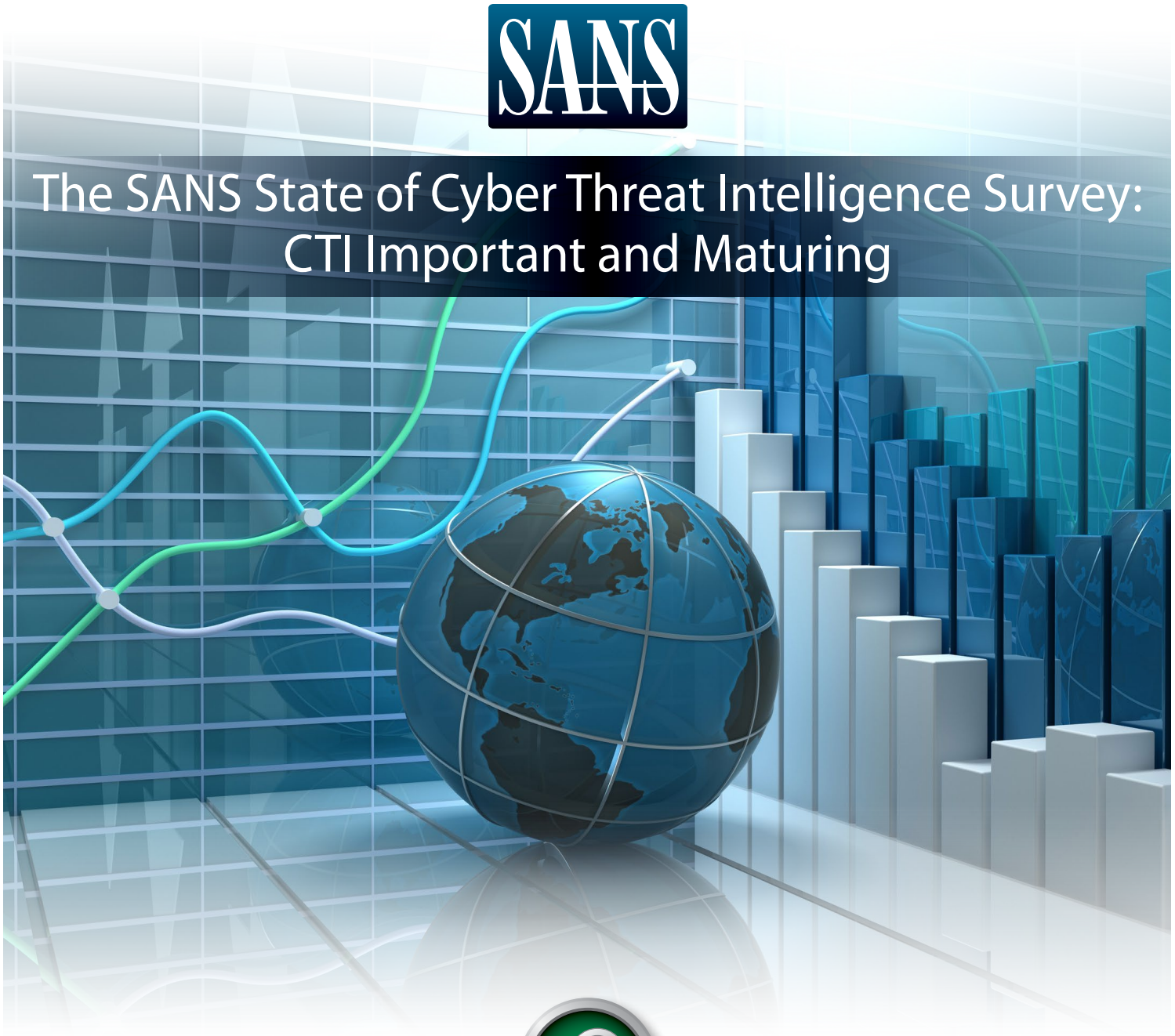
Interested in learning more about security?

SANS Institute InfoSec Reading Room

The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing

It s 2016, and the attacks (and attackers) continue to be more brazen than ever. In this threat landscape, the use of cyber threat intelligence (CTI) is becoming more important to IT security and response teams than ever before. This paper provides survey results along with advice and best practices for getting the most out of CTI.



The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing

A SANS Survey

Written by Dave Shackleford

August 2016

Sponsored by

AlienVault, Anomali, Arbor Networks, Hewlett Packard Enterprise, NETSCOUT, and Rapid7

Executive Summary

It's 2016, and the attacks (and attackers) continue to be more brazen than ever. Numerous organizations are being affected by organized criminal groups who deploy ransomware and demand payment to unlock critical data and systems. Spearphishing campaigns are finding their marks again and again, with millions of personal records accessed and stolen in the past year. More vulnerabilities are being found (and exploited) in mobile and Internet of Things (IoT) platforms, and the sophistication of malware overall is on the rise. Security teams are struggling just to keep up, let alone get ahead of the attackers.

In this threat landscape, the use of cyber threat intelligence (CTI) is becoming more important to IT security and response teams than ever before, according to the 2016 SANS survey on cyber threat intelligence. In it, 41% felt their use of CTI is maturing, and 26% felt their use of CTI is mature or very mature. Only 6% said they did not use CTI.

In previous SANS surveys on this subject conducted between 2014 and 2015, many security professionals felt somewhat unclear on exactly what CTI was and how best to make use of it, yet they were collecting some CTI data from disparate sources. Those that were utilizing CTI in 2014–15 were already reaping benefits, however, with 48% of respondents stating that they were able to reduce the number of incidents through early prevention related to use of CTI.[1]

Skills, Utilization and Aggregation at a Glance

- The biggest barriers to CTI implementation are a lack of skills (37%) and technical knowledge (59%), as well as poor management support (35%).
- The most valuable skills for working with CTI include intelligence analysis, ability to write correlation rules, and knowledge of normal network and system operations.
- Most organizations can only comfortably research and utilize between 1 and 100 threat indicators weekly.
- SIEM and intrusion monitoring platforms are the most common integration points for collecting and analyzing CTI data, followed by commercial CTI tools.

In this year's survey, respondents indicate they are more fully implementing CTI into their protection and response programs. For example:

- Traditional network security, endpoint security, and security information and event management (SIEM) vendors are providing the majority of useful intelligence feeds to security teams
- The top use cases for CTI include blocking malicious domains or IP addresses at egress points and adding context to investigations or compromise assessments
- Most security teams using CTI are acquiring the data from industry and community sharing groups (74%) and commercial feeds from security intelligence vendors (70%)

A large percentage of organizations (64%) was also able to quantify improvements. At this stage, more organizations feel comfortable quantifying improvements in response activities resulting from CTI than they do for preventing breaches. They are also short of staff and skills and unable to manage large volumes of intelligence indicators in any given week. These and other results, along with advice and best practices, are included in this report.

