CYBER EAGLE

PROACTIVE PREDICTIVE PROTECTED

Unified Offerings Catalog

Consulting · Managed Security · Quantum Trust

Consulting · Managed Security · Quantum Trust

Across IT, OT, and cyber-physical systems

Cyber Eagle serves organizations where digital failure becomes physical consequence. We operate across enterprise IT, operational technology, and critical infrastructure—delivering immediate control today and long-term trust survivability for the systems that cannot fail.

How to use this catalog

Choose a starting point:

CONSULTING OFFERINGS	MANAGED SECURITY SERVICES	QUANTUM TRUST SOLUTIONS
executive assessment	readiness programme	managed protection
01 • Executive Cyber Risk & Resilience Assessment	05 • Managed Threat Exposure & Response	10 • Exposure & Trust Longevity Assessment [VISION]
02 • CMMC Readiness Program	06 • Incident Readiness & Managed Response Retainer	11 • Post-Quantum Transition Blueprint [AGILITY]
03 • Regulatory, Insurance & Audit Readiness Program	07 • Continuous Risk Surface Monitoring	12 • Trust Foundations Deployment [COMPLIANCE]
04 • Incident Readiness & Executive Response Program	08 • Identity & Privilege Control as a Service	
	09 • X Labs Advanced Adversary Simulation & Validation	

- Each offering is designed to stand alone, and also to connect into an end-to-end maturity path.
- Timelines and investment ranges vary by scope, environment complexity and urgency.

01 · Executive Cyber Risk & Resilience Assessment (ECRRA)

You cannot manage cyber risk if you only see half the system.
This assessment shows where digital and physical risk converge and where disruption would actually hurt.

· What it does

A leadership-level assessment of where cyber risk can disrupt operations, safety, public services, or revenue in the next 12–18 months—across both IT and operational environments.

· What you get

01	02	03	04
Executive risk narrative tied to operational outcomes (not control checklists).	Prioritized remediation roadmap with clear ownership & sequencing.	Realistic threat scenarios and impact pathways (IT to OT & cyber-physical).	Board-ready briefing materials and a decision-focused risk register.

· How it works

1	2	3	4
Executive scoping	Targeted IT/OT gap analysis	Realistic threat scenarios	Board-ready risk brief & prioritized remediation roadmap

· At a glance

Ideal for

Boards, CEOs, CFOs, CIOs, CISOs, and critical infrastructure operators.

Typical timeline

2–5 weeks.

Typical investment

$125k–$250k fixed price (scope dependent).

Coverage

Enterprise IT, cloud, ICS/SCADA, IIoT, building management systems, and safety-adjacent environments.

02 · CMMC Readiness Program

CMMC failures rarely start with controls.
They start with proof—missing evidence, unclear ownership, and readiness that can't survive scrutiny. This program makes readiness defensible.

· What it does

A structured readiness program to prepare your organization for CMMC by turning requirements into accountable implementation and audit-ready evidence.

· What you get

01

CUI boundary and scope definition aligned to contracts and data flows.

02

CMMC gap analysis mapped to required practices and maturity expectations.

03

Prioritized readiness roadmap with owners, milestones, and dependencies.

04

Core compliance artifacts (e.g., policies, procedures, SSP/POA&M-ready inputs) and an evidence plan built to survive assessment.

05

Implementation check-ins to keep execution on track and de-risk surprises.

· How it works

1	2	3	4
Trigger identification	CMMC gap analysis	Prioritized readiness roadmap	Implementation check-ins

· At a glance

Ideal for

Defense Industrial Base (DIB) organizations and suppliers that handle CUI or support federal programs.

Typical timeline

4–8 weeks for readiness baseline and plan; implementation timelines vary by scope.

Typical investment

$125k–$250k depending on scope, urgency, and implementation support needs.

Coverage

Enterprise controls plus industrial safety requirements and sector-specific OT mandates (where applicable).

03 · Regulatory, Insurance & Audit Readiness Program (RIARP)

Cyber failures rarely happen in systems first. They happen in evidence, accountability, and preparedness. This program makes readiness defensible—while minimizing compliance overhead through intelligent use of technology.

· What it does

A cross-functional readiness program that prepares your organization to withstand regulatory scrutiny, insurance underwriting, and audit demands—across enterprise and operational environments.

· What you get

01

Regulatory and audit trigger identification (what you must prove, to whom, and when).

02

Gap analysis across control requirements and operational realities.

03

Evidence generation plan, including artifact standards and retention rules.

04

Auditor- & regulator-ready documentation package aligned to your environment.

05

A roadmap that reduces recurring compliance burden through automation and rationalized controls.

· How it works

1	2	3	4
Trigger identification	Regulatory gap analysis	Evidence generation	Auditor & regulator ready documentation

· At a glance

Ideal for

Regulated enterprises: financial services, utilities, transport, healthcare, and government-adjacent entities.

