Segurança IT - Artigo técnico do Voltaire-Monitor v2

Publicado em 2026-01-28 15:57:35

BOX DE FACTOS

- **Versão: Voltaire-Monitor v2** (Monitor + Shield + SIPA).
- **Objectivo:** observabilidade pragmática + detecção de padrões de ataque + mitigação controlada.
- **Princípio central: não criar uma nova vulnerabilidade** ao tentar vigiar tudo.

(EnvironmentFile / variáveis de ambiente).

- **Mitigação:** escalonada (alerta → contenção suave → isolamento com failsafe), evitando auto-sabotagem.

Voltaire-Monitor v2: Monitorização, Hardening e SIPA com Disciplina Operacional

> *Um monitor que abre portas a mais é um sentinela que adormece com a chave na mão. O **Voltaire-Monitor v2** assume uma regra simples: **vigiar sem se tornar vulnerável**, alertar com sinal e não com ruído, e mitigar sem cortar a própria garganta operacional.*

1. Arquitectura: quatro blocos e uma promessa

O Voltaire-Monitor v2 organiza-se em quatro blocos operacionais, desenhados para minimizar superfície de

A promessa é clara: cada componente deve poder falhar sem comprometer os restantes, e sem transformar o servidor num "laboratório de permissões". O monitor não é decoração. É disciplina.

2. Segredos fora do código: o primeiro selo de segurança

A versão v2 elimina credenciais hardcoded e adopta um modelo simples e robusto: **EnvironmentFile** (systemd) e variáveis de ambiente. Isto evita fugas acidentais em backups, repositórios, cópias, logs ou screenshots — a causa mais banal de incidentes evitáveis.

Modelo adoptado

- **/etc/voltaire-monitor.env** com permissões restritas (ex.: 600).
- Uso preferencial de **tokens** em vez de user/password (quando o endpoint o permite).
- Transporte seguro: **HTTPS** sempre que possível, mesmo em LAN (segredos não devem "viajar nus").

3. Execução como serviço systemd: hardening a sério

Correr 24/7 implica systemd. Mas correr 24/7 com segurança implica **confinamento**. A v2 adopta as directivas de hardening que reduzem o impacto de falhas, vulnerabilidades em dependências e execuções indevidas.

O princípio do menor privilégio é aplicado de forma prática: utilizador dedicado, filesystem protegido, proibição de elevação, e permissões de escrita apenas para **estado** e **logs**.

> **Nota operacional:** se o monitor apenas envia alertas, não deve "ouvir" rede. Se precisa de rede, deve ser **mínima**, explícita e auditável.

4. Métricas e thresholds: histerese, janelas e verdade útil

CPU, memória e disco continuam no centro — mas com critério. A v2 evita o "pisca-pisca" de alertas com: **VERIFICATIONS** (persistência), **histerese** (limiar de disparo e limiar de normalização), e **janelas temporais** (um pico curto não é uma crise).

5. Falhas SSH: contagem incremental (o fim dos falsos positivos)

Um erro clássico em monitores "caseiros" é contar falhas SSH com greps cumulativos em *auth.log*. Isso cresce indefinidamente e fabrica "ataques" onde só existe história antiga. A v2 corrige este problema com um modelo incremental:

- Guardar **offset** (posição) do ficheiro lido no ciclo anterior.
- Ler apenas **linhas novas** desde a última posição.
- Contar "Failed password" apenas na janela recente (ex.: últimos minutos).

O resultado é imediato: o SIPA passa a reflectir **acontecimentos**, não "cicatrizes antigas".

6. Integridade: SHA-256 e periodicidade inteligente

A v2 endurece o controlo de integridade, eliminando duas fragilidades comuns: hashes fracos e leitura parcial de ficheiros. Em vez de MD5 e 4 KB, adopta-se **SHA-256** e leitura por blocos, com limite razoável, reduzindo a probabilidade de bypass.

ignorar alertas.

A v2 aplica **periodicidade** (ex.: 10–30 minutos) e, quando necessário, amostragem dirigida. Segurança não é pressa. É consistência.

7. Conexões e tráfego: medir sem incendiar o CPU

A versão v2 assume uma realidade: certas chamadas (ex.: listagens completas de sockets) podem ser pesadas. Assim, a detecção de "conexões elevadas" privilegia fontes de baixo custo e indicadores sumários, e o tráfego é medido por diferença temporal (delta) com limiares claros.

A ideia é simples: o monitor não deve criar o mesmo sintoma que pretende detectar.

8. SIPA: pontuação inteligente com estados (NORMAL / SUSPEITO / ATAQUE)

O **SIPA** (Sistema Inteligente de Pontuação de Ataque) mantém o modelo de score, mas ganha disciplina: eventos

alterações críticas, CPU anómala, instabilidade de rede.

- **Janelas temporais:** cada regra mede o "agora" (últimos minutos), não o "desde sempre".
- **Cooldown de alertas:** um ataque não pode gerar spam; há deduplicação e escalada.

> **Critério que muda tudo**
>
> Um alerta só vale se for accionável. Na v2, cada notificação inclui: **o que aconteceu**, **porquê**, 9**pontuação** e **próximo passo**.

9. Mitigação escalonada: conter sem auto-sabotagem

O gesto dramático de desligar a bridge ou interfaces (*bro/ens, etc*) pode ser vital... ou pode deixar-te às escuras no pior momento. A v2 substitui "pânico automático" por mitigação escalonada:

- **Nível 1:** alerta crítico (com contexto e recomendação de acção).

automática após X minutos) ou com confirmação humana.

Isto protege o servidor sem destruir a tua capacidade de resposta. Segurança sem operação é teatro; operação sem segurança é roleta.

10. Logs, retenção e forense: a memória que te salva amanhã

A v2 mantém métricas em CSV diário (útil para análise e gráficos) e adiciona disciplina de logging: níveis, IDs de evento, e mensagens de "recuperação" quando um incidente normaliza.

Complementarmente, recomenda-se rotação (logrotate) e integração com journald, para que o monitor seja também um "relato" do sistema e não apenas um alarme de incêndio.

Conclusão: um guardião que não mente

O **Voltaire-Monitor v2** não tenta ser um SIEM corporativo nem um "dashboard de vaidade". Ele assume o essencial: medir, correlacionar, alertar e mitigar — com o menor risco possível de se tornar ele próprio um problema.

No fundo, é isto: **segurança é disciplina aplicada ao tempo**. E um servidor bem guardado é um servidor que,

Artigo Técnico de :

Francisco Gonçalves

Fragmentos do Caos News Team.

[backsites]

Para mais informações pode contactar-nos em **botão de Contactos**