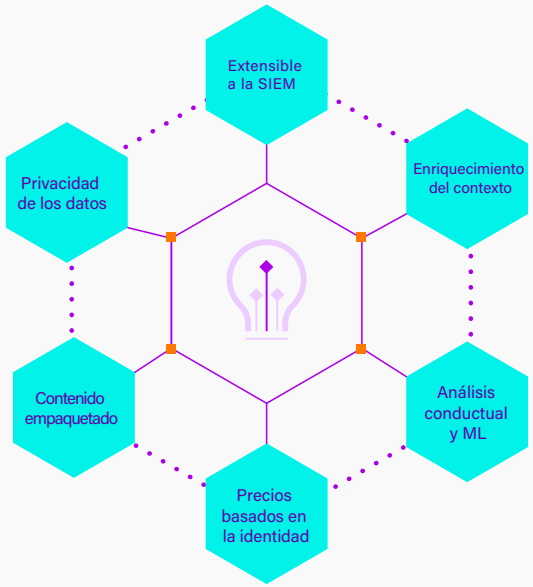
securonix

FICHA TÉCNICA

User and Entity Behavior Analytics

Detecte e investigue las amenazas ocultas en su entorno



Detección de amenazas desconocidas e internas

A medida que los ciberataques se vuelven más complejos, estas amenazas son más difíciles de detectar. Los enfoques tradicionales basados en reglas son ineficaces contra las amenazas avanzadas porque las soluciones basadas en reglas generan miles de alertas falsas.

Securonix UEBA rastrea el comportamiento anómalo de los usuarios, los movimientos laterales sospechosos y las amenazas internas dentro de su organización, ya sea en la nube o en el establecimiento. Su equipo obtendrá un monitoreo en la nube con API integradas para las principales infraestructuras en la nube, así como para muchas aplicaciones empresariales y de seguridad. Además, nuestra solución de UEBA (análisis del comportamiento de usuarios y entidades) reduce el ruido aprovechando las capacidades de aprendizaje automatizado y el contenido listo para usar de casos de uso, para que su equipo pueda centrarse en las alertas de mayor riesgo.

Esté un paso adelante de las amenazas avanzadas e internas

Las amenazas internas son siempre un riesgo, ya sea maliciosas o negligentes. Las soluciones tradicionales de seguridad no tienen la capacidad de identificar los cambios de comportamiento, lo cual dificulta la detección de las amenazas avanzadas e internas. Reaccionan cuando el daño ya está hecho o ni siquiera ven que se ha producido un ataque.

Securonix UEBA le ayuda a mitigar el riesgo de las amenazas internas. Nuestra solución de UEBA adopta un enfoque más proactivo al monitorear los comportamientos de los usuarios y las entidades. Aplica el aprendizaje automatizado y el análisis para asignar puntuaciones de riesgo en función de los patrones de comportamiento de los usuarios. Se marcan los usuarios de alto riesgo para el equipo de seguridad, por lo que los analistas pueden añadirlos a una lista de observación o investigar más a fondo su comportamiento. Securonix UEBA lo alerta sobre los comportamientos, como la exfiltración de datos, el abuso y el mal uso de las cuentas de privilegios, los usuarios comprometidos y las infecciones de botnets.

Reduzca los falsos positivos y el ruido con los análisis de comportamiento

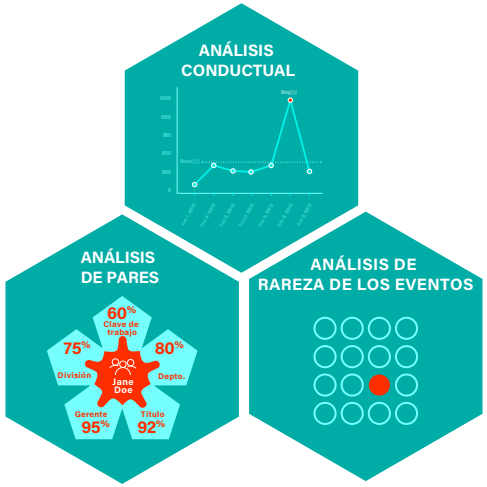
Muchas soluciones de SIEM (gestión de eventos e información de seguridad) generan un mar de falsos positivos que dificultan la identificación de las amenazas reales a tiempo para detener el daño. Con Securonix UEBA, encontrará amenazas complejas con un mínimo de ruido. Nuestra solución ayuda a correlacionar e identificar las amenazas que abarcan varios eventos.

Detecte las amenazas de forma más rápida

Una sola alerta de seguridad sin contexto ni conexión con eventos relacionados no es un método eficiente para detectar amenazas. Obtenga más eficiencia y descubra las amenazas de forma más rápida utilizando los modelos de cadenas de amenazas de Securonix. Nuestros modelos de cadenas de amenazas unen una serie de eventos que están relacionados. En lugar de perseguir varias alarmas por separado, los analistas reciben una sola alarma con todos los eventos relacionados. Sus equipos pueden identificar más rápidamente las amenazas complejas con Securonix.

Utilice análisis avanzados para detectar amenazas sofisticadas e internas

Comprender el comportamiento normal frente al anormal es fundamental para detectar las amenazas internas. Securonix UEBA utiliza cadenas de amenazas y análisis conductual avanzado de aprendizaje automatizado para identificar las amenazas complejas e internas.



Cadenas de amenazas: Reduzca el volumen de alertas uniendo los eventos relacionados para identificar los ataques bajos y lentos. Los modelos de cadenas de amenazas se aplican a los marcos de MITRE ATT&CK y US-CERT.

Análisis conductual: El análisis innovador encuentra rápidamente las amenazas complejas con un mínimo de ruido. Nuestros algoritmos patentados de aprendizaje automatizado lo alertan de las amenazas de varios niveles que se desvían de las líneas de base de comportamiento establecidas.

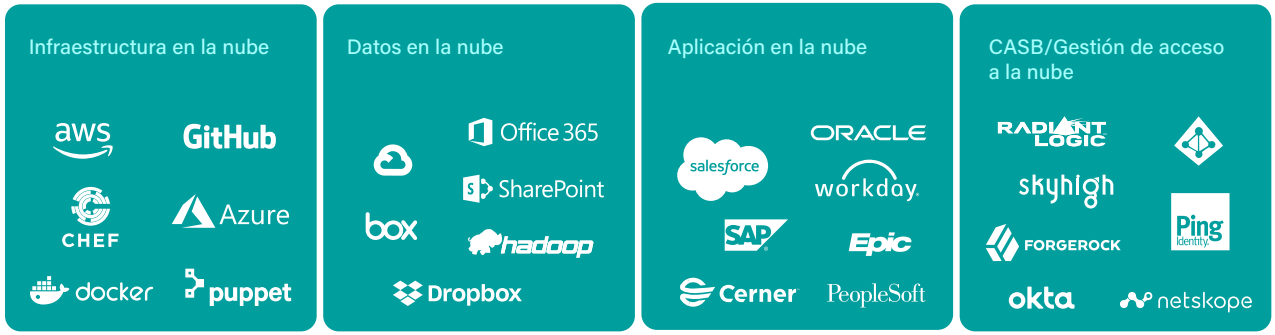
Obtenga un tiempo rápido para demostrar valor

Securonix UEBA es una solución de SaaS (*software* como servicio) que puede implementarse rápidamente, lo cual permite obtener un tiempo más rápido para demostrar valor para la detección y la respuesta. Nuestra solución viene con modelos de amenazas listos para usar, casos de uso preconfigurados y conectores integrados que permiten una rápida implementación y ayudan a sus equipos a identificar rápidamente las amenazas sofisticadas.

Casos de uso preconfigurados: Benefíciese de acceder inmediatamente con un solo clic al contenido para las amenazas internas, el robo de la IP, el fraude y mucho más.

Conectores integrados: Los conectores integrados le permiten investigar las amenazas y responder a ellas de forma rápida, precisa y eficiente dentro de la interfaz de usuario de Securonix. Más de cien conectores incorporados en la nube le permiten procesar datos de una variedad de fuentes a través de su infraestructura híbrida, lo cual le da un panorama completo del riesgo de su organización.

Conectores en la nube



Maximice la rentabilidad (ROI) de su inversión en SIEM

Actualícese sin tener que quitar ni reemplazar su SIEM existente. La pila tecnológica flexible de nuestra solución le permite actualizar fácilmente su solución tradicional añadiendo nuestros análisis UEBA.

SIEM + UEBA: Securonix UEBA se integra perfectamente a cualquier SIEM. Le ayudamos a ahorrar costos en sus inversiones de seguridad existentes sin la necesidad de reemplazar su solución actual.

Nativo en la nube: Nuestra plataforma le permite aprovechar todos los datos de su entorno de TI sin la necesidad de gestionar ninguna infraestructura.

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

securonix