INVEST IN THE WORLD'S LEADING

AI-POWERED CYBERSECURITY

OPERATING PLATFORM

CiBRAI
CYBER INTELLIGENCE · BEHAVIOURAL RESPONSE

CLARITY. NOT CHAOS

CYBER INTELLIGENCE · BEHAVIOURAL RESPONSE

CiBRAI | PINNACLE EQUITIES

CIBRAI Is Designed To Stop Cyber Teams From Drowning In A Sea Of Red Alerts - And Catch The One That Matters.

Intelligent 24/7 threat detection and response with agentic AI.

Built to enable simplified service offerings for SMEs to government-grade security operations.

Maiden Capital Raising of

A$0.5M for 12.5% equity

CYBER INTELLIGENCE · BEHAVIOURAL RESPONSE

THE PROBLEM:

When everything is urgent, nothing gets handled fast

CYBER SECURITY TEAMS ARE OVERLOADED, BUT THREATS KEEP ACCELERATING.

Too many alerts….
84,700 Cybercrime reports in Australia in FY 25….those that were reported!

In Jan to June 2025, The Office of Australian Information commissioner reported 532 notifiable breaches.

Small teams can't triage every signal — real threats get buried in noise.

Compliance pressure: Self reporting costs by businesses rose by 50% to $80,850 per report.

Building and staffing a 24/7 SOC is expensive, slow, and rarely complete.

Founder Andrew Curtis "Most Managed Security Service Providers provide a patchwork solution to service their client's cyber needs. By using CiBRAI as a primary tool, it saves time, clutter and cost. CiBRAI provides cyber coverage using a greater number of applications meshed in with AI into a manageable dashboard designed specifically to meet an organisation's cyber threat needs."

THE STATISTICS ARE STAGGERING - AND THE PROBLEM IS ONLY GETTING BIGGER

Massive market growth

Strong and sustained growth in cybersecurity driven by digital transformation, cloud adoption and rising threat sophistication

14.3%
CAGR (2023-2032) Australia cybersecurity market

Source: Fortune Business Insights (2024

Escalating threats & impact

Cyber incidents are increasing in frequency, complexity and cost, targeting organisations of all sizes.

$3B+
Estimated annual cost of cybercrime to Australian organisations?

Source: ACSC (2024)

Regulatory & compliance pressure

Tightening regulatory requirements and mandated reporting increase accountability and drive investment.

1,113
Notifiable data breaches reported in Australia in 2024 (+25% YoY)

Source: OAIC (2024)

Cyber talent shortage

Global shortage of skilled cyber professionals creates capacity constraints and operational risk.

4.8M
Global cybersecurity workforce gap by 20254

Source: (ISC) (2024

Data sovereignty & trust

Organisations require sovereign deployment options and assurance over where data lives and is processed.

Australian-hosted solutions increasingly a procurement priority

Source: ASD (2024

Tool sprawl & cost

Fragmented point solutions drive up cost, complexity and operational overhead.

25-40%
Higher total cost with disconnected tools

Source: ASD (2024)

Notes *1. Fortune Business Insights (2024). 2. ACSC (2024) Annual Cyber Threat Report. 3. OAIC (2024) Notifiable Data Breaches Report. 4. (ISC) (2024) Cybersecurity Workforce Study. 5. Panaseer (2023) The Hidden Cost of Tool Sprawl*

01 **TAM A$147.5B**
(Total Addressable Market)

02 **SAM A$101.2B**
(Serviceable Addressable Market)

03 **SOM A$2.02B**
(Serviceable Obtainable Market)

Finance, government, healthcare, defence supply chain, and critical infrastructure are pressured by compliance, risk, and the need for rapid response. These buyers are the first industry sectors that CiBRAI is targeting.

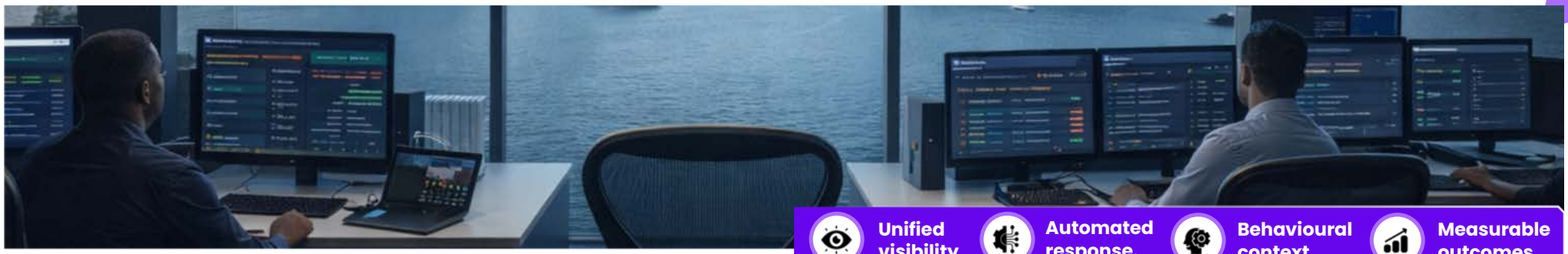
TEAMS ARE DROWNING IN A SEA OF RED ALERTS
CIBRAI PROVIDES TEAMS WITH FOCUS AND CLARITY

TODAY: OVERWHELMED AND REACTIVE

Security teams are buried in fragmented alerts, disconnected tools, and constant context switching. The result? Slower response. Higher risk.

WITH CIBRAI: CLARITY AND CONTROL

CIBRAI unifies intelligence, behaviour and response into one adaptive platform. The result? Faster decisions. Lower risk.



Unified visibility. **Automated response.** **Behavioural context.** **Measurable outcomes.**

FIVE CRITICAL PROBLEMS SECURITY TEAMS FACE

01 Alert overload

High volumes of low-fidelity alerts bury real threats, causing fatigue and missed signals.

02 Tool sprawl

Too many disconnected tools lead to silos, manual processes, and costly complexity

03 Escalating breach costs

Longer dwell times and inefficient response drive higher financial and reputational impact`

04 Data sovereignty and cloud risk

Increasing reliance on cloud services raises concerns around control, compliance, and data exposure

05 Cyber skills shortage

Talent gaps and burnout limit capacity to detect, investigate, and respond effectively

WHY THIS MATTERS

Faster detection and triage

Surface true threats sooner and act with confidence.

Lower operational friction

Unify workflows, reduce noise, and eliminate wasted effort.

Resilience with less

Do more with less-build adaptive defence that scales.

THERE ARE MANY SOPHISTICATED CYBERSECURITY APPS IN THE MARKET – Each provides a specific fragmented solution. Patchwork architecture results in poorer outcomes.

