SANS | Research Program

Survey

SANS CTI Survey 2024: Managing the Evolving Threat Landscape

Written by **Rebekah Brown** and **Andreas Sfakianakis**

May 2024

ANOMALI

Executive Summary

Over the past year, cyber threats have once again been top of mind for many organizations. The global geopolitical situation, evolving ransomware attacks, and the widespread use of emerging technologies such as generative AI have kept many CTI teams on their toes. In this year's survey we deep dive into how CTI professionals manage these tasks, the tools and cutting-edge technologies that support their work, and the challenges and opportunities they see ahead. Key survey findings include:

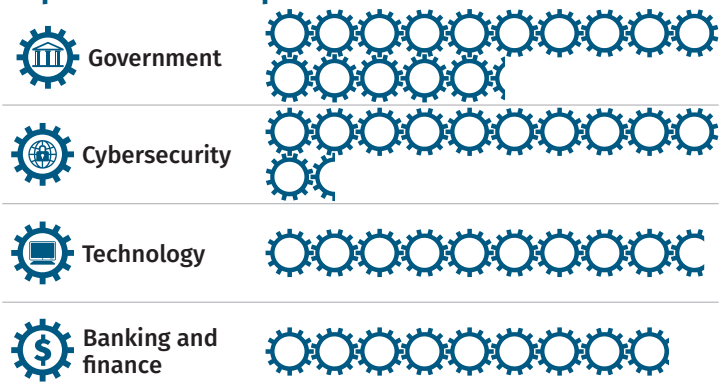
- Geopolitical and regulation landscapes are critical in the CTI team's tasks. Global conflicts often lead to increased cyber espionage, sabotage, and misinformation campaigns that CTI teams may get questions about or need to respond to. Similarly, new regulations may change a CTI team's requirements or drive the need for new processes. Both areas are covered in detail in the report.
- This year's survey highlights a key use for CTI teams—threat hunting. Threat hunting is a proactive approach for detecting threats that are either unidentified or not yet remediated within an organization's network. For the first time in the survey's history, it is the top use case for cyber threat intelligence.
- AI is starting to make its mark on CTI—nearly one quarter of respondents report leveraging AI in their CTI program, and another 38% of respondents plan to use it. Although many analysts are using AI themselves, there is also a growing concern about the adversarial use of AI and how defenders can prepare themselves to counter that threat.

Survey Respondents

This year, we received responses from 811 professionals from 22 industries, as shown in the word cloud and Figure 1 (seen on the next page). We saw significant expansion in transportation, legal, construction, real estate, food and agriculture, and gaming sectors. We also found:

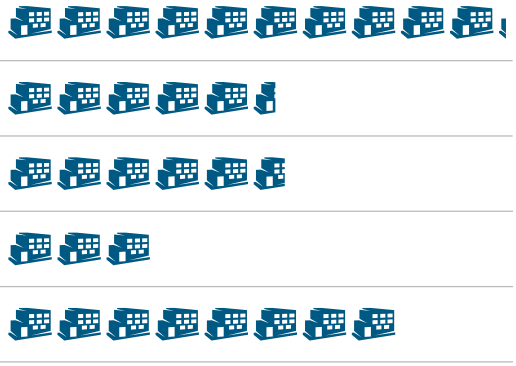
- The highest percentage of respondents came from an organization of 100,000 or more employees, followed by organizations with fewer than 100 employees.
- Three quarters of our respondents were from organizations headquartered in the United States. This was followed by organizations headquartered in the EU, at 10% of respondents.
- Government, cybersecurity, technology, and banking/finance sectors led in response rates for the eighth year. Responses from these four industries accounted for 56% of the total responses.

Top 4 Industries Represented



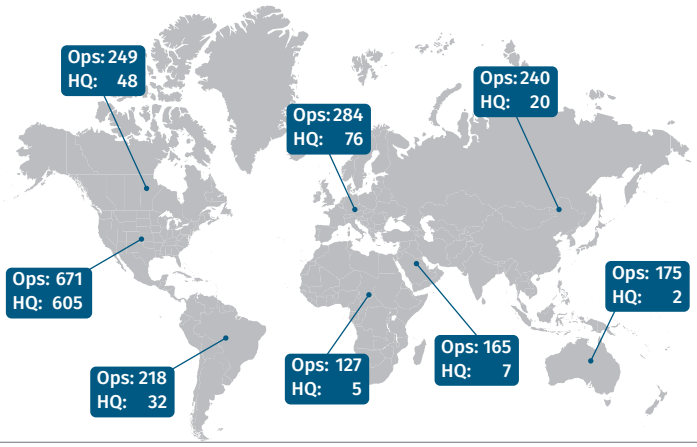
Each gear represents 10 respondents.

Organizational Size

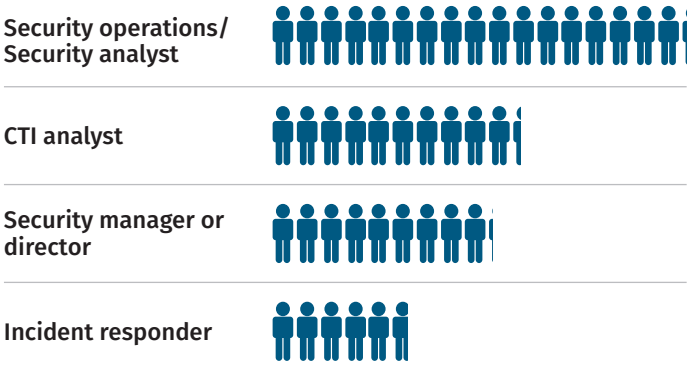


Each building represents 25 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 10 respondents.

Figure 1. Demographics of Survey Respondents

People and Teams

People are at the core of a CTI team's work. The "people" of CTI are often thought of as the analysts conducting the intelligence analysis; however, it is important to note that many individuals across an organization contribute to the CTI process. Whether they are helping create intelligence requirements, supporting CTI functions as a member of a different security team, or consuming reports from the CTI team and making decisions based on their findings, CTI truly does rely on people.

This year, we saw a significant increase in organizations that use a combination of in-house capability and a service provider, from 47% last year to 62% this year. When combined with organizations with a standalone CTI capability, 31%, the total percentage with some degree of in-house CTI capability has significantly increased from 83% last year to 93%!

Last year's trend of steady growth of organizations with dedicated CTI teams is consistent with this year's findings: 52% of organizations have a dedicated CTI team—the highest percentage we have ever seen in SANS CTI surveys. (See Figure 2.) That is not the only model for CTI teams, however. This year, one in four organizations reported that CTI is a shared responsibility with staff pulled from other security groups, indicating a "horizontal" structure of responsibilities. This percentage has been mostly stable throughout the last few years, suggesting that organizations following this approach have diverse perspectives, tooling, and increased collaboration resulting in a continuation of this model rather than an eventual move to a stand-alone team. Horizontal teams do come with challenges, and these teams may experience obstacles in coordination, have varied expertise levels, and struggle with issues related to resource allocation. Organizations struggling in these areas can assess the ideal structure of their CTI function, either as a shared responsibility or as a dedicated team.

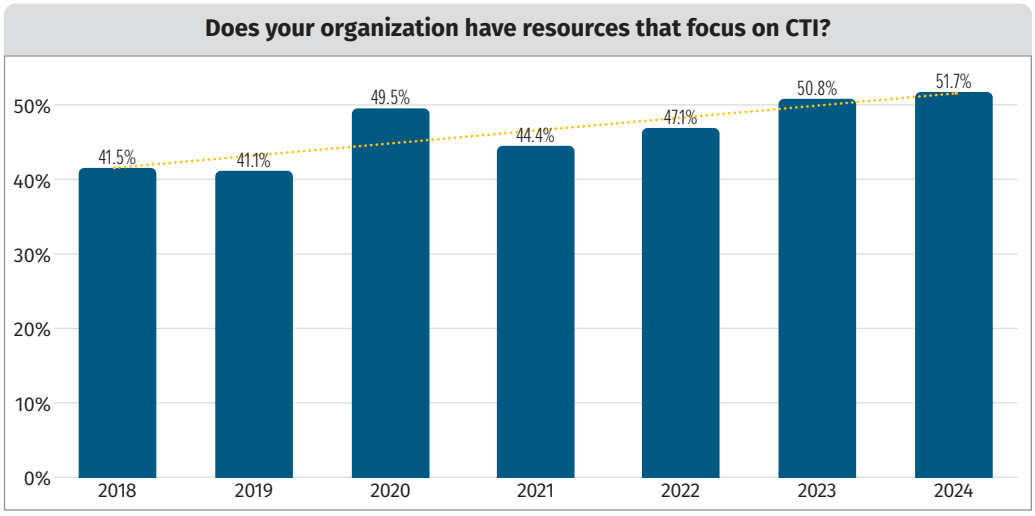


Figure 2. Growth in Organizations with Dedicated CTI Teams

This year, we introduced a question about the number of full-time equivalents (FTEs) working on CTI tasks. We observed that the clusters of 0.5–1 FTE, 1–2 FTEs, 2–4 FTEs, and >10 FTEs had similar percentages. (See Figure 3.) Nearly half of all respondents worked in organizations with between 0.5 and 4 FTEs within their CTI team. Just over 15% of the respondents are from an organization with a CTI team of more than 10 FTEs, suggesting that these are CTI teams of large organizations (more than 100,000 employees) or CTI teams of cybersecurity providers.

