Datasheet

Blockbit SIEM & SOAR

SECURITY INFORMATION AND EVENT MANAGEMENT & SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE

Monitoramento Inteligente | **Automação de Segurança** | **Resposta Orquestrada a Ameaças**

O **Blockbit SIEM & SOAR** é uma solução integrada de gerenciamento de eventos e automação de resposta a incidentes, projetada para oferecer detecção avançada, correlação de eventos e mitigação proativa.

Combinando inteligência artificial, machine learning e automação, a solução proporciona visibilidade total da segurança cibernética, acelera a resposta a incidentes e reduz a carga operacional das equipes de SOC.

A integração nativa com o Blockbit Cyber Threat Intelligence (CTI) e o Blockbit Sandbox fortalece ainda mais a detecção e resposta, permitindo análises dinâmicas de arquivos suspeitos e correlação em tempo real com inteligência global. Além disso, os dashboards avançados, como MITRE ATT&CK Framework, MITRE Radar, Attack Map e painéis customizáveis, proporcionam uma visão estratégica sobre táticas e técnicas adversárias, tendências de ameaças e comportamento da rede.

O **Blockbit XDR é compatível com mais de 150 tecnologias de mercado**, permitindo integração abrangente com dispositivos de rede, firewalls, NDR, EDR, XDR, sistemas de identidade e diversas outras soluções de segurança, garantindo visibilidade unificada e resposta coordenada em todo o ecossistema de segurança da organização.

Diferenciais da Solução:

Detecção Inteligente de Ameaças
Correlação avançada de eventos e análise comportamental para identificar ataques em tempo real.

Dashboards Avançados
Visibilidade estratégica com MITRE ATT&CK Framework, MITRE Radar, Attack Map e dashboards customizados.

Automação e Orquestração de Resposta
Playbooks automatizados reduzem a necessidade de intervenção manual e aceleram a mitigação.

Análise Comportamental e UEBA
Identificação de atividades suspeitas de usuários e entidades para detectar movimentações laterais e ameaças internas.

Integração com Blockbit CTI
Inteligência global de ameaças, enriquecendo alertas e reduzindo falsos positivos.

Gestão de Incidentes Unificada
Rastreabilidade completa de eventos e auditoria detalhada.

Integração Nativa com Blockbit Sandbox
Análise dinâmica e automatizada de arquivos suspeitos, detectando ameaças desconhecidas e evasivas.

Monitoramento e Conformidade
Relatórios personalizados para atender requisitos de LGPD, GDPR, ISO 27001, PCI-DSS e outras normas.

Integração com Blockbit XDR, NGFW & NDR
Monitoramento e correlação de eventos, aplicação automática de regras de bloqueio, detecção e mitigação de ataques avançados.

Flexibilidade de Implantação
Disponível para ambientes on-premises, nuvem pública, privada ou híbrida.

Principais Funcionalidades

Coleta e Correlação de Eventos (SIEM)

- **Monitoramento Contínuo:**
  Normalização e análise de logs em tempo real a partir de múltiplas fontes, incluindo endpoints, firewalls e serviços em nuvem.

- **Correlação Avançada:**
  Algoritmos inteligentes conectam eventos isolados para identificar padrões de ataque.

- **Detecção Baseada em Comportamento:**
  Machine learning para identificar atividades anômalas e prevenir ataques antes que ocorram.

Orquestração e Resposta Automatizada (SOAR)

- **Playbooks Inteligentes:**
  Automação de ações como bloqueio de acessos, isolamento de dispositivos e notificações automáticas.

- **Automação Multi-Camada:**
  Resposta coordenada entre firewalls, NDR, EDR, XDR, sistemas de identidade e outras ferramentas de segurança.

- **Análise Forense Integrada:**
  Investigação detalhada de incidentes com reconstrução da linha do tempo do ataque.

Análise Dinâmica de Ameaças com Blockbit Sandbox

Detecção Avançada de Malware	Análise Comportamental de Arquivos Suspeitos	Automação de Remediação
Identificação de malware desconhecido, variantes de ransomware e ataques evasivos.	Execução segura de artefatos para identificar ações maliciosas em tempo real.	Integração com SOAR para quarentena de arquivos, bloqueio de IOCs e resposta coordenada.

Inteligência de Ameaças com Blockbit CTI

Correlação Avançada de Dados

Uso de inteligência global para validar ameaças e reduzir falsos positivos.

Atualização Contínua sobre Novas Ameaças

Insights sobre malware, ataques direcionados e vulnerabilidades emergentes.

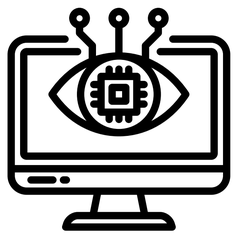
Detecção Preditiva

Identificação de padrões de ataque antes que afetem o ambiente.

Resolução Automatizada

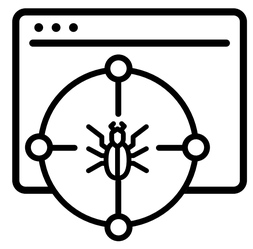
Aplicação de respostas baseadas em inteligência contextualizada para incidentes de alto risco.

Dashboards Avançados e Inteligência Visual



MITRE ATT&CK Framework

Mapeamento das táticas e técnicas utilizadas por adversários cibernéticos.



Threat Hunting

Investigação para identificar padrões de ataque e atividades ocultas às defesas tradicionais.

Attack Map

Monitoramento em tempo real das ameaças ativas e correlação com dado geolocalizados.

Dashboards Customizados

Personalização total dos relatórios e gráficos, adaptados às necessidades do SOC.

Redução de Tempo e Eficiência Operacional

Com automação inteligente, o Blockbit SIEM & SOAR reduz drasticamente o tempo necessário para um SOC 24×7 avançado detectar e mitigar ameaças.

Tarefa	Processo Manual (tempo médio)	Com Blockbit SIEM & SOAR
Enriquecimento de Artefatos (IOCs)	1 hora	3 minutos
Triagem de Eventos	30 minutos	2 minutos
Análise de Arquivos Suspeitos	2 horas	Automaticamente/Imediatamente
Isolamento de Dispositivos Comprometidos	15 minutos	Automaticamente/Imediatamente
Documentação de Incidentes	90 minutos	Automaticamente/Imediatamente
Bloqueio de IOCs em Firewalls	45 minutos	Automaticamente/Imediatamente
Resolução Completa do Incidente	**6 horas**	**5 minutos**

Total: **Redução de até 6 horas para apenas 5 minutos!**

Estas informações são meramente ilustrativas, baseadas em estimativas calculadas pela Blockbit. Cada ambiente e equipe possuem características únicas que podem resultar em variações significativas nos tempos apresentados.

Automação e Orquestração do SOC

A evolução dos ataques cibernéticos e o aumento do perímetro digital nas empresas, exigem SOCs cada vez mais eficientes. No entanto, o alto volume de alertas, a falta de integração entre ferramentas e a ausência de automação comprometem a detecção, investigação e resposta ágil a ameaças.

Triagem Inteligente e Enriquecimento de Alertas:
Redução de falsos positivos com inteligência CTI e correlação avançada de eventos.

Orquestração e Automação Total
Execução automática de playbooks para investigação, isolamento de ameaças e contenção imediata.

Integração com Mais de 150 Soluções
Unificação de ferramentas de segurança, proporcionando uma resposta coordenada e eficiente.

Redução no Tempo de Resolução de Incidentes
De horas para minutos, com automação inteligente e dashboards operacionais completos.

O Blockbit SIEM & SOAR transforma o SOC tradicional em um ambiente altamente eficiente e automatizado, reduzindo a carga operacional e acelerando a mitigação de ameaças. Com integração nativa ao Blockbit CTI, análise comportamental e automação inteligente, ele transforma a segurança cibernética em um ambiente altamente eficiente e resiliente.

- **Menos tempo de resposta com automação inteligente**
- **Detecção avançada e mitigação proativa de ameaças**
- **Visibilidade e correlação de eventos para um SOC moderno**
- **Conformidade e auditoria contínuas para atender normas regulatórias**

Sobre a Blockbit

A **Blockbit** é líder em produtos de cibersegurança, protegendo milhares de empresas e milhões de usuários de ataques e ameaças digitais.

+5M clientes corporativos

+2MM usuários protegidos