Can AI Bridge the Cybersecurity Gap?

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Russell Safirstein, President & CEO, NexAI Cyber

Welcome To The 11th Annual Hacking Conference

Check in Code: Cobra

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Russell Safirstein

Russell Safirstein is a cybersecurity, risk, and AI governance executive advising boards, CEOs, and leadership teams on cyber resilience, enterprise risk, advanced analytics, and responsible AI adoption.

He is Founder of **NexAI Cyber** and Co-Founder/Board Member of **RYLTI,** an AI-driven digital twin and knowledge engineering company. Previously, he served as President and CEO of Redpoint Cybersecurity and held senior audit and risk leadership roles at Liquidnet, MetLife, Roslyn Bancorp, PaineWebber, and KPMG.

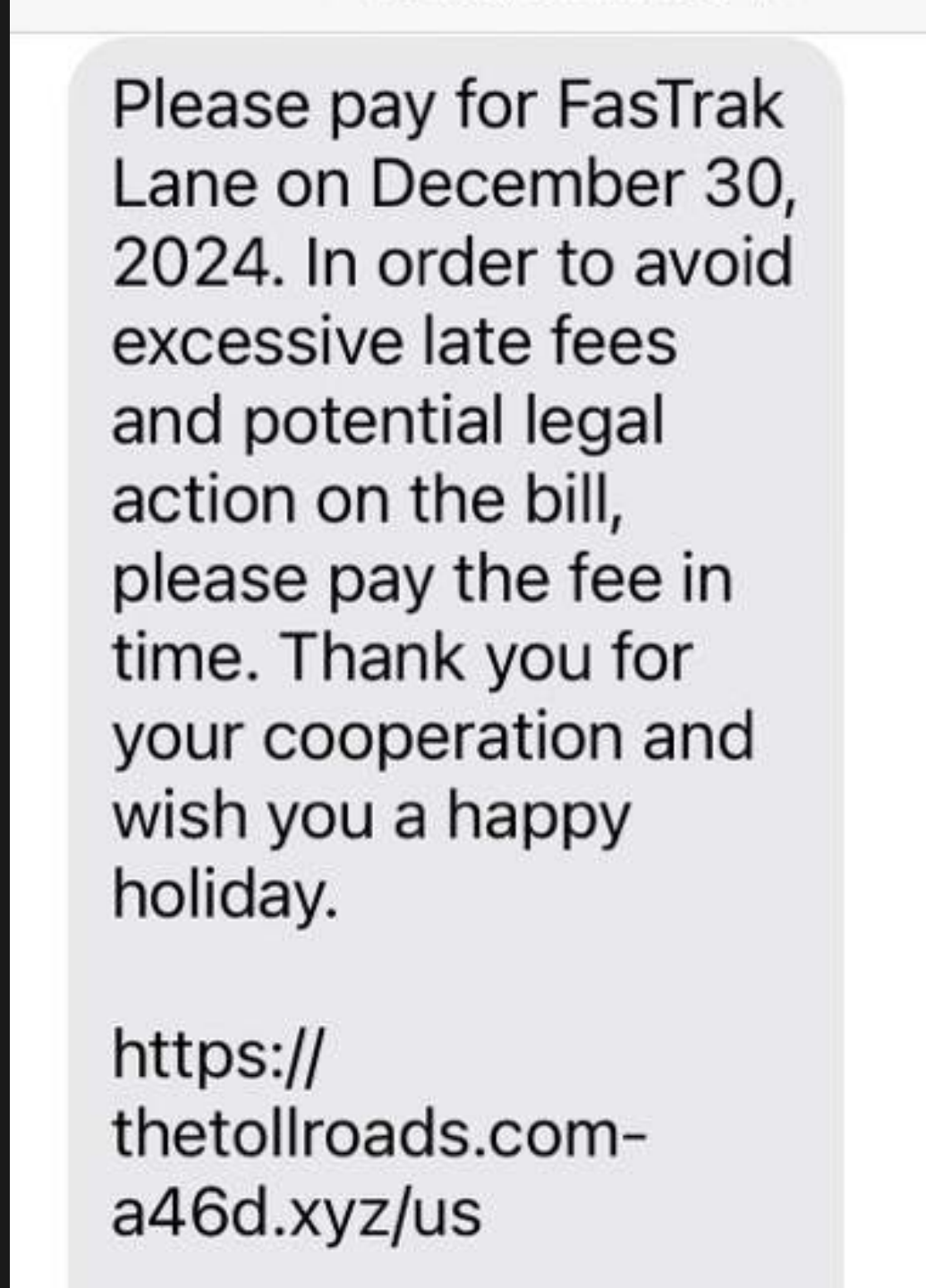
Russell has delivered 40+ keynotes and executive briefings at organizations including the Harvard Club, American Bar Association, AICPA and the Institute of Internal Auditors, focusing on AI governance, cyber resilience, risk intelligence, and the future of audit.He is a licensed CPA and holds several AI based patents.

NEXAI CYBER
Intelligence Secured.

Your highway toll payment is now past due

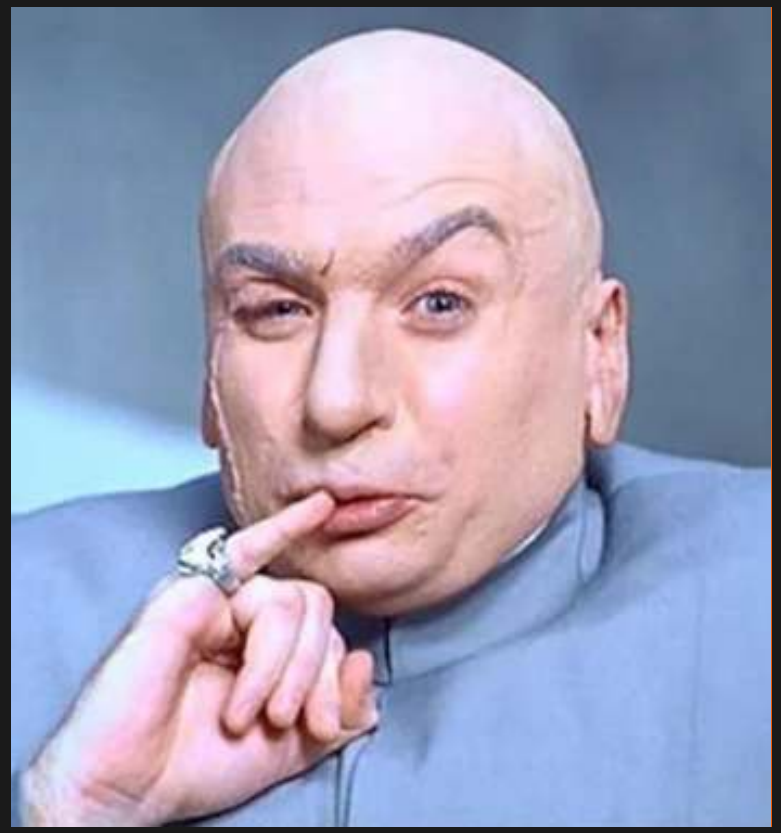
Polling Question #1:

How much do you think Chinese threat actors made from those annoying texts?



This Is What Machine-Scale Crime Looks Like

"This looks like a nuisance text. It is actually an industrialized fraud pipeline."



$1B

Gift Cards

SIM farms

WSJ

NEXAI CYBER Intelligence Secured.

Ransomware Rebounding

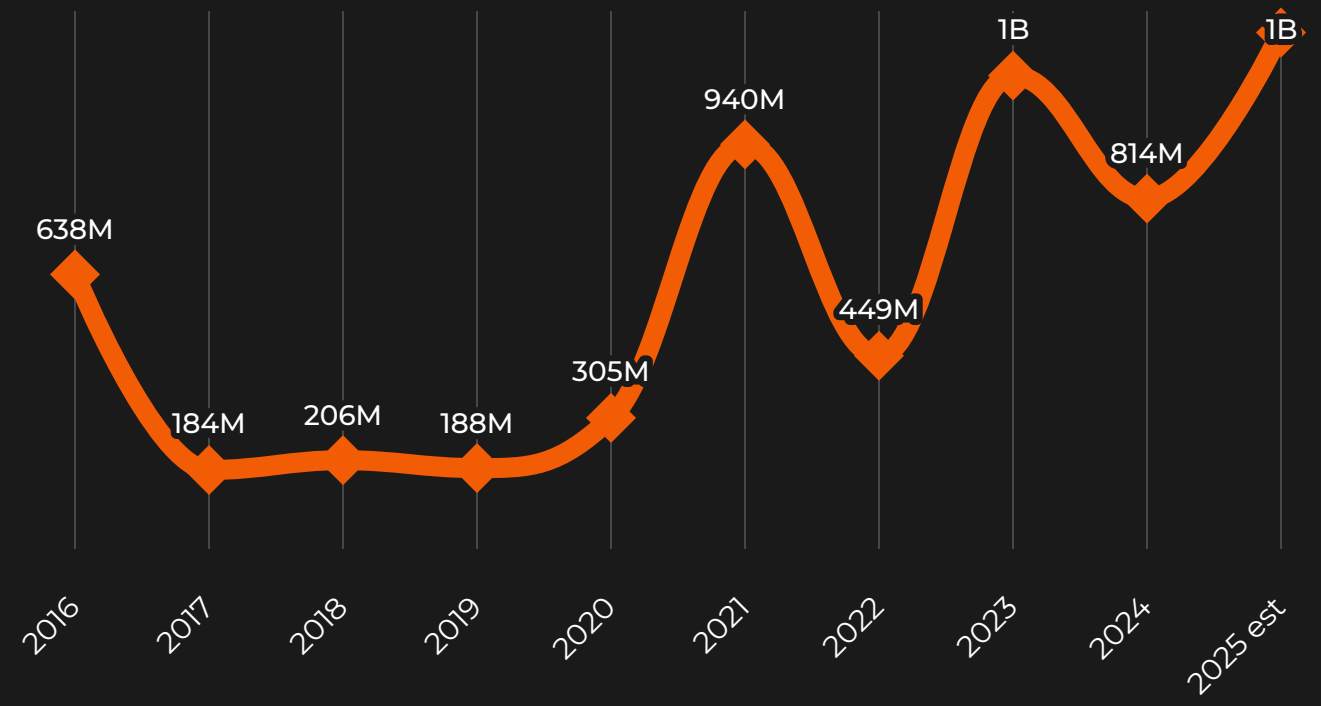
Coalition Insurance's 2025 Cyber Claims Report shows that ransomware claims severity stabilized in 2024, but the threat is resurging in 2025 as avg payment size skyrocketing

Initial attack vectors

- Compromised credentials (47%)
- Software exploits
- Social Engineering

Triple extortion is common

Annual number of ransomware attacks worldwide from 2016 to 2024



The Cyber Gap Has Never Been Wider

Technology alone can’t close the execution gap.

