CiBRAI
CYBER INTELLIGENCE - BEHAVIOURAL RESPONSE

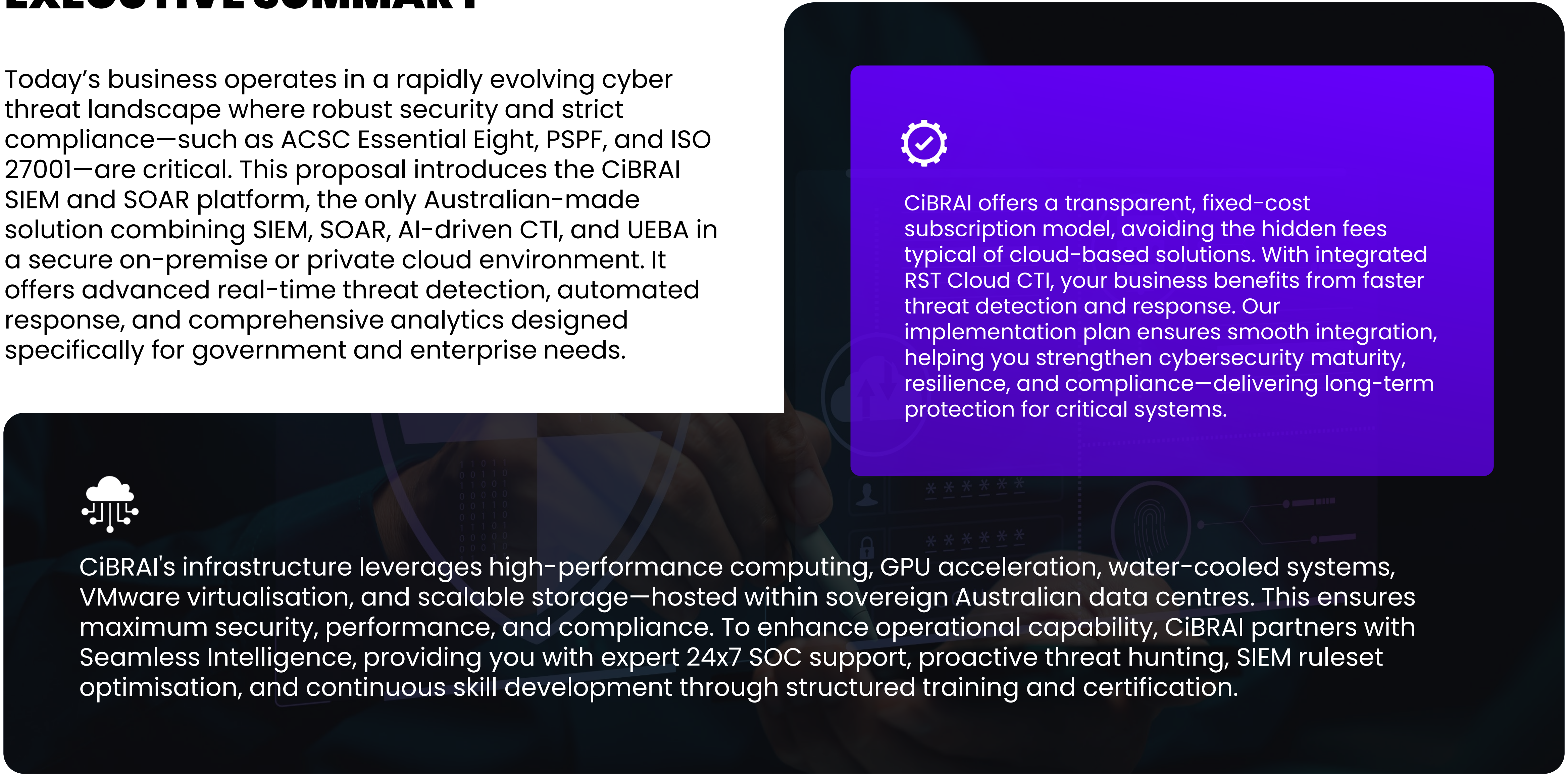
Agentic AI Cybersecurity Management Platform

The AI SIEM / SOAR / CTI Solution

Andy Curtis – Founder / CEO
support@cibrai.com
AU – 1800 928 982
USA - +1 818 649 9444

EXECUTIVE SUMMARY

Today's business operates in a rapidly evolving cyber threat landscape where robust security and strict compliance—such as ACSC Essential Eight, PSPF, and ISO 27001—are critical. This proposal introduces the CiBRAI SIEM and SOAR platform, the only Australian-made solution combining SIEM, SOAR, AI-driven CTI, and UEBA in a secure on-premise or private cloud environment. It offers advanced real-time threat detection, automated response, and comprehensive analytics designed specifically for government and enterprise needs.



CiBRAI offers a transparent, fixed-cost subscription model, avoiding the hidden fees typical of cloud-based solutions. With integrated RST Cloud CTI, your business benefits from faster threat detection and response. Our implementation plan ensures smooth integration, helping you strengthen cybersecurity maturity, resilience, and compliance—delivering long-term protection for critical systems.

CiBRAI's infrastructure leverages high-performance computing, GPU acceleration, water-cooled systems, VMware virtualisation, and scalable storage—hosted within sovereign Australian data centres. This ensures maximum security, performance, and compliance. To enhance operational capability, CiBRAI partners with Seamless Intelligence, providing you with expert 24x7 SOC support, proactive threat hunting, SIEM ruleset optimisation, and continuous skill development through structured training and certification.

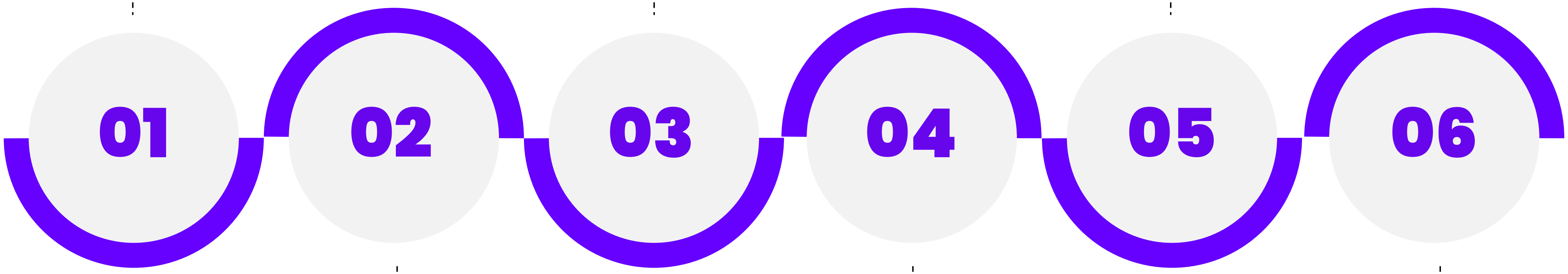
COMPANY OVERVIEW

CiBRAI is an Australian cybersecurity provider delivering advanced SIEM, SOAR, and CTI solutions powered by AI and machine learning. Our mission is to help organisations like yours manage cybersecurity risks through scalable, proactive security platforms tailored to government and enterprise needs. For this engagement, CiBRAI has partnered with Secure Collaboration and Seamless Intelligence—two trusted Australian firms with proven expertise in secure infrastructure, 24x7 SOC operations, and SIEM co-management—to deliver a comprehensive, sovereign solution.

Together, we offer an integrated, end-to-end cybersecurity service that ensures compliance, resilience, and performance. Hosted within sovereign Australian data centres, our solution combines cutting-edge infrastructure with continuous support, training, and threat intelligence. This partnership gives you the tools, visibility, and expertise needed to strengthen its cyber posture and meet stringent government standards.

COMPANY OVERVIEW

Key Benefits



01 Agentic AI-powered SIEM/SOAR platform with real-time detection, response, and analytics.

02 Secure, sovereign hosting within Equinix & Macquarie Data Centers.

03 24x7 SOC and co-managed services with proactive threat hunting and incident response.

04 Expert rule tuning and CTI integration for continuous system optimization.

05 Helping you achieve compliance with Essential Eight, PSPF, ISM, and ISO 27001.

06 Ongoing training and knowledge transfer to build internal capability.

UNDERSTANDING YOUR REQUIREMENTS

ADDRESSING CURRENT GAPS

We often see existing MSSP-based SIEMs lacking visibility, automation, and integration—hindering compliance with Essential Eight, ISM, and PSPF.

CLIENT-OWNED OPEN-CORE PLATFORM

CiBRAI offers a fully integrated SIEM, SOAR, and CTI solution with direct connectivity and full ownership, eliminating MSSP limitations.

COMPREHENSIVE VISIBILITY

Unlimited log ingestion and advanced analytics ensure centralised, real-time visibility across all digital assets and systems.

Advanced Automation & Orchestration

Seamless workflows and automated incident response reduce manual effort and accelerate threat mitigation.

UNDERSTANDING YOUR REQUIREMENTS

Scalable & Sovereign Deployment

On-premise or private cloud infrastructure hosted in Australian data centres, with high-performance compute and scalable storage.

Agentic AI Virtual SOC

AI-driven SOC capabilities support intelligent reporting, behavioural analysis, threat detection, and rapid integration of new systems.

Compliance-Ready Architecture

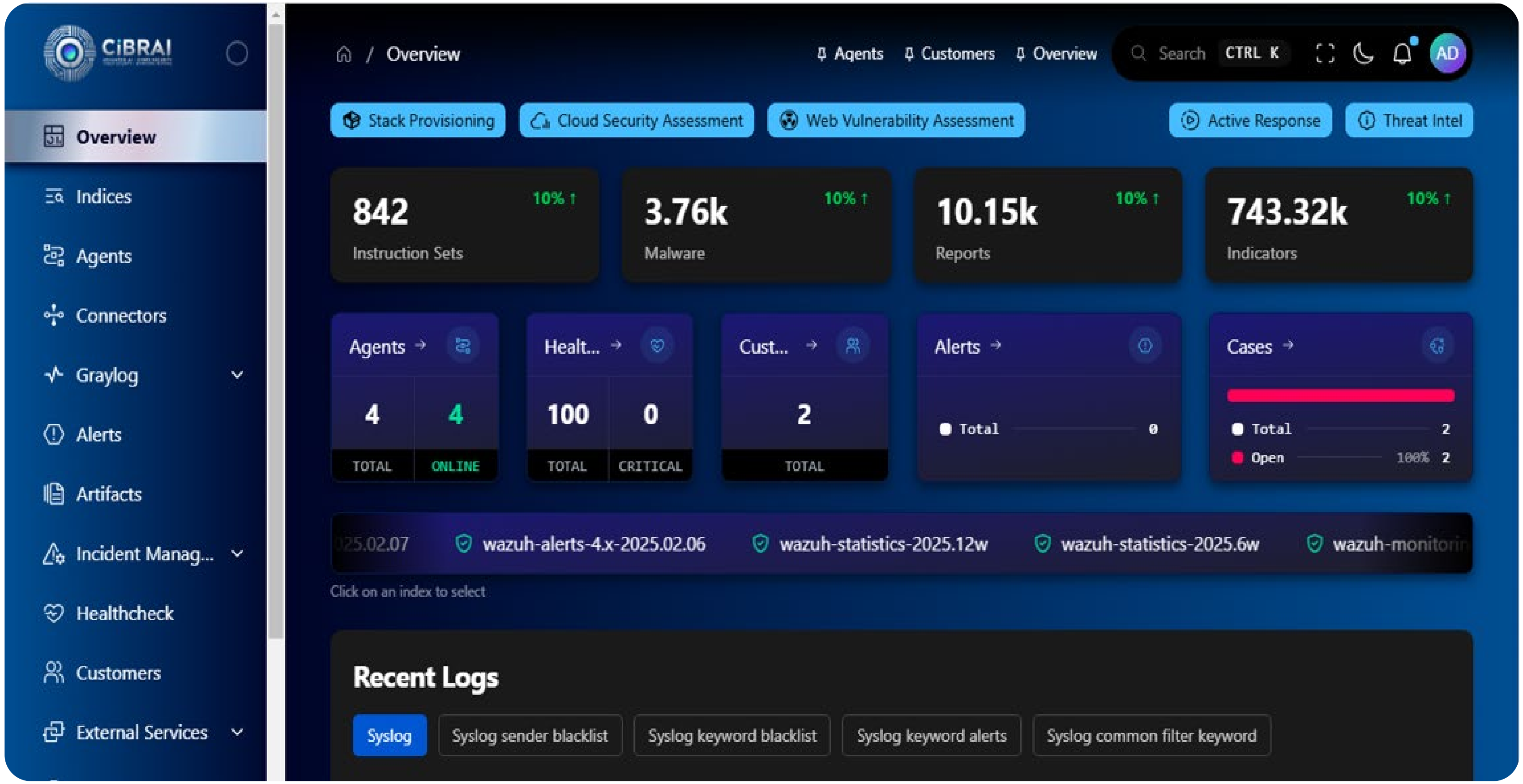
Fully aligned with Essential Eight, ISM, and PSPF, delivering auditable logs, reports, and dashboards for regulatory adherence.

Customisable & Future-Proof

Modular features, machine learning, 24x7 co-managed SOC support, and proactive health monitoring ensure long-term cybersecurity resilience.

DETAILED CIBRAI SOLUTION OVERVIEW

CiBRAI is a sovereign, Australian-managed cybersecurity platform offering an integrated SIEM, SOAR, and Cyber Threat Intelligence (CTI) solution enhanced with Agentic AI for automation and reporting. Purpose-built for Australian government agencies, it provides a future-ready cybersecurity posture that aligns with Essential Eight, ISM, and PSPF requirements. The modular design ensures adaptability to your compliance needs and operational goals.



842 10% ↑ Instruction Sets

3.76k 10% ↑ Malware

10.15k 10% ↑ Reports

743.32k 10% ↑ Indicators

Agents: 4 TOTAL, 4 ONLINE

Healt...: 100 TOTAL, 0 CRITICAL

Cust...: 2 TOTAL

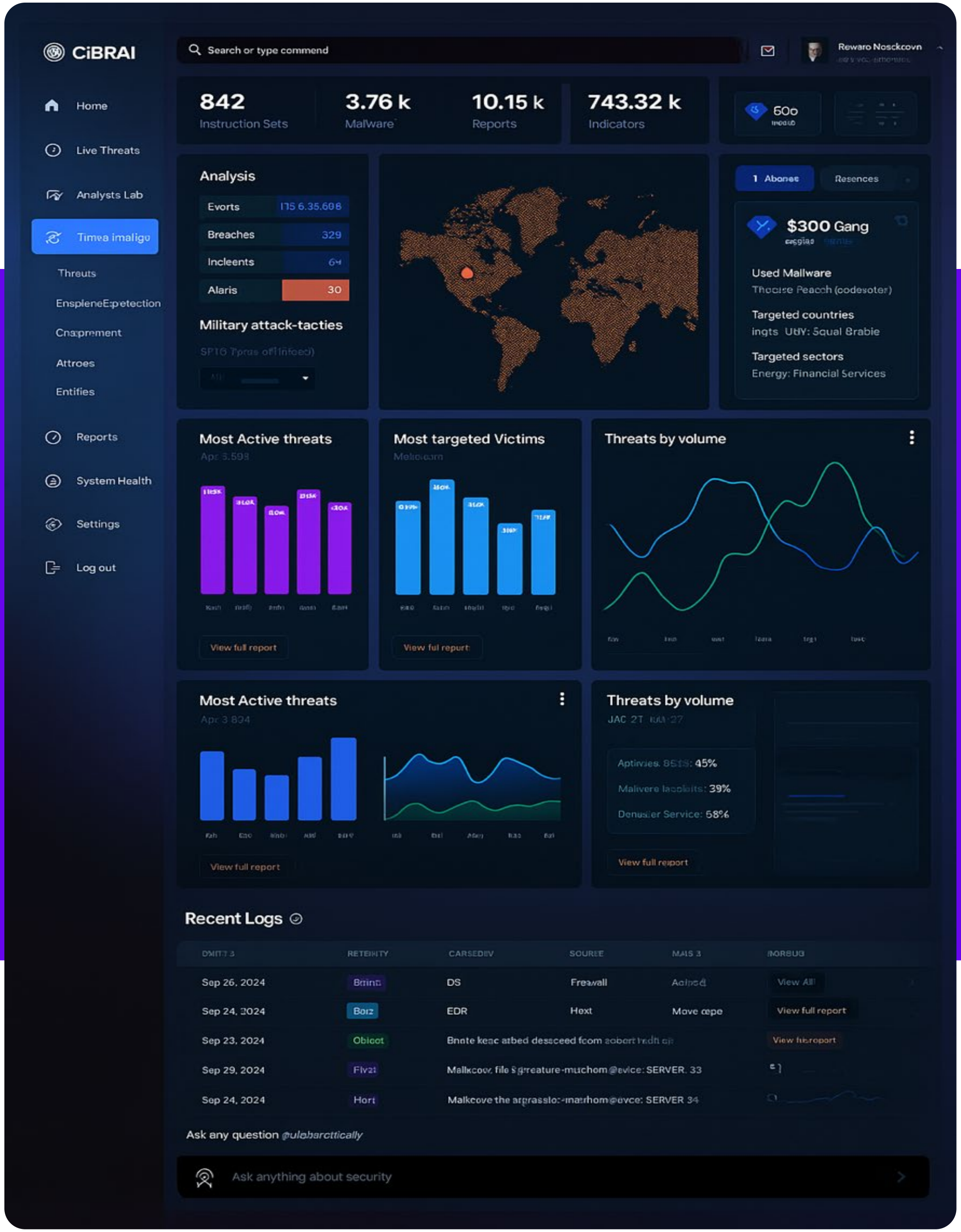
Alerts: Total 0

Cases: Total 2; Open 100% 2

25.02.07 wazuh-alerts-4.x-2025.02.06 wazuh-statistics-2025.12w wazuh-statistics-2025.6w wazuh-monitorin

Click on an index to select

DETAILED CIBRAI SOLUTION OVERVIEW



Analysis	
Evorts	175 6.35.608
Breaches	329
Incleents	64
Alaris	30

Used Mallware
Thecise Peacch (codesoter)

Targeted countries
ingts UtiY: Squal Brabie

Targeted sectors
Energy: Financial Services

Aptivies: 45%
Malivere lacdoits: 39%
Denusier Service: 58%

Recent Logs

DMIT3	RETEHITY	CARSEDIV	SOURCE	MAIS 3	MORBUG
Sep 26, 2024	Brino	DS	Frewall	Aciped	View All
Sep 24, 2024	Borz	EDR	Hext	Move cepe	View full report
Sep 23, 2024	Obicot	Bnnte keac atbed dessceed fcom aobert Irdh ai			View hisroport
Sep 29, 2024	Fivzi	Mallkcow file Sgreature-muchom @evice: SERVER. 33			
Sep 24, 2024	Hort	Malkcove the arprasslo:-inathom@evce: SERVER 34			

Ask any question *@ulabarctically*

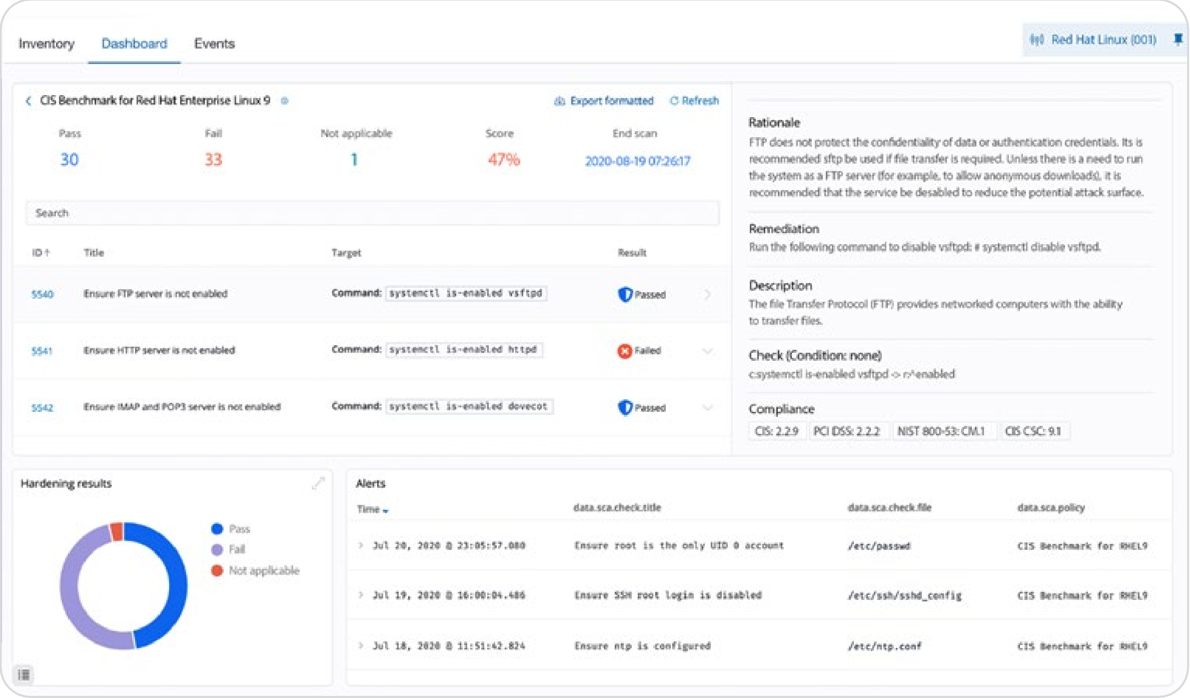
CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

CONFIGURATION ASSESSMENT

CiBRAI Core SIEM continuously evaluates the security configurations of endpoints, servers, cloud services, and network infrastructure against industry-standard baselines and compliance frameworks, such as CIS Benchmarks, PCI DSS, HIPAA, GDPR, SOX, NIST, and ISO 27001. Real-time assessment detects and flags misconfigurations and deviations, enabling immediate corrective actions and detailed reporting for audits. Configuration drift alerts ensure security settings remain aligned with organizational policies.

Use Case

Security teams effortlessly maintain audit readiness, automate compliance checks, and swiftly correct unauthorized changes, minimizing potential attack surfaces and ensuring regulatory adherence.



Pass	Fail	Not applicable	Score	End scan
30	33	1	47%	2020-08-19 07:26:17

ID ↑	Title	Target	Result
5540	Ensure FTP server is not enabled	Command: `systemctl is-enabled vsftpd`	Passed
5541	Ensure HTTP server is not enabled	Command: `systemctl is-enabled httpd`	Failed
5542	Ensure IMAP and POP3 server is not enabled	Command: `systemctl is-enabled dovecot`	Passed

Rationale

FTP does not protect the confidentiality of data or authentication credentials. Its is recommended sftp be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the service be desabled to reduce the potential attack surface.

Remediation

Run the following command to disable vsftpd: # systemctl disable vsftpd.

Description

The file Transfer Protocol (FTP) provides networked computers with the ability to transfer files.

Check (Condition: none)

c:systemctl is-enabled vsftpd -> r:^enabled

Compliance

CIS: 2.2.9 | PCI DSS: 2.2.2 | NIST 800-53: CM.1 | CIS CSC: 9.1

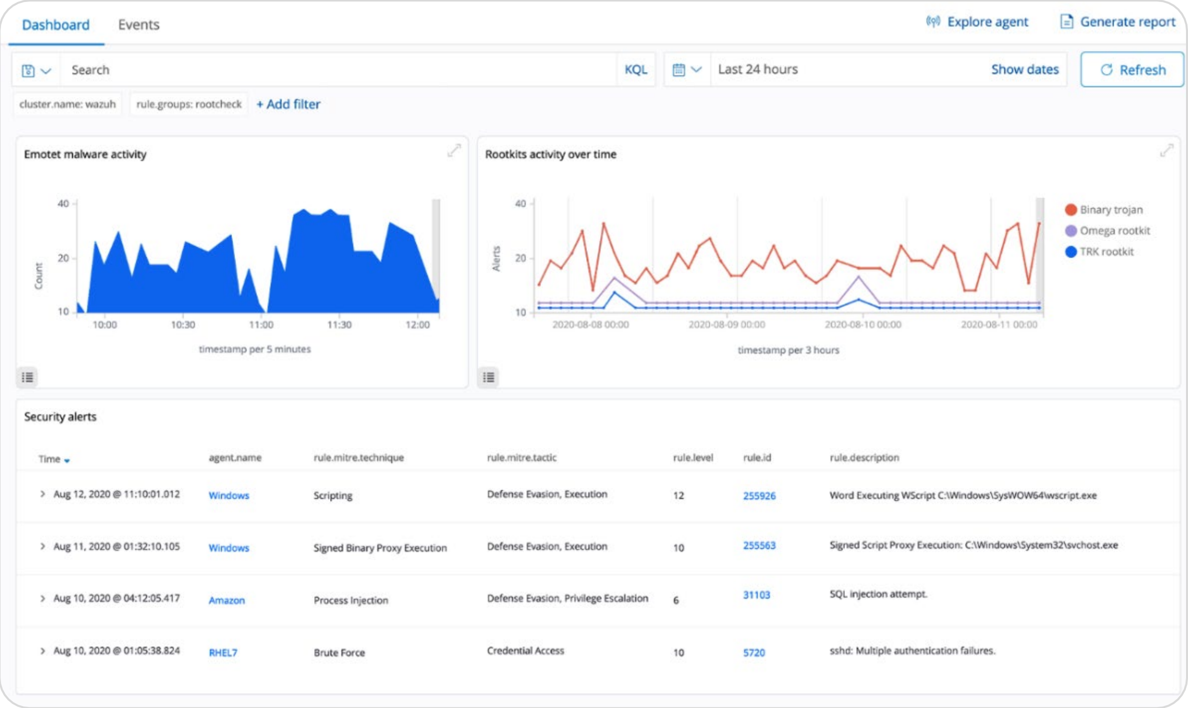
Alerts

Time	data.sca.check.title	data.sca.check.file	data.sca.policy
Jul 20, 2020 @ 23:05:57.080	Ensure root is the only UID 0 account	/etc/passwd	CIS Benchmark for RHEL9
Jul 19, 2020 @ 16:00:04.486	Ensure SSH root login is disabled	/etc/ssh/sshd_config	CIS Benchmark for RHEL9
Jul 18, 2020 @ 11:51:42.824	Ensure ntp is configured	/etc/ntp.conf	CIS Benchmark for RHEL9

CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

MALWARE DETECTION

CiBRAI employs real-time malware detection leveraging both signature-based and advanced behavior-based methodologies. It continuously monitors processes, system interactions, file activities, and network connections for suspicious or malicious patterns indicative of malware. Integrated threat intelligence further enhances detection capabilities by identifying known indicators of compromise (IOCS) and zero-day threats.



Security alerts

Time	agent.name	rule.mitre.technique	rule.mitre.tactic	rule.level	rule.id	rule.description
Aug 12, 2020 @ 11:10:01.012	Windows	Scripting	Defense Evasion, Execution	12	255926	Word Executing WScript C:\Windows\SysWOW64\wscript.exe
Aug 11, 2020 @ 01:32:10.105	Windows	Signed Binary Proxy Execution	Defense Evasion, Execution	10	255563	Signed Script Proxy Execution: C:\Windows\System32\svchost.exe
Aug 10, 2020 @ 04:12:05.417	Amazon	Process Injection	Defense Evasion, Privilege Escalation	6	31103	SQL injection attempt.
Aug 10, 2020 @ 01:05:38.824	RHEL7	Brute Force	Credential Access	10	5720	sshd: Multiple authentication failures.

Use Case

Rapidly detect and isolate malware, ransomware, and Advanced Persistent Threats (APTs) across endpoints, preventing lateral movement and minimizing potential impact.

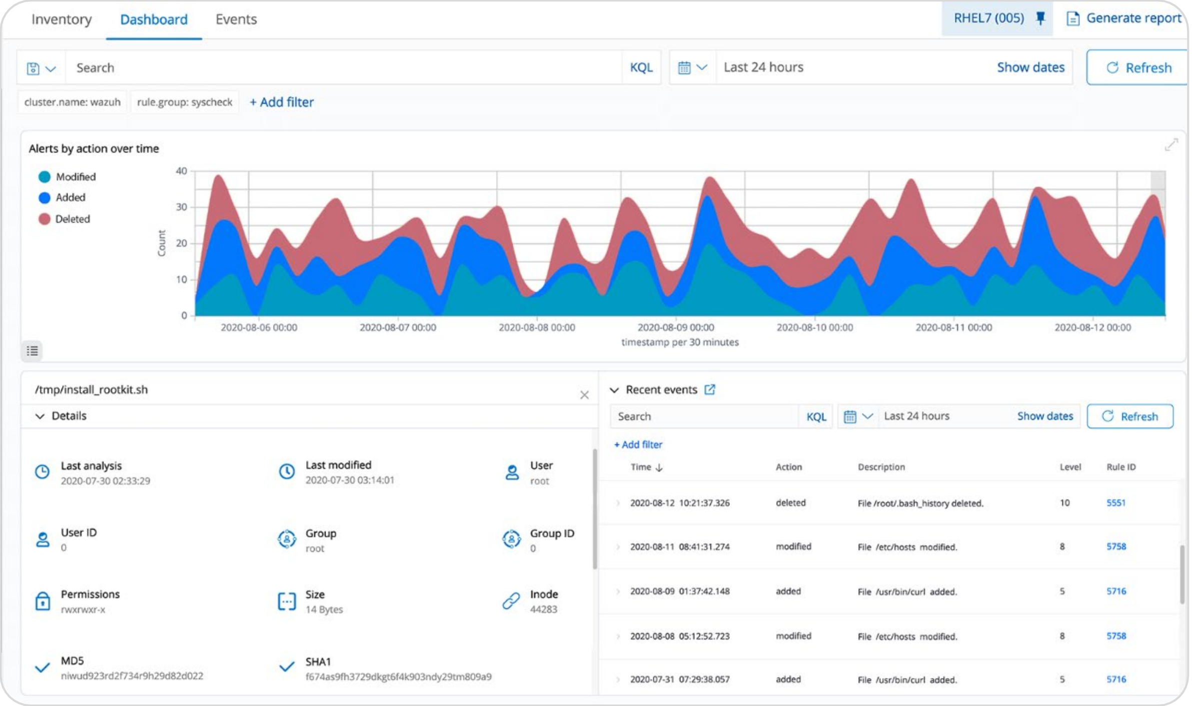
CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

FILE INTEGRITY MONITORING (FIM)

CiBRAI Core SIEM implements advanced real-time FIM using efficient kernel-level event tracing technologies (including eBPF) to monitor file modifications across servers and endpoints. Detailed forensic attribution ("who-data") reveals exactly which user or process initiated file changes, greatly aiding incident investigation and compliance management.

