



GUIDEBOOK



THE CTI DECISION-SPEED ASSESSMENT

Is Your Intelligence Keeping Pace with Modern Threats?

| A practical guide for threat intelligence
analysts & leaders

CONTENTS

- Introduction: The Intelligence Paradox 3**
 - 1.1 How this Guide Relates to CTI-CMM4
 - 1.2 Let’s Focus on Speed4
- Self Assessment: Where Does Your CTI Stand 5**
 - 2.1 Warm Up: How CTI Feels Today6
 - 2.2 Sourcing: What Feeds Your Intelligence.....6
 - 2.3 Context: How You Make Intelligence Relevant.....6
 - 2.4 Delivery: How Intelligence Reaches Decision Makers.....7
 - 2.5 Trust: Do Stakeholders Act on Your Intelligence.....7
 - 2.6 Velocity: How Fast You Move From “Threat Detected” to “Decision Made”7
 - 2.7 Scoring Your Assessment.....8
- The CTI Decision-Speed Ladder 9**
 - 3.1 Overview of the Four Stages.....9
 - 3.2 Stage 1: Reactive – We Have Feeds.....10
 - 3.3 Stage 2: Responsive – We Inform Decisions11
 - 3.4 Stage 3: Proactive – We Drive Risk Decisions12
 - 3.5 Stage 4: Strategic – We Accelerate Business Outcomes.....13
- Decision-Speed in Action: Use Cases and Scenarios14**
 - 4.1 Use Case 1: New Ransomware Variant Emerges.....15
 - 4.2 Use Case 2: Market Expansion Into a High Risk Region16
 - 4.3 Scenario Quiz 1: Vendor Risk Assessment.....18
 - 4.4 Scenario Quiz 2: Emerging Phishing Campaign19
- What Does Not Work: Common CTI Mistakes20**
 - 5.1 Mistake 1: Measuring CTI by Volume.....21
 - 5.2 Mistake 2: Distributing Raw Indicators.....21
 - 5.3 Mistake 3: Intelligence That Arrives After the Decision.....22
 - 5.4 Mistake 4: CTI as a Security Only Function22
 - 5.5 Mistake 5: Equating a TIP With a CTI Program.....23
 - 5.6 Mistake 6: No SLAs for Decision-Speed.....23
- Turning Insight Into Action24**
- Conclusion: From Feeds to Decisions25**
- Glossary of Terms.....26**

INTRODUCTION

The Intelligence Paradox

A few years ago, spotting a phishing email was almost trivial: broken English, blurry logos, obvious urgency. Today, AI generates messages that match your colleague's tone, writing style, and cadence. Fraud operations use automation to test thousands of paths before your policy review even begins. Every new SaaS app, vendor, and KYC provider expands the attack surface.

Far from suffering from a lack of information, most teams are dealing with too much of the wrong information, arriving at the wrong time, in the wrong format.

Threat intelligence teams live in this paradox every day. The volume of threat data has exploded: feeds, reports, telemetry, social chatter. Yet decision makers still ask the same questions:

- **Are we exposed to this?**
- **How urgent is it today?**
- **What do you recommend we do, and by when?**

In many organizations, CTI is still optimized for collection, not for decision-speed. Analysts are buried in feeds, manual enrichment, and one-off requests. Investigations sprawl across ad hoc virtual machines, shared spreadsheets, and risky browsing from production networks. Instead of working from safe, purpose-built environments, analysts stitch together whatever they can get, then hope nothing goes wrong.

The job of CTI has shifted. It is no longer about adding one more feed or hoarding more indicators. The core responsibility is to reduce uncertainty fast enough that the organization can choose a direction and move.

That requires:

- Focusing on relevance over raw volume
- Delivering intelligence on the timeline of the decision, not the report template
- Giving analysts secure analysis environments and sandboxes to handle malicious content and high-risk research at speed without introducing new exposure

This guide is designed to help you get there.



How this guide relates to CTI-CMM

If you already use CTI-CMM or similar capability models, treat this guide as a companion. CTI-CMM helps you evaluate capabilities across domains and set maturity targets. This guide helps you examine how those capabilities play out in practice: how quickly you can move from “new threat” to “decision,” how stakeholders experience CTI, and how safely analysts can do the highest risk parts of their job.

Let’s Focus on Speed

This guide is a practical diagnostic. It is meant to help you see how your CTI program behaves in day-to-day work and what it would take to turn that work into faster, safer decisions.

You will not find a full capability maturity model here. Excellent models like CTI-CMM already cover domains, practices, and program-level scoring. This guide sits one level closer to the ground. It will discuss how you source & filter intelligence, map it to your environment, deliver it to decision makers, and building trust in your team, so you can decrease the lag time between new signals and new actions.

Keep reading for:

- A self-assessment to score your current CTI posture across five levers: sourcing, context, delivery, trust, and velocity
- A four stage ladder that describes how CTI looks and feels at each level of decision-speed
- Before and after examples that show what changes when CTI is built around decisions instead of feeds
- Common traps that keep teams stuck in busywork and “feed consumption” mode

Throughout this guide, you will also see prompts about where the riskiest work happens in the real world. When analysts detonate malware, pivot through hostile infrastructure, or use AI to dig through sensitive data, this guide assumes they are working inside secure, governed environments that contain that risk and leave an audit trail – not improvising on their local machines.

Whether you are standing up CTI from scratch or evolving a mature function, the goal is to reinforce a shared language and a roadmap you can use with your analysts and stakeholders. Use it to show that CTI can operate as a decision engine for the business, not just another source of raw data.

SECTION 1

Self-Assessment: Where Does Your CTI Stand

Before you can improve decision-speed, you need a clear picture of how your CTI function behaves in everyday work. Not just which tools and processes you have, but how intelligence actually feels to the teams who depend on it.

This assessment focuses on five dimensions that shape decision-speed in practice:



Sourcing

What feeds your intelligence and how much noise you accept



Context

How clearly you map threats to your environment and priorities



Delivery

How intelligence shows up in the workflows of actual decision makers



Trust

Whether people change their behavior based on CTI, or ignore it



Velocity

How fast you move from *what* to *what to do about it*

As you work through the five topics, you will score your answers to build a clear picture of where your CTI program currently stands. Use this as a working document with your team. Mark what is true today, not what you wish were true. The goal is to understand how CTI feels on the ground so you can improve it, not to score a perfect result.

Warm Up: How CTI Feels Today

Check all that apply:

- ☐ We are drowning in feeds, reports, and alerts
- ☐ We spend more time collecting and formatting than advising
- ☐ We often get pulled into incidents late, as research support
- ☐ It is not clear who our primary internal customer actually is
- ☐ When a big story breaks, we scramble to figure out our exposure

What this tells you

If several of these are true, you are likely in Reactive or Responsive mode for most workflows.

Sourcing: What Feeds your Intelligence

- ☐ We primarily rely on free, or vendor-provided threat feeds
- ☐ We supplement feeds with OSINT and manual research
- ☐ We have curated, high fidelity sources tailored to our sector and threat landscape
- ☐ We integrate proprietary or partner intelligence that is specific to our environment
- ☐ We regularly retire noisy sources that do not influence decisions

What this tells you

If you are still in “ingest everything” mode, you are probably dealing with far more noise than signal. High maturity CTI programs treat sources as products that must justify their cost in attention, time, and money – and can point to specific decisions that improved because of each source.

Context: How You Make Intelligence Relevant

- ☐ We distribute raw indicators and let teams figure out if they matter
- ☐ We tag intelligence by threat actor, campaign, or TTP
- ☐ We map threats to our environment, assets, and risk profile
- ☐ We provide decision ready briefs that explain what this means for us and what we recommend
- ☐ We maintain a living map between key threats and business initiatives

What this tells you

Raw data is an input. Context turns a generic vulnerability announcement into “system X in business unit Y is exposed, and we recommend patching within 48 hours.”

Assessment continued on next page.

Delivery: How Intelligence Reaches Decision Makers

- ☐ We send weekly or monthly reports that summarize threat activity
- ☐ We brief stakeholders on request or when something big happens
- ☐ We have defined SLAs for delivering intelligence on breaking threats
- ☐ Intelligence is embedded in workflows, so stakeholders receive what they need when they need it, without asking
- ☐ We provide safe, standardized environments for high risk investigations, so CTA is not waiting on improvised infrastructure

What this tells you

If CTI arrives after the decision has already been made or after the window to act has closed, it is documenting the past instead of shaping the future. The more your delivery aligns with real decision points and the places where work happens day to day — ticketing systems, planning meetings, secure analysis environments — the more CTI will feel essential rather than optional.

Trust: Do Stakeholders Act on Your Intelligence

- ☐ Our reports get filed but rarely influence decisions
- ☐ Stakeholders ask for our input on major incidents or threats
- ☐ Leadership regularly incorporates CTI into risk and security planning
- ☐ Business teams, such as M & A diligence, vendor risk, and product, request CTI because it accelerates their work
- ☐ CTI is included in early stage planning for major initiatives, such as market expansion or significant contracts

What this tells you

Lack of action usually signals lack of relevance, timeliness, or track record. High performing CTI teams are measured by how often their work changes outcomes.

Velocity: How Fast You Move From “Threat Detected” to “Decision Made”

- ☐ When a new vulnerability or threat appears, it takes us days to assess relevance
- ☐ We can typically provide a relevance assessment within 24 hours
- ☐ For most priority threats, we deliver actionable intelligence within hours
- ☐ We use automation and existing context to deliver decision ready briefs within minutes for high priority threats
- ☐ We track metrics such as mean time to intelligence and work to improve them

What this tells you

Adversaries are not pacing themselves to your reporting cycle. Velocity determines whether your organization responds in time or reacts after the fact.

