2024 Report

GenAl Security Readiness Report

WWW.LAKERA.AI 2024 REPORT

Table of Contents

04	Executive Summary
09	Section 1: Respondent Background and Organizational Context
15	Section 2: Usage and Perception
20	Section 3: Encountering and Managing Vulnerabilities
25	Section 4: Security Measures and Best Practices
30	Section 5: Challenges and Future Directions
35	Methodology
27	Contributors

2024 REPORT FOREWORD

Foreword

Welcome to the GenAl Security Readiness Report 2024!

As we navigate the transformative era of Generative AI (GenAI) and Large Language Models (LLMs), it is evident that these technologies are reshaping the business landscape in profound ways. The unique capability of LLMs to interact and perform tasks through natural language has democratized the realm of hacking, making it accessible to virtually anyone. This shift underscores the necessity for heightened security measures tailored to the nuances of AI.

Across diverse industries, companies are eager to explore and harness the potential of Al. From enhancing customer experiences to streamlining operations, the promise of Al-driven efficiency and value is compelling. However, this enthusiasm comes with the critical need to address Al security, a domain still in its nascent stages. Our report highlights that the levels of preparedness for Al security vary considerably among organizations, reflecting the newness and complexity of the challenge.

The full extent of the risks associated with Al is yet to be fully realized, but at Lakera, we are committed to leading the charge in secure Al innovation. We stand at the forefront of this revolution, dedicated to ensuring that the benefits of Al can be enjoyed safely and responsibly.

I encourage you to explore this report to gain insights into the current landscape of AI security. It features perspectives from various stakeholders involved in AI safety, including quotes and opinions from CISOs of some of the world's foremost AI-first companies. Together, we can navigate this evolving terrain and build a secure AI-powered future.

Sincerely,



"The Al adoption explosion is fundamentally reshaping the cybersecurity landscape in 2024, presenting unique challenges and new opportunities for all cybersecurity leaders."

When it comes to protecting our organizations, Al is challenging, even overturning, our existing beliefs, approaches, and strategies. The threat landscape is evolving as we speak, but it's already clear that the new threats that Al exposes us to are more complex than and different from risks we have seen in the past. Traditional security measures alone cannot protect us. We need a paradigm shift in how we think about securing both traditional software and Al-powered systems as they merge in the future.

For us security leaders, this is the moment that will redefine our roles. We need to step up and help our organizations develop a new playbook that keeps our employees and customers safe. Lakera's Al Readiness Security Report is a great starting point.



Joe Sullivan CEO of Ukraine Friends and President of Joe Sullivan Security LLC

Executive Summary

Al Adoption Surges, Security Preparedness Lags Behind

The rapid adoption of Generative AI (GenAI) and Large Language Models (LLMs) is transforming industries, with nearly 90% of organizations actively implementing or exploring LLM use cases. However, this surge in adoption is juxtaposed with a strikingly low level of confidence in current security measures—only about 5% of organizations express high confidence in their GenAI security frameworks.

This report, informed by a survey of over 1,000 security professionals and real-world findings from Lakera's Al hacking game, Gandalf, reveals security risk may be underestimated. Gandalf, the world's largest Al red teaming exercise, has engaged over one million users, including cybersecurity experts, in discovering weaknesses. Remarkably, more than 200,000 players successfully completed seven levels of Gandalf defenses, demonstrating how easily Al systems can be exploited. These findings, juxtaposed with the survey insights, underscore the urgent need for robust, Al-specific security strategies to address the unique challenges posed by GenAl.

Key Insights



High Adoption, Low Preparedness

42% of organizations are actively using and implementing LLMs, while another 45% are exploring potential use cases. Despite this, only 5% of organizations feel confident in their ability to secure these systems against emerging threats like prompt attacks and Al-specific malware.



Diverse Expertise, Shared Concerns

The report draws on insights from over 1,000 respondents across various roles, including developers, security analysts, and executive-level positions like CISOs. Over 60% of these respondents have substantial experience in cybersecurity, yet they express significant concerns about the reliability, accuracy, and security of GenAl technologies.

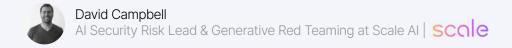


Deploying GenAl Without Al-Specific Security

40% of organizations that lack standard AI security best practices are actively using GenAI. Only 22% are doing AI-specific threat modeling.



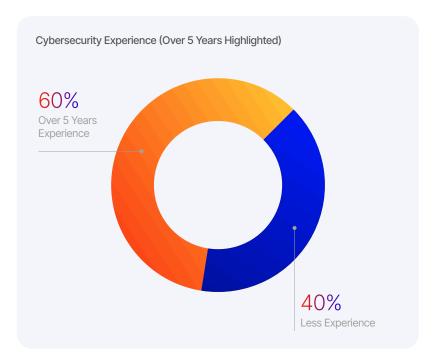
My advice to organizations starting to implement AI security measures is to integrate AI Red Teaming practices early in the development lifecycle. Waiting until after deployment can leave critical vulnerabilities unaddressed. Proactive Red Teaming helps identify and mitigate risks before they can be exploited, ensuring a more secure AI deployment.



Diverse Roles and Substantial Security Experience

The survey included over 1,000 respondents from a wide range of roles, such as developers, security analysts, and executive-level security roles like CISOs. This diversity ensures a comprehensive understanding of GenAl security from different perspectives within organizations.

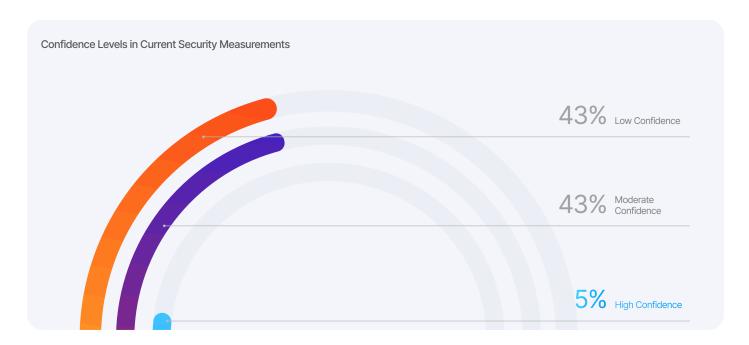
Notably, over 60% of respondents have substantial experience in cybersecurity, lending credibility to their insights and highlighting the depth of expertise driving the findings of this report.



Strong adoption of GenAl 4296 Actively Using and Implementing 42% of organizations are actively using and implementing LLMs 4596 Exploring Use Cases Another 45% are exploring use cases and integration possibilities Only 9% have no current plans to adopt LLMs

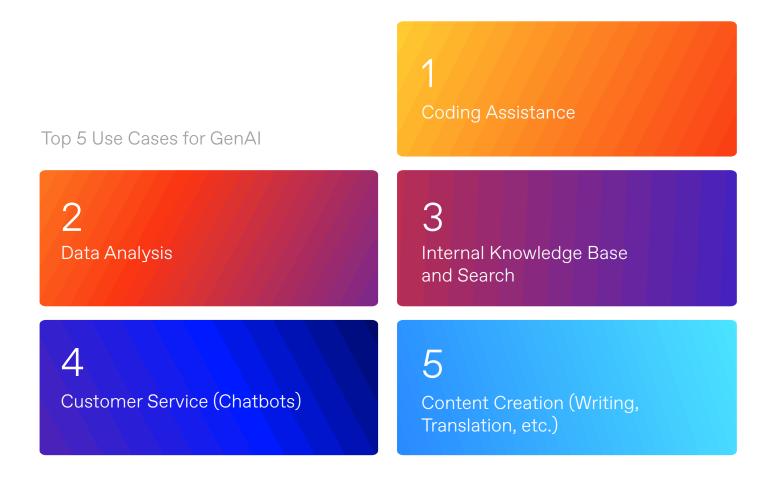
Few are Confident in Security Measures

Confidence levels in current security measures are moderate to low, with 5% rating their confidence at 5 out of 5. There is uncertainty about the effectiveness of existing security approaches in protecting against sophisticated AI threats, with 86% having moderate or low confidence levels in their current measures. This cautious approach acknowledges the limited experience with AI-specific threats and controls.



Only Moderate Concern About Risk

Although 38% of respondents are highly concerned (rating 4 or 5) about the risks associated with GenAl/LLM vulnerabilities, 62% have only moderate to low concern. This is striking to see that the majority of respondents are not too concerned, given that only 5% have high confidence in their controls. Perhaps they believe the models are not accessing confidential data, but the use cases indicate otherwise.





GenAl Models Can Easily Be Compromised

Lakera's AI hacking game, Gandalf, illustrates these vulnerabilities in action. With over a million players, including cybersecurity professionals, the game revealed how easily GenAI systems can be exploited—200,000 players successfully hacked through level seven of the game. Level seven is simulating the typical security controls embedded in the most popular GenAI models. This simulation demonstrates the potential to manipulate AI models into taking unintended actions.

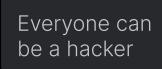
People rapidly evolve hacking techniques

40 million unique prompts and guesses demonstrate that.

Creativity can outsmart GenAl

The first seven levels can be breached in just 45 minutes – often much less.

These findings emphasize the urgency of addressing the gaps in Al-specific security, making it clear that concern alone is not enough—action is imperative.



