

Ciberseguridad en acción

De la detección a la prevención inteligente



Agenda



Resumen del panorama de amenazas



Centros de operaciones de seguridad (SOC) en la actualidad



Transformación de SecOps con una plataforma unificada



Ejemplos de escenarios de amenazas



Análisis técnico de seguridad proactiva con Microsoft Security



Conclusiones y próximos pasos



Threat landscape **BRIEFING**

POWERED BY:
Microsoft Threat Intelligence

78T Señales sintetizadas
por día (2024)

300+ Actores únicos del Estado-
nación y de la delincuencia
financiera

Las tres principales tendencias en el panorama de amenazas



Las **amenazas** están creciendo y vendiendo sus herramientas a otros



El ransomware está evolucionando para dirigirse a dispositivos no gestionados y vectores similares de baja visibilidad



La velocidad, la escala y la sofisticación de los ataques no tienen precedentes

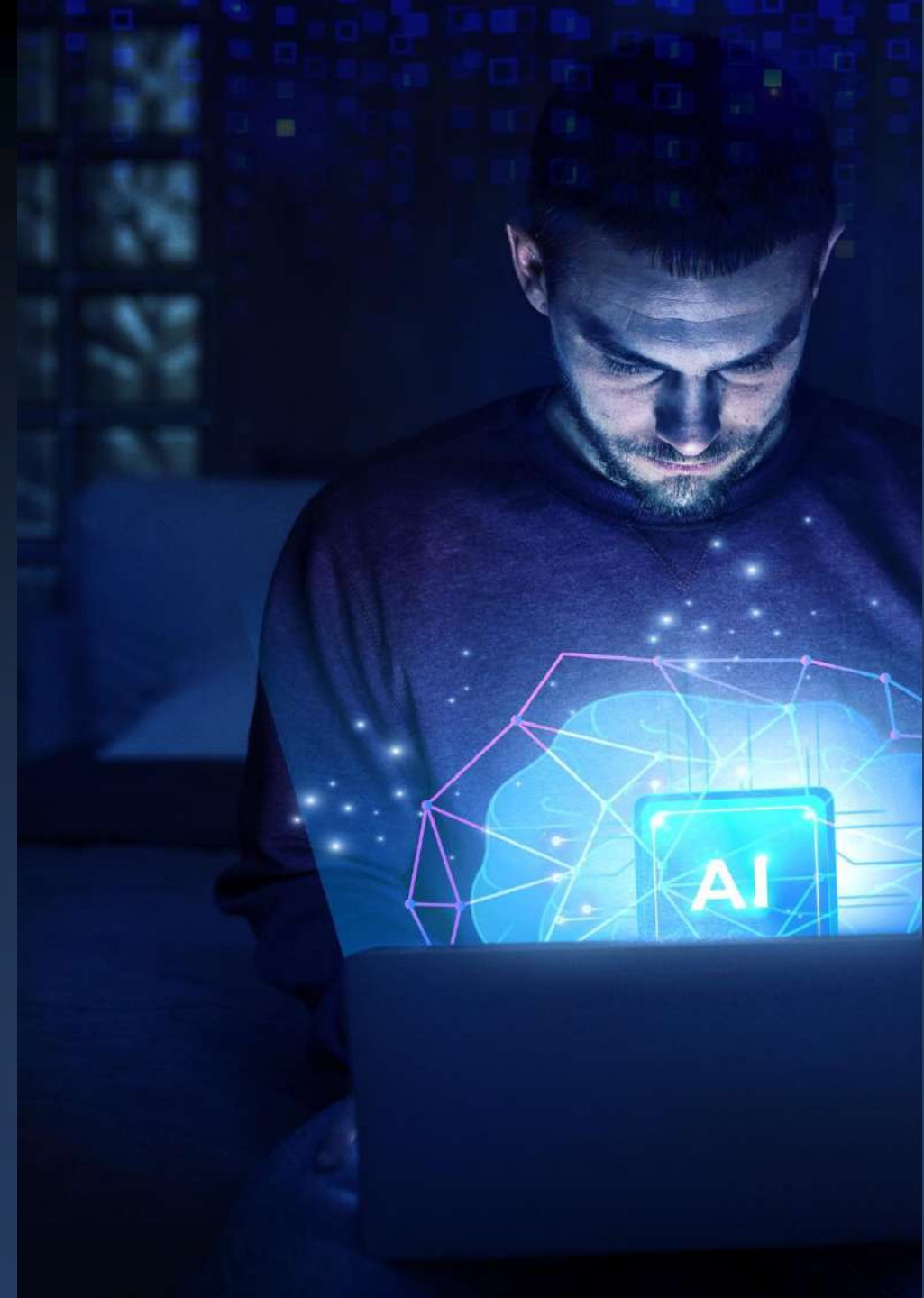
Inteligencia Artificial

Las empresas que utilizan la IA y la automatización para detectar y responder a las brechas de datos ahorran una media de 3 millones de dólares en comparación con las que no lo hacen.

En ambos bandos

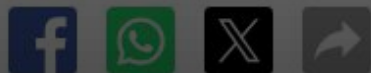
En 2023, más delincuentes usarán los algoritmos de IA para identificar sistemas con una seguridad débil.

Para 2030 el mercado de productos de ciberseguridad con IA tendrá un valor cercano a los 139.000 millones de dólares, lo que supone un aumento de casi diez veces el valor del mercado de 2021.



Los 'piratas' de la 'Dark Web', al acecho del control de ChatGPT

tan sobre riesgos de 'ChatGPT'



Primera modificación: 03/03/2023 - 03:47

Home > Tecnología

He probado a 'hackear' ChatGPT para que se salte las políticas de OpenAI y este es el resultado

TECNOLOGÍA Carolina González Valenzuela | 23 abr. 2023 1:00h.



Noticias · 20/04/2023

Por 7 se multiplica el número de hackers que hablan en la dark web sobre cómo manipular ChatGPT



Redacción Tekios · lectura 1 min · 770 vistas

Pánico con ChatGPT

TECNOLOGÍA

Fake news, manipulación y hackeos: cómo ChatGPT es un "profundo riesgo para la inteligencia artificial"

Por Matt Burgess, periodista de tecnología y seguridad en el equipo de investigación de

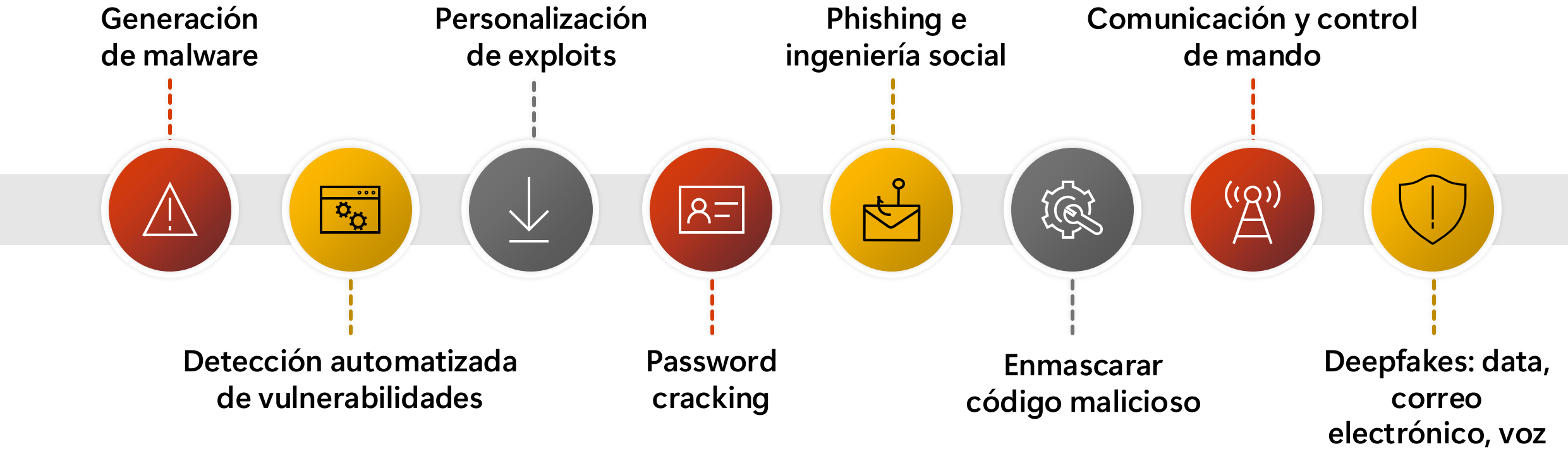
MATT BURGESS

SEGURIDAD 14 DE ABRIL DE 2023

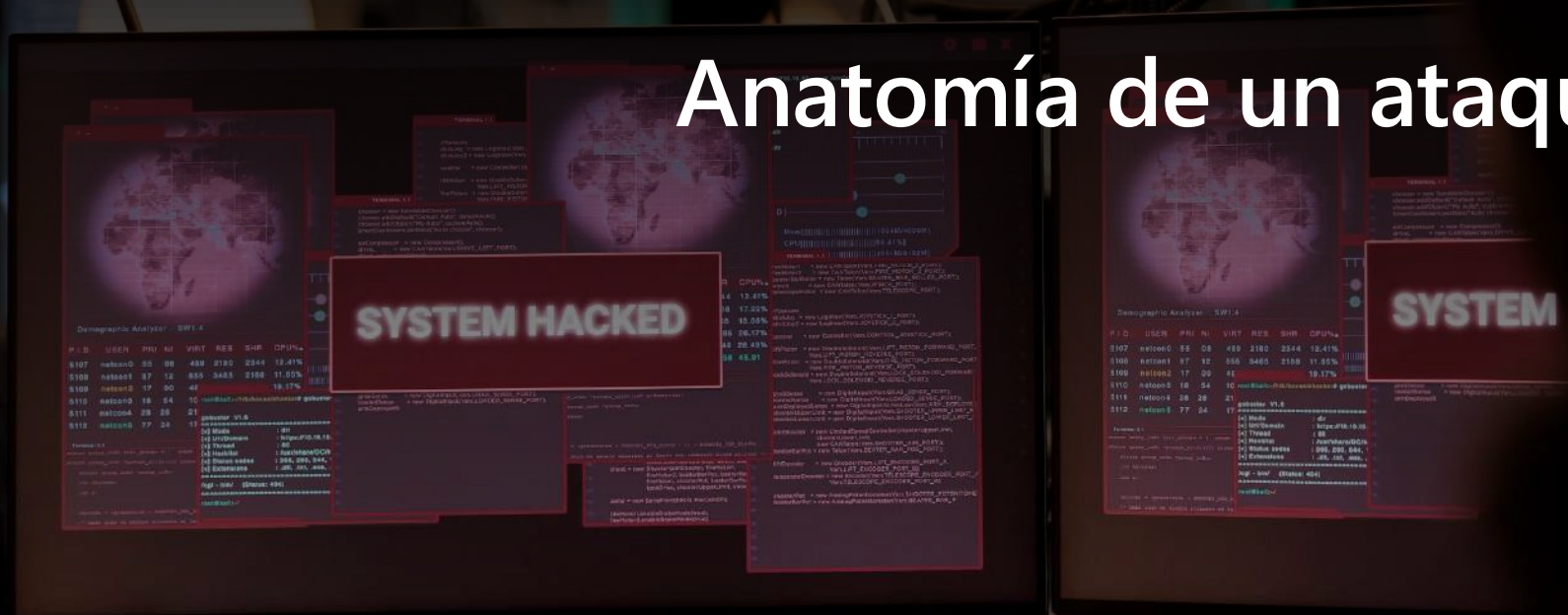
ChatGPT: el hackeo apenas comienza

¿Pánico por chatGPT?

Los adversarios utilizan la IA



Anatomía de un ataque





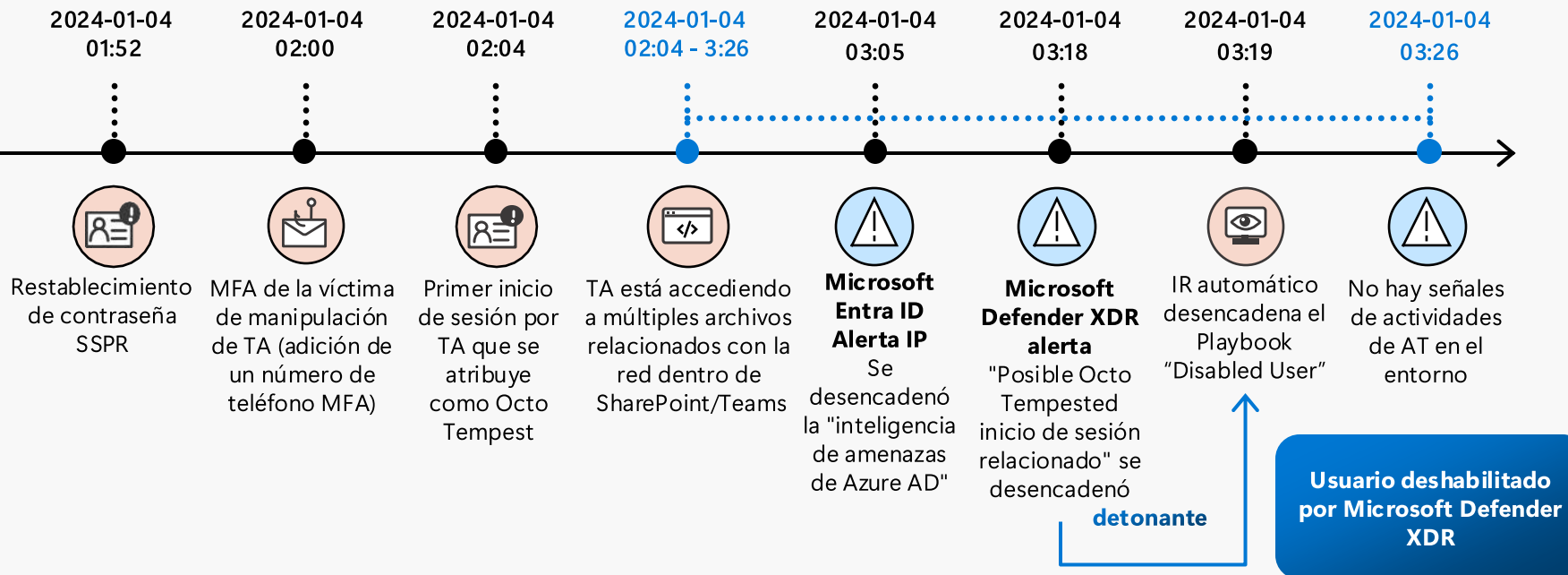
Intel profile: Octo Tempest

Motivación:
Financiera

Alias: Scattered
spider, Okatpus

Objetivos: Intercambios de SIM, robo de
criptomonedas o exfiltración de datos antes
de operaciones de extorsión o ransomware

Estudio de caso de una cadena de ataque real de Octo Tempest: Interrumpida



Acceso inicial

- > Ingeniería Social
- > Enmascaramiento y suplantación de identidad

Descubrimiento

- > Enumeración de la documentación interna
- > Reconocimiento ambiental continuo

Acceso a credenciales, movimiento lateral

- > Identificación de activos de nivel 0
- > Acceso a entornos empresariales a través de VPN
- > Recopilación de credenciales adicionales

Evasión de la defensa, ejecución

- > Aprovechar la EDR y las herramientas de gestión
- > Elusión del acceso condicional

Persistencia

- > Instalación de una puerta trasera de confianza
- > Manipulación de cuentas existentes
- > Establecer el acceso a los recursos

Acciones sobre objetivos

- > Preparación y exfiltración de datos robados
- > Implementación del ransomware BlackCat

Panorama actual de amenazas



91%

Ciberataques
que comienzan
con el correo
electrónico

30,720

Dominios generados
por delincuentes cada
tres días



\$1.8B

Pérdida atribuida al
compromiso del correo
electrónico empresarial
solo en 2020

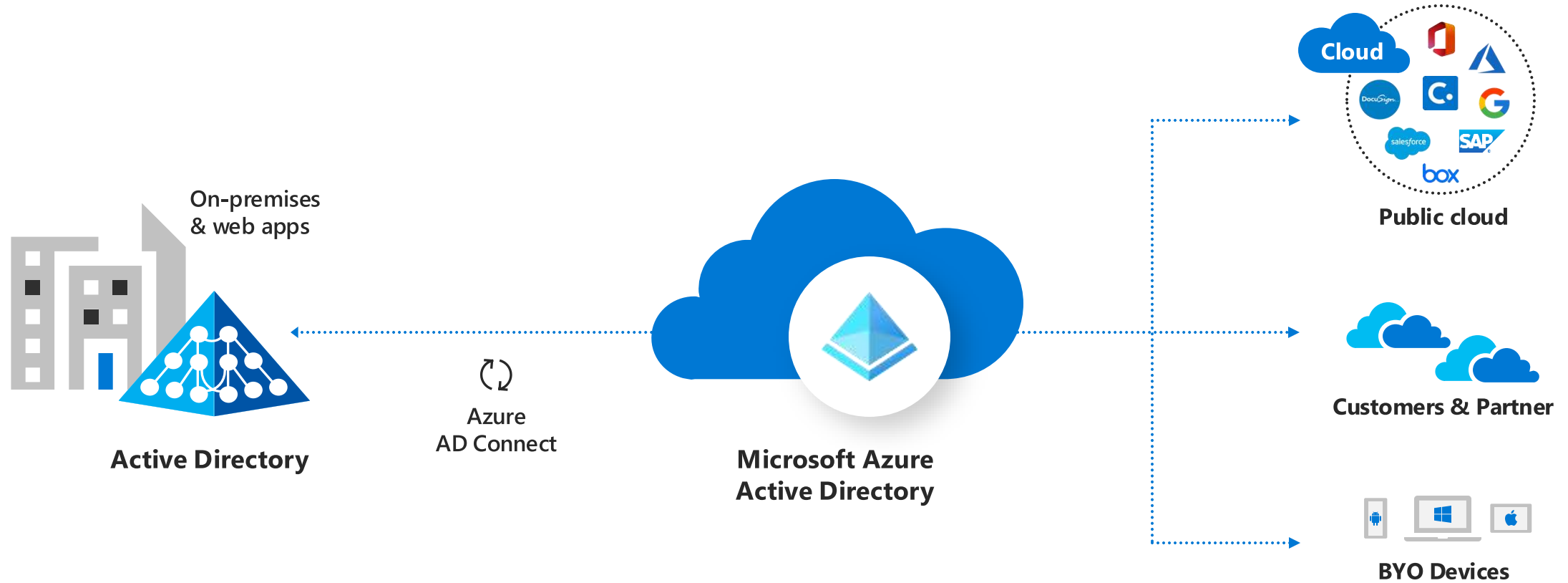
168K

Sitios de phishing
eliminados



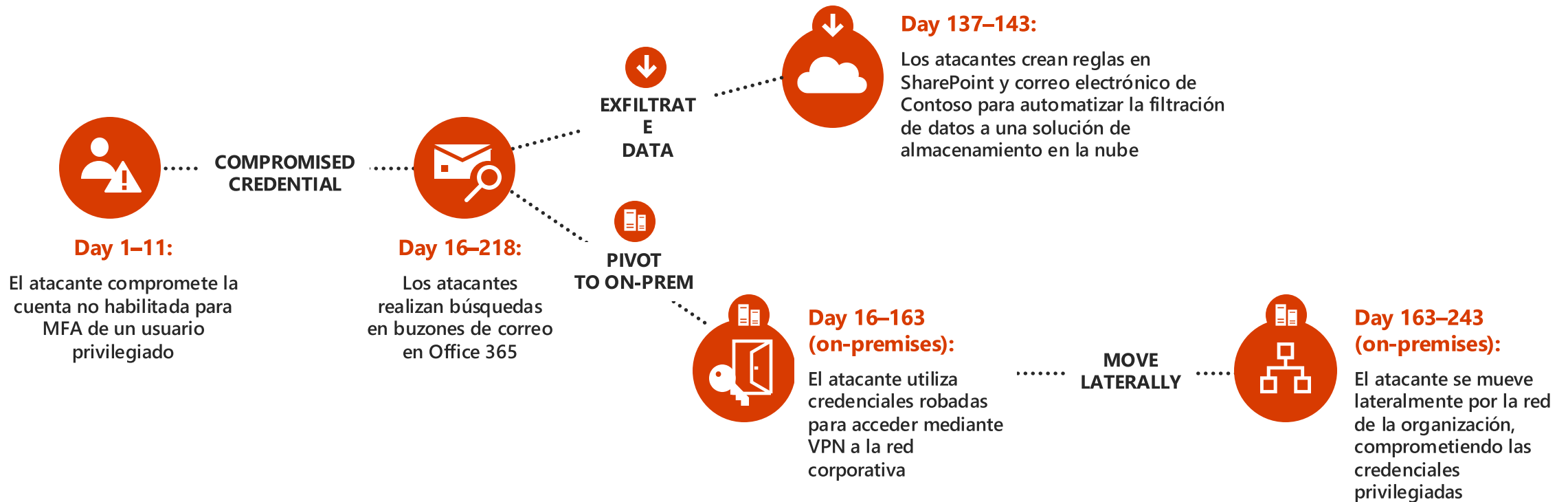
La complejidad del panorama de seguridad de la identidad empresarial

Los entornos de seguridad empresarial son complejos e incluyen activos tanto locales como en la nube.



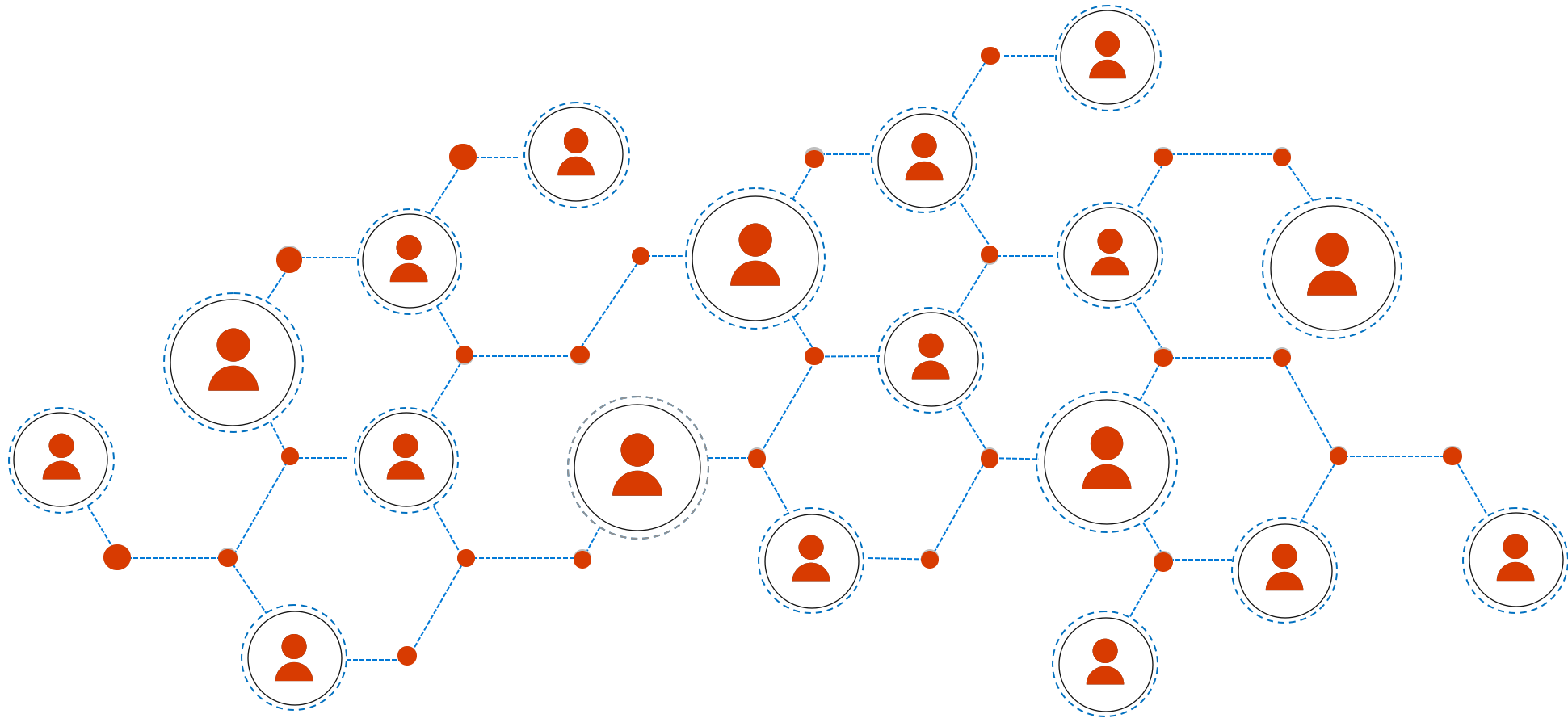
Anatomía de un ataque al entorno local y en la nube

Un ejemplo de cómo ocurre un ataque y compromete a toda una organización.



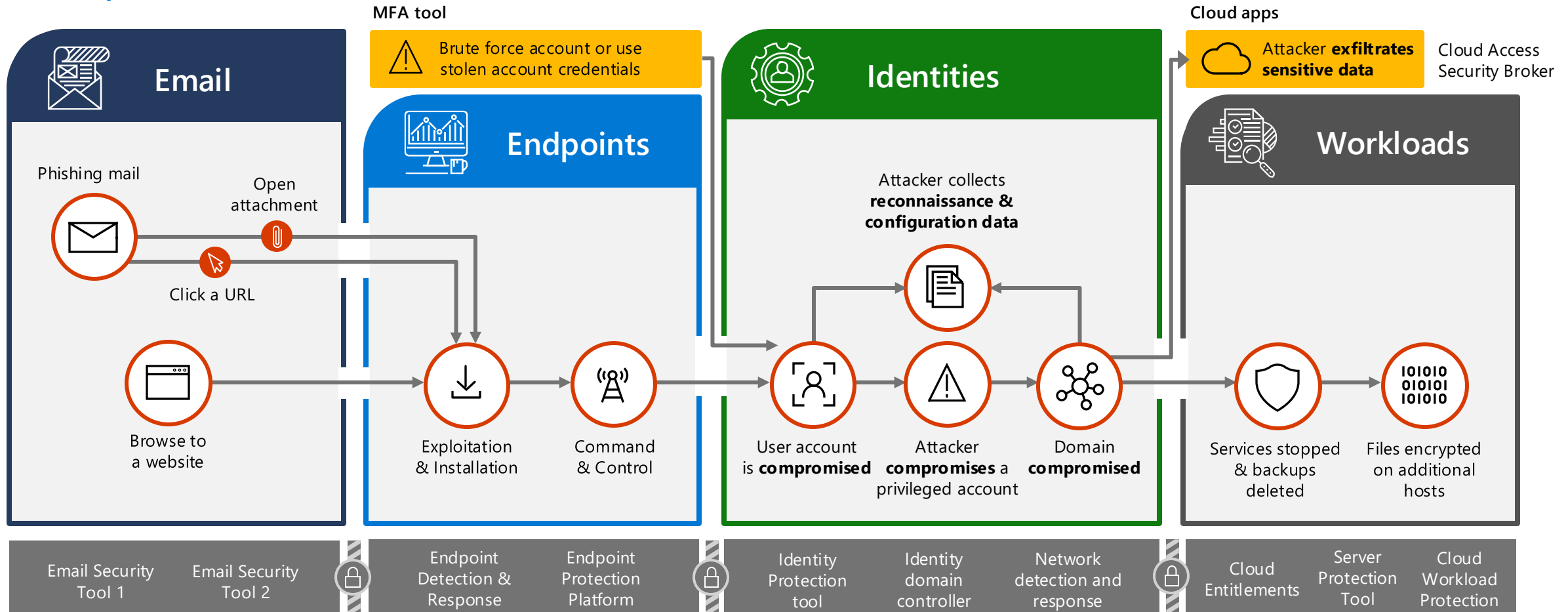
Un nuevo perímetro de seguridad - Identidad de usuario

Los usuarios son el nuevo perímetro y un solo usuario comprometido puede provocar el cierre de una empresa.

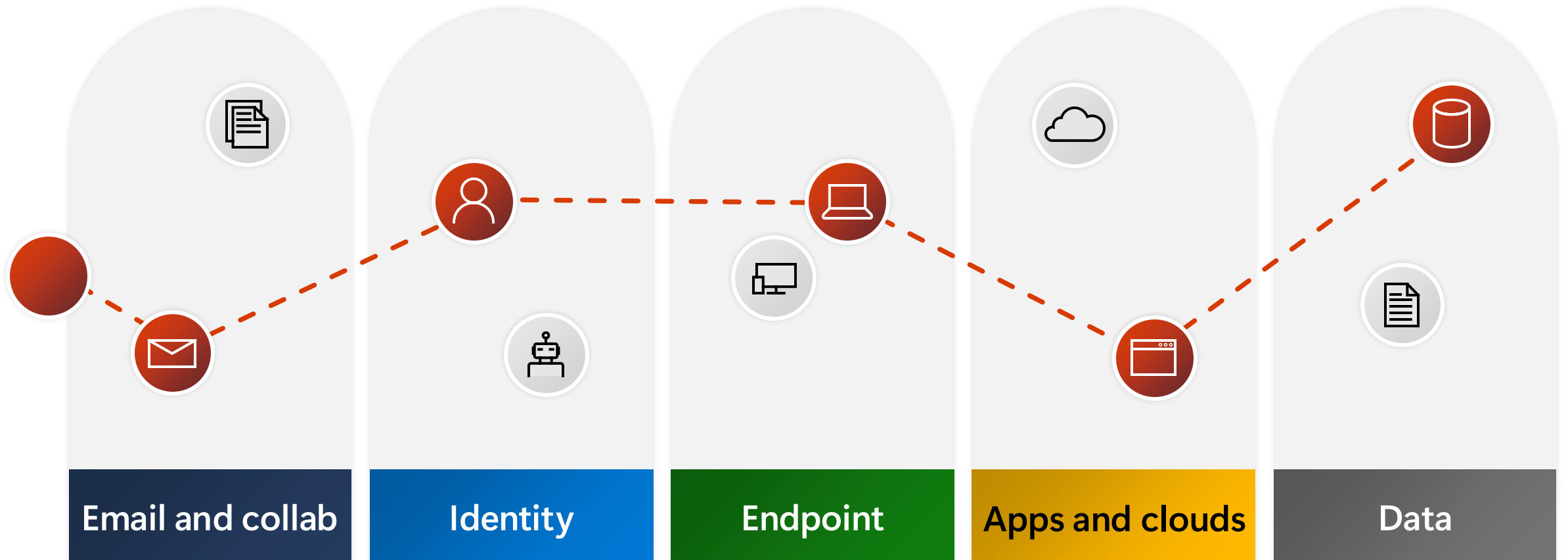


La seguridad aislada conduce a brechas en la cobertura

Múltiples herramientas que proporcionan una protección desigual a lo largo de la cadena de eliminación de ataques



Atacantes piensan en grafos



El tiempo medio para que un atacante acceda a los datos privados del phishing es de solo

72 minutos²

Los profesionales de SecOps trabajan dentro de portales







Múltiples soluciones de seguridad
Las soluciones están desconectadas

Detección
de
anomalías

Extremo
Protección

Infraestructura
Seguridad

Nube híbrida
Seguridad

Seguridad de datos
y aplicaciones

Fraude
Prevención

Gestión de la
seguridad

Centro de datos
Seguridad

Correo electrónico
Seguridad

Identidad y acceso
Administración

Montón
Seguridad

Gestión de los
derechos de
información

Amenaza
Detección

Acceso a la nube
Agente de seguridad

Pérdida de
datos
Prevención

Cumplimiento
Herramientas

SIEM

Visibility across your entire organization



XDR

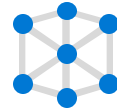
Protection across your end user and infrastructure environments

SIEM

Microsoft Sentinel

Visibility across your entire organization


Existing security
portfolio


IA

Microsoft 365 Defender

Secure your end users

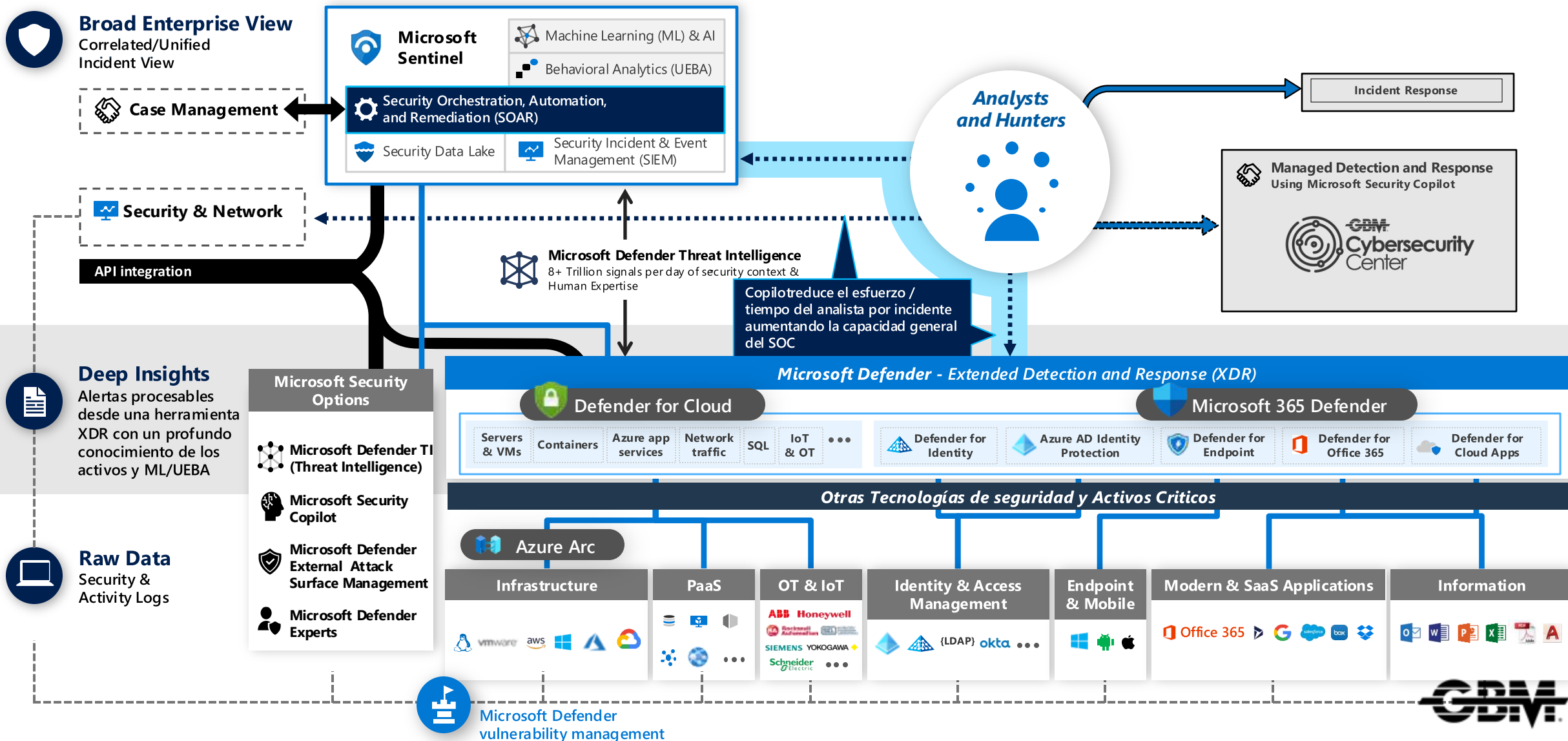
Microsoft Defender

Secure your infrastructure

XDR

Managed Detection & Response for Microsoft

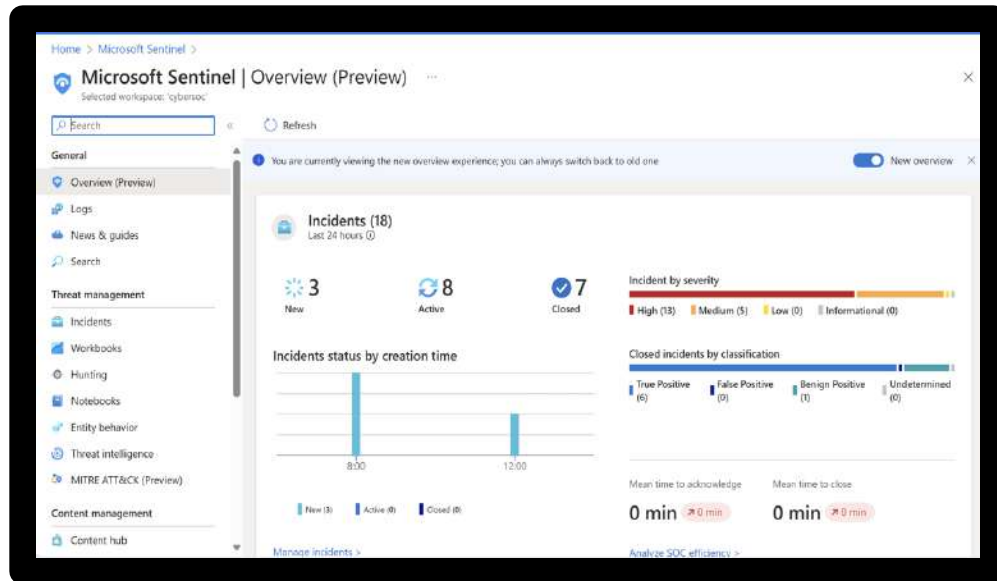
GBM Cybersecurity Center



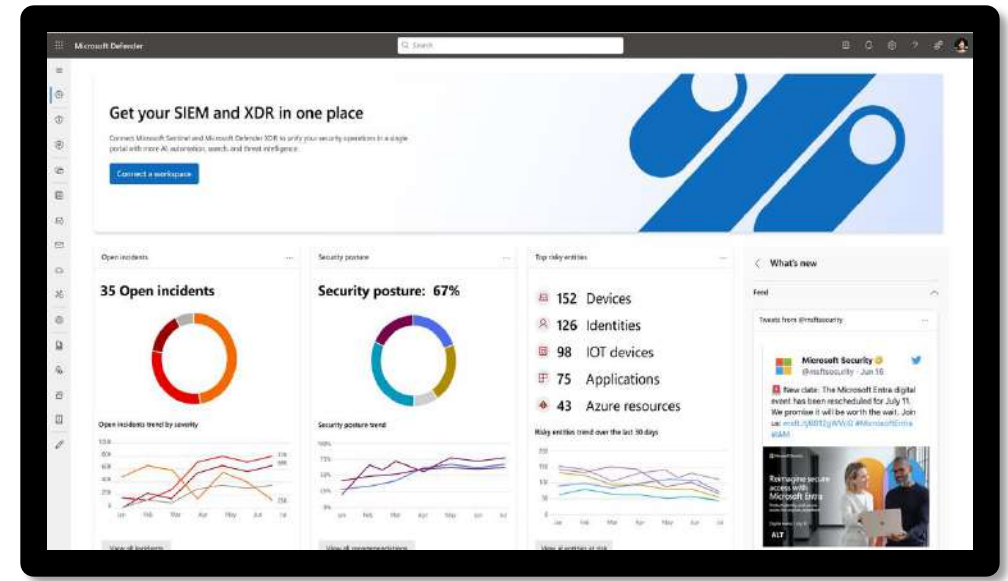
**XDR + SIEM se está convirtiendo en una
plataforma unificada de operaciones de seguridad**

Hacer más con menos

Acelere su defensa contra amenazas con Microsoft Sentinel y Defender XDR juntos



Información general de Microsoft Sentinel en Azure Portal



Descripción general de la plataforma unificada



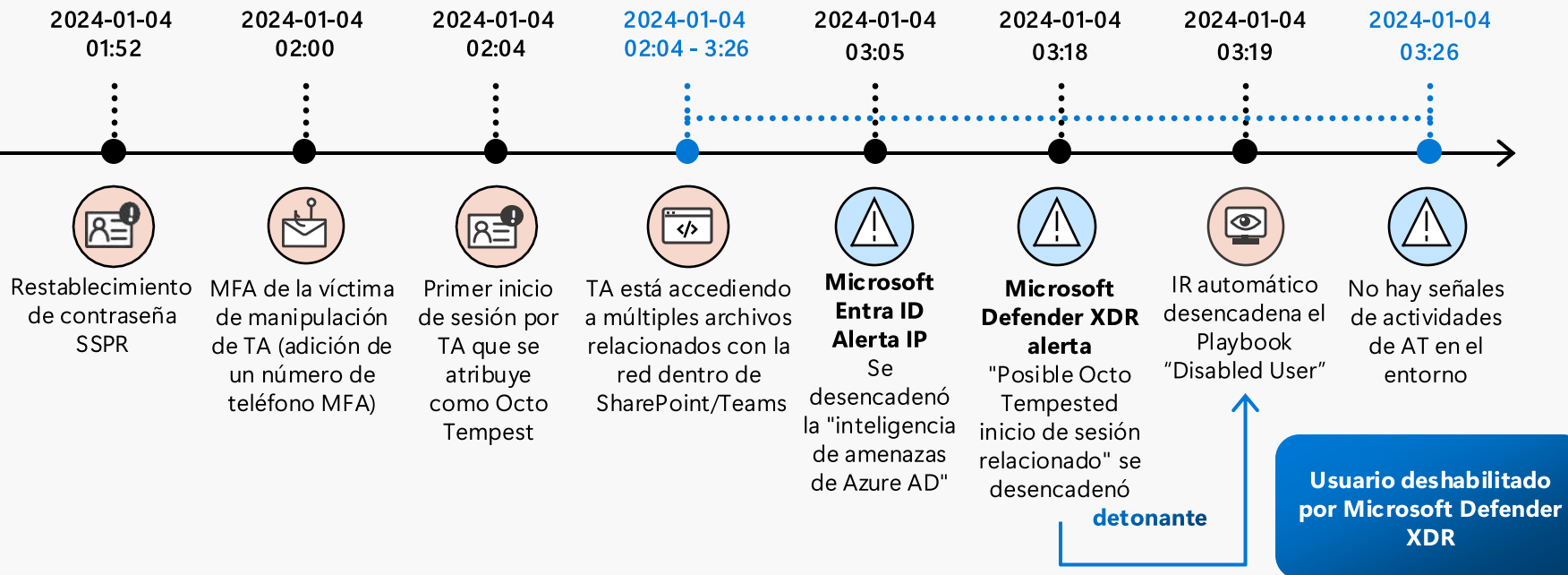
Intel profile: Octo Tempest

Motivación:
Financiera

Alias: Scattered
spider, Okatpus

Objetivos: Intercambios de SIM, robo de
criptomonedas o exfiltración de datos antes
de operaciones de extorsión o ransomware

