

JOGSZABÁLYI KÖVETELMÉNYEK ÉS  
MEGOLDÁSOK A NIS 2 ÉGISZE ALATT

# Jogszabályi követelmények és megoldások a NIS 2 égisze alatt



2024/04/11





# NIS2 és új lbtv.

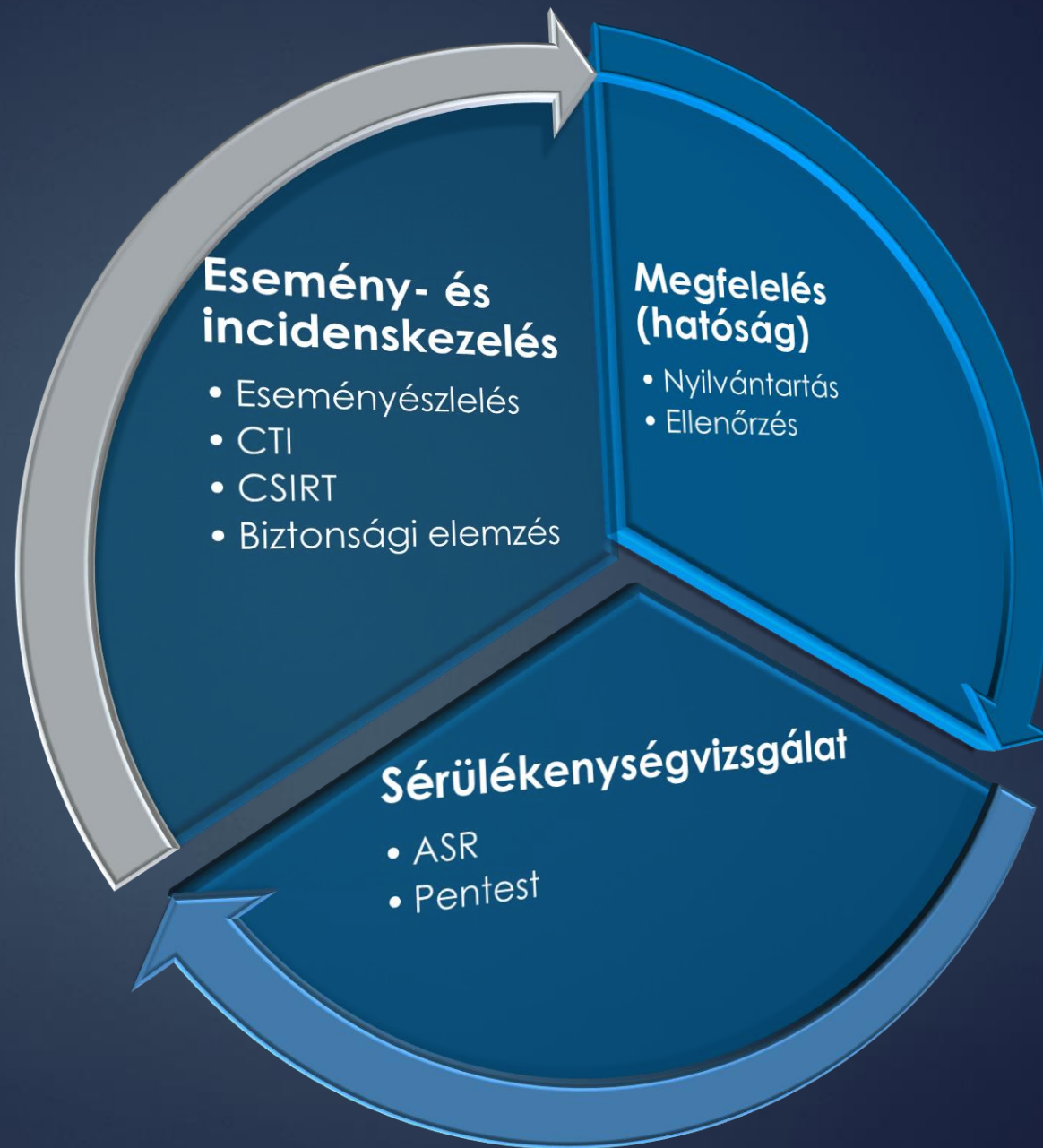
**Marsi Tamás**

NBSZ NKI

*tamas.marsi@nki.gov.hu*



# NKI







**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



**SZTFH**

Szabályozott Tevékenységek  
Felügyeleti Hatósága

NIS2 közigazgatás ágazat  
és kritikus szervezetek  
(kivéve DORA)



DORA



Honvédelmi ágazat



A törvény hatálya  
megbontásra kerül:

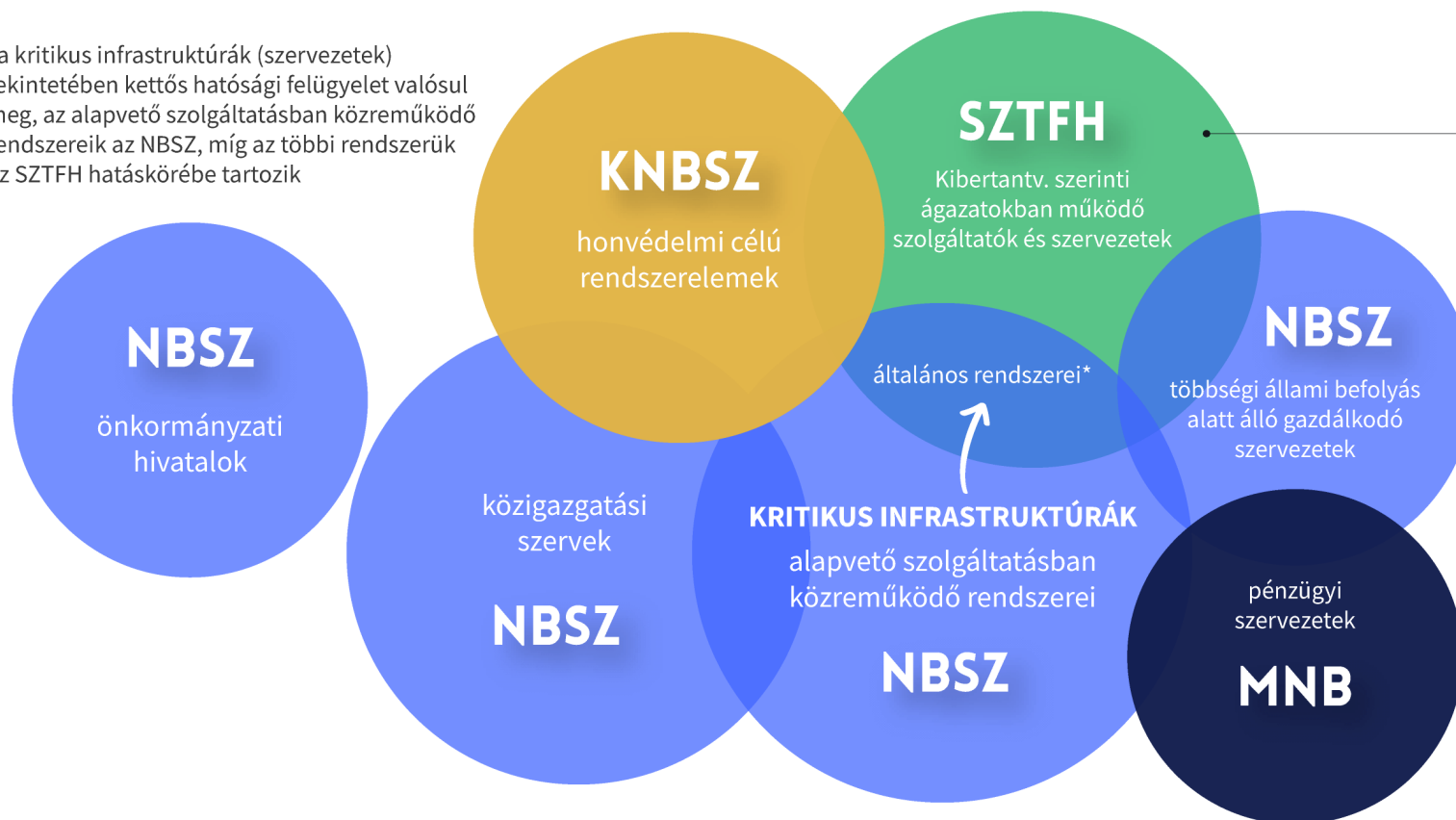
- **felügyelet** (hatóság)
- **incidenskezelés** (CSIRT)
- **sérülékenységvizsgálat**





# 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?

Incidens bejelentés

INTÉZET HATÓSÁG SZOLGÁLTATÁSOK IT BIZTONSÁG FIGYELMEZTETÉSEK

## RIASZTÁSOK

Főoldal > Riasztások

RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL – 2022. MÁRCIUS	2022.03.09.	<b>FIGYELMEZTETÉSEK</b> Sérülékenységek Káros kód leírások Riasztások Tájékoztatások Archívum Gyakran Ismételt Kérdések
RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL – 2022. FEBRUÁR	2022.02.09.	
RIASZTÁS DEADBOLT ZSAROLÓVÍRUS TERJEDÉSÉRŐL	2022.02.07.	
RIASZTÁS AZ INTERNETEN TERJEDŐ ADATHALÁSZ LEVELEKKEL KAPCSOLATBAN	2022.01.31.	
RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL – 2022. JANUÁR	2022.01.12.	
RIASZTÁS AZ INTERNETEN TERJEDŐ, ZSAROLÓ HANGVÉTELŰ LEVELEKKEL KAPCSOLATBAN	2022.01.05.	
RIASZTÁS MICROSOFT TERMÉKEKET ÉRINTŐ SÉRÜLÉKENYSÉGEKRŐL	2021.12.16.	<b>LEGFRISSEBB SÉRÜLÉKENYSÉGEK</b>
RIASZTÁS APACHE LOG4J KÖNYVTÁR ÉRINTŐ KRITIKUS SÉRÜLÉKENYSÉGGEL KAPCSOLATBAN	2021.12.12.	PAN-OS 0. napi sérülékenység
RIASZTÁS ÜGYINTÉZŐI MEGKERESÉSNEK ÁLCÁZOTT CSALÓ TELEFONHÍVÁSOKKAL KAPCSOLATBAN	2021.12.08.	

Incidens bejelentés

INTÉZET HATÓSÁG SZOLGÁLTATÁSOK IT BIZTONSÁG FIGYELMEZTETÉSEK

## TÁJKOZTATÓ A KASPERSKY TERMÉKEK HASZNÁLATÁRÓL

Főoldal > Tájékoztatások > Tájékoztató a Kaspersky termékek használatáról

Tisztelt Ügyfelünk!

csatornák 14:03

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibevédelmi Intézetéhez (NBSZ NKI) érkezett megkeresések alapján a **Kaspersky Lab** termékeinek használatáról az NBSZ NKI az alábbi tájékoztatást adja ki.

Az Amerikai Egyesült Államokban a 2017-es '17-01 Binding Operational Directive (BOD) dokumentum alapján a szövetségi kormányzati szervek és az ügynökségek nem használhatják a Kaspersky termékeit. Az Egyesült Királyság és Hollandia az előbbi dokumentumra hivatkozva szintén tiltják a használatát (érzékeny adatot kezelő és létfontosságú rendszerek esetében).

Az Európai Parlament 2018-as állásfoglalása „felhívja az Uniót, hogy végezze el az intézményekben használt szoftverek, informatikai és kommunikációs berendezések és infrastruktúra átfogó felülvizsgálatát a potenciálisan veszélyes programok és eszközök elhárítása és a bizonyítottan rosszindulatú eszközök – mint

### FIGYELMEZTETÉSEK

Sérülékenységek  
Káros kód leírások  
Riasztások  
Tájékoztatások  
Archívum  
Gyakran Ismételt Kérdések

### LEGFRISSEBB SÉRÜLÉKENYSÉGEK

PAN-OS 0. napi sérülékenység  
Apache HTTP szerver többszörös sérülékenység

Incidens bejelentés **Friess NKI riasztás jelent meg**

INTÉZET HATÓSÁG HÍREK TUDÁSKÖZPONT FIGYELMEZTETÉSEK

## Kiemelt témák

- Jelszavak
- Kéretlen levelek
- Zsarolóvírus
- Adathalászat

Hogyan cselezhetjük ki a QR-kódos csalókat?

## KÁROS KÓD LEÍRÁSOK

Főoldal > Káros kód leírások

HERMETICWIPER LEÍRÁS	2022.02.25.	MAGAS	<b>FIGYELMEZTETÉSEK</b> Sérülékenységek Káros kód leírások Riasztások Tájékoztatások Archívum Gyakran Ismételt Kérdések
EGREGOR RANSOMWARE LEÍRÁS	2020.11.02.	KÖZEPES	
SHELLBOT KÁROS KÓD LEÍRÁS	2020.11.02.	KÖZEPES	
TYCOON RANSOMWARE LEÍRÁS	2020.09.02.	KÖZEPES	
WASTEDLOCKER RANSOMWARE KÁROS KÓD LEÍRÁS	2020.08.18.	KÖZEPES	
NETWALKER RANSOMWARE	2020.07.06.	KÖZEPES	
KILLMR.CORN_A	2020.04.07.	KÖZEPES	<b>LEGFRISSEBB SÉRÜLÉKENYSÉGEK</b>
COVIDLOCK ZSAROLÓVÍRUS	2020.03.19.	KÖZEPES	

# Köszönöm a figyelmet!

[tamas.marsi@nki.gov.hu](mailto:tamas.marsi@nki.gov.hu)



Kibertámadás!  
podcast



LinkedIn



[nki.gov.hu](http://nki.gov.hu)



  
NEMZETI  
KIBERVÉDELMI INTÉZET



JOGSZABÁLYI KÖVETELMÉNYEK ÉS  
MEGOLDÁSOK A NIS 2 ÉGISZE ALATT





# Fájni fog-e vagy sem a 23-as hatás?

## Szabályozással egy biztonságosabb kibertérért



**Bor Olivér**

kiberbiztonsági és kommunikációs szakértő  
egyetemi vendégoktató



# SZTFH

Szabályozott Tevékenységek  
Felügyeleti Hatósága

# Két féle szervezet...

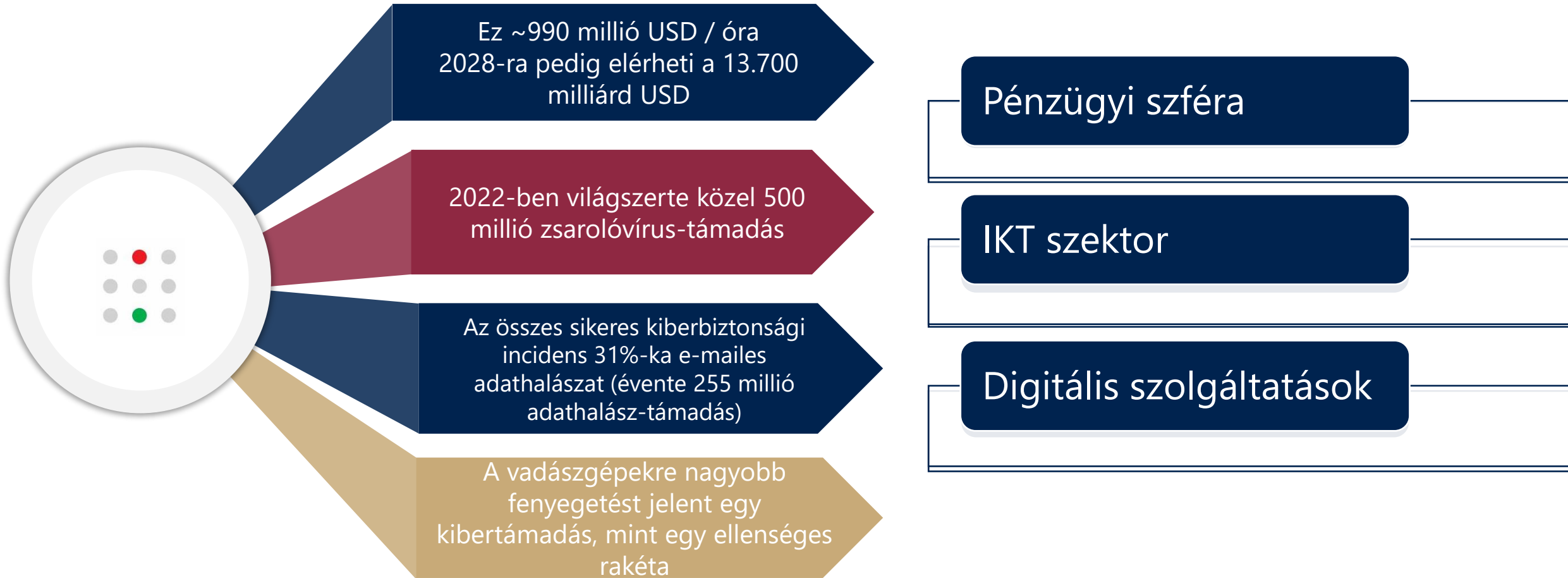
2012 ROBERT MUELLER, FBI



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

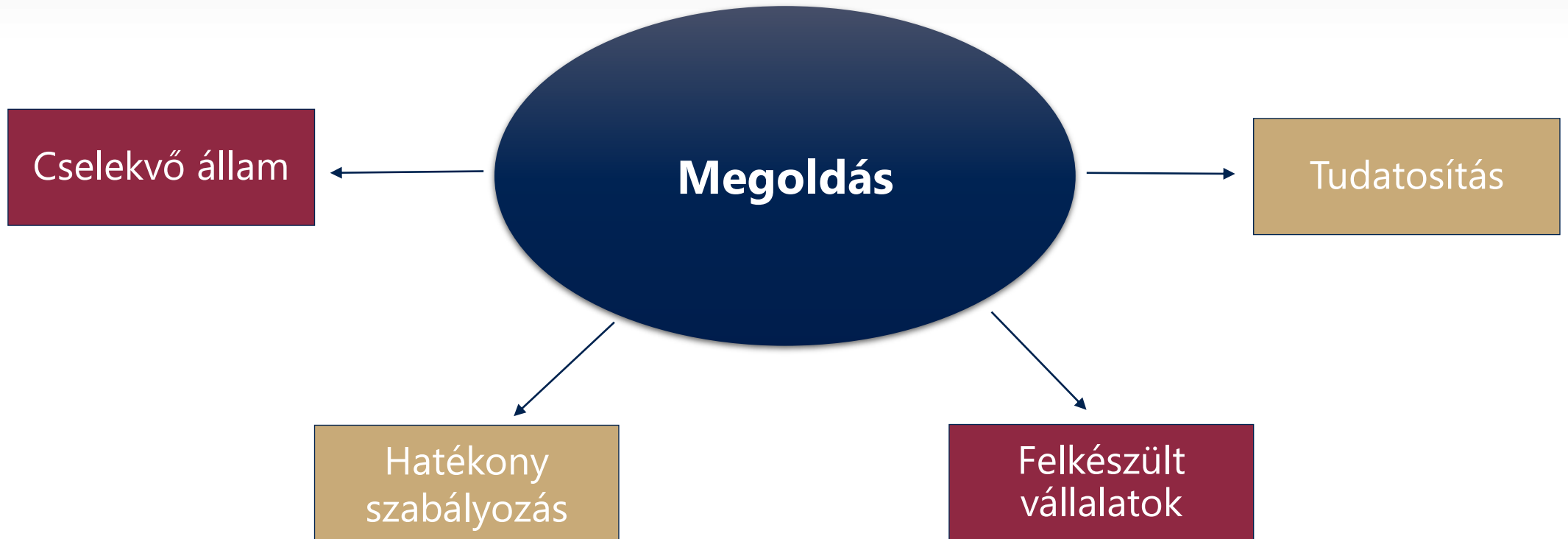
# Nincs kegyelem – tényleg fáj

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





# Kihívások és válaszok



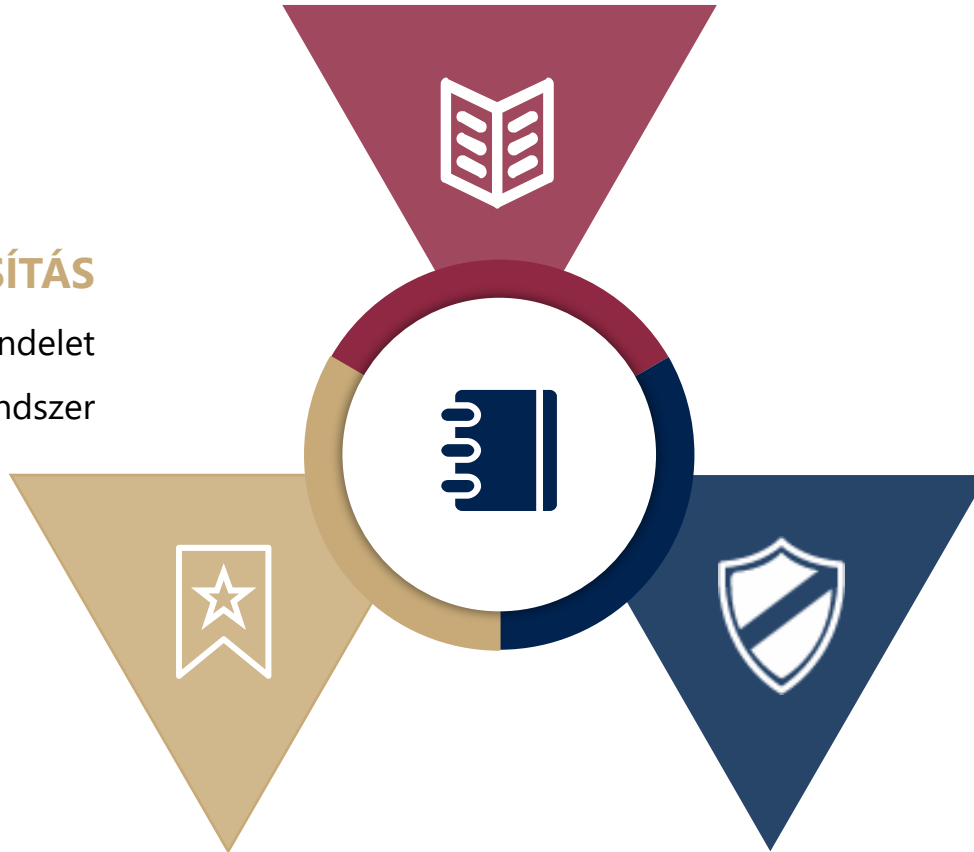
# Kibertan.tv – 2023. évi XXII. törvény

a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvény

## KIBERBIZTONSÁGI TANÚSÍTÁS

2019/881 (EU) rendelet  
Nemzeti tanúsítási keretrendszer

## ÉRTELMEZŐ RENDELKEZÉSEK



## KIBERBIZTONSÁGI FELÜGYELET

2022/2555 (EU) irányelv – NIS2

# Kiberbiztonsági felügyelet – érintett szervezetek





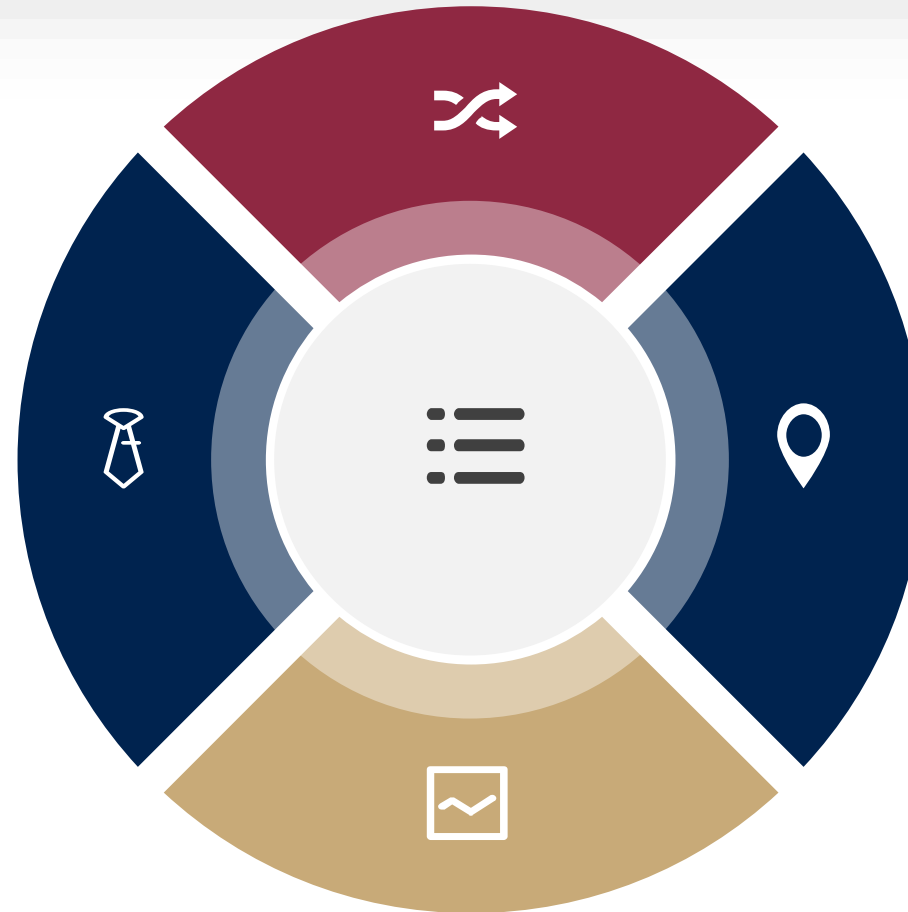
# Kiberbiztonsági felügyelet – érintett feladatai

## 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



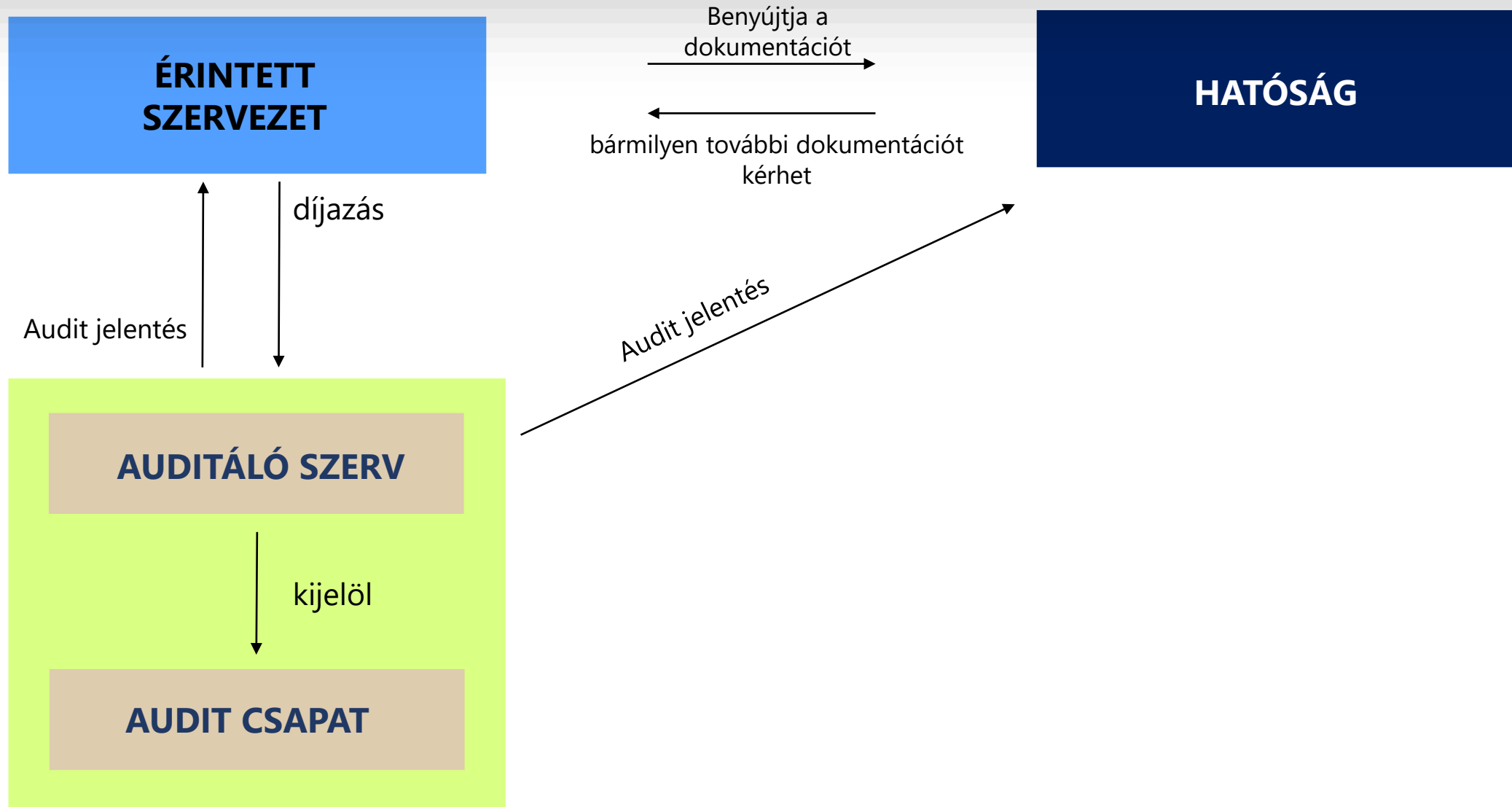
- Hatósági felügyelet – díj:
  - előző évi árbevétel 0,015 %-a, de max. 10M Ft.
- Nyilvántartás
- Hatósági ellenőrzés
- Rendkívüli ellenőrzés elrendelése
- Figyelmeztetés
- Eltiltás (egyéb hatóságokkal együttműködve)
- Bírság
- 10 000 000 EUR, de legfeljebb éves árbevétel 2%-a



