NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 5. hét

HÍREK

- A Microsoft nevével élnek vissza továbbra is leggyakrabban az adathalász támadásokban
- A Signal lehetővé teszi a régi üzenetek szinkronizálását új eszközök csatlakoztatásakor
- A Bitwarden többfaktoros hitelesítés (MFA) nélkül is megnehezíti a jelszószéfek feltörését
- A Windows januári biztonsági frissítései során meghibásodhat a hanglejátszás
- Az Android új funkciója zárolja az eszközbeállításokat, ha megbízható helyen kívül tartózkodunk

STATISZTIKAI ADATOK

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

BESZÁMOLÓ

- FIRST Cyber Threat Intelligence Conference 2024

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági

HÍREK

A Microsoft nevével élnek vissza továbbra is leggyakrabban az adathalász támadásokban

(blog.knowbe4.com)

A Check Point kutatásai szerint a Microsoft, az Apple és a Google voltak a leggyakrabban megszemélyesített márkák az elmúlt negyedév adathalász támadásaiban. **Bővebben...**

A Bitwarden többfaktoros hitelesítés (MFA) nélkül is megnehezíti a jelszószéfek feltörését

(bleepingcomputer.com)

A nyílt forráskódú jelszókezelő, a Bitwarden egy extra biztonsági réteget ad azoknak a fiókoknak, amelyeket nem védenek kétfaktoros hitelesítéssel (2FA). Ehhez e-mail alapú hitelesítést kér, mielőtt engedélyezné a hozzáférést a fiókokhoz. **Bővebben...**

A Windows januári biztonsági frissítései során meghibásodhat a hanglejátszás

(bleepingcomputer.com)

A Microsoft megerősítette, hogy a Windows 2025. januári biztonsági frissítések telepítése után a hanglejátszás meghibásodik egyes, külső DAC (digitális-analóg átalakítókkal) rendelkező hangrendszereken. **Bővebben...**

Az Android új funkciója zárolja az eszközbeállításokat, ha megbízható helyen kívül tartózkodunk

(thehackernews.com)

AA Google egy új funkciót vezetett be Identity Check (Személyazonosság ellenőrzés) néven a támogatott Android eszközökön, amelynek aktiválásával a megbízható helyeken kívül az érzékeny beállítások elérése csak biometrikus hitelesítést követően lesz lehetséges. **Bővebben...**

A Signal lehetővé teszi a régi üzenetek szinkronizálását új eszközök csatlakoztatásakor

(bleepingcomputer.com)

A Signal új funkciója lehetővé teszi a felhasználók számára, hogy szinkronizálják régi üzeneteiket elsődleges iOS vagy Android eszközeikről az újonnan csatlakoztatott eszközökre, például asztali számítógépekre vagy iPadekre.

Bővebben...

További hírekért, látogasson el **weboldalunkra**!

Statisztikai Adatok

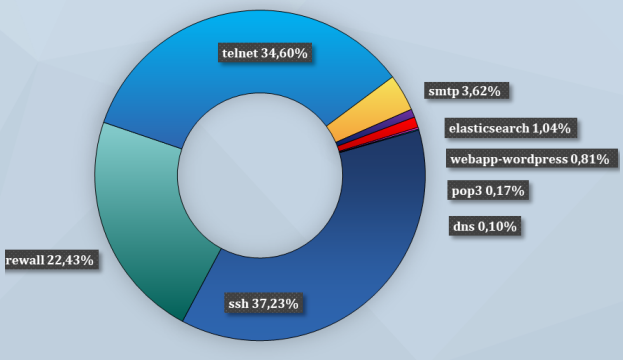
2025.01.24.-2025.01.30.

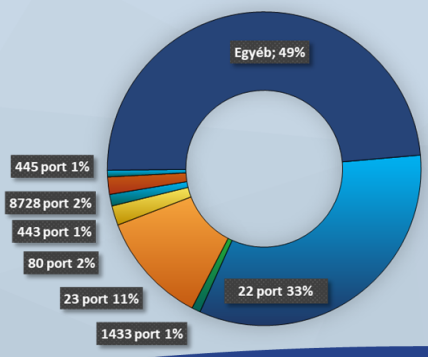
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony

Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!

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

#cyberthreatintelligence #llmtechnologiak

FIRST Cyber Threat Intelligence Conference 2024

2024. április 15-17.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** munkatársai **Széchenyi Terv Plus 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.

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

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

A **Forum of Incident Response Teams** (FIRST) 2016 óta évente megrendezésre kerülő konferenciájának célja a kiberfenyegetettségi hírszerzés (**Cyber Threat Intelligence**) területén dolgozó szakértők közötti tudásmegosztás. Az esemény fő célja a különböző ágazatokban dolgozó érdekelt felek közötti párbeszéd erősítése, új fejlesztési lehetőségek megvitatása egy nyílt fórumon.

A Berlinben megtartott esemény kiemelt témája a nyilvánosan, illetve privát módon rendelkezésre álló CTI adatok aggregálásának fontossága, és az ezen feladattal összefüggő nehézségek kezelése volt. Több előadás a nagy nyelvi modellekkel (**Large Language Models**) és a gépi tanuláson (**Machine Learning**) alapuló adatfeldolgozással és a technológia hasznosítással foglalkozott. Több prezentációban kiemelték annak fontosságát, hogy biztonságosabb **saját tudásbázisokon, lokális** megoldásokkal használni ezen technológiákat, mivel a nyilvános **LLM szolgáltatások** (például a **ChatGPT** – mint legközismertebb) használata során a modell információkielégítési célból kreálhat fiktív adatokat is (úgynevezett „hallucinációk”), illetve a nyilvánossága miatt az adatok bizalmassága sérülhet. Az előadások egy része a különböző CTI megoldásokat kínáló professzionális piaci szereplők reprezentációjáról és jó gyakorlatok megosztásáról szólt – elsősorban – a piaci alapokon működő FIRST tagokat célozva, a CTI folyamatok bevezetésére és fejlesztésére fókuszálva.

Kiknek ajánlott a beszámoló megismerése?

- **Minden kiberbiztonsági szakember** számára
- **CTI specialisták** számára
- **Incidenskezelők** számára
- **Digital forensic szakemberek**

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

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

„Tervrajz a fejlődéshez”: Testreszabott kiberfenyegetettség-elemző szervezeti érettségi modell (Cyber Threat Intelligence Maturity Model - CTI-MM) kidolgozása

Az előadó (**Kiraga Slawek**) bemutatkozásában megemlítette, hogy a különböző hírszerző szervezeteknél végzett munkája lehetővé tette számára, hogy megértse **azon tényezők sokaságát**, **amelyek befolyásolják az ügyfelek igényeit kielégítő hírszerzési „termékek” végső előállítását**. Ezek után feltette a kérdést, hogy biztos, hogy ezen termékek közül **mindegyik egyformán fontos lenne**? **Melyiket válasszuk ki, és melyek előállítására összpontosítsunk**, amikor a kiberfenyegetettségi hírszerzési (CTI) programunkat a nulláról építjük fel? Az előadó kiemelte a **különböző CTI érettségi modellek alkalmazásának hasznosságát**, például a jelenlegi képességek objektív felmérését, a más szervezetekkel való összehasonlítást, illetve ezen modellek használatát arra, hogy saját tervezetet készítsen a CTI érettségi szintjének nyomon követésére.

A CTI képességünk érettségi szintjének hatékony fejlesztésének **kulcsa a meglévő jó gyakorlatok felhasználása**, nincs szükség arra, hogy „újra feltaláljuk a kereket”! A szoftverfejlesztés terén **fókuszáljunk a tervünkben meghatározott** (biztonsági) **célkitűzésekre**; a döntéseket mindig az adataink alapján hozzuk; az alkalmazott technológiai megoldások mellett ugyanannyira lényeges a csapatmunka és a projekt-alapú szervezés és a tapasztalatok folyamatos gyűjtése és adaptálása. Az érettségi szintet az előadó 1-5 skálán határozta meg saját fejlesztésű CTI érettségi modelljében *(lásd: 1. ábra)*.

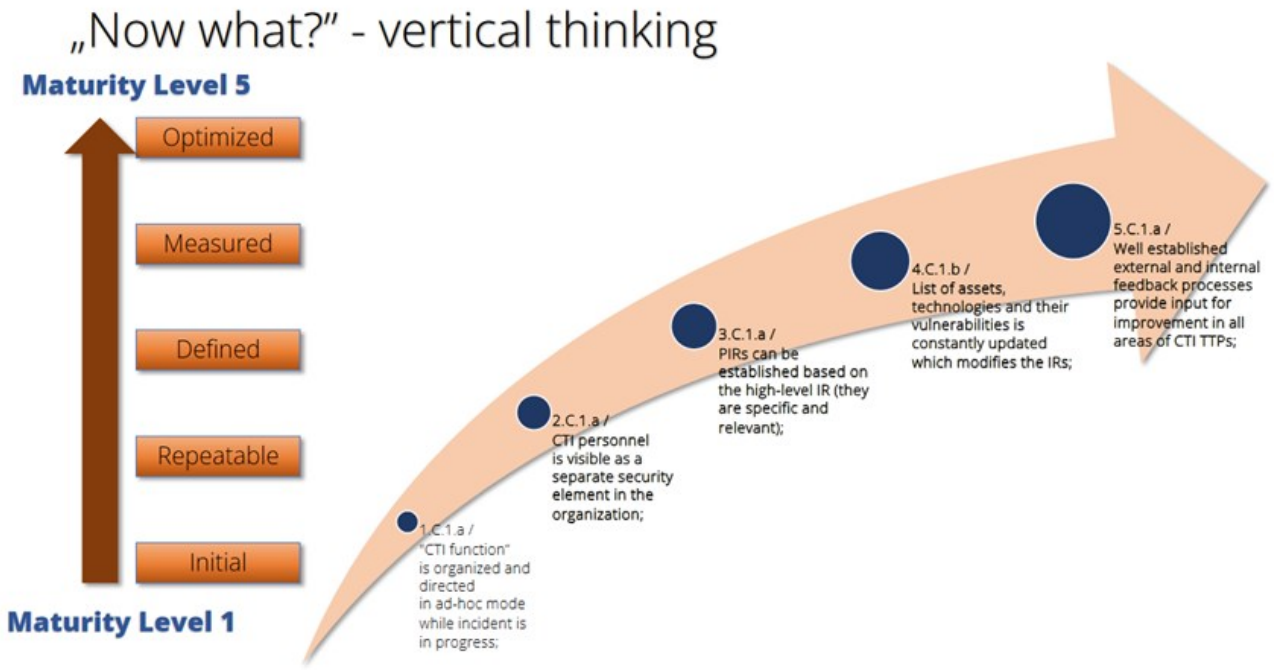
*Az előadói anyagok között kiemelten hasznos a lentebbi hivatkozáson elérhető **önértékelési táblázat**, amelynek segítségével bármely CTI képességet fejlesztő szervezet képes meghatározni, a saját fejlettségi szintjét:*

Előadói prezentáció

CTI-MM bővebb leírása a GitHubon

CTI-MM táblázat

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



1. ábra:
Az egyes CTI-MM szintek, és főbb jellemzőik

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

A CTI szektor inkoherenciájának megoldása egy élő, növekvő OpenCTI adattárban: STIX 2.1 kibővítése a siker reményében

Ez az előadás az OpenCTI keretrendszer három éven át tartó, több tucatnyi közreműködővel történő működtetésének kihívásait és bonyolultságát tárgyalta, **bemutatva azt a kaotikus állapotot, amelyet a címkék nem megfelelő használata, a duplikált bejegyzések, a helytelen betűzés/elírások és a különböző külső források** (például a SecureList, a Palo Alto Unit42 és a Trend Micro Research) az OpenCTI keretrendszerbe történő, nem strukturált **becsatornázásából adódó zűrzavar okozott**.

Az előadó konkrét példákkal illusztrálta, hogy az **adattisztítás hogyan vált lehetetlen küldetéssé** és **akadályozta a CTI szakembereket**. Mindennek egyik oka, hogy a kiberbiztonsági ipar szereplői **merőben eltérő taxonómiákat alkalmaznak**, mint a CTI szakterületen leginkább elterjedt, nyílt forrású **Structured Threat Information eXpression – STIX formátum**. Az előadó kitért az amerikai CISA és a STIX taxonómia közötti különbségekre, valamint a STIX 2.1-es verzió bővítésének szükségességére. A gyártói forrásokból származó adatok megfeleltetése elkerülhetetlen lépés, amit csak tervezetten lehet hatékonyan végrehajtani.

