

CYBER EAGLE QUANTUM SECURITY SUITE



Quantum Readiness, Migration, and Continuous Control

OVERVIEW

Quantum computing introduces a structural break in modern cryptography. Organizations face increasing exposure from cryptographic sprawl, legacy systems, and long lived data vulnerable to "harvest now decrypt later" attacks while regulatory mandates such as CNSA 2.0 and NIST post quantum standards rapidly approach enforcement.

The Cyber Eagle Quantum Security Suite provides a structured, low risk path from cryptographic discovery through post quantum migration and ongoing operational control without disrupting existing infrastructure.

1 • QUANTUM DISCOVERY & CBOM

Proof of Concept

Purpose

Establish immediate visibility into cryptographic assets and quantum exposure, creating a defensible baseline for quantum readiness.

Description

Cyber Eagle Quantum Discovery is a high speed, non intrusive Proof of Concept that maps cryptographic usage across on premises, cloud, and legacy environments. Using Cyber Eagle reconnaissance modules, organizations obtain a live Cryptographic Bill of Materials in days rather than months.



Key Capabilities

- Rapid reconnaissance across modern, legacy, and cloud systems
- Automated Cryptographic Bill of Materials generation
- Identification of weak algorithms, key lengths and certificates
- Detection of "harvest now, decrypt later" exposure
- Risk based prioritization of remediation
- Architecture specific migration roadmap

Deliverables

- Executive Discovery Report
- Machine readable CBOM
- Phased Migration Blueprint

Engagement Model

- Non intrusive deployment
- Typical deployment within one week
- 30 day Proof of Concept

Commercial Model

Flat fee: \$15,000 – \$25,000 per 30 day engagement



2 • QUANTUM RESILIENCE

Post Quantum Remediation

Purpose

Execute migration to post quantum cryptography while maintaining operational continuity and regulatory alignment.

Description

Cyber Eagle Quantum Resilience enables controlled migration to NIST standardized post quantum cryptography using orchestrated crypto agility. Legacy systems are protected through hybrid cryptographic models and post quantum tunnels, avoiding application rewrites or infrastructure replacement.

Key Capabilities

- Centralized crypto agility orchestration
- Post quantum TLS and secure tunneling for legacy systems
- Hybrid classical and post quantum cryptography
- Automated certificate rotation and policy enforcement
- CBOM driven remediation workflows
- Alignment with CNSA 2.0, NIST, and FIPS

Deliverables

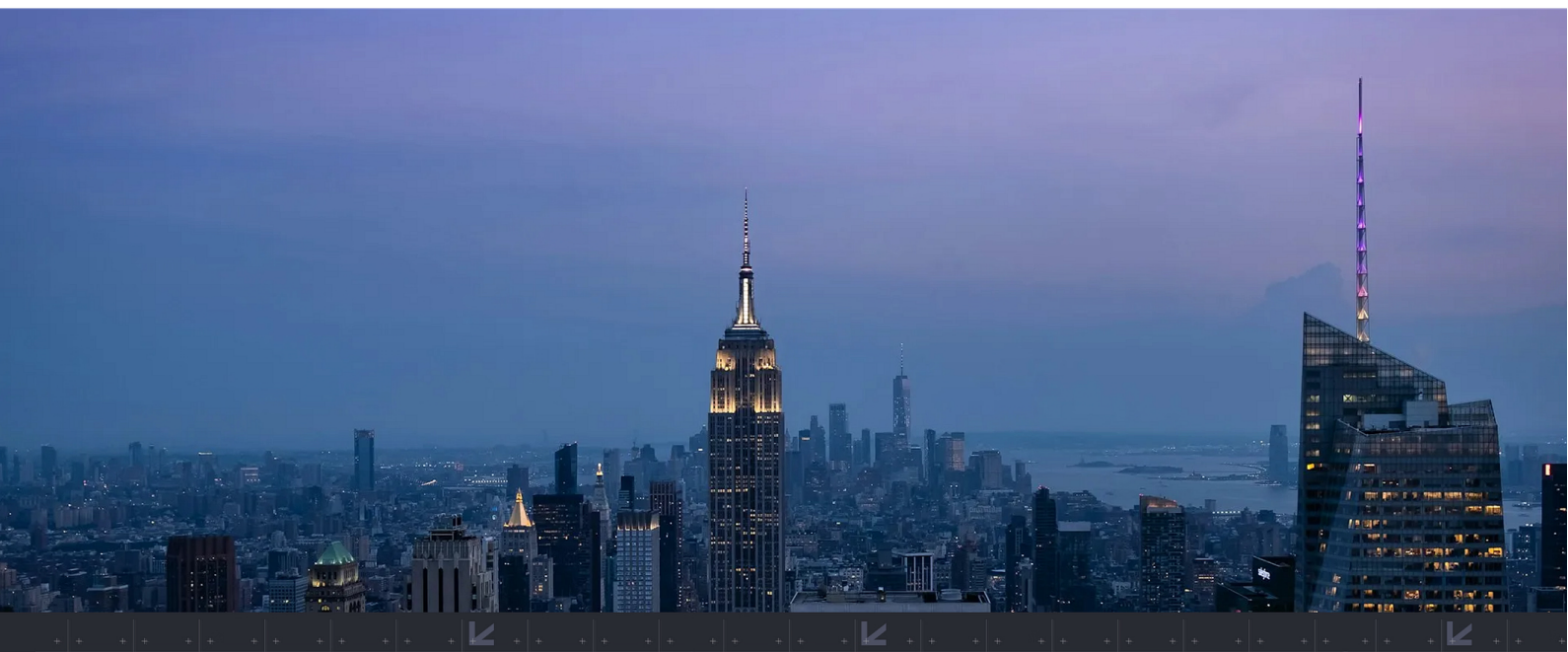
- Implementation plan aligned to CBOM prioritization
- Deployment of PQ enabled controls and tunnels
- Validation evidence for compliance and audit

Engagement Model

- Project based deployment
- Typical duration: 3–9 months
- Phased rollout by system criticality

Commercial Model

Project based pricing: \$100,000 – \$500,000+



Continuous Operations

Maintain a permanent quantum safe posture through continuous monitoring, reporting, and rapid cryptographic control.

Post quantum security is an ongoing operational requirement. Cyber Eagle Quantum Posture Management provides centralized oversight, compliance reporting, and instant crypto policy enforcement across the enterprise as standards and threats evolve.

- Continuous compliance reporting for CNSA 2.0, NIST and FIPS
- Real time cryptographic health monitoring
- Detection of unauthorized or shadow cryptography
- Instant global policy updates via centralized orchestration
- Automated lifecycle management of quantum safe keys and certificates

- Monthly CBOM refresh and drift analysis
- Audit ready reporting pack
- Orchestration support and runbooks

- Managed service or SaaS subscription
- 24~7 monitoring and support
- Monthly CBOM refresh

Subscription: \$5,000 – \$15,000 per month

- Non intrusive discovery with rapid time to value
- CBOM driven intelligence rather than theoretical assessment
- Crypto agility without application rewrites
- Designed for regulated and mission critical environments
- End to end lifecycle coverage from discovery to operations

- Critical infrastructure
- Financial services and insurance
- Government and defense supply chains
- Healthcare and regulated enterprises
- Large enterprises with complex legacy estates

- Discover cryptographic risk.
- Migrate with confidence.
- Operate quantum safe by design.

Cyber Eagle combines advanced automation, cryptographic intelligence, and policy aligned orchestration to help organizations transition safely through foundational shifts such as post quantum cryptography, AI driven threat environments, and regulatory transformation. Working alongside governments, enterprises, and a global partner ecosystem, Cyber Eagle enables resilient, future ready security operations without disrupting mission critical systems.

Availability and deployment timelines depend on customer environment, policy complexity, and regulatory scope. Engagement duration and outcomes may vary based on legacy systems, cryptographic sprawl, and compliance requirements.