International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I4P111

Volume 72 Issue 4, 87-94, April 2024
© 2024 Seventh Sense Research Group®

Original Article

Supercharged Attacks: Analyzing Generative AI Usage by Cyber Threat Actors

Varadharaj Varadhan Krishnan

Independent Researcher, Washington, USA.

Corresponding Author : varadharaj.krishnan@gmail.com

Received: 17 February 2024 Revised: 23 March 2024 Accepted: 10 April 2024 Published: 19 April 2024

Abstract *- This paper investigates cybercriminals using Generative Artificial Intelligence (AI) technology to improvise cyberattacks. Recent generative AI innovations like chatGPT and other pre-trained large language models have emerged as a double-edged sword in cybersecurity. The paper explores how malicious actors leverage large language models to improve their tactics, techniques, and procedures, ranging from refined phishing to advanced malware development and vulnerability research. By analyzing reports and data published by industry-leading cybersecurity organizations, this study reveals how generative AI is currently being used and how it can further supercharge cyberattacks. The paper also discusses in detail how generative AI technology makes it easier and lowers the barriers for cyber threat actors to become effective, along with strategies and approaches an organization can use to counter these supercharged attacks.*

Keywords *- Generative AI, Cybersecurity, Cyber Threat Actors, Cyber Defense Strategy, AI-Powered Cyber Attacks.*

1. Introduction

This paper analyzes different ways generative Artificial Intelligence (AI) is used by cybercriminals and how it empowers them to supercharge their traditional methods. The papers aim to capture different known use cases of generative artificial intelligence applications by cybercriminals, analyze the pattern, and further classify them for better comprehension. Existing research is limited in guiding organizations against these supercharged attacks [2][11][15][29], and this paper aims to aid organizations in understanding the actual and potential use cases and further devise a strategy against them. Machine learning-based generative AI models have been around for years. However, the launch of the chatGPT, a Pre-Trained Transformer model in 2022, and various other open-source initiatives made these machine-learning models available to the public, including the cyber threat actors, creating a new set of problems for cyber defenders. In this paper, we will discuss the emerging trends, tactics, and procedures around using generative AI for cyber-attacks.

Generative Artificial Intelligence, or GenAI, is a branch of artificial intelligence that involves using Machine Learning (ML) algorithms on vast amounts of data for training and then using the trained model to generate human-generated like text [1]. GenAI models can learn from patterns in text and use that learning to produce artificial text. These models can be trained on source code, logs, user activity records, etc., and this makes it a very good candidate for use in cyber security. These capabilities can be used by analysts who are defending against cyber threats as well as the cyber threat actors. Proprietary Generative AI models and open-source models are now readily available, and they are getting more powerful with each iteration. The easy accessibility, availability, and relatively low learning curve further lower the barrier for cyber threat actors to embrace these technologies. With relatively low resources and effort, cybercriminals can now use GenAI to develop sophisticated attacks. It also lowers the entry barrier for new cyber threat actors to conduct sophisticated attacks [3]. This paper aims to analyze all these aspects and provide a tangible countermeasure that organizations could leverage.

2. Methodology

Data for this study primarily comes from the public domain. This research investigates threat actors' Tactics, Techniques, and Procedures (TTPs) published by threat intelligence industry leaders like Microsoft, Crowdstrike, Palo Alto Networks, IBM, Check Point, Cisco, and more. Thematic analysis is performed on data related to security incidents, threat intelligence, and reports published by these industry leaders. These organizations are known for their extensive security services to their client companies and have privileged access to vast amounts of data regarding security incidents, vulnerabilities, and emerging threats. The reports selected for analysis are recognized for their reliability, depth of analysis, and relevance to the topic of study. This study meticulously reviews these reports to identify common trends, significant threats, and recommended security practices. Furthermore, an opinion of how these trends will evolve based on the current trends, combined with the cyber security domain knowledge and knowledge around rapidly evolving GenAI technology.

3. Understanding Generative AI

Generative Artificial Intelligence is a subdomain of the Artificial Intelligence domain; it is focused on developing ways like machine learning models to learn from a large corpus of data and then use that training to produce output that mimics human-generated digital content. When it comes to machine learning, has been around for decades, and there are different types of machine learning methods. Deep Learning is one of them, and it uses advanced multi-layered algorithms called neural networks that mimic the working of neurons in the human brain. Deep learning computer systems have evolved from very simplistic models to now more complex multi-layered models that can make decisions autonomously based on previously gained knowledge. A specific type of deep learning called Transformers uses efficient algorithms to analyze input data in parallel, speeding up the entire learning process. This has transformed the AI industry in recent years, giving birth to GPTs (Generative Pre-Trained Transformers).

Generative AI is now synonymous with the term GPT. The term 'Transformer' in GPT refers to the Transformer type of Neural Network. Transformer-based machine learning models have been in use for many years; the inflection point in transformer architecture came with the Self-Attention technique introduced in the paper "Attention is All You Need" by Vaswani et al. in 2017 [4]. This technique allowed the model to analyze dependencies between data elements in a sequence; it was able to identify long-range patterns, making it highly effective for learning from large data sets of type text, images, audio, and video. The transformer architecture was also known for its ability to scale and parallel execution. It eliminated the traditional bottleneck and paved the way for faster training on large amounts of data.

4. Generative AI and Cybersecurity

Forrester [6] categorizes the generative AI use case for Cybersecurity into three broad categories: Content Creation, Behavior Prediction, and Knowledge Articulation.

- Content Creation: Generate different forms of digital content, including text, images, audio, and videos.
- Behavior Prediction: Predict the next possible step given a sequence of data points.
- Knowledge Articulation: Summarization, explanation, and rewriting for better comprehension, articulation, and understanding.

These use cases can be applied differently for each security domain identified by NIST: Prevention, Identification, Detection, Protection, Response, and Recovery. At the same time, cyber threat actors can use these Generative AI to perform sophisticated attacks as well. A report published by Deepinstinct [5] revealed that 75% of cyber security professionals from organizations that participated in the survey witnessed an increase in cyber-attacks in the last 12 months, with 85% attributing this sudden rise to bad actors using generative AI to their advantage.

With more advancements and easy accessibility, Generative AI has become a lucrative technology for bad actors; for example, mentions of generative AI on the dark web proliferated in 2023 (Figure 2) [7]. Hackers posting about using chatGPT became a common scene.

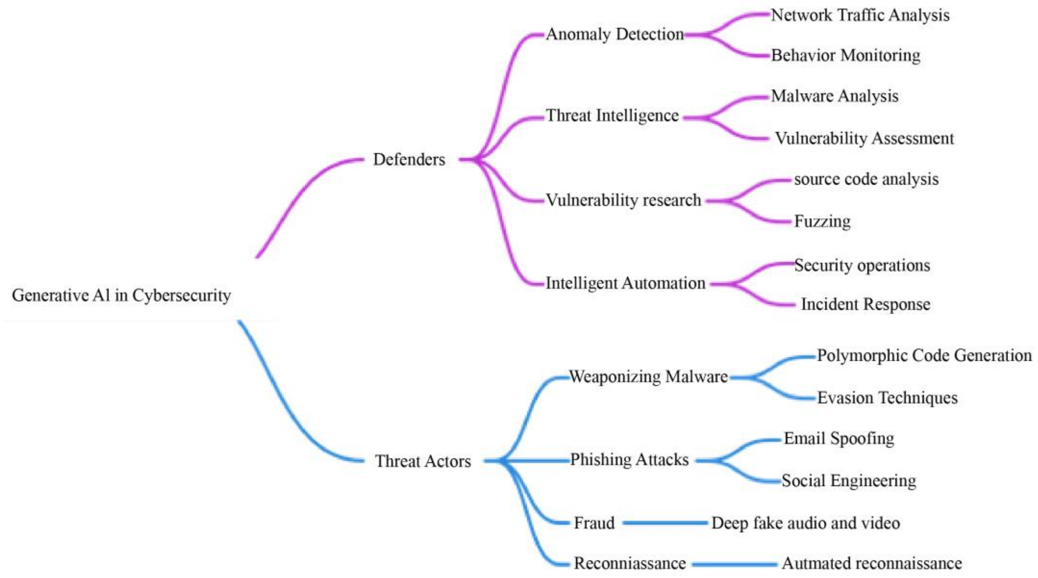
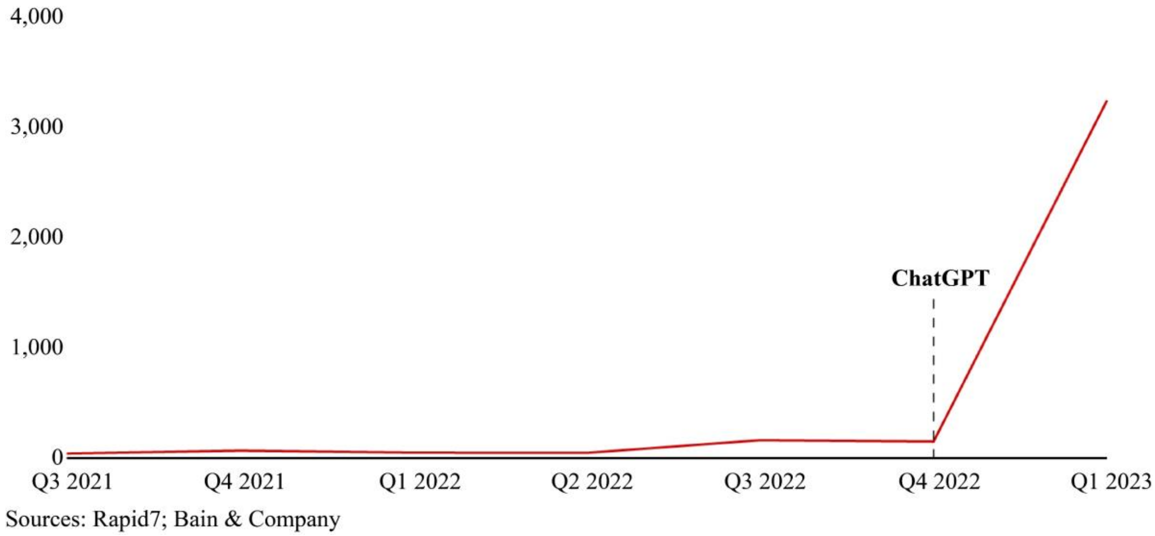


Fig. 1 Potential use of GenAI by defenders and threat actors



Sources: Rapid7; Bain & Company

Fig. 2 Number of dark web mentions of generative AI [7]

5. Generative AI-powered TTPs

5.1. Refined Social Engineering

In the cybersecurity domain, Social Engineering refers to the manipulation of individuals into performing certain actions or divulging sensitive information. With the Generative AI Large Language Model's ability to understand the requirements and context, as well as its excellent fluency in generating human-like text content, threat actors started leveraging it. One of the key applications was reconnaissance. Data collected from basic reconnaissance activity can be given as context to an LLM and asked to generate a convincing phishing email customized for the victim. Generative AI can make traditional phishing attacks more realistic, authentic, and less suspicious by eliminating grammatical and spelling errors, context-specific vocabulary usage, and persuasive and compelling writing styles. LLMs can insert current events related to the context and theme of the phishing topic to improve relevance and authenticity. Improved and automated reconnaissance helps bad actors switch to Spear Phishing easily instead of spray-and-pray. Spear phishing is a type of phishing in which a specific individual is targeted with more individual-specific content. LLMs can be applied in various ways to extract personalized information and recursively search the internet to collect more information and validate existing information. Information gathered from social media sites and previous data breaches are prime sources for crafting more personalized phishing messages. This presentation at Blackhat USA presentations [9][10][11] demonstrates how GenAI-generated spear phishing emails are very convincing and have high success rates.

Vishing: The term vishing is created from the terms ‘Voice’ and ‘Phishing’. It is a type of phishing where telephonic voice calls, voice messages, or voicemails are used to trick people. Like other types of phishing, vishing attacks typically carry all characteristics of traditional phishing, such as a sense of urgency. In a traditional vishing attempt, a bad actor calls or leaves a voice message pretending to be a trusted contact or an established authority in relation to the vishing context. A recent example is the MGM resort attack [12], which reportedly began with a voice call to the IT helpdesk impersonating an MGM resort IT employee. Generative AI can be used in two ways to perform a successful vishing; as previously discussed, it can be used for reconnaissance of data from the internet and, secondly, to create deep fake audio of the subject related to the vishing attempt.

5.2. Informed Reconnaissance

GenAI can be used to derive insights from open-source intelligence automatically [13]. Threat actors can now set up automated data collection pipelines from various social media platforms, online discussion forums, websites, and other digital spaces on the internet. They can also use LLMs to summarize vulnerabilities and how to exploit and act on them before the information is widely available and organizations act. LLMs, trained on a vast corpus of security threat intelligence reports and articles, can assist in identifying known vulnerabilities in software and systems used by the target. Threat actors can quickly probe for weaknesses in the systems by having LLMs use product documentation knowledge to answer queries.

LLMs can help represent a target network setup, systems, services, and devices based on the documentation supplied to it, and they could aid in finding vulnerabilities. This ability to visualize helps bad actors to plan an attack by identifying which systems to target and how to proceed. GenAI can be a powerful tool when it comes to cracking passwords and trying out password combinations for login. LLMs can be used to generate lists of passwords based on details gathered about a target or its organization. The effectiveness of the brute force attack can be further enhanced by recognizing different patterns and common behaviors among the target population.

5.3. Fake Digital Content for Fraud

Generative AI has lowered the barrier to entering cybercriminal activities [14]. It enables threat actors with limited computing resources and technical capabilities to produce high-quality content at scale. Large language models can be used to create digital content like articles, images, and videos corresponding to a specific narrative or produce content to impersonate authentic personalities. LLMs have also significantly reduced linguistic barriers faced by threat actors to target audiences in a foreign language. In a 2022 report by Mandiant [2], where they reported financially motivated actors using AI-generated video and audio in Business Email Compromise (BEC) scams, they showed documented evidence of North Korean cyber espionage actors actively using generative AI-created images to defeat Know-Your-Customer (KYC) requirements and fake voice recordings in social engineering targeting Israeli soldiers. Similarly, many media reports indicate the development of AI-powered tools like wormGPT, which allows malicious operators to create more persuasive BEC messages.

In March 2023, multiple media outlets reported a story about a Canadian couple scammed using the AI-generated voice of their son. Checkpoint [15] has observed financially motivated actors advertising generative AI capabilities, including deepfake technology as a service, on the dark web and in underground forums. This enables less capable threat actors to buy off-the-shelf services to perform sophisticated fraud.

5.4. Enhanced Malware

Malware is malicious software installed on a computer without the user's consent, and it performs various types of actions depending on the class of malware. It can range from information stealing to disrupting the system operations, controlling the system remotely, blocking access, and demanding a ransom to grant access back. Developing code for these malicious software requires skill, time, and often deep knowledge about the technology to understand the quirks and gaps. Large language model chat agents can now perform research quickly and get code created as per plain instructions in natural language [16]. LLMs are being used to perform automated code analyses to find vulnerabilities in open-source software as well.

Generative AI models built by training on a large amount of data, including sources from the internet, have inherent knowledge about existing malware. A study revealed how chatGPT [17] was used to get code for popular malware like Wannacry, Ryuk, and REvil and source code for Trojans, too. Reports from media show services that allow threat actors to bypass restrictions in popular LLMs and use them for malware development. Mandiant also has reported documented evidence of threat actors in the dark web and underground forums advertising LLM services and LLM-generated code between January and March 2023.

5.5. Enhanced Scripting Techniques

LLMs can be used to generate code snippets that can be added to compromised web and mobile applications. Hijack user interaction with remote backend servers, scrape the content from the web user interface, executing malicious tasks when users sign into a system. Unlike malware, these are bespoke script snippets built for specific steps of an attack chain. LLMs can be used to produce obfuscated and powerful scripts that can be leveraged in any stage of the attack chain to either automate or exploit vulnerabilities in the system. Next-generation LLMs built for code development can create SQL queries with basic database schema information. LLMs can be tuned to generate SQL injection queries to perform automated SQL injection attacks. LLM can be used to create attack payloads, pieces of malicious code that execute unauthorized actions like stealing secrets, deleting files, harvesting data, or launching further attacks. The research paper "From ChatGPT to ThreatGPT" [29] shows a demonstrated example of how chatGPT can be used to perform SQL injections.

5.6. Vulnerability Research Assistance

Next-generation LLMs like llama2 from meta [1] are trained explicitly for generating code. These models understand programming languages and code patterns. The models can be tuned to perform code reviews to look for potential vulnerabilities humans might miss. Common vulnerabilities like buffer overflows, SQL injections, and cross-site scripting (XSS) can be found by analyzing the code structure and logic. By feeding the model with descriptions of known vulnerabilities, LLMs can learn to be tuned or prompted to identify similar patterns in the code, potentially uncovering unknown vulnerabilities (zero-days).

The model is suitable for generating code comments and documentation to better understand the code flow and what it does. Threat actors can use this capability to understand the code better and look for areas of weakness with less time investment. LLMs can also analyze vast amounts of text data, including dark web forums, technical reports, and new articles, and generate insights into emerging threats and vulnerability trends, understanding attacker tactics, techniques, and procedures (TTPs).

5.7. Enhanced Detection Evasion

Understanding how security systems detect behavior allows attackers to utilize LLMs to create malware or attack plans that mimic genuine user actions, thus decreasing the chances of being detected. LLMs enable the development of exploit code that can evade security measures by adjusting the code until it avoids detection methods. This creates a new avenue for threat actors to rewrite and tweak well-known malware with enough obfuscation to evade defense mechanisms. Code obfuscation is another area where GenAI can bring varying levels of entropy [18]. Threat actors now have the luxury of creating new obfuscation for each attack with the help of the LLM model to rewrite the code, essentially making any code or process execution pattern-based detection useless. Any code pattern-based detections can be bypassed with the ability to heavily obfuscate code on demand. Also, by understanding how security tools detect unusual behavior, attackers can use LLMs to build strategies that would mimic normal user activity and escape detection.

6. Nation-State Threat Actors Using GenAI

Forest Blizzard (STRONTIUM)[3]: This Russian military intelligence entity, associated with GRU Unit 26165 and known as APT28 or Fancy Bear, targets various sectors, including defense and energy. Its use of large language models (LLMs) focuses on acquiring detailed knowledge of satellite communication and radar imaging technologies and enhancing its cyber operations with scripting techniques. These activities align with Russia's military and foreign policy objectives, especially regarding the conflict in Ukraine.

Emerald Sleet (THALLIUM) [3]: A North Korean threat actor, active throughout 2023, primarily using spear-phishing to target individuals with expertise in North Korea. By impersonating academic institutions and NGOs, they gather intelligence on foreign policies. Their LLM usage includes researching vulnerabilities, enhancing scripting for operational tasks, and generating content for social engineering, indicating a sophisticated approach to cyber espionage.

Crimson Sandstorm (CURIUM) [3]: Linked to Iran's Islamic Revolutionary Guard Corps, this group targets diverse sectors through social engineering and malware. Their LLM interactions suggest a focus on supporting .NET development, social engineering, and developing techniques to evade detection. This reflects their broader behavior patterns of utilizing custom malware and engaging in complex cyber operations.

Charcoal Typhoon (CHROMIUM) [3] is a Chinese state-affiliated actor with a global operational focus, known for targeting sectors such as government and higher education. Their engagement with LLMs is an exploration of augmenting their technical operations, including tooling development, understanding cybersecurity tools, and social engineering. This suggests a limited yet strategic incorporation of LLMs into their cyber operations.

Salmon Typhoon (SODIUM)[3] is another Chinese state-affiliated group with a history of targeting US defense and cryptographic sectors. Their interaction with LLMs in 2023 seems exploratory, focusing on information sourcing and operational command techniques. The engagement reflects an interest in leveraging LLMs for intelligence gathering on geopolitical matters, Cybersecurity, and technical challenges.

7. Defend Against AI-Powered Attacks

Basic cybersecurity hygiene forms the foundation of a strong defense for an organization. As discussed in the above sections of the paper, generative AI can give threat actors speed and finesse [19][20][21]. It lowers the barrier for cyber threat actors to scale and perform sophisticated attacks [3]. There is no silver bullet to protect against these supercharged attacks; instead, go back to basics and make sure organizations have strong foundational security hygiene like proper patch management, vulnerability management, multi-factor authentications, network segmentation, endpoint security solutions, and intrusion detection systems. In this section, we will not delve into the basics again but delve into additional capabilities and strategies organizations can take to mitigate or protect against these supercharged threat actors of the future.

7.1. Zero Trust Network Access

Zero Trust Network Access (ZTNA) methodology significantly differs from traditional solutions. ZTNA applies a "Never trust, always verify" approach to how organizations should protect their IT environments. ZTNA follows the principle of least privilege, ensuring that users and devices only have access to resources for their specific roles. By restricting access rights, ZTNA minimizes the surface area for attacks. It makes it harder for attackers to navigate across the network. Network segmentation is an aspect of ZTNA, as it divides the network into secure zones. This approach limits the impact of breaches by making it difficult for attackers to leverage an entry point to gain control over other parts of the network. Network segmentation is particularly effective against AI-driven attacks aimed at automating the identification and exploiting of network weaknesses. ZTNA solutions enforce identity verification for each user and device trying to access network resources. This may involve using layers of security such as multi-factor authentication (MFA) and behavioral analysis, which can pose challenges for AI-driven attacks attempting to circumvent them. Verifying and allowing access to ZTNA can prevent entry attempts even when sophisticated AI tools try to imitate legitimate user actions.

7.2. AI-Powered Automation in Security Operations

Generative AI-powered tools can reduce the workload of Security Operations Center (SOC) analysts by automatically analyzing cybersecurity incidents. Basic analysis can be offloaded to the intelligent agent, and SOC analysts could interact with the agent to perform additional analysis. Generative AI-powered intelligent agents can relieve SOC teams considerably by eliminating repeated tasks and basic analysis. It can be used to educate and train entry-level security analysts and flatten the learning curve. A Gen AI-powered security operations workbench can be built by aggregating traditional data sources like existing playbooks, asset lists or configuration management databases, known security findings and vulnerabilities, threat intel from external and internal sources, a malware knowledge base from sources like Virus Total and data from endpoint security agent could be aggregated in one place and an intelligent agent can be trained or supplied with this data to build an intelligent assistant for security operations team. Figure 4 provides an illustration of such a system. It can be further extended to automated, repeatable investigation tasks as well as execute incident response containment actions.

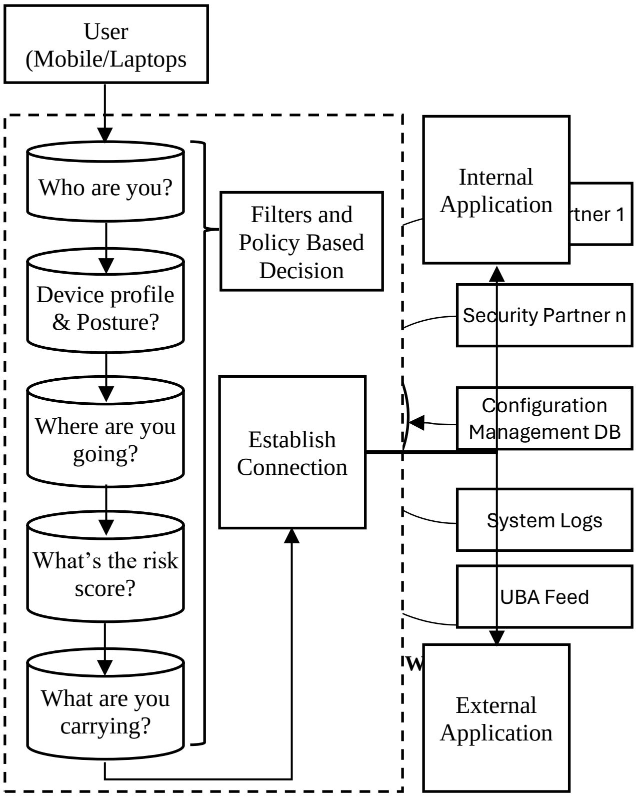


Fig. 3 Logical View - Zero Trust Network Access

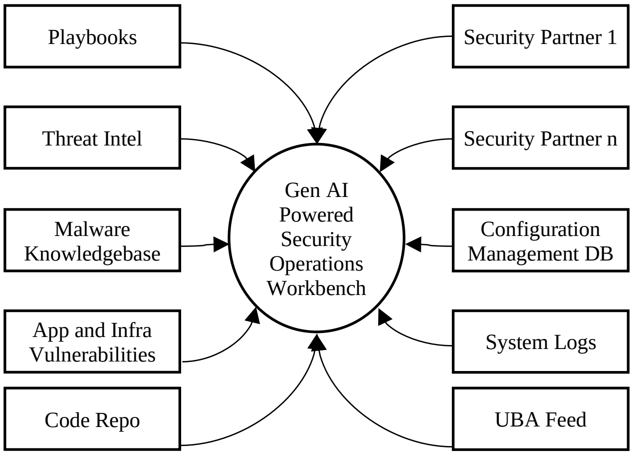


Fig. 4 Security operations workbench

7.3. User Behavior Analysis (UBA)

UBA is vital for safeguarding against cyber threats powered by GenAI [23][24]. Using machine learning and analytics, UBA monitors, detects, and responds to activities deviating from typical user behavior patterns. With the increasing sophistication of GenAI in cyber-attacks, conventional security measures may need to be revised. UBA provides a layer of security by focusing on user interactions with critical systems and data. UBA systems examine the behaviors of individual users or groups to identify deviations from these patterns. UBA can observe endpoint activities for signs of a GenAI-powered malware attack, such as file access patterns, data transfers, or alterations in system settings [27][28]. UBA aids in recognizing subtle data exfiltration or lateral movements commonly associated with APTs, providing an opportunity to thwart these threats early on.

7.4. AI-Powered Threat Intelligence

Threat Intelligence involves collecting, analyzing, and sharing information about potential or emerging security threats to help organizations improve their security posture and protect against cyber-attacks. LLMs can be used to build systems that source and analyze open-source intel. LLMs are good at processing vast amounts of data to identify potential security threats and generate actionable intelligence. LLMs can automatically generate threat intelligence reports based on various data sources, including social media, news articles, dark web forums, and other online sources. Like cyber threat actors, defenders can also use these capabilities to respond quickly to new threat intelligence.

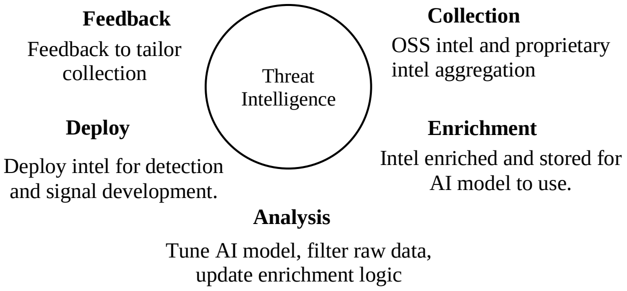

Feedback
Feedback to tailor collection
Threat Intelligence
Collection
OSS intel and proprietary intel aggregation
Deploy
Deploy intel for detection and signal development.
Enrichment
Intel enriched and stored for AI model to use.
Analysis
Tune AI model, filter raw data, update enrichment logic

Fig. 5 AI-Powered threat intelligence

7.5. Code Analysis and Vulnerability Research

Proactively, GenAI can be used for code analysis and vulnerability research. There is a definite path to automating the code review process by scanning source code for patterns associated with known vulnerabilities and poor coding practices. Google's oss-fuzz is a great open-source tool that can be used for this type of research. Extending that, AI models can be used to identify common vulnerabilities such as SQL injection, cross-site scripting (XSS), buffer overflows, and insecure authentication mechanisms [25][26] as well.

These AI-powered code reviews reduce the time and resources required for manual code reviews, making resources available for more complex tasks. GenAI can enhance Static Application Security Testing (SAST) tools by improving their ability to understand and analyze the context within the code, reducing false positives. GenAI-powered oss-fuzz open-source projects have uncovered thousands of vulnerabilities in open-source projects. Projects like oss-fuzz can help uncover vulnerabilities that cannot be found using traditional tools.

8. Conclusion

This research paper showed the current use and potential use of GenAI by cyber threat actors, shedding light on an emerging trend in Cybersecurity. By examining the tactics used by cyber threat actors employing GenAI, we have outlined how attacks are becoming more accessible and refined. GenAI technologies, while driving innovation in many sectors, are also being misused by cybercriminals. The capabilities of GenAI to create content, automate reconnaissance tasks, and strengthen malware and social engineering attacks make it an accelerator capability for threat actors. Organizations must integrate new technologies and approaches to counter this emerging wave of GenAI-powered tactics. Some effective Strategies include implementing Zero Trust Network Access (ZTNA), utilizing AI-driven automation for security operations, and enhancing User Behavior Analysis (UBA).

Additionally, utilizing AI-driven threat intelligence and proactive vulnerability exploration via GenAI are essential proactive measures organizations should take. These methods embody a comprehensive defense approach that can effectively reduce the dangers presented by cyber threats enhanced by GenAI. The dual role of GenAI as both a threat and a protective measure highlights the need for strategies and collaborative efforts within the cybersecurity community. By leveraging the capabilities of GenAI within a security-focused framework, we can not only counteract cyber threat actors' tactics but also pave the way for a more secure digital future.

References

[1] Lucia Stanham, Generative AI (Genai) in Cybersecurity, CrowdStrike, 2023. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/secops/generative-ai/

[2] Michelle Cantos, Sam Riddell, and Alice Revelli, The Use of Generative AI by Threat Actors: A Limited but Growing Concern, Mandiant, 2023. [Online]. Available: https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited

[3] Staying Ahead of Threat Actors in the Age of AI, Microsoft, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

[4] Ashish Vaswani et al., "Attention is All You Need," *Arxiv*, pp. 1-15, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[5] State of the Underground 2024, Cybersixgill, pp. 1-52, 2024. [Online]. Available: https://cybersixgill.com/resources/state-of-the-underground-2024

[6] Generative AI, Forrester. [Online]. Available: https://www.forrester.com/blogs/category/generative-ai/

[7] Syed Ali, and Frank Ford, Generative AI and Cybersecurity: Strengthening Both Defenses and Threats, Bain & Company, 2023. [Online]. Available: https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses-and-threats-tech-report-2023/

[8] Generative AI and Cybersecurity: Bright Future or Business Battleground?, Voice of Secops, 4th Edition, Deep Instinct, 2023. [Online]. Available: https://www.deepinstinct.com/pdf/voice-of-secops-4th-edition

[9] Phil Tully, and Lee Foster, "Repurposing Neural Networks to Generate Synthetic Media For Information Operations," *Black Hat USA*, pp. 1-41, 2020. [Google Scholar] [Publisher Link]

[10] John Seymour, and Philip Tully, "Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter," *Black Hat USA*, pp. 1-8, 2016. [Google Scholar] [Publisher Link]

[11] Eugene Lim et al., "Turing in a Box: Applying Artificial Intelligence as a Service to Targeted Phishing and Defending against AI-Generated Attacks," *Black Hat USA*, pp. 1-11, 2021. [Google Scholar] [Publisher Link]

[12] Arielle Waldman, MGM Faces $100M Loss from Ransomware Attack, TechTarget, 2023. [Online]. Available: https://www.techtarget.com/searchsecurity/news/366554695/MGM-faces-100M-loss-from-ransomware-attack

[13] Jannik Lindner, The Most Surprising AI Use In Cyber Security Statistics And Trends in 2024, Gitnux. [Online]. Available: https://gitnux.org/ai-use-in-cyber-security-statistics/

[14] Sangfor, How AI-Powered Solutions Revolutionize Cybersecurity, Sangfor, 2023. [Online]. Available: https://www.sangfor.com/blog/cybersecurity/how-ai-powered-solutions-revolutionize-cybersecurity

[15] Opwnai: Cybercriminals Starting to Use Chatgpt, Check Point Research, 2023. [Online]. Available: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/

[16] Thomas Brewster, Armed with ChatGPT, Cybercriminals Build Malware and Plot Fake Girl Bots, Forbes, 2023. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2023/01/06/chatgpt-cybercriminal-malware-female-chatbots/?sh=7790a9385534

[17] Carly Page, Is ChatGPT a Cybersecurity Threat?, Techcrunch, 2023. [Online]. Available: https://techcrunch.com/2023/01/11/chatgpt-cybersecurity-threat/

[18] Kyle Wiggers, Code-Generating AI can Introduce Security Vulnerabilities, Study Finds, TechCrunch, 2022. [Online]. Available: https://techcrunch.com/2022/12/28/code-generating-ai-can-introduce-security-vulnerabilities-study-finds/

[19] Ax Sharma, OpenAI's New ChatGPT Bot: 10 Dangerous Things it's Capable of, Bleeping Computer, 2022. [Online]. Available: https://www.bleepingcomputer.com/news/technology/openais-new-chatgpt-bot-10-dangerous-things-its-capable-of/

[20] Chris Wysopal, The Cyber Arms Race in the Age of Generative AI, CSO Online, 2023. [Online]. Available: https://www.csoonline.com/article/1259996/the-cyber-arms-race-in-the-age-of-generative-ai.html

[21] Shengdong Zhang et al., “A Novel Ultrathin Elevated Channel Low-Temperature Poly-Si TFT,” *IEEE Electron Device Letters*, vol. 20, no. 11, pp. 569-571, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[22] Kelli Vanderlee, China’s Capabilities for State-Sponsored, Mandiant, pp. 1-15, 2022. [Online]. Available: https://www.uscc.gov/sites/default/files/2022-02/Kelli_Vanderlee_Testimony.pdf

[23] Mark Sweney, “Darktrace Warns of Rise in AI-enhanced Scams Since ChatGPT Release,” *The Guardian*, 2023. [Google Scholar] [Publisher Link]

[24] Adam Greenberg, 14 Cyber Security Predictions for 2022 and Beyond, Mandiant. [Online]. Available: https://www.mandiant.com/resources/blog/security-predictions-2022-report

[25] Andrew Blake, Crimeware Tool WormGPT: AI for BEC Attacks, SC Magazine, 2023. [Online]. Available: https://www.scmagazine.com/news/crimeware-tool-wormgpt-ai-bec

[26] Britney Nguyen, A Couple in Canada were Reportedly Scammed Out of $21,000 After Getting a Call from an AI-Generated Voice Pretending to be their Son, Yahoo Entertainment, 2023. [Online]. Available: https://www.yahoo.com/entertainment/couple-canada-were-reportedly-scammed-194027194.html?guccounter=2

[27] Elias Groll, ChatGPT Shows Promise of Using AI to Write Malware, Cyber Scoop, 2022. [Online]. Available: https://cyberscoop.com/chatgpt-ai-malware/

[28] ChatGPT Created Malware BYPASSES EDR and claims Bug Bounty, Presented by CodeBlue29, Youtube, 2023. [Online]. Available: https://www.youtube.com/watch?v=qMd-m8GMweg

[29] Maanak Gupta, “From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy,” *IEEE Access*, vol. 11, pp. 80218-80245, 2023. [CrossRef] [Google Scholar] [Publisher Link]