Secureworks®
a SOPHOS company

WHITE PAPER

A Practical Guide to (and Benefits of) AI in Cybersecurity

Unlock the Future of Cybersecurity with AI

I. INTRODUCTION AND OVERVIEW

“By 2028, multiagent AI in threat detection and incident response will rise from 5% to 70% of AI implementations to primarily augment, not replace staff.”

“By 2026, 40% of development organizations will use the AI-based auto-remediation of insecure code from AST vendors as a default, up from less than 5% in 2023.”

Source: Gartner, AI-Based Cybersecurity System Transforms Security Experience, December 2023

Artificial Intelligence (AI) is changing the game in cybersecurity, and as security practitioners, we need to be on top of how it impacts both the threats we face and the solutions we have at our disposal. This paper dives into the role of AI in today’s evolving threat landscape, focusing on both generative and non-generative AI. We’ll break down the opportunities and risks that come with each, and more importantly, how to develop AI-driven security strategies that actually work.

To start, it’s essential to understand a few key concepts:

- Machine Learning (ML) is a core AI technology that allows systems to learn from data and improve on their own without needing explicit programming.
- Large Language Models (LLMs) are a type of AI model designed to understand, generate, and manipulate human language. In cybersecurity, LLMs can be used for tasks such as automating threat detection, generating security-related reports, or even simulating potential attack scenarios.
- Natural Language Processing (NLP) helps machines understand and generate human language.
- Non-Generative AI (Non-GenAI) helps us with tasks like threat detection, classification, and pattern recognition by working with existing data.

- Generative AI (GenAI), on the other hand, is about creating content—text, code, images, you name it—based on learned patterns. GenAI allows complex processes to be applied to loosely structured or unstructured data, as well as returning relevant supplementary data on the subject.

In terms of cybersecurity, non-GenAI is already at the forefront, helping us identify and classify threats faster and with more accuracy. It also plays a big role in predictive analysis to stay ahead of evolving attacks. On the flip side, GenAI is pushing boundaries in areas like threat simulation, training, and even active defense mechanisms. GenAI can be used to query security data using natural language, explain complex code, and provide insights into an organization’s threat landscape. But it’s not all upside—GenAI also opens doors for bad actors, making it easier to create convincing deepfakes or run sophisticated social engineering attacks.

The key challenge for us as security professionals is understanding both the immense potential and the serious risks that come with GenAI. The balance between leveraging its power and safeguarding against its misuse will define how well we can protect our organizations in an increasingly complex and AI-driven digital world. Let’s get to work on staying ahead of these threats.

II. TRENDS IN CYBERSECURITY

Trend Data

Cybercrime cost the world $9.5 trillion USD in 2024, according to Cybersecurity Ventures. If it were measured as a country, then cybercrime would be the world's third largest economy after the U.S. and China.

Global cybercrime damage costs are expected to grow by 15% this year, reaching $10.5 trillion USD annually in 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

For a Board, the stakes of a ransomware attack are high. Ransomware, the fastest growing type of cybercrime, is predicted to cost its victims $265 billion USD annually by 2031, with a new attack taking place on consumers and organizations every two seconds. This is up from $20 billion USD in damages and an attack every 11 seconds in 2021. The dollar figure is based on 30% year-over-year growth in damage costs over a decade.

A 2024 survey of annual reports from the biggest U.S. corporations are increasingly highlighting artificial intelligence as a possible risk factor. On the flip side, a Google survey indicates that 63% of IT and security professionals believe AI will improve corporate cybersecurity.

The surge in digital transformation, driven by cloud computing and remote work, has expanded the attack surface, introducing new vulnerabilities. While AI is a valuable tool for enhancing security, it has also empowered cybercriminals, giving rise to AI-generated social engineering attacks. As organizations face these threats, the need for advanced, AI-driven cybersecurity strategies has become more urgent than ever.

