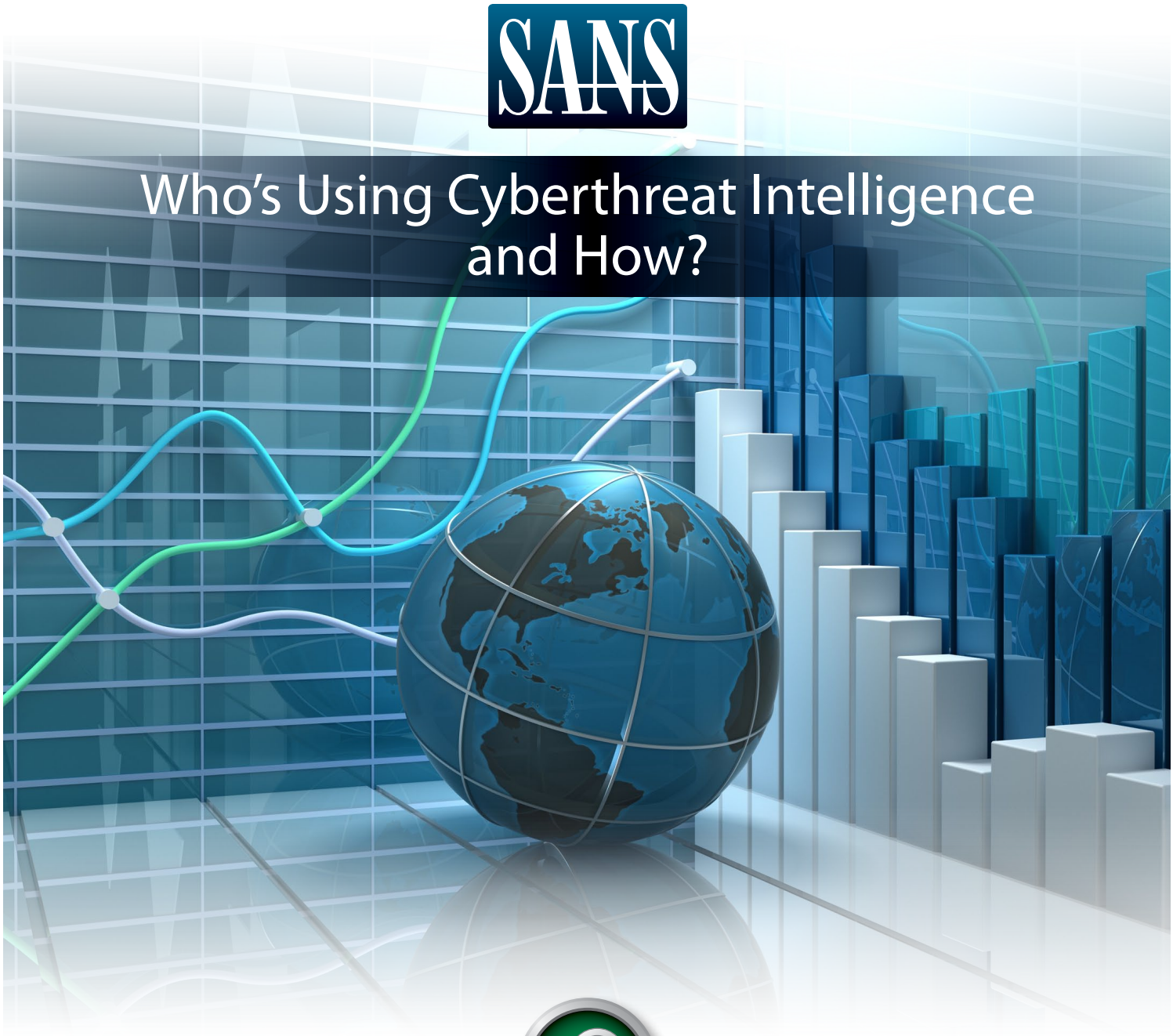
Interested in learning more about security?

SANS Institute InfoSec Reading Room

Who's Using Cyberthreat Intelligence and How?

Respondents to this SANS survey point to strong planning, leveraging internal systems and intelligence, and defining gaps in protection and workarounds as key best practices for developing cyberthreat intelligence capabilities. These best practices, along with adoption trends and definitions, are discussed in this paper.



Who's Using Cyberthreat Intelligence and How?

A SANS Survey

Written by Dave Shackleford

Advisor: Stephen Northcutt

February 2015

Sponsored by

AlienVault, Arbor Networks, BeyondTrust, Bit9 + Carbon Black, SurfWatch Labs, and ThreatStream

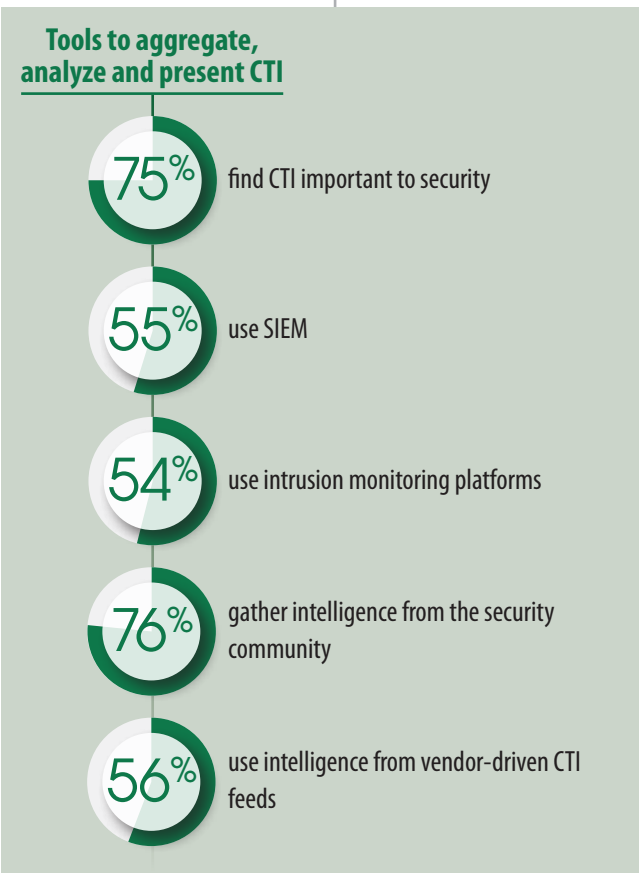
Introduction

Threat Intelligence

The set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators

In the last several years, we've seen a disturbing trend—attackers are innovating much faster than defenders are. We've seen the "commercialization" of malware, with attack kits available on underground forums for anyone who wants to perpetrate a variety of attacks. Large botnets are available for rent, allowing attackers to send spam or launch DDoS attacks at will. Many attackers reuse malware and command and control protocols and methods, adapting their "products" over time to keep ahead of the antimalware industry and security professionals. As more and more attacks occur, however, the likelihood increases that some organization or group has seen the attack before.

