Guardeon.

O Guardeon. é uma plataforma unificada de defesa cibernética que centraliza, em um único console, o monitoramento de segurança, a detecção de ameaças, a gestão de vulnerabilidades, a resposta a incidentes e a inteligência de ameaças. Construída sobre arquitetura **multi-tenant** e **offline-first**, integra com soluções de tecnologia e fontes externas de inteligência, entregando visibilidade total da postura de segurança em tempo real e com isolamento completo de dados por cliente.

Organizada em quatro módulos integrados, **Monitor, Vulnerabilities, Risk e CTI**. A plataforma transforma o volume de dados de segurança em decisões rápidas, com KPIs executivos, insights priorizados e drill-down investigativo em cada tela.

Guardeon

O núcleo da plataforma — uma só verdade para toda a segurança

Plataforma Unificada

Tudo em um único console

Reúne monitoramento, análise de postura, governança, gestão de risco, compliance, SIEM, gestão de vulnerabilidades e inteligência de ameaças em uma experiência integrada. Acabe com a fragmentação de ferramentas e tenha todas as respostas em um só lugar.

Arquitetura Multi-Tenant

Isolamento total por cliente

Cada tenant opera com banco de dados e cache dedicados, garantindo isolamento completo de dados. O tenant agrega a visão consolidada de todos os clientes para o time global.

Offline-First & Alta Disponibilidade

Funciona mesmo quando a fonte cai

Os dados são sincronizados para um PostgreSQL local e servidos via cache Redis. A plataforma continua operante e responsiva mesmo se as fontes externas ficarem indisponíveis.

Acesso Seguro & Governança

Acesso sob controle, sempre auditado

Autenticação JWT com MFA (TOTP) obrigatório, controle de acesso por papel (RBAC), gestão de sessões e trilha de auditoria completa de todas as ações dos usuários.

Design Mission Control

Decisão em segundos

Cada tela combina KPIs de topo, insights executivos com priorização automática, priority stacks acionáveis e gráficos interativos, do panorama ao detalhe em poucos cliques.

Sincronização Inteligente

Dados sempre atualizados em segundo plano

Agendador de jobs sincroniza agentes, alertas, vulnerabilidades e métricas em intervalos otimizados, com monitoramento de status de sincronização e políticas de retenção de dados.

Guardeon.
By VANELOS

Guardeon Monitor

Operação de segurança em tempo real — o pulso do seu SOC

Frota de Agentes

Visibilidade total dos endpoints

Painel em tempo real do estado dos agentes: ativos, desconectados, nunca conectados e pendentes. Monitora versão, sistema operacional e último keepalive, sinalizando agentes desatualizados e exportando para CSV.

Alertas 24h & Evolução

Enxergue o que está acontecendo agora

Resumo de alertas por severidade nas últimas 24h, detecção de picos, top regras e top agentes, com gráficos de evolução e detecção de tendência.

Cobertura MITRE ATT&CK

Conheça suas lacunas de detecção

Distribuição de detecções por tática e técnica do framework MITRE ATT&CK, percentual de cobertura sobre as 201 técnicas do Enterprise e priorização de gaps nas táticas mais críticas.

Performance do SOC

Meça e prove a eficiência da operação

Indicadores de SOC: MTTA, MTTD e MTTR, taxa de acurácia, alertas tratados, analistas ativos e conformidade frente às metas de SLA, tudo com tendência de 30 dias.

Top Regras & Falsos Positivos

Afine a detecção continuamente

Ranking das regras que mais disparam, correlação com o nível/severidade e identificação automática de candidatos a falso positivo para tuning constante.

Detalhe do Agente

Investigação profunda por ativo

Visão 360° de cada agente: últimos alertas, vulnerabilidades, forense de rede (IPs, portas, protocolos, geolocalização) e técnicas MITRE associadas, em uma linha do tempo de atividades.

Guardeon Vulnerabilities

Gestão e priorização de vulnerabilidades de ponta a ponta

Distribuição CVSS

Entenda o risco em um olhar

Visualização da base de vulnerabilidades por faixa CVSS (crítico, alto, médio e baixo), com histograma por pontuação e drill-down por severidade para investigação imediata.

Top CVEs & Catálogo KEV

Priorize o que realmente importa

Lista dos CVEs mais críticos com pontuação CVSS e ativos afetados, cruzando com o catálogo CISA KEV para sinalizar vulnerabilidades exploradas ativamente.

Ativos Afetados

Saiba onde concentrar esforços

Ranking dos ativos mais vulneráveis, com contagem de vulnerabilidades críticas e altas, informação de SO e risk score por ativo, os endpoints que mais exigem atenção.

Cobertura de Patches

Meça a maturidade da correção

Percentual geral de cobertura de patches frente à meta, divisão por sistema operacional/ativo e rastreamento de ativos críticos ainda sem correção.

Timeline / Burndown

Acompanhe a redução do risco

Gráfico de burndown de vulnerabilidades críticas abertas versus fechadas ao longo do tempo, com linha de previsão e meta de resolução, novas e fechadas nos últimos 7 dias.

SLA de Remediação

Garanta a correção no prazo

Metas de remediação por severidade, percentual de conformidade, status individual de cada vulnerabilidade e priority stack das violações de SLA, com tendência de 30 dias.

Guardeon Risk

Gestão de risco e resposta a incidentes com visão estratégica

Matriz de Risco

Risco traduzido para o negócio

Matriz de probabilidade × impacto com codificação de cores plotando os incidentes por severidade e destacando, em fila prioritária, os de maior risco.

Análise de Causa Raiz

Ataque a origem, não só o sintoma

Agrupamento de incidentes por causa raiz m gráfico, ranking de frequência, severidade dominante por causa, tendência e recomendações de ações preventivas.

Rastreamento de SLA

Resposta dentro do compromisso

Metas de resposta por severidade, status individual e conformidade consolidada com tendência por dias.

MTTR por Categoria

Onde a resposta precisa melhorar

Tempo médio de resposta agrupado por categoria de incidente, com média e percentual, distribuição de severidade e linha de referência da meta, destacando melhores e piores desempenhos.

Guardeon CTI

Inteligência de ameaças cibernéticas — antecipe-se ao ataque

Exposição de Vazamentos

Saiba antes que virem incidente

Busca de e-mails corporativos expostos em vazamentos de dados, com histórico de breaches por usuário, status da exposição e itens de ação como redefinição de senhas.

Campanhas APT

Acompanhe quem está em atividade

Campanhas e intrusion sets ativos com descrição, status, rótulos por setor e vetor, e correlação de IOCs com as detecções internas do ambiente.

Indicadores de Comprometimento (IOCs)

Correlacione o externo com o interno

Catálogo de IOCs (IPs, domínios, hashes, URLs) com classificação, contagem de detecções internas, veredito de reputação e correlação com campanhas conhecidas.

Monitoramento de Domínios

Vigilância contínua de reputação

Watchlist de domínios com verificação de reputação, pontuação de risco, histórico de checagens e detecção de typosquatting, phishing e domínios de comando e controle (C2).

Threat Hunting

Caça proativa às ameaças

Hipóteses de caça ativas associadas a táticas/técnicas MITRE, com responsável, sinais correlacionados, hits e linha do tempo de eventos do palpite à evidência.

Atribuição & Threat Actors

Conheça o adversário

Catálogo de atores de ameaça com aliases, nível de sofisticação, motivação, objetivos e datas de observação, além de um landscape executivo das táticas e setores mais visados.

Implantação & Arquitetura

Nós nos adaptamos à sua infraestrutura

SaaS Multi-Tenant Gerenciado

Nós cuidamos da infraestrutura por você

Plataforma entregue como serviço em nuvem, com provisionamento automatizado de clientes e isolamento total de dados por tenant. Ideal para quem busca segurança de alto nível sem o overhead de operar a infraestrutura.

On-Premises / Self-Hosted

Sua infraestrutura, sob seu controle

Implantação em ambiente via containers Docker e infraestrutura (PostgreSQL e Redis), containers endurecidos e administração total da solução pela sua equipe.

Agentes Multiplataforma

Cobertura de todo o parque

Coleta de telemetria por agentes nativos para Windows, Linux e macOS, com instaladores dedicados para detecção em endpoints e servidores.

Stack Moderna & Escalável

Tecnologia preparada para crescer

Construída para sincronização em segundo plano, cache em duas camadas e arquitetura offline-first que garante desempenho e disponibilidade mesmo sob alta carga.

Guardeon by Vanelos · Plataforma Unificada de Cibersegurança

Fale com a gente: comercial@vanelos.com.br · www.vanelos.com.br