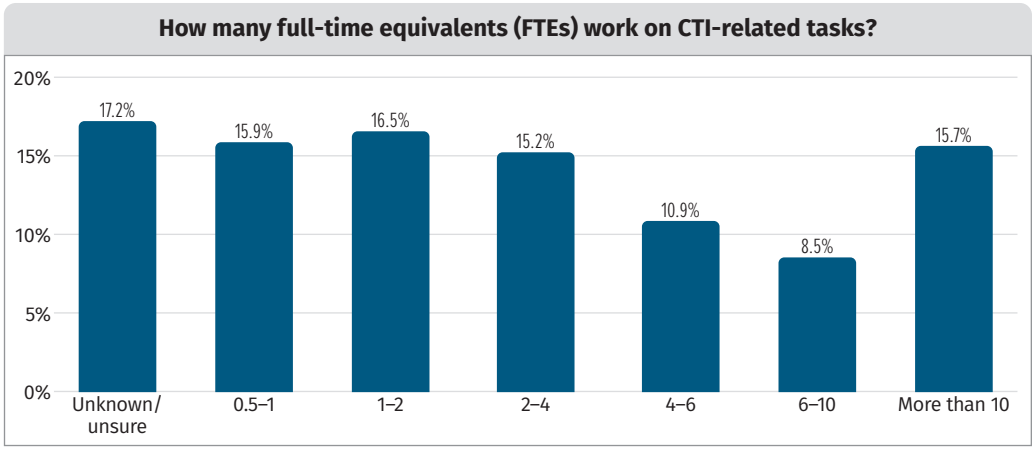


Figure 3. Staffing Levels for CTI

When it comes to the skill sets that make up the members of a CTI team, this year we saw a decrease in the respondents who identify as purely CTI analysts and an increase in security analysts, incident responders, and security managers or directors. This indicates that even though we saw a record number of dedicated CTI teams this year, the individuals that make up those teams often have other skill sets that are combined with threat intelligence capabilities or have other roles, such as a SOC analyst, that directly contribute to CTI. This could also indicate a preference for the larger scope of the "security analyst" title rather than the narrower focus of the cyber threat intelligence analyst, especially for individuals on horizontal teams who end up contributing in several places across their organization's security program.

Another interesting trend in this year's survey data is a spike in auditor roles working in the CTI field over the past two years. In 2022, less than 1% of respondents had this role; in 2024, that rate is nearly triple. This increase is most likely related to the trend observed in regulations and compliance, which we discuss more in the sections on CTI Fundamentals and Use Cases for CTI Data Utilization.

Now that we have a better understanding of the individuals and teams operating in the CTI space, we can dive more into the specifics of the work they are doing and the core CTI functions that help shape their work.

CTI Fundamentals

Although specific processes and tooling will vary from team to team, some fundamental aspects of a CTI program are beneficial to every team. Intelligence requirements, a collection plan, and a threat model are core components that provide a framework through which CTI functions can be addressed.

Intelligence Requirements

This year, just over half (52%) report that CTI requirements are clearly defined in their organization. There is also an overall increase in the number of teams that contribute to requirements, including CTI teams themselves, as well as incident response, security operations, and vulnerability management. It is also important to note that teams outside the traditional technical security focus, such as executives, business units, and risk management functions, may also have important perspectives and needs for cyber threat intelligence.

This is the first year that we included governance, risk management, and compliance as an option for teams that contribute to threat intelligence requirements, and 42% of respondents reported that these functions contributed to their requirements process. This highlights the importance of these areas, which we dive into more in the CTI Use Cases section below.

Intelligence requirements—Intelligence requirements, or CTI requirements, are a list of the most important questions about threats that a CTI program seeks to answer for its stakeholders.

Collection plan—A collection plan is used for data source identification, collection, quality, and integration. Managing this process longer term is known as collection management.

Threat model—A threat model outlines what threats have the potential to impact an organization or an individual and how likely they are to occur. Within an organization, it is important to have a process that is ideally documented so that it can be shared with other team members and stakeholders.]

Collection Plan

A CTI collection plan is crucial for structuring and managing information collection against the defined intelligence requirements. Nearly half of respondents reported that their CTI team's collection plan is clearly defined in their organization, with another 35% responding that their collection plan process is informal and ad hoc. It is encouraging to observe that most of the CTI teams have a process for their collection plan, and we expect that more teams will formalize this process in the future. Establishing a formal process for the CTI collection plan will help achieve the long-term success and efficiency of the CTI team.

Threat Model

This is the first year we asked about threat modeling as a formal process in the CTI survey. However, we have historically tracked threat modeling as a CTI use case and have seen a steady increase in its importance to an organization over the past four years.

Just under half (45%) replied that they have a formal, well-defined, and documented threat model (see Figure 4). Several write-in responses called out that they plan to use threat modeling in the future, indicating this is an area that many believe will support their use cases even if they are not currently fully implemented.

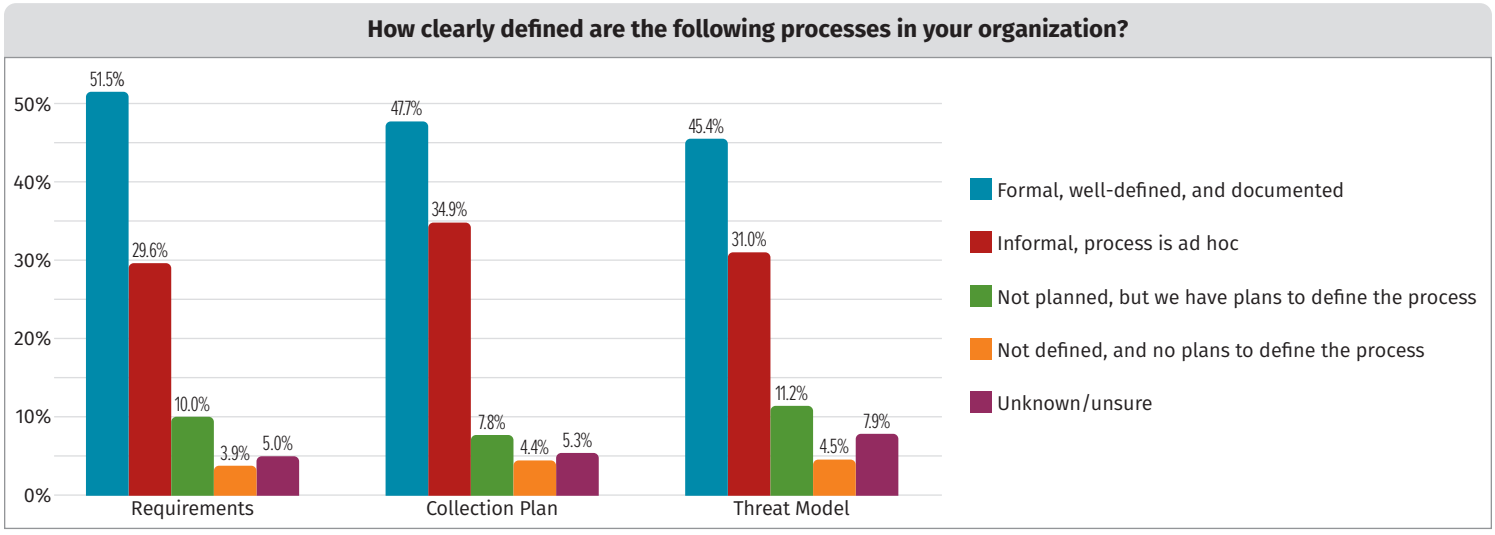


Figure 4. Formalization of CTI Processes

Threat Identification and Prioritization

Prioritizing the tasks related to CTI has historically been challenging for CTI teams. CTI analysts frequently grapple with key questions to effectively manage their workload: identifying the threat, assessing its relevance to their organization, and determining its priority compared to other threats. These decisions will need to be assessed and reassessed as new threats emerge and situations change.

