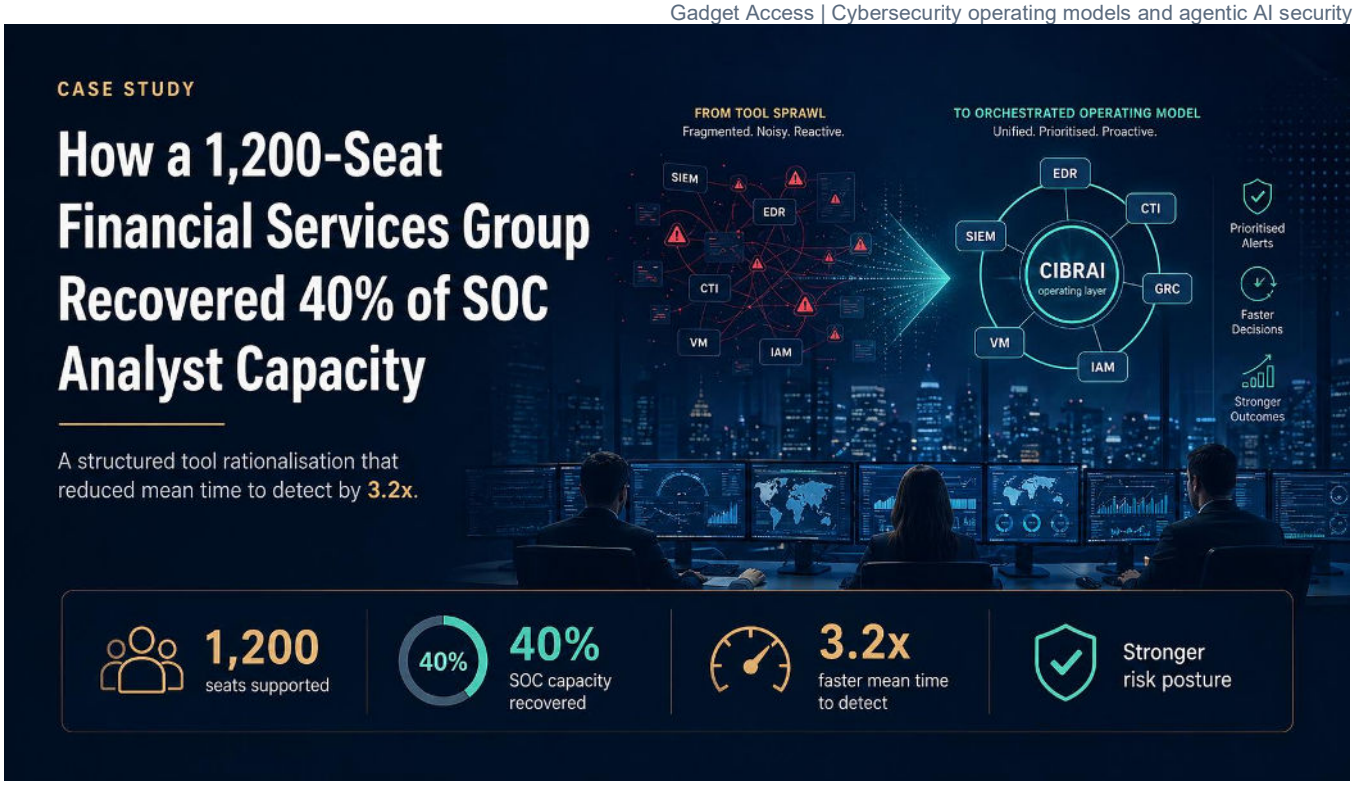

Case Study

How a 1,200-Seat Financial Services Group Recovered 40% of SOC Analyst Capacity

A structured tool rationalisation that reduced mean time to detect by 3.2x.

READ TIME	SECTOR	PRIMARY OUTCOME
5 minutes	**Financial services**	**40% SOC capacity recovered**

Security teams rarely recover 40% of their analyst capacity because someone bought a shinier dashboard. They recover it when someone has the nerve to ask a slightly rude question: which of these tools actually changes a decision?

That was the question at the centre of an eight-week engagement with a 1,200-seat Australian financial services group. The organisation was not immature. It had a modern SIEM, endpoint detection, identity controls, email security, a vulnerability scanner, threat intelligence feeds, ticketing, compliance tooling and reporting packs for management. It also had a familiar problem. Every control had its own queue. Every queue had its own owner. Every owner had a different definition of done.

The result was expensive operational drag. Analysts were busy, but too much of the work was swivel-chair triage, evidence copying, alert reconciliation and reporting archaeology. The SOC had plenty of signal. It was short on decision velocity.

The case at a glance

Client profile	1,200-seat financial services group with hybrid cloud, branch operations and regulated reporting obligations.
Starting point	37 cyber and compliance tools in scope, including 13 consoles used in routine analyst workflows.
Intervention	Structured tool rationalisation, evidence-flow redesign and a single case-and-control operating model.
Measured result	40% SOC analyst capacity recovered and MTTD reduced from 3h 12m to 1h 00m across priority use cases.
Sustained by	Gadget Access Continuous Compliance practices and the operating-layer pattern now formalised in CiBRAI.

Tool sprawl had become an operating model

The starting diagnosis was uncomfortable but useful. The SOC was not drowning because any one tool was bad. It was drowning because the tools had become the operating model. Analysts worked from the logic of licensing rather than the logic of investigations. A suspicious sign-in started in identity, moved to email, jumped to endpoint, detoured into the SIEM, then returned to a ticket where the evidence had to be pasted by hand. Somewhere in that journey, a human had to remember which dashboard was trustworthy this week.

The wider industry context made the finding more urgent. Panaseer has reported enterprise environments using an average of 61 security tools and 58 dashboards, with teams spending more than a third of their time gathering, analysing and reporting data. Tines has also found that analyst burnout is closely tied to tedious manual work, not a lack of commitment to the mission. In short, cyber teams are not short of screens. They are short of coherent flow.

Australian organisations are feeling that pressure directly. ASD's ACSC reported more than 84,700 cybercrime reports in FY2024-25, an average of one report every six minutes, and an average self-reported business cybercrime cost of $80,850. The same report notes that publicly reported CVEs increased by 28%. When the vulnerability queue grows and the SOC workflow fragments, the business inherits risk in the form of delay.

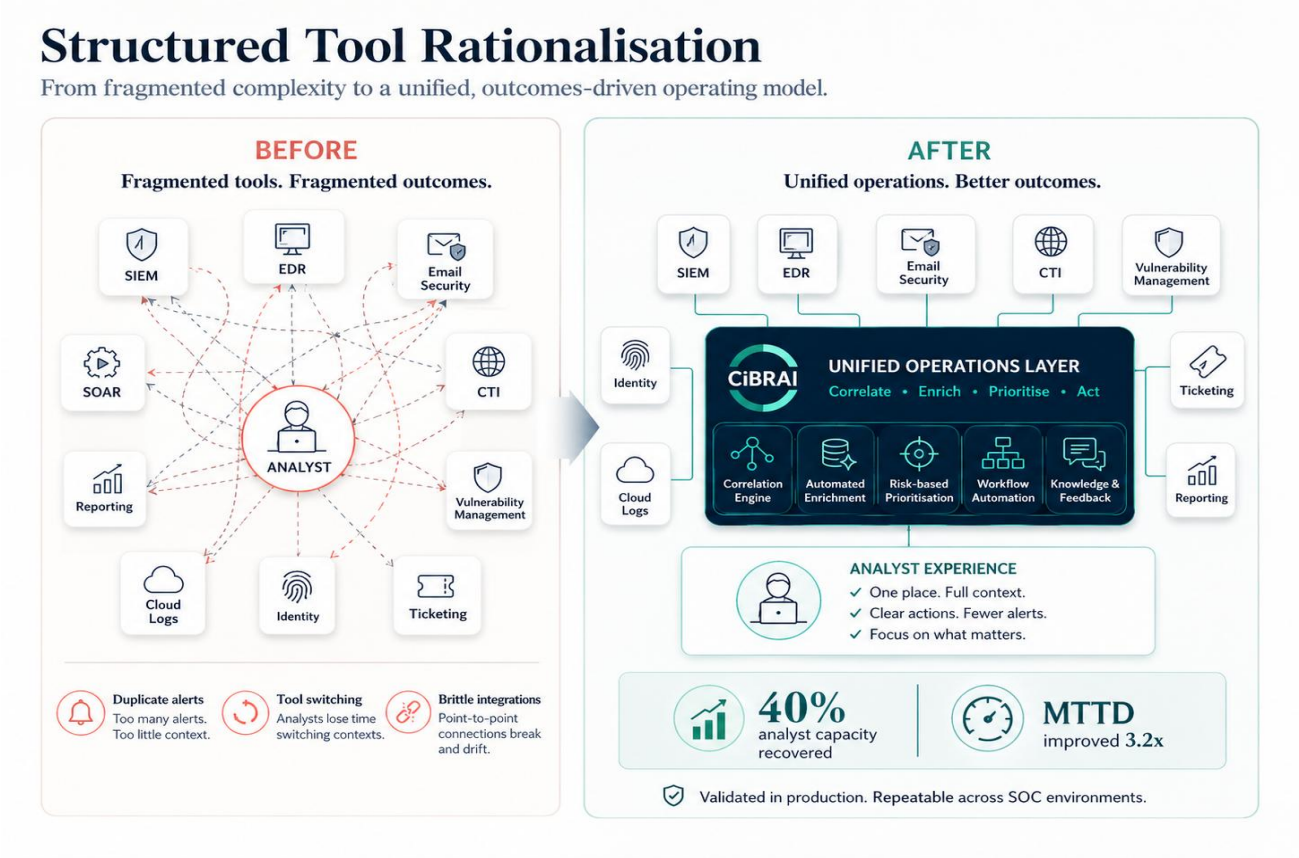

Figure 1. Tool rationalisation did not remove the need for SIEM, EDR, identity, vulnerability and compliance controls. It changed how analysts consumed them.

The rationalisation method

Gadget Access approached the work as an operating-model problem, not a procurement clean-up. The first step was to build a control-to-decision map. For each high-value use case, the team asked what the analyst needed to know, which tool produced the best evidence, which platform owned the workflow, and which person could approve the next action. This immediately exposed duplicate alerting and orphaned reports that existed because they had always existed.

The second step was deliberately practical. Tools were sorted into four categories: keep as a control, keep as a telemetry source, integrate into a common case workflow, or retire. That distinction mattered. A tool can be valuable without deserving a daily analyst console. A scanner, for example, may remain essential while its findings are normalised into a prioritised remediation queue rather than reviewed as yet another standalone dashboard.

The third step was to create a single case language. Priority detections, vulnerability exceptions, control evidence and incident actions were mapped into a shared taxonomy. This made handover cleaner and reporting less theatrical. Nobody should need a spreadsheet séance to explain whether a control is working.

The key insight: tool rationalisation is not a smaller shopping list. It is a clearer path from signal to decision.

What changed for analysts

After rationalisation, the analysts still had access to specialist tools. What changed was the daily path. Alerts entered a common triage pattern, evidence was assembled automatically where possible, and low-value duplicates were suppressed or demoted. The SOC lead could see whether a queue was genuinely growing or merely being counted in three places.

The recovered 40% was measured as analyst-hours removed from repeated low-value work over a normal operating month. Some of that capacity went back into faster detection. Some went into threat hunting, better detection logic, vulnerability validation and control tuning. This is the part of SOC improvement that budget discussions often miss. A saved hour is only valuable if it is reinvested into better decisions, not silently absorbed by the next wave of noise.

The group also changed how compliance evidence was handled. Gadget Access applied its Continuous Compliance framework so control evidence could be captured as part of normal operations. Essential Eight, PSPF, ISM, ISO 27001:2022 and NIST obligations were no longer treated as separate audit-season rituals. The same evidence that explained a security decision could support management reporting and uplift planning. That is a less glamorous sentence than 'autonomous SOC', but it is the sort of sentence boards should enjoy. It saves money.

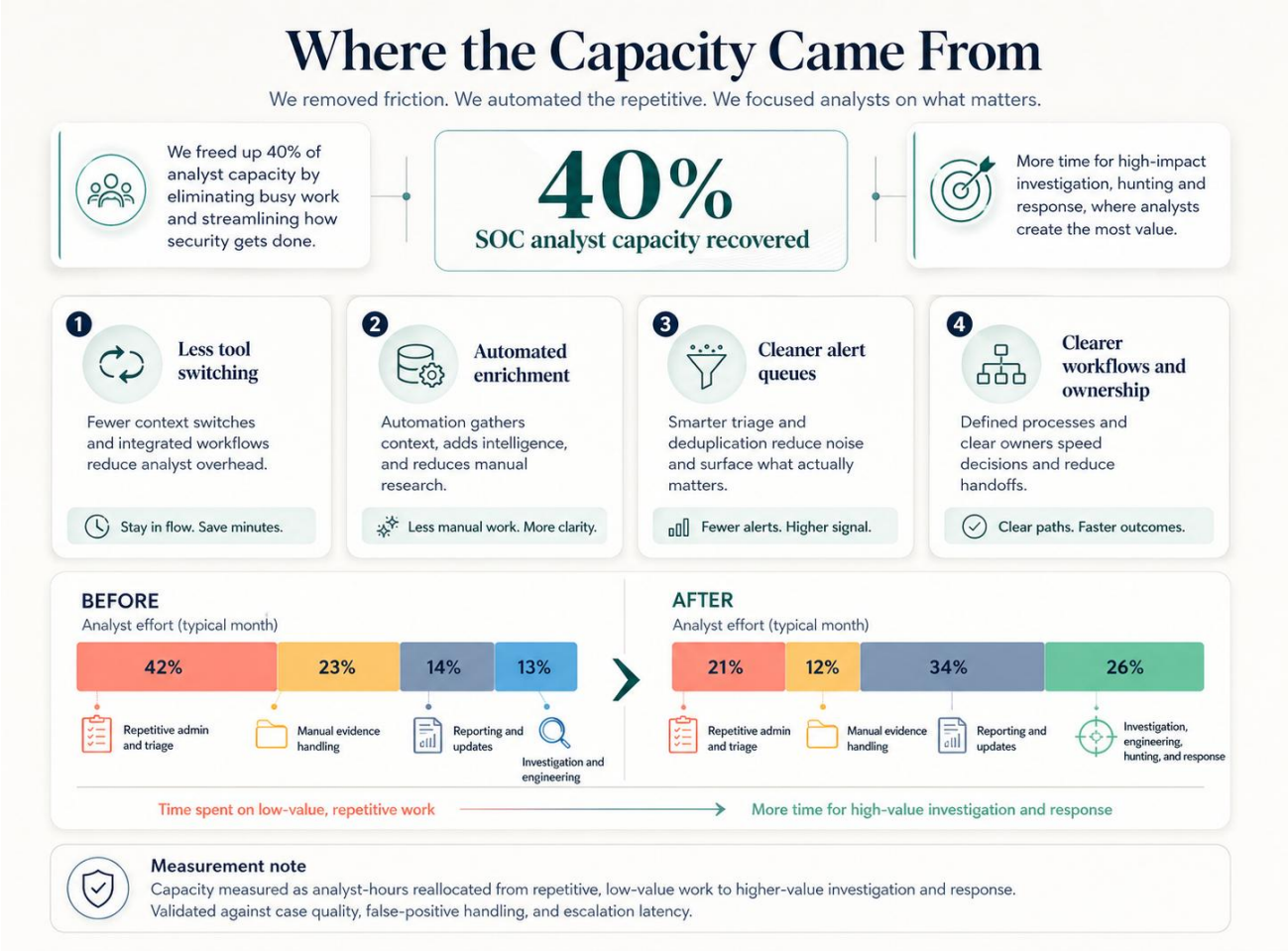

Figure 2. The programme recovered capacity by removing low-value work, not by pretending analysts could simply do more.

MTTD improved because ownership improved

The headline metric was mean time to detect. Across the agreed priority use cases, measured MTTD fell from 3 hours 12 minutes to 1 hour. That is a 3.2x improvement, but the number is less interesting than the cause. The improvement came from correlation, clean escalation paths and pre-agreed decision rights. When the analyst knew which evidence mattered and which action owner was accountable, the clock stopped being wasted on interpretation.

This distinction matters in the age of AI-assisted offensive security. Mandiant's M-Trends 2025 observed exploits as the most common initial infection vector in the cases it investigated, while Verizon's 2025 DBIR found vulnerability exploitation growing as an initial access step and perimeter-device remediation taking a median 32 days. Anthropic's Project Glasswing and Claude Mythos Preview push the industry toward the same conclusion from a different angle: vulnerability discovery is accelerating, so defensive operations must reduce waiting time between signal, prioritisation and action.

The lesson is not panic. The lesson is that defenders need operating models that can absorb new defensive AI without creating yet another queue. CiBRAI is designed around that principle. It can integrate approved on-premise and cloud LLMs for summarisation, evidence correlation and playbook support while keeping containment, exception and policy decisions under human governance. That means organisations can adopt newer defensive model capabilities without rebuilding the SOC every time a model improves.

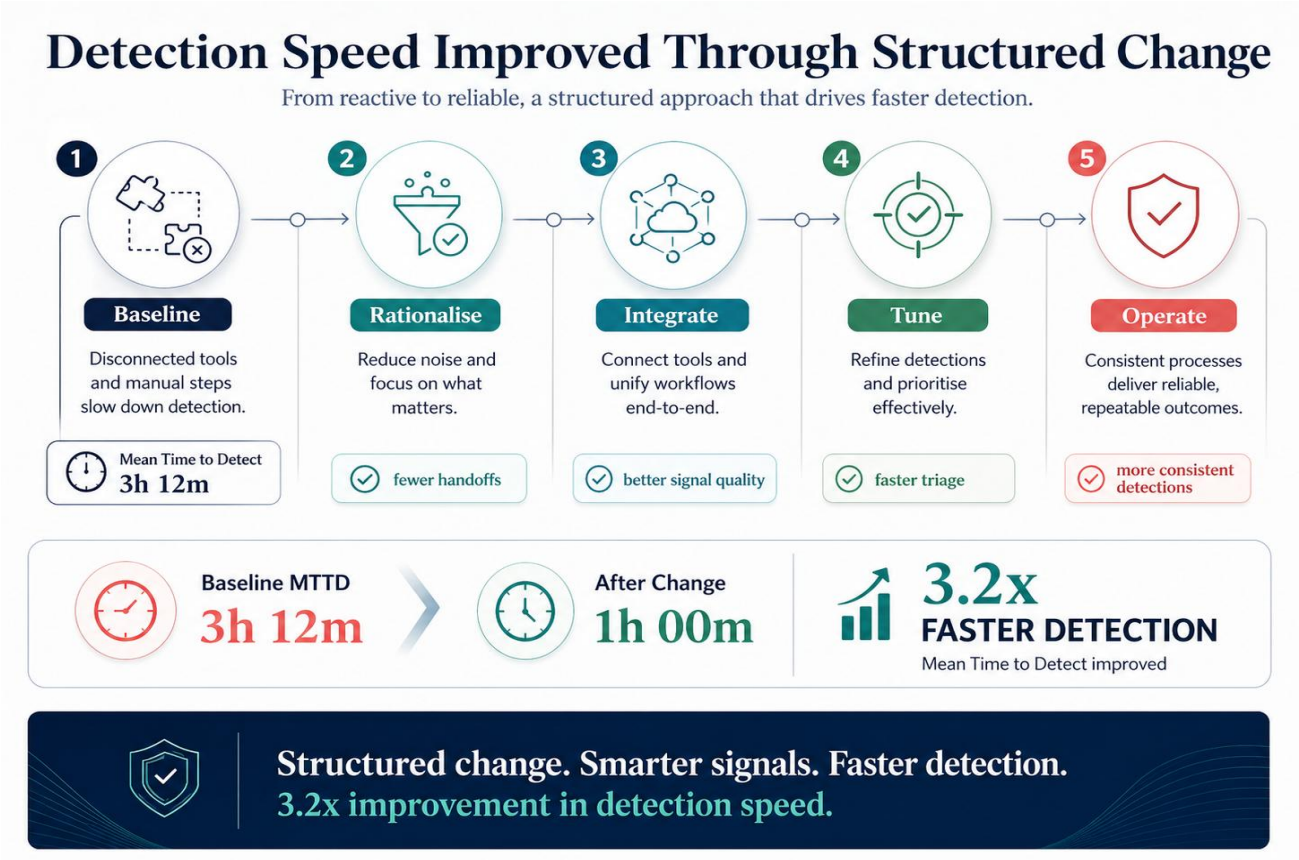

Figure 3. The 3.2x MTTD gain came from cleaner evidence flow and clearer decision ownership.

The board-level result

The board did not receive a diagram of every API call. It received a simpler message: fewer daily consoles, fewer duplicate queues, faster detection and a more reliable evidence base for compliance. That made cyber uplift easier to fund because the discussion moved from tool count to operating performance.

The group retained the controls it needed and removed the operating friction it did not. Some licences were retired. Some were renegotiated. Some were kept but taken out of the analyst's daily path. The most important saving, however, was not the line item. It was the return of analyst attention.

For financial services, government and critical infrastructure environments, that attention is becoming the scarce asset. AI will produce more vulnerability intelligence. Threat actors will automate more reconnaissance. Regulators will ask for clearer evidence. The answer is not to assemble a cybersecurity junk drawer and hope the handles line up. The answer is to simplify the operating model until good decisions become easier than bad ones.

How Gadget Access helps

Gadget Access brings 30 years of IT, cybersecurity, infrastructure, networking and vendor-management experience to this kind of problem. The work can look like vCISO support, technical consulting, vendor rationalisation, control testing, compliance uplift, reporting redesign or a full cyber operating-model reset. The common thread is pragmatic: make the environment more defensible, more explainable and less exhausting to run.

CiBRAI and the Continuous Compliance framework are how Gadget Access packages that thinking for the next era of cyber operations. The aim is not to replace the human analyst. It is to stop wasting them.

References and further reading

- Australian Signals Directorate. Annual Cyber Threat Report 2024-2025.
- Australian Signals Directorate. The Commonwealth Cyber Security Posture in 2025.
- Verizon Business. 2025 Data Breach Investigations Report.
- Google Cloud Mandiant. M-Trends 2025: Data, Insights, and Recommendations From the Frontlines.
- IBM. Cost of a Data Breach Report 2025.
- Tines. Voice of the SOC Analyst.
- Panaseer. Cybersecurity control failures cost enterprises $14 million a year.
- Anthropic. Project Glasswing: Securing critical software for the AI era.

Note: The client profile is anonymised. Non-material identifying details and exact platform names have been withheld, while the operating pattern and outcome metrics are presented for practical learning.