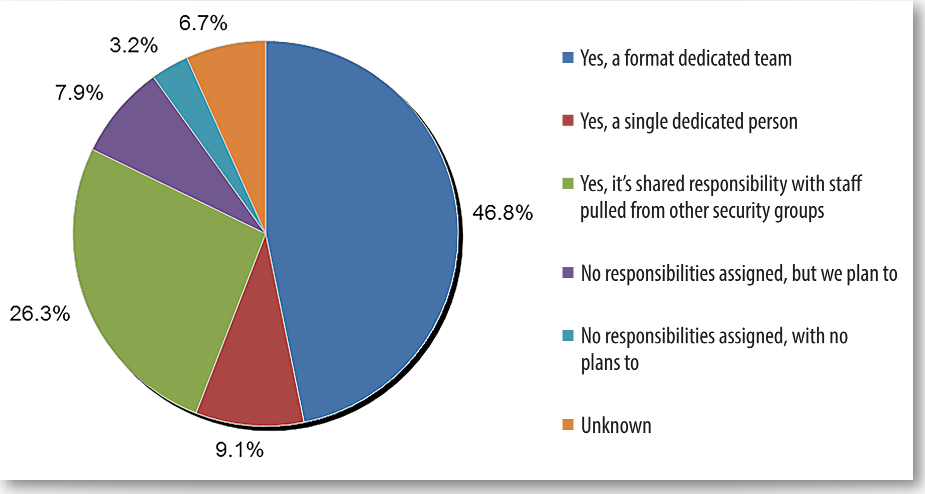


Figure 4. Staff and Team Allocation for CTI

In-house and in-house/outsourced CTI is almost evenly split: Most organizations employ an in-house team (48%), with another 47% outsourcing some aspects of this function. Only 6% outsource CTI entirely.[7] Sources of outsourced information can provide different intel, and perhaps different expertise and experience, but the trend is clearly moving toward more in-house CTI collection and management.

[7] The total is more than 100% due to rounding error.

Those organizations that do have dedicated staff for CTI predominantly situate them in the cyber security and incident response (IR) groups, similar to 2016, where most organizations had CTI-focused staff in the security operations center (SOC) and IR teams. Other 2017 respondents have CTI-focused staff in the enterprise security team, with a smaller number assigning these functions to IT teams, dedicated CTI teams or vulnerability management teams (see Figure 5).

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

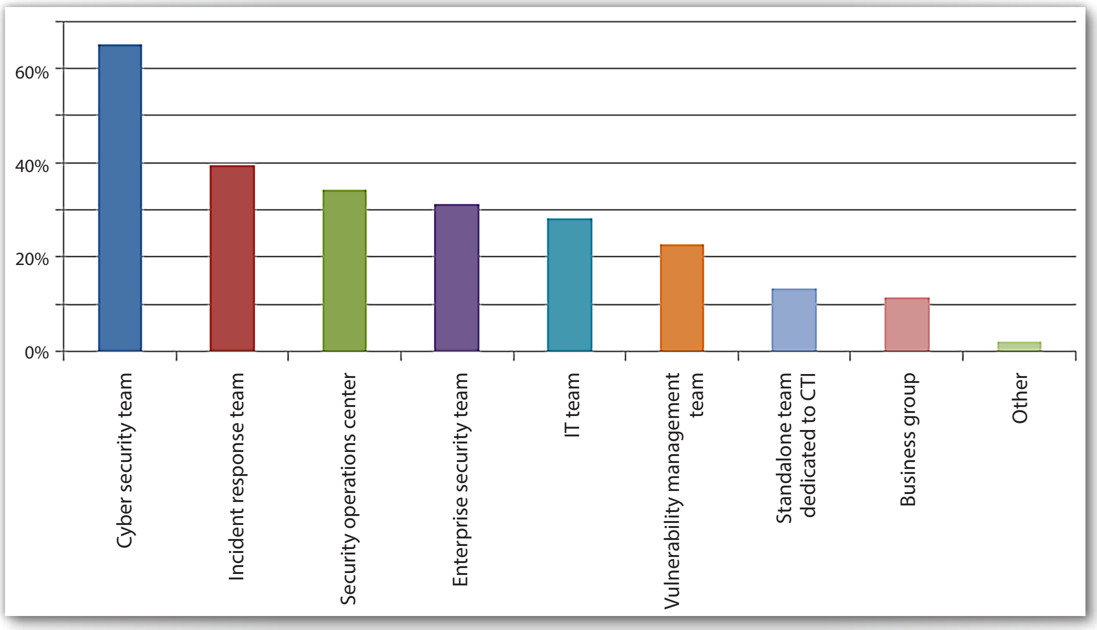


Figure 5. CTI Team and Staff Location

Note that respondents could select multiple responses, indicating that there is an overlap where the team members fill multiple roles and, thus reside in multiple locations, in both security and IR teams, for example. In fact, 41% chose just one location for team members, while the remaining 59% chose between two and eight locations, with three locations accounting for 14% of respondents.

