Generative AI Applications for Cybersecurity Teams

Accelerate, supplement, and uncover with Trend Micro

February 2024
Trend Micro

Contents

Generative AI is a New Opportunity for Security

Generative artificial intelligence (AI) is everywhere. Industries of all kinds see limitless applications for it, from accelerating medical research to generating dinner recipes. But what do recent strides in generative AI mean for cybersecurity teams?

Because the implications of generative AI are still evolving, some businesses are slower to adopt the technology, but the pace of adoption remains steady as organizations increasingly embed AI capabilities in their operations. Last year, 35 percent of companies were using AI for various purposes. One in every four companies is adopting AI to bridge labor and skills gaps, while two in every three companies are planning to apply AI to address sustainability goals.[1]

Generative AI's remarkable efficiencies have some serious potential to support cybersecurity teams in clear and confined ways. In particular, it can rapidly process vast quantities of data and communicate in natural language, both of which can support organizations' IT, development, and security teams.

What's the difference between AI and Generative AI?

Security teams can find AI in many of today's platforms, but the abilities and benefits are different than those of generative AI.

AI, including machine learning (ML), has been an integral part of various applications such as extended detection and response (XDR) solutions. ML excels at pattern recognition and behavioral analysis, while AI acts as a vigilant monitor in the security context, identifying potential threats based on the model's understanding of normal activities.

AI and ML in cybersecurity help us to identify patterns, analyze and predict threat activity, assess the tone and intention of email messages, and automate response. Further specific methods including data stacking and search based reduction help us to refine detection models to ensure we minimize false positives and surface important alerts within the mix and noise of raw logs.

Generative AI presents unique opportunities in the security vertical that are practical and easy to engage.

Today, we're integrating new generative AI technology to accelerate security operations and uplift security analysts through user-friendly chat assistants, custom threat response and risk remediation recommendations with prescriptive step-by-step guidance, and improving on-demand attack and phishing simulations.

Generative AI's adaptability and creativity make it a dynamic and disruptive tool in cybersecurity.

1. Trend Micro Midyear Cybersecurity Report, 2023

The 4 Core Benefits of Generative AI in Cybersecurity

Trend Micro has identified four primary benefits of using generative AI in cybersecurity, with more use cases actively in development. It's worth noting that these primary benefits can have secondary benefits, such as a higher employee retention rate, upskilling, and increased productivity. These use cases benefit analysts from junior to mid-level to senior analysts in different ways.

Let's look at four key ways cybersecurity teams can benefit from generative AI:

1. **Get time back.** Time is the most valuable currency of a security operations center (SOC). Generative AI reduces time spent on tasks using automation, freeing staff to focus on more proactive security processes. It can also surface prioritized tasks in new skills and interactive ways, which is often a challenge for security teams, helping them act faster.
2. **Reduce the impact of skills gaps and staff shortages.** For small- to mid-sized enterprises with constrained resources, generative AI can maximize the capabilities of existing staff. For large enterprises, it offers value in its ability to accelerate tasks such as searching, reporting, or setting up automated queries. In any organization, more junior team members can lean on generative AI to speed up processes while also learning from it. Senior staff can optimize routine tasks, freeing up more time to spend on value-adding initiatives.
3. **Improve mean time to understand.** Generative AI's capacity to efficiently process and logically assess huge volumes of data accelerates the time it takes to detect threats, aggregate insights, and remediate issues. It's ability to quickly explain what's happening in complex scenarios in easy-to-understand terms enables security experts to act swiftly. Teams can also effectively prioritize risks by using generative AI to rapidly identify which assets are most susceptible to specific threats.
4. **Speed time to value.** Generative AI amplifies the security analyst's work, helping on both the risk and threat side, without a lengthy ramp-up. Because it can be onboarded quickly and yields immediate benefits, organizations see a return on their investment soon after implementation.

92%

of surveyed executives say that generative AI is more likely to augment or elevate their security workforce than replace it.[2]

2. The CEO's Guide to Generative AI, IBM, 2023

Effective Use Cases for Every Organization

While Trend has identified more than 50 use cases for generative AI in the context of cybersecurity, we continuously work to prioritize and develop the most impactful applications for this emerging technology. Constant innovation in generative AI to embed it as both an integrated technology and a generally available assistant is proving to address pain points.

To get started with generative AI, we outline four use cases that are the fastest to implement and have the quickest time to value.

Explaining alerts

If you have complex multi-vector attacks touching emails, endpoints, workloads, and containers, for example, you can ask generative AI to provide contextual awareness in an easy-to-understand way that will prioritize responses. When a security team receives a threat alert, they must examine a significant amount of data to fully understand the situation. Generative AI can provide detailed information in natural language that offers context to security teams, including for more complex scenarios, so they can make informed decisions more quickly. For instance, if an alert comes through on suspicious activity in a containerized environment, a team member could ask a generative AI assistant, "Tell me more about what is happening in this containerized environment" for an instant explanation.

Script decoding

In a style of attack called fileless or "living off the land," hackers use something permissible or not overtly suspicious to deliver malicious scripts into the environment. Sometimes a security team sees a script and must investigate whether it is a threat. Now, when asked, generative AI can discern instantly if a script is malicious or benign. Since this is a harder skill set to learn, and more challenging to discern, it saves time and contributes to on-the-job training – particularly for tasks such as searching. From a skills gap perspective, this use can immediately neutralize adversaries' advantages. For seasoned security team members, this use case still creates a fast track to the end goal.

Searching and hunting

For searching telemetry or conducting full-blown threat hunting, generative AI can enable security teams to develop a hypothesis and generate better queries. It can translate a search to stronger, more sophisticated languages or syntax such as Kibana-style search languages. Organizations using plain-text search, for example, can generate a formal search language query to return higher fidelity results and pinpoint information quickly. Carrying out more efficient hunts is broadly useful, including to junior and senior analysts, and threat hunters.

Documentation and reporting

Trend supplies customers with a comprehensive repository of information to support self-help troubleshooting. While it's an essential resource, as with any large repository, it can be valuable to analysts to find the right information and the right answer—immediately and with fewer clicks. Generative AI removes that challenge as a practical time-saving finder. At request, it can surface relevant documents in any repository so teams can skip the time spent sorting through a long list of relevant results.

For reporting, time saved is even greater. Organizations have to report incidents which, depending on the complexity of an event, can take anywhere from 30 minutes to several hours. Generative AI can create a report entirely or, if security teams prefer, generate a draft they can edit and refine.

The Future of Security: What's Next for Generative AI?

Predictions are challenging to make because of the pace at which generative AI is evolving. But we're seeing emerging, creative applications that have the potential to become security best practices in the future.

Better risk management

The first is supporting how organizations handle risk to improve their security posture and better prevent incidents. When security risks go unaddressed, the likelihood of an event increases. Generative AI makes attack surface and exposure management more efficient. It does this by surfacing prioritized high-risk instances—including highly-exploitable vulnerabilities, security and cloud misconfigurations, and assets with observed attach techniques associated with them—in a user-friendly and accessible way. This practice can help close the gap between risk identification and remediation with a simple and familiar prompt-based interaction, integrated with their daily workflow. The opportunity for generative AI to enable security teams to access prioritization throughout the user interface, on demand, can offer a more flexible experience.

Step-by-step guidance

Generative AI is already improving user experiences and security outcomes by supplementing platforms through prioritizing and extending custom, contextualized, and prescriptive step-by-step guidance for both risk remediation and threat response. For example, when a security team receives an alert to a highly critical vulnerability, generative AI can deliver specific guidance on which assets are affected, their criticality, and how to patch the vulnerability to eliminate the risk.

Playbook creation

Finally, in the short-term, generative AI is likely to become a valuable asset in developing custom security playbooks, and when used in tandem with automation, can generate exponential time savings. This use case is ideal for SOC analysts looking for greater efficiency. For example, Trend provides playbook templates that customers can tailor to their requirements, but generative AI can help teams build custom templates from an entirely unique foundation for their environments and scenarios. From the beginning of the playbook drafting process, generative AI can provide a series of prompts, co-author a playbook, and build out automation—including endpoint response remediation, proactive risk remediation, and more.