

37. Országos Tudományos Diákköri Konferencia

Had- és Rendészettudományi Szekció

Budapest, 2025. április 22–24.

Nemzeti Köszolgálati Egyetem

Hadtudományi és Honvédtisztképző Kar

**A fenyegetettség elemző platformok felhasználásának lehetőségei
a kibertéri fenyegetések felderítésében**

Jelige: *Fekete Macska*

Pályamunka lezárásának időpontja: 2024. április

2025.

Tartalomjegyzék

1	Bevezetés és kutatási kérdések.....	4
2	A fenyegetettség elemzéssel kapcsolatos általános követelmények	6
3	A fenyegetettség elemzés szintjei.....	11
3.1	Stratégiai szint	12
3.2	Műveleti (operatív) szint	13
3.3	Taktikai/harcászati szint	14
3.4	Technikai szint.....	15
4	A fenyegetettségi információval és azok megosztásával kapcsolatos követelmények	17
5	Kihívások a CTI-al kapcsolatosan.....	20
6	A fenyegetések leírására használt módszertanok	24
6.1	Cyber Kill Chain.....	24
6.2	The Diamond Modell.....	28
6.3	Piramid of Pain	31
6.4	MITRE ATT&CK.....	33
6.5	A fenyegetettség elemző módszertanok összehasonlítása	35
7	A platformok:	37
7.1	Kereskedelmi platformok	39
7.1.1	Anomali ThreatStream	44
7.1.2	IBM X-Force Exchange.....	44
7.1.3	LookingGlass Cyber Solutions	45
7.1.4	Recorded Future	46
7.1.5	ThreatConnect	46
7.2	A kereskedelmi platformok közös jellemzői	47
8	Az ingyenes, nyílt forráskódú platformok.....	48

8.1.1	Malware Information Sharing Platform (MISP)	50
8.1.2	OpenCTI	51
8.1.3	Your Everyday Threat Intelligence (YETI).	51
8.1.4	Collective Intelligence Frameworks (CIF)	52
8.2	Az ingyenes platformok közös jellemzői	52
8.3	A kereskedelmi és a nyílt forráskódú platformok összehasonlítása	53
9	Összegzés további kutatási irányok.....	55
9.1	Összefoglalás	55
9.2	Megállapítások.....	57
9.3	További lehetséges kutatási irányok	59
10	Irodalomjegyzék	60

1 Bevezetés és kutatási kérdések

Az elmúlt években köszönhetően a digitalizáció nagyfokú elterjedésének egyre inkább megnőtt annak az igénye, hogy tisztában legyünk azzal milyen fenyegetésekkel kell szembenéznünk a kibertérben.

Az elmúlt évek történései, úgymint az orosz-ukrán háború és az Izrael és a Hamasz közötti konfliktus kibertéri eseményei bebizonyították, hogy a kibertérben a cselekmények már nemcsak az elektronikus információs rendszerek ellen irányulnak, hanem akár az állampolgárok nyugalmanak megzavarására, elégedetlenség szítására, vagy a szélsőséges esetben a fennálló politikai rend megzavarására is. Ennek fényében a kibertéri fenyegetések megismerése mindinkább kiemelt jelentőségűvé kezd válni.

Alapvetően a fenyegetés lehet az ellenérdekelt kibertéri szereplők azon szándéka, hogy kárt okozzanak a rendszereinkben, jelentheti azt az információt is, amely lehetővé teszi egy szervezet számára, hogy felkészüljön és megvédje a saját rendszereit, vagy adatvagyonát.

A rendszerek és az adatok megvédésére sokkal nagyobb az esély amennyiben egy szervezet válaszolni tud azokra a fenyegetettségekre vonatkozó kulcskérdésekre, hogy ki a lehetséges támadó, mi az, amit támadni akar, hol, mikor és miért, valamint, hogy melyek azok a rendszereim melyek a legfontosabban a vállalat működése szempontjából?

A fenyegetés elemzés hatékonyan tud hozzájárulni ahhoz, hogy egy adott szervezet megfelelően tudja csoportostani és tervezni az elektronikus információvédelem megvalósítására, a rendszerinek védelmére rendelkezésre álló forrásokat.

A kibertéri fenyegetettség elemzés nem csak a szervezet saját rendszerinek védelme tekintetében tud hasznos információkat nyújtani, hanem a vállalat más stratégiai döntéseit is képes támogatni. De ugyan úgy értelmezni lehet egy tágabb szektor vagy akár egy ország, országok közössége szempontjából is,

A fenyegetettség elemzést több szinten is végre lehet hajtani. Nem ugyan azokra az adatokra van szükség egy stratégiai döntés meghozatalához és egy adott rendszeren belül a támadás felismeréséhez és elhárításához.

Az információ önmagában nem elég. Azokat fel is kell dolgozni. Az információ feldolgozása és a különböző szintek számára történő „fogyaszthatóvá” tétele manapság már nem csak emberi erőforrás segítségével lehetséges. Rendelkezésre állnak fenyegetettség elemző platformok, amelyek képesek segítséget nyújtani a beérkező adatokat feldolgozásában.

Az információ feldolgozását követően azokat meg is kell osztani, ami szintén különbözőképpen történhet egy stratégiai szintű vagy egy taktikai szintű fenyegetettség elemzés eredménytermékét illetően.

A fenyegetettség elemzést jelen dolgozatomban egy szervezetre nézve vizsgálom, de ismételten ki kell hangsúlyozni, hogy a fenyegetettségi helyzetképnek nem csak egy szervezet és azok rendszereit illetően van létjogosultsága.

Dolgozatomban bemutatom, mely fenyegetettség elemzési szinteknek milyen információkra van szüksége és ezeket milyen forrásból lehet beszerezni.

Valamint arra próbálok rávilágítani, hogy a fenyegetettség elemzés melyik szintjén képesek a fenyegetettség elemző platformok által kínált megoldások a leginkább segítséget nyújtani.

A vizsgálat során megvizsgálom a kereskedelmi és az ingyenes nyílt forráskódú fenyegetettség elemző platformok szolgáltatását, miben hasonlítanak és mi a fő különbség közöttük, valamint, hogy a kereskedelmi vagy az ingyenes platformok azok, amelyek képesek támogatni nem csak a technikai és a taktikai, hanem az operatív és a stratégiai elemzést.

Hipotézis

1. hipotézis: A kereskedelmi platformok és az ingyenes nyílt hozzáférésű platformok egyaránt képesek támogatni a fenyegetettség elemzés végrehajtását.

Mind a kereskedelmi, mind az ingyenes platformok egyaránt hatékonyak, amennyiben technikai és taktikai fenyegetettség értékelésről van szó. A két platform típus által nyújtott szolgáltatások az operatív és a stratégiai szintű elemzés támogatásának kérdésében kezdenek elválni egymástól.

2. hipotézis: Stratégiai szinten amennyiben csak az elektronikus információs rendszerek védelmének kérdését vizsgáljuk a kereskedelmi platform szolgáltatások szélesebb körű támogatást tudnak nyújtani.

A nyílt hozzáférésű platformok jelenleg még nem kínálnak olyan szolgáltatást, mint egy-egy csoport tevékenységének, vagy egy támadás típusnak az összefoglaló jellegű bemutatása.

A kutatásom során kvalitatív módszerekkel dokumentum kutatást végeztem, majd a saját megfigyeléseimet és tapasztalataimat elemeztem ezek fényében.

2 A fenyegetettség elemzéssel kapcsolatos általános követelmények

A Cyber Threat Intelligence (a továbbiakban: CTI) a kiber fenyegetettség elemzésével foglalkozik. A fenyegetettség elemzés elsődleges célja az elektornikus információs rendszerekkel kapcsolatos, de hatékonyan tud hozzájárulni a szervezeten túli stratégiai helyzetkép kialakításához is.

A CTI-n belül adatok gyűjtése, feldolgozása és elemzése megy végbe, hogy megérthessük egy kibertéri szereplő motivációit, célpontját és viselkedését. A CTI lehetővé teszi a gyorsabb és hiteles információkra épülő, adatokkal alátámasztott döntéshozatalt a szervezet biztonsági szintjének növelése érdekében, illetve a proaktív fellépést a fenyegető szereplők ellen. A fenyegetettség elemzés egy szervezet elektronikus információvédelme szempontjából kiemelt jelentőségű. Segítségével a szervezet proaktívan képes a lehetséges fenyegetéseket megelőzni, a hatásaikat csökkenteni és segítséget nyújt az esetleges támadások utáni helyreállítás folyamatában is. Az által kapott információk segítségével nem csak az információbiztonsági vezetők, de az eseménykezeléssel, vagy a hálózatüzemeltetéssel foglalkozó kollégák is megfelelő döntéseket hozhatnak.¹

A megfelelő információk birtokában a szervezet képes felmérni, hogy a rá potenciálisan fenyegetést jelentő ellenérdekelt szereplők milyen technikákat, taktikákat és eljárásrendeket alkalmaznak és fel tud készülni, fel tudja készíteni a rendszereit ezen fenyegetések kivédésére.

A fenyegetettség elemzés segítségével priorizálni lehet a fenyegetéseket és a sérülékenységeket: Az információk birtokában a fenyegetések és a sérülékenységek osztályozásával az információbiztsága szánt költségvetés jobban tervezhető. A fenyegetések és a sérülékenységek a fenyegetettség elemzésből nyert információk segítségével súlyozható és így biztosítva lehet az is, hogy a legsúlyosabbak kerüljenek először elhárításra.²

Amikor bekövetkezik egy incidens a fenyegetettség elemzés értékes információval szolgálhat a támadás részleteiről, az abban részt vevő támadókról, valamint az általuk felhasznált eszközökről, technikákról és támadási módokról (TTP's³). Ezek az információk segítséget

¹ Nan Sun és mtsai., „Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives”, *IEEE Communications Surveys & Tutorials* 25, sz. 3 (2023): 1748–74, <https://doi.org/10.1109/COMST.2023.3273282>.

² „Threat Intelligence: What It Is, and How to Use It Effectively | SANS Institute”, elérés 2024. április 2., <https://www.sans.org/webcasts/threat-intelligence-is-effectively-102622/>.

³ Tactics, Techniques, and Procedures

nyújtanak az incidensek gyors és hatékony kezelésében, valamint a fenyegetések felfedezésében (threat hunting) is.

Az elemzések, azáltal, hogy bizonyítékokon alapuló betekintést nyújtanak a potenciális fenyegetésekbe segítséget nyújtanak a megfelelő stratégia kialakításába és a döntéshozatalba is.⁴

A CTI legfontosabb eleme és az alapja az adatgyűjtés. A CTI-nek képesnek kell lennie releváns adatok gyűjtésére különféle forrásokból, beleértve nyílt forrásokat, belső hálózati naplókat, hírszerzési adatokat, és egyéb megbízható információforrásokat. Az adatok forrásánál nem csak a technikai adatokra van szükség hanem elemzésekre, ajánlásokra, stratégiai dokumentumokra is⁵.

A gyűjtött adatokat elemezni kell a fenyegetések azonosítása, a támadási minták megértése és a potenciális sebezhetőségek feltárása érdekében. Az elemzésnek strukturált és ismételhető módszertanokon kell alapulnia.⁶

A fenyegetettség elemzés esetén kiemelt jelentősége van a megszerzett és az elemzett adatok megosztásának. Az információmegosztás fontos egy szervezetten belül a különböző szervezeti egységek között, de a szervezetek és a CSIRT⁷-ek között is. Az információk megosztásával erősíthető a saját szervezet védelme is, mert segít időben felkészülni egy adott támadásra.⁸

A fenyegetettség elemzés egyik alapját, mint már említettem a technikai adatok képezik. A hatékonyság érdekében a technikai adatokat biztosító CTI rendszereknek összekapcsolhatónak kell lennie a meglévő biztonsági eszközökkel és folyamatokkal, lehetővé téve az automatizált válaszokat és az operatív hatékonyság növelését.

A fenyegetettségi helyzetkép, az aktuális támadási trendek, technikák és taktikák is folyamatosan változnak. Főleg a technikai adatoknál kiemelt jelentősége van a folyamatos naprakészségnek és frissességnek. nem csak az adatoknak, hanem az adatok megszerzésének forrásait is naprakészen kell tartani.

⁴ Kris Hermans, *Mastering Cyber Threat Intelligence (CTI): A Comprehensive Guide to Implementing and Managing CTI in the Enterprise* (Independently published, 2023).

⁵ „Threat Intelligence: What It Is, and How to Use It Effectively | SANS Institute”.

⁶ „The Definitive Guide to Cyber Threat Intelligence.pdf”, elérés 2024. április 2., https://informationsecurity.report/Resources/Whitepapers/e8aee5ef-4086-4c84-9a33-4134848ea7fb_The%20Definitive%20Guide%20to%20Cyber%20Threat%20Intelligence.pdf.

⁷ Computer Security Incident Response Team

⁸ Hermans, *Mastering Cyber Threat Intelligence (CTI)*.

A CTI esetében kiemelt követelmény, hogy összhangba kell lenni a vonatkozó adatvédelmi és kiberbiztonsági előírásokkal, biztosítva az adatok bizalmas kezelését és a szabályozási követelmények tiszteletben tartását.

Fontos továbbá, hogy a CTI-nak támogatnia kell az incidensválasz csapatokat azáltal, hogy értékes betekintést és kontextust nyújt a fenyegetésekkel kapcsolatban, elősegítve a gyors és hatékony reagálást.

Az alábbi összefoglaló ábrán bemutatom, hogy mely információbiztonsági szerepköröknek miben nyújthat segítséget egy jó CTI elemzés⁹.

Elektronikus információbiztonsági vezetők, auditorok, kockázatmenedzsment	A szervezet szempontjából fontos és releváns fenyegetések felmérése és az azokkal kapcsolatos megfelelő döntések meghozatala érdekében
Red teaming	A szervezet szempontjából jelentőséggel bíró támadók taktikáinak és technikáinak szimulálása, a védelmi mechanizmusok tesztelése, a gyenge pontok azonosítása érdekében és hogy az ezeket kiküszöbölő biztonsági ajánlásokat lehessen tenni
Incidenskezelő állomány	Incidens esetén s fenyegetést jelentő szereplő által alkalmazott technikák ismeretében hatékonyabbá és teljesebb körűvé teszi annak eltávolítását az infrastruktúrából.
Threat hunting (fenyegetéseket és sérülékenységeket kereső állomány)	Proaktív, megelőző jellegű vizsgálatok folytatása, a szervezetre veszélyt jelentő kibertéri szereplők technikái és taktikái alapján.
Sérülékenység vizsgálatral foglalkozó állomány	Lehetővé teszi, hogy azonosítani és súlyozni lehessen a sérülékenységeket és azoknak a javításának a sürgősségét, az alapján, hogy van-e már azt kihasználó kód, vagy eljárásrend aktívan használatban a rosszindulatú szereplők között.
Rendszerüzemeltetők, rendszerfejlesztők	A rendszerek és a hálózatok azon szegmenseinek az azonosítása amelyet aktívan támadnak a szervezetre veszélyes kibertéri szereplők.

1. ábra: A CTI felhasználásának lehetőségei¹⁰

A CTI folyamat során keletkező dokumentumoknak több fajtája is lehet attól függően, hogy ki a címzett és mi a felhasználás módja. Az elkészült dokumentumnak mindig szervesen

⁹ „A Requirements-Driven Approach to Cyber Threat Intelligence”, Mandiant, elérés 2024. április 2., <https://www.mandiant.com/resources/blog/requirements-driven-approach-cti>.

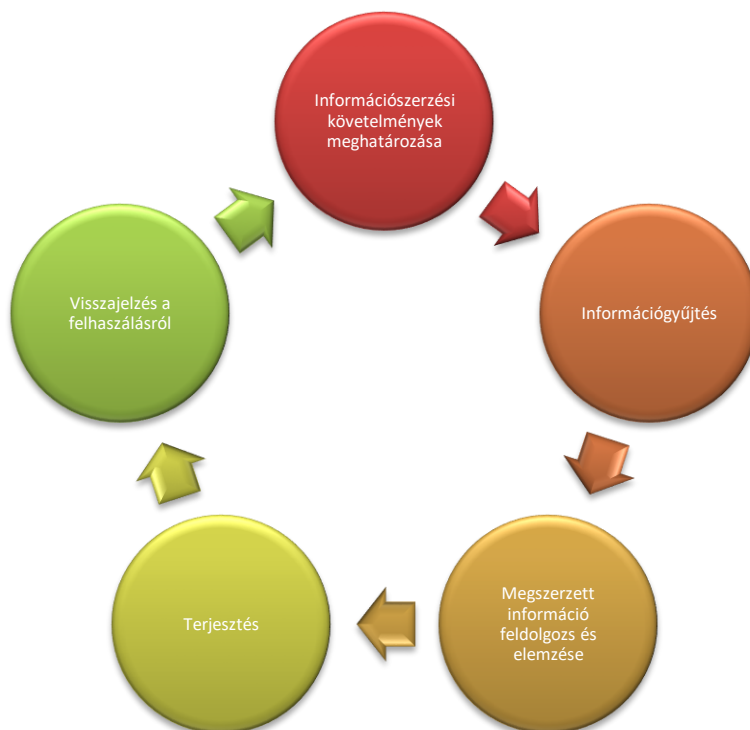
¹⁰ „A Requirements-Driven Approach to Cyber Threat Intelligence”.

illeszkednie kell a szervezet munkafolyamataiba és meg kell felelnie a „címzett” által támasztott követelményeknek.

Ennek megfelelően a dokumentumok fajtái az alábbiak lehetnek:

- rendszeres, időszakos riportok;
- fenyegetettségi riasztások;
- incidenskezelési jelentések;
- a red team tervezési folyamatait segítő dokumentumok;
- fertőzőettségi mutatók¹¹ (a továbbiakban: IoC) bővebb kifejtése, részletezése;
- technikai adatok becsatornázása a végpontvédelmi eszközökbe, vagy az azokat feldolgozni képes eszközökbe;
- stratégiai összefoglaló dokumentumok.

A fenyegetettség elemzés során általános érvényű, hogy minden szinten ugyan azok az alapfolyamatok zajlanak le, amelyet a 2 ábra mutat be.



2. ábra: A fenyegetettség elemzés folyamata (saját szerkesztés)

¹¹ „A BIZOTTSÁG (EU) 2017/ 1584 AJÁNLÁSA - (2017. szeptember 13.) - a nagyszabású kibebiztonsági eseményekre és válsághelyzetekre való összehangolt reakálásról”, é. n.

1. **Információszerzési követelmények meghatározása:** Ebben a fázisban meg kell határozni, hogy milyen információkra van szüksége az adott szervezetnek és azokat milyen forrásból lehet beszerezni. Itt kerülnek meghatározásra és priorizálásra azok a fő kérdések, amelyekre a szervezet választ szeretne kapni.
2. **Információgyűjtés:** A gyűjtési fázisban az első fázisban meghatározott követelmények alapján gyűjtik össze a szükséges információkat és adatokat. Az adatgyűjtés sok esetben automatikus módszerekkel történik.
3. **Feldolgozás és elemzés:** A feldolgozási fázisban a nyers adatokat feldolgozzák, hogy alkalmasak legyenek az elemzésre. A feldolgozás jelen esetben a fals pozitív, redundáns, nem kellően megalapozott, elavult adatok kiszűrését jelenti. Az elemzési fázisban pedig a feldolgozott adatokat alaposan megvizsgálják. Az elemzés célja, hogy választ adjon a kezdeti követelmények fázisában felmerült kérdésekre, ellenőrizze, hogy az adatok és a kapott eredmények összhangban vannak-e a kitűzött célokkal.
4. **Terjesztés:** Az elemzési fázisban összegyűjtött információkat ezután terjesztik a célzott fogyasztók és érdekelt felek felé automatizált vagy manuális módszerekkel.
5. **Visszajelzés:** A visszajelzés a fenyegetettség elemzési ciklus végét jelenti. Ez a lépés talán az egyik legfontosabb az elemzési ciklusban, ugyanis ez alapján lehet az adatforrásokat és a feldolgozási módszereket, de a címzettek köré is pontosítani.

