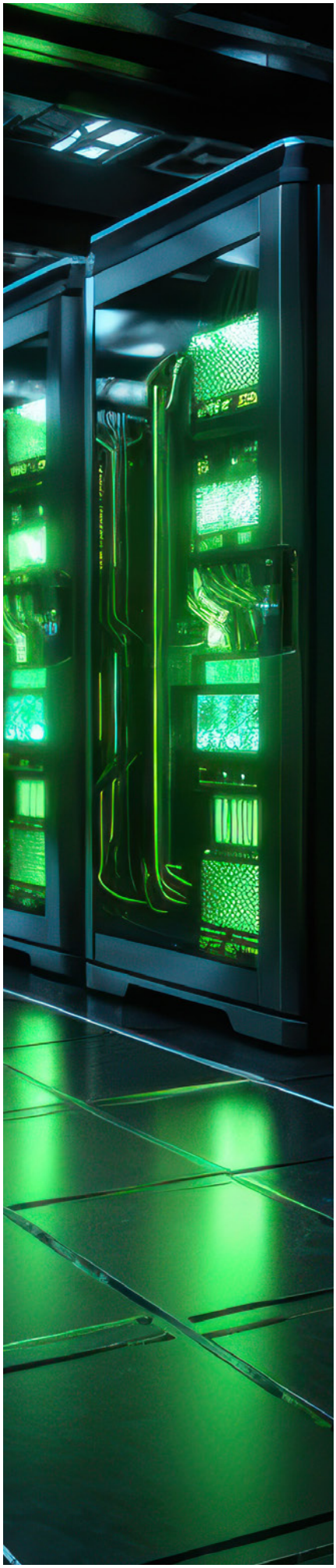
AI Cyber Insights

AI in Cybersecurity

Q3 2024 INSIGHTS

A quarterly comprehensive whitepaper on the latest advancements at the intersection of Artificial Intelligence and Cybersecurity

Table of Contents



Executive Summary

Q3 2024 marked a pivotal phase in the integration of Artificial Intelligence (AI) within cybersecurity. This quarter saw both promising advancements and significant challenges, highlighting the dual role AI plays in both protecting and exposing vulnerabilities in critical infrastructures

Key developments include:

- A robust funding environment with $2.15 billion raised across 73 publicly disclosed funding rounds in cybersecurity. [1]
- A sharp increase in AI-specific security funding, with $229 million secured in 14 deals.
- The discovery of several critical AI vulnerabilities, reinforcing the need for enhanced cybersecurity protocols to protect AI-driven platforms.
- Continued regulatory evolution, with notable AI-related legislation introduced in the European Union and California aimed at ensuring the responsible development and deployment of AI technologies.
- Expansion of AI-focused education and certification programs, underscoring the growing need for specialized knowledge in this rapidly evolving field.

These developments emphasize the growing reliance on AI to protect global digital infrastructures while simultaneously spotlighting the vulnerabilities AI introduces. This report provides a comprehensive overview of these shifts, offering actionable insights for businesses, policymakers, and international stakeholders seeking to navigate this complex landscape.

Introduction

As AI continues to transform industries globally, its integration into cybersecurity has accelerated in 2024, bringing both unprecedented opportunities and unique risks. The third quarter of 2024 witnessed significant advancements in AI-driven cybersecurity solutions, but it also highlighted the vulnerabilities inherent in these technologies.

This report zooms into Q3 2024's key developments, focusing on:

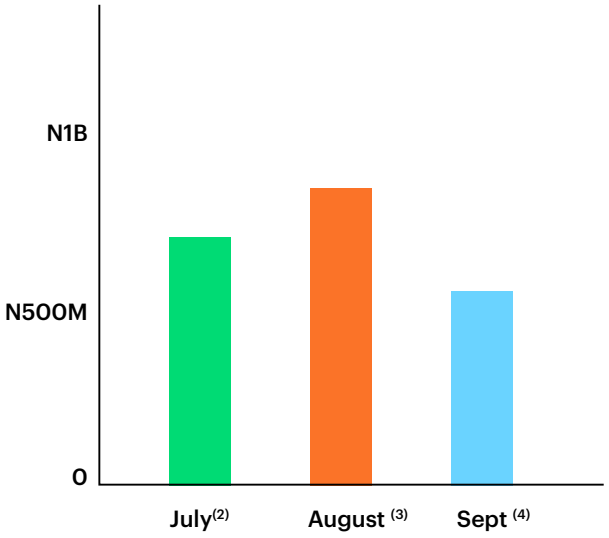
- A dynamic funding landscape driven by AI-driven innovations.
- Emerging AI cybersecurity educational initiatives and certifications.
- Critical AI vulnerabilities uncovered across widely-used platforms.
- Regulatory changes aimed at securing AI in various jurisdictions.

Our goal is to provide a global perspective, offering insights not only into the technical evolution of AI in cybersecurity but also the geopolitical, regulatory, and societal implications of these changes. The insights presented are based on extensive desk research, industry reports, and comprehensive analyses. This paper is designed to serve as a guide for policymakers, corporate leaders, and cybersecurity professionals in understanding and preparing for the future of AI-enhanced security.

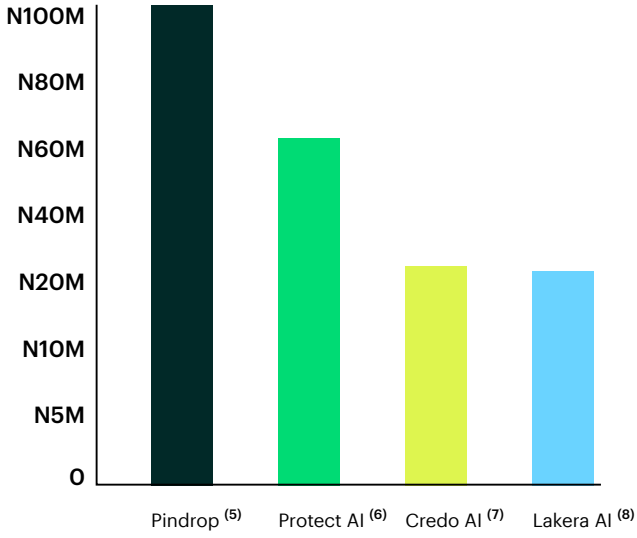
Funding Landscape

Q3 2024 continued to see robust investment in AI and machine learning applications in cybersecurity, even as overall cybersecurity funding saw a decline compared to Q2. This quarter was defined by a growing emphasis on AI-specific security solutions, which accounted for a larger portion of the funding landscape.

Total cybersecurity funding:
$2.15 billion raised across 73 rounds.

