Lista de comprobación de IA para proveedores de seguridad

Preguntas clave al evaluar la IA en soluciones de ciberseguridad

El alcance y la eficacia de la IA en las herramientas de seguridad es un tema candente en el sector, omnipresente tanto en las ponencias de las conferencias y como en las salas de juntas. Utilice esta lista de comprobación para asegurarse de que invierte adecuadamente en cualquier solución de ciberseguridad que incorpore la IA.

¿Qué expectativas tiene para la herramienta?

Muchas compañías confían en que las nuevas tecnologías de IA puedan acelerar determinados procesos, reducir redundancias o mejorar sus ciberdefensas pero, ¿son realmente objetivos viables? Aborde la adquisición de nuevas herramientas con un plan claro y objetivos definidos.

¿Qué datos se utilizan para crear y entrenar el modelo?

Antes de incorporar una nueva herramienta o producto basado en IA, es fundamental asegurarse de que el modelo se esté entrenando con datos en los que se pueda confiar.

¿Qué tipo o tipos de medidas de privacidad se han implementado?

¿Se utiliza información personal identificable (PII) como parte de esta tecnología? En caso afirmativo, ¿se anonimizan estos datos antes de utilizarse? ¿Qué medidas aplica el proveedor para evitar la posible reidentificación de los datos si se produce una filtración?

¿Qué tipo o tipos de supervisión humana existen?

Pregúntese y pregunte a su proveedor qué tipo de supervisión humana tiene previsto implementar en cualquier nueva herramienta de IA. Entre la posibles medidas podrían incluirse la verificación de hechos, el control de calidad o la monitorización manual.

¿Con qué facilidad puede integrarse la solución en su pila tecnológica actual?

Es fundamental entender de qué manera afectan los posibles cambios en las soluciones de seguridad actualmente en uso a la pila tecnológica de su organización. Esto incluso podría incluir la forma en que se implementan los parches.

¿Es la tecnología de IA optativa?

Pregunte al proveedor si la IA generativa es una función opcional o si está completamente integrada. Si es opcional, aclare si viene activada o desactivada por defecto.

13-01-2025 ES (DD)

SOPHOS