To address questions around threat identification and prioritization, over half of respondents report that they dedicate at least 40% of their time to analyzing open-source intelligence (OSINT) from various sources, including research reports and cybersecurity news. (See Figure 5.) The percentage of time has decreased from the previous year, possibly due to more efficient analytical tools that swiftly pinpoint key insights and summarize findings or because vendors provide summaries of open-source reporting.

Approximately what percentage of your CTI personnel's time is spent on responding to open source reporting from others, including threat reports from researchers and cybersecurity news stories that consumers ask questions about?

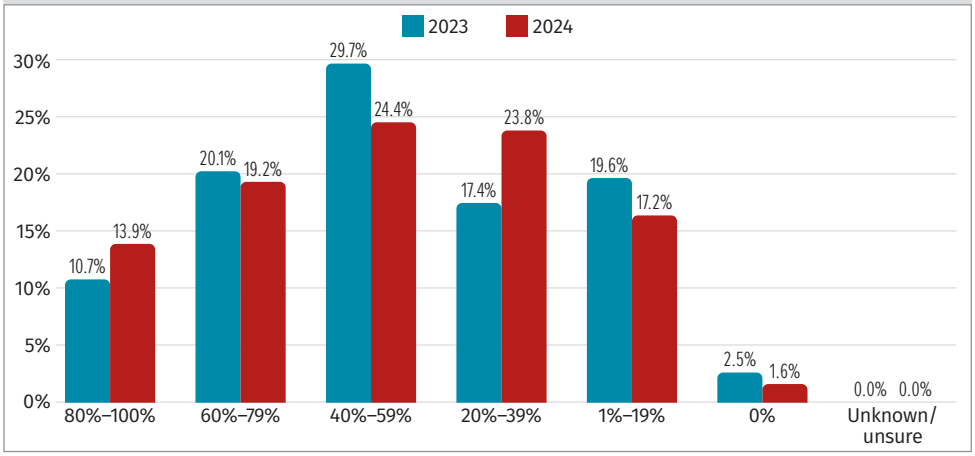


Figure 5. Time Spent Responding to Reporting

Several respondents shared their approaches for prioritizing their work, which fell under several main categories:

Prioritizing threats shared by trusted partners/peers in the organization's industry

"We ingest a lot of open-source reporting, but we also receive daily threat intel from the ISAC. We have found a high correlation in our environment to what others in the ISAC are seeing. It certainly has helped us prioritize what we look for and defend against."

Prioritizing reporting about threats related to the organization's industry, geography, and environment

"Prioritization of threat scenarios/attack paths based on reporting related to our industry, geography, and operating environment. By looking at common trends in reporting, we can draw some conclusions about where to prioritize defensive efforts."

Prioritizing internal incidents and requests for information (RFIs) from internal stakeholders

"Intel reporting based on internal incidents and then doing 'campaign analysis' to identify if any other internal incidents or reports of external incidents can be linked together to make up a given campaign."

Geopolitics

Geopolitics significantly shapes state and non-state actors' strategic interests and actions in the cyber domain. Political, military, and economic tensions between nations often lead to increased cyber espionage, sabotage, and misinformation campaigns to influence outcomes or gain strategic advantage.

Nearly 78% of the respondents reported that geopolitics plays a very important or somewhat important role in determining their intelligence requirements. (See Figure 6.) In 2023 and 2024, several key geopolitical events have shaped the CTI team's intelligence requirements worldwide, such as the war in Ukraine, the Israel–Hamas war, the Red Sea crisis, and China–Taiwan tensions.

This comment from a CTI analyst highlights how geopolitical events can influence a CTI team's priorities, even if it is just a temporary adjustment in intelligence requirements:

Our CEO made public statements about an international conflict, and though no impact was reflected in network activity, CTI analysts monitored the dark web, social media, and paid feeds for reflections, prioritizing reporting any cyber threats to the enterprise. The analysis was short-lived for three months but was very different than "brand protection/management" activity.

Figure 7. Use Cases for CTI Utilization

How important are geopolitics in developing your intelligence requirements (or tasks for the CTI function if you do not have formal requirements)?

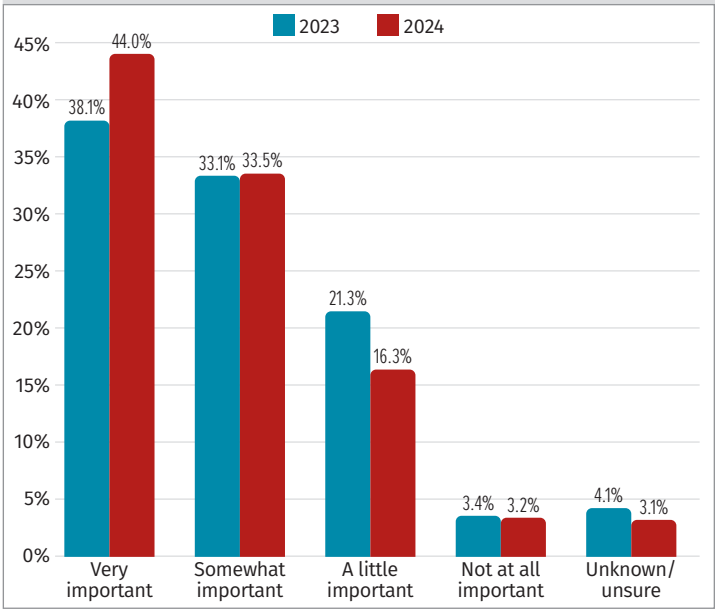


Figure 6. Impact of Geopolitics on Requirements

There are some situations where a CTI team will need to work closely with their organization's physical security and intelligence teams in response to an urgent or emerging situation. In many—but not all—situations, a physical threat also has a corresponding impact on digital security. In these situations, it is essential to identify common lines of effort and intelligence requirements and ensure that the teams work in a mutually supportive manner. Some key questions to ask are:

- **What are the geopolitical events impacting the security posture of the organization?**
- **What cyber activities can have an impact on the physical security posture of the organization?**
- **What are the cyber risks for critical physical locations of the organization (e.g., data centers)?**
- **What cyber threats may executives face when traveling to high-risk countries?**
- **What are the cyber threats related to key physical events organized by the organization?**

Leveraging CTI

One of our favorite parts of the annual CTI survey is learning more about how individuals and organizations use cyber threat intelligence to support their operations. This year, 75% of respondents mentioned that CTI is utilized for threat hunting. (See Figure 8.)

Threat hunting is a proactive approach for detecting threats that are either unidentified or not yet remediated within an organization's network. CTI plays a crucial role in this proactive identification and mitigation of threats. Over the years, respondents report a steady increase in CTI consumption of adversaries' behaviors and tactics, techniques, and procedures (TTPs), which is aligned with the wider adoption of threat hunting. Respondents report they "leverage threat intel to scope and target threat hunts against the organization" and "create threat hunt packs for particular malware or APTs." Many also highlight the use of frameworks like MITRE ATT&CK as a structured model to categorize TTPs, and communicate them via a common vocabulary.

