Deliver value by redefining security operations with AI.

Microsoft Security Copilot enabled by KPMG

KPMG (LLP) is helping organizations strategically deploy Microsoft Security Copilot to drive actionable insights, augment and automate security workflows, and increase the ability of Security Operations Center (SOC) professionals to manage incidents, threats, and vulnerabilities across the enterprise at increased scale. We achieve this through a business-led, technology enabled approach informed by a decades-long global alliance with Microsoft.

Microsoft Security Copilot improves the efficiency and effectiveness of your security professionals.

Results from a recent study* indicate that organizations can significantly improve the efficiency and effectiveness of their incident response professionals by using Microsoft Copilot for Security to drive processes within Security Operations Centers (SOC).

22%

faster end-to-end security incident management[1]

43%

more accurate security incident response[1]

72%

of IT professionals are prioritizing AI for security[2]

Statistics indicate a 22% faster end-to-end security incident management for security experts and 43% more accurate security incident response for junior analysts, allowing you to keep up with your peers and capitalize on innovation.*

This technology empowers your SOC teams to manage workflows more effectively by guiding remediation, accelerating documentation, and assessing incidents, alerts, threats, and vulnerabilities within your organization's unique technology ecosystem.

[1] Source: KPMG 2023 Generative AI Survey Report: Cybersecurity
[2] Source: Microsoft Randomized Controlled Trial for Copilot for Security (2024)

Microsoft Security Copilot can enhance the capabilities of Security Operations Centers.

Microsoft Security Copilot is an AI-powered security solution that generates insights based on data from applications across Microsoft's security stack, including Microsoft Defender and Microsoft Sentinel. Microsoft Security Copilot provides both standalone and embedded user experiences, delivering capabilities such as guided incident response, malicious script analysis, and attack surface summarization from a central application or within other Microsoft tools.

Out-of-the-box integrations with Microsoft and non-Microsoft tools in combination with custom plugins enable organizations to leverage data from across their cybersecurity program to drive value.

● Available as Microsoft Security Copilot Plugin

Identity & Access

Microsoft Tools & Capabilities

● Entra	Passwordless & MFA | ID Protection | ID Governance | PIM | External Identities

People Security

Supporting Programs

Attack Simulations	Insider Threat	Communications

Information Protection

Microsoft Tools & Capabilities

● Purview	File Scanner | Data Governance & Classification Advanced eDiscovery | Compliance

Informs

Monitors

Security Operations Center

Augmented with Microsoft Security Copilot

Centralized real-time and continuous monitoring, detection, and defense of technology assets, leveraging enterprise cyber data

● Defender XDR	Incident Response | Automation | Threat Hunting | Threat Intelligence
● Sentinel	Security Information & Event Management (SIEM) | Security Orchestration, Automation & Response (SOAR) | User & Entity Behavior Analytics (UEBA)

Feeds

Endpoint & Device Security

Protective measures and tools, such as vulnerability management and configuration management aimed at securing endpoints on a network, such computers, laptops, and devices.

Microsoft Tools & Capabilities

Defender for Endpoint	Web Content Filtering | Endpoint Data Loss Protection Threat & Vulnerability Management | EDR
● Intune	Mobile Device Management (MDM) | Mobile Application Management (MAM)

Infrastructure Security

Safety of on-prem and cloud-based IaaS/PaaS networks, servers, and data centers that establish the IT backbone of an organization.

Microsoft Tools & Capabilities

● Azure	WAF | DDoS Protection | Key Vault Bastion Firewall | Lighthouse
Defender for Cloud	Threat & Vulnerability Management | Detection & Response Capabilities

IoT & OT Security

Protection of both interconnected, smart devices (IoT), and operational technology (OT) systems that manage physical and industrial operations.

Microsoft Tools & Capabilities

Defender for IoT and OT	Asset & Vulnerability Management | Detection & Response

Software-as-a-Service (SaaS) Security

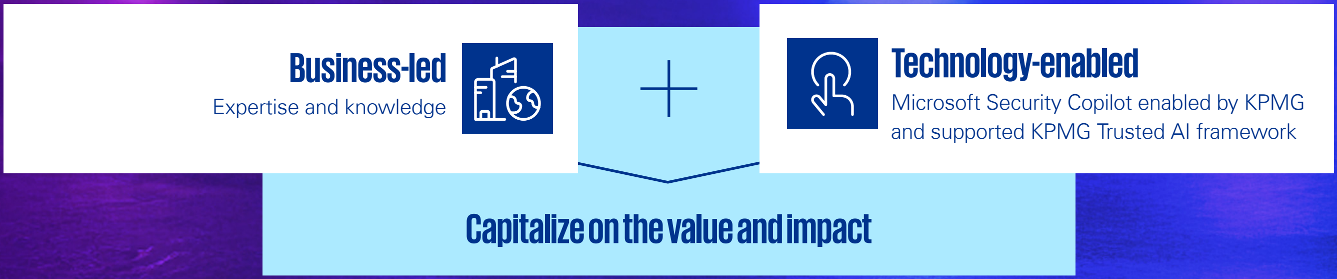
Protection of data, credentials, and interactions within cloud-based Software-as-a-Service applications and platforms.

Microsoft Tools & Capabilities

Defender for Cloud Apps	Discovery & Risk Scoring | Detection & Response Policy Audit /Enforcement | Session Monitoring | DLP
Entra Internet Access	Passwordless & MFA | External Identities

KPMG can help you capitalize on the value and impact of Copilot for Security.

KPMG is helping SOCs redefine their operations with a focus on AI enablement and Microsoft Security Copilot capabilities, enabling them to deliver business impact and value across the organization.



Business-led
Expertise and knowledge

+

Technology-enabled
Microsoft Security Copilot enabled by KPMG and supported KPMG Trusted AI framework

Capitalize on the value and impact

Our team of cybersecurity and AI professionals bring domain and technology-specific expertise to every client challenge, bridging the gap between data science and security proficiency. By combining this expertise with our KPMG Trusted AI framework and established organizational change program, we customize solutions to meet the strategic needs of each organization, empowering cybersecurity professionals with the right tools to drive positive change – all while improving the efficiency and accuracy of security operations.

The combination of this expertise and experience in implementing Microsoft solutions enables organizations to **capitalize on the value and impact** of Microsoft Copilot for Security within their technology ecosystem.

Through a phased deployment approach, KPMG can help you deliver measurable outcomes.

This phased deployment approach for enabling Microsoft Security Copilot considers the wide-reaching implications of GenAI-embedded workflows, ensuring organizations are prepared to drive value from reshaping the way their cybersecurity programs operate.

From strategic analysis to prioritizing use cases and from Proof of Concept (PoC) to redefining security operations, we help organizations automate and augment end-to-end workflows in multiple SOC domains.

The security GenAI enablement lifecycle

Strategy and process design

- **Define and document AI-enabled SOC processes** that factor in the potential of Microsoft Security Copilot.
- **Deliver a prioritized use case backlog** that recommends an initial proof-of-concept and documents tangible business impact.
- **Assess technical dependencies**, level-of-effort, and resource requirements for the implementation of each use case.

Proof-of-Concept

- **Demonstrate feasibility and value** by implementing highest ROI Microsoft Security Copilot use cases in a limited capacity.
- **Define AI enablement model** for the ownership and implementation of additional Microsoft Security Copilot use cases.
- **Explore customization** by identifying opportunities for custom plugins and data from sources outside the MS security stack.

End-to-end AI integration

- **Deploy Copilot for security at scale** by integrating AI capabilities throughout SOC workflows, including incident, threat and vulnerability management.
- **Conduct training with socialize capabilities** with an organizational change management effort that ensures security professionals can tap into the potential of Microsoft Security Copilot.

Managed support

- **Ongoing technical support of AI solutions** with a team of data scientists and security experts that owns long-term maintenance and enhancement
- **Managed detection and response** function that expands your capacity and leverages AI-enabled security processes to protect the organization (optional)

	Strategy and process design	Proof-of-Concept	End-to-end AI integration	Managed support
Outcome	AI augmented process definitions and prioritized roadmap	Tangible demonstration of value from Copilot for Security	AI-Integrated SOC workflows	Long-term support for AI solutions and additional SOC capacity
	Trusted AI Framework	**Organizational change management**	**Data science and security expertise**	**Value quantification**

SOC Use Cases

We have a comprehensive understanding of what end-to-end SOC operations should entail. We integrate use cases that enhance your existing workflows, driving outcomes and delivering tangible results.

Threat Management

Microsoft Security Copilot Use Cases	Outcome
Identify threats facing organizational assets, based on context from Microsoft threat intelligence	👥 🔍
Determine defenses along attack paths adversaries will likely take to threaten organizational assets	👥 » 🔍

Incident Management

Microsoft Security Copilot Use Cases	Outcome
Summarize and contextualize security alerts using data from Defender XDR and the Microsoft security stack	👥 🔍
Dynamically classify, prioritize, and reprioritize security alerts to assist with delegation and reporting	🔍
Generate KQL queries to explore structured security data when given a natural language prompt	👥 🔍
Summarize multiple forms of malicious content in natural language	👥 🔍
Recommend step-by-step incident response actions including containment, and remediation, then enact response actions directly from Copilot.	👥 » 🔍
Create closure documentation that synthesizes content from many sources and documents	📄
Identify data loss caused by incidents, and summarize data security and compliance impacts	🔍 🏛
Create after-action reports that use enterprise data to recommend process optimizations	🔍 📄
Define Sentinel playbooks that use Azure Logic Apps to streamline typical incident response flows	👥 »
Create simulation plans with scenario details, necessary team members, and success criteria	📄

Vulnerability & Attack Surface Management

Microsoft Security Copilot Use Cases	
Query and summarize attack surfaces for the organization, specific platforms, and assets, including metadata and key info	👥 🔍
Search for common vulnerabilities using natural language, such as expired certificates, open ports, and outdated software	👥 🔍
Determine whether assets are impacted by CVE vulnerabilities with a natural language search	👥 🔍
Integrate with vulnerability scanners, to interact and synthesize larger vulnerability datasets with AI	🔍
Identify critical vulnerabilities using CVSS to prioritize remediation efforts	👥 🔍
Recommend vulnerability remediation, including example code, command prompts, and step-by-step instructions	👥 » 🔍
Create closure documentation that recaps remediation steps, timeline, lessons learned, and other analyses	📄

- 👥 Increased capacity of SOC professionals
- » Accelerated remediation
- 🔍 Complete and accurate analyses
- 📄 Consistent and automated documentation
- 🏛 Risk and compliance awareness

So, why work with us?

Microsoft Security Copilot enabled by KPMG can revolutionize how SOC's operate.

As with any technology deployment, the expected return on investments comes faster with help.

KPMG can help deliver new business value so you can gain competitive advantage and win in your market.

KPMG and Microsoft – Strategic Global Alliance

The KPMG and Microsoft suite of solutions allow organizations to better manage their risk, compliance and security agendas, create meaningful data insights to inform intelligence decision making, and take advantage of the latest innovative technologies to drive new business value and growth.

Are you ready to deliver new business value? If so, contact us today:

Jim Wilhelm
Principal, Advisory
KPMG Cyber Security Services
E: jameswilhelm@kpmg.com

Joan Qafoku
Director, Advisory
KPMG Cyber Security Services
E: jqafoku@kpmg.com

Learn about us: in **kpmg.com**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.