Reducing Incident Response Time by 60%

How a security team used CiBRAI to improve response speed, reduce manual triage, and gain better visibility across its environment

Case study | Estimated reading time: 5 minutes

Representative scenario. This article presents a realistic enterprise response pattern based on common SOC bottlenecks, workflow compression opportunities, and blended human plus agentic AI operations.

Figure 1. High quality header visual showing a CiBRAI-enabled security operations environment with AI-assisted triage, unified telemetry, and human-led decision making.

The issue was not a lack of alerts. It was the time and cognitive effort required to turn alerts into confident action.

The real bottleneck was not detection

Most modern SOCs do not struggle to generate alerts. They struggle to turn those alerts into confident decisions quickly enough to matter. Detection has improved. Triage and investigation often have not.

That gap creates a familiar pattern. A signal lands in the SIEM, then the analyst pivots into endpoint telemetry, identity logs, email or cloud consoles, threat intelligence, case notes, and perhaps a SOAR workflow that automates only part of the journey. Every system contributes something. Together they create friction. Valuable minutes disappear while responders gather evidence that should already be coherent.

This representative case study began in that exact kind of environment. The team was capable and well tooled, but its operating model forced good analysts to behave like human middleware. Alerts were detected quickly enough. Decisions were not. Median response times for moderately complex incidents had stretched to a level leadership found increasingly hard to justify.

The problem was not a shortage of telemetry. It was a shortage of operational cohesion.

A representative environment under pressure

The organisation had assembled the kind of architecture seen across much of the industry: a SIEM, separate tooling for EDR and identity, cloud security consoles, threat intelligence feeds, case management, and a layer of scripts and workarounds that existed mainly because no single platform provided a complete picture. From a procurement point of view, the estate looked mature. From an analyst point of view, it looked busy.

That busyness had consequences. Alert triage often began with manual validation. Evidence gathering required repeated context switching. Investigations slowed because timelines had to be reconstructed from disconnected systems. Containment actions were possible, but operationally delayed, because the team needed to build confidence before acting.

Leadership did not want cosmetic improvement. It wanted a genuine reduction in response time without giving up governance or creating brittle over-automation. The brief was pragmatic: reduce manual triage, improve visibility across the environment, and help analysts move faster without surrendering judgement.

CiBRAI changed the operating model, not just the screen layout

CiBRAI was introduced as an operational layer rather than a rip-and-replace platform. That distinction matters. Security teams are rightly sceptical of grand transformation claims that require them to rebuild the SOC around a new product. CiBRAI focused instead on the problem that was actually hurting performance: fragmented context.

The design principle was simple. Bring context to the analyst instead of forcing the analyst to chase context. In practice, that meant using agentic AI to collect, correlate, and summarise evidence across existing systems, while keeping people firmly in charge of escalation decisions, containment authority, and business-impact judgement.

This moved beyond conventional automation. Traditional SOAR can be effective, but it often depends on long rule chains, brittle integrations, and a heavy maintenance burden. CiBRAI blended structured integrations with agentic workflows that could interpret incident context, assemble relevant evidence, and present it to responders in a more useful form. The analyst still made the call. The machine simply did far more of the repetitive lifting beforehand.

The response loop became shorter, clearer, and more disciplined

Once CiBRAI was embedded into the workflow, the team's response loop changed in a way that was both practical and measurable. Detection remained the trigger, but what followed became far more coherent. Relevant evidence was enriched automatically. Incidents were prioritised by likely impact rather than by raw noise. Investigation began from a unified case view instead of from a blank page. Recommended containment actions were surfaced with context and executed only when a responder approved them.

That last point was essential for trust. Security teams do not need theatrical autonomy. They need reliable acceleration with clear control boundaries. Human operators remained central throughout the process. Analysts decided when an incident warranted escalation, when containment was proportionate, and when broader business coordination was required. CiBRAI's role was to compress the time spent assembling facts so judgement could be applied sooner and with greater confidence.

