SandaS

Global Security Knowledge
for your Business

Conoce de forma ágil e inmediata qué está ocurriendo en la seguridad informática de tu empresa

Hoy en día las organizaciones se enfrentan a un contexto de amenazas informáticas muy complejo como ataques avanzados persistentes o espionaje industrial, y al mismo tiempo a la necesidad de cumplir con la legislación y regulaciones en materia de seguridad.

SandaS te ofrece un nuevo enfoque en la gestión externalizada de la seguridad de tu empresa. Su tecnología te ayudará a gestionar de manera global la seguridad de la información de tu empresa desde un punto de vista táctico y operacional.

Innovación
Detección avanzada de incidentes de seguridad gracias a la combinación de información interna y externa.

Inteligencia
Algoritmos de inteligencia que detectan incidentes de seguridad desapercibidos para los SIEMs.

Detección colaborativa
Agrega múltiples fuentes internas y externas de datos, adquiriendo información de Internet y el mundo físico.

Solución integral
Análisis, categorización, notificación y respuesta inmediata a los incidentes de seguridad de la información.

Tiempo real
Visualización en tiempo real de la información de las incidencias y alertas detectadas.

Beneficios

- Mejora el tiempo de resolución de incidencias y mitigación de su impacto gracias a la respuesta automática.
- Detección avanzada frente a otras soluciones del mercado gracias a la combinación de múltiples fuentes de información tanto internas como externas.
- Mayor eficiencia en la gestión gracias a la información en tiempo real ajustando las notificaciones relevantes a las personas indicadas para cada incidencia.
- Su inmediatez aporta una visualización en tiempo real de toda la información: incidencias y alertas, indicadores y niveles de servicio y cuadros de mando configurables.

¿A quién va destinado?

- Empresas que cuentan con una arquitectura TI y necesitan gestionar su infraestructura de seguridad.
- Organizaciones que necesitan una gestión a nivel preventivo y en tiempo real mediante la correlación de los eventos de los diferentes entornos y dispositivos.
- Empresas del sector privado y público, que necesitan velar por su seguridad y gestionar adecuadamente el riesgo, cumplir con las políticas internas y las obligaciones que les son impuestas por legisladores, reguladores y clientes.
- Organizaciones que necesitan resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Características técnicas

- Integración con los SIEMs de HP Arcsight, Alienvault e Intel Security para la recolección de alertas y eventos ampliando sus capacidades de correlación avanzada.
- Potente motor de reglas que permite al personal del SOC (Security Operations Center) configurar la categorización, notificación y respuesta a las alertas detectadas.
- Portal web con alertas en tiempo real y cuadros de mando operacionales y configurables para la gestión de incidentes de seguridad.
- API que permite la integración tanto con herramientas de ticketing del SOC como de tu propia organización.