JOGSZABÁLYI KÖVETELMÉNYEK ÉS MEGOLDÁSOK A NIS 2 ÉGISZE ALATT

Jogszabályi követelmények és megoldások a NIS 2 égisze alatt

2024/04/11

BLACK CELL
Protecting critical infrastructures

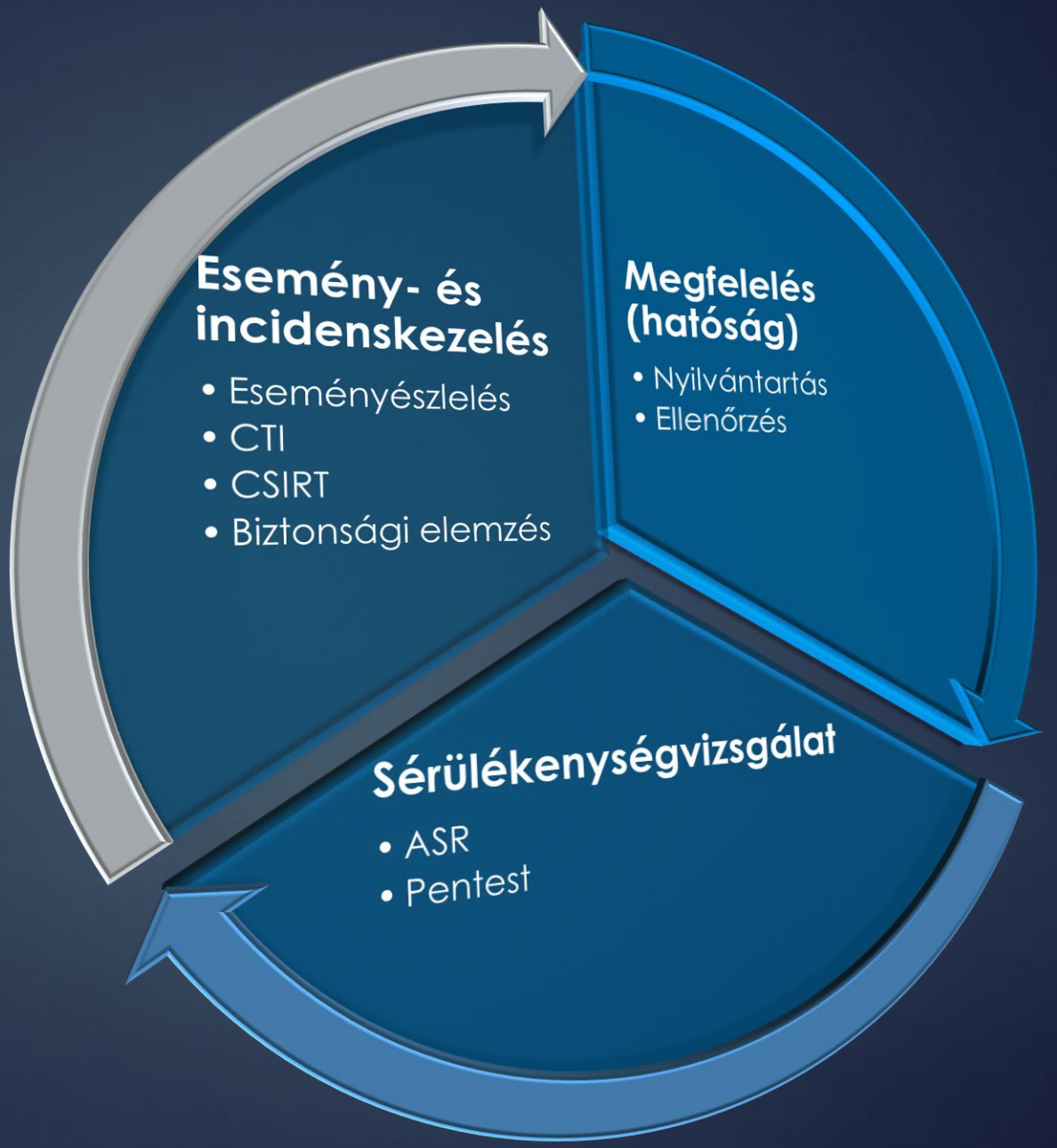
FOURSYS
CONSOLUTION

TLP:CLEAR

NIS2 és új Ibtv.

Marsi Tamás
NBSZ NKI
tamas.marsi@nki.gov.hu

NKI


Esemény- és incidenskezelés
• Eseményészlelés
• CTI
• CSIRT
• Biztonsági elemzés
Megfelelés (hatóság)
• Nyilvántartás
• Ellenőrzés
Sérülékenységvizsgálat
• ASR
• Pentest

NIS Directive

Critical Entities Resilience Directive (CER)

NIS2 Directive

JOGI KÖRNYEZET ALAKULÁSA

LRTV utódja 2012. évi CLXVI. törvény

IBTV utódja 2013. évi L. törvény

41/2015. (VII.15.) BM rendelet átdolgozása

2023. évi XXIII. törvény kibertanúsítás

A jövő

4 KIBERBIZTONSÁGI HATÓSÁG

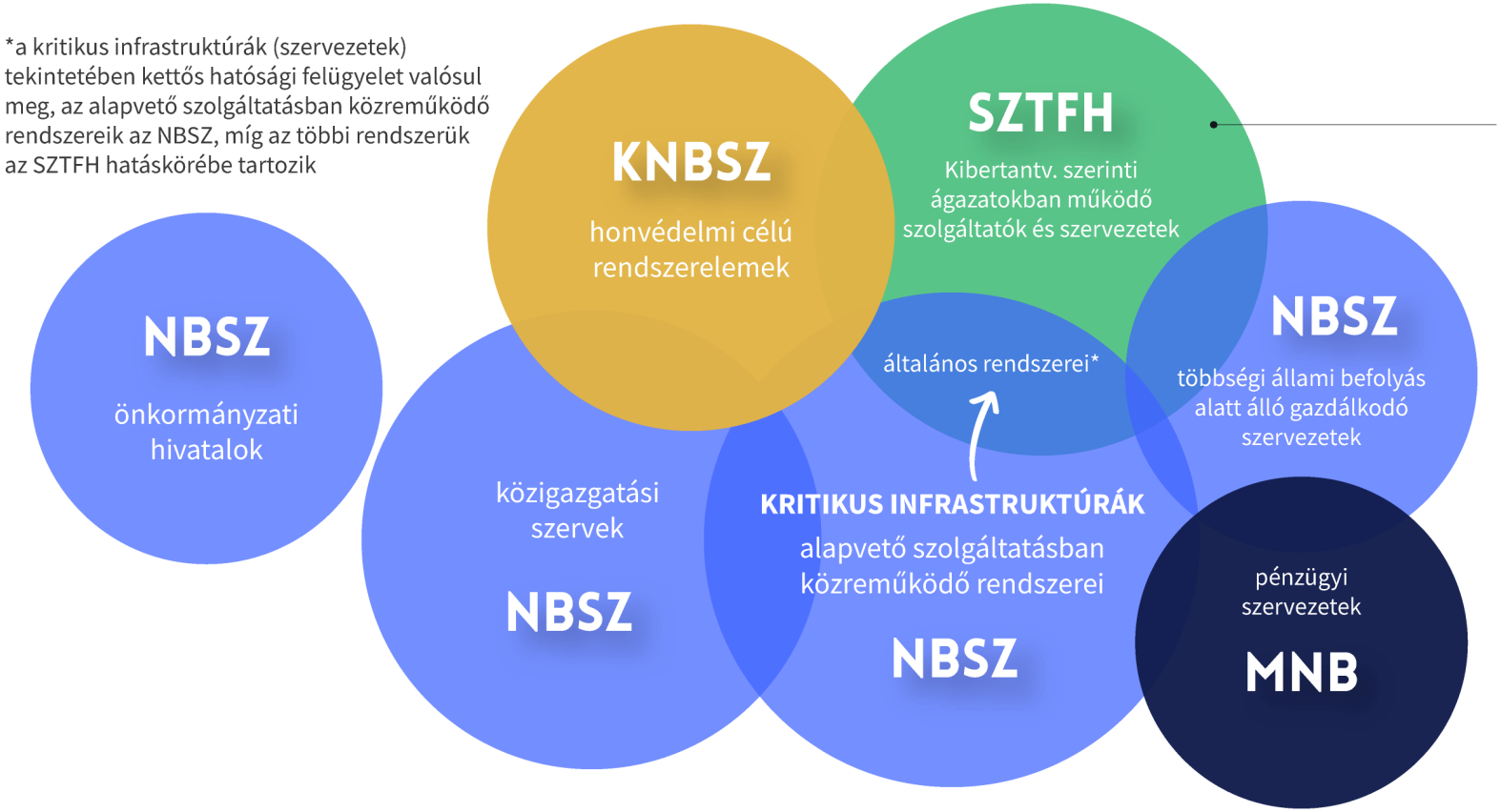
NIS2	NIS2 közigazgatás ágazat és kritikus szervezetek (kivéve DORA)	DORA	Honvédelmi ágazat
SZTFH Szabályozott Tevékenységek Felügyeleti Hatósága	1996 Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet	Magyar Nemzeti Bank	Katonai Nemzetbiztonsági Szolgálat A Hazáért becsülettel

A törvény hatálya megbontásra kerül:

- **felügyelet** (hatóság)
- **incidenskezelés** (CSIRT)
- **sérülékenységvizsgálat**

Ki kihez tartozik?

*a kritikus infrastruktúrák (szervezetek) tekintetében kettős hatósági felügyelet valósul meg, az alapvető szolgáltatásban közreműködő rendszereik az NBSZ, míg az többi rendszerük az SZTFH hatáskörébe tartozik



Energetika, Közlekedés, Egészségügy, Ivóvíz, szennyvíz, Hírközlési szolgáltatás, Digitális infrastruktúra, Kihelyezett IKT szolgáltatások, Űralapú szolgáltatás, Postai és futárszolgálatok, Élelmiszer előállítása, feldolgozása és forgalmazása, Hulladékgazdálkodás, Vegyszerek előállítása és forgalmazása, Gyártás, Digitális szolgáltatók, Kutatás

Biztonsági osztály és szint

Biztonsági szintbe sorolás kivezetése

Biztonsági osztályba sorolás

- biztonsági osztályoknál 3 fokozatú skála: **alap, jelentős, magas**
- összhang a kiberbiztonsági tanúsítási rendszerrel és a követelményrendszer alapját képező NIST 800-53-mal

Követelményrendszer

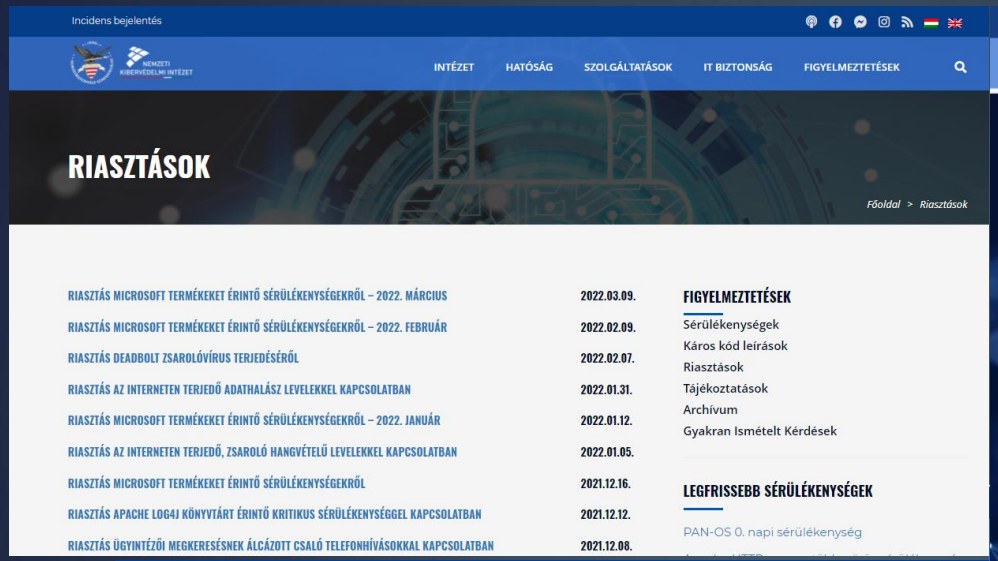
Alapja: **NIST 800-53 rev.5**

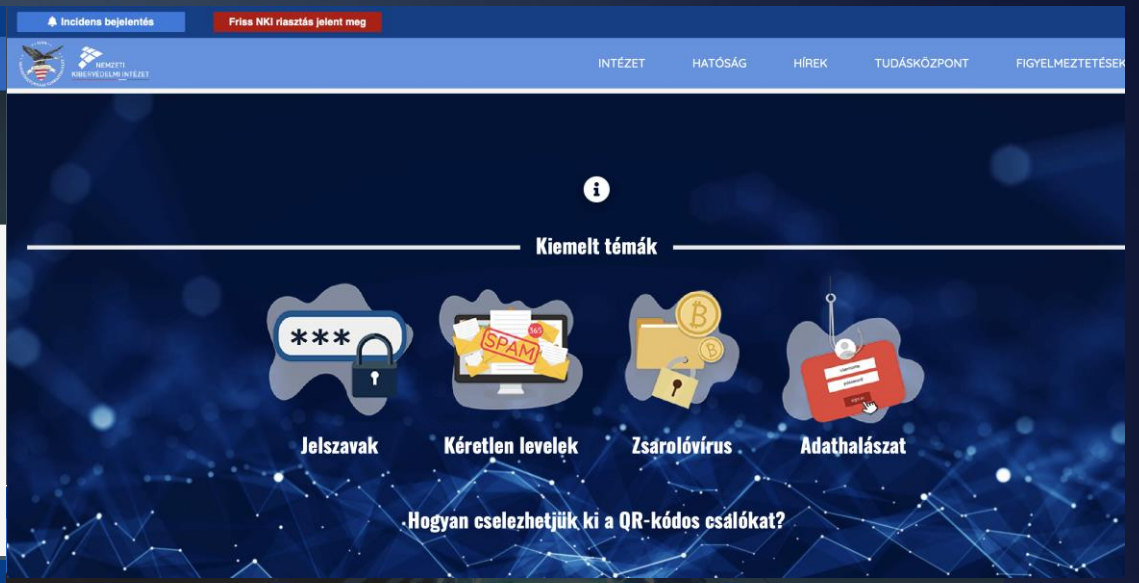
KÖZÖS

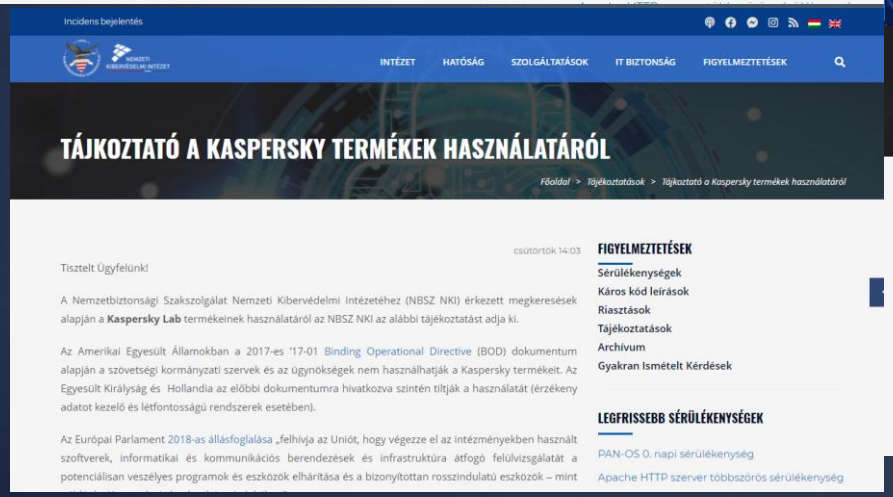
+külön felhő és OT követelményrendszer

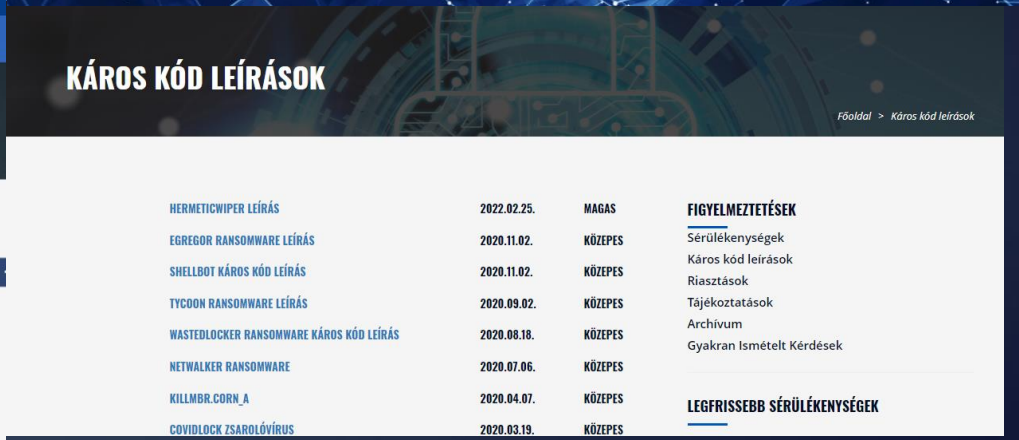
- **3 kategória** (alap, jelentős, magas)
- kockázatelemzés alapján **testreszabható**
- **intézkedések csoportosítása változik**
  (adminisztratív, fizikai, logikai helyett kontroll családok szerint)
- intézkedések **BSR besorolása megszűnik**
- **kiegészítő védelmi intézkedések** megjelenése
- TÁRSADALMI EGYEZTETÉS LEZAJLOTT, **HATÁLYBALÉPÉS BÁRMIKOR VÁRHATÓ**

Hol tájékozódjak?









Köszönöm a figyelmet!

tamas.marsi@nki.gov.hu

Kibertámadás! podcast

LinkedIn

nki.gov.hu

JOGSZABÁLYI KÖVETELMÉNYEK ÉS MEGOLDÁSOK A NIS 2 ÉGISZE ALATT

BLACK CELL
Protecting critical infrastructures

FOURSYS
CONSOLUTION

TLP:CLEAR

Fájni fog-e vagy sem a 23-as hatás?

Szabályozással egy biztonságosabb kibertérért

MINDEN KIBERÜL

Bor Olivér

kiberbiztonsági és kommunikációs szakértő

egyetemi vendégoktató

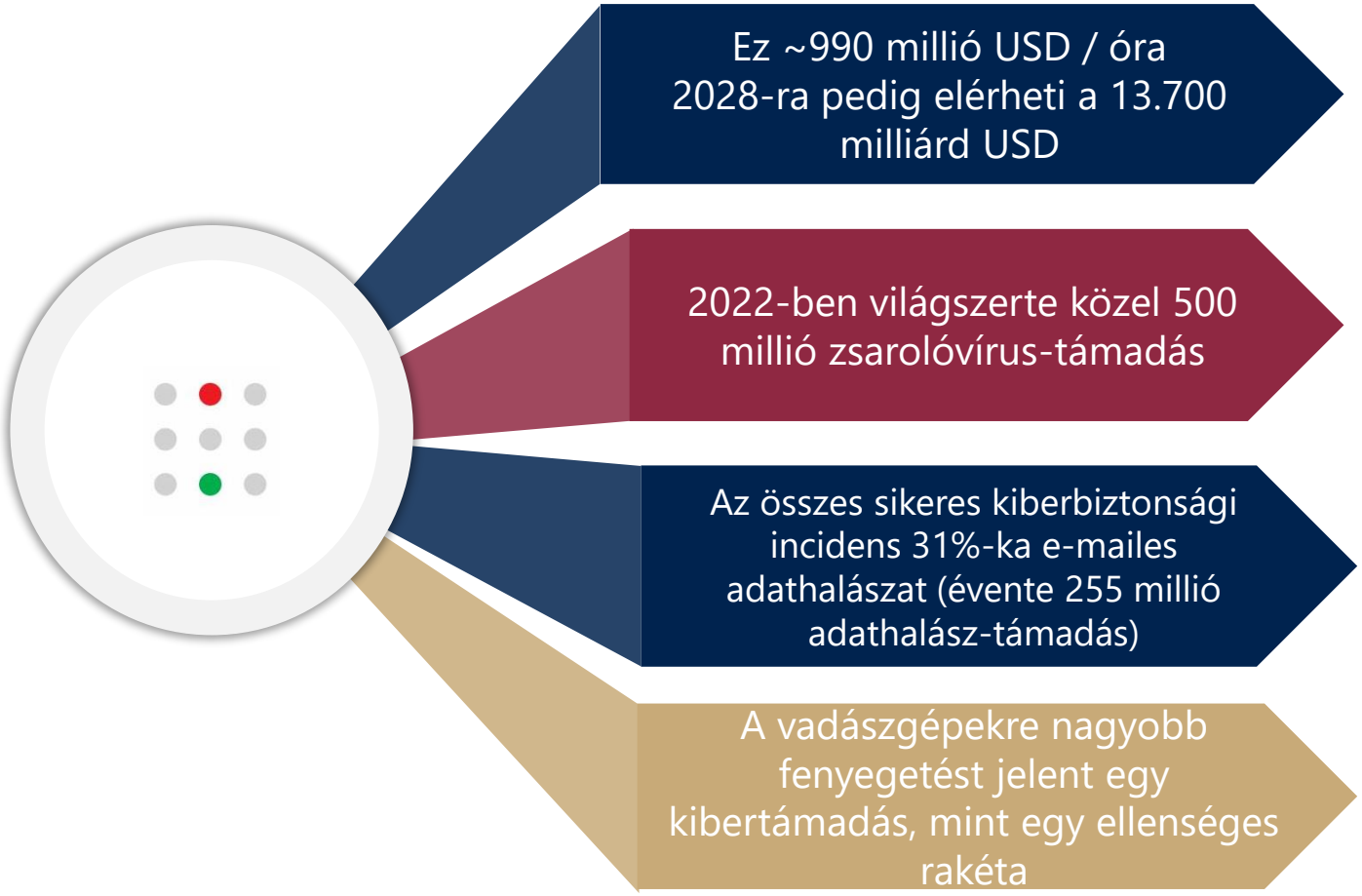
Két féle szervezet...

2012 **ROBERT MUELLER, FBI**

There are only two types of companies:
those that **have been hacked**,
and those that **will be**.

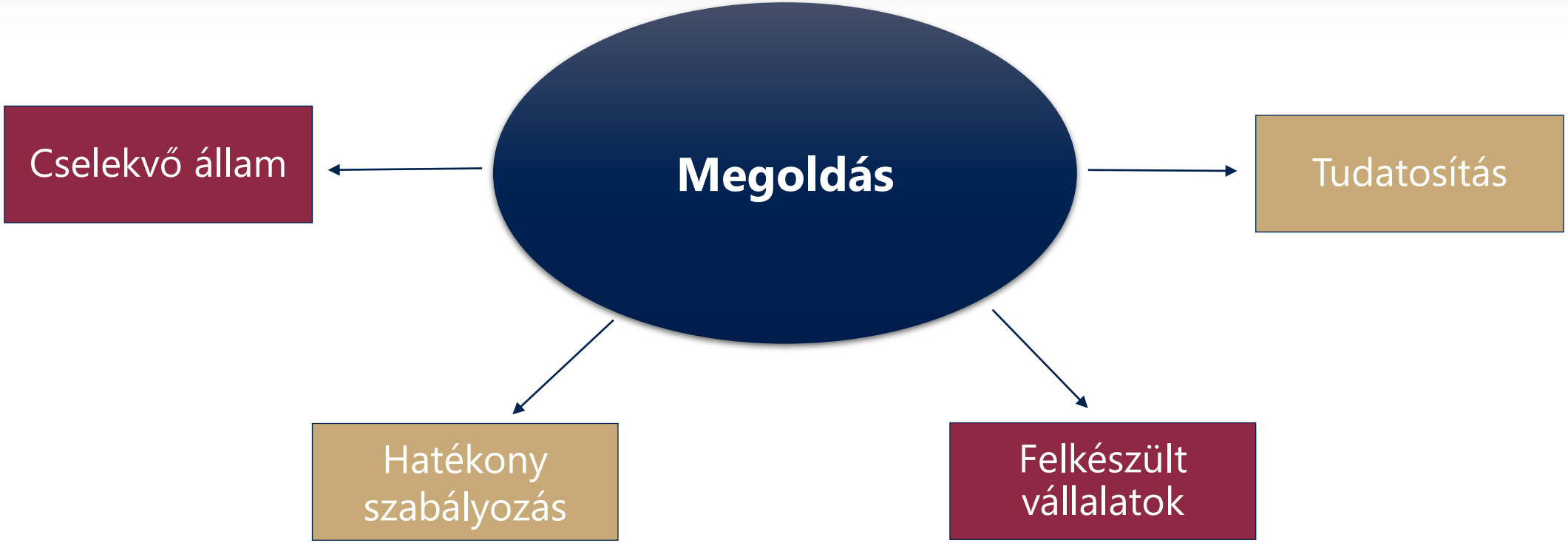
Nincs kegyelem – tényleg fáj

A kiberbűnözők által elkövetett támadások globális kárértéke 2023-ban: kb. 8000 milliárd USD



- Pénzügyi szféra
- IKT szektor
- Digitális szolgáltatások

Kihívások és válaszok



Kibertan.tv – 2023. évi XXIII. törvény

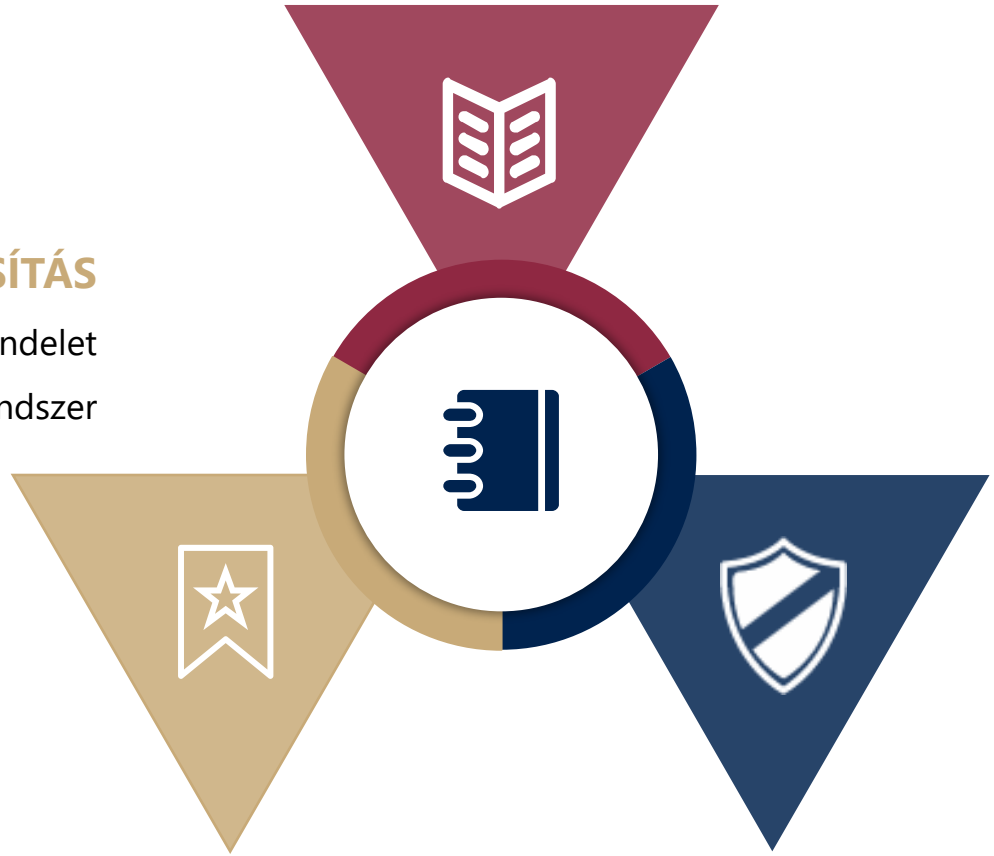
a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvény

ÉRTELMEZŐ RENDELKEZÉSEK

KIBERBIZTONSÁGI TANÚSÍTÁS

2019/881 (EU) rendelet

Nemzeti tanúsítási keretrendszer



KIBERBIZTONSÁGI FELÜGYELET

2022/2555 (EU) irányelv – NIS2

Kiberbiztonsági felügyelet – érintett szervezetek

Kiberbiztonsági felügyelet – érintett feladatai

Vezetői feladatok

Biztonságért felelős személy

Szervezeti szabályozások

Tudatosító oktatások és szinten tartás

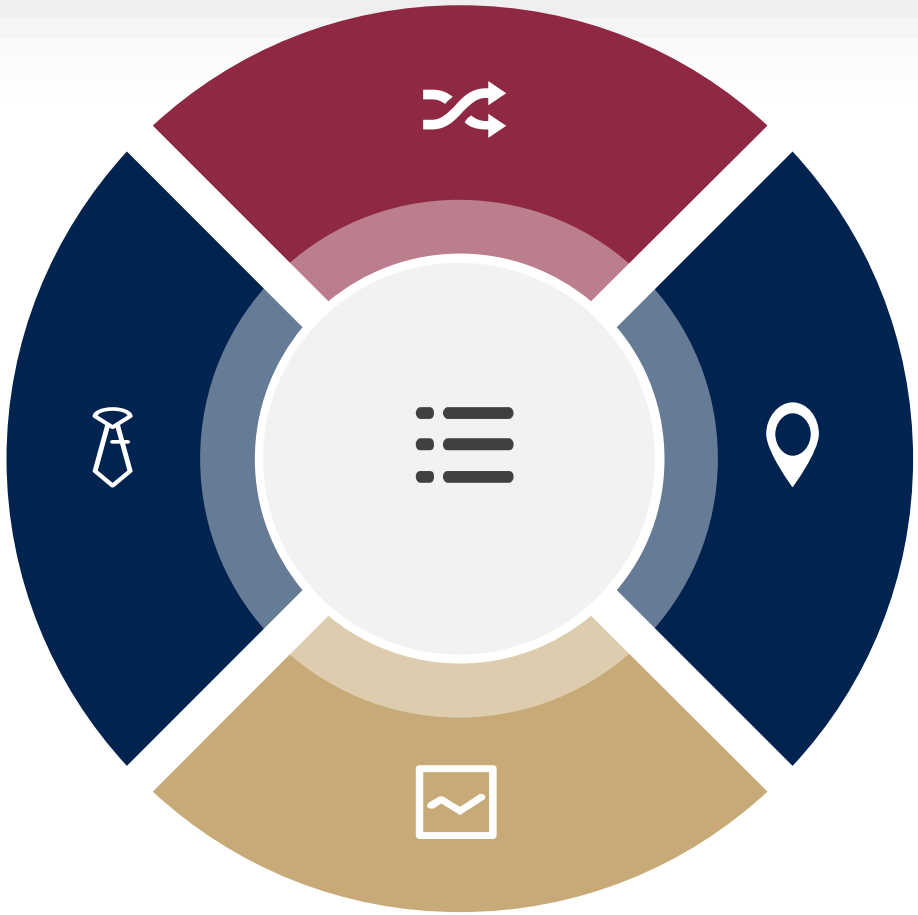
Kiberbiztonsági audit megrendelése

Biztonsági osztályba sorolás

alap

jelentős

magas



Védelem - mit

Hálózati és információs rendszerek + fizikai környezetük

Adatok/információk

Szolgáltatások

Célok

IBIR

Kockázatelemzés

Védelmi intézkedések

Incidensek megelőzése, kezelése, hatásának csökkentése

BC

Életciklus egészében megvalósuló védelem

Kiberbiztonsági felügyelet és ellenőrzés

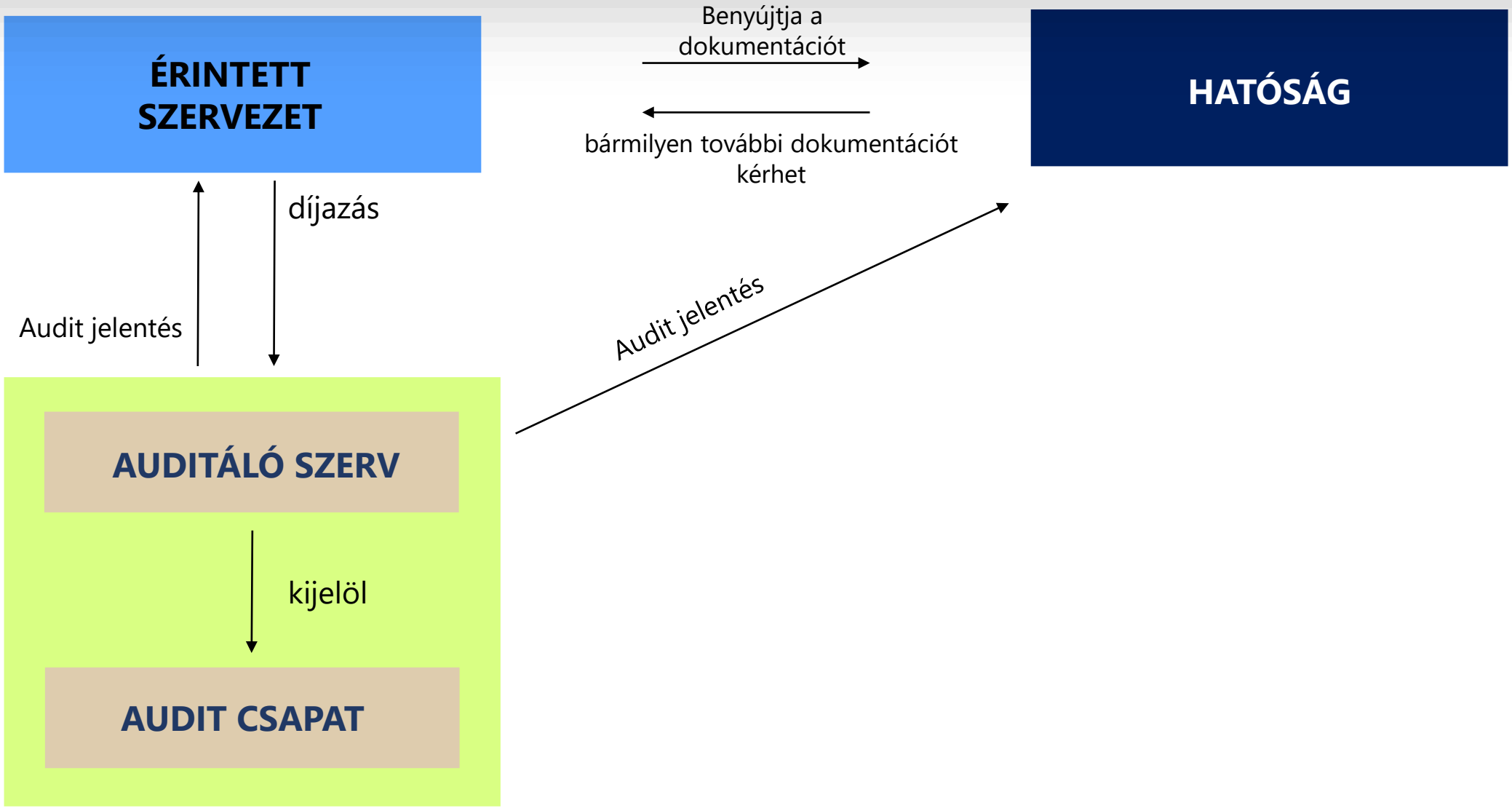
SZTFH

- Hatósági felügyelet – díj:
  - előző évi árbevétel 0,015 %-a, de max. 10M Ft.
- Nyilvántartás
- Hatósági ellenőrzés
- Rendkívüli ellenőrzés elrendelése
- Figyelmeztetés
- Eltiltás (egyéb hatóságokkal együttműködve)
- Bírság
- 10 000 000 EUR, de legfeljebb éves árbevétel 2%-a

Auditorok

- Érintett szervezet felkérésére
- Kiberbiztonsági audit
  - Biztonsági osztályba sorolás
  - Védelmi intézkedések
  - Sérülékenység- és behatolásvizsgálat
  - Kriptográfiai megfelelőség
  - Forráskód-vizsgálat
- Kétévente kötelező
- Eredmény

Feladatok és felelősségek



Kiberbiztonsági felügyelet - ütemezés

	2024. január 1 – június 30.	2024. október 18.	2024. december 31.	2025. december 31.
SZTFH	• Érintett szervezetek nyilvántartásba vétele • Auditorok nyilvántartásba vétele		• Felügyeleti tevékenység • Ellenőrzési tevékenység	
Érintett szervezet	• Önazonosítás, nyilvántartásba vételre bejelentkezés 2024. június 30-ig • Biztonsági osztályba sorolás • Elektronikus információs rendszerek biztonságáért felelős személy feladatköre és kijelölése	• Védelmi intézkedések alkalmazása • Felügyeleti díj megfizetése	• Első kiberbiztonsági audit vonatkozásában szerződéskötés az auditorral	• Első kiberbiztonsági audit lefolytatásának határideje

Kiberbiztonsági felügyelet és vhr-ei

23/2023. (XII. 19.) SZTFH rendelet

(ÖN)AZONOSÍTÁS → **FELELŐS** → **TECHNIKAI ADATOK** → **PARTNER ADATOK** → **KÉRELEM**

A2

Tevékenység

Szervezet mérete?

Közép- vagy nagyvállalkozás

Vizsgálandó tevékenységek:
- ✓ Kibertantv. 1 melléklet
- ✓ Kibertantv. 2. melléklet

Mikro- vagy kisvállalkozás

Vizsgálandó tevékenységek:
- ✓ elektronikus hírközlési szolgáltató
- ✓ bizalmi szolgáltató
- ✓ DNS-szolgáltatást nyújtó szolgáltató
- ✓ legfelső szintű domainnév-nyilvántartó
- ✓ domainnév-regisztrációt végző szolgáltató

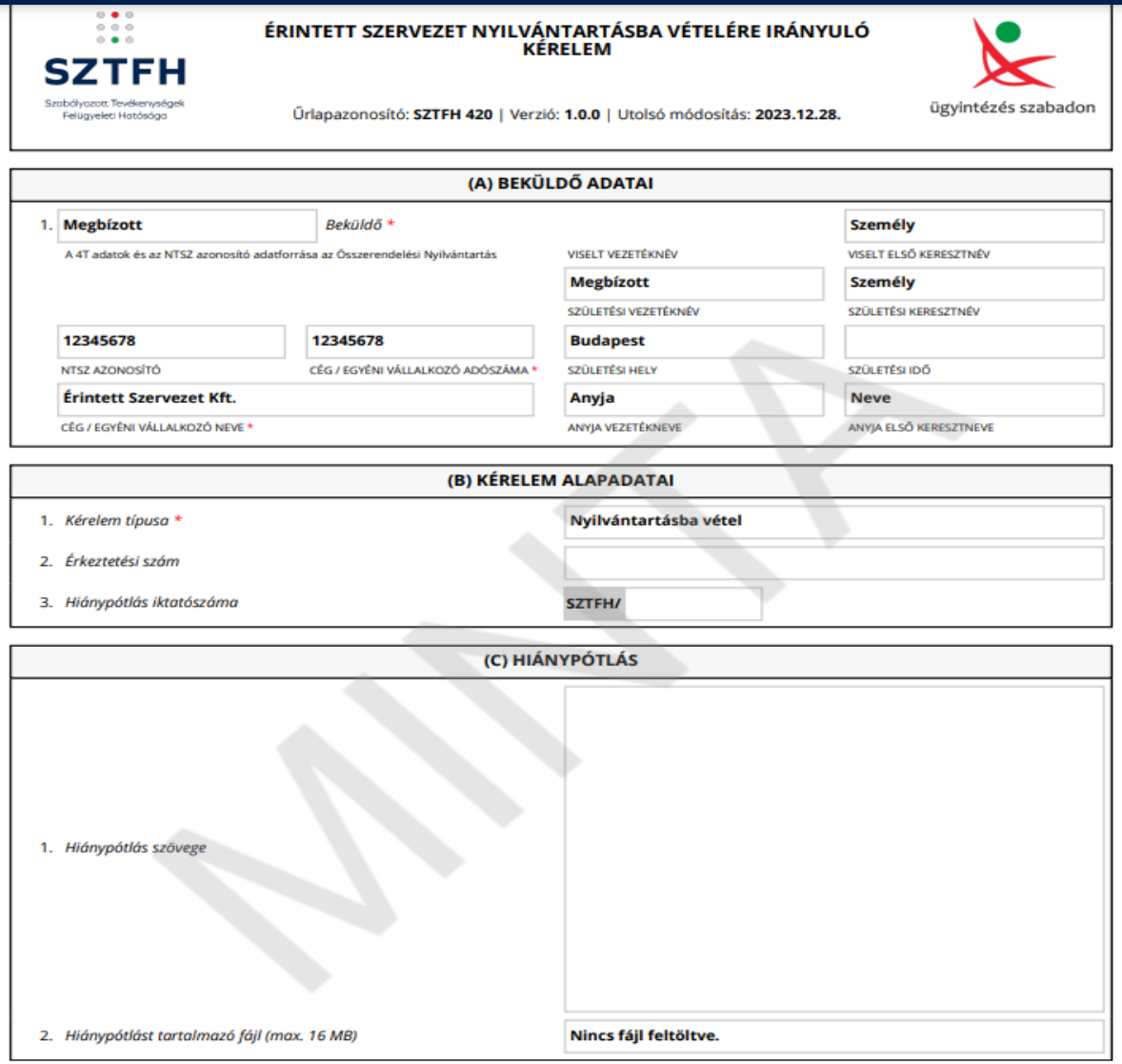
Végzi valamely tevékenységet?

nem

igen

érintett szervezet

Kiberbiztonsági felügyelet és vhr-ei



Köszönöm a figyelmet!

MINDEN KIBERÜL

LinkedIn

kiberbiztonsag@sztfh.hu

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

JOGSZABÁLYI KÖVETELMÉNYEK ÉS MEGOLDÁSOK A NIS 2 ÉGISZE ALATT

A NIS2 implementáció kihívásai és lehetőségei

Black Cell Compliance
Foursys Consolution

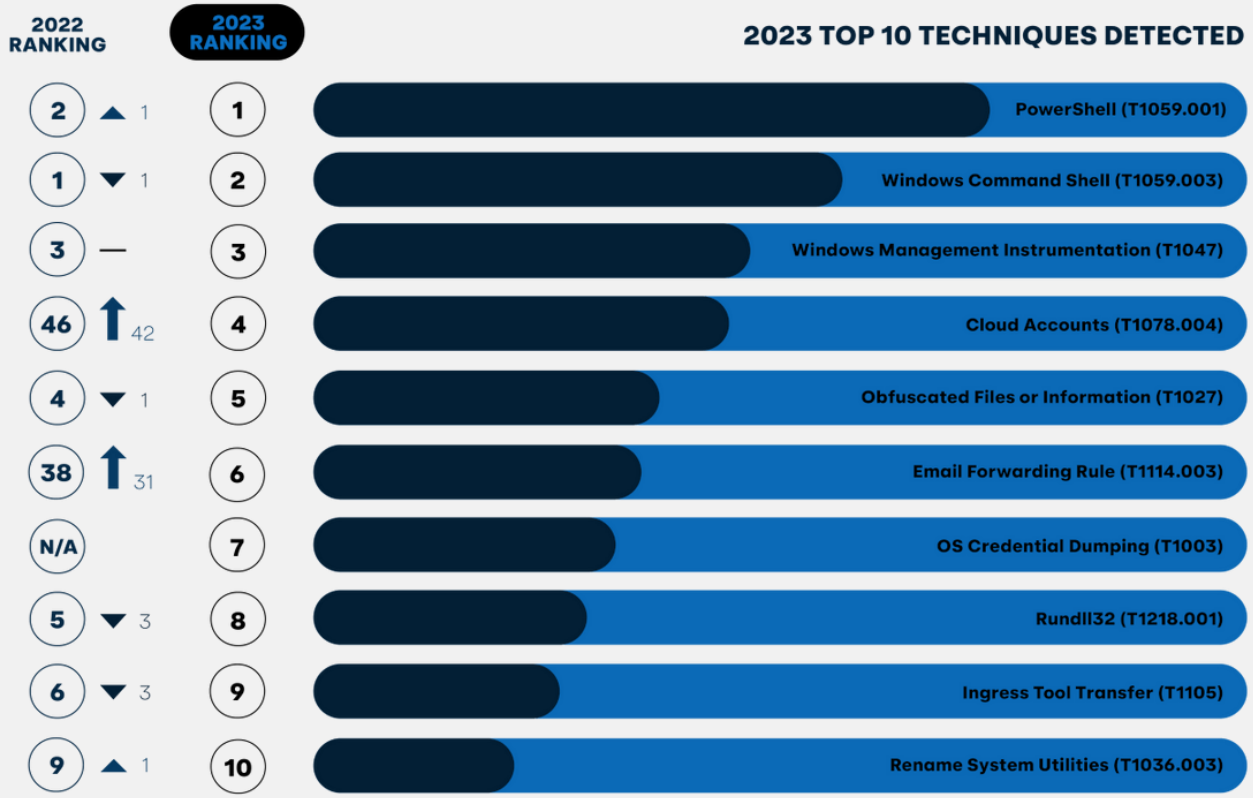
BLACK CELL
Protecting critical infrastructures

FOURSYS
CONSOLUTION

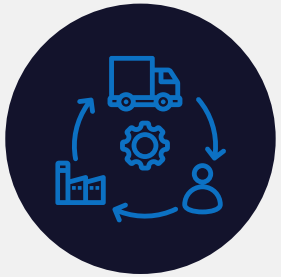
TLP:CLEAR

Fenyegetések aktualitásai

- Identitásalapú támadások prevalenciája (password spraying, credential stuffing, MitM) növekszik: zero trust mindenekelőtt
- Első számú kockázat továbbra is a felhasználó (pl. BEC): szerepkör alapú tudatosság-növelés alapvető fontosságú
- Csatasorba állt a generatív AI – túl a phishingen
- Felhő konvergencia és ennek kihasználása, ellátási lánc kockázatkezelésének prioritása



Jövőbeli fenyegetések

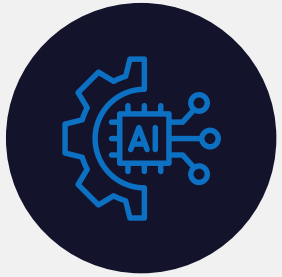


Szállítói lánc kompromittálódása

Szakértői erőforrások szűkössége

Legacy rendszerek exploitálása

Határokon átnyúló szolgáltatók, mint SPoF-ok



AI alapú visszaélések

Célzott zsarolóvírusok

Megfelelési kihívások

- Szűk határidő a felkészülésre
- Biztonsági osztályba sorolásra vonatkozó és védelmi intézkedéseket tartalmazó jogszabály hiánya
- Korábban kiberbiztonsági szabályozási szempontból érintetlen ágazatok érintettsége

Nemmegfelelés kockázatai

Első számú vezető személyes felelőssége

Megnövekedett működési kockázat, bizalmasság és sértetlenség sérülése

Potenciális bírság

Reputációs kitettség incidensek esetén

Megfelelőségi lehetőségek

- Nemzetközi módszertanra épülő, integrált követelményrendszer: NIST SP 800-53 Rev. 5
- Folyamatosan fejlődő kiberfenyegetéseire adekvát szervezési és technikai intézkedések: cél a reziliencia
- Meglévő információbiztonsági irányítási rendszer kihasználása a kontrollok bevezetésére, fenntartására

Megfelelés előnyei

Működési kockázatok csökkentése, kiszámíthatóság és tervezhetőség

Sokrétű szankciórendszer elkerülése

Reputációs kitettség csökkentése

Vezetői és szervezet szintű lehetőségek – folyamatfelmérés

- Átfogó szemléletet igényelnek a döntéshozás, a végrehajtás és az ellenőrzés folyamataiban egyaránt.

NIS2 technológiai kontrollokhoz kapcsolódó folyamatok felmérése, elemzése, hatékonyság növelése, automatizálása

Mélységi folyamatelemzés

Mi a folyamat?

- Egymáshoz kapcsolódó tevékenységek láncolata, ahol a cél egy előre meghatározott eredmény elérése

NIS2 technológiai kontrollokon túli folyamatok felmérése, elemzése, hatékonyság növelése, automatizálása

Folyamatfelderítés- és elemzés, következő legjobb lépések azonosítása

Visszajelzés a működésről (KPI, RCA)

Automatizáció (BPM, WF, RPA, ERP)

Hatékonyságelemzés

Pénzügyi elemzés

Hogyan fogunk hozzá?

NIS2 gap elemzésünk folyamata…

- Meglévő szabályozási rendszer elemzése
- Korábbi vizsgálatok (pl. sérülékenységvizsgálat, jogosultság-ellenőrzés), auditok (belső audit, kockázatértékelés) eredményének áttekintése
- Interjúk lefolytatása a nem (megfelelően) dokumentált kontrollok és üzleti folyamatok ellenőrzése érdekében

…és eredménytermékei

Gap elemzési jelentés

- Alkalmazandó kontrollkövetelmények azonosítása
- Meglévő megfelelési szint elemzése
- Nemmegfelelőség vagy fejlesztési lehetőség esetén javaslattétel

PowerBI jelentés

- Vezetői dashboard a megállapítások és intézkedések áttekintésére

Microsoft NIS2 cybersecurity solution assessment

Microsoft on-prem, Microsoft 365, Azure és egyéb publikus felhőszolgáltatások elemzésére

CISv8 kontrollok, NIS2 modullal, Microsoft által támogatva

Vizibilitás-növelésre hatékony eszköz – főleg a vonakodó felsővezetés meggyőzésére

GAP elemzési jelentés

A GAP elemzés adatai

Ügyfél	TESZ-T Kft.
Cégjegyzékszám	01-09-418500
Ügyfél oldali kapcsolattartó	Teszt Elek
BC + FS	Droppa Béla és Szabó László
WEB	https://consolution.hu/
Székhely	2024 Nagykároly, Október utca 18.

Kibertan.tv. hatálya: Kockázatos ágazat

Kiemelten kockázatos ágazat	**Kockázatos ágazat**	Küszöbérték felett	Méretkorlát nélkül alkalmazandó

(TEÁOR szám szerinti érintettség ~75%-os pontossággal), Digitális szolgáltatók, Élelmiszer előállítása, feldolgozása és forgalmazása, Gyártás, Hulladékgazdálkodás, Kutatás, Postai és futárszolgáltatások, Vegyszerek gyártása, előállítása és forgalmazása

Kontrollérettség áttekintése

NIS2 érintettség

NIS2 felmérés hatóköre

NIS2 felmérés eredménye

Intézkedési terv

Vizsgálati jelentés

Érintettség megállapítása

NIS 2 (Kibertantv.) érintettség: Igen

Kiemelten kockázatos ágazati érintettség

- Energetika / Villamos energia
- Kihelyezett IKT szolgáltatások / kihelyezett irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató

Kockázatos ágazatos ágazati érintettség

- Gyártás / Máshova nem sorolt gépek és berendezések gyártása

Indoklás

Méretkorlát

A szervezet közepes- vagy nagyvállalatnak minősül

Ágazati érintettség

Kiemelten kockázatos ágazat

Energetika::

- 3511 villamosenergia-termelés

Kihelyezett IKT szolgáltatások::

- 2080 Biztonsági rendszer szolgáltatás *(potenciális)*

Kockázatos ágazat

Gyártás:

- 2829 M. n. s. egyéb általános rendeltetésű gép gyártása
- 2821 Fűtőberendezés, kemence gyártása

Azonosítási kritérium

Energetika / villamos energia

Avillamos energiáról szóló törvény szerinti villamosenergia-ipari vállalkozás a közvilágítási üzemeltetési engedélyes kivételével (Villamosenergia-ipari vállalkozás: az a természetes vagy jogi személy, aki vagy amely az e törvény szerinti villamosenergia-termelést, villamosenergia-átviteli és rendszerirányítási tevékenységet, villamosenergia-elosztást, egyetemes szolgáltatói tevékenységet, villamosenergia-kereskedelmet, aggregálást, energiatárolást, közvilágítási berendezések üzemeltetését, vagy a közúti közlekedésről szóló törvény szerinti elektromos töltőberendezés üzemeltetési, vagy elektromobilitás szolgáltatási tevékenységet végez)

Kihelyezett IKT szolgáltatások

kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató *(potenciális érintettség: tovább vizsgálandó a tevékenység pontos jellege)*

Máshova nem sorolt gépek és berendezések gyártása

a gazdasági tevékenységek statisztikai osztályozása NACE Rev. 2. rendszerének létrehozásáról és a 3037/90/EGK tanácsi rendelet, valamint egyes meghatározott statisztikai területekre vonatkozó EK-rendeletek módosításáról szóló, 2006. december 20-i 1893/2006/EK európai parlamenti és tanácsi rendelet 28. ágazata szerinti „Gép, gépi berendezés gyártása” tevékenységet végző gazdálkodó szervezet

04 Naplózás és elszámoltathatóság

Legfontosabb megállapítások

- EIR-ek jelentős része bevonásra került a SIEM rendszerbe, de több kritikus naplóforrás hiányzik (pl. EDR).
- MITRE ATT&CK alapú detekciós lefedettség növelhető.
- Incidenskezelési eljárások nem minden EIR-re vonatkozóan állnak rendelkezésre.
- Naplózási szabályzat a detekciós képességfejlesztési változtatások alapján frissítendő.

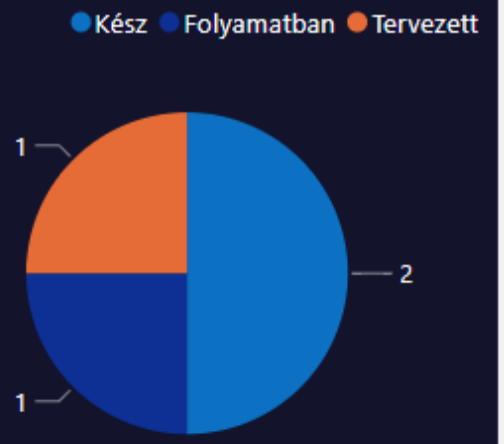
Naplózási lefedettség

, Alkalmazásszerver I., Domain controller, EDR, Mentő szerver, Webalkalmazás tűzfal

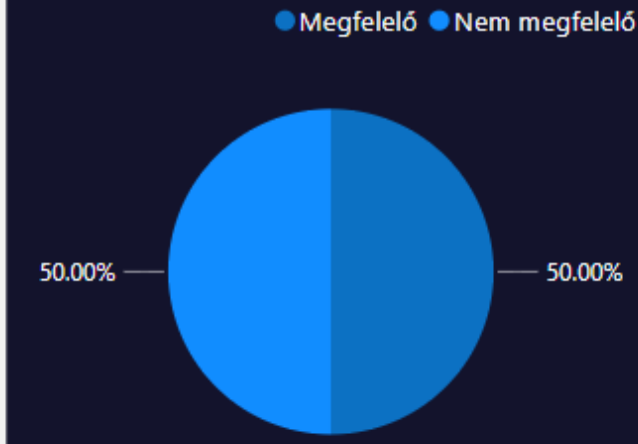
Megállapítások száma

4

IRP-k

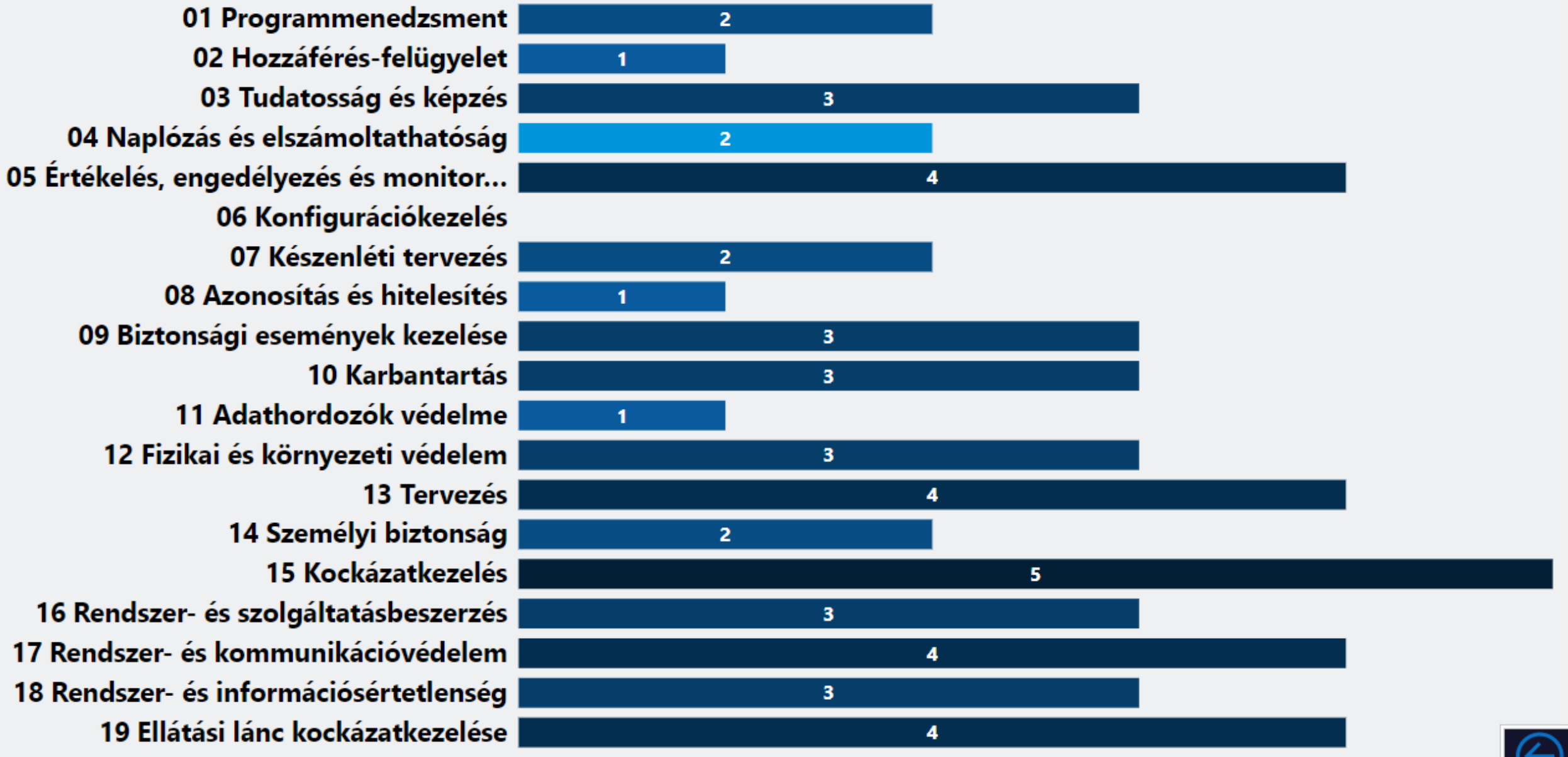


Detekciós lefedettség



, T1053 Scheduled Task/Job, T1072 Software Deployment Tools, T1102 Web Service, T1190 Exploit Public-Facing Application, T1204 User Execution, etc.

Kontrollérettség áttekintő



A hiányfelmérés megállapításai

JOGSZABÁLYI KÖVETELMÉNYEK ÉS MEGOLDÁSOK A NIS 2 ÉGISZE ALATT

Köszönjük a részvételt!

BLACK CELL
Protecting critical infrastructures

FOURSYS
CONSOLUTION