SANS | Research Program

SURVEY

2026 SANS Cyber Threat Intelligence (CTI) Survey Insights

From Indicators to Insights: How CTI Empowers Both Practitioners and Decision-Makers

Written by **Rebekah Brown**
& **Andreas Sfakianakis**
May 2026

BROADCOM
Dataminr
ESET
flare
INTEL471
SOCRadar Your Eyes Beyond
WIZ

Foreword

Every year, the SANS CTI Survey gets sharper. This year, it takes a step the field has needed for a while. For the first time, the 2026 survey includes a dedicated module for security executives, capturing responses from 67 CISOs and CSOs. That addition matters. CTI has always served two audiences, the analysts who produce intelligence and the leaders who act on it. Until now, this survey has captured the practitioner view with depth and rigor while leaving the executive perspective largely inferred.

Now we have both. And what the data reveals is not conflict between practitioners and executives, but rather a structural gap between recognition and influence that better threat reporting alone will not close.

For security leaders, the CISO module offers something rare: a direct look at how peers are experiencing CTI. What are other executives prioritizing? Where does intelligence fall short of informing decisions? That lateral visibility is hard to come by, and the findings are specific enough to act on.

For practitioners, it provides an unfiltered line of sight into what is actually on a senior leader's mind, not what you imagine they want, but what 67 executives reported directly when asked what intelligence they rely on and what would make CTI more central to their decisions.

CTI that never reaches the people who set direction and allocate resources is leaving most of its value on the table. Understanding both sides of that gap is the first step toward closing it. This year's survey, for the first time, gives us both.

Rebekah Brown
Certified Instructor Candidate

COURSES TAUGHT
FOR578:
Cyber Threat Intelligence

VIEW PROFILE

Andreas Sfakianakis
Certified Instructor

COURSES TAUGHT
FOR578:
Cyber Threat Intelligence

VIEW PROFILE

Cyber Leaders

SANS | Research Program

For the first time, **the 2026 SANS CTI Survey includes a dedicated CISO module, capturing responses from 67 security executives, primarily CISOs and CSOs. The findings do not reveal disagreement between executives and practitioners, but rather an alignment on value and a persistent gap on influence.**

Key Highlights

1. **The value-influence gap is the defining CISO finding.** 91% of CISOs value CTI, but only 26% say it significantly influences their decisions. That disconnect is the most important thing the CISO data reveals and the thread that runs through everything else in the section.
2. **CISOs want operational intelligence, not more intelligence.** Their top priorities are exploited vulnerabilities and adversary TTPs, not broader strategic reporting. They are not asking for more. They are asking for intelligence that tells them what to do next.
3. **Business-focused intelligence is CTI's biggest untapped opportunity.** Only 41% of CISOs find business-focused intelligence valuable today, almost certainly because they have rarely seen it. This is not a demand problem, it is a production problem, and the first team to fill that gap creates a new category of influence inside their organization.

The Value-Influence Gap

The majority of CISOs rate CTI as valuable or extremely valuable while a much smaller group indicate it significantly influences their decisions (see Figures C1 and C2). That gap is the headline and probably the most important point this data reveals. The problem is not credibility. CISOs are not questioning whether CTI is accurate. The problem is translation. Describing a threat accurately is not the same as telling an executive what to do about it. Until CTI products answer the questions that drive decisions, like which risks require action now, what to tell the board, and where to spend, the gap will persist.

How valuable do you consider CTI to your organization's overall cybersecurity strategy?

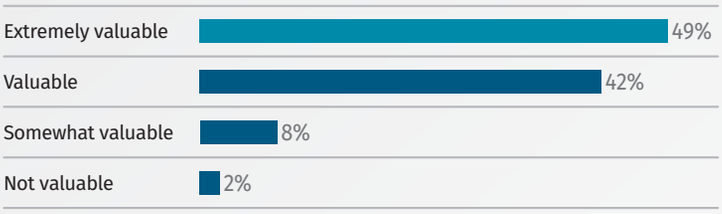


Figure C1. CISO CTI Value

To what extent does CTI influence executive decision-making?

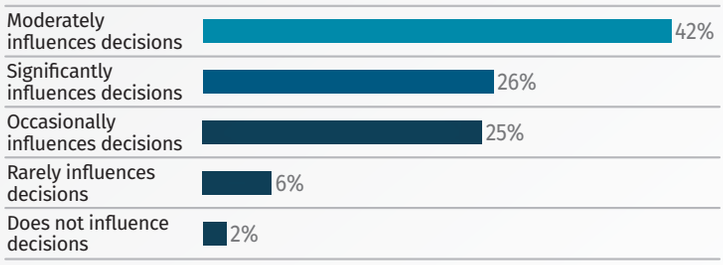


Figure C2. CTI Influence on Decision-Making

Cyber Leaders

SANS | Research Program

What Executives Actually Want

CISOs are not asking for more intelligence, they are asking for intelligence that feeds their decision-making. Their top priorities for the next 12 months are vulnerabilities being actively exploited and specific adversary TTPs (see Figure C3). The question they need answered is not which vulnerabilities exist, but which one's adversaries are weaponizing right now against organizations like theirs.

Which of the following CTI reports are most useful to understanding the threats facing your organization? *Select all that apply.*

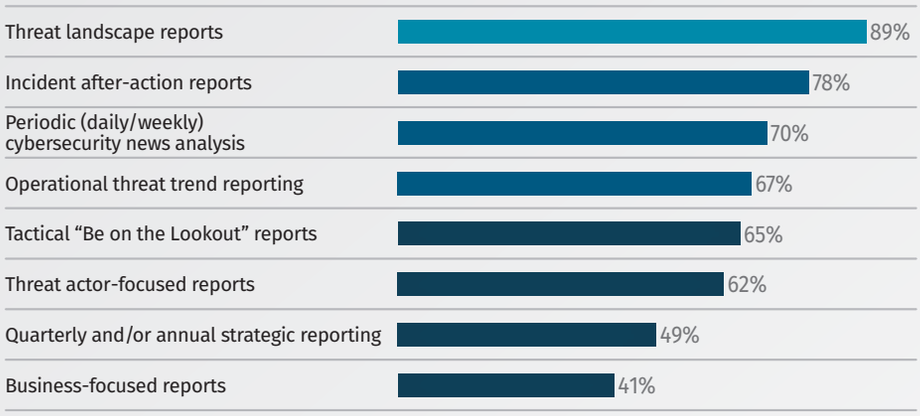


Figure C3. CTI Reports Most Useful to CISOs

The products CISOs value most reflect that same orientation toward real-world impact, with threat landscape reports and incident after-action reports leading by a wide margin (see Figure C4). Quarterly strategic reports and business-focused intelligence rank at the bottom, likely because most CTI teams are not producing them at scale, not because executives do not want them.

What information about digital threats will be most useful to your organization over the next 12 months? *Select all that apply.*

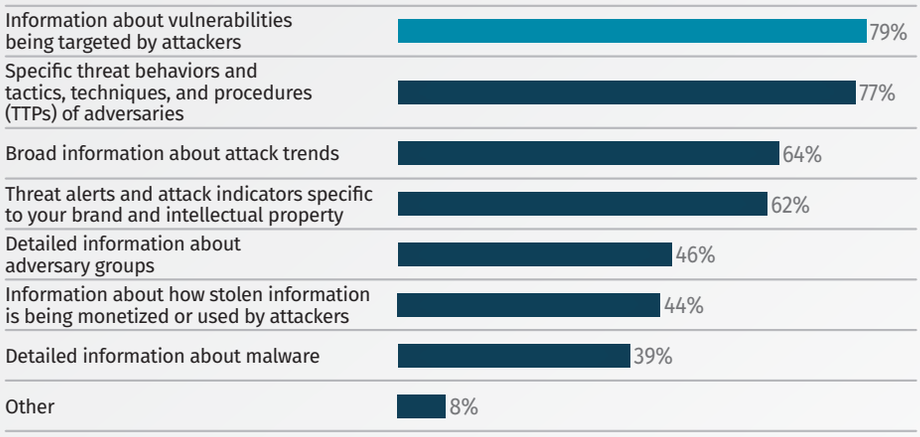


Figure C4. Threat Information Found to Be Most Useful

Cyber Leaders

SANS | Research Program

Four Actions to Close the Gap

The data makes the path forward clear. Closing the gap between how CISOs value CTI and how much they act on it does not require a larger team or a bigger budget. It requires four deliberate shifts in how intelligence is produced and delivered:

- **Build decision packages, not intelligence briefings.** Structure products around the decisions executives are making, not the threats analysts are tracking. Lead with the recommendation, support it with evidence, and make the required action explicit.

  RECOMMENDED ACTION: Interview two or three key stakeholders this quarter and ask what decisions they make monthly, then redesign one existing product to directly inform those decisions. This matters because intelligence that is not connected to a specific decision is easy to appreciate and easy to ignore. Tying products to real decision cycles is what turns CTI from a briefing into a business input.

- **Connect CTI directly to vulnerability management.** 79% of CISOs want to know which vulnerabilities are actively being exploited, and 63% of CTI teams already support vulnerability management. The capability exists on both sides. What is missing is making the connection explicit by showing decision makers how CTI directly shapes which vulnerabilities get patched first and how quickly.

  RECOMMENDED ACTION: Produce a monthly one-pager that maps actively exploited common vulnerabilities and exposures to your organization's environment and links each to a recommended remediation priority. This makes the CTI-to-patching connection visible and decision-ready, giving executives and vulnerability management teams a direct line from threat intelligence to action rather than leaving that translation to chance.

- **Make incident after-action reports a standard deliverable.** Every incident is an opportunity to demonstrate CTI value through real outcomes. Programs that do this consistently build a track record that is far more persuasive than any capability briefing.

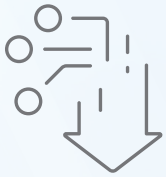
  RECOMMENDED ACTION: Add a CTI contribution section to every post-incident review that documents what intelligence was available before the incident, how it was used, and what it would have taken to act on it earlier. This is important because it creates a concrete, evidence-based record of CTI's role in real events, giving leadership something tangible to point to when evaluating the program's value and making the case for continued investment.

- **Pilot business-focused intelligence.** Only 41% of CISOs find business-focused intelligence valuable today, but that number almost certainly reflects how rarely it is produced rather than how little it is needed. Executives cannot ask for something they have never seen, and products like mergers and acquisitions risk assessments, executive travel briefings, business-unit specific threat briefings, and supply chain threat profiles represent an entirely new category of value waiting to be introduced.

  RECOMMENDED ACTION: Identify one upcoming business event, a merger, an acquisition, a major executive trip, or a new vendor relationship, and produce a single intelligence product tied to it. Use the response to that pilot to build the case for more. This is important because business-focused intelligence expands CTI's relevance beyond the security function and into decisions that drive the organization, creating new advocates for the program among stakeholders who previously had no reason to engage with it.