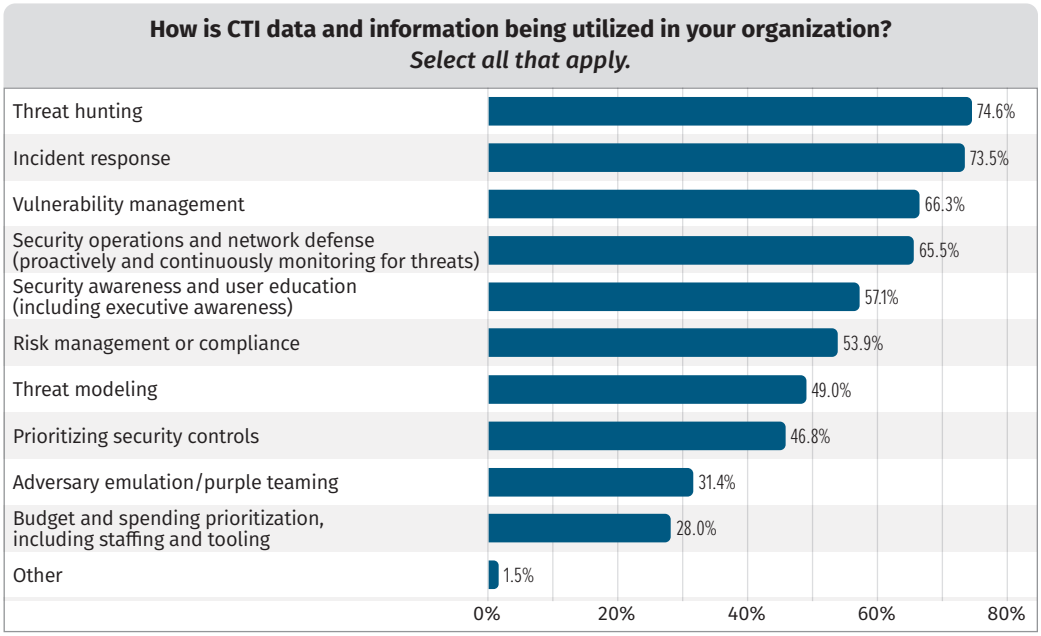


Figure 8. CTI Utilization

CTI is also increasingly used in vulnerability management, rising from 54% in 2017 to 66% this year. With 83% of respondents valuing insights on vulnerabilities exploited in the wild, CTI helps prioritize patches, especially for vulnerabilities listed in CISA's Known Exploited Vulnerabilities.[1] The growth (and increased targeting) of edge computing has also intensified the need to identify critical vulnerabilities like remote code execution that are actively exploited. Thus, CTI is utilized by vulnerability management teams to enhance their patch prioritization and end-to-end remediation processes.

New worldwide regulations impact cyber threat intelligence by imposing stringent compliance requirements across various sectors and regions. In the United States, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)[2] and new rules by the Securities and Exchange Commission (SEC)[3] introduced increased regulatory requirements, fostering a more collaborative environment between the private sector and government as well as improving the sharing and utilization of threat intelligence. Meanwhile, the EU has introduced the NIS2 Directive,[4]

[1] "CISA's Known Exploited Vulnerabilities," www.cisa.gov/known-exploited-vulnerabilities-catalog

[2] "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

[3] "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," www.sec.gov/news/press-release/2023-139

[4] "Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive)," https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

aiming to strengthen the cybersecurity requirements imposed on critical infrastructure across all member states. Australia's Security Legislation Amendment (Critical Infrastructure) Act 2021[5] and Security Legislation Amendment (Critical Infrastructure) Act 2022[6] enhance the security and resilience of critical infrastructure assets and systems of national significance by increasing the industry sectors recognized as critical infrastructure and establishing security obligations such as risk management and mandatory cyber incident reporting.

These developments are some examples across different regions that underscore the critical role of CTI in ensuring compliance with new regulations and safeguarding against cyber threats. Moreover, the ISO 27001 information security audit standard has been updated, and threat intelligence has been added as a new organizational control.[7] Organizations that want to comply with ISO 27001 will also be audited on how their threat intelligence process is implemented. All of the above have been reflected in the survey's responses—74% of respondents reported that new regulations and audit requirements play a very important or somewhat important role in CTI planning. (See Figure 9.)

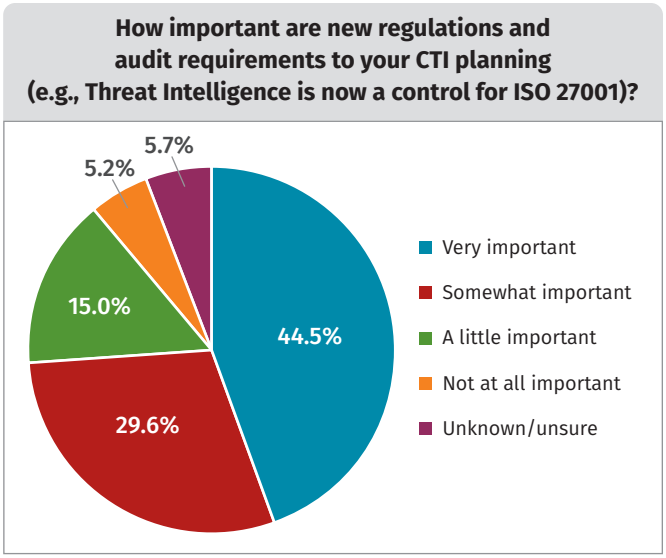


Figure 9. The Influence of Regulations on CTI Planning

Sources (Intelligence Collection)

Cyber threat intelligence involves analyzing information to provide insights about threats and their impact on an organization, and so the source of that information is incredibly important to the CTI process. It may be more accurate to say "sources" of data because this year, the percentage of respondents using each source in our survey increased across the board, showing how important it is to utilize information from many different sources.

The most used information source is external sources such as media reports and news at 86%, followed by published intelligence reports and vendor threats feeds. Internal data is used less commonly, with internal sources such as incident response and forensics data, and information from security analytics systems or a SIEM falling lower on the list. (See Figure 10.)

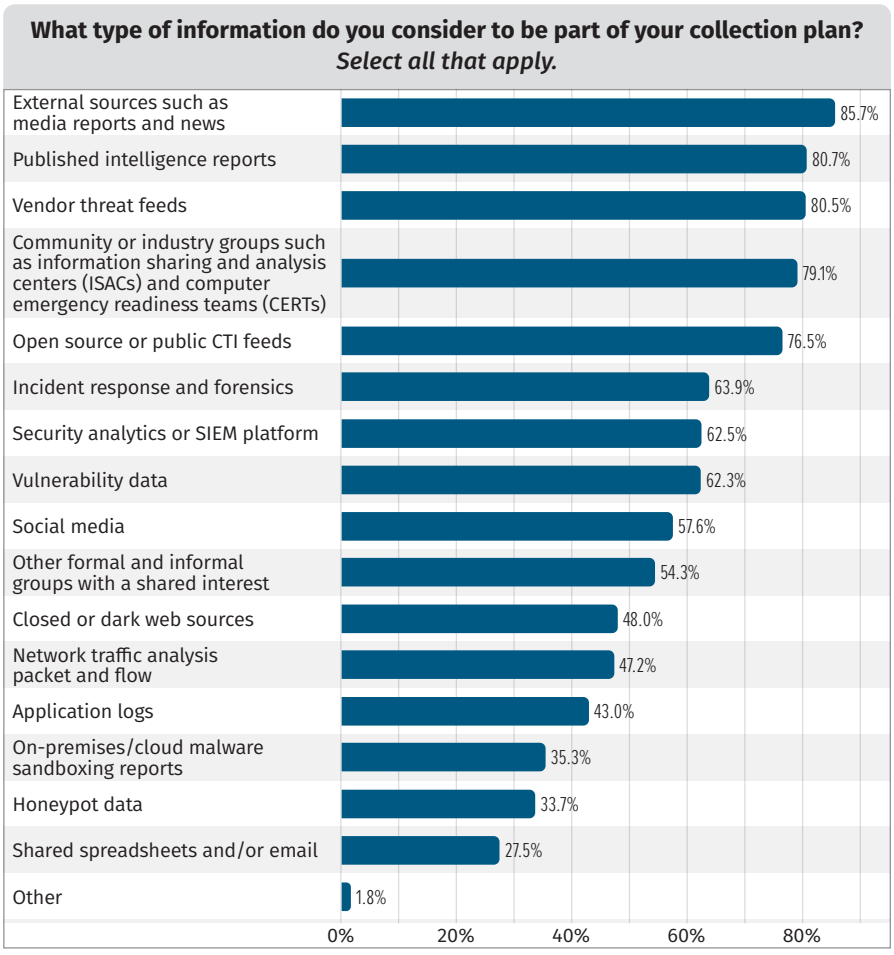


Figure 10. Data Collection Plans

[5] "Security Legislation Amendment (Critical Infrastructure) Act 2021," www.legislation.gov.au/C2021A00124/asmade/text

[6] "Security Legislation Amendment (Critical Infrastructure) Act 2022," www.legislation.gov.au/C2022A00033/asmade/text

[7] "ISO 27001:2022 Annex A Control 5.7," www.isms.online/iso-27001/annex-a/5-7-threat-intelligence-2022/

This year, we saw a general increase in using threat feeds as a data source. This could be tied to changes in the threat landscape, including rampant ransomware attacks and evolving malware-as-a-service capabilities. IOCs are more widely applicable to these types of threats, making threat feeds more valuable as a defensive mechanism. In addition, threat feeds are commonly integrated by default, with some open-source feeds automatically added as an option to ingest and most vendor threat feeds as optional add-ons.

