NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 4. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- RIASZTÁSOK
- TÁJÉKOZTATÁSOK
- CTI ELEMZÉS
- IT BIZTONSÁGI TIPP
- BBA+ BESZÁMOLÓK

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Kiberbiztonsági reformra készül az EU a magaskockázatú beszállítók ellen

(bleepingcomputer.com)

Az Európai Bizottság új kiberbiztonsági jogszabály bevezetését javasolja, amely kötelezővé tenné a magas kockázatú beszállítók eltávolítását a telekommunikációs hálózatok biztonsága érdekében, továbbá megerősítené a kritikus infrastruktúrákat és az államilag támogatott rendszereket célzó kiberbűnözői csoportokkal szembeni védelmet. **Bővebben...**

PDFSider malware pénzügyi szektort célzó támadásokban

(bleepingcomputer.com)

Egy, a pénzügyi szektorban működő, Fortune 100 vállalatot érintő zsarolóvírus-kampány során a támadók az új, PDFSider néven azonosított Windows-alapú malware-t alkalmazták. A malware elsődleges szerepe nem közvetlen károkozás, hanem egy rejtett, hosszú távú hozzáférést biztosító backdoor kialakítása volt, amely fejlett, APT csoportokra jellemző támadási módszertant tükröz. **Bővebben...**

Hamis utazási ajánlatok a közösségi média platformokon

(theguardian.com)

A január kiemelt időszaknak számít az utazással kapcsolatos átverések szempontjából. Ilyenkor a felhasználók tömegesen keresnek kedvező ajánlatokat, ami ideális támadási felületet biztosít az online csalók számára. A csalási módszer jellemzően egy, a közösségi médiában megjelenő, hitelesnek tűnő hirdetéssel indul, amely gyakran egy legitim, ismert utazási iroda eredeti hirdetésének megtévesztő másolata, vagy mesterséges intelligencia segítségével generált tartalom. **Bővebben...**

Vállalati adatokat vettek célba rosszindulatú Chrome bővítményekkel

(bleepigcomputer.com)

Öt olyan vállalati HR (Humánerőforrás) és ERP (Vállalati Erőforrás Tervezés) rendszereket célzó rosszindulatú Chrome böngészőbővítményt fedezett fel a Socket biztonsági cég, amelyek célja a hitelesítő adatok megszerzése és a biztonsági incidensekre reagáló felügyeleti oldalak blokkolása volt. **Bővebben...**

Böngészőbővítményekkel támad a GhostPoster – 840 ezerszer került letöltésre

(bleepingcomputer.com)

17 új, a GhostPoster kampányhoz köthető rosszindulatú böngészőbővítményt azonosítottak a Chrome, a Firefox és az Edge áruházaiban, amelyek együttesen mintegy 840 ezer telepítést értek el. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

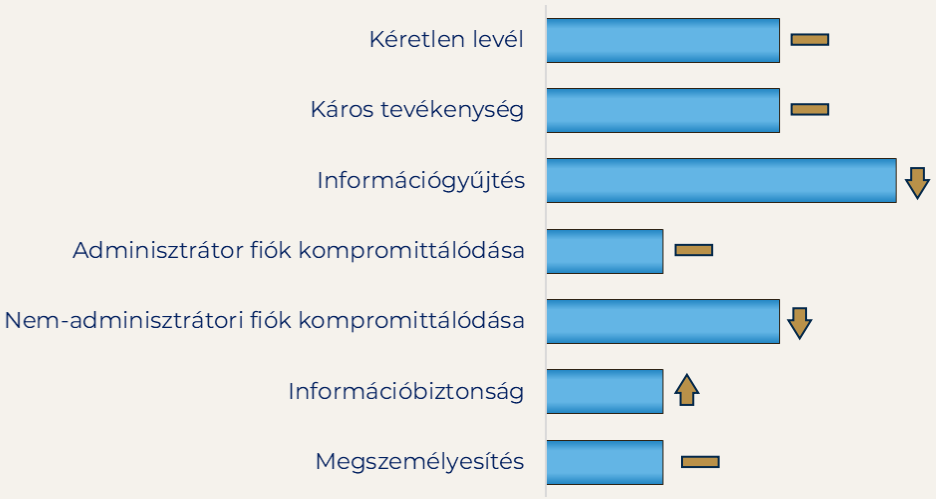
2026. 01. 16. — 2026. 01. 22.

Fenyegetettségi szint:

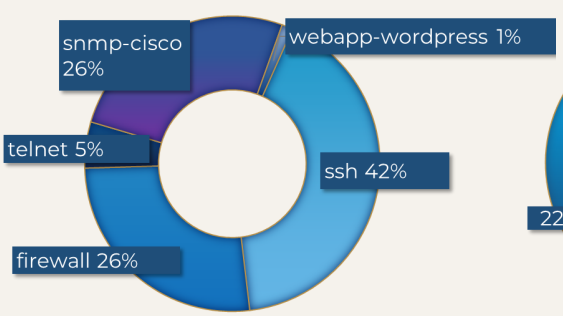
alacsony | közepes | magas | kritikus

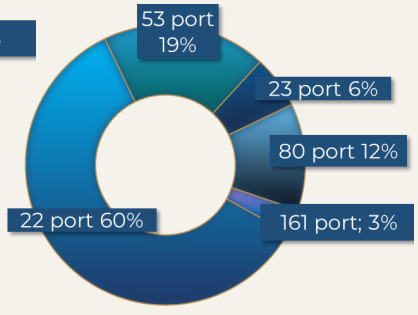
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





NEMZETI KIBERBIZTONSÁGI INTÉZET

RIASZTÁSOK TÁJÉKOZTATÁSOK

Riasztás az MVM Next Energiakereskedelmi Zrt. nevével visszaélő SMS üzenetekkel kapcsolatban

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) **riasztást ad ki az MVM Next Energiakereskedelmi Zrt. nevével és arculati elemeivel visszaélő, adathalász hivatkozást tartalmazó szöveges üzenetek (SMS) terjedése kapcsán**.

Intézetünkhöz megnövekedett számú állampolgári bejelentés érkezett az MVM Next Energiakereskedelmi Zrt. nevével és arculati elemeivel visszaélő, káros hivatkozást tartalmazó, valójában nem fennálló villanyszámla tartozás rendezésére felszólító, megtévesztő SMS üzenetekkel kapcsolatban.

Elolvasom

Tájékoztatás a 2026. évi választásokkal összefüggésben

Felhívjuk szíves figyelmüket, hogy a közelgő 2026. évi országgyűlési választásokkal összefüggésben – különösen az alábbi témakörökben: választási eljárásrend, határidők, jelöltek és listák stb. – a Nemzeti Választási Iroda (NVI) hivatalos weboldaláról (valasztas.hu), illetve az ott közzétett, hitelesített dokumentumokból és közleményekből tájékozódjanak.

Elolvasom

NEMZETI KIBERBIZTONSÁGI INTÉZET

CTI JELENTÉS

Kiberbiztonsági képzések Magyarországon

Jelen dokumentum célja, hogy áttekintést adjon a magyarországi, iskolarendszerű kiberbiztonsági képzési kínálatról, különös tekintettel azokra a programokra, ahol a kiberbiztonság nem kiegészítő témakör, hanem a képzés egyik szervező elve. A jelentés összegyűjti a releváns felsőoktatási alap és mesterképzéseket, valamint a szakirányú továbbképzéseket, és gyakorlati szempontok mentén segíti a döntéshozók, képzésszervezők, jelentkezők és munkaadók gyors tájékozódását.

Az NBSZ NKI célja, hogy a képzéseket összehasonlíthatóvá tegye fókusz, belépési háttér és karrierkimenet alapján, és ehhez közös keretként az ENISA European Cybersecurity Skills Framework (ECSF) szerepkörprofiljait használja.
A dokumentum tájékoztató jelleggel ECSF mappinget is ad, megmutatva, hogy az egyes képzések tipikusan mely kiberbiztonsági szerepekhez, például mérnöki, incidenskezelési, kockázatkezelési, megfelelőségi vagy jogi területekhez fejlesztenek kompetenciákat.

Elolvasom

Érdekesnek találta elemzésünket? Szívesen olvasna hasonló témakörben?

Figyelmébe ajánljuk *„Kiberbiztonsági kihívások és fenyegetések 2030-ig”* című jelentésünket!

NEMZETI KIBERBIZTONSÁGI INTÉZET

TIPP

Adatvédelmi Világnap – 2026

Minden év január 28-án ünnepeljük a Nemzetközi Adatvédelmi Világnapot, amelynek célja, hogy felhívja a figyelmet az adatvédelem fontosságára, különösen a mai, digitális korban.

Ennek kapcsán a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet külön figyelmet fordít azokra az alapvető, különösebb szakmai tudást nem igénylő, bárki által elvégezhető biztonsági intézkedésekre és információkra, amelyek hozzájárulhatnak a felhasználók adatainak mindennapi biztonságához. Az alábbi kiadványunkban olyan általános tanácsok és tudnivalók kerültek összegyűjtésre, amelyek megléte alapszintű védelmet biztosíthat adataink számára.

Elolvasom

Átverés az ajtónk előtt

További hasznos tippekért és szórakoztató játékokért, tekintse meg az ünnepi kiadványunkat!

BBA+ BESZÁMOLÓ

Nerdearla Es 2025 Konferencia

2025. november 13-15.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** munkatársai **Széchenyi Terv Plusz pályázat** részeként szakmai ismeretbővítésen vesznek részt a súlyos és szervezett, határon átnyúló bűncselekmények elleni küzdelem, illetve ilyen jellegű bűncselekmények megelőzésének fejlesztése céljából.

A projekt célja a kiberfenyegetések elleni fellépéshez szükséges friss ismeretek gyűjtése és megosztása a hazai kiberbiztonsági szakemberekkel.

BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

A Nemzeti Kiberbiztonsági Intézet munkatársai 2025. november 13-15. között részt vettek az **Madridban** megrendezésre kerülő éves **Nerdearla Es 2025** konferencián.

A konferencia már 11. éve nyújt platformot az információs technológia fejlesztőinek és open source kezdeményezéseknek a gondolatcserére és tudásmegosztásra. A mögötte álló bizottság kifejezetten a spanyol ajkú országokra fókuszál Argentína, Chile, Mexikó és Spanyolország hosztok között. Az esemény célja, hogy hozzáférhetővé tegye a legfrissebb tudást és innovációs megoldásokat a technológia, nyílt forráskód, mesterséges intelligencia, kiberbiztonság és szoftverfejlesztés területén, ingyenes belépéssel a résztvevők számára. A konferencia közösségi szemléletet képvisel, és arra törekszik, hogy összekapcsolja a kiberbiztonsági közösségeket, a szakembereket, fejlesztőket, kutatókat, vállalatokat és szponzorokat elősegítve a tudásmegosztást és az együttműködést. Viszonylag nagy támogatottságú esemény fő szponzorai a Google, az Amazon, a Suse és az ElevenLabs.

Kiknek ajánlott a beszámoló megismerése?

- Vállalati IT-biztonsági csapatoknak
- Kiberfenyegetés-kutatóknak és elemzőknek
- Biztonsági mérnököknek és fejlesztőknek
- Kiberbiztonsági szakemberek számára

A konferencia legfontosabb előadási az alábbiakban foglalhatók össze.

NEMZETI KIBERBIZTONSÁGI INTÉZET

Computer sovereignty

(Jon "maddog" Hall)

Az előadó a Linux közösségekben egy kifejezett úttörőnek tartott Jon „Maddog” Hall az előadásában a **számítógépes szuverenitást** tárgyalta. Jon életútjából fakadóan is megtapasztalta több nagyvállalat, köztük szabadalmazott és nyílt forráskódú termékeket forgalmazó cég filozófiáját és az általuk gyakorolt globális hatást.

Az előadás középpontjában **a digitális szuverenitás növekvő jelentősége** állt, amely egyre inkább globális technológiákra és szolgáltatásokra támaszkodik. Jon “Maddog” Hall, a szabad és nyílt forráskódú szoftvermozgalom egyik meghatározó alakja, bemutatta, miért elengedhetetlen a technológiai függetlenség, a helyi, adott tagállami, lokális infrastruktúra kiépítése és a nyílt forráskódú megoldások alkalmazása a magánszféra, a kiberbiztonság és a technológiai szabadság megőrzése érdekében.

Hall hangsúlyozta, hogy **a szuverenitás nem pusztán politikai fogalom, hanem gyakorlati szükségszerűség a nemzetek és közösségek számára**. Rámutatott, hogy a nyílt technológiákra épülő ellenálló ökoszisztémák létrehozása lehetővé teszi a nemzeti kormányok és az állampolgárok számára, hogy megőrizzék a digitális jövőjük és adataik feletti „kizárólagos tulajdonjogot”. Az előadó több évtizedes tapasztalata alapján példákat hozott arra, hogyan csökkenthető a függőség a zárt rendszerektől, miként érhető el költségcsökkentés és hogyan ösztönözhető az innováció a témában a kiberbiztonsági domain-ben. Hall „életutakat” is megosztott a nézőkkel, amelyen nyomon követhettük az állításai beigazolódásait.

BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Creating documentation that developers will actually read

(Damilola Ezekiel)

Az előadás központi témája az **IT fejlesztői dokumentáció minősége és annak hatása a felhasználói élményre**. Damilola Ezekiel számos open source projektbeli részvételi tapasztalataiból kiindulva (köztük a TechWriters Hub közösség vezetését ellátó projektben is) prezentációjában rávilágított arra, hogy a dokumentációkészítés gyakran háttérbe szorul, emiatt nehezen használható, hiányos vagy nem a felhasználó igényeire szabott. Ennek következményeként a fejlesztők sokszor inkább Stack Overflow-hoz vagy mesterséges intelligencia-alapú eszközökhöz fordulnak segítségért.

Az előadó hangsúlyozta, hogy **a dokumentáció a vonatkozó IT projekt elsődleges kapcsolódási pontja**, és **kulcsfontosságú** az adott projektbeli közreműködők és stakeholderek bevonásában. A 2024-es GitHub Open Source felmérés szerint a transzparens hozzáféréskezelés az egyik legfontosabb tényező, amelyek befolyásolja az open source projektekhez való csatlakozási hajlandóságot.

Az előadás során bemutatásra kerültek jó gyakorlatok (best practices), amelyekkel az IT dokumentáció valóban hasznossá válhat a mindennapi projektmunka során:

- Hogyan javítja a jó dokumentáció a fejlesztői élményt.
- Interaktív dokumentáció létrehozása olyan eszközökkel, mint a Swagger UI, StackBlitz, CodeS -andbox és Replit.
- Hatékony README és hozzájárulási útmutató megírása.
- Dokumentáció strukturálása különböző felhasználói igények szerint a Diátaxis keretrendszerrel.

- Interaktív demók beágyazása MDX vagy sandbox eszközök segítségével.
- Dokumentációkezelés az IT fejlesztői team együttműködése érdekében.
- Lokalizációs eszközök használata a globális elérhetőség biztosításához.
- DevRel-ről és fejlesztői oktatásról szóló tapasztalatok megosztása.

BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

Delay Accounting an underrated feature of the Linux kernel

(Nikolay Sivko)

Az előadás célja az volt, hogy bemutassa a Linux kernel egyik kevéssé ismert, de rendkívül hasznos képességét, a **delay accounting** funkciót. Nikolay Sivko meglátása szerint a CPU-idő hiányának megértése nem olyan egyszerű, mint a hagyományos mutatók – például a CPU-kihasználtság vagy a Load Average – vizsgálata. A Linux kernel beépített mechanizmusokkal rendelkezik, amelyek pontosan mérik, mennyi ideig vár egy-egy feladat a kernel erőforrásaira. Az előadás részletesen ismertette, **hogyan használható ez a funkció a teljesítményproblémák és az alkalmazások késleltetésének elemzésére**. A résztvevők bepillantást nyerhettek abba, hogyan lehet ezeket a metrikákat hatékonyan alkalmazni a rend-szer optimalizálása és a teljesítmény javítása érdekében. Nikolay Sivko a Coroot alapítója és vezérigazgatójaként küldetésének tekinti, hogy megkönnyítse a hibakeresést az IT fejlesztők számára az adott fejlesztői környezetükben. Az előadó megosztotta a hallgatósággal, hogy kifejezetten érdeklődik a Site Reliability Engineering (SRE) gyakorlatok, valamint az observability és a nyílt forráskódú megoldások iránt. Több mint egy évtizedes tapasztalattal rendelkezik az observability területén, és gyakorlati, valós példákat hozott előadásában.

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Apache Iceberg an Architectural Look Under the Covers

(Alex Merced)

Az előadás során az **Apache Iceberg** volt fókuszban, amely **új megközelítést kínál a Data Lake architektúrákban**. A Data Lake-ek célja az adatdemokratizálás, vagyis, hogy minél több felhasználó, eszköz és alkalmazás hozzáférhessen a vonatkozó adatokhoz. A Dremio Developer Advocat-jének megítélése szerint ehhez elengedhetetlen az adatszerkezetek és a fizikai adattárolás komplexitásának elrejtése a felhasználók elől.

Alex Merced, az O'Reilly által kiadott Apache Iceberg: The Definitive Guide társszerzőjeként előadásában a korábbi iparági szabvány, a Hive táblastruktúráról is szót ejtett, amelyet a Facebook 2009-ben vezetett be. Az előadó szerint ez bizonyos problémákat megoldott, de nagy adatmennyiség, felhasználói és alkalmazási skálán már nem bizonyult elégségesnek. Az előadás bemutatta, miért nem elegendő a Hive formátum, és hogyan kínál megoldást az Apache Iceberg, amelyet olyan vezető technológiai cégek alkalmaznak és fejlesztenek, mint a Netflix, Apple, Airbnb, LinkedIn, Dremio, Expedia és AWS.

How GitHub secures open source

(Joseph Katsioloudes)

Joseph Katsioloudes előadása a konferencián nem csupán technikai **betekintést adott az open source biztonsági faktorainak világába**, hanem **stratégiai perspektívát is nyújtott** arról, miért vált ez a terület kritikus fontosságúvá a digitális ökoszisztéma fenntarthatósága szempontjából. Az előadás központi gondolata az volt, hogy a nyílt forráskódú komponensek ma már nem „perifériás" elemek, hanem a modern szoftverek alapkövei. Ez azt jelenti az előadó szerint, hogy **minden sérülékenység**, amely ezekben a komponensekben megjelenik, **láncreakciót indíthat**

el, és kockázatot jelenthet nemcsak egyetlen alkalmazásra, hanem teljes infrastruktúrákra és iparágakra.

Joseph bemutatta a **GitHub Security Lab** eddigi eredményeit, amelyek önmagukban is figyelemre méltóak: több mint ezer feltárt sérülékenység és nyolcszáznál is több Common Vulnerabilities and Exposures (CVE), vagyis ismert biztonsági sérülékenység adatbázisban való rögzítése történt meg négy év alatt. Ezek az adatok nem pusztán számok, hanem annak bizonyítékai, hogy **a fenyegetések valósak és egyre komplexebb formában kísérnek minket** kiberbiztonsági munkánk során. Az előadás egyik legérdekesebb része az volt, amikor Joseph részletezte, hogyan építi be a GitHub a biztonságot a **Secure Software Development Life Cycle (SSDLC)**, vagyis a biztonságos szoftverfejlesztési életciklus minden szakaszába. Ehhez három fő pillért használ: mesterséges intelligenciát, fejlesztői élményt és közösségi együttműködést. Az AI szerepe különösen hangsúlyos, hiszen képes automatizálni a sérülékenységek felismerését és csökkenteni a manuális ellenőrzések terhét, ugyanakkor Joseph világossá tette, hogy az emberi felügyelet ebben az esetben továbbra is nélkülözhetetlen megítélése szerint.

Az előadás nem csupán az elméleti keretekről szólt, hanem gyakorlati megoldásokat is bemutatott. Szó esett a kódvizsgálati eszközökről, a függőségek menedzsmentjéről és az automatizációról, amelyek mind hozzájárulnak ahhoz, hogy az IT fejlesztők biztonságosabb szoftvereket készíthessenek. **Külön figyelmet kapott a biztonságtudatosság növelése** e domain-ben, amelyet Joseph innovatív módon gamifikációval támogat. Példaként említette a saját fejlesztésű, ingyenesen elérhető játékot (gh.io/secure-codegame), amely már tízezer játékost vonzott világszerte, valamint azokat az oktatóvideókat, amelyek összesen több mint 1,2 millió megtekintést értek el.

A közönségkérdések jól tükrözték az iparági aggodalmakat: hogyan lehet összeegyeztetni a gyors fejlesztési ciklusokat a magas szintű biztonsági követelményekkel? Milyen mértékben

BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

támaszkodhatunk az AI-ra a sérülékenységek felismerésében? Hogyan kezelhetők a komplex függőségi láncok és a szenzitív adatok biztonságos tárolása a bemutatott helyzetekben? Joseph válaszaiban hangsúlyozta, hogy bár az automatizáció és az AI jelentős előrelépést jelentenek, a biztonság nem teljesen „gépesíthető” folyamat: a kiberközösségi együttműködés és az emberi szakértelem továbbra is kulcsfontosságú.

Az előadás záró üzenete egyértelmű volt: **az open source biztonsága nem opcionális, hanem alapvető feltétele a digitális világ stabilitásának**. A GitHub stratégiája – amely a legmodernebb technológiákat, az oktatást és a kiberbiztonsági közösségi erőt ötvözi – jó példa arra, hogyan lehet a biztonságot nemcsak technikai, hanem kulturális szinten is beépíteni a fejlesztési folyamatokba.

Remote Development Enviroments

(Ivan Šarić)

A távoli és hibrid munkavégzés térnyerése bővítette a tehetségállományt, de logisztikai akadályokat is jelent. A távoli munkavégzéssel foglalkozó fejlesztőknek hatékony hozzáférésre van szükségük a berendezésekhez és útmutatásra a sikeres beilleszkedéshez és a termelékenységhez. A mikroszolgáltatás-architektúrákra való áttérés tovább bonyolítja a helyi fejlesztési beállításokat. A komplex rendszerkörnyezetek helyi gépen történő replikálása gyakran kihívást jelent a teljesítményigények és a bonyolult konfigurációk miatt, ami késlelteti a fejlesztők termelékenységét.

A **távoli fejlesztési környezetek** és a **kliens/szerver alapú IDE-k enyhítik ezeket a problémákat**. Biztosítják, hogy minden csapattag azonos konfigurációkhoz és eszközökhöz férjen hozzá, elősegítve ezzel a szabványosított fejlesztési folyamatokat. Ez jelentősen javítja a

fejlesztői élményt, csökkentve a rossz dokumentáció és az eszközök inkonzisztenciája miatt felmerülő többletköltségeket. Emellett lehetővé teszi a globális munkaerő-felvételt is, mivel biztosítja, hogy a távoli munkavállalók biztonságosan hozzáférjenek a vállalati infrastruktúrához, gyakran könnyebb vagy személyes munkaállomások használatával. Számos távoli fejlesztési termék áll rendelkezésre. A teljesen felügyelt megoldások, mint például a **GitHub Codespaces**, a szolgáltató felhőjében kerülnek telepítésre. Az önállóan üzemeltetett opciók, mint például a **JetBrains Fleet/Space** kombináció, teljes ellenőrzést biztosítanak. Mindkét típus megfelel a szigorú biztonsági előírásoknak.

A prezentáció mellett egy interaktív workshop jellegű esettanulmányt is bemutatott az előadó, amelyben egy saját „házi” projektet mutatott be távoli fejlesztési megoldásokkal.

Why CSS was created

(Håkon Wium Lie)

Az előadás igazi történeti és technológiai utazást kínált a web egyik legfontosabb alapkövének, a **Cascading Style Sheets-ek (CSS)**, vagyis a stíluslapok világába. Az előadó, Håkon Wium Lie, aki 1994-ben Tim Berners-Lee mellett dolgozva megalkotta e stíluslapok koncepcióját, nem csupán a technikai részleteket ismertette, hanem betekintést adott abba a gondolkodásmódba, amely a web fejlődését meghatározta a vizsgált történeti időszakban.

Az előadás első része a CSS létrejöttének történelmi kontextusát mutatta be. Håkon elmagyarázta, hogy a kilencvenes évek elején a web még rendkívül egyszerű volt: HTML biztosította a struktúrát, de a megjelenés szabályozása szinte lehetetlen volt. A tartalom és a forma szétválasztása volt az a forradalmi ötlet, amely a CSS megszületéséhez vezetett. Ez a

BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

koncepció nemcsak esztétikai szempontból volt jelentős, hanem alapvetően megváltoztatta a fejlesztési folyamatokat, lehetővé téve a skálázhatóságot és a szabványosítást. Håkon részletesen beszélt a CSS fejlődésének kulcspillanatairól, a W3C ajánlások kidolgozásáról (mint új webes autentikáció szabványosítási törekvések kidolgozásáról, amely biztonságosabb és rugalmasabb alternatívát kínált a weben a jelszó-alapú bejelentkezésnél), valamint arról, hogyan vált a CSS a HTML és a JavaScript mellett a web platform egyik alappillérévé. Külön érdekességként említette az **Acid2** tesztet, amelyet ő javasolt annak érdekében, hogy a böngészők egységesen támogassák a szabványokat. Az előadás során nemcsak a múltat idézte fel, hanem a jelen és a jövő kihívásaira is kitért, például arra, hogyan alkalmazható a CSS különböző eszközökön és formátumokon, megemlítette a Prince CSS-to-PDF formázót is.

A közönség számára különösen inspiráló volt Håkon személyes története és az a szenvedély, amellyel a web mindenki számára elérhetővé tételét és a szabványosítás propagálását képviseli. Megemlítette, hogy a **CSS nem csupán technológia, hanem „filozófiaként” is értelmezhető a területen**: a tartalom és a megjelenés szétválasztása a szabadságot és a rugalmasságot szolgálja. Az előadás végén arra ösztönözte a hallgatóságot, hogy „nézzenek a motorháztető alá”, értsék meg a CSS működését, és használják kreatív célokra.

Az esemény rávilágított arra, hogy **a web fejlődése nem lineárisan írható le, hanem inkább innovációk és kompromisszumok sorozataként**, amelyben a CSS kulcsszerepet játszott és játszik ma is. Håkon előadása egyszerre volt nosztalgikus és előremutató, bemutatva, hogy a három évtizeddel ezelőtt született ötlet hogyan maradt releváns és hogyan alakítja továbbra is a digitális világot.

Az AI/ML csapatokban az open source stratégia kezelésének kihívásai és kulcsfontosságú tényezői

(Ana Jiménez Santamaría)

Az előadás fókuszában az áll, **hogyan alakítja át a nyílt forráskód az AI-iparágat**, bemutatva annak gazdasági értékét, történeti fejlődését, valamint a nyílt AI megoldások bevezetésével járó lehetőségeket és kihívásokat. A prezentáció hangsúlyozza, hogy az open source-t nem csupán passzív fogyasztóként, hanem stratégiai erőforrásként érdemes kezelni a fejlesztési folyamatokban. A prezentációban többször példaként jött fel a PyThorch közösség, amely már az AI forradalom elején elkezdte formálni a fejlődés irányát.

A jelen megértése a szoftver alapjainak ismeretében

(Martí Cristobal)

Az előadás **a szoftverfejlesztés alapjainak és a mély technológiai tudás fontosságának jelentőségét hangsúlyozta** a gyorsan változó modern környezetben. Az előadó kiemelte, hogy a felszínes ismeretek — például csak a legújabb AI-eszközök vagy keretrendszerek használata — nem elegendőek, és a fejlesztőknek meg kell érteniük az algoritmusok, adatstruktúrák, adatbázisok és régi technológiák (pl. **Cobol, SQL**) alapjait is. Bemutatta, hogyan segít ez a tudás a komplex problémák megoldásában, a modern eszközök (pl. **TRPC, GraphQL**) mélyebb megértésében, valamint a függetlenség és a vendor lock-in elleni védelem biztosításában. Emellett hangsúlyozta az **interdiszciplinaritás**, a **folyamatos tanulás** és a **közösségi részvétel** szerepét a hatékony fejlesztési gyakorlatban. Összességében az előadás azt sugallja, hogy a stabil fundamentális ismeretek és a stratégiai szemlélet kulcsfontosságúak a hosszú távú sikerhez és a technológiai zaj közötti eligazodáshoz.

BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Hogyan lehet emlékezetes webes élményeket teremteni: a lenyűgöző dizájn mögött álló kód

(Mariana Beldi)

Az előadás a webes animációk fejlődését és modern technológiáinak gyakorlati alkalmazását mutatta be, különös tekintettel a **CSS** és **SVG** alapú megoldásokra. A beszélő bemutatta a **Flash-technológia** történeti szerepét és korlátait, majd kitért a natív webes eszközök előnyeire, például a reszponzivitásra, teljesítményre és hozzáférhetőségre. Részletes példákkal illusztrálta a CSS animációkat, clipping és masking technikákat, Scroll Driven Animations-t, valamint 3D CSS-transzformációkat, hangsúlyozva a GPU-gyorsítás és a modern böngészők nyújtotta lehetőségek fontosságát. Az előadás kiemelte **a designerek és fejlesztők közötti hatékony együttműködés**, az interaktív prototípusok és a hozzáférhetőség biztosításának szerepét. Végül gyakorlati tanácsokat adott a webanimációk elsajátításához, kezdve a CSS alapoktól az SVG és GSAP használatán át a komplex, görgetésvezérelt animációkig, bemutatva a modern webdesign irányvonalait és jövőbeli trendjeit.

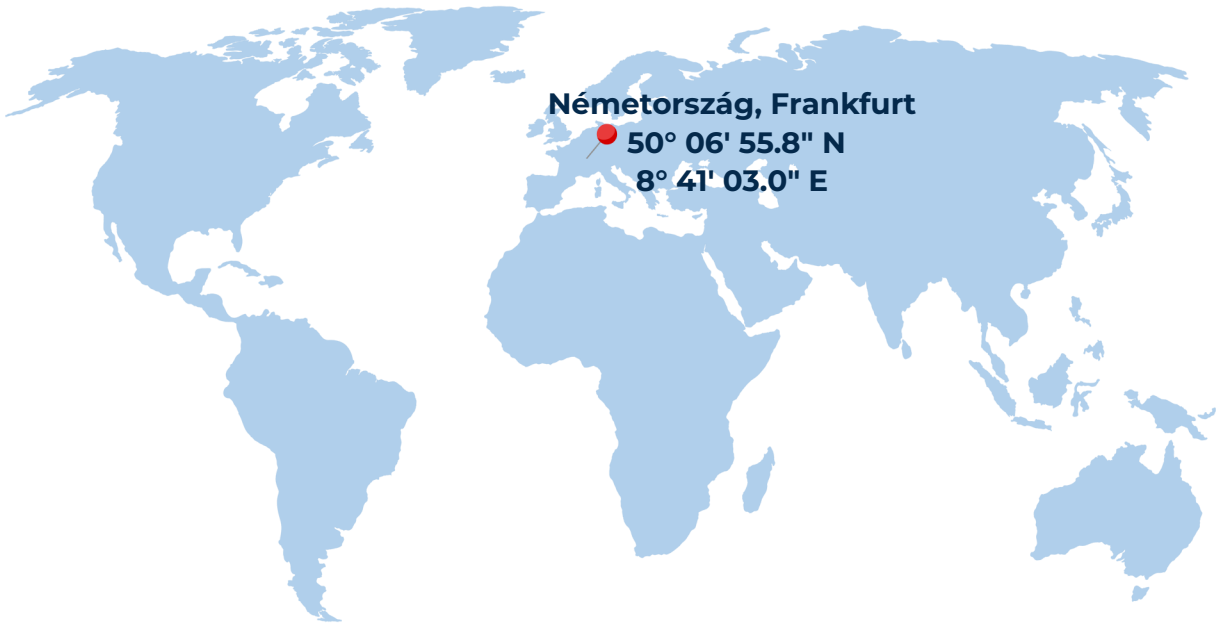
NEMZETI KIBERBIZTONSÁGI INTÉZET

Next IT Security 2025

2025. november 27.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** munkatársai **Széchenyi Terv Plusz pályázat** részeként szakmai ismeretbővítésen vesznek részt a súlyos és szervezett, határon átnyúló bűncselekmények elleni küzdelem, illetve ilyen jellegű bűncselekmények megelőzésének fejlesztése céljából.

A projekt célja a kiberfenyegetések elleni fellépéshez szükséges friss ismeretek gyűjtése és megosztása a hazai kiberbiztonsági szakemberekkel.



BBA-PLUSZ-312-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004 sz. pályázat részeként

A Nemzeti Kiberbiztonsági Intézet munkatársai 2025. november 27-én részt vettek **Frankfurtban** megrendezésre kerülő **Next IT Security 2025** konferencián.

A konferencia a **DACH Cyber Conference** a **DACH-régió kritikus infrastruktúráinak kiberbiztonságára fókuszál**. A kb. 150 fős, felsővezetői (CISO, CIO, CSO) körben megrendezett esemény célja, hogy a résztvevők megosszák tapasztalataikat a kritikus infrastruktúrákat érő fenyegetésekről, a bonyolult szabályozói környezet (például NIS2, DORA) gyakorlati kezeléséről, valamint a zero trust megközelítés és a beszállítói lánc (3rd party, supply chain) kockázatainak kezeléséről. Kiemelt téma a mesterséges intelligencia és az automatizáció szerepe az észlelésben és az incidenskezelésben, illetve a „shared responsibility model" gyakorlati kihívásait és lehetséges megoldásait, erős networking és tapasztalatcsere keretében.

Kiknek ajánlott a beszámoló megismerése?

- Vállalati IT-biztonsági csapatoknak
- Kiberfenyegetés-kutatóknak és elemzőknek
- Biztonsági mérnököknek és fejlesztőknek
- Kiberbiztonsági szakemberek számára

A konferencia legfontosabb előadási az alábbiakban foglalhatók össze.

NEMZETI KIBERBIZTONSÁGI INTÉZET

Critical Infrastructure at Risk:
DACH's Last Stand Against Cyber Catastrophe

(Helmut Spoecker)

Az előadásban Helmut Spocker, az SAP vállalati felhőjének CSO-ja bemutatta, hogy világszerte mintegy száz adatközpont védelméért felel, és felvezette a kritikus infrastruktúrák kiberbiztonsági kihívásait.

Kiindulópontként egy etikus hacker, Rafa Balogh gondolatait idézte, miszerint a jövő háborúi a kibertérben kezdődnek, és a digitális támadások már valódi emberi áldozatokat is okozhatnak. Rámutatott, hogy jólétünk alapja – az energiaellátás, az egészségügy, a kommunikáció, a közlekedés – kritikus infrastruktúrákra épül, amelyek a digitalizáció miatt egyre nagyobb támadási felületet kínálnak. Konkrét példákkal illusztrálta a fenyegetéseket, mint drónos reptérzavarások, áramszünetek, kórházi rendszerek elleni támadások vagy vízellátást érintő incidensek. Kiemelte, hogy a DACH-régió (Németország, Ausztria, Svájc) különösen vonzó célpont, mert magas a digitalizáció foka, kulcsszerepe van a globális ellátási láncokban, és politikai okokból is célkeresztben áll. A statisztikák szerint elsősorban Németországot támadják, utána Ausztriát, míg Svájc sem marad ki, csak valamivel kevésbé kitett. Az elmúlt 2–3 évből több jelentős incidensről beszélt, például nagyszabású DDoS-támadásokról, zsarolóvírustámadások hullámáról és beszállítói láncot érintő vízközmű-támadásról, de hangsúlyozza, hogy ezek csak a jéghegy csúcsa.

Ismertette az uniós és nemzeti szabályozási környezetet (NIS irányelv, kritikus infrastruktúra-regisztráció, 24 órás incidens-bejelentési kötelezettség), valamint a súlyos pénzbírságokat és vezetői felelősséget. Ugyanakkor rámutatott, hogy önmagában a szabályozás nem elég: az üzemeltetőknek, a teljes beszállítói láncnak és a hétköznapi felhasználóknak egyaránt felelősséget

BBA-PLUSZ-312-24-2024-000034 sz. pályázat részeként

BBA-PLUSZ-3.1.2-24-2024-00004 sz. pályázat részeként

kell vállalniuk a biztonságért. Javaslatként stratégiai, nem pusztán költségvezérelt beruházásokat sürget a robusztus, redundáns infrastruktúrákba, szoros állami-magán szektor együttműködést és 7/24-es monitorozást. Nagy hangsúlyt fektet a munkatársak folyamatos képzésére és tudatosítására, illetve bemutatja, hogyan növelheti a decentralizáció a rezilienciát azáltal, hogy csökkenti az egyedi hibapontokat és a támadások „robbanási sugarát".

Összegzésként leszögezte, hogy a DACH-régió már ma is folyamatos kibertámadások alatt áll, ezért több-rétegű kormányzási, technológiai és együttműködési megközelítésre van szükség a kritikus infrastruk-túrák folyamatos működésének biztosításához.

Zero Trust Unleashed: The End of Blind Trust in Third-Party

(Lyzia van Iterson, Florian Jörgens)

Az előadás arról szólt, hogy a beszállítói/supply chain támadások miatt a harmadik felek óriási kockázatot jelentenek, ezért szükség van a Zero Trust modellre, ahol senkinek nem hiszünk automatikusan, minden hozzáférést ellenőrzünk, és csak minimális jogosultságot adunk. Gyakorlati példákon keresztül mutatta be, hogyan lehet ezt a modellt a beszállítókra is kiterjeszteni, és így jelentősen csökkenteni a szervezet kitettségét.

NEMZETI KIBERBIZTONSÁGI INTÉZET

Trust No One: The Zero Trust Playbook for External Threats in 2025

(Rob Otto)

Az előadás központi témája a bizalmon alapuló működés és a Zero Trust megközelítés kapcsolata volt. Az előadó kiemelte, hogy bizalom nélkül nem működhet az üzlet, ugyanakkor az implicit bizalom jelentős kockázatokat hordoz. Bemutatta, hogyan élnek vissza a támadók azzal, hogy az emberek bizonyos technológiákban vagy folyamatokban automatikusan megbíznak. Példaként említette a business email compromise-t, a SIM-cserét, a szoftverellátási lánc támadásait és a deepfake-eket.

Rávilágított, hogy a bizalom helyreállításához bizonyítékokra, vagyis folyamatos identitás-verifikációra van szükség. Hangsúlyozta, hogy a Zero Trust célja az implicit bizalom megszüntetése és minden hozzáférési döntés bizonyítékokon alapuló ellenőrzése. Az identitás kulcsszerepet tölt be a Zero Trust modellben, hiszen a megfelelő hozzáférés biztosítása erős hitelesítésre és kontextusra épül. Az előadó bemutatta a „detektálás–döntés–irányítás” folyamatot, amely segít a hozzáférési kockázatok kezelésében. Kitért a harmadik felek és negyedik felek jelentette kockázatokra, illetve arra, hogy a szerződések nem védenek meg minden fenyegetéstől. Példaként említette, hogy több észak-koreai állami szereplőt is kiszűrtek alkalmazási folyamatok során. Beszélt a Ping Identity saját, kötelező belső identitás-verifikációjáról, melynek célja a bizalom újraépítése volt. Az előadás végén hangsúlyozta, hogy a vállalat célja a láthatóság és kontroll biztosítása minden identitás felett, beleértve a dolgozókat, ügyfeleket, partnereket és AI-ügynököket is.

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

BBA-PLUSZ-3.1.2-24-2024-00004 sz. pályázat részeként

Regulatory Storm Incoming:
How to Build Compliance Resilience in an Unforgiving World

(Jelena Zelenovic Matone, David Gerhardt)

Az előadás a megfelelőség (compliance) fontosságáról és annak fejlesztői környezetbe való beépítéséről szólt. A beszélő kiemelte, hogy a fejlesztők gyorsan akarnak haladni, miközben a jogi és biztonsági csapat feladata a kockázatok csökkentése és a szabályok érvényesítése.

Hangsúlyozta, hogy a nem megfelelő compliance a bizalom elvesztéséhez és akár a vállalat működésének ellehetetlenüléséhez is vezethet. Az előadás különbséget tett a belső irányelvek és a külső szabályozói megfelelés között, amelyek együtt biztosítják a vállalat fenntartható működését. A compliance megértésére egy „irodai hűtős” analógiát hozott, amely jól szemlélteti az ellenőrzés szükségességét. Rámutatott, hogy az AI által generált kód „Vadnyugatot” idéz, mert rengeteg új kód kerül be kevés kontrollal. A

megoldás a beépített szabályok és automatizált ellenőrzések alkalmazása, amelyek írás közben is érvényesítik a vállalati irányelveket. A beszélő ismertette, hogy a modern eszközök képesek átláthatóvá tenni a harmadik féltől származó könyvtárakat, licenceket és kockázatokat. Egy ügyfélpélda bemutatta, hogy a jobb láthatósággal könnyebbé vált a riportok készítése és a jogi figyelmeztetések követése. A fejlesztők így kevesebb hibás vagy tiltott komponenst használnak, mert a rendszer már azelőtt jelzi a problémát, hogy a kód bekerülne a rendszerbe. Ez lehetővé teszi a proaktív, nem pedig reaktív működést, így a kód „secure by design” módon jön létre. Az előadás végül hangsúlyozta, hogy a cél a fejlesztők támogatása úgy, hogy közben a compliance követelmények automatikusan teljesüljenek.

NEMZETI KIBERBIZTONSÁGI INTÉZET

Embedding Compliance at the Moment of Creation in AI Development

(Hani Alus)

Az előadás arról szólt, hogyan lehet **a megfelelőséget már az MI-rendszerek tervezésének és fejlesztésének pillanatába beépíteni**, ahelyett, hogy utólag próbálnánk „ráhúzni” a kész megoldásra. A kiindulópont az a helyzet, hogy rengeteg különböző szabályozási és keretrendszernek kell megfelelni, túl sok a riasztás és az elintézendő feladat, miközben kevés az idő a tényleges javításra, és közben nő a személyes felelősség és a jogi kockázat.

Az előadás **az MI-korszakot szintén egyfajta „vadnyugatként” írja le**: gyors, kiszámíthatatlan, kockázatokkal teli környezetként, amelyben, ha nem változtatunk a működésünkön, belefulladunk a komplexitásba. A session arról szólt, hogyan lehet visszavenni az irányítást úgy, hogy a compliance ne külön, utólagos kontrollréteg legyen, hanem a fejlesztési folyamat szerves része: az adatvédelem, az etikai és jogi megfelelés, valamint a kockázatkezelés már a tervezéskor és a fejlesztés során megjelenjen. Ennek része, hogy a fejlesztők, a jog, a compliance és a biztonság ne egymásnak feszülve, hanem egy közös folyamat részeként dolgozzanak, így csökkentve a kockázatokat, az utólagos tűzoltást, és átláthatóbb, védhetőbb MI-rendszereket hozva létre.

BBA-PLUSZ-312-24-2024-00004 sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004 sz. pályázat részeként

Dhaliwal, Sven Gölles From Friction to Flow: Making Secure Access Effortless for Every User, Everywhere

(Achi Lewis)

Az előadóktól meghallgathattuk, hogyan lehet a biztonságos távoli hozzáférést úgy kiterjeszteni több régióra, hogy közben ne növekedjen feleslegesen az IT-oldali komplexitás és üzemeltetési teher. Bemutatták, milyen stratégiákkal lehet elérni, hogy a felhasználók ne megkerüljék, hanem **elfogadják és valóban használják a biztonsági eszközöket**, és hogyan lehet úgy csökkenteni a hozzáférési „súrlódást", hogy a dolgozók bármilyen eszközről, bármilyen hálózatról zökkenőmentesen elérjék a szükséges alkalmazásokat, adatokat és szolgáltatásokat. Az előadás **gyakorlati lépéseket is ismertetett a leállások és kiesések csökkentésére**, például a tartós kapcsolatok, illetve az automatikus helyreállítási és biztonsági kontroll-visszaállítási megoldások alkalmazásával, hogy a biztonság a háttérben maradjon, miközben a felhasználók számára a munkavégzés folyamatos és kényelmes marad.

Code vs. Instinct: Enhancing Security or Cre-ating New Threats?

(Filip Nowak, Jelena Zelenovic Matone)

A vitaindító beszélgetés arról szólt, **hogyan alakítja át a mesterséges intelligencia a kiberbiztonság világát**, és hogy ez inkább erősíti-e a védelmet, vagy új kockázatokat hoz létre. A beszélgetés középpontjában **a „kód" és az „ösztön" ütközése állt**: egyrészt az MI-alapú rendszerek, amelyek képesek hatalmas adathalmazokból gyorsan mintázatokat felismerni, fenyegetéseket detektálni és incidensekre reagálni, másrészt az emberi ítélőképesség, amely kontextust, tapasztalatot és megérzést visz a döntéshozatalba. A

Az előadás továbbá azt járta körül, hogy **miként definiáljuk újra a védelmet** egy olyan korban, ahol az MI nemcsak a védekező oldalt segíti, hanem új támadási felületeket és sérülékenységeket is létrehoz. Felmerült továbbá az is, **mennyire hatékony az emberi intuíció az algoritmikus logikával szemben** a komplex, rejtett fenyegetések azonosításában, illetve hogyan lehet a kettőt egymást erősítve használni. Külön hangsúlyt kapott az automatizáció és a felelősség kérdése: ha egy MI-rendszer hoz biztonsági döntést, ki viseli a felelősséget egy téves riasztásért vagy egy elszalasztott támadásért.

Végül az előadás azt boncolgatta, hogy **az MI-alapú biztonsági eszközök valóban védőhálót jelentenek-e**, vagy egyfajta kétélű fegyverként a támadók is kihasználhatják őket, például kifinomult, automatizált vagy MI-vezérelt támadások formájában.

BBA-PLUSZ-312-24-2024-00004 sz. pályázat részeként

Dhaliwal, Sven Gölles AI in Command: Revolutionizing Cyber Incident Response with Machine Intelligence

(Achi Lewis)

2025-ben a mesterséges intelligencia és a gépi tanulás már nem a jövő technológiái, hanem a mindennapi működés elengedhetetlen részei a kiberbiztonságban. Mivel a kibertámadások egyre gyakoribbak és kifinomultabbak, a pusztán emberi erőforrásokra támaszkodó védekezés már nem elegendő. A

A session azt mutatta be, **hogyan egészíti ki az MI az emberi szakértelmet**: óriási adatmennyiségeket elemez, mintázatokat és rendellenességeket ismer fel, amelyeket az emberi szem könnyen átsiklathat.

BBA+ BESZÁMOLÓ

Konkrét példák is elhangzottak német szervezetek gyakorlatából, amelyek sikeresen alkalmaznak MI-alapú megoldásokat a kibertámadások valós idejű előrejelzésére és megelőzésére. Az előadók bemutatták, hogyan javíthatók így a fenyegetésészlelési mutatók, hogyan csökkenthető a reagálási idő, és miként szabadíthatók fel emberi kapacitások az összetettebb, stratégiai feladatok számára. A keynote célja az volt, hogy **inspirálja a résztvevőket MI-vezérelt biztonsági megoldások bevezetésére** a hatékonyság, a reziliencia és a fenyegetések elleni védekezés szintjének növelése érdekében.

BBA-PLUSZ-3.1.2-24-2024-00004 sz. pályázat részeként