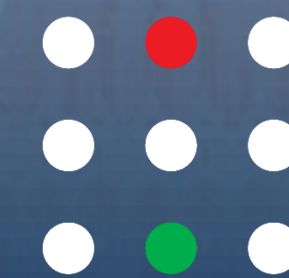


Kiberbiztonsági AUDIT szabályozási lehetőségei

dr. Bencsik Balázs

Kiberbiztonsági Igazgatóság



SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Stabil, kiszámítható működési és szabályozási környezet biztosítása a kiemelt ágazatok számára

- Szerencsejáték Felügyelet,
- Nemzeti Dohánykereskedelmi Nonprofit Zrt.,
- Felszámolók Névjegyzékét Vezető Hatóság,
- IM Bírósági végrehajtói felügyelet
- Magyar Bányászati és Földtani Szolgálat
- Kiberbiztonsági tanúsítás és felügyelet



A Szabályozott
Tevékenységek
Felügyeleti Hatósága

milliárd forint **2000**

Az iparági szereplők éves szinten több mint
2000 milliárd forintos árbevételt realizálnak.

ezer ember **50**

Az ágazati szereplők mintegy 50 ezer főnek
kínálnak munkahelyet.

ezer család **150**

Az ágazatok közvetve és közvetetten 100-150
ezer ember megélhetését biztosítják.

milliárd forint **700**

A felügyelt tevékenységekből évi 700 milliárd
forint adó és járulékbevétel származik.

Kiemelkedő jelenőség és felelősség, hatékony hatósági mozgástérrel párosítva.

Európai Unió jogszabályi környezet



Kibertan.tv – 2023. évi XXIII. törvény

a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvény

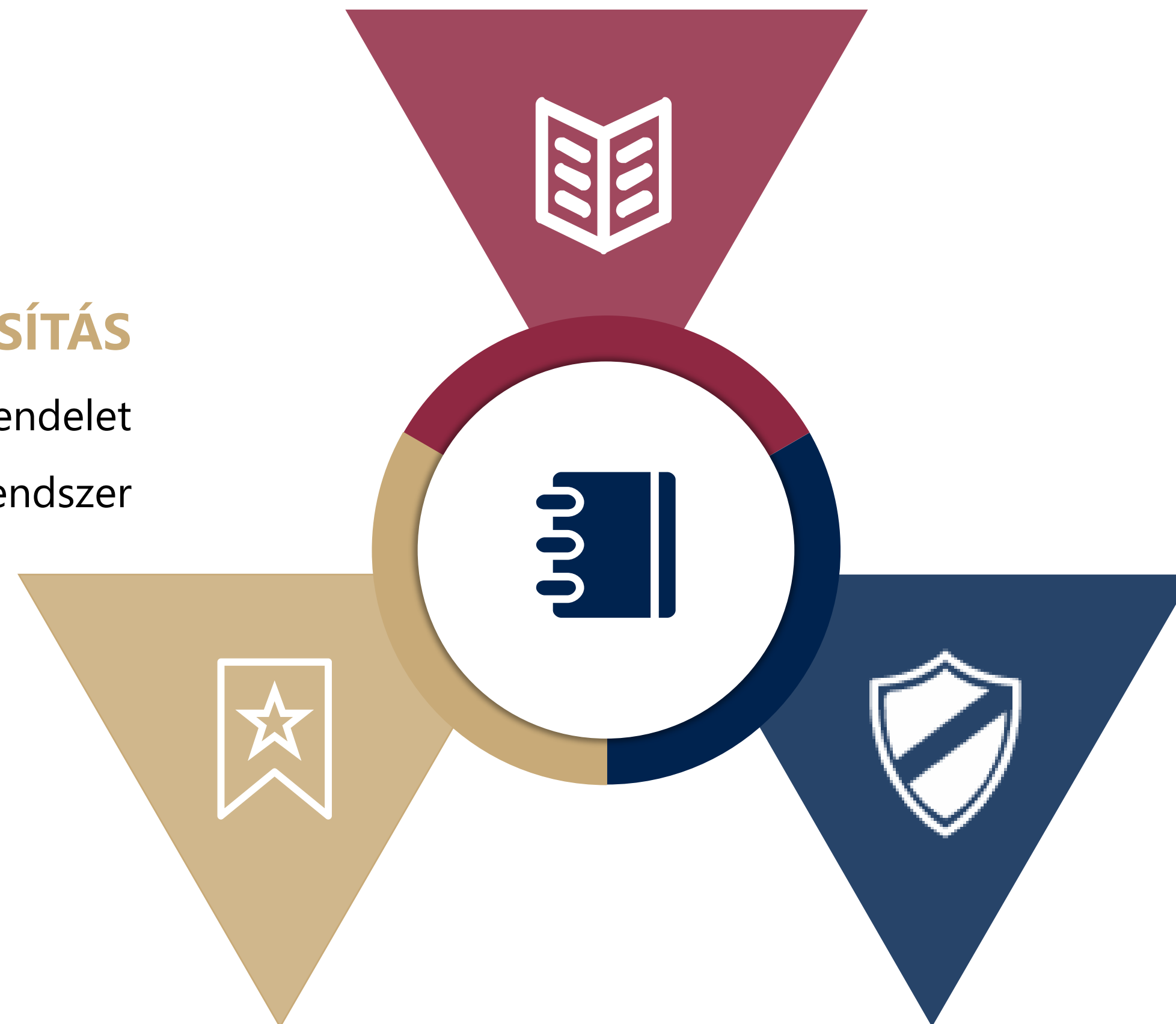
ÉRTELMEZŐ RENDELKEZÉSEK

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

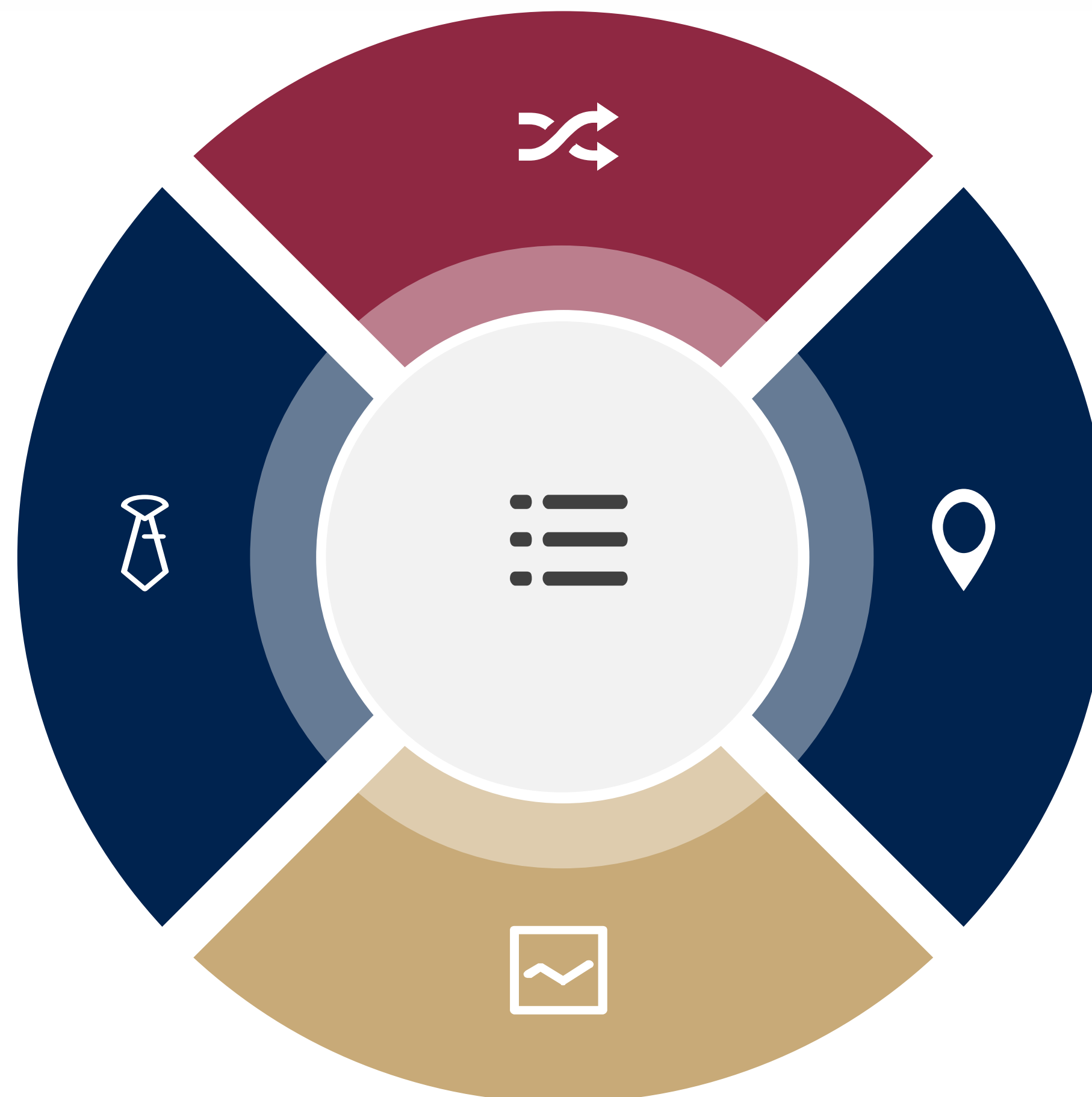
Kiberbiztonsági audit megrendelése

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



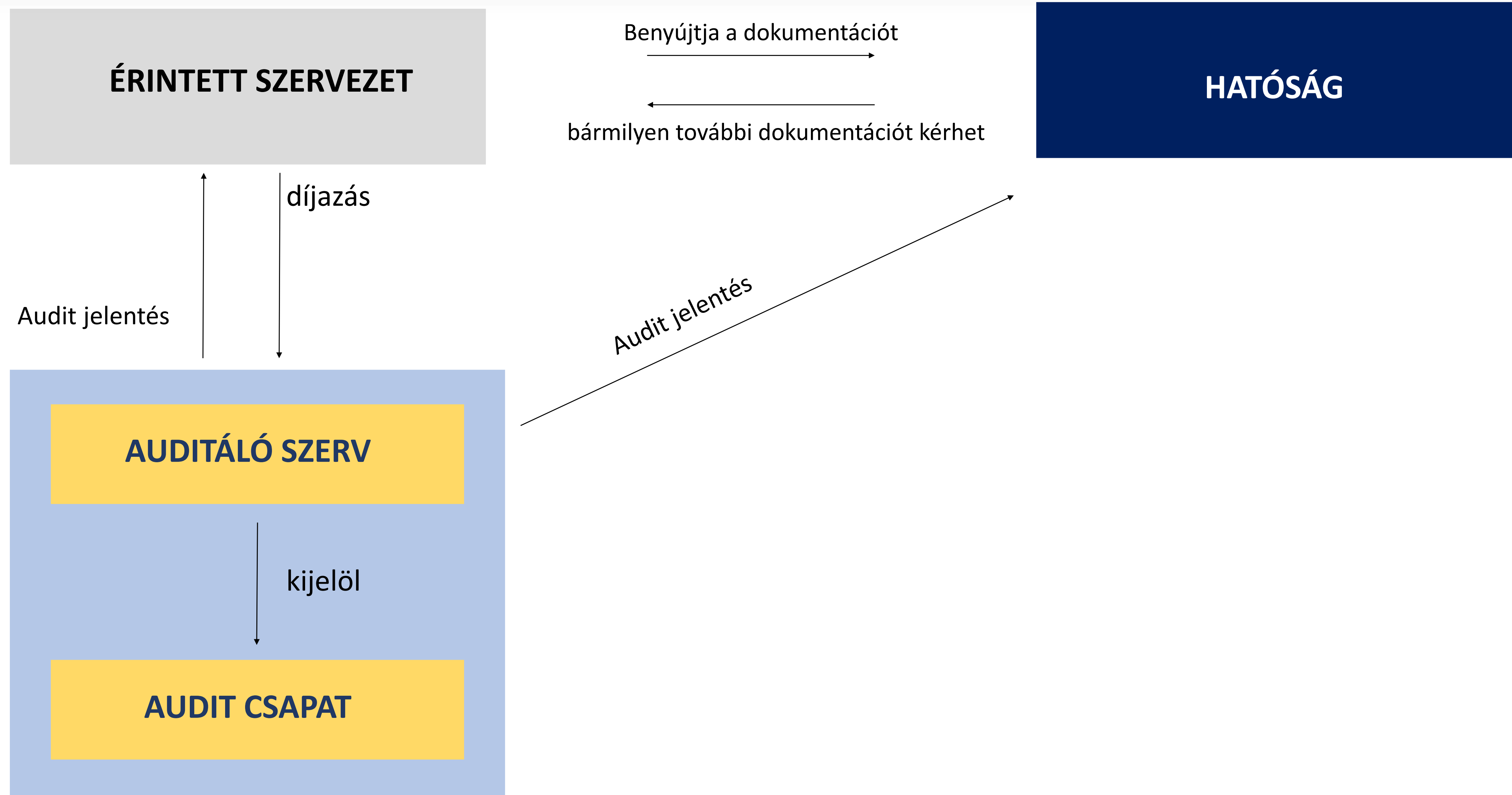
Auditorok

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

Kontrollszett

Követelménycsoport	Követelmény szövege	alap	jelentős	magas
Sikertelen bejelentkezési kísérletek	Az érintett szervezet: - Az általa meghatározott esetszám korlátot alkalmazza a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. - EIR-je automatikusan zárolja a felhasználói fiókot vagy csomópontot a meghatározott időtartamra, vagy ameddig a rendszergazda fel nem oldja annak zárolását, vagy késlelteti a következő bejelentkezési lehetőséget a meghatározott algoritmus szerint. Továbbá értesíti a rendszergazdát, ha a sikertelen próbálkozások maximális számát túllépték.	X	X	X
Eszköz zárolása	Az érintett szervezet: - Meghatározott időtartamú inaktivitás után vagy a felhasználó erre irányuló lépése esetén, az eszköz zárolásával megakadályozza az EIR-hez való további hozzáférést. - Fenntartja az eszköz zárolását mindaddig, amíg a felhasználó a megfelelő azonosítási és hitelesítési eljárásokat el nem végzi.	-	X	X
Munkaszakasz megszakítása – Megszakítási üzenet	Az EIR egyértelmű kijelentkezési üzenetet jelenít meg a felhasználók számára, amely jelzi a hitelesített kommunikációs munkaszakaszok befejezését.	-	-	-

