NOVEMBER 2025

# NEWSLETTER °2

# GO CLOUD GO SECURE

Co-funded by the European Union

## 🚀 Say Hello to Go Cloud! Go Secure!

**Kedves Olvasó!**

**Nagyon örülünk, hogy újra találkozunk! A Go Cloud! Go Secure! projekt második hírlevelét olvasod.**

**Az előző hírlevél óta rengeteg izgalmas dolog történt: leteszteltük és véglegesítettük a CSI Mátrixot, személyesen találkoztunk Bulgáriában, a csodás Szófiában, és nagy lendülettel dolgoztunk a Go Cloud képzési anyagok fejlesztésén.**

**Ez a szám tele van hasznos ötletekkel és információkkal, amelyekkel tovább növelheted a kiberbiztonsági tudásodat.**

**Köszönjük, hogy velünk tartasz!**

**A Go Cloud csapata**

## Kiemelt tartalmak



# A CSI MÁTRIX BELSŐ ÉS KÜLSŐ TESZTELÉSE

A WP2–A5 „A digitális CSI Mátrix tesztelése, értékelése és finomítása” munkarész részeként a partnerek valós környezetben végezték el a tesztelést, hogy felmérjék, mennyire hasznos, érthető és felhasználóbarát a Cloud Security Implementation (CSI) Mátrix.

## Belső Tesztelés

A belső tesztelés során olyan munkatársak próbálták ki a Mátrixot, akik nem vettek részt annak fejlesztésében, így friss és elfogulatlan visszajelzést adhattak. Összesen hét, releváns tapasztalattal rendelkező személy vett részt, többségük korábban is dolgozott felhőbiztonsági eszközökkel. A javasolt sérülékenységeket és a hozzájuk kapcsolódó megelőző intézkedéseket megfelelőnek találták, és nagyra értékelték az eszköz gyakorlati hasznosságát. A legtöbb tesztelő szerint a Mátrix intuitív és könnyen áttekinthető, különösen tetszett nekik a színkódolt kockázati rendszer. Bár az interfész összességében felhasználóbarát volt, néhány felhasználó kisebb hibákat tapasztalt, például PDF-export problémákat vagy időnkénti lefagyást. Az általános visszajelzés nagyon pozitív volt: a Mátrix áttekinthetőnek, jól felépítettnek és a kkv-k igényeihez jól illeszkedőnek bizonyult. Minden belső tesztelő jelezte, hogy használná és ajánlaná is az eszközt.

## Külső Tesztelés

A külső tesztelés szintén kiválóan sikerült. Minden partner túlteljesítette az öt fős célt, és széles körből gyűjtött visszajelzéseket kkv-munkatársaktól, IT- és felhőbiztonsági szakértőktől, szakképzési oktatóktól és más szakemberektől. A résztvevők köre szinte fele-fele arányban oszlott meg a felhőbiztonsági eszközökkel korábban dolgozók és a tapasztalattal nem rendelkezők között, így kiegyensúlyozott képet kaptunk. A visszajelzések szerint a Mátrix jól áttekinthető, releváns és megfelelő részletességű, bár a vélemények a felhasználói tapasztalattól függően eltértek. A résztvevők megerősítették, hogy a sérülékenységekhez rendelt megelőző intézkedések logikusak, és a Mátrix mind gyakorlati munkához, mind képzési célokra hasznos. Több mint 90% jelezte, hogy szakmai munkájában is használná, és minden résztvevő ajánlaná másoknak. A felhasználók intuitívnak találták az eszközt, a színkódolt kockázati logikát pedig különösen hasznosnak. Mindössze néhány kisebb technikai problémát jeleztek, ami alátámasztja a Mátrix megbízhatóságát és a felhasználók széles körű elégedettségét.

# ELKÉSZÜLT A MÁTRIX !

AVAILABLE NOW

## ISMERD MEG A CSI MÁTRIXOT, ÉS TEDD BIZTONSÁGOSSÁ FELHŐALAPÚ KÖRNYEZETED!

Örömmel jelentjük, hogy a Cloud Security Implementation Matrix, a Go Cloud! Go Secure! Erasmus+ projekt első elkészült eredménye, már elérhető a projekt honlapján.

A CSI Mátrix elsődleges célcsoportját azok a kis- és középvállalkozások jelentik, amelyek jelenleg is használnak – vagy fontolgatják – felhőszolgáltatások alkalmazását, de nem rendelkeznek saját biztonsági csapattal vagy felhőbiztonsági szakértelemmel.

Az eszköz célja, hogy egyszerű, rugalmas és kkv-barát legyen, elkerülve a túlzott technikai zsargont, így támogatva azokat a szervezeteket, amelyek felelősségteljesen szeretnék bevezetni a felhőmegoldásokat, miközben a biztonságot is szem előtt tartják.

A kkv-knak mindössze annyit kell tenniük, hogy kiválasztják a számukra releváns felhőmodellt, és a Mátrix máris megmutatja, értékeli és kezeli az adott modellhez kapcsolódó kockázatokat.

A CSI Mátrix négy egyszerű lépésben működik:

1. Válaszd ki, melyik felhőszolgáltatási modellt használod vagy tervezed használni (pl. SaaS, PaaS, IaaS).
2. A választásod alapján megtekintheted a felhőalapú környezetedre leginkább jellemző biztonsági kockázatokat.
3. A Mátrix értékeli, hogy az egyes fenyegetések mekkora kockázatot jelentenek a szervezeted számára — ezáltal segít priorizálni a számodra legfontosabb területeket.
4. Végül egyértelmű tanácsokat és útmutatást kapsz, amelyeket a jól ismert OWASP Top 10 keretrendszer alapján állítottunk össze.

A folyamat végén letölthető egy személyre szabott PDF, amely tartalmazza az összes eredményt és ajánlást. Az eszköz az angol mellett további öt európai nyelven is elérhető.

# 2. NEMZETKÖZI PARTNER TALÁLKOZÓ

2025.OKTÓBER 16-17.
SZÓFIA


A „Go Cloud! Go Secure!” projekt nemrég tartotta második nemzetközi találkozóját Szófiában, Bulgáriában, az Acta Consulting vendéglátásában. A magyar, olasz, osztrák és ciprusi partnerek személyesen egyeztették az eddigi eredményeket és a következő lépéseket.

A projekt egyik kulcsfontosságú eredménye, a **Cloud Security Implementation (CSI) Mátrix** digitális önértékelő eszköz alapos tesztelésen esett át. A külső pilot során ***öt országból 38 szakember adott visszajelzést***, és 100%-uk ajánlaná másoknak is. A résztvevők 81,1%-a „nagyon hasznosnak” találta a kockázatértékelési logikát, és megerősítették az eszköz stabil működését. A hét munkatárssal végzett belső tesztelés szintén kiemelte az eszköz értékét, mindössze néhány apró használhatósági javaslattal.

A következő szakaszban a 3. munkacsomag elkészíti az ötlépéses CSI megvalósítási modellt:

1. **Elemzés** (szolgáltatásleltár, kockázati térkép, megfelelés)
2. **Meghatározás** (szabályzat, szerepkörök, célok)
3. **Tervezés** (intézkedések, képzés)
4. **Megvalósítás** (technikai lépések, tudatosság)
5. **Ellenőrzés** (tesztelés, visszajelzés)

A CSI Modell támogatja a kkv-kat a biztonságos felhőrendszerek bevezetésében azáltal, hogy végigvezeti őket a kockázatok azonosításán, a biztonsági intézkedéseken és a folyamatos védelem fenntartásán. Ez növeli a digitális felkészültséget, csökkenti a kiberkockázatokat és erősíti az ügyfé bizalmat.

A jövőbe tekintve a 4. munkacsomag oktatási anyagokat készít, többek között előzetes felmérő kérdőívet, a CSI tananyag tantervét és egy online portált. A tanterv még az idei évben elérhető lesz, a valós üzleti példákra épülő mikro-tananyag videók pedig 2026 elején érkeznek.

# ÉRDEKES PROJEKTEK A KIBERBIZTONSÁG TÁMOGATÁSÁRA

## 🚀 Kiberbiztonsági képzés az operatív technológiai ellenállóképességről

**https://csector.eu/**

A CSecTOR projekt célja, hogy a gyártóiparban és más kritikus infrastruktúrákban működő kkv-kat felvértezze OT-kiberbiztonsági képességekkel.

A projekt középpontjában **a sérülékenységek azonosítása, a védelmi intézkedések bevezetése és az operatív technológiai rendszerekhez kapcsolódó incidenskezelési tervek kidolgozása áll.**

A kezdeményezés **egy testreszabott módszertant, önértékelő eszközt, valamint egy vegyes tanulási és e-learning platformot kínál a reziliencia növelésére** többek között a vegyiparban, a műanyagiparban, a textiliparban, a közművek területén, valamint az olaj- és gáziparban és a közlekedésben.

## 🚀 Közös kiberbiztonsági munkaerő-fejlesztési kezdeményezés az európai ipar számára a kiberbiztonsági szakemberhiány leküzdésére

**https://encrypt40.eu/**

Az Encrypt 4.0 projekt célja, hogy **erősítse a gyártóipari kkv-k képességét adataik, rendszereik és folyamataik védelmére az Ipar 4.0 környezetben.**

A projekt **segíti a vállalatokat a kiberkockázatok azonosításában, elemzésében és kezelésében, miközben támogatja a képzettebb kiberbiztonsági munkaerő kialakítását.**

Gyakorlati, könnyen használható eszközöket kínál, mint például a **Cyber Risk Audit Matrix, a gyakorlatorientált Cybersecurity Training Lab, valamint valós kiberincidenseket és védekezési stratégiákat** bemutató esettanulmány-gyűjtemény.

Az Encrypt 4.0 az interaktív, projektalapú tanulást helyezi előtérbe, segíti a kkv-vezetőket a proaktív kiberbiztonsági gyakorlatok bevezetésében, és ösztönzi a tudásmegosztást az ipari ökoszisztéma nagyobb ellenállóképessége és digitális felkészültsége érdekében.

# A KIBERBIZTONSÁG LENYŰGÖZŐ VILÁGA

## Vannak kiberkalózok is!

Az adathalászat (érzékeny adatok megszerzésére irányuló csalási kísérlet) kifejezés onnan ered, hogy a támadók „csalit” – például e-mailt vagy weboldalt – használnak az áldozatok „horogra akasztásához”, ahogy a horgászok is csalit vetnek a halaknak. A phishingről sok érdekességet megtudhatsz majd a képzési anyagainkból :)

## Az első vírus nem átverés volt.

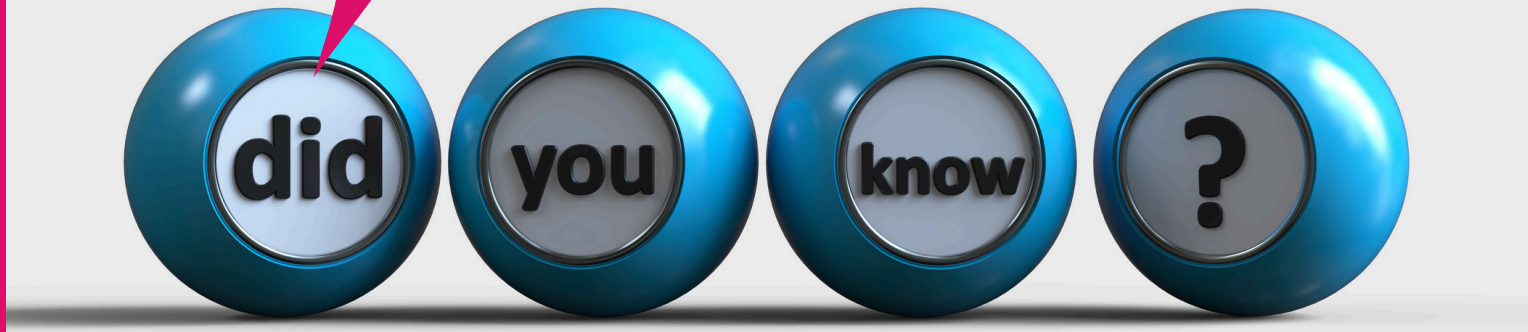
Az első ismert számítógépes vírus a Creeper volt, amelyet az 1970-es évek elején hoztak létre önmagát másoló programként. Nem okozott kárt — mindössze annyit tett, hogy megjelenítette ezt az üzenetet: „I'm the Creeper, catch me if you can!” Inkább egy technológiai kísérletnek számított, mintsem rosszindulatú támadásnak.

## A jelszavak továbbra is komoly gyenge pontot jelentenek.

A világon még mindig a „123456” a leggyakoribb jelszó, pedig évek óta figyelmeztetnek a gyenge jelszavak veszélyeire. A becslések szerint az adatbiztonsági incidensek mintegy 80%-át gyenge vagy ellopott jelszavak okozzák.

## Több a kibertámadás, mint gondolnánk.

A kibertámadások száma megdöbbentő: naponta mintegy 30 000 weboldalt törnek fel. Ez több mint 20 weboldal percenként!



GO CLOUD GO SECURE

2024-1-AT01-KA220-VET-000245093

Az Európai Unió
társfinanszírozásával

Az Európai Unió finanszírozásával készült. A közzétett nézetek és vélemények kizárólag a szerző(k) álláspontját tükrözik, és nem feltétlenül esnek egybe az Európai Unió vagy az Európai Oktatási és Kulturális Végrehajtó Ügynökség (EACEA) álláspontjával. Az Európai Unió és az EACEA nem vállal felelősséget ezekért.