PALO ALTO NETWORKS

CYBERPERSPECTIVES

ISSUE 2 | 2024

ACCELERATING REAL-TIME SECURITY OUTCOMES WITH AI

CYBER LEADERSHIP

ARTIFICIAL INTELLIGENCE

SECURITY AS A BUSINESS ENABLER

LATEST RESEARCH

AI in Cybersecurity — a CISO's Perspective

By Dena De Angelo

As AI technology matures and proves its worth, it is set to revolutionize the way security professionals approach their roles and responsibilities. This is not hyperbole, yet rather a credible assessment of the daily outcomes experienced in our own security operations and with our customers who benefit from deploying our AI-driven solutions. In a candid interview with Niall Browne, CISO of Palo Alto Networks, we explored the profound impact of artificial intelligence on the current and future landscape of cybersecurity.

AI's Journey in Cybersecurity

While AI is not a novel concept, its full potential is finally becoming a reality with the democratization of tools, such as generative AI. As such, there has been a noticeable shift as AI has seemingly entered the mainstream, available to anyone with access to a keyboard and an internet connection. And Browne envisions even more tectonic changes on the way.

Adversaries are already continually examining the tools used by organizations and exploring ways to leverage AI to compromise their targets. This battle will remain a nonstop game of cat-and-mouse for the next 5 to 10 years. Both defensive and offensive teams are constantly recalibrating their strategies and techniques, trying to one-up each other, but this game will look different as AI evolves.

AI-powered adversaries don't have the same limitations as humans. They never sleep or take breaks. They don't get distracted. They can move at machine speed. They can multitask in ways humans can't. AI can exploit vulnerabilities, move laterally, and compromise multiple targets simultaneously, posing a significant threat to organizations.

We have seen similar changes in financial markets with high-frequency trading, where technology advancements led to millisecond interactions. In a world of AI, cybersecurity will transition from humans dealing with threats over days to AI handling them in milliseconds.

Bolstered by AI's capabilities, initial compromises to data theft are possible in hours now. Coordinated wide-scale attacks are happening concurrently. And, attackers are increasingly showing a deep understanding of how business processes work. This all leads to an unprecedented increase[1] of security events and breaches. The relentless advancement of technology, coupled with the creative minds of malicious actors, paints a potentially grim picture for the cybersecurity landscape. Attacks are already increasing in "speed, scale and sophistication"[2] according to Wendi Whitmore, SVP, Unit 42.

That said, Browne sees an inflection point occurring right now where AI is being applied effectively to detect and respond to cyberthreats before they can cause harm. This transformation is akin to the paradigm shift that occurred when organizations embraced cloud computing. Browne elaborates on that comparison:

"The power of AI will be transformative for cybersecurity teams. We're now seeing the real potential for AI to detect attacks as they occur, and then to help the systems recover from those same attacks. I am certainly seeing there's a huge undertaking from cybersecurity teams to start embracing AI, similarly to the »

journey 6 or 7 years ago, when enterprises started embracing the move to the cloud.

I think AI will totally transform the way cybersecurity teams operate within their organization, from the security operations center, to application security teams, and beyond."

Understanding the Importance of Metrics in Security

Looking at the current state of technology, Browne details key performance metrics for evaluating the effectiveness of AI-powered solutions in cybersecurity. Metrics are crucial to understanding how to improve processes and where there are security gaps. But, he dismisses the idea of mean time to close as a top metric, comparing it to call center practices where the aim is to quickly end calls. Instead, he prefers to focus on metrics related to systems and AI capabilities:

- **Percentage of Systems Logged and Data Ingested**: Tracking how much data is ingested from various systems.
- **False Positives and True Positives Rates**: Ensuring a balance between accurate alerts (true positives) and avoiding unnecessary alerts (false positives).
- **Mean Time to Detect**: The time taken to detect an incident once it occurs. Browne's goal is a swift 10-second detection time.
- **Mean Time to Respond**: Measuring how quickly the security team responds to an incident, aiming for a 10-minute response time.

These metrics enable organizations to assess the efficiency and effectiveness of their cybersecurity operations. Browne also highlights the ease of comparing these metrics when transitioning from legacy SIEM (security information and event management) systems to AI-based SIEM, allowing for clear ROI calculations. Palo Alto Networks Cortex XSIAM®[3] is quickly demonstrating its prowess in handling data that can be ingested and integrated to feed machine learning, analytics and automation. With a SOC that ingests over 1 trillion events per month, nearly 40 billion per day, and intelligently groups and analyzes alerts, resulting in only eight incidents a day on average in need of human investigation.

"In the case of Palo Alto Networks, we use XSIAM and we leverage that on a day-to-day basis to go through approximately 75 TB gigabytes of data. And, that's allowed us internally to achieve a result of a mean time to detect of 10 seconds, and then a mean time to respond of 1 minute."

The Exponential Growth of AI in Cybersecurity

With the advent of AI and more automation, there is a shift away from traditional, four-tiered SOC structures, where human analysts handle most tasks, toward a model where AI takes over the initial triage and analysis.

Browne agrees with this evolution and shares that, in his vision, the lower tiers of a SOC (Tier 1, 2 and 3) will be primarily AI-driven, while human analysts will focus more on Tier 4 tasks. At Palo Alto Networks, Browne notes that we've eliminated lower SOC layers, creating a more dynamic workforce of specialists. This shift allows SOC analysts to concentrate on more engaging and valuable tasks, like threat hunting, ultimately leading to higher levels of job satisfaction and lower levels of attrition. »

As organizations increasingly embrace AI for cybersecurity, we are witnessing a profound transformation across various facets of the industry:

AI Data Concentration Risk: Internal AI systems will have access to a treasure trove of highly confidential information. This data concentration risk will ensure that AI becomes the top target for hackers. As such, organizations will need to deploy significant resources to ensure these AI systems are deployed and secured appropriately, from the start. To add to the complexity, some AI security controls may be nascent, and as such, compensating controls will become critically important.

Shift Left for Security: The concept of "shift left" in security emphasizes addressing vulnerabilities at the earliest stage of the development process (i.e., before they are introduced.) With AI assistance, developers can receive real-time feedback on potential security issues, leading to more secure code and infrastructure. This shift left approach ensures that security is not an afterthought but an integral part of the development process.

Security Operations Transformation: AI is poised to have the most significant impact on security operations. Security operations centers (SOCs) are currently overwhelmed by the sheer volume of alerts and incidents. AI-driven solutions can sift through vast amounts of data, prioritize threats, and significantly reduce false positives. This enables SOC teams to focus on high-value tasks, such as threat hunting and research, as opposed to low-value alerts. In fact the Palo Alto Networks SOC spends just a third of their time on alerts, enabling them time to focus on much higher value work.

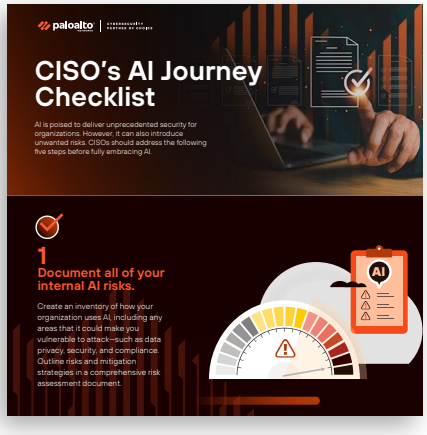
Reshaping Security Analyst Roles: With AI handling routine tasks, security analysts can evolve into high-value resources. They can dive deep into data analysis, threat intelligence and proactive threat hunting, driving overall security maturity within organizations.

The AI-Driven Future Looks Bright

Browne predicts that AI will transform the cybersecurity landscape in the next few years, delivering value that exceeds expectations. It's not just about potential; it's about real-world applications. AI is set to become an indispensable tool in the security arsenal, exponentially improving efficiency and effectiveness.

Imagine a world where AI serves as a co-pilot to developers, offering real-time guidance on secure coding practices. Envision security operations teams with drastically reduced alert fatigue, focusing on the most critical threats. Picture a security landscape where the attacker's job becomes exponentially more challenging due to AI-powered defenses. It's a future ripe for possibilities, and Palo Alto Networks is leading the charge with AI-driven products such as Cortex XSIAM and the whole Cortex suite of products.

AI is not just a buzzword but a tangible force shaping the future of cybersecurity. As organizations adopt AI-driven security solutions, they will experience a significant transformation in their security posture. With AI as a co-pilot, we are on the cusp of a more secure digital world, riding shotgun with some pretty cool tools. And as technology advances, defenders and organizations must adapt rapidly to stay ahead of the ever-more-sophisticated adversaries they face.



1. Goodkind, Nicole. "JPMorgan Chase says hacking attempts are increasing." *CNN*, 18 January 2024.
2. "How can AI be used to 'accelerate and automate work' against cyber attacks?" *Fox Business*, 17 January 2024.
3. Fink, Gonen. "XSIAM 2.0: Continuing to Drive SOC Transformation." Palo Alto Networks, 13 November 2023.

Dena De Angelo is a content marketing manager at Palo Alto Networks

Click the QR code above to view a CISO's AI Journey checklist

What Is Precision AI?

Precision AI™ is Palo Alto Networks proprietary AI system. It helps security teams trust AI outcomes by using rich data and security-specific models to automate detection, prevention, and remediation with industry-leading accuracy.

