Parte 4

Conoce a los defensores del mañana: agentes de IA que protegen tu perímetro digital

Los beneficios de los agentes de IA y los casos de uso para su implementación están creciendo en las empresas. Pero cuando se trata de ciberdefensa, las compañías aún están determinando cómo desplegar de manera efectiva agentes en sus Centros de Operaciones de Seguridad (SOC) para mejorar las capacidades de detección y respuesta ante amenazas.

En muchos entornos SOC, la ciberdefensa sigue siendo principalmente liderada por humanos, aunque la automatización determinista está aumentando en las plataformas de orquestación, automatización y respuesta de seguridad (SOAR). Los analistas tienen la tarea de procesar enormes flujos de alertas y registros, a menudo bajo intensas restricciones de tiempo. No importa cuán capacitados estén los equipos, clasificar alertas importantes entre el ruido puede ser un proceso metódico, propenso a errores y abrumador. Esto también puede llevar al agotamiento de la fuerza laboral.

Donde los equipos SOC tradicionales enfrentan desafíos, los agentes de IA pueden ofrecer velocidad de máquina, precisión y cobertura continua para ayudar a mejorar la eficiencia general. Pueden procesar telemetría en tiempo real, coordinar respuestas entre sistemas y mantener la vigilancia sin fatiga las 24 horas del día. Al encargarse de tareas rutinarias y de alto volumen, los agentes de IA pueden liberar a los analistas humanos para que se concentren en tareas de mayor valor, como manejar casos escalados y acciones complejas de respuesta ante amenazas.

Los primeros adoptantes están implementando agentes en producción para clasificación, investigación y respuesta en paralelo con equipos humanos, con el fin de evaluar rutas de decisión y perfeccionar el rendimiento. Sin embargo, muchas organizaciones siguen en la fase de experimentación mientras determinan la incertidumbre de costos, métodos para establecer límites, preparación del equipo y casos de uso específicos donde los agentes pueden trabajar de manera efectiva.

¿Cómo pueden los CISOs pasar de la exploración a la implementación?

Evalúa y asigna roles a los agentes para los flujos de trabajo del SOC

Comienza a identificar casos de uso con impacto real para ayudar a empoderar a tus analistas humanos y liderar a los agentes en operaciones tácticas de respuesta y búsqueda de amenazas.En PwC, priorizamos nuestros agentes del SOC en función de las alertas que los analistas ya estaban gestionando, lo que permitió que la tecnología abordara desafíos reales presentes en las operaciones diarias. Esto demuestra que la transformación puede ser práctica y alcanzable. Con base en nuestro análisis de telemetría SOC-MSSP, aquí están los escenarios que tu organización podría explorar para el SOC y otros entornos de defensa[1]:

43%	21%	20%	8%	6%	2%
Remediación de *phishing*: Capacita a los agentes para ayudar a clasificar incidentes de phishing reportados por usuarios. Identifica correos electrónicos que sean maliciosos, spam o benignos; recomienda acciones de remediación.	**Investigador de alertas de identidad:** Los agentes pueden clasificar alertas de identidad, como inicios de sesión desconocidos e intentos de acceso no autorizados, para investigar múltiples telemetrías de identidad disponibles en tu sistema de gestión de identidad y acceso (como Entra). También pueden proporcionar un puntaje de riesgo asociado al usuario.	**Investigador de alertas en *endpoints*:** Los equipos de seguridad pueden asignar agentes para examinar la detección y respuesta en *endpoints* y la detección y respuesta extendida (EDR/XDR), como *malware*, herramientas de *ransomware* o comportamiento sospechoso de procesos. También pueden correlacionar la telemetría del *host* con inteligencia de amenazas y datos de identidad para ayudar a confirmar el impacto, delimitar, y contener/erradicar.	**Detector de riesgos internos:** Identifica comportamientos riesgosos de usuarios que puedan causar pérdida de datos, violaciones de cumplimiento o amenazas internas. Este agente se integra con herramientas existentes de prevención de pérdida de datos (DLP) para ayudar a clasificar alertas, investigar violaciones de políticas (como el uso de herramientas no autorizadas) y monitorear información sensible enviada externamente.	**Investigador de alertas de red:** Obtén alertas basadas en red desde tus sistemas de detección y prevención de intrusiones (IDS/IPS) y *firewalls*, así como de tus plataformas de detección y respuesta en red (NDR). Reconstruye sesiones, identifica patrones de comando y control o exfiltración de datos y mapea los hallazgos al marco MITRE ATT&CK para ayudar a priorizar la respuesta.	**Agente de inteligencia de amenazas:** El agente de inteligencia puede equipar a tus equipos con la información más reciente sobre actores de amenazas mediante un informe semanal con recomendaciones y acciones a seguir.

Además de estos escenarios, considera adoptar agentes de búsqueda de amenazas para ayudar a mejorar las capacidades de defensa proactiva, reduciendo significativamente el tiempo y el esfuerzo operativo.

Con agentes SOC como estos, puedes agregar valor donde tus equipos de detección y respuesta más lo necesitan: para ayudar a reforzar los pasos de contención y ampliar la cobertura de defensa.

Avanza con agentes de IA en la primera línea

Una vez que hayas determinado las capacidades potenciales de detección, clasificación y búsqueda para los agentes en tu organización, necesitarás obtener el respaldo de los líderes del negocio y desarrollar un plan de implementación.

Después de todo, adoptar agentes de IA como defensores para el SOC no es una solución lista para usar. Requiere un enfoque personalizado basado en tu stack de herramientas actual, pasos claros de gobernanza, orquestación dentro de tu ecosistema tecnológico y retorno de inversión (ROI). Los puntos clave para comenzar incluyen:

Construyendo el caso de negocio para un valor a largo plazo

Comienza enfocándote en tareas con lógica repetitiva y alto esfuerzo por parte de los analistas. Define tus KPI desde el inicio y prepárate para medir el impacto financiero antes y después de la implementación. Planifica el uso más efectivo de los agentes y elige tu marco de trabajo en función de la flexibilidad de orquestación y la profundidad de integración con API. Luego, puedes optimizar costos utilizando modelos de alto razonamiento para la planificación y modelos de menor costo para la ejecución.

Incorporando una sólida gobernanza arquitectónica, IA segura y controles personalizados

Los agentes requieren un conjunto único de controles diseñados específicamente para sus comportamientos y acciones. Además, en lugar de adoptar un enfoque de seguridad como complemento, deben construirse mediante prácticas de IA segura desde las etapas de diseño y arquitectura. También es importante aplicar prácticas de IA responsable y establecer ciclos de revisión para adaptar la gobernanza a medida que el comportamiento del agente evoluciona con el tiempo.

Capacitación de tu fuerza laboral en ciberseguridad

Ejecuta agentes en modo sombra (donde observan, analizan y registran sus rutas de decisión), mientras los analistas humanos permanecen en el circuito (con visibilidad holística del flujo de trabajo del agente) para revisar y evaluar los resultados. Esto puede ayudarte a generar confianza en los agentes de IA, al mismo tiempo que das a tus equipos exposición práctica a nuevos flujos de trabajo. Proporciona parámetros de prueba para desarrollar el diseño de *prompts* y la gestión de autonomía en entornos de bajo riesgo. Y trabaja con los equipos de RR.HH., aprendizaje e ingeniería desde el inicio para co-diseñar rutas de capacitación que puedan mapearse a roles operativos y niveles de madurez.

Repensando el valor de la IA agéntica más allá de la automatización

Evalúa el valor empresarial de los agentes más allá de un aumento de productividad en el SOC. Esto podría significar incorporar elementos de IA agéntica en inversiones de seguridad existentes como SOAR, donde antes no habías podido operacionalizarlos. También podría implicar programar agentes para ayudar a desarrollar código y buscar comportamientos anómalos en los registros para investigaciones del SOC.

El camino a seguir puede ser claro si comprendes tus casos de uso para los agentes, identificas los recursos potenciales necesarios para escalar y abordas los riesgos que debes gestionar. A partir de ahí, puedes diseñar e implementar guardianes cibernéticos con seguridad y controles diseñados específicamente, así como sólidos lineamientos arquitectónicos.

[1] Fuente: análisis de telemetría de los Servicios Gestionados de Seguridad del SOC de PwC, calculando el total de incidentes que son clasificados.