Best practices AI and machine learning Microsoft Copilot for Security

5 min read

Microsoft Copilot for Security provides immediate impact for the Microsoft Defender Experts team

By Andrew Conway, Vice President, Security Marketing

February 8, 2024

Microsoft Defender Experts for Hunting Microsoft Defender Experts for XDR

Microsoft Security Experts

Organizations everywhere are on a lightning-fast learning trajectory to understand the potential of generative AI and its implications for their security, their workforce, and the industry at large. AI is quickly becoming a force multiplier—presenting significant opportunities for security teams to increase productivity, save time, upskill resources, and more. News and information about "the age of AI" is everywhere. But while AI generates a lot of buzz, it's not all just talk. Microsoft Copilot for Security is already showing immediate impact for security teams at Microsoft.

Our own Microsoft Defender Experts team has been using and exploring Copilot, and finding new ways it can streamline, inform, and optimize their daily work—from improving communication clarity to data analysis and upskilling. Through their work on the Microsoft Defender Experts for XDR service, they serve as an extension of our customers' security operations center (SOC) teams. They proactively hunt for serious cyberthreats using Microsoft Defender data. They triage, investigate, and expose advanced threats, identify the scope and impact of

malicious activity, and then take action on a customer's behalf to remediate the incident. And now with Copilot, Defender Experts have a powerful new security tool.

Microsoft Copilot for Security

Powerful new capabilities, new integrations, and industry-leading generative AI.

Learn more >

A leadership view of Copilot for Security

In this new series of short videos, our Defender Experts share real-world scenarios where Copilot is helping them navigate threat detection, investigation, and managed response. To begin, Ryan Kivett, Partner Group Manager for Defender Experts, Microsoft, shares his leadership view on how Copilot helps support learning and career growth for his team. Then Brian Hooper, Principal Research Lead for Defender Experts, Microsoft, talks about how Copilot can help minimize the mundane tasks that take security analysts away from their most important work—serious threat investigations.

Watch the video "A leadership view on deploying Copilot."

Save time and increase efficiency

From a leadership level, it's easy to see the potential of Copilot. But when every second counts—like during an active security incident—that potential needs to be fully realized and actionable. Copilot for Security puts critical guidance and context into the hands of your security team so they can respond to incidents in minutes instead of hours or days. In our next video clip, Phoebe Rogers, a senior member of the Microsoft Defender Experts analyst team, shares how Copilot helps her shave minutes off every script analysis—which adds up to real saved time, increased efficiency and understanding, and greater incident insight. Watch as she shares how she uses Copilot to analyze a suspicious script, step by step.

Watch the video "Script Analysis."

When security analysts communicate with customers, they need to provide a clear, concise, and comprehensive summary of an active incident in a timely manner, so customers have a deep understanding of the situation. In the following video, Brian Hooper shares a detailed walkthrough of how Copilot is helping analysts write up these incident narratives 90% faster than in the past.

Watch the video "Incident Summaries."

Upskill junior analysts and develop critical expertise

Most complex and sophisticated attacks like ransomware evade detection through numerous ways, including the use of scripts and PowerShell. Moreover, these scripts are often obfuscated, which adds to the complexity of detection and analysis. In our next video, Brian Hooper shows how the detailed, line-by-line script examination in Copilot allows security analysts to quickly assess and identify a script as malicious or benign. It also helps junior security analysts upskill their expertise. With Copilot, any analyst can use natural language prompts to initiate and perform tasks that they may not have a lot of experience with or expertise in, and the outputs of Copilot will help them both accomplish the right results quickly, and, more importantly, help them develop those critical skills for long-term use.

> "Copilot for Security really helps our junior analysts, as if they had a coach next to them, guiding them through the learning phase of their role. And for our senior analysts, it's really helping them push past what would have otherwise been possible, in terms of reaching their potential."
>
> *—Ryan Kivett, Partner Group Manager for Defender Experts, Microsoft*

Watch the video "Script Analyzer in Defender."

Get rich, contextual information with threat intelligence

Understanding an organization's external threat surface can take a lot of time and tools. Often, analysts must go to multiple repositories to obtain the critical data sets they need to assess a suspicious domain, host, or IP address. DNS data, WHOIS information, malware, and SSL certificates provide important context to indicators of compromise (IOCs), but these repositories are widely distributed and don't always share a common data structure, making it difficult to ensure analysts have all relevant data needed to make a proper and timely assessment of suspicious infrastructure. Getting threat intelligence data and rich, contextual information from Microsoft Defender Threat Intelligence and Copilot helps security analysts make determinations, like whether an IP is malicious or not. In the next video clip, Phoebe Rogers uses Defender Threat Intelligence and Copilot to compare a user's sign-in properties with their authentication history, surfacing the relevant information to streamline her analysis and determine whether or not it's a threat.

Watch the video "Getting threat intel data."

Once a determination is made, it can still take time and effort for an analyst to summarize and communicate a threat to affected parties. But Copilot can help. In our last video clip, Phoebe explains how Copilot can quickly explain the impact of common vulnerabilities and exposures (CVEs) and summarize relevant content like impacted products, bad actors known to exploit the vulnerability, and mitigation recommendations.

Watch the video "CVEs and Vulnerabilities."

Protect at the speed and scale of AI

When faced with incomplete and imperfect data and the need to investigate a potential threat, communicate that threat to a customer, or craft a timely response, security analysts are realizing tangible, measurable benefits from using Copilot in their daily work. It helps them protect and defend their organization at machine speed and scale. Of course, the ability to leverage generative AI is not exclusive to security teams. It may also be leveraged by potential threat actors. So, the sooner security teams can experience and evaluate generative AI to augment and improve their security, the better. That's why Brian Hooper encourages department leadership who are building their plan to deploy Copilot within their team to encourage exploration. "Let the team try different prompts. Let the team summarize incidents. Let the team analyze scripts. Let the team find out about intelligence that Microsoft knows about attacks. Organically, they will find all different places that it's going to help them."

Learn more

To learn more about Microsoft Copilot for Security, visit the product page, and for more helpful tips and information, view the Copilot for Security Playlist on the Microsoft Security Channel on YouTube.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (@MSFTSecurity) for the latest news and updates on cybersecurity.