

A kiberbiztonsági incidensek észlelése és az azokra való reagálás

Az uniós együttműködési keret kidolgozása jól halad, de a végrehajtás késedelmei és az elégtelen információmegosztás miatt még csak részben eredményes



Tartalomjegyzék

Bevezetés

01–23 | **Főbb megállapítások**

01–07 | **Miért fontos ez a terület?**

08–23 | **Megállapításaink és ajánlásaink**

24–01 | **Észrevételeinkről részletesebben**

24–74 | Az uniós kiberbiztonsági hálózatok és mechanizmusok támogatják az együttműködést és a reagálást, de az elégtelen információmegosztás és a hiányos végrehajtás csökkenti eredményességüket

24–51 | Az uniós hálózatok lehetővé teszik a tagállamok közötti együttműködést, de az elégtelen információmegosztás csökkenti hozzáadott értéküket

52–61 | Az uniós kiberbiztonsági tartalék az incidensekre való reagáláskor gyors szolgáltatásnyújtást tesz lehetővé

62–74 | Az európai kiberbiztonsági figyelmeztető rendszer célja a fenyegetések észlelését lehetővé tevő kapacitások javítása, de a rendszer nem működik

75–01 | A DIGITAL program keretében uniós finanszírozásban részesülő projektek célja a kiberbiztonság megerősítése, de e projektek a végrehajtás és a beszámolás terén kihívásokkal szembesülnek

75–81 | Késedelmes létrehozása miatt a kiberbiztonsági kompetenciaközösség nem tudta igényeinek megfelelően alakítani a DIGITAL programot

82–96 | Az uniós finanszírozású projektek célkitűzései relevánsak, de sok projekt operatív problémákkal küzd

97–01 | A legtöbb uniós finanszírozású projekt nem rendelkezik megfelelő teljesítménymérési kerettel, és a DIGITAL program kiberbiztonsággal kapcsolatos teljesítményadatai nem pontosak

Mellékletek

I. melléklet. Az ellenőrzésről

II. melléklet. Az Európai Unió kiberbiztonsági környezete

III. melléklet. Kiválasztott kiberbiztonsági fellépések

IV. melléklet. Az uniós finanszírozású kiberbiztonsági projektek számvevőszéki értékelése

Rövidítések

Glosszárium

A Bizottság válaszai

Az Európai Kiberbiztonsági Kompetenciaközpont (ECCC) válaszai

Az Európai Unió Kiberbiztonsági Ügynökség (ENISA) válaszai

Időrendi áttekintés

Ellenőrző csoport

Főbb megállapítások

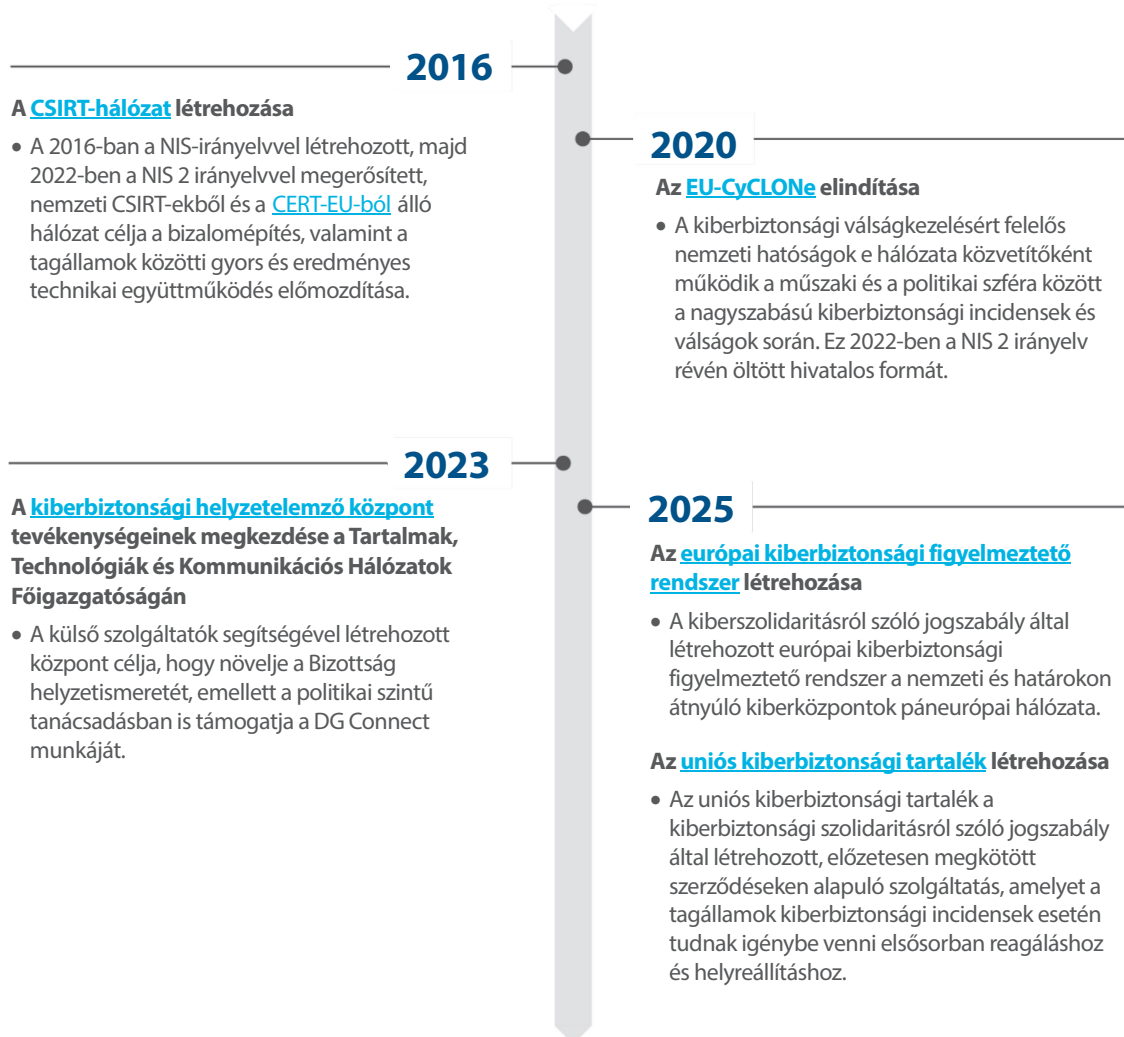
Miért fontos ez a terület?

- 01** Gazdaságunk és mindennapi életünk egyre nagyobb mértékű digitalizálódásával a kibertámadások kockázata is növekszik. Meghatározása szerint a kiberbiztonság „a hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és a kiberfenyegetések által érintett egyéb személyeknek a védelméhez szükséges tevékenységeket” jelenti¹. A kiberbiztonság holisztikus megközelítést igényel, amely a kiberfenyegetések megelőzésére, észlelésére, az azokra való reagálásra és az azokat követő helyreállításra irányuló tevékenységekből áll.
- 02** Az Európai Unió kiberbiztonsági környezete számos magán- és közszervezetet foglal magában regionális, nemzeti és uniós szinten a polgári szférából. A kiberbiztonság a nemzetbiztonságnak és nemzetvédelemnek is kulcsfontosságú alkotóeleme.
- 03** Elsődlegesen a tagállamok felelősek az őket érintő kiberbiztonsági incidensek és válságok megelőzéséért, az azokra való felkészülésért és reagálásért. Mivel az ilyen incidensek a belső piac zökkenőmentes működését is befolyásolhatják, jelentős incidensek vagy válságok fellépése esetén az Unió is fontos szerepet játszik. Az elmúlt években az Unió megerősítette folyamatosan változó kiberbiztonsági szabályozási keretét², továbbá hálózatokat és mechanizmusokat hozott létre (lásd: az alábbi **1. ábra** és **II. melléklet**).

¹ (EU) 2019/881 rendelet ([kiberbiztonsági jogszabály](#)).

² A Bizottság 2025 novemberében például javaslatot tett a [digitális omnibusz csomagra](#), 2026 januárjában pedig a felülvizsgált [uniós kiberbiztonsági jogszabályra](#).

1. ábra | Uniós kiberbiztonsági hálózatok és mechanizmusok, 2016–2025



CSIRT : számítógép-biztonsági incidensekre reagáló csoport

DG Connect: a Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága

EU-CyCLONe: az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata

NIS-irányelv: (EU) 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

NIS 2 irányelv: (EU) 2022/2555 irányelv az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről

Forrás: Európai Számvevőszék.

- 04** A jelenlegi, 2021–2027-es többéves pénzügyi keretben a kiberbiztonság finanszírozásának fő forrása a **Digitális Európa (DIGITAL) program**. E program teljes költségvetése 8,1 milliárd euró, amelyből 1,4 milliárd eurót a kiberbiztonság megerősítésére különítettek el.

05 Ellenőrzésünk célja annak értékelése volt, hogy az uniós fellépések eredményesen segítik-e elő a jelentős és nagyszabású kiberbiztonsági incidensek észlelését és az azokra való reagálást. A következők esetében értékeltük, hogy ez így volt-e:

- uniós szintű hálózatok és mechanizmusok (azaz a számítógép-biztonsági incidensekre reagáló csoportok hálózata [CSIRT-hálózat], az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata [EU-CyCLONE], az európai kiberbiztonsági figyelmeztető rendszer, a kiberbiztonsági helyzetelemző központ és az uniós kiberbiztonsági tartalék);
- a Digitális Európai (DIGITAL) program keretében finanszírozott intézkedések.

06 Reményeink szerint megállapításaink hozzájárulnak az Unió kiberrezilienciájának megerősítéséhez azáltal, hogy javítják az uniós hálózatok és mechanizmusok eredményességét és hatékonyságát, valamint az uniós finanszírozású intézkedések kiválasztásának és nyomon követésének módját.

07 Ellenőrzésünk a 2022 és 2025 közötti időszakra terjedt ki. Munkánk a vonatkozó dokumentumok vizsgálatán és elemzésén, három tagállamban (Írországban, Görögországban és Olaszországban) tett ellenőrző látogatásokon, valamint írásbeli kérdőíveken és az érintett érdekelt felekkel folytatott interjúkon alapul. Az ellenőrzés hatókörére és módszerére vonatkozó további háttér-információkat és részleteket az [I. melléklet](#) tartalmazza.

Megállapításaink és ajánlásaink

08 Összességében arra a következtetésre jutottunk, hogy az uniós intézkedések csak részben könnyítik meg a jelentős és nagyszabású kiberbiztonsági incidensek észlelését és az azokra való reagálást. Bár fokozatosan létrejött az együttműködési keret, a teljes rendszer felépítésére irányuló munka még jelenleg is folyik. Az elégtelen információmegosztás, az adatszolgáltatással kapcsolatos hiányosságok és a jelentős végrehajtási késedelmek miatt az uniós hálózatokban és mechanizmusokban rejlő lehetőségek nem használhatók ki teljes mértékben. A DIGITAL program által finanszírozott projektek releváns célokat tűztek ki, azonban közülük több is működési nehézségekkel és késedelmekkel küzd, és az átfogó teljesítménymonitoring-keretben is vannak hiányosságok.

- 09** A jelentős kiberbiztonsági incidensek észlelését és az azokra való reagálást elősegítő uniós hálózatok és mechanizmusok jelenlegi keretét fokozatosan alakították ki. A Tanács 2025-ben fogadta el a [kiberbiztonsági tervet](#), amely meghatározza a kiberválság-kezelés uniós keretét. Megállapítottuk, hogy a kiberbiztonsági terv általában véve tisztázza az uniós kiberválság-kezeléssel kapcsolatos feladat- és felelősségi köröket. Mindazonáltal a 2016-ban létrehozott CSIRT-hálózat és a hivatalosan 2023-ban működésbe lépett EU-CyCLOne együttműködésének módjára vonatkozó eljárási szabályok még nem öltöttek hivatalos formát ([24–30. bekezdés](#)).
- 10** Megállapítottuk, hogy e hálózatokon keresztül nem teljes körűen kerülnek megosztásra az információk. Ez főként [az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelv](#) (NIS 2 irányelv) késedelmes átültetésének, az incidensek határokon átnyúló hatása megállapításával kapcsolatos nehézségeknek, valamint az információmegosztást akadályozó nemzetbiztonsági jogszabályoknak tudható be. A hálózatok hozzáadott értéke jelentősen csökken, ha a tagállamok nem hajlandók időszerű és hasznosítható információkat megosztani ([31–44. bekezdés](#)).



1. ajánlás

A tagállamok közötti információmegosztás javítása

A kiberbiztonsági incidensek észlelésének és az azokra való reagálásnak a javítása érdekében a Bizottság az Európai Unió Kiberbiztonsági Ügynökség (ENISA) támogatásával:

- a) javasolja a hálózat- és információbiztonsággal foglalkozó együttműködési csoportnak, hogy végezzen részletes elemzést azokról a nemzetbiztonsági szabályozásokról, amelyek korlátozzák az információmegosztást és ezáltal befolyásolják az Unió kiberrezilienciáját, továbbá határozzon meg jogi és technikai megoldásokat az információmegosztás fokozására, a nemzetbiztonság határainak tiszteletben tartása mellett;
- b) a társjogalkotók határozatainak sérelme nélkül a tagállamokkal együttműködve biztosítsa, hogy a digitális omnibusz csomagban javasolt, a biztonsági incidensek bejelentésére szolgáló egyablakos ügyintézési pont képes legyen észlelni a potenciálisan határokon átnyúló incidenseket;
- c) dolgozzon ki olyan megoldásokat, amelyek lehetővé teszik a biztonsági incidensek valós idejű bejelentését az ENISA-nak.

Megvalósítás céldátuma: a) és b) esetében 2027, c) esetében 2028

- 11** 2022-ben a Bizottság egy külön részlegként „kiberbiztonsági helyzetelemző központot” hozott létre annak érdekében, hogy válságkezelési intézményi feladatainak jobb elvégzéséhez növelje helyzetismeretét. A központ működése elsősorban a külső szolgáltatókkal kötött szerződésen alapul. Megállapítottuk, hogy a helyzetismeret és a fenyegetések nyomon követése tekintetében a külső szolgáltatók által végzett munka részben átfedésben van az Európai Unió Kiberbiztonsági Ügynökség (ENISA) meglévő kapacitásával. Meglátásunk szerint a kiberbiztonsági helyzetelemző központot anélkül hozták létre, hogy a Bizottság és az ENISA által már rendelkezésre bocsátott információkat felhasználva kellőképpen kihasználták volna a racionalizálásban rejlő lehetőségeket. Ezenkívül az, hogy nincs átfogó, részletes terv a szerződés lejárta utáni időszakra vonatkozóan, kockázatot jelent a kiberbiztonsági helyzetelemző központ 2026 utáni működése szempontjából (45–51. bekezdés).



2. ajánlás

Az Unió kiberbiztonsági helyzetismereti képességeinek érszserűsítése és az információk terjesztésének optimalizálása

A hatékonyság növelése érdekében a Bizottság az ENISA-val együttműködve értékelje a helyzetismerethez szükséges információk közös megszerzésének és elemzésének megvalósíthatóságát. Emellett ezeket az információkat és a kiberfenyegetésekről szóló kapcsolódó jelentéseket tegye elérhetővé az Unió érintett szervezeti egységei és ügynökségei számára.

Megvalósítás céldátuma: 2027

- 12** A **kiberszolidaritásról szóló 2024. évi jogszabály** létrehozza az uniós kiberbiztonsági tartalékot, amelynek célja, hogy támogassa a tagállamokat a jelentős kiberbiztonsági incidensekre való reagálásban és az azokat követő helyreállításban. Az egyes tagállamok kiválasztott szolgáltatóiból áll, akik éjjel-nappal reagálni tudnak az eseményekre. Noha ez a megközelítés elősegíti a tagállamokban a sajátos követelmények teljesítését és a bizalom kiépítését, a rendelkezésre álló költségvetés egyenlően oszlik meg a tagállamok között, és nem veszi figyelembe az egyes tagállamok sajátos igényeit (52–57. bekezdés).

- 13** Meglátásunk szerint az előzetesen szerződött szolgáltatók igénybevétele lehetővé teszi az incidensreagálási szolgáltatások gyors nyújtását. Az uniós kiberbiztonsági tartalék elsődleges célja a reagálás és a helyreállítás támogatása, de amennyiben azt éppen nem biztonsági incidensekre való reagálásra használják fel, akkor a felkészültség javítására is bevethető. Ez a rugalmas megközelítés elejét veheti annak, hogy az előre fizetett szolgáltatások kihasználatlanul maradjanak. Így azonban fennáll a kockázat, hogy a tartalékot – ellentétben annak rendeltetésével – elsősorban felkészültségre, nem pedig reagálásra használják fel (58–61. bekezdés).
- 14** Az európai kiberbiztonsági figyelmeztető rendszer nemzeti és határokon átnyúló kiberközpontok hálózata, amelynek célja a kiberfenyegetések észlelésének, elemzésének és az azokra való reagálásnak a javítása. Megállapítottuk, hogy ellenőrzésünk idején az eszközök és szolgáltatások beszerzésének jelentős késedelve miatt sem a két központ (ATHENA és ENSOC), sem az európai kiberbiztonsági figyelmeztető rendszer nem működött (62–70. bekezdés).
- 15** Az európai kiberbiztonsági figyelmeztető rendszer egyik fő célkitűzése a tagállami klaszterek közötti érdemi információmegosztás ösztönzése. Bár ez megoldhat egyes, az információmegosztással kapcsolatos problémákat, nagy kihívást jelent a kiberközpontoknak a már amúgy is összetett kiberbiztonsági környezetbe való integrálása. Megállapítottuk, hogy az európai kiberbiztonsági figyelmeztető rendszer teljes körű működéséhez szükséges együttműködési megállapodások, közös taxonómia és interoperabilitási szabványok még nincsenek érvényben (71–74. bekezdés).



3. ajánlás

Az európai kiberbiztonsági figyelmeztető rendszer integrálása az uniós kiberbiztonsági környezetbe

A Bizottság az ENISA-val és a tagállamokkal együtt biztosítsa az európai kiberbiztonsági figyelmeztető rendszer, a CSIRT-hálózat és az EU-CyCLONe részét képező, határokon átnyúló központok közötti információmegosztást elősegítő együttműködési megállapodások és interoperabilitási szabványok meglétét.

Megvalósítás céldátuma: 2028

- 16** 2018-ban a Bizottság javaslatot tett az Európai Kiberbiztonsági Kompetenciaközpont (ECCC) létrehozására, amelynek a terv szerint 2021-től kellett kezelnie a DIGITAL program kiberbiztonsági komponensét. Az [ECCC-rendelet](#) egy – az ipar, a tudományos és kutatási szervezetek képviselőiből álló – kiberbiztonsági kompetenciaközösség létrehozását szorgalmazta. A kiberbiztonsági kompetenciaközösség egyes kiválasztott tagjai ezt követően stratégiai tanácsadó csoportot (SAG) alkotnának ([75–76. bekezdés](#)).
- 17** Megállapítottuk, hogy az ECCC pénzügyileg önállóvá válása, illetve a kiberbiztonsági kompetenciaközösség és a stratégiai tanácsadó csoport létrehozása késedelmes volt, és emiatt a két utóbbi nem tudott részt venni a DIGITAL programon belül a munkaprogramok kialakításában. Megítélésünk szerint ezzel elszalasztottak egy lehetőséget ([77–81. bekezdés](#)).
- 18** Megállapítottuk, hogy az általunk megvizsgált projektek mindegyike olyan releváns célkitűzések elérésére törekedett, amelyek elősegítik a DIGITAL program kiberbiztonsági célkitűzéseinek megvalósulását. Találtunk azonban olyan eseteket is, ahol a minőség vagy az elért eredmények nem voltak kielégítőek, elsősorban a végrehajtás késedelmei miatt ([82–87. bekezdés](#)).
- 19** A [Digitális Európa programról szóló rendelet](#) értelmében a kiberbiztonság finanszírozása biztonsági okokból a tagállamokban letelepedett és a tagállamok vagy azok állampolgárai által ellenőrzött szervezetekre korlátozható. Ehhez a tulajdonosi szerkezetre és az ellenőrzésre vonatkozó értékelést az ECCC nevében az [Európai Kutatási Végrehajtó Ügynökség](#) Központi Jóváhagyó Szolgálatá végzi el ([88–91. bekezdés](#)).
- 20** Harmadik feleknek nyújtott pénzügyi támogatás esetében a tulajdonosi szerkezetre és az ellenőrzésre vonatkozó értékelés a projekt kedvezményezettjeinek felelőssége, saját megközelítésük és módszertanuk alapján. Megállapítottuk, hogy az ECCC nem validálja módszertanát, és nem végez ellenőrzést annak biztosítására, hogy a kiválasztott harmadik felek uniós tulajdonban és uniós ellenőrzés alatt legyenek. Véleményünk szerint jelentős a kockázata annak, hogy a kedvezményezettek nem képesek megfelelően elvégezni ezeket az ellenőrzéseket. Ezt a kockázatot nem enyhítették megfelelően, ami érzékeny infrastruktúrák, működési adatok és biztonsági szempontból kritikus technológiák kitettségéhez vezethet ([92–96. bekezdés](#)).



4. ajánlás

Megbízható értékelés biztosítása a Digitális Európa program keretében uniós finanszírozásban részesülő szervezetek tulajdonosi szerkezetéről és ellenőrzéséről

Az Európai Kiberbiztonsági Kompetenciaközpont:

- a) szerezzen megalapozott bizonyosságot arról, hogy a harmadik feleknek nyújtott pénzügyi támogatásért felelős kedvezményezettek rendelkeznek-e a tulajdonosi szerkezetre és az ellenőrzésre vonatkozó értékelések megfelelő – az e kedvezményezettek rendelkezésére álló meglévő módszertanon alapuló – elvégzéséhez szükséges adminisztratív és technikai kapacitással;
- b) mintaalapú ellenőrzés keretében vizsgálja meg, hogy kizárólag a támogatható szervezetek részesültek-e uniós finanszírozásban.

Megvalósítás céldátuma: a) esetében 2026, b) esetében 2027

- 21** Az uniós finanszírozású projekteket irányító kedvezményezetteknek mérföldkövek és elérendő eredmények révén be kell számolniuk az ECCC-nek az elért haladásukról és az eredményeikről. Ezek döntő fontosságúak a projektek nyomon követése szempontjából, ezért megfelelően meg kell őket határozni. Megállapítottuk, hogy a mintánkban szereplő projektek közül szinte egyik sem követte a mérföldkövek és az elérendő eredmények meghatározására vonatkozó utasításokat, így ezek közül sok nem volt használható az előrehaladás nyomon követéséhez (97–99. bekezdés).
- 22** Megállapítottuk továbbá, hogy a kedvezményezettek által használt teljesítménymutatók jó része nem releváns vagy nem mérhető, illetve nem tartalmaz célértéket vagy alapértéket. Ezenkívül az ezekre a mutatókra vonatkozó adatszolgáltatás nem volt megfelelő, ezért nem szolgálhat a projektteljesítmény értékelésének alapjául (100–102. bekezdés).
- 23** A DIGITAL program egésze által elért eredmények nyomon követése érdekében minden projektnek be kell számolnia azokról a konkrét programmutatókról, amelyek alapul szolgálnak a Bizottság éves [programteljesítmény-kimutatásaihoz](#). Az e mutatókhoz tartozó adatok összegyűjtéséért és ellenőrzéséért az ECCC felelős. Több problémát tártunk fel az adatgyűjtés módjával és általános minőségével kapcsolatban. Nem találtunk bizonyítékot arra, hogy az ECCC ellenőrizte volna a bejelentett adatok pontosságát. Szűrőpróbaszerű ellenőrzéseink alapján úgy véljük, hogy a bejelentett adatok nem tükrözik pontosan az elért eredményeket (103–106. bekezdés).



5. ajánlás

A Digitális Európa programon belül a kiberbiztonsági komponens teljesítménymonitoring-keretének megerősítése

Az előrehaladás és a teljesítmény megfelelő nyomon követésének lehetővé tétele érdekében az Európai Kiberbiztonsági Kompetenciaközpont:

- a) biztosítsa a támogatás aláírása előtt, hogy minden projekt olyan mérföldköveket, elérendő eredményeket és teljesítménymutatókat határozzon meg, amelyek megfelelnek a pályázati úrlapon megadott utasításoknak;
- b) alakítson ki és vezessen be megbízható rendszert a Digitális Európa program kiberbiztonsági komponensének teljesítménymutatóihoz szükséges adatok gyűjtésére, nyomonkövethetőségére, ellenőrzésére és összesítésére, és így biztosítsa, hogy a mutatók pontosan tükrözzék az elért eredményeket.

Megvalósítás céldátuma: 2027

Észrevételeinkről részletesebben

Az uniós kiberbiztonsági hálózatok és mechanizmusok támogatják az együttműködést és a reagálást, de az elégtelen információmegosztás és a hiányos végrehajtás csökkenti eredményességüket

Az uniós hálózatok lehetővé teszik a tagállamok közötti együttműködést, de az elégtelen információmegosztás csökkenti hozzáadott értéküket

- 24** A jelentős kiberbiztonsági incidensek észlelését és az azokra való reagálást megkönnyítő hálózatok és mechanizmusok jelenlegi uniós keretét fokozatosan alakították ki, és ennek első lépése a [hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelv](#)³ (NIS-irányelv) volt, amely 2016 augusztusában lépett hatályba. A jelenlegi uniós környezetet a [II. melléklet](#) szemlélteti.

³ Az (EU) 2016/1148 irányelv.

Az uniós hálózatok technikai és operatív szinten is lehetővé teszik a tagállamok együttműködését

- 25** A NIS-irányelv létrehozta a [CSIRT-hálózatot](#), amelynek része a [CERT-EU](#) (az uniós intézmények, szervek, hivatalok és ügynökségek kiberbiztonsági szolgálata) és a tagállamok által kijelölt, számítógép-biztonsági incidensekre reagáló csoportok (CSIRT). A hálózat célja a nemzeti csoportok közötti bizalomépítés, valamint a tagállamok közötti gyors és eredményes operatív együttműködés előmozdítása.
- 26** Az [EU-CyCLONe](#) 2020-ban jött létre a kiberválságok kezeléséért felelős nemzeti hatóságok informális együttműködési hálózataként. A hálózat hídként szolgál a CSIRT-hálózat működésének technikai rétege, valamint az Európai Unió Tanácsának politikai rétege és annak [politikai szintű integrált válságelhárítási](#) intézkedései között. Az EU-CyCLONe szerepét a NIS 2 irányelv 2023. évi hatálybalépése tette hivatalossá, amely egyértelmű megbízatást adott neki.
- 27** Megvizsgáltuk, hogy ezek az uniós szintű hálózatok jól meghatározott feladat- és felelősségi körökkel rendelkeznek-e, és hogy lehetővé teszik-e a tagállamok együttműködését.
- 28** Az [ENISA](#) a CSIRT-hálózat és az EU-CyCLONe titkárságaként működik, és biztosítja számukra az erőforrásokat, szakértelmet, infrastruktúrát és informatikai eszközöket az információmegosztáshoz szükséges együttműködéshez és biztonságos kommunikációhoz. Az érdekelt felek elégedettségéről szóló, 2025 elején végzett felmérésben⁴ az ENISA jó pontszámokat kapott e hálózatok titkárságaként nyújtott teljesítményéért. A pozitív visszajelzést helyszíni vizsgálataink is megerősítették, ezek alkalmával a nemzeti kiberbiztonsági hatóságok elismerésüket fejezték ki.

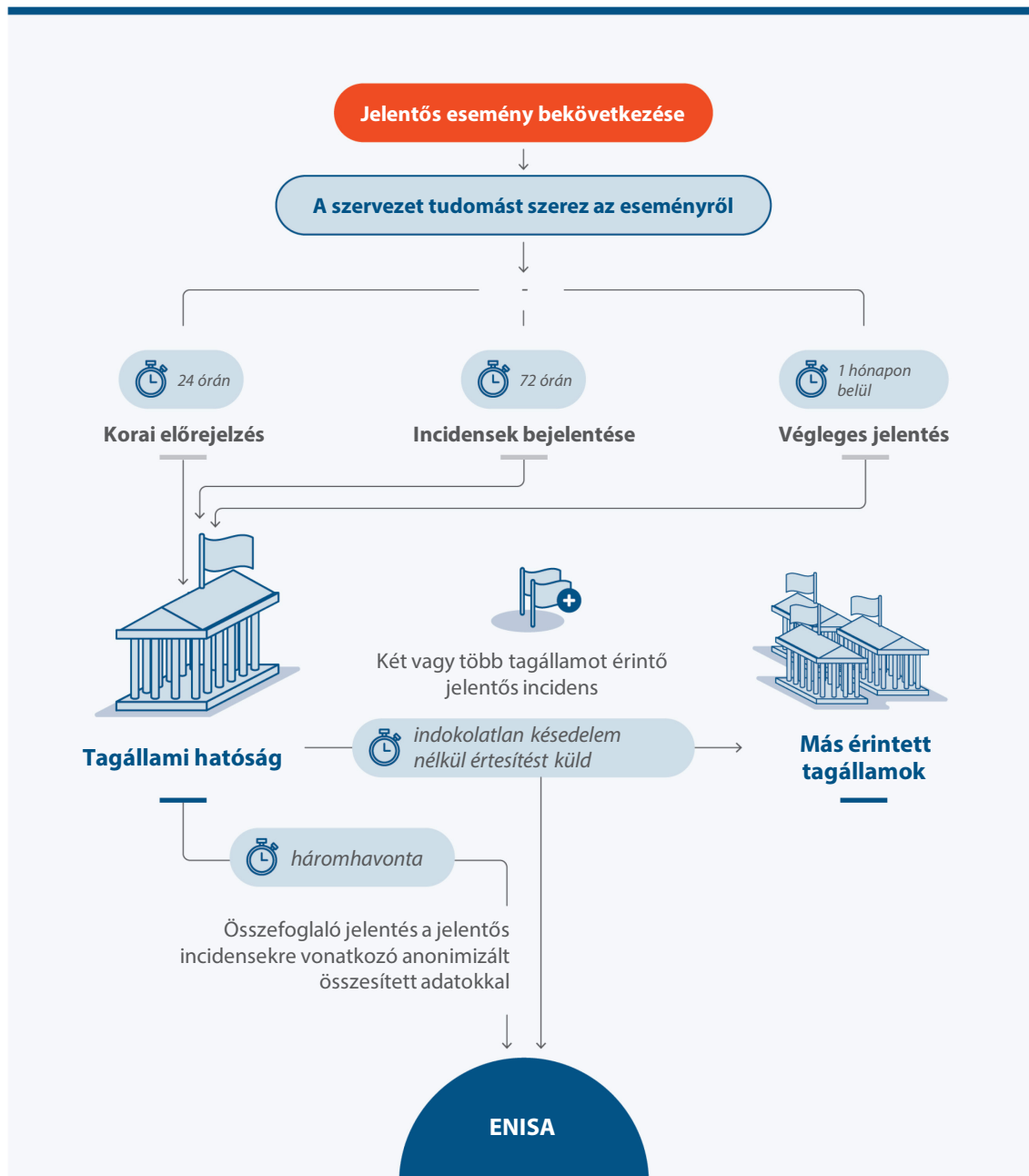
⁴ Az ENISA 2024. évi konszolidált éves tevékenységi jelentése, 33. és 36. o.

- 29** A Tanács 2025-ben fogadta el a [kiberbiztonsági tervet](#), amely meghatározza a nagyszabású kiberbiztonsági incidensekben, illetve kiberbiztonsági válsághelyzetekben részt vevő kulcsszereplők (többek között a CSIRT-hálózat és az EU-CyCLONe) feladat- és felelősségi köreit és az ezekben szerepet játszó mechanizmusokat. Megállapítottuk, hogy a kiberbiztonsági terv nagyrészt tisztázza az uniós kiberválság-kezeléssel kapcsolatos feladat- és felelősségi köröket, továbbá figyelembe veszi a 2017. évi első terv óta bekövetkezett változásokat. A terv az együttműködés három szintjét határozza meg: a technikai, az operatív és a politikai szintet. Emellett részletesen bemutatja a 2017 óta létrehozott új hálózatokat és struktúrákat – például az EU-CyCLONe-t, a hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatokat és az európai kiberbiztonsági figyelmeztető rendszert –, és arra is kitér, hogy a kiberválság-kezelést hogyan kell integrálni az Unió tágabb válságreakálási keretébe.
- 30** A CSIRT-hálózat 2016. évi és az EU-CyCLONe 2023. évi hivatalos létrehozása ellenére azonban a két hálózat mindaddig még nem tette hivatalossá az együttműködés módjára vonatkozó eljárási szabályokat. Arról sem állapodtak még meg, hogy a CSIRT-hálózatnak milyen kritériumok alapján kell tájékoztatnia az EU-CyCLONe-t arról, ha egy megfigyelt kiberbiztonsági esemény potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági incidensnek minősül. A két hálózatnak még meg kell állapodnia a biztonsági események súlyossági szintjeinek és az alapfogalmaknak (például: „fenyegetés”, „fenyegető szereplő”, „incidens” vagy „hatás”) a közös taxonómiájáról is, amely az automatizált információcsere lehetővé tételéhez szükséges. Jelenleg még eltérően értelmezhető, hogy egy esemény mikor minősül jelentősnek vagy nagyszabásúnak. A közös taxonómia hiányát mindhárom általunk felkeresett tagállam kiberbiztonsági hatóságai megemlítték.

Az elégtelen információmegosztás és a nem megfelelő beszámolás jelentősen csökkenti e hálózatok hozzáadott értékét

- 31** A földrajzi határok nem akadályozzák meg a kiberbiztonsági incidensek és kibertámadások bekövetkezését és terjedését. A tagállamok közötti, például a fenyegető szereplők által alkalmazott taktikákra és technikákra, valamint a hálózati vagy információs rendszerek megsértésére utaló digitális jelekre (a továbbiakban: „fertőzöttségi mutatók”) vonatkozó információmegosztás jelentősen növelheti a kiberbiztonságot.
- 32** Megállapítottuk, hogy az információmegosztás elégtelen volt, ami jelentősen csökkentette e hálózatok hozzáadott értékét. Ezzel kapcsolatban elsősorban a következőkből adódtak hiányosságok: a NIS 2 irányelv késedelmes átültetése, annak megállapítása, hogy egy esemény határokon átnyúló hatással jár-e, az információmegosztást korlátozó nemzetbiztonsági jogszabályok és a bizalom hiánya. A NIS 2 irányelv számos adatszolgáltatási követelményt vezet be a hatálya alá tartozó szervezetekre és a tagállami hatóságokra vonatkozóan (lásd: [2. ábra](#)).

2. ábra | Az incidensek bejelentésére vonatkozó időkeret az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelv (NIS 2 irányelv) értelmében



Forrás: Európai Számvevőszék, az ENISA tájékoztatása alapján.

- 33** A tagállamoknak 2024 októberéig kellett [átültetniük a NIS 2 irányelvet](#) a nemzeti jogba, de ezt a határidőt csak két tagállam tartotta be. A késedelmes átültetés jelentős hatással van az információmegosztásra, mivel a köztes időben a NIS 2 irányelv hatálya alá tartozó szervezetek jogilag nem kötelesek bejelenteni az incidenseket. A Bizottság becslése⁵ szerint a NIS-irányelv hatálya alá 15 500 szervezet, míg a NIS 2 irányelv hatálya alá több mint 110 000 szervezet tartozik. A közigazgatás területén például (az ENISA [fenyegetettségi helyzetéről szóló 2025. évi jelentése](#) szerint ez az Unió leginkább megcélzott ágazata) nem volt kötelező bejelenteni a NIS-irányelv szerinti incidenseket.
- 34** Az, hogy az ENISA felé háromhavonta (azaz jóval az esetleges incidens bekövetkezte után) kell jelenteni az incidensekre vonatkozó adatokat, csökkenti azok hozzáadott értékét. Ezek az adatok főként statisztikai célokra és a korábbi trendekkel kapcsolatos beszámolásra szolgálnak, nem pedig a felderítés és a reagálás javítására. Az ENISA [online eszközt](#) biztosít a tagállamok számára jelentéseik benyújtásához. Az adatszolgáltatási sablon tartalmazza a szolgáltatandó adatok minimális körét, például az incidens típusát és az érintett ágazatot. Emellett az ENISA azt javasolja, hogy a tagállamok nyújtsanak be további információkat az adatok mélyrehatóbb elemzésének (például az incidensek és konkrét sebezhetőségek összekapcsolásának) lehetővé tétele érdekében. Nem minden tagállam dönt azonban úgy, hogy ad ilyen információt, ami jelentősen csökkenti az összegyűjtött adatok minőségét és hozzáadott értékét.
- 35** Az ENISA az [Európai Unió kiberbiztonsági helyzetéről szóló 2024. évi jelentésében](#) kijelentette, hogy az incidensekről valószínűleg nem mindig számolnak be, mivel a bejelentett események száma alacsonynak tűnik. 2018 és 2021 között a tagállamok évente 100–500 eseményt jelentettek az ENISA-nak. Ez a szám fokozatosan nőtt, és 2024-ben elérte az 1276-ot⁶.

⁵ Európai Bizottság, 2020. évi [hatásvizsgálati jelentés](#).

⁶ A [CIRAS](#) 2024. évi adatai.

- 36** A [fenyegetettségi helyzetről szóló 2025. évi jelentésében](#), amely a 2024 júniusa és 2025 júniusa közötti időszakra terjedt ki, az ENISA mintegy 4800 kiberbiztonsági incidenst⁷ tárt fel nyílt forrásból származó értékelt felderítési információ, például újságcikkek révén. Ezen incidensek közül nem mindegyik lett volna bejelentendő a NIS 2 irányelv alapján, mivel az adatgyűjtés során az ENISA az incidensek szélesebb körét fedi le. Ezzel szemben számos jelentős incidensről nem számolnak be nyílt felderítési források. Mivel a tagállamok által bejelentett adatok anonimizáltak, az ENISA nem tudja összekapcsolni az általa megállapított incidenseket a tagállamok által bejelentettekkel. Ezért nem lehet pontosan meghatározni a be nem jelentett incidensek mértékét, de véleményünk szerint a tagállamok által bejelentett, illetve a fenyegetettségi helyzetről szóló jelentésben szereplő incidensek száma közötti különbség azt mutatja, hogy nem minden jelentős incidenst jelentenek be.
- 37** A valósnál alacsonyabb bejelentési arányra utal a más érintett tagállamoknak és az ENISA-nak küldött, jelentős, határokon átnyúló incidensekre vonatkozó bejelentések száma is. Hasonló követelmény már a NIS-irányelvben is létezett, de az eredménytelennek bizonyult, mivel a Bizottság 2020-ban megállapította⁸, hogy az előírás ellenére ritkán küldtek értesítéseket. A bejelentés elmulasztását arra vezette vissza, hogy nem voltak egyértelmű szabályok az információmegosztásra vonatkozóan, illetve az információmegosztást nem ösztönözték közös célkitűzések.
- 38** A többi tagállam tájékoztatására vonatkozó kötelezettség döntő fontosságú a biztonsági események továbbgyűjtésének megelőzése szempontjából; ennek elmulasztása negatívan befolyásolja az Unió kiberbiztonságát. 2025-ben összesen hét tagállam mindössze 14 jelentős, határokon átnyúló eseményt jelentett be. A tagállamok 2024-ben kettő, 2023-ban nulla, 2022-ben pedig három olyan incidensről nyújtottak be jelentést, amelyek határokon átnyúló hatással járhatnak. Ez azt mutatja, hogy igen kevés jelentős, határokon átnyúló biztonsági eseményről születik jelentés, ami nem tükrözi az ilyen támadások valódi mértékét. Ezt szem előtt tartva az ENISA a [fenyegetettségi helyzetről szóló 2024. évi jelentésében](#) 322 olyan incidenst mutatott be, amelyek kifejezetten két vagy több tagállamot céloztak meg. A Collins Aerospace-t érintő incidens (lásd: [1. háttérmagyarázat](#)) jó példa arra, hogy a tagállamok annak ellenére nem jelentenek be egy incidenst, hogy az jelentős határokon átnyúló hatással jár.

⁷ Az ENISA [fenyegetettségi helyzetről szóló 2025. évi jelentése](#).

⁸ Európai Bizottság, 2020. évi [hatásvizsgálati jelentés](#).

1. háttérmagyarázat

A repülőtéri műveleteket megzavaró kiberbiztonsági incidens

2025 szeptemberében a Collins Aerospace-t, a légi közlekedési ágazat egyik jelentős technológiai szolgáltatóját jelentős zsarolóvírus-támadás érte, amely az utasellenőrzési szoftvert célozta meg. A támadás miatt több nagy európai repülőtér kénytelen volt manuálisan biztosítani a működést, ami széles körben okozott járatkéséseket és járat törléseket. A fennakadás London Heathrow, Brüsszel, Berlin Brandenburg és Dublin repülőterén volt a legsúlyosabb.

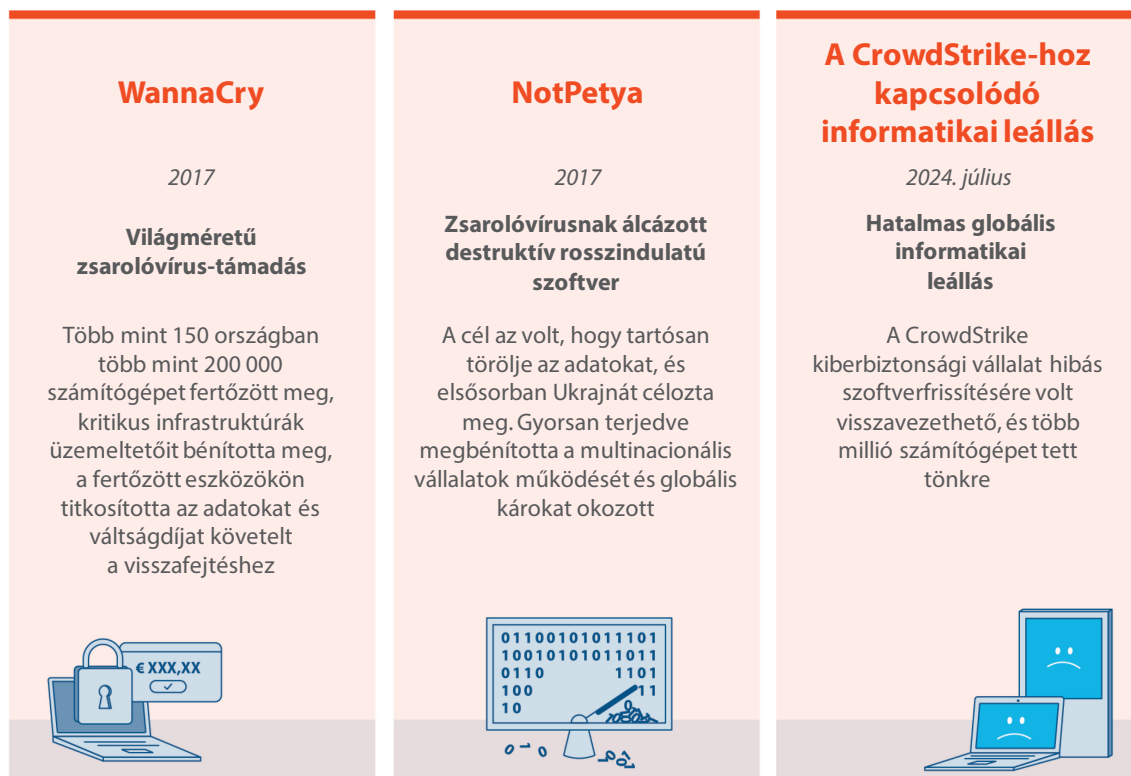
A NIS 2 irányelv szerint egy incidens többek között akkor minősül „jelentősnek”, ha súlyos működési zavart okoz a szolgáltatásokban, vagy pénzügyi veszteséggel jár az érintett szervezet számára. Ezt az incidenst azonban egyetlen tagállam sem kezelte jelentős vagy nagyszabású, határokon átnyúló eseményként. Ezért az érintett tagállamok egyike sem értesítette hivatalosan az ENISA-t, illetve más tagállamokat az eseményről. A CSIRT-hálózat nem nyújtott tanácsadást az EU-CyCLONe-nak, amely ezért nem biztosított támogatást az incidens összehangolt kezeléséhez.

Forrás: Az Európai Számvevőszék elemzése az ENISA munkatársaival készített interjúk alapján.

39 Egy másik ok, ami miatt a határokon átnyúló incidensek közül nem mindegyiket jelentik be, az, hogy az egyes tagállami hatóságoknak kell meghatározniuk, hogy a bejelentett incidensnek van-e határokon átnyúló hatása, illetve hogy melyek a további érintett tagállamok. A rendelkezésükre álló információk alapján előfordulhat, hogy az adatszolgáltató szervezetnek vagy a tagállami hatóságnak nincs tudomása egyes támadások határokon átnyúló jellegéről. Jelenleg nincs olyan uniós szintű platform, amelyre az incidensekről valós idejű jelentések érkeznének be valamennyi tagállamtól, és amely a határokon átnyúló incidensek felderítése érdekében összekapcsolhatná az ágazatokra, illetve a fertőzőtségi mutatókra vonatkozó információkat. Emiatt nagy a kockázata annak, hogy egyes határokon átnyúló incidenseket nem azonosítanak ilyenként és azokról nem számolnak be.

40 2016 óta egyetlen tagállam sem tekintett egyetlen kiberbiztonsági incidenst sem „nagyszabásúnak”. Elvben minden olyan incidens e fogalommeghatározás hatálya alá tartozik, amely legalább két tagállamot érint jelentős mértékben. Ennek ellenére még az olyan globális üzemszüneteket és jelentős károkat okozó kiberbiztonsági incidenseket sem tekintették nagyszabásúnak, mint amelyet a **3. ábra** mutat be. Ennek eredményeként az EU-CyCLONe eskalációs eljárását nagyszabású kiberbiztonsági incidens miatt soha nem aktiválták teljes mértékben.

3. ábra | Jelentős kiberbiztonsági incidensek (példák)



Forrás: Európai Számvevőszék, a Cloudflare, az ENISA, az Europol, a Wired, az IBM és a CrowdStrike adatai alapján.

- 41** Az információmegosztás megkönnyítése érdekében a szervezetekre és a tagállamokra rótt adatszolgáltatási kötelezettség mellett létrehozták a CSIRT-hálózatot is. A CSIRT-hálózat központi eleme a tagállamok közötti bizalom, ahol az információk megosztása önkéntes alapon történik. A hálózat hozzáadott értéke jelentősen csökken, ha a tagállamok nem hajlandók időszerű és hasznosítható információkat megosztani.
- 42** Az uniós szintű információmegosztásnak az egyes tagállamok nemzetbiztonsági jogszabályai szabnak korlátot. Ha egy tagállam úgy ítéli meg, hogy egy kritikus fontosságú szervezetre mért kibertámadással kapcsolatos információk minősítettek, illetve hogy egy adott incidens bejelentése nemzetbiztonsági szempontból hátrányt jelentene számára, nem köteles megosztani az információkat. A tagállamokban tett látogatásaink során a CSIRT-hálózat és az EU-CyCLONe képviselői kijelentették, hogy az információk megosztására csak a nemzetbiztonsági jogszabályok keretein belül kerülhet sor. Uniós szinten nem végeztek elemzést a tagállamok nemzeti jogi kereteinek és e keretek információmegosztásra gyakorolt hatásáról.

- 43** 2016-ban a CSIRT-hálózat 28 nemzeti CSIRT-ből állt, tagállamonként két képviselővel. Az információmegosztás hiánya állandó probléma. Amint a NIS-irányelv [Bizottság általi értékelése](#) is szóvá tette, a tagállamok nem osztják meg rendszeresen az információkat egymással, ami nagymértékben befolyásolja a kiberbiztonsági intézkedések eredményességét és az uniós szintű közös helyzetismeret szintjét. A NIS 2 irányelv alapján számos tagállam a számítógép-biztonsági incidensekre reagáló nemzeti csoportja (CSIRT) mellett ágazati csoportokat is kijelölt, aminek köszönhetően a hálózat jelentősen kibővült, ellenőrzésünk idején már 42 CSIRT-ből és több mint 700 egyéni résztvevőből állt. Ez még inkább megnehezíti a bizalomépítést, mivel nehéz szoros kapcsolatokat fenntartani az összes tag között.
- 44** A CSIRT-hálózat tud az információmegosztással kapcsolatos problémáról, és jelenleg mérlegeli, hogy milyen intézkedésekkel lehetne növelni a bővülő hálózatba vetett bizalmat. A tagállamok határokon átnyúló csomópontokat alkotó kisebb klasztereinek létrehozása (részletesen lásd: [62–74.](#) bekezdés) lehetne például egy olyan alternatív megközelítés az egész Unióra kiterjedő hálózatra nézve, amely megoldást jelenthet erre a nehézségre.

A kiberbiztonsági helyzetelemző központ szerződéses szolgáltatásai részben átfedésben vannak a már meglévő kapacitásokkal, és a központ jövőbeli működése nem egyértelmű

- 45** A NIS 2 irányelv értelmében azokban az esetekben, amikor egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági esemény jelentős hatással jár vagy valószínűleg jelentős hatással fog járni, a Bizottság az EU-CyCLONe tagjaként jár el⁹. Ez az új szerep és a fenyegetettségi helyzet alakulása arra készítette a Bizottságot, hogy 2022-ben a Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatóságán belül kiberkoordinációs munkacsoportot hozzon létre. Ez a munkacsoport magában foglal egy kiberbiztonsági helyzetelemző központot, amelynek segítenie kell a Bizottságot abban, hogy válságkezelési intézményi feladatainak jobb elvégzéséhez növelje helyzetismeretét, emellett pedig támogatnia kell a Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatóságát is a politikai szintű tanácsadásban.

⁹ A NIS 2 irányelv 16. cikkének (2) bekezdése.

- 46** A kiberbiztonsági helyzetelemző központ létrehozásában a Bizottságot nagyban támogatják külső szolgáltatók is, akik 2022 decemberében négy évre közel 18 millió euróra [kötöttek szerződést](#). Megvizsgáltuk a központ létrehozását, tevékenységének eddigi eredményeit és a jövőbeli működésére vonatkozó bizottsági terveket.
- 47** A nyújtott szolgáltatások részeként a vállalkozók a fenyegetésekre vonatkozó információk megjelenítése és megosztása érdekében létrehoztak egy a kiberfenyegetésekkel kapcsolatos kereskedelmi hírcsatornákon alapuló irányítópultot. Emellett különböző kiberfenyegetésekkel kapcsolatos hírszerzési jelentéseket is készítenek, köztük napi és heti jelentéseket, valamint az országokról, illetve a gazdasági ágazatokról szóló tematikus jelentéseket. A fizikai kiberbiztonsági helyzetelemző központot, amely a vállalkozók által üzemeltetett irányítópulthoz távolról csatlakoztatott munkaállomásokkal felszerelt helyiségből áll, a Bizottság egyik épületében hozták létre. Ellenőrzésünk idején a kiberbiztonsági helyzetelemző központ kisszámú bizottsági alkalmazottból állt, akiknek a munkáját a szerződéses partnerek számos elemzője, valamint az ENISA szakértői támogattak.
- 48** Megállapítottuk, hogy a külső szolgáltatók által a központ részére végzett munka részben átfedésben van az ENISA már meglévő kapacitásával. Az ENISA állandó kapacitással rendelkezik a helyzetismeret céljára és a fenyegetések nyomon követésére. Rendszeresen tesz közzé kiberfenyegetésekről szóló jelentéseket, ezek lehetnek konkrét eseményekről szóló gyorsjelentések, vagy a fenyegetéseket áttekintően bemutató heti jelentések. A jelentések nyílt forrásból származó értékelte felderítési információkon alapulnak, és hasonlóak a vállalkozók által készített jelentésekhez. Emellett az ENISA magas szintű tájékoztatókat készít a szakpolitikai döntéshozók számára válságok idején, illetve rész vesz ilyenek készítésében. Ezek a tájékoztatók összevethetők a kiberbiztonsági helyzetelemző központ által előállított információkkal is.
- 49** A kiberbiztonsági helyzetelemző központ által e jelentések elkészítéséhez felhasznált adatok a kiberfenyegetésekkel kapcsolatos kereskedelmi hírcsatornákon alapulnak, és hasonlóak a Bizottság más szervezeti egységei, például a Digitális Szolgáltatások Főigazgatósága és a CERT-EU által felhasznált adatokhoz. Meglátásunk szerint a kiberbiztonsági helyzetelemző központot anélkül hozták létre, hogy a Bizottság és az ENISA által már rendelkezésre bocsátott információkat felhasználva kellőképpen kihasználták volna a racionalizálásban rejlő lehetőségeket.

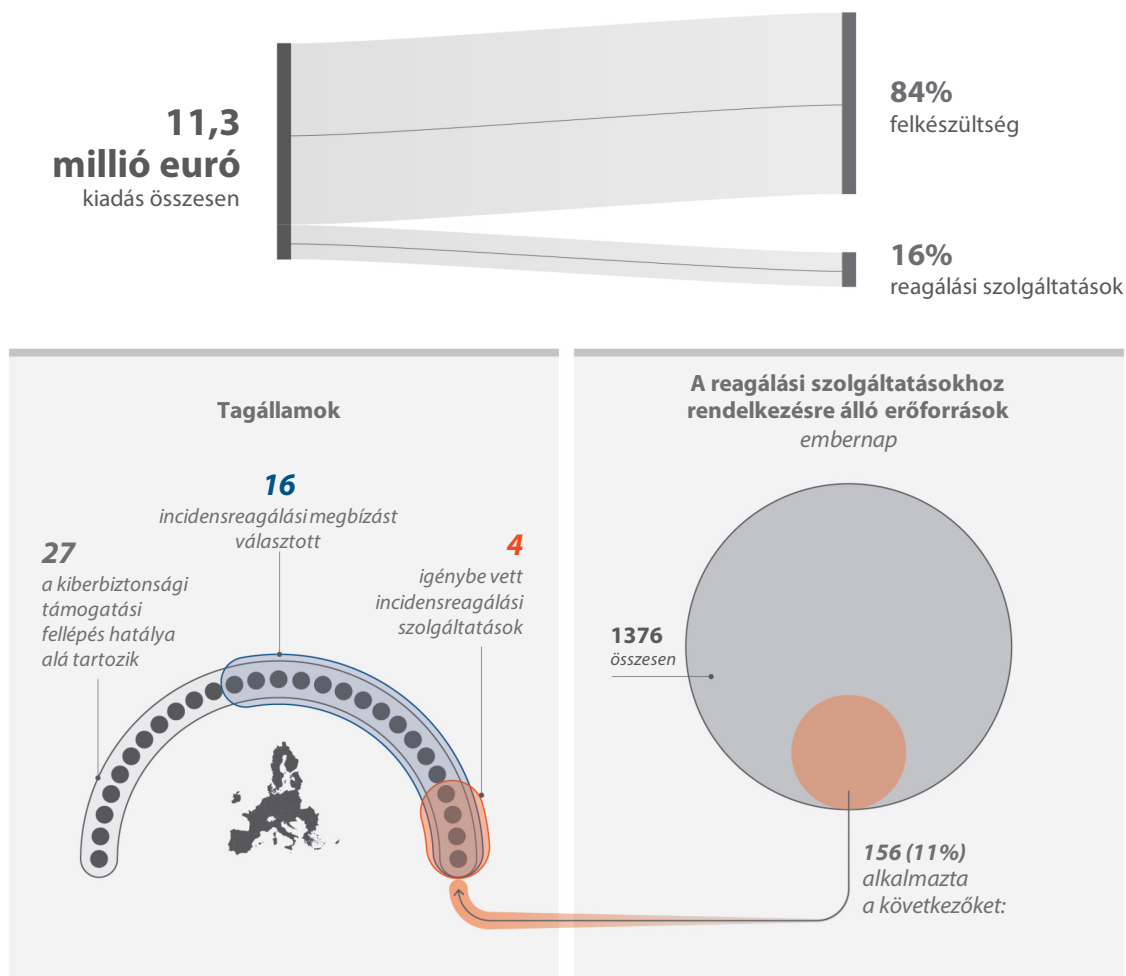
- 50** A szerződés 2026 decemberében jár le, ezt követően a vállalkozók nem nyújtanak szolgáltatásokat a kiberbiztonsági helyzetelemző központ számára. Ezek a szolgáltatások többek között az irányítópult adatainak rendelkezésre bocsátása és a fenyegetettségi jelentések készítése, és ezek teszik ki a központ tevékenységeinek legnagyobb részét. Az irányítópult átkerül a Bizottsághoz, de ha nem frissítik folyamatosan a kiberfenyegetésekkel kapcsolatos hírszerzés alapján, akkor el fogja veszíteni hozzáadott értékét.
- 51** Ellenőrzésünk időpontjáig a Bizottság nem dolgozott ki tervet arra nézve, hogy a külső szolgáltatók által nyújtott támogatása terén miként folytatódjon a kiberbiztonsági helyzetelemző központ működése a szerződés lejáta után. Meglátásunk szerint az, hogy nincs átfogó, részletes terv a szerződés lejáta utáni időszakra vonatkozóan, kockázatot jelent a kiberbiztonsági helyzetelemző központ 2026 utáni működése szempontjából.

Az uniós kiberbiztonsági tartalék az incidensekre való reagáláskor gyors szolgáltatásnyújtást tesz lehetővé

- 52** Felismerve, hogy a nagyszabású kibertámadások egyre elterjedtebbé válnak, a Bizottság 2022-ben, közvetlenül Oroszország Ukrajna elleni katonai agressziója kezdetét követően, 15 millió eurós rendkívüli finanszírozást biztosított az ENISA-nak az egy évvel később, 2023-ban elindított [kiberbiztonsági támogatási fellépés](#) kísérleti szakaszához. 2023-ban a Bizottság további finanszírozást (körülbelül 20 millió eurót) nyújtott a program 2026 végéig történő meghosszabbításához.
- 53** A Bizottság emellett javaslatot tett a [kiberszolidaritásról szóló jogszabályra](#), amelyet 2024 decemberében fogadtak el, felkészülésképpen a későbbi nagyszabású kiberbiztonsági eseményekre. A jogszabály létrehozza az uniós kiberbiztonsági tartalékot, amely incidensekre való reagálási szolgáltatásokat nyújt megbízható szolgáltatók igénybevételével. A tartalék 2025-ben fokozatosan kezdte meg működését, a 2025–2027-es időszakra 36 millió eurós költségvetéssel.
- 54** Megvizsgáltuk, hogyan szervezték meg a kiberbiztonsági támogatási fellépési programot, amely az uniós kiberbiztonsági tartalék alapját képezi. Azt is ellenőriztük, hogy a 2022 óta levont tanulságokat felhasználták-e az uniós kiberbiztonsági tartalék kialakításakor.

- 55** Az ENISA a kiberbiztonsági támogatási fellépést olyan mechanizmusként dolgozta ki, amely a nagyszabású kiberbiztonsági incidensek, illetve válsághelyzetek kapcsán támogató szolgáltatásokat nyújt a tagállami felkészültséghez és reagáláshoz. Az ENISA minden szolgáltatásra előzetesen köt szerződést, így a szolgáltatók azonnal megkezdhetik a munkát, amint a tagállamok erre kérik őket. Ez az ENISA felépítésének is köszönhető, ugyanis az ügynökség biztosítja, hogy a hét minden napján, napi 24 órában rendelkezésre álljon egy olyan tisztviselő, aki a tagállamok kéréseivel foglalkozik.
- 56** Az ENISA úgy döntött, hogy a rendelkezésre álló költségvetést egyenlően osztja el a tagállamok között. A gyakorlatban ez úgy történt, hogy az ügynökség nyílt közbeszerzési eljárást indított 27 (tagállamonként egy) részre osztva, amelynek révén 2026 végéig legfeljebb három magán biztonságszolgáltatót tervezett kiválasztani a szolgáltatások nyújtására. Emellett az ENISA egy páneurópai tétel keretében is kiválasztott néhány szolgáltatót, hogy egyrészt támogatható nem uniós országoknak, másrészt uniós intézményeknek, szervezeteknek és ügynökségeknek is nyújtson szolgáltatásokat, illetve támogassa a határokon átnyúló incidensekre való reagálást.
- 57** Ez a megközelítés lehetővé tette az ENISA számára, hogy figyelembe vegye a sajátos nemzeti követelményeket, így a nyelvismeretet, a nemzeti biztonsági tanúsítványokat vagy a tagállamokban való állandó jelenlétet. Másrészt, mivel a szolgáltatókat nem úgy választották ki, hogy az egész Unióban képesek legyenek szolgáltatásokat nyújtani, e megközelítés egyik fő hátránya az, hogy ha egy tagállam nem veszi igénybe az előzetesen szerződésbe vett szolgáltatásokat, az adott tagállamban ilyen szolgáltatásokra lekötött költségvetés nem használható fel egy másik tagállam támogatására.
- 58** A kiberbiztonsági támogatási fellépés esetében a tagállamok választhattak a felkészültségi vagy reagálási szolgáltatások, illetve a kettő kombinációja között. A tagállamok leginkább úgy döntöttek, hogy a rendelkezésre álló finanszírozást (a 2023. évi kiadások 84%-át) felkészültségük javítására használják fel. Azok a tagállamok, amelyek incidensreagálási megbízás alkalmazása mellett döntöttek (ez egy szolgáltatóval előre megkötött megállapodás, amely biztosítja a tagállam számára, hogy a kiberbiztonsági incidensekre való gyors reagálás érdekében kérésre hozzáférjen a szolgáltató által nyújtott szolgáltatásokhoz), azt ritkán vették igénybe (lásd: [4. ábra](#)). A három általunk felkeresett tagállamban a hatóságok szerint elismerést érdemelt az, ahogyan az ENISA a kiberbiztonsági támogatási fellépést irányította.

4. ábra | Az ENISA kiberbiztonsági támogatási fellépései 2023-ig



Forrás: Európai Számvevőszék, a ENISA adatai alapján.

- 59** A 2024–2026-os időszakra vonatkozóan mindössze kilenc tagállam igényelt incidensreagálási megbízást. Az ENISA-val és három tagállam hatóságaival készített interjúink szintén alátámasztották, hogy határozottan a felkészültségi tevékenységeket részesítik előnyben.
- 60** Bár az uniós kiberbiztonsági tartalék elsődleges célja a jelentős kiberbiztonsági incidensekkel kapcsolatos reagálás és helyreállítás támogatása, az uniós kiberbiztonsági tartalékból előzetesen lekötött, incidensekre való reagálásra fel nem használt szolgáltatások felkészültségi szolgáltatásokká is átalakíthatók. Ez a rugalmas megközelítés elejét veheti annak, hogy az előre fizetett szolgáltatások kihasználatlanul maradjanak.

- 61** Úgy látjuk, hogy az uniós kiberbiztonsági tartalékhoz választott modellhez a kiberbiztonsági támogatási fellépési program tanulságait vették alapul. A kiberbiztonsági támogatási fellépési program felhasználására vonatkozó adatok azonban rámutatnak annak kockázatára, hogy az uniós kiberbiztonsági tartalékot elsősorban felkészültségre, nem pedig reagálásra használják fel, ez pedig ellentétes a kiberbiztonsági szolidaritásról szóló jogszabályban meghatározott céllal.

Az európai kiberbiztonsági figyelmeztető rendszer célja a fenyegetések észlelését lehetővé tevő kapacitások javítása, de a rendszer nem működik

- 62** Az európai kiberbiztonsági figyelmeztető rendszer egyik fő célkitűzése az érdemi információmegosztás ösztönzése, és ezáltal a kiberfenyegetések észlelésének, elemzésének és az azokra való reagálásnak a javítása. A figyelmeztető rendszerben való részvétel önkéntes, de azoknak a tagállamoknak, amelyek úgy döntenek, hogy csatlakoznak egy határokon átnyúló kiberközponthoz, kötelezettséget kell vállalniuk arra, hogy a releváns információkat a többi taggal is megosztják. A klaszterekben, megbízható és biztonságos környezetben folytatott együttműködés révén a tagállamok elkerülhetnek néhány információmegosztással kapcsolatos problémát (lásd: [31–44.](#) bekezdés).
- 63** Ellenőrzésünk idejéig 13 tagállam döntött úgy, hogy részt vesz az európai kiberbiztonsági figyelmeztető rendszerben, és ezek a tagállamok két határokon átnyúló központot hoztak létre (ATHENA és ENSOC). Egy harmadik, határokon átnyúló kiberközpont, az NBCC 2026-ban kapott finanszírozást a létrehozásra, így a hálózat tagjainak száma összesen 20 országra nőtt (18 uniós tagállam, valamint Izland és Norvégia¹⁰) (lásd: [5. ábra](#)).

¹⁰ Az (EU) 2021/694 rendelet 10. cikke (1) bekezdésének a) pontja szerinti társult nem uniós országok.

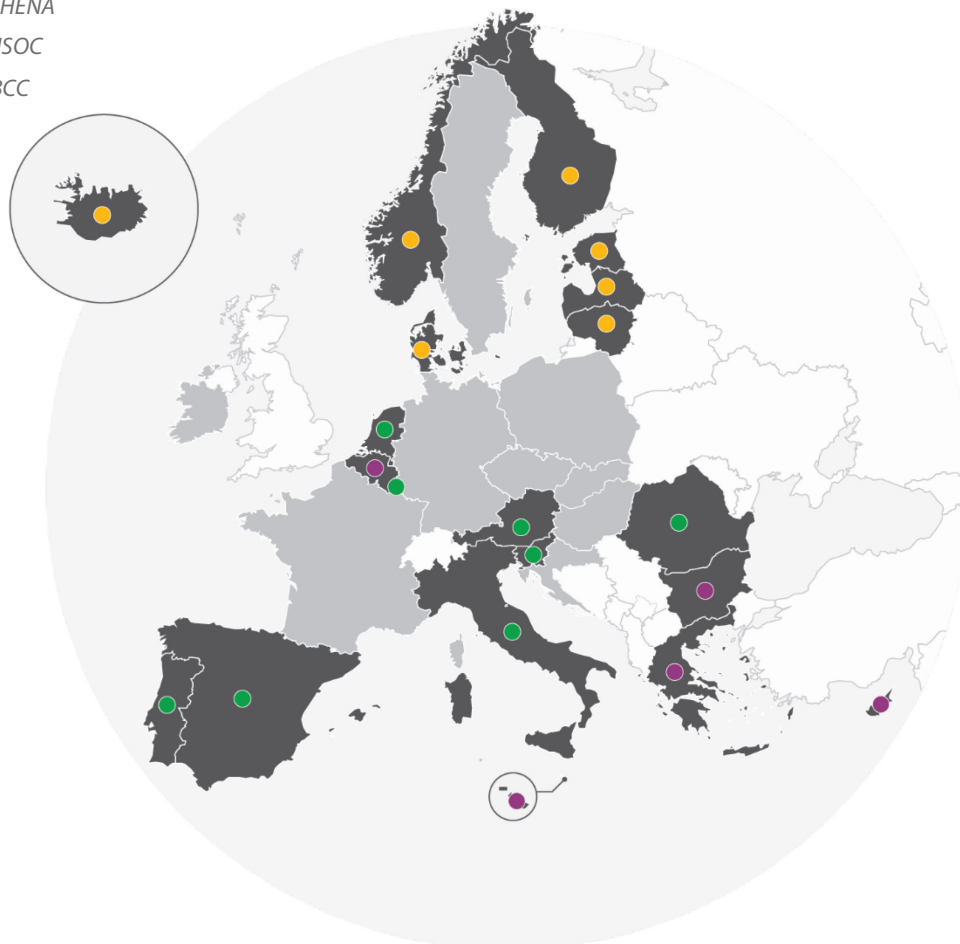
5. ábra | Az európai kiberbiztonsági figyelmeztető rendszerben részt vevő országok

■ Az európai kiberbiztonsági figyelmeztető rendszerben részt vevő országok

● ATHENA

● ENSOC

● NBCC



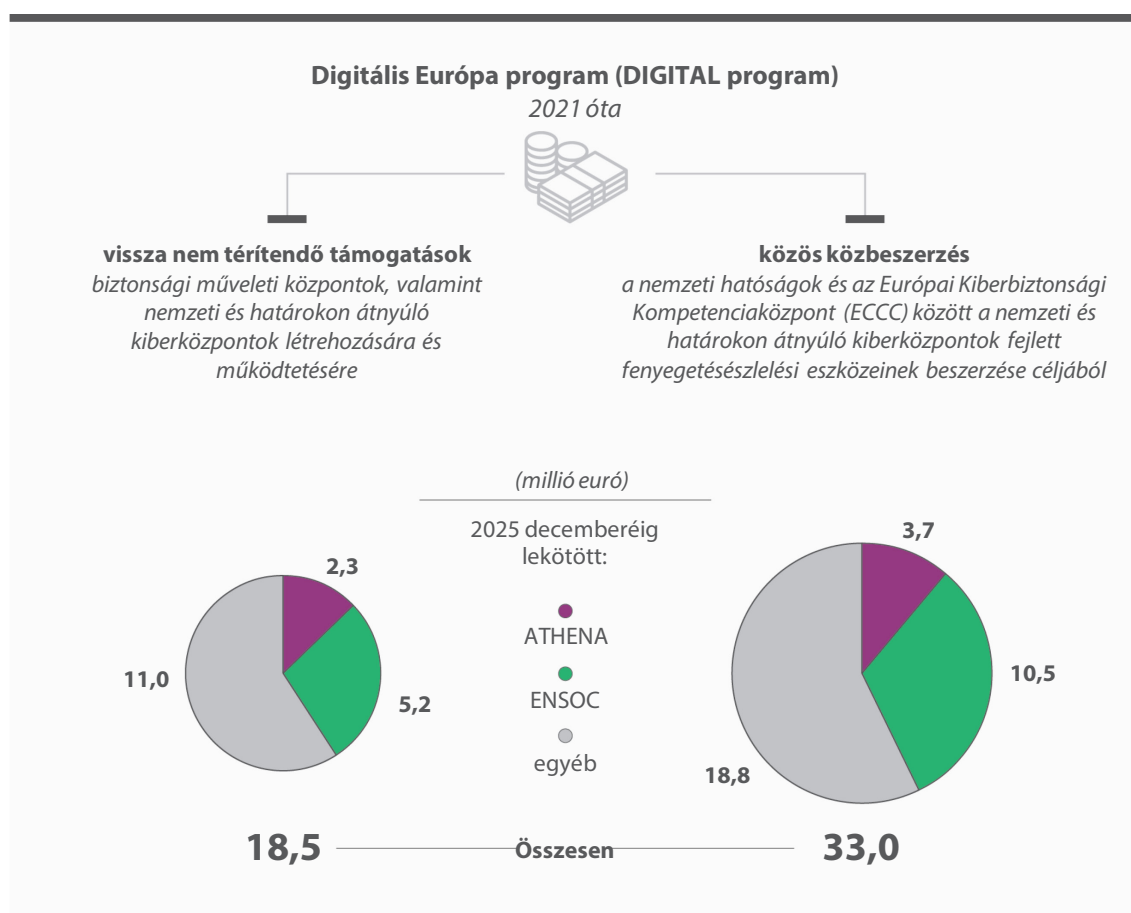
Forrás: Európai Számvevőszék.

64 Megvizsgáltuk, hogy miként hozták létre az első két, határokon átnyúló kiberközpontot, valamint hogy azok milyen előrelépést tettek az európai kiberbiztonsági figyelmeztető rendszer célkitűzéseinek megvalósítása terén. Megvizsgáltuk továbbá, hogy a határokon átnyúló kiberközpontok létrehozása hogyan illeszkedik a tágabb kiberbiztonsági környezetbe, és hogy az hogyan működik együtt a meglévő hálózatokkal és struktúrákkal.

A közbeszerzés jelentős késedelmei miatt eddig nem sikerült konkrét eredményeket elérni

65 A DIGITAL program keretében 2021 óta áll rendelkezésre finanszírozás a nemzeti és határokon átnyúló kiberközpontok létrehozásának támogatására. Ezt a finanszírozást egy összetett eljárás keretében nyújtják, két párhuzamosan meglévő forrásból: az egyik a központok létrehozását és működését támogató hagyományos vissza nem térítendő támogatások, a másik a fejlett fenyegetésészlelési eszközök beszerzésére irányuló közös közbeszerzés (lásd: [6. ábra](#)). Az ATHENA és az ENSOC a 2022. novemberi pályázati felhívást követően, 2024 januárjában kezdte meg munkáját.

6. ábra | A Digitális Európa program kiberközpontoknak nyújtott finanszírozása



Forrás: Európai Számvevőszék, a ECCC adatai alapján.

- 66** A kétszakaszos meghívásos közbeszerzési eljárásokat¹¹ az ATHENA és az ENSOC tagjai, valamint az első szakasz esetében a Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága, a második szakasz esetében pedig az újonnan létrehozott ECCC szervezte. A kétszakaszos megközelítés célja, hogy korlátozza az érzékeny információk terjesztését azáltal, hogy a részletes műszaki leírást csak az első szakasz után, a kiválasztott pályázóknak adja meg.
- 67** Az első szakasz az ENSOC esetében 2024 májusában, az ATHENA esetében pedig 2024 júliusában kezdődött. Az érdekelt vállalatoknak egy hónap állt rendelkezésükre, hogy jelentkezzenek. A sikeres pályázókat azonban csak 2025 áprilisában, közel egy évvel az eljárás megindítása után értesítették.
- 68** Ezenkívül akkoriban sem az ENSOC, sem az ATHENA közbeszerzési eljárásai nem tudtak továbblépni a második szakaszba, mivel a központ tagjai és az ECCC nem tudták biztosítani az előválogatott vállalatok számára az ajánlat benyújtásához szükséges műszaki leírásokat, mivel még dolgoztak azok véglegesítésén.
- 69** A közbeszerzési eljárások második szakasza csak 2025 augusztusában kezdődött meg az ENSOC egyes tételei esetében, az ATHENA esetében pedig 2026 elejére tervezték azt. Ellenőrzésünk idején, 18 hónappal a közbeszerzési eljárás megindítása után még egyik tételre vonatkozóan sem írtak alá szerződést. Véleményünk szerint a szerződések időben történő megkötését a megfelelő előkészítés hiánya és a közbeszerzési eljárások összetettsége hátráltatta.
- 70** Megállapítottuk tehát, hogy a határokon átnyúló központok nem haladnak megfelelően célkitűzéseik elérése felé. A fenyegetések észlelésére és az információk megosztására szolgáló eszközök nélkül ezek a központok működésképtelenek, és az európai kiberbiztonsági figyelmeztető rendszer sem működik, ami késlelteti a kiberfenyegetések és -események észlelésére és megelőzésére szolgáló fejlett képességek tényleges kiépítését. A támogatási megállapodás időtartamát módosítások révén meghosszabbították, így az tükrözi a közbeszerzési eljárások eddigi (az ATHENA esetében 15 hónapos, az ENSOC esetében pedig 18 hónapos) késedelmét.

¹¹ ENSOC ajánlati felhívás és ATHENA ajánlati felhívás.

A határokon átnyúló kiberközpontok további kommunikációs csatornákat hoznak létre, amelyekkel tovább nő az összetettség

- 71** A határokon átnyúló kiberközpontok egyik fő feladata releváns információk megosztása a fenyegetések észlelésének és az azokra való reagálásnak a javítása érdekében. Ilyen információk többek között azok, amelyek a kiberfenyegetésekre, a sebezhetőségekre, a fertőzöttségi mutatókra és a fenyegető szereplőkre vonatkoznak. A határokon átnyúló kiberközpontok feladatai részben átfedésben vannak a nemzeti CSIRT-ek és a CSIRT-hálózat feladataival, különösen ami a kiberfenyegetésekkel és -sérülékenységekkel kapcsolatos információk megosztását illeti. A határokon átnyúló kiberközpontok és a CSIRT-ek szerepe nem különül el egyértelműen. A 2025. évi kiberbiztonsági terv (29. bekezdés) szerint a határokon átnyúló kiberközpontoknak mind technikai (mint a nemzeti CSIRT-ek és a CSIRT-hálózat), mind operatív szinten (mint az EU-CyCLONe) működniük kell.
- 72** A kiberszolidaritásról szóló jogszabály előírja a határokon átnyúló kiberközpontok számára, hogy a könnyebb információmegosztás érdekében írjanak alá egymással együttműködési megállapodásokat. A kiberszolidaritásról szóló jogszabály értelmében az ENISA-nak 2026 februárjáig iránymutatásokat kellett volna kiadnia a határokon átnyúló kiberközpontok közötti interoperabilitásra vonatkozóan. Időközben (2025 decemberében) az ECCC támogatást ítelt oda egy konzorciumnak (ebben az ENSOC és az ATHENA egyes tagjai is részt vesznek) a határokon átnyúló kiberközpontok közötti interoperabilitás technikai keretének kialakítására. Az iránymutatások és a keret azonban csak akkor készülnek el teljes mértékben, ha a határokon átnyúló kiberközpontok már működésbe léptek. Amint arra a kiberszolidaritásról szóló jogszabályra irányuló javaslatról megfogalmazott 2023. évi véleményünkben¹² rámutattunk, fennáll a kockázat, hogy gyors megállapodás nélkül egymással összeegyeztethetetlen rendszereket fejlesztenek ki, ami a költségek megnövekedéséhez vezet.

¹² 02/2023. sz. vélemény a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról, 26. bekezdés.

- 73** A határokon átnyúló kiberközpontoknak emellett indokolatlan késedelem nélkül meg kell osztaniuk a nagyszabású kiberbiztonsági eseményekre vonatkozó releváns információkat az EU-CyCLONe-nal és a CSIRT-hálózattal. Tagállami szinten a nemzeti kiberközpontok létrehozása és a határokon átnyúló kiberközpontokban való részvétel további kommunikációs rétegeket hoz létre. Az olyan nem uniós tagállamokkal¹³ való koordináció, amelyek nem tagjai a CSIRT-hálózatnak vagy az EU-CyCLONe-nak, szintén növeli az összetettséget.
- 74** A közös taxonómiáról és az információmegosztás módjáról való egyeztetéshez, valamint az interoperabilitás biztosításához egyértelmű együttműködési megállapodásokra van szükség. A CSIRT-hálózatból levont tanulságok alapján elmondható, hogy ez egy jelentős kihívás. Megállapítottuk, hogy ellenőrzésünk időpontjáig nem született megállapodás az együttműködésre és az információmegosztásra vonatkozó eljárási szabályokról. Meglátásunk szerint a nemzeti, illetve a határokon átnyúló kiberközpontok létrehozása előmozdíthatná az eredményesebb információmegosztást. A határokon átnyúló központoknak a már amúgy is összetett kiberbiztonsági környezetbe való integrálása azonban kihívást fog jelenteni, és további kommunikációs csatornákra és együttműködési megállapodásokra lesz szükség.

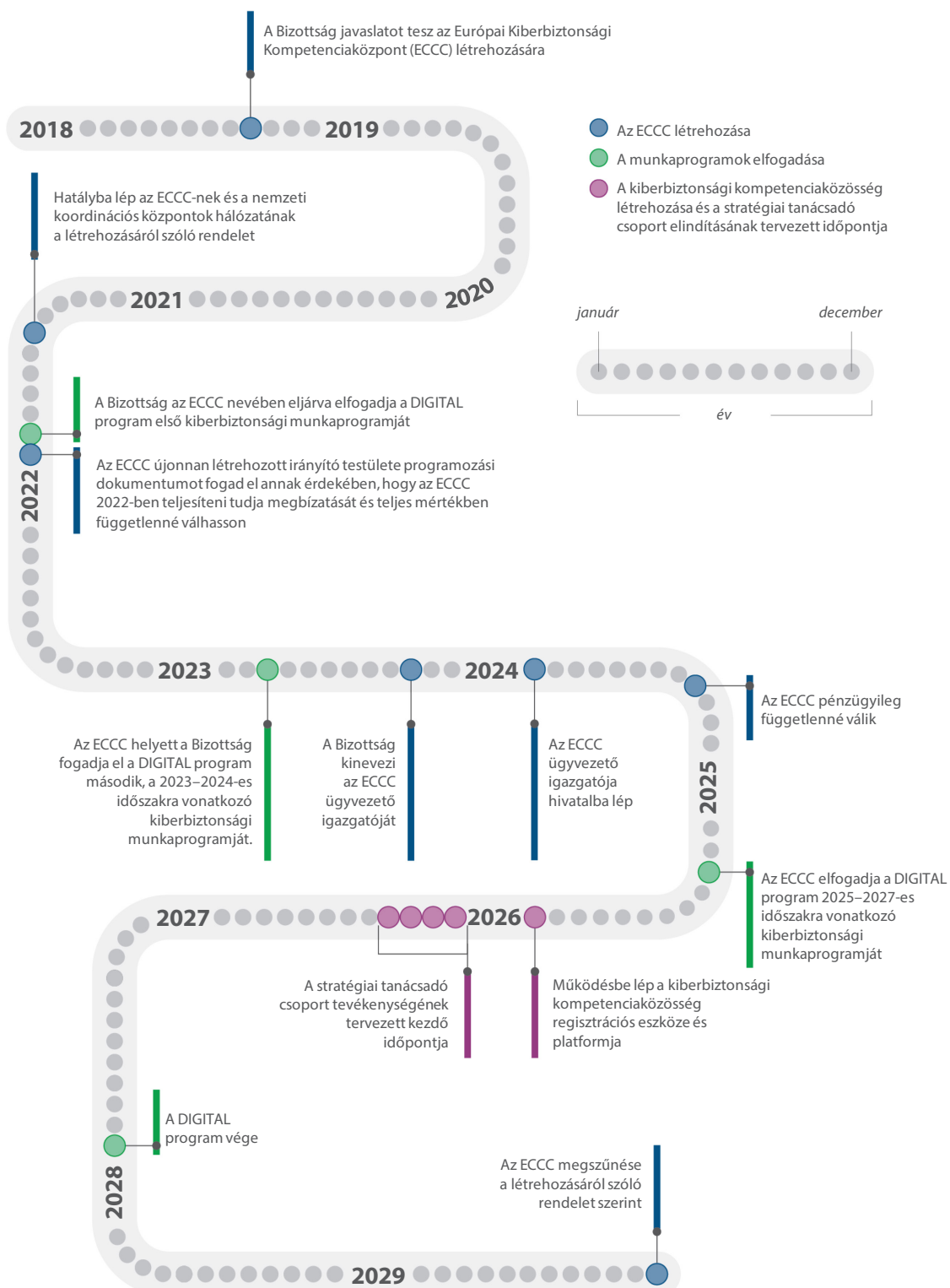
¹³ Izland és Norvégia.

A DIGITAL program keretében uniós finanszírozásban részesülő projektek célja a kiberbiztonság megerősítése, de e projektek a végrehajtás és a beszámolás terén kihívásokkal szembesülnek

Késedelmes létrehozása miatt a kiberbiztonsági kompetenciaközösség nem tudta igényeinek megfelelően alakítani a DIGITAL programot

- 75** A DIGITAL program kiberbiztonsági komponensének kezelése érdekében a Bizottság 2018-ban javaslatot tett az Európai Kiberbiztonsági Kompetenciaközpont (ECCC) létrehozására. Az ECCC-rendelet azt irányozta elő, hogy az ECCC tevékenységét egy 29 nemzeti koordinációs központból (tagállamonként egy, valamint Izlandból és Norvégiából egy-egy) álló hálózat támogassa. Szorgalmazta továbbá a kiberbiztonsági kompetenciaközösség (a továbbiakban: a közösség) létrehozását, amely az ágazat, a tudományos és kutatási szervezetek, valamint más érintett civil társadalmi szervezetek képviselőiből áll.
- 76** A közösség legfeljebb 20 tagját neveznék ki a stratégiai tanácsadó csoportba (SAG), amely az ECCC struktúráját alkotó három fő komponens egyike. A stratégiai tanácsadó csoport egyik fő feladata, hogy nyilvános konzultációkat szervezzon az ECCC menetrendjének és DIGITAL programon belüli munkaprogramoknak a kidolgozása érdekében.
- 77** Megvizsgáltuk, hogy a DIGITAL programot és munkaprogramjait az igények alapos elemzése alapján fogadták-e el, valamint azt, hogy az ECCC, a nemzeti koordinációs központok hálózata, a közösség és a stratégiai tanácsadó csoport hogyan tudott hozzájárulni a munkaprogramokhoz. A gyakorlatban az ECCC-t, a nemzeti koordinációs központok hálózatát, a közösséget és a stratégiai tanácsadó csoportot fokozatosan, több év alatt hozták létre (lásd: [7. ábra](#)).

7. ábra | Az Európai Kiberbiztonsági Kompetenciaközpont, a nemzeti koordinációs központok hálózata, a közösség és a stratégiai tanácsadó csoport létrehozásának időrendi sorrendje



Forrás: Európai Számvevőszék.

- 78** Mivel az ECCC csak 2024 szeptemberében vált teljes mértékben működőképpé, az ECCC nevében a Bizottság fogadta el a 2021–2022-es és a 2023–2024-es időszakra vonatkozó munkaprogramokat. A Bizottság által elfogadott két munkaprogramhoz a közösség nem tudott hozzájárulni.
- 79** Időközben a tagállamok megkezdték a közösség nemzeti szintű kapcsolattartó pontjaiként működő nemzeti koordinációs központjaik létrehozását. Létrehozásukat és működésüket a DIGITAL program társfinanszírozta, amely ellenőrzésünk időpontjáig több mint 90 millió euró összegű uniós finanszírozást nyújtott, ebből mintegy 44 millió eurót pénzügyi támogatás révén harmadik feleknek fognak továbbosztani. 2027-ig további 38 millió eurót irányoztak elő a nemzeti koordinációs központok támogatására.
- 80** Megállapítottuk, hogy 2025 decemberében, négy évvel az ECCC és a nemzeti koordinációs központok hálózatának létrejötte után még mindig nem hozták létre a közösséget, és a stratégiai tanácsadó csoportot sem nevezték ki. Az ECCC 2025. március 14-én fogadta el a DIGITAL program legutóbbi kiberbiztonsági munkaprogramját, amely a 2025–2027-es időszakra vonatkozik. Bár az ECCC a tagállamokkal és a nemzeti koordinációs központok hálózatával folytatott széles körű konzultációt követően készítette és fogadta el a munkaprogramját, a közösség, illetve a stratégiai tanácsadó csoport észrevételeit és tanácsait nem tudta felhasználni. Ez nem felel meg az alapító rendelet rendelkezéseinek, és meglátásunk szerint egy elszalasztott lehetőségről van szó.
- 81** A DIGITAL program 2027-ben lezárul, és ha nem hosszabbítják meg a megbízatását, az ECCC várhatóan 2029-ben megszűnik. A nemzeti koordinációs központok hálózatának, a közösségnek és a stratégiai tanácsadó csoportnak a támogatása tehát létrejöttüket követően csak rövid ideig lehet releváns.

Az uniós finanszírozású projektek célkitűzései relevánsak, de sok projekt operatív problémákkal küzd

82 Kiválasztottunk egy, a 2022–2025-ös időszakban a DIGITAL program keretében finanszírozott, a kiberbiztonsági események észlelése és az azokra való reagálás szempontjából releváns 11 projektből álló mintát (lásd: az [I. melléklet 5. ábrája](#) és a [III. melléklet](#)). A következőket vizsgáltuk meg:

- a projektek célkitűzései összhangban voltak-e a pályázati felhívásokban megfogalmazott elérendő eredményekkel és a DIGITAL program általános célkitűzéseivel;
- a projektek elérték-e eddig tervezett outputjaikat és eredményeiket;
- a projektek outputjai időben valósultak-e meg.

Ezen értékelés eredményét a [IV. melléklet](#) mutatja be.

Egyes projekteknél korai eredmények mutatkoznak, de sokuk operatív nehézségekkel és késedelmekkel szembesül

83 Megállapítottuk, hogy valamennyi projekt olyan célokat tűzött ki, amelyek hozzájárulnak a DIGITAL program kiberbiztonsági célkitűzéseinek¹⁴ eléréséhez, és le is fedik a pályázati felhívások legtöbb célkitűzését¹⁵.

84 A mintánkban szereplő 11 projekt közül két projekt a végrehajtás korai szakaszában volt, ezért teljesítményükről nem tudtunk következtetést levonni. A fennmaradó projektek közül négyet a tervezett outputok és eredmények elérése tekintetében kielégítőnek értékeltünk. Két projekt esetében úgy ítéltük meg, hogy mutatnak némi hiányosságot, három projektet pedig nem kielégítőnek értékeltünk (lásd: [IV. melléklet](#)).

85 A DIGITAL program kifejezett célja a kis- és középvállalkozások (kkv-k) kiberbiztonsági szintjének növelése. E tekintetben számos projekt kínál konkrét megoldásokat a kkv-k számára (lásd: [2. háttérmagyarázat](#)).

¹⁴ A Digitális Európa program létrehozásáról szóló (EU) 2021/694 rendelet 6. cikke.

¹⁵ Felhívások: *Capacity building of security operation centres; Deploying the network of national coordination centres with member states; Preparedness support and mutual assistance;* és *Novel applications of AI and other enabling technologies for security operation centres.*

2. háttérmagyarázat

Olyan projektek, amelyek kézzelfogható eredményeket hoznak a kkv-k számára (példák)

A **III. melléklet** 6. projektjének, a **GR-SME-SOC** projektnek a célja, hogy kiberbiztonsági eszközöket biztosítson és szolgáltatásokat nyújtson kkv-k számára Görögországban azáltal, hogy az igényeikhez igazított biztonsági műveleti központot (SOC) hoz létre. A 2024 januárjában indult projektet egy öt görög szervezetből álló konzorcium hajtja végre. A terv az, hogy 120 kkv számára egy évig díjmentesen kiberbiztonsági szolgáltatásokat kínáljanak, ezt követően pedig a szolgáltatások kereskedelmi forgalomban lesznek elérhetők. A projekt fejlett szolgáltatásokat kínál a kkv-k számára, például valós idejű nyomon követést, mesterséges intelligencián alapuló fenyegetésészlelést és az incidensekre való agilis reagálást.

A **III. melléklet** 3. projektje, az **NCC-IE** projekt keretében a projektkoordinátor mintegy 1,8 millió euró összegű vissza nem térítendő támogatást nyújtott Írországból több mint 50 kkv-nak kiberbiztonságuk javítása érdekében. A program 2–200 alkalmazottat foglalkoztató vállalkozásoknak, köztük családi vállalkozásoknak, induló innovatív vállalkozásoknak és különböző ágazatok globális exportőreinek nyújtott támogatást. Támogatásban kizárólag olyan vállalkozások részesülhettek, amelyek korábban átestek az Enterprise Ireland kormányzati ügynökség által irányított kiberbiztonsági felülvizsgálaton. A támogatás a felülvizsgálat ajánlásainak végrehajtásához szükséges költségek 80%-át fedezte (legfeljebb 60 000 eurós összegig).

Forrás: Európai Számvevőszék.

- 86** A mintánkban szereplő projektek közül sok esetében nehéznek bizonyul a határidők betartása, illetve működési kihívásokkal kell szembenézni (lásd: **IV. melléklet**). Négy projekt esetében állapítottunk meg jelentős késedelmet. Közöttük volt az ENSOC és az ATHENA is (részletesen lásd: **65–70.** bekezdés). Erre a **3. háttérmagyarázat** szolgál további példákkal.

3. háttérmagyarázat

Operatív kihívásokkal és késedelmekkel szembesülő projektek (példák)

A **III. melléklet** 8. projektje, az írországi **ILG-SOC** projekt támogatásának egyedüli kedvezményezettje a helyi önkormányzatok irányító hatósága (LGMA). A projekt célja egy központi biztonsági műveleti központ létrehozása 31 önkormányzat számára fejlett fenyegetésészlelési és -reagálási eszközök használata érdekében. A hároméves időtartamra tervezett projekt 2023 októberében indult. A félidős felülvizsgálat során valamennyi elérendő eredmény elutasításra került. A projekt több közbeszerzési eljárása kudarcot vallott vagy késedelmet szenvedett. A projekt időtartamát meg fogják hosszabbítani (de további források nélkül), ami elegendő időt biztosíthat a projekt sikeres lezárásához.

A **III. melléklet** 5. projektje, a görögországi **EL-SOC** projekt célja egy konszolidált biztonsági műveleti központ létrehozása nemzeti szinten, amely az ágazati biztonsági műveleti központoktól származó információkat gyűjtené össze. Ezzel valós idejű és átfogó áttekintés állna rendelkezésre a kiberbiztonsági helyzetről. A projektet 2024 januárja és 2026 decembere között hajtják végre. A hardverek és szolgáltatások tervezett beszerzése késedelmet szenvedett az ajánlati felhívás műszaki leírásának véglegesítésével és közzétételével kapcsolatos problémák miatt. A késedelem okaként a projektkoordinátor megemlítette a nemzeti társfinanszírozás biztosításával és a közbeszerzésért felelős személyzet korlátozott rendelkezésre állásával kapcsolatos problémákat is.

Forrás: Európai Számvevőszék.

- 87** Két másik, a mintánkban szereplő projekt teljesítése mérsékelten késedelmes. Három projekt esetében a teljesítés időben zajlik. Végezetül két projekt a végrehajtás korai szakaszában van, ezért ezekről nem tudunk következtetést levonni.

A nemzetbiztonsági szabályozások működési nehézségekhez vezettek, és jelentős kockázatok állnak fenn a kedvezményezettek által végzett ellenőrzések során

- 88** A Digitális Európa programról szóló rendelet értelmében a kiberbiztonság finanszírozása biztonsági okokból az Unióban letelepedett és a tagállamok vagy uniós polgárok által ellenőrzött szervezetekre korlátozható. E korlátozás célja, hogy csökkentse a nem uniós államok behatolásának vagy befolyásának kockázatát, és megakadályozza az érzékeny biztonsági információk nem uniós hatóságokkal való megosztását.
- 89** Az uniós tulajdonosi szerkezettel és az ellenőrzéssel kapcsolatos kötelezettség nemcsak a támogatások kedvezményezettjeire vonatkozik, hanem azok alvállalkozóira és a harmadik feleknek nyújtott pénzügyi támogatás (FSTP) kedvezményezettjeire is. Ez utóbbi kategória kivételével (lásd: [92–96.](#) bekezdés) az értékelést az [Európai Kutatási Végrehajtó Ügynökség Központi Hitelesítési Szolgálat](#)a végzi. A meghívásos pályázati felhívásokban való részvételre való jogosultságról azonban továbbra is a támogatást nyújtó hatóság, azaz a Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága vagy az ECCC dönt.
- 90** Ellenőrzési munkánk során a kedvezményezettek többször is megemlítették a tulajdonosi szerkezetre és az ellenőrzésre vonatkozó értékelések (OCA-értékelések) által támasztott gyakorlati kihívásokat. Az uniós tulajdonosi szerkezet és az ellenőrzés értékelése összetett és hosszadalmas folyamat lehet. Ehhez elemezni kell az egyes szervezetek teljes tulajdonosi szerkezetét és ellenőrzési láncát, beleértve az összes tulajdonosi réteget egészen a végső tulajdonosokig. A Központi Hitelesítési Szolgálat előírja, hogy minden szervezetnek nagyszámú [igazoló dokumentumot](#) kell benyújtania tulajdonosi szerkezetéről és konkrét jogairól, vállalatirányításáról, valamint az ellenőrzést biztosító kereskedelmi, pénzügyi vagy egyéb kapcsolatairól.
- 91** A mintánkban szereplő három uniós finanszírozású projektből később legalább egy konzorciumi kedvezményezettet kizártak, mivel úgy ítélték meg, hogy az az Unión kívüli tulajdonban vagy ellenőrzés alatt áll. A konzorciumi tagok kizárása azt mutatja, hogy az uniós tulajdonosi szerkezet és ellenőrzés fogalmát a DIGITAL program nem minden résztvevője érti meg teljes mértékben. A 2022–2025-ös időszakban összességében a Központi Hitelesítési Szolgálat adatai alapján a DIGITAL program kiberbiztonsági támogatásait kérelmező pályázók, illetve alvállalkozók 7%-a nem felelt meg az értékelésen. A támogatásra nem jogosult résztvevők pályázati felhívásra való jelentkezése késedelmet okoz (lásd: [4. háttérmagyarázat](#)).

4. háttérmagyarázat

Egyes kedvezményezetteket kizártak, mert nem mentek át a biztonsági ellenőrzéseken (példa)

A **III. melléklet** 7. projektje, az **NG-SOC** projekt konzorciumi tagjai közül kettő nem ment át a tulajdonosi szerkezetre és az ellenőrzésre vonatkozó értékelésen. Az értékelés eredményét körülbelül egy hónappal a támogatási megállapodás aláírásának határideje előtt jelentették be. A projektkoordinátornak meg kellett állapodnia arról, hogy átveszi a két kizárt tagra bízott munkát, mivel nem volt idő új partnert találni. Az egyik kizárt tag egy konkrét iparágban tevékenykedett, ahol a kifejlesztett megoldást tesztelni kellett. Emiatt a projekt jelentős része, amely a megoldások gyakorlati tesztelésére vonatkozott, nem tudott a terveknek megfelelően haladni. Ezt a helyzetet később úgy orvosolták, hogy új tagok felvétele érdekében módosították a támogatási megállapodást.

Forrás: Európai Számvevőszék.

- 92** Az általunk vizsgált projektek közül kettő (NCC-IE és CYberSynchrony) harmadik feleknek nyújt pénzügyi támogatást (FSTP). Ez a finanszírozási mechanizmus lehetővé teszi a támogatások kedvezményezettjei számára, hogy a vissza nem térítendő támogatás egy részét nyílt pályázati felhívásokon keresztül más szervezetek finanszírozására használják fel. Az FSTP megkönnyítheti az uniós finanszírozáshoz való hozzáférést. Ebben az esetben a tulajdonosi szerkezetre és az ellenőrzésre vonatkozó értékelések (OCA-értékelések) lebonyolításáért kizárólag a kedvezményezettek tartoznak felelősséggel, a Központi Hitelesítési Szolgálat azokban nem vesz részt.
- 93** 2021-ben a Bizottság általános nyilvános útmutatót tett közzé a meghívásos pályázati felhívásokra jelentkezők számára, amelyet 2026-ban aktualizált. Bár az FSTP 2021 óta működik a DIGITAL program felhívásai esetében, sem a Bizottság, sem az ECCC nem mutatott be részletes módszertant a kedvezményezettek számára arra vonatkozóan, hogyan végezzék el a tulajdonosi szerkezetre és az ellenőrzésre vonatkozó vizsgálatokat azon harmadik felek értékelése során, amelyeknek pénzügyi támogatást nyújtanak. 2025 júliusában az ECCC nem kötelező iránymutatást osztott meg a nemzeti koordinációs központok hálózatával, amely strukturált megközelítést mutat be az OCA-ellenőrzésekhez. Az iránymutatás általános elveket és lehetséges lépéseket tartalmaz. Azt azonban nem határozza meg, hogyan kell konkrétan elvégezni az ellenőrzéseket, tehát a kedvezményezettek feladata, hogy kidolgozzák saját megközelítésüket.

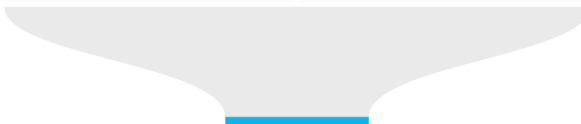
- 94** Megállapítottuk, hogy az ECCC nem validálja a kedvezményezettek által elfogadott módszertant, és mintavételen alapuló ellenőrzéseket sem végez annak biztosítására, hogy a módszertan kellően megalapozott legyen, és hogy a pénzügyi támogatás kiválasztott kedvezményezettjei valóban uniós tulajdonban legyenek és uniós ellenőrzés alatt álljanak.
- 95** [2024. évi éves jelentésünkben](#) megállapítottuk, hogy a Bizottság által a harmadik feleknek nyújtott pénzügyi támogatás kezelésével megbízott kedvezményezettek számára (a kutatás területén) nem kötelező bizonyítani, hogy ellenőrzéseik eredményesen biztosítják az uniós kiadások szabályszerűségét. Az ECCC azt sem értékeli, hogy a kedvezményezettek rendelkeznek-e megfelelő adminisztratív és technikai kapacitással az OCA-értékelések megfelelő lebonyolításához. Ez az értékelés összetett lehet, és azt uniós szinten egy külön erre a célra létrehozott, speciális szakértelemmel rendelkező részleg végzi el (részletesen lásd: [90.](#) bekezdés).
- 96** Ennek kapcsán úgy véljük, hogy jelentős a kockázata annak, hogy az OCA-ellenőrzések elvégzéséért felelős kedvezményezettek nem rendelkeznek az ellenőrzések megfelelő elvégzéséhez szükséges kapacitással. Tekintettel a finanszírozott tevékenységek jellegére, ez a hiányosság kitettséget jelenthet az érzékeny infrastruktúrára, működési adatokra és biztonsági szempontból kritikus technológiákra nézve.

A legtöbb uniós finanszírozású projekt nem rendelkezik megfelelő teljesítménymérési kerettel, és a DIGITAL program kiberbiztonsággal kapcsolatos teljesítményadatai nem pontosak

A legtöbb uniós finanszírozású projekt nem rendelkezik megfelelő teljesítménymérési kerettel

- 97** Az uniós finanszírozású projekteket irányító kedvezményezetteknek mérföldkövek, elérendő eredmények és mutatók révén be kell számolniuk az ECCC-nek az elért haladásukról és az eredményeikről (ennek szemléltetését lásd: [8. ábra](#)). Megvizsgáltuk, hogy az egyes projektekre vonatkozóan meghatározott mérföldkövek és elérendő eredmények megfelelően lehetővé teszik-e a projektmonitoringot. Értékeljük azt is, hogy a teljesítménymutatók relevánsak és mérhetőek-e, illetve hogy rendelkeznek-e alap- és célértékkel.

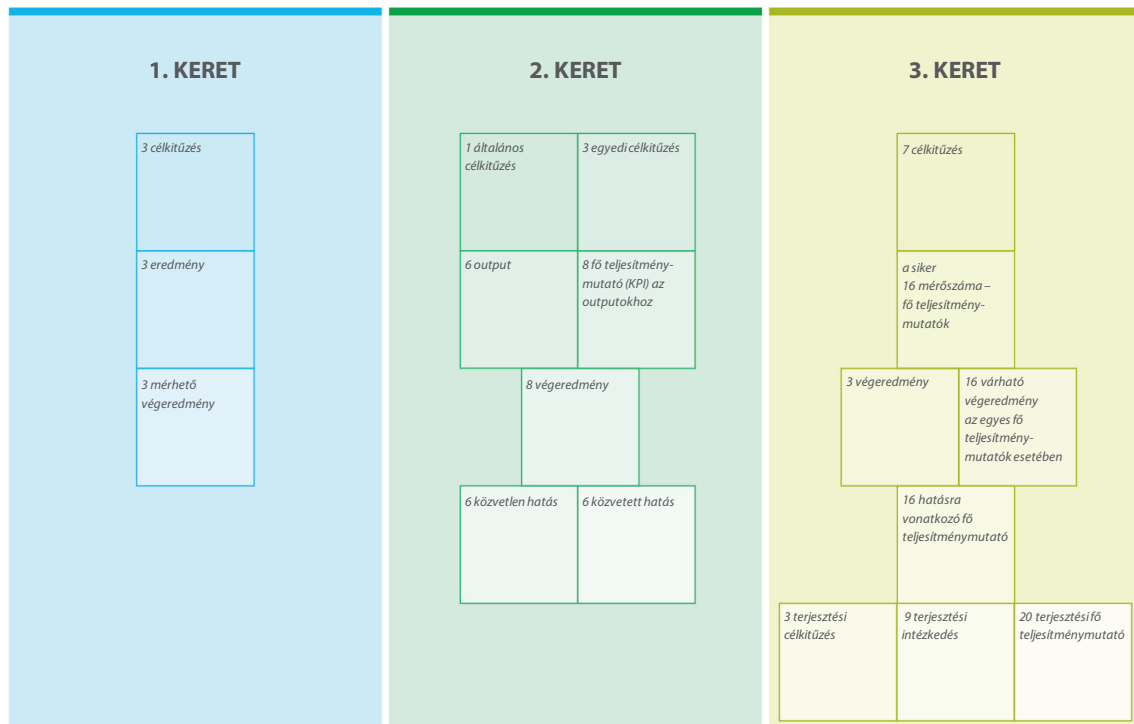
8. ábra | Mérföldkövek, elérendő eredmények és teljesítménymutatók a DIGITAL program projektjeiben

	 Mérföldkövek	 Elérendő eredmények	 Teljesítménymutatók
Meghatározásuk	szabályozási pontok a projekt során, amelyek segítenek az előrehaladás követésében	az előrehaladás bemutatása céljából benyújtott projektoutputok	az eredmények mérésére használják
Értékük megadása	csak a legfőbb outputokhoz kapcsolódik (számuk korlátozott)	csak a főbb outputok (projektenként legfeljebb 10–15)	konkrét, mérhető, megvalósítható, releváns és határidőhöz kötött
Példák	„a platform kísérleti szakaszának elindítása”	„a platform felhasználói kézikönyve”	„az incidensekre való reagálási idő 30%-os csökkentése”
	 Strukturált megközelítés, az online támogatáskezelési rendszer része		 Nem strukturált megközelítés

Forrás: Európai Számvevőszék, a [pályázati űrlap](#) alapján.

- 98** A projektjavaslatban a kedvezményezetteknek – a pályázóknak szóló utasításokban meghatározott strukturált megközelítést követve – meg kell határozniuk a mérföldkövet és az elérendő eredményeket. A nyomon követést segíti, hogy az elektronikus támogatáskezelési rendszer felsorolja az összes mérföldkövet és elérendő eredményt. Az ECCC általában kétszer vizsgálja felül az egyes projekteket: egyszer a projekt félidejében, egyszer pedig annak befejezése után. E felülvizsgálatok során külső szakértők ellenőrzik a mérföldkövek és eredmények elérését, majd az ECCC validálja azokat. A mérföldkövek és az elérendő eredmények tehát döntő fontosságúak a projektmonitoring szempontjából, ezért megfelelően kell őket meghatározni.
- 99** Megállapítottuk, hogy a mintánkban szereplő projektek közül szinte egyik sem követte a mérföldkövek és elérendő eredmények számára vonatkozó utasításokat: a mérföldkövek száma projektenként 8 és 39 között, míg az elérendő eredmények száma 8 és 45 között változik. Számos mérföldkő és elérendő eredmény nem felel meg a kidolgozásukra vonatkozó utasításoknak, ezért nem használhatók az előrehaladás nyomon követése szempontjából (ilyen például „a kutatási pályázati felhívás megszövegezésének kezdeményezésére tartott ülés” vagy „a projektülés hivatalos jegyzőkönyve”). Három projekt esetében az értékelőbizottság még a támogatás aláírása előtt feltárta ezeket a problémákat. Két esetben a kedvezményezettek csak kisebb változtatásokat javasoltak (pl. a határidők tekintetében), és nem foglalkoztak az alapvető kérdésekkel, míg a harmadik esetben semmilyen változtatást nem eszközöltek. A mintánkban szereplő hat másik projekt esetében elemzésünk rámutatott, hogy a mérföldkövek, illetve az elérendő eredmények nincsenek összhangban az utasításokkal, és esetenként nem megfelelőek. Meglátásunk szerint a nem megfelelően meghatározott, illetve túl sok elérendő eredmény vagy mérföldkő megnehezíti az előrehaladás nyomon követését.
- 100** A mérföldkövekkel és az elérendő eredményekkel ellentétben a teljesítménymutatók nem követnek strukturált megközelítést, és azokat nem konszolidálják egy táblázatban a támogatáskezelési rendszerben, hanem a pályázat egyes szakaszaiban határozzák meg. Ez a módszer azt eredményezte, hogy a kedvezményezettek számos különféle teljesítménymérési keretet javasoltak. Míg egyesek csak teljesítménymutatókhoz kapcsolt projektcélkitűzéseket határoztak meg, mások sokkal összetettebb teljesítménymérési kereteket dolgoztak ki. Ezekre a **9. ábra** mutat be néhány példát.

9. ábra | A projektekhez kialakított különböző teljesítménymérési keretek (példák)



Forrás: Európai Számvevőszék.

101 Elemzésünk alapján megállapítottuk, hogy a projektek által használt több teljesítménymutató nem releváns vagy nem mérhető, és nem tartalmaz célértéket vagy alapértéket (lásd: [5. háttérmagyarázat](#)). Emellett hét projekt 20 vagy annál több mutatót határozott meg, sőt egy projekthez 52 mutatót rendeltek. Ezen értékelés eredményét a [IV. melléklet](#) mutatja be.

5. háttérmagyarázat

Nem megfelelő teljesítménymutatók (példák)

Nem mérhető:

- „A fertőzöttségi mutató, illetve az egyéb, a kkv-k kiberbiztonsági kapacitáit erősítő szolgáltatásokra vonatkozó mutató”
- „Az EU-CyCLONe kommunikációs csatornákkal való integrációt lehetővé tevő incidensreagálási eszközök és módszerek biztosítása”

Nincs megadva alapérték vagy célérték:

- „legalább 20%-os javulás a személyzet felkészültségében”
- „a vonatkozó uniós kiberbiztonsági kezdeményezésekhez való igazodáshoz és az azoknak való megfeleléshez szükséges erőfeszítések legalább 20%-os csökkentése”

Nem teljesítményfüggő:

- „A projekt zárójelentésének elkészítése a finanszírozási szakasz végén”
- „Az összes képzésen részt vevő gyakornokok száma”

Forrás: Európai Számvevőszék, a projektdokumentáció alapján.

102 Összességében úgy véljük, hogy a teljesítménymérési keretek sokfélesége és a mutatók nem megfelelő kialakítása, illetve túlzott száma nagymértékben bonyolítja a teljesítmény nyomon követését. Mindezek miatt nem lehet megfelelően értékelni a projektek teljesítményét. Ezt tovább bonyolítja az a tény, hogy az adatszolgáltatási sablon nem tartalmaz külön szakaszt a projektek teljesítménymutatóiról, így a mintánkban szereplő projektek többsége nem is számolt be azokról.

A DIGITAL program kiberbiztonsági komponensére vonatkozó teljesítményadatok nem pontosak

- 103** A DIGITAL program eredményeinek nyomon követése érdekében a rendelet programmutatókat határoz meg, amelyekről minden projektnek be kell számolnia (részletesen lásd: [6. háttérmagyarázat](#)).

6. háttérmagyarázat

A DIGITAL program kiberbiztonsági mutatói

- 1.a) A közösen – többek között az európai kiberbiztonsági figyelmeztető rendszerrel összefüggésben – beszerzett kiberbiztonsági infrastruktúrák és/vagy eszközök száma
- 1.b) A közös beszerzésű alkalmazott kiberbiztonsági infrastruktúrák és/vagy eszközök száma
2. Az európai kiberbiztonsági létesítményekhez hozzáféréssel rendelkező felhasználók és felhasználói közösségek száma
3. A kiberbiztonsági incidensekre való felkészültséget és az azokra való reagálást támogató fellépések száma a kiberbiztonsági vészhelyzeti mechanizmus keretében

Forrás: A Digitális Európa program létrehozásáról szóló (EU) 2021/694 rendelet II. melléklete; a Digitális Európa program monitoring- és értékelési kerete (SWD(2024) 37).

- 104** Megvizsgáltuk, hogy a mintánkban szereplő projektek beszámoltak-e ezekről a mutatókról, illetve hogy az ECCC hogyan gyűjti és ellenőrzi ezeket az adatokat.
- 105** A félidős és a végső felülvizsgálat előtt minden projekt kapcsán be kell számolni a támogatáskezelési rendszerben a DIGITAL program mutatóiról. Megállapítottuk, hogy ellenőrzésünk idején hét projekt járt az ütemterv felénél, tehát be kellett volna számolniuk ezekről a mutatókról, azonban közülük csak három tett így. E három közül kettő nem szolgáltatott pontos információkat: az egyik nem a megfelelő mutatóról számolt be, a másik pedig az elért eredmények helyett a célértékeket adta meg.

106 A Bizottság a [programteljesítmény-kimutatásaiban](#) minden évben beszámol ezekről a mutatókról. Így az érdekelt felek is értékelhetik, hogy a program teljesíti-e célkitűzéseit. A 2024. évi programteljesítmény-kimutatások szerint a DIGITAL program kiberbiztonsági mutatói jó úton haladnak. Az ECCC kifejtette számunkra, hogy e mutatók összeállításához a projektek kedvezményezettjeinek küldött felméréseket használta, tehát azokhoz nem a támogatáskezelési rendszert vette alapul. Az ECCC által szolgáltatott lebontott adatok áttekintésekor számos problémát találtunk az adatgyűjtés módjával és általános minőségével kapcsolatban. Megállapítottuk, hogy az összegyűjtött adatok nem felelnek meg a programteljesítmény-kimutatásban szereplő értékeknek, ezért nem egyértelmű, hogy a bejelentett értékeket hogyan számították ki. Nem találtunk bizonyítékot arra, hogy az ECCC ellenőrizte volna a bejelentett adatok pontosságát. A mintánkban szereplő projektek ellenőrzése alapján, mivel a legtöbb érték hiányzik vagy pontatlan, úgy véljük, hogy a bejelentett adatok nem tükrözik megfelelően az elért eredményeket.

A jelentést 2026. június 16-i luxembourgi ülésén fogadta el a George-Marius Hyzler számvevőszéki tag elnökölte III. Kamara.

a Számvevőszék nevében

Tony Murphy
elnök

Mellékletek

I. melléklet. Az ellenőrzésről

- 01** Meghatározása szerint a kiberbiztonság „a hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és a kiberfenyegetések által érintett egyéb személyeknek a védelméhez szükséges tevékenységeket” jelenti¹. Kiberfenyegetés „bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat”². A kiberbiztonság holisztikus megközelítést igényel, amely a kiberfenyegetések megelőzésére, észlelésére, az azokra való reagálásra és az azokat követő helyreállításra irányuló, egymással összefüggő tevékenységek sorából áll (lásd: az alábbi [1. ábra](#)).

¹ (EU) 2019/881 rendelet (kiberbiztonsági jogszabály).

² A kiberbiztonsági jogszabály 2. cikke.

1. ábra | Kiberbiztonsági tevékenységek (példák)

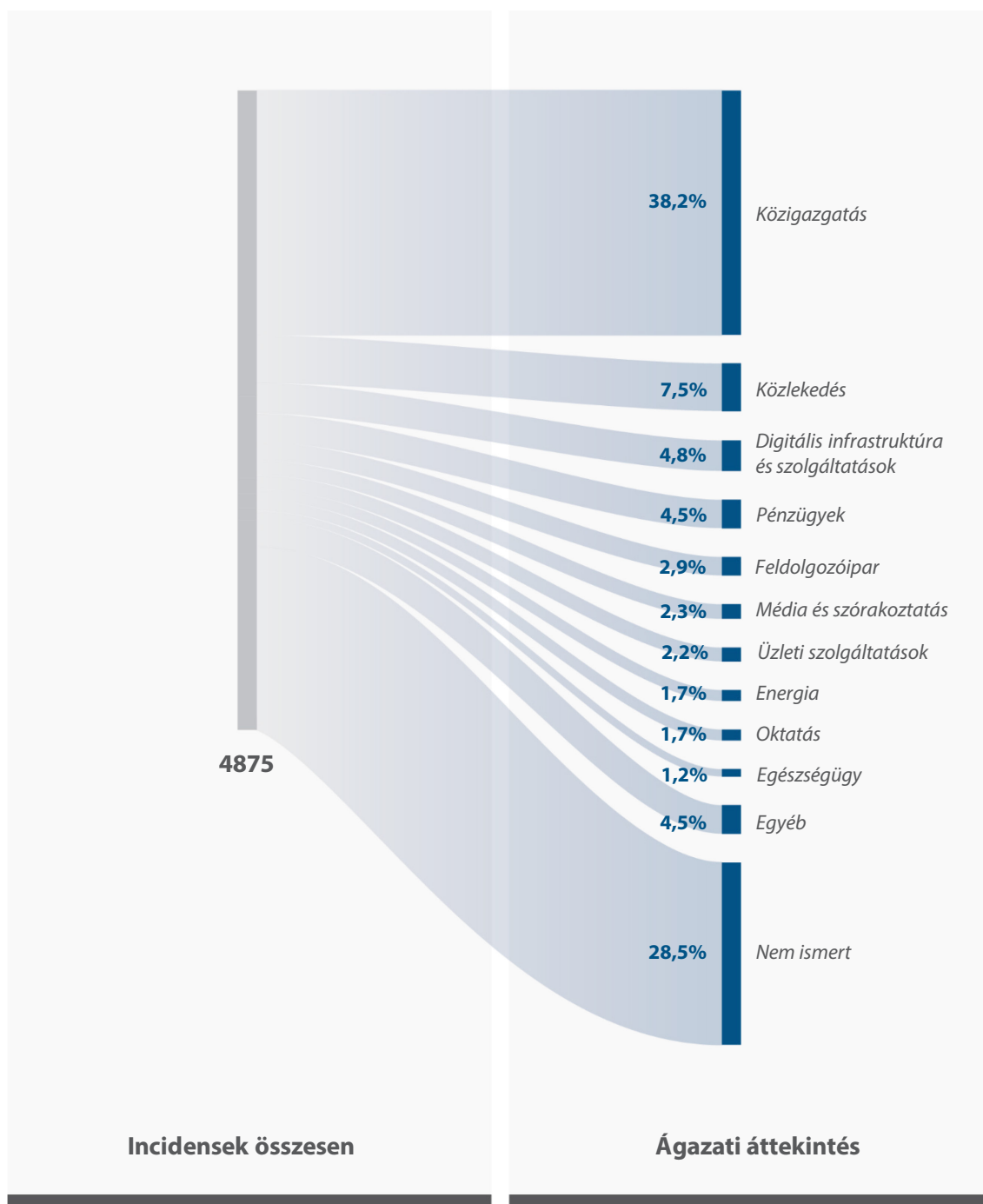
Megelőzés 	A kiberbiztonsági incidensek kockázatának csökkentése és lehetséges hatásainak minimalizálása <i>Példák: vírusirtó, tűzfalak, titkosítás, kétféle hitelesítés, szoftverfrissítés-kezelés, biztonsági tudatosságnövelő képzés a személyzet számára</i>
Feltárás 	Rossz szándékú tevékenység feltárása <i>Példák: hálózatmonitoring, helyzetismeret</i>
Reagálás 	A kiberbiztonsági incidensek kezelése és enyhítése a fenyegetés megfékezése és a további károk megelőzése révén <i>Példák: a fenyegetések eltávolítása, a szerverek elkülönítése és elszigetelése, a feltört fiókok letiltása és a jelszavak visszaállítása</i>
Helyreállítás 	Az érintett rendszerek, adatok és szolgáltatások biztonságos és működőképes állapotának helyreállítása <i>Példák: operációs rendszerek visszaállítása az érintett szerverekre, a biztonsági mentésekből származó adatok helyreállítása, tanulságok levonása, a szakpolitikák aktualizálása</i>

Forrás: Európai Számvevőszék, az egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló (EU) 2022/2555 irányelv (NIS 2 irányelv) (78) preambulumbekzdése alapján.

- 02** Az [Európai Unió Kiberbiztonsági Ügynökség \(ENISA\)](#) úgy véli, hogy a kiberbiztonsági fenyegetettség szintje jelentős, ugyanakkor megjegyzi, hogy a kiberbiztonsági fenyegetettség helyzete jóval összetettebbé vált és továbbra is az marad³. Ezek a fenyegetések rávilágítanak a kiberbiztonság létfontosságú szerepére az egyre inkább digitálissá váló gazdaságokban és társadalmakban. A [fenyegetettségi helyzetről szóló 2025. évi jelentésében](#) az ENISA a zsarolóvírusokat határozta meg az Unió legkritikusabb fenyegetéseként. Az érintett ágazatokat a [2. ábra](#) mutatja be.

³ Az ENISA 2024. évi jelentése az uniós kiberbiztonsági helyzetről.

2. ábra | A kibertámadások által érintett ágazatok



Forrás: Európai Számvevőszék, az ENISA tájékoztatása alapján.

Jelentős és nagyszabású kiberbiztonsági események

03 A kiberbiztonsági incidensek, amelyek kiberfenyegetéseket és nem szándékos (például a [3. ábrán](#) és a [40.](#) bekezdésben említett) eseményeket foglalnak magukban, „megakadályozhatják a közszolgáltatások nyújtását [és] a gazdasági tevékenységek folytatását, [...] jelentős pénzügyi veszteségeket okozhatnak, alááshatják a felhasználói bizalmat, jelentős károkat okozhatnak az uniós gazdaságnak és az Unió demokratikus rendszereinek, sőt egészségügyi vagy az emberi életet veszélyeztető következményekkel is járhatnak”⁴. Egy kiberbiztonsági incidens lehet⁵:

- **jelentős**, ha súlyos működési zavart okozott vagy okozhatott a szolgáltatásokban, ha pénzügyi veszteséget okozott vagy okozhatott az érintett szervezetnek, illetve ha jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett vagy érinthetett;
- **nagyszabású**, ha olyan mértékű zavart okozott, amely meghaladja a tagállam reakálási képességét, vagy amely jelentős mértékben érint legalább két tagállamot.

04 Egy nagyszabású kiberbiztonsági incidens teljes körű **uniós kiberbiztonsági válsággá** eszkalálódhat, ha megakadályozza a belső piac megfelelő működését, illetve ha több tagállamban vagy az Unió egészében súlyos közbiztonsági és védelmi kockázatot jelent a szervezetekre vagy a polgárokra nézve⁶.

⁴ Az (EU) 2025/38 rendelet (a [kiberszolidaritásról szóló rendelet](#)) (2) preambulumbekkezdése.

⁵ A [NIS 2 irányelv](#) 6. és 23. cikke, amelyeket az (EU) 2024/2690 bizottsági végrehajtási rendelet tovább részletez a digitálisinfrastruktúra-ágazatban működő számos szolgáltató tekintetében.

⁶ A [NIS 2 irányelv](#) (69) preambulumbekkezdése.

Uniós szakpolitikai keret

- 05** Az Unió összetett és többretegű kiberbiztonsági ökoszisztémája számos belpolitikai területen átível, így felöleli többek között a bel- és igazságügy, a digitális egységes piac és a kutatási politika területét is⁷. A külpolitikában a kiberbiztonság szervesen beépül a diplomáciába, és egyre fontosabb részét képezi az Unió kialakulóban lévő védelmi politikájának⁸.
- 06** Az elmúlt években az Unió megerősítette kiberbiztonsági szabályozási keretét. Az alábbi **3. ábra** a legrelevánsabb uniós szintű jogszabályokat és szakpolitikai eszközöket mutatja be. Ellenőrzésünk hatókörével összhangban (lásd: **13–14.** bekezdés) elsősorban a jelentős és nagyszabású kiberbiztonsági incidensek észlelésével és az azokra való reagálással foglalkozó eszközökre összpontosítottunk.

⁷ A Számvevőszék tájékoztatója az eredményes uniós kiberbiztonsági politika előtt álló kihívásokról, 12. o.

⁸ Például az Európai Unió kiberbiztonsági helyzete (2022), a hibrid hadjáratokra való koordinált uniós reagálásra vonatkozó keret (2022), az uniós kibervédelmi politika (2023) és a felülvizsgált kiberdiplomáciai eszköztár (2023).

3. ábra | A vonatkozó uniós jogszabályok és szakpolitikai eszközök

- Jogszabályok és szakpolitikai eszközök elfogadása
- Hálózatok és struktúrák létrehozása



Forrás: Európai Számvevőszék.

Feladat- és felelősségi körök

- 07** Az Európai Unió kiberbiztonsági környezete számos magán- és közszervezetet foglal magában regionális, nemzeti és uniós szinten a polgári szférából, köztük bűnüldöző szerveket is. A kiberbiztonság a nemzetbiztonságnak és nemzetvédelemnek is kulcsfontosságú alkotóeleme⁹. A jelenlegi uniós környezetet a [II. melléklet](#) szemlélteti.
- 08** Elsődlegesen a tagállamok felelősek az őket érintő kiberbiztonsági események és válságok megelőzéséért, az azokra való felkészülésért és reagálásért. Az [Európai Unióról szóló szerződés 4. cikkének \(2\) bekezdésével](#) összhangban a nemzeti szintű biztonság az egyes tagállamok kizárólagos felelőssége marad. Mivel a kiberbiztonsági incidensek a belső piac zökkenőmentes működéséhez szükséges kritikus információs infrastruktúrát is megzavarhatják és károsíthatják, jelentős incidensek vagy válságok fellépése esetén az Unió is fontos szerepet játszik azok elhárításában¹⁰. Az uniós szinten legjelentősebb szervezeteket az alábbi [4. ábra](#) mutatja be.

⁹ 02/2023. sz. vélemény a kiberbiztonsági szolidaritásról szóló rendeletre irányuló javaslatról.

¹⁰ A kiberbiztonsági válságkezelésre vonatkozó uniós terv.

4. ábra | A kiberbiztonságban meghatározó szerepet játszó uniós szintű szervezetek



Forrás: Európai Számvevőszék.

Unió finanszírozás

- 09** A jelenlegi, 2021–2027-es többéves pénzügyi keretben a kiberbiztonság finanszírozásának fő forrása a [Digitális Európa \(DIGITAL\) program](#). Ez a 2021-ben indított, összesen 8,1 milliárd eurós költségvetéssel rendelkező uniós program az első olyan program, amelynek célja kifejezetten az Unió digitális átalakulásának előmozdítása¹¹.
- 10** A DIGITAL program forrásai a 3. egyedi célkitűzés („Kiberbiztonság és bizalom”) keretében kiberbiztonsági intézkedéseket finanszíroznak. Egészen pontosan 1,4 milliárd eurós keretösszeg áll rendelkezésre a következőkre:
- a tagállami eszközök és adatinfrastruktúrák közötti kiberbiztonsági koordináció megerősítése;
 - a kiberbiztonsági megoldások széles körű bevezetésének támogatása a gazdaságban.
- 11** A DIGITAL programból a kiberbiztonságra irányuló finanszírozás nagy részét pályázati felhívások útján biztosítják: 2021 novembere és 2025 decembere között összesen 12 pályázati felhívást tettek közzé. E felhívások keretében összesen 825 millió euró finanszírozás állt rendelkezésre. 2026-ra és 2027-re új pályázati felhívásokat terveznek, amelyek keretében további 212 millió euró összegű vissza nem térítendő támogatást ítélnék oda.
- 12** A kiberbiztonságot egy másik fontos uniós program, a [Horizont Európa](#) is támogatja. A kiberbiztonsági projekteket főként a [3. klaszter](#) („A társadalmat szolgáló polgári biztonság”) keretében finanszírozzák. Ezek a kiforrottságot tekintve általában korai szakaszban vannak, mivel a Horizont Európa a kutatásra és az innovációra összpontosít. A [Helyreállítási és Rezilienciaépítési Eszköz](#) szintén biztosít finanszírozást a kiberbiztonsági intézkedésekhez.

¹¹ [Digitális Európa program](#).

Az ellenőrzés hatóköre és módszere

13 A kiberfenyegetések egyre nagyobb száma és azok lehetséges hatásai világossá tették, hogy meg kell erősítenünk a kibertámadásokkal szembeni kollektív ellenálló képességünket. Ellenőrzésünk célja annak értékelése volt, hogy az uniós fellépések eredményesen segítik-e elő a jelentős és nagyszabású kiberbiztonsági incidensek észlelését és az azokra való reagálást. Elsősorban a következők esetében értékeltük, hogy ez így volt-e:

- uniós szintű hálózatok és mechanizmusok (nevezetesen a CSIRT-hálózat, az EU-CyCLONe, az európai kiberbiztonsági figyelmeztető rendszer, a kiberbiztonsági helyzetelemző központ és az uniós kiberbiztonsági tartalék);
- a Digitális Európai (DIGITAL) program keretében finanszírozott intézkedések.

Ellenőrzésünk nem vizsgálta az uniós szintű bűnüldözési együttműködést, sem pedig a diplomáciai intézkedések, illetve védelmi tevékenységek révén uniós szinten végrehajtott kibereklrettentési intézkedéseket.

14 Ellenőrzésünk a 2022 és 2025 közötti időszakra terjedt ki. Munkánk a vonatkozó dokumentumok vizsgálatán és elemzésén, három tagállamban (Írországban, Görögországban és Olaszországban) tett ellenőrző látogatásokon, valamint írásbeli kérdőíveken és az érintett érdekelt felekkel folytatott interjúkon alapul. Az [5. ábra](#) bemutatja, hogyan szereztük be bizonyítékainkat észrevételeink megtételéhez.

5. ábra | Az elvégzett ellenőrzési munka

A következőket vizsgáltuk meg:

- A jelentős és nagyszabású kiberbiztonsági események észlelésére és az azokra való reagálásra alkalmazandó **jogi keret**
- Az uniós szinten létrehozott hálózatok és struktúrák **feladat- és felelősségi körei**

A következőket elemeztük:

- A **CSIRT-hálózat** és az **EU-CyCLONe** működésére vonatkozó dokumentumok
 - A **DIGITAL program programozásának és teljesítménymonitoring-keretének** dokumentációja
 - **13 kiválasztott uniós finanszírozású fellépés** dokumentációja (11 vissza nem térítendő támogatás és 2 szerződés – részletesen lásd: a III. melléklet listája)
- * Abban a három országban (Írország, Görögország és Olaszország) választottunk ki uniós finanszírozású intézkedéseket, ahol a vonatkozó DIGITAL-finanszírozás a legjelentősebb volt. A 11 vissza nem térítendő támogatás a fenyegetések észlelése és az azokra való reagálás szempontjából releváns 137 uniós finanszírozású projekt listájáról származott, és igyekeztünk minél többféle projektet kiválasztani.

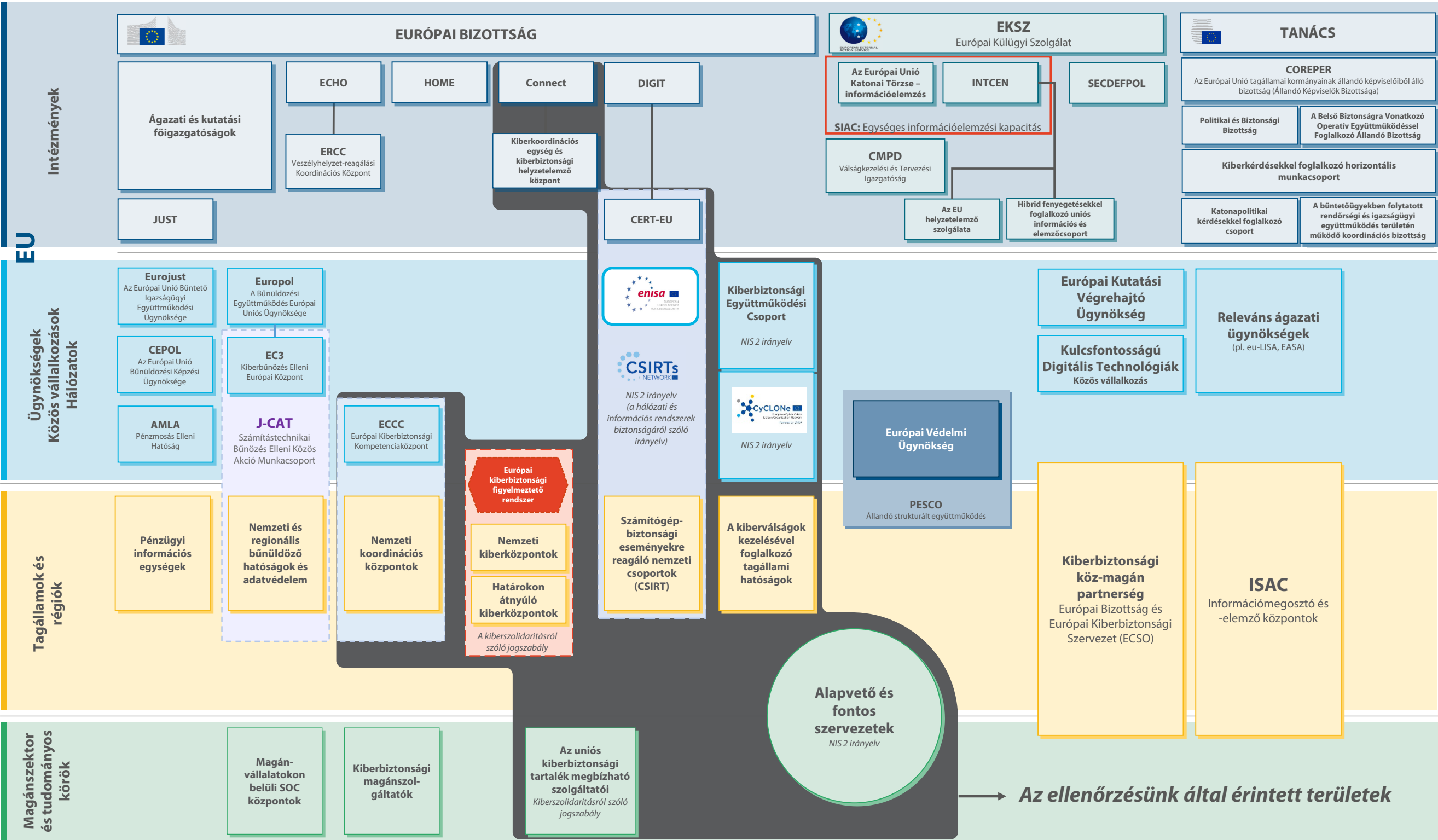
Interjút készítettünk a következőkkel:

- A **mintánkban szereplő 11 uniós finanszírozású, vissza nem térítendő támogatás** kedvezményezettjei
- **Három tagállam** (Írország, Görögország és Olaszország) nemzeti kiberbiztonsági hatóságainak képviselői
- Az Európai Bizottság (**DG Connect**), az **ENISA** és az **ECCC** képviselői

Forrás: Európai Számvevőszék.

- 15** Reményeink szerint megállapításaink hozzájárulnak a jelentős és nagyszabású kiberbiztonsági események uniós észlelése és az azokra való reagálás eredményességének és hatékonyságának javításához, valamint az uniós finanszírozású intézkedések jobb kiválasztásához és nyomon követéséhez. [Ellenőrzési módszertanunk](#) megfelel a [Legfőbb Ellenőrző Intézmények Nemzetközi Szervezete \(INTOSAI\)](#) által kiadott nemzetközi könyvvizsgálati standardoknak.

II. melléklet. Az Európai Unió kiberbiztonsági környezete



DG Connect: A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága
DG ECHO: Az Európai Polgári Védelem és Humanitárius Segítségnyújtási Műveletek Főigazgatósága

DG HOME: Migrációügyi és Uniók Belügyi Főigazgatóság
DG JUST: Jogérvényesítési és Fogasztópolitikai Főigazgatóság
DIGIT: Digitális Szolgáltatások Főigazgatósága
EASA: Az Európai Unió Repülésbiztonsági Ügynöksége

EU-CyCLONE: az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata
eu-LISA: A Szabadságon, A Biztonságon És A Jog Érvényesülésén Alapuló Téréség Nagyméretű IT-Rendszereinek Üzemeltetési Igazgatását Végző Európai Uniók Ügynökség

INTCEN: Az Európai Unió Helyzetelemző Központja
SECDEFPOL: Biztonság- és Védelempolitika
SOC: Biztonsági műveleti központ

III. melléklet. Kiválasztott kiberbiztonsági fellépések

Azonosító	Cím	Országok	Kezdő dátum	Záró dátum	Teljes költség (millió euró) és uniós hozzájárulás (%)	Hivatkozás az uniós finanszírozási és pályázati portálra
Vissza nem térítendő támogatások az európai kiberbiztonsági figyelmeztető rendszer részét képező, határokon átnyúló kiberközpontok számára						
1	Határokon átnyúló biztonsági műveleti központok létrehozása (ATHENA)	Bulgária, Görögország, Ciprus, Málta	2024.01.01.	2028.03.31.	4,7 (50%)	
2	ENSOC HATÁROKON ÁTNYÚLÓ PLATFORM (ENSOC)	Spanyolország, Olaszország, Luxemburg, Hollandia, Ausztria, Portugália, Románia	2024.01.01.	2028.06.30.	10,4 (50%)	
A nemzeti koordinációs központok (NCC) hálózatának tagállami kiépítéséhez nyújtott vissza nem térítendő támogatások						
3	Az írországi Nemzeti Kiberbiztonsági Koordinációs és Fejlesztési Központ (NCC-IE) fejlesztése és megvalósítása	Írország	2023.10.02.	2026.10.01.	4,2 (47%)	
4	Olasz Nemzeti Koordinációs Központ (NCC-IT)	Olaszország	2023.11.01.	2025.10.31.	2,0 (50%)	

Azonosító	Cím	Országok	Kezdő dátum	Záró dátum	Teljes költség (millió euró) és uniós hozzájárulás (%)	Hivatkozás az uniós finanszírozási és pályázati portálra
Vissza nem térítendő támogatások a biztonsági műveleti központok (SOC) kapacitásának kiépítéséhez, e központok számára a mesterséges intelligencia és más alaptechnológiák új alkalmazásainak előmozdításához, valamint felkészültségi támogatás és kölcsönös segítségnyújtás biztosításához						
5	A Görög Egységes Biztonsági Műveleti Központ (EL-SOC) kapacitásának növelése	Görögország, Ciprus	2024.01.01.	2026.12.31.	9,7 (50%)	
6	Görög Kis- és Középvállalkozások Biztonsági Műveleti Központja (GR-SME-SOC)	Görögország	2024.01.01.	2026.12.31.	12,1 (50%)	
7	Új generációs biztonsági műveleti központok (NG-SOC)	Görögország, Spanyolország, Ciprus, Luxemburg, Szlovénia, Norvégia	2024.01.01.	2026.12.31.	4,8 (50%)	
8	Ír Helyi Önkormányzatok Biztonsági Műveleti Központja (ILG-SOC)	Írország	2023.10.01.	2026.09.30.	8,3 (50%)	
9	A kiberbiztonsági koordinációs és reagálási hálózatok összekapcsolt rendszere (Cyber-CORE-hálózat)	Írország	2024.01.01.	2026.12.31.	3,6 (50%)	
10	Az emberek, folyamatok és technológiák harmonizálása a szilárd kiberbiztonság érdekében (CYberSynchrony)	Belgium, Görögország, Olaszország, Ciprus, Hollandia	2024.06.01.	2027.05.31.	7,0 (100%)	
11	Fejlett együttműködési biztonsági műveleti központok (ACSOC)	Görögország, Olaszország, Románia	2025.01.01.	2027.12.31.	3,0 (50%)	

Azonosító	Cím	Országok	Kezdő dátum	Záró dátum	Teljes költség (millió euró) és uniós hozzájárulás (%)	Hivatkozás az uniós finanszírozási és pályázati portálra
Keretszerződés az ENISA kiberbiztonsági támogatási fellépéséhez						
12	Az ENISA támogatása a kiberbiztonsági támogatási fellépés keretében történő szolgáltatásnyújtásban (28 tétel)	27 tagállami tétel 1 páneurópai tétel	2022.12.01 ¹	2025.12.31.	28,3 (100%)	
Szolgáltatási szerződés a Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatóságának kiberbiztonsági helyzetelemző központja számára						
13	Egyedi szolgáltatás az Európai Bizottság kiberbiztonsági helyzetelemző központjának támogatására	-	2022.12.30.	2026.12.30.	18,0 (100%)	

Forrás: Európai Számvevőszék.

¹ 2022 decemberében több szerződést írtak alá.

IV. melléklet. Az uniós finanszírozású kiberbiztonsági projektek számvevőszéki értékelése

Azonosító	Projekt				
		A projekt a felhívásban meghatározott igények többségét kielégíti	A projekt elérte eddig tervezett outputjait és eredményeit	A projektoutputok határidőre megvalósultak	A projekt teljesítménymutatói relevánsak és mérhetők, továbbá rendelkeznek alap- és céltétellel
		Kielégítő	Nem kielégítő	Vannak hiányosságok	Nem lehet (túl korai) következtetést levonni
1	Határokon átnyúló biztonsági műveleti központok létrehozása (ATHENA)				
2	ENSOC HATÁROKON ÁTNYÚLÓ PLATFORM (ENSOC)				
3	Az írországi Nemzeti Kiberbiztonsági Koordinációs és Fejlesztési Központ (NCC-IE) fejlesztése és megvalósítása				
4	Olasz Nemzeti Koordinációs Központ (NCC-IT)				
5	A Görög Egységes Biztonsági Műveleti Központ (EL-SOC) kapacitásának növelése				
6	Görög Kis- és Középvállalkozások Biztonsági Műveleti Központja (GR-SME-SOC)				
7	Új generációs biztonsági műveleti központok (NG-SOC)				
8	Ír Helyi Önkormányzatok Biztonsági Műveleti Központja (ILG-SOC)				
9	A kiberbiztonsági koordinációs és reagálási hálózatok összekapcsolt rendszere (Cyber-CORE-hálózat)				
10	Az emberek, folyamatok és technológiák harmonizálása a szilárd kiberbiztonság érdekében (CYberSynchrony)				
11	Fejlett együttműködési biztonsági műveleti központok (ACSOC)				

Rövidítések

Rövidítés	Meghatározás/Magyarázat
CSIRT	Számítógép-biztonsági incidensekre reagáló csoport
DG Connect	A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága
DIGITAL	Digitális Európa program
ECCC	Európai Kiberbiztonsági Kompetenciaközpont
ENISA	Európai Unió Kiberbiztonsági Ügynökség
EU-CyCLONe	Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata
FSTP	Harmadik feleknek nyújtott pénzügyi támogatás
Kkv	Kis- és középvállalkozás
NCC	Nemzeti koordinációs központ
NIS	Hálózat- és információbiztonság
OCA	A tulajdonosi szerkezetre és az ellenőrzésre vonatkozó értékelés
SAG	Stratégiai tanácsadó csoport
SOC	Biztonsági műveleti központ

Glosszárium

Terminus	Meghatározás/Magyarázat
Biztonsági műveleti központ	Kiberbiztonsági fenyegetések és események megelőzésével, valamint kapcsolódó hírszerzési információk gyűjtésével foglalkozó szervezeti egység.
Fenyegető szereplő	Olyan egyének vagy csoportok, akik az informatikai rendszerek, hálózatok és eszközök sebezhetőségeit kihasználva szándékosan kárt vagy zavart okoznak, illetve adatokat lopnak el.
Jelentős kiberbiztonsági incidens	Olyan kiberbiztonsági esemény, amely valamely szervezet számára súlyos zavart vagy pénzügyi veszteséget, illetve más jogalanyok vagy egyének számára jelentős kárt okozott vagy okozhat.
Kiberbiztonsági incidens	Adatok vagy számítógépes rendszerek elérhetőségének, valódiságának, integritásának vagy bizalmas jellegének károsításával járó esemény.
Kiberfenyegetés	A kibertér olyan potenciális felhasználása, amely adatok vagy számítógépes rendszerek elérhetőségének, valódiságának, integritásának vagy bizalmas jellegének károsításához vezet.
Kiberközpont	Különböző szolgáltatásokat, eszközöket és informatikai szakembereket összefogó központi platform, amelynek célja a kiberfenyegetések nyomon követésének, észlelésének és elemzésének javítása, a kiberbiztonsági incidensek megelőzése és a kiberfenyegetésekkel kapcsolatos hírszerzési információk előállításának támogatása.
Nagyszabású kiberbiztonsági esemény	Olyan kiberbiztonsági esemény, amelynek kezelése súlyosságánál fogva meghaladja egyetlen tagállam kapacitását, vagy amely legalább két tagállamra jelentős hatást gyakorol.
Taxonómia	A kiberbiztonsággal összefüggésben az alapfogalmakkal, például a fenyegetésekkel és a biztonsági eseményekkel kapcsolatos ismeretek rendszerezésére, kategorizálására és strukturálására használt osztályozási rendszer.
Zsarolóprogram	Rosszindulatú szoftver, amely megtagadja az áldozatokról a számítógépes rendszerhez való hozzáférést, vagy a fájlokat titkosítja és olvashatatlanná teszi általában azért, hogy az áldozat kénytelen legyen váltságdíjat fizetni a hozzáférés helyreállításáért.

A Bizottság válaszai

<https://www.eca.europa.eu/hu/publications/SR-2026–19>

Az Európai Kiberbiztonsági Kompetenciaközpont (ECCC) válaszai

<https://www.eca.europa.eu/hu/publications/SR-2026–19>

Az Európai Unió Kiberbiztonsági Ügynökség (ENISA) válaszai

<https://www.eca.europa.eu/hu/publications/SR-2026–19>

Időrendi áttekintés

<https://www.eca.europa.eu/hu/publications/SR-2026–19>

Ellenőrző csoport

Az Európai Számvevőszék különjelentései ismertetik az uniós szakpolitikákra és programokra, illetve az egyes költségvetési területek irányításával kapcsolatos témákra vonatkozó ellenőrzéseinek eredményeit. Hogy ellenőrzési munkája maximális hatást érjen el, témái megválasztásakor és feladatai megtervezésekor a Számvevőszék figyelembe veszi a teljesítmény-, illetve megfelelőségi kockázatokat, az érintett bevétel vagy kiadás nagyságát, a várható fejleményeket, valamint a politikai jelentőséget és a nagyközönség érdeklődését.

Ezt a teljesítmény-ellenőrzést a külső fellépések, biztonságpolitika és jogérvényesülés kiadási területeiért felelős, George-Marius Hyzler számvevőszéki tag elnökölte III. Kamara végezte. Az ellenőrzést George-Marius Hyzler számvevőszéki tag vezette Romuald Kayibanda kabinetfőnök és Annette Farrugia kabinetattasé, Cyril Messein ügyvezető, Frédéric Soblet feladatfelelős, valamint Jurgen Manjé és Flavia Di Marco számvevők támogatásával. Nyelvi támogatás: Zoe Amador Martínez. Grafika: Dunja Weibel.



Balról jobbra: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

SZERZŐI JOGOK

© Európai Unió, 2026

Az Európai Számvevőszék dokumentumainak felhasználását a nyíltadat-politikáról és a dokumentumok további felhasználásáról szóló [6–2019. sz. számvevőszéki határozat](#) szabályozza.

Ellenkező rendelkezés (pl. egyedi szerzői jogi nyilatkozatokban foglaltak) hiányában az Európai Unió tulajdonában lévő számvevőszéki tartalmak a [Creative Commons Attribution 4.0 International \(CC BY 4.0\) licenc](#) alá tartoznak. Ezért főszabály szerint a további felhasználás a forrás és a változtatások megfelelő feltüntetésével megengedett.

A Számvevőszéktől származó tartalmak további felhasználásakor azok eredeti értelme és mondanivalója nem torzulhat. A Számvevőszék nem vonható felelősségre a továbbfelhasználás esetleges következményeiért.

Ha az adott tartalomban azonosítható magánszemélyek is érintettek (például ha egy kép a Számvevőszék munkatársait ábrázolja vagy harmadik fél is szerepel a források között), adott esetben további engedélyt is be kell szerezni.

Amennyiben ez megtörtént, akkor a vonatkozó engedély érvényteleníti a fenti általános érvényű engedélyt, és az abban foglalt, egyértelműen meghatározott felhasználási korlátozások érvényesek.

Az olyan tartalmak felhasználásához vagy reprodukálásához, amelyek nem az Európai Unió tulajdonát képezik, adott esetben közvetlenül a szerzői jog tulajdonosától kell engedélyt kérni.

Borítófotó: © 4AXY – stock.adobe.com.

6. és 8. ábra, ikonok: Az ábrák kidolgozása a [Flaticon.com](#) eszközeinek felhasználásával történt. © Freepik Company S.L. Minden jog fenntartva.

5. ábra, térkép: [Eurostat](#).

Az iparjogvédelem alatt álló szoftverek és dokumentumok – pl. szabadalmak, márkajelzések, bejegyzett formatervezési minták, logók és nevek – nem tartoznak a Számvevőszék továbbfelhasználási politikájának hatókörébe.

Az Európai Uniónak az europa.eu címtartomány alá tartozó intézményi weboldalai külső oldalakra mutató hivatkozásokat is tartalmaznak. Ezek nem tartoznak a Számvevőszék hatáskörébe, ezért ajánlott elolvasni az ott közzétett adatvédelmi és szerzői jogi rendelkezéseket.

Az Európai Számvevőszék logójának használata

Az Európai Számvevőszék logója kizárólag a Számvevőszék előzetes hozzájárulásával használható fel.

HTML	ISBN 978-92-849-7873-1	ISSN 1977-5733	doi:10.2865/6823757	QJ-01-26-032-HU-Q
PDF	ISBN 978-92-849-7874-8	ISSN 1977-5733	doi:10.2865/3508609	QJ-01-26-032-HU-N

IDÉZÉS MÓDJA

Az Európai Számvevőszék [19/2026. sz. különjelentése](#): „A kiberbiztonsági incidensek észlelése és az azokra való reagálás: Az uniós együttműködési keret kidolgozása jól halad, de a végrehajtás késedelmei és az elégtelen információmegosztás miatt még csak részben eredményes”, az Európai Unió Kiadóhivatala, 2026.

A kiberbiztonsági incidensek kezelése céljából az Unió az elmúlt években megerősítette kiberbiztonsági szabályozási keretét, valamint hálózatokat és mechanizmusokat hozott létre. Az Unió a Digitális Európa program keretében is támogat kiberbiztonsági projekteket.

Arra a következtetésre jutottunk, hogy az uniós intézkedések csak részben könnyítik meg a jelentős és nagyszabású kiberbiztonsági incidensek észlelését és az azokra való reagálást. Bár fokozatosan létrejött az együttműködési keret, a teljes rendszer felépítésére irányuló munka még jelenleg is folyik. Az elégtelen információmegosztás, az adatszolgáltatással kapcsolatos hiányosságok és a jelentős végrehajtási késedelmek miatt az uniós hálózatokban és mechanizmusokban rejlő lehetőségek nem használhatók ki teljes mértékben. A projektek által kitűzött célok relevánsak, de közülük több is működési nehézségekkel és késedelmekkel küzd. Emellett az átfogó teljesítménymonitoring-keretben is vannak hiányosságok. Mindezek kezelésére ajánlásokat terjesztettünk elő.

A Számvevőszék különjelentése az EUMSZ 287. cikke (4) bekezdésének második albekezdése alapján.



EURÓPAI
SZÁMVEVŐSZÉK



Az Európai Unió
Kiadóhivatala

EURÓPAI SZÁMVEVŐSZÉK
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Telefon: +352 4398-1

Megkeresés: eca.europa.eu/hu/contact
Weboldal: eca.europa.eu
Közösségi média: @EUauditors