NAVIGATING GENAI THREATS AND OPPORTUNITIES IN CYBERSECURITY

Whitepaper

September 2024

GLOBAL CYBERSECURITY FORUM

Site

Foreword

Dr. Hesham Altaleb
Saudi Information
Technology Company (SITE);
Chairman of the Knowledge
Community: Future of Cybersecurity

As technology advances at an unprecedented pace, affecting nearly every aspect of our lives, cybersecurity is becoming an increasingly crucial priority. To address the evolving challenges and opportunities in this field, the 'Future of Cybersecurity' Knowledge Community is dedicated to exploring the dynamic landscape of Cyberspace.

This whitepaper sheds light on the rapid technological acceleration of generative artificial intelligence (GenAI), its many benefits, and its potential to transform cybersecurity by rethinking traditional practices, drawing insights from experts with deep technological understanding and cybersecurity experience who are part of the 'Future of Cybersecurity' Knowledge Community.

Contributors

- **Bilal Baig,** Trend Micro
- **Dr. Manar Alohaly,** Saudi Information Technology Company (SITE)
- **Dr. Yazeed Alabdulkarim,** Saudi Information Technology Company (SITE)
- **Radu Balanescu,** Boston Consulting Group (BCG)
- **Dr. Mohammed Alenezi,** National Company of Telecommunications and Information Security (NTIS)
- **Sulaiman Almohsen,** National Company of Telecommunications and Information Security (NTIS)
- **Naif Al Shaban,** Cisco

Knowledge Community: Future of Cybersecurity

The 'Future of Cybersecurity' is a Knowledge Community committed to exploring the potential opportunities and threats presented by the ever-evolving Cyberspace and developing mechanisms to maximize the benefits and address the risks looming on the horizon, by bringing together a diverse array of expertise from various stakeholder groups.

The community welcomes leading technology companies, global cybersecurity organizations, cybersecurity research centers, reputable think tanks, academic institutions, and other stakeholders with a vested interest in exploring and acting upon the future of cybersecurity.

Contents

1. Executive Summary

How prepared are organizations to face growing cyber threats in the digital realm?

GenAI is rapidly becoming a game-changer across industries, especially in cybersecurity, as the digital landscape continues to evolve. It is transforming traditional practices, opening up new opportunities in cybersecurity, and playing a critical role in shaping the future, particularly by enhancing threat intelligence and cyber defenses.

Recent findings reveal that of surveyed security executives, 93% of businesses have adopted public GenAI, with 91% of security teams integrating it into their operations.[1] At the same time, many anticipate challenges in dealing with GenAI-backed cyberattacks; about 45% of organizations fear that attackers will benefit more from this technology[2] and over half have not fully integrated it into their cybersecurity strategies,[3] indicating a gap in preparedness against AI-driven threats.

The duality of GenAI presents significant threats and opportunities. While it can enhance cyber defenses significantly, it can also empower malicious actors with sophisticated tools for crafting targeted attacks. Key threats, among many, include GenAI-enabled phishing attacks, malware generation, and deepfakes.

GenAI also introduces cybersecurity challenges within various business functions, requiring robust measures to secure AI systems. Organizations must adopt effective cybersecurity measures to harness the potential of GenAI while mitigating its risks. These measures should include enhancing data protection, addressing model vulnerabilities, ensuring secure GenAI integration, and creating advanced detection mechanisms. Setting policies for GenAI use within the workplace is also essential.

Furthermore, GenAI offers opportunities to strengthen cyber defenses, aiding in policy creation, generating synthetic training data, and producing fake data to mislead attackers. These applications improve detection and evasion in cybersecurity, enhance security measures, and contribute to the overall efficiency of cybersecurity controls.

GenAI's reshaping of Cyberspace offers both advantages and risks. By proactively implementing robust cybersecurity strategies, improving data protection, strengthening model training and inferencing processes, and fostering human-AI collaboration, organizations can secure their operations against sophisticated AI-driven attacks and capitalize on the transformative potential of a once-in-a-generation technological breakthrough.