2026 SANS Cyber Threat Intelligence (CTI) Survey Key Findings.

The 2026 SANS CTI Survey tells a story of a discipline at a strategic inflection point, one where CTI is widely recognized as essential but not yet structured to deliver the impact that recognition implies.



CTI is everywhere but stretched thin.

The discipline has achieved broad institutional adoption, yet most teams remain under four full-time employees (FTEs). The gap between what CTI is being asked to do and the resources available to do it is the defining structural challenge of 2026.

The influence gap is the headline.

CISOs overwhelmingly value CTI (91% rate it valuable or extremely valuable), yet only 26% say it significantly influences their decisions. Intelligence that is appreciated but not acted upon is not yet achieving its purpose.

AI has crossed from experiment to operations.

Nearly half of organizations (45%) are using AI in CTI today, primarily for summarization, reporting, and workflow automation. The human-in-the-loop model is holding, and AI is now an operational expectation, not a novelty.

Governance is the forgotten risk.

More than half of organizations (55%) lack legally reviewed CTI sharing processes, even as recent cyber regulations (e.g., NIS2 and the Cyber Resilience Act) impose new obligations. This is not a technical gap; it is a structural one.

CTI teams are losing time, not skill.

Lack of time (44%) and lack of funding (44%)—not lack of expertise—are the top barriers to implementing CTI. Burnout, organizational silos, and operational tempo are the day-to-day reality for analysts.

Security operations (SecOps) has reclaimed the top spot.

For the first time since 2022, SecOps (71%) has overtaken threat hunting as the leading CTI use case, signaling a shift toward embedding intelligence into daily defensive work.

The leadership perspective above reflects a curated view of the data. The full report that follows provides the complete picture; the survey results, trend analysis, and recommendations that inform it.

Executive Summary

Cyber threat intelligence (CTI) has arrived. It is embedded in security programs, staffed by dedicated teams, supported by AI, and recognized at the executive level as essential. The 2026 SANS CTI Survey confirms this, and then asks the harder question: What, exactly, is CTI essential to?

The central finding of this year's survey is not about adoption. It is about impact. CTI is valued by nearly every organization that uses it, yet only 26% of CISOs report that it significantly influences their decisions. Analysts cite lack of time and lack of funding as their top barriers to implementation, not lack of skill. Half of all programs do not systematically measure their own effectiveness. And more than half operate without legally reviewed sharing processes, even as new regulations begin to impose real obligations. These are not the problems of a discipline in its infancy. They are the problems of a discipline that evolved quickly and now has an opportunity to strengthen its foundations and fully realize its value.

CTI is no longer fighting for legitimacy. It is fighting for influence.

The 2026 data shows CTI programs that are more capable than ever: Smarter collection strategies, AI moving from pilots into production, and its applications, from SecOps to threat hunting, continue to grow. And yet these programs are operating inside structures that were never designed to support what CTI has become. Small teams. Reactive workflows. Ad-hoc portfolios. No measurement infrastructure. The CTI capability has outpaced the organizational structure built around it.

That gap between what CTI can do and what it is currently set up to deliver is what this report is about. Closing that gap does not require more headcount or bigger budgets. It requires deliberate program design, a sharper focus on outcomes and decision influence, and the organizational discipline to measure what matters. CTI is no longer fighting for legitimacy. It is fighting for impact. The data shows exactly where that fight needs to be won.[1]

[1] Survey demographics are located at the end of this report.

A Discipline That Grew Up and Is Now Showing the Strain

The most important structural finding in the 2026 survey is also the most persistent: CTI teams are small, and they are not growing proportionally to the demands placed on them. Although this is not a new observation, the implications are sharper than ever.

The Small Team Reality and Why Nothing Changing Is a Big Deal

Most organizations now report a formal dedicated CTI team (see Figure 1), the highest rate in this survey's history. A decade ago, having any assigned CTI resource was unusual. Today, it is the norm. And yet formal adoption has not translated into resource growth.

Nearly a quarter of organizations rely on a single dedicated person or a shared-responsibility model, suggesting that in many organizations, CTI is a side function rather than a focused capability. Even among organizations with formal teams, most remain below four full time employees (FTEs), and the largest CTI teams continue to be concentrated in large enterprises, government agencies, and managed service providers, consistent with what the survey has shown in prior years.

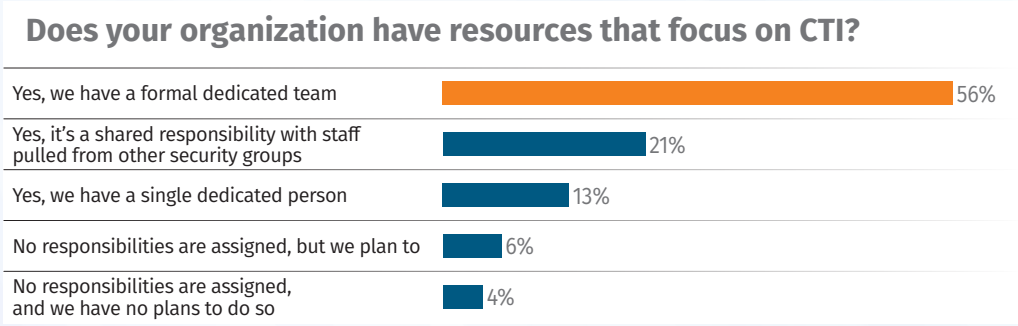


Figure 1. CTI Resources

This matters because the survey simultaneously shows CTI being asked to support an expanding set of use cases, security operations, incident response, threat hunting, vulnerability management, security awareness, adversary emulation, risk management, physical security intelligence, and executive decision-making. A team of two or three analysts cannot do all of that at high quality, and the result is triage rather than strategy, with CTI programs that should be shaping organizational posture who are instead reacting to the loudest immediate demands.

This is not surprising given what we know about organizational budgeting for security functions. What is notable is how little has changed despite growing awareness of CTI's value. It suggests organizations have adopted CTI as a capability faster than they have funded it as a function. Program leaders should stop expecting this to self-correct and start designing programs that are sustainable at small scale.

CTI has been adopted faster than it has been funded.

Expert Corner

As CTI programs grapple with limited size, increasing demands, and a push to integrate AI into stakeholder support workflows, establishing a self-service model that provides direct access to external vendor sources or internal platforms offers resource constrained teams with a measurable time savings option. In sharing vendor licenses or provisioning access, coupled with CTI-hosted training, this achieves scalability while providing data to support future budgetary discussions on CTI tools and data.

VIEW PROFILE

John Doyle
SANS Certified Instructor;
Director of CTI Services at Palo Alto Networks Unit 42

COURSES TAUGHT

FOR578:
Cyber Threat Intelligence

Keeping Analysts Engaged When There Is No Backup

In small teams under sustained operational pressure, analyst engagement is both critical and fragile. The data shows a skills-first approach, with external training and CTI vendor engagement leading as the top strategies. This approach makes sense given that technical and analytic skill gaps remain a consistent barrier and training directly addresses them (see Figure 2).

What is conspicuously absent is investment in analytic culture. Off-site retreats, internal analytic working sessions, and brown-bag sessions all rank far below formal training. Teams that develop skills in isolation, without shared analytic frameworks and institutional knowledge-building, are fragile. Individual analysts who leave take their context with them. Peer learning, shared methodologies, and collective analytic culture are what make small teams resilient over time, and they are being underinvested.

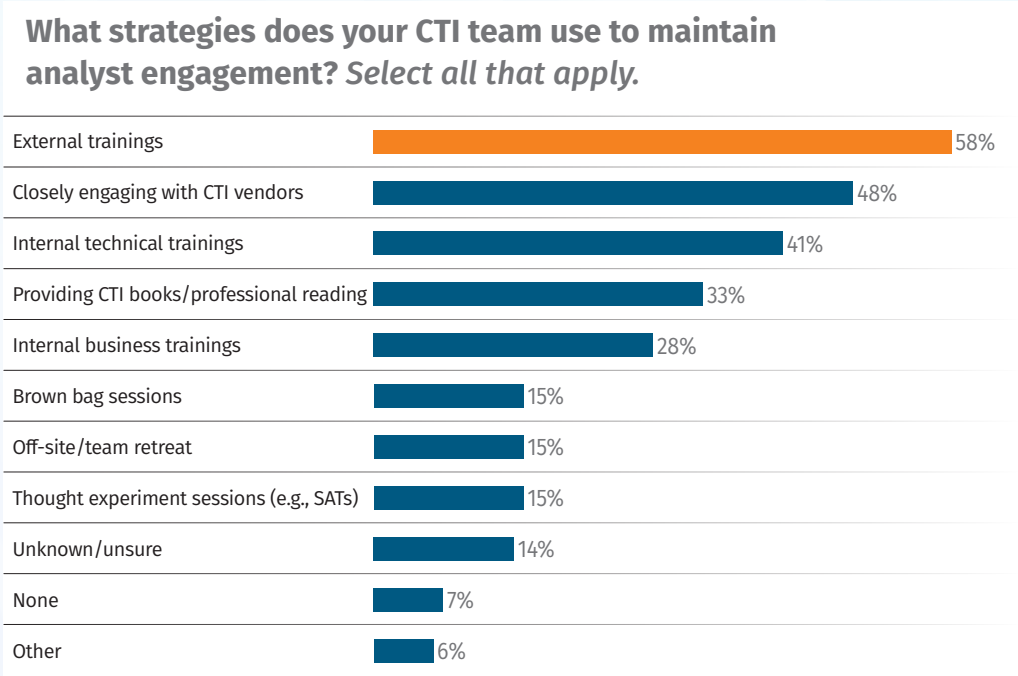


Figure 2. Analyst Engagement Approaches

Expert Corner

What stands out most to me in this year's survey is not whether CTI is valued (which it is), but whether it is influencing the decisions that matter most. CTI delivers its greatest value when it's tied to business impact, enterprise risk, and strategic decision-making, and when it's baked into policies, standards, and other governance changes across the organization. I'm encouraged by the progress reflected in the survey data, but truly mature programs still need to keep elevating CTI beyond a primarily tactical function and further it into a strategic one before we can say the mission is complete.

VIEW PROFILE

Sean O'Connor
SANS Certified Instructor Candidate; Global Head at The Equinix Threat Analysis Center

COURSES TAUGHT

FOR589: Cybercrime Investigations

From Collection to Dissemination, Quality Is Winning

How CTI programs collect, analyze, and share intelligence has undergone a quiet but meaningful shift in 2026. The trend is toward quality, specificity, and formalization, a maturity signal that reflects a discipline learning from its own outputs.

For five consecutive years, external media reporting and news were the dominant sources in CTI collection plans, peaking at 90% of organizations in 2025. In 2026, that number dropped significantly, with open source CTI feeds and published intelligence reports now ranking as the top sources, followed by vendor threat feeds and community or industry groups such as ISACs and CERTs (see Figure 3).