CTI teams consistently prefer engaging with community and industry groups (79%) and other groups with shared interests (54%), highlighting the importance of external outreach and intelligence sharing. Engagement with sharing sources has steadily increased over the past five years, underscoring the need for a structured external sharing process.

This year marked a notable increase in the use of closed or dark web sources for collection, rising from 27% in 2023 to 48% in 2024. This shift may stem from more frequent reports of adversaries, like ransomware actors or access-as-a-service brokers, who leak stolen information on these closed forums.

CTI sources play a critical role in providing diverse, timely, and accurate data essential for identifying cyber threats. This emphasizes the importance of a collection plan that structures and organizes the intelligence-gathering process, ensuring access to the most relevant and actionable information.

Analytic Processes (Analysis)

This is the third year we have asked survey respondents to share information about the processes and techniques used to conduct analysis. Based on the feedback from the previous years, we introduced "Knowledge bases like MITRE ATT&CK" in the survey, and unsurprisingly, the newest addition was the most widely used method in CTI analysis.

Over the past three years, there have been some interesting trends about analysis methods in CTI. "Intuitive or experience-based judgment" has been a top answer every year, with half of respondents reporting using this method frequently. Threat modeling and systems analysis methods have both increased in frequency of use since we first introduced this topic in the survey in 2022.

Structured analytic techniques (SATs) are designed to reduce bias, make an analytic process repeatable, and allow analysts to "show their work" when sharing their analysis with others. The downside of SATs is that they can be more time-consuming than other analysis methods and can easily be implemented incorrectly, undermining their utility. One way to overcome these challenges is to identify a few different SATs that are efficient and well-understood by the team and pair these with intuitive or experience-based judgments to account for biases and logical fallacies in a way that does not slow down the analytic process too much.

One of the largest changes from last year was a sharp decrease in the number of respondents who use structured analytic techniques. In 2023, 31% reported that they used this method frequently. This year, only 22% of respondents report that they frequently use structured analytic techniques, and over 30% do not. (See Figure 11.)

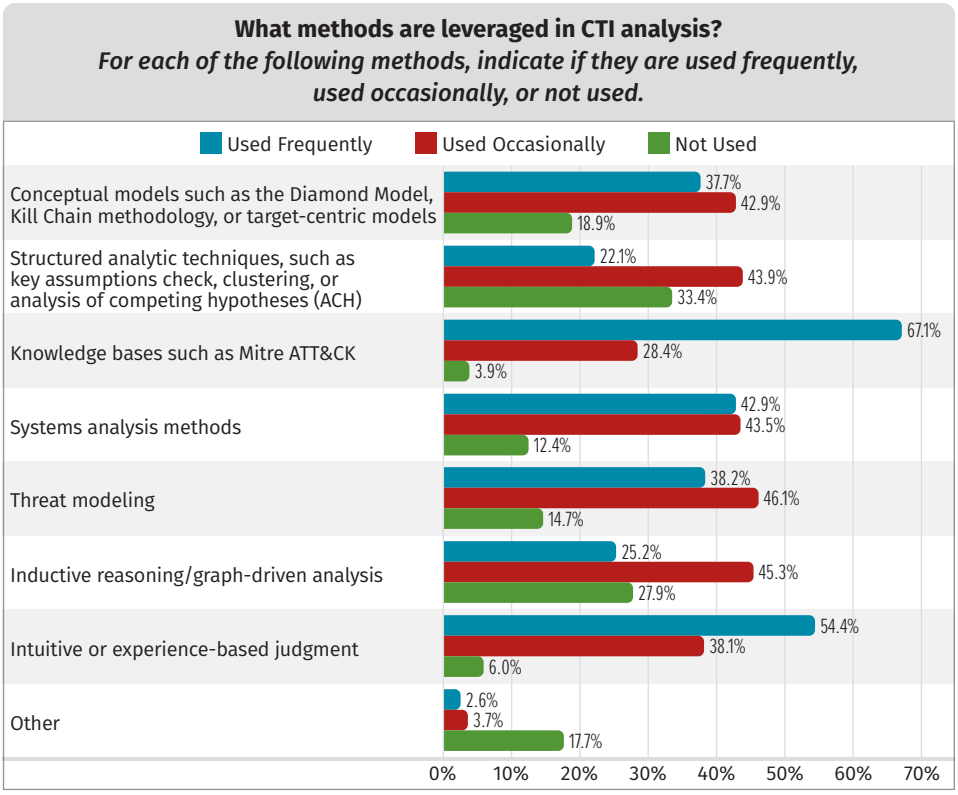


Figure 11. CTI Methodology

Dissemination and Feedback

Once information has been analyzed, it needs to be shared with the relevant stakeholders to be useful. Dissemination will take different forms based on who it is being provided to; regardless of the method, it is also critical to gather feedback on the intelligence's relevance and any next steps that are needed.

Although traditionally emails, spreadsheets, and presentations were the most preferred options to disseminate CTI, reporting emerged as the most prevalent method this year. Survey results show a rise in the use of reporting for dissemination, growing from 62% in 2022 to 74% in 2024. Similarly, the utilization of briefings to disseminate intelligence increased from 51% in 2019 to 64% this year. The uptick in reporting and briefings may reflect the evolving maturity of CTI, because both reports and briefings indicate a receptive audience of decision-makers. This underscores the importance of communication as a core skill for CTI analysts. (See Figure 12.)

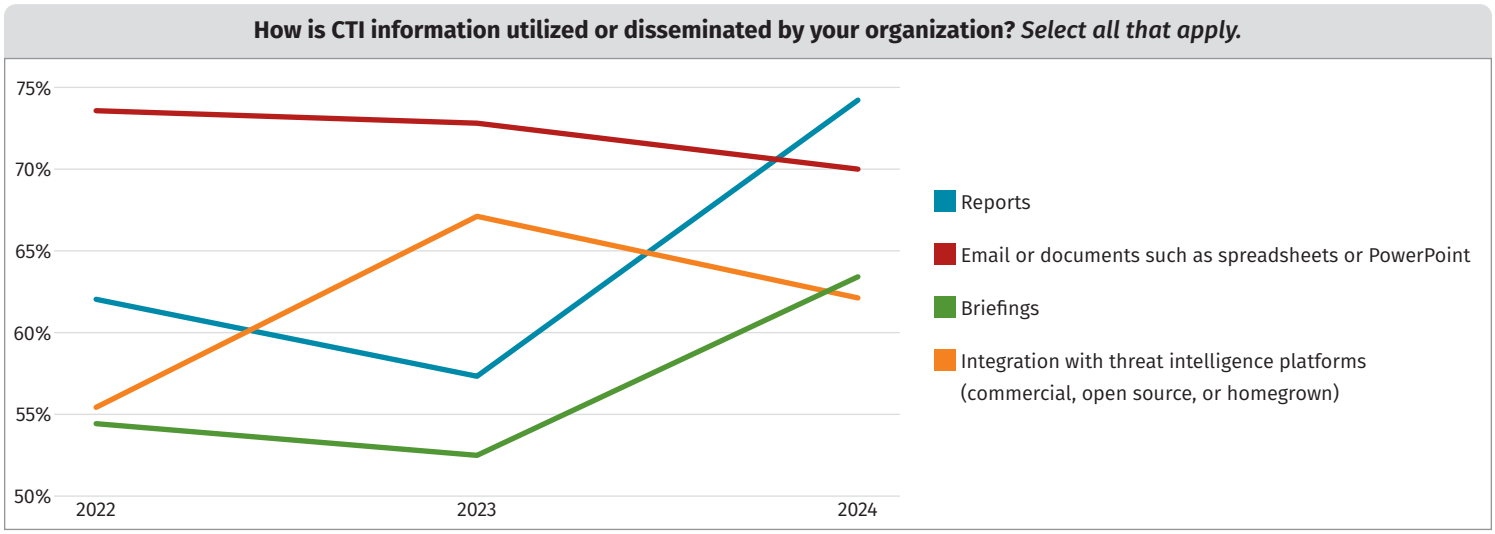


Figure 12. How CTI Is Utilized

Tools and Technologies

CTI analysts leverage various tools and technologies to enhance their intelligence processes. The integration of technology is crucial for achieving efficient and scalable CTI operations. This year, in addition to examining CTI management tools and CTI integration within an organization's security framework, we explored how CTI analysts are utilizing AI. Our interest lies in understanding this breakthrough technology's impact on CTI, including its adoption and practical applications, by introducing several questions related to the utilization of AI by CTI teams.

Almost one fourth of the respondents reported that they already leverage AI, while another 38% do not, but they plan to. The majority of these respondents reported that AI is most effective in CTI analysis, helping analysts prioritize and process vast amounts of information through scoring and summarization. Respondents also reported that AI provides value in the collection and exploitation phases of the CTI process. AI is used in the collection phase by collecting high-quality threat intelligence that feeds AI/ML model training. AI enhances the exploitation phase of the CTI process by structuring, normalizing, and enriching raw data through AI/ML-based information extraction and detection. (See Figure 13.)

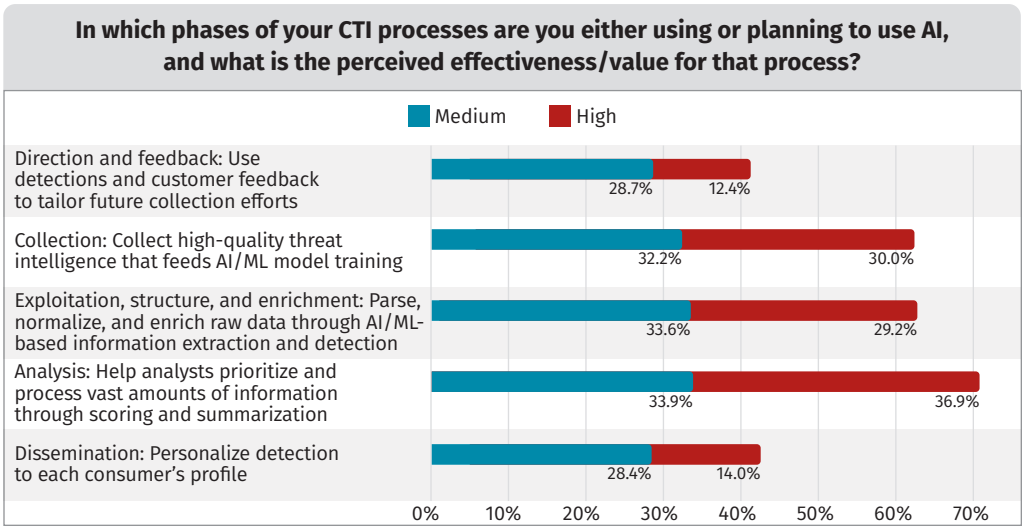


Figure 13. AI Usage in CTI Processes

When we asked the survey respondents about examples of AI utilization by the CTI team, the following categories of responses were provided:

- **Data collection enhancements—**AI is leveraged to better understand and de-duplicate similar CTI sources and discern the unique value of each feed. Moreover, some CTI teams use AI to prioritize the most relevant OSINT sources based on predefined intelligence requirements.
- **Parsing, normalization, and enrichment—**CTI teams reportedly use AI to parse, normalize, structure, and enrich source data. Some teams report that their vendors' built-in tools provide this capability.
- **Information extraction from unstructured data—**CTI teams report utilizing AI to extract entities from unstructured data and model them into structured formats like Malware Information Sharing Platform (MISP), Structured Threat Information Expression (STIX),™ Diamond Model, and MITRE ATT&CK TTPs. These examples underscore AI's capacity to parse, understand, and categorize data into standardized, actionable formats.

- **Analysis and report writing—**AI aids in the analysis phase by assisting with report writing, summarizing natural language sources, and creating summaries. A classic example is the utilization of AI to "help summarize short OSINT blurbs of analyst-curated news items affecting the company for weekly summary."
- **Automation and workflow enhancements—**AI applications streamline workflow, automate repetitive tasks, and focus on workflows and correlation. Examples include the automation of SIGMA rule generation, static and dynamic malware analysis, and indicator of compromise (IOC) analysis. AI is utilized within vendor tools, especially XDR and SOAR platforms, to improve operational efficiencies and threat response times.
- **Threat analysis and prioritization—**CTI teams utilize AI for threat detection, pivoting, and prioritization. Examples of how AI can augment day-to-day CTI analysis tasks include the "utilization of LLMs for threat actor and campaign analysis," "enrichment and pivoting," "create realistic phishing tests," and "daily advanced analytics for vulnerability remediation prioritization and securing the supply chain."

CTI Management Tools

This year, respondents indicated that SIEM or security analytics platforms are the leading tools for aggregating and analyzing CTI, with 62% utilization, marking the first time they've topped the list. Previously, spreadsheets were the most used tool, but they dropped to fifth place with 35% usage from 71% last year. We reserve judgment on the significant decrease in spreadsheet usage, considering it might be a transient trend that may not persist over time.

Threat intelligence platforms (TIPs) are often considered central to a CTI analyst's work. This year, 42% of respondents use an open-source TIP, and 54% use a commercial TIP. (See Figure 14.) One of the biggest factors when deciding between open-source or commercial is cost. Currently, commercial platforms are available at many different price points; however, for smaller teams, especially teams with only one or two analysts, some of the open-source options may work well and be relatively easy to stand up and maintain. For larger teams, open-source platforms will often need more customization and support, especially because the ways that the platforms are used often grow with larger teams.

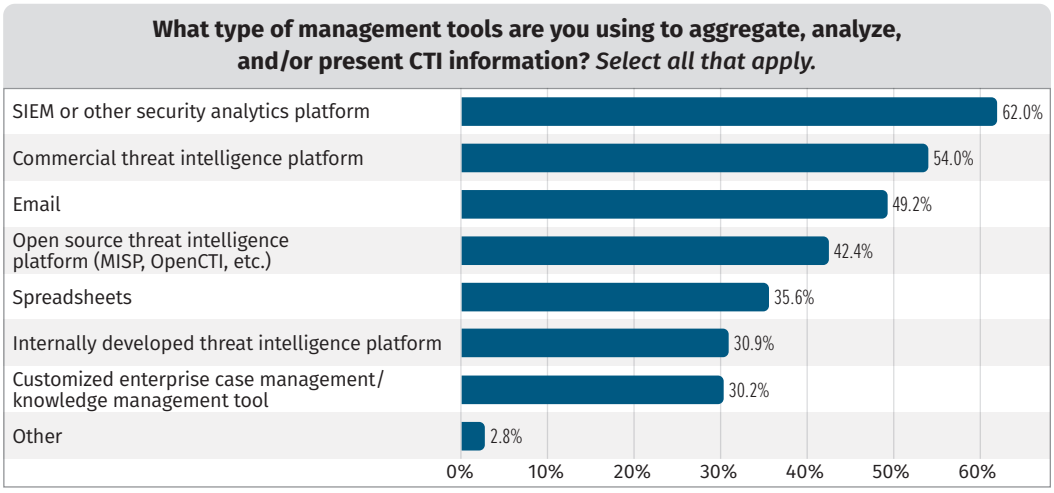


Figure 14. Management Tools

A third of the survey participants reported using case management tools to aggregate and analyze CTI. Such tools are crucial in enhancing team coordination, fostering collaboration, managing knowledge effectively, and tracking CTI metrics. This is why we introduced this option in this year's survey, because we would like to identify how teams utilize such tools for CTI management. (See Figure 15.)

