NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 25. hét

HÍREK

- Több mint 46.000 Grafana-példány van kitéve egy fiókeltérítési sebezhetőségnek
- Koordinált támadások az Apache Tomcat Manager ellen
- OpenAI jelentés: AI eszközöket használnak rosszindulatú célokra
- Hogyan használják ki a Google OAuth-ot a kiberbűnözők?
- Egy rejtett fenyegetés az Android rendszerekben

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás

CTI ELEMZÉS

- Végpontvédelem és annak megvalósítása I. Technológiai alapok és veszélyforrások

BESZÁMOLÓ

- FIRST Cyber Threat Intelligence Conference 2025 Berlin, Németország

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági
HÍREK

Több mint 46.000 Grafana-példány van kitéve egy fiókeltérítési sebezhetőségnek
(bleepingcomputer.com)

Több mint 46.000 interneten keresztül elérhető Grafana-példány továbbra sem rendelkezik frissített verzióval és így ezek egy kliensoldali open redirect sebezhetőségnek vannak kitéve, amely Ülehetővé teheti rosszindulatú bővítmények futtatását és akár a felhasználói fiókok átvételét is. **Bővebben...**

Koordinált támadások az Apache Tomcat Manager ellen
(gbhackers)

A **GreyNoise Intelligence** kiberbiztonsági kutatói egy jelentős, globálisan elosztott támadási kampányt azonosítottak, amely az **Apache Tomcat Manager** alkalmazás adminisztrációs felületeit célozza meg. **Bővebben...**

OpenAI jelentés: AI eszközöket használnak rosszindulatú célokra
(knowbe4.com)

Az OpenAI nemrég közzétett jelentésében a mesterséges intelligencia által **támogatott rosszindulatú tevékenységeket vizsgálja**. A dokumentumban kiemelik, hogy a kiberbűnözők egyre gyakrabban használnak mesterséges intelligencia eszközöket, különösen social engineering támadásokhoz. **Bővebben...**

Hogyan használják ki a Google OAuth-ot a kiberbűnözők?
(pcw) (c/side)

A c/side kiberbiztonsági cég nemrég egy különösen rafinált kliensoldali támadást azonosított a **parts[.]expert** nevű Magento-alapú e-kereskedelmi weboldalon. **Bővebben...**

Egy rejtett fenyegetés az Android rendszerekben
(gbhackers)

Az **Androidos** eszközök és alkalmazások védelme különösen nagy kihívásokba ütközik, mivel a támadók egyre **kifinomultabb módszerekkel** próbálnak meg hozzáférni az érzékeny információkhoz. Az új támadási vektorok között szerepelnek többek között a gyártók által biztosított **OEM** (Original Equipment Manufacturer) **engedélyek** és az alkalmazások, amelyek **túlzott rendszerhozzáférést** kérnek a **felhasználók tudta nélkül**. **Bővebben...**

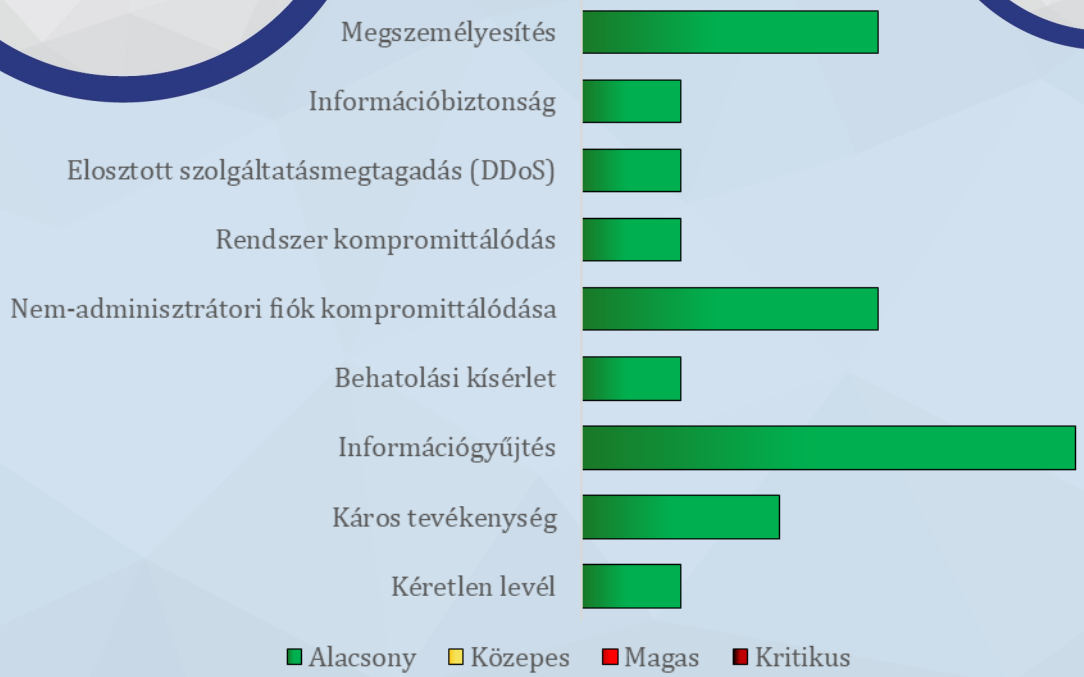
További hírekért, látogasson el **weboldalunkra**!

