

Cum îți protejăm firma, strat cu strat

Administram IT-ul a peste 80 de companii din România, între 10 și 300 de angajați. La toate, securitatea vine în același abonament ca suportul IT. **Cinci straturi de securitate pe care le montăm, le administrăm și pentru care răspundem noi, cu monitorizare non-stop.**

Atacurile vin din două direcții. Programul care păzește endpoint-urile nu vede ce se întâmplă în conturi, iar cel care păzește conturile nu vede ce se întâmplă pe endpoint-uri.

ENDPOINT

Laptopuri, PC-uri, servere, telefoane de serviciu

- Un ransomware care începe să cripteze fișiere.

CONTURI

Microsoft 365, parole, sesiuni de browser

- O autentificare din altă țară, la patru dimineața.

Amândouă ajung la aceeași analiști, în tură non-stop

Confirmă că e într-adevăr un atac, nu o activitate obișnuită, și îi opresc extinderea.

8 min

TIMP DE RĂSPUNS

De la alertă până când atacul e oprit

24/7

MONITORIZARE SOC

Analiști de securitate în tură, inclusiv noaptea și în weekend

100%

COPII DE SIGURANȚĂ

Testate, la toți clienții administrați

25 ani

EXPERIENȚĂ

Cu aceiași colegi din București care îți cunosc rețeaua

ISO/IEC 27001:2022

Certificat RO231109006, auditat extern anual, verificabil în IAF CertSearch

Microsoft Solutions Partner

Administram direct mediul tău Microsoft 365

Peste 80 de companii

Între 10 și 300 de angajați, din România

Inclusă în abonament

Securitatea intră în abonamentul de administrare IT

Ce s-a schimbat în România. În 2025, DNSC a raportat o creștere de 353% a conturilor compromise și de 153% a incidentelor de ransomware.

NIS2 e transpusă în România prin Legea 58/2024. Dacă firma ta intră sub incidența ei, măsurile de securitate nu mai sunt o alegere, iar răspunderea e a conducerii, nu a departamentului de IT.

Cele cinci straturi de securitate, plus două opționale

Fiecare strat prinde altceva și niciunul nu vede tot. Ce scapă de unul e preluat de următorul. **Cu cât cobori, cu atât intervine mai puțin programul și mai mult omul.** Ultimele două nu intră automat în abonament și se discută separat.

01

Fișierele cunoscute ca periculoase ANTIVIRUS

Blochează ce apare deja pe listele de amenințări cunoscute. E protecția pe care o are orice firmă, doar că la noi nu rămâne pe setările din cutie: o configurăm corect și verificăm lună de lună, pe fiecare dispozitiv, că încă rulează.

ANALOGIE Lista cu fețele cunoscute de la intrare.

ENDPOINT

02

Ce se întâmplă pe endpointuri EDR

Se uită la comportament, nu la fișiere: ce programe pornesc, un ransomware care începe săкриpteze, urmele lăsate de un atacator ca să poată reveni. Poate izola stația în câteva secunde, dar decizia o ia un analist, ca să nu oprim activitatea degeaba.

ANALOGIE Senzorii de mișcare din interiorul clădirii.

ENDPOINT

03

Cine intră în conturile de Microsoft 365 și ce face după ITDR

Învăță ce e normal pentru fiecare cont, apoi semnalează abaterile. Acces din altă țară la patru dimineața, sesiuni furate, reguli noi care ascund emailurile despre facturi, un cont obișnuit care capătă brusc drepturi de administrator.

ANALOGIE Portarul care verifică legitimația la intrare și urmărește ce face omul după ce a intrat.

CONTURI

04

Cineva care se uită, non-stop SOC

Telemetria de la straturile 02 și 03 ajunge împreună la centrul de monitorizare. Un analist se uită la alertă, decide dacă e atac real sau alarmă falsă și acționează: scoate calculatorul din rețea sau blochează contul, pe loc.

ANALOGIE Dispeceratul cu agenți în tură, non-stop.

AMBELE ZONE

05

Cineva care vine și repară ECHIPA TA DE SUPTOR IT

Verificăm ce a atins atacatorul înainte să fie oprit, curățăm stația, o reconectăm și scriem raportul de incident. Aici se închide lanțul, de asta e ultimul.

ANALOGIE Echipa care vine la fața locului și repune totul în ordine.

AMBELE ZONE

+

Evidența completă, într-un singur loc SIEM

Straturile 02 și 03 văd doar endpointurile și conturile. Acest strat adaugă înregistrările din Windows, de la firewall, de la VPN și de la celelalte echipamente conectate. Cu mai multe surse, aceiași analiști pot corela mai multe semnale și prind mai devreme ce altfel s-ar fi văzut târziu. Rămâne și evidența scrisă, păstrată ani de zile, utilă la audit.

OPȚIONAL

+

Oamenii care apasă pe linkuri SAT · SECURITY AWARENESS TRAINING

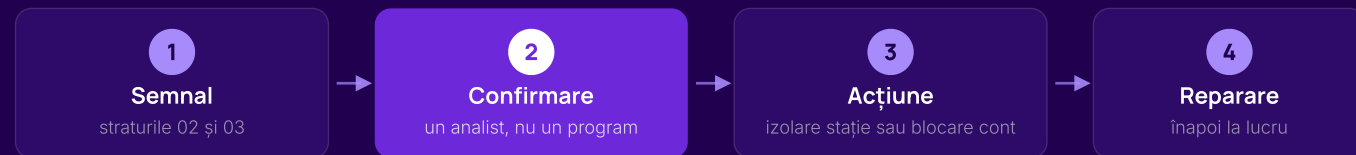
Traininguri lunare, scurte și interactive, urmate de simulări de phishing pe email. Teoria se verifică în practică: vezi cine a învățat și cine mai are nevoie. Nu înlocuiește niciun strat tehnic, dar oprește o parte din atacuri înainte să înceapă.

OPȚIONAL

Toate cele cinci le montăm, le administrăm și răspundem pentru ele. Ultimele două nu intră automat în abonament, dar le recomandăm la majoritatea firmelor.

Ce se întâmplă, pas cu pas

Ordinea contează: **nimic nu se izolează înainte să confirme un om**. Așa nu oprim activitatea firmei pentru o falsă alarmă.



Dacă alarma e falsă

- Analistul o închide și tu nu afli niciodată
- **Nu oprim pe nimeni din lucru**
- Rămâne scrisă în raportul tău

Dacă amenințarea e reală

- Scoatem calculatorul din rețea **în minute**, după confirmare
- Blocăm contul și îi anulăm sesiunile deschise
- Restul firmei lucrează mai departe, netulburat

MTTR de la alertă până când atacul e oprit. Curățarea vine după.

8 min

Media noastră, măsurată la fiecare incident.

Include și triajul făcut de un analist, nu doar detecția automată.

Opt minute înseamnă că un atac pornit la trei noaptea e oprit înainte să se facă dimineață. Când ajunge primul angajat la birou, incidentul e deja închis. **Asta se întâmplă la orice oră**, inclusiv noaptea, în weekend sau în sărbători.

Vrei să știi unde ești descoperit?

Evaluare gratuită de 45 de minute, online, cu raport scris după.
Alegi tu ora în calendar, fără obligații.

risksoft.eu/ro/securitate-cibernetica