Scoring Your Assessment

The scoring is a **decision-speed snapshot**, not a full program maturity score. Use it to understand how CTI behaves in your highest value workflows today.

For each dimension (Sourcing, Context, Delivery, Trust, Velocity):

1. Identify the highest level statement that accurately describes your current state.
2. Assign points:
 - First box: 1 point
 - Second box: 2 points
 - Third box: 3 points
 - Fourth or fifth box: 4 points
3. Add the points for all five dimensions. Total score is between 5 and 20.

5 to 9 points: Reactive

CTI operates primarily as a feed ingestion and lookup service. You have data, but limited structure, secure environments, or processes to turn that data into decision-speed.

10 to 13 points: Responsive

CTI informs incident response and some security decisions, but most work is requested rather than anticipated. Context is improving, yet delivery, velocity, and trust are uneven.

14 to 17 points: Proactive

CTI is structured around decision makers and business context. Threats are mapped to your environment, intelligence is delivered on a meaningful timeline, and the program is beginning to influence high value business decisions.

18 to 20 points: Strategic

CTI operates as a competitive advantage. Intelligence supports security and business moves. High risk investigations run in secure, standardized environments that let analysts work quickly without adding risk, and stakeholders rely on CTI to reduce uncertainty in their most important decisions.

Use this score as a baseline. The next section describes what each maturity stage looks like and how to move up.

SECTION 2

The CTI Decision-Speed Ladder

Most CTI programs pass through four recognizable stages of decision-speed, which we describe as a ladder. It is not a replacement for capability models such as CTI-CMM, which focus on domains and practices. Use this viewpoint alongside them to see how CTI behaves in your highest value workflows.

Each stage describes three things together: the role it plays for stakeholders, the tempo of decisions, and the guardrails around high risk work. Knowing where you are, and what the next stage demands, helps you focus investment in process, tooling, and secure environments.



Strategic
Proactive
Responsive
Reactive

Working with CTI models

Capability maturity models such as CTI-CMM focus on domains and practices. They help you discern which CTI capabilities you have, and how well each is performed.

The CTI Decision-Speed Ladder focuses on experience and outcomes instead. It helps you answer:

- ✓ How CTI feels to stakeholders at each stages
- ✓ How quickly you move from data to decision
- ✓ How safely analysts can carry out high risk work

You can use this ladder alongside any existing CTI maturity model as a way to understand how those capabilities play out in real workflows.

STAGE 1

Reactive: We Have Feeds

What it looks like

- CTI revolves around ingesting threat feeds from vendors, open sources, or information sharing groups
- Feeds flow into a SIEM or TIP, analysts triage alerts and perform lookups
- Intelligence is distributed as raw indicators, vulnerability lists, or broad summary reports
- Analysts spend most of their time collecting, normalizing, and formatting data
- Stakeholders see CTI as useful, but not essential for decisions

Common pain points

- Overwhelming volume of low fidelity data
- No clear process for prioritizing what matters
- Intelligence often arrives too late to influence decisions
- Stakeholders do not see direct impact on their work

Key capabilities at this stage

- Threat feed ingestion through standard formats and APIs
- Basic indicator enrichment and tagging
- Support for incident response through lookups and retrospective analysis

What is missing

- Clear relevance, for example “does this matter to our environment”
- Consistent speed in responding to breaking threats
- Trust that CTI will materially improve a decision

What it takes to move to Stage 2

- ✓ Identify your primary internal customers, such as SOC, incident response, or vulnerability management, and prioritize their use cases
- ✓ Replace indicator dumps with concise relevance assessments that answer whether you are exposed, how serious that exposure is, and what you recommend
- ✓ Review your sources and deprecate feeds that rarely lead to changed actions
- ✓ Establish a basic, sanctioned secure sandbox for malware detonation and high-risk browsing, instead of relying on improvised lab machines on production networks
- ✓ Document a simple playbook for breaking threats, including who is notified, which checks run first, and how soon a preliminary assessment is expected

STAGE 2

Responsive: We Inform Decisions

What it looks like

- CTI actively supports incident response, vulnerability management, and threat hunting
- Analysts provide context such as threat actor behavior and typical targets
- Intelligence is tailored by audience, for example indicators and rules for SOC, briefs for leadership
- The team is starting to build credibility, and stakeholders ask for input on major threats

Common pain points

- Work is still largely reactive and driven by requests
- Delivery speed is inconsistent: very fast for high profile stories, much slower for other issues
- Limited integration with business processes outside security

Key capabilities at this stage

- Threat actor tracking and campaign analysis
- Contextualized intelligence that reflects sector or geography
- Defined intelligence products, such as daily briefs, weekly summaries, and incident support
- Some automation for enrichment and correlation

