

Las probabilidades están  
en **contra** de los **analistas  
de seguridad** de hoy en  
día



**4,000**

Ataques de contraseñas por segundo



**72 mins**

Tiempo medio para que un atacante  
acceda a tus datos privados si eres  
víctima de un correo electrónico de  
phishing



**3.5M**

Escasez mundial de profesionales  
cualificados en ciberseguridad

# Los defensores necesitan un **nuevo enfoque**



Conjuntos de  
herramientas  
complejos



Deriva de  
la postura



Técnicas de  
ataque  
sofisticadas



Procesos  
desconectados



Escasez de talento  
y experiencia



Colaboración  
ineficiente



# La IA permite un **cambio de paradigma**



Evalúe y mejore continuamente la postura con visibilidad y contexto a hiperscala en tiempo real



Investigue y responda a amenazas con una velocidad y experiencia sin precedentes



Mejore la productividad y la colaboración con flujos de trabajo optimizados en lenguaje natural

# La consolidación de herramientas y la IA generativa pueden **transformar la seguridad**

## CONSOLIDACIÓN DE HERRAMIENTAS

Defensa coordinada en todos los vectores de amenazas para ofrecer visibilidad y cobertura de extremo a extremo



## IA

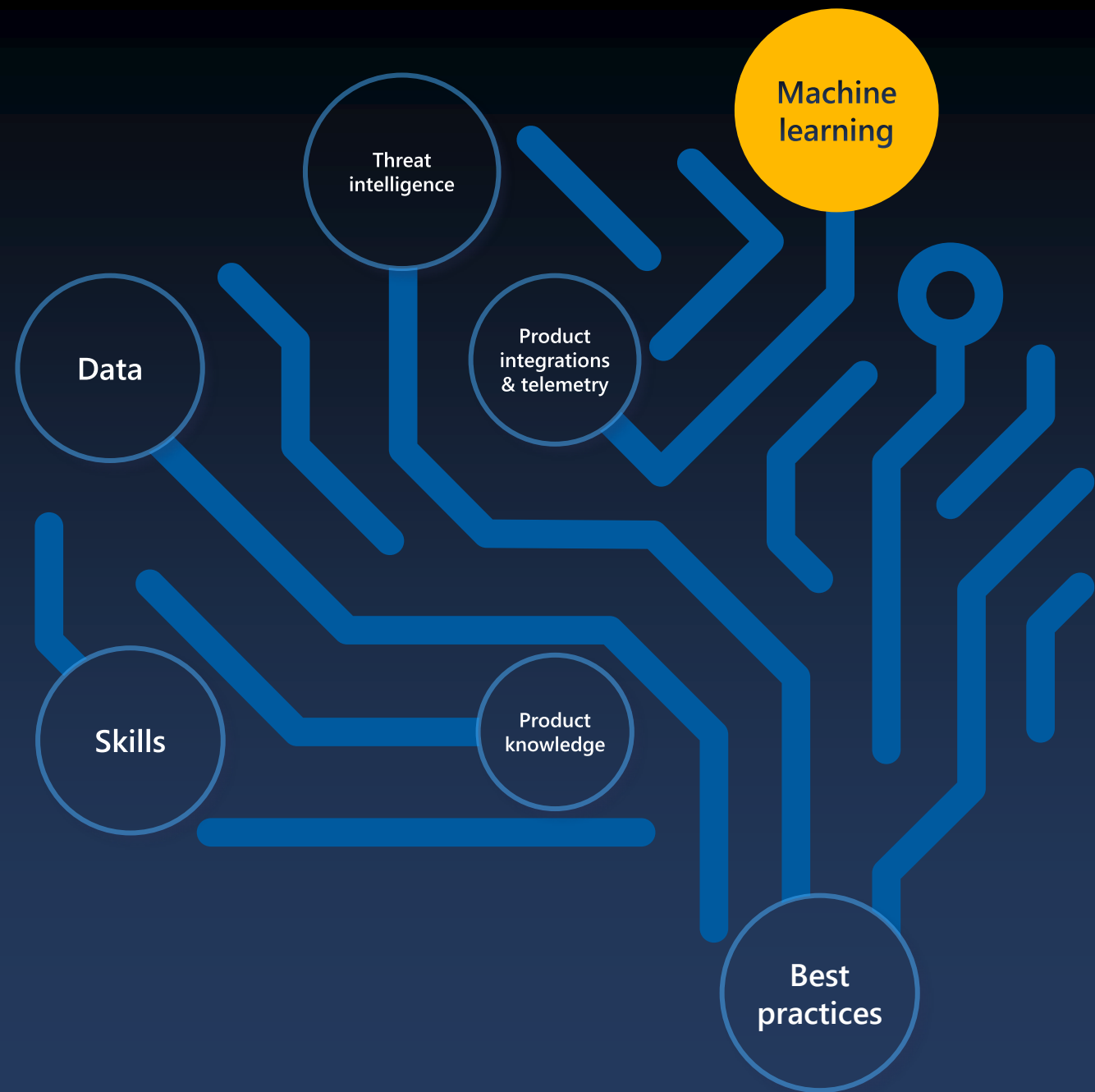
Ganancias exponenciales en experiencia humana y eficiencia para defender a la velocidad y escala de la máquina