Threat actors move faster than human teams can respond

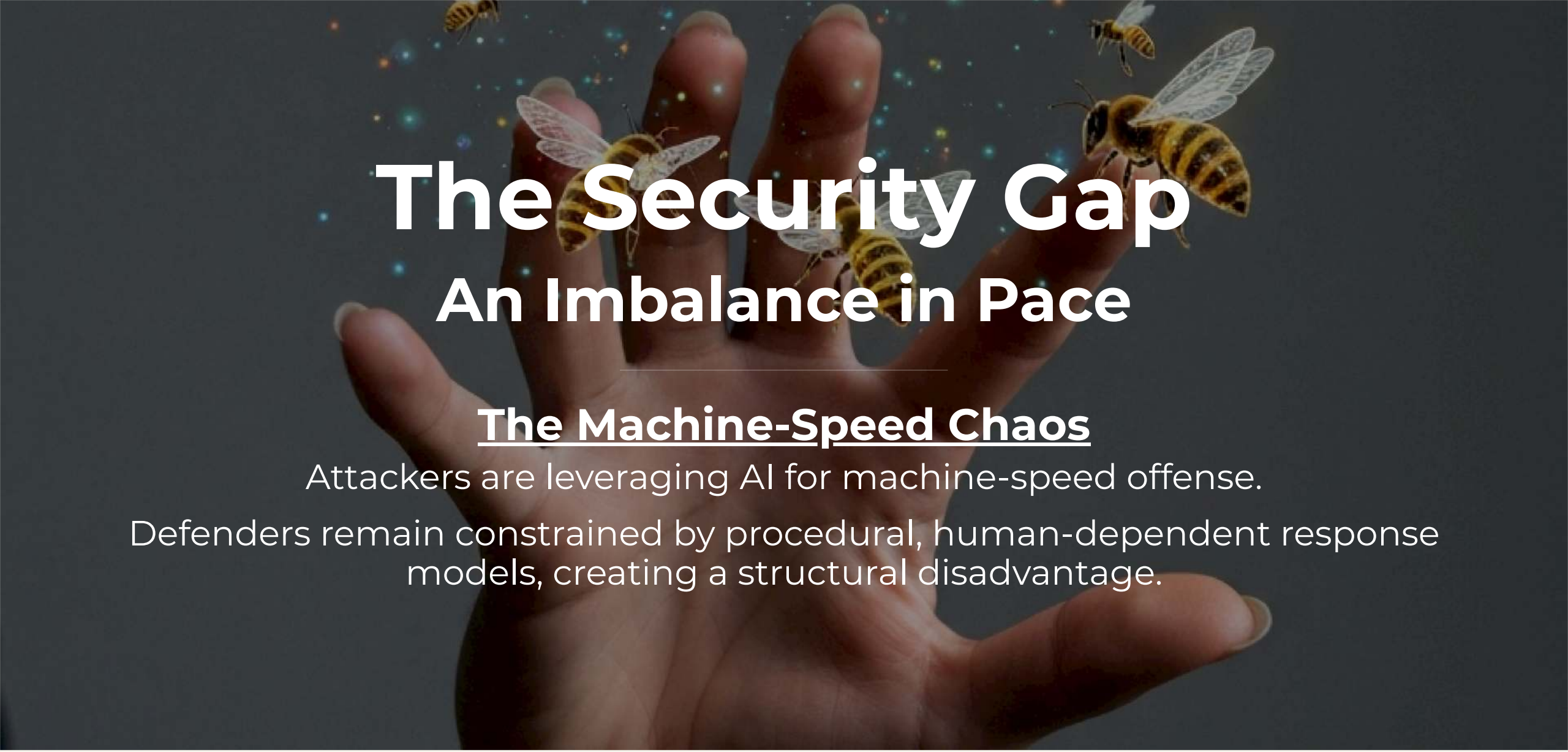
Compliance requirements expand faster than teams can update controls

Boards & insurers now demand continuous evidence

Tool sprawl creates blind spots and inconsistent processes

Global spend on cybersecurity tools rose in 2024, yet breach losses increased in 2025 signaling a widening execution gap.

NEXAI CYBER
Intelligence Secured.



The Security Gap

An Imbalance in Pace

The Machine-Speed Chaos

Attackers are leveraging AI for machine-speed offense.

Defenders remain constrained by procedural, human-dependent response models, creating a structural disadvantage.

HUMAN-SPEED PROCESSES ARE INSUFFICIENT TO COMBAT MACHINE-SPEED PROBLEMS.

Tools Rich Resource Poor Impact Limited

THE CORE ISSUE IS NOT A LACK OF TOOLS, BUT THE INABILITY TO UNDERSTAND, DECIDE, AND ACT QUICKLY ENOUGH IN THE FACE OF AI-DRIVEN ADVERSARY SPEED.

Question

Polling Question #2

What % of companies are experimenting with AI powered security tools?

The Skills Gap Has Become an AI Execution Gap

AI adoption is accelerating faster than governance, accountability, and control.

91%
Using or experimenting with AI-powered security solutions

84%
Say AI security tools improve team efficiency

60%
Say AI-specific security experience is a top recruiting challenge

42%
Would trust AI to handle core security functions independently

FROM: SKILLS GAP
People & Capacity Constrained

- Too few skilled analysts
- High alert & workload
- Slow manual processes

TO: AI EXECUTION GAP
Governance & Control Constrained

- Unclear ownership & accountability
- Policy & control lag behind AI speed
- Limited visibility & auditability

The real issue is not adoption — it is governance, accountability, and control at machine speed.

Source: SecureWorld / Fortinet Training Institute research

Can AI Bridge the Security Gap?

Most organizations possess an overwhelming array of cybersecurity tools.

Despite this extensive toolkit, breaches continue to occur.

Can we understand, decide, and act fast enough when the adversary is operating at machine speed?

NEXAI CYBER
Intelligence Secured.

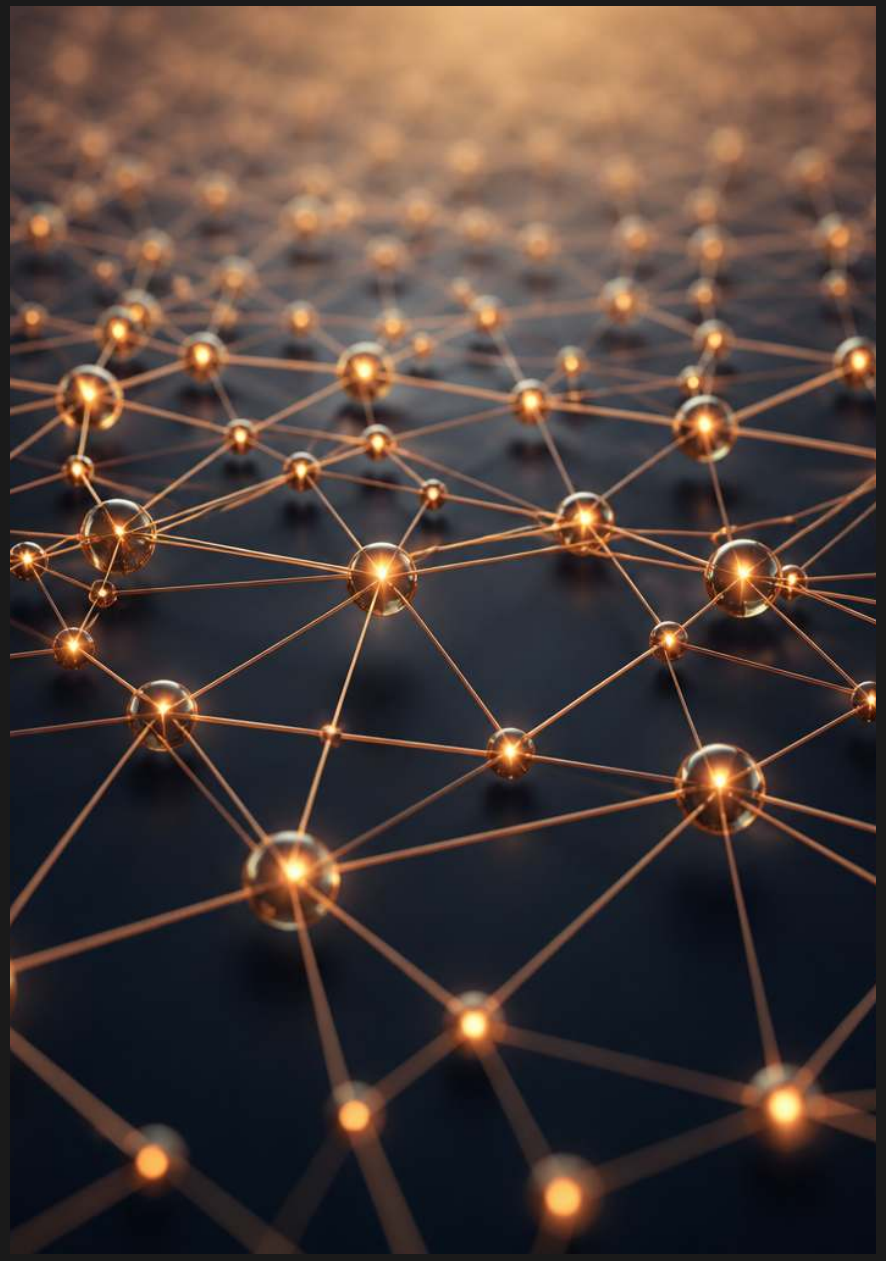
AI works when it creates:

