Cómo están transformando las herramientas SOAR la inteligencia sobre amenazas

Es evidente que la transformación digital ha traído un sinfín de ventajas a todas las empresas en general, pero no lo es menos que las tecnologías que la hacen posible han ampliado tanto la superficie de ataque que la seguridad se está viendo amenazada por nuevos riesgos. Ahora que la computación en la nube, la automatización y la inteligencia artificial están a la orden del día, se pueden perpetrar campañas de ataques a unos niveles de sofisticación y escala sin precedentes con una intervención humana mínima. Hoy en día, los ciberdelincuentes atacan ordenadores cada 39 segundos.[1] Según un estudio de Cybersecurity Ventures, en 2021 una empresa será víctima de un ataque por ransomware cada 11 segundos.[2] El motivo por el cual esto es posible es que los atacantes están consiguiendo actuar a velocidad de máquina.

1. «Hackers Attack Every 39 Seconds» («Los hackers atacan cada 39 segundos», disponible en inglés), Security Magazine, 10 de febrero de 2017, https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
2. «Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021» («Las predicciones apuntan a que en 2021 la ciberdelincuencia internacional costará 6 billones de dólares», disponible en inglés), Cybercrime Magazine, 7 de diciembre de 2018, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

¿Qué pueden hacer las empresas ante esta situación? Cada vez es más difícil implementar y mantener una estrategia de seguridad saludable que llegue a toda la empresa sin interrumpir su actividad. Por eso, el centro de operaciones de seguridad (SOC, por sus siglas en inglés) desempeña un papel crucial. Los equipos de los SOC son responsables de encarar este reto mediante el uso de una combinación de tecnologías de seguridad integradas, procesos optimizados y capacidad humana para detectar, investigar y responder a las ciberamenazas avanzadas.

Desafortunadamente, los equipos de seguridad, sean del tamaño que sean, se sienten sobrepasados e incapaces de funcionar a pleno rendimiento debido a la escasez de profesionales cualificados, a los altos volúmenes de alertas de baja fidelidad que reciben, al uso de herramientas de seguridad inconexas y a la descontextualización de las amenazas externas. Para superar estos retos, es necesario desgranar el funcionamiento interno de un SOC y hacernos una idea de qué se cuece entre bambalinas. Solo entonces seremos capaces de apreciar la enormidad a la que se enfrentan los equipos de los SOC y estaremos en condiciones de hallar soluciones.

En organizaciones más grandes, los equipos de operaciones de seguridad más experimentados manejan un número de piezas móviles insostenible. En definitiva, para que las operaciones de seguridad sean efectivas, se necesitan tres funciones básicas: los analistas del SOC, los responsables de responder a los incidentes y los analistas de amenazas.

Analistas del SOC

Los analistas del SOC examinan miles de alertas internas al día procedentes de las tecnologías de información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés), los sistemas de detección y respuesta en el endpoint (EDR, por sus siglas en inglés) y, en ocasiones, cientos de otras herramientas de seguridad internas. Su trabajo consiste en ser los ojos de la empresa: detectar incidentes de seguridad, investigarlos, averiguar su causa principal y responder de inmediato. Los analistas del SOC supervisan constantemente la red con herramientas de detección con el fin de detectar e investigar amenazas potenciales. Cuando encuentran un riesgo potencial, los analistas tienen que documentar sus observaciones y compartir recomendaciones con las distintas partes implicadas.

En resumen, los analistas del SOC suelen enfrentarse a los siguientes problemas:

- **Mal de alertas:** La empresa media recibe más de 11 000 alertas de seguridad al día3 y carece de personal suficiente para gestionarlas.
- **Falta de tiempo:**La desintegración que existe entre las muchas herramientas que tienen que utilizar los analistas ralentiza todas las fases del proceso.
- **Contexto limitado:** Investigar las amenazas y responder a ellas suele llevar días. Las herramientas de seguridad no proporcionan suficiente información contextual sobre las alertas ni sobre el impacto que tienen en el entorno, lo que obliga a los analistas a dar sentido a toda esta información de forma manual.

Para resolver estos problemas, los analistas necesitan:

- **Herramientas de automatización** que realicen las tareas diarias para que ellos puedan dedicarse a las que aportan valor a la empresa.
- **Colaborar en tiempo real** con el resto del equipo para que todo el mundo trabaje sincronizado siempre y aprenda de los demás.
- **Inteligencia sobre amenazas** que les dé el contexto que necesitan para valorar con acierto su importancia e impacto potencial.

Figura 1: Problemas a los que se enfrentan los analistas del SOC

Responsables de responder a los incidentes

A los responsables de responder a los incidentes les preocupa el control de los daños. Buscan posibles brechas de seguridad y, si encuentran indicios de que se ha producido una, su trabajo será investigarlas e impedir que se propaguen. Debido a la naturaleza sensible de las brechas, todos los indicios deben documentarse adecuadamente y compartirse con todas las personas implicadas. Los responsables de responder a los incidentes tienen acceso a herramientas que los ayudan a contener las brechas, como las de EDR, que eliminan el host de extremo. Se coordinan con los administradores de cortafuegos para implementar políticas que contengan la propagación por la red. Echan mano de inteligencia sobre amenazas externas para conocer los perfiles de los atacantes y las técnicas que suelen utilizar, lo cual les permite responder con confianza y precisión.

En consecuencia, los responsables de responder a los incidentes se enfrentan a problemas en los siguientes ámbitos:

- **Transferencia de conocimientos:** la falta de colaboración entre los distintos equipos da lugar a lagunas de seguridad.
- **Gestión de casos:** la manera genérica de gestionar los casos no es adecuada para los casos de uso de seguridad, lo que se traduce en ineficiencia y documentación de mala calidad.
- **Falta de inteligencia sobre amenazas:** muchos responsables de responder a los incidentes se ven obligados a utilizar procesos manuales defectuosos para contextualizar mejor las amenazas externas, lo que genera retrasos y riesgos.

Los responsables de responder a los incidentes necesitan:

- **Una metodología completa de gestión de los casos de seguridad** que les permita documentar sus observaciones en detalle y colaborar en tiempo real con el resto de las personas implicadas en estos procesos, así como proporcionar a toda la empresa medidas preventivas y de puesta en cuarentena.
- **Inteligencia sobre amenazas** para ofrecer un contexto más detallado sobre los atacantes y sus motivaciones.

Figura 2: Responsables de responder a los incidentes

3. Según un estudio por encargo llevado a cabo por Forrester Consulting para Palo Alto Networks, febrero de 2020. En el momento de publicar este documento, el informe aún no se ha difundido oficialmente.

Programas/analistas de inteligencia sobre amenazas

Los analistas de amenazas se dedican a detectar los riesgos potenciales presentes en la red que se han pasado por alto y suponen un peligro para las organizaciones. Proporcionan contexto sobre las amenazas potenciales combinando la inteligencia sobre amenazas externas procedente de distintos orígenes con la inteligencia humana. Según un estudio reciente dirigido por el SANS Institute, el 49,5 % de las organizaciones tienen algún tipo de equipo o programa de inteligencia sobre amenazas con una partida presupuestaria y un personal propios.[4] Esto es una muestra más del protagonismo cada vez mayor que tienen los analistas de inteligencia sobre amenazas, quienes ayudan a identificar a los atacantes y descubrir sus motivaciones, técnicas y procesos. Los equipos de inteligencia sobre amenazas envían sus conclusiones sobre los ataques e informes sobre la situación general de las amenazas a los equipos del SOC y de respuesta a incidentes para mejorar las medidas preventivas.

Los analistas de la inteligencia sobre amenazas se enfrentan a los siguientes problemas:

- **Falta de control** sobre las fuentes de inteligencia sobre amenazas, lo que los obliga a ajustar y puntuar los indicadores de riesgo (IOC, por sus siglas en inglés) de forma manual para adaptarlos a su propio entorno.
- **Procesos de trabajo inconexos** que deterioran la comunicación y la integración entre las herramientas, equipos y procesos de respuesta a incidentes e inteligencia sobre amenazas.
- **Dificultad para tomar medidas,** ya que traducir la inteligencia sobre amenazas en acciones concretas requiere mucho trabajo manual y delegar tareas en otros equipos.

Los analistas de la inteligencia sobre amenazas necesitan:

- **Control total** de los indicadores de las fuentes de inteligencia sobre amenazas para crear su propia lógica y reputación según las necesidades de su entorno y de su empresa.
- **Colaboración** con otros equipos para dotarlos rápidamente de contexto e información actualizada basada en investigaciones.
- **Documentación robusta** que refleje los datos cosechados.

Figura 3: Dificultades a las que se enfrentan los analistas de amenazas

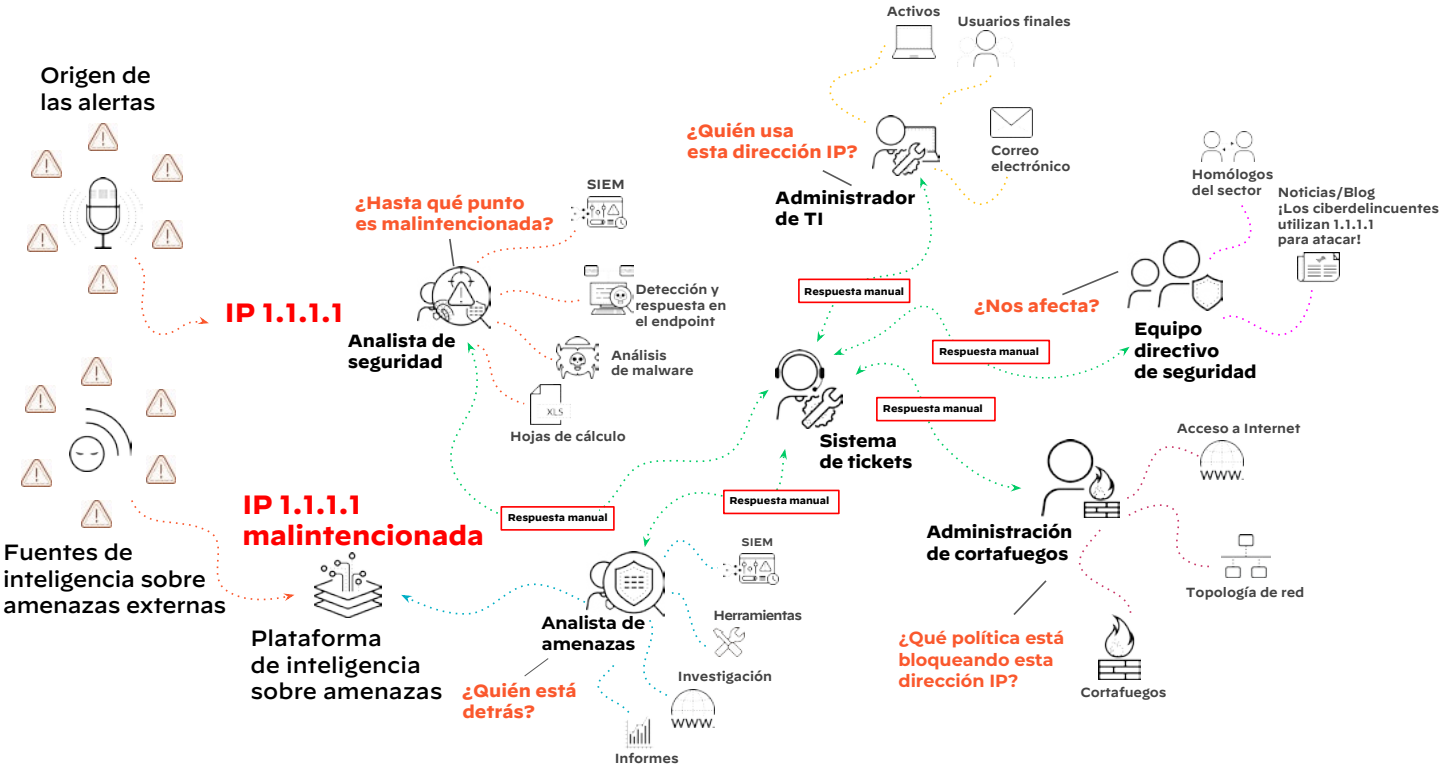

Figura 4: Visión holística de un día cualquiera en un SOC

4. «2020 SANS Cyber Threat Intelligence (CTI) Survey» («Encuesta de inteligencia sobre ciberamenazas de SANS 2020», disponible en inglés), SANS Institute, 11 de febrero de 2020, https:/www.sans.org/reading-room/whitepapers/threats/paper/39395.

SOAR al rescate

Hay algo que tienen en común todos estos equipos: Todos ellos necesitan automatización, gestión de casos, colaboración en tiempo real y un intercambio muy intenso de inteligencia sobre amenazas actualizada. Muchos SOC utilizan plataformas de orquestación, automatización y respuesta de seguridad (SOAR, por sus siglas en inglés) para gestionar las alertas procedentes de todos los orígenes, estandarizar los procesos con libros de estrategias y automatizar la respuesta para cualquier caso de uso de seguridad, pero sigue existiendo un gran vacío en cuanto a la gestión de la inteligencia sobre amenazas.

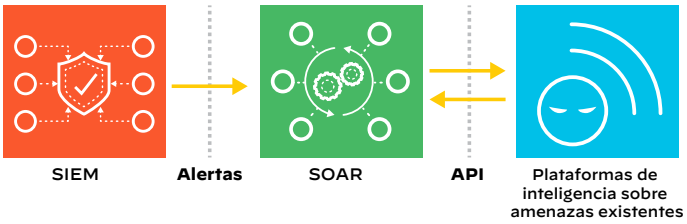

Figura 5: Una típica implementación inconexa de SOAR + TIP

Para ver las amenazas externas, los equipos de seguridad tienen que conformarse con unas plataformas de inteligencia sobre amenazas (TIP, por sus siglas en inglés) que funcionan de forma aislada y no cumplen bien su cometido, por lo que resulta casi imposible automatizar la aplicación de medidas sobre determinados indicadores en fuentes de amenazas inconexas. Los analistas del sector, conscientes de este problema, creen que la solución sería unir las plataformas SOAR y TIP. Las TIP no hacen más que añadir complejidad si agregan inteligencia de distintos orígenes sin el contexto real ni la automatización necesarios para tomar medidas rápidas y fiables. Salta a la vista que urge adoptar un nuevo enfoque.

Necesitamos una plataforma SOAR ampliada

Parece lógico recurrir a Cortex™ XSOAR, que cuenta con un sistema nativo de gestión de inteligencia sobre amenazas. Threat Intel Management, que forma parte de la plataforma ampliable Cortex XSOAR, define una nueva forma de unificar la agregación, puntuación e intercambio de datos de inteligencia sobre amenazas a través de una tecnología de automatización basada en libros de estrategias. Ofrece a los responsables de la seguridad la posibilidad de saber Con claridad cuáles son las amenazas más prioritarias para dar la respuesta adecuada en toda la empresa.

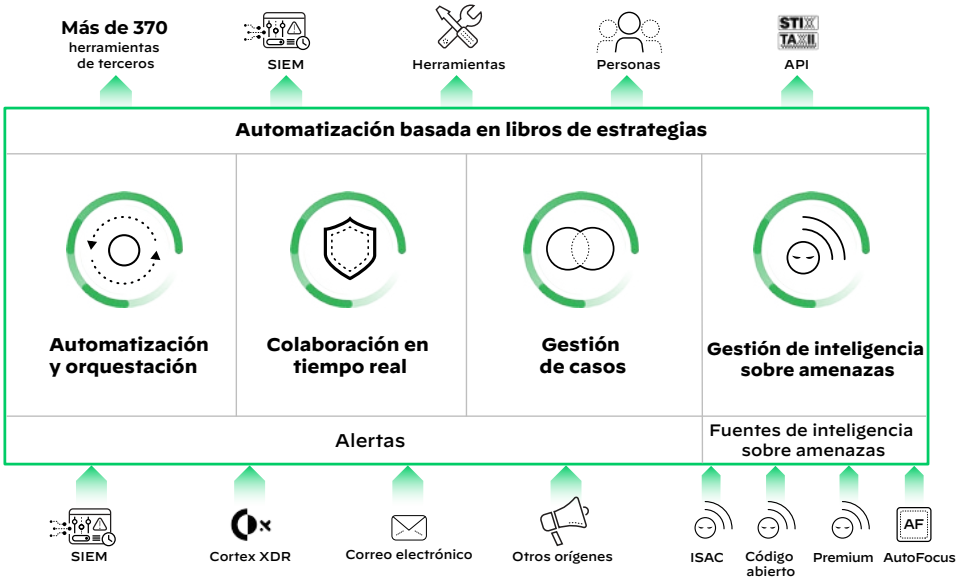

Figura 6: Automatización basada en libros de estrategias de Cortex XSOAR

Figura 7: Ventajas de la inteligencia sobre amenazas

Cortex XSOAR aúna la gestión de casos, la automatización, la colaboración en tiempo real y la gestión de inteligencia sobre amenazas nativa en la primera plataforma ampliada de orquestación, automatización y respuesta de seguridad del sector.

Cortex XSOAR también le permite:

- **Eliminar las tareas manuales** con libros de estrategias automatizados que permiten agregar, analizar, desduplicar y gestionar millones de indicadores diarios de fuentes de datos de distintos orígenes. Podrá ampliar y editar la puntuación de los IOC con facilidad, Así como encontrar los proveedores que tengan los indicadores más interesantes para su entorno en concreto.
- **Descubrir las amenazas cruciales** mediante la combinación de inteligencia sobre amenazas de terceros con incidentes internos para priorizar las alertas y tomar decisiones más acertadas a la hora de reaccionar. Podrá potenciar las investigaciones con la inteligencia sobre amenazas integrada de alta fidelidad que brinda el servicio AutoFocus™ de Palo Alto Networks. Asimismo, podrá complementar cualquier herramienta de detección, supervisión o respuesta con el contexto extraído de una inteligencia sobre amenazas seleccionada.
- **Actuar de forma automatizada** para bloquear de inmediato las amenazas que se ciernen sobre su empresa. Podrá llevar a cabo investigaciones más ambiciosas compartiendo fácilmente la inteligencia sobre amenazas tanto con sus equipos internos como con otras organizaciones fiables.

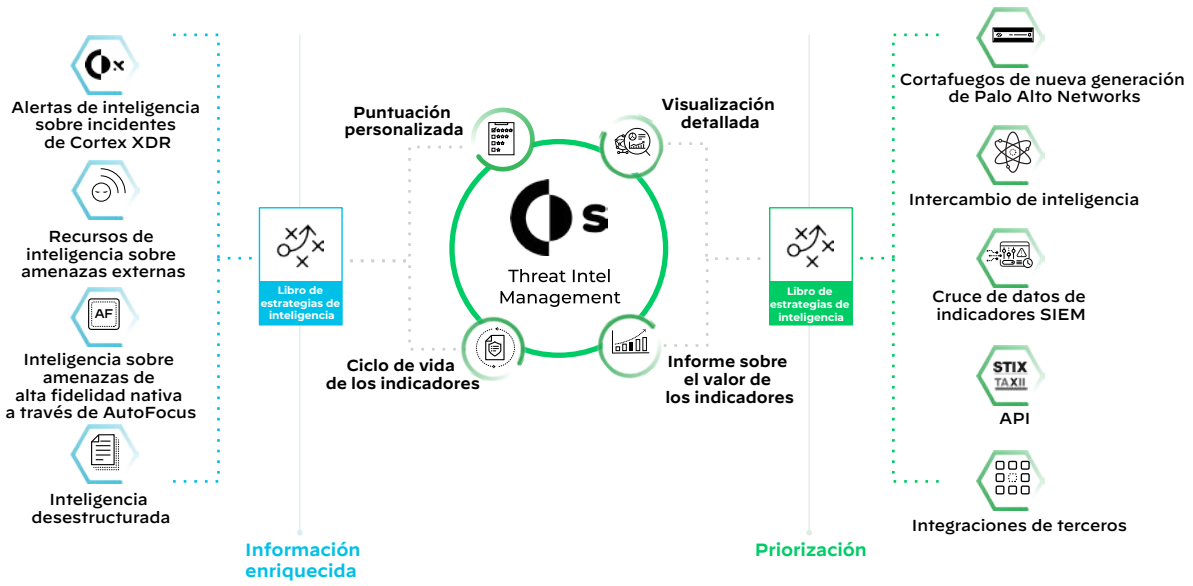

Figura 8: Mejora y priorización de la inteligencia sobre amenazas

Caso de uso: priorización de incidentes

Los analistas de seguridad gestionan millones de indicadores recabados de cientos de fuentes de inteligencia de orígenes diferentes. Estos indicadores carecen del contexto que necesitan los analistas para tomar decisiones con conocimiento de causa, actuar y responder con confianza y precisión. Las herramientas de que disponen son incapaces de gestionar todos los indicadores, así que los analistas terminan cambiando el orden de prioridad de los indicadores a mano para adaptarlos a su entorno. Cortex XSOAR se integra con una tecnología de gestión de inteligencia sobre amenazas nativa que pone en manos de los analistas todo el control y la flexibilidad que necesitan para incorporar la lógica de su empresa a sus sistemas de puntuación. Gracias a que se integra con más de 370 proveedores, los analistas pueden reaccionar en tiempo real conforme los indicadores se van procesando.

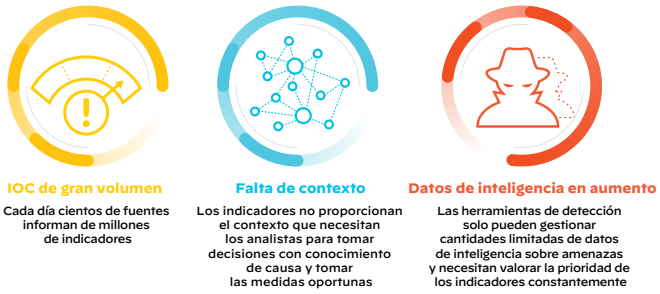

Figura 9: Problemas derivados del uso de herramientas de inteligencia inconexas

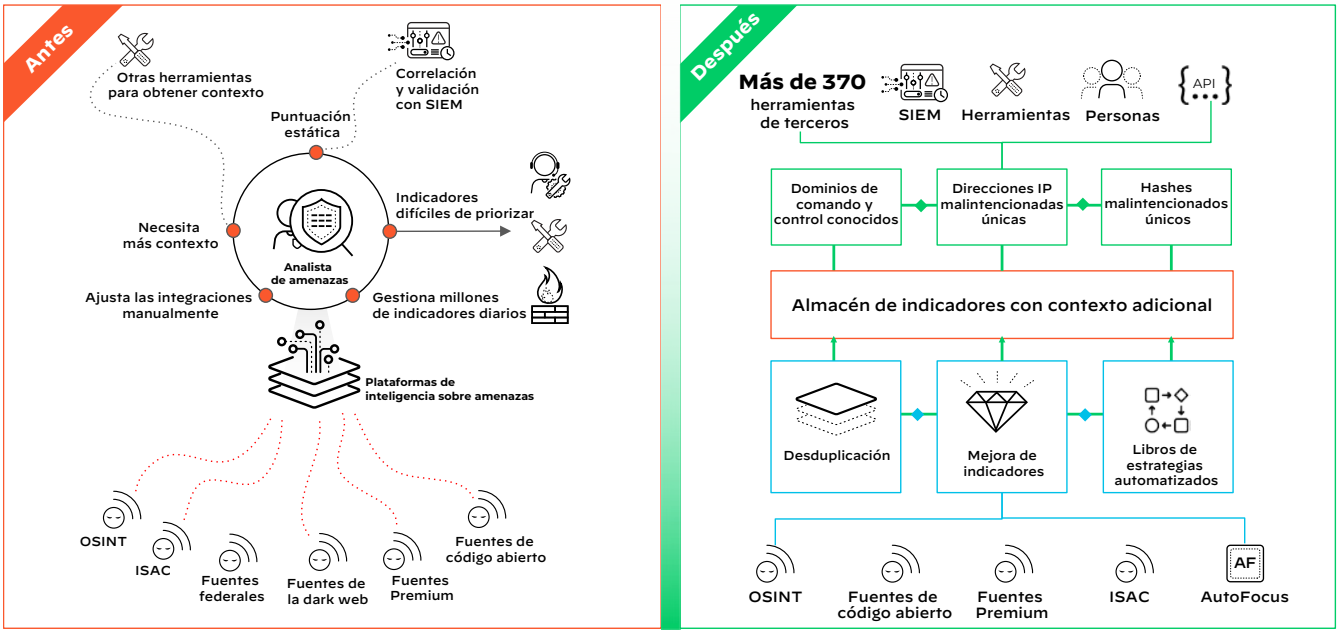

Figura 10: Gestión de la inteligencia: antes y después de Cortex XSOAR

Figura 11: Las ventajas de Cortex XSOAR para el SOC

Cortex XSOAR cubre un amplio catálogo de casos de uso

La plataforma Cortex XSOAR es abierta y ampliable, por lo que puede aplicarse en una gama de casos de uso muy diversa, incluso en procesos fuera del ámbito del SOC o del equipo encargado de responder a incidentes de seguridad. Los casos de uso más habituales se encuentran las técnicas de *phishing*, las operaciones de seguridad, la gestión de alertas de incidentes, la orquestación de la seguridad en la nube, la gestión de vulnerabilidades y la búsqueda de amenazas.

El futuro de las plataformas SOAR está abocado a incluir algún sistema de gestión de inteligencia sobre amenazas nativo que permita a los equipos acabar con la separación entre las operaciones de seguridad y la inteligencia sobre amenazas. Cuando todo ello se reúne en una misma plataforma, los analistas del SOC, los responsables de responder a los incidentes y los equipos de inteligencia sobre amenazas pueden aunar esfuerzos para combatir juntos a los adversarios avanzados, gracias a la optimización de la comunicación, de la eficiencia y del acceso a la información.

Cortex XSOAR redefine la orquestación, la automatización y la respuesta con la primera plataforma SOAR ampliada del sector en incluir automatización, orquestación, colaboración en tiempo real, gestión de casos y gestión de inteligencia sobre amenazas. Los equipos de seguridad tienen en sus manos todo lo que necesitan para seguir la pista a los atacantes y detenerlos, ahora y en el futuro.

Visite nuestro sitio web para obtener más información sobre Cortex XSOAR.

paloalto NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE, Ámsterdam, Países Bajos

Tel.: +31 20 888 1883
www.paloaltonetworks.es