StrongestLayer

Legacy Security vs. AI-Generated Threats: An Unfair Fight

How Artificial Intelligence is Reshaping the Threat Landscape and the Need for AI-Powered Defenses

“You can’t defend tomorrow’s threats with yesterday’s rules.”
-Alan LeFort (CEO)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The cybersecurity landscape is experiencing a significant transformation as artificial intelligence capabilities become increasingly accessible to threat actors. Legacy tools — built on rules, signatures, and supervised learning — can’t detect what they’ve never seen. Meanwhile, attackers are using generative AI to launch polymorphic, adaptive threats that evolve faster than traditional defenses can react.
The Result:

- Missed zero-days and AI-crafted attacks
- Overwhelmed SOC teams buried in false positives
- Outdated detection models stuck in a "look back" loop

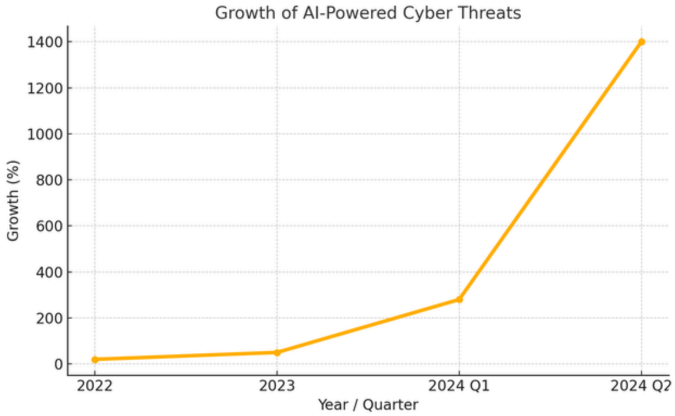
"The next breach won’t come from a known CVE. It’ll come from a novel behavior crafted in seconds by an LLM." notes from Rizwan (CTO)

StrongestLayer’s ongoing threat research has identified a concerning trend: while organizations are still implementing defenses against traditional attack vectors, adversaries are leveraging AI to develop fundamentally new approaches that bypass conventional security controls.
This thought leadership paper examines the most critical AI-enhanced threats targeting organizations today, based on our extensive threat intelligence gathering and incident response activities. By understanding how these emerging attack methodologies operate and their implications for existing security architectures, CISOs can develop more resilient defense strategies that protect their organizations in this evolving threat landscape.

Research reveals alarming trends: AI-generated phishing attacks achieving success rates of nearly 80% according to SoSafe Research, a 1400% increase in AI-powered attacks in early 2024 as reported by Biometric Update, and the emergence of sophisticated techniques like fake brand generation and polymorphic threats that can evade conventional detection methods.
These AI-enabled threats operate at unprecedented speed and scale, creating unique attacks for each target and constantly evolving to bypass signature-based defenses.

As cybercriminals leverage AI to automate and enhance their attacks, organizations must adopt AI-powered security solutions that can match this sophistication. This whitepaper provides a comprehensive analysis of the current threat landscape, detailed case studies of AI-powered attacks, and strategic guidance for implementing effective defensive measures in this new era of cybersecurity challenges.

AI-Powered Cyber Threats Growth



Source: Biometric Update Research Report, 2024

“Security teams writing rules while attackers write code with AI is the definition of an unfair fight” notes Rizwan (CTO)

INTRODUCTION: THE AI SECURITY PARADOX

The democratization of AI technologies presents a unique security paradox for organizations. On one hand, these technologies offer unprecedented opportunities to enhance security operations and threat detection capabilities. On the other, our threat intelligence team has observed a sharp increase in attacks leveraging these same technologies to evade traditional defenses.

"AI is definitely changing the landscape of threats," notes Joshua Bass (CPO).

What makes this shift particularly concerning is the growing asymmetry between attackers and defenders. StrongestLayer's analysis of recent incidents reveals that AI is reducing both the cost and technical expertise required to launch sophisticated attacks by as much as 90%, while defense costs remain relatively stable.

This creates a significant advantage for threat actors targeting organizations that may not have fully adapted their security programs to this new reality.

"AI is definitely upending a lot of how we think about protecting from threats both in terms of techniques, in terms of volume, in terms of speed," explains Rizwan (CTO).

This change is not merely incremental—it represents a fundamental shift in how cyber threats are created, deployed, and countered. The traditional cat-and-mouse game between attackers and defenders has accelerated dramatically, with AI serving as both the weapon and the shield.

Through our continuous monitoring of the threat landscape, we've identified seven evolving attack vectors that represent the most significant AI-enhanced threats to organizations. Let's examine these threats and their implications for security programs.

THE RISE OF AI-POWERED CYBER THREATS

Evolution of Cyber Threats in the AI Era

The cybersecurity landscape has undergone a dramatic transformation with the integration of artificial intelligence into attackers' arsenals. What was once a domain requiring significant technical expertise and manual effort has evolved into an environment where sophisticated attacks can be generated, deployed, and modified at machine speed with minimal human intervention.

"I think attackers have realized that they can leverage AI to do things that they couldn't do before—it was too costly or expensive to do so," notes Joshua Bass (CPO).

This fundamental shift has democratized advanced attack capabilities, making them accessible to a broader range of threat actors regardless of their technical sophistication.

Key Developments in AI-Powered Threats

- Automation at scale: AI enables attackers to automate the entire attack lifecycle
- Hyper-personalization: AI can generate highly personalized content for each target
- Rapid adaptation: AI-powered threats can evolve in real-time
- Lowered barriers to entry: AI effectively bridges the expertise gap

THE RISE OF AI-POWERED CYBER THREATS

Statistics and Research on AI-Generated Attacks

Research presents alarming statistics that highlight the growing prevalence and effectiveness of AI-powered attacks:

- SoSafe Research reveals that AI-generated phishing attacks achieve success rates of nearly 80%, with 21% of recipients clicking on malicious content
- A study from the Harvard Kennedy School and Avant Research Group found that when AI was used to craft phishing emails and profile employees, the click-through rate exceeded 50%
  In the first half of 2024, Pin Drop Security reported a staggering 1400% increase in AI-powered attacks compared to the
- According to Security Magazine and AJG Research, 85% of cybersecurity professionals believe that the increase in cyber attacks is directly attributable to generative AI use by threat actors

Economic Factors Driving Adoption by Threat Actors

The rapid adoption of AI by threat actors is driven by compelling economic incentives that fundamentally alter the cost-benefit equation of cybercrime:

AI dramatically reduces the human effort required to create convincing phishing campaigns, develop malware variants, or conduct reconnaissance, allowing attackers to operate more efficiently with fewer resources while achieving higher success rates.

KEY AI-ENABLED THREAT TECHNIQUES

AI-Generated Phishing Attacks

Phishing has long been a primary attack vector for cybercriminals, but AI has transformed this threat into something far more dangerous and difficult to detect. Traditional phishing relied on generic templates sent to thousands of recipients, hoping that a small percentage would fall victim. AI-generated phishing represents a fundamental shift in both quality and effectiveness.

Success Rates and Statistics

Research highlights alarming statistics about the effectiveness of AI-generated phishing:

- SoSafe Research shows that nearly 80% of humans open AI-generated phishing emails
- 21% of recipients click on malicious content within these emails
- Research from the Harvard Kennedy School and Avant Research Group found that when AI was used to craft phishing emails and profile employees, the click-through rate exceeded 50%

Personalization at Scale

What makes AI-generated phishing particularly dangerous is the ability to create highly personalized attacks at massive scale. As Alan Lefort (CEO) notes, "Why change the attack if you just use a different attack on every person? And that's what AI allows you to do."

KEY AI-ENABLED THREAT TECHNIQUES

Fake Brand Generation

AI tools now enable threat actors to create convincing fake brands, complete with logos, websites, and marketing materials that are nearly indistinguishable from legitimate businesses. These fake entities serve as fronts for various types of fraud, including investment scams, fake job offers, and supply chain attacks.

The sophistication of these fake brands has increased dramatically with AI, making traditional verification methods increasingly unreliable. Whereas previous fake websites contained obvious red flags like poor grammar or inconsistent design elements, AI-generated content can maintain perfect consistency across all brand touchpoints.

Polymorphic Malware Creation

AI has revolutionized malware development by enabling the creation of polymorphic threats that continuously change their code structure while maintaining their malicious functionality. This makes them extremely difficult to detect using traditional signature-based security tools.
Rizwan (CTO) explains: "AI allows attackers to create thousands of variants of the same malware, each with a unique signature but identical functionality. This overwhelms traditional security controls that rely on known signatures or patterns."

LIMITATIONS OF LEGACY SECURITY TOOLS

“Legacy systems don’t fail because they’re slow — they fail because they were never designed for the kind of threats AI makes possible” notes Rizwan (CTO).

Why Traditional Security Controls Fall Short

Legacy security tools were designed for a different era of cybersecurity—one where threats were more predictable, less sophisticated, and evolved at a much slower pace. These traditional controls typically rely on known signatures, predefined rules, and historical patterns to identify malicious activity.

While these approaches have been effective against conventional threats, they face significant limitations when confronted with AI-powered attacks that are designed specifically to evade detection:

Signature-Based Detection Limitations

Traditional antivirus and intrusion detection systems rely heavily on signatures—unique identifiers of known malicious code or behavior. AI-powered threats can generate unlimited variants with different signatures but identical functionality, rendering signature-based detection largely ineffective.

Static Rule Sets vs. Dynamic Threats

Many security controls operate based on static rule sets that define "normal" versus "suspicious" behavior. AI-powered threats can analyze these rules and adapt their behavior to appear legitimate, operating just below detection thresholds.

Volume and Velocity Challenges

Traditional security operations centers (SOCs) struggle with the sheer volume and velocity of alerts generated by modern environments. AI-powered attacks can exploit this limitation by launching numerous diversionary attacks while the primary attack proceeds unnoticed amid the noise.

LIMITATIONS OF LEGACY SECURITY TOOLS

Limited Contextual Understanding

Legacy tools often lack the contextual understanding needed to differentiate between legitimate and malicious activities that appear similar on the surface. AI-powered threats excel at mimicking legitimate behavior patterns while concealing their true intent.

The Detection Gap

The combination of these limitations creates a significant detection gap that AI-powered threats are designed to exploit. As Alan Lefort (CEO) explains: "Traditional security tools are playing a game of catch-up against threats that are constantly evolving and adapting. It's like trying to hit a moving target that changes direction unpredictably."

This detection gap is particularly concerning because it often results in longer dwell times—the period during which attackers remain undetected within a network. Longer dwell times correlate directly with more severe breach impacts and higher remediation costs.

CASE STUDIES OF AI-POWERED ATTACKS

Case Study 1: Hyper-Personalized Phishing Campaign

A multinational financial services company experienced a sophisticated phishing campaign that targeted their executive team with unprecedented precision. Unlike traditional phishing attempts, each email was uniquely crafted to match the recipient's communication style, professional interests, and recent activities.

Attack Methodology

- AI was used to analyze public information about executives from social media, company publications, and industry events
- The system generated highly personalized emails that referenced recent legitimate meetings, projects, and personal interests
- Each email contained a malicious attachment disguised as a relevant business document

Impact and Lessons

Despite robust security awareness training, three executives interacted with the malicious attachments, resulting in credential theft and unauthorized access to sensitive information. This case demonstrates how AI-generated content can overcome traditional security awareness by creating highly convincing personalized attacks.

CASE STUDIES OF AI-POWERED ATTACKS

Case Study 2: AI-Generated Deepfake Voice Fraud

A manufacturing company fell victim to a sophisticated fraud scheme involving an AI-generated deepfake of their CEO's voice. The attack targeted the company's financial controller.

Attack Methodology

- Attackers used AI to create a convincing replica of the CEO's voice based on public speeches and interviews
- The financial controller received an urgent call from the "CEO" requesting an immediate wire transfer for a confidential acquisition
- The deepfake voice accurately mimicked the CEO's speech patterns, accent, and verbal mannerisms

Impact and Lessons

The attack resulted in a fraudulent transfer of $1.7 million before it was discovered. This case highlights how AI-generated audio can bypass voice recognition security measures and exploit the human tendency to trust familiar voices, especially in high-pressure situations.

Joshua Bass (CPO) notes: "These case studies demonstrate that AI-powered attacks aren't theoretical—they're happening now, and they're succeeding against organizations with otherwise strong security programs."

AI-POWERED SECURITY SOLUTIONS

Fighting AI with AI: The New Security Paradigm

As AI-powered threats continue to evolve in sophistication and scale, organizations must adopt equally advanced defensive capabilities. The most effective approach is to leverage AI's strengths—pattern recognition, anomaly detection, and processing vast amounts of data at machine speed—to counter AI-powered attacks.

"You need to fight AI with AI," explains Alan Lefort (CEO). "Traditional security tools simply can't keep pace with threats that evolve and adapt at machine speed. Organizations need security solutions that can match this sophistication and scale."

AI-powered security solutions offer several key advantages over traditional approaches:

- Predictive capabilities: AI can identify potential threats before they materialize by recognizing subtle patterns and indicators
- Adaptive responses: AI security systems can continuously learn and evolve their detection methods as threats change

Contextual understanding: Advanced AI can consider the broader context of activities to reduce false positives while catching sophisticated attacks

KEY COMPONENTS OF AI-POWERED SECURITY

From static detection to dynamic understanding — the future of cybersecurity is autonomous, adaptive, and deeply contextual.

1. Adaptive Communication Threat Detection

Legacy email filters are blind to intent. AI-native systems analyze linguistic cues, behavioral baselines, and real-time context across communication platforms — email, Slack, Teams — to detect generative phishing, executive impersonation, and evolving BEC tactics that lack traditional indicators.

2. Behavioral Endpoint Defense

Modern threats no longer rely on files. AI-powered endpoint protection monitors process lineage, memory patterns, and execution context to detect code injection, LOLBins, and anomalous user behavior — even when no signature or hash exists.

3. Self-Learning Network Intelligence

Traditional NDR relies on human-written rules and rigid thresholds. AI-native systems continuously model your network's baseline activity — down to protocol behavior, asset roles, and flow dynamics — to surface subtle exfiltration, encrypted C2, or lateral movement with no reliance on predefined IOCs.

KEY COMPONENTS OF AI-POWERED SECURITY

4. Generative Threat Intelligence Engines

Threat actors now use AI to obfuscate payloads, scale infrastructure, and automate reconnaissance. Modern defense must respond in kind. AI-driven intelligence engines ingest vast telemetry and external signals to uncover attacker playbooks, adversarial infrastructure, and novel malware strains — even before they're weaponized. From passive feed consumption to predictive adversary modeling.

5. Cloud Identity and Access Intelligence

In a perimeterless world, cloud misconfigurations and identity abuse are top targets. AI maps identity usage patterns, access anomalies, and privilege escalation chains across SaaS, IaaS, and hybrid environments — detecting misuse in seconds, not days.

6. Autonomous SOC Co-Pilots

AI doesn't just detect — it triages, correlates, and recommends response actions. Integrated into the analyst workflow, it shortens MTTD and MTTR by automating investigation steps, reducing false positives, and highlighting the "needle in the haystack" faster than human teams ever could.

Joshua Bass (CPO) notes: "The most effective security programs we're seeing combine AI-powered tools with human expertise. The AI handles the speed, scale, and pattern recognition, while human analysts provide the strategic context and decision-making."

BEST PRACTICES FOR ORGANIZATIONS

1. Conduct a Threat-Driven Security Posture Assessment

Move beyond basic compliance audits. Conduct a zero-trust-aligned threat simulation focused on AI-generated risks:

- Test defenses against polymorphic phishing (e.g., GPT-generated BEC emails with no links/attachments).
- Evaluate how well your systems detect evasive malware (e.g., AI-written code obfuscated at runtime).
- Probe lateral movement across identity and SaaS misconfigurations — a rising vector in post-exploit stages.

Outcome:
Prioritize gaps not based on tech categories, but based on how attackers actually chain AI-powered techniques in the wild.

2. Prioritize Detection in Human-Prone Zones

Attackers use generative AI to bypass people — not just endpoints.
Your priority stack should be:

- Email Security 2.0:
- Ditch static training and signature filters. Use behavioral fingerprinting and in-workflow threat analysis to detect zero-day phishing.
- Identity Protection:
- Leverage AI to detect abnormal session behavior and access patterns across cloud identities and federated apps.
- Endpoint + Process Memory Monitoring:
- Traditional EDR is too reliant on known behaviors. Use ML models that detect execution context anomalies and DLL injection patterns — not just known bad hashes.

BEST PRACTICES FOR ORGANIZATIONS

3. Implement a Multi-Modal AI Defense Stack

Modern threats span multiple surfaces. So must your AI models.

- Cross-layer correlation engines — Stitch signal from email, identity, cloud, endpoint.
- Language models for intent detection — Filter emails or messages where tone, intent, or structure deviate from known safe patterns.
- Unsupervised anomaly detection — Monitor for baseline drift in SaaS behavior, service account activity, and internal comms.

Recommendation: Build your defense strategy assuming your attacker is using ChatGPT, Synthesia, and AutoGPT — and you're not.

4. Operationalize Human-AI Collaboration

AI isn't magic. It requires orchestration.

- Build a feedback loop between SOC and AI tooling — false positives must refine the model, not sit in ignored queues.
- Train analysts on interpreting model outputs — not just verdicts but contributing signals (e.g., which features led to the classification).
- Don't hire more SOC analysts — turn them into AI supervisors. Shift focus from chasing alerts to tuning detection logic and enriching telemetry.

BEST PRACTICES FOR ORGANIZATIONS

5. Stress-Test with AI-Driven Red Teaming

Red teams should evolve too.

- Use AI tools (e.g., WormGPT, phishing generators) to simulate real attacker capabilities.
- Launch auto-generated credential phishing across internal and external emails.
- Test prompt injection and LLM fuzzing if your apps integrate AI.

6. Rethink Metrics: Measure Detection Speed, Not Just Coverage

Legacy metrics like “number of alerts triaged” are obsolete. Track:

- Time to Detect and Mitigate (TTDM) AI-generated phishing
- % of zero-day threats blocked before user interaction
- False negative rates across unknown TTPs

CONCLUSION

You can’t defend tomorrow’s threats with yesterday’s rules.

The AI arms race is already here. Organizations that treat security as an AI-native discipline — not just a tooling update — will outpace adversaries.
The rise of AI-powered cyber threats represents a fundamental shift in the security landscape that requires organizations to reassess and transform their security programs. As we've explored throughout this whitepaper, traditional security approaches are increasingly ineffective against threats that leverage artificial intelligence to achieve unprecedented levels of sophistication, personalization, and evasion.
Joshua Bass (CPO) summarizes the challenge: "We're witnessing a step-change in threat capabilities that demands an equally significant evolution in how we approach security. Organizations that continue to rely solely on traditional defenses will find themselves increasingly vulnerable to these new classes of attacks."

Key Recommendations

Based on our research and experience helping organizations adapt to this new threat landscape, we recommend the following actions:

1. **Initiate an AI-native threat assessment** to uncover blind spots in your current defenses — including missed phishing attempts, deep impersonation tactics, and novel evasion techniques that bypass rule-based systems.
2. **Build a security roadmap rooted in attacker behavior, not compliance checklists** — prioritize adaptive, self-learning systems that can detect intent-based threats across communication, identity, and cloud environments.
3. **Replace legacy detection and manual triage** with AI-powered systems that autonomously detect, correlate, and respond to threats at machine speed — reducing analyst fatigue and exposure windows.
4. **Shift employee training from static courses to real-time, interactive guidance** — provide immediate alerts and tailored coaching within their workflows when they encounter AI-generated phishing or impersonation attempts.

THE PATH FORWARD

While the challenges posed by AI-powered threats are significant, they are not insurmountable. By taking a proactive, strategic approach to security transformation, organizations can not only defend against these advanced threats but also harness the power of AI to strengthen their security posture.

Alan Lefort (CEO) offers an optimistic perspective: "This is a pivotal moment in cybersecurity—one that presents both significant challenges and unprecedented opportunities. Organizations that successfully adapt their security programs will not only protect themselves against today's threats but will build the foundation for more resilient security in the future."

The key is to act now, before AI-powered attacks become even more sophisticated and widespread. By understanding the nature of these threats and implementing the appropriate countermeasures, organizations can navigate this new security landscape successfully.

TESTIMONIALS

“

StrongestLayer is a next Gen AI driven tool that can identify phishing email attacks that bypass the sophisticated email gateway controls in real-time and assist security operations in containing the spread of malicious content on corporate networks.

”

telenor Muphasa, CISO

ABOUT US

Our Contributors

Alan Lefort, CEO

Alan is the CEO & cofounder of StrongestLayer with extensive experience in cybersecurity leadership. Prior to founding StrongestLayer, Alan served as General Manager at McAfee and Proofpoint, giving him deep insights into enterprise security challenges and solutions. His vision drives StrongestLayer's mission to protect organizations from AI-powered threats.

Joshua Bass, CPO

Joshua is the Chief Product Officer & cofounder at StrongestLayer, bringing valuable experience from his previous roles at Google, Mandiant, and FireEye as a Product Lead. His background in machine learning and cybersecurity has been instrumental in developing the company's AI-powered security platform that addresses today's most sophisticated threats.

Muhammad Rizwan, CTO

Riz is the Chief Technology Officer and cofounder of StrongestLayer. He has deep experience building threat detection products, including leading the development of FireEye's zero-day engine (MVX). At Trellix and FireEye, he drove innovation that shaped modern malware defense. Riz combines technical depth with a strong focus on real-world problems, holding multiple patents in malware analysis. His mission: to pioneer "In-Workflow Threat Detection and Real-Time Protection" for the AI era—making security smarter, faster, and built for how threats work today.

Dr. Fahim A., PhD

Dr. Fahim is a Cybersecurity and AI Expert at StrongestLayer, bringing his extensive academic background and research expertise to the company's threat intelligence and solution development. His work focuses on the intersection of artificial intelligence and cybersecurity, helping organizations understand and defend against emerging AI-powered threats.

ABOUT STRONGESTLAYER

StrongestLayer is at the forefront of AI-powered cybersecurity, addressing three major challenges faced by security teams today: AI-Powered Phishing at Scale, SOC Team Overload, and Ineffective Training. Our mission is to protect organizations from the escalating threat of AI-generated phishing attacks by providing innovative solutions that operate at machine speed.

StrongestLayer functions like a team of 1,000 security analysts, evaluating emails with human-level reasoning to significantly reduce the workload for SOC analysts in email triage. Built natively on large language models, our platform analyzes intent and contextual relationships across email content, SMTP headers, and enriched signals from embedded URLs and attachments to deliver precise threat verdicts. This AI-first approach is purpose-built to tackle the most critical challenges of today’s evolving threat landscape.
Our approach to cybersecurity is built on addressing the key challenges in today's threat landscape:

1. AI-Powered Phishing at Scale: We recognize that AI-driven tools enable attackers to create novel and scalable threats, rendering traditional email security reactive and ineffective against these evolving tactics.
2. SOC Team Overload: Our solutions help reduce the burden on security operations teams by automating the analysis of potential threats, allowing your human experts to focus on strategic security initiatives.
3. Ineffective Training: We address the limitations of traditional security awareness training that often focuses solely on compliance and fails to prepare users for the sophisticated AI threats they now face.

With StrongestLayer, organizations can protect their emails in approximately 5 minutes, deploy security plugins in hours, and implement personalized training in days—providing immediate protection against tomorrow's threats.

REFERENCES

- SoSafe Research. (2024). "The Effectiveness of AI-Generated Phishing Attacks." Cybersecurity Insights Report, Vol. 8, Issue 2.
- Biometric Update. (2024). "Annual Threat Landscape Report: The Rise of AI-Powered Attacks." Biometric Update Research Division.
- Harvard Kennedy School & Avant Research Group. (2024). "AI and Social Engineering: Measuring the Impact of AI-Generated Phishing." Technology and Security Policy Paper Series.
- Security Magazine & AJG Research. (2024). "CISO Survey: Perceptions of AI in the Threat Landscape." Annual Security Leadership Report.
- Pin Drop Security. (2024). "Analysis of AI-Powered Attack Trends in Q1-Q2 2024." Quarterly Threat Intelligence Report.
- Gartner Research. (2024). "Market Guide for AI-Powered Security Solutions." Gartner Security & Risk Management.
- MIT Technology Review. (2024). "The Economics of AI-Powered Cybercrime." Special Report on Cybersecurity.
- Forrester Research. (2024). "The Total Economic Impact of AI in Cybersecurity." Forrester Consulting.
- World Economic Forum. (2024). "Global Cybersecurity Outlook: The AI Challenge." Annual Cybersecurity Report.
- NIST. (2024). "Framework for Managing AI Risks in Cybersecurity." Special Publication 800-Series.
- Ponemon Institute. (2024). "Cost of AI-Powered Data Breaches." Annual Cost of Data Breach Report.
- SANS Institute. (2024). "Defending Against AI-Enhanced Social Engineering." SANS Reading Room.
- Verizon. (2024). "AI-Generated Threats Analysis." Data Breach Investigations Report.
- IBM Security. (2024). "The Evolution of Polymorphic Malware in the AI Era." X-Force Threat Intelligence Index.
- Microsoft Digital Defense Report. (2024). "AI-Powered Threat Landscape." Annual Security Report.