Parte 1

IA agéntica: la próxima frontera de la ciberdefensa

Cómo los CISO pueden preparar a su personal

Los programas de ciberseguridad actuales se basan en un modelo operativo centrado en el ser humano, donde los analistas inician acciones, definen prioridades y responden manualmente a las amenazas. Este modelo ha sido muy útil para las empresas, especialmente gracias a que la IA ha ayudado a avanzar y automatizar el análisis de amenazas. Sin embargo, ya no es suficiente por sí solo para responder a ataques más sofisticados y específicos.

El auge de la IA agentica —sistemas autónomos y orientados a objetivos, capaces de tomar decisiones y ejecutar tareas con mínima intervención humana— marca un avance transformador para la ciberdefensa. Estos sistemas de IA ya no son solo herramientas que ayudan con el análisis; se están convirtiendo en compañeros de equipo digitales que pueden actuar de forma independiente, colaborar con equipos humanos e incluso iniciar respuestas de seguridad.

Para los CISO, esto no es solo una evolución técnica. Es un cambio cultural y organizativo que exige una nueva forma de pensar para ganarse la confianza y la aceptación de los equipos de seguridad.

Forjando una alianza en ciberdefensa

Con la IA con agentes, los CISO están entrando en una nueva era de equipos híbridos donde los agentes trabajan activamente junto con analistas humanos. Los agentes pueden detectar amenazas, clasificar incidentes, orquestar respuestas y aprender continuamente de sus entornos.

El rol humano ahora cambia de **ejecutor a supervisor, estratega y responsable ético.**

Esta transición desafía las suposiciones arraigadas sobre roles y responsabilidad. Los profesionales de la ciberseguridad deben desarrollar un nuevo tipo de alfabetización digital, pasando del uso de herramientas a la gestión de sistemas autónomos que operan de forma independiente.

Cómo los CISO pueden movilizar a sus equipos

Los equipos de seguridad deben aprender a colaborar y comunicarse con ellos —a menudo en su lenguaje natural— y comprender sus límites de decisión. Además, deben establecer un proceso de gobernanza para supervisar e identificar las medidas a tomar cuando se rompe la confianza.

Al considerar la incorporación de un enfoque de IA agente en su programa cibernético, los CISO pueden preparar a sus equipos de seguridad mediante:

Imagina sistemas inteligentes que detectan amenazas en tiempo real, coordinan respuestas en todas las redes, investigan vulnerabilidades y ajustan sus tácticas a medida que cambian las condiciones.

Centrándose en la colaboración humanos-IA, con los humanos al mando.

Capacita a tu fuerza laboral cibernética y desmitifica la IA agéntica. Comunica claramente las capacidades y limitaciones de la IA agéntica, y cómo puede colaborar con los humanos para mejorar la ciberseguridad. Que los colaboradores comprendan el propósito y los beneficios de la IA agéntica puede ayudar a alinear a los equipos con tu estrategia de ciberseguridad y objetivos de resiliencia.

Capacita a sus equipos para desarrollar casos de uso de IA con agentes. Establece un entorno donde los colaboradores puedan idear y presentar casos de uso para su desarrollo en el ámbito de la inteligencia artificial y así resolver problemas que les preocupan. Fomenta una cultura que promueva el intercambio de conocimientos y la resolución de problemas en torno al uso de herramientas cibernéticas de IA con agentes para resolver desafíos reales de ciberseguridad.

Hacer que la IA agéntica sea responsable y confiable en cada paso.

Establece controles robustos de gestión de identidad y acceso de IA. Los sistemas de IA agéntica necesitarán acceso y, en ocasiones, incluso "identidades" para establecer operaciones de ciberseguridad responsables. Otorga a la IA agéntica solo los privilegios necesarios para sus tareas, siguiendo los procesos y controles estándar de identidad y acceso (IAM). Supervisa constantemente su comportamiento y realiza revisiones periódicas de acceso e identidad.

Integra los principios de IA responsable desde el principio. La clave para la adopción y el éxito de la IA es generar confianza. Al aplicar los principios de la IA Responsable, puedes ayudar a generar confianza entre líderes, colaboradores, clientes y otras partes interesadas. Además, es importante supervisar continuamente las regulaciones y estándares del sector, especialmente dada la rápida evolución de la IA.

Anticipando cambios de paradigmas y roles.

De una defensa impulsada por analistas a una defensa reforzada por agentes. Los analistas humanos ascenderán a roles cada vez más estratégicos, como la supervisión, el modelado de amenazas y la estrategia de riesgos.

De roles fijos a una colaboración fluida. Los equipos evolucionarán dinámicamente, y los agentes asumirán diferentes responsabilidades según las necesidades.

De herramientas aisladas a ecosistemas interoperables. Los agentes de IA prosperarán en entornos donde se puedan integrar herramientas, datos y plataformas, lo que impulsará a los líderes cibernéticos a priorizar la interoperabilidad y la preparación para la IA en su conjunto tecnológico.

La IA agéntica no está reemplazando al profesional de la ciberseguridad, sino que está redefiniendo lo que significa serlo. Los CISO que adopten este cambio ahora podrán posicionar a sus organizaciones a la vanguardia de la defensa aumentada por IA. El futuro pertenecerá a quienes vean a estos agentes no como amenazas, sino como compañeros de equipo.