ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

BÁLINT FERENC

Kritikus infrastruktúrák, tömegtartózkodású objektumok, gépjárművek informatikailag megvalósítható védelme

Témavezető: Dr. Pető Richárd

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2025. 12. 31.

Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt Idézéséről

Alulírott **Bálint Ferenc** kijelentem, hogy a **Kritikus infrastruktúrák, tömegtartózkodású objektumok, gépjárművek informatikailag megvalósítható védelme** című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Budapest, 2025. december 31.

Bálint Ferenc

TARTALOMJEGYZÉK

BEVEZETÉS

A tudományos probléma megfogalmazás

A kritikus infrastruktúrák, tömegtartózkodású objektumok és járművek informatikailag megvalósítható védelme ma a biztonság- és rendszerszemléletű kutatás egyik legégetőbb gyakorlati és elméleti kihívása. Az elmúlt évtized digitalizációs lendülete, az ipari vezérlőrendszerek és épületfelügyeleti rendszerek hálózatba kapcsolódása, valamint a járművek egyre növekvő szoftver- és kommunikációs összetettsége új támadási felületeket hozott létre. Ezek a támadási felületek nem csak adatvédelmi vagy üzleti kockázatot jelentenek. A szolgáltatás folytonosság megszakadása, a fizikai rendszerhibák hatásai és a tömegek biztonságának veszélyeztetése közvetlen emberi és társadalmi következményekkel járhat.

A probléma első szintje a rendszerek heterogenitásából fakad. Kritikus infrastruktúrák, mint repülőterek, bank épületek, energia-, víz-, közlekedési és kommunikációs rendszerek, tömegtartózkodású épületek, stadionok, konferenciaközpontok, közlekedési-csomópontok, és járművek (beleértve a közúti, vasúti és autonóm járműveket) különböző tervezési elveket, üzemeltetési gyakorlatokat és biztonsági követelményeket hordoznak. Ez a heterogenitás eredményezi a szabványok, protokollok és biztonsági megoldások széttagoltságát, ami megnehezíti a skálázható védelmi architektúrák kidolgozását. Emellett a kereskedelmi és nyílt protokollok használata növeli a támadhatóságot, mivel a támadó által ismert feltörési mintázatok könnyebben átvihetők egy-egy szektorból a másikba.

A második szint a kockázatok összefüggő viselkedésének modellezése. Egy kritikus komponens meghibásodása nemcsak lokális kiesést okozhat, hanem láncreakciót indíthat el, amely más rendszerek működését is befolyásolja. Ezen hatások valószínűségének és következményeinek komplexitása, valós idejű megfigyelést és a rendszerek közötti kölcsönhatások mélyebb megértését igényli. A jelenlegi gyakorlatban alkalmazott, kockázatmodellek ritkán képesek megragadni az ilyen sokrétű kölcsönhatásokat, ami alacsony hatékonyságú beavatkozási stratégiákhoz és alul- vagy túlbiztosításhoz vezethet.

A harmadik szint a detektálás és reakció valós idejű képességeivel kapcsolatos. A hálózatba kötött rendszerek folyamatos adatfolyamot biztosítanak, amely lehetővé teszi az anomáliák gyors felismerését és automatikus reagálást. Gyakorlatban azonban az anomália észlelés megbízhatóságát rontja az adatminőség, a rendszerek közötti

különbségek és a hamis-riasztások. Az automatizált reagálás bevezetése szervezeti és jogi korlátokba ütközhet, különösen olyan döntések esetében, amelyek befolyásolják az emberi életet vagy kritikus szolgáltatások elérhetőségét. Ebből következik az igény hibrid megoldásokra, amelyek kombinálják a mesterséges intelligencia (MI) gépi gyorsaságot és a humán döntési kontrollt.

A negyedik szint, gyakran alul reprezentált aspektus az emberi és szervezeti tényezők integrálása. A műszaki megoldások bevezetése és fenntartása függ a szervezeti kultúrától, az üzemeltetői gyakorlatoktól, a jogi megfelelőségtől és a költséghaszon elvárásoktól. Egy technológia akkor lesz sikeres, ha az megfelel az üzemeltetők képességeinek, a fenntartás finanszírozhatóságának és jogi kereteknek.

A fentiek alapján a központi tudományos probléma így fogalmazható meg: hogyan lehet kidolgozni és demonstrálni egy integrált, többrétegű informatikai védelmi keretrendszert, amely skálázhatóan alkalmazható kritikus infrastruktúrákban, ezen belül a bankszektorban, repülőtereken, csökkentve a támadások és meghibásodások által kiváltott hatásokat, biztosítva a valós idejű detektálást, és egyben figyelembe véve az emberi, szervezeti és jogi korlátokat.

A módszertani megközelítés széles eszköztárat igényel: rendszerszintű modellezés és elemzés, a detektálás pontosságának és megbízhatóságának növelése, valamint digitális környezeti megoldások validálása. Kiegészítőleg szakértői, üzemeltetői szempontok igénybevétele, ami biztosítja, hogy a javasolt megoldások bevezethetőek és fenntarthatóak legyenek a gyakorlatban.

A kutatás várható hozzájárulásai elméleti és gyakorlati szinten is jelentősek lehetnek: hozzájárulás a kritikus rendszerek biztonsági elméletéhez egy egységes, hatásokra érzékeny modell formájában; architektúra és bevezetési iránymutatók, amelyek segítik az üzemeltetőket a védelmi beruházások priorizálásában; továbbá demonstrált anomália-észlelési és reagálási sémák, amelyek csökkentik a szolgáltatás-kiesések és fizikai károk valószínűségét. Összességében a kutatás olyan tudományos és gyakorlati alapot tervez létrehozni, amely növeli a társadalom ellenálló képességét a digitálisan összekapcsolt kritikus rendszerek fenyegetéseivel szemben.

Célkitűzések

A kutatás kiemelt célkitűzése az integrált, többrétegű informatikai védelmi keretrendszert összekötni a mesterséges intelligencia (MI) alkalmazási lehetőségeinek feltárása a kritikus infrastruktúrák informatikai védelmében. Az MI-alapú rendszerek képesek a nagymennyiségű adat valós idejű feldolgozására, az anomáliák automatikus felismerésére, valamint prediktív modellek kialakítására, amelyek előre jelezhetik a potenciális fenyegetéseket. A kutatás célja olyan MI és humán technikák azonosítása, amelyek hatékonyan alkalmazhatók a különböző védelmi szcenáriókban, különösen a viselkedésalapú támadásdetektálás, a hozzáférési mintázatok vizsgálata terén.

A kutatás további célja a kibertámadások elleni védekezési stratégiák rendszerezése és megvizsgálása, különös tekintettel a célzott támadások (targeted attacks), a szolgáltatás megtagadásos támadások (Distributed Denial of Service, továbbiakban: DDoS), valamint az ellátási láncokat érintő illegális pénzügyi tevékenységek elleni fenyegetések kezelése. A cél olyan védelmi mechanizmusok azonosítása, amelyek képesek a támadások, csalások korai felismerésére, az incidensek hatékony izolálására, valamint a rendszer-funkciók gyors helyreállítására. A kutatás során vizsgálatra kerülnek a kiberbiztonsági kérdések, valamint az automatizált monitorozó rendszerek elemzése, amelyek lehetővé teszik a gyors és célzott reakciót a különböző támadástípusokra.

Az MI integrálása a védelmi rendszerekbe nem csupán technológiai előrelépést jelent, hanem új biztonságpolitikai és etikai kérdéseket is felvet. A kutatás célja annak feltárása, hogy az MI-alapú döntéshozatal milyen mértékben képes támogatni az emberi oldalt, illetve milyen kockázatokat hordoz az autonóm válaszmechanizmusok alkalmazása. A cél egy olyan keretrendszer kialakítása, amely biztosítja az MI-rendszerek átláthatóságát, auditálhatóságát és felelősségi viszonyait a biztonsági infrastruktúrákban.

A kutatás gyakorlati célkitűzései közé tartozik továbbá MI-alapú védelmi megoldások hatékonyságának vizsgálata. Lehetőség nyílik a védelmi stratégiák finomhangolására, valamint a technológiai és szervezeti válaszlépések optimalizálására. A cél, hogy a kutatás hozzájáruljon egy olyan adaptív és intelligens védelmi modell kidolgozásához, amely képes alkalmazkodni a folyamatosan változó fenyegetési környezethez, és támogatja a biztonságpolitikai döntéshozatalt a kritikus rendszerek védelmében.

A téma kutatásának hipotézisei

A hipotézis, hogy a kritikus infrastruktúrák informatikai védelmének hatékonysága lényegesen növelhető egy integrált, többdimenziós megközelítéssel, amely egyszerre ötvözi a Mobil eszköz menedzsment (Mobile Device Management, továbbiakban: MDM) rendszerek és mesterséges intelligencia (MI) eszközeit, a pénzmosási kockázatok azonnali és proaktív figyelembevételét, valós idejű monitoring és reagálási stratégiákat. MI-alapú anomália- és viselkedéselemzés, valamint fenntartható, üzemeltetési irányok figyelembevétele elengedhetetlen. Ennek általános vetületei négy konkrét, vizsgálatra alkalmas hipotézisként fogalmazhatók meg.

Első hipotézis: A kibertámadások elleni védekezésből eredő rendszerüzemeltetési megközelítések vizsgálata — különös tekintettel az globális trendekre, megfelelő rendszer komponensekre és szolgáltatás alapú üzemeltetési stratégiákra — növelheti a védelmi intézkedések hosszútávú hatékonyságát.

Második hipotézis: A pénzmosási kockázatok és következmények beépítése a kritikus infrastruktúra informatikai védelmi architektúrájába csökkentheti az üzleti folyamatok manipulációjából eredő szolgáltatásmegtagadási kockázatokat.

Harmadik hipotézis: A valós idejű monitoring és reagálási stratégia, amely MI-t használ anomália detektálásra és automatizált reagálásra, jelentősen csökkentheti a támadás felfedezési és reakcióidőt, ezáltal csökkentve a károkat, minimalizálva a szolgáltatás-kiesés valószínűségét kritikus infrastruktúrák esetében.

Negyedik hipotézis: Az MDM rendszerek és MI integrációja jelentősen csökkentheti a mobil eszközökről eredő adatszivárgást, jogosulatlan hozzáférést, manipuláció kockázatát kritikus környezetekben.

Kutatási módszerek

A kutatás módszertana vegyes eljárás, egymásra épülő lépések sorozataként értelmezendő, amely egyszerre szolgál elméleti modellezést, adatvezérelt monitoring és MI integrációt. Fontos szempont a rendszerszintű architektúra-tervezés, valamint kvalitatív és kvantitatív módszerek alkalmazása. Elméleti részben szakirodalmi elemzés

történik a kritikus infrastruktúra védelem kereteiről, az MDM rendszerek képességeiről, MI algoritmusok anomália detektálási mintáiról, valamint a pénzmosás elleni rendszerek és kontrollok informatikai vetületeiről.

A megközelítés alapelvei: 1) a kibertámadások központi szerepe, 2) az MI mint döntéstámogató és anomália-észlelő réteg, 3) az MDM mint végpontbiztonsági és szabályozó komponens, valamint 4) emberi felügyelet és rendszerüzemeltetési szemlélet. A módszertan célja demonstrálni, hogy a fenti elemek kombinációja javítja a detektálás korai fázisát, csökkenti a hamis riasztásokat, és mérsékelheti a kaszkádhatásokból eredő szolgáltatáskieséseket.

A stratégia megalkotása nagyon fontos. A kísérleti rész két pillérre épül. Az első pillér a szimulációs vizsgálatok: egy reprezentatív, moduláris tesztkörnyezet kialakítása, amely tartalmaz valós MDM-kompatibilis klienseket, konténerizált szolgáltatásokat kritikus alkalmazások szimulációjára, hálózati forgalmat előállító modulokat és loggenerátorokat, valamint MI modelleket futtató feldolgozó egységeket. E környezet lehetővé teszi különböző támadási szcenáriók, belső visszaélések, anomáliák és pénzügyi visszaélési események detektálását. A célja az arányok, hamis-pozitív riasztások, és a reakcióidők elemzése MDM+MI konfigurációk és hagyományos kontrollok között. Különféle forrásokat tudunk a rendszerbe integrálni: hálózati és rendszerlogok, ipari vezérlőrendszerek, épületfelügyeleti rendszerek adatai, járművek jelzései, valamint mobil eszközök és végpontok MDM-mel gyűjtött metaadatai. Az adatok, logok feldolgozása során hangsúlyt kap az adatok időbeli szinkronizálása, formátumok egységesítése: incidensek és normál működés közötti határok kialakítása. Az adatvédelmi követelményeknek való megfelelés biztosítása érdekében érdemes bevezetni aggregálási mechanizmusokat, valamint auditált hozzáféréskezelést.

A modellarchitektúra hibrid: a gyors, szabályalapú szűrőréteg csökkenti a zajt és szűri a könnyen azonosítható ismert mintázatokat; ezt követi egy gépi tanuláson alapuló algoritmus, amely idősorelemzést, viselkedésalapú jellemzőket és hálózati gráf-topológiát egyesít. A skálázhatóság és a mintázatok felismerése indokolja, hogy minden kritikus riasztás mellé magyarázható változót generálunk MI technikákkal az operátori elfogadottság és auditálhatóság érdekében. A tanulási protokoll offline előtanítást és online folyamatos finomhangolást igényel: a kezdeti modelleket adatokon keresztül figyeljük, majd egyes környezetekből érkező valós telemetria alapján folyamatosan adaptáljuk, miközben modellkalibrációt alkalmazunk.

A másik komponens a monitorozási architektúra és MDM integráció: a rendszer több rétegből álló monitoringsémát használ, ahol helyi előfeldolgozást és gyors, alacsony késleltetésű riasztást biztosít; a központi réteg végzi a mélyebb MI-analitikát, és a reagálási logika végrehajtását; az MDM réteg pedig a mobil és IoT végpontok konfigurációs szabályozását, patch-kezelését, titkosítás és távoli zárolás funkcióit biztosítja. Az MDM-ből származó metaadatok (pl. eszköz státusz állapota, telepített szoftververziók, biztonsági szintek) valós időben táplálják az MI-detektort, így a riasztások pontossága javul. Emellett az MDM lehetőséget ad a gyors hozzáféréshez policy-alapú automatikus vagy humán beavatkozásra így az izolációra: bizonyos kockázati küszöbök felett a rendszeren keresztül képesek vagyunk távoli beavatkozásokat végrehajtani pl.: karanténba helyezni egyes végpontokat, lekapcsolni hálózati interfészeket vagy alkalmazásokat tiltani, mindezt előre meghatározott, ember által felülvizsgált forgatókönyvek szerint.

A szimulációs vizsgálat modellek segítségével elemzi a kaszkádhatásokat és a javasolt reagálási sémák rendszer-szintű hatását különböző támadási lehetőségeken keresztül. Itt mérhető a kaszkádszélesség, kiesési idő és a szolgáltatás-helyreállítási költség. A korlátozott számú kritikus eszköz, épületfelügyeleti komponens és mobil végpont kerül bevonásra üzemeltető területeknél. Metrikákat gyűjtünk: detektálási arány, hamis pozitív arány, riasztástól reagálásig eltelt idő, automatikus izolációk száma és sikeressége, valamint a kaszkádhatás mérséklésének mértéke. Üzemeltetői pontok meghatározása, használhatósági megfigyelések.

A módszertan fontos eleme a kísérleti protokoll formális tervezése: minden tesztszcenárió kiindulási állapotokkal rendelkezik, továbbá rollback mechanizmusokkal a rendszerek védelme érdekében. A konténerizált komponenseket és szimulációs paramétereket dokumentáljuk. Az elemzés statisztikai módszereket alkalmaz a teljesítménykülönbségek megítélésére.

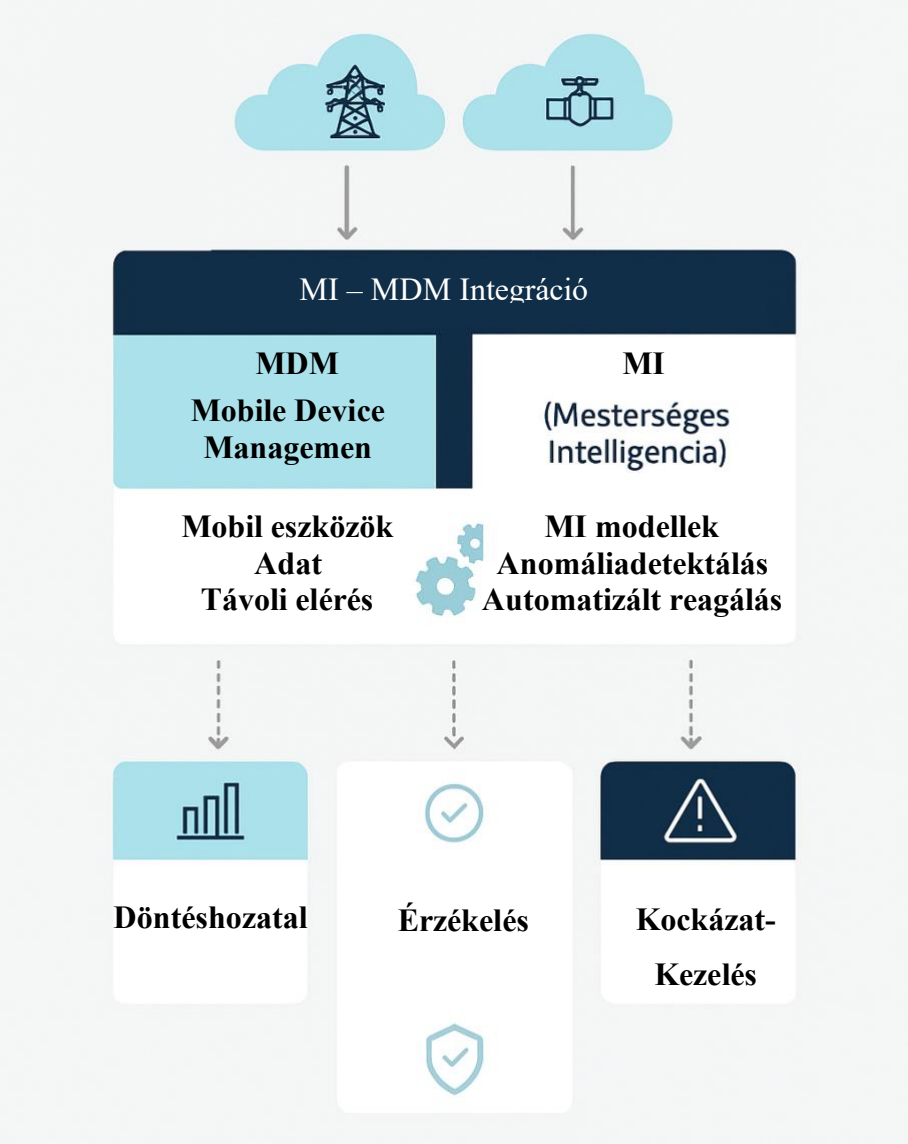
Szervezeti és jogi aspektusok módszertani integrációja során az MI döntéshozatali logikák átláthatóak és auditálhatóak legyenek, és hogy az MDM politikák megfeleljenek adatvédelmi előírásoknak. Etikai kontrollként bevezetjük az emberi felülvizsgálatot minden kritikus automatizált beavatkozásnál, valamint rendszeres auditokat az MI-modelleken.

A várható eredmények bizonyítják, hogy az MI-vezérelt monitorozás és MDM által támogatott végpontmenedzsment együttes alkalmazása csökkenti a detektálási késleltetést, javítja a riasztások pontosságát és mérsékli a kaszkádhatásokat. A

módszertan iteratív: a pilotok tapasztalatai visszaforgathatók a modellfejlesztésbe és a policy-k finomhangolásába, így a kutatás nemcsak elméleti hozzájárulást, hanem gyakorlati, bevezethető megoldást is ad a kritikus rendszerek védelméhez.

A fenti módszertan célzottan ötvözi az MI-modellezés elemeit, a valós idejű monitorozás gyakorlati architektúráját és az MDM által nyújtott végpontkontrollt. A kombinált kísérleti és szimulációs validáció biztosítja, hogy a javasolt megoldások mind technikailag megalapozottak, mind a szervezeti bevezetés szempontjából kivitelezhetőek legyenek.

Folyamatábra: **Az MI és MDM integrálása a kritikus infrastruktúrákban**



1. ábra: MI és MDM integrálás

Egyéni munkaterv bemutatása

A négy felsorolt hipotézis validálása, ami magában foglalja a kritikus infrastruktúrák biztonságának növelése érdekében egymással szorosan összefonódó célok megoldását, együttesen képezik a vizsgálati keretrendszer alapját.

Az értekezés négy fejezete, ami feldolgozza a következőket:

- *1. Kiberbiztonsággal kapcsolatos globális trendek*

Legfontosabb kiberbiztonsági fenyegetések ismertetése.
Fenyegetések forrásai, gyakorlatok alkalmazása.

- *2. Pénzmosási kockázatok*

A hatások becslésére szolgáló fogalmak és kockázatok ismertetése.
A kritikus infrastruktúrák ellátási láncaiban és szolgáltatási ökoszisztémáiban a pénzügyi tranzakciók nem csupán gazdasági események, hanem potenciális visszaélési felületek, amelyek közvetetten csökkenthetik egy szervezet kibervédelmi képességét, ami súlyos társadalmi és gazdasági következményeket okozhat.

- *3. Valós idejű monitorozási és reagálási stratégiák*

Monitoring rendszerek ismertetése és azok felhasználási területe.
• Infrastruktúraelemek főbb monitoring eszközei
• Modellek alkalmazása a lehetséges eseményláncokra és azok hatásaira.

- *4. Mobil eszközök szerepe MDM környezetben*

Az MDM rendszerek hagyományos szerepe az eszközkonfigurációk érvényesítése, szoftverfrissítések kezelése és alapvető távoli vezérlési funkciók biztosítása. Kritikus rendszerek esetében azonban az eszközök nem csupán informatikai végpontok, hanem működési folyamatok részei, amelyek pontról pontra hatnak a szolgáltatásbiztonságra.

MDM architektúra
A vizsgálat egy kialakított tesztkörnyezetben történik. A cél, hogy a rendszerek skálázhatóak, monitorozhatóak és biztonságosak legyenek, lehetővé téve különböző

infrastruktúra-típusokhoz való illesztést. A cél egy olyan architektúra formalizálása, amely modulárisan integrálja a következő komponenseket:

• Érzékelési réteg: fizikai és logikai szenzorok, amelyek valós idejű adatokat gyűjtenek a rendszer állapotáról (pl. hálózati forgalom, tűzfal, fizikai hozzáférés, környezeti paraméterek).

• Hálózati és irányítási logika: az adatok előfeldolgozása és továbbítása, valamint az automatizált döntési mechanizmusok (pl. szabályalapú vagy gépi tanuláson alapuló vezérlés).

• Felügyeleti monitoring interfészek: vizualizációs és beavatkozási felületek, amelyek lehetővé teszik az üzemeltetők számára az állapotmonitorozást és az eseményekre való reagálást és a különböző konfigurációk ellenőrzését.

Létrehoztam egy MDM teszt környezetet és integráltam:

• Létrehoztam egy MDM tesztkörnyezet, amely biztonságos terepet ad az eszközök és telepítések kipróbálásához.

• A rendszer integrációja során szolgáltatásokat és hálózati erőforrásokat összekapcsoltam, hogy a tesztelés valós működési feltételeket tükrözzön.

• A környezeten lehetővé tettem az eszközregisztrációt, konfigurációs elemeket, alkalmazáskezelést és biztonsági szabályok tesztelését, kockázatmentes módon.

Továbbá az alábbi szempontok elemzését tartalmazza:

• Észlelési pontok definiálása: érzékenység, pontosság, hamis riasztások kiszűrése.

• Monitoring hatékonysága: válaszidő, rendszerstabilitás, riasztási képesség.

• Üzemeltetői kompetencia: MI használhatósága, üzemeltetői képesség, képzési igény.

• Adatkezelési előírások, felelősségi kérdések, auditálhatóság.

• Következménybecslés: szolgáltatás-kiesés időtartama, gazdasági veszteség, kulcs teljesítménymutató (Key Performance Indicator, továbbiakban: KPI).

A munka befejezésének időpontja: 2025. december 31.

1 A KIBERBIZTONSÁGI TUDATOSSÁG

A fejezetben ismertetem a kutatás szempontjából releváns információkat. Először a sérülékenység és a kockázatok jelentőségére hívom fel a figyelmet, majd a mesterséges intelligencia térnyerését fejtem ki, kiemelve a monitoring jelentőségét a kockázatok szerepét.

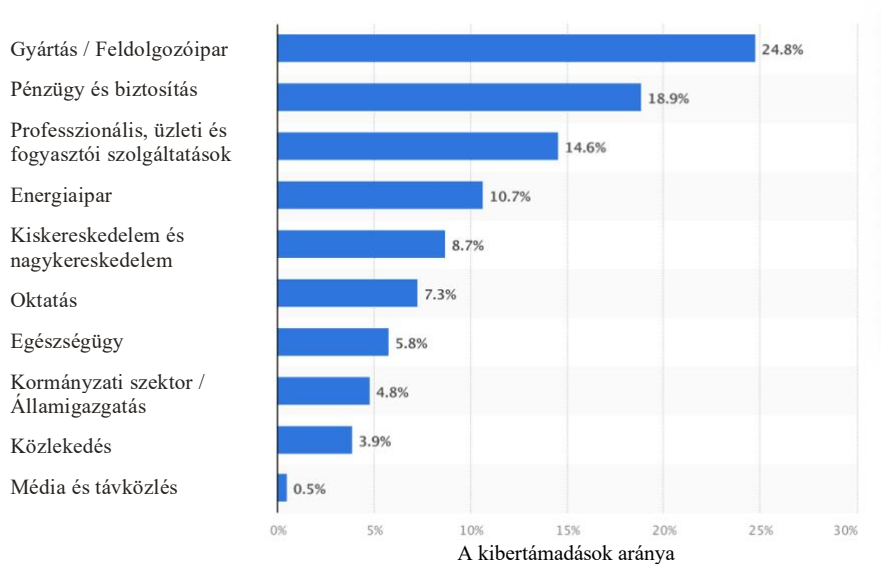
1.1 Globális trendek

A mai digitális világban a technológia különböző ágazatokba való integrálása óriási hatékonyságot biztosít. Ezekkel a fejlődésekkel azonban elkerülhetetlenül új kockázatok és kihívások is megjelennek. A digitális átalakulást tovább gyorsította a COVID-19 világjárvány. Rosszindulatú szereplők ki tudják használni ezt a digitális átalakulást, és komoly fenyegetést jelentenek a globális pénzügyi rendszerre, a pénzügyi stabilitásra és a pénzügyi ipar integritásába vetett bizalomra. A kiberbiztonsági helyzet egyértelmű növekedést mutat a támadások számában, miközben sok vállalat nincs megfelelő erőforrásokkal ellátva e fenyegetések kivédésére. A felhasználók többsége vagy nem kap vagy a költségekre hivatkozva nehezen kapott megfelelő oktatást, és olyan viselkedést folytat, amely kockázatot jelent a szervezet számára. A kiberbiztonsági tudatosság elsődleges fontosságú, például, ha a felhasználók többsége jelszavakat újra felhasznál és könnyen kitalálható kifejezéseket alkalmaz. Az emberi hiba továbbra is az adatszivárgások fő oka, ami aláhúzza az oktatás jelentőségét ezen könnyen megelőzhető probléma kezelésében. A kibertámadások anyagi veszteségekhez, reputációs károkhoz és működési zavarral járó következményekhez vezetnek; a vállalkozásoknak jelentős helyreállítási költségekkel és esetleges szabályozói bírságokkal kell szembenézniük. A kiberfenyegetések mérsékléséhez elengedhetetlen a robusztus kiberbiztonsági intézkedések, mint az erős jelszavak, a rendszeres szoftverfrissítések, a hálózatbiztonsági megoldások és az incidensreagálási tervek bevezetése. A kiberbiztonsági szakemberek kulcsszerepet játszanak a lehetséges fenyegetések azonosításában, a védekezési stratégiák kidolgozásában és a védelmi technológiák bevezetésében. Emellett a kormányok, szervezetek és kiberbiztonsági szakértők közötti együttműködés elengedhetetlen a globális kiberbiztonsági kihívások kezelése és az új fenyegetések hatékony mérséklése érdekében. Összességében a kiberfenyegetési környezet megértése és a védelmi intézkedések bevezetése alapvető a kibertámadások elleni védelemhez. [1]

A kiberbiztonság a számítógépes információs rendszerek, hardver, hálózat és adatok védelmének gyakorlata a kibertámadásokkal szemben. A kiberfenyegetésekről növekvő tudatosság világszerte emelkedő beruházásokhoz vezet a kiberbiztonsági infrastruktúrában. A digitális transzformáció a COVID-19 pandémia következtében elkerülhetetlenül új kiberbiztonsági fenyegetéseket hozott magával. A digitális átállással párhuzamosan várhatóan nő a kibertérben elkövetett csalások száma. Az igazgatásoknak fel kell készülniük az egyes ágazatok sérülékenységeire, hogy elkerüljenek bármilyen jelentős pénzügyi válságot. A megelőző és felderítő kontrollok fontossága mellett szükséges az együttműködés erősítése az egyes ágazatok és szereplők között, hazai és nemzetközi szinten egyaránt. Átfogó kiberbiztonsági megoldásokat kell alkalmazni a fejlődő fenyegetésekkel szemben. A digitális rendszerek ellenállóképességének növelése új szabályozói követelmények által is indokolt. Megfelelő kiberbiztonsági szakértelem, működési kockázatkezelés, harmadik féltől származó kockázatértékelések, belső kontrollok és kockázatkezelés elengedhetetlen elemei a kiberreziliencia építésének. A fenyegetési környezetbe egyre kifinomultabb mesterséges intelligencia technikák lépnek be, mint az előrehaladott adathalász kampányok és a deepfake-ek, amelyekre a szervezeteknek fel kell készülniük. A kiberbiztonsági szakemberek növelték a mesterséges intelligencia alkalmazását a kibertámadások felismerésében és megelőzésében. [2]

1.1.1 Ágazatonkénti elosztás

2022-ben a gyártóipar volt a legnagyobb részaránnyal rendelkező ágazat a világ vezető iparágai között a kibertámadások tekintetében, az összes támadás közel negyedét adva. A pénzügyi és biztosítási szervezetek követték őket, mintegy 19%-os aránnyal. A professzionális, üzleti és fogyasztói szolgáltatások harmadik helyen álltak, körülbelül 14,6%-kal. Ezek az eredmények kiemelik a szervezetek számára a különböző kiberbiztonsági kihívásokat és a robusztus védekezési intézkedések szükségességét. [3]



2. ábra: Támadások ágazatonkénti eloszlása

1.1.2 A világ legjelentősebb kiberbiztonsági fenyegetései

Manapság világszerte végzett információbiztonsági vezetők (Chief Information Security Officer, továbbiakban: CISO) körében végzett felmérés szerint a legfontosabb kiberbiztonsági kockázatok a következők:

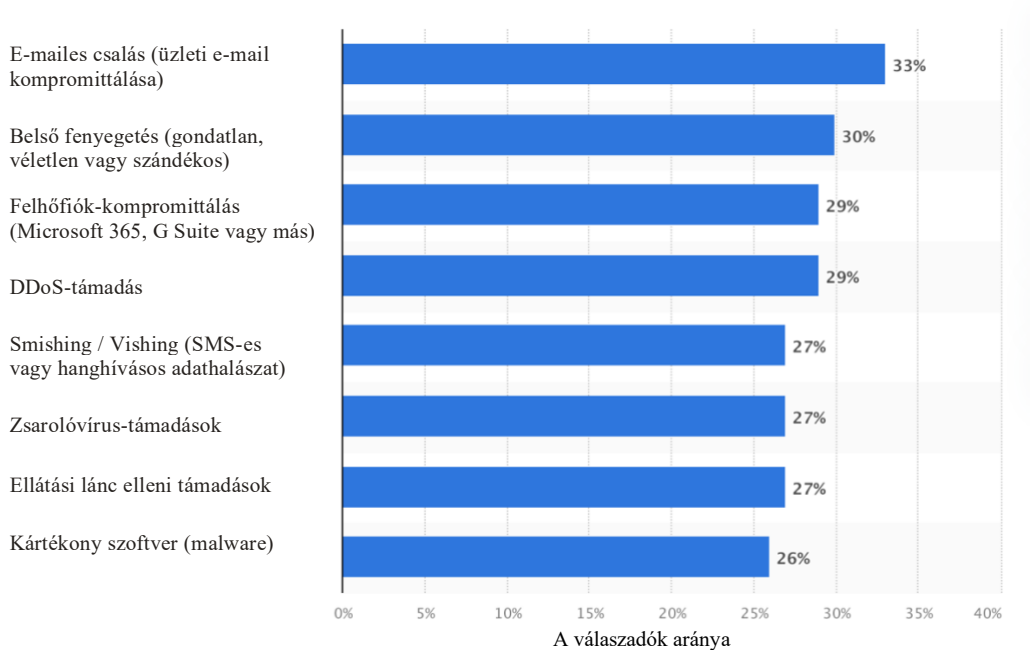
Email csalás: Az egyik legelterjedtebb, körülbelül 33%-a a csalásoknak az email-en elkövetett csalás. Ez a három legfontosabb kiberfenyegetés egyike. Az email csalás különféle rosszindulatú tevékenységeket foglal magában, például adathalász csalásokat és üzleti email kompromittálást, amelyek célja a személyek megtévesztése érzékeny információk kiadására vagy pénz átutalására.

Belső fenyegetések: A CISO-k mintegy 30%-a tartotta a belső fenyegetéseket jelentős kockázatnak a szervezetük kiberbiztonságára nézve. A belső fenyegetések alkalmazottaktól, vállalkozóktól vagy partnerektől származhatnak, akik hozzáféréssel rendelkeznek érzékeny adatokhoz vagy rendszerekhez, és szándékosan vagy véletlenül okoznak kárt.

Felhőfiók kompromittálás: Hasonlóképpen, a csalások 29%-a emelte ki a felhőfiók kompromittálását jelentős fenyegetésként. Ez akkor következik be, amikor támadók jogosulatlan hozzáférést szereznek felhőszolgáltatásokhoz, ami adatvédelmi incidensekhez és kompromittált biztonsághoz vezethet.

Distributed Denial of Service (DDoS) támadások: Ami úgyszintén hatalmas problémát okoz és több mint 29% a DDoS-támadások, ami jelentős fenyegetést jelentenek. Ezek a támadások a rendszerek és hálózatok túlterhelésére irányulnak túlzott forgalommal, így azok elérhetetlenné válnak. A DDoS-támadások üzleti működést zavarhatnak, szolgáltatási rendelkezésre állást csökkenthetnek és reputációs károkat okozhatnak.

Ezek az eredmények aláhúzzák annak fontosságát, hogy átfogó kiberbiztonsági intézkedéseket vezessenek be a szervezetek védelme érdekében az e-maileket, belső hozzáférést, felhőszolgáltatásokat és digitális eszközöket érintő egyre kifinomultabb fenyegetésekkel szemben. [4]



3. ábra: Támadások eloszlása

1.1.3 Legfontosabb kiberbiztonsági fenyegetések

A kiberfenyegetés bármely olyan tevékenység, amely negatívan befolyásolhatja egy szervezet rendszereit vagy adatait. A kiberbűnözők sérülékenységeket használnak ki információk megszerzésére, működés megzavarására és bűncselekmények elkövetésére, mint a csalás és az identitáslopás. Gyakori fenyegetések, melyek a kutatás tématerületeit is érintik.

Adathalászat (Phishing):

Az adathalászat olyan e-maileket jelent, amelyek látszólag megbízható forrásból származnak, de valójában adatlopásra vagy rendszerekbe való bejutásra irányulnak. Gyakran e-mailen, közösségi médián, szöveges üzeneteken vagy telefonhívásokon keresztül történik, és célja, hogy a címzettet érzékeny adatok kiadására vagy rosszindulatú hivatkozások letöltésére vegye rá. Az oktatás és a biztonsági szoftverek kulcsfontosságú védelmet jelentenek az adathalászat ellen.

Kártékony szoftver (Malware):

A kártékony szoftver egy gyűjtőfogalom minden olyan programra, amely rosszindulatú céllal készül. Gyakran e-maileken, alkalmazásokon vagy mellékleteken keresztül terjed. Jelentős károkat okozhat az infrastruktúrában, például blokkolhatja az adatokhoz való hozzáférést vagy ellophat érzékeny információkat. Az anti-malware szoftverek és a rendszeres frissítések segítenek mérsékelni a kockázatokat.

Zsarolóvírus (Ransomware):

A zsarolóvírus a kártékony szoftverek egyik típusa, amely nemcsak bejut a rendszerbe, hanem váltságdíjat is követel az adatok visszafejtéséért. Megfelelő adatmentési terv hiányában a vállalkozások kénytelenek lehetnek fizetni, hogy visszanyerjék a működőképességüket egy támadás után.

Szolgáltatásmegtagadás (DDoS) támadások:

Ezek túlzott forgalommal árasztják el az eszközöket vagy weboldalakat, megzavarva a normál működést. Az elosztott szolgáltatásmegtagadás (DDoS) támadások több forrásból érkeznek, és gyakran online szolgáltatásokat céloznak.