Az előadó tapasztalatai alapján javasolt legfontosabb jó gyakorlatok:

1. Csak **jól definiált** adatbeviteli csatornákat alkalmazzunk!
2. Az adattisztítást **mindenképp** az adatok importálása előtt végezzük el!
3. **Tartsuk meg** az eredeti riportot is!

Előadói prezentáció

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

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

Gépi tanuláshoz tervezett egységes CTI referencia-adatkészlet létrehozásának kezdeti megállapításai

Az előadás alapfelvetése szerint a **mesterséges intelligencia használata a CTI rendszerekhez nagy figyelmet kap** napjainkban. A **természetes nyelvi feldolgozást** (NLP), mint mutatót **egyre többen alkalmazzák** az elemzői munkaterhelés méréséhez. Problémát jelent azonban, hogy **jelenleg nincs** egy **elfogadott CTI NLP referencia adatkészlet**, azaz nem tudjuk összehasonlítani a különböző megoldásokat.

A referencia-adatkészletek rendkívül fontosak az **AI (és egyéb) rendszerek minőségének összehasonlításához**, valamint AI rendszerek esetében a **pontosságuk javításához** a „tanulási", illetve újratanulási futtatások során. A probléma megoldására a FIRST.org AI SIG egy önkéntesekből álló alcsoportot hozott létre.

*Az előadás kapcsán érdemes kiemelni – a még szakmabelieknek sem feltétlenül ismert – CTI riportokat tartalmazó, napi szinten frissülő **ORKL.eu** elnevezésű közösségi CTI könyvtárt.*

The Community Driven CTI Library

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

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

Fenyegetésjelentések és publikációk nagy volumenű feldolgozása Mesterséges Intelligencia és Gépi Tanulás használatával: Az elképzelés és a valóság

Az előadás a CTI elemzés egyik legfontosabb kérdésével foglalkozott: a számtalan CTI riport és más információforrás közül **hogyan szűrjük ki a relevánsakat**?

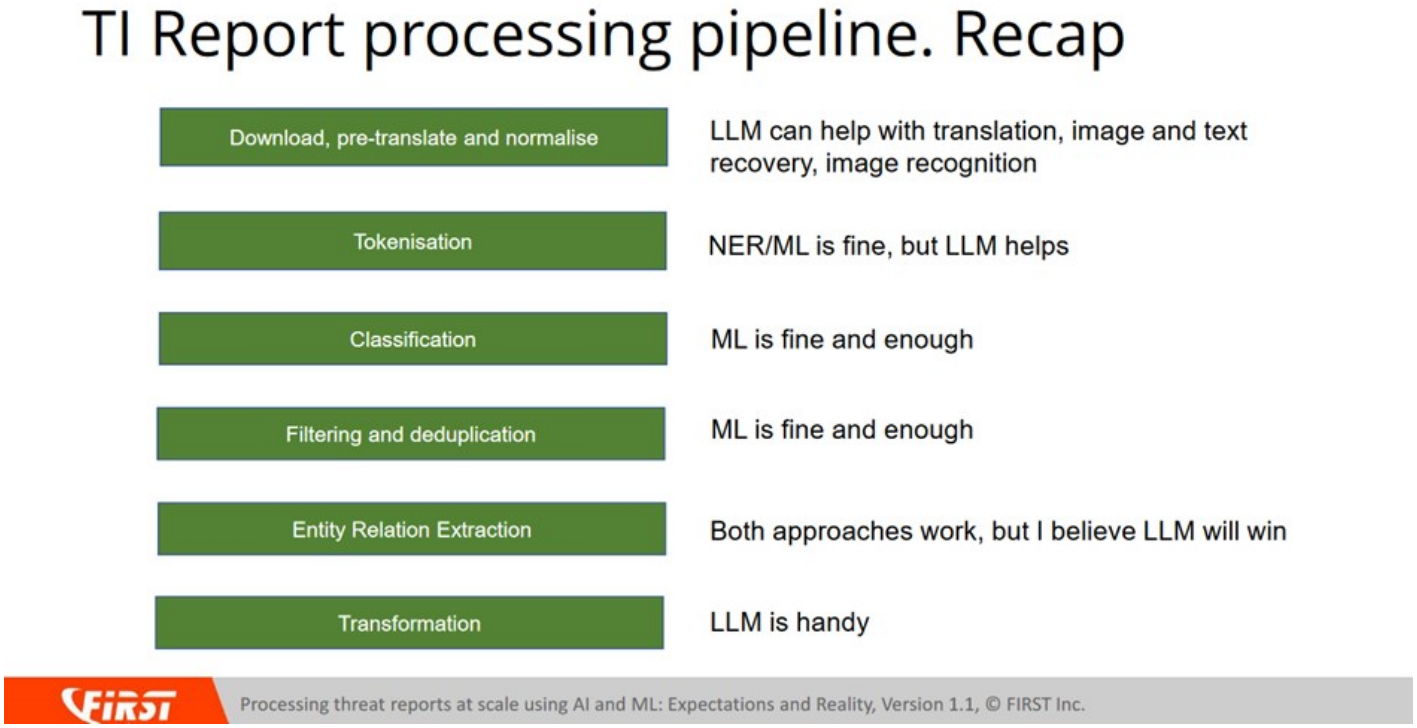
A **mesterséges intelligencia** (Artificial Intelligence) és a **gépi tanulás** (Machine Learning) használatának hangsúlyozásával az előadók egy automatizált megközelítés szükségességét mutatták be a fenyegetésekről szóló jelentések (APT-jelentések, DFIR-jelentések, rosszindulatú programok elemzéséről szóló jelentések stb.) gyűjtésére, feldolgozására és elemzésére, amelyre megoldási koncepciókat is felvázoltak.

A javasolt módszertan a technikai áttekintésre összpontosít, amely kiterjed a **releváns erőforrások azonosítására és felmérésére**, a **jelentések ML segítségével történő automatikus osztályozásra**, az **irreleváns információk kiszűrésére**, valamint az értékes fenyegetési adatok megőrzésére és kinyerésére hagyományos és mesterséges intelligenciát használó technikákkal. Az előadók ezen felül kitértek a **munkafolyamatok optimalizálására**, beleértve az értelmes információk kivonását a jelentésekből, az összegzési technikákat és a jelentések STIX formátumba történő automatikus átalakítását. Az előadás konklúziója, hogy a **legoptimálisabb gépi feldolgozás a NER/ML és a (privát) LM technológiák kombinált felhasználásával érhető el** *(lásd: 2. ábra).*

Előadói prezentáció

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

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



2. ábra
CTI jelentések gépi feldolgozásához javasolt technológiák

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

Haladó kiberfenyegetettségi hírszerzés - Hogyan olvassunk a támadók gondolataiban?

A Cyber Threat Intelligence – Special Interest Group részeként a **CTI-érettség három fázisát említették meg** az előadók – visszautalva egy már korábbi előadásra is, amely a CTI szervezetek érettségi modelljeivel foglalkozott. Az előadás során a 3. érettségi szintre jutott csapatok intézkedéseibe, folyamataiba és megközelítéseibe mélyedtek el. Bármilyen modellt is használjunk is (pl.: Diamond model, Pyramid of Pain) **tudnunk kell az elemzés során jó kérdéseket feltenni**.

Egy példán keresztül szemléltették, hogy amennyiben rendelkezünk egy IP címmel, akkor annak a WHOIS rekordjából egy bejegyzett cégnevet könnyedén ki tudunk nyerni. A cégnév alapján azután OSINT eszközökkel rengeteg egyéb információt szerezhetünk meg, például a cég neve alatt bejegyzett gépjárműveket, amelyből a közlekedési kamerák képei segítségével akár a támadó megközelítően pontos helyzetét is megállapíthatjuk.

Az előadók szerint a konklúzió az, hogy **tisztában kell lennünk a saját erősségeinkkel és korlátainkkal**, hiszen a fejlett technológiákat használó támadóknak **is megvannak a saját kockázat/ fenyegetés modelljük**, és minden lépésünk információval szolgál az ellenfelünk részére.

Végezetül a tanulságot úgy foglalták össze az előadók, hogy egy „kibernyomozás” lényegében nem különbözik egy „hétköznapi” bűntetőeljárásban végzett nyomozástól. A cél, hogy **a végén összeálljon egy koherens „elmesélhető” történet**, hiszen, ha ez hiányzik, akkor átadni se tudjuk az eseményeket hitelesen az érintett felek részére.

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

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

Hogyan alakítsuk ki a prioritás-alapú hírszerzési rendszerünket (Priority Intelligence Requirements) alacsony költségvetéssel

A CTI szakemberek egyre inkább azzal a nyomással szembesülnek, hogy minél **kevesebb erőforrással egyre több hírszerzési szolgáltatást és terméket kell nyújtaniuk**. Az eszkalálódó fenyegetések és a költségvetési megszorítások, valamint a korlátozott eszközök közötti egyensúlyozás a CTI-csapatokra nehezedik, ami kiégéshez és magas fluktuációhoz vezet.

A prioritások tisztázása érdekében a CTI-közösség bevezette a „**Kiemelt Hírszerzési Követelményeket**” (Priority Intelligence Requirements, röviden **PIR**). A PIR egy kulcsfontosságú **módszer az erőfeszítések és erőforrások összpontosítására**, illetve a **CTI csapatok és az érdekelt felek** (stakeholderek) **közötti kapcsolatok kiépítésére**, valamint a **nagyobb hatékonyság elérésére**.

Az előadó **egy lehetséges megoldást/módszert mutatott be** arra, hogy hogyan kezdjük el a PIR-ek költséghatékony gyűjtését, kidolgozását és szállítását, amivel a ráfordításokat is nyomon tudjuk követni. Útmutatást ad, hogy hogyan közelítsük meg a projekt első 90 napját, és hogyan biztosítsuk a PIR-ek végrehajtását anélkül, hogy eközben magas költségek merülnének fel.

Az előadás egy fontos konklúziója: **a siker kritikus eleme, hogy az összes releváns érdekelt féllel jól strukturált interjút kell készíteni, ami a későbbi tervezés alapjául szolgál**.

Előadói prezentáció

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

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

Az információmegosztás dilemmája a védelem biztosítása mellett

Az előadók a hírszerzési munka egyik alapvető dilemmájával foglalkoztak, ami nem más, mint **az egyes megszerzett információk nyilvánosságra hozatala**. A hírszerzési munka alapvető lényege, hogy az **döntéstámogató szerepet lásson el**, vagyis a megszerzett információk konkrét döntésekben és cselekvésekben reflektálódnak. Azonban az információk alapján meghozott döntések és a megfelelő lépések **a külvilág** (és ezáltal az ellenérdekelt felek**) számára is észrevehető változásokat eredményeznek**. Ezen túlmenően egyetlen incidens/eset feltárása **sokkal szélesebb körű** behatolás/ **káros tevékenység azonosításához vezethet,** ami ellen, ha megtesszük a megfelelő lépéseket az **veszélyezteti a későbbi hírszerzési adatgyűjtést** és így a további fellépést.

A **cselekvés nélküli hírszerzés azonban irrelevánsnak és feleslegesnek minősülhet**, ami nehéz helyzetbe hozhatja az elemzőket és a döntéshozókat. Az előadás során a kibertérben az **ellenfél alkalmazkodásához vezető hírszerzési információk nyilvánosságra hozatalának példáit** és a **kiberbiztonsági szakemberekre gyakorolt következményeit vizsgálták** az előadók. Az előadás végére a kiberfenyegetésekkel kapcsolatos hírszerzési munka alapjául szolgáló **„nyereség-veszteség" dilemma** részletes megismeréséig és annak mélyebb megértéséig jutottunk.

Az előadást néhány tanáccsal és gyakorlati példával zárták, amely a hírszerzési elemzőknek segít **hogyan próbálhatnak egyensúlyt teremteni** a folyamatos adatgyűjtés és a védelem támogatása között, és **milyen tényezők a legkritikusabbak** az ilyen kérdések eldöntésében.

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

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

A rosszindulatú programok kódhasonlóság-észlelésének javítása a Vectorsearch és a TLSH segítségével

Az előadó a rosszindulatú programok elemzésének egyik gyakorlati megközelítését mutatta be, amely a **rosszindulatú programminták kódhasonlóságainak felderítésére összpontosít** a vektorkeresés segítségével. A vektorkeresés hagyományos gépi tanulási módszerei helyett a **Trend Micro Locality Sensitive Hash (TLSH)** módszerét használta.

Ez a technika a bejövő bináris fájlok alapvető alkotóelemeire való szétszerelését, majd a TLSH-értékek ezen elemekre való kiszámítását jelenti. Az így kapott hashek kompaktak, és hatékonyan tükrözik a bináris állományok szerkezetét és tartalmát.

A módszer fontos eleme a **köztes nyelv (IL) használata** a bináris függvények konzisztens ábrázolásához, ami **segít azonosítani a különböző beállításokkal vagy platformokkal lefordított rosszindulatú programok hasonlóságait**. Ez a megközelítés lehetővé teszi, hogy hatékonyabban találjanak hasonló kódrészleteket a különböző rosszindulatú szoftverminták között.

Összefoglalva az előadás felhívta a figyelmet **a rosszindulatú szoftverek elemzésének egy viszonylag új és hatékonynak ígérkező megközelítésére**, természetesen annak minden jelenlegi kihívásával, mint az ezen hashekből épített adatbázis tárolásával és futtatásával kapcsolatos hardveres követelmények.

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

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

Fenyegetési szereplők (APT-k) nyomon követése képek segítségével: Egy kutatási és elemzési megközelítés

Az előadó a felvezetésében részletezte, hogy a képek a biztonsági elemzők számára mennyire értékes információforrást jelenthetnek. A legtöbb információ az APT-k által elkövettet támadásokról **a támadások későbbi szakaszából** – amikor már megtörtént a károkozás – **utólagos forensic munka eredménye**, ami messze **nem optimális**.

Az előadó kutatási munkája egy új módszerre összpontosít, amely **áthelyezi az információgyűjtést a támadások még korai, előkészítő szakaszára**. A fenyegetési szereplők által a dokumentumokban használt képek nyomon követésével betekintést nyerhetünk az eljárásaikba, valamint a potenciális célpontjaikba és a megszemélyesített vállalatokba. Ez a fajta megközelítés **segített például megtalálni** és **nyomon követni** az orosz **Gamaredon** kiberkémkedő csoport tevékenységét, vagy például a **Blind Eagle** néven ismert csoportot, amelyről feltételezik, hogy latin-amerikai és más APT-k/ bűnszervezetekhez köthető. Az előadás kitért a megközelítés kihívásaira és korlátaira is.

Előadói prezentáció

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

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

Láthatatlan karakterláncok (strings) - Az infrastruktúra-követés kortárs kihívásai és technikái

Az előadás a fenyegetések felderítésével foglalkozó csapatok egyik leggyakoribb feladatába mélyed el, amely jelentős betekintést nyújthat az ellenfél műveleteibe: **az ellenérdekelt felek infrastruktúrájának felderítésbe és nyomon követésébe**. A felhőszolgáltatások egyre szélesebb körű elterjedése és az adatvédelem alkalmazása lehetővé tette a fenyegetési szereplők (APT aktorok) számára, hogy a káros parancskiadási és vezérlő csomópontokat hasonló tulajdonságokkal és profillal rendelkező, legitim hosztokkal vegyítsék.

Az előadás célja az volt, hogy **bemutassa az infrastruktúra elemzéssel kapcsolatos egyes kihívásokat**, és olyan robusztus **módszertant javasoljon, amely rugalmasan nyomon követhető technikákhoz vezet**. Az előadásban Joe Slowik koncepcióját használva – amely az indikátorokat összetett objektumként kezeli – a hálózati artefaktumok, például a TLS-tanúsítványok, a kitett host-szolgáltatások és a tartományok profilozására összpontosítottak.

Több jellemző megfigyelésével és kombinálásával a kiberbiztonsági **elemzők olyan mintákat és aláírásokat hozhatnak létre, amelyek reprezentálják, hogy egy APT hogyan hozza létre az infrastruktúráját**, és ezt felhasználva nagyobb pontosságra tehetnek szert a korai felderítés és az attribúció terén. Az előadásban szó volt az infrastruktúra szervereinek támadások utáni nyomon követésére vonatkozó **felhasználási esetekről** és az **infrastruktúra-elemzés szerepéről** a APT csoportok azonosításában.

Előadói prezentáció

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