Microsoft Security

De la fatiga de alerta a la defensa proactiva

Lo que la IA generativa puede hacer por su SOC

Contenido

Introducción

Cómo transformar su SOC con IA generativa

Hoy en día, los Centros de Operaciones de Seguridad (SOC) operan en un panorama de amenazas cada vez más desafiante. La magnitud y sofisticación de las ciberamenazas sigue creciendo rápidamente, mientras que se espera que los equipos de seguridad sean más eficaces que nunca. Los analistas enfrentan una cantidad récord de falsos positivos que saturan sus colas de alertas, una amplia variedad de herramientas y una presión constante para proteger a sus organizaciones de ataques cada vez más complejos.

Los números cuentan la historia

Aumento de las estafas tecnológicas

12 veces han aumentado los incidentes diarios, ya que los atacantes aprovechan la superficie de ataque en expansión.[1]

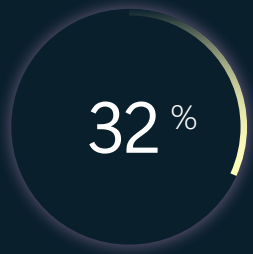
Complejidad de las herramientas

14 herramientas de seguridad diferentes utiliza un SOC promedio, lo que crea complejidad en lugar de claridad.[3]

Escasez de talento

de las organizaciones informan de carencias de habilidades, lo que dificulta mantenerse al día con las amenazas en evolución.[2]

Flujos de trabajo ineficientes



del día de un SOC se dedica a abordar incidentes que, en última instancia, no representan una amenaza.[4]

Para muchos equipos del SOC, esta realidad lleva a fatiga, amenazas sin detectar y corrección tardía, lo que permite que los actores de amenaza tengan un acceso prolongado y deja a las organizaciones cada vez más vulnerables a los ataques.

Pero hay esperanza. En medio de estos crecientes desafíos, la IA generativa ofrece capacidades transformadoras, que ayudan a los equipos del SOC a cerrar vacíos críticos y abordar la magnitud y complejidad de las amenazas sofisticadas actuales. Microsoft Security Copilot, con tecnología de IA generativa, ejemplifica la forma en que estos avances pueden empoderar a los analistas con respuestas guiadas, investigaciones simplificadas y búsqueda proactiva de amenazas, todo ello integrado a la perfección en los flujos de trabajo de seguridad existentes.

[1] "Informe de defensa digital de Microsoft 2024", página 37, Microsoft, 2024
[2] "ISC2 Cybersecurity Workforce Study: How the Economy, Skills Gap, and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce 2023", página 20, ISC2, 2023
[3] "La era de las plataformas de seguridad unificada ya está aquí", página 7, Microsoft, 2024.
[4] "Global Security Operations Center Study Results", página 6, IBM, marzo de 2023

La IA generativa puede mejorar cada etapa del flujo de trabajo de SecOps

La IA generativa está ayudando a los equipos del SOC a operacionalizar y contextualizar sus datos de seguridad e inteligencia sobre amenazas de formas que antes no eran posibles:

Respuesta guiada
Ofrezca recomendaciones paso a paso y adaptadas para la contención y corrección basadas en la composición del entorno y la configuración de los activos afectados, lo que permite a los analistas actuar con rapidez y confianza.

Búsqueda proactiva de amenazas
Guíe a los analistas a través de procesos clave y creación de consultas. Descubra las amenazas ocultas antes de que se intensifiquen, acelerando la búsqueda.

Investigaciones optimizadas
Enriquezca automáticamente las alertas, correlacione los datos relacionados y resuma la actividad del atacante, lo que elimina horas de trabajo de investigación manual y empodera a los analistas para que se centren en las tareas más críticas, como mitigar la amenaza y restablecer en línea los activos afectados.

Informes simplificados
Transforme los datos de seguridad complejos en conclusiones accionables y claras, adaptadas tanto a los equipos técnicos como a los líderes empresariales.

Los asistentes con tecnología de IA generativa tienen el potencial de transformar los SOC abordando desafíos críticos, como la magnitud, la complejidad y las ineficiencias operativas. Security Copilot de Microsoft ejemplifica este potencial integrándose a la perfección con Microsoft Defender para ofrecer respuestas guiadas, investigaciones simplificadas, búsqueda proactiva de amenazas e informes simplificados, todo ello a la vez que aprovecha la inteligencia global sobre amenazas. Mediante la inserción de la IA generativa en los flujos de trabajo existentes, las organizaciones pueden empoderar a sus analistas para que actúen más rápido, de manera más inteligente y con mayor confianza.