One of the most prominent threats today is ransomware, where attackers encrypt data and demand a ransom, often disrupting operations and causing significant financial losses. The practice of double extortion, in which cybercriminals steal and threaten to expose sensitive data, has intensified the pressure on victims. Ransomware groups are growing at an alarming rate.

Secureworks® recently observed a 30 percent year-over-year rise in active ransomware groups, highlighting the evolving and increasingly organized nature of these attacks. Alongside this, phishing attacks continue to thrive, leveraging AI to craft highly convincing, personalized messages to deceive victims. The rise of Internet of Things (IoT) attacks is another critical concern, as many IoT devices remain inadequately secured, offering easy targets for cybercriminals.

The widespread adoption of cloud environments and remote work has significantly altered the cybersecurity landscape. Traditional perimeter-based security models no longer suffice as organizations now rely on decentralized systems, remote access, and identity management systems. This shift requires the development of more dynamic security strategies with the speed of AI to protect digital assets effectively.

A major challenge in this new reality is the growing shortage of skilled cybersecurity professionals. As the demand for expertise outpaces the supply of trained workers, organizations are left struggling to bolster their defenses. AI tools offer a potential solution by automating routine tasks, allowing human experts to focus on more complex issues. However, integrating AI into cybersecurity frameworks requires careful planning and consideration.

The speed at which organizations detect and respond to cyberattacks is critical, especially in ransomware cases, where attackers often demand payment within hours. Secureworks Counter Threat Unit™ (CTU™) observed that one third of security intrusions saw ransomware deployed in less than a day. AI can significantly reduce the dwell time, or the length of time attackers remain undetected, helping organizations to react swiftly and minimize damage. Moreover, AI's scalability allows businesses to implement consistent security measures across vast digital infrastructures, an essential capability as the scale and complexity of cyberattacks continue to grow.

In the face of these challenges, AI-powered cybersecurity presents both risks and opportunities. While adversaries may exploit AI for malicious purposes, organizations can leverage it to strengthen their defenses, streamline operations, and ensure a faster, more proactive approach to securing their digital environments. The ongoing evolution of AI technologies promises even more advanced and adaptive cybersecurity solutions for the future.

Secureworks observed a

30%

year-over-year rise in active ransomware groups

III. GENAI - A SPECTRUM OF IMPACTS

> **"By 2027, generative AI will contribute to a 30% reduction in false positive rates for application security testing and threat detection by refining results from other techniques to categorize benign from malicious events."**

Source: Gartner, 4 Ways Generative AI Will Impact CISOs and Their Teams, December 2024

> **"By 2026, enterprises combining GenAI with an integrated platforms-based architecture in security behavior and culture programs will experience 40% fewer employee-driven cybersecurity incidents."**

Source: Gartner, Top Trends for Cybersecurity in 2025, December 2024

GenAI is rapidly reshaping the cybersecurity landscape, offering both immense opportunities and significant challenges. While it enhances defenses against cyber threats, it also enables attackers to craft more sophisticated, evasive attacks. This dual nature highlights the need for a nuanced understanding of AI's potential to strengthen defenses while acknowledging emerging threats.

A key contribution of AI is in revolutionizing threat detection and response. AI models analyze vast datasets—such as security logs and dark web chatter—to identify anomalies that traditional systems might miss. By generating patterns from historical and real-time data, AI can identify new attack patterns with unprecedented speed and accuracy.

GenAI also enhances automated threat hunting. Unlike traditional systems, which rely on predefined attack signatures, AI can identify previously unknown threats, including zero-day vulnerabilities. By simulating advanced persistent threats (APTs) and hacker strategies, AI can proactively identify defense gaps, minimizing damage from attacks like ransomware.

Another benefit is improved threat intelligence sharing. GenAI generates detailed reports that can be shared across organizations, enhancing collective understanding of attack methods and enabling more effective risk mitigation. Additionally, GenAI

increases efficiency in security operations by automating tasks like log analysis and threat classification, explaining complex information like detection logic, command lines, and alerts. This allows security professionals to focus on strategic decision-making.

AI-driven systems also support continuous monitoring, dynamically adjusting defenses like firewall rules and access controls in real time. Moreover, GenAI accelerates security research, helping researchers simulate new attacks, test system resilience, and create intelligent automation tools. GenAI can also accelerate security investigations by summarizing security incidents and adding contextual support.

However, the power of GenAI also aids adversaries. Attackers use it to develop advanced polymorphic malware that evades traditional detection methods. AI also enhances social engineering tactics, making phishing emails more convincing and enabling deepfakes to manipulate individuals or disrupt infrastructure. AI-powered bots can amplify Denial-of-Service (DoS) attacks, bypassing traditional defenses and complicating mitigation efforts.

In conclusion, GenAI is a double-edged sword in cybersecurity. While it improves threat detection, automation, and intelligence sharing, it also empowers cybercriminals to create more advanced and evasive attacks. Organizations must remain vigilant, adapt their strategies, and evolve their defenses to keep pace with the rapidly changing threat landscape.

IV. AI OPPORTUNITIES

The Human in the Loop

The "human-in-the-loop" (HITL) describes a system where human input is integrated into AI's learning and decision-making processes. This approach combines the strengths of both humans and machines to create more accurate, efficient, and reliable AI systems.

AI in cybersecurity enhances threat detection, response, and prevention. Organizations using AI-driven security solutions observe reduced risk and increased operational efficiency. Shifting from reactive to proactive, AI enables predictive and adaptive security postures. This strengthens defenses and improves operational effectiveness. AI empowers our security teams, allowing for tailored defenses against specific threats and organizational needs.

A proactive security posture, emphasizing anticipation and mitigation of threats before they cause damage, is significantly enhanced by AI, which enables organizations to predict, identify, and neutralize risks early. AI excels at analyzing vast amounts of data, including historical threat intelligence, real-time security logs, social media feeds, and even dark web chatter. This enables organizations to model potential threats and assess associated risks more accurately than traditional methods. By considering factors such as organizational vulnerabilities, industry specifics, and external factors like geopolitical events, AI can identify and prioritize high-risk areas. For example, AI can detect patterns in employee behavior to identify potential insider threats or assess the likelihood of specific attack types, allowing organizations to allocate resources effectively and address critical vulnerabilities before they are exploited.

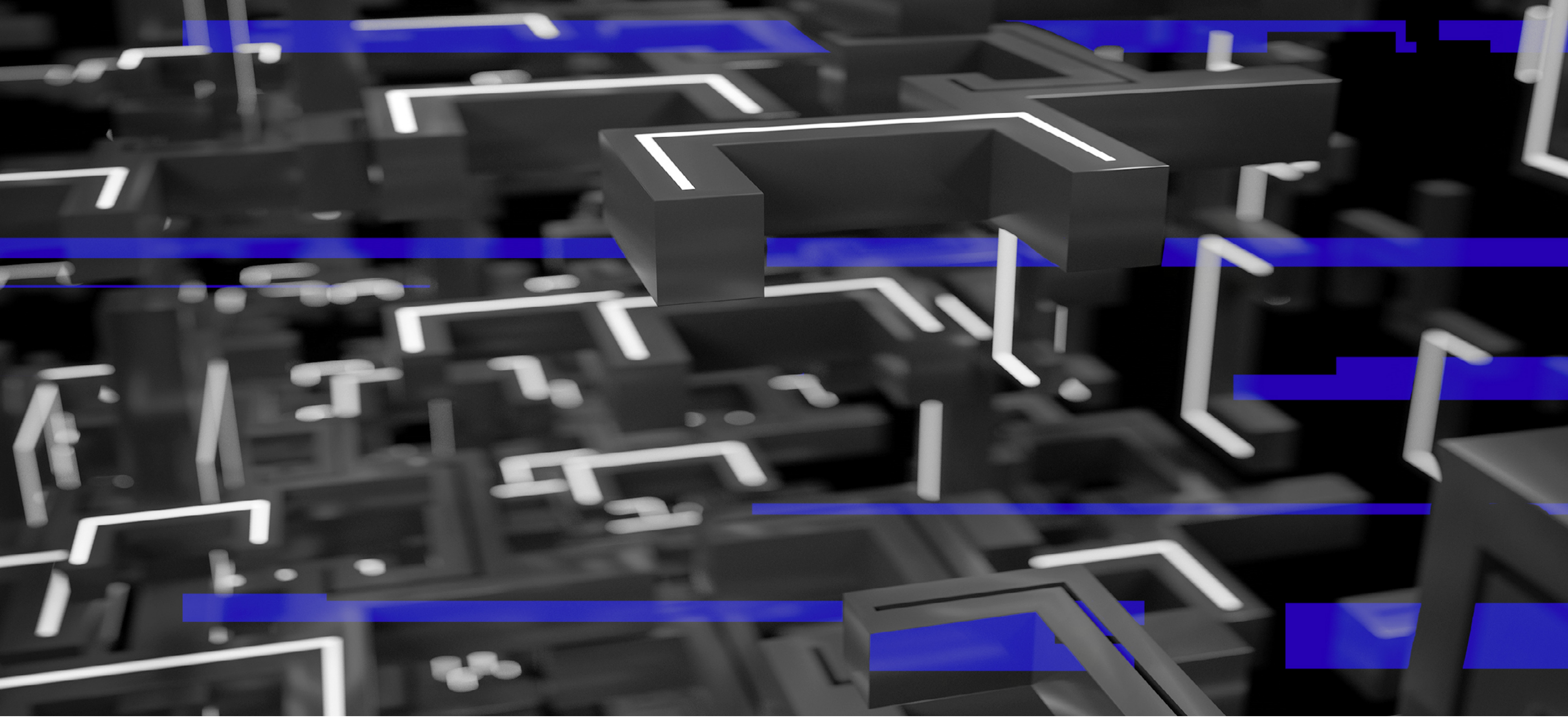
Furthermore, AI-driven automation ensures consistent enforcement of security policies, reducing the risk of human error. Automated controls for access management, data loss prevention, and endpoint security can monitor user activity in real time, identifying and responding to anomalies such as unusual login attempts or large data downloads. For instance, if suspicious behavior is detected, an AI system can automatically block access to sensitive systems or escalate the issue for further investigation. This strengthens security and frees security teams to focus on higher-value activities such as threat intelligence analysis and incident response.

AI-powered security systems continuously monitor evolving threats, adapting defenses in real time to stay ahead of attackers. Machine learning algorithms can analyze threat intelligence feeds, detect emerging attack vectors, and automatically adjust defenses, such as firewall rules or intrusion prevention systems. For example, if an uptick in phishing attacks targeting specific departments is identified, AI can immediately tighten email filtering protocols for those departments. This adaptive control ensures that defenses evolve alongside the threat landscape, maintaining robust protection.

AI also enhances the capabilities of human professionals. Tight coupling of AI capabilities with the “human in the loop” is essential to maximizing success. AI-powered tools streamline time-consuming tasks such as alert triage, threat hunting, and incident response. These tools can process massive volumes of security data, prioritize alerts based on severity, and identify patterns that might otherwise go unnoticed. For example, AI can correlate disparate security events across an organization's network, providing analysts with comprehensive insights into potential threats. While AI identifies and highlights risks, human experts provide oversight and make critical decisions, ensuring ethical and strategic considerations are considered.

Tight coupling of AI capabilities with the “human in the loop” is essential to maximizing success.

As AI becomes a cornerstone of cybersecurity, equipping professionals with relevant skills is imperative. Training programs should focus on machine learning fundamentals, AI-powered security tools, and the ethical implications of AI in cybersecurity. By fostering AI literacy, organizations ensure their security teams are prepared to leverage these technologies effectively.



AI systems and automation can also automate critical stages in the incident response process, including containment, eradication, and recovery. AI systems and automation can isolate compromised devices, quarantine malicious files, and restore affected systems from backups without manual intervention. This acceleration of response times minimizes the impact of cyberattacks on business operations. Furthermore, AI can analyze incident data to refine future response strategies, continuously improving resilience.

The rise of AI offers organizations unprecedented opportunities to enhance their cybersecurity posture. By leveraging AI-powered solutions, organizations can transition to a proactive, adaptive, and predictive security model, characterized by faster threat detection, more efficient incident response, and continuous optimization of defenses.

Equally important is investment in training cybersecurity professionals to harness the full potential of AI technologies. This combination of advanced tools and skilled personnel enables organizations to navigate the complex and dynamic cybersecurity landscape effectively. By embracing AI-driven solutions, organizations can build resilient security infrastructures capable of addressing the increasingly sophisticated threats of the digital age.

V. AI AND AUTOMATION PROVIDING BENEFITS AND RETURN ON INVESTMENT

Secureworks AI and Automation Drive Benefits and Return on Investment

50%+ noisy alerts are auto-remediated by machine learning. Patented alert prioritization, that learns hourly, reduced analyst workload by over 50%, which along with other automations led to an 80% reduction in customer notification times. Secureworks GenAI capabilities include:

- **Security incident summarization**
- **Command-line & code explanation**
- **Alert explanation**
- **Alert & investigation guidance**
- **Natural language search**
- **AI assistant**

Source: Secureworks SecOps

The integration of AI and automation into cybersecurity operations represents a significant advancement in the battle against increasingly sophisticated cyber threats. As cyberattacks grow more complex, frequent, and rapid, organizations must turn to more efficient and scalable solutions. AI technologies offer key benefits, such as reducing detection and response times, lowering operational costs, and ensuring business continuity. These advancements not only bolster an organization's security posture but also generate measurable returns on investment (ROI).

In the realm of cybersecurity, time is critical. The longer a threat remains undetected or unresolved, the greater the potential damage. AI plays a pivotal role in reducing both detection and response times, enabling faster threat containment than traditional methods. AI algorithms can analyze vast amounts of data in real time, identifying anomalies and suspicious activities indicative of cyber threats. AI platforms have demonstrated a reduction in mean time to detect (MTTD), allowing security teams to respond before an incident is escalated. Once a threat is detected, AI systems, which are tightly integrated with the human in the loop, can then accelerate and automate initial response actions, such as isolating compromised devices and blocking malicious traffic. This can reduce the need for slower, purely manual intervention during the critical early stages of an attack and significantly shorten the mean time to respond (MTTR).

AI enhances threat visibility by analyzing various data sources like network traffic, threat intelligence feeds, and user behavior to provide a comprehensive view of the threat landscape. This improved visibility helps organizations identify and mitigate threats that might otherwise go unnoticed. With AI's predictive capabilities, organizations can process information from various sources such as threat intelligence feeds, dark web forums, and social media, enabling them to anticipate emerging threats and take proactive measures. AI also improves threat hunting by automating the detection of unusual patterns, empowering security teams to uncover hidden threats, including insider attacks, which might evade traditional monitoring.

One of the biggest challenges in cybersecurity is the overwhelming workload placed on security teams. AI addresses this by automating routine tasks and improving the prioritization of alerts, increasing team efficiency and reducing alert fatigue. Security teams often face thousands of alerts daily, many of which are false positives. AI solutions can significantly reduce this volume by prioritizing alerts based on severity and context, allowing teams to focus on critical threats. Additionally, AI enhances decision-making by providing actionable insights and recommendations, helping teams respond more effectively and efficiently.

AI solutions can significantly reduce this volume by prioritizing alerts based on severity and context, allowing teams to focus on critical threats.

AI also offers cost-saving advantages. By automating labor-intensive tasks such as vulnerability scanning, patch management, and incident triage, organizations can lower operational expenses while maintaining robust security measures. AI tools streamline incident management by automating containment and analysis, which reduces the need for extensive human intervention and results in lower incident response costs and quicker recovery. These efficiencies help organizations minimize the financial impact of cyberattacks, such as reducing downtime and mitigating reputational damage.

AI's ability to minimize business disruptions from cyberattacks is another critical advantage. By enabling faster threat identification and response, AI reduces downtime and prevents data loss. Automated containment measures

can isolate compromised systems while allowing unaffected parts of the network to remain operational, preserving business continuity. Furthermore, AI systems can prevent data breaches by detecting and blocking malicious activity before it compromises sensitive information, safeguarding critical assets and improving overall business continuity.

Quantifying the ROI of AI investments is essential for securing stakeholder buy-in and sustaining ongoing funding. Key metrics to track include the reduction in MTTD and MTTR, the number of incidents mitigated, and the cost savings achieved by avoiding data-breach-related expenses. For example, the 2024 Cost of a Data Breach report, conducted by the Ponemon Institute, noted that the global average cost of a data breach in 2024 was 4.88M—a 10 percent increase over 2023 and the highest total ever. This underscores the financial value of proactive prevention. AI's role in improving security posture also leads to intangible benefits, such as increased trust among customers and partners, which can strengthen an organization's reputation and competitive edge.

In the final analysis, AI and automation offer organizations unparalleled capabilities in detecting and responding to cyber threats, improving visibility, and enhancing the efficiency of security teams. By reducing operational costs and minimizing disruptions, AI provides both immediate and long-term ROI. Monitoring key metrics such as MTTD, MTTR, and cost savings allows organizations to justify continued investment in AI-powered cybersecurity solutions, ensuring increased strength and resilience in the face of an increasingly complex and evolving threat landscape.

VI. SECUREWORKS LEADERSHIP AND EXPERIENCE IN AI

Secureworks Expertise

- 750B+ security events processed daily
- 51PB of diverse data (e.g., endpoint, cloud, network, email, etc.)
- 60M curated threat indicators (proprietary and third party)
- 20k+ curated detectors (ML/DL, UEBA, pattern/temporal-based, rules-based, etc.)
- 350+ integrations in production

Innovation

"Secureworks delivers XDR through Taegis™, an open, cloud-native platform that features more than 350 first- and third-party integrations with security controls that provide visibility over the endpoint, network, cloud, email, identity, application, and OT environments. The platform uses a newly introduced, AI-powered model to correlate the data and generate a threat score for prioritization. The model is trained with more than 750 billion events ingested into Taegis daily and reduces alert noise significantly beyond the regular XDR process of analyzing events."

Frost & Sullivan, Frost Radar™ Extended Detection and Response 2024

Secureworks, a Sophos comapny, is a global cybersecurity leader that secures human progress with Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Secureworks has been at the forefront of AI innovation in cybersecurity, processing over 750 billion security events daily and analyzing 51 petabytes of diverse data from sources such as endpoints, cloud, networks, and email. It's only possible to deliver these transformative innovations to customers because of the unique variety, volume, and timeliness of new security event data Secureworks possesses.

With 60 million curated threat indicators and more than 20,000 detectors powered by ML, and other advanced techniques, Secureworks offers a robust security solution to address the most complex cyber threats. The company integrates over 350 third-party systems, with a default data retention of one year and options up to five years, continuously refining its threat intelligence ecosystem.

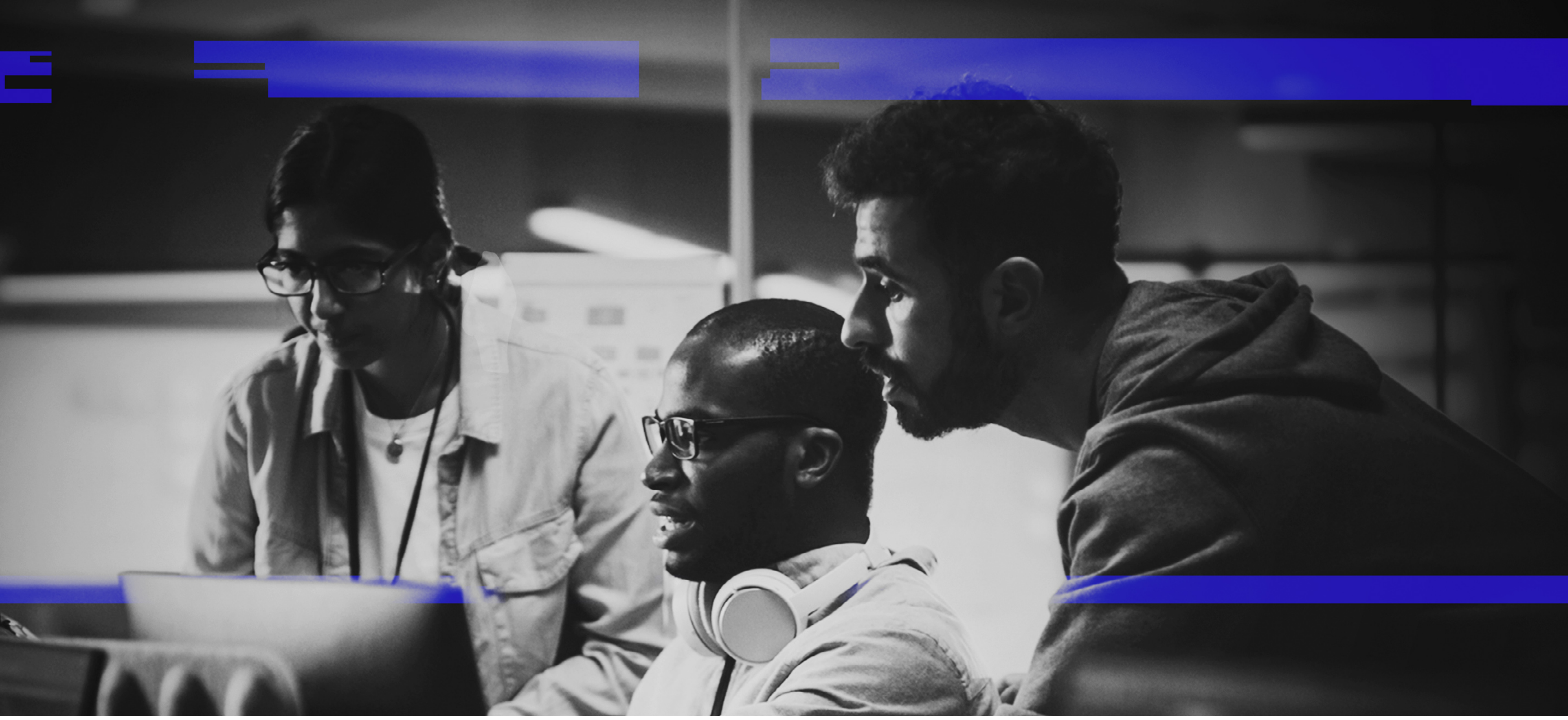
Secureworks' flagship platform, Taegis, exemplifies its commitment to AI-driven cybersecurity. Taegis leverages AI to enhance threat detection, response, and mitigation. Secureworks has always embraced AI, ML, and automation to reduce notification times and suppress noisy alerts. The Taegis Prioritization Engine uses a patent-pending machine learning model to continuously learn by processing more than 1 million alerts per month across the customer base. The engine removes irrelevant or benign alerts. In fact, 99.6 percent of alerts received from third-party security products are automatically filtered as false positives, giving important time back to analysts that otherwise could have been wasted. Internal use of the Prioritization Engine decreased the workload of the Secureworks SecOps team by over 50 percent.

Internal use of the Prioritization Engine decreased the workload of the Secureworks SecOps team by over

50%

The Taegis platform also excels at providing incident summaries and explaining complex command-line activities, as well as detection logic and detailed alert breakdowns that help analysts respond quickly and accurately. Secureworks leverages GenAI to draft summaries of security investigations, including important context and alert details, saving 90 percent of the time it typically takes to write investigations. By integrating AI and automation into incident investigation, analysts can perform investigations faster while simultaneously enhancing the quality and accuracy of their work. Through these enhancements, Secureworks has saved internal security analysts thousands of hours and improved its median time to notify customers of security incidents by over 80 percent.

Secureworks applies AI throughout its security operations, utilizing Large Language Models, Jupyter Notebooks, and native orchestration playbooks to automate investigations and provide AI-powered enrichments. These tools support automated response actions and workflows with integrated Security Orchestration, Automation, and Response (SOAR) capabilities, accelerating threat detection and mitigation. This comprehensive, AI-powered approach ensures rapid identification and response to threats, enhancing customers' security posture.



Secureworks is dedicated to continuous research and development, ensuring that its solutions evolve alongside emerging cyber threats. The company's investments in AI and ML allow it to deliver powerful, real-time insights that empower organizations to stay ahead of evolving risks and improve operational efficiency. Today, as a Sophos company, Secureworks continues in this mission, joining forces to further AI innovation and shape the future of cybersecurity.

VII. RECOMMENDATIONS

Key Recommendations for Leveraging AI:

- **Develop a comprehensive AI-driven cybersecurity strategy that aligns with your organization's goals**
- **Prioritize tools that automate routine tasks, support real-time decision-making, and predict emerging threats**
- **Empower teams with AI skills through regular training, collaboration, and industry-wide partnership**
- **Continuously monitor and adapt AI tools as the technology evolves**
- **Prioritize ethical considerations and ensure AI is used responsibly and fairly**

To fully leverage the power of artificial intelligence in cybersecurity, organizations should implement several strategic approaches. First, they should develop a comprehensive AI-driven cybersecurity strategy that aligns with the organization's goals. This involves clearly defining objectives, such as enhancing threat detection and response capabilities, identifying key use cases, and establishing a phased roadmap for integrating AI powered solutions into existing systems. AI-powered security tools and technologies such as Secureworks Taegis enhance current security frameworks, provide actionable insights, and can scale to meet evolving needs. It is essential to prioritize tools that automate routine tasks, support real-time decision-making, and predict emerging threats.

Equipping teams with the necessary skills is also crucial for maximizing AI's potential. Organizations should offer training programs to improve AI and machine learning skills, while leveraging AI tools to support junior analysts and enhance their capabilities. Supporting collaboration between cybersecurity professionals and AI specialists will also help create a more integrated and effective defense strategy. Collaboration and information sharing play a vital role in strengthening cybersecurity efforts. By engaging in industry forums, leveraging threat intelligence platforms, and establishing public-private partnerships, organizations can improve preparedness and response efforts by sharing best practices and insights.

Furthermore, organizations must continuously monitor and adapt their AI tools as the technology evolves. Regular assessments and updates, along with incorporating user feedback, will help refine strategies. Ethical considerations should also be a priority when deploying AI. Organizations should ensure that AI is used responsibly, respecting data privacy, maintaining transparency in decision-making, and addressing biases to foster trust and fairness. By adopting these recommendations, organizations can significantly enhance their security posture, improve response capabilities, and effectively defend against tomorrow's threats today, fortifying cyber resiliency.

Ready to take your cybersecurity to the next level with AI?

Now that you've explored this white paper, it's time to see how our cutting-edge, AI-driven solutions can safeguard your business. Whether it's advanced threat detection, rapid response capabilities, or proactive protection, Secureworks is here to help you stay one step ahead of cyber threats.

Reach out today to schedule a personalized demo and discover how Secureworks can tailor its cybersecurity solutions to meet your needs. Let us help you unlock the full potential of AI in securing your future.

Secureworks®
a SOPHOS company

Secureworks, a Sophos company, is a global cybersecurity leader that protects customer progress with Taegis, an AI-native security analytics platform built on more than 20 years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.