Responses indicate the need for highly specialized skills that are hard to come by. The overall most valuable skills listed were awareness of attack patterns and indicators of compromise (IOCs), intelligence analysis, incident response, and knowledge of normal and abnormal behaviors.

In 2016, correlation rule creation and knowledge of adversaries and campaigns were considered the most valuable skills for utilizing CTI. In this year's survey, awareness of attack patterns and knowledge of IoCs, intelligence analysis and incident response are the overall top skills needed to utilize CTI.

This year, correlation and analysis ranked fifth in overall value, preceded by knowledge of normal and abnormal behavior, while presentation and communication were ranked as the overall least valuable for using CTI (see Figure 6).

What skill sets are most valuable in leveraging CTI in detection and response?

Please identify your top 3, with "1" being the most valuable.

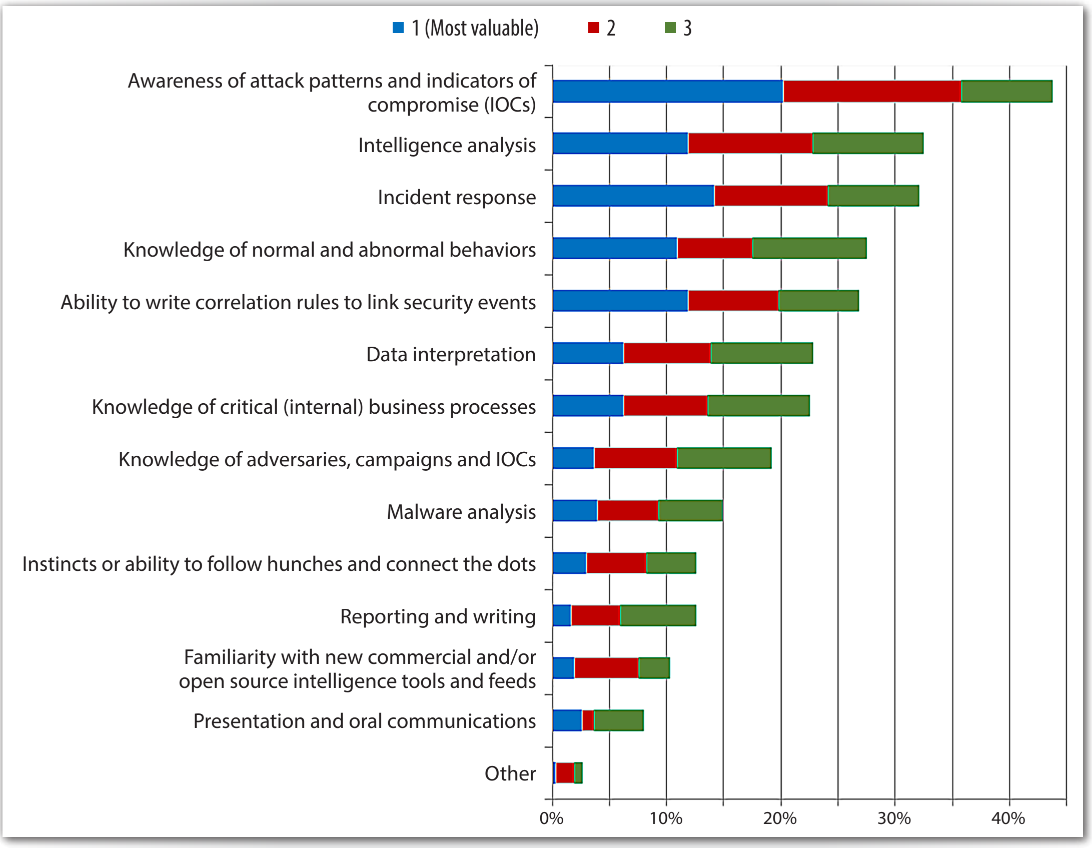


Figure 6. Valuable Skills for Leveraging CTI

TAKEAWAY

Team members with skills in intelligence analysis, incident response, and knowledge of normal and abnormal behavior and analysis will be in high demand for CTI work.

For organizations looking to improve their CTI skills, experience in detecting and responding to attacks is important; thus, dedicated CTI analysts could likely come from the SOC or IR teams. The ability to communicate threats and security posture, CTI reporting and data interpretation will need to improve, including the ability to understand and map vulnerabilities to the threat indicators, new intelligence sources and more.

CTI Uses and Benefits

Just as the largest group of respondents is housing its CTI teams in its cyber security departments, the majority of respondents (72%) are utilizing CTI information in security operations (locating sources and/or blocking malicious activities or threats). The same percentage of respondents (72%) is also using CTI for incident response. The full breakdown of responses is shown in Figure 7.

TAKEAWAY:

Given that we need intelligence and data analysis skills, as well as correlation and response skills, it's not surprising that many organizations are seeking to implement CTI in security operations (perhaps in the SOC) and IT teams.

