

Top questions that  
CISOs should be asking  
about AI (and answers)

# Table of Contents

Introduction .....	3
1. Essential AI insight.....	4
2. AI and Cyber Security .....	5
3. Safety and strategy .....	6
Conclusion .....	11

# Introduction

Artificial intelligence has transformed our world in unprecedented ways.

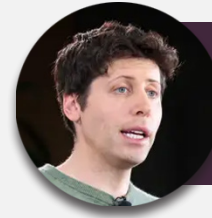
In the cyber security space, artificial intelligence introduces both exciting new possibilities, and little-known, scarcely understood risks.

In this eBook, we'll address top questions from CISOs and cyber security professionals surrounding what AI means for cyber security, how to leverage AI effectively, and how to maximize the opportunities that it presents.

Making the right decisions starts with asking the right questions. You've asked the questions here...

Let our answers support your enterprise growth.

## Influential Leaders on AI



*"AI will probably most likely lead to the end of the world, but in the meantime, there'll be great companies."*

Sam Altman, CEO OpenAI



*"We're on the verge of a very interesting revolution — the AI revolution."*

Gil Shwed, CEO of Check Point



*"In the AI-native era, what we need are AI-native applications at a scale of millions."*

Robin Li, CEO and Co-Founder, Baidu

# Essential AI insight

## 1. IS IT ALL JUST BUZZ AND IF IT IS, CAN I TRUST THE BUZZ?

There's no getting around the fact that AI has indeed become a buzzword. But AI's ascension to buzzword status doesn't necessarily mean that it's overrated – In fact, things typically attain buzzword status because they outperform everything else out there.

AI delivers. Artificial intelligence is improving outcomes and transforming businesses. Nearly 70% percent of executives have stated that AI results in higher efficiency for cyber security analysts within their organization.<sup>1</sup>

In 2023, organizations that applied robust AI and automation tooling saved nearly 1.8 million in data breach expenses. These organizations also effectively accelerated breach identification by more than 100 days, on average.<sup>2</sup>

AI doesn't just hold promise and potential for the future, but rather, it's being used to achieve hyper-growth results, across computing and cyber security, today.

It's simple. AI-powered tools accomplish more than prior generations of tools. AI is fast, organized and consistent – qualities that both people and legacy tools sometimes lack.

To make an analogy, right now, there's tremendous hype (and more than a few eye-rolls) around Tesla's Cyber Truck. However, for all the cynicism, the truck does actually offer higher torque, higher ground clearance and higher horsepower than other trucks on the market.

It can tow roughly double what Toyota Tacoma can, depending on technical specs. In short, the truck outperforms others on the market, in the same way that AI can outperform existing technologies and/or human capabilities.

## 2. CAN AI TECHNOLOGIES BE TRUSTED, IN GENERAL?

Artificial intelligence models are only as good as the data that they're trained on. Says Stanford professor James Zou, "One of the best ways to improve algorithms' trustworthiness is to improve the data that goes into training and evaluating the algorithm."<sup>3</sup>

In seeking out AI-based tools and cyber security solutions, look for those that provide products for a large customer base. Why? The more customers that an AI-based service/solutions provider retains, the more training data that a company has with which to feed the AI model. If leveraging trusted solutions from reputable, high-performing vendors, AI can offer powerful advantages.

1. AI Week 20203: All Artificial Intelligence, All Week, CyberTalk.org

2. Research Shows Extensive Use of AI Contains Data Breaches Faster and Saves Significant Costs, IBM, Jackie Lehmann, Lindsay Durfee, August 14, 2023

3. Unveiling the Power of AI in Cybersecurity: Three Questions CISOs Should be Asking, Forbes, Jonathan Fischbein July 13th, 2023 <https://www.forbes.com/sites/forbestechcouncil/2023/07/13/unveiling-the-power-of-ai-in-cybersecurity-three-questions-cisos-should-be-asking/?sh=1f1881df289a>

# AI and Cyber Security

## 3. WHAT CYBER SECURITY USE-CASES CAN AI EFFECTIVELY ADDRESS?

AI excels when it comes to threat prevention and detection. Artificial intelligence tools can analyze extensive quantities of data from a variety of sources, sifting through the data to identify patterns that may be indicative of a cyber attack.

AI-powered cyber security technologies can effectively help predict threats and stop cyber attacks, before they cause serious damage.

*Automated tools in the security space can also reduce the risk of human error, improve cost savings, increase scalability and serve to future-proof a business.*

## 4. HOW CAN I USE LLMS TO ENRICH MY SECURITY EVENT REPORTING?

LLMs reliant on logs that companies collect show that hacker activity is being analyzed in a few different ways: 1. LLMs are being used to help search for issues that were allowed by security tools. 2. They are also being used to perform historical searches for evidence of issues that occurred in the past and that are only now recognized as issues.

Security professionals can also leverage LLMs to reduce the number of false positives, fine-tuning the system so that it requires less human assistance and monitoring. Beyond that, security professionals can use the outcomes that they have high confidence in to auto-create rules, preventing those kinds of issue from affecting systems on a large-scale.

