Microsoft Security

Defensa coordinada: Creación de un SOC unificado con tecnología de IA

Contenido

El nuevo panorama de amenazas: resumen ejecutivo

El panorama de amenazas es más complejo que nunca. Mientras que los equipos de seguridad tienen que defender el entorno digital más diverso de la historia, los atacantes tienen más recursos y capacidad que nunca. Han pasado a organizar campañas sofisticadas que encadenan múltiples vulnerabilidades en tus sistemas, lo que crea cadenas de ataque complejas adaptadas específicas a tus entornos. Además, la rápida adopción y el crecimiento del cloud y la IA les están ayudando a ampliar sus operaciones, lo que marca el inicio de una nueva era de ingeniería social, descubrimiento de vulnerabilidades y alcance operativo.

Ya no basta con abordar las amenazas con enfoques tradicionales, como centrarse en proteger los puntos de conexión del ransomware o segmentar las redes para restringir el acceso. Los atacantes aprovechan múltiples vulnerabilidades en tus sistemas, como nodos de un gráfico complejo, para pasar desapercibidos y acceder a activos críticos y datos confidenciales. Las herramientas de seguridad tradicionales que funcionan en silos simplemente no están a la altura.

Las organizaciones de hoy en día necesitan implementar un enfoque de defensa en profundidad que utilice herramientas de seguridad profundamente integradas que funcionen juntas para coordinar la defensa en todas las capas de seguridad. Estas soluciones incluyen IA y automatización, lo que permite a tu organización pasar de la reacción manual a la defensa automatizada y proactiva.

El panorama de amenazas actual: un cambio de táctica

Los atacantes emplean cada vez más herramientas y técnicas avanzadas en ataques dirigidos de varias etapas. Entre las principales tendencias se incluyen:

Ingeniería social con tecnología de IA

Los atacantes utilizan la IA generativa para elaborar mensajes de correo electrónico de phishing sumamente personalizados y otras comunicaciones, a menudo orquestando ataques multicanal donde, por ejemplo, un ping aparentemente inocente en Teams prepara al objetivo antes de que llegue un correo electrónico malintencionado a su bandeja de entrada.

Muchos de estos ataques ni siquiera contienen enlaces sospechosos; en lugar de ello, podrían empezar con un mensaje aparentemente urgente de una dirección de correo electrónico suplantada que parece legítima, advirtiendo de una factura que «requiere el pago inmediato». **Estas comunicaciones sofisticadas son más difíciles de detectar a través de métodos tradicionales como el análisis de enlaces o las firmas de malware.** Cada mensaje es único, eludiendo los sistemas de reconocimiento de patrones.

Malware de autoaprendizaje

El malware que incorpora modelos de lenguaje de gran tamaño (LLM) puede adaptarse y reescribirse en función de la configuración específica del dispositivo en el que está instalado, todo ello sin ninguna comunicación externa. Esta adaptación autónoma aumenta su sofisticación y resiliencia, lo que la hace especialmente peligrosa, ya que puede funcionar y evolucionar incluso cuando está aislada de servidores de mando y control.

Explotación de la deuda técnica

Aunque la aplicación de parches de software y la implementación de MFA siguen siendo defensas cruciales, los actores de amenazas están aprovechando cada vez más la deuda técnica (sistemas obsoletos, vulnerabilidades sin parches, infraestructura obsoleta, etc.) que muchas organizaciones tienen dificultades para mantener. **Incluso las organizaciones que dominan las medidas de seguridad tradicionales son vulnerables, porque los atacantes apuntan específicamente a estos puntos débiles heredados.** Las integraciones de dispositivos no administrados y sistemas con poca supervisión se han convertido en objetivos particularmente atractivos debido a sus brechas de seguridad que suelen pasarse por alto.

Ataques a cuentas genéricas y multiusuario

Las identidades siguen siendo un objetivo principal: los ataques de contraseña aumentaron de 579 a 7000 por segundo desde 2021[1]. Los atacantes cada vez más dirigen sus ataques a las cuentas administrativas y compartidas, explotando las contraseñas obsoletas y el acceso compartido que complican la implementación de MFA. El número de actores que realizan estos ataques ha crecido considerablemente, de 300 en 2023 a 1500 en 2024[2].

[1, 2] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Lecciones aprendidas de la línea del frente

Como se ha demostrado claramente en los últimos 12 meses trabajando con listas de vulnerabilidades, no basta con mantenerse al día con los parches e implementar herramientas de seguridad para proteger vectores críticos. Ninguna organización, ni siquiera Microsoft, podrá superar a los atacantes simplemente aplicando parches. **Tenemos que dejar de centrarnos en las listas de vulnerabilidades y empezar a pensar como un atacante, viendo esas vulnerabilidades no como una gran colección de puntos aislados, sino como un conjunto ordenado de rutas que conducen a activos críticos.**

Los ciberataques recientes han dejado esta necesidad más clara que nunca. Una de las principales cosas que aprendimos fue que la deuda técnica representa la mayor debilidad de las organizaciones. Aunque es posible que utilices las últimas herramientas de seguridad para fortalecer tu entorno principal, los actores de amenazas encontrarán y explotarán puntos débiles en la infraestructura antigua, sistemas sin parches, configuraciones obsoletas y aplicaciones con privilegios excesivos, a menudo en áreas que los equipos de seguridad ni siquiera conocen.

El desafío se intensifica a medida que los actores malintencionados cuentan con más recursos y están mejor preparados, utilizando tácticas, técnicas y procedimientos (TTP) cada vez más sofisticados que ponen a prueba incluso a los mejores defensores de ciberseguridad del mundo. Nuestros clientes se enfrentan a más de 600 millones de ataques de ciberdelincuentes y de estados-nación cada día, que abarcan desde ransomware hasta phishing y ataques de identidad. Esto nos obliga a abordar las amenazas en el nivel de la técnica, no solo por vectores de ataque o vulnerabilidades más críticas.

