Anomali Match

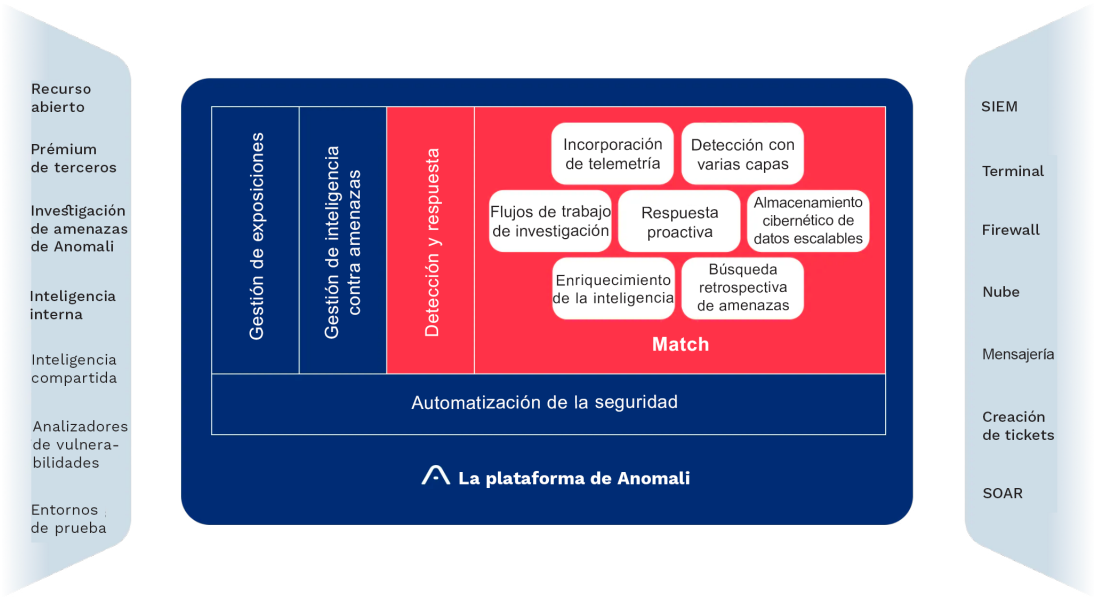
BENEFICIOS

- **Monitoreo en tiempo real:** recopile, almacene, analice e informe de forma continua los datos de registro para detectar amenazas en tiempo real y responder a los incidentes.
- **Protege, investiga, visualiza:** el motor de analítica profundiza en los registros de seguridad, saca a la luz patrones y convierte datos de seguridad sin procesar en información procesable.
- **Análisis forense retrospectivo:** si se produce una filtración, los datos históricos recopilados y almacenados por la plataforma de Anomali pueden impulsar el análisis forense y la investigación del incidente de seguridad.
- **Respuesta automatizada a los incidentes:** ofrezca respuestas automatizadas a tipos específicos de incidentes, lo que reduce el trabajo manual necesario para responder a ellos.
- **Reducción de falsos positivos:** a través de las reglas de correlación inteligentes y los algoritmos de aprendizaje automático, reduzca de forma significativa la cantidad de alertas de seguridad de falsos positivos, lo que libera el tiempo de los analistas.
- **Rentable:** almacene registros de seguridad de años por una fracción del costo y reduzca el espacio operativo para gestionar y asegurar su infraestructura.

Los equipos de seguridad con frecuencia enfrentan desafíos a la hora de identificar "puntos ciegos" en su infraestructura de TI, así como el uso y la interacción de los empleados y socios con estos sistemas, lo que da como resultado una visibilidad limitada de los activos fundamentales. Adquirir visibilidad puede ser costoso debido a la dependencia en soluciones anticuadas de gestión de eventos e incidentes de seguridad que no ofrecen una gestión rentable de los datos de telemetría en todos los controles de seguridad. Esto obstaculiza la capacidad de retener datos durante períodos prolongados y obliga a buscar un equilibrio entre la eficacia y el costo de la seguridad. Además, la información almacenada a menudo carece del contexto necesario para tomar medidas factibles de manera oportuna.

Security Analytics de Anomali Match recopila telemetría de seguridad de diversos controles de seguridad, como terminales, firewall, plataformas en la nube, proxies y el sistema de nombres de dominio (Domain Name System, DNS). Estos datos se almacenan en un lago de datos escalable y nativo de la nube, lo que garantiza un almacenamiento eficiente y una reducción significativa de los costos. El motor Security Analytics de Match utiliza varias capas de detección para identificar amenazas en tiempo real y realizar búsquedas retrospectivas en petabytes de datos en cuestión de segundos. Estas capas de detección abarcan miles de millones de indicadores de compromiso (Indicator of Compromise, IoC), reglas de comportamiento o indicadores de ataque (Indicators of Attack, IoA) y algoritmos de generación de dominios (Domain Generation Algorithm, DGA). Para proporcionar información valiosa a los analistas, las detecciones se contextualizan con inteligencia seleccionada a conciencia sobre los atacantes y sus tácticas, técnicas y procedimientos (Tactics, Techniques and Procedures, TTP). Esta información proporciona a los analistas no solo alertas, sino también conocimientos sobre los adversarios y flujos de ataque, lo que les permite prever y defender de forma proactiva los pasos posteriores. Esta capacidad de Security Analytics de Match se ve reforzada por la inteligencia artificial (IA) y la automatización, lo que simplifica y acelera los flujos de trabajo de los analistas a través de funciones como la búsqueda en lenguaje natural, la calificación y el enriquecimiento automatizados, las integraciones de flujo de trabajo y más.

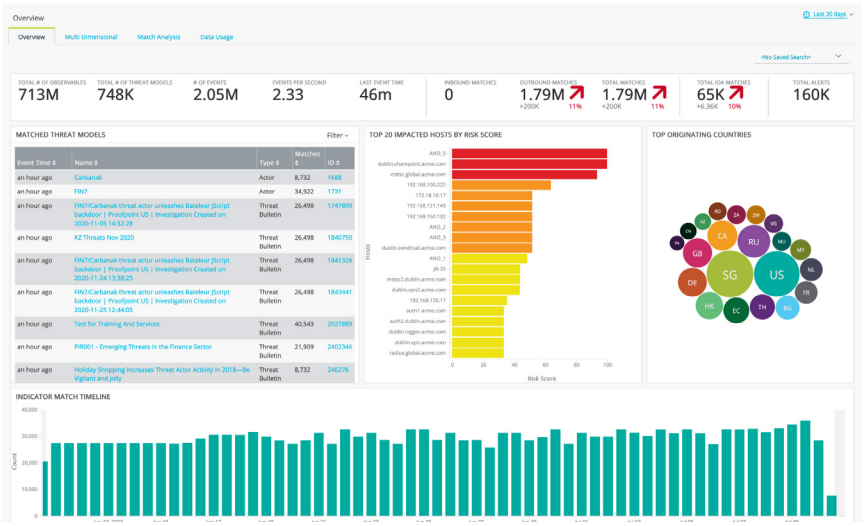
Security Analytics de Anomali Match ofrece una visibilidad completa a escala y rendimiento con información contextual para impulsar la toma de decisiones en tiempo real. Anomali Match permite a los clientes hacer más con menos.



Amplíe y actúe su visibilidad e impulse el enriquecimiento y la respuesta automatizados con Security Analytics potenciado con IA

Capacidades clave

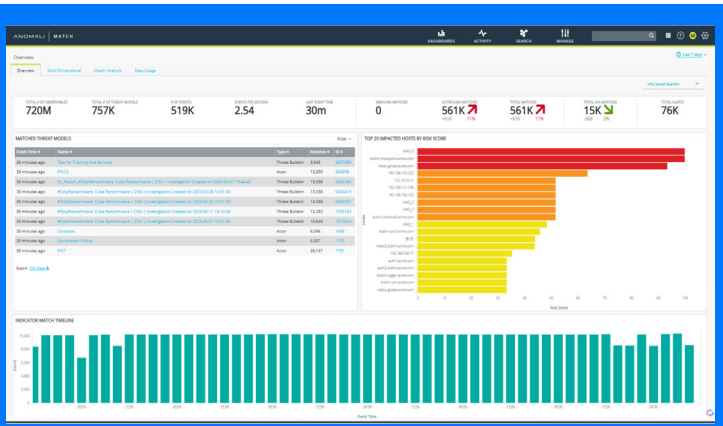
- **Detección automática de amenazas:** detecte amenazas con la detección de varias capas impulsada por indicadores de comprometimiento (IoC), detección de comportamiento o indicadores de ataque (IoA) y algoritmos de generación de dominio (DGA).
- **Agregado de registros:** incorpore la telemetría de todos sus controles de seguridad. Almacene años de datos para el cumplimiento de normas o casos de uso de seguridad.
- **Motor de analítica de Anomali:** busque a través de petabytes de datos a escala y cree paneles, visualizaciones e información procesable.
- **Lago de datos escalable:** almacene años de datos por una fracción del costo y obtenga información oportuna y retrospectiva para los eventos fundamentales.
- **Análisis avanzado:** investigue eventos de seguridad, analice el cumplimiento o traduzca la telemetría de seguridad en riesgo comercial. La plataforma de Anomali permite a los clientes buscar y analizar en segundos, lo que ofrece más de 140 millones de registros en menos de 45 segundos o ejecutar análisis simultáneos en tiempo real a una escala 10 veces mayor a la del mercado actual. Hágalo todo en lenguaje sencillo.
- **Análisis de comportamiento:** identifique anomalías de comportamiento con indicadores de ataque exclusivos para mantenerse un paso adelante del adversario.
- **Algoritmo de generación de dominio:** anticípese los dominios de comando y control maliciosos mediante DGA.
- **Flujos de trabajo de investigación:** enriquezca y acelere los flujos de trabajo de investigación y las alertas de acción con un banco de trabajo de investigación interactivo.
- **Enriquecimiento de alertas:** informe la priorización de alertas y las acciones de respuesta con información sobre actores, campañas, TTP y más.
- **Búsqueda de amenazas:** potencie la búsqueda de amenazas basada en hipótesis con información de los adversarios. Busque grandes cantidades de datos. Pase de boletines de amenazas a la acción en segundos con el poder de la IA.
- **Potenciado con GPT:** mejore la experiencia de los analistas con el poder de la IA generativa. Genere resúmenes e informes para los ejecutivos sobre amenazas e incidentes potenciados con el transformador generativo preentrenado (Generative Pretrained Transformer, GPT).
- **Automatización de las respuestas:** anticípese a los próximos pasos del atacante y defienda de forma proactiva los flujos de trabajo de respuesta integrados con Anomali Integrator. O bien, integre la respuesta con la orquestación, automatización y respuesta de seguridad (Security Orchestration, Automation and Response, SOAR) preferida.



Personalice su panel, conozca las principales amenazas activas, identifique los activos en riesgo y mucho más

Casos de uso

- **Detección precisa de ataques:** identifique las filtraciones con alta precisión mediante el mayor repositorio de inteligencia exclusivo con información sobre los indicadores de ataque y el comportamiento del atacante.
- **Cumplimiento:** sume años de registros de manera escalable y rentable, y facilite las búsquedas para alcanzar sus objetivos de cumplimiento.
- **Análisis de seguridad avanzado:** investigue eventos de seguridad, busque a través de petabytes de datos mediante lenguaje natural, enriquezca eventos de seguridad con información de inteligencia para hacerlos viables y traduzca la telemetría de seguridad en riesgo empresarial.
- **Investigaciones enriquecidas:** priorice las alertas y realice un seguimiento rápido de los incidentes críticos con información del atacante y contexto de la filtración.
- **Respuesta a incidentes informada y automatizada:** conozca al adversario, anticípese a sus próximos pasos y detenga el impacto de la filtración. Acelere y automatice las respuestas con flujos de trabajo integrados en todos los controles de seguridad o integre su SOAR.
- **Búsqueda de amenazas acelerada:** lleve el poder de sus datos al alcance de su mano. Almacene y busque años de telemetría de seguridad por una fracción del costo. Aproveche el poder de la IA para pasar de boletines a búsquedas en cuestión de segundos.
- **Flujos de trabajo de seguridad colaborativos:** rompa las barreras y asóciese con grupos de pares para acelerar el tiempo de detección y respuesta. Comparta información sobre amenazas y riesgos con sus pares y ejecutivos, incorpore datos de distintas fuentes y adapte la seguridad con las necesidades de la empresa.



Busque petabytes de datos de años atrás en cuestión de segundos con un lenguaje natural

ANOMALI