CRYPTOITDATA

Sentinel

Agent autonom de securitate pentru servere Linux expuse la internet. Detectează, decide, alertează în sub două minute și poate opri atacul singur.

PROBLEMA

Un server expus la internet e scanat continuu. Atacurile nu mai sunt făcute de oameni care obosesc: sunt automate, pornesc în minutul în care apare o vulnerabilitate publică și nu țin cont de programul tău de lucru.

Firmele mici nu au pe cineva care să se uite. Soluțiile mari presupun un om care citește alerte — și livrează mii pe lună. Diferența dintre „am fost atacat" și „am avut o pană" e cât de repede decide cineva, nu câte date s-au strâns.

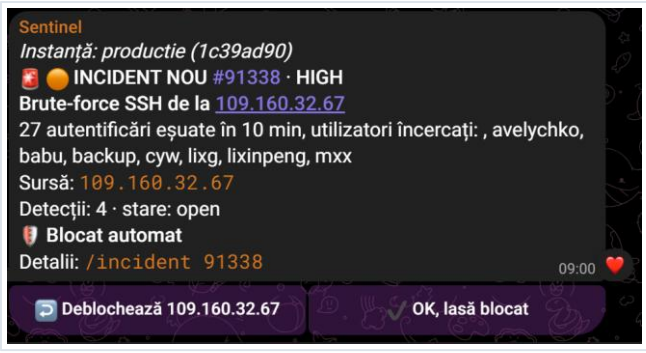
SOLUȚIA

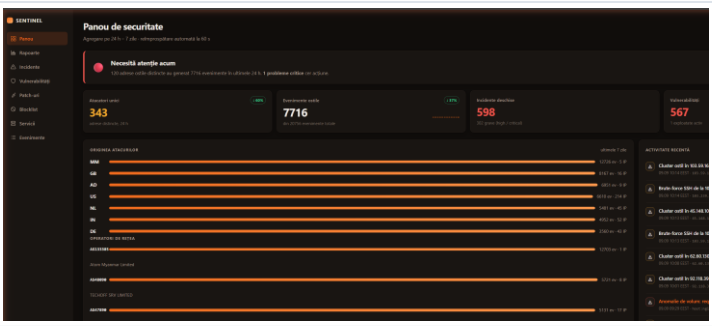
Sentinel rulează pe serverul tău și închide bucla singur: colectează, detectează cu reguli deterministe, corelează sutele de detecții într-un incident, cere modelului un verdict în română, te anunță pe Telegram și poate bloca sursa — cu durată și listă albă.

CUM FUNCȚIONEAZĂ, PAS CU PAS

01 **Colectare** journald (sshd, sudo, auditd), nginx, Suricata IDS, nftables. Pe gazdă, fără agent extern.
02 **Detecție** reguli deterministe, cu praguri calibrate pe traficul tău. Niciun model nu decide aici.
03 **Corelare** detecțiile aceleiași surse devin un incident, iar incidentele legate devin o campanie.
04 **Triaj AI** modelul citește incidentul deja format și scrie verdictul și procedura, în română.
05 **Notificare** Telegram, cu butoanele de acțiune chiar în mesaj. Mediana măsurată: 105 secunde.
06 **Răspuns** blocare în nftables, cu durată și listă albă. Primele 72 de ore rulează în mod «observă».
07 **Vulnerabilități** inventar, apoi semafor SSVC din datele CISA, EPSS și KEV — nu un scor care dă 80 la tot.
08 **Patching** planul e redactat de model, verificat de noi, și nu rulează fără semnătura ta.
09 **Verificare proprie** 79 de verificări la fiecare 5 minute, fiindcă un produs de securitate cade în tăcere.
10 **Martor extern** o mașină din afară confirmă că serverul e viu; dacă tace, sună ea.

CAPTURI REALE





Stânga: alerta pe telefon, cu butoanele în mesaj. Dreapta: panoul de pe mașina ta — incidente, surse, istoric.

CRYPTOITDATA

Cifre și prețuri

Tot ce urmează e măsurat pe serverul nostru de producție, pe ultimele 30 de zile. Nimic nu e estimat.

CE ÎL FACE DIFERIT

Decide pe server

Logurile nu pleacă nicăieri. Analiza se face unde se produc evenimentele.

Regula decide, modelul explică

Nicio ieșire a modelului nu ajunge la firewall, la shell sau la pachete.

Se verifică singur

79 de verificări caută exact felul în care un produs de securitate moare: tăcut.

Are un martor din afară

Un agent care moare nu poate raporta că a murit.

CE A FĂCUT, ÎN 30 DE ZILE

334.752 evenimente colectate **11.158 pe zi**	**53.642** detecții după reguli **auth 31.473 · rețea 12.241**	**1.741** incidente după corelare **doar 6 critice**	**100 %** cu acțiune automată **1.741 din 1.741**
105 s de la incident la telefon **mediană**	**1.047** adrese blocate acum **cu durată și listă albă**	**7.278** vulnerabilități rezolvate **din 9.215 găsite**	**2,76 $** costul stratului AI **pe 30 de zile, per server**

Cifra care contează cel mai mult: **fiecare incident, în fiecare lună, a primit acțiune automată.** Nu vindem „vezi alertele mai repede" — vindem „n-ai nevoie de cineva care să se uite".

PREȚURI

Ofertă de lansare: toate prețurile la jumătate, până pe 31 decembrie 2026.

Instalare

−50% 900 €

fără TVA · 1.089 € cu TVA · per server
o dată · alte țări UE: 1.000 € fără TVA

Evaluare, instalare pe stack-ul tău, calibrare 72 h, predare cu documentație.

Administrat

−50% 88 €

fără TVA · 106,48 € cu TVA · per server
pe lună · alte țări UE: 109 € fără TVA

Tot ce e în Instalare, plus: revizuim incidentele lunar, planuri de patch, raport lunar.

Flotă

la cerere

pe bază de proiect

Mai multe servere sau clienți: configurație per mașină, praguri proprii, SLA negociat.

Reduceri de volum −10 % de la 3 servere, −20 % de la 6, −30 % de la 11. **Plată anuală** −8 %. Instalarea e inclusă de la 3 servere. Angajament minim 24 de luni. Prețul de lansare rămâne blocat pe toată durata lui; de la 1 ianuarie 2027 se aplică prețul de listă.

— Nu e antivirus și nu acoperă stații Windows. Monitorizează servere Linux: AlmaLinux 9, Ubuntu 22.04 și 24.04.
— Nu colectează logurile din interiorul containerelor — se văd evenimentele gazdei și ale rețelei.