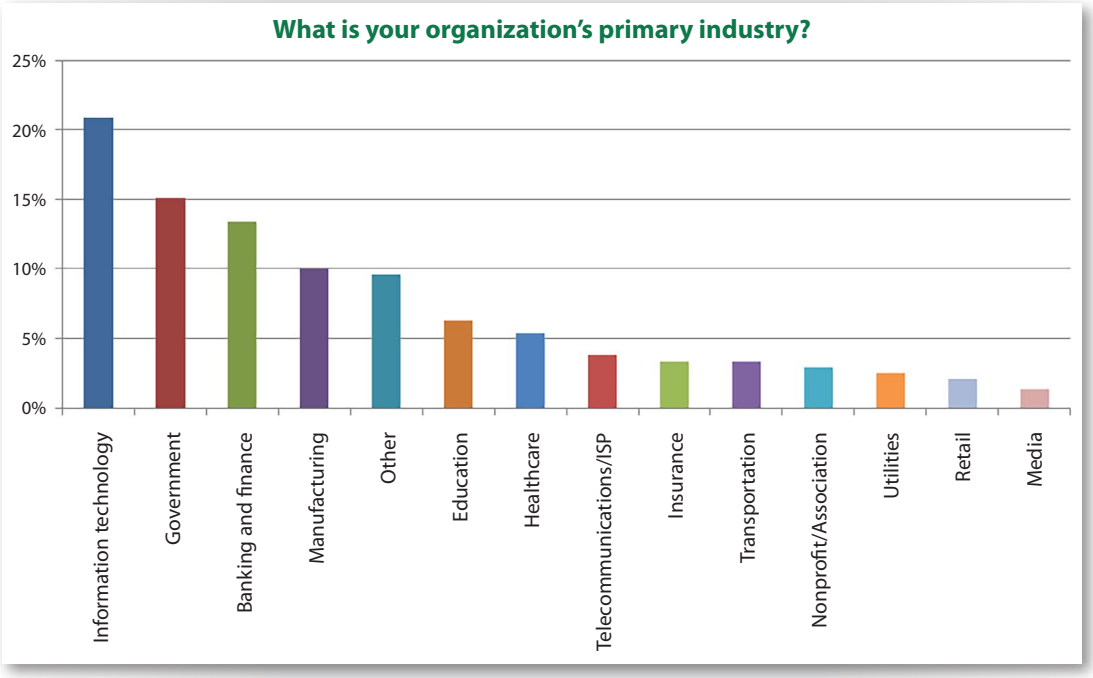
[1] "Who's Using Cyberthreat Intelligence and How," www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767

Who's Utilizing CTI?

This year's 220 respondents represented a broad range of industries, organizational sizes and job roles. The top vertical was IT, selected by 21% of respondents, followed by government, banking and finance, and manufacturing, with a mix of others that include education, healthcare, consulting and telecommunications. Respondent roles indicate representation of key roles in information security, with 39% filling the roles of security administrators or analysts and another 20% in security management roles (CSO and CISO). See Figure 1.

48% represented organizations of 5,000 or more:	
5,001–10,000	10.5%
10,001–15,000	5.0%
15,001–50,000	10.5%
50,001–100,000	10.5%
More than 100,000	11.3%

52% represented organizations with fewer than 5,000 employees:	
Fewer than 100	13.4%
101–1,000	19.7%
1,001–2,000	8.8%
2,001–5,000	10.5%



Key Job Roles:	
Security administration/Security analyst	38.5%
Security manager or director/CSO/CISO	20.1%
Other	11.7%
Network operations/System administrator	8.4%
IT manager or director/CIO/CTO	7.9%
Security design engineer	5.0%

Figure 1. Survey Demographics

Just 8% of respondents represented additional titles, which were not included in Figure 1. This survey sample is representative of the SANS member base, but it also indicates that security teams and their managers are primary consumers of CTI.

Maturity of Programs

All but 6% of respondents indicated that they currently have a CTI program in place. On the low end of the curve, 28% stated that their programs are currently emerging or immature, and in the largest stretch of the curve, roughly 41% stated that CTI was currently maturing in their environments, with another 26% saying their programs are mature or very mature. See Figure 2.

TAKEAWAY:

In last year's survey, 7% had never even heard of CTI, and 8% had no current CTI program and no intention of implementing one.

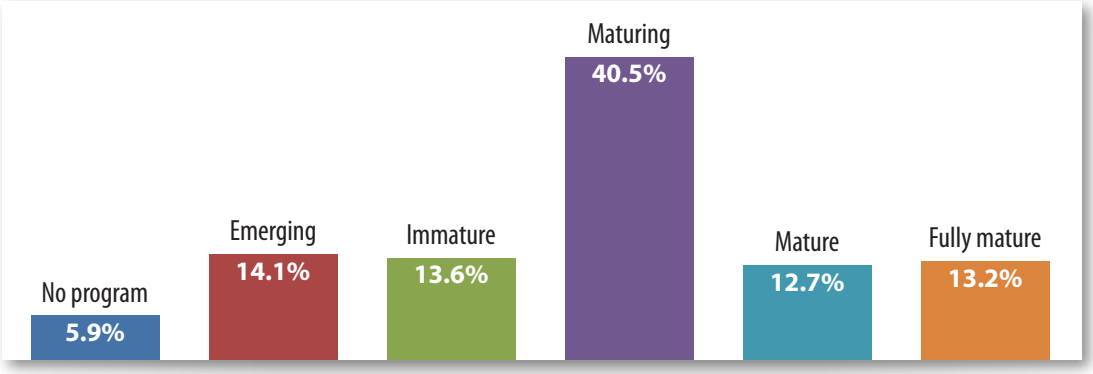


Figure 2. Maturity of CTI Programs

These numbers indicate that use of CTI is growing and that many organizations have the basics in place and can begin to fine-tune their CTI programs.

Specific Improvements

The majority of respondents (64%) felt that CTI had improved their security and response capabilities, with only 3% indicating that the use of CTI hadn't improved these functions. The other respondents answered "unknown." These numbers align very closely with the 2015 survey, where 63% also indicated that CTI was helping improve their detection and response capabilities.

For those 64% of respondents to this year's survey who felt that their security and response capabilities had improved:

- 73% felt that they could make better and more informed decisions with the use of CTI
- 71% saw improved visibility into threats, although 34% didn't know whether CTI had improved their capabilities
- 58% said CTI helps provide faster and more accurate response
- 53% said CTI helps detect unknown threats that they were previously unaware of
- 48% said CTI helps reduce breaches (actual exposure of sensitive data, business outage)
- 39% said the use of CTI has measurably reduced the impact of incidents through more intelligent blocking

Proactively using threat intelligence provides the opportunity to make better decisions about security posture based on having an understanding of threats. It also involves getting the message out to your firewalls, unified threat management (UTM), IPS and endpoint security tools to block new threat classes, categories and actions as they're discovered. In future surveys, we expect to see more use of threat intelligence in prevention devices such as these.

Benefits Year to Year

In our 2016 survey, the top benefit of CTI was to enable better decision making, followed by visibility into threats, and faster/more accurate response.

In our 2015 survey, respondents reported that CTI improved visibility and enabled a faster and more accurate response.

Difficult to Quantify

For more quantitative improvements, such as reducing breaches (48%) and measurably reducing the impact of incidents (39%), fewer respondents felt confident that CTI had provided benefits. Of those, 58% were able to quantify reduction in breaches as a result of CTI, while 42% of respondents did not know by what percentage breaches had been reduced as a result of using CTI. Only 7% reported breach reductions of 50% or more. At this stage in their CTI programs, most organizations lack tactical measurements and tools that security teams feel comfortable enough with to enable them to quantify the results of their CTI programs. See Figure 3 for the breakdown of responses.

By what percentage do you estimate breaches have been reduced as a result of using CTI?

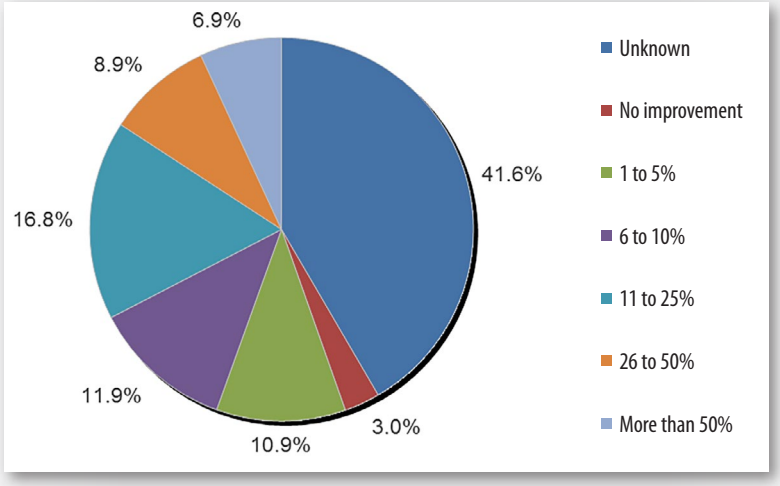


Figure 3. Improvements in Breach Prevention

Unlike breach prevention, higher percentages of respondents felt that CTI had provided measurable improvements to response capabilities overall. In 2015, 38% of survey takers did not know how much their response had improved with CTI, and that number is down to 19% in 2016. Likewise, the number who felt their response was more than 50% better and faster almost doubled from 2015, increasing from 7% to 12% in 2016. The majority (58%) of respondents felt that their CTI initiatives had improved response capabilities between 6% and 50%. See Figure 4.

How much do you estimate that your CTI tools and processes have improved your organization's ability to respond to events?

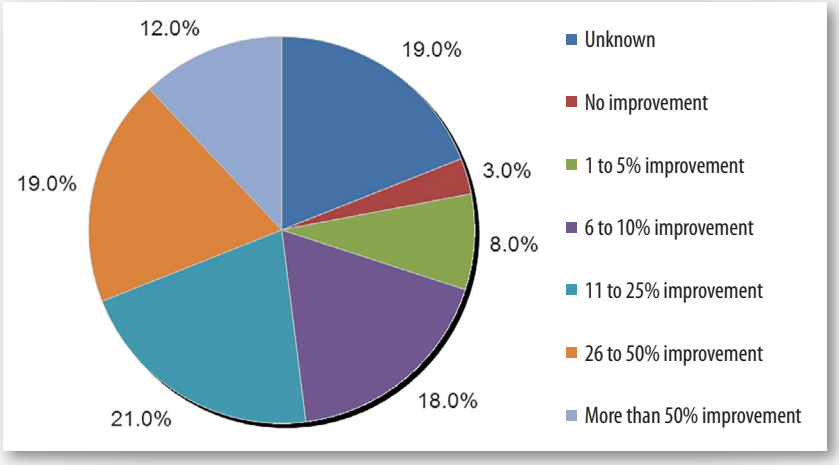


Figure 4. Incident Response Improvement from Use of CTI

Overall, it seems that more organizations feel that their CTI programs are bearing fruit in terms of incident response (and likely detection), but fewer are as comfortable quantifying breach prevention. This may be due to lack of data related to breaches, a lack of understanding as to what constitutes a breach (which we identified as exposure of sensitive data, IP, work outage, etc.) or other factors.

Acquiring and Using CTI

As security teams become more comfortable with leveraging CTI data, many are constantly seeking new and varied sources of CTI. Currently, 74% of security teams using threat intelligence are acquiring this information from industry and community sharing groups, and 70% are using commercial feeds from security intelligence vendors. Many are also leveraging open source CTI feeds, as shown in Figure 5.

Where does your CTI information come from?
Select those that most apply.

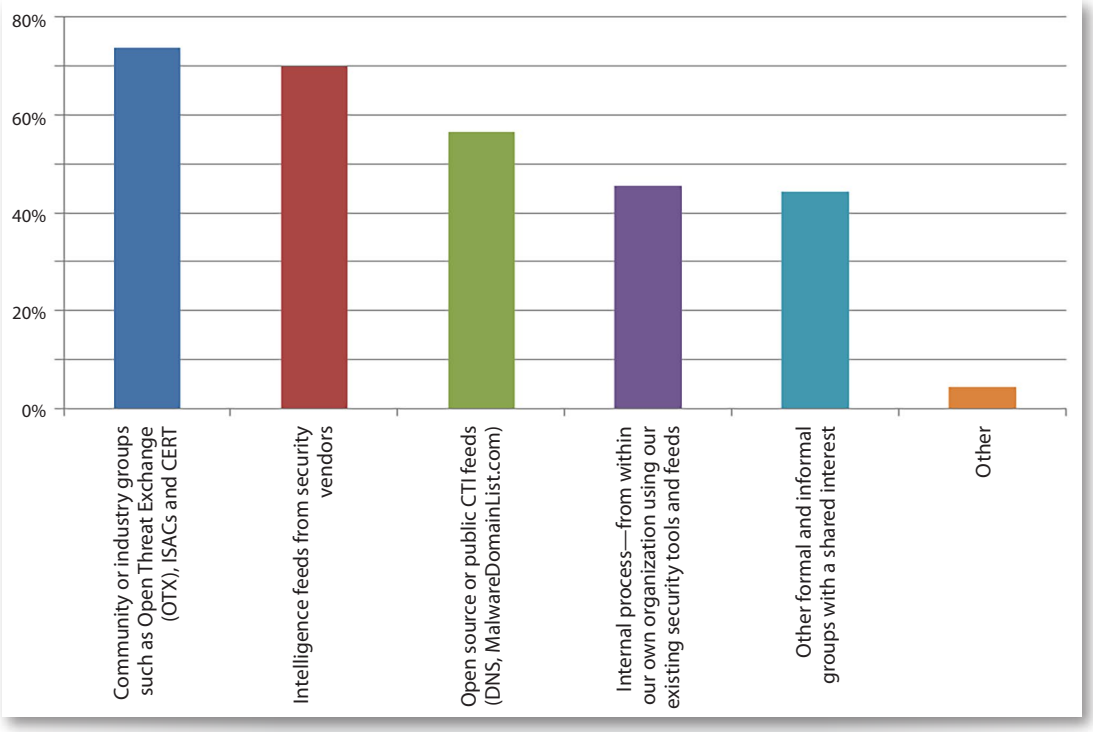


Figure 5. CTI Sources

TAKEAWAY:

There is no shortage of threat information types that can be applied to the threat intelligence ecosystem.

The 46% reutilizing threat data gathered from internal processes can be viewed as a sign of maturing organizations, in that it indicates the reuse of internally gathered threat information that is analyzed. However, judging from previous questions, even these organizations still need to better utilize this data for prevention.

Vendor-Provided CTI

For the 70% of security teams purchasing or acquiring CTI from vendors, 56% are gathering and analyzing information from alerts on their IDS, IPS, UTM and firewall solution, 47% from endpoint security vendors, and 44% from SIEM vendors, as illustrated in Figure 6. In 2015, the top source of vendor-provided threat intelligence was endpoint vendors, followed by IDS/IPS/firewall and CTI platform providers.

TAKEAWAY:

Most of the data in use today originates from more traditional vendors that have large install bases and significant exposure to large quantities of attack indicators and events.

If you selected "intelligence feeds from security vendors," please indicate which sources you use. ***Select all that apply.***

