



JAN. 2026

# 2026 CTI Practitioners Roundup

14 CTI perspectives on threats, workflows, and measuring success in 2026



# Table of Contents

|                                                         |           |
|---------------------------------------------------------|-----------|
| <b>Introduction</b>                                     | <b>03</b> |
| <b>Executive Summary</b>                                | <b>05</b> |
| <b>2026 Threat Forecast</b>                             | <b>06</b> |
| Attackers targeting valid credentials for IdPs and SaaS | 06        |
| Supply chain risk will increase in impact and severity  | 07        |
| AI makes existing attacks faster and cheaper            | 08        |
| <b>Workflow to Prioritize in 2026</b>                   | <b>10</b> |
| Build audience ID into intel production process         | 10        |
| CTI should reduce risk, not just monitor                | 11        |
| Solidify and speed up the intel cycle fundamentals      | 13        |
| <b>Under-Discussed or Overhyped?</b>                    | <b>14</b> |
| <b>Measuring Program Success</b>                        | <b>16</b> |
| What CTI teams can stop doing in 2026                   | 17        |
| How to operationalize these metrics                     | 18        |
| <b>Conclusion</b>                                       | <b>20</b> |
| <b>Meet Our Contributors</b>                            | <b>21</b> |



# Introduction

The end of the year gave CTI teams a moment to catch our breath before jumping back into the trenches. So, how do you prioritize what actually matters in this new year?

To cut through the noise, we surveyed **14 seasoned CTI practitioners** and leaders across industry, asking them to share their perspectives on four areas:

- **Q1:** What will be the most significant threat or risk in 2026?
- **Q2:** What workflow or process should CTI teams prioritize in 2026?
- **Q3:** What topic in CTI is either under-discussed or overhyped?
- **Q4:** What single metric best measures CTI program success?

## Who did we talk to?

The practitioners represent a cross-section of intelligence community: threat intelligence leads at large enterprises, independent researchers, former government analysts, and practitioners building CTI programs from the ground up. Their perspectives don't always align, and we've preserved that disagreement where it exists. But on several critical points, there was strong convergence.

Special thanks to the following participants for sharing their insights:

Paul McCarty, A. Stryker, John E. Stoner, Sam Flockhart, Adam Goss, Will Thomas, Freddy Murre, Sean O'Connor, Paul Prouse, Thomas Roccia, Ondra Rojčík, Mary D'Angelo, Marcelle Lee, Rebekah Brown

For bios, see the end of the report.

## How we made this report actionable

Practitioner roundups often deliver insight without application. You finish reading, think "interesting," and return to work unchanged. We built this guide with action in mind.

- 1. Themes + quotes.** We grouped 14 practitioners' responses into themes so you can see where the field agrees, disagrees, and why it matters. Direct quotes are preserved so you can assess the reasoning yourself.
- 2. How-to-action guidance.** We've provided two bullet points per theme on how to action or address the practitioners recommendations in Q1 and Q2.
- 3. Identified what you can stop doing.** We synthesized the practitioner's feedback on what is overhyped (Q3) into a list of items you can stop doing in 2026, saving yourself time and effort.
- 4. Metrics + how to implement.** The success metrics section (Q4) includes concrete steps to help you action the recommendations to move from activity tracking to outcome measurement.

## A warning for every analyst:

"Beyond the direct technical threats, there is a significant impact on the analyst's mindset. We need to remain adaptive as attacker behaviors change, all while operating under high stress. In these stressful situations, the brain wants to take shortcuts and fall back on assumptions and cognitive biases, which can make it harder to defend against these attacks. Staying mentally flexible and applying analytic rigor in these high-stress, dynamic situations is going to continue to be a challenge in 2026."



**Rebekah Brown**

Senior Researcher and SANS Instructor



# Executive Summary

Across 14 practitioner responses, several patterns emerged with unusual consistency.

## **Threats: Identity-centric attacks against SaaS platforms will dominate the 2026 landscape.**

- Attackers won't break through perimeters; they'll walk through the front door with valid credentials obtained from infostealers, access brokers, and social engineering.
- Supply chain risk surfaced as the second major theme, but practitioners forecast there will be a shift from it being a single attack category, to a systemic condition spanning more vendors, open-source dependencies, and AI-assisted development pipelines.

## **Workflows: Practitioners recommended prioritizing workflows that mature CTI programs from passive monitoring to active risk reduction**

- Stakeholder-centric communication, proactive exposure management, and disciplined threat hunting emerged as the workflows that separate programs that matter from programs that just generate reports.

## **Hype vs. under-discussed: The consensus about AI was striking.**

- AI threats are consuming disproportionate attention relative to their observed operational impact.
- Six practitioners explicitly called out AI threat narratives as overhyped, while seven identified fundamental capabilities (data engineering, HUMINT tradecraft, supply chain visibility, human factors) as neglected.

## **Measurement: Practitioners rejected activity metrics almost universally.**

- Report counts, IOC volume, and presentations delivered were dismissed as vanity metrics.
- Instead, practitioners converged on outcome-driven measures: decisions influenced, controls implemented, and time from intelligence to action. If you can't tie your metric to something that changed, you're measuring the wrong thing.

# 2026 Threat Forecast

**Q1: What do you forecast will be the most significant threat or risk in 2026?**

## **Theme 1: Attackers targeting valid credentials for IdPs and SaaS**

Attackers will increasingly bypass conventional security controls by obtaining valid credentials through infostealers, access brokers, and social engineering, then directly access identity providers (IdPs) and Software-as-a-Service (SaaS) platforms before pivoting into their customers' environments and data. They will likely leverage new techniques to bypass MFA or simply target accounts lacking MFA. These intrusions often look indistinguishable from legitimate user activity, making detection significantly harder.

### **Practitioner Quotes:**

**Sean O'Connor:** "The biggest risk in 2026 will be identity and SaaS compromise at scale, fueled by infostealer logs, access brokers, and AI-assisted social engineering. Once attackers get valid credentials or sessions, they walk straight into IdPs and business-critical SaaS like Salesforce or Snowflake, often looking like normal users. Overprivileged accounts, weak tenant configs, and poor monitoring of 'legitimate' logins turn identity into the primary attack surface, with data theft and extortion as the default outcome."

**William Thomas:** "Software-as-a-Service (SaaS) applications and platforms. Throughout 2025 we observed several major incidents involving platforms such as Salesforce, Salesloft, and GainSight. Despite 2FA/MFA being available, adversaries have developed new techniques to evade controls, such as voice phishing (aka vishing) and bulk data exfiltration tools."

**Adam Goss:** "Pure extortion attacks targeting SaaS applications. Unlike traditional ransomware that requires sophisticated encryption capabilities, these attacks leverage stolen credentials or API vulnerabilities to threaten data deletion or exposure. This is a dramatically lower barrier to entry for threat actors. The success of this tactic in 2025 (e.g., Snowflake, M&S, etc.) demonstrated that organizations often pay ransoms even without encryption."

## How CTI teams can address this

- **Operationalize exposure monitoring against underground sources.** Continuously hunt for your credentials, tokens, and session data in infostealer logs and access broker ads. Map indicators to specific accounts, privilege levels, and SaaS tenants, then drive immediate remediation: key rotation, session kills, revoke VPN session, reset password, reset MFA, etc.
- **Pivot collection from network IOCs to identity and SaaS telemetry.** Track infostealer malware campaigns, MFA bypass techniques, and access broker pricing trends. Correlate with internal signals: anomalous auth patterns, API abuse, bulk data access, and cross-tenant activity from residential IP ranges that traditional blocklists miss.

## Theme 2: Supply chain risk will increase in impact and severity

As organizations grow more dependent on third-party vendors, open-source software, and AI-driven development pipelines, supplier disruptions will increasingly cascade into widespread operational impact. Contractual risk transfer will do little to mitigate the real consequences of disruption, data loss, or downtime.

### Practitioner Quotes:

**Sam Flockhart:** "2026 could be the year we pay the price for our lack of control over the Software Supply Chain. Shai-Hulud, Glassworm and continued attacks against npm in 2025 have proved suitable warnings that should frighten cyber security teams into action."

**A. Stryker:** "Procurement teams have grandfathered vendors embedded into current processes without requiring updated control audits. And leadership likes to 'transfer risk': because the vendor claimed XYZ on the paperwork, it won't be the org's fault if a vendor fails to keep their own claimed controls and a breach happens. But for security personnel, it's still a breach they couldn't stop; and for organizations, it's still downtime, data loss, and long-term costs."

**Freddy Murre:** "Threat actors deliberately or by accident take down internet access of dependencies in the supply chain, rendering large portions offline for an extended time."



**Marcelle Lee:** "While AI has generated plenty of buzz, the reality is that supply chain attacks have emerged as one of the foremost challenges in today's cyber threat landscape. [...] Consider the numerous companies impacted by the Salesloft breach."

## How CTI teams can address this

- **Build and maintain supplier risk profiles for critical vendors.** Identify your organization's highest-impact dependencies, then actively monitor for breach disclosures, dark web mentions, and infrastructure compromises affecting those suppliers. Feed findings into vendor risk assessments and trigger re-evaluation of access permissions when a supplier threat materializes.
- **Implement malicious package detection for software dependencies.** EDR and traditional AppSec tooling (SAST/SCA) don't cover this gap. Deploy dedicated threat feeds and endpoint protections that detect malicious content at install time across npm, PyPI, and other package ecosystems your developers pull from.

## Theme 3: AI makes existing attacks faster and cheaper, not fundamentally new

AI is not creating fundamentally new attack types, but it will make existing tradecraft faster, cheaper, and more scalable. Social engineering will become more sophisticated and convincing at every tier, from commodity BEC scams to nation-state targeted operations. The proliferation of Shadow AI will simultaneously expand the attack surface.

### Practitioner Quotes:

**Thomas Roccia:** "Offensive automation will keep improving. In 2025, we saw early malware experiments leveraging LLMs and offensive frameworks built around agent orchestration. Most were still experimental, but they clearly show that attackers, like the wider industry, are moving in this direction. With more AI adoption, the attack surface will likely increase."

**John Stoner:** "The proliferation of more sophisticated and convincing social engineering schemes across the board. From low-level criminal BEC scams to sophisticated APT-level targeted social engineering operations. The AI tools have already allowed a significant increase in quality and quantity of these types of operations, so I see no reason why this won't continue to be a huge problem."

**Mary D'Angelo:** "The biggest risk we're likely to see expand in 2026 is artificial intelligence, while the most significant threat is the reshaping of the cybercriminal ecosystem by groups such as Scattered Lapsus\$ Hunters through evolved tradecraft, including insider recruitment and acting as an operational shield for other cybercriminal groups."

**Ondra Rojcik:** "'AI' is a 'bit' played out, but honestly, there's no way around it. It just makes things so much more efficient for the bad guys. Attackers will weaponize autonomous agents and GenAI to massively scale social engineering, think hyper-realistic deepfakes, and automate entire campaigns."

**Sam Flockhart:** "Defenders will once again be on the back foot as the mass roll out of Large Language Models (LLMs) will rapidly expand the attack surface alongside Shadow AI. The maturity of security controls will struggle to catch up with the rapid expansion of Prompt Injection attacks."

## How CTI teams can address this

- **Track AI-enabled tradecraft evolution, not hypothetical capabilities.** Monitor how threat actors actually use LLMs and automation in the wild: improved phishing lure quality, faster exploit development, deepfake-assisted vishing, and agent-based attack frameworks. Focus collection on observed TTPs rather than speculative "agentic AI" scenarios that haven't materialized at scale.
- **Inventory and monitor your organization's AI attack surface.** Coordinate with security and IT teams to identify Shadow AI deployments, LLM integrations, and AI pipelines. Assess exposure to prompt injection, data poisoning, and model abuse. CTI should treat AI infrastructure as a distinct asset class requiring dedicated visibility.

# Workflow to Prioritize in 2026?

## Q2: What workflow or process should CTI teams prioritize in 2026?

### Theme 1: Build audience identification into intelligence production process

Intelligence products fail when they're designed for the analyst rather than the consumer. Practitioners emphasized that audience identification should shape collection, analysis, and delivery from the start, not get retrofitted during editing. The core problem: CTI teams routinely produce outputs optimized to demonstrate analytical rigor rather than drive action.

#### Practitioner Quotes:

**A. Stryker:** "Reporting differentiation. Don't give the same report format or even information to your execs that you would to your operations team and expect it to be equally effective. It won't be. Either you care enough about something to report it, and so you format it in a way that makes it most likely to do something, or you don't. If the latter, spend your time doing something that will actually make your organization more secure... And that will actually get used... A whitepaper with a page-long summary and your entire thought process on how you came to your conclusions and recommendations is written for yourself to feel smart, not to actually help your org stay secure."

**Paul Prouse:** "Communication skills link collection and analysis back to the customer. All our good work is undone without effective communication."

**Freddy Murre:** "They should adapt AIMS (Audience, Intel Req, Message, and Storyline) at the beginning of analysis and when designing the finished product/presentation. Easy way to ensure you're delivering value to those that matter."

**John Stoner:** "Teams should be making sure the process of developing priorities and engaging stakeholders is done. We are seeing a lot of AI threat hype and FUD right now, and that is driving a lot of questions from senior leadership and senior stakeholders. Teams should be proactive to ensure cybersecurity messaging up the leadership chain is focused on threats to the organization. They should also proactively review any intelligence requirements and make sure stakeholders feel engaged."

## How CTI teams can action this

- **Apply the AIMS framework (Audience, Intelligence Requirement, Message, Storyline) before analysis begins.** Define who will consume the product and what decision it should enable upfront. This determines scope, depth, format, and delivery channel. A SOC analyst needs different content than a CISO, and retrofitting a technical deep-dive into an executive summary wastes effort and reduces impact.
- **Create differentiated product templates for each stakeholder tier.** Build separate formats for executives (decision-focused, business impact), security operations (actionable, detection-oriented), and technical teams (detailed TTPs, IOCs). Route intelligence to the right template based on the requirement it answers, not based on what the analyst finds interesting.

## Theme 2: CTI should actively reduce risk, not just monitor

CTI should evolve from passive reporting to actively participating in reducing exposure before incidents occur. Multiple practitioners described workflows in which CTI should directly inform hunting, detection engineering, and control adjustments, to close the gap between external threat awareness and the internal defensive posture.

### Practitioner Quotes:

**Sean O'Connor:** "CTI teams should prioritize a formal exposure-monitoring workflow that links underground visibility to specific identities, SaaS tenants, and vendors. That means continuously hunting for our accounts, tokens, and data in infostealer logs and access broker ads, mapping each hit to owners and privileges, and driving fast actions: key rotation, session kills, access changes. This is how CTI moves from 'reporting on threats' to systematically reducing real exposure in identity and SaaS."



**William Thomas:** "I assess that CTI teams should prioritize enriching network telemetry and monitor their edge devices and SaaS applications. Adversaries are continuously looking for an initial access vector into target organisation networks and will be probing using network-based interactions, reconnaissance, and exploitation attempts. Therefore, it is important to understand where network traffic is coming from and leaving to. Device exploitation, account takeovers, and data exfiltration all must involve network telemetry that can be enriched with intelligence (such as knowing which IPs are VPNs, Proxies, Scanners, and C2 servers) to detect and prevent such threats."