Precision AI by Palo Alto Networks incorporates the best AI capabilities:

- **Machine learning** ("ML"): Built into many of our products for more than a decade, ML allows our security applications to become more accurate at preventing, predicting, and remediating security problems by using precise, defined historical and current data as input to predict novel situations.
- **Deep learning**: This helps us build predictive models to anticipate and detect security issues in real time by learning from massive amounts of security data.
- **Generative AI** ("GenAI"): We use GenAI to enable our tools to "speak human," simplifying UX and summarizing large volumes of threat intelligence. We do this through our copilots, which, built on our own highly controlled datasets, reduce mean time to resolution ("MTTR").

Artificial intelligence has quickly become the most disruptive technology innovation since cloud computing. Organizations of all types and across all industries are racing to use AI to achieve competitive advantage, accelerate product development, improve productivity, reduce costs, and redefine many aspects of their business.

AI also opens up a veritable Pandora's box of new cybersecurity vulnerabilities. Cybercriminals are already using AI to scale and accelerate attacks, circumvent existing security controls, and improve existing attack methods such as phishing and prompt injection attacks.

This is just the tip of the iceberg. As AI becomes more widely adopted as a business tool, it will exponentially expand the attack surface and give criminals new vectors to target. Cybersecurity teams are already responding to incidents of adversarial AI used to poison data or write malicious code. Expect cybercriminals to continue being innovative in using AI to strengthen and sharpen their attacks. CISOs are increasingly concluding that the only way to fight AI is with AI. But traditional approaches have fallen short due to factors like inconsistent data quality, security silos, and a skills gap caused by a lack of individuals with expertise in both AI and cybersecurity. A new AI-first approach is needed.

Precision AI Capabilities

Precision AI by Palo Alto Networks is the next generation of AI used explicitly for cybersecurity. Precision AI is a proprietary system that builds on traditional AI/ML approaches but customizes it for security. Specifically, Precision AI brings high-resolution capabilities to cyber defenders by centralizing and analyzing data with security-specific models to help defenders automate detection, prevention, and response. Security has now transitioned to a data problem, requiring data with Precision AI to stop rapidly evolving bad threats in real time. By trusting Precision AI, security teams can confidently automate and achieve security outcomes faster.

The Key Elements of Precision AI: Data and Models

Data

Effective security requires a very high volume of security-specific data. Palo Alto Networks leverages one of the industry's largest footprints of tools and capabilities deployed across various sectors and verticals. We can observe even more adversarial events with each additional customer, giving all customers better security outcomes. We collect and analyze the most data of any pure-play cybersecurity leader in the industry, which we use to protect us all better. For security, resolution becomes a function of seeing data across: »

- **Attack types**: Gathering data on cyberattacks varies significantly based on targets, platforms, and more.
- **Threat actor activity**: Developing threat actor profiles based on methods across tools, techniques, and procedures across our entire customer base.
- **Sectors**: Identifying the type of attacks that are unique to specific geographies and verticals.
- **Data history**: Storing time-stamped information about the above data provides a compounding advantage.
- **AI-generated attacks**: Identifying when attackers use AI/ML or GenAI attacks to develop malware, phishing attacks, deep fakes, and more.

Models

To be useful in cybersecurity, Precision AI must be as close to 100% accurate as possible to find every true attack and avoid alerting on false positives. The only way to get there is to use security-specific combinations of AI techniques. While ML and deep learning are the core, Precision AI also takes inputs from GenAI-generated attacks to train defensive capabilities further.

Additionally, we combine the intelligence and findings of our expert security research teams into these models, creating features that leverage machine intelligence and domain expertise. The Precision AI proprietary system takes the best techniques from all forms of AI and intelligently combines them to get the right outcomes—detecting attacks, zero days, breaches, and more—while also rapidly helping fix issues.

How Palo Alto Networks Platforms Use AI

Palo Alto Networks has been a pioneer in integrating ML and AI capabilities into its products and workflows. On a typical day, we use more than 1,300 AI models to analyze millions of new telemetry objects globally. Each day, we detect approximately 1.6 million new and unique attacks that weren't there the day before and block about 8.6 billion attacks.

Precision AI is, in conjunction with the platform model, the cornerstone of the Palo Alto Networks approach to cybersecurity transformation. The AI-first platforms that Precision AI powers include Strata, Prisma Cloud, and Cortex.

Strata

Strata™ is a network security platform that uses AI to stop zero-day and mutated threats in real time, accurately identify new devices that have never been seen, and proactively improve security posture to prevent network disruptions. Precision AI powers Strata in the following ways:

- The industry's first ML-powered next-generation firewall and cloud-delivered security services to stop unknown zero-day attacks, enabling cyber teams to go beyond signature-based threat detection and block the most evasive threats.
- IoT security uses a patented, three-tiered ML learning model to identify new devices accurately. This enables cyber teams to understand risk better and apply security policy based on the principle of least privilege.
- Tools such as Strata Cloud Manager and Strata Copilot to optimize security posture, predictively identify potential disruptions and use generative AI to help cyber teams understand their top security priorities using natural language.

Prisma Cloud

Prisma® Cloud is a comprehensive, AI-driven platform that secures everything from code to cloud. It enables cybersecurity teams to effectively operationalize tooling, scale security to match DevOps velocity, and protect AI infrastructure from compromise. Precision AI powers Prisma Cloud in the following ways:

- Prisma Cloud Copilot to streamline product setup and troubleshooting by automating tedious tasks and simplifying the creation of customized queries, dashboards, and reports.
- AI-infused security to automatically detect attack paths, intelligently prioritize risk management, discover complex breaches using tools such as APIs and Kubernetes, and enable auto-generated remediation such as infrastructure as code (IaC) templates.
- Vulnerability scanning across the AI supply chain, monitoring and filtering malicious prompts, AI data protection, and enforcement of least privileged access. With Prisma Cloud, organizations can use Precision AI against adversarial AI by detecting and blocking attack paths, such as denial-of-service attacks on an LLM.

Cortex

Cortex® is a platform for security operations, empowering cyber teams with AI-infused detection, investigation, automation, and response capabilities to stop threats at scale and accelerate incident remediation. »

Precision AI powers Cortex in the following ways:

- Continuous collection, stitching, and normalization of raw data, not just alerts. Hundreds of out-of-the-box AI models connect alerts and provide the complete picture of an incident in one place, enabling better detection, analysis, and response.
- Cortex Copilot, an AI copilot, simplifies how analysts gather information and take security actions in Cortex XSIAM (Extended Security Intelligence and Automation Management). This includes risk-related actions such as investigation and automatic response, as well as operational tasks such as smart assignment of analysts to incidents.
- Attack surface management, including the ability to continuously scan the internet, uses ML models to continuously map the attack surface and immediately reduce attack surface risks with built-in automated playbooks.
- Accurate detection and prevention of incidents using behavioral analytics and more than 1,300 AI models. Alert grouping and AI-based incident scoring connect low-confidence events into high-confidence incidents that are prioritized based on overall risk.

Benefits of Precision AI

Products powered by Precision AI enable cybersecurity teams to be faster and more precise in responding to all types of attacks in real time, and it eases the burden on humans by giving them new levels of intelligence, analytics, and automation to do their jobs more efficiently. With Precision AI, cybersecurity teams can combat the latest threats, simplify security, and secure AI infrastructure.

Combat the AI-Driven Threats

Hackers use adversarial AI to improve phishing, scale attacks, create new attacks, and target vectors. Precision AI empowers organizations to evolve to real-time, autonomous security to stop advanced threats, improve MTTR, and address operational challenges. As AI becomes a more powerful weapon for adversaries, Precision AI by Palo Alto Networks enables cyber teams to anticipate and prevent new attack vectors in real time.

Simplify Security

Cybersecurity teams are already under enormous pressure, and organizations still face a shortage of people with important skills. Precision AI by Palo Alto Networks has the potential to revolutionize how practitioners interact with their security toolset. This improves access to information and insight, suggested actions, and less time spent trying to navigate user interfaces or consult product documentation. With products powered by Precision AI alleviating humans from many tedious tasks, cyber teams can be far more productive and effective.

Secure AI by Design

AI infrastructure represents a new and potentially crippling vulnerability. Attacks such as data poisoning or using AI to write malicious code are new vectors that are difficult to identify using traditional security tools and techniques. Products powered by Precision AI enable cybersecurity teams to protect AI infrastructure from compromise, using AI models to secure the entire AI roadmap.

Precision AI: Key Takeaways

AI is ushering in a new era of cybercrime and cybersecurity, and it is all happening at an extraordinarily rapid pace. Cybersecurity teams face new challenges that must be addressed quickly, efficiently, and comprehensively. These include:

- Gauging the impact of AI on businesses, employees, and customers.
- Understanding how their cybersecurity strategy needs to evolve.
- Quantifying incremental cybersecurity risk as a result of AI adoption.
- Implementing governance and compliance models for AI.
- Understanding how adversaries are leveraging AI to circumvent security.
- Deploying AI-based solutions that deliver real-time results with precision and accuracy.

It is an understatement to say a lot is at stake—everything is at stake. Hackers are already using AI to great effect in phishing, malware, and DDoS attacks.

If organizations are to harness AI's vast potential to transform their businesses, they must be able to use AI safely and defend against attacks using AI. They must be precise in preventing, detecting, and responding to attacks.

The Precision AI system is designed specifically for a new era of AI-first cybersecurity to help organizations combat the latest threats in real time. Precision AI simplifies security and enables organizations to secure new AI-related projects and infrastructure.

Accelerating Real-Time Security Outcomes with Precision AI

By Rob Rachwald

New capabilities enable customers to counter AI with AI, secure AI by design and simplify security.

AI Is already transforming every enterprise. AI has been driving productivity for over a decade, but over the past 18 months, it has hyper accelerated with broad adoption of generative AI. This has fueled AI adoption across the entire enterprise with employees finding uses for GenAI in every department. AI is revolutionizing our business world – how we defend against threats, the attacks lobbied against us, and the skills we must have to manage the new frontier. To help our customers combat new threats while also leveraging the promise of efficient security, Palo Alto Networks is introducing Precision AI™.

What Is Precision AI?

All of the existing and new capabilities of Palo Alto Networks are powered by Precision AI. Built on the world's largest security dataset among pure-play cybersecurity leaders, Precision AI combines machine learning's predictive accuracy and automated remediation with the accessibility of generative AI for instant, accurate and trustworthy security outcomes. Our approach to AI, delivered with platformization, reduces risk while simplifying operations, so you can focus on your business.

What Does AI Mean for Cybersecurity?

AI is creating a security inflection point. First, security teams can finally have the ability to analyze their data and put it to work. By analyzing terabytes of data, AI can transform cyber defense by recognizing and blocking attacks in real time. According to a study by Deloitte:

"The benefits are evident in the forecasts of the global AI in cybersecurity market size, which was evaluated at US$17.4 billion in 2022 and is expected to hit around US$102.78 billion by 2032, growing at a CAGR of 19.43% between 2023 and 2032."[1]

Second, threat actors are innovating with Adversarial AI, which means defenders have to rethink defense. With the quick and pervasive uptake of AI in the enterprise, there's a dark side that creates serious security risks, including data leaks, threats to the software supply chain with third-party code, reputational risk and the exposure of confidential information. Attacks will accelerate, scale and create new attacks. Britain's GCHQ report warned: »

"AI lowers the barrier for novice cybercriminals, hackers-for-hire and hacktivists to carry out effective access and information gathering operations. This enhanced access will likely contribute to the global ransomware threat over the next 2 years." [2]

More broadly, we see a fast increase in social engineering, deepfakes, phishing and new attacks, like the software supply chain.

How Should Security Teams React?

CISOs and security teams need to react and secure their enterprise AI transformation:

- Defend Against AI-driven Attacks – Identify and block AI-generated attacks.
- Secure Employee Usage – Inventory AI usage, protect data and apply policy controls across apps and users.
- Secure AI Development – Securing code and the AI software supply chain.
- Reduce Complexity – Siloed data, long response times and ever-changing products bring overhead for security teams.

How Does Palo Alto Networks Provide Security Protections for AI?

Palo Alto Networks has incorporated AI within our products for more than a decade – a heritage that prepares us for scale and automation. But with GenAI's fast-increasing footprint, we've also innovated with new products to help defenders defend with new capabilities.

Strategically, Palo Alto Networks has aligned our AI security approach with the three essential enterprise use cases:

Countering AI with AI

Only ML-powered, real-time protection can stop adversarial AI, using AI in an adversarial way to attack enterprise networks and data. Palo Alto Networks has been innovating AI-powered defense to identify and block AI-generated attacks, especially to detect and prevent acceleration of polymorphic threats. All of the Palo Alto Networks product portfolios – Strata, Prisma Cloud and Cortex – provide near real time detection and threat prevention with behavioral analytics and ML models. Strengthening our Palo Alto Networks product portfolio, we are introducing Advanced DNS Security, the industry's first real time prevention of DNS hijacking and other takeover attacks, using inline AI-powered analysis of DNS traffic.

Secure AI by Design

Protect enterprise apps that leverage AI models.

Prisma Cloud AI-SPM helps organizations discover, classify and govern AI-powered applications. Also, AI-SPM provides visibility into the entire AI ecosystem, including models, applications and resources, to reduce the risk of data exposure and compliance breaches. By identifying model vulnerabilities and prioritizing misconfigurations, it will improve the integrity of the AI security framework with key capabilities:

- Automatically discover all AI models, agents and associated resources for visibility of AI-powered applications and sensitive data involved.
- Identify model misconfigurations and supply chain vulnerabilities to reduce model and application risks.
- Continuously monitor and implement proper governance controls around AI usage.
- Integrate with AI Runtime Security to give your security teams the ability to secure your entire AI application ecosystem at runtime.
- Unit 42 AI Security Assessment provides expert guidance to secure AI-enabled application development.

Secure Enterprise AI Usage at Runtime

Securing Enterprise AI usage (employees using Enterprise AI apps) requires new levels of visibility and control to inventory and sanction AI usage and protect data, AI apps and AI models. Palo Alto Networks is introducing new tactics to help secure this new attack surface:

- AI Runtime Security – Protects Enterprise AI Applications and LLMs from emerging attacks at runtime. Secures business AI ecosystems discovering, detecting and preventing cyberattacks with operational excellence by deploying AI Runtime Security that protect runtime AI applications, models and datasets.
- AI Access Security – A comprehensive, cloud-delivered security solution that enables employees to safely access GenAI applications by eliminating data and security risks. It helps enterprises

»

understand and secure employee access to, and usage of, both sanctioned and shadow AI.

- Unit 42 AI Security Assessment – Proactively address AI threats with expert guidance on secure employee usage of generative AI and hardening of AI-enabled application development.

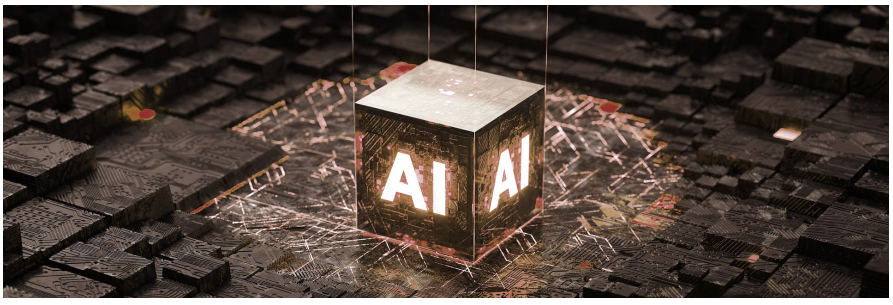
Simplifying Cybersecurity

Palo Alto Networks is introducing powerful copilot capabilities to revolutionize how customers respond to the latest threats across network, cloud and security operations. Leveraging the largest dataset among pure-play cybersecurity leaders in the world, new copilots leverage GenAI to simplify security, delivering rich insight paired with the most accurate security outcomes in the industry, powered by Precision AI. This greatly reduces the time required for our customers to perform key management tasks, get answers to questions, and ultimately take action. Learn more about Precision AI.

This article contains forward-looking statements that involve risks, uncertainties and assumptions, including, without limitation, statements regarding the benefits, impact or performance or potential benefits, impact or performance of our products and technologies. These forward-looking statements are not guarantees of future performance, and there are a significant number of factors that could cause actual results to differ materially from statements made in this article. We identify certain important risks and uncertainties that could affect our results and performance in our most recent Annual Report on Form 10-K, our most recent Quarterly Report on Form 10-Q, and our other filings with the U.S. Securities and Exchange Commission from time-to-time, each of which are available on our website at investors.paloaltonetworks.com and on the SEC's website at www.sec.gov. All forward-looking statements in this article are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

1. Charife, Tamer, and Michael Mossad. "AI in cybersecurity: A double-edged sword." *Deloitte*, 2023.
2. "The near-term impact of AI on the cyber threat." *National Cyber Security Centre*, 24 January 2024.

Rob Rachwald is the director of portfolio product marketing at Palo Alto Networks



Copilots in Cybersecurity — Realizing the Promise of Precision

By Paul Kaspian

There's been a dramatic leap forward in what's possible around Precision AI, and security professionals are looking for ways to leverage these advances in meaningful ways. Early instances of copilots within the cybersecurity industry left many practitioners uneasy, as demos and proof of concepts returned erroneous or even offensive responses to standard security-related questions. Relevancy and precision have become the most critical characteristics to the success of GenAI within cybersecurity.

For vendors, this means gaining access to high volumes of high-quality data, applying this data to AI models in meaningful ways, and having the in-house expertise to ensure the expected outcomes make sense. When applied in these ways, GenAI will have a tremendous impact on cybersecurity operations and outcomes as we know them. AI introduces the ability to ask questions in a natural language, producing operational advantages across the board. For example, operations can spend less time pouring through product documentation, leading to faster identification and remediation of critical vulnerabilities.

Supercharging Security Teams

With highly relevant, accurate answers, security teams will become dramatically more effective. Copilots have the potential to dramatically reduce perfunctory manual processes – from pouring through product documentation to metric and milestone gathering for the board. When done right, they have the ability to surface the most important security tasks, explain why they are critical, and more importantly, expedite fixing the issue.

This could be remediating a vulnerability, reining in overly permissive access controls or quickly thwarting an active attack. This also leaves experienced security professionals to focus on advanced security tasks – threat hunting, red teaming, proactive planning and other high-value activities. At the same time, this also makes less experienced team members more effective by increasing their productivity and flattening the learning curve by using natural language to eliminate the need for deep tool expertise.

Achieving Operational Outcomes — Insight Is Not Enough

Although we don't always like to face the statistics, mean time to detect (MTTD) and mean time to respond (MTTR) continue to be the metrics that don't lie. Copilot solutions need to go beyond delivering timely insight, to helping security professionals ensure these numbers are trending steadily down. This means that cybersecurity copilots need to contribute in tangible ways to alert prioritization, remediation recommendations and even orchestrated counter measures upon human review and approval.

Palo Alto Networks — Leading in AI Through Our Platform Approach

Palo Alto Networks has announced powerful copilot capabilities to revolutionize how customers respond to the latest threats across network, cloud and security operations. Powered by Precision AI, copilots leverage the largest cybersecurity dataset in the world among pure-play cybersecurity leaders. They simplify security by delivering rich insight paired with the extremely accurate security outcomes. New copilots present a powerful addition to Palo Alto Networks' extensive AI capabilities. This translates into direct operational advantages for our customers including a reduction in the time required to perform key management tasks, faster answers to security questions, and ultimately a reduction in mean time to respond (MTTR).

Paul Kaspian is a principal product marketing manager focusing on Zero Trust and AI at Palo Alto Networks

Counter AI Attacks with AI Defense

By Joshua Costa

While artificial intelligence (AI) technology has been around for a while, there is no arguing that it has become mainstream over the last year. Whenever new technology becomes mainstream, everyone looks for ways to use it to make their lives easier at home and work. While the rapid adoption of AI technology has certainly improved how we run our businesses, it has also created new opportunities for cyber threat actors.

Adversaries are increasingly utilizing AI to launch faster, broader and more effective cyberattacks. As a result, it is crucial for organizations to respond in kind by harnessing AI in their cybersecurity defense strategies. Precision AI by Palo Alto Networks is our proprietary AI system that helps security teams trust AI outcomes by using rich data and security-specific models to automate detection, prevention and remediation.

The Use of AI in Cyberattacks

Cyber threat actors are always looking for the path of least resistance to carry out their attacks. For example, they repurpose malware and often use off-the-shelf toolkits like Cobalt Strike and Brute Ratel C4 to exploit weaknesses and take malicious actions with minimal effort. This same pattern of behavior has been observed with new AI technology. As new AI tools hit the market, threat actors are increasingly using them to automate and enhance various attack vectors.

Here are some ways cyberthreat actors are using AI:

- **Conduct Reconnaissance** – cyberattacks often start with a threat actor gathering information about their potential targets. Using AI, they can scrape publicly available information from websites, social media platforms and other online sources to gather data about an organization. This data can include personal details, affiliations, connections and other valuable information that can be used to plan and execute a cyberattack.
- **Enhance Social Engineering** – Gone are the days when you could spot a phishing email because of some grammar or spelling issues. By using generative AI chatbots, threat actors can craft highly polished phishing emails, webpages and other content to increase the probability of tricking a user. This will continue to contribute to social engineering being one of the top threat vectors[1] used in cyberattacks.
- **Develop Malicious Code** – Threat actors can use AI tools to create malware and other code, even if they don't have coding skills. Many AI tools today offer the capability of modifying or creating code by providing simple instructions or input. Threat actors can create custom scripts, develop new malware variants and continuously evolve their toolkits to avoid detection and become more effective.
- **Automated Vulnerability Exploitation** – AI can be used to automate the process of discovering and exploiting vulnerabilities in applications or systems. By leveraging machine learning techniques, threat actors can quickly identify weaknesses and launch targeted attacks at a large scale.
- **Deepfake Attacks** – AI-generated deepfake videos, images or audio recordings can be used to manipulate or deceive individuals. »

Threat actors can exploit AI technology to create convincing fake content, potentially causing reputational damage or facilitating broader cyberattacks.

- **Prompt Injection** – Generative AI tools can be vulnerable to prompt injection attacks,[2] where a threat actor is able to manipulate the output generated by the tool. By getting these tools to answer questions in an unintended way, threat actors can use prompt injection to gather sensitive information and even execute malicious code.[3]

All of these techniques enable threat actors to carry out attacks faster and more effectively. The consequences of these attacks can be severe, ranging from financial losses and data breaches to reputational damage and operational disruptions. Moreover, the rapid evolution and adaptability of AI-driven threats make them particularly challenging for traditional cybersecurity measures to combat effectively. As a result, organizations are facing an unprecedented level of risk, necessitating a proactive and adaptive approach to cybersecurity defense. They must respond in kind by leveraging AI to counter adversarial AI.

How Organizations Can Use AI to Counter Cyberattacks

To effectively counter AI-driven cyberattacks, organizations must harness the capabilities of AI for their cybersecurity defense strategies. Implementing AI-powered security tools and strategies is a crucial aspect of countering cyberattacks.

There are some key ways organizations can leverage AI in their cybersecurity programs:

- **Threat Detection & Analysis** – One key area where AI can make a substantial impact is with threat detection and analysis. AI-powered security tools can analyze vast amounts of data in real time, enabling the rapid identification of anomalous activities and potential security incidents. By leveraging machine learning algorithms, organizations can detect patterns indicative of cyberthreats and take proactive measures to mitigate risks. These tools can provide real-time response capabilities, automatically adapting their defenses to emerging threats.
- **Automated Security Operations** – AI-powered security tools can automate security tasks, such as onboarding data sources, stitching disparate alerts and enriching security details. AI can also assist in automating incident response actions by rapidly analyzing and correlating security events, identifying the extent of the incident, and suggesting appropriate response actions. This reduces the burden on security teams, improves efficiency and allows them to focus on more complex and strategic security issues. High-fidelity automation can speed up mean time to detect (MTTD) and mean time to respond (MTTR), reducing the impact of cyberattacks and minimizing vulnerability windows.
- **Threat Intelligence Analysis** – Proactive threat intelligence and predictive analytics are essential components of a cybersecurity strategy. AI can analyze diverse security data sources in real-time to identify emerging threats and anticipate potential attack vectors. This may include leveraging adversarial AI techniques to generate and learn about attacks, so that defenses can be continuously improved. By leveraging AI for proactive defense, organizations can stay one step ahead of adversaries and mitigate risks before they turn into full-blown attacks.

Implementing these strategies today will strengthen an organization's ability to effectively detect and stop cyberattacks.

Future Trends and Recommendations

Looking ahead, the role of AI in cyberattacks and defense is expected to grow even further. Threat actors will continue to refine their AI-driven attack techniques, demanding constant innovation in cybersecurity strategies. To stay ahead of AI-driven threats, organizations should prioritize the following recommendations:

- **Invest in AI-powered cybersecurity solutions**: Organizations should allocate resources to implement AI-powered defense systems that can adapt to evolving threats in real time.
- **Collaborate and share threat intelligence**: Sharing threat intelligence with industry peers and security communities can enhance collective defense against AI-driven attacks. »

- **Foster a culture of cybersecurity awareness**: Educating employees about the risks and best practices related to AI-driven cyberattacks can strengthen the organization's overall security posture.
- **Stay updated with evolving AI technologies**: Organizations should remain informed about emerging AI technologies and their potential applications in both offensive and defensive cybersecurity efforts.

Harnessing AI Against Cyberthreats

In the ever-evolving landscape of cybersecurity, organizations must acknowledge the increasing use of AI by adversaries in cyberattacks. Harnessing AI for defense is no longer an option but a necessity to protect sensitive data, systems and infrastructure.

By leveraging AI for threat detection, implementing AI-powered defense systems and adopting proactive threat intelligence, organizations can strengthen their cybersecurity defenses and stay resilient against AI-driven attacks. Embracing AI in the cybersecurity landscape is not just about keeping up with adversaries; it is about staying one step ahead in the battle against cyberthreats.

1. Unit 42. "2024 Unit 42 Incident Response Report: Navigating the Shift in Cybersecurity Threat Tactics." *Palo Alto Networks*, 20 February 2024.
2. Burgess, Matt. "Generative AI's Biggest Security Flaw Is Not Easy to Fix." *Wired*, 6 September 2023.
3. Harang, Rich. "Securing LLM Systems Against Prompt Injection." *NVIDIA*, 3 August 2023.

Joshua Costa is the product marketing director for Cortex at Palo Alto Networks

The Dark Side of AI in Cybersecurity — AI-Generated Malware

By Dena De Angelo

As artificial intelligence (AI) continues to evolve at an unprecedented pace, its impact on the cybersecurity landscape is becoming increasingly apparent. While AI has the potential to revolutionize threat detection and defense strategies, it can also be exploited by malicious actors to create more sophisticated and evasive threats. In a thought-provoking interview on the Threat Vector podcast, Palo Alto Networks researchers, Bar Matalon and Rem Dudas, shed light on their groundbreaking research into AI-generated malware and their predictions for the future of AI in cybersecurity.