## 5. WHEN IT COMES TO CYBER SECURITY TOOLS, HOW ARE AI DATA MODELS TRAINED AND WHAT ARE THE SECURITY IMPLICATIONS?

The machine learning algorithms used in cyber security tools are trained on extensive datasets that include diverse threat scenarios and software behaviors. Models can also improve their own detection capabilities over time.

As AI algorithms assimilate new data, the models can iteratively refine themselves, resulting in increased accuracy when it comes to identifying emerging threat patterns.

# Safety and strategy

## 6. WITHIN THE SOLUTIONS THAT YOU DEPLOY, AS A SECURITY LEADER, HOW CAN YOU ENSURE AI SAFETY?

- Ensure that the tool complies with relevant industry-based data protection regulations (HIPAA, SOX...etc.).
- Test adversarial scenarios against the solutions to ensure resilience in the face of manipulative tactics.
- Develop a feedback loop that empowers cyber security analysts to validate and share thoughts on threat intelligence outputs.

These are just a few of the options.

Ensuring the safety of AI-based solutions may require tailoring security measures to the specific characteristics and requirements of a given tool, in addition to customizing your approach based on your industry, common threat types, previously seen false positive/negatives, and other unique data inputs.

## 7. WHAT'S THE LONG-TERM STRATEGY FOR AI WITHIN CYBER SECURITY?

From 2020 to 2022, the use of security-focused AI and automation jumped by nearly 20%. Due to the increasing volume of cyber threats and soaring data breach costs, organizations are currently seeking to increase investments in artificial intelligence.

Across the next two years, more than 80% of IT decision-makers intend to incorporate AI into cyber security strategies. If you haven't done so already, start thinking about high-potential AI use-cases; the ones in which AI will offer the greatest number of benefits to your organization.<sup>1</sup>

In the digital era, including AI within cyber security isn't merely an optional endeavor – it's critical to staying competitive and remaining ahead of the curve.

---

1. 35+ AI Statistics to Better Understand Its Role in Cybersecurity [2023], Secureframe, Anna Fitzgerald, June 05 2023

# CISO Perspectives

## AI in the cyber security space



### PETE NICOLETTI

Pete Nicoletti, Field CISO, Americas. Pete has 32 years of Security, Network, and MSSP experience and has been a hands-on CISO for the last 17 years and joined Check Point as Field CISO of the Americas. Pete's cloud security deployments and designs have been rated by Gartner as #1 and #2 in the world and he literally "wrote the book" and contributed to secure cloud reference designs as published in Intel Press: "Building the Infrastructure for Cloud Security: A Solutions View."

*"We're seeing companies quickly deploy and leverage AI in the security space. Companies know that adversaries are using AI to code new threats and to compose targeted phishing emails. Mature security program managers know that they must use AI engines to mitigate those threats."*



### JONATHAN FISHBEIN

Jonathan Fischbein has served as Check Point's Chief Information Security Officer for two full decades. He has more than 25 years' experience in high-tech security markets, shaping security strategies, and in developing ad-hoc solutions to help large corporations mitigate security threats.

*"Those harnessing the power of AI will overcome the competition. Those that are afraid of AI will remain behind..."*

*AI has the potential to bring about transformative changes in various industries, leading to increased efficiency, innovation and strategic advantages."*



### MARCO EGGERLING

Marco Eggerling is a passionate information security professional and transformational leader with more than 20 years of experienced focused on information governance and security, as well as risk management and compliance. He has strong experience in building and leading large-scale security programs and enabling organizations to deliver high-value products and services.

*"AI rapidly replaced the need for rule-based and manual security response capabilities and is helping to drive maturity of security programs across industries."*

# Where are we with AI regulation and what does it mean for businesses?

In a landmark initiative, the European Union is the first global governing body to pass comprehensive artificial intelligence regulations. The legislation requires that AI manufacturers adhere to transparency requirements, and that enterprises in the business of creating synthetic media must make adherence clear to users. In addition, use of facial recognition tools on the part of law enforcement agencies will be highly restricted. Those that flout the new regulations may face significant penalties. While the law does still need approval from the European Parliament, this is widely seen as a mere formality. The regulations are due to take effect in 2025.<sup>1</sup>

Canada is also at the forefront when it comes to championing responsible AI governance and legislation. Federal legislation intended to regulate AI is currently before the House of Commons. The country is committed to implementing transparency requirements, especially when it comes to collection of personal information. For example, if an enterprise intends to use AI to analyze a person's work performance, economic situation, health, personal preferences, interests or behavior, the enterprise must inform the individual about use of such a tool, and provide the individual with control over the collection of data. In some cases, legislation mandates that individuals have the right to review AI-based decisions with human beings.<sup>2</sup>

---

1. EU Reaches Landmark Deal on World's First Comprehensive AI Regulation, Kia Kokalitcheva, December 8th, 2023

2. Artificial Intelligence in Financial Services: The Canadian Regulatory Landscape, Fasken, November 23, 2023



In contrast with the E.U. and Canada, the United States has pursued a more decentralized approach. According to the Center for Strategic and International Studies, an American think tank, the U.S. government will likely boost spending around AI and AI research, especially as it relates to defense and intelligence, however, responsible AI initiatives may be patchy.<sup>3</sup>

In Asia, the urgency around artificial intelligence regulation, as encouraged by the European Union, has received a tepid response. “Many Asian countries favour a ‘wait and see’ approach, or are leaning towards a more flexible regulatory regime,” reports Reuters.<sup>4</sup>

**In Africa, artificial intelligence was at top of the agenda during the African Union summit, in November. Some experts believe that AI may benefit Africa more than any other continent, delivering more efficient and equitable access to goods, services and opportunities.**

3. AI Regulation is Coming – What is the Likely Outcome? Center for Strategic and International Studies, Bill Whyman, October 10, 2023

4. Exclusive: EU’s AI Lobbying Blitz gets Lukewarm Response in Asia, Reuters, Fanny Potkin, Sam Nussey, and Supantha Mukherjee, July 19th 2023



## 8. CAN AI-BASED TOOLS REPLACE A ZERO TRUST STRATEGY?

Although AI-based tools can serve as valuable components of a zero-trust strategy, they typically wouldn't replace the strategy itself.

AI can help reinforce the fundamental technologies and principles embedded within the zero trust model. For instance, AI can provide informed reference points when it comes to granting or denying resource access.

At present, IT teams often manually verify and provide access to requests. This can be time-consuming and legitimate users may have to wait for approval if there's a significant volume of requests. AI expedites the process.

In and of itself, AI isn't a silver bullet.

Rather, it should be part of a layered approach to cyber security.

## 9. HOW CAN AI SAFETY AWARENESS BE INTEGRATED INTO SECURITY AWARENESS, IF AT ALL (AND SHOULD IT BE)?

Within employee-focused cyber security awareness programming, consider adding an AI section. Exactly what that looks like will depend on the programs that your organization already has in-place, and the program delivery styles that work best for your industry and your unique group of employees.

However, broadly speaking, yes, AI safety should arguably be a part of cyber security awareness, as hacks and breaches can occur through AI-based tools.

*"Integrating AI safety awareness into security awareness is crucial, as the deployment of artificial intelligence systems poses unique risks and challenges."*

*A few examples of what your program should include: AI and security trainings, frequent personal updates about AI risk and threats, including ethical considerations of using AI, and cross-functional collaboration efforts involving all of those working on AI-related projects."*

– CISO Jonathan Fischbein, Check Point

## 10. WHERE CAN I LEARN MORE ABOUT AI-POWERED CYBER SECURITY TOOLS?

Additional AI and cyber security resources are accessible [here](#) and [here](#). For more information about AI-powered cyber security technologies that can enhance your organization's security and business outcomes, please connect with your local Check Point representative.

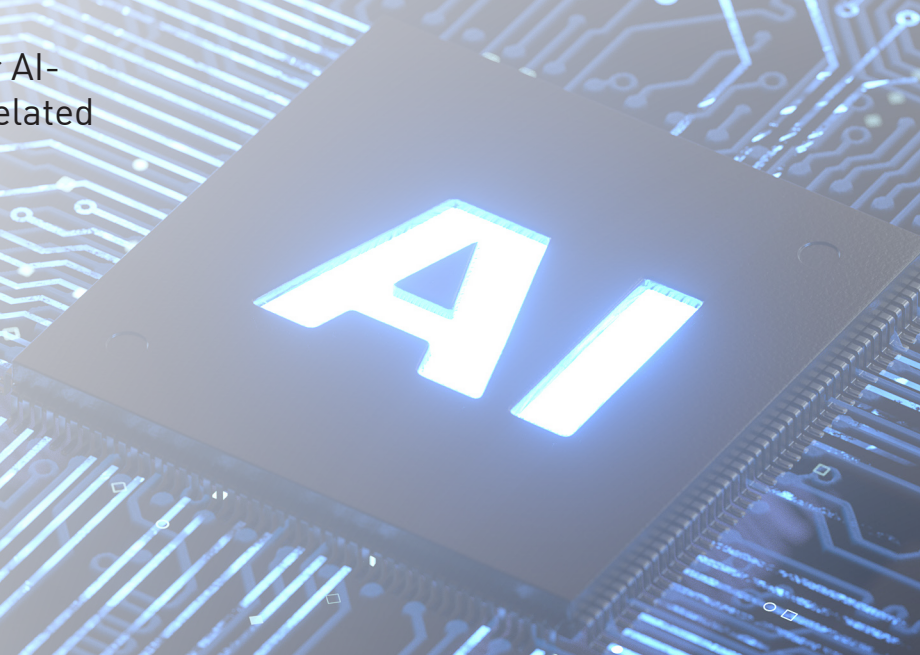


# In conclusion

Navigating the intersection of AI and cyber security won't be easy. And the landscape is unpredictable.

However, by continuously asking questions, seeking knowledge, embracing innovation and fostering collaboration, CISOs and cyber security professionals can ensure a secure and resilient future.

Reference this eBook as you continue to build your AI-powered cyber security initiatives. For additional related resources, please visit [www.cybertalk.org](http://www.cybertalk.org).



AI