## Auditorok

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

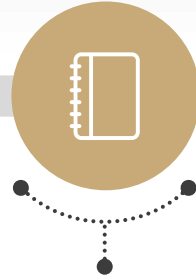
# Feladatok és felelőségek





# Kiberbiztonsági felügyelet - ütemezés

2024. január 1 – június 30.



- **Érintett szervezetek nyilvántartásba vétele**
- **Auditorok nyilvántartásba vétele**

**SZTFH**

**Érintett szervezet**

- **Önazonosítás, nyilvántartásba vételre bejelentkezés 2024. június 30-ig**
- **Biztonsági osztályba sorolás**
- **Elektronikus információs rendszerek biztonságáért felelős személy feladatköre és kijelölése**

2024. október 18.



- **Védelmi intézkedések alkalmazása**
- **Felügyeleti díj megfizetése**

2024. december 31.



- **Felügyeleti tevékenység**
- **Ellenőrzési tevékenység**

- **Első kiberbiztonsági audit vonatkozásában szerződéskötés az auditorral**

2025. december 31.



- **Első kiberbiztonsági audit lefolytatásának határideje**

# Kiberbiztonsági felügyelet és vhr-ei

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

(ÖN)AZONOSÍTÁS

FELELŐS

TECHNIKAI  
ADATOK

PARTNER  
ADATOK

KÉRELEM

# A<sub>2</sub>

Tevékenység

Szervezet  
mérete?

Közép- vagy  
nagyvállalkozás

Mikro- vagy  
kisvállalkozás

Vizsgálendő tevékenységek:

- ✓ Kibertantv. 1 melléklet
- ✓ Kibertantv. 2. melléklet

Vizsgálendő 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

## SZTFH 420 • Érintett szervezet nyilvántartásba vételére irányuló kérelem

KEZDŐLAP > ÜGYINTÉZÉS > NYOMTATVÁNYOK ÉS ŪRLAPOK > SZTFH 420 • ÉRINTETT SZERVEZET NYILVÁNTARTÁSBA VÉTELÉRE IRÁNYULÓ KÉRELEM

### ELEKTRONIKUS ŪRLAP

→ SZTFH 420 kitöltése

### LETÖLTÉSEK

→ SZTFH 420 ūrlap minta

### TOVÁBBI OLDALAK

→ E-ügyintézési tudnivalók

## Érintett szervezet nyilvántartásba vételére irányuló kérelem

A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (továbbiakban: Kibertan.tv.) 17. § alapján érintett szervezetnek minősülő szervezetek adataikat nyilvántartásba vétel érdekében kötelesek az SZTFH-nak megküldeni. A nyilvántartás vezetésének részletes szabályait az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról szóló 23/2023. SZTFH rendelet tartalmazza.

**Az ūrlap kitöltésére jogosult:** az érintett szervezet cégkapujához meghatalmazással rendelkező természetes személy.

Az ūrlapon megadandó és megadható adatok:

- szervezet alapadatai: cégjegyzékszám, székhely, alapítás dátuma, Kkv tv. szerinti besorolás, előző évi nettó árbevétel ezer forintba kerekítve, a hatóság által tájékoztatási célra használható elektronikus levelezési címe;
- a szervezet Kibertan.tv. 1. melléklete vagy 2. melléklete szerinti tevékenységei;
- az elektronikus információs rendszerek biztonságáért felelős személyre vonatkozó információk: jogi megbízott személy esetén annak cégadatai, foglalkoztatott vagy megbízáson keresztül kijelölt

### (A) BEKÜLDŐ ADATAI

1. <b>Megbízott</b> <small>Beküldő *</small>	<input type="text"/>	<b>Személy</b>	<input type="text"/>
<small>A 4T adatok és az NTSZ azonosító adatforrása az Összerendelési Nyilvántartás</small>		<small>VISELT VEZETÉKNÉV</small>	<small>VISELT ELSŐ KERESZTNÉV</small>
<input type="text"/>	<input type="text"/>	<b>Megbízott</b>	<b>Személy</b>
<small>NTSZ AZONOSÍTÓ</small>	<small>CÉG / EGYÉNI VÁLLALKOZÓ ADÓSZÁMA *</small>	<small>SZÜLETÉSI VEZETÉKNÉV</small>	<small>SZÜLETÉSI KERESZTNÉV</small>
<input type="text"/>	<input type="text"/>	<b>Budapest</b>	<input type="text"/>
<b>Érintett Szervezet Kft.</b>	<input type="text"/>	<small>SZÜLETÉSI HELY</small>	<small>SZÜLETÉSI IDŐ</small>
<small>CÉG / EGYÉNI VÁLLALKOZÓ NEVE *</small>	<input type="text"/>	<b>Anyja</b>	<b>Neve</b>
		<small>ANYJA VEZETÉKNÉVE</small>	<small>ANYJA ELSŐ KERESZTNEVE</small>

### (B) KÉRELEM ALAPADATAI

1. <b>Kérelem típusa *</b>	<input type="text" value="Nyilvántartásba vétel"/>
2. <b>Érkeztetési szám</b>	<input type="text"/>
3. <b>Hiánypótlás iktatószáma</b>	<input type="text" value="SZTFH/"/>

### (C) HIÁNPÓTLÁS

1. <b>Hiánypótlás szövege</b>	<input type="text"/>
2. <b>Hiánypótlást tartalmazó fájl (max. 16 MB)</b>	<input type="text" value="Nincs fájl feltöltve."/>

Köszönöm a figyelmet!



[kiberbiztonsag@sztfh.hu](mailto:kiberbiztonsag@sztfh.hu)



JOGSZABÁLYI KÖVETELMÉNYEK ÉS  
MEGOLDÁSOK A NIS 2 ÉGISZE ALATT

# A NIS2 implementáció kihívásai és lehetőségei

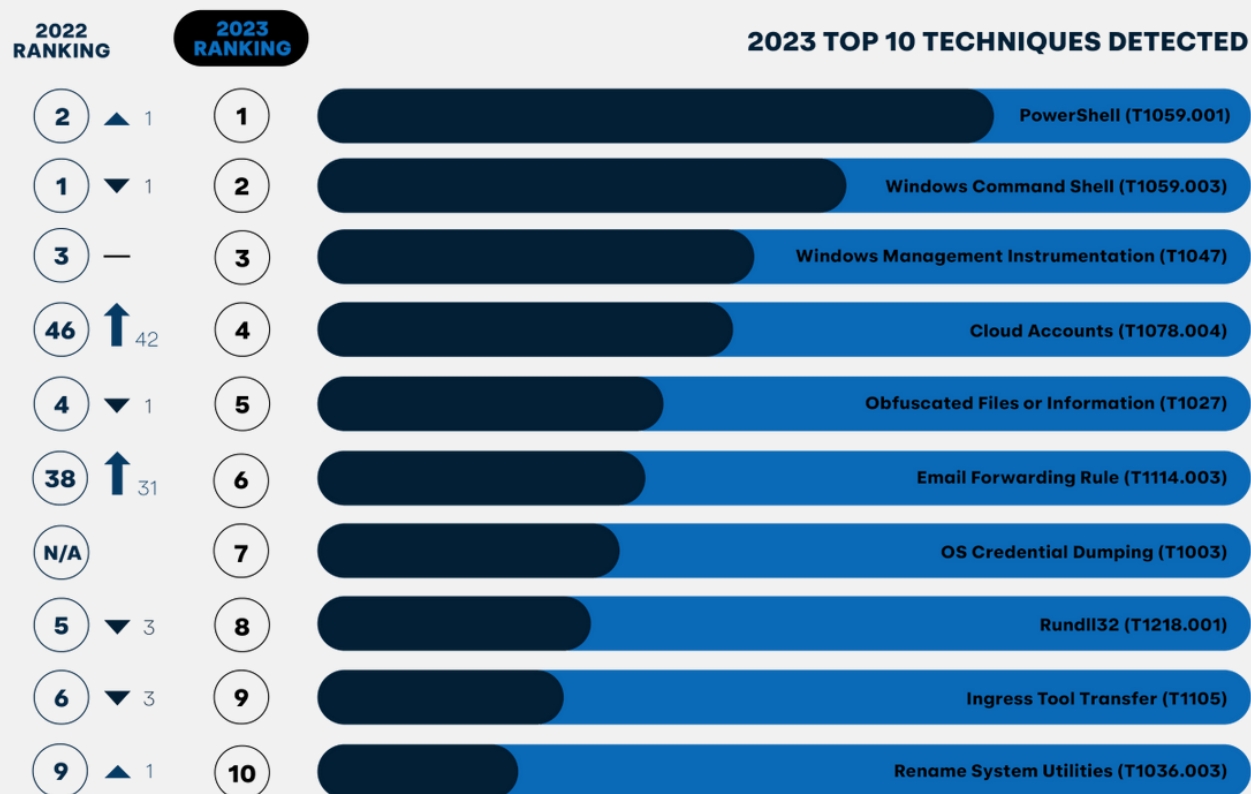
Black Cell Compliance  
Foursys Consolution





# 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 kitétség  
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





# Mélyégi 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**



# Hogyan fogunk hozzá?



# NIS2 gap elemzésünk folyamata...



**Biztonsági osztályba sorolás, védelmi intézkedések azonosítása**



**Kontrollérettség vizsgálata**



**Folyamatfelmérés**



**Vizsgálati jelentés és cselekvési terv átadása**

- 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 javaslattevés



### 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 vonatkozó felsővezetés meggyőzésére

## 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	<a href="https://consolution.hu/">https://consolution.hu/</a>
Székhely	2024 Nagykároly, Október utca 18.



## Kibertan.tv. hatálya: Kockázatos ágazat

**Kiemelten  
kockázatos  
ágazat**

**Kockázatos  
ágazat**

**Küszöbérték  
felett**

**Méretkorlát  
nélkül  
alkalmazandó**

## Kontrollérettség áttekintése

(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

NIS2 érintettség

NIS2 felmérés  
hatóköre

NIS2 felmérés  
eredménye

Intézkedési terv



## 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, energiátárolást, 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 vizsgálendő 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

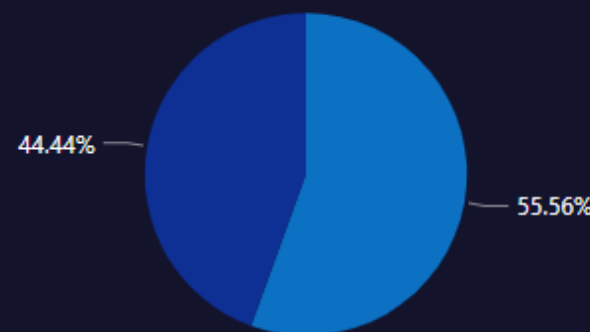


## Legfontosabb megállapítások

- 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

● Naplógyűjtésbe bevont ● Naplógyűjtésbe bevo...



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

## Megállapítások száma

4

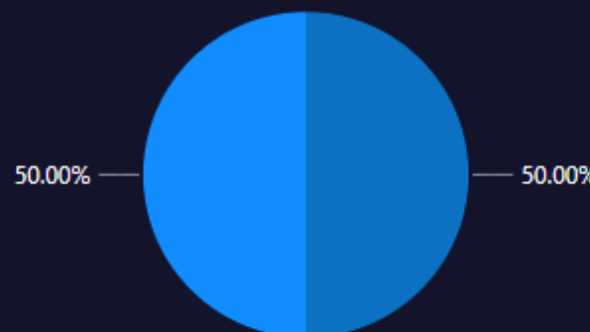
## IRP-k

● Kész ● Folyamatban ● Tervezett



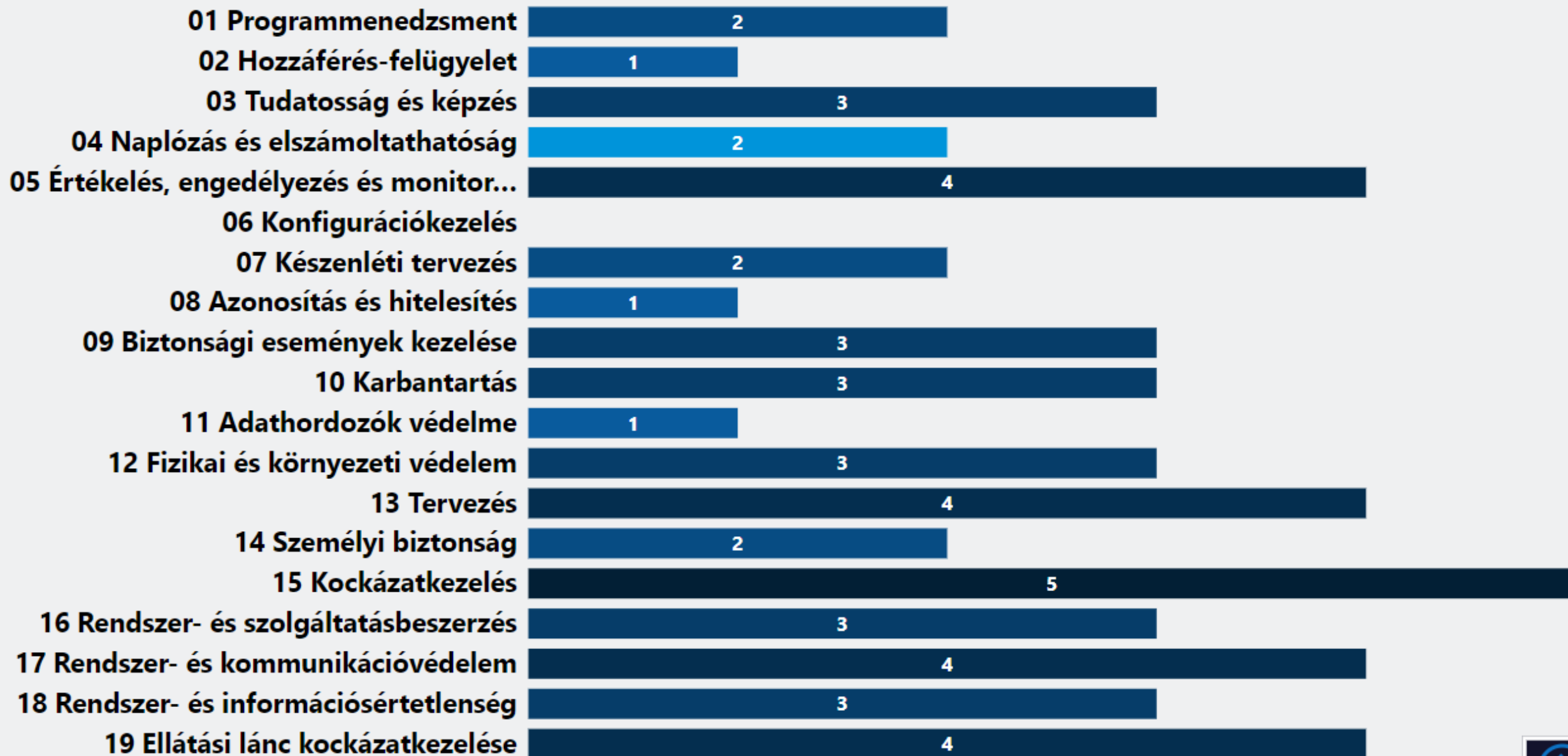
## Detekciós lefedettség

● Megfelelő ● Nem megfelelő



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





JOGSZABÁLYI KÖVETELMÉNYEK ÉS  
MEGOLDÁSOK A NIS 2 ÉGISZE ALATT

# Köszönjük a részvételt!

