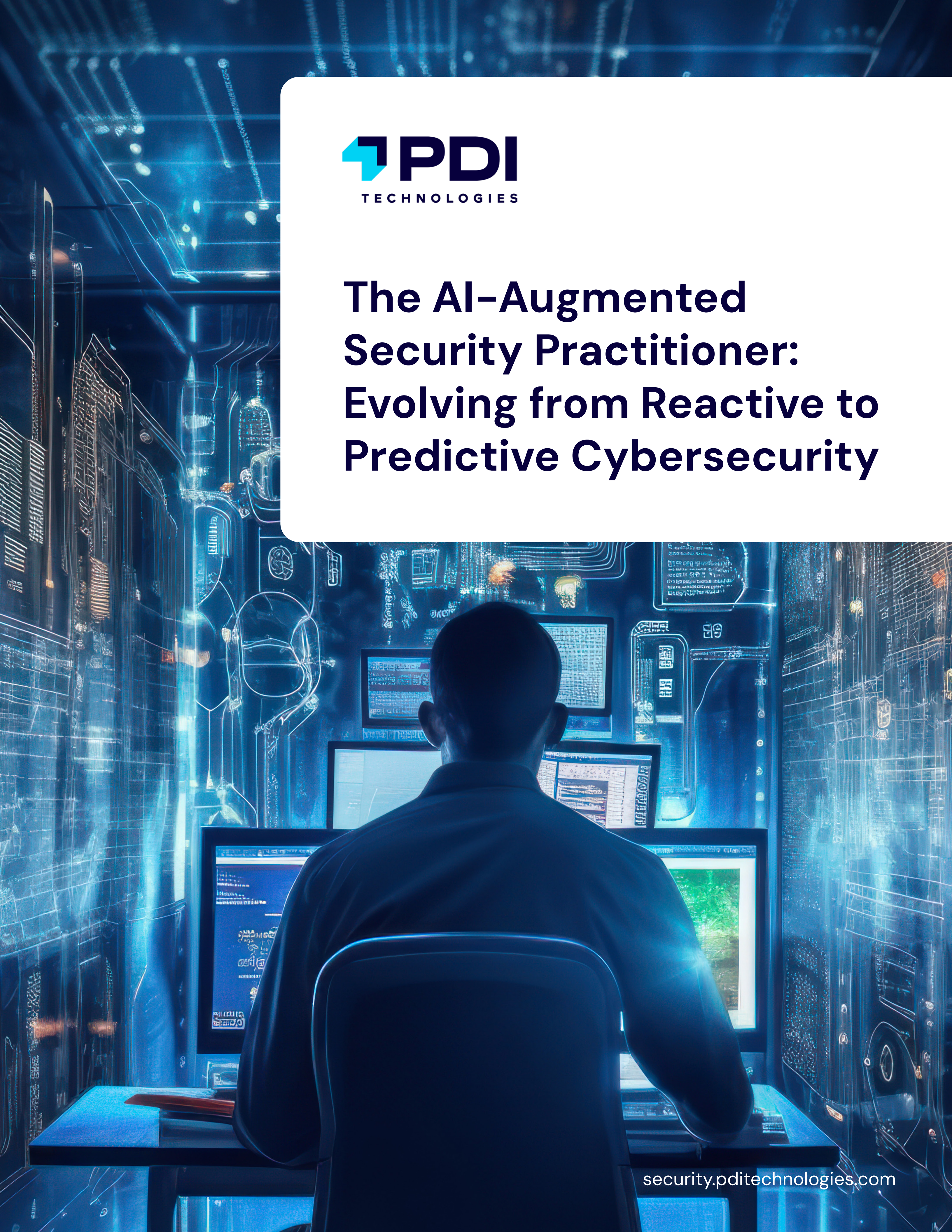
PDI
TECHNOLOGIES

The AI-Augmented Security Practitioner: Evolving from Reactive to Predictive Cybersecurity



security.pditechnologies.com

Table of Contents

Introduction

AI in Cybersecurity

The story of offenders versus defenders is timeless. Assault weapons have evolved from flaming tar buckets and catapults to malware, phishing, and spoofing. Current cybersecurity defenders are overwhelmed by talent shortages, restricted budgets, and the onslaught of security news, bulletins, and emails. Artificial intelligence in cybersecurity is revolutionizing threat management, offering defenders an opportunity to equalize the battlefield—and even gain the upper hand—by enabling crucial proactive, predictive, and preventive capabilities.

The use of AI won't replace security professionals. It assists humans so they can work efficiently with more precise insights. Speed counts against offenders who aggressively search for and exploit vulnerabilities in software, code, unpatched systems, and human behavior. With AI as an ally, you can strengthen your security posture, shrink the attack surface, and build organizational resilience.

Businesses increasingly emphasizing proactive cybersecurity measures, the demand for AI-driven SOC is expected to rise, further contributing to the SOC as a Service market growth.[1]

Chapter 1

Transforming Traditional Security Roles

Manual defensive actions slow down detection, analysis, and response. AI's speed helps to transform roles in areas such as:

01 **Compliance.** Practitioners spend hours comparing frameworks and standards such as the Health Insurance Portability and Accountability Act, Cybersecurity Maturity Model Certification, and NIST 800-53 to find commonality across controls. AI turns this effort into a quick-hit exercise. It compares the documents and identifies which controls need to be implemented to provide the highest compliance benefit across applicable standards. Plus, AI points out remaining gaps, allowing for faster decision-making regarding compliance controls.

02 **Threat detection.** Practitioners gather threat intelligence, analyze it, and determine the seriousness of threats before they act. AI can analyze the intelligence, find indicators of compromise (IOCs), provide context, and assign severity levels in a flash. In-house analysts can ask AI questions like "Should I care about X?" to obtain actionable information. Based on answers to simple questions, security services providers can advise customers to change a particular setting on a particular device immediately.

03 **Efficiency.** As it analyzes data, AI flags items that help practitioners make better decisions the first time, resulting in high-quality results and fewer repeat issues. Imagine spending far less time staring at data flying across the screen, sifting through noise, correlating data bits, and slashing the time bad actors have to regroup and charge again.

Use Case

Querying Top Threats

Without AI, practitioners sift through logs and dashboards to identify the top threats in an environment. With AI, you receive a detailed list in seconds, complete with severity, affected systems, and recommended actions.

Top AI Applications in Cybersecurity

- Threat detection
- Behavioral analytics
- Automated incident response
- Vulnerability management
- Security automation/orchestration

Chapter 2

New Skills and Competencies for Security Professionals

AI will require reskilling. Enterprises, schools, and universities are increasingly incorporating AI into courses and curricula to support this shift.

A high-priority competency is proficiency in soft skills such as creativity, adaptability, and communication. To use AI effectively, practitioners need to construct precise, concise prompts. Critical thinking and creative problem-solving come into play when AI output needs correction or nuance. Practitioners who share AI output, terms, and concepts need to adapt, sometimes on the fly, to audiences with varying amounts of AI knowledge.

Another crucial skill emerging in the AI era is AI-enhanced threat intelligence analysis. Security professionals need to interpret and act on AI-generated threat intelligence reports effectively. This involves understanding how AI processes vast amounts of data to identify potential threats, critically evaluating the AI's findings, and translating these insights into actionable security measures.

A skill that will be de-emphasized is rote memorization. Activation keys, anyone? And, how many of us learned the PCI standard to bridge gaps between the mostly unchanged PCI 1.0 and the modern context of microprocessors, touch to pay, and payment apps? AI thrives on real-time data, which broadens and deepens its knowledge. Relying on AI's excellent memory takes the pressure off security professionals, reduces human errors, and decreases stress.

Regulations on the Rise

Regulations sometimes lead and sometimes lag an industry. AI-specific regulations are a work in progress. The EU AI Act and U.S. AI Bill of Rights, along with some U.S. state-level legislation, are among the initial efforts to control the use of AI.

Simplifying Compliance

Consider the Gramm-Leach-Bliley Act, which contains "Chinese wall" rules to prevent investment banks and brokerages from sharing data. Traditionally, practitioners spend lots of time designing and building firewalls to isolate data. Multiply this effort by the regulations, frameworks, and standards you study. AI can replace compliance mapping tools, quickly make sense of complex requirements, and provide concise recommendations.

Chapter 3

Symbiosis Between Human Expertise and AI Capabilities

The talent shortage in cybersecurity persists. Yet phones have to be answered day or night. Incidents need to be dealt with as quickly as possible. Missteps may lead to costly consequences. High-pressure jobs lead to burnout. Turnover is high. AI can help.

Recruitment can be streamlined with AI's ability to create ideal candidate descriptions, automate screening and simplify onboarding—giving time back to overworked security professionals. AI also can personalize training courses to match an individual's skills and career goals, aiding retention.

While there are many benefits of AI to threat detection and response professionals, the human-AI symbiosis is affected by hallucination. AI companies are working hard to solve this persistent problem, but hallucination is a top reason why AI will become prevalent in non-critical sectors first. Applications like traffic management systems can't tolerate misinformation. Even after hallucination risk is reduced or eliminated, we still want humans to verify accuracy every day that we have AI in our lives.

> Four million people are urgently needed to plug the talent gap in the global cybersecurity industry.[2]

Use Case

Real-Time Incident Response

Without AI, practitioners receive critical alerts and drop everything to handle them. With AI, you don't have to be involved. Simply set it up to quarantine a threat, block malicious traffic, and supply a summary of actions taken automatically.

Chapter 4

Proactive Security: How AI Is Shifting Cybersecurity from Reaction to Prediction

AI enables the cybersecurity industry to shift gears and be less reactive and more proactive. Defensive technologies and services such as endpoint detection and response (EDR), managed detection and response (MDR), and vulnerability management (VM) are good investments for purposes of finding issues, but they aren't designed to catch bad code, prevent a vulnerability, or stop a phishing link.

AI uses machine learning (ML) and analytics to sift big data, recognize patterns, understand what normal is, and detect anomalies. For example, AI can spot new software on a user's computer, detect elevated credentials, and question unusual login behavior (why is Bob in China?).

With lightning speed, AI eliminates noise to improve threat detection, shorten response times, and predict threats. AI shines in areas such as analyzing malware and data sources, threat hunting, policy development, and forensic investigation. Insights and lessons learned are fed back to AI to sustain continuous learning.

Predictive cybersecurity is another area where AI excels. By analyzing historical data and current trends, AI can forecast potential future threats, allowing organizations to proactively strengthen their defenses.

Reactive Versus Proactive

Reactive security responds to a threat, event, or incident, so it's one or more steps behind bad actors. Proactive cybersecurity in the context of AI means stepping in and stopping assailants before they make their moves.

Use Cases

Automated Threat Hunting

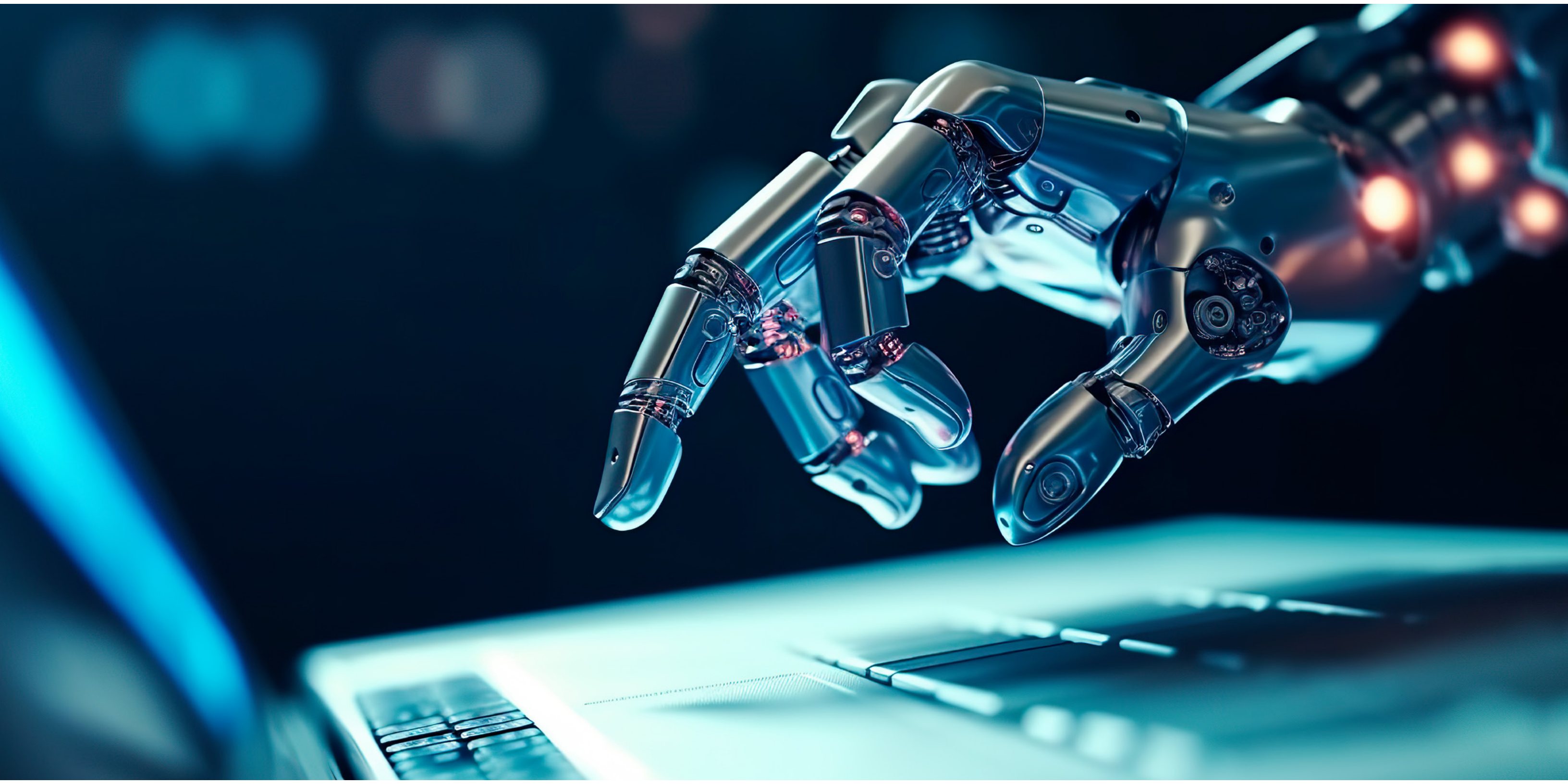
Threat hunting goes beyond EDR, MDR, and VM. Without AI, a threat hunt involves hours of gathering and analyzing intelligence from multiple sources to find unknown threats. With AI, you issue a natural language command to initiate a threat hunt that spans your entire network, identifies potential threats, and provides actionable insights, all with no manual intervention.

Code Development

Without AI, developers manually test and check code. Those who use AI tools in coding may introduce new vulnerabilities. With AI, teams can improve code with real-time analysis, predictive vulnerability detection, automated code review, and proactive security alerts.

Automated Threat Detection

AI-powered systems continuously monitor networks for suspicious activities, significantly reducing the time to detect potential threats.



Chapter 5

Advanced AI Techniques for Uncovering Hidden Threats and More

Advanced techniques for uncovering threats further prove AI's value. One cutting-edge technique is deep threat hunting that goes beyond knowns such as tactics, techniques, and procedures (TTPs). AI can look for unknowns and non-traditional IOCs.

Additionally, AI algorithms and analytics can be designed to detect anomalous network behavior in real time, providing visibility to practitioners who can proactively stop zero-day and advanced persistent threats (APTs). This is crucial, given that the mean time to identify and contain a breach is currently 258 days, according to IBM's "2024 Cost of a Data Breach" report. Real-time threat monitoring shortens this window significantly, helping to quickly identify attack vectors that might pose future risks.

Threat discoveries trigger change management, a common cybersecurity challenge. Keeping a workforce informed about updated security protocols, technologies, policies, and processes isn't easy. AI, possibly in chatbot form, can serve as a change management expert that answers employee questions or nudges workers to check out a policy or process before they take a particular action.

> ...84% of change management practitioners we surveyed are moderately familiar to very familiar with AI. However, only 48% say they currently use it in their change management work.[3]

Chapter 6

AI-Driven Security Orchestration: Unifying the Cybersecurity Ecosystem

Security orchestration facilitates connection and integration within security environments. AI improves orchestration in areas such as:

Integrating technologies

AI collects data from diverse devices and threat intelligence sources, hands it off to a platform, and normalizes the data to simplify correlation. It also shares threat intelligence across technologies and platforms to update the entire security ecosystem. And, AI provides a comprehensive security view by integrating network monitoring, cloud security, endpoint protection solutions, and more.

Connecting tools

By analyzing data from firewalls, intrusion detection systems, endpoints, and other tools, AI identifies patterns and correlations that point to potential threats. It catches threats that span vectors, something that unconnected tools miss.

Automating workflows

Manual anything slows down threat detection and response. AI automates tasks such as prioritizing SIEM alerts, executing predefined remediation actions such as isolating infected systems, scanning for known vulnerabilities and patching them, and analyzing user behavior to detect and respond to anomalies. Security automation powered by AI not only speeds up routine tasks but also enables more complex, intelligent, automated responses to security incidents. This advanced automation can adapt to new threats in real time, learning from each encounter to improve future responses.

Bolster proactive security by using AI to monitor network traffic, user behavior, and system logs continuously to find potential breaches.

Chapter 7

Responsible AI Development in Security Contexts

We don't know what we don't know about who is using AI for what purposes. But we in cybersecurity can do our part to avoid bad outcomes by addressing risk through ethical use. Risk management discussions usually refer to fairness, transparency, accountability, trustworthiness, and privacy. Support responsible AI use:

- Follow internationally recognized standards and guidelines for AI development and use.
- Complete due diligence on AI models. Some are safer and more responsible than others.
- Conduct continuous monitoring and auditing to identify and mitigate biases.

A core aspect of responsible AI is balancing privacy and security in AI-driven systems—a challenge that will be solved differently by each organization and cybersecurity services provider. The following suggestions may help you think about balance:

- Protect the data at all stages of use with encryption and/or measures that align with zero trust.
- Anonymize data that's used in AI models and applications unless you have an excellent reason and a secure way to use non-anonymized data.
- Leverage a closed AI environment for cybersecurity purposes. Open-sourced AI platforms can present additional risks, so relying on a closed environment helps ensure tighter control over the data and model integrity.
- Maintain role-based access control to limit access to data and models. The least-privilege principle applies.
- Develop strong data governance policies that include regular data classification reviews, data retention policies, and guidelines for data sharing.
- Maintain continuous real-time monitoring and logging, supplemented by regular audits and risk assessments.

Best Practices for Responsible AI Use

- Select use cases carefully and thoughtfully. Use rigorous business decision processes and risk analysis, keeping in mind the "black box" nature of AI.
- Keep humans at the center of AI use. AI assists us in many ways, and it should be controlled by people who understand how AI interacts with data and security.
- Provide security practitioners with ongoing AI training and development.
- Understand the data collection process to help avoid bias and discrimination. Be clear about what data is used when, by whom, and for what purposes.
- Ensure data privacy by writing and enforcing clear, consistent AI policies, processes, and safeguards for data use, storage, and protection.
- Comply with or exceed regulations in your state, country, and global region.
- Communicate with CISOs, board members, and other stakeholders about AI's role in cybersecurity, with metrics if possible.

Chapter 8

The Future of Human-AI Collaboration in Security Operations

```
GS_API_URL = os.environ['GS_API_URL']
DATABASE_URL = os.environ['DATABASE_URL']
JOB_INGESTION_LAMBDA_NAME = os.environ['JOB_INGESTION_LAMBDA_NAME']


@app.route('/')
def serve_react_app():
    return render_template('index.html')

@app.route('/login', methods=['POST'])
def login():
    request_json = request.get_json()
    email = request_json.get('email')
    password = request_json.get('password')
    api_auth_endpoint = '{}v1/auth/'.format(GS_API_URL)
    auth_response = requests.get(api_auth_endpoint, auth=HTTPBasicAuth(email, password))
    excluded_headers = ['content-encoding', 'content-length', 'transfer-encoding', 'connection', 'www-
    auth_response_headers = [(name, value) for (name, value) in auth_response.raw.headers.items() if n
```

Practitioners need to flex different AI muscles as security and IT work together to improve collaboration and reduce risk. The following trends point to opportunities for human oversight of and interaction with AI:

- Hyper-focused large language models (LLMs), including some specific to cybersecurity, will become the norm.
- Defensive strategies are broadening in scope from AI-assisted tasks to AI ecosystems.
- Cybersecurity programs are beginning to define policies and processes covering AI use throughout an organization, and in particular, how to better protect data and build trust.
- Regulations are being developed, fine-tuned, and/or expanded to address concerns related to the safe, responsible use of AI. ISO 42001:2023, for example, is an AI management system standard for AI governance.

Security professionals who are collaborating with AI are on the frontlines of an industry transformation. Get ahead of the curve by preparing for this upcoming adventure:

- Focus on reskilling in areas where human involvement with AI is necessary and valued. Think of climbing up the security ladder. A low rung consists of manual tasks, like analyzing log data—AI can do this faster and better. A higher rung is knowing how to contextualize and leverage AI output.
- Learn about AI as it functions in cybersecurity, about how AI is used in the business, and about business functions such as compliance and risk management that touch cybersecurity. Academia lags behind technology, so this might be a DIY effort.
- Follow emerging technologies involving AI, security strategies, and security controls.
- Study AI use cases, especially those that attempt to solve critical infrastructure challenges.
- Expect industries, cybersecurity being one, to move faster than law in some aspects of AI. Consider guardrails and ethics and how they evolve in a dynamic context.
- Maintain continuous real-time monitoring and logging, supplemented by regular audits and risk assessments.

Conclusion

AI Is Reshaping Cybersecurity

AI will change traditional security roles, but it won't replace humans. Security professionals who learn new skills to collaborate effectively with AI will be well-positioned to advance their careers.

AI assistance helps the cybersecurity industry progress from reaction to prediction—a crucial advantage for cyber defenders. As AI techniques become more refined and precise, expect to see AI being integrated in deeper, broader ways throughout security operations.

Evaluating AI Augmented Providers

AI will be implemented and used differently by cybersecurity services providers. How do you begin to evaluate their use of AI to find the right fit? Explore the following topics:

- The AI LLM and how it's trained and by whom
- The types of data and data sources used in the LLM
- Data security controls that apply throughout the data lifecycle
- Responsible AI and how it's implemented
- The level of integration of AI in dashboards and services such as monitoring, threat detection, and incident response
- The role of AI in threat intelligence
- Existence of an AI assistant, mobile app, or other customer experience functionality
- Examples of how customers interact with an AI assistant
- The amount and type of AI-driven orchestration
- The extent to which AI-augmented services are industry-specific
- Metrics that allow customers to track improvements in security posture linked to AI-augmented functionality

Conclusion

The PDI Cybersecurity Experience: Elevating Security with Intelligent Unification

For organizations seeking to harness the full potential of AI in their cybersecurity strategy, the PDI Cybersecurity Experience offers a groundbreaking solution. This experience is more than just a service; it's a comprehensive, AI-driven platform designed to unify and optimize your security operations.

By integrating advanced AI capabilities through PDI's AI assistant, the PDI Cybersecurity Experience helps you streamline operations, reduce costs, and enhance decision-making with real-time, actionable insights.

The PDI platform provides a holistic view across your entire security tech stack, enabling you to stay ahead of emerging threats and make data-driven decisions with confidence.

PDI's intelligent unification approach not only simplifies complex security environments but also extends your in-house capabilities with 24/7 expert support and a dedicated mobile app for real-time threat management on the go.

Learn more about how the PDI Cybersecurity Experience can transform your cybersecurity strategy.

References

[1] AV-TEST Institute, Malware. https://www.av-test.org/en/statistics/malware/

[2] World Economic Forum, Strategic Cybersecurity Talent Framework white paper, April 2024. https://www.weforum.org/agenda/2024/04/cybersecurity-industry-talent-shortage-new-report/

[3] Prosci, AI in Change Management: Early Findings, Challenges and Opportunities, August 1, 2024. https://www.prosci.com/blog/ai-in-change-management-early-findings

About PDI Security and Network Solutions

With over 25 years of expertise, PDI Security and Network Solutions (formerly known as Nuspire) is redefining cybersecurity and network management through intelligent unification and unparalleled protection. The company delivers fully managed security and network services, including managed detection and response (MDR), endpoint detection and response (EDR), Firewall as a Service, 5G as a Service, and Wi-Fi as a Service. This technology-agnostic platform seamlessly integrates human expertise, advanced AI, and cutting-edge technologies, providing holistic visibility across security and network infrastructure. PDI's 24x7 SOCs and expert teams enable organizations to stay ahead of emerging threats while optimizing investments.

PDI TECHNOLOGIES

security.pditechnologies.com

LinkedIn @pdisecurityandnetworksolutions

PDI Security and Network Solutions