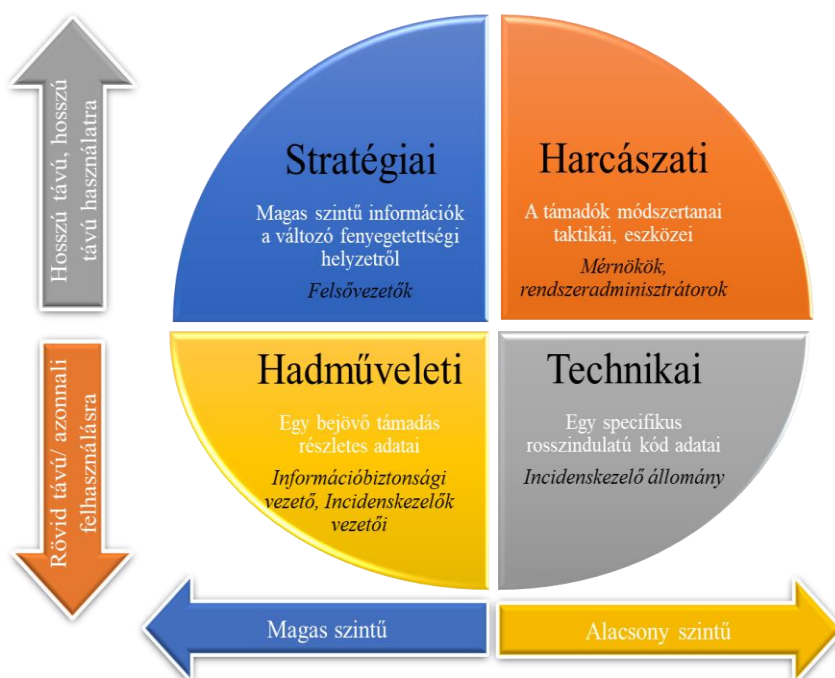
A fenyegetettség elemzés folyamata lehetővé teszi a szervezetek számára, hogy hatékonyan kezeljék a fenyegetéseket, és időben reagáljanak rájuk. A visszajelzési fázis különösen fontos, mivel lehetővé teszi a folyamatos fejlődést és a fenyegetettség elemzési tevékenységek finomítását.¹² A fenyegetettség elemzési ciklus ugyan azokat a lépéseket tartalmazza, mint a hagyományos elemző-értékelő ciklus. A fenyegetettség elemzés a hagyományos elemző munkától főleg abban különbözik, hogy a terjesztés az esetek nagy részben automatikusan történik, mivel a fenyegetettség elemzés során felhasznált adatok az esetke nagy többségében gépek által feldolgozható technikai adatok. Különbség továbbá, hogy mivel sok esetben technikai adatokról van szó ezért a visszajelzés is automatikusan történik.

¹² Halil Arslan és Ozkan Canay, „CYBER THREAT INTELLIGENCE SYSTEMS AND APPLICATIONS”, 2023, 103–16.

3 A fenyegetettség elemzés szintjei

A CTI, vagyis maga az elemzési folyamat ahogy az alapát képező elemzés- értékelés is több szinten végrehajtható folyamat. A CTI-n belül alapvetően négy szintet különböztethetünk meg: a stratégiai, a műveleti (operatív), a taktikai, illetve a technikai szinteket. A szintek rendeltetése és feladatai jelentős mértékben eltérnek egymástól, valamint az adott eseményekhez kapcsolódó cselekvés is más módon és mélységben megy végbe¹³. A kiber fenyegetettséget a szintekre vetítve, ugyanakkor komplex módon kell elemezni. A szintek között alá-fölérendeltségi viszony van attól függően, hogy milyen szinten zajlik a cselekvés, a döntéshozás, és mennyi felelősséggel jár az adott döntés. A szintek között különbség van a feldolgozott adatok, az adatforrások és sok esetben az alkalmazott elemzési módszertanokban is.

A szintek megkülönböztethetőek a végtermékként készülő dokumentumok jellege, formátuma, az azokat felhasználó és az abban foglaltakat végrehajtó felhasználói kör és az adatokat alkalmazó terület alapján is. Ezek összefoglalását a 3. ábra mutatja be¹⁴.



¹³ Milica Djekic, „Levels of Cyber Intelligence”, *Australian Science* (blog) (Australian Science, 2014. május 16.), <http://ozscience.com/internet-2/levels-of-cyber-intelligence/>.

¹⁴ Martyn Ruks és David Chismon, „Threat Intelligence: Collecting, Analysing, Evaluating” (MWR InfoSecurity Ltd, 2015), <https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf>.

3. ábra: A fenyegetettség elemzés szintjei (Ruks és Chismon, „Threat Intelligence: Collecting, Analysing, Evaluating” (pp: 36-42) alapján)

3.1 Stratégiai szint

A CTI stratégiai szintje különösen fontos, mivel ezen a szinten azonosítjuk és elemezzük a fenyegetéseket a magas szintű, felsővezetői, információbiztonsági vezetői döntéshozatal támogatása érdekében. A stratégiai CTI célja, hogy feltárja, ki áll egy adott fenyegetés mögött, és nyomon kövesse a kiberbiztonsági trendeket, miközben megpróbálja megérteni azokat a motivációkat, amelyek miatt egy adott szervezetet támadás célpontja lehet.

A stratégiai szintű CTI nem csak az információbiztonsági szakemberek számára nyújt információkat, hanem a magas szintű vezetők, számára is, akik a kapott információk alapján hozzák meg a kritikus üzleti és biztonsági és akár költségvetési döntéseket. Ezek a döntések érintik a személyzeti létszámot, az alkalmazott technológiát, a szervezet által kialakított kiberbiztonsági politikákat és stratégiát.

A CTI stratégiai szintű alkalmazása segít a szervezeteknek abban, hogy megértsék, mely fenyegetések jelentik a legnagyobb kockázatot. Anélkül, hogy tisztában lennének a potenciális kibertérből érkező fenyegetésekkel, a szervezetek nem tudnák hatékonyan allokálni az erőforrásaikat, ami sérülékenységet eredményezhet a kiberfenyegetésekkel szemben.

Az információgyűjtés kulcsfontosságú lépés a stratégiai CTI folyamatában. Stratégiai szinten az információforrások a nemzetközi szervezetektől (ENISA¹⁵, NIST¹⁶, CISA¹⁷, NSA¹⁸, FBI¹⁹, CERT-EU²⁰ stb.) származó ajánlások és úgynevezett „white paperek²¹”. Információforrások lehetnek továbbá a geopolitikai stratégiai elemzések. A környező nemzetek vagy érdekcsoportok által kiadott politikai közlemények, a hazai és külföldi sajtóban megjelent hírek, valamint a pénzügyi dokumentumok elemzése is információt szolgáltatathat. Ezek az információk magukba foglalhatnak országokra, vagy akár régiókra kiterjedő stratégiákat, törekvéseket, amelyek a szervezet saját stratégiáinak kialakításában elengedhetetlenül fontosak.

¹⁵ European Union Agency for Cybersecurity

¹⁶ National Institute of Standards and Technology

¹⁷ Cybersecurity and Infrastructure Security Agency

¹⁸ National Security Agency

¹⁹ Federal Bureau of Investigation

²⁰ Computer Emergency Response Team for EU Institutions

²¹ Olyan kiadvány, amely egy szervezet hivatalosnak tekinthető véleményét fogalmazza meg.

Stratégiai szinten az az elemzés alapvetően társadalmi-politikai szemléletet igényel, és általában olyan szakemberek végzik, akik a politikai és társadalmi elemzések terén jártasak.

A stratégiai szintű jelentések összeállítása során a fókusz a biztonsági események üzleti hatásaira és a különböző kockázatok felmérésére irányul. A jelentésekben szereplő információknak pontosnak, lényegre törőnek és időszerűnek kell lenniük, hogy támogassák a vezetői döntéshozatalt. Az elemzéseknek és jelentéseknek a célja, hogy rávilágítsanak a vezetés számára nem ismert kockázatokra is, elősegítve ezzel a tudatos döntéshozatalt.²²²³

3.2 Műveleti (operatív) szint²⁴

A műveleti szintű információszerzés a kiberbiztonság egyik kulcsfontosságú eleme, amely konkrét, azonnali cselekvésre irányuló információkra összpontosít, és lehetővé teszi a szervezetek számára, hogy hatékonyan reagáljanak a kiberfenyegetésekre. A folyamat során létfontosságú adatokat gyűjtünk a támadások természetéről, időzítéséről és potenciális hatásairól, ami lehetővé teszi, hogy előkészítsük, és összehangoljuk a válaszreakciókat.²⁵

A műveleti szintű CTI magában foglalja a támadások valós idejű azonosítását, a támadásokról szóló részletes információk gyűjtését, valamint az adott támadás várható bekövetkezésének időpontjáról szóló tájékoztatást. A műveleti szintű információszerzés célja, hogy részletes és azonnal használható információkkal lássa el a szervezetet, lehetővé téve a gyors és hatékony válaszadást.

Ezen a szinten a fő tevékenységek közé tartozik az aktív monitorozás, az azonosítás, az értékelés, a cselekvés és a helyreállítás. Az információk azonnali, gyakorlati használatra kerülnek, ellentétben a stratégiai szinttel, ahol a döntéshozatal a hosszabb távú tervezésre és a szélesebb körű trendek elemzésére összpontosít.

Az információgyűjtés a műveleti szinten kritikus fontosságú, amely magában foglalja a hálózati forgalom folyamatos figyelését, a rendszer naplófájlok elemzését, a biztonsági incidensek rögzítését, valamint a különböző intelligenciaforrásokból származó adatok integrálását. Az elemzés alapvetően fontos a fenyegetések priorizálásához, a megfelelő válaszhelyezkedések kiválasztásához, és a kiberbiztonsági helyzet dinamikus kezeléséhez.

²² Randy Borum és mtsai., „Strategic cyber intelligence”, *Information and Computer Security* 23 (2015. július 13.): 317–32, <https://doi.org/10.1108/ICS-09-2014-0064>.

²³ Jean Nestor M. Dahj, *Mastering Cyber Intelligence: Gain Comprehensive Knowledge and Skills to Conduct Threat Intelligence for Effective System Defense* (Packt Publishing Ltd, 2022).

²⁴ Katonai terminológiában alkalmazható a hadműveleti szint kifejezés egyaránt.

²⁵ „JP 1, Doctrine for the Armed Forces of the United States”, é. n., <https://irp.fas.org/doddir/dod/jp1.pdf>.

Az operatív szint információforrásai között túlsúlyba kerülhetnek a darkweben, különböző zárt közösségi média csatornáknban elérhető információk.

A műveleti szintű felhasználók körébe tartozik az eseménykezeléssel foglalkozó technikai állomány, a hálózat védelméért felelős állomány, a digitális nyomozati munkát végző-, illetve a csalások felderítésére szakosodott állomány. Mivel számukra mélyebb információ szükséges egy adott eseménnyel kapcsolatban, ezáltal képesek hamarabb felismerni, hogy a vizsgált esemény részét képezi-e egy összetettebb támadásnak, képesek a vizsgálatot kiterjeszteni a támadás egyéb elemeire, továbbá meghatározzák, hogy a rendszer melyik eleme kompromittálódott, és melyik rendszert kell helyreállítani.

Operatív szinten kiemelt jelentősége van az információk megosztásának és a megfelelő információ források kiválasztásának.

3.3 Taktikai/harcászati szint²⁶²⁷

A taktikai szintű információszerzés a leghasznosabb forma a szervezet védelme szempontjából. A fenyegető csoportok által alkalmazott TTP-k elemzésére koncentrálódik. A cél annak megértése, hogy a fenyegetettségi szereplők hogyan támadhatják meg a szervezetet, illetve annak feltérképezése, hogy a támadásokat hogyan lehet enyhíteni vagy észlelni. A taktikai szinten rendszeradminisztrátorok, mérnökök és a biztonsági személyzet hajt végre feladatokat. Az információk segítségével kiszűrhetők azok az IoC, amelyek nem bírnak jelentőséggel az adott eseménnyel kapcsolatban, vagy csak fals pozitív eredményt mutatnak. Lehetőség adódik a sérülékenységek rangsorolására annak érdekében, hogy a szervezet rendszerére legveszélyesebb kerüljön elsőként javításra. Lehetőség van továbbá automatizálni az adatfolyamokat a SIEM²⁸ rendszerek felé, így ezek a rendszerek gyorsabban és pontosabban össze tudják vetni az események és a folyamatban lévő támadások adatait. Ennek segítségével sorrendet lehet felállítani az IoC-k között, így a Biztonsági Műveleti Központ (Security, Operations Center, a továbbiakban: SOC)²⁹ elemző (level 1)³⁰ gyorsabban azonosíthatja azokat a figyelmeztetéseket, amelyek kivizsgálást, incidenskezelést igényelnek.

²⁶ Katonai terminológiában általában a harcászati kifejezést használják a szakterületek, míg a kiber szervezeteknél elfogadott a taktikai szint megnevezés is.

²⁷ JS, U.S., (2017)

²⁸ A Biztonsági Információ és Eseménykezelő (Security Information and Event Manager) rendszerek célja, hogy egy átfogó képet adjon egy szervezet informatikai biztonsági tevékenységéről és jelenlegi állapotáról.

²⁹ Biztonsági Műveleti Központ (Security Operations Center): A SOC egy olyan csapatot jelent, amely állandó műszakban működik, és amelynek egyaránt feladata a megelőzés, a felderítés és a kiberbiztonsági

Taktikai szinten a CTI az indikátorok, problémák és riasztások rangsorolásában, a hamis, fals pozitív jelzések kiszűrésében segít.

A taktikai felhasználók kezelik a tűzfalakat, az IDS/IPS³¹ rendszereket, a biztonsági átjárókat, a SIEM rendszereket, a SOAR³² platformot és az EDR³³-t. A taktikai szintű felhasználók az IoC-k segítségével közvetlenül akadályozzák meg a támadásokat a szervezet ellen. A taktikai szintű fenyegetettség elemzéshez hozzátartozik az is amikor a szervezet a saját rendszerinek sérülékenységeit és sebezhetőségeit méri fel (threat hunting).

Taktikai szinten a fő információforrások, a mások által közzétett incidens jelentések, a különböző káros kód vizsgálatokról készült jegyzőkönyvek. Ezen a szinten különös nagy jelentőség van az információ megosztásnak, a szervezetek között is két vagy többoldalú együttműködéseknek.

Ahogy az operatív szinten úgy a taktikai szinten is kiemelt jelentősége van a megfelelő információforrások kiválasztásának, és az információk megosztásának is.

3.4 Technikai szint

A technikai szint a támadó eszközeinek elemzését foglalja magába. Az eszközök mellett fontos szerepet töltenek be a támadás során használt kommunikációs csatornák, illetve a támadáshoz használt infrastruktúra elemek. A taktikai mutatóktól abban különbözik, hogy a technikai szinten a konkrét mutatókon van a hangsúly. Ilyenek pl. a domain nevek, IP címek, HASH kódok.

Ezeket a különböző mutatókat beépítik a védelmi infrastruktúrába, például tűzfalakba, levélszűrőkbe, végponti biztonsági elemekbe, ezzel lehetővé téve a támadók felderítését akár kapcsolat vagy naplóvizsgálat által. Ezen a szinten a legmagasabb fokú az automatizáció.

A technikai fenyegetettséggel kapcsolatos információszerzés összetett és költséges feladat, ugyanis analitikai megoldások és szigorú értékelések szükségesek a támadások sikeres

fenyegetésekre eseményekre adható válaszok kidolgozása, valamint a szervezet vagy létesítmény biztonsági előírásainak vizsgálata és értékelése.

³⁰ Az egyes szintű SOC elemző operatív szerepkör, amely a valós idejű biztonsági események megfigyelésére és a biztonsági események kivizsgálására összpontosít.

³¹ Behatolás jelző (Intrusion Detection System, IDS) és behatolás megelőző (Intrusion Prevention System, IPS) rendszerek.

³² A Security Orchestration, Automation and Response (SOAR) platformok olyan szoftveres megoldások és eszközök gyűjteménye, amelyek lehetővé teszik a szervezetek számára a fenyegetés- és sebezhetőségkezelést, az incidensekre reagálást, illetve a biztonsági műveletek automatizálását.

³³ A végpontészlelés és válasz (Endpoint Protection and Response) megoldás észleli és elemzi a fenyegetéseket. A végponton történő kezelés segít megszüntetni a fenyegetést és megakadályozni annak terjedését.

kivédése érdekében. Maguknak az adatoknak a megszerzése ugyanakkor az egyik legkönnyebb feladat, ugyanis rengetek az ingyenesen elérhető technikai adatforrás, úgynevezett „DataFeed” amelyek adatok millióival látnak el bennünket akár percek alatt is. Az információ szerzés költségét az adatok hitelességének ellenőrzése, a megfelelő adatok kiszűrése és validálása jelenti. Az ingyenes információforrások mellett természetesen szinten valamennyi kibervédelemmel foglalkozó vállalat kínál ilyen adatokat, a saját maga által gyártott védelmi megoldásokhoz.

A technikai mutatók adott esetben megosztásra kerülnek más szervezetekkel. A megosztás általában fórumokon CiSP³⁴³⁵, vagy közvetlen úton megy végbe, ugyanakkor fontos, hogy gépi olvasásra alkalmas formátumban kerüljenek közzétételre. Ez indokolt például az adathalász e-mailek esetében, mert gyakran szabják őket ágazatra. A harmadik féllel történő megosztás esetében fontos, hogy kizárólag ágazatspecifikus fórumokon keresztül vagy közvetlenül menjen végbe, és kizárólag mutatók kerüljenek megosztásra. Technikai szinten nem csak a támadásokhoz köthető technikai adatok elemzését hajthatjuk végre, hanem a saját rendszereinkhez tartozó adatokét is. Az úgynevezett „attack surface management” során feltérképezzük, hogy melyek azok a technikai adatok, amelyek mindenki számára láthatók (nyitott portok, eszközökről rendelkezésre álló információk) és ezáltal információt adhatnak a támadóknak, mely módszerekkel érdemes támadni a szervezetet.

³⁴ A Cyber Security Information Sharing Partnership (CiSP) egy olyan közös iparági és kormányzati kezdeményezés, amelyet azért hoztak létre, hogy a szervezetek biztonságos és bizalmas környezetben osszák meg a kiberfenyegetésekkel kapcsolatos információkat.

³⁵ „About CISP”, elérés 2024. április 4., <https://www.ncsc.gov.uk/cisp/home>.

4 A fenyegetettségi információval és azok megosztásával kapcsolatos követelmények³⁶

A CTI szintjeinek bemutatását követően az alábbi fejezetben magukkal az elemzés alapját képező adatokkal és az azok megosztásával kapcsolatos legfőbb követelményeket szeretném bemutatni.

A CTI információkkal szemben véleményem szerint a legfontosabb követelmény, hogy az elemzett információ megfelelő időben, a megfelelő megbízhatósággal és információtartalommal rendelkezésre álljon az adott döntések meghozatala érdekében.

Technikai szinten a nem megfelelő és nem időben rendelkezésre álló adat és információ a rendszerek védetten tartását veszélyezteti, de emellett rengeteg fals pozitív riasztást is generálhat.

Operatív szinten, amennyiben egy folyamatban lévő kampányról nem, vagy csak késve kap a szervezet információt abban az esetben fennáll a veszélye, hogy nem képes időben azonosítani az érintettségét az adott támadásban, ezáltal megakadályozni pl. az adatszivárgást, vagy a rendszereinek a feltérképezését. Amennyiben operatív szinten nem a megfelelő információkat kapjuk (pl. nincs olyan rendszerünk vagy rendszerelemünk, amely ellen aktív kampány folyik), az az információ feldolgozásának idejére elterelheti a figyelmet más, relevánsabb információkról. Taktikai szinten is hasonló problémákat okoz, kiegészítve azzal, hogy késedelmet szenvedhet a rendszerek felkészítése az aktuális fenyegetésekre.

Stratégiai szinten amennyiben a döntések előtt nem áll rendelkezésre valamennyi ahhoz szükséges információ, az akár elhibázott, elkésett vagy nem a fenyegetettségi helyzetnek megfelelő döntésekhez is vezethet.

A fenyegetettség elemzés taktikai, operatív és technikai szintjének olyan adatokat és információkat kell tartalmaznia, amely az adott szinten lévő technikai eszközök, vagy humán erőforrás által végrehajtható. Technikai szinten pl. olyan adatforrásokat, és adatfolyamatokat kell használni, amely közvetlenül, emberi beavatkozás nélkül feldolgozható a végpontvédelmi eszközök által.

Stratégiai szinten a vezetők számára, operatív és taktikai szinten a biztonsági személyzet számára, technikai szinten pedig a gépek számára érthetően kell fogalmazni. A stratégia CTI esetén elengedhetetlen, hogy az elemzéseket olyan emberek is megértsék, akik nem feltétlenül

³⁶ Christopher S. Johnson és mtsai., „Guide to Cyber Threat Information Sharing” (National Institute of Standards and Technology, 2016. október), <https://doi.org/10.6028/NIST.SP.800-150>.

értik a technikai szakkifejezéseket. Számukra azok az információk fontosak, amik a stratégia döntéseket támogatják, valamint hozzájárulnak a szervezet fenyegetettségének megértéséhez és segítik eldönteni, hogy az adott információbiztonsági beruházásra szükség van-e.

A fenyegetettség elemzés végterméke, az elkészült dokumentum, vagy akár az elemzett technikai információk is, amennyiben a szervezeten belül maradnak akkor talán az egyik legfontosabb velük szemben megfogalmazott követelménynek nem tesznek eleget, vagyis nem segítik a fenyegetések előrejelzését a megfelelő védelem kialakítását. A fenyegetések kezelése esetén kiemelt jelentősége van annak a magyar közmondásnak, hogy „Más kárán tanul az okos.”

A CTI esetén ezért is kiemelt fontosságú a keletkezett végtermékek megosztása. A megosztás alatt nem csak a szervezeten belül, a különböző szervezeti egysége között van jelentősége, hanem az ágazaton belül, az ágazatok között nemzeti szinten és nemzetközi szinten is.

A szervezeten kívüli megosztás esetén kiemelt figyelmet kell fordítani a megosztani tervezett információk hatására a saját szervezetünk esetében. Nem kerülhet megosztásra olyan információ vagy adat, amely bármilyen szinten negatívan érintené a szervezet stratégiai célkitűzéseit, vagy az elektronikus információs rendszereinek biztonságát. Az adatmegosztás, az adatok forrásának felmérése során az alábbiakat kell figyelembe venni.

- Minden esetben fel kell mérni milyen lehetőségek állnak rendelkezésre, hogy információt osszunk meg.
- Fel kell mérni milyen ágazati szervezetek vannak, akik rendelkeznek számunkra releváns információval és osztanak meg információt.
- A felmérés során figyelmet kell fordítani arra is, hogy milyen megosztható adatok állnak rendelkezésre és mi az, amit a többiek meg tudnak osztani, mennyire hasznosítható az.
- Fel kell mérni az automata módon megosztható adatok körét. A stratégiai szintem automatán megosztható adatok nem állnak rendelkezésre.
- Stratégiai szinten kiemelt figyelmet kell fordítani az információk érzékenységre. Bizonyos adatok megosztása akár a fenyegetettséget is növelheti.
- Figyelembe kell venni a továbbá az információk megosztására vonatkozó jogi előírásokat is. Ezek az előírások nem csak a megosztó félre vonatkozhatnak, hanem arra is aki az adott információt kapja.

- A stratégiai szintű adatmegosztásánál a TLP (Traffic light Protocoll) használat javasolt. A TLP szerint a RED jelzés esetén az információ csak a közvetlen résztvevőkkel osztható meg, GREEN esetén az információ a közösségen belül osztható meg. A WHITE jelzés esetén mindenféle korlátozás nélkül közzé tehető az információ, míg az AMBER esetén a legnehezebb a pontos meghatározás, ugyanis azt jelenti, hogy azokkal lehet megosztani az információt az adott szervezeten belül, akiknek érdeke fűződik hozzá. Az AMBER jelölés esetén a korlátozásokat az információ forrása jelöli meg.
- Az információmegosztásra kialakított eljárásrendet folyamatosan felül kell vizsgálni. A felülvizsgálat során felül kell vizsgálni, a megosztandó információk körét, a közösségeket ahonnan információt kapunk és akiknek információt adunk és figyelembe kell venni a megosztásra vonatkozó jogszabályi előírások változását is.

5 Kihívások a CTI-al kapcsolatosan³⁷

A Crowd Strike Global Threat Report³⁸ 2023 kiadványa szerint az elkövetőknek 2022-ben átlagosan 84 perc kellett ahhoz, hogy a hálózatban a megfertőzött gépről átmenjenek egy másik gépre (lateral movement). Ez az értéke 2021-ben még 98 perc volt. Ahhoz, hogy minimalizáljuk egy adott támadás gazdasági hatásait, ezalatt az idő alatt meg kell történnie a válaszadásnak a támadásra. A védekezés során igyekezni kell betartani az 1-10-60 perces szabályt. Észlelni kell a fenyegetést az 1 percen belül, 10 perc alatt meg kell érteni és 60 perc alatt válaszolni kell rá.

Az adatszivárgásokat átlagosan 206 nap alatt fedezik fel míg a megszüntetésükhöz további 876 napra van szükség átlagban³⁹.

A CTI elsősorban a hírszerzési-, számítástechnikai és számítógép-biztonsági területekre épít, mint például a rosszindulatú programok elemzésére, a számítógépes hálózatok biztonságára és a behatolástesztelés (vagy sérülékenységvizsgálat). Kisebb mértékben a helyzetfelismeréssel, kockázat-előrejelzéssel és kockázatkezeléssel kapcsolatos korábbi tapasztalatokra⁴⁰.

Összesen majdnem 28 ország gyanúsított azzal, hogy kiberműveleteket támogat. Ezek a műveletek a kémkedéstől a kritikus infrastruktúrák elleni támadásokig terjednek. A legtöbb műveletet az internetbiztonsággal foglalkozó vállalatok derítették fel.

Egyes szerzők szerint a CTI területén a technológiai kihívások már többé kevésbé megoldásra kerültek ugyanakkor még mindig tapasztalhatók kihívások a területen, de ezeket nem technológiai, informatikai szempontból kell megoldani, hanem növelni kell az elemző-értékelő képességet.

A CTI alapvetően a védekező tevékenységeket támogatja. Célja ugyanis a rendszerbe történő behatolások okozta kár mérséklése és a korai felismerés előrejelzés elősegítése. A támadók és a védekezők közötti tudáskülönbség csökkentése is a céljai közé tartozik.

Napi szinten a CTI inkább a beérkező riasztások, adatok és információk alapján dolgozik, mintsem előre megfogalmazott feltevések és koncepciók alapján.

³⁷ Kris Oosthoek és Christian Doerr, „Cyber Threat Intelligence: A Product Without a Process?”, *International Journal of Intelligence and CounterIntelligence* 34, sz. 2 (2021. április 3.): 300–315, <https://doi.org/10.1080/08850607.2020.1780062>.

³⁸ Crowdstrike. (2024) Global Threat Report 2024.

³⁹ „Cost of a Data Breach 2023 | IBM”, elérés 2024. április 8., <https://www.ibm.com/reports/data-breach>.

⁴⁰ „ENISA Threat Landscape 2023”, Report/Study, ENISA, elérés 2024. április 5., <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.

A hatékony CTI megvalósításához azonosítani szükséges, hogy milyen információkra van szükségünk. ezt legkönnyebben úgy tudjuk megtenni, ha különböző forгатókönyveket álltunk fel. A forгатókönyvek nem csak az incidenskezelés esetén, hanem a fenyegetettségi információ igények felmérése esetén is rendkívül hasznosak. A forгатókönyvek esetén mindig súlyozni szükséges az eseteket azok rendszerekre és a szervezet működésére gyakorolt hatása, valamint a pénzügyi veszteségek alapján is

Ezeket a forгатókönyveket úgy érdemes összeállítani, hogy abban pontosan definiálva legyenek, hogy mik a fenyegetettségi információ „fogyasztóinak” információigényei. ezeket milyen forrásból, milyen módon, milyen gyakorisággal és hogyan gyűjtjük a számukra, milyen módos és hogyan osztjuk meg velük, hogy azokat lehető legjobban támogassák az elérni kívánt célokat. A megfelelő priorizálás mellett, ami segít a CTI-t előállító csapatnak megszervezni a munkát, arra is figyelmet kell fordítani, hogy olyan célokat határozzunk meg amelyeket el lehet érni és teljesíteni lehet az információigényeket. Itt arra érdemes gondolni, hogy a „Kínával kapcsolatos fenyegetések” meghatározás túl tág ahhoz, hogy biztosan a megfelelő információkat szolgáltatassuk. Az igény pontos megfogalmazása pl. A XY pénzügyi rendszereket támadó csoportok jellemző behatolási technikája, vagy a villamosenergia elosztókat támogató SCADA rendszereket célpontnak tekintő csoportok technikái” sokkal specifikusabb, végrehajtható információkat eredményez. Az így meghatározott követelmények ezen kívül mérhetővé is teszik a teljesítményt.⁴¹

A hatékony CTI-hoz mindenképpen érdemes felállítani egy úgynevezett „Fenyegetettségi Profilt”, amely megmutatja a leginkább aktuális és figyelembe veendő fenyegetéseket és az azokhoz köthető elkövetőket⁴²:

A CTI folyamat végtermékét jelentő dokumentummal kapcsolatban érdemes megfontolni a készülő dokumentum nyelvezetét, ugyanis más megfogalmazás szükséges, az incidenskezelő állomány és más a felsővezetés tájékoztatás során. a nyelvezet mellett ugyan olyan fontos, hogy a felhasználók. Azt is érdemes megfontolni, hogy milyen gyakorisággal érdemes kiadni a dokumentumokat.

A célközönség azonosításakor figyelembe kell venni azon csoportok, szervezeti egységek funkcióit, feladatait, a rájuk vonatkozó szabályzókat is, akiknek a CTI-t szánjuk, valamint azt is, hogy milyen fenyegetettségi információkra van szükségük. Bizonyos esetekben magának a

⁴¹ Oosthoek és Doerr, „Cyber Threat Intelligence: A Product Without a Process?”

⁴² „A Requirements-Driven Approach to Cyber Threat Intelligence”.

fenyegetettség elemzésnek a népszerűsítésére is szükség lehet. Be kell mutatni annak előnyeit és hasznait is a bizonyos szervezeti egységek és főleg a vezetők számára. Ilyenkor érdemes példákkal illusztrálni, hogy milyen „végtermékeket” vagyunk képesek előállítani.

A CTI esetén az információk nagy része nem dokumentum formában kerül előállításra és megosztásra. Ezek az információk nagyrészt gépek által feldolgozható információk. A gépek közötti információmegosztásra is léteznek protokollok, mint például a STIX (Structured Threat Information eXpression), de CTI információk nagy többsége ugyanakkor továbbra is nem strukturált információ. A megosztás formátuma lehet .pdf dokumentum, vagy csak simán vesszővel elválasztott adatok.⁴³

Az IoC-k, vagyis a technikai adatok elsődleges feladata, hogy segítségükkel feltérképezzük a hálózatokat, kutatva azokban az esetleg kompromitáció jelei után. Ezek azonban sok esetben fals pozitív eredményeket is adhatnak. Sok szakember a csak IoC adatokat nem tekinti CTI - ak, mert a hálózatban megtalálható technikai adatok, logokkal történő összevetés nélkül nem lehet őket kontextusba helyezni. Ezáltal nem tekinthetők befejezett elemzett adatnak. inkább egy köztes terméknek, amelyet a fenyegetettségi környezettel együtt kell értékelni.⁴⁴

A CTI-t előállító cégek esetében, a humán elemző-értékelő tevékenység esetén is fennáll az elfogultság esete. Ezen cégek esetén nem az elemzés során, hanem az adatforrások esetén beszélhetünk elfogultságról. A cégek által kiadott jelentések elsősorban a nagy, államilag szponzorált hackercsoportokról szólnak, mivel ezekkel az elemzésekkel lehet előfizetéseket szerezni. Probléma tovább, hogy a cégeknek nem minden régióban van hozzáférése a rendszerekhez, ezért minden cég esetén vannak olyan területek, ahonnan nem rendelkeznek adatokkal.

Sok esetben az államilag támogatott hackercsoportokon kívül a nagy vállalatok nem rendelkeznek olyan kisebb államilag támogatott csoportokról adatokkal, akik szintén releváns fenyegetést jelenthetnek egy adott régióban, mint pl. a török vagy az indiai csoportok, akik szintén fenyegetést jelenthetnek.

Az internetbiztonsági vállalatok esetében nyílt titok az is, hogy bizonyos régiókkal kapcsolatos kibertevékenységeket nem figyelnek, nem késztenek róla jelentést. (CrowdStrike pl. nem

⁴³ Md Sahrom és mtsai., „Cyber Threat Intelligence – Issue and Challenges”, *Indonesian Journal of Electrical Engineering and Computer Science* 10 (2018. április 1.): 371–79, <https://doi.org/10.11591/ijeecs.v10.i1.pp371-379>.

⁴⁴ Ensar Seker, „Cyber Threat Intelligence Understanding Fundamentals”, 2019. szeptember 9.

jelen azamerikai csoportok tevékenységéről, ahogy a Kaspersky vállalat is ritkán készít átfogó jelentéseket orosz csoportok tevékenységéről)

A tevékenységek csoportokhoz történő kötése, vagyis az attributálás is kifejezetten problémás terület. Ezt megnehezíti az is, hogy a cégek esetén nem egységes a csoportok elnevezése.

Az Oroszországi Föderáció Fegyveres Erői Vezérkarának Felderítő Főcsoportfőnöksége (GU⁴⁵) köthető csoport elnevezése példaértékű: Fancy Bear (CrowdStrike), APT-28 (Mandiant/FireEye), Sofacy (Kaspersky), STRONTIUM (Microsoft), Sednit (ESET), Tsar Team (iSight), Swallowtail (Symantec), Pawn Storm (Trend Micro), TG-4127 (SecureWorks), Grizzly Steppe (U.S. kormányzata). Ezenkívül a különböző elnevezések az adatok összevetését is nagyban megnehezítik.

⁴⁵ Glavnoje razvedivatyelnoje upravlenyje

6 A fenyegetések leírására használt módszertanok

A fenyegetés elemzés végrehajtása során nem csak annak szintjén lehet meghatározni. A stratégiai szintű fenyegetettség elemzés a klasszikus elemző értékelő módszertanokat alkalmazza. Stratégiai szinten az elemzés ismeretanyaga a társadalomtudományi kutatások kvalitatív módszereire épít.

Operatív, taktikai és technikai szinten a fenyegetés vállalatra és azok rendszereire gyakorolt hatásának meghatározására számtalan módszertan került kialakításra.

A fenyegetés szintjének és hatásának meghatározására használt módszeranok sok esetben arról is adnak információt, hogy esetleg milyen hatékony ellenintézkedést tudunk végrehajtani a veszély csökkentése érdekében.

Mindegyik módszertan más alapján elemzi a támadásokat, a Lockheed Martin féle Cyber Kill Chain pl. a katonai harcérintkezés lépései szerint osztja különböző fázisra a támadásokat. A Diamond Modell alapvetően különbözik a Cyber Kill Chain-től és a MITRE ATT&CK keretrendszerétől is.

A Cyber Kill Chain például a támadások különböző fázisaira koncentrál a felderítéstől a támadás céljának végrehajtásáig, addig a Diamond Modell inkább a támadó és az áldozat közötti kapcsolatra helyezi a hangsúlyt.

A Diamond Modelltől eltérően a MITRE ATT&CK keretrendszer sokkal inkább az ellenfél TTP-inek részletezésére összpontosít, konkrét taktikákat leképezve a védekezési stratégiákra.

Mindegyik keretrendszer a kibertámadás különböző összetevőire vagy elemeire összpontosít, segítve az elemzőket, hogy holisztikus képet kapjanak az incidensről.

A Piramid of Pain módszertan alapja, hogy mennyire érinti fájdalmasan a támadót, ha meg kell változtatnia a támadása során az alkalmazott technikai paramétereket, taktikákat.

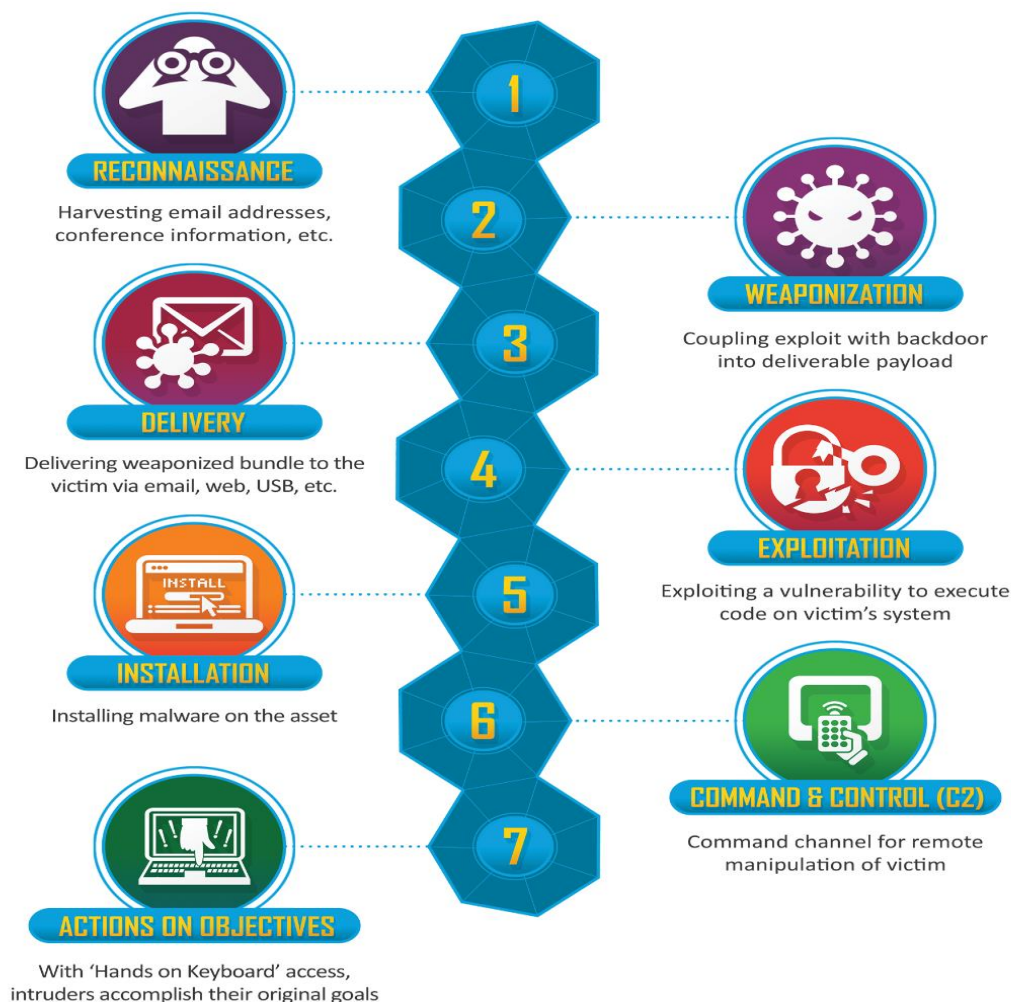
6.1 Cyber Kill Chain⁴⁶

A Lockheed Martin cég szakemberei által felállított modell alapját a katonai harcérintkezés lépései adják. Az egész modell alapját az indikátorok jelentik, amelyeket egyes szakaszokban meg lehet figyelni. Az indikátorok minden olyan információ részletet jelentenek, amit az egyes szakaszokban meg lehet figyelni.

⁴⁶ Eric Hutchins, Michael Cloppert, és Rohan Amin, „Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, *Leading Issues in Information Warfare & Security Research* 1 (2011. január 1.).

A modell a támadók szempontjából állít fel egy olyan keretrendszert, aminek segítségével nyomon követhetők a támadók lépései. Minden egyes lépésnél leírásra kerül a támadók magatartása és az is, hogy a védőknek milyen lépéseket kell megtenni az adott szakaszban a támadás megszakítása érdekében. Az elmélet szerint a támadás bármely szakaszában végrehajtott védekező művelet a támadás sikeres megszakításához vezet. Elsősorban a fejlett hosszantartó fenyegetést, vagyis az úgynevezett APT⁴⁷ támadásokat írja le.

A modell által felvázolt támadási lépéseket az alábbi ábra szemlélteti.



4. ábra: Cyber Kill Chain (<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>)

A támadás során az első lépés a „Felderítés” (Reconnaissance) vagyis a célpont(ok) beazonosítása.

⁴⁷ APT: advanced persistent threat, folyamatosan jelenlévő rejtett fenyegetés, olyan támadástípus, amely jellemzően kémkedésre és az adatok eltulajdonítására irányul és nem rongálásra, vagy a rendszerek elérhetetlenné tételére.

Ebben a fázisban a támadók a műveleteik megtervezését végzik, információt gyűjtenek, a megtámadni szándékozott szervezet rendszereiről és működéséről, esetleges hibák után kutatnak, amiknek a kihasználásával elérhetik a céljaikat. Az esetek nagy többségében az információkat OSINT⁴⁸ módszerekkel gyűjtik a nyílt, a dark- és a deepweben. Ide tartozik a nyitott portok felderítése és a közösségi médiás aktivitás elemzése is. Ebben a fázisban a támadók lépéseit nehéz észlelni, amennyiben nem vétének nagyobb hibákat. A támadási célpont felderítése ellen a védekező állomány célszerű, ha rendszeresen ellenőrzi az internet felől elérhető szerverek és egyéb hálózati eszközök logjait, rendszeresen ellenőrzi a nyitott portokat és időről időre figyelemmel kíséri a szervezetről megjelenő információkat. Ilyen információ lehet pl. a vezetők nevei, az email elérhetőségek formátuma, amikor, honnan és milyen időintervallumban jelentkeztek be a vállalat rendszereibe stb.

A második szakasz az úgynevezett “Fegyverkezés” (Weponization), amely során a támadók részéről megtörténik a felkészülés a műveletre. A támadók ebben a fázisban a korábban gyűjtött és elemzett adatokra építve elkezdik a felkészülést magára a támadásra. Ehhez általában publikusan, vagy csak zárt körben elérhető, esetleg házon belül, egyedileg fejlesztett eszközöket (exploit kit-eket, egyedi exploit-okat) használnak. A fájl-alapú exploit-okhoz elkészítik a megfelelő csali-dokumentumokat és előkészítik a kompromittált eszközökre szánt hátsó ajtókat biztosító szoftvereket (back door), valamint a C2 (command & control) infrastruktúrákat majd lefordítják a megalkotott programkódokat. Az elmúlt időszakban egyre többször fordulnak elő „living of the land” támadási technikák, amely során a támadók a rendszerekben található szoftvereket, programokat használják fel a támadás során. Ebben az esetben a támadó kódok fejlesztése elmarad, csak a rendszerekről begyűjtött adatok elemzése képezi ennek a fázisnak a feladatait.

Ez a fázis, alapvető fontosságú a védők számára, az előzőekben már használt rosszindulatú kódok (malware) elemzéseinek adatai segíthetnek átlátni a támadók módszereit és segíthet olyan eszközöket és technikákat kifejleszteni, amik javítják az adott szervezet észlelési képességeit. A védőknek ebben a fázisban érdemes figyelemmel követni, hogy a támadók milyen eszközöket (exploit kit-ek, újrahasznosított egyedi fejlesztési malware-ek, stb.) milyen támadásoknál használtak, azok széles körben használtak vagy csak néhány, jól meghatározható esetben? Ebben a fázisban kiemelt jelentősége van az

⁴⁸ Open Source Intelligence: nyílt forrású információgyűjtés

információmegosztásnak és a különböző internetbiztonsági cégek által közzétett jelentések nyomonkövetésének.

A harmadik fázis a modell szerint a „A támadás megindítása” (Delivery) amely során a malware célba juttatása történik meg. Ebben a fázisban a támadók szinte kizárólag két módszerrel szoktak élni, az első az aktív támadás, amikor az interneten elérhető szervereket veszik célba és azok sérülékenységeit kihasználva szereznek hozzáférést. A másik módszernél a különböző csali eszközöket (e-maileket vagy fizikai adathordozókat juttatnak a célponthoz vírusos fájlokkal, különböző közösségi oldalakon végrehajtott műveleteket vagy fertőző weboldalak, gyakran legitim weboldalakon elhelyezett exploitokat használva).

A védők ebben a fázisban tudják először megakadályozni magát a támadást. Ebben a fázisban kiemelt jelentőségű, hogy a védők folyamatosan elemezzék a támadó csoportokról rendelkezésre álló információkat, ismerjék a támadók által leggyakrabban használt malwareket, exploitokat és az infrastruktúra felépítését, és ismerjék a leggyakoribb támadási formákat.

A negyedik szakasz a „Sérülékenység kihasználása” (Exploitation) amely szakaszban a támadók Hozzáférést szereznek a célba vett rendszerhez. Ennek érdekében a támadók kihasználják a már korábban felfedett sérülékenységeket, amelyek lehetnek szoftveresek, hardveresek, de adódhatnak emberi mulasztásból vagy hibából. Szoftveres sérülékenység lehet egy nem telepített frissítés, vagy egy úgynevezett „0 day” megjelenése, emberi mulasztás pedig egy adathalász link megnyitása, vagy egy pszichológiai manipuláció (social engineering” során megadott hozzáférési adat.

A védők számára ebben az esetben a célba vett rendszerek esetén a hagyományos hardening-technikák nyújthatnak bizonyos fokú ellenálló képességet, de például a nulladik napi sérülékenységeket célzó támadások elhárításához egyedi képességekre is szükség van. A védekezésben fontos szerep jut a biztonságtudatossági képzéseknek, a fejlesztők biztonságos fejlesztési technikákra történő oktatása, rendszeres sérülékenység vizsgálatok és betöréstesztek végrehajtása.

Az ötödik lépés során történik meg a támadók részéről a „Hátsó ajtók telepítése” (Installation) ami tulajdonképpen a „hídfő” kiépítése az áldozat rendszerében. A támadók ebben a fázisban a megszerzett hozzáférés(ek) hosszabb időn át történő fenntartására koncentrálnak, különböző hozzáférési módok kialakításával, pl. webshell vagy különböző backdoor-ok telepítésével.

A védők ebben a fázisban leginkább a különböző végponti biztonsági eszközökkel, host IPS-ekkel és más végpontvédelmi megoldásokkal tudnak védekezni. A védekezésben sokat segíthet a végponti folyamatok ellenőrzése illetve a fájl konzisztencia ellenőrzésre használható megoldások, valamint a digitálisan aláírt futtatható állományok tanúsítványainak vizsgálata is.

A hatodik lépés az „Irányítás” (Command & Control - C2), amely a kompromittált rendszer távoli vezérlését jelenti. Ebben a fázisban a támadók olyan kétirányú kommunikációt próbálnak építeni a kompromittált eszköz és egy, a saját irányításuk alatt lévő szerver között, amivel később is a céljaiknak megfelelően tudják használni az adott eszközt.

A hetedik és egyben a támadás utolsó fázisa a „A cél elérése” (Actions on objectives). Ebben a fázisban a támadók végrehajtják a valódi céljaikat, adatokat, gyűjtenek és szivárogtatnak ki, megpróbálnak a rendszerhez magasabb szintű (adminisztrátori) hozzáférést szerezni, feltérképezni a teljes hálózatot, titkostani a rendszerben tárolt adatokat, stb.

Ebben a fázisban a védőknek az a célja, hogy minél előbb megszakítsák magát a támadó műveletet, és megkezdjék az incidens kezelés folyamatát.

6.2 The Diamond Modell⁴⁹

Szintén a kibertámadások azonosítására használható modell. A célja, hogy azonosításra kerüljenek a támadók taktikai technikái és eljárásrendjei, valamint maguk a támadók is.

A keretrendszerben az elemi eseményeket határozzák meg amelyeket aztán a továbbiakban „Diamond Eventnek” neveznek. Az elemzők ezeket az eseményeket összekötik egymással és ez alapján próbálják meghatározni, hogy hogyan és mi történhetett pontosan. A modell alapján az elemzést végzők azt is könnyen azonosíthatják, hogy melyek a hiányzó adatok az eseménnyel kapcsolatban.

A modellnek négy komponenst vesz figyelembe.

- Ellenérdekelte fél: a támadó vagy a csoport, aki a támadásért felelős.
- Infrastruktúra: az a technikai megoldás, amit a támadó fél használ.
- Képesség: az a módszer vagy eszköz, amit a támadó fél használ a támadás során.
- Áldozat: az az egyén vagy szervezet, amit a támadó fél megtámadott.

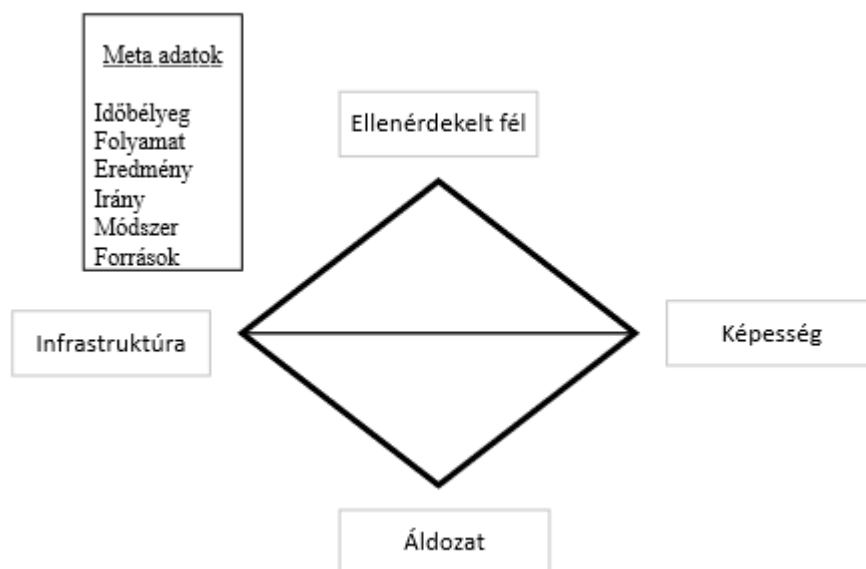
⁴⁹ Sergio Caltagirone, Andrew Pendergast, és Christopher Betz, „The Diamond Model of Intrusion Analysis”, 2013, <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>.

A felsorol komponensek között többfajta kapcsolat is lehetséges.

„Az ellenérdekelt felek használják a képességeiket az áldozaton az infrastruktúrájuk segítségével.”

A kapcsolatok közül az

1. ellenérdekelt fél és a támadó közötti kapcsolat: azt mutatja be, hogy a támadó miért ezt az áldozatot választotta és hogy mik az támadó fél motivációi;
2. A támadó fél és az infrastruktúra közötti kapcsolat: ez a kapcsolat arra keresi a választ, hogy a támadó, hogyan valósította meg a támadást;
3. az áldozat és az infrastruktúra közötti kapcsolat: az áldozat és a támadó technikai erőforrásai közötti kapcsolat. ez a kapcsolat arra keresi a választ, hogy a támadó fél, milyen eszközöket használ az áldozat infrastruktúráján;
4. áldozat és a támadó fél képességei közötti kapcsolat: azt írja le, hogy a támadó milyen taktikát, támadási vektort használ az áldozat ellen.



5. ábra: Diamon Modell (forrás: <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>) alapján saját szerkesztés

Az eredeti modellben 7 axioma (alapigazság) is megfogalmazásra kerül az eseményekkel, az ellenérdekelt felekkel és az áldozatokkal kapcsolatban. Ezeket érdemes szem előtt tartani amikor kivizsgáljuk az adott eseményt.⁵⁰

1. „Minden eseménynél létezik egy ellenfél, aki lépéseket tesz a kitűzött cél felé, hogy eredményeket érjen el úgy, hogy egy adott infrastruktúrán keresztüli képességet használ az áldozat ellen.”
2. „Létezik egy sor ellenfél (bennfentesek, kívülállók, egyének, csoportok és szervezetek), amelyek kompromittálják a számítógépes rendszereket vagy hálózatokat, hogy előmozdítsák szándékukat és kielégítsék szükségleteiket.”
3. „Minden rendszer, és tágabb értelemben minden áldozatnak van sebezhetősége és kitettsége.”
4. „Minden rosszindulatú tevékenység két vagy több fázist tartalmaz, amelyeket egymás után sikeresen végre kell hajtani a kívánt eredmény eléréséhez.”
5. „Minden behatolási eseményhez egy vagy több külső erőforrás szükséges ahhoz, hogy elégedett legyen a sikerrel.”
6. „Mindig létezik kapcsolat az Ellenfél és Áldozata(i) között, még akkor is, ha távoli, múltó vagy közvetett.”
7. „Létezik az ellenfelek halmazának egy részhalmaza, amelyek rendelkeznek a motivációval, erőforrásokkal és képességekkel, hogy jelentős ideig fenntartsák a rosszindulatú hatásokat egy vagy több áldozattal szemben, miközben ellenállnak a mérséklő erőfeszítéseknek. Az ellenfél-áldozat kapcsolatokat ebben az alhalmazban tartós ellenséges kapcsolatoknak nevezzük.

Az analitikai vizsgálat során a modellben egy pontból elindulunk és megpróbálunk minél több információt megtudni a többi pontról. Például az áldozat tanulmányozása segíthet, hogy több információhoz jussunk az ellenérdekelt fél képességeiről és infrastruktúrájáról.

A Diamond modell legnagyobb előnye nem abban van, hogy egy bizonyos eseményről legyen minél több információnk, inkább abban tud segítséget nyújtani, hogy az ellenérdekelt fél időbeni tevékenységét tanulmányozzuk a segítségével.

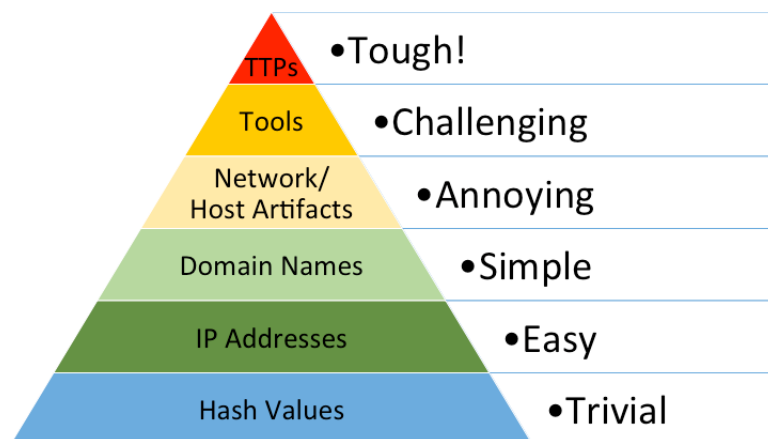
A támadó tevékenységének vizsgálata megmutatja, hogy az események hogyan kapcsolódnak egymáshoz, valamint azt is, hogy a többi áldozaton végrehajtott támadások között milyen ok-

⁵⁰ Chad Warner, „Diamond Model in Cyber Threat Intelligence”, *Medium* (blog), 2023. december 11., <https://warnerchad.medium.com/diamond-model-for-cti-5aba5ba5585>.

okozati összefüggések vannak. Az események összevetése a tevékenységeken keresztül segít azonosítani a kampányokat és segít abban is, hogy teljesebb képet kapjunk az ellenérdekelt fél viselkedéséről. A viselkedés jobb megismerése segít a védekezés jobb megtervezésében.

6.3 Piramid of Pain

A „Fájdalom Piramisa” David J Bianco találmánya, aki 2013-ban publikálta az egy blogpostban⁵¹. A módszertan azt igyekszik bemutatni, hogy az eseményekkel kapcsolatos egyes technikai paraméterek elleni ellenintézkedések mennyire érintik fájdalmasan a támadókat, mekkora problémát okoznak számukra az ellenintézkedések kikerülése.



6. ábra Piramid of Pain (forrás: <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>)

1. **Hash értékek:** SHA1, MD5 vagy más hasonló hash értékek, amelyek egy specifikus rosszindulatú, vagy gyanús fájlhoz tartoznak. Általában arra használják őket, hogy egyértelműen azonosítsanak egy rosszindulatú kódot vagy fájlt, ami egy támadásban szerepel.
2. **IP címek:** IP cím, de jelenthet netblock-ot is .
3. **Domain nevek:** ez lehet önmagában egy domain név (pl. valami.net) de lehet egy subnet domain is (pl. ez.aztan.valami.net).
4. **Hálózati „nyomok”:** Olyan megfigyelések (megfigyelhető változások), amiket a támadás során lehet a hálózatban megfigyelni. Technikai értelemben minden egyes byte, ami áthalad a hálózaton egy támadás során lehet ilyen, de valójában ezek olyan adatok/megfigyelések, amelyek segítségével meg lehet különböztetni a támadó tevékenységét a normál hálózati forgalomtól. Tipikusan ilyenek az URI minták, a

⁵¹ David J Bianco, „Enterprise Detection & Response”.

hálózati protokollba beágyazott C2 információk, különböző HTTP User Agent-ek vagy SMTP mailer értékek.

5. **Végponti „nyomok”**: Olyan megfigyelhető változások, amiket egy támadó okoz egy vagy több végponti eszközbe. Itt is olyanokat kell keresni, amik megkülönböztetik a legitim adatokat a rosszindulatú ellenérdekelt fél által okozott tevékenységtől. Ezek lehetnek registry key-ek, amelyeket egy specifikus rosszindulatú kód okozott, vagy speciális fájlok, könyvtárak amiket egy malware hoz létre.
6. **Eszközök**: Az ellenérdekelt felek által, a céljai eléréséhez használt szoftver. A legtöbb esetben ezek olyanok lesznek, amiket ők hoznak magukkal (bár mostanában kezd elterjedni a legitim az operációs rendszerben már meglévő szoftverek rosszindulatú használata). Ezek azok a segédprogramok, amelyek rosszindulatú dokumentumok létrehozására szolgálnak titkos adathalászat céljára, a C2 vagy jelszótörők létrehozására használt hátsó ajtók, vagy egyéb gazdagép alapú segédprogramok, amelyeket a támadók a feltörést követően használni akarnak
7. **TTP**
8. **-k**: Hogyan érik el a támadók a céljaikat, a felderítéstől egészen végig az adat kiszivárogtatásáig minden egyes lépésen keresztül. Az „adathalászat” egy tipikus TTP ahhoz, hogy be tudjanak hatolni a hálózatba. Adathalászat egy trójait tartalmazó .pdf fájlal, vagy káros kód letöltését lehetővé tévő linkkel.

