La división de nub de Google está siguiendo los pasos de Microsoft con el lanzamiento de Security AI Workbench, que aprovecha los modelos generativos de IA para obtener una mejor visibilidad del panorama de amenazas.

El paquete de seguridad cibernética está impulsado por Sec-PalM, un modelo de lenguaje extenso especializado (LLM) que está *«ajustado para casos de uso de seguridad».*

La idea es aprovechar los últimos avances en IA para aumentar el análisis de incidentes puntuales, la detección de amenazas y el análisis para contrarrestar y prevenir nuevas infecciones mediante la entrega de inteligencia confiable, relevante y procesable.

Con ese fin, Security AI Workbench abarca una amplia gama de nuevas herramientas impulsadas por IA, que incluyen VirusTotal Code Insight y Mandiant Breach Analytics para Chronicle, para analizar secuencias de comandos potencialmente maliciosas y alertar a los clientes sobre infracciones activas en sus entornos.

Los usuarios, al igual que con Security Copilot basado en GPT-4 de Microsoft, pueden *«buscar, analizar e investigar datos de seguridad de forma conversacional»* con el objetivo de reducir el tiempo medio de respuesta y determinar rápidamente el alcance total de los eventos.

Por otro lado, la función Code Insight en VirusTotal está diseñada para generar resúmenes de fragmentos de código en lenguaje natural para detectar y mitigar amenazas potenciales. También se puede usar para marcar falsos negativos y borrar falsos positivos.

Otra oferta clave es Security Command Center AI, que utiliza Sec-PaLM para proporcionar a los operadores un *«análisis casi instantáneo de los hallazgos y posibles rutas de ataque»,* así como los activos afectados y las mitigaciones recomendadas.

Google también está haciendo uso de modelos de aprendizaje automático para detectar y responder al abuso de API y ataques a la lógica empresarial, en los que un adversario usa

una funcionalidad legítima para lograr un objetivo malicioso sin activar una alerta de seguridad.

> *«Debido a que Security AI Workbench se basa en la infraestructura Vertex AI de Google Cloud, los clientes controlan sus datos con capacidades de nivel empresarial, como aislamiento de datos, protección de datos, soberanía y soporte de cumplimiento»,* dijo Sunil Potti de Google Cloud.

El desarrollo se produce días después de que Google anunciara la creación de una nueva unidad llamada Google DeepMind, que reúne a sus grupos de investigación de IA de DeepMind y el equipo Brain de Google Research para *«construir sistemas más capaces de forma más segura y responsable».*