



TechBridge
Making the World Smarter

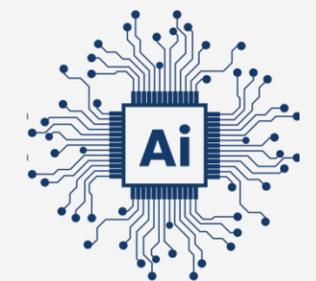
TechBridge



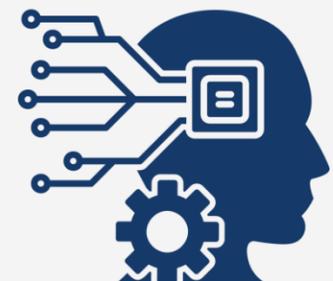
Making The World Smarter

At a Glance

COMPANY



Artificial Intelligence



Machine Learning

OUR OFFICES



OUR PRODUCTS



SUPPORTED CLOUDS



CUSTOMERS & PARTNERS



Certificates, Recognition and standards/ Forums

CERTIFICATES

RECOGNIZED BY

STANDARDS/FORUMS



- ISO 27001



- ISO 9001



- ISO/IEC 15408-1



- ISO/IEC 20000



- CMMI-DEV V.1.3



- PINK CERTIFICATE



- ET Telecom



- DSCI Member



- NCoE/DSCI Incubated



- TDB Recognized/Assisted

- EAL4+
- GDPR
- TMForum
- 3GPP
- ITU-T
- HIPAA

Our Vision and Mission

Making the World Smarter !



Vision

Empowering organizations worldwide to manage and protect critical infrastructure effectively.



