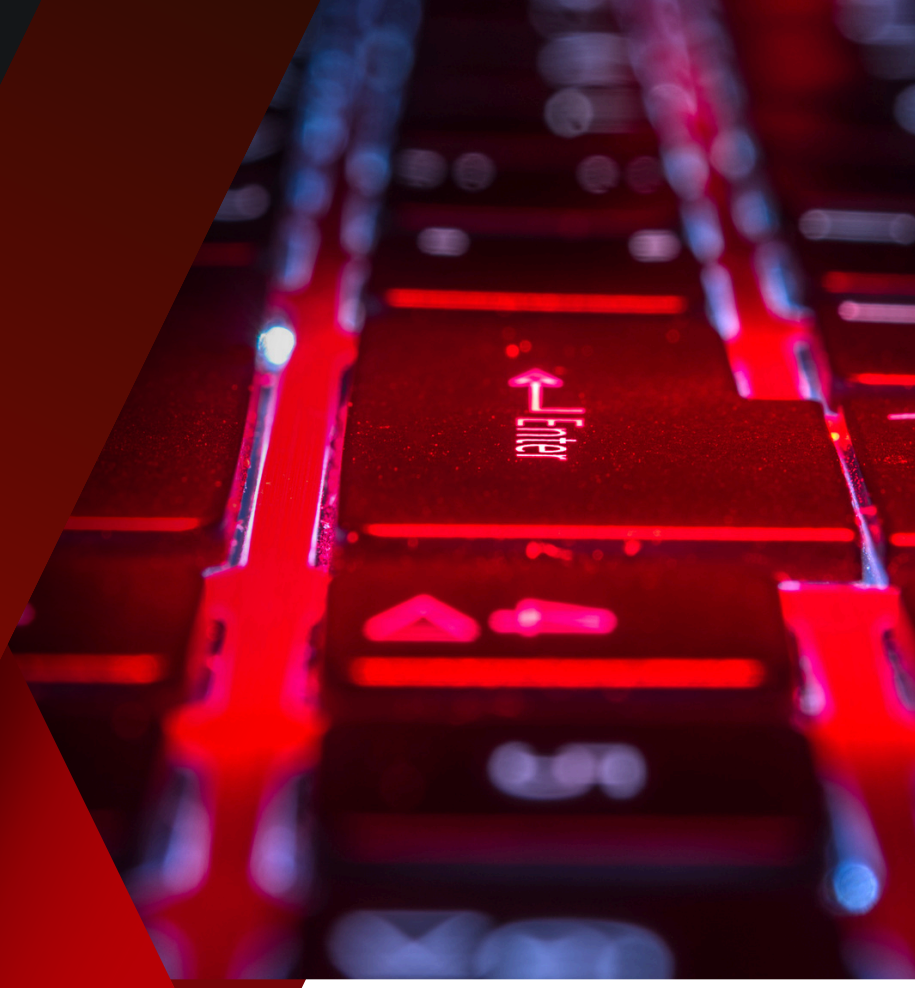
Infosecurity Magazine



Adapting to Tomorrow's Threat Landscape:

AI's Role in Cybersecurity Operations in 2024

Overview

Artificial intelligence (AI) is having a transformative impact on cybersecurity operations and can help organisations proactively counter cyber-attacks and reduce the burden on security professionals.

During a recent Infosecurity Magazine webinar, in partnership with SCC, a panel of experts discussed how AI-powered solutions are reshaping vital cybersecurity roles, including threat detection, incident response, and vulnerability management.

The session also discussed best practices on implementing AI tools into existing technology architecture effectively, and how to mitigate risks with these technologies, such as data leakage, bias and hallucinations.

Infosecurity Magazine SCC

Opening Presentation

The webinar began with an opening presentation by Paul Allen, Practice Director at managed service provider SCC. He emphasised that before deploying AI and automation tools, organisations must understand their current maturity and risk level, and where they see themselves in the future.

As an MSP, SCC is positioned to help organisations get a clear view and context of their enterprise to make informed decisions about the AI tools that can assist their journey.

"Without understanding the why, you can't drive automation and you can't achieve the sorts of results that you need. We need to be able to demonstrate that to you," explained Allen.

He also highlighted that the core elements of:

People Process Technology

must work in harmony for AI tools to be effective.

Allen identified several key areas where AI can have the biggest impact for organisations. These include:

· Data analysis – freeing up the time of security professionals
· Vulnerability management – rapidly identifying vulnerabilities early
· Incident response – triaging to allow defenders to prioritise resources and resolve issues quickly.

SCC's Aegis platform leverages advanced automation and AI to help security teams enrich, triage and respond to potential threats.

With SCC in the top 1% of Microsoft's security partners globally, Aegis is integrated into Microsoft's Copilot for Security AI solution. The platform is designed to interoperate with Copilot, augmenting the security functions provided in the large language model (LLM), which is available globally as of April 1, 2024.

TO WHAT EXTENT IS AI CURRENTLY BEING USED IN YOUR SECURITY TEAM'S OPERATIONS?

A. WE USE AUTOMATION, AI AND GENAI TECHNOLOGIES TO ASSIST GENERAL FUNCTIONS (18%)

B. WE USE AUTOMATION/ML TOOLS PRIMARILY FOR DATA ANALYSIS/THREAT DETECTION (18%)

C. WE ARE ONLY JUST STARTING TO USE AI TOOLS IN OUR SECURITY TEAM AND ARE DISCOVERING BEST PRACTICES (24%)

D. WE DO NOT USE ANY AI TECHNOLOGIES IN OUR SECURITY OPERATIONS (35%)

E. OTHER (6%)

Importance of Leveraging AI in Cybersecurity

AI-based security tools have become prevalent in recent years, with many cybersecurity vendors offering such capabilities in recent years. Therefore, the answers to the first audience poll question came as something of a surprise, with 35% of respondents stating that they do not use AI in their security operations.

Phil Robinson, Principal Security Consultant and Founder, Prism Infosec, believes that many of these respondents could be leveraging AI for security purpose without realising it, such as the Microsoft Defender tool on their desktops.

Allen said that we are reaching a stage where organisations have no choice but to apply AI in areas like data analysis, given the trillions of signals of data being generated every day on networks.

Allen emphasised

> *"If you don't lean into it and see this as a positive agent of change, you could be one of those dinosaur entities that gets left behind."*

AI and automation are now critical for analysing datasets effectively both in gathering intelligence and applying context to it.

Robinson also detailed how AI is assisting in offensive security and red teaming practices, an area he specialises in.

This includes gaining granular details on security assessments undertaken against large organisations, allowing large datasets to be analysed quickly.

It takes the "hard work and grind out of security testing," he added.

AI Deployment Requires Careful Planning

While AI offers enormous benefits for cybersecurity teams, organisations must be careful to select the appropriate solutions for their enterprise.

This is a challenge given the vast amount of marketing hype around AI-based security products, particularly since generative AI tools like ChatGPT have become publicly available.

It is crucial to recognise that AI is a tool that can assist security teams, just like any other technology, but it cannot be relied upon alone to protect organisations.

Allen commented:

> *"There's no such thing as a silver bullet in cybersecurity, but it is about the appropriate application of people, process and technology."*

He advised organisations to first speak to consulting firms like Gartner to gain a proper understanding the AI security product market, while MSPs can assist with helping them achieve the best outcomes for their entity with the technologies available.

A strong governance policy is crucial to clearly define the organisation's risk appetite and where it wants to go to as an organisation.

This will help establish the business problem that needs fixing and discover the most appropriate tool that can address that issue.

Munson advised:

"Ensure the solution you're looking at can interoperate with everything you already have and that it aligns with your existing security architecture."

Robinson concurred, urging organisations to ignore the dramatic headlines about AI in the mainstream media and treat it just the same as any other security tool.

"Have a risk assessment to work out how might it affect existing processes and people, and will the business have an overreliance on it," he stated.

WHAT IS THE BIGGEST RISK OF USING AI TOOLS IN SECURITY OPERATIONS?

A. ACCIDENTAL LEAKAGE OF SENSITIVE DATA ON GENERATIVE AI TOOLS (60%)

B. BIAS/DISCRIMINATION IN DATASETS (0%)

C. DATA POISONING AND OTHER ATTACKS TARGETING AI MODELS (27%)

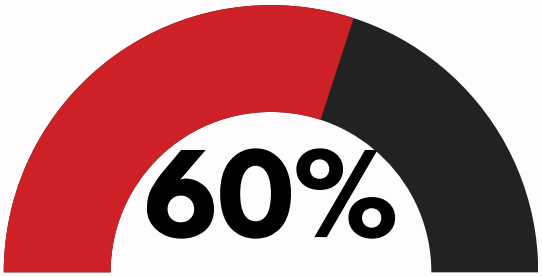
D. AI HALLUCINATIONS (13%)

E. OTHER (0%)

Addressing AI Risks

The security, privacy and legal risks posed by the deployment of AI in organisations is front of mind for many cybersecurity practitioners.

In the second audience poll question,



of respondents highlighted accidental leakage of sensitive data as the biggest risk around using AI tools in security operations.

This is an area all organisations should be concerned with, Allen noted, with cases of sensitive corporate data accidently being released into the wild via LLMs like ChatGPT already emerging.

"We don't want that information to be harnessed and used against us," said Allen.

If they haven't done so already, organisations should ensure they have a clear understanding of how they are controlling AI datasets and the type of information they are sharing with providers.

Allen urged organisations to implement policies that limit the use of LLMs across the workforce to prevent corporate secrets and source code being revealed during interactions with these models.

Lee Munson, Principal Research Analyst at the Information Security Forum, noted that many organisations are considering the risks of sensitive data being made public after being input into open-source AI tools like OpenAI's ChatGPT.

"A lot of the organisations I speak to are distinctly wary of LLMs and the risk of data leakage," he noted.

Addressing AI Risks (Continued)

Another concern highlighted by poll respondents was data poisoning, which Robinson highlighted as a very real danger to organisations.

If enough code is fed into LLMs, it could start using that code as examples for other developers – which may contain vulnerabilities. Robinson said there's even examples of such code being incorporated into online libraries.

The issue of bias in AI models was also highlighted, organisations could face legal consequences if discrimination is caused in business decisions as a result of AI datasets.

The best way of reducing the bias risk in AI tools is to work with very specific and defined datasets, and continuously review the training methods, advised Allen.

Allen shared,

> *"We have to ensure we aren't training in any potential for bias because that affects context, and ultimately can affect the outcome as well."*

Robinson added that it is vital that the dangers of AI are incorporated into security awareness training. Employees should be aware that they shouldn't trust everything that comes out of AI without validation, particularly when conducting sensitive operations or security processes within an organisation.

How AI Will Impact Cybersecurity Jobs

Allen, Munson and Robinson agreed that AI will inevitably have a significant impact on cybersecurity jobs, and this will be mostly positive.

AI's ability to analyse data quickly and efficiently will help free up the time of cybersecurity professionals to specialise in specific areas. This is especially important given the cyber workforce gap, estimated to be at 4 million globally.

Robinson emphasised:

> *People will always be fundamental in cybersecurity, even as AI becomes more sophisticated.*
>
> *Soft skills, such as interpreting business strategies, will be needed to ensure these enhanced capabilities translate into the right outcomes for organisations.*

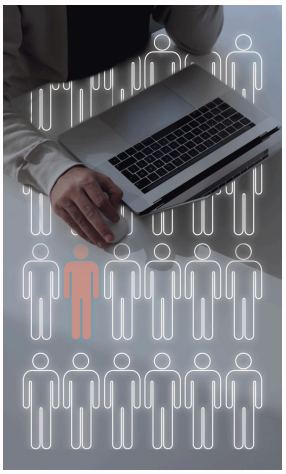
New types of jobs will also be created as adoption of AI continues, such as AI and data specialists.

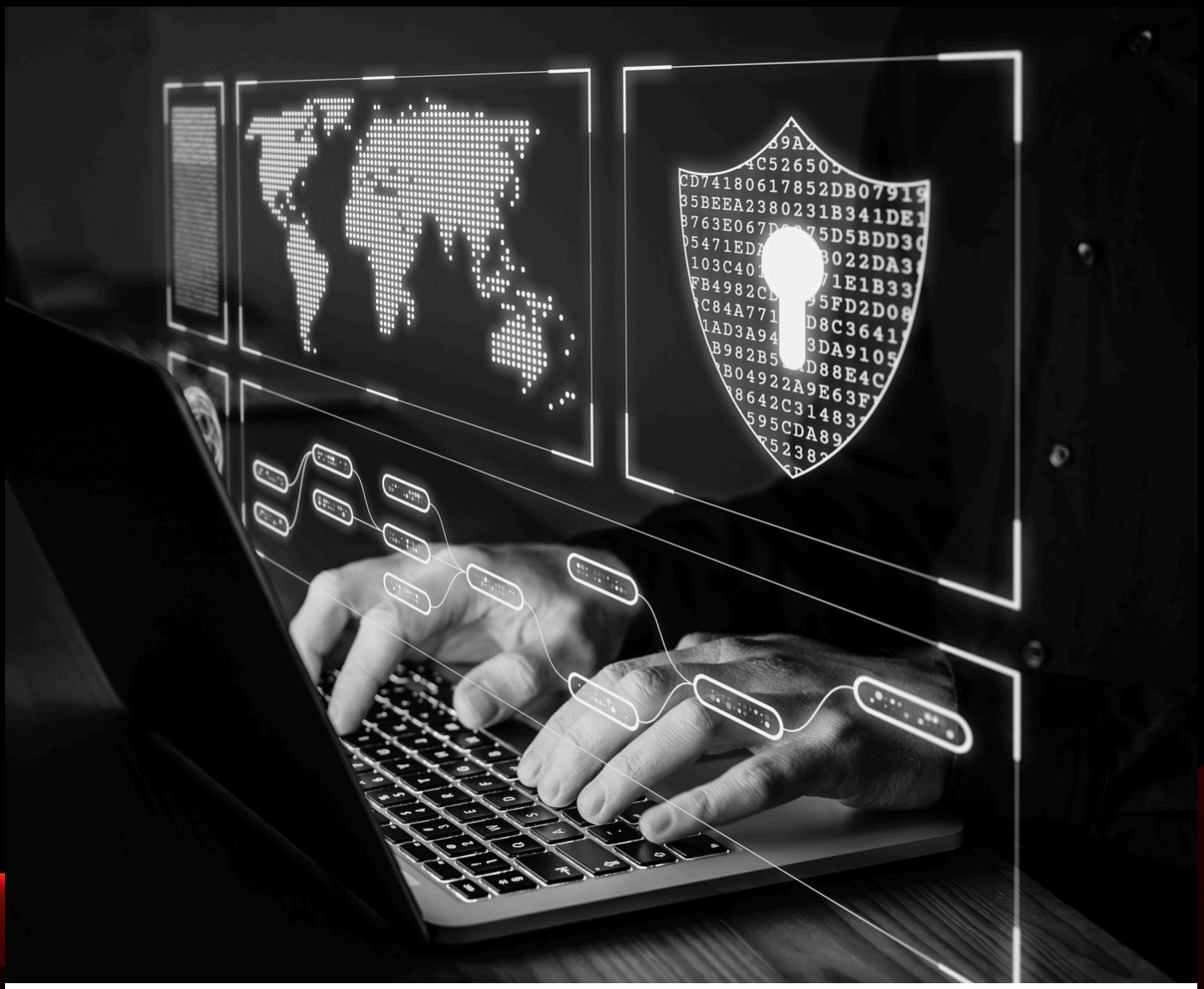
This will spawn "an entirely new industry," according to Allen.

"You are going to need people to handle the planning, the progression, the operational support, the in-life care and the interactions with the real world for all of these solutions," he explained.

However, Munson warned that organisations will need to plan longer-term for a changing cybersecurity workforce, with junior positions likely to be reduced by growing AI capabilities.

"This begs the question, who is going to fill the more senior positions of the future?" he asked.





CONCLUSION

While organisations should be seeking to utilise AI to enhance their cybersecurity operations, they must also understand its limitations and ensure they understand why it will benefit the business before going ahead with implementation.

> ***"Crawl, walk and then run – work out where you want to go and how you are going to get there."***
>
> ***Paul Allen, Practice Director at SCC***