En los siguientes capítulos, exploraremos cómo la IA generativa puede revolucionar su SOC, ayudando a su equipo a pasar de sentirse abrumado a empoderado. Comencemos.

Capítulo 1

Investigación y respuesta de IA: de la sobrecarga de datos a las conclusiones accionables

La IA generativa acelera la respuesta ante incidentes reduciendo la sobrecarga de alertas y permitiendo una clasificación y acción más rápidas.

La realidad actual del SOC: un desafío para mantenerse al día

Incluso los equipos del SOC con herramientas avanzadas que agrupan las alertas relacionadas en incidentes siguen dedicando un tiempo valioso a orientarse, comprender lo que sucedió y decidir los próximos pasos. Los analistas se enfrentan a interminables colas de alertas y procesos manuales, lo que dificulta responder eficazmente y, a menudo, provoca que no se detecten amenazas. Los incidentes doblemente críticos pueden pasar desapercibidos durante los momentos clave debido al gran volumen de alertas y al tiempo que se requiere para comprender su contexto, determinar las acciones necesarias y realizar seguimientos completos.

Esto lleva a retrasos en la contención y corrección, lo que deja a las organizaciones expuestas a las amenazas en desarrollo.

Resoluciones más rápidas, equipos más inteligentes

Security Copilot permite a los equipos del SOC iniciar investigaciones con resúmenes completos y acciones priorizadas. Como asistente con tecnología de IA generativa, reduce el ruido y proporciona conclusiones accionables, lo que ayuda a los analistas a responder con confianza. **Las organizaciones que usan Security Copilot informan una reducción del 30 %[5] en el tiempo medio de resolución (MTTR)**, lo que permite una contención de amenazas más rápida. Además, **Copilot reduce la cantidad de alertas por incidente en un 23 %[6]**, lo que permite a los analistas resolver las amenazas antes en la cadena de ataque a la vez que alivia las cargas de trabajo.

[5] "IA generativa y productividad del Centro de operaciones de seguridad: pruebas de operaciones en vivo", página 2, Microsoft, noviembre de 2024

[6] "IA generativa, operaciones de seguridad, prevención de pérdida de datos y administración de directivas de dispositivos: una historia de productividad", página 4, Microsoft, marzo de 2025

IA en acción

Guiar a los analistas a tomar decisiones rápidas y seguras

Considere a un analista del SOC que recibe una alerta sobre actividad de inicio de sesión inusual desde múltiples ubicaciones geográficas dirigida a una cuenta de usuario de alto privilegio. Gracias a la mejora del flujo de trabajo con la IA generativa, el analista puede hacer lo siguiente:

Optimizar la clasificación de alertas
La IA generativa consolida varias alertas relacionadas, identifica un ataque coordinado en cuentas privilegiadas y prioriza el incidente según su gravedad, lo que ayuda al analista a centrarse en la amenaza más crítica, en lugar de eliminar falsos positivos o vincular la actividad del atacante.

Recibir resúmenes prácticos
En lugar de examinar cuidadosamente los datos sin procesar, el analista obtiene un resumen conciso: "El incidente comenzó con múltiples intentos fallidos de inicio de sesión en el dispositivo 'vnevado-linux' (Linux) por parte del usuario 'root' desde la IP 172.16.0.4. El proceso sshd (PID: 20640) se estaba ejecutando con privilegios de root, lo que indica un intento de inicio de sesión fallido".

Tomar medidas precisas
Basándose en el incidente específico, la IA generativa recomienda los siguientes pasos personalizados, como aislar las cuentas afectadas, restablecer contraseñas, bloquear IP malintencionadas y supervisar posibles anomalías adicionales.

Crear confianza
La IA generativa proporciona orientación paso a paso para garantizar que las tareas se ejecuten con precisión, lo que ayuda a los analistas junior a crecer y permite a los analistas sénior centrarse en iniciativas de mayor prioridad.

Con el apoyo de la IA generativa, el analista resuelve el incidente rápidamente, lo que evita la filtración de datos y garantiza el cumplimiento de las políticas internas. Esto permite una respuesta ante incidentes más rápida y segura, lo que fortalece la capacidad del SOC para contener amenazas y proteger a la organización.

Capítulo 2

Análisis con tecnología de IA: desde scripts codificados hasta un resumen claro

La IA generativa simplifica las investigaciones, convirtiendo los análisis complejos en información clara que ayuda a los analistas a actuar con decisión.

La realidad actual del SOC: intervención limitada y tiempo perdido

Las investigaciones en los SOC suelen ser reactivas, impulsadas por alertas o actividades que involucran indicadores de compromiso (IoC) conocidos. Los analistas y buscadores de amenazas pasan horas analizando manualmente vastos conjuntos de datos, creando consultas y correlacionando la inteligencia sobre amenazas. Estos son esfuerzos que exigen experiencia especializada. Decodificar scripts potencialmente ofuscados es un desafío importante, que requiere habilidades técnicas de las que carecen muchos analistas. Esto obliga a los equipos a depender de colegas o recursos externos para obtener ayuda, lo que ralentiza las investigaciones y deja las amenazas críticas sin detectar hasta que se producen daños.

Investigaciones más inteligentes, analistas seguros

Security Copilot acelera las investigaciones automatizando tareas complejas y correlacionando la inteligencia sobre amenazas, lo que ayuda a los analistas a descubrir información crítica más rápido. Simplifica los flujos de trabajo, como la decodificación de scripts malintencionados, lo que reduce los tiempos de investigación de horas a segundos. **Las organizaciones que usan Copilot vieron una disminución del 18 %[7] en el tiempo para clasificar las alertas de DLP**, lo que permitió a los analistas actuar con decisión. Además, **el 97 % de los usuarios dicen que volverían a usar Copilot[8]**, mencionando la mejora en la productividad y la reducción del esfuerzo.

[7] "IA generativa, operaciones de seguridad, prevención de pérdida de datos y administración de directivas de dispositivos: una historia de productividad", página 6, Microsoft, marzo de 2025
[8] "Ensayo aleatorizado controlado para Security Copilot", página 8, Microsoft, enero de 2024

IA en acción

Convertir scripts complejos en conocimientos claros

Considere a un analista del SOC que encuentra un script de PowerShell sospechoso marcado durante la supervisión de rutina. Con la IA mejorando su flujo de trabajo, el analista puede hacer lo siguiente:

Desofuscar scripts instantáneamente
La IA generativa decodifica el script, identifica su propósito y proporciona un resumen conciso: "Este script descarga y ejecuta una carga útil desde [dominio malicioso]".

Correlacionar con inteligencia sobre amenazas
La IA generativa vincula el script con alertas recientes y familias de malware conocidas, lo que ofrece un contexto valioso para la atribución y la mitigación.

Validar hallazgos rápidamente
La IA generativa proporciona una guía paso a paso, ayudando a los analistas a confirmar los resultados con precisión, lo que aumenta la confianza de los miembros más jóvenes del equipo.

Acelerar los flujos de trabajo
Mediante la automatización de las tareas tediosas, la IA generativa reduce el tiempo de investigación de horas a minutos, lo que permite a los analistas sénior centrarse en iniciativas estratégicas como la búsqueda de amenazas.

Con el apoyo de la IA generativa, el analista descubre información crítica rápidamente, validando los hallazgos con confianza y mitigando las amenazas antes de que se intensifiquen. Esto permite a los analistas descubrir rápidamente información crítica, validar hallazgos y mitigar amenazas, lo que mejora la eficacia general del SOC.

Capítulo 3

Búsqueda proactiva de amenazas: de la defensa reactiva a la predictiva

Gracias a sus capacidades predictivas, la IA generativa permite que los SOC anticipen y mitiguen las amenazas antes de que se intensifiquen.

La realidad actual del SOC: reactivo y con recursos limitados

Los SOC muchas veces tienen dificultades para adelantarse a los atacantes debido a flujos de trabajo reactivos y recursos limitados. Los analistas deben examinar vastos conjuntos de datos, correlacionar la inteligencia sobre amenazas y crear numerosas consultas personalizadas, a menudo, mediante ensayo y error, para descubrir conclusiones accionables. Este proceso que consume mucho tiempo exige experiencia especializada y un esfuerzo considerable, lo que deja a las organizaciones vulnerables a amenazas no detectadas y respuestas tardías.

