EWS DISSZEMINÁCIÓ

PROGRAM:

09:00 - 09:10	KÖSZÖNTŐ dr. Bencsik Balázs, NBSZ-NKI igazgató
09:10 - 09:20	AZ EWS JOGSZABÁLYI HÁTTERE dr. Virányi Gergely, NBSZ-NKI
09:20 - 10:00	AZ EWS TECHNIKAI RÉSZLETEI Marsi Tamás, NBSZ-NKI
10:00 - 10:20	AZ EWS CSATLAKOZÁS TECHNIKAI KÉRDÉSEI Paulovics Miklós, NISZ Zrt.
10:20 - 10:45	KÉRDÉSEK-VÁLASZOK-KONZULTÁCIÓ

SZÉCHENYI 2020
MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Szociális Alap
BEFEKTETÉS A JÖVŐBE

KÖFOP-2.2.2-VEKOP-16-2016-00001

KÖFOP KERETÉBEN MEGVALÓSULÓ FEJLESZTÉSEK IT BIZTONSÁGÁNAK NÖVELÉSE, EZÁLTAL RENDSZEREKKEL ÖSSZEFÜGGŐ KORRUPCIÓS LEHETŐSÉGEK ÉS KOCKÁZATOK CSÖKKENTÉSE

KÖSZÖNTŐ

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE

KÖFOP-2.2.2-VEKOP-16-2016-00001

KÖFOP KERETÉBEN MEGVALÓSULÓ FEJLESZTÉSEK IT BIZTONSÁGÁNAK NÖVELÉSE, EZÁLTAL RENDSZEREKKEL ÖSSZEFÜGGŐ KORRUPCIÓS LEHETŐSÉGEK ÉS KOCKÁZATOK CSÖKKENTÉSE

AZ EWS JOGSZABÁLYI HÁTTERE

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE

AZ EWS-RŐL SZÓLÓ KORMÁNYRENDELET

- 214/2020. (V. 18.) Korm. Rendelet
- A szolgáltatás nyújtására az NBSZ került kijelölésre
- Jogosultak köre:
  - Ibtv. jogalanyok
  - Alapvető szolgáltatást nyújtók
  - Bejelentés köteles szolgáltatók
  - Európai vagy nemzeti létfontosságú rendszerelemek üzemeltetői
  - Központosított informatikai és elektronikus hírközlési szolgáltatók

KÖTELEZETTEK

- Kötelező igénybe venni:
  - Kormányzati Adatközpontban elhelyezett rendszerek esetében
  - KÖFOP-VEKOP Felhívás alapján NKI kezdeményezésére

VÉDETT INTÉZMÉNY KÖTELEZETTSÉGEI

- Csatlakozás érdekében együttműködés a rendszer üzemeltetőjével
- Az üzemeltetés során együttműködés a szolgáltatás korlátozásának, ellehetetlenítésének megakadályozása érdekében
- Rendszer-, szolgáltatásfejlesztés tervezetten, előre egyeztetett módon

VÉDETT INTÉZMÉNY JOGOSULTSÁGA

- Egyedi felhasználói felületen ellenőrizheti:
  - Az EWS által generált biztonsági naplót
  - Hibajelzéseket
  - Az események státuszát
  - Statisztika

RENDSZER-ÜZEMELTETŐ TEVÉKENYSÉGE

- Hálózati forgalom monitorozása
- A fenyegetésre utaló jelzéseket detektálja
- Biztonsági esemény bekövetkezésekor a rendszer a védett szervezeten túl, a CSIRT-et is értesíti

ADATVÉDELEM

- Az EWS koncepciója adatvédelmi szempontból átgondolt
  - figyelembe veszi a hatályos hazai jogszabályi környezetet
  - Műszaki adatkezésnek több jogalapja is van
  - illeszkedik az EU-s jogszabályokhoz, stratégiákhoz

- Az EWS fenntartója elkötelezett az adatvédelem mellett
  - átláthatóság: korábbi adatvédelmi audit, adatfeldolgozási szerződés
  - nemzetbiztonságilag ellenőrzött személyi állomány és telephelyek
  - jogszabályi előírások és legjobb gyakorlatokat szerinti IT biztonság

ADATVÉDELEM

- Teljes hálózati forgalom 14 napig
- A forgalom kivonata, jelzések, biztonsági napló 5 évig

kerül eltárolásra

Az adatokba betekinthet:

- Védett intézmény
- A központosított szolgáltató
- Eseménykezelő központ

KÖFOP-2.2.2-VEKOP-16-2016-00001

KÖFOP KERETÉBEN MEGVALÓSULÓ FEJLESZTÉSEK IT BIZTONSÁGÁNAK NÖVELÉSE, EZÁLTAL RENDSZEREKKEL ÖSSZEFÜGGŐ KORRUPCIÓS LEHETŐSÉGEK ÉS KOCKÁZATOK CSÖKKENTÉSE

AZ EWS TECHNIKAI HÁTTERE

SZÉCHENYI 2020

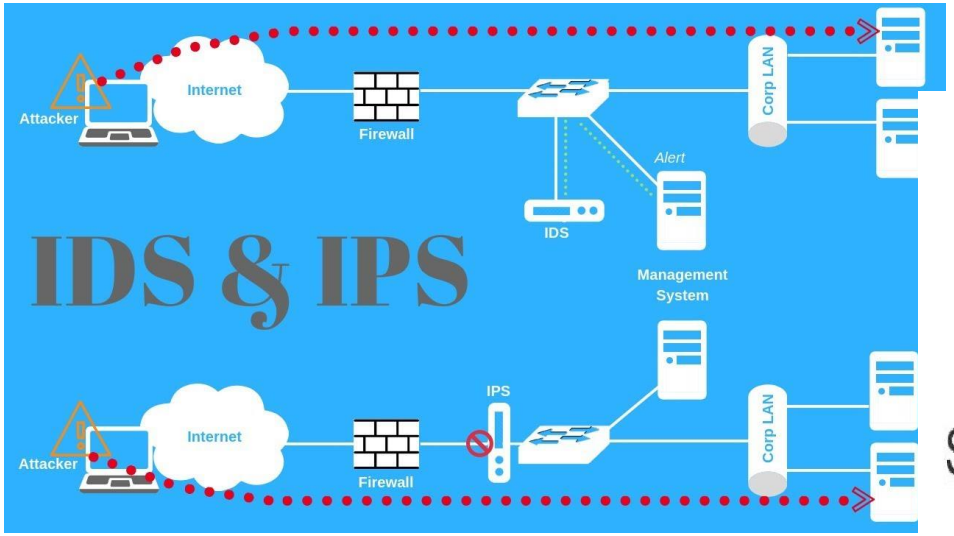
MAGYARORSZÁG KORMÁNYA

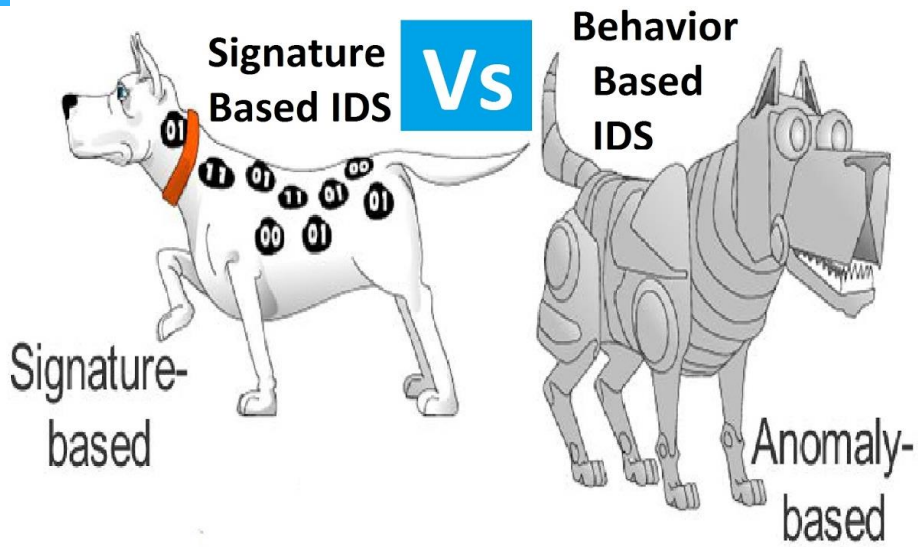
Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE

IDS-IPS

- IDS vs IPS
- Sziganatúraillesztés
- Anomáliadetekció





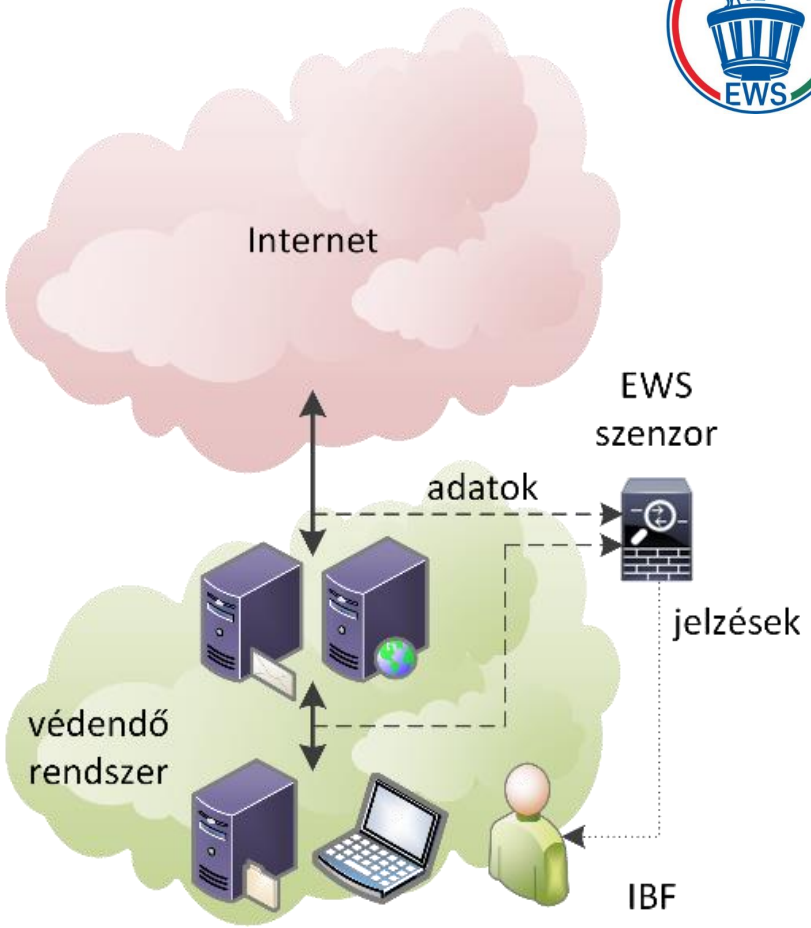
ALAPOK

- EWS: Early Warning System
  - Nemzetközi minták alapján
  - Központosított hálózatbiztonsági felügyeleti szolgáltatás

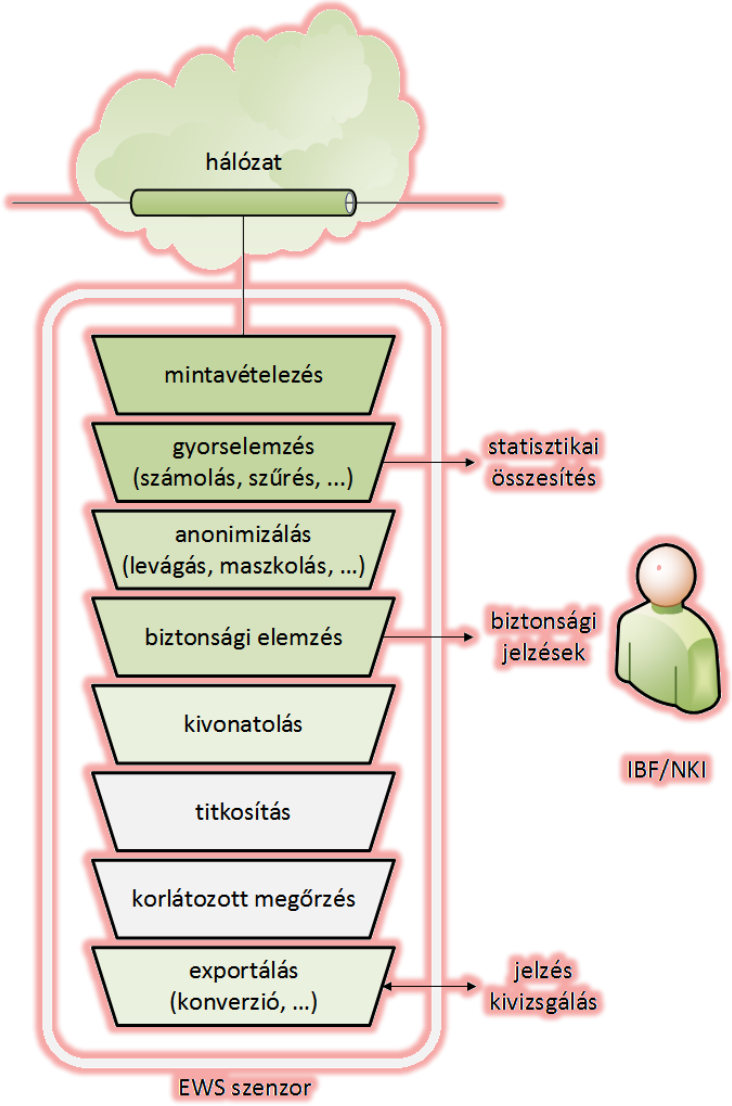
- Definíció
  - Egyirányúan összekapcsolt
  - Információs rendszerek hálózati forgalma
    - Elemzés
    - Kockázatok azonosítása
    - Támadás, visszaélés, kísérlet azonosítása
  - Szolgáltatás védett rendszereknek

FUNKCIÓK, FELÉPÍTÉS

- Több, mint IDS
  - Riasztások
  - Netflow
  - Nyers hálózati forgalom
  - Elemzési lehetőség
- EWS szenzor
  - IDS: Suricata
  - Forgalomgyűjtés és elemzés: Archime
- Központi rendszer
  - Elastic – kibana
  - Támogató portál



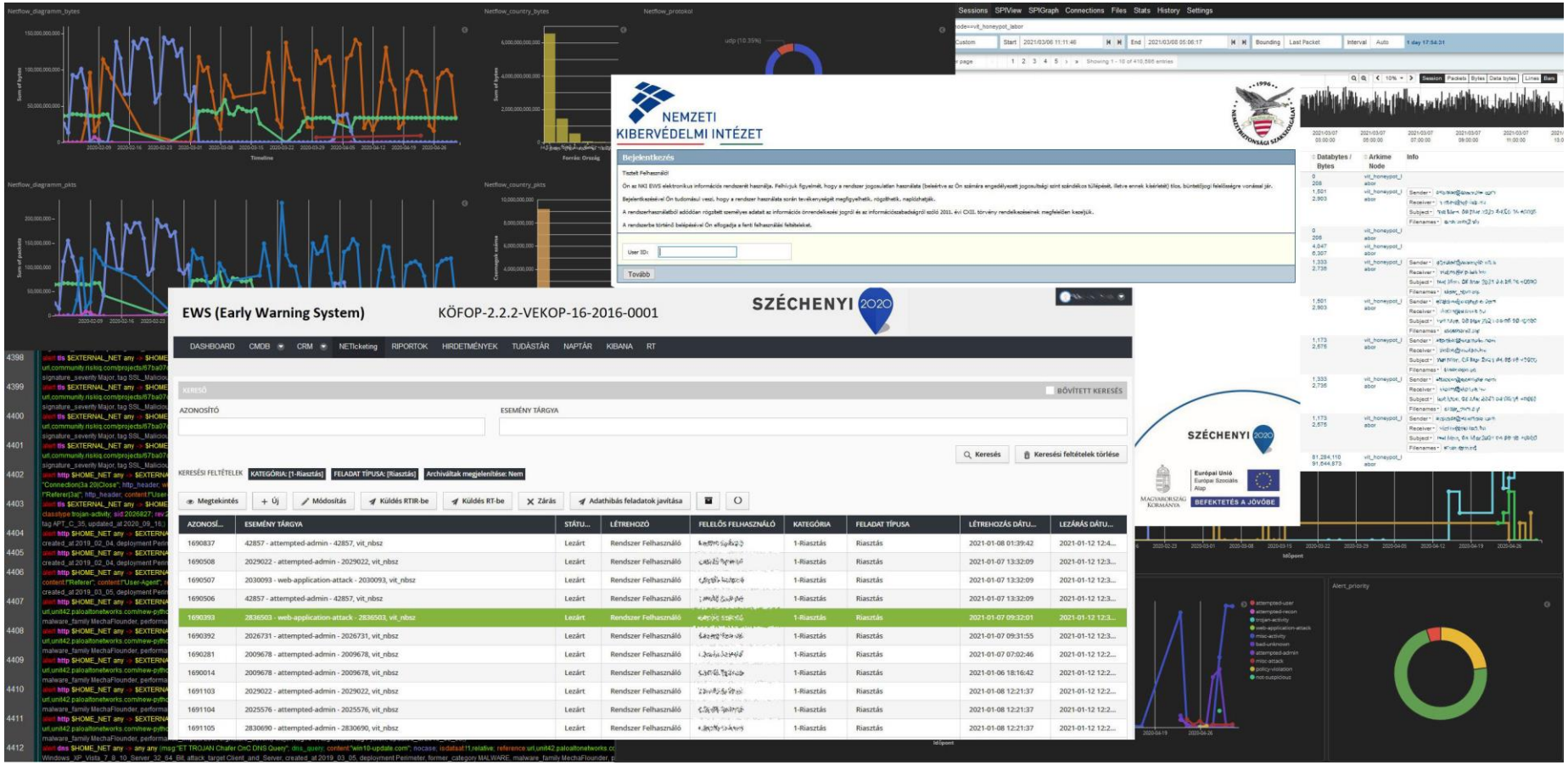
MŰKÖDÉS


hálózat
mintavételezés
gyorselemzés
(számolás, szűrés, ...)
anonimizálás
(levágás, maszkolás, ...)
biztonsági elemzés
kivonatolás
titkosítás
korlátozott megőrzés
exportálás
(konverzió, ...)
statisztikai
összesítés
biztonsági
jelzések
IBF/NKI
jelzés
kivizsgálás
EWS szenzor

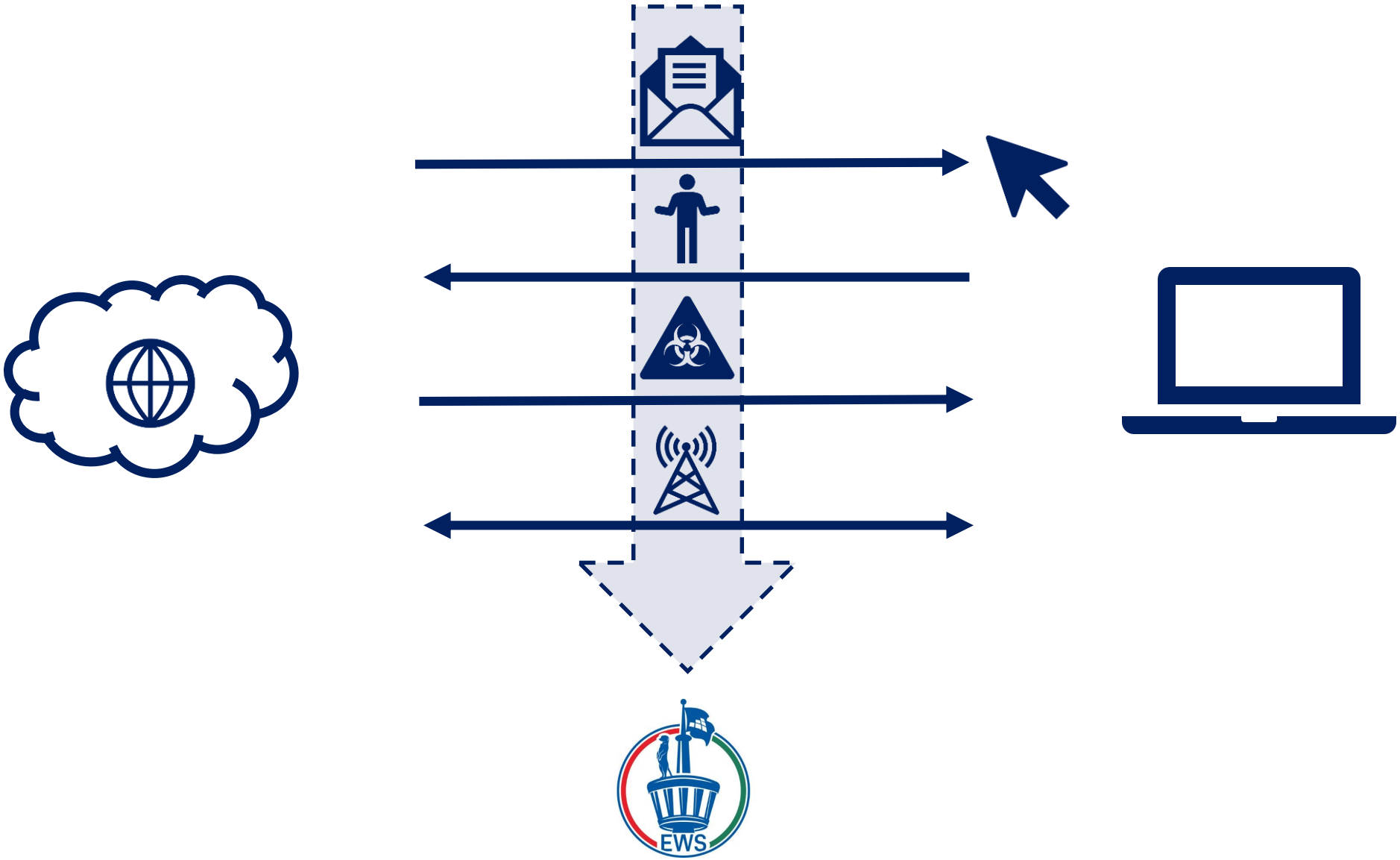
ELŐNYÖK

- Korszerű technológia
- Csökkennek az incidens kivizsgáláshoz kapcsolódó adminisztratív terhek
- Gyorsul a támadásokkal kapcsolatos reakció képesség
- Saját ticketing funkció
  - Nyomonkövetés
  - Incidens bejelentés az NKI-CSIRT-nek
- GDPR kompatibilis
- Folyamatosan aktuális szabálykészlet

EWS

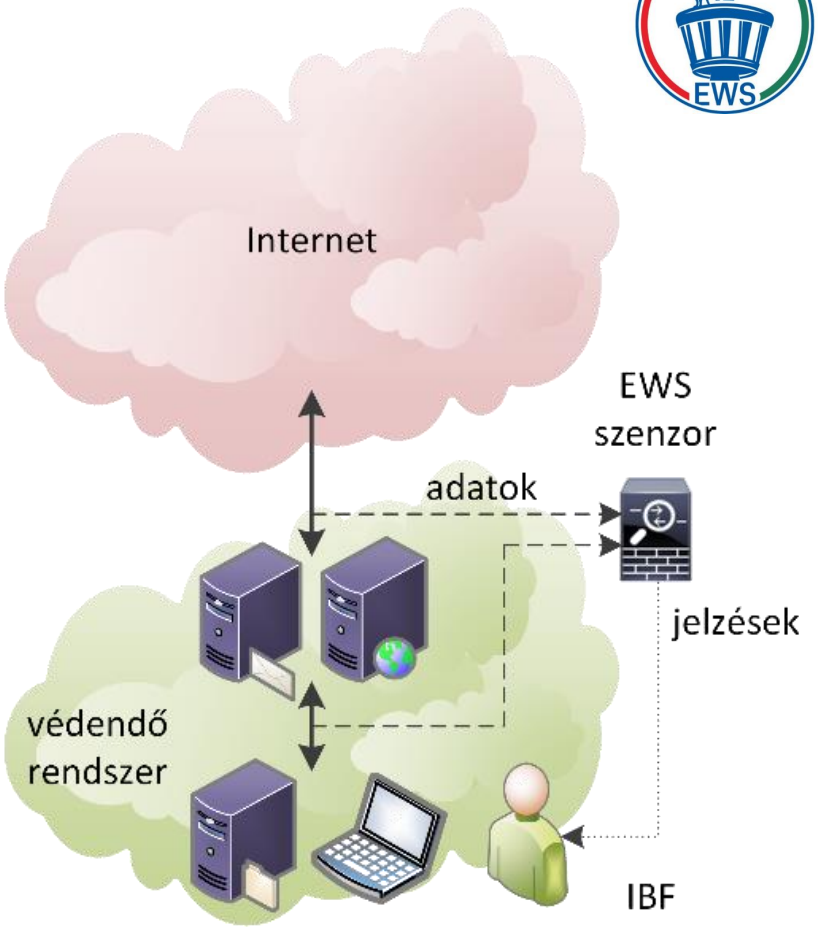

NEMZETI KIBERVÉDELMI INTÉZET
Bejelentkezés
EWS (Early Warning System)
KÖFOP-2.2.2-VEKOP-16-2016-0001
SZÉCHENYI 2020
DASHBOARD
CMDB
CRM
NETicketing
RIPORTOK
HIRDETMÉNYEK
TUDÁSTÁR
NAPTÁR
KIBANA
RT
AZONOSÍTÓ
ESEMÉNY TÁRGYA
Keresés
Keresési feltételek törlése
Megtekintés
Új
Módosítás
Küldés RTIR-be
Küldés RT-be
Zárás
Adathibás feladatok javítása
AZONOSÍ...
ESEMÉNY TÁRGYA
STÁTU...
LÉTREHOZÓ
FELELŐS FELHASZNÁLÓ
KATEGÓRIA
FELADAT TÍPUSA
LÉTREHOZÁS DÁTU...
LEZÁRÁS DÁTU...
BEFEKTETÉS A JÖVŐBE

GYAKORLAT

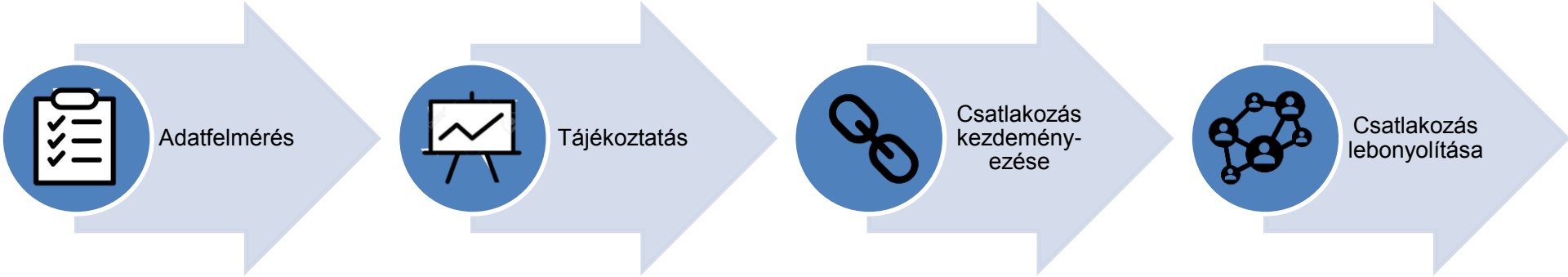


CSATLAKOZÁS (ÁLTALÁNOS)

- Csatlakozás műszaki követelmények
  - Hálózati forgalom átadása (tap/mirror)
  - Titkosítás feloldása
  - Kritikus hálózati csomópontok kialakítása
  - Naplókezelési minimumkövetelmények



CSATLAKOZÁSI FOLYAMAT



CSATLAKOZÁS

- Ha NISZ-KAK felhő
  - Egyszerű
  - Két opció

- Egyéb esetben tárgyalás szükséges

- Csatlakozási kérelem űrlap
  - NISZ és NBSZ-NKI közös formanyomtatványa
  - Word kitöltése
  - Aláírás és pecsét
  - E-mailben mindkét szervezetnek elküldeni
  - Részletes kitöltési útmutató

CSATLAKOZÁS

Korai figyelmeztető rendszer (EWS) csatlakozás adatkérő lap

Intézményi és rendszer adatok			
Intézmény neve*		Rendszer neve*	
Üzemeltető szervezet neve		Rendszer rövid neve	
Projekt KÖFOP azonosító		A rendszer éles?*	Igen / nem /fog futni de még nincs publikálva**
Az rendszer éles szolgáltatásait nagyságrendileg igénybe vevő felhasználói számossága			pl. 500 user
A opció *,***: A rendszer a NISZ-KAK-ban található, az SSL terminálás a NISZ KAK F5 perimeter eszközén valósul meg jelenleg is	[ ]	B opció *,***: A rendszer a NISZ-KAK-ban található, az SSL terminálás NEM a NISZ KAK F5 Perimeter eszközén valósul meg (részletes leírás alul)	[ ]

Kapcsolati adatok

Kapcsolattartó neve*	Kapcsolattartó szerepe*	E-mail cím(ek)*	Telefonszám	Státusz*
	IBF / VITO / INC / TECH **			aktív / passzív **
	IBF / VITO / INC / TECH **			aktív / passzív **
	IBF / VITO / INC / TECH **			aktív / passzív **
	IBF / VITO / INC / TECH **			aktív / passzív **

Rendszer részletes adatai (csak az éles sík kicsatolása szükséges az EWS irányába)

Publikus IP(k)*	Publikus port(ok)*	KAK (Privát) IP(k)*	KAK port*	VLAN ID	Megjegyzés
pl. 84.206.105.123	pl. 443	pl. 100.0.15.175	pl. 80	pl. 5474	

Időablak(ok) a beállítások élesítéséhez	

Megjegyzés

Kérelem és hozzájárulás*

Alulírott a fent nevezett szervezet nevében eljárva kérem a fent nevezett rendszer forgalmának kicsatolását az EWS rendszer irányába és a rendszer illesztését.

Hozzájárulok a forgalom kicsatolásához*** [ ]	Nem járulok hozzá a forgalom kicsatolásához*** [ ]

Dátum, aláírás és pecsét*

Kelt: ……, 2021. …… Hó …… Nap	……

nki.gov.hu/ews • nisz.hu
@ ewscsatlakozas@nki.gov.hu • helpdesk@nisz.hu és másolatban netsec@nisz.hu
☎ NKI: +36-1-336-4840 (Eseményészlelés)

KÖFOP-2.2.2-VEKOP-16-2016-00001

KÖFOP KERETÉBEN MEGVALÓSULÓ FEJLESZTÉSEK IT BIZTONSÁGÁNAK NÖVELÉSE, EZÁLTAL RENDSZEREKKEL ÖSSZEFÜGGŐ KORRUPCIÓS LEHETŐSÉGEK ÉS KOCKÁZATOK CSÖKKENTÉSE

AZ EWS CSATOLÁS

SZÉCHENYI 2020

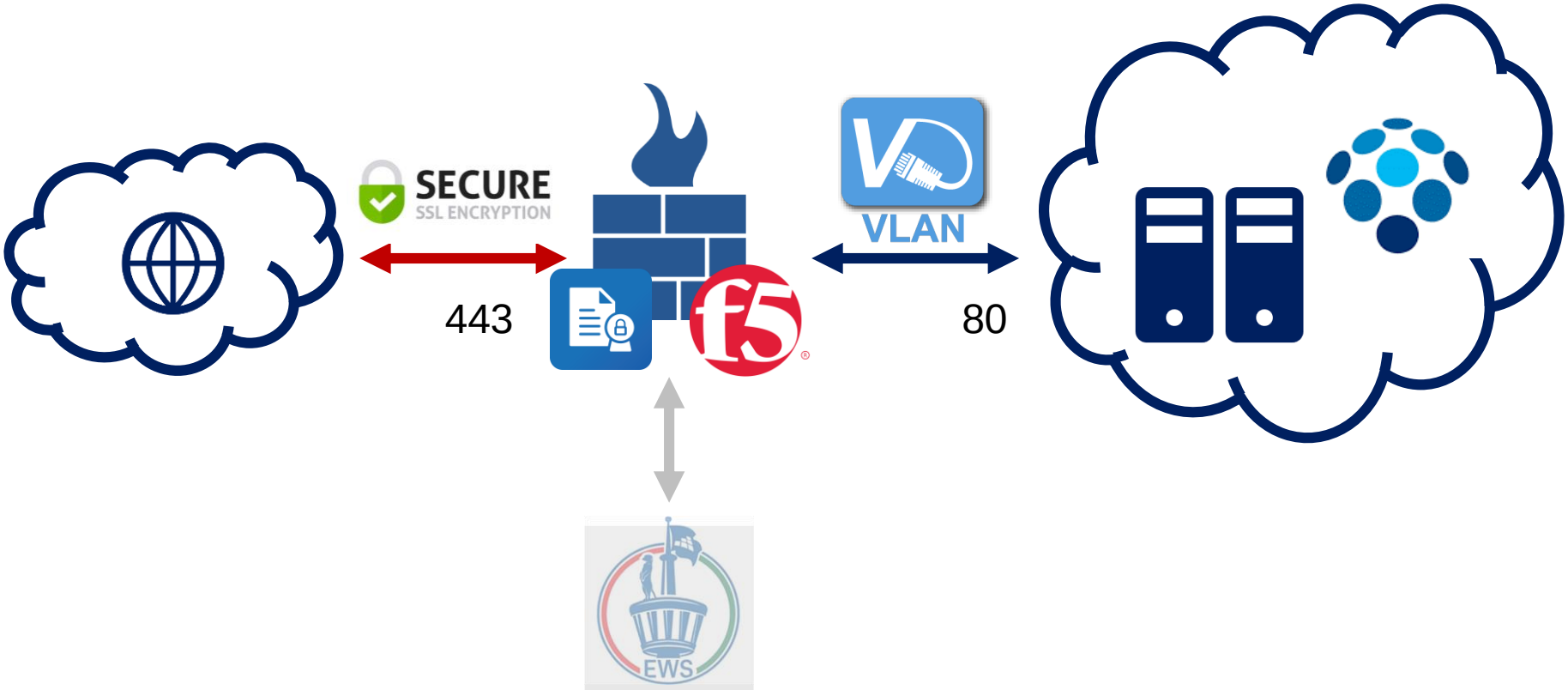
MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE

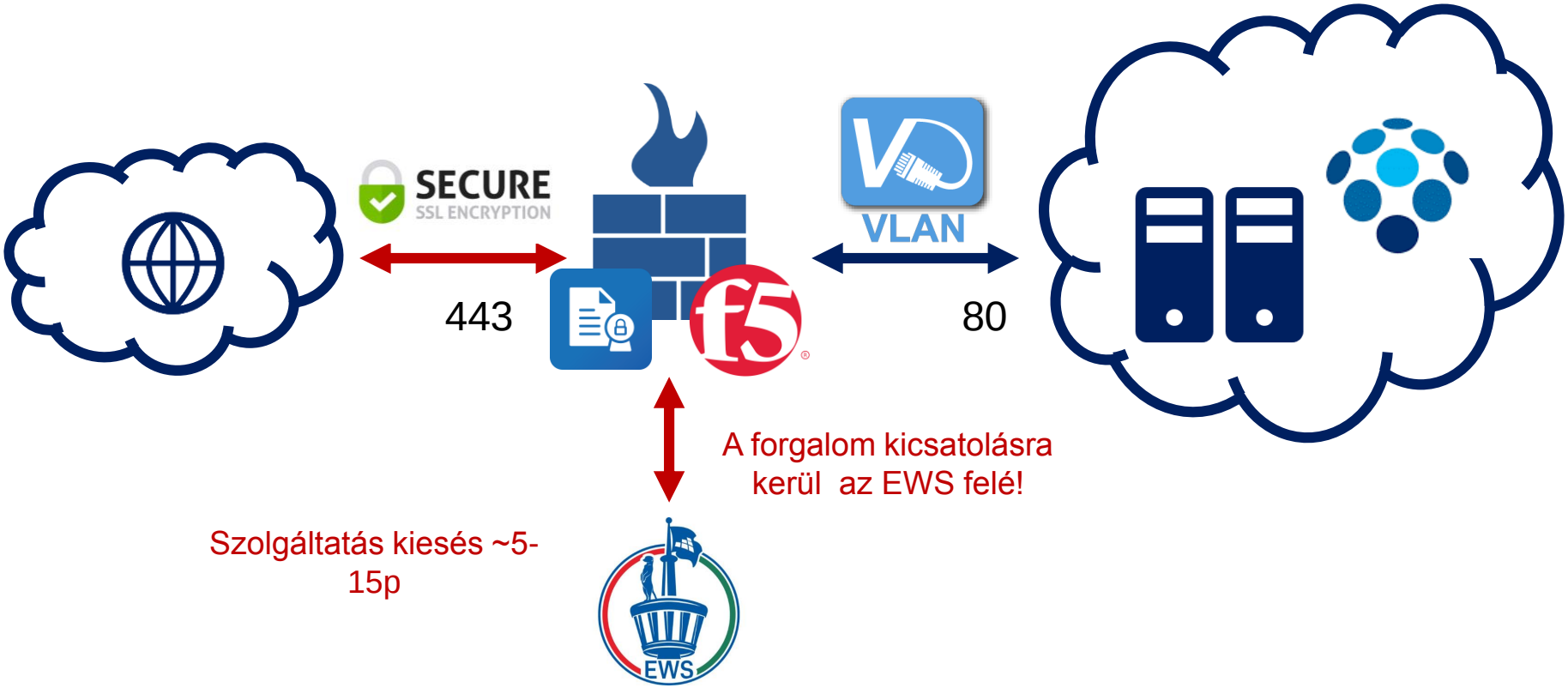
EWS CSATOLÁS

- NISZ-Kormányzati adatközpont felhő
- „**A**” opció
  - SSL offload az F5-ön végződik
  - Illesztés: adatkérő lap



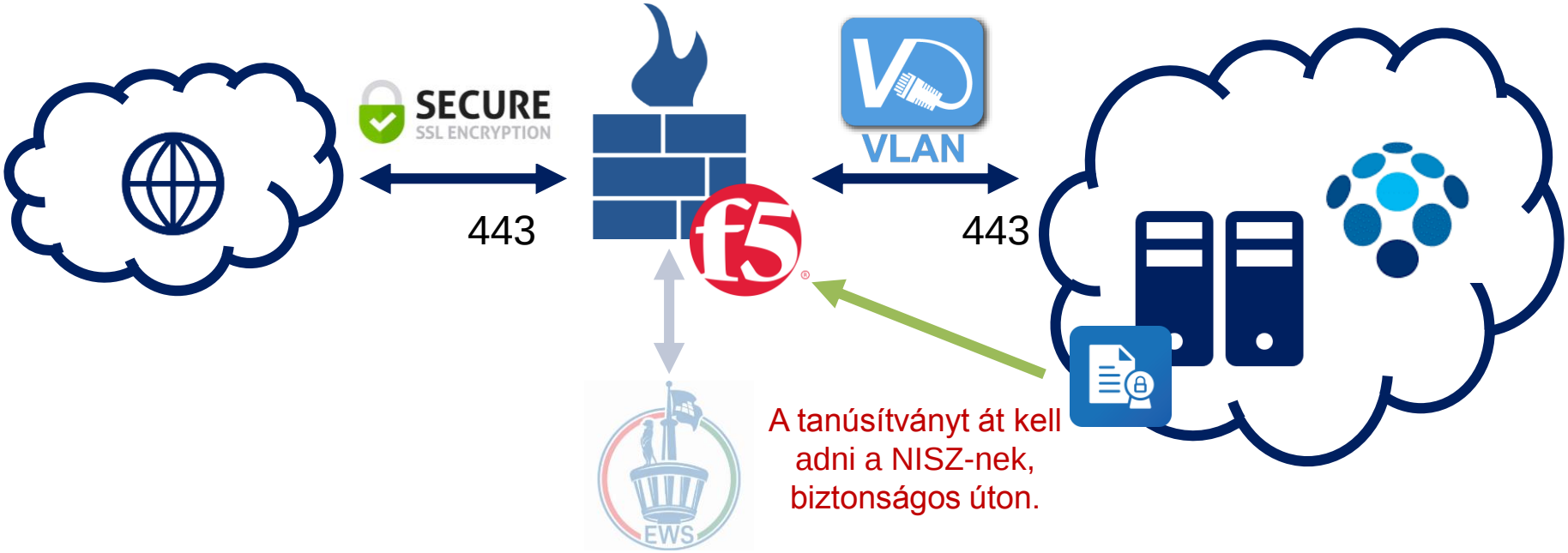
EWS CSATOLÁS

- NISZ-Kormányzati adatközpont felhő
- „**A**” opció
  - SSL offload az F5-ön
  - Illesztés: adatkérő lap



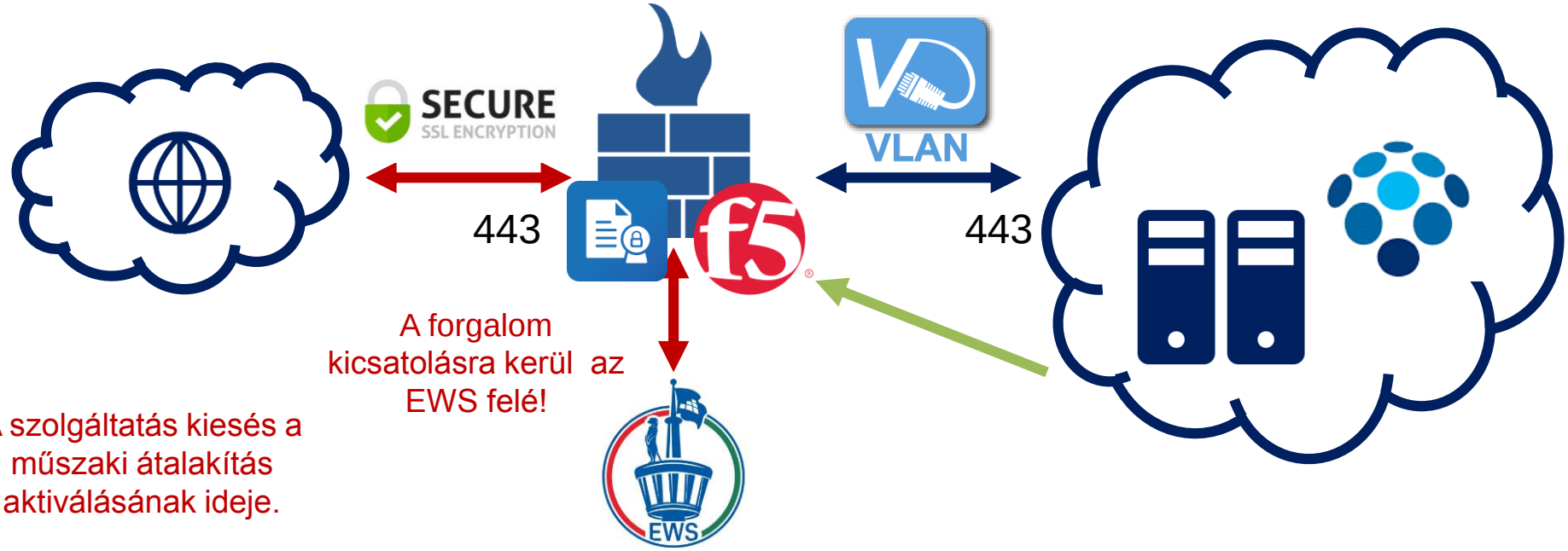
EWS CSATOLÁS

- NISZ-Kormányzati adatközpont felhő
- „B” opció
  - SSL offload szerveren (pl. egy VM-en) végződik
  - Illesztés: SSL terminálást át kell helyezni a az F5-re (a tanúsítványt át kell adni a NISZ részére) az adatkérő lapot ugyanúgy ki kell tölteni. Mérnöki együttműködést kíván.
  - Érdemes teszt rendszeren kipróbálni



EWS CSATOLÁS

- NISZ-Kormányzati adatközpont felhő
- **„B**” opció
  - SSL offload tenantban (pl. egy VM-en) végződik
  - Illesztés: SSL terminálást át kell helyezni a az F5-re (a tanúsítványt át kell adni a NISZ részére) az adatkérő lapot ugyanúgy ki kell tölteni. Mérnöki együttműködést kíván.
  - Érdemes teszt rendszeren kipróbálni



EWS CSATOLÁS

- Egyéb helyszín pl. NISZ-KAK hosting
  - Mindig egyedi tárgyalások szükségesek
  - NBSZ-NKI-nál vagy (ügyfél esetén) a NISZ-nél is kezdeményezhető
  - Szenzor valószínűleg szükséges
  - Kicsatolást és SSL terminálást egyedileg kell megoldani
  - Érdemes a tesztrendszeren (ha van) kipróbálni
  - Minden egyéb konfigurációmódosítást az ügyélnek kell kérni (Változó tűzfalszabályok …stb.)
  - Költség: kb. max. 40-50 M Ft

KÉRDÉSEK?

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE

KÖSZÖNJÜK A FIGYELMET!

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE