

# Know the threat. Act sooner. Protect more.

## Operational intelligence for Australian law enforcement.

Connect cyber defence, crime analysis and response in a sovereign platform, with specialist AI teams working under your authority.



NSW • QUEENSLAND • FEDERAL LAW ENFORCEMENT

Illustrative operational scene

## 84,700+

Cybercrime reports to ReportCyber in FY2024-25.  
About one every 6 minutes.

## >280%

Growth in DoS/DDoS incidents responded to by ASD's ACSC.  
More than 200 incidents.

## A\$80,850

Average self-reported business cybercrime cost.  
Up 50% year on year.

ASD FY2024-25 national figures. [1] Reports are not unique police cases. DoS/DDoS means denial-of-service attacks. The cost figure concerns business reports, not police breaches or the total cost of an incident.

## Every handoff can cost an opportunity.

Disconnected alerts, intelligence, case notes and approvals consume scarce analyst time. CiBRAI carries context from the first signal to a reviewed intelligence product and an authorised response.



### Faster validated leads

Enrich suspicious emails, domains, identities and endpoint activity in one workflow. Reduce repeated searching so investigators can test leads and act while the information is useful.



### Sharper actor insight

Connect indicators, infrastructure and MITRE ATT&CK behaviours. Retain source, recency and confidence to test threat-actor hypotheses and distinguish supported links from assumptions.



### Stronger case records

Build source-linked chronologies, capture decisions and retain records under agency controls. Better-prepared material supports specialist review while controls protect victims, intelligence and essential services.

#### NSW POLICE / FORCE2030 [2]

Technology, streamlined processes and accountable service. Configure shared context around commands, approved data and operational responsibilities.

#### QUEENSLAND POLICE / 2026-30 [3]

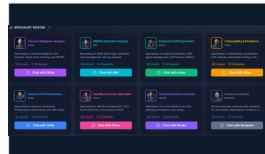
Trusted AI, integrated intelligence and evidence-informed investment. Strengthen frontline capacity while making operating effort and value visible.

# Eight connected workspaces.

A complete operating environment for intelligence, investigation, response and continuous compliance. Connect existing investments and carry operational context between teams.

## 01 ASSISTANT

Scale specialist capacity



Cyber Teams, reusable skills, visual playbooks, tool permissions, approvals, audit traces and cost analytics.

Run supervised research and triage in parallel. Give investigators more capacity while controlling tools, spend and authorised actions.

## 02 OBSERVE

Share the operational picture



Command Centre, War Room, security timelines, dashboards, SOC metrics and operational risk views.

Align commanders, cyber teams and analysts on priority incidents, service impact, handovers and the next accountable action.

## 03 INTELLIGENCE

Understand adversary tradecraft



CTI, indicator enrichment, MITRE ATT&CK mapping, Dark Web Monitor and approved OSINT research.

Connect behaviours and infrastructure, recognise related activity and test threat-actor hypotheses with source and confidence retained.

## 04 DETECT

Surface what needs attention

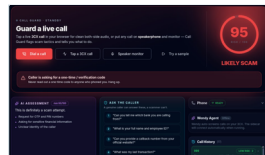


SIEM alerts, endpoint and network telemetry, anomalies, detection rules, vulnerabilities and response actions.

Bring signals from agency systems and exposure context together. Prioritise suspicious activity and reduce manual preparation before investigation.

## 05 INVESTIGATE

Develop a coherent case picture

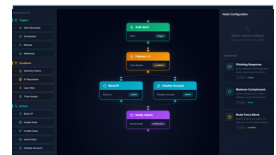


Global Search, Attack Stories, evidence artefacts, Email Analyser, Scam Watch, domain checks and sandbox analysis.

Bring approved records and technical artefacts together to assess cybercrime leads, document findings and prepare material for specialist review.

## 06 RESPOND

Turn findings into action



Cases & Incidents, forensics, playbooks, Project Rooms, Report Studio and incident exercises.

Assign validated findings, coordinate approved containment and record decisions. Keep analysts, service owners and responders working from shared context.

## 07 MANAGE

Keep protection and assurance current

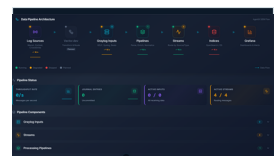


Asset inventory, patching, application control, ransomware readiness, compliance workflows, training and CISO views.

Assign remediation and reuse operational evidence for applicable controls. Protect sensitive information and the services communities depend on.

## 08 CONFIGURE

Fit the agency, command or client



Integrations, data pipelines, tenants, Sigma Rules, activity logs, scheduling and platform health.

Shape data access, separation and workflows around agency boundaries. Connect approved systems and sustain controlled operational growth.

# Add specialist capacity. Keep human command.

Increase the analytical capacity available to the force. CiBRAI virtual team members can work on approved enrichment, triage, investigation support and reporting tasks in parallel, with officers directing the operation.



## Eight digital specialists. One directed team.

Assign a mission, approved sources and tool permissions. Specialists prepare findings; people validate the evidence and authorise operational action.

Add statistical analysis of approved, aggregated crime and workload data, with checked definitions and human review. [5]

Illustrative CiBRAI virtual specialists, not sworn officers. The configured role descriptions below are grounded in the platform's specialist roster. [7]

### OLIVIA / Threat intelligence

Enrich indicators, map adversary tradecraft and prepare source-backed hypotheses for analyst validation.

### AMAN / Endpoint & EDR

Examine endpoint context and forensic artefacts; prepare containment options for human approval.

### SOFIA / Network & infrastructure

Connect network activity, dependencies and suspicious infrastructure to service and investigation context.

### DEVIKA / Communications security

Support suspicious communication analysis, phishing workflows and scam-related technical research.

### MEI / SIEM & detection

Triage alerts, correlate logs and help tune rules to focus attention on meaningful activity.

### ADAM / Vulnerability & exposure

Analyse vulnerabilities and exposure to prioritise weaknesses that threaten operational systems.

### GRACE / Identity & access

Examine access patterns and identity context to support investigation of compromised accounts.

### BENJAMIN / Research & briefings

Draft source-linked case notes, research summaries and statistical briefs from approved material for review.

#### ILLUSTRATIVE CAPACITY MODEL / 1,000 ROUTINE ITEMS PER MONTH

Manual



250 h

AI-assisted



150 h

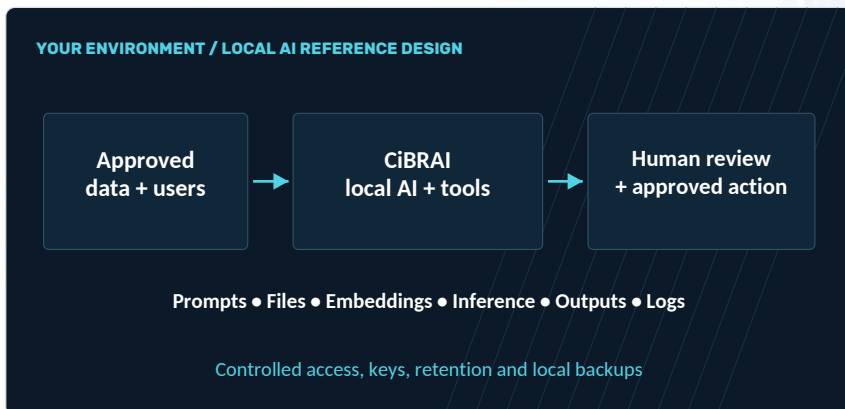
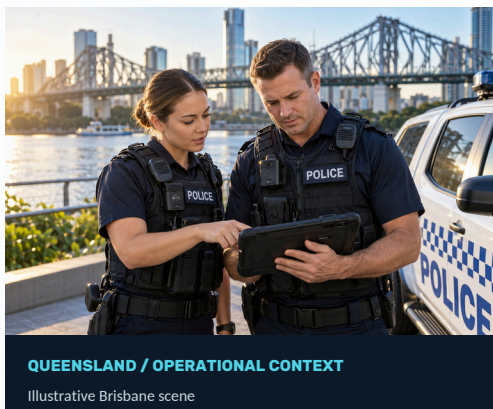
**100 h**

Capacity returned / month  
40% less effort for this task

Assumptions: 15 manual minutes versus 9 assisted minutes per item, including human review and exceptions. Timings are illustrative, not measured CiBRAI results. Validate quality and usable capacity in a pilot.

# Australian control. Operational value.

A platform and operating partnership built around the information you protect, the services you deliver and the outcomes your team is accountable for.



**Keep sensitive AI interactions inside your environment.** Dedicated Australian hardware, on-premises or private deployment. Block public AI endpoints and outbound model telemetry in the configured local design. Validate source permissions, egress, backups, operator access and classification before use. [4,6]

## CO-MANAGE THE CAPABILITY

Tailor alerts, specialist teams and playbooks to operational priorities. Agree service hours, escalation, access and response authority. Review control evidence and remediation together.

## MEASURE WHAT IMPROVES

Measure time to validated leads, analyst effort, backlog, evidence completeness, rework and authorised containment. Track cost per intelligence product and contribution to case outcomes.

## A\$144k / year

Illustrative capacity value: 100 hours/month × 12 × A\$120/hour. Capacity is not cash savings. Assess net value after deployment, infrastructure, platform, services and additional assurance costs.

**Security providers:** protect client records, control-room identities and remote access. Scope telemetry from alarm, CCTV and access-control environments; separate clients and tune escalation to site and contract priorities. [8]

### SOURCES & SCOPE / 10 SEPTEMBER 2026

1 ASD: Annual Cyber Threat Report 2024-25.

2 NSW Police: FORCE2030 strategic framework.

3 QPS: Strategic Plan 2026-30; 100-Day Review, rec. 59.

4 ASD: Engaging with AI; ethical AI principles.

5 QPS: Maps and statistics / interpretation guidance.

6 PSPF: NSW Cyber Security Policy.

7 CiBRAI platform brochure (supplied, 2026) / platform.

8 ASIAL: Electronic Security Standards.

*"Operational cyber intelligence and understanding threat actors can make the difference between a successful operation and a missed opportunity. Good systems help a good team respond faster, with the context to achieve better outcomes."*

**ANDREW CURTIS / FOUNDER & CEO, CiBRAI**

## Give your team the capacity to act sooner.

Book a confidential call. Scope one use case and its operational value.

[support@cibrai.com](mailto:support@cibrai.com) | 1800 928 982 | [www.cibrai.com](http://www.cibrai.com)

Australian technology. Australian services. Sovereign capability. Illustrative imagery; no agency endorsement implied.

