CRYPTOITDATA

Sentinel

Autonomer Sicherheitsagent für Linux-Server am offenen Internet. Er erkennt, entscheidet und alarmiert in unter zwei Minuten — und kann den Angriff selbst stoppen.

DAS PROBLEM

Ein Server am offenen Internet wird ununterbrochen gescannt. Angriffe werden nicht mehr von Menschen gefahren, die müde werden: sie sind automatisiert, sie starten in der Minute, in der eine Schwachstelle öffentlich wird, und sie kennen Ihre Arbeitszeiten nicht.

Kleine Firmen haben niemanden, der hinschaut. Große Lösungen setzen einen Menschen voraus, der Alarme liest — und liefern Tausende pro Monat. Der Unterschied zwischen „wir wurden angegriffen" und „wir hatten einen Ausfall" ist, wie schnell jemand entscheidet, nicht wie viele Daten gesammelt wurden.

DIE LÖSUNG

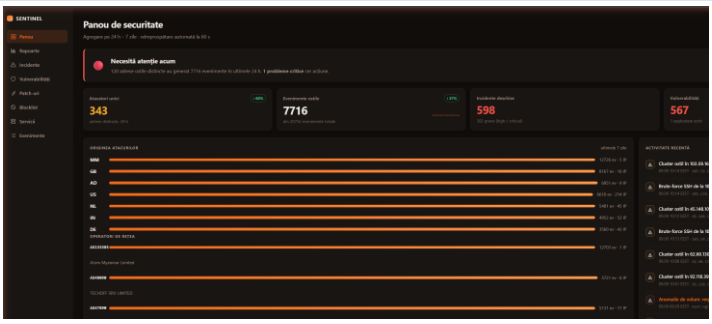
Sentinel läuft auf Ihrem Server und schließt den Kreis selbst: er erfasst, erkennt mit deterministischen Regeln, korreliert Hunderte Erkennungen zu einem Vorfall, lässt das Modell ein Urteil schreiben, benachrichtigt Sie über Telegram und kann die Quelle sperren — mit Ablauf und Ausnahmeliste.

SO FUNKTIONIERT ES, SCHRITT FÜR SCHRITT

01 **Erfassung** journald (sshd, sudo, auditd), nginx, Suricata IDS, nftables. Auf dem Host, ohne externen Agenten.
02 **Erkennung** deterministische Regeln, mit auf Ihren Verkehr kalibrierten Schwellen. Hier entscheidet kein Modell.
03 **Korrelation** Erkennungen derselben Quelle werden ein Vorfall, verwandte Vorfälle werden eine Kampagne.
04 **KI-Triage** das Modell liest den fertigen Vorfall und schreibt Urteil und Vorgehen.
05 **Benachrichtigung** Telegram, mit den Schaltflächen direkt in der Nachricht. Gemessener Median: 105 Sekunden.
06 **Reaktion** Sperre in nftables, mit Ablauf und Ausnahmeliste. Die ersten 72 Stunden laufen im «Beobachten»-Modus.
07 **Schwachstellen** Inventar, dann SSVC-Ampel aus CISA-, EPSS- und KEV-Daten — kein Score, der allem 80 gibt.
08 **Patching** der Plan wird vom Modell verfasst, von uns geprüft, und läuft nie ohne Ihre Unterschrift.
09 **Selbstprüfung** 79 Prüfungen alle 5 Minuten, weil ein Sicherheitsprodukt lautlos ausfällt.
10 **Externer Zeuge** eine Maschine von außen bestätigt, dass der Server lebt; schweigt er, meldet sie sich.

ECHTE SCREENSHOTS





Links: der Alarm auf dem Telefon, Schaltflächen in der Nachricht. Rechts: das Dashboard auf Ihrer Maschine — Vorfälle, Quellen, Verlauf.

Zahlen und Preise

Alles Folgende ist auf unserem eigenen Produktivserver gemessen, über die letzten 30 Tage. Nichts ist geschätzt.

WAS IHN UNTERSCHEIDET

Er entscheidet auf dem Server

Ihre Logs verlassen nichts. Die Analyse passiert dort, wo die Ereignisse entstehen.

Die Regel entscheidet, das Modell erklärt

Keine Ausgabe des Modells erreicht die Firewall, die Shell oder die Pakete.

Er prüft sich selbst

79 Prüfungen suchen genau danach, wie ein Sicherheitsprodukt stirbt: lautlos.

Er hat einen Zeugen von außen

Ein Agent, der stirbt, kann nicht melden, dass er gestorben ist.

WAS ER IN 30 TAGEN GELEISTET HAT

334.752
erfasste Ereignisse
11.158 pro Tag

53.642
Erkennungen nach Regeln
auth 31.473 · Netz 12.241

1.741
Vorfälle nach Korrelation
nur 6 kritische

100 %
mit automatischer Aktion
1.741 von 1.741

105 s
vom Vorfall bis aufs Telefon
Median

1.047
Adressen aktuell gesperrt
mit Ablauf und Ausnahmeliste

7.278
behobene Schwachstellen
von 9.215 gefundenen

2,76 $
Kosten der KI-Schicht
über 30 Tage, pro Server

Die Zahl, die am meisten zählt: **jeder Vorfall, in jedem Monat, hat eine automatische Aktion erhalten.** Wir verkaufen nicht „Alarme schneller sehen" — wir verkaufen „Sie brauchen niemanden, der hinschaut".

PREISE

Einführungsangebot: alle Preise zur Hälfte, bis 31. Dezember 2026.

Einrichtung

−50% 1.000 €

zzgl. MwSt. · einmalig, pro Server
in Rumänien: 900 € zzgl. MwSt.

Bewertung, Installation auf Ihrem Stack, 72-Stunden-Kalibrierung, Übergabe mit Dokumentation.

Verwaltet

−50% 109 €

zzgl. MwSt. · pro Monat, pro Server
in Rumänien: 88 € zzgl. MwSt.

Alles aus Einrichtung, plus: monatliche Durchsicht der Vorfälle, Patch-Pläne, Monatsbericht.

Flotte

auf Anfrage

projektbasiert

Mehrere Server oder Kunden: Konfiguration pro Maschine, eigene Schwellen, verhandeltes SLA.

Mengenrabatte −10 % ab 3 Servern, −20 % ab 6, −30 % ab 11. **Jährliche Zahlung** −8 %. Die Einrichtung ist ab 3 Servern enthalten. Mindestlaufzeit 24 Monate. Der Einführungspreis bleibt für die gesamte Laufzeit fest; ab 1. Januar 2027 gilt der Listenpreis.

— Kein Virenschutz und keine Windows-Arbeitsplätze. Überwacht Linux-Server: AlmaLinux 9, Ubuntu 22.04 und 24.04.
— Sammelt keine Logs aus dem Inneren von Containern — sichtbar sind Host- und Netzwerkereignisse.