

One Source Is Not Enough

No Single Threat Intelligence Perspective
Provides Enough Insight

by Scott Messick

Core Thesis

Threat intelligence is almost always treated as a sourcing problem. Organizations ask which provider is best, which source is strongest, or whether one source is enough. Those questions feel reasonable, but they point in the wrong direction. The problem is not choosing the one perspective that appears to provide enough visibility for the organization. It is connecting multiple external intelligence perspectives with internal observations well enough to determine what matters and what action should follow.

Executive Summary

Security teams hear a familiar pitch from intelligence vendors. Add this feed, switch to this service, and visibility will improve enough to close the gaps that matter. Those claims sound logical. They are also incomplete.

No single intelligence perspective can reliably see across all of the adversary activity relevant to any given organization. Every external perspective is shaped by a limited vantage point, including the telemetry, access, geography, and analytical focus behind what it can see. That perspective can be valuable and still leave critical blind spots.

Most organizations already operate across multiple intelligence perspectives, whether they formally recognize them or not. External reporting, internal telemetry, investigations, vulnerability data, and asset context all contribute to how threats are understood and prioritized. Threat intelligence becomes truly valuable when these perspectives are connected. Outside-in intelligence explains what is happening in the world. Inside-out intelligence reveals what is happening inside the organization's own environment. The overlay between them determines relevance and drives action.

Multi-source intelligence creates value by connecting perspectives in ways that increase confidence, reduce blind spots, and allow organizations to demonstrate what changed as a result of intelligence. A mature intelligence program values external expertise, recognizes internal signals as intelligence, and connects both through consistent analysis. The outcome is not assumed coverage. The outcome is demonstrable confidence in the decisions and actions taken to defend the organization.



Why Threat Intelligence Exists

The Adversary Problem Threat Intelligence Solves

Malicious actors continuously develop new techniques, infrastructure, and malware to gain access to systems, compromise networks, and exploit organizations for financial, political, or strategic gain. Security teams must understand how these actors operate to anticipate attacks, interpret signals from security tools, determine which threats are relevant to their environment, and prioritize the risks that require attention. Threat intelligence provides insight into how attackers operate by analyzing malicious activity observed across many environments and translating those observations into knowledge about adversaries, campaigns, and attack techniques.



How Threat Intelligence Is Produced

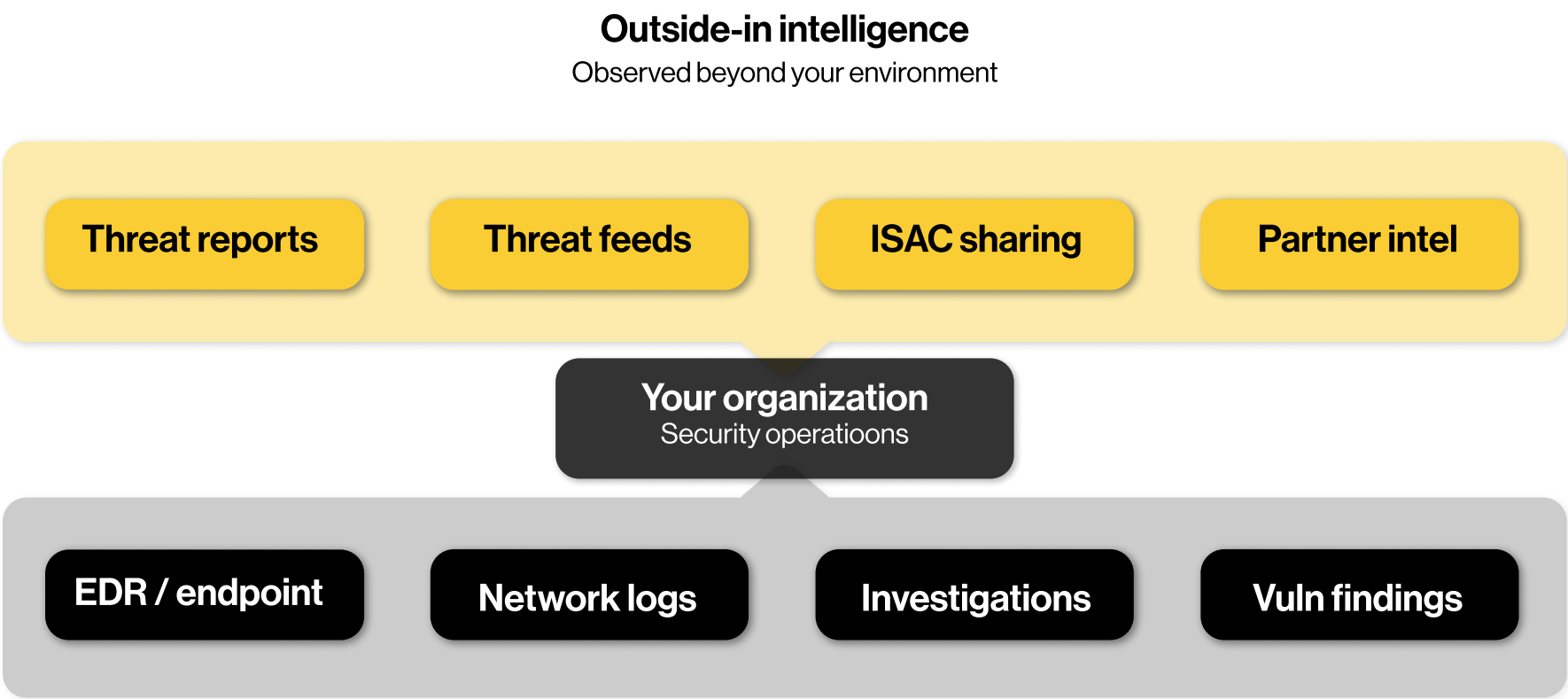
Researchers and analysts study attacker infrastructure, malware behavior, exploitation techniques, and intrusion campaigns to identify patterns in adversary activity. This analysis organizes and interprets raw technical artifacts such as IP addresses, domains, malware samples, and forensic evidence into contextualized knowledge about adversaries, campaigns, targeted organizations, and attack techniques. The resulting intelligence helps organizations determine which threats are relevant to their environment, prioritize defensive efforts, guide investigations, and make informed decisions about how to respond to malicious activity.



Many organizations and researchers across the security community produce threat intelligence. Security researchers publish research and reports on adversary campaigns. Commercial intelligence providers track attacker infrastructure, malware families, and operational patterns across large datasets. Industry sharing groups distribute warnings about threats affecting specific sectors. Vulnerability researchers disclose newly discovered software weaknesses. Open-source investigators analyze internet infrastructure and public communications where attackers exchange tools and techniques. Investigators also monitor underground forums and criminal marketplaces where stolen data, exploit kits, and access credentials are traded. Partner organizations and trusted relationships between analysts across organizations often provide additional intelligence through direct collaboration and information sharing.

The Value of Outside-In Intelligence

These external observations provide insight into malicious activity occurring across other organizations and environments. For clarity, in this paper, we refer to these externally produced observations collectively as outside-in intelligence because they originate outside the organization and describe activity observed elsewhere. Outside-in intelligence helps analysts, defenders, and security leaders understand what attackers are doing beyond their own environment. If attackers target organizations that share similar technologies, exposure, geographic presence, or operational environments, that activity may also affect other organizations with similar characteristics. Identifying attacker infrastructure, techniques, and operational patterns allows organizations to prepare investigations, detections, and defensive measures before those same techniques or attack patterns are used against them.



Inside-out intelligence

Observed within your environment

That multi-perspective reality is not theoretical. In the 2024 M-Trends executive edition, Mandiant reported that 54% of organizations first learned of a compromise from an external source, while 46% first identified evidence internally. Outside-in and inside-out perspectives are already part of how real organizations learn what is happening. The question is whether those perspectives remain separate or become connected.[1]

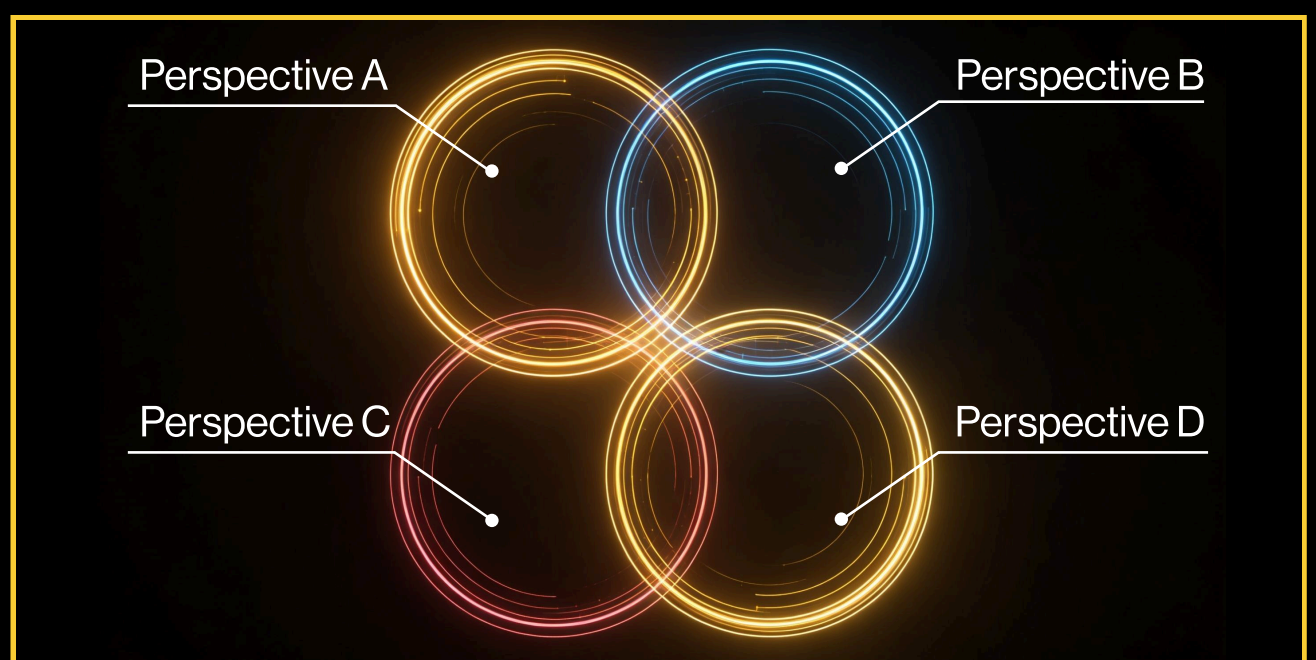


No Single Intelligence Perspective Sees the Whole Picture

Vantage Point Limitations

Every intelligence perspective is shaped by the visibility available to it and the method used to investigate activity. A perspective with deep visibility into one industry may have limited visibility into another. A research team focused on malware behavior produces fundamentally different insight than a team specializing in infrastructure tracking or incident response. A perspective built on broad internet-facing visibility may still lack the context available inside compromised environments. Those differences reflect structural limits built into how threat intelligence is collected and produced.

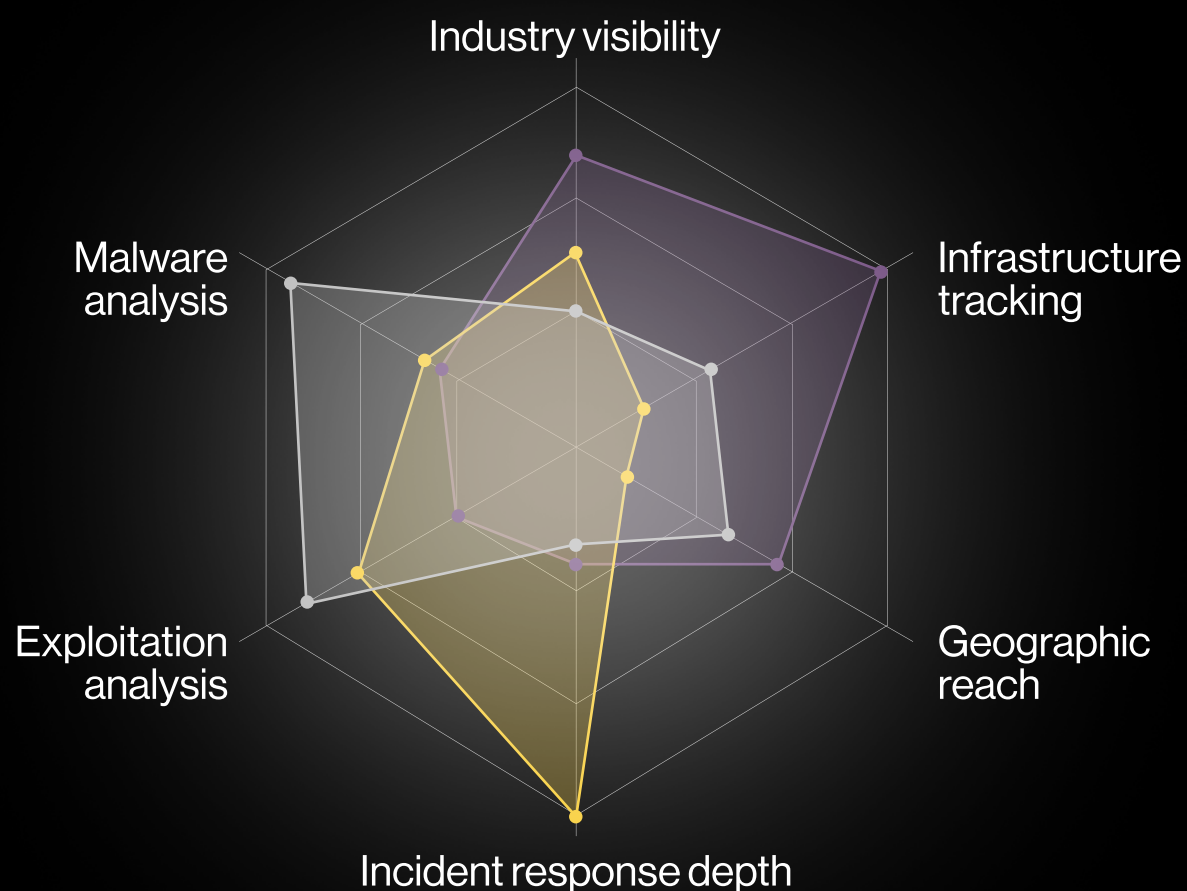
Each perspective is limited by its own visibility, methods, and access to different parts of attacker activity.



