

TERMÉKLAP

Az európai kiberbiztonsági technológiák, kapacitások és felkészültség megerősítése

Digital Europe Programme (DIGITAL)

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-DUALUSE | 2026. 09. 10.



INTENZITÁS

max. 50%



ELŐLEG

max. 80%

DÖNTÉSI ÖSSZEFOGLALÓ



Ez a felhívás olyan polgári-védelmi kiberbiztonsági együttműködéseket céloz, amelyek kettős felhasználású prototípusokat, piacra kész termékeket vagy operatív infrastruktúrákat fejlesztenek. Az EUR 10 milliós témaköltségvetés, az 50%-os támogatási arány, a 2027. január 14-i határidő és az indikatív EUR 3-5 milliós igényelhető tartomány konkrét, ágazatokon átívelő rendszereket megvalósító projekteket támogat. A jogosultságra a jelenlegi munkaprogramban alkalmazott, a 12. cikk (5) bekezdése szerinti kettős felhasználású korlátozás vonatkozik: tagállamban történő letelepedés vagy letelepedettnak tekintés, valamint tagállami vagy tagállami állampolgári ellenőrzés.

FIGYELMEZTETÉSEK



A 12. cikk (5) bekezdése lényeges jogosultsági/ellenőrzési feltétel: bár a felhívás adatlapja az EU-tagállamokat és az EGT-országokat sorolja fel, a felhívás hivatkozik a 12. cikk (5) bekezdésére, és a jelenlegi kettős felhasználású munkaprogram tagállami letelepedési/ellenőrzési korlátozást alkalmaz; ezért e témára a korlátozott tagállami szabály az irányadó. A tevékenységeknek, beleértve az alvállalkozásba adott munkát is, jogosult országokban kell megvalósulniuk, és tulajdonosi-ellenőrzési nyilatkozatok szükségesek. A projektenként kért EUR 3-5 milliós tartomány elvárt, nem pedig szigorú felső határ. A téma költségvetése EUR 10 millió, a benyújtási határidő pedig 2027. január 14., 17:00 CET.



BENYÚJTÁS KEZDETE

2026-09-01



BENYÚJTÁSI HATÁRIDŐ

2027-01-14 17:00:00+01:00



Részletes cél

Kettős felhasználású működő prototípusok, piacra kész termékek és a polgári, valamint védelmi környezetben egyaránt releváns kiberbiztonsági technológiákhoz, alkalmazásokhoz és eszközökhöz kapcsolódó operatív infrastruktúrák fejlesztése.

Kettős felhasználású kiberbiztonsági technológiák és alkalmazások, amelyek kiterjednek a kvantumbiztos kriptográfiára, a Zero Trust Architectures megoldásokra, a mesterséges intelligencia által vezérelt fenyegetésészlelésre és -elhárításra, kiber gyakorlóterekre/digitális ikrekre, SOAR-ra, a kritikus infrastruktúrák védelmére, a biztonságos kommunikációra, a hibrid fenyegetések kezelésére és a közbiztonsági alkalmazásokra.



Jogosult pályázói kör

Jogi személyek; a célzott érintettek közé tartoznak az ipari szereplők, a védelmi minisztériumok és ügynökségek, a belügyminisztériumok, a kkv-k, a start-upok, valamint a polgári és védelmi kiberbiztonsági szférában működő egyéb releváns szereplők.



TERÜLETI KORLÁTOZÁS

A projekttevékenységeknek, beleértve az alvállalkozásba adott munkát is, jogosult országokban kell megvalósulniuk.



KIZÁRÓ OKOK

Nem vehetnek részt azon pályázók, akikre uniós kizárási határozat vonatkozik, vagy akik olyan kizárási helyzetek hatálya alá tartoznak, mint a fizetéseképtelenség, társadalombiztosítási vagy adójogi kötelezettségek megsértése, súlyos szakmai köteleességszegés, csalás, korrupció, bűnszervezethez fűződő kapcsolat, pénzmosás, terrorizmussal kapcsolatos bűncselekmények, gyermekmunka vagy emberkereskedelem.



Támogatás és pénzügyek



ÁLTALÁNOS INTENZITÁS

50%

ELŐLEG MÉRTÉKE

Általában a maximális támogatási összeg 80%-a; kivételesen kevesebb előfinanszírozás vagy előfinanszírozás nélkül.



VÁRHATÓ HATÁS ÉS EREDMÉNYEK

A várt eredmények közé tartozik a biztonságos polgári-katonai adatmegosztás, a kiber- és hibrid fenyegetésekre vonatkozó európai szintű korai előrejelzés, a közös polgári/katonai képzés, az ágazatok közötti integrált fenyegetésészlelés, a kettős felhasználású technológiák harmonizált szabványai és az érintettek együttműködése.



Támogatható tevékenységek

- Kettős felhasználású működő prototípusok fejlesztése.
- Polgári és védelmi környezetben releváns, piacra kész kiberbiztonsági termékek fejlesztése.
- Kiberbiztonsági technológiákhoz, alkalmazásokhoz és eszközökhöz kapcsolódó operatív infrastruktúrák fejlesztése.
- Kvantumszámításon alapuló támadásokkal szemben ellenálló, kvantumbiztos titkosítási módszerek fejlesztése.
- Zero Trust Architecture keretrendszerek alkalmazása a végpontbiztonság növelése és a jogosulatlan hozzáférés megelőzése érdekében.
- MI-eszközök alkalmazása valós idejű fenyegetésészlelésre, -méréselésre és -elhárításra.
- Kiber gyakorlóterek és digitálisiker-technológia használata polgári és katonai rendszerek, valamint hálózatok elleni kibertámadások szimulálására.
- Security Orchestration, Automation, and Response (SOAR) platformok fejlesztése az incidenskezelés egyszerűsítése érdekében.
- Kettős felhasználású technológiák alkalmazása a kritikus infrastruktúrák védelméhez, a biztonságos kommunikációhoz, a hibrid fenyegetések kezeléséhez, valamint a digitális csalás és digitális erőszak közbiztonsági célú megelőzéséhez.



Kötelező tevékenységek

Az ECCC kérésére részvétel klaszterezési tevékenységekben a közös fellépések meghatározása, valamint a polgári és védelmi közösségek közötti szinergiák fokozása érdekében.



Elszámolható költségtípusok

- Személyi jellegű költségek
- Alvállalkozói költségek
- Utazási és megélhetési költségek
- Berendezések költségei
- Egyéb áruk, építési munkák és szolgáltatások



Ütemezés



KEZDÉS

Egyedi kezdési szabály

A projekt kezdőnapját a támogatási megállapodás rögzíti; rendszerint a támogatási megállapodás aláírását követő időpont, azonban kellően indokolt esetben kivételesen visszamenőleges időpont is lehetséges, de nem korábbi, mint a pályázat benyújtása.

A tevékenység indikativ időtartama 36 hónap; más időtartamok sincsenek kizárva.



Kötelező dokumentumok

- A pályázati űrlap A része
- A pályázati űrlap B része
- Tulajdonosi és ellenőrzési nyilatkozatok, beleértve a kapcsolódó partnerekre és az alvállalkozókra vonatkozókat is



FONTOS

A terméklap tájékoztató jellegű összefoglaló. A támogatási kérelem előkészítése előtt a hatályos felhívás, az ÁÚF és a kapcsolódó szakmai mellékletek teljes körű ellenőrzése szükséges.