

BYOAI

NOT ANOTHER BLACK BOX

Why Analyst1 believes security teams should bring their own AI into intelligence workflows

AI is everywhere in cybersecurity right now. Every vendor is racing to ship it. Every pitch deck leads with it. Every product page promises faster investigations, smarter triage, and better analyst productivity. But beneath the marketing, a pattern is emerging that should concern every security team paying attention: vendors are shipping AI features fast, not AI features well. There goes that old saying, “you can have it fast, cheap, and/or good. You can only pick two though.” And in the rush to be first, they are asking customers to hand over the most sensitive part of their operation — how they think about threats — to models they cannot choose, infrastructure they cannot control, and reasoning they cannot inspect.

Analyst1 has watched this unfold and made a deliberate choice: we are not going to bolt a black-box AI onto the platform and call it innovation. Not because we are behind. Because we have seen what happens when security tooling prioritizes speed-to-market over operational trust. The question is no longer whether AI belongs in cyber. The real question is who controls it, and whether the architecture respects the operational realities that security teams live with every day.

Key Idea:

In cybersecurity, trust is not built by shipping faster. It is built by giving teams the control to verify, adapt, and own their workflows. That includes AI.

The problem with one-size-fits-all AI

Most AI features in security products today are delivered as a sealed layer. The vendor picks the model. The vendor decides where prompts are processed. The vendor controls what data leaves your environment and how reasoning is shaped. You get a chat window and a button that says “Summarize.” What you do not get is any say in the architecture behind it. That may be fine for autocompleting a support ticket. It is not fine when the workflow touches threat intelligence, active investigations, or mission-sensitive data that your organization has a legal and operational obligation to protect.



Security teams do not all operate under the same conditions. Some organizations have strict data residency requirements. Some already have approved model providers or private AI environments. Others need tighter human review, stronger governance, or the flexibility to change models as policy and technology evolve. A vendor-controlled AI layer forces all of those teams into the same box.

Why BYOAI is the right architecture for cyber

Analyst1's position is straightforward: the platform should do what threat intelligence platforms are supposed to do — structure data, automate correlation, manage workflows, and produce operationally useful outputs — and it should do those things exceptionally well without requiring AI as a crutch. Analyst1 already automates ingestion, extraction, deduplication, scoring, correlation, and orchestration across SIEM, SOAR, ticketing, endpoint tools and more. That is not the easy part. That is the hard part, and it is where most platforms fall short regardless of how much AI they layer on top. Where AI adds genuine value — in summarization, enrichment, hypothesis generation, or natural-language querying — the customer should control how it is deployed. That is what Bring Your Own AI means.

With BYOAI, security teams can choose:

- the model provider that best fits their security and compliance requirements
- where prompts and context are processed, including private or enterprise-controlled environments
- how much analyst review remains in the loop for summaries, pivots, enrichment, or triage
- when to optimize for reasoning quality, speed, cost, locality, or policy alignment

That flexibility is not a luxury. It is an operational requirement. In cyber, control over data flow, model choice, and explainability is part of the security model itself.

Why this matters for threat intelligence

Threat intelligence is not a chatbot use case. It is not summarization-as-a-service. The value of AI in intelligence work depends entirely on the quality of the structured data and workflows surrounding it. A model that summarizes garbage produces confident-sounding garbage. Analyst1's NLP extraction, automated indicator linking, evidence correlation, actor profiling, investigation graphing, etc. already provide the structured foundation that makes AI useful rather than dangerous. The platform does not need AI to function. But when a customer wants AI to accelerate what the platform already does well — summarize an investigation, generate a draft report, suggest pivots, or translate structured intelligence into natural language — BYOAI ensures they can do it with the model they trust, in the environment they control, with the analyst still in the loop.



The Analyst1 view

Analyst1 is not cautious about AI because we do not understand it. We are cautious because we do. We have built a platform that many federal and enterprise commercial organizations depend on for real intelligence operations — including CISA. We know that the moment you embed a model into a production intelligence workflow, you inherit that model's biases, limitations, data handling, and failure modes. We are not willing to make that choice on behalf of our customers. They should make it for themselves, with full visibility, and the ability to change course when the landscape shifts. That is what BYOAI delivers: not a feature, but a principle. Integrate the AI you have already vetted. Run it where your security policies allow. Keep analysts in the loop at the points that matter. And never lose the ability to trace a decision back to the evidence that produced it.

The future of AI in cybersecurity will not be won by the vendor that ships the fastest or brands the loudest. It will be won by the platforms that earn trust through transparency, deliver value through operational discipline, and respect that every security team operates under constraints that a one-size-fits-all AI cannot accommodate. Analyst1 is building for that future. BYOAI is not a stopgap while we figure out our AI strategy. It is our AI strategy. Because in this domain, control is not a feature request. It is a security requirement.

