WHITE PAPER

IA Generativa en Operaciones de Seguridad

Incorporación de Inteligencia Artificial en Herramientas y Flujos de Trabajo de Seguridad

Resumen ejecutivo

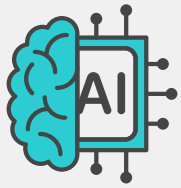
El panorama de ciberseguridad evoluciona rápidamente, caracterizado por amenazas cada vez más sofisticadas y un volumen creciente de ataques. Los equipos de operaciones de seguridad (SecOps) enfrentan una gran presión para identificar, investigar y responder de manera eficiente a estas amenazas. La IA generativa (GenAI) ofrece una oportunidad transformadora para que los equipos de SecOps mejoren la toma de decisiones, optimicen las operaciones y mejoren la postura de seguridad general de la organización. Al aprovechar GenAI como una herramienta complementaria dentro de una plataforma de ciberseguridad, las organizaciones pueden abordar desafíos clave como la fatiga de alertas, la escasez de personal y la necesidad de una respuesta rápida a las amenazas.

Desafíos persistentes en Ciberseguridad

Muchos desafíos de ciberseguridad persisten porque las organizaciones confían en herramientas y procesos obsoletos o mal integrados. Las medidas de seguridad tradicionales a menudo no pueden adaptarse a las tácticas sofisticadas que utilizan los atacantes. La ausencia de una plataforma de ciberseguridad o Security Fabric profundamente integrada crea brechas en la cobertura que los atacantes pueden aprovechar. Al utilizar tecnologías avanzadas como GenAI para mejorar sus capacidades, los equipos de SecOps pueden adoptar un enfoque más cohesionado y adaptable para superar estos desafíos.

La función de GenAI en SecOps

La IA generativa está revolucionando muchas industrias, incluida la ciberseguridad. En SecOps, aunque las herramientas como los sistemas de información de seguridad y administración de eventos (SIEM) manejan la recopilación y el análisis de grandes cantidades de datos para identificar patrones y anomalías, GenAI mejora significativamente este proceso. GenAI puede ayudar a los analistas a descifrar datos complejos, proporcionar mejores prácticas y ejecutar acciones. GenAI facilita un flujo de trabajo más intuitivo y eficiente, lo que permite a los analistas utilizar el lenguaje natural para interactuar con los sistemas, obtener rápidamente información relevante y recibir orientación sobre el mejor curso de acción. Debido a que la inteligencia artificial (IA) puede priorizar las alertas en función del impacto potencial, es crucial en entornos abrumados por los volúmenes de alertas. Puede ayudar con la asignación de recursos y mejorar la postura de seguridad general de una organización.



Para 2027, la IA generativa contribuirá a una reducción del 30% en las tasas de falsos positivos para las pruebas de seguridad de aplicaciones y la detección de amenazas.[1]

La utilización de la IA como arma está agregando combustible a un panorama de amenazas ya de por sí peligroso. La actividad de ransomware fue 13 veces mayor a finales del primer semestre de 2023 en comparación con principios de año, lo que intensifica la necesidad de defensas avanzadas impulsadas por IA.[2]

Implementación de GenAI en SecOps

La integración de GenAI en SecOps implica incorporar capacidades de IA en herramientas y flujos de trabajo de seguridad. Esta integración perfecta puede permitir a los analistas interactuar con la IA a través de sus interfaces estándar. La IA debe admitir múltiples fuentes, incluidas herramientas de administración y análisis centrales, sistemas SIEM, plataformas de inteligencia frente a amenazas y soluciones de respuesta y automatización de orquestación de seguridad (SOAR).

Para maximizar los beneficios de GenAI, las organizaciones deben capacitar soluciones de IA con datos relevantes y actualizarlos continuamente con nueva inteligencia frente a amenazas. Este proceso de aprendizaje continuo garantiza que la herramienta de IA pueda identificar y responder eficazmente a las amenazas emergentes. Es crucial establecer protocolos claros sobre cómo los analistas deben interactuar con la solución de IA y garantizar que comprendan sus capacidades y limitaciones. La integración de GenAI en una infraestructura de seguridad existente permite operaciones más cohesionadas y eficientes. Debido a que GenAI maneja tareas rutinarias y proporciona asistencia en tiempo real a los analistas, puede mejorar la eficiencia de SecOps de varias maneras.