93%

of surveyed organizations have adopted publically available GenAI models

91%

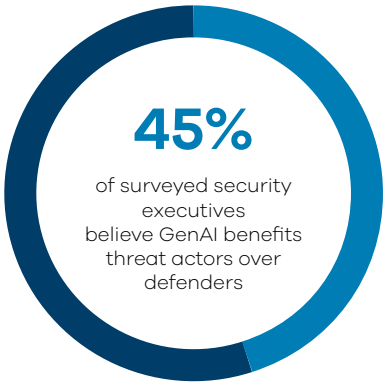
of security teams surveyed report adopting GenAI into their operations

2. Introduction

In just a few short years, GenAI's emergence has resulted in fundamental shifts across various domains, including cybersecurity. The advancement of this technology has already resulted in significant increases in productivity across multiple sectors, reshaping traditional ways of working with processes and means that are more intelligent.[4] However, the same technology that offers these benefits also presents significant risks, as malicious actors leverage GenAI to conduct more sophisticated and targeted attacks.[5] This double-edged nature of GenAI has sparked a race to harness its capabilities for both defensive and adversarial purposes[6] in cybersecurity, ushering in a new era of continuous competition between benevolent and malicious actors in Cyberspace.

Despite the widespread use of GenAI, organizations struggle to respond to GenAI-backed cyber-attacks, often compounded by complex and partly legacy cybersecurity infrastructure composed of various disintegrated solutions.

Moreover, the majority of organizations still lack clear GenAI policies and are unsure whether defenders or threat actors will benefit more from this technology, with 45% of security executives believing it benefits the latter more.[7]



One of the most pressing concerns is the threat of GenAI-enabled phishing attacks.

Formulating realistic, convincing and sophisticated phishing attacks is now easier than ever[8] because GenAI enables cybercriminals to avoid errors in spelling and generic messages to craft seemingly-credible and personalized phishing emails. Additionally, GenAI provides powerful tools for writing malware; even individuals with minimal programming experience can manipulate GenAI to generate malicious code, despite the built-in protections advertised. Impersonation is another significant threat. GenAI-based deepfake technology produces highly realistic text, voice, images, and videos that can bypass current cybersecurity measures and trick unsuspecting users into believing they are legitimate.[9]

In addition, GenAI, and AI in general, can pose risks to sensitive data. Companies implementing GenAI tools for various purposes, such as financial analysis or pricing strategies, can leave their organization vulnerable to cybersecurity risks, including data leakage. To prevent exploitation, companies need to govern the use of online GenAI services and secure internal AI systems.

It is crucial to address two key elements here: making GenAI systems more secure, and using it to strengthen organizational cybersecurity.

This whitepaper explores how to navigate GenAI cyber threats and opportunities, and provides a roadmap for its secure integration. It also presents case studies and success stories of GenAI use in cybersecurity.

3. Navigating GenAI Cyber Threats

Organizations implementing GenAI face a multitude of cybersecurity threats, from data exposure to model vulnerabilities and malicious manipulation.

Data Exposure

Data exposure refers to the unauthorized disclosure of confidential information. In the context of GenAI, the risk of data exposure increases as more data is fed into the model. This can happen in various ways, from copying and pasting confidential data into GenAI-powered tools to using proprietary data to fine-tune or augment a GenAI model without proper security measures.

Two main strategies are essential to prevent unwanted data exposure: Helping improve data protection measures, and ensuring secure GenAI integration. Implementing and enhancing data protection measures requires ensuring data privacy, securing data storage and transfer, and managing access controls effectively. Integrating GenAI technologies into existing IT ecosystems requires vetting third-party GenAI solutions for cybersecurity risks and ensuring their compatibility with existing cybersecurity controls.[10]

Along with these technical measures, companies should focus on the human aspect of preventing data exposure to GenAI. This means setting clear policies that outline proper data handling procedures when interacting with GenAI tools. Providing training and awareness to educate employees on best data security practices and the consequences of data leakage is essential to reinforce these policies.

Model Vulnerabilities

Model vulnerabilities are weaknesses or flaws within computational models, particularly those used in AI, which can be exploited by attackers to conduct successful attacks. These vulnerabilities can allow attackers to access confidential information or influence model results. They arise from poor data quality, algorithmic flaws, inadequate training processes, improper deployment practices, human errors, or lack of model interpretability. Inadequate training processes and lack of model interpretability, for example, can enable attackers to trick a GenAI model into bypassing filters and providing restricted content through carefully crafted prompts.

Multiple measures can be deployed to prevent model vulnerabilities. Ensuring data security and integrity is of paramount importance and can be achieved through secure collection, storage, and validation processes. Continuously updating training datasets with new adversarial examples will also help keep the model resilient in the face of evolving threats

Another critical measure is investing in AI training for engineers, developers, data scientists, and operational staff, to educate them on security best practices and specific threats resulting from the use of GenAI systems.

Malicious Manipulation

Organizations are facing rising threats, including credential stuffing, supply chain attacks, social engineering, and cryptojacking.[11] Among these threats, the malicious manipulation of GenAI has become a significant concern. Projections indicate that by 2028, enterprise spending on battling misinformation will exceed $500 billion, taking up 50% of marketing and cybersecurity budgets.[12]

GenAI has amplified social engineering risks by enabling the creation of sophisticated emails, realistic content, and automated attacks that are difficult to detect. Since 2019, high-profile AI attacks have increased in frequency and sophistication, making these threats more widespread and difficult to counter.

GenAI is now used in various stages of the cyberattack lifecycle, including reconnaissance and surveillance, vulnerability discovery and exploit development. This has led to a surge in complex and large-scale threats, posing significant risks, especially to organizations with inadequate defenses. Additionally, state-sponsored cyberattacks are another growing concern, as these attacks are difficult to attribute and can cause substantial damage.

Attackers primarily use GenAI to craft sophisticated phishing attacks that are increasingly difficult to distinguish from legitimate communications.

Organizations must proactively identify and defend against such attacks across all areas, including endpoints and networks.

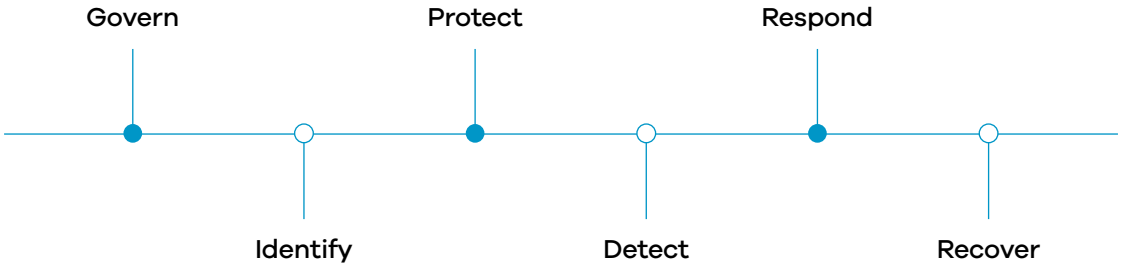
Besides phishing, GenAI can automate malware creation, simplifying the process for attackers to launch large-scale attacks from unknown and undiscovered vulnerabilities. This advanced technology also introduces the risk of bypassing traditional security measures of robotic identification, such as CAPTCHA and biometric authentication.

Another significant concern is using GenAI to create deepfakes – audio and video content nearly indistinguishable from the real ones. Deepfakes are often weaponized to spread disinformation, manipulate public opinion, and even impersonate individuals in real time, posing severe risks to personal and organizational security. A notable example is a recent incident where a financial analyst was deceived into transferring millions of dollars, believing they were communicating with the company's Chief Financial Officer. This incident highlights the critical role of GenAI in enabling such sophisticated attacks.[13]

Furthermore, GenAI is increasingly used to manipulate social media with fake profiles and automated interactions. These AI-driven activities can skew public discourse, manipulate social trends, and mislead individuals into trusting and sharing false information. GenAI also enables document forgery, such as fake invoices or reports, tricking victims into making payments or disclosing private information.

The convergence of GenAI and social engineering presents a formidable challenge for cybersecurity. As technology continues to evolve, so will techniques employed by malevolent actors. Organizations must stay ahead of these advancements by implementing robust cybersecurity measures and continuously updating their defense mechanisms to mitigate new risks posed by GenAI-driven attacks.

4. GenAI Possibilities in Cyber Defense



GenAI's use can be extended across the various domains of cybersecurity, offering opportunities to strengthen defenses within the core functions of the NIST Cybersecurity Framework 2.0 (CSF2.0), which is commonly used for managing cybersecurity risks.

By aligning applications with NIST's key functions – govern, identify, protect, detect, respond and recover – GenAI can play a vital role in enhancing cyber defense efforts and addressing the evolving threat landscape.

Govern

GenAI can support various aspects of policy creation and documentation within an organization, including developing and maintaining rules and policies related to data protection. This can help ensure that data protection governance and practices remain current and effective in the face of evolving threats. By analyzing large datasets and identifying patterns, GenAI can also provide valuable insights, making it easier to craft policies that are both comprehensive and relevant.

Identify

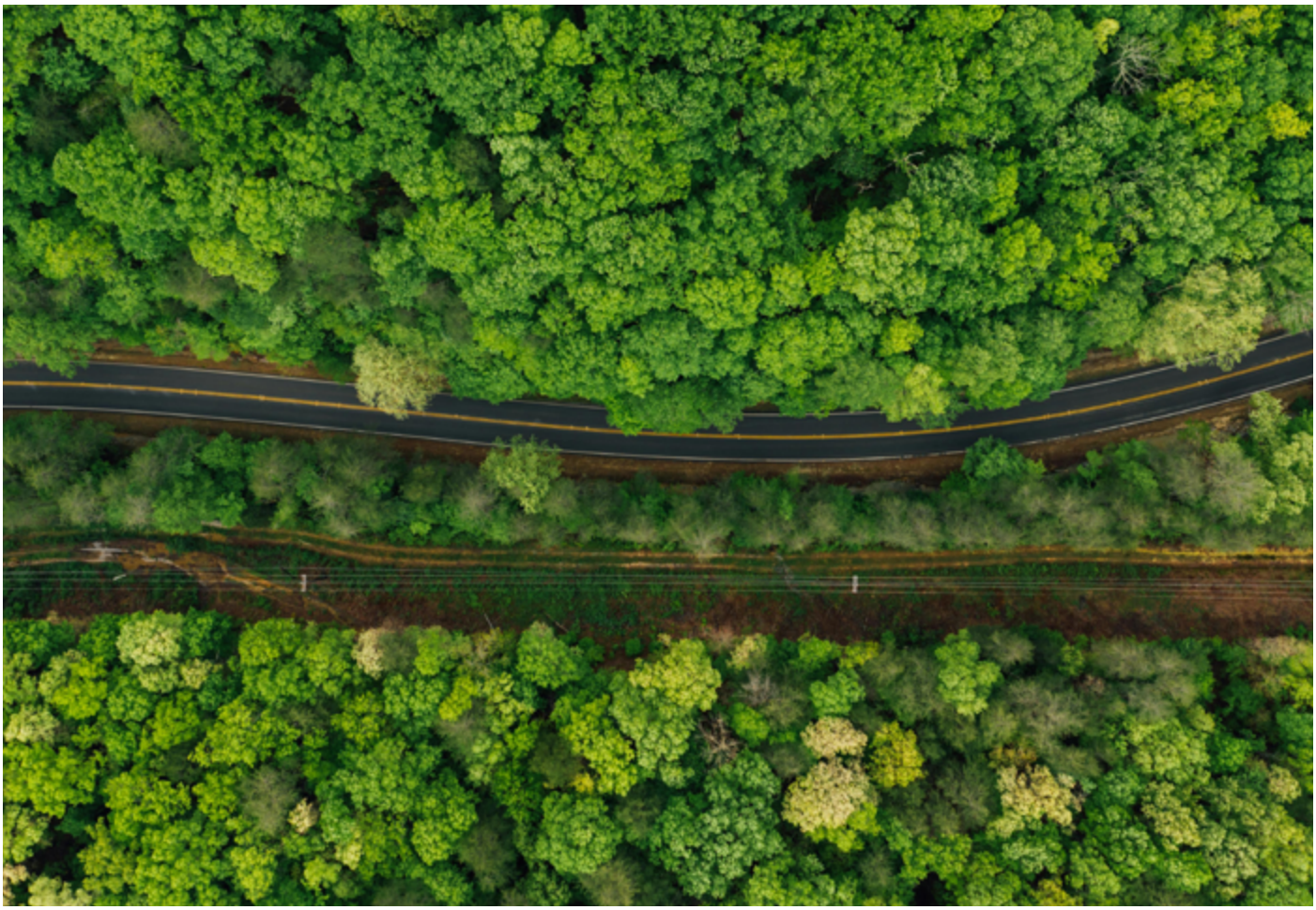
GenAI can play a significant role in understanding and managing cybersecurity risks, as well as identifying organizational assets, related vulnerabilities, and potential threats. It can rapidly process vast amounts of data from various sources to provide real-time insights about potential threats and vulnerabilities. This enables organizations to proactively address threats, often before they materialize. Additionally, GenAI can streamline risk assessments and third-party evaluations, helping to identify weaknesses and vulnerabilities within and outside an organization.

Protect

GenAI can enhance cybersecurity by providing automated, context-aware recommendations for defensive controls based on an organization's assets and risk tolerance. This allows organizations to streamline the authorization and identity management process with minimal human intervention and management overhead.

Detect

GenAI can help organizations detect cybersecurity incidents by identifying anomalies and suspicious activities. For instance, it can support the generation of diverse and realistic variants of malware and malware signatures, improving the performance of machine learning-based malware detection systems. Additionally, it can be employed to create realistic honeypots that deceive and detect malicious actors. These capabilities demonstrate how GenAI can strengthen an organization's ability to detect emerging cyber threats effectively.



Response
GenAI can help organizations in mitigating the impact of cybersecurity incidents once threats are detected. Key activities it can support include providing real-time decision-making assistance and offering actionable insights to guide response efforts. AI-driven platforms can also automate containment and remediation processes, ensuring incidents are handled swiftly and effectively. Additionally, GenAI can simulate incident scenarios, helping organizations test and refine response plans, ensuring they are prepared for various threats.

Recover
GenAI can help organizations recover more efficiently by simulating cyber-attacks and recovery scenarios to enhance response strategies and preparedness. This enables businesses to restore operations more efficiently after a cybersecurity incident. By automating recovery processes and analyzing past incidents through AI-driven models, organizations can minimize downtime and refine their business continuity plans to better cope with future disruptions.

The adoption of GenAI is also expected to impact the cybersecurity workforce significantly. It is anticipated that by 2028, the technology will help bridge the skills gap, potentially reducing specialized education requirements for 50% of entry-level cybersecurity roles.[14] Analysts will spend less time on routine tasks such as log analysis and reporting, and more on proactive threat hunting and developing strategic defensive measures. By liberating cybersecurity professionals from reactive firefighting, this shift will enable them to focus on strategic planning.[15]

5. Ensuring Secure and Responsible GenAI Integration

In an era of rapid technological progress, where GenAI is becoming increasingly integral to cybersecurity, a key question emerges: Where should organizations begin their GenAI journey?

We propose a three-step approach to integrating cybersecurity risk into a broader corporate Responsible AI framework while deploying initial GenAI use cases to enhance security and efficiency.

Step 1: Integrate Cybersecurity Risk into the Organization's Broader Responsible AI Framework

The first step focuses on augmenting existing processes, tools, and skillsets to effectively identify, manage, monitor, and respond to cybersecurity and privacy risks tied to GenAI. This requires a strategic integration of cybersecurity risk into a Responsible AI framework. Key actions in this step include:

- **Defining Policy Guardrails:** Establishing clear policies that guide the development and deployment of GenAI technologies, ensuring compliance and security from the ground up.
- **Adapting Risk Monitoring Strategy:** Modifying and enhancing risk monitoring strategies to better detect and mitigate potential GenAI threats.
- **Designing GenAI-centric Risk Assessments:** Creating risk assessment tools tailored specifically to GenAI's unique challenges and opportunities.
- **Creating "Take Action" Playbooks:** Developing comprehensive playbooks with step-by-step actions to take when responding to identified risks that have materialized, ensuring their swift and effective mitigation.

Step 2: Develop GenAI Use Cases That Are Secure and Include Privacy-by-Design

The second step emphasizes the importance of integrating security and privacy considerations early in the development of GenAI use cases. By identifying security and privacy requirements from the outset, organizations can ensure that security is not an afterthought but a foundational element. Key actions in this step include:

- **Embedding Security and Privacy Controls:** Incorporating robust security and privacy measures into the design and development phases of GenAI projects.
- **Addressing Current and Emerging Regulations:** Ensuring that all GenAI use cases comply with existing regulations and are adaptable to new regulatory requirements as they emerge.
- **Adding Security and Privacy Activities Throughout the Agile Software Development Lifecycle Execution:** Continuously integrating security and privacy activities within agile development processes to maintain a secure development environment.

Step 3: Unlock GenAI-Powered Benefits for Cybersecurity and Privacy Teams

The final step focuses on leveraging GenAI's advanced capabilities to enhance cybersecurity and privacy, accelerating the maturity of processes, decreasing cyber risk, and increasing human efficiency. Key actions here include:

- **Creating Automated Rules:** Develop automated rules and protocols that leverage GenAI to detect and respond to threats more efficiently.
- **Distilling and Simplifying Large Data Sets:** Use GenAI to process and analyze large volumes of data, extracting actionable insights to inform security strategies.
- **Implementing New GenAI-Based Processes and Playbooks:** Roll out new processes and playbooks that incorporate GenAI technologies to enhance overall cybersecurity measures.
- **Planning for New GenAI Threats:** Anticipate and prepare for potential threats posed by the evolving capabilities of GenAI, ensuring proactive defense mechanisms are in place.

By following this structured three-step approach, organizations can address current cybersecurity and privacy challenges while positioning themselves to leverage GenAI's potential. This ensures that organizations can innovate confidently, knowing that their security and privacy needs are comprehensively addressed.

A three-step approach to securely use GenAI

Step 1
Integrate Cybersecurity Risk into the Organization's Broader Responsible AI Framework

1. Defining Policy Guardrails
2. Adapting Risk Monitoring Strategy
3. Designing GenAI-centric Risk Assessments
4. Creating "Take Action" Playbooks

Step 2
Develop GenAI Use Cases that are Secure and Include Privacy-by-Design

1. Embedding Security and Privacy Controls
2. Addressing Current and Emerging Regulations
3. Adding Security and Privacy Activities Throughout the Agile Software Development Lifecycle Execution

Step 3
Unlock GenAI-powered Benefits for Cybersecurity and Privacy Teams

1. Creating Automated Rules
2. Distilling and Simplifying Large Data Sets
3. Implementing New GenAI-Based Processes and Playbooks
4. Planning for New GenAI Threats

6. Integrating GenAI in Cyber: Case Studies

Microsoft Security Copilot: A transformative tool that empowers security teams by leveraging the power of GenAI to enhance threat detection, streamline responses, and bolster overall cybersecurity defenses. It simplifies complex data and provides clear and actionable intelligence, enabling organizations to accelerate their threat response times from hours to mere minutes. Its advanced capabilities, including proactive threat hunting, and detailed incident analysis, allow security professionals to enhance their operations, ensuring a more resilient and fortified security posture.[16] Recently, a global insurance organization successfully utilized Security Copilot to reduce its detection and response times dramatically. Additionally, the company recognized the value of Copilot in helping them raise the maturity of SOC analysts due to its ability to respond to natural language queries.[17]

Google Gemini: Software that has transformed the technical and labor-intensive process of reverse engineering malware, addressing the ever-growing challenge of increasing malware volume and complexity. Gemini 1.5 Pro is capable of processing up to 1 million tokens to efficiently analyze entire malware files, including decompiled and disassembled code, in a single pass and often within 30-40 seconds. For instance, it processed the entire decompiled code of the WannaCry malware file in just 34 seconds, successfully identifying the kill switch.

This comprehensive processing ability eliminates the need to divide code into fragments, maintaining context and accuracy. Beyond reverse engineering, Gemini can also summarize threat reports into natural language, enabling enterprises to easily understand and analyze how these attacks might impact their operations.[18]

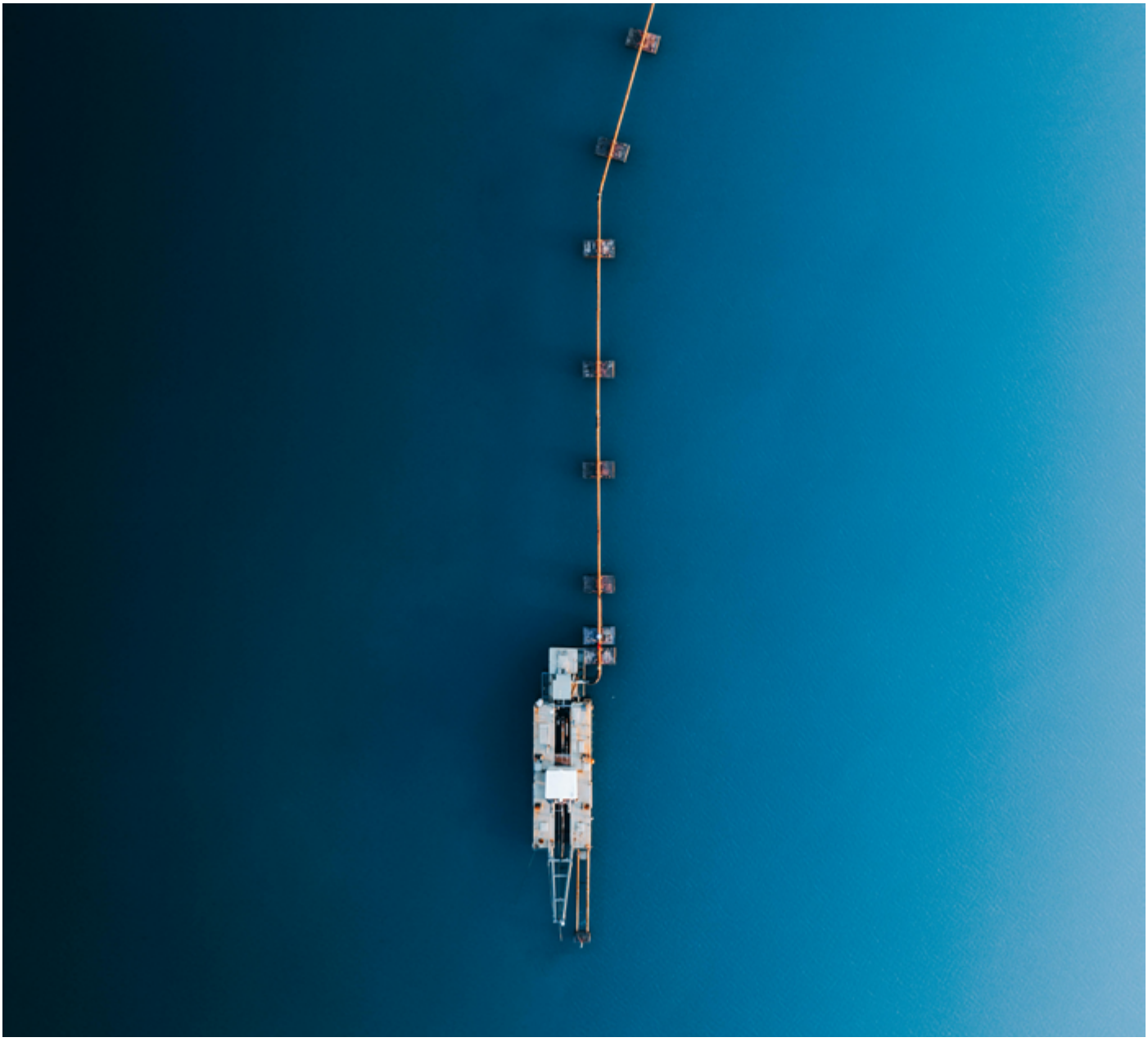
Gemini 1.5 Pro generates human-readable summary reports, making sophisticated malware behavior and indicators of compromise easily understandable for analysts. This breakthrough enhances the detection of new and sophisticated threats, strengthening cybersecurity defenses and optimizing response strategies.[19]

FortiAI: A cutting-edge tool that enhances the capabilities of cybersecurity teams by enabling rapid and informed decision-making, swift threat responses, and efficiency in handling complex tasks. It optimizes threat investigation and response, enabling customers to substantially reduce the time needed to identify and contain threats - from over 20 days to less than an hour. FortiAI's investigation and remediation guidance, combined with playbook templates, deliver critical information in natural language within seconds. This enables cybersecurity and operations teams to further reduce the average time to detect and respond to threats, improving their overall risk posture. FortiAI's advanced capabilities empower organizations to handle cyber threats more efficiently and effectively, ensuring robust protection against potential security breaches.[20]

7. Conclusion

GenAI is rapidly transforming the cybersecurity landscape, offering significant benefits but also introducing new risks. Malevolent actors are increasingly leveraging GenAI to conduct more sophisticated and targeted cyberattacks, making it challenging for organizations encumbered by complex, outdated cybersecurity infrastructure and a lack of clear policies to respond effectively. Additionally, there is a dramatic increase in the rise of AI-driven threats, such as advanced phishing and deepfake attacks, further highlighting the urgent need for robust cybersecurity measures and continuous industry engagement.

