

Transforming Adversarial Insights into Actionable Strategies

Author: **James Nixon**



The Situation

Cybersecurity sucks. No, not as a job. As a job that needs to exist. If bad guys didn't do bad things, would it even be required? Considering we still need basic training on "do not accidentally post our customer list on LinkedIn", yeah, it will be required. But instead of addressing more mundane origins, cybersecurity teams have an unprecedented volume of intelligence, logs, training requirements, response demands, questions to answer, and even their existence is questioned while literally trying to stop some new ransomware script kiddie from accidentally leaking company jewels with some AI-generated zero-day.

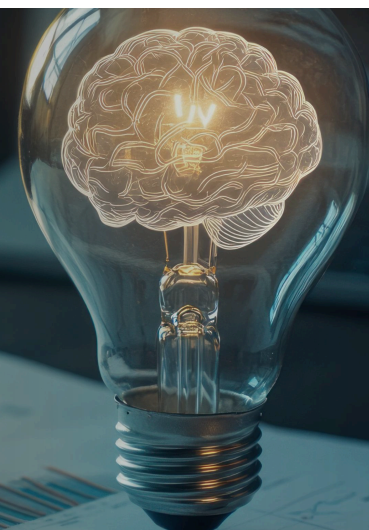
So maybe the job is hard and can suck, but the idea behind it does not, especially when you bring in intelligence. Because sharing cyber intel is fundamentally "I had a bad thing happen to me, how about you do not let it happen to you". Which is why, in all this volume, it is a terrible yet common outcome that shared intelligence still is not collected, not organized, not understood, and, worst of all, not actioned.

This document, from a threat intelligence platform vendor, aims to share thoughts on overcoming these challenges. Yes, we believe our platform can help with this. Otherwise, I would not have been granted marketing budget for the time to write and share this. However, I believe the principles can be applied to any organization. Also, behind the tools, it is the people who drive opportunities and policies.

I intend to encourage every team, of any size or mission, to shift from reactive security to proactive defense informed by real adversary activity. That you can connect your tools – SIEM, SOAR, XDR, firewalls, proxies, IDS, IPS, ABCs, XYZs, etc., into a systematic approach that de-fragments data for understanding, decision-making, and prevention. Yes, we at Analyst1 think a threat intel platform (ahem, ours) helps here too. But I'll do my best not to over-index on that as we go.



Starting with Adversary Insight



Awareness is not enough. Knowing APT5000 from “country” does bad things to your industry, or vertical changes nothing. We believe every step of intelligence must be focused on improving defensive outcomes. Better-trained people, better-deployed tools, better-managed allow/deny decisions.

Unfortunately, you all are facing an organized, persistent, and capable bad guys doing bad things. Advanced Persistent Threat (APT) groups and individuals change tactics, operate under different monikers, quickly shift infrastructure and geography, and use everything from cleverness to AI to bypass every control you put into place. But proactive defense is still possible.

Being more secure is more than alerts and logs. You need to understand:

- Who the adversaries are – tracking their identities, names, and origins
- What tools and malware they use for current immediate prevention and pattern recognition
- Which techniques they employ – to see above the technical specifics to their personality and comfort
- How their infrastructure changes over time – because patterns become good decisions

So, how do you learn this? Well, you have options. Some awful, some not. But all are available to all teams, depending on your ability to invest time, people, and actual financial cost. Listing them from most to least “expensive” on those variables:

- Direct dark web research – this is high-risk for your staff and high-cost across all variables; however, it is at the forefront of understanding what bad guys do next. Some organizations may find that, due to their attack surface, size, or global importance, they have to in-source this most critical function.
- Trusted intel vendors – as an intel platform, we enable the #GSD from intel, but do not provide it ourselves. There is a growing volume of cyber intel, 3rd-party risk, political intel, and other providers that do direct research, large-scale network monitoring, and assessments. Their output, threat reports/briefs/alerts/watches/warnings/etc., consolidates what many to most need to build their adversary pictures.
- Sharing communities / ISACs – common, but possibly overlooked in its true value, of being dedicated groups centered around the ideal of “if they hit me, they will not hit my peers” when sharing is done well. ISAC’s collection, research, and anonymization of attacks targeting its focused communities is the closest institutional effort we see to directly broker intelligence insights at the community level.
- Internal intelligence – I will try not to pontificate, but every hunt operation, closed ticket, incident response, vulnerability scan, and executive brief is necessary intelligence. If anything, as you see, this is “lower expense” because these are necessary operations; meaning they have to be done anyway, so pay the small “expense” to close the loop with their outputs as intel insights. Also, from what I see, this is of “highest value”. The points above all matter; however, tracking the actual successful or failed attacks against “you” for finding all the who, what, when, why, where, and how is just far, far more valuable. Especially when this internal perspective is the ideal pivot into every other intelligence form.



