# Anomali ThreatStream

## Obtenga visibilidad de sus adversarios

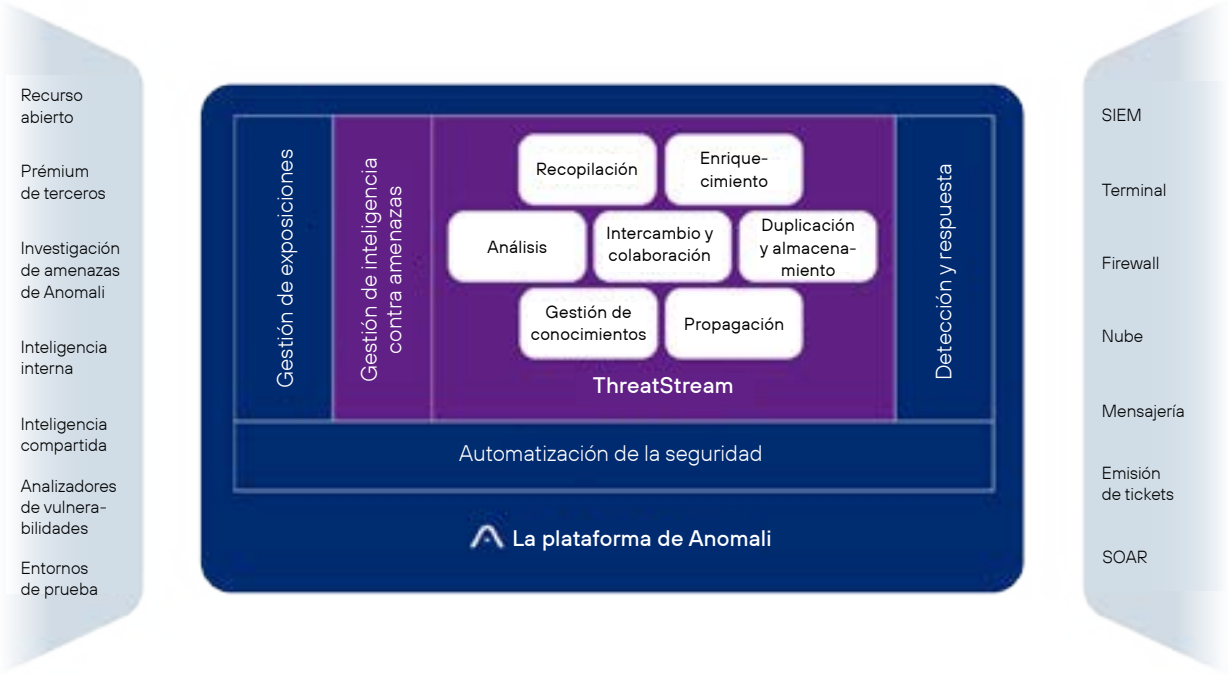
A medida que los delitos informáticos se intensifican, los equipos de seguridad enfrentan el desafío de gestionar grandes cantidades de datos sobre amenazas, identificar y priorizar las amenazas más relevantes e introducir esa información en controles y flujos de trabajo de seguridad, además de hacerlo rápido, antes de que los atacantes tengan la oportunidad de actuar.

Anomali ThreatStream transforma los datos sin procesar en inteligencia e información útil sobre amenazas para que pueda tomar decisiones informadas, responder con rapidez y bloquear las amenazas en tiempo real.

La inteligencia contra amenazas proveniente de cientos de fuentes diversas se organiza, centraliza y enriquece para proporcionar contexto a las alertas e investigaciones del centro de operaciones de seguridad (Security Operations Center, SOC). La inteligencia relevante se distribuye de forma automática a través de sus controles de seguridad existentes para detener las filtraciones y fortalecer la superficie de ataque. Un banco de trabajo de investigaciones integrado profundiza la información y acelera la investigación de amenazas.

## BENEFICIOS

- Elimina obstáculos para centrarse en las amenazas emergentes relevantes
- Reduce el riesgo con la distribución automatizada de inteligencia a sus controles de seguridad
- Mejora la productividad del equipo de seguridad y la eficiencia operativa
- Investiga y se centra en amenazas, TTP y actores
- Distribuye inteligencia de amenazas legible por máquinas en todo su sistema de seguridad
- Encuentra y evalúa con rapidez las fuentes de amenazas de terceros, la inteligencia y las herramientas
- Colabora y comparte amenazas de forma segura en todas las comunidades de confianza



Al conectar la plataforma de operaciones de seguridad de Anomali con la comunidad global de investigadores de seguridad informática, ThreatStream pone al alcance de su mano el mayor repositorio de inteligencia completa del mundo. Los datos de alta calidad ayudan a los equipos a investigar eventos de seguridad y evaluar amenazas en tiempo real. La inteligencia de ThreatStream, filtrada para aumentar su relevancia e incorporada en Anomali Match, se puede correlacionar de forma automática con las vulnerabilidades de su propio entorno para permitir operaciones de seguridad basadas en análisis.

## Transforme los datos sin procesar sobre amenazas en visibilidad y conocimiento

Al ser una plataforma de gestión de inteligencia contra amenazas de alto rendimiento, ThreatStream recopila y enriquece datos sin procesar de cientos de fuentes diversas de inteligencia de amenazas, incluidas las fuentes exclusivas de Anomali Labs, fuentes de inteligencia de código abierto (Open Source Intelligence, OSINT), fuentes prémium especializadas y centros de análisis e intercambio de información (Information Sharing and Analysis Centers, ISAC). Los paneles en tiempo real y la inteligencia de amenazas legible por máquinas ayudan a los equipos de seguridad a trabajar de manera rápida y eficaz para evaluar, priorizar y detener las amenazas de forma proactiva.

### Capture todos los datos relevantes sobre amenazas globales

La recopilación, el tratamiento y el enriquecimiento automatizados de inteligencia ayudan a los equipos de seguridad a comprender con rapidez el contexto de las alertas de gestión de información y eventos de seguridad (Security Information and Event Management, SIEM) y de orquestación, automatización y respuesta de seguridad (Security Orchestration, Automation and Response, SOAR) con análisis de actores, campañas, incidentes, malware, firmas, vulnerabilidades, indicadores de compromiso (IOC), indicadores de ataque (IOA) y tácticas, técnicas y procedimientos (TTP) de los atacantes.

Para garantizar la relevancia y la calidad a la vez que se reducen los obstáculos, la inteligencia de amenazas se correlaciona con su industria, sector, tecnología y geografía, y se elimina la información duplicada, desactualizada e inexacta. Las fuentes de amenazas de terceros, los enriquecimientos y las herramientas se pueden clasificar y licenciar con facilidad en un mercado integrado de inteligencia de amenazas para mejorar y personalizar sus recursos de inteligencia de amenazas.

### Obtenga visibilidad y conocimiento de las amenazas relevantes

Las fuentes de inteligencia de amenazas se evalúan y optimizan en función de la calidad y la relevancia para su organización, y las amenazas individuales se califican según su confianza y gravedad mediante un potente algoritmo de aprendizaje automático (Machine Learning, ML). Los paneles proporcionan una visibilidad instantánea de las métricas clave de todos sus datos sobre amenazas, y las poderosas herramientas de generación de informes le ayudan a compartir inteligencia con el nivel de detalle adecuado para las distintas partes interesadas.

### Ofrezca inteligencia operacional de amenazas en todos sus controles de seguridad

ThreatStream, desarrollado en una plataforma extensible con la interfaz de programación de aplicaciones (Application Programming Interface, API) y el kit de desarrollo de software (Software Development Kit, SDK) adecuados, permite la integración lista para usar con los principales controles de seguridad empresarial, incluido SIEM, firewall, EDR y SOAR, tanto para la incorporación de datos entrantes como para la organización de respuestas salientes. El bloqueo y el monitoreo automatizados y en tiempo real permiten una rápida respuesta a los posibles ataques.

### Acelere las investigaciones

Una plataforma integrada y un banco de trabajo de investigaciones para el análisis y la publicación de inteligencia finalizada por analistas aceleran los conocimientos. La aplicación de ATT&CK de MITRE proporciona una visión inmediata de las amenazas globales que afectan la postura de seguridad de su organización, con una investigación de análisis de enlaces visuales para expandirse desde el indicador hasta los modelos de amenazas asociados de alto nivel. Un entorno de prueba integrado permite la detección de archivos sospechosos para su investigación.

### Distribuya y colabore con inteligencia de alta calidad

Utilizada por más de 2000 organizaciones, ThreatStream Trusted Circles permite la visibilidad e identificación de amenazas, la respuesta rápida y segura y la colaboración continua de inteligencia con los pares de la industria. Dentro de su organización, las herramientas de generación de informes y publicación facilitan la distribución de boletines de amenazas y otros productos de inteligencia finalizada a las partes interesadas con el nivel de detalle deseado.

## Casos de uso clave

### Supervisar el panorama de amenazas

Conozca a sus adversarios con visibilidad y análisis de los actores, campañas, incidentes, malware, firmas, TTP y vulnerabilidades relevantes

### Automatizar y administrar el ciclo de vida de la inteligencia

Permita la recopilación, el tratamiento, la integración, el análisis y la publicación rápida y eficiente de la inteligencia contra amenazas

### Mejorar la eficacia del control de la seguridad

Automatice la distribución de inteligencia en tiempo real para bloquear y supervisar de forma proactiva

### Enriquecer los flujos de trabajo de SecOps

Acelere la evaluación y la respuesta a incidentes con información de los atacantes, los TTP, los flujos de ataque y los observables relacionados

### Posibilitar la colaboración

Colabore de forma segura con colegas internos y pares de organizaciones similares para acelerar la identificación de amenazas y obtener asesoramiento para ayudar a gestionarlas

© Copyright 2023 Anomali®. Todos los derechos reservados.
ThreatStream® es una marca registrada de Anomali Inc.
Anomali Match™ ("Match") y Anomali Lens ("Lens") son marcas comerciales de Anomali Inc.

ANOMALI