A piramis azt mutatja meg, hogy ha egy támadó rosszindulatú programokat használ a támadási láncon belüli végpont megfertőzésére, a védő tudni fogja, hogy az ilyen viselkedés észleléséhez és a támadás megállításához a fájl hash értékének blokkolásánál többet kell tennie. Ennek az az oka, hogy a támadók számára „triviális” megkerülni a technikát (egyszerűen újrafordíthatják a kártevő-mintát, így a védő által az eredeti minta észlelésére használt fájl hash értéke használhatatlanná válik). Hasonlóképpen, ha a védő hálózati védelmi eszközei IP-címet, CIDR-blokkot vagy akár ASN-tartomány feketelistáját használnak a rosszindulatú hálózati kommunikáció megzavarására, a Piramis azt sugallja, hogy továbbra is bajban lehet, mivel ezeket a vezérlőket „könnyű” megkerülni (ebben az esetben a támadó egyszerűen áthelyezheti a C2 infrastruktúráját vagy műveleti központját egy másik hálózati kiszolgálóra).

6.4 MITRE ATT&CK⁵²

A keretrendszer egy olyan adatbázis, amely szabadon, mindenki számára elérhető és a kibertéri támadók technikáinak és taktikáinak valós megfigyelésén alapul.

A MITRE ATT&CK alapként szolgált mind a privát, mind a kormányzati szférában a fenyegetettségi modellek előállítására.

Az adatbázist folyamatosan karbantartott információt szolgáltat a kibertérben tevékenykedő támadók viselkedéséről, annak megfelelően csoportosítva, hogy az a támadás melyik szakaszában figyelhető meg, valamint folyamatosan friss információt szolgáltat az APT és egyéb csoportok éppen aktuális célpontjairól. A keretrendszer főleg arra fókuszál, hogy a külső ellenérdekelt felek, hogyan hatolnak be és hogyan tevékenykednek a rendszerekben. A keretrendszer felépítése eredetileg abból alakult ki, hogy dokumentálni és rendszerezni szerették volna a Windows rendszer elleni támadásokat követően az elkövetők, technikáit, taktikáit és eljárásrendjeit, annak érdekében, hogy fejlesszék a rendszer védelmét és a támadások felismerésének képességét. A projekt ezt követően kiegészült a Linux és a macOS elleni támadások és ellenérdekelt felek tulajdonságainak és tevékenységének összegyűjtésével és kategorizálásával, a rendszerbe történő behatolást megelőző lépésekkel, valamint az elmúlt időszakban a keretrendszert kiegészítették olyan technológiákra is mind a mobil kommunikáció, a felhő alapú rendszerek és az ipari vezérlő rendszerek.

Alapvetően a MITRE ATT&CK keretrendszer az alábbi részegységekből épül fel:

- Taktika: rövid távú, a taktikai ellenérdekelt felek (, tactical adversary goals during an attack) rövid távú céljai a támadás során
- Technika: azokat az eszközöket írja le amelyekkel a támadó eléri a céljait
- Sub-techniques/ al/rész-technikák: sokkal specifikusabb eszközöket ad meg amellyel az ellenérdekelt felek eléri a taktikai céljaikat, ezek alacsonyabb szintűek, mint a technikák,
- A technikák, eljárásrendek és metaadatok leírásai.

Maga a keretrendszer a szoftverek elleni támadási technikákkal kapcsolatban nem teljes. Ezekre a vizsgálatokra alkalmasabb lehet a CAPEC⁵³ ami szintén a MITRE fejlesztése vagy a a CWE⁵⁴ használata.

⁵² Blake Strom és mtsai., „MITRE ATT&CK: Design and Philosophy”, 2020. március 31., <https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy>.

A keretrendszer a támadókkal és a kampányaikkal kapcsolatos információkat rendszerezi, a támadók taktikái szerint. Ezek a taktikák azok a technikai célok, amelyeket a támadók meg akarnak valósítani. Jelenleg az alábbi kategóriákat tartalmazza a keretrendszer:

- Felderítés (Reconnaissance): olyan taktikák, amelyek aktívan vagy passzívan információt gyűjtenek, a jövőbeni célzott támadások tervezése érdekében
- Erőforrás fejlesztés (Resource development): olyan taktikákat foglal magába amelyekkel a támadók erőforrásokat lopnak vagy vásárolnak, hogy egy jövőbeni támadás során használják fel;
- Kezdeti hozzáférés (Initial access): Azok a technikák amelyekkel a támadók különböző támadási vektorok segítségével hozzáférést akarnak szerezni a hálózathoz
- Végrehajtás (Execution): Olyan támadó technikák amikor a támadók rosszindulatú kódot próbálnak futtatni a helyi vagy a távoli rendszereken.
- Fenntartás (Persistence): Olyan technikák tartoznak ide amelyekkel a támadók megpróbálják fenntartani a jelenlétüket a távoli vagy a helyi rendszerekben.
- Privilegium eszkaláció (Privilege escalation): olyan technikák, amikor a támadó fél magasabb szintű hozzáférést próbál szerezni a szervezet rendszereihez.
- A védelem kijátszása (Defense evasion): támadó technikák, amikkel az észlelést próbálják elkerülni a támadók amikor a hálózatban mozognak.
- • Hitelesítési adatokhoz való hozzáférés (Credential access): Az érzékeny hitelesítő adatok, például jelszavak lekérésére összpontosító taktika.
- Felfedezés (Discovery): Amikor a támadók megpróbálják megérteni a megtámadott rendszer működését.
- Oldalra mozgás (Lateral movement): Olyan technikák amikor a támadók belépnek a rendszerekbe, és irányítják azokat, áthaladva a hálózaton.
- Összegyűjtés (Collection): Technikák amelyekkel a vállalat releváns (megfelelő) forrásaiból információt gyűjtenek.
- Irányítás és vezérlés (Command and Control, C2 vagy C&C): amikor a támadók kommunikálnak a megtámadott rendszerrel, hogy átvegyék felette az irányítást.

⁵³ „CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™)”, elérés 2024. április 8., <https://capec.mitre.org/>.

⁵⁴ „CWE - Common Weakness Enumeration”, elérés 2024. április 8., <https://cwe.mitre.org/>.

- Kiszivárogatás (Exfiltration): Olyan technikák, amelyek közvetlenül ellopják az adatokat a hálózatról.
- Hatás (Impact): Olyan technikák, amikor az ellenfelek az adatok elérhetőségének vagy integritásának megzavarására és az üzletmenet megzavarására összpontosítanak.

A technikák tartalmazzák maguknak a módszereknek a leírását, valamint az adott technikához tartozó rendszereket és platformokat, hogy mely ellenfél csoportok használják (ha ez ismert), a tevékenység mérséklésének módjait, valamint hivatkozásokat a való világban való használatára.

A keretrendszer jelenleg 188 technikát és 379 al-technikát tartalmaz a vállalati keretrendszerben (MITRE ATT&CK Enterprise)

A keretrendszer használatával lehetőség van arra, hogy feltérképezzük, hogy egy adott incidens során tapasztal technikák mely más technikákkal állhatnak kapcsolatba, és ezáltal eszközként használható a támadók tevékenységének szimulálására, úgynevezett ellenfél emulációs forgatókönyvek létrehozására⁵⁵. Ennek segítségével ellenőrizhetők a gyakori ellenséges technikák elleni védekezés tesztelés. Az emulációs forgatókönyveket a védők és a sérülékenységvizsgáló szakemberek is használhatják az összehangolásra és védekező intézkedések fejlesztésére.

Maga a keretrendszer hasznos lehet továbbá a „Red team”-ek támadási terveinek kidolgozásában és műveletek megszervezésében. Segítésével ki lehet dolgozni, hogy hogyan kerülhetők el bizonyos hálózatvédelmi intézkedések. Használható kutatási tervként is olyan műveletek végrehajtásának új módjainak kidolgozására, amelyeket az általános védelmi intézkedések nem érzékelnek.

6.5 A fenyegetettség elemző módszertanok összehasonlítása

A fent felvázolt fenyegetettség elemző módszertanok mind arra igyekeznek egy stratégiát felvázolni, hogy hogyan elemezzük a támadók viselkedését és hogyan, milyen módszerekkel tudunk még több információt összegyűjteni a támadókról és azok tevékenységéről. Mind a három keretrendszer más-mást helyez fókuszba.

A keretrendszerek között hasonlóság, hogy mindegyiket úgy tervezték, analitikai eszközként szolgáljanak, és felhasználhatóak legyenek a védekező stratégiák megtervezésére, segítsenek

⁵⁵ „Adversary Emulation Plans | MITRE ATT&CK®”, elérés 2024. április 8., <https://attack.mitre.org/resources/adversary-emulation-plans/>.

azonosítani a rendszerek sebezhetőségeit, és megállapítani, hogy milyen válaszhintézkedésekre lehet szükség, valamint segítenek abba is, hogy a szakemberek megértsék a kiberfenyegetéseket és a védekező módszerek közötti különbségeket.

Ugyanakkor ezek a modellek sok mindenben különböznek is egymástól.

Alapvető cél:

- **Cyber Kill Chain:** A támadás szakaszaira összpontosít, kiemelve a kiber behatolások lépésről lépésre történő progresszióját.
- **MITRE ATT&CK:** A támadók által használt taktikákra és technikákra koncentrál, biztosítva egy átfogó taxonómiát az támadási módszerek kategorizálásához és megértéséhez.
- **Piramid of Pain:** A különböző IoC-k megváltoztatásának nehézségét hangsúlyozza a támadók számára, iránymutatást adva a védőknek, hogy mire összpontosítsanak a támadók hatékony zavarásához.
- **Diamond Model:** Többdimenziós nézetet kínál egy támadásról, az ellenséges félre, képességeikre, az általuk használt infrastruktúrára és az áldozatokra való összpontosítással.

Szerkezeti megközelítés:

- **Cyber Kill Chain:** Lineáris, egymást követő szakaszok.
- **MITRE ATT&CK:** Mátrix alapú, kiemelve a támadási technikák széles skáláját a különböző szakaszokban.
- **Piramid of Pain:** Hierarchikus, bemutatva az IoC-k kezelésének növekvő nehézségét.
- **Diamond Model:** Geometriai, az egyes támadáselemek közötti összefüggésekre összpontosítva.

Hasznosság a védelem szempontjából:

- **Cyber Kill Chain:** Hasznos a támadások előrejelzésében és megzavarásában, megértve és megszakítva a folyamatot annak bármely szakaszban.
- **MITRE ATT&CK:** Segít a specifikusabb és informáltabb védelmi stratégiák kidolgozásában a részletes támadási technikák megértésével.

- **Piramid of Pain:** Elősegíti a védelmi mechanizmusok prioritizálását, célzottan azokra az IoC-kra összpontosítva, amelyeket a támadók nehezebben tudnak megváltoztatni.
- **Diamond Model:** Tágabb megértést nyújt a támadásokról azáltal, hogy elemzi a behatolás különböző elemeinek kölcsönhatását.

Alkalmazkodóképesség és evolúció:

- **Cyber Kill Chain:** Inkább statikus, a hagyományos behatolási lépésekre összpontosítva.
- **MITRE ATT&CK:** Nagyon dinamikus, folyamatosan frissül új technikákkal és taktikákkal.
- **Piramid of Pain:** Konceptuálisan stabil, de különböző IoC-k kontextusában alkalmazható.
- **Diamond Model:** Rugalmas az elemzésben, de nem konkrét, fejlődő technikákra vagy IoC-kre strukturált.

Mindegyik módszertan, hasznos és véleményem szerint fontos, hogy alkalmazzuk őket. Nem lehet kiemelni egyiket vagy másikat, hogy jobb vagy rosszabb. Alapvetően mind a négy más szemléletet követ. Azt azért érdemes megemlíteni, hogy a legtöbb fenyegetettség elemző platform a MITRE ATT&CK keretrendszert integrálja és azok alapján igyekszik támpontot adnia a szakembereknek a támadások felderítéséhez és a védekezéshez. A másik három elemző módszertan is érdemes ugyanakkor megismerni, és adott esetben egy-egy támadásnál alkalmazni.

7 A platformok:

A Recorded Future nevű vállalat 2023 augusztusában felmérést végzett, arról, hogy hogyan használják fel a fenyegetettségi információkat. Honnan származnak ezek az információk és hogyan tervezik fejleszteni a fenyegetettség elemzéssel kapcsolatos folyamataikat⁵⁶. A felmérésre válaszolók a CTI programok a vállalatoknál nagy többségénél már elég szilárd lábakon áll. A vállalatok 71%-nál már külön csapat van a fenyegetettség elemzés elkészítésére. 87%-uk a fenyegetettség-elemzési folyamataikat közepes vagy fejlett szintűnek tartja. Sőt mi több 98%-a a felmérésben résztvevőknek úgy gondolja, hogy a megalapozott és jól

⁵⁶ „2023 State of Threat Intelligence Report”, elérés 2024. április 8., <https://www.recordedfuture.com/state-of-threat-intelligence>.

megszervezett fenyegetettségi elemzés elengedhetetlen a kibervédelmi programjaik hatékonysága szempontjából.

A SANS Institute is minden évben készít egy felmérést a fenyegetettség elemzés állapotáról. A 2023-as felmérésben a válaszadók 51%-a jelezte, hogy rendelkezik külön CTI csoporttal. A válaszadók nagy többsége használ valamilyen külső CTI szolgáltatást. 47% kombinálja a külső szolgáltatásokat a saját maga szolgáltatásaival 17% pedig kizárólag külső szolgáltatást használ⁵⁷. A szolgáltatások kombinálása lehetőséget ad a szervezeteknek arra, hogy a szolgáltatótól egy szélesebb az adott szektorról szóló áttekintést kapjanak, míg a saját megoldásaik pedig az adott vállalatra specifikus fenyegetéseket dolgozza fel.

A számok közötti eltérés nagy valószínűséggel a felmérésben részt vett körében keresendő. Míg a Recorded Future vállalat csak olyan szervezeteket körében végezte a felmérést, amelyek több mint 1000 főt foglalkoztatnak a SANS felmérésében kis és közepes vállalatok is szerepeltek.

Mind a két felmérés megerősítette, hogy a szervezetek elkezdtek fejleszteni a fenyegetettség elemzési képességeiket. A felmérések sz. információk követelmények meghatározásával kapcsolatban és a használt információforrásokkal kapcsolatban is tettek fel kérdéseket.

Ebben is megállapítható, hogy a nagyobb vállalatok előrébb járnak a fejlettségben. Míg a nagyvállalatok nagy többsége rendelkezik forgatókönyvekkel, amelyekhez igazítani tudja az információigényeit a kis és közepes vállalatok esetén sokszor az információigényeket a nagyvállalatok által éppen aktuálisan felkapott hírek, támadások és sérülékenységek határozzák meg, kevésbé az, hogy azok mennyire lehetnek hatással a szervezetre. Az információforrásokat tekintve a nagyvállalatok több mint 90% 5 vagy annál több információforrást használ. Mind a két felmérés megerősítette ugyanakkor, hogy egyre több szervezet kezdte el használni a CTI platformok nyújtotta előnyöket.

A CTI platformok egyik alapvető értéke a szervezet biztonsági szintjének növeléséhez történő hozzájárulásin túl az, hogy segíti az információk megosztását is. A másik, hogy amennyiben a szervezet igényeihez mérten kerül kialakításra képes teljesíteni a fenyegetettségi

⁵⁷ Rebekah Brown és Katie Nickels, „SANS 2023 CTI Survey: Keeping Up with a Changing Threat Landscape”, 2023.

információkra vonatkozó követelményt, miszerint legyen, időszerű, pontos, végrehajtható és specifikus⁵⁸.

A vállalatok által használt platformok kiválasztásánál a legtöbb esetben elsődleges szempontnak kellene lenni, hogy mennyire támogatja az a szervezet kiberbiztonsági céljainak elérését, mennyire lehetséges azt beilleszteni a meglévő munkafolyamatokba. Ám sok esetben, még a nagyobb költségvetéssel rendelkező vállalatok esetén is nem a kiberbiztonság kerül előtérbe, hanem hogy mekkora összeget hajlandó az adott intézmény feláldozni a platform bevezetése érdekében.

A platformok között sok jól használható ingyenes megoldás és még ennél több fizetős megoldás is rendelkezésre áll. Szinte valamennyi nemzetközi kiberbiztonsággal foglalkozó vállalat kínál már CTI platform megoldást, vagy másnéven Threat Intel Platformot (a továbbiakban: TIP).

A nagyvállalatok által kínált megoldások esetében számolni kell azzal, hogy a vállalat számára igazán releváns és azonnal felhasználható információt csak abban az esetben kaphatunk, ha a rendszereinkkel kapcsolatos lehető legtöbb adatot megosztunk a szolgáltatást nyújtó céggel. Ugyanis csak ebben az esetben tudnak a lehető legteljesebb és a vállalat által prioritásként megjelölt területeket lefedő szolgáltatást nyújtani. Az adatok átadását megelőzően ugyanakkor elengedhetetlen egy kockázatelemzés elvégzése. Fel kell mérni mennyivel növeli a vállalat fenyegetettségi szintjét, vagy más néven a kitettségi felületét amennyiben a rendszernek a felépítéséről, a használt eszközökről és azok funkciójáról részletes adatokat ad át egy harmadik félnek.

7.1 Kereskedelmi platformok

A kereskedelmi platformok szolgáltatásai által biztosított funkciókról sok esetben csak a használat közben kaphatunk pontos információt. valamennyi platform a fenyegetettség elemzés mind a 4 szintjén kínál szolgáltatást.

A technikai szinten valamennyi megoldás SIEM⁵⁹, EDR⁶⁰ rendszerekbe integrálható, az általuk biztosított megoldások ígéreteik szerint megkönnyítik a sérülékenységek feltárását, az incidensek kezelését. Naprakész technikai és taktikai információkat szolgáltatnak.

⁵⁸ Hutchins, Cloppert, és Amin, „Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”.

⁵⁹ Security Information and Event Management

A kereskedelmi forgalomban kapható megoldások nagy többsége az alábbi szolgáltatásokat kínálja⁶¹:

- A fenyegetések osztályozás (az esetek többségében már a mesterséges intelligenciát is igénybe véve);
- Automatikus adatgyűjtés és megosztás (nyílt és korlátozott hozzáférésű csatornákon, dark és deep-weben, az információ megosztása az analysis centers (ISACs) keresztül);
- Adat tisztítás (az adatok korrelálása, a duplikáció megszüntetése, a fals pozitív adatok kiszűrése);
- Az adatfolyamok SIEM, SOAR⁶², EDS⁶³, tűzfalakba történő integrációja;
- API használat a rendszerekbe történő integrációhoz;
- A vállalat domainjéhez hasonló domaineinek nyomom követése;
- A fenyegetések osztályozása (legtöbb esetben a MITRE ATT&CK keretrendszer használatával), hogy a fenyegetéseket össze lehessen vetni a mások által tapasztalt fenyegetésekkel;
- Információ megosztás a hasonló platformot használók között;
- Az adatok vizuális megjelentése, „dash board”, figyelmeztetések, riasztások, a fenyegetések szintjében bekövetkezett változások megjelenítése;
- Korai figyelmeztető szolgáltatások, támadási felületek felmérése.
- IP címekkel, URL-ekkel kapcsolatos szolgáltatások.

A kereskedelmi platformok kínálta szolgáltatások mindegyike a technikai, és taktikai és az operatív szintű fenyegetettség elemzés végrehajtását támogatja. Egyes szolgáltatók (FireEye, Kaspersky) kínálnak negyedéves szektorokra jellemző támadásokról adatokat, felméréseket. ezek az elemzések minden esetben a vállalatok igényeire vannak szabva.

