Las empresas europeas comienzan a proteger agentes de inteligencia artificial

El gasto en ciberseguridad entra en una nueva fase. La seguridad de la identidad para sistemas autónomos se perfila como un nuevo motor de inversión clave, a medida que la ola de regulaciones de la UE se prepara para transformar el mercado, señala Context

Las organizaciones europeas están comenzando a invertir en la seguridad de sistemas de inteligencia artificial que operan sin supervisión humana directa, según un nuevo análisis de Context.

Context identifica la inversión en modelos de seguridad centrados en la identidad como una de las áreas de gasto en ciberseguridad de mayor crecimiento en el primer trimestre de 2026. Y es que, a medida que las empresas implementan sistemas de IA capaces de actuar de forma autónoma, estos sistemas crean nuevas identidades dentro de las redes corporativas que conllevan privilegios de acceso reales y riesgos reales. Protegerlas requiere un enfoque diferente al de la protección tradicional de endpoints o perímetros, y la demanda de las herramientas y arquitecturas pertinentes creció significativamente durante el trimestre.

“Este avance marca un cambio significativo en la forma en que las empresas abordan la ciberseguridad”, afirma Joe Turner, vicepresidente de investigación de Context. “Los límites de lo que se debe proteger se amplían más allá de las personas y los dispositivos para incluir agentes de IA autónomos que toman decisiones independientes en toda la infraestructura corporativa”.

Reevaluación de la postura de seguridad

Este cambio se produce paralelamente a una tendencia más amplia hacia las arquitecturas de confianza cero y las soluciones de cumplimiento automatizadas. En conjunto, estas tendencias apuntan a un ciclo de inversión fundamentalmente diferente al anterior.

Las anteriores oleadas de gasto en ciberseguridad fueron en gran medida reactivas, desencadenadas por brechas de seguridad o ciclos de renovación de hardware. El ciclo actual está siendo moldeado por cambios estructurales en la forma en que operan las organizaciones, donde la adopción de la IA y la presión regulatoria se combinan para forzar una reevaluación más sistemática de la postura de seguridad.

En el ámbito regulatorio, la presión está a punto de intensificarse considerablemente. Se prevé que NIS2, DORA y la Ley de IA impulsen un gasto significativo en cumplimiento normativo durante la segunda mitad de 2026, a medida que las organizaciones se enfrentan a requisitos más estrictos y posibles sanciones económicas sustanciales por incumplimiento. La previsión de Context de un fuerte crecimiento del software de ciberseguridad durante el resto del año se basa en gran medida en esta dinámica.

“La naturaleza de lo que las organizaciones necesitan proteger está cambiando más rápido de lo que la mayoría de las estrategias de seguridad han podido seguir el ritmo”, afirma Joe Turner. Un agente de IA con acceso a sistemas financieros o datos de clientes representa un riesgo de seguridad, al igual que un usuario humano con privilegios. Las herramientas para gestionarlo aún están en desarrollo, pero la inversión ya está comenzando, anticipándose a los plazos regulatorios que la convertirán en una necesidad imperiosa.

El hardware de ciberseguridad continuó su descenso, con una caída del 5,7 % en el primer trimestre, a medida que las organizaciones priorizaban las arquitecturas de seguridad definidas por software. Context prevé que esta divergencia persista, y que el hardware se convierta en un segmento cada vez más especializado, concentrado en infraestructuras soberanas, resiliencia industrial y entornos específicos de cumplimiento normativo.

Fuente: Las empresas europeas comienzan a proteger agentes de inteligencia artificial | Seguridad | IT User