Feladatok és felelősségek



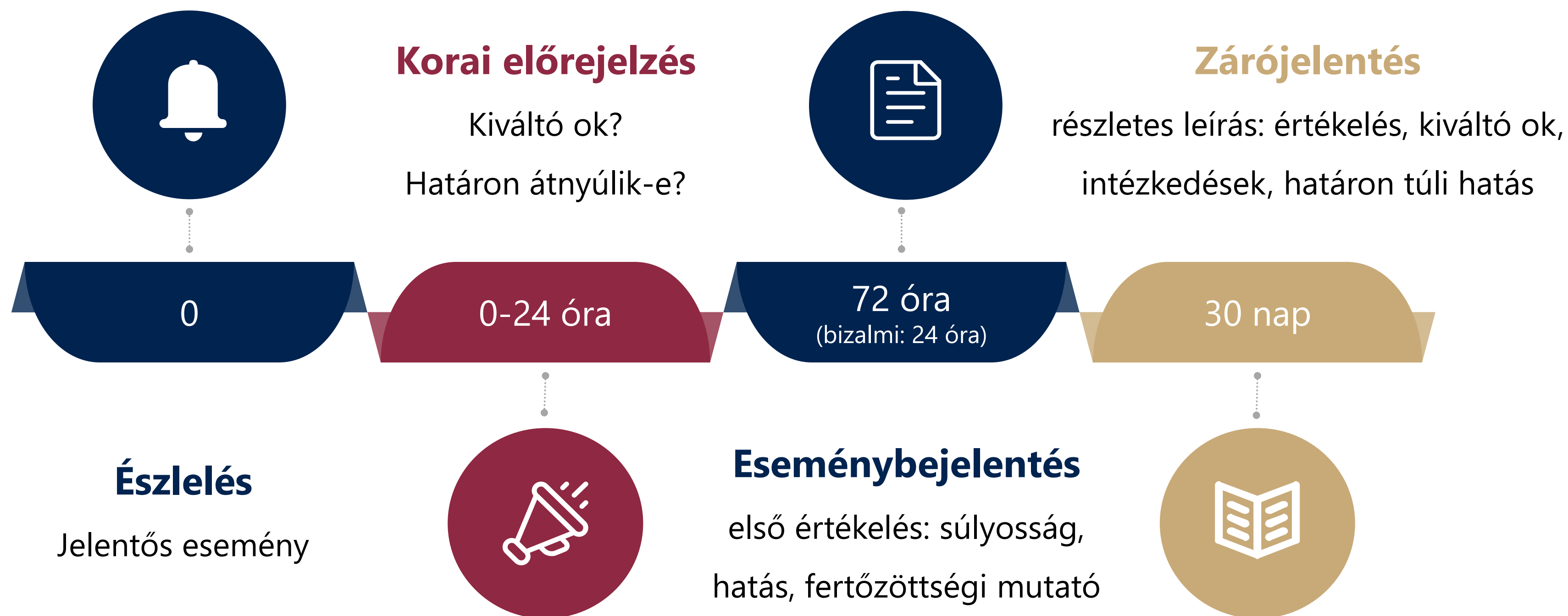
Biztonsági események jelentése

NIS1

olyan esemény, amely **ténylegesen** kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára

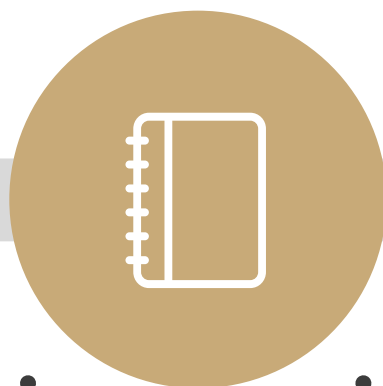
NIS2

olyan esemény, amely **veszélyeztet** a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát



Kiberbiztonsági felügyelet - ütemezés

2024. január 1.



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 biztonságaért 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

A₁

Szervezet mérete (Kkv tv.)

	mikro-	kis-	közép-	nagyvállalkozás	
foglalkoztatotti létszám	<10	<50	<250	≥250	fő
	és	és	és	vagy	
előző évi bevétel	<2	<10	<50	≥50	millió€
			vagy	vagy	
mérlegfőösszeg			<43	≥ 43	millió€

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

Mikro- vagy
kisvállalkozás

Vizsgálandó tevékenységek:

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

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

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

(ÖN)AZONOSÍTÁS

FELELŐS

TECHNIKAI
ADATOK

PARTNER
ADATOK

KÉRELEM

F

Ki láthatja el a feladatot?

A Kibertantv. nem szab feltételeket.

GYIK

Vegyünk fel plusz egy munkavállalót?

A szervezet mérlegelésén múlik...

Milyen tv-i kötelezettség van a kijelöléshez kapcsolódóan?

Kibertantv. 19. § (6) bekezdés a) pont

Külsőst bíznék meg, mire figyeljek?

Szakmai háttér, megbízhatóság, egyéb vállalt feladatai stb.

Megbízott jogi entitás esetén a szerződésben javasolt rögzíteni, hogy személy szerint ki fogja a feladatot ellátni!

Szükséges adatok

megbízott jogi entitás esetén:

- cég neve
- adószám
- cégjegyzékszám
- székhely

+

személy

- 4T adata
- telefonszáma (amin elérhető!)
- mail címe

Kiberbiztonsági felügyelet és vhr-ei

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

(ÖN)AZONOSÍTÁS

FELELŐS

TECHNIKAI
ADATOK

PARTNER
ADATOK

KÉRELEM



A szervezet nevére bejegyzett és általa használt domain nevek. (nem csak .hu!)

Domain nevek

IP-címek

FIX IP-címek (= dinamikus **X**), melyek a szervezethez rendelvek:

- egyedi IP-címként
- IP-tartományként (tól-ig)
- alhálózattal (/xx)

Olyan **informatikai háttérű szolgáltatás**, amely **széles körben elérhető**, pl:

- ✓ Telefonos ügyfélszolgálat
- ✓ Ügyfélportál
- ✓ Weboldal
- ✓ Online ügyfélszolgálat

Nyilvános
szolgáltatások

Kiberbiztonsági felügyelet és vhr-ei

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

(ÖN)AZONOSÍTÁS

FELELŐS

TECHNIKAI
ADATOK

PARTNER
ADATOK

KÉRELEM

P

Szolgáltatás:

Eht. 188. § 17. pont =

elektronikus hírközlési szolgáltató

általában **ellenszolgáltatásért** ... nyújtott szolgáltatás, amely [kivételekkel] magában foglalja

- a) az **internet-hozzáférési szolgáltatást**;
- b) a **személyközi hírközlési szolgáltatást**; és
- c) ... **jeleknek** elektronikus hírközlő hálózatokon történő **átviteléből**, ... **irányításából** álló szolgáltatást, ideértve a **gépek közötti szolgáltatást** és a **műsorterjesztésre használt átviteli szolgáltatást** is.

Ekertv. 2. § l) pont =

közvetítő szolgáltató

- egyszerű adatátvitel és hozzáférés-biztosítás
- gyorsítótárolás
- tárhelyszolgáltatás
- keresőszolgáltatás
- alkalmazásszolgáltató
- videómegosztóplatform-szolgáltató

Kibertantv. 19. § (4) bekezdés =

közreműködő

... **elektronikus információs rendszer** létrehozásában, **üzemeltetésében**, **karbantartásában** vagy **javításában** közreműködő ...

Partner

Kiberbiztonsági felügyelet és vhr-ei

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

(ÖN)AZONOSÍTÁS

FELELŐS

TECHNIKAI
ADATOK

PARTNER
ADATOK

KÉRELEM

K

Ki indíthatja?

az érintett szervezet cégkapujához meghatalmazással rendelkező természetes személy

Honnan indítható?

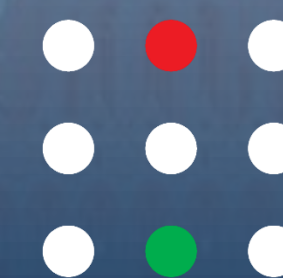


- magyarorszag.hu-ról kereséssel: **SZTFH 420 Érintett szervezet nyilvántartásba vételére irányuló kérelem**
- **SZTFH honlapjáról** (sztfh.hu): Ügyintézés/Nyomtatványok és űrlapok/ Kiberbiztonsági Ügyek/SZTFH 420/Részletek

Köszönöm a
figyelmet!

dr. Bencsik Balázs

kiberbiztonsag@sztfh.hu



SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága