GREYCORTEX

Securitate pentru profesioniști

Faceți rețelele IT/OT sigure și de încredere

GREYCORTEX Mendel folosește inteligență artificială avansată, machine learning și analiza datelor pentru a identifica amenințările, a găsi vulnerabilitățile și pentru a oferi echipei IT vizibilitate completă asupra rețelei, într-un mod cât mai eficient.

Atacurile Avansate sunt Reale și pot fi Greu de Depistat

8 Atacuri
sunt lansate anual în rețelele enterprise

40%
din amenințările cibernetice nu sunt depistate

49 de zile
sunt necesare pentru a depista o breșă folosind doar uneltele actuale

Soluții pentru atacuri, detectare și raportare a anomaliilor

Amenințări necunoscute

Amenințările necunoscute avansate precum malware, RAT sau ransomware, dacă rămân nedetectate, pot duce la:

- pierderea de date sensibile
- atacuri asupra organizației
- pagube materiale pentru companie
- pagube de reputație pentru companie

Lipsă de vizibilitate

Lipsa de vizibilitate asupra rețelei îngreunează identificarea actorilor malițioși si a dispozitivelor suspecte, dar și a:

- întârzierilor critice
- dispozitivelor cu comportament suspect
- timpului pierdut
- resurselor financiare pierdute

Neglijența angajaților

Angajații și partenerii pot încălca regulile, intenționat sau nu. Astfel pot apărea:

- scurgeri de informații sensibile
- atacuri asupra altor organizații
- probleme de conformitate
- nerespectarea GDPR
- încălcarea politicilor de securitate

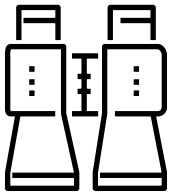
Riscul asupra Afacerii este Real

Peste 50% dintre clienți sau parteneri își pierd încrederea în companie.

Sunt necesare 1-3 zile pentru a atenua efectele unei breșe de date, perioadă cu pierderi financiare inevitabile.

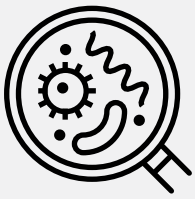
Poate apărea o scădere semnificativă a prețului acțiunilor.

GREYCORTEX Mendel



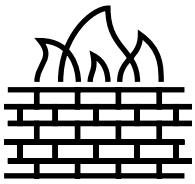
OFERĂ VIZIBILITATE COMPLETĂ ASUPRA REȚELEI

- Detalii de comunicare pentru fiecare dispozitiv, serviciu și subnet până la nivel de aplicație
- Detalii de comportament pentru dispozitivele BYOD și IoT
- Detalii despre utilizator și despre obiectele de inventar
- Performanța aplicațiilor, a dispozitivelor și a rețelei
- Înregistrare și descriere pentru traficul de date
- Potrivit și pentru rețelele IT și pentru rețelele industriale



DETECTEAZĂ AMENINȚĂRILE DE SECURITATE

- Identifică infracțiuni cibernetice, activități de hacking, ransomware și malware nedetectat
- Verifică statusul pentru firewall, securitatea endpoint și legătura VPN
- Monorizează configurările pentru greșeli sau modificări în exploatare
- Detectează încălcări ale politicilor de securitate
- Dispune de metode de detecție comportamentală inclusiv machine learning fără supraveghere, analiză statistică și corelare de evenimente
- Detectează semnături pentru atacuri tip IDS și threat intelligence
- Rulează analiză de trafic criptată



ADAPTABIL PENTRU NEVOILE DVS. DE SECURITATE

- Răspuns manual sau automat prin integrare cu firewall, NAC și consola de management pentru endpoint-uri
- Investigare și gestionare a incidentelor
- Integrare pentru funcțiile SIEM
- Date mereu ușor de găsit și de filtrat
- Analiză criminalistică pentru luni sau chiar ani din istoricul de date

Mendel poate fi implementat	On-premise Virtual sau prin aplicațiile HW	**Servicii oferite**	Monitorizare de securitate și răspuns la incidente	Centru de Operațiuni de Securitate (SOC)	Audit de Securitate
Mendel protejează	**Instituții publice**	**Companii și IMM-uri**	**Sistemul de sănătate**	**Sectorul industrial**	**Infrastructura**

Experiența Mendel

Încercați GREYCORTEX Mendel.
Vă putem oferi chiar și Audit de securitate a rețelei lunar.

Soluții distribuite în România de
axel Secured by trust.
www.axelsoft.ro | sales@axelsoft.ro

Purkyňova 127, 612 00 Brno, Czech Republic, +420 511 205 216, info@greycortex.com, www.greycortex.com