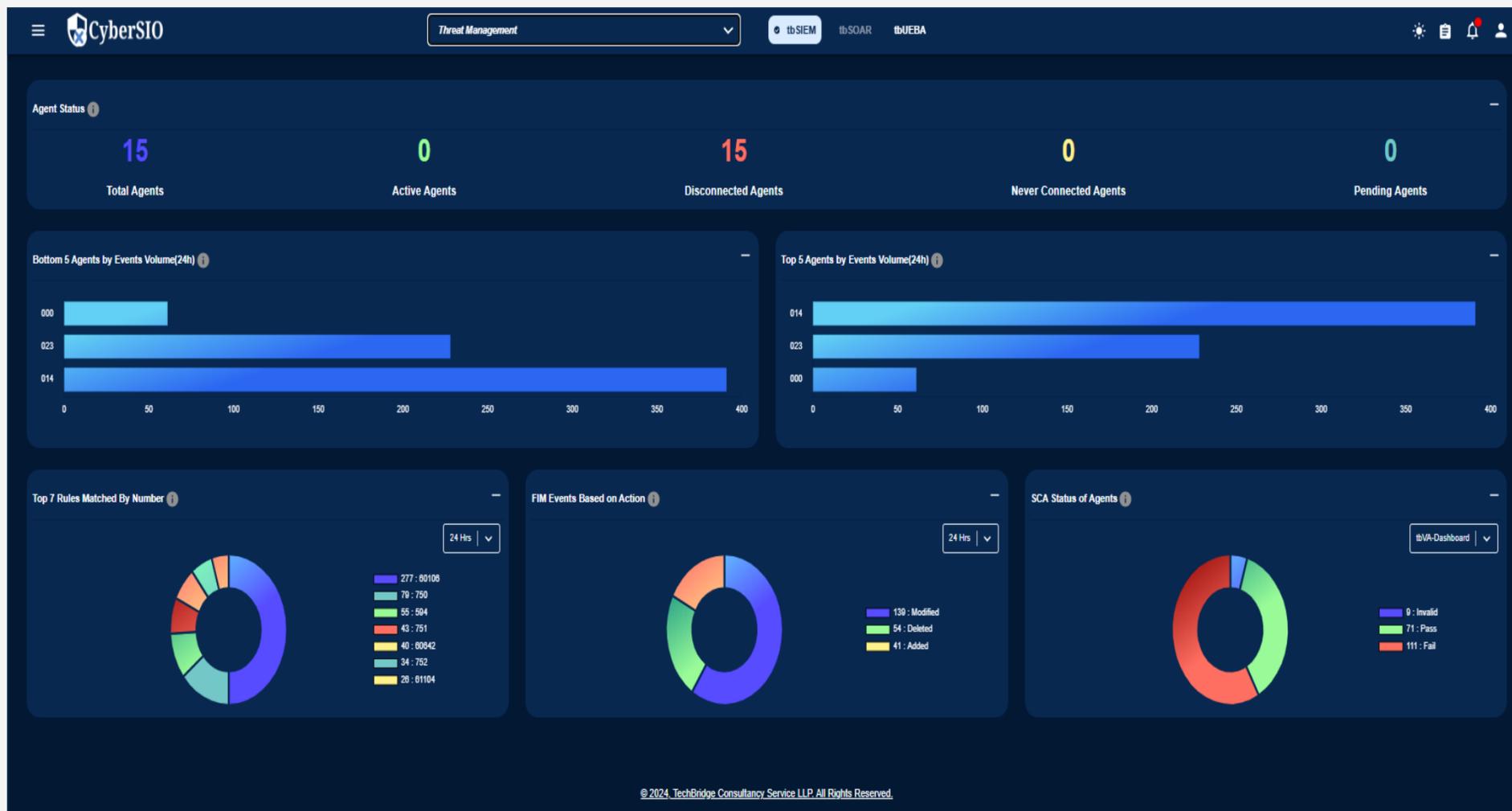
Mission

To provide secure, innovative solutions that empower organizations to protect and manage critical infrastructure effectively.

CyberSIO

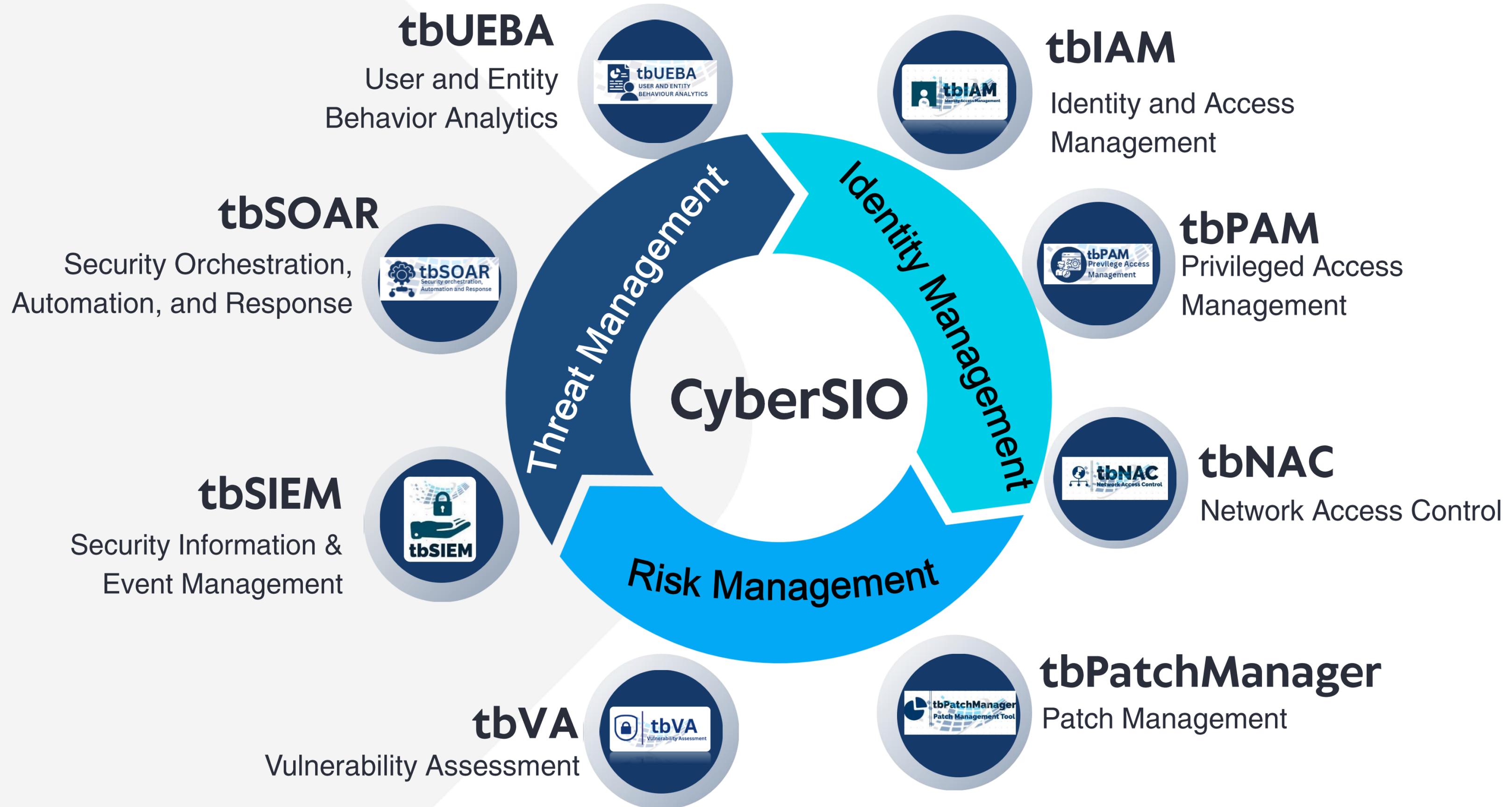
Secure | Intelligent | Orchestrated

CAPABILITIES



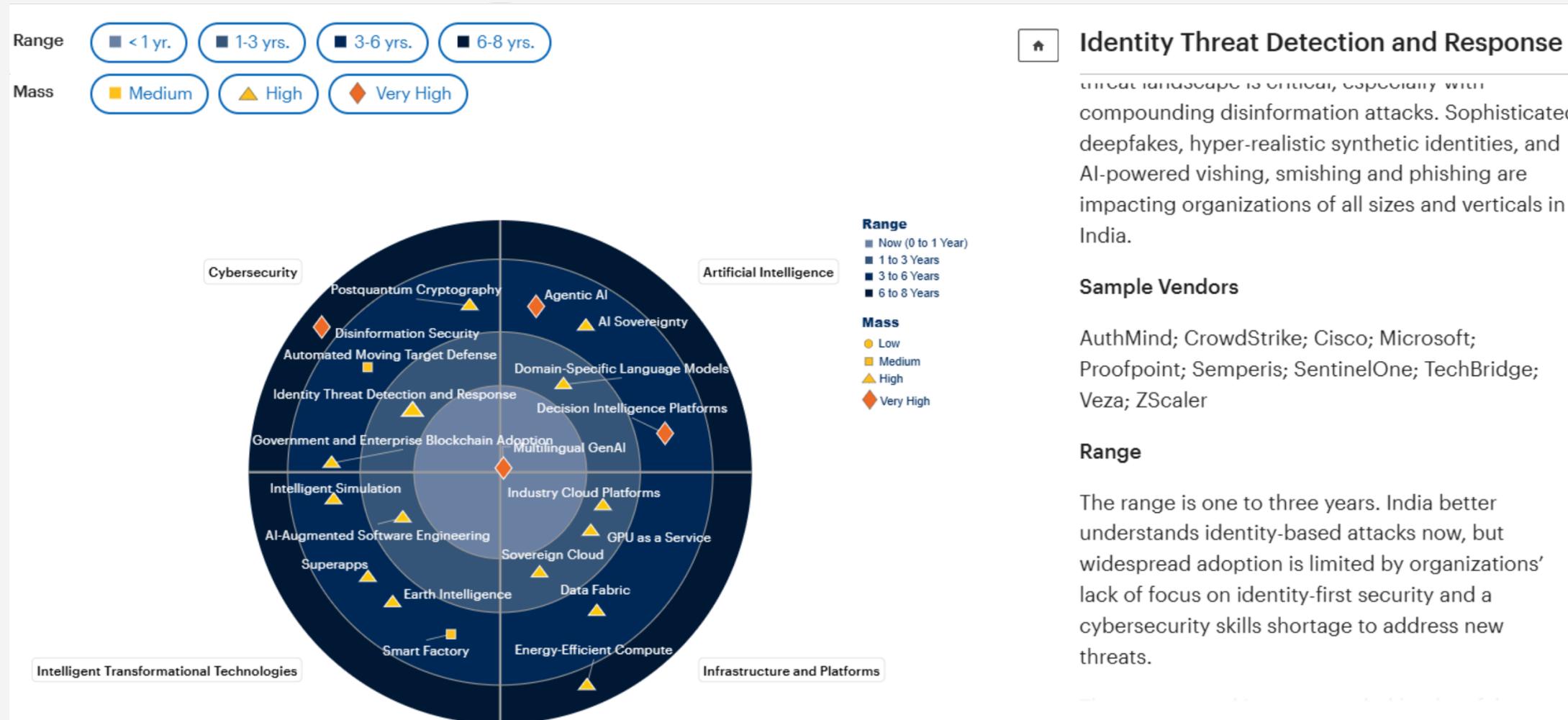
Threat Management | Identity Management | Risk Management

- ◆ Approx. ~60% efficiency for platform owners
- ◆ 250% Increase in SOC Analyst efficiency
- ◆ ‘SOC’ in a box
- ◆ AI Anomaly detection
- ◆ Unified Compliance Framework
- ◆ Automation, AI, Pre-Integrated Platform
- ◆ On-Premise, Hybrid, Cloud Support
- ◆ Scale: ~100k EPS
- ◆ ‘Zero Trust’ Networks



Recognised by Gartner

Pioneering Identity & Threat Management



Emerging Tech Radar Report 2025 – [Read Now](#)

• Identity Threat Detection and Response

• Disinformation Security

The New Battleground of Cybersecurity: Identity



80% of breaches today are identity-driven

Traditional SOCs struggle to detect sophisticated identity misuse

What if your SOC could stop identity threats before they become breaches?

Identity is the New Attack Surface

Organizations lack real-time visibility and response to identity threats.



Problem # 1

80%+ of breaches involve compromised credentials.



Problem # 2

Traditional SIEMs and IDPs (Identity Providers) miss advanced identity-based attacks.

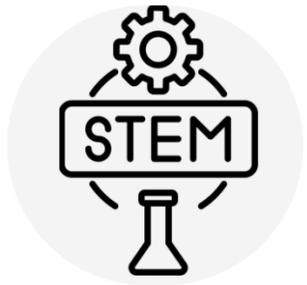


Problem # 3

Lateral movement and privilege escalation often go undetected.

Why Current Solutions Fail

Identity Threats require a specialized, dedicated solution: ITDR.



SIEMs are too generic; overwhelmed by alerts.



IAM systems detect policy violations, not active identity threats.



SOARs respond, but without deep identity threat context.

Introducing CyberSIO ITDR

SOC-in-a-Box with Identity at the Core

**Multi-modal
identity correlation**

**Purpose-built for
critical infrastructure,
BFSI, and government.**

**Consolidates
identity, and threat
management into
one pane of glass.**

**Reduces SOC
complexity while
improving
response speed.**

Why ITDR Matters Now

Compromise

- Attackers no longer “hack in,” they log in

Persistence

- SOC teams are blind to identity signals in legacy SIEM setups

Lateral Movement

- Privileged identities are exploited in 95% of attacks

Breach

- CyberSIO ITDR solves this gap by putting identity signals front & center

The Differentiator: Multi-Modal Identity Verification



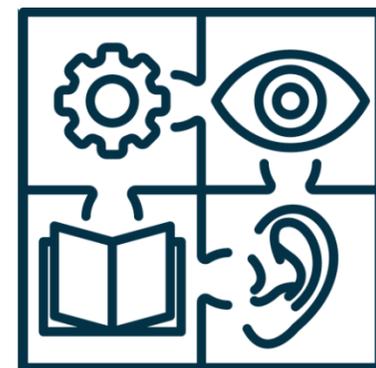
Goes beyond passwords and MFA
→ multi-layered identity assurance



