SANS | Research Program

2025 SURVEY

SANS 2025 CTI Survey

Navigating Uncertainty in Today's Threat Landscape

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

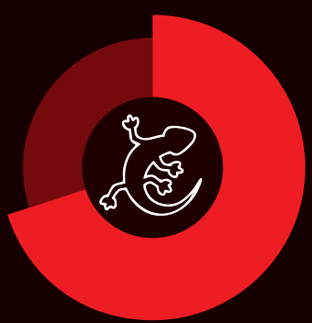
May 2025

INTEL471

SANS 2025 CTI SURVEY

Key Findings

Adaptation is key.



70.2% say an "increasingly complex digital landscape" drives the evolution of their CTI processes.

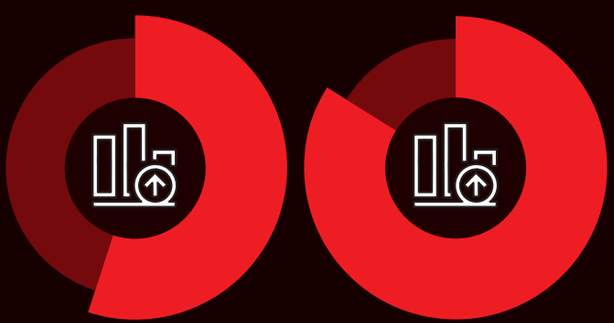
AI is (still) on the rise.

More than 1/3 of organizations now use AI in CTI processes.

Threat hunting and MITRE ATT&CK lead the way.

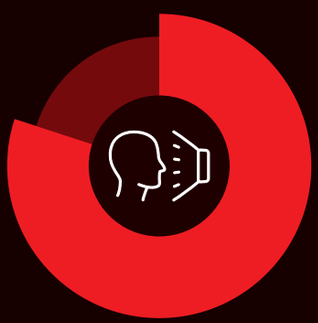
77% use CTI for threat hunting, and **86%** use MITRE ATT&CK.

The emphasis is on showing value.



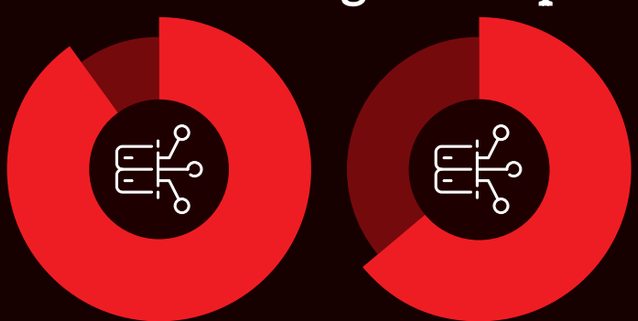
55% measure effectiveness, and **84%** gather direct feedback via meetings.

Communication in CTI is critical.



80% use reports to communicate intelligence.

CTI teams heavily favor external intelligence inputs.



While respondents might collect both, **90%** collect external data vs. **64%** who use internal sources.

Survey Authors

VIEW PROFILE

Rebekah Brown
Certified Instructor
Candidate

COURSES TAUGHT

FOR578: Cyber Threat Intelligence

Rebekah has over two decades of experience in threat intelligence. Her career started out in traditional military intelligence work, focused on cryptologic linguistics. She was then selected to cross-train as a network warfare analyst, which provided the opportunity to fuse her understanding of language and culture with network defense. Rebekah has since provided threat intelligence for numerous security programs ranging from national security operations to state and local governments and Fortune 500 companies, including Nike and Apple. She is currently a Senior Researcher at the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, where her work focuses on the intersection of digital security and human rights. She is a course instructor and student mentor at SANS, where she teaches FOR578: Cyber Threat Intelligence, a course she co-authored. She is also co-author of the book *Intelligence-Driven Incident Response*.

VIEW PROFILE

Andreas Sfakianakis
Certified Instructor

COURSES TAUGHT

FOR578: Cyber Threat Intelligence

Andreas is a seasoned cyber threat intelligence professional with over 15 years in cybersecurity. He specializes in cyber threat analysis and building threat management programs. Andreas believes in actively engaging the community, especially the new generation of CTI analysts; maturing threat management programs within organizations; as well as embedding CTI in policymaking. Andreas is the global threat operations lead of SAP's CTI team and the founder of SAND, a company that provides CTI consultancy services. He takes pride in helping students plan and achieve their goals within the CTI sphere. As Andreas put it, "Helping budding analysts motivates me to further my knowledge transfer activities and develop myself as an instructor and mentor."

Executive Summary

The 2025 SANS CTI Survey highlights a cyber threat intelligence field that is steadily maturing, with more organizations establishing dedicated CTI teams, increasingly integrating AI and automation into their workflows, and moving toward standardized adoptions of frameworks such as MITRE ATT&CK.™ Threat hunting remains the leading use case, and formal reporting continues to be the primary method of delivering intelligence to stakeholders. Limited resources, increasingly complex landscapes—in terms of both adversary sophistication and a diversified and fragmented digital footprint—and changing geopolitical and regulatory landscapes continue to present challenges to CTI professionals. Following are some key findings from this year's survey.

This year, we received 489 responses from CTI professionals across various industries. For a demographic snapshot of this year's respondents, see Figure 1.

