A

ARGOS · NoBug

v1 · 2026

SECURITY · OPERATIONS · 24×7

100 olhos.
Zero pontos cegos.

Argos é o Centro de Comando do SOC NoBug — SIEM aglutinado, IA Alice pra triagem, anti-phishing CloneGuard, playbooks SI e plantão integrado a Twilio.

MULTI-TENANT

IA + SOAR

PRONTO EM HORAS

Apresentação comercial · maio 2026 · NoBug Tecnologia

A O PROBLEMA

Times de SOC operam em silos e perdem o que importa.

Sem aglutinação de SIEM, EDR, ticket, plantão e IA num único contexto, o SOC vira reativo — e cada minuto extra de detecção custa caro.

204 dias

tempo médio para detectar um breach

Verizon DBIR 2024

R$ 4,9 mi

custo médio de um breach no Brasil

IBM Cost of Breach 2024

60%

do tempo do analista trocando de ferramenta

Forrester SOC survey

70%

do ruído eliminável com dedup + supressão

campo · clientes NoBug

A PROPOSTA

Centro de Comando que aglutina o ciclo inteiro.

Argos une SIEM (Wazuh multi-manager), GLPI, Shuffle SOAR, pfSense, Twilio Voice e Claude IA num único painel — operado por NoBug 24×7.

01 **Detecção aglutinada**

4 managers Wazuh + Sysmon + CrowdStrike + Snort + Cloudflare. Dedup via GLPI elimina ~70% do ruído.

02 **Triagem assistida por Alice**

LLM gera hipóteses, queries Wazuh e sugere playbook. Claude Opus com prompt caching, multi-tenant isolado.

03 **Resposta automatizada**

Shuffle dispara bloqueio em pfSense (BR-DF + SP-AZ). CloneGuard derruba phishing P0 automaticamente.

04 **Plantão 24×7 com voz**

8 plantonistas em paralelo, escalation Telegram → Twilio Voice BR/US, TwiML PT-BR com ack DTMF.

05 **Auditoria e governança**

Append-only audit trail em Postgres, relatórios PDF por ciclo, evidências pra LGPD e seguro cyber.

FLUXO

Do evento à resposta validada.

Três etapas, um único painel. Wazuh, GLPI, Shuffle e pfSense convergem em Argos.

01

STEP 01 · DETECTA

Aglutina ruído em sinal

Coleta nativa Wazuh multi-tenant, Sysmon, CrowdStrike, Snort, Cloudflare. Regras de supressão e dedup via GLPI eliminam ~70% do ruído antes do ticket.

02

STEP 02 · INVESTIGA

Alice IA acelera triagem

Cada ticket recebe triagem por LLM (Claude Opus): hipóteses, indicadores, queries sugeridas no Wazuh e link para playbook aplicável.

03

STEP 03 · RESPONDE

SOAR + plantão fecham o loop

Bloqueio automático em pfSense via Shuffle, escalation por Telegram + ligação Twilio pro plantão de turno, com TTS PT-BR e ack DTMF.

CAPACIDADES

Tudo num painel. Nada solto.

Seis módulos integrados. Você navega em um único contexto — sem trocar de janela.

Dashboard SOC

Tickets em Kanban, EPS em tempo real, mapa de origens de ataque, top-noisy hosts e KPIs por SOC (cliente).

Centro de Comando · Globo

Visualização 3D de origens de ataque com arcs animados, HUD live de EPS, conexões e feed de bloqueios.

Alice · IA assistente

Triagem por LLM, sugestão de hipóteses, queries Wazuh e contra-análise. Multi-tenant com isolamento por SOC.

Playbooks SI

Cinco playbooks acionáveis (ransomware, phishing, exfil, brute-force, supply-chain) com checklists e validação por IA.

CloneGuard anti-phishing

Detecta clones (dnstwist + crt.sh + similaridade HTML) e classifica risco P0–P3 com indicadores explicáveis.

Plantão + Voice

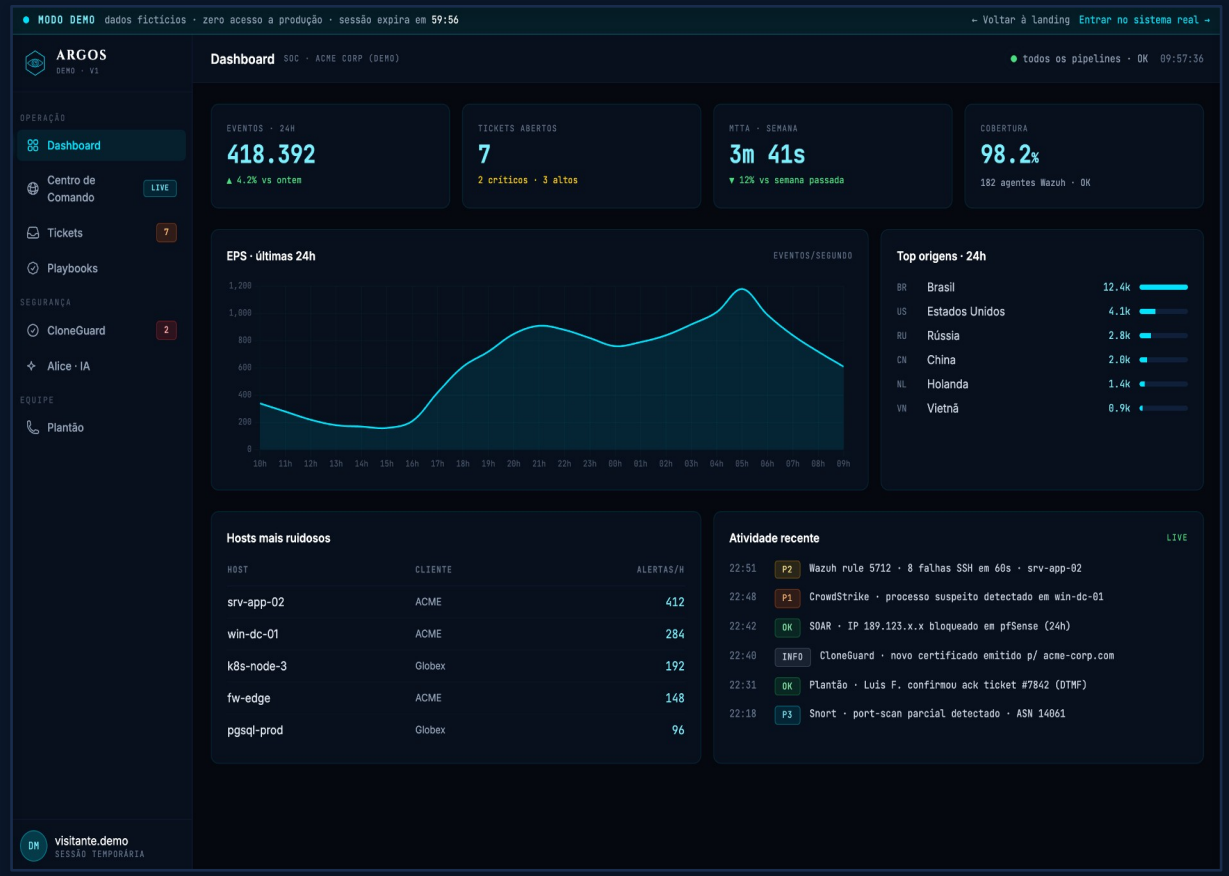
Escala 24/7 com rotação ISO, escalation Telegram → ligação Twilio BR/US, TwiML PT-BR, ack via DTMF.

PRODUTO · OPERAÇÃO

Dashboard SOC.

Visão de turno em tempo real: EPS, top origens, hosts ruidosos, atividade live e KPIs por cliente.

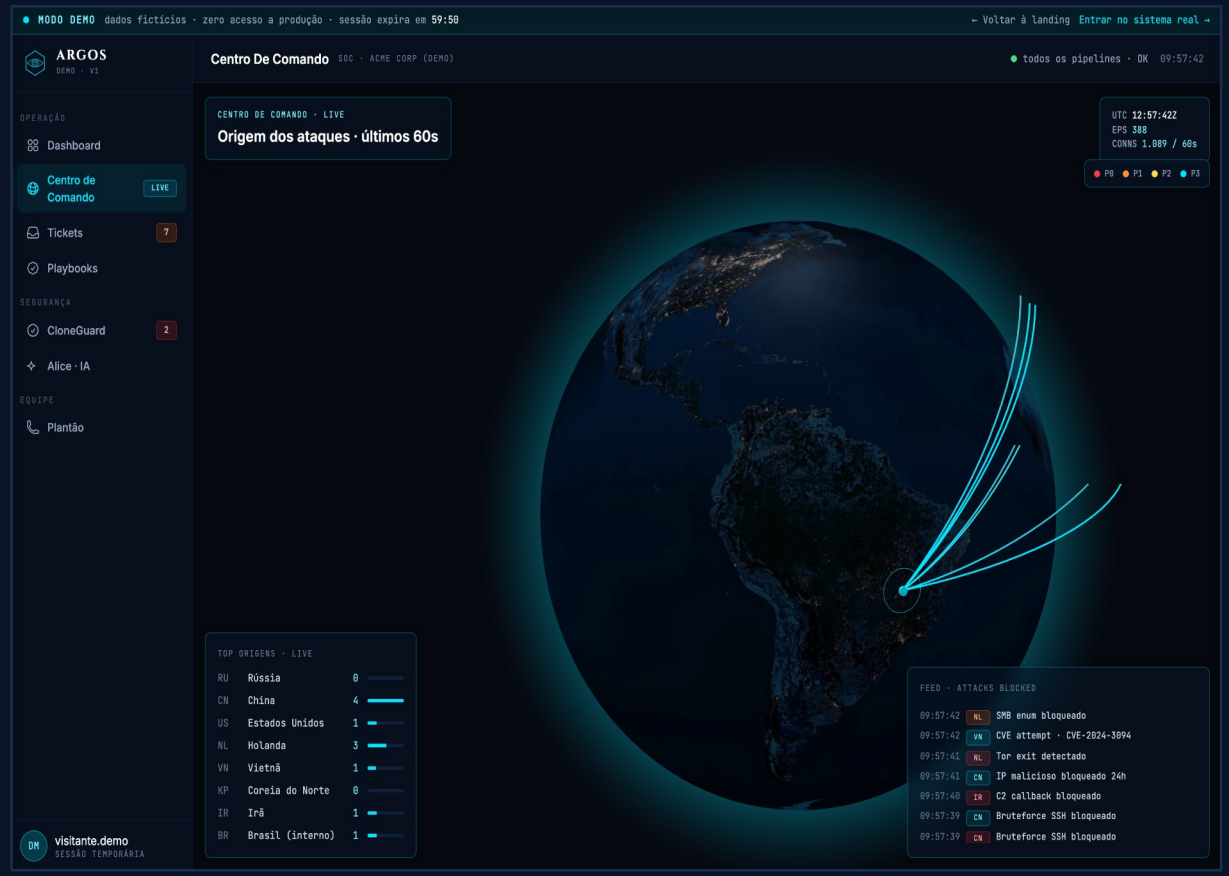
- KPIs em destaque (eventos, tickets, MTTA, cobertura)
- Mapa de origens com geolocalização
- Feed live de alertas críticos
- Multi-tenant: dados isolados por SOC



PRODUTO · OPERAÇÃO

Centro de Comando.

Globo 3D mostra origens de ataque em tempo real com arcs animados, HUD live e feed de bloqueios.

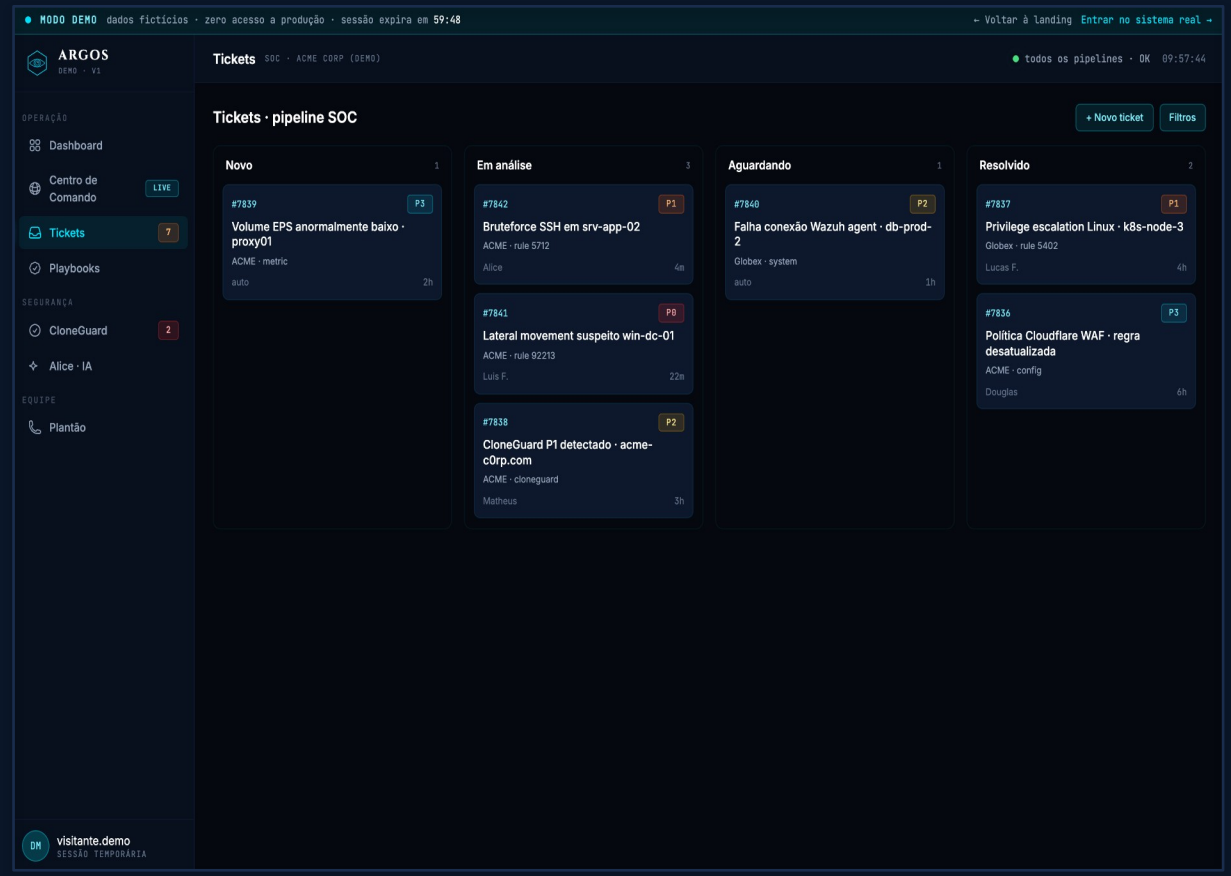


- Visualização imediata de campanhas globais
- HUD com EPS, conexões ativas, UTC live
- Origens classificadas por severidade P0–P3
- Feed de ataques bloqueados nos últimos 60s

PRODUTO · TRIAGEM

Tickets em pipeline Kanban.

Cada incidente flui em Novo → Em análise → Aguardando → Resolvido. Severidade P0–P3, owner e idade visíveis.

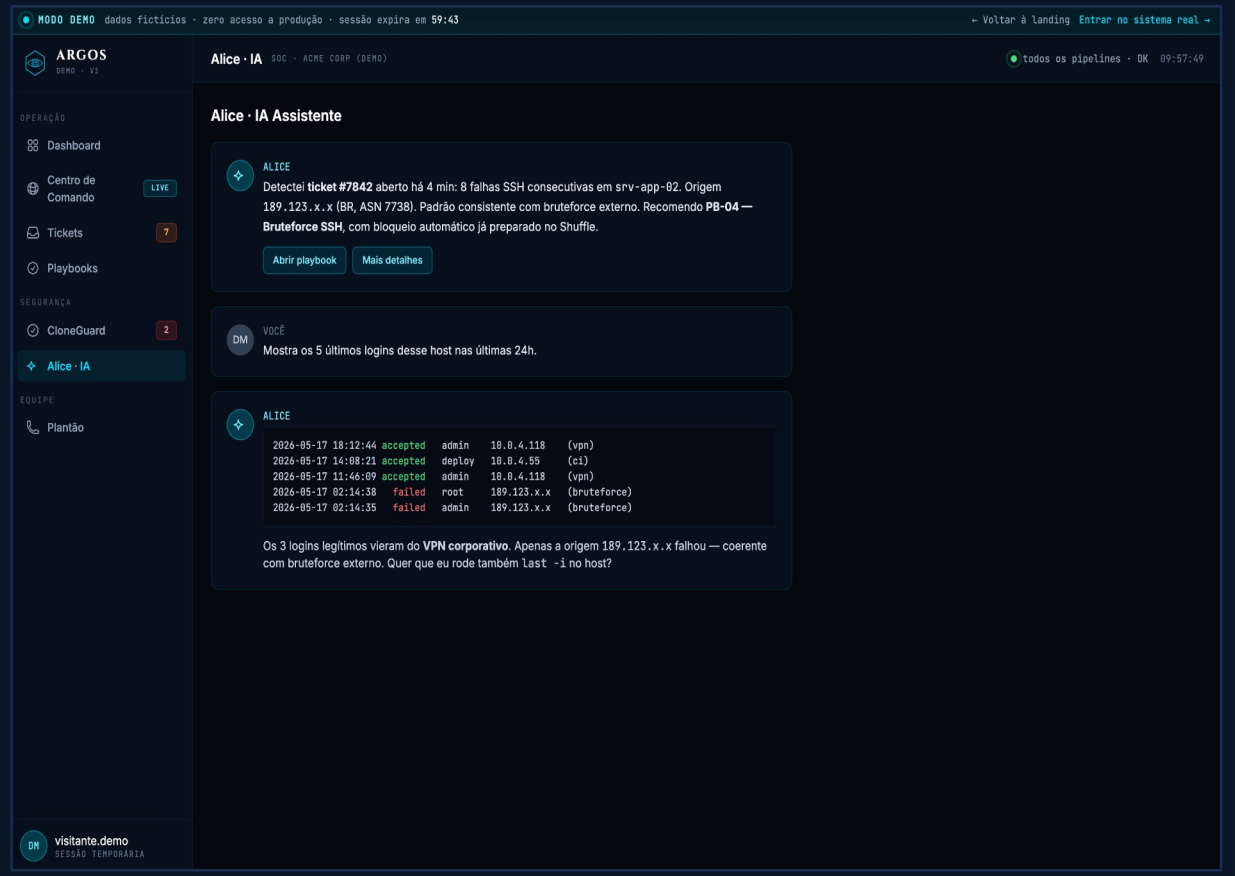


- Dedup automático via GLPI (source-of-truth)
- Severidade calculada por regra Wazuh
- Owner pode ser humano ou Alice
- Drill-down expõe contexto completo

PRODUTO · IA

Alice — assistente de investigação.

Triagem por LLM com hipóteses, indicadores e queries Wazuh sugeridas. Multi-tenant isolado, com audit trail.

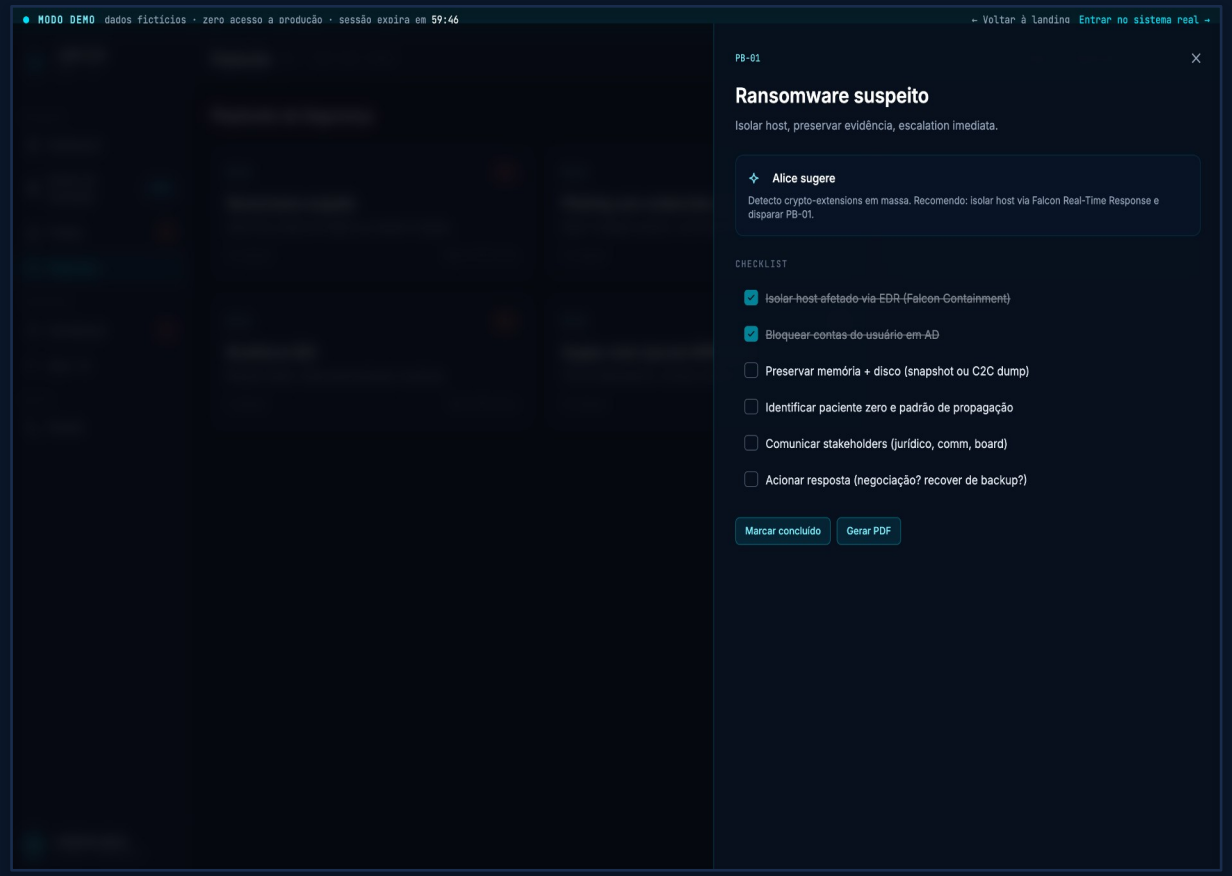


- Claude Opus com prompt caching (custo otimizado)
- Sugestão de playbook aplicável por ticket
- Consultas Wazuh prontas pra colar
- Redaction de PII antes do envio à API

PRODUTO · RESPOSTA

Playbooks acionáveis com checklist.

Cinco playbooks (ransomware, phishing, exfil, brute-force, supply-chain) com checklist progressivo e geração de PDF.

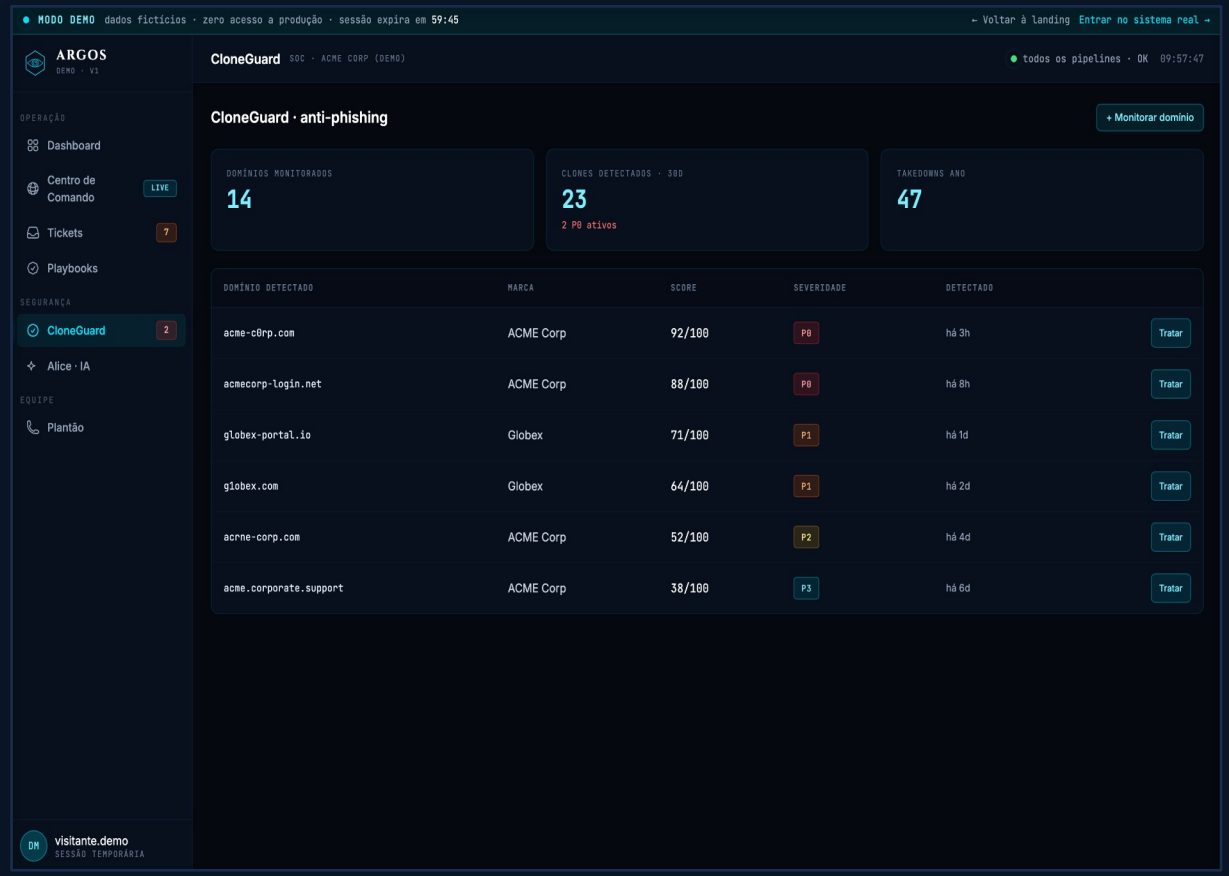


- Checklist marcável passo a passo
- Alice sugere playbook por contexto
- Geração de relatório PDF por execução
- Histórico de execuções auditável

PRODUTO · ANTI-PHISHING

CloneGuard · domínios falsos sob vigilância.

Monitora sua marca via dnstwist + crt.sh + similaridade HTML. Classifica P0–P3 com indicadores explicáveis.



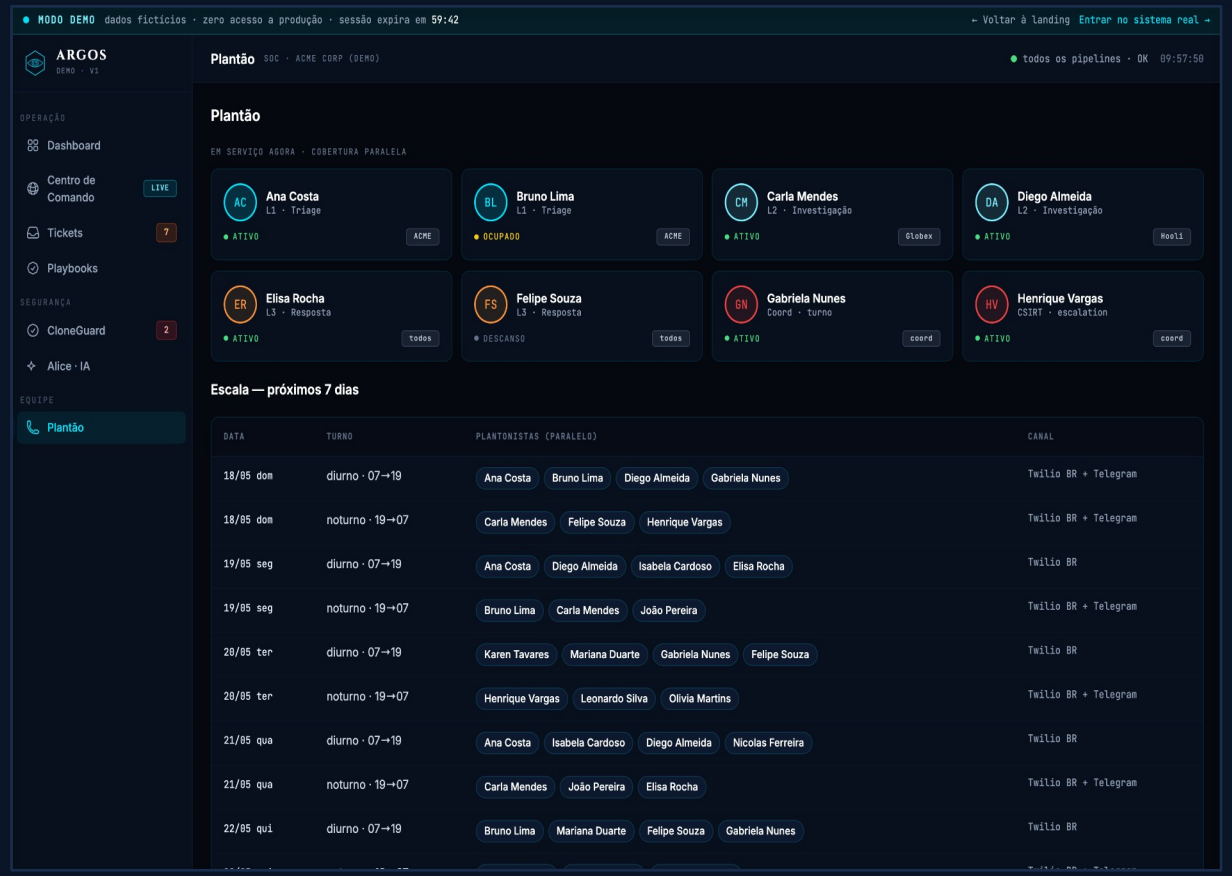
- 14+ domínios monitorados por cliente médio
- Score 0–100 com fatores transparentes
- P0 dispara takedown automático
- Histórico de 23 clones detectados em 30d

OPERAÇÃO · 24×7

Plantão paralelo com Twilio Voice.

8 plantonistas em paralelo cobrindo tiers L1/L2/L3 + Coord. Escalation por Telegram → ligação Twilio BR/US.

- Rotação por semana ISO automática
- L1 Triage · L2 Investigação · L3 Resposta
- Ligação Twilio + TTS PT-BR + ack DTMF
- Fallback automático após 60s sem ack



POR QUE ARGOS

Diferenciais técnicos.

Pragmático, multi-tenant, com governança de IA — não é um SOC montado em Excel.

Multi-tenant nativo

- Isolamento por SOC: dados, IA, audit trail
- 4 managers Wazuh aglutinados
- GLPI source-of-truth pra dedup de tickets

IA com governança

- Claude Opus com prompt caching ativo
- Redaction antes do envio (PII / segredos)
- Opcional: LLM on-premise (Ollama/vLLM)

Resposta automatizada

- Workflows Shuffle com aprovação opcional
- Bloqueio em pfSense (BR-DF + SP-AZ) + Cloudflare
- Twilio Voice BR/US com ack DTMF

Stack pragmático

- Docker Compose, ~4 GB RAM por nó
- Postgres + nginx + FastAPI + Alpine.js
- Zero dependência obrigatória de cloud

PRÓXIMOS PASSOS

Do interesse ao SOC em produção.

Quatro etapas, ciclo total de 3 a 4 semanas.

D + 1

Demo guiada e diagnóstico

Sessão com sua equipe técnica, mapeamento de fontes (SIEM, EDR, tickets), gaps e MTTRs atuais.

Sem 1

Onboarding técnico + escala de plantão

Provisionamento Argos + agentes Wazuh, regras-base, integração Shuffle e Twilio. Setup de escala 24×7.

Sem 2-3

Calibragem com casos reais

Triagem dos primeiros alertas, ajuste de supressões, criação de playbooks customizados, relatório semanal.

Sem 4 →

SOC em regime · revisão mensal

SLA medido (MTTA / MTTR / cobertura), relatório executivo PDF, revisão mensal com CSO/board.

Quer ver Argos rodando agora? demo ao vivo · sem cadastro argos.nobug.com.br/demo

A **ARGOS · NoBug**

Obrigado.

100 olhos. Zero pontos cegos.

Guilherme Mota Stockmann

Sócio · NoBug Tecnologia

guilherme@nobug.com.br

argos.nobug.com.br · nobug.com.br