Detects impossible logins,
deepfake attempts, and credential
replay in real-time



Fuses biometrics, behavioral
patterns, device posture, and
contextual signals

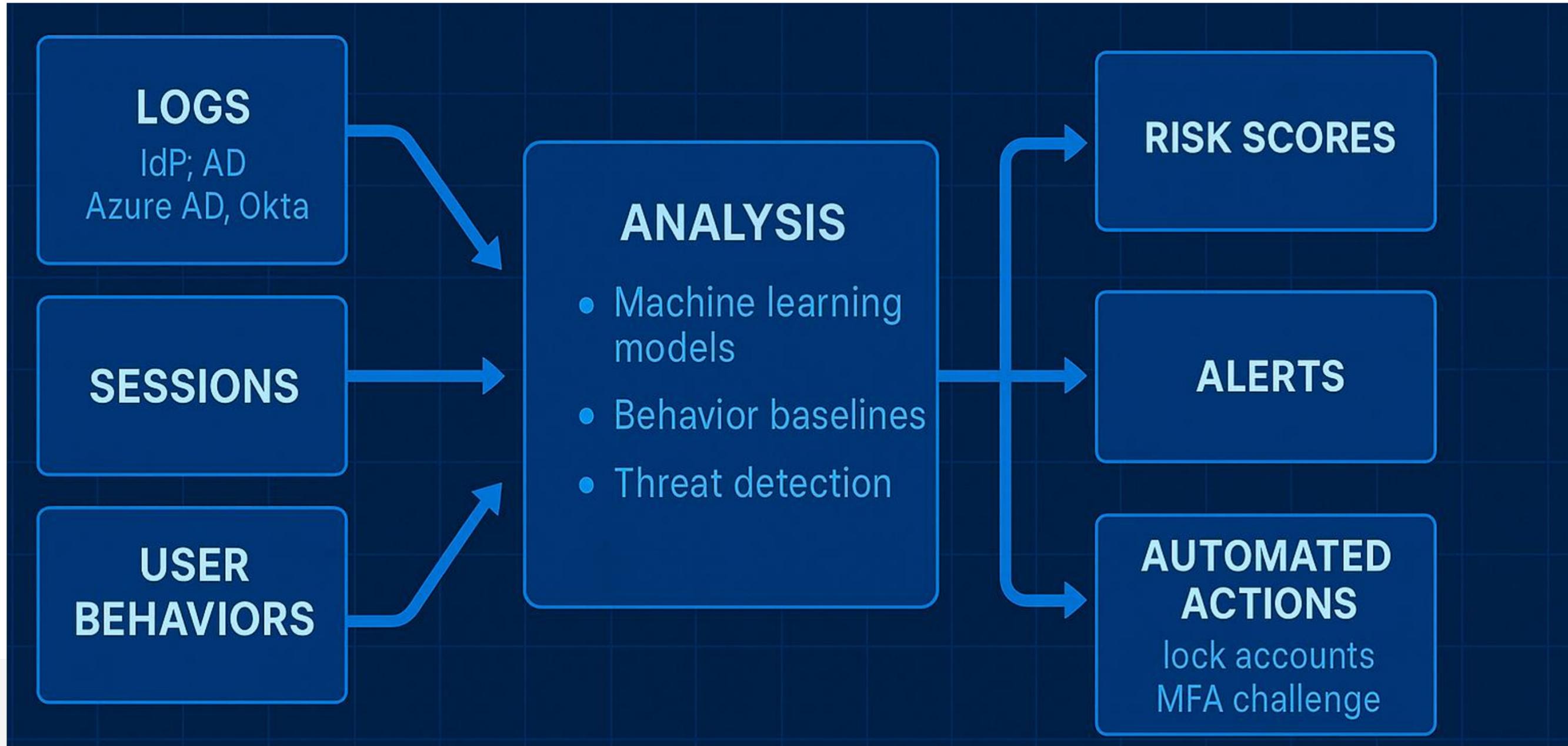


Patent pending in multi-modal
identity verification →
industry-first innovation from India

How CyberSIO ITDR Works



Workflow



CyberSIO ITDR

Purpose-built for Identity Threat Management.

Real-time detection of credential misuse, session hijacking, and privilege abuse.



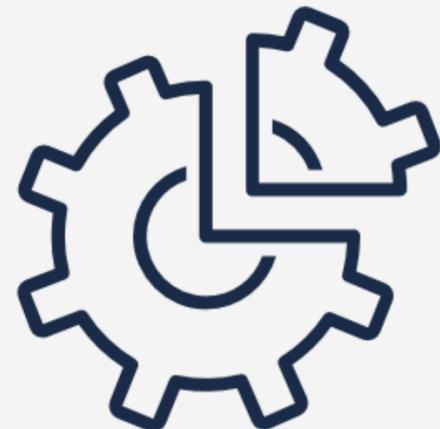
Machine learning-powered risk scoring per identity.



Automated, intelligent responses to stop attacks early.



Seamless integration with existing IAM, SIEM, and SOAR.



Key Features

Real-time Risk Scoring

Anomalous Behavior Detection

Credential Theft and Abuse Detection

Automated Threat Response Playbooks

Customizable Policies and Playbooks

Lateral Movement and Privilege Escalation
Detection

Integration with Okta, Azure AD, AD, Ping, and more



Cutting Edge Performance

1

Identity-Centric
Threat Detection



2

Lightweight Deployment



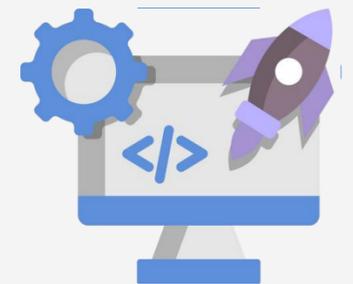
3

Adaptive
AI Models



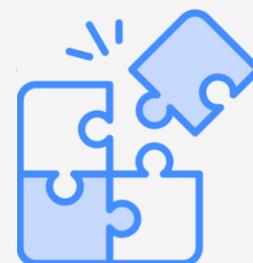
4

Actionable Risk Scores

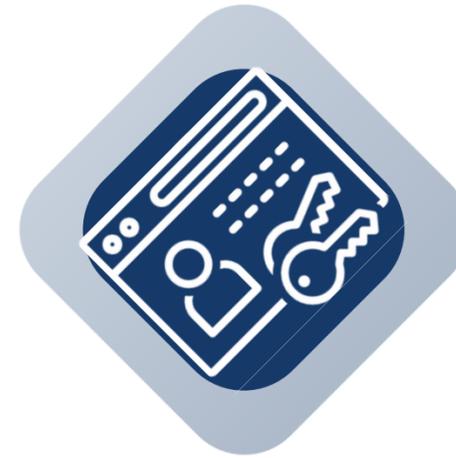


5

Plug-and-Play
Integrations



Benefits to Customers



Reduced Risk of Identity Breaches



Enhanced Zero Trust Initiatives



Faster Incident Response



Improved Compliance and Audit Readiness



Reduced Alert Fatigue

Use Cases



Protecting privileged accounts (Admin, DevOps, DBAs)



Detecting anomalous login behaviors (impossible travel, risky device access)