Sin embargo, hay razones para tener esperanza en este panorama en constante cambio. Hemos observado una reducción del 300 % en los ataques de ransomware realizados con éxito entre los clientes que utilizan Defender para punto de conexión, incluso aunque los encuentros de ransomware generales han aumentado en un 275 %. Esto demuestra la efectividad de implementar un enfoque basado en plataformas que unifique políticas y controles, y que utilice IA y automatización para abordar proactivamente las debilidades y responder de forma dinámica a ataques directos.

Como resultado directo de estas experiencias y conocimientos, lanzamos la Iniciativa para un futuro seguro (SFI), un compromiso de toda la empresa de priorizar la seguridad por encima de todo lo demás. La SFI es la piedra angular de nuestros esfuerzos por proteger no solo a Microsoft, sino también a nuestros partners y clientes. Creemos que la seguridad es un deporte de equipo, y la SFI encarna esta filosofía, haciendo que la seguridad sea la principal prioridad de todos.

Poner la seguridad por encima de todo

La Iniciativa para un futuro seguro (SFI) de Microsoft es una iniciativa de varios años para mejorar la forma en que diseñamos, creamos, probamos y utilizamos nuestros productos y servicios, con el objetivo de alcanzar los más altos estándares de seguridad posibles.

Es nuestro compromiso a largo plazo de proteger tanto a la empresa como a nuestros clientes en el panorama de amenazas en constante evolución.

730.000

Aplicaciones no conformes con SFI eliminadas

5,75 millones

Inquilinos inactivos eliminados, lo que reduce drásticamente la superficie de ciberataque potencial

Un nuevo paradigma previo/posterior al ataque

Hacer frente a tus vulnerabilidades requiere algo más que simplemente tachar elementos de una lista. Incluso pequeñas brechas de seguridad pueden provocar ataques devastadores cuando los atacantes las encadenan. Entender estas cadenas de conexiones en tu entorno es casi imposible con las herramientas tradicionales, porque no comparten eficazmente la información de señales y amenazas. **Los equipos de seguridad actuales necesitan herramientas que funcionen en varios dominios (identidades, correo electrónico, aplicaciones, etc.) y que integren las funciones clave de seguridad, conectando la prevención, la gestión de exposiciones, la detección y respuesta, la administración de identidades, la arquitectura en el cloud y otras funciones críticas.**

Con las herramientas tradicionales, los equipos de seguridad se enfrentan a un problema fundamental: deben conectar manualmente los puntos entre herramientas separadas que no se comunican bien entre sí. Este proceso manual significa que las vulnerabilidades se gestionan de forma aislada, lo que impide ver la imagen completa hasta que se produce un ataque. Los equipos carecen a menudo de los recursos para entender sistemáticamente cómo se atacó su sistema hasta después de un incidente, lo que genera una postura de seguridad siempre reactiva.

De un enfoque reactivo y manual a uno proactivo y automatizado

- **Analizar las rutas** de ataque y reducir la exposición
- **Interrupción** de ataques en tiempo real
- **Unificar** la experiencia de investigación y acelerar la respuesta

Plataforma de operaciones de seguridad unificada: información general y arquitectura

Una plataforma unificada de operaciones de seguridad integra funcionalidades de protección para puntos de conexión, identidades, correo electrónico, aplicaciones, datos y entornos en el cloud con las funciones de SecOps críticas de administración de la postura de seguridad, detección y respuesta e información sobre amenazas en una sola experiencia. Esto va más allá de la experiencia de los analistas para unificar el inventario de entidades, los modelos de detección, la información sobre amenazas, los controles de seguridad y los flujos de trabajo en todas tus herramientas de seguridad fundamentales, **lo que ayuda a los equipos de seguridad a pasar de una reacción apresurada a un cribado e investigación más ágiles, una mejora del enfoque proactivo y la búsqueda unificada de amenazas.**

En lugar de administrar varias consolas y de tener que trabajar con herramientas dispares, los equipos de seguridad obtienen una única fuente de información, lo que agiliza las operaciones y acelera los tiempos de respuesta. Una plataforma moderna combina la inteligencia global de amenazas con funciones de SIEM, XDR, seguridad en el cloud, gestión de la exposición e IA, que abarcan todo el ciclo de vida de las amenazas.

Operaciones de seguridad unificadas

Una arquitectura unificada transforma las operaciones de seguridad mediante la centralización de los datos y el uso de la IA para mejorar la experiencia humana, lo que permite escalar, adaptarse y mejorar continuamente todo el ciclo de vida de las amenazas.

Las bases: datos sin procesar (registros de seguridad y actividad)

Las operaciones de seguridad son tan eficaces como sus datos. Esta capa recopila y centraliza los datos de entidades y actividades de conectores, API, registros de seguridad brutos y fuentes de inteligencia de amenazas. Esta consolidación cambia el enfoque de recopilar datos a convertirlos en acciones concretas.

Procesamiento y enriquecimiento de datos

Esta capa estandariza los datos y utiliza la IA para crear un modelo de gráfico relacional de todo tu ecosistema digital. La plataforma enriquece este modelo con inteligencia sobre amenazas, relaciona las alertas con información práctica y lo prepara para servicios impulsados por la IA como agentes, modelado de rutas de ataque y respuestas automatizadas. Esto garantiza que los equipos actúen a partir de información precisa y contextualizada.

Plataforma principal de seguridad

Esta capa mejora la defensa proactiva al permitir que tu plataforma de seguridad identifique los ataques en curso, prevea los pasos de los atacantes y automatice las respuestas para bloquear el movimiento lateral. Por ejemplo, relaciona la vulnerabilidades con posibles rutas de ataque mediante inteligencia sobre amenazas en tiempo real, priorizándolas para su remediación. Durante los incidentes, esta información permite prever el movimiento lateral y contenerlo.

Asistencia de expertos y servicios administrados de seguridad

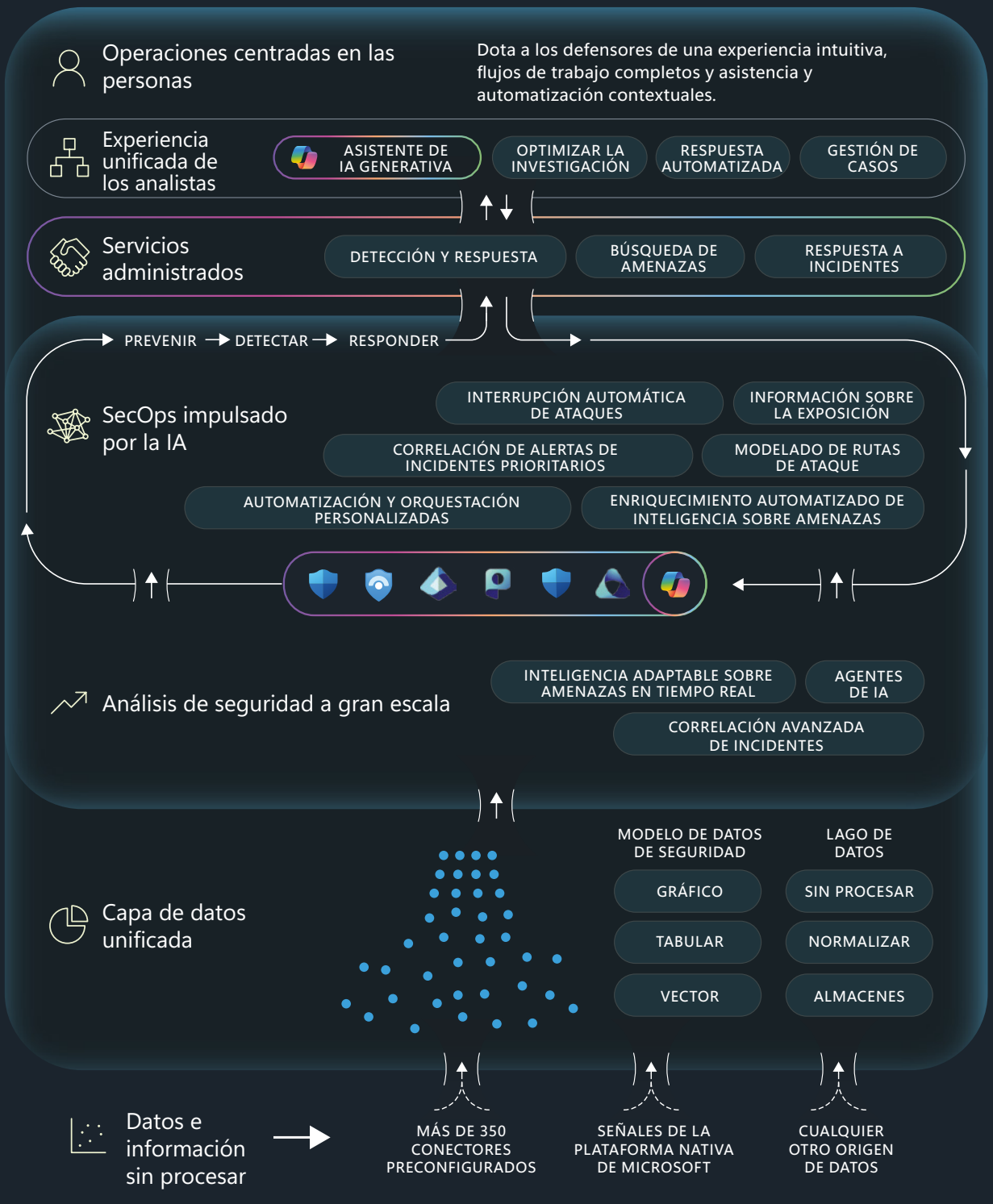
Muchos equipos de SOC utilizan servicios administrados para contar con experiencia y escalar sus operaciones. Una plataforma unificada integra flujos de trabajo de servicios administrados, que proporcionan a expertos externos visibilidad y conocimientos completos sobre las amenazas para una colaboración fluida con el equipo de SOC.

Experiencia unificada de los analistas

Esta capa proporciona una vista unificada de todos los datos de seguridad, alertas, incidentes y conocimientos. Los controles preventivos integrados permiten al equipo de SOC proteger la organización antes de que se produzca un ataque. Entre las características clave se incluyen la automatización para agilizar las tareas, la administración de casos para investigaciones y la IA generativa para mejorar el análisis y simplificar la generación de informes.

Arquitectura de SOC

La integración de datos, IA y conocimientos humanos permite a los equipos de seguridad prevenir, detectar y responder a las amenazas fácilmente durante todo el ciclo de vida.



Crear un enfoque de bucle cerrado para gestionar las amenazas

Una estrategia de seguridad moderna debe abordar el ciclo de vida completo de las amenazas, desde prevenir el acceso inicial hasta detectar e interrumpir ataques activos, así como investigar y responder a los incidentes. Una plataforma de seguridad unificada permite este enfoque de bucle cerrado conectando funciones de prevención, detección y respuesta en el entorno. **Examinemos cómo funciona cada fase en su conjunto para crear una estrategia de defensa completa.**

Prevenir: para una mejor defensa, piensa como un atacante

Una plataforma de seguridad unificada transforma la administración de vulnerabilidades mediante la consolidación de las funciones y los datos de seguridad básicos. El sistema puede crear un gráfico completo de toda la red, lo que genera una imagen completa de la superficie de ataque en una única interfaz. Esta vista consolidada elimina los puntos ciegos creados por las herramientas aisladas y permite a los equipos de seguridad identificar eficazmente todos los puntos de entrada y puntos débiles potenciales.

Con los puntos de entrada identificados, el modelado de rutas de ataque revela cómo un atacante podría encadenar las vulnerabilidades para acceder a activos críticos. Esto permite a las organizaciones priorizar la remediación en función del riesgo, lo que maximiza el impacto de las inversiones en seguridad. La inteligencia sobre amenazas proporciona contexto adicional sobre ataques activos y tácticas, técnicas y procedimientos (TTP) de los atacantes.

Pensar como un atacante pone de manifiesto la necesidad de una estrategia de detección y respuesta proactiva. **Una plataforma unificada integra herramientas esenciales, como SIEM, XDR y gestión de la exposición, para ayudar a los equipos de seguridad a detectar patrones en actividades sospechosas y descubrir posibles incidentes.** Este enfoque permite una detección de amenazas más rápida y una respuesta más eficiente a la vez que optimiza la administración, mejora la correlación y automatiza los flujos de trabajo.

Ventajas de la gestión unificada de la exposición

Mitigación de riesgos según la prioridad: Centra los esfuerzos de remediación en las vulnerabilidades más críticas.

Superficie de ataque reducida: Minimiza los puntos de entrada mediante configuraciones de seguridad coherentes.

Identificación proactiva de brechas: Identifica y aborda los puntos débiles de seguridad antes de que sean explotados.

Resiliencia mejorada: Adáptate a las amenazas en evolución con inteligencia en tiempo real y respuestas automatizadas.

Detectar: coordina la defensa e interrumpe los ataques en curso

Aunque contar con un entorno con una exposición prácticamente nula nos permitiría dormir mucho más tranquilos, esa no es la realidad. Y tenemos que estar preparados para que los atacantes intenten vulnerar continuamente nuestras defensas. **Además de una buena prevención, esto requiere modelos de detección avanzados que siempre se mantengan actualizados y se adapten a los atacantes a medida que evolucionan.**

A diferencia de las soluciones tradicionales que analizan periódicamente el malware conocido y se basan únicamente en las señales de los puntos de conexión, la interrupción de los ataques utiliza la IA y las señales entre dominios para prever el siguiente movimiento de un atacante y adaptar su respuesta. Esto significa que podemos bloquear el movimiento lateral en las primeras etapas de la cadena de ataque e impedir el avance del atacante. La interrupción detiene los ataques de ransomware en solo tres minutos de media.

Piensa en la interrupción de ataques como una serie de cuadernos de estrategias adaptables que se integran y se actualizan constantemente con la inteligencia sobre amenazas más avanzada y eficaz. Este proceso autónomo garantiza una respuesta en tiempo real a un ataque, independientemente de lo ocupado que esté el equipo de seguridad.

Principales ventajas de la interrupción de ataques

Respuesta rápida al ransomware:
Neutraliza los ataques de ransomware en solo tres minutos de media.

Aislamiento de amenazas en tiempo real:
Aísla inmediatamente las entidades vulneradas para frenar la intrusión.

Inteligencia de amenazas predictiva:
Utiliza la IA para prever los movimientos de los atacantes y adaptar proactivamente las defensas.

Visibilidad entre dominios:
Aprovecha las señales de todo tu entorno para una detección completa de las amenazas.

Defensa autónoma:
Automatiza las acciones de respuesta para garantizar una mitigación de amenazas coherente e inmediata.

Adaptación continua:
Actualiza dinámicamente las defensas con la última inteligencia sobre amenazas.

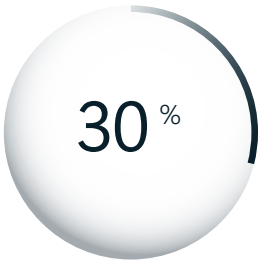
Investigar y responder: remedia rápidamente las amenazas con IA generativa

Los analistas están saturados de alertas y tareas de clasificación, lo que aumenta el riesgo de que una alerta crítica y urgente, al quedar rezagada en la cola, termine provocando un ataque catastrófico. Es muy probable que estén investigando una alerta rutinaria mientras pasan por alto incidentes graves en curso, que no se detectan correctamente porque están compuestos por múltiples alertas de bajo nivel. **Una plataforma unificada basada en IA generativa mejora la capacidad de respuesta del SOC al proporcionar una única cola de incidentes priorizada que correlaciona automáticamente las alertas, enriquece los incidentes con inteligencia de amenazas relacionada y establece prioridades en función de la gravedad.** Además, la experiencia unificada reduce el cambio de contexto y ofrece investigaciones más ágiles, enriquecidas con información sobre amenazas con guías paso a paso y automatización.

IA y automatización: impulsar la seguridad proactiva

Los asistentes de IA como Microsoft Security Copilot mejoran las plataformas unificadas al proporcionar conocimientos valiosos, automatizar tareas rutinarias y correlacionar alertas en incidentes completos. Esto permite a los analistas de seguridad centrarse en la toma de decisiones estratégicas.

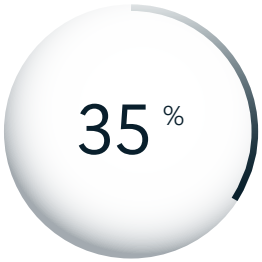
La IA y la automatización también ayudan a adaptarse al cambiante panorama de amenazas, lo que permite ofrecer respuestas eficaces a las nuevas tácticas de los atacantes. Por ejemplo, la visualización de posibles rutas de ataque durante una investigación puede revelar cómo los atacantes podrían atacar activos críticos, información que no está disponible con los enfoques tradicionales aislados.



resolución de incidentes más rápida[3]

Con Security Copilot, los analistas de seguridad ahorran un tiempo considerable con una **reducción del 30 % en el tiempo medio de resolución de incidentes (MTTR)**, recuperando 2,7 horas diarias que anteriormente se dedicaban a resolver incidentes.

[3] «Generative AI and Security Operations Center Productivity: Evidence from Live Operations», Microsoft, noviembre de 2024



decisiones más precisas[4]

Los estudios controlados muestran **resultados un 35 % más precisos** en las operaciones de seguridad, incluida la investigación de amenazas y la administración de políticas de dispositivos.

[4] «Randomized Controlled Trials for Security Copilot for IT Administrators», Microsoft, noviembre de 2024

ROI potencial[5]

Forrester prevé que las organizaciones pueden lograr hasta **1,76 millones de dólares en valor neto actual (NPV) con un ROI del 348 %** durante tres años, basado en un análisis de escenarios de alto impacto.

[5] «New Technology: The Projected Total Economic Impact™ Of Microsoft Security Copilot», Forrester, noviembre de 2024

Abordar tus dominios de seguridad más críticos

Un enfoque de seguridad verdaderamente eficaz requiere un enfoque unificado en todas las áreas de tu entorno. Las soluciones aisladas crean brechas que los atacantes aprovecharán. **A continuación, analizamos cinco dominios de seguridad comunes que demuestran cómo una plataforma unificada fortalece las defensas en cada área. Estos escenarios te ayudarán a identificar los puntos de partida más impactantes para tu organización.**

- Escenario 1: Proteger los puntos de conexión
- Escenario 2: Proteger las identidades
- Escenario 3: Proteger las aplicaciones nativas del cloud
- Escenario 4: Proteger toda la organización con SIEM y XDR
- Escenario 5: Proteger tus datos

Escenario 1: Proteger los puntos de conexión

Al conectar la seguridad de los puntos de conexión con otras defensas, las organizaciones pueden crear un enfoque unificado para protegerse contra las vulnerabilidades de ransomware, malware y dispositivos no administrados.

LEYENDA

- **Acción del atacante:** acciones realizadas por el atacante a lo largo de posibles rutas de ataque.
- **Acción de la plataforma:** cómo responde la plataforma a acciones específicas del atacante.
- **Resultado:** el resultado de la respuesta de la plataforma.

Defensa unificada de puntos de conexión: interrupción del ransomware

Este diagrama muestra cómo una plataforma de seguridad unificada puede interrumpir ataques de ransomware en varios puntos. Ilustra posibles rutas de ataque y la respuesta de la plataforma a acciones específicas del atacante.

Consideraciones clave para la protección de los puntos de conexión

Explora las tendencias críticas que conforman la seguridad de los puntos de conexión y las estrategias para contrarrestar el ransomware y las amenazas de malware.

El auge del ransomware

#1 El ransomware se sitúa como la principal amenaza externa entre los responsables de la toma de decisiones de TI de nivel sénior cuyo papel principal es la gestión de la seguridad[6].

[6] «La era de las plataformas de seguridad unificadas ya está aquí», Microsoft, 2024

Solución: **Microsoft Defender para punto de conexión** detecta y contiene el ransomware en el nivel del dispositivo, lo que detiene los intentos de movimiento lateral y cifrado. Como parte de **Microsoft Defender XDR**, se integra con **Security Copilot** para interrumpir los ataques en tres minutos, proporcionando análisis instantáneos y remediación guiada. Esta coordinación garantiza que la protección de puntos de conexión se alinee con las defensas más amplias entre dominios.

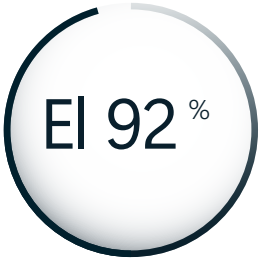
Malware generalizado

775 millones correos electrónicos con malware detectados el año pasado, lo que pone de relieve la amenaza continua de malware[7].

[7] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Solución: las defensas multicapa analizan las amenazas en el correo electrónico, la web y los puntos de conexión antes de que lleguen a los dispositivos. **Defender para punto de conexión** bloquea el contenido malintencionado, mientras que **Security Copilot** identifica patrones y automatiza las respuestas para reforzar las defensas contra las amenazas de malware en continuo cambio.

Dispositivos no administrados como puntos de entrada



de los ataques de cifrado remoto realizados con éxito explotan las vulnerabilidades en dispositivos no administrados[8].

[8] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Solución: la aplicación automatizada de políticas y la supervisión continua protegen los dispositivos no administrados sin necesidad de implementar agentes. **Defender para punto de conexión** detecta las amenazas de forma temprana, mientras que **Security Copilot** analiza el contexto y guía la remediación para evitar el movimiento lateral y contener los riesgos en el entorno.

Responde a la velocidad de la máquina frente al ransomware y el malware con **Defender para punto de conexión**, una funcionalidad clave en la solución **Defender XDR**.

Escenario 2: Proteger las identidades

Al unificar las señales de identidad, las organizaciones pueden detectar intentos de phishing, bloquear el robo de credenciales y evitar el movimiento lateral, garantizando una protección robusta contra el secuestro de cuentas y las amenazas internas.

LEYENDA

- **Acción del atacante:** acciones realizadas por el atacante a lo largo de posibles rutas de ataque.
- **Acción de la plataforma:** cómo responde la plataforma a acciones específicas del atacante.
- **Resultado:** el resultado de la respuesta de la plataforma.

Defensa de las identidades unificada: interrupción del phishing y el secuestro de cuentas

Este diagrama muestra cómo una plataforma de seguridad unificada puede interrumpir el phishing que deriva en el secuestro de cuentas en distintos puntos. Ilustra posibles rutas de ataque y la respuesta de la plataforma a acciones específicas del atacante.

Consideraciones clave para la protección de identidades

Conoce las amenazas emergentes basadas en la identidad y descubre cómo las defensas unificadas pueden prevenir el secuestro de cuentas.

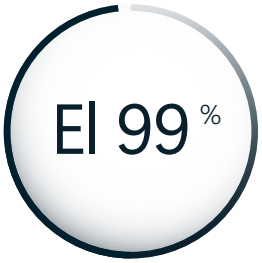
Ataques de phishing

#5 Los ataques de phishing se sitúan como la quinta amenaza externa más importante entre los responsables de la toma de decisiones de TI de nivel sénior cuya función principal es la gestión de la seguridad[9].

[9] «La era de las plataformas de seguridad unificadas ya está aquí», Microsoft, 2024

Solución: la solución **Identity Threat Detection and Response (ITDR) de Microsoft** analiza las señales de identidad en todo el entorno para detectar las credenciales robadas en tiempo real. Al correlacionar señales y automatizar las respuestas, ITDR unifica la protección de la identidad para detener las amenazas rápidamente. **Security Copilot** refuerza aún más ITDR al contener los incidentes de robo de credenciales y minimizar los daños con información.

Prevalencia de ataques basados en contraseña

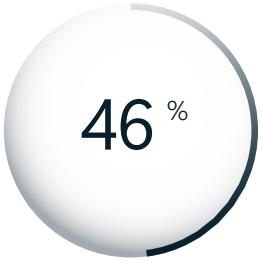


de los ataques de identidad se basan en contraseñas[10].

[10] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Solución: **Protección de Microsoft Entra ID**, parte de la solución **ITDR** de Microsoft, defiende contra las amenazas basadas en credenciales habilitando MFA y opciones sin contraseña en todo el entorno. **Security Copilot** mejora esta situación al supervisar las tasas de adopción y proporcionar recomendaciones para optimizar las defensas, garantizando una mejora continua contra los ataques basados en contraseñas.

Aumento de los ataques de phishing AiTM



aumento en los ataques de phishing AiTM[11].

[11] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Solución: al analizar los patrones de autenticación y las señales de identidad en todos los sistemas de identidad, tanto en el cloud como on-premises,**ITDR** puede detectar intentos de phishing AiTM avanzados. **Security Copilot** ayuda a investigar estas amenazas avanzadas y guía a los equipos a través de pasos de respuesta rápidos para proteger las credenciales de los usuarios.

Unifica tus señales de identidad e interrumpe los intentos de phishing con **Identity Threat Detection and Response (ITDR)**, que integra funcionalidades como **Protección de Entra ID** para una protección integral contra el secuestro de cuentas.

Escenario 3: Proteger las aplicaciones nativas del cloud

La seguridad unificada en el cloud detecta vulnerabilidades, bloquea la ampliación de privilegios y detiene el movimiento lateral, lo que permite a las organizaciones mitigar los riesgos, contener los ataques y proteger eficazmente los recursos críticos en el cloud.

LEYENDA

- **Acción del atacante:** acciones realizadas por el atacante a lo largo de posibles rutas de ataque.
- **Acción de la plataforma:** cómo responde la plataforma a acciones específicas del atacante.
- **Resultado:** el resultado de la respuesta de la plataforma.

Seguridad unificada en el cloud: interrupción de los ataques a la infraestructura en el cloud

Este diagrama muestra cómo una plataforma de seguridad unificada puede interrumpir los ataques a la infraestructura en el cloud en varios puntos. Ilustra posibles rutas de ataque y la respuesta de la plataforma a acciones específicas del atacante.

Consideraciones clave para proteger las aplicaciones nativas del cloud

Obtén información sobre las vulnerabilidades del cloud y las prácticas recomendadas para proteger los entornos de aplicaciones modernos.

Ataques al cloud

#2

Los ataques al cloud se sitúan como la segunda amenaza externa más importante entre los responsables de la toma de decisiones de TI de nivel sénior cuya función principal es la gestión de la seguridad[12].

[12] «La era de las plataformas de seguridad unificadas ya está aquí», Microsoft, 2024

Solución: Microsoft Defender for Cloud unifica la protección en todo el ciclo de vida de las aplicaciones, desde el código hasta el entorno de tiempo de ejecución, en todos los entornos del cloud. **Security Copilot** analiza continuamente las configuraciones y automatiza los controles de seguridad para evitar los intentos de acceso.

Vulnerabilidades del cloud

de las organizaciones tenían una ruta de ataque identificada en el cloud[13].

[13] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Solución: **Defender for Cloud** crea una vista unificada de las rutas de ataque en todo el entorno de cloud. **Security Copilot** prioriza las exposiciones críticas y coordina una rápida remediación en los sistemas afectados.

Riesgo de ataques cíclicos

300.000 servidores de aplicaciones en todo el mundo corren el riesgo de sufrir nuevos «ataques cíclicos»[14].

[14] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Solución: **Defender for Cloud** unifica la protección de los servidores en distintos entornos para bloquear las amenazas emergentes como los ataques cíclicos. **Security Copilot** aprende de los patrones de ataque para reforzar automáticamente las defensas en toda la flota de servidores.

Mitiga los riesgos del cloud y protege tus aplicaciones desde el código hasta el entorno en tiempo de ejecución con la protección unificada de **Defender for Cloud**.

Escenario 4: Proteger toda la organización con SIEM y XDR

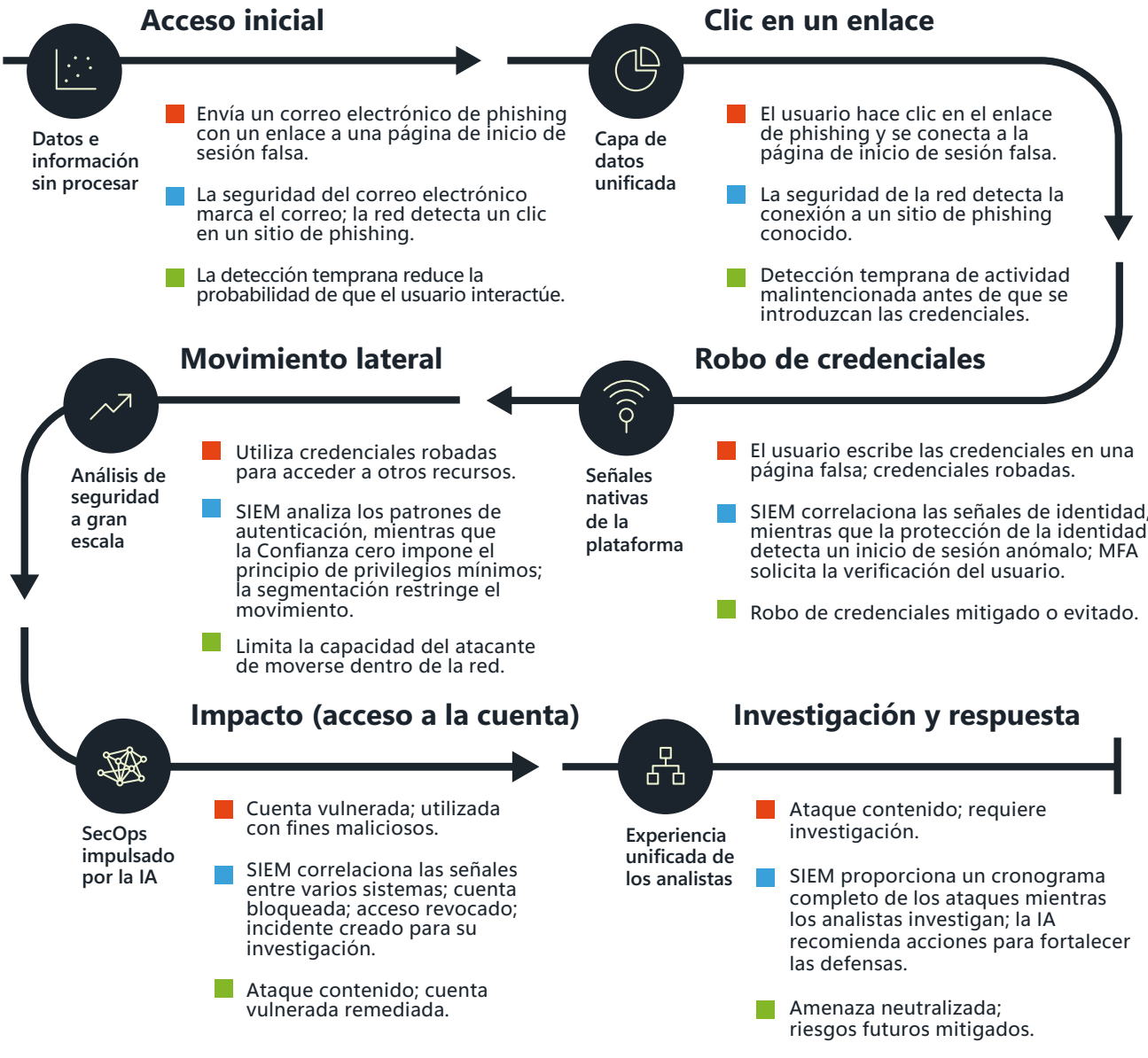
Al combinar SIEM y XDR en una sola plataforma, los equipos de seguridad obtienen protección nativa de nivel de plataforma de su XDR con la capacidad de correlacionar alertas de sus herramientas existentes e investigar y responder fácilmente a un incidente.

Seguridad unificada nativa del cloud: interrupción de los ataques de phishing AiTM

Este diagrama muestra cómo una plataforma de seguridad unificada puede interrumpir los ataques AiTM (adversary-in-the-middle) con una defensa por capas. Ilustra posibles rutas de ataque y la respuesta de la plataforma a acciones específicas de los atacantes.

LEYENDA

- **Acción del atacante:** acciones realizadas por el atacante a lo largo de posibles rutas de ataque.
- **Acción de la plataforma:** cómo responde la plataforma a acciones específicas del atacante.
- **Resultado:** el resultado de la respuesta de la plataforma.



Consideraciones clave para la integración de SIEM + XDR

Descubre cómo las herramientas integradas pueden ayudar a abordar las amenazas avanzadas persistentes y reducir los falsos positivos.

Amenazas persistentes avanzadas (APT)

#3 Las APT se sitúan como la tercera amenaza externa más importante entre los responsables de la toma de decisiones de TI de nivel sénior cuya función principal es la gestión de la seguridad[15].