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

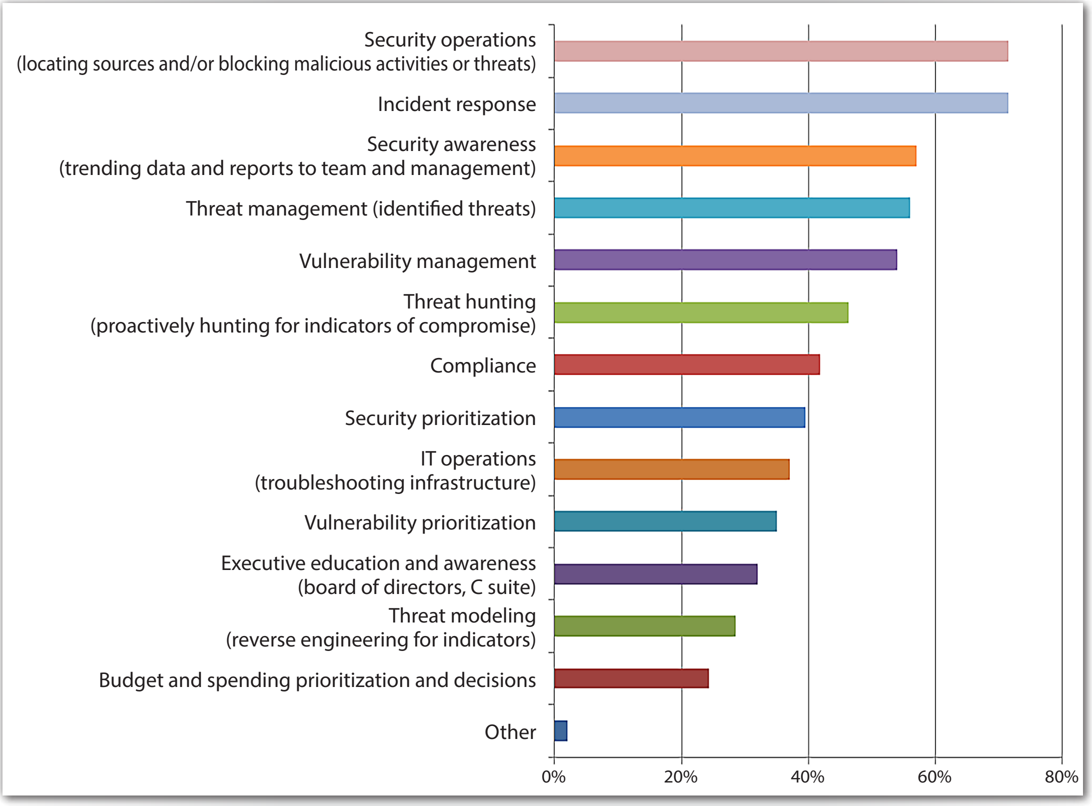


Figure 7. Top Use Cases for CTI Feed Data

Reutilizing the information for security awareness activities, threat management, vulnerability management and threat hunting were also very popular uses.

In the case of security awareness, results indicate that CTI is making inroads into end user and business-oriented security training and processes—in other words, asking: Who is attacking us, how are they attacking us, and how can we be ready?

When our SOC encounters malware threats, [its employees] send out announcements to the staff and give them information on how to handle suspicious events.

—2017 CTI survey respondent

CTI is used to generate scenarios and indicators of compromise, which are then used to inform the development of our detection capabilities. The CTI and stats around numbers of detected incidents are passed to the risk team, who can then use this information to ensure that cyber security controls are taken seriously and correctly prioritised.

—2017 CTI survey respondent

For a recent example [of how CTI can be used]: our immediate awareness of [the] Mirai botnet attack against critical DNS infrastructure.

—2017 CTI survey respondent

Real-Life Examples of CTI Usage

When we asked organizations to give specific examples of CTI use in the environment, more than 100 respondents wrote thoughtful answers that fell into these categories:

- Proactively stopping malware, ransomware and advanced threats
- Improving detection capabilities
- Threat modeling
- Prioritizing security and response
- Detecting phishing emails, desktop-related targeting and end user application compromise
- Reusing data for security staff awareness

Improvements with CTI

The majority of respondents (78%) felt that CTI had improved their security (protection and detection) and response capabilities, which is a significant increase from 2016, where 64% saw such improvements. In 2016, only 3% indicated that CTI *hadn't* improved detection and response, and that number went down to 2% in 2017. The remaining respondents weren't sure.

This, along with previous surveys, reveals an increase in usefulness and effectiveness of CTI for security operations and IR over the past two years. So this year, we also looked into how CTI usage has improved an organization's ability to prevent, detect and respond to threats. See Table 2 for results.

Table 2. Improvement Rates in Prevention/Detection and Response

Percentage Improvement	Security (Prevention and Detection)	Response
Unknown	29.0%	31.0%
No improvement	0.0%	0.5%
1–5%	3.0%	3.5%
6–10%	7.0%	8.5%
11–25%	17.5%	18.0%
26–50%	17.5%	18.0%
51–75%	19.0%	10.5%
76–100%	7.0%	10.0%

Unfortunately, 29% of respondents do not know by what percentage prevention and detection capabilities had been improved as a result of using CTI. This may speak to the need for organizations to measure their performance by a standard set of metrics. It is noteworthy, however, that not a single respondent stated that there was *no* improvement in prevention/detection capabilities.

Measures of Improvement

Of those who can quantify improvements in detection and prevention, 19% (the largest group) are experiencing 51–75% improvement, whereas only 11% experienced this level of improvement in incident response. With respect to improvements in response, two ranges tied for the highest percentage of improvement at 18%: 11–25% and 26–50%.

When it comes to response, fewer organizations can actually measure their level of improvements than in last year's survey. In 2016, 19% of security teams responded that they did not know how much their response had improved with CTI; in 2017, 31% don't know. In 2016, 3% stated that they saw no discernible improvement in response from using CTI, and that number is down to 1% this year, but the rest of the improvement categories are very spread out.

The perception that breaches were actually prevented and that "unknown" threats were detected is a very positive change from previous years.

Effectiveness of CTI

For those who felt that their security and response capabilities had improved, the majority (72%) felt that they have better visibility into threats and attack methodologies, a slight increase over 2016. In our 2017 survey, additional progress was noted in improving security operations and detecting unknown threats (both with 63%), as well as preventing breaches and improving incident detection and response times (both just over 50%). See Figure 8.

Both SOC teams and response and forensics teams will immediately benefit from greater visibility into attack methods and threats, as well as improved detection and response times.

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

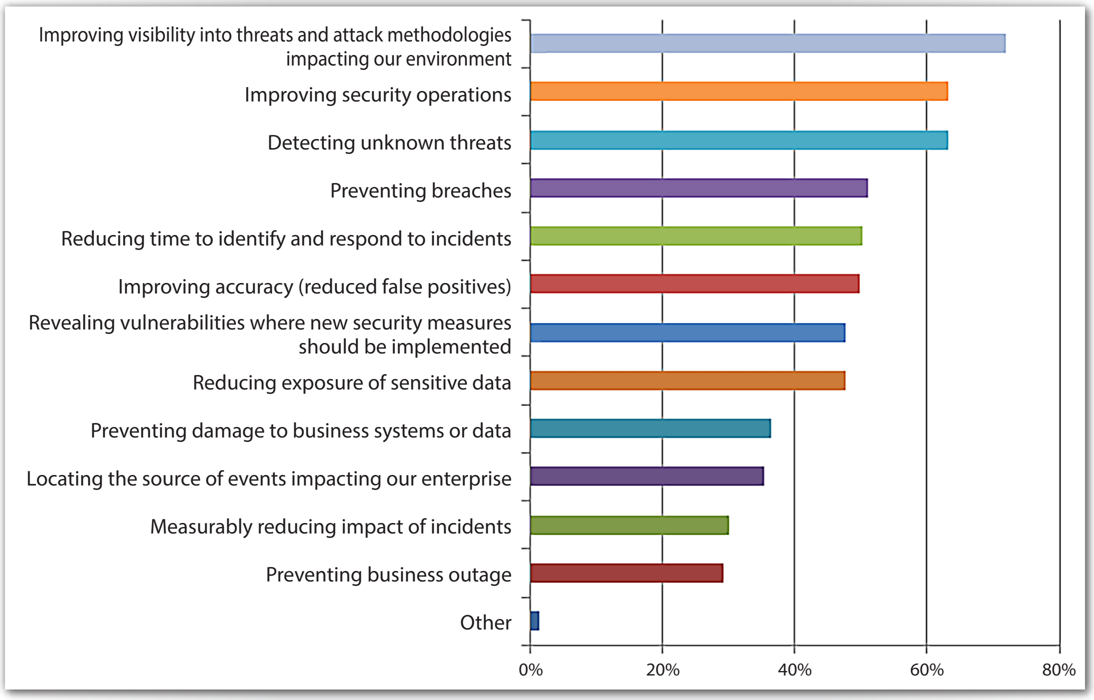


Figure 8. CTI Security and Response Improvements

As in years past, quantitative improvements, such as measurably reducing the impact of incidents, saw fewer respondents feeling confident that CTI had provided benefits. This may still reflect a lack of maturity in CTI implementation and program integration, but the perception that breaches had actually been prevented and "unknown" threats had been detected is a very positive change from years past, and could indicate that we're slowly seeing CTI use become better understood.

CTI Data Aggregation

Security teams are using a broad variety of tools to aggregate, analyze and present CTI in their environments. In 2016, 43% were using security information and event management (SIEM) systems in an integrated GUI, and another 26% used SIEM disparately with other tools and components. In 2017, SIEM is still the top tool for managing and using CTI, with slightly higher numbers (46% with a GUI and 27%, disparately). See Figure 9.

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.

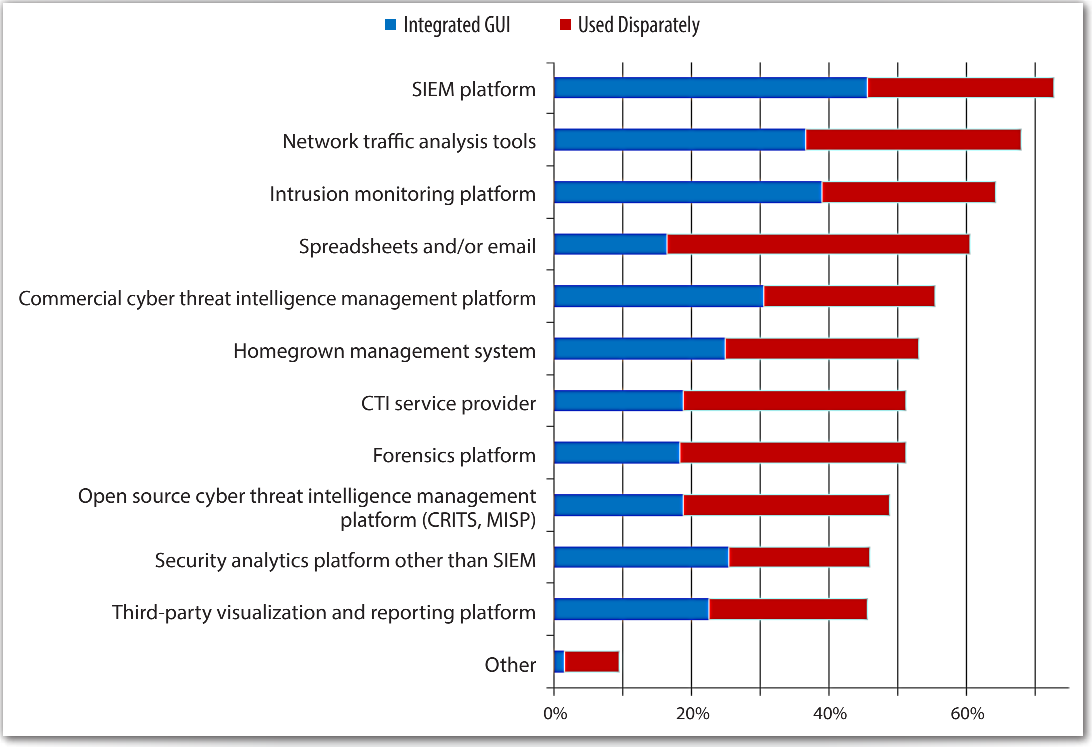


Figure 9. CTI Integration and Analysis Tools

Last year, intrusion monitoring platforms were a close second, also predominantly within a central GUI. In 2017, however, intrusion monitoring tools were third, behind network traffic analysis tools (mostly using a unified GUI as well). Commercial CTI management platforms were fifth this year, compared to third in 2016.

We were surprised to see spreadsheets taking fourth place at 61% utilization, given that they are not scalable or practical data management tools for most organizations with any real volume of data. It's as interesting to see that the commercial CTI tools, and even home-grown management, analytics platforms and third-party tools are more commonly used under the umbrella of an integrated GUI. This suggests that optimization is occurring, primarily through the vendor community.

Open source CTI platforms were used more often than in 2016 (in 2017, 49% used open source, compared to 43% in 2016), but they still required more disparate integration and coordination with other tools. Homegrown tools, analytics platforms, business intelligence tools and forensics tools were also cited.

CTI Integration

Anywhere from 20% to 47% of respondent organizations are using disparate intelligence feeds rather than through an integrated GUI, indicating a continued need for improvements in integrated visualization and workflow. Most respondent organizations are using APIs (47% are using vendor-provided APIs, and 46% are using custom APIs) to integrate security feeds into their environments. In addition to these tools, 41% use dedicated threat intelligence platforms (both commercial and open source). See Figure 10.

How are these intelligence feeds integrated into your defense and response systems?
Select all that apply.

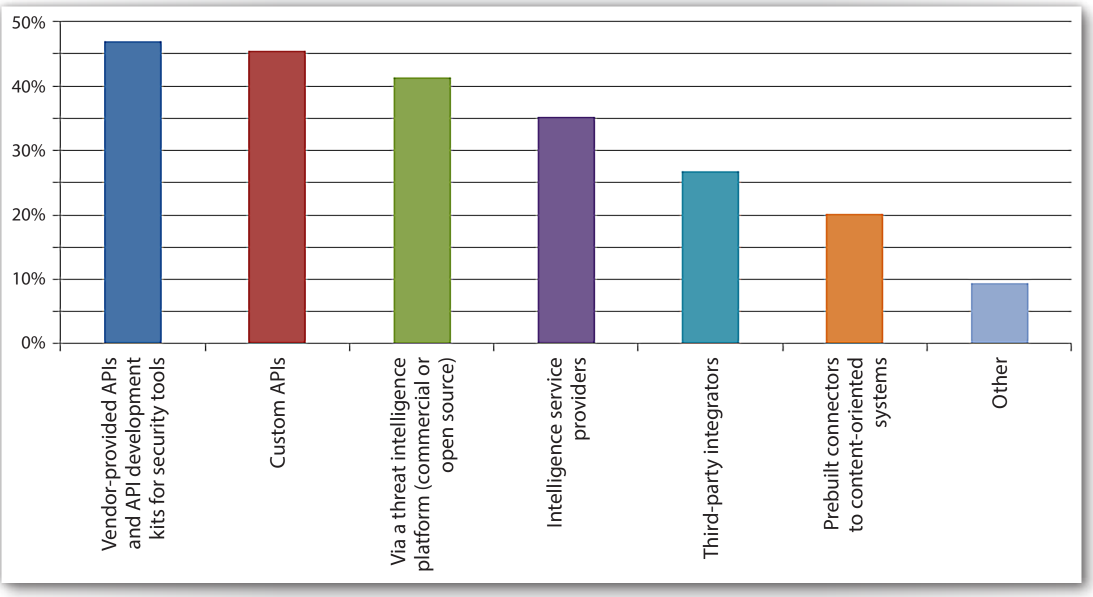


Figure 10. CTI Feed Integration

Given that so many organizations are using SIEM, network analysis tools and intrusion monitoring tools for managing and using threat intelligence, it makes sense that API-driven integration with these platforms would be prevalent.

CTI Reporting

More organizations are using CTI and procuring it from a number of sources. Many are also relying on external providers to get CTI reports, although some are also developing their own internally. Roughly 51% of respondents stated that their CTI reports and data are good, but they need some manual "cleaning" and manipulation. Only 14% felt that the reports were excellent, integrating cleanly into their detection and response programs today.

However, 32% acknowledged getting CTI data but not currently knowing how to make use of it. This goes back to the issues with normalizing and filtering the data for applicability in the target enterprise. Only 1% of respondents said CTI is currently entirely useless to them.

Organizations are using a variety of standards and frameworks to support feed integration, analysis and reporting. In our survey, 40% of respondents (the majority) are using Structured Threat Information Expression (STIX™). The Open Indicators of Compromise (OpenIOC) framework came in second this year with 38%, and the Collective Intelligence Framework (CIF) came in third at 32%. Many organizations marked the "other" category and listed commercial vendors, homegrown tools and more. The complete list is illustrated in Figure 11.

Percentage that collect CTI data but are unsure of how useful it is in their organizations

Which of the following standards or frameworks is your CTI information adhering to?
Select all that apply.

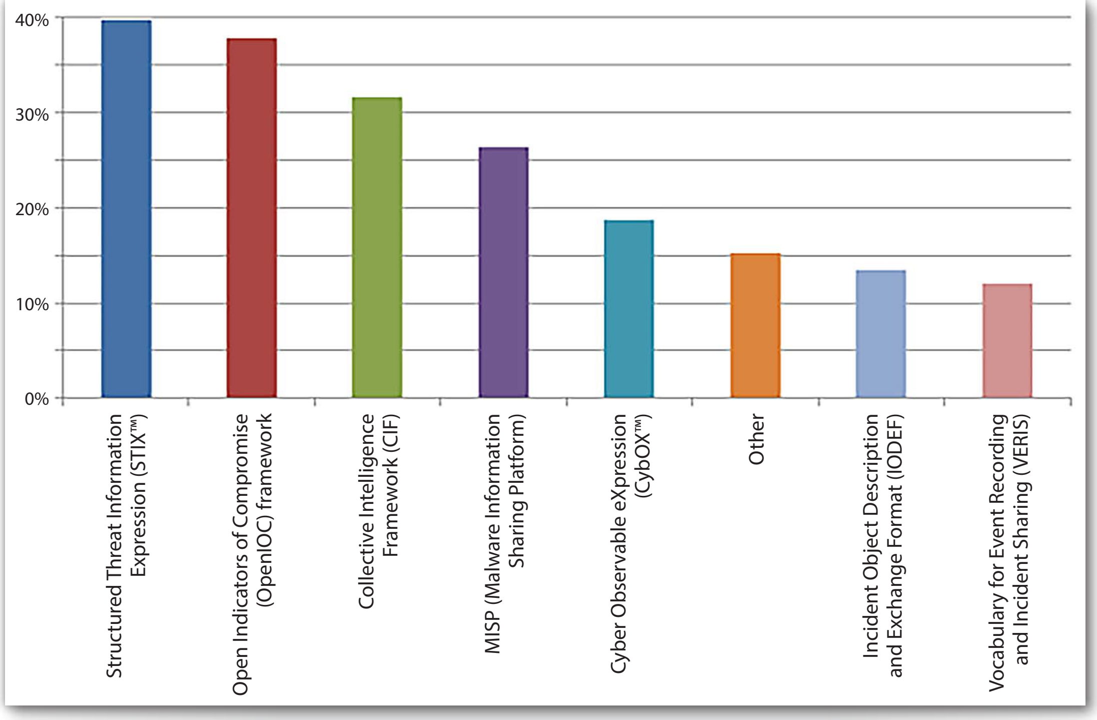


Figure 11. CTI Standards and Solutions

In contrast, in 2016 STIX™ was used by 29% of organizations, CIF was second with 26% and OpenIOC was third with 17%. All in all, not a major change year to year. Looking back over the past several years, we've seen some fluctuation in the types of tools and standards employed in CTI programs. Some of the MITRE standards, for example STIX™, have remained popular. But many community initiatives and tools have also emerged, including Cyber Observable Expression (CybOX™) and others. Today, it seems that there is no clear "winner" in these standards, although the same ones routinely surface as being the most prevalent overall.

Level of Satisfaction with CTI Elements

In general, teams are most satisfied with the relevance of threat data and information (80%), cleanliness and quality of data (76%), and timeliness of CTI and visibility into threats and IOCs (tied at 74% each). These are very critical points to note, given that most teams are leveraging CTI in their SOC and IR teams and finding the most valuable uses to be visibility into threats and attacks, as well as more rapid detection and response.

TAKEAWAY:

Organizations are getting good, relevant data in a timely fashion, which indicates that CTI providers and community sources are improving their game.

Table 3. Level of Satisfaction with CTI Elements

Answer Options	Very Satisfied	Satisfied	Overall Satisfied
Relevance of threat data and information	22.6%	57.6%	80.2%
Cleanliness and quality of data	14.7%	61.3%	76.0%
Timeliness of threat data and intelligence	23.0%	51.2%	74.2%
Visibility into threats and IOCs	18.4%	55.8%	74.2%
Reports (strategic and operational level)	21.7%	50.7%	72.4%
Comprehensiveness of coverage	18.0%	54.4%	72.4%
Searching and reporting	15.2%	57.1%	72.4%
Context	16.6%	54.8%	71.4%
Automation and integration of threat intelligence with detection and response systems	18.4%	51.2%	69.6%
Integrated data feeds	14.3%	54.8%	69.1%
Location-based visibility	15.2%	53.5%	68.7%
Identification and removal of expired IOCs and other old data	14.7%	46.5%	61.3%
Machine learning/Analytics	9.7%	39.2%	48.8%
Other	3.2%	8.3%	11.5%

TAKEAWAY:

Although satisfaction is generally high with reporting, CTI search capabilities, feed integration, and more, there is still much room to improve.

This is excellent news! We've still got a long way to go, though. Respondents were least satisfied with today's machine learning and analytics, identification and removal of expired IOCs and other old data, and location-based visibility.

Inhibitors to Effective Implementations

Similar to our 2016 responses, this year's majority (53%) felt that a lack of trained staff and skills are the biggest inhibitors to implementing effective CTI programs. Half of organizations said that a lack of funding is a major hurdle, and another 42% cited lack of time. See Figure 12.

Last year, a lack of management buy-in went up rapidly from 2015 (from 11% in 2015[8] to 35% in 2016). This number decreased slightly to 33% this year.

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

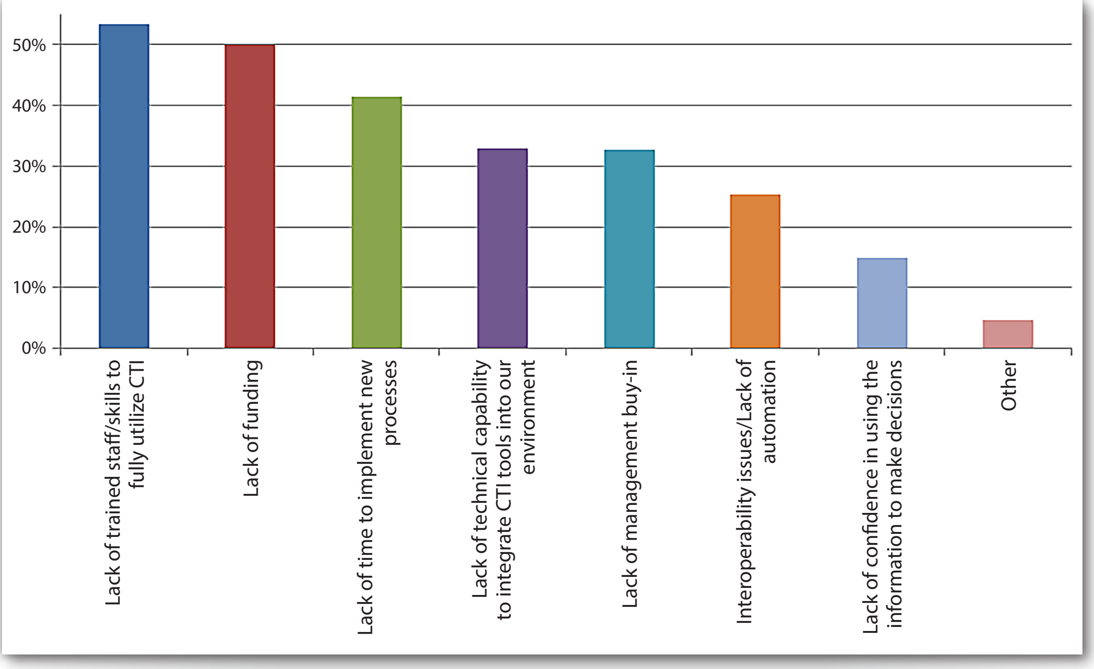


Figure 12. Challenges with CTI

The second most common issue from 2016, lack of technical integration capabilities, is now in fourth place in our 2017 survey (33%). This is a likely indicator that tools and CTI data are becoming more mature.

Other concerns include interoperability and automation challenges, as well as lack of confidence in using CTI to make decisions. Although 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 like. Given the usefulness of CTI in helping with security operations and response, this is surprising. However, we may be suffering from a lack of metrics and demonstrable improvements; recall that our "improvement percentages" were all over the map for all areas of security, likely showing us that we have no idea how to really demonstrate CTI's effectiveness to management.

[8] "Who's Using Cyberthreat Intelligence and How?" www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767

Conclusion and Looking Ahead

Based on this year's responses, it appears that CTI tools, technologies, capabilities and integration are improving. Security teams are finding more value than ever in collecting and using CTI for security operations and response (60% of teams are already using CTI, with another 25% planning to).

Integration of CTI into other tools and technologies is still immature; automation and analytics are still areas that need improvement; and we're still having trouble finding staff with the right skills. But this survey's results show we are moving in the right direction.

As we did in 2016, we asked survey respondents for their parting thoughts on what types of policies, standards, techniques, tools and intelligence feed data they feel are needed for future improvements in the use of CTI. A number of comments echoed sentiments already expressed in the data: that we need better integration and that standards are lacking. Many also expressed general dissatisfaction with the CTI data they see in feeds. One response stated that "most of the intel we receive is many years old." Others also acknowledged the fact that CTI is a tough sport, and there's not one type or source of CTI that will equally benefit everyone.

CTI is becoming more popular, more useful and more ubiquitous. We need more trained professionals who know what to do with this data and can build and maintain CTI programs and integration in large, complex organizations. We also need better metrics and reporting, especially given the fact that we're struggling for time and budget, with one-third of teams lacking management buy-in. As long as we can demonstrate the value that CTI brings in preventing, detecting and responding to today's attacks, we're likely to see CTI become more mature and important to security programs than ever.

About the Authoring Team

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.

Robert M. Lee (advisor), 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 cyber security company, where he focuses on control system traffic analysis, incident response and threat intelligence research. He has performed defense, intelligence and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Author of *SCADA and Me* and a nonresident National Cyber Security Fellow at New America, focusing on critical infrastructure cyber security policy issues, Robert was named EnergySec's 2015 Energy Sector Security Professional of the Year.

Sponsors

SANS would like to thank this survey's sponsors:

ANOMALI™

ARBOR® NETWORKS

DOMAINTOOLS®

LOOKINGGLASS

RAPID7

THREATCONNECT™

Last Updated: March 16th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tysons Corner Spring 2017	McLean, VAUS	Mar 20, 2017 - Mar 25, 2017	Live Event
SANS Abu Dhabi 2017	Abu Dhabi, AE	Mar 25, 2017 - Mar 30, 2017	Live Event
SANS Pen Test Austin 2017	Austin, TXUS	Mar 27, 2017 - Apr 01, 2017	Live Event
SANS NetWars at NSM Security Conference	Oslo, NO	Mar 28, 2017 - Mar 29, 2017	Live Event
SEC564: Red Team Ops	Atlanta, GAUS	Apr 06, 2017 - Apr 07, 2017	Live Event
SANS 2017	Orlando, FLUS	Apr 07, 2017 - Apr 14, 2017	Live Event
Threat Hunting and IR Summit	New Orleans, LAUS	Apr 18, 2017 - Apr 25, 2017	Live Event
SANS London April 2017	London, GB	Apr 24, 2017 - Apr 25, 2017	Live Event
SANS Baltimore Spring 2017	Baltimore, MDUS	Apr 24, 2017 - Apr 29, 2017	Live Event
Automotive Cybersecurity Summit	Detroit, MIUS	May 01, 2017 - May 08, 2017	Live Event
SANS Riyadh 2017	Riyadh, SA	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CAUS	May 09, 2017 - May 18, 2017	Live Event
SANS Zurich 2017	Zurich, CH	May 15, 2017 - May 20, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VAUS	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, GB	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, AU	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, SE	May 29, 2017 - Jun 03, 2017	Live Event
SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
ICS Security Summit & Training - Orlando	OnlineFLUS	Mar 19, 2017 - Mar 27, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced