CTI elemzés

A központosított NIDS a Nemzeti Távközlési Gerinchálózatban

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

Bevezető 4

Alapfogalmak, alapfokon 5

Főbb technológiai elemek és nemzetközi kitekintés 15

Miért központosított? 17

A projekt eredete és célja 19

A rendszer főbb képességei 20

Mire használható a gyakorlatban? 22

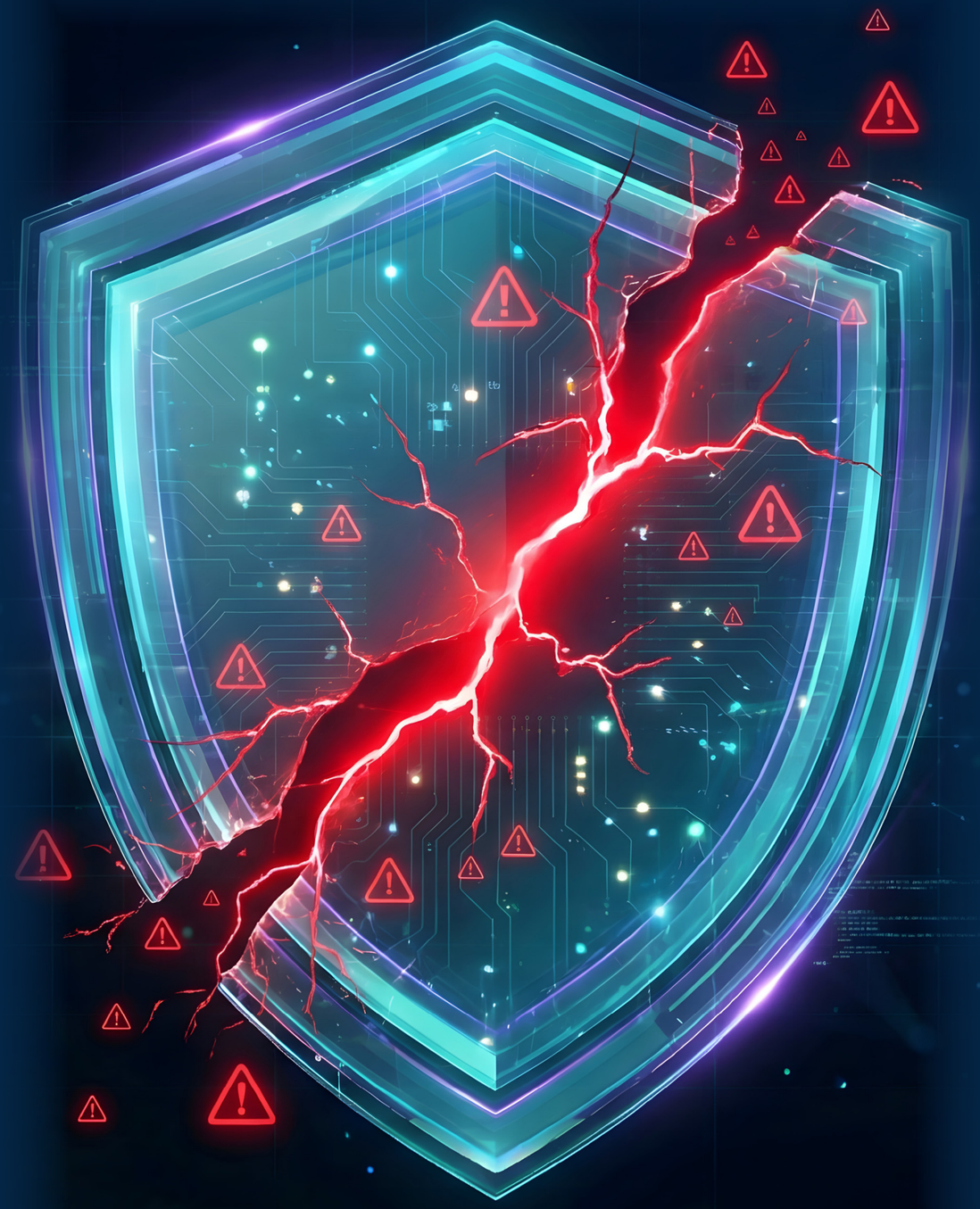
Miért hasznos az érintett szervezeteknek? 26

Korlátok és nehézségek 29

Merre tovább? 31

Zárszó 35

Források 36



Bevezető

A kormányzati informatikai rendszerek kiemelt célpontjai a kibertámadásoknak. A kritikus infrastruktúrák üzemeltetésének folyamatos biztosításához ezért elengedhetetlen a jól működő és minél kisebb reakcióidővel bíró többszintű védelem kialakítása. Ma már nem elegendő néhány végponti és hálózatvédelmi eszköz működtetése: ismerni kell az eszközök kommunikációját, figyelni kell a rendszerek forgalmát, és azonosítani kell a normálistól eltérő, veszélyt hordozó mintázatokat. Ezek alapján lehet a védelmi eszközök beállításait, szabályait és ellenőrzési logikáit az újabb fenyegetésekhez igazítani.

A modern támadások jelentős része hálózati kommunikációval jár: külső vezérlőszerverek elérésével, sérülékenység-kihasználási kísérletekkel, adatkiáramlásra utaló forgalommal, rendellenes csúcsokkal vagy szokatlan protokollhasználattal. Ezek felismerése nemcsak incidenskezelési kérdés, hanem a megelőzés és az üzemeltetésbiztonság szempontjából is fontos.

A központosított hálózati behatolásdetektáló rendszer (Network Intrusion Detection System, továbbiakban: NIDS) a Nemzeti Távközlési Gerinchálózatban (továbbiakban: NTG) olyan passzív, kiegészítő támogatást nyújtó képesség, amely a hálózati adatforgalom elsődleges vizsgálatával, adott ideig történő megőrzésével és további elemzések támogatásával segíti a biztonsági események és működési rendellenességek azonosítását.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet által működtetett rendszer neve Korai Figyelmeztető Rendszer (Early Warning System, továbbiakban: EWS). A rendszer

nem avatkozik be közvetlenül a forgalomba, nem helyettesíti az érintett szervezetek saját védelmi eszközeit, és nem veszi át az üzemeltetői vagy biztonsági felelősséget. Feladata az, hogy központi támogatással, nagyobb rálátást adjon a hálózati eseményekre, visszakereshetőséget és elemzési támogatást biztosítson. A központosított NIDS ennek megfelelően nem önálló megoldásként, hanem az egyes rendszerek biztonságáért felelős személyek, a biztonsági műveleti központok (Security Operations Center, továbbiakban: SOC) és a számítógép-biztonsági incidenskezelő csoport (Computer Security Incident Response Team, továbbiakban: CSIRT) feladatait támogató technikai adatforrásnak és elemzéstámogató eszköznek tekinthető. Értéke abban áll, hogy gyorsabb észlelést, megalapozottabb elemzést és hatékonyabb együttműködést tesz lehetővé a kormányzati informatikai rendszerek védelmében.

Alapfogalmak, alapfokon

- Alert log: a biztonsági eszközök által generált riasztásokat tartalmazó napló. Egy ilyen riasztás azt jelzi, hogy a rendszer egy szabály, minta vagy észlelési logika alapján gyanús eseményt azonosított. Az alert log nem maga az incidens, hanem olyan jelzés, amely szakértői értékelést igényel.
- API (Application Programming Interface, alkalmazásprogramozási interfész): olyan technikai kapcsolódási felület, amelyen keresztül különböző rendszerek szabályozott módon adatot cserélhetnek egymással.

- Arkime, korábbi nevén Moloch: nyílt forrású, nagy mennyiségű hálózati forgalom rögzítésére, indexelésére, visszakeresésére és megjelenítésére szolgáló teljes hálózati csomagrögzítő és elemzőrendszer.

- CADS (Cyber Analytics and Data System, kiberbiztonsági elemző és adatrendszer): a CISA modernizáltabb, adat- és elemzésközpontú kiberbiztonsági rendszerkörnyezete. Feladata a különböző forrásokból származó kiberbiztonsági adatok, köztük hálózati szenzoradatok összegyűjtése, feldolgozása és elemzése.

- CCN-CERT: Spanyolország nemzeti kormányzati incidenskezelő szervezete, amely a közigazgatási és állami rendszerek kiberbiztonsági védelmét támogatja. Feladatai közé tartozik a riasztások, ajánlások, sérülékenységi információk és incidenskezelési támogatások biztosítása.

- CERT (Computer Emergency Response Team, számítógépes vészhelyzet-kezelő csoport): a CSIRT-hez hasonló szerepkörű szervezet vagy csapat, amely informatikai biztonsági eseményekre reagál, figyelmeztetéseket adhat ki, és támogathatja a sérülékenységek, incidensek vagy fenyegetések kezelését. A két kifejezést sok környezetben hasonló értelemben használják.

- CISA (Cybersecurity and Infrastructure Security Agency, Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökség): az Amerikai Egyesült Államok szövetségi kiberbiztonsági és kritikus infrastruktúra-védelmi ügynöksége. Feladatai közé tartozik a szövetségi rendszerek védelmének támogatása, a kiberfenyegetésekkel kapcsolatos információmegosztás, riasztások kiadása, valamint a kritikus infrastruktúrák biztonságának erősítése.

- CSIRT (Computer Security Incident Response Team, számítógép-biztonsági incidenskezelő csoport): olyan szakértői csoport, amely számítógép-biztonsági incidensek kezelésével, koordinálásával és szakmai támogatásával foglalkozik. Feladata nemcsak a technikai elemzés, hanem az érintett szereplők közötti együttműködés támogatása is lehet.

- CTI (Cyber Threat Intelligence, kiberfenyegetési hírszerzés): feldolgozott fenyegetési információ, amely segíti a védekezést és a döntéshozatalt. Ide tartozhatnak például támadói módszerek, technikák, kampányok, sérülékenységek, indikátorok, IP-címek, domainek vagy kártevőkhöz kapcsolódó információk.

- Dashboard (áttekintő felület vagy irányítópult): olyan grafikus nézet, amely áttekinthetővé teszi a rendszerben keletkező adatokat. Egy jól kialakított dashboard segíthet abban, hogy az elemzők gyorsan képet kapjanak az aktuális eseményekről vagy az adott rendszer pillanatnyi biztonsági állapotáról.

- EDR (Endpoint Detection and Response, végponti észlelő és reagáló rendszer): olyan biztonsági megoldás, amely a munkaállomásokon, szervereken vagy más végpontokon figyeli a fájlműveleteket, folyamatokat, rendszereseményeket és gyanús viselkedéseket. Míg a NIDS hálózati nézőpontból vizsgálja a kommunikációt, az EDR azt mutatja meg, hogy mi történik magán az érintett eszközön.

- EINSTEIN: az Egyesült Államok szövetségi kormányzati hálózatainak védelmét támogató behatolásészlelési és -megelőzési képesség. Szenzoros hálózati megfigyelésre épült, és célja az ismert rosszindulatú vagy gyanús forgalmak azonosítása volt a szövetségi hálózatok irányába és azokból kifelé.

- Elasticsearch: nagy mennyiségű adat gyors keresésére, indexelésére és elemzésére szolgáló kereső- és analitikai motor. Biztonsági környezetben naplók, riasztások, forgalmi adatok és események tárolására, szűrésére és gyors lekérdezésére használható.

- Elastic Stack: az Elasticsearchre és a hozzá kapcsolódó adatfeldolgozó, adatgyűjtő és megjelenítő eszközökre épülő rendszerkörnyezet.

- EWS (Early Warning System, korai figyelmeztető rendszer): az ebben a cikkben bemutatott központosított hálózati monitoring rendszer neve. A „korai figyelmeztetés” nem előrejelzést vagy automatikus incidensmegállapítást jelent, hanem a hálózati forgalomban megjelenő korai technikai jelek felismerését, például gyanús külső kapcsolatokat, kártevőkommunikációra utaló mintákat, sérülékenység-kihasználási próbálkozásokat vagy szokatlan adatforgalmat.

- FIRST (Forum of Incident Response and Security Teams): nemzetközi szakmai együttműködési fórum, amely incidenskezeléssel és kiberbiztonsági reagálással foglalkozó szervezeteket kapcsol össze. Jelentősége abban áll, hogy támogatja a gyorsabb információmegosztást, a szakmai kapcsolattartást és a nemzetközi együttműködést.

- Frankenstack: kiberbiztonsági gyakorlatokhoz kialakított, nyílt forrású komponenseket összekapcsoló monitoring- és visszajelző keretrendszer.

- Host fejléc: a webes kérések egyik fontos mezője, amely megadja, hogy a kliens melyik kiszolgálót vagy webhelyet kívánja elérni. Ez különösen akkor hasznos, amikor egy IP-címen több webszolgáltatás is működik, mert segíthet azonosítani, hogy a kommunikáció ténylegesen melyik domainhez vagy alkalmazáshoz kapcsolódott.

- HTTP (Hypertext Transfer Protocol, hipertext átviteli protokoll): a webes kommunikáció egyik alapvető protokollja, amelyen keresztül a böngészők és webes alkalmazások adatot cserélnek a kiszolgálókkal. Feloldott forgalomban a HTTP-kérések és válaszok részletei, például a kért URL, a metódus, a válaszkód vagy egyes fejlécmezők biztonsági elemzésre is felhasználhatók.

- IOC (Indicator of Compromise, kompromittálódásra utaló indikátor): olyan technikai jel, amely arra utalhat, hogy egy rendszer támadással, fertőzéssel vagy más biztonsági eseménnyel érintett. Ilyen indikátor lehet például egy gyanús IP-cím, domainnév, fájlnév, hash érték, URL, e-mail-cím vagy olyan kommunikációs minta, amely ismert káros tevékenységhez kapcsolódik.

- Kibana: az Elastic Stack grafikus felülete, amely az Elasticsearchben tárolt adatok keresésére, szűrésére, vizualizálására és dashboardokon történő megjelenítésére szolgál. Jelen esetben NIDS-riasztások, netflow-adatok és egyéb naplók áttekintésére használható; az Elastic machine learning képességei pedig anomáliák, ritka események és szokatlan mintázatok felismerését is támogathatják.

- Machine learning (gépi tanulás): olyan elemzési megközelítés, amely nagy mennyiségű adatban próbál mintázatokat, eltéréseket vagy szokatlan viselkedéseket felismerni. Hálózati monitoring környezetben például forgalmi anomáliák, ritka események, időbeli eltérések vagy megszokottól eltérő kommunikációs minták azonosításában támogathatja az elemzői munkát.

- Nemzeti Távközlési Gerinchálózat (NTG): olyan központi távközlési infrastruktúra, amely kormányzati és közigazgatási rendszerek hálózati kapcsolataiban tölt be meghatározó szerepet. A központosított NIDS szempontjából azért fontos, mert a hálózati szintű láthatóság és elemzés ezen a központi infrastruktúrán keresztül tudja támogatni a védett rendszerek biztonsági felügyeletét.

- NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence, Kooperatív Kibervédelmi Kiválósági Központ): Tallinnban működő nemzetközi kibervédelmi szakmai központ, amely kutatással, képzéssel, gyakorlatokkal és szakmai elemzésekkel támogatja a kiberbiztonsági képességek fejlesztését.

- Netflow log: a hálózati kommunikáció összesített adatait tartalmazó napló. Megmutatja, hogy melyik forráscím melyik célcímmel kommunikált, milyen porton, mennyi ideig, és mekkora adatforgalom mellett. Tartalmi részleteket nem ad, de forgalmi mintázatok és anomáliák felismerésére jól használható.

- NCPS (National Cybersecurity Protection System, nemzeti kiberbiztonsági védelmi rendszer): az Egyesült Államok szövetségi hálózatainak védelmét támogató program- és rendszerkörnyezet, amelyhez az EINSTEIN képességei is kapcsolódtak. Célja a szövetségi rendszereket érintő kiberfenyegetések észlelése, elemzése és részben megelőzése központi kiberbiztonsági eszközökkel és szolgáltatásokkal.

- NIDS/NIPS (Network Intrusion Detection System / Network Intrusion Prevention System, hálózati behatolásdetektáló / hálózati behatolásmegelőző rendszer): a NIDS passzív módon figyeli és elemzi a hálózati forgalmat, majd gyanús vagy káros esemény esetén riasztást generál. A NIPS ezzel szemben aktív eszköz, amely beavatkozásra is képes lehet, például blokkolhat vagy megszakíthat egy támadási kísérletet. Alapvetően a rendszerbe való kapcsolódásuk miként határozza meg a felhasználás módjának lehetőségét. Amikor az éles forgalom átfolyik rajta, akkor képes beleavatkozni abba; ha kitükrözött forgalmat kap, akkor csak detektálni tud.

- NIDS/NIPS és tűzfal közötti különbség: a tűzfal elsődlegesen forgalomszabályozó eszköz, amely eldönti, hogy egy kapcsolat engedélyezett vagy tiltott. A NIDS/NIPS ezzel szemben a forgalom biztonsági tartalmát és mintázatait vizsgálja, ezért olyan eseményeket is észlelhet, amelyek önmagukban nem sértenek tűzfalszabályt, mégis kockázatosak lehetnek. A modern tűzfalak egy része szintén rendelkezik saját szignatúra- és IPS-képességekkel, de az eltérő működési logika miatt más jellegű detekciós, elemzési

lehetőségeket biztosítanak.

- PCAP (packet capture, csomagrögzítés): a hálózati adatcsomagok mentett formája, amely lehetővé teszi a forgalom későbbi részletes vizsgálatát. A pcap állományok nemcsak azt mutathatják meg, hogy két rendszer között kapcsolat jött létre, hanem az átvitt kommunikáció részleteinek utólagos elemzésére is alkalmasak.

- SAT-SARA / SAT-INET: a spanyol CCN-CERT korai figyelmeztető rendszerei, amelyek szenzoros hálózati monitoringgal támogatják a közigazgatási hálózatok védelmét. A SAT-SARA a spanyol közigazgatási SARA-hálózathoz, a SAT-INET pedig az internetkapcsolatok figyeléséhez kapcsolódik.

- SIEM (Security Information and Event Management, biztonsági információ- és eseménykezelő rendszer): különböző forrásokból származó naplókat és biztonsági eseményeket gyűjt össze, kereshetővé tesz, korrelál és megjelenít. Segítségével a különálló eseményekből átfogóbb biztonsági kép alakítható ki.

- SOC (Security Operations Center, biztonsági műveleti központ): olyan szervezeti egység, amely biztonsági eseményeket figyel, elemez és kezel. Feladata lehet a riasztások értékelése, incidensek elsődleges vizsgálata, eszkalációja, valamint a folyamatos biztonsági monitoring biztosítása.

- SPAN session (Switched Port Analyzer, kapcsolóport-tükrözési munkamenet): olyan hálózati kapcsolókon beállítható forgalomtükrözési megoldás, amely egy vagy több port, VLAN vagy hálózati irány adatforgalmának másolatát egy kijelölt megfigyelő portra továbbítja. A NIDS szempontjából azért fontos, mert így a rendszer a vizsgált hálózati forgalom másolatát elemzi, miközben nem kerül közvetlenül a kommunikáció útvonalába, tehát passzív módon működik.

- Suricata: nyílt forrású, nagy teljesítményű hálózati IDS (Intrusion Detection System, behatolásdetektáló rendszer), IPS (Intrusion Prevention System, behatolásmegelőző rendszer) és NSM (Network Security Monitoring, hálózatbiztonsági monitorozó) motor. A hálózati forgalmat szabályok és minták alapján vizsgálja, riasztásokat és naplókat készít, valamint pcap állományok utólagos feldolgozására is alkalmas. A Suricatát az OISF (Open Information Security Foundation) fejleszti.

- TLS (Transport Layer Security, szállítási rétegbeli biztonsági protokoll): széles körben használt titkosítási protokoll, amely a hálózati kommunikáció védelmét szolgálja, például webes kapcsolatok esetén. Biztonsági előnye, hogy védi az adatforgalom tartalmát az illetéktelen megismeréstől, ugyanakkor hálózati elemzési szempontból erősen korlátozza a lehetőségeket.

- Tűzfal: olyan hálózatvédelmi eszköz, amely szabályok alapján engedélyezi vagy tiltja a hálózati kapcsolatokat. A modern, új generációs tűzfalak már nemcsak IP-címek és portok alapján működnek, hanem alkalmazások, felhasználók, tartalmak, ismert fenyegetések és bizonyos viselkedési minták alapján is képesek szűrni a forgalmat.

- URL (Uniform Resource Locator, egységes erőforrás-helymeghatározó): egy webes erőforrás címe, amely megmutatja, hogy a kliens pontosan milyen tartalmat, útvonalat vagy szolgáltatást próbált elérni. Biztonsági vizsgálatnál egy gyanús URL fontos jelzés lehet, mert utalhat sérülékenység-kihasználási próbálkozásra, adathalász oldalra, kártevőletöltésre vagy nem várt külső kommunikációra.

- User-Agent: olyan HTTP-fejlécmező, amely általában a kliensprogramról, böngészőről, alkalmazásról vagy eszközről ad információt. Biztonsági szempontból azért hasznos, mert szokatlan, hamisított vagy ismert kártevőkhöz kapcsolódó User-Agent értékek gyanús automatizált forgalomra, exploit eszközre vagy kártevőkommunikációra utalhatnak.

- X-Forwarded-For: olyan HTTP-fejlécmező, amely proxyk, terheléselosztók vagy más köztes eszközök mögött segíthet az eredeti kliens IP-címének azonosításában. Központi monitoring környezetben azért lehet fontos, mert egy riasztás vagy webes kérés értelmezésekor nem mindig elég a közvetlenül látható forráscím; szükség lehet annak megállapítására is, hogy a kérés eredetileg melyik kliens felől indult.

Főbb technológiai elemek és nemzetközi kitekintés

Az EWS felépítése olyan nyílt forrású komponensekre épülő hálózatbiztonsági monitoring-architektúrát követ, amely nemzetközi példákban is visszaköszön. A rendszer alapja a kitükrözött hálózati forgalom feldolgozása: a vizsgált adatkommunikáció nem az EWS-en halad keresztül, hanem annak egy kicsatolt másolata (span session) kerül rögzítésre és elemzésre - ezért passzív a rendszerünk. A forgalom megfigyelése, naplózása és elemzése nem jár közvetlen hálózati beavatkozással, sikeres túlterheléses támadás esetén pedig a hálózati eszközök prioritása mindig a védett rendszer kiszolgálása.

A kitükrözött forgalmat az Arkime rögzíti pcap formátumban, és ehhez elemzői felületet is biztosít. Ez lehetővé teszi, hogy egy később gyanússá váló esemény ne csak naplóbejegyzések alapján legyen vizsgálható, hanem szükség esetén az eredeti hálózati kommunikáció is visszakereshető legyen. Az érintett munkamenetek az Arkime felületén kereshetők, szűrhetők és áttekinthetők, részletesebb vizsgálat esetén pedig a pcap állomány külön csomagszintű elemzőeszközzel, például Wiresharkkal is feldolgozható.

A hálózati forgalom biztonsági ellenőrzését a Suricata (itt IDS a passzív felépítés miatt) végzi. A Suricata az aktuális szabálykészletek alapján közel valós időben elemzi a forgalmat, és riasztásokat, valamint forgalmi naplókat állít elő. Ezek az alert és netflow jellegű adatok adják az elsődleges támpontot ahhoz, hogy a nagy mennyiségű hálózati forgalomból ki lehessen választani a biztonsági szempontból releváns eseményeket.

A keletkező logok megjelenítését és elemzését Kibana/Elastic alapú felület támogatja. Ez teszi lehetővé, hogy az elemzők ne nyers naplóhalmazokból dolgozzanak, hanem kereshető, szűrhető, grafikonokkal és dashboardokkal támogatott nézetekben vizsgálják a riasztásokat és forgalmi mintázatokat. A vizualizáció ebben a környezetben nem pusztán kényelmi funkció: a nagy mennyiségű adat értelmezéséhez, a trendek felismeréséhez és az anomáliák kiszűréséhez alapvető elemzői támogatást ad.

A három fő elem egymásra épülő munkafolyamatot alkot. A Suricata segít azonosítani, hogy mely események igényelnek figyelmet, a Kibana áttekinthetővé és kereshetővé teszi a riasztásokat és forgalmi adatokat, az Arkime pedig lehetőséget ad arra, hogy az elemző a releváns kommunikációt mélyebben, akár csomagszinten is megvizsgálja. Így a rendszer nemcsak riasztást ad, hanem az első jelzéstől a részletes visszakeresésig támogatja az elemzői munkát.

A nemzetközi példák azt mutatják, hogy az EWS technológiai és működési logikája nem elszigetelt megoldás. A NATO CCDCOE által fejlesztett Frankenstack keretrendszer technológiailag különösen közel áll ehhez a felépítéshez: tükrözött hálózati forgalomra, Arkime-alapú csomagrögzítésre és -indexelésre, Suricata-alapú NIDS-elemzésre, valamint Elasticsearch/Kibana alapú feldolgozásra és

megjelenítésre épül.

Hasonló elvet követnek a spanyol CCN-CERT SAT-SARA és SAT-INET korai figyelmeztető rendszerei is. Ezek szenzoros felépítéssel, IDS-alapú észleléssel és netflow-jellegű eseményfeldolgozással támogatják a közigazgatási hálózatok védelmét. A hangsúly ezekben az esetekben is azon van, hogy a központi vagy koordinált hálózati monitoring olyan rálátást adjon, amelyet az egyes intézmények önállóan nehezebben tudnának biztosítani.

Tágabb előképként ide sorolható az Amerikai Egyesült Államok EINSTEIN rendszere is, amely a CISA National Cybersecurity Protection System részeként behatolásészlelési és -megelőzési képességeket biztosított szövetségi hálózatoknál. Az EINSTEIN képességeinek egy része idővel a CADS által biztosított modernebb adatfeldolgozási és elemzési környezetbe integrálódott.

Miért központosított?

A központosított jelleg abból adódik, hogy nem egy-egy intézmény különálló, helyi érzékelő rendszeréről van szó, hanem a Nemzeti Távközlési Gerinchálózathoz kapcsolódó, központi hálózati szintű megfigyelési és elemzési képességről. A rendszer elsődleges elhelyezkedése a Kormányzati Adatközpont, ahol a védett rendszerekhez kapcsolódó, kitükrözött hálózati forgalom egységes technológiai környezetben rögzíthető, ellenőrizhető és visszakereshető.

A központosítás egyik legfontosabb előnye, hogy a vizsgált rendszerek eseményei nem elszigetelten jelennek meg. Egy újonnan azonosított gyanús IP-cím, domain, támadási minta vagy

rendellenes forgalmi jelenség több védett rendszer vonatkozásában is gyorsan visszaellenőrizhető. Ez különösen hasznos akkor, ha egy fenyegetés nem egyetlen rendszert érint.

A központi működés az elemzői munkát is hatékonyabbá teszi. Az egységes naplózás, kereshetőség és vizualizáció révén gyorsabban összevethetők az események, könnyebben felismerhetők a visszatérő mintázatok, és egyszerűbbé válik az incidensekhez kapcsolódó technikai adatok összegyűjtése. Ez támogatja a SOC- és CSIRT-feladatokat, valamint az érintett rendszerek üzemeltetőinek és biztonsági szakértőinek munkáját is.

Fontos ugyanakkor, hogy a központosított NIDS nem veszi át az érintett szervezetek biztonsági felelősségét. Kiegészítő szolgáltatásként működik: központi, hálózati szintű láthatóságot és elemzési támogatást biztosít, amely gyorsabb észlelést, jobb visszakereshetőséget és hatékonyabb együttműködést tesz lehetővé.

A projekt eredete és célja

Az EWS létrejötte egy hosszabb közigazgatási, digitalizációs és kiberbiztonsági folyamatba illeszkedik. Magyarországon már az 1990-es évektől megjelent az elektronikus közigazgatás fejlesztésének igénye, majd az EU-csatlakozást követően az uniós finanszírozású programok tovább gyorsították az állami nyilvántartások, ügyintézési folyamatok és központi szolgáltatások digitalizációját. Ahogy a közigazgatási feladatok mind nagyobb része vált elektronikus szolgáltatásként elérhetővé, úgy nőtt ezek biztonságának, ellenőrizhetőségének és védelmének jelentősége is.

A 2013-as uniós kiberbiztonsági stratégia és Magyarország nemzeti kiberbiztonsági stratégiája már egyértelműen állami működési és biztonsági kérdésként kezelte az elektronikus információs rendszerek védelmét. Ez a szemlélet különösen fontossá vált a közigazgatási rendszereknél, amelyek jelentős mennyiségű személyes, gazdasági, hatósági és döntés-előkészítési adatot kezelnek. Ezeknél nemcsak a működőképesség, hanem a visszaélések, rendellenességek és korrupciós kockázatok csökkentése is lényeges szemponttá vált.

Ebben a környezetben valósult meg a „*KÖFOP keretében megvalósuló fejlesztések IT biztonságának növelése, ezáltal rendszerekkel összefüggő korrupciós lehetőségek és kockázatok csökkentése*” című projekt. A fejlesztés célja olyan korai figyelmeztető képesség kialakítása volt, amely a közigazgatási információs rendszerek biztonságát hálózati szintű észleléssel támogatja, és segíti a támadások, visszaélések, rendellenességek, illetve ezek kísérleteinek gyorsabb felismerését.

Az EWS előkészítése ugyanabban az időszakban zajlott, amikor az Európai Unió elfogadta a NIS1 irányelvet. A 2016/1148/EU irányelv azt várta el, hogy a tagállamok alakítsák ki a hálózati és információs rendszerek magas közös biztonsági szintjéhez szükséges szervezeti és műszaki képességeket. Ide tartozott a CSIRT-működés, az incidensek figyelése, a korai figyelmeztetés, a riasztások kiadása és az incidenskezelés támogatása is. Ehhez a képességalapú megközelítéshez jól illeszkedett egy központi hálózati észlelő és figyelmeztető rendszer.

A NIS2 később tovább erősítette ezt az irányt. A 2022/2555/EU irányelv szélesebb szervezeti körre kiterjesztve fogalmazta meg a kiberbiztonsági elvárásokat.

A rendszer jelenlegi működési alapját a 214/2020. (V. 18.) Korm. rendelet adja az elektronikus információbiztonsági korai figyelmeztető rendszerről. A rendelet az EWS-t központosított előrejelző rendszerként határozza meg, amely a védett elektronikus információs rendszerek hálózati forgalmát szenzorokkal elemzi, és automatizált módon azonosít információbiztonsági kockázatokat, valamint kiberbiztonsági incidensekre, adatokkal való visszaélésre vagy ezek kísérletére utaló eseményeket.

A rendszer főbb képességei

Az EWS fő képessége, hogy a kicsatolt hálózati forgalmat passzív módon vizsgálja, naplózza, megjeleníti és korlátozott ideig visszakereshető formában tárolja. Mivel a rendszer kitükrözött forgalmat elemez, az ellenőrzés nem jár közvetlen hálózati beavatkozással. A vizsgálat IDS-szabályok alapján történik, amelyek ismert támadási minták, kártevőkommunikációk, sérülékenység-kihasználási

próbálkozások és más gyanús hálózati jelenségek felismerését segítik.

Különösen fontos a feloldott hálózati forgalom vizsgálata, mert a titkosított kommunikáció önmagában csak korlátozott képet ad. Ilyenkor jellemzően a kommunikáló IP-címek, portok, időpontok, adatforgalmi mennyiségek és egyes kapcsolatfelépítési adatok láthatók, az alkalmazásszintű tartalom és a részletes protokollmezők azonban nem. Feloldott forgalomnál ezzel szemben vizsgálható például a kért URL, a HTTP-metódus, a válaszkód, a Host fejléc, a User-Agent, illetve proxyzott környezetben az X-Forwarded-For mező.

Ez a többlet-láthatóság pontosabb elemzést tesz lehetővé. Segíthet sérülékenység-kihasználási kísérletek, gyanús webes kérések, rendellenes API-használat, szokatlan kliensazonosítók és lehetséges adatkiáramlási minták felismerésében. A feloldott forgalom vizsgálata ugyanakkor érzékeny adatkezelési kérdés, ezért az EWS csak a számára engedélyezett forgalmat vizsgálhatja.

A rendszer a legfrissebb szabálycsomagok alapján állít elő figyelmeztetéseket, és lehetőséget ad a védett rendszerek sajátosságaihoz igazodó egyedi szabályok alkalmazására is. Így az eltérő technológiákból, működési mintákból vagy kockázatokból fakadó célzott detekciók is megvalósíthatók.

A forgalomról készült netflow és alert logok a kommunikációs kapcsolatok összesített jellemzőit és a szabályok alapján gyanúsnak minősített eseményeket tartalmazzák. Ezek grafikus megjelenítése szűrhető, kereshető és vizuálisan értelmezhető formában támogatja a forgalmi mintázatok, riasztások és anomáliák vizsgálatát.

A kicsatolt, feloldott hálózati adatforgalom két hétig pcap formátumban érhető el. Ez biztosítja a retrospektív vizsgálatok

lehetőségét: ha egy esemény csak később válik gyanússá, vagy új indikátor alapján kell visszakeresni korábbi kommunikációkat, a nyers forgalom a tárolási időn belül újra elemezhető. A rendszer így több elemzési szintet biztosít: szabályalapú riasztást, forgalmi naplót, grafikus elemzési nézetet és szükség esetén nyers pcap állományt.

Mire használható a gyakorlatban?

Az EWS, a hálózati forgalom monitorozásából származó technikai adatokat olyan formában teszi elérhetővé, amely támogatja a napi üzemeltetésbiztonsági, SOC- és incidenskezelési feladatokat. A rendszer nem önállóan dönt arról, hogy egy esemény incidensnek minősül-e, hanem olyan riasztásokat, forgalmi adatokat és visszakereshető nyomokat biztosít, amelyek alapján az elemzők és az érintett rendszerek szakértői gyorsabban tudnak képet alkotni egy vizsgálatra érdemes eseményről.

A védett rendszerek IT-biztonsági szakértői számára az innen kinyerhető adatok napi riportok, időszakos összefoglalók és célzott technikai jelzések formájában is hasznosíthatók. Ezek a riportok segíthetnek abban, hogy az érintett szervezetek ne csak egyedi riasztásokat lássanak, hanem átfogóbb képet kapjanak a rendszereiket érintő hálózati aktivitásról. Egy rendszeresen visszatérő riasztás, egy szokatlan célországba irányuló kommunikáció, egy újonnan megjelenő külső IP-cím vagy egy rendellenes forgalmi mennyiség önmagában még nem feltétlenül jelent incidenst, de olyan jelzés lehet, amelyet érdemes ellenőrizni.

Támogatja az IP- és domaintiltások megalapozását is a Nemzeti Távközlési Gerinchálózaton. Ha egy külső cím vagy domain több védett rendszerrel kapcsolatban is gyanús aktivitást mutat, vagy ismert káros infrastruktúrához kapcsolódik, a hálózati forgalmi adatok segíthetnek a tiltási döntések előkészítésében. Ez különösen hasznos olyan esetekben, amikor egy indikátor nem elszigetelt eseményként jelenik meg, hanem több rendszerben vagy több időpontban is visszatérő mintázatot mutat.

Fertőzött szerverek, géptermi rendszercsoportok vagy munkaállomás-csoportok esetén az EWS a fertőzés lokalizálását és a kárcsökkentést is támogathatja. A hálózati forgalmi adatok alapján azonosítható lehet, hogy mely rendszerek kommunikálnak gyanús külső címekkel, mely belső címek mutatnak kártevőkommunikációra utaló mintázatot, illetve utal-e hálózati aktivitás arra, hogy a fertőzés más rendszerek irányába is továbbterjedhetett. Az incidens kezelése közben az EWS segíthet annak ellenőrzésében is, hogy a leválasztás, tiltás, tisztítás vagy újratelepítés után megszűnt-e a gyanús hálózati aktivitás. Így a rendszer nemcsak az első észlelésben, hanem a fertőzés behatárolásában, a kárenyhítésben és a felszámolás eredményének visszaellenőrzésében is hasznos technikai támpontot adhat.

Az üzemeltetésbiztonsági feladatokban a rendszer nemcsak támadások vagy kártevőkommunikációk felismerésére használható. Hálózati adatok alapján sokszor működési rendellenességek is azonosíthatók: hibás konfigurációk, váratlanul kommunikáló szerverek, nem tervezett külső kapcsolatok, szokatlan protokollhasználat vagy rendellenes forgalmi csúcsok. Ezek nem minden esetben kiberbiztonsági incidensek, de az üzemeltetés szempontjából fontos jelzések lehetnek, mert rávilágíthatnak hibás működésre, elavult komponensekre vagy nem megfelelően dokumentált rendszerkapcsolatokra.

A rendszer a CTI jellegű elemzések egyik fontos adatforrása is lehet. A hálózati riasztások, netflow-adatok és visszakereshető pcap állományok alapján nemcsak egyedi események vizsgálhatók, hanem hosszabb időszakra vonatkozó trendek is. Megfigyelhető például, hogy milyen támadási minták jelennek meg gyakrabban, mely szolgáltatásokat érik rendszeresen próbálkozások, vagy milyen külső infrastruktúrák kapcsolódnak visszatérően gyanús kommunikációkhoz. Ezek az információk időszakos elemzések, figyelmeztetések és védekezési javaslatok alapjául szolgálhatnak.

Az EWS különösen hasznos lehet rendszertesztek és fejlesztések hálózati visszaellenőrzésére is. Egy új szolgáltatás bevezetése, konfigurációmódosítás, alkalmazásfrissítés vagy infrastruktúraváltozás után ellenőrizhető, hogy a rendszer valóban úgy kommunikál-e, ahogyan azt tervezték. Láthatóvá válhatnak nem várt külső kapcsolatok, hibás API-hívások, indokolatlan adatforgalmak vagy olyan kommunikációs irányok, amelyek a fejlesztési vagy üzemeltetési dokumentációban nem szerepeltek. Ez a képesség nem klasszikus incidenskezelési funkció, mégis jelentős biztonsági értéke van.

A lehetséges adatszivárgások vizsgálatában a hálózati adatok

különösen fontos támpontot adhatnak. A rendszer segíthet annak ellenőrzésében, hogy történt-e szokatlan mennyiségű kifelé irányuló adatforgalom, volt-e kapcsolat gyanús külső címekkel, vagy megjelentek-e olyan kommunikációs minták, amelyek adatkiáramlásra utalhatnak. Feloldott forgalom esetén a vizsgálat mélysége ennél nagyobb is lehet: elektronikus levelezésnél a továbbított üzenetek tartalma és csatolmányai, fájltovábbításnál pedig az átvitt fájlok is megjelenhetnek a rögzített adatforgalomban. A pcap alapú visszakereshetőség a kéthetes megőrzési időn belül lehetőséget ad arra, hogy egy később felmerülő gyanú esetén ne csak a kapcsolat ténye, hanem adott esetben az átvitt tartalom is ellenőrizhető legyen.

Visszaélésgyanús vagy korrupciós kockázatot érintő ügyekben az EWS technikai háttérinformációt biztosíthat, ha a vizsgált eseménynek hálózati lenyomata is van. Ilyen lehet például egy jogosulatlan adatlekérdezést követő külső adattovábbítás, egy nem dokumentált rendszerkapcsolat, egy szokatlan időpontban végzett adatkommunikáció vagy olyan forgalmi esemény, amely egy belső szabálytalanság technikai körülményeit segíthet tisztázni. Fontos azonban, hogy a rendszer ebben az esetben sem önálló bizonyító vagy döntéshozó eszköz, hanem hálózati monitoringból származó technikai adatforrás, amely más naplókkal, rendszerinformációkkal, jogosultsági adatokkal és szakértői vizsgálattal együtt értelmezhető.

A gyakorlatban tehát az EWS nem egyetlen felhasználási területre korlátozódik. Egyszerre támogathatja a napi biztonsági monitoringot, az incidenskezelést, a fertőzött rendszerek lokalizálását, a forgalmi anomáliák felismerését, a védelmi intézkedések előkészítését, a CTI-jellegű elemzést, a rendszertesztek visszaellenőrzését és az utólagos

vizsgálatokat. Értéke abban áll, hogy a hálózati forgalomból származó jelzéseket központi, kereshető és elemzésre alkalmas formában teszi elérhetővé, így gyorsabb és megalapozottabb szakértői munkát tesz lehetővé.

Miért hasznos az érintett szervezeteknek?

A már felsorolt képességek által az EWS olyan kiegészítő IT-biztonsági támogatást jelent, amely nem helyettesíti a saját védelmi eszközöket és folyamatokat, de érdemben erősítheti azok működését. Előnye, hogy a hálózati események nemcsak helyi naplókból és biztonsági eszközökből, hanem központi hálózati nézőpontból is vizsgálhatók. Ez különösen akkor értékes, amikor egy esemény gyors értelmezéséhez az adott rendszer helyi adatai mellett a kommunikáció átfogóbb vizsgálatára is szükség van.

A szolgáltatás az ügyfelek részére ingyenes, kiegészítő biztonsági képességként jelenik meg. Ez azért fontos, mert a hálózati forgalom rögzítése, IDS-alapú ellenőrzése, naplózása és grafikus megjelenítése olyan erőforrásokat igényel, amelyeket nem minden szervezet tudna önállóan, azonos mélységben és folyamatosan fenntartani. A központosított működés így olyan többlet-láthatóságot biztosít, amelyhez az érintett szervezetek külön saját infrastruktúra kiépítése nélkül férhetnek hozzá.

Az EWS gyorsíthatja az incidensekkel kapcsolatos reakcióképességet is. Egy gyanús külső kapcsolat, kártevőkommunikációra utaló minta, sérülékenység-kihasználási

próbálkozás vagy szokatlan adatforgalom esetén már az első jelzéseknél hasznos technikai információt adhat. Segíthet annak tisztázásában, hogy mely rendszer, milyen időszakban, milyen külső vagy belső címekkel kommunikált, és az esemény elszigetelt jelenségnek vagy szélesebb mintázat részének tűnik-e. Innen ered az EWS elnevezésében szereplő „korai figyelmeztetés”: nem előrejelzést vagy automatikus incidensmegállapítást jelent, hanem a hálózati forgalomban megjelenő korai technikai jelek felismerését.

Az incidenskivizsgálás adminisztratív terhei is csökkenhetnek, mert a központi, kereshető adatforrás segíthet gyorsabban kijelölni a releváns rendszereket, időszakokat és kommunikációkat. Egy biztonsági esemény feltárásakor gyakran sok időt vesz igénybe a naplók összegyűjtése, az érintett rendszerek azonosítása és a különböző forrásokból származó adatok összevetése. Az EWS nem szünteti meg a helyi vizsgálat szükségességét, de célzottabbá teheti azt, mert az elemzők hamarabb meghatározhatják, mire kell koncentrálni.

A rendszer az NKI Nemzeti CSIRT felé történő incidensbejelentést is egyszerűbbé és megalapozottabbá teheti. Ha egy eseményhez már rendelkezésre állnak hálózati riasztások, forgalmi adatok, érintett IP-címek, időbélyegek, kommunikációs irányok vagy a megőrzési időn belül visszakereshető pcap-adatok, akkor az incidens leírása pontosabb lehet. Ez gyorsíthatja a bejelentés feldolgozását, az esemény besorolását és a további szakmai egyeztetést is.

Az érintett szervezetek számára további előny, hogy saját rendszereik működését hálózati nézőpontból is ellenőrizhetik. Az EWS-ből származó jelzések segíthetnek olyan kommunikációk azonosításában, amelyek a helyi üzemeltetésben nem mindig kapnak figyelmet, de biztonsági vagy üzemeltetési szempontból ellenőrzést igényelhetnek.

Ilyenek lehetnek például a rendszeresen visszatérő külső kapcsolatok, a váratlan forgalmi irányok, a szokatlan protokollhasználat vagy azok a forgalmi csúcsok, amelyek működési rendellenességre, hibás konfigurációra vagy nem megfelelően dokumentált rendszerkapcsolatra utalhatnak.

A központosított NIDS a megfelelési és biztonsági kontrollok erősítésében is szerepet kaphat. A GDPR szerinti adatbiztonsági elvárások és a NIS2-irányelvhez kapcsolódó kiberbiztonsági követelmények teljesítése nem pusztán dokumentációs kérdés: szükség van olyan technikai és szervezeti képességekre is, amelyek támogatják az események észlelését, vizsgálatát, nyomon követését és megfelelő kezelését. Az EWS ebben kiegészítő eszközként jelenik meg, mert hálózati monitoringból származó információkkal segíti az érintett szervezetek biztonsági kontrolljait és incidenskezelési folyamatait.

A rendszer egyik fontos előnye a folyamatosan aktualizált szabálykészlet. A támadási módszerek, kártevőkommunikációk és ismert indikátorok gyorsan változnak, ezért a detekciós képesség értéke nagymértékben függ attól, hogy a forgalom vizsgálata mennyire naprakész szabályok és észlelési logikák alapján történik. Az EWS központi működése lehetőséget ad arra, hogy az újonnan megjelenő fenyegetésekhez kapcsolódó szabályok és indikátorok gyorsan hasznosuljanak a védett rendszerek figyelésében.

Ugyancsak jelentős előny, hogy a felfedett trendek és indikátorok a rendelkezésre álló központi adatok alapján gyorsan visszaellenőrizhetők az érintett védett rendszereken. Ha egy rendszerben megjelenik egy gyanús domain, külső IP-cím, támadási minta vagy forgalmi anomália, akkor központi környezetben

ellenőrizhető, hogy az adott jelenség máshol is előfordult-e. Ez segít megkülönböztetni az elszigetelt eseményeket a szélesebb körű fenyegetésektől, és támogatja a gyorsabb, egységesebb védekezési intézkedéseket.

Az EWS haszna ezért nem egyetlen funkcióban ragadható meg. Az érintett szervezetek számára egyszerre ad többlet-rálátást a hálózati eseményeikre, támogatja a gyorsabb elsődleges értékelést, hatékonyabbá teheti az incidenskivizsgálást, pontosabb bejelentési alapot biztosíthat, naprakész detekciós támogatást nyújt, és lehetőséget ad az események központi összehasonlítására. Mindez, ahogy már volt róla szó, nem veszi át a helyi üzemeltetés és biztonsági felelősség szerepét. A központi monitoring értelmezési támogatást ad, de a tényleges helyzetfelméréshez és intézkedésekhez továbbra is szükség van az érintett szervezet helyi rendszerismeretére és döntéseire.

Korlátok és nehézségek

A központosított NIDS passzív eszköz. Ez nem hiányosság, hanem a rendszer működési sajátossága: nem avatkozik be közvetlenül a hálózati forgalomba, nem blokkol kapcsolatokat, és nem szakít meg támadási kísérleteket. Feladata az észlelés, a naplózás, a visszakereshetőség és az elemzési támogatás biztosítása.

A védett rendszerek üzleti, üzemeltetési és alkalmazásszintű összefüggéseit ismerő helyi szakértők tudása kell az EWS képességeinek kihasználásához. Ezért nem helyettesíti az érintett szervezetek saját védelmi eszközeit, biztonsági folyamatait és felelősségét. A helyi tűzfalak, végpontvédelmi rendszerek, naplógyűjtők, jogosultságkezelési folyamatok, sérülékenységkezelés és

incidenskezelési eljárások továbbra is nélkülözhetetlenek.

Fontos tudni, hogy a NIDS önmagában nem képes minden támadás vagy visszaélés felismerésére. Egyes események nem hagynak jól azonosítható hálózati nyomot, mások csak végponti naplók, alkalmazásnaplók, jogosultsági adatok vagy felhasználói tevékenységek alapján értelmezhetők. A titkosított, nem feloldott forgalom, az új vagy ritka támadási módszerek, a legitim csatornákat használó visszaélések, illetve a lassú, alacsony intenzitású adatmozgások különösen nehezíthetik az automatikus felismerést. A riasztás ezért nem maga az incidens, hanem vizsgálatot igénylő jelzés.

A rendszer hatékonyságát is több tényező együttesen határozza meg. Függ attól, hogy milyen forgalom kerül kitükrözésre, mekkora a feloldott adatok köre, milyen modulok állnak rendelkezésre, és mennyire frissek az IDS-szabálykészletek. Ugyanilyen fontos az érintett rendszerek biztonsági szakértőinek felkészültsége és terheltsége, mert a központi jelzések értelmezéséhez helyi rendszerismeretre is szükség van. Emellett a központi elemzői munka minősége, kapacitása és terhelhetősége is meghatározza, hogy a nagy mennyiségű hálózati adatból mennyire gyorsan és pontosan választhatók ki a valóban releváns események.

A központosított működés további feltétele az együttműködés. Az EWS akkor hasznosul megfelelően, ha az érintett szervezetek reagálnak a jelzésekre, visszajelzést adnak az események értékeléséről, és szükség esetén megosztják a helyi vizsgálathoz kapcsolódó információkat. Enélkül a központi rendszer csak riasztásokat és forgalmi adatokat biztosít, de az események teljes értelmezése, az okok feltárása és a tényleges intézkedések végrehajtása nehezebbé válik.

El kell fogadni, hogy ilyen mennyiségű hálózati forgalom vizsgálata már ipari szintű, jól támogatott eszközöket és tudatos fejlesztési tervezést igényel. A hálózati környezet folyamatosan változik: nő az adatforgalom, új protokollok és technológiák jelennek meg, a támadási módszerek alkalmazkodnak, az elemzői igények pedig bővülnek. Ezért a használt komponensek fejlesztése és karbantartása nem halogatható tartósan. Ahogy a technológiai alapok elavulnak, a rendszer fenntartása úgy válik egyre nehezebbé és drágábbá, miközben a detekciós és elemzői képesség pedig fokozatosan veszít az értékéből. Mindez jelentős anyagi ráfordítást és világos fejlesztési irányokat feltételez, amihez tiszta jövőképre van szükség.

Ezek a nehézségek nem a rendszer szükségtelenségét, hanem a szerepének pontos kijelölését indokolják. Az EWS akkor tud tartósan hasznos maradni, ha technológiai, szervezeti és ügyféloldali fejlesztései ezekre a működési feltételekre válaszolnak.

Merre tovább?

Az EWS fejlesztésének kulcskérdése, hogy a rendszer lépést tartson azzal a környezettel, amit támogatnia kell. A hálózati forgalom nő, a támadási módszerek változnak, az ügyféloldali igények bővülnek, a biztonsági elemzőknek pedig egyre gyorsabban kell értelmezhető választ adniuk arra, hogy egy jelzés valódi kockázatot jelent-e. Ehhez az EWS-nek nem statikus rendszerként, hanem folyamatosan fejleszthető, rugalmas központi monitoringképességként kell működnie.

Az első fontos irány a technológiai alapok megújítása. A NIDS, a csomagrögzítés, a forgalom-visszakeresés, az elemzői felületek és a

logmegjelenítés csak akkor maradnak hosszú távon használhatók, ha a rendszer képes a támogatott, naprakész és biztonságosan integrálható komponensverziók befogadására. A frissítések nem önmagukért fontosak: az újabb szabálycsomagok, protokolltámogatások, teljesítményjavítások és elemzői funkciók gyakran ezekre épülnek. Ha a keretrendszer elavul, akkor a karbantartás nehezebb, a fejlesztés drágább, a detekciós képesség pedig fokozatosan veszít az értékéből.

A technológiai megújításnak nemcsak verziókövetést kell jelentenie, hanem fenntartható üzemeltetési és fejlesztési keretet is. A használt komponenseknek illeszkednie kell egymáshoz, biztosítani kell a szabályfrissítések, naplófeldolgozási folyamatok, keresési funkciók és megjelenítési felületek működőképességét, valamint azt, hogy az elemzői igények ne csak egyedi megoldásokkal, hanem hosszabb távon is karbantartható módon jelenjenek meg a rendszerben.

A második irány a rugalmasság növelése. Megfelelő hálózati hozzáférés és engedélyezett adatkezelési keretek mellett a mobil vagy ideiglenesen telepíthető szenzorok olyan helyzetekben adhatnak többletet, amikor nem elég a már kiépített gerinchálózaton történő központi forgalomfigyelés. Fertőzött szervercsoportoknál, géptermi rendszereknél vagy incidens után alkalmasak lehetnek annak ellenőrzésére, hogy maradt-e gyanús kommunikáció, utal-e hálózati aktivitás tovább terjedésre, vagy sikeres volt-e a kárcsökkentés. Ugyanez a képesség alkalomszerű rendszer- és adatbiztonsági ellenőrzéseknél, fejlesztői teszteknél vagy üzemeltetési információgyűjtésnél is hasznos lehet. Egy jól elhelyezett ideiglenes szenzor sokszor gyorsabban mutatja meg a tényleges hálózati működést, mint a dokumentációk vagy a feltételezések.

A harmadik fejlesztési terület az ügyféloldali hasznosítás. Az EWS-ből származó jelzések akkor érnek igazán sokat, ha nem külön szigetrendszerben maradnak, hanem beépülnek az érintett szervezetek saját biztonsági munkafolyamataiba. Ennek egyik gyakorlati útja az elterjedt SIEM-rendszerek felé kialakított API-kapcsolat, amelyen keresztül a releváns, jogosultság szerint átadható logok és riasztások beépíthetők az ügyfél saját biztonsági folyamataiba. Így az ügyfél a saját naplóival, végponti adataival és incidenskezelési eljárásaival együtt tudja értelmezni a központi monitoringból érkező jelzéseket.

Szintén fontos a szabálycsomagok és események kezelésének egységesítése és priorizálása. Egy központi NIDS sok riasztást termelhet, ezek értéke azonban csak akkor jelenik meg, ha az elemzők gyorsan el tudják választani a lényeges eseményeket a zajtól. Ehhez jobb priorizálásra, áttekinthetőbb eseménykezelésre, egységesebb leírásokra és könnyebben karbantartható szabálykezelésre van szükség. A cél nem az, hogy több adat keletkezzen, hanem az, hogy a meglévő adatokból gyorsabban lehessen döntés-előkészítésre alkalmas információt nyerni.

A tudásmegosztás legalább ennyire fontos fejlesztési irány. Egy közös szakmai tudásbázis és kommunikációs felület alkalmas lehet a tapasztalatok, jó gyakorlatok, SOC-leírások és CTI-elemzéseket támogató adatbázisok megosztására. Végeredményben ez az, amivel a központi monitoring mindig többet tud nyújtani, hiszen a védett rendszerek sokszor hasonló fenyegetésekkel találkoznak. Amit az egyik szervezet vagy elemzői csapat már feldolgozott, az másoknál is lerövidítheti a vizsgálatot, javíthatja a reakcióidőt, és egységesebb szakmai értelmezést adhat.

A fejlesztéseknek az elemzői képességet is érinteniük kell. A központi monitoring értéke nemcsak a technológián múlik, hanem azon is, hogy van-e elegendő szakértői kapacitás a riasztások értékelésére, a trendek felismerésére, a szabályok karbantartására és az ügyféloldali visszajelzések feldolgozására. A rendszer akkor tud valódi támogatást adni, ha a technológiai működéshez megfelelő elemzői folyamatok, szakmai felelősségek és együttműködési csatornák kapcsolódnak.

Végül a technológiát csak akkor lehet jól használni, ha a szakemberek is vele együtt fejlődnek. Az érintett biztonsági szakértők, SOC-elemzők és üzemeltetők számára nem elég az elméleti ismeret: gyakorlati példákra, közös elemzésekre, visszajelzésekre és esettanulmányokra is szükség van. Az EWS akkor válik igazán hasznossá, ha a központi jelzések és a helyi rendszerismeret találkoznak.

A fejlesztés végső célja ezért nem pusztán egy korszerűbb technikai rendszer, hanem egy jobban használható, jobban érthető és gyorsabban reagáló közös védelmi képesség. Az EWS vagy bármilyen központosított hálózati monitoring akkor éri meg hosszú távon a fenntartást és megújítást, ha nem önálló, elszigetelt technikai rendszerként használjuk.

Zárszó

A központosított NIDS nem önálló, minden más védelmi képességet kiváltó biztonsági rendszer, hanem kiegészítő hálózati monitoringeszköz. Passzív módon többlet-rálátást ad a védett rendszerek kommunikációjára, támogatja a gyorsabb észlelést, a pontosabb elemzést és biztosítja az utólagos visszakereshetőséget.

Az EWS a hálózati forgalomból származó riasztásokkal, netflow-adatokkal és pcap-alapú visszakereséssel olyan technikai hátteret biztosít, amely segítheti a SOC-, CSIRT-, CTI- és üzemeltetési feladatokat. A rendszer önmagában nem dönt egy esemény súlyosságáról, de fontos támpontokat adhat incidensek, rendellenességek, adatszivárgási gyanúk, rendszertesztek vagy visszaélésgyanús helyzetek vizsgálatához.

A központi működés legnagyobb előnye, hogy az egyes események nem elszigetelten, hanem több védett rendszer tapasztalataival összevetve értelmezhetők. Ez gyorsabb felismerést, megalapozottabb döntés-előkészítést és hatékonyabb együttműködést tesz lehetővé.

Az EWS hosszú távú haszna attól függ, hogy technológiailag naprakész marad-e, képes-e alkalmazkodni az ügyféloldali igényekhez, és kapcsolódik-e hozzá megfelelő elemzői kapacitás, tudásmegosztás és szakmai együttműködés. Ebben az esetben nem csupán egy technikai szolgáltatásként, hanem a kormányzati kiberbiztonság fontos támogató képességeként működhet.

Források

Arkime Project. (é. n.) *Arkime.* https://arkime.com/ (Letöltve: 2026.05.20.)

Arkime Project. (é. n.) *Arkime GitHub Repository.* https://github.com/arkime/arkime (Letöltve: 2026.05.20.)

CCN-CERT. (2013) *La seguridad en las TICs en las Administraciones Públicas.* https://administracionelectronica.gob.es/pae_Home/dam/jcr%3A2ad6c044-eee7-44b4-b241-7e92b8c7bace/2013-12_Nota_Tecnica_CCN.pdf (Letöltve: 2026.05.20.)

CCN-CERT. (2016) *Servicios proporcionados por el CCN-CERT.* https://www.burgos.es/sites/default/files/file/destacado/2._ccn-cert_servicios_proporcionados.pdf (Letöltve: 2026.05.20.)

CISA. (2019) *National Cybersecurity Protection System (NCPS) Intrusion Detection Capabilities – Privacy Impact Assessment.* https://www.cisa.gov/sites/default/files/publications/ncps-intrusiondetection-pia-092019.pdf (Letöltve: 2026.05.20.)

CISA. (2020) *Federal Agency Compromised by Malicious Cyber Actor.* https://www.cisa.gov/news-events/analysis-reports/ar20-268a (Letöltve: 2026.05.20.)

CISA. (é. n.) *CISA Artificial Intelligence Use Cases.* https://www.cisa.gov/ai/cisa-use-cases (Letöltve: 2026.05.20.)

Club de Innovación. (2024) *¿Aún no conoces el Sistema de Alerta Temprana (SAT) del CCN-CERT?* https://www.clubdeinnovacion.es/au-sistema-alerta-temprana-sat-del-ccn-cert/ (Letöltve: 2026.05.20.)

Elastic. (é. n.) *Anomaly detection with machine learning.* https://www.elastic.co/docs/explore-analyze/machine-learning/anomaly-detection (Letöltve: 2026.05.20.)

Elastic. (é. n.) *Kibana Guide.* https://www.elastic.co/guide/en/kibana/index.html (Letöltve: 2026.05.20.)

Elastic. (é. n.) *Kibana: Discover, visualize, and analyze with AI.* https://www.elastic.co/kibana (Letöltve: 2026.05.20.)

Elastic. (é. n.) *Machine learning in Kibana.* https://www.elastic.co/docs/explore-analyze/machine-learning/machine-learning-in-kibana (Letöltve: 2026.05.20.)

ENISA. (2020) *How to setup CSIRT and SOC.* https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc (Letöltve: 2026.05.20.)

ENISA. (é. n.) *Glossary of Terms.* https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary (Letöltve: 2026.05.20.)

Európai Bizottság. (2013) *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2013:1:FIN (Letöltve: 2026.05.20.)

Európai Bizottság. (2014) *Közigazgatás- és Közszolgáltatás-fejlesztési Operatív Program – Hungary 2014–2020.* https://ec.europa.eu/regional_policy/in-your-country/programmes/2014-2020/hu/2014hu05m3op001_hu (Letöltve: 2026.05.20.)

Európai Parlament és Tanács. (2016) *Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról.* https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=hu (Letöltve: 2026.05.20.)

Európai Parlament és Tanács. (2016) *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.* https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32016L1148 (Letöltve: 2026.05.20.)

Európai Parlament és Tanács. (2022) *Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről.* https://data.europa.eu/eli/dir/2022/2555/oj?locale=hu (Letöltve: 2026.05.20.)

Federal News Network. (2023) *CISA lays out post-EINSTEIN future with shift to "Cyber Analytics and Data System".* https://federalnewsnetwork.com/cybersecurity/2023/03/cisa-lays-out-post-einstein-future-with-shift-to-cyber-analytics-and-data-system/ (Letöltve: 2026.05.20.)

FedScoop. (2023) *CISA considering the future state of EINSTEIN as agencies modernize.* https://fedscoop.com/cisa-considers-the-future-state-of-einstein-as-agencies-modernize/ (Letöltve: 2026.05.20.)

FIRST. (é. n.) *About FIRST*. https://www.first.org/about/ (Letöltve: 2026.05.20.)

Junta de Andalucía. (2023) *Pliego de prescripciones técnicas – Plataforma de monitorización para apoyo al Centro de Operaciones de Seguridad de la Junta de Andalucía / AndalucíaCERT.* https://www.juntadeandalucia.es/haciendayadministracionpublica/apl/pdc_sirec_documentacion/rest/descargar/documento/165444 (Letöltve: 2026.05.20.)

Pihelgas, Mauno; Kont, Markus. (2021) *Frankenstack: Real-time Cyberattack Detection and Feedback System for Technical Cyber Exercises.* https://ccdcoe.org/uploads/2021/11/Pihelgas_Kont_Frankenstack_v2.pdf (Letöltve: 2026.05.20.)

Nemzetbiztonsági Szakszolgálat. (é. n.) *KÖFOP-2.2.2-VEKOP-16-2016-00001 projekt bemutatása.* https://nbsz.gov.hu/gazdalkodas/palyazatok/kofop (Letöltve: 2026.05.20.)

Nemzeti Jogszabálytár. (2017) *467/2017. (XII. 28.) Korm. rendelet a Kormányzati Adatközpont működéséről.* https://net.jogtar.hu/jogszabaly?docid=a1700467.kor (Letöltve: 2026.05.17.)

Nemzeti Jogszabálytár. (2020) *214/2020. (V. 18.) Korm. rendelet az elektronikus információbiztonsági korai figyelmeztető rendszerről.* https://njt.hu/jogszabaly/2020-214-20-22 (Letöltve: 2026.05.20.)

Nemzeti Jogszabálytár. (2020) *A 214/2020. (V. 18.) Korm. rendelet indokolása az elektronikus információbiztonsági korai figyelmeztető rendszerről.* https://njt.jog.gov.hu/jogszabaly/2020-214-K3-22 (Letöltve: 2026.05.20.)

Nemzeti Kiberbiztonsági Intézet. (2020) *Hatályba lépett a korai figyelmeztető rendszerről szóló kormányrendelet.* https://nki.gov.hu/it-biztonsag/hirek/ews-csatlakozas/ (Letöltve: 2026.05.20.)

Nemzeti Kiberbiztonsági Intézet. (2022) *Projekt eredményeit bemutató kiadvány – KÖFOP-2.2.2-VEKOP-16-2016-00001.* https://nki.gov.hu/wp-content/uploads/2022/01/Osszefoglalo_kiadvany.pdf (Letöltve: 2026.05.20.)

Nemzeti Kiberbiztonsági Intézet. (é. n.) *Incidenskezelés*. https://nki.gov.hu/szolgaltatasok/tartalom/incidenskezeles/ (Letöltve: 2026.05.20.)

NISZ Zrt. (é. n.) *Nemzeti Távközlési Gerinchálózat (NTG) fejlesztése.* https://nisz.hu/projektjeink/nemzeti-tavkozlesi-gerinchalozat-ntg-fejlesztese-d21 (Letöltve: 2026.05.20.)

CTI elemzés NEMZETI KIBERBIZTONSÁGI INTÉZET

Open Information Security Foundation / SURICATA. (é. n.) *Suricata*. https://suricata.io/ (Letöltve: 2026.05.20.)

U.S. Government Accountability Office. (2020) *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*. https://www.gao.gov/products/gao-20-598 (Letöltve: 2026.05.20.)

U.S. Government Accountability Office. (2025) *Cybersecurity: Network Monitoring Program Needs Further Guidance and Actions*. https://files.gao.gov/reports/GAO-25-107470/index.html (Letöltve: 2026.05.20.)

CTI elemzés
NEMZETI KIBERBIZTONSÁGI INTÉZET

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

Kibertámadás!
podcast

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet

titkarsag@nki.gov.hu

nki.gov.hu

+36 (1) 325 7672

2026