**Paul McCarty:** "Gaining visibility into software supply chain threats and specifically, implementing a malicious package detection capability for their org. EDR doesn't cover this, and appsec tooling like SAST/SCA doesn't cover this, so specific threat feeds and endpoint protections are required."

## How CTI teams can action this

- **Establish a closed-loop exposure remediation workflow.** When you identify compromised credentials, leaked tokens, or organizational data in underground sources, route findings directly to asset owners with specific remediation actions (rotate keys, kill sessions, revoke access). Track time-to-detect (e.g., time from compromised credential found to assets owner/remediation team notified) as a core CTI metric rather than just logging the finding.
- **Embed CTI outputs into detection and control processes.** Feed threat intelligence directly into detection engineering (new rules, updated signatures), network telemetry enrichment (tagging traffic against known C2, proxies, scanners), and control adjustments (blocking malicious packages, tightening SaaS configs). If your intelligence doesn't change a detection or control, question whether it needed to be produced.

## Theme 3: Solidify and speed up the intel cycle fundamentals

Without strong prioritization, clear requirements, and fast feedback loops, teams risk allocating time to low-value signals while missing what matters most. Rather than chasing every emerging trend, practitioners urged CTI leaders to anchor workflows in the intelligence cycle and continuously evaluate how new tools improve or degrade analytical rigor and speed to action.

### Practitioner Quotes:

**Rebekah Brown:** "How their organizations adopt new technologies. As teams continue to roll out AI tools, automation platforms, and new SaaS services, often in an ad hoc manner, CTI teams need to understand what's being deployed, how it will be used, and what access it introduces. This is especially important given how many third-party platforms and integrations can quickly expand the attack surface and provide new paths into core systems. Attackers are aware of this and are targeting these weaknesses, and when that happens, CTI teams should already have the context they need to quickly determine whether they are exposed and what data or systems could be at risk."

**Thomas Roccia:** "CTI teams should stop reacting to trends and focus on sorting noise from the real signal. The goal should be tailored and predictive threat intelligence, not generic reporting. Teams need to speed up analysis and reaction. Faster loops between collection, assessment, and action will matter more than volume. With AI advancement, it generates more data, more alerts, and more false positives. The ability to separate true threats from misleading or low-value signals will become even more important for CTI teams."

**Paul Prouse:** "In 2026, prioritise the intelligence cycle - master the basics. There will be new tools, new techniques, and the lingering question over harnessing AI while mitigating its risks. The intelligence cycle is the fundamental workflow of intelligence practice. It has endured technological revolutions and many threat landscape changes. Two questions to ask with new tools and workflows: 'how does it fit into the intelligence cycle,' followed by 'what do I gain and what do I lose?'"

## How CTI teams can action this

- **Measure and reduce cycle time from collection to action.** Track how long it takes for data collection to result in a concrete outcome (detection rule, block, policy change, stakeholder decision). Identify bottlenecks in the process, whether in collection gaps, analysis time, or stakeholder dissemination, and systematically eliminate them.
- **Evaluate every new tool against the intelligence cycle.** Before adopting AI tools, automation platforms, or new feeds, ask two questions: where does this fit in the cycle (collection, processing, analysis, dissemination)? And what do we gain versus lose in rigor, speed, or analyst judgment? Tools that accelerate low-value work or generate noise without improving decisions aren't worth the integration cost.

# Under-Discussed or Overhyped?

## Q3: What topic in CTI is either under-discussed or overhyped?

The pattern is clear. Practitioners overwhelmingly view AI threats as overhyped while fundamental technical and human capabilities remain neglected:

- **CTI attention is misaligned with impact.** Foundational gaps (supply chain visibility, infrastructure evolution) are under-resourced, while speculative AI narratives dominate discussion.
- **AI is an accelerant, not a revolution.** Most practitioners see AI making existing threats faster and noisier, not fundamentally changing attacker capabilities.
- **Basics are being skipped.** Teams are discussing advanced AI threats without first solving visibility, sourcing, and human-factor problems that already drive compromise.

| Under-discussed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Overhyped                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Software package threats and supply chain visibility</b> "Most orgs have no visibility into software package based threats. Infosec counts on EDR to gain visibility into the developers laptop, but if EDR provides no protection against software package based threats from NPM, PyPI, etc, then how do they gain that visibility?" — <i>Paul McCarty</i>                                                                                                                                              | <b>Gen AI / AI threats</b> "Gen AI. It's over discussed without going through the basics. It's because threat analysts get bored of the same things, so they want the new shiny to pursue. I get it. But damn, we're all so enamored with what's <i>possible</i> , that we're ignoring very real basic issues right now!" — <i>A. Stryker</i>                                                                                                             |
| <b>The death of IOCs due to Operational Relay Box (ORB) networks.</b> "These are compromised SOHO devices that have been added to a customized Tor anonymization network used specifically by Chinese state-sponsored threat groups... ORB network IPs will appear like normal residential IP addresses in network logs and blocking them all is impossible due to the constant rotation." — <i>William Thomas</i>                                                                                           | <b>AI adoption that harms intelligence quality</b> "The widespread adoption of AI that, in many cases, does not enhance the quality of threat intelligence and, in some cases, even harms it. Poorly configured or inadequately trained models often generate excessive false positives, contributing to alert fatigue, or produce irrelevant and low-confidence outputs." — <i>Mary D'Angelo</i>                                                         |
| <b>HUMINT in cybercrime ecosystems</b> "Disciplined HUMINT in cybercrime ecosystems, evaluating source reliability, managing long-term adversarial relationships, and spotting manipulation, all inside clear legal and ethical boundaries. Most teams talk about 'dark web monitoring,' but not about real source handling." — <i>Sean O'Connor</i>                                                                                                                                                         | <b>Generic "AI + CTI" stories</b> "Generic 'AI + CTI' stories that rebrand enrichment and summarization as breakthroughs. AI helps, but it doesn't replace good collection, requirements, source vetting, and stakeholder relationships." — <i>Sean O'Connor</i>                                                                                                                                                                                          |
| <b>Human factors in CTI</b> "CTI must broaden its scope to include both systems and their users... Deliberate cultivation of a user to gain system access is different to an employee unwittingly clicking a malicious link. This insider threat requires different types of threat intelligence and mitigation. Understanding why people turn focuses on understanding human behaviour, starting with the four traditional motivations – money, ideology, compromise, and excitement." — <i>Paul Prouse</i> | <b>AI threat reports and "agentic attacks"</b> "Most of the AI threat reports going around right now are massively overhyped, and they're pulling defenders' attention away from the things that actually matter. We keep hearing breathless narratives about 'AI agentic attacks,' 'autonomous malware,' and 'world-changing offensive capabilities.'... There is zero evidence of fully autonomous AI attacks happening at scale!" — <i>John Stoner</i> |
| <b>Visibility into how threat actors leverage AI systems</b> "Visibility into how threat actors leverage AI systems... Most discussions focus on using AI for CTI. Very few focus on how to detect, investigate, and respond when AI systems are compromised. CTI needs an additional layer that covers AI assets, AI pipelines, and AI specific abuse." — <i>Thomas Roccia</i>                                                                                                                              | <b>AI-enabled attacks</b> "AI-enabled attacks are getting more attention than they should, distracting from more important concerns. Yes, threat actors are using AI and so are defenders. I'm not seeing anything particularly game changing on either side." — <i>Marcelle Lee</i>                                                                                                                                                                      |



# Measuring Program Success

## Q4: What single metric best measures CTI program success?

The practitioners we surveyed rejected traditional activity metrics like report counts or IOC volume. Instead, they converged on outcome-driven measures that answer one question: did the intelligence change anything?

### Consumption & Demand

- **Engagement signals:** "If you hear nothing back from your regular products and communications, then there is something extremely wrong with your intel distribution." – A. Stryker
- **Number of people informed:** "How many people were more informed about threats and how to protect themselves based on the work of the CTI program?" – Rebekah Brown
- **Ratio of proactive deliverables:** "Don't just answer questions in email without metrics; if you are putting serialization numbers into products, consider RFIs a serialized product to help track." – John Stoner

### Decision Support

- **Decisions made by stakeholders based on CTI:** "Only true way to see impact and demonstrate value to stakeholders." – Freddy Murre
- **Material risk decisions driven by CTI:** "Reports, IOCs, and dashboards are activity metrics; they don't prove impact. Counting meaningful decisions and control changes forces CTI to stay focused on changing outcomes." – Sean O'Connor
- **Threat-Driven Security Improvements:** "This is your end-to-end actionable threat management: transforming threat intelligence through the 'So What?' phase into actions that mitigate or remediate the threat." – Sam Flockhart



## Defensive Change

- **Ratio of proactive deliverables vs. RFIs:** "A high proactive ratio demonstrates the CTI team is on top of events and anticipates needs."  
– Ondra Rojcik
- **Package security coverage:** "How many packages do your engineers install per day, per month, per year, and what percentage of those are checked for malicious content?" – Paul McCarty
- **Time from intelligence to action:** "If intelligence does not change anything, it has no value; tracking how fast intelligence turns into action is the clearest indicator that a CTI program is effective." – Thomas Roccia
- **New controls tied to PIRs:** "Number of new controls introduced, which can be tied to specific PIRs of internal stakeholders." – William Thomas

## What CTI teams can stop doing in 2026

Based on CTI practitioners' input, there are multiple areas CTI teams can stop spending time on, enabling them to reallocate resources to the threats, workflows, and success metrics flagged in this report. Items you can stop doing include:

- Writing polished reports optimized for analytical rigor instead of stakeholder action
- Giving executives the same report format you give to the operational team
- Tracking report counts, IOC volume, or presentations delivered as success metrics
- Briefing stakeholders on AI threat narratives that lack evidence of real-world impact against your industry
- Chasing every emerging trend instead of working from intelligence requirements developed with stakeholders

## How to operationalize these metrics

The metrics above fall into three categories: engagement (are stakeholders consuming intelligence?), impact (did the intelligence change anything?), and speed (how quickly does intelligence turn into action?). Pick one category based on where your program has the least visibility.

### If you don't know whether stakeholders read your products:

- 1. Add a response prompt to every deliverable.** End reports with a specific question: "Does this change your assessment of X?" or "Does this change how you will action Y?" Track who responds and who doesn't. Silence from a stakeholder for 30+ days indicates something is not working, e.g., intel relevance, feedback mechanism friction, or dissemination format.
- 2. Check-ins after each RFI.** Create a simple log (spreadsheet is fine) with: request date, requester name and team, question asked, response date, and a field for "what action taken" that you fill in 7 days later (see below). If you're getting zero RFIs, your stakeholders either don't know you exist or don't trust you enough to ask.

### If stakeholders engage, but you can't prove impact:

- 1. Add a 7-day follow-up step to your workflow.** After delivering intelligence, the analyst is responsible for doing a check-in to ask: "Did this result in any action?" Document the answer even when it's "no"; patterns in non-action are useful feedback. Track the responses for both reactive intel (e.g., provided after RFI) vs proactive intel (e.g., CTI initiating informing stakeholder).
- 2. Partner with one stakeholder team to pilot impact tracking.** Start the shift to measuring impact metrics by picking the stakeholder most likely to cooperate (often vulnerability management, incident response or the SOC) and build a shared tracker: threat, date, intel delivered, action recommended, action taken. Expand after you have a working model.
- 3. Map controls back to intelligence after the fact.** Once per quarter, review new detection rules, policy changes, or vendor decisions with the relevant stakeholders. Ask "what influenced this?" Document the ones CTI has an influence on.

## If you want to measure speed:

1. Analyze 5 intelligence products per month. Track four timestamps for each: new threat detected/RFI request made/intel cycle kickoff, when you finished collection, when analysis was complete, and when you delivered to the stakeholder. The gaps between these timestamps tell you where your intel production cycle is slow. E.g., if collection-to-analysis is your bottleneck, that's likely a tooling, process, or staffing problem. If analysis-to-dissemination is slow, you're likely over-editing.

## What to do when you can't get the data:

The challenge with outcome metrics is that CTI teams often don't have much visibility into what stakeholders do. If you can't get outcome data directly:

- **Use proxy signals.** Was the intelligence referenced in an incident report? Did the stakeholder forward it to their team? Did it show up in a risk register or board briefing?
- **Negotiate access during PIR collection.** When you meet with stakeholders to collect their intelligence requirements, ask in what forum decisions are made or recorded, and ask if you can have access (e.g. sit in on operational weekly meetings, access to detection engineering backlog database). Make specific asks.
- **Accept that some impact will be harder to quantify.** Not every decision gets documented. Qualitative feedback ("your report on X changed how we think about Y") counts and should be recorded, even if you can't put it in a dashboard.

# Conclusion

The 14 CTI practitioners featured in this roundup provided clear, experience-backed guidance on the threats, workflows, focus areas, and metrics that will define effective CTI programs in 2026. Taken together, their responses indicate CTI is still grappling with a core problem: the gap between what CTI teams produce and what actually impacts security outcomes. Increasing your value requires addressing this gap.

## How to action these insights

For teams looking to translate this report into action, the practitioners in this roundup suggest a pragmatic starting point:

### **1. Audit your intelligence coverage against threats flagged by the 14 practitioners.**

Assess your visibility into infostealer logs, stolen credentials, or initial access broker activity. Do we monitor our SaaS tenants for anomalous OAuth grants or session token abuse? What's our actual coverage of open-source dependencies in production code? If you aren't monitoring these, you've found gaps you can work on closing.

### **2. Choose one workflow to improve this quarter.**

Review the workflows recommended in this report (Q2), select one that your team doesn't do or you know could be improved, and create a project to work on it. If you were surprised by any of the recommended workflows, that's an indication you should explore how they could improve your CTI program.

### **3. Stop one thing that isn't working.**

Multiple practitioners emphasized that CTI teams need to stop doing low-value work, not just add new initiatives. Check out the list under the metrics list in Q4. Identify a recurring deliverable that nobody acts on and retire it. The time you reclaim can be used to start tracking a new outcome-driven metric.

These steps will not transform a CTI program overnight. Aligning with what these practitioners recommended will take time, but it's worth the investment. In the months ahead, the question is no longer whether CTI teams will produce more intelligence, but whether that intelligence will make a measurable impact by reducing risk, avoiding cost, or protecting the organization.

# Meet Our Contributors



**Paul McCarty**

Founder of OpenSourceMalware  
and Head of Research at Safety

- Founded multiple startups in the '90s and worked with NASA, Boeing, Blue Cross/Blue Shield, John Deere, the U.S. military, and the Australian government.
- Founder and maintainer of OpenSourceMalware.com, an open database and collaboration platform for software supply chain threat intelligence.
- Head of Research at Safety (safetycli.com) and a DevSecOps OG.



**A.Stryker**

Director of Threat Analysis  
at Fable Security

- Threat intelligence analyst who triages technical findings and qualitative intelligence into organizational impacts for teams looking to prove the why - not just the what - behind budget requests and strategic plans.
- Presents at industry conferences and get-togethers, plays Backdoors and Breaches, and engages across the community to discuss why contextualized threat intelligence matters for organizations big and small.
- Focuses on evaluating the actual risk and business impact of a given threat, beyond surface-level indicators.



**John E. Stoner**

Cybersecurity Consultant & Instructor

- Cybersecurity professional with over 25 years of experience, including a decade in the U.S. Army specializing in Signals Intelligence (SIGINT) and 15 years focused on Cyber Threat Intelligence (CTI).
- Supported missions across the U.S. Government and commercial sectors, including work at NSA, CSE, CISA, and the DoD Cyber Crime Center (DC3).
- Volunteers extensively in the cybersecurity community and serves as Vice President of VetSec, supporting military veterans transitioning into cybersecurity careers.



**Sam Flockhart**

Head of Cyber Threat Management  
at Santander UK

- A former Military Intelligence Operator, serving 9 years in the British Army on operational deployment across the world including Beijing, Eastern Europe and the Middle East.
- Highly experienced in leading intelligence operations from the strategic to tactical, moving from analyst to leader, adapting from the kinetic space to cyber.
- Passionate Geopolitical and Russia focused Threat Analyst with experience advising the highest level of political and military leaders.



**Adam Goss**

CEO and Founder of Kraven Security

- Founder of Kraven Security, providing accessible education and consulting services in Cyber Threat Intelligence (CTI).
- Develops and delivers affordable CTI training and bespoke consulting to help organizations improve security capabilities, drawing on experience across MSSPs, telecommunications, and digital service providers.
- Actively creates and shares expert content on CTI, threat hunting, and custom tooling across X, LinkedIn, and YouTube.



**Will Thomas**

Senior Threat Intelligence Advisor  
at Team Cymru

- Senior Threat Intelligence Advisor for Team Cymru.
- Co-author of the SANS FOR589 Cybercrime class and co-founder of Curated Intelligence.
- Public speaker who has delivered talks at DEFCON, Sleuthcon, Underground Economy, and BSides London.



# Meet Our Contributors



## Freddy Murre

Senior Threat Intelligence Analyst  
at Nordic Financial CERT

- Intelligence professional with more than 13 years of practical experience across military and private sectors; prolific speaker on intelligence methodology, tradecraft, CTI, and how AI may change intelligence analysis.
- CEO, founder, and lead instructor at Intelligence Tradecraft; senior advisor of threat intelligence at Nordic Financial CERT (NFCERT); and PhD candidate at the Norwegian University of Science and Technology (NTNU).
- Ambassador for applying intelligence methodology and rigor to cyber threat intelligence, sharing research, articles, and PhD work with the community via LinkedIn.



## Thomas Roccia

Threat Researcher

- Threat Researcher with over a decade of frontline cybersecurity experience, handling major cyberattacks, leading critical investigations, and speaking at top security conferences worldwide.
- Founder of multiple open-source projects including the Unprotect Project, YaraToolkit, DocYara, and NOVA, with contributions across open-source initiatives and actionable research shared through detailed Jupyter notebooks.
- Early adopter of generative AI for threat intelligence, creator of real-world applications and the first advanced training in this field taught at BlackHat; author of Visual Threat Intelligence (2023), an international bestseller and Bronze Foreword INDIES Award winner.



## Sean O'Connor

Senior Manager, Information Security

- Information security leader with over 15 years of experience across private and public sectors.
- Global Head of the Equinix Threat Analysis Center (ETAC)™, leading a team that identifies and analyzes emerging threats and develops countermeasures to protect Equinix and its customers.
- SANS author and instructor for the FOR589: Cybercrime Intelligence course; frequent conference speaker who is passionate about volunteering and mentoring students and veterans entering cybersecurity.



## Ondra Rojčík

Principal Cyber Threat Intelligence  
Analyst at Red Hat

- Cyber Threat Intelligence professional with extensive experience in intelligence analysis, strategic assessments, and risk evaluation.
- Proven track record of establishing and leading successful CTI programs, providing insight into complex threats and guiding intelligence production across business organizations, NATO, and the Czech Republic's government sector.
- Passionate about mentoring future threat intelligence analysts through specialized courses and cultivating partnerships with internal teams, government agencies, and international partners.



## Paul Prouse

Owner, Astro Intelligence

- Founded Astro Intelligence in 2022 to help managers get more value from their intelligence systems through training and capability design.
- Led initiatives including the Practitioner's Handbook for the New Zealand Institute of Intelligence Professionals and New Zealand's only Intelligence Leadership Programme.
- Brings 20 years of military intelligence and operations experience, including senior leadership and instructor roles within New Zealand Defence.



## Mary D'Angelo

Cyber Threat Intelligence Solutions  
Lead at Filigran

- Cyber Threat Intelligence Solutions Lead for Filigran, helping organizations build practical threat intelligence programs and get real value out of OpenCTI.
- Writes about dark web intelligence and real-world threat activity, contributes to industry content, and has been featured on cybersecurity podcasts.
- Active advocate for Women in CTI, helping grow representation, community, and opportunities in the threat intelligence space; experienced presenter for technical and leadership audiences.

# Meet Our Contributors



**Marcelle Lee**

Cybersecurity consultant  
and researcher

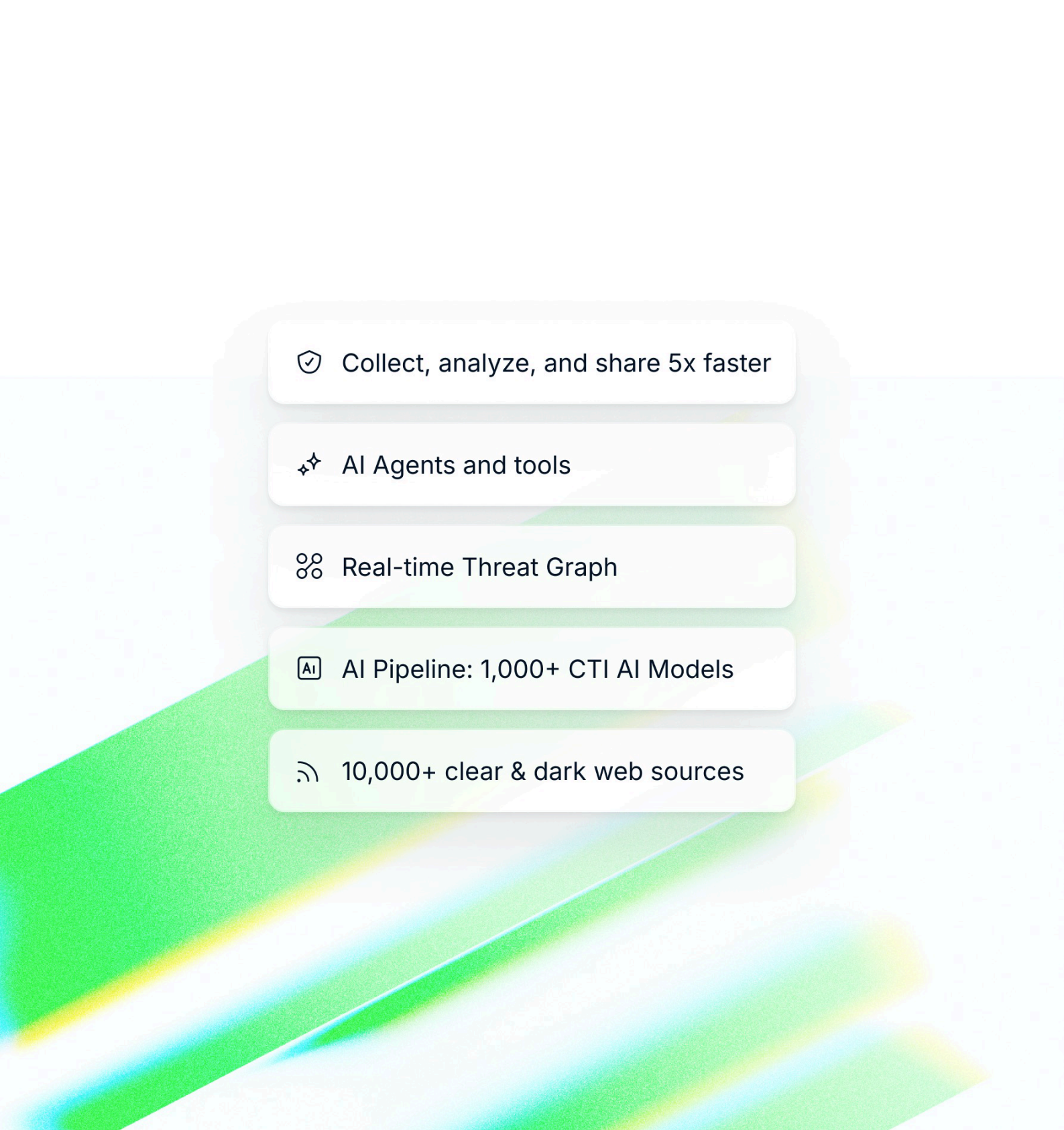
- Cybersecurity professional with over 12 years of experience, specializing in threat intelligence, digital forensics, and security operations.
- Speaker, educator, and advocate for diversity and inclusion, deeply engaged in the cybersecurity community.
- Holds numerous advanced certifications and a Master's degree in cybersecurity, and has been recognized with awards for technical expertise and volunteer contributions.



**Rebekah Brown**

Senior Researcher  
and SANS Instructor

- Helped develop threat intelligence programs at the highest levels of government, including experience as a National Security Agency network warfare analyst, U.S. Cyber Command training and exercise lead, crypto-linguist, and Cyber Unit Operations Chief for the U.S. Marine Corps.
- Has provided threat intelligence across national security operations, state and local governments, and Fortune 500 companies, including delivering a briefing at the White House.
- Senior Researcher at Citizen Lab; SANS course instructor and student mentor teaching FOR578: Cyber Threat Intelligence, which she co-authored, and co-author of Intelligence Driven Incident Response.



🛡️ Collect, analyze, and share 5x faster

✨ AI Agents and tools

🕸️ Real-time Threat Graph

🧠 AI Pipeline: 1,000+ CTI AI Models

📡 10,000+ clear & dark web sources



Feedly helps CTI teams cut through open-source noise and deliver actionable intelligence 5x faster with AI. Trusted by 400+ enterprises and government organizations worldwide. [Learn more](#)