GREYCORTEX

Security for Professionals

Ochrana a stabilita podnikových a průmyslových sítí

GREYCORTEX Mendel chrání sítě proti vnějším hrozbám – kyberkriminalitě, ransomware, malware, i proti selhání lidského faktoru. Zajišťuje dokonalou viditelnost všech zařízení a komunikace v síti. To vše s využitím pokročilých technologií založených na umělé inteligenci a strojovém učení. Včasným zastavením útoků a identifikací nedostatků v konfiguraci sítě šetří finanční náklady, lidské zdroje i čas.

Pokročilé hrozby jsou reálným rizikem a není snadné je odhalit

8 útoků
ročně se pokusí napadnout firemní sítě

40 %
kybernetických hrozeb se nepodaří odhalit

49 dní
trvá odhalení narušení bezpečnosti s využitím stávajících zdrojů

Rešení pro detekci a reporting útoků i anomálií

Pokročilé hrozby

Pokud nejsou pokročilé hrozby jako malware, RATs a ransomware včas odhaleny, mohou vést k:

- ztrátám citlivých dat,
- útokům na organizace,
- přímým finančním ztrátám,
- poškození reputace společnosti.

Špatná viditelnost

Nedostatek viditelnosti do sítě může znemožňovat včasnou identifikaci škodlivých zařízení v síti i možných útočníků, a způsobuje:

- kritická zpoždění,
- časové ztráty a prodlení,
- ztráty finančních prostředků,
- neschopnost detekce zařízení využívaných zloději dat a hackery.

Selhání zaměstnanců

Zaměstnanci mohou záměrně či neúmyslnou chybou porušit interní pravidla a nařízení. Dochází tak k:

- úniku citlivých dat,
- útokům na další organizace,
- problémům s compliance,
- porušením GDPR,
- porušení politik.

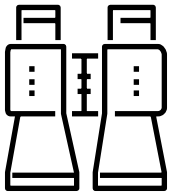
Reálná hrozba pro vaše obchodní operace

Více než 50 % zákazníků nebo partnerů ztrácí důvěru

Finanční ztráty za 1–3 dny potřebné k nápravě škod po průniku do sítě

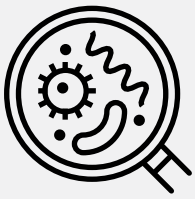
Dochází k významnému poklesu cen akcií

GREYCORTEX Mendel



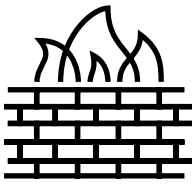
POSKYTUJE PLNOU VIDITELNOST V SÍTI

- Zobrazení komunikace každého zařízení, služby a podsítě až do aplikační úrovně
- Rozpoznání uživatelů a podrobný přehled jednotlivých zařízení
- Výkon zařízení, aplikací a sítě
- Záznam a dešifrování provozu
- Všechna BYOD a IoT zařízení
- IT i ICS/SCADA sítě



DETEKUJE BEZPEČNOSTNÍ HROZBY

- Kyber kriminalita, hackerské aktivity, ransomware, malware
- Ověření správného fungování firewallu, antivirů a VPN připojení
- Chyby a změny v konfiguraci sítě
- Porušení bezpečnostních zásad
- Nezávislé metody detekce založené na strojovém učení, změnách chování, analýze dat a korelaci událostí
- Threat intelligence a IDS signatury
- Analýza šifrovaného provozu



PŘIZPŮSOBÍ OCHRANU SÍTĚ VAŠIM POTŘEBÁM

- Manuální nebo automatická reakce prostřednictvím integrace s firewally, NAC a panelu správy koncových stanic
- Forenzní analýza historických dat
- Vyšetřování a management incidentů
- Integrace se systémy SIEM a SOAR
- Vyhledávání a filtrování dat

Nasazení MENDEL	Lokální uložení dat HW & Virtuálně	**Řízené služby**	Bezpečnostní monitoring a reakce	Security Operations Center (SOC)	Bezpečnostní audit
Mendel chrání	 **Veřejná správa**	 **SMB & Enterprise**	 **Zdravotnictví**	 **Průmysl**	 **Infrastruktura**

Vyzkoušejte si Mendel

Proof of Concept (POC)

Ověřte si požadované funkčnosti Mendel na vlastní síti nebo její části, lze rozšířit do úrovně bezpečnostního auditu sítě nebo její části.