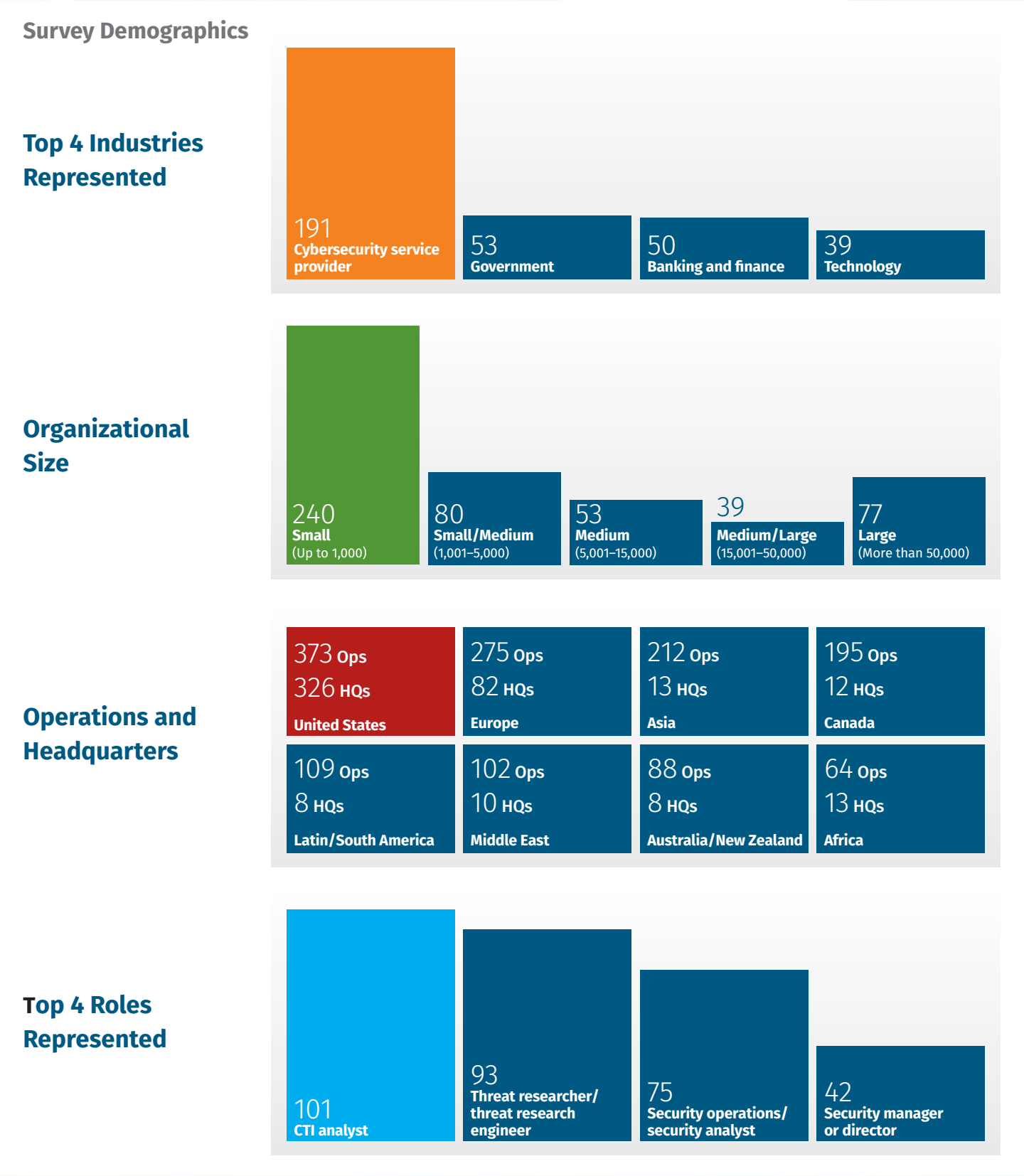


Figure 1. Demographics of Survey Respondents

The Role of a CTI Team

A full 93% of organizations now maintain some form of in-house CTI capability, ranging from one person to dedicated teams and hybrid models. Notably, more organizations than ever report having dedicated CTI teams—52% of respondents—representing an increase of 10 percentage points compared to 2018 (see Figure 2).

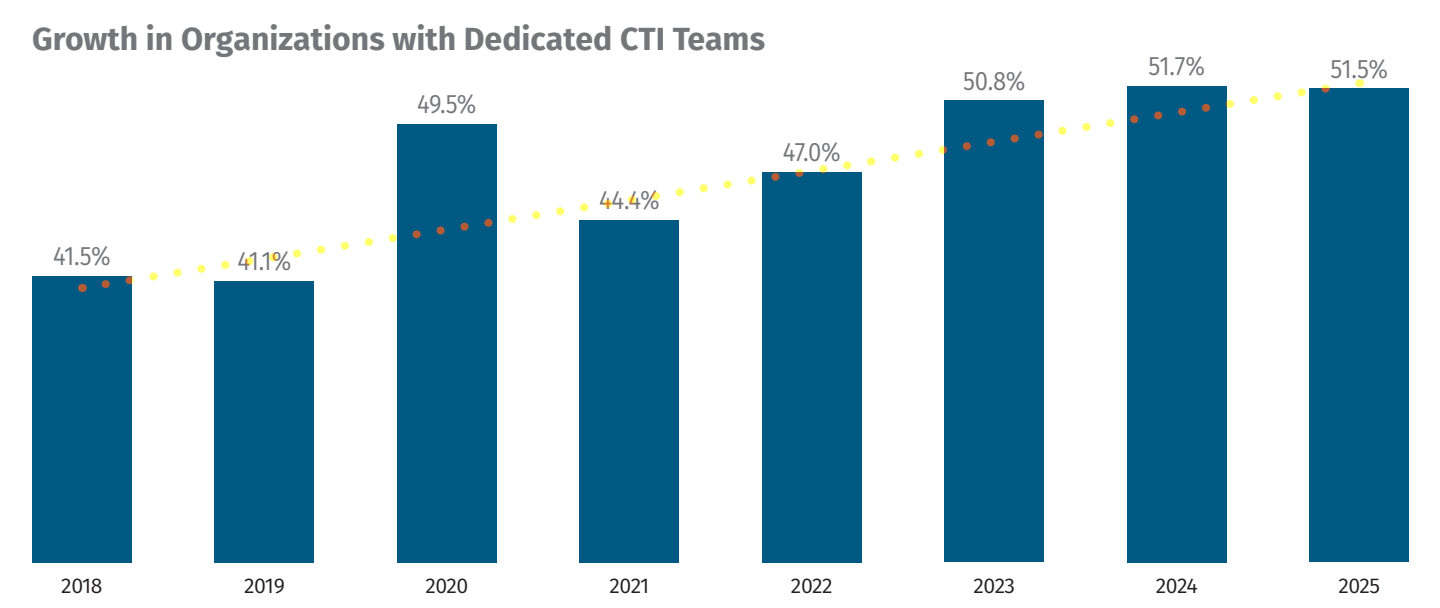


Figure 2. Growth of CTI Teams Over Time

Sixty-two percent of organizations have between 0.5 and 4 full-time equivalents (FTEs) dedicated to CTI, with 2 to 4 FTEs being the most common (see Figure 3). This reflects the value organizations see from CTI and the steady maturation of the CTI discipline as it evolves from a niche function to a core part of security operations.