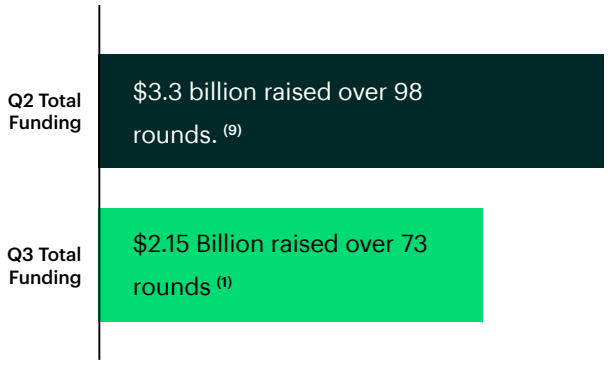


AI specific funding:
$246.5 million raised across 15 deals.

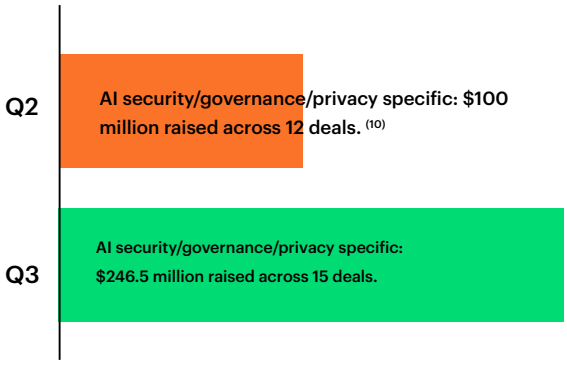


Comparison with Q2

Total Funding



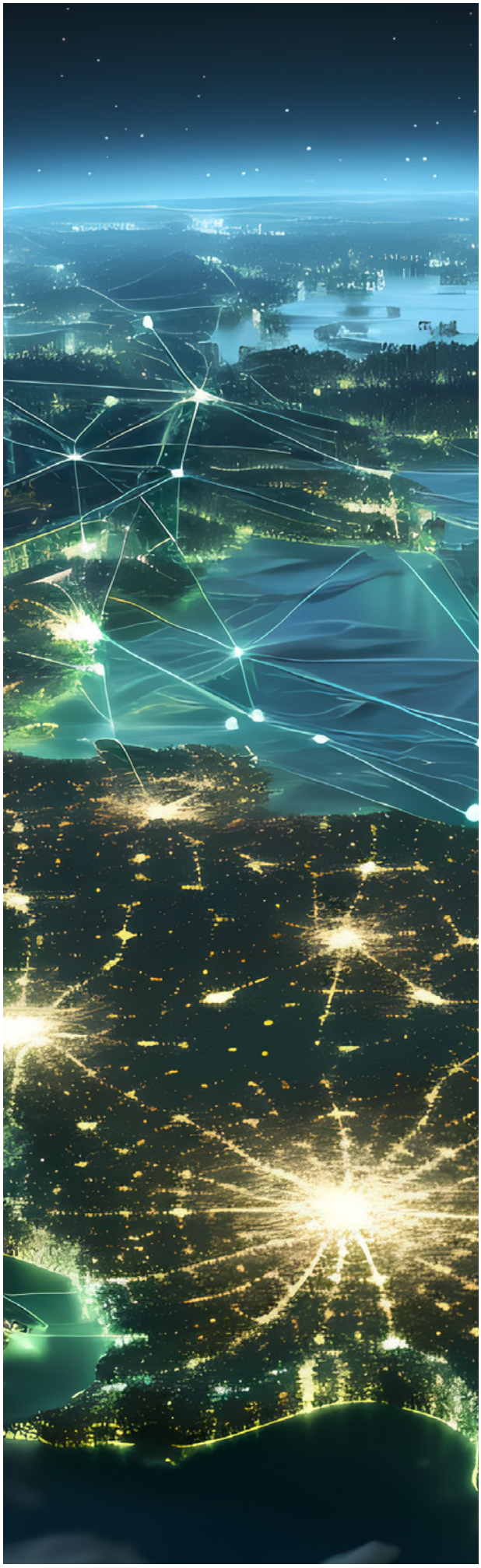
AI Specific Funding



Overall funding reduced by 34.8% from Q2 to Q3, with the number of funding rounds reducing by 25.5%. AI-specific security funding increased by 146.5% from Q2 to Q3, and the number of AI-specific deals increased by 25%

Global Trends and Insights

- **Geographical distribution:** Investments were not limited to the United States. Israel, Switzerland, South Korea, and the UK also attracted significant attention, showing the global demand for AI cybersecurity solutions.
- **Sectoral impact:** The rise in AI-driven security tools has been especially prominent in financial services, healthcare, and cloud infrastructures—industries where security breaches can have far-reaching consequences.
- **Comparison to Q2:** Overall funding decreased by 34.8%, but AI-specific investments grew by 146.5%, highlighting increasing investor confidence in AI-powered solutions despite economic slowdowns.
- **Continued growth in AI-related cybersecurity:** The number and size of AI-specific security deals increased, indicating growing investor confidence in this niche.
- **Large late-stage rounds:** Several companies secured significant late-stage funding, such as Abnormal Security ($250M Series D) [11] and Cribl ($319M Series E). [12]
- **Integration of AI into established categories:** Many funded companies are incorporating AI capabilities into traditional cybersecurity domains, rather than being pure-play AI security firms, a continuous trend from Q2. [10]



AI in Cybersecurity Education

As AI continues to reshape the cybersecurity landscape, the demand for specialized education and certifications has surged. Prestigious institutions and industry leaders are responding by developing courses tailored to the intersection of AI and cybersecurity. This evolution is creating a new breed of cybersecurity professionals who are equipped to manage AI-specific risks, vulnerabilities, and governance issues.

4.1 Expansion of AI Cybersecurity Courses

In recent years, several academic institutions and industry leaders have introduced AI-focused cybersecurity programs. These courses aim to provide professionals with the knowledge and practical skills to address AI-driven cyber threats:

- University of Oxford offers the course "Artificial Intelligence for Cyber Security",[13] an online program that blends the domains of AI and cybersecurity. The course focuses on equipping professionals with the skills to implement AI solutions to protect critical infrastructures from advanced cyber threats.
- IBM launched its "Generative AI for Cybersecurity Professionals Specialization",[14] a three-course series on Coursera that focuses on applying generative AI skills to real-world cybersecurity challenges. This specialization is designed for cybersecurity professionals looking to leverage AI technologies to strengthen security defenses and mitigate risks posed by malicious AI applications.
- DeepLearning.ai offers the "Red Teaming LLM Applications"[15] course, a beginner-friendly program that introduces students to the vulnerabilities inherent in large language model (LLM) applications. This course provides both theoretical knowledge and hands-on experience with red-teaming methods to identify weaknesses in LLM-based systems.
- EC Council introduced its comprehensive course "Generative AI for Cybersecurity",[16] which delves into the security implications of generative AI and large language models (LLMs). The course covers architectural design patterns, AI security frameworks, and the potential pitfalls associated with using AI in security-critical environments. Learners also gain practical experience in prompt engineering and fine-tuning AI models to avoid common security risks.
- A standout contribution to AI education in cybersecurity is Jason Haddix's course "Red Blue Purple AI".[17] This unique offering focuses on reverse engineering security programs and augmenting security

operations with AI tools. Covering topics from LLMs for power users to applying AI in red, blue, and purple team operations, this course equips security professionals with the advanced AI skills needed to defend against AI-driven threats.

4.2 Innovative Teaching Methods

Innovative approaches to AI education are also transforming how cybersecurity professionals learn. An example of this is Andrew Ng's AI Python course,[18] which leverages an AI chatbot to teach Python programming. This revolutionary approach showcases how AI-powered tools with vast knowledge bases can be used to enhance the learning experience. The application of AI in educational tools not only personalizes learning but also offers real-time feedback, simulating complex cybersecurity scenarios that students can learn from interactively.

The broader adoption of AI-assisted learning methods could further revolutionize cybersecurity training, making it more accessible and tailored to individual learning needs. For instance, future cybersecurity courses may increasingly use AI-driven simulations to train security teams on handling advanced cyber threats, including AI-generated attacks.

4.3 Emergence of AI Cybersecurity Certifications

The demand for validated AI expertise in cybersecurity has led to the rise of specialized certifications. One notable certification is the Certified AI/ML Pentester (C-AI/MLPen),[19] [20] [21] which focuses on assessing professionals' ability to identify and exploit vulnerabilities in AI/ML systems. This practical certification caters to pentesters, security operations center (SOC) analysts, and AI/ML security enthusiasts, ensuring that professionals are equipped to handle AI-driven threats.

Looking ahead, the number of certifications focused on AI in cybersecurity is expected to increase as AI technology becomes further integrated into various sectors. Certifications will likely focus on different aspects of AI in cybersecurity, such as AI ethics, privacy, governance, and threat detection.

4.4 Implications for Global Workforce Development

As AI becomes a critical component of cybersecurity, organizations must prioritize the upskilling of their workforce to manage these emerging technologies. This requires investment not only in employee education but also in continuous professional development through certifications and hands-on training programs. In a rapidly evolving threat landscape, cybersecurity professionals need to stay ahead of AI-driven threats by continually expanding their skill sets.

By expanding access to AI-focused courses and certifications, both academic institutions

and industry leaders are ensuring that cybersecurity professionals are well-prepared to protect digital infrastructures in an AI-driven world.

Disclosed AI Vulnerabilities

Q3 2024 revealed several critical AI vulnerabilities affecting widely used platforms and services. These vulnerabilities highlight the growing risks posed by integrating AI into enterprise and cloud environments, reinforcing the need for enhanced security measures and governance frameworks for AI systems. Each of these vulnerabilities underscores a broader issue related to the robustness and reliability of AI in cybersecurity, as well as the potential for AI systems to be exploited at scale.

5.1 Microsoft 365 Copilot Vulnerabilities

Multiple high-profile vulnerabilities were uncovered in Microsoft's AI-powered 365 Copilot suite, [22] [23] [24] including risks related to data exfiltration and prompt injection attacks. These vulnerabilities allowed attackers to manipulate AI outputs, gain unauthorized access to sensitive information, or inject malicious commands into the system.

Given the widespread use of Microsoft 365 in industries like finance, healthcare, and government, the exploitation of these flaws could lead to significant breaches of sensitive data and regulatory non-compliance.

Key Risks: Unauthorized access, data exfiltration, prompt injection, manipulation of AI outputs.

Global Impact: Industries relying on AI-driven productivity tools are particularly vulnerable, with potential consequences for global financial systems and healthcare infrastructure.

5.2 Slack AI Vulnerability

A critical flaw related to user data leaks was discovered in Slack's AI system, primarily stemming from insufficient input validation. [25] This vulnerability opened the door for attackers to gain access to sensitive communications, files, and workflows. [26] As a central collaboration tool used by enterprises globally, the potential for data breaches from this vulnerability raised concerns across sectors that depend on secure communication channels.

Key Risks: Data leaks, insecure input validation, unauthorized access to workflows.

Global Impact: Companies that rely on AI-powered collaboration tools face significant risks of unauthorized data exposure, impacting sectors from technology to legal and healthcare.

5.3 OpenShift AI Vulnerabilities

- Critical remote code execution (RCE) vulnerabilities were discovered in OpenShift AI, which is widely used for deploying AI models in cloud environments. [27] These vulnerabilities allow attackers to execute arbitrary code on servers, potentially compromising the integrity of AI models and the platforms that host them. Given OpenShift's integration in enterprise cloud infrastructures, such vulnerabilities represent a significant threat to global cloud security. [28]

Key Risks: Remote code execution, arbitrary code execution, compromise of AI models.

Global Impact: Enterprises using OpenShift for cloud AI deployments face significant risk, with potential ripple effects across industries relying on AI-driven cloud solutions.

5.4 Khoj AI XSS Flaw

A cross-site scripting (XSS) vulnerability was found in Khoj AI, allowing attackers to inject malicious scripts into the platform. [29] This type of vulnerability has the potential to launch supply chain attacks, where compromised AI models lead to downstream infections of other systems or platforms that rely on these models. The vulnerability poses risks to AI developers and engineers who utilize Khoj AI for AI development and deployment. [30]

Key Risks: Cross-site scripting, injection of malicious scripts, supply chain attacks.

Global Impact: AI model developers and downstream systems could be compromised, affecting companies relying on AI-driven automation and data analysis.

5.5 Mage AI Path Traversal Vulnerability

Mage AI was found to have a critical path traversal vulnerability, enabling attackers to gain unauthorized access to sensitive system files. [31] This flaw allows hackers to manipulate directory paths and access files outside of the application's intended reach. Given that Mage AI is used in data-sensitive environments, the exploitation of this vulnerability could result in serious data breaches and the exposure of proprietary or confidential information.[32]

Key Risks: Path traversal, unauthorized file access, exposure of sensitive data.

Global Impact: Companies handling sensitive information or intellectual property could face significant risks if this vulnerability is exploited, leading to data breaches and intellectual property theft.

5.6 Mage AI Path Traversal Vulnerability

Hackers exploited a critical vulnerability in Monica AI, allowing them to inject malicious inputs and steal sensitive data. [33] The root of the issue lay in the AI's failure to properly sanitize inputs, making it susceptible to injection attacks. Given Monica AI's use in sectors that deal with highly sensitive data, such as healthcare and finance, this breach had far-reaching implications for data security and compliance. [34]

Key Risks: Data theft, injection of malicious inputs, compromised system security.

Global Impact: Sensitive data in industries such as healthcare, finance, and legal sectors are at significant risk, with severe consequences for regulatory compliance and financial stability.

5.7 Haystack LLM Framework Vulnerability

A major security flaw was discovered in the Haystack large language model (LLM) framework, allowing attackers to execute unauthorized code. [35] This vulnerability enables hackers to compromise AI pipelines and tamper with the output of large-scale language models, which are widely used in enterprise applications. The Haystack vulnerability is particularly concerning due to the popularity of this framework in deploying AI-powered solutions.

Key Risks: Unauthorized code execution, AI pipeline tampering, compromised LLM outputs.

Global Impact: Enterprises relying on LLM-based AI solutions could face significant risks, with potential compromises in key business applications and decision-making systems.

5.8 SAP AI Core Flaws

Researchers identified multiple critical vulnerabilities in SAP AI Core, allowing attackers to hijack AI processes. [36] These flaws present serious risks for organizations using SAP AI in enterprise settings, as attackers could gain control over AI-driven workflows, resulting in data manipulation, sabotage of AI processes, and unauthorized access to enterprise systems. [37]

Key Risks: AI process hijacking, data manipulation, unauthorized system access.

Global Impact: Enterprise users of SAP AI could see significant operational risks, with the potential for widespread data breaches and business disruptions.

5.9 SuperAGI Vulnerability

A critical flaw in the SuperAGI autonomous AI platform allowed hackers to hijack its functionalities, injecting malicious code to gain unauthorized control over AI tasks. [38] This vulnerability poses a significant threat to organizations relying on SuperAGI for mission-critical operations, such as AI-driven decision-making and automation. [39] Exploiting this vulnerability could result in system failures, data theft, or tampering with business-critical processes.

- **Key Risks:** AI task hijacking, malicious code injection, system control takeover.
- **Global Impact:** Organizations utilizing autonomous AI platforms like SuperAGI are at risk of severe disruptions in critical AI operations, potentially leading to financial and operational losses.

Key Risks: AI task hijacking, malicious code injection, system control takeover.

Global Impact: Organizations utilizing autonomous AI platforms like SuperAGI are at risk of severe disruptions in critical AI operations, potentially leading to financial and operational losses.

Key Observations

The vulnerabilities disclosed in Q3 2024 illustrate several key trends in the intersection of AI and cybersecurity:

- **Weak Input Validation:** A recurring theme across multiple platforms is the lack of robust input validation in AI systems, making them susceptible to injection attacks, data exfiltration, and unauthorized system control.
- **Cascading Security Risks:** The interconnected nature of AI systems means that vulnerabilities in one platform can often lead to cascading effects across other systems, especially in environments where AI models are integrated into larger ecosystems or supply chains.
- **Regulatory Implications:** The exposure of these vulnerabilities has significant implications for global regulatory frameworks. As AI becomes more integrated into critical sectors, including finance, healthcare, and enterprise solutions, the need for stringent security protocols and compliance measures grows.

Key Developments in Q3 2024

Q3 2024 witnessed significant shifts in the AI and cybersecurity landscape. These developments underscore the dual role of AI as both an enabler of innovation and a source of new security challenges. Below are the most notable events shaping the sector during this period:

6.1 Rise of AI Exploits and Bug Bounty Programs

The growing number of AI exploits led to an increase in bug bounty programs aimed at identifying and mitigating vulnerabilities in AI systems. The Protect AI bug bounty program [40] continued to gain momentum, helping companies proactively address AI-specific security issues. In Q3 2024 alone, vulnerability disclosures increased by 20% compared to Q2, indicating a heightened focus on AI security.[41]

6.2 Expansion of AI in Business and Enterprise Solutions

- Microsoft 365 Copilot [42] and Slack AI witnessed widespread adoption in the business and enterprise sectors.
- Despite their significant growth, these platforms faced security scrutiny due to their vulnerability to prompt injection, data exfiltration, and insecure API usage [43].
- The growing use of AI in financial fraud detection and predictive healthcare diagnostics has generated concerns about the systems' accuracy. [44] [45].
- Q3 2024 saw a strong push for better vulnerability testing and ethical AI use in both healthcare and finance sectors.

6.3 Increased Focus on AI Ethics and Accountability

- AI's rapid expansion into sensitive sectors prompted discussions around AI transparency and accountability [46].
- Tools like the AI Explainability framework gained traction to address concerns about the opacity of AI decision-making processes in areas where AI significantly impacts human lives and financial security. [47] [48]

6.4 Notable Events

Mastercard's $2.65 Billion Acquisition of an AI Cybersecurity Company

- Mastercard announced its acquisition of an AI-driven cybersecurity firm for $2.65 billion [49].
- This move highlights the growing trend of major corporations investing heavily in AI solutions to enhance security infrastructure.
- Mastercard aims to leverage AI to detect fraud, manage risks, and streamline transaction security at scale [50].

Ireland's Investigation into Google's PaLM 2 for GDPR Compliance

- The Irish Data Protection Commission (DPC) opened an investigation into Google's PaLM 2 AI model over concerns about its compliance with GDPR [51] [52]
- This marks a critical development in the intersection of AI and privacy laws.
- Regulators are increasingly scrutinizing how large AI models manage and process personal data, setting the stage for tighter regulations surrounding AI's application in data-heavy industries [53].

OpenAI Co-Founder Raises $1 Billion for AI Safety

- One of OpenAI's co-founders successfully raised $1 billion to focus on AI safety [54].
- This fundraising effort emphasizes the growing concern within the AI community and beyond regarding the potential risks posed by unchecked AI development [55].
- The funds will be used to mitigate these risks by enhancing AI safety measures and ensuring that the rapid advancement of AI technology does not outpace necessary safeguards.

South Korea's Investigation into AI-Generated Explicit Content on Telegram

- South Korea initiated an investigation into the proliferation of explicit AI-generated content on Telegram [56].
- This raises concerns about how AI is being used to create harmful or illegal material [57].
- As AI content generation tools become more accessible, governments are under pressure to regulate and monitor their misuse, particularly in relation to privacy violations and exploitation [58].

Tech Giants team up to form a Coalition for Secure AI (CoSAI)

- Several leading technology companies have joined forces to create the Coalition for Secure AI (CoSAI).
- This coalition is dedicated to establishing best practices, security standards, and guidelines to mitigate risks in artificial intelligence systems.
- CoSAI aims to address vulnerabilities in AI models, prevent misuse, and promote

secure development practices across the industry. [59]

Paris 2024 Olympics uses AI to protect athletes online

- AI-powered monitoring tools are deployed to identify and mitigate online threats such as harassment, cyberbullying, and disinformation campaigns targeting athletes on social media platforms.
- This proactive approach aims to ensure a secure online environment, allowing athletes to focus on their performance without concerns about digital security risks.
- The initiative is part of a broader effort to integrate advanced technologies into sports security management. [60] [61]

OpenAI Disrupts Iranian Influence Operation

- OpenAI has disrupted an Iranian influence operation, Storm-2035, which used ChatGPT to spread content across topics related to the U.S. presidential campaign [62].
- The U.S. election season has already seen AI-generated deepfakes of candidates, portraying them as making statements they never said.
- The operation's reach was minimal, with low engagement on social media, but it highlights how AI is being weaponized in modern political landscapes [63].
- Despite the low impact, OpenAI's swift action, alongside Microsoft Threat Intelligence contained the operation.

Clearview AI Faces Sanctions Over GDPR Violation

- Clearview AI has been sanctioned for GDPR violations by the Dutch Data Protection Authority (DPA), which imposed a fine of €30.5 million ($33 million). [64]
- The violation stems from Clearview's unauthorized scraping of publicly available images without user consent, which were used to build a massive facial recognition database.
- The Dutch DPA has also threatened additional penalties if Clearview continues its non-compliance.
- Clearview argues that it has no business presence in the EU and thus is not subject to GDPR

Google's Effort to Flag AI-Generated Images to Combat Deepfakes

- Google announced its initiative to flag AI-generated images as part of its efforts to curb the spread of deepfakes [65].
- This proactive step highlights the increasing need for transparency in AI-generated content and the potential risks associated with manipulated media [66].
- Google's effort is seen as a vital measure to mitigate the use of AI in misinformation campaigns and cyberattacks involving fake content.

Generative AI Powers Sophisticated Malware Campaign

- A notable cybersecurity incident in Q3 2024 involved threat actors leveraging generative AI to create more convincing phishing emails and conduct sophisticated malware campaigns [67].
- This event illustrates the dark side of AI innovation, where malicious actors harness AI to enhance the effectiveness of cyberattacks.
- As AI continues to evolve, so too will the complexity of threats, posing new challenges for cybersecurity professionals.

LinkedIn's AI Data Controversy and UK Suspension

- LinkedIn faced backlash for using user data to train AI models without explicit consent [68].
- This led to the suspension of AI training with UK user data, sparking widespread debates about transparency, data privacy, and ethical AI practices [69].
- This controversy reflects broader concerns about the use of personal data for AI development and the need for clearer regulatory frameworks governing such activities.

Meta's Plan to Train AI Models with Public UK Social Media Data

- Meta's decision to use publicly available UK social media data to train its AI models raised privacy concerns [70].
- As data privacy regulations in Europe tighten, this move highlights the ethical dilemma of using public data for AI training and development [71].
- Meta's approach has fueled ongoing debates about user consent, data ownership, and the privacy implications of large-scale AI training.

Top Tech Companies Challenge EU's AI Regulations

- Tech giants like Google and Microsoft have pushed back against the EU's proposed AI regulations, arguing that the rules could stifle innovation [72].
- The ongoing conflict between regulators and industry leaders highlights the delicate balance between fostering AI innovation and ensuring security, transparency, and accountability in AI systems [73].
- The outcome of these regulatory battles will likely shape the future of AI governance worldwide.

Snapchat's AI Selfie Feature Raises Privacy Concerns

- Snapchat's introduction of an AI-powered selfie feature, which processes large amounts of personal data, has drawn scrutiny over how that data is handled [74].
- Privacy advocates have raised concerns about data storage, sharing, and potential misuse, particularly given the popularity of AI-enhanced consumer applications [75].
- This case illustrates the growing need for robust privacy protections in consumer-facing AI products [76].

White House Launches AI Datacenter Task Force

- The U.S. government has launched the AI Datacenter Task Force to ensure that datacenters supporting AI infrastructure are secure and resilient [77].
- This task force will focus on the operational and security aspects of AI datacenters, ensuring they are robust against cyber threats and environmentally sustainable [78].
- This marks an important step in securing the backbone of AI technologies in the U.S. and protecting sensitive data housed in these data centers [79].

Current AI Regulatory Landscape

As AI becomes a critical driver of economic and social change, the regulatory landscape is rapidly evolving to meet the challenges posed by these technologies. Globally, AI governance is being shaped by a combination of innovation-friendly policies and stringent security and ethical standards. Regulatory harmonization remains a challenge, particularly for companies operating across multiple regions. However, the convergence of global standards is expected as AI technologies become more integrated into critical sectors such as healthcare, finance, and law enforcement.

7.1 United States:

7.1.1 California's Groundbreaking AI Model Legislation

- California introduced pioneering legislation aimed at regulating AI models, focusing on AI security and accountability [80].
- This legislation is seen as a template for future regulations globally, addressing the ethical, security, and societal implications of AI deployment [81].
- The law mandates transparency in AI models and holds developers accountable for any harm caused by their AI products, setting a new standard for AI governance.

7.1.2 Governor's Rejection of AI Safety Bill:

- In a contrasting move, California's governor rejected the AI Safety Bill, citing concerns over stifling innovation with overregulation. [82]
- This decision has sparked debate on the balance between AI innovation and security oversight [83].

7.2 European Union:

AI Act and Comprehensive Regulation

- The EU continued its regulatory leadership with the AI Act, which focuses on high-risk AI systems in sectors such as law enforcement and healthcare [84].
- The Act mandates conformity assessments for AI models used in high-risk applications, ensuring transparency and safety.
- The EU also bans specific AI applications, such as real-time biometric surveillance, that are deemed too risky to public safety and human rights.

7.3 Asia-Pacific:

Innovation-Friendly Regulations

- China and Singapore led efforts to promote AI innovation while focusing on data privacy and security [85] [86]
- These countries implemented AI governance frameworks that ensure compliance with national security regulations while fostering AI-driven growth.

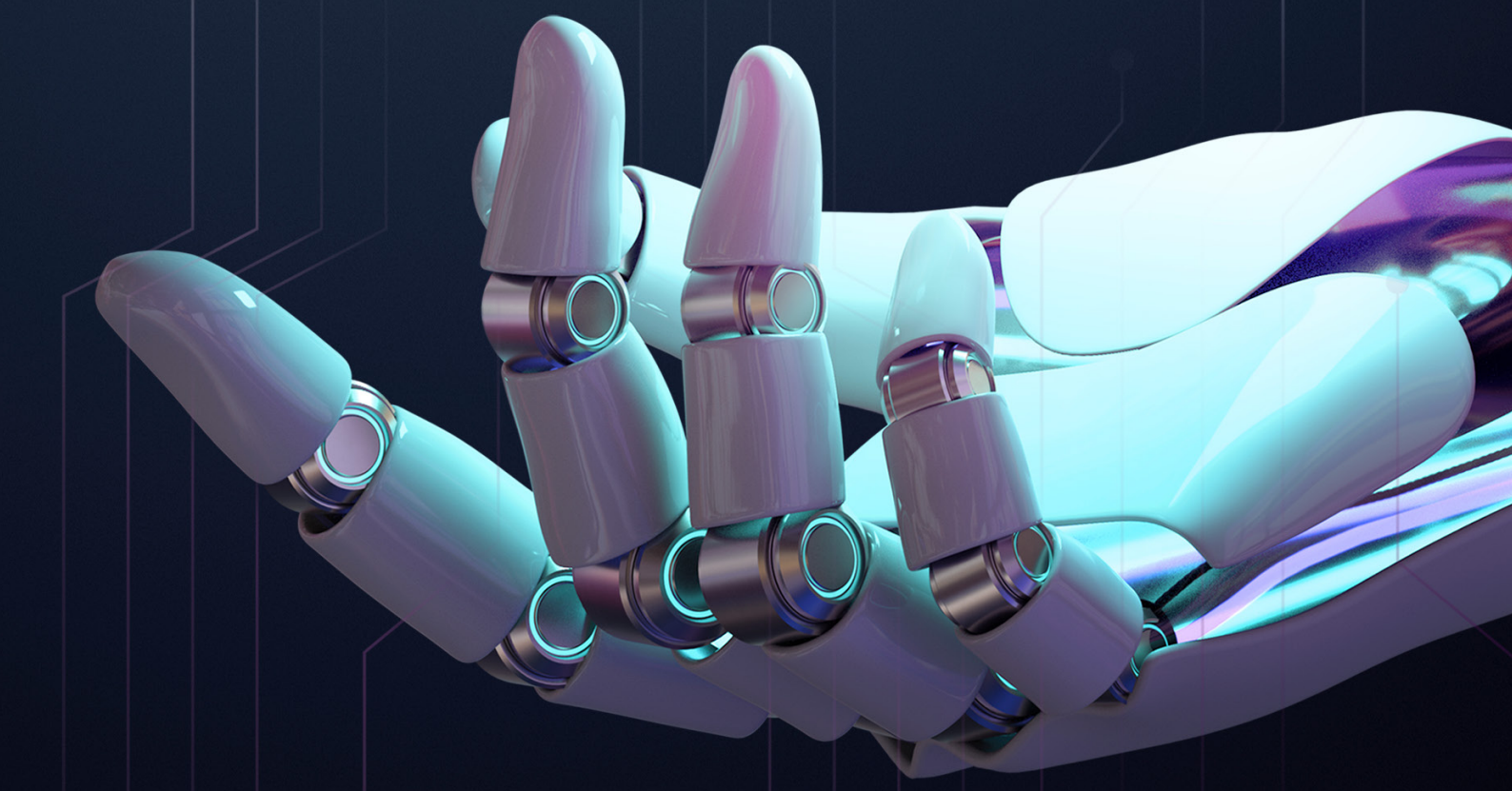
Conclusion

Q3 2024 has been a pivotal period in the ongoing integration of AI into cybersecurity. The substantial funding flowing into AI-driven cybersecurity solutions, coupled with the emergence of specialized educational programs, underscores the industry's recognition of AI's transformative potential in defending against evolving cyber threats.

However, the discovery of critical vulnerabilities in major AI platforms serves as a stark reminder of the challenges that lie ahead. These security issues highlight the need for robust testing, continuous monitoring, and the development of AI-specific security protocols.

The regulatory landscape is rapidly evolving to keep pace with technological advancements, with governments and international organizations striving to establish frameworks that foster innovation while ensuring responsible AI development and deployment.

As we move forward, it is clear that the intersection of AI and cybersecurity will continue to be a dynamic and critical area of focus. The ability to harness AI's potential while mitigating its risks will be crucial in shaping the future of cybersecurity. Stakeholders across the industry must remain vigilant, adaptive, and collaborative to navigate the complex challenges and opportunities that lie ahead in this AI-driven era of cybersecurity.



Appendix A:
Q3 2024 Funding Overview

July 2024 Funding Summary

WEEK 1

7 cybersecurity companies raised

$81.1M

across 7 unique product categories in 3 countries Source

Key Deals:

- **Command Zero:** $21.0M Seed (Security Operations and Investigation, USA) Source
- **Cytactic:** $16.0M Seed (Incident Response and Crisis Management, Israel) Source

WEEK 2

6 cybersecurity companies raised

$235.1M

across 6 unique product categories in 2 countries Source

Key Deals:

- **Pindrop:** $100.0M Debt Financing (Deepfake detection, USA) Source
- **XBOW:** $20.0M Venture Round (Autonomous Application Security Testing Patform, USA) Source

WEEK 3

14 cybersecurity companies raised

$507.0M

across 12 unique product categories in 3 countries Source

Key Deals:

- **Vanta:** $150.0M Series C (Automated Compliance Monitoring and Security, USA) Source
- **Chainguard:** $140.0M Series C (Software Supply Chain, USA) Source
- **Cowbell Cyber:** $60.0M Series C (Cyber Risk Insurance, USA) Source
- **Dazz:** $50.0M Venture Round (Application Security Posture Management, USA) Source
- **Lakera AI:** $20.0M Series A (LLM Security, Switzerland) Source
- **vijil:** $6.0M Seed (AI Governance and Safety Platform) Source
- **Promptfoo:** $5.0M Seed (AI Applications Security, USA) Source
- **ZEST Security:** $5.0M Seed (Cloud Threat Detection and Response, USA) Source
- **Blackbird.AI:** Undisclosed Venture Round (Cyber Threat Intelligence, USA) Source

WEEK 4

10 cybersecurity companies raised

$166.1M

across 8 unique product categories in 2 countries Source

Key Deals:

- **Protect AI:** $60.0M Series B (AI and ML Security, USA) Source
- **Credo AI:** $21.0M Series B (AI Governance and Safety, USA) Source
- **Lineaje:** $20.0M Series A (Software Supply Chain Security, USA) Source
- **Halcyon:** Undisclosed Venture Round (Endpoint Detection and Response (EDR) Triage and Automation Platform, USA) Source
- **Zenity:** Undisclosed Venture Round (Governance and Security Platform, Israel) Source

August 2024 Funding Summary

WEEK 1

5 cybersecurity companies raised

$290.6M

across 5 unique product categories in 2 countries Source

Key Deals:

- **Abnormal Security:** $250.0M Series D (Email Security, USA) Source
- **Anjuna:** $25.0M Series B (Confidential Computing Platform, USA) Source
- **Aurascape:** $12.8M Seed (Security Posture Management Platform for AI Applications and Workloads, USA) Source
- **Scamnetic:** $1.4M Pre-Seed (AI-based Fraud and Scam Threats Detection, USA) Source

WEEK 2

5 cybersecurity companies raised

$459.1M

across 4 unique product categories in 2 countries Source

Key Deals:

- **Kiteworks:** $456.0M Private Equity Round (Secure Data Collaboration and Messaging Solutions, USA) Source

WEEK 3

3 cybersecurity companies across 3 unique product categories raised funding in 2 countries Source

Key Deals:

- **CUBIG:** Undisclosed Venture Round (AI Applications Security, South Korea) Source

WEEK 4

7 cybersecurity companies raised

$335.4M

across 6 unique product categories in 5 countries Source

Key Deals:

- **Cribl:** $319.0M Series E (Security and Cloud Data Aggregation and Analytics Platform, USA) Source

WEEK 5

8 cybersecurity companies raised

$643.3M

across 7 unique product categories in 4 countries Source

Key Deals:

- **CGI:** $552.0M post-IPO debt round (Cloud and cybersecurity Services, Canada) Source
- **Acuvity:** $9.0M Seed (AI Governance, USA) Source

September 2024 Funding Summary

WEEK 1

12 cybersecurity companies raised

$168.0M

across 10 unique product categories in 3 countries Source

Key Deals:

- **Strider Technologies:** $55.0M Series C (Cyber Threat Intelligence, USA) Source
- **Operant:** $10.0M Series A (Runtime Application Security, USA) Source
- **Realm.Security:** $5.0M Seed (Security and Cloud Data Aggregation and Analytics Platform, USA) Source
- **SplxAI:** $2.0M Pre-Seed (AI Chatbot Applications Security, USA) Source

WEEK 2

14 cybersecurity companies raised

$239.6M

across 12 unique product categories in 5 countries Source

Key Deals:

- **Intezer:** $33.0M Series C (Security Operations Center (SOC) workflows AI Automation, Israel) Source
- **EasyDMARC:** $20.0M Series A (Email Deliverability Health and Security Platform, USA) Source
- **c/side:** $6.0M Seed (Client-side Security Monitoring Platform, USA) Source
- **Edera:** $5.0M Seed (Cloud Threat Detection and Response Platform for Kubernetes Deployments, USA) Source
- **ChillStack:** $2.5M Series A (AI Fraud Detection, Japan) Source
- **CyberCyte:** Undisclosed Non-Equity Assistance round (Continuous Threat Exposure Management (CTEM) Platform, UK) Source

WEEK 3

15 companies raised

$114.3M

across 14 unique product categories in 9 countries Source

Key Deals:

- **Torq:** $70.0M Series C (No-code Security Automation, USA) Source
- **Tamnoon:** $12.0M Series A (Continuous Threat Exposure Management (CTEM) Platform, USA) Source
- **Bluebricks:** $4.5M Seed (Cloud Infrastructure Security and Remediation Platform, Israel) Source
- **Pentra:** $167.1K Pre-Seed (Automated Pentesting and Reporting, Romania) Source
- **Aim Intelligence:** Undisclosed Seed (Threat Detection, Red Teaming, and Security Platform for AI models, South Korea) Source

WEEK 4

8 companies raised

$131.0M

across 8 unique product categories in 4 countries Source

Key Deals:

- **Harmonic Security:** $17.5M Series A (AI Privacy Assurance, USA) Source
- **Xmore AI:** Undisclosed Corporate Round (AI SOC Platform, USA) Source

Endnotes

1. https://pinpointsearchgroup.com/cyber-security-vendor-funding-report-q3-2024/
2. https://pinpointsearchgroup.com/july-24-cyber-security-vendor-funding-mampa/
3. https://pinpointsearchgroup.com/august-24-cyber-security-vendor-funding-mampa/
4. https://pinpointsearchgroup.com/september-24-cyber-security-vendor-funding-mampa/
5. https://techcrunch.com/2024/07/17/deepfake-detecting-firm-pindrop-lands-100m-loan-to-grow-its-offerings/
6. https://protectai.com/newsroom/protect-ai-raises-60m-in-series-b-financing
7. https://siliconangle.com/2024/07/30/credo-ai-raises-21m-help-enterprises-deploy-ai-safely-responsibly-compliant-way/
8. https://www.lakera.ai/news/lakera-raises-20m-series-a-to-deliver-real-time-genai-security
9. https://pinpointsearchgroup.com/cyber-security-vendor-funding-report-q2-2024/
10. https://aicyberinsights.com/ai-in-cybersecurity-q2-2024-insights/
11. https://news.crunchbase.com/cybersecurity/startup-ai-abnormal-security-funding-wellington/
12. https://cribl.io/blog/announcing-our-series-e/
13. https://www.conted.ox.ac.uk/courses/artificial-intelligence-for-cyber-security-online
14. https://www.coursera.org/specializations/generative-ai-for-cybersecurity-professionals
15. https://www.deeplearning.ai/short-courses/red-teaming-llm-applications/
16. https://codered.eccouncil.org/course/generative-ai-for-cybersecurity-course
17. https://jhaddix.gumroad.com/l/vsperu
18. https://www.deeplearning.ai/short-courses/ai-python-for-beginners/
19. https://secops.group/product/certified-ai-ml-pentester/
20. https://secops.group/free-mock-pentesting-exams/#
21. https://aicyberinsights.com/start-hacking-llms-and-become-certified/
22. https://aicyberinsights.com/microsoft-365-copilot-vulnerability-risks-user-data-exfiltration/
23. https://aicyberinsights.com/exposing-the-devastating-security-flaws-in-microsofts-copilot/
24. https://aicyberinsights.com/exposing-indirect-prompt-injection-exploitation-of-ai-vulnerabilities-in-microsoft-365-copilot/
25. https://aicyberinsights.com/slack-ai-security-vulnerability-what-you-need-to-know/
26. https://www.theregister.com/2024/08/21/slack_ai_prompt_injection/
27. https://aicyberinsights.com/exposed-openshift-ai-vulnerability-threatens-security-of-your-ai-models/
28. https://github.com/advisories/GHSA-rrc7-8w2h-xw89
29. https://aicyberinsights.com/critical-xss-flaw-in-khoj-ai-puts-your-ai-models-at-risk-what-you-need-to-know/
30. https://github.com/khoj-ai/khoj/security/advisories/GHSA-h2q2-vch3-72qm
31. https://aicyberinsights.com/mage-ais-critical-path-traversal-vulnerability-exposes-sensitive-data/
32. https://security.snyk.io/vuln/SNYK-PYTHON-MAGEAI-7830471
33. https://aicyberinsights.com/hackers-exploit-critical-monica-ai-vulnerability-to-steal-

Endnotes

sensitive-data/

34. https://nvd.nist.gov/vuln/detail/CVE-2024-45989
35. https://aicyberinsights.com/major-security-flaw-in-haystack-popular-llm-framework/
36. https://aicyberinsights.com/wiz-researchers-uncover-sap-ai-core-flaws/
37. https://www.wiz.io/blog/sapwned-sap-ai-vulnerabilities-ai-security
38. https://aicyberinsights.com/superagi-flaw-allows-hackers-hijack-your-autonomous-ai/
39. https://github.com/advisories/GHSA-8582-mjhv-rmrr
40. https://www.mescomputing.com/news/security/protect-ai-releases-bug-bounty-report-on-august-vulnerabilities
41. https://protectai.com/
42. https://partner.microsoft.com/en-us/blog/article/microsoft-build-2024
43. https://winbuzzer.com/2024/08/12/researchers-reveal-microsoft-copilot-ai-vulnerabilities-xcxwbn/
44. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10517477/
45. https://www.researchgate.net/publication/378297681_Reviewing_the_role_of_AI_in_fraud_detection_and_prevention_in_financial_services
46. https://cyber.harvard.edu/publication/2024/new-report-framework-ai-transparency
47. https://cltc.berkeley.edu/2024/07/02/new-cltc-white-paper-on-explainable-ai/
48. https://www.hitechnectar.com/blogs/explainable-ai-frameworks/
49. https://aicyberinsights.com/mastercard-begins-acquisition-of-ai-cybersecurity-company-for-2-65-billion/
50. https://www.mastercard.com/news/press/2024/september/mastercard-invests-in-continued-defense-of-global-digital-economy-with-acquisition-of-recorded-future/
51. https://aicyberinsights.com/irelands-data-protection-commission-investigates-googles-palm-2-for-gdpr-compliance/
52. https://siliconangle.com/2024/09/12/ireland-opens-privacy-probe-googles-palm-2-language-model/
53. https://www.hinckleyallen.com/publications/accelerated-scrutiny-of-ai-systems-in-2024-the-eu-ai-act-and-the-u-s-strategy/
54. https://aicyberinsights.com/openai-co-founder-raises-1-billion-for-ai-safety/
55. https://www.techerati.com/news-hub/openai-co-founder-raises-1-billion-for-new-safe-ai-start-up/
56. https://www.npr.org/2024/09/06/nx-s1-5101891/south-korea-deepfake
57. https://aicyberinsights.com/south-korea-probes-telegram-for-explicit-ai-generated-content/
58. https://www.un.org/en/ai-and-privacy
59. https://aicyberinsights.com/tech-giants-team-up-to-form-a-coalition-for-secure-ai-cosai/
60. https://aicyberinsights.com/paris-2024-olympics-uses-ai-to-protect-athletes-online/
61. https://olympics.com/ioc/news/ai-system-to-protect-athletes-from-online-abuse-during-

Endnotes

paris-2024

62. https://aicyberinsights.com/openai-disrupts-iranian-influence-operation/
63. https://www.bloomberg.com/news/articles/2024-08-16/openai-scrubs-iranian-accounts-using-chatgpt-for-influence-campaign
64. https://aicyberinsights.com/clearview-ai-faces-sanctions-over-gdpr-violation/
65. https://aicyberinsights.com/google-to-flag-ai-generated-images-fighting-deepfakes/
66. https://techcrunch.com/2024/09/17/google-will-begin-flagging-ai-generated-images-in-search-later-this-year/
67. https://aicyberinsights.com/how-generative-ai-fueled-a-sophisticated-malware-campaign/
68. https://aicyberinsights.com/linkedin-causes-controversy-over-user-data-and-ai-model-training/
69. https://www.bbc.com/news/articles/cy89x4y1pmgo
70. https://www.socialmediatoday.com/news/meta-gains-approval-use-uk-user-posts-ai-training/727046
71. https://aicyberinsights.com/meta-to-train-ai-models-with-public-uk-social-media-data/
72. https://aicyberinsights.com/top-tech-companies-fight-back-challenging-eus-ai-regulation/
73. https://www.cnn.com/2023/06/30/tech/eu-companies-risks-ai-law-intl-hnk/index.html
74. https://www.krock.com.au/trending/entertainment/privacy-alert-snapchats-new-ai-tool-may-use-your-face-in-ads
75. https://www.socialdiscoveryinsights.com/2024/09/23/snapchats-ai-driven-ads-spark-privacy-concerns/
76. https://aicyberinsights.com/snapchats-ai-selfie-feature-privacy-and-data-handling-concerns/
77. https://www.datacenterknowledge.com/ai-data-centers/white-house-launches-ai-data-center-task-force-with-industry-experts
78. https://aicyberinsights.com/white-house-launches-ai-datacenter-task-force/
79. https://www.whitehouse.gov/briefing-room/statements-releases/2024/09/12/readout-of-white-house-roundtable-on-u-s-leadership-in-ai-infrastructure/
80. https://aicyberinsights.com/californias-groundbreaking-ai-model-legislation-the-future-of-ai-security/
81. https://aicyberinsights.com/california-ai-bill-promoting-ai-safety-or-limiting-innovation/
82. https://aicyberinsights.com/californias-governor-rejects-ai-safety-bill/
83. https://www.bbc.com/news/articles/cj9jwyr3kgeo
84. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
85. https://fiscalnote.com/blog/china-ai-policy-development-what-you-need-to-know
86. https://www.edb.gov.sg/en/business-insights/insights/singapore-goes-full-throttle-on-ai-to-secure-future-for-workforce-allocates-s500m-for-advanced-hardware.html

www.aicyberinsights.com