Microsoft Security

Speed, Accuracy and Sentiment

Gains you can get with Copilot

In a randomized controlled trial (RCT), we tested 147 security professionals to measure the productivity impact from using Microsoft Copilot for Security.

We randomly gave Copilot to some analysts and not others, and then we subtracted their performance and sentiments to get the effect of Copilot, separate from any base effect. Study participants were experienced security professionals. **The results were astounding.**

Speed

Security professionals with Copilot were **22%** faster.

- **14%** faster at analyzing scripts.
- **19%** faster at analyzing incident reports.
- **39%** faster at summarizing an incident.

Accuracy

Security professionals with Copilot were **7%** more accurate.

- **12%** more accurate at script analysis.
- Analysts using Copilot created incident summaries with **49%** more incident facts.

Sentiment

97% of Security professionals said they want Copilot next time they do the same task.

- **93%** reported Security Copilot helped them improve the quality of their work.
- **85%** reported Copilot reduced effort on the task.
- **92%** reported Copilot made them more productive.

With the growing cost of security breaches, organizations need every advantage to protect against skilled and coordinated cyber threats.

To see more and move faster, they need generative AI technology that complements human ingenuity and refocuses teams on what matters.

Microsoft Copilot for Security is a generative AI-powered assistant for daily operations in security and IT. Copilot empowers teams to protect at the speed and scale of AI by turning global threat intelligence, industry best practices, and organizations' security data into tailored insights to outsmart and outpace adversaries.

The findings are based on our study of 147 security professionals.

Years Experience	<=2	3-4	5-8	>8
Analyst Level	1	2	3	4
Subject Count	9	28	58	52

Randomized controlled trial (RCT) methodology

We granted half of subjects ("treatment subjects") access to standard Microsoft Defender XDR (Defender XDR) with Microsoft Copilot for Security ("Copilot") features. The other half ("control subjects") had standard Defender XDR without Copilot features. We assigned subjects randomly to groups. Thus, the difference between treatment and control outcomes yields a measurement of the causal impact of Copilot – how we expect outcomes to change if an average control subject uses Copilot.

Our test environment included two sample scenarios. The first is a multi-stage, hands-on keyboard ransomware attack involving lateral movement, PowerShell script execution, and the use of Microsoft OneNote and Group Policy Objects to distribute payloads. The second is a BEC financial fraud attack involving a compromised inbox used for lateral movement as well as inbox rule creation, sending suspicious BEC emails, and deleting sent emails.

We provided subjects with an introduction to Defender XDR, then gave them a series of tasks including multiple-choice questions and an incident summary essay. We timed their work in all tasks.

Learn more: https://aka.ms/copilotforsecurity