Información más rápida, defensas más sólidas

Security Copilot permite a los equipos del SOC actuar antes de que las amenazas se intensifiquen mediante la correlación de vastos conjuntos de datos, la identificación de indicadores de alto riesgo y la identificación de rutas de ataque. En las pruebas, **Security Copilot mejoró la precisión de la guía de corrección en un 43 %**[9], lo que permitió a los analistas tomar medidas preventivas precisas para neutralizar las amenazas. Además, **Security Copilot reduce las reaperturas de incidentes en un 68 %**[10], lo que garantiza que los incidentes se resuelvan correctamente la primera vez y minimiza las amenazas no resueltas que podrían reaparecer más tarde.

[9] "Ensayo aleatorizado controlado para Security Copilot", página 9, Microsoft, enero de 2024

[10] "IA generativa, operaciones de seguridad, prevención de pérdida de datos y administración de directivas de dispositivos: una historia de productividad", página 5, Microsoft, marzo de 2025

IA en acción

Prever las amenazas antes de que se intensifiquen

Considere a un buscador de amenazas que busca proactivamente indicadores de compromiso (IoC) vinculados a un actor de amenaza conocido que se dirige a organizaciones de su industria. Gracias a la mejora del flujo de trabajo con la IA generativa, el buscador de amenazas puede hacer lo siguiente:

Crear teorías de búsqueda impactantes
La IA generativa ayuda a los analistas a consultar rápidamente las alertas de IoC emergentes o tácticas, técnicas y procedimientos (TTP) específicos de los atacantes dirigidos a su organización.

Formular preguntas orientadas
Al usar consultas en lenguaje natural como "¿Midnight Blizzard tiene como objetivo mi organización?", el buscador de amenazas recibe una respuesta instantánea con vínculos a alertas que indican un posible verdadero positivo. Cada alerta incluye explicaciones de por qué podría estar relacionada y conclusiones accionables.

Correlacionar patrones automáticamente
La IA generativa conecta puntos de datos a través de alertas, incidentes y vulnerabilidades, descubriendo relaciones ocultas que de otro modo podrían pasar desapercibidas.

Tomar medidas preventivas
La IA recomienda pasos de mitigación personalizados, como bloquear dominios malintencionados o aplicar parches a las vulnerabilidades, lo que permite a los equipos neutralizar las amenazas antes de que se intensifiquen.

Con el apoyo de la IA generativa, los analistas van más allá de los flujos de trabajo reactivos para descubrir y mitigar proactivamente las amenazas. Esto permite una defensa proactiva y predictiva, lo que fortalece la capacidad del SOC para prever y neutralizar las amenazas antes de que se intensifiquen.

Capítulo 4

Informes de seguridad simplificados: de la sobrecarga de datos a la comunicación clara

La IA generativa optimiza los informes de seguridad resumiendo automáticamente el incidente y las medidas correctivas adoptadas por el equipo, que se entregan en un informe listo para ser presentado a la junta directiva, lo que permite a las partes interesadas tomar decisiones más rápidas e informadas.

La realidad actual del SOC: Sobrecarga de informes

Ningún equipo del SOC quiere pasar horas o incluso días creando informes finales después de un incidente. El proceso suele ser largo, tedioso y manual. Los analistas deben recopilar y correlacionar datos de varias herramientas, incluidos registros, alertas e inteligencia sobre amenazas, para luego reescribirlos y reformatearlos para públicos técnicos y no técnicos.

Esta ineficiencia retrasa la comunicación, provoca la desalineación entre los equipos y deja a las organizaciones esforzándose por expresar claramente su posición de seguridad a las partes interesadas.

Informes más claros, mejores decisiones

Security Copilot transforma los informes automatizando la recopilación, organización y presentación de los datos de seguridad. Mediante la consolidación de la información entre herramientas y la generación de resúmenes listos para el público, **Security Copilot mejora la calidad y claridad de los informes en un 86 %,**[11] lo que ayuda a los equipos a tomar decisiones más rápidas. Más allá de los informes, **Security Copilot mejora los flujos de trabajo de TI con una reducción del 54 %**[12] **en el tiempo para resolver conflictos de directivas de dispositivos**, lo que ahorra tiempo a los analistas y garantiza que los dispositivos sigan siendo seguros y compatibles.

[11] "Ensayo aleatorizado controlado para Security Copilot", página 8, Microsoft, enero de 2024

[12] "IA generativa, operaciones de seguridad, prevención de pérdida de datos y administración de directivas de dispositivos: una historia de productividad", página 8, Microsoft, marzo de 2025

IA en acción

Informes de seguridad simplificados

Considere a un analista del SOC que resume un incidente reciente para públicos técnicos y ejecutivos. Gracias a la mejora del flujo de trabajo con la IA generativa, el analista puede hacer lo siguiente:

Consolidar al instante los datos
La IA generativa recopila y organiza información de múltiples fuentes, incluidos registros, alertas y comentarios de analistas en un informe unificado.