- modeled context
- simulated attack paths
- governed AI response tools
- faster decision loops
- continuous assurance evidence

AI fails when it is:

- another dashboard
- another alert layer
- unmanaged autonomy
- disconnected from identity, controls, and evidence

NEXAI CYBER
Intelligence Secured.



Key Challenges

The New Reality

Scale
Ransomware groups, affiliate ecosystems, fraud networks, and automated campaigns are expanding.

Speed
Breakout time and time-to-exploit are shrinking, compressing the window for defense.

Sophistication
Attackers increasingly combine identity abuse, social engineering, defense evasion, exfiltration, and AI-assisted adaptation.

The breach window is closing faster than traditional workflows can respond.

The Machine-Speed Chaos

The Problem

Attackers use AI for constant reconnaissance, automated exploit pathing, and real-time social engineering, creating a fast-changing threat landscape.

The Symptom

Defenders suffer from "Alert Fatigue" and "Compliance Theater," distracting from real security threats.

The Bottom Line

Human-speed processes are insufficient to combat machine-speed problems.

THE FUNDAMENTAL CHALLENGE IS THAT A MACHINE-SPEED PROBLEM CANNOT BE EFFECTIVELY ADDRESSED BY HUMAN-SPEED PROCESSES.

Modern Attacks Are Compressing the Kill Chain

1

Old Ransomware Model

Initial access → lateral movement → encryption → ransom

2

New Ransomware Model

Recon → credential abuse → defense evasion → exfiltration → leverage → optional encryption

3

What Changed

AI and automation compress discovery, targeting, deception, and exploit testing.

If the attacker compresses the kill chain, the defender must compress the decision cycle.

THE EXECUTION GAP

Execution Gap = signal volume x complexity x adversary speed / decision capacity

Risk increases when adversary speed exceeds decision speed.

Technical Capability

What your current stack is licensed to do. We are over-indexed on tools and under-indexed on the **reasoning layer** that connects them.

Operational Velocity

The actual speed at which your team can triage, isolate, and remediate. This is currently limited by human cognitive bandwidth.

The "Gap" is the playground for the automated adversary.

NEXAI CYBER
Intelligence Secured.

Simplifying Resilience Concepts

Digital Twins, Biomimicry, and Chaos Modeling

Digital Twin

Biomimicry

Chaos Modeling

NEXAI
CYBER
Intelligence Secured.

Biomimetic Digital Twins

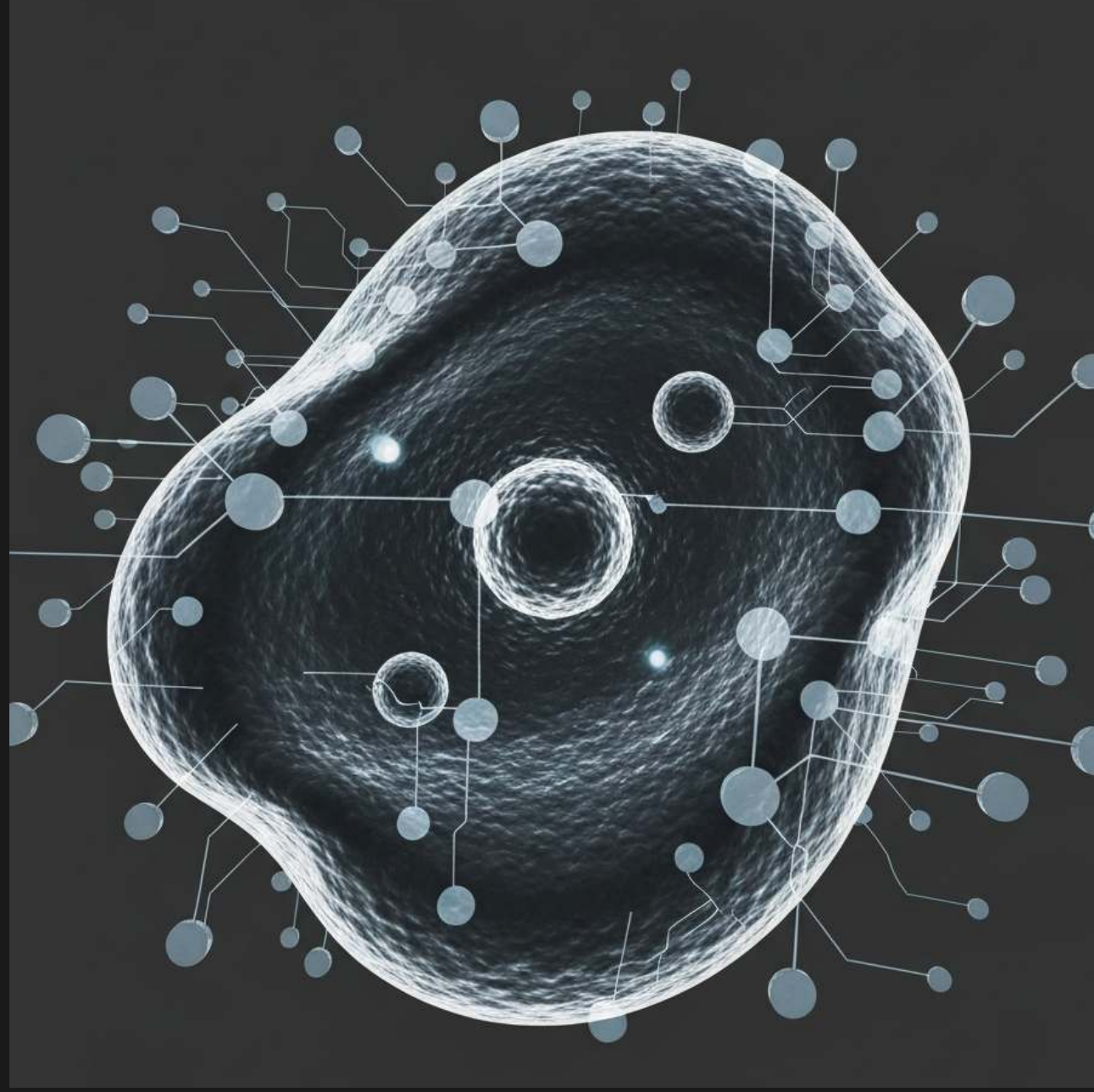
Modeling security after biological resilience.

- **Digital Twin:** A "live" digital twin of your environment that updates continuously based on telemetry.
- **Biomimicry:** Just as an immune system "simulates" threats through memory, the twin maps exposures and lateral movement paths without touching production.

Can simulate 100k+ breach scenarios daily

Identifies emergent lateral movement paths

Creates "immune memory" for AI agents



MOVE FROM "WHAT HAPPENED?" TO "WHAT COULD HAPPEN RIGHT NOW?"

Biomimicry

Modeling Threat Behaviors Like the Brain

- AI Maps
- Interdependent Frameworks
- Modeling Threat Behaviors
- Proactive Threat Detection
- Continuous Improvement

This approach allows for anticipation and mitigation of threats by modeling their interconnected and dynamic nature, ensuring continuous improvement and adaptation to evolving tactics.

Chaos Modeling

Rehearse failure before failure rehearses you - automating cyber incident preparedness

The Approach

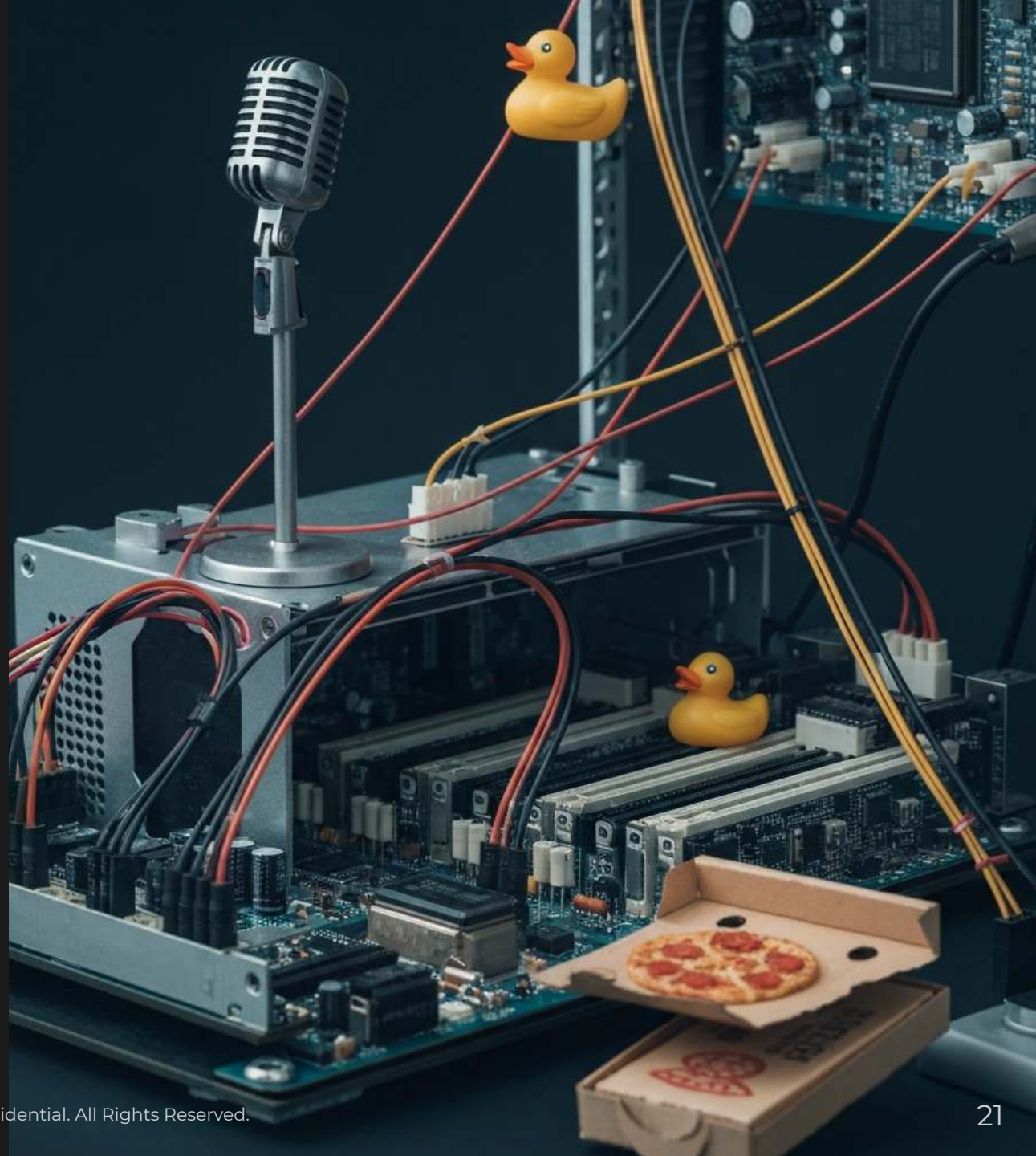
- Automate scenario design, exercise inputs, participant workflows and guided decision making.

Continuous Stress Testing

- Chaos Modeling is a continuous stress test. Make one-time exercises (pen testing, tabletops) repeatable with actions and follow up tracking.

Outcomes

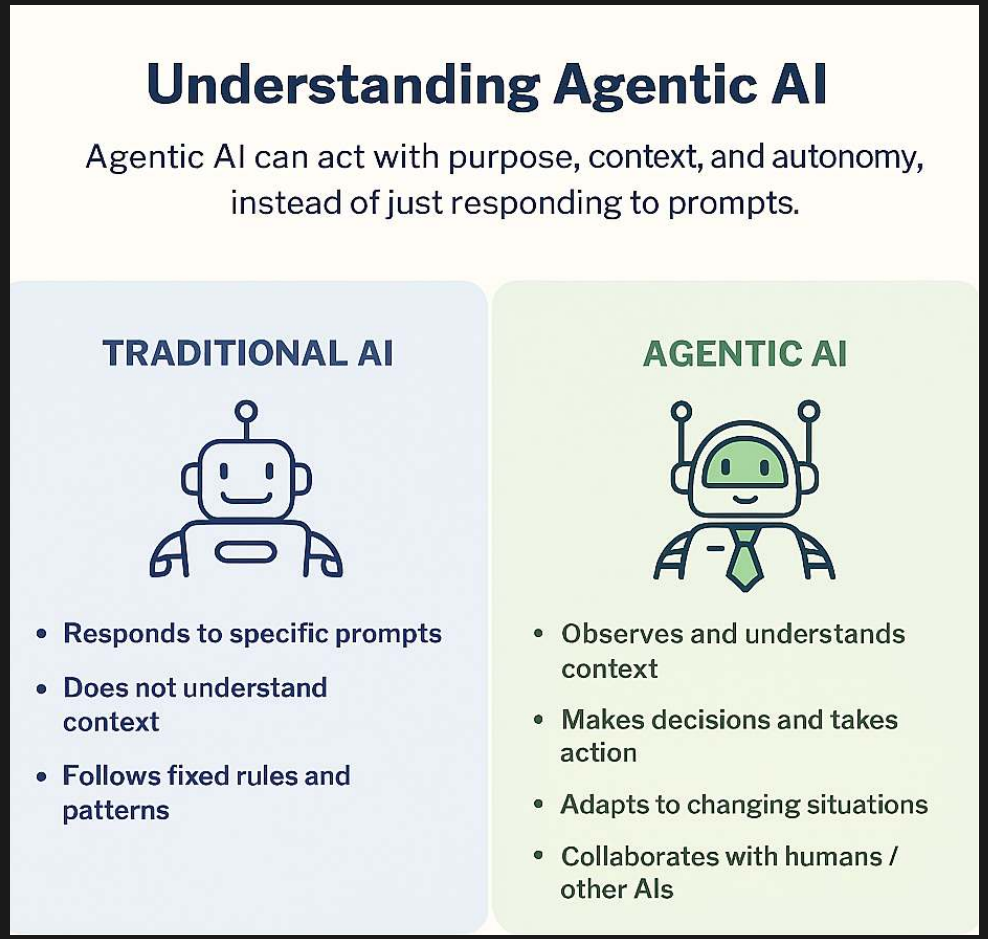
- Identify your "normal" and automate the response to deviations. Ensure readiness.



NEXAI CYBER
Intelligence Secured.

What Is Agentic AI?

- **Agentic AI** refers to systems designed to act more like intelligent agents rather than just passive tools.
- **Goal Oriented and Self Directed**
  - Goal-Directed Behavior
  - Autonomy
  - Adaptability
  - Decision-Making
  - Persistence



NEXAI CYBER
Intelligence Secured.

Polling Question #3

- Can you cook with Agentic AI?

NEXAI CYBER
Intelligence Secured.

Agentic AI - You've Already used it!

Autonomous travel agents

Expedia AI that book travel, reschedule flights, and optimize itineraries based on your preferences.

Robotic systems

Navigate and perform tasks in real-world environments (e.g., Amazon's warehouse robots).

Financial Trading Bots

Operate with goal-directed behavior such as maximizing returns and adapting to market changes.

AI Cooking Assistants

Samsung's Bespoke AI oven suggesting recipes based on food you have in your refrigerator, cooking settings and monitoring food

NEXAI CYBER
Intelligence Secured.

Agentic Execution During a Real SOC Incident

Identity-led attack, cross-domain correlation, policy-bound response

- Atypical login location
- Low-confidence session allowed
- Conditional access not triggered

- Mailbox rule created
- Cloud API access enumerated
- Endpoint token reuse detected

- Goals: Contain identity-led intrusion.
- Policies: Least privilege.

1. Revoke active identity token
2. Isolate lateral endpoint
3. Validate no new cloud roles

- Full action log available
- Decision trace visible
- Override possible at any step

EVERY CONTROL FIRED. THE DIFFERENCE WAS EXECUTION SPEED NOT DETECTION.

Securing Agentic AI Agents

What Auditors Need to Know

Every AI agent is a non-human identity with authority. Treat it like one.

- Understand AI Agent Capabilities
- Implement Secure Communication Protocols
- Establish Comprehensive Monitoring
- Enforce Strict Access Controls
- Implement Fail-Safe Mechanisms

IBM'S 2025 BREACH REPORT EMPHASIZES AN AI OVERSIGHT GAP AND NOTES THAT UNGOVERNED AI SYSTEMS ARE MORE LIKELY TO BE BREACHED AND MORE COSTLY WHEN BREACHED.

The Board Questions Have Changed

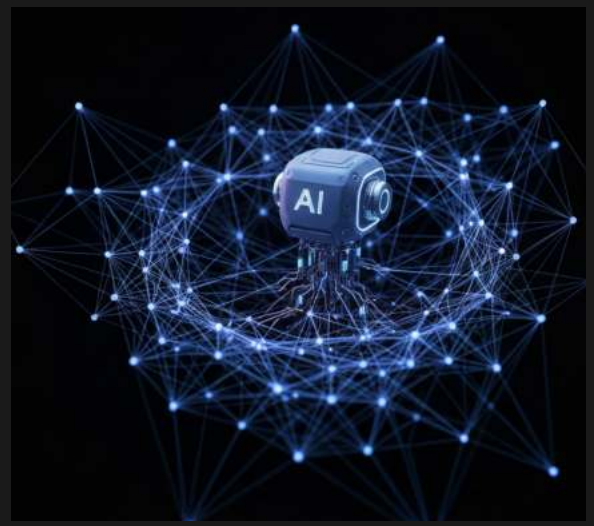
“What tools do we have?”

“Can we detect, decide, contain, and evidence faster than the adversary can adapt?”

