Elevate Security

AI in Cybersecurity: Future Trends for 2024

By 2030, the AI in Cybersecurity Market Size is projected to reach **USD 133.8 billion**

The rise of artificial Intelligence (AI) is intensifying the need to change the way we approach cybersecurity. As this new technology expands, it's critical to consider the security threats it might bring to organizations of all industries and sizes. Simultaneously, it's equally important to evaluate the positive Impact AI can and will have on cybersecurity programs.

We're stepping into a new world of AI in cybersecurity. It's exciting and fast-paced, but it can also be a bit nerve-wracking if you don't have the proper systems and processes in place to navigate this time of rapid innovation. To help you make sense of it all, we're highlighting the key AI trends expected to shape the cybersecurity landscape in 2024.

Top Concerns: AI-Enabled Security Threats & Attacks

AI-Enabled Fraud

By 2025, AI-enabled fraud will change the enterprise attack surface indefinitely. As a result, organizations will focus their efforts on security education and awareness.

AI-Enabled Phishing

68% of survey respondents believe AI could be used for impersonation and spear-phishing attacks against their organization.

AI-Enabled Attacks During Access & Penetration

56% of AI-enabled cyber attacks occurred during the access and penetration phase. **12%** were demonstrated in exploitation.

Despite these concerns, over half of enterprises report relying on AI for threat detection, leading prediction, and response. Additionally, 27% plan to implement security safeguards that leverage AI and machine learning.

What's Driving the Need for AI in Cybersecurity?

The Rise of Bots

of the internet consists of bots. Malicious bots create immense risk for organizations as they can be used for hacking, spamming, and compromising websites.

The average response time to cyber attacks varies depending on the size of the attack, the techniques used, and an organization's capability to respond. On average, **the time it takes to respond to an attack is 19 days.**

The Frequency and Complexity of Cyber Threats

The Rise of Social Engineering Attacks & Human Error

According to Verizon's 2023 DBIR,

of breaches involved the human element, which includes social engineering attacks, errors, or misuse. Through our extensive research, we know that **8% of users cause 80% of security incidents.**

The Future of AI in Cybersecurity

Nearly one-quarter of the AI software market will consist of cybersecurity by 2025.

The fastest-growing category of AI spend is cybersecurity. This category is rising at a **CAGR of 22.3%**

AI Will...

Help Security Leaders Make Data-Driven Decisions

By ingesting and analyzing vast amounts of diverse data, AI systems can swiftly identify patterns, anomalies, and potential threats that might evade human detection.

These insights provide security leaders with a comprehensive and real-time understanding of their organization's security posture.

AI enhances the decision-making process by converting raw data into actionable intelligence, bolstering security strategies and fostering a safer environment.

Augment Security Nudges & Access Control Policies

AI algorithms can gather and analyze data from various sources, such as identity platforms, email security and web gateways, endpoint management solutions, and more.

The analysis of this data would help AI identify patterns in user behavior and actions to determine optimal moments for delivering cybersecurity nudges.

By **leveraging AI-powered insights, organizations could strategically and automatically time nudges to align with users' online activities,** maximizing their impact and engagement.

Be Used to Detect Security Threats Automatically

AI can automatically detect cybersecurity threats in real time and around the clock.

AI can increase detection rates upwards of...

Be Used to Detect and Prevent User Risk

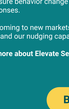
AI can be used to analyze users' historical data and interactions to **automate safeguards and responses to high-risk users.**

This analysis can provide valuable insights into an employee's cybersecurity vulnerabilities and automatically place stronger email security and web gateways controls on risky users, significantly decreasing the number of events to which they need to respond.

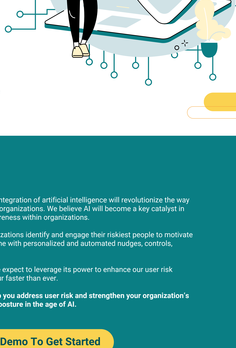
Increase the Efficiency of Incident Response Processes

Responding to cyber incidents can take days, even weeks, or months. AI can and will continue to speed up the response to these attacks.

of global executives report AI allows their organization to respond faster to breaches.



also believe AI is "necessary for an effective response to a cyberattack."



Final Thoughts

As the digital realm continues to evolve, the integration of artificial intelligence will revolutionize the way security teams protect their people and their organizations. We believe AI will become a key catalyst in reducing user risk and boosting security awareness within organizations.

Tools like Elevate Engage already help organizations identify and engage their riskiest people to motivate and measure behavior change in near real-time with personalized and automated nudges, controls, and responses.

With AI coming to new markets every day, we expect to leverage its power to enhance our user risk platform and our nudging capabilities to occur faster than ever.

Learn more about Elevate Security can help you address user risk and strengthen your organization's security posture in the age of AI.

Book Your Demo To Get Started

About Elevate Security

Elevate Security helps enterprise security leaders gain deep visibility into their biggest workforce security risks. Using Elevate Security, CISOs can fundamentally transform beyond simply managing incidents on a day-to-day basis into proactively addressing their riskiest users with our automated playbooks. Elevate Security's SaaS platform integrates with leading SIEM vendors, HR Systems, Identity products, and other popular security technologies to provide a Human Risk Score which allows security teams a deep understanding of each and every individual's risk and potential "blast radius" if they were breached.

For more information, please visit elevatesecurity.com |