The idea behind cyberthreat intelligence is to provide the ability to recognize and act upon indicators of attack and compromise scenarios in a timely manner. While bits of information about attacks abound, cyberthreat intelligence (CTI) recognizes indicators of attacks as they progress, in essence putting these pieces together with shared knowledge about attack methods and processes.



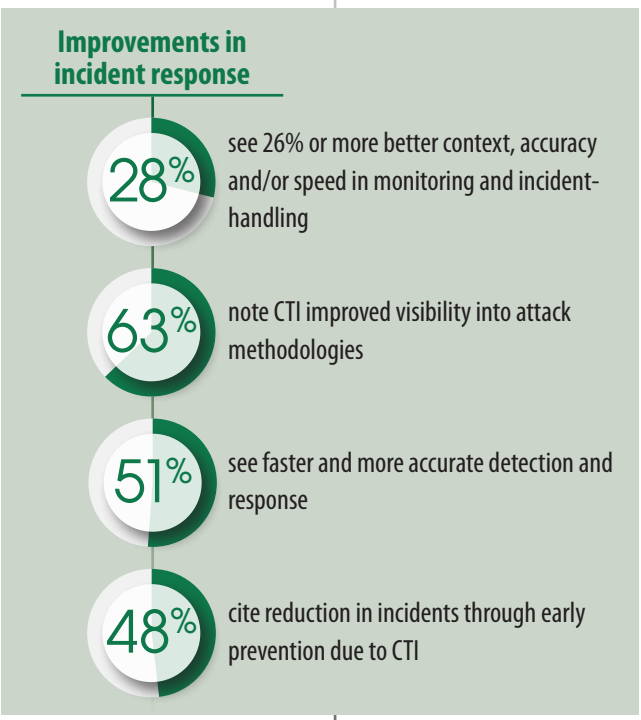
There's a lot of confusion around what threat intelligence is and how it's delivered and consumed, based on the SANS survey on Analytics and Intelligence published in October 2014.[1] So, in an attempt to define CTI and best practices for using CTI, SANS conducted a new survey about the state of cyberthreat intelligence policies and practices, and whether CTI has improved organizations' ability to detect and respond to attacks faster.

In this new survey, taken by 326 qualified respondents, 69% of respondents report implementing CTI to some extent, with only 16% saying they have no plans to pursue CTI in their environments. The commitment to working with CTI is evident, with 64% reporting they have a dedicated team, person or services organization assigned to implement and monitor intelligence.

[1] www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507

The survey shows respondent organizations are relying on multiple data feeds for aggregation and analysis that they'd like to consolidate in the next 12 months. The most common elements of CTI that have been achieved by organizations include raw, unfiltered data feeds with CTI information, tools to visualize and analyze CTI, and a wide variety of accurate and aggregated data integrated into the environment. Those who've adopted CTI report improvements in the following areas:

- Ability to see attacks in context
- Accuracy of detection and response
- Faster detection and response



They are accepting and consolidating feeds through their security information and event management (SIEM) and intrusion monitoring platforms, while relying on CTI feeds from a variety of sources, including the security community and vendor-driven feeds from the various tools they are using to secure their networks, systems and data. Respondents point to strong planning (selected by 57%), leveraging internal systems and intelligence (45%), and defining gaps and workarounds (43%) as key best practices contributing to successful CTI implementations.

These best practices, along with adoption trends and definitions, are discussed in this paper.

The total "campaign" involved in an advanced threat scenario may lead us to ask such questions as: "Who is targeting us?" "What methods are they using?" and "What systems are they after?" Understanding what you want to know about threat actors and their methods, and how to prevent or detect attacks, can help immensely when shaping policies and actions and allotting time to mitigate.

Figure 1 displays the different stages of a typical attack campaign and responses leading back to actor attribution. CTI can help victims more readily identify delivery mechanisms, indicators of compromise across infrastructure, and potentially actors and specific motivators as well.

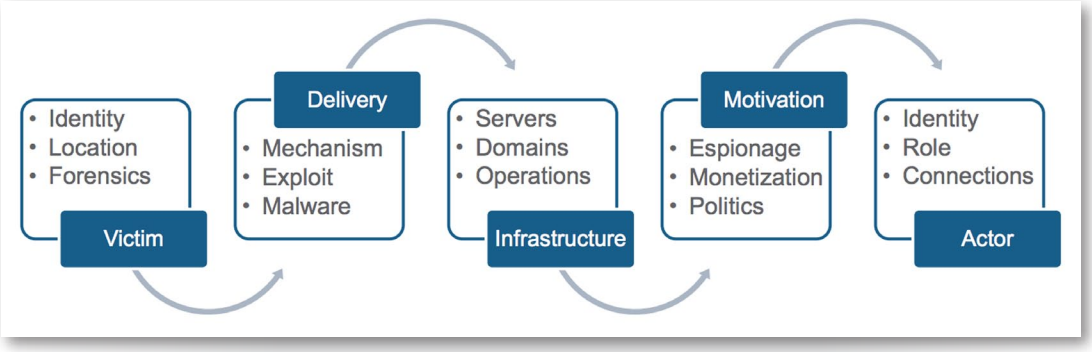


Figure 1. Stages of a Cyber Attack[2]

Cyberthreat intelligence, when used correctly, can help defenders detect attacks during—and ideally before—these stages by providing indicators of actions taken during every stage of the attack. For example, Graham Thomson, chief information security officer (CISO) at a financial group in the UK, is suspicious of logons and other key activities outside of the organization's areas of business.[3]

[2] www.countermeasure2012.com/presentations/VILLENEUVE.pdf

[3] Stephen Northcutt interviewed Thomson for his perspective on cyberthreat intelligence.

Some of the places defenders can detect these indicators of attack include logs, system reports and security alerts that can provide the following visibility:

- Account lockouts by asset and user
- All database access events (success/fail)
- Asset creation and deletion
- Configuration modifications to critical systems
- External activity to commonly hacked ports (1080, 135, 139, 1433, 21, 22, 23, 3306, 3389, 445)
- Activity on honeypot assets or files
- Login and access logs
- Denial-of-service attacks
- IDS and/or IPS events

The actual indicators they look for in these and other systems include:

- Activity in accounts of former staff
- Activity on same asset with different user names (within short time period)
- Outside-of-hours logins to systems with critical data
- Outside-of-hours systems' access by system and user
- Brute force logins
- Privileged accounts created or changed
- Remote email access from countries not typically involved in normal business operations
- Remote logins from countries not typically involved in normal business operations
- Repeated unsuccessful logins (administrative and user) by asset
- Systems accessed as root or administrator
- Traffic between test and development or live environments
- User logged in from two or more assets simultaneously

Respondents

The top industries represented in this survey—government (19%), banking and finance (16%) and IT (10%)—have been involved in threat intelligence for a long time. The survey base also represented a number of other industries, as shown in Figure 2.

What is your organization's primary industry?

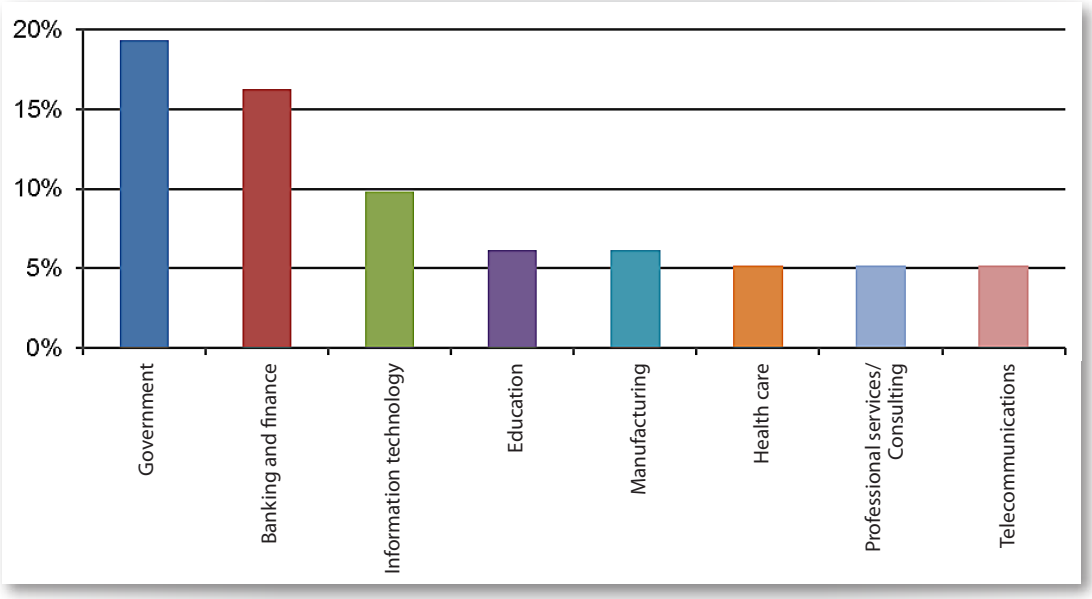


Figure 2. Top Industries Represented by Survey Respondents

Respondents' organizations ranged in size from very small (fewer than 100 employees) to very large (more than 15,000 employees), with the majority (72%) based in the U.S. Roughly one-third of survey respondents are in organizations larger than 10,000 employees, with another third ranging from 1,000–10,000 and the final third representing organizations with fewer than 1,000 employees.

All other major regions are well represented, with Europe and Asia-Pacific (APAC) coming in second and third, with 37% and 30%, respectively, as illustrated in Figure 3.

In which countries or regions is your organization located?
Select all that apply.

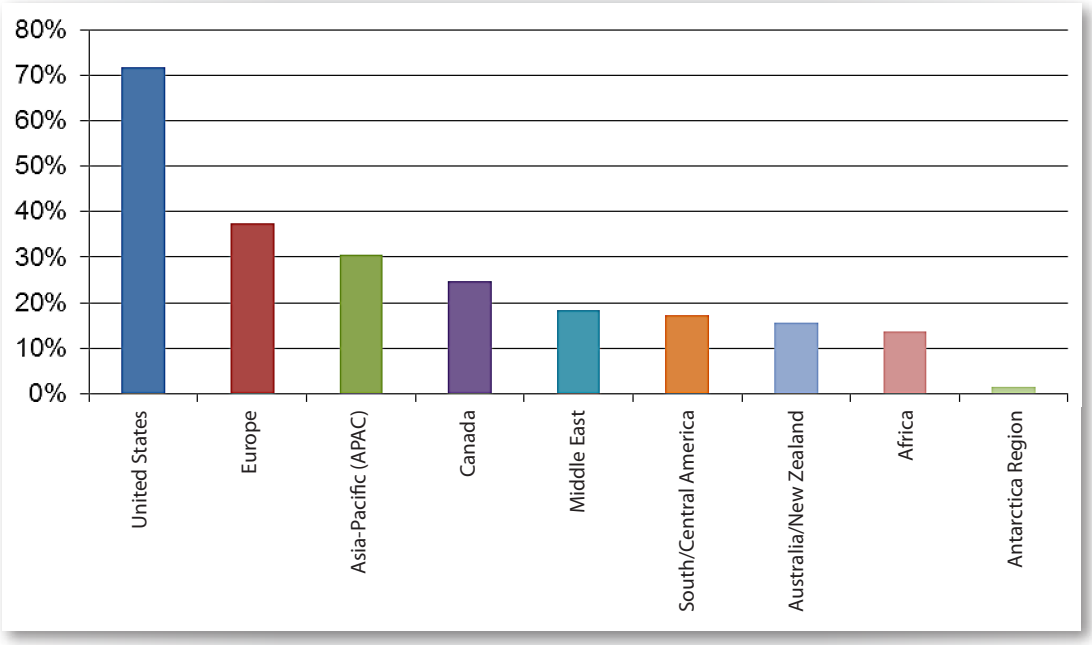
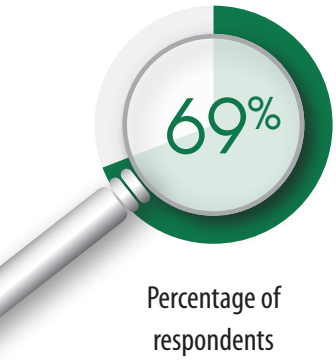


Figure 3. Regions Represented in the CTI Survey

Security administrators and analysts, actively working in more technical security-oriented roles through which threat intelligence would be implemented, make up 34% of the survey sample. However, 11% work in technical networking or systems administration roles without security titles, illustrating that some of the silos between security and network operations are breaking down. Another 19% are in security management positions (security manager, security director, chief security officer or CISO), and 9% fill other IT management roles. Smaller numbers of respondents cover the gamut of positions, ranging from IT operations and management to auditing and compliance, risk management, and systems and security architecture.

