

Milyen naplózási tevékenységeket és eljárásokat kell egy NIS2 kötelezett szervezetnek alkalmaznia ahhoz, hogy az incidenseket időben észlelje, kivizsgálja és bejelentse?

VFP3 KiberVéd - NIS2 Audit felkészítés szakmai
állásfoglalás 2026/49

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
0.9	2026.07.23	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A kiberbiztonsági törvény és a 7/2024. MK rendelet a naplózást nem öncélú adatgyűjtésként, hanem a kiberbiztonsági incidensek észlelésének, kivizsgálásának és bejelentésének alapjaként határozza meg. Az MK rendelet 2. mellékletének 4. követelménycsaládja (Naplózás és elszámoltathatóság) előírja, hogy a szervezetnek a biztonsági osztály (Alap, Jelentős, Magas) szintjétől függően kell meghatároznia a naplózandó eseményeket, valamint gondoskodnia a naplóbejegyzések gyűjtéséről, védelméről és rendszeres felülvizsgálatáról.

A vezetés közvetlen felelőssége, hogy incidens bekövetkezésekor a szervezet gyorsan és hatékonyan reagáljon, továbbá, hogy a kiberbiztonsági incidenseket határidőben jelentse a releváns hatóságok, ügyfelek, beszállítók felé. E kötelezettségek csak működő naplózási és incidensértékelési képességgel teljesíthetők, mert a bejelentések tartalmi alapját a naplókból felépített idővonal adja.

A naplózás akkor működik megfelelően, ha a szervezet dokumentált kezelési eljárásokat (runbook), felelősségi mátrixot és kockázatalapú naplóforrás-prioritást működtet.

2. A VIZSGÁLANDÓ KÉRDÉS

Adott egy NIS2 kötelezett szervezet, amely elektronikus információs rendszereit (EIR) biztonsági osztályba sorolta. Milyen naplózási kötelezettségek vonatkoznak rá, és mit kell naplóznia ahhoz, hogy a biztonsági események felismerhetők, kivizsgálhatók és bizonyíthatók legyenek, valamint a bejelentési határidők tarthatók maradjanak?

3. VÁLASZ

3.1 A naplózási kötelezettség jogszabályi alapja

A NIS2 irányelvet a 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) a szervezet vezetőjének felelősségi körébe utalja az incidensekre való reagálási képesség kialakítását:

A szervezet vezetője az elektronikus információs rendszer védelmének biztosítása érdekében az elektronikus információs rendszert érintő kiberfenyegetés, kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a gyors és hatékony reagálásról, az illetékes kiberbiztonsági incidenskezelő központnak való bejelentésről, a kiberbiztonsági incidensek kezeléséről, valamint a helyreállításról; [2024. évi LXIX. törvény 6. § (5) bekezdés e) pont]

A gyors és hatékony reagálás, valamint a bejelentés előfeltétele, hogy az incidens egyáltalán észlelhető és rekonstruálható legyen – ezt biztosítja a naplózás. A konkrét naplózási követelményeket a 7/2024. (VI. 24.) MK rendelet 2. mellékletének 4. követelménycsaládja (Naplózás és elszámoltathatóság) tartalmazza, a biztonsági osztálytól függő kötelezettségi

szinttel. A szervezetnek ennek keretében naplózási eljárásrendet kell kialakítania, meg kell határozni a naplózandó eseményeket, gondoskodnia kell a naplóbejegyzések gyűjtéséről, sértetlenségük védelméről és megőrzésükről, valamint a naplók rendszeres felülvizsgálatáról és elemzéséről.

Fontos: a naplózás nem attól felel meg, hogy sok adat gyűlik, hanem attól, hogy a szervezet dokumentáltan tudja, **mit** figyel, **miért** figyel, **ki** reagál rá, és **milyen bizonyíték** marad utána.

3.2 Mit javasolt naplózni, és mit nem célszerű?

A gyakorlatban az alábbi eseménykörök naplózása adja az incidenskezelés alapját:

Eseménykör	Naplózandó események	Miért fontos?
Adatbázis-módosítások	Bármilyen módosítás vagy módosítási kísérlet – ideértve az Active Directoryt is: létrehozás, változtatás, törlés, séma- és konfigurációváltozás.	Ki, mikor és mit változtatott; a jogosulatlan módosítás visszakövethető és visszaállítható.
Biztonsági események	Sikeres és sikertelen bejelentkezések, jogosultságmódosítások, jelszóváltoztatások, hozzáférési kísérletek.	A fiókkompromittálás és a jogosultsággal való visszaélés felismerhető, a belépési lánc rekonstruálható.
Üzleti tranzakciók (auditnaplók)	Pénzügyi tranzakciók, megrendelések státuszváltozásai, üzletileg jelentős műveletek.	Az üzleti folyamat sértetlensége igazolható, a visszaélés tételesen kimutatható.
Rendszerállapot és hibák	Nem várt kivételek, összeomlások, időtúllépések, kritikus erőforrások telítettsége.	A szolgáltatáskiesés oka megállapítható; a szándékos túlterhelés elkülöníthető a műszaki hibától.
Rendszerspecifikus naplózás	Az adott EIR fejlesztői vagy üzleti igényeit kielégítő naplózás.	Speciális vizsgálati igények kiszolgálása.

Kerülendő naplózni a következőket:

Kerülendő	Indok és helyes gyakorlat
Jelszavak, PIN-kódok, munkamenet-azonosítók, API- és titkosítási kulcsok olvasható formában.	A napló maga válik betörési célponttá. Ha a rögzítés technikailag elkerülhetetlen, az értéket maszkolni vagy hash-elni kell.
Bankkártyaadatok (teljes kártyaszám, CVC) és különleges személyes adatok, például egészségügyi adat.	Külön jogi és szabványkövetelmények alá esnek. A tranzakció ténye és azonosítója naplózandó, az érzékeny mező tartalma nem.
Üzenetek, dokumentumok és kommunikáció teljes tartalma, billentyűleütések rögzítése.	A biztonsági célhoz a metaadat (ki, mikor, mihez fért hozzá) általában elegendő; a tartalomrögzítés a 12. fejezet adatvédelmi védősávjaiba ütközik.
Tartós debug- vagy fejlesztői szintű naplózás éles környezetben.	Elfedi a valóban fontos eseményeket, feleslegesen emészt a tárhelyet, és gyakran érzékeny adatot is kiír. Hibakereséskor ideiglenesen, célzottan kapcsolható be.

Nem célszerű naplózni normál* esetben a változást nem okozó felhasználói bevitelt és navigációt (zajt termel), a jelszavakat, PIN-kódokat és kulcsokat (a napló maga válna kockázattá), a magánüzeneteket és billentyűleütéseket (adatvédelmi kockázat), valamint tartós debug szintű naplózást éles környezetben (érzékeny adatot írhat ki).

* Speciális esetben – például SQL injection típusú támadásnál – akár egy keresési mező bevitelét is naplózni kell, hogy megállapítható legyen, ki és mikor kísérelte meg a támadást.

3.3 A naplóbejegyzéstől az incidensig

A naplóbejegyzésből nem automatikusan lesz incidens elemzés, hanem értékelési lépcsőkön keresztül. A naplóbejegyzés technikai rekord; eseménnyé akkor válik, ha értelmezhető működési vagy biztonsági jelentése van. Riasztás akkor keletkezik, ha az esemény megfelel egy előre meghatározott szabálynak. Biztonsági eseménynek minősül, ha az esemény biztonsági szempontból releváns. Incidens akkor keletkezik, ha az értékelés alapján jogosulatlan hozzáférés, adatsérülés, szolgáltatászavar vagy védelmi kontroll kiesése történt, vagy ezek valószínűsíthetők.



1. ábra – Működési ciklus: naplóból kezelhető incidens

Minden riasztási területnél négy kérdésre kell előre, dokumentáltan választ adni:

- **Mit figyel?** Pontosan paraméterezett riasztási feltétel (például 5 sikertelen belépés 10 percen belül ugyanarra a fiókra).
- **Miért figyel?** A szabály mögötti kockázati indok, amely a célhoz kötöttséget auditon és adatvédelmi szempontból is igazolja.
- **Ki reagál rá?** Első reagáló szerepkör, bevonandó területek, eskalációs út – runbookban és RACI-mátrixban rögzítve.
- **Milyen bizonyíték marad?** Az eredeti naplóbejegyzések védett, változatlan formában, a döntésnapló idővonallal, az incidensjegy és a tanulságok.

Amennyiben bármilyen válasz hiányzik, a naplózás csak adatgyűjtés marad, nem biztosít tényleges incidenskezelési képességet.

3.4 Kapcsolódás a bejelentési kötelezettséghez

Amennyiben az értékelés eredménye incidens, és az súlyos működési zavart vagy pénzügyi veszteséget okozott, illetve más természetes vagy jogi személynek jelentős kárt okozhat, azon szervezetek számára, melyek felelős hatósága az NKI a Kiberbiztonsági tv. 66. §-a és a 418/2024. (XII. 23.) Korm. rendelet 77. §-a szerinti bejelentési határidők azonnal elindulnak. A bejelentések tartalmi alapját a naplóból felépített idővonal adja, ezért azt a vizsgálat közben kell vezetni, nem utólag összeállítani.

Lépcső	Határidő	Tartalmi alap a naplózásból
Korai előrejelzés (első)	A tudomásszerzéstől	Az első értékelés; feltételezhető-e rosszindulatú

Lépcső	Határidő	Tartalmi alap a naplózásból
bejelentés)	számított 24 órán belül.	cselekmény, lehet-e határokon átnyúló hatás.
Incidensbejelentés (eseménybejelentés)	A tudomásszerzéstől számított 72 órán belül.	A súlyosság és a hatás első értékelése, a már ismert fertőzőttségi mutatók (IoC).
Közbenső helyzetjelentés	A hatóság vagy az incidenskezelő központ kérésére.	A döntésnapló aktuális állapota, a folyamatban lévő intézkedések.
Zárójelentés	Az incidens kezelését követő egy hónapon belül.	Részletes leírás, valószínű kiváltó ok, mérséklő intézkedések, határokon átnyúló hatás.

3.5 Külső szolgáltatói és felhőalapú naplók

A törvény a közreműködők igénybevétele esetére is a szervezet vezetőjének felelősségévé teszi a követelmények érvényesítését:

ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, illetve a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenység ellátásához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek; [2024. évi LXIX. törvény 6. § (5) bekezdés d) pont]

Ennek megfelelően a naplózásra és a naplóátadásra vonatkozó elvárásokat szerződéses kötelemként kell a közreműködőre terhelni. A hazai szabályozás megkülönbözteti az eseti közreműködőt (fejlesztő, auditor, hibaelhárító) és a kihelyezett, irányított szolgáltatót (MSP, MSSP, tartós IaaS/PaaS-üzemeltető), amely állandó, jellemzően adminisztrátori szintű távoli hozzáféréssel dolgozik. Ez utóbbi az ellátási lánc egyik legérzékenyebb pontja, ezért a szolgáltatói fiókok tevékenységét a megbízó oldalán is naplózni kell; nem elegendő a partner saját nyilvántartására hagyatkozni.

Felhőszolgáltatás igénybevételekor szerződésben javasolt rögzíteni, hogy a szervezet milyen naplóeseményeket lát, mennyi ideig kérhetők vissza, milyen gyorsan és milyen formátumban adja át azokat a szolgáltató incidens esetén, valamint, hogy a naplók beköthetők-e a szervezet központi naplógyűjtőjébe.

3.6 Adatvédelmi korlátok

A biztonsági célú naplózást el kell határolni a munkavállalók általános ellenőrzésétől. A naplóadatokhoz való hozzáférés célhoz kötött és dokumentált legyen: minden riasztási használati esethez tartozzon biztonsági cél és kockázati indok, naplóadatot csak kijelölt szerepkör lásson, részletes vizsgálat csak dokumentált esemény vagy incidensgyanú esetén induljon, a megőrzési idők pedig kockázati és jogi szempontok szerint legyenek meghatározva. A felhasználói tájékoztatásból derüljön ki, milyen célból történhet biztonsági naplózás és vizsgálat.

3.7 Gyakorlati megvalósítás

A fenti kötelezettségek működő képességgé alakítását a jelen állásfoglalás melléklete, a „Naplózás – az incidenskezelés alapja” keretdokumentum támogatja. A melléklet tartalmazza a naplóforrások kockázatalapú prioritási modelljét, a riasztási használatieset-sablont és kezdő backlogot, a RACI-felelősségi mátrixot, az incidensvizsgálati munkalapot, a 90 napos bevezetési ütemtervet, valamint a kitölthető ellenőrzőlistákat és adatlapokat.

4. A HÁROM ALAPKÉRDÉS ÉS AZ ADMINISZTRÁCIÓ: MIT, MIÉRT, KI?

Minden lépcső akkor tekinthető rendben lévőnek, ha négy kérdésre előre, dokumentáltan megvan a válasz. Ha bármelyik hiányzik, a naplózás csak adatgyűjtés marad, nem incidenskezelési képesség.

1. Mit figyel? A figyelt eseménykört rögzíteni kell: mely EIR, mely naplóforrás, milyen esemény vagy mintázat. Nem elég annyit mondani, hogy „figyeljük a belépéseket”; azt kell rögzíteni, hogy **pontosan** mi váltson ki riasztást (például 5 sikertelen belépési kísérlet 10 percen belül ugyanarra a fiókra). A paraméterezés kulcsfontosságú: hány sikertelen kísérlet, mennyi időn belül, melyik fiókra? Enélkül akár az is riasztást válthat ki, ha a rendszer felhasználói együttesen egy év alatt öt alkalommal gépelik el a jelszavukat. A „mit” kérdésre adott válasz a use case backlogban és a riasztásiszabály-adatlapon jelenjen meg (lásd a Fogalmak fejezetet).

2. Miért figyel? Minden szabály mögött kockázati indoknak kell állnia: milyen visszaélést, támadást vagy hibát akarunk időben észrevenni, és mi történne, ha nem vennénk észre. Az indok nélküli szabály előbb-utóbb zajforrássá válik; az indokolt szabály viszont adatvédelmi szempontból és auditon is védhető, mert igazolja a célhoz kötöttséget. A „miért” kérdésre adott válasz szintén a use case backlogban és a riasztásiszabály-adatlapon jelenjen meg.

3. Ki reagál rá? Riasztásonként ki kell jelölni az első reagáló szerepkört, a bevonandó területeket és az eskalációs utat. Az első értékelést jellemzően az ügyeletes incidenskezelő vagy a vizsgálatra kijelölt szakember végzi a runbook kérdései mentén. A továbblépésnél az IT-biztonság, az EIR-felelős vagy a rendszerhez tartozó fejlesztő lép be, speciális esetekben az adatvédelem és a szolgáltatói kapcsolattartó. Aminek nincs gazdája, arra senki nem fog reagálni, vagy a reakció a hiányos forgatókönyv miatt elhúzódik. A felelősséget a RACI-mátrixban és a runbookban kell rögzíteni.

4. Adminisztráció, avagy a bizonyíték. Az esemény lezárása után visszakereshető nyomnak kell maradnia: az eredeti naplóbejegyzések védett, változatlan formában, a riasztás és annak minősítése, a döntésnapló az idővonallal, az incidensjegy, valamint a lezárást követően a tanulság és az intézkedés. Az adminisztráció és a bizonyíték nem melléktermék, hanem a folyamat része: audit során igazolhatóvá, jogi eljárásban felhasználhatóvá teszi a szervezet működését, és ebből tanul a következő szabályhangolás is.

5. NAPLÓINFORMÁCIÓBÓL -> INCIDENS

1. Naplóbejegyzés

A naplóbejegyzés önmagában csak technikai rekord. Például:

2026-07-03 08:42:11 - User: gombóc.artúr - Login failed - Source IP: 185.x.x.x

Ez önmagában még nem incidensről szól; csak azt jelzi, hogy volt egy történés.

2. Esemény

A naplóbejegyzés akkor mutat vizsgálendő eseményt, ha értelmezhető működési vagy biztonsági jelentése van. Példák:

Naplóbejegyzés	Esemény
1 sikertelen belépés	Hibás jelszópróba.
5 sikertelen belépés	Lehetséges brute force próbálkozás.
Admin jogosultság változott	Jogosultságmódosítás történt.
Tűzfal tiltott kapcsolatot	Külső kapcsolat blokkolva lett.
SIEM-ügynök leállt	A naplógyűjtés kieshetett.

3. Riasztás

Riasztás akkor keletkezik, ha az esemény megfelel egy előre beállított szabálynak. Például: ha 10 percen belül 5 sikertelen belépés történik ugyanarra a felhasználóra, riasztás keletkezik. Ez már figyelmet igényel, de még mindig nem biztos, hogy incidens.

4. Biztonsági esemény

Biztonsági eseményről akkor beszélünk, ha az esemény biztonsági szempontból releváns. Példák:

Esemény	Biztonsági esemény?	Miért?
Egyszeri rossz jelszó	Nem feltétlenül	Lehet egyszerű felhasználói hiba.
Sok rossz jelszó rövid idő alatt	Igen	Támadási kísérlet lehet.
Admin jog adása	Igen	Jogosultsági kockázat.
Sikertelen mentés (backup)	Igen	Helyreállíthatósági kockázat.
A SIEM nem kap naplót	Igen	Az észlelési képesség sérülhet.
Sikeres belépés külföldről, szokatlan időben	Igen	Gyanús hozzáférés lehet.

5. Incidens

A biztonsági eseményből akkor lesz incidens, ha az értékelés alapján legalább az egyik feltétel teljesül:

- jogosulatlan hozzáférés történt vagy valószínűsíthető;
- adat sérült, kiszivárgott, módosult vagy elérhetetlenné vált;
- szolgáltatás vagy rendszer működése sérült;
- védelmi kontroll kiesett vagy megkerülésre került;
- a kockázat meghaladja az előre meghatározott incidensküszöböt;
- több naplóbejegyzés együtt támadási mintát mutat.

A naplóbejegyzésből tehát nem automatikusan lesz incidens, hanem az elemzés és a besorolás alapján. Ha az incidens jelentősnek minősül, a 10.3 pont szerinti bejelentési határidők azonnal indulnak.

Példa egyszerű folyamatra

Kiinduló naplóbejegyzések:

08:01 - Login failed - user: admin - source: 45.x.x.x
 08:02 - Login failed - user: admin - source: 45.x.x.x
 08:03 - Login failed - user: admin - source: 45.x.x.x
 08:04 - Login failed - user: admin - source: 45.x.x.x
 08:05 - Login success - user: admin - source: 45.x.x.x
 08:07 - User added to Domain Admins

Értékelés:

Lépés	Minősítés
Több sikertelen belépés	Biztonsági esemény.
Ezt követő sikeres admin belépés	Gyanús hozzáférés.
Admin csoport módosítása	Kritikus biztonsági esemény.
A jogosulatlanság nem zárható ki	Incidens.

6. MUNKAFOLYAMATOK

A naplózási képességet több párhuzamos munkafolyamatban célszerű kialakítani. Így nem egyetlen technikai projektté válik, hanem szabályozási, üzemeltetési, incidenskezelési és adatvédelmi szempontból is kezelhető marad.

Folyamat	Cél	Fő kimenet	Tipikus résztvevők
WS-1 EIR- és naplóforrás-leltár	A releváns rendszerek és naplóforrások azonosítása.	Naplóforrás-leltár és hiánylista.	EIR-felelős, IT-üzemeltetés, információbiztonság.
WS-2 Riasztási használati esetek	A figyelendő kockázati történetek és a riasztási logika rögzítése.	Use case backlog és szabálykártyák.	Információbiztonság, incidenskezelő, IT.
WS-3 Hozzáférés és adatvédelmi védősáv	A naplóadatokhoz való hozzáférés és a betekintési korlátok meghatározása.	Hozzáférési mátrix és adatvédelmi kontrollpontok.	Adatvédelmi szakértő, információbiztonság, vezetés.
WS-4 Riasztás- és jegykezelés	A riasztások kezelhető folyamatba terelése.	Runbook, értesítési rend, incidensjegy-sablon.	Incidenskezelő, SOC vagy üzemeltetés.
WS-5 Tesztelés és bizonyíték	Annak igazolása, hogy a folyamat eseménytől intézkedésig működik.	Tesztjegyzőkönyv, idővonal, intézkedési terv.	Információbiztonság, IT, auditor.

6.1 katalógus

Dokumentumok	Mire való?	Frissítés gyakorisága
Naplóforrás-leltár	Megmutatja, mely rendszerekből milyen napló érkezik vagy hiányzik.	Új EIR, nagyobb változás vagy legalább negyedéves ellenőrzés.
Use case backlog	A tervezett, működő és visszavont riasztási logikák nyilvántartása.	Folyamatos, de legalább havi áttekintés.

Dokumentumok	Mire való?	Frissítés gyakorisága
Runbook-katalógus	Rövid vizsgálati és reagálási lépések gyűjteménye.	Riasztási szabály változásakor.
Hozzáférési mátrix	Kimutatja, ki férhet hozzá a naplóadatokhoz és milyen célból.	Jogosultságváltozáskor vagy legalább negyedévente.
Tesztjegyzőkönyv	Bizonyítja, hogy a riasztási, jegykezelési és vizsgálati folyamat működik.	Élesítés előtt és időszakos kontrollként.
Tanulmánylista	A lezárt incidensekből és a téves riasztásokból származó fejlesztések.	Minden lezárt, jelentősebb esemény után.

7. NAPLÓFORRÁS-PRIORITÁSI MODELL

A naplóforrásokat nem egyszerre, hanem kockázati alapon célszerű bekötni. A pontozás célja, hogy a szervezet ne a könnyen elérhető naplókval kezdje, hanem azokkal, amelyek a legtöbbet segítenek egy incidens felismerésében és rekonstrukálásában.

Szempont	1 pont	3 pont	5 pont
Üzleti kritikalitás	Támogató rendszer.	Fontos, de részben kiváltható.	Kritikus üzleti vagy alaptevékenységi rendszer.
Adatérzékenység	Kevés vagy nyilvános adat.	Belső használatú üzleti adat.	Személyes, bizalmas vagy kritikus adat.
Incidensrekonstrukciós érték	Kevés vizsgálati információt ad.	Egy teljes rendszerről összefogó képet ad..	Több rendszert összekötő bizonyító értéke van.
Fenyegetettség	Ritkán támadott, zárt környezet.	Belső hálózatról elérhető vagy sok felhasználót érint.	Internet felől, távolról elérhető vagy magas jogosultsággal érintett.
Bekötési nehézség	Nehéz- időigényes	Közepes fejlesztési vagy szolgáltatói feladat.	Könnyű bekötni.

A megkapott pontszám alapján érdemes a legtöbb pontszámot kapottal kezdeni a naplózási képesség kialakítását.

8. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.);
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről;
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról;
- az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS2 irányelv);
- Naplózás – az incidenskezelés alapja. Keret és megvalósítási sablon, v1.0 (melléklet);

9. FOGALMAK

Zaj (riasztási zaj): minden olyan riasztás vagy naplőesemény, amely a beállított szabály feltételeinek megfelel, de mögötte nincs valós biztonsági kockázat. Tipikus forrásai: ismert és jóváhagyott karbantartás, jogszerű változtatás (például tervezett jogosultságmódosítás), tesztelés, automatizmusok és ütemezett feladatok működése, felhasználói hiba (például elgépelte jelszó), valamint a túl érzékenyre hangolt riasztási szabály. A zaj nem ártalmatlan melléktermék: fárasztja az ügyeletet, elfedi a valódi támadást, és rontja a riasztásokba vetett bizalmat. Ezért a zajt nem figyelmen kívül hagyni, hanem kezelni kell: a téves riasztás okát minden esetben rögzíteni kell, az ismétlődő zajforrást pedig szabályhangolással, kivétellistával vagy a küszöbértékek módosításával meg kell szüntetni. Egy riasztás zajnak minősítése triage-döntés, amelyet a döntésnaplóban dokumentálni kell – így a minősítés utólag felülvizsgálható, és a zajarány a riasztási szabályok hatékonyságának mérőszámaként is használható.

Use case backlog: a szervezet a naplőzási és biztonságfelügyeleti használati eseteket use case backlogban tartja nyilván. A backlog célja, hogy dokumentáltan rögzítse, mely elektronikus információs rendszerhez, naplóforráshoz, eseménytípushoz vagy eseménymintázathoz kapcsolódik figyelési vagy riasztási igény, és az adott figyelés milyen biztonsági vagy működési kockázat kezelését támogatja.

A use case backlog minden használati esetről tartalmazza legalább az érintett EIR megnevezését, a naplóforrást, a figyelt eseményt vagy mintázatot, a riasztási feltételt, a kockázati indokot, a kapcsolódó biztonsági követelményt, az érintett szerepköröket, a prioritást, az állapotot, a felülvizsgálat gyakoriságát, valamint a kapcsolódó riasztási szabály és kezelési eljárás azonosítóját.

A backlog biztosítja, hogy a szervezet ne általánosságban, hanem előre meghatározott és indokolt eseménykörök alapján végezze a naplőbejegyzések figyelését és elemzését. Ennek keretében minden használati esetről rögzítésre kerül, hogy az adott eseménytípus miért alkalmas biztonsági események azonosítására, utólagos kivizsgálásuk támogatására, illetve a nem megfelelő vagy szokatlan tevékenységek felismerésére.

Új használati eset élesítése előtt a szervezet ellenőrzi, hogy a figyelés célja, hatóköre, naplóforrása, riasztási feltétele, felelőse és kezelési módja dokumentált-e. A működő használati eseteket a szervezet meghatározott gyakorisággal, valamint releváns rendszer-, kockázati vagy incidensváltozás esetén felülvizsgálja. A felülvizsgálat eredménye alapján a használati eset változatlanul fenntartható, módosítható, felfüggeszthető vagy kivezethető.

A use case backlog nem az események kezelésének részletes lépésrendje, hanem a figyelési és riasztási igények nyilvántartása. A backlog azt igazolja, hogy a szervezet mit figyel, mely EIR-ben figyeli, milyen indok alapján figyeli, milyen feltétel esetén keletkezik riasztás, és mely dokumentált kezelési eljárás kapcsolódik hozzá.

Runbook: a szervezet a biztonsági események és riasztások egységes kezelése érdekében runbookokat alkalmaz. A runbook célja, hogy a kijelölt személyek vagy szerepkörök számára előre meghatározott, követhető és visszaellenőrizhető lépésrendet adjon a riasztások értékeléséhez, a biztonsági események kezeléséhez, az eskalációhoz, a dokumentáláshoz és a lezáráshoz.

A runbook rögzíti az adott riasztáshoz vagy eseménytípushoz kapcsolódó elsődleges ellenőrzési lépéseket, a vizsgálandó naplóforrásokat, a döntési pontokat, az incidenssé minősítés szempontjait, az értesítendő vagy bevonandó szerepköröket, az eskalációs feltételeket, valamint az elvégzendő válaszlépéseket. Kitér arra is, hogy milyen bizonyítékokat kell megőrizni, milyen jegyben vagy nyilvántartásban kell dokumentálni az esemény kezelését, és milyen információknak kell szerepelniük a döntésnaplóban.

A runbook alapján a riasztás első értékelése során meg kell állapítani, hogy az esemény téves riasztásnak, normál működésből eredő eseménynek, biztonsági eseménynek, incidensgyanúnak vagy incidensnek minősül-e. Amennyiben az esemény jogosulatlan hozzáférésre, adatbiztonsági sérülésre, szolgáltatáskiesésre, védelmi kontroll hibájára, sértetlenségi problémára vagy más biztonsági kockázatra utal, a kezelést a szervezet biztonsági eseménykezelési eljárásrendje szerint kell folytatni.

A runbook támogatja a biztonsági eseménykezelési képesség következetes működését, mert ugyanazon típusú riasztások esetén az értékelés, az eskaláció, az intézkedés és a dokumentálás egységes módon történik. Használata hozzájárul ahhoz, hogy a szervezet a biztonsági eseményeket nyomon kövesse, dokumentálja, szükség esetén jelentse, valamint a lezárt események tapasztalatait beépítse az eljárások, a szabályok és a riasztási feltételek felülvizsgálatába.

A runbook nem a figyelési igények nyilvántartása, hanem az adott riasztás vagy eseménytípus kezelésének végrehajtási útmutatója. Azt igazolja, hogy a szervezet a riasztás bekövetkezésekor tudja, ki értékeli az eseményt, milyen adatok alapján dönt, mikor eskalál, milyen intézkedést hajt végre, és milyen bizonyítékot hagy hátra.

10. MELLÉKLET 1.: KERET ÉS MEGVALÓSÍTÁSI SABLON, V1.0

10.1 Naplóforrás-prioritási modell

Szempont	1 pont	3 pont	5 pont
Üzleti kritikalitás	Támogató rendszer.	Fontos, de kerülőúttal részben kiváltható.	Kritikus üzleti vagy alaptevékenységi rendszer.
Adatérzékenység	Kevés vagy nyilvános adat.	Belső használatú üzleti adat.	Személyes, bizalmas vagy nagy hatású adat.
Incidensrekonstrukciós érték	Kevés vizsgálati információt ad.	Egy szakaszt jól megmagyaráz.	Több rendszert összekötő bizonyító értéke van.
Fenyegetettség	Ritkán támadott, zárt környezet.	Belső hálózatról elérhető vagy sok felhasználót érint.	Internet felől, távolról elérhető vagy magas jogosultsággal érintett.
Bekötési nehézség	Könnyű bekötni.	Közepes fejlesztési vagy szolgáltatói feladat.	Nehéz; a pontszámot a tervezésnél fordítottnak kell kezelni.

A szakmai prioritás az első négy szempont összege. Döntőtábla:

Összpontszám	Besorolás	Javasolt döntés
17–20	Azonnali prioritás	Projekttervbe és felelőshöz kell rendelni.
13–16	Magas prioritás	A következő bevezetési hullámban kezelendő.
9–12	Közepes prioritás	Kockázati indoklással ütemezhető.
5–8	Alacsony prioritás	Csak akkor indokolt, ha gyorsan beköthető, vagy auditkérés kapcsolódik hozzá.

10.2 Riasztási használatieset-sablon

Mező	Kitöltési útmutató
Use case azonosító	Egyedi, rövid azonosító. Példa: UC-IAM-001.
Kockázati történet	Egy mondatban: milyen nem kívánt helyzetet akarunk észlelni.
Érintett EIR / szolgáltatás	Mely rendszerhez kapcsolódik a felismerés.
Szükséges naplóforrások	Mely forrásokból kell adat; jelölni kell, ha valamelyik hiányzik.
Riasztási feltétel	Üzleti nyelven, nem gyártóspecifikus lekérdezésként.
Első értékelési kérdések	Mit kell ellenőrizni az első 15–30 percben.
Téves riasztási okok	Ismert karbantartás, jogos változás, teszt, szolgáltatói művelet.
Kapcsolódó runbook	Melyik eljárás szerint kell haladni.
Felülvizsgálati dátum	Mikor kell újra ellenőrizni a szabály hasznosságát.

10.3 Kezdő use case backlog

ID	Kockázati történet	Első vizsgálati kérdés	Javasolt állapot
UC-IAM-001	Kiemelt jogosultság olyan folyamaton kívül változik, amelyre nincs előzetes jóváhagyás.	Van-e kapcsolódó jogosultsági kérelem vagy változásjegy?	Tervezendő
UC-OPS-002	Üzleti rendszer naplóforrása elnémul,	Műszaki hiba, szolgáltatói	Kiemelt

	miközben a szolgáltatás aktívnak látszik.	változás vagy szándékos leállítás történt?	
UC-END-003	Védelmi komponens állapota rövid idő alatt több végponton kedvezőtlenre változik.	Azonos telephely, verzió vagy frissítési hullám érintett?	Tervezendő
UC-DATA-004	Szokatlan mintázatú adatkinyerés történik egy magas értékű üzleti rendszerből.	Normál riportfuttatás vagy rendkívüli export?	Tervezendő
UC-CLD-005	Felhős adminfelületen konfigurációs változás történik az üzemi ablakon kívül.	Belső admin, szolgáltató vagy automatizmus végezte?	Kiemelt
UC-AI-006	Nem jóváhagyott online szolgáltatás irányába céges adatmozgás gyanúja merül fel.	Engedélyezett vállalati szolgáltatásról vagy árnyékhasználatról van szó?	Opcionális
UC-MSP-007	Kihelyezett szolgáltatói fiók a megállapodott karbantartási ablakon kívül vagy szokatlan helyről lép be.	Volt-e bejelentett szolgáltatói munkavégzés vagy nyitott hibajegy?	Kiemelt

10.4 Szerepek és felelősségek (RACI)

Tevékenység	Vezetés	Információ-biztonság	EIR-felelős	IT-üzemeltetés	Incidenskezelő	Adatvédelem
Naplózási célok és prioritások jóváhagyása	A	R	C	C	C	C
Naplóforrás-leltár karbantartása	I	A	R	R	C	I
Use case backlog kezelése	I	A/R	C	C	R	C
Technikai bekötés és hibaelhárítás	I	C	C	A/R	C	I
Riasztás első értékelése	I	A	C	C	R	I
Incidensvizsgálati bizonyítékok kezelése	I	A	C	C	R	C
Naplóhozzáférések felülvizsgálata	I	A	C	R	C	C
Adatvédelmi kontrollpontok meghatározása	I	C	I	C	C	A/R

Jelölések: R = végrehajtó (Responsible), A = elszámoltatható (Accountable), C = bevonandó (Consulted), I = tájékoztatandó (Informed).

10.5 Működési ritmus

Gyakoriság	Feladat	Kimenet
Napi	Magas prioritású riasztások áttekintése, nyitott incidensjelöltek ellenőrzése.	Triage-döntés, jegyfrissítés.
Heti	Zajos szabályok, elnémult források és visszatérő hibák áttekintése.	Szabályhangolási vagy technikai feladat.
Havi	A use case backlog és az új EIR-változások összevetése.	Új vagy módosított riasztási igény.
Negyedéves	Naplóhozzáférések, forráslefedettség és a tesztelt riasztások áttekintése.	Felülvizsgálati jegyzőkönyv.
Incidens után	Az érintett naplóforrások, a hiányzó bizonyítékok és	Tanulmánylista és intézkedési terv.

a téves riasztások értékelése.

10.6 Incidensvizsgálati munkalap

Első értékelés:

Mező	Kitöltendő tartalom
Esemény azonosítója	Jegyszám vagy riasztási azonosító.
Észlelés ideje	Mikor került a szervezet látókörébe.
Érintett rendszer	EIR, szolgáltatás, felhőkomponens vagy végpontcsoport.
Elsődleges hatás	Rendelkezésre állás, bizalmasság, sértetlenség vagy működési zavar.
Érintett fiók / folyamat	Felhasználó, szolgáltatásfiók, adminfolyamat vagy automatizmus.
Első döntés	Téves riasztás, biztonsági esemény, incidensjelölt vagy incidens.
Azonnali intézkedés	Elkülönítés, hozzáférés-felfüggesztés, a szolgáltató értesítése, bizonyítékmentés.

Bizonyíték- és döntésnapló:

Időpont	Forrás	Mit ellenőriztünk?	Megállapítás	Döntés / következő lépés
kitöltendő	kitöltendő	kitöltendő	kitöltendő	kitöltendő
kitöltendő	kitöltendő	kitöltendő	kitöltendő	kitöltendő
kitöltendő	kitöltendő	kitöltendő	kitöltendő	kitöltendő

10.7 Külső szolgáltatói naplók – ellenőrző kérdéssor

Kérdés	Szerződéses / működési elvárás	Bizonyíték
Milyen események érhetők el?	A szolgáltató naplózási körét szolgáltatásonként dokumentálni kell.	Szolgáltatói leírás, adminfelületi export vagy szerződésmelléklet.
Mennyi ideig kérhető vissza?	A visszakereshetőségi idő ne legyen rövidebb a szervezet vizsgálati igényénél.	Megőrzési tájékoztató vagy szerződéses pont.
Milyen gyors az átadás?	Incidens esetén legyen meghatározott kapcsolattartó és válaszidő.	Kapcsolattartási rend, SLA.
Ki férhet hozzá?	A szolgáltatói és a belső hozzáférések legyenek szerepkörhöz kötve.	Jogosultsági lista.
Exportálható-e a napló?	Legyen vizsgálathoz használható formátum és időtartomány szerinti export.	Mintafájl vagy exportleírás.
Küldhető-e központi gyűjtőbe?	Ha igen, a bekötés technikai és adatvédelmi feltételeit rögzíteni kell.	Integrációs dokumentáció.

10.8 Naplóforrás-onboarding ellenőrzőlista

Kérdés	Igen / Nem	Megjegyzés
Az EIR szerepel a nyilvántartásban?		Az EIR-nyilvántartás sorára hivatkozva.
Van kijelölt EIR-felelős?		Név és helyettes megadása.
Ismert, milyen naplóforrások állnak		A forráslista a leltár melléklete.

Kérdés	Igen / Nem	Megjegyzés
rendelkezésre?		
Rögzített a gyűjtési mód?		Központi gyűjtő, helyi tárolás vagy szolgáltatói felület.
Ismert a megőrzési idő?		Időtartam és rögzítésének helye (szabályzat, szerződés).
Van naplóforrás-kiesési jelzés?		Kapcsolódó use case: UC-OPS-002.
Van legalább egy kapcsolódó use case?		Backlog-azonosító megadása.
A hozzáférési jogosultságok dokumentáltak?		A hozzáférési mátrix vonatkozó sora.
Tesztelték, hogy a napló vizsgálathoz használható?		A tesztjegyzőkönyv száma és dátuma.

10.9 Riasztásiszabály-adatlap

Mező	Érték
Szabályazonosító	kitöltendő
Kapcsolódó use case	kitöltendő
Érintett naplóforrás	kitöltendő
Prioritás	alacsony / közepes / magas / kritikus
Első reagáló szerepkör	kitöltendő
Runbook-hivatkozás vagy -azonosító	kitöltendő
Tesztelés dátuma	kitöltendő
Utolsó felülvizsgálat	kitöltendő
Ismert téves riasztási okok	kitöltendő

10.10 Incidens utáni tanulságok sablonja

Kérdés	Válasz
Mely naplóforrás segítette legjobban a vizsgálatot?	kitöltendő
Mely szükséges adat hiányzott?	kitöltendő
Volt-e felesleges vagy zajos riasztás?	kitöltendő
Kellett-e kézi adatbekérés a szolgáltatótól?	kitöltendő
Milyen szabályt, runbookot vagy hozzáférést kell módosítani?	kitöltendő
Milyen határidővel és felelőssel kerül be az intézkedési tervbe?	kitöltendő

10.11 Bevezetési ütemterv (90 nap)

Időtáv	Fókusz	Konkrét kimenet
0–30 nap	Alapfelmérés és döntési rend.	EIR-lista, a naplóforrás-leltár első változata, prioritási pontozás, a szerepkörök rögzítése.
31–60 nap	Első használati esetek és hozzáférési védősávok.	5–10 kiemelt use case, hozzáférési mátrix, első runbookok, adatvédelmi kontrollpontok.
61–90 nap	Teszt és működési beépítés.	Riasztási tesztek, az incidensmunkalap próbája, a heti és havi működési rutin elindítása.

90 nap után

Bővítés és finomítás.

Új források bekötése, a téves riasztások csökkentése,
negyedéves felülvizsgálat, a tanulságok beépítése.