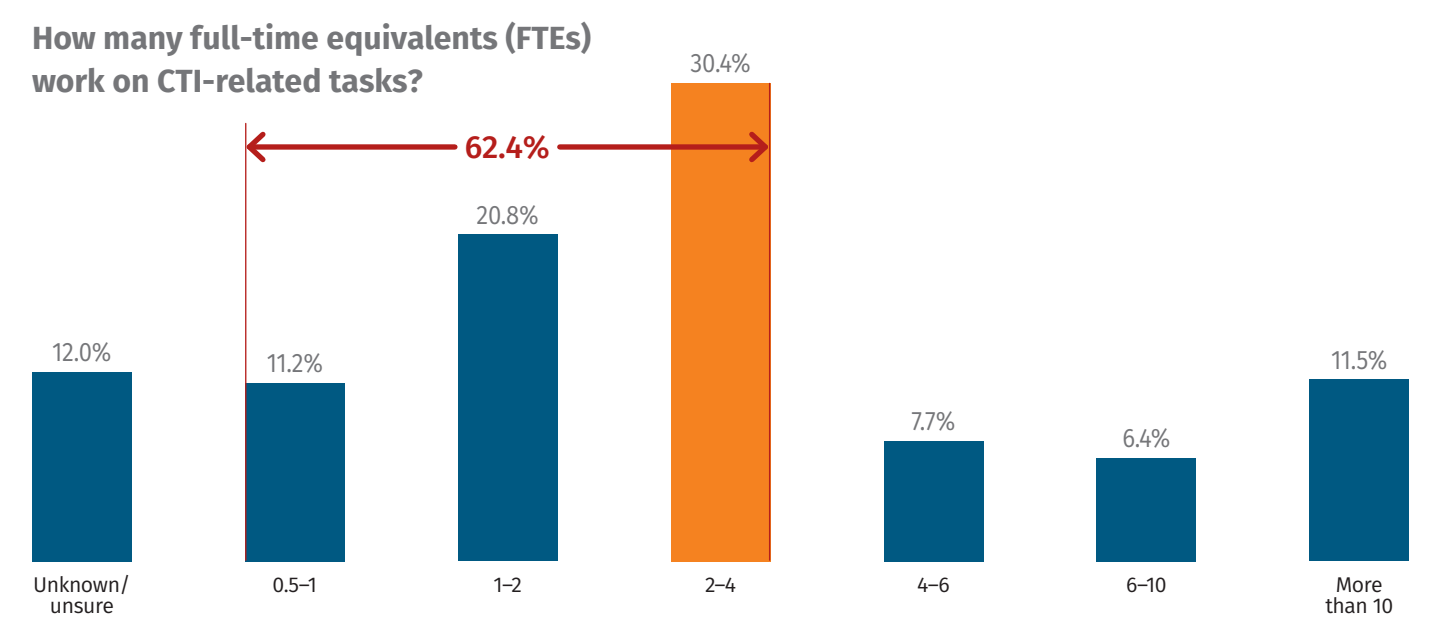


Figure 3. FTEs Working on CTI Tasks

Introduced last year, the question on fundamental CTI processes—intelligence requirements, collection planning, and threat modeling—shows a slight decline in formal adoption, with a rise in informal or ad hoc approaches. As this is only the second year we have asked this question, small shifts are expected. However, the overall pattern remains consistent: Intelligence requirements are the most formalized (44%), followed by collection planning (41%) and threat modeling (37%) (see Figure 4).

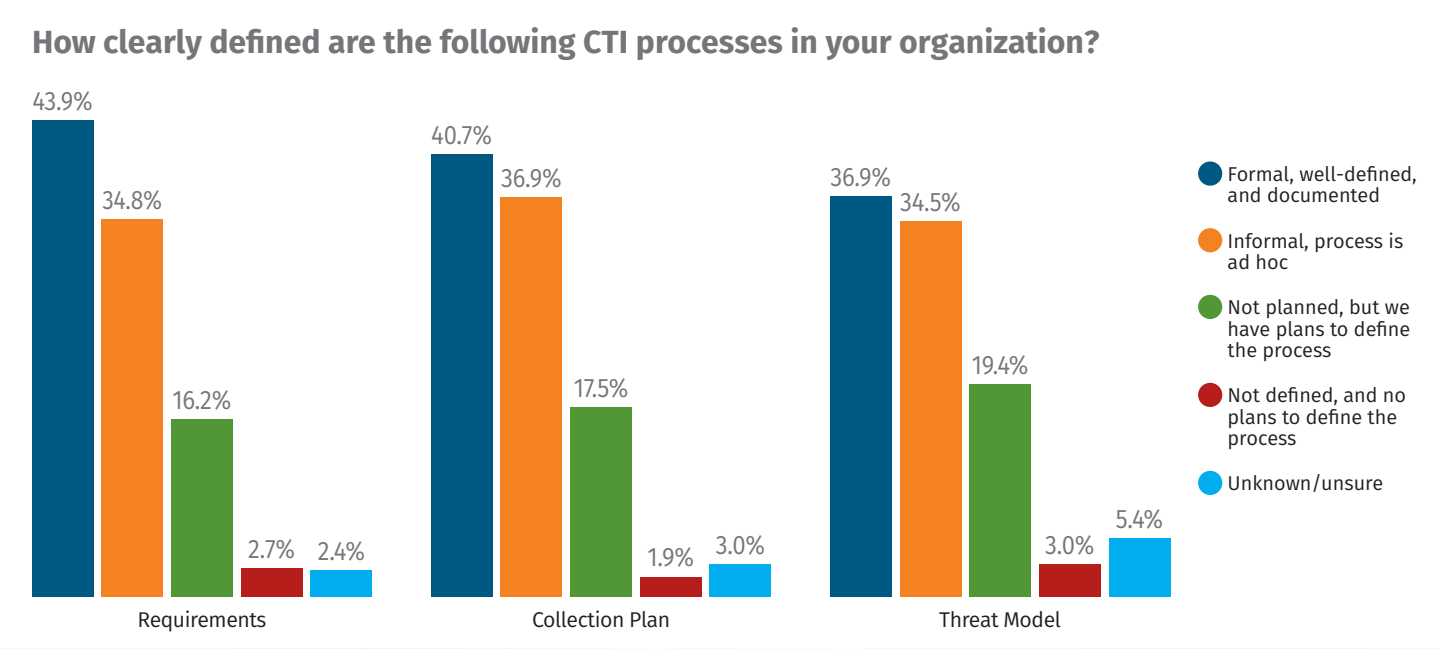


Figure 4. CTI Processes

Compared with last year, the 2025 survey shows a significant increase in contributions from executives (from 33% to 52%) and business units (from 23% to 39%) to the intelligence requirements process.

This trend suggests that CTI increasingly supports strategic decision-makers, reflecting its growing role beyond operational use cases. (See Figure 5.)

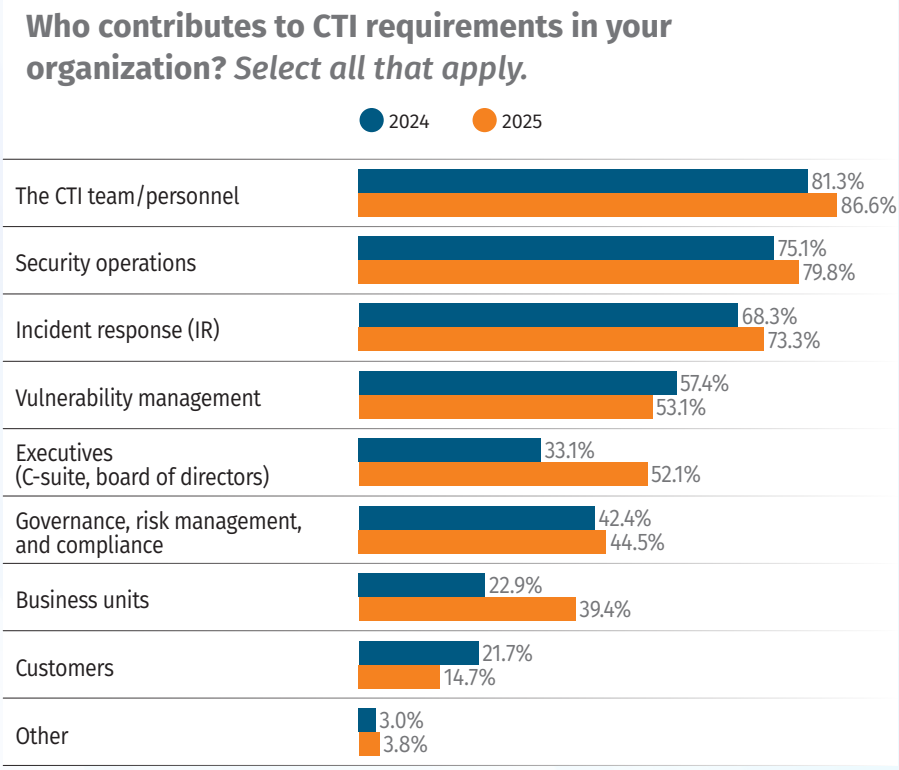


Figure 5. CTI Requirement Contributions

Survey respondents provided dozens of real-life examples of CTI in action, reflecting how diverse and valuable CTI has become across organizations. While many examples focused on phishing, ransomware, and supply chain attacks, CTI also was used for red teaming, strategic decision support, executive protection, and incident triage.