Use Case

Immediate detection of unauthorized file changes, suspicious activities such as configuration tampering, or sensitive data manipulation. Detailed forensic insights streamline investigations and response.



cluster.name: wazuh

rule.group: syscheck

/tmp/install_rootkit.sh

Details

Last analysis
2020-07-30 02:33:29

Last modified
2020-07-30 03:14:01

User
root

User ID
0

Group
root

Group ID
0

Permissions
rwxrwxr-x

Size
14 Bytes

Inode
44283

MD5
niwud923rd2f734r9h29d82d022

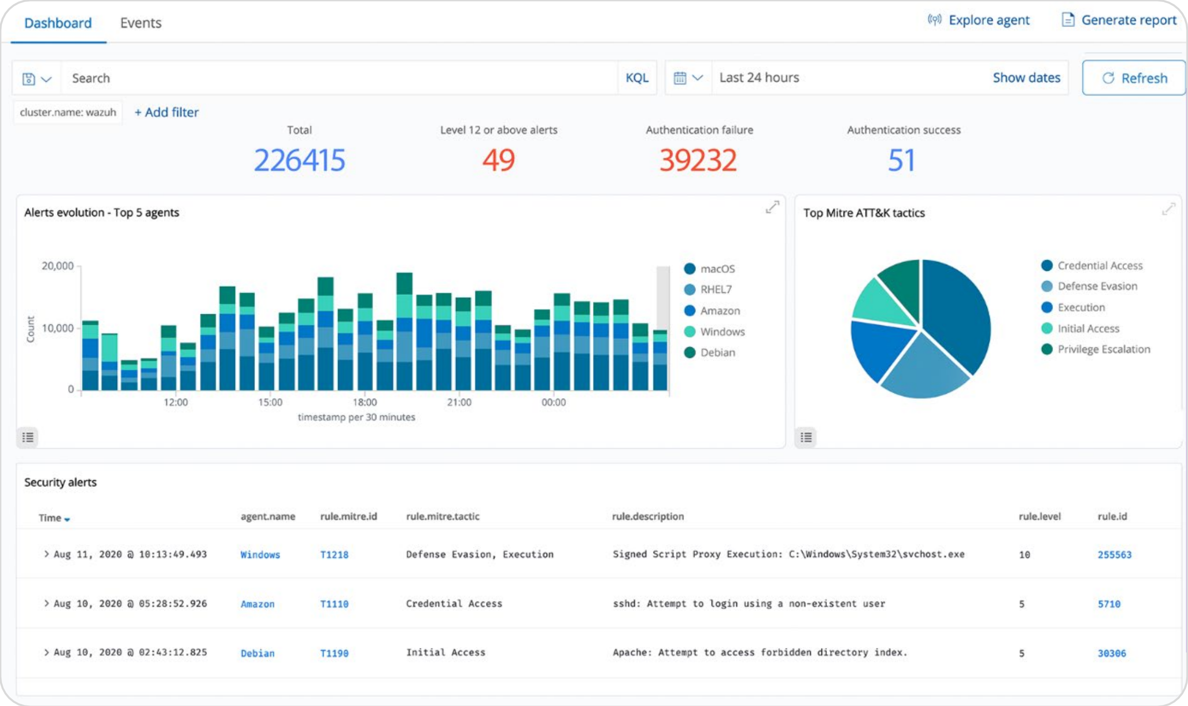
SHA1
f674as9fh3729dkgt6f4k903ndy29tm809a9

Time ↓	Action	Description	Level	Rule ID
2020-08-12 10:21:37.326	deleted	File /root/.bash_history deleted.	10	5551
2020-08-11 08:41:31.274	modified	File /etc/hosts modified.	8	5758
2020-08-09 01:37:42.148	added	File /usr/bin/curl added.	5	5716
2020-08-08 05:12:52.723	modified	File /etc/hosts modified.	8	5758
2020-07-31 07:29:38.057	added	File /usr/bin/curl added.	5	5716

CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

THREAT HUNTING

CiBRAI enhances threat hunting by leveraging sophisticated analytics and integrated AI-based capabilities. Analysts have direct access to comprehensive telemetry and enriched contextual information across endpoints, networks, cloud environments, and user activities. Advanced behavioral analytics identify anomalous patterns, empowering proactive threat discovery.



Last 24 hours

cluster.name: wazuh

Total	Level 12 or above alerts	Authentication failure	Authentication success
226415	49	39232	51

Security alerts

Time	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Aug 11, 2020 @ 10:13:49.493	Windows	T1218	Defense Evasion, Execution	Signed Script Proxy Execution: C:\Windows\System32\svchost.exe	10	255563
Aug 10, 2020 @ 05:28:52.926	Amazon	T1110	Credential Access	sshd: Attempt to login using a non-existent user	5	5710
Aug 10, 2020 @ 02:43:12.825	Debian	T1190	Initial Access	Apache: Attempt to access forbidden directory index.	5	30306

Use Case

Security analysts proactively hunt for elusive threats, previously undetected attacks, insider threats, and zero-day exploits through robust, AI-enhanced analytics, significantly reducing mean-time-to-detection (MTTD).

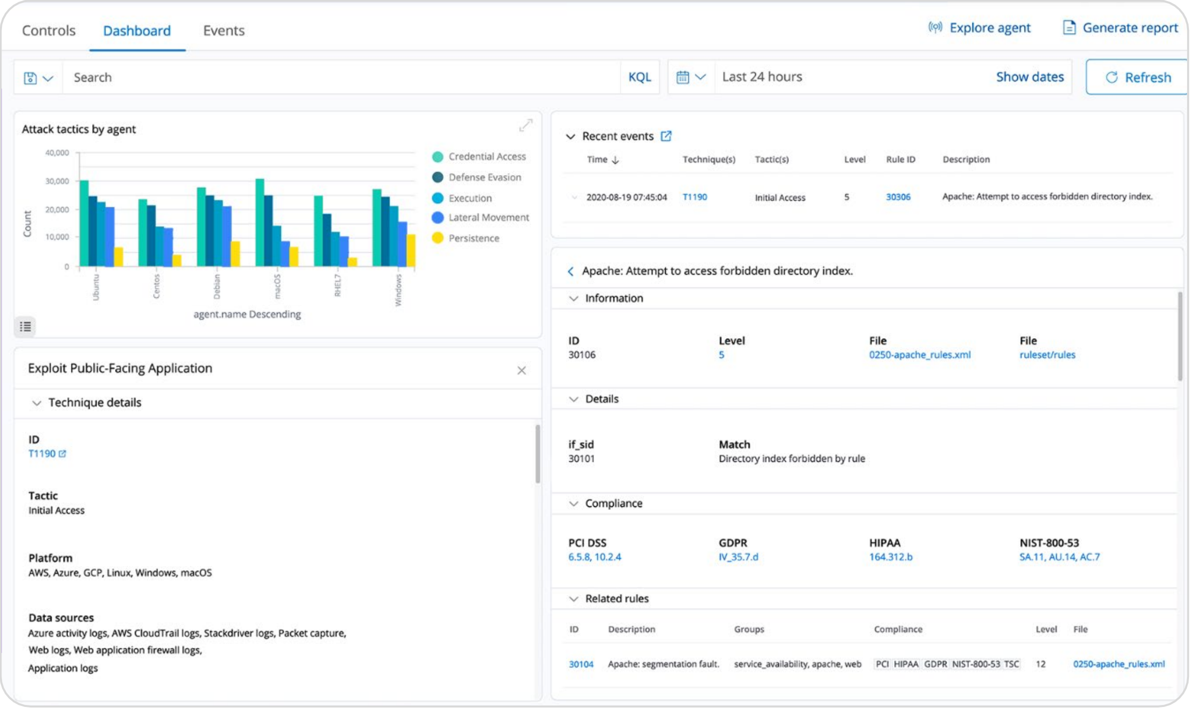
CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

LOG DATA ANALYSIS

CiBRAI collects, centralizes, and normalizes vast volumes of log data from endpoints, network devices, cloud infrastructures (AWS, Azure, GCP), and SaaS applications (Microsoft 365). Powerful search and correlation capabilities facilitate efficient log analysis, threat identification, and forensic investigation. Real-time analytics generate actionable alerts correlated across diverse data sources.

Use Case

Identify suspicious activities and incidents rapidly, ensuring timely detection, investigation, and remediation through comprehensive and contextualized log data analytics.



Recent events

Time ↓	Technique(s)	Tactic(s)	Level	Rule ID	Description
2020-08-19 07:45:04	T1190	Initial Access	5	30306	Apache: Attempt to access forbidden directory index.

Exploit Public-Facing Application

Technique details

ID
T1190

Tactic
Initial Access

Platform
AWS, Azure, GCP, Linux, Windows, macOS

Data sources
Azure activity logs, AWS CloudTrail logs, Stackdriver logs, Packet capture, Web logs, Web application firewall logs, Application logs

Apache: Attempt to access forbidden directory index.

Information

ID	Level	File	File
30106	5	0250-apache_rules.xml	ruleset/rules

Details

if_sid	Match
30101	Directory index forbidden by rule

Compliance

PCI DSS	GDPR	HIPAA	NIST-800-53
6.5.8, 10.2.4	IV_35.7.d	164.312.b	SA.11, AU.14, AC.7

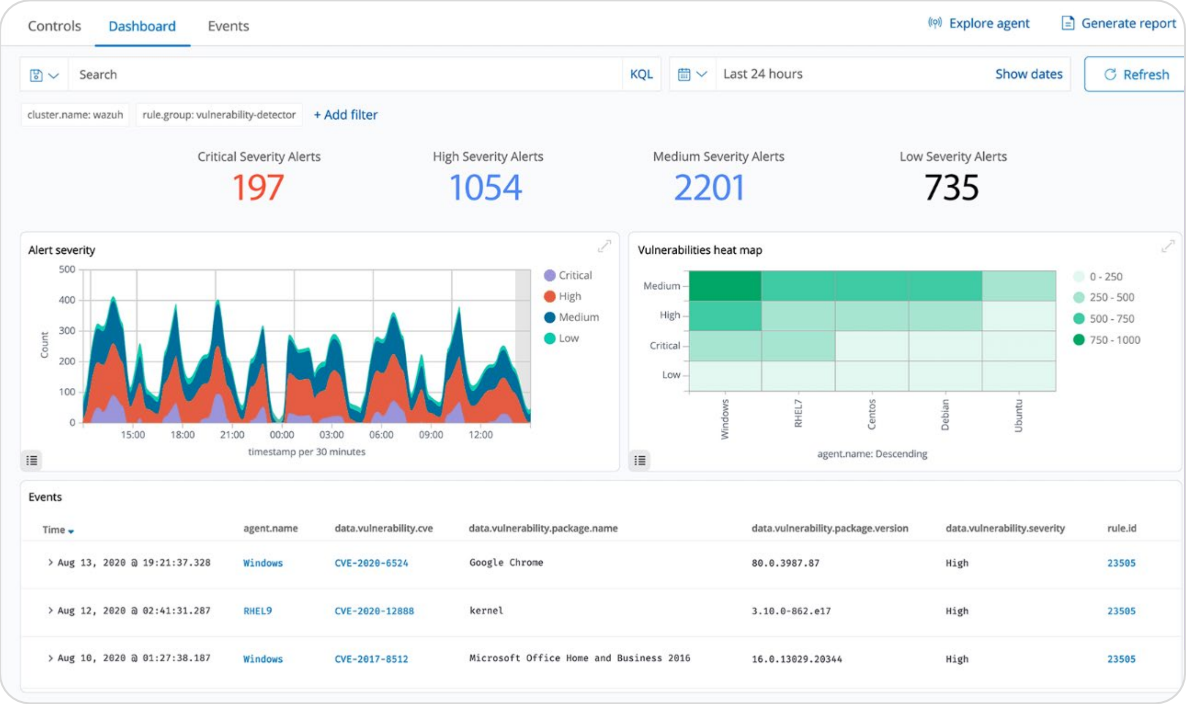
Related rules

ID	Description	Groups	Compliance	Level	File
30104	Apache: segmentation fault.	service_availability, apache, web	PCI HIPAA GDPR NIST-800-53 TSC	12	0250-apache_rules.xml

CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

VULNERABILITY DETECTION

Integrated vulnerability detection continuously monitors endpoints, applications, cloud workloads, containers, and network devices for known security weaknesses. CiBRAI correlates software inventory data with real-time threat intelligence feeds (CVEs, severity ratings, exploit details) for comprehensive risk analysis and prioritization.



Last 24 hours

cluster.name: wazuh

rule.group: vulnerability-detector

Critical Severity Alerts 197

High Severity Alerts 1054

Medium Severity Alerts 2201

Low Severity Alerts 735

Events

Time	agent.name	data.vulnerability.cve	data.vulnerability.package.name	data.vulnerability.package.version	data.vulnerability.severity	rule.id
> Aug 13, 2020 @ 19:21:37.328	Windows	CVE-2020-6524	Google Chrome	80.0.3987.87	High	23505
> Aug 12, 2020 @ 02:41:31.287	RHEL9	CVE-2020-12888	kernel	3.10.0-862.e17	High	23505
> Aug 10, 2020 @ 01:27:38.187	Windows	CVE-2017-8512	Microsoft Office Home and Business 2016	16.0.13029.20344	High	23505

Use Case

Prioritize vulnerability remediation effectively by clearly identifying high-risk threats actively exploited in the wild, enabling precise and targeted mitigation.

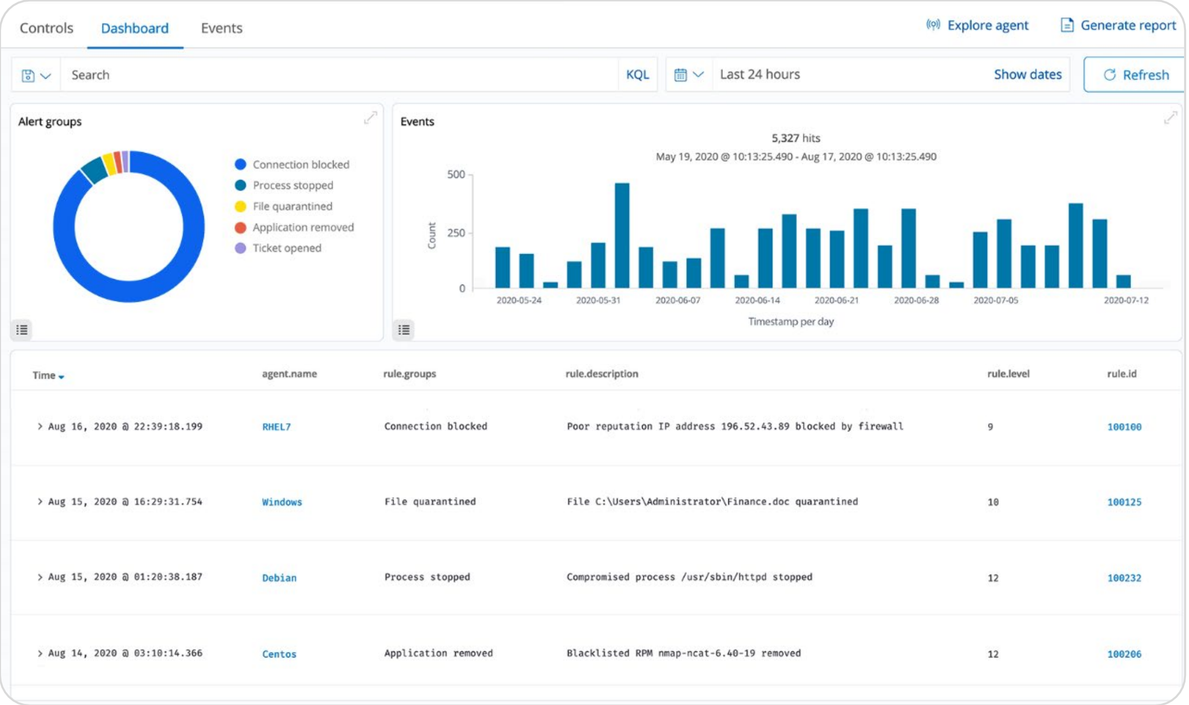
CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

INCIDENT RESPONSE

CiBRAI simplifies and accelerates incident response workflows by providing detailed contextual data, threat timelines, alert correlation, and forensic attribution. Incident timelines clearly reconstruct attack sequences, enabling rapid response and containment measures. Automated responses, including endpoint isolation and user access restriction, further strengthen response effectiveness.

Use Case

Security teams quickly neutralize threats, minimize impact, and return to normal operations swiftly, supported by automated response and forensic-quality event reconstruction.

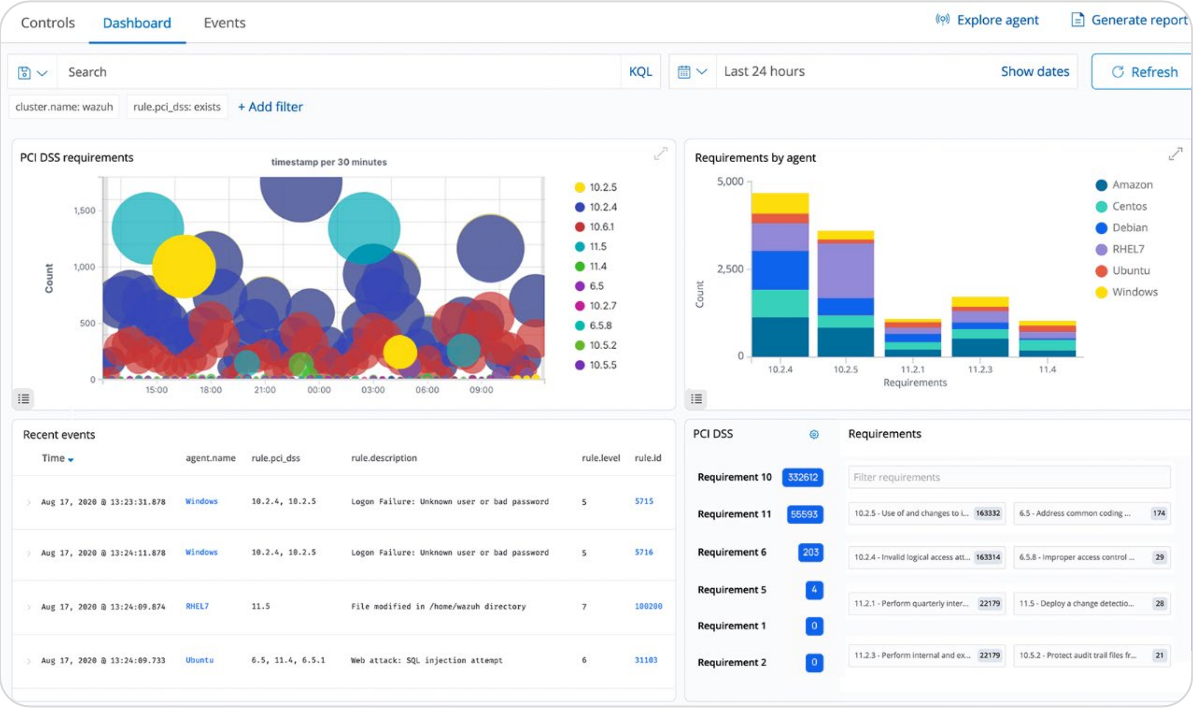


Time	agent.name	rule.groups	rule.description	rule.level	rule.id
› Aug 16, 2020 @ 22:39:18.199	RHEL7	Connection blocked	Poor reputation IP address 196.52.43.89 blocked by firewall	9	100100
› Aug 15, 2020 @ 16:29:31.754	Windows	File quarantined	File C:\Users\Administrator\Finance.doc quarantined	10	100125
› Aug 15, 2020 @ 01:20:38.187	Debian	Process stopped	Compromised process /usr/sbin/httpd stopped	12	100232
› Aug 14, 2020 @ 03:10:14.366	Centos	Application removed	Blacklisted RPM nmap-ncat-6.40-19 removed	12	100206

CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

REGULATORY COMPLIANCE

CiBRAI Core SIEM directly addresses complex regulatory compliance requirements, offering built-in templates and automated processes for standards including GDPR, HIPAA, PCI DSS, SOX, and NIST frameworks. Continuous monitoring and real-time configuration assessments enable consistent, demonstrable compliance. Detailed compliance reports support audit and governance requirements.



Recent events

Time	agent.name	rule.pci_dss	rule.description	rule.level	rule.id
Aug 17, 2020 @ 13:23:31.878	Windows	10.2.4, 10.2.5	Logon Failure: Unknown user or bad password	5	5715
Aug 17, 2020 @ 13:24:11.878	Windows	10.2.4, 10.2.5	Logon Failure: Unknown user or bad password	5	5716
Aug 17, 2020 @ 13:24:09.874	RHEL7	11.5	File modified in /home/wazuh directory	7	100200
Aug 17, 2020 @ 13:24:09.733	Ubuntu	6.5, 11.4, 6.5.1	Web attack: SQL injection attempt	6	31103

PCI DSS

Requirement 10	332612
Requirement 11	55593
Requirement 6	203
Requirement 5	4
Requirement 1	0
Requirement 2	0

Requirements

Filter requirements

10.2.5 - Use of and changes to i...	163332	6.5 - Address common coding ...	174
10.2.4 - Invalid logical access att...	163314	6.5.8 - Improper access control ...	29
11.2.1 - Perform quarterly inter...	22179	11.5 - Deploy a change detectio...	28
11.2.3 - Perform internal and ex...	22179	10.5.2 - Protect audit trail files fr...	21

Use Case

Organizations confidently manage compliance mandates with automated monitoring, simplified reporting, and rapid corrective capabilities to maintain regulatory adherence with minimal manual effort.

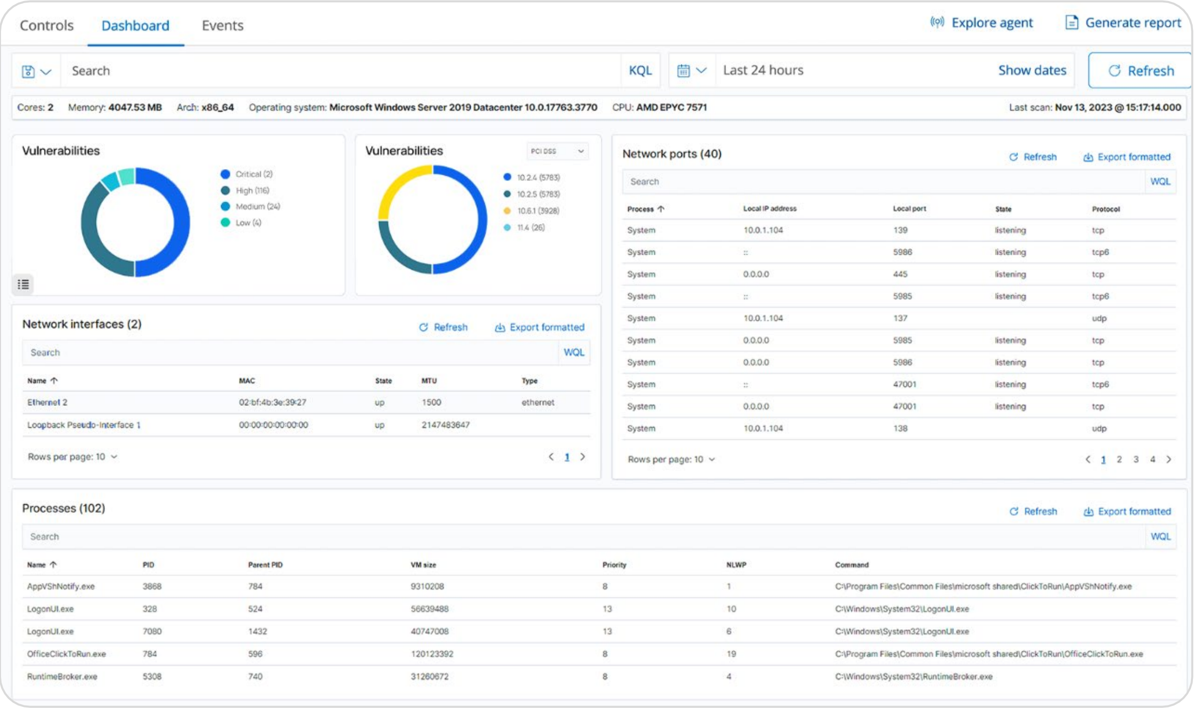
CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

IT HYGIENE

CiBRAI promotes robust IT hygiene through comprehensive asset visibility, inventory management, software tracking, and configuration control. Automated asset discovery and tracking identify unauthorized devices or software. Configuration assessments and patch-level monitoring prevent security gaps and reduce exploitable vulnerabilities.

Use Case

Maintain a secure and hygienic IT environment, proactively preventing unauthorized asset usage, unmanaged software installations, and non-compliant device configurations.



Cores: 2 Memory: **4047.53 MB** Arch: **x86_64** Operating system: **Microsoft Windows Server 2019 Datacenter 10.0.17763.3770** CPU: **AMD EPYC 7571** Last scan: **Nov 13, 2023 @ 15:17:14.000**

Network interfaces (2)

Name ↑	MAC	State	MTU	Type
Ethernet 2	02:bf:4b:3e:39:27	up	1500	ethernet
Loopback Pseudo-Interface 1	00:00:00:00:00:00	up	2147483647	

Rows per page: 10

Network ports (40)

Process ↑	Local IP address	Local port	State	Protocol
System	10.0.1.104	139	listening	tcp
System	::	5986	listening	tcp6
System	0.0.0.0	445	listening	tcp
System	::	5985	listening	tcp6
System	10.0.1.104	137		udp
System	0.0.0.0	5985	listening	tcp
System	0.0.0.0	5986	listening	tcp
System	::	47001	listening	tcp6
System	0.0.0.0	47001	listening	tcp
System	10.0.1.104	138		udp

Rows per page: 10

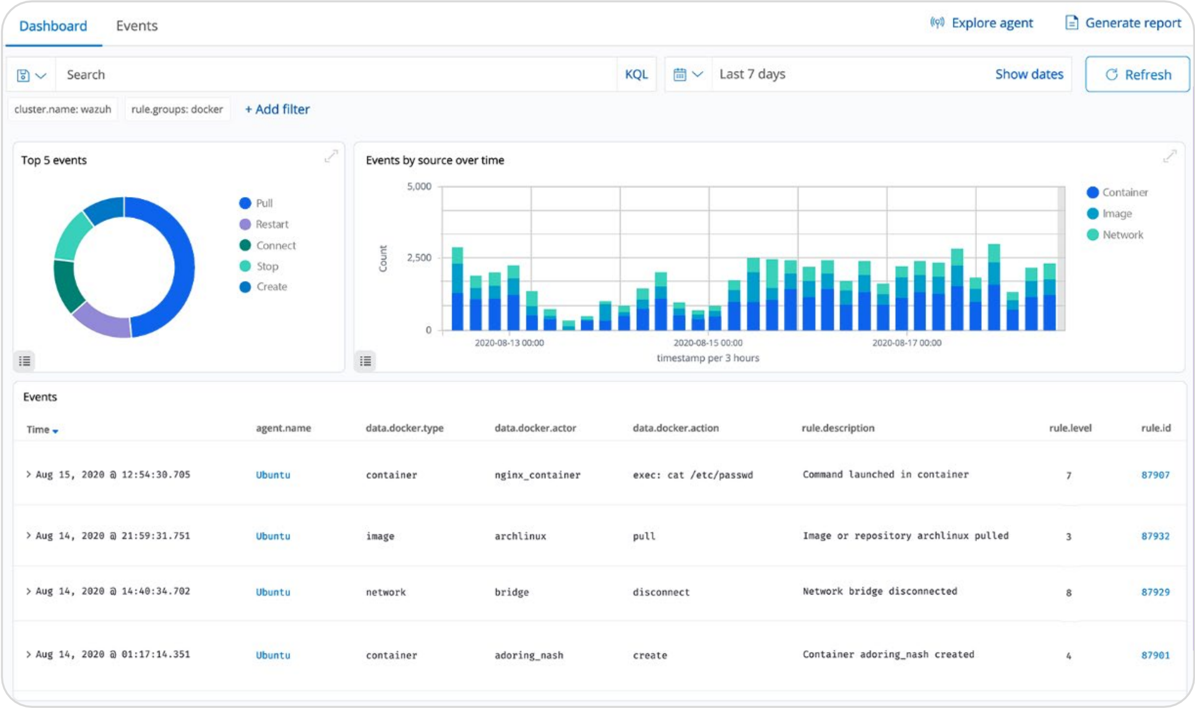
Processes (102)

Name ↑	PID	Parent PID	VM size	Priority	NLWP	Command
AppVShNotify.exe	3868	784	9310208	8	1	C:\Program Files\Common Files\microsoft shared\ClickToRun\AppVShNotify.exe
LogonUI.exe	328	524	56639488	13	10	C:\Windows\System32\LogonUI.exe
LogonUI.exe	7080	1432	40747008	13	6	C:\Windows\System32\LogonUI.exe
OfficeClickToRun.exe	784	596	120123392	8	19	C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeClickToRun.exe
RuntimeBroker.exe	5308	740	31260672	8	4	C:\Windows\System32\RuntimeBroker.exe

CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

CONTAINER SECURITY

CiBRAI Core SIEM ensures the secure deployment, runtime monitoring, and continuous security of containerized environments. Direct integration with Docker and Kubernetes APIs provides visibility into container activities, detects anomalous behavior, unauthorized deployments, insecure configurations, and runtime threats, ensuring secure orchestration and container security best practices.



Events

Time	agent.name	data.docker.type	data.docker.actor	data.docker.action	rule.description	rule.level	rule.id
> Aug 15, 2020 @ 12:54:30.705	Ubuntu	container	nginx_container	exec: cat /etc/passwd	Command launched in container	7	87907
> Aug 14, 2020 @ 21:59:31.751	Ubuntu	image	archlinux	pull	Image or repository archlinux pulled	3	87932
> Aug 14, 2020 @ 14:40:34.702	Ubuntu	network	bridge	disconnect	Network bridge disconnected	8	87929
> Aug 14, 2020 @ 01:17:14.351	Ubuntu	container	adoring_nash	create	Container adoring_nash created	4	87901

Use Case

Prevent unauthorized container deployments and privilege escalations, monitor anomalous runtime behavior, and maintain container compliance, ensuring secure operations in dynamic, orchestrated environments.

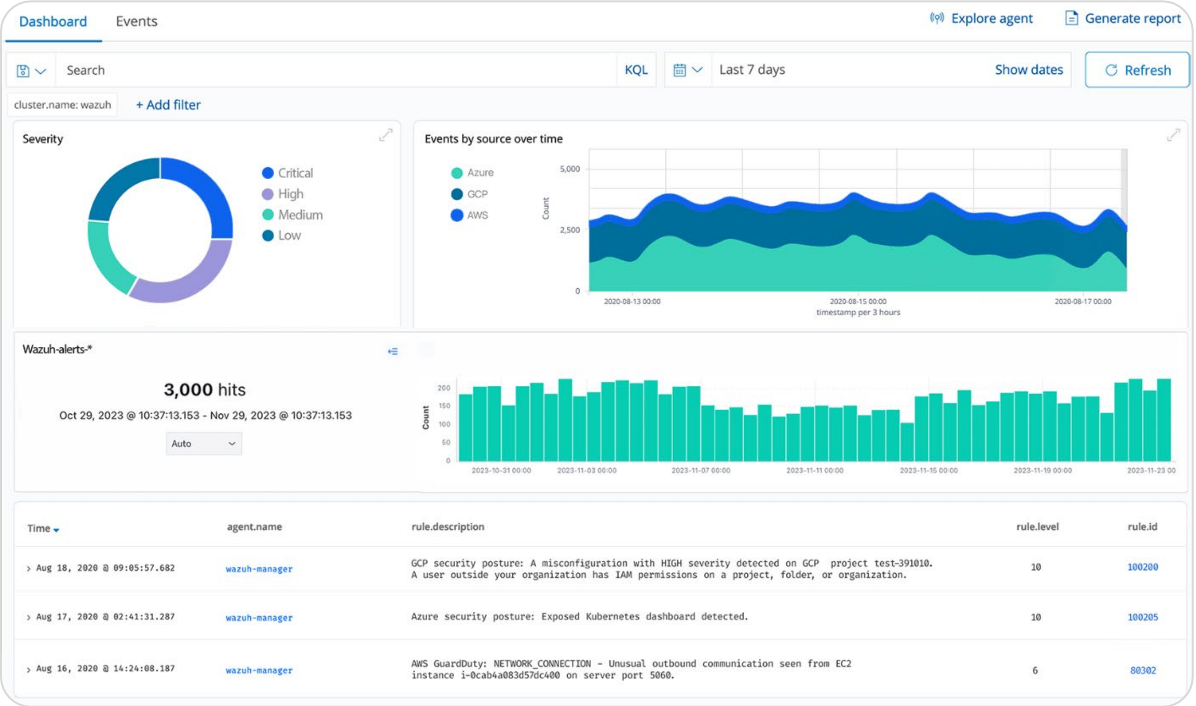
CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

POSTURE MANAGEMENT

Cloud Security Posture Management (CSPM) within CiBRAI automatically assesses cloud infrastructure across AWS, Azure, and GCP, identifying misconfigurations, insecure settings, overly permissive access policies, open storage buckets, and potential security exposures. Regular posture assessments ensure continuous compliance and robust security in multi-cloud and hybrid environments.

Use Case

Continuously maintain secure cloud configurations, quickly identify and remediate risky configurations, and maintain robust, auditable cloud security posture compliance.



3,000 hits

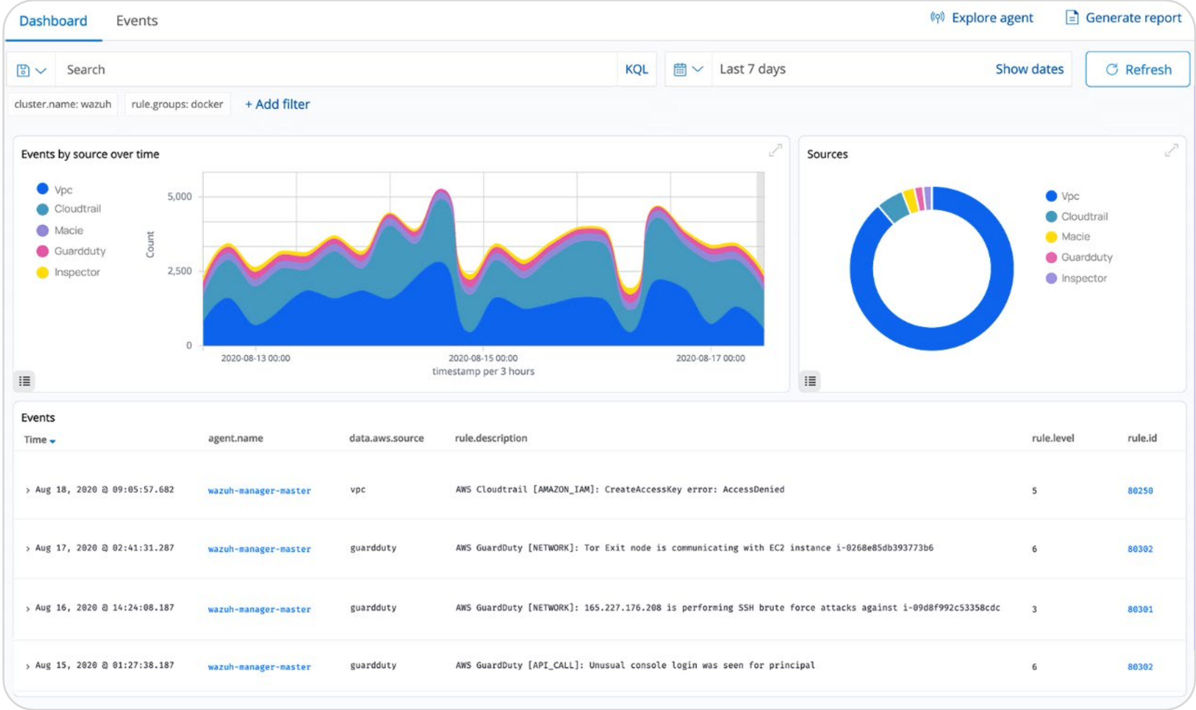
Oct 29, 2023 @ 10:37:13.153 - Nov 29, 2023 @ 10:37:13.153

Time	agent.name	rule.description	rule.level	rule.id
› Aug 18, 2020 @ 09:05:57.682	wazuh-manager	GCP security posture: A misconfiguration with HIGH severity detected on GCP project test-391010. A user outside your organization has IAM permissions on a project, folder, or organization.	10	100200
› Aug 17, 2020 @ 02:41:31.287	wazuh-manager	Azure security posture: Exposed Kubernetes dashboard detected.	10	100205
› Aug 16, 2020 @ 14:24:08.187	wazuh-manager	AWS GuardDuty: NETWORK_CONNECTION - Unusual outbound communication seen from EC2 instance i-0cab4a083d57dc400 on server port 5060.	6	80302

CIBRAI CORE SIEM MODULE – FEATURE OVERVIEW

WORKLOAD PROTECTION

CiBRAI provides comprehensive security monitoring, protection, and compliance enforcement across cloud, on-premises, and hybrid workloads. It combines real-time telemetry, vulnerability detection, behavioral analysis, FIM, and configuration assessments to provide multi-layered protection against threats targeting servers, VMs, cloud instances, and application workloads.



Events

Time	agent.name	data.aws.source	rule.description	rule.level	rule.id
› Aug 18, 2020 @ 09:05:57.682	wazuh-manager-master	vpc	AWS Cloudtrail [AMAZON_IAM]: CreateAccessKey error: AccessDenied	5	80250
› Aug 17, 2020 @ 02:41:31.287	wazuh-manager-master	guardduty	AWS GuardDuty [NETWORK]: Tor Exit node is communicating with EC2 instance i-0268e85db393773b6	6	80302
› Aug 16, 2020 @ 14:24:08.187	wazuh-manager-master	guardduty	AWS GuardDuty [NETWORK]: 165.227.176.208 is performing SSH brute force attacks against i-09d8f992c53358cdc	3	80301
› Aug 15, 2020 @ 01:27:38.187	wazuh-manager-master	guardduty	AWS GuardDuty [API_CALL]: Unusual console login was seen for principal	6	80302

Use Case

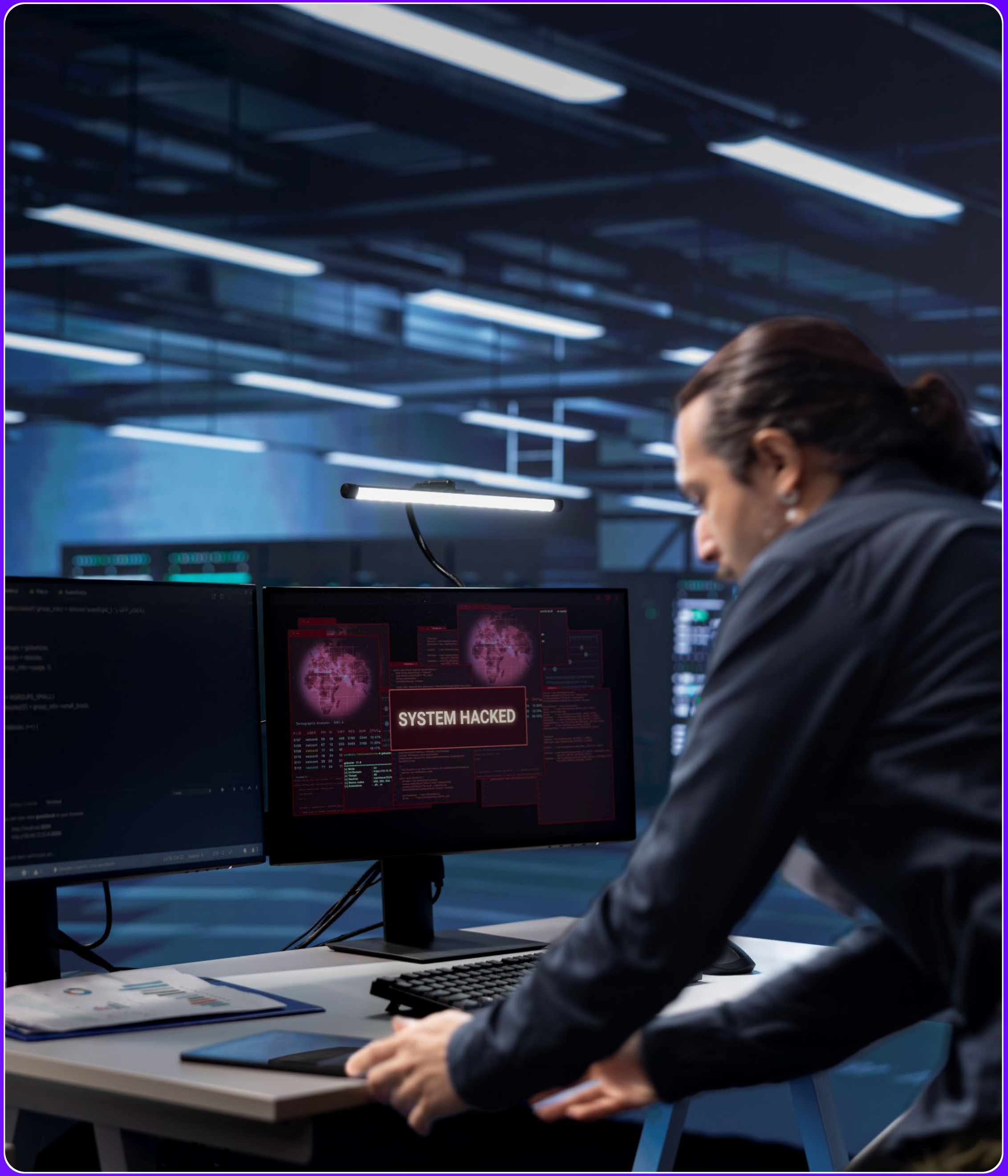
Ensure secure, compliant, and continuously protected workloads across diverse deployment scenarios, proactively addressing vulnerabilities, misconfigurations, malicious behavior, and unauthorized access attempts.

Proactive Threat Detection & Response

- Detects and prioritises high-risk threats in real time
- Automates response with fast containment and control

Automated Compliance & Governance

- Supports standards like GDPR, HIPAA, PCI DSS, NIST
- Delivers real-time dashboards and audit-ready reports



- CiBRAI enforces IT hygiene through automated asset discovery, inventory tracking, and configuration monitoring, detecting unauthorized devices or software and reducing vulnerabilities through real-time compliance and patch visibility.

- Container security is ensured via native integration with Docker and Kubernetes, enabling visibility into runtime activity, detecting misconfigurations, and blocking unauthorized deployments or privilege escalations.

- Cloud Posture Management automatically scans AWS, Azure, and GCP environments, identifying risky configurations and maintaining compliance with continuous assessments and remediation insights.

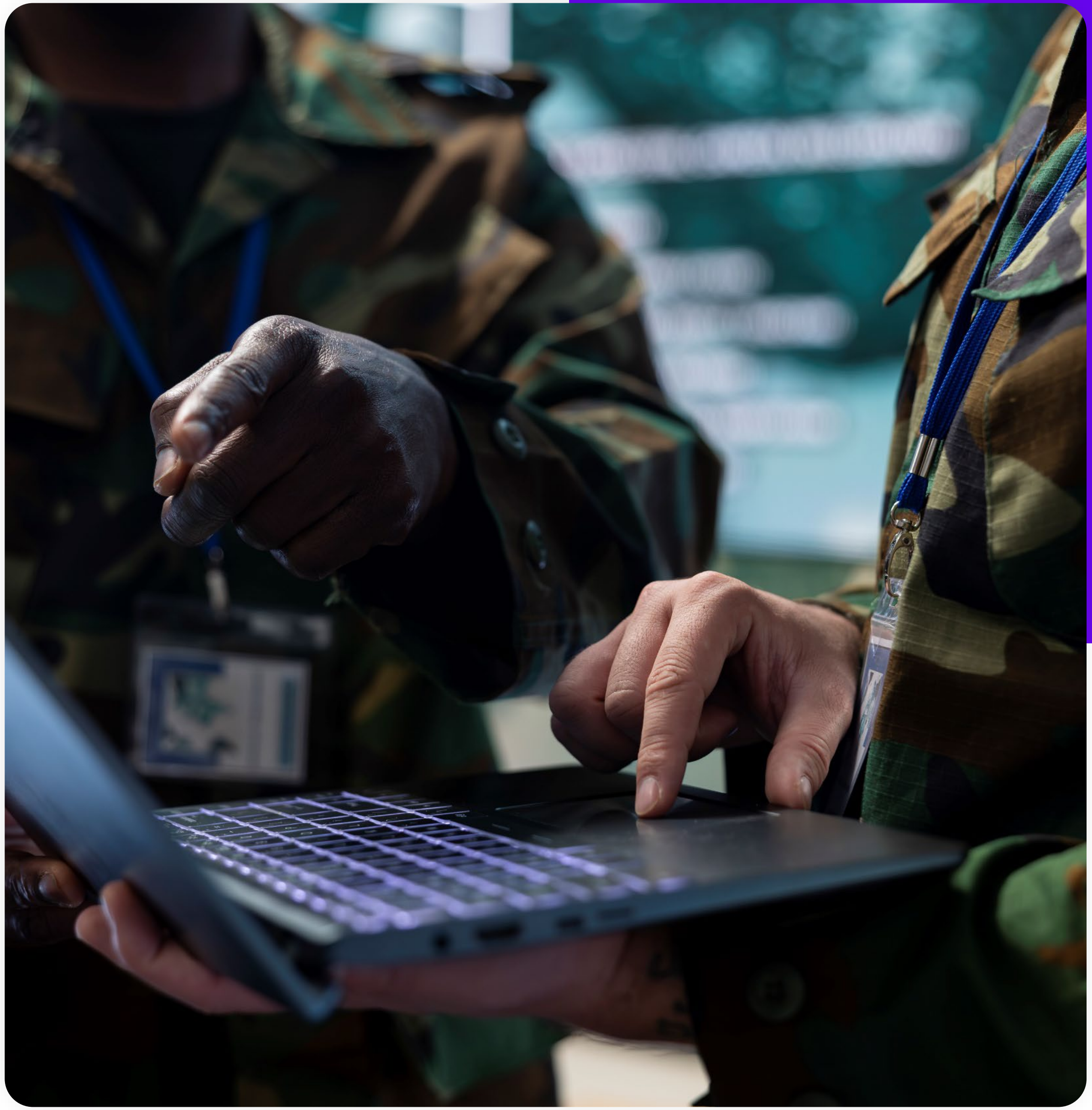
- CiBRAI secures workloads across all environments with layered protection, combining telemetry, behavior analytics, FIM, and vulnerability scanning to detect and stop threats targeting servers, VMs, and applications.

CiBRAI Core SIEM delivers a unified cybersecurity platform that streamlines threat detection, response, and compliance across modern enterprise and government environments. Its advanced AI-enhanced analytics provide real-time visibility, forensic depth, and proactive threat detection across endpoints, cloud, containers, and hybrid systems. The platform also simplifies regulatory compliance and IT hygiene through continuous automated assessments, while its scalable architecture supports everything from edge environments to large-scale data centers.

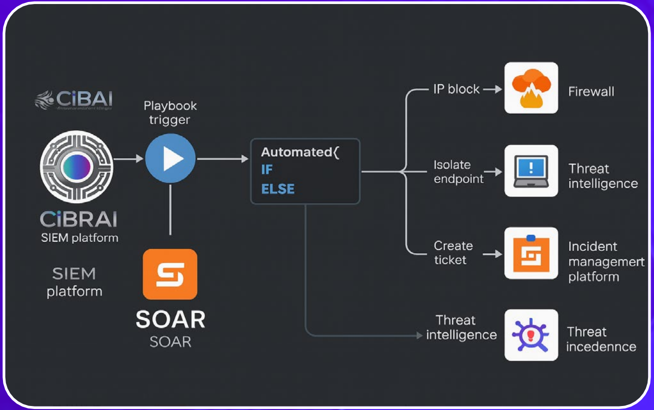
The integrated SOAR module addresses the growing complexity and volume of security incidents by embedding orchestration and automation directly into security workflows. It empowers SOC teams to respond rapidly and consistently, reduce alert fatigue, and automate repetitive tasks across diverse environments. By unifying SIEM logs, threat intelligence, and infrastructure data, CiBRAI SOAR dramatically improves operational efficiency and response speed.

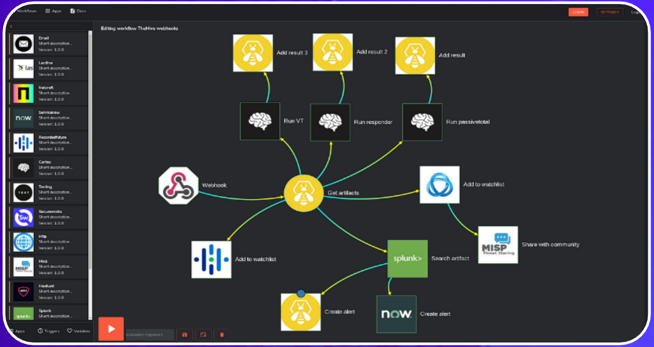
KEY BENEFITS INCLUDE

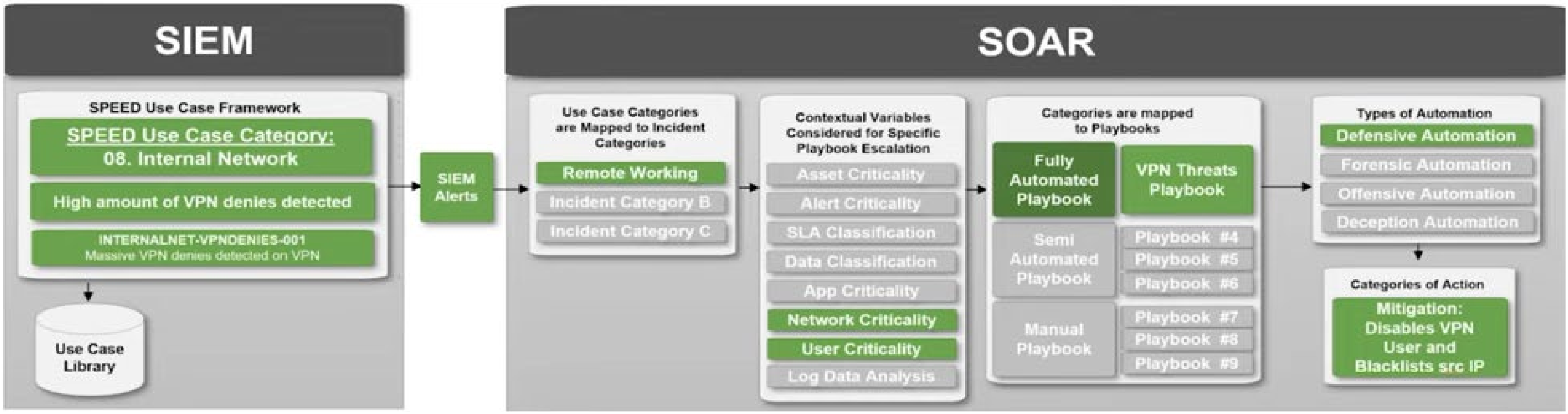
- Comprehensive visibility and forensic investigation capabilities.
- Reduced Mean Time to Detect (MTTD) and Respond (MTTR).
- Automated, playbook-driven incident response.
- Standardized compliance and configuration monitoring.
- Seamless orchestration across disparate security tools.
- Improved analyst productivity and reduced operational fatigue.



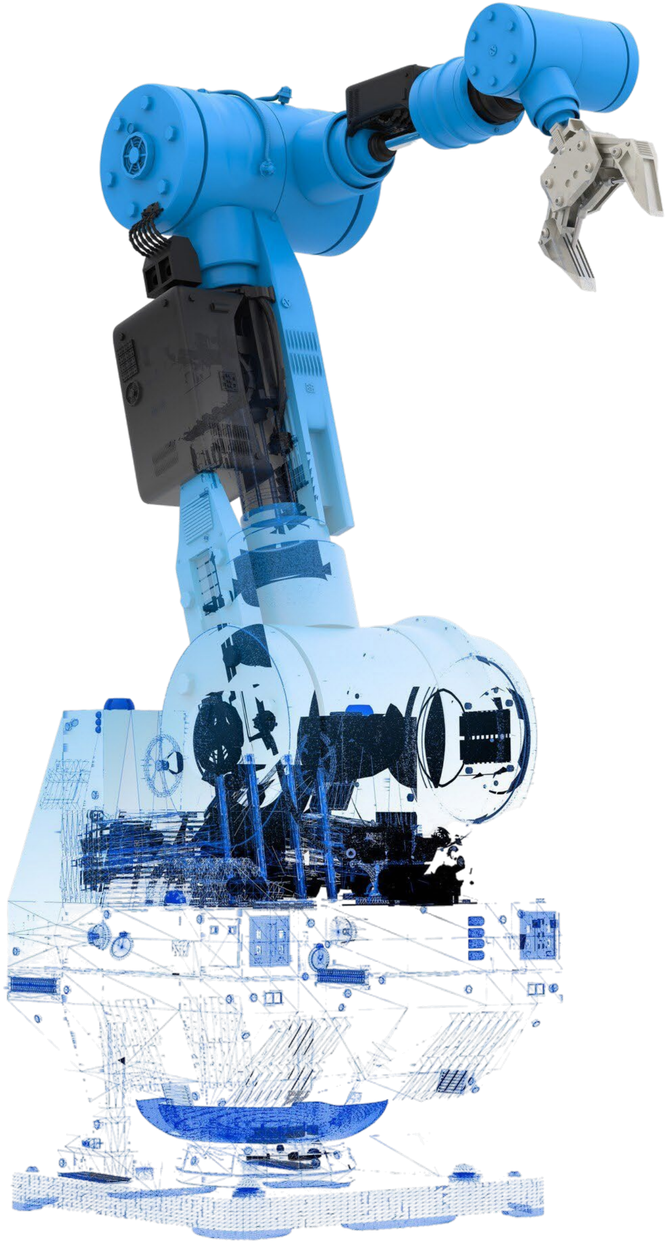
CiBRAI SOAR is an advanced, fully integrated orchestration and automation engine built into the CiBRAI Core SIEM. It enables security teams to automate repetitive tasks, accelerate threat response, and enhance incident consistency. Event-driven triggers launch preconfigured workflows that handle everything from threat enrichment and alert triage to containment and notification. With visual workflow builders, seamless API integrations, and threat intelligence feeds, SOAR delivers fast, intelligent, and automated decision-making. It empowers SOCs to manage complex threats like phishing, malware, and account compromise with minimal manual effort and maximum consistency.







- Designed for scalability and operational agility in diverse environments.
- Enables seamless cross-platform integration with secure, identity-aware execution (SSO).
- Rapidly onboards new tools using open standards like REST and OpenAPI.
- Automates high-frequency use cases such as suspicious emails, rogue assets, and privilege escalation.
- Logs every action to support compliance and governance requirements.
- Reduces operational costs while boosting analyst productivity.
- Improves incident containment times through intelligent automation.
- Delivers critical capabilities for modern security operations centers.

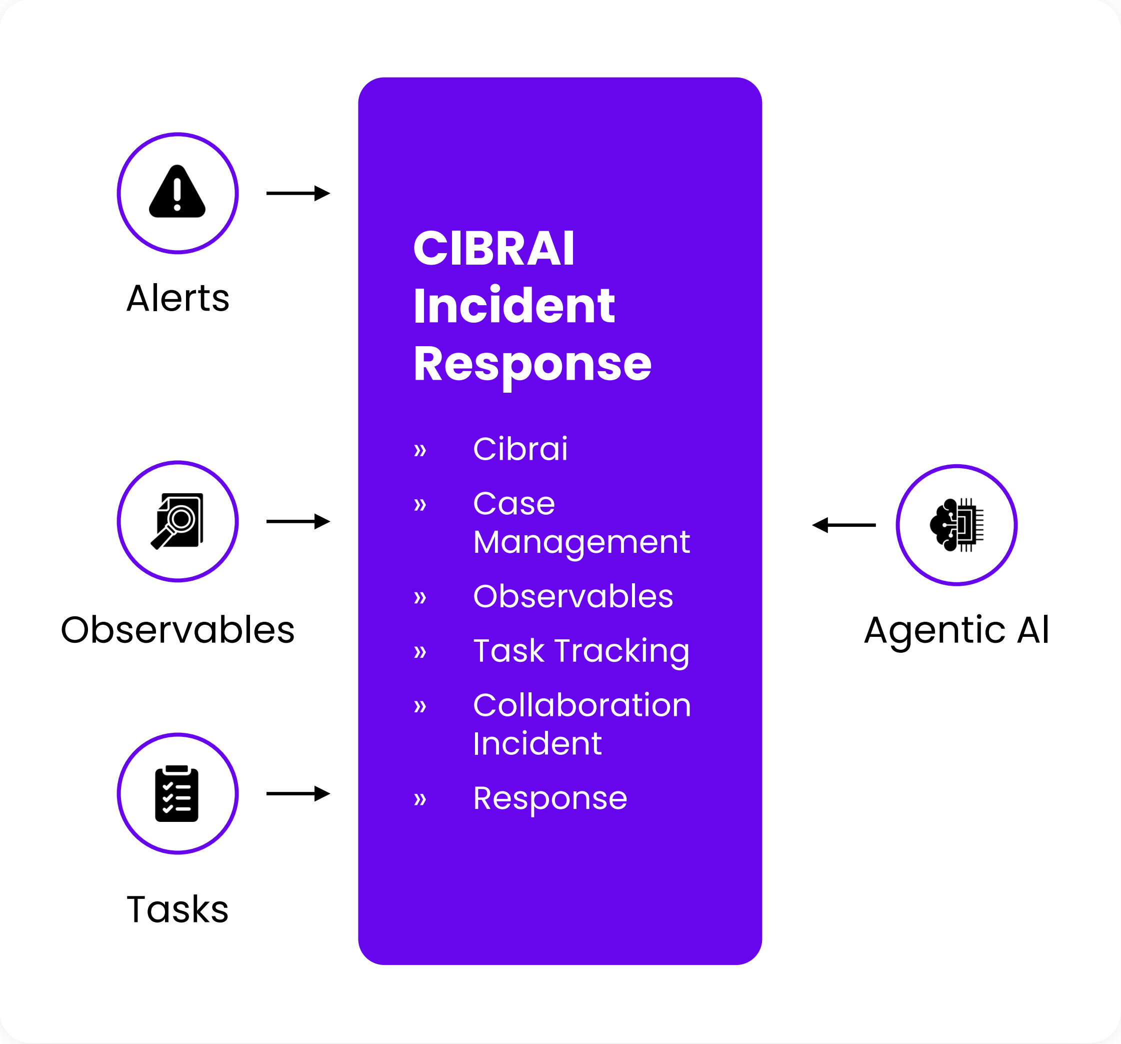


KEY CAPABILITIES

- **Event-Driven Automation** – Triggers respond to contextual alerts and initiate automated workflows.
- **Visual Workflow Orchestration** – Modular playbooks enrich, correlate, and respond to threats.
- **Integrated Threat Intelligence** – Real-time enrichment with feeds like MISP and VirusTotal.
- **Active Response Actions** – Auto-blocking, quarantine, user disablement, and team alerts.
- **Cross-Platform Compatibility** – Works across cloud, on-prem, and hybrid environments.
- **SSO & Identity-Aware Execution** – Secures automation with user-specific permissions.
- **Proven Use Cases** – Phishing response workflows save hours per incident.
- **Strategic Value** – Lowers costs, improves resilience, and ensures auditability and scalability.Ask ChatGPT

CIBRAI INCIDENT RESPONSE (WITH AGENTIC AI INTEGRATION)

An Enterprise-Grade Case Management System
In the modern threat landscape, SOCs and CSIRTs confront increasing alert volumes and complexity. CiBRAI's IR platform, based on TheHive & Cortex, delivers a robust, scalable, and collaborative incident response solution designed to streamline and enhance the entire lifecycle of incident handling—from ingestion and triage to deep analysis and resolution.



Alerts

Observables

Tasks

CIBRAI Incident Response

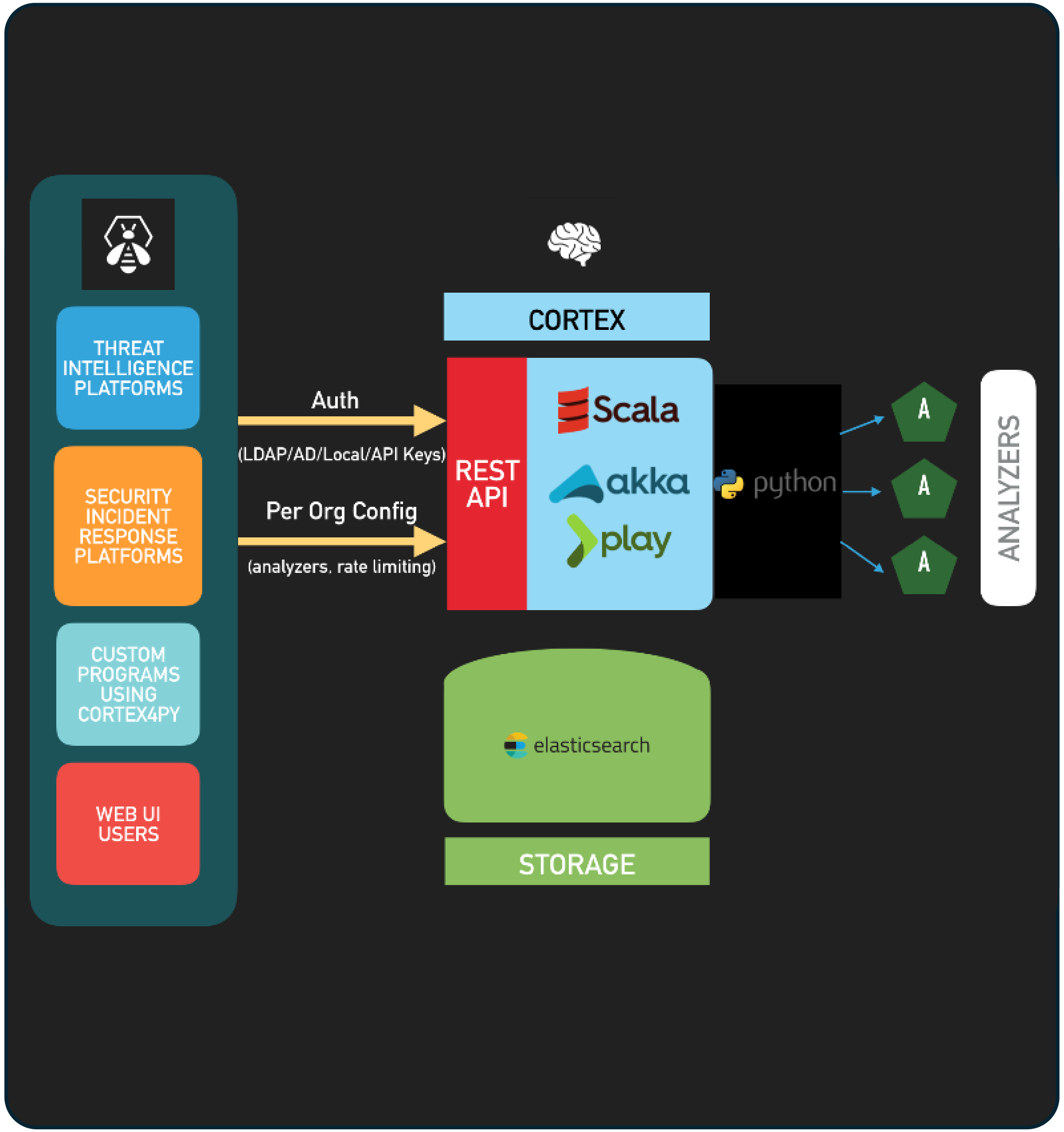
- » Cibrai
- » Case Management
- » Observables
- » Task Tracking
- » Collaboration Incident
- » Response

Agentic AI

CIBRAI INCIDENT RESPONSE (WITH AGENTIC AI INTEGRATION)

Core Features

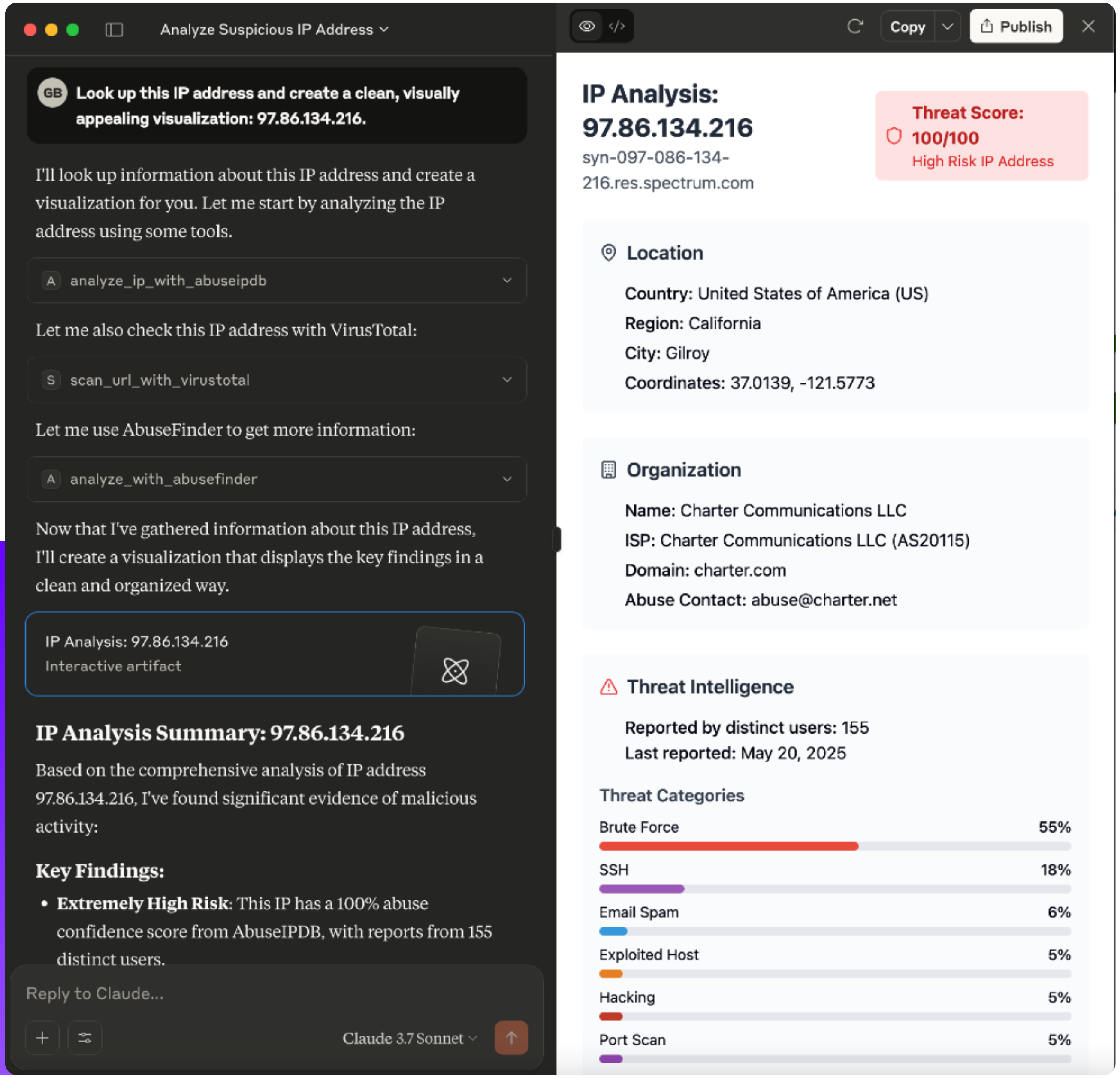
- Supports centralized alert collection across heterogeneous security tools.
- Integrates seamlessly with existing infrastructure via REST APIs and connectors.
- Enhances analyst efficiency by focusing attention on high-priority alerts.
- Facilitates structured incident creation from raw alerts.
- Reduces noise by filtering and prioritizing meaningful security signals.


THREAT INTELLIGENCE PLATFORMS
SECURITY INCIDENT RESPONSE PLATFORMS
CUSTOM PROGRAMS USING CORTEX4PY
WEB UI USERS
Auth
(LDAP/AD/Local/API Keys)
Per Org Config
(analyzers, rate limiting)
CORTEX
REST API
Scala
akka
play
python
A
A
A
ANALYZERS
elasticsearch
STORAGE

FLEXIBLE CASE & TASK MANAGEMENT

CiBRAI’s Incident Response (IR) platform offers a powerful, modular solution for modern SOCs, combining automated case management, real-time collaboration, and advanced threat enrichment. It supports customizable case templates, RBAC, and live-stream coordination, while integrating seamlessly with Cortex analyzers, SIEMs, and CTI platforms like MISP.

Features include bulk observable enrichment, automated responses (e.g., IP blocking, endpoint isolation), and flexible deployment across secure zones. Dashboards provide operational KPIs, audit trails ensure governance, and exportable reports support compliance. Designed for scalability, automation, and collaboration, CiBRAI IR accelerates response times, reduces analyst burden, and enhances threat management with clarity and control.



GB **Look up this IP address and create a clean, visually appealing visualization: 97.86.134.216.**

I'll look up information about this IP address and create a visualization for you. Let me start by analyzing the IP address using some tools.

A analyze_ip_with_abuseipdb

Let me also check this IP address with VirusTotal:

S scan_url_with_virustotal

Let me use AbuseFinder to get more information:

A analyze_with_abusefinder

Now that I've gathered information about this IP address, I'll create a visualization that displays the key findings in a clean and organized way.

IP Analysis: 97.86.134.216
Interactive artifact

IP Analysis Summary: 97.86.134.216

Based on the comprehensive analysis of IP address 97.86.134.216, I've found significant evidence of malicious activity:

Key Findings:

- **Extremely High Risk**: This IP has a 100% abuse confidence score from AbuseIPDB, with reports from 155 distinct users.

Reply to Claude...

Claude 3.7 Sonnet

IP Analysis: 97.86.134.216
syn-097-086-134-216.res.spectrum.com

Threat Score: 100/100
High Risk IP Address

Location

Country: United States of America (US)
Region: California
City: Gilroy
Coordinates: 37.0139, -121.5773

Organization

Name: Charter Communications LLC
ISP: Charter Communications LLC (AS20115)
Domain: charter.com
Abuse Contact: abuse@charter.net

Threat Intelligence

Reported by distinct users: 155
Last reported: May 20, 2025

Threat Categories

Brute Force	55%
SSH	18%
Email Spam	6%
Exploited Host	5%
Hacking	5%
Port Scan	5%

STANDARDS-BASED AGENTIC AI – MODEL CONTEXT PROTOCOL OVERVIEW

The Model Context Protocol (MCP) is the integration backbone of the CiBRAI ecosystem, enabling seamless, API-driven interoperability between the CiBRAI Core SIEM, Incident Response Platform, Cortex analyzers, and Agentic AI. MCP streamlines the flow of alerts, observables, and automated actions across detection, investigation, and response layers.

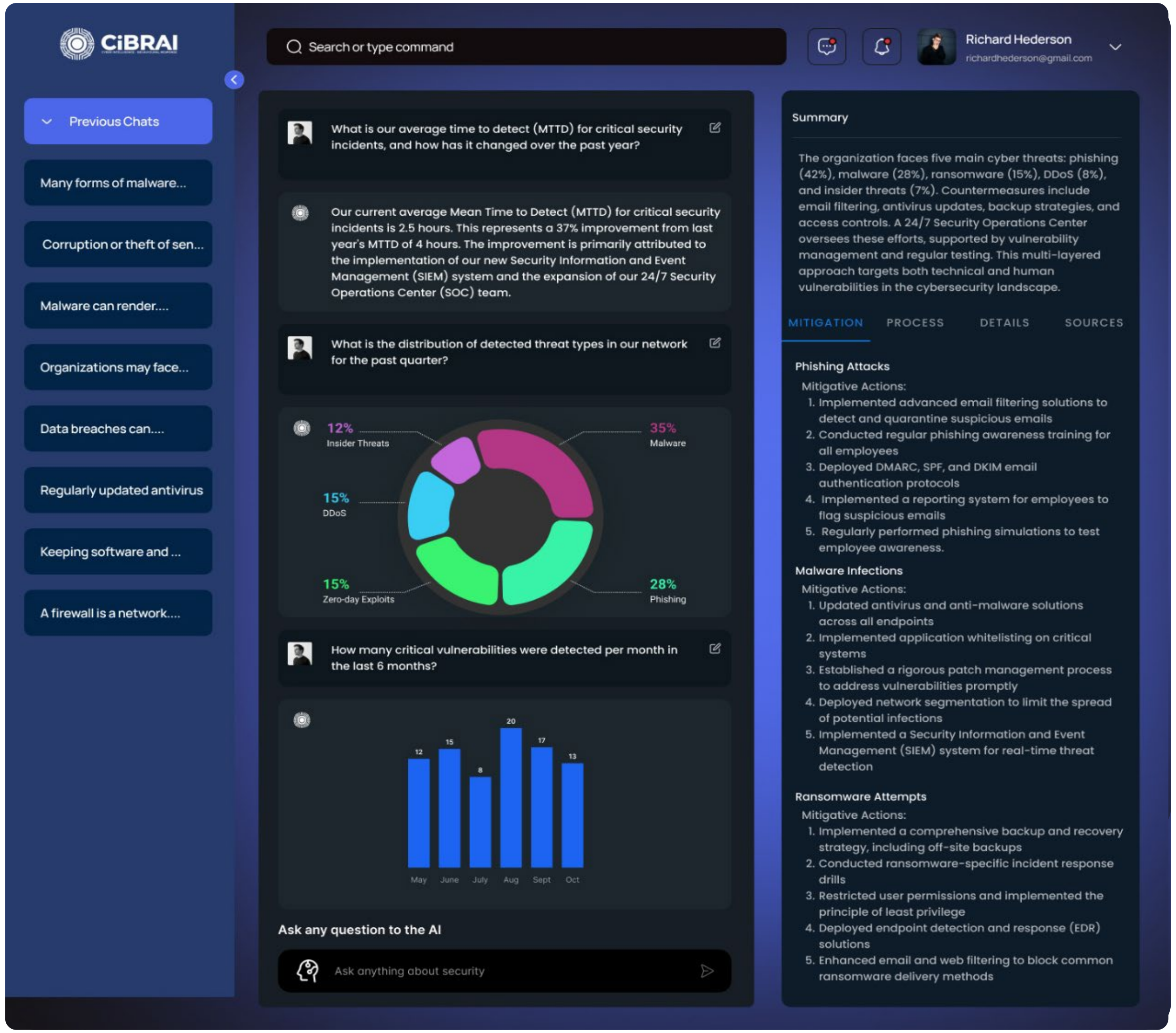
It supports real-time telemetry ingestion, enriched alert handling, structured case lifecycle management, and automated threat intelligence enrichment and response execution. By embedding AI-driven prioritisation and decision support into workflows, MCP empowers security teams to move from fragmented, manual processes to orchestrated, scalable, and intelligent cyber defense operations with full auditability.

CYBER THREAT INTELLIGENCE (CTI)

Integrates real-time threat intelligence to enrich security data with actionable insights.

Enhances detection accuracy and improves incident prioritization.

Strengthens strategic threat response through advanced intelligence integration.



What is our average time to detect (MTTD) for critical security incidents, and how has it changed over the past year?

Our current average Mean Time to Detect (MTTD) for critical security incidents is 2.5 hours. This represents a 37% improvement from last year's MTTD of 4 hours. The improvement is primarily attributed to the implementation of our new Security Information and Event Management (SIEM) system and the expansion of our 24/7 Security Operations Center (SOC) team.

What is the distribution of detected threat types in our network for the past quarter?

How many critical vulnerabilities were detected per month in the last 6 months?

Ask any question to the AI

Summary

The organization faces five main cyber threats: phishing (42%), malware (28%), ransomware (15%), DDoS (8%), and insider threats (7%). Countermeasures include email filtering, antivirus updates, backup strategies, and access controls. A 24/7 Security Operations Center oversees these efforts, supported by vulnerability management and regular testing. This multi-layered approach targets both technical and human vulnerabilities in the cybersecurity landscape.

Phishing Attacks

Mitigative Actions:

1. Implemented advanced email filtering solutions to detect and quarantine suspicious emails
2. Conducted regular phishing awareness training for all employees
3. Deployed DMARC, SPF, and DKIM email authentication protocols
4. Implemented a reporting system for employees to flag suspicious emails
5. Regularly performed phishing simulations to test employee awareness.

Malware Infections

Mitigative Actions:

1. Updated antivirus and anti-malware solutions across all endpoints
2. Implemented application whitelisting on critical systems
3. Established a rigorous patch management process to address vulnerabilities promptly
4. Deployed network segmentation to limit the spread of potential infections
5. Implemented a Security Information and Event Management (SIEM) system for real-time threat detection

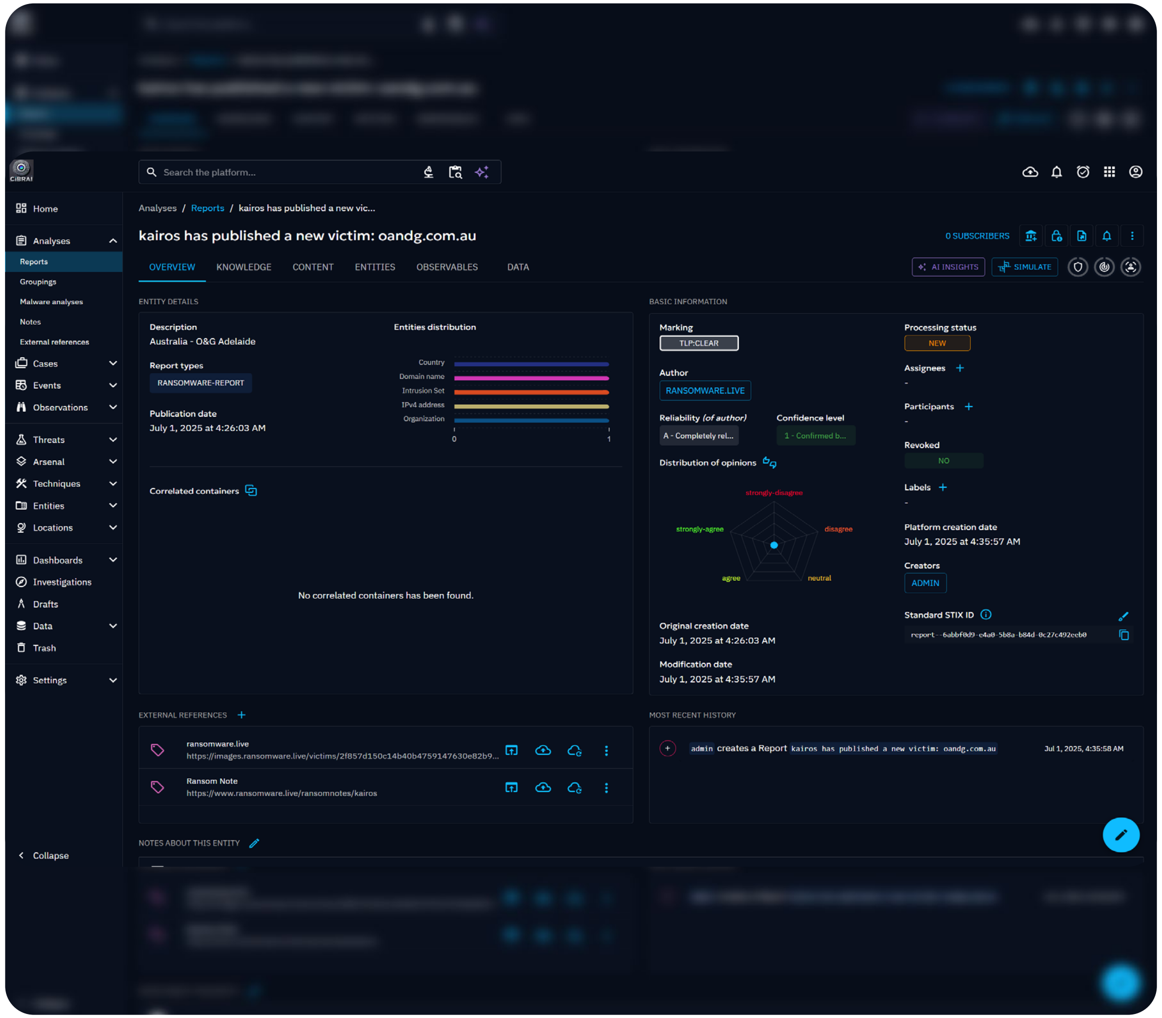
Ransomware Attempts

Mitigative Actions:

1. Implemented a comprehensive backup and recovery strategy, including off-site backups
2. Conducted ransomware-specific incident response drills
3. Restricted user permissions and implemented the principle of least privilege
4. Deployed endpoint detection and response (EDR) solutions
5. Enhanced email and web filtering to block common ransomware delivery methods

CYBER THREAT INTELLIGENCE (CTI)

Our full, enhanced CTI dataset is fully exposed using the integrated OpenCTI stack as seen above.



Analyses / Reports / kairos has published a new vic...

kairos has published a new victim: oandg.com.au

ENTITY DETAILS

Description
Australia - O&G Adelaide

Report types
RANSOMWARE-REPORT

Publication date
July 1, 2025 at 4:26:03 AM

Correlated containers

No correlated containers has been found.

BASIC INFORMATION

Marking
TLP:CLEAR

Author
RANSOMWARE.LIVE

Reliability *(of author)*
A - Completely rel...

Confidence level
1 - Confirmed b...

Original creation date
July 1, 2025 at 4:26:03 AM

Modification date
July 1, 2025 at 4:35:57 AM

Processing status
NEW

Assignees
-

Participants
-

Revoked
NO

Labels
-

Platform creation date
July 1, 2025 at 4:35:57 AM

Creators
ADMIN

Standard STIX ID
report--6abbf0d9-e4a0-5b8a-b84d-0c27c492eeb0

EXTERNAL REFERENCES

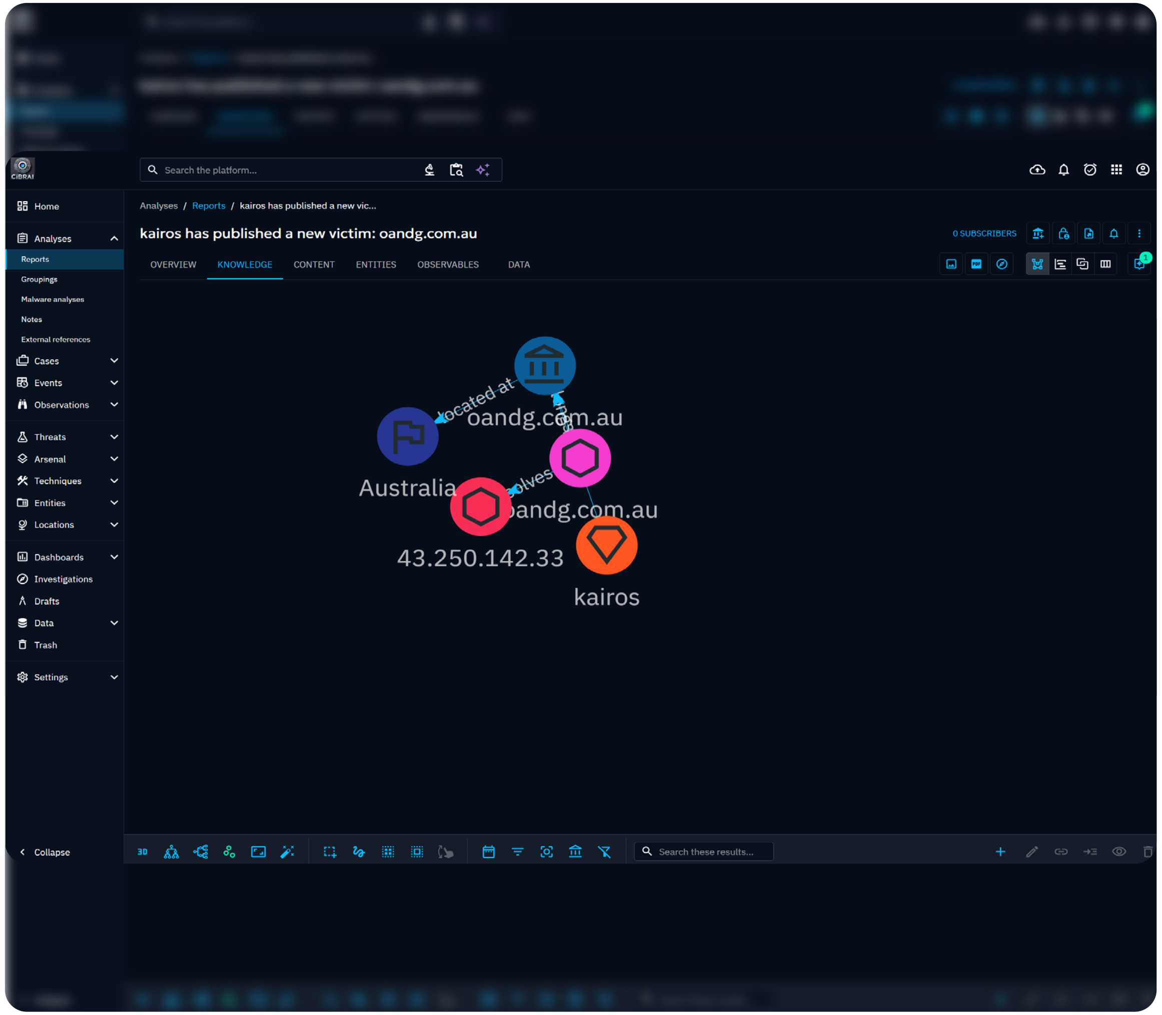
ransomware.live
https://images.ransomware.live/victims/2f857d150c14b40b4759147630e82b9...

Ransom Note
https://www.ransomware.live/ransomnotes/kairos

MOST RECENT HISTORY

admin creates a Report kairos has published a new victim: oandg.com.au — Jul 1, 2025, 4:35:58 AM

NOTES ABOUT THIS ENTITY



Analyses / Reports / kairos has published a new vic...

kairos has published a new victim: oandg.com.au

AGENTIXCYBER AI-ENHANCED CYBERSECURITY MODULE

01.

Ai-enhanced cybersecurity

CiBRAI leverages AgentiXCyber AI to boost internal cybersecurity with virtual SOC operators, real-time threat detection, and intelligent reporting.

02.

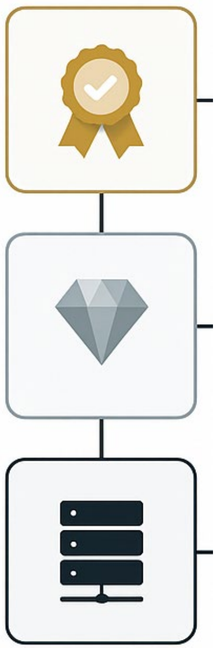
Evolving capabilities

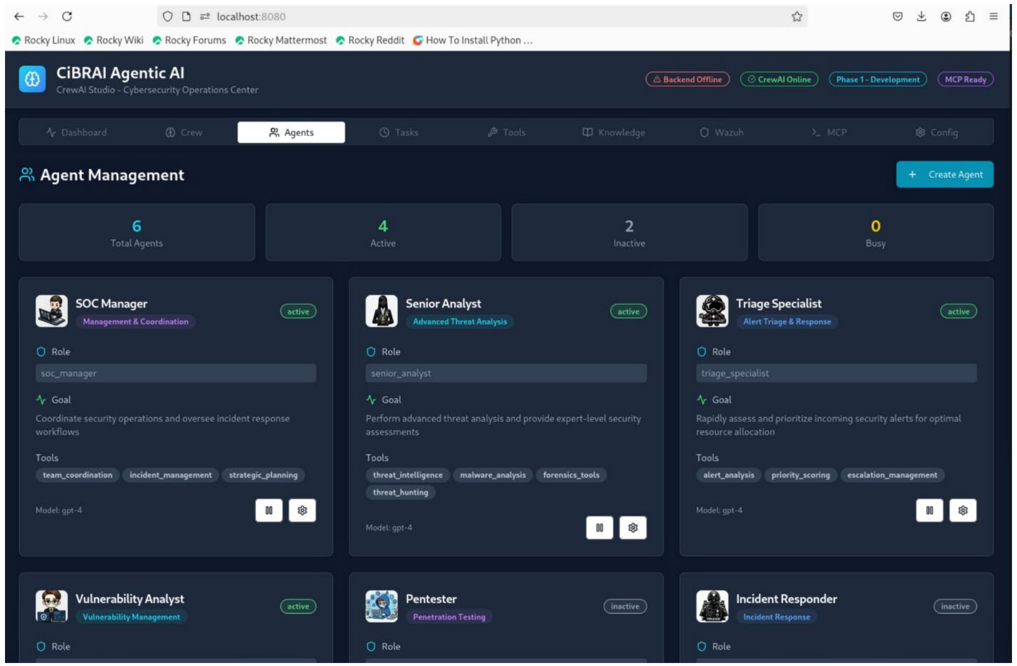
The platform continuously improves with each version, adding new features for proactive security operations.

03.

Scalable deployment options

CiBRAI offers Gold (shared), Platinum (dedicated), and Titanium (on-premise) tiers to match different operational and compliance needs.





CiBRAI Agentic AI

CrewAI Studio - Cybersecurity Operations Center

Agent Management

6 Total Agents | 4 Active | 2 Inactive | 0 Busy

SOC Manager — Management & Coordination — active

Role: soc_manager

Goal: Coordinate security operations and oversee incident response workflows

Tools: team_coordination, incident_management, strategic_planning

Model: gpt-4

Senior Analyst — Advanced Threat Analysis — active

Role: senior_analyst

Goal: Perform advanced threat analysis and provide expert-level security assessments

Tools: threat_intelligence, malware_analysis, forensics_tools, threat_hunting

Model: gpt-4

Triage Specialist — Alert Triage & Response — active

Role: triage_specialist

Goal: Rapidly assess and prioritize incoming security alerts for optimal resource allocation

Tools: alert_analysis, priority_scoring, escalation_management

Model: gpt-4

Vulnerability Analyst — Vulnerability Management — active

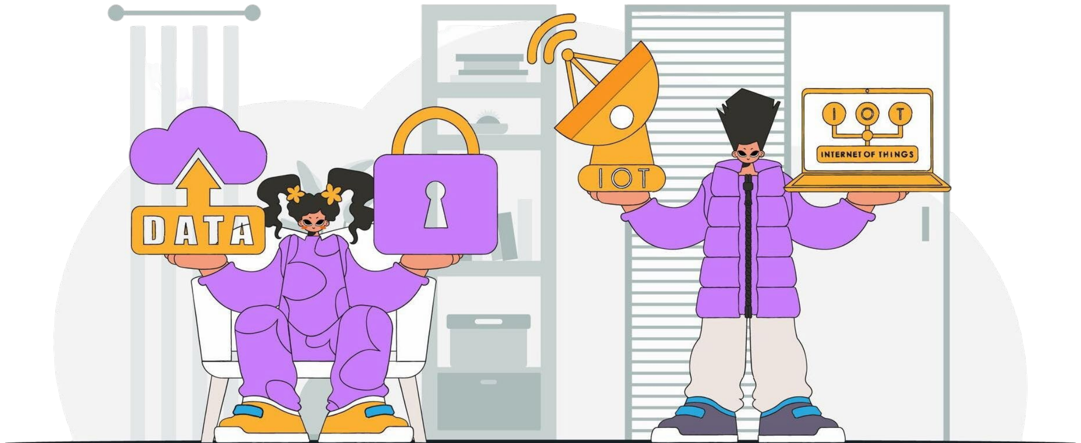
Role

Pentester — Penetration Testing — inactive

Role

Incident Responder — Incident Response — inactive

Role



TIERED PRICING AND DEPLOYMENT MODELS

COMPONENT	SILVER TIER	GOLD TIER	PLATINUM TIER	TITANIUM TIER (ON-PREMISE)
Positioning	Entry-level, cost-effective solution providing core cybersecurity features and analytics.	Mid-tier comprehensive security solution balancing cost and enhanced capability.	Premium-tier dedicated infrastructure with advanced AI integration, maximum capability, and scalability.	Fully client-owned, on-premise solution with maximum customisation, control, and operational flexibility.
Infrastructure Hosting	Shared virtualised infrastructure (Macquarie Park or Equinix Sydney)	Enhanced shared virtualised infrastructure (Macquarie Park or Equinix Sydney)	Dedicated private cloud infrastructure (Macquarie Park or Equinix Sydney)	Client-dedicated hardware infrastructure within own rack (Macquarie Park or Equinix Sydney)
Managed Storage Capacity	100TB	200TB	500TB	Dedicated storage (capacity based on client-managed hardware)
Data Ingestion Limits	Unlimited (up to 3,000 EPS)	Unlimited (no EPS cap)	Unlimited (no EPS cap)	Unlimited (limited only by hardware capability)
Platform & GPU Resources	Shared GPUs & hardware	Enhanced shared GPUs & hardware	Dedicated high-performance GPUs with advanced water-cooling technology	Dedicated GPUs & high-performance compute with advanced water-cooling (client-owned & managed)
Seamless Intelligence Co-Management	Optional	Included (5x9 primary support, 24x7 escalation)	Included (full 24x7 dedicated support & escalation)	Optional (24x7 support & escalation available)
Advanced Analytics & Threat Hunting	Optional	Optional	Included	Included
Cyber Threat Intelligence (RST Cloud)	Included	Included	Included	Included
Regular Compliance & Security Reporting	Optional	Optional	Included	Included
Annual Penetration Testing Allowance	Optional	Optional	Included (10 days annually)	Included (10 days annually)
Customisation & Integration Support	Optional (Time & Materials)	Optional (Time & Materials)	Included	Included
User Training & Certification	Optional	Optional	Included (Unlimited sessions annually)	Included (Annual Training Allowance)
Availability & Support Hours	5x9 Technical & operational support	5x9 Technical & operational support	24x7 Technical & operational support	24x7 Technical & operational support
Deployment Type	Shared Virtualised Infrastructure	Enhanced Shared Virtualised Infrastructure	Dedicated Private Cloud Infrastructure	Dedicated Hardware Appliance (On-Premise)
Licensing Model	Annual Subscription	Annual Subscription	Annual Subscription	Annual Licence & Maintenance
Scalability	Moderate (upgrade available to higher tiers)	High (flexible scalability)	High (dedicated, flexible scalability)	Completely flexible (limited only by client infrastructure)
AI Integration & Reporting	Standard AI Modules (Shared GPU)	Enhanced AI Modules (Shared GPU)	Advanced Dedicated AI Modules (Dedicated GPU)	Dedicated AI Modules (Dedicated GPU)
Data Sovereignty	Fully hosted within Australia (Sydney)	Fully hosted within Australia (Sydney)	Fully hosted within Australia (Sydney)	Fully hosted within Australia (Sydney)
SIEM Ruleset Development & Tuning	Optional via Co-Managed service	Included via Co-Managed service	Included via Co-Managed service	via Co-Managed service
Incident Response & Case Management	Optional via Co-Managed service	Included via Co-Managed service	Included via Co-Managed service	via Co-Managed service

ADVANCED HARDWARE AND COOLING TECHNOLOGY

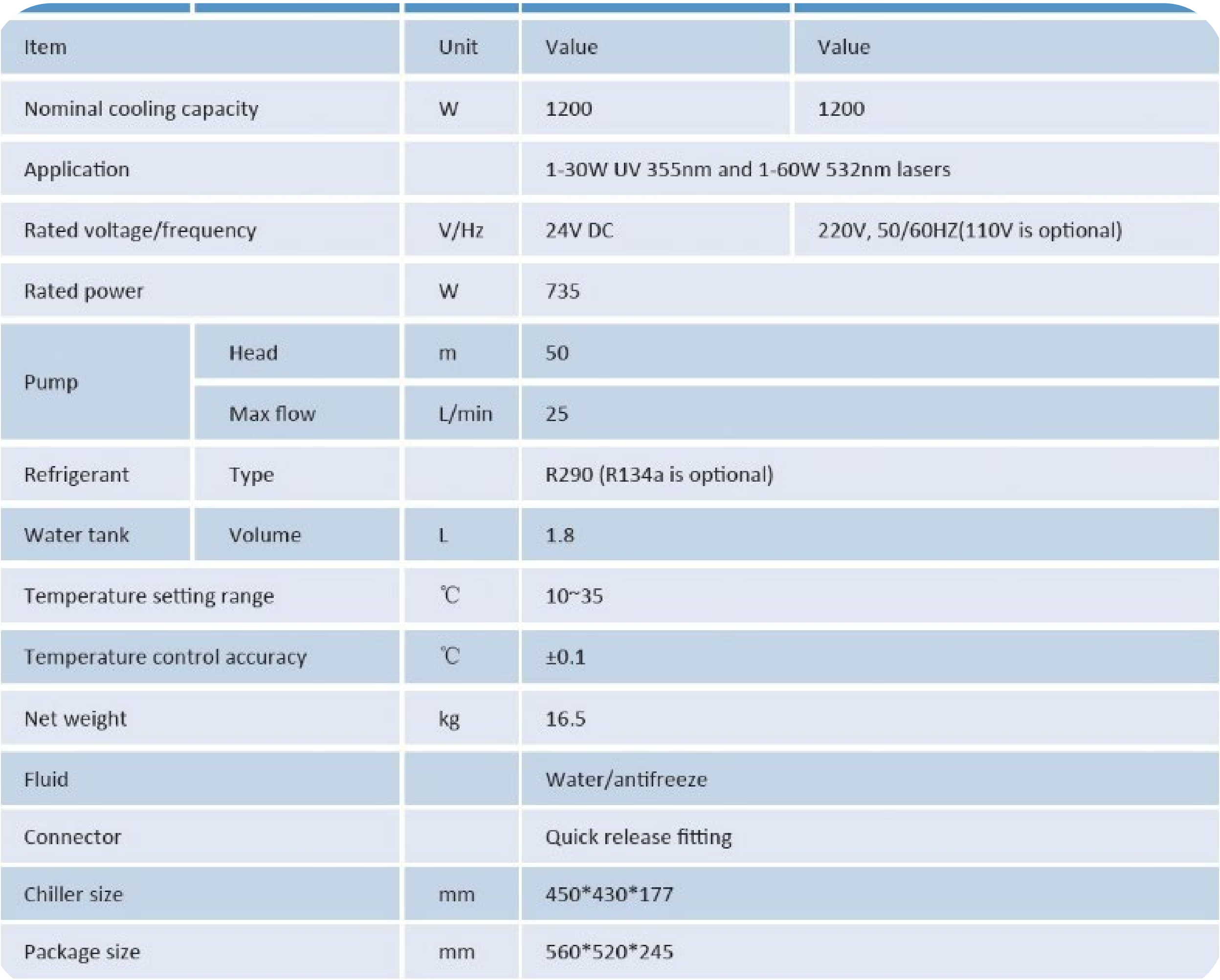
High-Performance Infrastructure

Platinum and Titanium tiers use GPU-accelerated, water-cooled hardware for efficient, reliable AI-driven cybersecurity.

Co-Managed SOC Integration

Seamless Intelligence provides 24x7 support and threat management to boost security and lighten your workload.

ADVANCED HARDWARE AND COOLING TECHNOLOGY



Item		Unit	Value	Value
Nominal cooling capacity		W	1200	1200
Application			1-30W UV 355nm and 1-60W 532nm lasers	
Rated voltage/frequency		V/Hz	24V DC	220V, 50/60HZ(110V is optional)
Rated power		W	735	
Pump	Head	m	50	
	Max flow	L/min	25	
Refrigerant	Type		R290 (R134a is optional)	
Water tank	Volume	L	1.8	
Temperature setting range		℃	10~35	
Temperature control accuracy		℃	±0.1	
Net weight		kg	16.5	
Fluid			Water/antifreeze	
Connector			Quick release fitting	
Chiller size		mm	450*430*177	
Package size		mm	560*520*245	

COMPLIANCE AND REGULATORY ALIGNMENT

Full Compliance

Meets Essential Eight, ISM, PSPF, and Australian data sovereignty requirements.

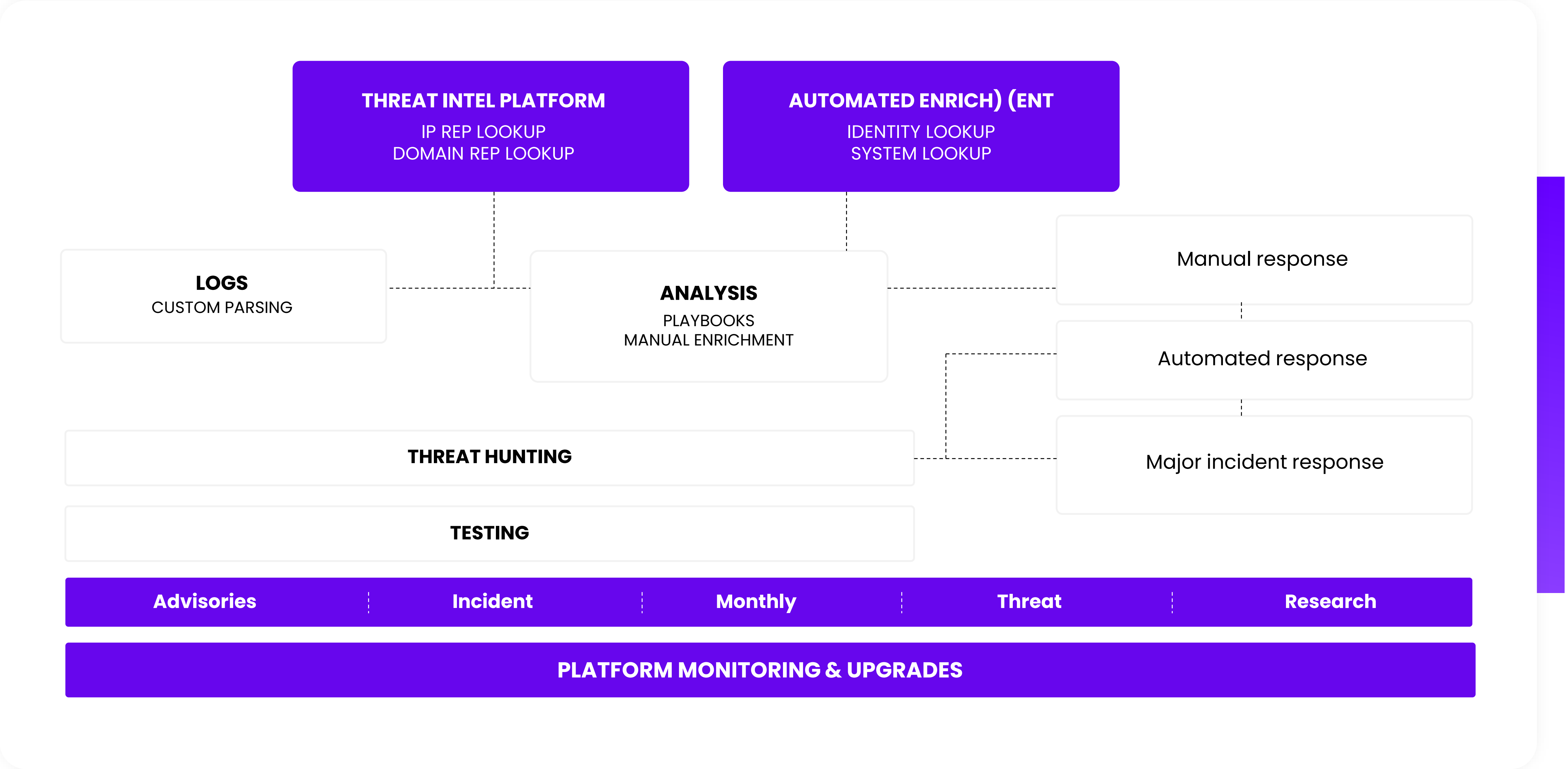
AI-Driven & Customisable

Delivers tailored AI-powered SOC capabilities with seamless system integration.

Scalable & Efficient

Offers flexible deployment tiers, co-managed SOC, and high-performance infrastructure.

COMPLIANCE AND REGULATORY ALIGNMENT



THREAT INTEL PLATFORM
IP REP LOOKUP
DOMAIN REP LOOKUP

AUTOMATED ENRICH) (ENT
IDENTITY LOOKUP
SYSTEM LOOKUP

LOGS
CUSTOM PARSING

ANALYSIS
PLAYBOOKS
MANUAL ENRICHMENT

Manual response

Automated response

Major incident response

THREAT HUNTING

TESTING

Advisories | **Incident** | **Monthly** | **Threat** | **Research**

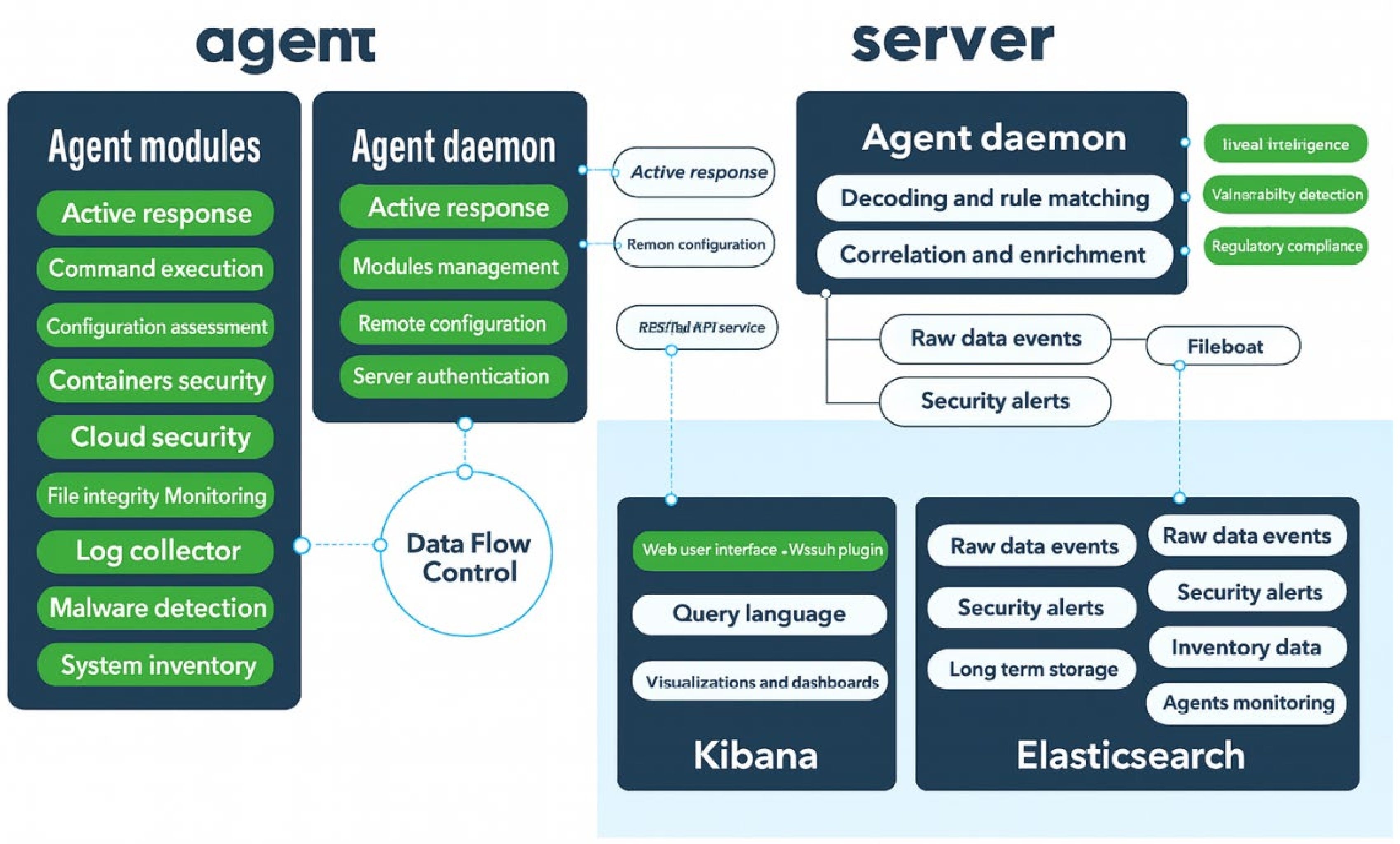
PLATFORM MONITORING & UPGRADES

SOLUTION TECHNICAL ARCHITECTURE

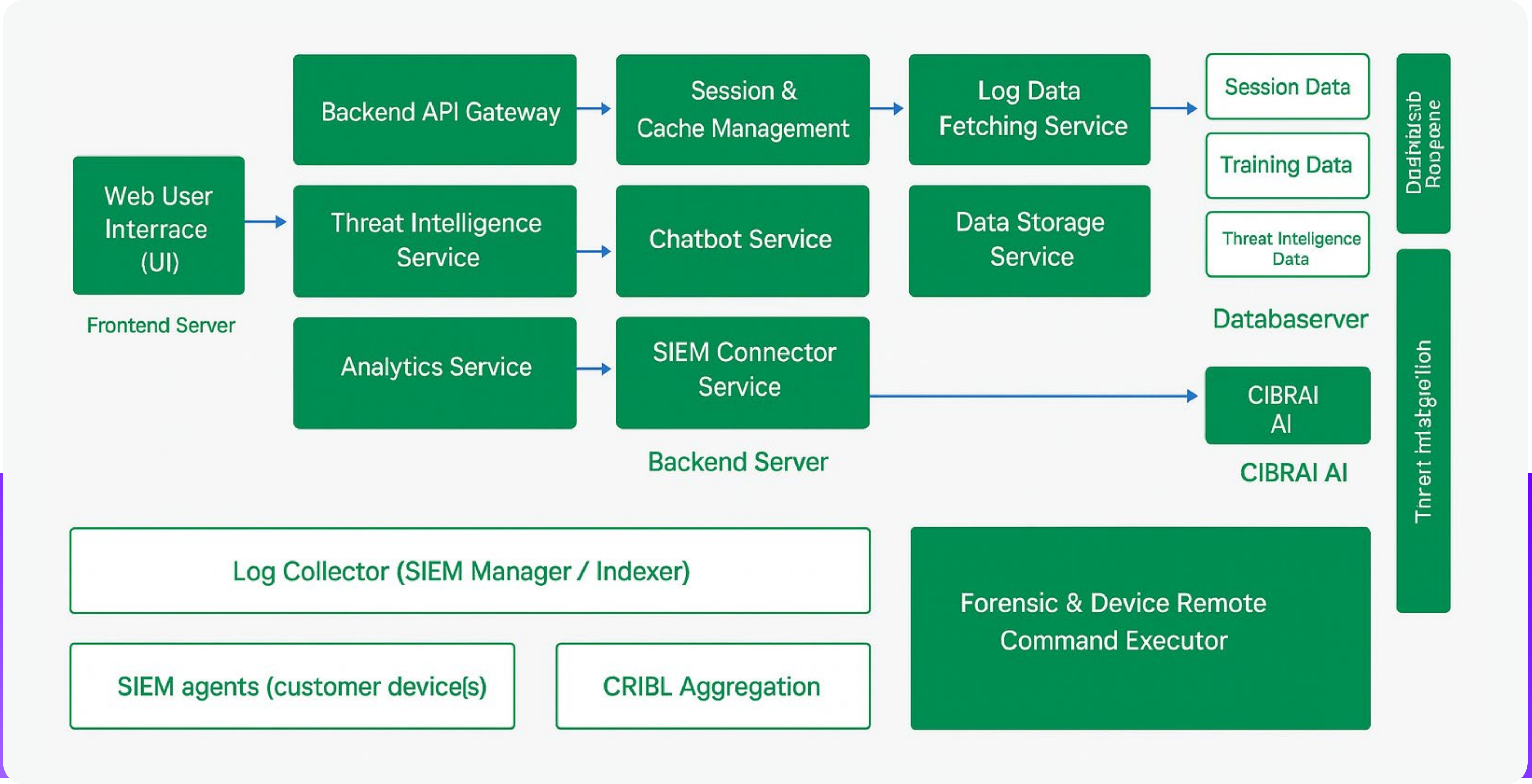
Overview

- Scalable on-premise cybersecurity architecture.
- Aligned with Australian standards (Essential Eight, ISM, PSPF)
- High-performance hardware and software integration.
- Ensures optimal protection and regulatory compliance.

SOLUTION TECHNICAL ARCHITECTURE



SOLUTION TECHNICAL ARCHITECTURE

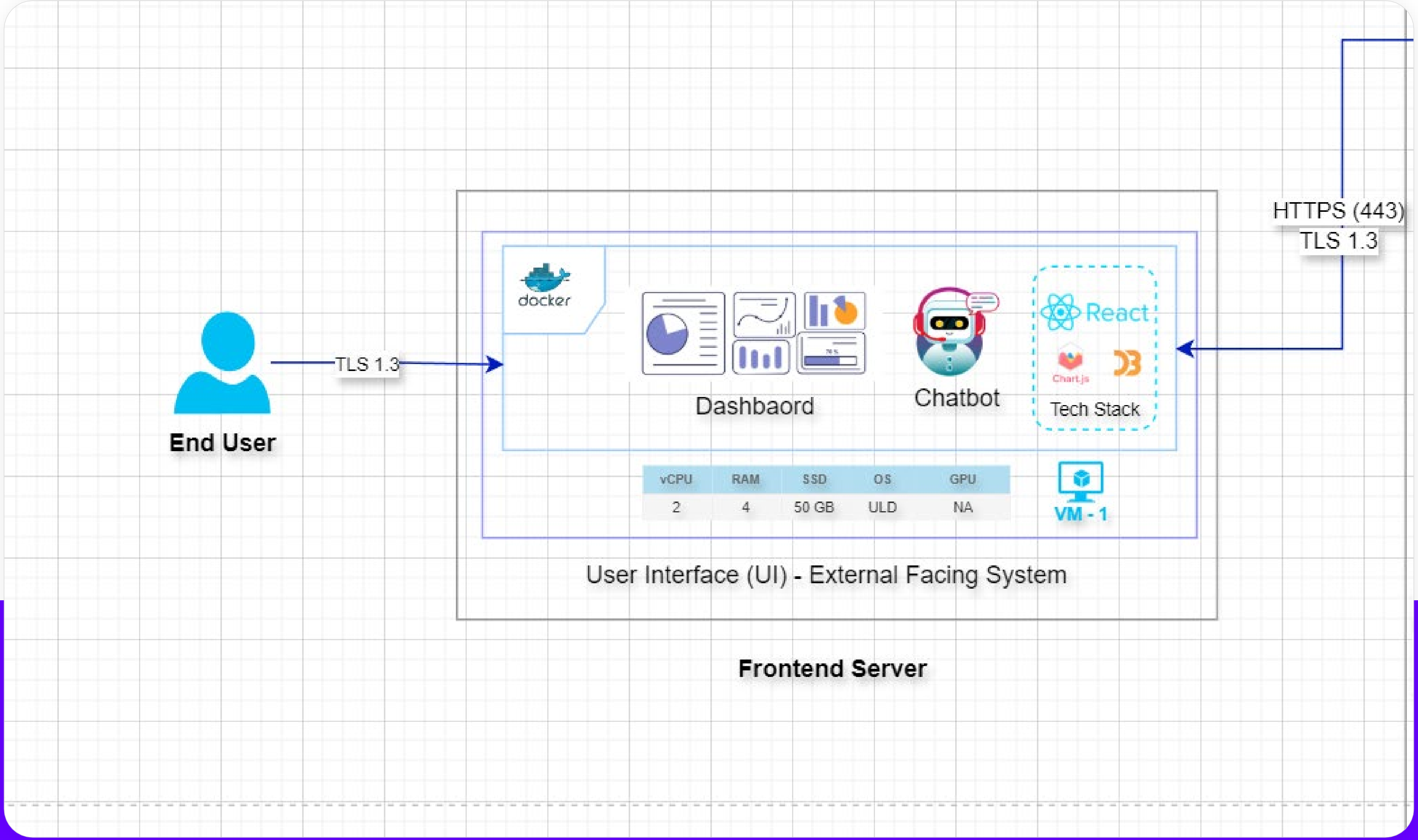


CORE ARCHITECTURAL COMPONENTS

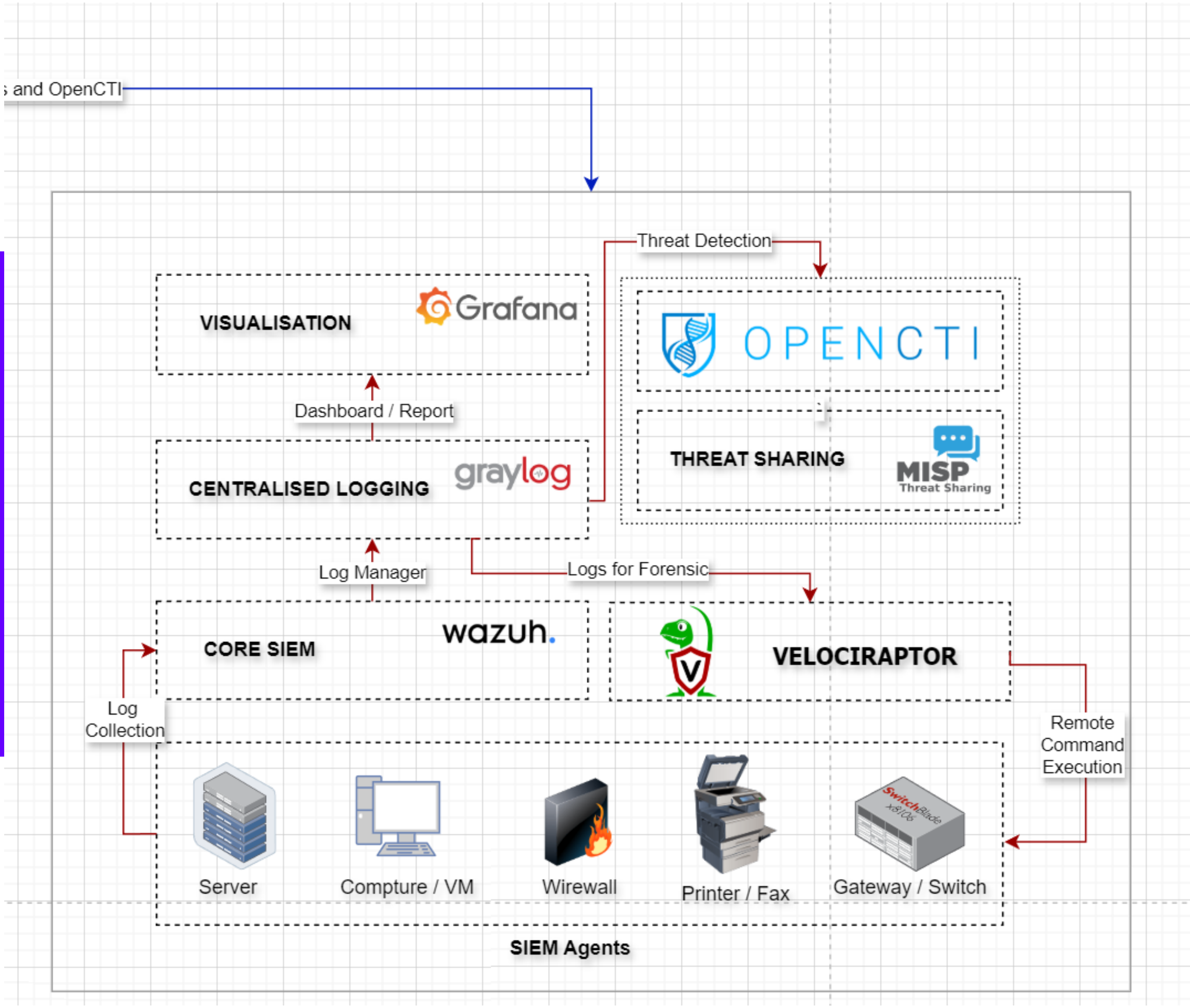
Core Architectural Components

- Includes a console-managed agent with built-in SIEM and forensics capabilities.
- Provides advanced, customizable dashboards for multi-level operational insights.
- Supports case management to track activities, incidents, and exceptions.
- Enables centralized visibility and control through an integrated architecture.

CORE ARCHITECTURAL COMPONENTS

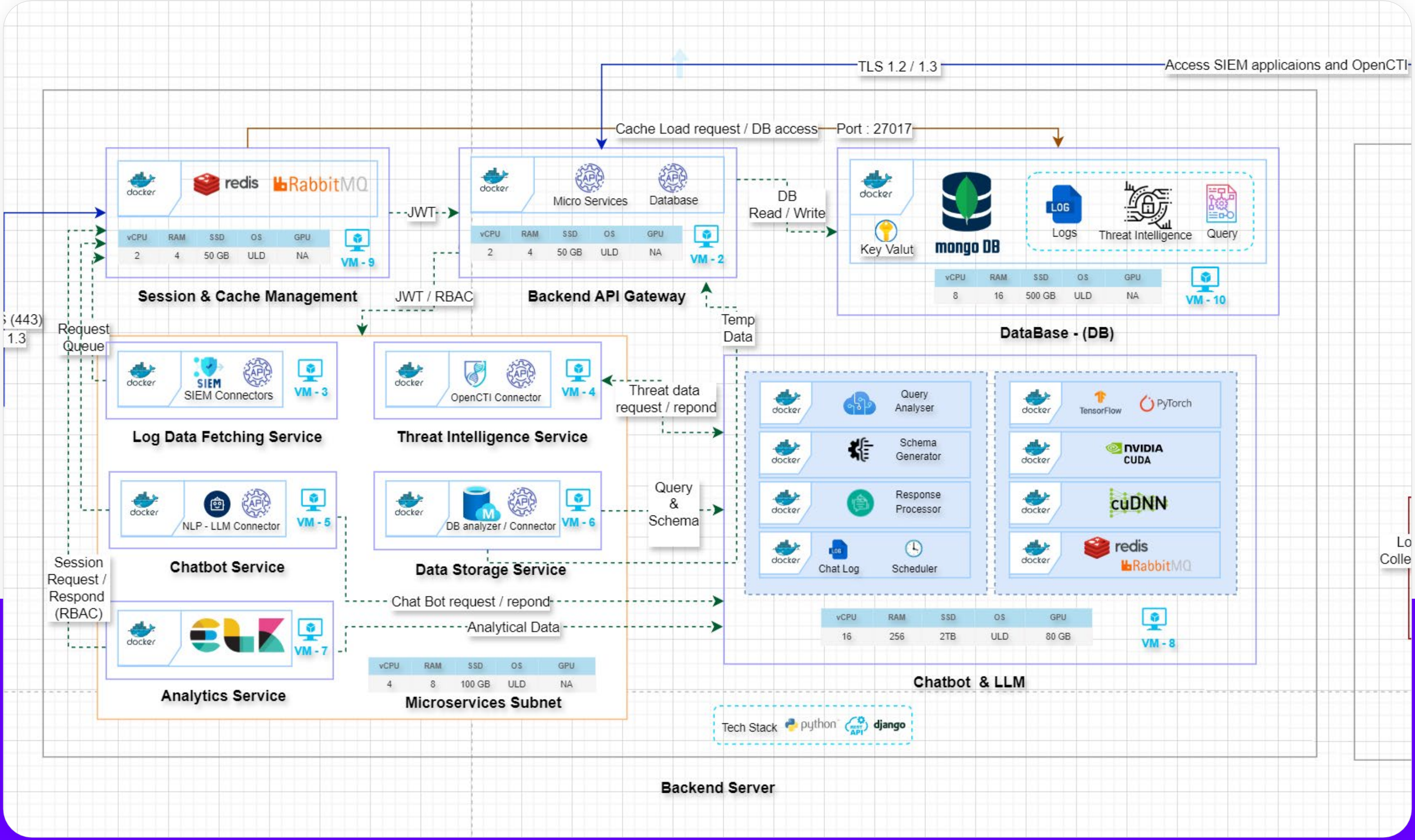


vCPU	RAM	SSD	OS	GPU
2	4	50 GB	ULD	NA



CORE ARCHITECTURAL COMPONENTS

CORE ARCHITECTURAL COMPONENTS



TLS 1.2 / 1.3

Access SIEM applicaions and OpenCTI

Cache Load request / DB access

Port : 27017

S (443)

1.3

JWT

JWT / RBAC

DB Read / Write

Temp Data

Request Queue

Threat data request / repond

Query & Schema

Session Request / Respond (RBAC)

Chat Bot request / repond

Analytical Data

Session & Cache Management

docker · redis · RabbitMQ · VM - 9

vCPU	RAM	SSD	OS	GPU
2	4	50 GB	ULD	NA

Backend API Gateway

docker · Micro Services · Database · VM - 2

vCPU	RAM	SSD	OS	GPU
2	4	50 GB	ULD	NA

DataBase - (DB)

docker · Key Valut · mongo DB · Logs · Threat Intelligence · Query · VM - 10

vCPU	RAM	SSD	OS	GPU
8	16	500 GB	ULD	NA

Log Data Fetching Service

docker · SIEM · SIEM Connectors · VM - 3

Threat Intelligence Service

docker · OpenCTI Connector · VM - 4

Chatbot Service

docker · NLP - LLM Connector · VM - 5

Data Storage Service

docker · DB analyzer / Connector · VM - 6

Analytics Service

docker · ELK · VM - 7

Microservices Subnet

vCPU	RAM	SSD	OS	GPU
4	8	100 GB	ULD	NA

Chatbot & LLM

docker · Query Analyser

docker · Schema Generator

docker · Response Processor

docker · Chat Log · Scheduler

docker · TensorFlow · PyTorch

docker · NVIDIA CUDA

docker · cuDNN

docker · redis · RabbitMQ

VM - 8

vCPU	RAM	SSD	OS	GPU
16	256	2TB	ULD	80 GB

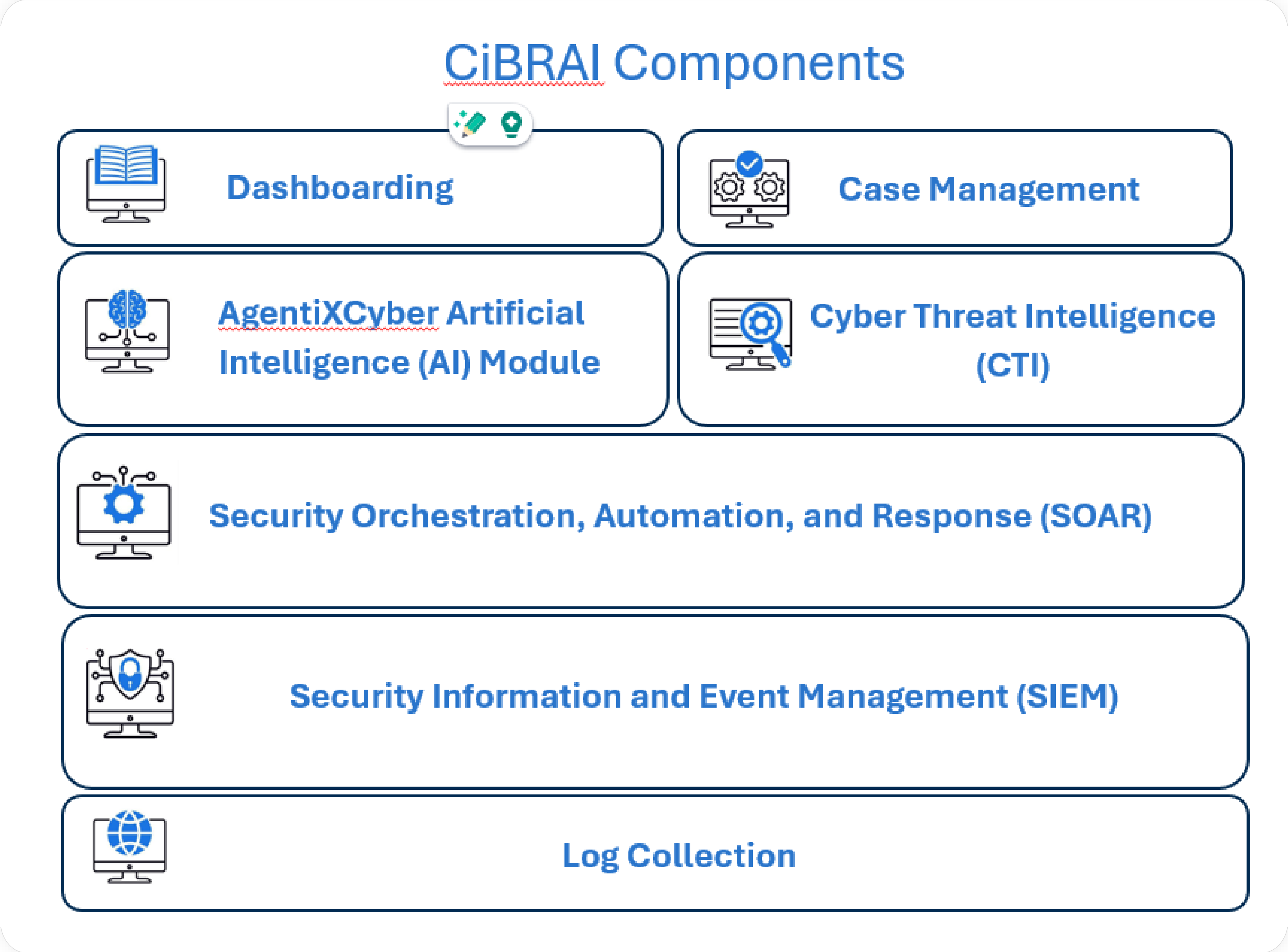
Tech Stack python API django

Backend Server

Lo

Colle

CORE ARCHITECTURAL COMPONENTS



CiBRAI Components

Dashboarding

Case Management

AgentiXCyber Artificial Intelligence (AI) Module

Cyber Threat Intelligence (CTI)

Security Orchestration, Automation, and Response (SOAR)

Security Information and Event Management (SIEM)

Log Collection

AGENTIXCYBER ARTIFICIAL INTELLIGENCE (AI) MODULE

01

AI-Powered Security

AgentiXCyber delivers automated threat detection, virtual SOC operations, and intelligent reporting.

02

Integrated Intelligence & SIEM

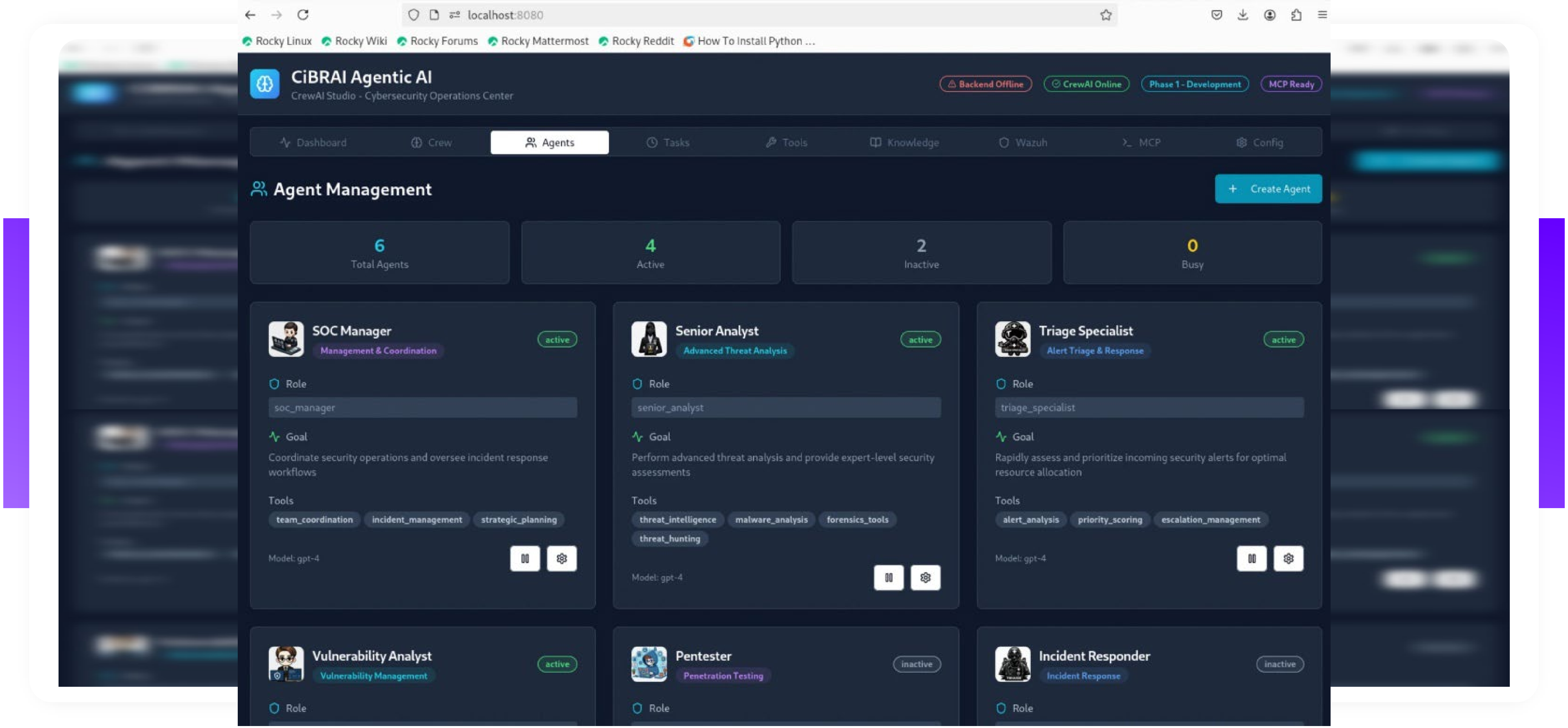
Real-time threat feeds, unlimited logging, and analytics ensure strong detection and compliance.

03

Automated Response

SOAR and event logging streamline incident handling with custom playbooks and system integration.

AGENTIXCYBER ARTIFICIAL INTELLIGENCE (AI) MODULE



CiBRAI Agentic AI

CrewAI Studio - Cybersecurity Operations Center

Agent Management

6 Total Agents

4 Active

2 Inactive

0 Busy

SOC Manager — Management & Coordination — active

Role: soc_manager

Goal: Coordinate security operations and oversee incident response workflows

Tools: team_coordination, incident_management, strategic_planning

Model: gpt-4

Senior Analyst — Advanced Threat Analysis — active

Role: senior_analyst

Goal: Perform advanced threat analysis and provide expert-level security assessments

Tools: threat_intelligence, malware_analysis, forensics_tools, threat_hunting

Model: gpt-4

Triage Specialist — Alert Triage & Response — active

Role: triage_specialist

Goal: Rapidly assess and prioritize incoming security alerts for optimal resource allocation

Tools: alert_analysis, priority_scoring, escalation_management

Model: gpt-4

Vulnerability Analyst — Vulnerability Management — active

Role

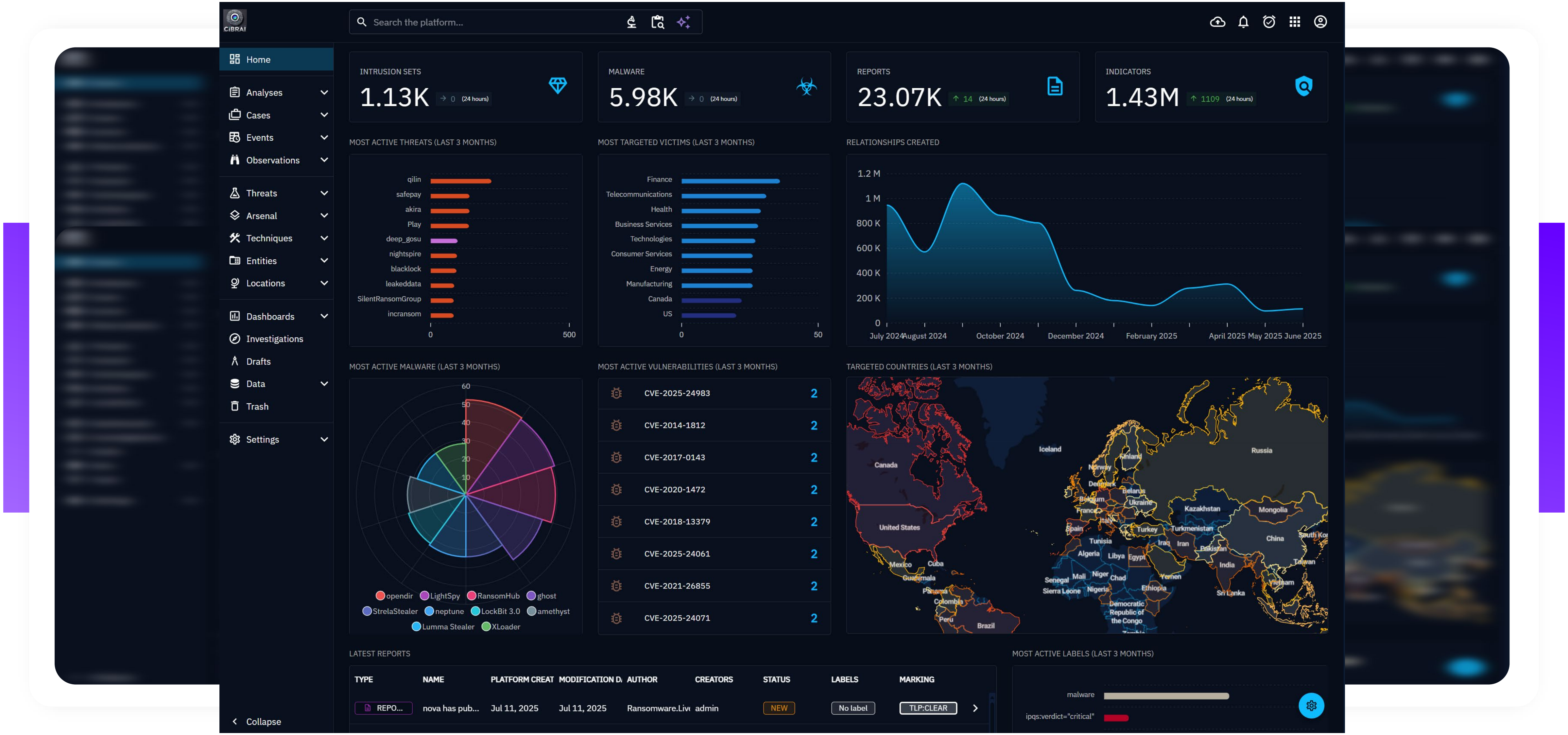
Pentester — Penetration Testing — inactive

Role

Incident Responder — Incident Response — inactive

Role

AGENTIXCYBER ARTIFICIAL INTELLIGENCE (AI) MODULE



INTRUSION SETS 1.13K → 0 (24 hours)

MALWARE 5.98K → 0 (24 hours)

REPORTS 23.07K ↑ 14 (24 hours)

INDICATORS 1.43M ↑ 1109 (24 hours)

MOST ACTIVE THREATS (LAST 3 MONTHS)

MOST TARGETED VICTIMS (LAST 3 MONTHS)

RELATIONSHIPS CREATED

MOST ACTIVE MALWARE (LAST 3 MONTHS)

MOST ACTIVE VULNERABILITIES (LAST 3 MONTHS)

CVE-2025-24983	2
CVE-2014-1812	2
CVE-2017-0143	2
CVE-2020-1472	2
CVE-2018-13379	2
CVE-2025-24061	2
CVE-2021-26855	2
CVE-2025-24071	2

TARGETED COUNTRIES (LAST 3 MONTHS)

LATEST REPORTS

TYPE	NAME	PLATFORM CREAT	MODIFICATION D.	AUTHOR	CREATORS	STATUS	LABELS	MARKING
REPO...	nova has pub...	Jul 11, 2025	Jul 11, 2025	Ransomware.Live	admin	NEW	No label	TLP:CLEAR

MOST ACTIVE LABELS (LAST 3 MONTHS)

» High-performance compute with dedicated GPUs.

» Optional water-cooling for energy efficiency.

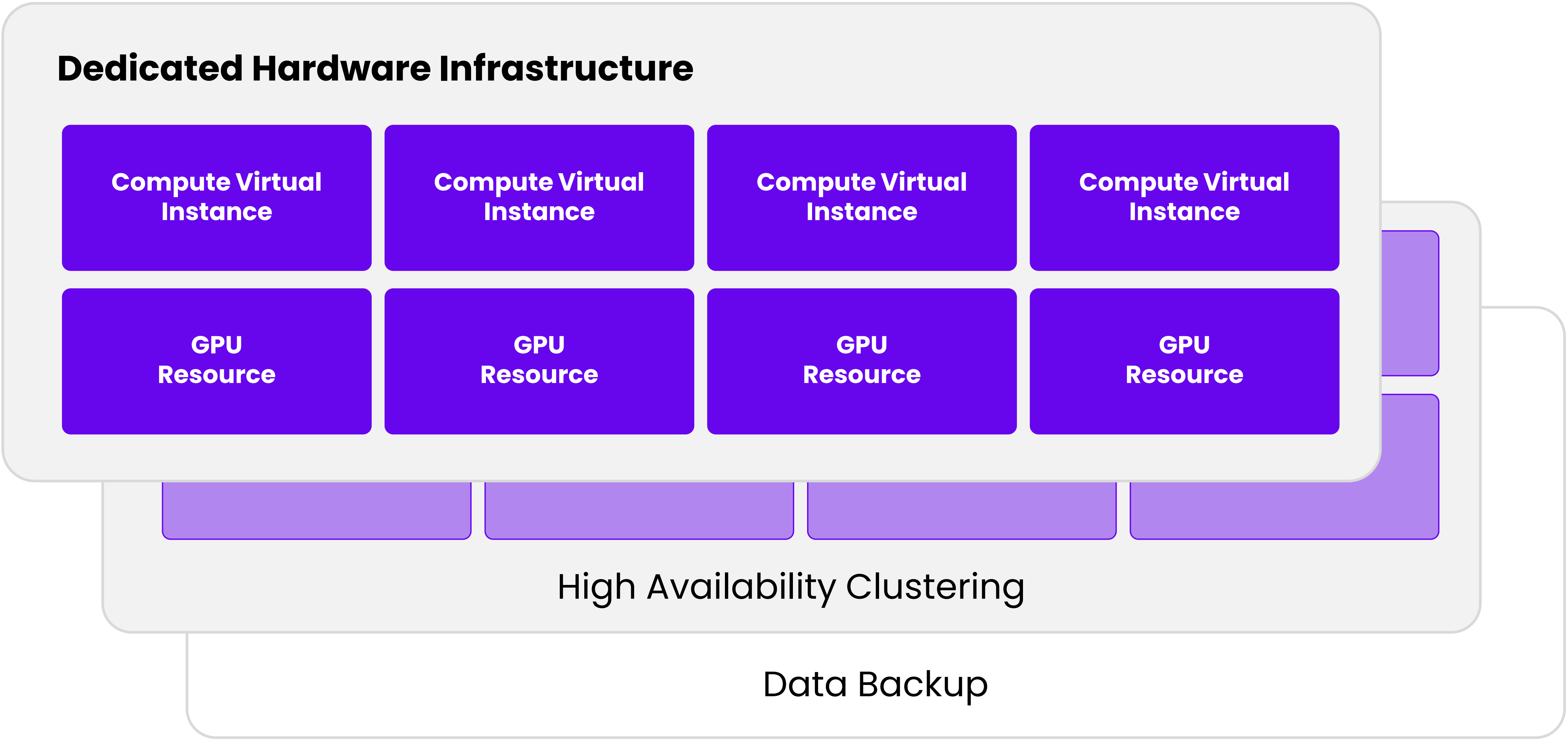
» Robust VMware-based virtualization.

» Hosted in secure Australian data centres.

» Resilient design with clustering and failover.

» Encrypted backups with optional AWS/Azure integration.

CIBRAI Hardware Architecture



Dedicated Hardware Infrastructure

Compute Virtual Instance

Compute Virtual Instance

Compute Virtual Instance

Compute Virtual Instance

GPU Resource

GPU Resource

GPU Resource

GPU Resource

High Availability Clustering

Data Backup

The CiBRAI On-Premise Technical Architecture delivers you a scalable, fully compliant cybersecurity solution with integrated SIEM, SOAR, CTI, and AI-driven automation via AgentiXCyber. It features dedicated high-performance infrastructure, optional co-managed SOC support, and full alignment with Essential Eight, ISM, PSPF, and ISO 27001. Built on an open-core framework, it ensures customisation, seamless integration, and future-ready security resilience.