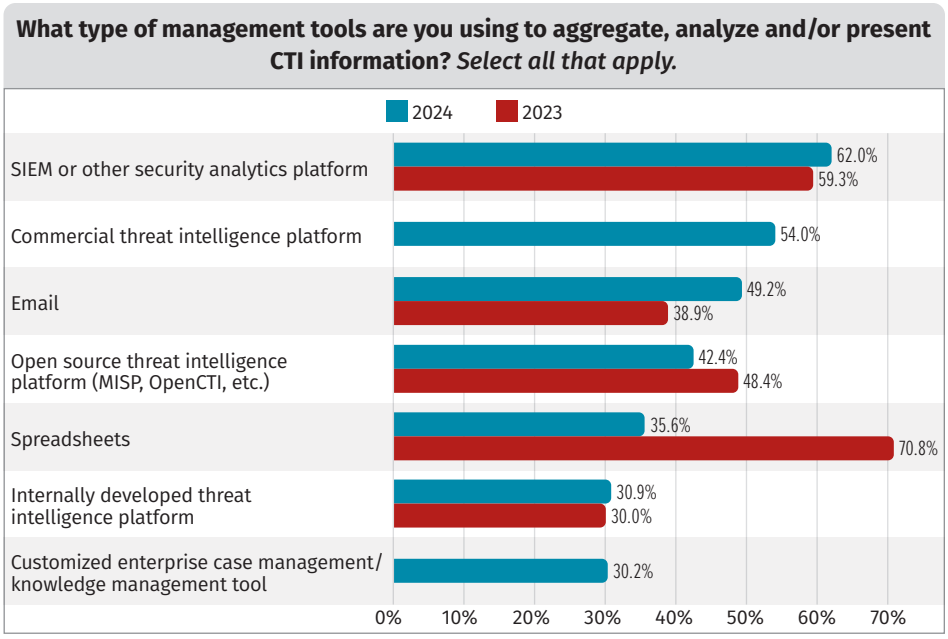


Figure 15. Change in Management Tool Use over Time

This year, most respondents reported integrating CTI information into their detection and response systems through built-in integrations of their TIPs, whether commercial or open source, with 58% indicating this method. This capability is seen as an obvious advantage and a critical requirement in selecting a threat intelligence platform, showcasing an area where TIPs offer significant value and demonstrate maturity. Integration via vendor APIs follows with 38%, and using custom APIs for CTI integration is reported by 35% of the respondents.

Impact of CTI

Gathering feedback about the impact of CTI efforts is one of the best ways to ensure that your CTI program is focused on the right priorities and is providing the best possible support to an organization's overall security.

This year, 83% of the respondents report that CTI has helped improve security prevention, detection, and response whereas only 36% indicate that they measure the effectiveness of their CTI programs. This shows that although many can perceive the value of leveraging CTI, it can be challenging to implement ways to measure and report its effectiveness.

The top area that respondents felt had been improved through CTI is visibility into threats and attack methods (52%), followed by improved ability to detect unknown threats (51%). (See Figure 16.)

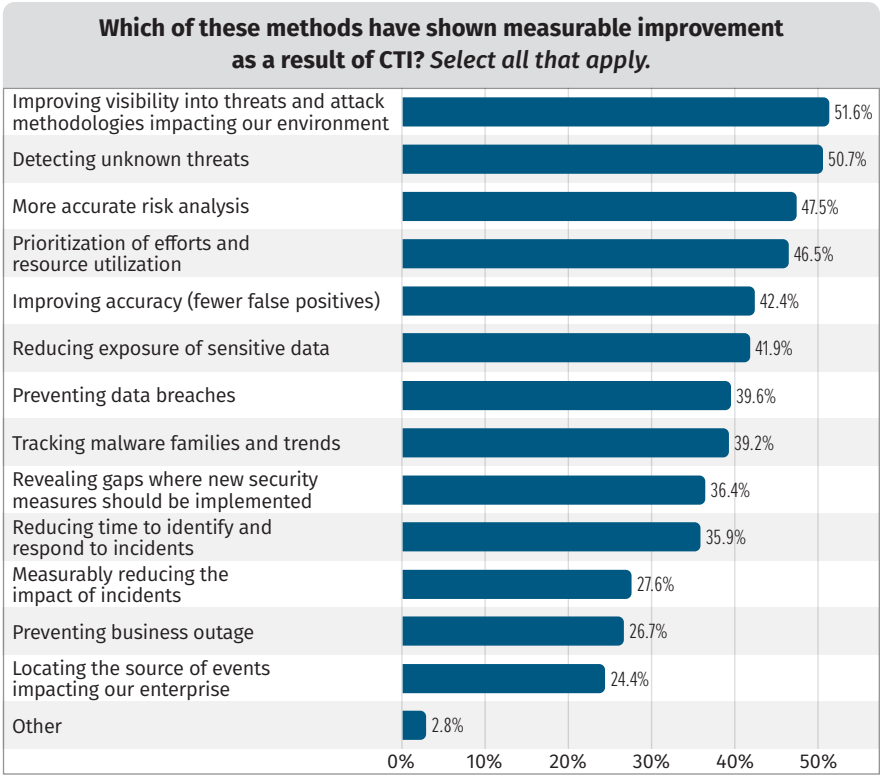


Figure 16. Methods Showing Improvement Due to CTI

One interesting response to how CTI has improved overall security was through increased stakeholder engagement. Stakeholder engagement is critical to a successful CTI program, and it can be one of the tangible ways to measure the effectiveness of a CTI program. It can also be more straightforward to measure, for example, by tracking the number of stakeholders contributing to CTI requirements.

In addition, respondents shared additional details on the most effective ways to measure impact. The diversity of their responses shows that both the methods for tracking effectiveness and how it is measured will depend on the requirements and goals of each individual team. Many called out metrics tied to the support provided to incident response teams and processes, whereas some highlighted detection-related metrics, such as mean time to detection and the ability to detect malicious actions across many phases of the Cyber Kill Chain.[8]

Challenges and Limitations

One of the top challenges from respondents this year is lack of funding, with 52% of respondents citing it as a concern. One way to adapt when funding is an issue is to "live off the land." We know that attackers have been known to "LOTL" by abusing native tools and systems to compromise a network. The issue is so prevalent that a multi-agency, multi-national report[9] was released to help defenders combat these types of attacks—but that is not what we are talking about here. CTI teams can leverage their existing systems and tooling, or those of their partner teams, to increase their capabilities with limited additional funding needed. Throughout the survey, we have seen multiple ways that respondents are making the best use of the tools that they already have, including fully leveraging capabilities of threat intelligence platforms; using enterprise platforms such as JIRA/Confluence, Microsoft 365 suite, and Google Productivity Suite; or making use of emerging capabilities such as AI being built into existing platforms to optimize their processes.

Another top challenge cited by respondents is the lack of interoperability and automation with CTI tools. Although spreadsheets falling from the most-used CTI tool was a sign of things moving in the right direction as far as automation is concerned, it can still be challenging to align tools and processes in a way that allows analysts to do their work efficiently. Thirty-one percent reported a lack of technical skills on the CTI team, which can make it more difficult to do automation work themselves.

[8] "The Cyber Kill Chain," www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[9] "Joint Guidance: Identifying and Mitigating Living Off the Land Techniques," https://media.defense.gov/2024/Feb/07/2003389936/-1/-1/0/JOINT-GUIDANCE-IDENTIFYING-AND-MITIGATING-LOTL.PDF

Conclusion

This year, respondents anticipate that the most valuable type of CTI in the next 12 months is intelligence on adversaries' use of AI,[10] with 57% prioritizing this area. Following that are detailed insights into adversary groups at 42%, in-depth information about malware families and trends at 40%, and analysis of threat behaviors, including TTPs, employed by adversaries, at 39%. (See Figure 17.)