Securing AI systems is now crucial to prevent exploitation and mitigate risks like data exposure and model vulnerabilities. Organizations must implement more effective data protection measures, foster a culture of cybersecurity awareness, and stay informed and ahead of emerging threats. By taking these steps, they can harness the full potential of GenAI while mitigating its associated risks.



Endnotes

1. Splunk. (2024). State of Security 2024. https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2024.pdf
2. Splunk. (2024). State of Security 2024. https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2024.pdf
3. Cisco. (2024). 2024 Cisco Cybersecurity Readiness Index. https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf
4. M. Gupta, C. Akiri, K. Aryal, E. Parker and L. Praharaj. (2023). "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," in IEEE Access, vol. 11, pp.80218-80245 . https://ieeexplore.ieee.org/document/10198233
5. ISACA. (2023) "Generative AI and the Potential for Nefarious Use." https://www.isaca.org/resources/news-and-trends/industry-news/2023/generative-ai-and-the-potential-for-nefarious-use
6. Sangfor Technologies. (2023). "Generative AI in Cybersecurity: Offensive and Defensive Approaches." https://www.sangfor.com/blog/cybersecurity/what-is-generative-ai-cybersecurity
7. Splunk. (2024). The State of Security 2024. https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2024.pdf
8. innov-acts. (2023). "The impact of generative ai on cybersecurity: opportunity or challenge?" https://innov-acts.com/the-impact-of-generative-ai-on-cybersecurity-opportunity-or-challenge/
9. BBC Newsround. (2024). "Deepfake Technology: What Is It, How Does It Work, and What Can It Be Used For?" https://www.bbc.co.uk/newsround/69009887
10. IDC: The premier global market intelligence company. (2023). "IDC - CSO Summit - GenAI in Cybersecurity: A Treat or Threat?" https://www.idc.com/ap/event/cso-summit/genai-in-cybersecurity-a-treat-or-threat
11. Cisco. (2024). 2024 Cisco Cybersecurity Readiness Index. https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf
12. Gartner. (2024). "Gartner Unveils Top Eight Cybersecurity Predictions for 2024." https://www.gartner.com/en/newsroom/press-releases/2024-03-18-gartner-unveils-top-eight-cybersecurity-predictions-for-2024
13. Chen, H., & Magramo, K. (2024). Deepfake used to scam Hong Kong CFO out of $35 million, police say. CNN. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
14. Gartner. (2024). "Gartner Unveils Top Eight Cybersecurity Predictions for 2024." https://www.gartner.com/en/newsroom/press-releases/2024-03-18-gartner-unveils-top-eight-cybersecurity-predictions-for-2024
15. Secureframe. (2024). "How Can Generative AI Be Used in Cybersecurity? 10 Real-World Examples." https://secureframe.com/blog/generative-ai-cybersecurity
16. Microsoft Copilot for Security | Microsoft Security (2024). https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security
17. Microsoft Copilot for Security | Customer Stories. (2023)."WTW raises certainty in an uncertain world with AI-driven Microsoft Security solutions." https://customers.microsoft.com/en-us/story/1703669067334366976-wtw-insurance-microsoft-security-copilot
18. Google Cloud Blog. (2024). "Introducing Google Threat Intelligence: Actionable Threat Intelligence at Google Scale." https://cloud.google.com/blog/products/identity-security/introducing-google-threat-intelligence-actionable-threat-intelligence-at-google-scale-at-rsa/
19. Google Cloud Blog. (2024). "From Assistant to Analyst: The Power of Gemini 1.5 Pro for Malware Analysis." https://cloud.google.com/blog/topics/threat-intelligence/gemini-for-malware-analysis
20. Fortinet .(2023). "Meet Fortinet Advisor, a Generative AI Assistant That Accelerates Threat Investigation and Remediation." https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortinet-advisor-a-generative-ai-assistant-accelerating-threat-investigation-and-remediation


GLOBAL
CYBERSECURITY
FORUM
Site