Why No Single Perspective Has Complete Visibility

No single perspective should be treated as a complete answer to any one organization's intelligence needs. Malicious activity unfolds across many environments, sectors, geographies, and stages of an intrusion. Infrastructure reused in one campaign may surface differently elsewhere. Techniques observed during one investigation may appear later in another environment under different conditions. What one perspective sees clearly, another may not see at all yet. What one perspective describes in detail, another may only partially observe.





■ Commercial provider ■ Open-source research □ Internal telemetry

No single perspective covers all dimensions. Each excels where others have gaps.

Why “Which Provider Is Best” Is the Wrong Question

Those limits also explain why the market’s usual comparison of which provider is best leads buyers to the wrong conclusion. A provider can be excellent yet incomplete. That remains true even when a provider is especially strong in a given sector, region, or customer segment. Strong coverage or insight for organizations with similar technologies, sectors, or exposure profiles does not eliminate the partial nature of any single vantage point. What matters is whether reliance on a single vantage point causes the organization to overestimate its visibility into threats and therefore make decisions based on an incomplete view of available information.

Once the limits of any single vantage point are understood, the need for multiple intelligence perspectives becomes clear. Organizations seek multiple intelligence perspectives because no single vantage point can consistently provide enough context, corroboration, and relevance on its own.



Why Organizations Turn to **Multiple Intelligence Sources**

Organizations turn to multiple intelligence sources for a practical reason: one source rarely provides enough context to support confident decisions on its own. The need is for broader visibility, stronger corroboration, and better interpretation of what observed activity actually means.

Coverage

Coverage is the most immediate reason organizations add sources. Different sources observe different parts of attacker activity. One source may identify infrastructure associated with a campaign affecting a particular sector. Another may report related activity targeting organizations in a different region. A third may publish a detailed analysis of the techniques used during intrusions uncovered through incident response investigations. Relying on more than one source reduces the chance that meaningful activity gets missed simply because it fell outside one source's field of view.

Corroboration

Corroboration strengthens confidence in what teams are seeing. Security teams routinely make decisions before they have complete information. When multiple sources independently report related infrastructure, techniques, or targeting patterns, confidence increases. What matters is whether separate observations reinforce one another, fill in missing context, or reveal where uncertainty remains. Not all apparent corroboration is independent. Different sources sometimes repackage or reinterpret the same upstream observations, creating the appearance of confirmation where there may only be duplication. This makes it even more important to understand how reporting was produced and how observations relate across sources.

Interpretation

Threat activity becomes useful when teams understand what it means for their environment. One source may describe a campaign at a strategic level while another provides technical details that change how the activity should be investigated or prioritized. A third may clarify whether the activity reflects broad opportunism, sector-focused targeting, or a more specific operational pattern. Multiple sources help organizations move beyond collection and into judgment.

The outcomes of this analysis extend beyond the intelligence team. When analysts can interpret activity accurately and determine its relevance, security teams can prioritize investigations, detection engineering efforts, and defensive actions more effectively. Leadership gains clearer insight into which threats pose real risk to the organization, and which do not. The value of multiple intelligence sources extends beyond improved awareness for analysts, enabling better-informed decisions across the security function and the broader organization.



You Already Have Multiple Intelligence Perspectives

Internal Signals Already Provide Intelligence

Many organizations believe they operate under a single-source intelligence model because they rely on a single external intelligence source. In practice, their understanding of threats is seldom formed by a single source alone. Even when a team relies on one primary intelligence service or source, its judgments are shaped by several other perspectives simultaneously.

External reporting is only one part of that picture. Security teams within the organization also work with endpoint telemetry, network observations, authentication and identity activity, vulnerability findings, cloud alerts, investigation notes, and operational knowledge about critical systems and business processes. These inputs influence threat understanding just as directly, even when teams do not label them as intelligence. They shape what gets investigated, what gets prioritized, and what gets dismissed.



These inputs already shape what a team investigates, prioritizes and dismisses - even when only one is formally labeled "intelligence". The multi-perspective reality is already here. Whether the perspectives connect is a separate question.

Multiple Perspectives in Everyday Security Controls

The same pattern appears in many security controls. Firewall, endpoint, email, and cloud security products often apply detections, rules, and protections derived from their vendors' telemetry and intelligence. A firewall does not enforce detections shaped by endpoint intelligence from another vendor, and likewise, an endpoint tool does not inherit the intelligence perspective built into a different network product. Even the controls within the environment are shaped by multiple partial intelligence viewpoints rather than a single shared intelligence picture.

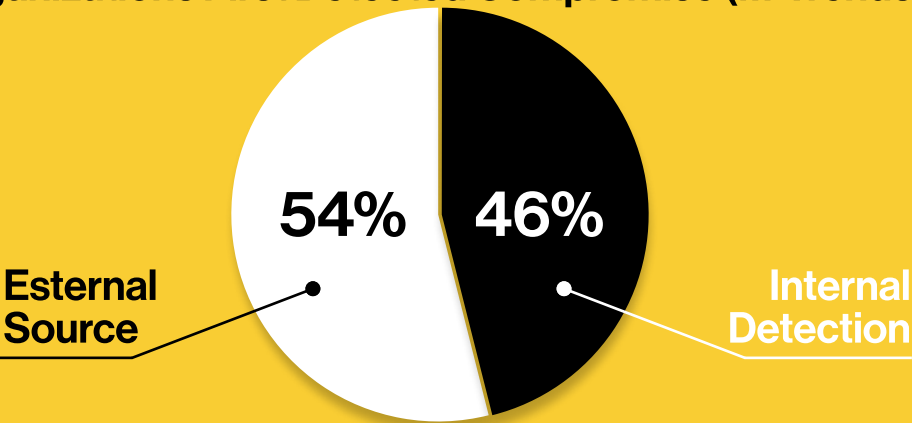


Outside-In and Inside-Out

The distinction between outside-in and inside-out perspectives helps clarify where intelligence comes from, how it flows, and how those perspectives contribute to the same problem. Outside-in intelligence begins with observations gathered beyond the organization, such as reporting on adversary infrastructure, campaigns, malware, vulnerabilities, or targeting patterns seen across other environments. Inside-out intelligence begins with what the organization learns from its own environment, including suspicious activity, blocked attempts, control failures, investigative findings, and defensive observations produced by internal analysis. These categories represent two directions of visibility into the same problem.

