ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK	Hallgató neve:	**Molnár Attila István**
2023	Hallgató törzskönyvi száma:	**T/008045/FI12904/N**

Óbudai Egyetem
Neumann János Informatikai Kar
Kiberfizikai Rendszerek Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Molnár Attila István**
Törzskönyvi száma: T/008045/FI12904/N
Neptun kódja: [redacted]

A dolgozat címe:

Ipari kiberbiztonsági fenyegetések felderitése
Industrial cyber security advance threat detection

Intézményi konzulens: Balázsné Dr. Kail Eszter
Külső konzulens:

Beadási határidő: 2022. május 15.

A záróvizsga tárgyai: Informatikai rendszerek üzemeltetésének biztonsága
IT hálózatbiztonság

A feladat

Az infromatika fejlődése napjainkban megállíthatatlan, és annak minden területén vitathatatlan. Igaz ez a kibertámadásokra is, vagyis a frekventált infrastruktúrák-hálózatok elleni kifinomult kibertámadások veszélye is folyamatosan nő. Az ilyen irányú támadásokkal szemben egyetlen vállalat sincs biztonságban, függetlenül az általa használt védelmi eszközök sebezhetőségétől. Az ipar világában rendkívül fontos a kibertámadások elleni védelem, mivel a hálózatok elleni sikeres támadás mélyreható hatással járhat, sok esetben óriási gazdasági veszteséget okozva. Potenciális támadások elleni hatékony védekezéshez a vállalatok számára elengedhetetlen a folyamatos fejlesztés, monitorozás, behatolásészlelés-megelőzés, hálózati szegregáció. A gyorsan fejlődő és egyre kifinomultabb informatikai támadásokkal szemben a védekezés egyik eszköze lehet a Cyber Security Advance Threat Detection megoldás, illetve a védelemi rendszerek Packet Brokerrel történő egyesítése, amely tovább erősíti az ipari rendszerek hatékony működését.
Szakdolgozatomban arra vállalkozom, hogy bemutassam a MOL Nyrt-nél jelenleg fejlesztés alatt álló Cyber Security Advance Threat Detection rendszert, illetve annak gyakorlati megvalósítását megelőző fejlesztési folyamatot. Különösen a kialakítás tervezését, a tesztelési időszak során felmerült esetleges problémákat, azok megoldásait, valamint a valós ipari biztonsági környezethez való adekvát alkalmazás problémáit.

A dolgozatnak tartalmaznia kell:

- védelmi rendszerek rendszerezését és elemzését,
- Cyber Security Advance Threat Detection és a Packet Broker ismertetését,
- a védelmi rendszer biztonsági megoldásának megtervezését, tervezési szempontokat,
- a tesztkörnyezet tervét és megvalósítását,
- a rendszer tesztelését, a tesztelés során dokumentált mérések eredményeit,
- a tesztelés értékelését, a program bevezethetőségének értékelését, anticipációját.

Ph.

ÓBUDAI EGYETEM Neumann János Informatikai Kar 1. Budapest

.....
Dr. habil. Lovas Róbert
intézetigazgató

A szakdolgozat elévülésének határideje: **2024. május 15.**
(OE TVSz 55.§ szerint)

A dolgozatot beadásra alkalmasnak tartom:

.....
külső konzulens

.....
intézményi konzulens

Titoktartási megállapodás

amely létrejött egyrészről a

MOL MAGYAR OLAJ- ÉS GÁZIPARI NYILVÁNOSAN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG

Székhelye: 1117 Budapest, Október huszonharmadika U. 18.
Cégjegyzékszám: 01 10 041683
Adószám: 10625790-4-44

Képviseli:
Név, beosztás: Kapócs Tamás, Head of Cyber Security Strategy and Architecture
Telefon: +36-70-3820791
E-mail: tkapocs@mol.hu
(a továbbiakban: **Társaság**)

másrészről a

Óbudai Egyetem

Székhelye: 1034 Budapest, Bécsi út 96/b
Intézményi azonosító: OM-FI12904
Adószáma: 19308760-2-41
Képviseli: Dr. Póser Valéria
(a továbbiakban: **Egyetem**)

együttesen Felek (a továbbiakban: **Felek**)

között az alább jelzett napon és helyen, a következő határidőkhöz és feltételekhez igazodva.

1. **Előzmények**

1.1. Molnár Attila István (tanulmányi azonosító: IMSGBK) (a továbbiakban: Hallgató), az Óbudai Egyetem Neumann János Informatikai Karának BSc/MSc szakos hallgatója, az „ Ipari kiberbiztonsági fenyegetések felderítése" című szakdolgozatában/diplomamunkájában (továbbiakban: Szakdolgozat) olyan bizalmasnak minősülő információkat, adatokat rögzít, amelyek zártkörű kezelése (a továbbiakban: titkosítása) indokolt a Társaság üzleti érdekeinek védelme érdekében.

1.2. Felek rögzítik, hogy az Óbudai Egyetem Tanulmányi és Vizsgaszabályzatának és Tanulmányi Ügyrend szabályzatának (a továbbiakban együtt: Szabályzat), megfelelően a Hallgató és a Társaság kérelmezték a Szakdolgozat titkosítását.

2. **A megállapodás tárgya**

2.1. Az Egyetem jelen megállapodás aláírásával tudomásul veszi, hogy a Szakdolgozatban szereplő, a Szakdolgozattal összefüggésben a Társaságtól származó személyes, informatikai, üzleti, műszaki és egyéb információ (a továbbiakban együttesen: Információ) bizalmas természetű és a Társaság tulajdonát képezi. Felek jelen megállapodás aláírásával tudomásul veszik és kijelentik, hogy az elkészült Szakdolgozat és mellékletei jelen titoktartási megállapodás hatálya alá tartoznak.

3. Felek jogai és kötelezettségei

3.1. A 2.1. pontban foglaltakra tekintettel az Egyetem a Szakdolgozatot a titoktartás szabályai és a Szabályzatban foglaltak szerint köteles kezelni. Az Egyetem vállalja, hogy a Szakdolgozatot üzleti titokként kezeli, azt a szerződés időtartama alatt harmadik személyek tudomására nem hozza, illetve semmilyen módon nem teszi hozzáférhetővé a Társaság előzetes írásbeli engedélye nélkül.

3.2. Társaság kijelenti, hogy az Óbudai Egyetem Szabályzatának a titkosított szakdolgozatok kezelésének eljárási rendjében foglaltakat megismerte és az abban foglalt rendelkezéseket a jelen megállapodás alkalmazásának vonatkozásában elfogadja.

3.3. Az Egyetem vállalja, hogy a Szabályzat szerinti eljárásrend alkalmazásával kerül sor a titkosított Szakdolgozat megvédésére. A 3.1. pontban előírt titoktartási kötelezettség alól kivételt képez a Szakdolgozat megvédésének folyamata, ahol az értékelő bizottság tagjai – előzetes titoktartási nyilatkozat aláírását követően – megismerik a Szakdolgozat tartalmát.

3.4. Az Egyetem kötelezettséget vállal arra, hogy kizárólag azok a munkavállalói ismerhetik meg a Szakdolgozat tartalmát, akik tekintetében ez feltétlenül szükséges a Szakdolgozat intézményen belüli, szabályos kezelése céljából. Az Egyetem köteles gondoskodni arról, hogy a titoktartási kötelezettség kiterjed az Egyetem munkavállalóira.

3.5. Társaság tudomásul veszi, hogy a Szakdolgozat elektronikus formátumú változata a Szabályzat értelmében feltöltésre kerül az intézményi könyvtárakba, ahol lehetőség van a titkosításhoz szükséges elérési jogosultsági szint beállítására.

3.6. Felek megállapodnak, hogy a titkosított Szakdolgozat kapcsán az alábbi adatok nyilvánosak, azaz nem képezik jelen megállapodás tárgyát:

a) a szakdolgozat címe, a szerző és témavezető neve és a védés időpontja

b) a titkosítás ténye és a titkosítás határidejének várható lejárta.

3.7. Felek megállapodnak, hogy jelen megállapodás időtartama az aláírásának napjától számított **...3.....** év időtartamra szól. Ennek megfelelően a Szakdolgozatra vonatkozóan az Egyetem titoktartási kötelezettsége **.....3.....** év elteltével megszűnik és Társaság hozzájárul, hogy ezen idő leteltét követően a Szakdolgozat nyilvánosságra kerüljön.

3.8. Felek rögzítik, hogy az üzleti titok védelméről szóló 2018. évi LIV. törvény alapján az üzleti titok akkor is törvényes védelem alatt áll, ha külön szerzői jogi védelemben, szabadalmi oltalomban, használati mintaoltalomban vagy egyéb, jogszabályokban meghatározott, szellemi alkotásokra vonatkozó jogi védelemben nem részesül.

3.9. Felek rögzítik, hogy a jelen megállapodás szerinti titoktartási kötelezettség nem érvényesíthető államigazgatási (így különösen adóügyi) és bírósági eljárásban, továbbá azokban az esetekben, amikor jogszabály írja elő, hogy az információt a jogszabályban megjelölt személlyel közölni kell (pl. közérdekű, vagy közérdekből nyilvános adatok közlése), ezért ezekre nézve kölcsönösen és előzetesen mentesítik egymást a titoktartási kötelezettség alól, azzal a feltétellel, hogy Felek kötelesek előzetesen értesíteni egymást a jogszabályi kötelezettségről, illetve az eljárások tényéről és jogszabály alapján, illetve az eljárás során átadandó információk mértékéről.

3.10. Nem állapítható meg titoktartási kötelezettség továbbá az információk következő csoportjára:

(i) azon információ, amely nem az Egyetem hibájából vagy szerződésszegésének következtében került nyilvánosságra;

(ii) azon információ, amely a Társaság tudtán kívül már az átadás időpontjában közismert vagy bárki számára megismerhető volt;

(iii) azon információ, amely olyan személy által jutott nyilvánosságra, akiért Felek nem felelnek.

3.11. Felek a következő kapcsolattartó személyeken keresztül értesítik egymást jelen szerződéssel kapcsolatosan.

Az Egyetem részéről: Oktatási dékánhelyettes
Név, beosztás: Dr. Póser Valéria
Telefon: 0616665585
E-mail: poser.valeria@nik.uni-obuda.hu

A Társaság részéről:
Név, beosztás: Kapócs Tamás, Head of Cyber Security Strategy and Architecture
Telefon: +36-70-3820791
E-mail: tkapocs@mol.hu

Felek a kapcsolattartók személyében bekövetkezett változásokról kötelesek egymást haladéktalanul, de legfeljebb három munkanapon belül írásban tájékoztatni.

4. Egyéb rendelkezések

4.1. Felek a jelen megállapodásból eredő vitás kérdéseket elsődlegesen tárgyalás útján egymás között rendezik, amennyiben ez 60 napon belül nem vezet eredményre, úgy Felek a Polgári Perrendtartásról szóló törvény mindenkori szabályai szerint járnak el.

4.2. A jelen megállapodásban nem szabályozott kérdések tekintetében a Ptk. rendelkezései, a hatályos magyar jogszabályok és a Szabályzat rendelkezései az irányadók.

4.3. Jelen megállapodás 4 (azaz négy) egymással szó szerint egyező eredeti példányban készült.

Felek jelen szerződést, mint akaratukkal mindenben megegyezőt, jóváhagyólag és saját kezűleg írták alá.

A MOL Nyrt.
képviseletében:

.....
Meayki Rita
Csoportszintű HR Megoldások Vezető

Az Óbudai Egyetem
képviseletében:

.....

ÓBUDAI EGYETEM * Neumann János Informatikai Kar * 1. Budapest

A fenti megállapodásban foglaltakat megismertem és tudomásul vettem:

Budapest, 2022. 06. 08

MOL Magyar Olaj- és Gázipari Nyilvánosan Működő Részvénytársaság
Humán Erőforrás - Képzés - Fejlesztés
1117 Budapest, Október huszonharmadika u. 18.

.....

hallgató

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

HALLGATÓI NYILATKOZAT

Alulírott hallgató kijelentem, hogy a szakdolgozat / diplomamunka saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem.

Budapest, 2022. december 09.

.....

hallgató aláírása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve:	Neptun kód:	Tagozat:
Molnár Attila István	[redacted]	**Levelező**

Telefon: Levelezési cím (pl: lakcím):

[redacted]

Szakdolgozat / Diplomamunka[1] címe magyarul:

Ipari kiberbiztonsági fenyegetések felderítése

Szakdolgozat / Diplomamunka[2] címe angolul:

Industrial cyber security advance threat detection

Intézményi konzulens:	Külső konzulens:
Balázsné Dr.Kail Eszter	**Kapócs Tamás**

Kérjük, hogy az adatokat nyomtatott nagybetűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2022.10.12	SZAKDOLGOZAT TERVEZETT ÁTBESZÉLÉSE.	Kail
2.	2022.10.20	EDDIGI MUNKA ÉS FORMAI KÖVETELMÉNYEK ÁTBESZÉLÉSE.	Kail
3.	2022.11.17	SZAKDOLGOZAT STRUKTÚRÁJA.	Kail
4.	2022.11.29	SZAKDOLGOZAT VÉGLEGESÍTÉSE, PREZENTÁCIÓ	Kail

A Konzultációs naplót összesen 4 alkalommal, az egyes konzultációk alkalmával kell láttamoztatni bármelyik konzulenssel.

A hallgató a Projektlabor 1. / 2. / 3. / Záródolgozati projekt tantárgy követelményét teljesítette, beszámolóra/védésre bocsátható. A javasolt érdemjegy: jeles (5)

Budapest, 2022.12.09

Kail

.....
intézményi konzulens

[1] Megfelelő aláhúzandó!
[2] Megfelelő aláhúzandó!

TARTALOMJEGYZÉK

1 BEVEZETÉS

Szakdolgozatom célja, hogy az IT védelem terén olyan biztonsági rendszer kiválasztást, tesztelési folyamatát mutassam be, amelynek fő funkciója az ipari hálózatok forgalmának előszűrése, védelemének hatékony növelése. Erre a témára részben személyes kíváncsiságból, részben pedig munkahelyem anyavállalatánál, a MOL Magyarország Nyrt-nél (továbbiakban: MOL) jelenleg folyó Cyber Security Advanced Threat Detection rendszer tervezett megvalósításának hatására esett a vállasztásom. Az utóbbi időben szerte a világban jellemzően erősödik a kibertérből érkező fenyegetések száma, amivel arányosan növekszik a rögzített biztonsági események száma is. Ezek az incidensek már napi szinten megjelennek az ipari rendszerek világában, ahol egy jól irányított támadással jogosulatlan hozzáférés szerezhető az informatikai vagy a folyamatirányitási rendszerhez. A kiberbiztonsági szakértők évek óta mondogatják: nem az a kérdés, hogy feltörik-e egy vállalat rendszerét, hanem az, hogy mikor. Minden jel arra mutat, hogy még több támadás várható, ezért célszerű azonosítani a gyenge pontokat, és megerősíteni a védelmet, erre való törekvés az ipari rendszerekben egyre erősödő tendenciát mutat. A védelmi megelőző tevékenységek hatékonysága növelhető, ha különböző elemző technikákat ötvözünk, amelyek így ellenállnak célzott támadásoknak is. Szem előtt tartva, hogy az egymásra épülő rendszereknek rugalmasnak és skálázhatónak kell lennie, a fokozott védelem elérése céljából. Ipari vagy szolgáltatói környezetben egy vélelmezett hacker támadásból adódó esetleges üzemzavar esetén, nemcsak az érintett rendszer szenved károkat, hanem az arra szervesen ráépülő egyéb szolgáltatásokban és folyamatokban is zavarok keletkezhetnek. A rendszerek termelésből történő kiesésese vagy a nyújtott szolgáltatások elakadása hatással lehet a gazdaságra, a társadalomra, és károkat okozhat, sőt akár nemzetbiztonsági érdekek is veszélybe kerülhetnek. Éppen ezért fontos a mai gazdaság-, társadalom szereplői számára a kibertámadások elleni fokozott védekezés. Az informatikairendszerek és az internet gyors fejlődése lehetővé tette, hogy megfelelő tudás, affinitás birtokában szinte bárkiből kiberterrorista válhat. Az interneten elérhető információkon túl számos szoftver és hardver eszköz is segítségükre van cselekményeik kivitelezéshez. Ezeknek az eszközöknek a beszerzése, összeszerelése, használatának elsajátítása a hétköznapi emberek számára is elérhető. Ez az a körülmény, ami fokozott kockázatként jelenik meg a mindennapokban az informatikai infrastruktúrákat üzemeltetők számra. A MOL-nál jelenleg zajló Cyber Security Advanced Threat Detection rendszer tervezett bevezetése 2022-2023. év. A megvalósítása jelenleg a tesztelés fázisánál tart, melyre a cég egy év időtartamot irányzott elő, és kezdetben két vállalati helyszínen Pozsonyban és Százhalombattán kívánják a tesztelési folyamatot megvalósítani. A vállalat a bevezetett biztonsági rendszer végső eredményeként olyan határvédelmi protokoll elérését reméli, amely annak ellenére, hogy a támadók sok esetben előrébb járnak az ipari szereplőktől, az incidensek döntő többsége elkerülhetővé válik. Ehhez természetesen szükséges, hogy a hálózati vé-

delmet egy rugalmas, gyorsan adaptálható, tehát naprakész IT-biztonsági rendszerekre és a rendszereket üzemeltető jól felkészült szakemberekre bízzuk. Egy olyan nagyvállalat, mint a MOL, amely kiemelt energetikai gazdasági szereplő, amely folyamatosan törekszik az informatikai rendszereinek védelmére a külső támadásoktól, hogyan teszteli az említett biztonsági rendszert, és annak bevezetését, annak érdekében, hogy a bevezetését követően valóban adekvátan szolgálja az eredeti elképzelést. Szakdolgozatomban arra vállalkozom, hogy bemutassam annak folyamatát, hogy a kiválasztott rendszernek milyen tesztelési eljáráson kell megmérettetni ahhoz, hogy a cégcsoport az adott rendszert használni kezdje valamennyi üzleti-, üzemi egységénél, illetve a tesztidőszak alatt milyen esetleges problémák, kockázati tényezők, működési kívánalmak merülnek fel, és ezekre adott válaszok, módosítások hogyan tudnak illeszkedni a vállalati környezetbe.

2 KIBERTÁMADÁSOK, KIBERBŰNÖZÉS

A kiberháború, kiberbűnözés, kibertámadás manapság gyakran használt kifejezés, de mit is jelent valójában? A kiberbűnőzés számítógépek valamint csoportba szervezett számítógépes rendszerek segítségével, számítógépek vagy hálózatok kárára elkövetett bűncselekmények gyűjtőfogalma.

2.1 A kiberbűnözők típusai

Klasszikus kiberbűnözők: akiket a gyors pénzszerzés motivál, csak az illegálisan megszerezett profit, vagy a szándékos károkozás a céljuk.

Hacktivisták: akik az internetet használják fel politikai vagy társadalmi okokból történő demonstrálására.

Hackercsoport: azon elkövetők, akik összetett komoly támadást kezdeményeznek kifinomult technikákkal, aminek eredménye lehet egy ipari terültet működésének ellehetetlenítése.

A 2022 év leghírhedtebb hackercsoportjai:

Anonymous
Az Anonymous néven elhíresült nemzetközi csoport talán a leghíresebb a hackerek közül. Rendszeres célpontjai a kormányzati hálózatok, vállalatok, közintézmények. A csoport 2003-ban hallatott magáról először. Az anonim tagok Guy Fawkes-ról mintázott maszkot viseltek, ami elrejtette eredeti személyazonosságukat és később a védjegyük lett. Legutóbbi ismert támadásuk a jelenlegi orosz-ukrán háború kezdetén több állami tulajdonú weboldal ellen irányult, melynek során az orosz védelmi minisztérium webhelyének feltörését is felvállalták.

Lapsus
Jellemző a csoport módszereire, hogy nem titkosítják a megtámadott rendszereket, csupán „csak" ellopják az adatokat. Az eddigi akcióik alapján elmondható, hogy adatlopásra és zsarolásra fókuszálnak. Többnyire adathalász módszerekkel szereznek az áldozatok rendszereihez hozzáférést. Az adatlopás során az adatok között szelektálnak, kifejezetten érzékeny adatokat tartalmazó fájlokat tulajdonítanak el. Legutóbbi ismert támadásaik a Microsoft, Cisco, Samsung, NVIDIA cégcsoportok ellen irányultak.

Conti
A Conti ransomware csoport valójában 2022 májusában megszűnt, ugyanakkor a csoportból megmaradt kis közösség feltörte a Costa Rica-i kormány rendszereit. DDoS (Distributed Denial of Service) túlterheléses támadásokat indítottak különböző szerverek ellen, valamint európai humanitárius és nonprofit szervezetek ellen.

Lazarus Group
Az észak-koreai székhelyű Lazarus Group egy kiberbűnözői csoport, és a világ legnagyobb hackercsapata. Deklaráltan főképpen az észak-koreai kormány megbízásából dolgozik. A Lazarus-nak tudhatók be a világ legnagyobb kibertámadásai, mint például 2014-ben a Sony cégcsoport hackelése. Emellett az ő nevükhöz fűződik a Wannacry ransomware vírus is. Azonban a csoport elsősorban dél-koreai vállalatok ellen aktív, de támad katonai célpontokat, kormányszerveket, kutatóközpontokat, IT (Information Technology) és telekommunikációs cégeket, valamint oktatási intézményeket is.

A kibertámadások vonatkozásában beszélnünk kell egy speciális „elkövetői" csoportról, az **etikus hackerekről**, vagyis azon szakemberek, akik előre egyeztetve, szerződésben foglat feltételek mellet támadnak egy informatikai rendszert, rendszereket. El kell őket különítenünk a kiberbűnözőktől, mivel céljuk, hogy a rendszer hibát feltárják és azok javításra javaslatot tegyenek azért, hogy biztonságos, stabil rendszerrel megakadályozzanak egy esteleges rendszerbe történő betörést, adatszivárgást. Attitűdjük tehát mindenképpen pozitív előjelű a támadás során, szemben az egyéb kibertámadások elkövetőivel.

2.2 Kibertámadás fogalma

Kibertámadásnak nevezünk minden olyan támadást, amely a kibertéren keresztül valósul meg magánszemélyek, cégek, ipari létesítmények számítástecnikai eszközei ellen. Célja az adatok integritásának megsemmisítése, információ szerzés, jogosulatlan felügyelet átvétel az érintett informatikai eszközök felett.

2.3 Kibertámadások típusai

A kibertámadások leggyakoribb típusai közül meg kell említenünk néhányat. A leggyakrabban használt támadási formák az alábbiakban felsoroltak:

SQL (Structured Query Language) injektálás, amely az injektálásos támadások adatbázisok sérülékenységét kihasználó formája. Ennek során tulajdonképpen egy olyan kódot telepítenek az adatbázisba, melyet az adatbázist tartalmazó memóriacsomag tulajdonosa nem ellenőriz, így a használat során lefut az adott SQL, ezáltal biztosítva hozzáférést a megszerezni kívánt adatokhoz.

A nem publikus adatok megszerzésének másik jelentős formája a jelszavak támadása. Itt tulajdonképpen nem maga a jelszó megszerzése a cél, hanem a jelszóval védett adattartalomhoz való hozzáférés. Ennek a gyakorlatban több formája is létezik, mint például a **„próbálkozásos"** támadások, amikor véletlenszerű jelszavak generálásával igyekeznek megtalálni az adott jelszóval való egyezést.

Ezen kívül jellemző az **adathalászat**, ahol a támadó jól ismert cégnek, weboldalnak mutatja magát és így próbál megszerezni személyes adatokat, bankkártya adatokat, illetve jelszavakat. Jellemzően e-mailben kapott üzenettel, nem ritkán pszichológiai ráhatással próbálja az adatokat megszerezni. Leggyakoribb adathalászati módszer az E-mail-alapú, ami hamis hivatkozásokkal próbálja rávenni a címzetteket személyes adatok megosztására. Hasonlóan elterjedt módszer a kártevő alapú adathalászat, ahol a kártevő megbízható mellékletnek álcázza magát. A legtöbb adathalász támadásnak nincsenek konkrét célpontjai, a célzott adathalászat azonban adott személyek ellen irányul a munkájukkal és a közösségi életükkel kapcsolatos kutatás során összegyűjtött információkat kihasználva. Ezek a támadások nagymértékben testre szabottak, így különösen hatékonyak az alapvető kiberbiztonsági intézkedések megkerülésben.

Meg kell említenünk a **zsarolóvírusokat** is, melyek olyan kártevők, amelyek azzal fenyegetik az áldozatot, hogy megsemmisítik a kritikus fontosságú adatokat vagy rendszereket, illetve blokkolják az ezekhez történő hozzáférést, amennyiben az áldozat nem fizet váltságdíjat. Korábban a zsarolóvírusok magánszemélyeket céloztak meg, ám a közelmúltban a szervezeteket célzó és ember által üzemeltetett zsarolóvírusok váltak a jelentősebb, nehezebben megelőzhető és elhárítható veszélyforrásokká.

A kibertámadások közé soroljuk még a hálózati támadásokat. Ennek egyik formája a **lehallgatás**. Ilyen támadás esetén a támadónak a hálózati lefedettségen belül kell tartózkodnia ahhoz, hogy adatcsomagokat tudjon elkapni és abból számára fontos információkat szerezzen. Nem titkosított hálózaton ez viszonylag könnyen megvalósítható, de a

titkosítással védett hálózatból is megfelelő mennyiségű adatgyűjtést és elemzést követően kinyerhető az információ.

Hálózati támadások további típusa, amikor a támadó a két fél közötti kommunikációt manipulálja MITM (Man-In-The-Middle) **közbe-ékelődéssel**. Valójában a támadó a hálózaton küldött adatokat úgy módosítja, hogy mindkét fél azt hiszi, egymással „beszél", miközben mindketten a támadóval vannak kapcsolatban és így az adatok kompromittálódnak.

Annak ellenére, hogy egyre több kifinomultabb támadást ismerünk, továbbra is kedvelt a **szolgáltatás-megtagadással** járó (DDOS) támadás. Ebben az eseteb a cél a hálózati eszközök, szerverek túlterheléssel történő megbénítása. A támadás azonos időben több számítógépről indítva a normális hálózati forgalom többszörösével árasztja el az áldozatát, ezzel üzleti kárt okozva.

Álljon itt példaként néhány elhíresült kibertámadás [1] az elmúlt 40 évből:

Logic Bomb az első igazán káros trójai vírus

A Logic Bomb a Trans-Szibéria gázvezeték 1982-es robbanását okozta. A felügyeleti szoftverbe egy trójai modult rejtettek, melyet a CIA (Central Intelligence Agency) által megbízott programozók írtak. A trójai vírus feladata az volt, hogy időzítetten a szivattyúk és szelepek szabályozásának változtatásával olyan magas nyomást idézzen elő a vezetékben, melyet sem a varratok, sem a berendezések nem tudtak elviselni.

Titan Rain célkeresztben az USA (United States of America) kormányzata

2003-ban a Titan Rain (titáneső) indított összehangolt támadást az USA számítógépes rendszerei ellen, melyet később Kína kormányának tulajdonítottak. A támadások célja katonai titkok megszerzése volt, és a hackerek több, az amerikai kormánnyal szerződésben álló fegyvergyártó hálózatába is bejutottak, mint például a Lockheed Martin, a Sandia National Laboratories, vagy a Redstone Arsenal, de a NASA-t (National Aeronautics and Space Administration) sem kímélték.

Hackertámadás a dél-koreai kormányzat ellen

2009 júliusában hackertámadás érte a dél-koreai elnöki hivatalt, illetve több kormányzati ügynökség és magánvállalat internetes oldalát; a honlapokat órákon keresztül nem lehetett elérni.

BlackEnergy az ukrán áramszünet okozója

2015. december 23-án súlyos kibertámadás érte Ukrajna energiaszektorát, melynek következtében csaknem 225 ezren maradtak áram nélkül.

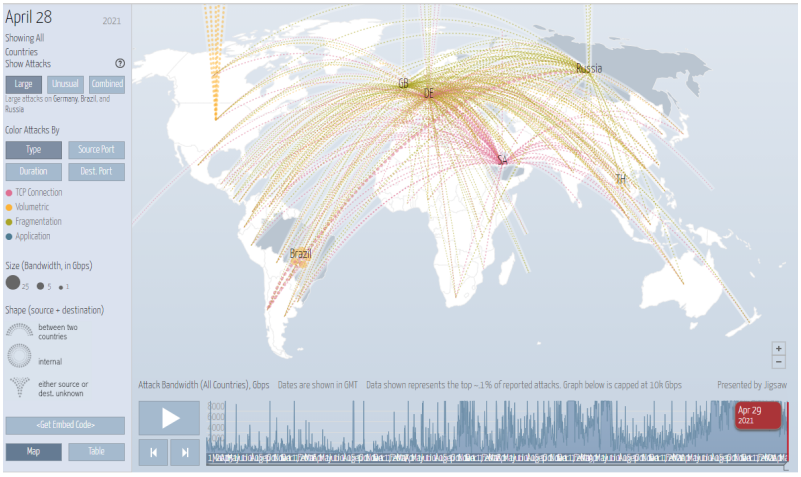
A fentiek alapján látható tehát, hogy fontos a kibertámadások elleni védelem, mivel egy ilyen incidens kapcsán sérülhetnek:

- ipari adatok
- tervek
- receptúrák
- szerződések
- személyes adatok

Colonial Pipeline

2021. április 29. napján a Colonial Pipeline elleni ransomware -támadás talán az egyik legjelentősebb kibertámadás, ami az energiaszektor ellen irányult. Ennek során a hackerek egy inaktív VPN (Virtual Private Network) fiókon keresztül jutottak be a vállalati hálózatba. A fiók jelszava elérhető volt a sötét weben fellelhető jelszavak sorozatán belül. Nagy valószínűséggel a nem megfelelő jelszó kezelésből adódott a lehetőség a támadásra. Feltehetően egy Colonial Pipeline alkalmazott ugyanazt a jelszót használhatta egy másik, már korábban feltört fióknál is. Az eset egészen addig észrevétlen maradt, amíg a váltságdíj-követelés nem jelent meg a számítógép képernyőjén kriptovalutát követelve fizetségül.

A védekezés vagy megelőzés első, vagy 0. lépése az, hogy észlelni tudjuk a kibertámadást, illetve annak lehetőségét. Erre ma már vannak törekvések, mint például az Arbor Networks, amely védi a világ legnagyobb igényeit kiszolgáló hálózatokat a DDoS támadások és fejlett fenyegetések ellen. A Google-el együttműködve hozták létre azt a valós idejű térképet [2], ami megmutatja a világon jelenleg zajló egyik globális problémát jelentő támadást, az úgynevezett elosztott túlterheléses támadást.



2.1. ábra: DDoS támadások (forrás: http://www.digitalattackmap.com)

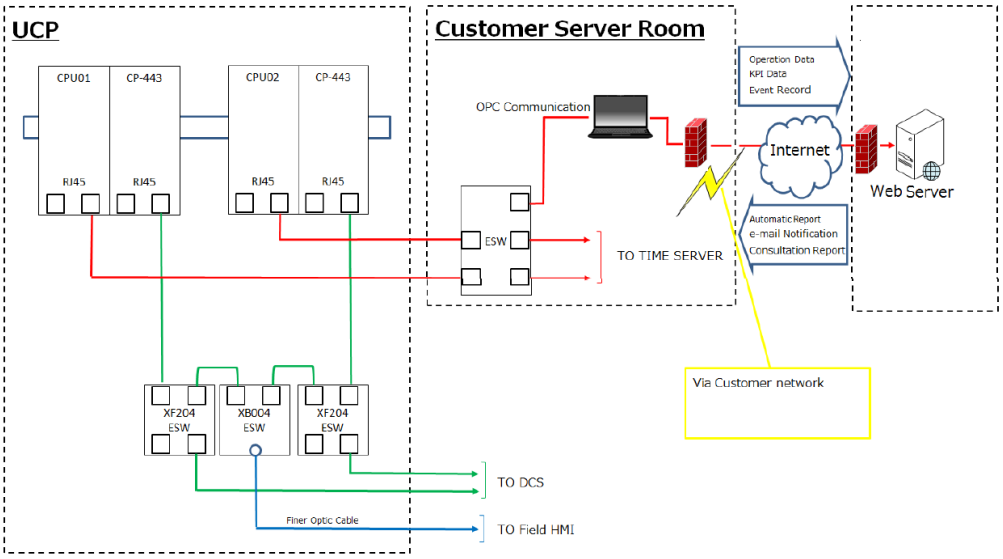
De említhetjük a vírusirtó megoldásairól ismert Kaspersky Labot is, amely egy olyan valós idejű világtérképet készített, amely az általuk detektált pillanatnyi kiberfenyegetéseket mutatja meg [3].

2.2. ábra: Kaspersky Lab (forrás: https://cybermap.kaspersky.com)

A kiberbtámadások hatásának súlyát Leon Edward Panetta a CIA korábbi igazgatója nagyon találékonyan fogalmazta meg: "A következő Pearl Harbor egy számítógépes támadás lesz."

3 KIBERVÉDELEM AZ IPARI RENDSZEREKEN

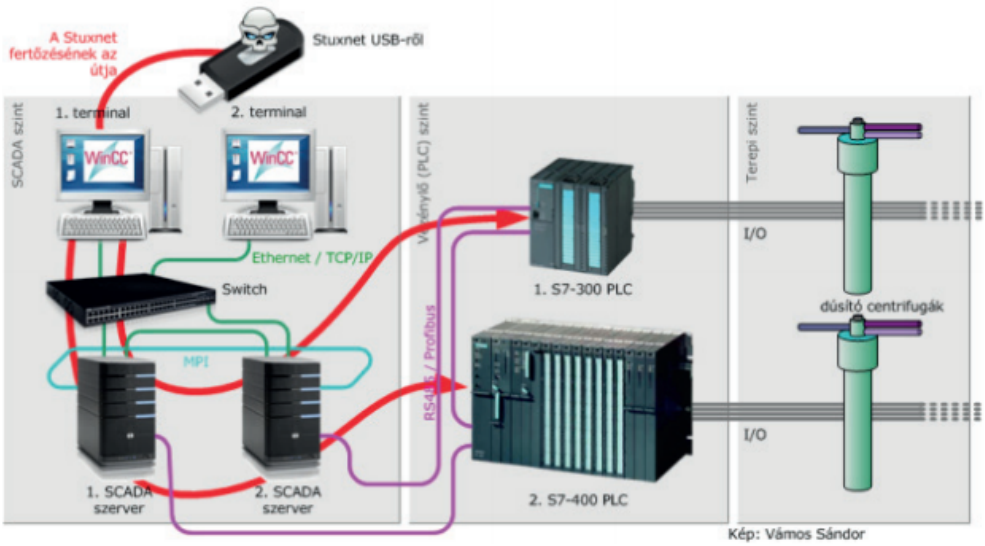
Magas anyagi haszon reményében az incidensek 70-80 százaléka a nagyvállalatokat érinti. Az automatizálás az ipari környezetben is jelentősen elterjedt, a rendszerek nagymértékben függnek egymástól, működésük egymással szinkronban van, központi irányító rendszerük pedig gyakran az interneten keresztül kapcsolódik a hálózatokhoz, ezáltal számos fenyegetésnek teszi ki az ipari vezérlőrendszereket. Egy incidens végzetes következményekkel járhat. Az alábbi ábra szemlélteti, hogy egy belső ipari rendszer hogyan kommunikál az interneten keresztül egy külső szolgáltatóval. Az ábra bal oldalán láthatók a folyamatvezérlő PLC (Programmable Logic Controller) eszközök, amelyek felé beérkeznek az adatok a kihelyezett műszerektől, pl. egy kompresszor rezgésdiagnosztikai műszerétől, és amelyek egy swich védett portján keresztül jutnak el egy központi adatgyűjtő serverhez. Az összesített adatokat a server tűzfalon, proxyn keresztül a vállalati protokoll szerint titkosított formában továbbítja a műszer forgalmazója felé visszajelzés, és az esetleges hibák detektálása érdekében. Az alábbi ábrán is látható, hogy az adattovábbítás az interneten történik, amely egyben a rendszer sérülékenységét, illetve a támadhatóságát is jelenti az esetleges kibertámadások szempontjából.



3.1. ábra: Adatgyűjtés PLC-n keresztül (forrás: MOL Nyrt)

Ipari környezetben elsőként a Stuxnet számítógépes féreg okozott riadalmat 2010-ben. A kártevőt Iránban egy erőmű egyik számítógépén fedezték fel. A vezérlőrendszer (WinCC PCS7) hibáit kihasználva indított támadást. Megközelítőleg 45 ezer felügyeleti számítógép és szerver hordozta a vírust, és megfertőzött százezer számítógépet. A Stuxnet tulajdonképpen a termelési és a logikai biztonság szintjén indított támadást ipari rendszerek ellen. A férget kimondottan arra fejlesztették és használták fel, hogy ipari célpont ellen

támadást valósítsanak meg, melynek során az ipari alkalmazások felügyeleti vezérlését végző SCADA (Supervisory Control and Data Aquisition) rendszereket vették célba. A program sajátossága volt, hogy rejtőzködött és önmagát replikálta. A rendszer újra programozása során a féreg az általa végzett módosításokat elrejtette, a rendszerekből történő adatgyűjtés, kémkedés nyomaival együtt. Felfedezését követőn kiderült, hogy az erőműre közvetlen veszélyt nem jelentett, bár működésbeli zavart igen, így a sikeres támadás mindenképpen elgondolkodtató volt a biztonsági szakemberek számára. A Stuxnet-sztori bebizonyította, hogy az ipari létesítmények elleni támadásokkal számolni kell, felhívta a figyelmet arra, hogy egy kibertámadás milyen mértékű lehet, illetve arra, hogy milyen mértékű veszéllyel, kockázattal kell szembenézni a jövőben. Ez be is következett, hiszen 2010 óta számos támadást hajtottak végre különböző ipari létesítmények ellen szerte a világon. Az ipari rendszerek ellen irányuló támadások hatással vannak a rendszer rendelkezésre állására, integritására, az ipari adatokra (receptúrák, gyártási folyamatok, tervek), azok bizalmasságára és természetesen az informatikai események nyomon követhetőségére is. A legtöbb ipari rendszer sebezhetősége abból adódik, hogy telepítésükkor még csak a fizikai hozzáféréstől kellet védelmet biztosítani. Sebezhetőségük további sarokköve Modbus protokoll (Modbus Plus, Modbus/TCP) és a felügyeleti terminál.



3.2. ábra: Stuxnet (forrás: http://passport.blog.hu/2017/06/30/a stuxnet sztori

A támadások kedvelt célpontjai:

- kőolaj feldolgozók
- erőművek
- nukleáris létesítmények

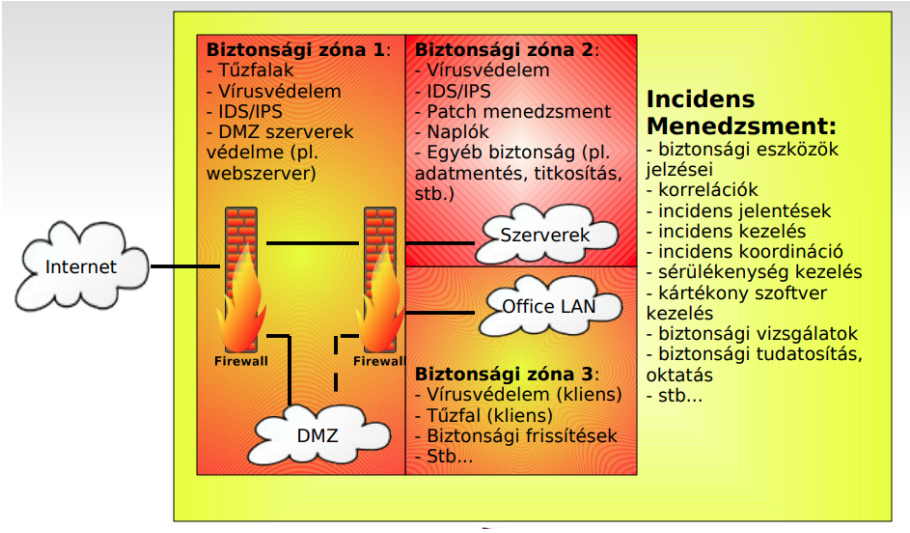
Egy ipari létesítmény védelmi rendszerén történő áthatolás komoly tudást igényel. Az elmúlt évek tapasztalati arra világítanak rá, hogy a támadók egy része ostrom alá vette az ipari létesítményeket. A biztonsági rendszer kijátszásával gyakorlatilag bármelyik rendszer felett át lehet venni irányítást, és ezt a rendszerkezelők lehet, hogy észre sem veszik

3.1 Megelőző intézkedések

A megelőző intézkedések segítségünkre vannak a biztonsági eseményekre való felkészülésben, védelmi intézkedések meghozatalában. Ezek leggyakrabban:

- Biztonsági auditok
- Biztonsági eszközök fejlesztése
- Riportok, értesítések (sérülékenységről, kártékony szoftverekről)
- Technológia figyelés (trend analízisek, védelmi technikák)
- Hálózat monitoring (behatolás figyelés)

Az internet kínálta előnyök miatt, a világháló elterjedt és szükségszerű használatával az elvárható biztonság megvalósításához a rendszerek elszigetelése, az internetről történő leválasztása ma már nem lehet megoldás. A megfelelő védelem megtervezésénél ennél is tovább kell menni, azt is ellenőrizni kell, hogy a rendszerek nem csatlakoznak-e egyéb olyan környezetekhez, amelyek viszont csatlakoznak az internethez, ezáltal kockázatot jelenthetnek a kártevőkkel történő fertőzés szempontjából. Éppen ezért az ipari folyamatvezérlő rendszerek ellen irányuló kiberfenyegetések, támadások felfedezéséhez és blokkolásához nem elegendő egyetlen, az ipari hálózat védelméhez kialakított tűzfalra támaszkodni. A hatékonyság növelésére célszerű olyan biztonsági modellt alkalmazni, amely az ipari tűzfal előnyeire építve további dedikált folyamatvezérlési tűzfal használata mellet egyéb védelmi intézkedéseket, mint például víruskereső szoftvert, behatolás-érzékelést, hálózati csomagtükrözést (Network Packet Brokers) is alkalmaz. Az ilyen jellegű védelmi modellt mélységi védelemnek nevezzük, melyet az alábbi ábra szemléltet.

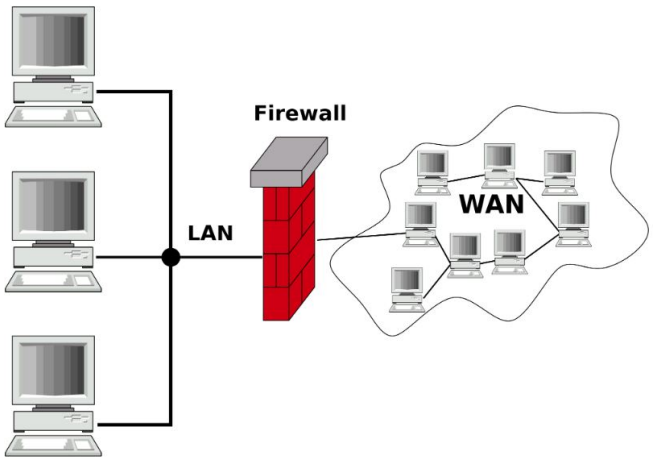


3.3. ábra: Megelőző intézkedések (forrás:Benyó Pál:Az információbiztonság speciális témakörei)

3.2 Védelmi eszközök

Tűzfalak

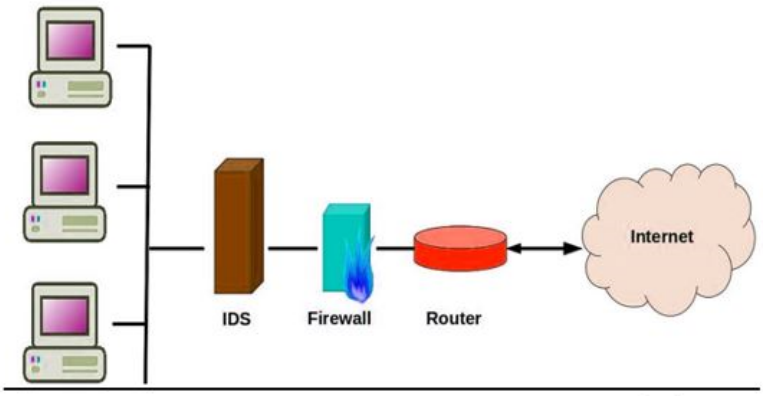
A tűzfalakkal kezdődik a hálózatok védelme [4]. A hálózat belépési pontjain elhelyezett eszközök feladata, hogy a hálózatok között csak olyan forgalmak valósuljanak meg, aminek az eredetéről és „tisztaságáról" meg vagyunk győződve. Minden olyan forgalmat, ami nem azonosított, vagy kártékony, megakadályozzon. Az új típusú tűzfalak NGFW (Next Generation Firewall) védelme már nem csak belépési pontra koncentrálódik, hanem a felhasználó végpontok védelmét is ellátja



3.4. ábra: Tűzfal (forrás: https://www.infysec.com/services/security-and-defense/firewall-auditing)

IDS (Intrusion Detection Systems)

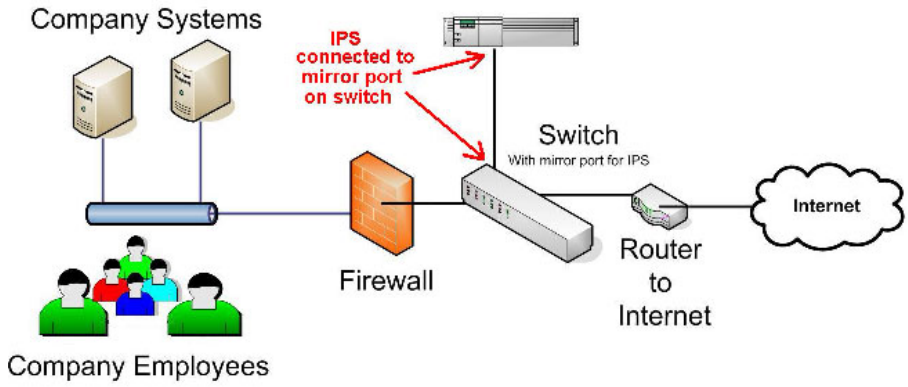
A behatolás-észlelő rendszer, azaz Intrusion Detection Systems [5], melynek rövidítése: IDS [6], amely felügyeli a hálózat és a rendszer állapotát a különféle támadási kísérletek vagy támadási eredmények észlelése érdekében. Ezzel biztosítja a hálózati rendszer erőforrásainak titkosságát, integritását és elérhetőségét.



3.5. ábra: IDS (forrás: https://www.comodo.com/ids-in-security.php)

IPS (Intrusion Prevention System)

A Intrusion Prevention System [7] - rövidítése IPS -, azaz behatolás-megelőző rendszer. Az IPS eszköz elemzi az adatforgalmat. A beállított biztonsági házirend alapján intézkedéseket tehet, például: riasztást küld, illetve a támadás blokkolása érdekében eldobja a csomagot, leválasztja az érintett alkalmazást.



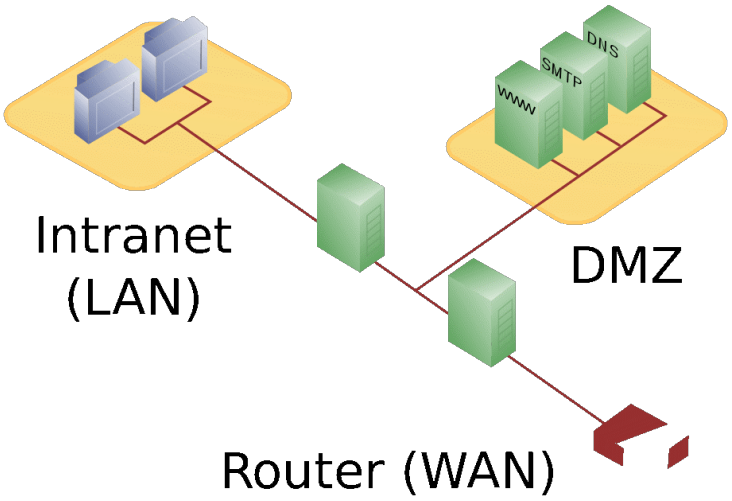
3.6. ábra: IPS (forrás:https://www.comodo.com/intrusion-prevention-systems.php)

Vírusvédelem

A vírusvédelmi szoftvereket úgy fejlesztették ki, hogy megvédjék a számítógépeket, az okostelefonokat vagy a táblagépeket a vírusok és a kártevő programok ellen. Meg kell említeni, hogy napjainkban a hagyományos vírusvédelmi szoftvereket leváltja az ismert és még ismeretlen nulladik napi kártevő ellen is védő EDR- (Endpoint Detection and Response) védelemmel kiegészített megoldás.

DMZ (Demilitarizált zóna)

A DMZ [8]védelem lényege, hogy a vállalati hálózatok megbízható védelme érdekében a nyilvános hálózatok WAN (Wide Area Network) felől érkező külső támadó csak a DMZ-ben található eszközökhöz férhet hozzá, nem az egész hálózathoz.



3.7. ábra: DMZ (forrás:https://www.ionos.com/digitalguide/server/security/what-is-a-demilitarized-zone)

4 KIBERVÉDELMI INTÉZKEDÉSEK A MOL NYRT IPARI KÖRNYEZETÉBEN

A MOL-csoport több mint 40 országban jelenlévő nagyvállalat, amely a régió vezető energetikai vállalata, és annak kiemelkedő fontosságú gazdasági szereplője. MOL Nyrt. törekszik az innovatív informatikai biztonságtechnológiai eszközök bevezetésére, üzemeltetésére - elkötelezettséget vállalva az információs értékek védelme mellett - , hosszú távon az informatikai biztonság megteremtésére.

4.1 Hálózati kommunikáció védelme

A MOL-csoport Kiberbiztonsági Architektúra csapata 2020. október 19-től november 20-ig három olyan iparbiztonsági eszközt tesztelt, amelyek elsődleges célja a hálózatikommunikáció láthatóvá tétele az ipari hálózatokon [9], belül. Az eszköznek képesnek kell lennie arra, hogy figyelmeztetést adjon gyanús behatolási kísérletről, megszokottól eltérő hálózati kommunikációról, jelentést kell tennie a kihasználható sebezhetőségekről.A rendszer együtt kell, hogy működjön a Packet Brokerrel, aminek ebben az esetben feladta az ipari hálózat forgalmának gyűjtése, tükrözése a kiberbiztonsági elemzéshez.

Tesztelt eszközök:

- SCADAfence Platform [10]
- Nozomi Guardian [11]
- Claroty CTD [12]

Mindhárom eszköz közel azonos tudással van felszerelve, nagyon hasonló szolgáltatásokat nyújtva. Ugyanakkor a Nozomi Network Guardian (továbbiakban: Nozomi) előnye a másik két rendszerhez képest az volt, hogy az ipari protokollokat széleskörűbben és mélységeiben jobban ismerte a konkurens gyártók termékeinél. Ennek megfelelően a bemutatott védelmi eszközök közül a Nozomi termékre esett a döntéshozók választása. A kiválasztási folyamatban a vendorok (beszállítók/termékforgalmazó) online értekezleteken mutatták be saját termékeiket, és azok tulajdonságait demo hálózati modelleken. Ezeken az online értekezleteken megfigyelőként én is részt vehettem, így megismerhetővé váltak számomra a lehetséges későbbi kiberbiztonsági eszközök és működésük, valamint a kiválasztási szempontrendszer. Ez utóbbi valójában a bemutatott információk függvényében időről-időre módosult, rugalmasan alakult az újabb és újabb felvetett kérdések, problémák és szükségletek vonatkozásában.Végül is a kiválasztási szempontok között szerepelt az eszköz célszerűsége, műszaki paraméterei, minőségi megfelelősége, ipari környezetben nyújtott működési megbízhatósága, a folyamatos műszaki support és a költséghatékonyság is. A beérkezett ajánlatok közül ezen kritériumoknak a Nozomi

eszköz felelt meg leginkább. A fenti kiválasztási kritériumok meghatározását indukálta az ipari területen található vezérlő eszközök magaszíntű támogatásának és a vállalati információk illetéktelen hozzáférés és nyilvánosságra hozatal elleni védelmének hatékony megvalósításának igénye. A cég számára kiemelten fontos a jelenlegi ipari hálózatba történő integrálás problémamentes megvalósítása.

5 SCOPE ÁLTAL ÉRINTETT TERÜLETEK

A kiválasztott ipari területen az alábbi Honeywell Szabályozástechnikai Kft. (továbbiakban: Honeywell) eszközei találhatóak:

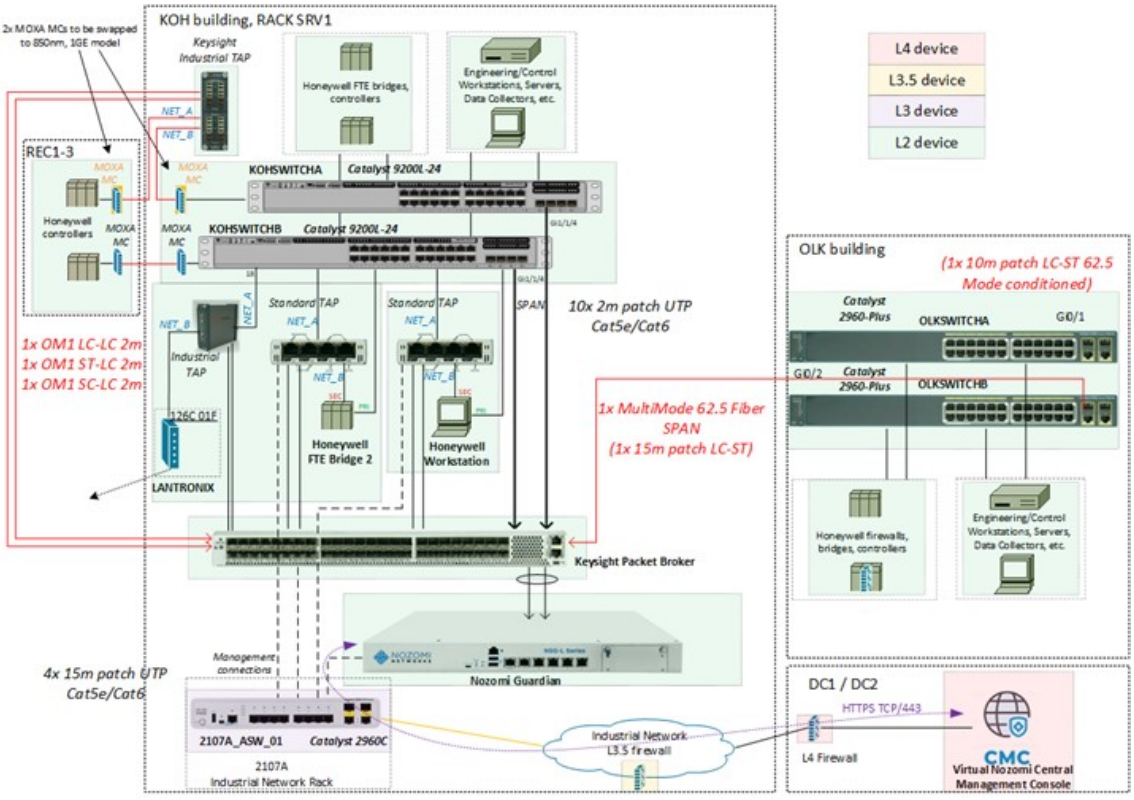
- Lube Oil Hydrofinishing rendszer (KOH) (Honeywell FTE Bridge, C300 vezérlők, munkaállomások, szerverek).
- Recirkulációs hűtővíz rendszer (REC1-3) (Honeywell tűzfal, vezérlő).
- Kenőolaj-keverés (OLK) (Honeywell tűzfal, vezérlő, FTE Bridge).

A KOH-ban és az OLK-ban a Honeywell eszközök Cisco Catalyst switches csatlakoznak. A vezérlők, FTE Bridges és kritikus szerverek, munkaállomások redundánsan kapcsolódnak a Catalyst switchez. Az épületek OM1 múltimodusú optikai kábellel vannak összekötve.

6 RENDSZER FELÉPÍTÉSE SPAN PORTOKKAL ÉS HÁLÓZATI TAP-EKKEL – KÉSŐBBI SZAKASZ

Az alábbiakban bemutatásra kerülő lehetőség még nem elfogadott, és csak a 10. szakaszban bemutatott teszt rendszer lehetséges jövőbeli kiterjesztéseként tekinthető.

Az opcionális architektúra további hálózati TAP-eket (Test Access Point) és egy Packet Broker eszközt használ az adatforgalom összegyűjtésére. Ennek a tervezésnek az a célja, hogy tapasztalatot szerezzen a réz és az optikai szálas TAP működéséről, miközben a kiválasztott gazdagépek csak egyszeri, átmeneti redundanciáját okozza. A javasolt architektúrában egy kiválasztott Honeywell Bridge redundáns, másodlagos interfészét, egy Honeywell munkaállomást és egy Lantronix eszköz csatlakozását a réz hálózati TAP-okhoz helyeznék át. Ezenkívül a KOH és az OLK közötti redundáns szálkapcsolatot egy optikai szálas TAP beillesztésére használnák, amint azt az alábbi ábra mutatja:



6.1. ábra: Rendszerarchitektúra SPAN kapcsolatok és TAP-ek (forrás: MOL Nyrt)

A REC1-3 épület és a KOH közötti üvegszálas TAP teszteléséhez 2x MOXA médiakonvertert le kell cserélni egy olyan modellre, amely 850 nm-es lézert és 1G Ethernet sebességet használ.

Az OLK és a KOH közötti kábel hossza (400 m) nem teszi lehetővé multimódusú TAP telepítését. Az Ixia jelenleg értékeli az 1310 nm-es lézer használatát az ipari üvegszálas TAP-jain (amelyek OM1 és 850 nm lézertanúsítvánnyal rendelkeznek), de hivatalos eredmény, ajánlás nem áll rendelkezésre a szakdolgozat készítésének időpontjában. Emellett az 1310 nm-es 100Base-FX átvitel még nem támogatott a Packet Broker oldalon.

Megjegyzés: A 100Base-FX alapú átvitelt széles körben használják a MOL-ban.

A TAP-ok sikeres beillesztése után a SPAN (Switch Port Analyzer) konfigurációt úgy alakítják ki, hogy kizárják a TAP-ok által már felügyelt forrás-interfészeket, és az összes TAP-nak és az összes SPAN-interfésznek minden monitorozott interfésze egy csomagközvetítőhöz csatlakozik, amely továbbítja a forgalmat a Guardian készülékhez.

A végső megvalósítás előtt még feladatot jelent a MOL és a Honeywell közötti TAP-ok segítségével egyedi monitorozás alá eső hostok kiválasztásának egyeztetése.

A kiválasztott megoldásnak figyelembe kell majd vennie a működési megbízhatósági követelményeket (és az esetleges kockázatokat). A választáshoz a Honeywell-el való egyeztetése és annak jóváhagyása szükséges.

6.1 Kezelői kapcsolatok

Ebben az architektúrában a Guardian készüléken kívül további felügyeleti interfésszel rendelkező eszközök is lesznek, amelyeket a hálózathoz kell csatlakoztatni:

- 1 db Packet Broker (10/100/1000 Base-T, RJ45 csatlakozó)
- Opcionális: 2db réz TAP (10/100/1000 Base-T, RJ45 csatlakozó)

7 SZENZOR INTERFÉSZEK, TAP-EK , PACKET BROKER

A Guardian érzékelő interfészei valószínűleg 2x 10/100/1000Base-T (RJ45) interfészek lesznek, amelyek alapértelmezés szerint elérhetők a készüléken (bővítőkártya nélkül). Ezek az interfészek a Packet Broker Tool portjaihoz csatlakoznak. Az interfészeken terheléselosztás konfigurálva lesz.

A Packet Broker hálózati portjai (fogadó interfészek) az alábbiak szerint csatlakoznak a TAP monitor portjaihoz és a SPAN csatlakozásokhoz:

- 4 réz monitor port 2 TAP-ról
- 2 MM optikaiszálas monitor portok 1 TAP-ről
- 2 réz SPAN port
- 1 MM optikaiszálas SPAN port

8 ESZKÖZÖK ÉS SZOLGÁLTATÁSOK

8.1 Adatelfogási lehetőségek

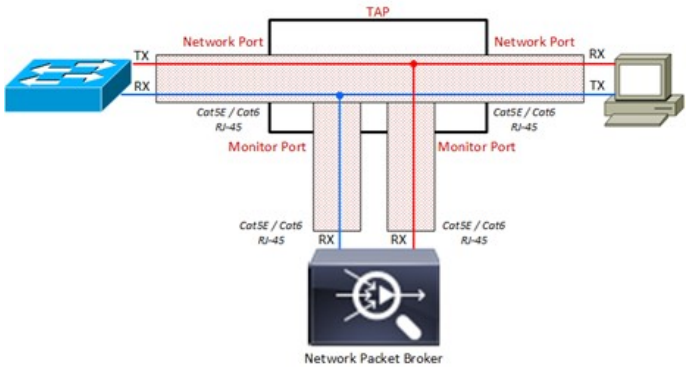
A Guardian készülék (vagy bármely más IDS készülék) hatékony működése nagymértékben függ attól, hogy mennyi adatot kap az elemzéshez. Ha a készülék több adatot fog el, tanulási hatékonysága az adatnagysággal arányosan megnövekszik. Több adatból, több naplófile készül, mely a rendszerüzemeltető számára több információt szolgáltat a hálózaton áthaladó adatokról. Az adatelfogás megvalósítására különféle stratégiák, eszközök és lehetőségek állnak rendelkezésre. Az alábbiakban az a két adatelfogási lehetőség kerül bemutatásra, amely kivitelezhető lehet a projekt jelenlegi fázisában:

8.2 Port tükrözés a switcheken (SPAN)

A legegyszerűbb és legolcsóbb módszer az ipari hálózaton működő Cisco Catalyst kapcsolók porttükrözési képességeinek használata. A javasolt rendszerarchitektúra 1. opciója ezt a módszert használja a hálózati forgalom elfogására, és ez az egyetlen jóváhagyott megoldás a Honeywell által. Két különböző épületben (KOH és OLK) található 2-2 switch, amelyeken lehetőség van SPAN portok konfigurálására.

8.3 Standard réz hálózati TAP-ek -opcionális

A réz TAP-ok aktív eszközök, mivel részt kell venniük a kommunikáló gazdagépek közötti Ethernet-kapcsolat szintű sebesség-tárgyalási folyamatban, de nincs MAC (Media Access Control) címük, így ezeket tekinthetjük ISO/OSI (Open Systems Interconnection Model) Layer 1-es eszközöknek (mint a régi Ethernet HUB-ok). Bármilyen forgalom is halad a hálózati portok között, az tükröződik a Monitor/TAP portokon, ahogy az alábbi ábrán látható:



8.1. ábra: Réz TAP működési logikája (forrás: MOL Nyrt)

A TAP-ok használatának előnye, hogy segítségükkel még az ethernet szintű hibákat is továbbíthatunk adatelemzésre. Valamint a TAP-portok túljelentkezése miatt nem vesznek el adatok, az Ethernet forgalom minden iránya saját, dedikált fizikai Ethernet interfésszel rendelkezik, ahol az átvitel történik. A SPAN portok használatának előnyeit és hátrányait, valamint a TAP-ek használatának jellemzőit az alábbi táblázat mutatja be:

A SPAN portok használatának jellemzői	A hálózati TAP-ok használatának jellemzői
Olcsó (csak konfigurációs és patch kábelek szükségesek)	Drágább
Gyorsan megvalósítható, anélkül, hogy megzavarná a termelési környezetet	A telepítés zavaró lehet
Fenn kell tartani	Nem igényel karbantartást (az optika TAP-ek teljesen passzívak, a réz TAP-ek ISO/OSI L1 eszközök)
Hajlamos az operációs rendszer, hibáira és sebezhetőségeire	A kezelési és adattovábbítási síkok fizikailag elkülönülnek egymástól, a hálózati adatok semmilyen módon nem érintettek. Az optikai TAP-ek teljesen passzívak.
Alacsony prioritású folyamat (eredetileg csak hibaelhárításra szánták), a csomagtovábbítás nem garantált	Dedikált eszköz, garantált adatátvitel, magas MTBF, különösen robusztus TAP-ek (100.000+ óra), áramkimaradás esetén, optikai TAP-eknek még áramforrásra sincsenek szükségük
Nehezen nyomon követhető	Nyomon követhető a Packet Broker Side oldalon (egyes réz TAP-ek kezelői felületekkel is rendelkeznek)
Csomagvesztés a lehetséges túljelentkezés miatt (sok forráskapcsolat 1 vagy 2 célfelülethez)	Nincs túljelentkezés
Az Ethernet-szintű hibákat nem továbbítják	Ethernet-szintű hibák továbbításra kerülnek (riasztást lehet emelni az analizátorokon)
Összefoglalva: a jó kiindulási pont, de csak a legjobban működő adatforrással javasolt mert nem biztosítja a 100% -os láthatóságot az idő 100% -ában	Minden csomag folyamatosan továbbításra kerül. Az egyetlen megoldás a 100%-os láthatóság érdekében

8.2. ábra: TAP-ek összehasonlítása (forrás: MOL Nyrt)

A TAP-ek lehetnek menedzselhető és nem menedzselhető, vagy más szempontból standard vagy ipari kivitelű réz kábelezésű és optikai TAP-ek, amelyeket az alábbiakban mutatok be:

8.4 Ipari kivitelű TAP-ek

Az ipari kivitelű TAP-ek az alapoktól kezdve úgy készültek, hogy megfeleljenek a zord környezet követelményeinek. A TAP redundáns sorkapocs tápcsatlakozókkal van ellátva, annak érdekében, hogy ha az elsődleges áramforrás meghibásodik, a TAP automatikusan áttudjon váltani a tartalék áramforrásra. Ha mindkét bemeneti áramforrás meghibásodik vagy eltávolítják azt, a TAP továbbra is továbbítja a forgalmat a hálózati portjai között (fail-open). Ez az eszköz azonban nem menedzselhető, nem programozható.

8.3. ábra: Ipari TAP (forrás:https://www.keysight.com)

8.5 Standard réz hálózati TAP-ek

A szabványos réz TAP-eket úgy tervezték, hogy mindennapos környezeti feltételek mellett működjenek. A Keysight frissen kiadott réz TAP-je intelligens TAP-ként használható. Lehetőség van az eszköz kezelőfelületen keresztül történő elérésére, valamint az eszköz működési adatainak nyomon követésére és gyűjtésére (úgy mint: interfész állapota, teljesítményállapota, forgalmi statisztikák). A teszt fázisban a megbízhatóság megítélése érdekében hasznos a megfigyelt réz ethernet kapcsolatok állapotának követése a TAP webes felhasználói felületén keresztül, és az SNMP (Simple Network Management Protocol) alapú monitorozás beállítása. Az eszköz eléréséhez három különböző jogosultsági szint áll rendelkezésre a portok, a porthasználat és küszöbérték, az eszközinformációk, megbízható alhálózatok, kapcsolatszűrés, sebességstatisztika, SNMP csapda attribútumok vonatkozásában. A jogosultsági szintek a hozzájuk rendelt jogosultságokkal az alábbiak:

- a rendszergazda megtekintheti és konfigurálhatja azokat
- az operátor információkat tekinthet meg a fenti attribútumokról, valamint konfigurálhatja a portokat, a port kihasználtságot és küszöbértéket, valamint a hálózatkezelést
- a felhasználó információkat tekinthet meg az attribútumokról.

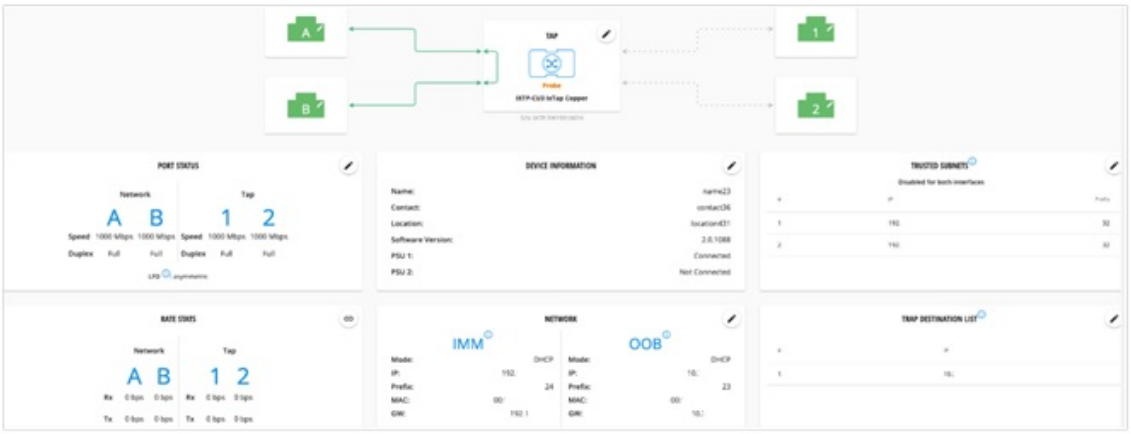
Az eszköz további előnye, hogy beépített tűzfallal is rendelkezik, amely csak megbízható alhálózatokról engedélyezi a kapcsolatokat.

Az eszköz fizikai elrendezése:

8.4. ábra: Standard réz TAP (forrás:https://www.keysight.com)

A TAP jellemője, hogy egyetlen RU-ban 4 db réz TAP szerelhető fel egy szerelőkészlet segítségével. Mindegyik TAP-nak 2 tápegysége van, és lehetőség van az összes TAP táplálására egyetlen külső tápegység használatával, amely szükség esetén 16 TAP-ot tud kiszolgálni.

A készülék webes felülete az alábbi ábrán látható:

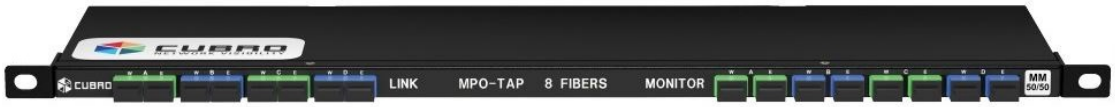


8.5. ábra: Standard réz TAP felügyeleti felülete (forrás:https://www.keysight.com)

A tervezés jelen fázisában a fenti TAP megvalósítása látszik célszerűnek, de az elképzelések között szerepel az optikai hálózatokra illeszthető TAP-ek beszerzése is. Azonban ez utóbbi költségesebbnek mutatkozik, illetve nem sikerült megfelelő, megbízható szolgáltatót találni ennek megvalósításához, ezért a jelenlegi álláspont szerint a fentiekben bemutatott TAP-ek kiépítésére kerül sor nagy valószínűséggel a cégnél. Ennek ellenére szeretném dolgozatomban néhány szóban bemutatni az optikai hálózatokra illeszthető TAP-eket is.

8.6 Optikai hálozatok TAP-jei

Az üvegszálas TAP-ek teljesen passzívak, és egyszerű „Y” kábelnek vagy optikai prizmának tekinthetők. Előre meghatározott arányban osztják meg a fény energiáját a hálózat és a monitor-portok között. Az optikai TAP az alábbi grafikán látható:

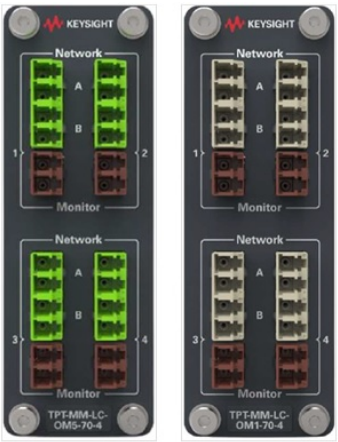


8.6. ábra: Optikai TAP specifikáció (forrás: https://www.cubro.com)

Az ábrán látható kék színű portok olyan hálózati portok, ahol élő forgalom folyik a hálózati eszközök között. Ezen hálózati portokról érkező forgalom tükröződik a zöld színű portokra. Különböző felosztási arányok állnak rendelkezésre a hálózat és monitor közötti megosztás szempontjából, mely arányok 90/1-tól 50/50-ig (hálózat/monitor) terjedhetnek. Általában 70/30-as megosztású forgalom ellenőrzés elegendő a megfelelő információ szerzéshez az adatokról, ami jellemzően 2,4 dB veszteséggel jár a hálózati kapcsolaton

8.7 Ipari hálozatok optikai TAP-jei

Az ipari TAP-eket kifejezetten extrém környezetben való működésre tervezték, teljesen passzívak és DIN (Deutsches Institut für Normung) sínre szerelhetők. Egyetlen TAP modul négy TAP-et tartalmaz és csak MultiMode, és 70/30-as (hálózati/monitoros) verziók állnak rendelkezésre, mint ahogyan az alábbi ábrán látható:

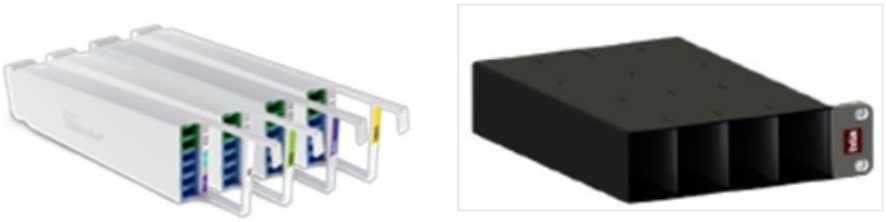


8.7. ábra: Ipari hálózat Optikai TAP (forrás:https://www.keysight.com)

Ahogyan az fenit ábrán is látható a Flex Tough Tap kialakítása a „Run to Fail” üvegszálas hálózatokhoz van optimalizálva. Igaz ez a régi és új technológiára egyaránt. Jelenleg két modellben kapható: 1G OM1 multimódusú optikai szál a régebbi hálózatokhoz (62,5 um), és a legújabb OM5 multimódusú (50 um) optikai szál az újabb üvegszálas hálózatokhoz.

8.8 Standard Optikai TAP-ek

Standard optikaiszálas TAP-ek SingleMode és MultiMode változatban állnak rendelkezésre, különböző felosztási aránnyal 90/10 és 50/50 között.

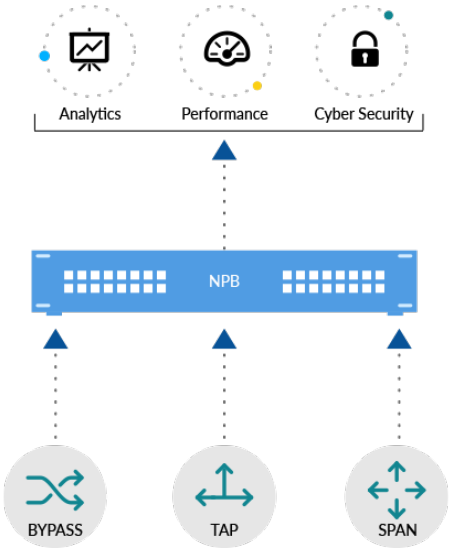


8.8. ábra: Standard Optikai TAP modelljei (forrás:https://www.keysight.com)

Összefoglalásként elmondható, hogy a MOL Nyrt-nél olyan TAP-ek beszerzése szükséges a rendszer megbízható működése szempontjából, amely ipari környezetben megbízhatóan folyamatos jelleggel használható. Ez szükségszerűen azt jelenti, hogy ipari és réz kábelezésű TAP beszerzésére fog sor kerülni.

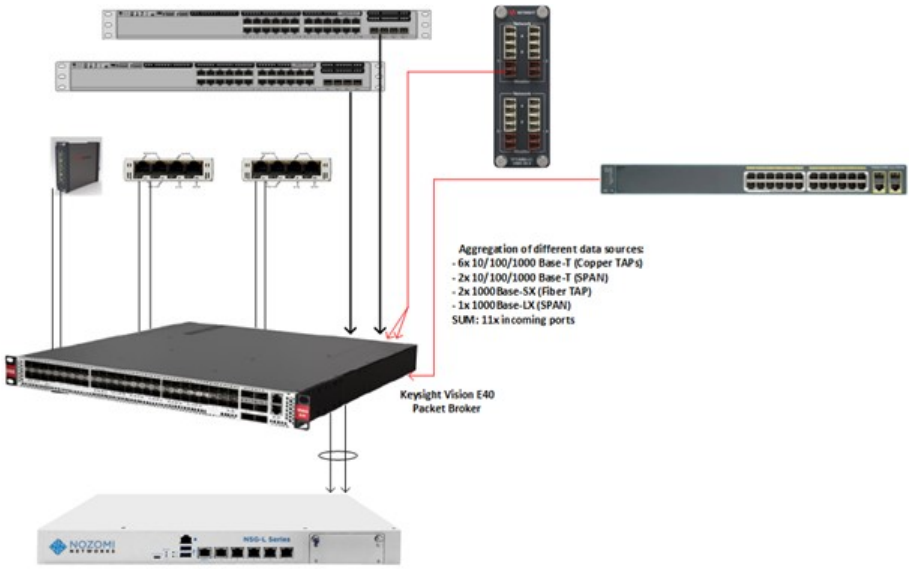
8.9 Adatgyűjtés: Network Packet Broker

A Network Packet Broker [13] olyan hardvereszköz, aminek a segítségével betekintést nyerhetünk abba, hogy pontosan mire van szükség a hálózat és eszközeinek jobb teljesítményéhez. Ezt az információt a biztonság és a megfigyelési technológiák elősegítésével állítják elő. A Network Packet Brokers képes csökkenteni az erőforrások pazarlását, a költségeket és természetesen a hekkelés lehetőségeit. Ennek oka, hogy az Network Packet Broke konkrét szabályokat és szűrőket alkalmazhatnak, mielőtt továbbítják a forgalmat a különböző hálózati eszközökre, például a teljesítménymenedzsmentre, a hálózati biztonságra és más felügyeleti eszközökre.



8.9. ábra: Packet Broker (forrás: https://www.cgstowernetworks.com)

A Network Packet Broke segítenek a különböző adatforrásokból (SPAN-ek, TAP-ek), különböző átviteli médiától (réz, üvegszál) érkező különböző adatsebességű (1-100 Gbps) adatok egyetlen eszközbe gyűjtésében, az opcionális szűrés és adatkezelés mellett. A begyűjtött adatok kiküldése egy vagy több adatelemző eszközre, egy vagy több interfészen terheléselosztással vagy összesített módon is történhet. A projekt ezen szakaszában a Honeywell egy Packet Broker eszközt fog telepíteni, amely a SPAN portokról érkező hálózati forgalmat összesíti, és továbbítja a Nozomi Guardian készülékhez. A Packet Broker alapú rendszer és a TAP-ok lehetséges jövőbeli bővítése az alábbi ábrán látható:



8.10. ábra: Lehetséges központosított architektúra (forrás: MOL Nyrt)

A TAP-ek és SPAN portok adatelfogásra is használhatók, a csomagközvetítő megkönnyíti a különböző adatforrásokból származó adatok gyűjtését az alábbiak szerint:

- forgalom 3x réz hálózatú TAP-ről
- forgalom egy üvegszálas TAP-ről
- forgalom a helyi KOH switch-ről (2x SPAN kapcsolat)
- forgalom a távoli OLK switch-ről (1x SPAN csatlakozás)

A TAP-ek és a SPAN az adatokat összesítik, opcionálisan előszűrik, majd szelektíven továbbítják a Nozomi Guardian elemzőkészülékhez.

8.10 Nozomi Network Guardian eszköz

Nozomival a begyűjtött információk elemzése, megjelenítése, értelmezése hatékonyan megvalósítható és megjeleníteni a különböző ipari protokollokon zajló kommunikációt is. A Nozomi rendelkezik beépített riport-funkcióval, mely lehetővé teszi, hogy PDF (Portable Document Format) formátumban áttekinthető legyen egy adott időszak aktuális és teljes eszközleltára, az eszközök sérülékenysége, vagy az utolsó 10 riasztás jellemzője, részletei. A riportok generálása igény szerint ütemezhető és bizonyos mértékben formailag és tartalmilag is testre szabható. A kiolvasott értékek visszamenőlegesen is figyelemmel követhetők, a megszokott értékektől történő eltérés esetén pedig riasztást küldhet a rendszer. A különböző támadások, illetve protokollok szignatúráit, eszközök viselkedésének jellemzőit a Nozomi Labs részlege folyamatosan karbantartja, ha kell, reverse engineering módszerrel vissza is fejti és beépíti az operációs rendszer frissítéseibe.

A tervekben szereplő Nozomi Guardian készülék megfelelő licenc birtokában NSG-L 100-ról NSG-L 250 teljesítményszintre skálázható, így jövőbiztos befektetés lehet. A teszt szakaszban a cég NSG-L 100 licenccel tervez indulni.

8.11. ábra: Nozomi NSG-L 100 (forrás: https://www.nozominetworks.com)

A megoldás-készlet a következő elemeket tartalmazza:

Termékkód	Termék	Termék leírása	Mennyiség
NSGL-HW-P	Guardian NSG-L PerpetualHardware készülék - ACPower ellátással	Guardian NSG-L Perpetual Appliance - csak hardver - váltakozó áramú tápegységgel (Az NSG-L-250 vagy NSG-L-100 készülékekhez különböző módon értékesített szoftvert és támogatást igényel)	1
NSGL100-SW-SP-1YR	Guardian NSG-L-100 kifejezés szoftver licenc & támogatás 1 év	Guardian NSG-L-100 Term SoftwareLicense és 1 éves támogatás (a HardwareAppliance külön vásárolható meg)	1
HWA-4P-SFP-1G-P	Guardian 4 Port SFP kiegészítő kártya (1 Gbps)	Guardian 4 port SFP kiegészítő kártya (1 Gbps)	1
HWA-TRS-SX-P	Guardian SFP+ adó-vevő,1000Base-SX/10GBase-SW, 1G/10G	Guardian SFP+ adó-vevő,1000Base-SX/10GBase-SW, 1G/10G	2
SP-NSGL100-1YR	Intelligens szavazás - NSG-L-100 - 1Year	Smart Polling - 1 éves időtartamú licencguardian készülékhez NSG-L-100, includessupport, PrePaid	1
AI-NSGL100-1YR	Eszközintelligencia - NSG-L-100 - 1 Év	Asset Intelligence - 1 éves időtartamú licencguardian készülékhez NSG-L-100, beleértve a támogatást, a PrePaid-ot	1
TI-NSGL100-1YR	Fenyegetés intelligencia - NSG-L-100 - 1 Év	Threat Intelligence - 1 éves időtartamú licencguardian készülékhez NSG-L-100, beleértve a támogatást, a PrePaid-ot	1

8.12. ábra: készlet leltár (forrás: https://www.nozominetworks.com)

9 JAVASOLT RENDSZER

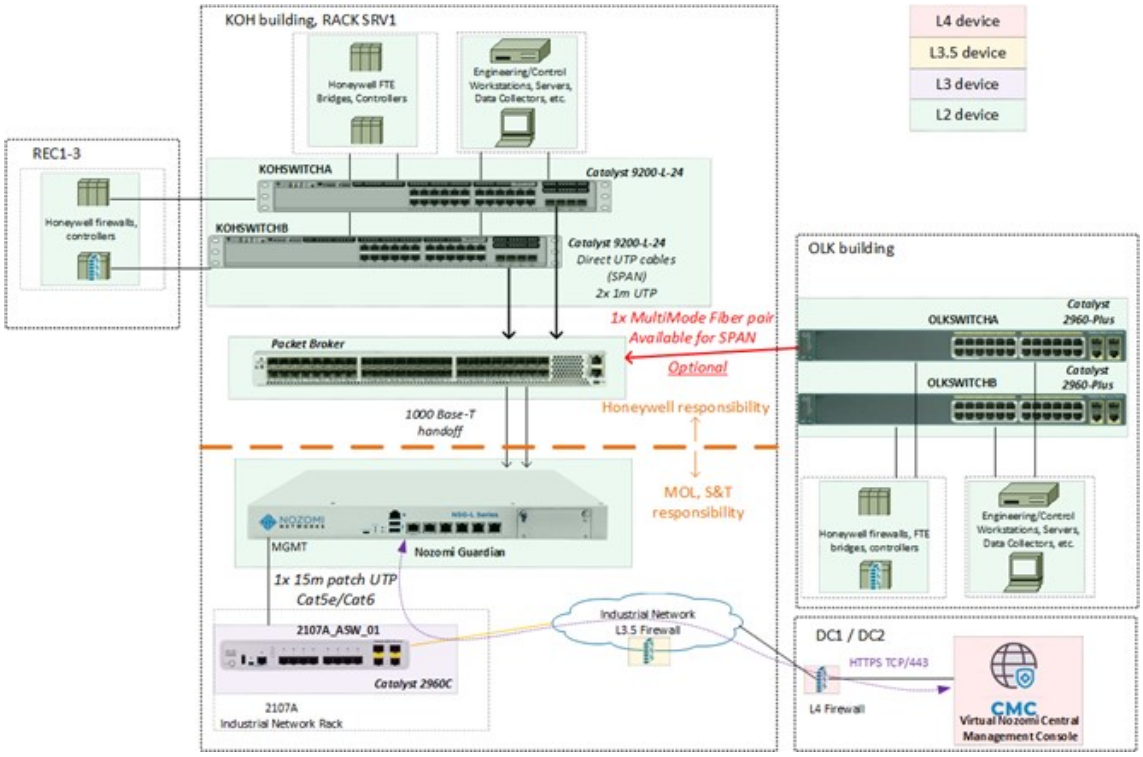
A jelenlegi teszt rendszer SPAN alapú, amihez először el kell készíteni a megfelelő konfigurációt. Emellett meg kell vizsgálni a TAP alapú megoldás megvalósíthatóságát, és az architektúrát az ipari hálózat kívánt helyein megvalósított TAP-okkal bővíteni.

A Honeywell képviselőivel folytatott konzultáció alapján, jelenleg az egyetlen elfogadható megoldás a hálózati forgalom összegyűjtésére a SPAN portok használata a Catalyst switch-en. A funkció bevezetése előtt a Honeywellnek meg kell határoznia, hogy hogyan valósítható meg ez a funkció a helyi feltételek alapján, például a kapcsolók típusa, a hálózati forgalom mennyisége alapján.

A SPAN portokból történő forgalomszűrést a Honeywell által telepített és üzemeltetett, harmadik féltől származó Packet Broker eszköz fogja befejezni. Ez a Packet Broker eszköz átadja a forgalmat a Nozomi Guardian készüléknek.

10 RENDSZER FELÉPÍTÉSE, AHOL A SPAN PORT AZ ADATFORRÁS

A kiválasztott ipari területről érkező forgalomelemzés legegyszerűbb és leggyorsabb módja a port-tükrözés funkció konfigurálása a kapcsolókon, majd a tükrözés célinterfészeinek közvetlen csatlakoztatása a Nozomi készülékhez az alábbi ábra szerint:



10.1. ábra: Rendszerarchitektúra SPAN kapcsolatokat használva (forrás: MOL Nyrt)

Ez a módszer nem igényli a fizikai hálózati kapcsolatok ideiglenes megszakítását, csak a tükrözési funkciót kell konfigurálni a kapcsolókon egy karbantartási ablakban. Az adatok forrása az összes fizikai interfész lenne, ahol a gazdagépek csatlakoznak. A Honeywell felelőssége az összes forgalom összegyűjtése és átadása a Nozomi Guardian készüléknek.

10.1 Kezelői kapcsolatok

A Nozomi Guardian készülék felügyeleti felületéhez egy dedikált felügyeleti Ethernet interfészen keresztül lehet hozzáférni. Ezt az interfészt az ipari hálózathoz kell csatlakoztatni. A fenti diagramon az ipari hálózathoz való csatlakozás látható a helyileg elérhető ASW eszközön keresztül. Az ASW eszköz dedikált VLAN-t (Virtual LAN) biztosít a Nozomi eszköz felügyeleti Ethernet interfészéhez. Ennek a VLAN-nak az alapértelmezett

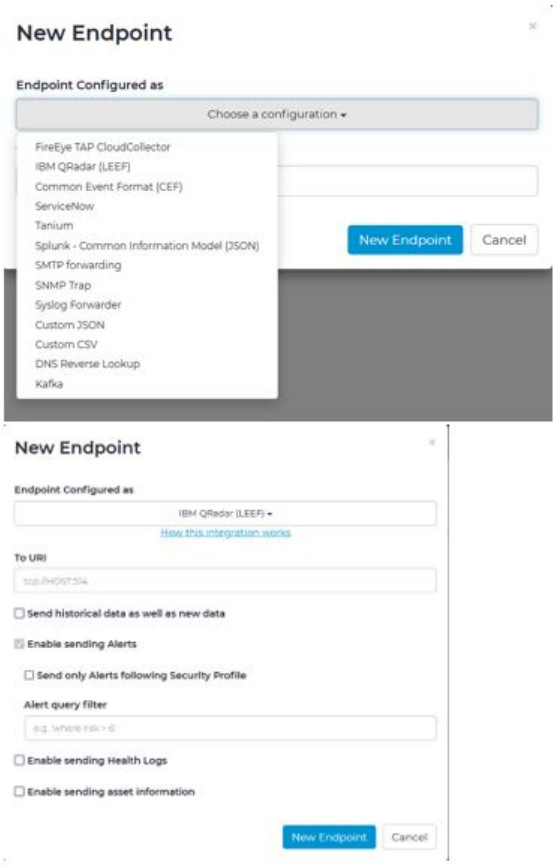
átjárójára és biztonsági átjárójára L3.5 tűzfal kerül telepítésre. Az adatelemzés eredményének megtekintéséhez a központosított hozzáférés biztosítása érdekében a Guardian készülék logikailag csatlakoztatható egy Central Management Console virtuális készülékhez, későbbi szakaszaiban részletezzük.

11 AZ ÚJ RENDSZER FUNKCIÓI

A rendszer elsődleges funkciója, hogy betekintést és részletes elemzést nyújtson a kiválasztott ipari hálózat forgalmáról, az alábbi részletekre összpontosítva:

- készítsen részletes eszközlistát
- végezzen sebezhetőségi elemzést az eszközökön
- vizualizálja a hálózati topológiát
- készítsen forgalmi viselkedés elemzést
- reagálni (riasztást generálni) az azonosított fenyegetésekre folyamatos forgalomelemzés alapján, vagy ha bármely gazdagép viselkedése eltér a megszokottól.

A Guardian készülék integrált irányítópultja a felügyelt hálózatban észlelt események valós idejű és előzményadatait biztosítja és megjeleníti. Az integrált műszerfalon kívül az adatok különböző formátumokban küldhetők ki harmadik fél készülékeibe, amint az a következő ábrán látható:



11.1. ábra: Adatintegrációs lehetőségek riasztáshoz (forrás: MOL Nyrt)

A MOL követelményei, biztonsági policy-ja alapján az adatokat harmadik fél készüléke(i)nek küldjük ki. Éppen ezért fontos a rendszerbiztonság vizsgálata és ismerete. A következő részben erről szeretnék néhány gondolatot megemlíteni.

11.1 Rendszer biztonság

Az „admin” felhasználó alapértelmezett jelszavát az első rendszerindításkor meg kell változtatni.

A Guardian elérésének elsődleges módja csak a MOL CyberArk PUAM (Privileged User Account Management) rendszerén keresztül lesz engedélyezve.

Lehetőség van a Guardian készülék beépített tűzfalának konfigurálására is, annak érdekében, hogy korlátozza, engedélyezze a hozzáférést bizonyos IP-hálózatokról a felügyeleti Ethernet interfészen. Ez a funkció engedélyezésre kerül majd. Az engedélyezett IP-hálózatok listája későbbiekben kerül meghatározásra és a végleges rendszerterv, illetve telepítési jegyzőkönyv fogja tartalmazni.

A rendszerhez kapcsolódni fog egy menedzsment felület, a CMC (Central Management Console), amely a hálózati incidensek által kiváltott riasztásokat tudja megjeleníteni. Emellett ez az alkalmazás látja majd el a rendszerkarbantartás és rendszerműködtetés funkcióit is.

11.2 CMC és Guardian eszközök összehasonlítása

A központi rendszerkarbantartáson és -működtetésen kívül tehát a CMC láthatóságot biztosít az összes riasztáshoz, csomóponthoz és potenciális sebezhetőségi információhoz az összes készülékről. A Guardianhez képest néhány további funkciót adtak hozzá, amelyek lehetővé teszik több száz készülék egyszerű kezelését, és eltávolítottak néhány egyéb, az élő forgalom elérhetőségétől függő funkciót, mint például a csomagrögzítés, az élő grafikon megjelenítése, és az élő munkamenetek.

A CMC különböző táblákban jeleníti meg a műveleteket. Az alábbiakban bemutatom ezek – a felhasználás szempontjából fontos - néhány jellemzőjét.

A CMC a csomóponttáblában csak a „Figyelmeztetések megjelenítése” és a „Navigálás” műveleteket kínálja (ugyanabban a táblában a készüléken találhatók a „Csomópont konfigurálása”, a „Kért nyomkövetés megjelenítése” és a „Nyomkövetés kérése” műveletek is):

11.2. ábra: Csomóponttábla-különbségek (forrás: MOL Nyrt)

A „Környezeti hivatkozások” táblában csak a „Figyelmeztetések megjelenítése” és a „Navigálás” műveletek érhetők el (a készüléken ugyanabban a táblában található még „Konfigurálás” hivatkozás, „Nyomkövetés megjelenítése”, „Nyomkövetés kérése” és „Események megjelenítése” műveletek is):

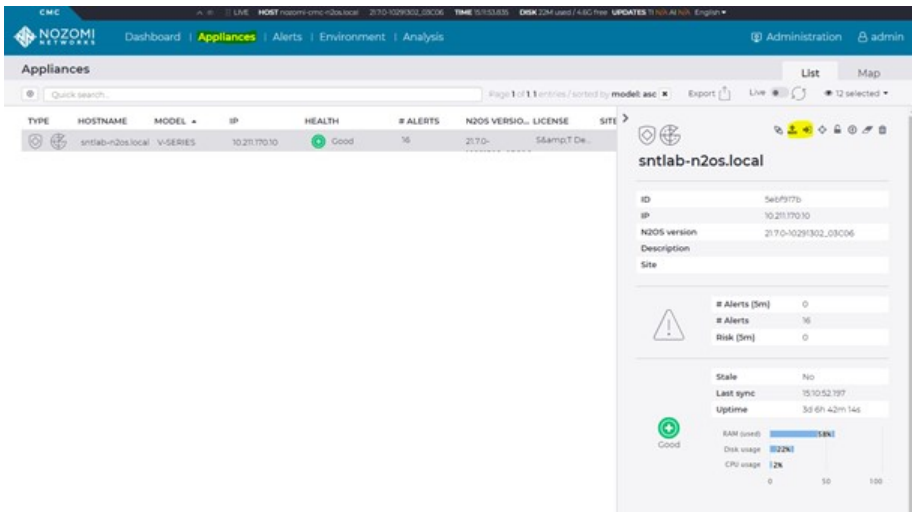
11.3. ábra: A hivatkozások táblák különbségei (forrás: MOL Nyrt)

A „Process View” táblában a változó konfigurálása művelet nem engedélyezett, de a többi művelet (Változó részletei, Hozzáadás a kedvencekhez és Navigálás) továbbra is elérhető:

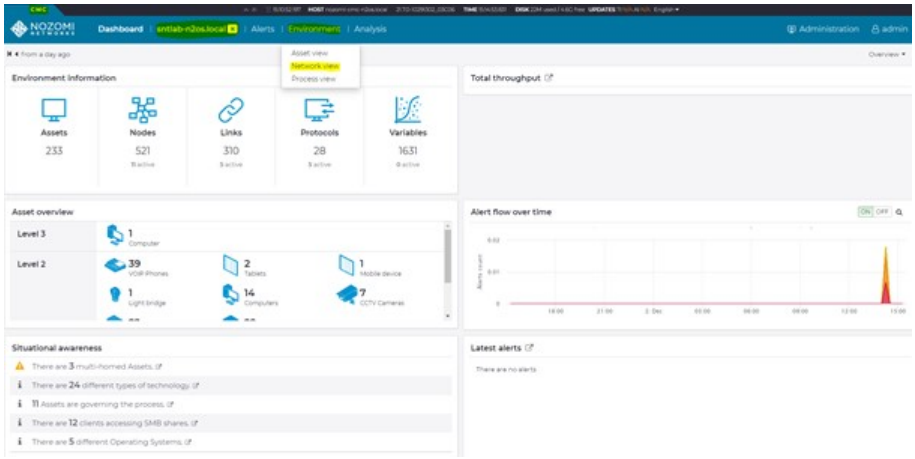
11.4. ábra: A folyamattábla különbségei (forrás: MOL Nyrt)

A konfigurációs műveletek és a nyomkövetési kérés (csomagrögzítés) funkciók csak a készülék felhasználói felületén érhetők el.

Ha több információra van szükség a Guardian készülékektől a CMC-n keresztül, lehetőség van a hálózat bármely Guardian készülékére „fókuszálni”, ekkor a hálózat vizualizációs grafikonja és a kiválasztott Guardian műszerfala is elérhetővé válik a CMC-n:



11.5. ábra: Fókusz opciók (forrás: MOL Nyrt)

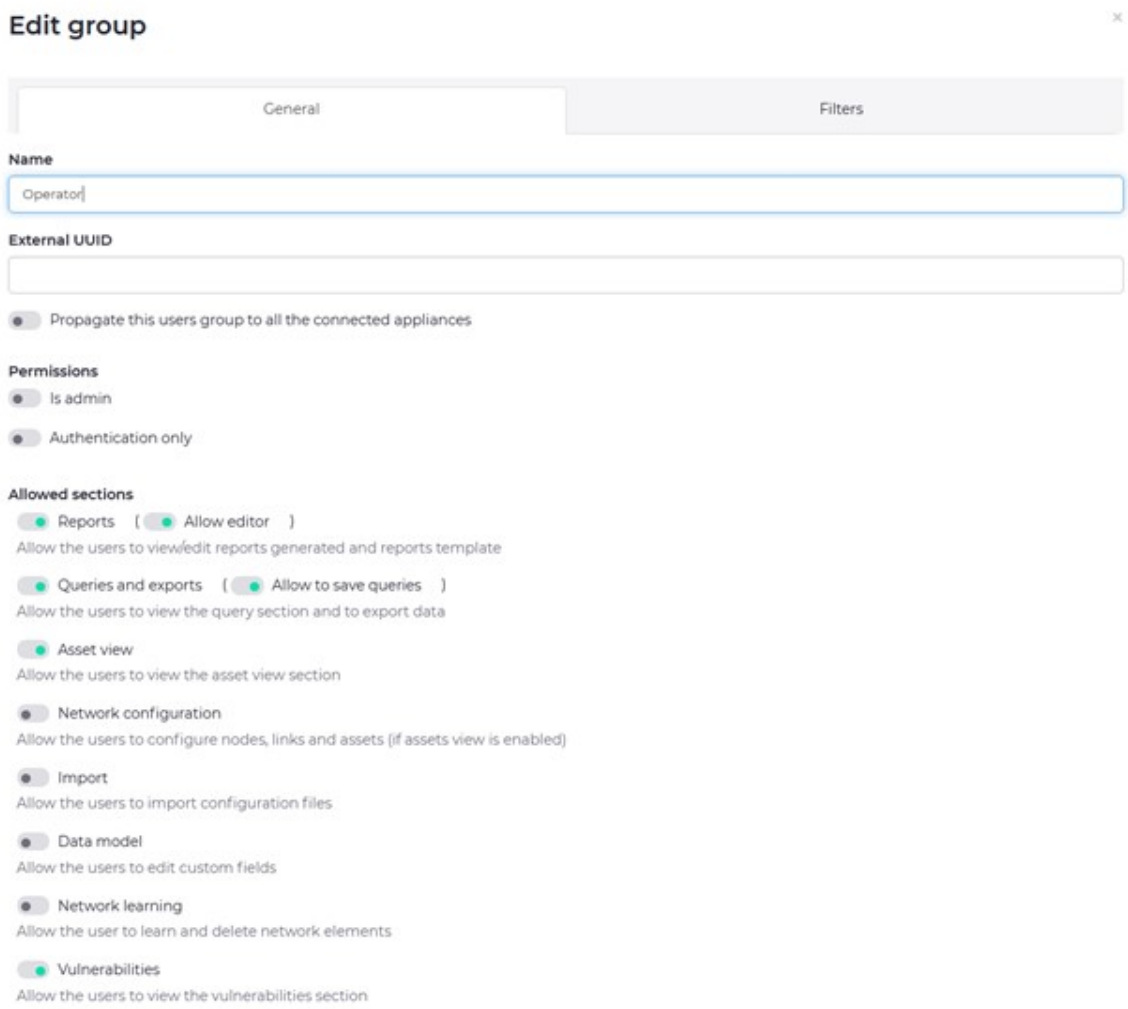


11.6. ábra: Egy készülékre fokuszált CMC irányítópult (forrás: MOL Nyrt)

Opcionálisan a CMC-n keresztül is be lehet jelentkezni a Guardian készülékbe. Ebben az esetben megnyílik egy új webböngésző lap, amelyen a kiválasztott Guardian webes felülete elérhetővé válik a CMC IP-címén. A kapcsolatot teljes egészében a CMC kezeli. Bejelentkezés után a Guardian összes funkciója elérhető lesz. A CMC-n keresztül egyszerre csak egy bejelentkezés támogatott. Ennek előnye, hogy a rendszer kezelése egy központi helyről történhet.

11.3 AAA (Authentication, Authorization, Accounting) funkciók és jelszó kezelés

A MOL szabályzatának megfelelően Active Directory alapú hitelesítés szükséges PUAM-on keresztül a bejelentkezéshez, felhasználóazonosításhoz. Lehetőség van a Nozomi AD-kiszolgálóval való integrálására a felhasználói hitelesítéshez, valamint a felhasználók és felhasználói csoportok információinak gyűjtéséhez. A felhasználók, felhasználói csoportok számára részletes jogosultsági paraméterek állíthatók be, amint az az alábbi képernyőképen látható:



11.7. ábra: Kezelés (forrás: MOL Nyrt)

A felhasználói csoportokat és a hozzájuk tartozó jogosultságokat a MOL biztosítja. A Nozomi oldali konfiguráció véglegesítése a MOL által szolgáltatott adatok alapján történik. Vészhelyzeti célokra a helyi rendszergazdai fiók összetett jelszóval lesz konfigurálva. Alapértelmezés szerint a Guardian szigorú jelszószabályokkal rendelkezik, az alábbiak szerint:

Shell jelszó házirendek: A helyi konzol és SSH (Secure Shell) fiókok jelszavainak összetettségei követelményeknek kell megfelelniük. Az érvényes jelszónak a következő osztályok karaktereit kell tartalmaznia:

- nagybetűk
- kisbetűk
- számjegyek
- egyéb karakterek

Ezen túl, a jelszavaknak legalább 12 karakterből kell állniuk, és a közös mintát alkotó karaktereket eldobjuk.

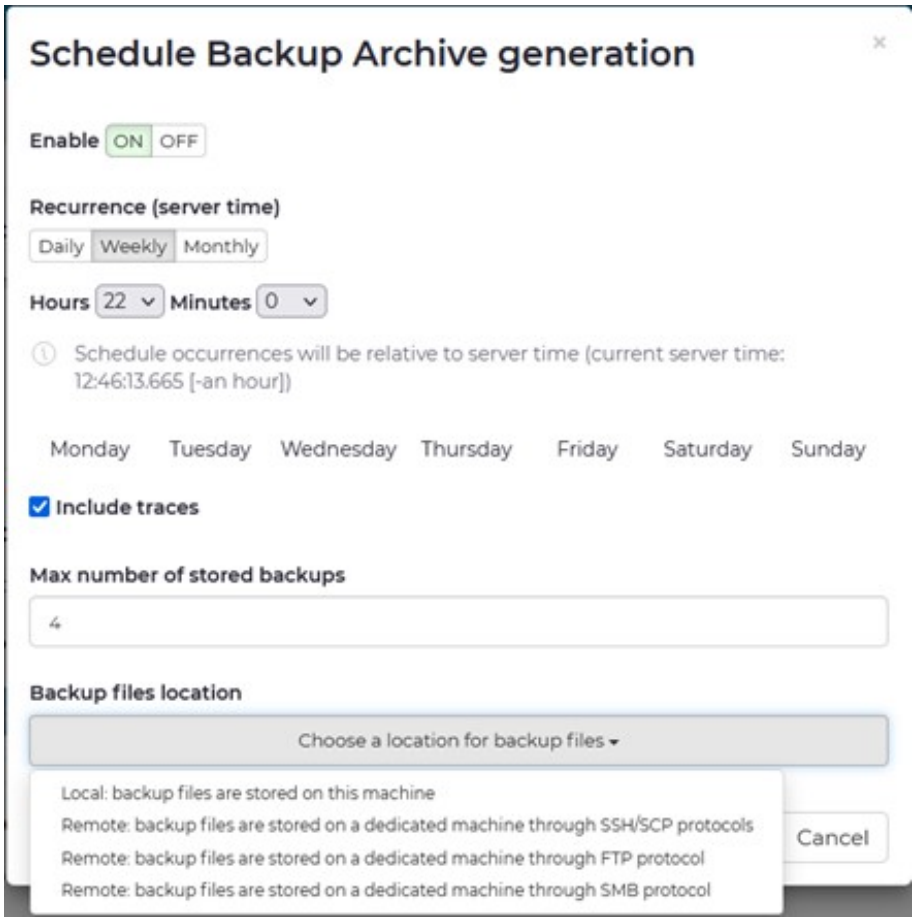
A webes grafikus felhasználói felület jelszavainak házirendje:

- a jelszavaknak legalább nyolc karakterből kell állniuk, és tartalmazniuk kell nagy- és kisbetűk és számok kombinációját.

Az alapértelmezett házirendek a CLI-n (Command Line Interface) keresztül módosíthatók, hogy a legjobban megfeleljenek a szervezeti követelményeknek.

11.4 Konfigurációkezelése és biztonsági mentés

A Guardian összes adatáról (beleértve a konfigurációs paramétereket és a környezeti adatokat is) manuálisan és ütemezett módon lehet biztonsági másolatot készíteni, ahogy az a következő képernyőképen látható:



11.8. ábra: Nozomi biztonsági mentési lehetőségek (forrás: MOL Nyrt)

A biztonsági mentési fájl tárolási helye lehet helyi vagy távoli. Távoli biztonsági mentés esetén a következő protokollok használhatók:

- SSH/SCP (Secure Shel/Secure Copy Protocol)
- FTP (File Transfer Protocol)
- SMB (Server Message Block)

Meg kell említeni, hogy a végleges rendszerterv és telepítési jegyzőkönyv fogja tartalmazni a MOL igényei és a rendelkezésre álló erőforrások alapján véglegesített, az elfogadott biztonsági mentési protokollt és a távoli szerver IP (Internet Protocol) címét.

12 RENDSZERÜZEMELTETÉS - SZEREPEK ÉS FELADATOK A PILOT KÖRNYEZET ÜZEMELTETÉSÉHEZ

12.1 Rendszerelemek és üzemeltetési feladatok

S&T Consulting Hungary Rendszerintegrációs & Technológiaátadási Kft. (továbbiakban: S&T Kft):

- Nozomi komponensek tervezése, telepítése, konfigurációja, működése és felügyelete stb.
- Csomagközvetítő komponensek tervezése, telepítése, konfigurációja, működése és felügyelete stb.
- TAP tervezés és konfiguráció (műveletek és felügyelet, ha a TAP-en engedélyezve van a kezelés).
- Rendszerriasztások kezdeti elemzése, a konfiguráció finomhangolása, rendszeres jelentések (kezdetben heti, később havi és végső összefoglaló).
- Javaslatot tegyen és tekintse át a Honeywell által biztosított SPAN konfigurációs paramétereket.
- Teljes körű adminisztratív hozzáférés a Nozomi és a Packet Broker komponensekhez a PUAM-on keresztül.
- Tájékoztatást és részletes műszaki dokumentumokat nyújtani a pilot környezetben végrehajtott változtatásokról (MOC).
- Rendszeres és ad hoc heti találkozók és megbeszélések elősegítése.
- Rendszerspecifikus képzés biztosítása.

A működtetés során, a tervek szerint, bármilyen HW megvalósítási lépést a MOL Csoporton beül működő Petrolszolg Karbantartó és Szolgáltató Kft. (továbbiakban: Petrolszolg) végez előre jóváhagyott engedély birtokában. Minden módosítás a Honeywell által csak a Petrolszolg jelenlétével valósítható meg.

Honeywell:

- SPAN konfiguráció létrehozása a switcheken.
- Biztosítani kell, hogy az egyeztetett és megvalósított SPAN konfiguráció érintetlen maradjon a pilot időtartama alatt.
- A TAP tervezésének és megvalósításának támogatása.
- Támogató tesztek a hálózati forgalom átirányítása, generálása, újra konfigurálása tekintetében.
- DCS (Digital Combat Simulator) rendszerspecifikus szakértelem biztosítása a Nozomi rendszer riasztásainak elemzéséhez, a finomhangolási tevékenységek támogatása (havi 2-3 munkanap).

– Támogatja a rendszerkonfiguráció elemzését és finomhangolását a DCS rendszer sajátosságaira tekintettel.

Petrolszolg:

– Eszközök (HW konfiguráció) implementálása a fizikai helyre az S&T Kft támogatásával.
– Csak olvasási (nem rendszergazdai) hozzáférés a Nozomi platformhoz, támogatás elemzése és a rendszerkonfiguráció finomhangolása.
– Hálózati konfiguráció megvalósítása L2-ről L4-re a Nozomi komponensek összekapcsolása tekintetében.

API csapat (informatikai csoport):

– Csak olvasási (nem rendszergazdai) hozzáférés a Nozomi platformhoz, támogatás elemzése és a rendszerkonfiguráció finomhangolása.
– DCS rendszerspecifikus szakértelem biztosítása a Nozomi rendszer riasztásainak elemzéséhez, a finomhangolási tevékenységek támogatása.
– MOC kérés benyújtása és módosítások jóváhagyása.

Karbantartás:

– A pilóta rendszeres jelentéseinek elemzése.

Kibervédelmi Központ (CDC):

– Csak olvasási (nem rendszergazdai) hozzáférés a Nozomi platformhoz, támogatás elemzése és a rendszerkonfiguráció finomhangolása.
– Beépített Nozomi rendszernaplók és riasztások a SIEM-re, a pilótakörnyezetre jellemző használati esetek létrehozása.

Csoportos kiberbiztonsági architektúra:

– Csak olvasási (nem rendszergazdai) hozzáférés a Nozomi platformhoz, támogatás elemzése és a rendszerkonfiguráció finomhangolása.
– Jóvá hagyja a pilot beállításának konfigurációs módosításait a pilot időtartama alatt.
– Rendszeres és ad hoc heti találkozók és megbeszélések elősegítése.
– Szervezzen negyedévente áttekintő üléseket szélesebb közönség számára, amely kiterjed más helyszínekre és részlegekre is.

12.2 Eszközállapot felügyelete

A készülék üzembiztonsági állapotáról élő információ a webes felhasználói felületen, a készülék kezelői felületén keresztül érhető el. Az élő adatokon kívül az eszköz állapotára vonatkozó információk SNMP protokollon keresztül továbbíthatók, amelyet engedélyezni kell a készülék CLI-jén.

A rendszerállapot-adatok továbbításának egyéb lehetőségei is lehetségesek a beépített adatintegrációs módszerek használatával. Ily módon az állapotnaplók meghatározott formátumban továbbíthatók harmadik fél készülékei számára. Az események formátuma, a célkészülékek típusa a következő lehet:

- Gyakori eseményformátum.
- SMTP (Simple Mail Transfer Protocol) továbbítás.

Mivel a MOL-csoport már rendelkezik működő, a Petrolszolg által üzemeltetett Nagios szerverrel az ipari hálózatban lévő eszközökhöz, ezért tervezzük ennek az ICMP ((Internet Control Message Protocol) és SNMP (Simple Network Management Protocol) alapú megoldásnak a Nozomi környezetbe való integrálását.

13 RENDSZER TESZTELÉSE

A védekezést szolgáló informatikai céleszközök, a tesztelésbe bevont ipari területen beüzemelésre kerültek 2022 szeptember 26. napjával. A pilot projekt tervei szerint a kiberbiztonsági rendszer a jelenlegi formájában egy évig fog működni, ami valójában a teszt időszaka lesz. A tesztelési folyamat és időszak eredményeinek, tapasztalatainak monitorozását követően kerülhet majd sor a tényleges működésére a nagyipari környezetben.

Az egy évre tervezett, viszonylag hosszú tesztelési időszaknak több célja is van. Egyrészt, hogy a tesztelő apparátus megismerje magát a terméket és annak működési sajátosságait, egyértelművé váljon, hogy a vállalat szempontjából a rendszer mennyire hasznos, milyen információk nyerhetők ki belőle, és azok mennyire segítik az üzemeltetést, illetve a security munkáját. Másrészt annak vizsgálata, hogyan lehet használni és működtetni a rendszert, milyen erőforrások szükségesek a hosszútávú működtetéshez, esetlegesen milyen folyamatokat kell szabályozni, illetve a működtetés a cégcsoport struktúrájába hogyan illeszthető be a leghatékonyabban. A tesztelő apparátus tagjai között én magam is helyet kaptam, így aktívan részt vehetek az egy évig tartó folyamatos tesztelésben együttműködve a tesztrendszer üzemeltetését ellátó szervezeti egységekkel. A teszt időszak természetesen kiértékeléssel fog zárulni, melyben szintén részt veszek majd.

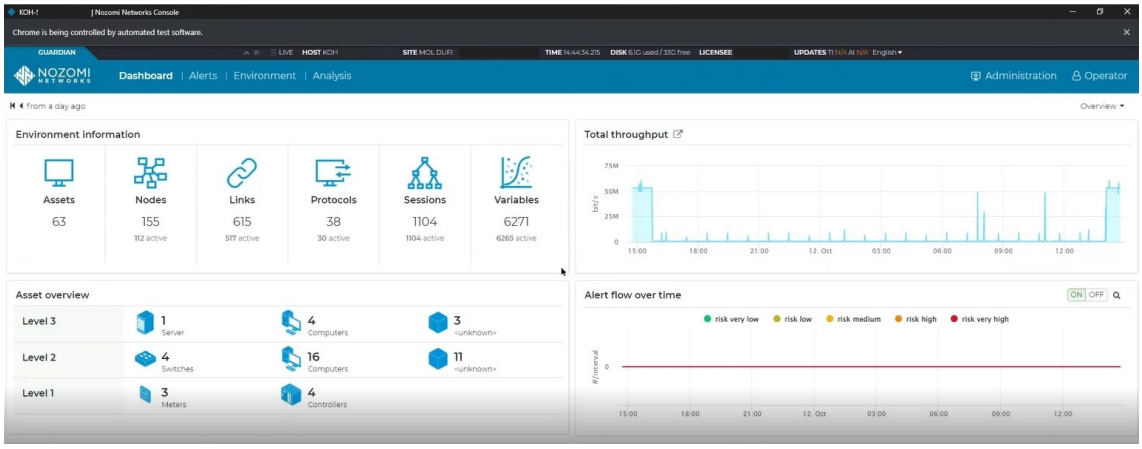
A teszt rendszer a MOL-csoporton beül, a százhalombattai Dunai Kőolajfinomítóban került telepítésre. A megvalósított implementáció az előzetes tervek szerinti, a Honeywell eszköz biztosítja a szükséges hálózati forgalmat, ami egy általa preferált és telepített Packet Brokertől érkezik a OT (Operation Technology) rendszerbe.

A rendszer jelenleg tanulási fázisban működik, de már jelenlegi formájában is képes szignatúra alapon a megváltozott forgalmi mintákat felismerni és a támadást megakadályozni. Képes OT területen értelmezni az ipari protokollokat, feltérképezi a hálózatot, észleli az ott lévő eszközöket, azokról információkat ad, valamint sérülékenységi információt ad a hálózatban található eszközökről. Vizualizációs felületén látható, hogy egyes eszközök hogyan kapcsolódnak egymáshoz, az eszközök, rendszer-elemek hogyan kommunikálnak egymással. Viselkedés alapú feltérképezéssel folyamatosan felügyeli a hálózati kommunikációt, ha eltérést tapasztal a megszokottól riasztást generál. A tesztelési folyamatban érintett résztvevőknek, így nekem is, a rendszer tanulási fázisában a Nozomi által a részlegesen, vagy tévesen felismert eszközök elnevezését megfelelőre módosítani szükséges a beazonosíthatóság érdekében. A megjelenő riasztások elemzésére is ebben a fázisban kerül sor. Fontos megtanítani a rendszernek, hogy melyek a valós riasztások és melyek a tévesek. Ezen túl a tesztelő apparátussal feladatunk még a naplóelemzés, az adatforgalomelemzés, esetleges adatszivárgások felismerése, a hálózatban található eszközök frissítése lekövetésének ellenőrzése. Mindezen feladatok szoros együttműködést kívánnak meg a

tesztelő apparátustól és a Nozomi supportját biztosító partnertől.

A teszt üzemeltetési időszak alatt elvárás a megvalósított ipari hálózat védelmét ellátó rendszerrel szemben, hogy detektálja, megelőzze és megvédje a hálózatban található informatikai és folyamatirányító eszközöket az esetleges információbiztonsági incidensektől. A rendszer üzemeltetői részére folyamatos információt adjon a hálózati eszközök állapotáról.

Az alábbi képen egy alapképernyőt, tulajdonképpen egy gyors áttekintő ábrát lehet látni a kicsatolt adatok alapján, amely egy egynapos adattömegből generálódót.



13.1. ábra: Áttekintő (forrás: MOL Nyrt)

Az áttekintő tábla fontos információkat tartalmaz. Legfontosabb elemei:

Assets: megmutatja a teszt hálózatban található fizikai eszközök darabszámát.

Nodes: utal minden logikai entitásra, ami kommunikál ezen a hálózaton. Egy fizikai eszköznek lehet több logikai paramétere is, rendelkezhet több IP címmel, több MAC címmel is, és ez mind-mind egy-egy nodnak számít a hálózaton.

Protokoll: információt ad a Telnet, SSH (Secure Shell), tehát a hagyományos IT-s (Information Technology) protokollokról, illetve az OT (Operation Technology) és IoT-ról (Internet of Things) és természetesen az ipari protokollokról is. A közvetített információkból kinyerhetünk olyan hasznos adattartalmakat, mint például a regiszter értékek, amelyek közlekednek a hálózaton kiolvasás vagy írás során, például a modbus protokollon keresztül. Ezt a rendszer észreveszi és értelmezni tudja.

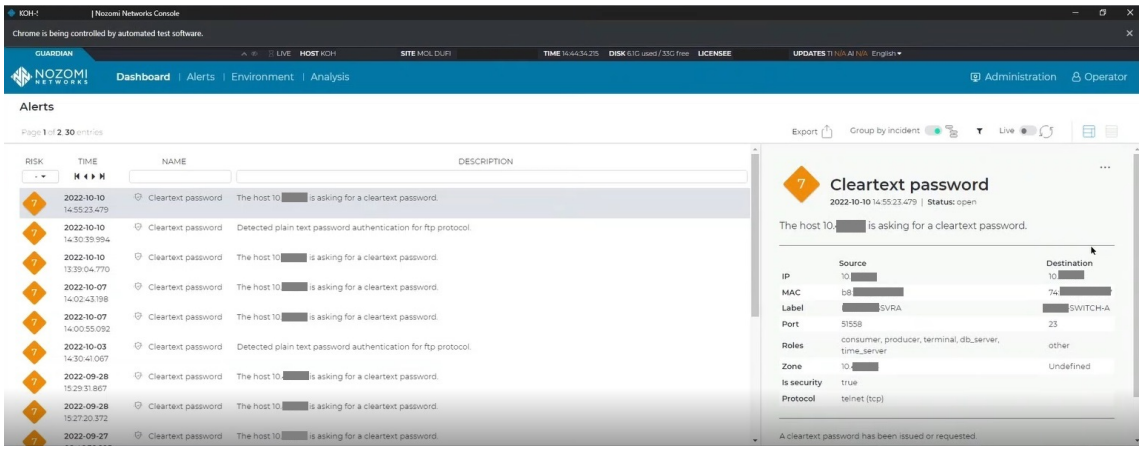
Asset overview: a guardian eszköz megpróbálja besorolni a hálózatban található eszközöket Level 1-2-3-ba, attól függően, hogy mennyire biztosan tudta beazonosítani ezeket

az eszközöket a guardianbe programozott különböző adatbázisok alapján. A guardien egy modulja az Asset Intelligenc, mely az adatbázis elemeit értékelve az egyes eszközök kommunikációjának jellemzője alapján meg tudja állapítani annak a konkrét eszköznek hardves szoftveres összetevőit, operációs rendszerét, különböző tulajdonságait. Ezeket felhasználva történik meg a hálózatban található eszközök besorolása Level 1-2-3-ba. Természetesen a besorolást szükség esetén kézzel felülírhatjuk.

Situational awareness: a rendszerben fellelhető potenciális kockázatkákról ad információt.

Latest alerts: a riasztásokról ad információt. A rendszernek van egy olyan adatbázisa, ahol a jelenleg publikusan elérhető összes káros kód, forgalom, támadási típus le van tárolva. Ha a rendszer hasonlót észlel, azt egy riasztás formájában jelzi. Jellegzetessége a rendszernek, hogy teljesen bizalmatlan a viszonyulása az ipari hálózathoz, tehát például az elavult protokollokat ebben az esetben egy 7-es riszálási értékkel jelenítette meg, amely a legmagasabb veszélyességi érték, mivel a besorolási skálája 0-7-ig terjed.

A következő ábrán látható, hogy a 7-es veszélyességi fokba sorolt kockázatról milyen riasztást ad az eszköz



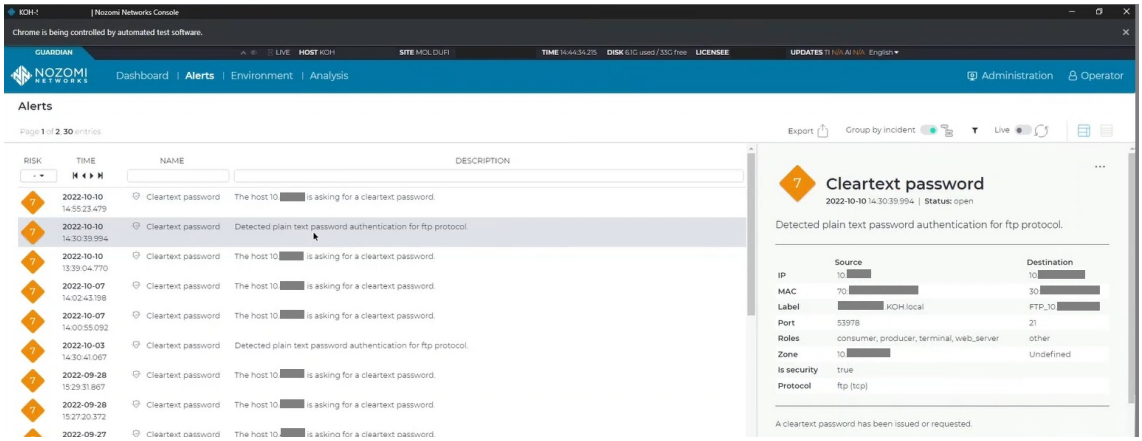
13.2. ábra: Telnet riasztás (forrás: MOL Nyrt)

A képen azt láthatjuk, hogy az SVRA kommunikálni szeretne a SWITCH A-val, eközben a jelszó nem titkosított formában halad keresztül a hálózaton. Ennek oka, hogy ez egy telnet protokoll, ami egy hálózati eszköz menedzselésére manapság már elavultnak számít. Valójában ez a kommunikáció egy belső szigetrendszerben zajlik, nem az interneten keresztül. Tehát potenciálisan nem tudja egy idegen visszakódolni azt a jelszót, ami ehhez a switchez tartozik, így nem jelent komolyabb, azonnali fenyegetettséget, de az eszköz által megjelenített protokoll mindenképpen kiemelt figyelmet kíván. Valójában az lenne az

optimális, ha telnet helyett SSH-t használnánk erre a kommunikációra, mert az tikosított formában szállítja az adatokat.

Ugyanezzel a ténnyel szembesültünk egy FTP (File Transfer Protocol) kommunikáció során, ahol az eszköz már nem csak ebben a zártsziget hálózatban kommunikál. Ugyanakkor ismert az üzemeltetés számára, hogy ez valójában az ipari hálózatnak a része, tehát egy ellenőrzött környezetben van, de végül is az FTP protokollra is igaz, hogy titkosítatlan formában utazik a jelszó, amin keresztül feltöltődnek az adatok a tárhelyre. Tulajdonképpen ez sem egy korszerű kommunikációs forma.

A rendszer tehát a fentieket detektálja és riasztást küld. A leni képen ezt láthatjuk:

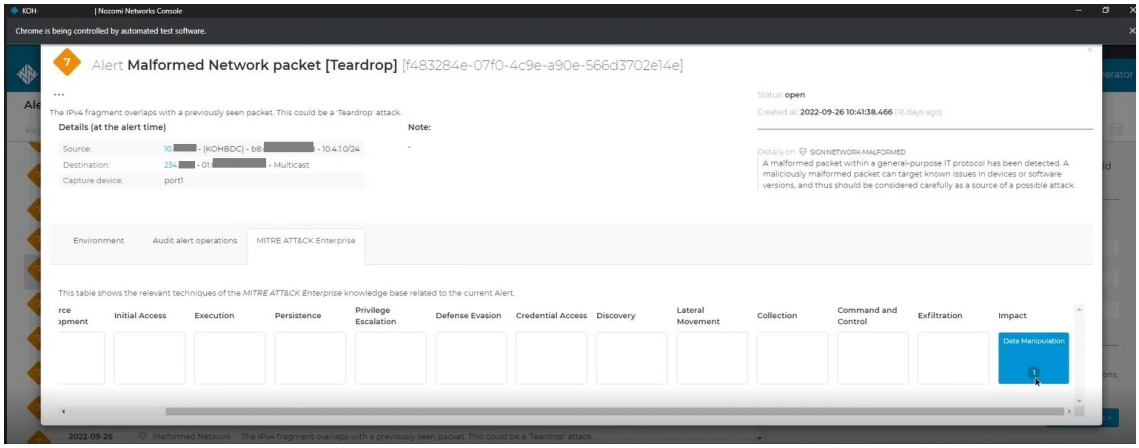


13.3. ábra: FTP riasztás (forrás: MOL Nyrt)

A tesztelés első hónapjában gyűjtött adatok értékelését követően elmondható, hogy nagy problémákat egyelőre nem tárt fel a rendszer. Az elején volt néhány érdekes riasztás, ami egyébként lehet a Honeywell rendszer sajátosága is. Ilyen például, hogy a rendszer packet tördelést észlelt, amit generálódhatott a kommunikációban beálló átmeneti zavarból, de akár lehetett egy bizonyos támadási típusnak a jele is. Az esemény további vizsgálatot igényel, mely már betervezésére került, de elmondható, hogy ebben az esetben is szerencse, hogy a kockázat a zárt szigetrendszeren belül történt, és nem interneten keresztüli, vagy zónák közötti kommunikáció vonatkozásában riasztott a rendszer.

A riasztások további jellemzője, hogy a riasztásról egy bővebb kifejtés is elérhető, ami arra vonatkozik, hogy konkrétan milyen veszélyt is jelenthet a fent említett veszélyességi skálán.

Az alábbi ábra bemutat egy további kockázati egy ilyen riasztási elemzést, amely egy adatmanipulációra utaló esetet jelenthet, melynél elképzelhető, hogy módosították a hálózati csomagot:



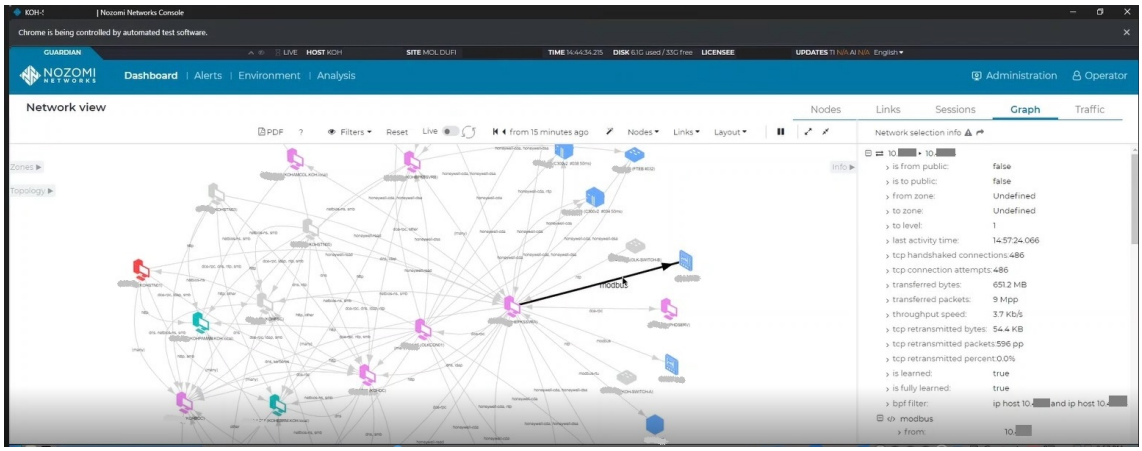
13.4. ábra: Riasztási elemzés (forrás: MOL Nyrt)

A fentieken túl a rendszer érdekessége, hogy az elmúlt időszak alatt gyűjtött adatok alapján a képes felrajzolni a hálózatban található egyes pc-ket, workstationokat. Ennek előnye, azon túl, hogy igen látványos, hogy ezeket egyesével megvizsgálhatjuk, bizonyos paramétereiket szükség szerint módosíthatjuk.

A rendszer tulajdonképpen egy pontos leltárt készít az érintett hálózatról, amelyben nem csak azt lehet látni, hogy vannak sziget-szerűen működő ipari rendszerek, de ezek tulajdonságai rejtve maradnak, hanem a Guardian segítségével felrajzolódik az is, hogy a hálózat konkrétan milyen eszközökből áll, hogyan és milyen irányokba, milyen protokollokon keresztül történik a kommunikáció, illetve, hogy ezek az eszközök jelentenek e veszélyt önmagukban a hálózat működésére.

A lenti képén a mintavételezés utolsó 15 percének adatát láthatjuk, ahol kijelöltünk egy hostot, amely vonatkozásában a rendszer megmutatja, hogy modbus protokollon keresztül kommunikál éppen. Gyakorlatilag bitszinten lebonthatók a két eszköz kommunikációjának elemei és jellemzői. Természetesen lehetőség van arra is, hogy ne csak jelen időben tudjuk ezt megtenni, hanem kijelölhetünk múltbeli időintervallumot is, annak adatait is elemezhetjük. Ennek előnye, hogy láthatóvá válik számunkra, hogy volt-e változás, vagy kommunikáltak-e más host-ok is esetleg.

Az összegyűjtött adatok alapján információt kapunk a hálózaton lévő minden egyes eszközről, arról, hogy az általa használt protokollok alapján milyen szerepe van a hálózatban. A használt protokollok a forgalmazott adatokkal együtt jeleníthetők meg. Egyesével felsorolásra kerülnek az eszköz hálózati kapcsolatai, kommunikációs mintázatai, az általa elért más eszközök, és a közvetített adatok.



13.5. ábra: Kommunikációs minta (forrás: MOL Nyrt)

14 TESZTELÉS ÉRTÉKELÉSE, A TÉNYLEGES MŰKÖDÉS ANTICIPÁCIÓJA

Ez alatt a közel két hónapos, de viszonylag még rövid működési időszak alatt a rendszer rávilágított arra, hogy üzemeltetési és security szempontból is fontos adatokat, hasznos információkat képes átadni a felügyeletet, a támogatást ellátó szakemberek részére. Összességében elmondható, hogy a rendszer teljesíti a feladatát, még az elvártakon felül is. Gondolok itt arra, hogy most először látjuk egyben a hálózat összes eszközét és ismerhetjük meg azok viselkedését. A technológia gyorsan és pontosan észleli a rosszindulatú és rendellenes tevékenységet. A rendszer már most olyan potenciális sérülékenységre hívta fel a figyelmet, ami eddig nem volt világosan, ennyire „kézzelfoghatóan" látható, de mindenképpen megoldást kell találni azokra. Idáig hallgatólagos hamis biztonságérzetett adhatott az a tény, hogy az ipari rendszerek eddig nem kommunikáltak az internet felé, de mára ez megváltozott.

Ugyanakkor szem előtt tartva, hogy egy ipari rendszerhez nem megfelelő behatolás detektáló, behatolást megelőző rendszer választása hasonló károkat okozhat, mint egy esetleges kiberbiztonsági incidens, megállapíthatjuk, hogy a Nozomi Guardian eszköz erős védelemnek bizonyul mind ipari, mint OT és mind IoT rendszerek felügyeletében a hálózat láthatóságának figyelemmel kisérésében.

Biztonsági szempontból képes a forgalmamat valós időben elemezni sérülékenységi szabályok, adatbázisok alapján. Gyakorlatilag mintákat keres, és a találatokat kritikusság alapján bekategorizálja 0-7 fokozatú skála-értékek között. Ezt követően a felhasználóra van bízva, hogy a találatokat kielemezve valósnak vagy false pozitívnak értékeli azokat. Gyakorlatilag az eszköz a natív adatforgalmat valós időben figyeli, a minták alapján elemezi, amit a Nozomi kiegészít viselkedés alapú minták vizsgálatával is. Az eszköz leíró adatbázisa tartalmazza modbusos kapcsolatnál a megfelelő adtaforgalom paraméterit, ha ahhoz képest eltérést észlel, azonnali jelzést generál.

A rendszer figyeli a különböző gyártók által használt protokollok forgalmát, ha valamely elem az adatbázisban felépített viselkedési mintával nem egyezik, riasztást küld arra vonatkozóan. Potenciális veszélyforrásként figyelmeztet az elavult protokollok használatára, mint például a telenet használata, ahogyan arra korábban már utaltam. A Nozomi segítségével mélyebben megismerhetjük, hogy egyes alkalmazások milyen protokollokat használnak, van-e közöttük olyan, amely nem a megengedett módon kommunikál.

A Nozomi további előnye, hogy részletes inventoryt tud készíteni, network mappel egyesítve. A rendszer egyesíti az eszközöket, vagyis felfedezés, hálózat vizualizáció, sebezhetőség-értékelés, kockázat figyelés és fenyegetés észlelés valósul meg egyetlen eszközben.

A rendszer segítségével rálátunk L2 és L3 eszközök teljes forgalmára, amelyek ismerete szintén kiemelt fontosságú lehet biztonsági szempontból. Ezek forgalmak eddig rejtve voltak, vagy nehezen voltak kinyerhetőek ezekre vonatkozó adatok.

A rendszer működési jellemzője, hogy a Packet Brokertől érkező adatokat már a Packet Brokerben elő lehet szűrni. Amit nem szeretnék elemezni, az kivehető belőle, mint például a biztonsági mentés, ami nagy adatforgalommal jár. Ezen túl a Packet Broker kiszűri a duplikált adatokat is.

A rendszer további előnye, hogy nem csak a biztonsági oldalon könnyíti meg a munkát, hanem felderíthetők vele mind szoftveres, mind hálózati kapcsolatból adódó anomáliák, vagy akár indokolatlan hálózati túlterhelés is.

A rendszer valójában kétféle üzemmódban tud működni, vagy csak detektál, vagy meg is szakítja forgalmat, megszüntetve a hálózati kapcsolatot. A tesz időszak alatt a kritikusság miatt egyelőre csak detektál a rendszer és riasztást küld. Ezt követően vizsgálni kell a problémát. Az eszköz segítségével viszont ki tudjuk bontani az adatokat, bele tudunk nézni az adatcsomagokba, így értékelhető a kockázat. A MOL-csoportnál a gyár és a termelés sajátossága a fokozott robbanásveszély, amely miatt kiemelt biztonsági kockázatú, ezért nem célszerű az eszközt úgy üzemeltetni, hogy a megszakítsa az adatforgalmakat, mivel ezzel termelési nehézséget, de adott esetben balesetet, vagy emberéletet veszélyeztető katasztrófát is generálhat.

A teszt időszak nem csak azért fontos, hogy az eszköz és a rendszer megismerhető legyen, láthatóvá váljanak az előnyei, hanem azért is, hogy kirajzolódjanak az egyes hibák, vagy a vállalat vonatkozásában az esetleges meg nem felelősségei is.

A tesztelés során máris látható, hogy figyelemmel kell kísérni, hogy ha esteleg történik egy nagyobb DCS frissítés és azt a Nozomi nem követi le, abban az esetben lehet, hogy újra kell tanítani a rendszert. További fontos elem, hogy ezek a rendszerek nem tudják az SSL bontást, a titkosított adatforgalmat nem tudják kibontani. Általánosan mondható, hogy hátránya ezeknek az eszközöknek az említett hiányosság, különösen annak ismeretében, hogy a mai világban a forgalmak nagy része valamilyen titkosított csatornán halad, igy a forgalom ezen része kieshet az ellenőrzésből. Erre a feladatra azonban vannak külön céleszközök, de a Nozomi önmagában ezt nem tudja. Figyelemmel kell lenni arra, hogy a hálózati forgalomban az SSL bontás nagymértékű késleltetést is jelenet, erre a fel-

adatra erős hardverre van szükség. Ha egy kártékony kód egy tikosított csatornán utazik két pont között, a csomag nem a két pont között fog kompromittálódni, hanem az elején vagy a végén ül rá a csomagra, és így eljut a célállomásra. Ha nincs olyan rendszer, ami ezt tudja detektálni, mert nem tud belenézni a titkosított csomagba, akkor ez a kockázat rejtve marad előttünk. Mindez természetesen csak akkor igaz, ha OT, IoT hálózatról van szó. Az ipari területen fő szabály szerint egyelőre az ipari protokollok (modbus) teljesen titkosítatlanok, így a Nozomi teljes mélységében látja azokat, és ezért a működése megfelelő a nagyipari hálózatra. A rendszer valójában teljesíti az elvárásunkat, hogy minden pillanatban tudjuk, mi történik az ipari hálózaton.

15 ÖSSZEFOGLALÓ

A fizikai védelem mellett mára kiemelten fontossá vált adataink, információink védelme. A kibervédelem különösen fontos az ipari területen, mivel a lehetséges kockázatok, okozott károk is jelentős mértékűek lehetnek személyi, baleseti, gazdasági és a MOL-csoport esetében nemzetbiztonsági okokból. A kibervédelem előkészítése és technikai műszaki megvalósítása az informatikai biztonsággal foglalkozó szakemberek feladata. Legyen az office vagy ipari hálózat, elsődleges cél az eszközök közötti adatcsere védelme, mivel legfontosabb tulajdon az adat. A védelem megvalósítása csak tűzfallal ma már nem elegendő. A biztonságos védelem kialakításhoz a tűzfal mellé célszerű üzembe helyezni egyéb határvédelmi eszközöket is, mint például IDS/IPS (Intrusion Detection / Intrusion Prevention), új generációs végpont védelmet ellátó eszközöket.[14] Ezek az eszközök az egyszerű szabályrendszerektől kezdve, a bonyolultabb viselkedés alapú vizsgálatokat használva védik a hálózattokat. Gondoskodni kell az adatszivárgás elleni védelemről is, ami biztosítja, hogy különböző csatornákon, adathordozókon ellenőrzés nélkül ne juthassanak illetéktelen kezekbe személyes vagy céges adatok. Bejelentkezéshez használt klasszikus felhasználó-jelszó páros könnyen törhető, kétfaktoros azonosítással történő kiegészítéssel viszont a biztonság növekszik. A privilegizált felhasználók adatinak tárolása, a belépéshez használt megfelelő erőségű jelszavak időszakos cseréje, kezelése, a kompromittálódás megakadályozása szintén kiemelt feladat az adatvédelem terén. A kiberbiztonság fontos része kell legyen az életünknek, a mindennapi tevékenységünkben, munkánk biztonságos elvégzésben a jövőben egyre fontosabb és kiemelt szerep jut neki. Ezt felismerve döntött a MOL-csoport vezetése arról, hogy a kibervédelmet kiemelten kell kezelni, és a kiberbiztonsági architektúra kezdeményezésére és vezetésével egy informatikai biztonságtechnológiai rendszer felállításáról döntött. A rendszer üzembehelyezése egy éves tesztidőszakot követően fog megtörténni. Szakdolgozatom írásáig beszerzésre kerültek a védelmet biztosító eszközök, szoftverek, valamint megkezdődött az egy évig tartó teszt időszak. A tesztidőszakból még csak közel két hónap telt el, de már így is sok előnye felrajzolódott a rendszernek. Láthatóvá vált, hogy az eszköz képes a hálózat valamennyi elemét jól megjeleníteni, adatokat szolgáltatni azokról, valamint képes gyorsan és pontosan értékelni a biztonsági kockázatokat, és azokról riasztást küldeni. A MOL-csoport produktív tevékenységi körének sajátosságai miatt a rendszer detektáló működése kiemelt fontosságú.

Szakdolgozatomat Stéphane Nappo nemzetközi információbiztonsági szakértő gondolatával zárom:

“A reputációd kiépítése 20 évbe telik, de az egészet lerombolhatja egy pár perces kiberbiztonsági incidens.”

16 SUMMARY OF IDEAS

Today, aside physical security, the protection of data and information has become especially important.

Cybersecurity is crucial in industrial environments, as possible risks and damages are of great personal, economic, and, in the case of MOL Group, national security concern. Preparation and technical realization of cybersecurity systems is the task of Information Security professionals. Be it an office or industrial network, the primary goal is the protection of data exchanged between devices, as information is a most important possession. By now, firewalls do not provide ample security. Additional defense measures, such as IDS/IPS (Intrusion Detection Systems / Intrusion Prevention Systems) and new-generation endpoint security devices have become an absolute necessity in maintaining network security. These devices provide protection in different ways, from simple rulesets to complex behavioral analysis. Preventing data breaches is necessary to insure no channels, or storage devices can be used to move personal or corporate data illicitly. The classic username-password pair method of identification is easy to crack, additional two-factor authentication should be used to increase security. Secure storage of privileged data, sufficiently strong login credentials, frequent changing and appropriate handling thereof, as well as taking steps to prevent their becoming compromised are all especially important for data protection.

Cybersecurity has to become an important part of our lives, practices and everyday work-activities, as its role only stands to become even more critical in the future.

Realizing this lead MOL Group decision makers to turn their attention to cybersecurity, and commission the creation of a new cybersecurity architecture and information security system. Use of the system will commence after a year-long test period. During the work on my thesis the acquisition of required devices and software was completed, and the test period began. Approximately two months of testing have passed, yet numerous advantages of the system have already become obvious. It has become evident that the devices are capable of visualizing and assessing all elements of the network, providing information about them, and quickly and accurately assessing security risks, as well as giving alerts of security events. Due to the nature of MOL Group's production activities, the detection capabilities of the system are of crucial importance.

I conclude my work with the words of the international Information Security expert, Stéphane Nappo:

"It takes 20 years to build a reputation, and a few minutes of cyber-incident to ruin it."

17 ÁBRAJEGYZÉK

18 IRODALOMJEGYZÉK

[1] „Elhíresült kibertámadások”. (), cím: https://www.kiberhaboru.hu/ (elérés dátuma 2022. 10. 27.).

[2] DDOS. „valós idejű térkép”. (2021. márc. 16.), cím: https://http://www.digitalattackmap.com/ (elérés dátuma 2022. 10. 27.).

[3] Kiberfenyegetés. „valós idejű térkép”. (), cím: https://cybermap.kaspersky.com/ (elérés dátuma 2022. 10. 27.).

[4] „Tűzfalak”. (), cím: https://tudasbazis.sulinet.hu/hu/szakkepzes/konnyuipar/informacio-es-adatgyujtes/halozati-alapfogalmak-eszkozok/tuzfalak-es-atjarok (elérés dátuma 2022. 10. 01.).

[5] IDS. „Intrusion Detection Systems”. (), cím: https://www.comodo.com/ids-in-security.php (elérés dátuma 2022. 10. 10.).

[6] *A novel network intrusion detection system*. Elsevier, 2022, utoljára megtekintve: 2022.10.01. DOI: 10.1016/j.compeleceng.2022.108455.

[7] IPS. „Intrusion Prevention System”. (), cím: https://www.comodo.com/intrusion-prevention-systems.php (elérés dátuma 2022. 10. 10.).

[8] „Demilitarizált zóna”. (2016. okt. 17.), cím: https://www.ionos.com/digitalguide/server/security/what-is-a-demilitarized-zone/ (elérés dátuma 2022. 10. 27.).

[9] A. S. Tanenbaum, C. András és C. Andrásné, *Számítógép-hálózatok*. Novotrade, 1992.

[10] SCADA. „SCADAfence Platform”. (), cím: https://www.scadafence.com/platform/ (elérés dátuma 2022. 10. 27.).

[11] Nozomi. „Nozomi Guardian”. (), cím: https://www.nozominetworks.com/products/guardian/ (elérés dátuma 2022. 10. 27.).

[12] „Claroty CTD”. (), cím: https://claroty.com/industrial-cybersecurity/ctd (elérés dátuma 2022. 10. 27.).

[13] „Ixia Vision”. (), cím: https://www.tempestns.com/ixia-vision-e40-e100-network-packet-brokers/ (elérés dátuma 2022. 10. 01.).

[14] *Digital Communications and Networks*. Elsevier, 2022, utoljára megtekintve: 2022.10.01. DOI: 10.1016/j.dcan.2022.05.027.