Typical timeline

4–8 weeks.

Typical investment

200k–$400k depending on scope and urgency.

Coverage

Enterprise controls plus industrial safety requirements and sector-specific OT mandates.

04 · Incident Readiness & Executive Response Program (IRERP)

When cyber incidents affect operations, hesitation is as dangerous as malware.

This program ensures leaders are ready before it matters.

· What it does

An executive-focused incident readiness engagement that ensures leadership can make fast, correct decisions during incidents that threaten operations, safety, or trust.

· What you get

01

Review of incident response plans, authority models, and decision paths.

02

Executive-ready playbooks for ransomware, outages, and OT disruption scenarios.

03

Facilitated tabletop simulations tailored to your environment and risk profile.

04

Post-exercise remediation roadmap and prioritized improvements.

05

Optional alignment with legal, communications, and insurer requirements.

· How it works

1	2	3	4
Executive intake	Plan & authority review	Facilitated tabletop simulations	Post-exercise remediation roadmap

· At a glance

Ideal for

Boards and executive teams in critical infrastructure and high-consequence enterprises.

Typical timeline

4–6 weeks.

Typical investment

150k–$300k.

Coverage

Enterprise incidents, ransomware, OT outages, and cyber-physical cascading failures.

05 · Managed Threat Exposure & Response (MTER)

Cyber threats do not stop at the factory gate.
This service ensures attacks on operations are handled before they disrupt production or safety.

· What it does

24×7 monitoring, detection, investigation, and response for threats targeting enterprise IT, cloud platforms, and OT-connected systems.

· What you get

01

Telemetry onboarding and baseline creation across endpoints, cloud, and key OT-IT convergence points.

02

Continuous monitoring with triage, investigation, and containment actions.

03

Actionable guidance for eradication and recovery with clear executive visibility.

04

Monthly reporting that ties findings to risk posture and operational impact.

05

· How it works

1	2	3	4
Telemetry onboarding	Baseline	Continuous monitoring & response	Monthly executive reporting

· At a glance

Ideal for

Organizations that need 24×7 coverage without building a full internal SOC.

Typical timeline

Onboarding in weeks; ongoing service via annual contract.

Typical investment

$12k–$40k per month (annual contracts).

Coverage

Endpoints, cloud workloads, industrial gateways, and OT-IT convergence points.

06 · Incident Readiness & Managed Response Retainer (IRM2R)

When incidents escalate, time and judgment matter more than tools.
This retainer ensures expert response is available immediately.

· What it does

A guaranteed-access retainer for experienced responders during incidents that threaten operations, safety, or continuity—paired with pre-incident readiness alignment.

· What you get

01

Pre-incident readiness review and response plan alignment.

02

Guaranteed access to responders when an incident occurs.

03

Incident leadership support: containment, coordination, and decision guidance.

04

Post-incident reporting and lessons learned to prevent recurrence.

05

· How it works

1	2	3	4
Pre-incident readiness review	Retainer activation	Incident response	Post-incident reporting

· At a glance

Ideal for

Boards and CISOs who want assured response capacity under pressure.

Typical timeline

Retainer activated immediately upon signature; annual term.

Typical investment

$150k–$300k annual retainer.

Coverage

Enterprise incidents, OT disruptions, and plant shutdown scenarios.

07 · Continuous Risk Surface Monitoring (CRSM)

Digital expansion quietly increases operational risk.

This service shows how exposure grows before it becomes visible through an incident.

· What it does

Continuous monitoring of your external attack surface, cloud assets, remote access paths, and OT-connected exposure—so risk is addressed before it accumulates into failure.

· What you get

01

Asset discovery and exposure mapping across internet-facing and cloud environments.

02

Continuous detection of misconfigurations, vulnerabilities, and risky access paths.

03

Prioritized alerts with clear remediation guidance and ownership alignment.

04

Monthly posture reporting to track risk trends and improvement.

05

· How it works

1	2	3	4
Asset discovery	Continuous monitoring	Prioritized alerts	Monthly risk posture reporting

· At a glance

Ideal for

Fast-scaling enterprises and risk teams seeking continuous visibility.

Typical timeline

Onboarding in weeks; ongoing service via annual contract.

Typical investment

$8k–$25k per month.

Coverage

External perimeter, cloud, and shadow OT connectivity.

08 · Identity & Privilege Control as a Service (IPCS)

Most breaches start with access that should never have existed.

This service prevents identity from becoming the weakest link.

· What it does

Managed identity, access, and privilege governance across enterprise, cloud, and operational environments—designed to support Zero Trust and audit demands.

· What you get

01

Identity and privilege review with a baseline of high-risk access paths.

02

Continuous enforcement of least privilege and privileged access controls.

03

Detection of identity threats and anomalous privilege behavior (where supported).

04

Audit-ready reporting for access, exceptions, and privileged activity.

05

· How it works

1	2	3	4
Identity review	Privilege baseline	Continuous enforcement	Audit-ready reporting

· At a glance

Ideal for

Hybrid IT/OT enterprises where privileged access is business-critical.

Typical timeline

Onboarding in weeks; ongoing service via annual contract.

Typical investment

$10k–$30k per month.

Coverage

Remote vendor access, plant engineering accounts, and privileged OT access.

09 · Eagle X Labs — Advanced Adversary Simulation & Validation (AASV)

Compliance shows intent.

This service proves whether defenses hold when adversaries target operations.

· What it does

A high-fidelity adversary simulation and validation engagement that tests whether defenses withstand realistic attacks against enterprise and operational systems.

· What you get

01

Threat modeling aligned to your sector, adversary profile, and operational constraints.

02

Adversary simulation across IT and, where appropriate, OT-IT convergence points.

03

Response validation: detection, escalation, containment, and executive decision paths.

04

- Executive resilience scoring with prioritized hardening and response improvements.

05

· How it works

1	2	3	4
Threat modeling	Adversary simulation	Response Validation	Executive resilience scoring

· At a glance

Ideal for

Mature security programs, financial services, and critical infrastructure operators.

Typical timeline

3–6 months (engagement dependent).

Typical investment

$250k–$750k per engagement.

Coverage

Enterprise, industrial systems, and safety-adjacent controls.

10 · Quantum Exposure & Trust Longevity Assessment (Quantum Vision)

Operational systems last decades. Cryptography often does not.

This assessment shows where trust will age badly—and what to do first.

· What it does

An assessment that identifies where the cryptography protecting data, software, firmware, and operational systems will fail to remain trustworthy over time.

· What you get

01

Cryptographic discovery and inventory across key trust domains.

02

Exposure classification (data at rest, data in transit, signing, and embedded/firmware trust).

03

Risk prioritization based on longevity, operational constraints, and regulatory pressure.

04

Action roadmap for mitigation and post-quantum transition planning.

05

· How it works

1	2	3	4
Executive scoping	Cryptographic discovery	Exposure classification	Action roadmap

· At a glance

Ideal for

CISOs, boards, critical infrastructure operators, and financial institutions.

Typical timeline

3–6 weeks.

Typical investment

$150k–$300k.

Coverage

Enterprise PKI, software signing, industrial controllers, and firmware.

11 · Post-Quantum Transition Blueprint (Quantum Agility)

You cannot replace industrial systems overnight.

This blueprint shows how to transition trust without breaking operations.

· What it does

A regulator-defensible migration path to post-quantum cryptography across enterprise and operational systems—sequenced to avoid operational disruption.

· What you get

01

System and trust-domain prioritization based on business and operational criticality.

02

Hybrid PQC strategy that supports phased adoption and interoperability.

03

Migration sequencing plan aligned to vendor cycles and operational constraints.

04

Compliance and governance documentation to support audits and regulators.

05

· How it works

1	2	3	4
System prioritization	Hybrid PQC strategy	Migration sequencing	Compliance documentation

· At a glance

Ideal for

CIOs, CISOs, regulated enterprises, and governments.

Typical timeline

6–10 weeks.

Typical investment

$250k–$500k.

Coverage

Legacy OT constraints and long-lived infrastructure.

12 · Quantum Trust Foundations Deployment (Quantum Compliance)

We protect what must remain trusted the longest, first. Everything else can wait.

· What it does

Deployment of post-quantum trust controls for the assets and trust domains that must remain trustworthy the longest—paired with validation and governance documentation.

· What you get

01

Selection of trust domains (e.g., signing, firmware, PKI, secure communications) based on longevity and impact.

02

Hybrid PQC deployment and configuration with validation testing.

03

Operational runbooks and governance documentation for auditability and continuity.

04

Transition plan for adjacent systems to expand coverage over time.

05

· How it works

1	2	3	4
Select trust domains	Hybrid PQC deployment	Validation	Governance documentation

· At a glance

Ideal for

Critical infrastructure operators and organizations with long-lived trust requirements.

Typical timeline

3–6 months per trust domain.

Typical investment

$500k–$2M per trust domain.

Coverage

Firmware signing, industrial controllers, and safety systems.

Next Steps

A typical engagement starts with a short scoping call to confirm environment boundaries, constraints, and urgency.

1. Select the right starting point (assessment, readiness, or managed protection).
2. Confirm scope and success criteria (IT, OT, cloud, sites, and critical workflows).
3. Finalize timeline and investment range based on complexity and speed-to-value.
4. Kick off with executive alignment and a clear evidence and ownership model.

To schedule a scoping call contact your Cyber Eagle representative or email us below:

CONTACT US [email]

2001 L Street Northwest
Suite 500
Washington, DC 20036

info@cybereagle.ai