NIS 2 update!

Hogy állunk most?

Bor Olivér

kiberbiztonsági és kommunikációs szakértő

egyetemi vendégoktató

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága

Fenyegetések (ENISA 2023-es jelentése alapján)

Ransomware

Az érintett szervezetek ~40%-a fizetett

Internet infrastruktúra elleni támadás

Leállás, aktív cenzúra, forgalomátirányítás

Dezinformáció

Ellátási lánc elleni támadás

2020-ban < 1%, 2021-ben >17%

2022-ben 61%

Malware

Egyre több 0.day, egyre több mobilos kártevő

Social engineering

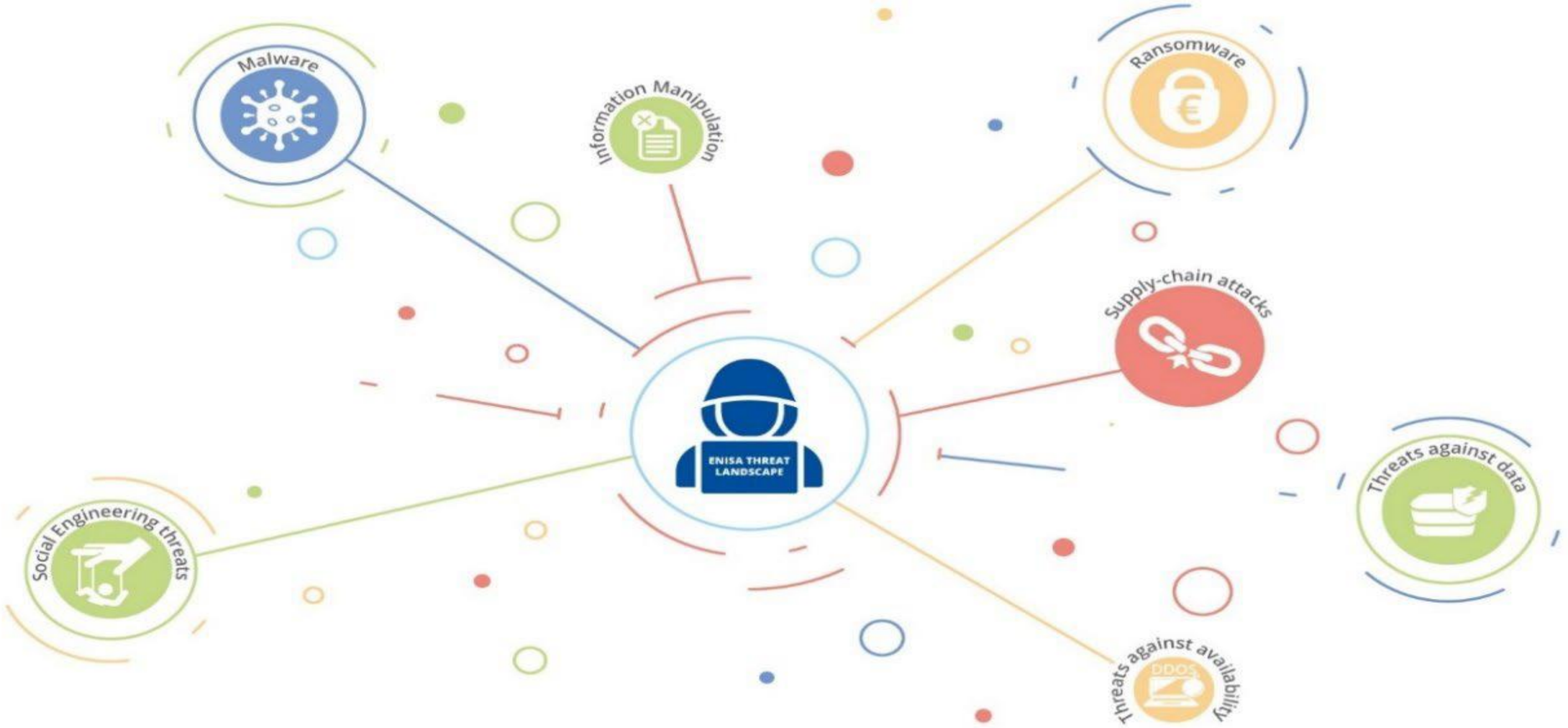
BEC, Spear-phising, whaling, smishing, vishing

Adatokkal kapcsolatos fenyegetés

Szolgáltatásmegtagadásos támadás

Orosz-ukrán konfliktus óta nem látott mértékben növekszik…

Fenyegetések (ENISA 2024-es jelentése alapján)



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 €

NIS2

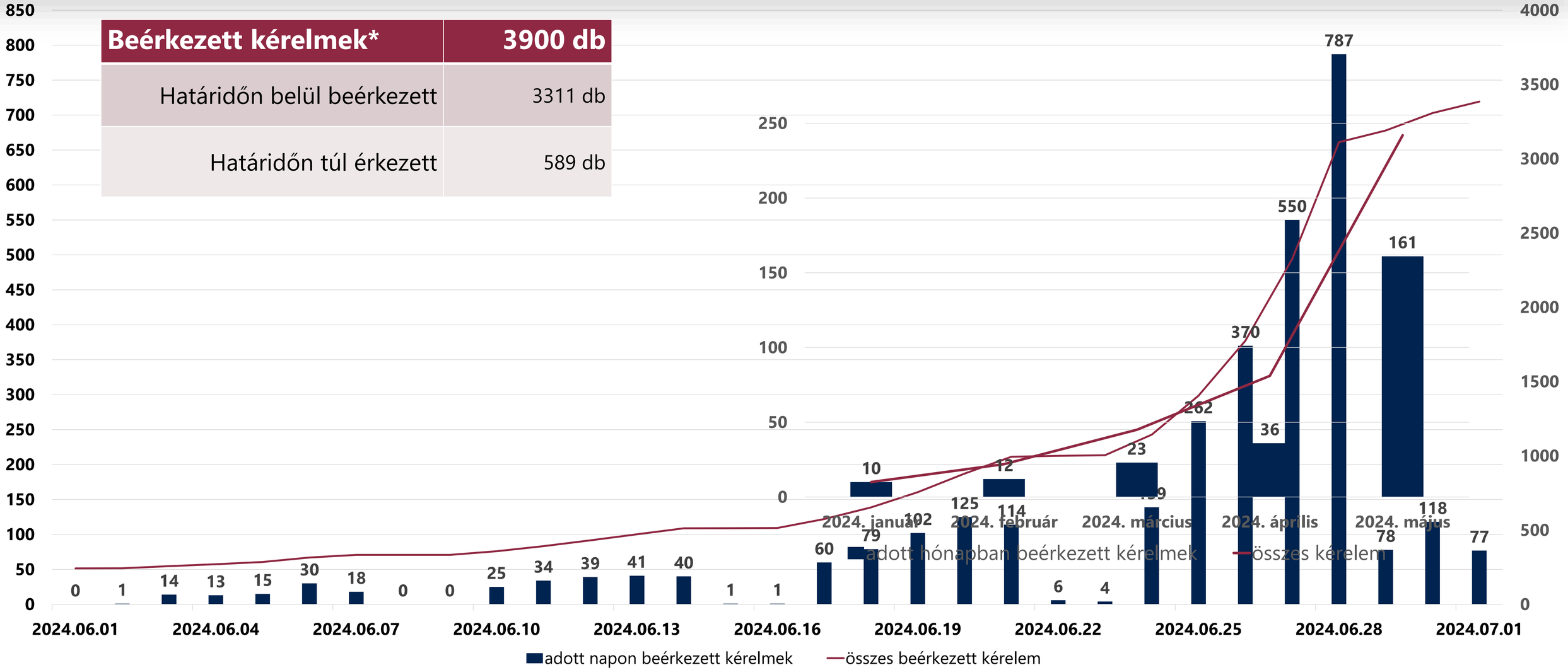
Nyilvántartásba bejelentkezett

~3900

Több, mint 50 vagy 10M €

Nyilvántartásba vételi kérelmek számokban

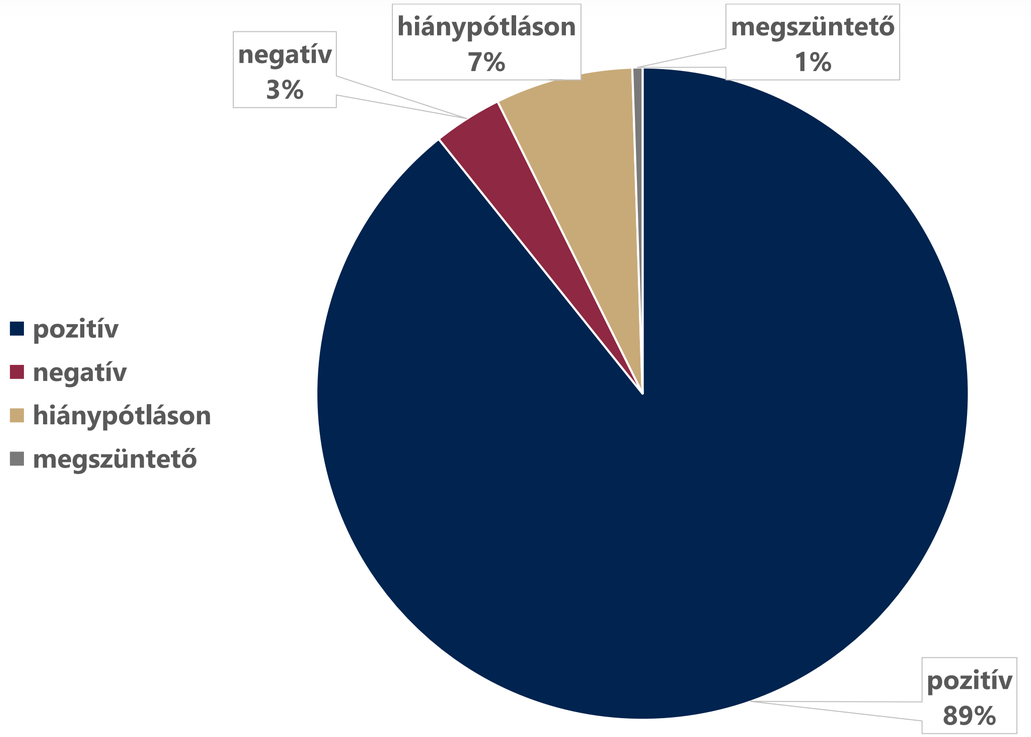
Beérkezett kérelmek*	3900 db
Határidőn belül beérkezett	3311 db
Határidőn túl érkezett	589 db



* 2024. november 11-ei állapot, többszörös beadások miatt még korrigálódhat

Nyilvántartásba vételi kérelmek feldolgozása

A hatósági eljárásban a tényállás tisztázása a cél, hogy az adott szervezet valóban érintett-e!



Hiánypótlások okai:

1. Rossz tevékenység-megjelölés
   - véletlen („azt hittem, hogy…”)
   - szándékolt („negatív határozatban reménykedtem”, „azt mondta az IT-s, hogy mindegy milyen adatokkal, de adjuk be”)
2. A megjelölt tevékenység igazolása közhiteles nyilvántartásokból nem lehetséges
   - kérelmező felszólítása (tipikusan NÉBIH esetén)
   - szakhatósági megkeresés keretében, egyedileg tisztázza az SZTFH a helyzetet
3. Nem is középvállalkozás…

* A diagram arányosított értékeket tartalmaz, azzal, hogy a hiánypótlási kör eredménye befolyásolja a hatósági döntést!

Nyilvántartásba vétel elmulasztása

	A	B	C
1.	A szabálytalanság megnevezése	A bírság legkisebb mértéke	A bírság legnagyobb mértéke
2.	A Kibertan.tv. 26. § (1) bekezdése szerinti nyilvántartásba vétel érdekében történő **adatszolgáltatás nem teljesítése**	az érintett szervezet **előző üzleti évi nettó árbevétel**ének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának **0,5%-a, de legalább 1 000 000 forint**	az érintett szervezet **előző üzleti évi nettó árbevétel**ének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának **legfeljebb 2%-a**, de **legfeljebb 150 000 000 forint**
3.	A Kibertan.tv. 26. § (1) bekezdése szerinti nyilvántartásba vétel érdekében történő a**datszolgáltatás határidőn túl történő teljesítése**	**50 000 forint**	az érintett szervezet **előző üzleti évi nettó árbevétel**ének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – vagy előző évi költségvetési bevételi előirányzatának **legfeljebb 0,1%**-a, de **legfeljebb 15 000 000 forint**

… 2024. október 18-tól!

Felügyeleti díj – jövőbeni SZTFH rendelet*

Mennyi az annyi?

Törvényi maximum 0,015% vagy 10 millió HUF

nem a maximális % lesz!

sávozás várható

Mikorra?

Törvény szerint október 18-TÓL

≠ fizetési határidővel

valószínűleg jövőre

Ki állapítja meg?

A szervezet, de segíteni fogunk…

Fizetés módja?

Utalással

SZTFH számlára, meghatározott közleménnyel

* Ezek tervek, konkrétumok SZTFH rendeletben várhatóak!

Követelménykatalógus – 7/2024 MK rendelet

Védelmi intézkedés kategória (7/2024. MK rendelet 2. melléklete alapján)	Biztonsági osztály			Védelmi intézkedések száma				
	Alap	Jelentős	Magas	Alap	Jelentős	Magas	Kiegészítő	Összesen
PROGRAMMENEDZSMENT				20	0	0	3	23
HOZZÁFÉRÉS-FELÜGYELET				11	28	7	83	129
TUDATOSSÁG ÉS KÉPZÉS				5	1	0	8	14
NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG				10	6	9	27	52
ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS				9	2	3	12	26
KONFIGURÁCIÓKEZELÉS				9	12	9	23	53
KÉSZENLÉTI TERVEZÉS				5	17	13	14	49
AZONOSÍTÁS ÉS HITELESÍTÉS				12	9	2	27	50
BIZTONSÁGI ESEMÉNYEK KEZELÉSE				7	6	5	20	38
KARBANTARTÁS				4	5	3	13	25
ADATHORDOZÓK VÉDELME				4	3	3	8	18
FIZIKAI ÉS KÖRNYEZETI VÉDELEM				10	8	7	24	49
TERVEZÉS				6	1	0	4	11
SZEMÉLYI BIZTONSÁG				9	0	1	3	13
KOCKÁZATKEZELÉS				7	5	0	10	22
RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS				9	7	4	80	100
RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM				10	15	5	102	132
RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG				6	12	10	55	83
ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSE				11	1	2	13	27
				164	138	83	529	914

Auditor feltételek – 7/2024. SZTFH rendelet

FELTÉTELEK

Legalább két műszaki vagy informatikai felsőfokú végzettség.

Referencia: alap biztonsági osztály esetén legalább 5, jelentős biztonsági osztály esetén legalább 15.

Felelősségbiztosítás: alap biztonsági osztály esetén min. 15 millió forint, jelentős biztonsági osztály esetén min. 50 millió forint.

Sérülékenységvizsgálat lefolytatására alkalmas gazdálkodó szervezetek nyilvántartása -> TBT

Magas biztonsági osztály esetén szerepelni kell a SZTFH elnökének az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendelete szerinti megfelelőségértékelő szervezetek jegyzékén „magas” megbízhatósági szinten.

- 250 millió forintos felelősségbiztosítás
- Elmúlt 9 évben legalább 7 éven keresztül TBT
- Legalább 10 fő rendelkezik SZBT-vel

Kiberbiztonsági ellenőrzés

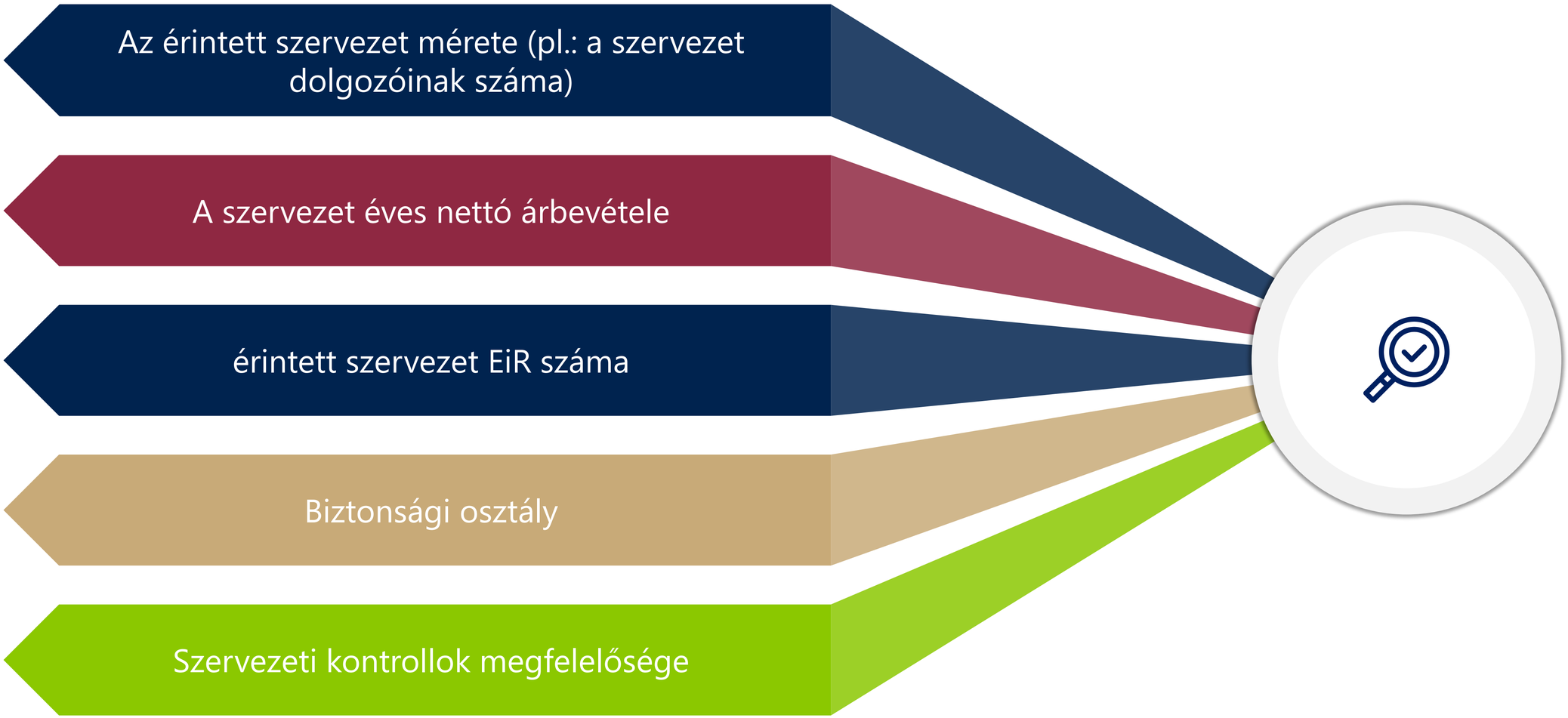
Auditorok

Szervezet	Biztonsági osztály
Alverad Kft.	Alap
Certop Kft.	Jelentős
Ernst & Young Kft.	Alap
Hunguard Kft.	Magas
Kürt Zrt.	Jelentős
NETI Kft.	Alap
Valilab Kft.	Alap
Veritan Kft.	Alap

Auditálás

- Szerződés alapján
- SZTFH rendelet előírásai szerint:
  - Biztonsági osztályba sorolás
  - Védelmi intézkedések vizsgálata
  - Sérülékenységvizsgálat
  - Behatolásvizsgálat, forráskód-vizsgálat
- Kétévente kötelező

Auditálás díj-maximuma - tényezők



Fogalmak és egy kis matek

Kiberbiztonsági audit

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

Audit jelentés

Az ellenőrzési eredményeket tartalmazó dokumentum:

- $VMI(\textit{Védelmi Megfelelőségi Index}) = 100 - 100 * \frac{2*\sum_{i=1}^{n} b_i + \sum_{j=1}^{m} t_j}{20n+10m}$
  - Minősítés: az elektronikus információs rendszer a védelmi intézkedéskatalógus elvárásainak -> megfelel, alacsony kockázattal felel meg stb.

- $SZEKI(Szervezet\ ellenálló - képességi\ index) = \frac{\sum_{i=1}^{n} VMI_i}{n}$
  - Minősítés: a szervezet a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló törvény szerinti kiberbiztonsági auditon megfelelt stb.

Köszönöm a figyelmet!

LinkedIn

kiberbiztonsag@sztfh.hu

SZTFH

Szabályozott Tevékenységek
Felügyeleti Hatósága