Deloitte.

# Cyber AI & Automation. *Cyber accelerated.*

## AI-fueled advantages for the modern enterprise

### AI is amplifying cyber attacks …

- AI-powered cyberattacks estimated to reach 1.31 million complaints by 2025 and losses reaching $18.6B[1]
- 40% of all phishing attacks are generated by AI[2]
- Generative AI will multiply losses from deepfakes and other attacks by 32%, reaching $40 billion annually by 2027[3]

### … and advancing cyber capabilities

- The global AI market's 30% growth prediction for 2025 promises cutting-edge advancements in cybersecurity[4]
- 83% of malware variants are now detected through AI/Machine Learning (ML) models[5]
- AI reduces the average time to detect a cyberattack by up to 96%[1]

## We can help you set the vision and build a path to AI for transformation and advanced cyber capabilities

### CYBER AI FOUNDATIONS

*Being AI ready with a strategic vision and the building blocks needed to adopt and scale AI for near-term outcomes*

**Cyber AI strategy** – a clear plan to meet objectives on efficiency and value delivery, and navigate evolving technology for build vs. buy decisioning

**Data for advanced analytics & AI** – cyber data preparedness for quality, cost optimization, and to enable analytics and AI

**AI workforce** – organizational shifts and skills for workforce of the future across AI engineering, MLops, and data science

### CYBER OPS OPTIMIZATION

*Meeting challenges around growing volume and complexity of operations with automation, orchestration, and AI*

**AI-enabled security compliance** – AI to increase productivity/ speed of security controls, risk assessments, and protocols

**Secure development automation** – enable secure DevSecOps for code development, vulnerability identification, and remediation

**Digital Security Operations Center (SOC) Analysts** – increased speed and accuracy in reviewing and making rapid responses to security decisions

### CYBER AI TRANSFORMATION

*Harnessing advanced AI technology or building bespoke solutions to bring net-new AI-powered cyber capabilities*

**AI enterprise technology** – design and implementation of enterprise-wide embedded AI technology and modules

**Autonomous cyber agents** – agentic cyber AI architecture and fleet to triage, respond to, and resolve cyber tasks

**Purpose-built advanced cyber AI/ML** – proprietary and fine-tuned sophisticated AI models as a force multiplier in cyber defense

## Cyber AI Accelerators

Deployment-ready solutions– We've developed Generative AI (GenAI) and advanced AI/ML solutions that provide near real-time monitoring, automated responses, and proactive threat mitigation to safeguard critical assets and sensitive data

Delivery accelerators– We have proprietary frameworks, approaches, technology assets, and toolkits to speed up the execution of cyber AI initiatives with solutions across cloud providers, open source, on-premise, and on-device

Co-innovation with AI alliances– We collaborate with leading AI providers (including AWS, Databricks, Google, CrowdStrike, CyberArk, Palo Alto Networks, Nvidia) and academic research institutions (Virginia Tech Hume Center, Notre Dame) to provide you with leading technologies, capabilities, and platforms

Specialized AI talent – We've acquired AI/ML specialists with experience in deep learning and GenAI that, combined with our analyst- recognized cyber experience and deep industry and domain knowledge, provide value-driven outcomes



## Launch Cyber AI solutions at scale and proactively mitigate risks of GenAI

### GenAI for Third-Party Risk Management (TPRM)

Organizations spend significant time and resources conducting routine third-party risk assessments and manually reviewing large, unstructured documents (e.g., SOC2, policies, vulnerability reports) to evaluate whether security practices are compliant with regulatory requirements and policies. Our TPRM large language model (LLM)-based solution automates the identification and assessment of risks against customized security questionnaires:

- Operation & cost efficiency – reduce hours reviewing documentation and conducting assessments by 30%; increase efficiency and speed to third-party onboarding with reprioritization of analysts to high-value tasks
- Process standardization & assessment consistency – increase quality and consistency of assessments through AI-enabled human review

### Tackling attacker lateral movement with AI

Traditional threat detection techniques are hampered by shortcomings of heuristic and rule-based signature detection. Emerging solutions use anomaly detection models on internal network data and existing attack tactics, techniques, and procedures within the MITRE ATT&CK ® framework to analyze sequences of events that may indicate lateral movement of adversaries:

AI reduces the average time to detect a cyberattack by up to 96%[1]

- Reduces false alarms - utilize interpretable lateral movement events in near real time with prioritization based on false-positive rates
- Workflow automation – automate manual and repetitive tasks to free up cyber analysts' time

Sources:

1. The State of Cloud-Native Security 2024 Report (https://start.paloaltonetworks.com/state-of-cloud-native-security-2024)
2. Email Threat Trends Report 2024 (https://vipre.com/resources/email-threats-latest-trends-q2-2024)
3. Deepfake and AI fraud (https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html)
4. Cost of a Data Breach Report 2024 (https://www.ibm.com/reports/data-breach)
5. AI in Cybersecurity Statistics: Key Trends and Insights (https://seosandwitch.com/ai-cybersecurity-stats/)

Deloitte.

# Secure AI. *AI adoption accelerated.*

## Innovate with trust and unlock your future business with Secure AI

While many organizations are embracing AI as critical to market competitiveness and business performance, rising challenges across risk and scalability are limiting overall adoption and speed to market.

- 75% of leaders do not feel well prepared to address governance and risk concerns around AI, especially around user trust and security issues[6]
- 55% of organizations reported avoiding certain GenAI use cases because of data-related issues, namely managing data privacy and security and using sensitive data in models[6]

### AI GOVERNANCE & RISK

*Developing sound AI risk management practices to provide the foundation for safe and secure use of AI*

**AI policies & standards and operating model**– develop AI-focused security policies, standards, and operational constructs

**AI cyber program strategy & risk assessment**– analyze existing capabilities and processes against proprietary and National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF) standards to identify gaps and provide actionable recommendations for program enhancement

### SECURE AI PRODUCT DEVELOPMENT

*Supporting the trusted design and implementation of innovative AI capabilities within products and applications*

**Secure by design**– embed privacy, security, and trust across the project lifecycle, facilitating safe and secure AI development at ground zero

**Stress testing & AI red teaming**– simulate adversarial activity and attacks to identify vulnerabilities and weaknesses of an AI product or application

### SECURE AI PLATFORMS

*Embedding essential security and trust solutions within AI platforms and architecture*

**AI security posture management**– increase visibility and continuous monitoring of AI data, models, and infrastructure for improved risk mitigation, response, and regulatory compliance

**AI firewalls**– integrate firewall and guardrail solutions to help mitigate risks through near real-time intervention and monitoring of anomalous activity

## Accelerators

We offer a wide range of assets and accelerators to activate foundational exercises and capabilities:

- AI Risk Program Maturity Assessment Framework
- Secure MLOps Playbook
- Security Framework and Threat Library
- AI Red Teaming and Stress Testing Toolkits
- Technical Guardrail Design Playbook

## Analyst and Industry Accolades

Ranked #1 in market share for Security Consulting Services in Gartner® Market Share report, for the 12th year in a row based on revenue[7]

Deloitte named a leader in Cybersecurity Incident Response Services by Forrester[8]

Deloitte named a leader in Worldwide AI Services by IDC MarketScape[9]

Deloitte named a worldwide leader in Managed Cloud Security Services by IDC MarketScape[10]



## We bring firsthand experience to accelerate your program maturity

Our experience in designing and implementing Secure AI across programmatic, operational, and technology priorities will enable your AI adoption and transformation journey, such as:

### AI Governance Program
*Leading Hospitality Organization*

Our client sought to develop a Secure AI program that enabled innovation while balancing risk. We assessed their current AI readiness posture and defined the overall strategy to enhance maturity

- Jumpstarted their Secure AI program with clear strategic vision and a roadmap of prioritized initiatives
- Defined roles and responsibilities through a Trusted and Secure AI operating model
- Cataloged Cyber AI use cases for development

### Application AI Guardrails
*Large Media Organization*

Our client wanted to prepare for the launch of a customer-facing, LLM-backed chatbot to enable protection of proprietary data and mitigation of harmful or inappropriate content from jailbreaking. We conducted safeguard testing, implemented guardrails, and recommended custom safety rules and other measures to reduce risk exposure:

- Improvement in security exposure of the GenAI product and proprietary content
- Repeatable AI testing approach and scalable solution for AI products

## Meet the team

**Kieran Norton**
**Principal | Head of Cyber AI**
Deloitte & Touche LLP
kinorton@deloitte.com

**Alison Hu**
**Managing Director**
Strategy Transformation & Enablement
Deloitte & Touche LLP
aehu@deloitte.com

**Jane Chung, PhD**
**Managing Director**
AI Engineering & Technology
Deloitte & Touche LLP
jachung@deloitte.com

**Chris Knackstedt**
**Managing Director**
AI Platforms
Deloitte & Touche LLP
cknackstedt@deloitte.com

Sources:

6. The State of Generative AI in the Enterprise (https://www2.deloitte.com/us/en/pages/consulting/articles/state-of-generative-ai-in-enterprise.html)
7. Gartner Market Share Security Consulting Services, Worldwide, 2024
8. Jess Burn et al., "The Forrester Wave: Cybersecurity incident response services, Q1 2022,"Forrester Research, March 28, 2022
9. IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2023 Vendor Assessment, by Cathy Huang, September
10. 2023, IDC # US48761022 10: IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment, by Craig Robinson and Christina Richmond, November 2021, IDC# US46741420