SQL-befecskendezéses (SQL injection) támadások:

Olyan rosszindulatú kód beillesztését jelentik SQL-beviteli mezőkbe, amely jogosulatlan módon fér hozzá, módosít érzékeny adatokat. A megelőzéshez fontos az adathozzáférési jogosultságok beállítása és a paraméterezett lekérdezések használata.

Lehallgatásos (Eavesdropping) támadások:

Akkor fordulnak elő, amikor hackerek kommunikációs csatornákat figyelnek meg, hogy elemezzék vagy módosítsák az átvitt adatokat. A kockázatok csökkentéséhez fontos a nyilvános Wi-Fi használatának körültekintése és VPN alkalmazása.

Jelszótámadások:

Az egyszerű találgatástól a kifinomult jelszótörő eszközökig terjedhetnek. Gyakori módszerek a billentyűleütés-naplózó (keylogger) szoftverek, a brute force támadások és a social engineering technikák.

Belső fenyegetések:

Olyan jelenlegi vagy volt alkalmazottak jelentik, akik jogosultságaikat rosszindulatúan használják fel. A megelőzéshez szükséges a hozzáférések folyamatos felügyelete és szükség esetén azonnali visszavonása.

Személyazonosság elleni támadások:

Más személy megszemélyesítésével jogosulatlan hozzáférést vagy csalást követnek el. A védekezéshez elengedhetetlen a hitelesítő adatok védelme és a többtényezős hitelesítés alkalmazása. [5]

1.1.4 Kiberbiztonsági trendek

2023-ban a kiberbiztonság váratlan kihívásokkal szembesült, beleértve a generatív mesterséges intelligencia (GenAI) megjelenését és a zsarolóvírus támadások növekedését, amelyek helyi önkormányzatokat céloztak.

E kihívások ellenére pozitív fejlemények is történtek, például a NIST Cybersecurity Framework 2.0 megjelenése és a Fehér Ház kiberbiztonsági terve.

Ahogy beléptünk 2024-be, a szervezeteknek felül kell vizsgálniuk és meg kell újítaniuk kiberbiztonsági stratégiáikat, hogy hatékonyan tudjanak eligazodni a folyamatosan változó fenyegetési környezetben.

A következő jelentős trendek várhatóak az MI felhasználásával:

Megtévesztési taktikák:

A kiberbűnözők várhatóan mesterséges intelligenciát fognak használni kifinomult megtévesztési módszerekhez. Ide értve a deepfake-eket és az MI által készített adathalász e-maileket, kihasználva olyan nagy globális eseményeket, mint például a választások.

Generatív MI hatása:

A GenAI forradalmasíthatja a kiberbűnözést hamis tartalmak és adathalász e-mailek létrehozásával, valamint a lopott adatok hatékonyabb pénzzé tételének lehetőségével.

Identitás felfegyverzése:

A Dark Weben elérhető, egyre nagyobb számú hitelesített felhasználói adat birtokában a támadók ellopott személyazonosságokat fognak felhasználni célzott és összetett kiberműveletek végrehajtásához.

MI által vezérelt támadások:

Az MI alkalmazása a kibertámadásokban várhatóan fokozódni fog és akár az első, nagyszabású, MI által tervezett kibertámadáshoz is vezethet, hasonlóan az 1988-as Morris-féreg incidenshez. Az 1988-as Morris-féreg incidens az első jelentős internetes kártevő-támadás volt, amely megbénította az akkori hálózatok 10%-át, és mérföldkőnek számít a kiberbiztonság történetében.

A zsarolóvírusok fejlődése:

A zsarolóvírus-üzemeltetők a csökkenő váltságdíj-bevételek miatt áttérhetnek a nagy nyomású adatzsarolási támadásokra. Ennek ellenére a zsarolóvírus-fenyegetések várhatóan fennmaradnak, mivel a kiberbűnözők folyamatosan alkalmazkodnak taktikáikban és erőforrásaikban.

Adatbiztonsági kihívások:

Ahogy a generatív mesterséges intelligencia (GenAI) beépül a vállalati infrastruktúrába, a CISO-knak (információbiztonsági vezetőknek) prioritásként kell kezelniük a kritikus adatok védelmét és újra kell értékelniük a biztonsági intézkedéseket az MI által bevezetett új kockázatok mérséklése érdekében.

A biztonsági elemzés szerepének erősödése:

A generatív MI képessé teszi a biztonsági csapatokat adminisztratív feladatok automatizálására, és lehetővé teszi, hogy a kevésbé tapasztalt csapattagok magasabb szintű feladatokat is ellássanak.

Fenyegetés-előrejelzési mérföldkő:

A kiberbiztonsági iparág a nagyléptékű fenyegetés-előrejelzés küszöbén áll, ami a fenyegetések észlelését és kezelését proaktív előrejelzéssé és megelőzéssé alakíthatja.

„Identity Fabric" megközelítés:

A szervezetek egy úgynevezett „identity fabric" (identitásszövet) megközelítést fognak alkalmazni annak érdekében, hogy kezeljék a felhő- és helyszíni rendszerek

eltérő identitáskezelési képességeinek összetettségét, és egységes hitelesítési folyamatokat alakítsanak ki.

Kvantumszámítástechnikai kockázatok:

A kvantumtechnológiai fejlődés kockázatot jelent a hagyományos rendszerekre, mivel fennáll a „most gyűjtsd be, később fejtsd vissza" típusú támadások veszélye. A kvantumbiztos titkosításra való átállásra való felkészülés kulcsfontosságú e kockázatok mérsékléséhez. [6]

1.1.5 A kiberbiztonsági fenyegetések forrásai

A kiberbiztonsági fenyegetések forrásai széles skálán mozognak, és sokféle szereplőt foglalnak magukban, eltérő motivációkkal és taktikákkal. A kutatási témában is az alábbi szereplők vannak jelen:

Kiberbűnözők: Olyan egyének vagy csoportok, akik elsősorban anyagi haszonszerzés céljából követnek el kiberbűncselekményeket. Tevékenységeik közé tartoznak a zsarolóvírus-támadások, az adathalász csalások, valamint érzékeny információk – például hitelkártyaadatok vagy szellemi tulajdon – ellopása.

Hackerek: Olyan személyek, akik technikai tudással rendelkeznek számítógépes hálózatok vagy rendszerek feltöréséhez. Nem minden hacker rosszindulatú; az etikus hackerek segítenek a szervezeteknek azonosítani a sebezhetőségeket szimulált kibertámadások révén.

Nemzetállami szereplők: Kormányzati finanszírozású szereplők, akik célja érzékeny adatok ellopása, kémkedés vagy más nemzetek kritikus infrastruktúrájának megzavarása. Tevékenységeik gyakran jól finanszírozottak és összetettek, ami komoly kihívást jelent felderítésük szempontjából a védelem számára.

Belső fenyegetések: A belső fenyegetések nem szándékos emberi hibából vagy rosszindulatú cselekedetekből eredhetnek. Míg egyes bennfentesek akaratlanul is kiberkockázatoknak teszik ki a hálózatokat, mások személyes haszonszerzésre, bosszúra vagy a munkaadóik elleni kémkedésre használják ki a hozzáférésüket. [7]

1.1.6 A kiberbiztonsági kockázatkezelés

A kiberkockázatkezelés az információs rendszereket fenyegető kockázatok azonosításának, rangsorolásának, kezelésének és monitorozásának folyamata. Ez az oka

annak, hogy a kiberkockázatkezelés a vállalati kockázatkezelési erőfeszítések létfontosságú részévé vált.

Az iparágakban működő vállalatok nagymértékben támaszkodnak az információ-technológiára, ami különféle kiberbiztonsági fenyegetéseknek teszi ki őket, mint például a kiberbűnözői tevékenységek, az alkalmazottak hibái és a természeti katasztrófák. Ezek a fenyegetések kritikus rendszereket veszélyeztetnek, vagy hatalmas veszteségeket okozhatnak, ami bevételkieséshez, adatlopáshoz, hosszú távú hírnévkárosodáshoz és szabályozási bírságokhoz vezethet. Bár ezeket a kockázatokat nem lehet teljesen kiküszöbölni, a kiberkockázatkezelési programok kulcsszerepet játszanak hatásuk és valószínűségük csökkentésében.

A kiberbiztonsági kockázatkezelési folyamat több lépésből áll, beleértve a kockázat-keretezést, a kockázatértékelést, a kockázatra való reagálást és a monitorozást. A kockázatkeretezés magában foglalja a kockázati döntések kontextusának meghatározását, figyelembe véve olyan tényezőket, mint a hatókör, az eszközök rangsorolása, a szervezeti erőforrások és a jogi követelmények. A kockázatértékelés segít azonosítani a fenyegetéseket, a sebezhetőségeket és a lehetséges hatásokat, a kritikus kockázatokat a valószínűség és a súlyosság alapján rangsorolva.

A kockázatra való reagálás során a vállalatok kockázatcsökkentési, elhárítási vagy átadási stratégiákat választhatnak az azonosított kockázatok valószínűségétől és hatásától függően. Végül a folyamatos monitorozás biztosítja, hogy a biztonsági ellenőrzések továbbra is hatékonyak és relevánsak maradjanak, lehetővé téve a szervezetek számára, hogy kiberbiztonsági programjaikat az új fenyegetésekre vagy az informatikai környezetükben bekövetkező változásokra reagálva módosítsák.

A kiberkockázatkezelés kulcsfontosságú a folyamatosan változó fenyegetési környezet kezelésében és az olyan szabályozásoknak való megfelelésben, mint az Általános Adatvédelmi Rendelet (General Data Protection Regulation, továbbiakban: GDPR) és az Egészségbiztosítási Hordozhatósági és Elszámoltathatósági Törvény (Health Insurance Portability and Accountability Act, továbbiakban: HIPAA). Kiemeli az olyan keretrendszerek szerepét, mint a NIST Kiberbiztonsági Keretrendszer (Cybersecurity Framework, továbbiakban: NIST CSF) és a NIST Kockázatkezelési Keretrendszer (Risk Management Framework, továbbiakban: NIST RMF) a szervezetek kockázatkezelési erőfeszítéseinek irányításában, különösen az ügynökségek és a vállalkozók esetében.

Összességében a kiberkockázatkezelés kritikus szerepet játszik a modern szervezetekben, gyakorlatias megközelítést kínálva a kiberbiztonsági kockázatok kezelésére és a szabályozási megfelelés biztosítására az egyre összetettebb IT környezetben. [8]

1.1.7 Bevált gyakorlatok magánszemélyek és vállalkozások számára

Ahogy a kiberfenyegetések egyre kifinomultabbá válnak, és a kibertámadások egyéneket és családokat, kis- és középvállalkozásokat, valamint nagyvállalatokat is céloznak, mindannyiuknak fontos szerepük van digitális világunk biztonságában.
Magánéletünk védelme érdekében négy egyszerű lépést kell követnünk az online biztonság megőrzése érdekében:

- Használjon erős jelszavakat (hosszú, véletlenszerű és egyedi).
- Kapcsolja be a többtényezős hitelesítést minden olyan fiókban, amely ezt kínálja.
- Ismerje fel és jelentse az adathalászatot („gondolkodjon el, mielőtt kattint”).
- Frissítse a szoftvereket (engedélyezni és alkalmazni kell a frissítéseket).

A vállalatok számára a kibertámadások megelőzéséhez többrétegű megközelítésre van szükség:

Erős jelszavak: A jelszószabályzatok bevezetése és az összetett, egyedi jelszavak használata segít megelőzni a fiókokhoz való jogosulatlan hozzáférést.
E-mail biztonsági eszközök: Az e-mail biztonsági megoldások, például a spamszűrők és az e-mail titkosítás alkalmazása segít az adathalász támadások és más e-mail alapú fenyegetések észlelésében és enyhítésében.
Víruskereső szoftver: A megbízható víruskereső szoftverek használata segít a rosszindulatú programok észlelésében és eltávolításában, további védelmi réteget biztosítva a kiberfenyegetésekkel szemben.
Tűzfalak és VPN-ek: A tűzfalak és virtuális magánhálózatok (Virtual Private Network, továbbiakban: VPN) telepítése segít megvédeni a hálózatokat a jogosulatlan hozzáféréstől, és titkosítja a nyilvános hálózatokon továbbított adatokat, növelve a biztonságot.
Többtényezős hitelesítés (MFA): Az MFA (Multi-Factor Authentication, továbbiakban: MFA) engedélyezése további biztonsági réteget biztosít azáltal, hogy a felhasználóknak több ellenőrzési formát kell megadniuk a fiókok vagy rendszerek eléréséhez.

Biztonsági tudatossági képzés: Az alkalmazottak kiberbiztonsági legjobb gyakorlatokkal és a lehetséges fenyegetésekkel kapcsolatos képzése segít csökkenteni az emberi hibák kockázatát, és javítja az általános biztonsági helyzetet.

Fejlett végpontbiztonság: A fejlett végpontbiztonsági megoldások, például a végpontvédelmi rendszer (Endpoint Detection and Response, továbbiakban: EDR) eszközök bevezetése segít a végpontokat, például a számítógépeket és a mobileszközöket célzó fenyegetések észlelésében és kezelésében. Hálózati biztonsági megoldások: A behatolásérzékelő rendszerek (Intrusion Detection System, továbbiakban: IDS), behatolásmegelőző rendszerek (Intrusion Prevention System, továbbiakban: IPS) és egyéb hálózati biztonsági megoldások telepítése segít a hálózati forgalom monitorozásában és védelmében, valós időben észleli és mérsékli a kiberfenyegetéseket.

Fenyegetésészlelés és incidensekre való reagálás: A legmodernebb fenyegetésészlelési technológiákba való befektetés és a robusztus incidensekre való reagálási folyamatok létrehozása segít a kiberbiztonsági fenyegetések gyors azonosításában és kezelésében, minimalizálva a potenciális károkat és zavarokat.

Egy átfogó kiberbiztonsági stratégia elfogadásával, amely magában foglalja ezeket az intézkedéseket, a szervezetek megerősíthetik védekezésüket, és megelőzhetik a folyamatosan változó kiberfenyegetéseket. [9]

1.1.8 Az információbiztonságért felelős vezetők szerepe és felelősségi köre

A kiberbiztonsági szakemberek kulcsszerepet játszanak személyes és szakmai életünk védelmében a technológia széles körű elterjedése miatt egyre gyakoribbá vált kiberfenyegetésekkel szemben. Feladataik közé tartozik az informatikai infrastruktúra, eszközök, hálózatok és adatok védelme, valamint a behatolások megelőzése és a támadásokra való reagálás. Míg a technikai készségek fontosak, a gondolkodás, a kíváncsiság és a folyamatos tanulás iránti elkötelezettség ugyanolyan fontos ezen a területen.

Ezek a szakemberek folyamatosan frissítik tudásukat, hogy naprakészek maradjanak a hackerek által alkalmazott új biztonsági fenyegetésekkel és taktikákkal kapcsolatban. A konkrét feladatok közé tartozik a hozzáférés-vezérlés beállítása és megvalósítása, a hálózati és alkalmazásteljesítmény monitorozása anomáliák szempontjából, auditok elvégzése a biztonsági gyakorlatoknak való megfelelés biztosítása érdekében, végpont-észlelő és -megelőző eszközök telepítése, javításfrissítések kezelése, sebezhetőség-kezelő rendszerek megvalósítása, valamint az informatikai műveletekkel való együttműködés a

katasztrófa utáni helyreállítási tervek kidolgozása érdekében. Ezenkívül a kiberbiztonsági szakemberek az emberi erőforrás menedzsmenttel és a vezetőkkel együttműködve oktatják az alkalmazottakat a gyanús tevékenységek azonosítására, hangsúlyozva a kollektív erőfeszítés fontosságát a kiberbiztonság fenntartásában. [10]

2023-tól a kiberbiztonsági munkaerőpiac növekedést és kihívásokat is tapasztalt. Miközben a kiberbiztonsági szakemberek száma rekordmagas, 5,5 millió fős volt, továbbra is jelentős hiány mutatkozik a képzett munkaerő iránti növekvő kereslet kielégítésében. A munkaerőnek évente 12,6 százalékkal kell bővülnie a változó fenyegetési környezet kezelése érdekében, mégis 2023-ban csak 8,7 százalékkal nőtt. [11]

Minden üzletágnak figyelembe kell vennie a kiberbiztonságot a napi üzleti folyamatai során. De egyes iparágak jobban ki vannak téve a veszélynek, mint mások. A magas kiberbiztonsági igényű iparágak közé tartozik a pénzügy, az egészségügy és az energia, míg a feltörekvő ágazatok, mint például a digitális eszközök és a mesterséges intelligencia technológia, szintén veszélyben vannak. A meglévő alkalmazottak továbbképzése ajánlott, és a szervezetek képzési programokat kínálnak a készséghiány áthidalására. Az alapvető technikai készségek, mint például az operációs rendszerek, a kódolási nyelvek és a hálózatépítés, elengedhetetlenek, de a felhőalapú számítástechnika és a mesterséges intelligencia olyan területeken való specializációja egyre fontosabb. A technikai készségek mellett a soft skillek is ugyanolyan fontosak lehetnek, mint a technikai készségek. A felhőalapú számítástechnika biztonsága mögött a kommunikációs készségek állnak a második helyen a listán. [11]

1.1.9 A kiberbiztonság irányítási és védekezési keretrendszere

A NIST az Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Szabványügyi és Technológiai Intézete. A NIST kiberbiztonsági keretrendszere segít minden méretű vállalkozásnak jobban megérteni, kezelni és csökkenteni kiberbiztonsági kockázataikat, valamint megvédeni hálózataikat és adataikat.

A 2014. évi kiberbiztonság-fejlesztési törvény kibővítette a (NIST) szerepét, hogy kiberbiztonsági kockázati keretrendszereket dolgozzon ki a kritikus infrastruktúra tulajdonosai és üzemeltetői számára önkéntes használatra. Ez formalizálta a NIST korábbi, a 13636. számú végrehajtási rendelet szerinti 1.0-s keretrendszer-verzióval kapcsolatos munkáját, amely a kritikus infrastruktúra kiberbiztonságának javítására összpontosított anélkül, hogy további szabályozási követelményeket róna a vállalkozásokra. [12]

A keretrendszer hangsúlyozza az üzleti mozgatórugók használatát a kiberbiztonsági tevékenységek irányításához, és integrálja a kiberbiztonsági kockázatokat a szervezet átfogó kockázatkezelési folyamataiba. Három részből áll: a keretrendszer magjából, a megvalósítási szintekből és a keretrendszer profiljaiból. A mag kiberbiztonsági tevékenységeket és eredményeket tartalmaz, míg a profilok segítenek a szervezeteknek összehangolni a kiberbiztonsági tevékenységeket az üzleti követelményekkel és a kockázattűrési határokkal. A szintek segítenek a szervezeteknek megérteni a kiberbiztonsági kockázatok kezelésére vonatkozó megközelítésüket.
Bár kritikus infrastruktúrára fejlesztették ki, a Keretrendszert bármely szektorban működő szervezetek használhatják. Rugalmas megközelítést kínál a fizikai, kiber- és emberi dimenziókat érintő kiberbiztonsági kockázatok kezelésére, beleértve az adatvédelmi szempontokat is. Modellként szolgál a kiberbiztonsággal kapcsolatos nemzetközi együttműködéshez, és segítséget nyújthat a különféle technológiákra, többek között az információtechnológiára, az ipari vezérlőrendszerekre és az internetre támaszkodó szervezeteknek.

A Keretrendszer nem előíró jellegű; a szervezetek az egyedi kockázataik és prioritásaik alapján szabják testre a gyakorlatokat. Különböző megvalósítási megközelítéseket tesz lehetővé, például megvalósítási szintek használatát vagy a kockázatkezelési portfóliók elemzését. Élő dokumentumként a keretrendszer folyamatosan fejlődik az iparági visszajelzések és a tanulságok alapján, biztosítva relevanciáját a dinamikus kiberbiztonsági kihívások kezelésében. [13]

1.1.10 Kritikus infrastruktúra biztonsága és ellenálló képessége

A kritikus infrastruktúra olyan eszközök, rendszerek és hálózatok, amelyek az életmódunkhoz szükséges funkciókat biztosítják. 16 kritikus infrastruktúraágazat alkotja egy összetett, összekapcsolódó ökoszisztéma részét, és ezekre az ágazatokra leselkedő bármilyen fenyegetés potenciálisan gyengítő nemzetbiztonsági, gazdasági, közegészségügyi vagy biztonsági következményekkel járhat.
Az európai uniós és magyar szabályozások által meghatározott kritikus infrastruktúra-ágazatok létfontosságúak a társadalom működése, a gazdaság stabilitása, a közegészségügy és a közbiztonság szempontjából. Ezek az ágazatok a következők:

Vegyipari ágazat: A Belbiztonsági Minisztérium (DHS) által a Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökségen (CISA) keresztül kezelt ágazat, amely a vegyipari létesítmények biztonságának és ellenálló képességének fokozására összpontosít.

Kereskedelmi létesítmények ágazata: A nyilvánosság számára nyitott terek védelme az összehangolt támadásoktól, a CISA stratégiai iránymutatást nyújt a különböző alágazatokban.

Kommunikációs ágazat: Földi, műholdas és vezeték nélküli rendszerek bevonása, a CISA együttműködésével az érdekelt felekkel a kockázatkezelési keretrendszerek megvalósítása érdekében.

Kritikus gyártási ágazat: A nemzeti jelentőségű gyártóipar azonosítása, értékelése és védelme a katasztrófákkal szemben.

Gátak szektor: Több mint 90 000 gát kezelése az Egyesült Államokban a kritikus vízvisszatartási és -szabályozási szolgáltatások biztosítása érdekében.

Védelmi ipari bázis szektor: Anyagok, szolgáltatások és létesítmények mozgósítása, telepítése és fenntartása az amerikai katonai műveletekhez.

Sürgősségi szolgálatok szektor: Képzett személyzet és erőforrások támogatása az életmentés, a vagyon védelme és a vészhelyzetek utáni helyreállítás érdekében.

Energia szektor: Villamosenergia-, olaj- és földgázforrások és -eszközök védelme a folyamatos energiaellátás biztosítása érdekében.

Pénzügyi szolgáltatási szektor: Pénzügyi intézmények védelme áramkimaradások, katasztrófák és kibertámadások ellen a pénzügyi stabilitás fenntartása érdekében.

Élelmiszeripari és mezőgazdasági szektor: Magántulajdonban lévő élelmiszeripari és mezőgazdasági létesítmények védelme a különféle kockázatokkal szemben interszekcionális együttműködéssel.

Kormányzati létesítmények szektor: Segítségnyújtás a kormányzati épületeknek az egyedi kockázati tényezők azonosításában és a potenciális támadások elleni védelemben.

Egészségügyi és közegészségügyi szektor: A lakosság egészségére összpontosít, és reagál a nagyszabású veszélyekre, mint például a terrorizmus és a természeti katasztrófák.

Információtechnológiai szektor: A kiberfenyegetések és sebezhetőségek azonosítása és elleni védelem egy egyre inkább technológiától függő környezetben. Nukleáris ***Reaktorok, Anyagok és Hulladék Szektor:*** Polgári nukleáris infrastruktúra, beleértve az erőműveket és az orvosi izotópok, kezelése.

Közlekedési Rendszerek Szektor: Az országon belüli személy- és árumozgatáshoz elengedhetetlen közlekedési rendszerek védelme.

Víz- és Szennyvízrendszerek Szektor: Az ország stabilitásának és egészségének biztosítása az emberi tevékenységhez elengedhetetlen vízrendszerek védelmével. [14]

A kritikus infrastruktúra védelmének biztosítása átfogó megközelítést igényel, beleértve a kiberbiztonsági intézkedéseket, a katasztrófafelkészültségi és elhárítási terveket, a rugalmas infrastruktúra tervezést, az ellátási lánc biztonságát, a köz- és magánszféra együttműködését, valamint a folyamatos monitoringot és kockázatértékelést. A változó kibertámadási trendek rávilágítanak a folyamatos éberség, az oktatás és a kiberbiztonságba való beruházás szükségességére minden ágazatban, hogy hatékonyan mérsékeljék a változó fenyegetési környezetet.

1.1.11 Összegzés

Első hipotézis: A kibertámadások elleni védekezésből eredő rendszerüzemeltetési megközelítések vizsgálata — különös tekintettel az globális trendekre, megfelelő rendszer komponensekre és szolgáltatás alapú üzemeltetési stratégiákra — növelheti a védelmi intézkedések hosszútávú hatékonyságát.

A globális trendek, MI-integráció és szolgáltatásalapú üzemeltetés együttesen valóban növelik a védelmi intézkedések fenntarthatóságát és hatékonyságát, a nemzetközi gyakorlat és kutatási eredményeim ezt alátámasztják.
A hipotézis szerint a körültekintő tervezés, megfelelő rendszerekkel kombinálva plusz az MI által támogatott komponensek lehetővé teszi a döntéshozók számára, hogy korlátozott források mellett maximalizálják a védelmi hatékonyságot, miközben megfelelnek szabályozási és üzemeltetési követelményeknek.

Az első hipotézisem az alábbiakkal validálható:

- A globális trendek az MI-alapú támadások térnyerését mutatják.
- A megfelelő rendszerkomponensek (MDM, MI, audit) technikailag és szabályozásilag is megalapozottak.
- A szolgáltatásalapú üzemeltetés költséghatékony és skálázható.
- Az MI támogatás lehetővé teszi a hatékonyságot.

2 AZ INFRASTRUKTÚRAVÉDELEM METSZÉSPONTJAI

A fejezetben ismertetem a kutatás szempontjából releváns információkat. A pénzmosási kockázatok bemutatása során a hatások becsléséhez szükséges fogalmak és kockázati tényezők ismertetése elengedhetetlen, mivel a kritikus infrastruktúrák ellátási láncaiban és szolgáltatási ökoszisztémáiban a pénzügyi tranzakciók nem csupán gazdasági események, hanem potenciális visszaélési felületek is. Ezek a visszaélések közvetetten gyengíthetik a szervezetek kibervédelmi képességeit, ami hosszú távon súlyos társadalmi és gazdasági következményekhez vezethet.

2.1 Pénzmosás elleni védelem, mint a kritikus infrastruktúra kulcseleme

A pénzmosás elleni védelem a kritikus infrastruktúrák biztonsági architektúrájának meghatározó eleme, mivel a pénzügyi rendszerekbe történő illegális beavatkozás nemcsak gazdasági károkat okozhat, hanem közvetetten veszélyeztetheti az ellátási láncok, szolgáltatási ökoszisztémák és digitális rendszerek működőképességét is. A pénzügyi visszaélésekből származó kockázatok torzíthatják a szervezetek kockázatérzékelését, gyengíthetik a kontrollkörnyezetet, és olyan rejtett sérülékenységeket hozhatnak létre, amelyek a kibervédelem, az üzemfolytonosság és a társadalmi biztonság szempontjából egyaránt kritikusak. Emiatt a pénzmosás elleni védelem nem pusztán megfelelési követelmény, hanem stratégiai jelentőségű védelmi vonal a nemzeti és ágazati infrastruktúrák stabilitásának fenntartásában.

2.1.1 Integrált monitoring rendszerek a pénzmosás kockázatok szűrésére

A pénzmosás elleni küzdelem (Anti-Money Laundering, továbbiakban: AML) és a terrorizmus finanszírozása elleni fellépés (Counter-Terrorist Financing, továbbiakban: CTF) olyan egyre szigorodó szabályozások és gyakorlatok összességét jelenti, amelyek célja a pénzmosáshoz és a terrorizmus finanszírozásához kapcsolódó illegális tevékenységek megelőzése és felismerése. Így a kritikus infrastruktúrák védelmében egyre nagyobb szerepet kapnak a prediktív analitikák és gépi tanulási algoritmusok, amelyek képesek előre jelezni a pénzmosásra utaló viselkedésmintákat. Az ilyen rendszerek nemcsak a pénzügyi szektort, hanem az energetikai és közlekedési infrastruk-

túrákat is segíthetik abban, hogy időben reagáljanak a gazdasági bűncselekményekből fakadó fenyegetésekre.

2.1.2 Pénzmosás és a kritikus infrastruktúrák védelmének összefonódása

A pénzmosás (AML) és a terrorizmus finanszírozása elleni fellépés (CTF) olyan egyre szigorodó szabályozások és gyakorlatok összességét jelenti, amelyek célja az illegális pénzügyi tevékenységek megelőzése és felismerése. Ezek a mechanizmusok kiemelt szerepet játszanak a kritikus infrastruktúrák különösen a pénzügyi, energetikai és közlekedési rendszerek informatikai védelmében, mivel a gazdasági bűncselekmények közvetlenül veszélyeztethetik a nemzetbiztonságot és a szolgáltatások folytonosságát.
A pénzmosás jogellenes folyamat, amelynek során bűncselekményekből származó pénzeszközöket például kábítószer-, fegyverkereskedelemből, csalásból vagy illegális szerencsejátékból származó bevételeket úgy tüntetnek fel, mintha legális forrásból erednének. Az ENSZ becslése szerint a világ GDP-jének 2–5%-át mossák tisztára évente, ennek körülbelül 10%-át sikerül ténylegesen felderíteni.

A pénzmosás jellemzően három szakaszban történik:

- Elhelyezés (Placement): a bűncselekményből származó pénzeszközök bekerülnek a pénzügyi rendszerbe pl.: banki utalások, valutaváltás vagy készpénzbefizetés révén.
- Rétegzés (Layering): a pénz eredetének elfedése összetett pénzügyi tranzakciókkal, offshore struktúrákkal vagy könyvelési manipulációkkal. Itt kapnak szerepet a SIEM (Security Information and Event Management, biztonsági információ- és esemény-kezelés) rendszerek, amelyek képesek anomáliákat és gyanús mintázatokat észlelni.
- Integráció (Integration): a pénz visszajuttatása a legális gazdasági körforgásba, például befektetések, ingatlanvásárlás vagy vállalati bevételek formájában.

A terrorizmus finanszírozása olyan folyamat, amelynek során pénzeszközöket juttatnak el különböző terrorista csoportok műveleti tevékenységeinek támogatására. A jótékonysági szervezeteket gyakran magasabb kockázatúnak tekintik e célból, mivel könnyebben felhasználhatók a pénzmozgások elfedésére. Számos ország világszerte intézkedéseket vezetett be a terrorizmus finanszírozásának megakadályozására, és ezeket az AML kontrollrendszerekbe integrálták. Az MI és a gépi tanulás egyre fontosabb szerepet kap a pénzmosás és terrorizmus finanszírozása elleni küzdelemben, különösen a kritikus infrastruktúrák védelmében. Az MI képes előre jelezni a gyanús viselkedés-

mintákat, automatizálni a kockázatmodellezést, és támogatni az incidenskezelést. A magyar Büntető Törvénykönyv értelmében a pénzmosás és a terrorizmus finanszírozása bűncselekménynek minősül, és különösen súlyosnak tekinthető, ha az kritikus infrastruktúrát érint vagy annak működését veszélyezteti.

2.1.3 Jogi és szabályozási követelmények

A pénzügyi intézmények világszerte nemcsak jogszabályi kötelezettség alapján kötelesek megakadályozni, hogy bűnözők használják platformjaikat, hanem ez saját jól felfogott érdekük is. A pénzmosás és a terrorizmus finanszírozása jelentős kockázatot jelent nemcsak az egyes pénzügyi szereplők, hanem az egész szektor stabilitására nézve. A pénzmosási botrányok bankok összeomlásához vezettek, országokat ráztak meg, és végső soron a társadalom fizeti meg az árát — a pénzügyi rendszerbe vetett bizalom megingásával. A megfelelő AML/CTF kontrollkeretrendszer bevezetése elengedhetetlen a súlyos felügyeleti bírságok, szabályozói szankciók, pénzügyi veszteségek és reputációs károk elkerülése érdekében. A szabályozói szankciók magukban foglalhatják az üzleti tevékenység korlátozását, sőt akár az intézmény működési engedélyének visszavonását is. Mivel a pénzügyi szektor a nemzetgazdaság kritikus infrastruktúrájának része, az AML/CTF rendszerek nemcsak jogi és üzleti szempontból fontosak, hanem informatikai védelmi prioritást is élveznek. A mesterséges intelligenciával támogatott monitoring, a valós idejű anomáliaészlelés és a kockázatmodellezés kulcsszerepet játszik abban, hogy a pénzügyi rendszerek ellenállóak maradjanak a gazdasági bűncselekményekkel és a nemzetbiztonságot érintő fenyegetésekkel szemben. A magyarországi pénzügyi intézményeknek az alábbi törvényeknek és rendeleteknek kell megfelelniük:

- 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról; [15]
- 2017. évi LII. törvény az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi korlátozások végrehajtásáról; [16]
- 26/2020. (VIII.25.) MNB rendelet a pénzmosás és a terrorizmus finanszírozása elleni intézkedésekről; [17]
- 21/2017. (VIII.3.) NGM rendelet a belső szabályzat kötelező tartalmi elemeiről. [18]

Ezeknek a szabályoknak az a célja, hogy megakadályozzák a bűncselekményekből származó pénzek határokon átnyúló tisztára mosását a pénzügyi rendszeren, a tőkepiacon

és más veszélyeztetett területeken keresztül, valamint, hogy visszaszorítsák a terrorizmus finanszírozását. A magyar pénzügyi intézményeket a Magyar Nemzeti Bank (továbbiakban: MNB) felügyeli. Az ellenőrzések egyik fő szempontja, hogy az adott intézmény pénzmosás és terrorizmusfinanszírozás elleni rendszere megfelelően működik-e. Ha az MNB hiányosságot talál, akkor külön tételként bírságot szabhat ki. A Pénzügyi Akció Munkacsoport (Financial Action Task Force, továbbiakban: FATF) egy független, kormányközi szervezet, amely olyan szabályozási elveket dolgoz ki és népszerűsít, amelyek célja a globális pénzügyi rendszer védelme az illegális tevékenységekkel szemben — különösen a pénzmosás, a terrorizmus finanszírozása és a tömegpusztító fegyverek terjedésének finanszírozása ellen. [19]

A FATF nemzetközi szabványokat határoz meg annak érdekében, hogy a nemzeti hatóságok képesek legyenek felismerni az olyan bűncselekményekhez köthető pénzmozgásokat, mint a kábítószer-kereskedelem, az illegális fegyverkereskedelem, a kibercsalás és más súlyos bűncselekmények.

Összesen több mint 200 joghatóság vállalta, hogy végrehajtja a FATF által meghatározott szabványokat, ezzel segítve a szervezett bűnözés, a korrupció és a terrorizmus elleni globális fellépést. [20]

2.1.4 Pénzmosási sebezhetőségek Magyarországon

Magyarországon három kulcsfontosságú terület minősítése kiemelten fontos AML szempontból:

• Banki szolgáltatások: a bankok és pénzügyi intézmények bevezették a fokozott ügyfélátvilágítási (Enhanced Due Diligence, továbbiakban: EDD) intézkedéseket, ami egy szigorított ellenőrzési eljárás, amelyet magas kockázatú ügyfelek vagy tranzakciók esetén ír elő a pénzmosás és terrorizmus finanszírozása elleni törvény.

• Kiválasztás és képzés: a magyar pénzügyi intézményeknek belső szabályzatokat kell naprakészen tartaniuk és intézkedéseket kell alkalmazniuk annak érdekében, hogy megfelelő szaktudással rendelkező szakemberek feleljenek az AML/CTF rendszerekért.

• Átláthatóság és tényleges tulajdonosi viszonyok: Magyarország olyan intézkedéseket vezetett be, mint például a cégek vezetőinek teljes körű feltüntetése a cégjegyzékben, a

tényleges tulajdonosokra vonatkozó adatok naprakészen tartása, valamint a regisztrációs adatok frissítésére vonatkozó határidő betartása. [21] [22]

Ugyanakkor Magyarországnak további megfelelőségi fejlesztésekre van szüksége az AML/CTF intézkedések terén az alábbi területeken:

- Civil szervezetek (non-profit szektorban az átláthatóság növelése),
- Új technológiák alkalmazása (pl. Kriptovaluták, fintech szolgáltatások szabályozása),
- Készpénzszállítók (ellenőrzés és szabályozás növelése).

2.1.5 Három védelmi vonal

Az első védelmi vonal az ügyfél-azonosításhoz és beléptetéshez kapcsolódik. Az érintett üzleti terület végzi az ügyfelek átvilágítását (due diligence) a belépés során, ezzel segítve a pénzmosás megelőzését.

A második védelmi vonal két fő területből áll:

- Compliance (megfelelőség): elsődleges felelőse a pénzmosás és a terrorizmus finanszírozása elleni védelemnek. Feladata az AML szempontból gyanús ügyfelek és tranzakciók folyamatos nyomon követése, valamint annak biztosítása, hogy az intézmény megfeleljen a vonatkozó jogszabályoknak és előírásoknak.
- Kockázatkezelés: szintén a második vonal része, fontos szerepet játszik a kockázatok felmérésében, csalásmegelőzésben és a kiberbiztonsági műveletekben.

A harmadik védelmi vonal az belső ellenőrzés (Internal Audit, továbbiakban: IA), amely független biztosítékot nyújt az intézmény számára. Feladata, hogy értékelje az AML szabályzatok, folyamatok és kontrollrendszerek jogi és szabályozási megfelelőségét, valamint működési hatékonyságát. A belső ellenőrzés azt vizsgálja, hogy elegendő kockázatcsökkentő intézkedés van-e a pénzmosás és terrorizmusfinanszírozás elleni védelemhez, és javaslatokat tesz, hogyan kezelje az intézmény a hiányosságokat. [23]

2.1.6 A pénzmosás megelőzés ellenőrzési keretrendszer

A pénzügyi bűncselekményekhez kapcsolódó minden kockázat háromféle ellenintézkedést igényel: az ügyfél azonosítását és hitelesítését, a tranzakciók és

viselkedési minták figyelését és az anomáliák észlelését, valamint a kockázatok mérséklését. A pénzmosás elleni belső kontrollrendszer az alábbi fő elemekből áll:

AML irányítás – szervezeti keretek, írásos szabályzatok, tudatosság

Minden pénzügyi intézménynek ki kell neveznie egy kijelölt AML megfelelőségi tisztviselőt, aki az egész pénzmosás elleni programot felügyeli. Emellett az intézménynek a kockázati szinthez és a szervezet méretéhez igazodó megfelelő erőforrásokat kell biztosítania. Az intézményeknek olyan AML szabályzatokat és eljárásokat kell kidolgozniuk, amelyek ésszerűen alkalmasak a pénzmosás és a terrorizmus finanszírozásának felismerésére, és ezekhez megfelelő belső kontrollokat kell bevezetniük. Ezek a belső szabályok minden munkavállalóra nézve kötelező érvényűek. Rendszeres AML-képzéseket kell biztosítani minden munkatárs számára, amelyek igazodnak az intézmény kockázati profiljához és tevékenységi köréhez. A dolgozóknak meg kell ismerniük az alkalmazandó AML/CTF jogszabályokat és előírásokat, hogy képesek legyenek felismerni azokat az üzleti kapcsolatokat és tranzakciós megbízásokat, amelyek pénzmosásra vagy terrorizmus finanszírozására utalhatnak.

Ismerd meg az ügyfeledet

Az „Ismerd meg az ügyfeled” (Know Your Customer, továbbiakban: KYC) ellenőrzés kiemelten fontos folyamat, amelynek célja az ügyfél személyazonosságának megállapítása és hitelesítése az ügyfél beléptetésekor, valamint időszakosan a kapcsolat fennállása alatt. A KYC folyamat során a pénzügyi intézmény jogszabályban előírt adatokat és dokumentumokat gyűjt és tárol, például személyazonosító okmányokat (személyi igazolvány – személyazonosság igazolása) és közüzemi számlákat (lakcím igazolása), hogy ellenőrizze ezek megfelelőségét és hitelességét. A szigorú KYC eljárások alkalmazása — például biometrikus azonosítás a digitális beléptetés során, többfaktoros hitelesítési mechanizmus az ügyfélazonosításhoz, valamint a mobil eszközök azonosítása az online banki tranzakciók hitelesítéséhez — megelőző kontrollintézkedésként szolgál a pénzügyi intézmények számára a pénzmosás és visszaélések elleni védekezésben. [24]

Ügyfél átvilágítás

A vonatkozó magyar jogszabályok szerint az ügyfél-átvilágítás (Customer Due Diligence, továbbiakban: CDD) jogilag meghatározott esetekben kötelező. Különösen akkor kell

CDD-eljárást lefolytatni, amikor új ügyfélkapcsolat jön létre, ha a készpénzes tranzakció eléri vagy meghaladja a 4,5 millió forintot, illetve ha a pénzváltás összege meghaladja a 300 000 forintnak megfelelő értéket.

A pénzügyi intézményeknek kockázatalapú megközelítést kell alkalmazniuk az ügyfelek folyamatos átvilágítása során, hogy megértsék az ügyfélkapcsolatok jellegét és célját. A CDD-eljárás része az összes pénzmosás elleni szempontból releváns adat és dokumentum begyűjtése, azonosítása és ellenőrzése a leendő vagy meglévő ügyfél (beleértve a képviselőjét és a tényleges tulajdonost) esetében. Ez magában foglalja az ügyfél személyazonosságának, pénzeszközei forrásának, vagyonának eredetének, foglalkoztatási hátterének és előéletének vizsgálatát is. A jogszabályi megfelelés érdekében a pénzügyi intézményeknek minden ügyfél-azonosítási adatot és dokumentumot naprakészen kell tartaniuk. Ennek megfelelően elengedhetetlen az ügyfélkapcsolatok és tranzakciók folyamatos nyomon követése, valamint a jogszabályoknak való megfelelés rendszeres ellenőrzése. A fokozott ügyfél-átvilágítás (EDD) még alaposabb vizsgálatot és mélyebb kockázatelemzést jelent, és azokra az ügyfelekre kell alkalmazni, akik magas kockázati besorolásba tartoznak. Ilyenek például a politikai közszereplők (Politically Exposed Person, továbbiakban: PEP), a stratégiai hiányosságokkal rendelkező magas kockázatú harmadik országokból származó ügyfelek, a magas kockázatú üzleti szektorok szereplői, valamint azok az ügyfelek, akik indokolatlanul bonyolult üzleti struktúrával rendelkeznek. Az ügyféladatok ellenőrzéséhez a pénzügyi intézmények különféle belső és külső, harmadik féltől származó szoftvereket használnak, amelyek célja a gyanús vagy hamis adatok és dokumentumok azonosítása. Az ügyfél kockázati besorolásától függően az átvilágítás történhet közvetlen vagy közvetett elektronikus kommunikációs csatornákon keresztül is.

Tranzakciófigyelés és gyanús tranzakciók jelentése

A FATF nyilvántartást vezet azokról az országokról, amelyek pénzmosás és terrorizmusfinanszírozás elleni gyakorlatukban stratégiai hiányosságokat mutatnak — ezeket szürke és fekete listaként is emlegetik. A gyanús tranzakciók automatikus szűrőrendszerekkel történő figyelése — beleértve a nemzetközi szankciós listákat (pl. ENSZ, EU, OFAC), a politikai közszereplők (PEP) listáit, a kockázatos szereplők kiszűrését és a negatív médiamegjelenések figyelését — alapvető eleme a pénzmosás és a terrorizmus finanszírozása elleni küzdelemnek. [25]

A monitoring rendszerekben előre definiált gyanús forgatókönyvek (például tranzakciók száma, összege, partner típusa, érintett országok) olyan detektív kontrollok, amelyek segítenek kiszűrni és akár blokkolni a gyanús tranzakciókat, valamint szigorítani a csalásfelderítési szabályokat.

Jellemző gyanús tranzakciós minták:

- Nagy vagy kis összegű tranzakciók közvetlenül a számlanyitás után
- Azonnali készpénzfelvétel vagy nagy összegű utalás
- Pénzmozgás magas kockázatú pénzmosási országokba vagy onnan
- Harmadik fél által indított tranzakciók

A folyamatos, valós idejű tranzakciófigyelés lehetővé teszi a pénzügyi intézmények számára, hogy időben felismerjék a gyanús tevékenységeket, kiszűrjék a téves riasztásokat, és a gyanús tranzakciókat legkésőbb öt munkanapon belül jelenteni tudják.
A gyanús tranzakciók azonosításának, kivizsgálásának és jelentésének folyamatát egyértelműen dokumentálni kell az AML szabályzatban és eljárásrendben. A gyanús tevékenységről szóló jelentés (Suspicious Activity Report, továbbiakban: SAR) olyan mechanizmus, amely nyomon követi a szokatlan pénzügyi eseményeket, és tartalmazza az ügyfélre vonatkozó releváns adatokat, valamint a pénzmosásra utaló tranzakciós információkat. Magyarországon a NAV Központi Hivatala, mint Magyar Pénzügyi Információs Egység (HFIU) felelős a gyanús tranzakciókról szóló jelentések fogadásáért, elemzéséért és továbbításáért. [26] [27]

2.1.7 Kiberkockázat és illegális folyamatok, kiberbiztonsági intézkedések

A mai digitális világban a technológia pénzügyi rendszerekbe történő integrálása óriási hatékonyságnövekedést eredményez, ugyanakkor ezekkel a fejlesztésekkel új kockázatok és kihívások is megjelennek, különösen a pénzmosás elleni (AML) területen. A kiberbiztonság alapvető szerepet játszik a pénzmosás elleni küzdelemben, mivel védi a pénzügyi intézményeket és ügyfeleiket a kiberveszélyektől. A pénzügyi intézményeket különféle tényezők kockáztatják: nemcsak az automatizálásból és digitalizációból eredő, a csalásra és pénzügyi bűncselekményekre való sebezhetőség, hanem a tranzakciós volument növelő tendencia is. A kiberbűnözés és a rosszindulatú feltörések gyakorisága is fokozódott; a digitális szolgáltatások a mindennapi élet részévé váltak, és mivel egyre több polgár vesz részt online tevékenységekben, az információ- és pénzmozgások egyre inkább határokon átívelővé válnak. A COVID-19 járvány felgyorsította az ügyintézés

digitalizációját, például az online ügyfélazonosítást, számlanyitást és fizetéseket, miközben a közösségi médián keresztüli csalások jelentősen megszaporodtak; ez a változás a pénzmosási környezetet is átalakította, különösen a digitális bankolás, a fizetési platformok és a távoli tranzakciók terjedésével. A pénzügyi intézmények kötelesek érzékeny információkat gyűjteni és tárolni ügyfeleikről és tranzakcióikról, és ezeknek a rendszereknek a sebezhetősége adatvédelmi incidensekhez vezethet. Az intézményeknek megfelelő kiberbiztonsági intézkedéseket kell bevezetniük az adatok, rendszerek, eszközök és hálózatok illetéktelen hozzáférés elleni védelmére, továbbá biztosítaniuk kell az információk bizalmasságát, sértetlenségét és rendelkezésre állását. Emellett a hatékony, folyamatosan fejlesztett csalás- és kiberkockázat kezelés rendszeres belső kockázatértékelést és a kontrollkeret folyamatos kiigazítását követeli meg. Bár az információbiztonsági kockázatok az egyedi megvalósítástól és rendszerektől függően eltérhetnek, az AML-folyamatokhoz kapcsolódóan több általános kockázat ismert: adatszivárgás, vagyis az ügyfél érzékeny adataihoz, személyazonosító adatokhoz és pénzügyi nyilvántartásokhoz, való illetéktelen hozzáférés vagy azok nyilvánosságra kerülése, amelyet a támadók bűncélokra használhatnak fel vagy eladhatnak a dark weben. Elégtelen ügyfélazonosítás, amely hamis ügyfélfiókok létrejöttéhez vezethet, lehetővé téve a pénzmosók számára valódi személyazonosságuk elrejtését; rendszer-sebezhetőségek, amikor az AML-rendszerek malware, adathalászati támadások vagy zsarolóvírusok révén sérülnek, ami jogosulatlan hozzáféréshez, az integritás kompromittálásához vagy a működés megzavarásához vezethet; belső fenyegetések, amikor jogosultsággal rendelkező alkalmazottak vagy más belső szereplők szándékos visszaélései manipulatív vagy kártékony tevékenységekhez vezetnek. Dezinformáció és félretájékoztatás terjedése az online médiában, amely félelmet és bizonytalanságot kelthet; az adatelemzés időbeni hiánya, mivel az AML-rendszereknek a gyanús minták vagy tevékenységek észleléséhez valós idejű megfigyelésre és elemzésre van szükségük, és az elemzési késedelmek vagy hiányosságok miatt potenciális pénzmosási tevékenységek észrevétlenek maradhatnak; valamint a szabályozói megfelelés kockázata, mert az AML-szabályozás folyamatosan változik, és a megfelelés elmulasztása bírságokhoz, jogi következményekhez és reputációs károkhoz vezethet. Minden kiber eseményt gyanús tranzakcióként kell kezelni. A kiberkockázatok mérséklése érdekében a szervezeteknek robusztus biztonsági intézkedéseket kell alkalmazniuk, például titkosítást, hozzáférés-szabályozást, biztonságos adattárolást és rendszeres biztonsági felülvizsgálatokat; a kiberbiztonsági technológiák segíthetnek a pénzügyi tranzakciókban

megjelenő gyanús minták vagy anomáliák felismerésében. Emellett elengedhetetlen a munkatársak képzése, a szigorú ügyfélazonosítási eljárások alkalmazása és az AML-rendszerek folyamatos monitorozása az információbiztonság megerősítése érdekében az AML/CTF folyamatokban. [28] [29] [30]

2.1.8 Esettanulmány: Informatikai sérülékenységek hatása

A Pénzmosás és Terrorizmusfinanszírozás Elleni Szakértői Bizottság (MONEYVAL) Magyarországra vonatkozó legutóbbi értékelései hangsúlyozzák, hogy a hazai pénzügyi szektor AML/CTFrendszereinek hatékonysága nagymértékben függ az informatikai infrastruktúra megbízhatóságától és az adatok teljességétől. E megállapítások különösen relevánsak egy olyan informatikai incidens fényében, amely egy magyarországi közepes méretű hitelintézetnél következett be. A pénzintézet kiléte nem ismert, ugyanakkor az eset részletei jól illeszkednek a MONEYVAL által azonosított rendszerszintű kockázatokhoz. [31] [32]

Az incidens során egy hibás rendszerkapcsolati interfész több napon át akadályozta a tranzakciós adatok betöltését az AML/CTF monitoringrendszerbe. A hiba részleges és nehezen észlelhető adatvesztést okozott, amelynek következtében több ezer tranzakció nem esett át kockázati értékelésen, és több gyanús ügylet késedelmesen jutott el a pénzügyi információs egységhez. A MONEYVAL Fifth Round Mutual Evaluation Report (Ötödik Értékelési Jelentés, 2024) és a Followup Report & Technical Compliance ReRating (Nyomonkövetési Jelentés és Technikai Megfelelési Újraértékelés, 2024) kiemeli, hogy Magyarországon továbbra is jelentős kihívást jelent az adatintegritás, a bejelentések minősége és az AML/CTF monitoring tényleges működési hatékonysága.

A vállalatirányítási struktúra hiányosságai tovább súlyosbították a helyzetet. Az informatikai és AML/CTF kockázatok elkülönült kezelése miatt nem volt egyértelmű felelőse annak, ki értékeli az AML/CTF funkciók működőképességét egy technológiai zavar során. A hitelintézet üzletmenetfolytonossági tervei nem tartalmaztak AML/CTFspecifikus forgatókönyveket, így nem állt rendelkezésre olyan eljárás, amely biztosíthatta volna a monitoring átmeneti fenntartását. Ez a hiányosság különösen jelentős annak fényében, hogy a MONEYVAL következetesen hangsúlyozza a kockázatkezelési kultúra és a szervezeti együttműködés fontosságát.

A legkritikusabb tanulság az automatizált rendszerek túlzott dominanciájára vonatkozik. A névtelenül kezelt hitelintézet teljes mértékben automatizált AML/CTF monitoringra támaszkodott, és nem tartott fenn manuális kompenzáló kontrollokat, amelyek informatikai incidens esetén átmenetileg pótolhatták volna a kieső funkciókat. A MONEYVAL értékelései szerint a magyar pénzügyi szektorban továbbra is kihívást jelent a monitoringfolyamatok tényleges hatékonyságának biztosítása, különösen akkor, amikor az adatok teljessége vagy időszerűsége sérül.

Összességében az eset megerősíti, hogy az AML/CTF kontrollrendszerek működőképessége szorosan összefügg az informatikai infrastruktúra minőségével, az adatintegritással és az operációs ellenállóképességgel. A MONEYVAL által feltárt rendszerszintű kihívások és a konkrét, nyilvánosságra nem hozott hitelintézeti incidens együttesen jelzik, hogy a pénzügyi intézményeknek a technológiai és megfelelési funkciókat integrált módon kell kezelniük, és a reziliencia biztosítása érdekében elengedhetetlen a manuális szakmai kompetenciák és alternatív kontrollmechanizmusok fenntartása. [31] [32]

2.1.9 Fenyegetési térkép és hatása a kritikus infrastruktúrában

- A digitalizáció következményei: online ügyfélazonosítás, digitális számlanyitás, mobil- és platformalapú fizetések növelik a tranzakciós volumeneket és a határokon átívelő pénzmozgásokat, ezáltal új támadási felületeket teremtenek.
- Pénzügyi bűncselekmények evolúciója: a rétegzés és integráció digitális eszközökkel válik kifinomultabbá; kripto-eszközök, fintech platformok és harmadik fél szolgáltatók facilitálják a gyors és nehezen visszakövethető tranzakciókat.
- Kibertámadások és insider kockázatok: adatlopások, rendszertámadások, jogosultságok visszaélése közvetlenül rontják az AML mechanizmusok hatékonyságát és integritását.
- Nemzetbiztonsági következmények: a pénzmosás és terrorizmusfinanszírozás alááshatja a pénzügyi rendszer stabilitását, szolgáltatáskimaradások révén hatással van energetikai, közlekedési és kommunikációs kritikus rendszerekre.

2.1.10 A mesterséges intelligencia és analitika a kritikus infrastruktúrában

Az MI kulcsszerepet játszik a pénzügyi és hálózati rendszerek védelmében. Főbb alkalmazásai: anomáliák felismerése, ügyfélprofilok elemzése, tranzakciós hálók feltérképezése, automatikus SAR előszűrés, valamint rugalmas szabályrendszerek kialakítása. Modellarchitektúrák és adatigények:

- Kombinált tanulási módszerek: szabályalapú riasztások és gráfelemzés a rejtett minták feltárására.
- Heterogén adatok: ügyféladatok, tranzakciós idősorok, hálózati telemetria, nyilvános források, szankciós és PEP listák.
- Magyarázhatóság: auditálható döntések, emberi ellenőrzési pontok.

Implementációs kihívások:

- Adatminőség, historikus torzítások, false positive/negative riasztások kezelés.
- Valós idejű követelmények és skálázhatóság.
- Jogszabályi megfelelőség és adatok védelme az ML folyamatban.

Az MI képes összekapcsolni kiberbiztonsági eseményeket és pénzügyi anomáliákat, így hatékonyabbá téve a visszaélések feltárását.

2.1.11 Kibernetikus csalás

A kibereszközökkel elkövetett csalások egy növekvő, nemzetközi szervezett bűnözési forma. Ezek a bűnszövetkezetek gyakran jól szervezett, specializált alcsoportra tagolódnak, amelyek között a pénzmosás is jelentős szerepet kap; ugyanakkor előfordul, hogy lazábban szerveződnek és több joghatóságra kiterjedően, decentralizáltan működnek. Mivel a bűncselekményekből származó bevételek több harmadik ország pénzügyi rendszerén keresztül mosódhatnak tisztára, a pénzügyi átvilágítási keretrendszer, (Customer Enhanced Framework, továbbiakban: CEF) tevékenységek vizsgálata különösen bonyolulttá válik. A digitalizáció lehetővé tette, hogy a kiberes csalók nagyságrendekkel növeljék illegális tevékenységeik volumenét, kiterjedését és sebességét; a közösségi média és az üzenetküldő platformok révén határokon átnyúlóan toboroznak pénzküldő bérlogisztikákat (money mule-okat), gyakran nagy léptékben. A virtuális magánhálózatok (VPN) és az anonim kommunikációs hálózat (The Onion Router, továbbiakban: Tor) használata anonimitást biztosít az elkövetőknek, megnehezítve a hatóságok számára azonosításukat és a pénzmosási tevékenységek feltárását. A bevételek gyorsan moshatók tisztára egy számlahálózaton keresztül, amely gyakran több joghatóságra és pénzintézetre terjed ki. A joghatóságoknak többoldalú

együttműködésre van szükségük ahhoz, hogy hatékonyan és gyorsan észleljék és megakadályozzák a határokon átnyúló CEF-bevételek tisztára mosását; ennek érdekében hasznos meglévő többoldalú mechanizmusokra (például INTERPOL) támaszkodni és azokat támogatni a gyors nemzetközi együttműködés és információcsere érdekében. Az INTERPOL globális adatbázisokat tart fenn a bűnözőkről és bűncselekményekről, továbbá operatív és igazságügyi támogatást nyújt pénzügyi bűnözés és korrupció megelőzéséhez, a terrorizmus elleni küzdelemhez, a kiberbűnözés és a szervezett bűnözés elleni fellépéshez.

2.1.12 Illegális pénzügyi mozgások megakadályozása

Az első erős, kollektív elköteleződés a nemzetközi szervezett bűnözés és hálózataik elleni fellépésre az Egmont Csoport, a FATF és az INTERPOL közös projektje. Az Egmont Csoport a pénzügyi információs egységek nemzetközi fóruma, amely a pénzügyi információs egységek együttműködését hivatott előmozdítani a pénzmosás elleni küzdelemben. A nemzetközi illegális pénzáramlások és a megtévesztő társadalmi mérnökségi módszerek számos különböző bűnözési típushoz vezethetnek: üzleti e-mailes csalás (BEC), amikor e-mailes utasítások alapján az áldozatokat új fizetési számlákra történő átutalásra kérik; adathalászat, amely során az áldozatokat érzékeny adatok — személyes adatok, banki adatok vagy fiókbelépési hitelesítő adatok — kiadására csábítják, amelyeket az elkövetők aztán a pénz kifosztására, új számlák nyitására vagy hamis tranzakciókra használnak; közösségi média és távközlési személyesítő csalások, amikor a bűnözők mobilon vagy közösségi alkalmazásokon keresztül kormányzati tisztviselőnek, rokonnak vagy barátnak kiadva magukat az érzelmekre hatva kényszerítik az áldozatot fizetésre vagy a számlák átadására, illetve pénzügyi műveletek végrehajtására; online kereskedési/platform csalások, ahol hamis hirdetések vagy tanácsadók csalják be az áldozatokat nem létező vagy csalárd kereskedési és befektetési platformokra; online romantikus csalások, amikor az áldozatot romantikus viszony felmutatásával ráveszik pénzküldésre; valamint álláscsalások, ahol hamis állásajánlatokkal csalják el az embereket és különböző ürügyekkel pénzt kérnek tőlük. Ennek következtében az elkövetők különféle technikákkal és informatikai eszközökkel lopják el vagy hamisítják meg személyazonosságokat, többek között adathalászattal, vásárlással vagy azzal, hogy valakit megtévesztenek és önként átadják személyazonosságukat. Az egyik ilyen technológiai eszköz a deepfake; gépi tanulási algoritmusok segítségével a csaló létrehozhat valakinek a hang- vagy videóhamisítványát,

amely telefonon vagy biometrikus hitelesítési rendszerekben való személyesítésre használható. Az elkövetők ezeket az ellopott vagy hamisított identitásokat felhasználva közvetlenül létrehozhatnak és irányíthatnak számlákat, ami megnehezíti a pénzmosási tevékenységek felderítését, mivel a számlatulajdonosok gyakran nincsenek tudatában az érintettségüknek. Az INTERPOL Global Crime Trend Report 2022 szerint az online csalások a kiberbűnözési trendek közül globálisan olyan fenyegetésnek minősülnek, amelyet „magas" vagy „nagyon magas" kockázatúnak tartanak. [33]

2.1.13 Gépi tanulás

A FATF tanulmánya alapján a magán- és közületi tapasztalatok azt mutatják, hogy a csalás elleni és az AML folyamatok kiegészítik egymást. A csalásmegelőző intézkedések közé tartozik a technológia alkalmazása a felhasználók automatikus védelmére a hamis üzenetek ellen, fiókbiztonsági funkciók, kontrollok és szabályok létrehozása, vírusirtó figyelmeztetések a lehetséges adathalász oldalakra, valamint a tranzakciók valós idejű monitorozásának bevezetése. A CEF és az azzal összefüggő pénzmosás hatékony megelőzése nemzeti és nemzetközi szinten valósul meg, miközben a megelőző és detektív kontrollintézkedéseket tovább erősítik az alábbiak szerint. A hazai koordináció erősítése a köz- és magánszféra között: a joghatóságoknak koordinációs mechanizmusokat kell kialakítaniuk a releváns illetékes hatóságok összefogására a CEF és a kapcsolódó bevételek tisztára mosása elleni fellépésre; ez magában foglalja a technikai kiberbűnözési szakértőket és a hagyományostól eltérő szereplőket, például közösségi médiaplatformokat, e-kereskedelmet, telekommunikációs és internetszolgáltatókat. A joghatóságoknak ki kell használniuk a köz- és magánszféra partnerségeit a felismerés és a nyomozások javítására, valamint az operatív vagyonvisszaszerzési intézkedések felgyorsítására. Jó gyakorlatként ajánlott egy dedikált, központosított egység létrehozása, amely kontrollálja a releváns információkat és koordinálja a tevékenységeket a különböző köz- és magánszektorbeli szereplők között, beleértve a nyomozásokat, vagyonvisszaszerzést és csalásmegelőzést. A többoldalú nemzetközi együttműködés támogatása: a joghatóságoknak együtt kell működniük a CEF-bevételek gyors elfogására; a beavatkozás általában a leghatékonyabb egy CEF-eseményt követő 24–72 órán belül. A CEF-bevételek több joghatóságon átmosódva történő visszakövetése és visszaszerzése érdekében globális, egységes megközelítés szükséges. Ennek érdekében a joghatóságoknak ki kell használniuk és támogatniuk kell a meglévő (és jövőbeli) többoldalú mechanizmusokat (például az INTERPOL I-GRIP programját és az Egmont

Csoport BEC projektjét) a gyors nemzetközi együttműködéshez és információcseréhez a CEF elleni küzdelemben; az ilyen többoldalú mechanizmusok lehetővé teszik a joghatóságok számára, hogy együttműködjenek és kollektívan felszámolják a nemzetközi CEF-bűnszindikátusokat. A detektálás és megelőzés megerősítése: a felismerés javítása érdekében a joghatóságoknak biztosítaniuk kell az áldozatok számára az egyszerű bejelentési lehetőségeket, például dedikált, egyszerűsített bejelentési platformok létrehozását; emellett együtt kell működniük a magánszektorral a gyanús tranzakciók bejelentésének javítása érdekében. A joghatóságoknak népszerűsíteniük kell a tudatosságot és éberséget a CEF-pel szemben közoktatási kampányokkal, a CEF jellegzetes jeleinek megosztásával és a kiberismeretek erősítésével; a megelőzés kulcsszerepet játszik a CEF-szervezetek általános nyereségességének csökkentésében. A joghatóságok a magánszektori szereplőkkel együttműködve támogathatják a CEF-megelőzési stratégiákat, ideértve a fogyasztóvédelmi intézkedéseket és a bűncselekményi eszközök eltávolítását.

2.1.14 Közösségi finanszírozás

A közösségi finanszírozás (crowdfunding) egy innovatív adománygyűjtési megoldás, amelyet világszerte használnak emberek ötletek, projektek vagy üzleti vállalkozások támogatására. Bár a közösségi finanszírozási tevékenységek túlnyomó többsége jogszerű, a Pénzügyi Akció Munkacsoport (FATF) kutatásai szerint az etnikai vagy faji alapon motivált terrorista személyek és csoportok visszaéltek ezzel a lehetőséggel, hogy pénzt gyűjtsenek terrorizmus finanszírozására.

A FATF jelentése négy fő visszaélési módot azonosít, amelyek révén a közösségi finanszírozási platformokat TF célokra használhatják:

1. Humanitárius, jótékonysági vagy nonprofit célokkal való visszaélés: Ezek a célok hatékony fedést nyújthatnak pénzügyi támogatás kérésére, és bizonyos esetekben TF célokra használják őket.
2. Dedikált crowdfunding platformok vagy weboldalak használata: EoRMT személyek és csoportok ilyen platformokon keresztül gyűjtenek pénzt különféle tevékenységekre — egyesek jogilag védettek, mások gyűlöletet vagy erőszakot propagálnak.

3. Közösségi média platformok és üzenetküldő alkalmazások használata: A terroristák stratégiailag használják ezeket a csatornákat TF célokra, kampánylinkeket és fizetési utasításokat osztanak meg követőikkel, támogatókat toboroznak, tanácsokat adnak a hatóságok elkerülésére, és kihasználják az olyan funkciókat, mint a titkosítás, hogy érzékeny adatokat továbbítsanak.
4. Közösségi finanszírozás és virtuális eszközök (VA) összekapcsolása: A digitális fizetési formák globális fejlődésével párhuzamosan a crowdfunding iparág is beépítette a VA-hoz kötött finanszírozási lehetőségeket. Bár a Bitcoin a legismertebb, egyre több figyelmet kapnak az olyan alternatívák, mint a „privacy coin”-ok, amelyek egyedi kihívásokat jelentenek a nyomozóhatóságok számára.

A gyakorlatban a bűnözők és terroristák többféle módszert és technikát kombinálnak a pénzgyűjtéshez. Bár egyes joghatóságok és iparági szereplők proaktívan lépéseket tesznek e kockázatok mérséklésére, az AML/CFT szabályozás világszerte nem egységes. A crowdfunding műveletek összetettsége, az adatok hiánya és az anonimizáló technikák alkalmazása tovább nehezíti a nyomon követést a bűnüldöző szervek, jelentéstételi kötelezettséggel rendelkező szervezetek és felügyeleti hatóságok számára. Ezért a közösségi finanszírozásban érintett joghatóságoknak és szereplőknek azonosítaniuk és megérteniük kell a TF-hez kapcsolódó kockázatokat, és kockázatalapú intézkedéseket kell bevezetniük a lehetséges visszaélések megelőzése érdekében.

A digitális átalakulás elkerülhetetlenül új kiberbiztonsági fenyegetésekhez vezetett, különösen a COVID–19 világjárvány és az ukrajnai háború következtében. A megváltozott politikai és gazdasági környezet új lehetőségeket teremtett a kiberbűnözők számára, miközben a pénzmosás és a terrorizmusfinanszírozás elleni (AML/CTF) jogszabályoknak való megfelelés kulcsfontosságú a pénzügyi szektor védelme szempontjából.

A kibereszközökkel elkövetett csalások (CEF) várhatóan tovább növekednek a digitalizáció globális térnyerésével. A joghatóságoknak fel kell készülniük azokra a sebezhetőségekre, amelyeket a bűnözők különböző ágazatokban kihasználhatnak a pénzmosási technikák fejlesztésére. A megelőző és detektív kontrollok fontossága mellett és a CEF decentralizált jellege miatt, elengedhetetlen a különböző szektorok és szereplők közötti együttműködés megerősítése nemzeti és nemzetközi szinten egyaránt.

A megbízható AML/CTF szabályzatok és eljárások, valamint az erős kiberbiztonsági intézkedések bevezetése alapvető fontosságú a pénzügyi rendszer biztonságának, stabilitásának, megbízhatóságának és integritásának megőrzésében. A hatás azonban nem korlátozódik pusztán pénzügyi veszteségekre, a társadalmi és gazdasági következmények is súlyosak lehetnek.

Magyarország folyamatosan dolgozik AML/CTF belső kontrollrendszerének megerősítésén annak érdekében, hogy fokozza az ügyfelek és az egész pénzügyi szektor biztonságát. Az Európa Tanács pénzmosás elleni testülete, a MONEYVAL által készített követő jelentés alapján Magyarország jelentős előrelépést mutatott a FATF-ajánlásoknak való megfelelés terén. [34]

2.1.15 Összegzés

Második hipotézis: A pénzmosási kockázatok és következmények beépítése a kritikus infrastruktúra informatikai védelmi architektúrájába csökkentheti az üzleti folyamatok manipulációjából eredő szolgáltatásmegtagadási kockázatokat.

Az informatikai adatok (tranzakciók, rendszerlogok, hozzáférési események) MI-alapú összefüggéselemzése korai előrejelzést tesz lehetővé a pénzügyi visszaélésekhez vezető tevékenységekre, és ezzel megelőzhetőek a másodlagos hatások (pl. koordinált támadások, visszaélések) a kritikus rendszerekre.
Ezért a pénzmosási kockázatok beépítése nemcsak biztonsági, hanem stratégiai előnyt is jelentenek.

A második hipotézis validálható: a pénzmosási kockázatok informatikai integrációja valóban csökkenti a szolgáltatásmegtagadási és reputációs kockázatokat, különösen kritikus infrastruktúrák esetében, ahol a pénzügyi visszaélések rendszerszintű hatásokat okozhatnak.

3 A MONITOROZÁS FONTOSSÁGA

Az informatikai rendszerek monitorozása a folyamatos működésnek egyik legkritikusabb biztonsági és üzemeltetési pillére, mivel a digitális infrastruktúrák összetettsége, összekapcsoltsága olyan környezetet hoz létre, amelyben a hibák, anomáliák vagy rosszindulatú tevékenységek korai felismerése nélkülözhetetlen a működőképesség fenntartásához. Az informatikai monitoring nem csupán technikai felügyeletet jelent, hanem egy olyan folyamatos, adatvezérelt megfigyelési és értékelési folyamatot, amely képes a rendszerállapotok, teljesítménymutatók, hálózati forgalom és biztonsági események adatinak megjelenésére. Ennek révén az üzemeltetők nemcsak gyorsabban reagálhatnak az incidensekre, hanem proaktív módon azonosíthatják a rejtett sérülékenységeket, kapacitásproblémákat vagy konfigurációs eltéréseket is. A monitoringrendszerek által biztosított valós idejű láthatóság és adatelemzés lehetővé teszi a trendek felismerését, a prediktív karbantartást és a kockázatalapú döntéshozatalt, ami fontos a magas rendelkezésre állást, üzembiztonságot és megfelelőséget megkövetelő környezetekben.

3.1 Az infrastruktúra monitorozás a kritikus infrastruktúrában

A kritikus infrastruktúrák esetében az infrastruktúra-monitorozás olyan komplex, felügyeleti tevékenységet jelent, amely a fizikai, informatikai és szolgáltatási komponensek folyamatos állapotértékelésére épül, és amelynek célja a nemzeti, társadalmi és gazdasági működés szempontjából létfontosságú rendszerek zavartalan üzemének biztosítása. Itt a környezetekben a monitorozás nem korlátozódhat a hagyományos informatikai szemléletre, mivel a fizikai infrastruktúra (energiaellátás, víziközművek, közlekedési rendszerek, banki szolgáltatások stb.) és a digitális vezérlőrendszerek szoros integrációja olyan összetett kockázati térképet eredményez, ahol egyetlen komponens meghibásodása vagy kompromittálódása láncreakciót indíthat el. A kritikus infrastruktúrák monitorozása ezért magában foglalja a környezeti paraméterek, fizikai állapotváltozások, hálózati forgalom, vezérlési parancsok, hozzáférési mintázatok és szolgáltatási teljesítménymutatók együttes, valós idejű elemzését. A cél nem csupán az incidensek detektálása, hanem a működési anomáliák korai előrejelzése, a szolgáltatás-folytonosság biztosítása még extrém terhelés, kibertámadás vagy fizikai meghibásodás esetén is. A kritikus infrastruktúrák sajátossága, hogy a monitorozási adatok nemcsak technikai, hanem stratégiai jelentőséggel is bírnak: támogatják a döntéshozatalt, a kockázatkezelést, a szabályozói megfelelést. Emiatt az

infrastruktúra-monitorozás nem pusztán operatív feladat, hanem a kritikus rendszerek védelmének egyik legfontosabb, integrált eleme, amely nélkül a modern társadalmak működése kiszámíthatatlanná és sérülékennyé válna.

3.1.1 Történelmi áttekintés

A globálisan összekapcsolt informatikai környezetben az infrastruktúra-felügyeleti eszközök kulcsszerepet játszanak a rendszerek teljesítményének, biztonságának és megbízhatóságának fenntartásában. A technológiai fejlődés, különösen az MI és gépi tanulás (ML) integrációja, új dimenziókat nyitott a proaktív kockázatkezelés és az automatizált válaszintézkedések terén.

Az infrastruktúra-felügyelet fejlődése az alábbi főbb korszakokra bontható:

- 1960-1980 – Manuális ellenőrzés
- 1980-1995 – Szabványosítás
- 1995-2010 – Integrált felügyelet
- 2010-2020 – Teljesítményorientált megközelítés
- 2020- AI/ML alapú automatizálás

Az IT-infrastruktúra felügyeletének fejlődése szorosan összefügg az informatikai biztonság és működési hatékonyság alakulásával. A mesterséges intelligencia és automatizálás révén a szervezetek képesek proaktívan kezelni a kockázatokat, biztosítva a rendszerek megbízhatóságát és védelmét. Az infrastruktúra-monitorozás és automatizálás története jól szemlélteti, hogyan fejlődött a technológia az iparágak változó igényeinek kielégítése érdekében. A kezdeti időszakban a szervezetek nehezen tudták kezelni a folyamatosan bővülő technológiai infrastruktúrájukat, és alapvető, manuális eszközökre támaszkodtak a hálózati felügyelet terén. Ez a helyzet gyökeresen megváltozott az automatizált megoldások megjelenésével, amely fordulópontot jelentett: a vállalatok a reaktív megközelítésről proaktív monitorozásra tértek át. A mesterséges intelligencia integrációja jelentette a következő nagy áttörést, amely intelligens, adaptív monitorozó rendszereket hozott létre. Ezek képesek az adatmintákból tanulni, előre jelezni a problémákat, és dinamikusan reagálni a változó körülményekre. Ez a technológiai ugrás jelentősen növelte a monitorozás sebességét és pontosságát, és az IT-ökoszisztémákat dinamikusabbá, rugalmasabbá tette. Az iparágak szintén jelentős szerepet játszottak ebben az evolúcióban. A digitális korszak térnyerése, valamint a virtualizált környezetekre és felhőalapú platformokra való átállás új kihívásokat teremtett,

amelyek speciális monitorozási megoldásokat igényeltek. Az egészségügyben például a valós idejű monitorozás kulcsfontosságúvá vált a kritikus alkalmazások teljesítményének és rendelkezésre állásának fenntartása érdekében. Ezzel párhuzamosan a pénzügyi szektorban a nagy mennyiségű érzékeny adat védelmére alkalmas monitorozó eszközök iránti igény biztonságközpontú fejlesztéseket eredményezett. Ezen iparágspecifikus dinamikák vizsgálata értékes betekintést nyújt az infrastruktúra-monitorozás és automatizálás fejlődését mozgató erőkbe. Ez a történeti kontextus elengedhetetlen ahhoz, hogy megértsük, miként formálták az iparágak a modern IT-infrastruktúra menedzsmentet. Az alkalmazási trendek további tisztánlátást biztosítanak abban, hogyan fogadták be a szervezetek ezeket a technológiákat. Ahogy a vállalatok felhőalapú infrastruktúrákra tértek át, olyan monitorozó megoldásokat kerestek, amelyek képesek kezelni a dinamikus felhőkörnyezeteket. A felhő-natív monitorozó eszközök széles körű elterjedése kulcsfontosságú trenddé vált, mivel a szervezetek elsődleges célja az alkalmazások teljesítményének, rendelkezésre állásának és biztonságának biztosítása lett a felhőben. Azáltal, hogy megvizsgáljuk, hogyan navigáltak a szervezetek ezen alkalmazási fázisokon keresztül, jobban megérthetjük az infrastruktúra-monitorozás és automatizálás átfogó trendjeit, valamint azokat a stratégiai döntéseket, amelyek meghatározták az IT-menedzsmentet a digitális korszakban. [35] [36]

3.1.2 Kulcsfontosságú felügyeleti eszközök

A SIEM rendszerek naplóadatokat gyűjtenek, korrelálnak és elemeznek valós időben. Kiemelt példák:

- IBM QRadar.
- Splunk Enterprise Security.
- ArcSight.

Ezek képesek a fenyegetések azonosítására, incidenskezelésre és megfelelőségi jelentések generálására. A SIM rendszerek a biztonsági állapot folyamatos figyelésére szolgálnak, gyakran SIEM-mel integrálva. Céljuk a biztonsági események gyors észlelése és dokumentálása. Az APM eszközök az alkalmazások teljesítményét monitorozzák, beleértve a válaszidőt, hibaarányt és tranzakciós metrikákat. Példák:

- Dynatrace.
- AppDynamics.
- DX APM.

Az MI és ML integrációja új lehetőségeket teremtett:
Predektív detektálás: viselkedéselemzés
Anomáliafelismerés: Statikus szabályok helyett dinamikus minták
Automatizált válasz: SOAR platformok (pl. Palo Alto Cortex XSOAR)

Ezek a megoldások csökkentik a téves riasztások számát, gyorsítják az incidens-válaszokat, és növelik az infrastruktúra ellenállóképességét. A nagy mennyiségű adat valós idejű feldolgozása, a gyorsan változó fenyegetések és a komplex rendszerek miatt elengedhetetlen az eszközök integrált alkalmazása. A SIEM, SIM, APM és MI-alapú megoldások együttesen:

- Optimalizálják a biztonsági stratégiákat.
- Növelik az üzemeltetési hatékonyságot.
- Biztosítják a kritikus infrastruktúrák védelmét. [36]

3.1.3 Kritikusinfrastruktúrák szerepe és védelme

A kritikus infrastruktúrák alapvető fontosságúak a modern társadalom működése szempontjából, mivel olyan létfontosságú szolgáltatásokat támogatnak, mint az elektromos energia, a víz- és gázellátás, a közlekedés, a kommunikációs hálózatok, valamint az egészségügyi és pénzügyi rendszerek. E rendszerek számos kockázatnak vannak kitéve, beleértve a kibertámadásokat, természeti katasztrófákat és technikai meghibásodásokat, amelyek súlyos gazdasági és társadalmi következményekhez vezethetnek. Ezért elengedhetetlen a biztonságuk és folyamatos működésük biztosítása a potenciális fenyegetések mérséklése és a stabilitás fenntartása érdekében. A kritikus infrastruktúrák számos biztonsági kihívással szembesülnek. A legfőbb fenyegetések kibertámadók, terroristák, sőt állami szereplők részéről érkezhetnek, akik célja az alapvető rendszerek megzavarása vagy megsemmisítése. A természeti katasztrófák – például viharok, árvizek és földrengések – szintén jelentős kockázatot jelentenek. Emellett az emberi hibák és technikai meghibásodások, ha nem megfelelően kezelik őket, katasztrofális következményekkel járhatnak.

A kritikus infrastruktúrák védelmére széles körű biztonsági megoldások állnak rendelkezésre. A kibertámadások elleni védekezéshez tűzfalak, behatolásérzékelő rendszerek (IDS), valamint biztonsági protokollok alkalmazása szükséges. A természeti katasztrófák esetén elengedhetetlenek a vészhelyzeti felkészülési tervek, a stratégiai

infrastruktúra-elhelyezés, valamint az épületek és berendezések megerősítése. Az emberi hibák és technikai problémák megelőzése érdekében rendszeres ellenőrzésekre, monitorozásra és karbantartásra van szükség. A mai gyorsan változó, technológia-vezérelt világban a folyamatos, 0–24 órás monitorozás kulcsfontosságú az incidensek időben történő azonosításához és kezeléséhez, mielőtt azok súlyosbodnának. A monitorozó eszközök valós idejű megfigyelést tesznek lehetővé, korai riasztásokat biztosítanak a biztonsági fenyegetésekről, a rendszer teljesítményéről és rendelkezésre állásáról. Ezek az eszközök a rendszeroptimalizálásra is alkalmazhatók. Az MI-alapú monitorozó eszközök egyre fontosabbá válnak, mivel automatizálást és olyan elemzési képességeket kínálnak, amelyek csökkentik a téves riasztások számát és növelik az üzemeltetési hatékonyságot. Ahogy az infrastruktúrák egyre összetettebbé válnak, az MI és az automatizálás integrációja a monitorozó rendszerekbe elengedhetetlenné válik a hatékonyság növelése érdekében. Az MI lehetővé teszi a prediktív fenyegetésdetektálást, az anomáliák azonosítását és az automatizált válaszintézkedéseket, ezáltal csökkentve az emberi beavatkozás szükségességét és egyszerűsítve az üzemeltetést. Az MI által nyújtott prediktív betekintések segítenek a téves riasztások csökkentésében és a gyökérok-elemzés pontosságának javításában, ami gyorsabb problémamegoldást tesz lehetővé. A hatékony monitorozó rendszerek számos IT-folyamatot támogatnak, például az incidenskezelést, problémakezelést, változáskezelést, valamint az adat- és kapacitásmenedzsmentet. Ezek a rendszerek több rétegre terjednek ki, beleértve a hálózati, operációs rendszer, alkalmazás, tároló és adatbázis rétegeket, biztosítva a teljes körű lefedettséget. Az alkalmazásnaplók, metrikák és események automatizált elemzése révén a monitorozó eszközök gyorsan képesek azonosítani a problémákat, minimalizálva a manuális beavatkozást és lehetővé téve az erőforrások optimalizálását.

A monitorozó rendszer részeként az alkalmazásteljesítmény-menedzsment (Application Performance Management, továbbiakban: APM) kulcsszerepet játszik az IT-rendszerek zavartalan működésének biztosításában. Az APM-megoldások nyomon követik az alkalmazások teljes működési folyamatát, a felhasználói interakcióktól a háttérrendszerekig, azonosítva azokat a szűk keresztmetszeteket vagy problémákat, amelyek hatással lehetnek a teljesítményre. Például az APM alkalmazható online áruházak tranzakcióinak monitorozására, észlelve a válaszidő késéseit vagy az adatbázis-lekérdezések hibáit. Ez a képesség különösen fontos nagy forgalmú időszakokban, például ünnepek vagy akciók idején, amikor az automatikus skálázás biztosítja a rendszer

teljesítményének stabilitását. A sikeres monitorozás megköveteli a rendszerarchitektúra mélyreható ismeretét, beleértve az adatbázisokat, szolgáltatásokat, mikroszolgáltatásokat és külső megoldásokat. A mai többplatformos környezetben figyelembe kell venni a mobil eszközöket, webböngészőket és biztonsági védelmeket, például a biometrikus azonosítást vagy PIN-kódokat is. A monitorozó eszközöknek képesnek kell lenniük ezen sokszínű környezetek nyomon követésére a biztonságos és funkcionális rendszer fenntartása érdekében. Ahogy a kritikus infrastruktúra-rendszerek egyre integráltabbá és összetettebbé válnak, a folyamatos monitorozás elengedhetetlen a biztonságuk és teljesítményük biztosításához. A modern monitorozó eszközök – beleértve az MI-t és az automatizálást – alkalmazásával a szervezetek hatékonyan kezelhetik a kockázatokat, optimalizálhatják a teljesítményt, és biztosíthatják a kritikus infrastruktúrák ellenállóképességét. A hatékony monitorozás nem csupán a rendszerállapot nyomon követéséről szól – hanem a proaktív válaszintézkedések lehetővé tételéről, a leállások minimalizálásáról és azoknak az alapvető szolgáltatásoknak a védelméről, amelyek a modern társadalom működését támogatják.

3.1.4 Automatizálási terület fő szempontjai

A monitorozási és automatizálási technológiák fejlődését jelentős mértékben formálták azok a meghatározó iparági szereplők, akik nemcsak úttörő megoldásokat vezettek be, hanem erős piaci jelenlétet is kiépítettek. Az olyan vállalatok, mint az IBM, a Microsoft és a Cisco kulcsszerepet játszottak az iparág meghatározásában átfogó monitorozási és automatizálási portfólióikkal. Különösen a Microsoft emelkedik ki a System Center termékcsaládjával, amely magában foglalja a System Center Operations Manager (SCOM) és a System Center Orchestrator (SCORCH) megoldásokat. Ezek az alapvető eszközök lehetővé teszik a szervezetek számára az infrastruktúra hatékony monitorozását és automatizálását. A SCOM például teljes körű alkalmazás- és infrastruktúra-monitorozást kínál, mély betekintést nyújtva a rendszerek teljesítményébe és általános állapotába. A Microsofthoz hasonló vezető szereplők hatásának megértése kulcsfontosságú, mivel segíti a szervezeteket abban, hogy bevált megoldásokat alkalmazzanak, miközben bővítik a vállalati alkalmazásmonitorozás hatókörét. A meghatározó szereplők mellett új innovátorok is megjelentek, akik friss szemlélettel és új technológiai megoldásokkal alakítják át a hagyományos monitorozási és automatizálási piacot, válaszul az IT-kihívások folyamatos változására. Az olyan cégek, mint a Datadog, a Splunk és a Dynatrace képviselik azt az innovációs lendületet, amely előre viszi az

iparágat. A Datadog például kiemelkedő szereplővé vált a felhőalapú monitorozás és analitika terén, egységes rálátást biztosítva az alkalmazások, szerverek és infrastruktúra teljesítményére. Az új innovátorok hatásának felismerése különösen fontos azoknak a szervezeteknek, amelyek sokszínű, az egyedi IT-igényeikhez igazított megoldásokat keresnek. A monitorozási és automatizálási szektoron belüli együttműködések dinamikus ökoszisztémát hoznak létre, ahol a közös fejlesztési erőfeszítések elősegítik a legkorszerűbb megoldások integrációját. A hardvergyártók, szoftverfejlesztők és felhőszolgáltatók közötti partnerségek olyan együttműködési környezetet teremtenek, amely fokozza a technológiai képességeket. Például a Cisco és vezető felhőszolgáltatók közötti együttműködések eredményeként integrált, felhőalapú monitorozási megoldások jöttek létre. E stratégiai partnerségek értékének megértése segíti a szervezeteket abban, hogy olyan monitorozási és automatizálási megoldásokat válasszanak, amelyek összhangban állnak átfogó IT-stratégiájukkal. [40]

3.1.5 A főbb biztonsági monitoring eszközök szerepe a védelemben

A hatékony monitorozás minden informatikai környezet alapköve. A biztonsági információmonitorozás (Security Information Monitoring – SIM) területén számos fejlett eszköz áll rendelkezésre, amelyek segítik a szervezeteket a kritikus infrastruktúrák kibertámadásokkal szembeni védelmében. Ezek az eszközök különböző IT-rendszerekkel integrálódnak, valós idejű monitorozást, fenyegetésdetektálást és válaszintézkedéseket biztosítanak.

- **Microsoft Azure Sentinel**

Az Azure Sentinel a Microsoft által fejlesztett, felhőalapú Security Information and Event Management (SIEM) megoldás, amely mesterséges intelligenciát (MI) és gépi tanulást (ML) alkalmaz a biztonsági fenyegetések valós idejű felismerésére, kivizsgálására és kezelésére. Felhőalapú platformként skálázhatóságot, rugalmasságot és zökkenőmentes integrációt kínál a Microsoft-megoldásokkal és külső eszközökkel egyaránt. Az Azure Sentinel MI-alapú fenyegetésdetektálási képességei lehetővé teszik az anomáliák és potenciális támadások pontosabb azonosítását. Folyamatosan gyűjti és elemzi az adatokat különböző forrásokból, mint például hálózati forgalomból, alkalmazásokból és végpontokból, és valós idejű biztonsági analitikát nyújt. Emellett előre definiált „playbookok” segítségével automatizálja a válaszintézkedéseket, jelentősen csökkentve a biztonsági csapatok manuális terhelését. Az Azure Monitor különösen fontos szerepet

játszik a riasztások finomhangolásában. A rendszergazdák küszöbértékeket állíthatnak be annak érdekében, hogy csak valódi problémák váltsanak ki értesítéseket, csökkentve a riasztási zajt és gyorsítva a valódi problémák azonosítását. Az Azure Monitor nemcsak a felhőinfrastruktúra adatainak elemzését támogatja, hanem felhasználói szinten is beavatkozik, MI-alapú segítséggel. A riasztások konfigurálásakor elengedhetetlen a megfelelő metrikák kiválasztása és a küszöbértékek pontos beállítása. Ezek rendszeres felülvizsgálata biztosítja, hogy a rendszerek az elvárt paraméterek között működjenek. A riasztási szabályok kulcsfontosságú elemei a rendszernek, mivel aktiválásuk esetén különböző műveleteket indítanak el – akár MI-alapú beavatkozással is. Az Action Group automatizálja az értesítési folyamatot (SMS, e-mail, push-értesítés), és integrálható például az Opsgenie szolgáltatással. A riasztások 30 napig kerülnek megőrzésre, majd automatikusan törlésre kerülnek.

- **Splunk**

A Splunk az egyik legismertebb biztonsági információmonitorozási eszköz, amely kiválóan alkalmas gépi adatok gyűjtésére, indexelésére és elemzésére különböző forrásokból. A biztonsági csapatok számára értékes betekintést nyújt a potenciális sebezhetőségekbe. A Splunk képes adatokat fogadni alkalmazásokból, operációs rendszerekből, hálózati eszközökből és felhőkörnyezetekből. Fejlett analitikai képességei révén valós idejű fenyegetésfelderítést biztosít, segítve az összetett támadási minták azonosítását. Testreszabható irányítópultjai lehetővé teszik a biztonsági szakemberek számára, hogy az eszköz felületét saját igényeikhez igazítsák. A Splunk zökkenőmentesen integrálható számos biztonsági eszközzel és platformmal, és magas szintű skálázhatóságot kínál, így kisvállalatok és nagyvállalatok számára egyaránt alkalmas.

- **IBM QRadar**

Az IBM QRadar egy átfogó SIEM eszköz, amely valós idejű biztonsági intelligenciát és automatizált incidensdetektálást biztosít. Kiemelkedik az erőteljes adatgyűjtési, elemzési és korrelációs képességeivel. A QRadar integrálható fenyegetési intelligenciaforrásokkal, így segíti az új fenyegetések azonosítását. A platform normalizálja a különböző forrásokból származó adatokat, megkönnyítve az incidensek korrelációját és azonosítását. Automatizálja a biztonsági események detektálását, priorizálását és kezelését, gyorsabb és hatékonyabb válaszadást biztosítva. Előre konfigurált jelentései

segítik a szervezeteket a megfelelőségi követelmények teljesítésében – különösen az egészségügyi és pénzügyi szektorban.

- **LogRhythm**

A LogRhythm egységes platformot kínál SIEM, naplókezelés és hálózatmonitorozás céljára, azzal a céllal, hogy a biztonsági csapatok gyorsabban észleljék és kezeljék a fenyegetéseket. A platform folyamatosan monitorozza a szervezet hálózatán áthaladó adatokat, valós idejű incidensdetektálást biztosítva. Kiemelkedő funkciója a User and Entity Behavior Analytics (UEBA), amely segít az insider fenyegetések azonosításában a felhasználói vagy entitásviselkedésben mutatkozó anomáliák alapján. A LogRhythm automatizált válaszintézkedéseket is kínál, csökkentve a fenyegetések kezeléséhez szükséges időt. Széles körű integrációs lehetőségei révén egységes képet nyújt a szervezet biztonsági állapotáról.

- **Rapid7 InsightIDR**

A Rapid7 InsightIDR egy SIEM eszköz, amely a biztonsági incidensek monitorozására, detektálására és kezelésére fókuszál. Egyszerűsíti a biztonsági műveleteket, miközben értékes információkat nyújt a biztonsági csapatok számára. A platform Endpoint Detection and Response (EDR) képességeket integrál, lehetővé téve a végponti aktivitás nyomon követését – ez kulcsfontosságú az ún. „advanced persistent threat” (APT) típusú támadások azonosításához. Az InsightIDR viselkedéselemzést alkalmaz a rosszindulatú tevékenységek – például szokatlan bejelentkezések vagy jogosultságemelések – felismerésére, és folyamatos monitorozást, valamint automatizált válaszokat kínál a sebezhetőségek gyors kezelésére. Felhőszolgáltatásokkal való jó integrációja miatt hibrid és felhőalapú környezetekben is jól alkalmazható.

- **Zabbix**

A Zabbix egy nyílt forráskódú monitorozási megoldás, amely IT-infrastruktúrák – például hálózatok, szerverek, alkalmazások és felhőszolgáltatások – állapotának és teljesítményének figyelésére szolgál. Valós idejű monitorozást, riasztást és jelentéskészítést biztosít, lehetővé téve az IT-csapatok számára a problémák korai felismerését. A Zabbix skálázható és testreszabható, kiterjedt integrációs lehetőségeket, sablonokat és intuitív webes felületet kínál a monitorozási feladatok kezelésére nagy,

elosztott környezetekben. Közepes és nagyvállalatok számára ideális, akik ingyenes, mégis robusztus monitorozási megoldást keresnek.

4. ábra: Zabbix nyílt forráskodú monitoring rendszer

- **McAfee Enterprise Security Manager (ESM)**

A McAfee Enterprise Security Manager (ESM) egy vállalati szintű SIEM eszköz, amely valós idejű biztonsági monitorozást és fenyegetésdetektálást biztosít. Központosított eseménykezelést, naplógyűjtést és biztonsági analitikát kínál, lehetővé téve a biztonsági csapatok számára az incidensek gyors felismerését és kezelését. A McAfee ESM magas szintű skálázhatóságáról ismert, így különösen alkalmas nagy szervezetek számára, amelyek összetett biztonsági infrastruktúrával rendelkeznek. A kritikus infrastruktúrák elleni kibertámadásokkal szembeni védekezésben elengedhetetlen a robusztus Security Information Monitoring (SIM) eszközök alkalmazása. Ezek a platformok valós idejű rálátást, fenyegetésdetektálást és incidenskezelést biztosítanak, így nélkülözhetetlenek a mai kifinomult kibertámadások elleni védelemben. A megfelelő SIM eszköz kiválasztása a szervezet egyedi igényeitől, a működés méretétől és az infrastruktúra komplexitásától függ. A közös cél azonban minden esetben az, hogy a biztonsági csapatok gyorsan azonosítsák és mérsékeljék a kockázatokat, mielőtt azok súlyos fennakadásokhoz vezetnének. Ezzel szemben az Application Performance Management (APM) az

alkalmazások teljesítményének monitorozására és optimalizálására fókuszál. Az APM eszközök lehetővé teszik a szervezetek számára, hogy proaktívan nyomon kövessék alkalmazásaik állapotát, korán felismerjék a problémákat, és javítsák a teljesítményt a zökkenőmentes felhasználói élmény érdekében. Folyamatosan monitorozzák a kulcsfontosságú metrikákat, mint például a válaszidő, rendelkezésre állás és áteresztőképesség. Az APM gyökérok-elemzést is kínál, segítve a teljesítményproblémák – például lassú adatbázis-lekérdezések vagy nem hatékony kód – pontos azonosítását. Emellett az APM eszközök értékelik a végfelhasználói élményt is, mérve, hogyan lépnek interakcióba a felhasználók az alkalmazással. Ha a teljesítményküszöbök túllépésre kerülnek, az APM rendszerek riasztásokat és diagnosztikát indítanak, valós idejű megoldásokat kínálva. Továbbá optimalizálási javaslatokat is nyújtanak a hatékonyság növelése és a zavartalan működés biztosítása érdekében.

- **Vezető APM és monitorozási megoldások**

Dynatrace: Az egyik vezető APM megoldás, amely mély betekintést nyújt az alkalmazások, infrastruktúra és felhasználói élmény teljesítményébe. Mesterséges intelligenciát alkalmaz az alkalmazás teljes életciklusának monitorozására – a felhasználói élménytől a háttérrendszerekig. Automatikusan észleli a teljesítménybeli szűk keresztmetszeteket, részletes gyökérok-elemzést biztosít, és valós idejű monitorozást kínál a felhő-natív és mikroszolgáltatás-alapú környezetekben.

Datadog: Átfogó monitorozási platformot kínál felhőalkalmazásokhoz. Adatokat gyűjt szerverekből, konténerekből, adatbázisokból és külső szolgáltatásokból. Segíti a DevOps csapatokat a leállások megelőzésében, a teljesítményproblémák kezelésében és az optimális felhasználói élmény biztosításában.

CA Application Performance Management (APM): Valós idejű alkalmazás monitorozásra tervezett eszköz, amely segíti a szervezeteket az alkalmazások teljesítményének kezelésében és optimalizálásában. Teljes képet nyújt az alkalmazás állapotáról, beleértve az infrastruktúrát, hálózati teljesítményt és végfelhasználói élményt. Valós idejű diagnosztikája révén gyors problémakezelést tesz lehetővé.

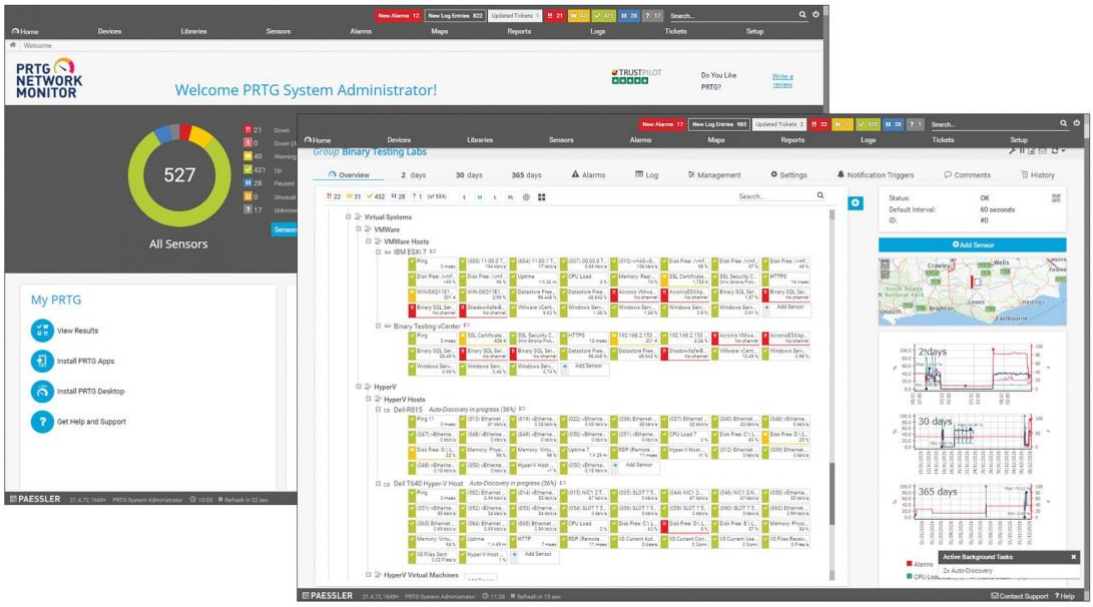
DX Application Performance Management (APM): Fejlett APM eszköz, amely proaktív monitorozást, valós idejű betekintést és részletes gyökérok-elemzést kínál. Segít

az IT-csapatoknak a teljesítményproblémák korai felismerésében, és teljes körű láthatóságot biztosít az alkalmazástranzakciók és mikroszolgáltatások szintjén.

Prometheus & Grafana: A Prometheus egy nyílt forráskódú monitorozó és riasztási eszközkészlet, amely időalapú adatok gyűjtésére szolgál, különösen felhő-natív és mikroszolgáltatásalapú környezetekben. A Grafanával kombinálva erőteljes irányítópultokat és valós idejű metrikákat kínál az alkalmazások teljesítményének és az infrastruktúra állapotának nyomon követésére. Széles körben alkalmazzák Kubernetes klaszterek és konténeres környezetek monitorozására.

Nagios: Az egyik legnépszerűbb nyílt forráskódú monitorozó eszköz, amely hálózati eszközök, szerverek és alkalmazások állapotának és teljesítményének nyomon követésére szolgál. Valós idejű monitorozást, riasztást és jelentéskészítést biztosít. Skálázható, így kis rendszerektől a nagy, elosztott infrastruktúrákig alkalmazható. Széles körű plugin-támogatással bővíthető.

PRTG Network Monitor: Átfogó monitorozó eszköz, amely az IT-infrastruktúra különböző aspektusait figyeli. Hálózatok, szerverek, alkalmazások és infrastruktúra teljesítményét és rendelkezésre állását követi nyomon. Valós idejű monitorozást kínál testreszabható riasztásokkal és értesítésekkel, biztosítva, hogy a problémák időben felismerésre és kezelésre kerüljenek. Könnyen telepíthető és használható, így minden méretű szervezet számára népszerű választás. Széles körű eszköz- és rendszerintegrációs képességei révén sokoldalú megoldást kínál. [37] [38] [39] [42]



5. ábra: *PRTG mint hálózati eszköz*

3.1.6 Megoldások a kiberbiztonsági kockázatok kezelésére

Az ipari vezérlőrendszerek (Industrial Control Systems, továbbiakban: ICS) elleni kiberbiztonsági kockázatok az elmúlt években jelentősen megnövekedtek, elsősorban az állami szereplők és a kibertámadók fokozódó aktivitása miatt. Ezek a támadók egyre kifinomultabb módszereket alkalmaznak, ami megnehezíti az incidensek időben történő felismerését és kezelését. A kiberfenyegetések, amelyek az informatikai (IT) és az ipari vezérlési technológiát (ICT) egyaránt érintik, ma már számos támadási vektoron keresztül jelentkeznek, például:

- zsarolóvírusok (ransomware),
- közműszolgáltatásokat megzavaró kártékony szoftverek,
- vezető beosztású személyek elleni célzott adathalász kampányok,
- üzleti email kompromittálás (Business Email Compromise, továbbiakban BEC),
- adatlopás,
- szociális manipuláció, érzékeny információk kinyerése.

Korszerű védekezési megoldások ICS környezetben:
A folyamatosan fejlődő fenyegetésekkel szembeni hatékony védekezés érdekében az ICS-re szabott kiberbiztonsági megoldásoknak az alábbi képességeket kell integrálniuk:

- valós idejű viselkedési anomáliaészlelés,
- gyorsított incidenskezelés,
- intelligens hálózati vizualizációk az összekapcsolt rendszerek átláthatósága.

A SIEM rendszerek kifejezetten ezen igények kielégítésére szolgálnak: eseményadatokat gyűjtenek, aggregálnak, tárolnak és korrelálnak az infrastruktúra különböző pontjairól. A SIEM rendszerek kulcsszerepet játszanak a modern biztonsági műveleti központokban (Security Operations Center – SOC), mivel képesek különféle szenzorokból – például behatolásérzékelő rendszerekből, tűzfalakból, antivírus szoftverekből – származó eseményeket összegyűjteni és korrelálni, így átfogó képet nyújtanak a potenciális fenyegetésekről. Ezáltal a SIEM rendszerek hatékonyan segítik a biztonsági csapatokat az incidensek felismerésében, kezelésében és jelentésében. [39]

A piacon elérhető SIEM megoldások között jelentős különbségek figyelhetők meg, amelyek az egyes rendszerek képességeiben, erősségeiben és gyengeségeiben mutatkoznak meg. Ezek a különbségek gyakran tükrözik a SIEM rendszerek piaci pozícióját is. Egyes megoldások olyan nagy múltú IT-vállalatoktól származnak, mint az IBM, a McAfee vagy a HP, míg mások – például az AlienVault vagy a Splunk – innovatív funkciókat kínálnak, amelyek a modern kiberbiztonság összetett igényeit célozzák meg.

A SIEM rendszerek jellemzően több összekapcsolt komponensből épülnek fel:

- eseménygyűjtés,
- naplóelemzés és normalizálás,
- szabálymotorok,
- naplótárolás,
- eseményfigyelés.

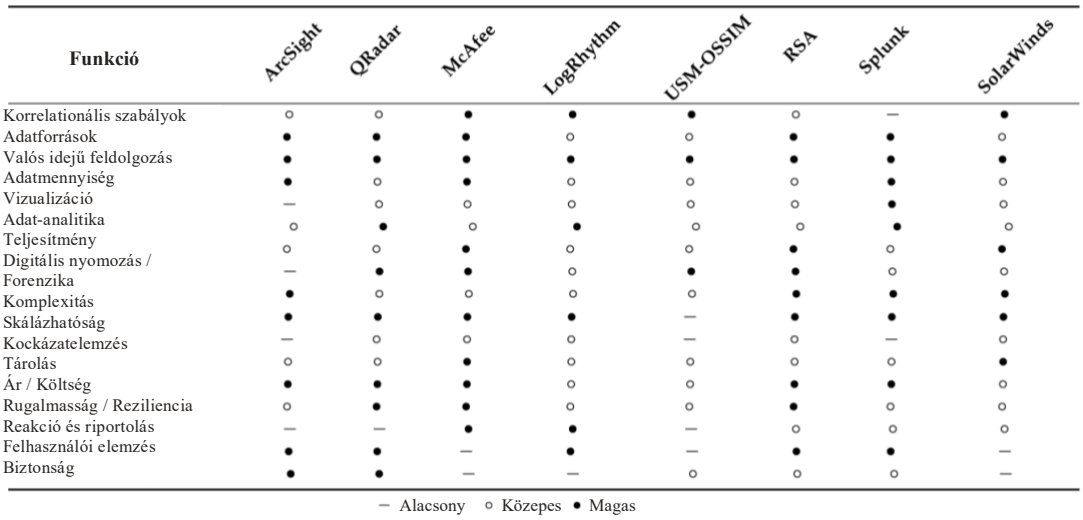
Ezeknek az elemeknek zökkenőmentesen kell együttműködniük a rendszer megfelelő működéséhez. Bár sok SIEM megoldás már kínál automatizált válaszfunkciókat, amelyek lehetővé teszik a biztonsági intézkedések kiválasztását és alkalmazását, ezek a funkciók gyakran korlátozottak az összetett támadások hatásának és a válaszlépések következményeinek átfogó elemzésében. A SIEM rendszerek folyamatosan fejlődnek, válaszul a kiberfenyegetések növekvő kifinomultságára. Elengedhetetlen eszközt jelentenek az incidensek valós idejű felismerésében és kezelésében, értékes betekintést nyújtanak a hálózati aktivitásokba, és segítik a biztonsági csapatokat a proaktív védelmi stratégia fenntartásában. Ahogy a kiberbiztonsági fenyegetések környezete tovább fejlődik, úgy kell a SIEM megoldásoknak is folyamatosan fejlődniük – különös figyelmet fordítva az automatizálás bővítésére, az adatelemzés fejlesztésére és a válaszképességek finomítására, hogy hatékonyan kezeljék az újonnan felmerülő kockázatokat.

A SIEM rendszerek alapvető eszközei a szervezetek számára, mivel lehetővé teszik az informatikai infrastruktúra által generált biztonsági események gyűjtését, tárolását és elemzését. Bár minden SIEM megoldás rendelkezik ezekkel az alapvető képességekkel, jelentős különbségek figyelhetők meg a funkciók, teljesítmény és implementációs lehetőségek terén. Ezek a különbségek gyakran tükrözik az adott SIEM rendszer piaci pozícióját: az egyszerűbb, kis léptékű bevezetésre tervezett megoldásoktól egészen a nagyvállalati környezetekben alkalmazott, összetett biztonsági igényeket kielégítő fejlett rendszerekig terjednek.

A SIEM rendszerek értékelésekor elengedhetetlen, hogy a szervezetek számos olyan jellemzőt vegyenek figyelembe, amelyek közvetlen hatással vannak a rendszer hatékonyságára a biztonsági incidensek felismerésében és kezelésében. Ilyen szempontok például:

- az eseménygyűjtés és normalizálás képessége,
- a szabályalapú és viselkedésalapú korrelációs motorok teljesítménye,
- az automatizált válaszintézkedések lehetősége,
- a skálázhatóság és integrációs képességek más biztonsági eszközökkel,
- valamint a jelentéskészítési és megfelelőségi támogatás.

A megfelelő SIEM rendszer kiválasztása nemcsak technikai, hanem stratégiai döntés is, amely hosszú távon meghatározza a szervezet biztonsági műveleteinek hatékonyságát és reagálóképességét a folyamatosan változó kiberfenyegetésekkel szemben.



6. ábra: *Eseménykezelési trendek*

A SIEM rendszerek egyik kulcsfontosságú jellemzője az események korrelálásának képessége. A korrelációs szabályok képezik a SIEM eseménydetektálási képességeinek gerincét, mivel meghatározzák, hogyan elemzi és kapcsolja össze a rendszer a különböző forrásokból származó eseményeket a potenciális biztonsági incidensek azonosítása érdekében. Bár a legtöbb SIEM alapvető korrelációs szabályokat kínál, a fejlettebb rendszerek összetett keresési nyelveket is támogatnak, amelyek lehetővé teszik a biztonsági elemzők számára, hogy kifinomult lekérdezéseket írjanak és mélyebb adatvizsgálatokat végezzenek. Ezek a rendszerek képesek szélesebb körű események kezelésére, és hatékonyabban azonosítják a rosszindulatú tevékenységek finom mintázatait. Az adatok sokféle forrásból történő gyűjtésének képessége szintén alapvető fontosságú egy SIEM esetében. A biztonsági események az IT-infrastruktúra számos pontjáról származhatnak, például szerverekből, tűzfalakból, behatolásérzékelő rendszerekből és végponti eszközökből. Egy SIEM hatékonysága nagyrészt attól függ, milyen jól képes adatokat gyűjteni ezekből a különböző forrásokból. Sok SIEM natívan támogat többféle adatforrást, beleértve különböző szenzorokat és adatfajtákat, például fenyegetési intelligenciaforrásokat. Ugyanakkor egyes megoldások további komponenseket vagy integrációkat igényelhetnek az összes kívánt adatforrás eléréséhez, ami bonyolíthatja a bevezetést és növelheti az összköltséget. A valós idejű adatfeldolgozás szintén létfontosságú jellemzője a SIEM rendszereknek, mivel a

biztonsági környezet folyamatosan változik. Az adatok valós idejű feldolgozásának és elemzésének képessége lehetővé teszi a SIEM számára, hogy a fenyegetéseket azok bekövetkezésekor észlelje és kezelje, nem pedig utólag. Ez jelentős számítási kapacitást igényel, mivel a SIEM-nek másodpercenként akár több millió eseményt kell kezelnie a teljesítmény csökkenése nélkül. A fejlett SIEM rendszerek képesek valós idejű monitorozást és riasztást biztosítani, lehetővé téve a biztonsági csapatok számára a gyors incidensazonosítást és kezelést. A nagy mennyiségű adat kezelése szintén kritikus kihívás a SIEM megoldások számára. Ahogy a szervezetek növekednek és egyre több eszközt és szenzort telepítenek, az előállított adatmennyiség exponenciálisan nő. Bár a nagy adathalmazok elemzése értékes betekintést nyújthat a biztonsági eseményekbe, költséges és gyakorlatlan lehet az összes begyűjtött adat korlátlan ideig történő tárolása. Ezért sok SIEM úgy van kialakítva, hogy rövid időn keresztül képes nagy mennyiségű adat kezelésére, hatékony indexelésre, korrelációra és tárolásra összpontosítva. Ez lehetővé teszi a biztonsági csapatok számára, hogy visszamenőleg is rálássanak az eseményekre anélkül, hogy túlterhelnék a tárolási kapacitásokat. Az adatvizualizáció gyakran alulértékelt funkció a SIEM rendszerekben, pedig kulcsfontosságú a biztonsági események hatékony elemzéséhez. Sok SIEM nem rendelkezik robusztus vizualizációs eszközökkel, ami megnehezíti az elemzők számára az adatokkal való interakciót és azok feltárását. Ennek kezelésére a fejlettebb megoldások testreszabható irányítópultokat és vizualizációkat kínálnak, amelyek segítik a biztonsági csapatokat az események jobb megértésében és értelmezésében. Ezek a funkciók javítják a döntéshozatalt, és segítenek a trendek vagy új fenyegetések könnyebb azonosításában. Az elmúlt években a fejlett adatelemzési képességek SIEM-be történő integrációja jelentős trenddé vált. A modern SIEM rendszerek képesek integrálódni anomáliaészlelő eszközökkel, amelyek a felhasználók és alkalmazások viselkedését elemzik, gyanús vagy rosszindulatú tevékenységek jeleit keresve. Ezek a rendszerek gépi tanulást és mesterséges intelligenciát alkalmaznak szokatlan mintázatok felismerésére – például ha egy alkalmazott érzékeny adatokhoz fér hozzá, amit normál esetben nem tenne, vagy ha egy külső alvállalkozó próbál kihasználni egy sebezhetőséget. Ez a viselkedéselemzés fokozza a SIEM képességét olyan fenyegetések azonosítására, amelyeket a hagyományos szabályalapú megközelítések nem feltétlenül észlelnének.

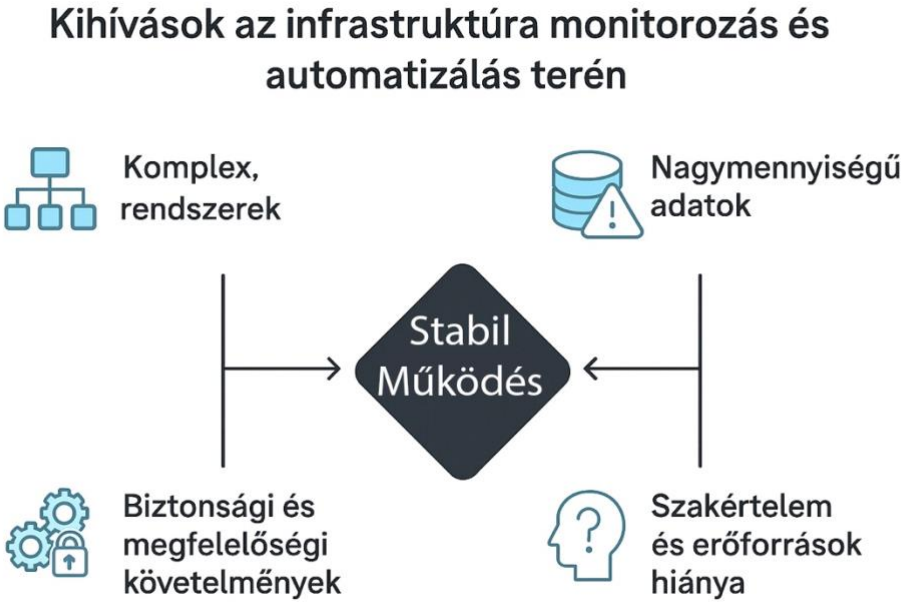
A teljesítmény szintén kulcsfontosságú szempont a SIEM megoldások értékelésekor. Egy SIEM-nek képesnek kell lennie a nagy mennyiségű adat feldolgozásának, esemény-korrelációnak és információtárolásnak számítási igényeit hatékonyan kezelni. A nagy

teljesítményű rendszerek gyors adatfeldolgozást, robusztus tárolási képességeket és skálázhatóságot kínálnak a szervezet infrastruktúrájának növekedésével párhuzamosan. A digitális kriminalisztika (forensics) szintén kritikus funkció bizonyos SIEM rendszerek esetében. Az eseménynaplózáson túl egyes rendszerek beépített kriminalisztikai képességeket kínálnak, például hálózati szekciók rögzítését. Ezek az eszközök lehetővé teszik a biztonsági csapatok számára, hogy az eseménynaplókon túlmenően rekonstruálják a rosszindulatú tevékenységeket – például a hálózati forgalom visszajátszásával megértsék egy támadás teljes lefolyását. Nem minden SIEM rendelkezik ilyen képességekkel, és a kriminalisztikai részletesség szintje jelentősen eltérhet a különböző megoldások között. A bevezetés összetettsége fontos tényező a SIEM megoldás kiválasztásakor. Míg egyes rendszerek viszonylag könnyen telepíthetők és kezelhetők, mások jelentős konfigurációs és karbantartási erőfeszítést igényelnek. A bevezetés komplexitása függhet a rendszer funkcióitól, skálázhatóságától, valamint a gyártó által biztosított támogatástól. Az ArcSight például ismert arról, hogy nehezen telepíthető és kezelhető, míg a LogRhythm és a Splunk gyakran dicséretet kap felhasználóbarát felületéért és egyszerűbb beállítási folyamatáért. A skálázhatóság szintén kulcsfontosságú jellemző. Ahogy a szervezetek növekednek, úgy nőnek a biztonsági igényeik is. Egy SIEM-nek képesnek kell lennie nemcsak hardveres szinten skálázni, hanem az egyre növekvő biztonsági eseménymennyiség feldolgozására és elemzésére is. Ez különösen fontos a digitális transzformáció kontextusában, ahol folyamatosan új eszközök, szenzorok és végpontok kerülnek a hálózatra. [39]

3.1.7 Kihívások az infrastruktúra monitorozás és automatizálás terén

Az infrastruktúra-monitorozás és automatizálás világában az iparágak számos egyedi kihívással szembesülnek, amelyek közvetlen hatással vannak arra, hogyan figyelik és védik működésüket. Az egyik legjelentősebb akadály a szabályozási megfelelés, amely szinte minden szektorban kiemelt aggodalomra ad okot. A szabályozási keretrendszerek szigorú előírásokat támasztanak, amelyeket az informatikai műveleteknek teljesíteniük kell, és elengedhetetlen, hogy a monitorozási és automatizálási folyamatok összhangban legyenek ezekkel a normákkal. Például az egészségügyben az Egyesült Államokban érvényes Health Insurance Portability and Accountability Act (HIPAA) előírja, hogy az egészségügyi szervezeteknek robusztus monitorozási rendszereket kell fenntartaniuk a betegadatok védelme érdekében, biztosítva azok bizalmasságát, sértetlenségét és rendelkezésre állását. Az ilyen környezetekben való megfelelés megköveteli a valós idejű

monitorozást és az automatizált válaszintézkedéseket minden biztonsági rés vagy sebezhetőség esetén, ami kiemeli a vállalati alkalmazásmonitorozás bővítésének fontosságát a szabályozási keretek betartása mellett. A szabályozási megfelelés mellett a szenzitív adatok kezelése szintén komoly kihívást jelent, különösen azokban az iparágakban, ahol az információbiztonság elsődleges szempont. A pénzügyi szektor például hatalmas mennyiségű érzékeny pénzügyi adatot dolgoz fel, ezért olyan kifinomult monitorozási megoldásokra van szüksége, amelyek részletes betekintést nyújtanak anélkül, hogy veszélyeztetnék az adatok biztonságát. Ez az egyensúly rendkívül fontos, mivel bármilyen kompromisszum súlyos következményekkel járhat. Annak megértése, hogyan kezelik az iparágak az érzékeny adatok védelme és a hatékony monitorozás közötti egyensúlyt, kulcsfontosságú a hatékony megoldások kialakításához.
A skálázhatóság egy újabb kihívás, amellyel a gyorsan növekvő iparágaknak szembe kell nézniük. Az e-kereskedelem és az online szolgáltatások jó példák erre, ahol a monitorozási rendszereknek horizontálisan kell skálázódniuk, hogy támogassák a növekvő felhasználói bázist és a tranzakciók számának emelkedését. Az automatizálás ezekben a környezetekben alapvető eszközzé válik, amely segít az erőforrások automatikus kiosztásában, a teljesítmény optimalizálásában, és biztosítja, hogy a monitorozási infrastruktúra a szervezet növekedésével párhuzamosan fejlődjön.
A skálázhatósági kihívások kezelése értékes tanulságokat kínál azoknak a vállalkozásoknak, amelyek fejleszteni kívánják monitorozási és automatizálási képességeiket a növekedés során. Végül a technológiai fragmentáció egy állandó probléma, különösen az olyan szektorokban, mint a gyártás, ahol az operatív technológia (OT) és az informatikai rendszerek (IT) gyakran egymás mellett működnek. Az ilyen eltérő rendszerek kezelése összetett feladat, amely alkalmazkodó monitorozási megoldásokat igényel, amelyek képesek különböző technológiák integrálására. Az OT és IT rendszerek közötti szakadék áthidalása lehetővé teszi a szervezetek számára, hogy egységes képet kapjanak teljes infrastruktúrájukról, míg az automatizálásnak képesnek kell lennie a különböző technológiai rétegek kezelésére az incidensek és események zökkenőmentes menedzselése érdekében. A technológiai fragmentáció leküzdése kulcsfontosságú a diagnosztikai és helyreállítási folyamatok automatizálásához, és hozzájárul egy egységesebb, hatékonyabb monitorozási megközelítés kialakításához az összetett technológiai környezetekben.



7. ábra: *Stabil működés*

3.1.8 Az infrastruktúra monitorozás és automatizálás előnyei

A gyorsan változó üzleti környezetben az operatív hatékonyság kulcsfontosságú a zökkenőmentes és eredményes folyamatok fenntartásához. A monitorozás és az automatizálás együttműködve segítik a vállalatokat a működés racionalizálásában. A monitorozó eszközök valós idejű betekintést nyújtanak, előre jelezve a lehetséges problémákat, például teljesítményzavarokat vagy szűk keresztmetszeteket. Ez lehetővé teszi a vállalatok számára, hogy proaktívan beavatkozzanak, mielőtt a zavarok ténylegesen bekövetkeznének. Az automatizálás ezt követően átveszi a rutinfeladatokat, előre definiált munkafolyamatokat hajt végre precízen, biztosítva, hogy a szervezet megszakítás nélkül a kijelölt pályán maradjon. A két technológia kombinációja folyamatos, gördülékeny működést eredményez.

A költségmegtakarítás szintén jelentős előnye a monitorozásnak és az automatizálásnak. A gondos monitorozás révén a vállalatok azonosítani tudják az alulhasznált erőforrásokat, és hatékonyabban tudják azokat allokálni, ezáltal optimalizálva a költségvetést.

8. ábra: *Monitorozás és automatizálás előnyei*

Az automatizálás csökkenti a manuális munkavégzést, mivel átveszi az ismétlődő feladatokat, ezáltal csökkentve az üzemeltetési költségeket. Ez a kombináció nemcsak a hatékonyságot növeli, hanem hozzájárul a pénzügyi sikerhez is, miközben segít a költségek kézben tartásában. A biztonság terén a monitorozás és az automatizálás kéz a kézben működnek a digitális infrastruktúrák védelme érdekében. A monitorozó eszközök folyamatosan pásztázzák a rendszereket fenyegetések és anomáliák után kutatva, míg az automatizálás azonnal életbe lépteti a biztonsági protokollokat, amikor szükséges. Ez a proaktív megközelítés biztosítja, hogy a biztonsági problémák azonnal kezelésre kerüljenek, csökkentve az esetleges károkat. Ennek a szinergiának jó példája egy vezető amerikai befektetési bank, amely fejlett IT-menedzsment megoldásokat alkalmaz a monitorozás és automatizálás integrálására, így gyorsan semlegesíti a fenyegetéseket és megerősíti biztonsági rendszerét. Az alkalmazkodóképesség szintén kiemelkedő előnye a monitorozás és automatizálás integrációjának. Azok a szervezetek, amelyek nyitottak ezekre az eszközökre, hatékonyabban tudják kezelni a technológiai és iparági változásokat. Az automatizálás rugalmas megoldásokat kínál, amelyek segítenek a szervezeteknek megelőzni a kihívásokat, lehetővé téve számukra, hogy alkalmazkodjanak a változásokhoz anélkül, hogy lemaradnának. A proaktív monitorozás és automatizálás révén a vállalatok nem csupán reagálnak a külső változásokra, hanem aktívan formálják saját jövőjüket. Összefoglalva, a monitorozás és az automatizálás erőteljes kombinációt alkotnak, amely elősegíti az operatív hatékonyságot, a költségmegtakarítást, a biztonságot és az alkalmazkodóképességet – mindezt úgy, hogy a

szervezetek versenyképesek és ellenállóak maradjanak a folyamatosan változó környezetben.

3.1.9 A biztonsági információ- és eseménykezelő rendszerek jövője

A biztonsági információ- és eseménykezelő rendszerek (SIEM) jövőjét számos, egymással összefüggő tényező formálja, amelyek a politikai, gazdasági, társadalmi, technológiai, jogi és környezeti szférákhoz kapcsolódnak.

Politikai szempontból a kormányzatok – különösen az Európai Unióban – egyre inkább felismerik a kiberbiztonság stratégiai jelentőségét, és jelentős mértékben növelik az ezen a területen végrehajtott beruházásokat. Ennek mozgatórugója az érzékeny információk és kritikus infrastruktúrák védelme az egyre gyakoribb és kifinomultabb kibertámadásokkal szemben. Ahogy a kormányzati szereplők fokozzák a kiberbiztonság megerősítésére irányuló erőfeszítéseiket, ezek az intézkedések várhatóan ösztönözni fogják a SIEM megoldások elterjedését és fejlesztését, biztosítva, hogy ezek képesek legyenek kezelni a digitális biztonsági kihívások növekvő komplexitását. A beruházások mellett a magas minőségű, megfizethető és interoperábilis kiberbiztonsági termékek iránti igény további innovációt fog generálni a SIEM rendszerek terén. Gazdasági trendek szintén kulcsszerepet játszanak a SIEM technológia fejlődésében. A rövid távú és szabadúszó munkavégzés térnyerése átalakítja a foglalkoztatási struktúrákat, és mivel egyre többen dolgoznak ideiglenes vagy projektalapú szerepkörökben, a vállalatoknak biztonsági rendszereiket ehhez az új munkaerődinamikához kell igazítaniuk. Ez azt jelenti, hogy a SIEM rendszereknek felhasználóbarátabbá és rugalmasabbá kell válniuk, olyan felületeket kínálva, amelyek könnyen kezelhetők a sokszínű és változó munkaerő számára. Emellett a kiberbiztonsági szakemberek iránti kereslet növekedése új lehetőségeket teremt a SIEM rendszerek piaci térnyerésére. A globalizáció hatására a vállalatok egyre nagyobb léptékben és összetettebb hálózatokban működnek, ami megköveteli, hogy a SIEM rendszerek képesek legyenek ezeket a környezeteket hatékonyan kezelni. A kis- és középvállalkozások, amelyek gyakran sebezhetőbbek a kibertámadásokkal szemben, kulcsfontosságú célpiaccá válhatnak a SIEM szolgáltatók számára, akiknek megfizethető és könnyen bevezethető megoldásokat kell kínálniuk. Társadalmi változások szintén ösztönzik a SIEM rendszerek fejlődését. Ahogy a társadalom egyre inkább az információs és kommunikációs technológiákra támaszkodik, úgy válik egyre sürgetőbbé a hatékony biztonsági rendszerek iránti igény. A fiatalabb

generációk – különösen azok, akik tisztában vannak a világ összekapcsoltságával és a kiberbiztonsági kockázatokkal – nyomást gyakorolnak a vállalatokra, hogy robusztusabb védelmi intézkedéseket vezessenek be. A közösségi média térnyerése és mindennapi életbe való integrációja hatalmas mennyiségű adatot generál, amely – ha megfelelően elemezzük – értékes információkat szolgáltathat a biztonsági eseményekről. Ugyanakkor ezeknek az adatoknak a monitorozása és védelme új kihívásokat jelent a SIEM rendszerek számára. A kritikus infrastruktúrákat érő támadások számának növekedése tovább erősíti az igényt a fejlett SIEM megoldások iránt, amelyek képesek az ilyen fenyegetések felismerésére és elhárítására.

Technológiai szempontból a SIEM rendszerek jelentős előnyöket élveznek a felhőalapú számítástechnika, a mobiltechnológiák, a big data analitika és a gépi tanulás fejlődéséből. Ezek az innovációk lehetővé teszik, hogy a SIEM rendszerek nagyobb adatmennyiséget dolgozzanak fel, javítsák a valós idejű fenyegetésdetektálást, és fokozzák a döntéshozatali képességeket. Ugyanakkor ezek az előrelépések új kihívásokat is teremtenek, különösen a mobil eszközök védelme és az IoT (Internet of Things) által generált adatmennyiség kezelése terén. Ahogy az adatok mennyisége és komplexitása növekszik, a SIEM rendszereknek alkalmazkodniuk kell, hogy hatékonyan tudják kezelni és biztosítani ezeket az információkat, miközben gyors és pontos válaszokat adnak a biztonsági eseményekre.

A SIEM rendszerek jövőjét alakító technológiai trendek:

- **Felhőtárolás**

A felhőtárolás egyértelműen előnyös technológia a SIEM rendszerek számára, mivel lehetővé teszi a hálózati események big data analitikáját hatékonyabban, anélkül, hogy aggódni kellene a naplók, információk és adatok tárolási korlátai miatt.

- **Felhőszolgáltatások integrációja**

Ez a technológia külön kezelendő a felhőtárolástól, mivel nem csupán az adatok statikus tárolására szolgál, hanem a szoftverek távoli szerveren történő futtatására fókuszál. Ez biztosítja az alkalmazások skálázhatóságát és magas rendelkezésre állását, mivel azok már nem helyi hardverhez kötöttek, és bárhonnan elérhetők.

- **Mobiltechnológiák**

A mobil eszközök számának növekedése új fenyegetéseket hoz, amelyeket a SIEM rendszereknek elemezniük kell. Egyre gyakoribb, hogy a munkavállalók céges és saját eszközeiket egyaránt használják munkavégzésre. A vállalati adatok védelme – különösen otthoni munkavégzés esetén, saját eszközökön (BYOD – Bring Your Own Device) – számos kihívást jelent. Ezek az eszközök gyakran nem esnek az IT-osztály felügyelete alá, nem rendelkeznek előtelepített biztonsági megoldásokkal, az adatok nem titkosítottak, és az alkalmazások nem mindig követhetők nyomon.

- **Big data analitika**

A SIEM rendszerek egyre inkább adatfeldolgozó platformokká válnak. A kapcsolt környezetekben keletkező adatmennyiség exponenciális növekedése miatt elengedhetetlen a valós idejű eseményelemzésre, döntéstámogatásra és egyéb kritikus feladatokra alkalmas, nagy teljesítményű elemző eszközök alkalmazása. Az adatfeldolgozási módszerek fejlesztése kulcsfontosságú lehetőséget jelent a SIEM rendszerek számára.

- **Gépi tanulás**

A nagy teljesítményű számítógépek, modern hardverek és programozási nyelvek fejlődése, valamint az adatelemzés lehetővé teszi ok-okozati összefüggéseken alapuló adatmodellek létrehozását. A SIEM rendszerek ezeket a technológiákat kihasználva képesek javítani az eseménydetektálást és a döntéshozatali folyamatokat.

- **IoE kommunikációs hálózat**

Az „Internet of Everything” (IoE) egy átfogó kommunikációs hálózat, amely valós világban létező objektumok és fizikai tevékenységek milliárdjaitól gyűjt, kezel és hasznosít adatokat. Az IoE az IoT koncepcióját bővíti ki azáltal, hogy embereket, folyamatokat, helyszíneket és egyéb tényezőket is integrál. Ez a technológia jelentős hatással van a SIEM rendszerekre, mivel hatalmas mennyiségű adatot és eseményt biztosít elemzésre, ami új lehetőségeket és kihívásokat teremt a biztonsági információkezelésben.

Az 5G hálózatok a kommunikációs technológiák következő generációját képviselik, amelyeket a jövő alkalmazásainak és forgatókönyveinek igényeihez terveztek. A megnövelt adatátviteli sebesség révén az 5G jelentősen növelheti azt az adatmennyiséget, amelyet a SIEM rendszereknek egy adott időegység alatt elemezniük kell. Ez potenciálisan bonyolíthatja az események detektálását, és új technológiai megoldásokat

igényel a valós idejű feldolgozás és válaszadás biztosításához. A közösségi média analitika szintén egyre fontosabbá válik. Az olyan platformok, mint a Twitter, hatalmas információforrást kínálnak, amelyet nemcsak a kiberbiztonsági cégek, hanem a támadók is aktívan használnak. A támadások áldozatai gyakran osztják meg tapasztalataikat, meglátásaikat és technikai részleteket a sebezhetőségekről és exploitokról, így a közösségi média értékes adatforrássá válik a biztonsági események elemzésében. Összességében a SIEM rendszerek jövőjét számos tényező együttes hatása alakítja. A politikai és gazdasági nyomás fokozza a kiberbiztonsági beruházásokat, míg a társadalmi és technológiai trendek egyre fejlettebb, rugalmasabb és felhasználóbarátabb SIEM megoldásokat követelnek. Ezeknek a rendszereknek folyamatosan fejlődniük kell, hogy képesek legyenek kezelni az új biztonsági kihívásokat, beleértve a változó munkakörnyezeteket, a közösségi média térnyerését és a globális digitális infrastruktúrák növekvő komplexitását. A mesterséges intelligencia (MI) és a gépi tanulás (ML) integrációja kulcsfontosságú lesz a SIEM rendszerek hatékonyságának növelésében. Az MI lehetővé teszi a prediktív elemzést, amely különösen hasznos a hálózati forgalomban, eszközhasználatban és felhasználói viselkedésben megjelenő rendellenességek azonosításában. Bár jelenleg csak néhány SIEM platform – például a LogRhythm és a QRadar – alkalmaz gépi tanulást a fenyegetési intelligenciából való tanulásra és támadások enyhítésére, az MI/ML integráció lehetőségei jelentősek.

Az MI/ML integrációja a Security Orchestration, Automation and Response (SOAR) rendszerekbe – közvetlenül a SIEM platformokba építve – javíthatja a kibertámadások felismerését, kezelését és megelőzését. Az MI-alapú védelmi rendszerek képesek nagy adatmennyiségek elemzésére, és gyanús mintázatok azonosítására valós időben vagy közel valós időben. Az MI/ML gyakori alkalmazási területei a SIEM rendszerekben:

- behatolásérzékelés (pl. hálózati támadások),
- adathalászat és spam detektálása (pl. e-mailek),
- felhasználói viselkedéselemzés.

Az MI-alapú SIEM rendszerek hatékonyabbak a döntéshozatalban és viselkedésük adaptálásában, mivel képesek rejtett fenyegetések feltárására, csökkentik a manuális beavatkozás szükségességét, és minimalizálják a téves riasztások számát. Ezek a rendszerek képesek a szabályalapú elemzést MI-mechanizmusokkal kombinálni, hogy azonosítsák a felhasználói aktivitásban bekövetkező eltéréseket, felismerjék a szokatlan

viselkedést a hasonló szerepkörű felhasználókhoz képest, és gyorsan, pontosan reagáljanak a fenyegetésekre. A jövőbeni SIEM fejlesztések magukban foglalhatják az olyan szenzorokat, amelyek felügyelet nélküli tanulás (unsupervised learning) alapján képesek felhasználói és alkalmazási viselkedési minták kialakítására, lehetővé téve az anomáliák detektálását és pontosabb riasztások generálását. Emellett a felhasználói viselkedéselemzés profitálhat a kiugró értékek detektálásából és más felügyelet nélküli gépi tanulási technikákból, amelyek javítják a profilkezelést és a biztonsági válaszintézkedések pontosságát.

3.1.10 A Mesterséges intelligencia szerepe a kiberbiztonsági megoldásokban

A mesterséges intelligencia (MI) és a gépi tanulás (ML) egyre fontosabbá válik a kiberbiztonság területén, ahogy a fenyegetések egyre összetettebbé válnak. Bár ezek a technológiák jelentős potenciált kínálnak, különösen a gépi tanulás és a természetes nyelvfeldolgozás (NLP) területén, nem tekinthetők univerzális megoldásnak. A biztonsági szakembereknek az MI-t hagyományos módszerekkel kell integrálniuk annak érdekében, hogy hatékonyan kezeljék a kockázatokat. Ahogy az MI iránti igény növekszik a kiberbiztonságban, elengedhetetlen, hogy a szervezetek megalapozott döntéseket hozzanak annak alkalmazásáról. A kiberbiztonsági környezet egyre nagyobb nyomás alatt áll, mivel a vállalatok egyre kevesebb platformra konszolidálják működésüket, ami összetettebb támadási felületet eredményez. A hibrid munkavégzés és az olyan kollaborációs eszközök elterjedése, mint a Microsoft Teams vagy a Slack, új sebezhetőségeket hozott létre, amelyek célzott támadásoknak teszik ki a szervezeteket. A digitális eszközök konszolidációja és a tömeges adatok magas értéke miatt a nagy szolgáltatók vonzó célpontokká váltak, ami növeli az adatvédelmi incidensek kockázatát és költségeit. Ez a változás kifinomultabb támadásokhoz vezetett, amelyek aláássák a hagyományos emberi védekezési mechanizmusokat.

Bár az MI jelentős előnyöket kínál, például nagy adatmennyiség gyors feldolgozását, idővel okosabb döntéshozatalt és feladatok automatizálását, fontos felismerni, hogy az MI csupán egy eszköz, amelyet megfelelően kell integrálni a védelmi stratégiákba. A generatív MI-t például már kihasználták rosszindulatú szereplők meggyőzőbb adathalász e-mailek létrehozására, ami hozzájárult az ilyen típusú támadások számának növekedéséhez. Bár a generatív MI teljes hatása még nem ismert, világos, hogy jelentősen felerősítette a kiberbiztonsági fenyegetéseket. A kiberbiztonságban kulcsfontosságú

döntések születnek arról, hogy mit engedélyezzenek, blokkoljanak vagy kezeljenek. Az MI segíthet ezekre a kérdésekre gyorsabb és hatékonyabb válaszokat adni nagy léptékben, de csak akkor, ha egy átfogó védelmi stratégia részeként kerül alkalmazásra. A vezető biztonsági szolgáltatók az MI-t a védelem megerősítésére, a fenyegetések semlegesítésére és a biztonsági csapatok terhelésének csökkentésére használják. Az MI azonban akkor működik a leghatékonyabban, ha hagyományos módszerekkel kombinálják, ezáltal javítva a detektálást és növelve a biztonságot. A gépi tanulási technológiák megfelelő alkalmazást igényelnek, amelyet szakértelem és minőségi adatok támogatnak. Ahogy az MI-technológiák fejlődnek, úgy nő a kibertámadások kifinomultsága is. A kiberbűnözők előtt való előny megtartása érdekében elengedhetetlen az MI hatékony használata és többrétegű védelmi stratégiákba való integrálása. Az MI-t ott kell alkalmazni, ahol nagy adathalmazok állnak rendelkezésre – például anomáliaészlelés esetén –, és folyamatos visszacsatolási ciklusokkal kell támogatni a teljesítmény javítása érdekében. Az emberi szakértelem kulcsfontosságú az MI-alapú biztonsági intézkedések finomhangolásához, biztosítva a nagyobb pontosságot és alkalmazkodóképességet. Az MI és a gépi tanulás sikeres alkalmazása a kiberbiztonságban a magas minőségű adatokon és a megalapozott emberi felügyeleten múlik. Gyenge adatok vagy hibás fejlesztési döntések hibás eredményekhez vezethetnek, ami kiemeli az adatok minőségének és az emberi irányításnak a fontosságát a megbízható MI-alapú védelem kialakításában. Az MI már most is kritikus eleme a többrétegű kiberbiztonsági megoldásoknak, amelyek elengedhetetlenek a kommunikáció, az emberek és az adatok védelméhez. Alkalmazása stratégiai kell, hogy legyen, olyan területekre összpontosítva, ahol az MI erősségei maximálisan kihasználhatók, miközben figyelembe vesszük annak korlátait. Az MI alkalmazása a kiberbiztonságban várhatóan tovább fog terjedni, bár teljes potenciálját még csak most kezdjük megérteni. Noha a jövő bizonytalan, az MI lehetőségei hatalmasak – és azok képzelete és szakértelme fogja meghatározni, akik képesek kiaknázni ezt a technológiát. Csak az idő fogja megmutatni, milyen mértékű hatást gyakorol majd a mesterséges intelligencia a kiberbiztonság jövőjére. Az infrastruktúra-monitorozás jelentősége a kritikus rendszerek védelmében nem hangsúlyozható eléggé. Ahogy a modern informatikai rendszerek egyre összetettebbé és sebezhetőbbé válnak a kiberbiztonsági fenyegetésekkel szemben, úgy válik elengedhetetlenné a fejlett monitorozó eszközök alkalmazása. A jelen fejezet bemutatta a monitorozási megoldások fejlődését, kiemelve azok kulcsszerepét a rendszer teljesítményének, biztonságának és megbízhatóságának javításában. A jövőre tekintve a SIEM rendszerek várhatóan még

kifinomultabb platformokká fejlődnek. Ezek a rendszerek mélyebb analitikai képességeket integrálnak, kihasználva a mesterséges intelligencia erejét a valós idejű fenyegetési intelligencia és prediktív elemzések biztosítására. Mivel egyre nagyobb mennyiségű adat gyors feldolgozására van szükség, a jövő SIEM megoldásai a skálázhatóságra, alkalmazkodóképességre és automatizálásra fognak összpontosítani, így nélkülözhetetlenné válnak a dinamikusan változó kiberbiztonsági környezetek kezelésében. Emellett a mesterséges intelligencia szerepe a kiberbiztonságban tovább fog bővülni, alapvetően átalakítva azt, ahogyan a szervezetek védik kritikus infrastruktúráikat. Az MI fokozza a képességet az olyan anomáliák és fenyegetések azonosítására, amelyeket a hagyományos rendszerek esetleg nem észlelnek, páratlan sebességet és pontosságot kínálva a potenciális biztonsági rések detektálásában. Ahogy az MI és a gépi tanulás fejlődik, hozzájárulásuk a kiberbiztonsághoz túlmutat a monitorozáson: kulcsszerepet játszanak a kockázatelemzésben, a válaszintézkedések automatizálásában és a stratégiai döntéshozatalban. A SIEM rendszerek fejlődésének és az MI-alapú technológiák átalakító képességeinek kombinálásával a szervezetek proaktívan kezelhetik a felmerülő kockázatokat, biztosíthatják ellenállóképességüket, és fenntarthatják kritikus infrastruktúráik integritását. Ezek az innovációk továbbra is a kiberbiztonság élvonalában maradnak, és irányt mutatnak az iparágak számára egy biztonságosabb és hatékonyabb jövő felé. [42]

3.1.11 Csökkenő reakcióidő

A hagyományos monitorozási eszközök gyakran nem veszik észre időben a teljesítményromlást, mert csak infrastruktúra-szintű metrikákat figyelnek. Teszt rendszeren végzett vizsgálat alapján a kritikus hibák több mint 50%-a észrevétlen maradt, ami jelentős üzleti veszteséget okozhat. Az AI-alapú monitoring eszközök ezzel szemben 70%-kal gyorsabban detektálták a hibákat, akár percek alatt, és automatizált riasztásokkal, valamint újraindítási folyamatokkal jelentősen csökkentették a manuális beavatkozás szükségességét. Az 5 napos tesztidőszakban a detektálási idő a több óráról pár percre, a helyreállítási idő is hasonlóképpen lecsökkent, ami valós helyzetben hatalmas veszteségeket eredményezhetett volna.

3.1.12 Összegzés

Harmadik hipotézis: A valós idejű monitoring és reagálási stratégia, amely MI-t használ anomália detektálásra és automatizált reagálásra, jelentősen csökkentheti a támadás felfedezési és reakcióidőt, ezáltal csökkentve a károkat, minimalizálva a szolgáltatás-kiesés valószínűségét kritikus infrastruktúrák esetében.

A harmadik hipotézis validálható: A valós idejű MI-alapú monitoring és az emberi reagálás, különösen hibrid architektúrában, bizonyítottan csökkenti a felfedezési és reakcióidőt, ezáltal mérsékli a károkat és a szolgáltatáskiesés kockázatát kritikus infrastruktúrákban. Tudunk valós időben észlelni anomáliákat a rendszer viselkedésében, például szokatlan adatforgalmat, jogosulatlan hozzáféréseket. Az MI képes azonnal reagálni például rendszer manipulációra, GPS vagy utasbiztonsági eseményekre egyaránt. Ez a stratégia nemcsak technológiai, hanem szabályozási és gazdasági szempontból is előremutató.

4 FENNTARTHATÓ BIZTONSÁG

A mobil eszközök menedzsmentje a fenntartható biztonság egyik kritikus pillére, mivel a modern szervezetek működése egyre inkább a dinamikusan változó és földrajzilag szétszórt eszközök ökoszisztémájára épül. A fenntartható biztonság nem csupán a pillanatnyi kockázatok csökkentését jelenti, hanem a hosszú távon stabil védelmi architektúra kialakítását is, amely képes kezelni a mobilitásból fakadó folyamatos konfigurációs, hálózati és felhasználói változásokat. Az MDM rendszerek ebben a kontextusban olyan integrált kontrollréteget biztosítanak, amely egységesíti az eszközök életciklus-kezelését, automatizálja a biztonsági házirendek érvényesítését, és valós idejű állapot monitoringot tesz lehetővé, ezáltal csökkentve az emberi hibából eredő kitettséget. A fenntarthatóság szempontjából különösen jelentős, hogy az MDM nem reaktív, hanem proaktív kontrollmechanizmus: képes a sérülékeny vagy nem megfelelős állapotú eszközök automatikus izolálására. Mindez hozzájárul a szervezet kialakításához, amelyben a mobil eszközök nem kockázati tényezőként, hanem kontrollált, auditálható és fenntartható módon integrált erőforrásként jelennek meg.

4.1 Az alkalmazások és a mesterséges intelligencia együttes működése

A modern informatikai alkalmazások és az MI együttes működése olyan szinergikus architektúrát hoz létre, amely alapvetően átalakítja a szervezeti folyamatok hatékonyságát és fenntartható működését. Az MI-komponensek képesek értelmezni a környezeti adatokat, optimalizálni a döntési folyamatokat és előre jelezni a rendszerállapotok változásait. Ez a kooperatív működés lehetővé teszi, hogy az alkalmazások ne statikus funkcionális egységek legyenek, hanem önfejlesztő rendszerek, amelyek képesek reagálni a felhasználói viselkedés, a hálózati környezet vagy a biztonsági fenyegetések mintázataira. A fenntartható biztonság szempontjából különösen jelentős, hogy az MI-vel támogatott alkalmazások képesek a konfigurációs anomáliák, a teljesítményromlás vagy a kockázati indikátorok korai detektálására, ezáltal csökkentve a reaktív beavatkozások szükségességét. Az MI és az alkalmazások integrációja tehát nem csupán technológiai fejlesztés, hanem egy olyan rendszerszintű evolúció, amely a szervezeti működés skálázhatóságát és hosszú távú biztonsági stabilitását alapozza meg.

4.1.1 Mobil eszközök szerepe a biztonság védelmében

A mobil eszközök menedzsmentjének fontossága és kritikus szerepe és fejlesztési irányai elengedhetetlen a városi környezetek biztonságának növelésében, különös tekintettel az adatok és alkalmazások védelmére. Az MDM a létfontosságú infrastruktúrák – például kormányzati épületek, bankok, közműszolgáltatások, közlekedési hálózatok, kommunikációs rendszerek, egészségügyi szolgáltatások és pénzügyi intézmények – védelme a kibertámadásokkal és a terrorizmus fenyegetéseivel szemben nagyban segítheti megteremteni a biztonságot. Az MDM lehetővé teszi a mobil eszközök biztonságos kezelését, biztosítva az érzékeny adatok biztonságos feldolgozását, üzleti tranzakciók lebonyolítását és IT-alkalmazásokhoz való hozzáférést. Ez a stratégia célja, hogy megerősítse a modern városok biztonságát és ellenállóképességét, biztosítva a megbízható és védett digitális működést. A kritikus infrastruktúra védelme biztonságos technológiai megoldásokon keresztül kulcsfontosságú a kockázatok mérséklése és a folyamatos működés fenntartása szempontjából. Az egyes infrastruktúraelemek eltérő funkciókat látnak el, és specifikus szerkezeti megfontolásokat igényelnek. Bár a biztonságos épületek hozzájárulnak a városi biztonsághoz, számos kihívással szembesülnek ennek megvalósítása során, ideértve a kibertámadásokat és az infrastruktúra megzavarására irányuló kísérleteket. Napjainkban számos mindennapi tevékenység, legyen az szakmai vagy magánjellegű, erősen támaszkodik a mobil eszközökre. Ezek a tevékenységek magukban foglalják az érzékeny vállalati adatok kezelését, üzleti levelezést, személyes és szakmai hívások lebonyolítását, banki tranzakciók végrehajtását, valamint különféle IT-alkalmazások használatát. Bármely épület biztonsága nagymértékben függ a robusztus informatikai infrastruktúrától. Ugyanakkor fontos felismerni, hogy az IT-rendszerekhez jogosult személyek hozzáférhetnek, és akár ki is kapcsolhatják azokat. Az MDM ebben a kontextusban kulcsfontosságú megoldásként jelenik meg, amely biztosítja a vállalatok és alkalmazottaik által használt mobil eszközök biztonságos kezelését. [43] [44] [45]

4.1.2 Mobil eszközök menedzselésének megoldásai

A mobil eszközök, amelyeket eredetileg személyes fogyasztói kommunikációs eszközként terveztek, mára a vállalati működés alapvető elemeivé váltak, hálózatokhoz való hozzáférésre és érzékeny adatok feldolgozására használják őket. A készülékek funkcionalitásának bővülésével ezek az eszközök kulcsszerepet játszanak a termelékenység növelésében, ugyanakkor egyedi biztonsági kihívásokat is jelentenek

mobilitásuk és a fenyegetések sokszínűsége miatt. A modern technológiák fogyasztói és vállalati szintű elterjedése a mobil kártevők és sebezhetőségek számának növekedéséhez vezetett. Az érzékeny adatok kiszivárgásának kockázatának mérséklése érdekében a szervezeteknek javasolt robusztus irányelveket, folyamatokat és infrastruktúrákat kialakítani a mobil eszközök, alkalmazások és tartalmak hatékony és biztonságos kezelésére. A Mobile Device Management (MDM) a mobil eszközök – például okostelefonok, táblagépek és laptopok – vállalati környezetben történő adminisztrációját és menedzselését jelenti. Lehetővé teszi az IT- és biztonsági csapatok számára, hogy monitorozzák, kezeljék és biztosítsák az összes, a vállalati hálózathoz csatlakozó mobil eszközt. Ez magában foglalja mind a vállalati tulajdonú, mind a személyes (Bring Your Own Device – BYOD) eszközöket. A mobil eszközök munkahelyi alkalmazásával párhuzamosan az átfogó MDM megoldások elengedhetetlenné váltak. A különböző MDM rendszerek támogatják a szervezeteket az eszközök kezelésében, monitorozásában és védelmében, függetlenül attól, hogy azok milyen mobil szolgáltatónál vagy operációs rendszeren működnek. Az MDM megoldások elengedhetetlenek ahhoz, hogy a szervezetek fenntartsák az irányítást a különböző mobil eszközeik felett, biztosítva, hogy azok biztonságosak, megfelelők és hatékonyan kezeltek maradjanak. Az MDM (Mobile Device Management) megoldások leegyszerűsítik azt a kihívást, amellyel az IT- és biztonsági csapatok szembesülnek a sokféle mobil eszközpark manuális felügyelete során. Ezek a megoldások kiterjedt funkciókat kínálnak, mint például eszközregisztráció, javítócsomag-kezelés, konfigurációs szabályzatok, alkalmazásmenedzsment és távoli hibaelhárítás. Azáltal, hogy ezeket a funkciókat egyetlen platformba integrálják, az MDM világosabb rálátást biztosít az eszközök állapotára anélkül, hogy több különálló eszközre vagy manuális frissítésekre lenne szükség. Továbbá az MDM lehetővé teszi a távoli menedzsmentet egy központi konzolon keresztül, ami különösen előnyös a távoli vagy hibrid munkavégzést alkalmazó vállalatok számára. Ez a képesség biztosítja, hogy minden végpont folyamatosan frissített és védett legyen, kiküszöbölve az IT-csapatok helyszíni eszközregisztrálásának vagy hibaelhárításának szükségességét.

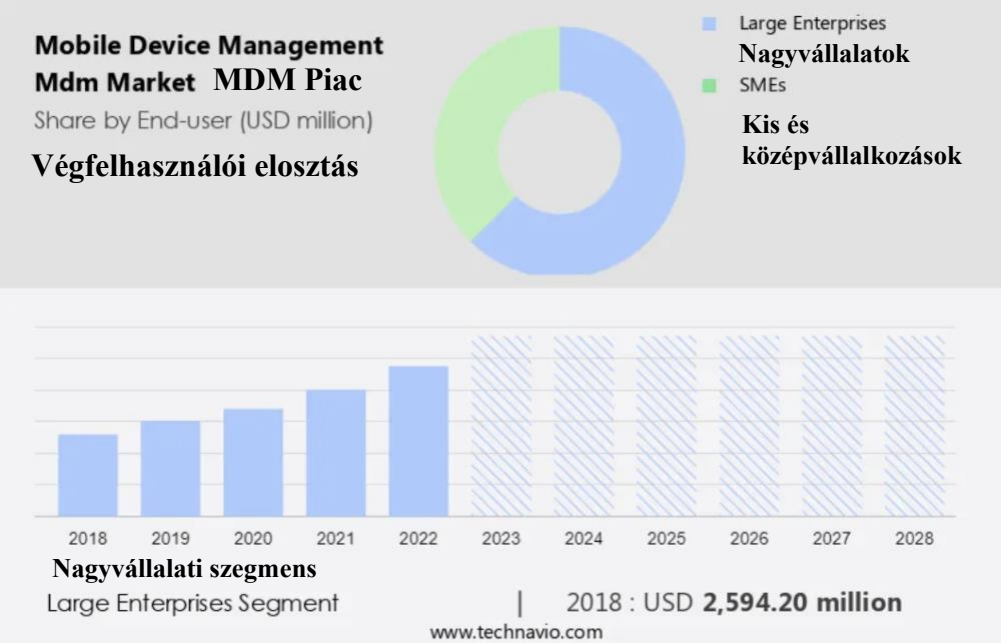
A mobil eszközökhöz való távoli hozzáférés és az alkalmazások biztonságos futtatása olyan vezető MDM megoldásokkal biztosítható, mint az Ivanti [46], a Microsoft Intune [47] és a VMWare Workspace ONE Unified Endpoint Management [48]. Ezek a megoldások jelentősen csökkentik az adatvesztés kockázatát azáltal, hogy biztonságos hozzáférést biztosítanak a belső erőforrásokhoz, miközben lehetővé teszik

biztonságosabb mobil eszközök használatát. Az MDM megoldások folyamatosan fejlődnek, ami egyszerre jelent kihívásokat és lehetőségeket. Az MDM rendszerek fejlesztése nemcsak mobil eszközökre terjed ki, hanem olyan számítógépekre is, amelyek különböző operációs rendszereken – például Windows, Linux és MacOS – futnak. Az elsődleges cél a rosszindulatú alkalmazások kiszivárgásának megelőzése, valamint a vállalatok által tárolt személyes és érzékeny adatok védelme. Az MDM megoldásokkal a vállalati tulajdonú és a magán mobil eszközök egyaránt használhatók minimális korlátozásokkal, mivel a beépített biztonsági szabályozások biztosítják a vállalati és magánadatok szétválasztását. Az Android és az iOS – a két legnépszerűbb mobil operációs rendszer – teljeskörűen támogatott a belső erőforrásokhoz való távoli hozzáféréshez. Az MDM rendszerek modern integrációs megoldásokat kínálnak, amelyek javítják a felhasználói élményt mind az alkalmazottak, mind a rendszergazdák számára. Ez az integráció lehetővé teszi különféle szolgáltatások és alkalmazások egységes működését egy biztonságos hálózati platformon. Emellett az MDM integrálható beléptető rendszerekbe, hozzáférési jogosultságok kezelésébe, röntgenrendszerekbe [49], CCTV rendszerekbe és számos egyéb alkalmazásba, átfogó megközelítést kínálva a mobil eszközök és azok szervezeten belüli használatának kezelésére és védelmére.

4.1.3 Mobil eszközkezelés piaci elrendezése

A Mobile Device Management (MDM) piac jelentős növekedést él meg, és várhatóan mérhetően bővül a következő években. 2026-ban a piac mérete hozzávetőlegesen több mint 10,8 milliárd USA-dollár lesz, és várhatóan körülbelül 30 milliárd USA-dollárra nő 2032-re. [50] [51]

A növekedés fő hajtóerejei közé tartozik a mobil eszközök egyre szélesebb körű vállalati használata, ezen eszközök hatékony kezelése iránti szükség, valamint a növekvő kiberbiztonsági aggályok. A munkahelyi BYOD (Bring Your Own Device) trend és a felhőalapú MDM-megoldások iránti növekvő bizalom szintén hozzájárul a piac bővüléséhez. Regionális elemzés alapján Észak-Amerika rendelkezik a legnagyobb piaci részesedéssel, melyet az fejlett mobiltechnológiák korai elterjedése, a szigorú adatok védelmére vonatkozó szabályozások, valamint a jelentős MDM-szállítói jelenlét indokol. A gyorsabb növekedésre az Ázsia–Csendes-óceáni régió számíthat, amelyet a mobil eszközhasználat növekedése, a fiatal lakosság aránya és a BYOD-trendek ösztönöznek olyan országokban, mint Kína, India és Japán. [52] [53]



9. ábra: *MDM piac méret elemzés 2018-2028.*

Az iparági vertikumok tekintetében a banki, pénzügyi szolgáltatási és biztosítási (BFSI) szektor a legnagyobb piaci szegmens, mivel erős kereslet mutatkozik a biztonság és a megfelelés iránt. Jelentős további szektorok közé tartozik az egészségügy, a gyártás és a kiskereskedelem. A nagyvállalatok uralják a piacot, mivel robosztus MDM-megoldásokat igényelnek a nagy mobileszköz-hálózatok kezeléséhez és a biztonság több részlegen és telephelyen átívelő biztosításához.

4.1.4 A Mobil eszközkezelés főbb jellemzői

Az MDM-megoldások egyszerűsítik a regisztrált eszközök kezelését, miközben nagy mennyiségű eszköz tömeges regisztrációját is lehetővé teszik. Az MDM támogatja az over-the-air (OTA) beállítások és alkalmazások biztosítását. Az MDM a szervezetek számára biztonságkezelési eszközként szolgál, érvényesíti a biztonsági szabályzatokat, mint a jelszókomplexitás és az eszköztitkosítás, valamint elveszett vagy ellopott eszközök esetén távoli zárolási és törlési képességet biztosít. Az alkalmazáskezelési funkció támogatja az alkalmazások telepítését, frissítését és eltávolítását; az alkalmazás-fehérlista és fekete lista képességek MDM-en keresztül valósíthatók meg, továbbá támogatja a vállalati alkalmazások házon belüli terjesztését. Az MDM lehetővé teszi az eszközbeállítások, például Wi-Fi, VPN és e-mail konfigurálását, és korlátozó beállításokkal kontrollálja az eszközfunkcionalitást. Az eszközök állapotának és

megfelelőségének valós idejű monitorozása és jelentéskészítése kiemelten fontos; az MDM követi az eszköz helyzetét és használati mintáit, részletes jelentéseket szolgáltatva az eszközhasználatról, biztonsági eseményekről és megfelelőségről, ezáltal növelve a kockázattudatosságot és segítve a kockázatcsökkentést. A tartalomkezelés keretében az MDM kezeli a vállalati dokumentumok és tartalmak terjesztését és hozzáférés-szabályozását, biztosítva a biztonságos megosztást, együttműködést és mentési lehetőségeket. A megfelelőség és szabályzatok alkalmazása beépítetten jelenik meg automatikus megfelelőség-ellenőrzésekkel és szabályzatfrissítésekkel. A felhasználó- és eszközkezelés lehetővé teszi a felhasználóalapú menedzsmentet, szabályok hozzárendelését szerepek szerint; támogat több eszköztípust és operációs rendszert, és integrálódik szolgáltatásokkal, például Active Directory-val a felhasználói hitelesítéshez. Az MDM hálózati hozzáférés-vezérlése az eszköz megfelelőségi állapota alapján szabályozza a vállalati hálózathoz való hozzáférést, hálózati szeparációt és feltételes hozzáférési szabályokat biztosítva az eszköz egészségi állapota alapján. Az integrációs és interoperabilitási képességek biztosítják, hogy az MDM más IT-menedzsment eszközökkel és rendszerekkel integrálható legyen; az API-támogatás egyedi integrációkat tesz lehetővé, és a rendszer együttműködik a meglévő infrastruktúrával, mint e-mail szerverek és VPN-ek. A felhasználói élmény önkiszolgáló portálok révén javítható, amelyek lehetővé teszik a felhasználók számára saját eszközeik kezelését; az MDM intuitív felületeket biztosít adminisztrátoroknak és végfelhasználóknak, minimalizálva az eszköz teljesítményére és a felhasználói produktivitásra gyakorolt hatást. A skálázhatóság és teljesítmény kritikus: az MDM-megoldások képesek több ezer eszköz kezelésére több telephelyen át, magas rendelkezésre állást és redundanciát biztosítva, így gyors válaszképesség tartható fenn nagy eszközpark mellett; ezek a jellemzők együttesen lehetővé teszik a szervezetek számára, hogy hatékonyan kezeljék és védjék mobil eszközeiket, biztosítva azok termelékeny használatát anélkül, hogy a biztonság sérülne.

4.1.5 Hatékony mobil központi felügyelet architektúra fejlesztése

Az effektív MDM-architektúra kialakítása több kritikus követelményt foglal magában annak érdekében, hogy a mobil eszközök átfogó kezelése, biztonsága és skálázhatósága biztosított legyen egy szervezeten belül. Az architektúra tervezésekor számos fontos szempontot kell figyelembe venni: elengedhetetlen a felhőalapú környezetben való üzemeltetés, továbbá szükséges egy biztonságos és elkülönített hálózat létrehozása;

kulcsfontosságú a saját fejlesztésű vagy megbízható forrásból származó mobilalkalmazások telepítése; a különböző rendszerek kommunikációjának integrálása, biztonságos hálózatra helyezése és ezeknek az alkalmazásoknak a menedzselése összetett feladat, jelentős integrációs erőfeszítéseket igényel. Ezek az alkalmazások és szerverek jelentős tárolókapacitást igényelnek rendszerszintű megoldással; minden komponensnek saját tárolóra van szüksége a működési adatok gyors elérésének biztosítása érdekében. A biztonságos kommunikáció SSL (Secure Sockets Layer) és TLS (Transport Layer Security) protokollokkal valósítható meg. A felhőinfrastruktúrán futtatható környezet létrehozható úgy, hogy egyszerre szolgálja ki az egész alkalmazáskomplexumot. A felhasználók azonosításához hitelesítés szükséges, amely megvalósítható felhő-megoldással, például Microsoft Entra ID-vel; ez a komponens független szolgáltatásként működik majd a megfelelő jogosultságok kiosztására és kezelésére. A naplókezelés szintén kritikus szolgáltatás, amely rendszer-szintű szolgáltatásként kell, hogy működjön, mivel elengedhetetlen a rendszerfelügyelethez; a monitorozás magában foglalja a hardver- és szoftverműködési mutatók gyűjtését az alkalmazások és szerverek helyes működésének ellenőrzésére, és az operátorok feladata ezen adatok elemzése a magas rendelkezésre állás biztosítása érdekében. Emellett figyelembe kell venni az orientációt, beleértve a mobil eszközmenedzsmenttel és az integrált szolgáltatásokkal érintett területek megjelenítését és megközelítését, hogy a felhasználói beavatkozás és interakció hatékonyan támogatott legyen. [54] [55] [56] [57]

4.1.6 Mobil központi felügyelet környezetének létrehozása

A fejlesztési, teszt- és éles IT-környezetek létrehozása fontos előfeltétel. A teszt- és éles környezetek több integrált rendszerrel fognak működni, ami több virtualizált környezetet jelent. Ezeken a virtuális szervereken számos automatizált folyamatot kell létrehozni, többek között mentési, archiválási és visszaállítási folyamatokat. Ezeket külön dokumentumban is rögzíteni kell. A mentési ciklusok például lehetnek teljes, differenciális vagy inkrementális mentések. A teljes mentés magában foglalja a kiválasztott összes adat és konfiguráció elmentését. A teljes mentés képezi a differenciális mentés kiindulópontját. A differenciális mentés csak a teljes mentéshez képest hozzáadott vagy megváltozott adatok mentését jelenti, míg az inkrementális mentés szintén a teljes mentésre épül, de abban különbözik a differenciálistól, hogy az új mentések a korábbi mentéseket használják összehasonlítási referenciaként. Felhasználói profilok beállítása, jogosultságok meghatározása, fájl- és mappastruktúrák kialakítása, előre definiált

üzemeltetési feladatok és naplóelemzési folyamatok szintén a kidolgozandó feladatok közé tartoznak. A kiépített rendszerek szükséges tesztelése elengedhetetlen. A széles körben elfogadott tesztelési gyakorlat szerint a működési és tesztelési költségek csökkentése érdekében meghatározandó egy optimális tesztelési stratégia.

4.1.7 Központi naplóelemző rendszer integrációja

Még a legjobban strukturált IT-rendszerek és szabályozások mellett is előfordulhatnak biztonsági rések és incidensek. Egy hatékony megelőzési és detektálási módszer minden eszköz központi naplóelemző rendszerhez való csatlakoztatása, amely algoritmusokat alkalmaz a naplóbejegyzések elemzésére és kategorizálására; ez a folyamat kritikus a folyamatban lévő támadások észleléséhez, a további károk megelőzéséhez és az esemény utáni vizsgálathoz. A központosított naplógyűjtés és eseménymenedzsment rendszerek hatékonyan szolgálják ezeket a célokat, a Security Information and Event Management (SIEM) rendszerek kiváló megoldást nyújtanak a biztonsági incidensek és események kezelésére. A SIEM olyan biztonsági megoldás, amely segíti a szervezeteket a potenciális fenyegetések és sebezhetőségek azonosításában és kezelésében, még mielőtt ezek üzleti működést zavarnának; a SIEM rendszerek lehetővé teszik vállalati biztonsági csapatok számára a felhasználói viselkedés anomáliáinak észlelését és a mesterséges intelligencia alkalmazását a fenyegetésészleléshez és incidensválaszhoz kapcsolódó számos manuális folyamat automatizálására. A részletes elemzéshez és visszakereshetőséghez hosszú távú adattárolás szükséges, amely magában foglalja az adatok elemzését és megjelenítését, mintázatok felismerését és a normálistól eltérő tevékenységek vagy adatok keresését. Korrelációs elemzés: a SIEM rendszereket úgy tervezték, hogy az adatokat értelmezhető egységekké rendezzék, amelyek hasonlóságokat és közös pontokat mutatnak; a korreláció elsődleges célja a nyers adatok hasznos és átlátható információvá alakítása, ami jelentősen növeli a fenyegetésészlelés és válaszadás hatékonyságát. Riasztások és értesítések: a SIEM rendszerek riasztási küszöbértékeket állapítanak meg a gyűjtött adatokra a potenciális biztonsági problémák azonosításához; ezeknek a küszöböknek a túllépésekor a rendszerek protokollokat indíthatnak el a felhasználók figyelmeztetésére; ezek az értesítések különböző módokon érkezhetnek, például push értesítések, automatizált e-mailek vagy SMS-ek formájában, továbbá megjelenhetnek irányítópultokon vagy a Mobile Device Management (MDM) rendszerek által kezelt mobil eszközökön. Adataggregáció: a SIEM rendszerek képesek adatokat gyűjteni széles körű, csatlakoztatott rendszerekből, beleértve szervereket, hardvert, hálózatokat,

adatbázisokat, szoftvereket és összetett üzemi alkalmazásokat; ez az átfogó adataggregáció lehetővé teszi a kiterjedt monitorozást és elemzést az egész IT-infrastruktúrán belül. Figyelembe véve az IT- és biztonsági eszközök által generált hatalmas naplómennyiséget, a naplósorok közötti korrelációk elemzése szinte lehetetlen egy biztonsági naplóelemző rendszer nélkül; elengedhetetlen a belső erőforrások hatékony elosztása a SIEM rendszer működtetésének biztosításához, beleértve a rendszer által gyanúsnak ítélt incidensek kivizsgálását. Egy központi naplóelemző rendszer, mint a SIEM, integrálása alapvető a szervezet IT-környezetének biztonságának és integritásának fenntartásához; az MI-t a fenyegetésészleléshez használva, az incidensválasz folyamatokat automatizálva és a hosszú távú adatelemzést engedélyezve a SIEM rendszerek javítják a megelőzés, észlelés és hatékony reagálás képességét a biztonsági eseményekre. [58]

4.1.8 Mobil központi felügyelet incidenskezelési és monitoring megoldásai

Az IT- és biztonsági rendszerek szerves részeihez tartozó eszközök és alkalmazások naplófájlokat generálnak, amelyek létfontosságúak a rendszerek biztonsági állapotának és tevékenységeinek nyomon követéséhez; elengedhetetlen meghatározni a naplózandó események optimális körét és az egyes eseményekhez rögzítendő konkrét adatokat. A biztonsági eseménynaplókat a törvény által előírt ideig meg kell őrizni, ezért ezt figyelembe kell venni a mentési eljárások meghatározásakor. Az elszámoltathatóság és az auditálhatóság biztosításához a biztonsági naplóknak lehetővé kell tenniük az esemény utáni visszakeresést és a rendszerben bekövetkezett biztonsági események azonosítását; a rendszernek képesnek kell lennie minden felhasználó vagy felhasználói csoport által végrehajtott művelet rögzítésére. A rendszerindítások és leállások során keletkező naplóbejegyzések különösen értékesek hiba, incidens vagy tervezett beavatkozás esetén, mivel megkönnyítik a leállások okainak azonosítását; emellett a rendszerórabeállítások, például az óraátállítások miatti változások kritikus események a naplókban. Óra visszaállításakor fontos a naplók mentése, mert a kritikus egyórás periódust meg kell őrizni, hogy az új naplók ne írják felül az előző órában keletkezetteket. Azonosítási és hitelesítési folyamatoknak különféle tevékenységeket kell követniük a biztonság és elszámoltathatóság biztosítása érdekében; ez magában foglalja a sikeres bejelentkezések, bejelentkezési kísérletek és kijelentkezések naplózását, valamint a felhasználó által kezdeményezett és a rendszer által kikényszerített jelszóváltoztatások nyomon követését, amelyek elengedhetetlenek a jelszóintegritás fenntartásához. A rendszernek rögzítenie

kell a fiókok zárolási és feloldási eseményeit, legyenek azok automatikusak vagy kézi beavatkozással történők, valamint dokumentálnia kell olyan műveleteket, mint felhasználói fiókok tiltása vagy törlése, különösen, ha egy munkavállaló hozzáférési jogosultságait visszavonják. Alkalmazásmenedzsment: az alkalmazások és szolgáltatások tevékenységét folyamatosan monitorozni kell; a rendszernek naplóznia kell az alkalmazások, szolgáltatások vagy feladatok indítási és leállási eseményeit, beleértve a hibák vagy incidensek miatti szabályos leállásokat is, ami segíti a problémák diagnosztizálását és megoldását. Konfigurációs fájlok és scriptek kezelése (Linux, Windows): a konfigurációs fájlok és scriptek menedzsmentje kritikus; ezekkel a fájlokkal kapcsolatos tevékenységeknek tartalmazniuk kell a létrehozást, törlést, módosítást és lekérdezési folyamatokat, biztosítva, hogy minden változás dokumentált legyen a későbbi visszakeresés és elszámoltathatóság érdekében. Erőforráskezelés: a rendszererőforrások, mint a CPU, memória és tárhely változásait gondosan rögzíteni kell; ide tartozik ezen erőforrások létrehozása, törlése, növelése vagy csökkentése, ami elengedhetetlen az optimális rendszer-teljesítmény és erőforrás-allokáció fenntartásához. Munkavállalói műveletek: az eltérő jogosultsággal rendelkező munkavállalók által végzett, a rendszer működését és biztonságát érintő műveleteket alaposan nyomon kell követni; ez magában foglalja felhasználói fiókok létrehozását, technikai felhasználók háttérscriptek futtatását, felhasználói jogosultságok módosítását, valamint felhasználók tiltását vagy törlését. Hasonlóképp minden Active Directory szerepváltozást — létrehozás, jogosultságadás, módosítás vagy törlés — naplózni kell a felhasználói tevékenységek teljes körű nyomon követéséhez. Tevékenység- és érzékeny adat lekérdezések: az eszközök tevékenységének és az érzékeny adatok kezelésének monitorozása pontos dokumentációt igényel; a rendszernek rögzítenie kell az érzékeny adatok létrehozását, módosítását, törlését, másolását és áthelyezését, biztosítva, hogy minden művelet átlátható és visszakövethető legyen. Esemény- és biztonsági riasztáskezelés: események és biztonsági riasztások kezelésekor létfontosságú rögzíteni az esemény észlelésének idejét és az okot, illetve törekedni az ok feltárására, ha az ismeretlen; részletes leírást kell adni az eseményről, beleértve rövid és hosszú távú üzleti hatásait, valamint dokumentálni kell az eseménnyel kapcsolatos karbantartási tevékenységeket és azok sikerességét vagy sikertelenségét. A rendszernek priorizálnia kell a biztonsági riasztásokat, azonosítania a riasztáshoz kapcsolódó felhasználói köröket és csoportokat, meghatározni a kapcsolódó objektumokat és épületeket, továbbá rögzíteni azokat a felhasználókat és csoportokat, amelyek az esemény megoldásáért felelősek, valamint a riasztást kiváltó megelőző

intézkedéseket. Ezeknek a részletes elvárásoknak való megfelelés esetén az azonosítási és hitelesítési folyamatok biztonságos és elszámoltatható IT-környezetet biztosítanak, megkönnyítve az alkalmazások, erőforrások, munkavállalói műveletek, adat-tevékenységek és biztonsági események hatékony kezelését. Az adathordozók (beleértve a papír- és digitális formátumokat) védelmére szolgáló intézkedéseket gondosan ki kell dolgozni és végrehajtani. A hozzáférést csak jogosult személyekre szabad korlátozni, és a hozzáférési jogosultságokat beléptetéskor, kiléptetéskor és rendszeres, évközi időközönként felül kell vizsgálni. Különös figyelmet kell fordítani az adathordozók beszerzésére és selejtezésére, különös tekintettel a megfelelő jelölésre, biztonságos szállításra és tárolási gyakorlatokra annak érdekében, hogy ne sérüljön a szervezet integritása. Az adathordozókat zárt, biztonságos helyen kell tárolni az illetéktelen hozzáférés és a lopás elleni védelem érdekében. [59]

4.1.9 Mobil központi felügyelet biztonsági rendszerterv

A mobil eszközök menedzsmentje (MDM) kulcsfontosságú a kritikus környezetek védelmében, különösen természeti katasztrófák esetén, mivel biztosítja a kritikus adatokhoz és kommunikációs csatornákhoz való megszakítás nélküli hozzáférést árvíz, földrengés vagy hurrikán idején; az MDM által biztosított protokollok és szolgáltatások lehetővé teszik a gyors reagálás-koordinációt, az időérzékeny riasztások kézbesítését, a mentési műveletek összehangolását és az alapvető szolgáltatások folyamatos működtetését kedvezőtlen körülmények között is. Az MDM emellett jelentősen csökkenti a kiberfenyegetésekből eredő kockázatokat azáltal, hogy konzisztens biztonsági intézkedéseket érvényesít a mobil végpontokon, megőrizve az adatintegritást a sebezhetőségek közepette, valamint mérsékli az emberi hibákból fakadó incidenseket azáltal, hogy egységes szabályozást és automatizált kontrollokat alkalmaz a vállalati és személyes eszközök felett; ezen intézkedések beépítése a katasztrófavédelmi tervekbe növeli az ellenállóképességet, megerősíti az infrastruktúra biztonságát, és javítja a közbiztonságot mind természetes, mind mesterséges (kiber-) veszélyek esetén. Az auditálási követelmények teljesítéséhez elengedhetetlen minden egyes biztonsági rendszerre vonatkozó részletes rendszerterv kidolgozása, amely tartalmazza a kritikus infrastruktúra-elemek védelmi szintjének felmérését, a rendszerek 1–6-ig terjedő kategorizálását (a magasabb számok nagyobb biztonsági követelményt jelölnek), valamint a rendszer típusának, verziójának és fejlesztési életciklusának meghatározását a teljes körű tervezés érdekében. A dokumentációnak világosan rögzítenie kell a

szerepköröket, jogosultsági mátrixokat és napi üzemeltetési eljárásokat; a rendszertervnek részleteznie kell a funkciókat, hálózati elemeket, protokollokat és szolgáltatásokat, valamint egyértelműen definiálnia kell a biztonsági határokat és védelmi mechanizmusokat a kitűzött célok eléréséhez. Az integrációt kapcsolódási diagramok segítik, továbbá a rendszerkódok és interfészek alapos tesztelése és értékelése szükséges az üzemkész állapot garantálásához. Az üzemeltetés és felügyelet biztonságának garantálásához 0–24 órás, dedikált IT-szakértői ügyeleti csoport létrehozása szükséges a teljes IT-biztonsági környezet folyamatos monitorozására és távoli menedzsmentjére; emellett kötelező külső támogatói és beszállítói szerződések megléte a gyors incidenskezelés érdekében, valamint azonnali eljárások a meghibásodott eszközök sürgős helyettesítésére. Az IT-szolgáltatásmenedzsment bevett gyakorlatait tükröző ITIL-irányelvek követése ajánlott az üzemeltetési és fejlesztési folyamatok standardizálására. A hitelesítési és hozzáférés-kezelési szabályok tekintetében a jelszók követelményei szigorúak: legfeljebb 120 karakteres maximális és legalább 12 karakteres minimális hossz, a kis- és nagybetűk, számok és speciális karakterek kombinációjának alkalmazásával; az adatintegritás biztosítására robusztus kriptográfiai algoritmusok alkalmazandók, például SHA-512/256, SHA3-224 és SHA3-256; a hálózati forgalom és adatkapcsolatok védelmét a legnagyobb verziószámú TLS protokollal kell biztosítani, figyelembe véve a protokollok alkalmazási környezetre szabott konfigurációját és a folyamatos biztonsági frissítések szükségességét.

4.1.10 Folyamatos fejlődési területek

A Mobile Device Management (MDM) rendszerek alapvetővé váltak az adatok védelmében és az alkalmazások menedzselésében, különösen a kritikus infrastruktúrák, gépjárművek esetében, ugyanakkor a meglévő MDM-megoldások több területen továbbfejleszthetők hatékonyságuk és használhatóságuk javítása érdekében. Kiemelt funkcionális követelmények közé tartozik a megbízható felhasználóazonosítás, a vállalati belső erőforrásokhoz való biztonságos hozzáférés, az e-mail rendszerekbe integrált eseménymenedzsment, az alkalmazáshasználat követése, az eszközlokalizáció és a jogosulatlan hozzáférési kísérletek naplózása; működésbiztonsági szempontból elengedhetetlen a kritikus infrastruktúrák megszakítás nélküli üzemeltetésének biztosítása, melyet az integrált rendszerek hatékonyságának növelése támogat. A növekvő kifinomultságú kiberfenyegetések elleni védekezés megköveteli fejlett biztonsági intézkedések alkalmazását, így az MI és gépi tanulás bevonását a

fenyegetésészlelésbe, valamint a zero trust elv szerinti, granuláris hozzáférés szabályozást. A skálázhatóság és a teljesítmény kritikus tényezők; szükséges az eszközterhelés növekedésének kezelése és az erőforrás-felhasználás optimalizálása a teljesítményromlás elkerülése érdekében. A megfelelőség és jelentéskészítés megerősíthető automatizált megfelelőség-monitorozással és részletes, testreszabható riportfunkciókkal, amelyek napi, heti, havi és éves statisztikákkal képesek kiemelni a váratlan eseményeket és elősegíteni az előre tervezett intézkedéseket. Az MI alkalmazása támogatja az incidensek és kérések dinamikus kezelését, javítja a felhasználói támogatást és lehetővé teszi az adaptív reagálást az új trendekre; e célból indokolt a Unified Endpoint Management (UEM) bevezetése, amely egyetlen platformról kezeli a mobil, asztali és IoT végpontokat, továbbá bővíteni kell az alkalmazásmenedzsment képességeit a telepítés, monitorozás és életciklus-védelem terén. A jövőorientált MDM-rendszereknek támogatniuk kell a felmerülő technológiákat, például az 6G hálózatokat és az IoT-eszközöket, valamint integrálniuk kell az edge computing elemeit a gyorsabb adatfeldolgozás és a csökkentett késleltetés érdekében; az adatok védelmét korszerű titkosítási módszerek alkalmazásával kell erősíteni, egyidejűleg több kontrollt biztosítva a felhasználók számára a magánszféra-beállításaik felett a bizalom és a megfelelés fenntartása céljából. A távoli menedzsment képességei javíthatók fejlett távoli diagnosztikai és hibajavító eszközökkel, valamint egyszerűsített frissítési és javítófolyamatokkal; költséghatékony integrációs lehetőségek vizsgálata is lényeges, például az alkalmazástérképek megjelenítése az MDM-felületen a problématerjedelem gyors meghatározására, incidencialapú űrlapok automatikus kitöltése és feladatkiosztás a vállalati e-mail rendszeren keresztül, illetve automatizált értesítések küldése a releváns kollégáknak, csökkentve a fizikai kontaktusok szükségességét, minimalizálva a járványok idején a fertőzéskockázatot és lerövidítve a reagálási és végrehajtási időket. Az MDM-ek hatékony használatához átfogó képzési programokra és fejlett ügyféltámogatási szolgáltatásokra van szükség a felhasználók és az IT-személyzet támogatására; továbbá fontos a testreszabott szabályzatok és rugalmas telepítési opciók (on-premise, felhőalapú és hibrid) biztosítása, hogy a szervezetek saját működési és szabályozási igényeik szerint alakíthassák rendszereiket. E területek következetes kezelése révén az MDM-rendszerek robusztusabbá, felhasználóbarátabbá és alkalmasabbá válhatnak a modern vállalatok és a kritikus infrastruktúra menedzsmentjének folyamatosan változó követelményeinek kielégítésére. [60] [61]

4.1.11 Kritikus infrastruktúrák biztonságának javítására való lehetőségek

A biztonság növelése érdekében az MDM rendszereknek több kritikus funkciót kell támogatniuk. Például elengedhetetlen a különböző riasztási lehetőségek — tűzriasztás, behatolásérzékelés és tiltott tárgyak detektálása — integrálása a rendszerbe; gyorsan azonosítani kell a riasztási esemény helyszínét, hozzáférni az esemény közelében elhelyezett kamerák élő képéhez, valamint meghatározni a kollégák GPS-koordinátáit a legrövidebb útvonal megtervezéséhez a riasztási pontig. Ez az integráció magában foglalja a menekülési útvonalak tervezését evakuációs helyzetekre, továbbá biztosítania kell, hogy az épület vészjelző rendszereinek hang- és vizuális figyelmeztetései mobil eszközökön is megjelenjenek.

Az MDM folyamatos koordinációt tesz lehetővé a biztonsági járőrökkel úgy, hogy dinamikusan számolja és optimalizálja a járőrök útvonalait, valamint egyszerűvé teszi a járőrtevékenység követését és támogatását kamerarendszeri képek felhasználásával. A digitális információs kijelzők fontos szerepet játszanak forgalmas csomópontokban a dinamikus tartalmak megjelenítésében, segítve a biztonsági beavatkozásokat, például forgalomtereléseket; ezek a kijelzők sugározhatnak videót, nyújthatnak vizuális segédletet vészhelyzetben és közérdekű tájékoztatást. Különösen fontos, hogy a digitális táblákon megjelenített üzenetek elérhetőek legyenek mobil eszközökön is, mert ez felgyorsítja a vészhelyzeti beavatkozást. A példák beépítésével az MDM rendszerek jelentősen növelhetik a városi környezetek biztonságát és hatékonyságát, biztosítva, hogy a kritikus infrastruktúrák és a közbiztonsági intézkedések következetesen menedzselhetők és fenntarthatók legyenek. A városi infrastruktúra biztonságának garantálása nagymértékben függ a megbízható Mobile Device Management gyakorlatok bevezetésétől; ez alapvető a különféle fenyegetések hatékony mérsékléséhez. A természeti katasztrófák — árvíz, földrengés, hurrikán — jelentős kockázatot jelentenek a kritikus rendszerekre, veszélyeztetve mind a fizikai eszközöket, mind a lakosság biztonságát. Az üzemeltetési figyelmetlenségből vagy hanyagságból eredő emberi hibák tovább növelik az infra rendszerek sérülékenységét, súlyos következményekkel járva, ami alapos felügyeleti és szabályozási eljárások szükségességét támasztja alá. Ezen túlmenően a céltudatos támadások és a kiberbűnözés komoly kihívást jelentenek: a rosszindulatú szereplők kritikus rendszerek ellen irányuló támadásokkal fennakadásokat okozhatnak vagy érzékeny adatokat kompromittálhatnak, veszélyeztetve a gazdasági stabilitást és a közbizalmat.

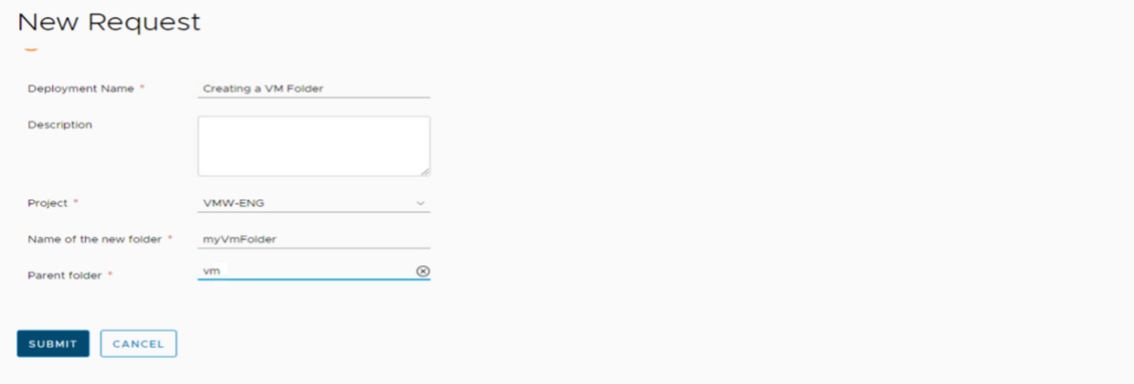
Az átfogó MDM-stratégiák alapvető szerepet játszanak ezen kockázatok mérséklésében azáltal, hogy szigorú biztonsági intézkedéseket érvényesítenek, folyamatosan monitorozzák az eszközhozzáférést és használatot, valamint gyorsan reagálnak az esetleges megsértésekre. Átfogó MDM-megoldások bevezetésével a kritikus infrastruktúrák környezetei ellenállóbbá tehetők a különféle fenyegetésekkel szemben, biztosítva az alapvető szolgáltatások folytonosságát és integritását. A mobil eszközök proaktív menedzsmentje nemcsak a működési hatékonyságot növeli, hanem erősíti az általános biztonsági helyzetet is, védelmet nyújtva az egyre összetettebb kockázatokkal szemben egy mindinkább összekapcsolt világban. A bevett gyakorlatok követése és az új trendek figyelemmel kísérése biztosítja, hogy az MDM-stratégiák továbbra is megbízhatók és hatékonyak maradjanak.

4.1.12 Teszt környezet létrehozása

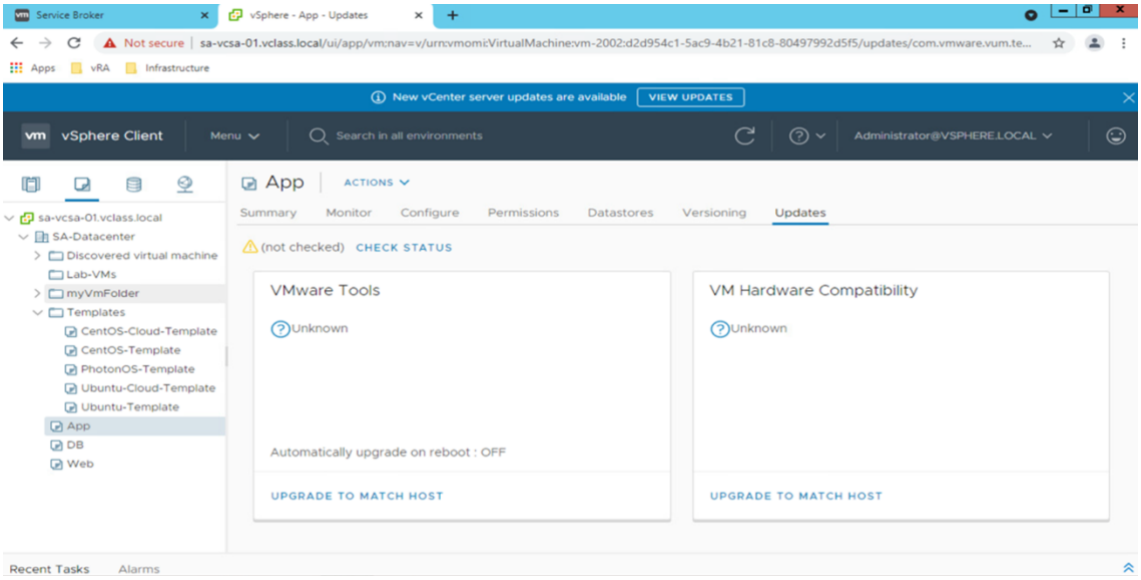
A mobil eszközmenedzsment (MDM) rendszerek és a mesterséges intelligencia (MI) integrációja egyre meghatározóbb szerepet tölt be a kritikus informatikai környezetek védelmében, különösen olyan infrastruktúrák esetében, ahol a mobil hozzáférés, a decentralizált eszközhasználat és az érzékeny adatkezelés együttesen jelentős kockázatokat hordoz. A 4. hipotézis szerint az MDM és MI együttes alkalmazása képes jelentősen csökkenteni az adatszivárgás, a jogosulatlan hozzáférés és a manipuláció kockázatát — ennek tudományos szintű igazolását egy célzottan kialakított telepítési tesztkörnyezetben tudom megvalósítani.

A tesztkörnyezet lehetőséget biztosít az MDM-rendszer az eszközszintű viselkedésmintáinak és MI-alapú döntési mechanizmusainak szimulált, kontrollált körülmények közötti vizsgálatára. Ezáltal validálható, hogy az MI képes-e időben detektálni, azonosítani az incidenseket, jogosultsági anomáliákat, és automatizáltan beavatkozásni. A tesztkörnyezet tudományosan igazolja a 4. hipotézisben megfogalmazott állítást: az MDM és MI integrációja képes proaktívan csökkenteni a mobil eszközökből eredő biztonsági kockázatokat. A tesztkörnyezetben kapott eredmények hozzájárulnak a rendszer éles bevezetésének biztonsági megalapozásához.

Létrehoztam a Mobile Device Management szervereket VMware környezetben.
Az alábbi felhasználóval (administrator) belépek a vSphere Client (sa-vcsa-01) szerverre és a SA-Datacenteren belül a myVMFolderbe létrehozom a teszt szervereket, beállítom a hálózatot és a jogosultságokat:

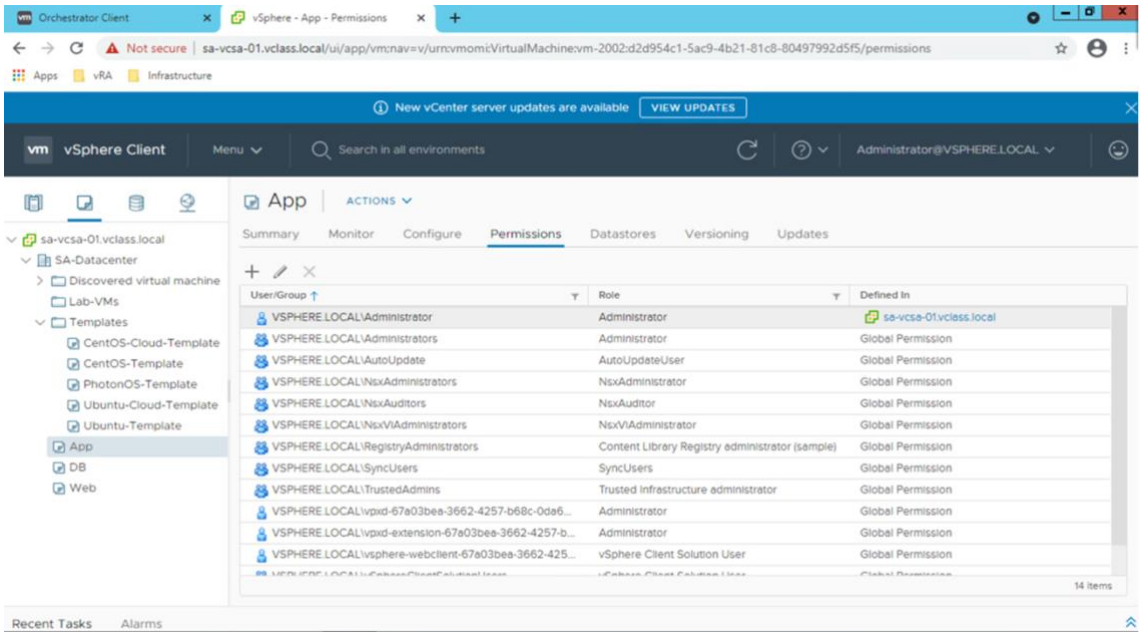


10. ábra: *VM könyvtár*



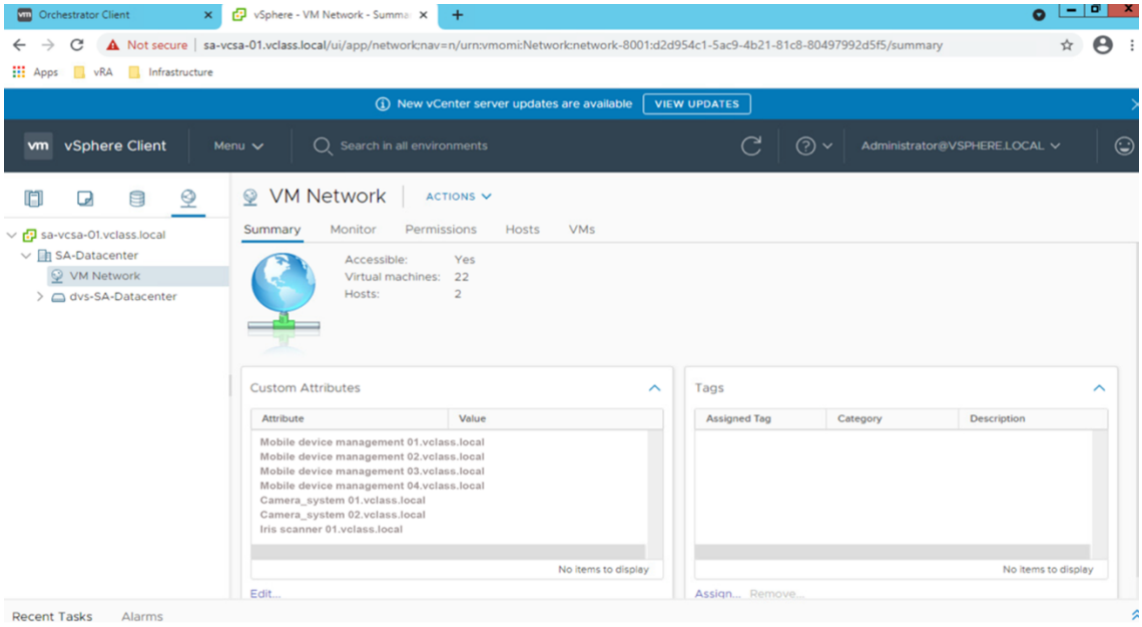
11. ábra: *vSphere Client*

Létrehoztam a jogosultsági köröket, amivel a szerverekhez és a különböző feladatok elvégzéséhez szükséges hozzáférnem.



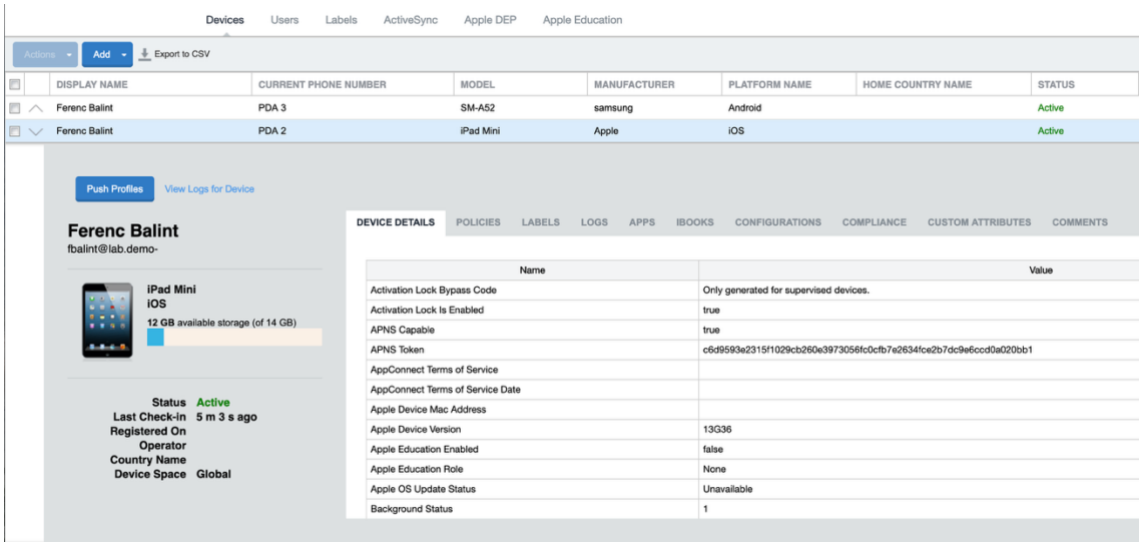
12. ábra: *vSphere Client - jogosultságok*

Elvégzem a SA-Datacenter hálózati beállításait. Létrehoztam 22 db virtuális teszt szervert. A teszt szerverek feladatait és az integrációkat a 4.1.13. fejezet architektúra ábráján szemléltetem.



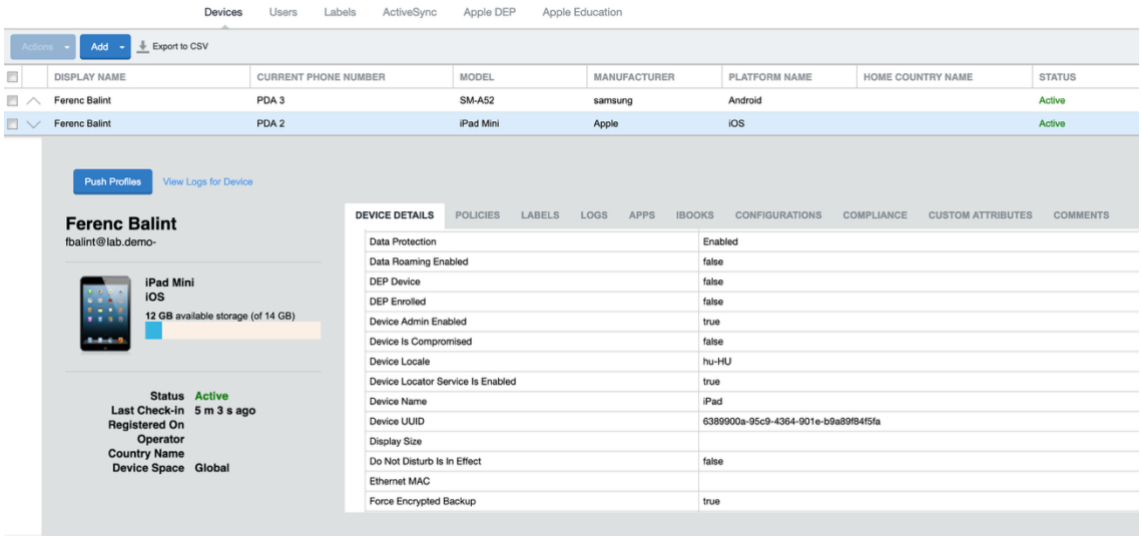
13. ábra: *vSphere Client - jogosultságok folytatás*

Az alábbi képen látható a létrehozott szervereken elindítom az MDM alkalmazást. Az MDM alkalmazásban elindítom az IOS teszt eszköz telepítését.

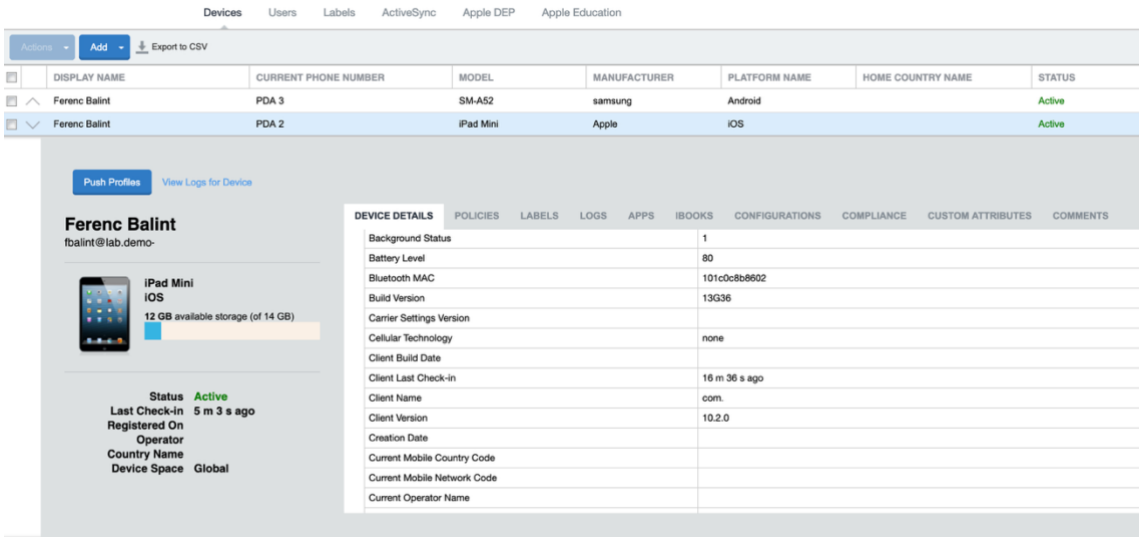


14. ábra: *MDM alkalmazás – eszközök telepítése*

Az MDM alkalmazásban pontosítom az IOS eszköz beállításait és ellenőrzöm a konfigurációs értékeket.

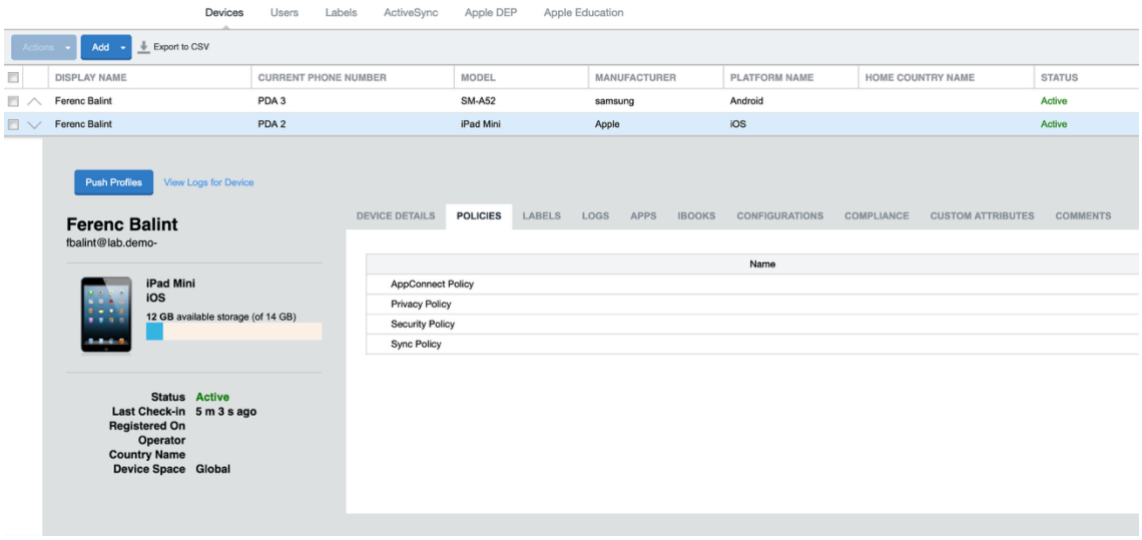


15. ábra: *MDM alkalmazás – eszközök telepítése folytatás*



16. ábra: *MDM alkalmazás – értékek ellenőrzése*

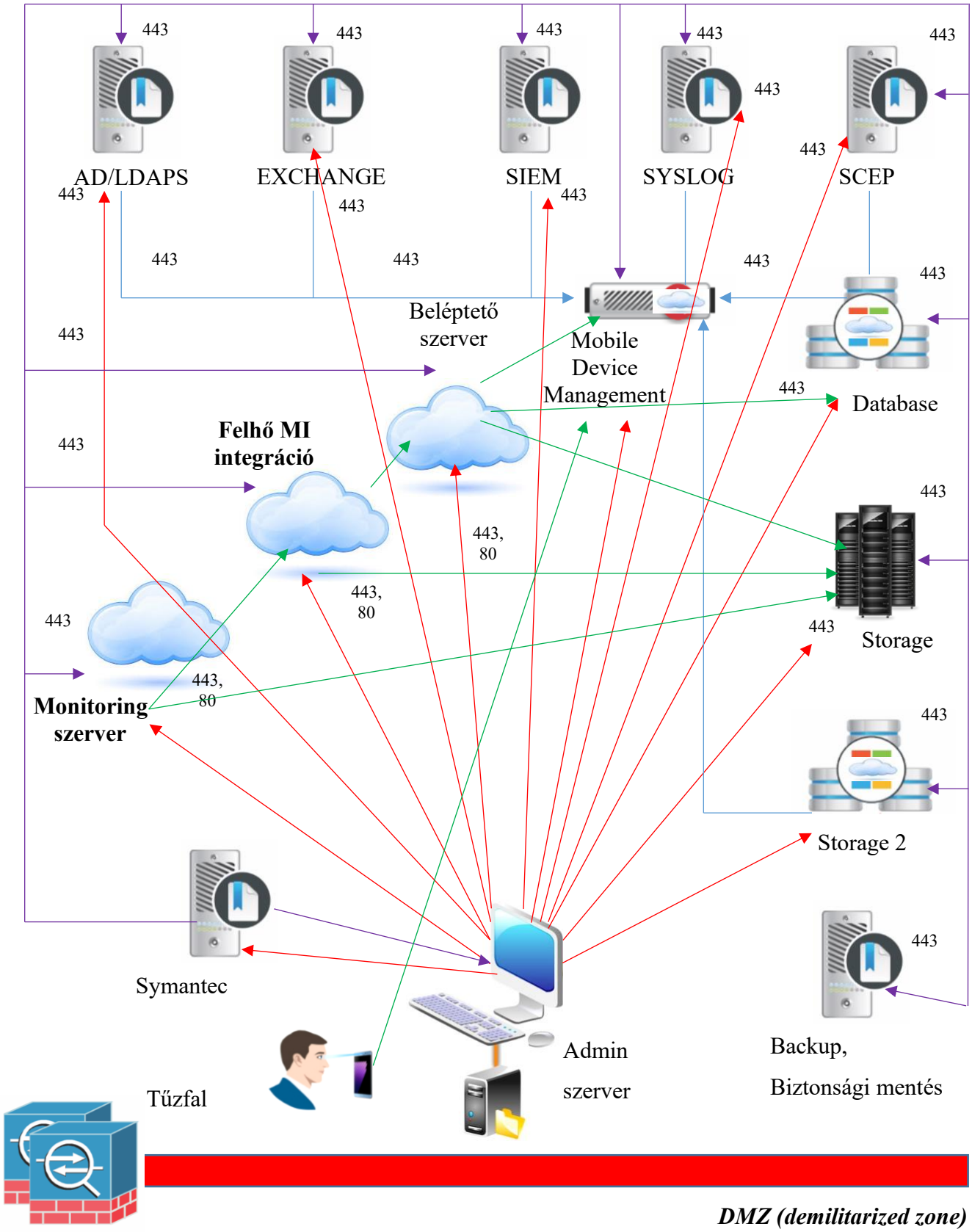
Az MDM alkalmazásban beállítom a policy-kat és hozzárendelem az IOS eszközhöz.



17. ábra: *MDM alkalmazás – értékek ellenőrzése folytatás*

4.1.13 Teszt környezet integrálása

Az előző fejezetben a létrehozott szervereket integrálom MI + monitoring és log managementel. Az integráció kialakítása mellé még számos különböző moduláris infrastruktúra típusokhoz való illeszkedést is megvalósítom, ezután ellenőrzöm a működést.



18. ábra: *Integráció – Forrás: saját kép*

Az ábrán látható rövidítések meghatározása:

AD = Active Directory szerver (Felhasználók kezelése, jogosultság kezelés)

Exchange = Levelező szerver

Symantec = Vírusírtó szerver

SYSLOG = LOG (naplóbejegyzés) gyűjtő szerver

SCEP = Tanúsítványkezelő szerver (felhasználóknak, szervereknek)

SIEM = Biztonsági incidensek és események kezelésére szolgáló szerver

Storage = Háttértár a szervereknek

Storage 2 = Lokális háttértár

Database = Adatbázis szerver

Admin szerver = központi szerver – szerver admin jogosultsággal lehet belépni rá

MDM = MDM kapcsolati szerver a DMZ zónában lévő többi MDM szerverekkel. Innen lehet majd kapcsolódni az Internet irányába az MDM szerverein keresztül. Ez ahhoz szükséges, hogy titkosított 443 porton keresztül a megfelelő jogosultsággal rendelkező felhasználók mobil készülékeivel be tudjanak lépni a rendszerkomponensekbe, alkalmazásokba.

A kialakított architektúrában fontos, hogy a rendszerek skálázható, monitorozható és biztonságosak legyenek, lehetővé téve különböző infrastruktúra típusokhoz való illesztést. A cél egy olyan architektúra formalizálása, amely modulárisan integrálja a következő komponenseket:

- Érzékelési réteg: fizikai és logikai szenzorok, amelyek valós idejű adatokat gyűjtenek a rendszer állapotáról (pl. hálózati forgalom, tűzfal, fizikai hozzáférés, környezeti paraméterek).
- Hálózati és irányítási logika: az adatok előfeldolgozása és továbbítása, valamint az automatizált döntési mechanizmusok (pl. szabályalapú vagy gépi tanuláson alapuló vezérlés).
- Felügyeleti monitoring interfészek: vizualizációs és beavatkozási felületek, amelyek lehetővé teszik az üzemeltetők számára az állapotmonitorozást és az eseményekre való reagálást és a különböző konfigurációk ellenőrzését.

4.1.14 Az előre definiált szempontok elemzése

• Észlelési pontok definiálása: érzékenység, pontosság, hamis riasztások kiszűrése.
Az érzékenység azt mutatja meg, hogy a rendszer milyen arányban képes felismerni a valódi biztonsági eseményeket (pl. jogosulatlan hozzáférés, konfigurációs manipuláció, nem engedélyezett tevékenységek).

Az alábbi tesztelési módszereket alkalmazom:

- Szimulált támadás (pl. social engineering, belső visszaélés).
- Viselkedésminták összehasonlítása normál és anomális működés között.
- MI-alapú előfeldolgozás: érzékenységi küszöbök hangolása a tanulási fázisban.
- A magas érzékenység növeli a hamis riasztások számát, ezt optimalizálni kell.

• Monitoring hatékonysága: válaszidő, rendszerstabilitás, riasztási képesség.
A válaszidő azt mutatja meg, hogy a rendszer milyen gyorsan képes észlelni és reagálni egy biztonsági eseményre. Ez különösen fontos tömegtartózkodású helyszíneken, ahol a késlekedés emberéleteket is veszélyeztethet.

Mérési pontok:

- Észlelési idő: az esemény bekövetkezésétől a detektálásig eltelt idő.
- Reagálási idő: a detektálástól a végrehajtásig (pl. izoláció, riasztás)
- Teljes válaszidő: az esemény bekövetkezésétől a válaszintézkedésig eltelt idő.

Optimalizálási lehetőségek:

- Edge MI alkalmazása: a lokális feldolgozás csökkenti a hálózati késleltetést.
- Prioritás-alapú feldolgozás: kritikus események előnyt élveznek a listán
- Aszinkron feldolgozás: párhuzamos eseménykezelés több szálon.

Célértékek:

- Kritikus eseményeknél: < 15 másodperc (pl. jogosulatlan hozzáférés, rootolás).
- Nem kritikus eseményeknél: < 60 másodperc.

Rendszerstabilitási mutatók:

- Uptime: a rendszer rendelkezésre állása (pl. 99,99%).
- Crash rate: a monitoring komponensek összeomlásának gyakorisága.
- Skálázhatóság: a megnövekedett eseménymennyiség kezelése (pl. DDoS)

Értékelési szempontok:

- Riasztási pontosság: valódi pozitív riasztások aránya.
- Hamis riasztások aránya: túl sok téves riasztás csökkenti az operátori bizalmat.
- Riasztási csatornák: e-mail, SMS, SIEM integráció, mobil push, dashboard.
- Riasztási prioritás: súlyosság szerinti osztályozás (pl. közepes, kritikus).
- MI-alapú súlyozás: minden eseményhez kockázati szint rendelése.

Riasztási képesség:

- Prioritásos riasztás (kritikus, közepes, alacsony).
- Többcsatornás értesítés: SIEM, e-mail, mobil push, dashboard.

• Üzemeltetői kompetencia: MI használhatósága, üzemeltetői képesség.

Erre a megoldás egy 7x24-es szakemberekből álló csapat. Egy ilyen (minimum 4-5 fős) csapat képes az IT-biztonsági megoldásokat üzemeltetni, felügyelni. Fontos szempont a naprakész tudás és a hozzá kapcsolódó képzések. Ki kell emelni az MI-vel kapcsolatos képzések elvégzését.

Központi MI réteg (Cloud Analytics)

- Mély tanulás (LSTM, GNN) időbeli és hálózati mintákra.
- Többforrású korreláció: MDM logok, tranzakciós adatok, hálózati naplók szükségesek.
- Riasztási döntéshozatal: súlyozott kockázati index alapján.

• Adatkezelési előírások, felelősségi kérdések, auditálhatóság.

A kritikus infrastruktúrákban alkalmazott MDM és MI rendszerek személyes adatokat kezelnek (pl. eszközhasználati minták, biometrikus azonosítók, helyadatok), így az adatkezelésnek meg kell felelnie az alábbi alapelveknek: GDPR és MI Act alapján.

A ***GDPR*** (General Data Protection Regulation) az Európai Unió által bevezetett általános adatvédelmi rendelet, amely 2018. május 25-én lépett hatályba. Célja, hogy egységes szabályozást biztosítson a személyes adatok kezelésére, megvédve az egyének magánélethez való jogát az EU-n belül. A rendelet szigorú követelményeket ír elő az adatkezelők és adatfeldolgozók számára, beleértve az átláthatóságot, hozzájárulás-kérést, adatbiztonságot és az érintettek jogainak biztosítását.
Az ***MI Act*** (Artificial Intelligence Act) az Európai Unió első átfogó jogszabálya, amely a mesterséges intelligencia rendszerek biztonságos, átlátható és jogszerű használatát szabályozza. Célja, hogy az MI technológiák fejlesztése és alkalmazása során megvédje az alapvető jogokat, miközben ösztönzi az innovációt.

Felelősségi kérdések:

- *Adatkezelő:* Az a szervezet, amely meghatározza az adatkezelés célját és módját (pl.: infrastruktúra-üzemeltető).
- *Adatfeldolgozó:* Az a szervezet vagy technológiai partner vagy szolgáltató, aki az adatkezelő nevében végzi az adatfeldolgozást (pl. MDM szolgáltató, MI platform üzemeltető).

Auditálhatóság:
Az auditálhatóság biztosítja, hogy az adatkezelés megfelel a jogszabályoknak és belső szabályzatoknak.

- Jogosultságkezelés: Hozzáférés-ellenőrzés, ki, mikor és milyen célból fér hozzá az adatokhoz – ezt naplózni és rendszeresen felül kell vizsgálni.
- Rendszeres auditok: Belső és külső auditok szükségesek az adatkezelési gyakorlatok, MI modellek és biztonsági intézkedések felülvizsgálatára.
- MI auditálhatóság: Az MI Act előírja, hogy a magas kockázatú rendszereknek rendelkezniük kell használati utasítással, amely tartalmazza a rendszer célját, működését, korlátait és kockázatait.

- **Következménybecslés: szolgáltatás-kiesés időtartama, gazdasági veszteség, KPI**

A szolgáltatás-kiesés időtartama az egyik legfontosabb következmény, amelyet egy biztonsági incidens okozhat. Az MDM+MI rendszer célja ennek minimalizálása.

Forgatókönyv-alapú modellezés: különböző típusú támadások (pl. ransomware, belső visszaélés) hatásának vizsgálata.

Tipikus értékek kritikus rendszerekben, monitoring adatok alapján:

- Minimális célérték: < 5 perc
  (pl. járműirányítás, tömegirányítás, kritikus infrastruktúra).
- Elfogadható érték: < 30 perc
  (pl. Rendszerkomponensek, adatfeldolgozó háttérrendszerek esetén).
- Kritikus határérték: > 1 óra – reputációs és gazdasági kár valószínűsége.

Csökkentési lehetőségek:

- Redundáns komponensek kiépítése, automatikus failover.
- MI gyors izolációs képessége.
- Prioritásos incidenskezelés és rollback mechanizmusok kidolgozása.

Becslési komponensek:

- Közvetlen veszteség: kiesett bevétel, helyreállítási költségek, eszközcsere.
- Közvetett veszteség: reputációs kár, ügyfélvesztés, jogi költségek.
- Pénzmosási következmények: bírságok, hatósági eljárások, auditköltségek.

Példaértékek:

Egy 30 perces szolgáltatás-kiesés egy budapesti tömegközlekedési rendszerben: akár 10–50 millió Ft közvetlen veszteség is lehet. Ez függ a helytől és az idősávtól. Egy pénzmosási incidens feltárása után: 50–100 millió Ft bírság + reputációs kár is előfordulhat.

KPI – Kulcsfontosságú teljesítménymutatók

A KPI-ok segítenek objektíven mérni egy biztonsági rendszer hatékonyságát és fejlődését, rendelkezésre állását. Ezek adatok alapján tudunk azon részegység működésébe beavatkozni, ahol látjuk hol szükségszerű változtatni vagy finomítani.

A KPI-ok meghatározásánál nagy segítséget nyújtanak a monitoring rendszerek, ahol az adatok a kiolvashatóak a rendszer rendelkezésre állása esetén.

- Átlagos helyreállítási idő egy incidens után (pl: Jira Jegykezelő rendszerek)

- Átlagos észlelési idő egy esemény bekövetkezése után (Monitoring rendszerek)
- Havi incidensek száma (pl: Jira Jegykezelő rendszerek)
- Téves riasztások aránya (Monitoring rendszerek)
- Rendszerek rendelkezésre állásának mutatói (Monitoring rendszerek)

4.1.15 Összegzés

Negyedik hipotézis: Az MDM rendszerek és MI integrációja jelentősen csökkentheti a mobil eszközökről eredő adatszivárgást, jogosulatlan hozzáférést, manipuláció kockázatát kritikus környezetekben.

Az MDM (Mobile Device Management) rendszerek alapvető biztonsági kontrollokat biztosítanak.

- Eszközregisztráció és hitelesítés
- Alkalmazás- és konfigurációmenedzsment
- Távoli törlés, zárolás és hozzáférés-szabályozás

Ezek a funkciók önmagukban is csökkentik az adatszivárgás és jogosulatlan hozzáférés kockázatát, szabályalapúak, így korlátozottan reagálnak új, dinamikus fenyegetésekre. Ezenfelül az MI integrációnak számos előnye van, amit sikeresen teszteltem. Felismerik a szokatlan mintákat (pl.: szokatlan adatforgalom). Gyors reakcióidő miatt számos incidens megelőzhető, ilyen a jogosulatlan hozzáférések kezelése, terheléses támadások elleni védekezés. Az adatok biztonságos eszközökön való felügyelete.

A hipotézis minden eleme validálható:

- Az MDM rendszerek MI-integrációval hatékonyabbak lesznek.
- Csökken az adatszivárgás, jogosulatlan hozzáférés kockázata.
- Javul a detektálás pontossága, csökken a hamis riasztások száma.
- Fenntarthatóbb üzemeltetés valósul meg, alacsonyabb emberi terheléssel.

Ez a megközelítés különösen ajánlott kritikus infrastruktúrákban és gépjárművekben, ahol a mobil eszközök biztonsága kiemelt fontosságú.

KUTATÁSI TEVÉKENYSÉGEK ÖSSZEGZÉSE

A kutatási céljaim elérése érdekében tanulmányoztam a hazai és a külföldi szakirodalmakat. A kutatási tevékenységem több, egymást erősítő technológiai pillérre épült: a kiberbiztonságra, a mobil eszközmenedzsment rendszerekre (MDM), a valós idejű infrastruktúra monitorozásra, a mesterséges intelligencia (MI) alapú biztonsági és üzemeltetési megoldásokra és a pénzmosási kockázatokra. A kutatásom során ezeknek a területeknek az összekapcsolása vált meghatározóvá, különösen a kritikus infrastruktúrák, tömegtartózkodású objektumok védelmének vizsgálatában. A kutatási munka elméleti és gyakorlati alapjait jelentősen erősítették azok a nemzetközi és hazai szakmai események, amelyeken részt vettem, és amelyek révén naprakész tudást szereztem.

1. Atlassian Team 2022 – Felhőalapú üzemeltetés, monitoring

2022. május 5–7. között részt vettem az Atlassian Team 2022 konferencián, amelyet a Las Vegas-i Venetian Expo & Convention Centerben rendeztek meg. A rendezvény több ezer mérnököt, fejlesztőt és üzemeltetési szakembert vonzott, így volt lehetőségem konzultálni hazai és külföldi szakemberekkel, amiben kiemelt fókuszt kapott a felhőalapú szolgáltatásokra épülő üzemeltetés, a skálázható monitoring, valamint a csapatmunkát támogató integrált platformok jövője.

A konferencián szerzett tapasztalatok több szempontból is hozzájárultak a kutatásomhoz:

• Felhőalapú üzemeltetés térnyerése: egyértelművé vált, hogy az Atlassian ökoszisztéma fejlesztési iránya döntően a cloud-verziókra koncentrál. A plugin-fejlesztők több mint 50%-a már kizárólag felhőre fejleszt, ami az üzemeltetési modellek átalakulását is jelzi.

