Google’s AI plans now include cybersecurity

As people try to find more uses for generative AI that are less about making a fake photo and are instead actually useful, Google plans to point AI to cybersecurity and make threat reports easier to read.

In a blog post, Google writes its new cybersecurity product, Google Threat Intelligence, will bring together the work of its Mandiant cybersecurity unit and VirusTotal threat intelligence with the Gemini AI model.

The new product uses the Gemini 1.5 Pro large language model, which Google says reduces the time needed to reverse engineer malware attacks. The company claims Gemini 1.5 Pro, released in February, took only 34 seconds to analyze the code of the WannaCry virus – the 2017 ransomware attack that hobbled hospitals, companies, and other organizations around the world – and identify a kill switch. That’s impressive but not surprising, given LLMs’ knack for reading and writing code.

But another possible use for Gemini in the threat space is summarizing threat reports into natural language inside Threat Intelligence so companies can assess how potential attacks may impact them – or, in other words, so companies don’t overreact or underreact to threats.

Google says Threat Intelligence also has a vast network of information to monitor potential threats before an attack happens. It lets users see a larger picture of the cybersecurity landscape and prioritize what to focus on. Mandiant provides human experts who monitor potentially malicious groups and consultants who work with companies to

block attacks. VirusTotal’s community also regularly posts threat indicators.

The company also plans to use Mandiant’s experts to assess security vulnerabilities around AI projects. Through Google’s Secure AI Framework, Mandiant will test the defenses of AI models and help in red-teaming efforts. While AI models can help summarize threats and reverse engineer malware attacks, the models themselves can sometimes become prey to malicious actors. These threats sometimes include “data poisoning,” which adds bad code to data AI models scrape so the models can’t respond to specific prompts.

Google, of course, is not the only company melding AI with cybersecurity. Microsoft launched Copilot for Security , powered by GPT-4 and Microsoft’s cybersecurity-specific AI model, and lets cybersecurity professionals ask questions about threats. Whether either is genuinely a good use case for generative AI remains to be seen, but it’s nice to see it used for something besides pictures of a swaggy Pope.

https://www.theverge.com/2024/5/6/24150610/google-gemini-cybersecurity-mandiant