Awareness and Consumption of CTI



Percentage of respondents implementing CTI to some extent

To get a sense for how aware respondent organizations are of CTI and its potential use cases, we asked professionals whether their teams produced, consumed and/or used CTI for detection and response. The majority fully or partially embrace this concept, while only 7% are unaware of the concept:

- 27% indicated that their teams have fully embraced the concept of CTI and integrated response policies across systems and staff.
- 41% have partially embraced CTI concepts by applying some intelligence to monitoring and incident response processes, but also indicated that have a long way to go for full integration into response procedures and systems.
- 16% haven't implemented any procedures yet, but are aware of CTI and plan to start deriving and/or using intelligence in the next 12 months.
- 8% don't currently use CTI and have no plans to adopt the concept.
- 7% aren't aware of CTI at all.

Those who partially embraced the concepts admit to having a long way to go for full integration of CTI into their response procedures and systems. Still, this marks a significant shift in information security. More than two-thirds (69%) of respondents are implementing CTI to some extent. However, just over 27% of respondents are actively using CTI extensively and 41% are heading down the path of CTI implementation. This also coincides with the rapid rise in vendor product and service offerings, as well as integration capabilities with existing detection and response tools.

CTI Investment

Organizations are already investing time and money into people and services for CTI, with 64% of respondents indicating that they have a dedicated team, person or services organization working to implement and monitor CTI information for their organizations. The majority (34%) say they are building an internal team, and 14% are dedicating a single person to CTI, as shown in Figure 4.

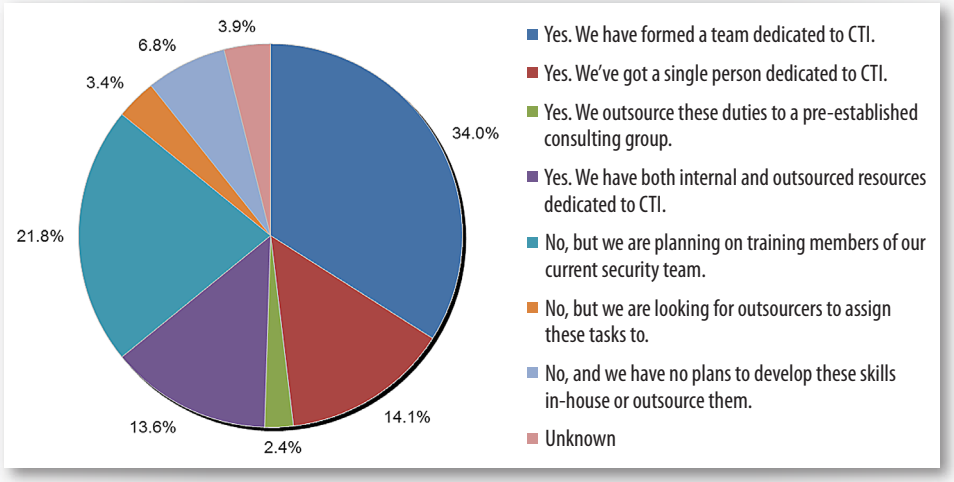


Figure 4. Staffing Plans for Implementing and Using CTI

Critical Elements

Most organizations are making good progress in achieving implementation of CTI concepts, with full or partial achievement across most categories of CTI capabilities, as shown in Table 1.

Table 1. CTI Elements and Planning

Answer Options	Planned for next 12 months	Partially achieved	Achieved
Tools and presentation methods for effective visualization and understanding of CTI	23.3%	37.7%	15.7%
Ability to aggregate information from virtually every source	29.6%	33.3%	11.9%
Data aggregated from reliable sources and cross-correlated for accuracy	26.4%	34.0%	11.9%
Raw, unfiltered feed(s) that can provide answers for my organization on possible threats	18.2%	32.7%	20.8%
Accurate, timely and complete (as possible)	21.4%	38.4%	11.3%
Full-picture view that wraps events with indicators of compromise	28.9%	32.1%	8.8%
Processed, sorted information that is evaluated and interpreted using machine learning	25.8%	29.6%	10.1%
Only completely actionable events are brought to our attention, while other event information is stored for analysis	22.6%	31.4%	10.1%
Other	6.3%	5.0%	3.1%

The top focal area for planning in the next 12 months is the ability to aggregate information from any source.

The most common elements of CTI that have been achieved by organizations at this point in their development include raw, unfiltered data feeds with CTI information, tools to visualize and analyze CTI, and a wide variety of accurate and aggregated data integrated into the environment.

There is also some sense of accuracy and timeliness related to CTI integration and use. Surprisingly, almost a third of respondents felt that they had partially achieved all aspects of CTI, including those previously noted and more advanced concepts such as differentiation of actionable versus nonactionable events, processed and sorted information, and a full-picture view of events and possible indicators of compromise.

Now they need to work on aggregating it all to detect indicators of compromise quickly and respond accurately. Therefore, respondents' top focal area for planning in the next 12 months, chosen by 30% of respondents, is the ability to aggregate information from any source. Another 29% are planning to add tools and processes that offer a "full-picture view" of events and indicators of compromise.

Tools and Tactics

To get to that visibility, 55% are currently using SIEM, and 54% are using intrusion monitoring platforms to aggregate, analyze and present CTI. This makes sense, because many of the SIEM and intrusion monitoring products are now able to collect and make use of CTI data from a variety of sources. See Figure 5.

Which of the following tools are you using to aggregate, analyze and/or present CTI information? ***Select all that apply.***

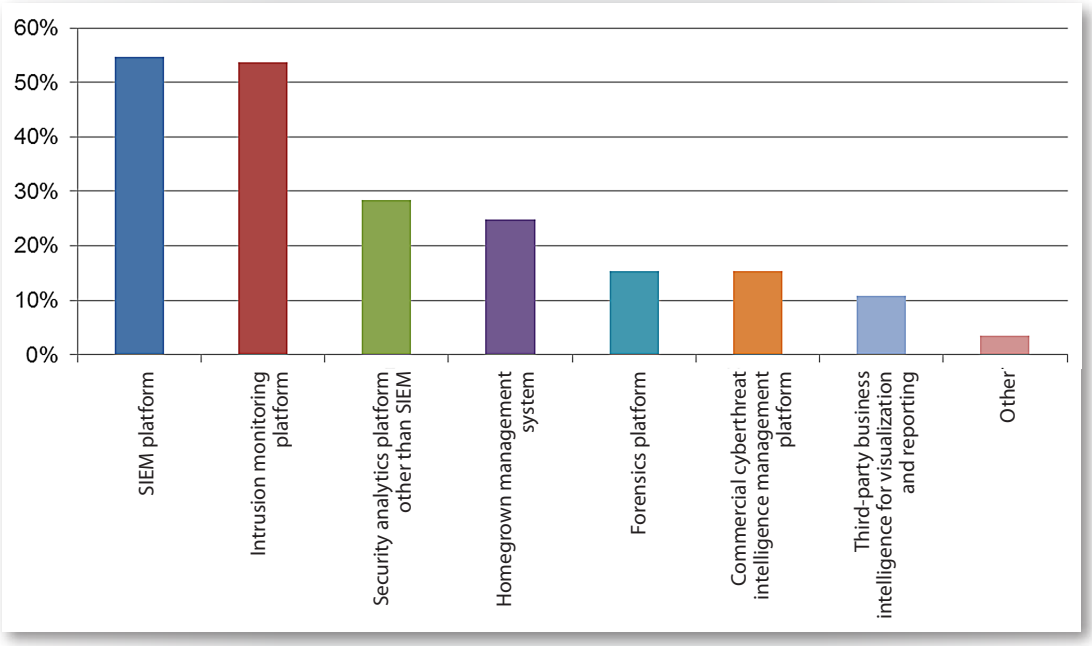


Figure 5. Tools for Aggregating and Using CTI

Another 28% are using other types of analytics platforms to aggregate and use CTI data, with 25% using some sort of homegrown tools. Others are using dedicated CTI platforms from vendors, forensics tools and third-party business services. At first glance, this seems to indicate that organizations are using every type of tool or service available to collect, aggregate and use CTI data. On the surface, that's at least partially true today.

Varying Degrees

Most organizations are not yet mature at gathering or using CTI. However, the trend is obvious: CTI is yet another type of event or profile data that contributes to security monitoring and response, and most organizations are accustomed to using SIEM and intrusion monitoring platforms for this purpose. A variety of homegrown response tools will also be factors, but they will usually come as a result of individual vendor offerings within their own tools. As noted in the 2014 SANS Analytics and Intelligence Survey,[4] 61% of security professionals say that big data or analytics will play at least some role in detection and response efforts, and CTI will naturally feed into those platforms as the analytics market matures, as well.

In addition to the 59% stating they are gathering intelligence from their internal systems, 76% of respondents say their organizations are gathering intelligence from the security community at large. The external sources they are gathering information from include:

- 56% gather intelligence from their vendor product's CTI feeds
- 54% gather intelligence from their public CTI feeds
- 53% gather intelligence from open source feeds

A small number of answers in the "Other" category included private feeds for government agencies and law enforcement, as well as social media and sites such as the SANS Internet Storm Center (ISC).

[4] www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507

Intelligence Feeds

We asked those who selected "vendor-driven CTI feeds" what types of vendors were providing these. The range of responses was very broad, and many teams are obviously using CTI data from a number of different types of vendors. Endpoint security vendors led with 51%, but 43% of respondents are also getting CTI information from unified threat management (UTM)/firewall/IDS vendors and 40% from CTI platform vendors, vulnerability management providers and SIEM vendors. Smaller numbers are getting intelligence data from application security vendors and a variety of others, as shown in Figure 6.

If you selected "vendor-driven CTI feeds," please indicate what types you use.
Select all that apply.

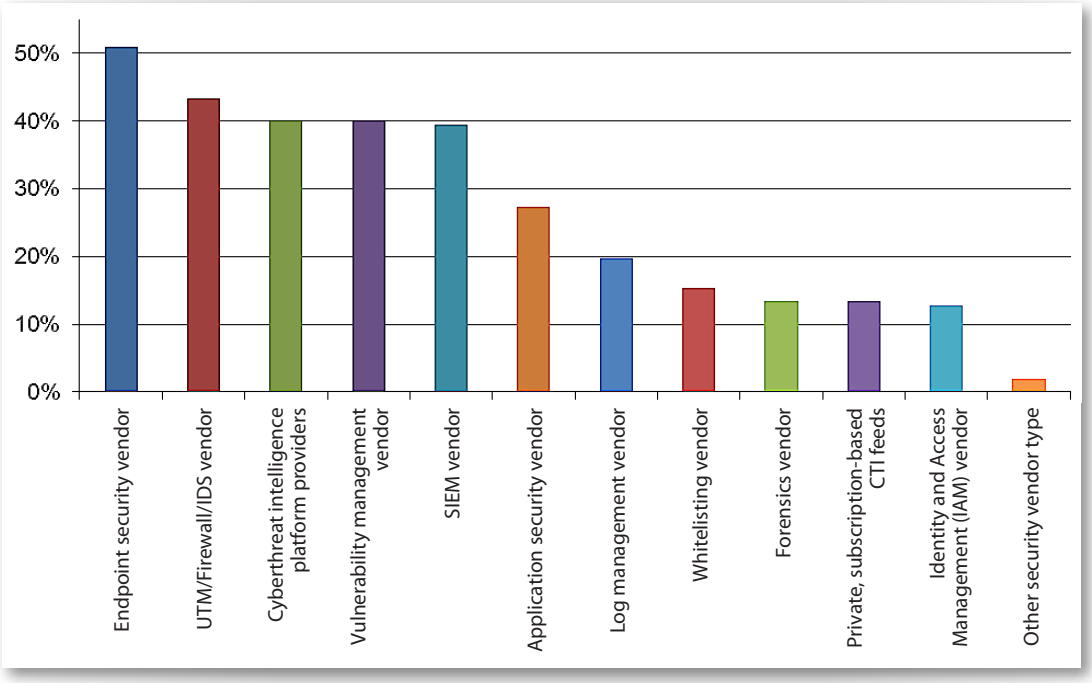


Figure 6. Vendors Providing CTI Data

Much of the tactical threat intelligence data consists of specific attacker attributes and granular indicators of compromise. Network and host-based security vendors that regularly see malware samples, malicious network traffic patterns and signatures, and real attacks emanating from certain subnets and systems are in a better position to provide tactical data than many other vendors, which may explain the higher percentages in these categories. Vulnerability management vendors have real-time experience with malware, exploits and vulnerabilities in systems and applications, which can also provide highly useful information.

The question now is: How are all these feeds coming together to detect indicators of compromise and improve response? We discuss this in the next sections.

Improving Detection and Response

When it comes to cyberthreat intelligence, Mason Pokladnik, manager of IT operations at Walter P. Moore, an international engineering firm, wants his solution to provide these top three advantages:[5]

1. **Provide true intelligence.** His team needs distilled information on new persistence mechanisms, including command and control channels (such as fake images, DNS names and cascading style sheets), to keep consumers of intelligence situationally aware, with drill-down information and links to source data if needed.
2. **Help find evil.** Which systems are talking to a certain IP address or performing a DNS lookup for a suspicious site? Which endpoints are running the same suspicious process, and how long has it been there? This level of context should be available with easy searches and alerts.
3. **Help them respond.** Along with basic vulnerability information, tell the team how to identify vulnerable hosts and fully remediate them. For example, with Heartbleed they'd need to re-issue SSL certificates with a new private key. Continue to notify clients when new information becomes available, while providing workarounds when patches are not immediately available. Of those that are implementing CTI, 63% of respondents indicated that CTI did, in fact, contribute to improving detection and response. Within the survey, 28% of those implementing CTI reported 25% improvement in context, accuracy or speed in their ability to detect and handle incidents (see Figure 7).

Can you estimate overall how your CTI tools and processes have improved your organization's response to events in terms of context, accuracy and/or speed?

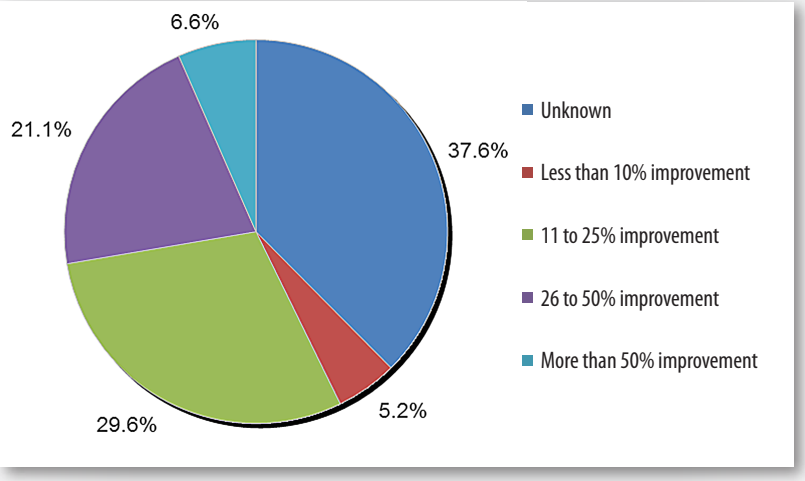


Figure 7. Percentage improvement with CTI

These results are promising in light of recent breaches, in which infiltrators entered, spread and had the time they needed to gut the affected companies of their intellectual property and personal employee data. In high-profile attacks, time and accuracy of detection information is critical for reducing the fallout of such attacks.

[5] Stephen Northcutt interviewed Pokladnik for his perspective on cyberthreat security.

What's Improving

Improved visibility into attack methodologies was reported by 63% of respondents. As the attacker landscape has gotten more sophisticated, understanding the malware tactics is vital. With this improved visibility and context, 51% said they are able to respond more quickly to incidents. Another 48% say their use of CTI has reduced incidents through early prevention, as shown in Figure 8.

TAKEAWAY:

CTI helps improve visibility into attack methodologies and improves speed and accuracy of incident response.

Please select all the options that describe how the use of CTI has improved your security and response.

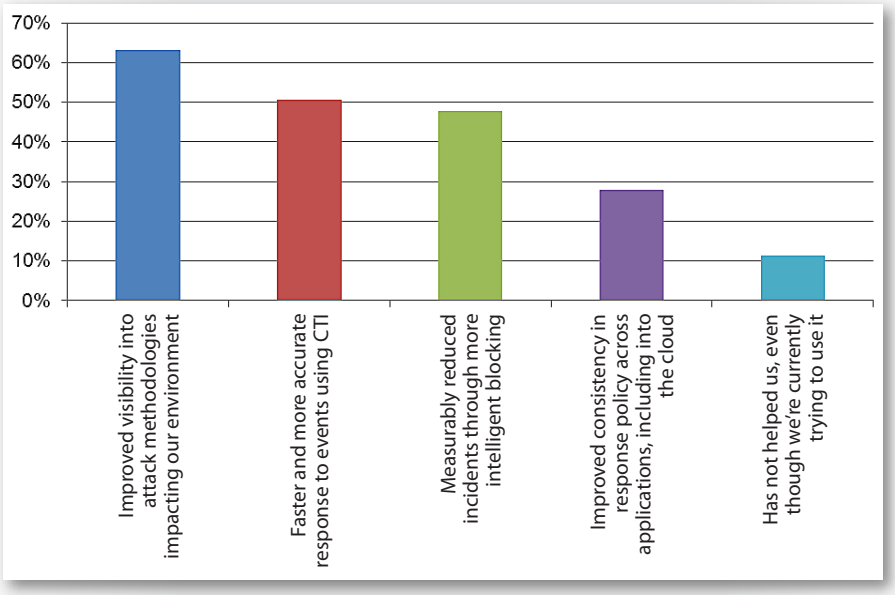


Figure 8. How CTI Improves Detection and Response

With CTI, defenders can gain some insight into the types of malware, delivery mechanisms, local exploits, network traffic patterns and overall attack strategies other organizations are seeing in the wild. For this reason, visibility into attacker strategy and tactics is considered by many to be the most valuable benefit of CTI currently. With sound CTI data, security teams can more readily look for indicators and patterns of malicious activity, and thus respond more rapidly. Over time, this will naturally lead to fewer incidents or more consistent approaches to incident detection and analysis in enterprise environments.

Integrating CTI Feeds

Responses show that organizations are integrating many tools into their CTI feed information, including their edge and host security, application security, identity and access management (IAM) systems, and vulnerability management systems, as shown in Table 2.

Table 2. CTI Integration for Detection and Response

Answer Options	Detection	Response	Both
Firewalls/UTMs	25.3%	8.9%	39.2%
IPS	22.2%	10.1%	41.1%
Vulnerability management	28.5%	12.7%	30.4%
SIEM	26.6%	8.2%	31.6%
Host security systems	15.8%	7.6%	34.8%
Application security systems	19.0%	7.0%	27.2%
Identity and access management	17.1%	7.6%	25.9%
Forensics analysis tools	13.3%	18.4%	17.7%
Analytics platform other than SIEM	12.0%	7.0%	21.5%
Big data (Hadoop, commercial solutions built around Hadoop)	13.3%	6.3%	13.9%
Other	0.0%	3.8%	5.7%

These results indicate that more security teams have successfully integrated CTI into detection tools than into response tools. For detection only, the top tools for integration include vulnerability management, SIEM, firewalls and UTM platforms (with IPS following close behind). For response tool integration, only forensic analysis tools and vulnerability management made a significant contribution in terms of integration.

The most promising indicator of CTI integration is shown in the survey responses that demonstrate both detection and response, which include a total of 41% that integrate with IPS, 39% that integrate with firewalls and UTMs, and 35% integrated with their host security systems. All of these tools allow for both detection and blocking/quarantining of threats, which aligns well with the purpose of integrating CTI in the first place (better visibility and more rapid detection and response).

Organizations found a number of ways to integrate CTI data feeds into these defense and response systems. For example, 45% used prebuilt connectors from vendors, 34% utilized custom APIs and vendor-provided APIs and API development kits, while 33% engaged the services of intelligence service providers and third-party integrators. A small percentage of responses mentioned manual processing and CTI feed and transport formats.

CTI Best Practices

When it comes to the best practices for integrating CTI intelligence into their detection and response programs, 57% feel that strong planning is key to their success, 45% find success in leveraging internal systems and intelligence, and another 43% define gaps and workarounds. Finding talent was also noted as important by 42%, as was looking at and attempting to adhere to emerging CTI data standards (37%). A number of other best practices are listed in Figure 9.

What do you consider the best practices you use to update and integrate CTI into your systems? ***Select all that apply.***

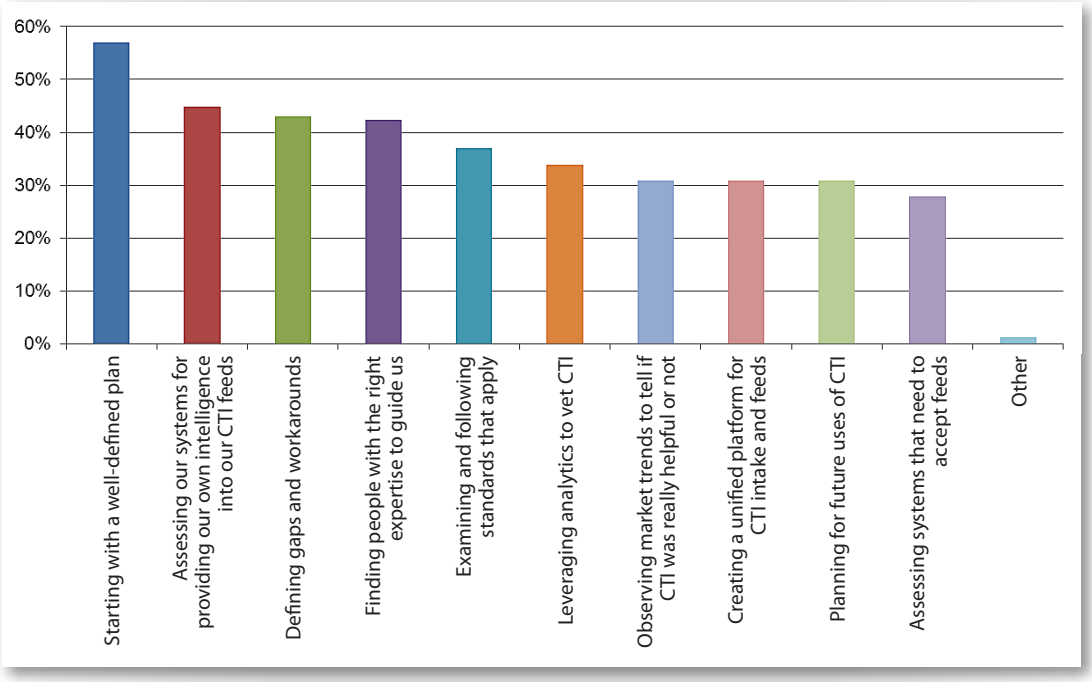


Figure 9. CTI Integration Best Practices

Planning for CTI

Organizations planning to invest in CTI feeds, tools and internal capabilities should assess their readiness for using CTI now and in the future.

1. **Decide what you intend to do with CTI data and to whom you will assign to CTI planning duties.** Most organizations that attempt to implement CTI ad hoc, with no budget, staff, tools or goals, tend to reap minimal rewards.
2. **Focus on tools and feeds.** Once you've decided what you plan to do with CTI (improve detection capabilities, add more granular correlation rules to your SIEM, add host-based forensics indicators, etc.), focus on two areas: What kinds of tools will you use to aggregate and collect CTI data? And will you use commercial feeds, open source and community data, or both? Many SIEM providers are now integrating CTI feeds and information readily. Be sure to look at standard import data formats if you are bringing in feeds.
3. **Consider your goals.** Once you've decided on the basics of what data you want and where it will be aggregated, think about the short- and long-term goals of the program and how you'll measure progress.

The Importance of Good Help

Interestingly, while 42% cite finding the right talent as a best practice, 35% of respondents stated that they lack budget and staff to support their CTI programs, as shown in Figure 10.

What is holding your organization back from achieving integrated CTI capabilities?

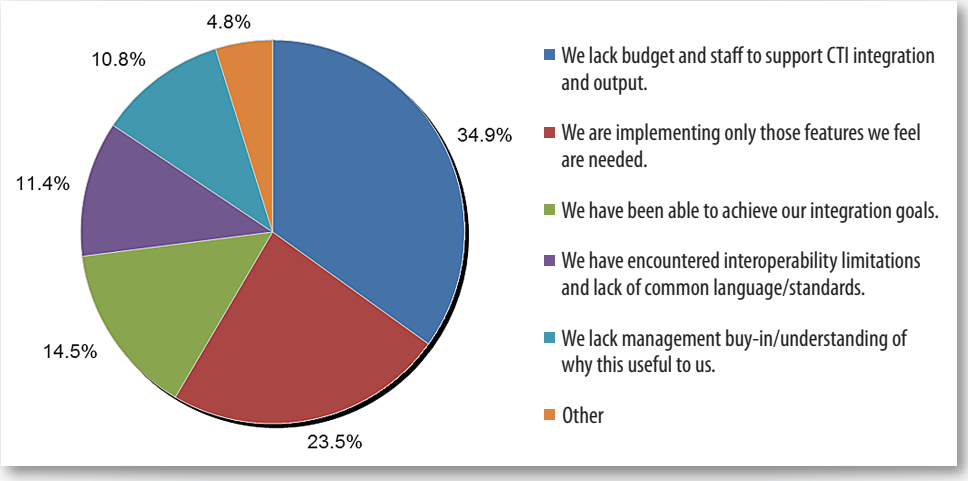


Figure 10. Limitations in CTI Implementation

Respondents cited knowledge of normal network and systems operations, followed by data analysis capabilities, knowledge of indicators of compromise, and incident response skills as the most valuable skill sets to have for managing CTI. Last on their list was familiarity with new commercial tools.

Other issues holding organizations back from more thorough adoption and use of CTI are lack of management buy-in and interoperability.

CTI Standards and Tools

While it is not the biggest issue being encountered, a shortage of standards and interoperability around feeds, context and detection may become more problematic as more organizations add more sources of CTI into their detection and response programs.

Without the proper standardization of CTI feed information, organizations could still miss indicators of compromise.