That multi-perspective reality is not theoretical. In the 2024 M-Trends executive edition, **Mandiant reported that 54% of organizations first learned of a compromise from an external source, while 46% first identified evidence internally.**

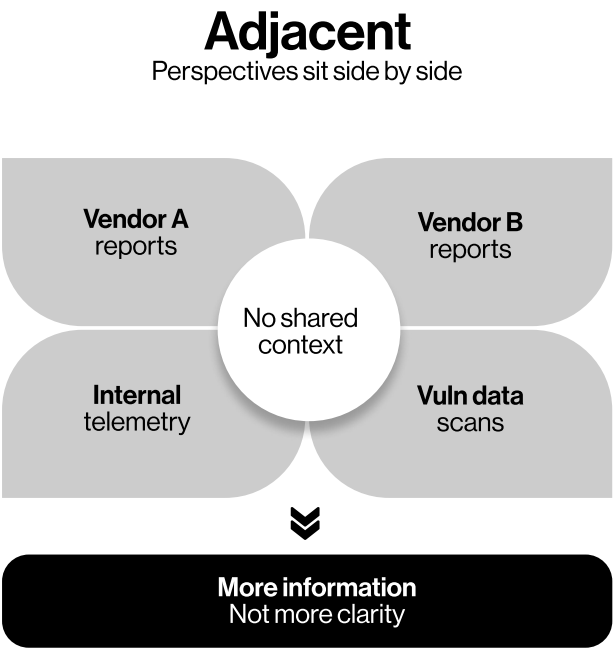
How organizations First Detected Compromise (M-Trends 2024)



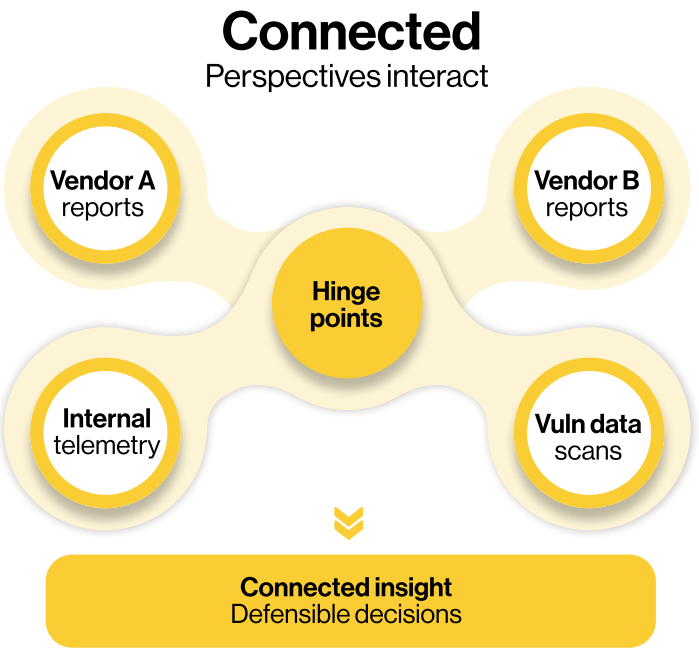
Outside-in and inside-out perspectives are already part of how real organizations learn what is happening. The question is whether those perspectives remain separate or become connected.[1]

Adjacent vs. Connected

Most organizations are already operating across multiple intelligence perspectives, whether they formally recognize them or not. A team can rely on a single external source and still operate within a multi-perspective reality. It can also work across five external sources and still fail to connect them.



When perspectives remain adjacent, they sit beside one another without clarifying what matters.



When perspectives become connected, they interact to produce correlated insight, reduce blind spots, and enable defensible decisions. What matters is whether those perspectives remain adjacent or become connected.



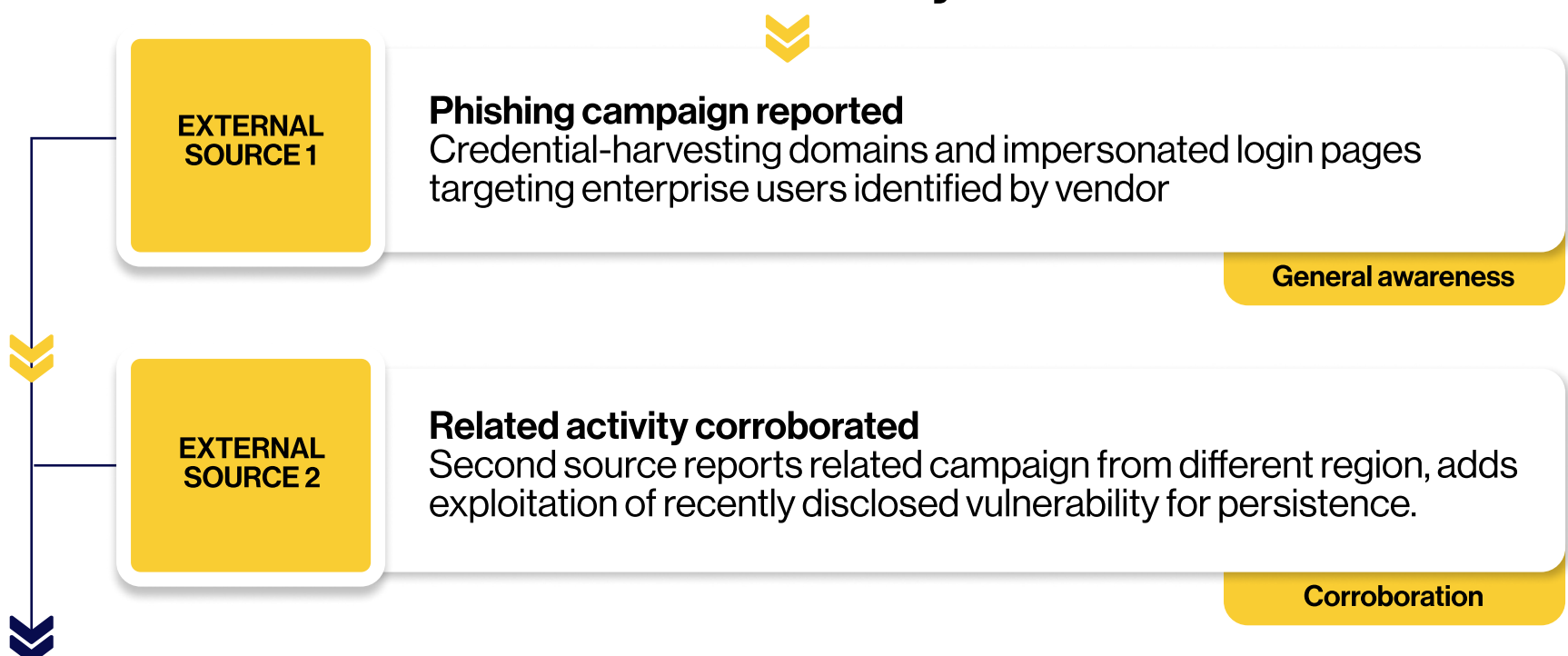
Where External Intelligence Meets Internal Signals