What is missing

- Proactive intelligence that shapes plans before threats materialize
- Consistent velocity, not only during high visibility incidents
- Strong alignment with business units outside the core security group

What it takes to move to Stage 3

- ✓ Anchor CTI to business initiatives, such as cloud migrations, product development, strategic vendors, and new tool evaluation
- ✓ Standardize decision ready formats, for example a one page brief that clearly states the threat, relevance, exposure, recommended actions, and timeline
- ✓ Define SLAs that reflect business impact, such as faster assessments for systems that support revenue or critical operations
- ✓ Move high-risk investigations into fully isolated, logged environments so analysts can handle malware, suspicious links, and untrusted tools without waiting for exceptions or approvals
- ✓ Track where CTI recommendations change patch timelines, vendor contracts, or project plans, and use those stories to reinforce value

STAGE 3

Proactive: We Drive Risk Decisions

What it looks like

- CTI shapes security and risk strategy, not just incident response
- Intelligence is mapped to business context, such as which threats matter for vendor risk, product development, or regional expansion
- You have explicit SLAs for decision-speed, such as “breaking threat to actionable brief in under two hours”
- Stakeholders trust CTI enough to alter plans based on intelligence
- Effectiveness is measured by outcomes, such as decisions accelerated, risks avoided, and time saved

Common pain points

- Scaling intelligence delivery without burning out analysts
- Maintaining quality and relevance as the organization grows or changes
- Demonstrating return on investment in a language that resonates with executives

Key capabilities at this stage

- Automated contextualization that maps threats to your assets, technologies, and risk appetite
- Intelligence embedded in workflows such as vulnerability management, vendor assessments, and incident response
- Support for multiple functions, including security, legal, GRC, and line of business teams
- Forward looking analysis of adversary behavior, emerging campaigns, and trends

What is missing

- Full integration with business strategy, where CTI is consulted early for major moves
- A model for providing intelligence as a service, with clear intake, offerings, and self-service patterns
- Standard patterns for when work must run in secure analysis environments instead of on production networks

What it takes to move to Stage 4

- ✓ Position CTI as a shared service that supports security and business teams through defined offerings and intake paths
- ✓ Package secure workspaces as reusable environments for common use cases, such as “innovation lab”, “vendor evaluation lab”, or “investigation lab”, with preconfigured access controls, logging, and approval flows
- ✓ Align with finance and strategy on how CTI influences revenue, cost avoidance, and speed of execution
- ✓ Automate collection, enrichment, and environment provisioning so analysts can spend their time on analysis, judgment, and stakeholder conversations
- ✓ Make CTI input a standard element of governance for high risk decisions, such as large contracts or entry into new markets

STAGE 4

Strategic:

We Accelerate Business Outcomes

What it looks like

- CTI is treated as a competitive advantage instead of a background function
- Business teams request CTI early because it reduces uncertainty and shortens their timelines
- Intelligence informs decisions around market expansion, vendor selection, product security, regulatory strategy, and more
- High risk work runs in secure, standardized environments that support rapid experimentation and investigation without increasing exposure
- CTI operates as a service, with self-service for routine questions and clear escalation paths for complex or sensitive work

Common pain points

- Sustaining performance requires continued investment, executive sponsorship, and cross functional collaboration
- Rising demand can turn CTI into a bottleneck if capacity and automation lag

Key capabilities at this stage

- Real time or near real time intelligence delivery for critical events
- AI assisted analysis and contextualization to scale without excessive headcount growth
- Deep integration with business processes and decision cycles
- Mature feedback loops for measuring value in business terms, such as deals closed faster, losses avoided, and delays prevented

At this stage, performance is measured by CTI's effect on decisions and outcomes, rather than by counts of indicators or feeds.



SECTION 3

Decision-Speed in Action: Use Cases & Scenarios

Theory is helpful, but examples make the concept real. This section shows what decision-speed CTI looks like in practice. Two scenarios are written out in full. Two more are designed as quizzes you can use in workshops with your team and stakeholders.

USE CASE 1

New Ransomware Variant Emerges

Before: Reactive CTI

A new ransomware variant appears on a Friday afternoon. It dominates the headlines. Early reports say it targets healthcare and exploits a zero day in a widely deployed software platform.

Your CTI analyst sees the first reports and starts researching:

- Pulls threat reports from vendors and information sharing communities
- Tries to confirm whether your organization uses the affected software
- Looks for indicators to search in your SIEM
- Tries to understand whether your sector is being targeted

By Monday, the analyst has a draft brief: the ransomware targets healthcare organizations that use Software X, your sector might be interesting to these actors, and you may have exposure. The brief recommends further investigation.

The document moves from analyst to SOC manager, then to the CISO, then to IT or infrastructure leaders who own the relevant systems. By the time a complete risk assessment is ready and leadership approves a plan, it is Wednesday. If you were exposed, the proactive window has closed.

After: Decision-Speed CTI

Same ransomware variant, same Friday. This time, your CTI function has:

- Curated sources instead of an unfiltered set of feeds
- An inventory that maps Software X to specific business units and systems
- An established secure analysis environment where analysts can safely inspect reports, tools, and samples related to the ransomware without putting production networks at risk

Within 90 minutes, CTI delivers a one page brief:

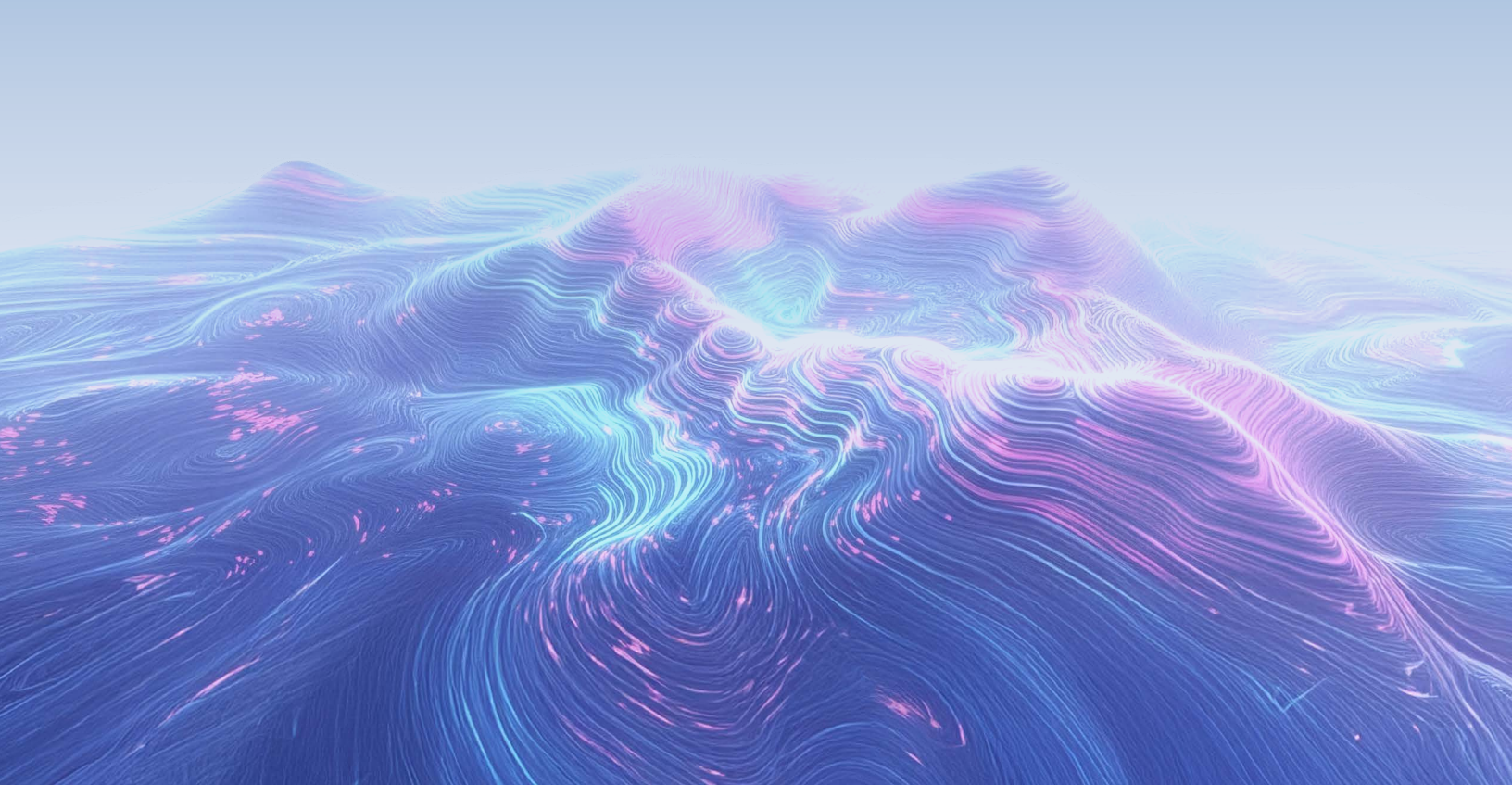
- **Threat:** New ransomware exploiting Software X
- **Exposure:** 4 systems in Finance and HR on vulnerable versions, 8 other instances already patched
- **Current coverage:** Endpoint tools have partial detection based on known indicators, with identified gaps
- **Recommended actions:**
 - Patch vulnerable systems within 48 hours
 - Deploy additional monitoring on affected endpoints
 - Brief Finance and HR about phishing patterns seen in this campaign
- **Timeline:** Patch window closes Monday end of day

Leadership approves the plan on Friday. Patches deploy over the weekend. When the first large scale exploitation wave arrives, your risk is already reduced.