Unraveling the Complexity of AI-Generated Malware

When asked about the possibility of AI generating malware, Dudas responded unequivocally, stating, "The answer is yes. And there is a bit of a longer version for that answer. It's a lot more complex than it seems at first." The researchers embarked on a journey to generate malware samples based on MITRE ATT&CK techniques, and while the initial results were lackluster, they persevered and eventually generated samples that were both sophisticated and alarming. Dudas explains their process further:

"The main stage after the basic tinkering with the AI models was trying to generate malware samples that perform specific tasks based on MITRE techniques. If you're familiar with those, for example, we would »

like to generate a sample that does credential gathering from Chromium browsers. So, we tried generating those, and for each technique that we found interesting, we tried generating a specific sample. We did that for different operating systems – for Windows, macOS and Linux. And, we tested all of those samples against our product [Cortex], as well. That was the first stage I'd say."

Impersonation and Psychological Warfare

One of the most disconcerting discoveries made by the researchers was the ability of AI models to impersonate specific threat actors and malware families with uncanny accuracy. By providing the AI with open-source materials, such as articles analyzing malware campaigns, the researchers were able to generate malware that closely resembled known threats, like the Bumblebee web shell.[1]

Dudas predicts that "Impersonation and psychological warfare will be a big thing in the coming years," He cautions:

"...if you've tried asking generative AI to write a letter like Jane Austen would, the results are scary. Similarly, threat actors can impersonate others and plant false flags for researchers to uncover. I mean, that's purely speculative at this point, but imagine a nation actor with ill intent using psychological warfare, mimicking another nation's arsenal, kit or malware and planting false flags, trying to make it look as if another country or another threat actor made a specific attack. It opens the door for a lot of nasty business and makes attribution and detection pretty difficult for the defending side."

The Perils of Polymorphic Malware

Another alarming trend highlighted by the researchers is the potential for AI to generate a vast array of malware variants with similar functionalities and overwhelming security professionals. Dudas warns, "Polymorphic malware – giving LLMs snippets of malware source code – could lead to a staggering amount of slightly different samples with similar functionalities that will overwhelm researchers."

This proliferation of polymorphic malware, combined with the increasing sophistication of AI-generated threats, could render traditional signature-based detection methods obsolete. As Dudas puts it, "Signature-based engines are dying. Detecting malware based on specific strings or other identifiers is already too wide a net. With the addition of polymorphy and automatically generated malware, this net could be torn completely."

Key characteristics of polymorphic malware include:

- **Mutation** – The malware automatically modifies its code each time it replicates or infects a new system, making it difficult for signature-based detection methods to identify it.
- **Encryption** – Polymorphic malware often uses encryption to hide its payload, further complicating detection and analysis.
- **Obfuscation** – The malware employs various techniques to conceal its true functionality, such as dead code insertion, register renaming and instruction substitution.
- **Functionality Preservation** – Despite the constant changes in its code, polymorphic malware retains its original malicious functionality.
- **Harder to Detect and Analyze** – Due to its changing nature, polymorphic malware is more challenging for antivirus software to detect and for security researchers to analyze and understand.

The Evolution of Phishing and Scamming

Dudas also foresees a significant transformation in the area of phishing and scamming, due to the advanced natural language capabilities of large language models (LLMs). He explains:

"Since LLMs usually sound so natural to end users, I'd say the field of phishing and scamming will undergo the biggest alteration. For example, weird grammar, a sense of urgency and pressure, as well as spelling errors are the easiest ways to recognize a phishing email. With LLMs, these telltale signs are a thing of the past. You could generate an entire convincing campaign from scratch in no time with a basic understanding of what makes people tick, even if you do not speak the language."

AI algorithms can analyze vast amounts of publicly available data to create highly personalized phishing emails, tailored to specific »

individuals, increasing the likelihood of the recipient falling for the scam. AI-powered natural language generation (NLG) can create convincing and contextually relevant phishing emails that mimic human writing styles, complete with proper grammar and tone, making it harder for recipients to identify them as fraudulent.

Likewise, AI-driven chatbots and voice synthesis can be used to create realistic conversational interactions, tricking victims into divulging sensitive information or performing actions that benefit the scammer. Deepfakes, generated by AI, can produce fake audio and video content, such as impersonating a company executive or creating a false sense of urgency to manipulate victims into complying with the scammer's demands. AI can also analyze data on user behavior, such as when they are most likely to open and respond to emails, allowing scammers to optimize the timing and targeting of their phishing campaigns for maximum impact.

Fortifying Defenses Against AI-Generated Malware

To combat the rising threat of AI-generated malware, Bar Matalon advises investing in cutting-edge tools that employ dynamic detections and behavioral rules, such as Palo Alto Networks Cortex XDR or Cortex XSIAM. He emphasizes, "I think one of the best practices for organizations is to invest in advanced tools that leverage dynamic detections and behavior rules to detect all these new threats and stop them."

These AI-powered systems can identify and neutralize novel threats by analyzing program behaviors and connections in real-time. Matalon predicts, "Security tools will increasingly leverage AI to dynamically identify new threats and stop them," highlighting the critical role AI will play in bolstering cybersecurity defenses.

The Shifting Landscape of Cybersecurity

As AI becomes more ubiquitous, the cybersecurity landscape is poised for significant disruption. Matalon cautions, "AI will help people with less technical knowledge become cyberthreats, lowering the barriers for more threat actors to join." He further predicts, "AI will be used to create lots of new types of malware, flooding the digital world with different threats," and "...threat actors will use AI to automate their work and be much more effective." This will lead to an increase in the volume and sophistication of attacks. Moreover, Matalon warns, "It would be much harder for researchers to attribute an attack to the threat actor behind it, since it would be possible to mimic another actor's tools and TTPs."

The Promise of AI in Threat Detection

Despite the daunting challenges posed by AI-generated malware, Dudas believes that AI will also play a pivotal role in enhancing threat detection capabilities. He envisions a future where "'Cybersecurity researchers' models that have been trained on content and material related to threat research... will be able to perform the same analysis tasks as researchers and will yield quality results in much shorter time frames."

This application of AI could potentially level the playing field and empower cybersecurity professionals to stay ahead of the security curve.

The insightful research conducted by Bar Matalon and Rem Dudas serves as a clarion call for the cybersecurity community. As we navigate the uncharted waters of an AI-driven threat landscape, it is imperative that we remain vigilant, adaptable and proactive in our approach to defense. By harnessing the power of AI in our own security tools and strategies, we can fortify our defenses and stay one step ahead of the malicious actors seeking to exploit this transformative technology. As Matalon aptly puts it, "Maybe that's the way we'll do that in the future – that the best solution for a bad person with an AI model is the good person with an AI model. Right?"

1. Falcone, Robert. "xHunt Campaign: New BumbleBee Webshell and SSH Tunnels Used for Lateral Movement." Unit 42 Blog, *Palo Alto Networks*, 11 January 2021.

Dena De Angelo is a content marketing manager at Palo Alto Networks

Click the QR code above to get your Unit 42® AI Security Assessment

AI in Cyber Is Here to Stay — How to Weather This Sea Change

By Dena De Angelo

In this article, we interviewed Jon Huebner, an extended expertise engineer and consultant for Cortex XSIAM® at Palo Alto Networks, who shared his insights and predictions on the impact of AI in this domain.

Foreseeing a Shifting Job Market and Workflows

One of Huebner's top predictions is that AI will massively affect the job market and how developers and engineers work, especially within enterprises. As AI becomes more integrated into cybersecurity tools and processes, it will likely lead to significant shifts in the way cybersecurity practitioners operate. Huebner elaborates further:

"It's also going to affect the security of enterprises, of how people use them, how people share their data. Both good and bad ways. It's going to affect productivity in a massive way. A lot of these cloud services will also go through some changes because a lot of that compute power needs to be purchased. It needs to run on a lot of resources. It gets warm, it's a great space heater, and then it's also going to start to impact if companies are hosting their own local LLMs for security, for fine-tuning reasons, and how they're going to be training their own models."

One of the primary ways AI is projected to transform cybersecurity is by automating many of the repetitive and time-consuming tasks currently performed by humans. This includes tasks, such as log analysis and incident response. By automating these tasks, AI will allow cybersecurity practitioners to focus on more strategic and complex issues, such as developing new security architectures and forensic investigations.

ISC² or the International Information System Security Certification Consortium (a non-profit organization that specializes in training and certifications for cybersecurity professionals) surveyed cybersecurity professionals worldwide to understand the impact of emerging technologies, including AI, on their roles and responsibilities.

Their Cybersecurity Workforce Study, 2022[1] found that while AI is seen as a valuable tool for improving cybersecurity, many professionals are concerned about the potential for AI to be used maliciously and the need for new skills and knowledge to work effectively with these systems. They will need to understand how AI systems work, how to interpret their outputs, and how to ensure that they are operating effectively and ethically. This may require cybersecurity professionals to develop expertise in other areas, such as machine learning, data science and ethics, as the technology matures.

Another potential shift in job roles and responsibilities may occur as AI takes over certain tasks, freeing up cybersecurity professionals to focus on more strategic initiatives. For example, as AI improves in its ability to detect and respond to threats, cybersecurity analysts may spend more time on proactive measures, such as threat hunting and risk assessment.

Huebner also highlighted the potential implications of AI on enterprise security and data sharing practices, noting, "It's also going to »

affect the security of enterprises, of how people use them, how people share their data. Both good and bad ways." The integration of AI into cybersecurity systems could enhance security measures, but it also opens up new avenues for potential misuse and vulnerabilities:

- **AI-Powered Cyberattacks**
  - Adversarial AI can be used to automate and scale cyberattacks, making them more difficult to detect and defend against.
  - Attackers can leverage AI to identify and exploit vulnerabilities in systems and networks more efficiently.
  - AI-generated phishing emails and social engineering attacks can be more convincing and harder for humans and traditional security systems to identify.
- **Poisoning and Evasion of AI Models**
  - Attackers can manipulate the training data of AI models, leading to incorrect classifications or behaviors (data poisoning attacks).
  - Adversarial examples can be crafted to deceive AI models and evade detection, compromising the integrity of AI-based security systems.
- **Lack of Transparency and Explainability**
  - The opaque nature of some AI models, particularly deep learning systems, can make it difficult to understand how they arrive at decisions, leading to potential biases or errors that could be exploited.
  - The lack of explainability in AI-driven security systems can make it challenging to audit and trust their decisions.
- **Insider Threats and Misuse of AI Tools**
  - Insiders with access to AI-powered security tools could misuse them for malicious purposes, such as espionage, sabotage or data theft.
  - Insider knowledge of AI systems could be used to manipulate or bypass security measures.
- **Privacy and Data Protection Concerns**
  - AI-driven security systems often require vast amounts of data for training and operation, raising concerns about data privacy and potential breaches.
  - The collection and storage of sensitive data for AI-based security could create new targets for attackers.
- **Over Reliance on AI and Automation**
  - Organizations may become overly dependent on AI-driven security solutions, leading to a false sense of security and potentially overlooking human expertise and intuition.
  - Over reliance on automation could lead to delayed or ineffective responses to novel or complex threats that require human intervention.

To mitigate these risks, it is crucial for organizations to adopt a holistic approach to AI-driven cybersecurity. This includes rigorous testing and validation of AI models, regular audits and updates, as well as maintaining human oversight and intervention capabilities. Transparency, explainability and ethical considerations should be prioritized in the development and deployment of AI-based security systems.

LLMs Can Do Some Heavy Lifting

Productivity is another area where Huebner expects AI to have a profound impact. He predicts, "Productivity is going to improve as these LLMs help out." Large language models[2] (LLMs) and other AI technologies are poised to streamline processes, augment human capabilities, and boost overall productivity in various sectors, including cybersecurity.

Large language models (LLMs) are becoming increasingly valuable tools for cybersecurity professionals, particularly in the context of incident response. When a cyberattack occurs, defenders often face the challenge of quickly piecing together information from various sources to understand the scope and nature of the threat. LLMs can greatly assist in this process by rapidly analyzing vast amounts of data, such as system logs, network traffic and threat intelligence feeds.

These AI-powered models can identify relevant patterns, anomalies and indicators of compromise, providing defenders with a clearer picture of the ongoing attack. Moreover, LLMs can translate complex technical data into plain language summaries, making it easier for incident responders to communicate findings and coordinate their efforts effectively. »

The Impact of AI on Cloud Computing Infrastructure and Services

Further in the conversation, Huebner touched upon the impact of AI on cloud services, stating, "A lot of those cloud services will also go through some changes because a lot of those compute power that needs to be purchased. It needs to run."

The increasing demand for computational resources to power AI models and systems could drive changes in cloud service offerings and pricing models. As AI becomes more integral to various industries and applications, the need for robust, scalable and cost-effective computing infrastructure will continue to grow. To meet this demand, cloud service providers are likely to develop more specialized AI-focused offerings:

- **AI-Optimized Hardware** – Cloud providers may invest in hardware specifically designed to accelerate AI workloads, such as GPUs, TPUs and FPGAs, to provide better performance and efficiency for AI models.
- **Pre-Trained Models and AI Services** – Providers may offer a wider range of pretrained AI models and APIs, allowing businesses to easily integrate AI capabilities into their applications without the need for extensive in-house expertise or infrastructure.
- **Hybrid and Edge Computing Solutions** – To address latency and data privacy concerns, cloud providers may expand their hybrid and edge computing offerings, enabling AI workloads to be processed closer to the data source.
- **Flexible Pricing Models** – As AI workloads can be computationally intensive and vary in resource requirements, cloud providers may introduce more flexible and granular pricing models, such as serverless computing and pay-per-use options, to help businesses optimize costs based on their specific needs.
- **Collaboration and Data Sharing Platforms** – Cloud providers may develop secure platforms that facilitate collaboration and data sharing among organizations, researchers and developers working on AI projects, fostering innovation and accelerating progress in the field.

Enhancing the Detection of Custom Attack Prevention and Ensuring Responsible Implementation

Addressing the application of AI in cybersecurity, Huebner acknowledged the limitations of current approaches: "A lot of people want it to be that magic black box that is just going to spit out, 'Hey, this is an alert based off of these log sources, but I don't think that's fully accurate at this time.'" He emphasized that AI is currently focused on grouping and finding similarities between security events, optimizing analyst workflows, and reducing workloads.

Looking ahead, Huebner envisioned AI enabling better detections and more customized solutions. "As we get more data, as we find more use cases for these AIs and LLMs, we're going to start to find new ways for cybersecurity to take off," he predicted. When it comes to specific threats, Huebner believes AI-powered systems will be particularly effective at detecting and preventing tailored and custom attacks. He explains:

"I think a lot of them are going to be more tailored and custom attacks. We're seeing a lot more attackers using AIs, but defensively, these systems are able to detect when it's a more custom attack, and flag it and raise the severity, and make sure it's more seen and more visible, and handled accordingly."

Spy Vs. Spy

Huebner also acknowledged the possibility of AI being used by attackers against one another, creating a "battle" for control and stealing code, stating:

"We've actually seen some of that just starting already as well. Some of these codes are kind of... poisoning other models. They're poisoning other attackers. They're trying to ensure that they're the only ones that create, generate and use the code that they create, and then poison everyone else's model. So they're getting something different."

To protect AI models from adversarial attacks and evasion techniques, Huebner underscored the importance of a robust security posture and defense-in-depth approach:

"Having the right security, the right security posture and then defense in depth – it's pretty much a lot of those products are out there in the security market. A lot of the security is there. It's really doing that security in depth and having a solid cybersecurity group or team on your side that understands what these attacks could be." »

Huebner also discussed key performance metrics for evaluating the effectiveness of AI-powered security solutions, highlighting mean time to respond (MTTR) and the duration of open incidents as crucial factors. He stresses the importance of measuring analyst productivity, false positives and wasted time, noting that these metrics may vary across organizations due to specific nuances and workflows.

Lastly, Huebner stressed the significance of proper training and engineering processes to ensure AI models are implemented responsibly and transparently in security systems: "I believe a lot of this is going to come down to training and your engineering team; how they're building their things and how they're doing it. It's coming and it would really need to be a process and workflow that's built from the ground up." He emphasized the need for rigorous data verification, tailored models and well-defined processes.

In conclusion, Jon's predictions and insights underscore the transformative potential of AI in cybersecurity, while also highlighting the challenges and considerations that security practitioners must address. As AI continues to advance, staying vigilant, adapting defenses and fostering responsible implementation will be paramount in navigating the evolving threat landscape.

1. "Revealing New Opportunities for the Cybersecurity Workforce." *ISC2*, 2022.
2. Tannenbaum, Yitzy. "AI, Cybersecurity and the Rise of Large Language Models." *Palo Alto Networks*, 2 April 2024.

Dena De Angelo is a content marketing manager at Palo Alto Networks

Three Principles of Data Security in the AI Era

By Dan Benjamin

AI hype and adoption is seemingly at an all-time high with nearly 70% of respondents to a recent S&P report on Global AI Trends[1] saying they have at least one AI project in production. While the promise of AI can fundamentally reshape business operations, it has also created new risk vectors and opened the doors to nefarious individuals that most enterprises are not currently equipped to mitigate.

In the last 6 months, three reports (S&P Global's 2023 Global Trends in AI report,[2] Foundry's 2023 AI Priorities Study,[3] and Forrester's report Security And Privacy Concerns Are The Biggest Barriers To Adopting Generative AI[4]) all had the same findings: data security is the top challenge and barrier for organizations looking to adopt and implement generative AI. The surging interest in implementing AI has directly increased the volume of data that organizations store across their cloud environments. Unsurprisingly, the more data that is stored, accessed and processed across different cloud architectures that typically also span different geographic jurisdictions, the more security and privacy risks arise. »

If organizations don't have the right protections in place, they instantly become a prime target for cybercriminals which according to a Unit 42 2024 Incident Response Report[5] are increasing the speed at which they steal data with 45% of attackers exfiltrating data in less than a day after compromise. As we enter this new "AI era" where data is the lifeblood, the organizations that understand and prioritize data security will be in pole position to safely pursue all that AI has to offer without fear of future ramifications.

> **While the promise of AI can fundamentally reshape business operations, it has also created new risk vectors and opened the doors to nefarious individuals that most enterprises are not currently equipped to mitigate.**

Developing the Foundation for an Effective Data Security Program

An effective data security program for this new AI era can be broken down into three principles:

Securing the AI: All AI deployments – including data, pipelines, and model output – cannot be secured in isolation. Security programs need to account for the context in which AI systems are used and their impact on sensitive data exposure, effective access, and regulatory compliance.

Securing the AI model itself means identifying model risks, over permissive access and data flow violations throughout the AI pipeline.

Securing from AI: Just like most new technologies, artificial intelligence is a double-edged sword. Cyber criminals are increasingly turning to AI to generate and execute attacks at scale. Attackers are currently leveraging generative AI to create malicious software,[6] draft convincing phishing emails and spread disinformation online via deep fakes. There's also the possibility that attackers could compromise generative AI tools and large language models themselves. This could lead to data leakage, or perhaps poisoned results from impacted tools.

Securing with AI: How can AI become an integral part of your defense strategy? Embracing the technology for defense opens possibilities for defenders to anticipate, track, and thwart cyberattacks to an unprecedented degree. AI offers a streamlined way to sift through threats and prioritize which ones are most critical, saving security analysts countless hours. AI is also particularly effective at pattern recognition, meaning threats that follow repetitive attack chains (such as ransomware) could be stopped earlier.

By focusing on these three data security disciplines, organizations can confidently explore and innovate with AI without fear that they've opened the company up to risks.

1. Patience, Nick, and David Immerman. "2023 Global Trends in AI Report." *WEKA*, August 2023.
2. Ibid.
3. "2023 AI Priorities Study." *Foundry*, an IDG, Inc. Company, 2023.
4. Pollard, Jeff, et al. "Security And Privacy Concerns Are The Biggest Barriers To Adopting Generative AI." *Forrester*, 5 December 2023.
5. Unit 42. "Incident Response Report 2024." *Palo Alto Networks*, 2024.
6. Satter, Raphael. "Exclusive: AI being used for hacking and misinformation, top Canadian cyber official says." *Reuters*, 20 July 2023.

Dan Benjamin is a senior director of product management at Palo Alto Networks

AI Powers Sabre's Enhanced Threat Detection & Response

By Dena De Angelo

Precision AI™ by Palo Alto Networks Elevates Security Posture

As the cyberthreat landscape continues to evolve at an unprecedented pace, security teams are turning to artificial intelligence (AI) to bolster their defense capabilities. According to research from Deloitte,[1] the market for AI-powered cybersecurity solutions is projected to reach a staggering $102.78 billion by the year 2032, underscoring the widespread embrace and integration of AI technologies across the cybersecurity landscape.

Scott Moser, CISO at Sabre, a leading software technology company for the travel industry, shares his insights on how AI is transforming cybersecurity at his organization.

Sabre, headquartered in Texas, is the largest global distribution systems provider for air bookings and offers more than 200 hundred software products that enable the entire travel ecosystem from reservations and revenue optimization to delivery. Moser joined Sabre in 2019 to lead the company in modernizing its security tooling, focused on solving the complexity of a multi-vendor security environment with uncontrolled spending.

The Disruptive Potential of Generative AI

Moser acknowledges that, "AI is one of those fundamental technology changes that occurs in our lifetime that can rapidly alter how we live and how we conduct business." While some security leaders initially focused on governance concerns around AI usage, "those conversations have changed and deepened over time," to explore how generative AI can enhance security solutions.

However, the rise of generative AI also introduces new risks. Moser cautions, "Companies today are facing many significant and emerging threats against generative AI." He highlights the importance of, "appropriate control and understanding of where that data came from and how the data is being used," when training AI models and crafting prompts.

Despite the challenges, Moser firmly believes:

"AI actually creates an advantage for businesses and security companies. Ultimately, the use of AI is allowing us »

to respond faster to threats, to determine what those threats are, and then define remediation to any attacks that occur to us."

At Sabre, AI plays a pivotal role in enhancing security operations. Moser states, "We're using AI in our security solutions, both in solutions that we acquire from our partners, such as Palo Alto Networks, and also in solutions that we create ourselves that are able to do functions faster than we ever were able to do them before."

Addressing the Talent Gap with Natural Language Processing

One significant hurdle security teams face is ensuring they have adequate staffing to effectively utilize the plethora of security tools at their disposal. According to a 2022 research study by Palo Alto Networks,[2] 77% of security leaders want to reduce the number of security vendors and tools they rely on. In the same report, 41% of global organizations work with 10 or more cybersecurity vendors, with vendors using almost 32 security tools/solutions on average.

Moser sees AI as a potential solution, noting, "The ability for more team members to query firewalls and all of the security tools using natural language interface is extremely valuable in ensuring very quick response to security threats as well as getting better answers to the questions they ask."

Comprehensive Visibility and Control

As organizations increasingly adopt AI, Moser stresses the importance of implementing comprehensive visibility and control measures. This is because data can flow bi-directionally, with internal employees accessing external AI tools and external customers or partners accessing the company's internal AI tools. This two-way data flow creates potential security risks that must be addressed through proper monitoring and access controls. Moser stresses, "First of all, the ability to identify what generative AI is in use by the employees of our company is critically important. Secondly, the deployment of security policies surrounding the access and use of those generative AI technologies will be extremely important."

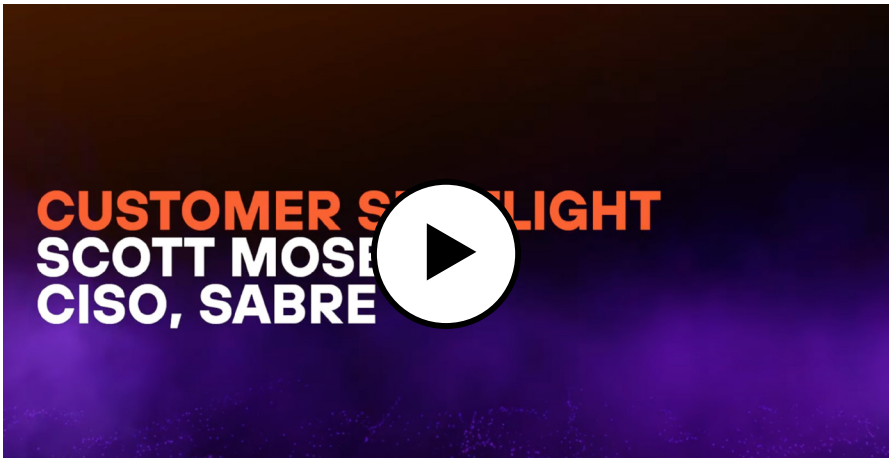
Moreover, Moser underscores the importance of actively detecting and preventing threats targeting an organization's own AI implementations, stating, "Perhaps most important though is the ability to detect and to prevent threats against our own use of generative AI in our environment."

> **Recently, Palo Alto Networks announced Precision AI, the proprietary AI system that helps security teams trust AI outcomes by using rich data and security-specific models to automate detection, prevention and remediation.**

Precision AI Technology in the Security Operations Center (SOC)

With Cortex XDR's cloud-delivered architecture and lightweight agent, Sabre rapidly rolled out the solution to thousands of endpoints across their environment. Once deployed, Cortex XDR ingested data from across the organization to begin looking for attack behavior. Utilizing Precision AI technology, Cortex XDR applies machine learning models precisely tuned to detect malicious activity, uncovering threats within Sabre's specific environment and providing prioritized, actionable alerts and context. He explains further:

"Most recently, we deployed Cortex XDR replacing our previous endpoint security solution. That was by far the fastest deployment of any security tool that we've had over many years. Achieving 85% deployment in only a matter of three months over an environment of almost 40,000 endpoints. The partnership and the assistance »



that we've gained from Palo Alto Networks has significantly improved the maturity of our security program across the board.

As security leaders, we understand that the speed and complexity of attacks will continue to increase each and every year. We know that it's critically important that the security solutions we put in place are tightly integrated with security orchestration and automation tools. And so the use of this automation is our way of staying ahead of attackers to be able to detect, respond and mitigate the threats against us."

He highlights the pivotal role by Palo Alto Networks in enhancing Sabre's security maturity, stating, "Palo Alto Networks has helped us continually mature our own security program over time, and at the same time to reduce the impact of security threats that we face."

Embracing Automation and Integration

As the speed and complexity of cyberattacks intensify, Moser emphasizes the criticality of tightly integrating security solutions with orchestration and automation tools. He declares:

"We understand that the speed and complexity of attacks will continue to increase each and every year. We know that it's critically important that the security solutions we put in place are tightly integrated with security orchestration and automation tools."

While machine learning and automation will certainly enhance outcomes, such as response times, accuracy and remediation, especially for repetitive tasks, attracting, training and retaining skilled security personnel (including engineers, analysts and architects) must be an integral part of any comprehensive security strategy. By leveraging automation technologies, organizations can optimize their efforts in protecting the business.

The Future Looks Bright

Under Moser's leadership, Sabre has seen reduced and controlled expenditures, decreased complexity through platformization, and achieved heightened alignment across the organization. The comprehensive and effective security posture of Sabre today is a testament to his dedication and expertise in the field.

Moser concludes with a powerful statement:

"The use of this automation is our way of staying ahead of attackers to be able to detect, respond, and mitigate the threats against us. And, combined with Cortex XDR's Precision AI, we have the added power of machine learning, deep learning and generative AI to ensure real-time security for even greater, more efficient security outcomes."

In the ever-evolving cybersecurity battleground, AI emerges as a game-changing force, empowering organizations to enhance their defenses, accelerate threat detection and response, and fortify their overall security posture. As trailblazers like Sabre embrace the power of AI, they pave the way for a future where human ingenuity and artificial intelligence converge to safeguard digital frontiers.

1. Charife, Tamer, and Michael Mossad. "AI in cybersecurity: A double-edged sword." *Deloitte*, 2023.
2. "What's Next in Cyber, A Global Executive Pulse Check." *Palo Alto Networks*, December 2022.

Dena De Angelo is a content marketing manager at Palo Alto Networks

Today's Attack Trends — Unit 42 Incident Response Report

By Wendi Whitmore

Each year, Unit 42 Incident Response and Threat Intelligence teams help hundreds of organizations assess, respond and recover from cyberattacks. Along the way, we collect data about these incidents.

Our 2024 Unit 42 Incident Response Report[1] will help you understand the threats that matter. It's based on real incident data and our security consultants' experience.

Read the report to learn how to safeguard your organization's assets and operations:

- Threat actors, their methods and their targets.
- Statistics and data about the incidents our team worked on.
- A spotlight on the Muddled Libra threat group – one of the most damaging ransomware groups today.
- How artificial intelligence affects cybersecurity now and in the future.
- In-depth recommendations for leaders and defenders.

As an executive responsible for safeguarding your organization, you'll find analysis and recommendations to help you make strategic decisions about where to invest your time, resources and budget.

Use the following takeaways to start a conversation with your leadership team and encourage them to download the 2024 Unit 42 Incident Response Report to review the expert analysis in full.

Key Takeaway — Speed Is Critical

Speed matters. Attackers are acting faster, not only at identifying vulnerabilities to exploit, but also stealing data after they do:

- In 2023, the median time from compromise to data exfiltration fell to just two days, which is much faster than the nine days we observed in 2021.
- In approximately 45% of cases this year, attackers exfiltrated data within a day of compromise.
- For non-extortion-related incidents in 2022 and 2023, the median time to data exfiltration has consistently remained under one day, meaning defenders must react to a ransom attack in less than 24 hours.

Attacker "dwell time" (the duration between when an attacker was detected and the earliest evidence of their presence) has also accelerated. The median dwell time was just 13 days in 2023 – half of what it was in 2021.

But, that's not necessarily a bad thing. Other data in our report indicates it may be that defenders are improving. »

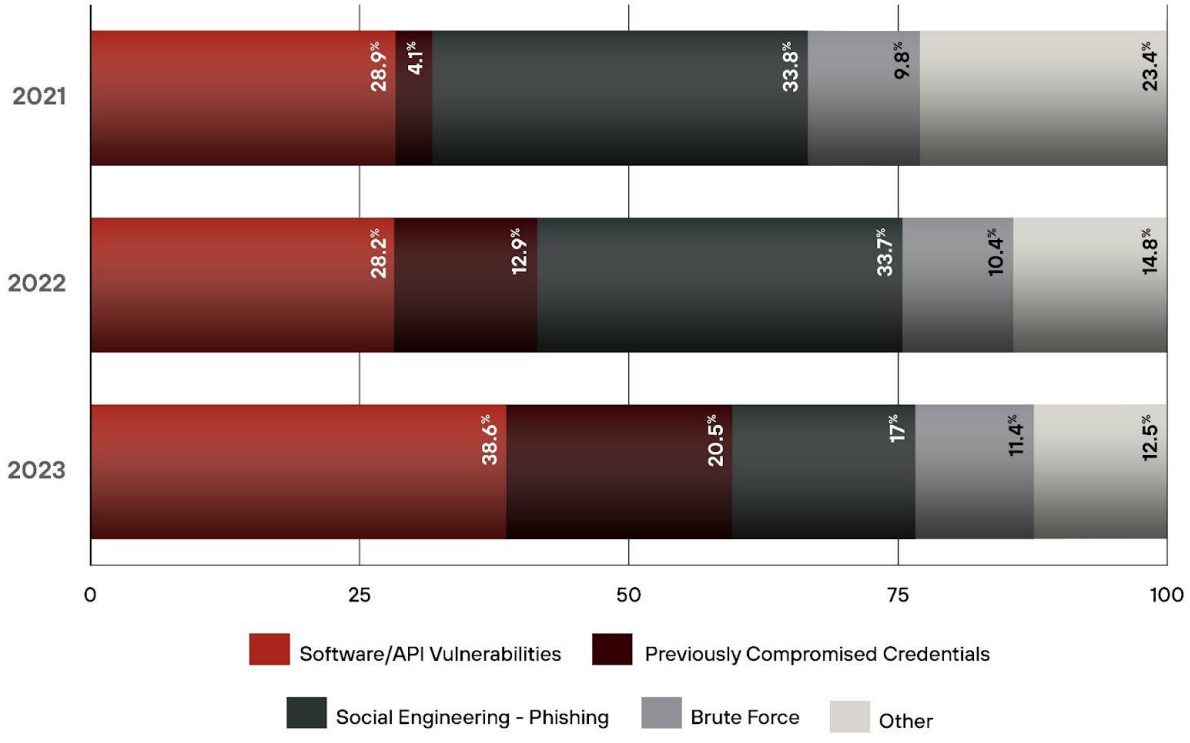


Figure 1: Initial access vectors per year, from 2021 through 2023

Key Takeaway – Software Vulnerabilities Remain Important

In 2023, attackers used internet-facing vulnerabilities to get into systems more often. This tactic occurred in 38.6% of our IR cases, making it the leading method of initial access.

Vulnerability exploitation surpassed phishing as the leading initial access method. Exploiting weaknesses in web applications and internet-facing software played a significant role in some of the largest and most automated cyberattacks.

This change emphasizes the importance of good patching practices and attack surface reduction. While that work can be challenging for large organizations to implement comprehensively, organizations must act swiftly and use multiple layers of defense to protect themselves. If you don't find and fix the exposure, attackers will.

Key Takeaway – Threat Actors Continue to Use Sophisticated Approaches

Cyberthreat actors are adopting sophisticated strategies, organizing into specialized teams and effectively leveraging IT, cloud and security tools. They've become more efficient, defining and repeating processes for quicker results.

Attackers are now using defenders' own security tools against them, compromising highly privileged accounts and infrastructure to access tools and move within their target network. Vigilance and proactive defense are crucial as threat actors adapt and innovate.

Five Recommendations to Better Protect Your Organization from Cyberthreats in 2024

Here are five key recommendations from our cybersecurity consultants to enhance your cybersecurity posture based on our insights from 2023's cyber incidents:

1. **Improve Organizational Visibility**: Prioritize comprehensive visibility across your network, cloud and endpoints. Actively monitor unmonitored areas, manage vulnerabilities effectively with robust patch management and secure internet-exposed resources such as remote desktops »

and cloud workloads. Insufficient and incomprehensive visibility makes incidents more frequent and more severe.

2. **Simplify**: Streamline the complexity of cybersecurity operations by consolidating point products. Centralize and correlate security telemetry data from various sources into an analytics platform. The best strategy enhances threat detection and response efficiency with machine learning (ML) and analytics.
3. **Enforce Zero Trust Principles**: Implement a Zero Trust security strategy. Deploy robust authentication methods, network segmentation, lateral movement prevention, Layer 7 threat prevention and the principle of least privilege. Prioritize comprehensive multifactor authentication (MFA), passwordless solutions and single sign-on (SSO). Regularly audit and update authentication systems.
4. **Control Application Access**: Control application usage and eliminate implicit trust between application components. Restrict access to specific applications, especially those exploited by threat actors. Emphasize monitoring and alerting on remote management applications and unsanctioned file-hosting services.
5. **Segment Networks**: Employ network segmentation to reduce the attack surface and confine breaches to isolated zones. Implement Zero Trust network access (ZTNA) to verify users and grant access based on identity and context policies to ensure users or devices are not trusted until continuously verified.

In addition to the findings outlined here, the report spotlights current threats as well as the impact of emerging technologies, including artificial intelligence (AI) Social Engineering, Large Language Models (LLMs), DevSec and DevSecOps, as well as the continued use of cloud-based technologies.

1. Unit 42. "2024 Unit 42 Incident Response Report: Navigating the Shift in Cybersecurity Threat Tactics." *Palo Alto Networks*, 20 February 2024.

Wendi Whitmore is SVP of Unit 42 at Palo Alto Networks

Download the complete 2024 Unit 42 Incident Response Report to learn more in-depth recommendations for improving your security posture and focus on the risks you need to mitigate.

paloalto NETWORKS | PRISMA CLOUD

The State of Cloud-Native Security

GenAI is changing everything. The report, which surveys over 2,800 cloud security executives and professionals, highlights eye-opening realities that organizations are facing:

64%
report a big increase in data breaches

47%
anticipate AI-driven supply chain attacks

90%
say that the number of point tools they use create blind spots

GET "THE STATE OF CLOUD-NATIVE SECURITY" 2024 REPORT

paloalto NETWORKS | STRATA

Hello, unexpected threats.

We've been expecting you.

Predict what's coming and proactively secure against it with the Zero Trust, AI-powered network security platform built to secure whatever whenever wherever.

To learn more, visit,
paloaltonetworks.com/network-security


paloalto®
NETWORKS
PREPARE FOR A BRAND-NEW FIGHT
See how Precision AI™ provides the predictive ability to protect against tomorrow's threats
WATCH ON DEMAND