Estudio de caso de una cadena de ataque real de Octo Tempest: Interrumpida



Acceso inicial

- > Ingeniería Social
- > Enmascaramiento y suplantación de identidad

Descubrimiento

- > Enumeración de la documentación interna
- > Reconocimiento ambiental continuo

Acceso a credenciales, movimiento lateral

- > Identificación de activos de nivel 0
- > Acceso a entornos empresariales a través de VPN
- > Recopilación de credenciales adicionales

Evasión de la defensa, ejecución

- > Aprovechar la EDR y las herramientas de gestión
- > Elusión del acceso condicional

Persistencia

- > Instalación de una puerta trasera de confianza
- > Manipulación de cuentas existentes
- > Establecer el acceso a los recursos

Acciones sobre objetivos

- > Preparación y exfiltración de datos robados
- > Implementación del ransomware BlackCat

Los equipos de seguridad necesitan **una fuerza multiplicadora**



Los ataques
ocurren en minutos
y horas
no días o meses



Los atacantes se
están aprovechando
de **las herramientas**
aisladas



No hay suficiente ancho
de **banda** para abordar la
exposición al riesgo de
manera eficaz



¿Cómo la IA y GBM hacen su parte?

Las probabilidades
están en **contra** de
los **analistas de
seguridad** 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 calificados en ciberseguridad

Necesitamos cambiar
las reglas del juego

Use it to tell Copilot what insights
your security data.

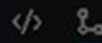
Confirm

Off-target



Produce a visual to explain the activity of the download, the exploit and how it moved through
the incident.

12:40 PM



Microsoft Security Copilot

se
t,
e execution vulnerability
ers to inject malicious code via JNDI

2021 and several proof of concepts were
nd exploitation attempts by various threat actors.

ware families, such as Mirai, Kinsing, Muhstik,
/ptocurrency miners, ransomware, and remote
on malicious domains or IP addresses that can be

d 2.16.0 to address the vulnerability by disabling
older versions may still be vulnerable and
e JndiLookup class from the classpath or setting
je.

content can conta
sure it's accurat

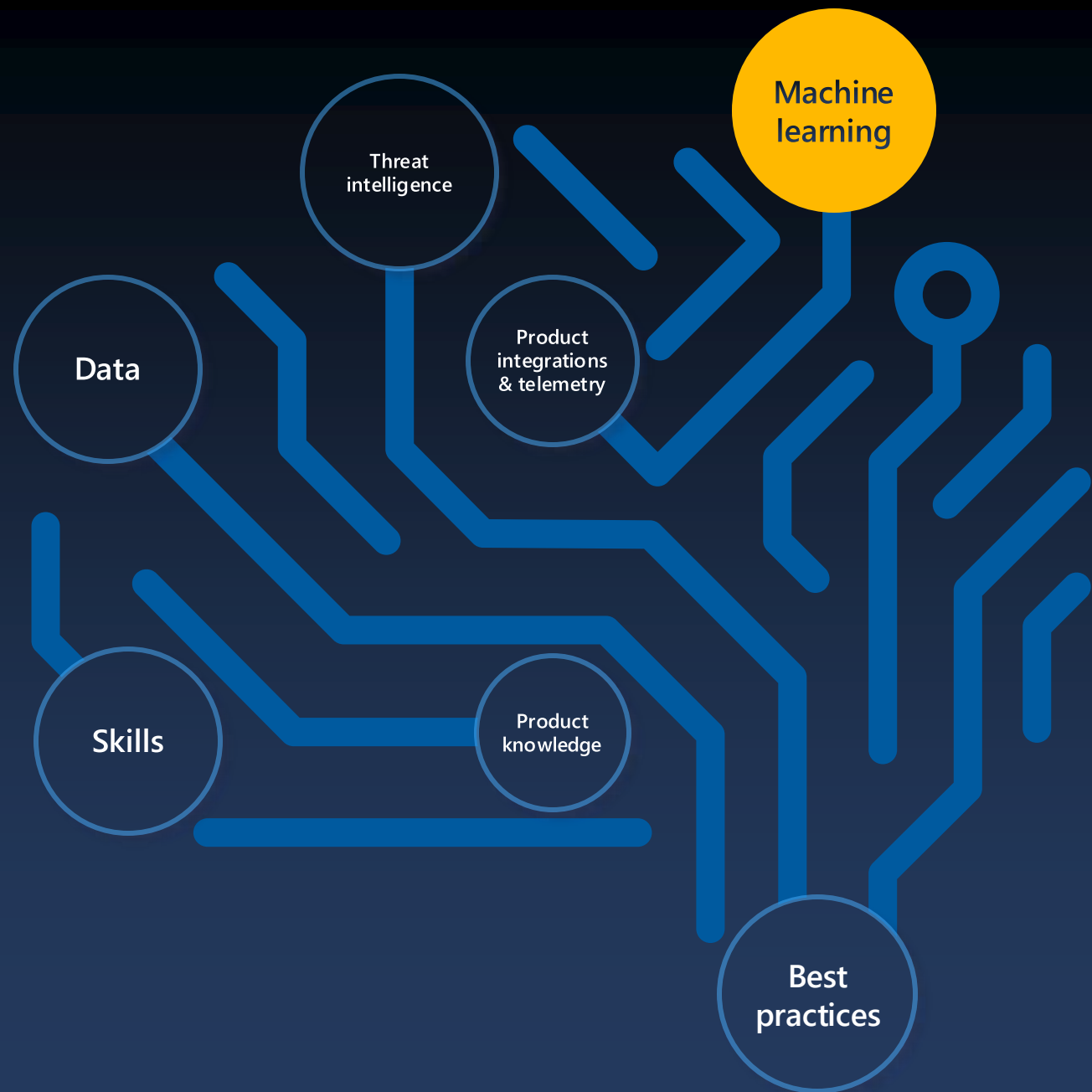
Sources

Microsoft Security



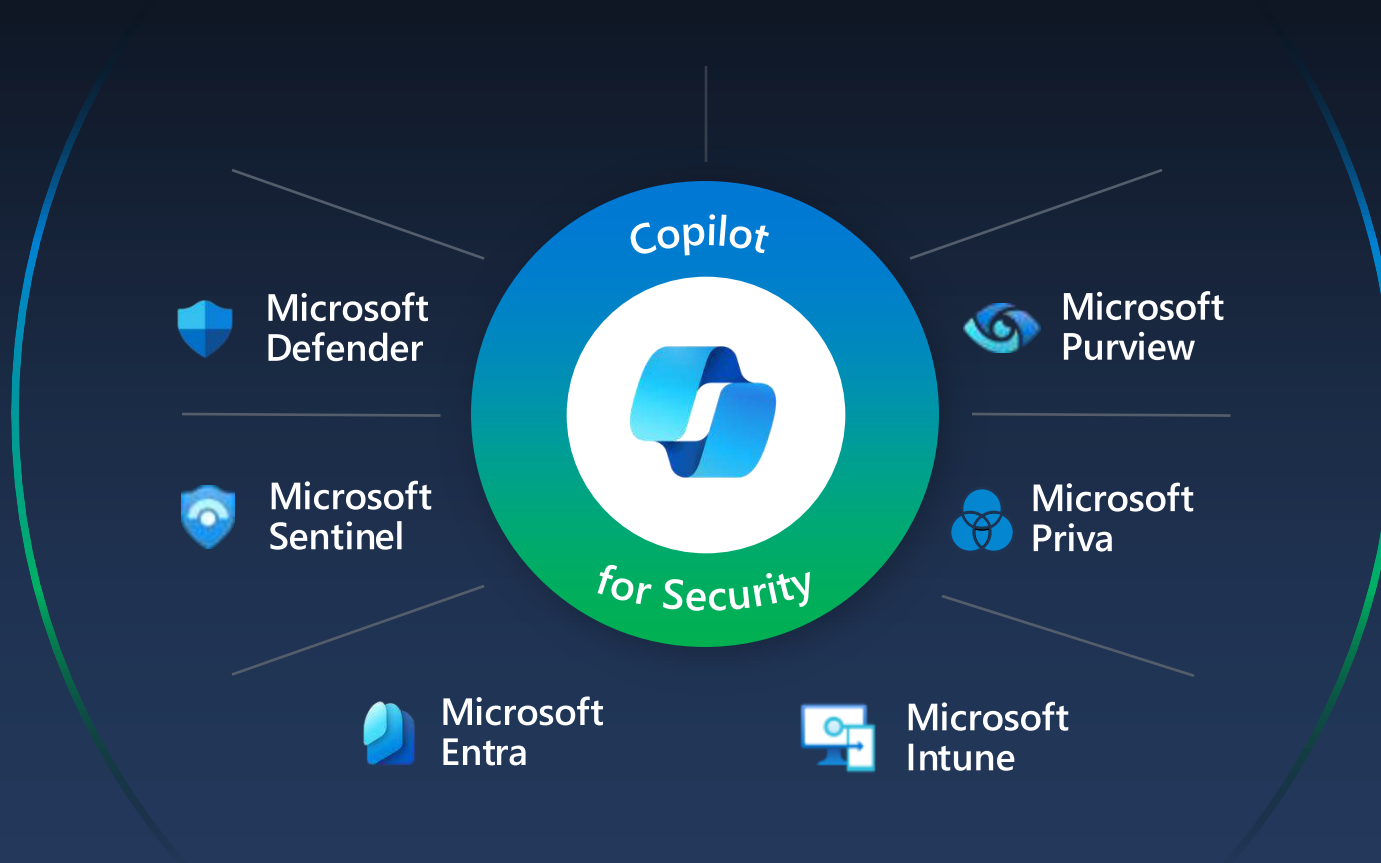
Microsoft Security Copilot

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



Microsoft's End-to-End Security

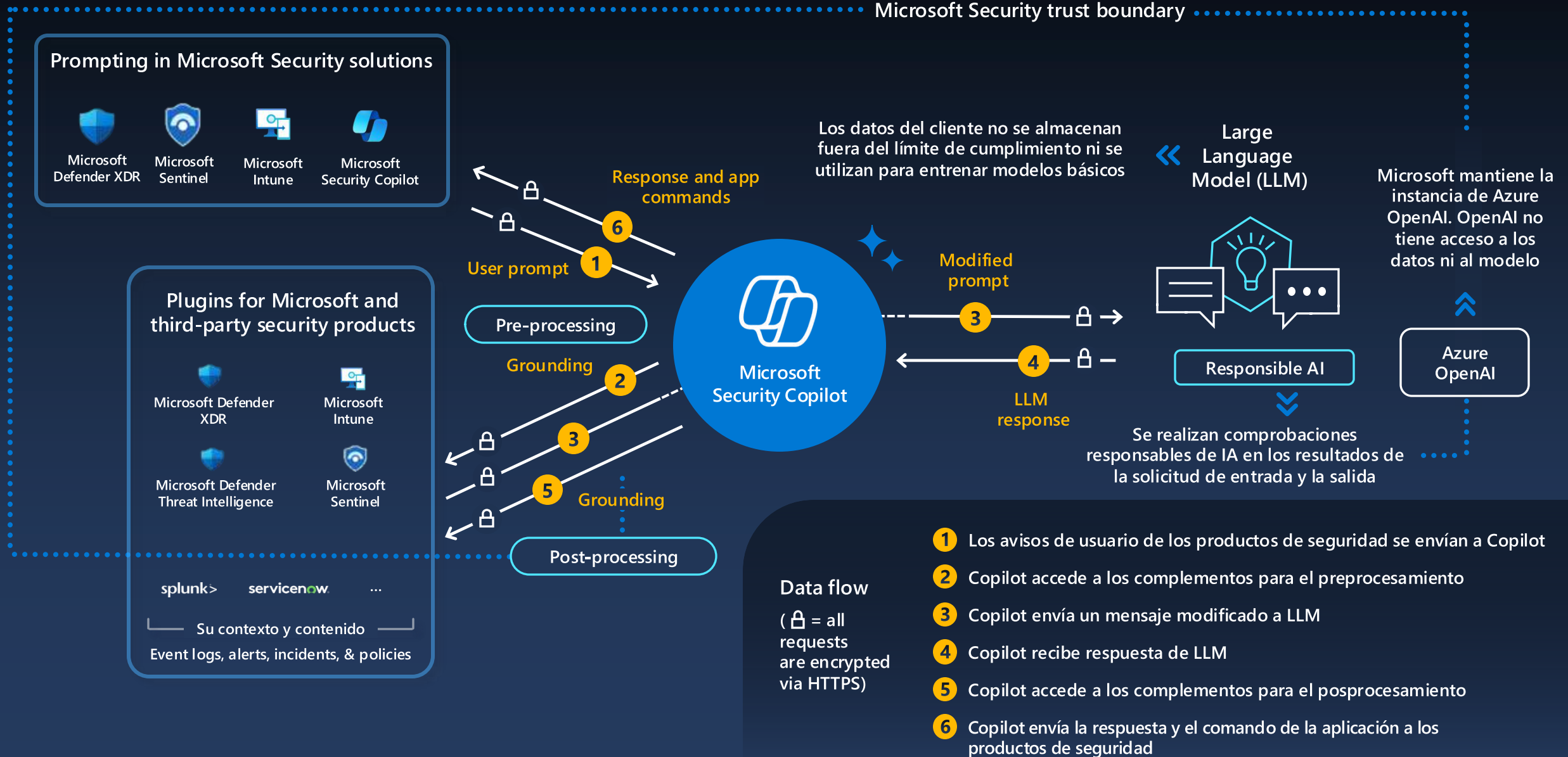
Microsoft Threat Intelligence



GBM Cybersecurity Center

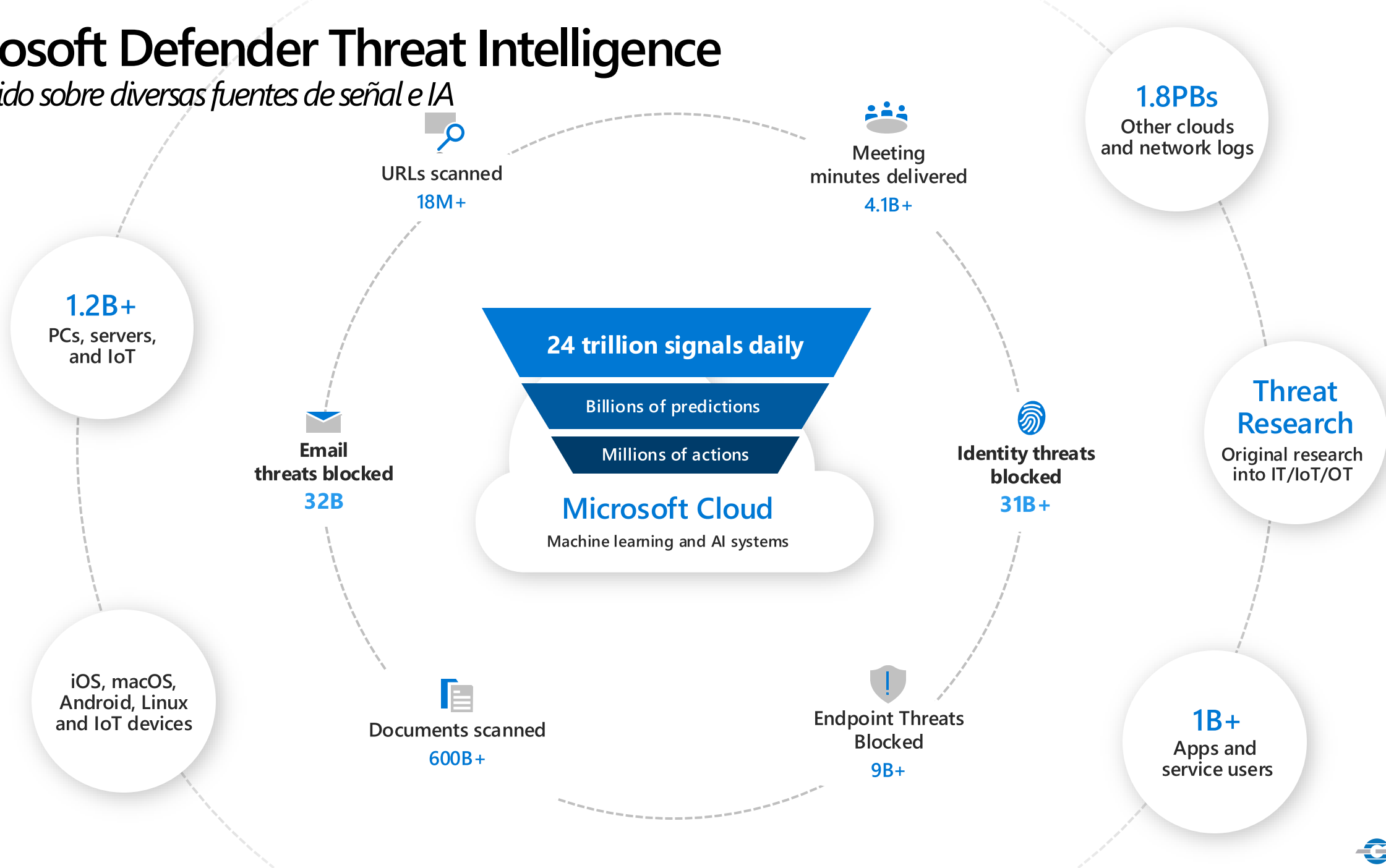


Flujo de datos para Microsoft Copilot for Security

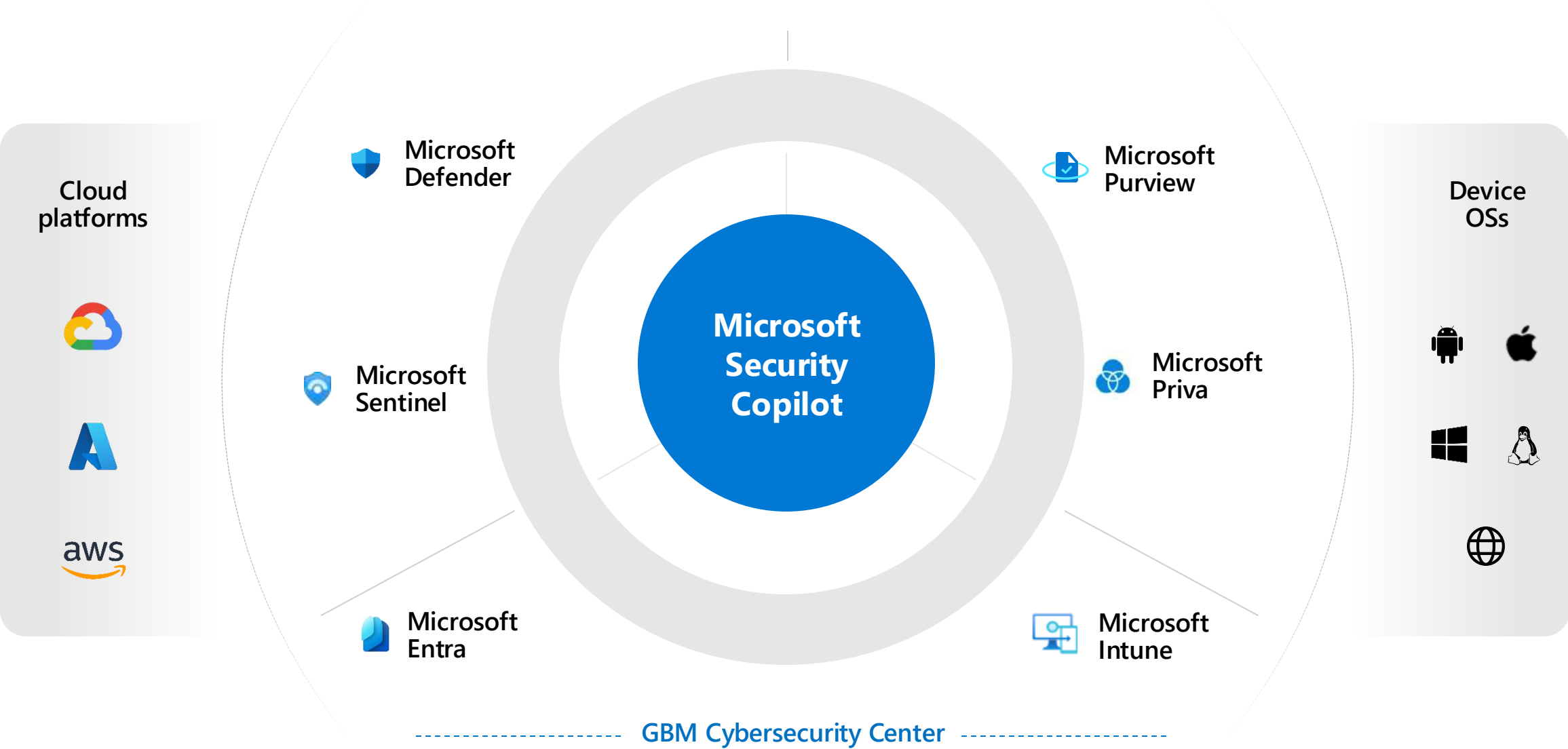


Microsoft Defender Threat Intelligence

Construido sobre diversas fuentes de señal e IA



Portafolio de Seguridad de Microsoft



 ¿Cómo puedo mejorar mi postura de seguridad?

 ¿Alguna de mis máquinas se ve afectada?

 Resume este incidente en viñetas.

 ¿Cuáles son las alertas que más se activan?

 ¿Qué es log4shell?

 Cuéntame sobre el incidente de Defender 20259.

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

Security Copilot in Unified SOC Platform

Contexto inteligente para alertas e incidents

Evaluación rápida para las amenazas emergentes y la exposición de su organización. Respuestas con información enriquecida e impulsada por IA.

Investigación y respuesta rápidas

Security Copilot proporciona soporte integral a los analistas. Desde resúmenes de incidentes y respuestas, hasta la evaluación del impacto de los incidentes, pasando por recomendaciones prácticas para una investigación y corrección más rápidas.

Desbloquea habilidades avanzadas de SOC

Desbloquea nuevas habilidades que permiten a los analistas de todos los niveles completar tareas complejas, traduciendo lenguaje natural a KQL o analizando scripts maliciosos.

The screenshot displays the Microsoft Defender Unified SOC Platform interface. The left sidebar contains a navigation menu with the following items: Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, SOC optimization, Reports, Learning hub, Trials, and More resources. The main content area shows an incident titled "SAP financial process manipulation (attack disruption)". The incident details include a severity of "High", a status of "Active", and a user "ajourn@woodgrove.ms". A yellow banner indicates: "Important! Attack disruption has automatically locked the SAP user account. For more details, select the Assets > Users tab or go to the Action center." Below this, there are tabs for "Attack story", "Alerts (36)", "Assets (10)", "Investigations (6)", "Evidence and Response (45)", "Recommended actions (20)", "Summary", and "Similar incidents (2)". The "Alerts" tab is selected, showing a list of alerts with timestamps and descriptions such as "Email messages containing malicious URL removed after delivery". A central "Incident graph" shows a network diagram of the incident. On the right, the "Copilot" panel provides a summary of the incident and a detailed "InitialAccess" section, which states: "The high severity incident 'SAP financial process manipulation' occurred between 2024-02-25 00:13:55 UTC and 2024-02-29 20:20:07 UTC. It was tagged as Credential Phish and triggered an automatic Attack Disruption action." The "InitialAccess" section also includes details about the incident's timeline and the user's actions.

Security Copilot in Microsoft Intune

Respuesta más rápida

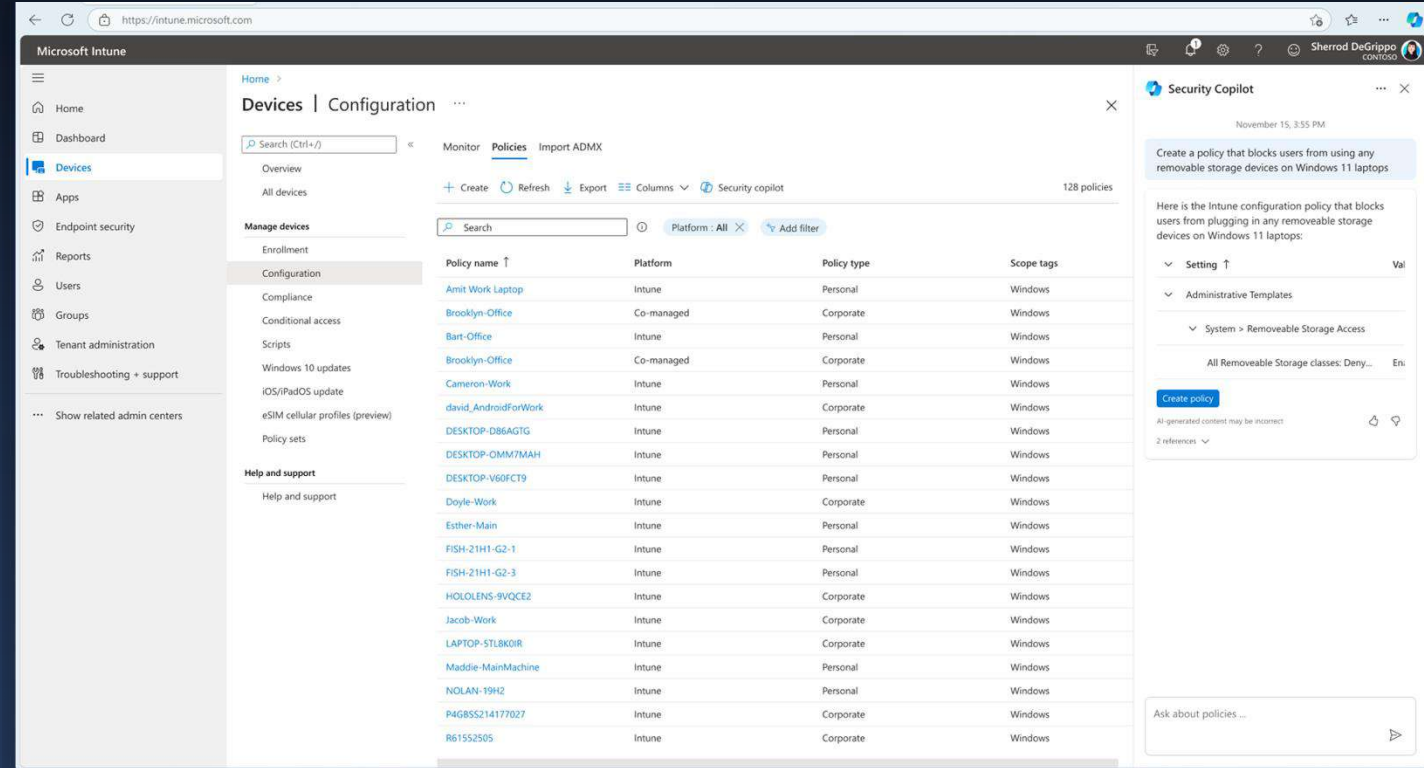
Responde rápidamente a amenazas, incidentes y vulnerabilidades con el contexto completo del dispositivo y la información y las acciones asistidas por IA.

Resultados más informados

Aplica de forma proactiva políticas específicas y solucione los problemas de los endpoints con análisis hipotéticos, orientación práctica y una comprensión profunda del estado del dispositivo, el usuario y la aplicación.

Gestión simplificada de la postura

Traduce rápidamente la intención empresarial en configuraciones y políticas recomendadas y compatibles mediante lenguaje natural.



Security Copilot in Microsoft Entra

Investigación rápida de riesgos de identidad

Explora los inicios de sesión y los usuarios de riesgo, comprendiendo el "por qué" y obteniendo información contextualizada sobre qué hacer para proteger las cuentas, todo en lenguaje natural.

Solución de problemas más rápido

Con el contexto al alcance de la mano, se encuentran brechas en las políticas de acceso, generando flujos de trabajo de identidad y llegando a la raíz del problema más rápido.

Nuevos niveles de eficiencia

Las recomendaciones guiadas permiten a los administradores de todos los niveles completar tareas complejas, como investigaciones de incidentes. El análisis del registro de inicio de sesión elimina la necesidad de realizar una inspección manual.

The screenshot displays the Microsoft Entra admin center interface. The left sidebar shows the navigation menu with categories like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, User experiences, Hybrid management, Monitor & health, Sign-in logs, Audit Logs, and Learn & support. The main content area is titled 'Sign-in events' for the 'Contoso' tenant. It includes filters for Date (Last 24 hours), Show dates as (Local), User contains (Adriana Giorgi), and Authentication requirement (Multifactor authentication). A table lists sign-in events with columns for Date, Request ID, User, Application, Status, IP address, and Location. The table shows several failed sign-in attempts for user 'Adriana Giorgi' from IP addresses 131.107... and 167.220... on 08/24/2023. A 'Copilot can help troubleshoot' button is visible. On the right, a 'Security Copilot' panel provides a natural language explanation: 'Why was Adriana Giorgi forced to MFA? The user was attempting to access the Microsoft Office 365 Admin portal. This application is in scope of the Conditional access policy 'Require MFA for admin portals' which requires all users requesting access to satisfy MFA.' It also includes a 'View sign-ins' link and a disclaimer: 'All generated content may be incorrect.' At the bottom of the panel, there are prompts like 'Which applications had the most failed sign-ins in the last 24 hours?' and 'What is the MFA requirement policy?'. The top right of the interface shows the user profile 'Connie Wilson' and the 'Copilot' logo.

Date	Request ID	User	Application	Status	IP address	Location
08/24/2023, 7:56...	bd008295...	Adriana ...	Salesfo ...	Failed	131.107...	Redmond...
08/24/2023, 7:56...	ff3f5f53-f...	Adriana ...	Salesfo ...	Failed	167.220...	Bellevue...
08/24/2023, 7:56...	683a2c9c...	Adriana ...	Salesfo ...	Success	131.107...	Redmond...
08/24/2023, 7:56...	167b3ed9...	Adriana ...	Salesfo ...	Success	131.107...	Redmond...
08/24/2023, 7:56...	cd632fc0l...	Adriana...	Salesfo ...	Success	167.220...	Bellevue...
08/24/2023, 7:56...	a4a26c12...	Adriana ...	Salesfo ...	Interrupted	167.220...	Bellevue...
08/24/2023, 7:56...	35c8243e...	Adriana ...	Salesfo ...	Success	131.107...	Redmond...

Security Copilot in Microsoft Purview

Visibilidad escalada

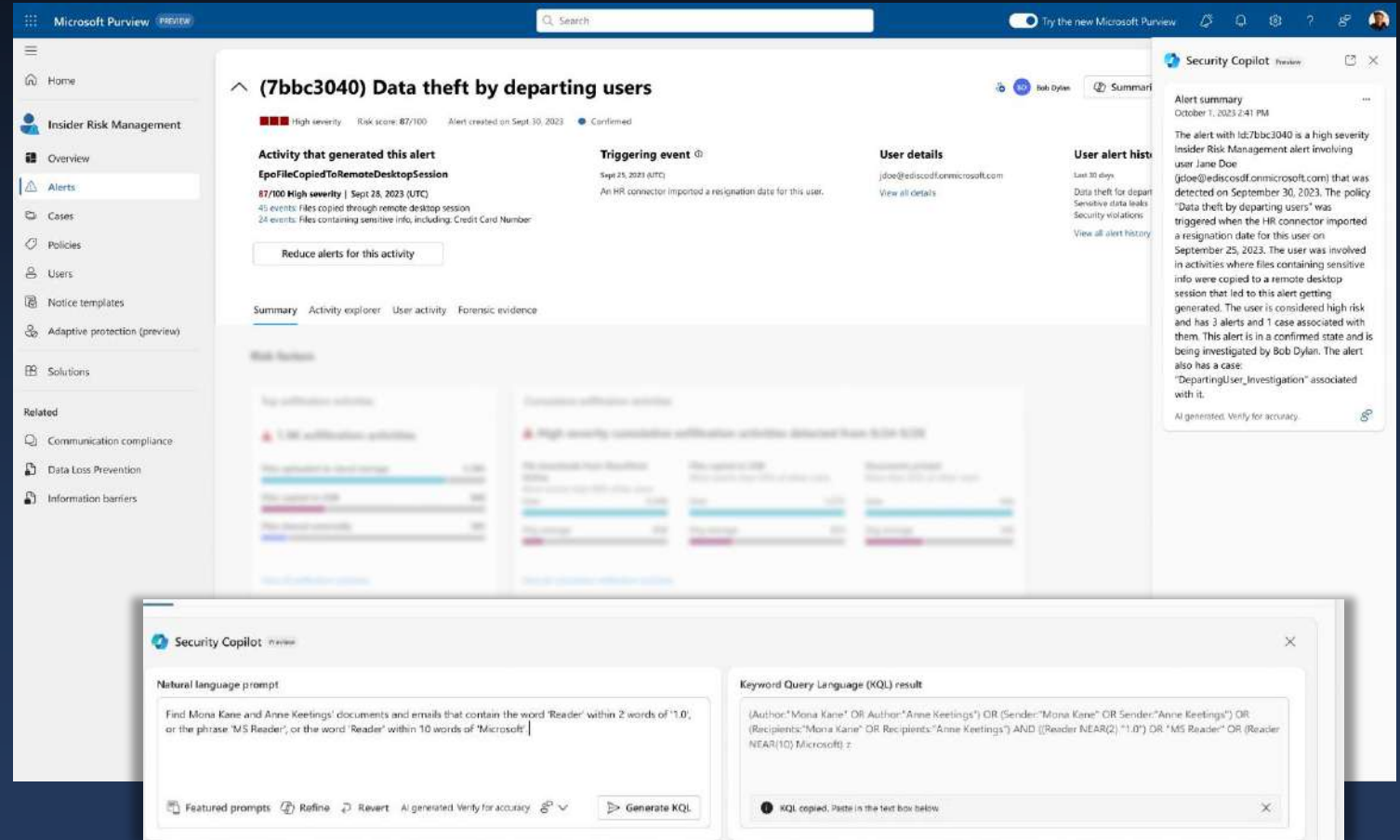
Visibilidad completa e integrada de todas las soluciones y una visión de los requisitos normativos de cumplimiento relevantes.

Resumen para la velocidad

Resumen rápido de las alertas que contienen una amplia gama de señales y contenido extenso para revisarlas desde el punto de vista de las políticas de seguridad y cumplimiento de datos.

Desbloquea habilidades expertas

Orientación paso a paso, realizando búsquedas en lenguaje natural y realiza investigaciones avanzadas sin lenguaje de consulta de palabras clave.



Security Copilot in Microsoft Defender for Cloud

Comprensión rápida de la postura

Identifica los riesgos más rápido aprovechando la información contextual de los datos confidenciales, las vulnerabilidades críticas, el movimiento lateral y mucho más.

Corrección guiada

Profundiza los riesgos críticos y recibe recomendaciones guiadas para priorizar las acciones de corrección más rápido, todo en lenguaje natural.

Trabaja de forma más inteligente

Información contextual sobre el riesgo, desgloses resumidos y orientación paso a paso a lo largo de una investigación. Identifique rápidamente a los usuarios clave y delegar la corrección.

The screenshot displays the Microsoft Defender for Cloud Recommendations interface. The main panel shows a list of recommendations categorized by risk level (Critical, High, Medium, Low, N/A). The 'Active recommendations by risk' section shows 48 Critical, 55 High, 180 Medium, 1297 Low, and 3448 N/A recommendations. The 'Defender resource coverage' section shows 105 Full, 105 Partial, and 207 Not covered resources. The 'Risk factors' section shows 216 Active attack paths, 1811 Affected resources, and 342 Overdue recommendations.

The 'Recommendations' table lists the following items:

Risk level	Title	Affected resource	Risk factors	Attack paths	Status
Critical	Management ports should be closed on your virtual machine	mdc-demo-w2022	Exposure to the internet	4	Overdue
Critical	All network ports should be restricted on network security group...	mdc-demo-w2022	Exposure to the internet	+2	Overdue
Critical	API endpoints in Azure API Management should be authenticated	modify-resource	Exposure to the internet	+3	Overdue
Critical	SQL databases should have vulnerability findings resolved	samplecrmesdemo1	Exposure to the internet	+2	Overdue
Critical	API endpoints in Azure API Management should be authenticated	submitsession	Exposure to the internet	+3	Overdue
Critical	EC2 instance should use IMDSv2	mdc-demo-w2022	Exposure to the internet	+1	Unassigned
Critical	EC2 instance should not have a public IP address	i-09e4c865a0f5675ec1	Exposure to the internet	+3	Unassigned
Critical	EC2 instance should not have a public IP address	i-04e65c8f12mz75ec1	Exposure to the internet	+3	Unassigned
Critical	EC2 instance should not have a public IP address	i-02e65438f0f5675ec1	Exposure to the internet	+2	Unassigned
Critical	EC2 instance should not have a public IP address	i-03e6123ct0f5675ec1	Exposure to the internet	+2	Unassigned
Critical	EC2 instance should not have a public IP address	i-15ev7438d15675ec1	Exposure to the internet	+3	Unassigned
Critical	EC2 instance should not have a public IP address	i-06e52438f0f5675ec1	Exposure to the internet	+1	Unassigned
Critical	EC2 instance should use IMDSv2	i-07e65ht560f5675ec1	Exposure to the internet	+3	Unassigned
Critical	Management ports of EC2 instances should be protected with...	i-01e6ty56f0f5675ec1	Exposure to the internet	+3	Unassigned
Critical	Management ports of EC2 instances should be protected with...	i-06e34w856a575ec3	Exposure to the internet	+2	Unassigned
Critical	EC2 instance should not have a public IP address	i-01e6k3u6erf5675ec1	Exposure to the internet	+2	Unassigned

The 'Security Copilot' sidebar on the right provides a summary of the findings:

- 13 publicly exposed resources require attention
- There are 13 publicly exposed resources, each carrying a range of potential threats such as unmanaged workloads, human errors, misconfigurations, data breaches, privacy and compliance issues, performance degradation, and security vulnerabilities.
- Here's a breakdown of the specific resources at risk:
 - 9 VMs with internet exposure and high severity vulnerabilities
 - 1 AWS S3 bucket that's publicly accessible, housing sensitive data
 - 1 SQL with excessive internet exposure, allowing basic authentication and containing sensitive data
 - 2 API endpoints lacking authentication, transmitting sensitive information.

The sidebar also includes a 'Show results' button and a note: 'AI generated. Verify for accuracy.'

Microsoft Defender Threat Intelligence (MDTI)

Inteligencia de amenazas terminada

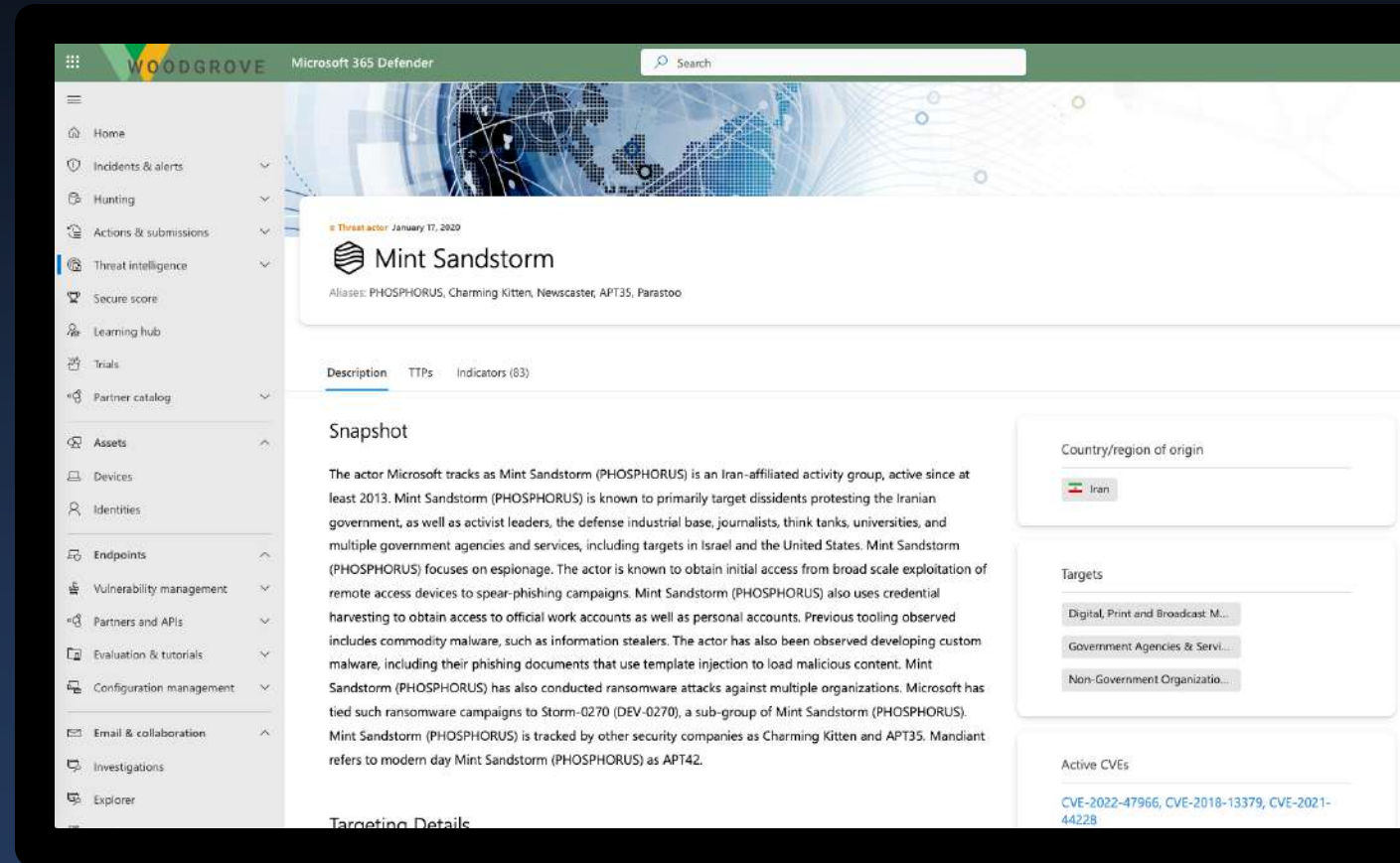
Consulte una biblioteca de artículos de inteligencia terminados, perfiles de inteligencia e informes de actividad, incluidos indicadores procesables y TTP creados y mantenidos por 10.000 expertos en seguridad para comprender y contextualizar rápidamente las amenazas.

Inteligencia de amenazas sin procesar

Pivote sobre conjuntos de datos únicos creados a partir de la detección automatizada y el análisis continuo en toda la infraestructura mundial para ayudarle a comprender la gravedad de una amenaza, bloquear los ataques de forma proactiva e inocular a la organización de futuras amenazas.

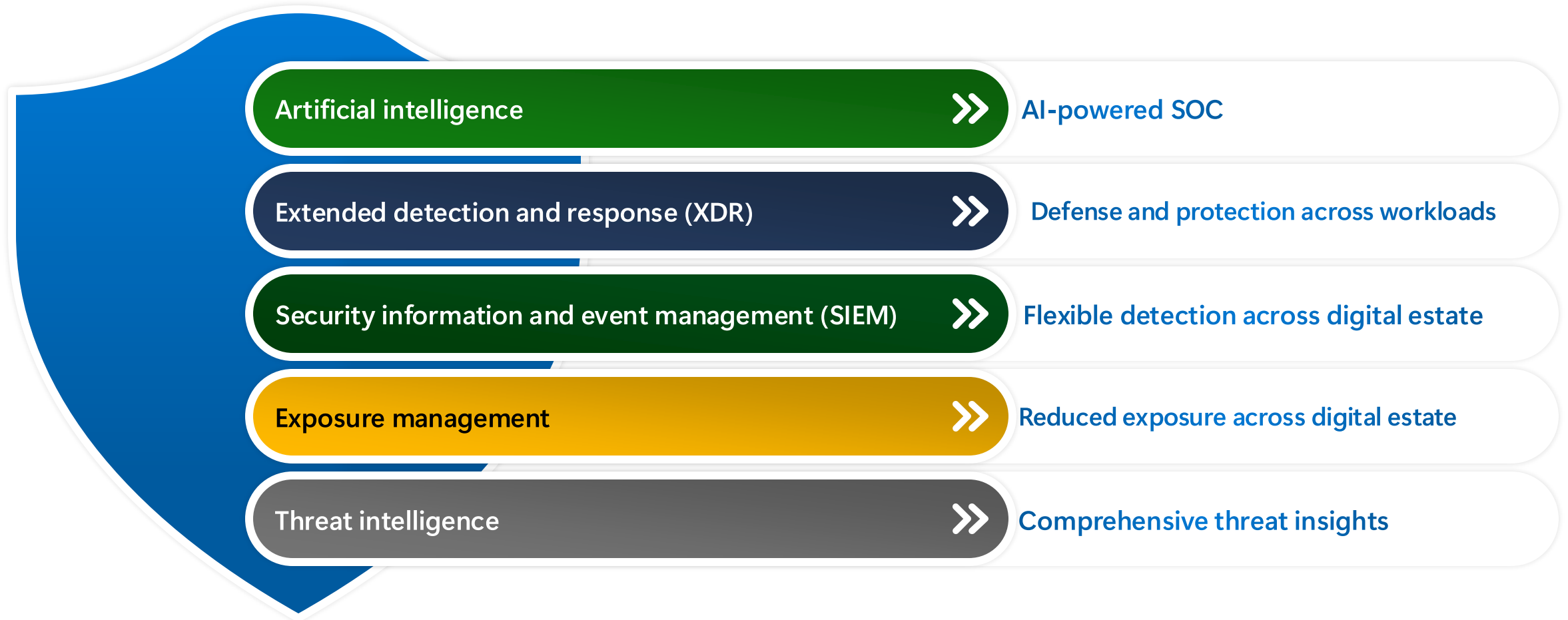
MDTI API

Mejore las herramientas y los flujos de trabajo existentes de SIEM y XDR enriqueciéndolos con inteligencia de amenazas hiperrelevante y un profundo conocimiento del panorama global de amenazas.



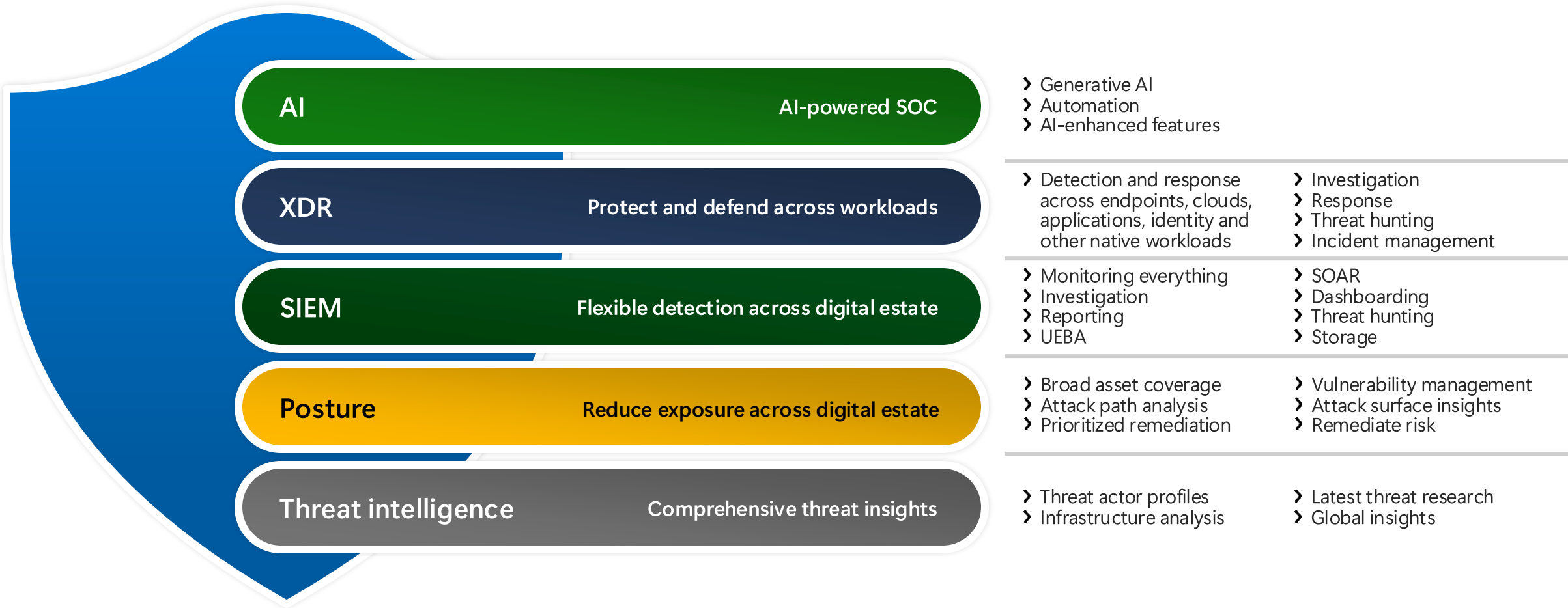
Under NDA only

Transforme SecOps con una **Plataforma unificada**



Construido desde cero para operaciones de seguridad

Experiencia de analista optimizada | Asistencia específica | Protección y corrección automatizadas



Microsoft Security Exposure Management

Reduzca su exposición al riesgo

Reducción de la superficie expuesta a ataques
con una gestión unificada de la exposición



- 
-  Exposure management

 Overview

 Attack surface

 Map

 Attack paths

 Exposure insights

Initiatives

Metrics

Recommendations

Events

 Secure score

 Data connectors

 Assets

 Endpoints

 Identities

 Email & collaboration

 Cloud apps

 Reports

 Health

 Permissions

 Settings

 More resources

Exposure management overview

 Add a suggestion

 Guided tour

How protected is your organization?

Our security exposure management tool offers key insights, metrics and customized initiatives for a centralized overview of your risk landscape.

Your assets, at a glance



Vulnerability status



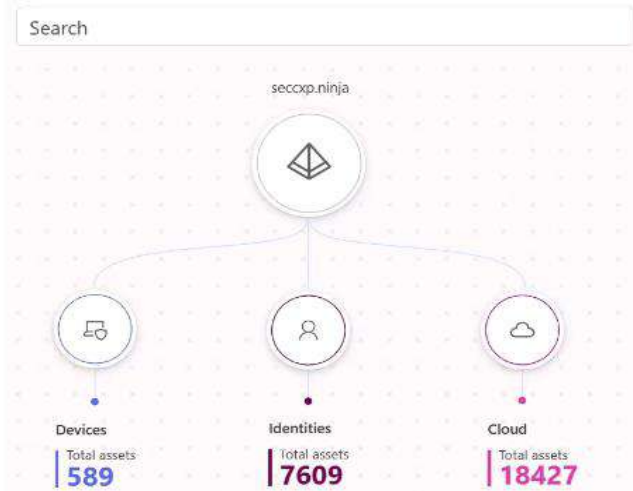
Key initiatives

[See all](#)

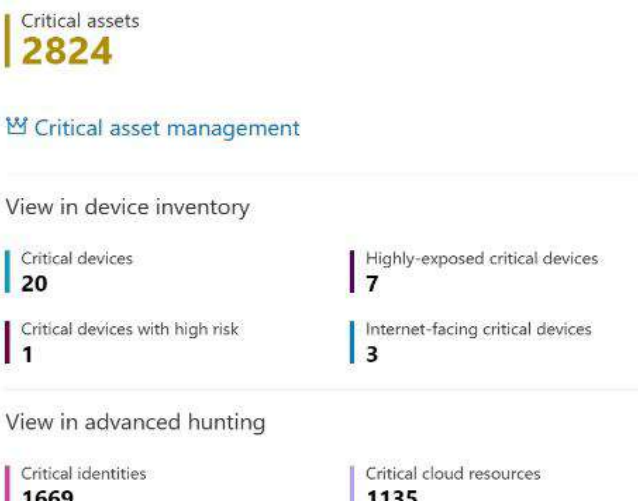
Top metrics

Name	Current V
% of missing best practices for devices against "On-premise...	100%
% of endpoints where the host Firewall is disabled or misco...	100%
% Azure relational database without geo-redundant backup...	100%
% containers images with high severity vulnerabilities	100%
% of missing best practices in Sharepoint Admin Center to ...	100%
% storage accounts without network access restriction usin...	99.17%

Attack surface map



Critical asset summary



Managed Detection & Response for Microsoft

GBM Cybersecurity Center



GBM Managed Detection and Response

+100 Specialist Cybersecurity

Incident Response | Forensic Analysis | Purple Teaming
Recover | Cybersecurity Execution Support | Staffing

Alliance Partners



Threat Intelligence
70M+ signals per day of security context



Microsoft Security Copilot



Machine Learning (ML) & AI
Behavioral Analytics (UEBA)

Case Management

Security Orchestration, Automation, and Remediation (SOAR)



Microsoft Defender XDR

Microsoft 365 Defender

Defender for Cloud

Defender for Identity | Entra ID Protection | Defender for Endpoint | Defender for Office 365 | Defender for Cloud Apps