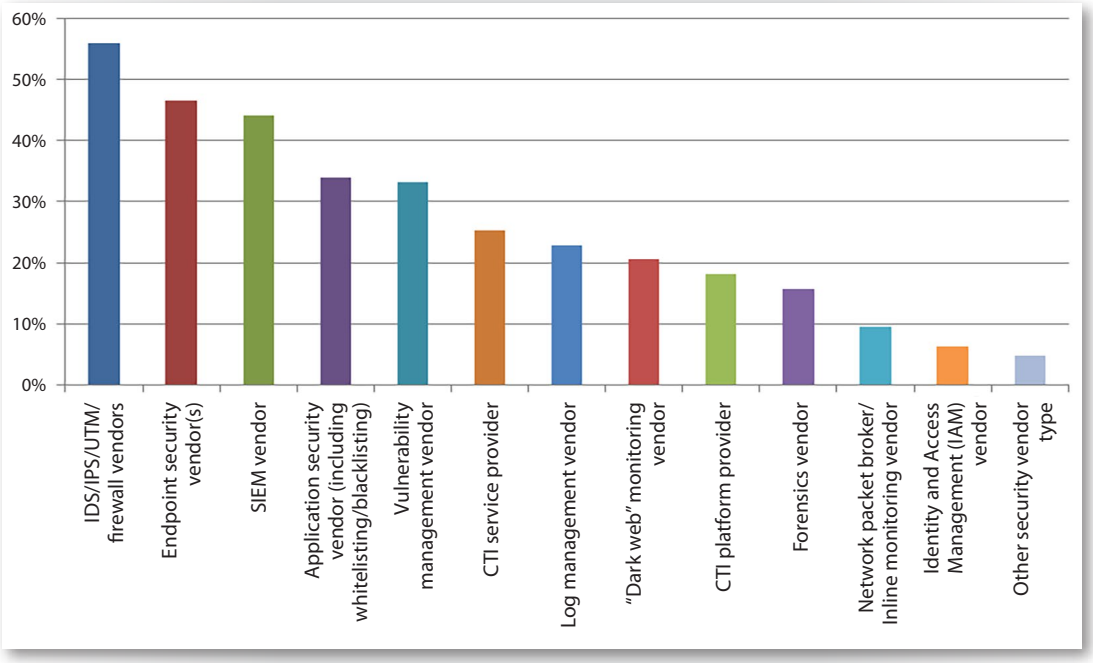


Figure 6. CTI Vendor Sources

Interestingly, only 25% of respondents used dedicated CTI service providers, which was somewhat surprising. This indicates that, for respondents, most of the data being used today originates from more traditional vendors that have large install bases and significant exposure to large quantities of attack indicators and events. (In 2015, roughly 40% of respondents were using dedicated threat intelligence platform vendors versus only 18% this year, for example). With that said, however, CTI service providers are much more recent additions to the tools available. It will be interesting to see how the use of CTI services and dedicated CTI platforms changes over time in comparison.

Top Uses for CTI

In 2015, SANS asked survey respondents to describe their primary goals with CTI, and the theme of the responses was: "Detect and respond faster and more effectively." We went further this year by asking the community members to list their top three use cases for CTI feed data, with a bit more emphasis on specifics and tactical use cases. In order, the top three use cases for CTI data are:

- Blocking malicious domains or IP addresses at egress points (e.g., firewalls) (63%)
- Adding context to investigations or compromise assessments (50%)
- Examining DNS server logs for malicious domains or IP addresses (30%)

The idea of adding context to investigations resonates closely with sentiments from last year, where security teams indicated that they wanted to know more about the attacks against them and attacker techniques, and to improve detection and response capabilities overall.

In this year's survey, the other two major use cases indicate security processes at focal areas at a network or infrastructure level of the environment (network egress and DNS). The full breakdown of responses is shown in Figure 7.

TAKEAWAY:

The most viable immediate use cases are more centered on the "big picture" of behavior in the environment at the moment.

What are your top use cases for your CTI feed data?

Select your top three uses, order is not important.

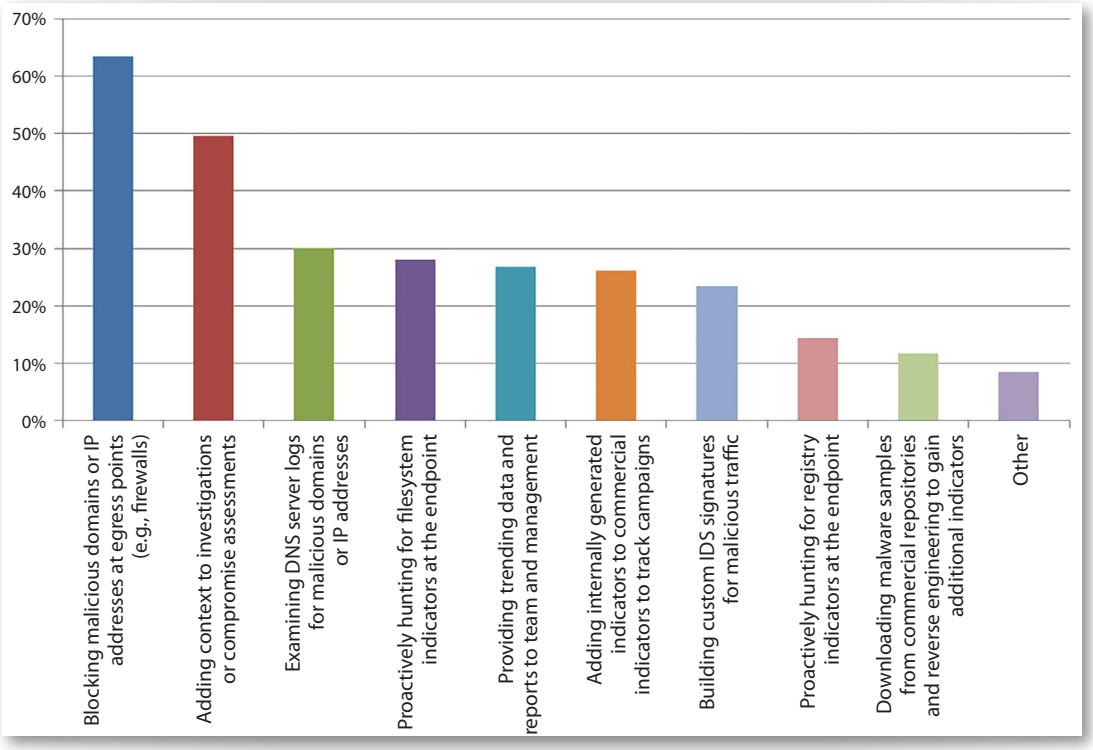


Figure 7. Top Use Cases for CTI Feed Data

Defense and Response

To actually take their feeds and apply them to defense and response systems, 41% (the majority) of respondents say their teams are using vendor-provided APIs, while 36% are building their own custom APIs to integrate CTI data into their security tools and processes, as shown in Figure 8.

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

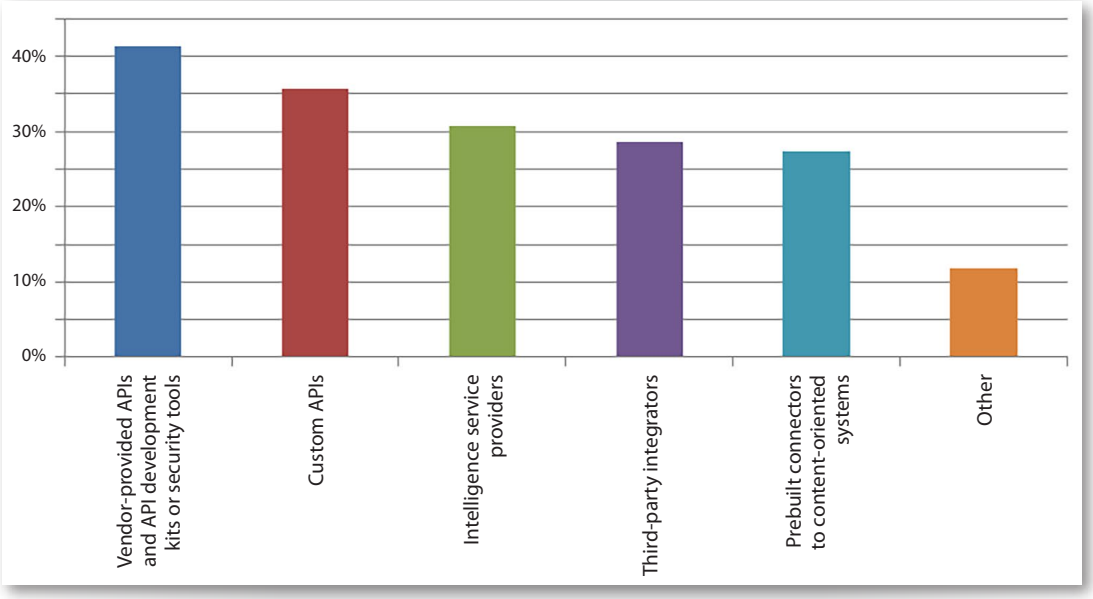


Figure 8. Top Integration Methods for CTI Data

Intelligence providers and third-party integrators are also fairly commonly used, as are prebuilt connections to content-oriented systems used for collection and analysis.

Processing of CTI

SIEM systems are the dominant means of managing CTI feeds, according to respondents. More than 43% of respondents say their organizations use SIEM in an integrated GUI to centralize and manage their threat intelligence, and another 26% use SIEM disparately with other tools and components. See Figure 9.

Which of the following tools are you using to aggregate, analyze and/or present CTI information?

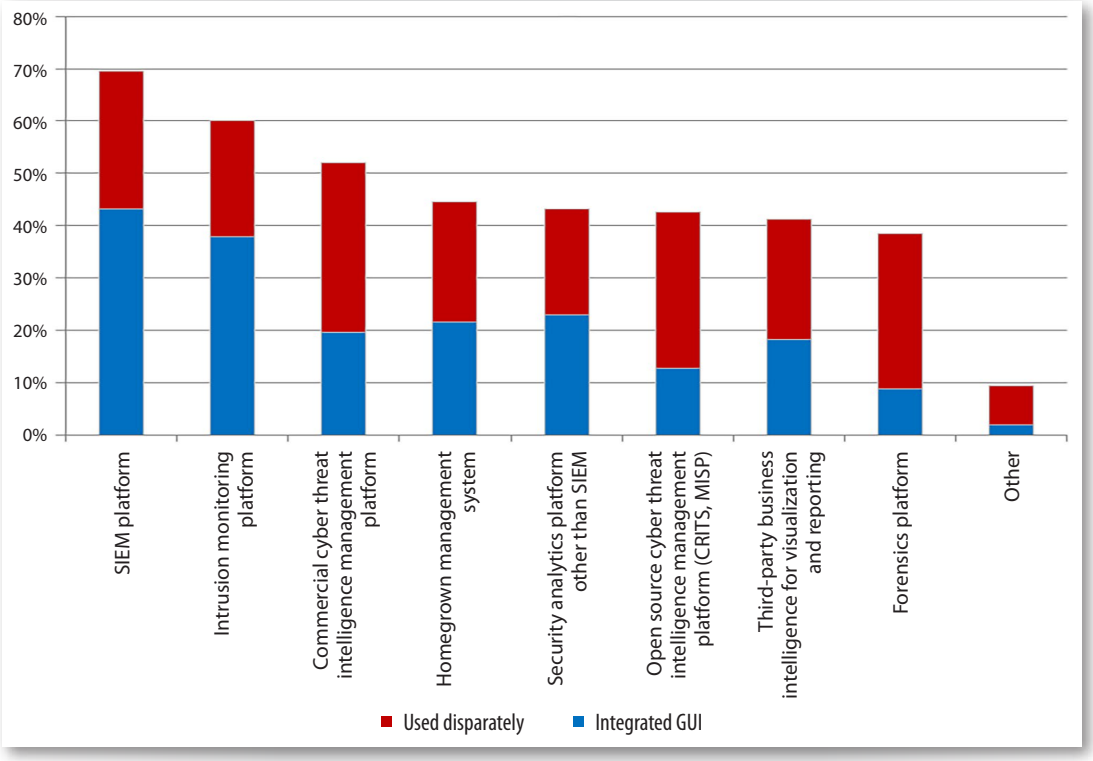


Figure 9. CTI Integration and Analysis Tools

This aligns well with the list of top vendor intelligence feed sources, where SIEM vendors ranked third. Intrusion monitoring platforms are the second most commonly used tool to manage CTI feeds, also used predominantly within a central GUI (60%). Commercial CTI management platforms were a close third, at 52%, but they were used in a much more disparate way with other tools, versus offering a self-contained GUI to manage all aspects of CTI collection, correlation and analysis. Open source CTI platforms were used less frequently (43% of responses) but also required more integration and coordination with other tools. Homegrown tools, analytics platforms, business intelligence tools and forensics tools were also cited.

Machine Analytics

Security teams tapped the Malware Information Sharing Platform (MISP), at 35%, as the top threat intelligence management tool or protocol in their programs today. TAXII is used by 23% of the respondents, as is Collaborative Research Into Threats (CRITs), an open source malware and threat repository for storing and analyzing CTI data. See Figure 10.

Which of the following threat intelligence management solutions is your team using?
Select all that apply.

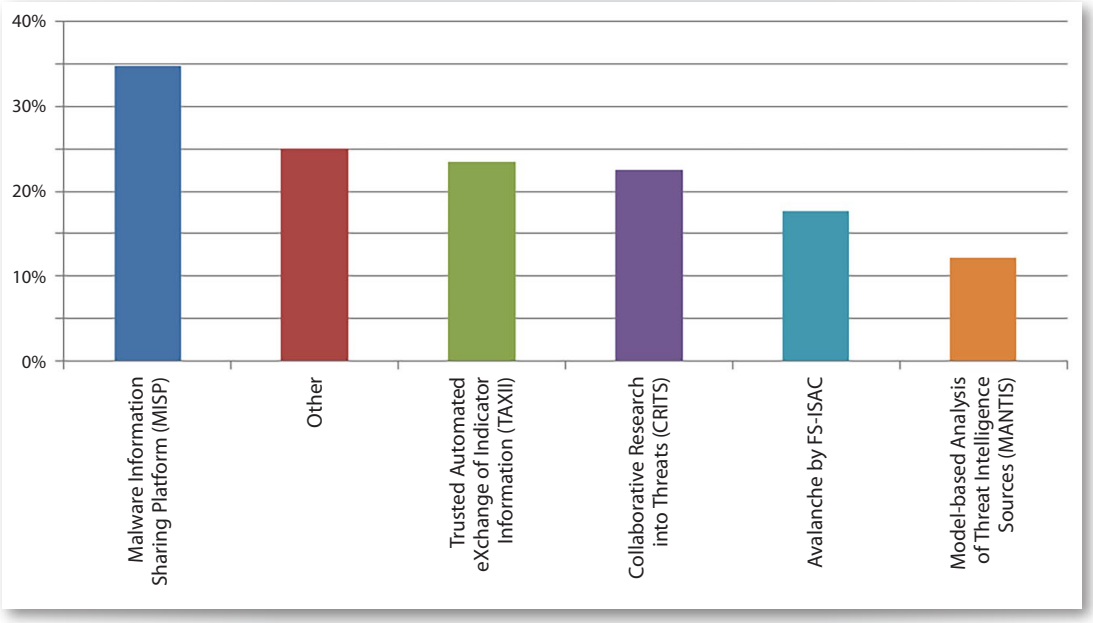


Figure 10. CTI Management Solutions

TAKEAWAY:
The landscape today is very fragmented, and there are few consistent themes in terms of approaches organizations are taking: lots of tools, lots of "standards" and little agreement on which are best may lead to more confusion. For the future, organizations must be able to use tools and CTI data in a more integrated way.

Many organizations marked the "other" category and listed commercial vendors, homegrown tools and the classic "prefer not to say" option. The FS-ISAC Avalanche tool and the Model-based Analysis of Threat Intelligence Sources (MANTIS) platform rounded out the list.

Platforms, Exchanges and Repositories

- MISP (Malware Information Sharing Platform) is a well-supported open platform that can integrate with numerous security and ticketing/reporting tools, as well as share information readily between organizations and teams as desired.
- MITRE's Trusted Automated eXchange of Indicator Information (TAXII) is a standard developed to exchange CTI data securely. It was recently transitioned to OASIS.
- CRITs (Collaborative Research into Threats) is an open source malware and threat repository for storing and analyzing CTI data.

Standards and Frameworks

In the 2015 and 2016 surveys, we asked security teams what standards and frameworks they were using in their CTI programs. The comparison of key standards in use in 2015 and 2016 is shown in Table 1.

Table 1. CTI Standards and Frameworks in Use

Standard/Framework	2015	2016
Open Threat Exchange (OTX)	50.8%	40.0%
Structured Threat Information Expression (STIX)	45.9%	29.2%
Collective Intelligence Framework (CIF)	39.3%	26.2%
Open Indicators of Compromise (OpenIOC) Framework	32.8%	16.9%
Other	6.6%	13.8%
Cyber Observable eXpression (CybOX)	26.2%	11.5%
Vocabulary for Event Recording and Incident Sharing (VERIS)	19.7%	9.2%
Incident Object Description and Exchange Format (IODEF)	23.0%	8.5%
Trusted Automated eXchange of Indicator Information (TAXII)	32.8%	N/A
Traffic Light Protocol (TLP)	27.9%	N/A

Across the board, fewer respondents indicated that they were using these well-known standards and frameworks. Why? Several of the "other" responses stated that they were using custom APIs and homegrown solutions, which may be a growing trend (although the number of these responses was small). STIX is a very common standard in use at many organizations the author has worked in, but commercial options and other methods may be growing.

Consumers of CTI

Almost 61% of respondents indicated that their teams primarily consumed threat intelligence information, which is not surprising given the range of roles represented in the survey. Another 33% both produced and consumed CTI, while only 7% focused on producing CTI.

The two top consumers of CTI were nearly tied, with 64% naming the security operations center (SOC) as the primary consumer and 63% saying incident responders were the big consumers. This makes a good deal of sense, because most CTI programs seek to improve and enable detection and response activities, and these are the primary teams involved in most cases. See Figure 11.

Who are the primary consumers or customers of CTI in your organization?
Select all that apply.

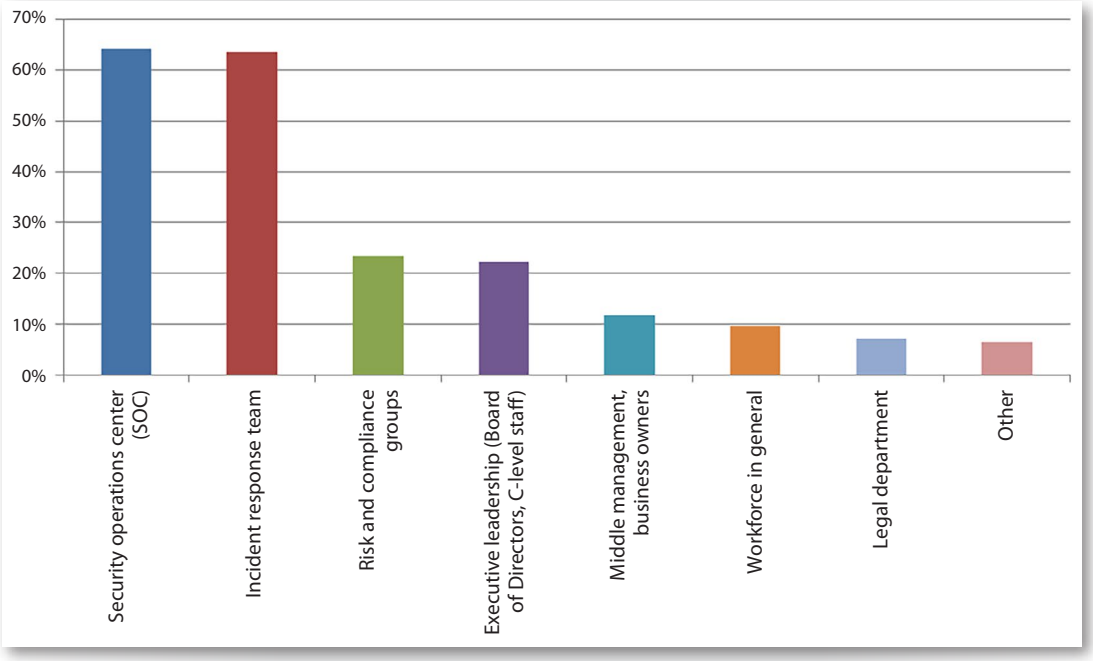


Figure 11. Top Consumers of CTI

Intelligence Reporting

Most consumers of CTI (43%) received standalone reports, while 37% cited integrated data and metrics along with other security program reports. In addition, 28% of respondents' organizations also conduct dedicated CTI awareness training, and others opted to provide direct access to CTI data to the consumers themselves. Some organizations weren't sure how consumers were getting CTI information, and several responses in the "other" category included informal socialization, emails and routine staff meetings, and security awareness training.

Building Threat Intel Teams

In this year's survey, 28% of respondents indicated that they have a formal team dedicated to CTI currently, which is down from 2015, when 34% selected this option. Another 18% have a single team member dedicated to CTI (an increase from the 14% in 2015), and another 21% of respondents stated they don't currently have a person or team dedicated to CTI, but are planning to put this in place soon by training existing staff (similar to 2015). See Figure 12.

TAKEAWAY:

Most organizations are clearly looking to keep some or most of the skills they need for CTI in-house.

Do you have a dedicated person or team that focuses on CTI?

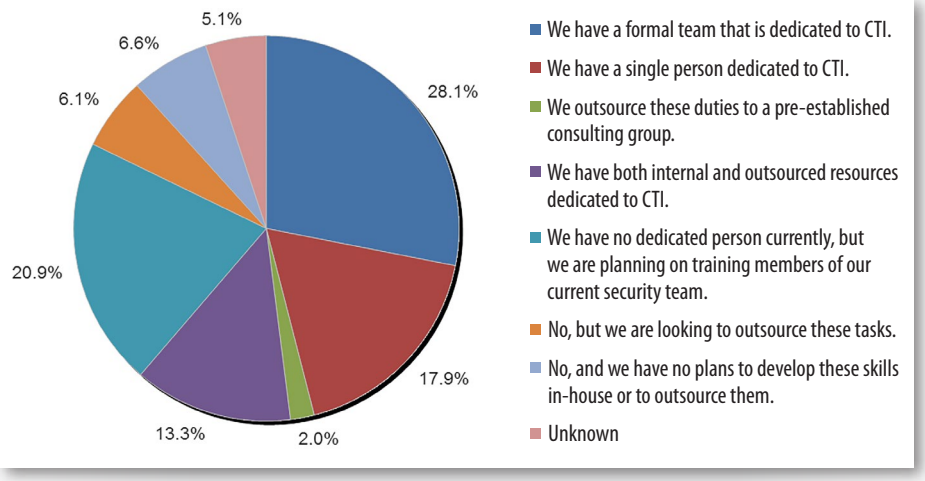


Figure 12. Staff and Team Allocation for CTI

While only 2% say they outsource their CTI duties completely, another 13% use some outsourcing, and another 6% are looking to outsource in the future.

Incident Response and SOC Teams

Those organizations that do have dedicated staff for CTI predominantly situate them in the incident response or security operations center (SOC) teams. Others have CTI-focused staff within the enterprise security team as well, with a smaller number assigning these functions to IT teams, dedicated CTI teams or vulnerability management teams, among others (see Figure 13).

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

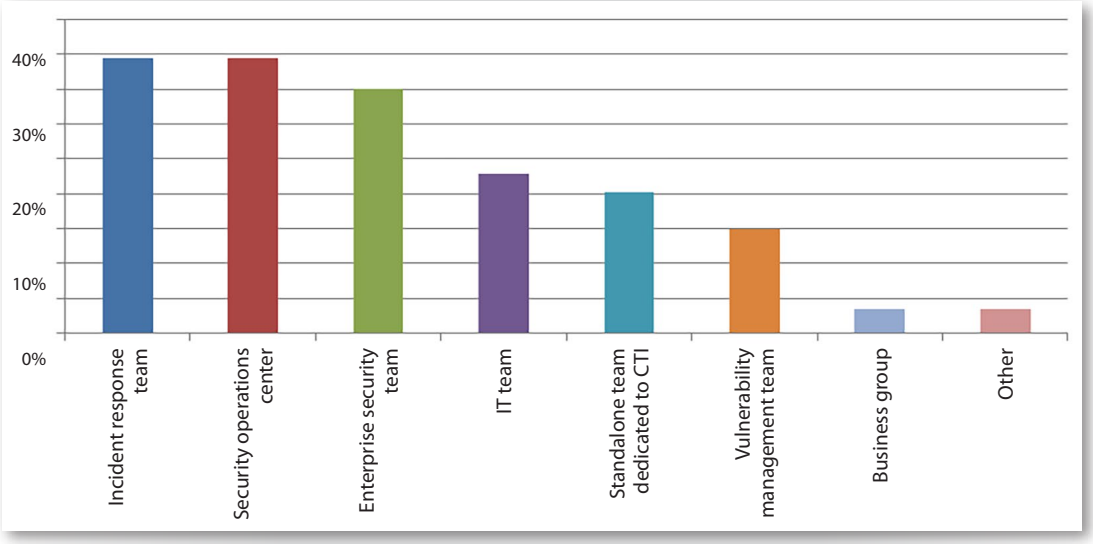


Figure 13. CTI Team and Staff Location

Given these team and staff locations, it's not surprising that the vast majority report to the SOC leadership or CISO/CSO, with a smaller number reporting to IT leadership, as shown in Figure 14.

To whom do CTI team members report?

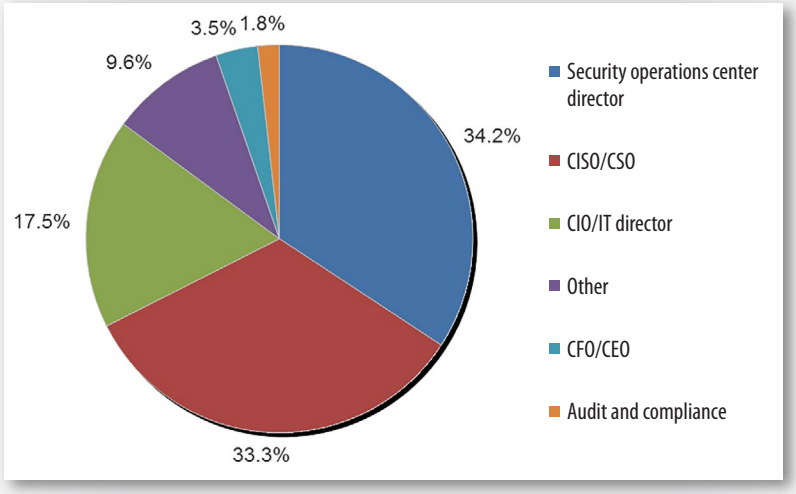


Figure 14. CTI Reporting Structure

Skills Required

TAKEAWAY:

Intelligence analysis skills seem to be the most valuable by far, with correlation rule creation close behind. A combination of network and system knowledge and incident response skills makes up the balance of primary skills. The problem? These skills are very difficult to come by, and finding one person with all of those skills is even more elusive. The challenge of finding people with the right combination of skills will likely continue for some time.

We asked respondents to tell us what skills were most valuable to leverage CTI in detection and response activities, ranking their top three (with "1" being the most valuable). The "most valuable" skills listed were intelligence analysis, correlation rule creation, and knowledge of normal network and system operations to detect abnormal behaviors. Incident response skills, knowledge of critical (internal) business processes, and knowledge of adversaries and campaigns were also ranked relatively high. See Table 2.

Table 2. Valuable Skills for Leveraging CTI

Answer Options	1 (Most Valuable)	2	3	Response Count
Intelligence analysis skills	26.9%	19.9%	10.3%	57.1%
Ability to write correlation rules to link security events	15.4%	9.6%	8.3%	33.3%
Knowledge of normal network and system operations to detect abnormal behaviors	13.5%	19.2%	9.6%	42.3%
Incident response skills	12.8%	10.9%	12.8%	36.5%
Knowledge of critical (internal) business processes	10.3%	10.9%	12.2%	33.3%
Knowledge of adversaries and campaigns	9.0%	7.7%	6.4%	23.1%
Malware analysis skills	3.8%	5.1%	10.3%	19.2%
Reporting/writing skills	1.3%	9.0%	5.8%	16.0%
Familiarity with new commercial tools and feeds	4.5%	3.2%	6.4%	14.1%
Presentation/oral communications skills	1.9%	3.2%	4.5%	9.6%
Other	0.6%	0.6%	1.3%	2.6%

Other skills ranging from reporting, malware analysis and familiarity with new tools were listed too, with presentation skills ranked as the least valuable overall.

A Matter of Capacity

Are we asking too much of CTI? Do we even have the right ideas about how to properly make use of CTI data? Very few organizations, it turns out, can either research or effectively use more than 100 threat indicators every week. Cumulatively, only 12% of respondents could research more than 100, and 15% could effectively utilize more than 100. Just under 30% felt that they could effectively research between one and 10 threat indicators, and 20% felt that they could use one to 10 adequately. When the range increased from 11 to 100, 22% felt they could use the indicators effectively, but only 15% could take the time to research these indicators. See Table 3.

Table 3. Research and Utilization of CTI indicators

Given your current workflow, how many new threat indicators can your incident response or hunt teams effectively utilize on a weekly basis? How many does the team actually research on a weekly basis?

Answer Options	Effectively Utilize	Actually Research	Response Count
Unknown	22.4%	13.8%	36.2%
None	3.3%	2.6%	5.9%
1–10	19.7%	29.6%	49.3%
11–100	22.4%	15.1%	37.5%
101–250	4.6%	3.3%	7.9%
251–500	3.9%	2.0%	5.9%
501–1,000	3.3%	3.9%	7.2%
1,001–5,000	0.7%	0.7%	1.3%
5,001–10,000	1.3%	1.3%	2.6%
Greater than 10,000	1.3%	0.7%	2.0%

What this data tells us is that most organizations can really handle only between one and 100 indicators comfortably, both in terms of researching the threats and acting upon CTI data to perform detection and response activities. Anything more would be overload.

Number 1 Inhibitor

In the 2015 survey, almost 35% of respondents indicated that a lack of budget and/or staff was holding back their CTI initiatives. The responses to this year's survey reflected some of the same concerns. The majority (59%) felt that a lack of trained staff and skills were the biggest issues, as shown in Figure 15.

What inhibitors are holding your organization back from implementing CTI effectively?

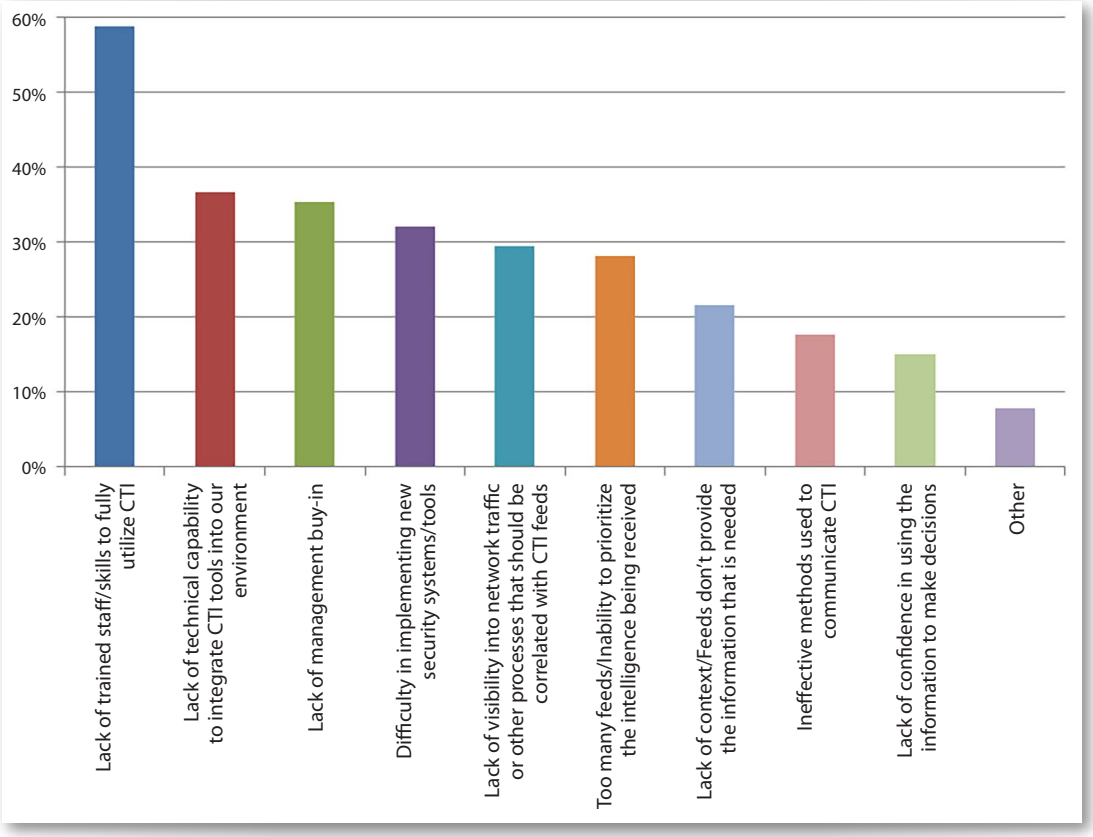


Figure 15. Barriers to Implementation

TAKEAWAY:

Why was there much less management buy-in? That is hard to say. It could be the specific respondents we talked to this year versus last, a lack of visibility into how CTI supports security operations, an inability to provide meaningful metrics to management, or it may be that it is difficult to produce tangible results and improvements from CTI. This is a trend we'll be watching closely.

Another 37% cited lack of technical integration capabilities, while 35% said they lacked management buy-in—the latter of which increased dramatically from 11% in 2015 to 35% in 2016.

Other technical concerns include challenges with implementing new tools for CTI, integrating feeds data, gaining the needed visibility into network traffic and other processes, and gleaning the appropriate context from feeds in use. These shortcomings may be leading to a lack of demonstrable results that cause management to hesitate in committing resources to CTI programs in some organizations.

Looking Forward

Most respondents (69%) feel that CTI will be very important for defense and response, and 54% feel it will be important for risk prioritization and decision making over the next five years. Only 3% of responses projected that CTI would not be important in either category.

To achieve better integration and use of their CTI data in the future, respondents asked for better alignment with standards, reduced false positives, better coverage of the industrial control system (ICS) industry, better data enrichment and analysis, less confusion around standards, and better management buy-in. As one put it in this write-in answer, "[The] largest need is for leadership to understand what threat intelligence means and work with business leaders to drive requirements to integrate intelligence for informed business insight, direction and policy."

Conclusion and Wrap-Up

The importance of CTI seems to be a foregone conclusion, especially looking through to the next five years. The tools, knowledge and processes around practical CTI implementation are maturing, but they need to mature more in order for organizations to detect, block and investigate threats as needed. Currently, however, there is an enormous amount of confusion and discord in the CTI marketplace, both commercial and community-driven, and entirely too many competing standards and lackluster sources of data and results to satisfy security professionals today.

A number of comments echoed sentiments already expressed in the data, namely that the tools are immature and getting management buy-in is a big challenge right now. They also expressed a lack of technical and procedural knowledge about deriving value from their programs.

A major source of frustration for many security professionals is the overly general nature of many CTI feeds. Security teams feel that more-customized and targeted feed data would be vastly more useful than generic threat intelligence that is somewhat shallow and less geared toward their organization or vertical. In addition, several admitted that they need to focus on building better internal CTI sources and data integration, even as commercial feeds improve. Revising policies to better reflect the integration and use of CTI was another area cited as needing work.

Regardless of CTI's current state of maturity, our advice to readers is similar to what we offered last year: Prepare for CTI if you're not doing it currently, and for those currently moving into CTI or using CTI readily, keep fighting the good fight. This is a new area for many in the security industry—one that shows enormous promise and will likely help us tremendously in the near future.

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.

Rob Lee (advisor) is the curriculum lead and author for digital forensic and incident response training at the SANS Institute. With more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention and incident response, he provides consulting services in the Washington, D.C. area. Before starting his own business, Rob worked with government agencies in the law enforcement, defense and intelligence communities as a lead for vulnerability discovery and exploit development teams, a cyber forensics branch, and a computer forensic and security software development team. He also worked for a leading incident response service provider and co-authored *Know Your Enemy: Learning About Security Threats*, 2nd Edition.

Sponsors

SANS would like to thank this survey's sponsors:

ALIEN VAULT

Hewlett Packard Enterprise

ANOMALI™

NETSCOUT®
Packet Flow Switch (PFS) Business Unit

ARBOR® NETWORKS

RAPID7

Last Updated: September 13th, 2016

Upcoming SANS Training

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

SANS ICS London 2016	London, GB	Sep 19, 2016 - Sep 25, 2016	Live Event
MGT517 - Managing Security Ops	San Diego, CAUS	Sep 26, 2016 - Sep 30, 2016	Live Event
Security Leadership Summit	Dallas, TXUS	Sep 27, 2016 - Oct 04, 2016	Live Event
SANS DFIR Prague 2016	Prague, CZ	Oct 03, 2016 - Oct 15, 2016	Live Event
SANS Seattle 2016	Seattle, WAUS	Oct 03, 2016 - Oct 08, 2016	Live Event
SANS Oslo 2016	Oslo, NO	Oct 03, 2016 - Oct 08, 2016	Live Event
SANS Baltimore 2016	Baltimore, MDUS	Oct 10, 2016 - Oct 15, 2016	Live Event
SANS Tokyo Autumn 2016	Tokyo, JP	Oct 17, 2016 - Oct 29, 2016	Live Event
SANS Tysons Corner 2016	Tysons Corner, VAUS	Oct 22, 2016 - Oct 29, 2016	Live Event
SANS San Diego 2016	San Diego, CAUS	Oct 23, 2016 - Oct 28, 2016	Live Event
SANS FOR508 Hamburg in German	Hamburg, DE	Oct 24, 2016 - Oct 29, 2016	Live Event
SANS Munich Autumn 2016	Munich, DE	Oct 24, 2016 - Oct 29, 2016	Live Event
SOS SANS October Singapore 2016	Singapore, SG	Oct 24, 2016 - Nov 06, 2016	Live Event
Pen Test HackFest Summit & Training	Crystal City, VAUS	Nov 02, 2016 - Nov 09, 2016	Live Event
SANS Sydney 2016	Sydney, AU	Nov 03, 2016 - Nov 19, 2016	Live Event
SANS Gulf Region 2016	Dubai, AE	Nov 05, 2016 - Nov 17, 2016	Live Event
DEV534: Secure DevOps	Nashville, TNUS	Nov 07, 2016 - Nov 08, 2016	Live Event
SANS Miami 2016	Miami, FLUS	Nov 07, 2016 - Nov 12, 2016	Live Event
DEV531: Defending Mobile Apps	Nashville, TNUS	Nov 09, 2016 - Nov 10, 2016	Live Event
European Security Awareness Summit	London, GB	Nov 09, 2016 - Nov 11, 2016	Live Event
SANS London 2016	London, GB	Nov 12, 2016 - Nov 21, 2016	Live Event
Healthcare CyberSecurity Summit & Training	Houston, TXUS	Nov 14, 2016 - Nov 21, 2016	Live Event
SANS San Francisco 2016	San Francisco, CAUS	Nov 27, 2016 - Dec 02, 2016	Live Event
MGT517 - Managing Security Ops	Washington, DCUS	Nov 28, 2016 - Dec 02, 2016	Live Event
SANS Hyderabad 2016	Hyderabad, IN	Nov 28, 2016 - Dec 10, 2016	Live Event
SANS Cologne	Cologne, DE	Dec 05, 2016 - Dec 10, 2016	Live Event
SEC 560@ SANS Seoul 2016	Seoul, KR	Dec 05, 2016 - Dec 10, 2016	Live Event
SANS Dublin	Dublin, IE	Dec 05, 2016 - Dec 10, 2016	Live Event
SANS Cyber Defense Initiative 2016	Washington, DCUS	Dec 10, 2016 - Dec 17, 2016	Live Event
SANS Amsterdam 2016	Amsterdam, NL	Dec 12, 2016 - Dec 17, 2016	Live Event
SANS Frankfurt 2016	Frankfurt, DE	Dec 12, 2016 - Dec 17, 2016	Live Event
SANS London Autumn	OnlineGB	Sep 19, 2016 - Sep 24, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced