Bansilal Ramnath Agarwal Charitable Trust's
Vishwakarma Institute of Technology
(An Autonomous Institute affiliated to Savitribai Phule University)
DEPARTMENT OF INFORMATION TECHNOLOGY

IT Bulletin January 2025

Artificial Intelligence in Cybersecurity

Vishwakarma Institute of Technology, Pune - Welcome to the August 2024 edition of the IT Bulletin on AI in Cyber Security. Inthis month , we're diving into the world of cyber security with AI to see together the latest progress and achievements in the world of cyber security with the introduction of AI.

INTRODUCTION

AI for cybersecurity uses AI to analyze and correlate event and cyberthreat data across multiple sources, turning it into clear and actionable insights that security professionals use for further investigation, response, and reporting. If a cyberattack meets certain criteria defined by the security team, AI can automate the response and isolate the affected assets. Generative AI takes this one step further by producing original natural language text, images, and other content based on patterns in existing data.

EVOLUTION OF AI IN CYBERSECURITY

- In the beginning, security teams used rules-based systems that triggered alerts based on parameters they defined.
- Starting in the early 2000s, advances in machine learning, a subset of AI that analyses and learns from large data sets, has allowed operations teams to understand typical traffic patterns and user actions across an organization to identify and respond when something unusual happens.
- The most recent improvement in AI is generative AI, which creates new content based on the structure of existing data. People interact with these systems using natural language, allowing security professionals to dive deep into very specific questions without using query language.

Impact of generative AI in cybersecurity

Generative AI is still in the early stages and has only recently been introduced in security with the announcement of Copilot for Security. It has the potential to radically simplify security for analysts and other security professionals by:

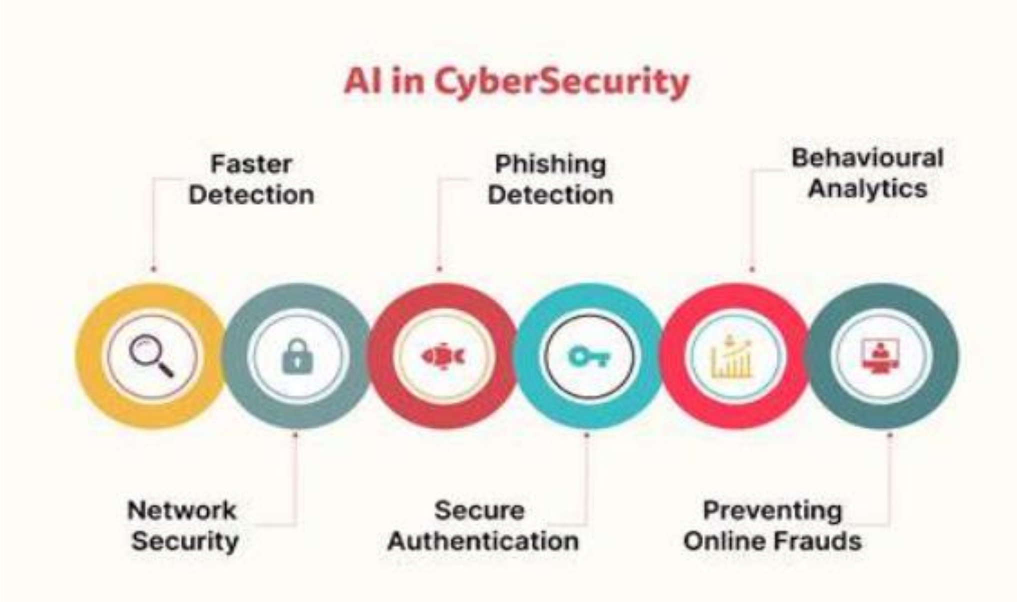
- Synthesizing data into actionable recommendations and insights with appropriate context to help guide incident investigations.
- Creating human-readable reports and presentations that analysts can use to help others in the organization understand what’s happening.
- Answering questions about an incident or vulnerability in natural language or graphics.

