NEMZETI KIBERBIZTONSÁGI INTÉZET



HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 44. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- ESEMÉNY
- IT BIZTONSÁGI TIPP
- BBA+ BESZÁMOLÓ

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET



HÍREK

HTTP2Shell: Kritikus sérülékenység fenyegeti a Brotli tömörítést használó alkalmazásokat

(aikido.dev)

Egy széles körben használt adattömörítési könyvtár kritikus sérülékenysége miatt számos népszerű programozási környezet és webes alkalmazás válhat támadhatóvá. A CVE-2026-111497 azonosítón nyilvántartott, HTTP2Shell, illetve Node2Shell néven is emlegetett biztonsági hiba távoli kódfuttatást, érzékeny adatok kiszivárgását és szolgáltatásleállást is lehetővé tehet. **Bővebben...**

Tailscale SSH hibák engedhetik a támadóknak a hálózaton belüli root hozzáférést

(cybersecuritynews.com)

Egy új biztonsági jelentés szerint a Tailscale SSH-ban található hibák miatt egy már kompromittált eszközről kiindulva a támadó root-jogosultságot szerezhet más szervereken is. A Tailscale a jelentés megjelenéséig nem erősítette meg az eredményeket, és nem adott ki hozzájuk hivatalos közleményt, CVE azonosítót vagy javított verziót. **Bővebben...**

Új, Yggdrasil-hálózatban rejtőző backdoort használtak ukrán logisztikai vállalat elleni adattörlő támadásban

(thehackernews.com)

Az ESET kutatói egy korábban nem dokumentált, MythicRatatoskr nevű backdoort azonosítottak, amelyet az UAC-0099 (más néven Earth Sirrush) használhatott az ukrán kormány, a gabona szállítmányozás, az energia szektor, valamint egy logisztikai vállalat elleni támadásban. **Bővebben...**

A Signal egy hibája miatt nem lehetett megszakítani a csaló hívásokat

(securityweek.com)

A Signal nemrég adott ki javítást egy kritikus súlyosságú sérülékenység miatt, amely kihasználása lehetővé tette a rosszindulatú hívók számára, hogy a hang-és videócsatornákat akkor is aktívan tartsa, miután a felhasználó bontotta a vonalat. **Bővebben...**

Kiberbiztonsági incidens miatt irányították át a betegeket egy új-mexikói kórházból

(securityweek.com)

Egy kiberbiztonsági esemény hatására a University of New Mexico Health System hétfőn több, mint 30 klinikáján törölte az előjegyzett időpontokat és arra kérte betegeit, hogy ne jelenjenek meg a Albuquerque-ben található központi kórház rendelésein. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2026. 10. 22. - 2026. 10. 29.

Fenyegetettségi szint:

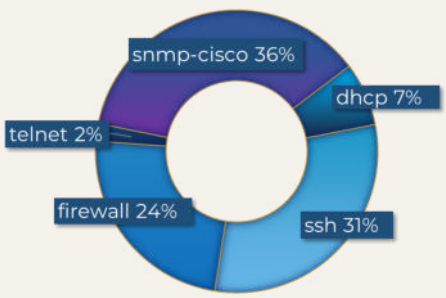
alacsony | közepes | magas | kritikus

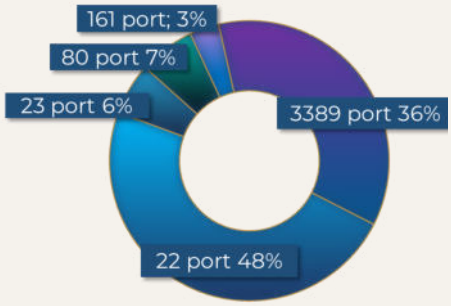
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





NEMZETI KIBERBIZTONSÁGI INTÉZET



ESEMÉNY

Future IT 2026

2026. november 10-12.
Siófok, Azúr Hotel

Nagy örömmel jelentjük be, hogy idén ismét **saját színpaddal készülünk** az ICT Global Future IT konferenciáján, ahol izgalmas témákról beszélgetünk a kiberbiztonság **kiváló, elismert szakembereivel**. Az esemény idén is **több színpaddal és sokszínű, tartalmas programmal** várja az érdeklődőket, remek lehetőséget teremtve a kapcsolatépítésre, az új gondolatok megosztására és az értékes szakmai beszélgetésekre.

2026. szeptember 1. és 2026. október 31. között a **FUTUREIT2026-NKI-VIP** promóciós kód **15% kedvezményt** biztosít a normál jegyárakból.

A kedvezmény a szállásdíjra nem vonatkozik.

Érdekel

Ne maradjon le!

Látogasson el a **kibernaptar.hu** weboldalra és tudja meg milyen további hazai és nemzetközi kiberbiztonsági események várhatók!



IT BIZTONSÁGI TIPP

ECSM 2026 – Összefoglaló

Az Európai Kiberbiztonsági Hónap (ECSM) az Európai Unió éves kiberbiztonsági **tudatosságnövelő kezdeményezése**. A program célja, hogy felhívja a figyelmet a **tudatos internethasználatra** és a **digitális biztonság fontosságára**.

Az NBSZ NKI a Kiberhónap egyik meghatározó magyarországi szakmai szereplőjeként minden évben igyekszik különböző szakmai konferenciákkal és egyéb megjelenésekkel, illetve különböző online is elérhető **tudatosító tartalmakkal hozzájárulni a program sikerességéhez**.

A különböző online csalási módszereket, védelmi intézkedéseket, illetve IT biztonsági tanácsokat az idei évben a felhasználók által már jól ismert **hétköznapi közmondásokba csomagoltuk**. A kiberhónap során közzétett tartalmaink célja, hogy a generációk alatt kialakult, és közismertté vált tudást átültessük a digitális életbe, így alapozva meg a felhasználókban egy szinte önálló, azonnal működésbe lépő védelmi faktort.