KEY DESIGN BENEFITS/FIT FOR PURPOSE

Comprehensive Cybersecurity Solution

On-premise solution with SIEM, SOAR, CTI, and AI via AgentiXCyber. Optional SOC support included.

Flexible & Compliant

Open-core design with full integration and alignment to Essential Eight, ISM, PSPF, and ISO 27001.

SECURITY AND COMPLIANCE STANDARDS ALIGNMENT

Essential Eight Compliance

- Centralised logging and application control
- Automated patching aligned with Essential Eight

ISM & PSPF Compliance

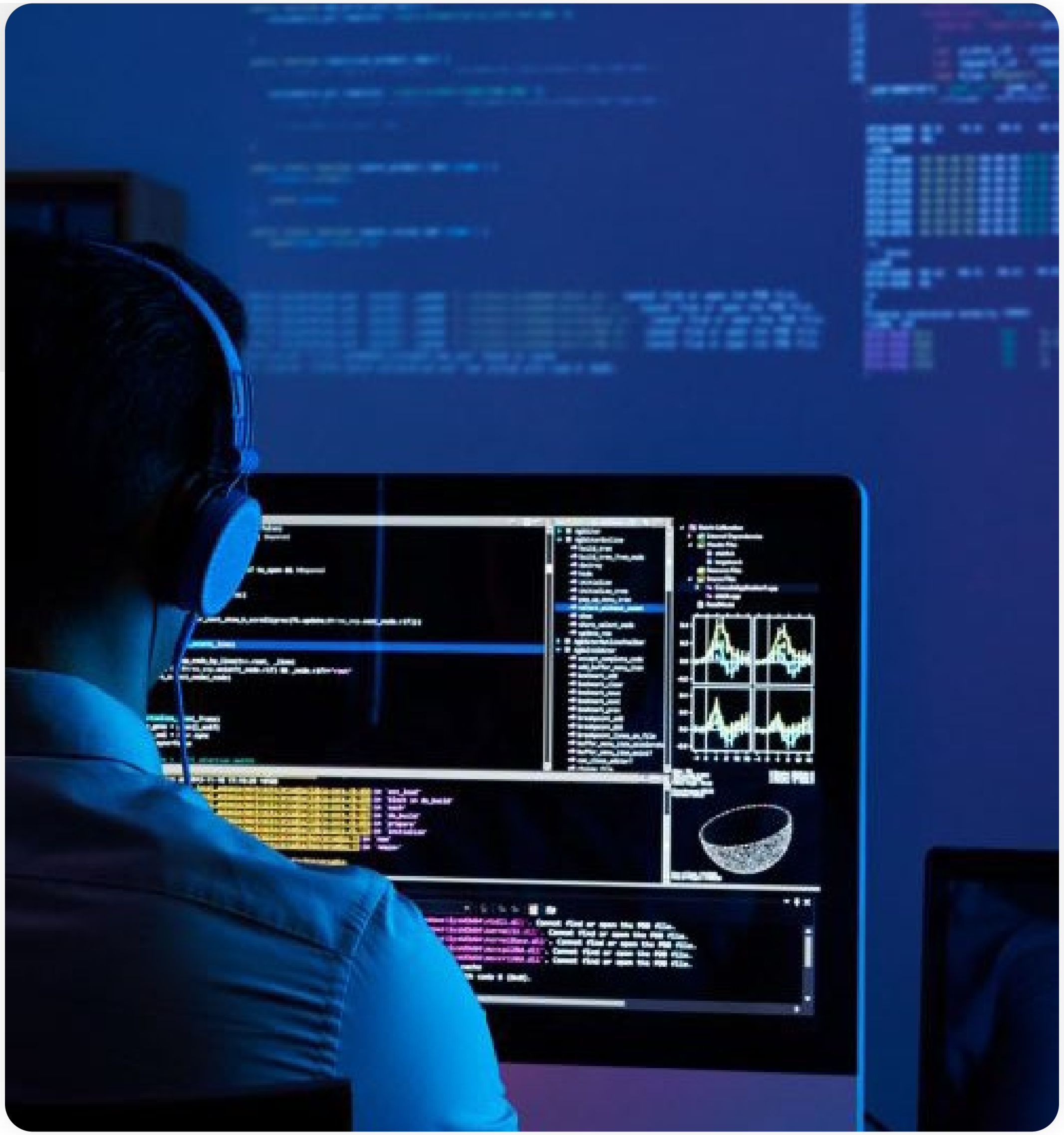
- Continuous monitoring and robust auditing
- Encryption and controls aligned with ISM and PSPF

ISO 27001 Certification Alignment

- Rigorous platform security and operations
- Compliance aligned with global best practices

SEAMLESS INTELLIGENCE CO-MANAGED SOC INTEGRATION

CIBRAI's technical architecture is engineered for extensive scalability, accommodating future growth and evolving cybersecurity requirements with ease



Modular Architecture

» Ability to easily scale storage, compute, and GPU resources, accommodating future growth.

Flexible Virtualisation

» Robust VMware-based virtualisation allowing rapid provisioning and expansion of virtual resources

Expandable Storage and Processing Capacity

» Seamless expansion of infrastructure without operational disruption, ensuring long-term sustainability.

SCALABILITY & FUTURE-PROOFING

Optional co-managed SOC by Seamless Intelligence offers expert support, advanced incident response, and continuous ruleset optimisation.

24x7 Dedicated Support

» Continuous monitoring, expert analysis, and incident response available around-the-clock.

Advanced Threat Intelligence & Hunting

» Real-time intelligence integration, advanced analytics, proactive threat detection, and hunting activities.

Structured Training & Knowledge Transfer

» Ongoing training, certifications, and capability building to strengthen ACQSC's cybersecurity maturity.

CUSTOMISATION AND INTEGRATION CAPABILITY

CiBRAI's open-core technical architecture provides extensive customisation, flexible integration, and tailored cybersecurity management

Open-Core Model

- Ensures easy integration and connectivity of SIEM, SOAR, and CTI components with existing ACQSC infrastructure.

Flexible Integration Capabilities

- Custom integrations with ITSM, on-call tools, cloud platforms, and third-party security systems.

Customised Cybersecurity Workflows

- Custom incident playbooks, automated workflows, and SIEM rules tailored to ACQSC needs.

IMPLEMENTATION PLAN

Structured & Collaborative Deployment

CiBRAI ensures a timely, tailored deployment aligned with your operational and compliance needs, supported by clear governance and communication.

Phase-Based Methodology

Each implementation phase includes defined objectives, tasks, and milestones to ensure clarity, accountability, and efficient delivery.

IMPLEMENTATION PLAN

Our implementation methodology consists of four structured phases

Phase 1

Initiation Planning.

Phase 2

Solution Design &
Infrastructure Deployment.

Phase 3

Platform Configuration,
Integration & Validation.

Phase 4

Platform Configuration,
Integration & Validation.

DETAILED PHASES & ACTIVITIES

Phase 1: Initiation & Planning

This 2-week phase involves project kickoff, stakeholder engagement, and requirements validation, culminating in a detailed project plan, risk strategy, and formal sign-off to begin execution.

01

Phase 2: Design & Deployment

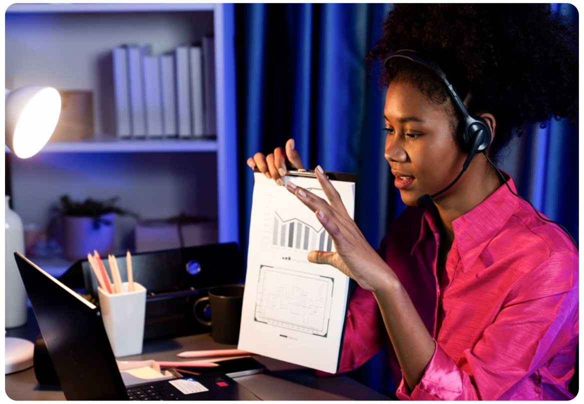
This 4-week phase finalises the CiBRAI architecture, deploys and configures dedicated hardware, and validates compliance, scalability, and HA/DR setup, concluding with infrastructure deployment sign-off.

02

Phase 3: Configuration & Integration

This 4-week phase installs and configures CiBRAI components, integrates with your systems, and validates detection rules, log ingestion, and security through UAT and penetration testing.

03



Phase 4: Go-Live & Handover

This phase finalises readiness checks, delivers training, and completes the CiBRAI go-live with operational handover and 2 weeks of hypercare support.

04

IMPLEMENTATION TIMELINE & RESOURCES:

CiBRAI follows a structured, milestone-driven implementation with clear roles, strong governance, and proactive risk management to ensure smooth project delivery.

The platform undergoes rigorous testing, including UAT, penetration testing, and performance validation to meet all compliance and security requirements.

Expert-led deployment, seamless integration, and in-depth training enable you to achieve full operational readiness with minimal disruption.

IMPLEMENTATION TIMELINE & RESOURCES:

MILESTONE	DURATION	COMPLETION TARGET
Project Initiation & Plan Sign-off	2 Weeks	Week 2
Infrastructure Deployment Completion & Validation	4 Weeks	Week 6
Platform Configuration & Validation	4 Weeks	Week 10
Training & Knowledge Transfer Completion	2 Weeks	Week 12
Operational Go-Live & Handover (Hypercare Complete)	2 Weeks	Week 14

IMPLEMENTATION TIMELINE & RESOURCES:

ROLE	ORGANISATION	RESPONSIBILITY
Project Manager	CiBRAI	Overall project management & governance
Security Solution Architect	CiBRAI / Secure Collaboration	Architecture design & deployment supervision
Infrastructure Engineer	Secure Collaboration	Hardware installation, deployment & validation
SIEM/SOAR Technical Specialist	CiBRAI	Software installation, integration & configuration
SOC Analyst (24x7 coverage)	Seamless Intelligence	Initial rule development, tuning & operational handover
Project Liaison	Your Team	Coordination & internal communications
IT Infrastructure Team	Your Team	Support infrastructure integration & validation
Training & Certification Lead	CiBRAI / Seamless Intelligence	Delivery of structured training & knowledge transfer

SEAMLESS INTELLIGENCE CO-MANAGED SERVICE MODEL

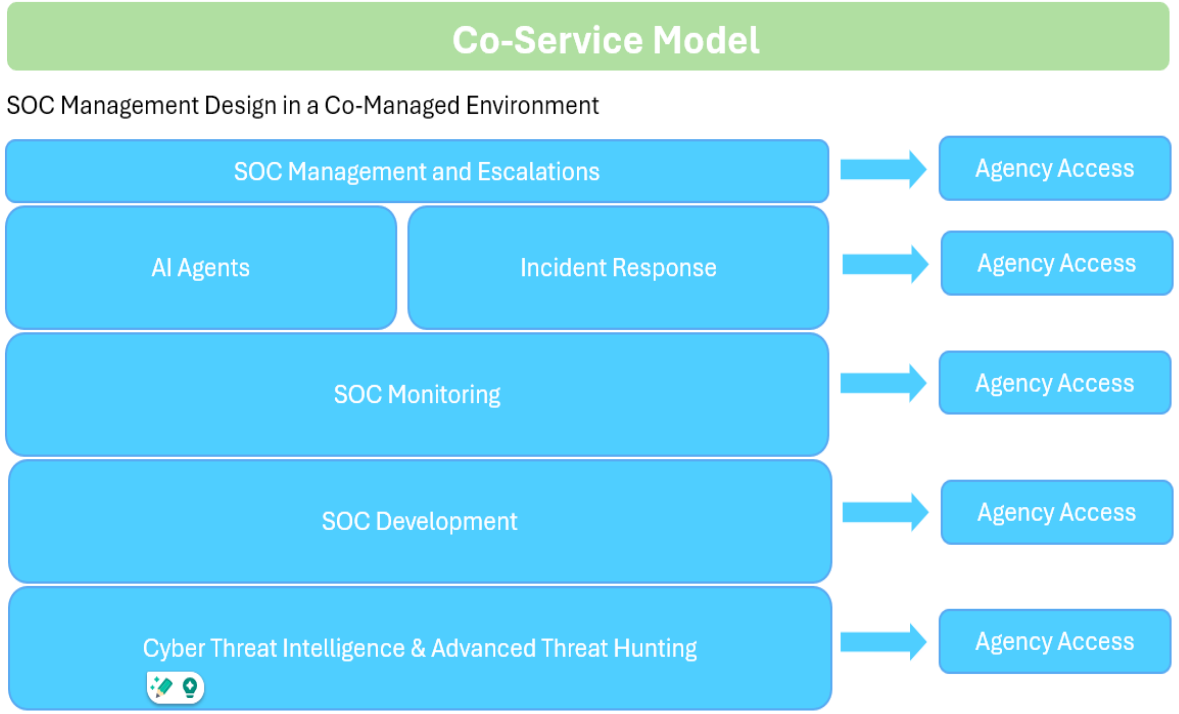
Seamless Intelligence provides 24x7 SOC monitoring, rapid incident response, and expert escalation to ensure continuous protection.

AI-driven virtual SOC operators automate reporting, threat analysis, and complex tasks to enhance operational efficiency.

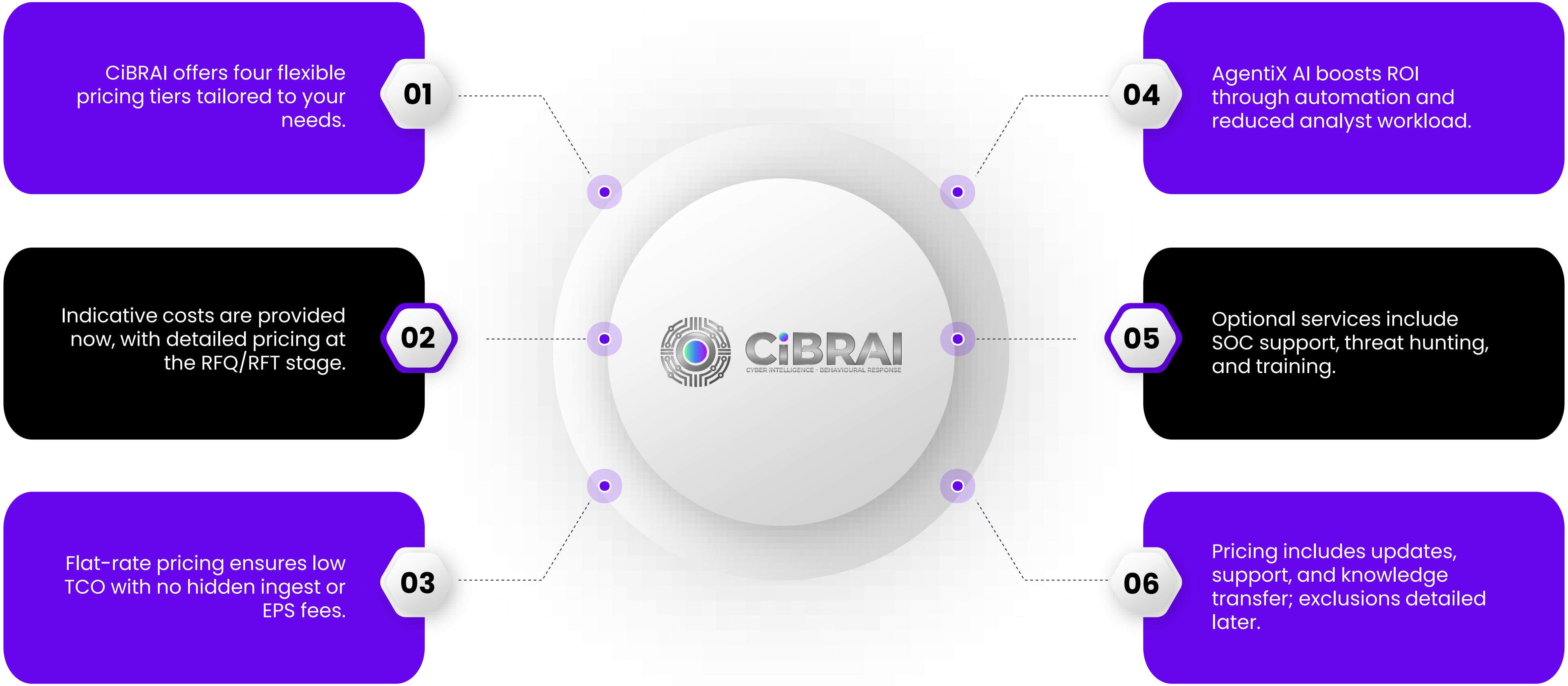
The service includes continuous SIEM ruleset tuning, proactive threat hunting, and advanced behavioural analytics for accurate detection.

Optional services like annual penetration testing, custom integrations, compliance reporting, and training further strengthen cybersecurity posture.

Dedicated service delivery, regular reviews, and structured governance ensure ongoing improvement and alignment with your objectives.



PRICING AND COMMERCIALS



01 CiBRAI offers four flexible pricing tiers tailored to your needs.

02 Indicative costs are provided now, with detailed pricing at the RFQ/RFT stage.

03 Flat-rate pricing ensures low TCO with no hidden ingest or EPS fees.

04 AgentiX AI boosts ROI through automation and reduced analyst workload.

05 Optional services include SOC support, threat hunting, and training.

06 Pricing includes updates, support, and knowledge transfer; exclusions detailed later.

TRAINING AND SUPPORT

- CiBRAI provides you with structured, role-based training programs—including administration, analyst, and advanced user certification—delivered through online, on-site, and on-demand formats.

- This ensures all internal teams gain the knowledge and skills needed to operate the platform effectively, with continuous access to updated training and tailored sessions that align with your workflows and compliance needs. Seamless Intelligence enhances internal capability through ongoing mentorship, advanced scenario-based exercises, and knowledge transfer.

- Platinum and Titanium tier clients benefit from unlimited or annual training allowances, ensuring teams stay up to date with evolving threats, platform advancements, and security best practices. CiBRAI's support services include 24x7 expert assistance, proactive platform monitoring, scheduled updates, and clear escalation paths.

- Clients also gain access to a rich knowledge base, peer-driven community forums, and dedicated service delivery management, enabling continuous improvement, operational resilience, and regulatory compliance.

COMPLIANCE AND REGULATORY ALIGNMENT

Complete Compliance

CiBRAI meets Essential Eight, ISM, PSPF, and APPs requirements with secure logging, incident response, and sovereign data hosting.

AI-Driven Automation

AgentiXCyber AI automates compliance reporting, monitoring, and audit logging.

Robust Security

Delivers proactive threat detection, data protection, and transparent Governance. Ask ChatGPT.

RISK MANAGEMENT APPROACH

Risks across technical, infrastructure, operational, and compliance areas are identified early through structured assessments and workshops.

Targeted mitigation strategies include phased deployment, redundancy planning, and continuous threat monitoring.

Ongoing risk tracking is ensured via regular review meetings, structured reporting, and real-time escalation.

Continuous improvement through periodic reassessments, feedback loops, and adaptive security measures.

This approach ensures strong compliance, operational continuity, and reduced cybersecurity exposure for your business.

RISK MANAGEMENT APPROACH

RISK CATEGORY	POTENTIAL RISK	MITIGATION STRATEGIES
Technical & Integration	Integration delays or technical compatibility issues.	Pre-deployment validation, phased approach, rigorous testing.
Infrastructure & Hardware	Hardware performance degradation or infrastructure failures.	HA infrastructure, redundancy planning, rigorous validation.
Cybersecurity & Operational	Cybersecurity breaches or operational downtime.	Advanced threat monitoring, structured response, backup & DR.
Compliance & Regulatory	Non-compliance with Essential Eight, ISM, PSPF, or APP requirements.	Regular compliance auditing, continuous monitoring, real-time alerting.
Project Management & Delivery	Project delays, unclear roles or inadequate resources.	Structured project governance, regular reporting, proactive planning.
Change Management & Adoption	User adoption issues, resistance to change, or knowledge gaps.	Structured training, stakeholder engagement, continuous capability building.

RISK MANAGEMENT FRAMEWORK

CIBRAI utilises a structured, phased approach for ongoing risk identification, assessment, mitigation, and monitoring. Our framework encompasses:

Risk Identification and Assessment

01

Risk Mitigation Strategies

02

Monitoring and Reporting

03

Continuous Risk Improvement

04

REFERENCE CASE STUDIES AND TESTIMONIALS

CiBRAI and Seamless Intelligence have delivered proven cybersecurity solutions across critical Australian sectors.

Deployments achieved full compliance, faster response times, and stronger internal capabilities.

Clients saw major risk reduction, fewer false positives, and improved security visibility.

Their co-managed SOC ensures continuous protection and compliance.

Structured training and automation boost efficiency and maturity.

Your business gains a trusted, regulation-aligned solution with measurable outcomes.

REFERENCE CASE STUDIES AND TESTIMONIALS

CiBRAI and Seamless Intelligence have delivered proven cybersecurity solutions across critical Australian sectors.

Clients saw major risk reduction, fewer false positives, and improved security visibility.

Structured training and automation boost efficiency and maturity.

REFERENCE CASE STUDIES AND TESTIMONIALS

Deployments achieved full compliance, faster response times, and stronger internal capabilities.

Their co-managed SOC ensures continuous protection and compliance.

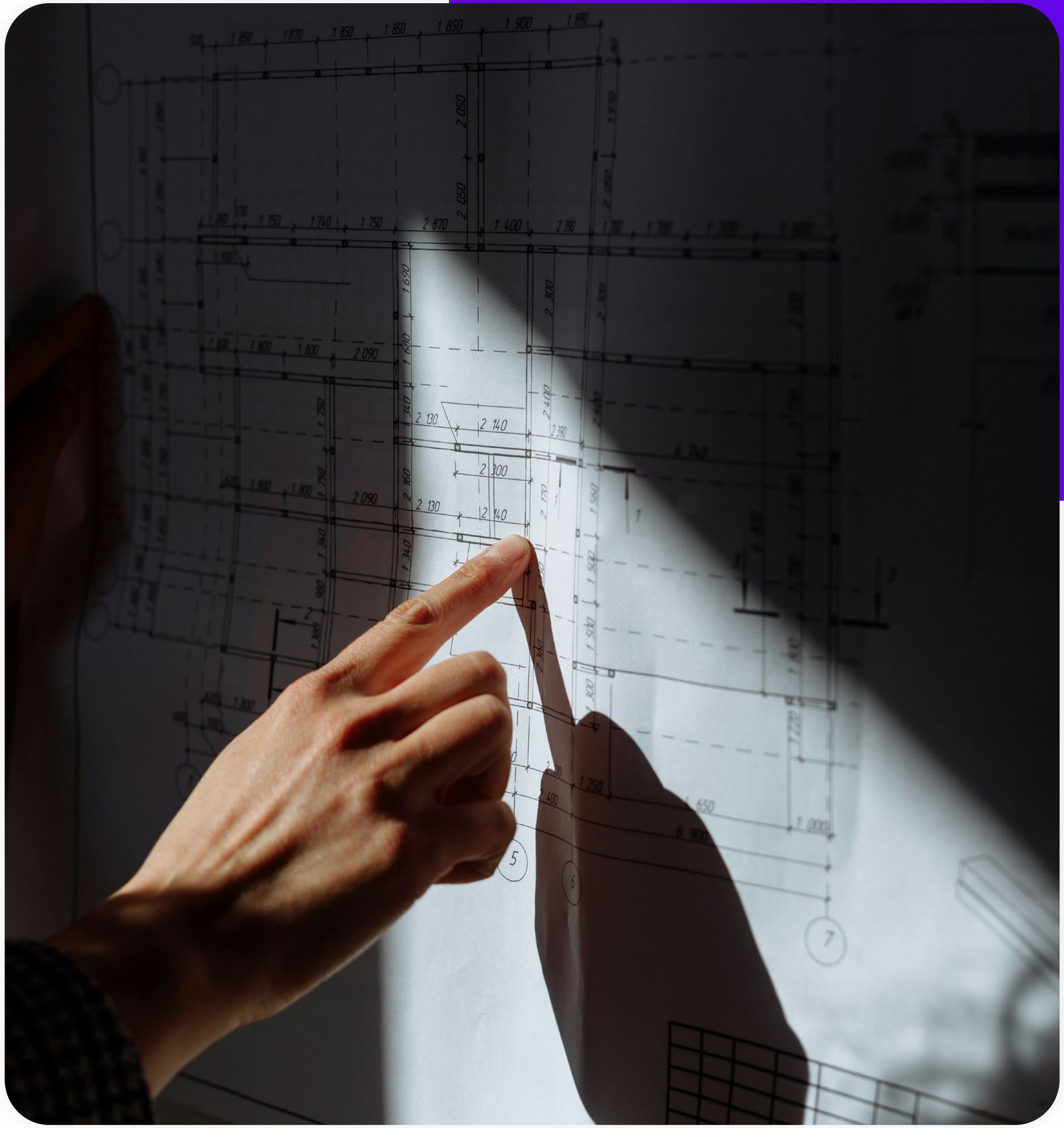
Your business gains a trusted, regulation-aligned solution with measurable outcomes.

APPENDICES

Includes glossary, technical specs, and pricing details.

Provides draft runbook and training paths.

Shares team credentials for project alignment.



APPENDICES

Includes detailed compliance mapping aligned with Essential Eight, ISM, PSPF, and APPs, supported by technical diagrams of architecture and workflows.

01

Provides client reference letters and case studies showcasing proven success across Australian government and enterprise sectors.

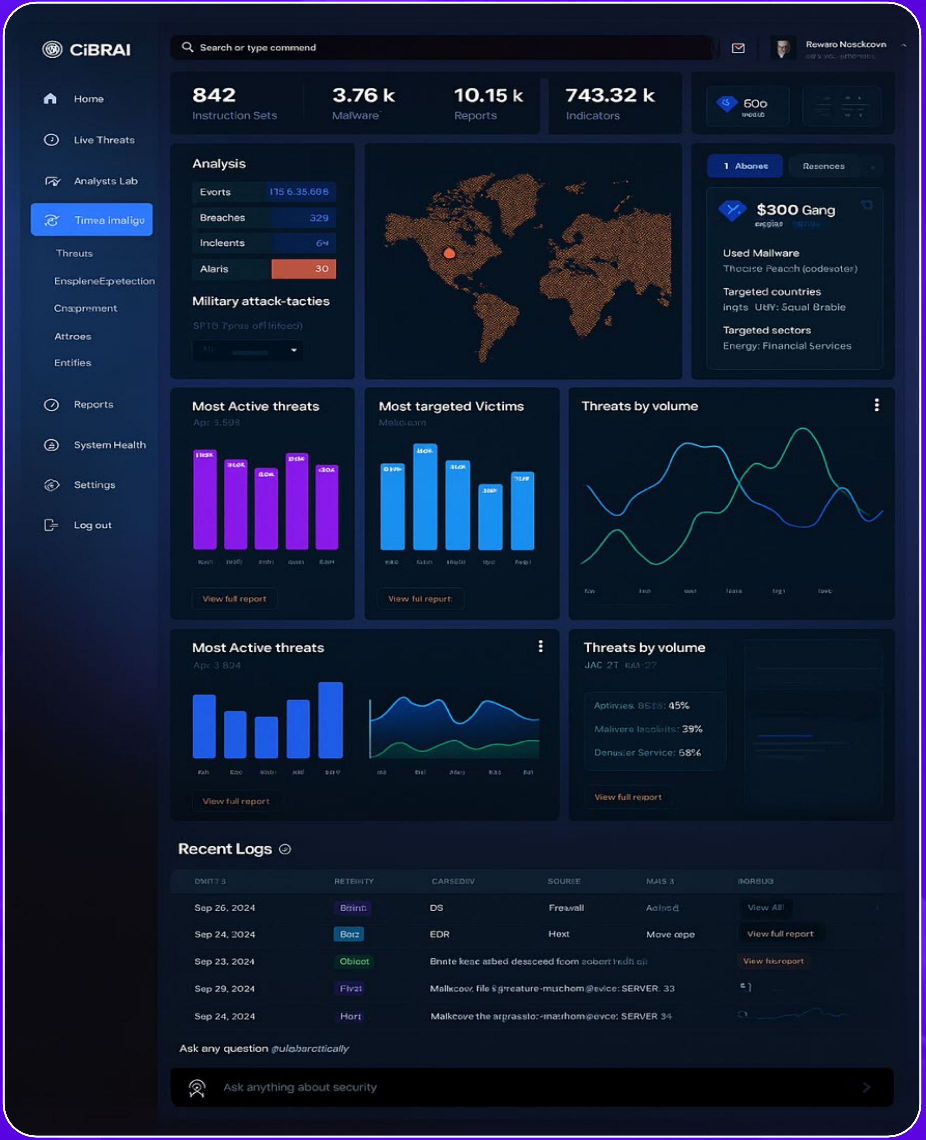
02

Offers sample reports and dashboards demonstrating AI-driven analytics, reporting, and real-time compliance monitoring for operational oversight.

03

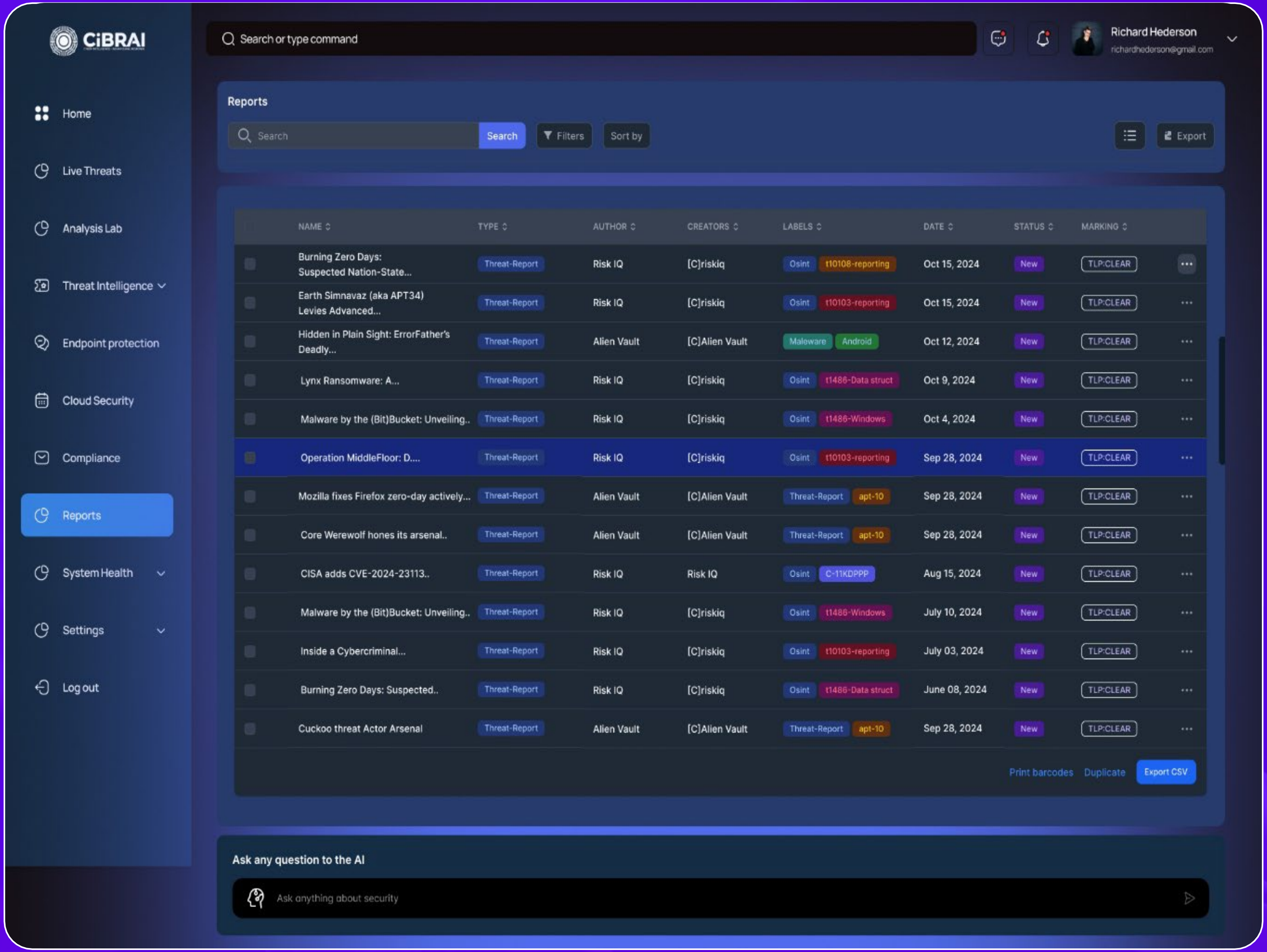
APPENDIX J – SAMPLE REPORTS AND DASHBOARDS

- Provides sample compliance reports
- Includes interactive dashboards
- Showcases AI-powered analytics
- Demonstrates automation in action
- Supports informed decision-making
- Highlights compliance capabilities
- Includes draft and conditions for engagement



DMITT 3	RETEHITY	CARSEDEV	SOUREE	MAIS 3	MORBUG
Sep 26, 2024	Brinc	DS	Frewall	Aoipod	View All
Sep 24, 2024	Borz	EDR	Hext	Move cepe	View full report
Sep 23, 2024	Obicot	Bnnte keac atbed dessceed fcom aobort I'edh cp			View fisroport
Sep 29, 2024	Fivzi	Mallkcoor file Sgreature-muchom@evice: SERVER. 33			
Sep 24, 2024	Hori	Malkcove the arprasslo:-matrhom@evce: SERVER 34			

APPENDIX J – SAMPLE REPORTS AND DASHBOARDS

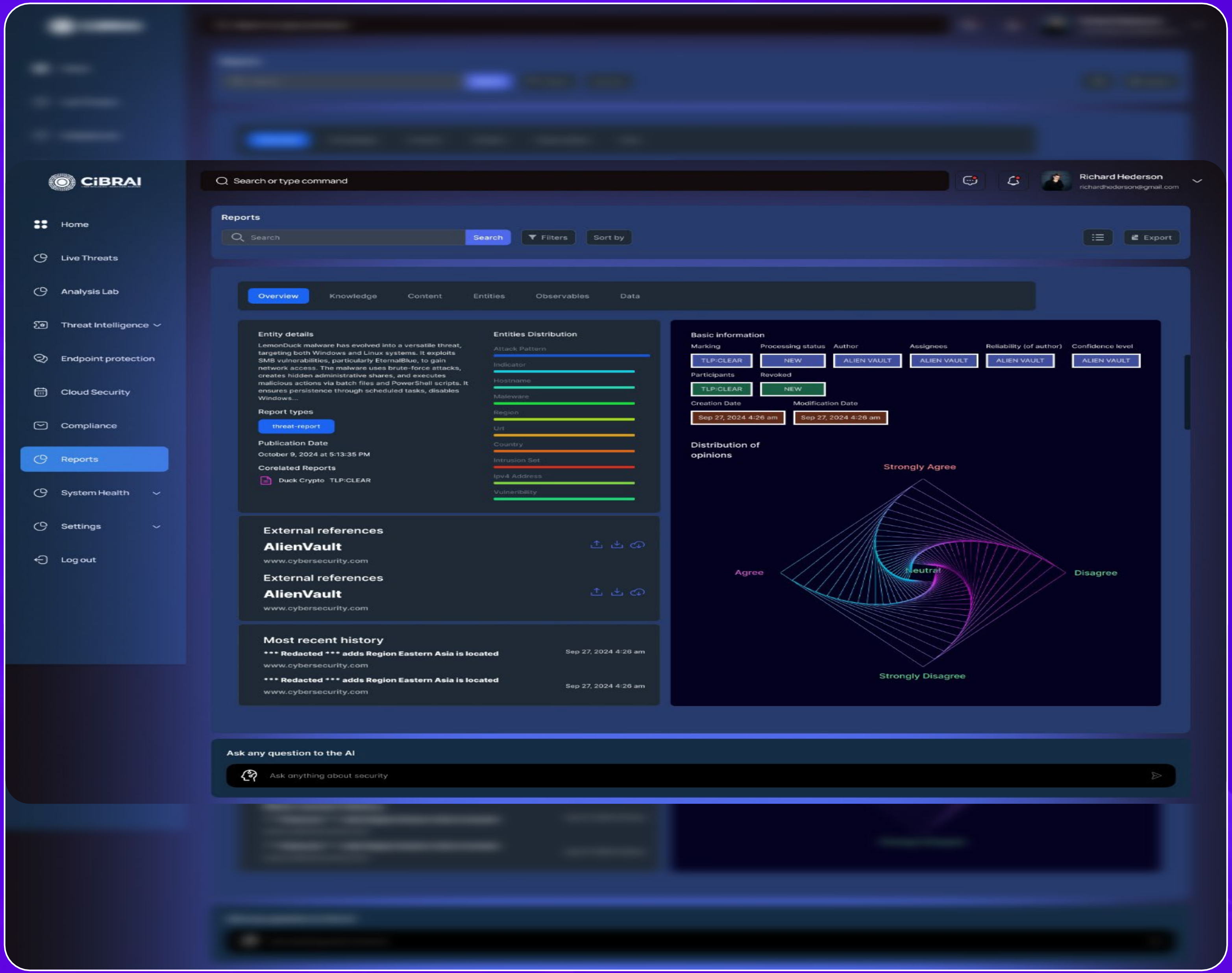


Reports

	NAME	TYPE	AUTHOR	CREATORS	LABELS	DATE	STATUS	MARKING
□	Burning Zero Days: Suspected Nation-State...	Threat-Report	Risk IQ	[C]riskiq	Osint t10108-reporting	Oct 15, 2024	New	TLP:CLEAR
□	Earth Simnavaz (aka APT34) Levies Advanced...	Threat-Report	Risk IQ	[C]riskiq	Osint t10103-reporting	Oct 15, 2024	New	TLP:CLEAR
□	Hidden in Plain Sight: ErrorFather's Deadly...	Threat-Report	Alien Vault	[C]Alien Vault	Maleware Android	Oct 12, 2024	New	TLP:CLEAR
□	Lynx Ransomware: A...	Threat-Report	Risk IQ	[C]riskiq	Osint t1486-Data struct	Oct 9, 2024	New	TLP:CLEAR
□	Malware by the (Bit)Bucket: Unveiling..	Threat-Report	Risk IQ	[C]riskiq	Osint t1486-Windows	Oct 4, 2024	New	TLP:CLEAR
□	Operation MiddleFloor: D....	Threat-Report	Risk IQ	[C]riskiq	Osint t10103-reporting	Sep 28, 2024	New	TLP:CLEAR
□	Mozilla fixes Firefox zero-day actively...	Threat-Report	Alien Vault	[C]Alien Vault	Threat-Report apt-10	Sep 28, 2024	New	TLP:CLEAR
□	Core Werewolf hones its arsenal..	Threat-Report	Alien Vault	[C]Alien Vault	Threat-Report apt-10	Sep 28, 2024	New	TLP:CLEAR
□	CISA adds CVE-2024-23113..	Threat-Report	Risk IQ	Risk IQ	Osint C-11KDPPP	Aug 15, 2024	New	TLP:CLEAR
□	Malware by the (Bit)Bucket: Unveiling..	Threat-Report	Risk IQ	[C]riskiq	Osint t1486-Windows	July 10, 2024	New	TLP:CLEAR
□	Inside a Cybercriminal...	Threat-Report	Risk IQ	[C]riskiq	Osint t10103-reporting	July 03, 2024	New	TLP:CLEAR
□	Burning Zero Days: Suspected..	Threat-Report	Risk IQ	[C]riskiq	Osint t1486-Data struct	June 08, 2024	New	TLP:CLEAR
□	Cuckoo threat Actor Arsenal	Threat-Report	Alien Vault	[C]Alien Vault	Threat-Report apt-10	Sep 28, 2024	New	TLP:CLEAR

Ask any question to the AI

APPENDIX J – SAMPLE REPORTS AND DASHBOARDS



Entity details

LemonDuck malware has evolved into a versatile threat, targeting both Windows and Linux systems. It exploits SMB vulnerabilities, particularly EternalBlue, to gain network access. The malware uses brute-force attacks, creates hidden administrative shares, and executes malicious actions via batch files and PowerShell scripts. It ensures persistence through scheduled tasks, disables Windows...

Report types: threat-report

Publication Date: October 9, 2024 at 5:13:35 PM

Corelated Reports: Duck Crypto TLP:CLEAR

Basic information

Marking	Processing status	Author	Assignees	Reliability (of author)	Confidence level
TLP:CLEAR	NEW	ALIEN VAULT	ALIEN VAULT	ALIEN VAULT	ALIEN VAULT

Participants	Revoked
TLP:CLEAR	NEW

Creation Date	Modification Date
Sep 27, 2024 4:26 am	Sep 27, 2024 4:26 am

External references

AlienVault

www.cybersecurity.com

External references

AlienVault

www.cybersecurity.com

Most recent history

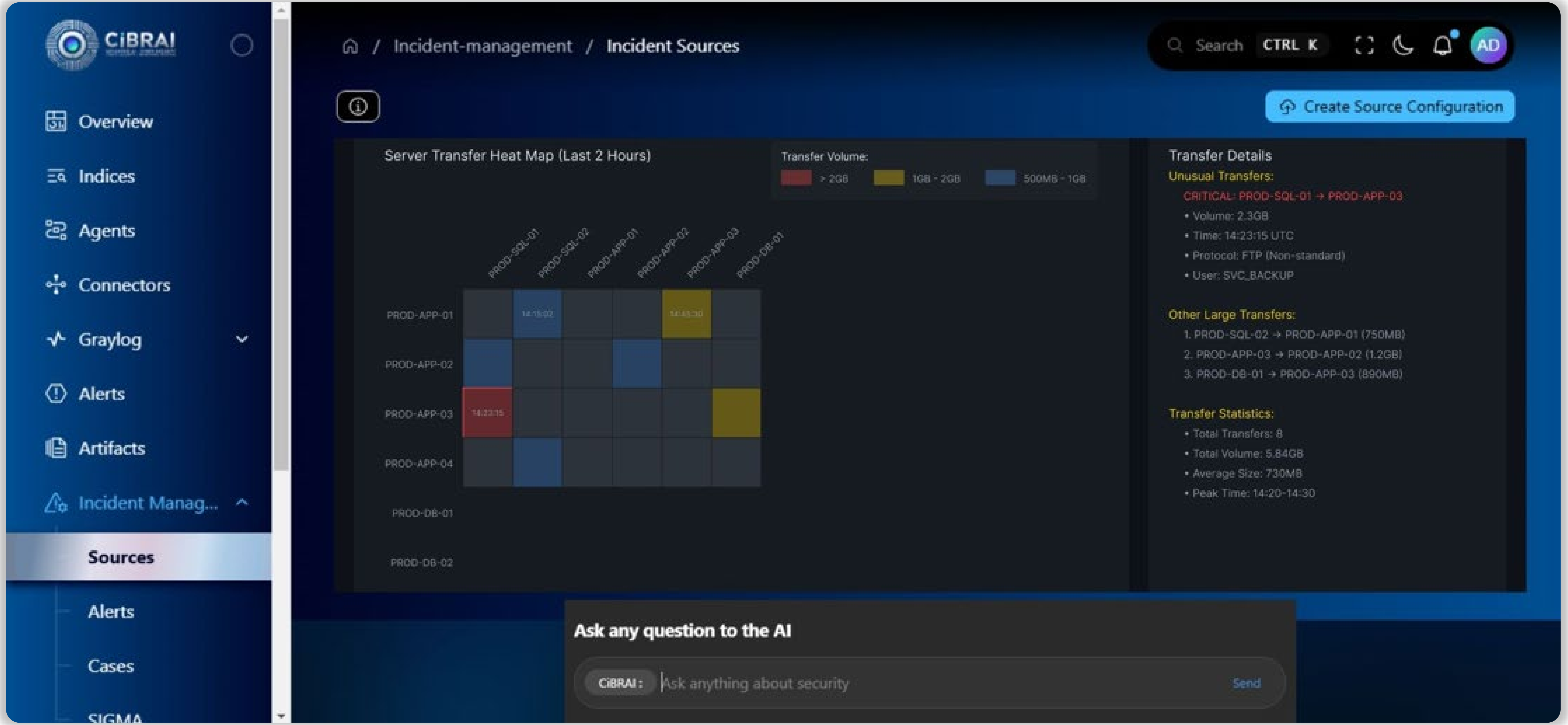
*** Redacted *** adds Region Eastern Asia is located — Sep 27, 2024 4:26 am

www.cybersecurity.com

*** Redacted *** adds Region Eastern Asia is located — Sep 27, 2024 4:26 am

www.cybersecurity.com

APPENDIX J – SAMPLE REPORTS AND DASHBOARDS



Transfer Details

Unusual Transfers:

CRITICAL: PROD-SQL-01 → PROD-APP-03

- Volume: 2.3GB
- Time: 14:23:15 UTC
- Protocol: FTP (Non-standard)
- User: SVC_BACKUP

Other Large Transfers:

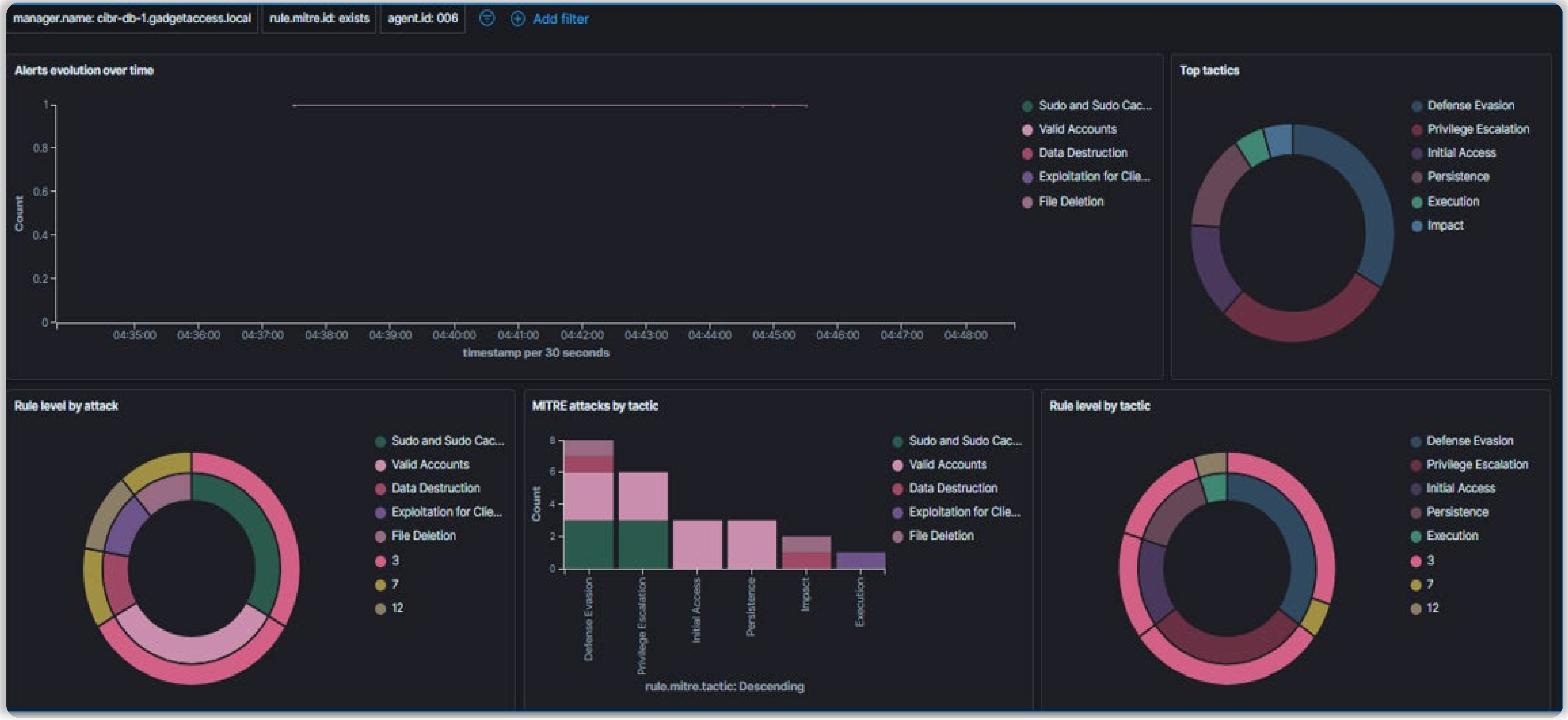
1. PROD-SQL-02 → PROD-APP-01 (750MB)
2. PROD-APP-03 → PROD-APP-02 (1.2GB)
3. PROD-DB-01 → PROD-APP-03 (890MB)

Transfer Statistics:

- Total Transfers: 8
- Total Volume: 5.84GB
- Average Size: 730MB
- Peak Time: 14:20-14:30

Ask any question to the AI

APPENDIX J – SAMPLE REPORTS AND DASHBOARDS

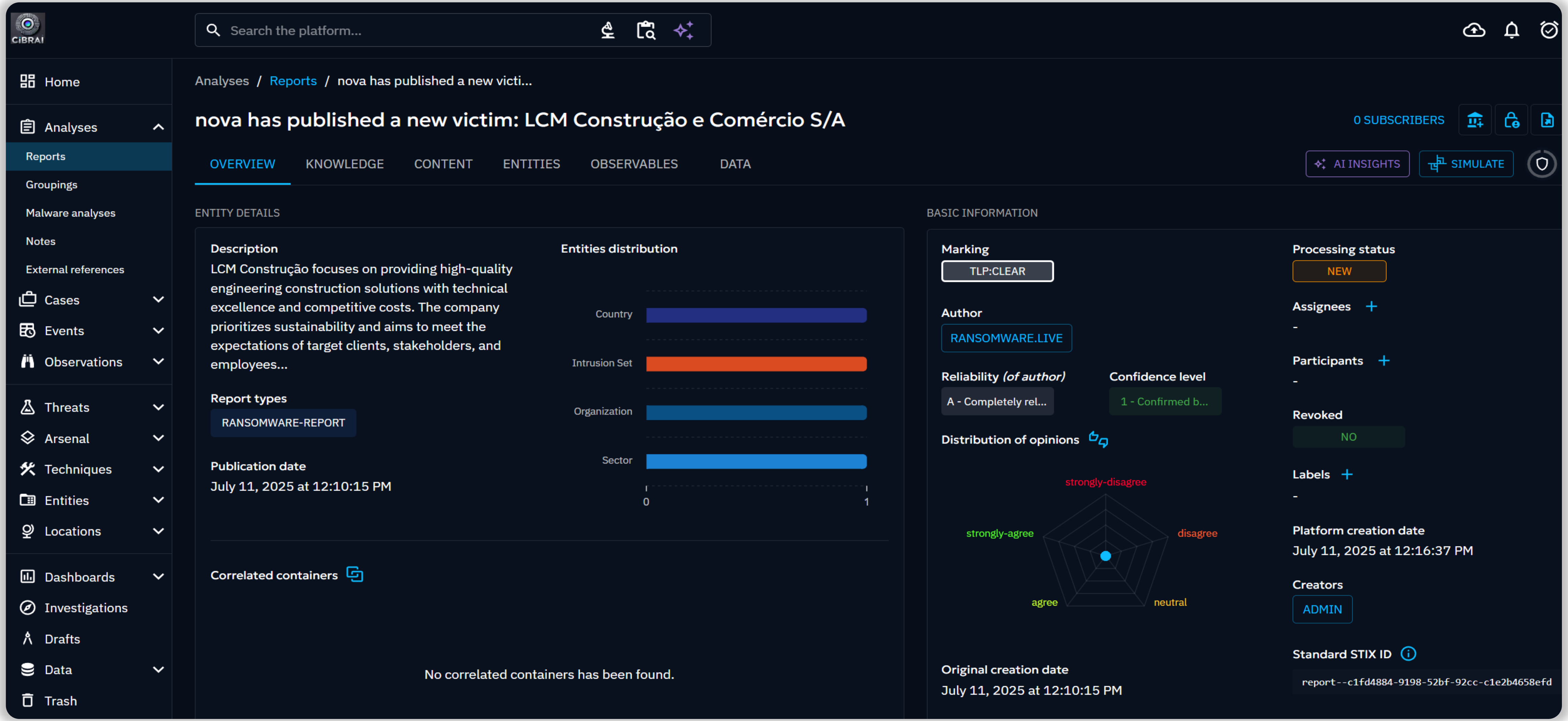


manager.name: cibr-db-1.gadgetaccess.local

rule.mitre.id: exists

agent.id: 006

APPENDIX J – SAMPLE REPORTS AND DASHBOARDS



Analyses / Reports / nova has published a new victi...

nova has published a new victim: LCM Construção e Comércio S/A

ENTITY DETAILS

Description

LCM Construção focuses on providing high-quality engineering construction solutions with technical excellence and competitive costs. The company prioritizes sustainability and aims to meet the expectations of target clients, stakeholders, and employees...

Entities distribution

Report types

RANSOMWARE-REPORT

Publication date

July 11, 2025 at 12:10:15 PM

Correlated containers

No correlated containers has been found.

BASIC INFORMATION

Marking

TLP:CLEAR

Author

RANSOMWARE.LIVE

Reliability *(of author)*

A - Completely rel...

Confidence level

1 - Confirmed b...

Distribution of opinions

Original creation date

July 11, 2025 at 12:10:15 PM

Processing status

NEW

Assignees

-

Participants

-

Revoked

NO

Labels

-

Platform creation date

July 11, 2025 at 12:16:37 PM

Creators

ADMIN

Standard STIX ID

report--c1fd4884-9198-52bf-92cc-c1e2b4658efd

TERMS AND CONDITIONS

Flexible Subscription Model

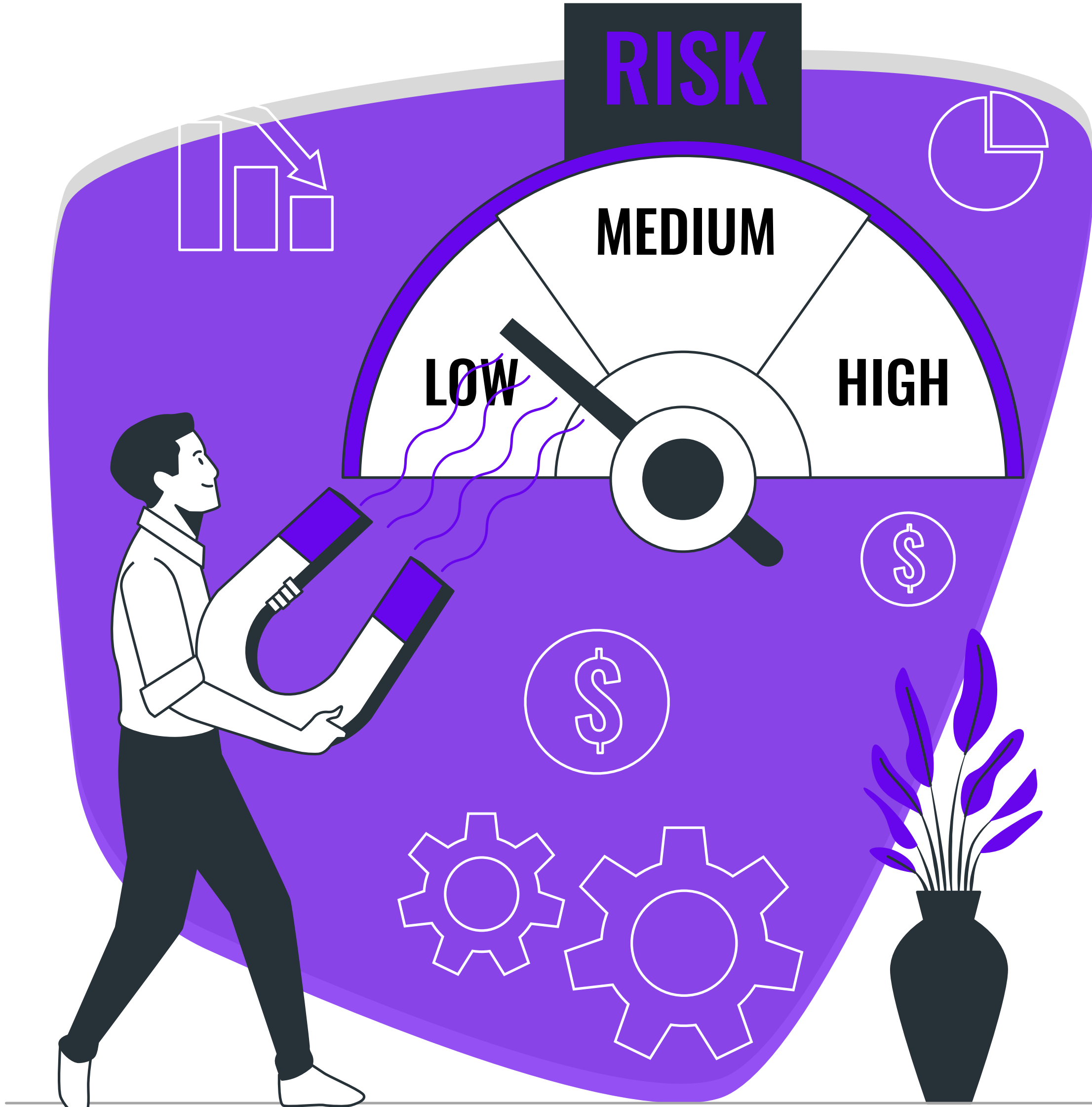
CiBRAI provides tiered service options (Silver to Titanium) with clear pricing, defined milestones, and structured change management tailored to your needs.

Secure, Compliant Infrastructure

Solutions are hosted in Australian data centres with SLAs, sovereign data protection, and full compliance with ISM, PSPF, and APPs.

Built-in Training & Risk Assurance

The agreement includes structured training, risk management, and renewal flexibility, with terms refined during the RFT/RFQ stage to meet your business's standards.



CONTACT INFORMATION

For any questions, further clarification, or additional information regarding this CiBRAI SOC proposal, please reach out to the primary contacts provided below:

NOTE – These will be filled as part of the RFP submission.

CONTACT TYPE	NAME	POSITION	ORGANISATION	EMAIL ADDRESS	PHONE NUMBER
Executive Sponsor					
Primary Sales Contact					
Technical Lead					
Infrastructure Management					
Cybersecurity Operations					
Project Management Lead					
Service Delivery Manager					
Financial/Commercial Queries					
SOC integration Training					
Incident Response Lead					

CiBRAI
CYBER INTELLIGENCE - BEHAVIOURAL RESPONSE

THANK YOU