What Changed

CTI combined relevant sources, context, a secure analysis environment, and a clear process to produce a decision within hours. The team did not just describe the threat. They explained precisely what it meant for your environment and what should happen next, while there was still time to act.



USE CASE 2

Market Expansion Into a High Risk Region

Before: CTI as a Late Check

Your company is planning to expand into a new region. The opportunity looks strong: new customers, favorable pricing, and a clear competitive gap. Strategy and sales are driving the plan and want to announce within the quarter.

Security hears about it during a planning meeting. There are a few high level concerns about regional cybercrime, local regulations, and potential state linked activity, but nothing specific. Someone asks CTI for a short summary of regional threats “for the deck.”

CTI has limited context and little time.

- You search for general threat reports that mention the region
- You pull a few examples of recent incidents affecting companies there
- You note that ransomware and credential theft are common, and that some sectors have seen state linked activity

You deliver a two page summary one week later. It provides background, but it does not change the expansion plan, the architecture of the new deployment, or the go to market timeline.

The company enters the region with a slightly updated playbook and hope that standard controls will be enough.

After: CTI as a Business Enabler

Same region, same growth opportunity.

This time CTI is brought in when the expansion is still in the evaluation stage. The team has a rough idea of product, timeline, and target customers, but no one has committed yet. Within a few days, CTI delivers a focused brief:

Regional threat landscape:

- High rates of financially motivated cybercrime and organized fraud
- Active state linked groups with a history of targeting local and foreign companies in your sector
- Frequent use of compromised local vendors and service providers as stepping stones

Regulatory and data considerations:

- Specific data residency requirements that affect how you host customer information
- Local interception or monitoring laws that may limit where and how you operate security tooling
- Known enforcement actions against companies that mishandled local data

Operational risks:

- Common attack patterns against companies similar to yours
- Local third parties and infrastructure providers with weak security track records
- High prevalence of phishing and social engineering against local staff and partners

Recommendations:

- Use a separate regional deployment with stricter network segmentation and dedicated monitoring
- Route high risk investigations and local fraud analysis through secure analysis environments rather than from regional user workstations
- Build regional vendor and partner vetting into the project plan and budget
- Stage the rollout so that security controls, secure sandboxes, and monitoring are in place before customer data is onboarded

Strategy, security, and legal review the brief together. The company decides to proceed, but with a modified architecture, a different data residency approach, and a phased rollout that reflects CTI findings.



What Changed

CTI influenced where and how the company entered the market, which providers it trusted, and how it protected customer data. Intelligence showed up early enough to shape design and sequencing, and secure environments for investigations were built into the plan instead of bolted on later.

USE CASE 3

Vendor Risk Assessment: Scenario Quiz

Your company is evaluating a new SaaS vendor that will handle sensitive customer data. Procurement is excited. The vendor has completed a standard security questionnaire. On paper, everything looks fine.

You have two days before the signing meeting.

Which option sounds most like your current reality?

A. Stage 1, Reactive

You skim the security questionnaire, ask a few generic follow up questions, and sign off. You flag a few items for future review, but there is no clear process or capacity to revisit them.

B. Stage 2, Responsive

You check for public breaches, ask for the latest summary of penetration testing, and review their compliance reports. You sign off with a recommendation to perform a deeper review in the next annual cycle.

C. Stage 3, Proactive

You run a focused external risk assessment, examine their third-party dependencies, look for signs of credential reuse and exposed admin portals, and negotiate stronger breach notification and remediation terms in the contract.

D. Stage 4, Strategic

You do everything in option C, and you also use a standardized secure vendor evaluation environment to test the vendor's application and integrations without touching production systems. Procurement treats CTI input as a mandatory step, not a nice to have. The outcome is documented, repeatable, and measured.

Use this scenario in workshops. Ask stakeholders which option is closest to today, then define what would need to change in process, tooling, and secure environments to move from one letter to the next.

USE CASE 4

Emerging Phishing Campaign: Scenario Quiz

A sophisticated credential phishing campaign starts to target organizations in your sector. You see early reports in sharing communities and on a few vendor feeds. Some peers report incidents on social channels.

You are responsible for CTI. How does this play out in your organization?

If your program is at Stage 1 or 2

- You collect information and wait to see if related alerts appear in internal systems
- When employees start receiving phishing emails, SOC investigates individual alerts and handles them case by case
- After the first incident, CTI produces a retrospective report describing the campaign and recommending additional controls

If your program is at Stage 3

- Within 24 hours, you brief SOC and the security awareness team
- You deploy indicators to email gateways and endpoint tools, tune detections, and push targeted awareness to high risk users such as finance or executives
- When the first wave arrives, most messages are blocked and the few that get through are recognized and reported by users

If your program is at Stage 4

- You are already tracking the adversary's infrastructure and TTPs from earlier activity against peers
- You update a phishing response playbook, test updated controls in a secure environment, then roll those changes into production with confidence
- You send a concise update to business leadership that explains what is happening and how prepared you are, before they have to ask

Use this scenario to connect maturity levels to outcomes that matter. The same threat looks very different depending on how you structure CTI and how quickly you can move from signal to decision.



SECTION 4

What Does Not Work: Common CTI Mistakes

Many CTI programs struggle not because they lack data, but because they are optimized for activity that does not change outcomes. The patterns below keep organizations stuck.

MISTAKE 1

Measuring CTI by Volume

What it looks like

- “We ingest 50 threat feeds”
- “We processed 10 million indicators last quarter”
- “Our platform contains half a million records”

Why it fails

More data does not guarantee better intelligence. Measuring volume encourages teams to collect more feeds, process more indicators, and publish more reports, regardless of actual relevance.

Analysts spend their time managing data flows. Stakeholders receive large, generic products that do not help them decide faster or with more confidence.

What to do instead

Measure CTI by decision-speed and influence.

- How quickly can you deliver a relevance assessment for a breaking threat
- How often do stakeholders act on CTI recommendations
- How many material decisions did CTI inform or improve this quarter

When your metrics focus on inputs only, you are optimizing for motion, not progress.

MISTAKE 2

Distributing Raw Indicators

What it looks like

- Daily or weekly files with thousands of new indicators sent to SOC
- Minimal context or prioritization
- No clear guidance about which indicators matter or what teams should do with them

Why it fails

Indicators without context create work for every downstream team. SOC must tune rules. Incident responders must guess at priority. Leadership has no idea what any of it means.

Most indicators also have a short shelf life. By the time they are distributed, analyzed, and operationalized, adversaries may have shifted to new infrastructure.

What to do instead

Shift from distributing indicators to distributing decisions.

Rather than “here are 500 new domains,” deliver “campaign X is active against our sector, these 12 domains are relevant to us, we have deployed blocks at the email gateway, and if you see traffic to these addresses you should escalate.”

Context plus prioritization plus recommended action creates intelligence that teams can use.

MISTAKE 3

Intelligence That Arrives After the Decision

What it looks like

- Weekly or monthly threat reports that summarize activity long after the fact
- Intelligence delivered on a fixed publishing schedule rather than on decision timelines
- Reports that are informative, but rarely drive specific action

Why it fails

If intelligence arrives after the decision has been taken or the opportunity to act has passed, it does not influence outcomes. It may help with awareness or compliance, but it does not protect the organization or accelerate progress.

Leaders do not need a recap of last month's landscape. They need support for questions that are in front of them right now.

What to do instead

Align intelligence products with decisions and their timing.

- Ask stakeholders which decisions they will face in the next week or month, and what information would let them move faster
- Reserve scheduled reports for background awareness, and separate them clearly from decision support products
- Use SLAs for time sensitive work so CTI understands what "on time" really means for each audience

MISTAKE 4

Treating CTI as a Security Only Function

What it looks like

- CTI focuses on SOC, incident response, and threat hunting
- No regular engagement with business teams such as procurement, legal, or product
- Intelligence framed entirely in terms of threats and vulnerabilities

Why it fails

Security operations are important customers, but they are not the only ones. Business teams also make high risk choices that shape exposure, such as selecting vendors, entering new markets, or acquiring companies.

If CTI does not participate early in those decisions, the organization carries more risk than necessary, and security teams inherit problems they could have prevented.

What to do instead

Position CTI as a business enabler.

- Build specific products for business use (procurement, product, and legal)
- Use language that connects intelligence to revenue protection, customer trust, and operational continuity
- Offer structured intake paths so business units know how and when to engage CTI

When non security teams start requesting CTI because it shortens their timelines and reduces uncertainty, you know the function is maturing.

MISTAKE 5

Equating a TIP With a CTI Program

What it looks like

- “We deployed a threat intelligence platform, so now we have CTI”
- Most CTI effort goes into managing integrations, normalizing data, and tuning correlation rules
- Stakeholders still do not receive clear, actionable intelligence

Why it fails

A platform is infrastructure. It can help collect and organize inputs, but it does not produce intelligence on its own. Analysts and well-designed processes create intelligence.

If analysts are spending all their time maintaining tools, they have less capacity to interpret, advise, and influence decisions.

What to do instead

Define your program first, then your tools.

- Start with your core intelligence products and the decisions they support
- Map the process from raw data to recommendations
- Choose or configure platforms that support this process instead of driving it

Tools should reduce manual work, enable secure analysis environments, and help you share intelligence effectively. They should not become the center of the function.

MISTAKE 6

No SLAs for Decision-Speed

What it looks like

- CTI responds “as soon as possible”
- No clear commitments for how quickly the team will assess new threats
- Speed varies wildly depending on who is shouting the loudest

Why it fails

Without expectations and measurements, it is hard to know whether CTI is keeping pace with stakeholder needs. Over time, response times drift, and stakeholders stop relying on CTI for timely input.

What to do instead

- Establish and track SLAs for intelligence delivery
- Define response times for critical, high, and medium priority threats
- Align SLA categories with business impact, not just CVSS scores or media noise
- Measure performance over time, identify bottlenecks, and invest in automation or staffing where needed

Speed is not optional. It is the difference between CTI that shapes events and CTI that simply records them.



SECTION 5

Turning Insight Into Action

You cannot transform a CTI program in a week, but you can create visible change with focused effort.

A practical starting point for the next 30 days could include:

- ✓ Selecting one high value workflow, such as breaking threats or vendor evaluation
- ✓ Defining what “decision ready” intelligence looks like for that workflow
- ✓ Setting a specific time target for relevance assessments and recommendations
- ✓ Standing up or standardizing a secure environment for investigations tied to that workflow
- ✓ Capturing one or two concrete stories where CTI changed an outcome, and sharing those with stakeholders

Use this guide as the foundation, then build a simple 30 day plan that fits your team’s capacity. Treat that plan as an experiment. At the end, review what improved, what stayed stuck, and where investments in process, automation, or secure workspaces will have the most impact.

CONCLUSION

From Feeds to Decisions

CTI has spent many years focused on collecting and distributing data. Feeds grew. Dashboards multiplied. Reports became longer. Yet the core questions from decision makers remained the same: “Are we exposed, how urgent is this, and what should we do”.

The problem is rarely a shortage of information. It is a shortage of clarity, speed, and trust.

Modern threats move faster than a monthly report. AI generated phishing looks legitimate. Fraud operations search constantly for new angles. Every new vendor and SaaS application adds to the attack surface. Intelligence that arrives after the decision has already been taken does not help.

You have an opportunity to reframe CTI as a decision engine.

That means structuring work around the decisions that matter most, aligning intelligence products with decision timelines, and giving analysts the secure environments and tools they need to handle high risk work at speed. It means measuring success in terms of decisions influenced, risks avoided, and time saved, rather than the number of feeds or indicators.

Use the self assessment to understand where you are. Use the Decision-Speed Ladder to describe where you want to be next, not five years from now. Use the use cases and scenarios to show colleagues how CTI can support them when it is designed for decision-speed.

You do not need perfect data or unlimited resources. You need focus, honest assessment, and a willingness to design CTI around the organization’s most important choices.

The teams that do this will stop drowning in feeds and start turning intelligence into a real advantage.

Glossary

CTI (Cyber Threat Intelligence)

The practice of collecting, analyzing, and delivering information about adversaries, their capabilities, and relevant threats in order to support decisions.

IOC (Indicator of Compromise)

An artifact associated with malicious activity, such as IP addresses, domains, file hashes, registry keys, or process names.

Feed

A continuous stream of threat data, usually containing indicators or signatures, from a vendor, community, or open source.

OSINT (Open Source Intelligence)

Intelligence derived from publicly available sources, including websites, social media, public records, and community forums.

Threat Actor

An individual or group that conducts or intends to conduct malicious activity, for example criminal groups, insiders, or state aligned operators.

Campaign

A series of related malicious activities or operations that share common objectives, infrastructure, or tools.

TTP (Tactics, Techniques, and Procedures)

The behaviors, patterns, and methods that adversaries use to achieve their objectives.

TIP (Threat Intelligence Platform)

A tool used to aggregate, normalize, enrich, and manage threat data from multiple sources, often integrated with detection and response systems.

SIEM (Security Information and Event Management)

A platform that collects and correlates security logs and events, providing alerts and analytical views.

SOAR (Security Orchestration, Automation, and Response)

Technology that automates security workflows, orchestrates tools, and standardizes response playbooks.

Decision-Speed

The time required to move from initial awareness of a new threat or signal to a clear decision and approved action.

SLA (Service Level Agreement)

A formal commitment that defines expectations for service quality, including response times for different kinds of requests or incidents.

MTTD (Mean Time to Detect)

Average time between the onset of an incident and its detection.

MTTR (Mean Time to Respond or Recover)

Average time between detection of an incident and its containment or resolution.

Secure Analysis Environment

A fully isolated and controlled workspace used to conduct high risk activities such as malware detonation, suspicious link inspection, and untrusted tool evaluation, designed to protect production systems while allowing analysts to work freely.

Secure Sandbox

A specific type of secure analysis environment where potentially malicious files, URLs, or tools can be executed and observed without allowing them to affect real users or systems.

High Risk Work

Activities that involve interacting with malicious content, untrusted tools, or sensitive data, for example threat investigations, deep OSINT collection, technical diligence, or testing new AI powered services.
