

TERMÉKLAP

MI-re épülő kiberbiztonságos eszközök, technológiák és szolgáltatások

Digital Europe Programme (DIGITAL)

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



INTENZITÁS

max. 50%



ELŐLEG

max. 80%

DÖNTÉSI ÖSSZEFOGLALÓ



Ez a felhívás olyan technológiai szolgáltatók, Cyber Hub-üzemeltetők, közintézmények és NIS 2 szervezetek, kiberbiztonsági szervezetek, akadémiai szereplők és más érdekelt felek számára megfelelő, amelyek MI-alapú kiberbiztonsági eszközöket fejlesztenek vagy alkalmaznak. A téma olyan MI-alapú kiberbiztonsági alkalmazásokra vonatkozik, amelyek tevékenységeinek a felsorolt operatív felhasználási esetek közül legalább egyet magukban kell foglalniuk. A téma költségvetése 15 millió EUR, a támogatási arány 50%; a felhívás 2026. szeptember 1-jétől 2027. január 14-én 17:00 CET-ig nyitott, az EU-/EGT-beli letelepedési, tulajdonosi/ellenőrzési és biztonsági követelmények függvényében.

FIGYELMEZTETÉSEK



Döntés szempontjából kritikus feltételek: a felhívás 2027. január 14-én 17:00 CET-ig nyitott; a szervezeteknek jogosult országokban kell letelepedettnek lenniük, és onnan kell ellenőrzés alatt állniuk; a 12. cikk (5) bekezdése szerinti biztonsági korlátozások alkalmazandók, a minősített információkra vonatkozó feltételes FSC-követelményekkel; a 36 hónapos időtartam indikatív, és más időtartamok nincsenek kizárva.



BENYÚJTÁS KEZDETE

2026-09-01



BENYÚJTÁSI HATÁRIDŐ

2027-01-14T17:00:00+01:00



Részletes cél

A téma az MI-alapú technológiákkal, beleértve a GenAI-t is, foglalkozik a nemzeti és illetékes hatóságok, Cyber Hubok, CSIRT-ek, közintézmények és NIS 2 szervezetek számára; továbbá foglalkozik az MI-megoldások biztonságával, robusztusságával és megbízhatóságával, valamint az AI Actnek, a szellemi tulajdonjogoknak és a GDPR-nak való megfeleléssel.

Az intézkedéseknek olyan MI-alapú kiberbiztonsági rendszereket és eszközöket kell fejleszteniük és alkalmazniuk, amelyek kiterjednek a fenyegetések és sérülékenységek észlelésére, a fenyegetések mérséklésére, az önhelyreállító incidenshelyreállításra, az adatelemzésre és az adatmegosztásra; a javasolt MI-megoldásoknak kiberbiztonságosaknak is kell lenniük.



Jogosult pályázói kör

Jogi személyek (köz- vagy magánszervezetek).



TERÜLETI KORLÁTOZÁS

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



Támogatás és pénzügyek



ÁLTALÁNOS INTENZITÁS

50%

Egyszerű támogatások.

ELŐLEG MÉRTÉKE

Rendes esetben a maximális támogatási összeg 80%-a előfinanszírozási rendelkezésre álló összegként; kivételesen alacsonyabb összegű vagy előfinanszírozás nélküli eset is lehetséges.



VÁRHATÓ HATÁS ÉS EREDMÉNYEK

MI-alapú technológiák alkalmazása Cyber Hubok, CSIRT-ek, NCSC-k, NIS SPOC-ok és mások számára; validált MI-alapú kiberbiztonsági eszközök; fokozott információmegosztás; a CTI-folyamatok automatizálása; az uniós jogszabályoknak megfelelő biztonságos MI-megoldások; valamint hozzájárulás a szabványosításhoz és tanúsításhoz.



Támogatható tevékenységek

- Mintázatok folyamatos észlelése és olyan anomáliák azonosítása, amelyek az IKT- vagy operatív technológiai infrastruktúrákban kialakuló fenyegetésekre és új támadási vektorokra utalhatnak.
- Újszerű fenyegetésészlelési képességeken alapuló kiberfenyegetési hírszerzés létrehozása.
- Valós idejű hálózatmonitorozás a biztonsági incidensek azonosítása, valamint riasztások generálása vagy automatizált válaszok kiváltása érdekében.
- Rosszindulatú programokhoz kapcsolódó fenyegetések mérséklése a kód viselkedésének, a hálózati forgalomnak és a fájljellemzőknek az elemzése révén.
- Sérülékenységek azonosítása és kezelése több információforrás felhasználásával.
- Kiberbiztonságos eszközök és megoldások, amelyek kockázatcsökkentést nyújtanak az MI, az IoT, az intelligens hálózatok vagy más gyártási láncok metszetében.
- Önhelyreállítási képességekkel támogatott incidenshelyreállítás.
- Automatizált sérülékenységvizsgálat és penetrációs tesztelés a gyengeségek megelőző azonosítása érdekében.
- Üzleti szempontból érzékeny adatok védelme hozzáférési minták elemzésével és rendellenes viselkedés észlelésével.
- A CRA követelményeivel összhangban termékbiztonságot vagy beépített/alapértelmezett kiberbiztonságot biztosító eszközök és megoldások.



Elszámolható költség típusok

- Személyzeti költségek.
- Alvállalkozói költségek.
- Beszerzési költségek.
- Eszközköltségek.
- Egyéb áruk, munkák és szolgáltatások.
- Közvetett költségek.



Ütemezés



KEZDÉS

Egyedi kezdési szabály

A projekt kezdőnapját a támogatási megállapodás rögzíti; rendes esetben a támogatási megállapodás aláírását követő időpont, kivételesen visszamenőleges kezdés is lehetséges, de nem lehet korábbi a pályázat benyújtásának napjánál.

A CYBERAI intézkedés indikatív időtartama 36 hónap; más időtartamok nincsenek kizárva.



Kötelező dokumentumok

- Pályázati űrlap, A rész.
- Pályázati űrlap, B rész.
- Tulajdonosi és ellenőrzési nyilatkozatok, beleértve a társult partnerekre és alvállalkozókra vonatkozó nyilatkozatokat is.

✓☰ Kötelező vállalások

- A projekt első hat hónapjában további disszeminációs és hasznosítási teljesítendő eredményt kell benyújtani.
- A projekt teljes időtartama alatt 12 havonta további éves teljesítendő eredményeket kell benyújtani a releváns KPI-k teljesüléséről és a projektkimenetekről.
- A téma keretében fejlesztett rendszereket, eszközöket és szolgáltatásokat kedvező piaci feltételek mellett licencelés céljára hozzáférhetővé kell tenni a meghatározott Cyber Hubok, CSIRT-ek, illetékes hatóságok és más releváns hatóságok számára.



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.