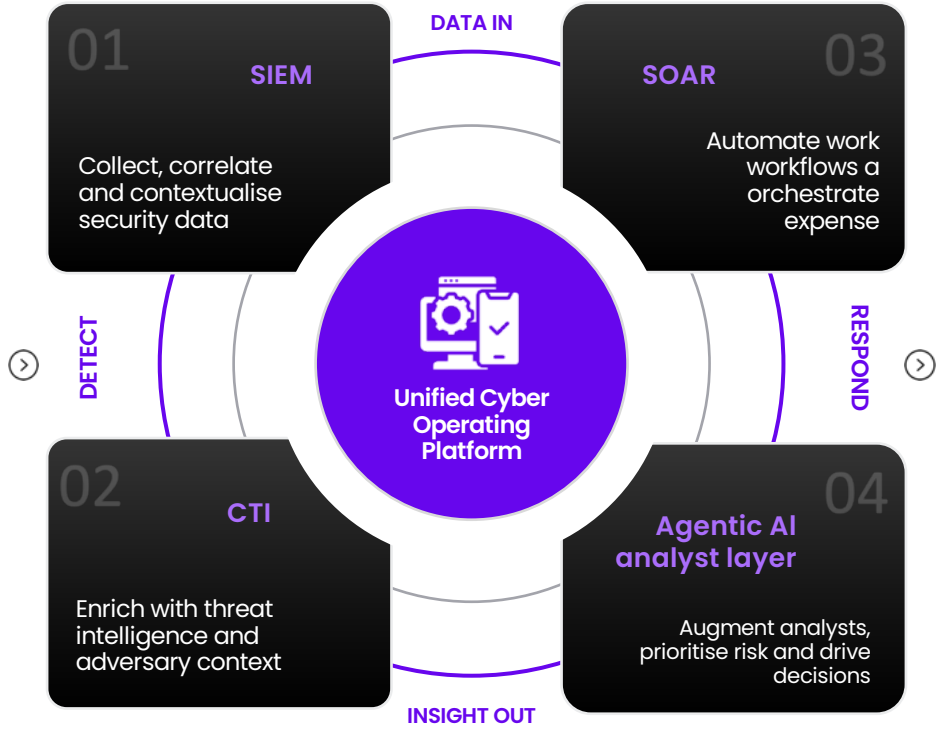
CiBRAI | PINNACLE EQUITIES

CiBRAI Philosophy of "Total Integration" unifies and filters security measures for a simplification of security responses.

Fragmented Tool Stack

Multiple point solutions. Disconnected data. Siloed workflows. Higher cost. Slower outcomes

Large enterprises report an average of 76 security tools



Integrated Operating Model

Unified data. Automated response. Measurable outcomes. Lower cost.

- MTTD/MTTR improvement ↑
- Time to ticket closure ↑
- False-positive reduction ↑
- Analyst hours saved ↑
- Tool rationalisation, operational cost reduction ↑

How to measure value

Capture baseline
Establish current state across key security and operational metrics

Integrate telemetry and workflows
Ingest data, standardise context and automate response workflows.

Compare pre/post performance
Measure impact across security, operational and business metrics

Track savings and uplift over time
Quantify cost reductions and productivity gains: optimise continuously

Andrew Curtis "There is no identified vendor, in the United States, Europe or elsewhere, that combines all four of the following into a single product:

1. Agentic AI security operations at SOC scale,
2. A natively unified platform, painlessly replacing the point tool stack,
3. Delivery sized and priced for the 50 to 5000 plus seat organisation, and.
4. Australian or regional sovereignty.

To the best of our knowledge, there is no Australian built sovereign product that addresses all of the above requirements.

The nexus right now that needs to be overcome in the cyber security marketplace is that any sovereign developed AI security platform is being marketed into a sceptical, compliance-driven buyer.

That buyer is persuaded by visible expertise and third-party validation before they are persuaded by advertising. Yet there is little evidence of delivery of a product that satisfies these 4 requirements. Lots of claims but not much else!

CiBRAI has spent over $1m in R & D capital outlays to develop a platform that addresses these four points.

CiBRAI - THE FIRST HYBRID CYBER SECURITY OPERATING PLATFORM

One secure stack for detection, automation, response and intelligence. CiBRAI is designed to:

Break the Cost Adoption Barrier as it is designed to work with existing tools not just replace them.

Augment existing security teams and technical stacks, unifying these environments and progressively rationalize duplicated workflows……in essence covering more outcomes with less resources.

Adapt to client's needs and security outcomes. A client's decision is often based around a compliance need, data protection, client confidentiality, or simply cost……therefore a flexible solution is required as one size does not fit all.

CiBRAI

The ultimate agentic AI layer that behaves like a tireless Tier-1 / Tier-2 analyst:

- Groups Alerts into incidents.
- Collects security events and finds suspicious patterns.
- Runs response playbooks and automates repetitive actions.
- Adds context and priority.
- Helps drive response steps.
- Works 24/7.

Sovereign-ready deployment options

WHY WE CAN WIN BUSINESS

We stand out in a competitive Marketplace

CAPABILITY	CIBRAI	IBM	MICROSOFT	DARKTRACE
AI-driven threat detection and testing	✓	✓	—	✓
Seamless on/off-premise integration	✓	✓	—	—
Fully customisable solutions – integrated designer	✓	✓	—	—
Real-time data protection for Windows, Linux, Mac	✓	✓	✓	✓
Sovereign compliance & privacy	✓	✓	✗	✗
Sovereign AI HW / SW platform – Battlefield ready	✓	—	✗	✗
Agentic AI built for classified data	✓	✗	✗	✗

Powered by Sphere

"CIBRAI's platform and team have made cyber security compliance simple, painless and cost effective for us. The tooling does the heavy lifting, the team makes sure we are pointing it at the right things." (Cooper Morrison – IT Security Manager, Sphere Drones)

UNLIKE LEGACY VENDORS, CIBRAI COMBINES AGENTIC AI WITH SIEM, SOAR, AND THREAT INTELLIGENCE FOR REAL-TIME THREAT AND VULNERABILITY MANAGEMENT — SOVEREIGN-READY BY DESIGN.

BUSINESS ROLLOUT

CiBRAI is not a start up, we have our first beachhead clients and Proof of Concept deployments with many more on the runway.

Founder has 20+ years of cyber consulting experience. He is well known and highly respected in the cybersecurity market. Potential clients are now engaging and mutual discussions are focused on scoping the solution for specific projects.

Funds are required to purchase;

- Additional AI infrastructure,
- Increased branding and marketing to support industry positioning, and
- Convert the runway of potential clients.

Current Client Runway & Momentum is Growing!			
	Early-Stage	Negotiation	Demo
Government	1	2	3
Semi Government	2	3	3
Managed Services	1	1	2
Large Insurance	1	0	0
Small Private	8	10	20
Total ($)	**13 ($500k)**	**15**	**27**

PRIMARY

PLATFORM SUBSCRIPTION

Core recurring revenue. Packaging supports both cloud and on-premise deployments.

SECONDARY

DEPLOYMENT & ONBOARDING

Implementation, integrations, and playbook setup so customers reach their security needs quickly.

GROWTH

EXPANSION REVENUE

Tailored solutions and managed operations for higher-assurance environments.

Founder Andrew Curtis is an experienced industry operator with his consultancy company Gadget Access and has runway of interested clients looking to adopt CiBRAI's philosophy. These range from Government through to large stand-alone Enterprises, through to industry security aggregators; Managed Security Service Providers.

SALES PIPELINE

40 ACTIVE OPPORTUNITIES

68% already in live demos

A qualified pipeline in active motion — every opportunity has an engaged buyer, not a cold list.

EARLY-STAGE

13 33% of pipeline

Qualified first contacts and warm introductions, with $500k in identified deal value already scoped.

»

LIVE DEMOS

27 68% of pipeline

Active product demonstrations, technical evaluation and solution-scoping discussions.

»

IN NEGOTIATION

15 56% of demos

Of the 27 in demo, 15 have progressed to commercial discussion with strong buying signals and repeat meetings.

BROAD, HIGH-TRUST MARKET COVERAGE

- Government, semi-government, MSSPs & managed services, insurers and private enterprise.
- Key verticals: property, wealth management, accounting, technology and education.
- Top of funnel keeps refilling: weekly email program reaching ~42,000 contacts drives inbound interest.

PATH TO CLOSE

- Support champions with business-case development inside each account.
- Progress deals through commercial evaluation, procurement / RFP and Board sign-off.
- Cycle time of weeks to months — standard for government and enterprise security buying.

Momentum is compounding: 27 of 40 opportunities are already in live demos — 15 of them in commercial negotiation — spanning Government through to MSSPs and large private enterprises.

ANDREW CURTIS FOUNDER: BACKGROUND

Respected serial entrepreneur developing technology solutions that have been adopted by major clients, including Telstra, Wilson Security, Defence and many others.

In 1992, Andrew founded Leading Edge PC, a systems network integrator that went on to become an Internet Service Provider. He successfully scaled it to a team of 90.

Founded Gadget Access in 2010 for the provision cybersecurity solutions.

Gadget Access has invested in excess of AU$1M in R&D to bring the CiBRAI vision to life.

INITIAL LEADERSHIP TEAM

Andrew Curtis

Founder & CEO with 20+ years in cybersecurity, leading innovative strategies and research.

Manny Farr

CFO with 20+ years of expertise in financial strategy and sustainable growth. Recognised for hands-on leadership and as a notable CEO.

Felix La Spina

CMO with 30+ years of both Sales and Marketing experience.

Gavin Brown

Experienced solutions, presales consultant & customer success specialist. Over 30 years in the IT industry with deep cybersecurity experience .

SEEKING $500,000 EQUITY SUBSCRIPTION.

Satisfy Client Enquiry with necessary funding to accelerate go-to-market strategy, support the technical team, purchase necessary AI infrastructure uplift, maintain marketing efforts and compliance levels.

A$0.5M FOR 12.5% EQUITY

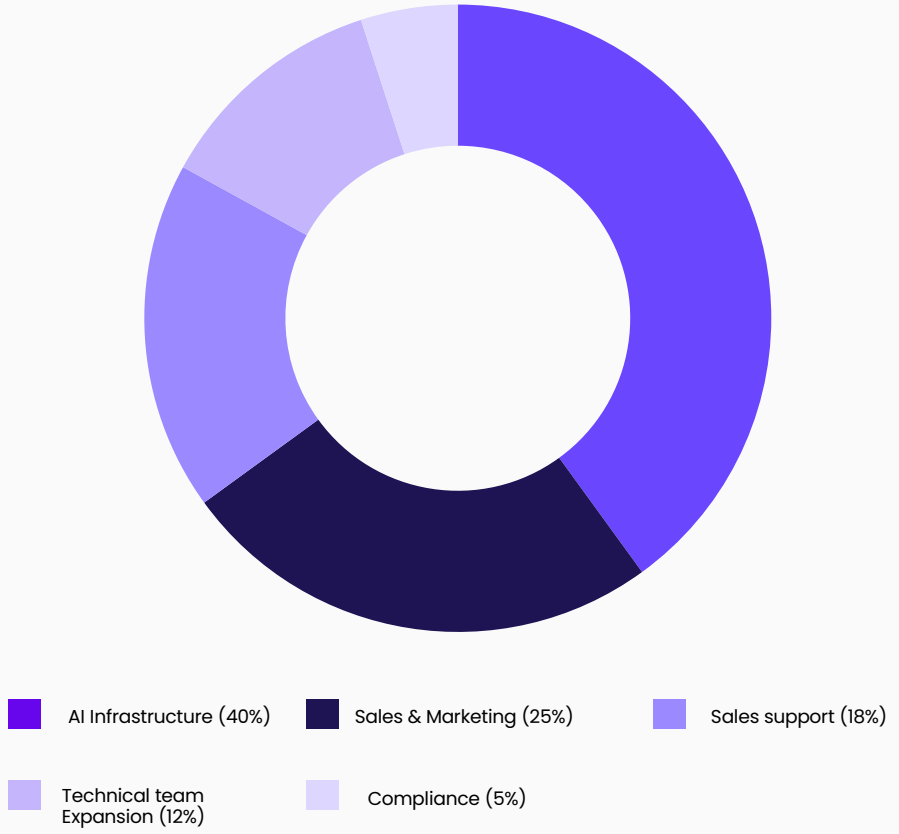
(Founder has invested over $1M establishing CiBRAI)

Focus on the now, but with an eye to the Future

Rising demand for agentic AI cybersecurity and sovereign AI solutions — driven by regulation and unprecedented attack volume.

Grow business organically with launch in Australia. Once traction is proven, follow-on funding will be secured to expand Globally.

USE OF FUNDS



NEXT STEPS: CONTACT OUR CORPORATE ADVISORS @ PINNACLE EQUITIES

DREW WILLIAMS

PRINCIPAL ADVISOR

+61 411 24 25 29

drew.williams@pinnaclequities.com

Pinnacle Equities • AFSL 300776

GUY AIRD

DIRECTOR & RESPONSIBLE MANAGER

+61 411 767 177

guy.aird@pinnaclequities.com

Pinnacle Equities • AFSL 300776