

Clarity. Not Chaos.

The Agentic AI Cybersecurity Operating Platform

One platform. Every mission.

Disconnected tools slow teams down. CiBRAI connects SIEM, SOAR, intelligence, investigation, response and compliance in one operating environment. Specialist AI assistants carry context through the work, helping people prioritise threats, coordinate action and turn evidence into improvement.

AUSTRALIAN OWNED. SOVEREIGN OPTIONS.



More capability. Less operational friction.

Built on decades of delivery experience. Augment your SOC or establish a complete capability.



See the incident that matters

SIEM, CTI, behaviour and asset context help prioritise meaningful threats and reduce repetitive triage.



Extend the capacity of your team

Specialist agents support analysis, research, notes and reporting so people can focus on judgement.



Move from insight to action

Cases, response actions and visual playbooks carry the investigation into coordinated containment.



Turn cyber activity into assurance

Compliance, patching, risk views and evidence connect operational findings to visible improvement.



Make existing investments work harder

Integrations, APIs and data pipelines connect your tools and reduce manual handoffs between consoles.



Keep control as you scale

Approvals, trace records, cost analytics and tenant management support accountable operations.

ONE SHARED OPERATING CONTEXT

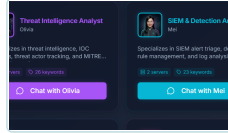
Signals + intelligence → Investigation → Authorised response → Remediation + evidence

Eight connected workspaces.

A complete operating environment, with purpose-built tools for every stage of cyber work.

01 ASSISTANT

Scale expertise. Govern execution.



Configure cyber teams and reusable workflows, then control how agents use tools, spend and act.

Cyber Teams · Skills Library · Agent Flow · Swagger-MCP Integration · Trace (Audit) · Approvals · Tool Catalog · Playbooks and Visual Editor · Cost Analytics · Design Systems

02 OBSERVE

Give every role a shared operational picture.



Unify live events, performance and risk so analysts, incident commanders and leaders can align.

Command Centre · Dynamic Dashboard · Attack Map · World Monitor · War Room · SOC Metrics · Security Timeline · Risk Radar

03 INTELLIGENCE

Put adversary context into decisions.



Research threats, enrich indicators and map activity to tradecraft to sharpen investigation priorities.

Threats · CTI Dashboard · Dark Web Monitor · MITRE ATT&CK · OSINT Lab

04 DETECT

Connect signals to what needs attention.

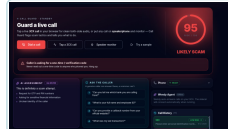


Bring telemetry, exposure and behaviour together to identify suspicious activity across the estate.

SIEM Alerts · Network Monitor · Agents & Assets · Endpoint Security · Detection Rules · Response Actions · Vulnerabilities · Anomaly Detection · Impossible Travel

05 INVESTIGATE

Follow the whole story. Preserve the evidence.



Search across data and specialist analysis tools to understand scope, identity, infrastructure and impact.

Global Search · Saved Searches · Attack Stories · Log Search · Artifacts & Evidence · User Analytics · Email Analyser · Scam Watch · Scam Domain Check · Call Guard · Sandbox Analysis · Cloud Security · Network Topology · BloodHound AD · Risk Scoring

06 RESPOND

Coordinate action with accountability.



Connect cases, people, response workflows and reporting; rehearse and improve your response capability.

Cases & Incidents · Forensics · AD Response · Report Studio · Project Rooms · IR Drills · Playbook Builder · Offensive Security

07 MANAGE

Keep security posture moving forward.

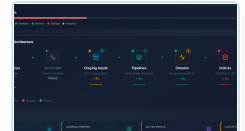


Join assets, endpoint controls, patching, readiness and governance in a practical improvement workflow.

Deploy Agent · Asset Inventory · Endpoint Groups · Sysmon Config · AppLocker Manager · Patch Management · CISO Console · Compliance · Ransomware Readiness · Patch & Update Status · Cockpit Console · GPU Monitoring · Knowledgebase · Security Training · Dev Logs · User Engagement · User Profile · Admin Panel

08 CONFIGURE

Shape the platform around your operation.



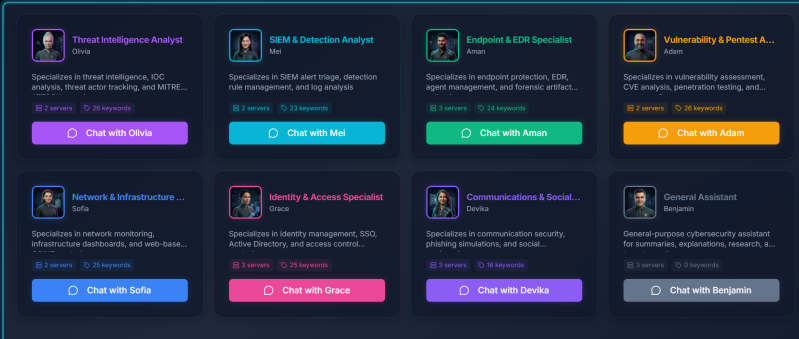
Connect data and services, manage tenants and rules, and maintain visibility of platform health.

Integrations · Graylog · SIEM Data Pipeline · Vector Pipeline · Grafana Dashboards · Platform Health Alerts · Customers · Tenants · Healthcheck · Scheduler · Sigma Rules · Activity Logs · Services & Containers

Illustrative product views. Feature availability and integration scope are agreed for each deployment.

Specialist assistants. Real cyber work.

Turn scarce expertise into a repeatable operating capability, with people directing the work.



Your cyber team, extended

Threat intelligence. Detection engineering. Endpoint and EDR. Vulnerability and pentest analysis. Network operations. Identity and access. Communications security. General assistance.

CIBRAI specialist roster | product interface detail

FROM REQUEST TO ACCOUNTABLE ACTION

01 DIRECT

Define the task, team and operating scope.

→ 02 REASON

Collect context and prepare the next action.

→ 03 AUTHORISE

Apply tool permissions and human approvals.

→ 04 EXECUTE + TRACE

Run the workflow; retain actions and evidence.

Reusable skills + visual playbooks + Swagger-MCP tools + cost visibility

Close the loop on exposure

A suspicious login becomes more useful when it is connected to endpoint activity, the affected asset and the user's role. CIBRAI brings search, attack stories, risk scoring and case handling into the same workflow.

CONTINUOUS COMPLIANCE IN DAILY WORK

Use asset, patch, application control and readiness data to support Essential Eight and ISO 27001 evidence workflows. CISO views connect findings, risk and improvement work, helping teams keep assurance grounded in operational reality.

Extend cyber into fraud and scams

Email Analyser, Scam Watch, Scam Domain Check and Call Guard support the investigation of suspicious communications. SIP-integrated call workflows can add live scam context and agent-assisted interaction.

FRAUD AND AML INVESTIGATION SUPPORT

Extend agentic workflows across indicators, research and case evidence to help specialists assess suspicious activity. Configure the data sources, controls and expert review for the mission, retaining human accountability for decisions.

SOVEREIGN AI. FROM CLOUD TO RACK.

Choose where the capability runs.

Local data. Local models. Local control.

Australian sovereign services, private and on-premises deployments, and engineered disconnected options. Custom water-cooled GPU solutions bring local AI into the rack, with clustering, GPU monitoring and environmental and cost visibility.



Hardware image is conceptual. Final configurations, compatibility and operational qualification are application-specific.

Australian capability. Wider possibilities.

From the smallest cyber team to a sovereign defence installation.



Government & defence

Design sovereignty, oversight and deployment around the mission, from Australian services to private installations and custom in-rack GPU capability.



Healthcare & aged care

Bring asset, endpoint, vulnerability and response work together to protect sensitive information and support continuity of essential clinical services.



Transport, utilities & industry

Build a shared picture across distributed IT and OT estates. Align response and local deployment to operational dependencies and availability needs.

SME & growing businesses

Monitoring, investigation and reporting in one platform. Give small teams specialist assistance, clearer priorities and structured security workflows.

MSPs, MSSPs & partners

Manage multiple customers and tenants centrally. Reuse approved skills and playbooks, coordinate delivery and generate clearer customer reports.

Banking, payments & finance

Connect threat, identity and communications context. Support fraud, scam and AML investigations with evidence, approvals and accountable case handling.

Build with CiBRAI.

Cybersecurity partners welcome. Bring us a service model, integration challenge or specialist mission. Custom teams, tools and workflows can be configured and rapidly deployed to an agreed scope.



“We are proud to pioneer Australian agentic cyber defence. Sovereignty means the freedom to decide, act and improve on our own terms. CiBRAI brings human judgement and autonomous capability together in an independent, future-focused platform built to protect what matters.”

ANDREW CURTIS | FOUNDER & CEO, CiBRAI

Andrew brings more than 30 years of technology entrepreneurship and over 20 years in cybersecurity. He built a 90-person technology business. Today, the CiBRAI team combines security architecture, cyber operations, governance and AI engineering, with experience advising Australian and allied governments and working across enterprise, banking, payments, health, aged care, transport and utilities.

Our team's experience includes work with Telstra, NSW Police, CSIRO, Parliamentary Services, the Premier's Department, the Australian Taxation Office, Sydney Trains, the Australian Bureau of Statistics, the Aged Care Quality and Safety Commission, Leidos and Raytheon.

Make your next cyber program an operating advantage.

Book a platform demonstration, discuss the partner program or scope a custom solution. Cybersecurity and AI consulting available across Australia, the USA, UK and Canada.

Learn more: cibrai.com · Deployment · AI hardware · Company background | September 2026

AUSTRALIA 1800 928 982 | +61 2 8005 6562 | +61 2 9000 1137
support@cibrai.com www.cibrai.com

USA +1 818 649 9444
Clarity. Not Chaos.