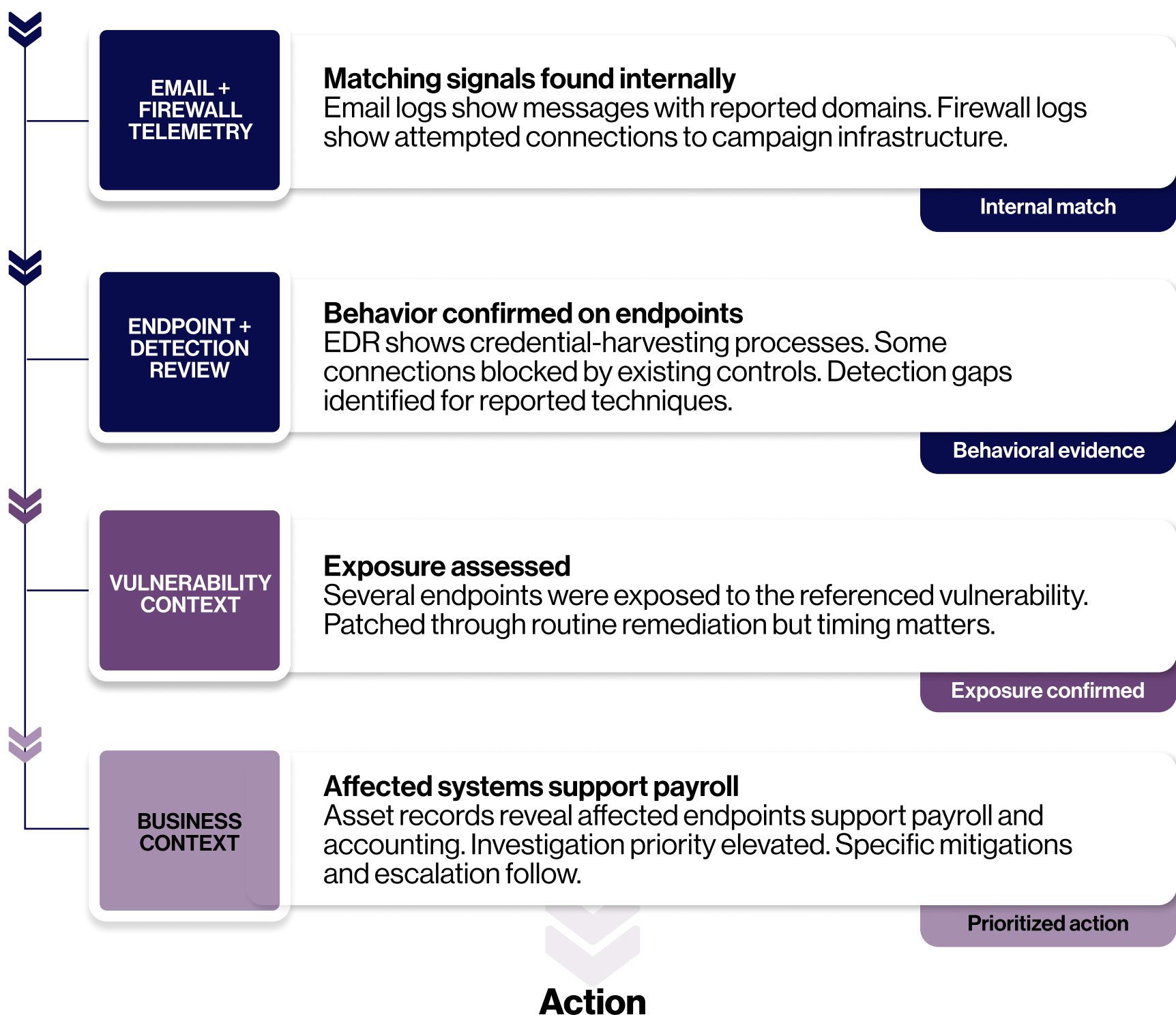
The difference between adjacent intelligence and connected intelligence becomes easiest to see in practice. Consider a common scenario in which an external source reports a phishing campaign using credential-harvesting domains and impersonated login pages aimed at enterprise users. On its own, that reporting is useful because it tells defenders that a campaign exists, describes some of the infrastructure involved, and provides a basis for searching internal systems. A second source independently reports related activity from another region and describes exploitation of a recently disclosed vulnerability used to establish persistence after initial access. At that point, the organization has more than one external perspective, but still does not know whether the activity matters to its own environment.

Internal review begins to answer that question. The intelligence team identifies the reporting, relates the external observations, frames the initial hypotheses and priorities for investigation by other teams. Email telemetry reveals messages containing domains that match the reported patterns. Firewall logs show attempted connections to the infrastructure identified in the reporting. Endpoint telemetry shows processes consistent with credential-harvesting behavior, while some connections appear to have been blocked by existing controls. Detection engineering teams review the defensive rules already in place for the infrastructure and techniques described in the external reporting.

Vulnerability management teams examine the scan history and determine that several endpoints were exposed to the vulnerability referenced in the intelligence, though they were later patched through routine remediation. Business context changes the meaning of those findings again. Asset and ownership records show that some of the affected endpoints support payroll and accounting systems. What began as general external reporting now intersects with internal observations tied to sensitive business operations. That raises the priority of the investigation and changes the urgency of the decisions that follow.

Decision clarity





A composite pattern observed across mature security organizations reflects how significant investigations often unfold in practice. In large enterprises with specialized intelligence, hunt, sensor, vulnerability, identity, and incident response teams, significant investigations rarely begin in one place or remain within a single workflow. External reporting, analyst suspicions, partner warnings, tickets, leadership questions, SIEM findings, EDR activity, vulnerability data, and forensic results all begin to shape the picture at different times and across different tools. Teams work in parallel, information changes across meetings, indicators are reclassified midstream, and leadership briefings often lag the live picture developing across the operation. The problem is not a lack of information. The problem is that external reporting, internal telemetry, asset context, vulnerability exposure, and investigative findings remain fragmented until they are connected well enough to determine what is real, what systems matter, and what action should follow.

Multi-source intelligence becomes operationally valuable when external reporting, internal telemetry, vulnerability data, and asset context are connected. External reporting describes activity observed elsewhere. Internal telemetry shows whether related signals exist inside the environment. Vulnerability and asset context help determine exposure and business significance. None of these observations is sufficient on its own. The decision value emerges only after they are connected.

That example captures the broader argument. Organizations struggle when separate perspectives never become one connected understanding. Threat intelligence becomes useful only when those perspectives are joined well enough to establish relevance, increase confidence, and guide action.



Why Intelligence Perspectives Differ

Different Vantage Points

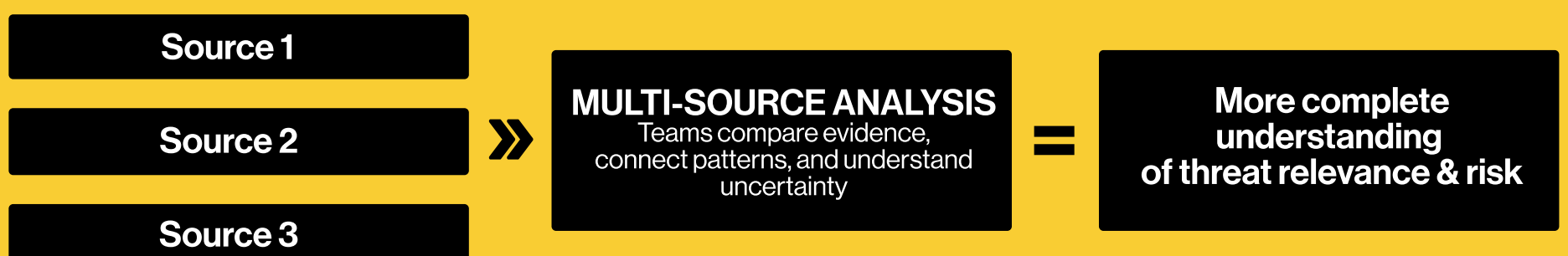
Differences across intelligence perspectives are often treated as evidence that multi-source analysis is confusing or hard to trust. In practice, however, those differences often necessitate multi-source analysis. Teams new to working across multiple intelligence sources often assume that related activity will be described in comparable ways. They quickly discover that naming, framing, and emphasis can vary far more than expected.

Perspectives differ because they observe different parts of the same reality. One may see infrastructure early because it has broad visibility into internet-facing activity. Another may identify malware behavior later through reverse engineering or incident response. A third may focus on exploitation patterns, sector targeting, or intrusion timelines. These differences often reflect the fact that adversary activity is distributed across time, systems, geography, and stages of execution, while each perspective captures only part of it. Terminology can make that overlap harder to see. One perspective may group activity under a campaign name, another under a malware family, and another under an actor cluster or intrusion set. Each may emphasize different artifacts, techniques, or stages of the intrusion based on its method and purpose.

What Convergence and Divergence Reveal

Convergence across sources can increase confidence. Divergence can be just as useful when it reveals uncertainty, incomplete visibility, or another dimension of the activity. A single source may sound cleaner because it presents one narrative. Multiple sources often sound messier because they expose the problem more transparently.

The complexity created by those partial and overlapping views is exactly what the “best provider” frame fails to capture. The value comes from what those differences mean, where they originate, and whether connecting them yields a clearer view of their relevance to the organization. Multi-source intelligence becomes more useful when it teaches teams to reason through partial agreement, incomplete overlap, and evolving evidence, rather than expecting a single source to resolve the question of relevance or meaning on its own.

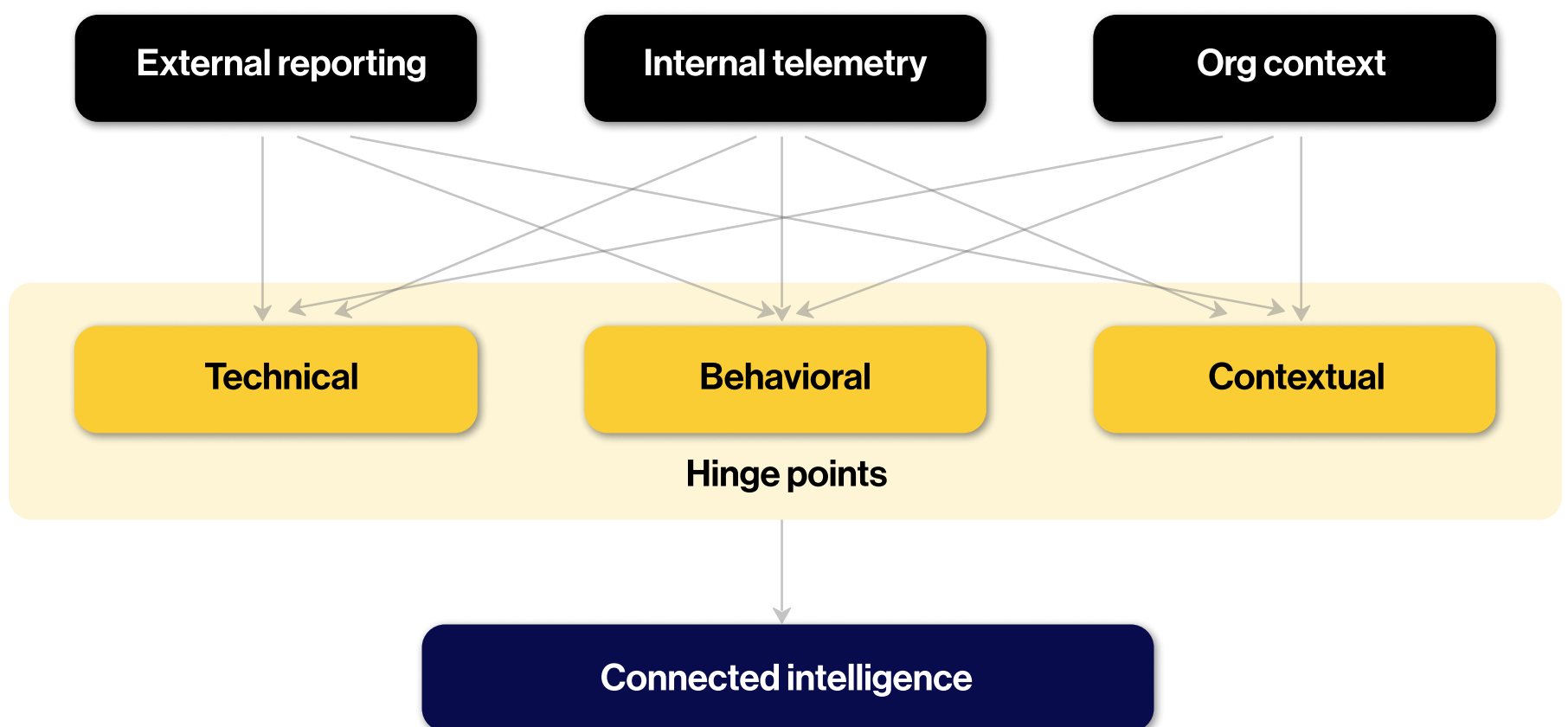


Hinge Points: Connecting Intelligence Across Sources

What Hinge Points Are

If multi-source intelligence matters because it brings together different perspectives, those perspectives become useful only when analysts can identify the points at which separate observations relate to the same underlying activity. Those points are hinge points.

Hinge points are where separate observations stop remaining adjacent and start becoming intelligence. A hinge point can be an artifact, a behavior, or a contextual element that allows separate observations to be related in a way that improves understanding. Some hinge points are technical: domains, IP addresses, URLs, hashes, file paths, certificates, mutexes, and other artifacts. Some are behavioral: techniques, execution patterns, exploit chains, persistence methods, and targeting approaches. Others are contextual: a vulnerable asset, a critical business function, a user population, or a geographic footprint. Each can connect threat reporting to organizational relevance in a different way.



These hinge points matter because they turn collection into analysis. Without them, organizations may have multiple sources but still be left with parallel streams of information that never meaningfully interact. One report may describe adversary infrastructure, another may describe a malware capability, and internal telemetry may show suspicious behavior. Yet none of it improves decision-making unless those pieces can be connected through common reference points. Hinge points provide the mechanism for connecting different intelligence into a coherent picture.

Hinge points also show why simply adding more sources does not solve the problem. If perspectives cannot be connected, more reporting often yields more adjacent information rather than greater understanding. A team may collect broad external reporting and rich internal telemetry, but still fail to determine whether the observed activity reflects the same campaign, the same adversary behavior, or the same exposure path. In that situation, the organization has more information without much more clarity.

As illustrated in the previous example, different teams pivot across these hinge points while examining intelligence reports, telemetry, vulnerability data, and asset information. Using hinge points to connect reporting, telemetry, vulnerability data, and asset context turns multi-source collection into connected intelligence. It allows organizations to determine whether reported activity is relevant to their systems and what investigation, decisions, or operational actions should follow.



Hinge points are the shared references that connect separate intelligence sources and internal data, turning disconnected information into meaningful analysis that supports investigation and decision-making.

Where **Multi-Source Intelligence** Becomes Difficult

Connecting intelligence across multiple sources and internal observations introduces practical challenges. For most organizations, the problem is not simply gaining access to more reporting. The harder problem is connecting different observations in ways that establish meaning for the organization. Access to multiple intelligence sources is often easy. Analysts can consult vendor portals, research reports, information-sharing communities, publicly available research, and open-source reporting. A vendor may provide multiple ways to access its intelligence through portals, feeds, APIs, and reports, but those channels can still reflect a single external perspective. They can make access easier, but they do not change the fact that a single perspective remains incomplete.

The paper's argument is not that organizations need more delivery methods. They need more than one perspective, and those perspectives need to be connected to internal observations. Turning those observations into a clear understanding and consistent operational decisions requires significantly more effort.

Representation Differences

Different intelligence sources often describe the same activity using different naming conventions or technical representations. Intelligence reports frequently overlap. The same campaign may appear under different names depending on the source. Malware families may be labeled differently across sources. Infrastructure artifacts may be described using different formats or an incomplete context. Technical indicators can also vary across reports and tools. A file may appear in one report as an MD5 hash while another source reports a SHA-256 value derived from the same file. Security tools may also accept only certain formats when searching for indicators or enforcing detection and prevention rules, making it difficult to compare intelligence artifacts across multiple datasets and systems immediately. Analysts must reconcile differences in reporting, attribution, and investigative conclusions while determining whether the activity described across multiple sources is related, relevant to their organization, or unrelated to the threats they are prioritizing. These representational differences make it difficult to determine whether multiple reports describe the same underlying activity and complicate efforts to correlate intelligence across sources.

Scale and Data Volume

Multi-source intelligence also introduces challenges related to scale. External intelligence feeds, research reports, and open-source investigations continuously produce new information about adversary infrastructure, malware, and techniques. Internal environments generate enormous volumes of telemetry from endpoints, networks, identity systems, and cloud platforms. Connecting intelligence across these datasets requires organizations to analyze large volumes of information and identify the relatively small subset that is meaningful for their environment.



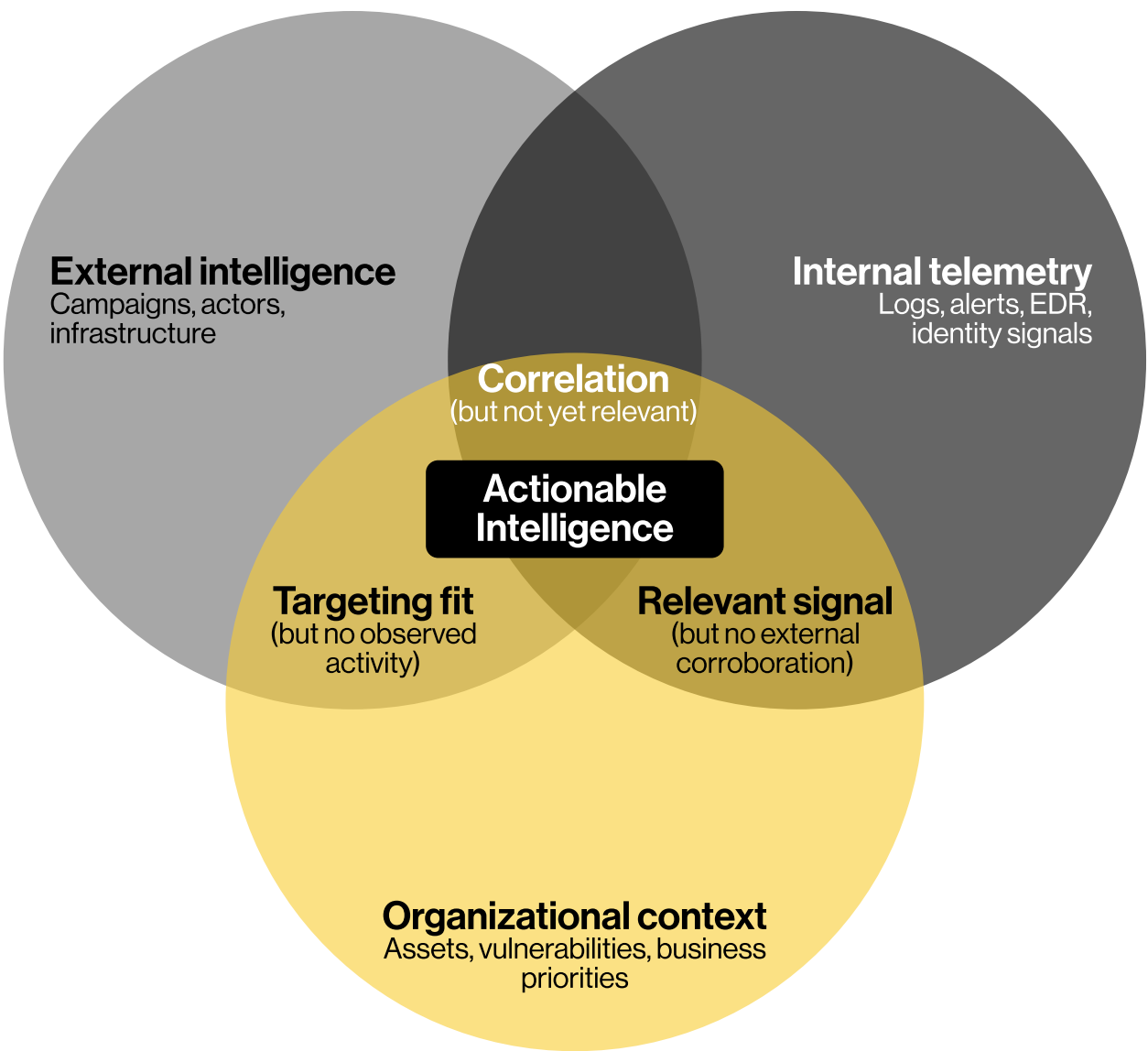
Without effective filtering and prioritization, the combination of external intelligence and internal telemetry can overwhelm analysts and obscure important signals. Automation can accelerate correlation, but it does not replace the need for relevance, corroboration, and context.