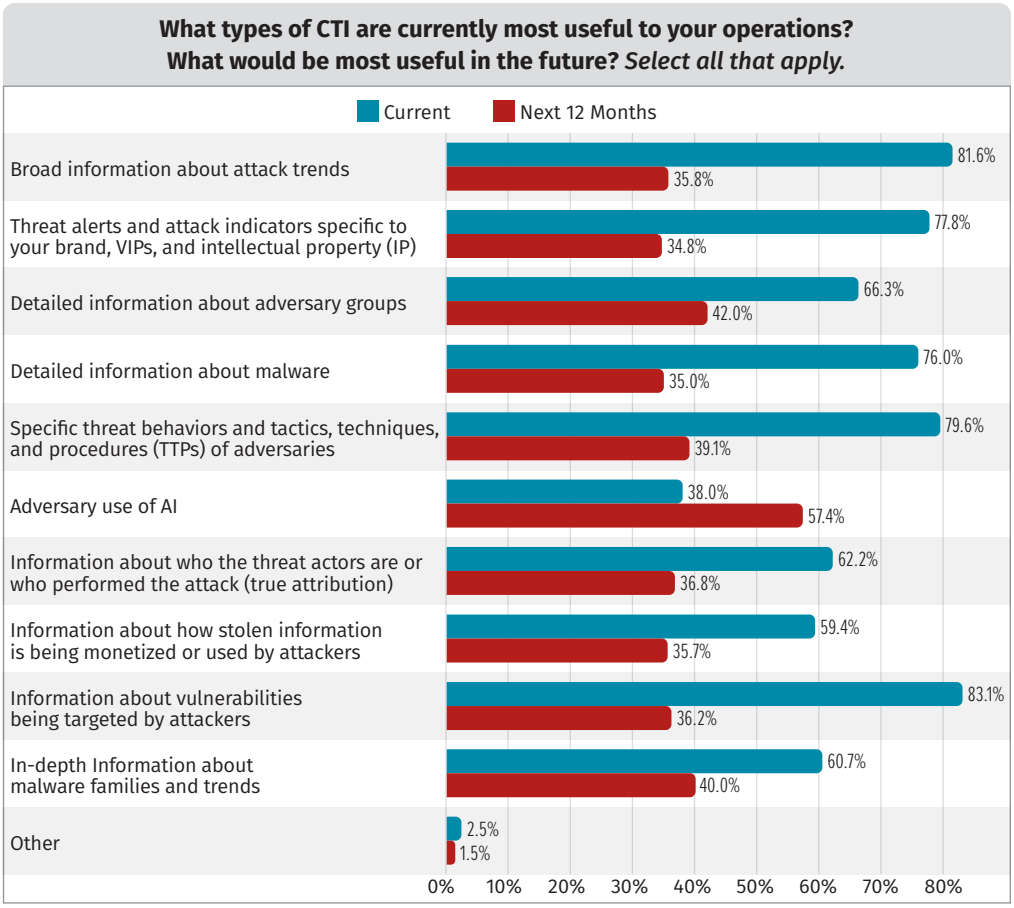


Figure 17. Most Useful CTI in the Next 12 Months

In addition to tracking the adversarial use of AI, we anticipate that CTI teams' own use of generative AI and other emerging technologies will reduce time spent on specific tasks. Many respondents indicated that their current AI capabilities primarily stem from integrated AI features in their vendors' tools, and some emphasized a desire for "more vendors that leverage cutting-edge AI technology." It is strongly recommended that organizations undertake such evaluations and establish guidelines for their staff on the appropriate use of these technologies, ensuring alignment with the organization's risk tolerance.

Throughout the survey, it is clear that although certain use cases remain steadfast over time, new and less conventional scenarios are emerging. Some not-so-common CTI use cases include leveraging CTI as a business enabler, during mergers and acquisitions, for strategic planning, and to inform risk and compliance strategies. Addressing supply chain threats and enhancing third-party risk management are also cited. Respondents underscore the importance of looking at the "bigger picture" through executive summaries of the threat landscape, incorporating geopolitical analysis, and utilizing CTI for data-driven decision making.

[10] "Threat-Actors-use-of-Artifical-Intelligence," https://github.com/cybershujin/Threat-Actors-use-of-Artifical-Intelligence

Sponsor

SANS would like to thank this survey's sponsor:

ANOMALI

SANS | Research Program

Product Briefing

CTI with Anomali: Insights from the 2024 SANS Institute Survey

May 2024

As the threat landscape evolves, organizations are prioritizing threat hunting to stay ahead of malicious actors. The SANS CTI Survey finds threat intelligence teams are putting threat hunting at the top of their lists of activities, and that means CTI teams need solid threat hunting technology to empower their work.

Anomali

Anomali is a cloud-native, AI-driven security operations platform that combines unparalleled threat intelligence with internal monitoring to quickly provide security teams with actionable intelligence. It overcomes the common challenges of SecOps systems with powerful and fast queries and customizable lookback timeframes, correlating IoCs across multiple threat feeds (see Figure 1, on the next page).

Respondents in the SANS CTI Survey said one of their top challenges was funding. There has long been a shortage of experienced threat hunters, and inadequate budgets make it even more difficult to hire and retain top talent. Anomali uses automation to lighten the load of existing team members. By eliminating parsing, indexing, and archival, organizations can get the critical intelligence they need without adding additional staff.

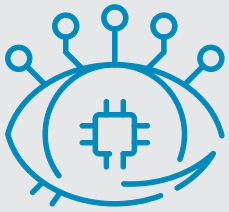
The principles behind Anomali are business-focused, and the system seeks to inform and act while freeing up business teams to focus on their core competencies. Anomali's designers built in the idea that the product can be customized to meet business needs and integrate with business systems.

Users interact with Anomali through the Copilot analyst interface, which uses natural-language processing to deliver threat insights and augment an analyst's own knowledge. This draws on both ThreatStream—a time-tested and constantly updated threat intelligence processing capability—and Security Analytics, which operates on data generated by the business's own systems and networks.

Analysts can pose questions to Copilot in more than 100 languages and receive an immediate answer, accompanied by links to sources to check the response for accuracy (see Figure 2, on the next page).

Key Findings
from the 2024 SANS CTI Survey

AI is most effective in CTI analysis, helping analysts prioritize and process vast amounts of information through scoring and summarization.



83% of respondents value insights on vulnerabilities exploited in the wild.

This year, we saw a general increase in using threat feeds as a data source.

Anomali has best-in-class processing speed, scanning petabytes of data in seconds. That speed is especially important when a business is under attack. It is perilous to waste precious moments wading through log entries or combing through threat intelligence feeds while allowing a breach to progress. A sophisticated, easy-to-use threat intelligence platform with access to best-in-class data and the ability to provide relevant information in real time can make all the difference. In some cases, Anomali can identify and neutralize a potential threat even before an attack is launched.

Figure 1. Anomali UI

Anomali's browser extension lets analysts detect attacks and flag relevant log issues by specifying a particular threat, threat actor, or vulnerability and matching it against the business's own environment. They can then start investigations and generate reports right from the Anomali SecOps platform, identifying the attack methods and techniques to which the organization may be particularly vulnerable. They can even send the information about a threat directly to the firewalls or other defense systems for automatic blocking.

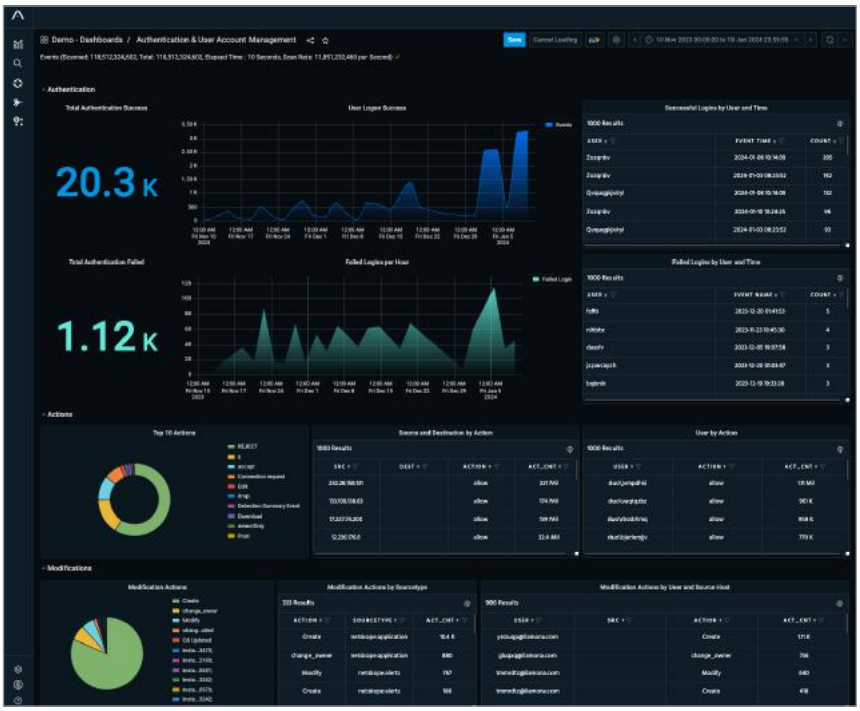


Figure 2. Anomali Dashboard

Anomali has a global reach and a long track record of providing scalable threat intelligence to governments and leading corporations. Its cloud-first architecture allows the company to competitively price its market-leading offering.

As SANS CTI Survey respondents noted, not only are many analysts using AI, they are defending against malicious actors who leverage the same technologies. The speed and power that Anomali brings to the table can raise the odds in your favor.

If you're looking for a threat intelligence tool designed for business needs and real-world SOC challenges, consider Anomali. Its easy-to-use, integrated platform offers the power and speed you need to stay ahead of bad actors, saves your team time, and speeds incident response.

To learn more about Anomali's CTI capabilities, visit **www.anomali.com**