HOMOKOZÓBAN JÁTSZVA

A biztonságos elemzési környezet felépítése és buktatói.



Katus Gábor nb. alezredes
Nemzeti Kiberbiztonsági Intézet
Biztonsági Elemző Főosztály
Elemző osztály vezetője

LEVÉL ELEMZÉSE

Magyarország Ügyészségének nevével visszaélő 2026. szeptemberi ransomware-kampány.

TÁJÉKOZTATÁS

„Büntetőeljárás van folyamatban…”

Feladó: @outlook.hu
Hivatalos ügyészségi cím: @mku.hu

GOOGLE SHARE LINK

https[:]//share.google/X1975DGZdmzsJDjmH

HAMIS WEBOLDAL

ugyeszseg[.]hu[.]8yt45d[.]sbs

Káros állomány

Homokvári_Izolda_25375453-2-13_büntetőügy_iratai.hta

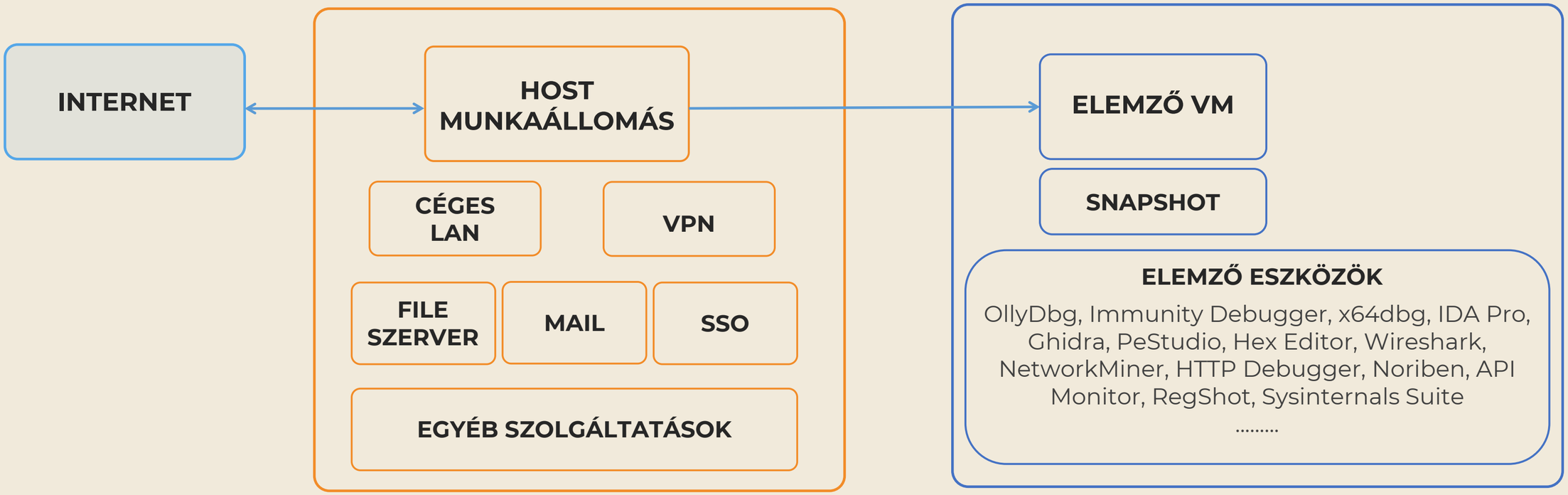
FIGYELEM!

Dokumentumok, képek, archívumok és más állományok titkosítása.

A felhasználó számára a lánc első része még legitimnek tűnhet.

ÉPÍTSÜNK GYORSAN EGY LABORT.

Van VM. Van Analysis Toolset. Van snapshot.



✓ külön VM ✓ snapshot ✓ sandbox

„Biztonságban vagyunk… igaz?”

ELSŐ INDÍTÁS.

Van VM. Van Analysis Toolset. Van snapshot.

Homokvári_Izolda_25375453-2-13_büntetőügy_iratai.hta

DOUBLE CLICK

...

10 másodperc múlva

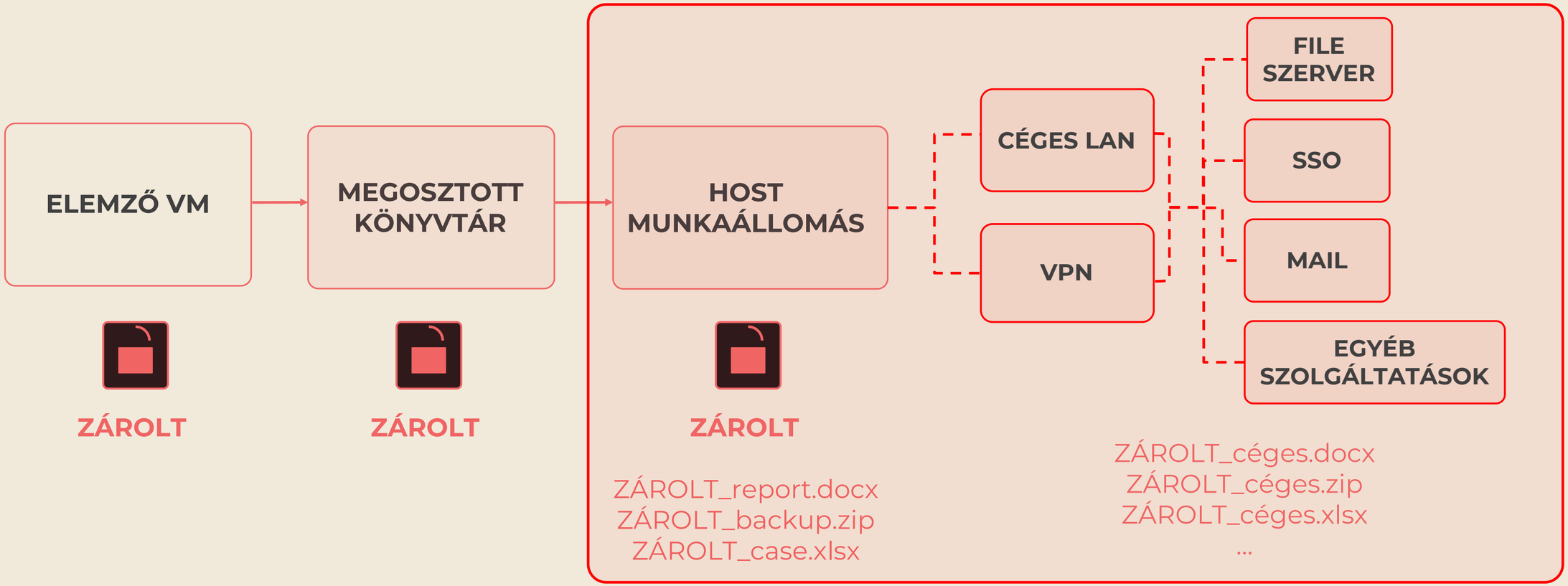
EREDMÉNY

Van VM. Van Analysis Toolset. Van snapshot.



A VM-ET VISSZAÁLLÍTJUK. ÉS A TÖBBIT?

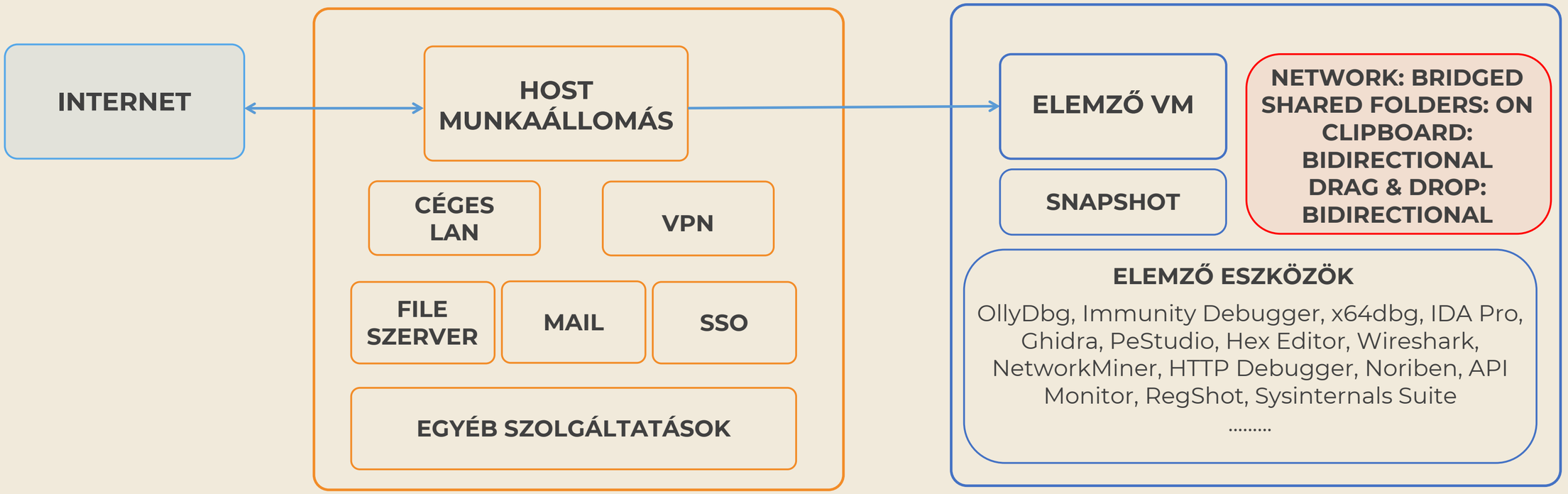
A rossz laborban az elemzési célpont és az értékes erőforrások között túl sok útvonal maradt.



„A snapshot a VM-et visszahozza, és a többit?”

ÉPÍTSÜNK GYORSAN EGY LABORT.

Mit csináltunk rosszul?



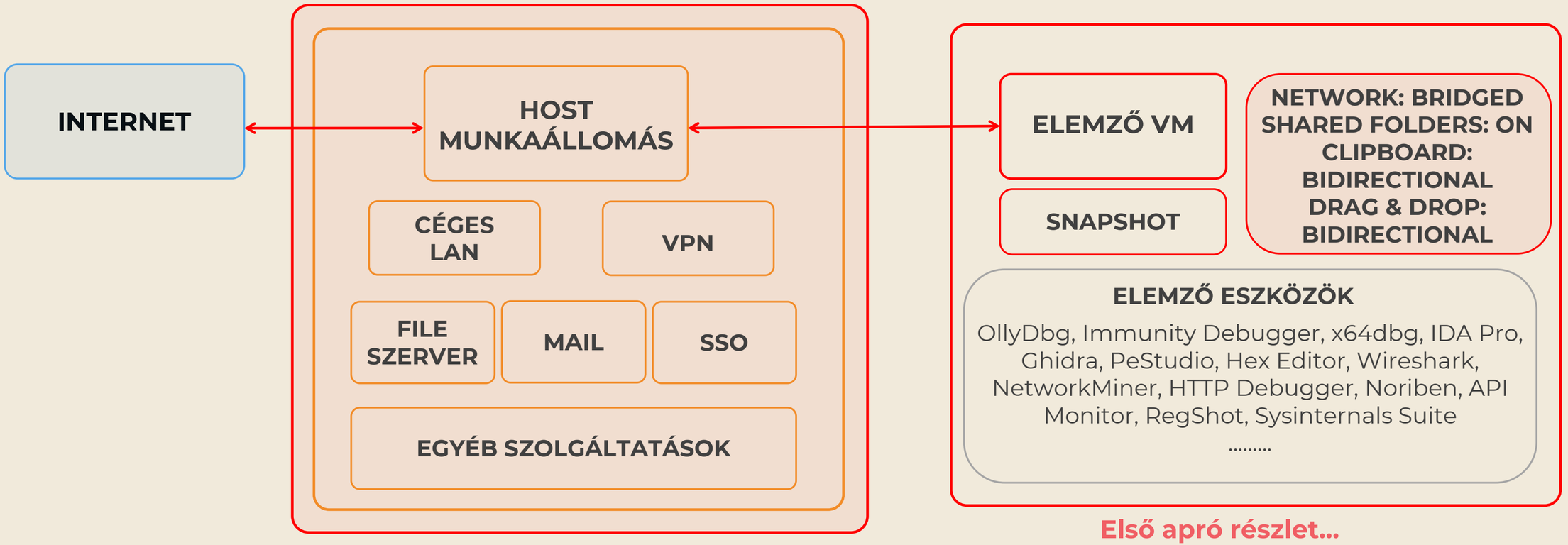
Első apró részlet...

✓ külön VM ✓ snapshot ✓ sandbox

„Biztonságban vagyunk... igaz?” Vagy mégsem?

ÉPÍTSÜNK GYORSAN EGY LABORT.

Mit rontottunk el?



CÉGES KÖRNYEZET
A host közben hozzáfér a vállalati erőforrásokhoz!

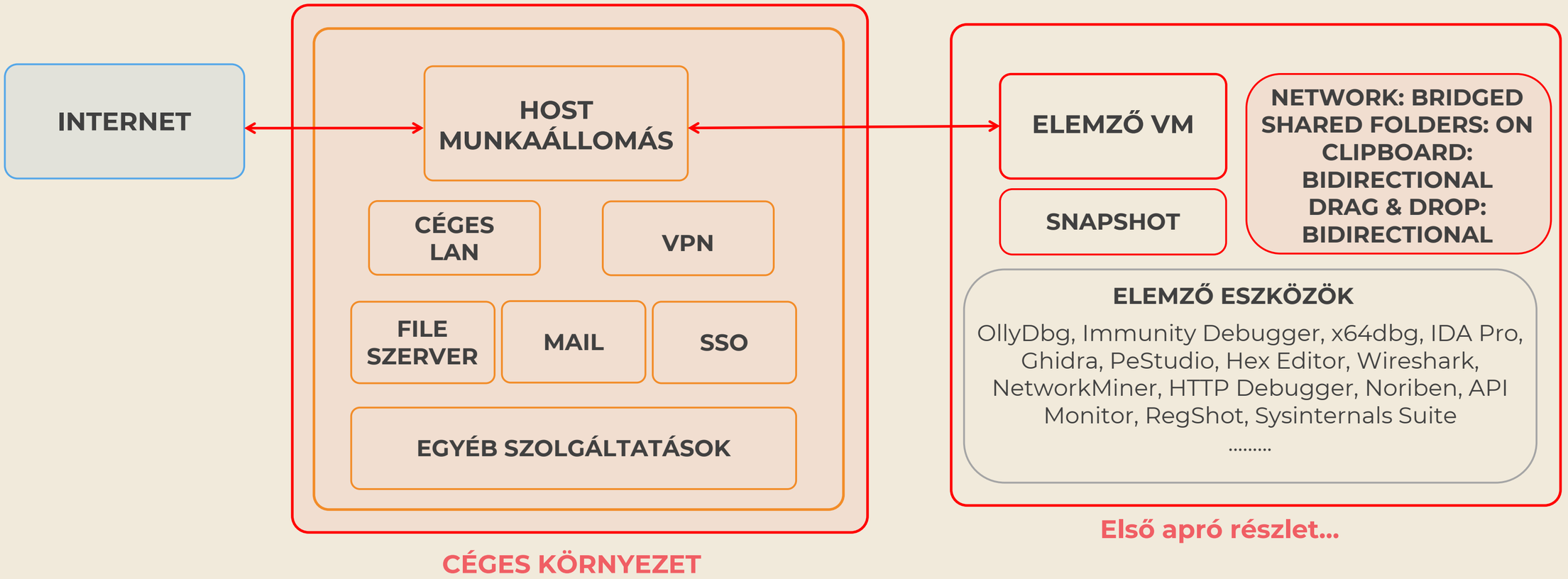
Első apró részlet...

✓ külön VM ✓ snapshot ✓ sandbox

„Bajba vagyunk?”

ÉPÍTSÜNK GYORSAN EGY LABORT.

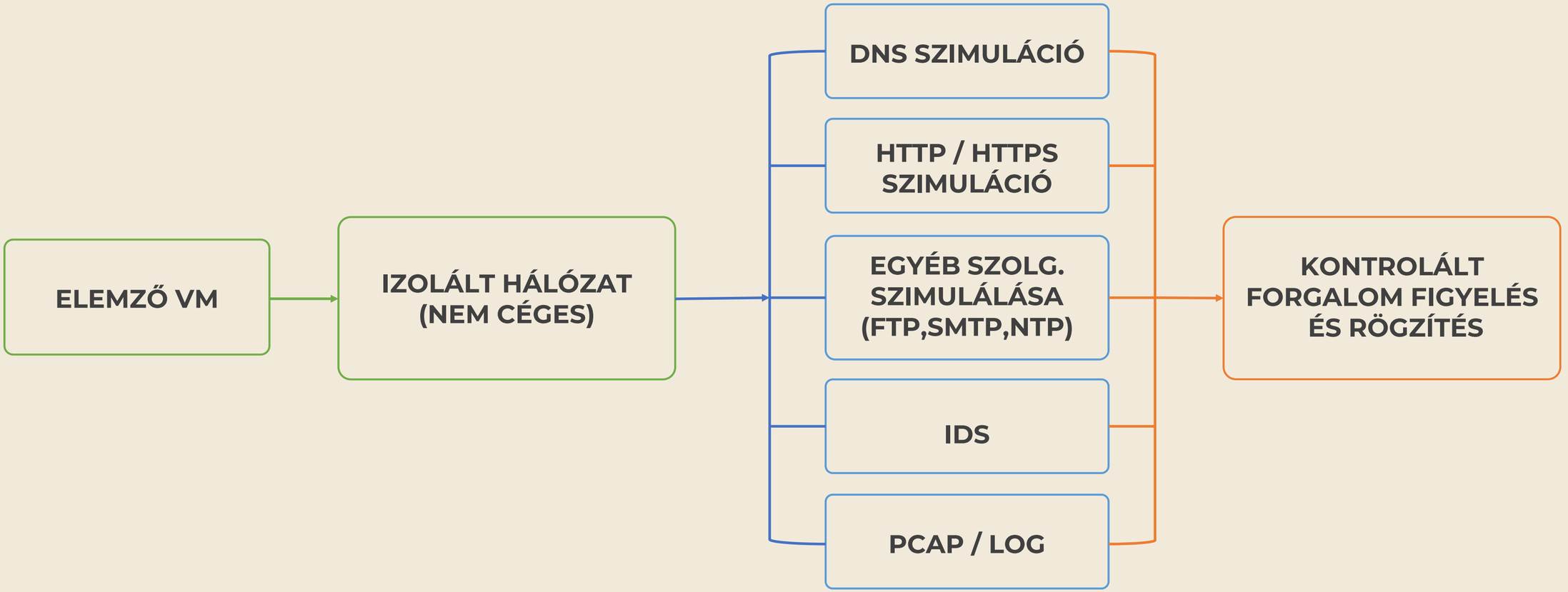
Nem egyetlen hiba volt — a kontrollok hiánya összeadódott.



A snapshot a visszaállítást segíti - nem az izolációt.

ELSŐ JAVÍTÁS: LEVÁLASZTJUK A HÁLÓZATOT.

Az elemzési hálózat ne legyen a vállalati hálózat része.



Nem azt akarjuk, hogy „ne csináljon semmit”.
Azt akarjuk látni, mit csinálni.

MÁSODIK JAVÍTÁS: BEZÁRJUK A FELESLEGES AJTÓKAT.

A kényelem nem lehet alapértelmezett adatút a host és a guest között.



Default deny: ami nem szükséges az elemzéshez, azt kikapcsoljuk.

HARMADIK JAVÍTÁS: AZ IDENTITÁST IS IZOLÁLJUK.

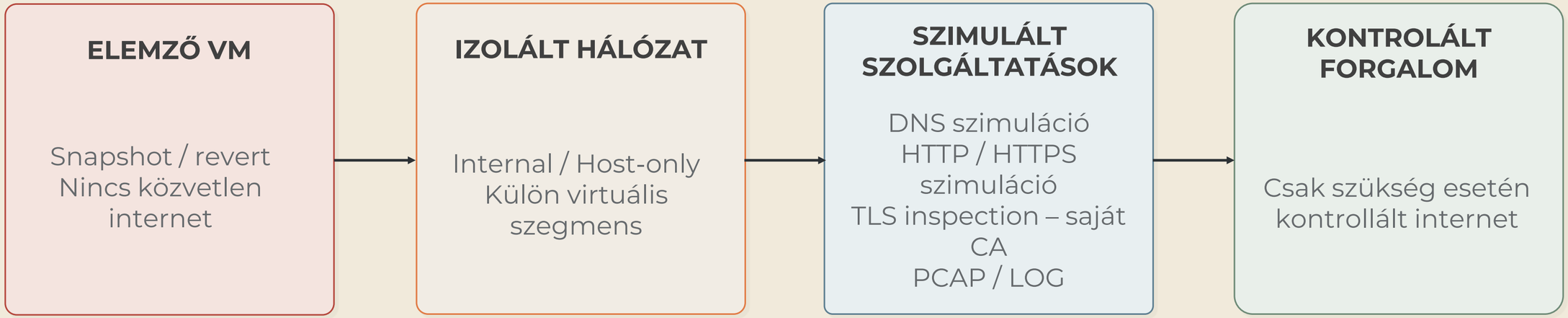
Az áldozat VM nem munkaállomás, nem használjuk másra.

NE VIDD BE	HELYETTE
Céges SSO	Teszt felhasználó
Valódi jelszavak	Dummy adatok
VPN profilok	Külön profil
SSH / API kulcsok	Minimális jog
Valódi dokumentumok	Eldobható környezet
Egyéb szolgáltatások	Hamis szolgáltatások

Az egész környezet legyen eldobható, de látszódjon valódinak.

ÉPÍTSÜNK OKOSAN EGY KONTROLLÁLT ÉS IZOLÁLT LABORT.

A minta csak kontrollált, megfigyelt hálózati szolgáltatásokkal kommunikálhat.

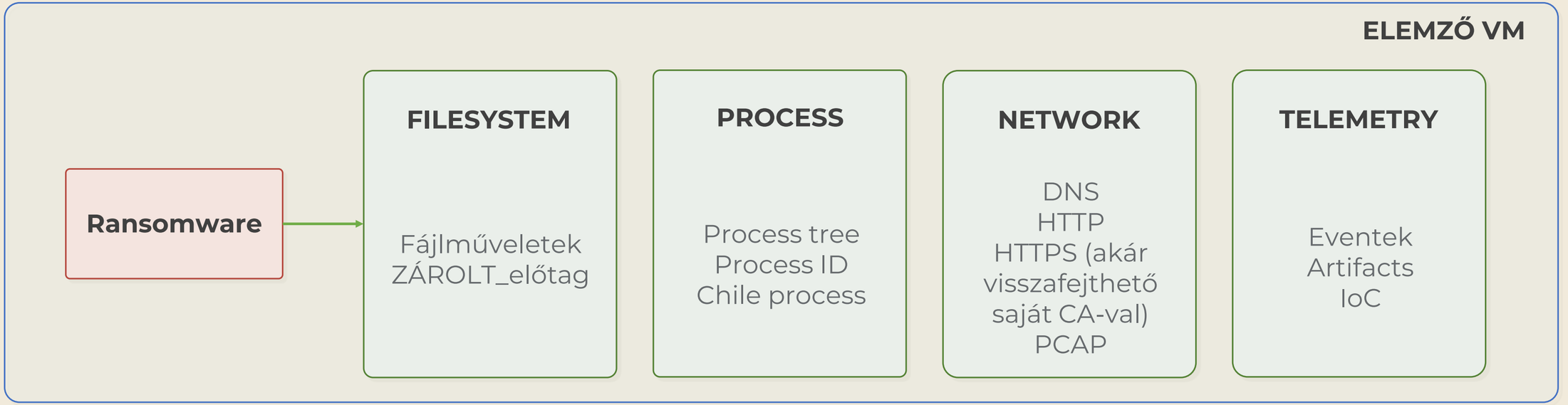


VM INTEGRÁCIÓK KIKAPCSOLVA Drag & Drop OFF | Shared Folder OFF | Clipboard OFF | USB passthrough OFF

A snapshot a visszaállítást segíti – az izolációt a hálózati kialakítás és a letiltott kapcsolatok adják.

UGYANAZ A RANSOMWARE. MÁSODIK FUTTATÁS.

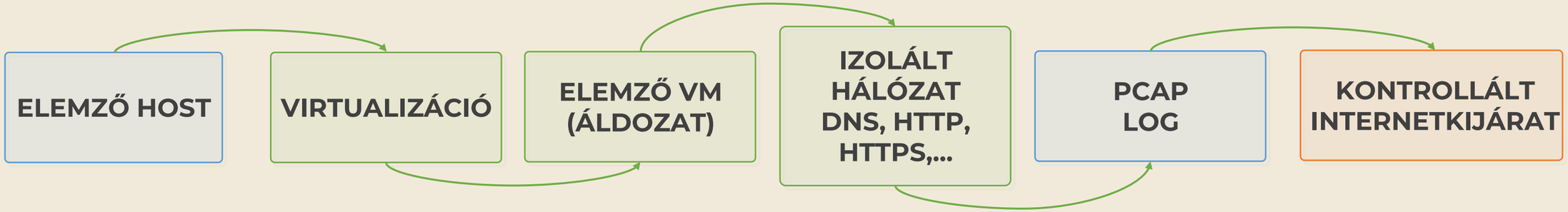
Most már nem ő figyel minket — mi figyeljük őt.



A host és hálózati telemetria, artefaktumok, IoC-k és viselkedési indikátorok kontrollált és izolált elemzői környezetben történő gyűjtése, elemzése és korrelációja.

A KÉSZ HOMOKOZÓ.

Rétegzett izoláció · megfigyelhetőség · reprodukálhatóság.



HOST: nincs éles hitelesítő adat

GUEST: tiszta VM állapot

HÁLÓZAT: nincs céges LAN

IGENTITÁS: tesztfiókok

MEGFIGYELÉS: telemetria

RESET: snapshot

sandbox != virtuális gép

KÜLÖNLEGESSÉGEK

A normál sandboxon túl.

01

ANTI-VM / ANTI-DEBUG

A malware felismerheti az elemzőkörnyezetet és megváltoztathatja a viselkedését.

02

FIZIKAI SANDBOX

Fizikai PC és teljes fizikai elemző infrastruktúra, ha a virtualizáció már befolyásolja a mintát.

03

AUTOMATIZÁLT ANALÍZIS

Automatizált malware elemző sandbox környezet, egy nagy komplex homokozó.

„Létezik egyáltalán a sandboxok Szent Grálja?”











Malware Analyzer Sandbox

https://sandbox.nki.gov.hu

Köszönöm a figyelmet!

Katus Gábor
gabor.katus@nki.gov.hu

NKI SANDBOX
sandbox@nki.gov.hu