Megnézem

Sorozatunk epizódjainak listája:

- *Nem tudhatod, hogy ki áll a profil mögött. A farkas is bújhat báránybőrbe.*
- *Sok lúd disznót győz... Használj több faktort fiókjaid védelméhez!*
- *Van, amikor jó, ha a cica elviszi a nyelved. Csalók ellen a hallgatás aranyat ér.*
- *Kecskére sem bíznád a káposztát...ahol lehet gyenge jelszó helyett, válts jelszómentes megoldásra!*
- *A Gombóc szuper név a kutyádnak, de nem jó jelszónak.*
- *Ajándék lónak nézd meg a fogát! Ami túl szép ahhoz, hogy igaz legyen, valószínűleg nem az.*
- *Ki lesz a gyorsabb? Ne várd meg a választ... frissíts rendszeresen!*



NEMZETI KIBERBIZTONSÁGI INTÉZET

BBA+ BESZÁMOLÓ

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

SANS DFIR Europe Summit 2026

2026. október 04.

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.





NEMZETI KIBERBIZTONSÁGI INTÉZET

A Nemzeti Kiberbiztonsági Intézet munkatársai **2026. október 04-én** részt vettek a **Prágában** megrendezésre kerülő éves **SANS DFIR Europe Summit 2026** konferencián.

A SANS Institute a világ egyik legismertebb és legelismertebb kiberbiztonsági oktatási és tanúsítványt nyújtó szervezete. Célja, hogy releváns és naprakész tudást adjon át hallgatóinak, melyet közvetlenül alkalmazhatnak a való életben a kibertér védelme érdekében – legyen szó szervezetek eszközeinek, adatainak vagy emberek biztonságáról. A SANS oktatásait, azok gyakorlati szemlélete, a szervezet tapasztalt oktatói és az iparági sztenderddé vált GIAC tanúsítványai teszik különösen értékessé a szakemberek számára világszerte.

A SANS DFIR Summit a SANS egyik kiemelt éves eseménye, amely a digitális elemzés (DF – Digital Forensics) és az incidensreagálás (IR – Incident Response) területére fókuszál.

A rendezvény célja, hogy gyakorlatorientált előadásokon és tréningeken keresztül mutassa be a legújabb technikákat, esettanulmányokat és eszközöket. A DFIR Summit lehetőséget ad a közösségépítésre is, mivel összehozza a világ vezető szakértőit, kutatóit és gyakorlati szakembereit, akik megosztják tapasztalataikat és tudásukat.

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

A konferencián elhangzott előadások rövid összefoglalója a továbbiakban olvasható.

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



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

Sarah and Kat's Adventures in Data Creation

[Kathryn Hedley@ Khyrenz Ltd; Sarah Edwards @ iVerify]

Sarah Edwards és Kathryn Hedley a digitális forenzikus képzésekhez és CTF feladatokhoz, vagyis gyakorlati kiberbiztonsági kihívásokhoz szükséges adatkészletek előállításának tapasztalatait mutatta be. Személyes, utazási példákon keresztül szemléltették, hogy az **életszerű gyakorlóanyagok elkészítése jelentős tervezést, eszközparkot és folyamatos munkát igényel**. Az előadás központi megállapítása szerint **a hiteles adatkészletek létrehozásához ténylegesen végre kell hajtani a vizsgálni kívánt tevékenységeket**, mert a mesterségesen módosított adatok eltérő nyomokat hagyhatnak, és nem feltétlenül tükrözik a valós felhasználói működést.

Az előadók megkülönböztették az egy-egy feladathoz készített, rövid időszakot lefedő adatokat a hosszabb távon fenntartott oktatási és kutatási adatkészletektől. Utóbbira Sarah Edwards egy több éve használt, fiktív felhasználói személyazonosság köré épített Apple eszközkörnyezetet mutatott be. Ebben a telefonok, számítógépek és táblagépek mellett okosóra, felhőszolgáltatások és okosotthon-eszközök is szerepeltek. A megközelítés célja az volt, hogy az elemzők az egyes eszközökön található nyomok mellett azok kapcsolatait és az adatok különböző rendszerek közötti megjelenését is vizsgálhassák. Az **eszközigényt ezért a tervezett forgatókönyvhöz kell igazítani:** egy csoportos beszélgetés vagy különböző operációs rendszerek közötti kommunikáció vizsgálata több készüléket és megfelelően kialakított felhasználói fiókokat igényelhet.

A gyakorlati példák között helyadatok, fényképek, üzenetváltások, vezeték nélküli kapcsolatok, digitális pénztárcák és egészségügyi adatok előállítása is szerepelt. Az előadók bemutatták, hogy a tényleges utazás, fényképezés vagy testmozgás egymással összefüggő digitális nyomokat hoz létre, amelyek alkalmasak összetettebb elemzési feladatok kialakítására. Külön kitértek arra, hogy az automatikus és a kézi időzónaváltás eltérően jelenhet meg az adatokban. A példák azt is érzékeltették, hogy a kívánt adatok keletkezése függhet a hálózati hozzáféréstől, a szolgáltatások regionális sajátosságaitól és a teszteléshez létrehozott fiókok működőképességétől.



A módszertani tanulságok közül kiemelkedett az előzetes tervezés, a rendszeres ellenőrzés és a dokumentálás fontossága. Egyes naplók és adatbázisok csak rövid ideig őrzik meg a szükséges információkat, ezért az **adatmentés időzítése meghatározó**. Az előadók rendszeres biztonsági mentéseket, köztes állapotmentéseket és annak ellenőrzését javasolták, hogy a végrehajtott műveletek valóban létrehozták-e a kívánt nyomokat. A tevékenységek időbélyegzett videóval, képernyőképpel vagy jegyzettel történő rögzítése lehetővé teszi a később feltárt adatok összevetését a tényleges eseményekkel.

Az előadás a **személyes adatok védelmére is felhívta a figyelmet**: egy fiktív felhasználó eszközeinek otthoni használata például a készítő valós tartózkodási helyét is felfedheti. A bemutatott tapasztalatok alapján a megbízható oktatási és tesztadatok előállítása önálló szakmai feladat, amelyhez időt, infrastruktúrát és ellenőrzési lépéseket kell rendelni. Az így kialakított adatkészletek a képzés mellett elemzési módszerek és eszközök tesztelésében is hasznosíthatók.

Find The Unfindable

[Jean-Philippe Noat @ Cellebrite]

Két emberölési ügyben is olyan, a **telefonokon megőrzött rendszeradatok segítették az események rekonstruálását**, amelyek jelentőségét a forenzikus eszközök automatikus feldolgozása nem tárta fel.

Az egyik vizsgálatban **iPhone-ok közelségét kellett megállapítani** a halálesetet közvetlenül megelőző időszakban, a másikban egy évekkel később lefoglalt **Android készülék korábbi működését és hálózati kapcsolatait kellett visszakövetni**. Az esetek rávilágítottak arra, hogy a kinyert adatok között a **szoftverek által nem értelmezett bejegyzések** is **érdemi bizonyítékot hordozhatnak**. Feltárásukhoz célzott elemzésre, az időbélyegek pontos kezelésére és a következtetések kísérleti ellenőrzésére volt szükség.

Az első esetben egy erkélyről lezuhant személy halálának körülményeit vizsgálták. A lakásban tartózkodó két másik személy azt állította, hogy az esemény idején a fürdőszobában voltak, és nem tudták, mi történt az erkélyen.

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



BBA+ BESZÁMOLÓ

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

A telefonok hagyományos vizsgálata nem tárt fel érdemi kapcsolatot az érintettek között, ezért az elemzés a készülékek fizikai közelségére utaló **Bluetooth adatokra** irányult. Az előadó az Apple rendszerbejegyzéseit, a Biome adatokat és az egységes rendszernaplókat együttesen használta fel a készülékazonosítók, az időbélyegek és a vett jelerősség összevetésére. Az elemzést a véletlenszerűsített Bluetooth címek és az egyes adatforrások nehezen értelmezhető időadatai is bonyolították.

A beszámoló szerint a naplóadatok arra utaltak, hogy az **áldozat és az egyik érintett telefonja az esemény előtt mintegy tíz másodperccel néhány méteres közelségben volt egymáshoz**. A Face ID használatára vonatkozó bejegyzés további támpontot adott a készülék használatához. A közelség becslése a Bluetooth jelerősségen alapult, amelyet az előadó is közelítő adatként kezelt. Az egymással összekapcsolt nyomok ugyanakkor megkérdőjelezték a korábbi vallomást, és olyan összefüggést tártak fel, amely a szokásos üzenet- és hívásadatokból nem volt megállapítható.

A második ügyben egy 2025-ben lefoglalt Android készüléken kellett rekonstruálni egy 2023-as emberölés körüli tevékenységet. A **gyanúsított szerint a telefon lemerült**, miközben egy, az eseményt követő WhatsApp hívás nyoma arra utalt, hogy **a készülék mégis működött**. Az automatikusan feldolgozott adatok nem adtak választ a hálózati kapcsolatra és az akkumulátor állapotára vonatkozó kérdésekre. Az áttörést egy **Survey Uploader nevű adatbázis részletes vizsgálata** hozta meg, amely alkalmazáshasználati, hálózati, energiaellátási és más rendszereseményeket is tartalmazott. Az előadó szerint ezekből megállapítható volt, hogy a telefon az emberölés idején repülő üzemmódban, körülbelül 90 százalékos töltöttséggel működött, a WhatsApp hívás pedig az áldozat Wi-Fi hálózatán keresztül zajlott. A készüléket ezt követően kikapcsolták.

Az előadás külön hangsúlyt helyezett az **időbélyegek ellenőrzésére**. Az Android adatbázisban tapasztalt eltérést az előadó az amerikai **és európai óraátállítás eltérő időpontjához kapcsolódó hibára** vezette vissza, amelynek működését azonos Android verziójú tesztkészüléken reprodukálta. A szolgáltatói hívásforgalmi adatok külső időbeli viszonyítási alapot biztosítottak. A bemutatott esetek azt szemléltették, hogy a forenzikus szoftverek eredményeinek értékeléséhez a nyers adatok vizsgálatára, több forrás



összevetésére és ellenőrizhető tesztekre is szükség lehet, különösen akkor, ha a megállapításokat később bírósági eljárásban kell alátámasztani.

Beyond Signal and WhatsApp: DFIR Investigation of Meshtastic

[Lorenzo Dina @ Bit4Law]

A **Meshtastic** hálózat egy SIM-kártya, mobilhálózat és központi szolgáltató nélkül is létrehozható üzenetküldésre alkalmas **kommunikációs hálózat**. A topológiát kis méretű, alacsony fogyasztású, LoRa rádiótechnológiát használó eszközök alkotják, amelyek egymás üzeneteit is továbbíthatják. Az ilyen hálózatok vizsgálata eltér a megszokott üzenetküldő alkalmazások elemzésétől: nincs feltétlenül felhasználói fiók vagy telefonszám, és központi szolgáltatótól sem kérhetők le a kommunikáció adatai. A bemutató azt járta körül, **milyen nyomok maradnak mégis az eszközökön és a kapcsolódó alkalmazásokban, valamint az internet felé kialakított átjárókban.**

A vizsgálat első nehézségét már az eszközök felismerése jelenti. A Meshtastic **különféle hardvereken működhet**, az egyszerű, házilag összeállított rádiós moduloktól, a kijelzővel és billentyűzettel felszerelt készülékeken át, a helymeghatározásra használt nyomkövetőkig. A hálózat részét képezhetik napelemes, tartósan telepített továbbítóállomások is. A feltárható adatok több helyen oszlanak meg: a rádiós eszköz memóriájában, a hozzá csatlakozó telefon vagy számítógép alkalmazásában, illetve az esetleges internetes továbbítás során. Emiatt az **adatgyűjtés** megtervezéséhez a készülék mellett, annak **kapcsolatait és tényleges beállításait is meg kell ismerni**.

Kiemelt figyelmet kapott az **MQTT protokoll** használata, amellyel a rádiós hálózat üzenetei internetes kiszolgálókra továbbíthatók. A bemutatott példákban nyilvánosan elérhető **MQTT kiszolgálókon** üzenetek és helyadatok is megjelentek. Az üzenettartalom értelmezését egyes esetekben az ismert vagy nyilvánosan megosztott csatornakulcsok tették lehetővé. Az előadó arra is rámutatott, hogy a nehezen értelmezhető alkalmazásbeállítások miatt a felhasználók nem feltétlenül látják át, mikor kerülnek

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



BBA+ BESZÁMOLÓ

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

adataik az internetre. **A rádiós működés és a titkosítás használata ezért önmagában nem jelenti azt, hogy a kommunikáció kizárólag a helyi hálózaton marad.**

A forenzikus elemzéshez a kapcsolódó **alkalmazások és a fizikai eszközök** egyaránt **értékes adatforrásnak** bizonyultak. A bemutatott **macOS kliens SQLite adatbázisa** olvasható üzeneteket, helyadatokat, észlelt hálózati csomópontokat és kapcsolódási információkat is tartalmazott. Az **Android alkalmazásból** konfigurációs adatok, üzenetek és csomópontlisták voltak kinyerhetők. A rádiós eszközök közvetlen vizsgálatánál USB kapcsolaton keresztüli adatmentés, illetve a flashmemória és a benne tárolt konfigurációs állományok feldolgozása került elő. Ezek összevetése segítheti a kommunikációs kapcsolatok rekonstruálását és egy lefoglalt készülék összekapcsolását a korábban megfigyelt hálózati azonosítókkal.

A módszerek alkalmazhatóságát ugyanakkor az eszköztípus, a szoftververzió és az adatmegőrzés korlátai is befolyásolják. Egyes készülékek csak kevés üzenetet tárolnak, miközben a kapcsolódó alkalmazások hosszabb előzményeket őrizhetnek meg. A fejlesztés alatt álló változások az azonosítók képzését, az adatbázisok szerkezetét és a tárolt adatok védelmét is érinthetik, ezért az **elemzési eljárásokat rendszeresen ellenőrizni kell**. Bár az előzetes programleírás konkrét ügyet helyezett kilátásba, az elhangzott bemutató elsősorban **kutatási és módszertani áttekintést** adott; az előadó a kérdésekre válaszolva jelezte, hogy közvetlen bűnügyi esettapasztalattal nem rendelkezett. A feltárt adatforrások ettől függetlenül gyakorlati kiindulópontot adtak az ilyen kommunikációs eszközök későbbi vizsgálatához.



Ghosts in the RAM: Your Phone's Secret Travel Diary

[Alex Coley @ MSAB]

A telefon akkor is hagyhat nyomot a mozgásáról, ha használója nem indít navigációt, és nem csatlakozik a környező vezeték nélküli hálózatokhoz. Az Android rendszer működése során észlelt Wi-Fi és Bluetooth eszközök adatai a memóriában is megjelenhetnek, időbélyegekkel és jelerősségi információkkal együtt. Az előadás azt vizsgálta, **hogyan használhatók fel ezek a nyomok egy készülék útvonalának rekonstruálására**, illetve annak megállapítására, hogy **két telefon mikor tartózkodhatott ugyanazon a helyen**. A bemutatott módszer a környezetben érzékelt **rádiós jelek és az ismert helyszínek összekapcsolására épült**.

A kutatásban **három Android készülék** és összehasonlításként **egy iPhone** vett részt. A telefonokat előzetesen gyári állapotba állították vissza, és nem telepítettek rájuk további alkalmazásokat, hogy csökkentsék a vizsgálatot befolyásoló tényezőket. A kísérlet helyszínén, egy angliai kisvárosban először **rádiós felmérés készült a WiGLE alkalmazással**. Ez rögzítette a környéken észlelhető hálózati azonosítókat és azok megfigyelési helyeit. Ezt követően a résztvevők párokba rendezett telefonokkal **különböző útvonalakon haladtak, egy előre meghatározott helyen találkoztak, majd ismét különváltak**. A készülékeken bekapcsolva maradt a Wi-Fi és a Bluetooth, de a teszt során nem kapcsolódtak a környező eszközökhöz, és hívást sem kezdeményeztek.

Az Android telefonok memóriájának kinyerését az **MSAB XRY eszközével** mutatták be. A **nyers adatokból saját Python szkriptekkel** keresték ki a hálózati azonosítókat, az időbélyegeket és a kapcsolódó információkat. Ezeket a helyszíni rádiós felmérés eredményeivel vetették össze, majd az egyezéseket térképen, **QGIS** segítségével jelenítették meg. A vizsgálat a hagyományos hozzáférési pontok mellett például vezeték nélküli nyomtatókhoz, kapucsengőkhöz és járművekbe szerelt kamerákhoz kapcsolódó nyomokat is felszínre hozott. Ez arra mutatott rá, hogy a helyszínek azonosításához a környezetben működő eszközök szélesebb köre is támpontot adhat.

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



BBA+ BESZÁMOLÓ

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

A kísérletben **sikerült visszakövetni a telefonok útvonalát**, azonosítani a közös találkozási helyet, és közelítően meghatározni az ott töltött időt. Az egyik készülékpár adatai több ezer megfigyelési pontot szolgáltattak a viszonylag rövid útvonalról. Az iPhone fájlrendszeréből szintén kerültek elő a térképezéshez használható hálózati azonosítók, azonban ezekhez nem álltak rendelkezésre megfelelő időbélyegek. Ennél a készüléknél ezért a helyekhez való kapcsolódást lehetett vizsgálni, a mozgás időrendjét ugyanazzal a módszerrel nem lehetett meghatározni.

A bemutató fontos korlátként kezelte a megfelelő összehasonlítási adatok szükségességét: **a memóriában talált hálózati azonosító önmagában nem ad földrajzi helyet**. A következtetésekhez helyszíni felmérésre vagy más, ellenőrizhető helyinformációra van szükség, és az ismételt látogatások elkülönítése is nehezítheti az elemzést. A tesztadatokat körülbelül két nappal a bejárás után nyerték ki, de az adatok fennmaradására nem határoztak meg általánosan érvényes időtartamot. A módszer így kiegészítő lehetőséget kínált olyan vizsgálatokhoz, amelyekben hiányoznak a hagyományos helyadatok. Egyúttal azt is szemléltette, hogy **a telefon alapvető vezeték nélküli működése a felhasználó számára kevéssé látható, utólag elemezhető mozgási nyomokat hozhat létre**.

AI-Assisted IR Without the Lies: A Browser Forensics Case

[Oren Biderman & Amnon Kushnir @ Daylight Security]

Egy meggyőzően megírt incidensjelentés is lehet teljesen téves, ha az elemzés során feltételezések válnak bizonyítottnak tekintett tényekké. A bemutatott fejlesztés éppen ilyen tapasztalatból indult: **egy nagy nyelvi modell a rendelkezésére bocsátott böngészési előzményekből hihető, de valótlan magyarázatot készített a fertőzés menetéről**. Ez indokolta a vizsgálati folyamat átalakítását, amelyben az AI feladatait szűkítették, az adatfeldolgozást előre meghatározott lépésekhez kötötték, és megkövetelték az állítások bizonyítékokra való visszavezethetőségét.



Az előadás ezen a példán keresztül mutatta be az **AI támogatott incidenskezelés gyakorlati lehetőségeit és korlátait.**

A böngésző forenzikus vizsgálatát a felhasználói megtévesztésre épülő támadások tették különösen fontossá. A tárgyalt **ClickFix módszernél** például egy weboldal látszólagos hiba elhárítására vagy ellenőrzés végrehajtására hivatkozva veszi rá a felhasználót egy káros parancs futtatására. Az események megértéséhez fel kell tárni, milyen oldalakat látogatott meg a felhasználó, honnan érkezett ezekre, és milyen műveletek követték egymást. Ez jelentős előkészítést igényelhet: azonosítani kell a megfelelő felhasználót, böngészőt és profilt, ki kell gyűjteni az adatbázisokat, majd értelmezni kell az időbélyegeket és a táblák közötti kapcsolatokat.

Az átdolgozott munkafolyamatban az AI ügynökök a végpontvédelmi rendszer által biztosított, korlátozott műveletekkel gyűjtötték össze a releváns böngészőadatokat. **Az adatbázisok feldolgozását viszont előre rögzített lekérdezések és szabályok végezték.** A nyelvi modell már az így előállított, **a riasztás időszakára és tárgyára szűkített adatokból készített időrendet és értelmezést**. A kiegészítő fenyegetési információk beszerzése is ellenőrzött szolgáltatásokon keresztül történt, hogy érzékeny vizsgálati adatok ne kerüljenek nyilvánosságra. A strukturált kimenetben külön helyet kaptak a bizonytalanságok, a további vizsgálati javaslatok és az alapul szolgáló bizonyítékokra mutató hivatkozások.

Két valós riasztás szemléltette a megoldás működését. Az egyszerűbb esetben a riasztást kiváltó **domain közvetlenül szerepelt a böngészési előzményekben**, és a kiegészítő információk **ClickFix tevékenységhez kapcsolták**. A másik esetben a **keresett domain hiányzott az előzményekből**, az időben közeli böngészés egy íjászati foglalkozásokhoz kapcsolódó keresésre vezetett. A modell **téves riasztásként való kezelést javasolt,** de **további weboldalvizsgálatot is szükségesnek tartott**. Ez utóbbi feltárta, hogy a meglátogatott oldal a háttérben kapcsolatot kezdeményezett a rosszindulatú domainnel, majd hamis ellenőrzési felületen próbálta parancsfuttatásra rávenni a felhasználót. Az eset megmutatta, miért nem elegendő önmagában a böngészési előzményekben keresett közvetlen egyezés.

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



BBA+ BESZÁMOLÓ

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

A **megbízhatóság fenntartását** korábbi ügyeken végzett teszteléssel és emberi szakmai ellenőrzéssel támogatták. A modell vagy az utasítások változtatását újraértékelés követte, mert ezek az elemzés eredményét is módosíthatják. Az **ellenőrző szakember** feladata annak megállapítása volt, hogy az elkészült magyarázatot **valóban alátámasztják-e a rendelkezésre álló adatok.** A bemutatott, éles működésben is alkalmazott megoldás így a jól körülhatárolt részfeladatok gyorsítására épült, miközben a következtetések ellenőrzése és a végleges jelentésért viselt felelősség a szakembereknél maradt.

A Pinch of Salt Typhoon: Dissecting a Cross-Platform Espionage Intrusion

[Roey Gideon Shua @ Check Point Software Technologies]

Egy általános kártevőriasztás egy ázsiai, állami tudományos szervezet ellen végrehajtott, összetett kémkedési művelet feltárásához vezetett. A vizsgálat **Linux és Windows rendszereken átívelő támadói jelenlétet azonosított**, amelynek célja hitelesítési adatok és érzékeny tudományos információk megszerzése volt. A beszámoló a feltárás sorrendjében követte az eseményeket: minden új nyom további rendszerekhez, eszközökhöz és támadási lépésekhez vezette az elemzőket. A szervezet Windows gépeinek csak egy részén működött végpontvédelem, ráadásul kizárólag észlelési módban, így a riasztások **nem akadályozták meg a támadó tevékenységét**.

A kiindulópont egy **három állományból álló, DLL betöltéssel működő kártevőegyüttes** volt. Egy átnevezett, digitálisan aláírt program rosszindulatú DLL-t töltött be, amely egy további állományból fejtette vissza és indította el a támadói kódot. A kezdeti adatok alapján felmerült, hogy a kártevő egy legitim Windows folyamatba rejtőzött, de ennek igazolásához memóriavizsgálatra volt szükség. A **Velociraptor és a HollowsHunter** együttes alkalmazásával több gépen is **sikerült feltárni a befecskendezett kódot**. A Windows környezetben emellett távoli hozzáférést előkészítő, rendszerleltárt készítő, hitelesítési adatokat megszerző és billentyűleütéseket rögzítő eszközök is előkerültek.



A **Linux** rendszerek felé egy **bejelentkezési esemény** terelte a vizsgálatot. A Windows naplóban szereplő forrás IP cím egy Linux szerverhez tartozott, miközben a hitelesítést kezdeményező gép neve Windows munkaállomásra utalt. Más hálózati nyomokkal együtt ez arra utalt, hogy a hozzáférés egy köztes rendszeren keresztül, tunneling hálózati kapcsolat használatával valósulhatott meg. A nagy teljesítményű tudományos szervereken a hatalmas adatmennyiség miatt, a teljes fájltartalom átvizsgálása helyett, **először a fájlok metaadatait elemezték**. A támadó a módosítási időket korábbi dátumokra állította, hogy az állományok beleolvadjanak a környezetükbe, de a metaadatok változási ideje árulkodó maradt. Az időadatok és a végrehajtási jogosultságok összevetése így keresési mintává alakította az elrejtési kísérletet.

A Linux környezetben **legitim rendszerszolgáltatásnak álcázott** hátsó kapukat, hálózati továbbítást biztosító eszközöket és módosított SSH programokat azonosítottak. Az utóbbiak hitelesítési adatokat gyűjtöttek, valamint a szokásos naplózást megkerülő hozzáférést is lehetővé tettek. Egy moduláris hátsó kapu a kiegészítőit betöltés után eltávolította a fájlrendszerből, ami tovább növelte az élő memóriavizsgálat jelentőségét. A rekonstruált támadási folyamat szerint **a Linux rendszereken megszerzett hozzáférések és hitelesítési adatok segítették a Windows környezetbe történő továbblépést.** A gyűjtés belső információkra, böngészőadatokra és érzékeny tudományos modellezési állományokra is kiterjedt, amelyeket a támadó az elszállítás előkészítéséhez összecsomagolt.

A kártevők kódja, közös kriptográfiai adatai és vezérlési infrastruktúrája egy szélesebb nemzetközi kampányhoz is kapcsolatot adott. Az előadó a tevékenységet a Check Point által **Copper Dragon** néven követett szereplőhöz kapcsolta, és ismertette a **FamousSparrow**, illetve **Salt Typhoon** elnevezésekhez kötődő összefüggéseket. A vizsgálat gyakorlati értékét a végponti és hálózati észlelések, a memóriavizsgálat, a fájlmetaadatok elemzése és a fenyegetési információk együttes felhasználása adta. Az így feltárt hozzáférési útvonalak és fennmaradást biztosító eszközök ismeretében lehetett előkészíteni az **incidens elhatárolását és a támadói jelenlét megszüntetését**.

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



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

Cache Me If You Can

[Elliot Glendye @ Control-F Digital Forensics]

Egy iPhone-on megtalált kép jelenléte önmagában nem bizonyítja, hogy a felhasználó elküldte, fogadta vagy tudatosan elmentette azt. Ezt a bizonyítási problémát állította középpontba az előadás, amely egy brit **digitális forenzikus egység** megkeresésből indult. A vizsgálók egy rendszerkönyvtárban talált képek eredetét és jelentőségét szerették volna tisztázni, mert az adott helyen jogellenes tartalom is előkerült. A kutatás azt tárta fel, **hogyan kapcsolhatók össze a háttérben létrejött képfájlok az alkalmazásokhoz kötődő rendszerbejegyzésekkel**, és meddig terjednek az ezekből levonható következtetések.

A vizsgált **Intents Images könyvtár** gyorsítótárra jellemző sajátosságokat mutatott: eltérő méretű, gyakran négyzetes képek és számos másolat szerepelt benne. Az állományok UUID alapú, egyedi azonosítót tartalmazó fájlnevet kaptak, és PNG formátumban kerültek tárolásra. A könyvtár elnevezése az **iOS App Intents keretrendszeréhez** adott támpontot, amely lehetővé teszi, hogy az alkalmazások műveleteket és kapcsolódó adatokat tegyenek elérhetővé a rendszer számára. Ezek a műveletek például a **Parancsok alkalmazáshoz vagy a Siri használatához is kapcsolódhatnak**. Lényeges körülmény, hogy egyes műveletleírásokat maga az alkalmazás hoz létre, ezért jelenlétük nem feltétlenül jelent felhasználó által kialakított automatizálást vagy végrehajtott műveletet.

Két fiktív felhasználóval az összefüggések feltárásához dokumentált tesztadatok készültek, majd kinyerték a telefon teljes fájlrendszerét. A képfájlok azonosítóit a **Biome kapcsolódó App Intents** bejegyzéseiben keresték meg. A SegB **állományokban tárolt, Protobuf formátumú adatok** kibontásával időadatok, alkalmazásazonosítók és a képek tárolási helyére mutató hivatkozások váltak értelmezhetővé. A bemutatott módszer így összekapcsolta a gyorsítótárban talált képet az azt létrehozó alkalmazás rendszerbejegyzésével. Az elemzéshez ugyanakkor az egymásba ágyazott adatszerkezetek **részletes vizsgálatára volt szükség,** mert a forenzikus eszközök támogatása és az összetartozó adatok automatikus összerendelése korlátozott volt.



A teszt egyik meghatározó eredménye egy **Signalhoz kapcsolódó kép eredetének azonosítása volt**. A rendszerbejegyzés **üzenetküldéshez kötődő művelettípust** jelzett, a dokumentált használat azonban egy szavazás létrehozásához kapcsolódott. A gyorsítótárban megjelent kép a **másik felhasználó profilképe** volt, amelyet a rendszer tárolt el. Nem olyan médiatartalomról volt szó, amelynek elküldését vagy fogadását a feltárt bejegyzés igazolta volna. A példa világosan megmutatta, hogy egy művelet elnevezése és a hozzá kapcsolódó kép együtt sem elegendő az üzenetküldés tényének megállapításához.

A kutatás alapján az ilyen nyomokból **meghatározható lehet a képhez kapcsolódó alkalmazás és rendszeresemény**, de a **konkrét felhasználói cselekmény bizonyításához további adatok szükségesek**. Az előadás azokat az eredményeket is értékesnek tekintette, amelyek kizárnak egy kezdetben valószínűnek tűnő értelmezést. A kapcsolódó Biome bejegyzések bemutatott, körülbelül 28 napos megőrzési ideje az időben történő adatgyűjtés jelentőségére is rámutatott. A gyakorlati tanulság az volt, hogy a képek értékelésekor a fájl tartalma mellett annak keletkezési körülményeit, rendszerbeli szerepét és más adatforrásokkal való kapcsolatát is vizsgálni kell.

When Evidence Lies: AI-Fabrications in Litigation

[Calum Baird @ Systal Technology Solutions]

A generatív mesterséges intelligencia **jelentősen csökkentette a hitelesnek látszó hamisítványok előállításához szükséges időt és szakértelmet**. Módosított dokumentumok, mesterségesen létrehozott üzenetváltások és szintetikus tanúvallomások már tényleges bírósági ügyekben is megjelentek. Az előadás ezek felismerését vizsgálta, különös figyelemmel arra, **hogyan ellenőrizhető a digitális bizonyíték eredete és megbízhatósága**, mielőtt az érdemben befolyásolja a döntéshozatalt. A bemutatott megközelítésben a technikai elemzés mellett a független megerősítés és a bizonyíték keletkezési körülményeinek feltárása is meghatározó szerepet kapott.

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



BBA+ BESZÁMOLÓ

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

Két eltérő problémakört különítettek el: a **nyelvi modellek által kitalált jogi hivatkozásokat** és a **bizonyítékként benyújtott hamisított tartalmakat**. Az előbbiek ellenőrzését segíti, hogy a hivatkozott döntések és jogi szövegek létezése megfelelő adatbázisokban vizsgálható. A képek, videók és dokumentumok hitelességének megítélése összetettebb, különösen akkor, ha az eredeti állomány helyett csak képernyőkép vagy továbbított másolat áll rendelkezésre. A felidézett ügyekben módosított bizonylatok, szokatlan megjelenésű üzenetképek és mesterséges tanúvallomást tartalmazó videó is szerepelt. Több esetben a gyanút a tartalom nyelvi hibái, a felület következetlenségei vagy a beszéd és az ajakmozgás eltérései keltették fel.

A **forenzikus ellenőrzésben** a metaadatok és a tartalomhoz fűzött magyarázat összevetése is hasznosnak bizonyult. Egy példában a videó rendellenes megjelenését Apple Intelligence használatával indokolták, miközben az állomány metaadataiban olyan régi iPhone modell szerepelt, amely ezt a magyarázatot nem támasztotta alá. Az ilyen **ellentmondások további vizsgálati irányt adhatnak**, de önmagukban nem feltétlenül bizonyítják, hogy a tartalom AI-al készült. A hamisítás felismerése és az előállítás konkrét módszerének azonosítása ezért külön kérdésként jelent meg.

Az **automatikus deepfake-detektorokkal kapcsolatban** az előadó **óvatosságot javasolt**. A bemutatott kutatások szerint a kontrollált tesztadatokon mért teljesítmény jelentősen eltérhet a változatos, valós környezetből származó anyagokon elért eredményektől. A generáló modellek fejlődése, valamint a képek „újramentése”, tömörítése vagy ismételt képernyőképként történő rögzítése is befolyásolhatja az észlelhetőséget. A **metaadatokba ágyazott eredetjelzések elveszhetnek**, ezért hiányuk nem igazolja a hitelességet. A zajmintázatok és más, szemmel nem látható jellemzők elemzése további támpontot adhat, de a bemutató ezekre sem tekintett általánosan biztos döntési módszerként.

A gyakorlati vizsgálat alapját az eredet, a megjelenés és a független adatforrások összevetése adta. Egy híváslistáról készült képernyőkép például a telefonból kinyert hívásadatokkal vagy szolgáltatói nyilvántartással ellenőrizhető; egy dokumentum esetében pedig lényeges, hogy közvetlenül a kibocsátótól vagy az ügyben érdekelt



személytől származik-e. Az azonos készülékről és alkalmazásból származó, ismert eredetű állományok összehasonlítási alapot biztosíthatnak. Ha az eredmények nem egyértelműek, a szakvéleményben az észlelt eltéréseket és a következtetések korlátait kell pontosan megfogalmazni. Az előadás a **digitális bizonyítékok értékelését** így több forrásra támaszkodó, ellenőrizhető szakértői feladatként mutatta be, amelyben az automatikus eszközök eredménye is értelmezést és megerősítést igényel.

Agentic Triage, Unlocking New Possibilities

[Matias Bevilacqua @ Mandiant (Google)]

Nagyobb incidensek során jelentős elemzői kapacitást köt le az érintett gépek adatainak átvizsgálása, a támadói események kiválasztása és az eseménysor összeállítása. A bemutatott fejlesztés ezt a munkát **több, összehangolt AI ügynökkel támogatta**: a rendszer forenzikus adatokat, kompromittálódásra utaló indikátorokat és vizsgálati háttérinformációkat kapott, majd megjelölte a támadói tevékenységhez kapcsolódó eseményeket, és időrendi beszámolót készített. A fejlesztés központi követelménye az volt, hogy az **eredmény minden állítása visszakövethető legyen** a felhasznált bizonyítékokhoz és az azt előállító vizsgálati lépésekhez.

A tapasztalatok szerint a legnagyobb kihívást az ügynökök működésének szabályozása, az adatmennyiség kezelése és a folyamat átláthatósága jelentette. A fejlesztő ezért **erősen korlátozott felépítést** választott, amelyben az ügynökök meghatározott eszközökkel és feladatkörökben dolgoztak. A **központi koordinátor** átlátta a vizsgálat egészét, de maga nem végzett elemzést: feladatokat osztott ki, majd az eredmények alapján jelölte ki a következő lépéseket. **Külön ügynökök** foglalkoztak a fájlok beszerzésével, tartalmuk vizsgálatával, a kártevőelemzéssel és a minőség ellenőrzésével. Ez a felépítés a költségek, a hibák és az ismételhetőség kezelését is segítette.

Konkrét példák mutatták be, hogy a megbízhatósághoz az utasítások pontosításán túl **technikai ellenőrzésekre is szükség van**. A hosszú eseményazonosítók másolásakor a

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



BBA+ BESZÁMOLÓ

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

nyelvi modellek időnként hibáztak, ami téves bizonyíték megjelöléséhez vezethetett. Ennek csökkentésére rövid, feldolgozási egységenként kiosztott azonosítókat alkalmaztak, majd ellenőrző számjeggyel egészítették ki őket. A bonyolult lekérdezések előállítását külön tesztelési folyamat támogatta, amelyben az ügynökök a tényleges adatforráson próbálták ki a lekérdezéseket, és a hibák alapján javították az útmutatást. A megoldások azt szemléltették, hogy **a modell hibáit a munkafolyamatnak észlelnie és kezelnie kell**.

A **nagy adatmennyiség feldolgozásához az eseményeket kisebb egységekre bontották**, részben párhuzamosan elemezték, majd összesítették. A rendszer mintavételezéssel, az ismétlődő naplóüzenetek csoportosításával és a fájlútvonalak tömörített megjelenítésével segítette a háttértevékenység kiszűrését. Az időrendi beszámoló fokozatosan bővült, hogy az egyes részletek összefüggő történetté álljanak össze. A kódfuttatást igénylő fájlelemzés elkülönített környezetben történt, míg a kártevővizsgálatot erre szolgáló elemzési szolgáltatás támogatta.

Az **alkalmazás bevezetésére fokozatos átmenetet javasoltak**. Elsőként a már kiválasztott eseményekből készülő összefoglalók írása automatizálható. Ezt követheti az emberi vizsgálat független megismétlése AI-jal, majd a két eredmény összevetése, amely az elemzői hiányosságokat és az ügynök hibáit egyaránt felszínre hozhatja. A következő szakaszban az AI végezheti az első elemzést, az ember pedig a minőség ellenőrzésére összpontosíthat. Távolabbi lehetőségként a folyamatos feldolgozás és a korábban vizsgált gépek újraellenőrzése is felmerült, amikor új indikátor válik ismertté. Az előadás ugyanakkor nyitott kérdésként kezelte, **hogyan őrizhető meg az új szakemberek gyakorlati tudásszerzése**, ha a kezdő elemzői feladatok jelentős részét automatizálják, az ügynökök ebben oktatási és visszajelzési eszközként is szerepet kaphatnak.



Closing Keynote: Scaling, Failing, Improving — Two Decades of DFIR Practice

[Heather Barnhart @ SANS Institute]

A digitális forenzika és az incidenskezelés fejlődését a **szakmai hibákból levont tanulságok** éppúgy alakítják, mint az új technológiák. A záróelőadás közel huszonöt év személyes tapasztalatain keresztül mutatta be, hogyan befolyásolja a vizsgálatok megbízhatóságát az időnyomás, az előzetes feltételezés, a hiányos ellenőrzés és a túlzott feladatvállalás. A visszatérő üzenet az volt, hogy a **szakembernek a bizonyítékokból kell kiindulnia**, akkor is, ha azok nem támasztják alá a megrendelő, a nyomozó vagy a saját korábbi elképzelését.

A felidézett esetek kézzelfoghatóvá tették a **dokumentálás és a szakmai kontroll** jelentőségét. Egy pályakezdőként végzett bizonyítékgyűjtésnél egy kamera sorozatszámának elmaradt rögzítése okozott komoly bizonytalanságot. Egy másik ügyben a felületes jelentésellenőrzés miatt titkosítottnak minősítettek olyan alkalmazásadatokat, amelyek valójában csak kódoltak voltak. Az esetek azt szemléltették, hogy egy egyszerű adminisztratív hiányosság vagy technikai félreértés is érdemben befolyásolhatja a további vizsgálatot. A hibák feltárásához ezért olyan **szakmai környezetre van szükség**, amelyben az ellenőrzés és a korrekció természetes része a munkának.

Külön hangsúlyt kapott az **elfogultság veszélye**. Egy védelem számára végzett vizsgálatban a feltárt kommunikáció megkérdőjelezte azt a történetet, amelyet az előadó kezdetben maga is elfogadott. Más ügyekben ígéretesnek tűnő digitális nyomok értelmezéséhez további kutatás kellett, vagy a remélt kapcsolatot nem sikerült kimutatni. Ezekből az a szakmai elv következett, hogy a **bizonytalanságot nyíltan jelezni kell**: az „ezt még nem tudjuk” vagy a „további vizsgálat szükséges” megállapítás indokolt lehet, és nem helyettesíthető magabiztos feltételezéssel. A **szakmai kapcsolatok és a független kollégák bevonása** szintén segítheti az ismeretlen nyomok ellenőrzését.



BBA+ BESZÁMOLÓ

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

A vezetői tapasztalatok között a fenntartható munkavégzés, a **egyértelmű határok és a tudásátadás** szerepelt. A folyamatos rendelkezésre állás és a túl sok vállalás kimerüléshez vezethet, ami az elemzés minőségére is hatással lehet. A munkatársak képzését és fejlődését ezért támogatni kell, a kezdőknek pedig meg kell érteniük az adatok tárolását és keletkezését, mielőtt kizárólag egy eszköz kezelőfelületére támaszkodnak. A szakmai önállóság részeként az előadó annak fontosságát is kiemelte, hogy az elemző ne adja a nevét olyan jelentéshez vagy bizonyítékbemutatáshoz, amelynek megalapozottságával nem ért egyet.

A mesterséges intelligencia alkalmazása ugyanezeket az alapelveket tette ismét aktuálissá. Heather Barnhart az AI-t olyan eszközként értékelte, amely megfelelő szakértelem mellett segítheti a munkát, de **nem veheti át a bizonyítékok hitelességének végső ellenőrzését**. Különösen **kockázatosnak** tartotta az olyan felhasználást, amely **visszafordíthatatlan műveleteket érint**, vagy amelynek eredményét az alkalmazó nem képes önállóan ellenőrizni. Ismertette a digitális forenzikára és az incidenskezelésre külön kialakított, közösségi továbbfejlesztésre szánt AI ajánlásokat is. A felelős alkalmazás feltételeként az adott feladat ismerete, az AI közreműködésének átláthatósága és az eredmények következetes ellenőrzése jelent meg, miközben a szakmai felelősség továbbra is az elemzőnél marad.