Cyber Resilience:

Shifting from Risk to Readiness

Tia Hopkins

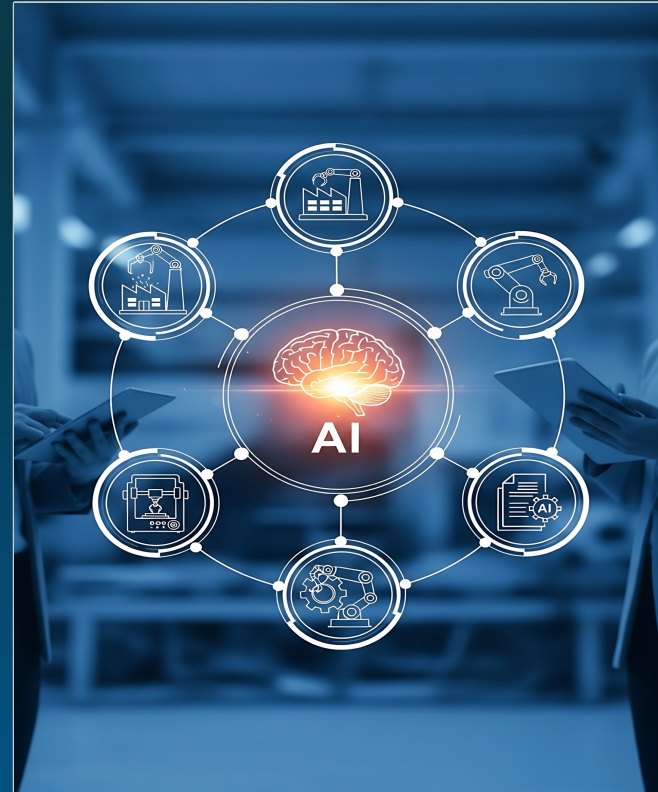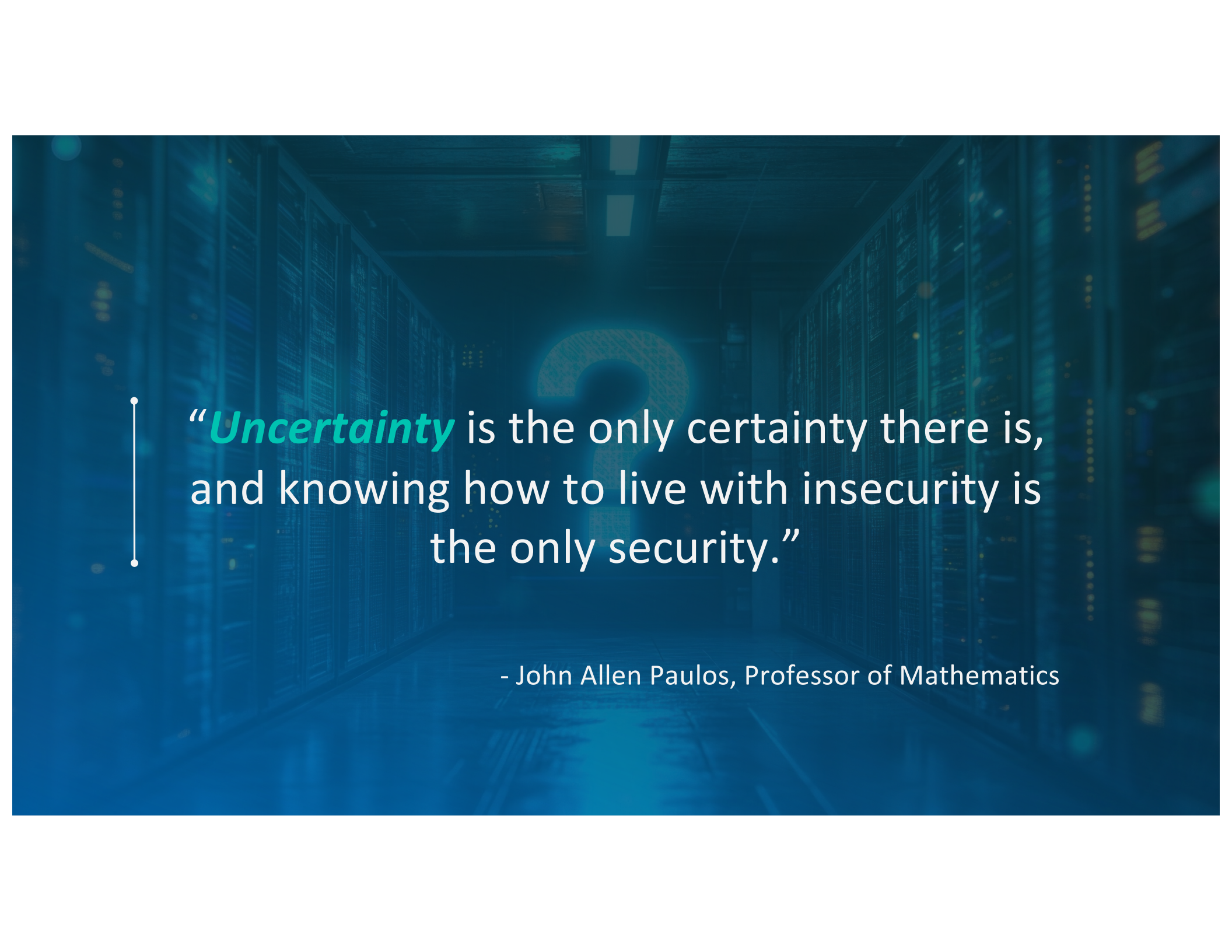*Chief Cyber Resilience Officer & Field CTO*

eSENTIRE

The Struggle is Real

Attackers are relentless; defending the enterprise is becoming more challenging

AI transforming network operations management

"*Uncertainty* is the only certainty there is, and knowing how to live with insecurity is the only security."

- John Allen Paulos, Professor of Mathematics

If uncertainty is the baseline, how do we lead with confidence?

Cyber Resilience...

What the heck is that?

> **"**
>
> Cyber resilience is the ability to *anticipate*, *withstand*, *recover* from, and *adapt* to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.
>
> - NIST SP 800-160 Vol. 2 Rev. 1

The Mindset Shift – Security vs Resilience Outcomes

SECURITY	RESILIENCE

SECURITY

How safe are we?

Prevent what we know to protect against

Reactive controls, patching, perimeter defense

Fragile — success defined as "no incidents"

VS.

RESILIENCE

How ready are we?

Prepared for the unexpected

Continuous improvement, adaptation
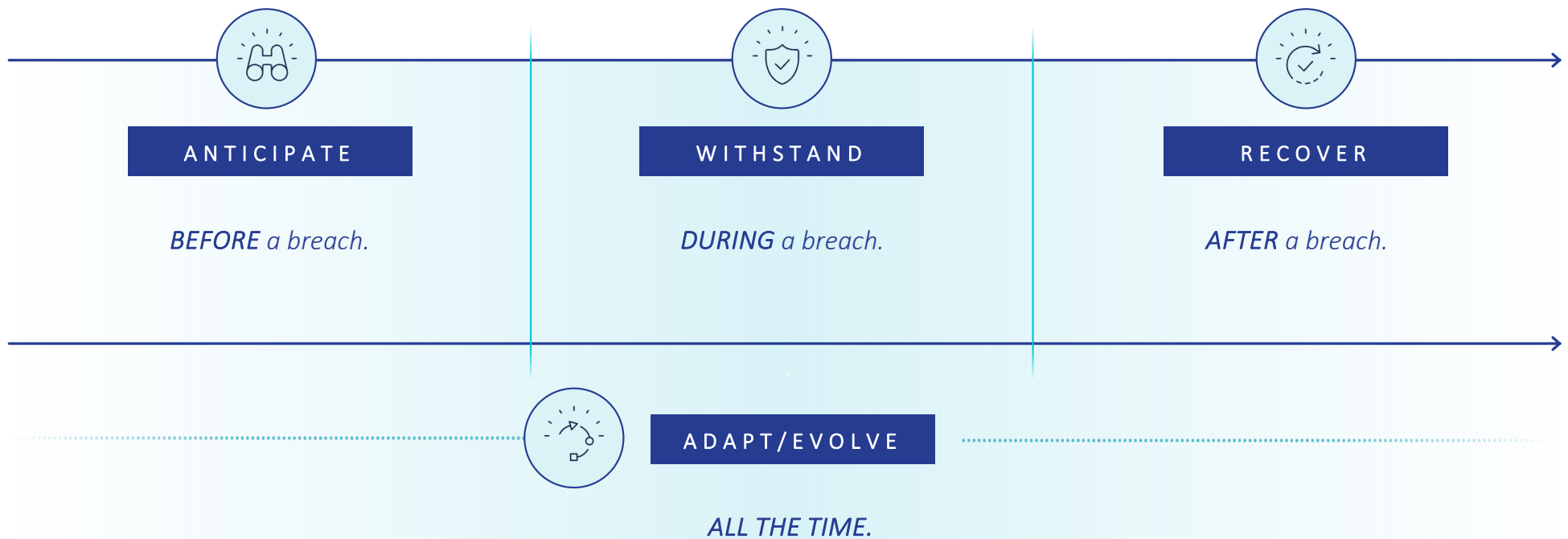
Durable — success defined as continuity + adaptability

It's No Longer a Matter of 'If'. It's a Matter of 'When'. *How Ready Are You?*

BUILD RESILIENCE. PREVENT DISRUPTION.

Anticipate, Withstand, and Recover from cyber attacks. Continuously Adapt and Evolve your program based on your learnings.

ANTICIPATE

BEFORE a breach.

WITHSTAND

DURING a breach.

RECOVER

AFTER a breach.

ADAPT/EVOLVE

ALL THE TIME.

Cyber Resilience Realized...

ANTICIPATE

Continuous Threat Exposure Management

TAKE CONTROL OF CYBER RISK BEFORE ATTACKERS EXPLOIT IT

WITHSTAND

Managed Detection & Response

PREVENT THREATS BECOMING BUSINESS DISRUPTING EVENTS

RECOVER

Digital Forensics & Incident Response

CONTAIN INCIDENTS QUICKLY AND RESTORE BUSINESS OPERATIONS WITH CONFIDENCE

ADAPT/EVOLVE | CONTINUOUSLY ADAPT DEFENSES AND EVOLVE WITH EMERGING THREATS

Continuous Threat Exposure Management (CTEM)

Anticipate

Anticipate: Continuous Threat Exposure Management

Continuous Threat Exposure Management (CTEM):

A proactive cybersecurity approach that aligns security efforts with business goals by continuously identifying, prioritizing, and mitigating exposures.

✓ SCOPING

Understand the organization's environment, assets, and business context to define the scope of threat exposure management.

✓ DISCOVERY

Identify vulnerabilities, attack surfaces, and exposure points across the organization's people, processes, and technologies.

✓ PRIORITIZATION
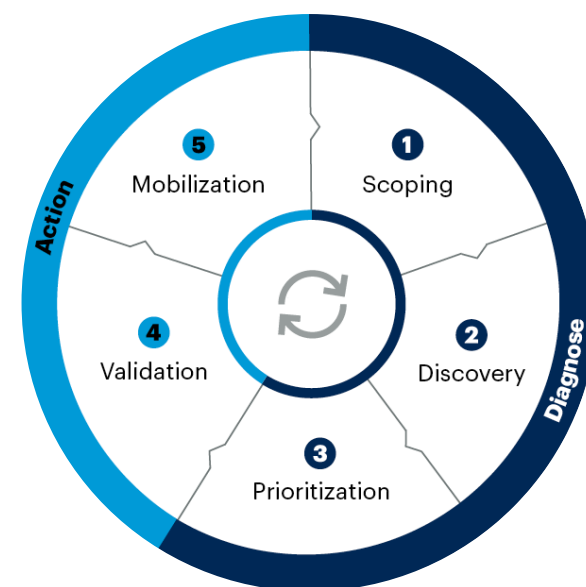
Assess and rank threats and vulnerabilities based on business impact, exploitability, and risk severity to focus remediation efforts.

✓ VALIDATION

Test and confirm the effectiveness of controls and remediations, ensuring vulnerabilities are resolved and risks are mitigated.
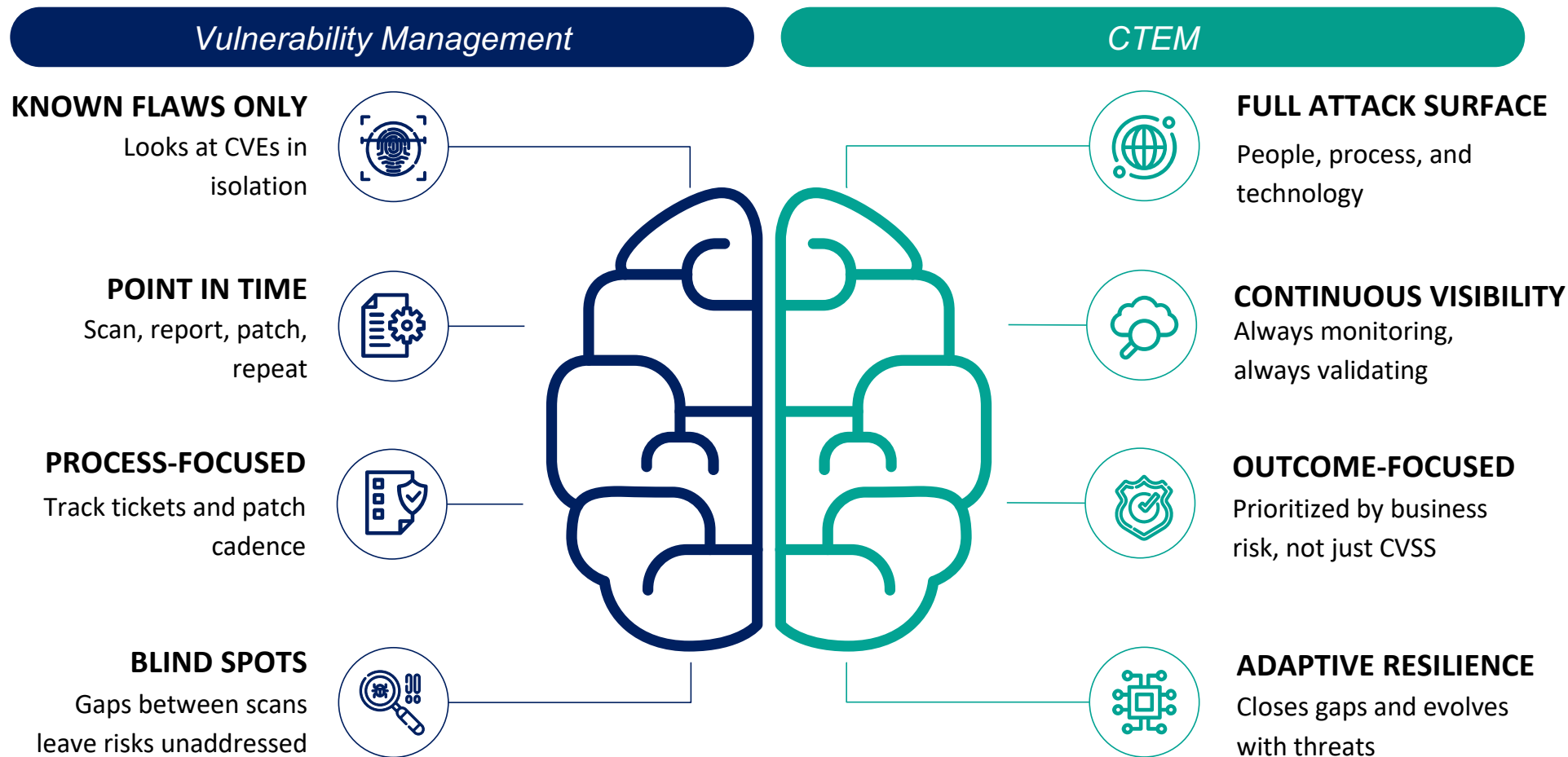
✓ MOBILIZATION

Establish a plan and execute actions to improve security posture, ensuring alignment with organizational priorities, cross-functional teams and operational readiness.
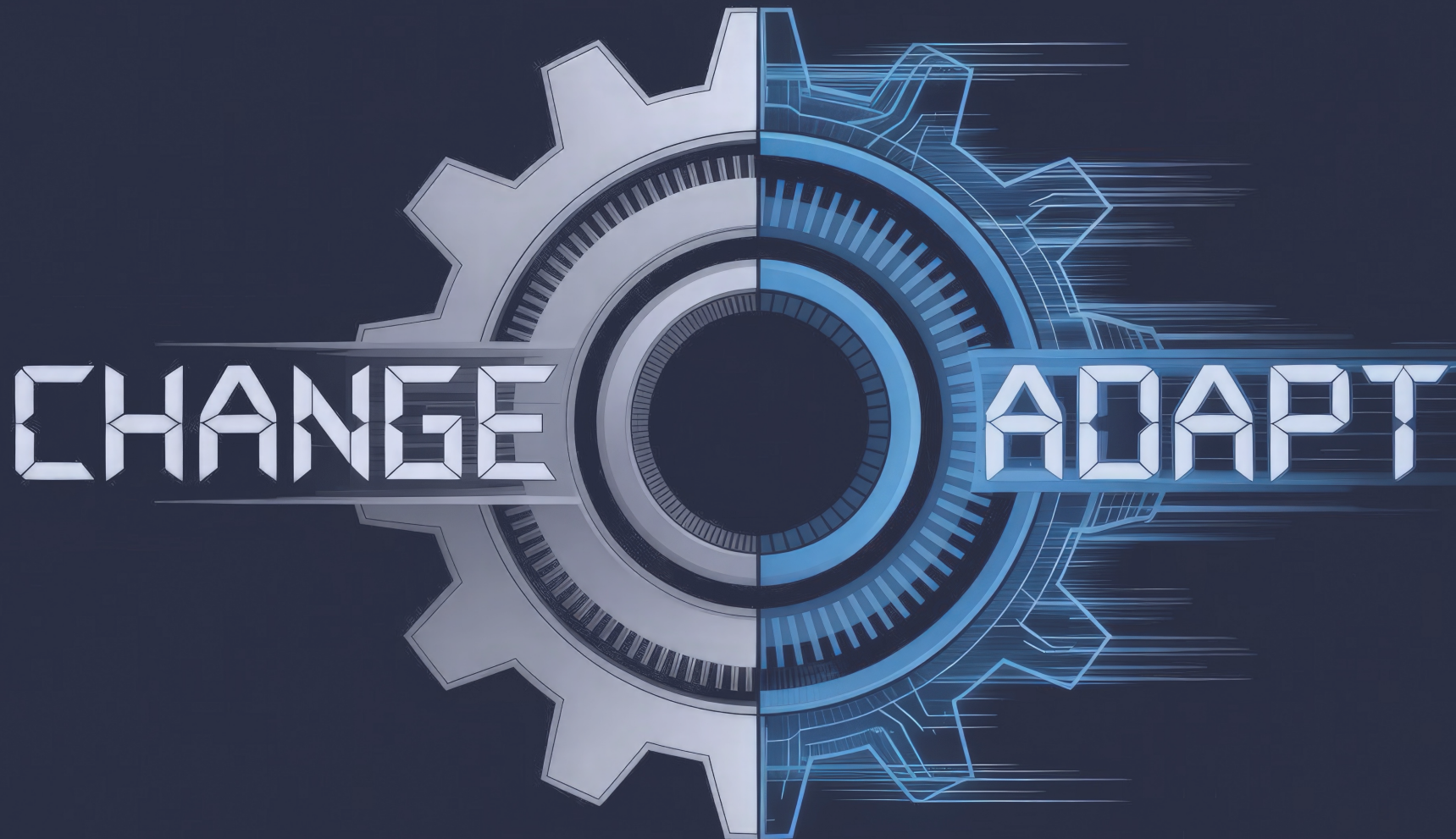
Beyond Vulnerabilities: Managing Real Exposure

Vulnerability Management	CTEM

KNOWN FLAWS ONLY
Looks at CVEs in isolation

POINT IN TIME
Scan, report, patch, repeat

PROCESS-FOCUSED
Track tickets and patch cadence

BLIND SPOTS
Gaps between scans leave risks unaddressed

FULL ATTACK SURFACE
People, process, and technology

CONTINUOUS VISIBILITY
Always monitoring, always validating

OUTCOME-FOCUSED
Prioritized by business risk, not just CVSS

ADAPTIVE RESILIENCE
Closes gaps and evolves with threats

Managed Detection & Response (MDR)

Digital Forensics & Incident Response (DFIR)

Recover

Adapt

CTEM + MDR = Adaptive Advantage

CTEM Enhancing MDR

MDR Enhancing CTEM

CTEM

MDR   CTEM

MDR
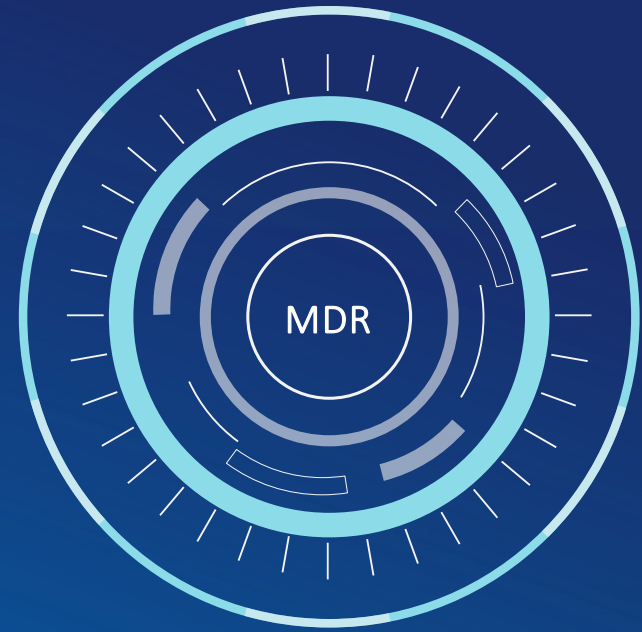
Humans + AI

AI + Human Synergy

AI = The Force Multiplier

01 Scale
Processes massive volumes of data far beyond human capacity.

02 Speed
Detects anomalies and surfaces signals at machine pace.

03 Consistency
Executes repetitive tasks with reliability and without fatigue.

01 Context
Understand business priorities, nuance, and impact.

02 Strategy
Align actions to long-term goals, not just immediate fixes.

03 Accountability
Own the decisions, the communication, and the outcomes.

HUMANS = The Compass

17

AI as a Force Multiplier

AI in Action

Anticipate

CTEM

Humans define business priorities; *AI* processes data at scale to map exposures against them.

Recover

DFIR

AI handles rapid forensic data analysis; *humans* investigate impact, coordinate response, and lead communication.

Withstand

MDR

AI accelerates triage and anomaly detection; *humans* interpret context and decide how to respond.

Adapt

CONTINUOUS IMPROVEMENT

AI identifies recurring patterns and trends; *humans* apply lessons to strengthen strategy and resilience.
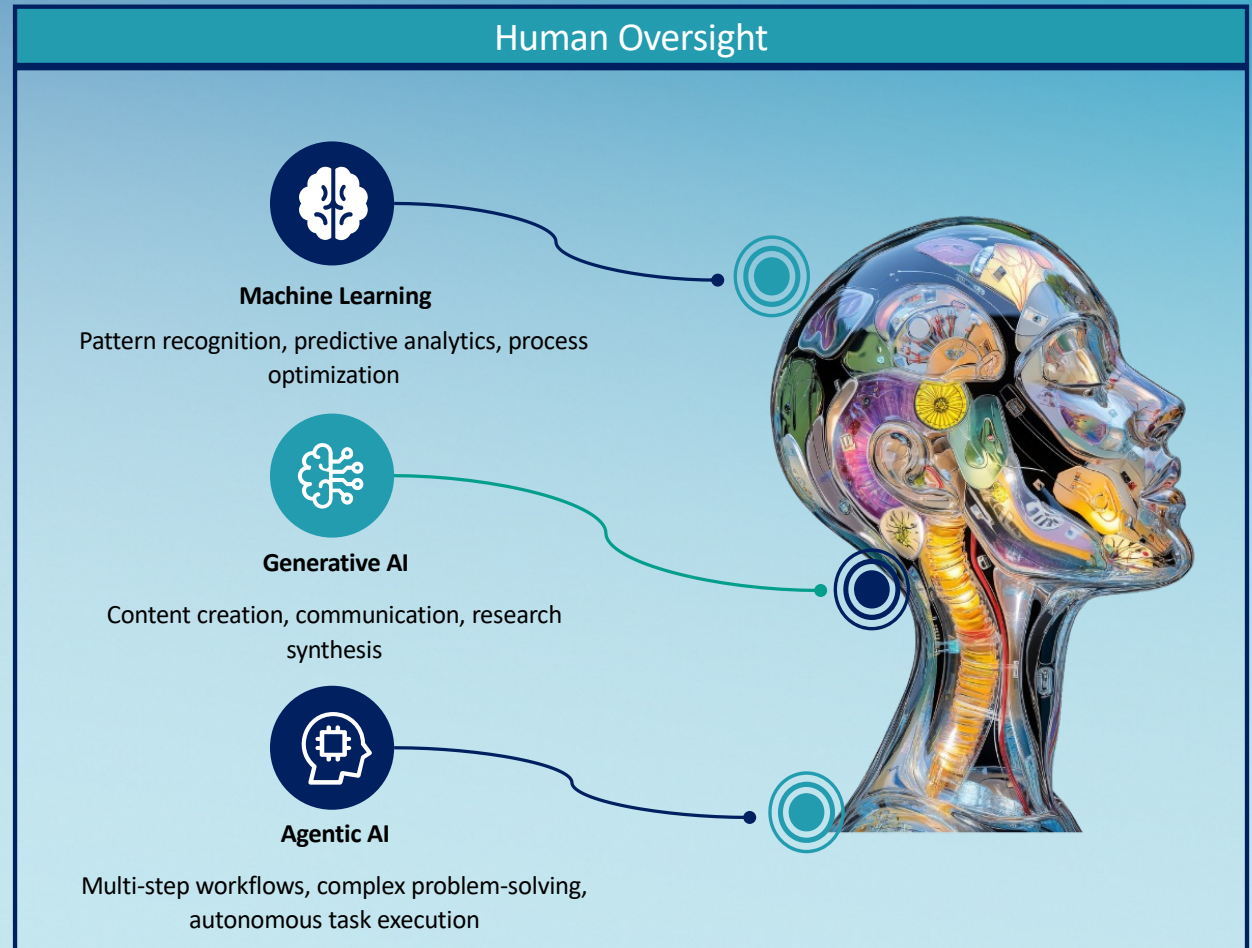
AI Business Process Transformation

S cope and assess current state

C ategorize by AI readiness

A lign technology to value

L ayer human oversight

E xecute responsibly

Human Oversight

Machine Learning
Pattern recognition, predictive analytics, process optimization

Generative AI
Content creation, communication, research synthesis

Agentic AI
Multi-step workflows, complex problem-solving, autonomous task execution

Sooo... how do we lead with confidence?

Thriving in the Face of Uncertainty

BUILD RESILIENCE. PREVENT DISRUPTION.

Anticipate, Withstand, and Recover from cyber attacks. Continuously **Adapt** and **Evolve** your program based on your learnings.

ANTICIPATE

Control the controllables.

WITHSTAND

Limit the scope.

RECOVER

Get back to normal.

ADAPT/EVOLVE

Learn from our mistakes.

Resilience is a Team Sport

Better Together

People + **Process** + **AI/Technology** + **Partnerships**

Cyber Resilience

THANK YOU!

✉ tia.hopkins@esentire.com

in linkedin.com/in/yatiahopkins

🔗 esentire.com | tiahopkins.com