Statisztikai Adatok

2025.06.13.-2025.06.19.

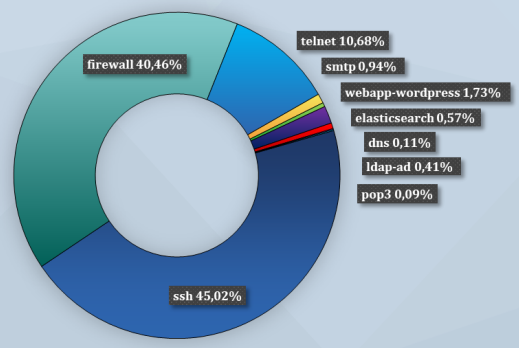
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

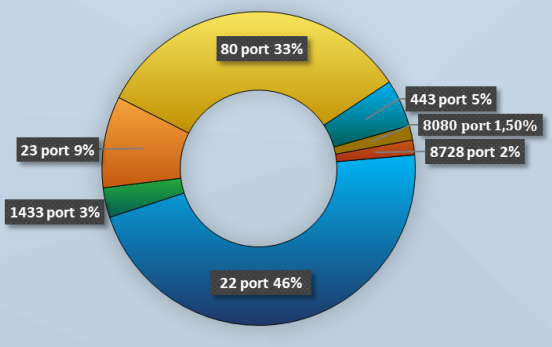
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:





További érdekességekért, látogasson el **weboldalunkra**!

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

Végpontvédelem és annak megvalósítása I. Technológiai alapok és veszélyforrások

Jelen dokumentum célja, hogy **felhívja a figyelmet a végpontvédelem fontosságára** azáltal, hogy bemutatja a végpontok típusait, azokat a veszélyeket és fenyegetéseket, amelyekkel a végpontvédelem során nézünk szembe, illetve ismerteti azokat a technológiákat és eszközöket, amelyekkel csökkenthetők a kockázatok.

Elolvasom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!

FIRST Cyber Threat Intelligence Conference 2025
Berlin, Németország

2025. április 21. – április 23.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi 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-3.1.2-24-2024-00004. sz. pályázat részeként

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

A Nemzeti Kibervédelmi Intézet munkatársai részt vettek a **2025. április 21-23. között Berlinben megrendezésre kerülő éves FIRST Cyber Threat Intelligence Conference 2025** eseményen.

A Forum of Incident Response and Security Teams (FIRST) 2016 óta évente megrendezésre kerülő konferenciájának célja a **kiberfenyegetettségi elemzés** (Cyber Threat Intelligence) területén dolgozó **szakértők tudásmegosztása**.

A konferencia a **CTI aktuális kihívásait**, **gyakorlati megközelítéseit** és **fejlődési irányait** járta körül. Esettanulmányokon és technikai bemutatókon keresztül kaptak a résztvevők átfogó képet a CTI szerepéről. A konferencián kiemelt fókuszt kapott az automatizáció, a forráskritikus elemzés, a geopolitikai kockázatok hatásai, valamint a CTI integrációja más biztonsági funkciókkal.

Kiknek ajánlott a beszámoló megismerése?

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

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

Egy évtized dekódolása - 10 év alkalmazott CTI gyakorlat

(Andreas Sfakianakis, Rebekah Brown)

Az előadás a **kiberfenyegetettségi elemzés** (Cyber Threat Intelligence, továbbiakban: CTI) **elmúlt tíz évének fejlődését mutatta be**, amely során a szakterület egy kezdeti, feltörekvő pozícióból a kiberbiztonsági védekezés egyik kulcselemévé vált. A prezentáció alapját a **SANS intézet által végzett CTI felmérések** eredményeinek a tízéves adatsora képezte, amely alapján részletes elemzést kaphattunk arról, hogyan reagált a CTI a fenyegetések, technológiák és szervezeti prioritások változásaira az évek alatt.

Az előadó **három fejlődési szakaszt** ismertetett:

- Az **„alapozó évek”** (2015–2018), amikor a figyelem középpontjában a **reaktív megközelítés**, a **nyers „információ”** és az **alapvető gyakorlatok meghonosítása** állt. Ebben az időszakban kezdtek megjelenni az első CTI platformok és „termékek”, amelyek már valamelyest túlmutattak az egyszerű információk halmazán és az összefüggéseket is kereső elemzések irányába kezdtek elmozdulni. Ebben az időszakban kezdtek el megjelenni a SIEM rendszerekkel való integrációk is.
- Az **érési szakasz** (2019–2021), amelyet a **taktikai CTI mélyebb integrációja és alkalmazása** jellemzett. Ebben az időszakban a pandémia miatt **megnőtt a RaaS** (Ransomware as a Service – Szolgáltatásként Terjesztett Zsarolóvírus) szolgáltatások **népszerűsége**, ami magával hozta a CTI felértékelődését is. Ebben az időszakban kezdtek el a CTI szakemberek **iparági sztenderdeket felállítani**, a **sajtót/médiát is adatforrásként beépíteni** és az információkat egyre gyakrabban **egymás között megosztani.**
- A **modern korszak** (2022–2024), amikor a **CTI már aktívan elkezdte alkalmazni a mesterséges intelligenciát**, figyelembe vette a geopolitikai hatásokat is az informatikai és szakmai környezeten túl, és előtérbe helyezte a stratégiai megközelítést. Ebben az időszakban kezdett el igazán **bővülni a CTI közösség** és egyre több lehetőség, illetve szakmai fórum alakult ki a kollaborációra és az információk, „best practice”-ek, illetve a „know how”-k megosztására.

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

Az éretlenség szórakoztató is lehet – kivéve, ha CTI-ról van szó

(Gert-Jan Bruggink, Andreas Sfakianakis)

Az előadás során bemutatásra került egy új CTI érettségi modell a **Cyber Threat Intelligence Cabality Maturity Model**, vagyis a **CTI CMM** (https://cti-cmm.org/). Csakúgy, mint a CSIRT-ek esetében, a CTI csapatok számára is elérhetőek különféle érettségi keretrendszerek, melyek célja, hogy az adott csapat képességei és eszközei egy **meghatározott rendszer szerint fejlődhessenek, bővülhessenek**. Az előadó egy ilyen CTI érettségi keretrendszert mutatott be. A CMM modell alapján történő CTI „fejlődési pálya" a folyamatok kialakításán és a „**Felmér – Tervez – Végrehajt/Bevezet – Mér/Visszajelez**" lépéseken végighaladva, azok fejlesztésén alapszik.

Számháború: A kiberfenyegetések rangsorolása számokkal

(Scott Small)

A CTI szakemberek egyetértenek abban, hogy **a fenyegetéseket száma egyre csak nő**, a CTI erőforrások pedig limitáltak, így **priorizálni** kell. A rangsorolásra azonban különböző megközelítési módok léteznek. Az előadás azt a kérdést járta körül, hogy **miként lehet a kiberfenyegetéseket objektíven rangsorolni**, különösen olyan összetett jelenségek esetén, mint az APT csoportok vagy zsarolóvírus-kampányok. A fenyegetéseket valamilyen módon normalizálni és számszerűsíteni kell, hogy utána összehasonlítani/ rangsorolni lehessen őket. Erre a felvetett problémakörre kínál megoldást a Tidal Security módszere, amely lényegében egyfajta **fenyegetettség rangsorolási keretrendszer**.

A kockázatelemzési modell részletes leírása az alábbi linken érhető el.

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

A modell lényege a gyakorlatban, hogy egy adott **fenyegetettség súlyossága**, az a támadó aktor **szándékának**, **képességeinek** és **lehetőségeinek** a szorzatából épül fel. (**Threat = Intent x Capability x Opportunity**). Az előadó kiemelte, hogy bár kiindulási pontnak jó ez a kockázatelemzési mátrix, a szakértők véleményét is figyelembe kell venni. A bemutató második felében az előadó áttekintést nyújtott a nyilvánosan elérhető forrásokról, amelyek használhatóak a kiberfenyegetések rangsorolásához (AlienVault OTX, Palo Alto Unit42 Playbooks, Crowdstrike Threat Landscape).

Az előadás prezentációja az alábbi linken érhető el.

Navigálás a háborús ködben: geopolitikai feszültségek értelmezése CTI szempontból

(Simone Kraus)

Az előadás **3 geopolitikai konfliktuson** (Oroszország - Ukrajna, Irán-Hamasz-Izrael, Kína – Tajvan) keresztül mutatta be a geopolitika bevonásának fontosságát a CTI elemzésekbe. Az előadás a **PESTLE** (Politikai, Gazdasági, Társadalmi, Technológiai, Környezetvédelmi, Jogi) és a **DIMEFIL** (Diplomáciai, Információs, Katonai, Gazdasági, Pénzügyi, Hírszerzési, Rendészeti) analitikai keretrendszerek bemutatásával kezdődött, amelyeket gazdasági, katonai vagy politikai döntéshozatalhoz használnak az államok.

Az előadó szerint az „informatikai hadviselés” egyfajta „**soft power**” az államok kezében, amelyet az állami beavatkozási lehetőségek kiszélesítése (politikai-, katonai-, gazdasági kémkedés, támadás) érdekében használhatnak. Az előadás során bemutatásra kerültek a 3 említett konfliktusban résztvevők támadási kapacitásai és szereplői. Tovább figyelmet kaptak azok az új, korábban nem követett fenyegető csoportok, mint például a GRU 29155-ös egység operátorai, akik az orosz-ukrán konfliktus során jelentek meg.

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

A geopolitikai hírszerzés alkalmazása a magánszektorban – tanulságok egy több iparágat érintő kutatásból

(Brian Hein, David Hunt, Lukas Vaivuckas)

A felszólalók egy több iparágra kiterjedő kutatás kvalitatív eredményeit mutatták be, amely azt vizsgálta, hogy a különböző szektorokban működő vállalatok hírszerzési csapatai **miként használják fel az elemzéseket a geopolitikai kockázatok kezelésére a napi működés során**.

A kutatás alapját 2024 nyarán a privát/piaci szférában tevékenykedő cégekkel készített interjúk adták. Az előadás betekintést adott abba, hogyan alkalmazzák az intelligencia-alapú megközelítést az üzleti döntéshozatalban és válságkezelésben – különös tekintettel arra, miként lehet előnyre szert tenni ilyen bizonytalan környezetben.

Jellemzően az ilyen vállalatoknál dolgozó CTI csapatok kétféleképpen kerülnek kapcsolatba geopolitikai eseményekkel:

- **Katalizátor események révén** – olyan, jelentős bizonytalanságot kiváltó történések kapcsán, amelyekhez a szervezetnek alkalmazkodnia kell. A magánszektor szereplői ezekre általában nem közvetlen reagálással (pl. evakuálással) válaszolnak, hanem például erőforrás-átrendezéssel, célkitűzések (KPI-ok) módosításával vagy üzleti prioritások újratervezésével.
- **Közös eszközök és integrált munkafolyamatok révén** – a CTI-feladatkörök egyre szorosabban integrálódnak az üzleti működésbe. Az előadók ezt szemléltették azzal a példával, hogy egy CTI-elemző napja során egyszerre találkozik egy Kína–Tajvan gazdasági kapcsolatait érintő elemzéssel és a havi rendszeres „Patch Kedd” feladataival, jelezve a geopolitikai és technikai kockázatok párhuzamos kezelésének szükségességét.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

SOC elemző nappal, CTI fejlesztő éjjel – egy CTI program bevezetésének tanulságai

(Bianka Bálint)

Az előadás gyakorlati példákon keresztül ismertetett **három különböző CTI-integrációs megközelítést**, kiemelve azok előnyeit, valamint a bevezetésük során felmerülő kihívásokat. A modellek a szervezeti elhelyezkedés és a kialakítás módja szerint különültek el:

1. Egy hírszerzési elemző (vagy csapat) a **saját módszereivel elkezd tevékenykedni** kiberbiztonsági területen
2. A felülről szerveződő „**akadémikus megközelítés**”
3. A lentről felfelé épülő „**agilis**” (a szoftverfejlesztésben gyakran használt keretrendszer) megközelítés

A prezentáció alapját a CTI program **bevezetési és korai fázisai során szerzett tapasztalatok** képezték, különösen arra fókuszálva, hogy még alapos tervezés, az érintettek részletes felmérése és bevált gyakorlatok alkalmazása mellett is miként vallhat kudarcot egy kezdeményezés.

Feltártuk, hogy **milyen hibalehetőségek** rejlenek még egy jól strukturált CTI programban is, illetve azt is, hogyan lehet egy **alulról szerveződő, kisebb CTI csapat mégis sikeresebb** bizonyos területeken, mint egy érettebb, központosított, különálló szervezeti egység. Az előadás közvetlen tapasztalatokra is épített, különösen azokra az esetekre, amikor a gyakorlati munka és a fejlesztés párhuzamosan zajlik – például, amikor valaki nappal biztonsági operációs központban (SOC) dolgozik, este pedig CTI integrációs rendszerek fejlesztésén.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

Szakadékok áthidalása a CTI-ben: a PIR-ek szerepe a fenyegetésalapú biztonságban

(Keith Swagler, Ondra Rojcik)

„Az előadás annak lehetőségeit vizsgálta, **hogyan alkalmazhatók a kiemelt hírszerzési igények** (Priority Intelligence Requirements, PIR-ek) hatékonyan **a napi szintű CTI-, SOC- és kibervédelmi műveletekben**. Bár a szakemberek többsége elismeri ezek stratégiai jelentőségét, gyakran tekintenek rájuk mint akadémikus, az operatív valóságtól elszakadt gyakorlatokra.

A bemutató rávilágított arra, hogy ha a PIR-eket jól strukturált módon határozzák meg és vezetik be, akkor nemcsak a CTI munka fókuszáltságát javítják, hanem megerősítik a szervezet teljes információbiztonsági stratégiáját azáltal, hogy azt a valós, aktuális fenyegető szereplőkhöz és a vállalat specifikus rizikófaktoraihoz igazítják.

Az előadás egy rövid gyakorlati összefoglalót is adott a PIR-ek kidolgozásához és az aktív alkalmazásuk elkezdéséhez:

- A szervezet PIR-eken alapuló **fejlesztési lehetőségek** ismertetése
- **Prioritást élvező fenyegető szereplők azonosítása**
- Ezen szereplőkhöz tartozó **fontos TTP-k** (taktikák, technikák, eljárások) **meghatározása**
- A **TTP-k alkalmazása** detekciós szabályokban, threat huntingban, red teamingben, valamint a biztonsági kontrollok frissítésében

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

Sérülékenységek értékelése a Fediverse aktivitási adatai alapján

(Cédric Bonhomme, Alexandre Dulaunoy)

Az előadás azt vizsgálta, hogyan lehet közösségi aktivitás alapján már a **hivatalos publikáció előtt értékelni és priorizálni a sérülékenységeket**. A tapasztalatok szerint a sérülékenységekről, proof-of-concept (PoC) kódokról és javítási lehetőségekről szóló iparági diskurzus gyakran megelőzi a hivatalos közzétételt – néha csak néhány órával, máskor akár hetekkel is.

Az előadó kitért arra is, hogy a Twitter API hozzáférésének korlátozása komoly hatást gyakorolt azokra a közösségekre, amelyek korábban ezen a platformon követték nyomon a kiberbiztonsági diskurzusokat. Ezzel párhuzamosan a Mastodon és más Fediverse-alapú rendszerek egyre nagyobb teret nyernek – különösen a kiberbiztonsági közösség körében –, ami **decentralizáltabb, nehezebben megfigyelhető** kommunikációs környezetet eredményez. Így az ilyen beszélgetések monitorozása is több technikai akadályba ütközik.

Az előadás hangsúlyozta, hogy nemcsak a közösségi hálózatok figyelemmel kísérése fontos, hanem általánosságban az internetes diskurzusoké is. A **korai és aktív érdeklődés vagy információcsere** egy adott sérülékenységgel kapcsolatban erős indikátor lehet arra, hogy az adott problémát kiemelten kell kezelni.

Az előadó bemutatta hogyan használható fel ez az előzetes aktivitás arra, hogy a biztonsági elemzők már **a hivatalos CVE-megjelenés előtt** releváns kontextussal és súlyozással dolgozhassanak – növelve ezzel a gyors reagálás és a védekezés hatékonyságát. Hiszen, ha már korábban követtük a kérdéses sérülékenységről szóló diskurzust sokkal könnyebben tudunk majd reagálni a CVE megjelenés után legyen szó patchelésről vagy threat huntingról.

Az előadás prezentációja az alábbi linken érhető el.

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

Újragondolt adatvizualizáció a CTI szolgálatában

(Chris Horsley)

Az előadás célja az volt, hogy bemutassa, hogyan lehet **hatékonyabban és céltudatosabban** megjeleníteni a kiberfenyegetési hírszerzés (Cyber Threat Intelligence, CTI) területén felhalmozott adatokat. Az előadó arra hívta fel a figyelmet, hogy bár gyakran használunk ismert vizualizációs eszközöket – például grafikonokat vagy térképeket –, ezek sok esetben **nem segítik kellőképpen az adatok értelmezését**. Gyakran túlságosan leegyszerűsítettek, vagy nem tükrözik megfelelően az adott elemzési kontextust. Az adatvizualizációk közül megkülönböztettünk informatív/felfedező és „narratív" vizualizációkat aszerint, hogy csak adatot közül az adott vizualizáció vagy összefüggésekre világít rá.

A szakemberek láthatták, hogy miért van szükség vizualizációra a CTI területén, és milyen szerepet tölt be az adatok értelmezésének segítésében. Az előadó kifejtette, hogy **mitől lesz egy adatvizualizáció valóban hasznos**, és melyek azok az alapelvek, amelyek mentén a vizuális megjelenítést érdemes felépíteni. Rávilágított arra is, hogy számos népszerű vizualizációs forma – bár elterjedt – bizonyos helyzetekben kifejezetten félrevezető lehet.

Az előadás kitért olyan, kevésbé ismert, de a **CTI kontextusában kifejezetten hatékony vizualizációs típusokra is**, amelyek segítenek a komplex összefüggések áttekinthető megjelenítésében. Végül bemutatott olyan egyszerű, gyakorlatias módszereket , amelyekkel a szakemberek gyorsan és hatékonyan készíthetnek saját, testreszabott vizualizációkat a napi munka során – **akár különösebb grafikai vagy programozási háttér nélkül is**.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

Alkalmazkodj vagy bukj el: szoftver-ellátási lánc fenyegetések a CTI szolgálatában

(Paul McCarty)

Az előadás azt járta körül, **hogyan integrálható a szoftver-ellátási lánc biztonságára vonatkozó CTI** a már működő vállalati hírszerzési keretrendszerekbe. A prezentáció egy konkrét példán, az **npm ökoszisztémán keresztül** mutatta be a főbb megközelítéseket és tanulságokat.

Az előadó átfogó képet nyújtott az **aktuális szoftver-ellátási láncot** érintő fenyegetésekről, különös tekintettel a csomagkezelő ökoszisztémák ellen irányuló támadási trendekre és taktikákra. Az előadás kiemelte, hogy az ilyen típusú támadások **különösen alattomosak lehetnek**, mivel megbízhatónak tűnő szoftverkomponenseken keresztül jutnak be a rendszerekbe. Egy aggodalomra okot adó statisztika, hogy a káros csomagok 78%-a npm installációs módszereket alkalmazott.

Példákat néztünk arra vonatkozóan, hogy **milyen módszerek alkalmazhatók** a konkrét fenyegetésindikátorok azonosítására különböző platformokról, és hogyan lehet ezeket strukturált módon integrálni a napi CTI-munkafolyamatokba. Az előadás egyértelműen jelezte: a **szoftver-ellátási lánc biztonsága nem külön kezelendő terület, hanem a vállalati CTI szerves része kell, hogy legyen**.

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

Az alkalmazkodás művészete – hogyan derítsünk ki többet a támadókról a már meglévő információk alapján

(Alexandre Dulaunoy)

A **luxemburgi CIRCL** (Computer Incident Response Center Luxembourg /nemzeti CSIRT/) munkatársai osztották meg tapasztalataikat arról, hogyan lehet **már meglévő adatokból új összefüggéseket feltárni** a fenyegetettségi intelligencia során – különösen olyan esetekben, amikor a támadók aktívan próbálják elrejteni tevékenységük nyomait.

Az előadás számos technikát mutatott be, amelyekkel **új „pivotpontok”** (támpontok) **hozhatók létre**, és ezáltal addig rejtett kapcsolatok tárhatók fel különböző fenyegető szereplők között. A példák között szerepelt többek között:

- **közös favicon-fájlok elemzése** a támadó infrastruktúrák azonosításához,
- **QR-kódok és vonalkódok nyomon követése**, amelyeket a kiberbűnözők gyakran használnak kommunikációs és terjesztési célokra.

Az előadó csapat bemutatta, hogy **milyen eszközökkel lehet automatikusan generálni pivotpontokat**, és **hogyan lehet ezekkel grafikusan feltérképezni** a fenyegető entitások közötti kapcsolatokat. Az előadók hangsúlyozták, hogy a cél az volt, hogy a résztvevők olyan gyakorlati módszereket ismerjenek meg, amelyekkel meglévő adatok alapján új irányokba lehet elindulni a fenyegetések feltérképezésében – anélkül, hogy feltétlenül új információforrásokra lenne szükség.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

Ha minden prioritás… az is rendben van!

(Jake Nicastro)

A Mandiant szakértője az előadás során a „Ha minden prioritás, akkor semmi sem prioritás” kijelentést igyekezett **megcáfolni, újraértelmezni**. Véleménye szerint a várakozások menedzselése a kulcs az ilyen esetekben.

A prezentációban olyan valós esettanulmányokat és tanulságokat osztottak meg, ahol minden valóban egyszerre volt „prioritás”, mégis sikerült eredményesen, fókuszáltan dolgozni. A tapasztalatok részben az amerikai hadsereg gyakorlatából is származtak, és az előadó bemutatta, **hogyan alkalmazhatók ezek az elvek** a biztonsági csapatok irányításában – különösen olyan helyzetekben, amikor több, párhuzamosan sürgető feladat között kell navigálni.

Az előadásban elhangzottak „őszinte, néha kellemetlen igazságok” is – egyaránt az elemzőknek és a vezetőknek címezve. Ugyanakkor a cél az volt, hogy önbizalmat adjon ahhoz, hogy **merjük újragondolni a prioritás fogalmát,** és **megértsük**: ha minden prioritásnak tűnik, az még nem jelenti azt, hogy rosszul működnek a folyamataink és a projektjeink – lehet, hogy épp így kell jól működni.
Néhány **konkrét tanulság** az előadásból:

- Egy bemutatott eset szerint, ha a Mandiant saját környezetében incidens történik, az **ügyfeleik továbbra is elsődleges prioritást élveznek**, vagyis a belső válság sem írhatja felül a szolgáltatási kötelezettséget – ez hangsúlyozza a szervezeti fegyelem és külső elköteleződés fontosságát.
- A **U.S. Army Ranger kézikönyv** egyes elemei is bemutatásra kerültek, mint olyan katonai szintű irányelvek, amelyek alkalmazhatóak a CTI- és kiberbiztonsági műveletekben – különösen a gyors helyzetfelismerés és reagálás terén.
- A fenyegetések kezelése során kiemelt jelentőséget kapott a **meglévő csapatprioritások megőrzése**: egy új fenyegetés megjelenése nem zárhatja ki a többi, párhuzamosan futó feladat fontosságát, ezért elengedhetetlen az arányos erőforrás-allokáció.

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

- Az előadás ismertette az **Eisenhower-mátrix elvét**, mint idő- és feladatmenedzsment eszközt, amely segít a sürgős és fontos teendők közötti hatékony priorizálásban – különösen stresszes, információtúlterhelt környezetekben, mint amilyen egy CTI-funkció működése is lehet.
- Az előadás egyik fontos üzenete volt, hogy az **elvárásmenedzsment szükségszerűen prioritásmenedzsmentté alakul**: ha a csapatokra vagy egyénekre külső vagy belső elvárások nehezednek, azok automatikusan befolyásolják a feladatok sorrendiségét és fontosságát is. Éppen ezért elengedhetetlen, hogy minden szervezet megtalálja a számára működő, testreszabott prioritáskezelési módszertant.

Megérzéstől módszertanig: az admiralitási rendszer bevezetése a CTI területén

(Freddy Murstad)

Az előadás során egy interaktív bemutatón keresztül ismertették az **admiralitási rendszert**, amely eredetileg a hírszerzésben alkalmazott információmegbízhatósági értékelési keretrendszer, és mostanra egyre inkább alkalmazhatóvá válik a CTI területén is.

A prezentáció középpontjában a rendszer két alappillére állt:

- **Forrásmegbízhatóság** (Source Reliability) és
- **Információhitelesség** (Information Credibility).

Az előadó bemutatta, hogyan lehet ezek alapján objektívebb, átláthatóbb módon értékelni a CTI-ban használt forrásokat és információkat, **elkerülve a túlzott szubjektivitást vagy ösztönös megítélést** („megérzést”). Előfordul, hogy nem ellenőrzött támadók „magukra vállalnak” elkövetett kiberbiztonsági incidenseket az elismerésért vagy éppen gyártók próbálnak minél jobban „eltemetni” sérülékenységeket, incidenseket, azokat csendben javítani.

Az előadás során a rendszer működését néztük meg valós CTI helyzetekben, illetve kitértünk arra is, hogy **milyen előnyei** lehetnek annak, ha egy standardizált, strukturált megközelítést alkalmazunk az információk értékelésére és priorizálására.

Az előadás prezentációja az alábbi linken érhető el.

HA – nem „magas rendelkezésre állás” (High Avaliability), hanem „automatizált vadászat” (Hunting Automation)

(Xavier Mertens)

Az előadás egy frappáns szófordulattal indult: ezúttal a „**HA**” nem a megszokott High Availability (magas rendelkezésre állás) rövidítést jelentette, hanem a **Hunting Automation** fogalmára utalt – vagyis arra, **hogyan lehet automatizálni a fenyegetésvadászat** (threat hunting) **alaplépéseit**.

Az előadó rámutatott, hogy a napi szinten begyűjtött több ezer malware-minta feldolgozása során kulcsfontosságú, hogy a gyakori, jól ismert **kártevőket automatikusan kiszűrjük**, hogy az elemzők a valóban érdekes, új vagy különleges esetekre – a „friss húsra” – tudjanak fókuszálni.

A bemutató során gyakorlati példákon keresztül ismertették, **hogyan lehet az alapvizsgálatokat automatizálni** különböző eszközökkel és szkriptekkel (Karton keretrendszer egy MWDB adatbázissal mögötte), és hogyan lehet bevezetni egy olyan vizsgálati folyamatot, amely hatékonyan támogatja a prioritásokra épülő döntéshozatalt. A cél: a zaj kiszűrése és az értékes idő megtakarítása az elemzők számára.