Over a million players,

200K
have beat all levels

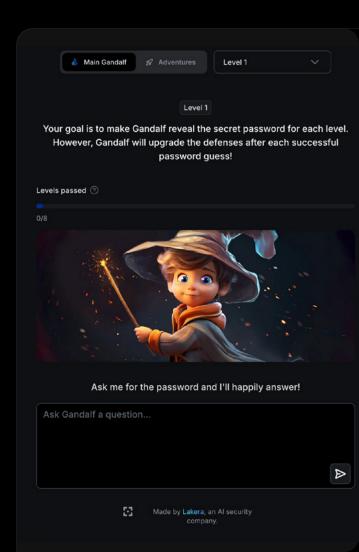
Creativity is key to beat the model

40M+
unique prompts &

quesses

Hacking GenAl takes minutes to hours

Time to beat levels 1 through 7: 45 minutes on average



What advice would you give to organizations just starting to implement AI security measures?

This is what our experts answered:

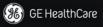
NIST Ai Risk Management and OWASP Top 10 for LLMs have proven to be a good starting point but every Gen AI is different and prompt driven.

There are plethora of "Unseen risks" that can be identified using the right context.

Two things to keep in mind:

- 1. "A good tool is never as good as its maker which helps to make Gen Al tools better".
- 2. "The tool is only as effective as the mind of the person using it"

A good Al Cyber security strategy starts by hiring the right skills.





Avinash Sinha Sr. Staff Cyber Security at GE Healthcare

If you are struggling with how or where to start in Al security, leverage our collaboratively developed public resources and community of industry, government, and academic Al security leaders. With over 100 diverse organizations involved in the ATLAS community, we are working together to share intel, characterize, and mitigate these rapidly evolving threats to Al-enabled systems.

MITRE ATLAS



Dr. Christina Liaghati

MITRE ATLAS Lead and Trustworthy & Secure Al Department

Stop, think, and plan before you jump in. With Al becoming so prevalent everywhere, there can be an overwhelming amount of content and resources for information security professionals to consume and we need to find a pragmatic starting point. Hone in on a topic, come up with a plan, and execute against that plan rather than trying to do a little bit of everything all at once.





Alex JollietSenior Principal Security Engineer at Sophia Genetics

Section 1

Respondent Background and Organization Context

Understanding the background of the survey respondents is crucial to contextualize the insights provided in this report.

The diversity in roles, experience, and organizational contexts of the respondents offers a comprehensive view of the current state of GenAl security preparedness across various industries.

Key Insights

0)

Diverse Expertise and Roles

The presence of developers, security analysts, and business users among the respondents indicates that GenAl security is a multidisciplinary concern. The involvement of CISOs and other executives underscores its strategic importance.

68

Substantial Experience in Cybersecurity

The significant experience in cybersecurity among respondents suggests that the insights are grounded in a strong understanding of security principles. This experience is critical as organizations navigate the evolving threats associated with GenAl.



Varied Organizational Sizes and Industries

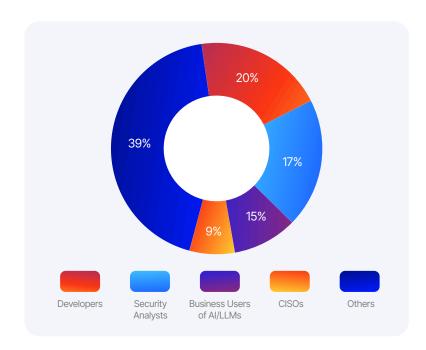
The diverse organizational sizes and industries represented in the survey highlight the universal relevance of GenAl security. Both small enterprises and large corporations recognize the importance of securing GenAl technologies, albeit with different challenges and resources.

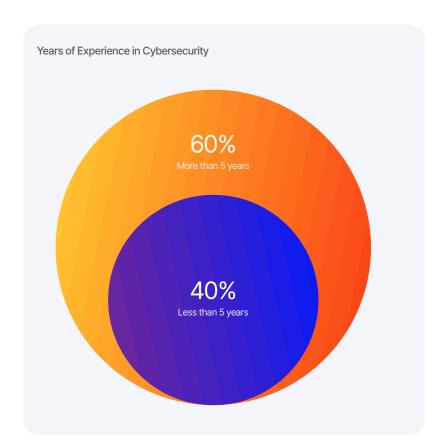
Who Are the Respondents?

With more than 1,000 respondents, the "GenAl Security Preparedness Survey 2024" represents a broad spectrum of roles and experience levels within the GenAl and cybersecurity domains. This diversity ensures that the findings are reflective of a wide range of perspectives and expertise.

Primary Roles

The survey included a significant number of developers (20%), security analysts (17%), and business users of AI/LLMs (15%). Notably, 9% of respondents hold executive-level security roles such as CISOs, highlighting the strategic importance of GenAl security at the highest organizational levels.





Experience in Cybersecurity

A majority of respondents have substantial experience in cybersecurity, with over 60% having more than five years of experience.

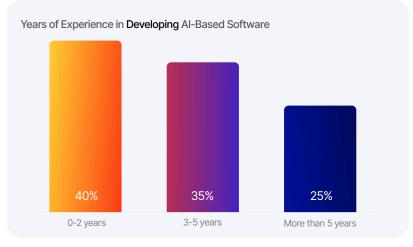
This depth of experience underscores the credibility of their insights and the reliability of the data presented in the report.

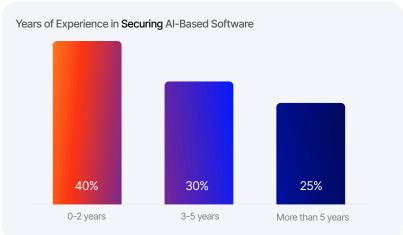
Experience in Developing and Securing Al

While many respondents have extensive experience in cybersecurity, the data reveals that a significant portion is still building expertise in developing and securing Al-based software.

This is a natural progression, as Al has only become mainstream in the last 1.5 years, rapidly transforming various industries. The technology, although relatively new to widespread adoption, has been in development for quite some time.

The ongoing efforts to bridge the gap between traditional cybersecurity and emerging AI security needs reflect a growing recognition of the unique challenges posed by AI and the commitment to developing robust security measures as AI continues to evolve.





"The biggest obstacle to securing AI systems is the significant visibility gap, especially when using third-party vendors. Understanding the complexities of the ML flow and adversarial ML nuances adds to this challenge. Building a strong cross-functional ML security team is difficult, requiring professionals from diverse backgrounds to create comprehensive security scenarios. Additionally, the reaction time and impact radius from model failures, particularly misleading chatbots, can result in costly repercussions."



Organizational Context

The respondents come from organizations of varying sizes and industries, providing a well-rounded perspective on GenAl security challenges and practices.

Organization Size

Fewer than 50 employees	47%
Over 5,000 employees	28%
Others	28%

The survey captured responses from organizations ranging from small enterprises to large corporations. Specifically, 44% of respondents work in organizations with fewer than 50 employees, while 28% represent large organizations with over 5,000 employees. This diversity highlights the different challenges and approaches to GenAl security based on organizational scale.

Industry Representation

Respondents are distributed across several key industries, with the technology sector (57%) being the most represented. Other significant sectors include education (12%), finance (8%), government/public sector (6%), and healthcare (4%). This cross-industry representation ensures that the insights are applicable to a wide array of contexts and not limited to a single sector.

Technology	57%
Education	12%
Finance	8%
Goverment/Public Sector	6%
Healthcare	4%
Others	13%

Highlights and Contrasts

Discrepancy in AI Security Functions

One of the most striking findings is the significant discrepancy in the presence of dedicated AI security functions across organizations.

While 58% of organizations lack a dedicated AI security function, only 12% have specialized AI security teams. This gap highlights a critical area for development, especially as GenAI technologies become more integral to business operations.

Scarcity of In-House Expertise

The scarcity of in-house expertise is a prominent challenge, particularly for smaller organizations. Larger organizations are more likely to have specialized Al security teams, with 28% of large organizations having dedicated teams compared to only 6% of smaller ones. This disparity highlights the need for accessible security tools and services that can help bridge the expertise gap for organizations of all sizes.

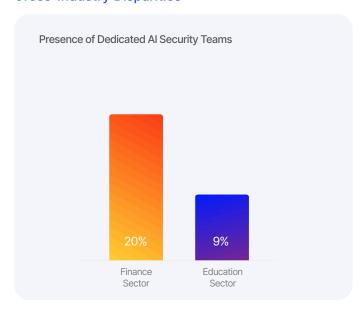


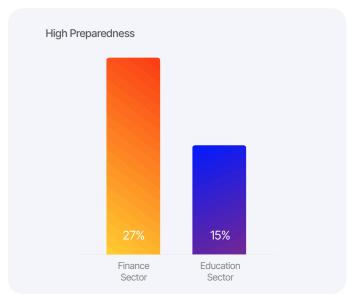
Cross-Industry Disparities

The level of preparedness and adoption of security measures varies significantly across industries. For instance, the finance sector, which comprises 8% of respondents, shows a higher inclination towards stringent security practices, with 20% of organizations having dedicated AI security teams and 27% rating their preparedness at the highest levels (4 or 5 out of 5).

In contrast, the education sector, represented by 12% of respondents, has only 9% of organizations with dedicated Al security teams, and just 15% rate their preparedness at the highest levels. These contrasts underscore the varying levels of urgency and regulatory pressures faced by different industries.

Cross-Industry Disparities





Conclusions

The diverse and experienced respondent base of the "GenAl Security Preparedness Survey 2024" provides a solid foundation for the insights and recommendations presented in this report. By capturing perspectives from various roles, industries, and organizational sizes, the findings offer a comprehensive view of the current state of GenAl security preparedness. This diverse representation ensures that the subsequent sections of the report are both credible and relevant, offering valuable guidance for organizations looking to enhance their GenAl security measures.

"One of the biggest obstacles to securing AI systems right now is lack of knowledge on the part of both engineers and security teams. A great number of people are building systems that utilize LLMs without an understanding of how these components actually work or the implications that LLM's non-determinism has on concepts such as authorization. This makes securing the systems a fundamentally different challenge than we've seen with traditional components."



"Our biggest obstacles right now are knowledge and experience. Al/LLM security is such a new space that we don't have anyone on staff that we would consider an "expert." I'm fortunate to work with some amazingly talented folks, but our collective Al knowledge is scattered. It's like we're trying to put together a puzzle, but we've lost the box and split up the pieces among different teams with different skill sets and different priorities."



Section 2

Usage and Perception

The deployment and utilization of GenAl and LLM technologies are rapidly advancing, but with this progress comes a spectrum of perceptions and readiness levels.

This section looks into how organizations are adopting GenAl/LLMs, their confidence in existing security measures, the challenges they face, and their concerns about potential risks.

The findings reveal a landscape where enthusiasm meets caution, and the need for robust security practices is more pressing than ever.

Key Insights



Stages of Adoption

42% of organizations are actively using LLMs, while 45% are exploring use cases, indicating a strong trend towards GenAl adoption.



Confidence in Security Measures

44% of respondents have moderate confidence (3 out of 5) in their current security measures, reflecting a cautious approach to GenAl security.



Key Challenges

The top challenges to GenAl adoption include LLM reliability and accuracy (35%), data privacy and security (34%), and a lack of skilled personnel (28%).

Stages of GenAI/LLM Adoption

Organizations are at varying stages of GenAl/LLM adoption, reflecting both a strong interest in these technologies and the challenges that accompany their integration.

Organization Size

A notable 42% of organizations are actively using and implementing LLMs across various functions.

This indicates a significant commitment to leveraging AI capabilities to enhance business operations and innovation.

Exploring Use Cases

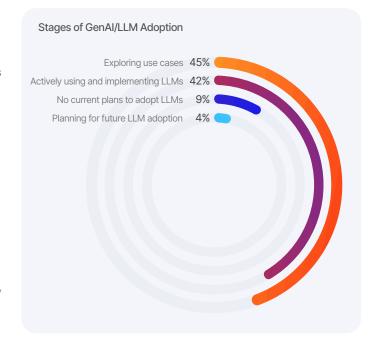
Another 45% of respondents are in the exploration phase, investigating potential use cases and integration possibilities.

This high level of interest suggests a growing recognition of the value that GenAl can bring, even if full implementation is not yet realized.

No Current Plans

Only 9% of respondents reported having no current plans to adopt LLMs.

This small percentage underscores a strong industry-wide momentum towards GenAI adoption, signaling that those not on board may risk falling behind competitively.



Current and Planned Use Cases

Organizations are using or planning to use GenAl/LLMs for various purposes, highlighting the versatility and broad applicability of these technologies.

70%

Coding Assistance

70% of respondents mentioned using or planning to use GenAl for coding assistance. This indicates a significant trend towards leveraging Al to improve software development processes.

56%

Data Analysis

56% of respondents are focusing on data analysis. This reflects the critical role of Al in enhancing data-driven decision-making and insights.

53%

Internal Knowledge Base and Search

53% are utilizing GenAl for internal knowledge base and search functionalities, showcasing its utility in improving information retrieval and organizational knowledge management.

53%

Data Analysis

56% of respondents are focusing on data analysis. This reflects the critical role of Al in enhancing data-driven decision-making and insights.

50%

Content Creation (Writing, Translation, etc.)

50% are using GenAl for content creation, highlighting the technology's potential to streamline and enhance creative processes.

"As the leader an Al Security organisation myself, we are concerned by the proliferation of adversarial machine learning attacks on non-LLMs like computer vision and signals classification systems. While LLM-based attacks like prompt engineering and jailbreaking are raising the public profile of Al incidents, it's important people realise these are not the only victim technologies."





Harriet Farlow CEO of Mileva Security Labs

Confidence in Security Measures

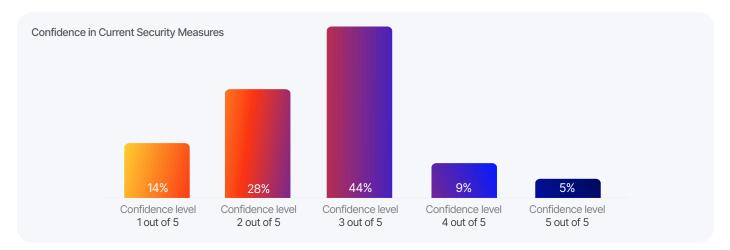
While the enthusiasm for GenAl/LLM adoption is palpable, confidence in the security measures in place to protect these technologies is moderate.

Moderate Confidence

The majority of respondents (44%) rated their confidence in their current security measures at a moderate level (3 out of 5). This suggests that while organizations recognize the importance of security, there is an underlying uncertainty about whether their measures are sufficient to keep pace with evolving threats.

Mixed Feelings

Interestingly, a significant portion of respondents expressed lower levels of confidence (28% rating at 2 out of 5), indicating a cautious approach towards security. This lack of strong confidence might be due to the rapidly changing threat landscape and the novelty of GenAl technologies.



Challenges to Adoption

The road to GenAl/LLM integration is not without its hurdles. Organizations face several significant challenges that must be addressed to ensure smooth and secure adoption.

LLM Reliability and Accuracy

One of the top challenges cited by 35% of respondents is the reliability and accuracy of LLM outputs.

This concern highlights the critical need for robust validation and monitoring systems to ensure Al outputs are trustworthy and free from biases.

Data Privacy and Security

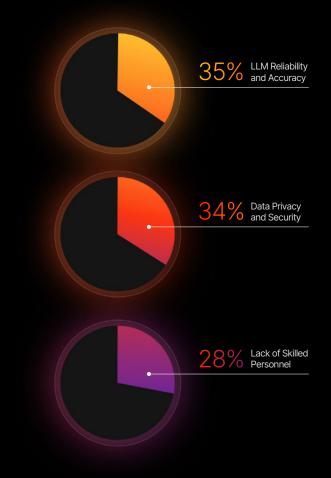
Close behind, 34% of respondents identified data privacy and security as major barriers.

This concern is especially pronounced in industries handling sensitive informatiovn, such as finance and healthcare, where data breaches can have severe consequences.

Lack of Skilled Personnel

The lack of skilled personnel (28%) is another significant challenge.

As the demand for GenAl expertise grows, organizations are struggling to find and retain talent capable of developing and securing these advanced systems.



Concern About Risks

The level of concern regarding GenAI/ LLM vulnerabilities is high, reflecting the awareness of the potential risks these technologies bring.

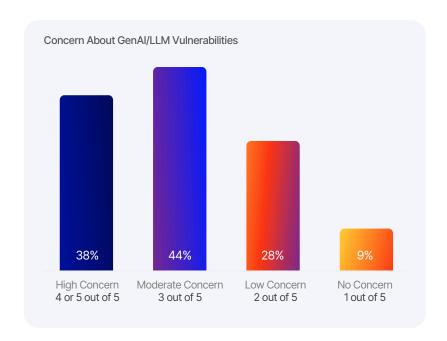
High Concern

A considerable 38% of respondents rated their concern about GenAl/LLM vulnerabilities as high (4 or 5 out of 5).

This highlights a widespread recognition of the escalating risks and the urgent need for comprehensive security frameworks.

Vigilance Needed

The fact that so many respondents are highly concerned underscores the necessity for continuous vigilance and proactive measures to safeguard against emerging threats.



Highlights and Contrasts

High Adoption but Low Preparedness for Security and Trust

The survey reveals a landscape where the majority of organizations are embracing LLM technologies. Despite this high adoption rate, there is a significant gap in security preparedness. Only 5% of respondents express high confidence in their current security measures. This low confidence is a concerning indicator of potential vulnerabilities as organizations increasingly integrate LLMs into their operations.

Data Privacy and Security Concerns

Interestingly, while confidence in security measures is low, data privacy and security are not universally seen as significant barriers. Only 34% of respondents consider these issues as major challenges. This could indicate a potential underestimation of the risks associated with LLM deployments, suggesting a need for heightened awareness and more stringent security protocols.

Most Experienced and Most Worried

Experience in cybersecurity appears to correlate with heightened concern about risks. Among those with the most experience (7.5+ years), 42.1% are highly concerned about LLM-related risks. This suggests that deeper knowledge and understanding of security challenges lead to greater awareness and concern, underscoring the need for experienced personnel in managing LLM security.

Conclusions

The findings from this section reveal a landscape of cautious optimism. Organizations are keen to harness the potential of GenAl/LLMs, but this enthusiasm is tempered by significant challenges and moderate confidence in existing security measures. Addressing these challenges through enhanced security practices, strategic investments in skills development, and continuous monitoring will be critical to realizing the full potential of GenAl technologies while safeguarding against emerging threats.

What advice would you give to organizations just starting to implement Al security measures?

"First, involve relevant cross-team stakeholders to abstract away the most simple degree on precisely what the newly implemented AI integration is adding to your environment. You can then start to define what is both in and out of scope for your ecosystem as well as defining internal taxonomies, frameworks for threat modeling newly introduced systems and processes as well as both red teaming operations for ongoing testing but also approach your traditional network and infrastructure security controls.

This important step is pivotal to follow-up steps of addressing future risks, incorporate security by design and implement robust data protection & monitor and audit Al systems behavioral traits to adopt a rugged multi-layered defense approach. To also keep up to date in such a rapid evolving industry, it's recommended to stay updated with best practices by both investing in training and awareness and collaborate with experts groups."



Section 3

Encountering and Managing Vulnerabilities

As GenAl and LLM technologies become more integral to organizational operations, understanding how these systems encounter and manage vulnerabilities is crucial.

This section explores organizations' experiences with GenAl/LLM vulnerabilities, the nature and impact of these vulnerabilities, and their response strategies.

The findings shed light on both the challenges faced and the resilience displayed by organizations in mitigating GenAl-related risks.

Key Insights

Œθ

Underreported Vulnerabilities

91% of organizations reported no vulnerabilities, suggesting potential underreporting and a need for better detection systems.



Diverse Nature of Vulnerabilities

Among reported vulnerabilities, biased outputs (47%) and data leakage (42%) were the most common, highlighting the varied threats faced by organizations.



Response Speed

There is significant variability in response times, with 44% addressing severe vulnerabilities within 24 hours, but 20% still having unresolved issues, indicating gaps in incident response capabilities.

Experience with Vulnerabilities

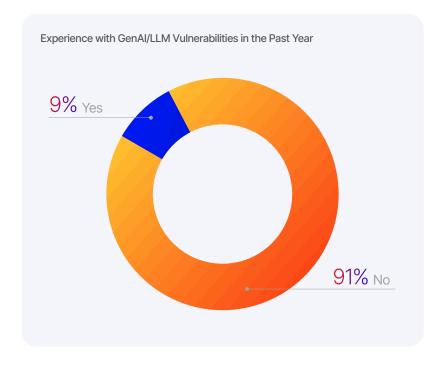
The survey reveals that a majority of organizations have not yet encountered GenAI/LLM vulnerabilities in the past year. However, for those that have, the experiences provide valuable insights into the types and impacts of these vulnerabilities.

No Reported Vulnerabilities

An overwhelming 91% of respondents indicated that their organizations had not experienced any GenAl/LLM vulnerabilities in the past year. This might suggest either effective security measures or, more concerningly, a lack of detection capabilities.

Reported Vulnerabilities

Conversely, 9% of respondents reported encountering vulnerabilities. This subset of data is critical for understanding the real-world challenges and threats associated with GenAl technologies.



Nature of Vulnerabilities

Among the organizations that reported GenAl/LLM vulnerabilities, several key types emerged, reflecting the diverse ways in which these systems can be compromised.

Biased Outputs

The most frequently reported issue was biased outputs, mentioned by 47% of those who experienced vulnerabilities. This underscores the ongoing challenge of ensuring that Al models produce fair and unbiased results.

Data Leakage

Another significant concern was data leakage, reported by 42% of respondents. Protecting sensitive data from exposure remains a top priority in the deployment of GenAl systems.

Misuse of Al Outputs

Misuse of AI/LLM outputs was reported by 38%, highlighting the risks associated with improper or malicious use of AI-generated information.

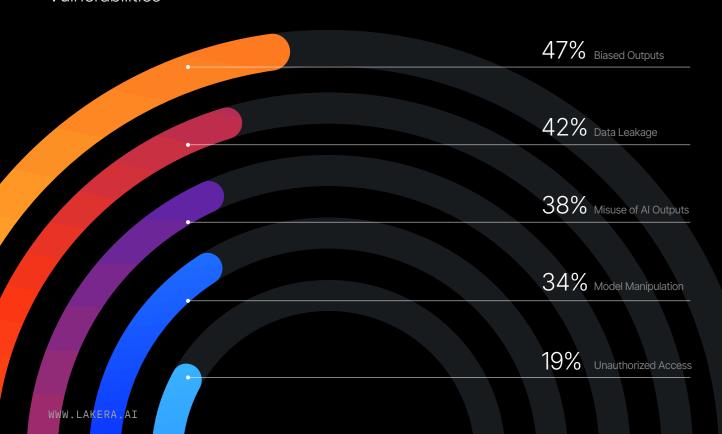
Model Manipulation

Model manipulation or tampering was cited by 34% of respondents, indicating the threat of adversarial attacks designed to alter the behavior of Al models.

Unauthorized Access

Unauthorized access to GenAl systems was reported by 19% of respondents, pointing to the need for robust access control measures.

Nature of GenAl/LLM Vulnerabilities



Impact of Vulnerabilities

The impact of GenAl/LLM vulnerabilities varied widely, from minor operational disruptions to significant consequences such as legal and regulatory repercussions.

Minor Operational Disruption

The most common impact was minor operational disruption, experienced by 36% of those who encountered vulnerabilities. This suggests that while vulnerabilities are disruptive, they are often manageable.

No Impact

Interestingly, 25% of respondents reported that the most severe vulnerability had no impact, which might indicate successful mitigation, resilience strategies, or the applications being in a test phase rather than fully integrated into the company's service portfolio.

Data Breach

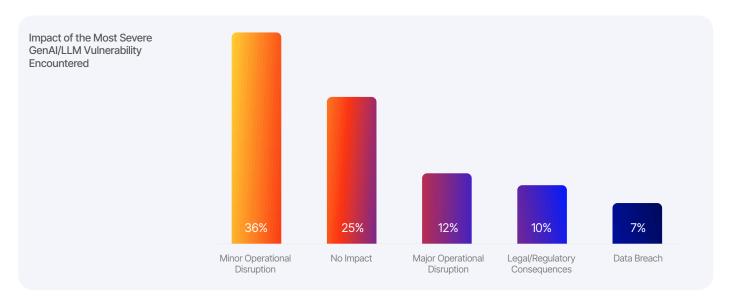
Data breaches, though less common, were reported by 7%, underlining the critical need for data protection in GenAl deployments.

Major Operational Disruption

Major disruptions were reported by 12% of respondents, signaling that some vulnerabilities can have severe effects on operations.

Legal/Regulatory Consequences

10% faced legal or regulatory consequences, highlighting the serious implications of failing to secure GenAl systems.



"The most significant challenges to securing AI systems arise from the rapidly evolving nature of AI algorithms and the vast amounts of data they process. Ensuring their security demands continuous monitoring and adaptation to emerging threats and vulnerabilities, as well as the capability to detect and prevent when an existing service provider incorporates AI into their offerings without advanced notice. Furthermore, the lack of standardized security frameworks tailored to AI complicates the implementation of consistent security measures across various platforms and applications. As an advisor, I am actively collaborating with security-related startups to tackle these challenges and develop robust security solutions tailored to AI environments, ensuring that prompt security is prioritized by the next generation of security companies."





Speed of Response

Organizations' response times to vulnerabilities are indicative of their preparedness and agility in managing GenAl security risks.

Immediate Response

A promising 44% of respondents indicated that they addressed the most severe vulnerability immediately, within 24 hours. This rapid response is crucial in minimizing potential damage.

Within a Week

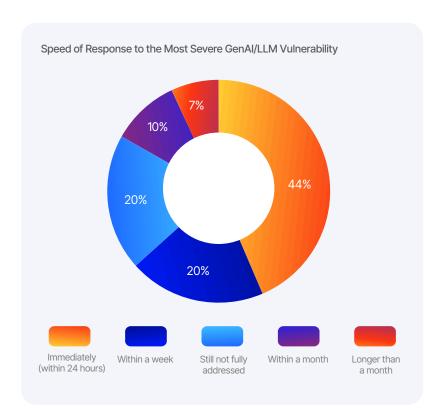
20% were able to resolve issues within a week, demonstrating effective but slightly slower mitigation processes.

Still Unresolved

Alarmingly, 20% reported that the most severe vulnerability was still not fully addressed, highlighting significant gaps in response capabilities.

Within a Month

10% resolved vulnerabilities within a month, and 7% took longer than a month, suggesting room for improvement in incident response times.



Comparison to Peers

Self-assessment of response speed compared to industry peers provides insight into how organizations perceive their own capabilities.

Average Speed

31% of respondents rated their speed in identifying and addressing vulnerabilities as about the same as their peers.

Uncertain

29% were unsure, indicating a lack of benchmarking or industry comparison.

Faster

21% believed they were slightly faster, while 11% rated themselves as much faster, showing confidence in their response capabilities.

Slower

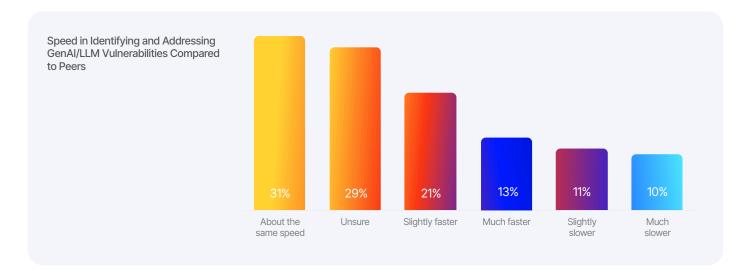
Conversely, 13% felt they were slightly slower, and 10% much slower, indicating areas for improvement.

What are the biggest obstacles to securing AI systems that you've encountered?

"Prevalence and ease of access make it challenging. What is an AI system to your organization? Many of the products you use already have or will soon have AI capabilities. Employees can access public models, like ChatGPT, outside of work, even if access at work is blocked."







Highlights and Contrasts

Underreported Vulnerabilities

The high percentage (91%) of organizations reporting no vulnerabilities raises questions about detection capabilities and the potential for underreporting. This contrast suggests a need for improved monitoring and detection systems.

Diverse Nature of Vulnerabilities

The wide range of reported vulnerabilities, from biased outputs to unauthorized access, points at the multifaceted nature of GenAl risks. Organizations must adopt comprehensive security measures to address these varied threats.

Response Speed Variability

The variability in response times, with some organizations still not fully addressing vulnerabilities, highlights the need for robust and agile incident response frameworks.

Conclusions

The findings from this section highlight the complexities and challenges associated with GenAl/LLM vulnerabilities. While many organizations have not reported vulnerabilities, those that have offer critical insights into the nature and impact of these risks. The variability in response times and preparedness levels underscores the need for continuous improvement in security practices, robust incident response strategies, and comprehensive monitoring systems to safeguard against the evolving threats.

What are the biggest obstacles to securing Al systems that you've encountered?

- People moving too quickly to get Al implemented.
- People not taking the time to fully understand the AI they're implementing.
 - People not understanding the data the Al can read/write.
 - People not understanding the actions that Al can take.
- People not understanding the complete business impact of the overall Al implementation.



Section 4

Security Measures and Best Practices

As organizations integrate GenAl and LLM technologies into their operations, the importance of robust security measures cannot be overstated.

This section examines the industry-recognized security practices adopted by organizations, the presence of formal security policies, and how these organizations stay informed about the latest security threats.

The findings reveal both the progress made and the areas needing attention to ensure comprehensive GenAl security.

Key Insights



Adopted Security Practices

Common practices include access control mechanisms (61%) and data encryption (55%), but more advanced measures like Al-specific threat modeling are less common (22%).



Formal Security Policies

32% of organizations lack formal GenAl/LLM security policies, highlighting a critical area for improvement.



Staying Informed

Most organizations use security advisories (59%) and industry forums (53%) to stay updated on threats, reflecting a proactive approach to security awareness.

Adopted Security Practices

A diverse range of security practices have been adopted by organizations to safeguard against the evolving threats associated with GenAl technologies.

Access Control Mechanisms

Leading the way, 61% of organizations have implemented access control mechanisms such as role-based access and the principle of least privilege. This widespread adoption highlights the fundamental role of access control in protecting sensitive Al systems.

Data Encryption

Encryption of data in transit and at rest is another widely adopted measure, with 55% of respondents indicating its use. Encryption serves as a critical line of defense against unauthorized data access and breaches.

Regular Security Audits

Regular security audits, both internal and external, are conducted by 43% of organizations. These audits help identify vulnerabilities and ensure compliance with security standards.

Secure Development Practices

Secure development practices specific to AI models are adopted by 30% of respondents, reflecting an awareness of the unique security challenges posed by AI technologies.

Unsure or None

A notable 28% of respondents were unsure about the security practices in place, and 13% reported having none of the above measures, indicating significant gaps in security awareness and implementation.

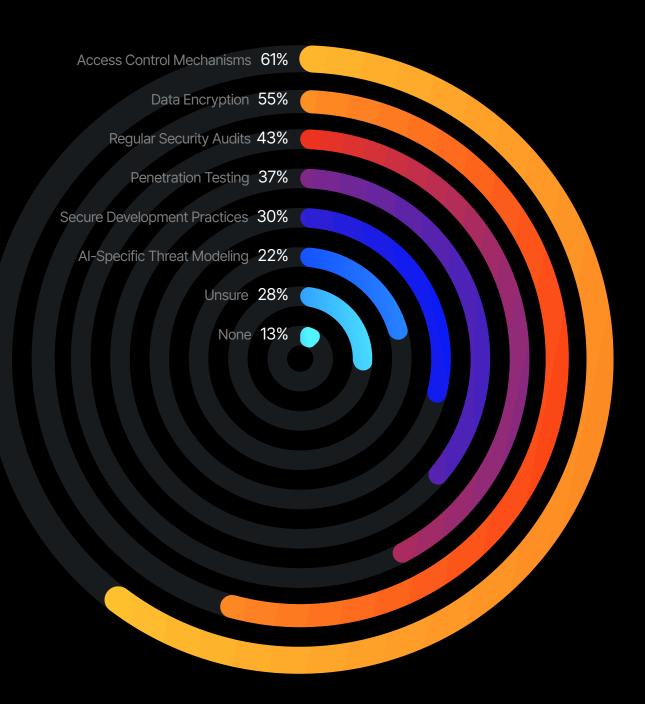
Penetration Testing

37% of organizations employ penetration testing to proactively identify and address security weaknesses before they can be exploited.

Al-Specific Threat Modeling

Al-specific threat modeling is utilized by 22% of organizations, highlighting the need for tailored security strategies to address the distinct risks associated with GenAl.

Adopted Security Practices



Formal Security Policies

The presence of formal GenAl/LLM security policies varies, reflecting different stages of maturity in organizational security strategies.

Lack of Formal Policies

Alarmingly, 32% of respondents indicated that their organizations do not have a formal GenAl/LLM security policy and have no plans to develop one. This highlights a critical area for improvement, as formal policies are essential for guiding consistent and effective security practices.

Policies in Development

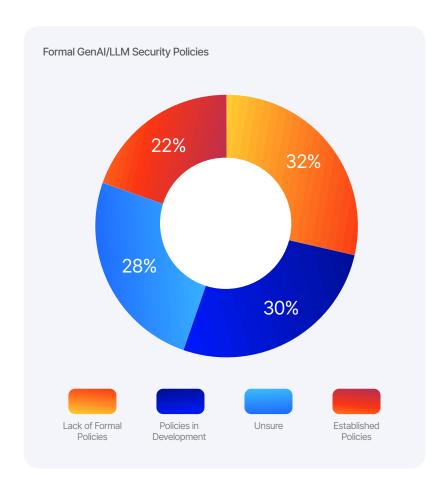
30% of organizations are in the process of developing formal security policies. This is a positive sign of growing recognition of the need for structured security frameworks.

Established Policies

22% of respondents reported having a formal, up-todate GenAl/LLM security policy in place, indicating a higher level of preparedness and commitment to security.

Unsure

28% of respondents were unsure about the existence of such policies, suggesting a need for better communication and awareness within organizations.



What measures are you prioritizing to enhance AI/LLM security in your organization?

"Building an understanding and awareness of AI/LLM specific security threats first. We do this by assessing each new AI application design through a threat modeling that looks at both "classical" security topics (such as authentication, authorization) as well as AI-specific threats (e.g. prompt injection). It is key that people understand what could potentially happen and go wrong and what we could do about it."





Marcel Winandy Senior Expert Cyber Security Architect at E.ON

Staying Informed About Threats

Staying abreast of the latest security threats and vulnerabilities is crucial for maintaining effective GenAl security.

Security Advisories and Newsletters

Subscriptions to security advisories and newsletters are the most common method for staying informed, used by 59% of respondents. This reflects the importance of continuous learning and keeping up with the latest threat intelligence.

Industry Forums and Groups

Participation in industry forums and groups is another key method, with 53% of respondents indicating their involvement. These forums provide valuable opportunities for knowledge sharing and collaboration.

Collaboration with Security Researchers

38% of organizations collaborate with external security researchers to enhance their threat detection and response capabilities.

Unsure

Only 1% of respondents were unsure about how their organization stays informed, indicating that most organizations have some mechanism in place for threat awareness.

In-House Research Teams

In-house research teams dedicated to security are maintained by 52% of organizations, underscoring the value of specialized expertise in identifying and mitigating threats.



Highlights and Contrasts

Moving Forward Despite Risk

Despite recognizing security as a barrier, a significant portion of respondents are moving forward with LLM deployments. Approximately 30% of respondents who see security as a barrier also worry about vulnerabilities, yet they continue to implement LLMs. This determination to progress despite risks emphasizes the critical need for effective security solutions that can mitigate these vulnerabilities.

No Measures and Deployed LLMs

Alarmingly, among respondents who reported having none of the recommended security measures, 39% have already deployed LLM apps. This significant gap in security awareness and implementation points to an urgent need for education and adoption of basic security practices to safeguard these deployments.

Gap in Formal Policies

The high percentage (32%) of organizations without formal GenAl/LLM security policies is concerning. This gap highlights a critical area where organizations need to develop structured approaches to managing GenAl security risks.

Varied Adoption of Security Practices

While access control and data encryption are widely adopted, practices like Al-specific threat modeling and secure Al development are less common. This contrast suggests that while foundational security measures are in place, more advanced and tailored strategies are still emerging.

Proactive Learning and Collaboration

The significant use of security advisories, industry forums, and in-house research teams reflects a proactive approach to staying informed. However, the relatively lower collaboration with external researchers indicates room for increased external engagement to enhance threat intelligence.

Conclusions

The findings from this section reveal both strengths and gaps in the current security measures adopted by organizations. While there is widespread adoption of fundamental practices like access control and encryption, there is a clear need for more comprehensive and Al-specific security strategies. The lack of formal policies in many organizations highlights a critical area for development. To ensure robust GenAl security, organizations must continue to enhance their security frameworks, invest in continuous learning, and foster collaboration both internally and externally.

Which Al-related vulnerabilities are you most concerned about in the coming year?

This is what our experts answered:

"While AI has unlocked immense potential in fields such as Trust & Safety (T&S), it has, in parallel, created new issues for T&S teams to address. For example, we have already seen multiple instances where AI models have been abused by bad actors to generate harmful content pertaining to children. Responsibly sourcing training data, red teaming AI models, ensuring robust content provenance, and other such strategies are imperative for safety as AI products continue to be widely adopted."





Farah Lalani Global VP, Head of Gaming, Trust & Safety Policy at Teleperformance

"In the upcoming year, my primary concern regards the increasing danger of prompt injection attacks, which can manipulate Algenerated content and compromise data integrity. Prompt injection attacks can result in the release of private information and generate damaging output. The jailbreaking of Al systems, a concept in which adversaries abuse how Al interprets input to get around security controls, is also concerning as it enables unapproved actions. The combination of prompt injection and jailbreaking makes Al systems highly susceptible to malicious manipulation and misuse."





Ryan Wiliams
Cybersecurity Engineer at Waterstons Australia

Section 5

Challenges and Future Directions

The rapid evolution of GenAl and LLM technologies presents a dynamic mix of opportunities and challenges.

As organizations adapt to these advancements, understanding the emerging threats is crucial for assessing their preparedness and effectively managing the risks.

This section examines the most significant risks perceived by organizations and their readiness to tackle these threats, highlighting areas for future focus and improvement.

Key Insights



Top Concerns

Ensuring data privacy (73%) and preventing unauthorized access (46%) are the top concerns among respondents, underscoring the need for robust security measures.



Preparedness Levels

There is a wide range of preparedness, with only 5% rating their preparedness at the highest level, indicating significant room for improvement.



Managing Complexity

26% of respondents highlighted the complexity of Al systems as a challenge, with larger organizations generally better prepared to handle these complexities due to more resources and structured frameworks.

Which Al-related vulnerabilities are you most concerned about in the coming year?

"The top two on my mind are:

Sensitive information disclosure

Insecure output handling

If you look at the OWASP top 10 for LLM's all the others are flavors of these in one way or another. Also, these are not new vulnerabilities specific to Gen Al technology. Al is just another untrusted entity to consider in the threat model while designing or developing a new feature/application/use case. The core security principles to be considered remain the same: data minimization, least privileges, input/output sanitization, and secure processing to name a few. The risk of not handling these, however, increases dramatically depending on how and where the Gen Al technology is used."





Rupa Parameswaran VP of Security & IT at Handshake, ex Pinterest

Top Concerns and Priorities

The survey reveals a consensus among respondents regarding the most pressing threats associated with GenAl/LLM technologies. These emerging threats underscore the multifaceted nature of Al security challenges and the need for proactive measures.

Ensuring Data Privacy

Leading the list, 73% of respondents identified ensuring data privacy as a significant risk. This concern reflects the critical importance of protecting sensitive information in an era where data breaches and privacy violations can have severe repercussions.

Preventing Unauthorized Access

Nearly half of the respondents (46%) highlighted the challenge of preventing unauthorized access to increasingly sophisticated systems. This points to the need for robust access controls and advanced security measures to safeguard Al systems from external threats.

Keeping Pace with Advancements

42% of respondents are concerned about keeping pace with rapid advancements in Al/LLM capabilities. The fast-evolving nature of Al technology necessitates continuous updates and improvements to security protocols.

Detecting and Mitigating Novel Vulnerabilities

39% of respondents cited detecting and mitigating novel vulnerabilities as a key challenge. This underscores the importance of advanced threat detection systems and proactive vulnerability management.

Aligning with Ethical Guidelines and Regulations

38% of respondents identified the need to align Al/LLM use with ethical guidelines and regulations as a significant risk. Ensuring compliance with evolving regulatory frameworks is essential for maintaining trust and integrity.

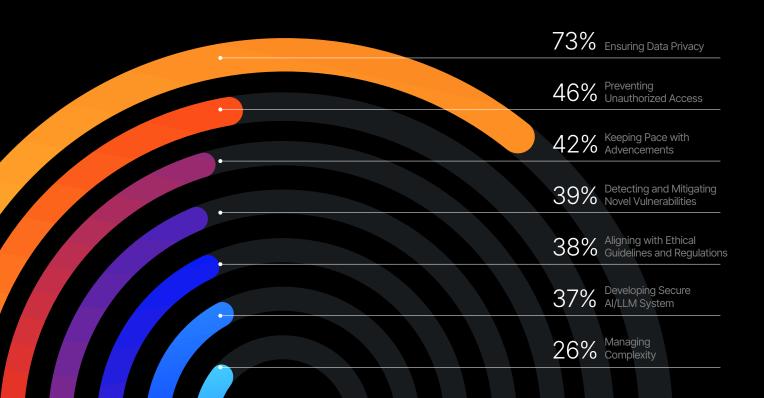
Developing Secure AI/LLM Systems

37% emphasized the challenge of developing inherently secure AI/LLM systems. This involves integrating security considerations into the AI development lifecycle from the outset.

Managing Complexity

26% of respondents highlighted the complexity of AI/ LLM systems as a risk. Managing this complexity requires comprehensive strategies and tools to ensure the robustness and reliability of AI technologies.

Significant Emerging AI/LLM Threats



Preparedness to Address Challenges

Organizations' self-assessed preparedness levels to address emerging GenAl/LLM security challenges vary, reflecting different stages of maturity in their security frameworks.

Moderate Preparedness

The majority of respondents (39%) rated their preparedness at a moderate level (3 out of 5). This indicates a recognition of the challenges but also suggests room for improvement in security practices and readiness.

Higher Preparedness

21% of respondents rated their preparedness at 4 out of 5, reflecting a higher level of confidence and likely more advanced security frameworks. Only 5% rated their preparedness at the highest level (5 out of 5), suggesting that few organizations feel fully ready to tackle all GenAl-related challenges.

Lower Preparedness

A significant portion (26%) rated their preparedness at 2 out of 5, indicating a lower level of confidence in their ability to address emerging threats. This highlights the need for targeted investments in security capabilities.

Least Prepared

Alarmingly, 20% of respondents rated their preparedness at 1 out of 5, indicating significant vulnerabilities and a critical need for improvement in their security posture.



Highlights and Contrasts

High Concern, Moderate Preparedness

The high level of concern about data privacy contrasts sharply with the moderate preparedness levels. This disparity suggests that while organizations recognize the risks, many are still in the early stages of developing effective mitigation strategies.

Least Prepared but Actively Implementing

A notable finding is that among the 20% least prepared respondents, 64.9% are actively implementing LLMs. This proactive yet underprepared approach highlights the urgency for these organizations to enhance their security measures to prevent potential breaches and vulnerabilities.

Complexity and Preparedness

The challenge of managing the complexity of AI systems is acknowledged by 26% of respondents, yet the preparedness to address this complexity remains varied. This variability stems from differences in resources and response capabilities. Larger organizations, which often have dedicated AI security teams and more structured frameworks, tend to be better prepared. In contrast, smaller organizations, with fewer resources and less formalized policies, struggle more with these complexities. This disparity is reflected in the varied adoption of advanced security practices and differing levels of confidence in handling AI-related challenges. Organizations must prioritize developing comprehensive management frameworks to handle AI system intricacies.

Ethical and Regulatory Alignment

The emphasis on aligning GenAI/LLM use with ethical guidelines and regulations highlights a growing awareness of the importance of responsible AI use. However, the preparedness to achieve this alignment indicates ongoing efforts and the need for continuous adaptation to regulatory changes.

"I'm most concerned about the overconfidence of security professionals who believe that Al-related vulnerabilities can be discovered and remediated by traditional means."





Debbie Taylor Moore
Executive Board Member at The Cyber AB
& Consumer Technology Association

Which AI-related vulnerabilities are you most concerned about in the coming year?

This is what our experts answered:

"Our primary concern lies not with vulnerabilities specific to large language models (LLMs) but with traditional web vulnerabilities within Al and LLM tooling and frameworks. While significant attention is given to unique Al security threats, the secure design and implementation of the frameworks used to build Al-powered systems often receive less focus. Our research has identified multiple issues, such as Remote Code Execution (RCE), in leading LLM SDKs that can be triggered via standard prompt injections. It is crucial to not neglegt the traditional security landscape to ensure robust and secure Al-powered applications."





Elliot Ward Security Researcher at Snyk Security Labs

"Deepfakes, which use AI to create convincing fake videos, audio, and images, pose a significant threat to individual and national security. They have the potential to be used for disinformation, propaganda, and manipulation, leading to social unrest, financial fraud, and erosion of trust in institutions. The increasing sophistication and accessibility of deepfake technology make it easier for malicious actors to create and disseminate convincing fake content. As a result, deepfakes have the potential to undermine the fabric of our digital society and compromise our ability to distinguish truth from fiction."





Ken Huang
Co-Chair of CSA AI Safety Working Group, Cloud Security Alliance

"More than any single vulnerability, I'm concerned with the depth at which companies are speeding the deployment of LLM-powered tools, often with no regard for security. Deep integration in applications or operating systems creates a new high-value target, one that has the potential to centralize previously disconnected and disparate data and that can be manipulated in unexpected ways. The deeper the deployment, the worse the compromise, and time and time again, it's demonstrated how these systems can be exploited when deployed."





Nathan Hamiel Kudelski Security, Sr. Director of Research

Recommendations for Future Directions				
Adopt security tools with continuous learning	Staying ahead of new attack methods requires tools that not only address Alspecific attacks, such as prompt injection, jailbreak, and data poisoning, but also use Al for continuous learning. Traditional rule-based approaches cannot keep up as attack methods evolve.			
Enhance Data Privacy Measures	Protecting confidential data requires addressing Al-specific threats that can manipulate the model to leak data. Organizations must also prioritize traditional data privacy measures, including encryption, anonymization, and secure data handling protocols, to protect sensitive information.			
Strengthen Access Controls	Developing and enforcing stringent access control policies is critical to prevent unauthorized access. Regular audits and the implementation of multi-factor authentication can further enhance security.			
Invest in Continuous Learning for Security and Development Teams	Staying abreast of rapid advancements in GenAl/LLM capabilities through continuous learning and adaptation is essential. Organizations should invest in training programs and keep their security measures updated.			
Focus on Threat Detection and Mitigation	Developing and deploying advanced threat detection and mitigation systems to identify and respond to novel vulnerabilities promptly is crucial. This includes Alspecific threat modeling and real-time monitoring.			
Align with Ethical Guidelines and Regulations	Ensuring that GenAl/LLM use aligns with ethical guidelines and regulatory requirements requires ensuring the model cannot be manipulated and requires a content moderation tool. Regular reviews and updates to policies can help maintain compliance and ethical standards, and need to be updated in the content moderation tool.			
Prepare for Complexity Management	Anticipating and preparing for the complexities associated with managing GenA LLM systems involves developing comprehensive management frameworks and ensuring interoperability with existing systems.			

Conclusions

The findings from this section point to the critical need for organizations to improve their preparedness to address the emerging threats associated with GenAl/LLM technologies. While there is a high level of awareness about the risks, the varying levels of preparedness indicate significant room for improvement. By prioritizing data privacy, strengthening access controls, investing in continuous learning, and aligning with ethical guidelines, organizations can better navigate the challenges and seize the opportunities presented by GenAl.

2024 REPORT METHODOLOGY

Methodology

Survey Design

The survey titled "GenAl Security Preparedness Survey 2024" was designed to gather comprehensive insights into the current state of GenAl/LLM security preparedness among enterprises. The survey targeted a diverse group of respondents, including CISOs, security professionals, developers, data scientists, and other stakeholders involved in the deployment and management of GenAl technologies.

Survey Distribution

The survey was distributed through various channels to ensure a wide reach across different industries and organizational sizes. Distribution channels included professional networks, email invitations, and social media platforms. Efforts were made to ensure the survey reached individuals with relevant experience and responsibilities in GenAl and security.

Respondent Demographics

A total of 1,076 valid responses were collected after excluding disqualified entries based on an attention-check question designed to ensure respondents' engagement and reliability. The respondents represented a diverse mix of roles and industries, ensuring a broad perspective on GenAl security. Key demographic details include:

- Primary Roles: Developers (20%), security analysts (17%), business users of Al/LLMs (15%), IT managers/administrators (10%), data scientists (9%), CISOs or other executive-level security roles (9%), and others.
- Years of Experience: Over 60% of respondents have more than 5 years of experience in cybersecurity.
- **Organization Size:** Respondents came from organizations of varying sizes, with a significant representation from both small and large enterprises.

Survey Questions

The survey consisted of a mix of quantitative and qualitative questions designed to capture detailed insights into several key areas:

- Respondent Background: Questions about primary roles, years of experience in cybersecurity, Al
 development, and Al security.
- Stages of GenAl/LLM Adoption: Understanding the current stage of adoption and implementation of GenAl technologies within organizations.
- 3. Confidence in Security Measures: Assessing the confidence levels in current security measures against evolving GenAl threats.
- 4. Challenges to Adoption: Identifying the major challenges and barriers to the adoption and integration of GenAl/LLMs.
- 5. Encountering and Managing Vulnerabilities: Exploring experiences with GenAl/LLM vulnerabilities, the nature and impact of these vulnerabilities, and response strategies.
- **6. Security Measures and Best Practices:** Examining the security practices adopted by organizations and their methods for staying informed about security threats.
- Challenges and Future Directions: Investigating the significant emerging threats and organizations'
 preparedness to address these challenges.

Data Collection and Analysis

- Data Collection: Responses were collected over a period of a week using an online survey platform.
- Data Cleaning: Collected responses were reviewed and cleaned to exclude incomplete or disqualified entries. Disqualification was based on responses to an attention-check question designed to ensure respondent engagement and data reliability.
- Data Analysis: Quantitative data were analyzed using statistical methods to calculate frequencies, percentages, and trends. Qualitative data from open-ended questions were categorized and summarized to capture key themes and insights.

2024 REPORT METHODOLOGY

Limitations

While the survey provides valuable insights into GenAl security preparedness, it is important to acknowledge certain limitations:

- Sampling Bias: The survey sample may not be fully representative of all industries or regions.
- Self-Reported Data: Responses are based on self-reported data, which may be subject to biases or inaccuracies.
- Evolving Threat Landscape: The rapidly evolving nature of GenAl threats means that the findings represent a snapshot in time and may need periodic updates.

Want to learn more about how Lakera Guard can help you build safe and secure AI?

Stop worrying about security risks and start moving your exciting LLM applications into production. Sign up for a free-forever Community Plan or get in touch with us to learn more.

Book a Demo



2024 REPORT CONTRIBUTORS

Contributors

Aayush Gangwar Andre Sookram Belkacem Cherfa Connor Brennan Abdul lah Andrea Brambilla Ben Jian Corey Murphy Abe Gizaw Andrea Ricci Ben Kereopa-Yorke Cristina Pinneri Abhishek Andrea Rojas Rozo Ben Tyner Curtis Chin Adam Abramov Andreas Pung Beni Eugster Cyprian Kiplangat Adam Danko Andreas Sophiadis Benji Zorella Daen Rebel Adebogun Timothy Andrei Chirvasie Bernard Ong Dagmara Zawada Adir Mancebo Junior Andrej Alfirević Bishwas Sagar Dalila Aouabed Damian Klimczak Aditya Chandrakant Musale Andreja Torkar Blythe Nguyen Aditya Pathak Andrew Jones Bonnie Green Dan Goetsch Admir Skomorac Andrew Muirhead Boris Vavrik Dan Hunter Adrià Recort I Fernandez Andrey Holz Borys Palka Daniel Blanchfield Adrian Wheldon Daniel Calvo Cerezo Andrius Kavaliūnas **Brad Morian** Adriana Roman Andy De Backer **Brad Smith** Daniel Coyne Ahmad Luay Eleiwy Aneesh Dahiya Bram Jonkers Daniel Furnivall Ahtesamuddin Brandon Ritter Daniel Garifulin Angel Martínez-Tenor Aitor Astorga Saez de Vicuña Annie Tang Brenda Ong Daniel Henrique Nascimento Akash Kundu Antoine de Langlois Brendon Page **Daniel Tolley** Akshay Mondal Antoine Stocker Bruno Silva Daniela Natalia Sánchez Aksshar Ramesh Anton Anis Bahou Bryanna Davis Danilo Lessa Aleio Perez Gomez Anton Szorkin Byron Coetzee Dave Cadoff Aleksandra Dubovik Anubhav Singh Cameron Carpenter Dave Leonard Alex Rispo Constantinou Carlo Esposito Anupam Kumar and David Gauthier Alex Schapiro Anurag Saxena Carlo Esposito David Rodríguez Alex V Arda Sevinç David Sharp Alex Wang Areeb Ahmed Tariq Casey Schadewitz **David Taylor** Alexander Dean Arib Yousuf Chandler Smith Davide Fauri Alexander Hurren Ariel Kwiatkowski Chelsea Hsu Davide Torno Alexander Madden Arjun BM Cheychou Mouafo Junior Dean Cazes Alexander Singh Chi-Chun Tsai Arnab Maji Dean Jackman Alexis Stewart Chiara Vollmer Atakan Yenihayat Dean Kastelic Ali A. Athit Charupattanapornkit Chittaranjan Velambur Debaditya Ghosh Allen Holman Atlas Guo Deborah Erlanger AMAN KADAM Auricia Michelle Blount El Christian Ferranti Deepanshu Rekhi Avia Avraham Christopher Lu Amdjed Bensalah Deniece Tan Amir rad Avinash Nutalapati **Christopher Petito** Devansh Pal Amir Uval Avishek Dutta **Christopher Small** Dhanush Nair Chuck Durfee Amitesh Roneel Singh Aymeric Alixe Dhaval Rajendra Suthar Ana Kolkhidashvili Bailey Dalton Cihangir Günbay Dhruva Goyal Anastasiya Guenov Bakhta Elamar Claudia Morfin Dillon Buchanan Anatoli Kalysch Bart de Goede Cody Crumrine Divya Nair Anatoliy Zhestov Beenish Sami Colm Ó hAonghusa

Gaurav Agnihotri

DJ Lipman Geetika Tripathi James Duncan Jorge Isaac Chiu Valderrama Geoffrey Iwata **Dmitry Kolesov** James Koplin Jose Ignacio Rojo Rivero Jose Manuel Cardona Fab-Dobromila Wlodarska Georg Dresler James Tribe rega Jamie Dalton Harrell Dominic Scafidi George Spyropoulos Joseph Christensen Dominic Troman. Gerrit Meyer zu Driehausen Jan Hertsens Joseph Soultanis Dominik Fidziukiewicz Gianfranco Romani Jannik Wiedenhaupt Josh A Dominik Uršič Giselle Jhunihnuwala Jannik Wiedenhaupt Josh Dean Donny Schreiber Jar Kovar Joshua Loftes dovi newman Jason Ross Joshua Quick Dr. Barun Kumar Saha Godwin Vincent Jason Wright Joshua VanderLaan Dr. Kari J Lippert Gordian Zomer Jaspreet Sehmi Jude Ray **Edouard Raynaud** Greg Brooks Jasu A. Edward (Ted) Kwartler Javier García Arredondo Greg Kuhn Julie Rask Nørballe Edwin Martinez II Grégory Alary Javier Gómez Pereda Jun TEE Eishad Uzzaman Jayne Samuel-Walker Gregory Su Junyi Hou Ellie-Anne Watts Jean GEBAROWSKI Jussi Kujansuu **Emanuel Bahr** Guillaume Groell Jean Pierre Taute Kaish Khan Emilia Korona Haidar Jomaa Jean-Francois Noel Karan Kakwani Hannah Chambers Emirali Gungor Jef Theysmeyer Karin Haus Hannes Lange Jeff Brown Enjui Chang. Karla Congson Harleen Kaur Eran Jordan Jemma Gates Karol Wrotniak Erfan Hosseini Harrison Mamin Jenifer Tabita Ciuciu-Kiss Karthick Kannan Eric Coleman Harrison Pope Jennisa Chakratphahu Katarzyna Dymarek Erik Demitz-Helin Jens Kronvall Harshitha Machiraju Kate Kligman Erik Nordby Hasan Shehzeb Jeremy Wyler Ken Ke Heather Leffew Erik Stenberg Jerzy George Janiec Ken Smallwood Eris Dhionis Sako Jess Daswani Heidi Varpenius Kenneth Myers Ethan K. Gordon Hélain ZIMMERMANN João Caxaria Kevin Konrad João Miguel Garcia Teixeira **Evangelos Matragkos** Henry Wong Khalil Ghimaji Himanshu Reddy João Pedro de Bragança Evgeniy Kokuykin Khang Luong Dinh Evgeny Modin Hocky Yudhiono Joel Hokkanen Khoa Hoang Trinh Eythan Soysa Hsin-Wen Chang Joey Neilson Kieran Klukas Facundo Batista Huang Chih Hsiang Joey Neilson Klaus Adamhuber Felix Leber **Humberto Ponce** Johan S Daniel Koji Kanao fenixar@gmail.com Ian Cuthbert Johann Groß Konstantin Kostadinov Florian Licausi Ignacio Gavira John Keating Konstantinos Barmpas Francisco Lopez Garcia John Paul Jones Jr. Igor Malikovic Konstantinos Passadis Francois Capel Ildar Khuzhiakhmetov Johnson Arokiadoss Kostis Gourgoulias Frank Finelli Ioanna Zapalidi Krish Agarwal Fred Roth V Ismael Ricardo Packer Jonathan Grant Kriti Shewaramani G R Sharveshram Ivan Pashchenko Jonathan Mena Krzysztof Krzywinski Galvin Widjaja Jacob Field Jonathan Rodgers Krzysztof Marczyński Jacob Lehenbauer Jordan Jon Brace Garry Stanley

WWW.LAKERA.AI 39

Jorge Andres Padilla

James DeMong

Kyle Belcher

Kyle Williams

Lars Lemmermann Martin Sanders Miguel Berfelde Owen To amain Le Anh Trung Martino Governo Pablo Navarro Ming Liu Lea Grubisic Martyna Zigouras Miroslav Cermak Pablo Zaidenvoren Lee Mooney Martzen H. Miroslav Petrik Panagiotis Klironomos Lee Wee Liang Masakatsu Kubota Mohamed el Mahdi Debbagh Paras Rawat Leong Kwok Hing Mason Franceschi Mohammed Irfan Patrick Hood LEPORC Matthieu Mason Landry Muhammad Arham Khan Patrick Mullen Leslie Riach Muhammed akcil Patrick Schüle masoumeh Chapariniya Levan Shugliashvili Paul Jacobs Mathias Sahlander Muhammed Batuhan Berk Paul Larsen Lew Ayotte Mathieu de Borman Munnangi Sravya Liken Tan Matias liäs Mustafa Yusuf Sertkaya Paul Mendelson Lim Kelvin Matias Paglioni Myles Barney Paulo Marcon Lisanu Tebikew Yallew Matt Buck Name Amit Kumar Paulo Mota Lorena Bellano Matt Mastracci Nassim Hamer Pavandeep Singh Lorenzo Fratus Matthew Huff Natalia Sokołowska Pavel Zhelnov Louis-Philippe Morier Matthew Rastovac Natasha J. Stillman Pavel 7ubarev Lu Sanchez Matthew Rossi Nathan Collins Pawel Luty Luca Flora Matthew 7hou Nathan Rees Paweł Możejko Luca Sambucci Matthias Kraft Nathan Virot Paweł Pająk Lucas Finger Grachten Matthieu Billaux Neha Kumari Pedro Henrique Amaral Santos Lucas Palma Mattia Sanvito Neo Saxena Pedro Joaquin Luciano Chaparin Luisi Maurizio Oristanio Nibin Philip Pedro Lopes Ludwig Sickert Max Leijtens Nick Tsagkas Pedro Lucas Gomes Luis C. Pastor Nicolai Jacobsz Max Lieb Pehr Collins Lukas Rost Nicolas Gandar Max Martynov Per Olav Stryken Haug Luke Ballantine Nikitha Matta Maxence Godeneche Peter Carney Maxime HUBERT Luke Smytheman Nils Hellberg Peter Ciccolo Luke Teitell MD ABU SAYED Ninad Shringarpure < Peter Hendy Luliam Tekle Md. Ashrafuzzaman Bhuiyan Nir Gottlieb Péter László Maalika Brown Megan Hayes Nir Kligsberg Pieter de Bruin Maciei Wieczorek Mehran Sattar Nischith R Piotr Leniartek Madhavendra Thakur Melissa Carlton Norman Reimer Piotr Ż. Oliver Furrer Maharaj M, PMP Mert Dora Güleç Piyush Surana Micah Jank Oliver P. Mayor Mandy Gu Plamen Mitev Michael Backes-Bogerd Marcel Pieper Olzhas Yergali Pooia H P Marina Tetzlaff Michael Eller Omer Talmy Poojan Vachharajani Mario Martinez Michael Grev Omkar Ukirde Prajwal Srinivas Mario Matteis Michael Knell ONUR KARAN Pranshu Malhotra Mario Stylianou Michael Lai Prince Singh Mark Scott Michael Lester Orestis Ousoultzoglou Quentin Loisel Markus Hupfauer Michael Perry Oriane Krebs Raahul Singh Marta Mazelanik Michael Thomas Oscar Garcia Rachel Kent Martín Gotelli Ferenaz Michaela Klopstra Oscar Satre Rafael Cortes Martin Milbradt Michał Butkiewicz Osman Tataroglu

Rahim Khanani
Rahul Kumar
Ralph Aouad
Raman Thakur
Raphael Ballet
Raphaël SABRAN
Ravjoth Brar
Regina Griffin
Remco Jongschaap

Regina Griffin

Remco Jongschaap

Remya Praveen

Richard Gehklhaar

Richard Porteous

Riley Williams

Rob O'Connor

Robert Finn

Robert Marshall Robin Hugo Robyn Bertrand

Rodrigo Matías Alvarez Igarzabal

Rogene Lacanienta

Rohan Bajaj Roman Bakuridze

Ron Sneh

Roshan Rateria Roy Weisfeld

Ryan Brown
Ryan McConnell

n, an modernion

Ryan Peng Sagun Raj Lage

Samir Sharma
Sandra Elsom
Sani Djaya
Sanjay Sankaran

Santiago Zanella-Beguelin

Saranyan Meenadchisundaram

Sanjid Hasan

Sathvik Kuthuru
Satu Minea Korhonen
Satyam Nagpal
Sawyer Miller

Sean Murdoch Sébastien Portebo

Selin Erdinc

Sergio Bajo Navarro

Sergio Ruiz
Shafqat Hassan
Shane Martin
Sharbell Paul Rosell

Shaswat Deep

Shlomo Tannor

Shaunak Chattopadhyay

Shmulik Rosen
Shourya De
Shreyas Dongre
Siebren Meines
Sigmar Eskelsen

Simona Cancian
Simone Dowsett
Snorre Fagerland

Soraia Vanessa Lúcio da Silva

Sören Helms Sorin Beţişor

Souradip Mookerjee

Stan Beddinkhaus Stephen Littman

Sterling Grogg

Steve Grello

Sune Ørnemark Lægdsmand

Suvan Banerjee Swastik Mishra

Syed Muhammad Zain Ul

Abideen

Sylvestre Canard
Teddy Benson
Tensagram/EddieDean

Tenshi Ninsin

Thanassis THOMOPOULOS

Thiago de Assis Costa Thibault Ferrand

Thomas Barber
Thomas Wolfe
Tiago Almeida
Tiago Kiill

Timothy Aitchison
Tingting Zhao
Tobias Seibel
Tom Kersten

Tom Samson

Tomáš Halamiček Tomasz Świtoń Tomasz Wislicki Tony Pai

Travis DePuy Trishit Debsharma

Travis DePuv

Trucy Petter

Tyler almeida Uğur Özöz Umair Hussain Unmesh Bandekar

Uri Danan Valen Tagliabue

Vali Irimia

Vamsi Krishna Bonam Varun Sudarsanan Vedant Gosavi | Victor Rivas

Vignesh Venkatachalam

Vishal Gupta

Viswanath Srinivasan Chirra-

vuri

Vivek Vinod Sharma Vladimirs Rastopcins

Vyshnav Premlal Njattuketty.

Walter Sargent Wayne Billman

Will Chilcutt

Weerawat Pawanawiwat

William Byatt
Wilson Huynh
Wyatt Harvey
YAH XUAN LEONG
Yakov Keselman

Yang An Yi Yash Kiran Marathe

Yelena Hania

Yilmaz Baris Kaplan Yordanos T. Legesse Yotam Dekel-Tzelgov

You Liangliang
Youness Nait oufkir
Yuksel Kurtbas
Yuri Hechter

Zachary Zibrat
Zachory Powell
Zack Budai
Zeid Marouf
Zhen Xiong Lim
Zino Omoefe
Zoltán Ságodi
Zong-Ze WU

Zvonimir Petkovic