

AI-Empowered Security with Microsoft Copilot

Driving efficiency in security operations at the speed and scale of AI

Business drivers

Aside from traditional security challenges around threat intelligence, data security and IT efficiency, organizations also suffer from challenges in its security operations center (SOC):

- ▶ Scarce security talent and skills to meet market demand with lack of automation in analyzing data and investigating alerts
- ▶ Complexity of security operations tasks with a myriad of disconnected products
- ▶ Difficulty of enriching and contextualizing data for full investigation and converting indicator of compromise (IoC) into mitigation

Solution overview

AI-Empowered Security with Microsoft Copilot is a generative AI (GenAI)-powered security solution that helps increase the efficiency and capabilities of defenders to improve security outcomes at machine-speed and scale, while remaining compliant to responsible artificial intelligence (AI) principles. It works by:

- ▶ Combining data from your security tools to provide customized guidance for your organization
- ▶ Supporting security professionals in end-to-end scenarios, such as incident response, threat hunting, intelligence gathering and posture management

Solution benefits

By leveraging advanced technologies and automation to rapidly transform security operations, the AI-Empowered Security with Copilot solution assists organizations in:

- ▶ **Augmenting the human experience** to enhance skills, reduce training gaps and help enable analysis
- ▶ **Increasing speed and efficiency** to help enable automated intelligence gathering, accelerate investigation, and reduce response time and time-consuming tasks
- ▶ **Improving scalability and reporting** to reallocate analysts for critical incidents handling and generate audience-targeted reporting and contextual summarization

Problem statement

Cybersecurity staffing and skills shortage

- ▶ Analyst shortage intensifies with growing digital transformation

Manual security data analysis

- ▶ Workflow disruption due to complex alert investigation and tool switching for analysts

Alert artifacts require enrichment

- ▶ Alert investigation demands manual data enrichment and security playbook configuration

Incident response

- ▶ Complex infrastructure complicates incident scope identification and triage

AI-Empowered Security with Microsoft Copilot solution

AI triage

Streamlines alert analysis and triage, reducing skill barriers for quality assessments

Automatically-generated insights

Curate data for user-friendly security investigations within Microsoft tools

Orchestrated intelligence gathering

Automates context identification and enrichment with Microsoft intelligence and third-party plugins

Incident impact investigated by AI

Identifies potential asset impacts and compromises by analyzing alerts

Joint value proposition

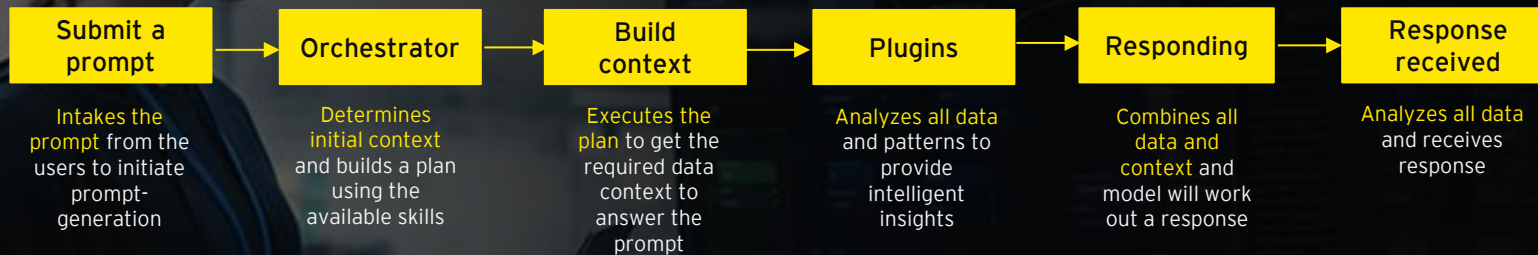
- ▶ The EY organization has driven various third-party integrations, developed data visualizations for identifying incident trends and changes in data ingestion, and built alert triage strategies.
- ▶ With Microsoft's SOC transformation experience, the solution helps clients streamline transition processes, enhance deployment and accelerate modernization of security operations.
- ▶ The EY teams' experience in threat-response and compliance integrated with Microsoft's AI-powered cybersecurity technology increases the clients' SOC efficiency and capabilities, which helps address security issues quickly and responsibly.

Solution differentiators

The solution helps the EY organization and Microsoft gain a competitive advantage in the marketplace by:

- ▶ Combining an improved language model with Microsoft's security features, informed by global threat intelligence and over 65 trillion daily signals.
- ▶ Augmenting the ingenuity and experience of cybersecurity professionals with the capabilities, processing speeds and adaptability of AI.
- ▶ Integrating the data and signals from other Microsoft security products to generate customized guidance.

How AI-Empowered Security with Microsoft Copilot works



Products integrated with Copilot for Security



Key use cases

- ▶ Investigation and summary creation of security incidents
- ▶ Find threat actor names and tactics, techniques and procedures (TTPs) and provide threat intelligence indicators
- ▶ Reputation check for IP addresses and domains
- ▶ Check authentication methods enabled for the users involved and entities related
- ▶ Mitigation and defense techniques to protect
- ▶ Generate reports

Contacts

EY



Nicole Koopman
Managing Director
Ernst & Young LLP
nicole.koopman@ey.com

Microsoft



Jodi Lustgarten
Microsoft Alliance Director
Microsoft Corporation
jodise@microsoft.com

EY and Microsoft: Helping the world work better to achieve more

Every day, throughout the world, businesses, governments and capital markets rely on EY business ingenuity and the power of Microsoft technology to solve the most challenging global issues.

EY and Microsoft bring a compelling formula to spark the potential of the cloud and unlock the power of data. We solve our clients' most challenging issues by blending trusted industry expertise with innovative cloud technology. Our strategic relationship draws on decades of success developing visionary solutions that provide lasting value.

For more information, visit: ey.com/Microsoft.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.



EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2024 EYGM Limited.
All Rights Reserved.

EYG no. 009222-24Gbl
CSG no.
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com