CYBER EAGLE

PROACTIVE PREDICTIVE PROTECTED

STRATEGIC OVERVIEW

Building the orchestration layer for cyber resilience in critical infrastructure

Why Cyber Eagle Exists:

Cyber risk has fundamentally shifted from IT failure to operational & national security concern · The transformation demands a new approach

Most security environments are optimized for detection & alerts while leadership is accountable for uptime, safety & trust · Cyber Eagle addresses this critical mismatch

Operational Disruption

Cyber incidents now directly threaten operations, safety protocols, and business continuity across critical sectors

AI-Accelerated Threats

Artificial intelligence dramatically increases both attack speed and sophistication, outpacing traditional defenses

Regulatory Accountability

New regulations place direct accountability on executives and boards for cyber resilience and incident response

Fragmented Solutions

Security stacks remain tool-centric and siloed, unable to provide unified visibility or coordinated response

The Market Gap We Address

The Problem: **Too many tools · not enough decision clarity**

- Security signals remain siloed across vendors and platforms
- IT and OT visibility rarely converge in meaningful ways
- Executives lack unified, defensible risk perspectives
- Regulators receive fragmented, inconsistent evidence

The Reality

Well-funded organizations cannot answer basic leadership questions: What truly matters? What is at risk? What should be done first? The issue is not lack of tools—it's the absence of orchestration and governance.

What Cyber Eagle Is

Cyber Eagle is an orchestration & decision layer, not another detection tool.

We make security **actionable at executive scale.**

Integration Layer

Sits above existing security technologies without replacing them

Intelligence Engine

Aggregates and contextualizes security signals across the entire environment

Risk Translation

Converts technical findings into operational impact assessments

Governance Output

Produces board-ready and regulator-ready documentation and evidence

Our value proposition is not detection • it is decision support, prioritization & governance at the institutional level

Our Core Architecture · A unified system for cyber resilience

01

Command Nexus

Central orchestration and control plane that coordinates all system components and enables unified decision-making

02

Agentic AI

Intelligent assessment, dynamic prioritization, and autonomous coordination across security domains

03

Sector Context

Industry and regulatory requirements embedded by design, ensuring compliance and sector-specific intelligence

04

Technology Integration

Curated connections with best-in-class security vendors and platforms

The architecture is intentionally modular allowing evolution over time without locking institutions into rigid technologies

How We Think About Vendors · Vendor-Neutral by Design

Our philosophy is clear: vendors should do what they do best. Cyber Eagle exists to integrate, contextualize, and operationalize those capabilities.

No Competition

We do not rebuild best-in-class capabilities that already exist in the market

Vendor Ownership

Security vendors retain their IP, differentiation, and customer relationships

Orchestration Focus

Cyber Eagle concentrates on coordination, governance, and decision support

Integration Over Competition

We succeed when security technologies work together more effectively

Where We Focus · Environments where failure is not acceptable

Energy & Utilities

Power generation, transmission, and distribution systems requiring continuous operation and regulatory compliance

Transport & Logistics

Aviation, rail, maritime, and supply chain infrastructure with complex operational technology environments

Financial Institutions

Banking, payment systems, and financial markets where trust and availability are non-negotiable

Healthcare Systems

Medical facilities and health networks where cyber incidents directly impact patient safety

Government & National Infrastructure

Sovereign systems and national security environments requiring the highest assurance levels

These sectors share common characteristics: long asset lifecycles, extensive regulatory oversight & zero tolerance for operational disruption


EAGLE
L4BS

Service and Delivery Model · **Eagle X LABS**: Execution & Delivery

Our service arm enables pragmatic entry into complex environments, reducing friction and demonstrating value before deeper platform adoption.

Executive Cyber Risk Consulting

Board-level advisory and strategic risk assessments tailored to critical infrastructure requirements

Quantum Readiness Programs

Long-term trust architecture planning and post-quantum cryptography migration strategies

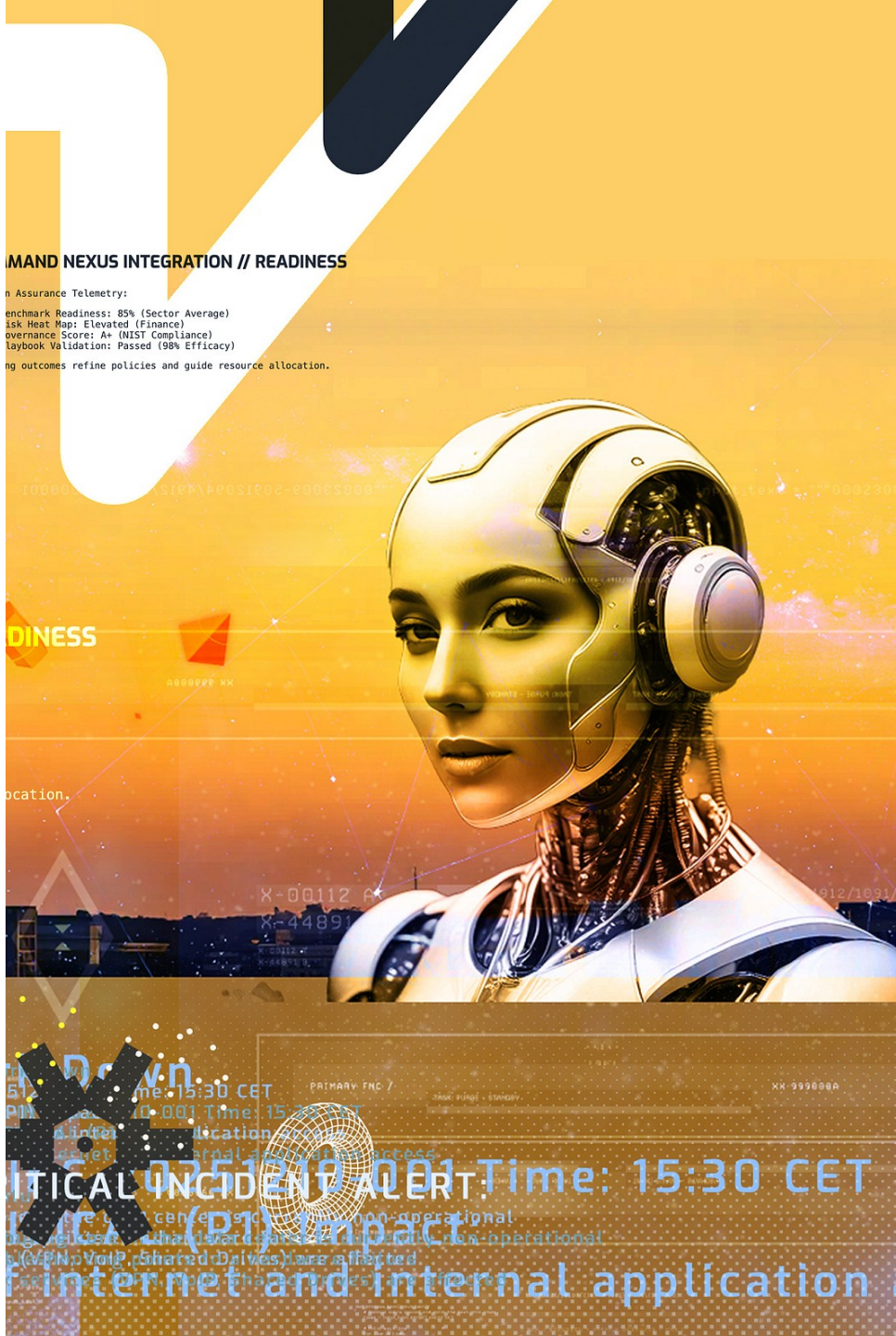
Managed Security Services

Dedicated security operations for critical environments requiring 24/7 monitoring and response

Institutions can start with assessments or advisory services before committing to full platform adoption allowing trust to build organically

Quantum and Long-Term Trust Strategy:

Quantum readiness is strategic infrastructure not a science project.



Long-Lived Trust Domains

Focus on infrastructure w. 20-30 year operational lifecycles requiring cryptographic assurance beyond current standards

Practical Migration Planning

Real-world transition strategies, not theoretical research—addressing operational complexity and legacy systems

Specialist Partnerships

Cryptographic depth delivered through partnerships with experts like QuSecure for post-quantum cryptography

Orchestration at Scale

Cyber Eagle provides governance, deployment coordination, and regulatory alignment for quantum transitions

We separate roles deliberately:

Cryptography experts handle technical implementation, while Cyber Eagle focuses on orchestration, governance & deployment at institutional scale.

How We Go to Market

Executive-Led Trust-Based Engagement

Initial Entry

Assessments, pilots, or strategic advisory engagements that demonstrate value and build credibility

Service Expansion

Growth into managed security services and specialized consulting as trust deepens

Platform Adoption

Full Command Nexus deployment once decision-makers understand strategic value

Long-Term Partnership

Ongoing evolution as a trusted infrastructure partner for cyber resilience

This is not high-velocity selling.

Our buyers are C-suite executives, regulators and national security stakeholders. Credibility and clarity matter more than speed.

Geographic Strategy

Sovereign-Aligned + Regionally Grounded

- **Regional Structures**

  Independent operating entities aligned with local governance and sovereignty requirements

- **Data Residency**

  Full respect for data sovereignty, regulatory boundaries, and national security considerations

- **Long-Term Presence**

  Permanent regional operations over temporary reseller or distributor models

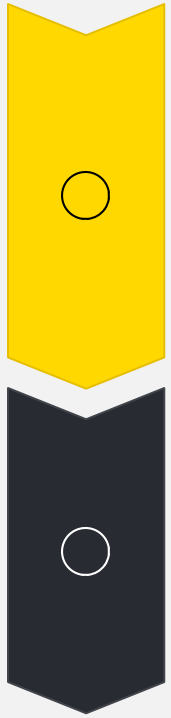
- **Market Focus**

  Initial concentration on allied nations and highly regulated markets where trust is paramount

Cyber Eagle does not operate as a global fly-in vendor.

Each region represents a long-term commitment aligned with local requirements.

Credibility & Execution Signals · Built for trust at the highest levels



Proven Leadership

Executive team with deep experience in national security, critical infrastructure protection & large-scale enterprise security programs

Protected Innovation

Proprietary architecture protected across multiple patent families, demonstrating technical differentiation and long-term value

Sovereign Trust

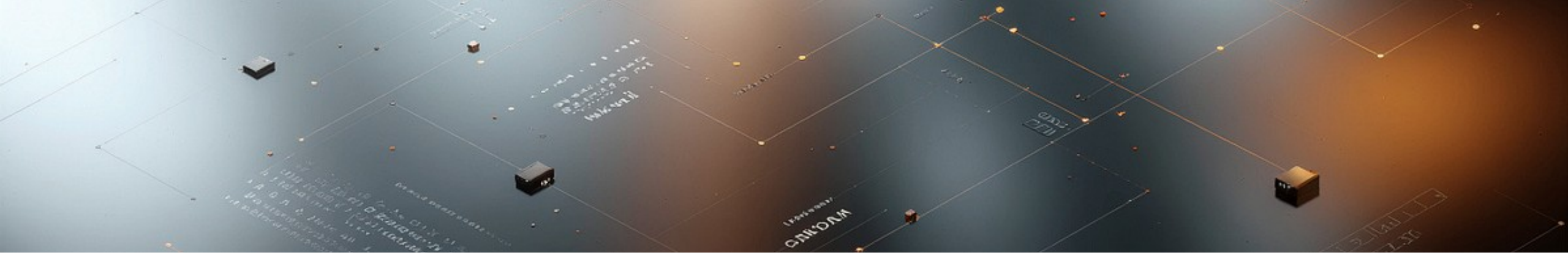
Deployed in mission-critical and sovereign contexts where security, reliability, and accountability are rigorously evaluated

Strategic Partnerships

Collaboration with globally recognized firms including KPMG and Microsoft in defined capacities that enhance credibility

In our markets credibility is not optional.

Buyers must defend decisions to boards, regulators, and governments. We are structured to support that reality.



What Cyber Eagle Is Not · Clarity Matters

We are explicit about boundaries to avoid confusion and ensure alignment with partners and customers.

→ Not a point security product

We do not compete with detection, prevention, or response tools

→ Not a generic SOC

We orchestrate, not just monitor—focused on governance and decision support

→ Not a marketplace

Technology partnerships are curated and strategic, not pay-to-play

→ Not a vendor replacement

We enhance and integrate existing investments, never displace them

Cyber Eagle exists as an enabling layer that amplifies the value of security technologies already in place

What We Are Building Over Time · A system of record for cyber resilience

Unified Visibility

Single source of truth for cyber risk and operational readiness across IT and OT environments

Intelligent Automation

Increasing automation of assessment, prioritization, and coordinated response as AI capabilities mature

Regulatory Integration

Deeper connections with regulatory reporting systems and insurance underwriting processes

National Coordination

Capabilities for sector-wide and national-scale cyber resilience coordination during crisis scenarios

Over time Cyber Eagle becomes infrastructure • not just for security teams but for how cyber risk is governed reported and acted upon at institutional and national levels

Building the orchestration layer cyber ecosystems are missing

Design for Complexity

Purpose-built for environments where failure impacts operations, safety and national security

Built for Governance

Architected to meet the accountability demands of executives, boards and regulators

Focused on Resilience

Cutting through noise to enable clear decisions about the most fundamental & critical matters

Cyber Eagle is building infrastructure for how cyber risk is managed in a world of AI acceleration, regulation & geopolitical complexity • We welcome future conversations where objectives align

CYBER EAGLE

PROACTIVE PREDICTIVE PROTECTED