CYBER EAGLE

PROACTIVE PREDICTIVE PROTECTED

Incident Readiness & Managed Response Retainer

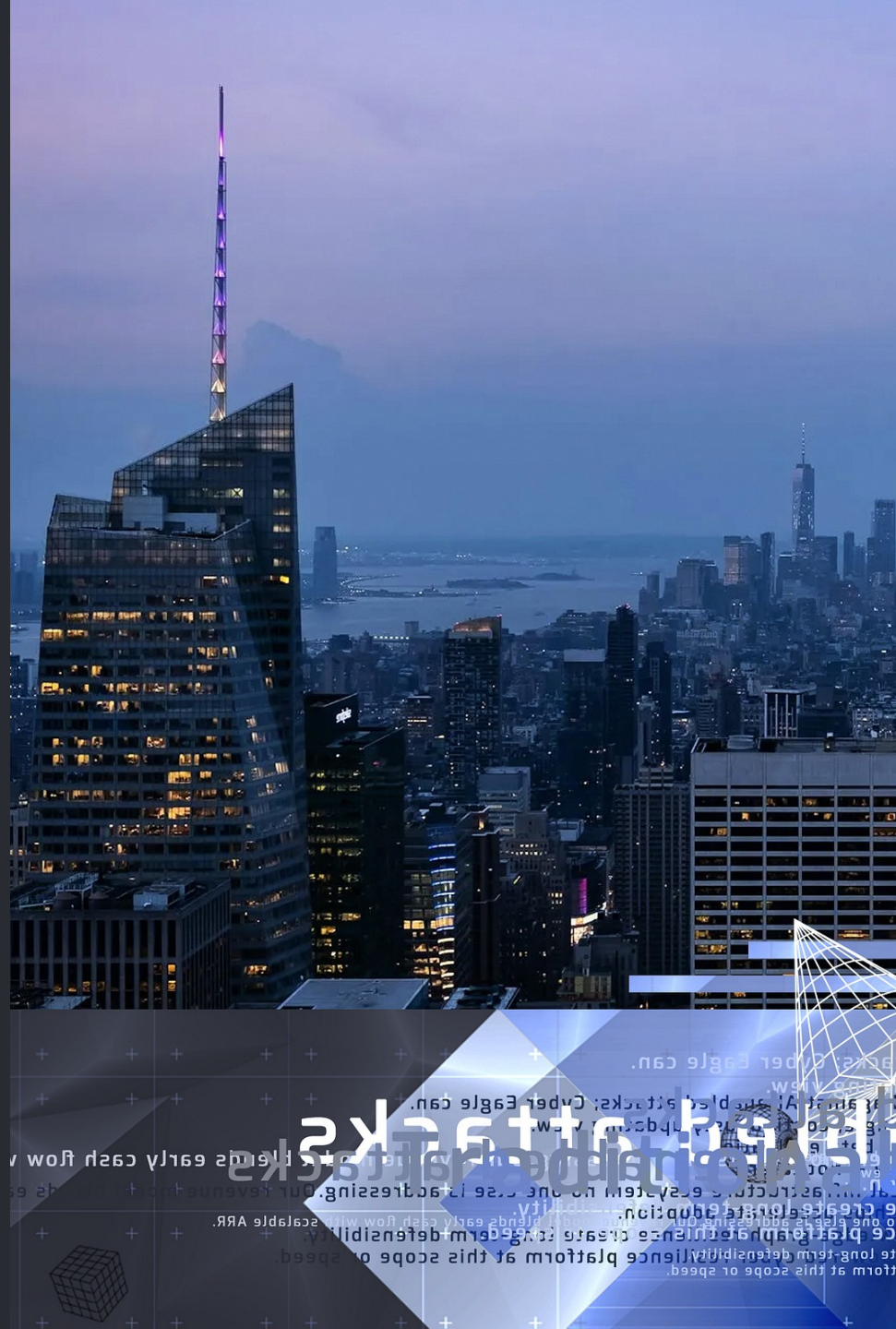
Why this matters now?

Cyber risk is no longer contained within IT systems.

Across industries, digital issues increasingly produce operational, regulatory, and trust consequences that leadership teams must answer for - often without having been shown the full picture.

As systems become more interconnected and long-lived, the cost of misunderstanding risk grows faster than the cost of addressing it.

This offering exists to address that gap.



What this is

A standing retainer that ensures immediate access to experienced incident responders during significant cyber events affecting operations, safety, or trust.

This is about preparedness, not panic buying.

The problem addressed

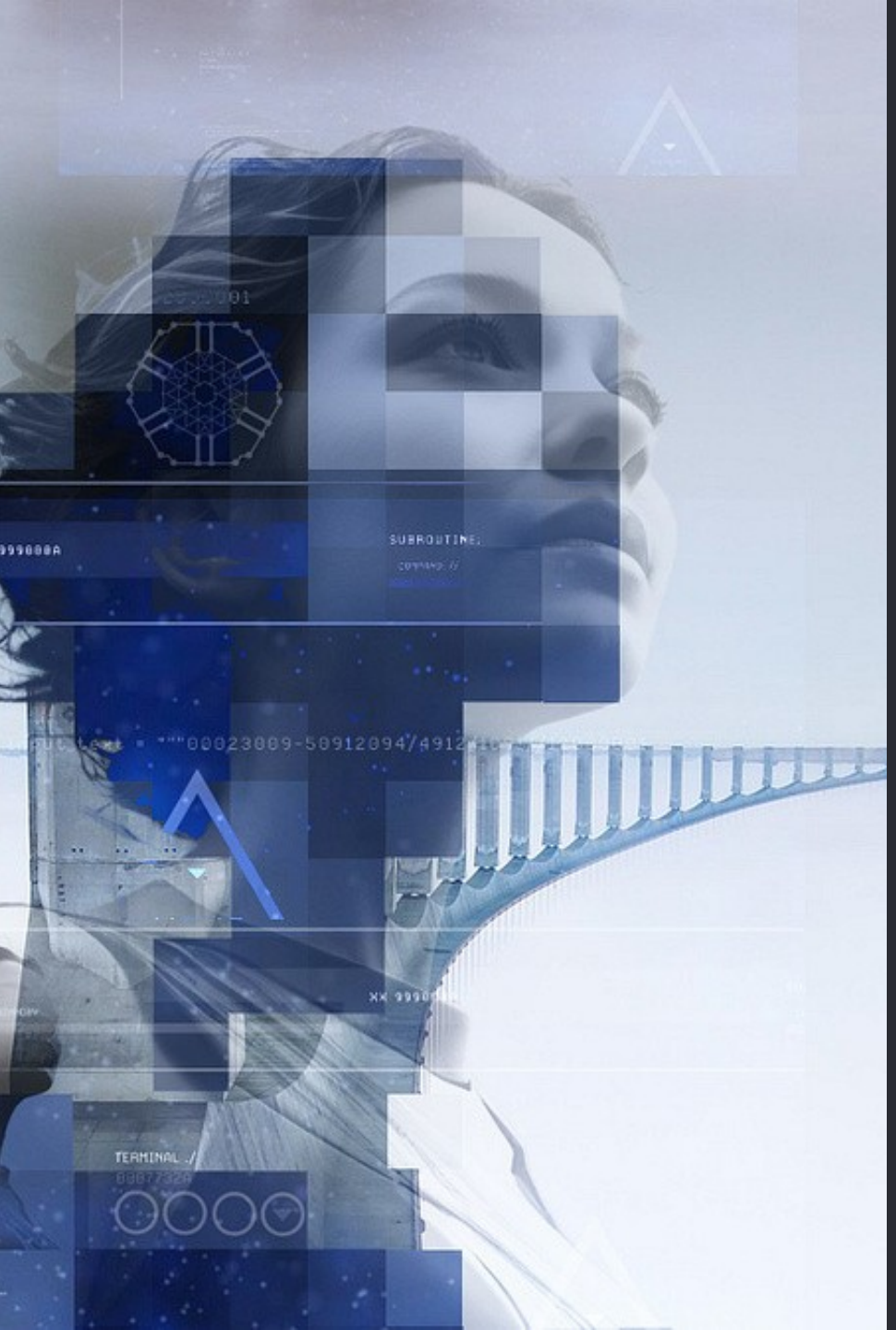
During incidents, time is lost securing expertise, clarifying authority, and coordinating response.

Delays increase impact.

What it does

The retainer guarantees rapid access to skilled responders who support both technical containment and executive decision-making.

- Provides on-call incident response
- Supports containment and investigation
- Advises leadership during crisis decisions
- Assists with coordination and communications



How it works

- Pre-incident readiness alignment
- Defined activation procedures
- Immediate response when triggered
- Post-incident review and improvement

What you receive

- Immediate access to response expertise
- Faster containment and recovery
- Reduced executive burden during crises
- Clear post-incident guidance

Who is this for

Boards, executive teams, and organizations where downtime or confusion would have material consequences.

When organizations typically engage

Organizations engage when leadership recognizes that existing tools or reports no longer provide sufficient confidence, but before disruption forces reactive decisions.

This engagement is designed to:

- Create shared understanding
- Enable defensible decisions
- Reduce uncertainty at the executive level

It is intentionally scoped, proportionate, and designed to fit where the organization is today.

EAGLE

L4BS

Book a strategy briefing

Document: Managed Threat Exposure & Response | Category: Active Defense & Threat Management | Version: 1.0 | Date: 2026-09-18 Target Audience: Organizations requiring continuous protection without internal security operations management Summary: Outcome-led service ensuring cyber threats targeting enterprise IT, cloud environments, and OT-connected systems are detected and handled before disrupting operations. Keywords: managed threat exposure, active defense, continuous monitoring, threat response, IT and OT security, operational impact, threat investigation, incident containment.