

2026 MÁJUS

# HÍRLEVÉL 03

## GO CLOUD GO SECURE

### Ismerd meg a Go Cloud! Go Secure! új biztonsági tartalmait és eszközeit!

Örülünk, hogy ismét velünk tartasz! A Go Cloud! Go Secure! projekt 3. hírlevelét olvasod.

Izgalmas újdonságokról számolhatunk be: projektünk három kiemelt eredménye már elérhető a weboldalunkon:

- A CSI önértékelő eszköz segítségével felmérheted saját tudásodat, és azonosíthatod azokat a területeket, ahol még érdemes fejlődnöd.
- A CSI kurzus gyakorlati, könnyen követhető tananyagokat kínál a felhőbiztonság témakörében.
- A CSI-modell segít megérteni, hogyan használhatod biztonságosabban a felhőszolgáltatásokat, és milyen lépéseket tehetsz a biztonság növelése érdekében.

Jelenleg mindhárom erőforrás angol nyelven érhető el, de hamarosan elkészülnek a lefordított változatok is.

Aktuális számunkban hasznos híreket, új szakmai anyagokat és gyakorlati információkat találsz, amelyek segítenek megerősíteni szervezeted kiberbiztonsági szintjét.

Köszönjük, hogy velünk tartasz!

A Go Cloud! csapata



Az Európai Unió támogatásával

### Tartalom

Üzenet a Go Cloud! csapatától  
– 1. oldal

A felhőbiztonsághoz vezető út  
– 2. oldal

CSI önértékelő eszköz  
– 3. oldal

CSI kurzus  
– 4. oldal

CSI Megvalósítási Modell  
– 5. oldal

Tesztelőket keresünk!  
– 6. oldal

Hamarosan érkeznek a projektzáró események!  
– 7. oldal

Érdekességek a kiberbiztonság világából  
– 8. oldal





# A felhőbiztonsághoz vezető út

Gyakorlati útmutató KKV-k és szakképzési szolgáltatók számára: mérd fel jelenlegi helyzetedet, fejleszd felhőbiztonsági készségeidet, majd ültess át a megszerzett tudást a gyakorlatba.

Hogyan fejlesztheted szervezeted felhőbiztonságát lépésről lépésre?



## 1 Kezdd önértékeléssel

A CSI önértékelő eszköz segítségével mérd fel jelenlegi felhőbiztonsági tudatosságodat, mindennapi gyakorlataidat és döntéshozatali szokásaidat. Az eszköz segít azonosítani az erősségeidet, a hiányosságokat és a kiemelt fejlesztési területeket.

## 2 Azonosítsd az igényeket és a hiányosságokat

Tekintsd át az eredményeket, hogy megértsd, mely területeken van leginkább szükség fejlődésre – a felhőalapú szolgáltatások alapjaitól és a megosztott felelősségtől kezdve a gyakori fenyegetéseken át a biztonsági gyenge pontokig.



## 3 Fejleszd készségeidet a kurzussal

Tanuld meg felismerni és megérteni a felhőhasználat kockázatait és a gyakori fenyegetéseket, sajátítsd el a biztonságosabb felhőkörnyezetek kialakításának alapjait, és alkalmazz hatékony irányítási gyakorlatokat.



## 4 Alkalmazd a CSI-modellt

Használd a CSI-modellt, hogy a megszerzett tudást valódi intézkedésekké alakítsd. Térképezd fel a szolgáltatásokat, a kockázatokat és a megfelelési követelményeket, majd határozd meg a prioritásokat, a szerepköröket, a szabályzatokat és a megfelelő biztonsági kontrollokat.



## 5 Fejlődj és növekedj biztonságosan

Kövess nyomon az előrehaladást, finomítsd a gyakorlatokat, és folyamatosan erősítsd szervezeted ellenálló képességét. Eszközeink támogatják a folyamatos fejlődést, a munkatársak biztonságtudatosságának növelését és a magabiztos digitális átalakulást.

**Siker!**





# CSI ÖNÉRTÉKELŐ ESZKÖZ

## FELHŐBIZTONSÁGI ÁLLAPOTFELMÉRÉS

VÁLASZOLJ 15 KÉRDÉSRE - ÉS AZONNAL MEGKAPOD AZ  
EREDMÉNYT!

CLICK HERE >

MÁR ONLINE IS ELÉRHETŐ



### MÉRD FEL FELHŐBIZTONSÁGI HELYZETEDET

Mennyire biztonságos a felhőhasználatod? A CSI önértékelő eszköz egyszerű és gyakorlatias módon segít a KKV-knak, oktatóknak és tanulóknak átgondolni a valós életből vett felhőbiztonsági helyzeteket.

A kérdőív olyan kulcsfontosságú témákat érint, mint a felhőszolgáltatási modellek, a megosztott felelősség, az adatvédelem, a zsarolóvírusok elleni védekezés, a Zero Trust megközelítés, a hozzáférés-szabályozás, az irányítás és az incidenskezelés.

Itt nincs szó stresszes „vizsgahelyzetekről” – csak olyan hasznos kérdésekről, amelyek segítenek felmérni, mit tudsz már, és mely területeken érdemes még fejlődnöd.

## A MINDENNAPI KOCKÁZATOKTÓL A JOBBI DÖNTÉSEKIG

A felhőbiztonság összetettnek tűnhet, különösen a korlátozott idővel és erőforrásokkal rendelkező kisebb vállalkozások számára. A **CSI önértékelő eszköz** ezért a témát olyan gyakorlati kérdésekre bontja, amelyek közvetlenül kapcsolódnak a mindennapi üzleti döntésekhez. Segítségével átgondolhatod többek között a jelszavak biztonságát, a többtényezős hitelesítést, a biztonsági mentéseket, az adatszivárgást, a biztonságos felhőkörnyezetek kialakítását és a felelősségi körök egyértelmű meghatározását.

A kérdések megválaszolásával jobban megértheted, mely területek igényelnek nagyobb figyelmet, és milyen ismeretek segíthetik a felhőszolgáltatások biztonságosabb használatát.

## EGYSZERŰ ELSŐ LÉPÉS AZ ERŐSEBB FELHŐBIZTONSÁG FELÉ

A CSI önértékelés célja nem a számonkérés, hanem a tudatosság növelése. Gyors és hasznos lehetőséget ad arra, hogy felmérj tudásodat, azonosítsd tanulási igényeidet, és magabiztosabban mozogj a felhőbiztonság témaköreiben.

KKV-k, oktatók és tanulók számára egyaránt praktikus kiindulópontot jelent az erősebb kiberbiztonsági szokások kialakításához és a biztonságosabb felhőhasználatra való felkészüléshez.

# FEJLESZD FELHŐBIZTONSÁGI KÉSZSÉGEIDET!

A CSI kurzus gyakorlati, könnyen követhető képzésen keresztül segít fejleszteni a KKV-k felhőbiztonsági ismereteit. Megmutatja, hogyan ismerheted fel a kockázatokat, hogyan védheted az adatokat, hogyan hozhatsz jobb mindennapi biztonsági döntéseket, és miként használhatod magabiztosabban a CSI-modellt.

22  
SELF-PACED HOURS

06  
PRACTICAL  
MODULES

06  
LANGUAGES

Yes  
CERTIFICATE

## WHAT YOU'LL ACHIEVE

### Walk out with a security posture you can defend.

Each module ends with a practical artefact – a policy, a configuration, or a decision log – that you keep for your business.

01

Understand the main cloud security risks affecting SMEs and how to recognise weak points before they become serious issues.

02

Apply practical controls for safer cloud use, including access management, data protection, backup planning, and secure configuration.

03

Use the CSI Model to assess your current situation, prioritise improvements, and make clearer security decisions.

04

Build confidence to support staff awareness, training delivery, compliance readiness, and long-term secure digital transformation.

CLICK HERE >

## CSI KURZUS

### Hat modul elfoglalt vállalkozóknak

- **1. modul – A felhőbiztonság alapjai KKV-k számára**
  - Megismerheted a felhőalapú számítástechnika alapjait, a szolgáltatási és telepítési modelleket, azok KKV-k számára jelentkező előnyeit és kihívásait, valamint a biztonságos felhőhasználat és a megosztott felelősség alapelveit.
- **2. modul – Fenygetettség környezete és KKV-specifikus kihívások**
  - Megismerheted a KKV-kat érintő leggyakoribb kiberbiztonsági fenyegetéseket, többek között az adathalászatot, a zsarolóvírusokat, a belső fenyegetéseket és az árnyék-IT-t, valamint az ezekkel szemben alkalmazható gyakorlati és költséghatékony megelőzési intézkedéseket.
- **3. modul – Biztonságos felhőkörnyezetek kialakítása**
  - Megismerheted a biztonságos felhőarchitektúrák kialakításához szükséges alapelveket és kontrollokat, beleértve az identitás- és hozzáférés-kezelést, a titkosítást, a többrétegű védelmet, a szegmentálást, a monitorozást és a „secure by design”, azaz beépített biztonság elvét.
- **4. modul – Felhőbiztonsági irányítás**
  - A modul bemutatja a felhőbiztonsági irányítás fő területeit: a titkosítást és kulcskezelést, az adatvédelmet, a kockázatértékelést, a jogszabályi megfelelést, a beépített adatvédelmet (privacy by design), az üzletmenet-folytonosságot és az elismert kiberbiztonsági keretrendszereket.
- **5. modul – A CSI-modell: az elmélettől a gyakorlatig**
  - Megismerheted, hogyan alkalmazhatják a KKV-k a Cloud Security Implementation Modellt a kockázatok értékelésére, a prioritások meghatározására, a biztonsági intézkedések megtervezésére és végrehajtására, valamint azok hatékonyságának folyamatos monitorozással és fejlesztéssel történő ellenőrzésére.
- **6. modul – Kapacitásépítés szakképzési szolgáltatók számára**
  - A modul segít a KKV-k igényeire szabott felhőbiztonsági képzések kialakításában, személyre szabott tanulói profilok, gyakorlati oktatási módszerek, digitális értékelési eszközök és iparági partnerekkel való együttműködés alkalmazásával.



### A kurzus felépítése

A CSI kurzus végigvezet a felhőbiztonság alapjain, a fenyegetések felismerésén, a biztonságos felhőkörnyezetek kialakításán, az irányításon, a CSI-modellen és a kapacitásépítésen.

Segít biztonságosabb döntéseket hozni, növelni a munkatársak biztonságtudatosságát, javítani a megfelelési felkészültséget és magabiztosabban végrehajtani a digitális átalakulást.

# CSI MEGVALÓSÍTÁSI MODELL

## GYAKORLATI ÚTITERV A BIZTONSÁGOSABB FELHŐHASZNÁLATHOZ

A felhőszolgáltatások gyorsabbá, rugalmasabbá és versenyképesebbé tehetik a KKV-kat – de csak akkor, ha biztonságosan használják őket.

A CSI Megvalósítási Modell segít megérteni a felhőhasználattal kapcsolatos kockázatokat, egyértelmű prioritásokat meghatározni és gyakorlati lépéseket tenni az erősebb kiberbiztonság érdekében.

### CSI Implementation Model

Phase 1: ANALYSE

Phase 2: DEFINE

Phase 3: PLAN

Phase 4: IMPLEMENT

Phase 5: VERIFY

#### A kockázatoktól a cselekvésig

A CSI-modell a felhőszolgáltatások, a lehetséges kockázatok és a megfelelési követelmények részletes elemzésével kezdődik. Ez segít felismerni, hol a legsérülékenyebb a szervezeted, és mely területeken szükséges elsőként fejlesztéseket végrehajtani.

#### KKV-k igényeire szabva

A modellt úgy alakították ki, hogy gyakorlatias és könnyen követhető legyen. Segít szabályzatokat kialakítani, kijelölni a felelősségi köröket és reálisan megvalósítható biztonsági intézkedéseket választani – szükségtelen bonyolultság nélkül.

#### Öt szakasz az erősebb felhőbiztonságért

A CSI Megvalósítási Modell öt kulcsfontosságú szakaszon vezet végig:

**1. Elemzés – 2. Meghatározás – 3. Tervezés – 4. Megvalósítás – 5. Ellenőrzés**

Lépésről lépésre segít eljutni a kockázatok megértésétől a tényleges biztonsági intézkedések alkalmazásáig.

A modell hangsúlyozza a képzés, a monitorozás és a visszacsatolás fontosságát is. A felhőbiztonság így nem ér véget az intézkedések bevezetésével, hanem a tanulás, ellenőrzés és fejlesztés folyamatos folyamatává válik.

[CLICK HERE](#)



A CSI-modell olyan gyakorlati keretrendszert biztosít, amely segít biztonságosabb döntéseket hozni, megvédeni az adatokat, javítani a megfelelőséget és hosszú távon magabiztosabban használni a felhőtechnológiákat.

# TESZTELŐKET KERESÜNK!



**GO CLOUD!  
GO SECURE**

## PROJEKT TESZTELÉSI SZAKASZÁBALÉPETT

A Go Cloud! Go Secure! projekt újabb fontos mérföldkőhöz érkezett: megkezdődik a CSI Megvalósítási Modell, valamint a kapcsolódó képzési program tesztelése.

Ennek a szakasznak a célja annak felmérése, hogy a kidolgozott eszközök mennyire hasznosak, egyértelműek és relevánsak a vállalkozások, oktatók és felhőbiztonsági szakemberek számára.



### Gyakorlati eredmények szakértői visszajelzések alapján

A tesztelési folyamat és az eredmények értékelése várhatóan 2026 szeptemberére fejeződik be. A végső módosításokat követően a Cloud Security Implementation Model és a képzési program mind az öt projektnyelven elérhető lesz.

**WE WANT YOUR  
FEEDBACK!**

### Külső szakértők is bekapcsolódnak a tesztelésbe

A projektpartnerek munkatársai mellett külső szakértők és a célcsoportok képviselői is részt vesznek a tesztelésben. Visszajelzéseik segítségével a konzorcium tovább finomíthatja a modellt és a képzési anyagokat annak érdekében, hogy azok a lehető legjobban megfeleljenek a kis- és középvállalkozások gyakorlati igényeinek.

### Várható eredmények 2026 szeptemberére

A pilot tesztelés lezárása

A modell és a kurzus finomítása

Elérhetőség öt nyelven



Te is hozzájárulhatsz a Go Cloud! eredményeinek  
véglegesítéséhez értékes visszajelzéseiddel!

**[Link a teszteléshez](#)**

# HAMAROSAN ÉRKEZNEK A PROJEKTZÁRÓ ESEMÉNYEK!

2026. szeptember–október |  
Öt európai országban

2026.  
SZEPTEMBER –  
OKTÓBER

PROJEKTZÁRÓ ESEMÉNYEKET  
SZERVEZÜNK:

AUSZTRIÁBAN,  
MAGYARORSZÁGON,  
OLASZORSZÁGBAN,  
BULGÁRIÁBAN,  
CIPRUSON.

**Mire számíthatsz? Vegyél részt a helyi eseményen, ha:**

- Ismerd meg a projekt eredményeit és innovatív eszközeit!
- Sajátítsd el gyakorlati felhőbiztonsági stratégiákat!
- Cserélj tapasztalatot szakértőkkel és helyi érintettekkel!
- Meríts inspirációt és építs értékes szakmai kapcsolatokat!
- KKV tulajdonosa vagy vezetője vagy,
- informatikai szakember vagy,
- kiberbiztonsági szakember vagy,
- tanácsadó vagy,
- oktató vagy,
- vagy egyszerűen érdekel a felhőbiztonság.

## Kövesd híreinket!

A részletes programokat, időpontokat és regisztrációs információkat hamarosan közzétesszük a projekt weboldalán és közösségimédia-felületein.

**Ne hagyd ki a lehetőséget, hogy te is részese legyél egy erősebb és biztonságosabb digitális Európa megteremtésének!**



# A KIBERBIZTONSÁG LENYŰGÖZŐ VILÁGA

## A kiberbiztonságban még a méz is lehet csapda!

A honeypot, vagyis „mézesbödön” egy szándékosan csábítóvá tett ál-rendszer, amelynek célja a kibertámadók becsalogatása. Miközben a behatolók azt hiszik, hogy értékes célpontot találtak, a biztonsági szakemberek észrevétel nélkül megfigyelhetik módszereiket, és az így megszerzett ismeretek alapján hatékonyabban védhetik a valódi rendszereket.

## Egyes számítógépek digitális szigeteken élnek!

A különösen érzékeny számítógépeket esetenként „air-gapped”, vagyis fizikailag leválasztott módon üzemeltetik. Ez azt jelenti, hogy nincs közvetlen kapcsolatuk az internettel vagy más hálózatokkal. Azonban még egy ilyen „digitális sziget” is elérhető lehet egy fertőzött USB-meghajtón vagy más cserélhető adathordozón keresztül.

## Egy fénykép titkos utast is rejthet!

A szteganográfia olyan eljárás, amelynek során információt rejtenek el egy hétköznapi tünő képben, hangfelvételben vagy videóban. A fájl teljesen normálisnak tűnhet, miközben titokban rejtett üzenetet vagy akár rosszindulatú kódot tartalmaz.

## Minden fájlnak van digitális ujjlenyomata!

A kriptográfiai hash egy fájl egyedi digitális ujjlenyomataként működik. Már egyetlen karakter megváltoztatása is teljesen eltérő hashértéket eredményezhet, így észlelhető, ha az adatokat titokban módosították.

did

you

know

?



GO CLOUD GO SECURE

2024-1-AT01-KA220-VET-000245093



**Az Európai Unió  
támogatásával**

Az Európai Unió társfinanszírozásával. A kifejtett nézetek és vélemények kizárólag a szerző(k) álláspontját tükrözik, és nem feltétlenül egyeznek meg az Európai Unió vagy az Európai Oktatási és Kulturális Végrehajtó Ügynökség (EACEA) álláspontjával. Sem az Európai Unió, sem az EACEA nem tehető felelőssé értük.