KPMG

Unleash the Power of AI

Three ways AI can be a game-changer for your security operations center

kpmg.com

A year ago the narrative around artificial intelligence was largely about the fear of job losses, but those concerns have diminished. Now security leaders are looking for long-term AI strategies and solutions to address the rapidly changing threat landscape.

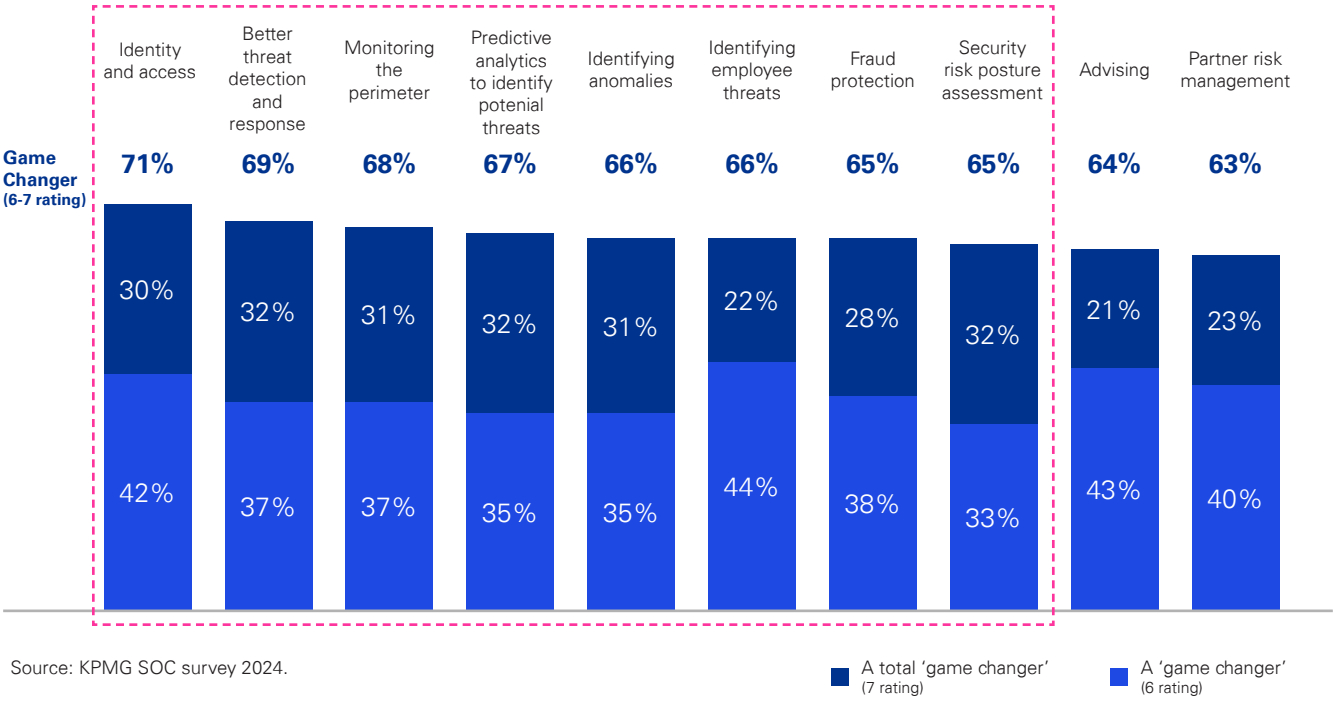
According to the latest research from KPMG LLP (KPMG), within security operations centers (SOCs) at least six in 10 SOC leaders see AI as a "game changer" across virtually every key security function, from fraud protection and identifying anomalies to perimeter monitoring and identity and access management.[1]

[1] KPMG Security Operations Center survey, "The time to transform is now," 2024.

A majority of security leaders believe AI will be a "game changer" across virtually every security function

Security leaders most commonly identify AI as transformative in identity access.

Areas in which AI will be a "game changer" in identifying and remediating threats/vulnerabilities



Source: KPMG SOC survey 2024.

Security leaders are looking to AI-based automation to stay ahead of new and emerging threats and to increase SOC agility and response. SOC measurement and reporting, and the availability of resources through increased productivity resulting from AI-based automation, are also highly desired.

Desired benefits of AI-based automation for SOC (up to three responses allowed)

% selected as one of up to three benefits

New strategies and solutions

Response teams routinely field hundreds if not thousands of potential security incidents every year. Common viruses can be easily recognized most of the time and don't need to be investigated. An AI model can determine a true positive alert and automatically delete the file in a triage process typically conducted by a junior analyst.

But what if you need more complex threat intelligence research? Or to build additional response automation to prioritize threats? Worse yet, what if you don't know where to start or how to identify areas where AI will be useful? That's true of 17 percent of our survey respondents. Nearly a quarter also say they lack internal knowledge to take advantage of AI solutions (23 percent), while 24 percent find it difficult to demonstrate the ROI.

What does it require, then, to take full advantage of AI in the SOC and gain the confidence that you have visibility into your entire security ecosystem in a cost-effective manner?

01

Pioneer new approaches

Recognize what situations AI is especially useful for and where it needs to be enhanced to improve the value proposition. Deep learning models and neural networks—computer systems modeled on the human brain—don't explain why they make the predictions they make when identifying potential threats. Moreover, these models live in software that is notoriously difficult to secure. Attacks against them are unique, making them challenging to defend.

When attacks do occur, you have millions—if not billions—of actions you can take. How do you prioritize which thousands you should actually be doing? How do you put those actions in context in terms of the vulnerabilities that are being actively targeted? If 100 email boxes are compromised, for example, you'll want to fix your CEO's mailbox before those of your support staff. But how do you create the context that drives what actions you take against these events and when you should take them?

Machine learning and automation provide considerable value for prioritization. A model can be trained on your organization's historical data to assess all the data points. Analysts, in comparison, can assess only a few hundred before they're overloaded. A model also self-learns. As more historical data accumulates, the model automatically updates to accommodate new information. And, unlike humans, AI models work 24/7.

02

Be proactive

With attackers and defenders both using AI for different ends, it's not enough to be battle tested. Empowering your SOC with a risk-based approach to prioritize threats can secure an organization's most critical systems.

The KPMG AI security framework gives security teams a tailored playbook to proactively assess their organization's AI systems in development and production environments. The framework helps secure those systems against such threats as backdoor attacks and model inversion and respond effectively in the event of an attack.

Bottom line, considering the limitations of the human team, it's critical to augment the analyst's abilities—a task for which AI is perfectly suited. Our red-teaming services conducts penetration testing against AI models to identify weaknesses before a breach occurs. Employing AI this way can help companies understand and anticipate the methods attackers may use to circumvent the organization's defenses.

In this capacity, AI enables testing of the effectiveness of existing digital forensics and incident response capabilities and can simulate a more realistic threat environment through which to fine tune the overall Security Information Event Management (SIEM) solution set. In a fluid environment, AI can reduce the number of alerts and automate the response, which helps analysts learn from the tactics, techniques and practices they're seeing on a daily basis.

03

Get better at measuring AI effectiveness

Many security leaders are struggling to demonstrate the value of AI solutions. Nearly one-quarter (24 percent) of our survey respondents say they don't have strong use cases. It's tricky to quantify the dollar value of prevention, for example. When a phishing attack occurs, how much is a priority three alert worth versus a priority one alert? Implementing a model that can auto-prioritize threats adds another layer of complexity to a costing exercise.

What's needed are better measurements. AI can be very useful in turning data into insights, improving decision-making and contributing to cost savings and a strengthened security posture.

In measuring overall performance, using AI to automate incident responses and detect anomalies allows SOCs to quickly identify and respond to cyber threats and take proactive measures to prevent future incidents.

At the process level, security leaders can use AI to create more accurate detection rules. For example, AI can compare how an organization performs event logging against leading practices and identify gaps. It can identify which security tools are missing and recommend where to invest in new tools. AI can answer questions about performance over time, compare performance over specific intervals, and generate a monthly CISO scorecard.

By monitoring and evaluating AI performance, organizations can enhance the benefits of AI in their SOCs and help ensure long-term security resilience.

KPMG can help

Despite the increasing sophistication of AI responses to new cyber threats, we're still in early days. About half of security leaders say they have "major issues" with retention (47 percent) and maintaining up-to-date knowledge (46 percent), skills, and expertise (45 percent) to identify, analyze, and remediate emerging threats.

The issue is not about developing additional technical capability when dedicated teams are already at work. The larger issue is the lack of strategy and long-term vision for AI solutions. KPMG AI security professionals have deep experience in business processes and risk, coupled with extensive knowledge of AI application, data science, and cybersecurity.

We know that the transformative power of AI can only reach its full potential when paired with human expertise and ingenuity. That's what makes AI the game-changer it has become.

Contact us

Matthew P. Miller
Principal, Advisory
Cyber Security Services
KPMG US
E: matthewpmiller@kpmg.com

Ryan Budnik
Director, Advisory
Cyber Security Services
KPMG US
E: rbudnik@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**