



JUNE 2025

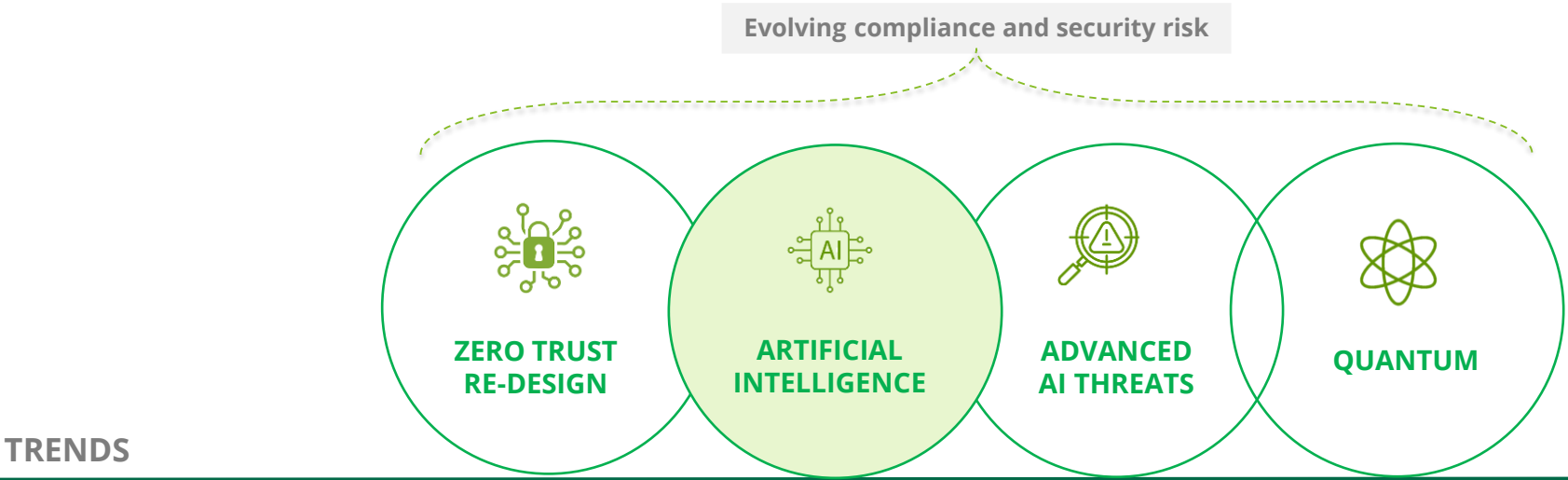
# Reimagining the modern cyber organization

DON'T JUST DEFEND WHEN THE RULES OF THE GAME ARE CHANGING



Rapid technology change is

# Creating the opportunity to reimagine how modern Cyber organizations function



**TRENDS**

**IMPACTS**

**RELATED CYBER CHANGES**

- |  |   |  |   |  |
|--|---|--|---|--|
| <ul style="list-style-type: none"><li>• Re-architecture, re-platforming</li><li>• Technology refresh and up-skilling</li></ul> | <ul style="list-style-type: none"><li>• Redefine controls and testing</li><li>• Redesign of control assessments</li></ul> | <ul style="list-style-type: none"><li>• System discovery and remediation</li><li>• Tech-replacement and migrations</li></ul> | <ul style="list-style-type: none"><li>• Faster detection and response</li><li>• More advanced AI detection technology</li></ul> | <ul style="list-style-type: none"><li>• AI augmentation of human FTE</li><li>• Adoption/ redesign of operations to benefit from AI</li></ul> |
|--|---|--|---|--|

**BUSINESS IMPACT**

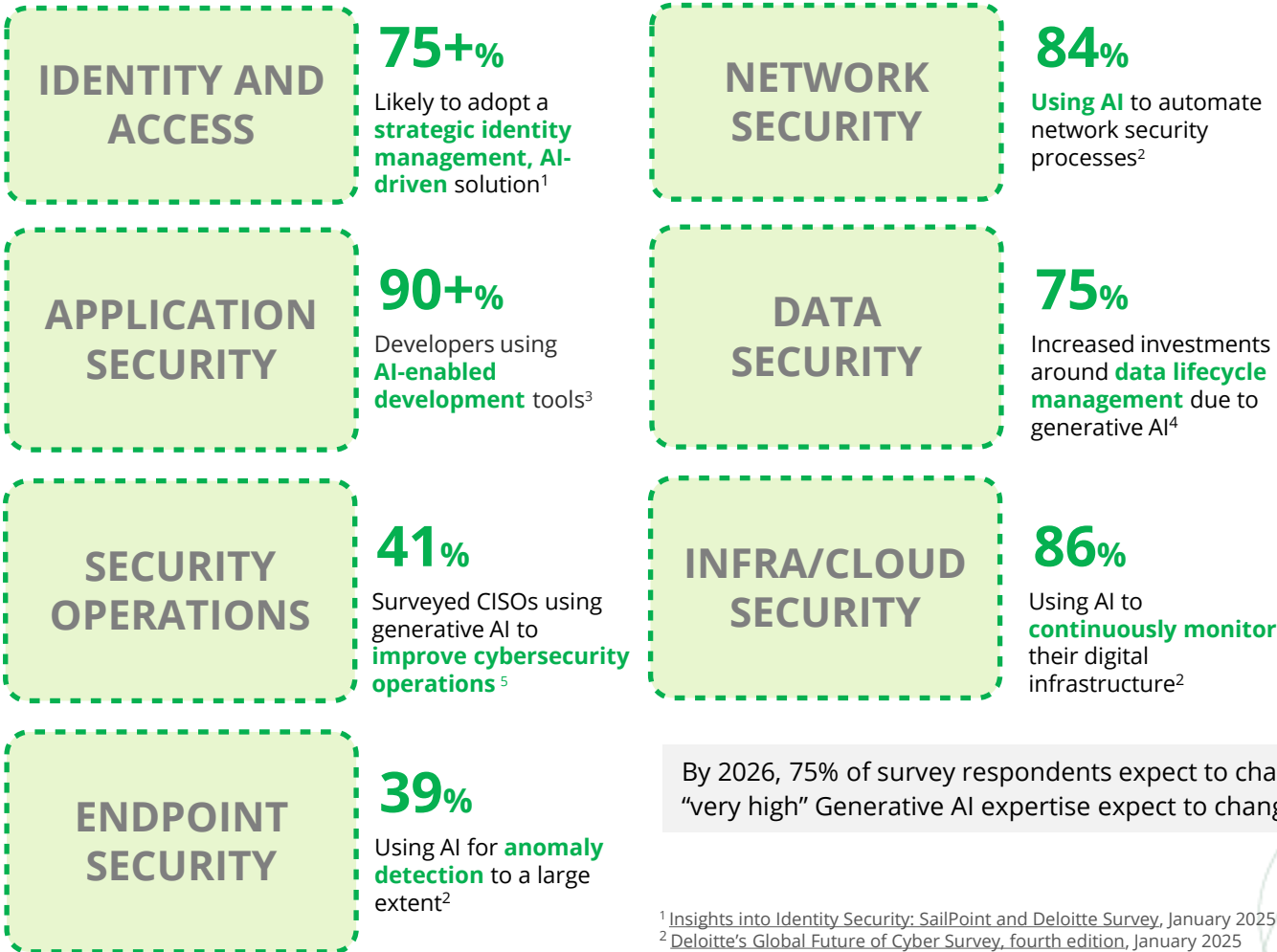
- |   |   |  |  |   |
|---|---|--|--|---|
| Significant redesign of technology and operations | Increasing process complexity and manual effort | Security exposure and system integration risks | Increasing security fatigue and cyber exposure | Revised tech architecture, workforce, and operating model |
|---|---|--|--|---|

**TAKEAWAY: DON'T JUST DEFEND, ADAPT AND TRANSFORM**

- ✓ The Cyber organization of the future will be very different from today
- ✓ CISOs need to start early to harness the benefits and the opportunity

# Across cyber capabilities, the work can be refactored and reimaged

Combining commercial, customized, and home-grown AI solutions, the opportunity is significant



**+50% of the work delivered today can either be augmented by AI or redefined**

By 2026, 75% of survey respondents expect to change their talent strategies in response to Generative AI. Organizations reporting “very high” Generative AI expertise expect to change their talent strategies even faster, with 32% already making changes.<sup>6</sup>

<sup>1</sup> Insights into Identity Security: SailPoint and Deloitte Survey, January 2025

<sup>2</sup> Deloitte's Global Future of Cyber Survey, fourth edition, January 2025

<sup>3</sup> Jessica Ji, Jenny Jun, Maggie Wu, and Rebecca Gelles, "Cybersecurity Risks of AI-Generated Code" (Center for Security and Emerging Technology, November 2024). <https://doi.org/10.51593/2023CA010>

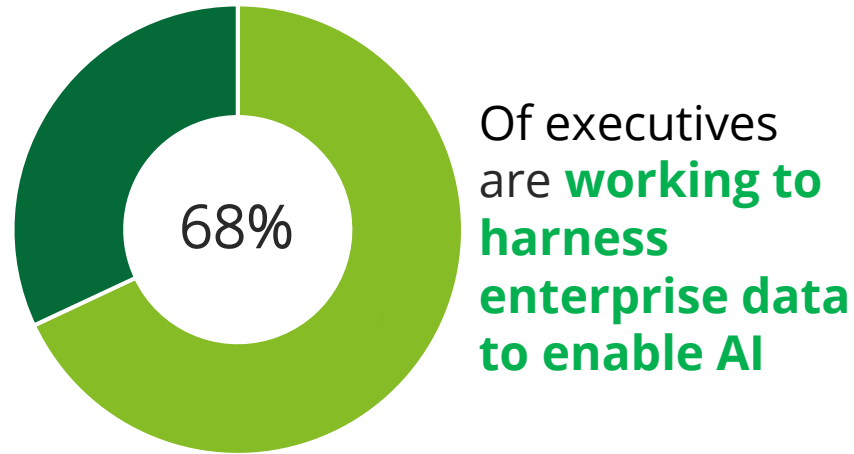
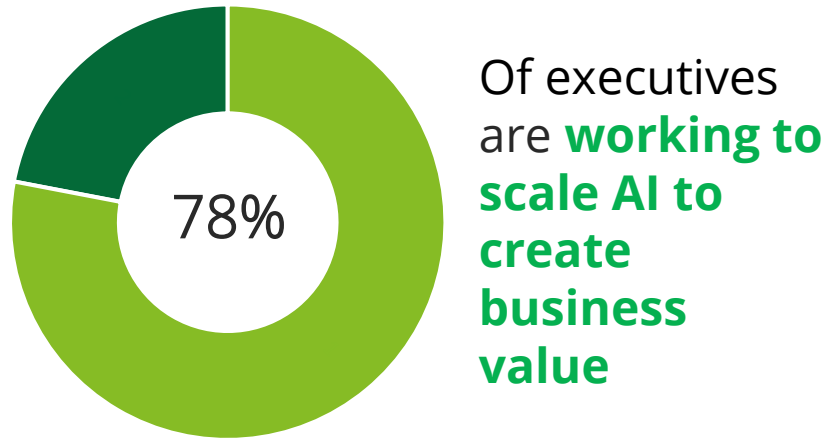
<sup>4</sup> Now decides next: Moving from potential to performance, August 2024

<sup>5</sup> 2024 Deloitte-NASCIO Cybersecurity Study, September 2024

<sup>6</sup> State of Generative AI in the Enterprise, April 2024

# It's not just a cyber imperative, it's a broader business imperative

Cyber leaders have a responsibility and **opportunity to harness the momentum**



## +90% of how cyber security is delivered will be different in the next 5-10 years

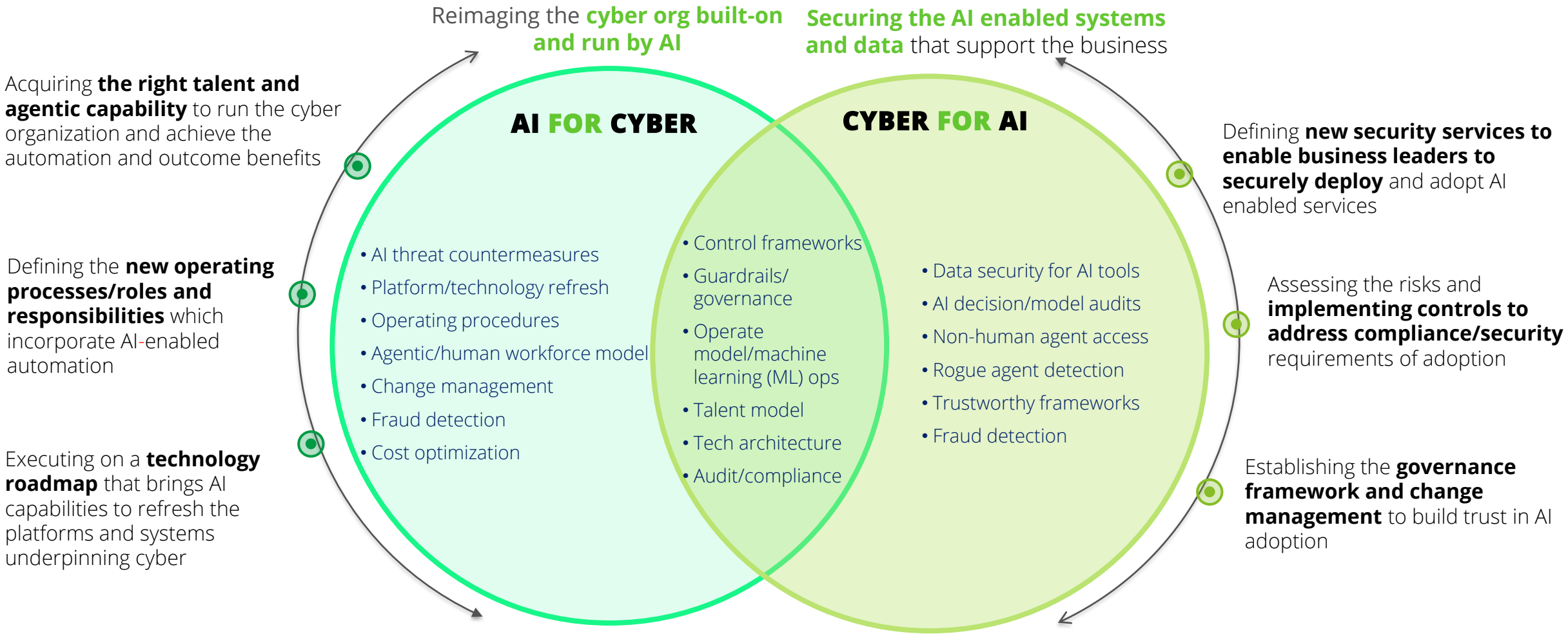
*"In the next five to ten years we will see how quickly we can adapt, and companies that fail to adapt, no matter how big, are going to disappear."*

Noriko Rzonca, Chief Digital Officer, Cosmo Energy Holdings

- When business depends on the AI and IP at the core, protecting it is everything.
- Organizations should implement integrated governance models, guardrails and trust frameworks to enable AI, and cybersecurity teams will own these responsibilities

# Security organizations have to both secure AI systems and reimagine how Cyber runs on AI

Scaling AI requires lots of data, system integration, guardrails, and controls to enable outputs that are trustworthy leaders have a responsibility and **opportunity to harness the momentum**



Reinventing how cybersecurity works in an AI-powered organization

# AI-driven attacks will require new strategies and tactics leveraging AI countermeasures

The landscape of threats will evolve by learning from past attacks and using this input to drive future success

## AI ATTACKS

Deep Fake Impersonation

**Personalized Phishing**

AI Social Engineering

**FraudGPT**

**Brute Force Attacks**

AI-enabled password cracking

Credential Harvesting

Disinformation Campaigns

## COUNTERMEASURES

**Intelligent Threat Monitoring**

Human AI Synergy

**AI Phishing Filters**

Continuous Identity Proofing

AI Attack Modeling/Simulation

Moving target defense

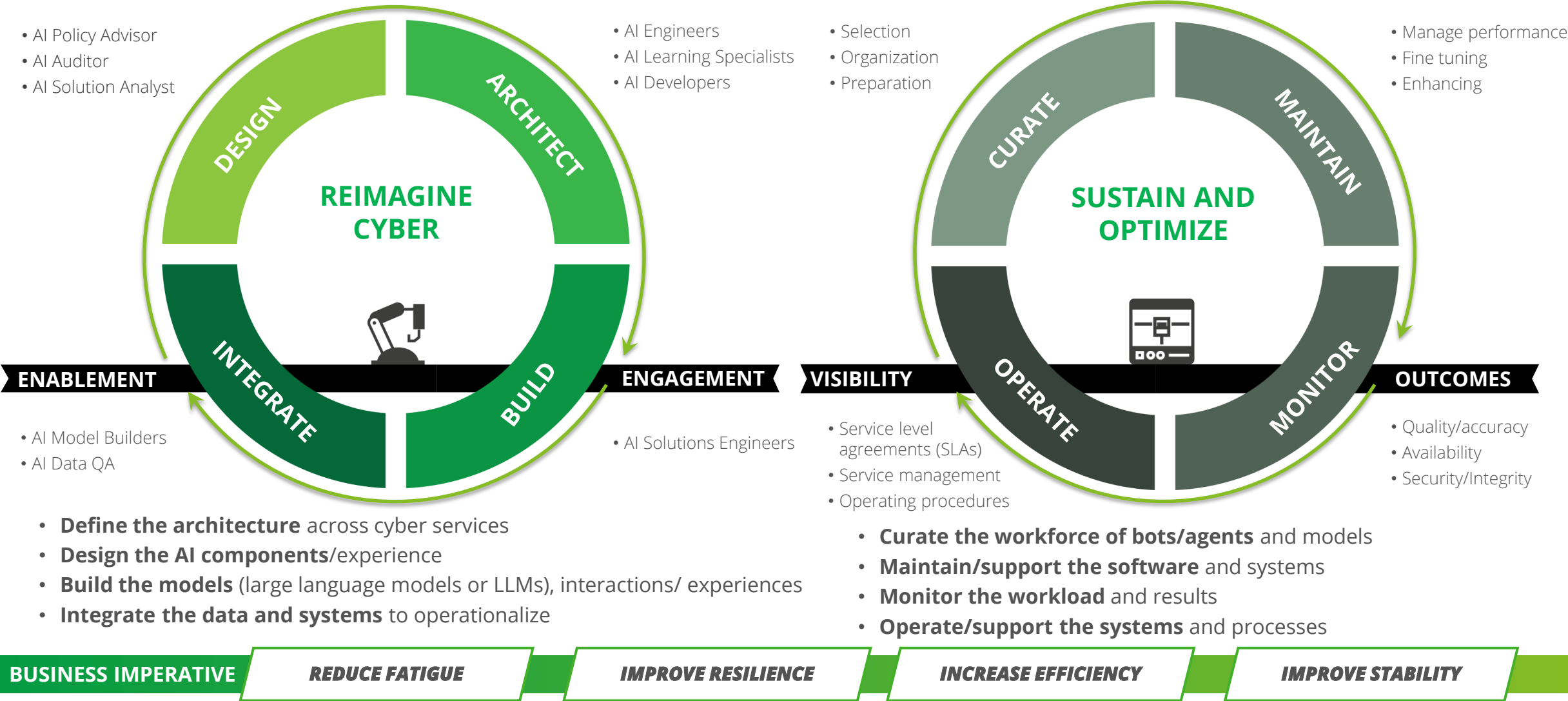
**AI Automated Threat Management**

**Behavior Analytics**

On the new cyber frontier, AI will shape the delivery and increasing sophistication of attacks and the counter measures

# Organizations need a blueprint to combine agentic AI and Generative AI (GenAI) with physical full-time equivalents (FTEs) to create results

The modern organization will need new skills/talent and operations teams to sustain and drive outcomes



# The blueprint is designed to accelerate the journey to reshaping the cyber organization

Components of the blueprint include a workforce structure, technology architecture, operating model, and governance

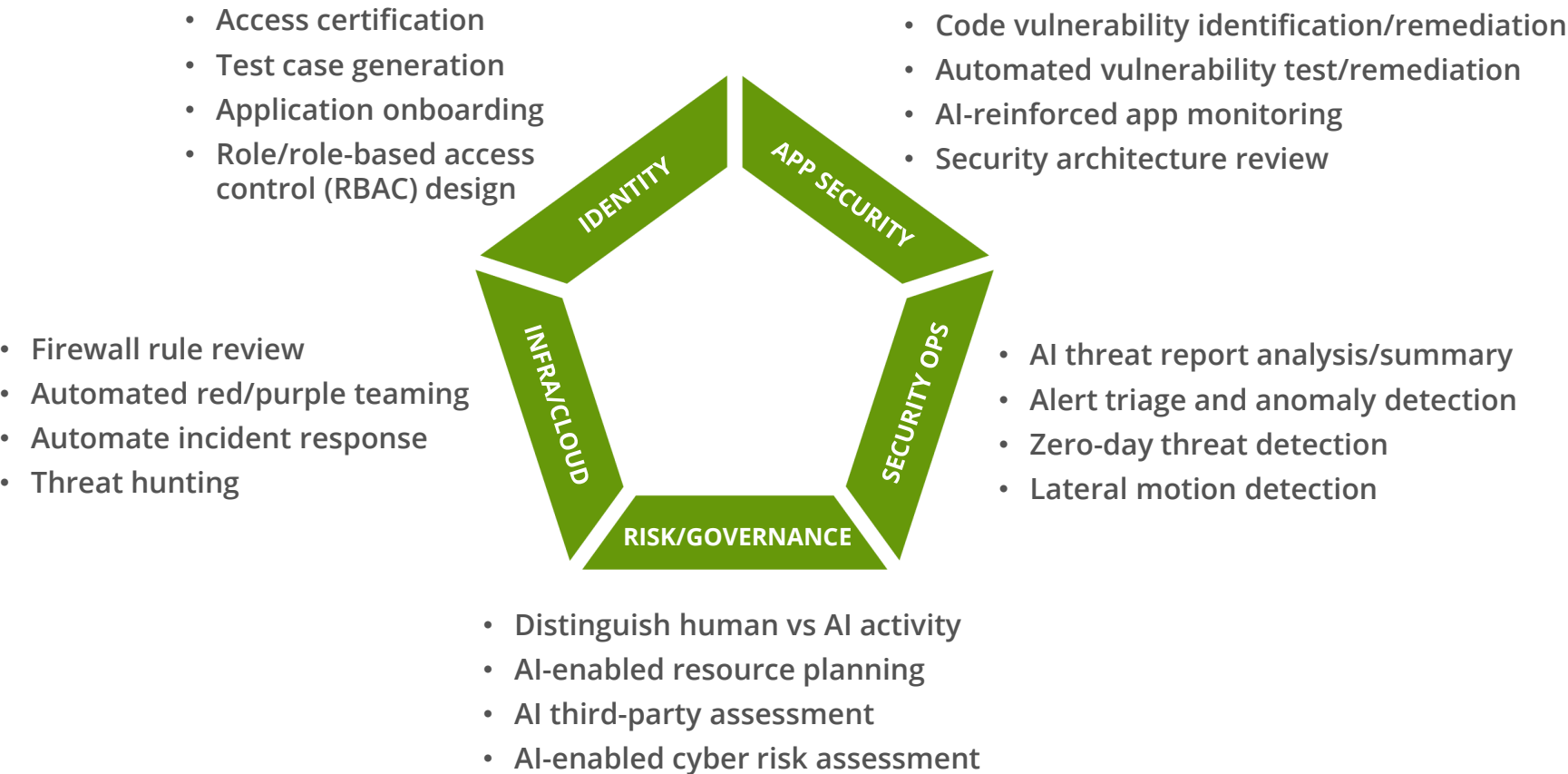
<b>WORKFORCE DESIGN</b>	Agentic AI patterns and capabilities combined with human interaction	<ul style="list-style-type: none"><li>• Skills and roles</li><li>• AI inclusion approach</li></ul>	<ul style="list-style-type: none"><li>• Change management</li><li>• Training and enablement</li></ul>
<b>TECHNOLOGY ARCHITECTURE</b>	Aligning the capabilities needed to deliver on business outcomes	<ul style="list-style-type: none"><li>• Technology choices</li><li>• Selection and comparison</li></ul>	<ul style="list-style-type: none"><li>• Roadmap</li><li>• Timeline and plan</li></ul>
<b>OPERATING MODEL</b>	Establishing the operating processes, practices and responsibilities, and cost optimization	<ul style="list-style-type: none"><li>• Operational assessment</li><li>• Technology enablement</li></ul>	<ul style="list-style-type: none"><li>• Operating procedures</li><li>• Organization structure</li></ul>
<b>GOVERNANCE MODEL</b>	Business case, roles, and responsibilities to drive the execution	<ul style="list-style-type: none"><li>• Governance structure</li><li>• Business alignment</li></ul>	<ul style="list-style-type: none"><li>• Agent operations</li><li>• Trustworthy AI™ framework</li></ul>

**The blueprint establishes a north-star to help reimagine the cyber organization**



# A few examples reshaping the cyber operating model and economic potential

Reshaping the organization is a “ground up” understanding of core assumptions against business requirements across cyber and how the organization can get better results



**ADOPT AI CYBER PRACTICES**

**AI THREAT  
SIMULATION**

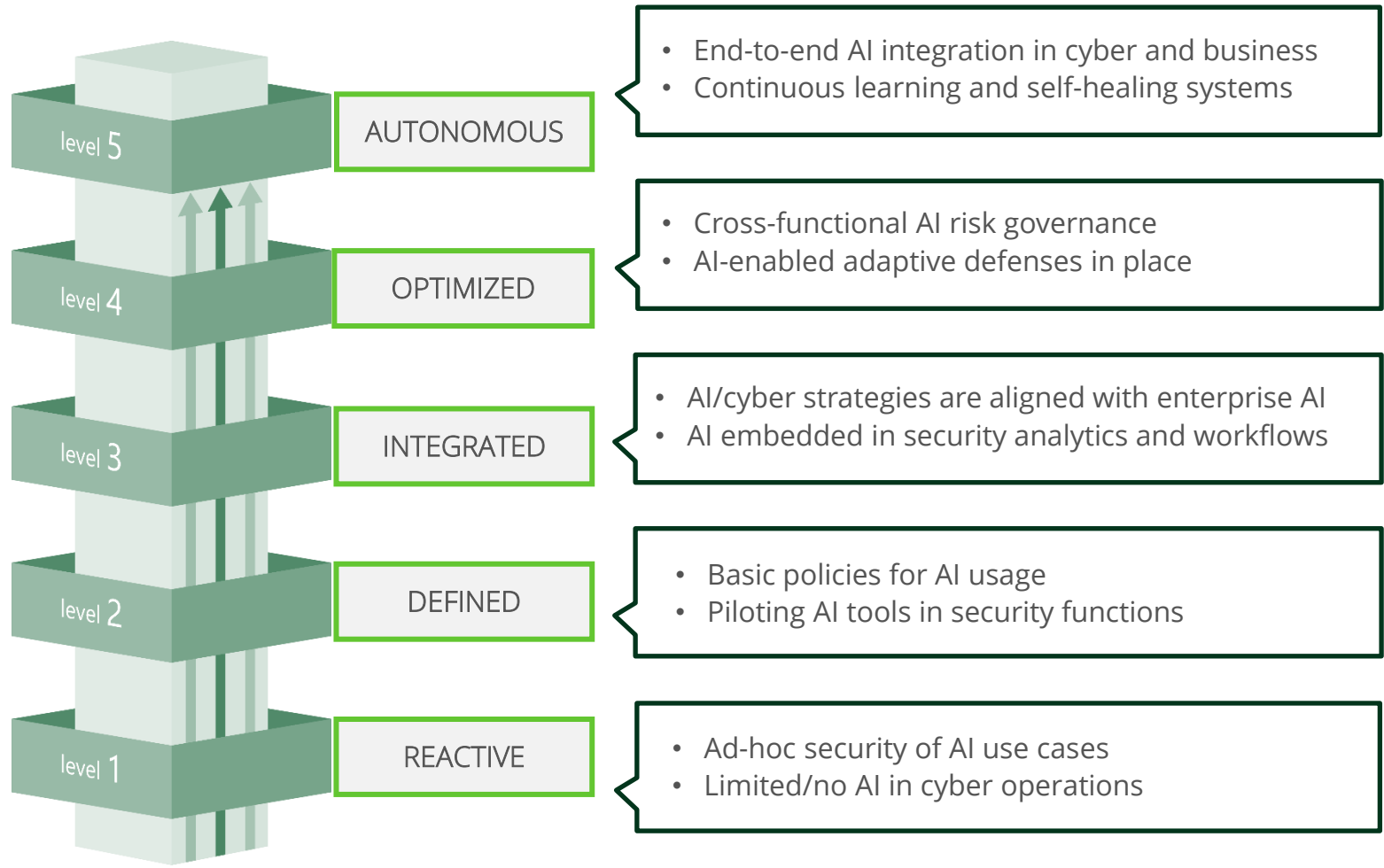
**AI AUTOMATED  
THREAT MANAGEMENT**

**SYNTHETIC DATA  
GENERATION**

**PRE-EMPTIVE/MOVING  
TARGET DEFENSE**

# The blueprint supports the maturity model to help the cyber organization evolve

Using operational discipline and incidents to establish a learning motion to drive greater maturity and resilience

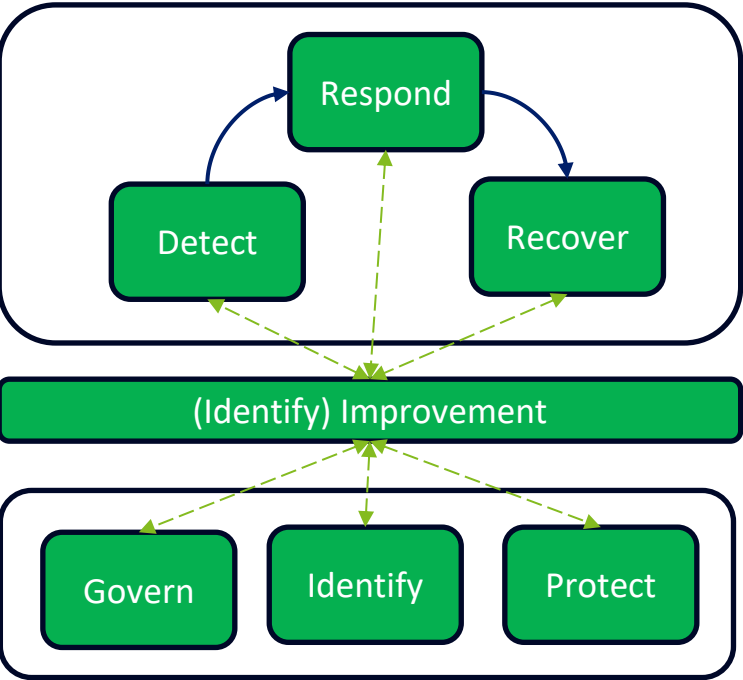


**Create the maturity,  
manage the risk  
reduction, and  
achieve efficiency  
gains aligned with  
industry leading  
practices**

# Example: Reimagining the National Institute of Standards and Technology (NIST) incident response framework in an augmented agentic model

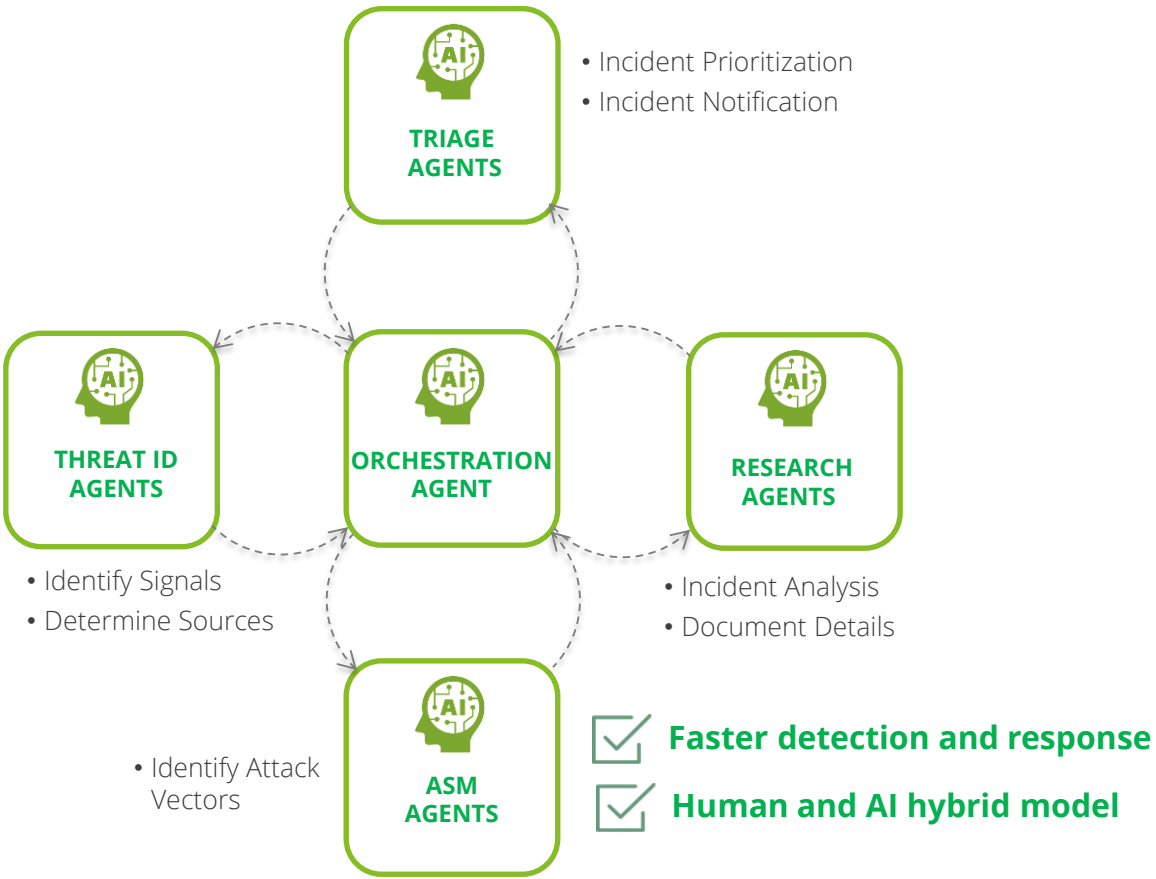
By taking an agentic approach, fatigue can be reduced, quality improved, and better talent leverage can be created

NIST INCIDENCE RESPONSE FRAMEWORK



80%+ human executed

INCIDENT RESPONSE AGENTIC AI MODEL



80%+ AI executed

# Case study: A large health insurance provider reimagining the cyber organization

By taking an AI-driven approach, the client wanted to drastically redesign the cyber function while improving services

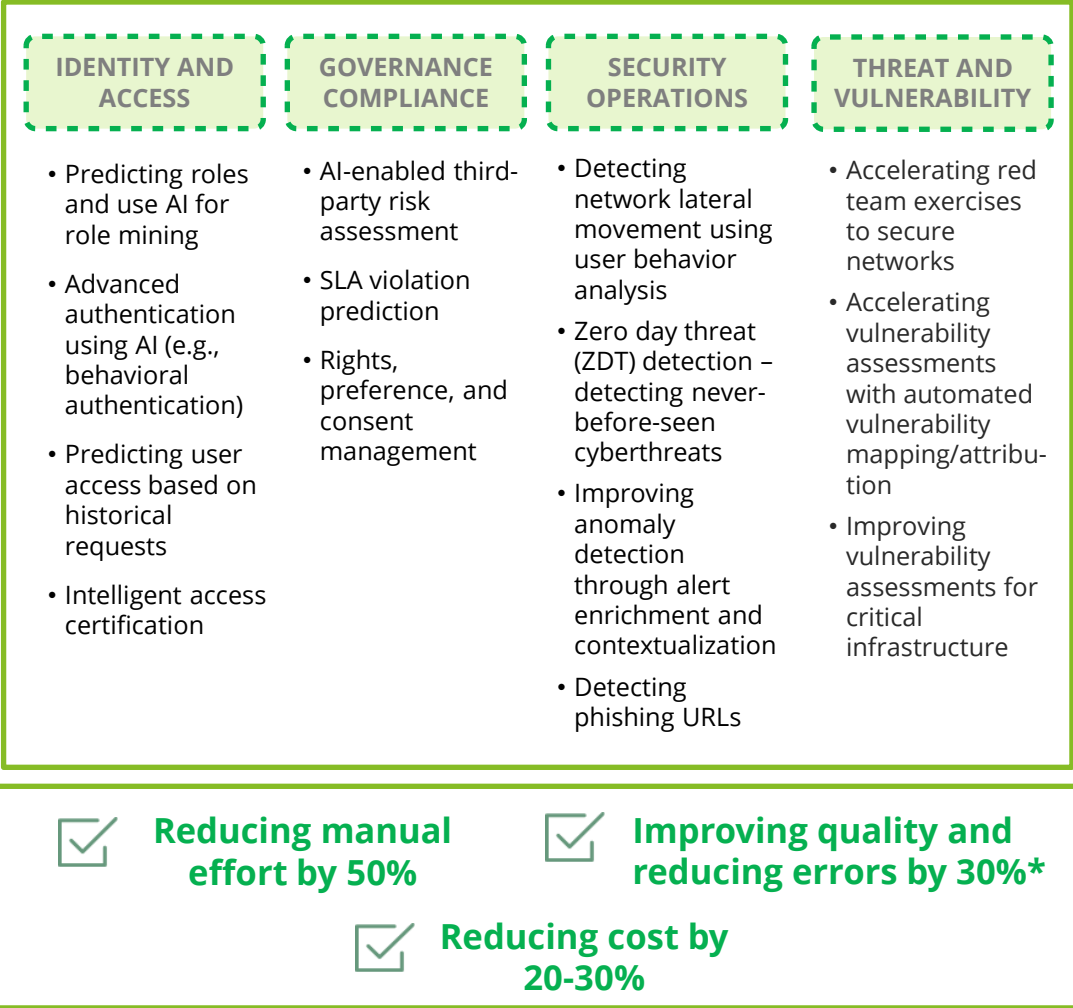
## KEY CHALLENGES:

- Security fatigue and staff turnover
- Audit exposure and lack of visibility and reporting
- Heavily manual security processes and low quality of results

## APPROACH:

Focused effort on key pillars of cyber with the biggest cost and opportunity for AI-inclusion and benefits



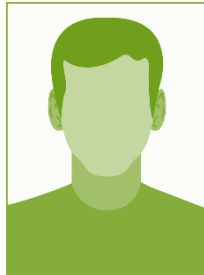



### A CROSS PILLAR CYBER TRANSFORMATION/BLEUPRINT



\* Actual savings may vary based on individual facts and circumstances

Cyber will not be the only organization on the journey:

# Cyber teams will need to align with a broad set of organizational stakeholders

					
<b>CEO</b>	<b>CMO/CDO</b>	<b>CIO</b>	<b>CPO</b>	<b>CFO</b>	<b>CHRO</b>
<ul style="list-style-type: none"><li>• Cost efficiency</li><li>• Competitive advantage</li></ul>	<ul style="list-style-type: none"><li>• Brand and reputation</li><li>• Privacy and customer security</li></ul>	<ul style="list-style-type: none"><li>• Technology arbitrage and modernization</li><li>• Business alignment and efficiency</li></ul>	<ul style="list-style-type: none"><li>• Privacy/security of AI data Models</li><li>• Consent and preference management.</li></ul>	<ul style="list-style-type: none"><li>• Operating cost and efficiency</li><li>• Technology cost and cost containment</li></ul>	<ul style="list-style-type: none"><li>• Talent experience and productivity</li><li>• AI enablement, upskilling and augmentation</li></ul>

----- **KEY CONCERNS** -----

**TAKEAWAY: DON'T JUST DEFEND, HARNESS THE ORGANZATIONAL MOMENTUM**

- ✓ Connect cyber to the broader organization transformation
- ✓ Embed cyber in every area of the business

# Take the “fast lane” to accelerate your cyber transformation journey

We can help define your AI-powered cyber roadmap, implement the capabilities needed, and manage/operate to maturity

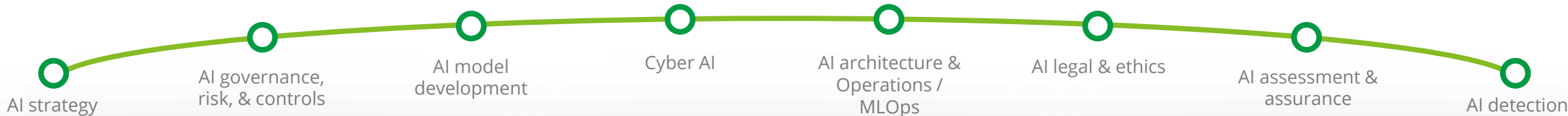
	1 DEFINE A STRATEGY AND ROADMAP TO THE CYBER ORG OF THE FUTURE	2 IMPLEMENT/BUILD THE CAPABILITIES AND SOLUTIONS TO TRANSFORM	3 MANAGE/OPERATE THE PROGRAM TO ACHIEVE LONG TERM MATURITY AND RESULTS
SERVICES	<ul style="list-style-type: none"><li>• AI readiness assessment</li><li>• AI cyber strategy</li><li>• Technology roadmap/selection</li><li>• Modernization business case</li></ul>	<ul style="list-style-type: none"><li>• AI/ML development/ML Ops</li><li>• System integration &amp; data science</li><li>• AI tuning and prompt engineering</li><li>• Technology implementation</li></ul>	<ul style="list-style-type: none"><li>• Support and SLAs</li><li>• Level 3 engineering and development</li><li>• Solution management and governance</li><li>• Governance and change management</li></ul>
ACCELERATORS	<ul style="list-style-type: none"><li>• AI-enabled cyber risk assessment</li><li>• Workforce analysis tools</li><li>• Capability/maturity framework</li><li>• Use case repositories</li></ul>	<ul style="list-style-type: none"><li>• Blueprints to reimagine cyber</li><li>• Pre-built AI enabled use cases</li><li>• Reference architecture</li><li>• AI methodology/accelerators</li></ul>	<ul style="list-style-type: none"><li>• Operating models/procedures</li><li>• Trustworthy AI frameworks</li><li>• Governance models</li><li>• AI quality and automation tools</li></ul>



# Deloitte is well-positioned to help cyber organizations reimagine the future

We assist our clients on their AI adoption journeys and embed AI across our solutions to bring data-driven insights, efficiencies, and performance through cutting-edge research

Breadth of experience across AI strategy, operations and risk needs



## AI ACCELERATORS

### Ecosystem

We have strategic relationships across technology vendors, start-ups, and academia to understand the most complex industry and domain issues.

### Responsible & Ethical AI

Deloitte's Trustworthy AI™ framework and methodologies enable risk-informed development and adoption of AI

### AI Platform

Kubernetes-based AI Platform that supports AI developments and Deep Learning at scale

## SPECIALIZED AI/ML TALENT

Amongst a global AI presence of 6000+ practitioners, our AI research hub, the AI Center of Excellence (AI CoE), consists of specialized AI talent with deep technical skills

Computer Vision

Image Processing

Natural Language Processing

Time Series Analysis

100+

AI Specialists

15  
PhDs

58  
Masters

We help clients conceptualize, design, and operationalize AI-enabled insights and services

ML Engineers

Data Engineers

Platform Engineers

Prompt Engineers

AI Strategists

AI Trust & Ethics Specialists

## AI THOUGHT LEADER

### Publications & Eminence

9 Peer Reviewed Scientific Journals

Industry Conference Presentations at RSA, NVIDIA GTC, Robust Intelligence, AI Summit

Collaboration on AI Perspectives with Harvard Business Review and Wall Street Journal

### Awards and Recognition

1<sup>st</sup> Place in 2 of 4 categories in Generative AI Text Detection during 2023 SEPLN Conference<sup>1</sup>

Check out [Deloitte's AI Institute](#) for our thought leadership and publications

Delivering innovative AI applications in predictive maintenance | healthcare & financial fraud | cyber detection | document intelligence and more



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this presentation, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2025 Deloitte Development LLC. All rights reserved