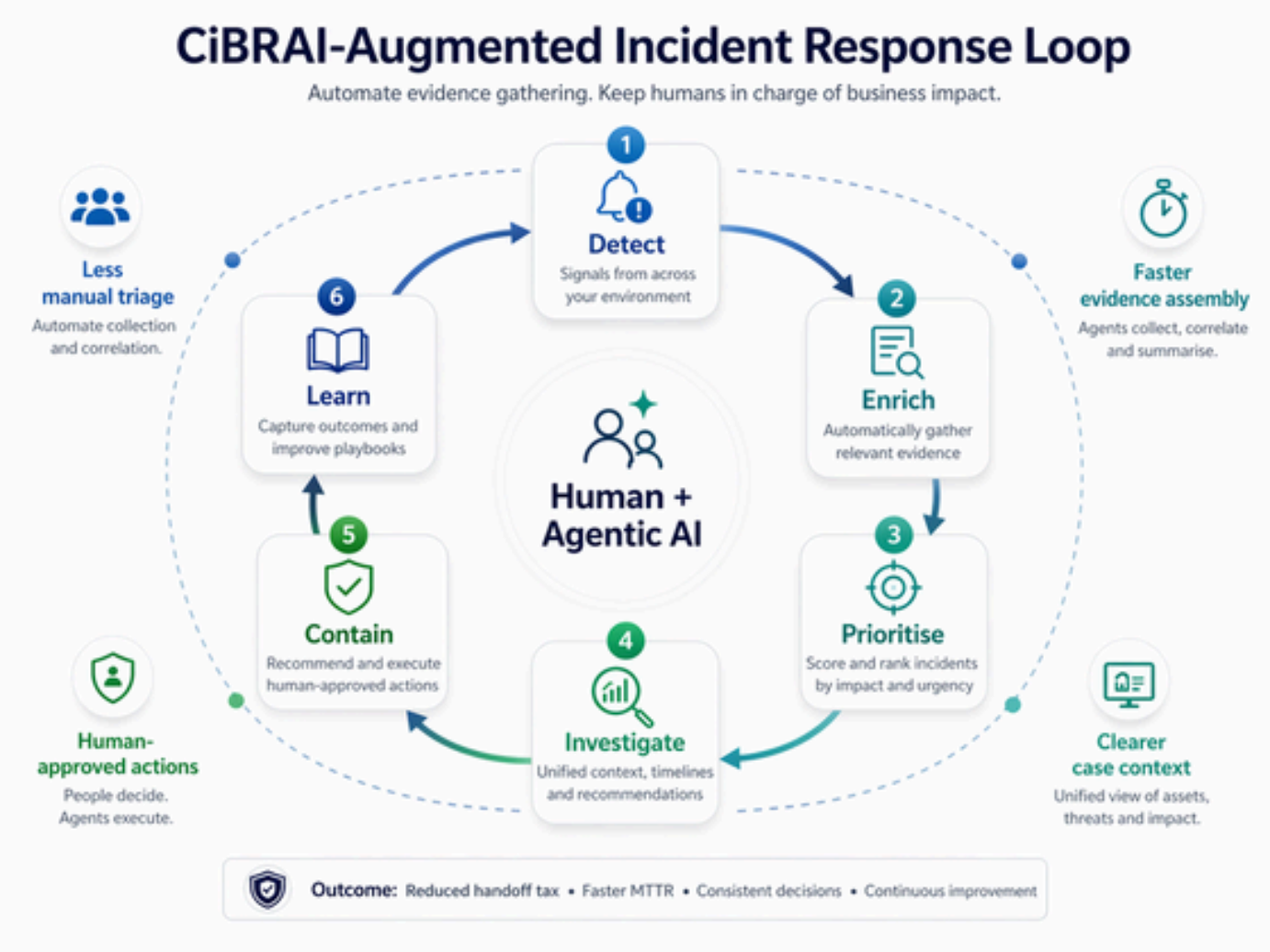

Figure 2. The CiBRAI-augmented incident response loop. Evidence is enriched and prioritised earlier, while containment remains human-approved and outcome driven.

Where the 60 per cent improvement actually came from

The headline number did not come from one dramatic feature. It came from cumulative gains across the workflow. Alert triage improved because analysts no longer had to verify the obvious by hand before deciding whether a case deserved attention. Evidence gathering accelerated because artefacts from multiple systems were assembled automatically instead of being hunted down one console at a time. Investigation time dropped because timelines, relationships, and likely paths of activity were already visible. Containment coordination improved because the team could move from a more complete picture with fewer internal pauses.

In representative terms, alert triage fell from roughly 25 minutes to 10. Evidence gathering dropped from around 40 minutes to 15. Investigation time reduced from about 60 minutes to 25. Containment coordination moved from approximately 25 minutes to 10. Viewed one by one, those reductions are sensible rather than magical. Together they are transformational. Median response time across comparable incidents fell by about 60 per cent.

The value was not that analysts were pushed harder or that critical decisions were handed to a black box. Time was saved by reducing ambiguity, eliminating repeated low-value work, and creating a far more coherent path from alert to action.

Figure 3. Representative workflow compression across triage, evidence gathering, investigation, and containment coordination.

Visibility mattered as much as speed

One of the strongest outcomes was not visible on a stopwatch. It was visible in the quality of understanding. Traditional SOC environments often present only fragments of reality. Endpoint tools know endpoints. Identity tools know identities. Cloud platforms know their own slice of the estate. The human responder is left to stitch those fragments together under pressure while stakeholders ask for confidence, scope, and likely business impact.

CiBRAI changed that dynamic by presenting a more unified case context. Analysts could see cross-domain relationships earlier. They could move from isolated indicators to an intelligible incident narrative without performing the same manual joins over and over again. That reduced cognitive load significantly. Responders spent less time proving to themselves that they had enough information and more time deciding what should happen next.

Speed matters in incident response, but speed without context is mostly just a faster route to rework. The more durable advantage is confidence.

Why this model fits the next phase of SOC evolution

The broader significance of the case study lies in what it says about the direction of cybersecurity operations. For years, the industry has responded to complexity by adding more products, more connectors, and more layers of orchestration. That approach can only go so far. Beyond a certain point, every new tool increases the management burden, the training burden, and the integration burden. Teams become impressive on paper and exhausted in practice.

The next step is not simply another dashboard. It is a more coherent operating model. That is why agentic AI has become such an important theme. Projects such as Glasswing and Mythos, along with the rapid improvement of cloud and on-premise large language models, point toward workflows in which machines do more of the assembly, correlation, and summarisation work that currently consumes human time. The real opportunity is not novelty. It is leverage.

CiBRAI fits squarely in that transition. Its value is not that it makes cybersecurity look futuristic. Its value is that it makes security operations work better.

A faster response is really a lower-friction response

Reducing incident response time by 60 per cent makes for a strong headline, but the more important achievement is simpler than that. The team removed friction. It reduced the amount of operational waste between detecting something suspicious and doing something useful about it.

That is the real lesson of this case study. Security operations do not become effective just because they acquire more telemetry or more automation. They become effective when the right people can understand the right facts quickly enough to make the right decision. CiBRAI helped this team get there by unifying context, compressing manual effort, and keeping the human operator at the centre of meaningful control.

For SOC leaders, the implication is hard to ignore. The future of incident response will not be defined by which organisation buys the most tools. It will be defined by which organisation creates the most effective partnership between human responders and agentic systems. The teams that get that blend right will not just move faster. They will operate with more clarity, consistency, and confidence when it matters most.

Suggested further reading

• Cisco. Global State of Security Operations Report.

• IBM Security. Cost of a Data Breach Report.

• Industry reporting and technical commentary on Project Glasswing, Mythos, and the emerging use of large language models in defensive security operations.

CiBRAI
CYBER INTELLIGENCE - BEHAVIOURAL RESPONSE