POTENCIAL DIGITAL

CDTIC Centro Demostrador TIC

CIBERSEGURIDAD PARA UN FUTURO CONECTADO

PROTECCIÓN EN LA ERA DIGITAL

Ponencia 2: Agentes de IA, el refuerzo multiplicador de los Servicios de Centros de Operaciones de Seguridad

Roberto Nuevo Marcos

Ingeniero Senior Ciberseguridad

evolutio

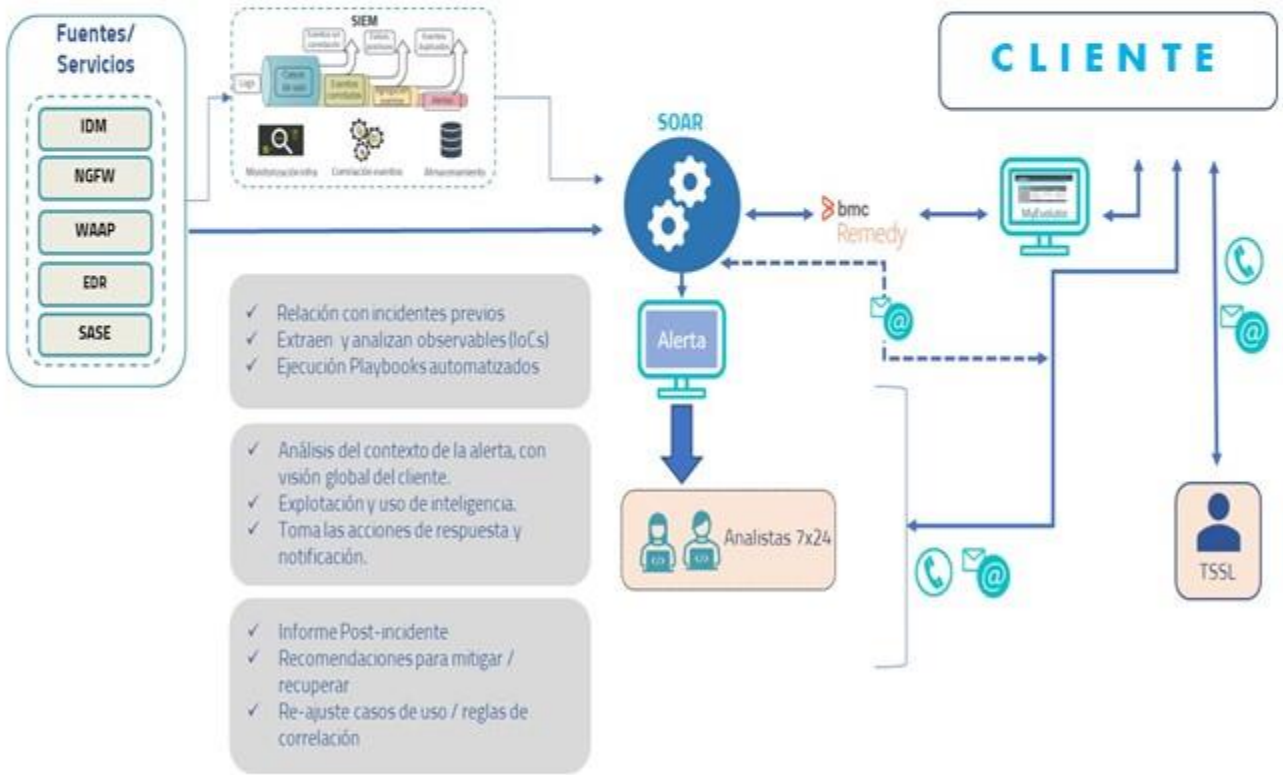
CDTIC Centro Demostrador TIC

JUNTA DE EXTREMADURA
Consejería de Economía, Empleo y Transformación Digital

Cofinanciado por la Unión Europea

Centro de Operaciones de Seguridad SOC

Los servicios de SOC son la primera línea de Defensa en Ciberseguridad y permiten responder a las amenazas avanzadas que actualmente enfrentan las organizaciones, tanto publicas como privadas.



Un SOC opera bajo presión constante, enfrentando un volumen abrumador de alertas y amenazas. La sobrecarga genera fatiga analítica, estrés crónico y **riesgo elevado de errores críticos en la respuesta**.

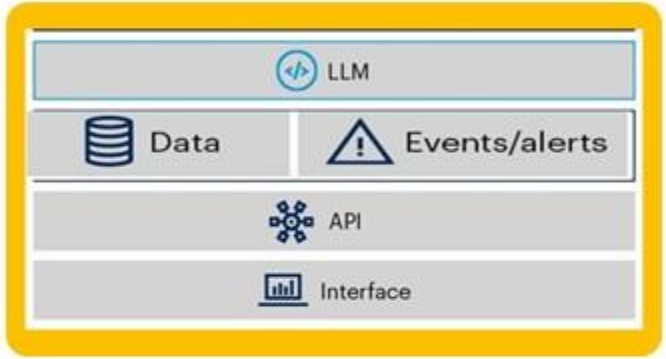
El uso de la IA para la evolución del SOC

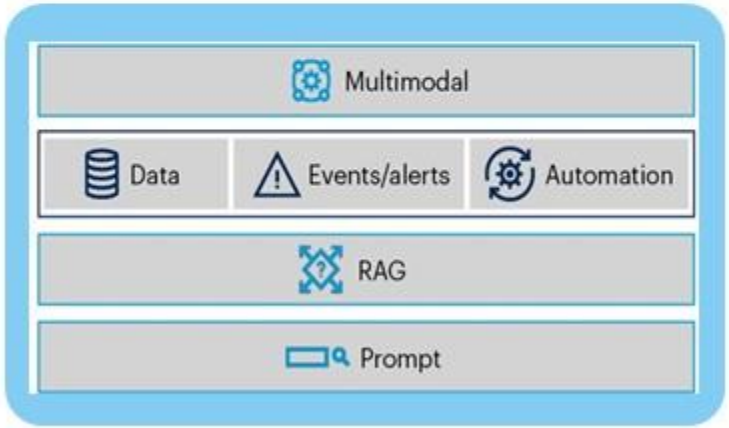
Principales puntos de desarrollo con IA:

- **Sobrecarga de alertas** : los modelos de IA filtran el ruido y priorizan las amenazas que importan
- **Flujos de trabajo manuales** : la automatización de la seguridad reduce las tareas repetitivas y que consumen mucho tiempo.
- **Fragmentación de herramientas** : la IA integra diversas herramientas de seguridad en soluciones SOC cohesivas
- **Capacidad humana limitada** : los SOC impulsados por IA respaldan a los humanos en el SOC, mejorando el rendimiento sin aumentar la plantilla.
- **Detección en tiempo real** : la IA mejora la visibilidad y la velocidad de respuesta en todo el panorama del SOC, lo que garantiza una mayor seguridad.

Modelos de aplicación de IA en un SOC

Soporte a tareas con una herramienta externa : A menudo una función de back-end, limitada a consultas individuales a un LLM comercial (por ejemplo, GPT de OpenAI) para generar contenido que anteriormente el equipo del proveedor de ciberseguridad crearía de una manera más manual. Algunos ejemplos son **el resumen de alertas o añadir contexto a informes**.





Producto integrado en una solución comercial: Funciones y **Agentes de Seguridad**, que pueden respaldar el uso de los productos del proveedor para una función particular y llevar a cabo una variedad de **tareas y funciones de proceso** en el contexto de lo que está disponible para ese conjunto de herramientas directamente. Algunos ejemplos típicos son productos o suscripciones basados en indicaciones interactivas para apoyar a los analistas de SOC.

Retrieval-Augmented Generation (Generación Aumentada por Recuperación).

Soluciones comerciales de fabricantes lideres

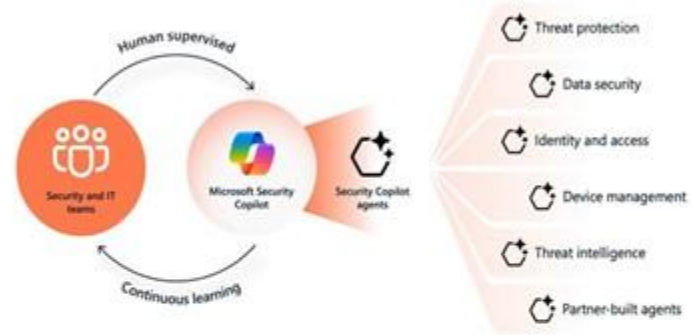
Gemini for Google SecOps es un asistente de IA que acelera la investigación de amenazas analizando grandes volúmenes de datos y generando resúmenes contextuales. Facilita la detección, respuesta y automatización de incidentes, mejorando la eficiencia del SOC. Además, integra inteligencia de amenazas de Mandiant y VirusTotal para decisiones más rápidas y precisas.
Ofrece análisis avanzados en lenguaje natural directamente sobre grandes volúmenes de datos de seguridad.

Copilot for Security es un asistente de IA de Microsoft que optimiza la detección, investigación y respuesta a incidentes. Analiza datos de seguridad en tiempo real, genera insights contextuales y automatiza tareas repetitivas. Integra información de Microsoft Defender y Threat Intelligence, mejorando la rapidez y precisión en los SOC.
Integración profunda con el ecosistema Microsoft 365 y Defender XDR, optimizando por ejemplo la protección de identidad.

Charlotte AI de CrowdStrike es un asistente de IA que acelera la investigación y respuesta ante amenazas en la plataforma Falcon. Interpreta datos de seguridad, genera análisis detallados y automatiza procesos complejos. Aprovecha inteligencia de amenazas de CrowdStrike para mejorar la eficiencia y precisión del SOC.
Aprovecha la telemetría masiva de millones de endpoints globales de Falcon para ofrecer respuestas de alta fidelidad.

Precision AI de Palo Alto Networks es una suite de IA que potencia la detección, prevención y respuesta a amenazas en toda su plataforma. Analiza datos en tiempo real, correlaciona eventos y automatiza decisiones de seguridad. Mejora la velocidad, precisión y eficacia operativa en entornos SOC complejos.
Combina múltiples motores de IA (Machine Learning, Deep Learning y LLMs) para ofrecer una detección predictiva y respuesta automatizada en todo su ecosistema de firewalls, XDR y SASE.

Implementación en las soluciones de Microsoft Security



Copilot for Security (el producto principal)

Es la **plataforma completa** de IA generativa de Microsoft para seguridad.

Funciona como un **asistente unificado** para SOCs y equipos de IT.

Objetivo: Ayudar a detectar, investigar y responder a amenazas, automatizar tareas de seguridad y reducir la carga operativa.

Integra datos de Defender, Sentinel, Intune, Purview, Entra, y Microsoft Threat Intelligence.

Funciona a través de:

- **Chat interactivo**: preguntas en lenguaje natural.
- **Instrucciones contextuales**: análisis automático de incidentes, generación de scripts, investigación guiada.
- **Workbooks/Dashboards**: resultados visuales integrados en el portal.

El cerebro y motor de IA para todas las operaciones de ciberseguridad dentro del ecosistema Microsoft.

Security Copilot Agents (los agentes específicos)

Son agentes especializados, construidos sobre Copilot for Security.

Están diseñados para tareas específicas o áreas concretas de seguridad.

Objetivo: Ofrecer asistentes expertos en cada dominio de seguridad para tareas más profundas o específicas.

Ejemplos:

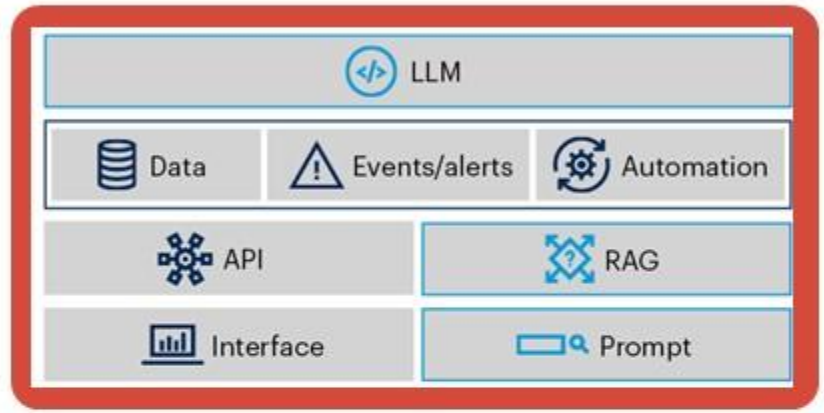
- **Defender Threat Intelligence Agent:** facilita análisis de amenazas avanzadas.
- **Entra Agent:** especializado en gestión de identidades y accesos.
- **Purview Agent:** enfocado en cumplimiento y protección de datos.

Se pueden integrar en flujos de trabajo automáticos o como asistentes independientes en sus respectivos portales (Defender, Entra, Sentinel...).

Los Security Copilot Agents son extensiones especializadas que aprovechan la IA central de Copilot for Security pero se enfocan en funciones particulares.

Modelos de aplicación de IA en un SOC (continuación)

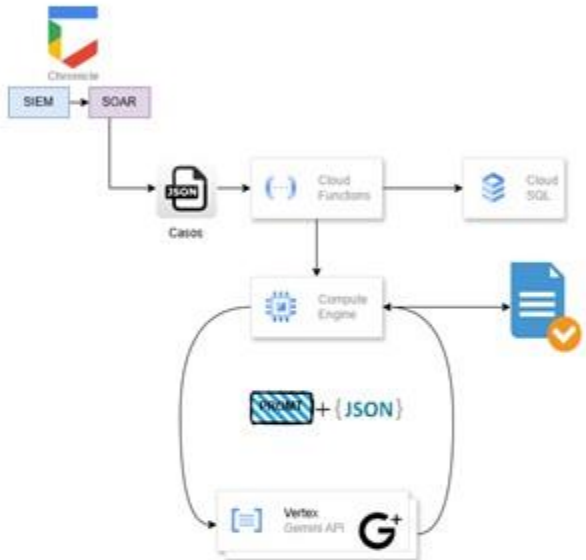
Soporte a Procesos: Por lo general, se entrega como un Prompt integrado en una interfaz de usuario existente. Estas funciones de asistente apoyan preguntas en relación con una actividad actual llevada a cabo por el usuario y a menudo apoyan un **proceso repetitivo**, ofreciendo sugerencias para las acciones del siguiente paso. Algunos ejemplos típicos son la búsqueda guiada de amenazas (Threat Hunting).



Implementación real en Evolutio – proyecto esponsorizado por INCIBE

Es un proyecto desarrollado por Evolutio en base a los fondos Next Generation, gestionados por **INCIBE**. Su objetivo era demostrar la potencia de la IA en los Servicios de SOC. Se ha conseguido desarrollar el proyecto con éxito y es parte de las capacidades actuales del SOC de Evolutio. Habiendo obtenido **evidencias importantes**.

Caso práctico del proyecto : Informes de Ciberincidentes



Flujo:

1. Extracción de caso
2. Enriquecimiento con guías de ciberseguridad (mitre, cve,..)
3. Prompting
4. Generación automática de informe

¿ La IA sustituirá a los Analista en los Servicios de SOC ?

A corto y medio plazo NO

Más adelante ...