securonix

FICHA TÉCNICA

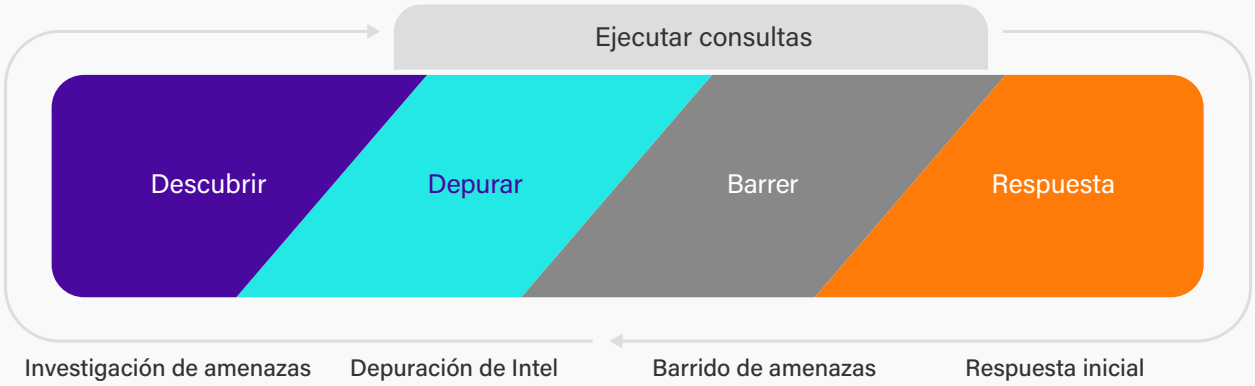
Autonomous Threat Sweeper

Automatice los avisos de amenazas y la detección *post-hoc* para obtener una respuesta cibernética rápida

Proteja su SOC

Los equipos de seguridad están bajo una enorme presión porque tienen que seguir el ritmo de las veloces amenazas nuevas y emergentes. Como los ciberataques siguen aumentando en amplitud y escala, las organizaciones necesitan soluciones autónomas que puedan evaluar la exposición a las amenazas emergentes de forma continua.

Aprovechando las últimas investigaciones y el contenido de amenazas de Securonix Threat Labs, el Autonomous Threat Sweeper (ATS), o barredor autónomo de amenazas, codifica muchos de los aspectos manuales de la investigación. Nuestra solución actúa como una protección para su equipo de seguridad al automatizar el proceso de evaluación de su exposición e iniciar la respuesta a los incidentes.



ATS le ayuda a detectar las amenazas desconocidas que están presentes en su entorno con una inteligencia depurada de amenazas, y la investigación e ingeniería de detección automatizada.

Los beneficios de ATS

Adelántese a las amenazas emergentes y en desarrollo

Permita que su equipo priorice las amenazas de alto riesgo con una inteligencia continuamente depurada de amenazas. ATS actúa como una extensión de su SOC con búsquedas retroactivas en grandes volúmenes de registros y marcos temporales históricos.

Conozca rápidamente su exposición

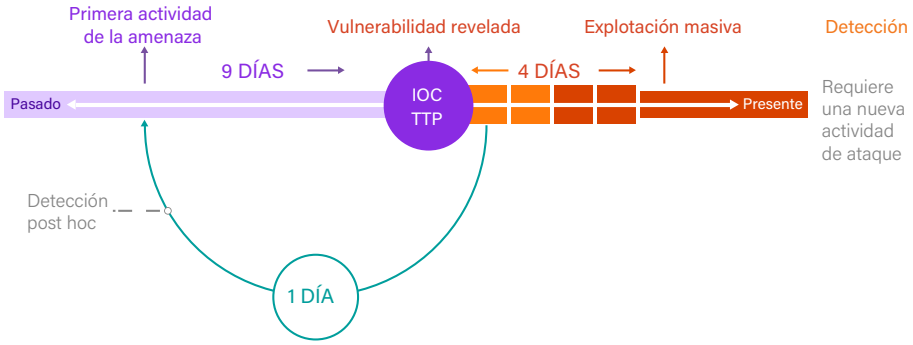
Conozca rápidamente su exposición a las amenazas emergentes con la detección centrada en ataques IOC y basada en TTP. ATS mejora su SIEM (gestión de eventos e información de seguridad) con la capacidad de detectar amenazas bajas y lentas a través de la detección *post-hoc* de los IOC y TTP, extraídos y codificados por Securonix Threat Labs.

Acelere la respuesta cibernética rápida

Acelere la respuesta cibernética rápida con los informes y las alertas automatizados, además de la creación de incidentes. Mediante el monitoreo continuo de su entorno y la depuración de la inteligencia de amenazas emergentes, ATS ayuda a los equipos de seguridad a reducir el tiempo medio de respuesta (MTTR) y a priorizar las amenazas cruciales.

Desbloquee la eficiencia del SOC con el Autonomous Threat Sweeper

El sólido conjunto de funciones de ATS permite a los equipos de seguridad deshacerse de muchas tareas de investigación diarias para que puedan centrarse en las amenazas que más importan.



Avisos de amenazas depuradas

Sepa cuándo hay amenazas con los informes y el contenido de amenazas actualizados.

Inteligencia sobre amenazas: Obtenga contenido de amenazas actualizado y depurado por los expertos de nuestro equipo de Threat Labs.

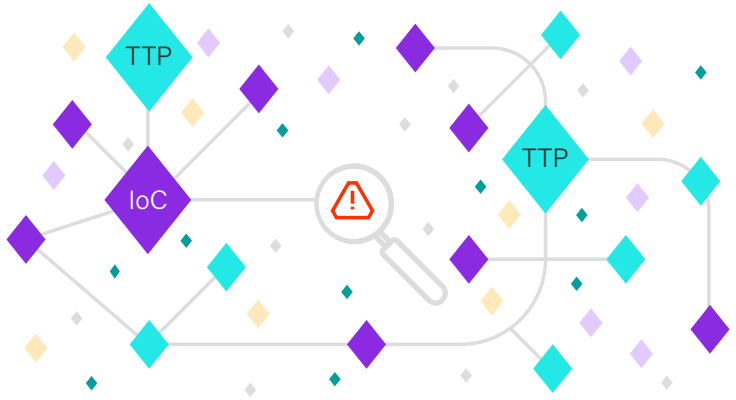
Informes de reconocimiento de amenazas: Reciba una notificación inmediata cuando aparezcan amenazas emergentes y cruciales en su entorno.

Modo de detección multivectorial

Aproveche las múltiples metodologías de detección para descubrir tanto los indicadores de compromiso que "sabemos que conocemos" como los indicadores de acción que "sabemos que no conocemos" derivados de los TTP.

Modo de detección de IOC: Extrae los Indicadores de compromiso (IOC) de la inteligencia de amenazas para buscar amenazas emergentes ocultas en sus datos históricos a largo plazo.

Modo de detección de TTP: Analiza los Procedimientos, tácticas y técnicas (TTP) ayudando a los buscadores de amenazas a identificar los indicadores de acción en caso de no haber conocimiento previo sobre los IOC.



Informes y alertas avanzadas

ATS alerta a su equipo de seguridad y proporciona informes completos, la creación automatizada de incidentes y una orientación práctica para la reparación.

Automatización: ATS acelera la detección y la respuesta mediante la ejecución de búsquedas y consultas para barrer automáticamente su entorno en busca de signos de compromiso en los datos actuales e históricos.

Orientación práctica: Obtenga conclusiones detalladas y orientación para la reparación si se detectan IOC y TTP en su entorno.

Para obtener más información sobre el Securonix ATS, programe una demostración en www.securonix.com/request-a-demo

securonix