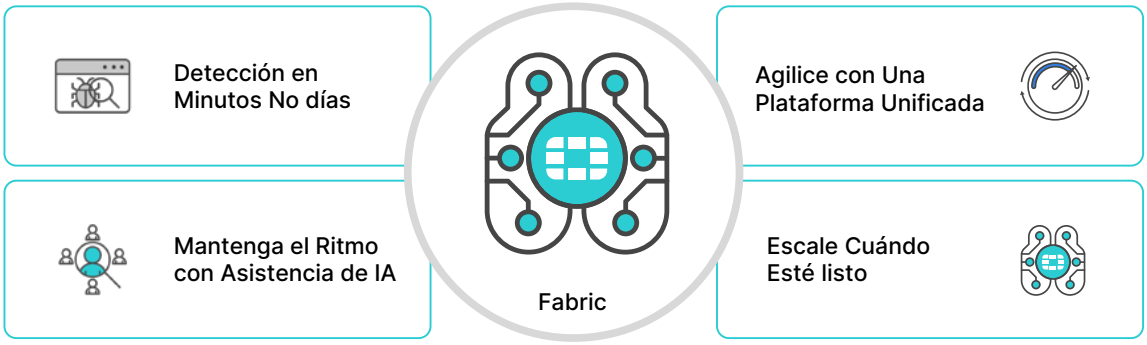


Figura 1: Unifique la respuesta a amenazas con la ayuda de la IA.

Aborde la escasez de personal y agilice las operaciones

La escasez de personal y el agotamiento son desafíos importantes en la industria de la ciberseguridad. Con profesionales calificados limitados disponibles y más trabajo por recorrer que los analistas, las organizaciones a menudo se esfuerzan por crear y mantener equipos de SecOps efectivos. GenAI ayuda a aumentar las capacidades del personal existente y reduce la dependencia de habilidades altamente especializadas. GenAI permite a los equipos de seguridad operar de manera más eficiente automatizando las tareas rutinarias y proporcionando información procesable. Los analistas pueden dedicar menos tiempo al análisis manual de datos y más a la toma de decisiones estratégicas y la respuesta a incidentes.

Simplificar los procesos a través de GenAI también permite a los analistas menos experimentados realizar tareas que anteriormente requerían experiencia de nivel sénior. Esta democratización de habilidades ayuda a cerrar la brecha creada por la escasez de personal y garantiza que el equipo de seguridad pueda mantener un alto nivel de rendimiento incluso con recursos limitados. GenAI alivia la carga de los altos volúmenes de alertas y las constantes presiones de respuesta a amenazas, lo que reduce el agotamiento del analista de seguridad.

Al automatizar las tareas repetitivas y proporcionar recomendaciones claras y procesables, GenAI permite a los analistas enfocarse en aspectos más atractivos y recompensadores de su trabajo, mejorando así la satisfacción laboral y la moral. La facilidad de interactuar con GenAI utilizando el lenguaje natural reduce la frustración y mejora la productividad, lo que permite a los analistas obtener rápidamente la información y la orientación necesarias sin navegar por interfaces complejas ni documentación extensa.

Simplificación y aceleración de investigaciones de amenazas complejas

GenAI desempeña un papel crucial en la simplificación y aceleración de investigaciones de amenazas complejas. Los procesos tradicionales de investigación de amenazas pueden requerir mucho tiempo y trabajo. A menudo, los analistas deben investigar y correlacionar manualmente los datos de múltiples fuentes y unir la secuencia de eventos. GenAI, con herramientas de administración y análisis de datos, automatiza gran parte de este trabajo al analizar rápidamente grandes conjuntos de datos, identificar patrones relevantes y proporcionar una narrativa coherente del incidente. Por ejemplo, GenAI puede ayudar a generar informes sobre los principales incidentes durante los últimos 30 días. Esta tarea normalmente requeriría muchos recursos si se realiza manualmente, pero esta capacidad de GenAI ahorra tiempo y garantiza que los analistas puedan acceder rápidamente a información crítica y enfocarse en tareas de alta prioridad. GenAI puede ayudar con estas tareas:

- **Analice las alertas:** Al examinar alertas y registros, GenAI puede generar resúmenes detallados de incidentes, destacando aspectos clave como vectores de ataque, sistemas afectados y posible impacto.
- **Correlacione los datos:** GenAI puede correlacionar información de varias fuentes, incluidos SIEM, inteligencia frente a amenazas y datos de endpoint, para proporcionar una visión integral del incidente.
- **Genere informes:** GenAI puede generar informes, como un resumen de los principales incidentes en los últimos 30 días, que de otro modo sería un proceso manual que agota los recursos.

- **Proporciona recomendaciones:** Según el análisis, GenAI puede sugerir acciones específicas para la contención, corrección e investigación adicional, ayudando a los analistas a tomar decisiones informadas rápidamente.

Estas capacidades aceleran el proceso de investigación, mejoran la precisión y ayudan a reducir la posibilidad de que se pasen por alto detalles críticos.

Reducción del tiempo promedio para detectar y responder

Una de las métricas más críticas en SecOps es el tiempo que lleva detectar y responder a las amenazas. Reducir el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR) es esencial para minimizar el impacto de los incidentes de seguridad. GenAI ayuda a reducir la MTTD y el MTTR al proporcionar análisis y recomendaciones en tiempo real que respaldan el proceso de investigación. Con GenAI, junto con las capacidades de detección de un equipo de seguridad, los analistas pueden identificar rápidamente posibles amenazas y comprender su contexto sin gastar recursos en investigaciones de falsos positivos. Una solución de IA puede analizar datos históricos, identificar patrones y predecir el impacto potencial de un incidente. Un enfoque proactivo puede resultar en una detección más rápida y una toma de decisiones más informada durante la fase de respuesta. Al automatizar partes de los procesos de investigación y respuesta, GenAI ayuda a reducir el tiempo requerido para remediar incidentes y, en última instancia, mejora la resiliencia de una organización contra las ciberamenazas.

Maximización de las inversiones existentes

La implementación de GenAI en SecOps también puede ayudar a las organizaciones a maximizar sus inversiones existentes en infraestructura de seguridad. Las organizaciones pueden mejorar sus capacidades al integrar GenAI con las herramientas y plataformas actuales sin requerir recursos extensos. GenAI puede trabajar con herramientas de administración centralizada y analítica existentes, sistemas SIEM, soluciones SOAR y plataformas de inteligencia frente a amenazas para proporcionar información más profunda y respuestas a amenazas más efectivas. La implementación de GenAI puede mejorar el retorno de la inversión de las herramientas existentes y ayudar a las organizaciones a aprovechar todo el potencial de su infraestructura de seguridad. GenAI puede ayudar a los equipos de SecOps a lograr mejores resultados mientras controlan los costos.

El futuro de las Operaciones de Seguridad

GenAI tiene una promesa significativa de transformar las operaciones de seguridad. Al mejorar la toma de decisiones, optimizar los flujos de trabajo y mejorar la productividad, GenAI aborda algunos de los desafíos más apremiantes que enfrentan los equipos de SecOps en la actualidad. A medida que las organizaciones continúan integrando la IA en sus operaciones de seguridad, pueden esperar ver mejoras en su capacidad para detectar, responder y mitigar amenazas, lo que finalmente conduce a un ciberentorno más seguro y resistente. El futuro de SecOps sin duda se verá forjado por los avances en la tecnología de IA, lo que impulsará medidas de seguridad más proactivas y eficientes. Al mantenerse a la vanguardia y adoptar GenAI, las organizaciones pueden seguir siendo sólidas y ágiles frente a las ciberamenazas en evolución.

[1] Jeremy D'Hoinne, Avivah Litan, Peter Firstbrook, Gartner Research, "4 Ways Generative AI Will Impact CISOs and Their Teams," ID G00793265, 29 de junio de 2023

[2] Fortinet, "Cyberthreat Predictions for 2024: An Annual Perspective from FortiGuard Labs," 7 de noviembre de 2023.

August 25, 2024 9:32 PM / 2757450-0-0-EN