

Cum vă protejăm firma, strat cu strat

Administram IT-ul pentru 70+ companii din România. Majoritatea au 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 endpointurile nu vede ce se întâmplă în conturi, iar cel care păzește conturile nu vede ce se întâmplă pe endpointuri.

ENDPOINTURI

Laptopuri, PC-uri, servere, telefoane de serviciu

- Un ransomware care începe să crijteze fișiere.

CONTURI

Microsoft 365, parole, sesiuni de browser

- O autentificare din altă țară, la patru dimineața.

Amândouă ajung la aceiași analiști, în tură non-stop

Confirmă că e într-adevăr un atac și îi opresc extinderea.

8 min**TIMP MEDIU DE
RĂSPUNS**

De la alertă până
când atacul e oprit

24/7**MONITORIZARE
SOC**

Analști specializați
cu care lucrăm,
inclusiv noaptea și
în weekend

5**STRATURI DE
SECURITATE**

Incluse în
abonament, la toți
clienții administrați

25+ ani**EXPERIENȚĂ**

Administrare IT din
2001, cu sediul în
București

**ISO/IEC
27001:2022**

Certificat
RO231109006, auditat
extern anual,
verificabil în IAF
CertSearch

**Microsoft
Solutions
Partner**

Pentru Modern Work:
administrăm direct
mediul Microsoft 365
al firmei

70+ companii

Din România,
majoritatea între 10 și
300 de angajați

**8 recenzii
Google**

Toate de 5 stele,
publice în profilul
Google al firmei

Ce s-a schimbat în România. Raportul de activitate DNSC pentru 2025 arată o creștere de 353% a conturilor compromise și de 153% a incidentelor de ransomware.

NIS2 e transpusă în România prin OUG 155/2024, aprobată prin Legea 124/2025.

Dacă firma 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. **Cu cât coborâți, cu atât intervine mai puțin programul și mai mult omul.**

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: îl administrăm central, iar detecțiile ajung la analiști, non-stop.

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 să cripteze. Blochează singur tiparele clare, cum e un atac fără fișier, și semnalează restul. Calculatorul se izolează doar după ce un analist confirmă că e un atac.

ANALOGIE *Senzorii de mișcare din interiorul clădirii.*

ENDPOINT

03

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

Învață ce e normal pentru fiecare cont și semnalează abaterile: acces din altă țară la patru dimineața, sesiuni furate, drepturi de administrator apărute brusc. O autentificare cu o parolă furată sau o regulă ascunsă pentru emailurile despre facturi le blochează singur.

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. Analiști specializați cu care lucrăm confirmă că e într-adevăr un atac și îi opresc extinderea: scot calculatorul din rețea sau blochează contul.

ANALOGIE *Dispeceratul cu agenți în tură, non-stop.*

AMBELE ZONE

05

Cineva care vine și repară **ECHIPA DE SUPTOR IT**

Verificăm ce a atins atacatorul, curățăm calculatorul, îl reconectăm și vă explicăm ce s-a întâmplat și ce am schimbat. Aici se încheie lanțul, de asta e ultimul.

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

AMBELE ZONE

Cele două straturi opționale

Nu intră automat în abonament. Le recomandăm la majoritatea firmelor.



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, analiștii văd mai mult și pot prinde mai devreme un atac care altfel s-ar fi văzut târziu. Singur, nu oprește nimic. Rămâne și evidența scrisă, păstrată ani de zile, utilă la audit.

OPȚIONAL

Oamenii care apasă pe linkuri **SAT · SECURITY AWARENESS TRAINING**

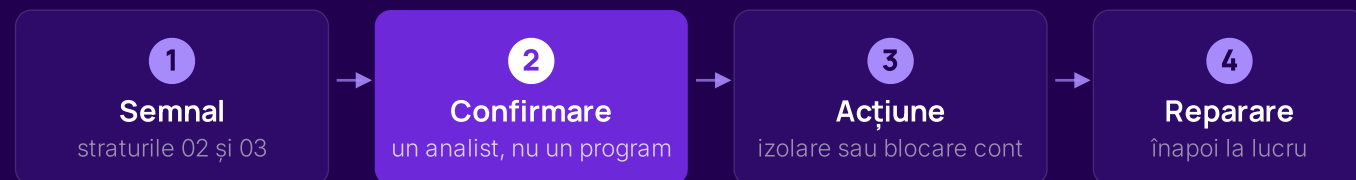
Traininguri lunare, scurte și interactive, urmate de simulări de phishing pe email. Teoria se verifică în practică: vedeți cine a învățat și cine mai are nevoie. Nu înlocuiește niciun strat tehnic, dar oprește o parte din atacuri înainte să înceapă.

OPȚIONAL

Pe acestea două le montăm, le administrăm și răspundem pentru ele la fel ca pentru cele cinci straturi incluse. Se adaugă la abonament doar dacă le alegeți.

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, fără să vă deranjeze
- **Nu oprim pe nimeni din lucru**
- Rămâne notată în evidența alertelor

Dacă amenințarea e reală

- Calculatorul e scos din rețea **în minute**, după confirmarea analistului
- Contul e blocat, sesiunile deschise se închid, parola se schimbă
- Restul firmei lucrează mai departe, netulburat

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

8 min

Timpul mediu de răspuns, la noi.

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.

Monitorizarea funcționează la orice oră, inclusiv sâmbătă noaptea sau în prima zi de Crăciun.

Vreți să știți unde sunteți descoperiți?

Evaluarea gratuită de 45 de minute, online.
După evaluare primiți oferta în scris. Alegeți ora în calendar, fără obligații.

risksoft.eu/ro/securitate-cibernetica