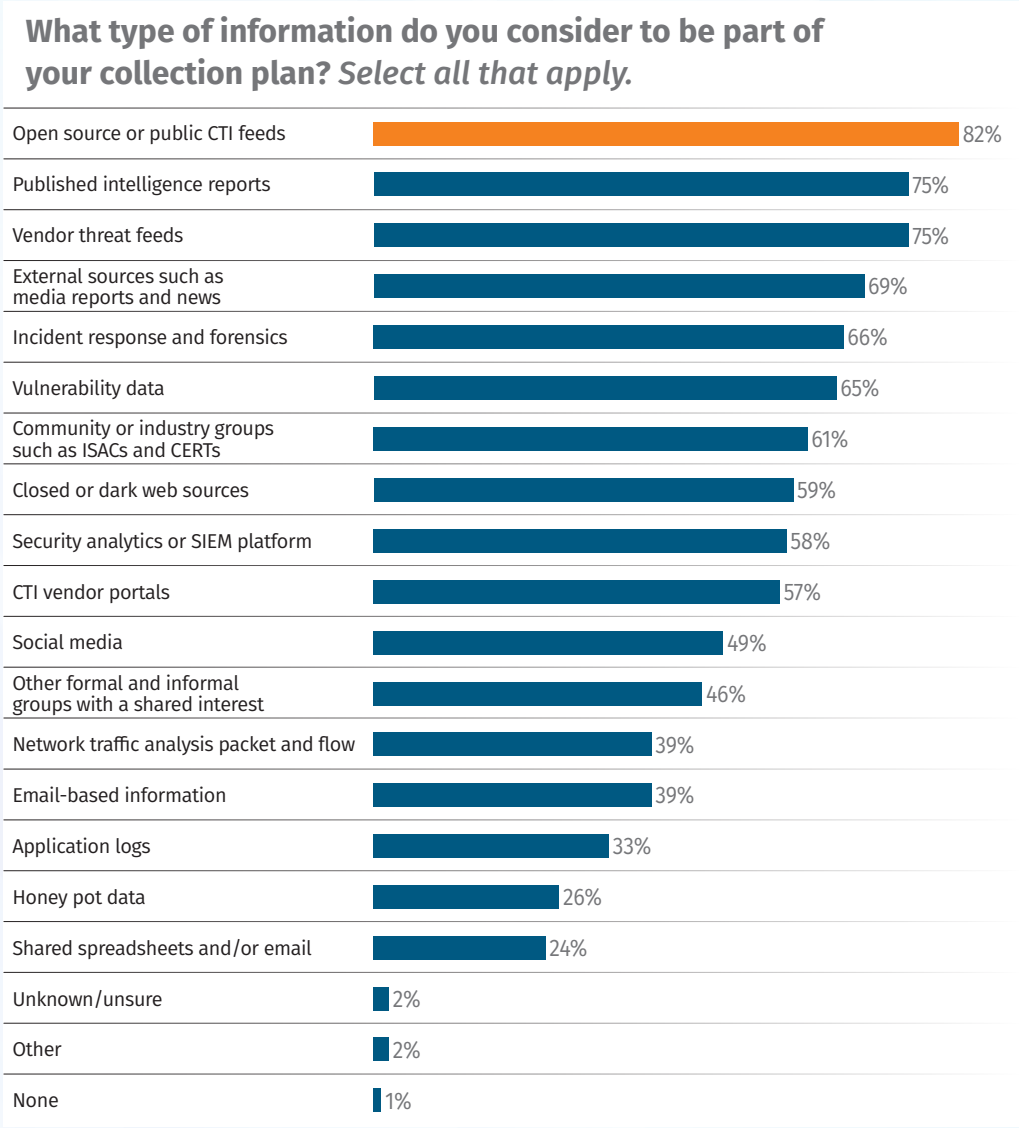


Figure 3. Collection Plan Information

This shift deserves attention. It does not necessarily indicate that media reporting has become less useful, but it does suggest that CTI programs are becoming more selective in how they incorporate it. One possible explanation for the sudden decrease is that practitioners are exercising greater caution in response to the growing prevalence of AI-generated content, which can require additional time and effort to verify its authenticity and reliability. In this new environment, media sources may introduce more analytic overhead compared to other vetted intelligence sources. Similarly, social media usage in collection dropped from 65% in 2025 to 49% in 2026, reinforcing the same pattern. One solution to this problem is to leverage AI tools themselves to help filter and validate reporting to reduce this new overhead.

What makes this shift particularly interesting is the persistence of an opportunity the SANS CTI Survey data has flagged consistently. Incident response (IR) and forensic data remain underutilized as a CTI source despite being cited by 66% of respondents. This is arguably the richest source of organization-specific, reliable, and contextually validated intelligence available to any program, and the gap likely reflects organizational silos between IR and CTI teams rather than any lack of awareness that the opportunity exists.

The richest source of CTI many organizations are sitting on is their own incident response data.

Analysis Frameworks: ATT&CK Holds, Gaps Remain

MITRE ATT&CK® continues to function as the common language of CTI analysis, reflecting its durability as a cross-team communication framework. Because CTI serves diverse consumers, SOC analysts, IR teams, vulnerability management, and executives, a shared framework enables findings to be understood and acted upon across organizational boundaries. For the 20% of teams not yet using a knowledge base, adoption could unlock significantly more intelligence value by giving analysts and stakeholders a shared vocabulary for interpreting and acting on findings.

The Dissemination Gap: Reports Still Lead, But Portfolios Are Missing

Reports remain the dominant mode of CTI dissemination, followed by platform integrations, and briefings (see Figure 4). The more striking finding is the state of CTI product portfolios. 2026 marks the first year this survey asked about defined portfolios, and the results are a maturity indicator with significant implications because only about a third (34%) report a fully defined portfolio of CTI products (see Figure 5).

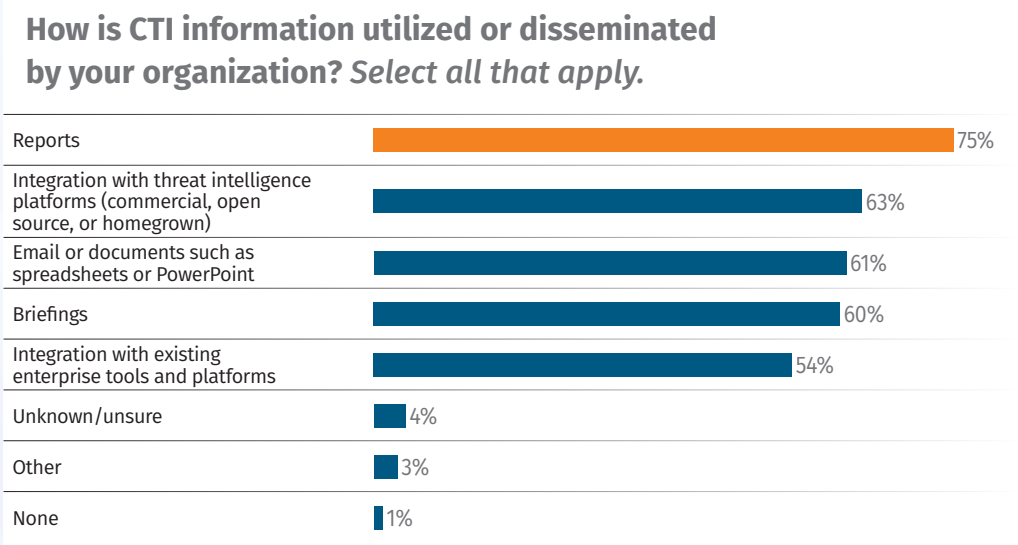


Figure 4. CTI Dissemination

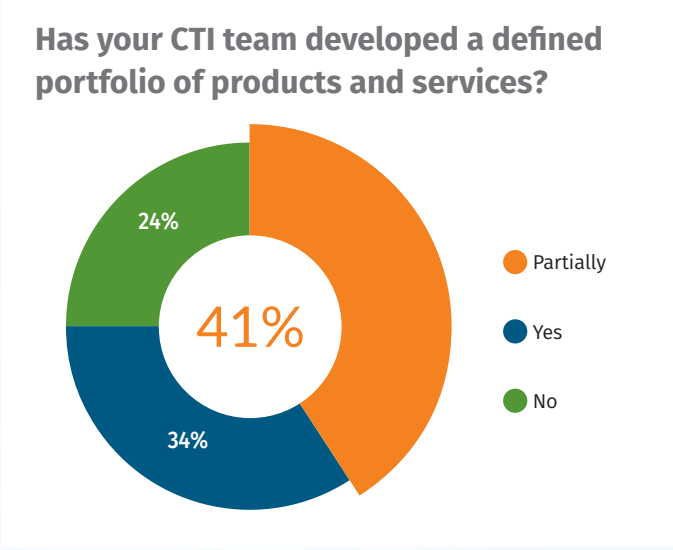


Figure 5. CTI Portfolio Definition Status

This is important to note because without a defined portfolio, CTI teams risk being perpetually reactive, responding to ad hoc requests rather than delivering against a planned set of outputs. Ad hoc work is harder to measure, harder to justify to leadership, and harder to protect during budget cycles. A formal CTI services and products portfolio is the infrastructure that lets small teams say no to low-value requests and demonstrate impact systematically. Of those who do have portfolios, 45% report they are both shared across the organization and supported by delivery or project management functions, a signal of what best practice looks like.

CTI's Defining Challenge

If there is a single finding that defines the 2026 survey, it is that CTI is valued by the organizations that use it, but that value does not consistently translate into decisions, actions, or outcomes. This influence gap is visible in the practitioner data and confirmed sharply by the CISO data as well.

CTI earns recognition from nearly every organization that uses it, but that recognition isn't impacting change in budgets, priorities, or decisions. This gap between recognition and impact is the story of 2026.

Security Operations Reclaims the Top Spot

SecOps has emerged as the leading CTI use case in 2026 (see Figure 6), reclaiming the top position it last held in 2022. One possible explanation for this shift is that insights generated during the peak of threat hunting, which held the top spot between 2023 and 2025, are now being operationalized into day-to-day defensive workflows. As organizations mature their detection engineering capabilities, intelligence derived from hunting can be codified into rules and playbooks, reducing the need for sustained, resource-intensive hunting at the same level.

Regardless of the cause, the shift to SecOps is broadly positive because it means CTI is informing the most operationally intensive security function in most organizations. But it also creates risk. When CTI becomes primarily a support function for reactive operations, the capacity for strategic, forward-looking intelligence work diminishes. The same small teams feeding the SOC's daily needs have less time to develop the longer-horizon intelligence products that influence executive decision-making. The triage problem becomes self-reinforcing. When CTI becomes captured by daily operations, strategic intelligence suffers, and so does the case for more resources.

