ISPFocus
NETWORK SOLUTIONS

DOCUMENTO TÉCNICO EXECUTIVO • CIBERSEGURANÇA & INFRAESTRUTURA

MONSYS: Plataforma de Orquestração, Telemetria e Imunização Linux

Visibilidade em Tempo Real, Imunização Rápida de Vulnerabilidades Exploradas por IA e Governança Crítica sob Arquitetura Pós-Quântica (PQC)

Combata a Janela de Exploração Zero-Day com Agilidade, Precisão e Zero Portas Abertas (Zero Inbound)

Desenvolvido para: **Diretoria de Tecnologia, Engenharia de Redes, CISO/SysOps & ISPs**
Foco Estratégico: **Mitigação Ativa de CVEs, Uptime Contínuo e Automação Segura de Upgrades**
Stack Tecnológica: **Rust (Axum + Tokio + MariaDB) • Svelte 5 • PQC ML-KEM-768 • AES-256-GCM**

ISPFocus NETWORK SOLUTIONS

CENÁRIO DE AMEAÇAS & AGILIDADE

A Guerra de Velocidade na Era da Inteligência Artificial

O cenário global de cibersegurança sofreu uma ruptura definitiva. O advento e a popularização de modelos avançados de Inteligência Artificial concederam aos agentes maliciosos capacidades sem precedentes de automação ofensiva: **a janela entre a divulgação pública de uma vulnerabilidade crítica (CVE) e a criação massiva de exploits automatizados encolheu de semanas para meras horas**.

Horas

TIME-TO-EXPLOIT ATUAL

Ataques automatizados via IA scaneiam a internet minutos após o patch.

Zero

INBOUND PORTS

O cliente não expõe portas abertas, eliminando superfícies de invasão.

< 30s

TEMPO DE RESPOSTA

Detecção e distribuição atômica de ações em todo o parque de servidores.

Provedores de internet (ISPs) e datacenters corporativos operam dezenas ou centenas de servidores GNU/Linux (DNS Autoritativo/Recursivo, CGNAT, RPKI, BGP, bancos de dados, proxies e firewalls). Gerenciar essas atualizações manualmente via SSH terminal por terminal é uma abordagem lenta, suscetível a esquecimentos humanos, causadora de indisponibilidades acidentais e **incompatível com a velocidade dos ataques modernos impulsionados por IA**. O **MONSYS** surge como a solução definitiva para fechar essa brecha operacional:



Figura 1: Topologia de Segurança MONSYS — Central com TLS PQC coordenando agentes com comunicação 100% outbound e zero listeners expostos.

ISPFocus NETWORK SOLUTIONS

SEGURANÇA POR DESIGN

Engenharia Criptográfica e Imunização Sem Superfície de Ataque

O **MONSYS** foi projetado em Rust sob os preceitos mais rigorosos de Segurança por Design (SSDLC). Diferente de ferramentas legadas de monitoramento que exigem túneis SSH abertos com chaves mestras ou portas de escuta locais (listeners) que se tornam alvos fáceis de intrusão, o MONSYS implementa uma blindagem arquitetural intransponível:

🔒 Zero Inbound Listener nos Servidores

O daemon `monsys-agent` opera como um cliente desprivilegiado nos hosts monitorados. Ele **não abre nenhuma porta TCP ou UDP de escuta**. Toda a comunicação ocorre estritamente de dentro para fora (Outbound HTTPS) em direção à central, inviabilizando varreduras externas e acessos não autorizados por atacantes.

⚡ Criptografia Pós-Quântica (PQC Kyber)

O canal de transporte entre agente e central emprega TLS 1.3 avançado equipado com PQC (**ML-KEM-768 / Kyber** através da engine de criptografia de alto desempenho `aws-lc-rs`). Seus dados e comandos ficam permanentemente protegidos contra ameaças futuras e o modelo de espionagem *Harvest Now, Decrypt Later*.

🔑 Autenticação Criptográfica HMAC + Nonce

Cada frame de telemetria e comando é assinado digitalmente por chave simétrica exclusiva de 256 bits gerada aleatoriamente. Cabeçalhos rigorosos contendo `Nonce` único e `Timestamp` (janela de tolerância estrita de 60s) impedem matematicamente qualquer tentativa de ataques de repetição (Replay Attacks).

🗃️ Cifragem de Repouso AES-256-GCM

As chaves de API e credenciais nunca residem em texto claro no banco de dados MariaDB. Todas as chaves são cifradas com **AES-256-GCM autenticado** utilizando chave mestre independente do sistema operacional, garantindo proteção total mesmo em caso de dump acidental de disco.

Garantias de Execução Segura e Resiliência Operacional

- 🛡️ **Fila Serial Determinística (FIFO Universal):** A central despacha tarefas em fila estritamente ordenada (ex: checar atualizações ➔ aplicar upgrades ➔ reiniciar daemons). Se uma etapa falhar, o pipeline aborta em cascata automaticamente (*fail-fast*), impedindo que comandos erráticos danifiquem o host.
- 🛡️ **Ciclo de Vida Real do Reboot com Reconciliação:** Ao ordenar um reboot, o agente tira um snapshot completo dos serviços em execução antes de reiniciar. No retorno do boot, ele confere se todos os daemons críticos subiram saudáveis, alertando o operador caso algum serviço tenha ficado inativo.
- 🛡️ **Substituição Atômica no Auto-Update do Agente:** Quando uma nova versão do MONSYS é lançada, o agente baixa o binário, valida seu hash SHA-256 criptográfico, executa um teste preliminar de integridade (`--version`) em diretório isolado e só então substitui o executável atomicamente via systemd.
- 🛡️ **Sanitização Estrita contra Injeção de Comandos:** Barreira delimitadora `--` e validação por Regex de todas as units do systemd, bloqueando qualquer vetor de *Command Injection* ou privilégios abusivos.

OPERAÇÃO & VISIBILIDADE

Dashboard Operacional: Consciência Situacional Instantânea

O Dashboard do MONSYS foi desenhado sob a ótica de Engenharia de Operações (NOC/SOC): foco em dados vitais, eliminação de ruídos visuais e feedback reativo instantâneo. Em uma única tela, a liderança técnica obtém a radiografia exata de 100% dos servidores gerenciados, identificando anomalias e riscos sistêmicos em segundos.

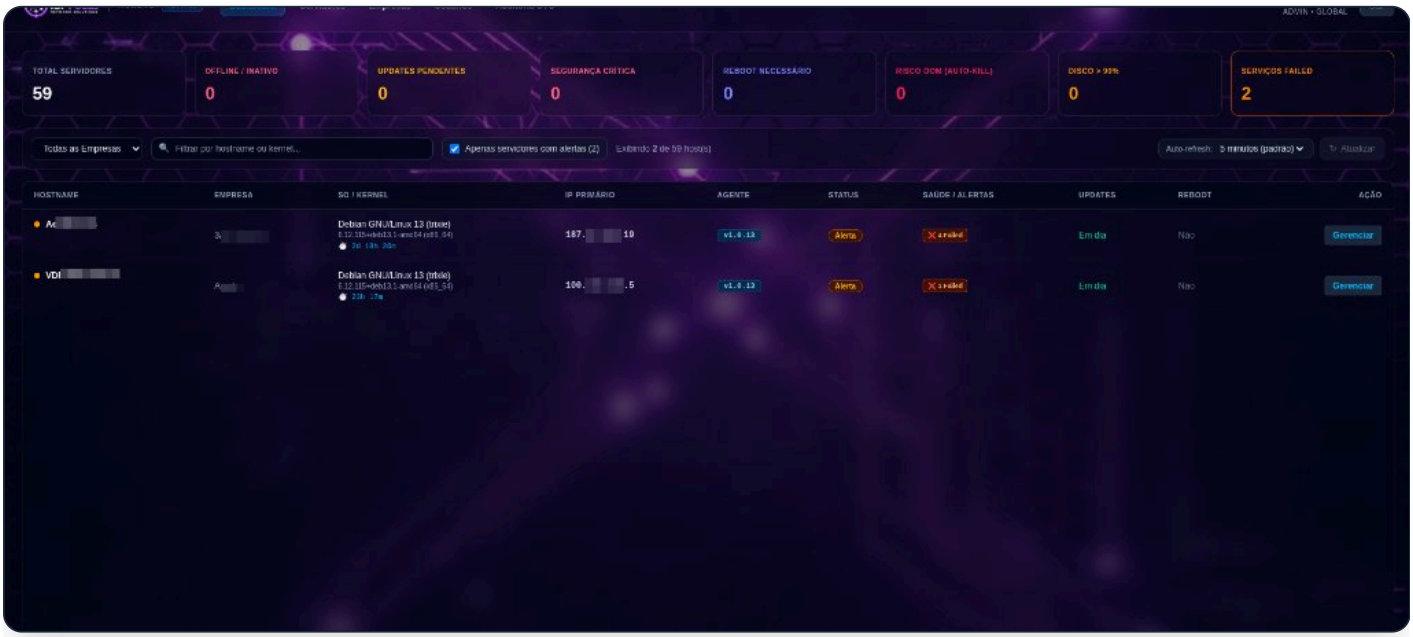

Figura 2: Dashboard Operacional do MONSYS — Monitoramento centralizado com contadores de saúde, telemetria de kernel e filtros dinâmicos.

Métricas Estratégicas e Sensores Preventivos

🚨 Risco OOM (Auto-Kill da Memória)

Sensor algorítmico que avalia o esgotamento conjunto de RAM e Swap (ambos acima de 90%). Emite alerta antes que o mecanismo OOM-Killer do kernel seja forçado a derrubar daemons de missão crítica (como Unbound, Graylog ou CGNAT) por exaustão total de memória.

🛡️ Pacotes Críticos de Segurança

Diferenciação visual explícita entre atualizações corriqueiras e **patches críticos de segurança** (canais `Debian-Security` / `RHEL Errata`). O operador sabe imediatamente quais hosts estão expostos a vulnerabilidades ativas.

💾 Saturação de Disco (> 90%)

Varredura contínua de pontos de montagem locais (`/`, `/var`, `/var/log`), prevenindo o travamento de bases de dados MariaDB/ClickHouse e o colapso de logs rotativos de auditoria por falta de espaço em disco.

🔍 Filtro Dinâmico de Alta Performance

Barra de busca reativa com suporte a substrings case-insensitive: filtre simultaneamente por nome de host (ex: `VDR`, `CGNAT`), versão de kernel (ex: `6.12`), distribuição GNU/Linux ou faixa de endereçamento IP.

Controle Granular do Servidor e Rastreabilidade Total

Ao abrir o modal de detalhes de qualquer host monitorado, o operador tem acesso ao cockpit operacional completo do servidor. A interface apresenta diagnósticos em nível de sistema operacional (Kernel, Uptime, Needrestart, RAM, Swap e Partições) e um terminal auditável com o histórico completo de comandos executados.

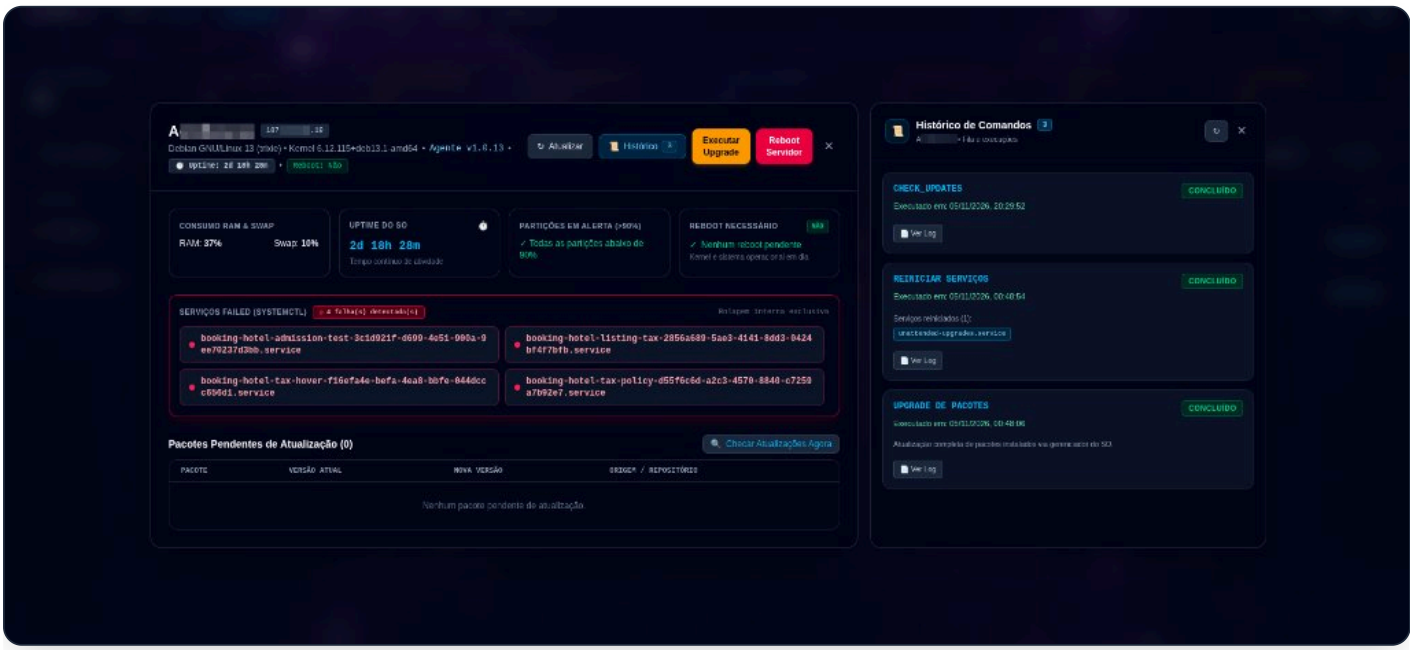

Figura 3: Diagnóstico Detalhado do Host — Lista de serviços failed, inspeção de pacotes pendentes e histórico de execução com saída de logs isolada.

Recursos Chave de Gestão e Remediação

- ✓ **Identificação e Reinicialização Cirúrgica de Serviços Falhos:** O painel lista com exatidão quais unidades systemd entraram em estado `failed`. O administrador pode inspecionar e disparar o reinício seguro de serviços em lote diretamente pela interface web, sem necessidade de sessão SSH manual.
- ✓ **Needrestart Integrado (Reboot ou Reinício de Daemons):** Detecção nativa de bibliotecas compartilhadas (ex: `glibc`, `openssl`) atualizadas em memória que continuam usando código defasado. O sistema aponta se o host necessita apenas de reinício de daemons ou de um reboot do kernel.
- ✓ **Log de Execução Transparente e Isolado:** Cada comando disparado (varredura de pacotes, upgrade ou restart) gera um card de auditoria com status (`CONCLUÍDO`, `FALHOU`), data/hora de execução e botão **Ver Log** com exibição isolada por UUID do `STDOUT` e `STDERR` completos do sistema operacional.
- ✓ **Fila Fail-Fast com Cancelamento Emergencial:** O operador pode acompanhar a fila de comandos em tempo real e realizar o cancelamento preventivo de tarefas enfileiradas antes que sejam processadas pelo nó cliente.

ISPFocus NETWORK SOLUTIONS

Inventário Dual-Stack, Governança Multi-Tenant e Auditoria

Projetado para atender tanto operações corporativas centralizadas quanto provedores com múltiplos CNPJs ou empresas clientes, o MONSYS oferece governança de nível empresarial, rastreabilidade imutável e compatibilidade nativa com redes de nova geração.

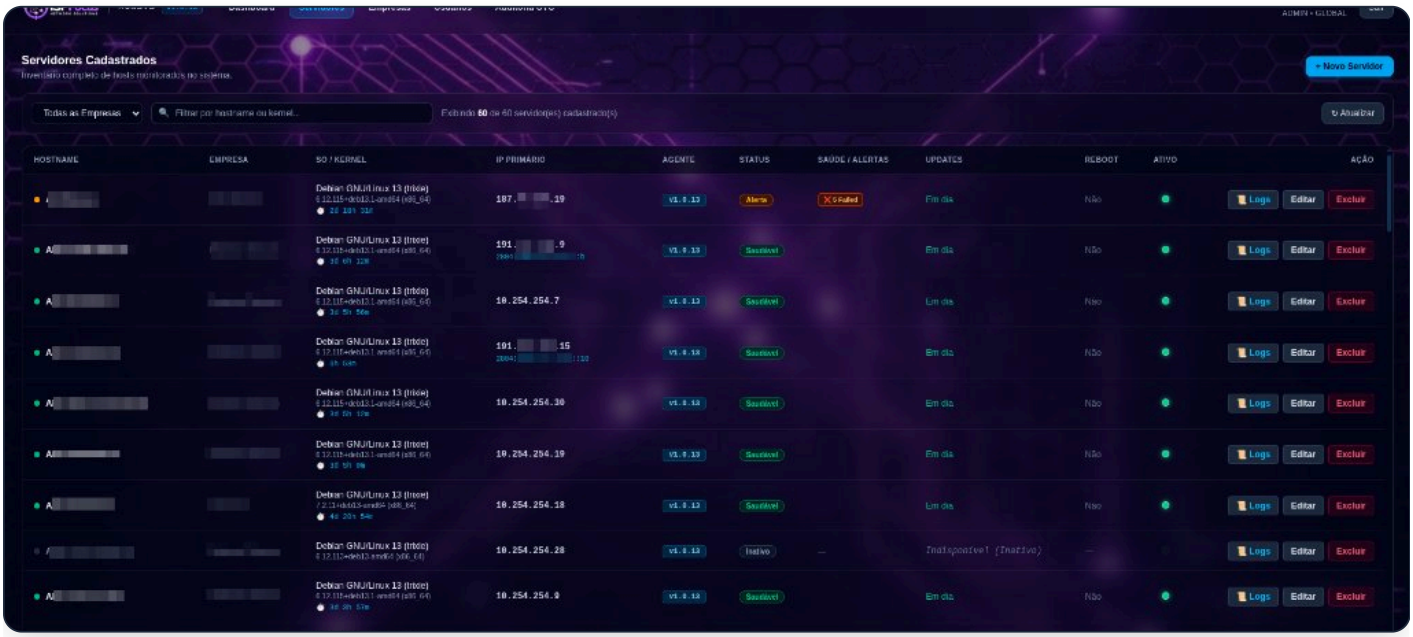

Figura 4: Inventário Centralizado de Servidores — Dual-Stack IPv4/IPv6 real, versão homologada do agente e controle dinâmico de monitoramento.

🌐 Autodescoberta Dual-Stack IPv4/IPv6

O agente analisa a tabela de roteamento do kernel (`ip route`) e extrai o endereço IPv4 e IPv6 público global da interface de rota padrão. Ele descarta automaticamente endereços locais de gerência ou link-local (`fe80::`), garantindo inventário fidedigno.

🏢 Isolamento Multi-Tenant por Empresa

Segregação rigorosa de servidores por Empresa/Tenant. A inativação de uma empresa suspende o monitoramento e o processamento de tarefas de todos os seus servidores em cascata, impedindo vazamento de dados entre operadores de diferentes filiais.

📜 Trilha de Auditoria UTC Imutável

Todas as ações sensíveis (criação de servidores, disparos de upgrades, reboots, exclusões e logins) são registradas com timestamp UTC de precisão microscópica, IP de origem do operador, usuário e payload JSON completo, com visualizador interativo em modal.

🛡️ Defesa Ativa Contra Brute-Force

Mecanismo nativo de proteção na tela de login: limite estrito de 5 tentativas por minuto por IP, hash de credenciais com Argon2id e desafios dinâmicos de CAPTCHA em SVG com assinatura HMAC de uso único, neutralizando robôs e ataques de dicionário.

A Diferença Entre Reagir a um Incidente e Estar Imunizado

Em um ecossistema digital onde falhas de segurança são exploradas em velocidade maquinal por inteligências artificiais, manter servidores desatualizados é assumir o risco de invasões com sequestro de dados (ransomware), desvio de tráfego BGP e degradação de reputação de rede.

Critério Operacional	Gestão Manual / Tradicional	Com a Plataforma MONSYS
Tempo de Resposta a CVEs	Dias ou semanas; depende de janelas manuais.	Minutos; visibilidade imediata e upgrade em 1 clique.
Portas e Acessos Expostos	Chaves SSH distribuídas e portas de escuta abertas.	Zero Inbound Listener; canal fechado via HTTPS PQC.
Risco de Travamento pós-Up	Alto; serviços falhos passam despercebidos.	Mitigado; snapshot pré-reboot e reconciliação ativa.
Auditoria e Rastreabilidade	Histórico fragmentado e volátil nos servidores.	Trilha forense UTC imutável com logs por UUID.
Economia de Recursos	Agentes pesados em Python/Java consomem RAM/CPU.	Binário nativo Rust com consumo ínfimo (< 15MB RAM).

Impacto Estratégico no Negócio

- ✓ **Blindagem Ativa da Reputação e Conformidade:** Protege o Autonomous System (ASN) contra participação involuntária em botnets, sequestro de rotas ou ataques DDoS orquestrados por terceiros.
- ✓ **Redução Drástica do Custo Operacional (OPEX):** Libera a equipe sênior de infraestrutura de tarefas mecânicas e repetitivas de manutenção terminal a terminal para focar na expansão da rede.
- ✓ **Paz de Espírito para a Liderança Técnica:** Certeza matemática de que todo o parque de servidores está auditado, atualizado e funcionando com zero pendências críticas de segurança.

Fale com nossa equipe técnica e comercial: comercial@ispfocus.net.br | Fone/WhatsApp: (22) 99743-9060 | ISPFocus - https://ispfocus.net.br