

BRIEFING PAPER



Closing the Gap Between Threat Intelligence and Action

Why Speed and Safety in Threat Investigation
Are a Competitive Advantage

Closing the Gap Between Threat Intelligence and Action

Executive Summary

Threat intel feeds, MSSPs, and IR retainers deliver real value, but they're built for thoroughness, not the decision a security leader has to make within the first day of an attack that now moves in hours.

The institutions that win are the ones that can test new intelligence against their own environment immediately, alongside their external providers, in an environment built to protect the bank, the mission, and the practitioners doing the work, all at once.

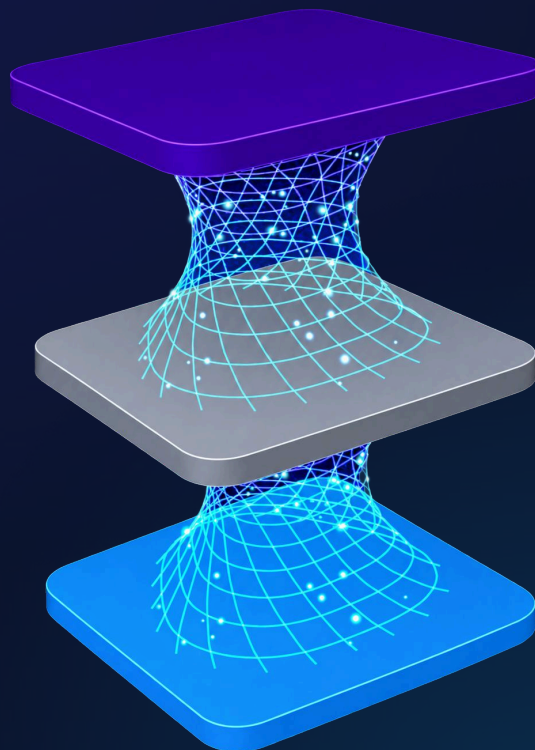
The question leadership needs answered isn't "can someone eventually tell us what this means?"
It's "can we move on this opportunity, and protect our customers, without slowing down?"

The Timing Gap

When new threat intelligence arrives, leaders need immediate answers, not a report next week:

- ◆ Does this affect us, and are we running the vulnerable technology?
- ◆ Can we observe this activity in our environment right now?
- ◆ Should we begin threat hunting, update detections, or isolate assets?
- ◆ Does this require notifying the business, the risk committee, or a regulator?

None of this can wait. Third-party analysis is valuable, but it typically validates a decision the institution has already had to make internally.



Intelligence Loses Value Fast

Time After Intelligence	Primary Value
First 24-72 hours	Operational decisions, hunting, prevention
First week	Detection engineering and mitigation
First month	Process improvement and defensive tuning
Several months	Strategic and historical context only

Attackers Are Outpacing Traditional Response

18 hrs ransomware deployment & exfiltration	40 min full domain compromise	4x faster year-over-year (2026)	90%+ incidents enabled by gaps & misconfigs
--	--	--	--

Source: Palo Alto Networks, 2025 & 2026 Unit 42 Global Incident Response Reports

Lengthy investigative processes can no longer be the default first step before action is taken.

Growth, Customer Trust, and Market Position

New intelligence about active exploitation can point at core banking platforms, payment rails, or a vendor with access to customer data. Leadership can't wait weeks to know whether funds are at risk.

- ◆ Product launches and fintech integrations stall when security review is the bottleneck, and competitors move first
- ◆ Internal teams that can validate risk fast can also clear new vendors, APIs, and AI tools fast
- ◆ Every hour customers spend on a platform that stays available and protects their funds reinforces the trust that keeps their business

Protecting the Bank, the Mission, and the Practitioners

Investigating from corporate laptops exposes the institution to unnecessary risk and creates attribution problems for the investigators themselves. Browser isolation or a one-off VM isn't enough. A governed environment has to protect three things at once:

Protecting the Bank

- ◆ Isolation and network separation from corporate endpoints and production infrastructure
- ◆ File governance to safely inspect, detonate, and destroy malicious artifacts

Protecting the Mission

- ◆ Controlled, disposable environments for malware analysis, phishing, and reverse engineering
- ◆ Auditability and rapid provisioning, so investigators start the moment intelligence arrives

Protecting the Practitioners

- ◆ Identity separation so enterprise and personal credentials stay shielded
- ◆ Attribution protection, so an investigator's activity can't be traced back to them

This is the model Replica Cyber's Trusted Execution environment is purpose-built to deliver.

The Internal Governance and Regulatory Case

Risk, compliance, and internal audit have a stake here too, often the most exacting one. Without a governed environment, investigations don't leave the record these functions need most: a defensible, auditable account of what happened, when, and by whom.

That gap surfaces at the worst moment, such as:

- ◆ Determining whether an incident meets the 36-hour notification threshold under the OCC, Federal Reserve, and FDIC's joint rule
- ◆ Assessing materiality for an SEC Item 1.05 disclosure
- ◆ Responding to a FINRA or state regulator inquiry, or producing records during an exam

A governed environment gives risk and compliance what they need: a time-stamped activity record, clear chain of custody, and access logs, so findings hold up to examiner and board-level scrutiny.

From “Yes or No” to “Where”

Today, a high-risk request puts IT and security in a binary spot: approve it and accept the exposure, or block it and accept the workaround or shadow IT that follows. Replica Cyber removes that binary. It doesn't ask whether high-risk work happens, only where.

IT and security no longer have to choose between yes and no. They can say yes, do it on internal systems, or yes, do it in Replica.

Product, deal, and innovation teams get a fast, governed path to yes, so the institution moves on the market's timeline. not security's.

A Modern Operating Model

External providers and internal teams aren't doing the same job, and this model doesn't ask them to. Providers bring breadth: visibility across thousands of environments, which is what makes campaign analysis and threat-actor attribution possible. Internal teams bring depth: the ability to safely get hands-on with that same malware, phishing infrastructure, and artifacts inside their own environment, the moment it matters to them.

External Providers	Internal Investigation Capability
Campaign analysis	Environmental impact assessment
Cross-customer attribution & threat-actor tracking	Hands-on investigation of malware, phishing, and live infrastructure
Industry visibility	Detection development
Long-term recommendations	Risk prioritization and operational decisions

Together, these capabilities compress the time from receiving intelligence to an informed decision, from weeks down to hours.

Conclusion

Threat intelligence only creates value once an institution can act on it. The real question is never whether someone can eventually explain what happened. It's whether customers and systems are safe today, and whether the business can keep moving on the opportunities growth depends on.

The institutions that close this gap respond faster, decide better, launch sooner than competitors, and give customers a reason to keep trusting them with their money.