"Vulnerability data from the infrastructure side and the web application side could be better standardized. CVE and CVSS are great places to start by providing taxonomy and common nomenclature, and they provide a great way to quickly name/categorize a finding so multiple analysts from different organizations are speaking about the same finding/weakness," says David Screws, director of security engineering at Equifax.[6] "Then it all starts to break down when information is coming from vendors and the internal team supporting vendor tools."

As an example, he describes a response scenario in which Microsoft contends that local privilege escalation is only a medium priority. That priority level, combined with the threat researcher who may or may not have written proof of concept code, the fresh information from a researcher who opened the incident definition, the unique organizational environment and compensating controls, and the external alert involving the attacker who posted alarmist code on exploit-dB, presents a difficult detection and response scenario. Says Screws, "When gathering all this related data, different security vendors seem to have come from different planets."

[6] Stephen Northcutt interviewed Screws for his perspective on cyberthreat security.

On CTI formats, Pokladnik from Walter P. Moore adds: "If you're sending indicators of compromise, please add value by also sending them prepackaged in a standard format [OpenIOC, STIX, Snort signatures].

Interestingly, only 38% are using CTI data in "standard" formats and well-known open source toolkits. Those that do, employ the following:

- Open Threat Exchange (OTX)—51%
- Structured Threat Information Expression (STIX)—46%
- Collective Intelligence Framework (CIF)—39%
- Open Indicators of Compromise (OpenIOC) framework—33%
- Trusted Automated eXchange of Indicator Information (TAXII)—33%
- Traffic Light Protocol (TLP)—28%
- Cyber Observable eXpression (CybOX)—26%
- Incident Object Description and Exchange Format (IODEF)—23%
- Vocabulary for Event Recording and Incident Sharing (VERIS)—20%

OTX is very popular tool, with 51% of respondents using it. And CIF is also well-used, at 39%. While OpenIOC is in use by 33% of organizations, the clear majority uses the set of standards that include STIX, TAXII and CybOX. All of these standards and tools are still very much works in progress; however, the author has seen STIX and TAXII most commonly in enterprise organizations.

Cloud Considerations

As another indicator of how CTI is growing with our ever-changing enterprise architecture and IT operations, 50% of respondents indicated that CTI currently extended to their cloud and virtual environments. Another 19% plan to extend CTI there in the next 12 months, as shown in Figure 11.

Does your CTI program extend to cloud and virtual environments?

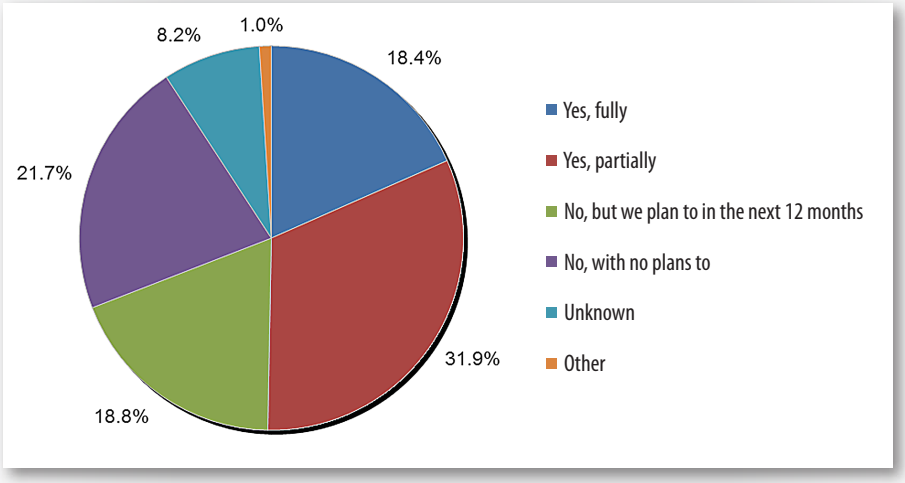


Figure 11. CTI Extending to Cloud and Virtual Environments

The major difference in collecting and using CTI information in cloud environments is the level of visibility and control that organizations may have into cloud-based assets. For example, CTI that emphasizes network traffic behavioral patterns or indicators and logs on hypervisor platforms may be less effective (or completely ineffective) in cloud environments because security teams may not have this level of visibility and/or control.

Looking Forward

When asked about how useful CTI would be for defense and response over the next five years, 75% of respondents felt it was very important and would be embedded into most detection and response systems. Another 20% felt it would be somewhat important, but wouldn't be an embedded, ubiquitous part of detection and response, and just 1% think it's a fad or another layer of security we don't need.

CTI is here to stay, but it's definitely not currently a mature area for most organizations. Today, large enterprises and government agencies will likely have more experience in CTI implementation and more budget to invest in technologies and staff focused on CTI. The state of vendor offerings in CTI is also very ill-defined at the moment. Few organizations understand how to differentiate good intelligence from mediocre intelligence data, and it will take more time for the market to flesh out the most useful types of data and for providers to mature and provide more-effective tools. All of the data structure and delivery formatting standards are still being debated as well—and although STIX and TAXII seem to be common, there's no guarantee these will end up being the only formats used by commercial and open source CTI providers. Most organizations should start planning for CTI (if they haven't already) and investigate options in tools, data feed sources and internal use cases.

Conclusion

CTI is likely here to stay and is growing more mature and important. More tools are integrating CTI feeds and data, and teams are currently seeing improvements in detection and response capabilities as a result.

Interestingly, we are seeing these improvements even during incremental adoption. Thus, the process of CTI collection, consumption and utilization will continue to improve as adoption grows and becomes more thorough in enterprise organizations. As it does, providers of CTI information will need to focus on accuracy, standardized methods of expressing indicators of compromise and more automated processes that tie detection to response actions.

Many survey respondents provided general comments and suggestions on what they feel is needed to improve CTI and make it more impactful now and over time. The majority of comments focused on automation, better real-time intelligence, and improved vetting and accuracy of intelligence data. Numerous respondents mentioned improvements in standards and tools that can collect, digest and integrate CTI. Watch for rapid advancements from vendors and the security community alike.

About the Author

Dave Shackleford is the founder and principal consultant with Voodoo Security, a SANS analyst, instructor and course author, and a GIAC technical director. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. He is a VMware vExpert and 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 is the author of the Sybex book *Virtualization Security*. Recently, Dave co-authored the first published course on virtualization security for the SANS Institute. Dave currently serves on the board of directors at the SANS Technology Institute and helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsors

SANS would like to thank this survey's sponsors:

Last Updated: January 31st, 2016

Upcoming SANS Training

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

SANS Scottsdale 2016	Scottsdale, AZUS	Feb 08, 2016 - Feb 13, 2016	Live Event
SANS Secure Japan 2016	Tokyo, JP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
Cyber Threat Intelligence Summit & Training	OnlineVAUS	Feb 03, 2016 - Feb 10, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced