SZOLGÁLTATÁSI AJÁNLAT — 2026

Kiberfertőzöttségi szűrővizsgálat.

AI alapú mélytanulási fenyegetésdetektálás. Preventív kockázatfeltárás — még a támadások előtt.

A NEM LÁTHATÓ FENYEGETÉS

Miért van szükség kiberfertőzöttségi szűrővizsgálatra?

> *„A támadások nem ott kezdődnek, ahol gondoljuk — hanem ott, ahol nem ellenőriztünk.”*

A modern kibertámadások már nem zajosak. A fejlett, célzott fenyegetések gyakran hónapokig észrevétlenül maradnak a vállalati infrastruktúrában — adatot gyűjtenek, jogosultságokat emelnek, vagy előkészítik a későbbi támadást.

// METRIC_01

277 NAP

átlagos rejtett benn-tartózkodás egy sikeres támadás után

// METRIC_02

70%

a hagyományos vírusvédelmek által nem észlelt fileless támadások aránya

// METRIC_03

20ms

alatti detektálás — viselkedés-alapú mélytanulási modell

AKTÍV BEAVATKOZÁS — NEM CSAK ÁLLAPOTFELMÉRÉS

Mit ad többet a Cyber Operations szűrővizsgálata egy hagyományos auditnál?

01 · DEEP LEARNING AI

Mélytanuló MI-modell

A normálistól eltérő viselkedést tárja fel — olyan támadásokat is megtalál, amelyeket a szignatúra-alapú vírusvédelmek nem ismernek fel.

02 · 20+ ÉV BANKI HÁTTÉR

Banki tapasztalatú mérnökök

Senior szakértőink minden gépi találatot manuálisan validálnak — fals pozitívokat kizárva, üzleti kontextusba helyezve.

03 · ONLINE & TÁVOLI

Üzletmenet-megszakítás nélkül

A vizsgálat teljes egészében online, távolról zajlik. A szoftver telepítése kb. 1 óra, a megfigyelés a napi munkát nem zavarja meg.

04 · INCIDENS-VÁLASZ

Közreműködés az elhárításban

Aktív fertőzés azonosítása esetén nem hagyjuk magára a kritikus találatok kezelését — közreműködünk a kontrollált elhárításban.

MIT TARTALMAZ A VIZSGÁLAT?

Módszertani lépések a Deep Learning AI alapú szűrőfolyamatban

STEP 01

Mélytanuló MI alapú végpont- és szerverelemzés

A szűrőszoftver elemzi a kijelölt végpontok és szerverek teljes állapotát, futási folyamatait és hálózati viselkedését.

STEP 02

Rejtett kártékony komponensek azonosítása

Feltárjuk a hagyományos vírusvédelmek által nem észlelt fileless malware-eket, perzisztencia-mechanizmusokat és támadási mintázatokat.

STEP 03

Kompromittált rendszerek feltárása

Azonosítjuk azokat a végpontokat, amelyeken jelenleg vagy a múltban illetéktelen hozzáférés vagy adatszivárgás történhetett.

STEP 04

Lateral movement nyomok vizsgálata

Elemezzük az oldalirányú mozgás nyomait — a hálózaton belüli gyanús eszközök közötti kommunikációt és jogosultságemelési kísérleteket.

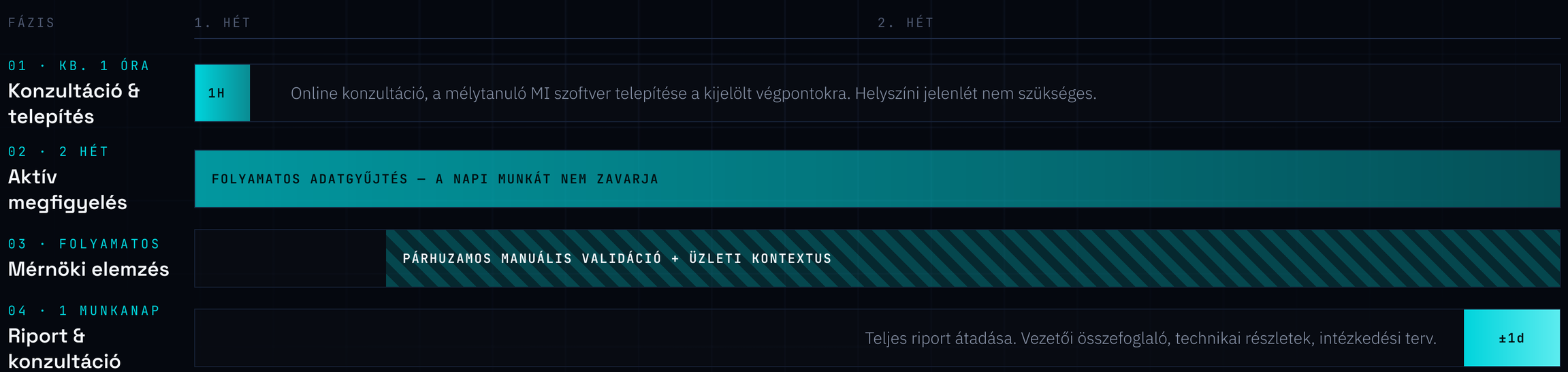
STEP 05

Manuális szakértői validáció

Senior, banki környezetben edzett biztonsági mérnökeink minden gépi találatot manuálisan megvizsgálnak — kizárva a fals pozitívokat.

MEGVALÓSÍTÁSI ÜTEMTERV

A teljes folyamat üzletmenet-megszakítás nélkül, kb. 2 hét alatt zajlik.



ÁTADANDÓK ÉS EREDMÉNYEK

Mit kap a partner cég a vizsgálat lezárásakor?

// DELIVERABLE_01 — 01

Fertőzöttségi állapotjelentés

Objektív, dokumentált jelentés a vizsgált végpontok aktuális biztonsági állapotáról — minden találat technikai részletekkel és bizonyítékkal alátámasztva.

// DELIVERABLE_02 — 02

Kockázati besorolás

KRITIKUS MAGAS KÖZEPES ALACSONY

Minden azonosított eltéréshez kockázati szint társul — kiegészítve az üzleti hatáselemzéssel.

// DELIVERABLE_03 — 03

Prioritizált intézkedési terv

Konkrét, sorrendezett teendőlista a feltárt kockázatok kezeléséhez — mit, milyen sürgősséggel és milyen erőforrással szükséges végrehajtani.

// DELIVERABLE_04 — 04

Közreműködés az elhárításban

Azonosított aktív fertőzések esetén közreműködünk a kontrollált elhárításban — nem hagyjuk magára a kritikus találatok kezelését.

A SZOLGÁLTATÁS TERJEDELME

Tisztán mit tartalmaz a csomag — és mi nem része.

✓ AMIT TARTALMAZ A CSOMAG

INCLUDED

- [+] Kiválasztott végpontok és szerverek vizsgálata
- [+] Deep Learning AI alapú elemzés
- [+] Manuális szakértői validáció
- [+] Lateral movement nyomok feltárása
- [+] Részletes állapotjelentés és kockázati besorolás
- [+] Prioritizált intézkedési terv
- [+] Közreműködés azonosított fertőzések elhárításában

× MI NEM RÉSZE A CSOMAGNAK

EXCLUDED

- [-] A megrendelt terjedelmen túli rendszerek vizsgálata
- [-] Folyamatos (24/7) felügyelet
- [-] Végpontvédelmi szoftver licensz (külön)
- [-] Fizikai biztonsági audit
- [-] Penetrációs teszt (külön ajánlat)
- [-] Hálózati infrastruktúra teljes audit
- [-] NIS2 / DORA compliance tanácsadás

MIÉRT A CYBER OPERATIONS GROUP?

Amit a vizsgálat mögött szakmai garanciaként kínálunk.

20+ ÉV

Banki cybersecurity tapasztalat

Mérnökeink banki környezetben edződtek, ahol a hibatűrés és a támadásdetektálás kritikus szintű. Ezt a szigort hozzuk minden vizsgálatba.

AI

/* DL */

Deep Learning detektálás

Nem szignatúra-alapú, hanem viselkedés-alapú mélytanulási modell — 20 ms alatti detektálással, amely a hagyományos vírusvédelmek vakfoltjait is lefedi.

NIS2

Szabályozási megfelelőség

A vizsgálat hozzájárul a NIS2 és iparági kibervédelmi elvárások bizonyíthatóságához — auditálható dokumentációval támasztjuk alá az eredményt.

TOVÁBBLÉPÉS — CYBR SHIELD CSOMAGOK

A szűrővizsgálat eredményeire építve hosszú távon fenntartható védelmi rendszert alakítunk ki.

// TIER_01

CYBR SHIELD PRO

KKV-SZEGMENS

Deep Learning AI alapú végpontvédelem. Fejlett megelőző technológia, kevesebb mint 20 ms alatti detektálással. Ideális induló megoldás.

- Deep Learning AI EDR
- Megelőző detektálás
- KKV-knak optimalizált

// TIER_02

CYBR SHIELD MAX

KÖZEPES & NAGY SZERVEZETEK

OpenSOC XDR alapú kiterjesztett detektálás. Központi felügyelet, IT–OT–cloud láthatóság, automatikus válaszadás.

- XDR kiterjesztett detektálás
- IT–OT–cloud láthatóság
- Automatikus válaszadás

FLAGSHIP

// TIER_03

CYBR SHIELD PRO MAX

KRITIKUS INFRASTRUKTÚRA

Ultra Defense Level — teljes körű védelem. Több rétegű, vállalati szintű kibervédelem 24/7 SOC-felügyelettel.

- Több rétegű védelem
- 24/7 SOC felügyelet
- Vállalati szintű

// A CSOMAGOK DÍJAZÁSA MINDEN ESETBEN EGYEDI ÁRAJÁNLAT ALAPJÁN KERÜL MEGHATÁROZÁSRA.

KÖVETKEZŐ LÉPÉSEK

Hogyan indul el a közös munka.

1

Ajánlat visszaigazolása

Az ajánlat elfogadása és aláírása írásban, e-mailben.

2

Vizsgálati terjedelem egyeztetése

A vizsgálandó végpontok és szerverek listájának véglegesítése, az időablak kijelölése.

3

Telepítés indítása

Online konzultáció keretében a Deep Learning AI szoftver telepítése (kb. 1 óra).

4

2 hetes vizsgálati időszak

Folyamatos adatgyűjtés és mérnöki elemzés — üzletmenet-megszakítás nélkül.

5

Riport átadása

Vezetői összefoglaló, technikai részletek és prioritizált intézkedési terv átadása.

// SLA Az írásos visszaigazolás után a telepítés és a vizsgálat indulása jellemzően **1–2 munkanapon belül** megtörténik.

KAPCSOLAT

Várjuk megtisztelő válaszát.

// KAPCSOLATTARTÓ

Sági Roland

Operatív Igazgató

EMAIL roland.sagi@cyberoperations.hu

TEL +36 30 586 9850

WEB cyberoperations.hu

// CYBER OPERATIONS GROUP KFT.

HIGH-TECH SECURITY SOLUTIONS

SZÉKHELY 2481 Velence, Bográcsu. 1.

CÉGJEGYZÉK 07-09-035340

ADÓSZÁM 32449150-2-07