• Monitoring és riasztáskezelés: a működésének megértése különösen fontos volt a kutatásom szempontjából, mivel az alkalmazás használatának feltétele volt az aktív MDM-felügyelet. A riasztási logikák, eszkalációs szabályok és folyamatok elemzése közvetlenül hozzájárult a valós idejű monitoring és automatizált reagálási stratégiák vizsgálatához.

• Vizualizáció és architektúra-tervezés (draw.io, Compass): a draw.io és a Compass eszközök bemutatói megerősítették a kutatás vizuális modellezési részét, különösen a hibrid monitoring-architektúrák és MDM-folyamatok ábrázolásában.

• Csapatműködés és információ-integráció: a felhő platform betekintést adott abba, hogyan lehet a szervezeti tudást és feladatokat összefogni. Ez a szemlélet a kritikus infrastruktúrák üzemeltetési modelljeinek összehangolásában is releváns.

A konferencia során szerzett tapasztalatok megalapozták az MDM-rendszerek és monitoring eszközök integrációjának gyakorlati megértését, és hozzájárultak a négy hipotézis validációjához.

2. Microsoft Application Innovation Day 2023 – A jövő üzemeltetése és MI-alapú működés

2023-ban részt vettem a Microsoft Application Innovation Day szakmai tréningen, amely a modern üzemeltetés, a felhőalapú architektúrák és az MI-vezérelt működés jövőjét vizsgálta. A rendezvény különösen értékes volt abból a szempontból, hogy a kutatásom központi témáját a kritikus infrastruktúrák informatikai védelmét közvetlenül össze tudtam kapcsolni a Microsoft által bemutatott technológiai irányokkal.

A tréning során szerzett tapasztalatok:

• MI-alapú üzemeltetés: betekintést kaptam abba, hogyan képes a mesterséges intelligencia automatizálni a hibadetektálást, optimalizálni az erőforrás-felhasználást és csökkenteni a reakcióidőt.

• Felhő architektúrák: a konténerizáció, a microservice-alapú rendszerek és a skálázható felhőmegoldások vizsgálata hozzájárult a monitoring-architektúrák hibrid modelljeinek vizsgálatához.

• Biztonsági megfelelés: a Microsoft Zero Trust modelljének részletes megismerése.

Ez a tréning segített abban, hogy a kutatás elméleti modelljeit összehangoljam a legmodernebb iparági gyakorlatokkal, és megerősítette az MI-alapú monitoring relevanciáját a kritikus infrastruktúrák védelmében.

3. Microsoft Cloud and AI Business Solutions Day 2025 – Felhő, MI és üzleti alkalmazások

2025 februárjában részt vettem a Microsoft Cloud and AI Business Solutions Day szakmai eseményen, amely a felhőalapú szolgáltatások és a mesterséges intelligencia üzleti alkalmazásait mutatta be. A rendezvény különösen értékes volt abból a szempontból, hogy a kutatásom fókuszterületeit érintette.

A legfontosabb tapasztalatok:

• Skálázhatóság: a felhőalapú rendszerek működési stabilitása és automatikus skálázása közvetlenül kapcsolódik a kritikus infrastruktúrák üzemeltetési kihívásaihoz.

• Adatvezérelt döntéshozatal: a monitoring rendszerekből származó adatok MI-alapú feldolgozása lehetővé teszi a prediktív karbantartást és a proaktív incidenskezelést.

• Nemzetközi trendek: betekintést kaptam abba, hogyan alkalmazzák a pénzügyi és biztonsági szektorban a felhő- és MI-megoldásokat, ami közvetlenül támogatta a kutatás összehasonlító elemzéseit.

Az alkalmazott kutatási módszerek, tanulmányok, konferenciák és gyakorlati tapasztalatok hozzásegítettek, támogatták a disszertációm elkészülését.

AJÁNLÁSOK

A négy validált hipotézis alapján megállapítható, hogy az MDM rendszerek és mesterséges intelligencia integrációja, a pénzmosási kockázatok informatikai beépítése, a valós idejű monitoring hibrid architektúrája, valamint a szolgáltatásalapú üzemeltetési megközelítések együttesen képesek jelentősen növelni a kritikus infrastruktúrák informatikai védelmének hatékonyságát, fenntarthatóságát és szabályozási megfelelőségét.

Az értekezés eredményei új kutatási irányokat nyithatnak a mobil eszközmenedzsment, a mesterséges intelligencia alapú kockázatértékelés és a hibrid monitoring architektúrák területén. A bemutatott modellek alkalmasak arra, hogy alapjául szolgáljanak további vizsgálatoknak, különösen az eszközfelügyelet és a szolgáltatásalapú kiberbiztonsági ökoszisztémák formalizálása terén. A kutatás eredményei publikációs szempontból is relevánsak, mivel hozzájárulnak a kritikus infrastruktúrák digitális fenntarthatóságának, fejlődési irányainak és az MI-vezérelt biztonsági rendszerek bővítéséhez.

A gyakorlati megközelítések közvetlenül alkalmazhatók az üzemeltetési gyakorlatban, különösen olyan szervezetek számára, amelyek komplex, földrajzilag kiterjedt infrastruktúrákat működtetnek. Az MDM-MI integráció, a valós idejű monitoring hibrid architektúrája és a szolgáltatásalapú üzemeltetési modell olyan keretet biztosít, amely csökkenti az emberi hibából eredő kockázatokat, növeli a rendszer stabilitást, és lehetővé teszi a gyors, automatizált beavatkozást. A pénzmosási kockázatok informatikai beépítése pedig új szintre emeli a pénzügyi és informatikai rendszerek biztonsági megfelelőségét, különösen a kritikus infrastruktúrák tranzakciós környezeteiben.

A kutatás eredményei stratégiai szinten is hasznosíthatók a szabályozási környezet fejlesztésében. A bemutatott modellek támogatják olyan keretek kialakítását, amelyek figyelembe veszik a mesterséges intelligencia és a mobil eszközök biztonsági szerepét a kritikus infrastruktúrákban. A szolgáltatásalapú üzemeltetés és a valós idejű monitoring integrációja új szabványosítási irányokat jelölhet ki, különösen az auditálhatóság és a fenntartható biztonsági működés területén. Emellett az eredmények oktatási szempontból is relevánsak: hozzájárulnak olyan képzési programok kialakításához, amelyek a jövő szakembereit a mesterséges intelligencia-vezérelt kiberbiztonsági rendszerek tervezésére és üzemeltetésére készítik fel.

HIPOTÉZISEK ÖSSZEGZÉSE

Hipotézis	Vizsgálati módszer	Igazolás/következtetés
Első hipotézis: A kibertámadások elleni védekezésből eredő rendszerüzemeltetési megközelítések vizsgálata — különös tekintettel az globális trendekre, megfelelő rendszer komponensekre és szolgáltatás alapú üzemeltetési stratégiákra — növelheti a védelmi intézkedések hosszútávú hatékonyságát.	A globális trendek, MI-integráció és szolgáltatásalapú üzemeltetés együttesen valóban növelik a védelmi intézkedések fenntarthatóságát és hatékonyságát, a nemzetközi gyakorlat és kutatási eredményeim ezt alátámasztják. A hipotézis szerint a körültekintő tervezés, megfelelő rendszerekkel kombinálva plusz az MI által támogatott komponensek lehetővé teszi a döntéshozók számára, hogy korlátozott források mellett maximalizálják a védelmi hatékonyságot, miközben megfelelnek szabályozási és üzemeltetési követelményeknek.	*Az első hipotézis validálható:* • A globális trendek az MI-alapú támadások térnyerését mutatják. • A megfelelő rendszerkom-ponensek (MDM, MI, audit) technikailag és szabályozásilag is megalapozottak. • A szolgáltatásalapú üzemel-tetés költséghatékony és ská-lázható. • Az MI támogatás lehetővé teszi a hatékonyságot. Ezért a hipotézis nemcsak elméletileg megalapozott, hanem a gyakorlatban is releváns és alkalmazható.
Második hipotézis: A pénzmosási kockázatok és következmények beépítése a kritikus infrastruktúra informatikai védelmi	Az informatikai adatok (tranzakciók, rendszerlogok, hozzáférési események) MI-alapú összefüggéselemzése korai előrejelzést tesz lehetővé a pénzügyi visszaélésekhez vezető	*A második hipotézis validálható:* a pénzmosási kockázatok informatikai integrációja valóban csökkenti a szolgáltatásmegtagadási és reputációs kockázatokat,

architektúrájába csökkentheti az üzleti folyamatok manipulációjából eredő szolgáltatásmegtagadási kockázatokat.	tevékenységekre, és ezzel megelőzhetőek a másodlagos hatások (pl. koordinált támadások, visszaélések) a kritikus rendszerekre. Ezért a pénzmosási kockázatok beépítése nem-csak biztonsági, hanem stra-tégiai előnyt is jelentenek.	különösen kritikus infrastruktúrák esetében, ahol a pénzügyi visszaélések rendszerszintű hatásokat okozhatnak.
Harmadik hipotézis: A valós idejű monitoring és reagálási stratégia, amely MI-t használ anomália detektálásra és automatizált reagálásra, jelentősen csökkentheti a támadás felfedezési és reakcióidőt, ezáltal csökkentve a károkat, minimalizálva a szolgáltatáskiesés valószínűségét kritikus infrastruktúrák esetében.	A teszt (3.1.11 fejezet) egyértelműen kimutatta, hogy az MI-vezérelt monitoring 40–70%-kal csökkenti a detektálási időt, míg az automatizált reagálás jelentősen mérsékli a szolgáltatáskiesés időtartamát és a károk mértékét.	*A harmadik hipotézis validálható:* A valós idejű MI-alapú monitoring és az emberi reagálás, különösen hibrid architektúrában, bizonyítottan csökkenti a felfedezési és reakcióidőt, ezáltal mérsékli a károkat és a szolgáltatáskiesés kockázatát kritikus infrastruktúrákban. Tudunk valós időben észlelni anomáliákat a rendszer viselkedésében, például szokatlan adatforgalmat. Az MI képes azonnal reagálni. Ez a stratégia nemcsak technológiai, hanem szabályozási és gazdasági szempontból is előremutató.

Negyedik hipotézis: Az MDM rendszerek és MI integrációja jelentősen csökkentheti a mobil eszközökről eredő adatszivárgást, jogosulatlan hozzáférést, manipuláció kockázatát kritikus környezetekben.	Az MDM (Mobile Device Management) rendszerek alapvető biztonsági kontrollokat biztosítanak. • Eszközregisztráció és hitele-sítés • Alkalmazás- és konfigu-rációmenedzsment • Távoli törlés, zárolás és hozzáférés szabályozás Ezek a funkciók önmagukban is csökkentik az adatszivárgás és jogosulatlan hozzáférés kockázatát, szabályalapúak, így korlátozottan reagálnak új, dinamikus fenyegetésekre. Ezenfelül az MI integrációnak számos előnye van, amit sikeresen teszteltem.	A hipotézis minden eleme validálható: • Az MDM rendszerek MI-integrációval hatékonyabbak lesznek. • Csökken az adatszivárgás, jogosulatlan hozzáférés kockázata. • Javul a detektálás pontossága, csökken a hamis riasztások száma. • Fenntarthatóbb üzemeltetés valósul meg, alacsonyabb emberi terheléssel. Ez a megközelítés különösen ajánlott kritikus infrastruktúrákban, ahol a mobil eszközök biztonsága kiemelt fontosságú.

SAJÁT PUBLIKÁCIÓK JEGYZÉKE

Tudományos közlemények

P1: Bálint Ferenc, Pető Richárd
Sustainable And Safe Cities Through Computer Applications
INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS
WoS (Web of Science)
(ISSN:1334-4684 1334-4676): 23 3 pp 207-216 (2025)

P2: Bálint Ferenc
Anti-money laundering with a special focus on the cyber security threats and vulnerabilities
The Role of Internal Control Functions of Hungarian Financial Institutions for AML Compliance.
NATIONAL SECURITY REVIEW: PERIODICAL OF THE MILITARY NATIONAL SECURITY SERVICE (ISSN: 2416-3732): 2023 2 pp 144-157 (2023)

P3: Bálint Ferenc
Global Cybersecurity Threats and Trends
NATIONAL SECURITY REVIEW: PERIODICAL OF THE MILITARY NATIONAL SECURITY SERVICE (ISSN: 2416-3732): 2024 1 pp 121-135 (2024)

P4: Bálint Ferenc
The Strategic Role of Monitoring in Modern Critical Infrastructure Management
INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS
(ISSN: 0975-8887) 187 8 pp 60-65 (2025)

P5: Bálint Ferenc, Pető Richárd
A biztonságtechnikai mérnöki képzés múltja és jövője
MŰSZAKI KATONAI KÖZLÖNY
(ISSN: 1219-4166, 2063-4986): 34 Különszám pp 191-204 (2024)

P6: Bálint Ferenc

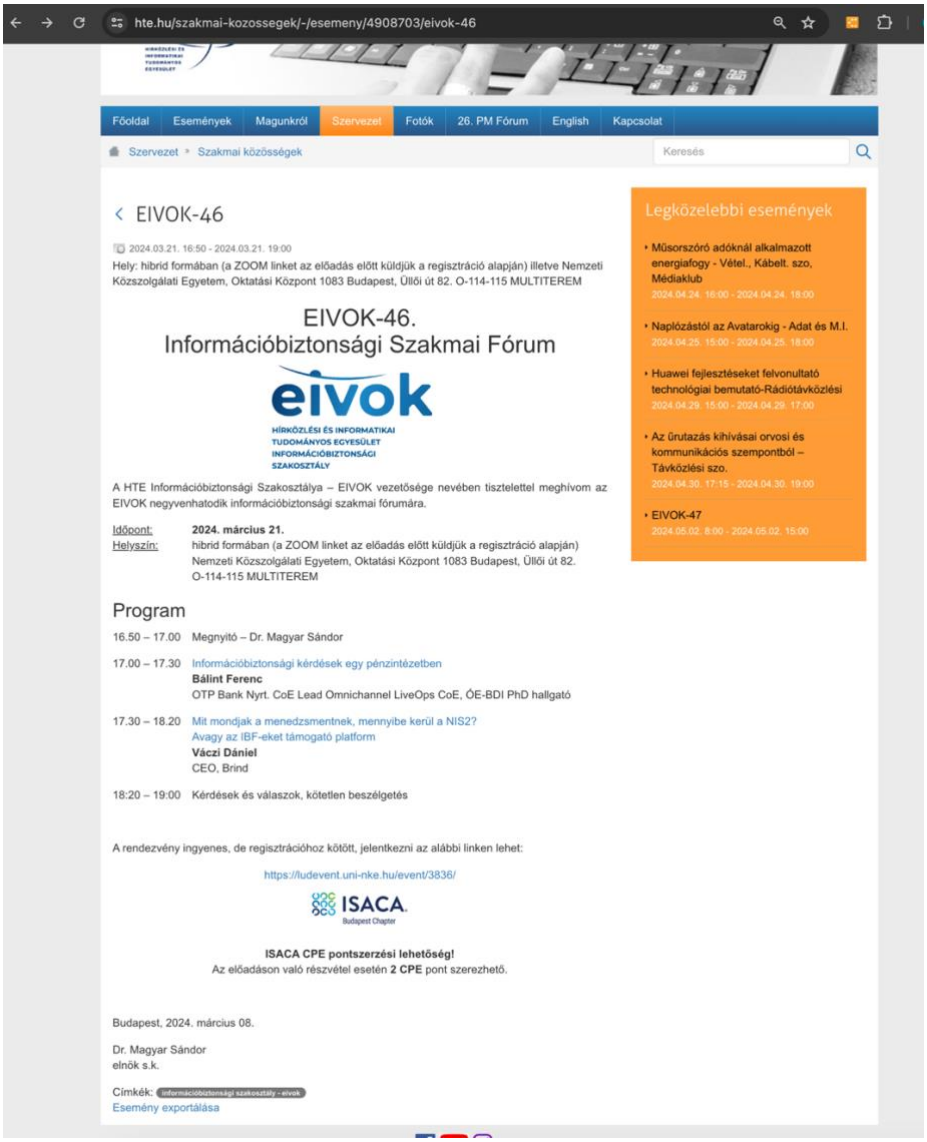
Infrastructure Monitoring for the Resilience of Critical Infrastructure

INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING AND MANAGEMENT RESEARCH (ISSN: 2456-3676) 10 : 6 pp. 368-387. , 17 p. (2025)

Szakmai konferenciák

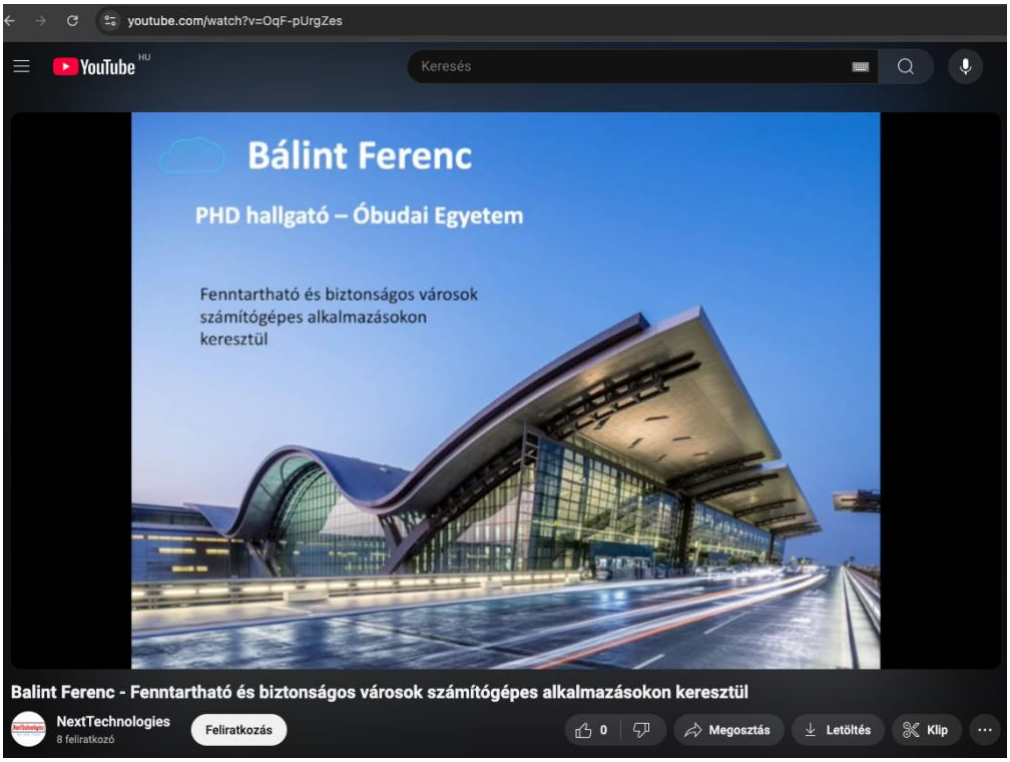
Előadás 1:

Konferencia neve: EIVOK-46. Információbiztonsági Szakmai fórum
Konferencia helyszíne: Nemzeti Közszolgálati Egyetem, Oktatási központ.
1083. Budapest, Üllői út 82. O-114-115 Multiterem.
Ideje: 2024. március 21.
Előadó neve: Bálint Ferenc
Külső hivatkozás (link): https://www.hte.hu/beszamolok/-/esemeny/4908703/eivok-46



Előadás 2:

Konferencia neve: SMART SUSTAINABLE AND SAFE CITIES CONFERENCE NextTechnologies
Konferencia helyszíne: Online
Előadó neve: Bálint Ferenc
Külső hivatkozás (link): https://www.youtube.com/watch?v=OqF-pUrgZes
Fenntartható és biztonságos városok számítógépes alkalmazásokon keresztül



IRODALOMJEGYZÉK

[1] Ferenc Bálint: *Anti-Money Laundering with a special focus on the cyber security threats and vulnerabilities - The role of internal control functions of Hungarian financial institutions for AML compliance.*
National Security Review: 2023: 2 pp. 144-157. , 11 p. (2023)
URL:https://s2prodstorage.blob.core.windows.net/s2cmsblob/Files/National%20Security%20Review/2023_2_NSR.pdf?sp=r&st=2025-03-25T09:37:58Z&se=2035-03-25T16:37:58Z&spr=https&sv=2024-11-04&sr=c&sig=PAOb3jtCphbbzRgBEutrTUH2uSjRNnF3G8dVaL8Y3Z0=
(letöltve: 2024. március 8.)

[2] Security Intelligence: *Cybersecurity trends: IBM's predictions for 2024*
URL: https://securityintelligence.com/articles/cybersecurity-trends-ibm-predictions-2024/ (letöltve: 2024. február 25.)

[3] Cyber attacks top industries, Statista: Cyber Crime and Security
URL: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/
(letöltve: 2024. március 14.)

[4] Cybersecurity threats at companies, Statista: Cyber Crime and Security
URL: https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/
(letöltve: 2024. március 14.)

[5] YourShortlist: What are the 8 Most Common Types of Cyber Attacks?
URL: https://yourshortlist.com/what-are-the-8-most-common-types-of-cyber-attacks/ (letöltve: 2024. február 12.)

[6] Security Intelligence: Cybersecurity trends: IBM's predictions for 2024
URL: https://securityintelligence.com/articles/cybersecurity-trends-ibm-predictions-2024/ (letöltve: 2024. február 18.)

[7] IBM Cloud Team: Types of cyberthreats
URL: https://www.ibm.com/blog/types-of-cyberthreats/
(letöltve: 2024. március 8.)

[8] IBM Cloud Team: What is cyber risk management?
URL: https://www.ibm.com/topics/cyber-risk-management
(letöltve: 2024. március 8.)

[9] IBM Cloud Team: Types of cyberthreats
URL: https://www.ibm.com/blog/types-of-cyberthreats/
(letöltve: 2024. március 10.)

[10] Simplilearn: Roles and Responsibilities of Cyber Security Professionals
URL: https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article (letöltve: 2024. március 1.)

[11] Security Intelligence: *What the cybersecurity workforce can expect in 2024*
URL: https://securityintelligence.com/articles/cybersecurity-workforce-trends-2024/ (letöltve: 2024. február 28.)

[12] NIST – National Institute of Standards and Technology:Framework for Improving Critical Infrastructure Cybersecurity
URL: https://www.nist.gov/
URL: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
(letöltve: 2024. február 16.)

[13] Cybersecurity and Infrastructure Security Agency:
Framework for Improving Critical Infrastructure Cybersecurity
URL: https://www.cisa.gov/resources-tools/resources/framework-improving-critical-infrastructure-cybersecurity
(letöltve: 2024. február 28.)

[14] Cybersecurity and Infrastructure Security Agency:
Critical Infrastructure Sectors
URL: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
(letöltve: 2024. március 5.)

[15] 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról
URL: https://net.jogtar.hu/jogszabaly?docid=a1700053.tv
(letöltve: 2025. február 5.)

[16] 2017. évi LII. törvény az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi korlátozások végrehajtásáról
URL: https://net.jogtar.hu/jogszabaly?docid=a1700052.tv
(letöltve: 2025. február 5.)

[17] 26/2020. (VIII.25.) MNB rendelet a pénzmosás és a terrorizmus finanszírozása elleni intézkedésekről
URL: https://njt.hu/jogszabaly/2020-26-20-2C
(letöltve: 2025. február 5.)

[18] 21/2017. (VIII.3.) NGM rendelet a belső szabályzat kötelező tartalmi elemeiről
URL: https://net.jogtar.hu/jogszabaly?docid=a1700021.ngm
(letöltve: 2025. február 5.)

[19] Central Bank of Hungary – Supervision, Anti-Money Laundering
URL: https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen
(letöltve: 2023. július 2.)

[20] Financial Action Task Force (FATF)
URL: https://www.fatf-gafi.org/en/the-fatf/who-we-are.html
(letöltve: 2023. augusztus 3.)

[21] Council of Europe – Newsroom – MONEYVAL report on Hungary: improvements in fighting money laundering and terrorist financing have led to upgraded ratings
URL: https://www.coe.int/en/web/moneyval/-/moneyval-report-on-hungary-improvements-in-fighting-money-laundering-and-terrorist-financing-have-led-to-upgraded-ratings (letöltve: 2023. augusztus 3.)

[22] Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL (monitoring body of the Council of Europe) – Anti-money laundering and counter-terrorist financing measures Hungary, 5th Enhanced Follow-up Report, 2022. május
URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-fur/Moneyval-FUR-Hungary-2022.pdf.coredownload.pdf (letöltve: 2023. július 15.)

[23] The Institute of Internal Auditors – The IIA's Three Lines Model
URL: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf (letöltve: 2023. július 15.)

[24] Wolters Kluwer Legal and regulatory research – Anti-money laundering
URL: https://net.jogtar.hu
(letöltve: 2023. július 30.)

[25] International Monetary Fund – ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM (AML/CFT)
URL: https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm#typologies
(letöltve: 2023. július 30.)

[26] Trulioo - KYC: 3 Steps to Achieving Know Your Customer Compliance
URL: https://www.trulioo.com/blog/kyc
(letöltve: 2023. augusztus 9.)

[27] Central Authority of the National Tax and Customs Administration, the Hungarian Financial Intelligence Unit (HFIU) - NAV PEI
URL: https://nav.gov.hu/penzmosas
(letöltve: 2023. augusztus 11.)

[28] FAFT – Illicit Financial Flows from Cyber-Enabled Fraud, November 2023
URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf
(letöltve: 2023. október 11.)

[29] McKinsey & Company – Risk & Resilience – Financial crime and fraud in the age of cybersecurity
URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity#/
(letöltve: 2023. augusztus 20.)

[30] Cybergate International – Exploring how Cyber security and Anti Money Laundering go hand-in-hand
URL: https://cybergateinternational.com/blog/exploring-how-cyber-security-and-anti-money-laundering-go-hand-in-hand/
(letöltve: 2023. augusztus 23.)

[31] MONEYVAL – Hungary: Fifth Round Mutual Evaluation Report (2024),
URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-mer/MER-Hungary-2016.pdf.coredownload.inline.pdf (letöltve: 2025. szeptember 2.)

[32] MONEYVAL – Hungary: Follow-up Report & Technical Compliance ReRating
URL: https://rm.coe.int/moneyval-2024-3-hy-5thround-6thenhfur/1680b06af8
(letöltve: 2025. szeptember 2.)

[33] 2022 Interpol Global Crime Trend Summary Report,
URL:https://www.interpol.int/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf
(letöltve: 2023. október 2.)

[34] FATF – FAFT Report Crowdfunding for Terrorism Financing,
URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf
(letöltve: 2023. október 11.)

[35] SentinelOne: Emerging Trends in Cybersecurity Monitoring
URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-monitoring/
(letöltve: 2024. március 11.)

[36] NiCE IT Management Solutions GmbH: Navigating Industry-Specific Challenges in Infrastructure Monitoring and Automation,
A White Paper by NiCE IT Management Solutions,
URL: https://www.nice.de/wp-content/uploads/2024/03/Monitoring-and-Automation-Whitepaper-by-NiCE-2024Q1.pdf
(letöltve: 2024. március 11.)

[37] Uptrace:_Top 11 Best Monitoring Tools for IT Infrastructure
URL: https://uptrace.dev/tools/monitoring-tools-for-it
(letöltve: 2025. január 15.)

[38] Will Kelly, Emily Foster: Compare 8 tools for IT monitoring in 2025,
URL: https://www.techtarget.com/searchitoperations/feature/Compare-8-tools-for-IT-monitoring
(letöltve: 2024. december 20.)

[39] González-Granadillo, G.; González-Zarzosa, S.; Diaz, R.: Security Information and EventManagement (SIEM): Analysis, Trends,
and Usage in Critical Infrastructures, Sensors,
URL:https://www.researchgate.net/publication/353214895_Security_Information_and_Event_Management_SIEM_Analysis_Trends_and_Usage_in_Critical_Infrastructures
(letöltve: 2025. január 30.)

[40] What is Best DataDog Competitors in 2025
URL: https://uptrace.dev/blog/datadog-competitors
(letöltve: 2025. március 20.)

[41] What is Infrastructure Monitoring?
URL: https://uptrace.dev/glossary/what-is-infrastructure-monitoring
(letöltve: 2025. március 22.)

[42] mimecast: White Paper AI and Cybersecurity: The Promise and Truth of the AI Security Revolution,
URL: https://www.mimecast.com/resources/white-papers/ai-and-cybersecurity/
(letöltve: 2025. január 25.)

[43] Muha L., Krasznay Cs.; Managing the security of electronic information systems, 2014, in Hungarian
URL:https://nkerepo.uninke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9sej%C3%B3.pdf?sequence=5&isAllowed=y
(letöltve: 2023. december 20.)

[44] Marcel Pikhart.: The Use of Mobile Devices in International Management Communication: Current Situation and Future Trends of Managerial Communication, p 1736-1741, 2020,
URL: https://www.sciencedirect.com/science/article/pii/S1877050920311674,
(letöltve: 2023. december 18.)

[45] Paul Steiner.: Going beyond mobile device management, p 19-20, 2014,
URL: https://www.sciencedirect.com/science/article/abs/pii/S136137231470483X
(letöltve: 2023. december 21.)

[46] Ivanti: Everywhere Work. Elevated.
URL: https://www.ivanti.com/, (letöltve: 2023. december 21.)

[47] Microsoft: Microsoft Intune
URL: https://www.microsoft.com/en-us/security/business/microsoft-intune,
(letöltve: 2023. december 21.)

[48] Wmware: *space ONE Unified Endpoint Management*
URL: https://www.vmware.com/products/workspace-one/unified-endpoint-management.html, (letöltve: 2023. december 21.)

[49] Smith detection: Making the world a safer place
URL: https://www.smithsdetection.com/
(letöltve: 2023. december 21.)

[50] imarc: Mobile Device Management Market Report
URL: https://www.imarcgroup.com/mobile-device-management-market,
(letöltve: 2024. május 10.)

[51] imarc: Mobile Device Management Market Report
URL: https://www.researchandmarkets.com/reports/5946677/mobile-device-management-market-report-type,
(letöltve: 2024. május 15.)

[52] Global Mobile Device Management Market Size
URL: https://www.marketdataforecast.com/market-reports/mobile-device-management-market,
(letöltve: 2024. május 15.)

[53] Global Mobile Device Management Market Analysis
URL: https://www.technavio.com/report/mobile-device-management-market-industry-analysis
(letöltve: 2024. május 18.)

[54] Azure: Alkalmazkodás és fejlődés
URL: https://azure.microsoft.com/hu-hu,
(letöltve: 2024. január 5.)

[55] Hewlett Packard Enterprise: HPE Storage
URL: https://www.hpe.com/us/en/storage.html,
(letöltve: 2024. január 8.)

[56] Cloudflare: What is SSL? SSL definition
URL: https://www.cloudflare.com/en-gb/learning/ssl/what-is-ssl/,
(letöltve: 2024. január 8.)

[57] Microsoft Security: Azure Active Directory is now Microsoft Entra ID
URL: https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id,
(letöltve: 2024. január 10.)

[58] IBM: What is security information and event management (SIEM)?
URL: https://www.ibm.com/topics/siem,
(letöltve: 2024. január 10.)

[59] IBM: What is artificial intelligence (AI)?
URL: https://www.ibm.com/topics/artificial-intelligence,
(letöltve: 2024. január 10.)

[60] TechTarget: ITIL (Information Technology Infrastructure Library)
URL: https://www.techtarget.com/searchdatacenter/definition/ITIL,
(letöltve: 2024. január 15.)

[61] Okta: Hashing Algorithm Overview: Types, Methodologies & Usage
URL: https://www.okta.com/identity-101/hashing-algorithms/,
(letöltve: 2024. január 15.)

[62] AI szintek meghatározása
URL: https://www.forbes.com/sites/jodiecook/2024/07/16/openais-5-levels-of-super-ai-agi-to-outperform-human-capability/
(letöltve: 2025. október 25.)

RÖVIDÍTÉSJEGYZÉK

AD	Címtárszolgáltatás – Active Directory
AI	Mesterséges intelligencia – Artificial Intelligence
AI Act	Mesterséges Intelligencia Rendelet – Artificial Intelligence Act
AML	Pénzmosás elleni fellépés – Anti-Money Laundering
APM	Alkalmazásteljesítmény-kezelés – Application Performance Management
BFSI	Banki, pénzügyi szolgáltatások és biztosítási szektor – Banking, Financial Services and Insurance
BYOD	Saját eszköz használata – Bring Your Own Device
CDD	Ügyfél átvilágítás – Customer Due Diligence
CEF	Európai Hálózatfinanszírozási Eszköz – Connecting Europe Facility
CCTV	Zártláncú kamerarendszer – Closed-Circuit Television
CI/CD	Folyamatos integráció és folyamatos kiadás – Continuous Integration / Continuous Delivery
CISO	Információbiztonsági vezető – Chief Information Security Officer
CTF	Terrorizmus finanszírozás elleni fellépés – Counter-Terrorism Financing
DDOS	Elosztott szolgáltatásmegtagadás – Distributed Denial of Service
DEVOPS	Fejlesztés és üzemeltetés integrációja – Development and Operations
DMZ	Demilitarizált zóna – Demilitarized Zone
EDD	Fokozott átvilágítás – Enhanced Due Diligence
EDR	Végponti észlelés és válaszadás – Endpoint Detection and Response
ESM	Vállalati biztonsági menedzsment – Enterprise Security Manager
FATF	Pénzügyi Akció Munkacsoport – Financial Action Task Force
GDPR	Általános Adatvédelmi Rendelet – General Data Protection Regulation
GENAI	Generatív mesterséges intelligencia – Generative Artificial Intelligence
ICS	Ipari irányítórendszerek – Industrial Control Systems
IDR	Intelligens észlelés és válaszadás – Intelligent Detection and Response
IDS	Behatolásérzékelő rendszer – Intrusion Detection System
IoE	Kommunikációs hálózat – Internet of Everything
IoT	Hálózati eszközök – Internet of Things
ITIL	IT infrastruktúra-szabványgyűjtemény – Information Technology Infrastructure Library

KPI	Kulcs teljesítménymutató – Key Performance Indicator
KYC	Ismerd meg az ügyfeled – Know Your Customer
MDM	Mobil eszköz menedzsment – Mobile Device Management
MI	Mesterséges intelligencia – Artificial Intelligence
ML	Gépi tanulás – Machine Learning
NLP	Mesterséges Intelligencia egyik ága – Natural Language Processing
OFAC	Az USA Pénzügyminisztériumának Különleges Ellenőrzési Hivatala – Office of Foreign Assets Control
OTA	Vezeték nélküli frissítés/átvitel – Over-the-Air
RANSOMWARE	Zsarolóvírus – Ransomware
SAR	Gyanús tevékenységről szóló jelentés – Suspicious Activity Report
SCOM	Rendszerfelügyeleti menedzser – System Center Operations Manager
SCORCH	Rendszerautomatizációs eszköz – System Center Orchestrator
SIEM	Biztonsági információ- és eseménykezelés – Security Information and Event Management
SMS	Rövid szöveges üzenet – Short Message Service
SOAR	Biztonsági orchestráció, automatizáció és válaszadás – Security Orchestration, Automation and Response
SSL	Biztonsági kapcsolatot biztosító réteg – Secure Sockets Layer
TLS	Szállítási réteg biztonság – Transport Layer Security
TOR	Anonimizáló hálózati protokoll – The Onion Router
UEM	Egységes végpontmenedzsment – Unified Endpoint Management
VPN	Virtuális magánhálózat – Virtual Private Network
Wi-Fi	Vezeték nélküli hálózat – Wireless Fidelity

ÁBRAJEGYZÉK

FÜGGELÉK

AI szintek meghatározása [62]

Szintek	Megnevezés	Jellemzők	Példák
1. szint	„Beszélgető” AI	Képes kommunikálni	Ügyfélszolgálati chatbotok
2. szint	Feladat specifikus (érvelő) AI	Komplex feladatokat old meg egy adott területen.	AI tartalomgeneráló eszközök
3. szint	Általános (autonóm) AI (AGI)	Emberi szintű intelligencia, képes tanulni, alkalmazkodni és problémákat megoldani	Fejlesztés alatt
4. szint	Szuperintelligencia (innovatív) AI	Bizonyos területeken összetett feladatok elvégzésére, emberi képességeket meghaladó tudás.	Elméleti szint, kutatási cél
5. szint	Teljes szuperintelligencia	Minden területen túlszárnyalja az emberi intelligenciát, új tudományos felfedezésekre képes.	Kutatási, jövőbeli cél

Forrás: https://www.forbes.com/sites/jodiecook/2024/07/16/openais-5-levels-of-super-ai-agi-to-outperform-human-capability/

KÖSZÖNETNYILVÁNÍTÁS

Mindenekelőtt köszönettel tartozom a Édesanyámnak: Bálint Ferencnének, Édesapámnak: Bálint Ferencnek és a Testvéremnek: Bálint Attilának a doktori tanulmányaim és kutatómunkám során nyújtott támogatásukért, türelmükért.

Ezenfelül nagy köszönettel tartozom Kedvesemnek, Bognár Anitának, hogy az elmúlt időszakban támogatott a tanulmányaim befejezésében.

Köszönöm Dr. Pető Richárd témavezetőként nyújtott szakmai és emberi támogatását.

Természetesen köszönöm az Óbudai Egyetem Biztonságtudományi Iskola oktatóinak, munkatársainak segítségét.