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

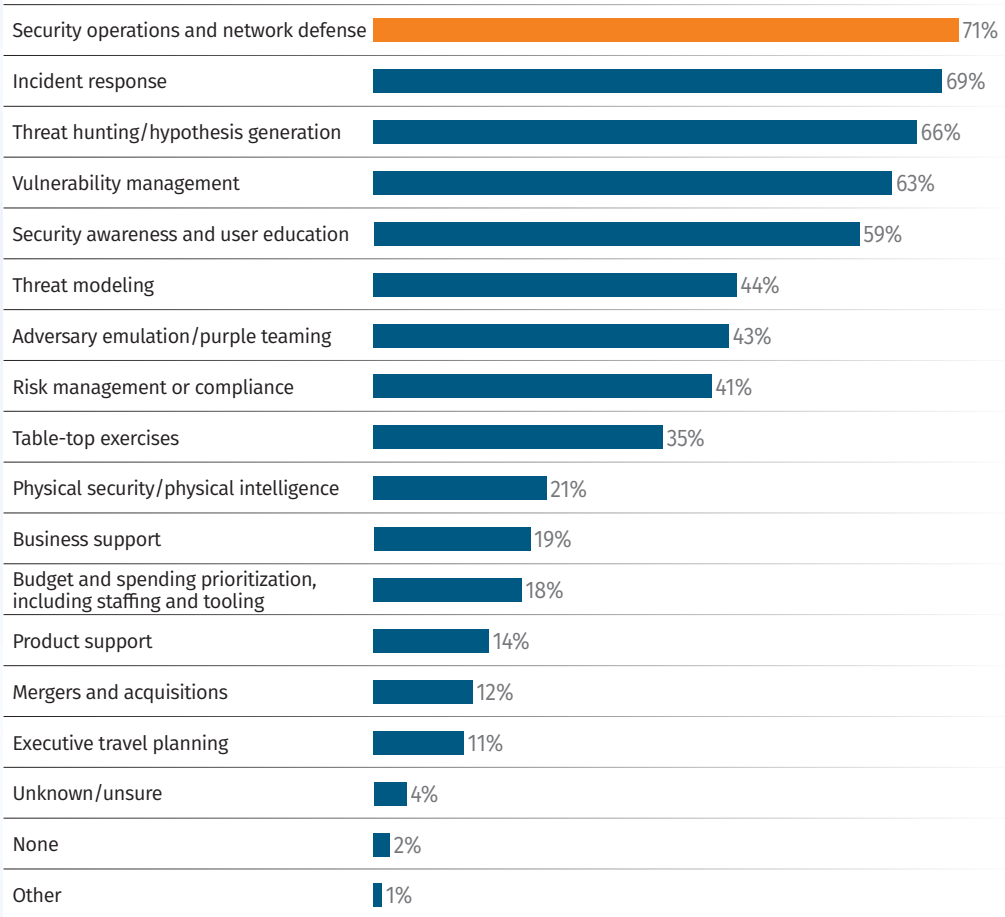


Figure 6. CTI Utilization by Use Case

Feedback Loops: Half the Field Is Flying Blind

Just over half of organizations actively gather feedback on CTI effectiveness, which is slightly down from 2025 (see Figure 7) and among those who do, direct meetings dominate. The meeting-based approach provides nuanced context and enables rapid adjustment, but it is qualitative, relationship-dependent, and impossible to scale or benchmark.

More alarming is that 43% of programs do not track CTI maturity over time (see Figure 8). Taken together, these numbers mean a significant portion of CTI programs cannot demonstrate improvement, cannot make a data-backed case for additional resources, and cannot identify which investments are producing results. In an environment where 44% cite lack of funding as a top barrier, that is not an abstract problem, it is an existential one.

Previous years tell the same story where feedback and measurement have consistently been underprioritized relative to their strategic value. The organizations that will sustain CTI programs through budget pressure are the ones that can point to measurable impact.

You can't defend a budget you can't measure.

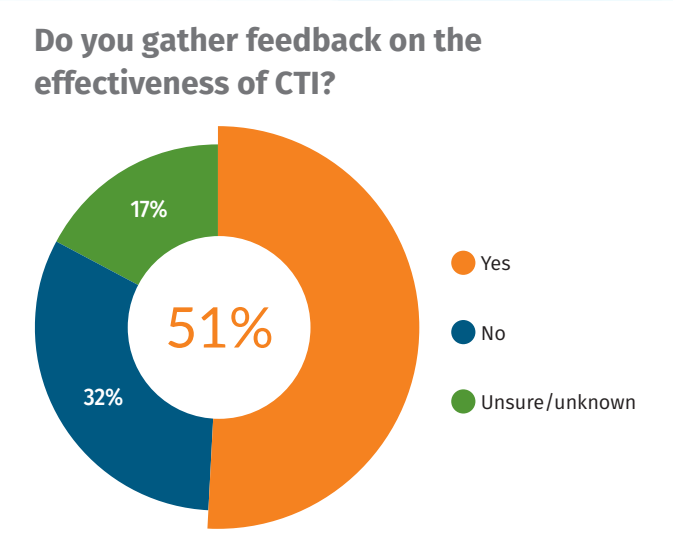


Figure 7. CTI Effectiveness Feedback

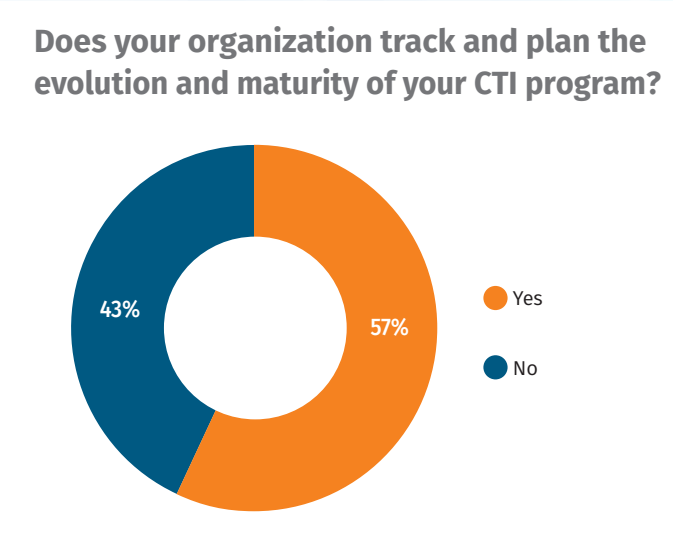


Figure 8. Maturity Tracking

Expert Corner

It would benefit a lot of CTI teams to mandate breaking down the barrier between them and Incident Response. We know it's a best practice to analyze incident data, we have the tools, we have the Diamond Model of Intrusion Analysis, but we don't build the relationship to make access to intrusion data sustainable enough to turn it into a quality intelligence source. This highlights the importance of core skills in CTI—especially the role that relationship building has in getting access to internal data sources, improving collection, and producing more relevant intelligence. Make a point of buying coffee or lunch for your Incident Responders (outside of a live incident) and discuss how CTI can better support them. Ensure you have a strong foundation of providing value before asking for access to data.

VIEW PROFILE

Josh Darby MacLellan
SANS Certified Instructor Candidate;
Staff Threat Intelligence Advisor
at Feedly

COURSES TAUGHT

FOR478:
Cyber Threat Intelligence Foundations

Communication: The Undervalued Half of CTI

Periodic written reports and executive summaries remain the primary internal communication vehicle, followed by collaboration tools and situational awareness or threat landscape newsletters (see Figure 9). The variety of channels reflects a mature understanding that different stakeholders consume intelligence differently. What is missing is evidence that these channels are being used strategically to build CTI's internal profile, connecting intelligence products to decisions that were made well and making the value of CTI visible to the people who control budgets.

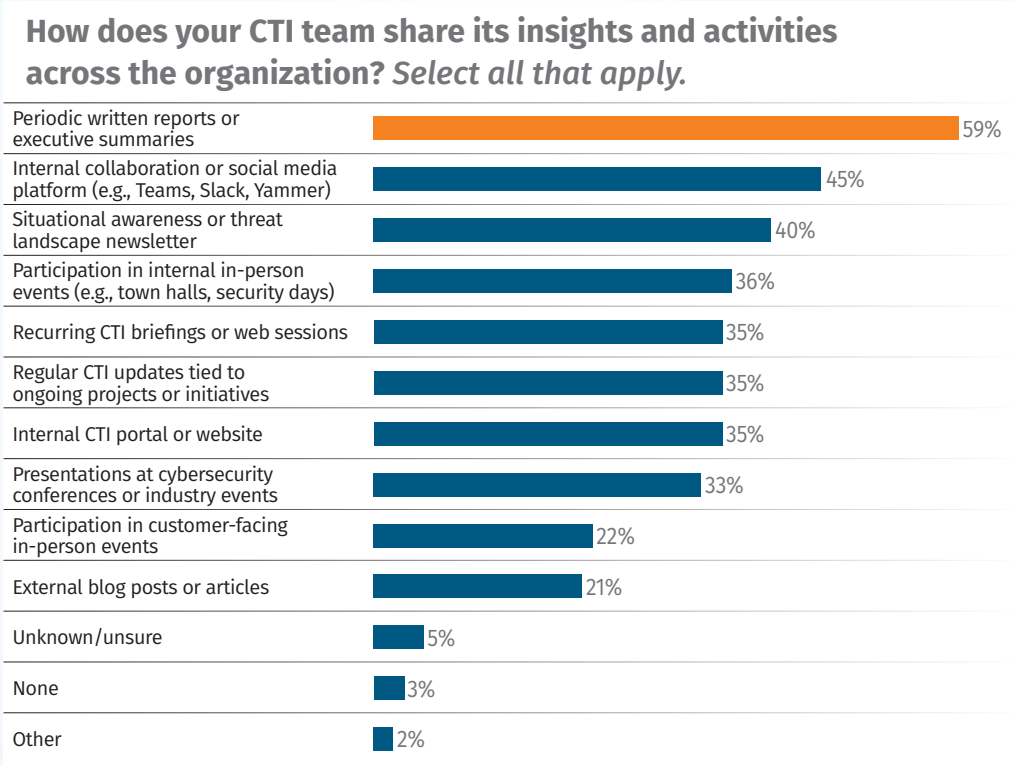


Figure 9. Internal CTI Communication Methods

AI Has Arrived

The 2026 data confirms what many CTI practitioners suspected: Artificial intelligence (AI) has crossed from experimentation into operational deployment. The question is no longer whether AI will affect CTI practice, but instead around how programs should scale and govern its use. AI momentum is unmistakable with almost half of organizations reporting using AI in their CTI programs today and another third planning to adopt AI (see Figure 10).