- Open intelligence – pick your website, blog, RSS feed, or some platform that, to be direct, makes revenue through advertising but genuinely shares valuable insights. Though there is no subscription, these internet sources have to do their best to be accurate and useful, or they cannot survive as publishers. Therefore, they cannot be overlooked and do need vetting. If you email **info@analyst1.com**, we will send you the current advised starting list we use with our customers.

Ok, that was longer than I wanted... I needed to ensure my perspective was clear. These are the source categories I keep in my head. The outputs above need to be organized to identify the patterns, trends, and real risks to you right now. If I say more here, it will feel too much like a “buy a TIP!” pitch. So I will not. I will instead focus on the principles of value of the above, and then move into the operational goals to follow as next steps, once the above is organized.

Start with Indicators of Compromise



I am 99% confident someone will throw their phone or laptop after reading that heading. If that's you, I'm not reimbursing your device. But if we meet at an event, I will buy you a chamomile tea.

Indicators of compromise (IOCs) are the “lowest tier in the pyramid of pain” and remain a bane of cyber teams' existence. Why? Because when you ask to block one wrong domain, whose head rolls? And when that happens, don't questions around the whole CTI process get thrown around?

However, when properly operationalized, in proactive defense and reactive assessments, they are undeniable sources of truth to work into maturation. Starting with IOCs is a valid starting point because there is no fluff or interpretation. With IOCs, it is binary, you will or will not:

- Block malicious infrastructure at **firewalls, proxies, or DNS controls**
- Detect suspicious activity within **IDS/IPS systems**
- Trigger alerts or investigations in **SIEM and XDR platforms**
- Identify malicious files and behaviors through **EDR telemetry**

It is binary because, one, you will push the IOC to those tools. Then, two, the bad guys did activity with that IOC or not. Ok, maybe it's quadrinary since that is technically two binaries, but you get the point. I hope...

Also, under the presumption that you have achieved good adversary telemetry, you can then use IOCs for true threat assessments. Yes! It is limited to what was actually tried against you and actually caught in auditing or alerts! But if the IOC is used as the branch back to reporting, tactics, approaches, and patterns, it can begin to build a whole picture.

It is one of the strong reasons we advise “block the obvious bad IOCs” early in our platform adoption (I said I would minimize, not avoid this completely, or marketing will not post this to LinkedIn) When you can home in on provable, recent actions, with vetting of the intel provider, the confidence to deny increases. Which then means you get to focus on allowed actions to triage incidents and move on to using IOCs to begin building context.

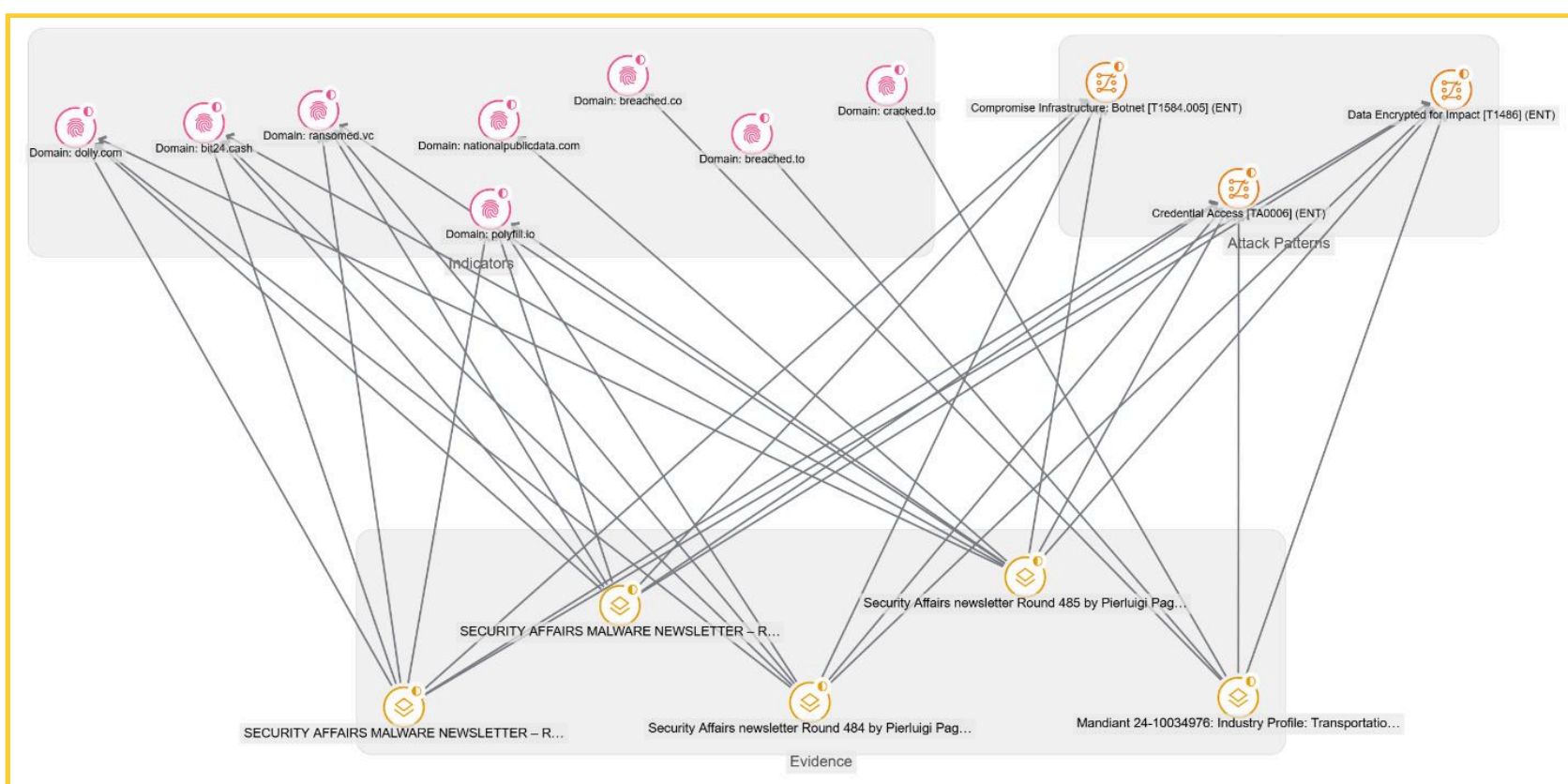


Building Adversary Context



Each blocked/attempted IOC is a piece of data that can intersect with the adversary's identity, recently used tactics, commonly abused malware, and the glorious CVEs they will exploit. (Seriously, without vulnerabilities, could bad guys even do bad things? And yes, I am including “human error” in the vulnerability bucket; looking at you, phishing clickers.)

Knowing how an adversary operates, when looking at the wealth of potential self-authored or collected reporting, can create some really pretty graphics and presentations. However, that is just potential. An adversary with multiple kinds of campaigns is noise relative to the signal of how they, or those like them, have actually attacked you before. That is why I went on at length above about “internal intelligence” and found that using IOCs as a signal to present current operations is valuable.



This lovely visual shows the idea, where the IOCs (red/pink nodes) pointed to overlapping reporting (yellow nodes) which had a common set of MITRE ATT&CK TTPs being discussed across all. Actual bad guy names have been removed for the fun of seeing if anyone can “guess” who this is talking about. Also deliberately used older reporting... please do not block these IOCs just because they are used here!

Intersecting the adversary’s potential campaigns with real, recent signals of attempts or successes suddenly changes the narrative. Focusing on the correctly associated malware families, TTPs (tactics, techniques, & procedures), the peers they target, or partner groups is valuable research time. Now the cyber intel teams producing hunt packages on related TTPs/IOCs spawned by real alerts/recent IOC hits become relevant.

Note: This is where MITRE ATT&CK can provide useful methods for mapping observed behaviors across campaigns. Though TTPs are often very observable, they still have a problem of being less directly detectable in tools. That is why signatures (Suricata, Yara, Grandpa Snort) are associated with ATT&CK, because they indicate that kind of TTP.



So why do you want to know all this? For security teams, this enrichment transforms isolated signals into meaningful intelligence. Instead of seeing a single domain or hash, or a single phishing variant, analysts can recognize patterns that reveal:

- How attackers establish persistence
- How they move laterally
- How they communicate with the command-and-control infrastructure
- Which techniques they rely on to evade detection

This context allows defenders to prepare for more than a single artifact—it enables them to prepare for the adversary's behavior. Which then makes you much better at making cost-benefit choices to defend yourselves proactively.

Tangent: Cost/Benefits?