[15] «La era de las plataformas de seguridad unificadas ya está aquí», Microsoft, 2024

Solución: **Microsoft Sentinel** unifica las señales de seguridad de los distintos clouds y plataformas para exponer patrones de APT ocultos. **Security Copilot** cartografía estas complejas cadenas de ataque y automatiza las acciones de respuesta en todo el entorno.

Falsos positivos

de los incidentes investigados por los equipos de SOC terminan sin plantear ninguna amenaza[16].

[16] «Global Security Operations Center Study Results», IBM, marzo de 2023

Solución: Sentinel y Defender XDR reducen drásticamente el número de falsos positivos en las colas de alertas con detecciones de XDR «out-of-box».

Expansión de la superficie de ataque

incremento interanual de los activos cibernéticos[17].

[17] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Solución: Sentinel proporciona recomendaciones personalizadas para ayudar a los ingenieros de seguridad a mejorar la cobertura y administrar los costes. Los clientes que han implementado recomendaciones han aumentado su cobertura de seguridad hasta en un 17 % y han podido aumentar el uso de los datos en un 31 %.

Protege tu organización con la eficacia combinada de Sentinel y Defender XDR, componentes clave de la plataforma de seguridad unificada de Microsoft

Escenario 5: Proteger tus datos

La protección de datos unificada detecta las amenazas internas, bloquea el acceso no autorizado y evita la filtración, lo que permite una investigación, remediación y protecciones más rápidas contra futuros ataques en toda la organización.

LEYENDA

- **Acción del atacante:** acciones realizadas por el atacante a lo largo de posibles rutas de ataque.
- **Acción de la plataforma:** cómo responde la plataforma a acciones específicas del atacante.
- **Resultado:** el resultado de la respuesta de la plataforma.

Protección de datos unificada: interrupción de la filtración de datos desde el interior

Este diagrama muestra cómo una plataforma de seguridad unificada puede interrumpir la filtración de datos desde el interior en varios puntos. Ilustra posibles rutas de ataque y la respuesta de la plataforma a acciones específicas del atacante.

Consideraciones clave para proteger tus datos

Examina los principales desafíos para proteger los datos confidenciales y mitigar eficazmente los riesgos internos.

Amenazas internas

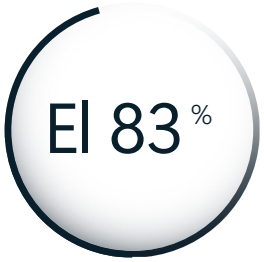
#6

Las amenazas internas se sitúan como la sexta preocupación de seguridad más importante entre los responsables de la toma de decisiones de TI de nivel sénior cuya función principal es la gestión de la seguridad[18].

[18] «La era de las plataformas de seguridad unificadas ya está aquí», Microsoft, 2024

Solución: **Microsoft Purview** unifica las políticas y controles de protección de datos en toda la organización para exponer los riesgos internos. **Security Copilot** identifica patrones de acceso a datos sospechosos y automatiza las medidas de protección en todos los entornos.

Filtraciones de datos repetidas



de las organizaciones se enfrentan a filtraciones repetidas[19].

[19] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Solución: **Purview** crea una protección de datos coherente en todo tu patrimonio digital a través de controles y políticas unificados. **Security Copilot** supervisa continuamente las brechas y automatiza las mejoras para evitar filtraciones recurrentes.

Exposición de credenciales

1,5 millones credenciales expuestas en los repositorios entre enero y junio de 2024[20].

[20] «Informe de defensa digital de Microsoft 2024», Microsoft, 2024

Solución: **Defender XDR** unifica la supervisión de credenciales en todos los sistemas de identidades, revelando riesgos de exposición que las herramientas aisladas no logran identificar. **Security Copilot** automatiza la detección y la respuesta para proteger las credenciales en todo el entorno.

Detecta amenazas internas, evita la filtración de datos y refuerza las protecciones con las políticas y controles de protección de datos unificados de **Purview** y la supervisión avanzada de credenciales de **Defender XDR**.

Conclusión

El futuro de las operaciones de seguridad exige un cambio fundamental de una defensa reactiva a una proactiva. Una arquitectura de SOC unificada hace que esto sea posible:

- Eliminando las barreras entre las funciones de seguridad
- Permitiendo la automatización basada en IA en todo el entorno
- Creando un bucle continuo de protección y mejora

La plataforma de seguridad integrada de Microsoft ofrece esta transformación a través de:

- Detección de amenazas en tiempo real y respuesta automatizada
- Visibilidad unificada de todo tu patrimonio digital
- Investigación y remediación mejoradas por la IA
- Gestión de la exposición y optimización de la seguridad continuas

El resultado

Una operación de seguridad más rápida, más inteligente y más resiliente, lista para proteger tu organización de las amenazas sofisticadas de hoy en día y de los desafíos emergentes del mañana.

Impulsa la seguridad de tu organización con la plataforma de seguridad unificada de Microsoft

Refuerza tu postura de seguridad con una arquitectura de SOC unificada

Defender XDR
Protección de puntos de conexión y supervisión de credenciales

Defender para punto de conexión
Detección de puntos de conexión multiplataforma, respuesta e interrupción del ransomware

Sentinel
SIEM y seguridad en toda la organización

Protección de Entra ID
Administración de identidad y acceso

Defender for Cloud
Seguridad de las aplicaciones nativas del cloud

Purview
Protección y gobierno de los datos

Security Copilot
Análisis y automatización basados en IA en todos los escenarios

Para conocer más detalles sobre los datos incluidos en estas infografías, así como sobre la evolución del panorama de amenazas, el rol central de la seguridad en las organizaciones y las primeras señales del impacto de la IA en la ciberseguridad, consulta el **Informe de defensa digital de Microsoft 2024**.