- **Tactical CTI example—**One organization proactively identified a phishing campaign targeting executives by monitoring adversary infrastructure and tactics. Countermeasures were deployed early, preventing credential theft.
- **Operational CTI example—**A financial institution used automation and AI tools to reduce intelligence summary delivery time by 60%. The team tailored intelligence newsletters to different stakeholders, improving relevance and engagement.
- **Strategic CTI example—**During an acquisition, a CTI team provided intelligence that revealed potential cyber risks in the target company. Their analysis enabled leadership to implement mitigation steps before finalizing the deal.

Changing Processes in CTI

This year, we asked respondents whether they had needed to change their CTI processes in response to changes in the threat landscape, and the vast majority responded that they had (see Figure 6).

Have your standard CTI processes evolved in response to the increasingly complex digital landscape (changes in adversaries, technologies, and internal business processes)?

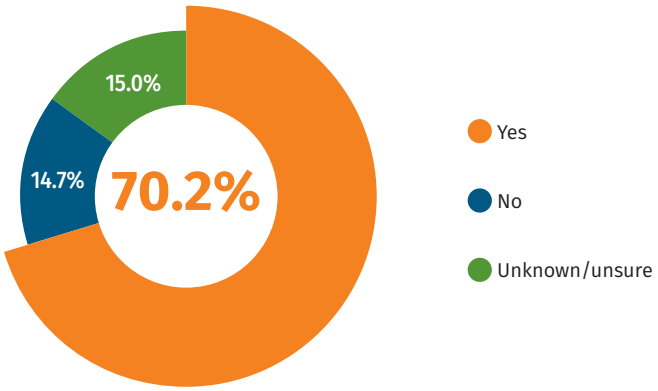


Figure 6. Changing CTI Processes

These changes reflect both changes in the threat landscape, which have forced CTI teams to cover more ground (cloud threats, third-party risks, AI, etc.), and changes to tools that support formalization of processes or more efficient workflows.

When asked directly about process changes, the most frequently cited example was a shift toward automation, moving from manual collection and analysis to automated threat data ingestion, alert triage, and incident response. Much of this automation involves SOAR tooling as well as threat intelligence platforms (TIPs), which account for more than 70% of CTI integration into detection and response systems.

Respondents also called out a shift from a more reactive use of indicators of compromise (IoCs) to proactive threat monitoring, threat actor tracking, and greater adoption of MITRE ATT&CK for mapping TTPs and structuring hunts. Finally, we also noticed a shift in the sourcing of information used by CTI analysts. As Figure 7 shows, external information remains an important part of many CTI teams' collection plans, expanding to include geopolitical events, social media, and Telegram channels. There is also an interest in utilizing internal sources, supported by process automation mentioned previously. Internal data often requires breaking silos, custom integrations, and cross-team collaboration. This highlights an opportunity: Leveraging internal, context-rich insights can significantly boost the relevance and value of CTI that is currently utilized at a lower level (see Figure 8).

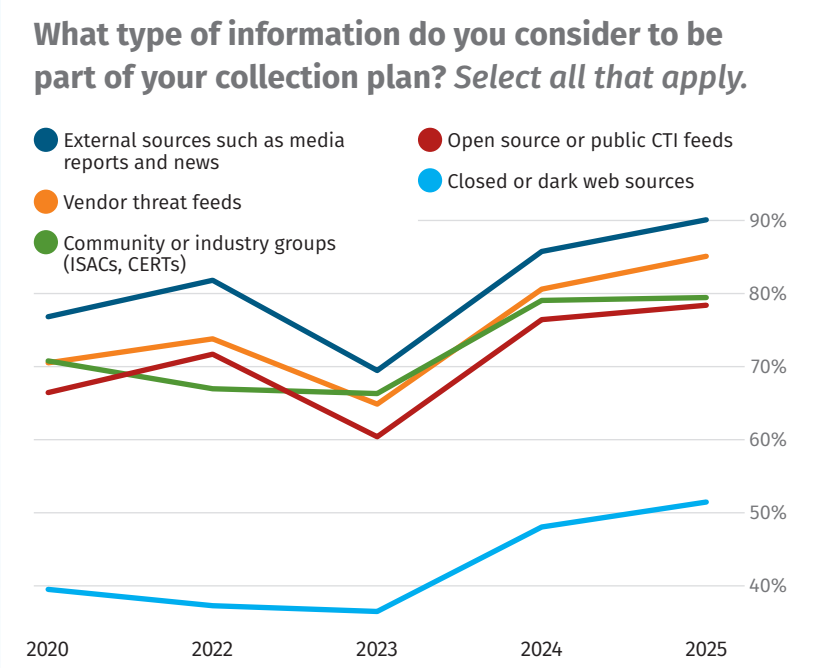


Figure 7. External CTI Sources Over Time

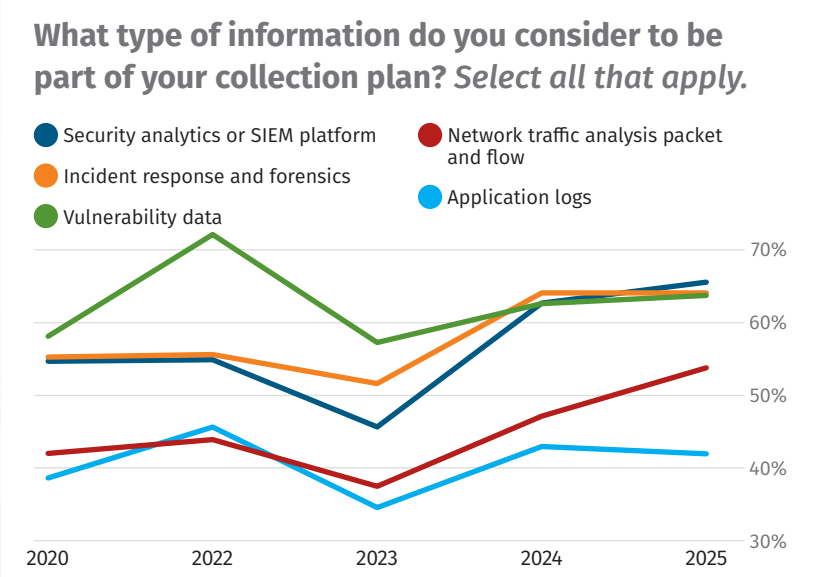


Figure 8. Internal CTI Sources Over Time

John Doyle
Certified Instructor

COURSES TAUGHT

FOR578: Cyber Threat Intelligence

VIEW PROFILE

"The uptick in CTI teams leveraging dark web monitoring services as a job function showcases the expansion of CTI as a service to organizational stakeholders like risk, identity and access management (IAM), and security architecture. This deviation from the primary use cases of CTI to service hunt and incident response functions or provide executive leadership insights speaks not only to the utility of CTI but also to the need for researchers and analysts to have wider knowledge and skills."

Finally, as Figure 9 shows, in 2025 respondents reported a stronger impact from both geopolitical shifts and regulatory changes compared to 2024. This reflects growing pressure on CTI teams to provide timely geopolitical context and meet evolving compliance and audit requirements (such as ISO 27k,[1] NIS2 Directive,[2] DORA,[3] NIST CSF 2.0,[4] and CIRCIA[5]).

As global tensions and cybersecurity regulations increase, CTI processes must adapt accordingly.

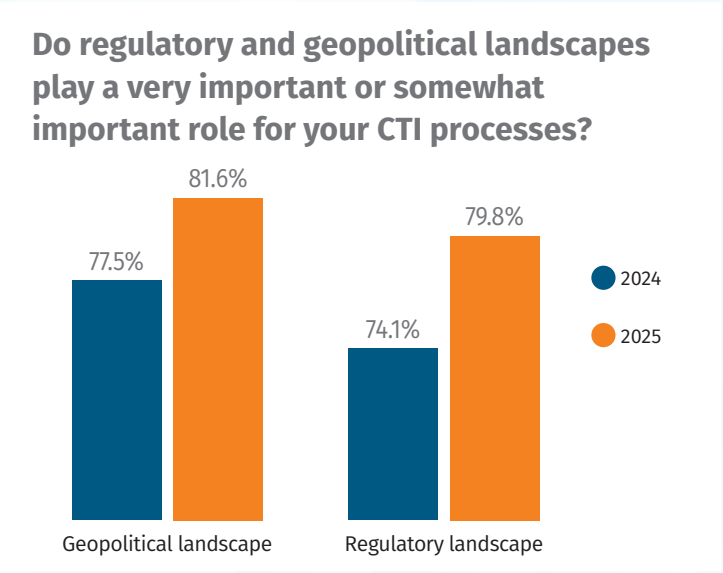


Figure 9. Geopolitical and Regulatory Impact

The Rise of ATT&CK

The MITRE ATT&CK[6] framework has become the de facto language within the CTI community for organizing and communicating adversary behavior. Survey results confirm that 86% of CTI teams use ATT&CK across various use cases.

As seen in Figure 10, threat hunting was the most common use case for MITRE ATT&CK, cited by 84% of respondents. In the 2024 survey, threat hunting emerged as the No. 1 CTI use case for the first time. This trend is confirmed and reinforced by the 2025 data: 77% of respondents use CTI for threat hunting, topping all other use cases.

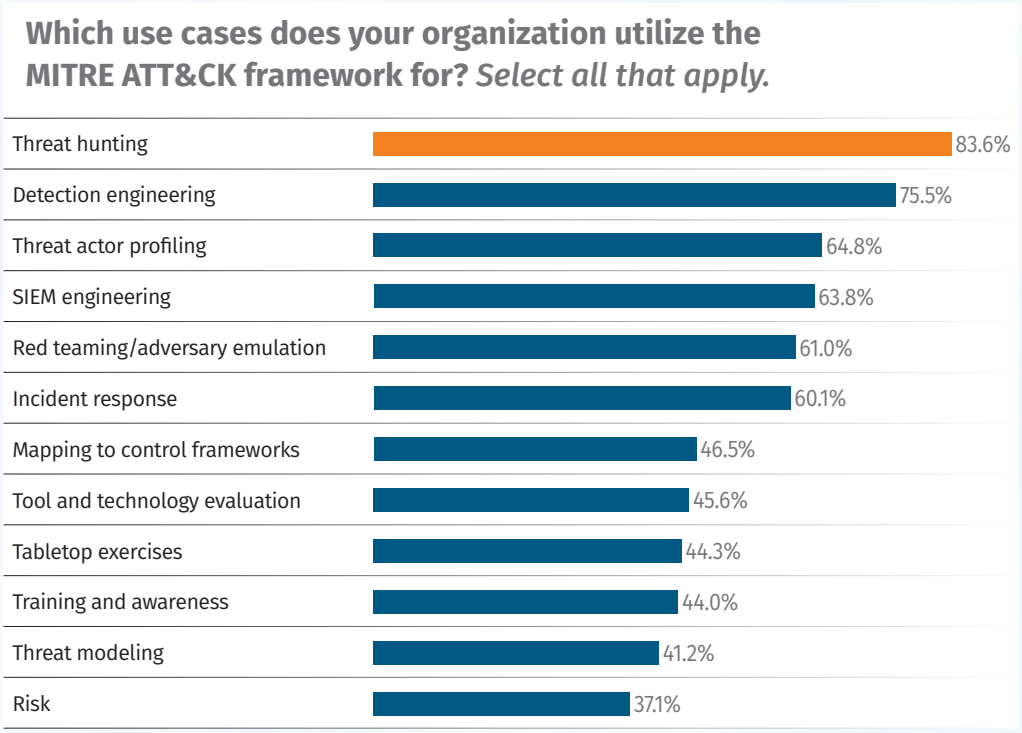


Figure 10. Use Cases for MITRE ATT&CK

[1] "ISO/IEC 27000 Family," www.iso.org/standard/iso-iec-27000-family

[2] "NIS2 Directive: New Rules on Cybersecurity of Network and Information Systems," https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[3] "Digital Operational Resilience Act," www.dora-info.eu

[4] "Cybersecurity Framework," www.nist.gov/cyberframework

[5] "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

[6] "ATT&CK," https://attack.mitre.org

A large portion of respondents use ATT&CK for detection (76%) and SIEM engineering (64%) use cases. CTI provides intelligence on adversary techniques, and by mapping those to ATT&CK, detection engineers can identify detection gaps and operationalize detection signatures across the organization's security stack. Typically, the central location where these detection signatures are deployed is the SIEM platform. These platforms are configured to map logs and detection alerts to ATT&CK, enabling improved detection and alert prioritization, streamlined triage and response, and better assessment of detection coverage.

Sixty-five percent of the respondents use MITRE ATT&CK for threat profiling, which includes the identification of the adversaries that are relevant to their organization, collecting their behaviors, and mapping them to ATT&CK for further analysis and tracking. This threat profiling process can be utilized later as an input to other use cases like detection engineering, threat hunting, and adversary emulation.

