EM360 | ENTERPRISE MANAGEMENT 360

INDUSTRY REPORT

The Intersection of AI in Cybersecurity: A 2024 Industry Report

This report explores the impact of Artificial Intelligence (AI) on cybersecurity. It examines AI's role both as a defence mechanism and a weapon for sophisticated cybercrime with case studies and expert commentary to demonstrate how security teams can leverage AI to defend against evolving cyber threats.

Table of contents

About EM360Tech

Audience

EM360Tech has a global audience of **over 640,000 active users** made up of IT experts, business leaders and industry analysts from across the enterprise landscape.

Scope

Our content delves deep into the latest trends in **AI**, **cybersecurity**, **data**, **infrastructure management** and **emerging technologies**, providing actionable insights and community analysis.

Enterprise Management 360 (EM360Tech) is the only place where IT experts and business leaders converge to discuss the latest tech trends, share insights, and shape the future of enterprise technology.

Our vibrant community of over 640,000 thought leaders and industry experts are the driving force behind the next big tech breakthroughs, providing our community with the knowledge, tools, and strategies to turn technology into a force for innovation.

Our content is made for IT leaders, by IT leaders. Whether it's **data**, **cybersecurity**, **AI** or **infrastructure management**, our dynamic team of editors work closely with trusted industry advisors and analysts to provide actionable insights and community analysis across the enterprise tech landscape.

Join EM360Tech to access exclusive analyst-led content, connect with industry leaders and tap into our global community of tech leaders and industry experts as you gain insights and expand your network.

Our content

Analyst-led products

The award-winning EM360 Podcast pairs trusted industry analysts with leading technology companies to discuss the latest industry trends and solutions in the enterprise tech landscape.

Tech articles

Our tech articles delve deep into the latest news and analysis across the enterprise tech world, whether it be the latest AI innovation or large-scale cyber attack.

Top 10s

Our Top 10s delve deep into different areas of the enterprise landscape to find the ten top trends or providers that are shaping the field.

Industry Interviews

The EM360Tech editorial team attends various industry events to speak to industry experts and our partered analysts about all things enterprise tech.

Executive summary

Artificial intelligence (AI) is transforming cybersecurity in a manner like that of the dot-com era's disruptive influence. Its integration into organisational processes is no longer optional but necessary, driven by advancements in technology and cloud computing.

The appeal of AI in cybersecurity lies in its ability to provide real-time threat detection, automation, and proactive defence for security teams. But as cybercriminals also exploit the technology to launch sophisticated, AI-powered attacks, it is becoming a double-edged sword.

This report delves into AI's increasingly complex role in cybersecurity, exploring how organizations are leveraging the technology to improve their security posture and dissecting the challenges that can arise when they do so.

It examines how machine learning (ML) intertwines with AI to bolster security, bringing prediction and even identification of potential new threats before they happen. We provide case studies that examine how different industries can implement an ML-driven solution, resulting in improved threat prediction, faster response times and improved protection of data.

The report also takes a look at other emerging technologies, such as blockchain and IoT, exploring their impact on cybersecurity and the challenges they've brought with them while showcasing expert-backed best practices for implementing them correctly.

We hope this report gives you the insights, and knowledge to enable you and your organisation to better harness the power of AI and other emerging technologies in your cybersecurity strategy.

Michael S Lodge

Michael Lodge
CEO at EM360Tech

Emerging technologies in cybersecurity

> AI is not going to pan out the way everybody thinks it's going to pan out. I think AI is here to stay and is going to revolutionise the industry, but I don't think it's going to go the way many people think it is.[1]

Joshua Chessman
Advisor at Lionfish Tech Advisors

Artificial Intelligence (AI) is emerging as the defining technological advancement of the decade. Its transformative potential is a focal point at every business across the technology landscape and within companies in various industries. The drive to integrate AI into organisational processes has become almost universal, reflecting the potential value and anticipated impact of the technology across the enterprise landscape

While development generative AI has accelerated since the explosive launch of OpenAI's large language model (LLM) ChatGPT in 2022, AI has been a field of study and development for over sixty years. Many of the AI algorithms used today are not new but are now feasible due to the convergence of several key technologies. These include advancements in GPU technology, which provides the necessary computational power to process and interpret vast amounts of data, and the massive connectivity offered by cloud computing, which allows data to be collected, exploited, and utilised at scale. [2]

As the AI revolution burns on, cybersecurity experts are being forced navigate this rapid evolution; both for its opportunities and dangers.

Some of the biggest trends expected in 2024 are:

Over **50%** of companies plan to incorporate AI technologies in 2024.[3]

56% largest % of AI usage is held by Customer service.[4]

51% of AI usage is in Cybersecurity and fraud prevention.[4]

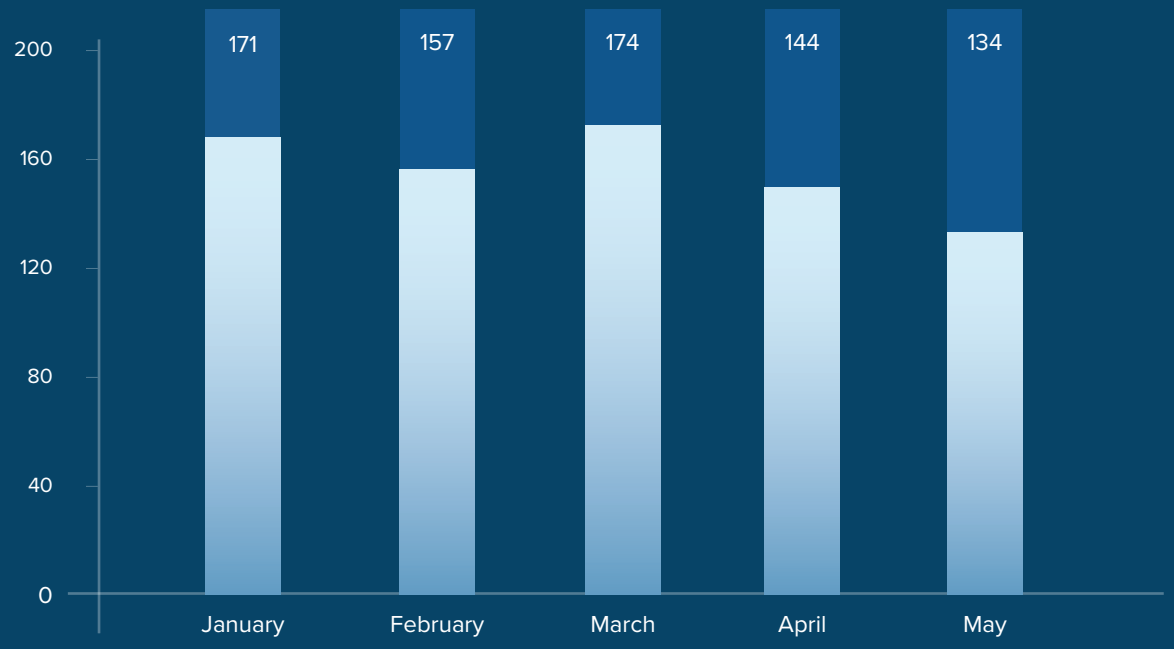
58% of companies in China have implemented AI solutions, leading globally in AI deployment within businesses as of 2024.[5]

1. Paulina Rios Maya (Host) (2024). In The Cybersecurity Strategist, EM30Tech
2. Brett et al., 2017
3. Data Hub, 2024
4. Haan, 2024
5. IBM, 2024

Developers actively create and share new AI programs on platforms like Product Hunt. Once development is complete, Product Hunt is the go-to site for launching these innovations. Analysing the latest products launched on Product Hunt offers insights into the direction of pre-seed companies. EM360Tech found that over the first five months of 2024, the number of new AI products receiving over 100 upvotes has steadily increased, indicating their popularity on the platform (See table below).

Number of New AI Products listed on Product hunt

January - May 2024



Source: EM360Tech

While expected by many, this surge in AI development is being compared to the transformative impact of the dot-com era. Some industry leaders have even dubbed this phenomenon "bigger than .com," [6] highlighting the trend of companies rebranding to incorporate '.ai' in their names to signify their commitment to AI integration.

Adopting AI is now not merely a trend but a strategic imperative driven by its promise to revolutionise the industry, enhance operational efficiencies, and fortify its measures. As organisations continue to explore and implement AI solutions, its role in shaping the future of business and technology becomes increasingly critical.

This section is a deep dive into the transformative impact of emerging technologies, with a special focus on AI's impact on the cybersecurity industry.

We aim to shed light on two pivotal questions:

Opportunities for improvement

How can AI and other emerging technologies enhance cybersecurity measures and protect products more effectively?

Risks and exploitation

Conversely, how might these technologies be leveraged by malicious actors to exploit information systems and compromise organisational functions?

6. Paulina Rios Maya (Host) (2024). In Tech Transformed. EM30Tech.

Opportunities for improvement

> Looking forward, the most significant threats will involve AI-powered attacks capable of rapid adaptation and surgical precision. Enterprises and startups must adopt a multi-layered strategy, incorporating AMTD and other innovative measures, to withstand the increasingly sophisticated assaults of the future.[7]

Brad Laporte
Advisor at Lionfish Tech Advisors

AI and emerging technologies are revolutionising cybersecurity, offering unprecedented threat detection and response capabilities. For industry leaders, understanding and leveraging these advancements is critical to protecting products and systems effectively.

It is crucial for industry leaders and enterprises to understand the advantages and disadvantages of utilising AI and other emerging technologies to enhance cybersecurity measures and protect their products more efficiently. This section provides an in-depth analysis of some of the most significant advancements in this area:

Real time data analysis and threat detection

AI systems excel at processing and analysing vast amounts of data in real-time, which is essential for identifying patterns and anomalies indicative of cyber threats.[8] Traditional security measures often struggle with the sheer volume of data generated in today's digital environments. AI's ability to sift through this data rapidly and accurately allows for the early detection of sophisticated threats.

7. Paulina Rios Maya (2024). Interview with Brad Laporte. EM360Tech.
8. NCSC, 2024

Case study

XYZ Corporation, a global leader in the financial services industry, faced increasing challenges in protecting its vast and complex IT infrastructure from sophisticated cyber threats. With millions of transactions processed daily, the company needed a robust, real-time threat detection system that could monitor and analyse large volumes of data quickly and accurately.

XYZ Corporation's traditional security measures struggled to keep pace with evolving threats. The sheer volume of data generated by its operations made it difficult to identify and respond to threats promptly. The company experienced several incidents where breaches were detected too late, resulting in significant financial and reputational damage.

Solution

XYZ Corporation implemented an advanced AI-driven cybersecurity solution focused on real-time data analysis and threat detection to address these challenges. The critical components of the solution includes:

- AI-powered SIEM (Security Information and Event Management)
- Machine Learning Algorithms
- Automated Response Mechanisms
- Integration with IoT Devices

The implementation process involves several steps:

- **Data integration:** The first step was integrating various data sources into the AI-powered SIEM system. This included network traffic logs, user authentication records, transaction data, and IoT sensor inputs.
- **Model training:** ML models were trained using historical data, including records of known threats and benign activities. This training enabled the system to differentiate between normal and suspicious behaviour accurately.
- **Deployment and testing:** The system was deployed in a controlled environment for initial testing. Real-time data feeds were monitored to ensure the AI algorithms could detect and respond to threats effectively.
- **Full-scale rollout:** The solution was rolled out across XYZ Corporation's entire IT infrastructure after successful testing. Continuous monitoring and fine-tuning ensured optimal performance.

Some of the benefits of the implementation of AI-driven real-time data analysis and threat detection gave the following benefits for XYZ Corporation:

- Improved threat detection.
- Reduced response time
- Enhanced operational efficiency
- Lowered financial and reputational risk

The case of XYZ Corporation demonstrates the transformative impact of AI and real-time data analysis in cybersecurity. The company significantly improved its threat detection and response capabilities by leveraging advanced machine learning algorithms and automated response mechanisms.

Machine Learning and predictive capabilities

Machine learning (ML), a core component of AI, enhances threat detection by continuously learning from previous incidents and adapting to new attack vectors. This learning process improves the accuracy of threat identification, enabling security systems to detect known threats and predict and identify emerging ones.[9] Industry leaders can leverage these predictive capabilities to anticipate potential attacks and implement preventative measures, thereby reducing the risk of breaches.

Beyond protecting sensitive data, including personal and financial information, reducing breach risk is crucial for maintaining trust and safeguarding reputation. A single breach can erode the confidence of customers, partners, and stakeholders, leading to long-term damage. Moreover, the financial repercussions are significant, encompassing not only the direct costs of the breach but also the expenses associated with regulatory fines, legal fees, and remediation efforts.

9. Loaiza et al., 2019

Case study

ABC Healthcare, a leading provider of healthcare services, operates numerous hospitals and clinics across the country. The organisation handles vast amounts of sensitive patient data and relies heavily on its IT infrastructure for operations. With the increasing frequency of cyber threats targeting the healthcare industry, ABC Healthcare needed a robust solution to enhance its cybersecurity measures, particularly focusing on predictive capabilities to prevent attacks before they could occur. ABC Healthcare faced several challenges, including the need to protect sensitive patient information from breaches, managing an increasing volume and complexity of sophisticated cyber threats, and addressing the limitations of existing security measures that were largely reactive, leading to delays in threat detection and response.

Solution

To address these challenges, ABC Healthcare implemented a machine learning-driven cybersecurity solution to enhance its predictive capabilities. The key elements of this solution includes:

- Machine Learning Models
- Predictive Analytics
- Real-Time Monitoring
- Automated Threat Hunting

The implementation process involves several steps:

1. **Data collection and integration:** Historical data, including records of past cyber incidents, network traffic logs, and user activity, were aggregated and fed into the machine learning models.
2. **Model training and validation:** Machine learning models were trained using this historical data to recognise patterns associated with both benign and malicious activities. The models were then validated and fine-tuned to ensure high accuracy.
3. **Deployment and continuous learning:** The trained models were deployed across ABC Healthcare's IT infrastructure. Continuous learning mechanisms were established, allowing the models to adapt to new data and evolving threats.
4. **Automated response systems:** Automated response protocols were integrated, enabling immediate action upon detection of potential threats.

The deployment of machine learning and predictive capabilities yielded significant improvements for ABC Healthcare:

- Enhanced threat prediction
- Reduced incident response time
- Increased accuracy
- Improved resource allocation

The case of ABC Healthcare demonstrates the powerful impact of machine learning and predictive capabilities in cybersecurity. By leveraging advanced algorithms and real-time data analysis, the organisation significantly bolstered its defences, moving from a reactive to a proactive security posture. This case study underscores the importance of adopting machine learning-driven solutions to anticipate and mitigate cyber threats, ensuring the protection of sensitive data and the smooth operation of critical services.

Automation of security tasks

> Automation is crucial for improving operational efficiency, allowing human resources to focus on more complex and strategic cybersecurity challenges.

AI can also automate routine security tasks such as monitoring network traffic, analysing logs, and responding to low-level alerts. This automation is crucial for improving operational efficiency, allowing human resources to focus on more complex and strategic cybersecurity challenges. Implementing automation is key to operational enhancement, particularly within cybersecurity firms. By automating mundane tasks and processes such as threat detection and incident response, these companies can optimise operational efficiency significantly. This strategic utilisation of automation not only streamlines workflows but also liberates human resources to focus on tackling more intricate and strategic cybersecurity challenges. [10]

This shift allows skilled professionals to allocate their expertise where it's most needed, thereby fortifying the company's ability to respond adeptly to evolving threats. Consequently, cybersecurity firms can augment their competitive advantage by delivering higher-value services and increasing their capacity to navigate threats and vulnerabilities.

10. Palo Alto, 2024

Case study

GHI Tech, a leading technology company, handles vast amounts of sensitive data and is frequently targeted by cyber threats. To stay ahead in the competitive tech industry and ensure the security of its data and systems, GHI Tech needed to enhance its cybersecurity measures. The company decided to implement automation to streamline and improve its security operations.

GHI Tech encountered significant challenges in its cybersecurity operations, including a high volume of security alerts inundating its security operations centre (SOC) on a daily basis, posing difficulties in discerning genuine threats from false positives. Moreover, reliance on manual processes for security tasks led to inefficiencies and heightened the risk of human error. Additionally, the company grappled with slow incident response times, prolonging the duration required to detect, investigate, and mitigate security incidents, thereby elevating the potential for substantial damage from cyber attacks.

Solution

To overcome these challenges, GHI Tech implemented an automated security solution that includes the following components:

- Security Orchestration, Automation, and Response (SOAR)
- Automated Threat Intelligence
- Automated Incident Response

The implementation process involves several steps:

- **Integration of security tools:** The SOAR platform was integrated with GHI Tech's existing security tools, including firewalls, intrusion detection systems, and SIEM (Security Information and Event Management) systems.
- **Development of automated playbooks:** Security analysts developed automated playbooks for common security incidents, such as phishing attacks, malware infections, and unauthorised access attempts.
- **Training and testing:** The security team was trained on the new system, and extensive testing was conducted to ensure the automated processes were effective and reliable.

The implementation of automated security tasks yielded significant benefits for GHI Tech:

- Improved efficiency
- Faster incident response
- Reduced human error
- Enhanced threat detection

The case of GHI Tech demonstrates the transformative impact of automating security tasks on improving cybersecurity operations. By implementing a SOAR platform and automating routine tasks, GHI Tech enhanced the efficiency and effectiveness of its security measures, leading to faster incident response times and a stronger security posture. This case study highlights the importance of leveraging automation to address the growing complexity and volume of cyber threats in the technology sector.

Integration with emerging technologies

In the same vein, emerging technologies like blockchain and the Internet of Things (IoT) further enhance AI-driven security measures.

For instance, blockchain's decentralised architecture ensures data integrity and transparency, making it invaluable for authentication and securing data exchanges. Concurrently, the proliferation of IoT devices enriches data repositories, empowering AI algorithms to detect anomalies and thwart potential security breaches in real-time.

Similarly, blockchain's immutable ledger ensures data integrity and transparency, making it more difficult for attackers to alter information without detection. IoT devices equipped with AI capabilities can monitor their environment and report anomalies, providing an additional layer of security.

This symbiotic relationship between blockchain, IoT, and AI fosters robust cybersecurity ecosystems, enabling organisations to proactively safeguard against diverse cyber threats while enhancing operational efficiency and resilience

Case study

JKL Logistics, a global logistics and supply chain management company, operates a vast network of warehouses, transportation fleets, and distribution centres worldwide. With the increasing complexity and security challenges in the logistics industry, JKL Logistics recognised the need to leverage emerging technologies to enhance operational efficiency and ensure the integrity and security of its supply chain.
JKL Logistics faced critical challenges in its supply chain management operations. Ensuring data integrity and transparency across the supply chain network was critical to combat fraud, theft, and counterfeit goods. Real-time tracking of assets, including inventory, vehicles, and shipments, was essential for optimising operations and minimising disruptions. Moreover, building trust among stakeholders, such as customers, suppliers, and regulatory authorities, required robust security measures to protect sensitive data and prevent unauthorised access or tampering. These challenges underscored the need for comprehensive solutions to enhance transparency, streamline asset management, and bolster security in JKL Logistics' supply chain processes.

Solution

To address these challenges, JKL Logistics implemented a comprehensive solution that integrated emerging technologies such as blockchain and the Internet of Things (IoT) into its supply chain operations. The key elements of the solution includes:

- Blockchain-based Supply Chain Platform
- IoT-enabled Asset Tracking
- Smart Contracts and Automated Transactions

The implementation process involves several steps:

- **Infrastructure setup:** JKL Logistics established the necessary infrastructure, including blockchain nodes, IoT sensors, and connectivity solutions, to support integrating emerging technologies into its supply chain operations.
- **System integration:** The blockchain platform and IoT devices were integrated with existing supply chain management systems, ERP (Enterprise Resource Planning) software, and logistics platforms to enable seamless data exchange and interoperability.
- **Pilot testing:** A pilot project was conducted to test the functionality and performance of the integrated solution in a controlled environment. Feedback from stakeholders was gathered to fine-tune the system and address any issues or concerns.
- **Full-Scale deployment:** Upon successful pilot testing, the integrated solution was deployed across JKL Logistics' entire supply chain network, encompassing warehouses, distribution centres, transportation fleets, and partner facilities.

The integration of blockchain and IoT technologies yielded significant benefits for JKL Logistics:

- Enhanced Data Integrity
- Improved Asset Visibility
- Streamlined Operations
- Enhanced Trust and Compliance

JKL Logistics showcases how blockchain & IoT revolutionize supply chains. These technologies boosted data integrity, visibility, efficiency, and trust, solidifying JKL's position as a logistics leader. This case underlines the importance of embracing innovation to tackle evolving challenges and opportunities.

Analyst take

Jonathan Care
Advisor at Lionfish Tech Advisors

In the past few years, the cybersecurity threat landscape has undergone significant transformations, becoming more sophisticated and multifaceted. Previously, threats were largely confined to malware and phishing attacks. However, recent trends have seen a rise in ransomware, state-sponsored attacks, and supply chain vulnerabilities, targeting not just large corporations but also small businesses and startups. This evolution is largely driven by technological advancements and the increasing value of digital data.

The most significant threats looming on the horizon for enterprises and startups alike include AI-powered attacks, which can learn and adapt to security measures, and deepfake technology that can bypass biometric securities. Furthermore, as the Internet of Things (IoT) continues to expand, the sheer number of connected devices presents a growing attack surface.

Predictively, cybersecurity in the near future will have to contend with quantum computing, which can potentially break traditional encryption methods, thereby jeopardizing data security across all sectors. Organizations, therefore, must remain vigilant, continuously updating and adapting their security strategies to fend off these evolving threats. [11]

11. Paulina Rios Maya (2024). Interview with Jonathan Care. EM360Tech.

Strategic insights for implementation

While these case studies highlight the significant advantages of integrating AI into organisational systems, enterprises must exercise caution and thorough consideration before making substantial investments in these technologies.

Leaders must recognise that investing in AI entails more than just financial commitment; it also necessitates adequate training and upskilling of staff to use these tools effectively. This is particularly crucial in critical industries such as healthcare and defence, where the stakes are high, and the proper use of AI can have profound implications for operations and outcomes.

In this section, we delve into essential considerations and potential pitfalls to consider before investing in AI technologies for enterprise implementation. For industry leaders, the implementation of AI and emerging technologies requires a few key considerations:

Data quality and diversity

While AI is often hailed as the future of threat intelligence, many industry leaders overlook the critical need for high-quality, diverse data sets to train these AI systems.

AI is indeed revolutionising the industry. However, it is crucial to temper expectations with a realistic understanding of its current capabilities. AI systems can analyse vast amounts of data and execute tasks as programmed, enhancing efficiency and enabling new possibilities. Yet, it is important to recognise that AI does not possess human-like understanding or intuition. AI operates based on predefined algorithms and data inputs, executing tasks as instructed. This means that while AI can process data and identify patterns, its responses are not truly autonomous or real-time in the human sense. It follows programmed instructions and learns from data, but its decision-making capabilities are limited to its training and programming scope.

Human oversight

While AI can automate many aspects of cybersecurity, human expertise remains essential. Security professionals must oversee AI operations, interpret complex threat landscapes, and make strategic decisions based on AI insights.

There is a prevalent belief that AI will solve all cybersecurity challenges, but it is essential to recognise that human expertise remains crucial. AI is a powerful tool, but it cannot replace the nuanced understanding and interpretation that security professionals provide.

> **Enterprises must understand that AI enhances, rather than replaces, the capabilities of human analysts and solution providers.**

AI can significantly reduce analyst burnout by automating routine tasks and processing vast amounts of data quickly and accurately.[12] This allows human experts to focus on more complex and strategic aspects of cybersecurity. However, the successful implementation and operation of AI systems still require skilled professionals to interpret outputs, manage systems, and address issues that AI might overlook.

Thus, while AI will transform the way we work by increasing efficiency and enabling more proactive threat detection and response, it will not eliminate the need for human expertise within organisations.

> **Ensuring that AI systems run smoothly and effectively will always depend on the knowledge and skills of experienced cybersecurity professionals.**

12. Wilner, 2018

Aparna Sundararajan

Director, CyberCX

Aparna, an ex-Gartner analyst, is a trusted technology expert for global C-suite leaders, specializing in AI, Cloud, data analytics, blockchain, and cybersecurity transformation challenges and solutions.

QUESTION

How should organisations balance their reliance on technology with human factors in cybersecurity?

People are your first line of defense. People are also your weakest link! There are three emerging technologies that are bound to become the digital building blocks of our evolving world. Artificial intelligence (AI), Distributed Ledger technology (DLT), and Quantum Computing.

AI is reshaping the cyber security threat landscape and is creating unprecedented levels of attack sophistication. Simultaneously, organisations are exploring AI to enhance their threat detection, monitoring, and response capabilities. However, AI used for cyber-attacks currently exceeds AI used for cyber defense.

DLT is being explored to have potential to truly build secure-by-design systems while Quantum computing is expected to completely disrupt encryption methods as we know them today.

Amongst these three technologies, organisations will benefit the most from investing in trainings pertaining to secure AI usage for business growth, while deploying AI in cyber defense areas of threat & vulnerability detection, incident monitoring & alerting and risk assessments.

Continuous improvement

The threat landscape is constantly evolving. Continuous improvement and updating of AI systems and cybersecurity protocols are necessary to stay ahead of emerging threats. Integrating AI brings significant benefits[13] but also introduces new challenges, including the necessity for continuous improvement and maintenance.[14]

As AI systems become an integral part of cybersecurity infrastructure, **organisations face the burden of keeping their traditional security measures up to date while ensuring that their AI tools are current and effective.** This added layer of responsibility means that security analysts must monitor and mitigate imminent threats and address vulnerabilities within the AI systems themselves.

The need for regular updates and improvements in AI technology underscores the importance of vigilance and proactive management. Organisations must allocate resources to maintain and enhance their AI capabilities, ensuring that these systems operate optimally and securely. By doing so, they can fully leverage AI's advantages while mitigating the risks associated with its implementation.

Thus, while AI can significantly enhance threat detection and response, it also requires a commitment to continuous improvement and careful oversight. Companies must be prepared to invest in the ongoing development and updating of their AI systems to stay ahead of emerging threats and maintain robust cybersecurity defences.

Cross-functional collaboration

Effective cybersecurity requires collaboration across various functions within an organisation. Integrating AI-driven security measures with broader business processes ensures a cohesive and comprehensive security strategy.

This misconception leads to frequent missteps and a lack of expertise. For example, an analyst may have an engineering background, securing their position through technical skills, while another may have honed their abilities through practical experience as a hacker. This disparity often results in a skills gap within cybersecurity teams.

Continuous staff training is essential to mitigate this issue. However, enterprises must consider the substantial investment required to train individuals who have entered the field due to a passion for computers rather than formal education. Before adopting new technologies and following industry trends, organizations must assess their current capabilities and the expertise of their personnel. Cross-functional teams, while valuable for bringing

> In the realm of cybersecurity, one significant challenge that many thought leaders have encounteredisthemisconception that cybersecurity is inherently difficult. [15]

Joshua Chessman
Advisor at Lionfish Tech Advisors

13. Calderon, 2019
14. DarkTrace, 2024
15. Paulina Rios Maya (Host) (2024). In The Cybersecurity Strategist. EM30Tech.

diverse perspectives, can exacerbate expertise gaps if not managed properly. When team members from various backgrounds—such as IT, engineering, and operations—collaborate, their differing levels of cybersecurity knowledge can lead to misunderstandings and inefficiencies. It is crucial for organisations to ensure that all team members have a fundamental understanding of cybersecurity principles to facilitate effective collaboration. Integrating AI requires a workforce capable of understanding and effectively utilizing these systems.

While investing in AI and other emerging technologies can enhance cybersecurity, organisations must evaluate their existing capabilities and invest in ongoing staff training. This approach ensures that technology adoption is supported by a knowledgeable and skilled workforce, minimising risks and maximising the benefits of new innovations.

> **Enterprises must determine whether to focus on foundational issues and staff training or invest in advanced technologies like AI.**

Conclusion

In conclusion, AI and other emerging technologies significantly enhance cybersecurity measures by enabling more efficient threat detection, rapid response to incidents, and proactive defence strategies. These technologies provide advanced tools to safeguard products, ensuring robust protection against evolving cyber threats.

AI's ability to analyse vast amounts of data in real-time allows for the identification of patterns and anomalies that might indicate a security breach. ML algorithms continuously improve by learning from past incidents, which helps in predicting and mitigating future threats more effectively.

Furthermore, the integration of AI with other technologies, such as blockchain and the Internet of Things (IoT), offers a multi-layered defense approach, enhancing the overall resilience of security frameworks. Automated responses reduce the time taken to counteract attacks, minimizing potential damage. By leveraging AI, businesses can improve their security posture, protect sensitive data, and maintain the integrity of their operations in an increasingly digital landscape. As cyber threats become more sophisticated, the adoption of AI-driven solutions will be essential for staying ahead in the fight against cybercrime.

With this in mind, several critical considerations demand attention before investing in these technologies. Firstly, the quality and diversity of data sets must be thoroughly evaluated, as AI's efficacy heavily relies on the availability of robust data for training. Moreover, human oversight remains paramount, acknowledging that while AI can automate numerous tasks, human expertise is indispensable for deciphering intricate threat landscapes and making informed decisions.

Continuous improvement is equally imperative, necessitating regular updates and enhancements to AI systems and cybersecurity protocols. Additionally, fostering cross-functional collaboration within the organisation is vital to ensure a unified and comprehensive approach to cybersecurity. By meticulously considering these factors, enterprises can harness the full potential of AI technologies while effectively managing associated risks and challenges.

Risks and exploitation

Trust in AI technologies such as ML and neural networks to perform cybersecurity tasks is a double-edged sword. While AI can significantly enhance cybersecurity practices, it can also introduce new vulnerabilities, as AI applications themselves can become targets of sophisticated attacks, posing severe security threats.[16] In this section, we delve into the potential exploitation of information systems by malicious actors by utilising emerging technologies, thereby jeopardising organisational functions.

While cybersecurity leaders are often cognizant of these risks, EM360Tech asserts that this report serves as a capacity-building resource for enterprises and individuals. By shedding light on how these technologies can be leveraged for nefarious purposes, this report aims to equip stakeholders with the knowledge and strategies necessary to fortify their defences against cyber threats.

AI chatbots

Attackers can leverage AI in several ways, with one of the most accessible methods being using AI chatbots. Just as individuals use chatbots to assist with tasks such as drafting resumes or composing emails, attackers use them to craft more convincing phishing attacks with fewer detectable errors.

Enhanced phising attacks

Traditional phishing attempts often rely on poorly written emails with clear signs of fraud, such as grammatical errors and generic language. AI chatbots, however, can generate highly convincing phishing emails that are grammatically correct, contextually appropriate, and personalised. This sophistication makes it much harder for recipients to distinguish phishing emails from legitimate communications, thereby increasing the success rate of these attacks.

> In 2023, Kaspersky reported that phishing pages imitating global internet portals (16.46%) regained the top position in terms of attempted redirects. Moreover, threat actors also targeted users of smaller web services (14.66%), indicating a broadened scope of interest in their malicious activities.

16. Taddeo et al., 2019

Arik Atar

Senior Threat Intelligence Researcher, Radware

Arik Atar joins Radware's Threat Research team, bringing his 7-year cyber threat hunting expertise. From uncovering attacker tactics to hunting application threats, his diverse background offers unique insights on application security.

QUESTION

How might future advancements in GPT and similar technologies reshape cyber threats?

Host - Alejandro Leal
Analyst at KuppingerCole

First of all, the creative ways in which LLMs are being exploited are constantly evolving. So, the first of it will be staying up on the news. And if we are talking about the news, recently, there has been a huge discussion about a new attack vector on GPT itself, which is AI package hallucination.

In this case, we came across—I think it was two weeks ago—it was published all around the medium that a group of hackers basically asked GPT a lot of questions related to coding, and when it provided a lot of false names of software packages, libraries, and Python-like libraries, they created those libraries and then injected malicious code within them.

So anyone else that went to these libraries and downloaded automatically was providing them a backdoor to his infrastructure. This is a really sophisticated and simple threat because it doesn't evolve with manipulating the database of ChatGPT. It's just using and exploiting the hallucinations, the incorrects so they can spread their own malware.

So basically this impact is across all programming languages. While Python and Node are particularly vulnerable due to their open package ecosystems, languages like Go and Net are inherently, they have inherent protection due to their structure, such as lack of centralized repository or the use of reversed prefixes.

Which prevent easy expectations so first there are more vulnerable languages than others this is something that we need to acknowledge and mitigation strategies the first one is an awareness because it's like every new technology involvement in the beginning we have 100 % trust in it and afterwards, we understand those scams.

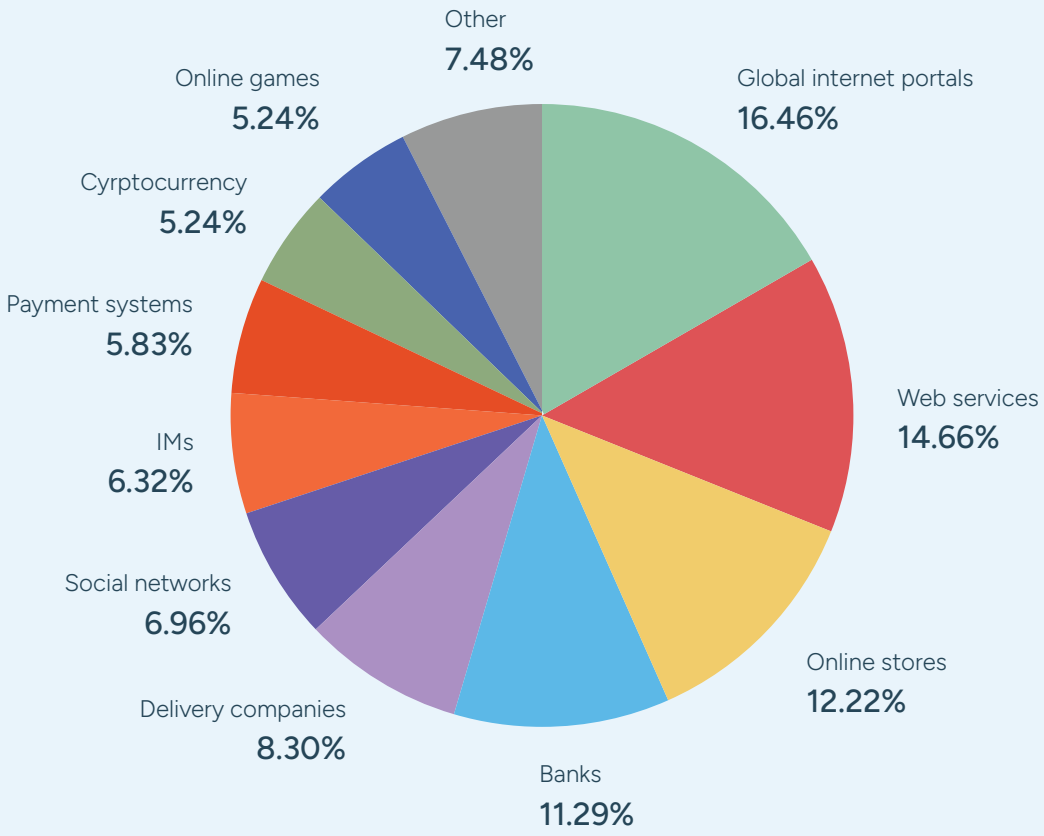
Fake websites

Creating a fake website, particularly for malicious purposes like phishing, is both unethical and illegal. However, understanding how such websites are crafted can help develop robust defences against them.

Websites crafted with AI leverage advanced technologies to streamline the design, development, and maintenance processes, ensuring high efficiency and customisation. AI-driven tools can automatically generate website templates, design layouts, and even create content based on user preferences and behaviour.

These tools utilise machine learning algorithms to analyse large datasets, understanding trends and user interactions to optimise user experience and interface design. AI can also integrate chatbots for real-time customer support, personalise content to individual users, and enhance security by detecting and mitigating potential threats.

Fake website examples[17]



17. Kulikova et al., 2021

When discussing malicious actors, it's crucial to grasp how they exploit AI to fabricate these deceptive websites:

Typosquatting

- Registering domains that are slight misspellings of legitimate websites (e.g., "gooogle.com" instead of "google.com").
- Using Similar Characters: Using characters that look similar to legitimate ones (e.g., using "rn" instead of "m").

Website cloning

- **Copying HTML/CSS:** Duplicating the look and feel of a legitimate website by copying its HTML, CSS, and JavaScript.
- **Content Duplication:** Reproducing content such as logos, text, and images from the legitimate site.

Phishing mechanisms

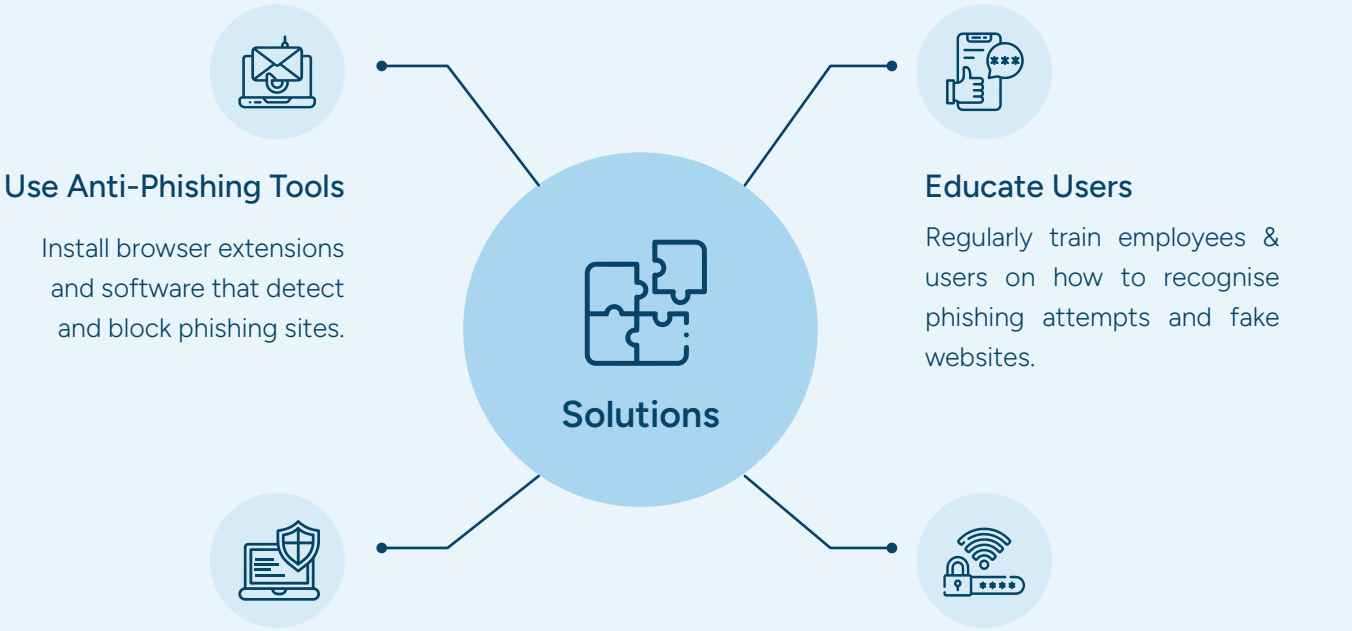
- **Fake Forms:** Creating forms that capture user credentials, credit card information, etc.
- **Malicious Links:** Embedding links that lead to malicious downloads or further phishing pages.

Hosting and SSL certificates

- **Hosting:** Using low-cost or free hosting services to set up the fake site.
- **SSL Certificates:** Obtaining SSL certificates to make the fake site appear secure (e.g., showing "https" in the URL).

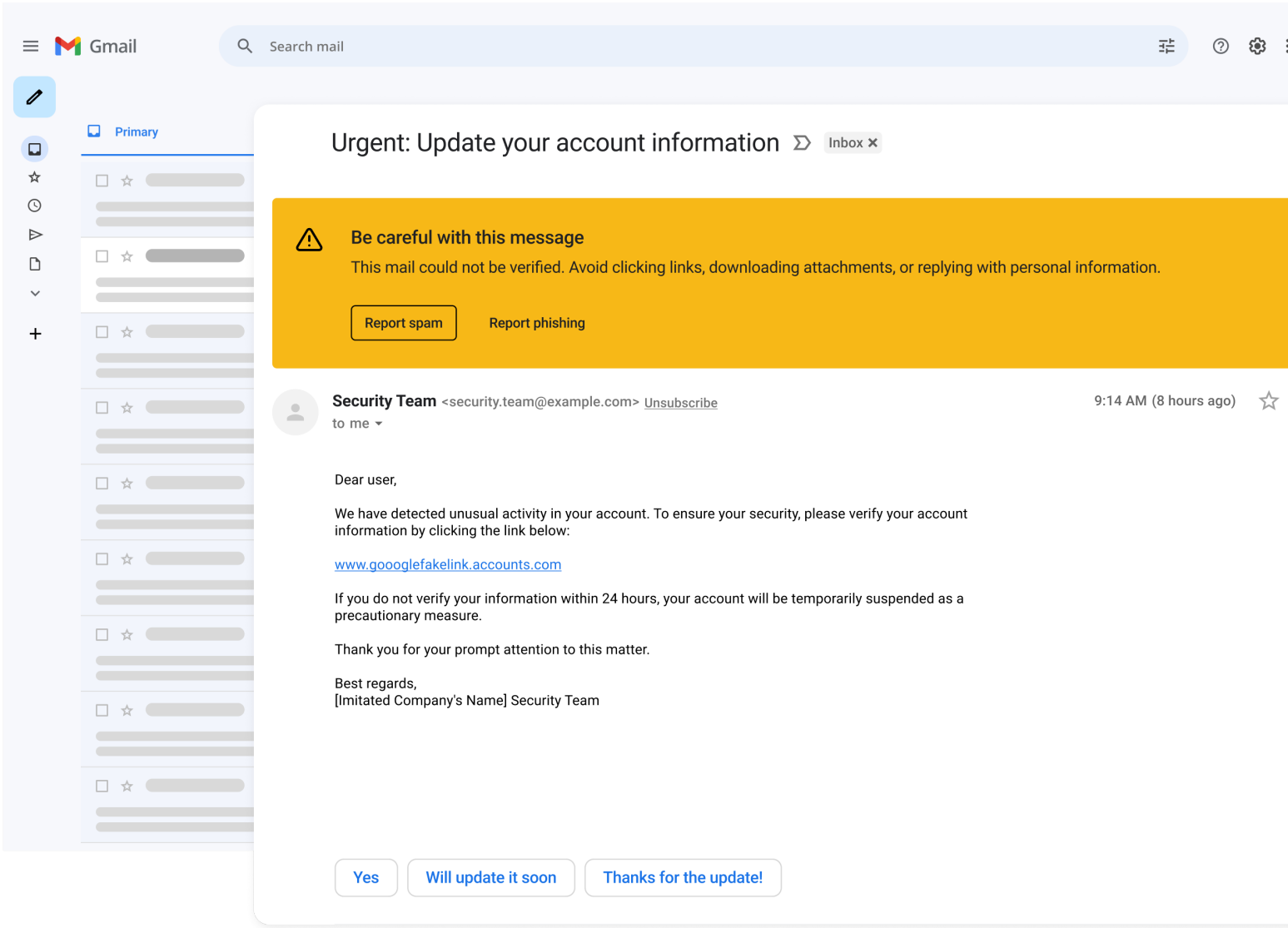
Defending against fake websites

In defending against potential attacks by fake websites, it is crucial for organisations to adopt a proactive and specialised approach. Establishing a dedicated monitoring team to oversee and counter these threats is crucial. For instance, in the e-commerce sector, such attacks can result in substantial financial losses, often amounting to thousands of dollars. Any sales diverted to fraudulent websites directly impact the organization's revenue. Therefore, investing in robust monitoring and defense mechanisms is essential to protect both the business and its customers from the significant economic and reputational damage caused by these malicious activities.



Example of a Phishing Email created by AI

As AI technology continues to become integral to various industries, organisations must develop robust strategies to address the accompanying challenges. The adoption of AI solutions, such as ChatGPT, is inevitable and increasingly embraced by businesses of all sizes, including small enterprises. This widespread adoption requires a comprehensive understanding of how to implement AI effectively while mitigating potential risks. One of the crucial concerns surrounding AI integration is the impact on employee roles and the potential risks to privacy and security.

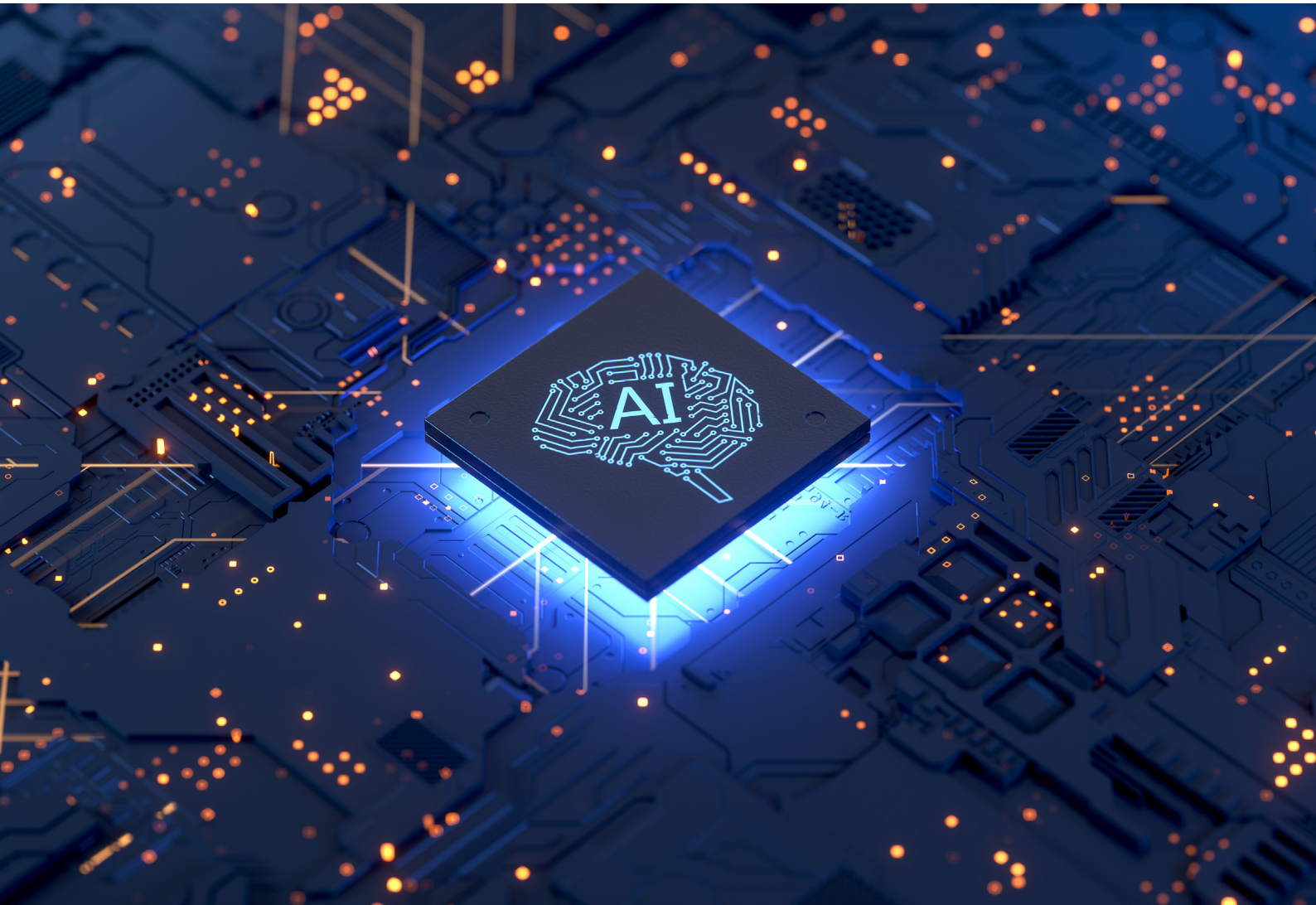


Shadow AI

It requires minimal effort for employees to use publicly available text-based generative AI systems to boost their productivity. This ease of access leads to the rise of "shadow AI"—the use of popular AI tools without organizational approval or oversight. Consequently, security risks such as inadvertent exposure of sensitive information or intellectual property are becoming an increasingly pressing concern.

While we will address this topic in detail in a future section, it is crucial to keep the concept of shadow AI in mind when considering the implications and risks for enterprises. Shadow AI could necessitate a more robust capacity-building effort to mitigate potential threats effectively.

Shadow AI refers to the use of AI tools and technologies by employees without the knowledge or approval of their organization. This often involves the use of publicly available text-based generative AI systems to increase personal productivity. While such tools can offer significant benefits, their unauthorised use poses several risks to organisations.



Spear Phishing and Social Engineering

QUESTION

[...] one of the things I've also seen in the press is that there's this concern around romance scammers and this idea of pig butchering. Lovely title, but essentially it means that the scammers fatten up one's ego before slaughtering one's bank account. And I'm curious, what's Radware seen in this area?

Jonathan Care
Advisor at Lionfish Tech Advisors

So practically our threat research team has noticed that bots allow those scammers to scale. It's the most important thing that startup will talk about is scalability. And this is exactly what hackers are on the hunt for. Because bots simulate real humans and it can do it in a way like hiring 30 ,000 people that will start a conversation with adults on dating apps and try to social engineering takes a lot of money and a lot of time and human resources that hackers didn't have before. But now every kid can simulate this with the powerful tools that developed over the years and maybe even utilise existing tools.

Six months ago, I came across in the Russian marketplace, one 18 year old hacker that bragged about the fact that he was managing to run around 10,000 sessions on really popular dating app. He used practically a chat bot that was meant for enterprises for support. So it's the same chat bot that is used for minimizing the amount of people that is handling customer support. Just take the first steps to understand what the customer needs and have this kind of script. Now those tools have AI capabilities. And those are legit services that are being offered all the time online.

But they are using it for different purposes. They are running it with scripts they took from dating apps. And all of a sudden, the chat bot knows how to react to comment in a way that will look really even cynical. They can use humor. It's not just a standard conversation that start with, Hey, let's meet up or send pictures or something like that. It can be much more persuasive in the way. So people that will didn't fall for that, like two years ago, now they're in the risk because understanding which session is about or not is almost impossible for, from the victim point of view. So it's really interesting trend. Although we can see people like threat actors constantly upgrading their scripts and constantly that the conversation scripts are being updated through the AI tools that are being out there. So I can go to ChatGPT right now and tell him, let's simulate a conversation between a male and a female on dating app that results in the man providing his credit card.

And ChatGPT will be really creative, but he will create this kind of conversation. I can even impose, like introduce myself to ChatGPT, of course not as an hacker, but as a UI designer that works for Tinder and wants to improve their user experience. Therefore he needs to simulate this kind of conversations. So the

18. Jonathan Care (Host) (2024). In The Next Phase of Cybersecurity. EM30Tech.

way that LLMs works as a statistical tool that was trained for so long on a large database, all of a sudden provides them capabilities they never had before to extend the way that the bots are interacting with us.[18]

Romance scams, particularly the "pig butchering" method, are becoming increasingly sophisticated with the use of bots and AI. These scams involve boosting a victim's ego before defrauding them of their money. Hackers now utilise bots to simulate real human interactions on dating apps, enabling them to conduct thousands of fraudulent sessions simultaneously.

These bots, originally designed for enterprise support, have been repurposed with AI capabilities to create highly persuasive and realistic conversations. This technological evolution allows scammers to constantly refine their tactics, making it nearly impossible for victims to detect fraud. AI tools' enhanced scalability and realism have significantly amplified the threat, posing a growing challenge to cybersecurity efforts.

> **But now every kid can simulate this with the powerful tools that developed over the years and maybe even utilise existing tools.**
>
> Arik Atar
> Senior Threat Intelligence Researcher, Radware

Enjoyed this interview?

You can listen to the full version

Listen to the conversation between Jonathan Care & Arik Atar for their insights on the current threat landscape, what are the tactics for modern attacker, romance Scams & Pig Butchering.

Listen here

Deepfakes

> According to deepfake statistics, there was a notable surge in identity fraud related to deepfakes in the US and Canada during the first quarter of 2023. Specifically, the rate of such activities in the US escalated from 0.2% to 2.6%, while in Canada, it rose from 0.1% to 4.6%.

AI also facilitates the creation of deepfakes, which can be used for misinformation or propaganda campaigns. **Evidence suggests that bad actors employ AI to conduct larger-scale attacks, rapidly cycling through attack vectors to identify effective entry points.**

AI chatbots can be combined with deepfake technology to create highly convincing impersonations of individuals, such as company executives or family members. These deepfakes can be used in video or voice communications to deceive victims into believing they are interacting with a legitimate person, thereby gaining their trust and extracting sensitive information or money.

The use of AI reduces the cost and increases the speed of executing numerous simultaneous attacks, targeting multiple vulnerabilities. Additionally, AI accelerates post-exploitation activities such as lateral movement and reconnaissance within compromised systems.

Although much attention has been given to the potential of AI-generated malware, current research indicates that AI is more valuable to attackers as an aid in developing malware rather than as an independent creator. AI can assist in developing specific functionalities within malware, but such efforts still generally require the expertise of a knowledgeable human operator.

Want to know more about deepfakes?[19]

Visit website

19. Stewart, 2024

Automated Interactions

Perhaps one of the most dangerous aspects of AI is its potential for automated misuse. While many organisations deploy AI to enhance customer interactions through 24/7 chat services, malicious actors can exploit these same technologies.

This three-pronged process begins with AI's adeptness at scouring open-source intelligence, delving into victims' social media profiles, and pinpointing potential targets ripe for exploitation. AI chatbots can perform automated reconnaissance to gather information about potential targets. By scraping public data and interacting with users, AI can build detailed profiles of individuals and organisations. This information can be used to identify vulnerabilities, preferences, and behaviours, which are then exploited in targeted attacks.

Subsequently, AI harnesses this information to masquerade as trusted individuals, such as close friends or family members, seamlessly deceiving unsuspecting victims. Moreover, AI enables automated conversational patterns, further enhancing the illusion of authenticity. This automated interaction makes it difficult for victims to discern the authenticity of the person they are communicating with, especially on platforms like dating apps. AI can handle large volumes of interactions simultaneously, sending thousands of phishing emails or engaging with multiple targets simultaneously. This scalability enables cybercriminals to reach a broader audience with minimal effort, maximising their chances of success.

Real-time Adaptation and Learning

Similarly, AI chatbots can learn from interactions and adapt their tactics in real-time. If a target detects and reports a phishing attempt, the AI can analyse the failure and modify its approach for future attempts. This continuous learning process makes AI-driven attacks more resilient and difficult to counteract as the tactics evolve to bypass common security measures.

While debates surrounding AI primarily centre on its potential impact on employment and human labour, there exists a critical need to recognise the darker application of AI in the hands of malicious entities. It is imperative that stakeholders within the cybersecurity industry remain vigilant and proactive in assessing the potential risks associated with the malicious utilization of AI technology for manipulation and targeted attacks on individuals and organizations alike.

Mitigating the Threat

To mitigate the threat posed by AI chatbots used by hackers and scammers, industry leaders should consider the following measures:

Advanced Email Filtering: Implement sophisticated email filtering solutions that use AI and machine learning to detect and block phishing emails before they reach end-users.

Capacity Building: Regularly train employees on the latest phishing tactics and how to recognise and respond to suspicious communications.

Multi-Factor Authentication (MFA): Use MFA to add an additional layer of security, making it harder for attackers to gain access to systems and data even if they obtain login credentials.

Regular Security Audits: Conduct frequent security audits to identify and address potential vulnerabilities in the organisation's infrastructure.

By understanding and addressing the ways in which AI chatbots are being used maliciously, industry leaders can better protect their organizations from these sophisticated and evolving threats.

Bibliography

1. Brett, M. et al. (2017) Artificial Intelligence for cybersecurity: Technological and ethical implications technological and ethical implications on JSTOR, Artificial Intelligence for Cybersecurity: Technological and Ethical Implications
2. Calderon, R. (2019) The benefits of artificial intelligence in Cybersecurity, La Salle University Digital Commons
3. DarkTrace (2024) State of AI cyber security 2024, DarkTrace
4. Data Hub (2024) AI startups fall by 69%, people turn to bootstrap, Data Hub
5. Haan, K. (2024) How businesses are using Artificial Intelligence in 2024, Forbes
6. IBM (2024) IBM watsonx.ai, IBM
7. Kulikova , T. et al. (2021) Kaspersky Spam and phishing report for 2023, Securelist English Global securelist.com
8. Loaiza, F. et al. (2019) Utility of Artificial Intelligence and machine learning in cybersecurity on JSTOR, Utility of Artificial Intelligence and Machine Learning in Cybersecurity
9. NCSC (2024) AI and cyber security: What you need to know, NCSC
10. Palo Alto (2024) Incident response 2024 report, Palo Alto Networks
11. Stewart, E. (2024) What are deepfakes and why are they dangerous?, What are Deepfakes and Why are They Dangerous? | Enterprise Tech News EM360Tech
12. Taddeo, M., McCutcheon, T. and Floridi, L. (2019) 'Trusting artificial intelligence in cybersecurity is a double-edged sword', Nature Machine Intelligence, 1(12), pp. 557–560. doi:10.1038/s42256-019-0109-1
13. Wilner, A. (2018) Artificial Intelligence and deterrence: Science, theory and practice

www.EM360tech.com info@EM360tech.com