Hybrid Infrastructure – IaaS, PaaS, On-Premises

API Integration

Passwordless & MFA

Hello for Business
Authenticator App
FIDO2 Keys

Entra ID Protection
Leaked cred protection
Behavioral Analytics

ID Governance

Microsoft Entra PIM

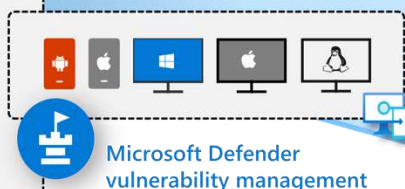
External Identities

Defender for Identity

Active Directory



3P SaaS



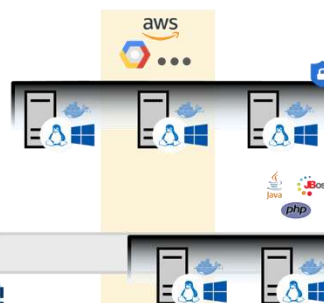
Microsoft Defender vulnerability management

Microsoft Azure

Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Arc

Microsoft Sentinel

3rd party IaaS & PaaS



On Premises Datacenter(s)

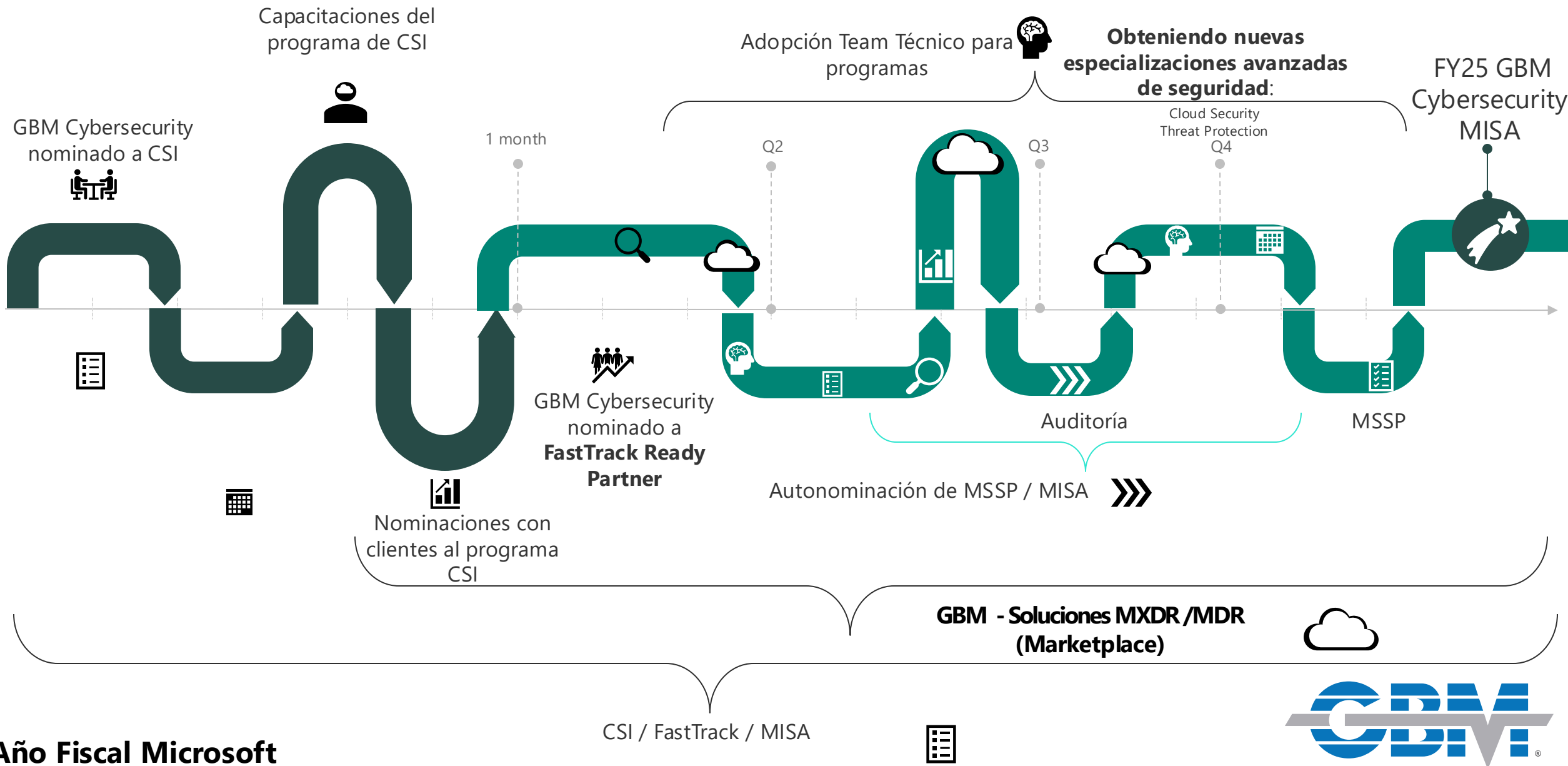
Security & Network

Firewalls
Edge DLP
IPS/IDS/NDR
VPN & Proxy

Carbon Black, Symantec, Fortinet, Sophos, Zscaler, Fireeye, CyberArk, Lookout, Palo Alto, Check Point, Cisco, etc.

GBM Managed Security Service for Microsoft

GBM Cybersecurity FY25 | Overview





GBM Cybersercurity Investment



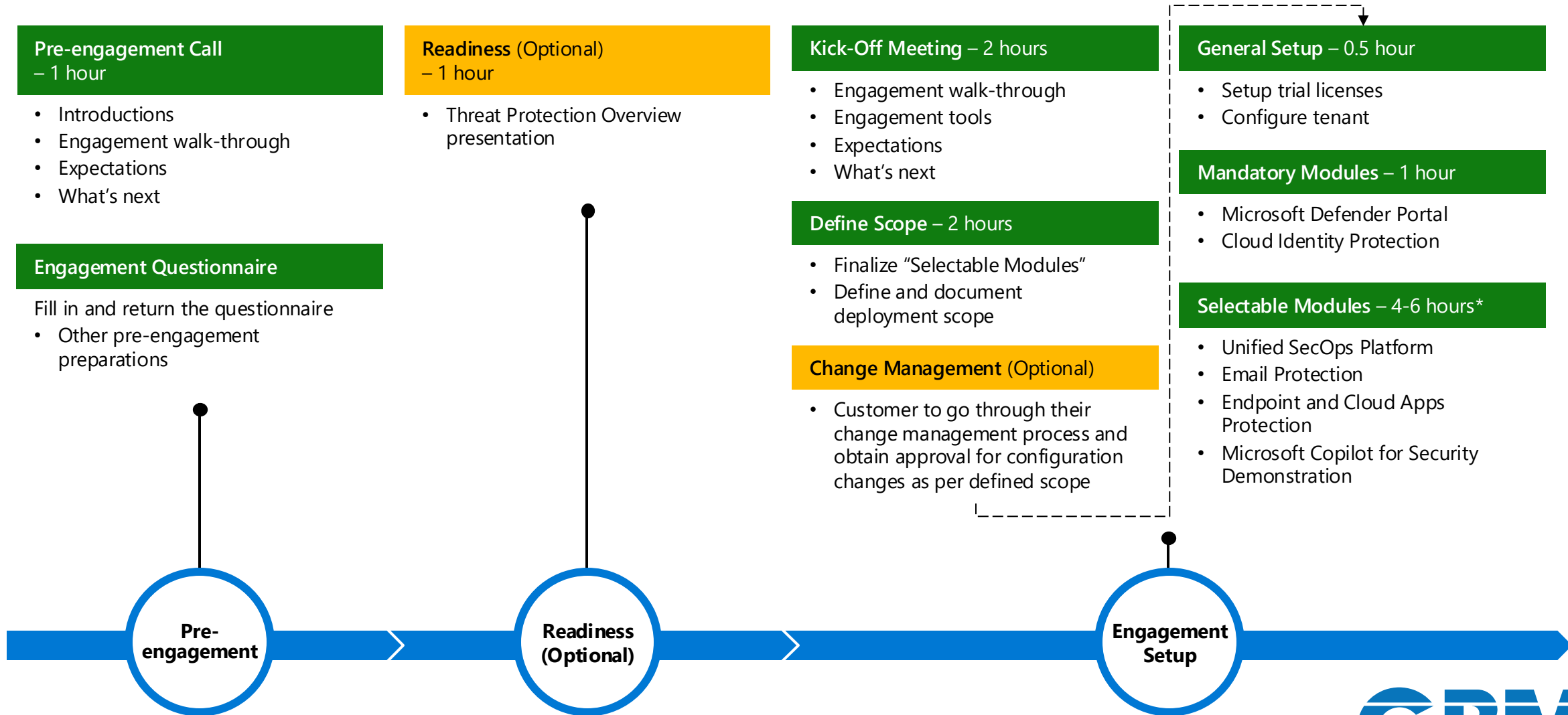
GBM en las Américas ahora forma parte de la iniciativa de **Inversión en Ciberseguridad (CSI) de Microsoft**. El programa de CSI es una inversión solo por invitación realizada por Microsoft a socios que cumplan ciertas especializaciones avanzadas de seguridad. Esta inversion está diseñada para acelerar **la adopción de plataformas de seguridad Microsoft 365 y Azure Security** a través de actividades de consultoría con los clientes.

Esta inversion tiene un alcance de dentro del año fiscal de Microsoft (FY25) el cual, nos permite posicionar a GBM como un asesor de seguridad de confianza.

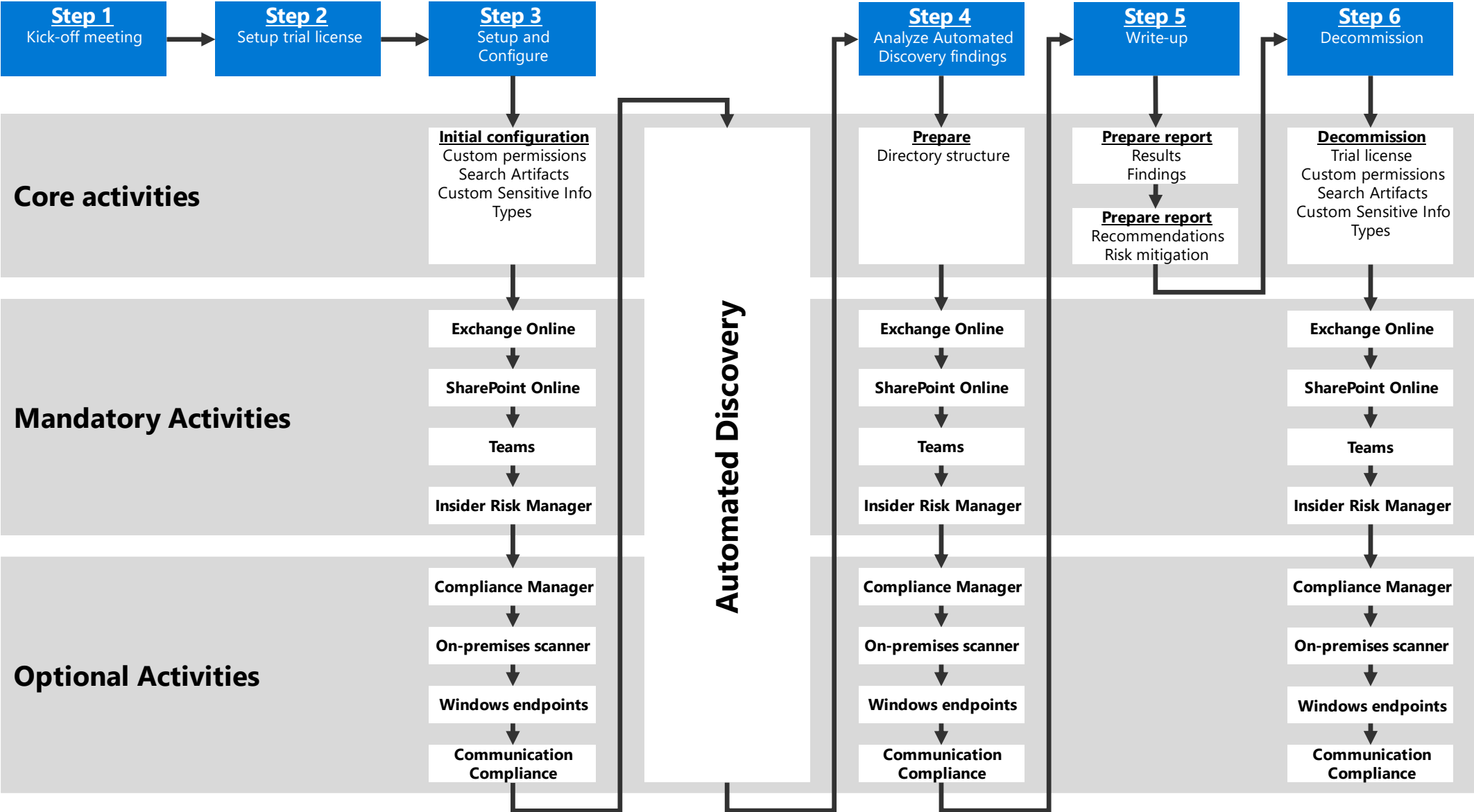
- Threat Protection Engagement (Microsoft Defender XDR)
- Data Security Engagement (Microsoft Purview)
- Modern Sec Ops (Microsoft Sentinel / Microsoft Copilot for Security)

Requisitos: (+500 licencias de Microsoft Entra ID Premium P1 y +250 usuarios activos en Exchange Online, SharePoint Online or Teams).

Threat Protection Engagement



Data Security Engagement



FAQ'S





¡Gracias!

ευχαριστώ Salamat Po متشكراً شكراً Grazie

благодаря ありがとうございます Kiitos Teşekkürler 谢谢

ໝາຍຄຸນຄວັບ Obrigado شكریه Terima Kasih Dziękuję

Hvala Köszönöm Tak Dank u Wel ДЯКУЮ Tack

Mulțumesc спасибо Danke Cám ơn Gracias

多謝晒 Ďakujem תודה நன்றி Děkuji 감사합니다