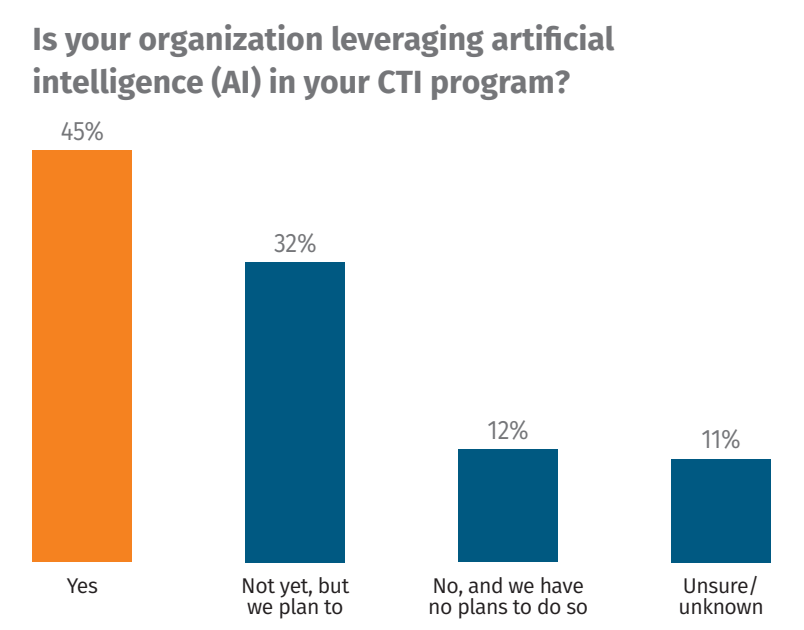


Figure 10. AI Adoption

Specifically, AI does well in the CTI context with data summarization and report writing in the lead, followed by data parsing and normalization, workflow automation, and improving data collection (see Figure 11). These are all tasks that reduce analyst burden on high-volume, low-insight work, exactly the kind of work that was consuming time that should be spent on analytic judgment.

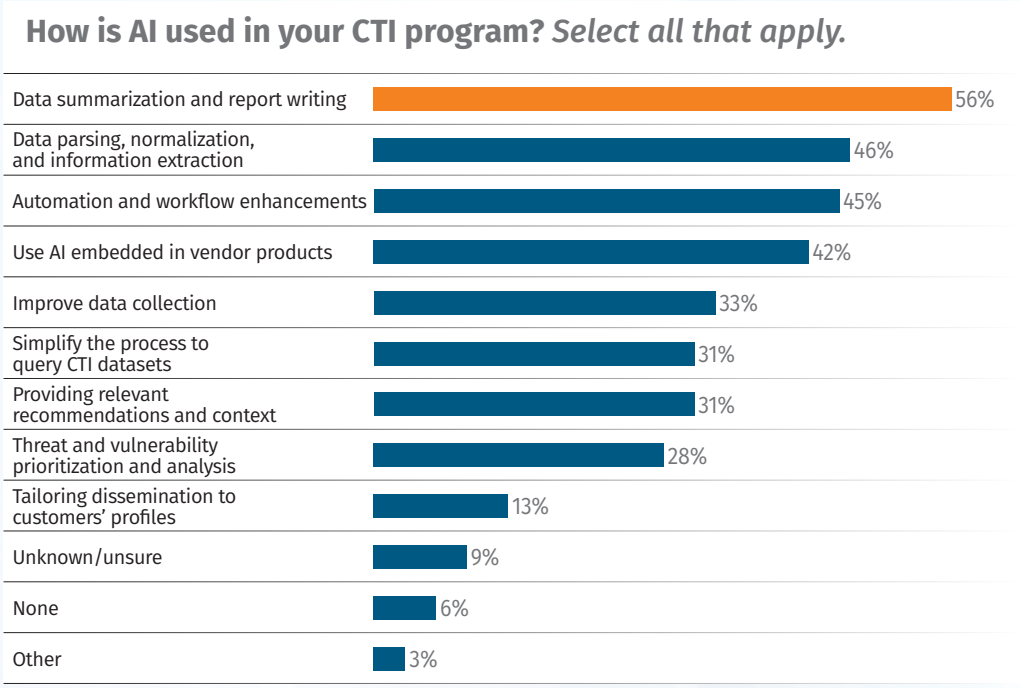


Figure 11. AI Usage

The human-in-the-loop model is holding strong. Write-in responses consistently emphasized analyst oversight as essential, particularly for high-stakes decisions where accuracy, confidence calibration, and trust are paramount. Organizations building sustainable AI-enhanced CTI programs keep human analysts accountable for final judgments, using AI to accelerate the work rather than replace the thinking.

In 2024 and 2025, AI in CTI was largely a story of cautious experimentation with uneven results, unclear use cases, and lingering questions about whether the outputs could be trusted. The 2026 data reflects a shift to scaling proven use cases; integrating AI into SIEM, TIP, and SOAR workflows; and operationalizing productivity gains from early pilots. Organizations that invested early have identified where AI delivers reliable value and are expanding those applications. The window for competitive advantage from early AI adoption is narrowing.

AI is not replacing CTI analysts. It is giving them time back to do the work that AI cannot do.

Expert Corner

The finding that CTI isn't consistently influencing decisions matches what I've seen in practice. As a field, we've been very effective at proving CTI is needed, but far less effective at demonstrating its value after the investment is made. In constrained environments, teams need a relentless focus on stakeholder outcomes. That doesn't come from gathering requirements once, it comes from continuously engaging, collecting feedback, and adapting to changing needs. In a world where AI can generate and distribute generalized threat information at scale, the differentiator for human analysts is their ability to understand what their stakeholders actually need and ensure intelligence stays relevant to real decisions.

VIEW PROFILE

Katie Nickels
SANS Certified Instructor;
Director of Intelligence at Red Canary

COURSES TAUGHT

FOR578:
Cyber Threat Intelligence

Geopolitics, Governance, and the Regulatory Tide

Two forces are reshaping the external environment for CTI in 2026: expanding geopolitical instability and an accelerating regulatory agenda. Both create new intelligence requirements, and both expose gaps in how CTI programs are structured to respond.

Geopolitics Is Now an Intelligence Requirement

Most respondents say geopolitics is very or somewhat important to their intelligence requirements (see Figure 12). Physical security and physical intelligence appear as a CTI use case for 21% of organizations, a niche-but-growing signal that the convergence of cyber and physical threats is real and accelerating. Organizations with global operations, executive protection concerns, or exposure to politically sensitive regions are driving this adoption.

One factor that may be driving this risk is the increased personalization of risk. Executives are being targeted as individuals by cyber criminals, but also by politically motivated actors in response to public positions, corporate decisions, or perceived affiliations. This creates a threat landscape where online activity, public perceptions, and real-world exposure intersect, requiring close coordination between CTI and physical security teams.

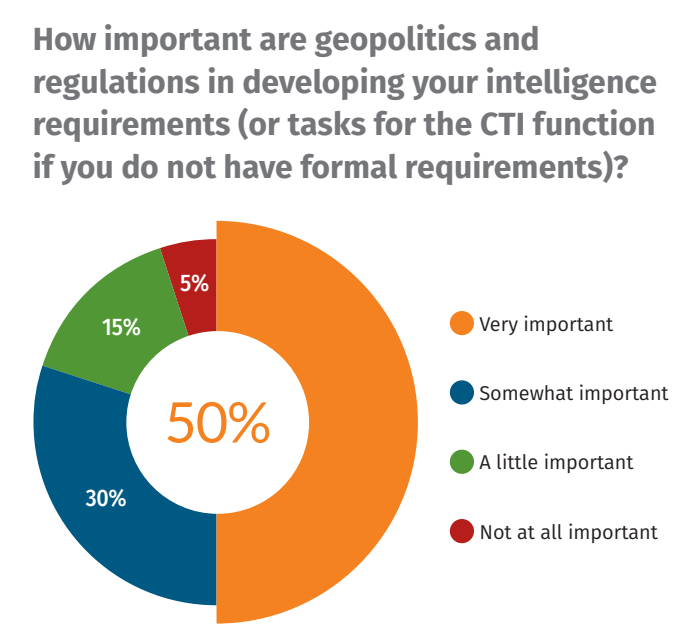


Figure 12. Importance of Geopolitics

If geopolitical instability continues to intensify, the organizations without a framework for integrating geopolitical intelligence into their CTI programs may find themselves without early warning on an expanding class of threats.

The Governance Gap

More than half of organizations report that their CTI sharing processes have not been formally reviewed by legal counsel (see Figure 13). At the same time, 50% of respondents say regulations are very important to their intelligence requirements, and new obligations are already arriving. The EU's NIS2 Directive imposes cybersecurity, risk management, and incident reporting requirements across essential sectors, and the Cyber Resilience Act implements new reporting requirements beginning this year. The gap between regulatory awareness and legal readiness is not a minor administrative oversight but rather a structural risk.

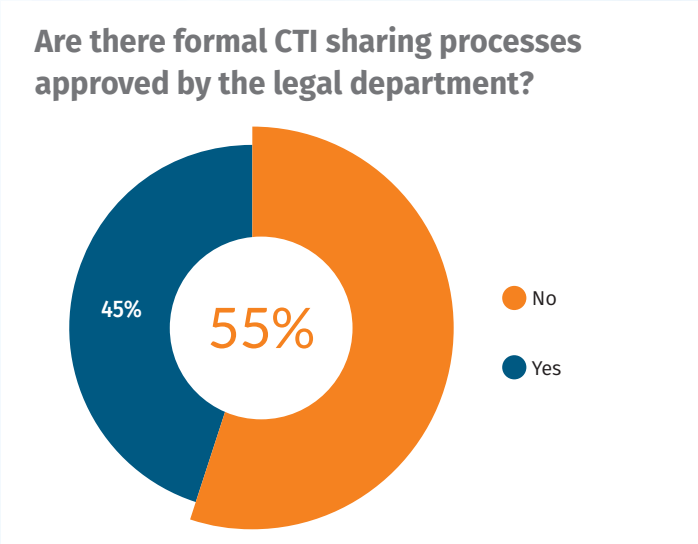


Figure 13. Legal Review

Regulatory importance and the absence of legal review, creates a tension that CTI teams cannot afford to ignore. The practical consequence of this gap is that CTI teams facing uncertainty about legal exposure tend to share less. They withhold intelligence that could benefit the broader community, are hesitant to participate in sharing networks, and slow down collaborative responses to emerging threats. The irony is that the goal of information sharing is undermined by the absence of the governance that would make it safe to share.

If CTI cannot share intelligence safely, the core premise of the discipline breaks down.

The Barriers Are Structural, Not Skill-Based

For years, the CTI field has debated the skills gap, and the 2026 data offers a provocative reframe of that question. The data shows that a lack of time to implement new processes and lack of funding are the top barriers to effective CTI implementation (see Figure 14). These are not skill deficits but rather resource deficits. The good news is that technical and analytic skill gaps, while real, rank well below structural constraints. Organizations have made genuine progress in developing CTI talent. The bottleneck is now organizational, not human.

The implication is significant, because the solutions that follow from a resource deficit are very different from the solutions that follow from a skill deficit. Training on its own is not likely to resolve challenges rooted in time and funding constraints. Instead, training efforts are most effective when they are explicitly designed to help analysts work more efficiently under real-world conditions, focusing on prioritization and the effective use of tools, including AI, to reduce manual efforts. Organizations will benefit most from restructuring CTI workflows to minimize low-impact work, define clear portfolio boundaries, and build measurement infrastructure to make the case for additional resources.