Mivel szinte valamennyi internetbiztonsággal foglalkozó vállalat rendelkezik platform szolgáltatással ezért nehéz feltettem a ChatGPT 4.0 ⁶⁴-nak és a Microsoft Copilot⁶⁵, valamint

⁶⁰ Endpoint Detection and Response

⁶¹ Chad Kime, „Top 7 Threat Intelligence Platforms & Tools | eSP”, eSecurity Planet, 2023. február 10., <https://www.esecurityplanet.com/products/threat-intelligence-platforms/>.

⁶² Security orchestration, automation and response

⁶³ Endpoint Detection system

⁶⁴ <https://chat.openai.com>

⁶⁵ <https://copilot.microsoft.com>

a Google Gemini⁶⁶ mesterséges intelligencia platformnak is ugyan azt a kérdést: „Melyek a legnépszerűbb cyber threat intelligence platformok?”

A Microsoft Copilot válasza⁶⁷:

„A legnépszerűbb cyber threat intelligence platformok közé tartoznak a következők¹²:

1. ****Anomali ThreatStream****
2. ****IBM X-Force Exchange****
3. ****IntSights Threat Intelligence Platform****
4. ****LookingGlass Cyber Solutions****
5. ****Recorded Future****
6. ****SolarWinds Security Event Manager****
7. ****ThreatConnect****

Ezek a platformok különböző eszközökkel és funkciókkal rendelkeznek, amelyek segítenek a szervezeteknek a belső és külső fenyegetések azonosításában és kezelésében. Mindig érdemes alaposan megvizsgálni az egyes platformokat, hogy megtaláljuk a legmegfelelőbbet a szervezet igényeihez.

Forrás: Beszélgetés a Binggel, 2024. 03. 19.

(1) Top 7 Threat Intelligence Platforms & Tools | eSP - eSecurityPlanet.
<https://www.esecurityplanet.com/products/threat-intelligence-platforms/>.

(2) 10 Best Threat Intelligence Platforms, Tools & Vendors 2024 - Comparitech.
<https://www.comparitech.com/net-admin/best-threat-intelligence-platforms/>.

(3) Top 6 Threat Intelligence Platforms for IT Security. <https://sigmacybersecurity.com/top-6-threat-intelligence-platforms-for-it-security/>.

(4) 7 Best Cyber Threat Intelligence Platforms for IT. <https://sigmacybersecurity.com/7-best-cyber-threat-intelligence-platforms-for-it/>.

(5) Top 7 Threat Intelligence Platforms for IT Security. <https://sigmacybersecurity.com/top-7-threat-intelligence-platforms-for-it-security/>.”

⁶⁶ <https://gemini.google.com/app>

⁶⁷ <https://copilot.microsoft.com/?wlexpsignin=1> (a válasz időpontja: 2024. 03. 18. 19:00)

A Chat GPT 4.0 tól az alábbi válasz érkezett⁶⁸:

„A felsorolt CTI platformok közül a "legnépszerűbb" kategóriájúak meghatározása kissé szubjektív lehet, mivel a népszerűség függ a piaci részesedéstől, a felhasználói elégedettségtől, a brand ismertségtől és egyéb tényezőktől. Azonban a következő hét platformot gyakran említik a szakértők és az iparági jelentések a kiberfenyegetés-intelligencia terén a leginkább elismert és széles körben használt megoldások között:

1. ****Recorded Future****: Magas színvonalú előrejelzések és elemzések miatt széles körben ismert és elismert a piacon.
2. ****Anomali****: Egy átfogó platform, amely különböző CTI funkciókat integrál, így széles körben használják a kiberbiztonsági szakemberek.
3. ****ThreatConnect****: A ThreatConnect ötvözi a fenyegetés-intelligencia funkciókat a biztonsági operációk támogatásával, ami vonzóvá teszi sok vállalat számára.
4. ****FireEye Threat Intelligence****: A FireEye a kiberbiztonsági incidensekben szerzett tapasztalatával és széles körű intelligenciájával kiemelkedik.
5. ****IBM X-Force Exchange****: Az IBM hírneve és az X-Force Exchange által nyújtott gazdag adatforrások miatt ez a platform széles körben elterjedt.
6. ****Flashpoint****: Különösen erős a sötét web és a belső fenyegetések elemzésében, ezáltal egyedi betekintést nyújt a kiberfenyegetések világába.
7. ****LookingGlass****: Az integrált megközelítése, amely magában foglalja a fenyegetésfigyelést és a válaszadást, vonzóvá teszi a vállalatok számára.

Bár ezek a platformok rendkívül népszerűek, a választás mindig az adott szervezet igényeitől és céljaitól függ. A CTI eszközök kiválasztásakor fontos, hogy a szervezetek értékeljék a saját kiberbiztonsági keretrendszerüket, az adott eszköz integrálhatóságát meglévő rendszereikbe, valamint a költség-haszon arányt.”

A Google Gemini válasza⁶⁹:

„A legnépszerűbb kiberfenyegetési hírszerző platformok a következők:

****Kereskedelmi platformok:****

⁶⁸ <https://chat.openai.com/c/4910a2ea-3d88-434b-8345-f28d45a82097> (a válasz időpontja: 2024. 03. 18. 19:30)

⁶⁹ <https://gemini.google.com/app/a060809e500bd018> (a válasz időpontja: 2024. 03. 18 19:45)

* **Anomali ThreatStream:** Ezz a platform mesterséges intelligenciát és gépi tanulást használ a fenyegetések azonosítására és elemzésére.

* **IBM X-Force Exchange:** Ezz a platform fenyegetésinformációk széles skáláját kínálja, beleértve a mutatókat, jelentéseket és eszközöket.

* **IntSights Threat Intelligence Platform:** Ezz a platform valós idejű fenyegetésinformációkat és elemzéseket kínál.

* **LookingGlass Cyber Solutions:** Ezz a platform nyílt forráskódú fenyegetésinformációs platform, amely összegyűjti és elemzi a fenyegetésinformációkat a különböző forrásokból.

* **Recorded Future:** Ezz a platform prediktív fenyegetésintelligenciát kínál, amely segít a szervezeteknek megelőzni a támadásokat.

* **SolarWinds Security Event Manager:** Ezz a platform fenyegetésészlelést és -válaszadást (EDR) is kínál a fenyegetésinformációk mellett.

* **ThreatConnect:** Ezz a platform egy协作式平台，用于共享和分析威胁情报。

****Nyílt forráskódú platformok:****

* **AlienVault Open Threat Exchange:** Ezz a platform ingyenesen használható, és fenyegetésinformációkat kínál különböző formátumokban.

* **OpenCTI:** Ezz a platform egy nyílt forráskódú platform, amely lehetővé teszi a szervezetek számára a kiberfenyegetési hírszerző információk tárolását, szervezését és vizualizálását.

A legmegfelelőbb platform kiválasztása az Ön igényeitől és a szervezetének méretétől függ. Fontos figyelembe venni a platform által kínált funkciókat, az árazást és a támogatási lehetőségeket.

Ezenkívül érdemes megfontolni a következőket is:

* **A platform milyen típusú fenyegetésinformációkat kínál?**

* **A platform mennyire pontos és naprakész?**

* **A platform mennyire könnyen használható?**

* **A platform integrálható-e a meglévő biztonsági infrastruktúrájával?**

A kiberfenyegetési hírszerző platformok hatékony eszközök lehetnek a szervezetek kiberbiztonságának javítására. Azonban fontos, hogy a megfelelő platformot válassza ki az Ön igényeinek és a szervezetének méretétől függően”

Mind Google Gemini és a Microsoft Copilot ugyan azt a 7 platformot nevezte meg, míg a Chat GPT a IntSights Threat Intelligence Platform és a SolarWinds Security Event Manager platform helyet a FireEye Threat Intelligence-t és a Flaspont megoldását ajánlotta.

Ennek alapján megnéztem az alábbi öt platformról regisztráció nélkül, szabadon hozzáférhető rendelkezésre álló adatokat.

7.1.1 Anomali ThreatStream⁷⁰⁷¹

Az Anomali ThreatStream egy mesterséges intelligenciával (AI) és gépi tanulással (ML) támogatott kiberbiztonsági platform. Az Anomali ThreatStream számos forrásból gyűjti a fenyegetésinformációkat, beleértve a nyílt forráskódú hírszerzést, prémium hírfolyamokat és a platform saját fenyegetésfelderítő adatait.,

A ThreatStream platform használja a MACULA nevű gépi tanulási algoritmust, amely pontozza és súlyozza az indikátorokat, és eltávolítja a hamis pozitívumokat. A platform automatizálja a hagyományosan manuális adat beviteli feladatokat, és integrálható más biztonsági termékekkel, beleértve a SIEM-eket, tűzfalakat, végponti termékeket és többet. Az incidensek kivizsgálását, az IoC-k MITRE ATT&CK szerinti osztályozásával segíti. A platformon keresztül lehetőség van a közösségi információmegosztásra.

7.1.2 IBM X-Force Exchange⁷²

Az IBM X-Force Exchange egy felhőalapú fenyegetési hírszerzési platform, amely lehetővé teszi a felhasználók számára, hogy gyorsan kutassanak a legújabb globális biztonsági fenyegetésekről, összegyűjtsenek cselekvésre kész adatokat, konzultáljanak szakértőkkel és együttműködjenek társaikkal.

Az IBM X-Force Exchange támogatja az emberi és gépi hírszerzést, az információk megosztása a STIX⁷³ és TAXII⁷⁴ szabványok vagy egy RESTful API⁷⁵ használatával JSON⁷⁶

⁷⁰ „ThreatStream_Datasheet .pdf”, elérés 2024. április 8., https://assets-global.website-files.com/6454d31338f3f4b0b5ecdf5f/64cbc0602b63db10504e6589_Datasheet%20ThreatStream.pdf.

⁷¹ „Threat Intelligence Management | Anomali ThreatStream”, elérés 2024. április 8., <https://www.anomali.com/products/threatstream>.

⁷² „IBM X-Force Exchange”, 2023. június 21., <https://exchange.xforce.ibmcloud.com/exchange.xforce.ibmcloud.com>.

⁷³ Structured Threat Information eXpression

formátumban lehetséges. Ennek a platformnak a szolgáltatásait is integrálni lehet a biztonsági eszközökkel, tűzfalakkal, IDS/IPS és SIEM rendszerekkel. A platform lehetőséget kínál tovább a felhasználók közötti információmegosztásra. A felületen nyomon lehet követni az aktuálisan megjelent sérülékenységeket, az IBM saját szakértői által válogatott híreket, korai figyelmeztetéseket. Lehetőség van rosszindulatú kód elemzések, és adathalász támadásokhoz köthető IoC-k letöltésére.

7.1.3 *LookingGlass Cyber Solutions*⁷⁷

A LookingGlass Cyber Solutions, melyet 2023-ban az ZeroFox felvásárolta⁷⁸, korábban egy innovatív kiberbiztonsági vállalat volt, amely fenyegetésfelderítési megoldásokat kínált szervezetek számára. Fő profiljuk a kiberfenyegetési hírszerzés volt, vagyis olyan adatok és információk gyűjtése, elemzése és terjesztése, amelyek segítik a szervezeteket a fenyegetések azonosításában és elhárításában. Jelenleg a szolgáltatások a ZeroFox által kínált megoldások között lehet megtalálni.

A LookingGlass három fő terméket kínált:

- **scoutPrime:** Ez egy fenyegetésinformációs platform volt, amely több mint 100 különböző forrásból gyűjtött adatokat, beleértve rosszindulatú programokat, adathalász kísérleteket (phishing), és egyéb fenyegető jelzéseket
- **scoutThreat:** Ez egy fenyegetésmodellező eszköz volt, amely lehetővé tette a szervezetek számára, hogy modellezzék saját hálózatukat és azonosítsák a lehetséges támadási felületeket. A scoutThreat segítségével a szervezetek megelőző intézkedéseket hozhattak a sebezhetőségek kijavítására és a támadások megakadályozására.
- **scoutInspect:** Ez egy támadási felület felügyeleti megoldás volt, amely folyamatosan monitorozta a szervezetek külső és belső környezetét, hogy azonosítsa a lehetséges

⁷⁴ Trusted Automated Exchange of Intelligence Information

⁷⁵ „What Is REST API (RESTful API)?”, App Architecture, elérés 2024. április 8., <https://www.techtarget.com/searchapparchitecture/definition/RESTful-API>.

⁷⁶ JavaScript Object Notation

⁷⁷ „Looking Glass Cyber”, ZeroFox, elérés 2024. április 8., <https://zerofox.wpenginepowered.com/looking-glass-cyber/>.

⁷⁸ ZeroFox Inc, „ZeroFox to Acquire LookingGlass, Broadening Global Attack Surface Intelligence Capabilities”, GlobeNewswire News Room, 2023. április 17., <https://www.globenewswire.com/en/news-release/2023/04/17/2647671/0/en/ZeroFox-to-Acquire-LookingGlass-Broadening-Global-Attack-Surface-Intelligence-Capabilities.html>.

fenyegetéseket. A scoutInspect segítségével a szervezetek proaktívan azonosíthatták a sebezhetőségeket és megakadályozhatták a támadásokat.

7.1.4 *Recorded Future*

A Recorded Future egy fenyegetési hírszerzési felhőplatform, amely valós idejű intelligenciát, AI/ML analitikát, és kontextualizált kockázati értékelést nyújt. A platform lehetővé teszi a szervezetek számára, hogy azonosítsák és enyhítsék a kiber-, ellátási lánc-, fizikai és csalási területeken felmerülő fenyegetéseket. A platform automatikusan gyűjti, strukturálja és elemzi a fenyegetési adatokat. Az Intelligence Graph, amelyet a Recorded Future használ, dinamikus összekapcsolja és elemzi az adatokat valós időben, 24/7/365.⁷⁹ A Recorded Future platform integrálható a jelenleg használt biztonsági munkafolyamatokba. A platformot széles körben használják a kockázat csökkentésére, például a zsarolóvírusok elleni védekezésben, a biztonsági munkafolyamatok automatizálásában, az ellátási lánc kockázatának kezelésében és a digitális kockázatok elleni védekezésben.

7.1.5 *ThreatConnect*⁸⁰

A ThreatConnect egy közösségi platform, ahol a szervezetek megoszthatják egymással a fenyegetésinformációkat, például mutatókat, jelentéseket és elemzéseket. A platformon keresztül a szervezetek hozzáférhetnek más résztvevő szervezetek által gyűjtött fenyegetésinformációkhoz. Ez a megoldás is integrálható más biztonsági eszközökkel, például tűzfallal és EDR-rendszerekkel. A megoldás vizualizációs eszközöket is kínál, amelyek segítségével láthatók a fenyegetések közötti kapcsolatok. Lehetővé teszi a szervezetek számára, hogy létrehozzanak és használjanak „playbook”-okat a fenyegetésekre való reagálásra. Ez segít a biztonsági csapatoknak a következetes és hatékony reagálásban.⁸¹

A ThreatConnect platformot széles körben használják a kockázat csökkentésére, például a zsarolóvírusok elleni védekezésben, a biztonsági munkafolyamatok automatizálásában, az ellátási lánc kockázatának kezelésében és a digitális kockázatok elleni védekezésben.

⁷⁹ „The Recorded Future Intelligence Cloud”, elérés 2024. április 8., <https://www.recordedfuture.com/platform/intelligence-cloud>.

⁸⁰ „ThreatConnect Modernize Your TIP - ThreatConnect Content Hub | Engagement360”, elérés 2024. április 8., https://viewer.mediafly.com/threatconnect0725_share/s/692352f244fe490c9ef8d4be8b787aa4#/document/f910b2f75d704a95968a5359167c435aproduct947334?c=eyJ0IjoxLCJ2IjoimDY0MmMzNDI0NzE1MzA5MDZlZjk3MGlyNmE4ZmEyYmUifQ%3D%3D&page=2&parentSlug=f910b2f75d704a95968a5359167c435aproduct346208&shareSlug=692352f244fe490c9ef8d4be8b787aa4.

⁸¹ „Cyber Threat Intelligence Operations Platform | Threat Intel Platform”, *ThreatConnect* (blog), elérés 2024. április 8., <https://threatconnect.com/threat-intelligence-operations-platform/>.

7.2 A kereskedelmi platformok közös jellemzői

A lenti táblázatban összefoglaltam a platformokról nyíltan elérhető információkat. Ezek alapján megállapítható., hogy a kereskedelmi platformok elkezdtek alkalmazni az adatok elemzése, prioritizálása és a fenyegetések osztályozása során a mesterséges intelligencia és a gépi tanulás adat előnyöket. Szinte az össze kereskedelmi TIP szolgáltatás esetében lehetőség van az általuk kínált „data feed” programozható interfacen (API) keresztül összekapcsolhatók a végpontvédelmi rendszerekkel. A kereskedelmi platformok egyik fő szolgáltatása, a fenyegetettségi információk súlyozása. A nyílt információk alapján nem sikerült kideríteni, hogy ezt az igény-bevevők adatai alapján is megteszik-e vagy csak az alapján, hogy az adott sérülékenységet mennyire könnyű kihasználni és, hogy rendelkezésre áll-e a kihasználására vonatkozóan részletes leírás (proof of concept).

A fenyegetettségi felszín (attack surface management) is az elterjedt szolgáltatások közé tartozik.

Az eddig felsorol funkciók mind a fenyegetettség technika, taktikai vagy operatív szintjét támogatják. Az egyes platformok esetében kínált egyedi elemzői kapacitás az incidensek elemzését és a további lehetséges vizsgálati irányok meghatározását segíti.

A nyíltan elérhető információk alapján nem lehet megmondani, hogy a most bemutatott platformok és a kereskedelmi platformok mennyire képesek a stratégiai fenyegetettség elemzés elkészítéséhez hozzájárulni. A legtöbb vállalat amennyiben a megrendelő hozzáférést ad a rendszerihez, vagy részletes leírást ad azok komponenseiről, személyre szabott riasztási rendszeren keresztül képes értesíteni a felhasználókat az éppen aktuális fenyegetésekről.

A stratégiai elemzés minden esetben akkor hatékony, ha az adott vállalat igényeire és fenyegetettségi környezetére van szabva. A platformok nyíltan elérhető elemzéseink inkább sektorspecifikus fenyegetettségi helyzetképet kínálnak, amelyből a vállalatnak saját magának kell előállítania az éppen aktuális döntéshez szükséges fenyegetettségi helyzetképet. A kereskedelmi platformok nagy részben a rendszerekkel és az adott támadásokkal, csoportokkal kapcsolatban biztosítanak stratégiai szintű információkat, azonban azokat közvetlenül egy döntéshez nem lehet felhasználni, mindenképpen az adott stratégiai kérdésnek megfelelően testre kell szabni.

A kereskedelmi platformok vizsgálata alapján megállapítható, hogy képesek nagyban automatizálni a technikai és a taktikai szinten szükséges elemzési lépéseket, nagyban hozzájárulnak az operatív szintű fenyegetés elemzés elkészítéséhez, automatikus

adatkorrelálással és a lehetséges támadók megnevezésével. A fenyegetettség elemző módszertanok közül a legtöbb a MITRE által kidolgozott ATT&CK módszertan szerint osztályozza a vizsgálatok során kinyert IoC-et. Stratégiai szinten szolgáltatnak adatokat, riasztásokat és szektor vagy akár vállalat specifikus elemzéseket, de ezeket mindenképpen ki kell egészíteni és finomítani kell az aktuális stratégiai megfontolásoknak megfelelően. Egyes vállalatok kínálnak olyan szolgáltatást, amikor egy dedikált elemző a szervezetnél végzi a munkát és akkor teljes egészében rálátása van a működésre, de a legtöbb esetben ezt a szervezetek biztonsági és anyag okokból nem engedhetik meg maguknak.

	Technikai szint	Taktikai szint	Operatív szint	Stratégiai szint	Egyéb
Anomali ThreatStream	√	√	√	-	ML, AI,
IBM X-Force Exchange	√	√	√	√	felhő alapú,
LookingGlass Cyber Solutions	√	√	-	-	
Recorded Future	√	√	√	√	ML, AI, felhő alapú platform,
ThreatConnect	√	√	√	-	

1. táblázat: Kereskedelmi platformok összehasonlítása (saját szerkesztés)

8 Az ingyenes, nyílt forráskódú platformok

Az ingyenes, nyílt forráskódú platformok esetén is sokféle lehetőség van a választásra attól függően, hogy mire is szeretnénk használni. Az ingyenes platformok a legtöbb esetben nyílt forráskódúak, de van arra is példa, hogy egyes kereskedelmi szolgáltatók ingyenes verziót is

kínálnak a szolgáltatásaikból. (pl Anomali, IBM-X Force). De ezek az ingyenes hozzáférések nem tudják a fizetős verzió valamennyi szolgáltatását.

Az ingyenes és szabadon hozzáférhető megoldásra a legtöbb lehetőség akkor adódik, ha főleg technikai CTI adatokra, IoC-kra és egyéb gépek által fogyasztható formátumú adatra van szükség.

Szűkebb a lehetőség abban az esetben, ha már elemzett információkat szeretnénk kapni, valamint szeretnénk a nem feltétlenül technikai képzettséggel rendelkező személyekkel is információt megosztani belőlük. A legtöbb ingyenes platform elsősorban a technikai, incidenskezelésben, behatolástesztelésben, sérülékenységvizsgálatban részt vevő állomány számára nyújt feldolgozható és hasznos információt⁸².

A szakirodalom áttanulmányozását követően, kiválasztottam azt a 4 ingyenes, nyílt forráskódú platformot, amelyeket a legtöbb esetben vizsgálták az információmegosztás hatékonysága⁸³, a platformok fenyegetettség értékeléshez történő hozzájárulása⁸⁴, vagy akár a kibervédelemben történő felhasználásuk lehetősége szerint⁸⁵.

Az ingyenesen (open-source) elérhető platformok közül a legelterjedtebb a MISP⁸⁶ (Malware Information Sharing Platform). Az összehasonlító tanulmányok során szinte minden esetben vizsgálatra kerül még az OpenCTI és az ENISA által ajánlott Collective Intelligence Frameworks (CIF), és a YETI platform vizsgálata.

Ebben a fejezetben ahogy az előzőben is, bemutatom az említett négy platform tulajdonságait és hogy a fenyegetettség elemzés mely szintjén járulnak a szervezetek fenyegetettségi helyzetképének kialakításához.

⁸² Yansi Keim és A. K. Mohapatra, „Cyber threat intelligence framework using advanced malware forensics”, *International Journal of Information Technology* 14, sz. 1 (2022. február 1.): 521–30, <https://doi.org/10.1007/s41870-019-00280-3>.

⁸³ Alessandra de Melo e Silva és mtsai., „A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence”, *Future Internet* 12, sz. 6 (2020), <https://doi.org/10.3390/fi12060108>.

⁸⁴ Mario Faiella és mtsai., *Enriching Threat Intelligence Platforms Capabilities*, 2019, <https://doi.org/10.5220/0007830400370048>.

⁸⁵ H. Sonwani és mtsai., „A Comprehensive Study on Threat Intelligence Platform”, in *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, 2022, 1–5, <https://doi.org/10.1109/IC3IoT53935.2022.9767985>.

⁸⁶ Thanasis Chantzios és mtsai., *The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform*, 2019, <https://doi.org/10.5220/0007978103690376>.

8.1.1 Malware Information Sharing Platform (MISP)

A leginkább elterjedt nyílt forráskódú platform, amely érzékel, valamint segítségével meg lehet osztani technikai és nem technikai információkat rosszindulatú kód mintákról, incidensekről, támadókról és az azokhoz tartozó elemzésekről. A MISP-en belül lehetőség van a feltöltött adatok egymással automatikusan történő összevetésére.

Magát a platformot 2012-ben hozták létre. A fejlesztéséhez hozzájárul többek között a Luxemburgi CERT és Belgiumi Honvédelmi Minisztérium, a NATO Eseménykezelő központja is. Folyamatosan fejlesztés alatt van a felhasználói visszajelzések alapján. Nem csak technikai adatok, hanem az adott incidenssel összefüggésben elemzések és egyéb megjegyzések is feltölthetők. A felépítése rendkívül rugalmas, sokféle rendszerrel összeköthető és a legtöbb eszköz számára felhasználható formátumban⁸⁷ lehet exportálni belőle az adatokat. A feltöltött incidenseket „galaxysokba”⁸⁸ lehet rendezni, ami nagy segítséget nyújt a kapcsolódó események és a TTP-k keresésében. A feltöltött adatok összevetése automatikusan megtörténik, de a feltöltött eseményekhez (amennyiben ezt a beállítások lehetővé teszik) bárki hozzáadhat IoC-t vagy elemzési eredményt. A MISP-ben lehetőség van a TTP-k MITRE ATT&CK adatbázisban tárolt TTP-khez való hozzárendelésre, amely szintén megkönnyíti az incidenskezelők munkáját. A platform lehetősége biztosít szabad szavas importálásra is, hogy valóban bármilyen rendszerhez hozzá lehessen illeszteni. A platform tartalmaz előre beállított címkéket is „galaxysokat”, de minden felhasználónak lehetősége van sajátot beállítani az eljárásrendjének és a saját maga által használt megnevezéseknek megfelelően. A MISP-et lehetőség van intézményen belül, önálló szerveren futtatni, de ebben az esetben az információ csak szervezeten belül kerül megosztásra. Lehetőség van csatlakozni közösségek által fejlesztett MISP-ekhez. Ilyenek pl. a NATO MISP, amelyben a NATO tagországok, szervezetei osztanak meg információt. Ez a MISP szerver összeköttetésben van továbbá a NATO vállalatok által üzemeltetett és a nem NATO tagországok szervezetei számára létrehozott MISP szerverekkel. De nem minden feltöltött esemény adata kerül mindenkivel megosztásra.

Minden MISP „event” vagyis esemény feltöltéskor beállítani, hogy kikkel szeretnénk azt megosztani. Számtalan beállítás közül lehet választani. Van olyan opció amikor csak a saját szervezetem tagjai láthatják, de lehet korlátozni akár úgy is, hogy pl. a NATO MISP esetén

⁸⁷ XML, JSON, OpenIOC, STIX

⁸⁸ pl. Locky vagy APT28 vagy Wannacry vagyis ismert kártevők vagy csoportok szerinti csoportosítás

a nem NATO tagországok láthassák, de a vállalatok partnerek viszont már nem. Előnye, hogy nagyon nagy közösség és aktívan fejleszti erőteljesen figyelembe véve a felhasználói igényeket.

8.1.2 OpenCTI⁸⁹

Az Open CTI elsődleges célja, hogy segítsen a szervezeteknek megszerezni, tárolni és elemezni a kiberfenyegetésekkel kapcsolatos információkat. Az információ magába foglalhat technikai adatokat, például IP-címeket és fájlkivonatokat, valamint nem technikai adatokat, például hírszerzési jelentéseket és támadási módszereket. A platformon belül lehetőség van a felhasználók közötti információmegosztásra is. Az Open CTI integrálható más biztonsági eszközökkel, például tűzfallal és EDR rendszerekkel. Ez lehetővé teszi a szervezetek számára, hogy automatikusan reagáljanak a fenyegetésekre.

Az Open CTI vizuális térképeket és diagramokat kínál, amelyek segítségével a felhasználók láthatják a fenyegetések közötti kapcsolatokat és megérthetik a támadások lépéseit.

A platform rendelkezik egy API-val (Application Programming Interface), amely lehetővé teszi a fejlesztők számára az Open CTI integrálását más eszközökkel. A fenyegetések osztályozására lehetőség van a MITRE ATT&CK keretrendszer segítségével. A platformnak most már van a vállalatok számára fejlesztett verziója is.

8.1.3 Your Everyday Threat Intelligence (YETI)⁹¹

A YETI szintén nyílt forráskódú platform ami megfigyelések (observable) eredményeit, IoC-et, TTP-et és más fenyegetettségi adatokat gyűjt egy helyben. A megoldás automatikusan több információval látja el a megfigyelt adatokat (pl. feloldja a domain neveket, IP geolokációval látja el) a felhasználó helyett. A megoldás felhasználói felülettel és API összeköttetéssel is rendelkezik, aminek segítségével könnyen összeköthető más CTI megoldásokkal. A YETI platform is képes a technikai és a fenyegetettségi adatok közötti kapcsolatot grafikusán megjelteni, hasonlóan a MISP és az OpenCTI platformokhoz⁹², segítve ezzel a fenyegetések jobb megértését és a kapcsolatok feltérképezését.

⁸⁹ „Getting started - OpenCTI Documentation”, elérés 2024. április 8., <https://docs.opencti.io/latest/usage/getting-started/>.

⁹⁰ Frédéric Garnier, „CTI & Information Fusion Benefits and Challenges”, <https://www.enisa.europa.eu/events/2019-cti-eu/presentations/200130-cti-info-fusion-tlp-white>.

⁹¹ „Welcome to the Yeti Documentation Site!”, elérés 2024. április 8., <https://yeti-platform.io/>.

⁹² Chen Erlich, „Threat Hunting Using YETI and Elastic Stack”, *Medium* (blog), 2020. április 9., <https://medium.com/@chenerlich/threat-hunting-using-yeti-and-elastic-stack-29735c51195f>.

8.1.4 *Collective Intelligence Frameworks (CIF)*^{93 94}

Az ENISA által is ajánlott keretrendszer, amely lehetővé teszi a különböző forrásokból származó ismert rosszindulatú fenyegetési információk összekapcsolását. A leggyakrabban tárolt adatok az IP címek és az URL-ek. A tárolt indikátorokat ez a platform is automatikusan ellátja kiegészítő információkkal, mint pl geolokáció. Ennél a platformnál is lehetőség van a más rendszerekkel történő összekapcsolásra.

8.2 Az ingyenes platformok közös jellemzői

A nyílt forráskódú ingyenes fenyegetettség elemző platformoka az elmúlt időszakban megközelítették a kereskedelmi platformok által kínált szolgáltatások színvonalát. A négy leggyakrabban említett és vizsgált platform az elmúlt időszakban jelentős fejlesztéseken ment keresztül és már mindegyik képes a fenyegetettségi adatok automatikus korrelálására, ismert támadó csoportokhoz való kötésére. Valamennyi nyílt és ingyenes hozzáférésű platform integrálható a szervezetek már meglévő végpontvédelmi vagy hálózatvédelmi megoldásaiba. A MISP platform esetén már beépítésre került a szolgáltatások közé a MITRE ATT&CK fenyegetettség-elemzés módszertan szerinti osztályozás, ezzel is megkönnyítve az együttműködést közös értékelési keretrendszer használatán keresztül.

Valamennyi nyílt forráskódú platformnál a fejlesztők kiemelt figyelmet fordítanak a felhasználók visszajelzéseire és azoknak megfelelően fejlesztik tovább a megoldásokat. Mivel valamennyi itt bemutatott nyílt forráskódú platform közös jellemzője, hogy nem csak egy fejlesztője van, hanem bárki javasolhat és fejleszthet hozzájuk kiegészítőket, vagyis együttműködésen alapul a fejlesztésük. Ez az információbiztonság szempontjából hátrány is egyben, hiszen a kiegészítő funkciókat minden esetben alaposan le kell tesztelni mielőtt telepítjük a rendszerekbe. Ez a közösségi fejlesztés ugyanakkor azt is jelentheti, hogy bizonyos megoldások ezeknél platformoknál hamarabb is megjelenhetnek, mint a kereskedelmi megoldások esetén.

Az alábbi táblázatban összefoglaltam, hogy a fenyegetettség elemzés melyik szintjén, kínálnak szolgáltatásokat a fent bemutatott platformok.

⁹³ wes@csirtgadgets.com, „Collective Intelligence Framework”, CSIRT Gadgets, LLC, elérés 2024. április 8., <https://csirtgadgets.com/collective-intelligence-framework>.

⁹⁴ „Detect, SHARE, Protect” (ENISA, 2013), <https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs>.

	Technikai	Taktikai	Operatív	Stratégiai	Megjegyzés
MISP	√	√	√ közösségen belüli információmegosztás	„galaxys”-n keresztül	integrálható más rendszerbe,
OpenCTI	√	√	√ közösségen belüli információmegosztás	-	integrálható más rendszerbe
YETI	√	√	√ közösségen belüli információmegosztás	-	integrálható más rendszerbe
CIF	√	√	√ közösségen belüli információmegosztás	-	integrálható más rendszerbe

2. táblázat: Nyílt forráskódú, ingyenes platformok összehasonlítása (saját szerkesztés)

8.3 A kereskedelmi és a nyílt forráskódú platformok összehasonlítása

Amennyiben egy szervezet eldöntötte, hogy CTI platformot szeretne használni a fenyegetettségi információk könnyebb kezelése érdekében akkor, sok szempontot figyelembe lehet venni akkor amikor egy szervezetnek döntést kell hoznia arról, hogy nyílt forráskódú, ingyenes, vagy kereskedelmi szolgáltató által biztosított megoldást alkalmaz.

A legtöbb nyílt forráskódú platform megoldás ma már a kereskedelmi platformokkal közel azonos szolgáltatásokkal rendelkezik, amennyiben technikai vagy taktikai szintű fenyegetettség elemzésről van szó. Minden esetben az elmúlt években kialakításra kerültek a grafikus felületek is a jobb felhasználói élmény érdekében.

A nyílt platformok egyik előnye az alacsony kialakítási költség, viszont ezt ellensúlyozza az, hogy a telepítésükhöz és a beállításokhoz sokkal nagyobb szaktudás kell. Viszont ezek a megoldások sokkal magasabb szinten igazíthatók a szervezet igényeihez. A kereskedelmi platformok esetén kész rendszereket adnak a szolgáltatók. A kereskedelmi és a nyílt

forráskódú platformok esetén egy másik lényeges különbség, hogy nyílt platform esetén nem kell információkat megosztani a fejlesztőkkel és a közösséggel arról, hogy milyen rendszerbe tervezzük beintegrálni a megoldást. A kereskedelmi platformok esetén mivel kész megoldást kapunk minden esetben a lehető legtöbb információt szeretné megkapni a forgalmazó annak érdekében, hogy a legjobb megoldást tudja nyújtani. Ebből a szempontból az olyan szervezetek esetén, ahol kiemelt figyelmet fordítanak arra, hogy minél kevesebb információt adjanak ki másoknak a saját rendszereikről jobb megoldásnak ígérkezik egy nyílt forráskódú platform használata.

A nyílt platform megoldások hátrányai közé tartozik még, hogy stratégiai szinten kevésbé járulnak hozzá a fenyegetettség elemzés végrehajtásához. Szektorspecifikus, vagy általános elemzéseket egyik platform sem kínál ellentétben a kereskedelmi megoldásokkal.

A másik hátránya lehet a nyílt forráskódú platformoknak, hogy jelenleg még semmilyen formában nem alkalmazzák a kereskedelmi platformok esetén már egyre jobban elterjedt mesterséges intelligencián és gépi tanuláson alapuló megoldásokat. Ennek segítségével könnyebben és gyorsabban tudják összevetni egymással a technikai adatokat és kiszűrni a nem megfelelő adatokat, a duplikációkat, valamint a rendelkezésre álló információk alapján súlyozni a fenyegetéseket.

A kereskedelmi platformok egy másik előnye lehet az ingyenes platformokkal szemben, hogy ezek a megoldások már kínálnak felhő alapú hozzáféréseket is.

9 Összegzés további kutatási irányok

9.1 Összefoglalás

A fenyegetés elemzés kulcsfontosságú a szervezetek számára a kiberbiztonsági kockázatok kezelésében. Számos előnye van, amelyek segítséget nyújtanak abban, hogy proaktívan hatóak, értékelhetőek és mérsékelhetőek legyenek a potenciális biztonsági fenyegetések. A fenyegetés elemzés által nyújtott átfogó betekintés nem csupán a jelenlegi, hanem a lehetséges jövőbeli kiberfenyegetésekre is kiterjed. Ez magában foglalja a különböző támadási vektorok, módszerek és a támadók potenciális motivációinak megértését. A szervezetek így képesek felmérni saját kiberbiztonsági helyzetüket, azonosítani a biztonsági réseket és meghatározni a védelem kiemelt területeit. A fenyegetés elemzés hozzájárul a szervezet kiberbiztonsági tudatosságának növeléséhez, lehetővé téve a kiberfenyegetések teljesebb körű megértését és a proaktív cselekvési tervek kidolgozását.

A fenyegetés elemzés átfogó betekintést nyújt a jelenlegi és potenciális kiberfenyegetésekbe, lehetővé téve a szervezetek számára, hogy jobban megértsék a kiberbiztonsági környezetüket. Az elemzés segít azonosítani a fenyegetések előjeleit, így lehetővé téve a szervezetek számára, hogy előre felkészüljenek és reagáljanak a támadásokra még azelőtt, hogy azok kárt okoznának. Ezeken túl a fenyegetés elemzés pontos és releváns információkat biztosít, amelyek alapján a döntéshozók tájékozott biztonsági stratégiákat és politikákat alakíthatnak ki. A megfelelő elemzés segítségével a szervezetek prioritást tudnak adni a kiberbiztonsági erőfeszítéseiknek, koncentrálva a legkritikusabb fenyegetésekre és kockázatokra, valamint gyorsabbá és hatékonyabbá lehet tenni az incidensekre történő reakciót, ezáltal csökkenthető egy esetleges incidens által okozott kár. Ezen túl optimalizálhatóak a fejlesztések és azok költségvetése is.

Nem csak az incidensek kezelésében és az azokra történő reagálásban, valamint a kockázatelemzésben nyújt hatékony segítséget, hanem a fenyegetések elemzése közben nyert információ segítséget nyújthat egy olyan tudásbázis kialakításában, amely megkönnyíti a jövőbeni fenyegetések azonosítását és az ellenük való védekezést is. Valamint ezeknek az adatoknak köszönhetően könnyebben feltérképezhetőek a szervezet rendszereinek sérülékenységei és gyenge pontjai is, továbbá fenyegetés elemzés lehetőséget biztosít a szervezeteknek, hogy tanuljanak a múltbeli és jelenlegi biztonsági eseményekből, folyamatosan fejlesztve a kiberbiztonsági stratégiájukat, és emeljék a rendszereik biztonsági szintjét.

Manapság már nem az a kérdés, hogy honnan tudunk adatokat szerezni egy fenyegetés elemzés elkészítéséhez, hanem hogy meghatározzuk, hogy melyek a számunkra releváns adatok. Kihívást jelent továbbá az is, hogy melyek a fontos és melyek a kevésbé fontos adatok.

A fenyegetés elemzést több szinten is végre lehet hajtani. Mindegyik szint más és más információkból dolgozik és más az elkészült végtermék címzettje is. A szintek között megkülönböztetünk technikai, taktikai, operatív és stratégiai szintet. A technikai szint jellemzően a gépek által feldolgozható adatok szintje, míg a taktikai és operatív szinten már nagyobb jelentősége van az adatok közötti összefüggéseknek, ugyanis ezek a szintek már egy-egy támadó szempontjából vizsgálják az adatokat. A taktikai szint egy általánosabb leírást ad az egyes csoportok, elkövetők, vagy elkövetési módok technikáiról és taktikáiról, míg az operatív fenyegetés elemzés az éppen folyamatban lévő támadásokra koncentrál.

