AI's Role in Cybersecurity Threats and Defenses - Examples of Concrete Solutions

Dragan Pleskonjić, Glog.AI, dragan@glog.ai
Luka Tica, Glog.AI, luka.tica@glog.ai
Vladimir Jelić, Glog.AI, vladimir.jelic@glog.ai
Dušan Todorović, Glog.AI, dusan.todorovic@glog.ai
Anthony English, Bot Security Solutions Inc., tony@botsecuritysolutions.com

Abstract: Artificial Intelligence is transforming cybersecurity into a high-speed chess game. While AI can detect, respond, and even prevent cyberattacks faster than ever, it is also being weaponized by threat actors at an alarming rate. This paper will delve into the potential misuse of AI in orchestrating cyberattacks and subsequently explore how AI and ML are being strategically applied within projects like Glog.AI, INPRESEC, Security Predictions, and vSOC to fortify software, information systems, and networks against these evolving threats. It also explores the Security-Analyst-in-the-Loop (SAIL) concept employed by Glog.AI and INPRESEC, illustrating how human-AI synergy helps mitigate the risks posed by over-automated systems. As digital transformation accelerates across industries, the role of AI in cybersecurity becomes not just a technical issue but a strategic imperative for organizations worldwide.

Keywords: Cybersecurity, Software Security, Artificial Intelligence, Risk Assessment, Security Analyst in the Loop

1. Introduction: Weaponizing Intelligence for Cyberattacks

The inherent capabilities of AI – its ability to learn, adapt, automate, and process vast amounts of data – make it a powerful tool that can be turned towards malicious ends in the cybersecurity landscape. Traditional cyberattacks often rely on predictable patterns and known vulnerabilities. However, AI empowers attackers to develop and deploy threats that are far more sophisticated and adaptive, posing a significant challenge to existing security measures.

The democratization of AI tools—such as open-source large language models and automated coding assistants—further complicates the threat landscape. Cybercriminals no longer need deep technical expertise to generate attack scripts, automate reconnaissance, or mimic legitimate communication, increasing the scale and frequency of AI-powered threats. One of the primary areas of concern is the use of AI to enhance social engineering and phishing attacks. By analyzing massive datasets of personal information and communication styles, AI can craft highly personalized and convincing phishing emails, text messages, or even voice calls. Natural language processing (NLP) allows attackers to mimic trusted individuals with remarkable accuracy, increasing the likelihood of successful deception. Deepfake technology further amplifies this threat by enabling the creation of realistic audio and video of individuals, potentially leading to more elaborate and believable scams.

2. Current Uses of AI in Cybercrime

AI can also be leveraged for automated vulnerability exploitation. Instead of relying on manual reconnaissance and exploitation, AI-powered bots can be trained to autonomously scan networks and systems for a wider range of vulnerabilities, including zero-day exploits. These intelligent agents can learn from past successful attacks, adapt their scanning techniques in real-time, and even chain together multiple vulnerabilities to achieve deeper system penetration. This automation significantly accelerates the attack lifecycle and reduces the need for extensive attacker intervention.

Furthermore, AI can be integrated into evasive malware. Polymorphic and metamorphic malware, which change their code to avoid signature-based detection, can be significantly enhanced with AI. Machine learning algorithms can enable malware to learn which code mutations are most effective at evading specific antivirus solutions and intrusion detection systems. Reinforcement learning could even allow malware to adapt its behavior dynamically based on the security environment it encounters.

Figure 1: Current Uses of AI in cybercrime

The orchestration of more sophisticated Distributed Denial-of-Service (DDoS) attacks is another area where AI poses a threat. Instead of simply overwhelming targets with sheer volume, AI-driven botnets can analyze network traffic patterns, identify critical infrastructure components, and launch targeted attacks designed to disrupt specific services. These botnets can also adapt their attack vectors in real-time to evade mitigation efforts, making them significantly more challenging to defend against.

Beyond these examples, AI can also be misused for AI-powered cryptojacking, where malicious AI agents optimize resource utilization and evasion techniques for illicit cryptocurrency mining, and potentially for bypassing biometric authentication systems through the development of sophisticated spoofing techniques. The versatility and adaptability of AI make it a potent weapon in the hands of cybercriminals, demanding a paradigm shift in how we approach cybersecurity defense.

3. Current uses of AI in Cyber Defense

There are multiple examples of use of AI in cyber defense. Here are some examples.[1]

Security analysts use AI to enhance threat detection, automates responses, and improve overall security posture. Even more are depicted in the figure below.

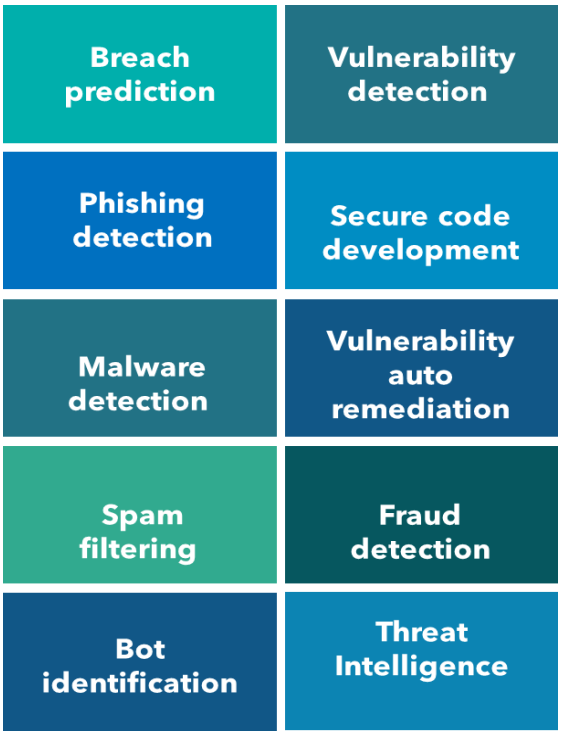


Figure 2: Current Uses of AI in Cyber Defense

AI techniques used in cyber defense include:

- Machine Learning (ML): For pattern recognition and anomaly detection.
- Deep Learning (DL): For advanced threat detection and analysis.
- Natural Language Processing (NLP): For analyzing and understanding text-based threats.
- Knowledge Representation and Reasoning (KRR): For decision-making and automated reasoning.

We present here some of our specific examples developed by Glog.AI.

AI security risks are increased when AI operates in isolation. This underscores the value of SAIL-based defenses, which reintroduce human reasoning into the decision pipeline. Instead of AI replacing human analysts, it augments their capabilities, allowing them to focus on high-value tasks that require critical thinking, contextual understanding, and strategic decision-making.

4. Glog.AI – Securing Software with AI-Powered Vulnerability Remediation

Figure 3: Glog.AI

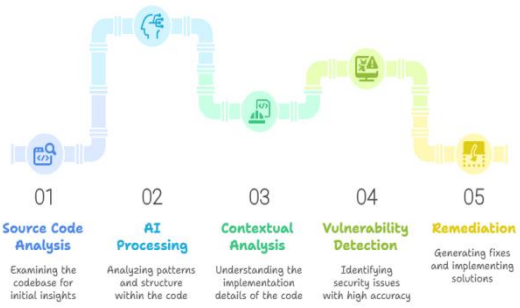
Glog.AI directly addresses the challenge of software security by leveraging AI to seamlessly identify and remediate security vulnerabilities within software code [2]. Recognizing that vulnerabilities in software are a significant entry point for many cyberattacks, Glog.AI empowers development teams to build more secure products from the outset.

At its core, Glog.AI employs AI-powered vulnerability detection. This goes beyond traditional static and dynamic analysis techniques by utilizing machine learning models to understand the context and semantics of the code [3]. This allows Glog.AI to identify genuine vulnerabilities with greater accuracy and significantly reduce the number of false positives that often plague traditional security scanning tools. By focusing on the actual risks, development teams can prioritize their remediation efforts more effectively.

A key differentiator of Glog.AI is its drive towards automated security vulnerability remediation. While currently focused on intelligent identification, the ultimate goal is to autonomously fix identified vulnerabilities. This would represent a significant leap forward in software security, allowing for true agility by embedding security directly into the development pipeline without causing delays. Imagine a system that not only identifies a flaw but also automatically applies the necessary fix, allowing developers to focus on building features rather than spending extensive time on manual remediation.

Glog.AI also provides seamless integration into the software development lifecycle (SDLC). By embedding its analysis capabilities within the development workflow, Glog.AI ensures that security is considered early and often – a principle known as "extend-to-left." This early detection and remediation of vulnerabilities is far more efficient and cost-effective than addressing them in later stages of development or in production.

Furthermore, Glog.AI empowers development teams by providing them with clear and actionable remediation advice. When a vulnerability is identified, the platform offers specific guidance on how to fix the issue, often including code examples and best practices. This not only helps in resolving the immediate vulnerability but also educates developers on secure coding practices, leading to more secure code in the future. By making security



a more integrated and less disruptive part of the development process, Glog.AI aims to foster a culture of security within development teams.

Figure 4: Glog.AI pipeline

5. INPRESEC and Security Predictions – Proactive Network and Threat Intelligence with AI/ML

INPRESEC (Intelligent Predictive Security) and Security Predictions represent a proactive approach to cybersecurity, leveraging AI and ML to anticipate and prevent attacks on networks and endpoints. Sensor component works on the Linux platform.[4]

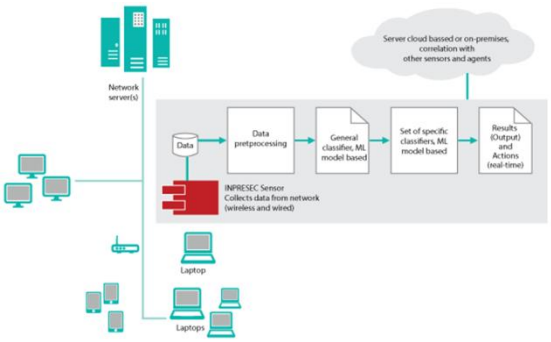


Figure 5: INPRESEC Sensor

INPRESEC focuses on network and endpoint security by employing AI and ML to detect anomalies in behavior, identify security threats, and predict potential attacks. Its novel approach aims to shift from reactive defense to proactive prevention. By analyzing network traffic patterns, user behavior, and system logs, INPRESEC's AI algorithms can establish baselines of normal activity. Deviations from these baselines, which could indicate malicious activity or the early stages of an attack, are flagged for investigation. The "intelligent predictive security" aspect lies in its ability to analyze these anomalies and other indicators to predict the most likely cyberattacks that an organization might face [5]. This predictive capability allows for the planning and implementation of optimal preventive and proactive cybersecurity defensive measures, effectively hardening systems before an attack can fully materialize.

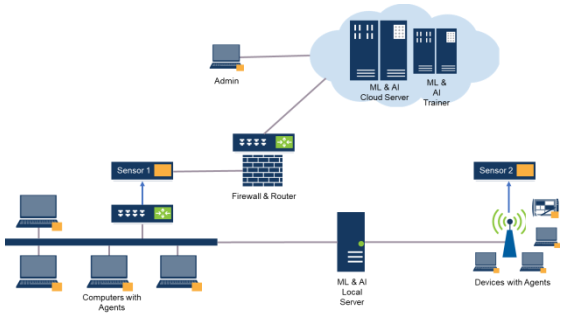


Figure 6: INPRESEC Deployment Model

Security Predictions focuses on threat intelligence, utilizing AI and ML to analyze a wide array of internal and external data sources. This data can include security reports, vulnerability databases, dark web activity, social media trends, and network traffic analysis. By applying proprietary algorithms to this vast dataset, Security Predictions generates probabilities of potential future threats and attacks. This predictive threat intelligence allows organizations to stay ahead of emerging threats, understand attacker tactics, and proactively adjust their security posture to mitigate potential risks. For example, if Security Predictions identifies a surge in discussions about a specific vulnerability being exploited, organizations can prioritize patching those systems.

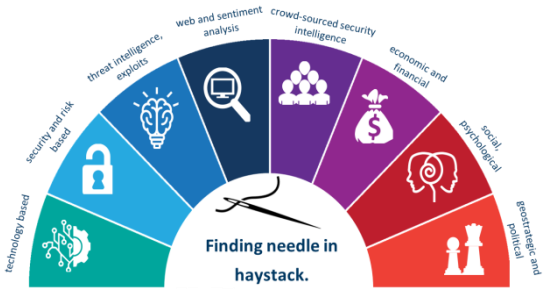


Figure 7: Security Predictions - Example of inputs

The synergy between INPRESEC and Security Predictions is evident. Security Predictions can provide INPRESEC with valuable insights into emerging threats and attack trends, allowing INPRESEC to refine its anomaly detection models and better predict the specific types of attacks that are likely to target the network and endpoints it protects. This collaborative approach, powered by AI and ML, enables a more dynamic and adaptive security posture.

6. vSOC (Virtual Security Operations Center) – Orchestrating AI-Powered Defense

The vSOC (Virtual Security Operations Center) automation by using AI represents a holistic approach to cybersecurity operations by integrating the capabilities of Glog.AI, INPRESEC, and Security Predictions, along with other security tools, into a centralized and AI-driven platform. The goal of a vSOC is to create a more efficient, effective, and proactive security operations capability.

Figure 8: vSOC

By leveraging Glog.AI's vulnerability detection and remediation insights, the vSOC can gain a deeper understanding of the security posture of the organization's software assets. This allows for proactive measures to address potential weaknesses before they can be exploited in a network attack.

INPRESEC's network and endpoint anomaly detection and predictive capabilities form a crucial layer of the vSOC, providing real-time monitoring and alerting on suspicious activities and potential attacks targeting the infrastructure. Its predictive nature allows the vSOC to anticipate and prepare for likely attack scenarios.

Security Predictions' threat intelligence feeds the vSOC with valuable context about the evolving threat landscape. This information allows the vSOC to prioritize alerts, understand attacker motivations and tactics, and proactively hunt for potential threats that might be emerging.

The "virtual" aspect of the vSOC emphasizes the potential for automation and remote operation, leveraging AI to augment and, in some cases, automate tasks that traditionally require significant human intervention. AI within the vSOC can be used for intelligent alert correlation, reducing alert fatigue by grouping related events and providing a more comprehensive picture of an incident. It can also facilitate automated incident response by triggering pre-defined playbooks based on the type and severity of the detected threat. Furthermore, AI can enhance threat hunting activities by identifying subtle patterns and anomalies that human analysts might miss.

In essence, the vSOC acts as an intelligent orchestration layer, bringing together the specialized AI and ML capabilities of Glog.AI, INPRESEC, and Security Predictions to provide a comprehensive and proactive defense across the entire IT ecosystem – from the software development lifecycle to network infrastructure and endpoint security. This integrated, AI-powered approach is essential for effectively countering the increasingly sophisticated and AI-driven cyber threats of today and the future.

Glog.AI’s penetration testing services, enhanced by the power of Artificial Intelligence, offer a more efficient, comprehensive, and insightful approach to identifying security vulnerabilities compared to traditional methods

7. Continuous Learning with Security Analyst in the Loop (SAIL)

In the context of Glog.AI and INPRESEC, SAIL is not just a theoretical model—it is a core operational strategy that enables rapid development of new security capabilities and ongoing refinement of existing ones. Through SAIL, AI becomes an intelligent partner that empowers cybersecurity professionals to work more efficiently, adapt faster, and make better-informed decisions.

When deploying AI/ML systems to detect novel cyber threats or address new attack surfaces, the first hurdle is the availability of high-quality training data. Security analysts play a vital role in

bridging this gap. By labeling and annotating raw data, they create the foundational datasets that enable supervised learning. This human-labeled data allows AI models to learn the distinction between benign and malicious activity, drastically improving their accuracy from the outset.

One of the most challenging scenarios for AI is the so-called cold start problem—where historical data is insufficient to bootstrap a new model. Here, SAIL excels by enabling analysts to provide initial labels and feedback that guide the model in its early learning stages. As a result, AI systems under the SAIL model reach maturity faster and begin delivering value more quickly than those trained in isolation. Before any AI model is widely deployed, it must be validated on live or representative datasets. Analysts test the model's performance, flag incorrect assumptions, and verify whether the model is detecting the right types of threats.

SAIL ensures that human analysts remain actively involved in this evolution. Their feedback is fed directly into the system to reduce false positives and false negatives, which remain one of the biggest sources of inefficiency and alert fatigue in cybersecurity operations.

8. Conclusion

The rise of AI presents a double-edged sword for cybersecurity. As AI technologies evolve, so must our approach to cybersecurity — not as a series of reactive measures, but as a continuously learning and adapting system. While malicious actors can leverage its power to create more sophisticated and evasive attacks, AI and ML also offer unprecedented opportunities to enhance our defensive capabilities. The question is not whether AI will dominate the cybersecurity landscape, but how we ensure it does so on the side of defense. Projects like Glog.AI, with its focus on AI-driven software security, INPRESEC's intelligent network and endpoint protection, Security Predictions' proactive threat intelligence, and the integrated AI-powered operations of a vSOC represent a crucial step forward in building more resilient and adaptive security postures. By strategically applying AI and ML across the security landscape, we can strive to stay ahead of evolving threats and protect our increasingly digital world.

References

[1] Dragan Pleskonjic, "AI in Cybersecurity and Software Security", *European Lotteries and World Lottery Association (EL/WLA) Security & Operational Risks Seminar: New Threats & Opportunities: Evolving AI & Security Risks*, Marseille, France, 2024.

[2]. Website Glog.AI, May 2025.

[3] Dragan Pleskonjic, Vladimir Jelic, "How IGT Protects Clients and Players with Rigorous Application Security Practices", *Think 2019*, San Francisco, California, USA, 2019.

[4] Borislav Đorđević, Dragan Pleskonjić, Nemanja Maček, "Operativni sistemi: UNIX i Linux", *Viša elektrotehnička škola*, Beograd, 2004.

[5] Dragan Pleskonjic, "Wireless intrusion detection systems (WIDS)", *19th Annual Computer Security Applications Conference*, Las Vegas, Nevada, USA, 2003.