SAYCON CONSULTORIA

WAZUH SIEM XDR

Visibilidade completa, detecção avançada e resposta ativa para sua infraestrutura

Monitore, detecte, investigue e responda a ameaças em tempo real com uma plataforma open source poderosa e escalável.

O Wazuh é uma plataforma open source de SIEM e XDR que unifica recursos de monitoramento, detecção de ameaças, resposta a incidentes e conformidade.
Ele coleta e analisa eventos de servidores, estações, aplicações, dispositivos de rede, containers e ambientes em nuvem, proporcionando visibilidade completa e proteção contínua.
Com o Wazuh, sua empresa aumenta a segurança, reduz riscos e atende requisitos de auditoria e conformidade de forma eficiente.

Mais visibilidade.
Mais segurança.
Mais conformidade.
Menos riscos.

- Monitoramento em tempo real
- Inventário de ativos e software
- Correlação e enriquecimento
- Investigação e threat hunting
- Automação com resposta ativa

COMPONENTES DO WAZUH

WAZUH AGENT
Instalado em endpoints, servidores e cloud para coletar logs, eventos, FIM, inventário e muito mais.

WAZUH SERVER
Recebe, decodifica, analisa e correlaciona os eventos, aplica regras, integrações e gera alertas.

WAZUH INDEXER
Armazena e indexa os eventos em tempo real, com alta performance, cluster e retenção.

WAZUH DASHBOARD
Interface web intuitiva para visualizar alertas, relatórios, dashboards, compliance e gerenciar o ambiente.

INTEGRAÇÕES
Integra com Service Desk, SIEMs, EDRs, firewalls, APIs, scripts, webhooks e muito mais.

RECURSOS TÉCNICOS AVANÇADOS

ANÁLISE DE LOGS
Suporte a múltiplas fontes: SO, aplicações, firewalls, bancos, containers, cloud e dispositivos de rede.

DETECÇÃO DE AMEAÇAS
Regras avançadas, comportamento, MITRE ATT&CK e inteligência de ameaças.

INTEGRIDADE DE ARQUIVOS
Monitora alterações em arquivos, diretórios e registro do Windows em tempo real.

VULNERABILIDADES
Inventário automático e avaliação de vulnerabilidades com bases atualizadas e políticas.

CONFIGURAÇÃO E COMPLIANCE
Verifica configurações de segurança, hardening e conformidade com normas como CIS, NIST, PCI DSS.

RESPOSTA ATIVA
Ações automáticas como bloqueio de IP, kill de processo, scripts e isolamento de host.

MALWARE DETECTION
Integração com VirusTotal, YARA, ClamAV e análise de arquivos suspeitos.

MONITORAMENTO DE NUVEM
Coleta via API e agentes em AWS, Azure e GCP com visibilidade completa.

CONTAINERS E KUBERNETES
Visibilidade de eventos, logs e segurança em Docker e Kubernetes.

INVENTÁRIO COMPLETO
Hardware, software, patches, grupos, usuários, serviços e configuração do sistema.

VANTAGENS DO WAZUH EM RELAÇÃO A OUTRAS PLATAFORMAS

OPEN SOURCE
Sem custos de licença por volume, com liberdade e transparência.

BAIXO CUSTO TOTAL
Menor custo de aquisição e operação em comparação a soluções proprietárias.

CONTROLE DOS DADOS
Pode ser instalado on-premises, cloud ou híbrido, com total controle e privacidade.

ESCALÁVEL
Arquitetura preparada para crescer com sua empresa, com alta disponibilidade.

RECURSOS COMPLETOS
SIEM, XDR, FIM, Vulnerabilidades, Compliance, Resposta ativa e Dashboard em uma única plataforma.

COMUNIDADE ATIVA
Comunidade global ativa e documentação completa e atualizada.

INTEGRAÇÃO SEM LIMITES

SIEM · Firewall · Active Directory · E-mail · Service Desk · APIs · Dashboards · Threat Intelligence · Scripts

TRANSFORME DADOS EM PROTEÇÃO

Com o Wazuh, sua empresa tem visibilidade completa, detecção avançada e resposta inteligente para proteger o que realmente importa: seus dados, seus sistemas e seu negócio.

SEGURANÇA INTELIGENTE PARA AMBIENTES MODERNOS COM O PODER DO OPEN SOURCE.

FALE COM A SAYCON CONSULTORIA

IMPLANTAÇÃO • CONSULTORIA • INTEGRAÇÃO • SUPORTE

saycon.com.br | 11 98053-9425 | @sayconconsultoria | SAYCON CONSULTORIA