Sixty-one percent of respondents use ATT&CK to feed adversary emulations, allowing them to emulate specific threat actors by following the known sequence of ATT&CK techniques those actors use. CTI provides these attack paths, and using ATT&CK to structure them (e.g., by utilizing ATT&CK Flow[7]) makes communicating and planning these adversary emulation activities easier.

The broad usage of ATT&CK across the above use cases underscores its versatility, and CTI teams can utilize it for defense, testing/validation, and communication. The results encourage any CTI program not yet leveraging ATT&CK to strongly consider doing so, given its benefits and the industry momentum behind it. Finally, the survey's analysis of analytic methods found that knowledge bases like ATT&CK are the most frequently used methods in CTI analysis, with around 68% of respondents using them regularly—far more than many other methods.

Kevin Holvoet
Certified Instructor

COURSES TAUGHT

FOR578: Cyber Threat Intelligence

VIEW PROFILE

"In 2025, CTI teams say written reports are now their main delivery method, a sign that teams prefer durable narratives to raw data dumps. Intelligence only earns its keep when it is packaged for human decisions. That packaging is finally reaching the right desks. More than half of the questions CTI sets out to answer now come from boardrooms, not just the SOC. When leadership helps frame the questions, CTI can't stay on its own island. Analysts must link threats to budget, brand, and uptime—the things the business really cares about."

[7] "Attack Flow v2.3.3," https://center-for-threat-informed-defense.github.io/attack-flow

Reports and Communication

For the second year, reporting is the top CTI dissemination method, rising from 62% in 2022 to 80% in 2025. This highlights a key insight:

Intelligence has little value if it isn't communicated effectively.

Reports are followed by TIP integrations (72%), emails or slide decks (68%), and briefings (61%). Because reports drive decision-making, CTI teams should focus on creating clear, polished, and actionable deliverables.

As Figure 11 shows, CTI teams produce a range of report types to meet strategic and tactical needs, with threat landscape reports being the most common. Sixty-eight percent of teams produced these reports to provide leadership with situational awareness on emerging threats, adversary activity, and sector-specific trends. Their popularity highlights CTI's role in helping executives understand "what's out there," informing long-term security decisions, and guiding investment. Over half of teams publish quarterly or annual trend reports (56%), while 26% produce business-focused intelligence, including mergers and acquisitions assessments or reports tied to executive travel in high-risk regions.

Figure 11. Types of CTI Reports Produced

At the operational level, CTI teams commonly produce tactical "be-on-the-lookout" (BOLO) alerts (64%) and incident after-action reports (61%) to support security operations and incident responders. BOLO alerts warn of active threats—like phishing campaigns or malware outbreaks—enabling preparedness and prompt response. Incident after-action reports contextualize incidents, link them to threat actors, and guide future improvements. Additionally, 59% of teams develop threat actor profiles detailing adversary TTPs and motivations to support SOC analysts, threat hunters, and red teams. These deliverables highlight CTI's critical role in day-to-day security operations.

Survey responses show that CTI teams are tracking threats and increasingly curating intelligence into structured, reusable deliverables.

The growing emphasis on formal reporting reflects a maturing discipline focused on clarity, consistency, and tailoring outputs for technical and strategic stakeholders.

Interestingly, only 13% of respondents identified limited communication skills as a barrier to effective CTI implementation. However, anecdotal feedback and industry experience indicate that written and verbal communication remain underdeveloped among CTI analysts. We encourage CTI professionals to actively build these skills by reading and writing reports, attending relevant training courses, presenting at conferences, and engaging with peers across the community.

Technology Enablement

The growth of CTI has been accelerated by greater support from leadership, the growth and development of a skilled analytic workforce, and technologies that support CTI processes.

Artificial intelligence (AI) adoption in CTI has accelerated significantly, with more than a third of organizations now leveraging AI in some part of their CTI program.

Areas where AI has a high impact include the gathering and processing of data, as well as processing and scoring to assist with prioritization (see Figure 12).

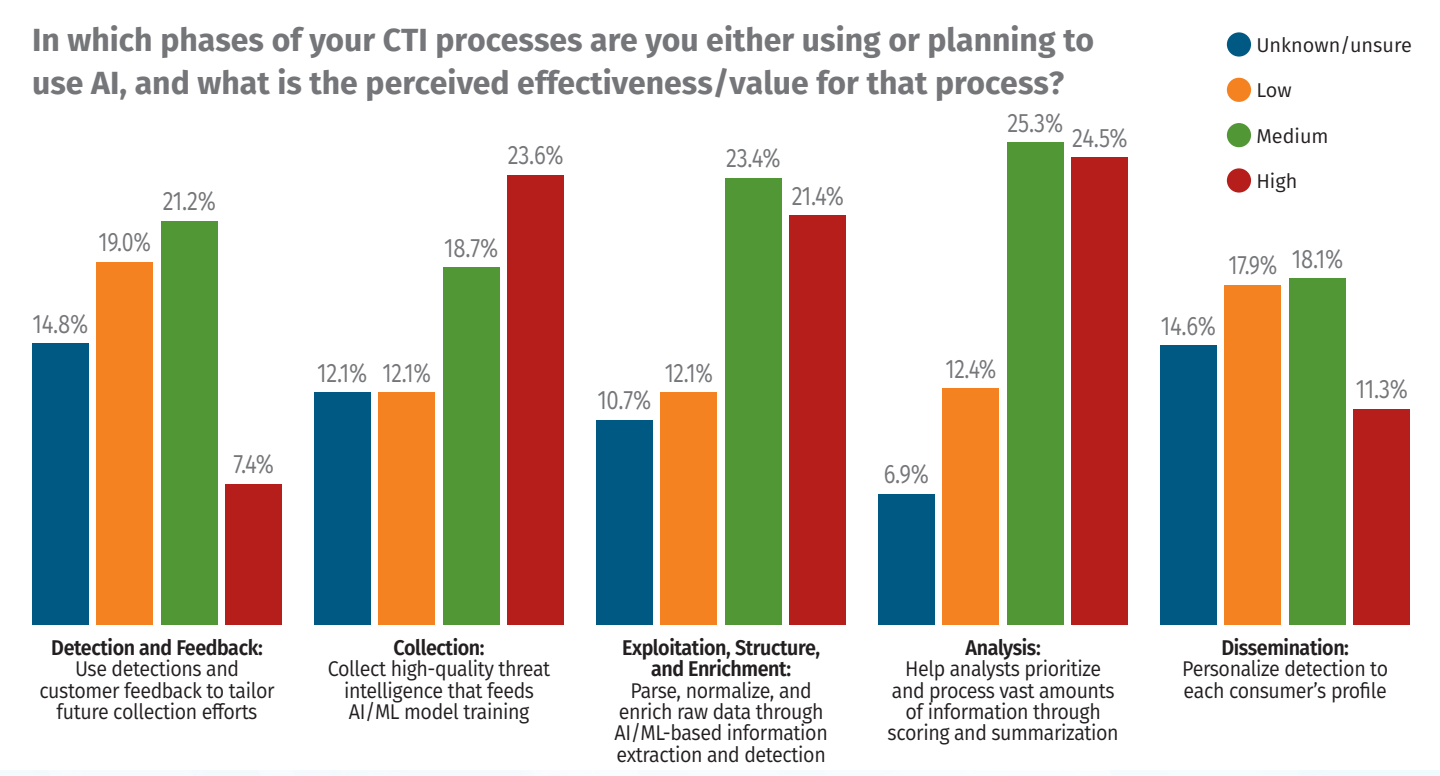


Figure 12. Application of AI Across the Intelligence Cycle

Pattern recognition was called out as a specific area where AI can support analysis. As CTI analysts consume increasing amounts of external information through threat reports and media reporting, AI can speed this process by highlighting areas for analysts to focus their attention.