A stratégiai szintű fenyegetés elemzést értelmezhetjük a szervezet szintjén, azok elektronikus információs rendszereinek tekintetében, de a szervezet, az ágazat, az ország vagy akár régió szempontjából is. Stratégiai szinten már nem csak technikai adatokkal dolgozunk, sőt ezekből kell a legkevesebb az elemzések elkészítéséhez. Ezen a szinten kiemelt jelentősége van a biztonságpolitikai, gazdasági és egyéb elemzéseknek is. A stratégia fenyegetettség elemzések átfogó képet adnak a csoportok, vagy az azokat támogató kormányok, szervezetek céljairól. de stratégiai elemzés készíthető egy vállalat esetében arról is, hogy a jövőben tervezett beruházásai milyen fenyegetésekre számíthatnak a kibertérben.

A fenyegetések szintjének azok mibenlétének meghatározására több módszertan is használatos. ezek közül dolgozatomban bemutattam az egyik legtöbbször emlegetett és a fenyegetés elemzések esetében sokszor hivatkozott Cyber Kill Chain keretrendszert, amely a katonai harcérintkezés lépéseit ültette át a kibertéri fenyegetések elemzésébe. A keretrendszer nem csak meghatározza, hogy egy-egy támadásnak milyen fázisai vannak és abban mit tesznek a támadók, de tanácsot is ad a védekezőknek arra, hogy hogyan tudnak védekezni az egyes szakaszokban. A Diamond Modell szintén elterjedt elemzési módszertan, amelynek a célja, hogy azonosításra kerüljenek a támadók taktikai technikái és eljárásrendjei, valamint maguk a támadók is. A rendszer vizsgálja a támadókat, az általuk használt infrastruktúrát, a támadók képességeit és az áldozatot, vagyis azt akit az ellenérdekelte fél megtámadott. A keretrendszer elemi események meghatározásán alapul, amiket aztán összekötnek egymással és ezek segítségével feltérképezik a hiányzó adatokat és azt is hogy mi történhetett pontosan.

Ezáltal segítenek meghatározni a támadók, technikáit és taktikait, és segítenek abban is hogy feltérképezzük a jövőbeni támadások lehetséges lépéseit.

A Pyramid of Pain egy olyan rendszer amely arra világít rá, hogy a támadók által használt technikák elleni védekezés mennyire nehezíti meg a támadók életét. Egyfajta támpontot ad a védőknek, hogy milyen védelmi intézkedéseket érdemes bevezetni a rendszereikben.

A MITRE ATT&CK alapként szolgált mind a privát, mind a kormányzati szférában a fenyegetettségi modellek előállításra. A keretrendszer egy olyan adatbázis, amely szabadon, mindenki számára elérhető és a kibertéri támadók technikáinak és taktikáinak valós megfigyelésén alapul. Folyamatosan karbantartott információt szolgáltat a kibertérben tevékenykedő támadók viselkedéséről, annak megfelelően csoportosítva, hogy az a támadás melyik szakaszában figyelhető meg, valamint folyamatosan friss információt szolgáltat az a csoportok éppen aktuális célpontjairól.

A fenyegetés elemzések végrehajtásnak megkönnyítésére manapság már elérhetőek kereskedelmi forgalomban kapható, de nyílt forráskódú, ingyenes fenyegettség elemző platformok. Ezek a platformok segítséget nyújtaak az adatok összegyűjtésben azok összevetésében. Segítenek a fenyegetések osztályozásában, az incidensek kezelésében is. További hatalmas előnyük, hogy mindegyik – ingyenes és kereskedelmi forgalomban kapható – mögött áll egy közösség, amelyen belül meg lehet osztani az információkat, tanácsokat, tapasztalatokat lehet gyűjteni. Az információmegosztásnak ugyanis kritikus szerepe van a fenyegetés elemzések során, mivel a kapott információk segítenek felkészülni a támadásokra, vagy elkerülni azokat, de megkönnyítik a már bekövetkezett támadások kivizsgálását, a rendszerekben található sérülékenységek feltárását.

9.2 Megállapítások

A dolgozatomban megvizsgált kereskedelmi platformok között már találhatók olyanok amelyek a gépi tanulást és a mesterséges intelligenciát is használják az adatok összevetése és súlyozása során. A kereskedelmi és a nyílt forráskódú platformok is rendelkeznek ma már grafikus felülettel a felhasználói élmény növelése és a könnyebb átláthatóság érdekében.

A nyílt és a kereskedelmi forgalomban elérhető CTI platformok összehasonlítása során arra a következtetésre jutottam, hogy a ma használatos megoldások, technikai, taktikai és operatív szinten mind a két esetben kellően hatékonyak és jó segítséget nyújtanak. A nyílt hozzáférésű platformok egyetlen hátránya, hogy a meglévő rendszerekbe történő integrációjuk nehezkesebb és nagyobb szaktudást igényel. előnyül viszont az, hogy a használatuk úgymond

„házon belül” is megoldható, nem kell a rendszerünkről minden információt átadni egy harmadik félnek.

A vizsgálataim során megállapítottam, hogy operatív és stratégiai szintű használat során kezdenek elválni egymástól a nyújtott szolgáltatások. A kereskedelmi platformok sok esetben készítenek átfogó elemzéseket egy-egy adott támadó csoportról vagy összegzik az adott ágazatra jellemző fenyegetési trendeket. A nyílt forráskódú platformok nem kínálnak ilyen szolgáltatást. Ezeknek az összefoglaló jelentéseknek az egyik nagy előnye, hogy ha nem is közvetlenül, átdolgozás nélkül, de nagyon jól alkalmazhatók a vezetők tájékoztatása során amennyiben a rendszerek védetten tartására vagy a rendszerek fejlesztési irányára vonatkozó stratégiáról van szó.

A platformok vizsgálata során arra a következtetésre jutottam, hogy technikai, taktikai szinten nincs különbség a kereskedelmi és az ingyenes, nyílt hozzáférésű platformok között. Mind a két esetben hatékonyan képesek hozzájárulni a rendszerek védetten tartásához. A kereskedelmi platformok előnye viszont, hogy az elemzéseikhez már aktívan használják a mesterséges intelligenciát, ami az ingyenes platformok esetében még nem jelent meg a szolgáltatások között, de ez véleményem szerint csak idő kérdése.

A fenyegetettség elemzés operatív szintjén a kereskedelmi platformok jobban átlátható képet adnak egy folyamatban lévő támadásról. A kereskedelmi platformok kínálnak olyan szolgáltatást is mely során lehetőség van egy adott incidens kivizsgálásához dedikált szakértői segítséget kérni. Az ingyenes platformok esetén csak a közösség erejére támaszkodhatunk amennyiben segítségre van szükségünk. Ez nem feltétlenül jelent hátrányt, de amennyiben egyedi támadással nézünk szembe nem biztos, hogy elegendő a kivizsgálás meggyorsítására.

A stratégiai fenyegetettség elemzési szint esetén, amennyiben nem a szervezetek szintjén vagyunk kíváncsiak a fenyegetettségi helyzetképre, hanem ágazat, szektor vagy a kár régió szinten a nyílt hozzáférésű platformok jelentős hátrányba kerülnek. Míg a kereskedelmi platform gyártók rendszeresen készítenek átfogó elemzéseket, a nyílt hozzáférésűek esetén erre nem találtam példát. Ez nem azt jelenti, hogy ne járulnának hozzá ennek elkészítéséhez, hiszen a platformon valamennyi adat rendelkezésre áll az információmegosztó közösségek által, de ezeket még tovább kell elemezni ahhoz, hogy trendeket lehessen felállítani.

Amennyiben a stratégiai fenyegetés elemzést a felsővezetés stratégiai céljaira és irányaira leselkedő kibertérből érkező fenyegetések felmérésére, egy kiemelt esemény szempontjából fontos kibertéri fenyegetések meghatározására szeretnénk használni, akkor sem a

kereskedelmi, sem a nyílt hozzáférésű platformok nem nyújtanak átfogó megoldást. A kereskedelmi platformok által készített jelentések viszont jó támpontot adhatnak a további elemzéseknek. Az átfogó képe elkészítéséhez viszont mindenképpen szükség van más forrásokra, geopolitikai, stratégiai elemzésekre, amelyek segítségével főleg a kormányok által támogatott csoportok esetén hatékonyabban meghatározhatók a jövőbeni támadási irányok. Ezekre a csoportokra ugyanis kiemelten jellemző, hogy az őket támogatók céljai és a csoportok célpontjai nagy mértékben megegyeznek.

9.3 További lehetséges kutatási irányok

A mesterséges intelligencia, a gépi tanulás egyre több lehetőséget kínál, amely a fenyegetettség elemzésben is hatékonyan felhasználható. Technikai és taktikai szinten a kereskedelmi platformok már beépítették a szolgáltatásaikba és a mesterséges intelligencia segíti az adatok összevetését és súlyozását.

Sok esetben manapság a szervezetek e fenyegetettség elemzésnek csak a taktikai és a technikai szintjén gondolkodnak, nem sok szervezet jutott még el az érettségnek arra a fokára, amikor valamennyi stratégiai döntés esetében a kibertérből érkező fenyegetéseket is figyelembe veszik.

Amennyiben ez bekövetkezik a fenyegetettség elemző platformok felé elvárás lesz, hogy ezeket a stratégiai döntéseket is támogassák.

A nagy nyelvi modellek alkalmasak lehetnek arra is, hogy a stratégiai szintű elemzésekben segítséget nyújtsanak. Vannak kutatások arra, hogy hogyan lehet a taktikai és az operatív szintű szöveges elemzésekből adatokat kinyerni.

Dokumentumok elemzéséhez már használják a természetes nyelvi feldolgozást (NLP⁹⁵), amely ahhoz, nyújt segítséget, hogy dokumentumokból összefoglalókat, kivonatokat készítsünk a mesterséges intelligencia segítségével. Véleményem szerint ezek az eljárások a stratégiai fenyegetettség elemzés elkészítésében is nagy segítséget nyújthatnak.

⁹⁵ Natural Language Process

10 Irodalomjegyzék

- „2023 State of Threat Intelligence Report”. Elérés 2024. április 8. <https://www.recordedfuture.com/state-of-threat-intelligence>.
- „A BIZOTTSÁG (EU) 2017/ 1584 AJÁNLÁSA - (2017. szeptember 13.) - a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról”, 2017
- „About CISP”. Elérés 2024. április 4. <https://www.ncsc.gov.uk/cisp/home>.
- „Adversary Emulation Plans | MITRE ATT&CK®”. Elérés 2024. április 8. <https://attack.mitre.org/resources/adversary-emulation-plans/>.
- App Architecture. „What Is REST API (RESTful API)?” Elérés 2024. április 8. <https://www.techtarget.com/searchapparchitecture/definition/RESTful-API>.
- Arslan, Halil, és Ozkan Canay. „CYBER THREAT INTELLIGENCE SYSTEMS AND APPLICATIONS”, 103–16, 2023.
- Bianco, David J. „Enterprise Detection & Response: The Pyramid of Pain”. *Enterprise Detection & Response* (blog), 2013. március 1. <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>.
- Borum, Randy, John Felker, Sean Kern, Kristen Dennesen, és Tonya Feyes. „Strategic cyber intelligence”. *Information and Computer Security* 23 (2015. július 13.): 317–32. <https://doi.org/10.1108/ICS-09-2014-0064>.
- Brown, Rebekah, és Katie Nickels. „SANS 2023 CTI Survey: Keeping Up with a Changing Threat Landscape”, 2023.
- Caltagirone, Sergio, Andrew Pendergast, és Christopher Betz. „The Diamond Model of Intrusion Analysis”, 2013. <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>.
- „CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™)”. Elérés 2024. április 8. <https://capec.mitre.org/>.
- Chantzios, Thanasis, Paris Koloveas, Spiros Skiadopoulos, Nikos Kolokotronis, Christos Tryfonopoulos, Vasiliki Bilali, és Dimitrios Kavallieros. *The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform*, 2019. <https://doi.org/10.5220/0007978103690376>.
- „Cost of a Data Breach 2023 | IBM”. Elérés 2024. április 8. <https://www.ibm.com/reports/data-breach>.
- „CWE - Common Weakness Enumeration”. Elérés 2024. április 8. <https://cwe.mitre.org/>.
- Dahj, Jean Nestor M. *Mastering Cyber Intelligence: Gain Comprehensive Knowledge and Skills to Conduct Threat Intelligence for Effective System Defense*. Packt Publishing Ltd, 2022.
- „Detect, SHARE, Protect”. ENISA, 2013. <https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs>.
- Djekic, Milica. „Levels of Cyber Intelligence”. *Australian Science* (blog). Australian Science, 2014. május 16. <http://ozscience.com/internet-2/levels-of-cyber-intelligence/>.
- ENISA. „ENISA Threat Landscape 2023”. Report/Study. Elérés 2024. április 5. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>.

- Erlich, Chen. „Threat Hunting Using YETI and Elastic Stack”. *Medium* (blog), 2020. április 9. <https://medium.com/@chenerlich/threat-hunting-using-yeti-and-elastic-stack-29735c51195f>.
- Faiella, Mario, Gustavo Granadillo, Ibéria Medeiros, Rui Azevedo, és Susana Gonzalez-Zarzosa. *Enriching Threat Intelligence Platforms Capabilities*, 2019. <https://doi.org/10.5220/0007830400370048>.
- Garnier, Frédéric. „CTI & Information Fusion Benefits and Challenges”. Előadás CTI EU Workshop, 2020. <https://www.enisa.europa.eu/events/2019-cti-eu/presentations/200130-cti-info-fusion-tlp-white>.
- „Getting started - OpenCTI Documentation”. Elérés 2024. április 8. <https://docs.opencti.io/latest/usage/getting-started/>.
- H. Sonwani, M. Divya, A. Dhawan, A. Mantri, D. G, és H. Kumar. „A Comprehensive Study on Threat Intelligence Platform”. In *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, 1–5, 2022. <https://doi.org/10.1109/IC3IoT53935.2022.9767985>.
- Hermans, Kris. *Mastering Cyber Threat Intelligence (CTI): A Comprehensive Guide to Implementing and Managing CTI in the Enterprise*. Independently published, 2023.
- Hutchins, Eric, Michael Cloppert, és Rohan Amin. „Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”. *Leading Issues in Information Warfare & Security Research* 1 (2011. január 1.).
- „IBM X-Force Exchange”, 2023. június 21. <https://exchange.xforce.ibmcloud.com/exchange.xforce.ibmcloud.com>.
- Inc, ZeroFox. „ZeroFox to Acquire LookingGlass, Broadening Global Attack Surface Intelligence Capabilities”. GlobeNewswire News Room, 2023. április 17. <https://www.globenewswire.com/en/news-release/2023/04/17/2647671/0/en/ZeroFox-to-Acquire-LookingGlass-Broadening-Global-Attack-Surface-Intelligence-Capabilities.html>.
- Johnson, Christopher S., Mark Lee Badger, David A. Waltermire, Julie Snyder, és Clem Skorupka. „Guide to Cyber Threat Information Sharing”. National Institute of Standards and Technology, 2016. október. <https://doi.org/10.6028/NIST.SP.800-150>.
- „JP 1, Doctrine for the Armed Forces of the United States”, é. n. <https://irp.fas.org/doddir/dod/jp1.pdf>.
- Keim, Yansi, és A. K. Mohapatra. „Cyber threat intelligence framework using advanced malware forensics”. *International Journal of Information Technology* 14, sz. 1 (2022. február 1.): 521–30. <https://doi.org/10.1007/s41870-019-00280-3>.
- Kime, Chad. „Top 7 Threat Intelligence Platforms & Tools | eSP”. eSecurity Planet, 2023. február 10. <https://www.esecurityplanet.com/products/threat-intelligence-platforms/>.
- Mandiant. „A Requirements-Driven Approach to Cyber Threat Intelligence”. Elérés 2024. április 2. <https://www.mandiant.com/resources/blog/requirements-driven-approach-cti>.
- Melo e Silva, Alessandra de, João J. Costa Gondim, Robson de Oliveira Albuquerque, és Luis J. García Villalba. „A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence”. *Future Internet* 12, sz. 6 (2020). <https://doi.org/10.3390/fi12060108>.

- Oosthoek, Kris, és Christian Doerr. „Cyber Threat Intelligence: A Product Without a Process?” *International Journal of Intelligence and CounterIntelligence* 34, sz. 2 (2021. április 3.): 300–315. <https://doi.org/10.1080/08850607.2020.1780062>.
- Ruks, Martyn, és David Chismon. „Threat Intelligence: Collecting, Analysing, Evaluating”. MWR InfoSecurity Ltd, 2015. <https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf>.
- Sahrom, Md, Siti Rahayu Selamat, Aswami Ariffin, és Y. Robiah. „Cyber Threat Intelligence – Issue and Challenges”. *Indonesian Journal of Electrical Engineering and Computer Science* 10 (2018. április 1.): 371–79. <https://doi.org/10.11591/ijeecs.v10.i1.pp371-379>.
- Seker, Ensar. „Cyber Threat Intelligence Understanding Fundamentals”, 2019. szeptember 9.
- Strom, Blake, Andy Applebaum, Douglas Miller, Kathryn Nickels, Adam Pennington, és Cody Thomas. „MITRE ATT&CK: Design and Philosophy”, 2020. március 31. <https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy>.
- Sun, Nan, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, Yonghang Tai, és Jun Zhang. „Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives”. *IEEE Communications Surveys & Tutorials* 25, sz. 3 (2023): 1748–74. <https://doi.org/10.1109/COMST.2023.3273282>.
- „The Definitive Guide to Cyber Threat Intelligence.pdf”. Elérés 2024. április 2. https://informationsecurity.report/Resources/Whitepapers/e8aee5ef-4086-4c84-9a33-4134848ea7fb_The%20Definitive%20Guide%20to%20Cyber%20Threat%20Intelligence.pdf.
- „The Recorded Future Intelligence Cloud”. Elérés 2024. április 8. <https://www.recordedfuture.com/platform/intelligence-cloud>.
- „Threat Intelligence Management | Anomali ThreatStream”. Elérés 2024. április 8. <https://www.anomali.com/products/threatstream>.
- „Threat Intelligence: What It Is, and How to Use It Effectively | SANS Institute”. Elérés 2024. április 2. <https://www.sans.org/webcasts/threat-intelligence-is-effectively-102622/>.
- ThreatConnect. „Cyber Threat Intelligence Operations Platform | Threat Intel Platform”. Elérés 2024. április 8. <https://threatconnect.com/threat-intelligence-operations-platform/>.
- „ThreatConnect Modernize Your TIP - ThreatConnect Content Hub | Engagement360”. Elérés 2024. április 8. https://viewer.mediafly.com/threatconnect0725_share/s/692352f244fe490c9ef8d4be8b787aa4#/document/f910b2f75d704a95968a5359167c435aproduct947334?c=eyJ0IjoxLCJ2IjoimDY0MmMzNDI0NzE1MzA5MDZlZjk3MGlyNmE4ZmEyYmUifQ%3D%3D&page=2&parentSlug=f910b2f75d704a95968a5359167c435aproduct346208&shareSlug=692352f244fe490c9ef8d4be8b787aa4.
- „ThreatStream_Datasheet .pdf”. Elérés 2024. április 8. https://assets-global.website-files.com/6454d31338f3f4b0b5ecd5f/64cbc0602b63db10504e6589_Datasheet%20ThreatStream.pdf.
- Warner, Chad. „Diamond Model in Cyber Threat Intelligence”. *Medium* (blog), 2023. december 11. <https://warnerchad.medium.com/diamond-model-for-cti-5aba5ba5585>.

„Welcome to the Yeti Documentation Site!” Elérés 2024. április 8. <https://yeti-platform.io/>.
wes@csirtgadgets.com. „Collective Intelligence Framework”. CSIRT Gadgets, LLC. Elérés
2024. április 8. <https://csirtgadgets.com/collective-intelligence-framework>.
ZeroFox. „Looking Glass Cyber”. Elérés 2024. április 8.
<https://zerofox.wpenginepowered.com/looking-glass-cyber/>.