SENTINEL

Serverul tău e atacat chiar acum. Vezi de cine.

Agent de securitate care rulează 24/7 pe un singur server Linux: colectează din șase surse, ridică incidente, îți dă butonul de blocare pe telefon, scanează vulnerabilități și generează proceduri de patch cu cale de întoarcere verificată.

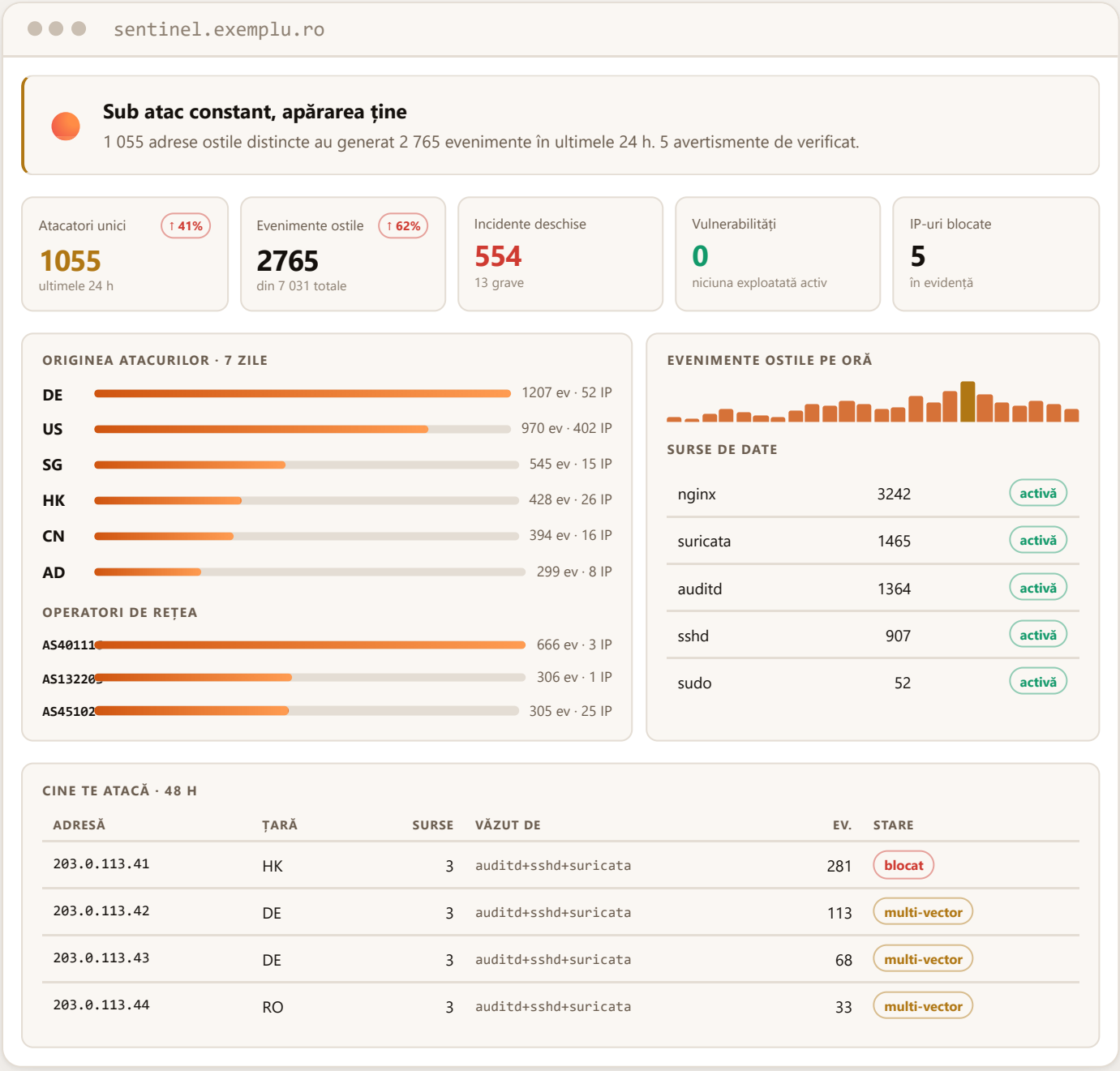
Cifrele de mai jos sunt reale, dintr-o instalare în producție — AlmaLinux 9, 14 aplicații monitorizate, ultimele 24 de ore.

1 055	2 765	6	0	14
atacatori unici / 24h	evenimente ostile	surse de colectare	vulnerabilități deschise	servicii active

PANOUL DE SECURITATE

Prima linie răspunde la o singură întrebare: sunt ok?

Ordinea de citire e designul. Verdict, apoi cifrele care îl susțin, apoi interpretarea, apoi tabelele din care a ieșit. Cine citește doar prima linie are deja răspunsul corect.



Panoul real, cu datele de producție de azi. „Multi-vector” înseamnă că adresa a fost văzută de trei colectoare independente — un scanner de masă atinge o singură suprafață; cine încearcă trei te-a ales.

INTERPRETARE

Un număr nu e o observație.

„2 765 de evenimente” e o cifră. „root a fost țintit de 1 086 de ori de la 93 de adrese — dezactivează autentificarea cu parolă pentru root” e o observație. Motorul rulează reguli deterministe peste date și scoate doar lucruri pe care poți acționa.

5 adrese te atacă pe mai multe fronturi simultan

Apar în 3 surse independente în ultimele 48 h. Un scanner de masă atinge o singură suprafață; cine încearcă trei te-a ales pe tine.

```
De făcut: /block 203.0.113.41 24h
```

root e ținta #1 — 1 086 încercări de la 93 adrese

Cât timp autentificarea SSH cu parolă pentru root e posibilă, fiecare dintre aceste încercări are o șansă.

```
De făcut: grep PermitRootLogin /etc/ssh/sshd_config
```

Infrastructură concentrată de atac: Netiface America, Inc.

666 evenimente ostile de la doar 3 adrese din aceeași rețea. Asta e infrastructură închiriată pentru atac, nu calculatoare compromise răspândite — iar următoarea adresă va veni din același loc.

5 blocări figurează în evidență dar nu mai sunt în firewall

Blocările nu supraviețuiesc intenționat unui reboot — e plasa anti-lockout. Panoul ți-o spune în loc să te lase să crezi că ești protejat.

Campanie activă împotriva GLPI: 560 sondări

Persistentă și țintită — dar nu rulezi GLPI, deci nu te poate atinge. E zgomot de fond, util doar ca să știi în ce val ești.

Zero vulnerabilități de securitate deschise

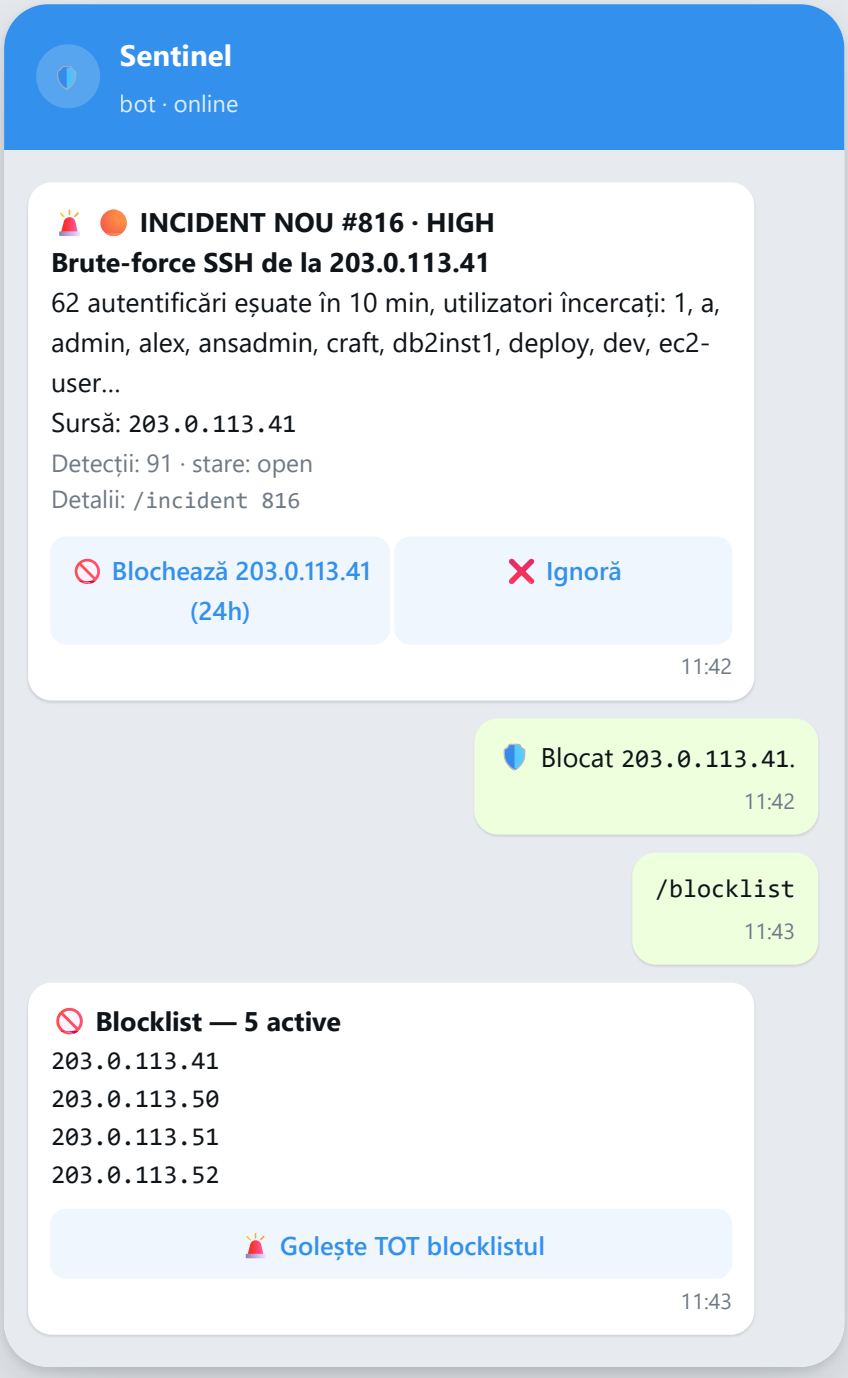
4 716 au fost reparate și confirmate de scanarea următoare.

Toate cele 11 observații de mai sus sunt generate din datele reale ale serverului, fără apel la un model — pagina se randează instant și spune același lucru de două ori la rând.

CANALUL DE URGENȚĂ

Alerta ajunge pe telefon cu butonul de oprire sub ea.

Long-polling, deci niciun port deschis în plus și niciun endpoint public de falsificat. Funcționează chiar dacă nginx sau certificatul sunt stricate — exact când ai nevoie de el.



Apăsarea butonului trece prin aceeași verificare de rol ca o comandă scrisă, iar executorul refuză oricum să blocheze adresa de administrare — chiar dacă butonul e apăsat din greșeală.

DE LA PACHET LA DECIZIE

Ce se întâmplă între atac și butonul de pe telefon.

01 · COLECTARE

Șase surse, filtrate la colector

sshd, sudo/su, nginx, auditd, Suricata. Zgomotul e respins înainte de bază — 96 000 de diagnostice de motor pe zi nu ajung niciodată acolo.

02 · DETECȚIE

Reguli deterministe, la 10 secunde

Praguri oneste peste SQL indexat: brute-force, enumerare web, alerte IDS, anomalie de volum. Zero cost per eveniment.

03 · INCIDENT

Deduplicat pe amprentă

400 de încercări de la o adresă devin un incident, nu 400. Actorul primește țară și operator din baze geo locale.

04 · TRIAJ AI

Judecată, nu scoruri

Modelul recalibrează severitatea și scrie rezumatul în română. Verdictul determinist rămâne alături — dezacordul e vizibil.

05 · DECIZIE

A ta, cu un tap

Auto-block există și e testat, dar se livrează **oprit**. Primele 72 h îți arată ce *ar fi* blocat.

VULNERABILITĂȚI ȘI PATCHING

Scanarea e ușoară. Ce repari întâi e partea grea.

Prioritizare din `CVSS × EPSS × KEV × expunere × criticitate`. Un CVSS 6.5 pe lista CISA de exploatare activă întrece un 9.8 pe care nu-l exploatează nimeni.

sentinel.exemplu.ro/patches/3

Plan de patch #3 validat

țintă **postgresql** · hash `909a1d35a818de31…`

RISC ȘI IMPACT

Nivel de risc	high
Impact	single-service
Downtime estimat	0s
Reversibil	da
Necesită reboot	nu

PREFLIGHT — VERIFICĂRI ÎNAINTE

`verifica_disc`	disk_free
`fara_incident`	no_open_incident
`curl_instalat`	pkg_version

APLICARE · REVENIRE

apply	`dnf -y update curl`
rollback	`dnf -y downgrade curl-7.76.1-29.el9`
backup	`rpm_state · curl`

Plan real, generat automat și validat din prima încercare. Rollback-ul fixează corect versiunea veche — soluția plictisitoare care funcționează.

01

Generare

Din faptele deterministe ale scanării. Nu i se dă niciun shell.

02

Validare

Fiecare comandă e o listă, primul element dintr-o listă permisă, `rm` interzis. Invalid → o reîncercare → respins.

03

Aprobare

Două confirmări pe Telegram, token de unică folosință legat de hash.

04

Backup

Punct verificat prin recitirea arhivelor. Fără el, patch-ul nu pornește.

05

Aplicare

Pas cu pas, scris în bază *înainte* de fiecare comandă.

06

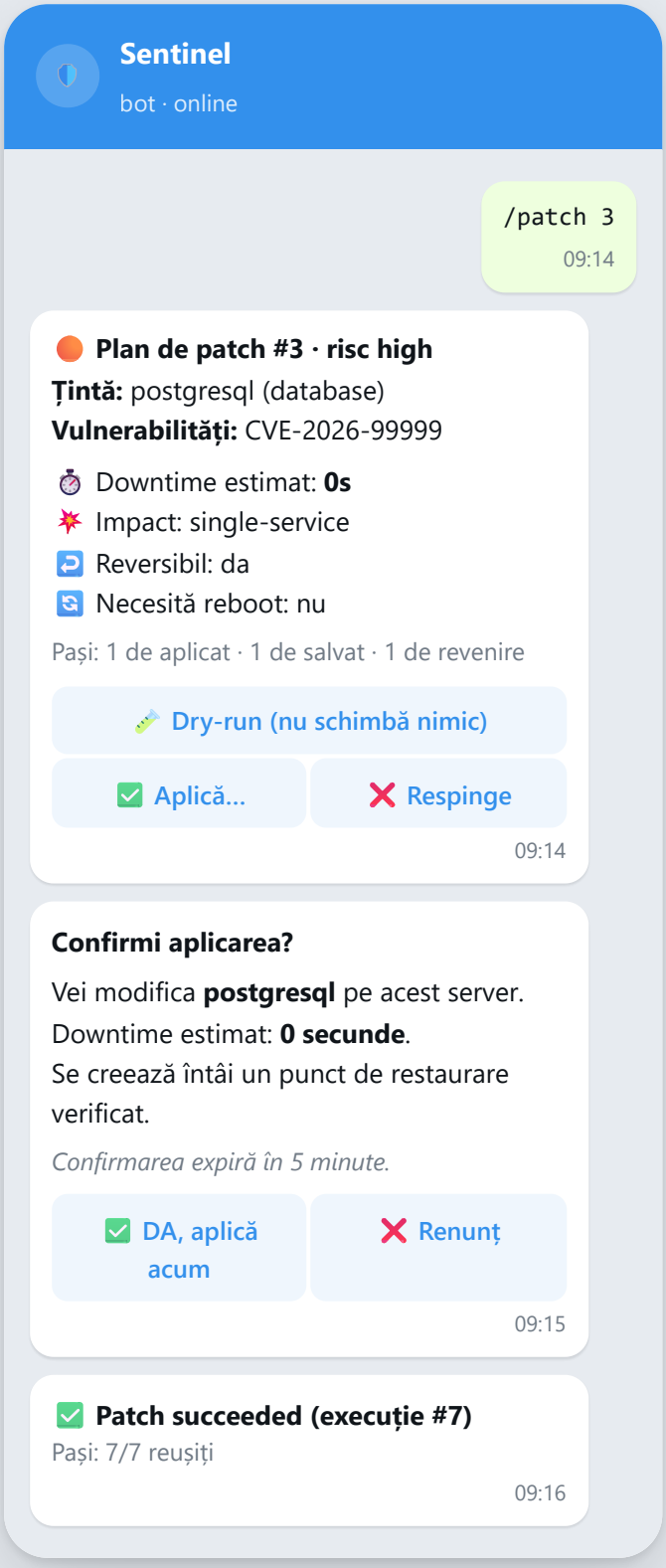
Revenire

Automată la orice eșec. Un rollback eșuat e stare separată, mai gravă.

APROBAREA PATCH-URILOR

Primul tap nu aplică nimic.

Un buton trăiește în istoricul unui chat pentru totdeauna. Deci butonul nu *e* autoritatea — poartă o referință către una: token de unică folosință, legat de chat și de hash-ul planului, cu expirare.



Al doilea ecran aduce informație pe care primul n-o avea — altfel „ești sigur?” e doar un dialog pe care oamenii îl închid din reflex. Dacă planul se regenerează între timp, hash-ul se schimbă și toate butoanele vechi mor.

ARHITECTURA DE SIGURANȚĂ

Un agent care poate bloca internetul trebuie judecat după ce refuză.

Tot ce e privilegiat trece printr-un singur proces root de câteva sute de linii, fără dependențe și fără niciun import din restul aplicației. Restul rulează neprivilegiat.

Nu te poate încuia afară

Două straturi independente: tabela nftables are `policy accept` cu allowlist înaintea blocărilor, iar executorul refuză direct adresa de administrare. Verificat live — refuzul funcționează.

Panoul nu poate bloca pe nimeni

Interfața web poate doar *anula* o blocare, niciodată crea una. Un panou compromis rămâne o scurgere de date, nu o preluare de control.

`rm`

Absent din lista de binare permise pentru patch-uri. Ștergerea trece printr-o singură operație, limitată strict la directorul de backup, cu calea reverificată după rezolvare.

Scriptul de restaurare se scrie singur

Generat *în interiorul* executorului, din ce vede el pe disc. Text venit din partea neprivilegiată nu devine niciodată o linie executabilă rulată ca root.

Un backup gol nu e un backup

Arhivele sunt recitite și rehash-uite la sigilare. Un artefact de dimensiune zero e respins — altfel arată ca o cale de întoarcere exact până când ai nevoie de ea.

Nu poate fi păcălit prin loguri

Liniile de log sunt împachetate ca date neîncrezute, iar modelul poate returna doar un verdict structurat. O injecție reușită schimbă o etichetă, niciodată sistemul.

Retenția nu șterge ultima cale

Nu se șterge niciodată ultimul punct de restaurare al unui asset, oricât de vechi. O retenție care poate face asta e pierdere de date pe cronometru.

Golire de urgență

`touch /etc/sentinel/PANIC` golește blocklistul la fiecare 10 secunde cât timp fișierul există. Blocările nu supraviețuiesc unui reboot — repornirea e mereu o ieșire.

INSTALARE

O comandă, și nimic nu se schimbă până nu spui da.

Wizard-ul își dă seama singur unde rulează: pe laptopul tău întreabă o țintă și instalează prin SSH, pe server sare peste jumătatea de SSH.

bash

```
$ git clone https://github.com/dragosnimu/sentinel.git
$ cd sentinel && ./scripts/wizard.sh --dry-run

✓ AlmaLinux 9.8 (familia rhel)
✓ python3.12 — 5208 MB memorie — 94 GB liberi
✓ nginx deține 80/443 → modul „shared" e disponibil
! portul 8443 e ocupat de altcineva

--dry-run: nu s-a modificat nimic.
```

01 · ÎNTREABĂ

Nimic nu se ghicește tăcut

Ținta, domeniul, modul nginx, adresa ta de administrare, Telegram, cheia AI. Unde există un default rezonabil, îl vezi înainte să-l accepți.

02 · VERIFICĂ

Doar citește

Distribuție, memorie, disc, cine deține 80/443, dacă portul cerut e liber, dacă domeniul rezolvă aici. Nimic nu se atinge.

03 · REZUMĂ

Ultimul punct de ieșire

Tot ce urmează să se schimbe, pe ecran, înainte de confirmare. Un installer care a editat deja nginx când te întreabă, te minte.

04 · INSTALEAZĂ

Numerotat și reluabil

Fiecare pas are marker pe disc. Dacă un serviciu al tău s-a oprit, instalarea face rollback singură.

Secretele nu ajung în tabela de procese

Tokenul de bot și cheia API se citesc cu ecoul stins și călătoresc pe stdin. Ca argument de linie de comandă, `ps` le-ar arăta oricărui cont de pe gazdă.

Două familii de distribuții, un singur fișier

RHEL (AlmaLinux, Rocky, CentOS Stream, Fedora) și Debian (Debian, Ubuntu). Tot ce diferă stă în `deploy/lib/distro.sh`.

Ce nu e suportat, e refuzat pe nume

`unsupported distribution` O gazdă la care instalarea a eșuat vizibil e recuperabilă. Una care pare protejată și nu e, nu.

Răspunsurile se pot salva și relua neasistat — al doilea server, sau o refacere, nu mai cer nicio întrebare.

STADIU

Ce e livrat și rulează în producție.

514 teste automate	**31** invariante de siguranță	**7** servicii systemd	**13** migrații de schemă
0 dependențe CDN			

Colectare din șase surse, detecție deterministă, incidente cu triaj AI, blocare cu buton pe Telegram, scanare de vulnerabilități cu prioritizare KEV, generare și aplicare de patch-uri cu backup verificat și revenire automată. Interfață web fără JavaScript terț, cu politică de securitate strictă și zero resurse externe.

Auto-block-ul se livrează **oprit** — mașinăria e completă și testată, dar primele 72 de ore sunt de observare, ca să găsești fals-pozitivele înainte să tai pe cineva la 3 dimineața. Patch-urile se generează automat; nu se aplică niciodată fără două confirmări explicite.

Sentinel 0.19.1 · RHEL sau Debian, cu systemd · cifrele din această pagină sunt extrase dintr-o instalare reală în producție, la momentul generării.