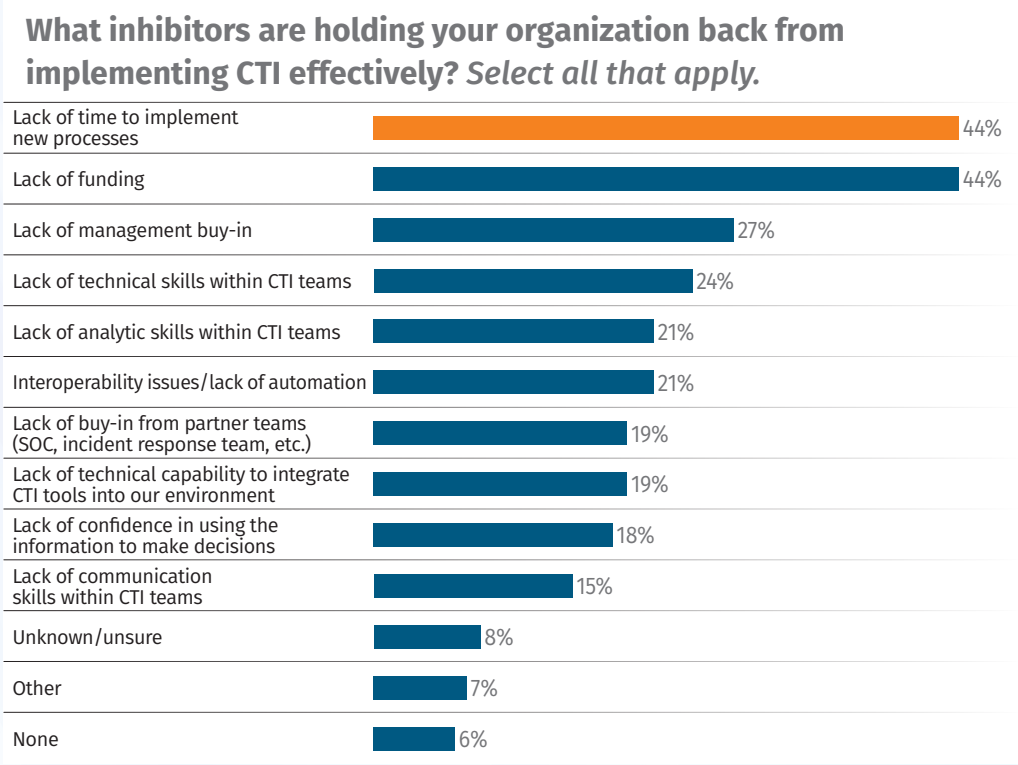


Figure 14. Implementation Barriers

That structural pressure does not stop at the program level. When asked about challenges limiting analyst effectiveness, the top responses paint a picture of structural dysfunction rather than individual failure, with organizational silos and poor cross-team collaboration leading, followed by burnout, constant high-tempo operations, and unclear prioritization (see Figure 15).

Burnout appearing this prominently in an effectiveness survey is a signal that deserves organizational attention. The disciplines that lose their best analysts to burnout pay a compounding cost when institutional knowledge walks out the door, replacement requires months of ramp-up, and small teams are particularly vulnerable to the departure of even one experienced practitioner.

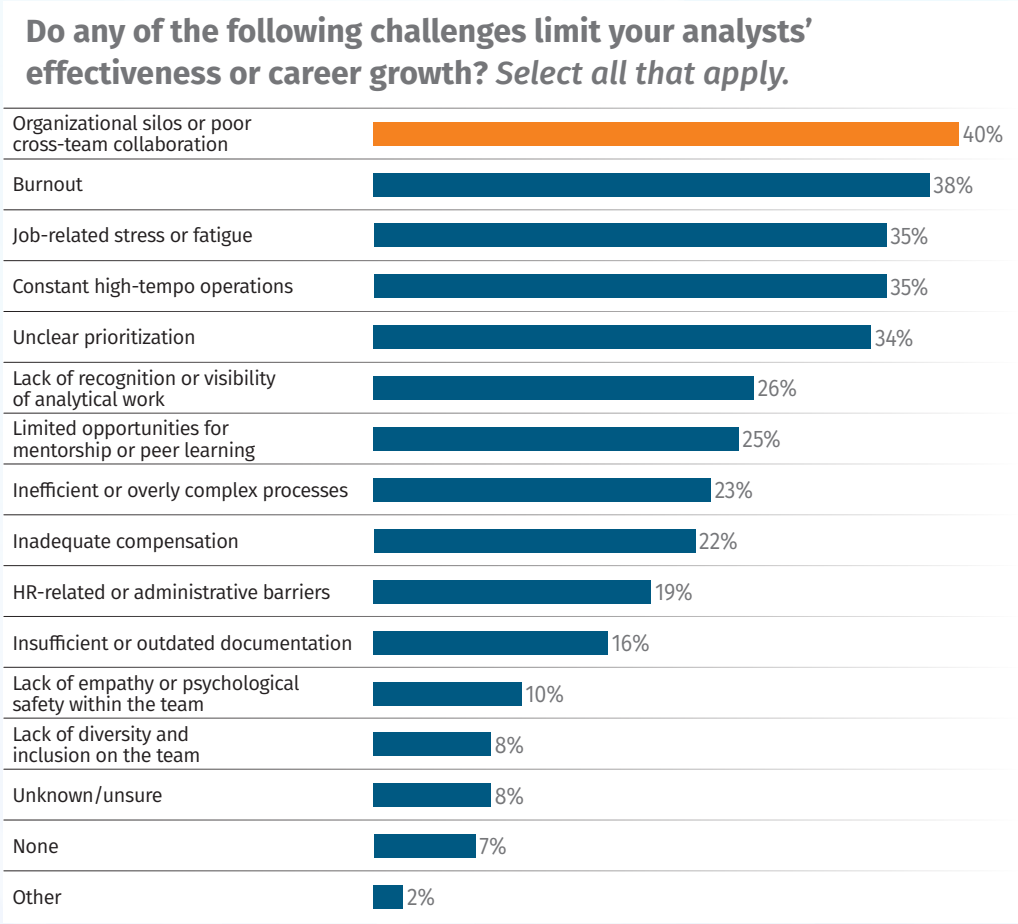


Figure 15. Challenges to Analyst Effectiveness

The structural response to burnout and the structural response to the staffing constraint point to the same solutions: workload management, realistic scope definition, and operational tempo control. Notably, compensation, diversity, and empathy rank significantly lower as barriers in 2026, which suggests that the community has made genuine progress on some dimensions of workplace culture, even as structural and operational challenges intensify.

When CTI loses analysts to burnout, the impact cascades.

Act Now

The data speaks to a clear set of priorities for CTI programs with five clear actions:

1. **Design for small teams. Don't wait to grow.**

   The persistent reality of small CTI teams is a planning input, not a temporary problem. Stop designing programs for the team you *hope to have* and start building for the team you have. Notably, build a team for sustainability at small scale, not for a future headcount that may never arrive. Three things make the difference between a small team that thrives and one that burns out:

   - Automate low-value, high-volume tasks aggressively. AI-assisted and automation workflows, especially with vetted, trusted, and structured data, exist precisely to create capacity in small teams.
   - Define and defend a clear product portfolio. Without explicit scope boundaries, small teams get pulled into every urgent request and never build the strategic work that justifies investment.
   - Align stakeholder expectations to realistic delivery. Promising more than a small team can deliver is the fastest way to lose credibility and, eventually, resources.

2. **Close the measurement gap before the budget cycle.**

   The 43% of programs not tracking maturity and the 49% not gathering systematic feedback are programs that cannot defend their budgets with data. Build these three things before the next budget conversation happens:

   - Defined metrics for each major CTI product (reach, utilization, decision impact)
   - A structured feedback mechanism beyond informal stakeholder conversations
   - A maturity tracking framework (Refer to CTI-CMM, which was widely cited by respondents as an effective starting point.)[2]

3. **Engage legal before the regulation lands.**

   CTI programs without legally reviewed sharing processes face compliance exposure and the chilling effect that legal uncertainty creates on sharing itself. Schedule the meeting with legal. Define what can be shared, with whom, and under what conditions. Most CTI sharing is already responsible and formalizing it gives analysts the confidence to share rather than the instinct to hesitate.

[2] https://cti-cmm.org

4. **Invest in analytic culture, not just analytic skills.**

   Training budgets default to technical skills and tool certifications. Although that is necessary, it's not sufficient. The teams that stay resilient over time are the ones that build a shared analytic culture through structured peer review, internal working sessions where analysts share and test their judgment, and shared methodologies that survive individual departures. These are not expensive programs; they are deliberate habits. Pick one internal practice to start this quarter and build from there.

5. **Position CTI as a decision support function.**

   The influence gap is not closed by producing better reports. It is closed by understanding the specific decisions that executives and stakeholders are making and tailoring intelligence to directly inform those decisions. Find out what decisions your key stakeholders make on a monthly and quarterly basis. Then ask whether your current intelligence products directly inform any of them. If the answer is no, that is where to start. The shift from reporting on threats to recommending actions is where CTI influence is won or lost.

Survey Demographics

The 2026 SANS CTI Survey collected responses from 401 qualified cybersecurity professionals globally between November 2025 and January 2026 (excluding the CISO targeted portion of the survey). Respondents were required to be responsible for evaluating, purchasing, or managing security operations technology products and services. Duplicate and unqualified responses were removed prior to analysis.

The respondent base is practitioner-heavy, with security analysts, CTI specialists, and security engineers comprising the largest segments. This ensures the data reflects hands-on operational experience rather than purely managerial perspectives. Geographic distribution is consistent with prior years, with North America and Europe representing the largest respondent populations—an important consideration given that regulatory environments, threat landscapes, and resource availability differ significantly by region.

The top four participating sectors are consistent with previous years: financial services, government and military, technology, and healthcare. Manufacturing, insurance, telecommunications, education, and transportation also contributed meaningful participation, reflecting CTI's reach into operational technology and critical infrastructure environments.

The survey likely underrepresents organizations with severely resource-constrained CTI programs and almost certainly excludes organizations that have discontinued or never established CTI functions. The data captures programs that continue to operate despite challenges, which may understate the barriers to CTI adoption and overstate the baseline capabilities of the field.

Sponsors

SANS would like to thank this survey's sponsors:

SANS | Research Program

About the SANS Research Program

The SANS Research Program is a key initiative by the SANS Institute and a premier global provider of cybersecurity research and information. SANS Research Program is designed to provide cybersecurity practitioners and leaders with data-driven insights, thought leadership, and solutions that help them better understand and respond to evolving security challenges. All content is authored by SANS instructor experts from around the world who apply their years of experience from hands-on practitioner work in the field, advisory roles, and the classroom to provide education, guidance, and actionable insights that help make the cyber world a safer place.

To learn about sponsorship opportunities for research, content, and in-person or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.

SANS | Research Program

Product Briefings for CTI

The 2026 CTI Survey represents the latest edition of SANS Institute's poll of security professionals. The sponsors of this year's survey all offer advanced capabilities that we believe will be of interest to SANS' clients, and, for this reason, we're presenting the following product briefings on a relevant offering.

BROADCOM

SANS | Research Program

PRODUCT BRIEFING

Actionable CTI Operationalized: Broadcom Cyber Threat Intelligence

Insights from 2026 SANS Cyber Threat Intelligence (CTI) Survey

May 2026

Cyber threat intelligence (CTI) provides security teams with actionable insights that improve threat detection, speed up incident response, reduce overall risk, lower false positives, and support more informed strategic security decisions.

The 2026 SANS Cyber Threat Intelligence (CTI) Survey shows that CTI is no longer considered a niche or experimental function. Instead, it is a standard element of modern cybersecurity programs, shifting the focus from whether CTI is present to how it can be effectively implemented and used. As CTI becomes increasingly integrated into both operational activities and executive decision-making, expectations for its impact continue to grow.

Broadcom Cyber Threat Intelligence

CTI from Broadcom—through its Symantec and Carbon Black solutions—provides a modern, integrated approach to endpoint protection and threat intelligence. Beyond core capabilities, the solutions help organizations address common operational challenges, including resource and budget limits, a shortage of skilled professionals, tool sprawl in hybrid environments, and the need to rapidly detect, assess, and contain active attacks. Together, these platforms support more efficient, informed, and resilient security operations.

Symantec Endpoint Security Complete

Symantec Endpoint Security (SES) Complete is an integrated endpoint security platform, providing endpoint detection and response (EDR), threat hunting, application control, Active Directory defense, and rapid remediation via a single agent and console. Through its Adaptive Protection capability, it can learn and analyze endpoint behavior to adjust security policies automatically, block anomalous activities, and reduce attack surface.

SES Complete reduces the volume of alerts and safeguards all endpoints—laptops, desktops, servers, and mobile devices across the entire attack chain. A Forrester Total Economic Impact study indicates a 180% return on investment, driven by cost reductions, improved efficiency, and better prevention of breaches.

[1] "The Total Economic Impact™ Of Symantec Endpoint Security Complete," September 2025, https://tei.forrester.com/go/Broadcom/SESComplete/index.html?lang=en-us

Key Findings

AI Adoption and Uses

45% currently use AI,
32% plan to use AI

56%
Data summarization and report writing

46%
Data parsing, normalization, and information extraction

45%
Automation and workflow enhancements

Carbon Black Cloud

Carbon Black Cloud is a cloud-native endpoint protection platform that integrates EDR, next-generation antivirus (NGAV), and behavioral analytics to identify and block emerging threats, including malware, fileless attacks, ransomware, and living-off-the-land (LOTL) techniques.

Carbon Black Cloud continuously monitors endpoint behavior and attacker patterns, providing visibility across attack vectors, real-time auditing, and rapid remediation. Live response capabilities enable secure remote diagnosis and resolution on any protected endpoint, allowing administrators to address issues directly in real time without resource-intensive reimaging.

Broadcom's Response to Critical Operational Challenges

Broadcom addresses several critical cybersecurity challenges identified in the 2026 SANS Cyber Threat Intelligence Survey.

AI Use Has Shifted from Experimental to Operational Efficiency

The survey found that CTI has moved from "nice-to-have" to "must-have," with 91% of CISOs rating it as valuable or extremely valuable. It further showed increased adoption of AI for production use, with 45% of the respondents already using AI in operations and another third (32%) planning to adopt AI. Currently, AI is most frequently used for data summarization, report writing, parsing and normalizing large amounts of available information, and automating workflows.

Symantec Endpoint Security Complete helps teams operationalize AI with industry-first Incident Prediction, a powerful security capability that enables security teams to predict, stop, and rapidly recover from incidents. Leveraging advanced AI, it identifies and disrupts LOTL attacks and other sophisticated threats before damage occurs. Trained on a massive catalog of over 500,000 real-world attack chains curated by Symantec and Carbon Black's elite Threat Hunting Team, Incident Prediction gives defenders a decisive advantage by anticipating attackers' next moves, blocking them—even when using LOTL techniques—and quickly restoring the organization to normal operations.

This proactive approach prevents and detects sophisticated attacks, resulting in up to an 80% reduction in the risk of malware, ransomware, and targeted attacks. Its machine learning and behavioral analysis differentiate legitimate activities from true threats, leading to more precise alerts and up to a 30% decrease in false positives. Customers also benefit from an 8% reduction in help desk tickets, delivering significant IT support time savings.

CTI Is Operating at Scale but Not Scaling in Size

The survey reveals that while the scope of CTI, executive expectations, and demands for integration all have increased significantly, team sizes have remained largely unchanged. This "do more with less" reality is a key driver behind downstream challenges outlined in the report.

Large CTI units are relatively rare: 62% of the respondents reported teams with four or fewer full-time employees, and 39% with two or fewer. Limited staffing can result in several challenges that limit analyst effectiveness, including poor cross-team collaboration (cited by 40% of respondents), analyst burnout (38%), job-related stress or fatigue (35%), and constant, high-tempo operations (35%).

Carbon Black Cloud helps scale CTI by integrating rich threat data with advanced AI-driven analytics and automation. It correlates signals across endpoints and attack surfaces into high-confidence incidents, significantly reducing noise from scattered alerts. Its Threat Tracer (see Figure 1) enhances investigations by revealing the full web of relationships between entities—including devices, users, processes, and files—far beyond traditional process trees. Analysts gain dynamic, interactive visual maps that uncover strategic remediation opportunities while avoiding alerting adversaries.

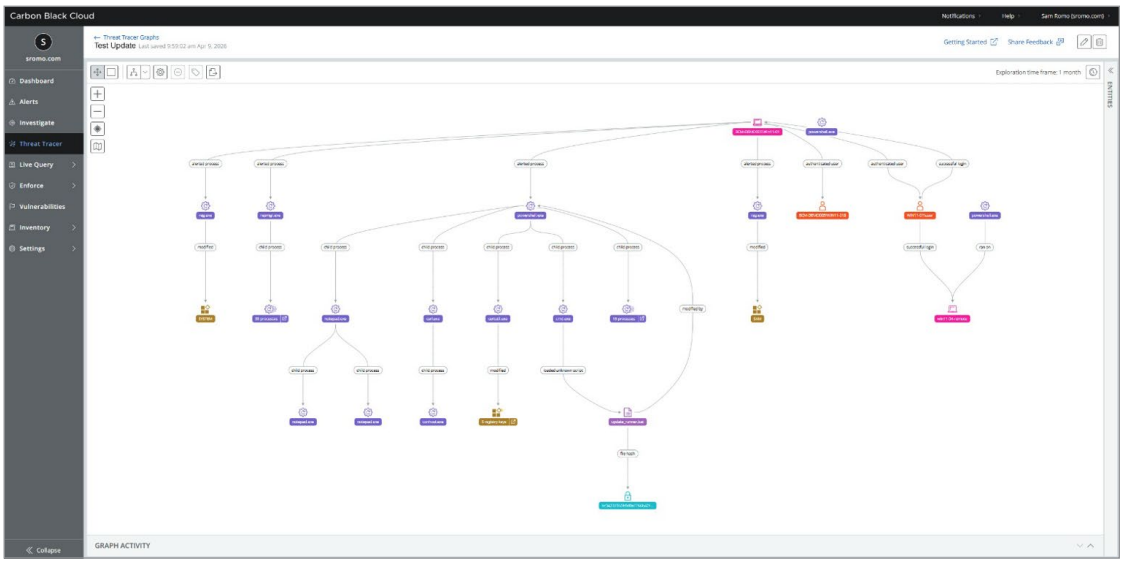


Figure 1. Threat Tracer

Carbon Black Cloud's faster investigation and remediation results in a 75% reduction in mean time to resolution (MTTR) and a 40% reduction in the risk of large-scale data breaches. It also results in reduced downtime—without added headcount. Its Live Response capabilities allow secure remote remediation, cutting reimaging by 55% by providing administrators with an instant, secure remote shell on any protected endpoint. Automated guidance and AI-assisted workflows minimize low-value alerts, reduce analyst fatigue, and free security teams to focus on strategic priorities.

Request a Demo: See CTI in Action

Want to learn more about how to leverage your investment in CTI, visit https://engage.broadcom.com/ESG-contact-us to set up a demo?

Dataminr

SANS | Research Program

PRODUCT BRIEFING

Unified Cyber Risk Intelligence: Dataminr for Cyber Defense

Insights from 2026 SANS Cyber Threat Intelligence (CTI) Survey

May 2026

Dataminr for Cyber Defense is the first end-to-end system that operationalizes Unified Cyber Risk Intelligence—combining external threat detection, internal exposure, and business impact in one decision model. Most CTI tools deliver feeds; Dataminr delivers a system.

The 2026 SANS Cyber Threat Intelligence Survey shows that CTI is a standard part of modern cybersecurity programs, with 90% of surveyed organizations now having assigned CTI resources. Rather than asking "if" CTI is valuable, the survey focused on how organizations are effectively implementing and using CTI. As CTI becomes more integrated into daily operations and executive decision-making, organizations face growing challenges around scale, prioritization, and demonstrating sustained impact.

Dataminr for Cyber Defense

Dataminr for Cyber Defense is an intelligence-driven threat and exposure management suite that correlates external threats, internal security posture, and business impact to operationalize Unified Cyber Risk Intelligence (UCRI). Instead of generating isolated alerts, it automates the entire intelligence life cycle, often delivering predisclosure exploits hours or days *before* vulnerabilities are reported through traditional feeds. Dataminr combines four key capabilities—threat intelligence, investigation insights, the agentic threat intelligence platform, and continuous control monitoring with risk quantification—into three integrated solutions.

Client-Tailored Threat Intelligence

Client-Tailored Threat Intelligence (CTTI) instantly correlates rapidly evolving external threats with an organization's internal assets and exposure. Unlike generic feeds that only report external events, CTTI directly maps threats to an organization's assets and infrastructure, providing precise information about which threats affect its environment. Intel agents automatically link actors, TTPs, and IoCs to the organization's internal telemetry based on data sourced from over 1 million open, deep, and dark web sources

Key Findings

Sources of Information

- **77%** Open source or public CTI feeds
- **75%** Published intelligence reports
- **75%** Vendor threat feeds
- **69%** External sources (e.g., media reports and news)

AI Adoption and Uses

- **56%** Data summarization and report writing
- **46%** Data parsing, normalization, and information extraction
- **45%** Automation and workflow enhancements
- **28%** Threat and vulnerability prioritization and analysis

CTI Team Size

- **39%** have 2 or fewer full-time equivalents (FTE)
- **62%** have 4 or fewer FTE
- **73%** have 6 or fewer FTE

Agentic TI Ops

Dataminr's Agentic TI Ops collects, enriches, correlates, and structures millions of signals into a single unified threat library. Intel agents score relevance, route prioritized intelligence, and operationalize it directly into detection, prevention, and response across more than 200 native integrations. Multi-modal fusion AI minimizes human labor while preserving human judgment. Investigation insights overlay analyst workflows with relevant intel snippets in real time, delivering actionable intelligence inside existing workflows.

Predictive Threat Exposure Management

Dataminr's Predictive Threat Exposure Management (PTEM) leverages AI to provide real-time insights into emerging threats, helping organizations proactively mitigate risks. By analyzing vast amounts of publicly available data, PTEM detects control gaps as they occur, predicts where attackers are most likely to strike, and ranks vulnerabilities by probable financial impact. This enables teams to focus remediation on actions that reduce expected loss and improve cyber-risk outcomes.

Dataminr's Response to Critical Operational Challenges

Dataminr (see Figure 1) addresses several critical cybersecurity challenges identified in the 2026 SANS Cyber Threat Intelligence Survey.

The Collection Paradox

CTI quality reflects the sources behind it. This year, external media dropped to fourth place and social media fell from 65% to 49% as teams shifted toward higher-signal inputs: CTI-specific feeds (82%), published intel reports (76%), and vendor threat feeds (75%).

This trend aligns well with Dataminr for Cyber Defense's approach to UCRI. In most organizations, external intelligence, internal exposure, and business context live in separate tools, owned by separate teams. UCRI solves this by bringing together disparate data streams into a single, cohesive framework that can provide a clear, unified view of an organization's cybersecurity posture.

The Value-Influence Gap

91% of CISOs say CTI is valuable. Only 26% say it "significantly influences" their decisions. That gap isn't a data problem but a tooling problem. Decision makers need answers to three questions:

- What's our exposure?
- What does it cost?
- What's our next move?

Dataminr changes that paradigm by compressing detection-to-understanding from hours to seconds. It provides real-time correlation of threat intelligence with an organization's internal assets, infrastructure, and risk exposure. Continuous control monitoring with risk quantification translates the threat into probable financial impact and shows which actions reduce exposure the most.

AI Is Used for Describing Problems, Not Solving Them

AI adoption continues to rise, with 45% of respondents using AI in operations and another third planning adoption. However, the primary uses cited by respondents are summarization (56%), parsing (46%), and workflow automation (45%). Only 29% report using AI for threat and vulnerability prioritization and analysis.

Dataminr applies AI at the deciding layer—100-plus specialized intel agents running in parallel to prioritize threats—not at the describing layer the survey reports (summarization, parsing, automation). Dataminr for Cyber Defense's multi-modal AI analyzes text, images, audio, and video from over 1 million public sources to detect early signs of emerging threats. Agentic AI then correlates these signals with an organization's assets, vulnerabilities, and controls. By automating the intelligence life cycle and applying predictive risk modeling, Dataminr prioritizes threats based on likelihood and potential business impact, enabling faster and more informed security decisions.

Request a Demo

CTI has won the existence argument. The next decade belongs to programs that answer what's coming, what it costs, and what to do—at the speed the business runs.
Contact us for a demo today.

SOCRadar® Your Eyes Beyond

SANS | Research Program

PRODUCT BRIEFING

Your Eyes Beyond: SOCRadar Extended Threat Intelligence

Insights from 2026 SANS Cyber Threat Intelligence (CTI) Survey

May 2026

The 2026 SANS Cyber Threat Intelligence (CTI) Survey shows that threat intelligence has matured from a reactive, IoC-focused function into a core component of security strategy. The focus has shifted to proactive adversary analysis and anticipating threats *before* they materialize. As adoption grows, teams face new scaling challenges and evolving use cases, driving vendors to expand and innovate.

SOCRadar Extended Threat Intelligence

SOCRadar Extended Threat Intelligence (XTI) provides proactive threat detection and risk mitigation. It helps organizations monitor and analyze external threats, including data breaches, phishing campaigns, brand impersonation, and dark web activity. SOCRadar uses agentic AI agents and the Model Context Protocol to automate threat analysis, prioritize alarms, and integrate directly with leading large language models (LLMs). It integrates CTI, attack surface management, and digital risk protection into one platform, eliminating the need for separate vendors for external visibility and threat feeds. SOCRadar XTI supports security teams by combining five cybersecurity disciplines into a single, modular environment driven by AI automation.

Cyber Threat Intelligence (CTI)

SOCRadar's CTI module provides organizations with actionable insights from one of the industry's largest threat intelligence databases. It combines multiple modules (including threat hunting, vulnerability intelligence, and dark web monitoring) to help organizations detect risks early and respond effectively. SOCRadar CTI monitors dynamic changes and trends in the cyber threat landscape as well as threat actor behavior to provide tactical, operational, and strategic intelligence through a single platform.

Key Findings

Benefits of CTI

- **77%** Improving visibility into threats and attack methodologies impacting our environment
- **66%** Revealing gaps where new security measures should be implemented
- **63%** Detecting unknown threats
- **59%** Prioritization of efforts and resource utilization
- **58%** Reducing time to identify and respond to incidents

CTI Data Utilization

- **71%** Security operations and network defense
- **69%** Incident response
- **66%** Threat hunting/hypothesis generation
- **63%** Vulnerability management

AI Adoption and Uses

- **45%** Currently use AI, **32%** plan to use AI
- **56%** Data summarization and report writing
- **46%** Data parsing, normalization, and information extraction
- **45%** Automation and workflow enhancements

Attack Surface Management (ASM)

SOCRadar's Attack Surface Management module provides continuous discovery and monitoring of an organization's outward-facing digital footprint. Its external attack surface management advanced monitoring algorithms automatically discover and track vulnerable software, exposed assets, SSL certificates, DNS records, and shadow IT without manual inventory.

Advanced Dark Web Monitoring

The Dark Web Monitoring module continuously tracks over 10,000 dark web, deep web, and surface web forums and marketplaces to detect any mentions of an organization. It flags data breaches, PII exposures, stolen credentials, underground chatter, ransomware activity, and VIP information. Real-time alerts include source details, while a searchable dark web engine lets users query the database for keywords, IoC, and curated industry- or country-specific news feeds.

Brand Protection

SOCRadar's Brand Protection module monitors the web, social media platforms, deep web, and dark web 24/7 to identify brand impersonation, phishing domains, rogue mobile apps, fraudulent social media accounts, and unauthorized use of intellectual property. It uses AI-powered workflows with specialized agents for logo similarity analysis, OCR text recognition, and website content inspection.

Supply Chain Intelligence

SOCRadar's Supply Chain Intelligence module continuously evaluates the security posture of an organization's entire supply network. Powered by SOCRadar's database of over 50 million vendor organizations, it integrates CTI, digital risk protection, and ASM to provide a complete 360-degree view of third-party risks.

SOCRadar's Response to Critical Operational Challenges

SOCRadar (see Figure 1) addresses several critical cybersecurity challenges identified in the 2026 SANS CTI Survey.

The Shift from AI Hype to Operational Utility

The 2026 CISO survey confirms CTI has reached executive-level legitimacy: 91% of CISOs rate it as valuable, and nearly half are already using AI in their CTI programs for summarization, reporting, and workflow automation. SOCRadar is built for exactly this moment. Security teams are drowning in high-volume, low-context alerts, and a global talent shortage means analysts can't keep up. SOCRadar's MCP Server tackles this directly, connecting industry-standard LLMs to the SOCRadar platform to embed intelligence into existing workflows via automated queries, real-time enrichment, and AI-driven analysis. The SOCRadar XTI then correlates that intelligence with IoC data to prioritize threats by impact, accelerating triage and cutting manual effort. The goal throughout: AI as a force multiplier, with humans staying in the loop.

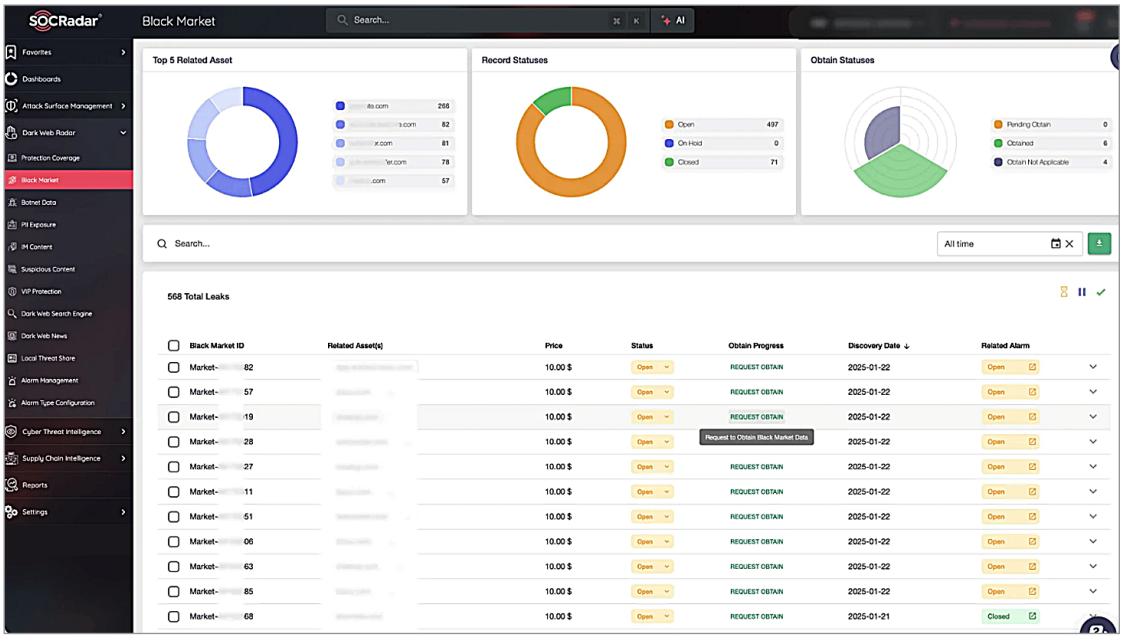


Figure 1. SOCRadar Dashboard

The Scaling Paradox: Small Teams vs. Expanding Scopes

90% of surveyed organizations have dedicated CTI resources, but teams stay small, with 60% having four or fewer FTEs. With skills shortages and tightening budgets, CTI functions are stretched thin. Tools must do more of the heavy lifting.

SOCRadar XTI addresses this directly as a single platform covering the full threat life cycle. It eliminates the context-switching tax of juggling disparate tools and lets small teams operate with the reach of a much larger department. AI-driven automation combined with human validation cuts false positives and reduces manual effort, shifting teams from reactive response to proactive risk management.

Request a Demo: See CTI in Action

Want to learn more about SOCRadar's powerful, easy-to-use platform designed to detect threats, monitor your external attack surface, and stop breaches before they happen? [Contact us for a demo today.]