CYBER EAGLE

PROACTIVE PREDICTIVE PROTECTED

Managed Threat Exposure & Response

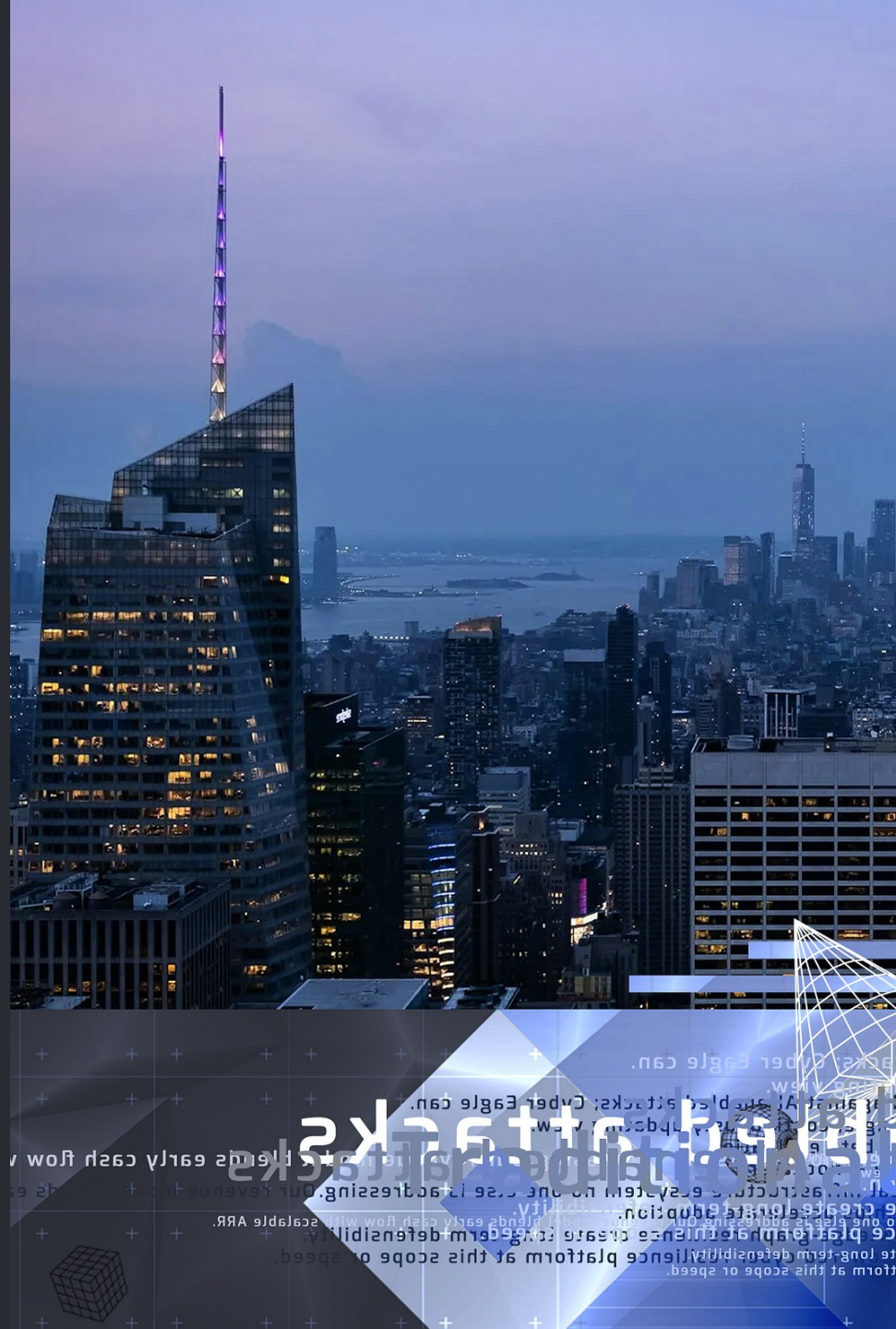
Why this matters now?

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

An outcome-led service that ensures cyber threats targeting enterprise IT, cloud environments, and OT-connected systems are detected and handled before they disrupt operations.

This is not about generating alerts.
It is about owning response outcomes.

The problem addressed

Many organizations have monitoring tools but lack the ability to respond continuously and decisively.

Common challenges include:

- Alerts without action
- Gaps outside business hours
- Limited visibility across IT and OT
- Delayed escalation during real incidents

As a result, small issues escalate into operational disruptions.

What it does

Managed Threat Exposure & Response provides continuous detection, investigation and response.

- Monitors for material threats across IT, cloud, and OT-connected systems
- Investigates suspicious activity to determine real risk
- Contains incidents before escalation
- Provides executive-level visibility into exposure and response

The focus is always on operational impact

How it works

- Environment onboarding and baseline establishment
- Continuous monitoring for threats and anomalies
- Active investigation and response when events occur
- Executive reporting focused on material risk and outcomes

What you receive

- Always-on protection across critical environments
- Incidents handled, not just logged
- Reduced operational disruption
- Clear executive visibility into threat activity

Who is this for

Organizations that require continuous protection but do not want to build or manage security operations internally.

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.