The New Asymmetry: AI vs. AI

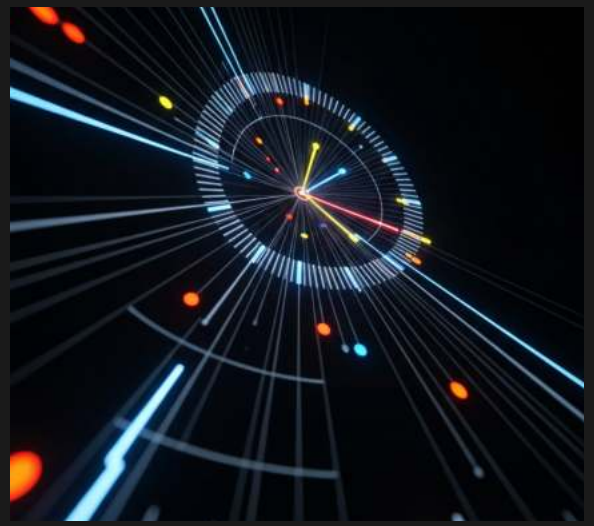
A Shift in Cyber Defense

Attackers



Automate reconnaissance, exploitation, and adaptation using AI.

Defenders



Advantage relies on cycle time, not just tools. Must detect, decide, and respond faster than automated adversaries.

CISO Implication

The core security question: 'Can we detect, decide, and respond faster than automated adversaries?'

Board-Level Risk

Risk exposure compounds silently if security workflows are human-gated.

NEXAI CYBER
Intelligence Secured.

AI Governance Is Now an Operating Requirement

The Governance Gap

- Where is AI being used?
- Which use cases are high risk?
- Who approves new tools, agents, or models?
- What data is being exposed?
- How are outputs monitored, logged, and reviewed?

Business Impact

Cyber risk: data leakage, prompt abuse, insecure integrations

Compliance risk: undocumented use, weak controls, policy gaps

Operational risk: poor outputs, drift, unmanaged automation

Leadership risk: limited visibility for executives, audit, and board stakeholders

AUDITORS MUST MAINTAIN AWARENESS OF IMPLEMENTATION INITIATIVES OCCURRING THROUGHOUT THEIR RESPECTIVE ORGANIZATIONS.

Governed AI Rollout

From Discovery to Ongoing Oversight

Inventory AI tools, copilots, agents, vendors, and use cases.

Outputs: AI inventory, ownership map, data/use-case catalog.

Assess business value, risk, sensitivity, and regulatory impact.

Outputs: Risk tiering, quick wins, high-risk use-case flags.

Define policies, approval workflows, controls, and accountability.

Outputs: Governance framework, control mapping, role ownership.

Support controlled rollout of approved AI use cases and workflows.

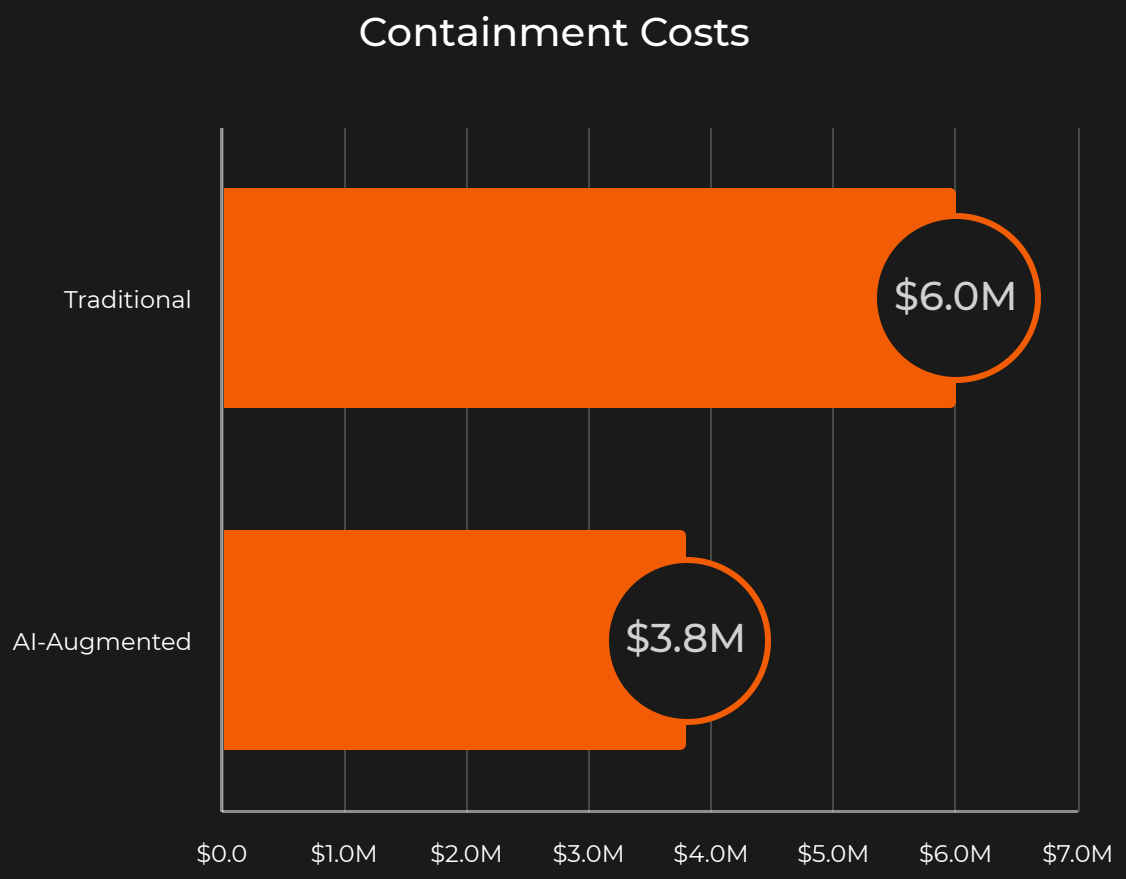
Outputs: Guardrails, deployment review, monitoring requirements.

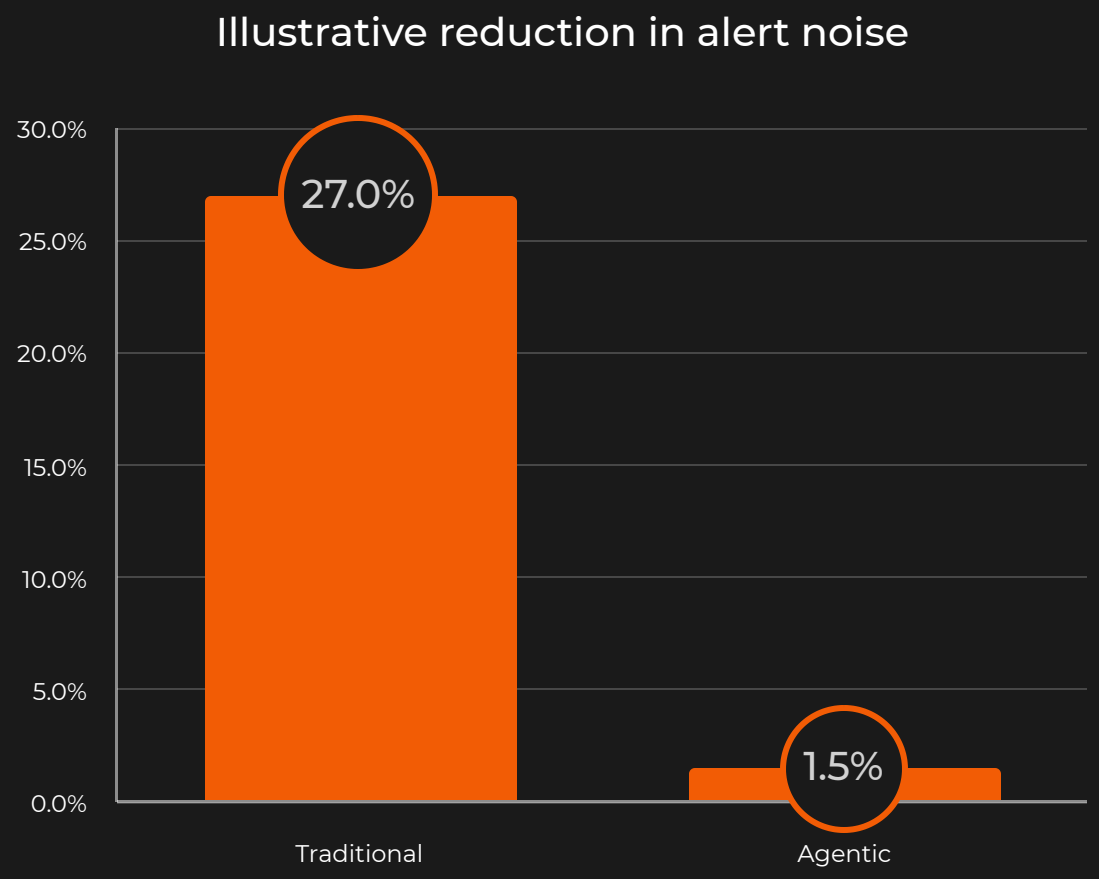
Provide ongoing oversight, reporting, issue escalation, and maturity uplift.

Outputs: Evidence trail, exception tracking, board-ready reporting.

NEXAI CYBER
Intelligence Secured.

The Economics of AI Defense





CISO Executive Briefing: Cybersecurity in 2026

What Changes, What Breaks, What Matters

- In 2026, cybersecurity is no longer a tooling problem, it is a **speed, cognition, and governance problem**.
- AI-powered attackers scale faster than human teams. Defenders that rely on headcount, static controls, or disconnected tools will fall behind.

Winning organizations will:

- Operate agent-driven security workflows
- Treat governance and explainability as first-class controls
- Shift CISOs from “tool buyers” to risk orchestration leaders

NEXAI CYBER
Intelligence Secured.

Closing the Execution Gap

Agentic AI for Cyber Operations

- Autonomous, context-aware agents
- Minimal human supervision
- Digitally replicated knowledge and reasoning

Digital Twins of Risk Posture

- "Always-on" digital twins of business units, endpoints, and networks.
- Digital twins can be stress-tested, modeled, and probed as if under live attack

Chaos Modeling as a Cyber Discovery Engine

- Discover non-linear emergent risks through simulation of attacker paths across controls and assets.
- Model "what the system allows" vs "what the threat actor can do"

NEXAI CYBER
Intelligence Secured.

The Next Cyber Advantage

Not more alerts. Faster, governed understanding.

Model the environment.

Establish a comprehensive understanding of your cyber infrastructure.

Simulate failure.

Test your defenses and response strategies through realistic simulations.

Govern the agents.

Maintain control and compliance over automated cyber defense systems.

Compress the decision cycle.

Accelerate response times for critical security events.

NEXAI CYBER
Intelligence Secured.

What's Next? **The Future of Cybersecurity**

Agentic & Autonomous Defense

Defense must now operate at the speed of AI-driven reconnaissance, exploit chaining, and adaptive attack execution.

Cryptographic Agility

We are now in the migration phase, not just the "thinking about it" phase.

Machine Identity & Shadow AI

The new attack surface is not just devices it is unauthorized AI agents, non-human identities, and ungoverned automation.

Identity & Governance

Prompt injection, model misuse, data leakage, vendor AI risk, and unapproved agents are now core cybersecurity and board-level governance issues.

*"The future is a race of autonomy. Success will be defined by moving from **human-speed** detection to **machine-speed** resilience, where identity is the only verifiable perimeter."*

Any questions?

NexAI Cyber: Human Intelligence Meets AI-Driven Resilience

- **Human-Led Precision:** NexAI Cyber integrates human intelligence with AI-driven resilience to deliver precision in all engagements.
- **Extensive Expertise:** Backed by experience from over 2,000 incident response engagements, NexAI Cyber brings valuable learnings to its clients.
- **Modernized Security & Operational Resilience:** NexAI Cyber empowers clients to modernize their security posture and build lasting operational resilience.
- **AI in Cybersecurity:** NexAI Cyber leverages AI to enhance threat detection, automate responses, and identify patterns at speeds beyond human capability.

NEXAI
CYBER
Intelligence Secured.

RYLTI

Biomimicry of Human Abstract Thinking

A New Class of Cognitive Computing

Modeled after how humans think abstractly, contextually, and dynamically. Our patent pending methodology is currently the only one that truly computes meaning, not just data

Human Abstract Thinking	RYLTI Platform Parallel
Humans connect patterns across intuition experience, and context	RYLTI connects, data, logic, and context through dynamic ontologies
We form conceptual frameworks to understand complex problems	RYLTI models thru Purpose, Theory of Value, & Relevance frameworks
We reason through analogy, synthesis, and reflection	RYLTI's biomimetic engine dynamically assembles relationships & tests scenarios
Our thinking adapts as new information reshapes understanding	RYLTI's engine dynamically adapts to new inputs for exploration without retraining

Thank You

Russell Safirstein, President & CEO, NexAI Cyber

russell@nexaicyber.com

516.551.5546

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter