Synergy Advisors - Copilot for Security Hands-On-Lab [HOL]

A Next-Gen AI-Powered Security Solution for Enhanced Efficiency and Capabilities of defenders to improve security outcomes at machine speed and scale.

The odds are against today's security analysts

In today's digital age, cybersecurity is crucial. Our digital defenses are constantly tested by password attacks, phishing e-mails, and a shortage of skilled professionals. Protecting our digital assets has become a top priority for individuals, businesses, and governments.

4,000	72 mins	3.5M
...Password attacks per second tests the fortitude of our digital defenses	...Median time for an attacker to access your private data if you fall victim to a phishing e-mail	...Global shortage of skilled cybersecurity professionals

Defenders urgently require a fresh approach to address evolving cybersecurity challenges

In the rapidly evolving digital landscape, the realm of cybersecurity stands as a crucial bastion against a barrage of threats. However, despite advancements in technology and strategies, defenders find themselves facing a myriad of challenges. Defenders need a new way to tackle new threats:

Disconnected processes

Current disjointed processes can result in gaps in threat detection and response, necessitating streamlined and integrated workflows to enhance overall security effectiveness.

Complex toolset

The complexity of existing cybersecurity tools makes it challenging for organizations to manage and maintain their security posture efficiently. Simplifying toolsets or providing better integration options can alleviate this burden.

Shortage of talent and expertise

A lack of skilled cybersecurity professionals may hinder organizations' ability to identify and respond to threats promptly. Investing in training and development programs can help bridge this gap.

Posture drift

Changes in the cybersecurity landscape can lead to posture drift, where outdated security controls or lack of regular reviews leave organizations vulnerable. Implementing regular assessments and proactive monitoring can mitigate this risk.

Inefficient collaboration

Collaboration inefficiencies can cause delays in threat detection and response efforts. Improving communication channels and fostering a culture of collaboration can enhance overall response capabilities.

Sophisticated attack techniques

Cyber adversaries continually evolve their tactics, making it challenging for organizations to keep up. Investing in advanced detection and response capabilities can help organizations better defend against these evolving threats.

Introducing Microsoft Copilot for Security

This pioneering and generative AI security product is designed to empower security and IT teams to defend the organization at unprecedented machine speed and scale. Elevating the efficiency and capabilities of defenders, Microsoft Copilot for Security enhances security outcomes and upholds a commitment to responsible AI principles, ensuring a comprehensive and compliant approach to digital defense.

How does Copilot for Security work?

Microsoft Copilot for Security enhances security capabilities through both standalone and embedded experiences within various Microsoft security products. The integration of foundational language models and proprietary Microsoft technologies forms a cohesive system that boosts defenders' efficiency and expands their capabilities, ultimately elevating security outcomes at machine speed and scale.

Here you will find a variety of questions, all in natural language, which are just examples of what Copilot for Security could provide a response to.
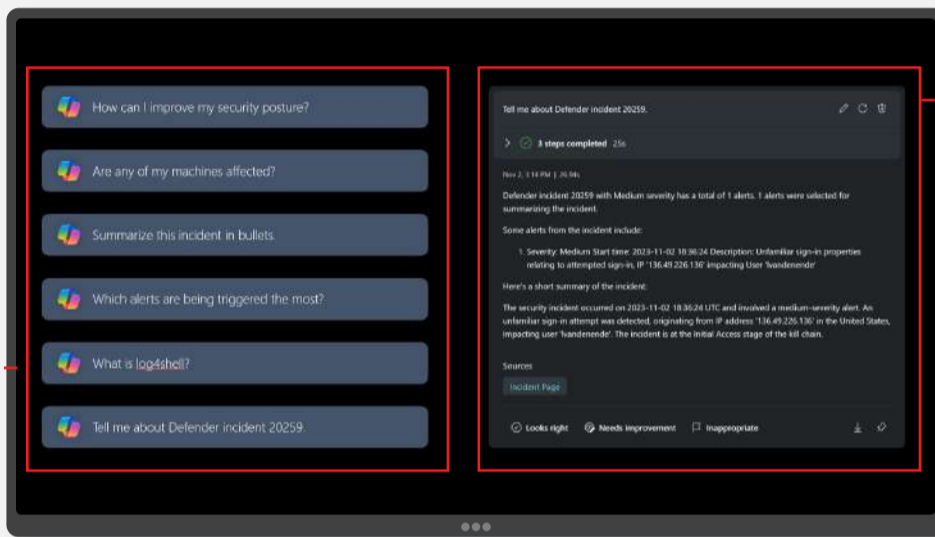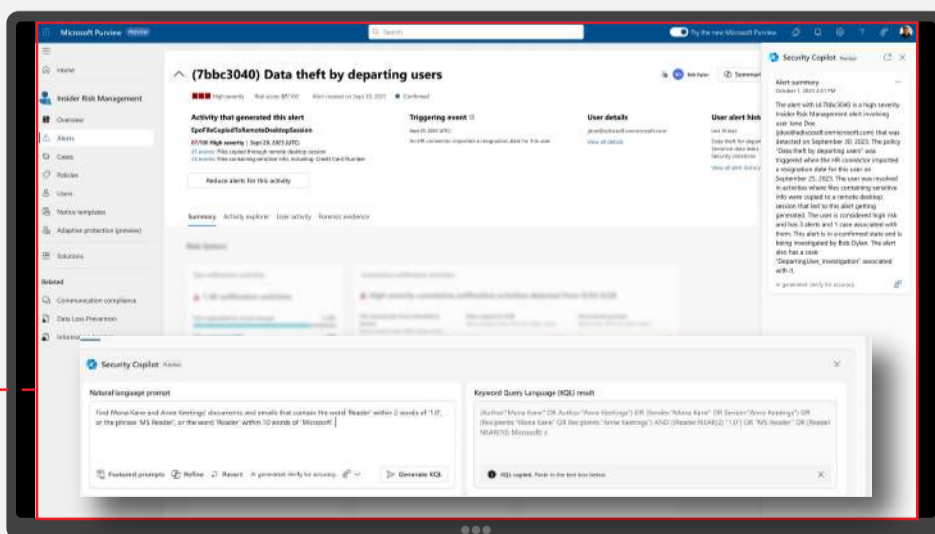

You'll find Copilot for Security's response: It includes the start time, IP, and user involved. The incident is noted to be in the initial access stage of the eradication chain, all summarized in a single, natural language message.
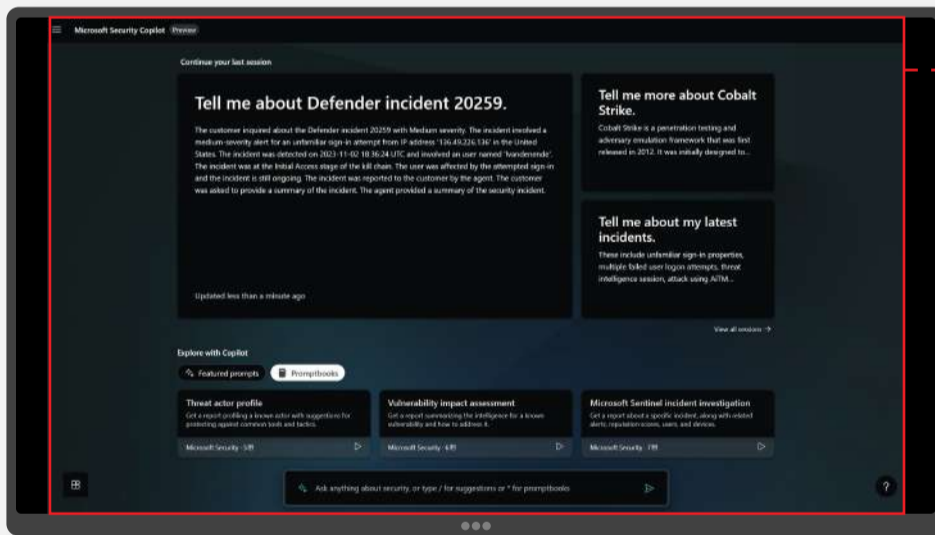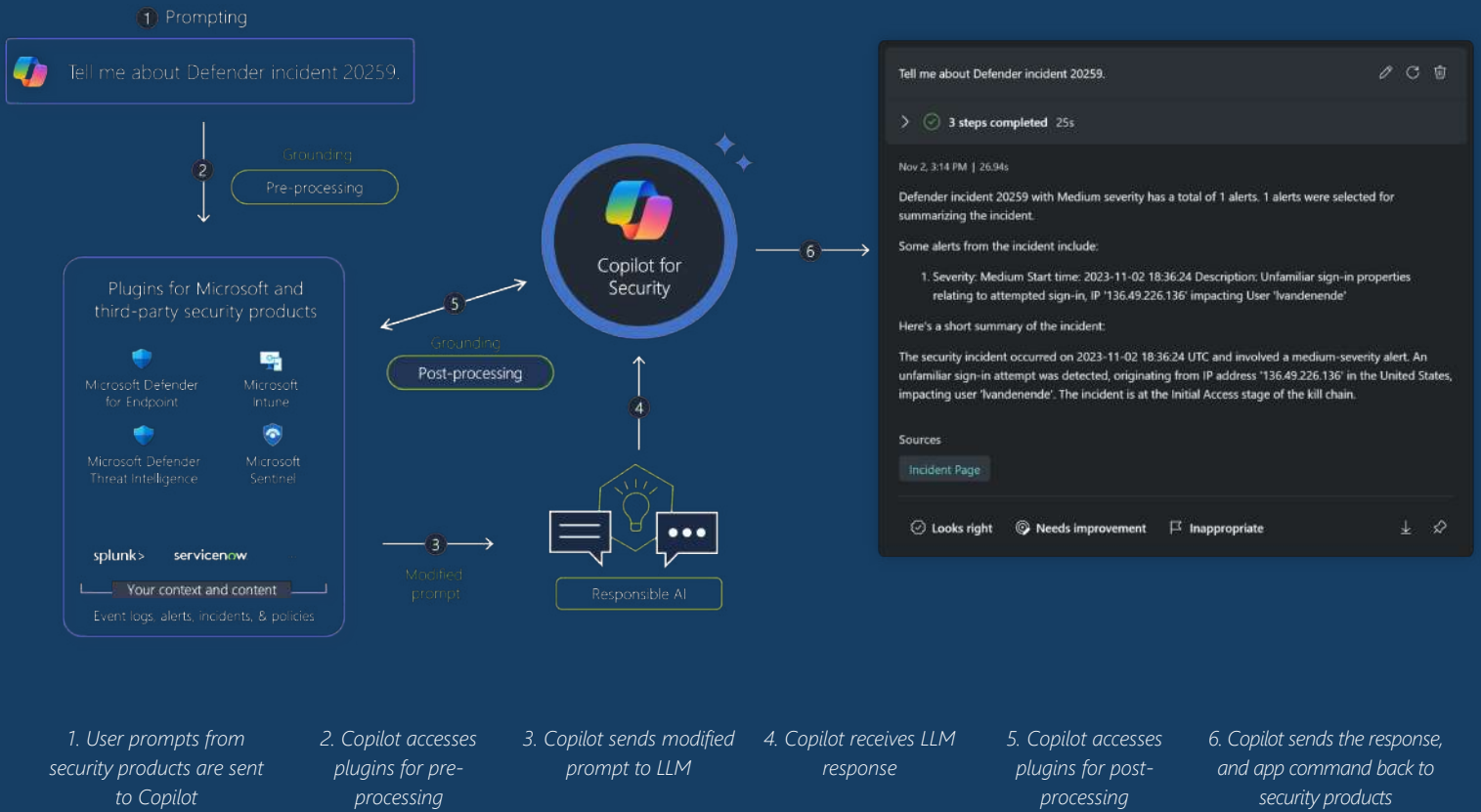
Standalone: Helps teams gain a broader context to troubleshoot and remediate incidents faster within Copilot for Security itself, with all use cases in one place, enabling enriched cross-product guidance.

Embedded: Offers the intuitive experience of getting Security Copilot guidance natively within the products that your team members already work from and are familiar with.

Data Flow Architecture - Copilot for Security

1. User prompts from security products are sent to Copilot

2. Copilot accesses plugins for pre-processing

3. Copilot sends modified prompt to LLM

4. Copilot receives LLM response

5. Copilot accesses plugins for post-processing

6. Copilot sends the response, and app command back to security products

Unlocking Security Excellence: Copilot for Security Value Proposition

Automated Repetitive Tasks

Automates repetitive tasks such as alert classification, threat investigation, and incident response. This frees up security analysts' time to focus on more strategic and high-value tasks.

Faster Threat Detection and Response

Leveraging AI, Copilot for Security detects and responds to threats faster and more accurately than humans. This can help organizations reduce incident response times and minimize the impact of threats.

Enhanced Visibility and Situational Awareness

Provides security teams with a unified view of all threats and vulnerabilities in their environment. This helps improve their understanding of the threat landscape and make more informed decisions on how to protect their organization.

Reduction in Security Costs

Can assist organizations in reducing security costs by automating tasks, improving efficiency, and reducing incident response times.

Regulatory Compliance

Copilot for Security aids organizations in complying with security and privacy standards by automating compliance tasks and detecting potential violations.

Optimized SecOps leveraging Microsoft Copilot for Security

Step into the realm of advanced cybersecurity with our hybrid **Hands-On-Lab [HOL]** experience, where we delve deep into the transformative capabilities of Microsoft Copilot for Security. Join us as we embark on a journey to revolutionize your SecOps strategy through the power of AI-driven insights and recommendations.

By participating in this Hands-On-Lab, you will...

Gain a deep understanding of Microsoft Copilot for Security and its role in revolutionizing SecOps.

Learn how to swiftly respond to cybersecurity threats and assess risk exposure with machine speed.

Explore practical scenarios to analyze risks, incidents, and false positives using Copilot's Gen-AI technology.

Maximize Microsoft Copilot's potential by using its automation capabilities to execute multiple tasks (promptbooks) and send alerts to your SOC team based on Gen-AI analysis.

Hands-On-Lab Phases - [3-4 Hours]

Introduction to Microsoft Copilot for Security	Hands-on-lab Overview	Explore Scenarios (Up to two)	Maximize Copilot's Automation Capabilities
Understand the fundamentals of Copilot and the evolving cybersecurity threat landscape: Microsoft Copilot fundamentals • AI concepts • Prompt engineering • Promptbooks • Automation (overview) • Pricing and usage monitoring	We begin the technical discussion by reviewing a lab diagram and presenting various incidents that participants can select to experience the capabilities of Microsoft Copilot for Security.	• Demystifying Script analysis using Microsoft Copilot for Security • Reduce false positives analysis Microsoft Copilot for Security • Mitigating user risk at the front door using Microsoft Copilot for Security and Microsoft Entra • Optimized device compliance troubleshooting	• Maximize the potential of Microsoft Copilot by leveraging its automation capabilities to execute multiple tasks (promptbooks) and send alerts and notifications to your SOC team based on Gen-AI analysis. • Leverage knowledge bases to enrich prompts and provide additional context

Maximizing value with Microsoft Security solutions

Microsoft Sentinel	Microsoft Defender XDR	Microsoft Intune	Microsoft Defender Threat Intelligence	Microsoft Entra
Collect security data and correlate alerts from virtually any source with intelligent security analytics.	Prevent and detect cross-domain cyberattacks at the speed of AI. Copilot for Security is now embedded in Microsoft Defender XDR for early access customers.	Mitigate cyberthreats to devices, protect data, and improve compliance across clouds—now embedded with Copilot for Security for early access customers.	Understand cyberthreats and expose suspicious infrastructure with dynamic threat intelligence, now included in Copilot for Security at no additional cost.	Efficiently manage, safeguard, and govern identities and access, covering user administration, threat detection, access control, and compliance with security standards for cloud-based resources.

Additional information

• This HOL is tailored for technical decision makers, and IT professionals interested in enhancing their SecOps capabilities.

• Experience in managing Microsoft 365/Azure Security solutions for cybersecurity incident management scenarios.

• Participants will have hands-on experience with real-world scenarios and practical exercises.

• Technical support and guidance will be provided throughout the HOL session.

Contact Us for more information about the '**Synergy Advisors' Copilot for Security Hands-on-lab**' or our **Consulting Services**:

LEARN MORE

If you want to take your organization's security and compliance posture to the next level, if you are taking your first steps and want to quickly assess this technology as you progress along your path, **we offer the following options**:

Architecture Design Sessions [ADS]

The Copilot for Security ADS is a 1.5 to 2-day workshop involving key stakeholders. It focuses on designing, operating, and implementing Copilot for Security, including knowledge transfer on best practices, and understanding your current environment to identify requirements. Additionally, it offers insights into common scenarios and unique use cases. LEARN MORE

Proof of Concept [PoC]

The Copilot for Security PoC provides a streamlined approach to evaluating and demonstrating the capabilities of the solution within your organization. This (PoC) includes all necessary components, tools, and resources required to conduct a comprehensive assessment and showcase the functionality of Copilot for Security. LEARN MORE

Pilot

The Copilot for Security Engagement is a high-level session to prepare your organization for Copilot deployment. It involves evaluating readiness, reviewing usage and integration, validating use cases, implementing scenarios, configuring plug-ins, and providing knowledge transfer sessions on best practices. LEARN MORE

Why choose Synergy Advisors as your strategic partner?

Consulting Services

+12 years, +100 Top customers, and, with specializations in Security, Modern Work, Azure Data & AI, and Azure Infrastructure

We support our customers in the correct implementation of Microsoft solutions, aimed at improving their security postures and Modern Work, accompanied by a strategy that seeks to increase the adoption of these technologies and generate more upsell and cross-sell projects.

Managed Services

Leverage cybersecurity experts to review and monitor organizations' Microsoft 365 and Azure infrastructure and security. In-depth assessments of cloud applications, deployments as we help draft prioritized plans for improvements based on organizations unique security goals. Highly trained staff who monitor end-user activity through robust log analysis to provide you reliable monitoring, proactive and reactive incident response, and troubleshooting

Solutions (E-Suite)

Synergy Advisors' E-Suite seamlessly integrates various products with Microsoft 365, extending its features to address common advanced use cases encountered in organizations we've partnered with.
  • E-Visor
  • E-Visor Teams App
  • E-Inspector
  • E-Cryptor
  • E-Vigilant
  • E-Migrator