



ARGOS · NoBug

v1 · 2026

SECURITY · OPERATIONS · 24x7

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

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

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.

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.

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.

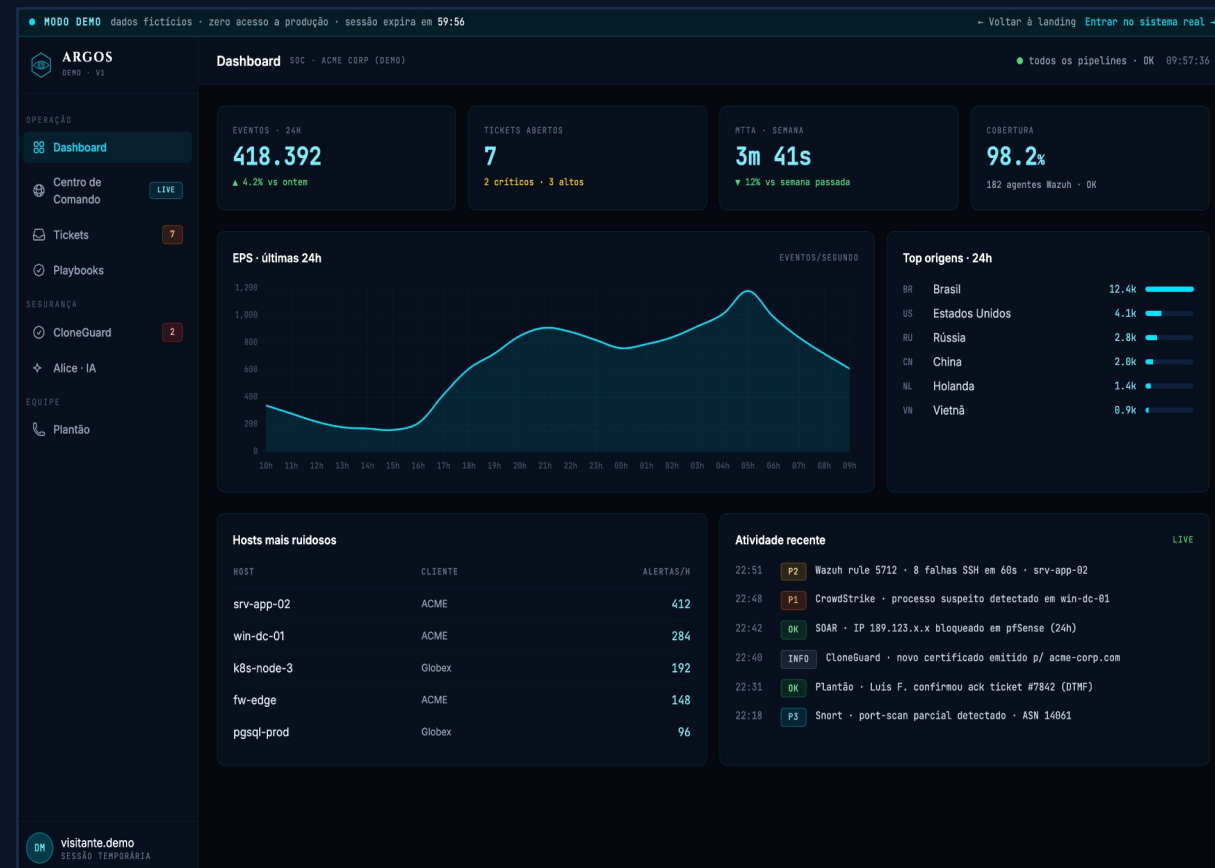
Plantão + Voice

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

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



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

ARGOS
DEMO - V1

Centro De Comando SOC - ACRE CORP (DEMO)

todos os pipelines - OK 09:57:42

UTC 12:57:42Z
EPS 388
CONNS 1.089 / 60s

● P0 ● P1 ● P2 ● P3

OPERAÇÃO

- Dashboard
- Centro de Comando **LIVE**
- Tickets 7
- Playbooks

SEGURANÇA

- CloneGuard 2
- Alice - IA

EQUIPE

- Plantão

TOP ORIGENS - LIVE

RU	Rússia	0
CH	China	4
US	Estados Unidos	1
NL	Holanda	3
VN	Vietnã	1
KP	Coreia do Norte	0
IR	Irã	1
BR	Brasil (interno)	1

visitante.demo
SESSÃO TEMPORÁRIA

FEED - ATTACKS BLOCKED

- 09:57:42 NL SMB enum bloqueado
- 09:57:42 VN CVE attempt - CVE-2024-3094
- 09:57:41 NL Tor exit detectado
- 09:57:41 CN IP malicioso bloqueado 24h
- 09:57:48 TR C2 callback bloqueado
- 09:57:39 CN Bruteforce SSH bloqueado
- 09:57:39 CN Bruteforce SSH bloqueado

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

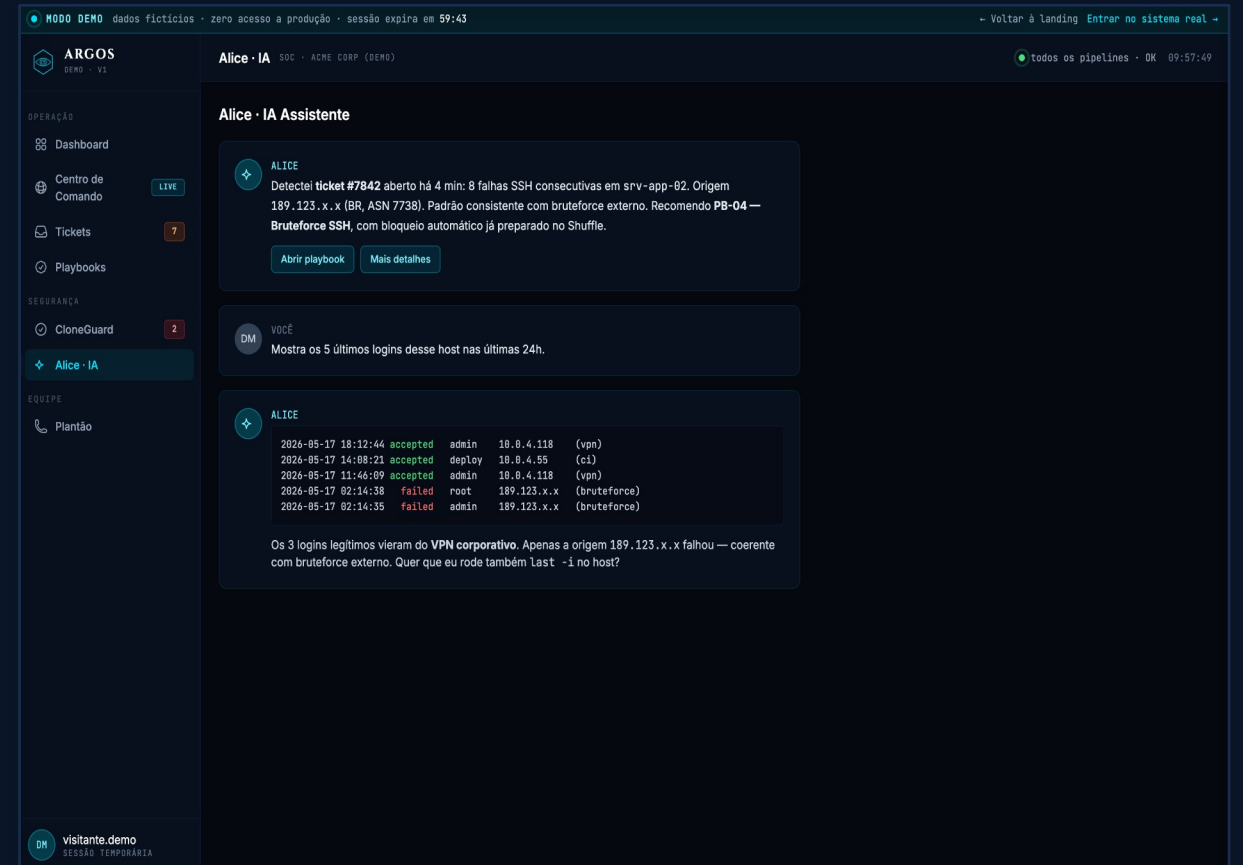
The screenshot displays the ARGOS SOC dashboard interface. At the top, it shows 'MODO DEMO' and 'dados fictícios · zero acesso a produção · sessão expira em 59:48'. The main header includes 'ARGOS DEMO - V1' and 'Tickets SOC - ACME CORP (DEMO)'. A left sidebar contains navigation options: 'Dashboard', 'Centro de Comando' (LIVE), 'Tickets' (7), 'Playbooks', 'CloneGuard' (2), 'Alice - IA', and 'Plantão'. The main area is titled 'Tickets · pipeline SOC' and features a Kanban board with four columns: 'Novo' (1 ticket), 'Em análise' (3 tickets), 'Aguardando' (1 ticket), and 'Resolvido' (2 tickets). Each ticket card shows a number, title, severity (P0-P3), owner, and age. For example, ticket #7839 is 'Novo' with severity P3, title 'Volume EPS anormalmente baixo - proxy01', owner 'ACME - metric', and age '2h'. Ticket #7842 is 'Em análise' with severity P1, title 'Bruteforce SSH em srv-app-02', owner 'Alice', and age '4m'. Ticket #7840 is 'Aguardando' with severity P2, title 'Falha conexão Wazuh agent - db-prod-2', owner 'Globex - system', and age '1h'. Ticket #7837 is 'Resolvido' with severity P1, title 'Privilege escalation Linux - k8s-node-3', owner 'Lucas F.', and age '4h'. Ticket #7836 is 'Resolvido' with severity P3, title 'Política Cloudflare WAF - regra desatualizada', owner 'ACME - config', and age '6h'. Ticket #7841 is 'Em análise' with severity P0, title 'Lateral movement suspeito win-dc-01', owner 'Luis F.', and age '22m'. Ticket #7838 is 'Em análise' with severity P2, title 'CloneGuard P1 detectado - acme-c0rp.com', owner 'ACME - cloneguard', and age '3h'. The bottom left corner shows a user profile for 'visitante.demo' with a 'SESSÃO TEMPORÁRIA' indicator.

Alice — assistente de investigação.

Triagem por LLM com hipóteses, indicadores e queries Wazuh sugeridas.

Multi-tenant isolado, com audit trail.

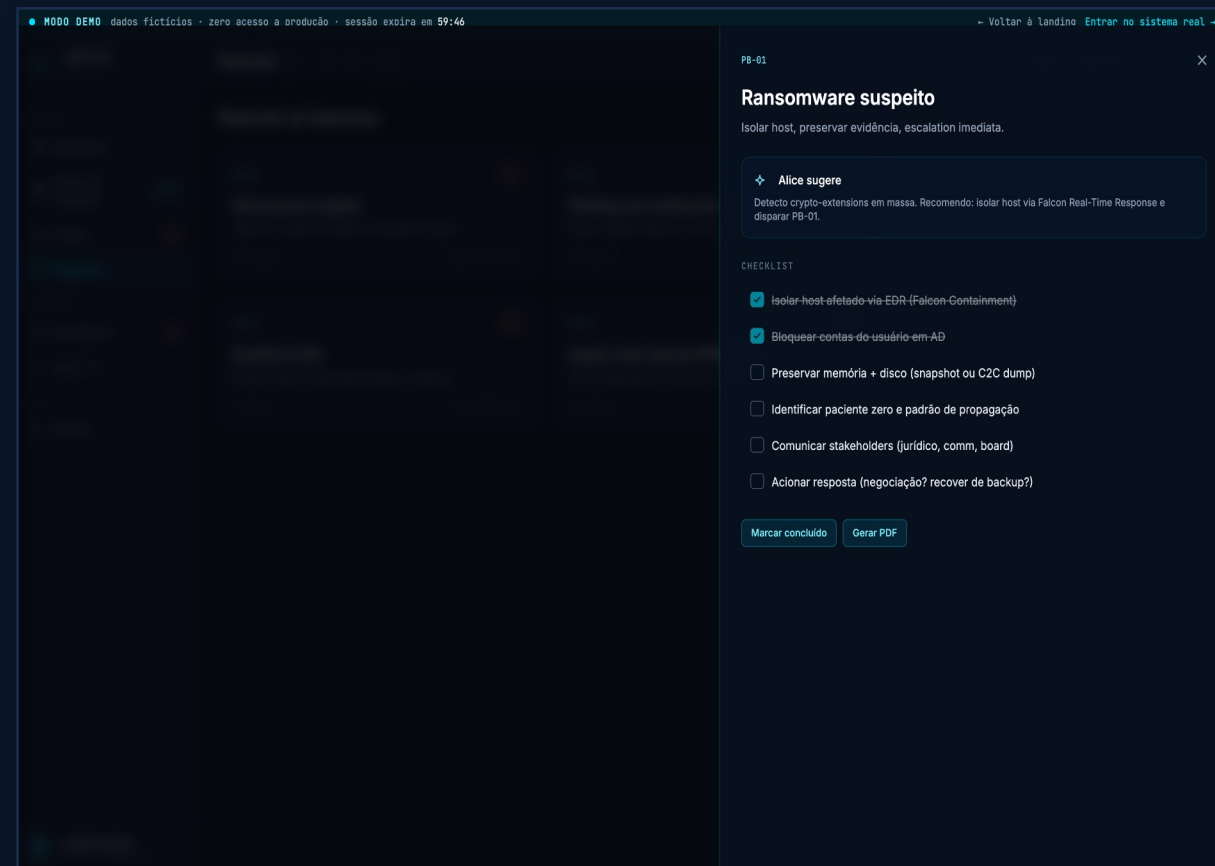
- Claude Opus com prompt caching (custo otimizado)
- Sugestão de playbook aplicável por ticket
- Consultas Wazuh prontas pra colar
- Redaction de PII antes do envio à API



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



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

ARGOS DEMO - V1

CloneGuard SOC - ACME CORP (DEMO)

CloneGuard - anti-phishing

DOMÍNIOS MONITORADOS: 14

CLONES DETECTADOS: 23 (2 P0 ativos)

TAKEDOWNS AND: 47

DOMÍNIO DETECTADO	MARCA	SCORE	SEVERIDADE	DETECTADO	
acme-c0rp.com	ACME Corp	92/100	P0	há 3h	Tratar
acmecorp-login.net	ACME Corp	88/100	P0	há 8h	Tratar
globex-portal.io	Globex	71/100	P1	há 1d	Tratar
globex.com	Globex	64/100	P1	há 2d	Tratar
acme-corp.com	ACME Corp	52/100	P2	há 4d	Tratar
acme.corporate.support	ACME Corp	38/100	P3	há 6d	Tratar

visitante.demo
SESSÃO TEMPORÁRIA

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

The screenshot displays the ARGOS SOC dashboard. The top navigation bar includes 'MODO DEMO', 'dados fictícios', 'zero acesso a produção', 'sessão expira em 59:42', and a 'Voltar à landing Entrar no sistema real' link. The main content area is titled 'Plantão' and shows a grid of team members with their status (e.g., ATIVO, OCUPADO, DESCANSO) and roles (e.g., L1 - Triage, L2 - Investigação, L3 - Resposta, Coord - turno, CSIRT - escalation). Below this is a table titled 'Escala — próximos 7 dias' showing the on-call schedule for the next week, including dates, shifts, and the names of the team members covering each shift.

DATA	TURNO	PLANTONISTAS (PARALELO)	CANAL
18/05 dom	diurno · 07→19	Ana Costa, Bruno Lima, Diego Almeida, Gabriela Nunes	Twilio BR + Telegram
18/05 dom	noturno · 19→07	Carla Mendes, Felipe Souza, Henrique Vargas	Twilio BR + Telegram
19/05 seg	diurno · 07→19	Ana Costa, Diego Almeida, Isabela Cardoso, Elisa Rocha	Twilio BR
19/05 seg	noturno · 19→07	Bruno Lima, Carla Mendes, João Pereira	Twilio BR + Telegram
20/05 ter	diurno · 07→19	Karen Tavares, Mariana Duarte, Gabriela Nunes, Felipe Souza	Twilio BR
20/05 ter	noturno · 19→07	Henrique Vargas, Leonardo Silva, Olivia Martins	Twilio BR + Telegram
21/05 qua	diurno · 07→19	Ana Costa, Isabela Cardoso, Diego Almeida, Nicolas Ferreira	Twilio BR
21/05 qua	noturno · 19→07	Carla Mendes, João Pereira, Elisa Rocha	Twilio BR + Telegram
22/05 qui	diurno · 07→19	Bruno Lima, Mariana Duarte, Felipe Souza, Gabriela Nunes	Twilio BR

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

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 24x7.

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



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