# Microsoft Copilot for Security

El primer producto de seguridad de IA generativa que permite a los equipos de seguridad y TI proteger a la velocidad y escala de la IA





# Copilot puede ayudar

## SOC

### Investigación de alertas

Considera los datos de varios sistemas y responde con un resumen detallado de los incidentes.

### Inteligencia de amenazas

Razones sobre el contenido de Microsoft Defender Threat Intelligence (MDTI) y análisis de amenazas y proporciona un resumen de la inteligencia relacionada.

### Remediación

Proporciona los siguientes pasos recomendados para remediar un incidente.

## TI

### Cumplimiento

Hace referencia a complementos y políticas en la base de conocimientos para determinar el cumplimiento del dispositivo.

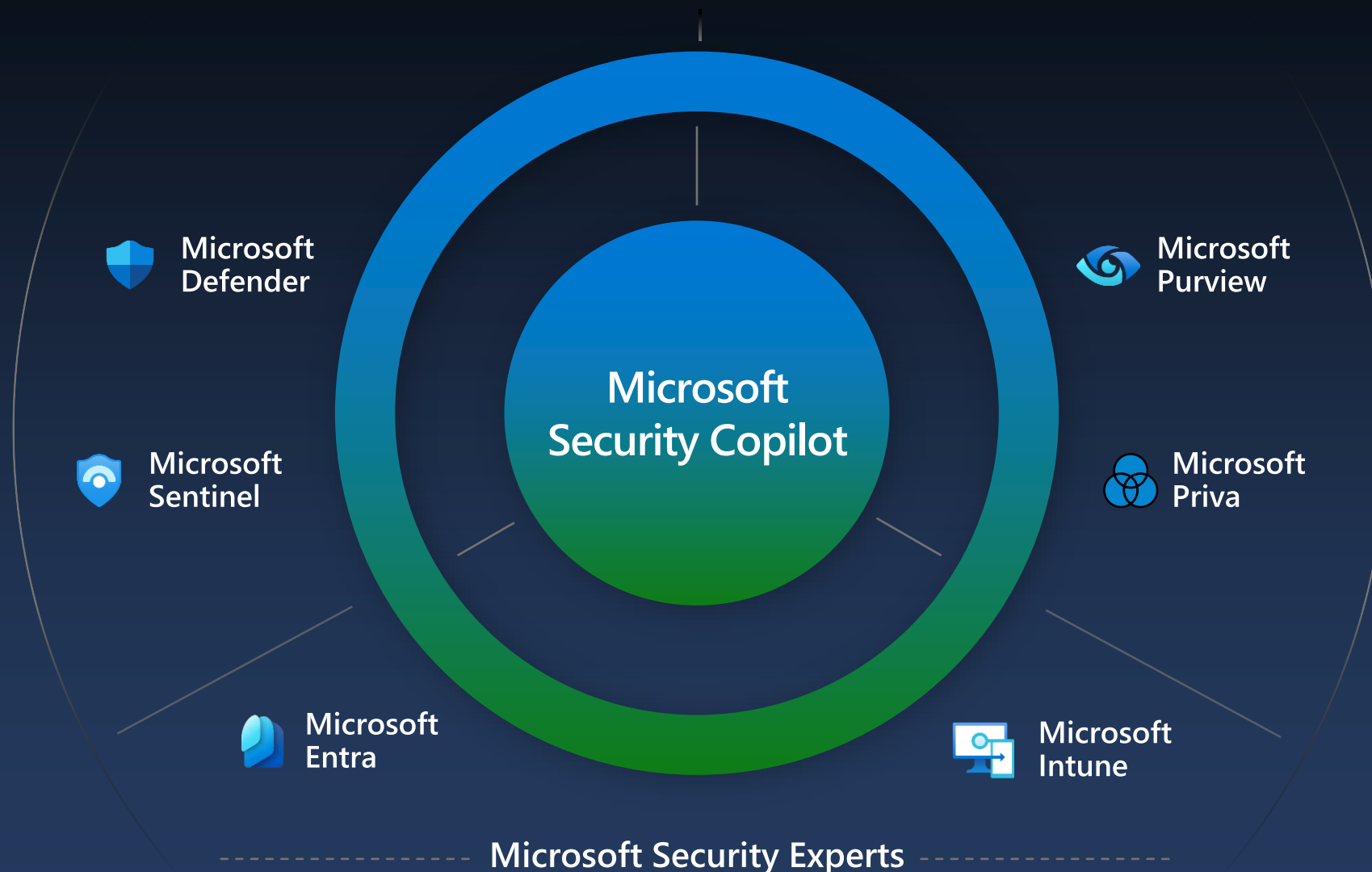
### Gestión de dispositivos

Proporciona orientación sobre cómo configurar e implementar un piloto de dispositivo MacOS mediante Intune.

### Actualizaciones de firmware

Identifica complementos para el estado del dispositivo y evalúa el estado del firmware

# Seguridad de extremo a extremo de Microsoft

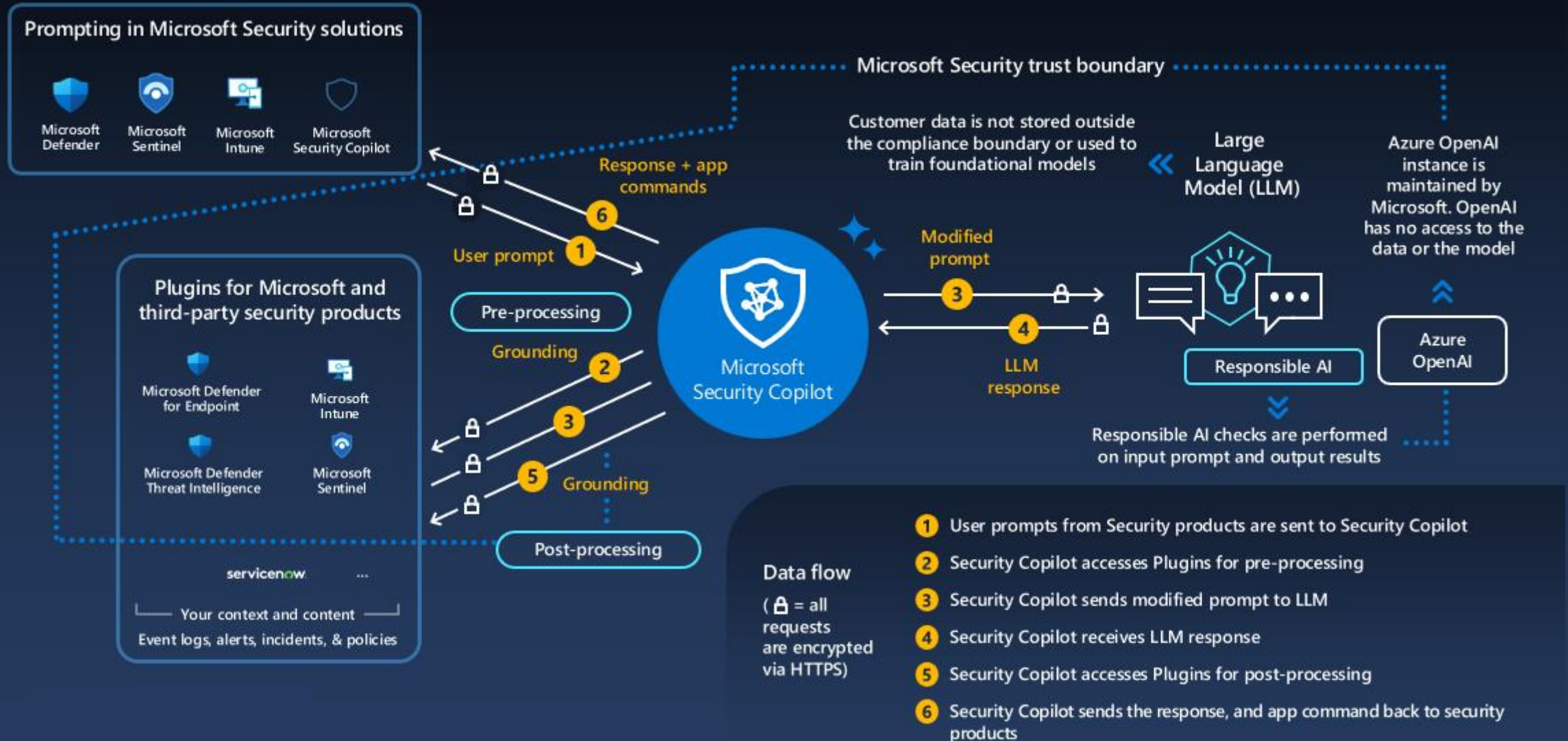


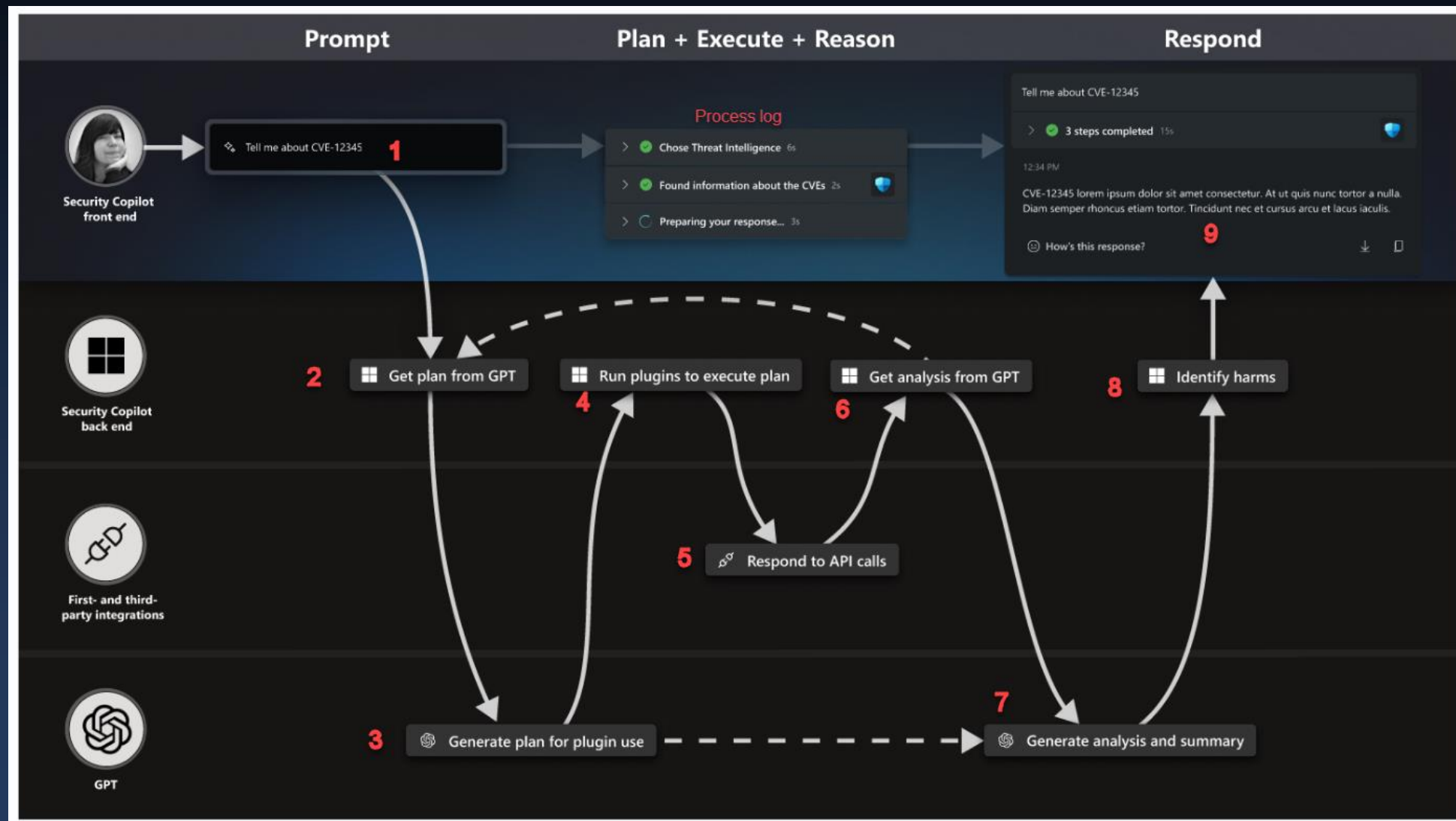






# Flujo de datos para Microsoft Copilot for Security

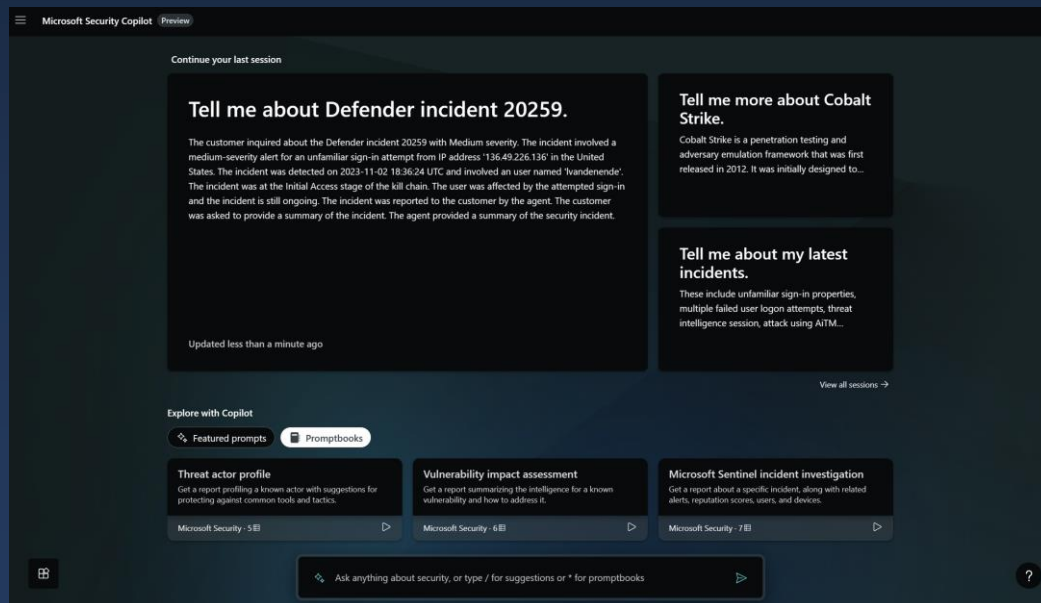




# Experiencias para conocerte dónde y cómo trabajas

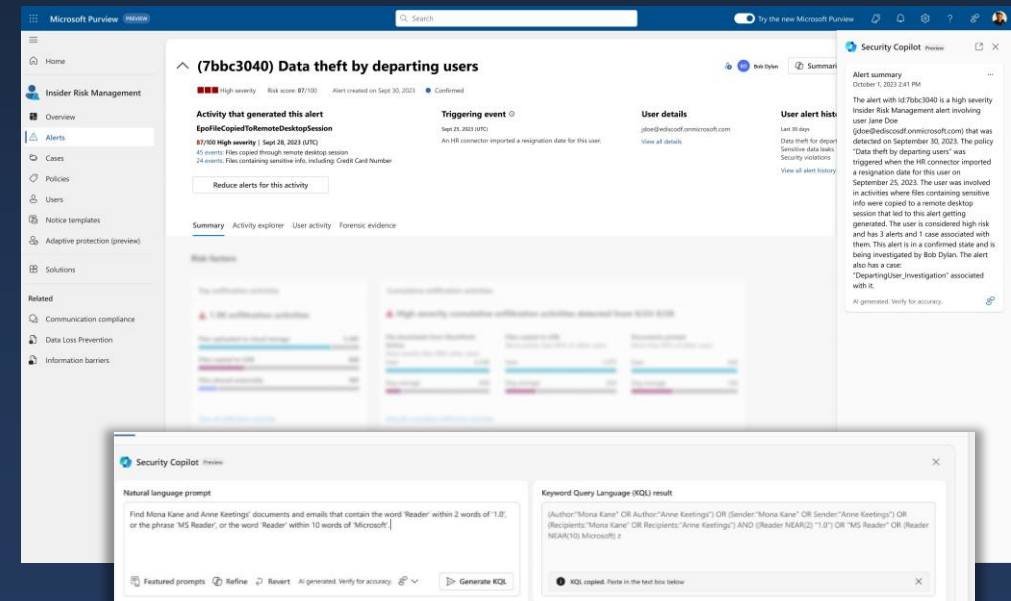
## Independiente

Ayuda a los equipos a **obtener un contexto** más amplio para solucionar problemas y remediar incidentes más rápido dentro de Security Copilot, con **todos los casos de uso en un solo lugar**, lo que permite **una guía enriquecida entre productos**.



## Incrustado

Ofrece la experiencia **intuitiva** de obtener orientación de Security Copilot de forma **nativa** dentro de los productos con los que los miembros de su equipo ya trabajan y con los que están familiarizados.



# Escenarios de Security Copilot

## Respuesta al incidente

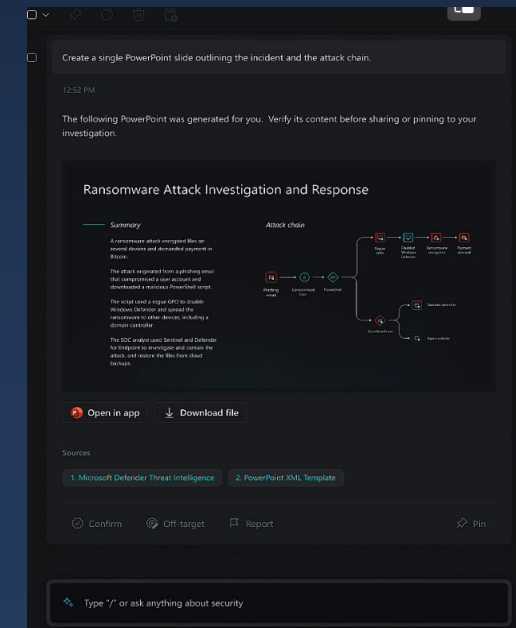
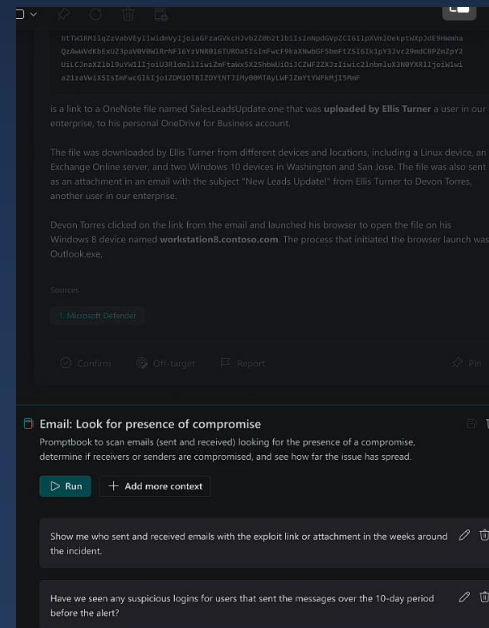
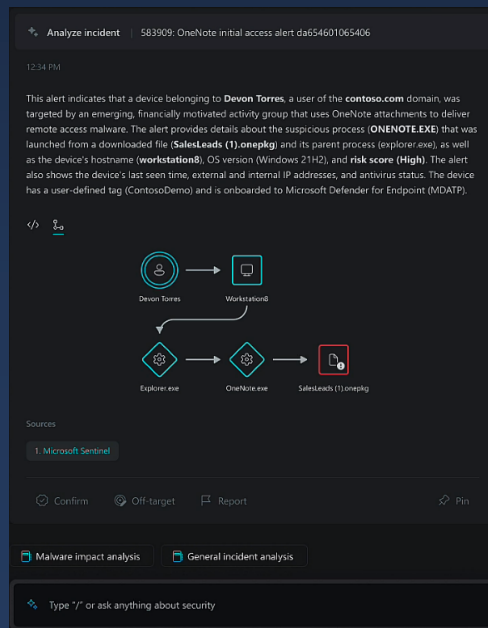
Detecte ataques en curso, calcule su alcance y reciba orientación para solucionarlos basándose en estrategias comprobadas en incidentes de seguridad del mundo real.


## Caza de amenazas


Descubra si su organización está en riesgo debido a vulnerabilidades y exploits conocidos. Examine cada recurso de su entorno en busca de signos de una violación de seguridad.


## Informes de Seguridad


Resuma eventos, incidentes o amenazas en minutos y prepare la información en informes individuales que se pueden compartir directamente para la audiencia deseada.



 ¿Cómo puedo mejorar mi postura de seguridad?

 ¿Alguna de mis máquinas está afectada?

 Resume este incidente en viñetas.

 ¿Qué alertas se activan más?

 ¿Qué es log4shell?

 Cuéntame sobre el incidente 20259 del Defender.

Tell me about Defender incident 20259.



>  3 steps completed 25s

Nov 2, 3:14 PM | 26.94s

Defender incident 20259 with Medium severity has a total of 1 alerts. 1 alerts were selected for summarizing the incident.

Some alerts from the incident include:

1. Severity: Medium Start time: 2023-11-02 18:36:24 Description: Unfamiliar sign-in properties relating to attempted sign-in, IP '136.49.226.136' impacting User 'lvandenende'

Here's a short summary of the incident:

The security incident occurred on 2023-11-02 18:36:24 UTC and involved a medium-severity alert. An unfamiliar sign-in attempt was detected, originating from IP address '136.49.226.136' in the United States, impacting user 'lvandenende'. The incident is at the Initial Access stage of the kill chain.

Sources

[Incident Page](#)



Looks right



Needs improvement



Inappropriate





# Modelo de negocio

- Copilot for Security está disponible para su compra como una oferta de consumo.
- Un modelo de negocio en toda la cartera de seguridad de Microsoft que permite experiencias independientes e integradas.
- Las empresas de todos los tamaños pueden comenzar fácilmente aprovisionando capacidad en unidades informáticas de seguridad (SCU).
- Las SCU potencian las capacidades de IA generativa de Copilot for Security

SCU es la unidad de medida de la potencia informática para ejecutar cargas de trabajo de Copilot for Security.

## Comience hoy mismo

Comience ahora con un modelo de consumo, sin cargos por usuario o por dispositivo

## Aprovisionamiento flexible de SCUs

Aprovisionamiento de unidades informáticas de seguridad (SCU) para ejecutar todas las cargas de trabajo de Copilot for Security

## Gestione fácilmente los costes

Supervise el uso y gestione fácilmente los costos en el panel de control del producto

# Detalles de precios

- Copilot for Security está disponible para su compra con carácter general. Los clientes pueden comprar capacidad en cuatro regiones: Este de EE. UU., Sur de Reino Unido, Europa Occidental y Este de Australia, con regiones adicionales agregadas en el futuro.
- Las SCU tendrán un precio de \$4 en todas las geografías de GA.

SKU	Precio por hora	Precio estimado por mes
Provisionado	\$4	\$2,920 <sup>1</sup>

[ <sup>1</sup> La estimación de la factura mensual es de 1 SCU aprovisionada durante 24 horas diarias durante todo el mes. Las SCU se aprovisionan por hora y se facturan mensualmente.]

- Factura mensual estimada = (SCU/hora) x (precio de SCU por hora) x 730 horas/mes.
- Supervise el uso de la capacidad con el panel de control del producto y ajuste de forma flexible la capacidad aprovisionada en cualquier momento.

## Ejemplo de facturación:

- Un cliente ha aprovisionado 3 SCU por hora durante las 24 horas del día los 365 días del año, su:
  - Factura mensual =  $3 \times 4 \times 730 = \$8,760$
  - Factura anual = \$105,120

[ <sup>1</sup> La factura cambiará si los clientes cambian las SCU provisionadas en cualquier momento.]