Captar detalles críticos
Los informes incluyen marcas de tiempo para acciones clave (por ejemplo, creación de incidentes, pasos de investigación, corrección), decisiones impulsadas por analistas y respuestas automatizadas, lo que garantiza que no se pase nada por alto.

Destacar conclusiones accionables
La IA generativa resume la historia del ataque, los activos afectados y los próximos pasos, y proporciona recomendaciones claras para las acciones de seguimiento o los problemas no resueltos.

Exportar y compartir sin esfuerzo
Con solo unos clics, los informes se pueden exportar a formatos como PDF, lo que facilita compartir los hallazgos con las partes interesadas o usarlos en las revisiones posteriores al incidente.

Con el apoyo de la IA generativa, los analistas crean informes concisos y listos para el público que permiten tomar decisiones de forma más rápida e informada. Esto transforma los informes de seguridad, lo que permite tomar decisiones más rápidas e informadas, y libera a los equipos del SOC para que se centren en mejoras de seguridad estratégicas.

Conclusión

El futuro de SecOps está aquí con la IA generativa

La IA generativa está revolucionando las operaciones de seguridad, permitiendo que los equipos del SOC trabajen de manera más inteligente, sin un mayor esfuerzo. Al abordar los desafíos más apremiantes de la actualidad, redefine la forma en que las organizaciones enfrentan la ciberseguridad. Desde la clasificación hasta la generación de informes, los asistentes con tecnología de IA generativa mejoran todos los aspectos del flujo de trabajo de SecOps, lo que permite tener respuestas más rápidas, defensas más sólidas y una toma de decisiones más segura.

A la vanguardia de esta transformación se encuentra Security Copilot, que unifica herramientas, operacionaliza la inteligencia sobre amenazas y guía a los analistas a través de flujos de trabajo complejos. Ya sea mediante la aceleración de la respuesta ante incidentes, la simplificación de las investigaciones o la habilitación de la búsqueda proactiva de amenazas, Security Copilot permite que los equipos del SOC se adapten con facilidad a las amenazas en desarrollo.

Aspectos claves

En esta guía, hemos explorado diferentes escenarios que resaltan el poder transformador de la IA en las operaciones de seguridad.

Respuesta guiada por IA
Convertir la sobrecarga de datos en conclusiones accionables para una clasificación y resolución más rápidas.

Investigaciones guiadas por IA
Simplificar análisis complejos, como decodificar scripts ofuscados o correlacionar la inteligencia sobre amenazas, lo que permite a los analistas descubrir información crítica rápidamente y actuar con confianza.

Búsqueda de amenazas proactiva
Transformar la búsqueda de amenazas con estrategias predictivas para descubrir riesgos y actuar antes de que las amenazas se intensifiquen.

Informes de seguridad simplificados
Optimizar la comunicación mediante la transformación de los datos sin procesar en información clara y lista para el público para las partes interesadas.

Estos ejemplos demuestran cómo la IA generativa no solo aborda las ineficiencias operativas, sino que también abre nuevas oportunidades para que los SOC se mantengan a la vanguardia de las amenazas en evolución a la vez que mejoran el rendimiento y la moral del equipo.

El panorama general

La IA generativa representa un cambio de paradigma en las operaciones de seguridad, puesto que unifica herramientas y aprovecha la inteligencia global de amenazas para ayudar a las organizaciones a adaptarse a las amenazas en desarrollo. Security Copilot crea resiliencia para los desafíos actuales y las incertidumbres del mañana, lo que permite a los equipos del SOC adelantarse a los atacantes, mitigar los riesgos de forma proactiva y escalar con volúmenes de datos crecientes.

Comience su transformación

La promesa de SecOps impulsado por IA no es solo una visión del futuro: ya está disponible. Con Security Copilot, su equipo puede pasar de sentirse abrumado a empoderado, abordando los desafíos de hoy con confianza y preparándose para las incertidumbres del mañana.

Para obtener más información sobre cómo la plataforma de SecOps unificada de Microsoft puede transformar su organización, visite nuestra página de Plataforma de operaciones de seguridad con tecnología de IA.

Su proceso de sentirse abrumado a empoderado comienza ahora.