Every cyber choice has a cost-benefit ratio. Briefly, time is the obvious cost when good tools are in place, and bad guys are not doing bad things, which is the obvious benefit we all want. There is also the cost of error, meaning the wrong IOC is blocked or the wrong perimeter policy is chosen, against the benefit of proactive defense. The reality I will not be tongue-in-cheek about is organizational risk. Behind all this paper and all cyber operations is some organization trying to do its job. Serve energy, fly planes, sell products, or operate our government. The reason for the organization is the point. Cyber defense is to remove the risk to those organizational operations and allow the organization's intent to exist to move forward without hindrance. You, as a member of the organization, have to advocate for and own the balance between cost/benefit and risk/reward as you move from contextual understanding to informed, proactive decisions. This is an immense responsibility, in my opinion. However, the cyber analysts I work with all demonstrate the quality and character I trust to do just this.



Decisions: Deny, Detect, Hunt, or Harden

If you understand the malware, TTPs, campaigns, geographies, and recency in all these factors of adversary behavior, you are “dangerous for good” in how you can move an organization. This is because at this conceptual point, you have mapped real activity to related, recent intelligence and then built some overall advice.



This lovely picture looks at “a specific country's actors” which happen to be relevant, showing their reporting over time, most common areas of attack, and then the origin IOCs which began the overall discovery up to this larger picture.

What should your advice be? If you want to improve defense, all of these need to be improved based on adversarial assessments.

Deny

Network controls can automatically block high-confidence malicious infrastructure. Firewalls, proxies, DNS systems, and intrusion prevention systems can deny communication with known adversary infrastructure.

Hunt

Lower-confidence intelligence or emerging techniques may warrant proactive search operations. Analysts can launch hunts across historical telemetry to identify previously undetected adversary activity.

Detect

When blocking may introduce risk or false positives, indicators and techniques can instead trigger detection alerts within SIEM, XDR, or EDR systems.

Harden

Technique-level intelligence can reveal systemic weaknesses in defensive posture. Organizations may respond by improving logging, strengthening authentication controls, or deploying new detection rules aligned to specific ATT&CK techniques.



Repeatable Intelligence-Driven Defense Loop

Operationalizing intelligence is not a one-time activity. It is an ongoing process that improves with each new observation.

A mature intelligence-driven workflow typically follows a cycle:

- 1 Collect intelligence from internal telemetry and external sources
- 2 Enrich and correlate indicators with malware, TTPs, and adversary context
- 3 Operationalize intelligence across security controls
- 4 Observe defensive outcomes through detections and telemetry
- 5 Refine intelligence models based on real attack attempts

Over time, this cycle transforms threat intelligence into a continuously improving defensive capability. Meaning, you are always getting better. You have to. Bored high schoolers have AI tools to mirror state-sponsored jerks. Aggressive posturing on deny/detect/hunt/harden choices, with continuous, humble, no-arrogance improvement, is how you stay culturally ahead of the game.

Measuring

With all this work, can you prove the value? Organizations often struggle to quantify the operational value of threat intelligence. However, several metrics can provide insight into whether intelligence is truly driving defensive action.

Examples include:

- Time from intelligence ingestion to operational deployment
- Number of indicators actively enforced across controls
- Detection coverage across relevant MITRE ATT&CK techniques
- Threat hunts initiated from intelligence insights
- Security posture improvements identified through campaign analysis

These measurements help ensure that intelligence programs remain focused on operational outcomes rather than information volume. Please, for God's good name, do not ever present the number of IOCs or reports collected alone. The above are examples that communicate actions and decisions, showing cyber operations at work. Sharing up simple raw, not operationalized counts sound cool; but would they reflect stopping the next ransomware event finding your weak spot?



Closing Thoughts

Threat intelligence becomes valuable only when it changes how organizations defend themselves. Period. Otherwise, it is like pen pals that do not write back to each other.

Indicators provide the first opportunity for action, enabling immediate blocking and detection. When those indicators are enriched with malware analysis, adversary techniques, and threat actor context, they reveal the behaviors and strategies behind current attacks directly affecting “you”. IOCs are never the end goal.

By operationalizing intelligence across the security stack, organizations can transform fragmented threat data into a repeatable defense workflow. We think our threat intel platform helps with this. The organizational comfort with making change, being proactive, and leaning forward in defense is, however, far more important than any specific tool.

The result, if done, is a shift from reactive incident response toward proactive defense informed by real adversary activity.

Whew. That was fun. And maybe one day we can make it so frustrating to succeed in cyber attacks that the bad guys get bored and go home. Like C.S. Lewis said, “badness is only spoiled goodness.” Could being so good at cyber defense cause a heart change in the adversary to use those competencies for nobler gains? Eh, not likely. But I am naïve enough to say “let’s try”.





 **ANALYST1[®]**