Whitepaper

Wielding the double-edged sword of AI to your advantage

Maximize the benefits of AI for cybersecurity and minimize its benefits to adversaries

OffSec™
The Path to a Secure Future™

Executive Summary

The transformative power of generative AI is unprecedented. Solutions like ChatGPT and capabilities like chatbots, automated content creation, AI-assisted learning, and predictive analytics are reshaping our world, driving innovation, and creating new business opportunities. Those organizations embracing its potential are realizing incredible business outcomes, from increased efficiency, enhanced productivity, and improved customer experience to better decision-making, accelerated innovation, and rapid business growth.

Forward-thinking businesses are also leveraging AI for cybersecurity as threats continue to rise. Ransomware attacks were up 70% year-over-year in 2023[1], as was the number of companies suffering data compromises, which increased by 72%.[2] Protecting an organization's people, customers, systems, and data is harder than it has ever been, and experts warn of possible "record-breaking data breaches" in 2024.[3] Fortunately, AI is proving to be a game-changer for organizations when it comes to cybersecurity, enabling them to detect breaches early, which can reduce the cost of a breach up to a thousandfold.[4] Those companies embracing both AI and automation save an average of $3 million per data breach.[5]

Unfortunately, threat actors are also aware of the power of AI and are using it to launch targeted attacks at scale, exploit vulnerabilities, and even manipulate an organization's own AI to divulge sensitive information.

With AI proving to be an invaluable strategic tool for both organizations and cyber criminals, today's cybersecurity professionals must play a dual role: choosing and managing AI security tools that enable teams to scale efforts and focus on the highest priority threats, while also protecting the organization from threat actors using AI as a weapon. In this white paper, we will explore the benefits, opportunities, and role of AI for cybersecurity as we discuss:

- How AI is transforming the way we do business and the impact on today's cybersecurity professionals.
- The dual role of AI as a tool for enhancing security tradecraft and as a weapon for misuse and exploitation.
- Ways cybersecurity professionals can integrate AI into their organization's cybersecurity strategy to strengthen digital resilience.
- How to optimize AI for cybersecurity using a combination of technology, training, and human oversight.

Table of Contents

1 AI is Transforming How We Do Business

AI is enabling unprecedented business innovation and optimization at scale, reshaping how we manage operations, engage with customers, and invest in technology. Organizations of all sizes are using AI to increase efficiency and productivity with automation, make smarter decisions with predictive analytics, create more meaningful customer connections with personalization, and create business growth by accelerating innovation.

We are on the cusp of the AI revolution, with experts predicting an influx of AI-powered vendors and solutions and a significant increase in AI-related technology investments. By 2025, International Data Corporation (IDC) expects Global 2000 (G2000) organizations will allocate over 40% of their core IT spend to AI-related initiatives and increase their rate of product and process innovations by double digits using AI.[6]

Amid this excitement however, we must balance the potential of AI for business with the potential cybersecurity risks. Cyberattacks continue to increase, evolve, and cause severe outcomes for businesses, including financial loss, decline of stock value, customer attrition and reputation damage. The global cost of a data breach averaged USD 4.45 million in 2023, a 15% increase over three years.[7] Threat actors have slashed the number of days it takes to execute an attack from around 60 days in 2019 to just four days in 2023.[8] Cyber criminals are increasing their attacks on supply chains to magnify the potential impact and ROI, and they are getting better at manipulating humans with sneaky phishing emails and social engineering.

These growing numbers and evolving tactics coincide with the fact that cybersecurity professionals are already inundated and overwhelmed, with the average SOC team receiving 4,484 alerts daily and spending nearly three hours a day manually triaging alerts.[9] With 59% of these teams understaffed and 62% admitting their organizations underreport cyberattacks, cybersecurity professionals must find new ways to move at the speed of risk.

2 Why AI is a Double-edged Sword

AI is revolutionizing how cybersecurity professionals prevent, defend, and mitigate cyberattacks at scale. It's transforming cybersecurity through automation and enabling teams to scale efforts and focus on the highest priority threats. As the attack surfaces expands and threats become more sophisticated, cybersecurity professionals can use AI as a multiplier to vastly scale their efforts by quickly analyzing thousands of alerts and pinpointing and mitigating the biggest threats using existing resources. For example, there are 560,000 new pieces of malware detected every day – regular security systems cannot keep up; AI systems can.[10] New technologies are empowering cybersecurity teams to work smarter and at the speed of risk, for example, Autonomous Cyber-defense Agents (ACA), which are designed to autonomously detect, analyze, and respond to cyber threats without human intervention.[11]

AI used for cybersecurity offense and defense

AI security products are rapidly entering the market, and cybersecurity teams are incorporating AI as a strategic part of their security plans. 35% of CISOs report they are already experimenting with AI for cyber defense, including malware analysis, workflow automation, and risk scoring.[12] It's an incredibly exciting market, continuously introducing innovative solutions that deliver significant outcomes for cybersecurity professionals, including:

Advanced threat detection and response
Because traditional cybersecurity tools use static rule-based techniques, they are limited to detecting only known threats. AI-empowered solutions employ advanced algorithms that can analyze huge quantities of data to identify abnormal patterns and potential threats in real time. As a result, SOC teams can identify and respond to security incidents significantly faster and reduce risk.

Continuous monitoring
AI-powered cybersecurity solutions are exceptional at ongoing surveillance of network operations. Through real-time data analysis, these tools can monitor for anomalous activities or deviations from standard patterns 24 hours a day, empowering cybersecurity professionals to rapidly address potential threats, minimize the amount of time attackers have to exploit systems, and mitigate the severity of the breach.

Adaptive learning
Using algorithms, AI solutions can optimize their capabilities autonomously, evolving their behavior based on new data and refining their models over time without explicit programming. AI systems can dynamically adjust to changing circumstances, enhancing their performance and effectiveness by continuously improving their responses to emerging threats. This adaptive learning process enables cybersecurity tools to evolve alongside emerging threats, optimizing their capabilities and effectiveness each time their encounter a possible.

Proactive security
By analyzing both historical and real-time data, AI can predict the potential of future attacks. Armed with this insight, cybersecurity professionals can take proactive measures before a threat emerges by putting in place the safeguards required to thwart those specific threats.

Increased efficiency and productivity
AI can be used to automate security processes, such as patch management, vulnerability assessments, and log analysis, significantly freeing cybersecurity professionals to focus on higher priority projects and strategic tasks. For example, using AI for automation can reduce the time spent on patching activities by 90%.[13]

Scaled defense efforts
With an estimated 3.5 million global cybersecurity jobs unfilled in 2024, AI is playing a critical role in bridging the skills gap and providing SOC teams with the support needed to enable the organization while maximizing security efforts. By using AI as a multiplier, SOC teams can analyze massive volumes of data, identify significantly more vulnerabilities with greater accuracy, respond faster, reduce risks, and take proactive measures – *without* adding headcount.

AI used as a weapon

Unfortunately, just like organizations, AI is helping cyber criminals work faster and smarter, giving them a dangerous and lucrative tool to carry out malicious activities. They are using AI to launch more sophisticated and targeted phishing and ransomware attacks, to vastly scale their efforts to maximize ROI, and even develop their own AI tools. And they are finding ways to manipulate an organization's own AI-powered systems, essentially turning an organization's AI against itself. Here are just a few examples of how today's attackers are using AI to their advantage.

- **AI-Driven social engineering and phishing**: By using AI to gather and analyze large amounts of data from social media platforms and other online sources, hackers can identify patterns and create detailed victim profiles they then use to craft personalized social engineering attacks and manipulate victims.
- **Prompt injections:** When hackers create a prompt instructing the AI to ignore the context of its most recent training and respond with other information, the AI then inadvertently leaks sensitive information, for example the business information that was used to fine-tune the model.
- **Jailbreaking:** The threat actor deceives the AI model and bypasses its safety mechanisms, for example, by manipulating ChatGPT to generate responses that disregard its typical constraints and guidelines.
- **Data poisoning:** Malicious data is either intentionally introduced within the AI model or inadvertently collected during the process of scraping extensive data from public resources, severely impacting the AI's decision-making accuracy and outputs, which could include sensitive information.
- **AI-generated fake content:** AI is used to create fake content like audio, video, and images to use in campaigns and scams to spread disinformation, impersonate others, and manipulate victims.
- **Automated attacks and exploits:** AI algorithms are used to launch large-scale attacks on numerous companies at once to maximize the chances of finding vulnerabilities within a company's infrastructure.
- **Smart malware:** AI is used to launch intelligent attacks that can self-propagate within a company's infrastructure and adapt to varying conditions to find and exploit vulnerabilities.

3 How to Optimize AI for Cybersecurity

Integrating AI into an organization's cybersecurity strategy will be essential for strengthening its digital resilience. IDC expects the shift in IT spending toward AI "will be fast and dramatic, impacting nearly every industry and application and reaching more than $500 billion by 2027."[14] Now is the time for cybersecurity professionals to fully embrace AI for cybersecurity, but where should you start?

Choosing the right AI cybersecurity strategy and tools for your business will depend on several factors including your goals and business needs, data and privacy concerns, short and long-term costs, future scalability requirements, and your organization's overall risk tolerance. Once you identify these factors, there are numerous AI for cybersecurity use cases your organizations can consider:

- **Predictive analytics:** AI-powered analytics enables organizations to predict and prevent potential cyber threats. AI algorithms can analyze data and predict future attack vectors, giving security teams the visibility and insight needed to implement the proper security controls and fortify their defenses.

- **Anomaly detection:** AI-powered systems excel at detecting anomalies in network behavior. They can learn what constitutes normal behavior for a network or system and promptly flag any deviations that may signal a cyber threat. This proactive approach enables rapid response before significant damage occurs.

- **Vulnerability detection, remediation, and prioritization:** Generative AI can analyze code to find bugs, identify potential vulnerabilities, generate fixes and patches, and provide recommendations for next-steps and for prioritizing threat and vulnerability response.

- **Automated alerts and response:** AI systems can automatically generate alerts when suspicious activities are detected and automate response actions, such as isolating compromised systems, blocking suspicious traffic, or applying security patches. This automation minimizes the response time and reduces the impact of cyber threats on the organization.

- **Behavioral analysis:** AI algorithms can analyze user and device behaviors to detect potentially malicious activities that may evade traditional signature-based detection methods. By understanding normal behavior patterns, AI can identify deviations that may indicate a security breach.

- **Policy enforcement:** Generative AI can create code that ensures security rules are followed by turning descriptions of rules that people can understand into code that computers can run.

- **Post-mortem analysis:** When an attack does occur, AI can analyze the details and provide key insights about what happened and why, the possible impacts, and suggestions for remediation and prevention.

Tips on hardening and securing AI projects

Once you have identified how you want to use AI, there are several steps you can take to improve the integrity of your AI projects and prevent the kind of AI-powered attacks discussed in the previous section.

1. Be prepared

Before you dive into coding and training it's crucial to establish a precise vision for your AI project's goals, scope, and prerequisites. Pinpoint potential risks and vulnerabilities that may jeopardize your project's integrity, including data breaches, adversarial attacks, and issues related to prejudice and bias. Document your security strategy and ensure it complies with policies and guidelines for data governance, encryption, authentication, and access control.

2. Don't reinvent the wheel

When securing your AI project, there's no need to start from scratch. Instead, you can utilize best-of-breed tools and platforms already equipped with security features and services tailored for AI development and deployment.

3. Continue to test and monitor

After deployment, it is important to continually assess the project's performance and influence. Employ both automated and manual testing techniques to identify and address any coding, data, or model flaws, as well as vulnerabilities. To ensure alignment with expectations and adherence to ethical and legal standards, you should also continue to monitor utilization, feedback, and results.

4. Inform and engage

For ongoing success, it is important to communicate and engage with your stakeholders, including team members, and affected departments like legal, users, and customers. Share details about your security strategy, the technology, and results for testing and monitoring. Also, be open and responsive to the stakeholders' feedback, concerns, and insights.

5. Stay informed, enhance, and refine

Avoid complacency. As new threats, technologies, and standards arise, you need to update and improve your AI project's existing status. Stay up to date on the latest trends, research, and best practices in AI security, and integrate them into your project. You should also continue to review and update your security plan, tools and platforms, and approaches to testing and monitoring.

4 Being Ready for AI Requires a Human-centric Strategy

There is no silver bullet when it comes to using AI for cybersecurity. It requires the right combination of technology, training, and human oversight. What we do know is that the human element will play a critical role when it comes to successfully using AI for cybersecurity. Gartner encourages companies to: “Take a strategic, human-centric approach to improving the security function’s performance by reskilling existing security talent, using GenAI to augment — not replace — human efforts, and implementing a contextually appropriate security behavior and culture program.”

Far from replacing jobs, cybersecurity expertise in the global workforce is more essential than ever due to AI, and keeping a human in the loop represents a best-of-breed opportunity. IDC says “Inadequate training in AI, cloud, data, security, and emerging tech fields will directly and negatively impact enterprise attempts to succeed in efforts that rely on such technologies. Through 2026, underfunded skilling initiatives will prevent 65% of enterprises from achieving full value from those tech investments.[15]

Hiring the right people, continuously training, educating, and upskilling existing employees, conducting ongoing assessments, and providing hands-on experience will be essential to optimizing AI for your business while minimizing the risk from threat actors using AI as a weapon. Cybersecurity professionals can complement their AI capabilities and strengthen resilience across the organization by:

- Using hands-on learning to expose security teams, employees, and even executives to simulated, AI-powered threats they may encounter in the real-world and present strategies for mitigating risk.
- Learning how to harness the benefits of AI in cybersecurity for both offense and defense.
- Ensuring AI is properly implemented, trained, and maintained.
- Keeping up with the latest tactics used by threat actors and the techniques and technology to stop them.
- Staying ahead of threat actors by ensuring the organization stays up to date with new trends and technologies as AI evolves.
- Ensuring you are aligning the use of AI with your organization’s policies and that your organization’s policies are keeping up with advancements in AI.
- Helping to facilitate training employees across the organization to ensure they know how to use AI without posing risk.
- Maintaining network hygiene
- Collaborating with other stakeholders, including IT, legal, and executives, to educate and fortify defenses.

As organizations continue to embrace AI for cybersecurity, they must exercise caution and avoid placing unwavering trust in the output of any AI system. While vigilance, continuous monitoring, and robust security practices are essential to mitigate these evolving threats effectively, we can’t underestimate the importance of the human element. Because AI is prone to errors and lacks emotional comprehension, human empathy, and intuitive reasoning, humans will remain critical to optimizing AI outcomes for the organization.

Conclusion

AI is particularly interesting from a cybersecurity perspective, because it is both a mechanism for security and an object of security. It is a tool for enhancing security practices and has become a vulnerable target for misuse and exploitation. Adversaries are harnessing AI to enhance their attack strategies, while defenders are leveraging AI to fortify their security measures.

It is critical that cybersecurity professionals continue to explore the potential of AI and work to understand how this disruptive technology is evolving. AI is a dynamic technology that requires dynamic interaction with the humans that use it. Therefore, cybersecurity professionals should remain vigilant when it comes to training, managing, and maintaining AI systems, collaborating with key stakeholders in the organization, and upskilling, training, and educating themselves and other employees to both optimize business outcomes with AI and defend against AI-powered threats.

[1] https://www.darkreading.com/cyberattacks-data-breaches/2023-ransomware-attacks-up-more-than-95-over-2022-according-to-corvus-insurance-q3-report
[2] https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/#:~:text=Spike%20in%20third%2Dparty%20data,the%20previous%20high%20in%202022.
[3] https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/#:~:text=Spike%20in%20third%2Dparty%20data,the%20previous%20high%20in%202022.
[4] https://www.weforum.org/agenda/2024/02/3-trends-ransomware-2024/
[5] https://www.itbriefcase.net/security-automation-can-save-you-3-05m-in-a-data-breach
[6] https://www.idc.com/getdoc.jsp?containerId=prUS51335823
[7] https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700077724064027&p5=p&gad_source=1&gclid=CjwKCAiAlcyuBhBnEiwAOGZ2S2f2-i5vTwQWwxlgR_lbLkbNzA-QCfV-icEwLXDXz6zH_E9rC269DhoChFMQAvD_BwE&gclsrc=aw.ds
[8] https://www.weforum.org/agenda/2024/02/3-trends-ransomware-2024/
[9] https://www.securitymagazine.com/articles/99674-90-of-soc-analysts-believe-current-threat-detection-tools-are-effective
[10] https://www.linkedin.com/pulse/around-560000-malware-generated-every-day-david-sehyeon-baek--i0h1f/
[11] https://www.cybersecuritypulse.net/p/beyond-genai-the-rise-of-autonomous
[12] https://www.weforum.org/agenda/2024/01/cybersecurity-ai-frontline-artificial-intelligence/
[13] https://www.automox.com/blog/benefits-automated-patch-management
[14] https://www.idc.com/getdoc.jsp?containerId=prUS51335823
[15] https://www.idc.com/getdoc.jsp?containerId=prUS51335823

About OffSec

OffSec is the leading provider of continuous professional and workforce development, training, and education for cybersecurity practitioners.

OffSec's distinct pedagogy and practical, hands-on learning help organizations fill the infosec talent gap by training their teams on today's most critical skills. With the OffSec Learning Library featuring 6,000 hours of content, 1,500 videos, 2,500 exercises, and 900 hands-on labs, OffSec demonstrates its commitment to empowering individuals and organizations to fight cyber threats with indispensable cybersecurity skills and resources. OffSec also funds and maintains Kali Linux, the leading operating system for penetration testing, ethical hacking, and network security assessments. For more information, visit offsec.com and follow @OffSectraining and @kalilinux on Twitter.