As the security community builds generative AI into security products and solutions, it will be important to build it responsibly. People need to know that new systems respect privacy and are reliable and safe. Accuracy and truthfulness are known issues with current generative AI models, but as the technology improves, it will help organizations stay ahead of AI-driven cyberthreats.

Working OF AI IN CYBER SECURITY

AI for cybersecurity works by evaluating massive amounts of data across multiple sources to identify patterns of activity across an organization, such as when and where people sign in, traffic volumes, and the devices and cloud apps that employees use. Once it understands what's typical, it can identify anomalous behavior that may need to be investigated. To maintain privacy, an organization's data isn't used for the AI output at other organizations. Instead, AI uses global threat intelligence synthesized from multiple organizations.

AI uses machine learning algorithms to continuously learn based on the data the system evaluates. When generative AI identifies certain known cyberthreats, such as malware, it can help contextualize threat analysis and make it easier to understand by generating new text or pictures to describe what's happening.



AI security use cases

Rather than replace security professionals, AI is most effective when it’s used to help them do their jobs more effectively. Some common uses cases for AI security are:

- **Identity and access management**: AI detects unusual login patterns, enforces two-factor authentication, and blocks compromised accounts.
- **Endpoint security**: AI helps track and update devices, while identifying malware and signs of cyberattacks.
- **Cloud security**: AI provides visibility into risks across multicloud environments.
- **Cyberthreat detection**: AI-powered XDR and SIEM solutions detect threats across the enterprise and trigger automated responses.
- **Information protection**: AI identifies sensitive data and prevents unauthorized transfers.
- **Incident investigation**: AI speeds up investigation by analyzing and correlating events, with generative AI providing natural language summaries.

Benefits of AI in security

With a growing number of cyberthreats, increasing amounts of data, and an expanding cyberattack surface, there are several ways that AI helps security operations teams be more effective.

- **Faster cyberthreat detection:** AI quickly identifies important incidents and correlates suspicious behaviors across activities to detect threats.
- **Simplifies reporting:** Generative AI creates easy-to-understand reports from multiple data sources for efficient sharing.
- **Identifies vulnerabilities:** AI detects risks like outdated systems, unknown devices, and unprotected data.
- **Skill development for analysts:** Generative AI helps junior analysts learn by translating complex data into natural language and suggesting remediation steps.
- **Enhanced threat analysis:** AI processes large amounts of data to uncover hidden patterns in cyberattacks and prioritize threats for professionals.

AI security for cyberthreat detection and prevention

One of the most critical uses of AI for cybersecurity is cyberthreat detection and prevention. There are several ways that machine learning algorithms and AI help identify and prevent cyberthreats:

- Supervised learning models use labeled and classified data to help train a system. For example, certain known malware has unique signatures that make it distinct from other types of cyberattacks.

- In unsupervised learning, machine learning algorithms identify patterns in data that haven't been labeled. This is how AI detects advanced or emerging cyberthreats that don't have known signatures. They look for activity that falls outside the norm, or they look for patterns that mimic other cyberattacks.

- With user and entity behavior analytics, systems evaluate user traffic patterns to understand known behaviors so that they can identify when a user does something unexpected or suspicious, which could indicate account compromise.

- AI systems also use natural language processing to analyse unstructured data sources like social media to generate threat intelligence.

AI-powered cybersecurity tools

- **Next-generation firewalls and AI:** Traditional firewalls make decisions about allowing or blocking traffic based on rules defined by an administrator. Next-generation firewalls go beyond these capabilities, using AI to tap into threat intelligence data to help identify novel cyberthreats.

- **AI-enhanced endpoint security solutions:** Endpoint security solutions use AI to identify endpoint vulnerabilities, such as an outdated operating system. AI can also help detect whether malware has been installed on a device or if unusual amounts of data are being exfiltrated to or from an endpoint. And AI can help stop endpoint cyberattacks by isolating the endpoint from the rest of the digital environment.

- **AI-driven network intrusion detection and prevention systems:** These tools monitor network traffic to uncover unauthorized users who are trying to infiltrate the organization through the network. AI helps these systems process data faster to identify and block cyberattackers before they do too much damage.

- **AI and cloud security solutions:** Because so many organizations use multiple clouds for their infrastructure and apps, it can be hard to track cyberthreats that move across different clouds and apps. AI helps with cloud security by analyzing data from all of these sources to identify vulnerabilities and potential cyberattacks.

- **Securing Internet of Things (IoT) devices with AI:** Much like endpoints and apps, organizations typically have many IoT devices that are potential cyberattack vectors. AI helps detect cyberthreats against any single IoT device and also uncovers patterns of suspicious activity across multiple IoT devices.

- **XDR and SIEM:** XDR and SIEM solutions pull information from multiple security products, log files, and external sources to help analysts make sense of what's happening in their environment. AI helps synthesize all of this data into clear insights.

Best practices for AI for cybersecurity

Using AI to support security operations takes careful planning and implementation, but with the right approach, you can introduce tools that make meaningful improvements in operational effectiveness and your team's wellbeing.

- Develop a strategy: Choose AI tools that address your security challenges and integrate well with your existing systems.
- Integrate security tools: Ensure AI tools like XDR and SIEM work together for full visibility across your organization.
- Manage data privacy and quality: Clean and protect data to ensure AI delivers accurate insights and decisions.
- Continuously test AI systems: Regularly test AI for bias and quality issues as new data is introduced.
- Use AI ethically: Prevent AI from making biased or unfair decisions by being mindful of data accuracy and transparency.
- Define generative AI policies: Set clear rules about how employees can use generative AI to protect sensitive information.

The future of AI for cybersecurity and solutions

The role of AI for security will only continue to grow. Over the coming years, security professionals can anticipate that:

- AI will get better at detecting cyberthreats with fewer false positives.
- Security operations teams will automate their more tedious work as AI gets better at responding to and mitigating a greater variety of cyberattack types.
- Organizations will use AI to help address vulnerabilities and improve security posture.
- Security professionals will still be in high demand.
- People will take on more strategic roles, such as addressing the most complex security incidents and proactive cyberthreat hunting.

It isn't just the security community that will get more effective with AI. Cyberattackers are also investing in AI and will likely use this technology to:

- Crack large amounts of passwords at once.
- Create sophisticated phishing campaigns that are difficult to distinguish from genuine emails.
- Develop malware that's incredibly difficult to detect.

As bad actors integrate more sophisticated AI into their cyberattack methods, it will become even more imperative for the security community to invest in AI to stay ahead of these cyberthreats.

References-

[1]Microsoft, “What Is AI for Cybersecurity?,” Microsoft Security. https://www.microsoft.com/en-in/security/business/security-101/what-is-ai-for-cybersecurity (Microsoft 2024).

[2] IBM, "Artificial Intelligence (AI) Cybersecurity," IBM, 2024. [Online]. Available: https://www.ibm.com/ai-cybersecurity. [2024].

[3] Red Hat, "4 Use Cases for AI in Cyber Security," Red Hat, 2024. [Online]. Available: https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security.

[4] S. B. Sagar, N. Kashyap, N. S. Niranjan, and S. D. N., "Providing Cyber Security using Artificial Intelligence – A Survey," in Proceedings of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019), IEEE, 2019, Art. no. CFP19K25-ART. ISBN: 978-1-5386-7808-4.

[5] M. A. Khder, S. Shorman, D. A. Showaiter, A. S. Zowayed, and S. I. Zowayed, "Review Study of the Impact of Artificial Intelligence on Cyber Security," in 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD), Manama, Bahrain, 8-9 March 2023. IEEE, 2023. doi: 10.1109/ITIKD56332.2023.10099788.

[6] A. Ali, M. A. Khan, K. Farid, S. S. Akbar, A. Ilyas, and T. M. Ghazal, "The Effect of Artificial Intelligence on Cybersecurity," in 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 7-8 March 2023. IEEE, 2023. doi: 10.1109/ICBATS57792.2023.10111151.

Student Editors

Indrakumar Naragude
(TY-IT-B)

Parth Musne
(TY-IT-B)

Vaibhav More
(TY-IT-B)

Shriyog Muley
(TY-IT-B)

Rohit Mutha
(TY-IT-B)