Context and Relevance

Even when intelligence from multiple sources is successfully correlated, determining whether that information is relevant to a specific organization remains difficult. External reporting may describe threats targeting industries, technologies, or geographic regions that do not apply to a particular environment. Intelligence artifacts may appear in internal telemetry without indicating malicious activity. Suspicious internal signals may also appear without immediately matching known intelligence reporting. Determining relevance, therefore, requires connecting intelligence artifacts with contextual information about the organization’s environment, including its systems, technologies, vulnerabilities, and operational priorities. When organizational context is absent, multi-source intelligence can still look rich while remaining operationally shallow.

Multi-source intelligence often disappoints teams that approach it mainly as a collection strategy. More reporting is easy to acquire. Relevance is harder to build. The breakdown happens when perspectives remain adjacent rather than connected, when data is accumulated without interpretation, and when external reporting never meets the internal conditions that determine whether action is warranted. Organizations fall short when separate perspectives are never connected, interpreted, and tested against the realities they are supposed to inform.

Actionable intelligence is the intersection, not what’s left after filtering



Each pair gets partway. Only the triple overlap supports action - and context is what gets you there, not what’s left after filtering.



From Assumed Coverage to Demonstrable Confidence

Threat intelligence programs require investment in data, technology, and people, yet many organizations still struggle to show what that investment has changed. Reporting is easy to point to. Defensive improvement is harder to demonstrate. That gap matters because access to intelligence is often treated as proof of value, even though access alone does not show whether the organization understood the right threats, prioritized correctly, or made better decisions.

Measuring Activity vs Impact

Many programs start with measuring the wrong things. Organizations count feeds, indicators, alerts, events blocked, or assets scanned because those numbers are easy to collect. Those metrics describe activity, not effect. A team can process large volumes of intelligence and still be unclear about which threats are relevant, which signals matter, or whether its defensive actions were appropriate. A more meaningful standard is whether the increase in intelligence justified confidence in the decisions. That confidence comes from showing how different intelligence perspectives were connected, how that connected view clarified relevance, and how it influenced investigation, mitigation, or risk decisions. Intelligence creates value when it helps an organization move from partial observation to a defensible understanding of what matters and what should happen next.

Measuring activity

Describes volume, not effect

- Feeds consumed

Volume

- Indicators processed

Volume

- Alerts generated

Volume

- Events blocked

Volume

- Assets scanned

Volume



Demonstrable confidence

Shows how intelligence influenced decisions

- Campaign linked to internal signals

Connection

- Corroboration across sources

Confidence

- Coverage gap identified and closed

Impact

- Investigation prioritized by context

Decision

- Risk decision defensible to leadership

Outcome



Demonstrable Confidence

Demonstrable confidence is the ability to explain, with evidence, how intelligence influenced defensive choices. A relevant campaign is identified through external reporting. Internal telemetry reveals related activity or confirms its absence. Existing controls are reviewed. Vulnerabilities, assets, and business context are examined. Based on that connected view, the organization investigates, prioritizes, blocks, mitigates, or escalates. When that sequence can be shown clearly, intelligence has done more than inform awareness. It has contributed to a defensive outcome.

Examples of demonstrable confidence include showing that a relevant campaign was identified through external reporting, correlated with internal observations, linked to exposed assets, and resulted in specific mitigations, investigation outcomes, or risk decisions. Evidence of this may include an investigation launched because connected reporting indicated the activity was relevant, a control updated because correlated intelligence exposed a coverage gap, or assets prioritized for remediation. After all, external exploitation matched internal exposure.

Even when an intelligence provider is strong, the question of the best provider remains too narrow. The question is whether the organization can demonstrate that connected intelligence improved the understanding of threats and decision-making. Confidence should come from showing how connected intelligence influenced defensive choices, not from assuming that a subscription delivered sufficient visibility.

Demonstrable confidence means being able to prove, through connected evidence and outcomes, that threat intelligence directly improved security decisions and defensive actions.



Conclusion

Multi-Source Is Necessary

Threat intelligence is often discussed as if the central problem were choosing the right provider or source. That framing is appealing because it turns a difficult analytical problem into a simpler procurement decision. It suggests that enough visibility can be bought if the right provider is selected. The reality is more complex and more consequential than that. No single intelligence perspective can reliably provide sufficient visibility into all adversary activity relevant to every organization. Each perspective reflects a particular vantage point shaped by its telemetry, investigative method, analytical focus, and environmental reach. Those limits make any single perspective partial. For that reason, the question of which provider is best is usually the wrong place to begin.

Organizations turn to multiple sources because they need more than additional reporting. They need broader visibility, corroboration, and better interpretation. Even organizations that believe they operate with a single-source model are usually already working across multiple perspectives through internal telemetry, investigations, vulnerability context, and operational analysis.

Connection Creates Value

The value of multi-source intelligence is realized only when separate observations are connected well enough to turn fragmented reporting into coordinated understanding. Hinge points make that possible. They connect reporting, telemetry, vulnerabilities, assets, and other observations in ways that clarify relevance, reveal exposure, and support action. Without those connections, intelligence remains fragmented and operationally shallow. With them, organizations can decide what is real, what matters, and what to do next.

Confidence Proves Value

The objective is to build enough connected understanding to decide what matters. The effectiveness of an intelligence capability is determined by how effectively the organization connects intelligence perspectives, interprets the signals they produce, and translates those insights into informed decisions and actions. Organizations that continue to treat threat intelligence as a single-source selection problem will keep overestimating coverage. Organizations that treat threat intelligence as a problem of connection, interpretation, and decision-making will make better decisions with greater confidence. One perspective is not enough because no one vantage point sees enough. Multi-source intelligence becomes operationally meaningful only when those partial views are connected well enough to determine what matters and what action should follow.





References

[1] Google Cloud Security. M-Trends 2024 Special Report: Executive Edition. Mandiant, 2024.
<https://services.google.com/fh/files/misc/m-trends-2024-executive-edition.pdf>