One area where AI is perceived as being of lower value or utility is dissemination. This could be an opportunity to explore in the future, especially with reporting cited as the top dissemination method. AI can provide ways to customize reports to a specific audience and technical level, increasing the applicability of reporting.

Automation has also become a focal point for CTI programs striving to handle large volumes of data and improve efficiency. Seventy-four percent of respondents have built tooling into their processes to support automation. When respondents elaborated on their tooling processes, many wrote that automation has been centered around integrating CTI-specific tools into existing workflows and processes. These tools include integration with both vendor tools and open source tools, which have both been cited as challenges in past years' surveys. Increased levels of automation in CTI tooling specifically show the progress made in the industry in addressing past challenges. However, there is still work to be done, because 41% still cite lack of tool interoperability and automation as a challenge.

Assessing CTI ROI/CTI Metrics

One of the toughest questions for any CTI program leader to answer is: "How do we know our threat intelligence is actually making a difference?" Unlike reactive functions like incident response, where impact is more visible, showcasing the value of a proactive or analytic capability has historically been difficult to quantify in concrete metrics or ROI terms. Throughout SANS CTI surveys, respondents have acknowledged this challenge and stressed the importance of establishing measures of effectiveness.

Today, 55% of respondents measure the effectiveness of their CTI program, 32% do not, and 14% are unsure whether any efforts are made to measure effectiveness.

Of those who do measure effectiveness, many leverage more than one method of gathering feedback, but the most common is seeking feedback directly through meetings (84%), which indicates that most CTI programs do have a feedback loop mechanism (although it may be ad hoc in nature). If the meetings are regularly scheduled exclusively to gather feedback on the CTI program, then they are likely part of a formal process. However, if the practice is instead to use a portion of existing meetings to cover CTI efficiency, then the feedback process can be deprioritized or passed up for other, more pressing events. Other prevalent methods include surveys or emails, comparison with baseline metrics, and indirect feedback. These approaches show that both qualitative and quantitative measures are in play (see Figure 13).

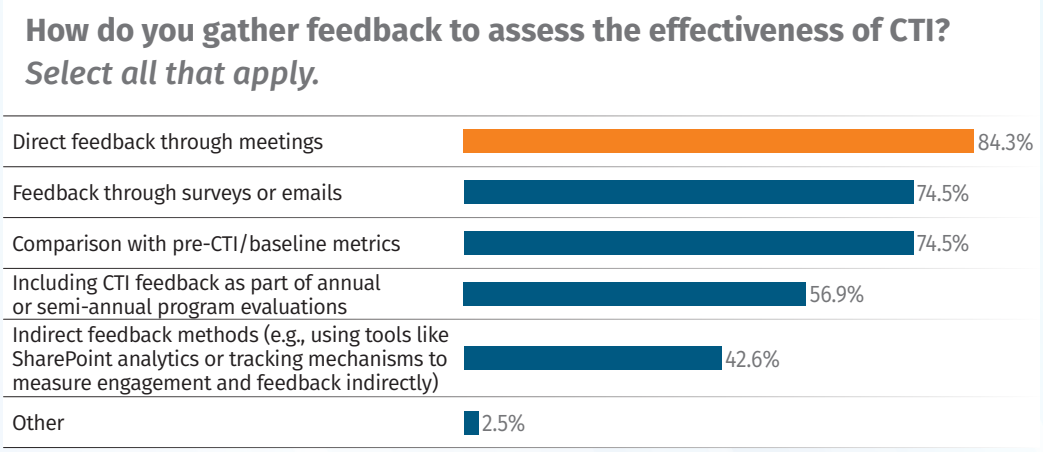


Figure 13. Methods for Gathering Feedback on CTI

Feedback is also critical for assessing CTI program maturity and guiding long-term planning. Respondents cited using strategic roadmaps, custom maturity models (often aligned with the NIST Cybersecurity Framework), regular gap assessments, and industry benchmarking. Some have adopted specific key performance indicators (KPIs), while others struggle to prioritize planning due to daily operational demands. A few reported implementing the CTI Capability Maturity Model (CTI-CMM)[8]—a community-driven framework that helps align CTI efforts with organizational goals. Version 1.2 of the model introduces metrics[9] that can support effective measurement and continuous improvement.

Although qualitative feedback is common—even among mature programs—it should ideally be supplemented with performance metrics over time.[10]

We highly recommend that CTI practitioners utilize maturity frameworks (e.g., CTI-CMM) and incorporate the relevant metrics to strengthen their programs.

[8] "CTI-CMM," https://cti-cmm.org

[9] "Metrics," https://github.com/cti-cmm/Metrics

[10] "Beyond Meh-trics: Examining How CTI Programs Demonstrate Value Using Metrics," January 2025, www.sans.org/blog/beyond-meh-trics-examining-how-cti-programs-demonstrate-value-using-metrics

Key Roadblocks

Lack of funding has been a consistent issue reported by CTI professionals throughout the years. However, this year it hit a new high with 62% reporting it as a key blocker, an increase from 52% in 2024 and 40% in 2023. This is likely a result of the continuation of budget cuts and hiring freezes over the past few years. Despite reports of much greater executive-level contributions to intelligence requirements—which sits at 52% this year, up from 32% in 2023 and 33% in 2024—lack of management buy-in also has increased. When budgets are tight and resources are limited, it is important to find ways to demonstrate the benefits of the CTI program to leaders. Even if you are not currently an organization experiencing funding issues, focusing on ROI and demonstrating impact now can help prevent this trend from continuing to increase at such high rates (see Figure 14).

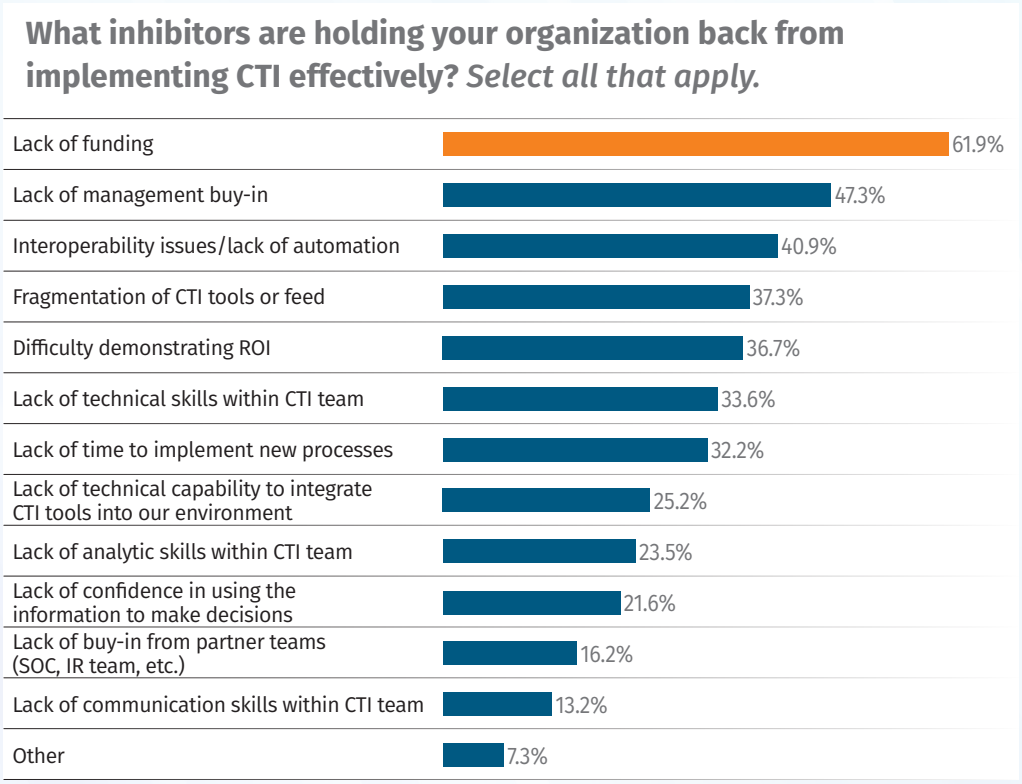


Figure 14. Key Blocks to CTI

Another blocker is a lack of technical skills in an organization's CTI analysts. Roughly one-third (34%) of respondents felt that this was an area that held their organization back from effectively implementing a CTI program, higher than the number who felt that a lack of analytic skills on their CTI team (24%) was a blocker.

This highlights the multifaceted role many in the CTI field are expected to take on. Although CTI analysts are often considered investigators and interpreters, there are also more technically focused roles, sometimes called cyber threat intelligence engineers, that focus primarily on building and maintaining the infrastructure to collect and enrich the information needed to generate threat intelligence.

Without that infrastructure, it can be challenging to scale up analysis, integrate disparate tool sets, and automate processes—all areas that are important to the functioning of a strong CTI program.

Although these challenges highlight the barriers organizations face, they also point to areas where CTI teams can focus their efforts to unlock growth opportunities and improve efficiency in their CTI programs.

Opportunities for Growth

The increased adoption of automation, expanded CTI tooling, and increased leveraging of AI, specifically large language models (LLMs), present significant opportunities for teams to continue to optimize their processes. Additional emphasis on the skills required for CTI engineering functions will support the continued evolution. Respondents also report that they leverage existing vendor capabilities for implementing AI into their current processes or plan on leveraging these built-in integrations when they start implementing AI. This shows an opportunity for the CTI vendor community to continue partnering with organizations to support both existing and emerging use cases.

AI also can support CTI teams in disseminating intelligence by helping to more easily tailor CTI products to specific stakeholders or use cases, including user education, raising awareness of threats to leadership, or partnering with vulnerability management teams. As the interest in and applicability of CTI products grow, and as CTI teams identify their own risk appetite for leveraging tools such as AI within their sometimes-sensitive environments, using these resources to customize analytic findings can reduce the time needed to create specific intelligence products for a variety of consumers. As with all aspects of the intelligence cycle, it is important to validate any work supported by AI and customize reports to individual organizations' unique needs.

Another area of opportunity is to **increase the variety of internal information used in CTI programs.** Currently, CTI collection sources emphasize external data. The top sources of information used in CTI analysis include media reporting, vendor reports/data feeds, and threat information from sharing groups. Including additional internal information, especially information outside of the purely technical realm, can provide additional context and help analysts know when to prioritize or key in on relevant external information. CTI teams can work with other internal teams such as business operations, communications, HR, executive travel, and others to understand the unique threats their organizations may be facing and identify the types of internal information available (e.g., internal newsletters, travel logs, executive calendars, insider risk indicators, etc.) for them to stay connected to internal changes that may impact CTI requirements.

Gathering feedback is another area where opportunities exist. Although feedback is a critical part of the intelligence process, in practice, many CTI teams dedicate limited time and resources to this final stage of the intelligence cycle. This often-overlooked step is a missed opportunity to assess the value of the intelligence produced and to tailor it more effectively to stakeholder needs. We encourage CTI practitioners not to neglect this critical phase and to invest in capturing meaningful feedback to strengthen relevance, impact, and continuous improvement.

Moving Forward

In the coming years, these are a few of the developments we expect to see in CTI:

- **Maturation of the CTI field—**Over the past decade, CTI has professionalized as a discipline, moving from being viewed as more of an art to a true profession with dedicated teams, focused reporting, and continually evolving tool sets. The creation of frameworks like MITRE ATT&CK helped by giving the industry a common lexicon to talk about threats. As time progresses, we hope to see more models, such as CTI-CMM and the newly released metrics model, continue to provide additional structure and roadmaps to follow. Having strong foundational structures like these in place allows the profession to move from relying on intuition or ad hoc methods to repeatable processes that can be applied consistently while still leaving room for adaptations and improvements over time.
- **Skills, training, and core competencies—**As cyber threats become more sophisticated and varied, there is a growing demand for skilled CTI professionals. Investments in education and training programs are essential to equip the workforce with the necessary expertise to analyze and counter emerging threats. Although different organizations will have different intelligence requirements for their teams to focus on, all professionals will still need core fundamental skills, including critical thinking and communication skills, in addition to technical and analytic threat intelligence skills. These skills also often include engineering skills required to help build and integrate the tools to support CTI work. Frameworks such as the Mandiant CTI Analyst's Core Competencies Framework[11] can help organizations identify the skills needed to meet their unique needs and build the right teams.
- **Partnering with commercial vendors—**CTI teams continue to rely on partnerships with CTI providers, whether they provide vendor threat data feeds, create tools or platforms that integrate with internal systems, or are part of hybrid functions integrated with the CTI teams themselves. One important area to watch is how the commercial sector evolves over time. As CTI products prove their value, we see an increase in acquisitions of CTI-focused companies into larger corporate entities, which may change the way that they operate and result in larger, more global solutions. We also may continue to see a market for smaller, niche offerings as organizations tune in to their unique needs, whether that is for ultra-regional intelligence due to shifts in the regulatory landscape or an innovative way to acquire and apply specific types of threat data. Furthermore, as questions around digital and intelligence data sovereignty continue to take shape, the evolution of the commercial CTI sector will be a place to watch.

[11] "Introducing the Mandiant Cyber Threat Intelligence (CTI) Analyst Core Competencies Framework," May 2022, https://cloud.google.com/blog/topics/threat-intelligence/cti-analyst-core-competencies-framework

Sponsor

SANS would like to thank this survey's sponsor: