DOI: 10.24387/CI.2024.4.1

Szekeres Attila[1] *– Róbert Gábor*[2]

Mesterséges intelligencia az incidenskezelésben

Összefoglalás

A mesterséges intelligencia és gépi tanulás technológiák egyre jelentősebb szerepet töltenek be az incidenskezelésben, javítva az IT-szolgáltatások hatékonyságát. E tanulmány célja áttekinteni a mesterséges intelligencia alkalmazásának lehetőségeit és kihívásait ezen a területen. Szakirodalmi áttekintést végeztünk, elemezve a legújabb tudományos publikációkat és szakmai jelentéseket az automatizált döntéshozatal, prediktív incidenskezelés és gépi tanulási technikák terén. Az gép tanulás alapú megoldások felgyorsítják az incidensek kategorizálását és megoldását. A felügyelt és felügyelet nélküli tanulási módszerek kombinációja különösen hatékony. A prediktív incidenskezelés lehetővé teszi a problémák megelőzését. Egyes algoritmusok kiemelkedő teljesítményt mutatnak az incidensek osztályozásában. A mesterséges intelligencia jelentős potenciállal bír, de kihívásokat is felvet az adatminőség, etika és rendszerintegráció terén. Célunk bebizonyítani, hogy a technológia valóban képes hatékonyan szolgálni az incidenskezelést.

Kulcsszavak: mesterséges intelligencia, incidenskezelés, gépi tanulás, prediktív analitika, IT-szolgáltatásmenedzsment

***Jel-kód*:** C88, L86, O33

Bevezetés

A mesterséges intelligencia (MI) és gépi tanulás (ML – Machine Learning) alkalmazása az incidenskezelés területén forradalmi változásokat hozott az IT-szolgáltatásmenedzsmentben. Az MI-alapú rendszerek bevezetése nem csak a hatékonyságot növelte, de új lehetőségeket is teremtett a proaktív problémakezelésre és a kiberbiztonság javítására. A kutatás során a szakirodalmi áttekintés és adatelemzés kombinációját alkalmaztuk, hogy átfogó képet kapjunk az MI-alapú rendszerek típusairól, működési elveiről, előnyeiről és kihívásairól. A kutatás kiterjedt az automatizált döntéshozatal, prediktív incidenskezelés és gépi tanulási technikák legújabb fejleményeire, valamint ezek gyakorlati alkalmazására az IT-biztonság területén. Az elemzés során anonimizált adatokat használtunk fel, figyelembe véve olyan kulcsfontosságú mutatókat, mint az incidens megoldási idő, a hamis pozitívok aránya és a detektálási pontosság. Az eredmények azt mutatják, hogy az MI-vezérelt rendszerek jelentősen javítják az incidensdetektálás és elemzés hatékonyságát, lehetővé téve a valós idejű anomália észlelést és a proaktív fenyegetéskezelést. Az automatizált incidenskezelés révén a szervezetek képesek gyorsabban és pontosabban reagálni a kiberfenyegetésekre, miközben a prediktív analitika segítségével előre jelezhetik és megelőzhetik a potenciális problémákat. A gyorsabb gyökérok-analízis és a megnövekedett skálázhatóság további előnyöket kínál, lehetővé téve a komplex IT-környezetek hatékony kezelését. Ugyanakkor a technológia alkalmazása számos kihívást is felvet, beleértve az adatminőség és integráció problémáit, az etikai megfontolásokat az automatizált döntéshozatalban, valamint a rendszerintegráció és magyarázhatóság kérdéseit. Az MI-alapú incidenskezelés jövője ígéretes, de megköveteli a folyamatos fejlesztést, az etikai irányelvek kidolgozását és a felelősségteljes alkalmazást a maximális hatékonyság és biztonság érdekében.

[1] PhD hallgató Neumann János Egyetem Gazdálkodás- és Szervezéstudományok Doktori Iskola, IT Szolgáltatások divízó vezető, Nissan Motor Corporation

[2] PhD hallgató Neumann János Egyetem Gazdálkodás- és Szervezéstudományok Doktori IskolaRendszerüzemeltetési osztályvezető, Nissan Motor Corporation

Módszertan

A mesterséges intelligencia incidenskezelésben betöltött szerepének vizsgálatához a szakirodalmi áttekintés és a kvantitatív adatelemzés kombinációját alkalmaztuk. A szakirodalmi áttekintés során szisztematikusan elemeztük a legújabb tudományos publikációkat, a szakterület jelentéseit és szakmai cikkeket az automatizált döntéshozatal, prediktív incidenskezelés és gépi tanulási technikák terén. Kulcsszavak meghatározásával, adatbázisok kiválasztásával és szigorú keresési kritériumok alkalmazásával azonosítottuk a releváns forrásokat. A kiválasztott publikációkat részletesen elemeztük, fókuszálva az MI-alapú incidenskezelő rendszerek típusaira, működési elveire, előnyeire és kihívásaira. A kvantitatív adatelemzés során számszerű adatokat gyűjtöttünk és elemeztünk az MI-alapú és hagyományos incidenskezelő rendszerek teljesítményének összehasonlítására. Mivel a gyakorlatban is foglalkozunk IT incidenkezeléssel, első kézből tudtunk anonimizált adatokkal dolgozni, figyelembe véve olyan mutatókat, mint az incidens megoldási idő, hamis pozitívok aránya és detektálási pontosság. A két módszer eredményeinek szintézise lehetővé tette, hogy átfogó képet kapjunk az MI szerepéről az incidenskezelésben, azonosítsuk az elméleti megállapítások és a gyakorlati teljesítmény közötti összefüggéseket. Ez a kombinált megközelítés biztosította, hogy megalapozott következtetéseket vonhassunk le az MI hatékonyságáról és jövőbeli potenciáljáról az incidenskezelés területén, ötvözve az elméleti hátteret a gyakorlati teljesítménymutatókkal.

Eredmények

Fejlett incidensdetektálás és -elemzés

A fejlett incidensdetektálás és -elemzés területén az MI-rendszerek forradalmi változást hoztak a kiberbiztonságban. Ezek a rendszerek folyamatosan monitorozzák a hálózati forgalmat, rendszernaplókat és felhasználói viselkedést, lehetővé téve a valós idejű anomália észlelést. A gépi tanulási algoritmusok kulcsszerepet játszanak ebben a folyamatban, képesek felismerni a szokatlan mintázatokat és potenciális biztonsági kockázatokat, még mielőtt azok komolyabb incidensekké válnának. Ez a proaktív megközelítés jelentősen csökkenti az incidensek

azonosításához és kezeléséhez szükséges időt. Az MI-alapú elemzőrendszerek egyik legnagyobb előnye, hogy hatalmas mennyiségű biztonsági adatot képesek gyorsan és hatékonyan feldolgozni, azonosítva a trendeket, összefüggéseket és anomáliákat, amelyek rosszindulatú tevékenységre utalhatnak. Ez segíti a biztonsági szakembereket a fenyegetések priorizálásában és a hatékony válaszlépések megtervezésében. Az MI lehetővé teszi a prediktív analitika alkalmazását is, amely historikus adatok alapján előrejelzi a specifikus fenyegetések vagy sebezhetőségek valószínűségét, segítve a szervezeteket az erőforrások priorizálásában és a legjelentősebb kockázatokra való összpontosításban. Az automatizált fenyegetés-osztályozás révén az MI egyszerűsíti az incidenskezelést, automatikusan értékelve a detektált fenyegetések súlyosságát és priorizálva azokat. Ez a komplex, MI-vezérelt megközelítés jelentősen javítja a szervezetek képességét a kiberfenyegetések kezelésére, lehetővé téve a gyorsabb, pontosabb és proaktívabb biztonsági stratégiák kialakítását, ami nem csak az incidensek hatékonyabb kezelését eredményezi, de jelentősen csökkenti a potenciális károk mértékét is.

Automatizált incidenskezelés és válasz

Az automatizált incidenskezelés és válasz területén a mesterséges intelligencia (MI) és gépi tanulás (ML) technológiák forradalmi változásokat hoztak, jelentősen javítva a szervezetek képességét a kiberfenyegetések kezelésére. Az MI-vezérelt automatizálás lehetővé teszi az incidenskezelési folyamatok széles körű automatizálását, beleértve az incidensek kategorizálását, priorizálását és az előre meghatározott válaszlépések végrehajtását.

Az MI-alapú rendszerek egyik kulcsfontosságú előnye a folyamatos tanulás és adaptáció képessége. Ahogy a fenyegetések fejlődnek és új támadási módszerek jelennek meg, az MI-rendszerek képesek stratégiáikat módosítani, proaktívabb megközelítést kínálva a kiberbiztonságban. Ez a dinamikus alkalmazkodóképesség különösen fontos a gyorsan változó fenyegetési környezetben.

Az automatizált incidenskezelés nem csak a reakcióidőt csökkenti, de javítja a pontosságot is. Az MI-algoritmusok képesek nagy pontossággal elemezni az adatokat, minimalizálva a hamis pozitív és negatív eredményeket a fenyegetések észlelésében. Ez a pontosság segít a szervezeteknek elkerülni az időpazarlást és az erőforrások pazarlását a nem fenyegető események kivizsgálására, miközben biztosítja, hogy a valódi fenyegetéseket ne hagyják figyelmen kívül.

Prediktív incidenskezelés

A prediktív incidenskezelés az információtechnológia és a kiberbiztonság területén forradalmi változást hozott, jelentősen javítva a szervezetek képességét a potenciális problémák előrejelzésére és megelőzésére. Ez a fejlett megközelítés a mesterséges intelligencia (MI) és gépi tanulás (ML) technológiák integrálásán alapul, amelyek lehetővé teszik a múltbeli incidensadatok mélyreható elemzését, mintázatok és trendek azonosítását, valamint ezek alapján a jövőbeli problémák előrejelzését. Karlzén és Sommestad (2023) átfogó tanulmánya rámutatott, hogy az MI-alapú rendszerek nem csak gyorsabban és pontosabban detektálják az incidenseket, de felülmúlják a hagyományos módszereket a proaktív problémamegelőzésben is. Ez az agilitás lehetővé teszi a szervezetek számára, hogy jelentősen csökkentsék a potenciális hatásokat és minimalizálják a szolgáltatási zavarokat. A Gartner előrejelzése szerint 2025-re a rutinszerű szolgáltatási feladatok 80%-át autonóm módon fogják kezelni, ami alátámasztja a prediktív incidenskezelés növekvő jelentőségét. Az MI-vezérelt prediktív analitika nem csak az incidensek előrejelzésében játszik kulcsszerepet, hanem a kockázatok priorizálásában és a leghatékonyabb válaszlépések meghatározásában is. Ez a megközelítés lehetővé teszi a szervezetek számára, hogy proaktívan kezeljék a potenciális fenyegetéseket, jelentősen csökkentve az átlagos helyreállítási időt (MTTR – Mean Time To Repair) és növelve a kritikus alkalmazások rendelkezésre állását. A Forrester tanulmánya kimutatta, hogy az AIOps és az obszerválhatóság kombinációja akár 50%-kal is csökkentheti az MTTR-t, ami jelentős megtakarítást eredményez mind idő, mind erőforrások tekintetében. Ahogy az MI-rendszerek egyre több adatot dolgoznak fel, pontosságuk és hatékonyságuk idővel növekszik, lehetővé téve a szervezetek számára, hogy lépést tartsanak az állandóan változó fenyegetési környezettel. Ez a dinamikus alkalmazkodóképesség különösen fontos a gyorsan fejlődő technológiai környezetben, ahol új típusú fenyegetések és sebezhetőségek jelennek meg rendszeresen. Összességében a prediktív incidenskezelés paradigmaváltást jelent az IT-üzemeltetésben és a kiberbiztonsági stratégiákban, lehetővé téve a szervezetek számára, hogy proaktívan és hatékonyan kezeljék a potenciális problémákat, jelentősen javítva ezzel működési hatékonyságukat és ellenálló képességüket a digitális korszak kihívásaival szemben.

Gyorsabb gyökérok-analízis

Ezek a fejlett rendszerek képesek gyorsan és átfogóan elemezni a komplex eseményláncokat, korrelálni az adatokat a különböző rendszerekből és azonosítani az incidensek mögött húzódó alapvető okokat. Az MI algoritmusok, különösen a gépi tanulás és a mély tanulás technikák, lehetővé teszik a hatalmas mennyiségű adat gyors feldolgozását és értelmezését, olyan mintázatokat és összefüggéseket fedezve fel, amelyek az emberi elemzők számára nehezen észrevehetők lennének. Ez a képesség nem csak a problémák gyorsabb megoldását teszi lehetővé, de jelentősen hozzájárul a hasonló incidensek jövőbeli megelőzéséhez is. Az MI-vezérelt gyökérok-analízis egyik fő előnye, hogy képes kontextusba helyezni az eseményeket, figyelembe véve a rendszerek közötti komplex kölcsönhatásokat és függőségeket. Ez különösen értékes a modern, összetett IT-infrastruktúrákban, ahol egy incidens gyakran több rendszert is érinthet. Az automatizált elemzés segít a szakembereknek gyorsan azonosítani a kritikus pontokat és a leghatékonyabb beavatkozási lehetőségeket. Emellett az MI-rendszerek folyamatosan tanulnak és fejlődnek minden elemzett incidensből, így idővel egyre pontosabbá és hatékonyabbá válnak. Ez a folyamatos fejlődés lehetővé teszi a szervezetek számára, hogy proaktívan kezeljék a potenciális problémákat, jelentősen csökkentve az incidensek számát és súlyosságát. A gyorsabb gyökérok-analízis nem csak az incidenskezelés hatékonyságát javítja, de pozitív hatással van a szervezet egészére is. A gyorsabb problémamegoldás csökkenti az állásidőt, javítja a szolgáltatások minőségét és növeli az ügyfelek elégedettségét. Emellett lehetővé teszi az IT-csapatok számára, hogy több időt fordítsanak stratégiai feladatokra és innovációra, ahelyett, hogy folyamatosan tűzoltással foglalkoznának. Az MI-alapú gyökérok-analízis tehát nem csak egy technológiai fejlesztés, hanem egy stratégiai eszköz, amely segíti a

szervezeteket a működési hatékonyság és a szolgáltatásminőség folyamatos javításában, miközben csökkenti a kockázatokat és optimalizálja az erőforrás-felhasználást.

Skálázhatóság és hatékonyság

Az MI-alapú incidenskezelő rendszerek rugalmas kapacitása és hatékonysága forradalmasította az IT-biztonság és üzemeltetés területét, lehetővé téve a szervezetek számára, hogy lépést tartsanak a folyamatosan növekvő adatmennyiséggel és a egyre összetettebb fenyegetésekkel. Ezek a fejlett rendszerek képesek exponenciálisan növekvő adathalmazokat és incidensszámokat kezelni anélkül, hogy arányosan növelni kellene az emberi erőforrásokat, ami különösen értékes a gyorsan bővülő vagy komplex IT-infrastruktúrával rendelkező vállalatok számára. Az MI algoritmusok, különösen a gépi tanulás és a mély tanulás technikák, lehetővé teszik a rendszerek számára, hogy folyamatosan tanuljanak és adaptálódjanak az új fenyegetésekhez és mintázatokhoz, így idővel egyre hatékonyabbá és pontosabbá válnak. Ez a dinamikus alkalmazkodóképesség elengedhetetlen a mai gyorsan változó technológiai környezetben, ahol új típusú fenyegetések és sebezhetőségek jelennek meg napi szinten. Az MI-vezérelt automatizáció jelentősen csökkenti a rutinfeladatokra fordított időt és erőforrásokat, lehetővé téve a biztonsági szakemberek számára, hogy magasabb értékű, stratégiai fontosságú tevékenységekre összpontosítsanak. Ez nem csak a hatékonyságot növeli, de javítja a szervezet általános biztonsági helyzetét is, mivel a szakemberek több időt tudnak fordítani a komplex fenyegetések elemzésére és a proaktív védelmi stratégiák kidolgozására. A skálázhatóság egyik kulcsfontosságú aspektusa, hogy az MI-rendszerek képesek párhuzamosan feldolgozni és elemezni hatalmas mennyiségű adatot különböző forrásokból, beleértve a hálózati forgalmat, rendszernaplókat, felhasználói viselkedést és külső fenyegetés-intelligenciát. Ez a képesség lehetővé teszi a szervezetek számára, hogy átfogó és valós idejű képet kapjanak biztonsági helyzetükről, gyorsan azonosítva és reagálva a potenciális fenyegetésekre. Különösen értékes a felhő-alapú és hibrid infrastruktúrák esetében, ahol a hagyományos, statikus biztonsági megközelítések gyakran elégtelennek bizonyulnak. Ezek a rendszerek képesek dinamikusan alkalmazkodni a változó környezethez, biztosítva a konzisztens védelmet a gyorsan bővülő és változó IT-ökoszisztémákban. Emellett az MI-vezérelt incidenskezelés jelentősen csökkenti a hamis pozitívok számát, ami gyakran jelentős erőforrás-pazarlást okoz a hagyományos rendszerekben. A pontosabb detektálás és kategorizálás lehetővé teszi a biztonsági csapatok számára, hogy a valódi fenyegetésekre összpontosítsanak, optimalizálva az erőforrás-felhasználást. Összességében az MI-alapú incidenskezelő rendszerek méretezhetősége és hatékonysága nem csak technológiai előrelépést jelent, hanem stratégiai versenyelőnyt biztosít a szervezetek számára. Lehetővé teszi számukra, hogy hatékonyan kezeljék a növekvő biztonsági kihívásokat, miközben optimalizálják erőforrás-felhasználásukat és javítják általános működési hatékonyságukat. Ez a megközelítés nélkülözhetelen a modern, digitális-központú üzleti környezetben való sikerhez és a hosszú távú ellenálló képesség kiépítéséhez.

Kihívások és megfontolások

Az MI-alapú incidenskezelés kihívásai és megfontolásai komplex és többrétű témakört alkotnak, amely alapos vizsgálatot igényel a technológia hatékony és felelősségteljes alkalmazása érdekében. Az egyik legjelentősebb kihívás az adatminőség és integráció kérdése. Az MI-modellek hatékony működéséhez elengedhetetlen a nagy mennyiségű, jó minőségű adat, amely különböző forrásokból származik. Ez a követelmény gyakran jelentős akadályt jelent a szervezetek számára, különösen azok esetében, amelyek hagyományos, silókba rendezett adatstruktúrákkal rendelkeznek. Az adatok összegyűjtése, tisztítása és integrálása komplex folyamat, amely jelentős erőforrásokat és szakértelmet igényel. Ráadásul az adatok minősége közvetlenül befolyásolja az MI-modellek teljesítményét és megbízhatóságát, így a folyamatos adatminőség-ellenőrzés és -javítás kritikus fontosságú.

Az automatizált döntéshozatal, különösen kritikus rendszerek esetén, számos etikai kérdést vet fel. Például, hogyan biztosítható az átláthatóság és elszámoltathatóság az MI által hozott döntések esetében? Milyen mértékben támaszkodhatunk kizárólag az MI-re kritikus biztonsági döntések meghozatalában? Ezek a kérdések különösen fontosak olyan helyzetekben, ahol az MI-rendszerek döntései közvetlen hatással lehetnek az emberi életre vagy a kritikus infrastruktúrára. Az etikai irányelvek kidolgozása és betartása, valamint az MI-rendszerek folyamatos felügyelete és auditálása elengedhetetlen a felelősségteljes alkalmazás biztosításához.

A rendszerintegráció szintén jelentős kihívást jelent az MI-megoldások implementálása során. Az MI-technológiák zökkenőmentes integrálása a meglévő IT Service Management (ITSM) folyamatokba és eszközökbe gyakran komplex feladat. Ez nem csak technikai kihívásokat jelent, hanem szervezeti és kulturális változásokat is igényel. Az MI-rendszerek bevezetése gyakran megköveteli a meglévő munkafolyamatok és eljárások újragondolását, ami ellenállást válthat ki a személyzet körében. Emellett az MI-megoldások gyakran jelentős kezdeti beruházást igényelnek, mind pénzügyi, mind emberi erőforrások tekintetében, ami további akadályt jelenthet a szervezetek számára.

Az MI-modellek magyarázhatósága és interpretálhatósága szintén kritikus kérdés, különösen a biztonsági területen. Az úgynevezett „fekete doboz" MI-modellek, amelyek döntéshozatali folyamata nem átlátható, problémásak lehetnek olyan helyzetekben, ahol a döntések indoklása és auditálhatósága indokolt. Ez a kihívás szorosan kapcsolódik az etikai megfontolásokhoz, és megköveteli olyan MI-technikák fejlesztését és alkalmazását, amelyek lehetővé teszik a döntések nyomon követését és magyarázatát.

A folyamatosan változó fenyegetési környezet további kihívást jelent az MI-alapú incidenskezelő rendszerek számára. Az MI-modellek hatékonysága nagyban függ attól, hogy mennyire képesek adaptálódni az új típusú fenyegetésekhez és támadási módszerekhez. Ez folyamatos tanulást és frissítést igényel, ami jelentős erőforrásokat és szakértelmet követel meg. Emellett az MI-rendszerek maguk is célpontjai lehetnek a támadásoknak, például az úgynevezett „adversarial attacks" révén, amelyek célja az MI-modellek megtévesztése vagy manipulálása.

Az adatvédelem és szabályozási megfelelés szintén elengedhetetlen szempontok az MI-alapú incidenskezelésben. Az MI-rendszerek gyakran érzékeny adatokkal dolgoznak, ami szigorú adatvédelmi követelményeket támaszt. A GDPR és más adatvédelmi szabályozások betartása különös figyelmet igényel az MI-alkalmazások tervezése és implementálása során. Emel-

lett az iparág-specifikus szabályozások, például a pénzügyi vagy egészségügyi szektorban, további komplexitást adnak a megfelelőségi követelményekhez.

Következtetések

Az MI-alapú incidenskezelés jelentős gazdasági előnyöket kínál a szervezetek számára, amelyek túlmutatnak a puszta technológiai fejlesztéseken. A gyorsabb és pontosabb incidensdetektálás, valamint az automatizált válaszlépések révén jelentősen csökken az átlagos helyreállítási idő (MTTR), ami közvetlenül hozzájárul a szolgáltatások magasabb rendelkezésre állásához és az üzletmenet folytonosságához. Ez nem csak a közvetlen költségmegtakarításban mutatkozik meg, hanem az ügyfél elégedettség növekedésében és a potenciális bevételkiesés minimalizálásában is. Az MI-vezérelt prediktív analitika lehetővé teszi a proaktív problémakezelést, ami csökkenti a váratlan leállások és biztonsági incidensek számát, ezáltal mérsékelve a kapcsolódó pénzügyi veszteségeket. Az automatizáció révén csökkennek a munkaerőköltségek, mivel kevesebb emberi beavatkozás szükséges a rutinfeladatok elvégzéséhez, lehetővé téve a szakemberek számára, hogy magasabb értékű, stratégiai tevékenységekre összpontosítsanak. Ez nem csak a működési hatékonyságot növeli, de hosszú távon hozzájárul az innovációhoz és a versenyelőny megszerzéséhez. Az MI-rendszerek skálázhatósága lehetővé teszi a szervezetek számára, hogy rugalmasan alkalmazkodjanak a növekvő adatmennyiséghez és komplexitáshoz anélkül, hogy arányosan növelniük kellene az erőforrásaikat, ami jelentős költségoptimalizálást eredményez. Fontos kiemelni, hogy MI-alapú megoldások javítják a megfelelőségi folyamatokat és csökkentik a biztonsági kockázatokat, ami közvetetten csökkenti a potenciális büntetések és adatvédelmi incidensek okozta pénzügyi veszteségek kockázatát.

Irodalmi feldolgozás

BOUTABA, R. – SALAHUDDIN, M. A. – LIMAM, N. – AYOUBI, S. – SHAHRIAR, N. – ESTRADA-SOLANO, F. & CAICEDO, O. M. (2023): AI and Machine Learning for Network and Security Management. Wiley. https://www.wiley.com/en-us/AI+and+Machine+Learning+for+Network+and+Security+Management-p-9781119835899

CLOUDFABRIX (2024): How AI and ML Are Revolutionizing Incident Management in IT Ops. https://cloudfabrix.com/blog/how-ai-and-ml-are-revolutionizing-incident-management-in-it-ops/

CM-ALLIANCE (2024, March 6). Artificial Intelligence & Machine Learning: Role in Incident Response. https://www.cm-alliance.com/cybersecurity-blog/artificial-intelligence-machine-learning-role-in-incident-response

GYARAKI, RÉKA (2023): A mesterséges intelligencia felhasználási lehetősége és fejlesztésének szükségessége a jogalkalmazásban. In: Kovács Z. (szerk.) A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata. Katonai Nemzetbiztonsági Szolgálat, Budapest, 393-422.

KARLZÉN, H. & SOMMESTAD, T. (2023): Automatic incident response solutions: a review of proposed solutions' input and output. In The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29-September 01, 2023, Benevento, Italy. ACM. https://doi.org/10.1145/3600160.3605066

KOVÁCS, ZOLTÁN – GURÁLY, ROLAND (szerk.) (2023): A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata. Katonai Nemzetbiztonsági Szolgálat, Budapest.

RADIANTSECURITY (2024): AI-Driven Incident Response: Definition and Components. https://radiantsecurity.ai/learn/ai-incident-response/

REDRESSCOMPLIANCE (2024): Top 15 Real-Life Use Cases For AI In the Cybersecurity Industry. https://redresscompliance.com/top-15-real-life-use-cases-for-ai-in-the-cybersecurity-industry/

SÁFRÁN, JÓZSEF (2023): A mesterséges intelligencia és a rendvédelmi szervek, valamint a közigazgatás kapcsolata. Nemzetbiztonsági Szemle, 11(4), 20-34.

SHARMA, S. & KAUR, R. (2024): A Comprehensive Review on Artificial Intelligence and Machine Learning Techniques for Cybersecurity. International Journal of Computer Science and Engineering Research and Development, 14(1), 21-32. https://ijcserd.com/index.php/home/article/view/IJCSERD_14_01_003

SHU, X. – TIAN, K. & CIAMPAGLIA, G. L. (2024): Artificial Intelligence for Cybersecurity: A Survey. arXiv preprint arXiv:2404.01363. https://arxiv.org/abs/2404.01363

VORECOL (2024): How can Artificial Intelligence be leveraged to improve threat detection in cybersecurity? https://vorecol.com/blogs/blog-how-can-artificial-intelligence-be-leveraged-to-improve-threat-detection-in-cybersecurity-141954