Monitoring lateral movements inside Active Directory



Real-time response to session hijacking attacks

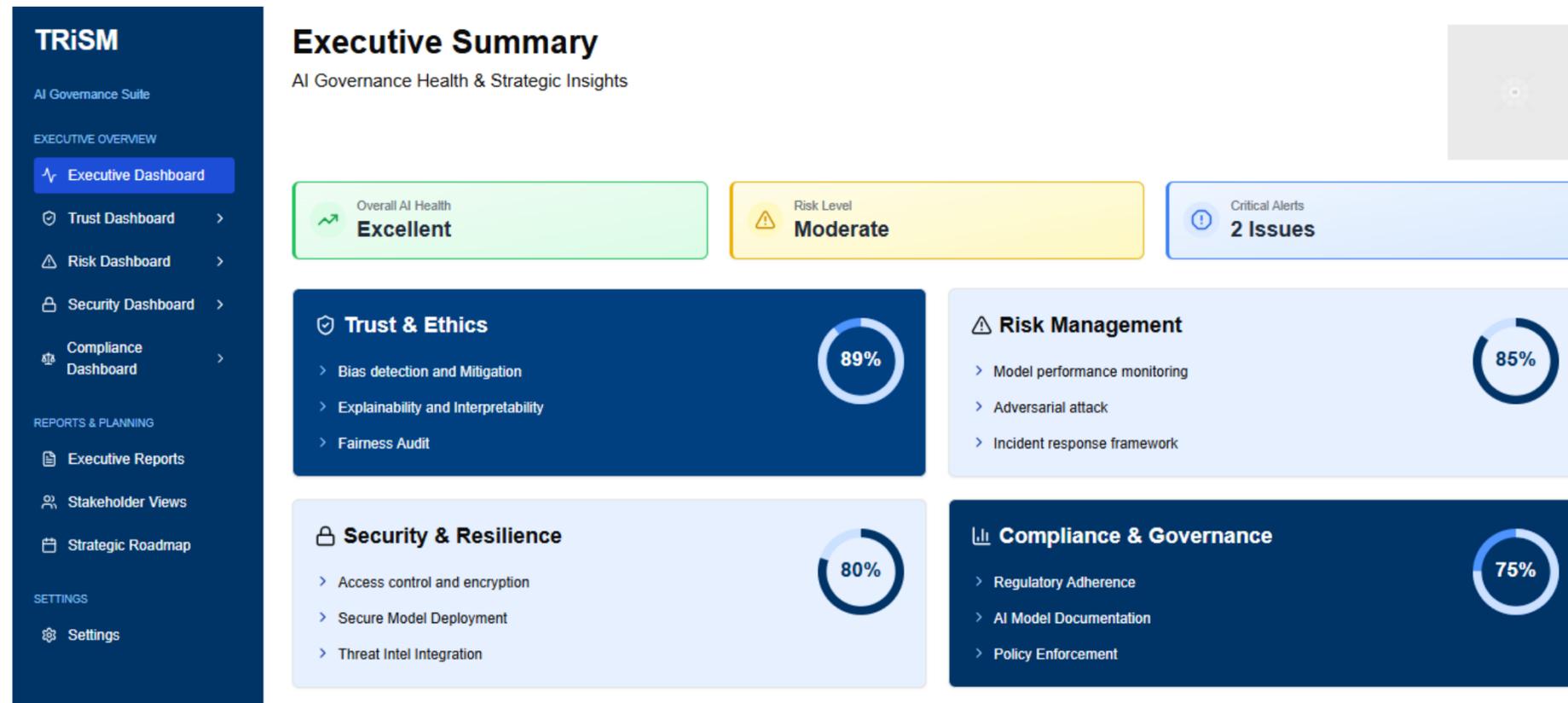


AI Security/Governance

TRISMIq

- **Trust**
Establish transparency, accountability, and model explainability.

- **Security**
Protect AI assets from adversarial attacks and data poisoning.



- **Risk Management**
Identify and mitigate risks in AI models, data, and governance.

- **Compliance**
Enforce policies aligned with ethical and regulatory standards.

Our Offered Services

- ◆ Deployment services
- ◆ Consulting Services
- ◆ Annual Maintenance

Connect with us.



Email

marketing@tech-bridge.biz



Website

www.tech-bridge.biz



Call us

+91 9289440084

