



SandaS

Global Security Knowledge
for your Business

DATA LEAK

Ransomware

MALWARE

Conheça de forma ágil e imediata o que está acontecendo na segurança da sua empresa

Nos dias de hoje, além de enfrentar um contexto de ameaças digitais muito complexo, como ataques avançados persistentes ou espionagem industrial, as organizações enfrentam ainda a necessidade de cumprir com a legislação e regulamentações em questões de segurança.

SandaS oferece-lhe um novo enfoque sobre a gestão terceirizada da segurança da sua empresa. Sua tecnologia o ajudará a administrar globalmente a segurança da informação da sua empresa de um ponto de vista tático e operacional.



Inovação

Deteção avançada de incidentes de segurança graças à correlação entre informação interna e externa.



Inteligência

Algoritmos de inteligência que detectam incidentes de segurança que passam despercebidos para os SIEMs.



Deteção colaborativa

Agrega diversas fontes internas e externas de dados, obtendo informação da Internet e do mundo físico.



Solução completa

Análise, categorização, notificação e resposta imediata aos incidentes de segurança da informação.



Tempo real

Visualização em tempo real da informação dos incidentes e alertas detectados.

Vantagens

- Melhora o tempo de resolução de incidentes e reduz o seu impacto graças à resposta automática.
- Deteção avançada em comparação a outras soluções do mercado graças à combinação de diversas fontes de informação, tanto internas quanto externas.
- Maior e ciência na gestão, graças à informação em tempo real, ajustando as notificações relevantes às pessoas designadas para cada incidente.
- Sua capacidade de pronta resposta proporciona uma visualização em tempo real de toda a informação: incidências e alertas, indicadores e níveis de serviço e painéis de controle configuráveis.

A quem é dirigido

- Empresas que contam com uma arquitetura TI e precisam administrar sua infraestrutura de segurança.
- Organizações que precisam de uma gestão a nível preventivo e em tempo real por meio da correlação dos eventos dos diferentes ambientes e dispositivos.
- Empresas dos setores público e privado que precisam zelar por sua segurança e gerenciar adequadamente o risco, cumprir com as políticas internas e as obrigações que lhes são impostas por legisladores, reguladores e clientes.
- Organizações que precisam resguardar e proteger a informação, procurando manter sua confidencialidade, disponibilidade e integridade.

Características técnicas

- Integração com os SIEMs da HP Arcsight, da AlienVault e da Intel Security para a coleta de alertas e eventos ampliando suas capacidades de correlação avançada.
- Motor de regras potente, que permite ao pessoal do SOC (Security Operations Center) configurar a categorização, notificação e resposta aos alertas detectados.
- Portal web com alertas em tempo real e painéis de controle operacionais e configuráveis para a gestão de incidentes de segurança.
- API que permite a integração tanto com ferramentas de ticketing do SOC quanto com sua própria organização.