Deloitte.

11 Ways Deloitte's Cyber AI and Automation Services Can Help CISOs

In our experience, the role and mission of an enterprise cybersecurity program can be impacted by Artificial Intelligence (AI) across three major dimensions: the threats and vulnerabilities associated with the use of AI and related expanded attack surface; external threats and attacks enhanced by AI; and AI-enabled cyber transformation. **CISOs should look to build confidence that AI is operating as intended and is secured from cyber risks, and set the vision for how to leverage AI to advance cyber capabilities.** Deloitte—ranked #1 out of Top Five Security Consulting Service Providers, Worldwide, 2024[1] for the eighth consecutive year, and a Leader in AI Services[2]—is at the forefront of cyber and AI. We offer services in AI governance, program orchestration and automation, secure, trusted Software Development Life Cycle (SDLC), and cyber-AI solution design and implementation. Here are several ways that Deloitte can help CISOs effectively enable safe AI and automation adoption for their business, as well as enhance their organization's cybersecurity program.

1 **Our award-winning Cybersecurity services[3] are bolstered by Deloitte's AI Institute and Trustworthy AI™ Framework:** Deloitte's AI Cyber Risk Management Framework can help CISOs identify and manage AI-related risks and controls while driving innovation and adoption at scale. Our Generative AI (GenAI) practice includes a team focused on the rapid development of pilot programs, demos, and proofs of concept. We advise clients on operationalizing solutions based on leading foundation models. We also offer end-to-end Advise, Implement, and Operate (managed) services with technology solutions.

2 **Fighting AI with AI for Advanced Threat Detection and Response:** AI is turbocharging the speed and scale of attacks. As threat actors start using AI to advance their tactics, techniques, and procedures to infiltrate and then execute malicious activities, **CISOs need to deploy sophisticated defenses** to counter these attacks. Deloitte, in collaboration with industry leaders, has developed end-to-end, AI-driven solutions to help clients rapidly identify and respond to sophisticated cyber threats. **By leveraging machine learning, GenAI, and automation, CISOs can gain an edge in detecting threats, predicting attacks, and neutralizing risks.**

3 **Proactive Vulnerability Management**: Deloitte's cyber practice helps CISOs stay ahead by aggregating, analyzing, risk ranking and auto generating update packages based on vulnerability, configuration, patch management, asset management, and other cyber data. Our proactive approach helps clients reduce the vulnerability exposure window while increasing systems management efficiency.

4 Efficient Incident Handling: Automation streamlines incident response workflows. Our solutions can authorize and orchestrate actions, collect evidence, and facilitate collaboration among security teams, helping to **reduce incident resolution time, analyst alert fatigue, and human error**.

5 Enhanced, Automated Security Operations Center (SOC): Deloitte's AI Native Security Operations Platform™ offers next-generation security operationalization to orchestrate intelligent resilience. It combines data modeling and integration with automated analytics and detection to reduce alert volumes and ease the burden on security engineers. This allows CISOs and their teams to focus on strategic decisions.

6 Secure Software Development Lifecycle™ (SSDL): Our SSDL model is a strategic and continual improvement process aimed at delivering continuous security, increased efficiency, enhanced compliance, and reduced costs in every phase of the DevOps Lifecycle.

7 Automated Compliance Monitoring by Industry: As a leader in compliance advisory services, Deloitte can help CISOs understand the regulatory requirements of their environment through our dedicated **cybersecurity specialists in these verticals: financial services; energy, resources, and industrials; life sciences and health care; telecom and telecommunications; consumer; and government/public services**. Our AI Institute publishes cutting-edge research and case studies, advising on ethics, AI regulation, and other policies that shape AI development while protecting the public.

8 Scalability and Resource Optimization: Our AI-driven automation scales with less effort. This efficiency can improve resource allocation, time, and reduces operational costs.

9 Threat Hunting and Intelligence: Deloitte's cyber practice combines AI with threat intelligence feeds. It proactively hunts for emerging threats, zero-day vulnerabilities, and indicators of compromise to help organizations stay one step ahead. **AI can act as a force multiplier** in support of executing the cyber mission, providing advancements/efficiencies.

10 Proprietary and Customizable Playbooks and Accelerators: Deloitte tailors automation playbooks to create **bespoke solutions** for your organization's specific needs. Whether it's incident response, user provisioning, or network segmentation, CISOs can automate processes specific to their environment. Our proprietary accelerators can enable you to weave safety, compliance, and security into your organization's AI fabric.

11 Continuous Learning and Adaptation: Deloitte's cyber trained AI models are continuously improved, adapting to evolving threats. Our models are evaluated, selected, and trained based on criteria that represent risk. CISOs can benefit from an **ever-improving defense system** that evolves alongside the threat landscape. So, we are helping you protect against the threats of tomorrow, not just today.

Because every organization's needs differ, we welcome CISOs to assess how Deloitte's Cyber AI and Automation practice can help them achieve their specific goals and challenges. Get in touch to see how we can help you. We are ***Cyber, Accelerated.***

Contact

Kieran Norton
Principal
Cyber & Strategic Risk
Deloitte & Touche LLP
kinorton@deloitte.com

Jane Chung
Managing Director
Cyber & Strategic Risk
Deloitte & Touche LLP
jachung@deloitte.com

(1) Source: Gartner® Market Share Analysis: Security Consulting Services, Worldwide, August, 2024 - GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

(2) Source: Deloitte is named a **Leader in Worldwide AI Services** by IDC three times in a row. *IDCMarketScape: Worldwide Artificial Intelligence Services 2023 Vendor Assessment.*

(3) IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment.