Microsoft to release security AI product to help clients track hackers

March 14 2024, by Dina Bass, Bloomberg News

Credit: Unsplash/CC0 Public Domain

Microsoft Corp. plans to release artificial intelligence tools on April 1 that will help cybersecurity workers produce summaries of suspicious incidents and ferret out the devious methods hackers use to obscure their

intentions.

Microsoft unveiled its Copilot for Security about a year ago and has been trialing it with corporate customers ever since. Testers include BP Plc and Dow Chemical Co. and now number "hundreds of partners and customers," according to Andrew Conway, Microsoft's vice president of security marketing. Customers will pay a fee based on usage, much as they do with the company's Azure cloud services.

The security Copilot is part of Microsoft's ongoing effort to infuse its major product lines with artificial intelligence tools from partner OpenAI and persuade corporate customers to buy subscriptions.

While AI can help generate content and synthesize corporate data, it also makes errors that can be costly or embarrassing. Because computer security is so critical and the risks so high, Conway said the software giant has taken extra care with this Copilot. The software combines the power of OpenAI's model with the massive troves of security-specific information that Microsoft collects.

"There are a number of things, given the seriousness of the use case, that we're doing to address [risks]," he said, including seeking constant feedback on the product and where it falls short. "All of that said, security is still a place today where security products generate false positives and generate false negatives. That's just the nature of the space."

The Copilot works with all of Microsoft's security and privacy software, offering an assistant pane that can produce summaries and answer questions. For example, one of the company's security programs already collects a variety of security alerts and combines the related ones into a single incident.

Now, when a user clicks on each incident, the Copilot can summarize the data and write a report, a typically time-consuming process. Often during an attack, hackers will use complicated programming scripts to obfuscate what they're trying to do, making it harder to track. The Copilot is designed to explain the attacker's aim.

The software will free up experienced cybersecurity workers for more complex tasks and help newer ones get up to speed more quickly as well as supplement their skills, Conway said. In its tests, Microsoft said newer security workers performed 26% faster and with 35% more accuracy. That's helpful because the cybersecurity industry is suffering from a chronic labor shortage.

Microsoft said the AI program can also link to security software from rival companies, not just Microsoft's.

Twenty to 30 BP employees have been testing the Copilot, said Chip Calhoun, the oil giant's vice president of cyber defense. Setting it up required just one or two clicks, he said, but it took a few months for his security professionals to really get used to using the tool. Some members of his team are using the Copilot to hunt for threats, relying on the AI to quickly scan masses of data and alerts for evidence of security compromises.

More experienced analysts can ask the tool questions—in plain English sprinkled with security speak the AI is trained to understand. For example, an analyst could ask for evidence that a hacker is moving through BP systems using "living off the land techniques," a type of attack that uses a network's own tools to evade security defenses. Such intrusions are popular with Russia- and China-linked hackers.

"The bad guys are getting faster, and we're having to get faster as well, so tools like this really help us," said Calhoun, whose team also builds its

own customized AI tools from publicly available models. "It's not perfect yet. It will get perfect."