VOTIRO

Navigating AI in Cybersecurity: Balancing Innovation and Risk

Global organizations are rapidly adopting artificial intelligence (AI) and machine learning (ML) to help enhance their business and operations. However, with as many organizations embracing AI, there are still many more holding back due to concerns about creating exposure for their organization.

With existing shortages in cybersecurity skills, it's sensible to be cautious about new sources of risk; however, avoiding AI to entirely mitigate this risk is not practical.

- Over 80% of enterprises are working with or planning to adopt generative AI... — watsonx.ai - IBM
- "GenAI has increased the degree of AI adoption throughout the business and made topics like AI upskilling and AI governance much more important." — Sr Director Analyst at Gartner

It's not that organizations are scared of AI as a whole, but rather the potential it poses when misused. With AI's rapid evolution and adoption, news headlines showing its benefits and risks have become commonplace, but the abusive use of AI is the most striking. Looming threats of automated attack platforms, AI-enhanced malware, and the rapid discovery of vulnerabilities has created tangible fears that the cyber-threat landscape will only worsen with time. With AI's ability to function at a large scale and high velocity, cyber attacks may become more extensive and inflict more damage in a much shorter time frame, making AI threats particularly daunting.

Let's explore legitimate challenges that organizations face from AI and look into some solutions to help teams prepare.

AI Threats Haunt Businesses

Automated Attacks

A primary fear is that AI will automate sophisticated cyber attacks. AI's capability to execute large-scale operations like phishing campaigns or network intrusions autonomously adds complexity. These AI-powered attacks can employ diverse tactics simultaneously, making it hard for traditional defenses to keep up. This problem worsens with AI's ability to learn and adapt based on the defensive measures they encounter, constantly evolving their strategies to bypass security protocols.

This is compounded by the unsupervised nature of AI. Once deployed, AI-driven attacks can function independently, requiring minimal oversight from attackers. This autonomy increases the efficiency of attacks, allowing criminals to disassociate from the direct execution, making it more challenging to trace and counteract.

AI-Enhanced Malware Permutations

Some AI platforms help enhance coding and streamline processes for developers. Yet, there's fear that these tools can be subverted, allowing AI to enhance malware or speed up the development of novel strains. Rather than spending costly developer time to create malware permutations, AI can rapidly change code and behavior to evade traditional signature-based detection methods. Such adaptability renders many conventional AV solutions less effective and is leading organizations to seek more proactive solutions.

In addition, AI-enhanced malware can exhibit self-repair and resilience features. If such malware is partially disabled or damaged by security measures, it has the potential to self-repair, restoring its functionality and prolonging its presence in infected systems. This resilience makes it more challenging to eradicate the malware, allowing it to persist over extended periods and cause more significant damage.

Targeted Attacks

AI in targeted attacks also poses a significant threat as it allows for analyzing vast amounts of data to pinpoint vulnerabilities in specific systems or networks. This leads to more precise and effective malware attacks. AI enhances the personalization of phishing attacks, tailoring them to individual targets and significantly increasing their likelihood of success.

By analyzing user behavior, AI can determine the most opportune moments and attack methods. AI can also enable malicious activities to mimic normal network behavior, bypassing anomaly-based detection systems, making AI-driven attacks particularly hard to detect and counteract, further complicating the landscape.

Developing Solutions

While the threats from AI make cybersecurity harder, there is no reason to assume that it is impossible to prevent threats. They are not fundamentally different from existing threats like Advanced Persistent Threats (APTs) and organized cybercrime. The innovation and creativity of seasoned cybercriminals have long been a concern, and while AI brings derivative capabilities, it still falls short of human ingenuity. The focus should remain on building robust and effective security systems and embracing the power of AI to improve operations.

Best Practices

Adhering to best practices is a critical first step in mitigating AI-related threats. AI threats take advantage of existing vulnerabilities, so taking the following steps will help form the foundation to make AI attacks less likely to succeed:

Implement Regular Security Audits

Conduct frequent assessments to identify vulnerabilities and enhance security measures.

Continual Staff Training

Educate staff about the latest cybersecurity trends and threats, especially phishing, to make them harder targets.

Backup and Recovery Procedures

Establish robust data backup and recovery protocols to minimize breach damage.

Use of Multi-Factor Authentication (MFA)

Enhance security by requiring additional forms of verification before access is allowed.

Stay Updated with Threat Intelligence

Keep abreast of the latest threat intelligence to anticipate and prepare for emerging threats.

Network Segmentation

Divide networks into segments to contain and limit the impact of any breach.

Incident Response Planning

Develop and regularly update a comprehensive incident response plan.

Prepare for All Malware

Addressing AI-driven malware threats necessitates a multi-layered approach. Traditional antivirus (AV) solutions are critical for eliminating known threats that might be part of AI attack campaigns. They are fast, efficient, and can address conventional and AI-enhanced threats, creating a solid first line of defense. However, AV may not initially detect new malware variants as it takes time for signature files to update.

Content Disarm and Reconstruction (CDR) technology addresses this gap. CDR steps in where AV solutions might fall short by using a sanitization process that rebuilds files from known-safe components. This method effectively eliminates unique malware variants that might slip through AV defenses. So, even if a phishing attempt bypasses initial security layers, the malware embedded within can still be neutralized.

Manage Attack Surfaces

Effectively managing attack surfaces is another critical strategy in combating AI-powered cyber threats. Attack surface management takes a deep dive into reviewing your organization to discover and prioritize all assets, their organizational value, and potential exposures they have. This process involves thoroughly assessing the IT infrastructure to identify and mitigate vulnerabilities. Organizations can effectively prioritize their security efforts by understanding the value and risks associated with each asset. This proactive approach minimizes potential attack vectors, reducing the opportunity for AI-powered cyber threats to exploit these vulnerabilities.

Votiro Helps Defend Against Advanced AI Threats

Not only does Votiro provide proactive file-borne threat prevention, the advanced Data Detection & Response (DDR) platform revolutionizes cybersecurity with its real-time privacy masking and actionable threat analytics. This enables organizations to tackle advanced AI-driven threats more efficiently while streamlining the investigation process to focus on true positives, minimize false positives, and reduce alert fatigue.

Combined with its CDR capabilities and AV protection, Votiro is able to provide multiple advantages: safeguard against known threats, enable privacy compliance, and equip teams with tools to effectively understand and manage vulnerabilities.

Contact us today to learn how Votiro provides the visibility your organization needs to efficiently stop hidden threats in files, including those designed by AI.