# Kiberbiztonsági szabályozás

# Kibertantv.


**dr. Bencsik Balázs**

Kiberbiztonsági Tanúsítási Igazgatóság

# Európai Uniós 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

# Kiket érint? – kiemelten kritikus ágazatok

**ENERGIA**
villamosenergia, olaj, földgáz, távhő, **hidrogén**

**BANKI ÉS PÉNZÜGYI SZOLGÁLTATÁSOK**

**VÍZ**
ivóvíz, szennyvíz

**DIGITÁLIS INFRASTRUKTÚRÁK**
hírközlés, IXP-k, **bizalmi szolgáltatók**, felhő- és **adatközpont szolgáltatók**, TLD-nyilvántartók, DNS-szolgáltatók

**VILÁGŰR**
**földi támogató infrastruktúrák**

**SZÁLLÍTÁS**
légi, vasúti, vízi, közúti

**EGÉSZSÉGÜGY**
egészségügyi szolgáltatók, **referencialaboratóriumok**

**KÖZIGAZGATÁS**

**GYÓGYSZERIPAR**
**K+F, gyógyszeralapanyag és gyógyszerkészítmény gyártás, kritikus orvostechnikai eszközök**

**KIHELYEZETT (BIZTONSÁGI) SZOLGÁLTATÓK**

# Kiket érint? – kritikus ágazatok

**POSTAI- ÉS FUTÁRSZOLGÁLATOK**

**ELEKTRONIKAI GYÁRTÁS**

**orvostechnikai eszközök, elektronikai- és optikai termékek, villamos berendezések, egyéb gépek**

**JÁRMŰGYÁRTÁS**

**járművek, pótkocsik**

**KUTATÓHELYEK**

**HULLADÉKGAZDÁLKODÁS**

**ÉLELMISZER ELŐÁLLÍTÁS ÉS FORGALMAZÁS**

**DIGITÁLIS SZOLGÁLTATÁSOK**

online piactér, online keresőmotor, **közösségimédia-szolgáltatási platform**

**VEGYIPARI GYÁRTÁS ÉS FORGALMAZÁS**

# Kiberbiztonsági felügyelet – érintett szervezetek

| Kategória | Főtevékenység | Teljes tevékenységi kör |
|---|---|---|
| Kiemelten kockázatos ágazatok | 432 | 528 |
| Kockázatos ágazatok | 1247 | 339 |
| **Összesen** | 1679 | 867 |
| | **2546** | |


**50 és 10M €**

**250 és 50M €**

**NIS 2**

**Több, mint 50 vagy 10M €**

# Kiberbiztonsági felügyelet – érintett feladatai

## Vezetői feladatok

Biztonságért felelős személy

Szervezeti szabályozások

Tudatosító oktatások és szinten tartás

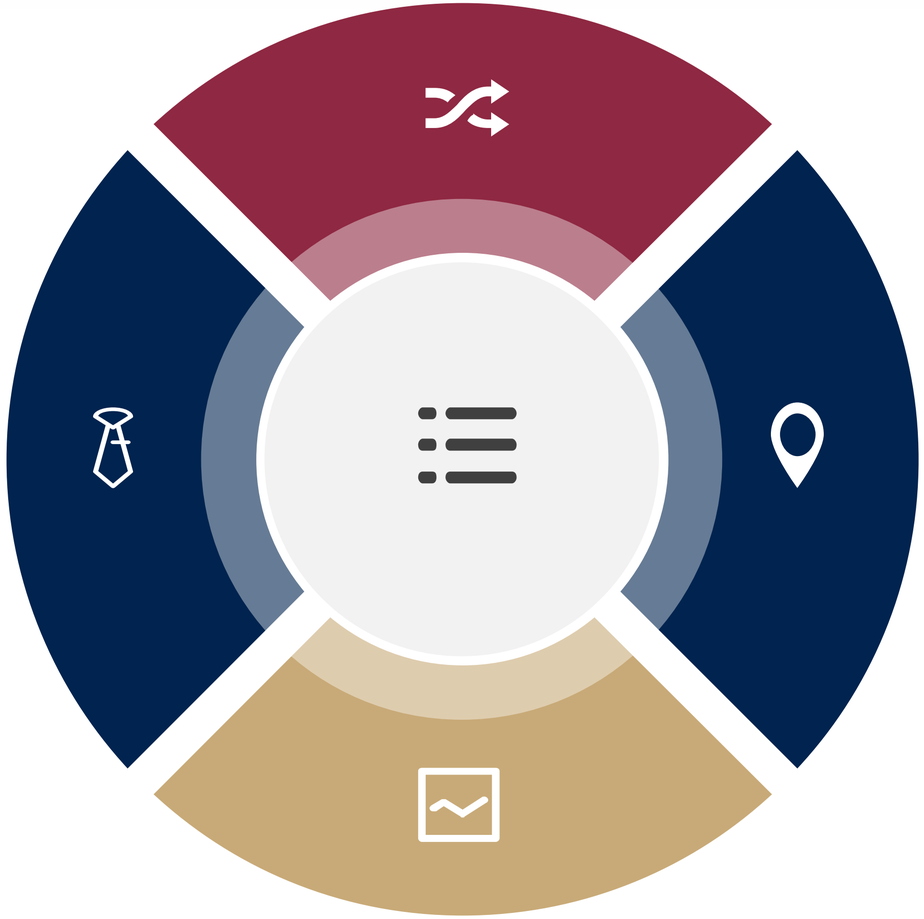
Kiberbiztonsági audit megrendelése

## 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

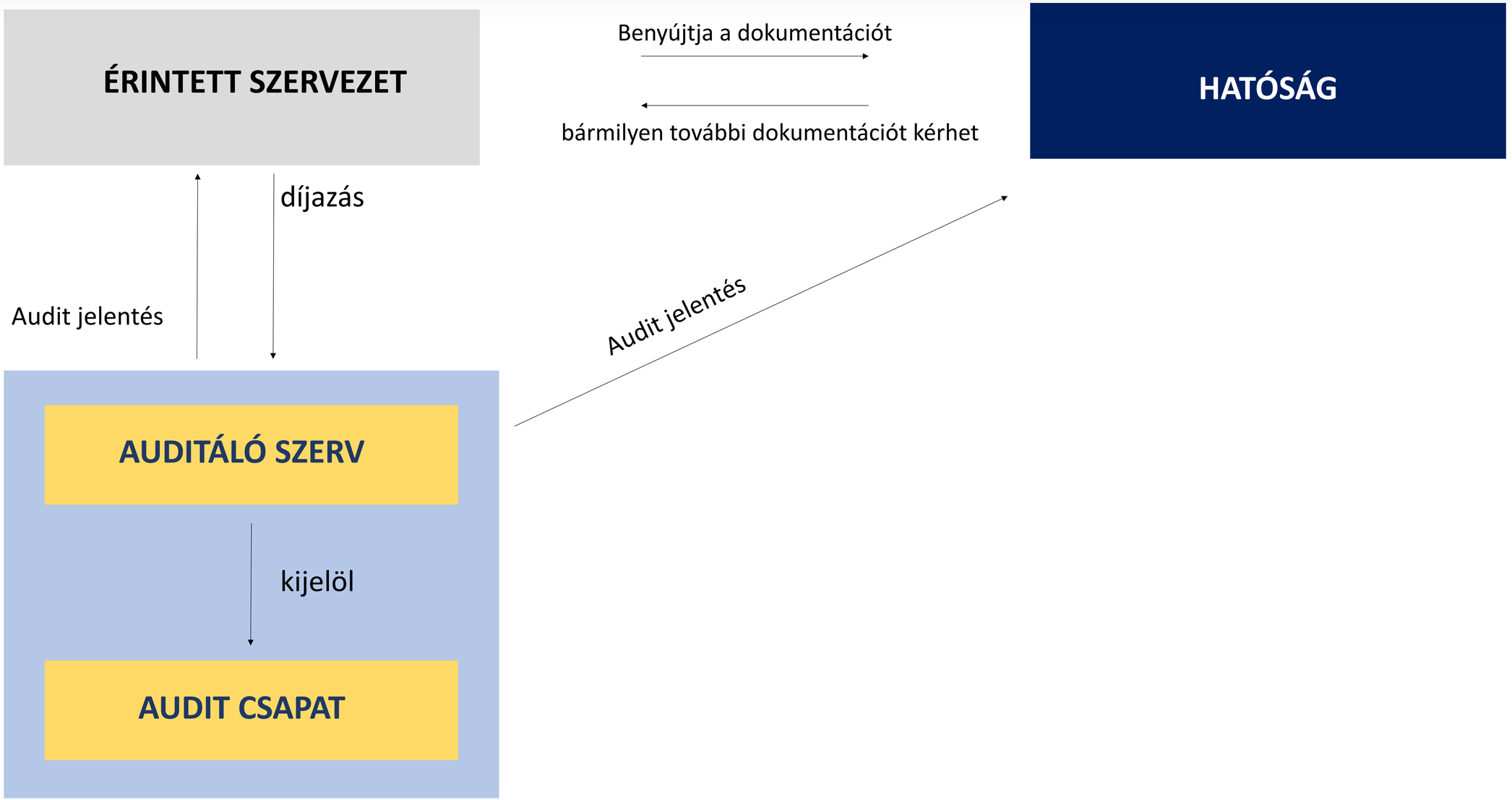
## SZTFH

- 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



# Fogalmak

**Kiberbiztonsági audit**

Az elektronikus információs rendszerek tekintetében a kiberbiztonsági követelmények teljesülésére vonatkozó vizsgálat, ellenőrzés.

**Audit jelentés**

Az ellenőrzési eredményeket tartalmazó dokumentum.
Az ellenőrzési jelentést az ellenőrző szerv készíti el, és bemutatja az érintett szervezetnek és a hatóságnak. A hatóság kérheti a felülvizsgálat alapjául szolgáló dokumentáció (pl. informatikai biztonsági koncepciók, folyamatdokumentáció, audit jelentés, üzletmenet-folytonosság-kezelés és kontingenciakoncepciók) benyújtását.

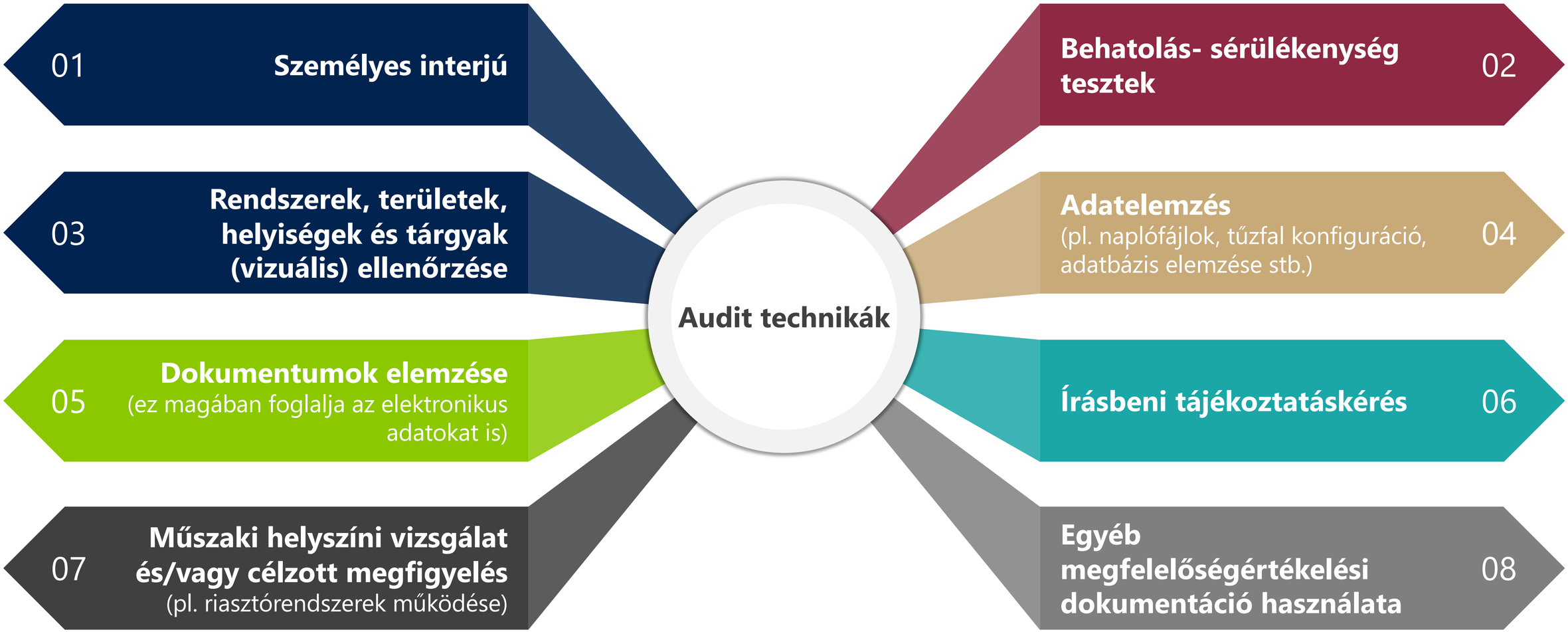
# Ellenőrzés témái és technikái


**Ebben az összefüggésben azokat az vizsgálandó szempontokat kell megvizsgálnia és értékelnie az auditornak, mint minimum:**

- ✓ **az alapvető szolgáltatás funkcionalitását**
- ✓ **alkalmasságot és szükségességet**
- ✓ **teljességet**

# Lehetséges audit technikák

**Audit technikák alatt egy helyzet felmérésére szolgáló metódust értünk. Egy audit során különböző technikák is alkalmazhatók az alábbiak közül.**



# Audit mélység

**Az első alkalommal végzett ellenőrzések mélységének meghatározása magában foglalja például:**

# Hiányosság kategóriák

A biztonsági hiányosságokat két dimenzióba kell osztályozni:

1. Az érintett IT-biztonsági probléma
2. A hiányosság súlyossága


**Súlyos vagy jelentős eltérés/biztonsági hiányosság**

Sürgős cselekvésre van szükség. Az eltérést azonnal vagy amilyen gyorsan csak lehetséges, el kell távolítani, mivel az alapvető szolgáltatás bizalmassága, integritása, hitelessége vagy elérhetősége súlyosan veszélyeztetett, és jelentős károkra lehet számítani.

**Kisebb eltérés/biztonsági hiányosság**

Egy "kisebb eltérés" fenyegetést és kockázatot jelent. Nincs sürgős cselekvésre szükség. Az alapvető szolgáltatás bizalmasságát, integritását, hitelességét vagy elérhetőségét középtávon kell helyreállítani.

**Ajánlás**

Az "ajánlás" egy javaslat a fejlesztésre. Az ajánlás végrehajtásával növelhető a biztonság.

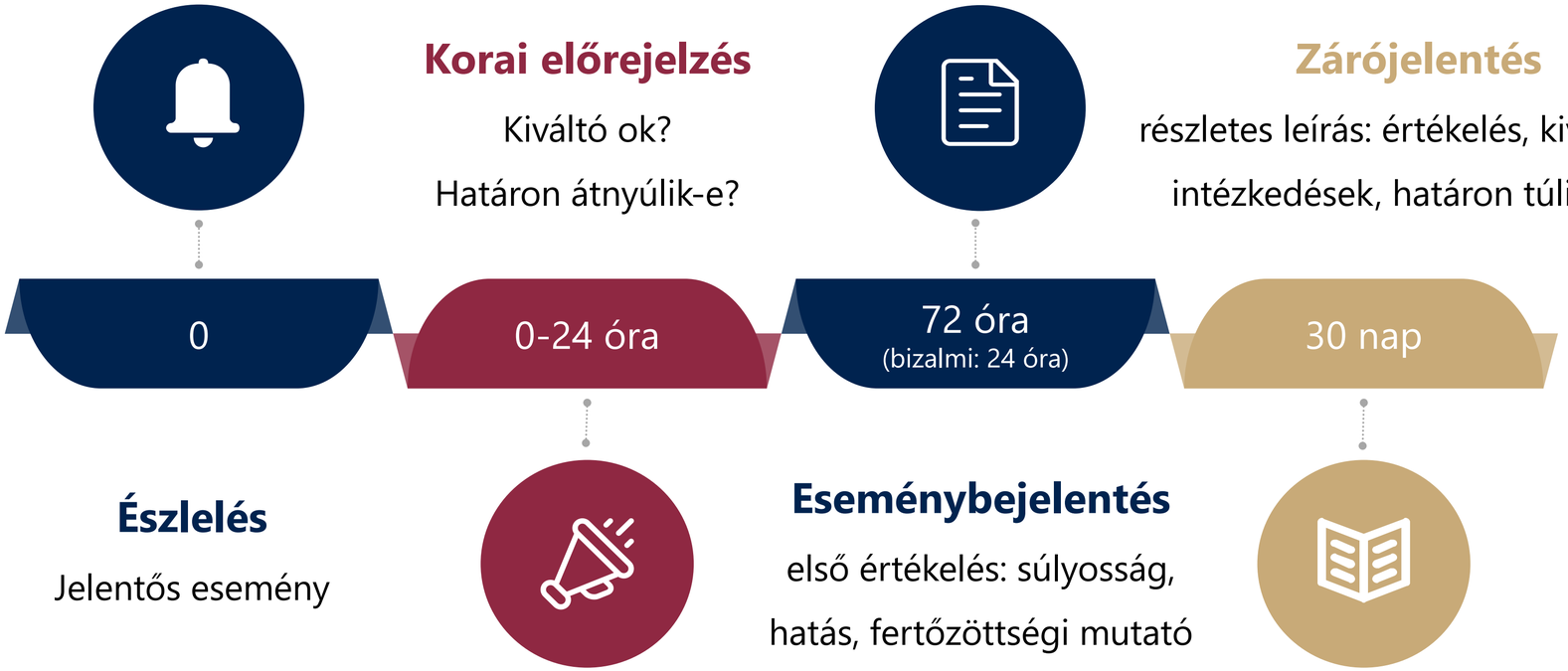
**Nincs eltérés**

Nincs biztonsági hiányosság, ha az összes követelményt teljes egészében betartották, és ha minden védelmi intézkedést teljes mértékben, hatékonyan és megfelelően hajtottak végre.

# Biztonsági események jelentése

**NIS1** olyan esemény, amely **ténylegesen** kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára

**NIS2** olyan esemény, amely **veszélyezteti** 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<br>• Auditorok nyilvántartásba vétele | • Felügyeleti tevékenység<br>• Ellenőrzési tevékenység | | |
| **Érintett szervezet** | • Önazonosítás, nyilvántartásba vételre bejelentkezés 2024. június 30-ig<br>• Biztonsági osztályba sorolás<br>• Elektronikus információs rendszerek biztonságáért felelős személy feladatköre és kijelölése | • Védelmi intézkedések alkalmazása<br>• Felügyeleti díj megfizetése | • Első kiberbiztonsági audit vonatkozásában szerződéskötés az auditorral | • Első kiberbiztonsági audit lefolytatásának határideje |

# Köszönöm a figyelmet!

**dr. Bencsik Balázs**

kiberbiztonsag@sztfh.hu

LinkedIn

MINDEN KIBERÜL

SZTFH

Szabályozott Tevékenységek Felügyeleti Hatósága