PwC and Microsoft

Copilot for Security

Advancing Your Cybersecurity Capabilities

Empower your organization to address evolving cyber threats with industry leading-leading AI assistance.

Mitigating Key Security Challenges with Copilot for Security

Resource and Skill Constraints
Organizations struggle with **limited resources** and a **shortage of skilled cybersecurity professionals**. Copilot for Security can help bridge this gap, enhancing operational efficiency and supplementing teams with generative AI capabilities at machine speed.

Dynamic Cyber Threats
Facing **ever-evolving cyber threats**, organizations often find their defenses outpaced.**Copilot for Security employs advanced AI** to swiftly adapt, identifying and neutralizing threats rapidly, keeping your operations secure.

Benefits of Copilot for Security

AI-Driven Threat Detection
Utilize advanced AI to quickly identify and mitigate threats, reducing response times and enhancing your security posture.

Empowered Response
Strengthen your SOC team with custom plugins, promptbook SOPs and advanced solutions for a more proactive and quicker security response.

Operational Efficiency
Enhance efficiency with automated processes, freeing up critical human resources for strategic tasks.

Insightful Analytics
Gain deep insights from Copilot for Security's analytics to help drive decision-making and improve incident handling.

Unified Security Enhancement
Copilot for Security interfaces with your current security setup, enhancing capabilities and protecting investments.

Skills Enhancement
Elevate your team's abilities with AI-powered support, closing skill gaps in cybersecurity knowledge.

How we can help modernize your security operations with Copilot for Security

PwC's Two-Step Security Empowerment Approach for Copilot for Security

Rapid Readiness Assessment	Implementation and Integration
Assessing Your Defenses: A Preliminary Check	Securing Your Future: Deployment and Integration

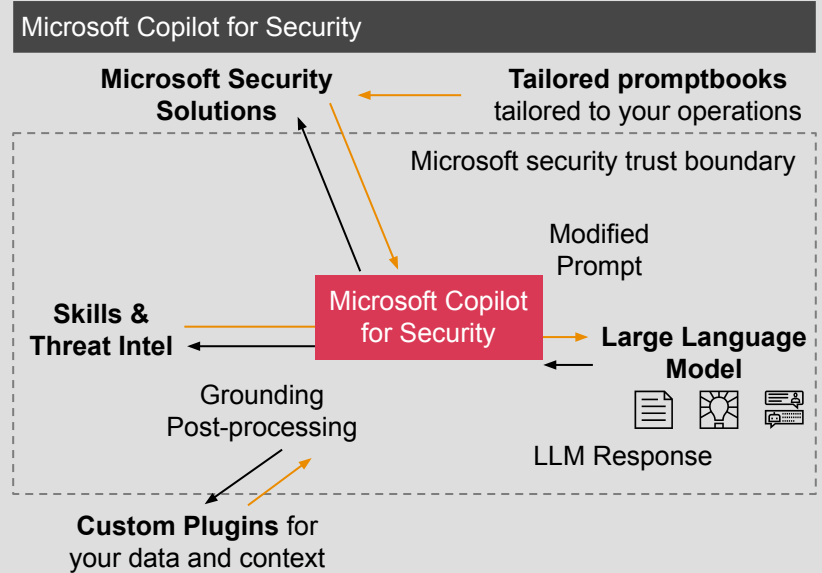## Phase 1: Microsoft Copilot for Security Rapid Readiness Assessment

Readiness Assessment Approach

Our readiness assessment offers a holistic analysis of your organization's requirements and potential addressable gaps for the Copilot for Security implementation.
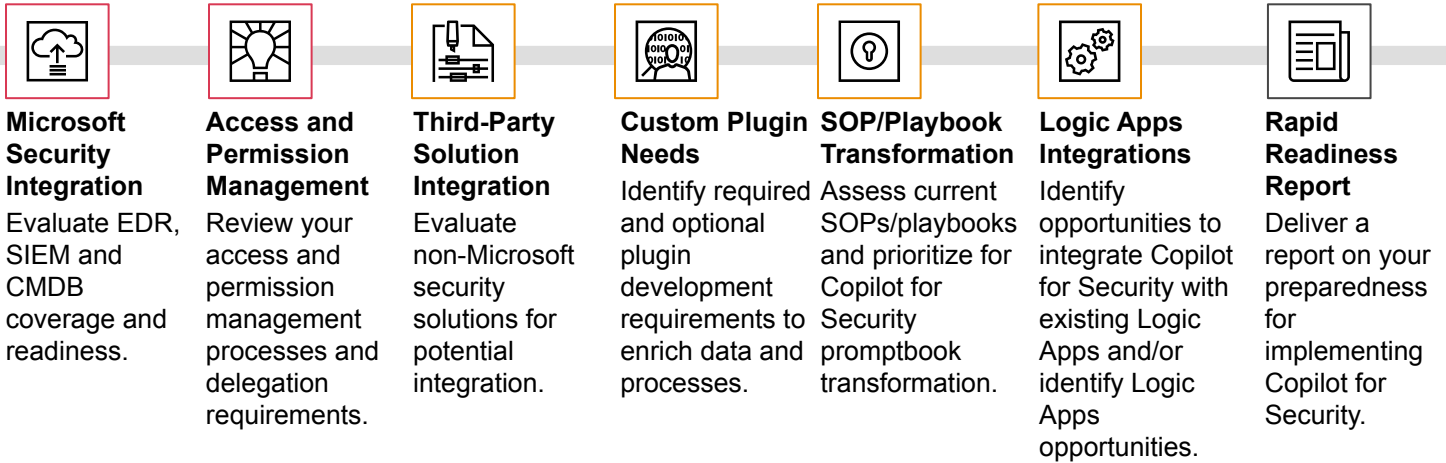
This assessment covers the technical requirements for the solution, tailored development needs, and the SOC adoption timeline and current standard operating procedures.

Readiness Assessment Outcomes

Our report and recommendations can provide insights regarding your organization's readiness to adopt Copilot for Security, including but not limited to upskilling opportunities, technology and solution integration options and other recommendations to help modernize your defenses and provide return on your investment.

Microsoft Copilot for Security

- Microsoft Security Solutions
- Tailored promptbooks tailored to your operations
- Microsoft security trust boundary
- Modified Prompt
- Microsoft Copilot for Security
- Skills & Threat Intel
- Large Language Model
- LLM Response
- Grounding Post-processing
- Custom Plugins for your data and context

Technical Readiness	Requirements and Opportunities	Report

Microsoft Security Integration
Evaluate EDR, SIEM and CMDB coverage and readiness.

Access and Permission Management
Review your access and permission management processes and delegation requirements.

Third-Party Solution Integration
Evaluate non-Microsoft security solutions for potential integration.

Custom Plugin Needs
Identify required and optional plugin development requirements to enrich data and processes.

SOP/Playbook Transformation
Assess current SOPs/playbooks and prioritize for Copilot for Security promptbook transformation.

Logic Apps Integrations
Identify opportunities to integrate Copilot for Security with existing Logic Apps and/or identify Logic Apps opportunities.

Rapid Readiness Report
Deliver a report on your preparedness for implementing Copilot for Security.

Core Components of the Rapid Readiness Report

01
Rapid Readiness Assessment summary

02
A prioritized list of actionable recommendations

03
Implementation roadmap

04
Custom plugin, skills and promptbook development requirements

Phase 2: Copilot for Security Implementation and Integration

Transition to advanced cybersecurity through tailored integration of Copilot for Security. Streamline SOC operations with sophisticated automation and empower teams with leading training and knowledge transfers.

Technical Implementation

Tailored Security Integration
- Custom setup of Copilot for Security
- Integration of Copilot for Security with existing systems and data sources
- Development of custom plugins to enhance functionality

SOC Workflow Integration

Enhanced SOC Operations
- Alignment of Copilot features with SOC operational processes
- Optimization of incident response workflows using Copilot
- Integration of knowledge bases for enriched processes and context

Training & Knowledge Transfer

Empowered Security Teams
- Holistic training programs tailored for SOC teams
- Relevant promptbooks that provide clear guidance for SOC teams
- Implement continuous learning pathways

Copilot for Security Services by PwC

Tailored Integration Services	Tailored Promptbooks	Custom Skill Development
Custom Plugins and Logic Apps	Policy Development & Compliance	Incident Response Planning

Why choose PwC?

PwC has been recognized by multiple analysts for excellence in cybersecurity services.

We know Microsoft; we have a substantial and growing alliance with Microsoft to build and deliver Microsoft's solutions to help you transform your business right, the first time.

Related services

Microsoft Copilot for M365

Integrated incident response solution with Microsoft and PwC

Your contacts

Vimal Navis
Principal, Cyber Risk & Reg
PwC US
M: +1 469 590 8899
E: vimal.navis@pwc.com

Norbert Vas
Director, Cyber Risk & Reg
PwC US
M: +1 617 530 5000
E: norbert.vas@pwc.com

pwc