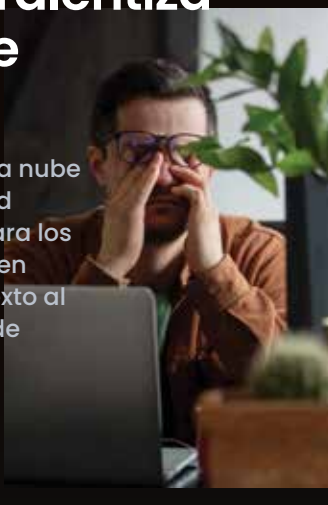
Stream.Security

Investigar con registros lleva tiempo y ralentiza los procesos de remediación



El rápido ritmo de cambio en la nube y el impacto de cada actividad hacen que sea inadecuado para los equipos de seguridad confiar en registros sin formato sin contexto al clasificar e investigar alertas de amenazas.

www.stream.security

El SIEM está diseñado para recopilar registros sin procesar. Cuando se abusa de él para investigar incidentes en la nube, se ralentiza a los equipos de seguridad en tres áreas clave:

- Descalifica tus falsos positivos
- Descubra la explotabilidad de las alertas y el impacto de la alerta
- Revelar toda la historia del ataque

Es hora de que los equipos de seguridad detecten y respondan a la velocidad de la nube.

El crecimiento de la Detección y Respuesta en La Nube

CDR (Detección y Respuesta en La Nube) se creó para ayudar a los equipos de seguridad a superar el desafío de proteger el panorama fluido de la nube y superar al adversario.

Adiós Registros sin Contexto; ¡Hola *CloudTwin*®!

Stream Security, es lider en CDR!
CloudTwin es un modelo simulativo que mapea todas tus acitvidades, configuraciones e identidades de nube en un gráfico en tiempo real, que revela el impacto de cada actividad en los entornos de nube.

¿Cómo funciona?

Detectar

Identifique anomalías de comportamiento en función de sus patrones de comportamiento únicos y enriquezca las alertas SIEM con su impacto.

Clasificación

correlacione automáticamente todas las actividades relacionadas en función de sus principios compartidos y descubra la explotabilidad y el impacto en función de las propiedades de su entorno en tiempo real

Investigar

utilice una máquina del tiempo de investigación para revelar todas las actividades del adversario en una línea de tiempo basada en gráficos, revelando todos los activos comprometidos e identificando la causa raíz.

Responder

Aproveche los manuales de solución listos para usar y validados según su postura en tiempo real o intégrelos con sus herramientas SOAR existentes para eliminar las amenazas con confianza.

Hear from our customers:

HiBob

Stream.Security significantly shortens cloud security investigation processes and time to root cause"
With Stream analyst time that was previously spent on figuring out resource communication and configuration can now be spent on advanced security research. Freeing up cycles allows for better and faster mitigation and remediation."

Tamir Ronen
CISO

RingCentral

"Stream's platform is extremely powerful not only for investigating the current posture, but also for understanding historical changes and configuration states for our AWS environment. Seeing our posture alongside VPC flow logs accelerates investigations and shows us all the context we need in one place."

Petr Zuzanov
SecOps Architect

SONY CATO NETWORKS TiVo RingCentral
PayU GPO shield. Bancolombia kaltura

Stream.Security

SOC 2 TYPE 2

aws PARTNER