

Követelményelemzés

DLP Rendszer

8. csoport

1	Revision History	2
2	Bevezetés	5
3	Követelmények.....	6
3.1	Számozás és felépítés.....	6
3.2	Ellenőrző rendszer	6
3.3	Szabályok megadása és ellenőrzése	7
3.4	Naplózó rendszer.....	8
3.5	Felhasználók és Szerepkörök.....	9
3.6	Riasztó rendszer	9
3.7	Felhasználói interfész	10
3.8	Biztonság.....	12
3.9	Skálázhatóság.....	13
3.10	Teljesítmény és megbízhatóság.....	14
3.11	Tesztelési terv.....	15
3.12	Egyéb	16
4	Szójegyzék	17

1 Revision History

Verzió	Dátum	Szerző(k)	Leírás
1.0	2024.11.14.	Markó Gábor	Bevezetés és általános követelmények megfogalmazása
1.1	2024.11.15	Markó Gábor	Technikai és funkcionális követelmények kifejtése és szabály alapú működés leírása
2.0	2024.11.23	Szabó-Thalmeiner Bence	Teljes dokumentum szerkezetének átdolgozása, bevezető és szójegyzék hozzáadása, Követelmények területeinek meghatározása
2.1	2024.11.23	Szabó-Thalmeiner Bence	Minden részleghez alapvető követelmények hozzáadása, kombinálva a fenti verziókban leírtakat további, saját esetekkel
2.2	2024.11.24	Pallai Hunor	Alfejezetek kiegészítése további követelményekkel, kitérve a felhőtechnológiákkal való integrálásra, typo-k javítása,

			valamint szójegyzék kiegészítése
2.2.1	2024.11.25	Szabó-Thalmeiner Bence	Template részleg hozzáadva a könnyebb bővíthetőség érdekében.
2.3	2024.11.25	Szabó-Thalmeiner Bence	Általános leírások hozzáadva a legtöbb kategóriához
2.3.1	2024.11.25	Palotai Bálint	Szabályok szekció kiegészítése és felhasználói kivétel kérések
2.3.2	2024.11.28	Amamou Martin	Leírások hozzáadva a Skálázhatóság és az Egyéb kategóriákhoz.
2.3.4	2024.11.30.	Kiss Péter	Leírások hozzáadva a Felhasználói interfész, Riasztó rendszer és Biztonság kategóriákhoz.
2.4	2024.11.30	Solti Martin Szi-Benedek Balázs	Alfejezetek kiegészítése (3.3, 3.4, 3.7, 3.9 fejezetekben), néhány meglévő követelmény pontosítása további fejezetekben is, typo-k javítása, header számozás, tartalomjegyzék hozzáadása
2.5	2024.12.01.	Barczikay Kristóf	Alfejezet 3.5 kiegészítése, és alfejezet 3.10

			hozzáadása és kidolgozása
2.6	2024.12.01.	Szlotta Levente	Alfejezetek 3.8 kiegészítése, 3.5 kiegészítése és pontosítása, 3.10 bevezető hozzáadása
2.7	2024.12.01.	Smid Levente	Alfejezet 3.11 hozzáadása és kidolgozása
2.8	2024.12.01.	Liszkai Dorka	Alfejezetek kiegészítése (3.7, 3.8, 3.9, 3.11, 3.12)
2.9	2024.12.01.	Szabó-Thalmeiner Bence	Utolsó simítások, Template elemek kivétele, rendezés

2 Bevezetés

A Data Loss Prevention System egy, az operációs rendszer szinten működő, adat figyelő eszköz, aminek fő célja a belső rendszerből távozó adatok ellenőrzése, valamint bizalmas adatok megállítása. Veszélyes adat megállítása esetén riasztás generálódik, ami figyelmezteti a felelősöket és a hibázó felhasználót a problémára. A rendszer mögött egy robosztus naplózási rendszer is működik, ami menti az összes kimenő adatot és azt, hogy ki küldte őket. A rendszer szorosan együttműködik az OTP már meglévő rendszereivel, mind a naplózó, mind pedig a riasztó rendszer szoros kapcsolatban áll a már meglévő technológiákkal.

A sikeresség fő feltétele az adatok védelme (biztonság) és a skálázhatóság.

Alapvető szempont a teljes kimenő adatfolyam ellenőrzése, hogy semmilyen bizalmas adat ne hagyhatta el a belső rendszerünket. Érdekes a veszélyes adatküldési próbálkozásokról komoly naplót készíteni, ami bizonyítékként szolgál a problémás esetről, valamint egy gyors riasztó rendszerre is szükség van, hogy hamar ellene lehessen tenni a rossz indulatú szivárogtatási próbálkozásoknak.

A projektet az OTP bankkal szorosan együttműködve valósítjuk meg, belsős fejlesztők segítségével, hiszen az alapszabályok létrehozásához nem csak komoly jogi ismeretek szükségesek, hanem a belső szabályrendszer komoly ismerete is. Emellett csökkentjük a rossz indulatú személyek interferenciájának lehetőségét is, ha nem dolgozunk külső alvállalkozókkal.

3 Követelmények

3.1 Számozás és felépítés

Minden követelményt azonos módon definiálunk, egy egyedi azonosítóval és követelmény szöveges leírásával. Az azonosítók formátuma a következő:

- A_ID, ahol A a követelmény terület, ID pedig a követelmény azon belüli egyedi azonosítója

A követelmények területei és azok azonosítói a következők:

- E – Ellenőrző rendszer
- Sz – Szabályok megadása és ellenőrzése
- N – Naplózó rendszer
- FS – Felhasználók és Szerepkörök
- R – Riasztó rendszer
- I – Felhasználói interfész
- B – Biztonság
- S – Skálázhatóság
- T – Teljesítmény és megbízhatóság
- TE – Tesztelési terv
- Eg – Egyéb

3.2 Ellenőrző rendszer

Az ellenőrző rendszer feladata a kimenő forgalom megfigyelése, a bizalmas adatok megtalálása üzenetekben, valamint bizalmas adatok megtalálása esetén az adott üzenet blokkolása.

Azonosító	Leírás
E_01	A rendszernek hozzáféréssel kell rendelkeznie a belső rendszer összes, a külvilággal való lehetséges kapcsolódási pontjával, hogy megfigyelhesse a problémás adatok áramlását.
E_02	A rendszernek automatikusan ellenőriznie kell az adott eszköz összes kimenő forgalmát, ha telepítve van rá, ezzel védelmet nyújtva a mobil eszközökön és számítógépeken is.
E_03	A rendszernek automatikusan érzékelnie kell a nemzetközileg bizalmasnak tekintett adatokat bármilyen kimenő adatforgalomban.
E_04	A rendszernek képesnek kell lennie sajátos szűrők alapján is kimenő üzeneteket és adatokat megállítani
E_05	A rendszernek veszélyes adat észlelése esetén képesnek kell lennie az adott üzenet megállítására, az incidens naplózására, valamint egy riasztás kiküldésére

E_06	A rendszernek csak a külvilág felé irányuló adatforgalommal kell foglalkoznia, a belső üzeneteket nem figyeli
E_07	A kimenő csatornák sokfélék, a következőkre mindenképp fokozottan figyelni kell: <ul style="list-style-type: none"> • E-mail üzenetek • USB eszközre és egyéb adathordozókra való másolás • Internetes fájlfeltöltés • Nyomtatás külső eszközön

3.3 Szabályok megadása és ellenőrzése

A veszélyes adatok meghatározására a rendszernek szüksége van egy robosztus szabályrendszerre, aminek segítségével ki tudja válogatni ezen problémás elemeket. A félreértések elkerülése végett bizonyos szabályok a felhasználóknak is láthatóak kell legyenek.

Azonosító	Leírás
Sz_01	A rendszer képes kell legyen egyszerűbb szabályok ellenőrzésére regex kifejezések alapján
Sz_02	A rendszer képes kell legyen komplexebb problémák felderítésére AI eszközök segítségével
Sz_03	A rendszer képes kell legyen egyszerűbb szabályok ellenőrzésére fájlformátumok alapján
Sz_04	A szabályokat csak adminisztrátor felhasználók tudják létrehozni, módosítani és törölni.
Sz_05	A rendszerben jelen van egy, a szabály változtatásokkal kapcsolatos logolási rendszer, ami tartalmazza, hogy mely felhasználó milyen elemeken végzett változtatásokat. Ezek a változtatások a következők lehetnek: <ul style="list-style-type: none"> • Új szabály készítése • Meglévő szabály módosítása • Meglévő szabály törlése
Sz_06	Új szabály készítésénél lehetőségünk van adott kulcsszavak vagy fájlformátumok megadására, regex szabályok beépítésére, vagy természetes nyelven leírt kritériumok megadására.
Sz_07	Lehetőségünk van olyan szabályok létrehozására, amik csak egy adott felhasználói csoportot érintenek
Sz_08	Minden szabályhoz lehetőségünk van kivételes eseteket definiálni, melyek esetén nem generálódik riasztás. Ezek lehetnek speciális szöveggörnyezeti esetek, konkrét felhasználók vagy felhasználók csoportja
Sz_09	Egy szabály lehet publikus vagy privát, annak függvényében, hogy a felhasználók megtekinthetik-e
Sz_10	Egy szabály attribútumai a következők: <ul style="list-style-type: none"> • A szabály meghatározása

	<ul style="list-style-type: none"> • A szabály hatása alá eső személyek, csoportok • A szabály publikussága • A szabályt létrehozó- és utoljára módosító adminisztrátor neve • A szabály létrehozásának- és legutolsó módosításának dátuma • A szabályra vonatkozó kivételes esetek
--	--

3.4 Naplózó rendszer

A rendszer képes kell legyen saját működésének naplózására annak érdekében, hogy felügyelni lehessen ennek működését, valamint, hogy az egyes szabályokat sértő személyek is visszakereshetők legyenek. Ezen elemek tárolásánál a biztonság az egyik legfőbb szempont.

Azonosító	Leírás
N_01	A rendszer minden szabálysértés esetén létre kell hozzon egy új naplóbejegyzést, aminek tartalma a következő: <ul style="list-style-type: none"> • Az adott forgalom azonosítója • A forgalmat előidéző alkalmazott neve • A talált veszélyes adat, és annak leírása • A megsértett szabály- vagy szabályok azonosítója • A teljes üzenet archiválva
N_02	Az adott forgalom azonosítója egyedi, mely leírja, mikor és milyen eszközről volt indítva az üzenet, amely kiváltotta a problémát
N_03	Az előidéző alkalmazott neve alapján egyértelműen meg tudjuk határozni a hibát okozó személy kilétét, felhasználói fiókját
N_04	A talált veszélyes adat tartalmazza a problémás karaktersorozatot
N_05	A problémát kiváltó teljes üzenetet archivált formában elmentjük későbbi emberi felülvizsgálat céljából
N_06	A rendszer a napló elemeket a fő rendszerrel kompatibilis formában kell tárolja
N_07	A rendszernek képesnek kell lennie a naplózott adatok biztonságos tárolására felhő alapú technológiák használatával, biztosítva a skálázhatóságot és a hozzáférhetőséget
N_08	A felhő alapú naplózási megoldásoknak meg kell felelniük a nemzetközi adatvédelmi és biztonsági szabványoknak, mint például a GDPR és az ISO 27001
N_09	A rendszernek biztosítania kell a naplózott adatok titkosított átvitelét és tárolását a felhőben, hogy megvédje azokat az illetéktelen hozzáféréstől
N_10	A naplózási rendszernek támogatnia kell a felhő alapú analitikai eszközökkel való integrációt, lehetővé téve a naplózott adatok valós idejű elemzését és jelentéskészítését

N_11	A rendszernek képesnek kell lennie a naplózott adatok automatikus archiválására és visszaállítására a felhőben, biztosítva az adatok hosszú távú megőrzését és helyreállíthatóságát
------	---

3.5 Felhasználók és Szerepkörök

A rendszer helyes működtetése és a felhasználók azonosítása érdekében szükségünk van felhasználókra, valamint szerepkörökre, így bizonyos privilégiumokkal láthatjuk el a rendszert működtető személyeket, valamint minden felhasználóra könnyen hivatkozhatunk.

Azonosító	Leírás
F_01	A cég összes alkalmazottjához tartoznia kell minimum egy felhasználónak, hogy könnyen azonosíthassuk a szükséges személyeket
F_02	Minden felhasználó hozzárendelhető adott csoport(ok)hoz, ami(k)re sajátos szabályok is vonatkozhatnak
F_03	A felhasználó tagja lehet a következő szerepköröknek: <ul style="list-style-type: none"> • Adminisztrátor • Bizalmas adatot kiküldő • Tesztelő • Felhasználó
F_04	Egy felhasználó egyszerre több szerepkörrel is rendelkezhet
F_05	Egy felhasználó egyszerre több csoportnak is tagja lehet
F_06	Az adminisztrátor jogosultságú felhasználó képes a szabályok, valamint a felhasználói csoportok módosítására, létrehozására
F_07	Az adminisztrátor jogosultságú felhasználó képes hozzárendelni a felhasználókat az adott felhasználói csoport(ok)hoz.
F_08	A bizalmas adatot kiküldő jogkörrel rendelkező felhasználók szabadon küldhetnek ki bármilyen adatot a kívül világ irányába is
F_09	A tesztelő jogkörrel rendelkező felhasználók üzenetei ugyanúgy blokkolódhatnak, de a riasztás csak a fejlesztést felügyelő személyekhez jut el
F_10	A felhasználói szerepkör felhasználónak megadatik, tagjainak lehetősége van a kiírt publikus szabályok megtekintésére

3.6 Riasztó rendszer

A rendszerhez tartoznia kell egy riasztó rendszernek is, ami a szabályok sértése esetén gyorsan és megbízhatóan értesíti a felelős személyeket, valamint a szabálysértőt is.

Azonosító	Leírás
R_01	Minden egyes elkapott veszélyes információ esetén a rendszernek generálnia kell egy riasztást.
R_02	A riasztásnak tartalmaznia kell az érzékeléskor készített naplóbejegyzést és annak összes elemét
R_03	A rendszer a generált riasztást kiküldi a vétkes felhasználó csoportjáért felelős személyeknek, valamint a riasztást generáló felhasználónak is
R_04	A riasztó rendszer teljesen beépíthető kell legyen a meglévő rendszerekbe, a riasztás eljuttatását a központi rendszernek kell végeznie
R_05	A riasztások különböző szinteken generálódhatnak, de a szint meghatározása a központi rendszer feladata
R_06	A riasztási rendszernek képesnek kell lennie a felhőalapú infrastruktúrákkal való integrációra, hogy a riasztások valós időben elérhetők legyenek a felhőben tárolt adatok esetén is
R_07	A rendszernek támogatnia kell a felhőalapú szolgáltatások (pl. AWS, Azure, Google Cloud) riasztási mechanizmusait, hogy a riasztások közvetlenül ezekbe a rendszerekbe is továbbíthatók legyenek
R_08	A riasztási rendszernek biztosítania kell a riasztások skálázhatóságát a felhőalapú környezetekben, hogy nagy mennyiségű adatforgalom esetén is hatékonyan működjön
R_09	A rendszernek lehetőséget kell biztosítania a riasztások felhőalapú naplózására, hogy a riasztási adatok biztonságosan tárolhatók és elemezhetők legyenek a felhőben
R_10	A riasztási rendszernek támogatnia kell a felhőalapú biztonsági szabványokat és protokollokat, hogy a riasztások megfeleljenek a felhőszolgáltatók által előírt biztonsági követelményeknek
R_11	Riasztási rendszer integrálása mobilalkalmazásokkal, hogy a riasztások távolról is elérhetők legyenek.
R_12	A riasztások egy dedikált „hamis pozitív” kezelő felületre is irányíthatók legyenek, hogy minimalizálják a téves riasztásokat.

3.7 Felhasználói interfész

A rendszer helyes beállítása és a működése ellenőrzésének érdekében szükségünk lesz egy felhasználói interfészre, melyen keresztül az átlag felhasználók megismerkedhetnek a rájuk vonatkozó szabályokkal, valamint az adminisztrátorok felkonfigurálhatják azt.

Azonosító	Leírás
I_01	A rendszerhez tartoznia kell egy grafikus felhasználói felületnek, aminek segítségével kapcsolatba léphetünk a rendszerrel.
I_02	A felületnek rendelkeznie kell megfelelő felhasználókezeléssel. Ez magában foglal egy bejelentkezési felületet, bejelentkezés után az

	adott felhasználónak engedélyezett/releváns adatok megjelenítését, valamint engedélyezett műveletek elvégzésének lehetőségét.
I_03	A felhasználói felületnek tartalmaznia kell a következő oldalakat: <ul style="list-style-type: none"> • Felhasználóra vonatkozó publikus szabályok • Szabály készítő oldal • Csoport menedzser oldal • Statisztikai oldal • Profil oldal • Bejelentkezési felület
I_04	A Felhasználóra vonatkozó publikus szabályok oldalon a felhasználó megtekinthet minden olyan publikus szabályt, ami releváns számára, azaz ami vagy mindenkire, vagy az ő egy csoportjára érvényes.
I_05	Az adminisztrátor fiókok számára elérhető a szabály készítő oldal, amiben a felhasználónak lehetősége van a szabályrendszer változtatására új szabályok bevezetésével, már meglévők módosításával vagy törlésével
I_06	Az adminisztrátor fiókok számára elérhető a csoport menedzser oldal, amiben a felhasználóknak lehetősége van új felhasználói csoportok létrehozására, már meglévők módosítására vagy törlésére, valamint más felhasználók csoportokhoz való hozzárendelésére vagy kivételére
I_07	A statisztika oldalon az adminisztrátor felhasználók megtekinthetik a rendszer metrikák grafikonjait. Ezek a következők: <ul style="list-style-type: none"> • Elkapott veszélyes üzenetek száma időszakokra lebontva • Legveszélyesebb felhasználók • Legtöbbször sértett szabályok
I_08	A profil oldalon a felhasználó megtekintheti a saját fiókjához kapcsolódó metrikákat, mint hogy hányszor váltott ki riasztást, a saját riasztások listáját, valamint a hozzá tartozó jogosultságokat és csoportokat
I_09	A felhasználók számára legyen egy felület, ahol kivételt kérhetnek szabályokra, ezeket a kéréseket egy adminisztrátor tudja elfogadni
I_10	Az adminisztrátorok számára legyen egy felület, ahol a feléjük irányuló kivétel kéréseket el tudják fogadni vagy visszautasítani
I_11	Biztosítson sandbox környezetet az adminisztrátorok számára az új szabályok tesztelésére az éles bevezetés előtt.
I_12	A rendszernek támogatnia kell a többnyelvűséget, így a felhasználói felület könnyen lokalizálható különböző nyelvekre és régiókra, hogy globális felhasználók számára is elérhető legyen.
I_13	A felületnek biztosítania kell az akadálymentességet, hogy a fogyatékkal élő felhasználók is képesek legyenek azt használni. Ez magában foglalja az akadálymentes szabványok, például a WCAG betartását, valamint a képernyőolvasók és más segédeszközök támogatását.
I_14	A rendszer támogassa az értesítési rendszert, amely a felhasználókat figyelmezteti a szabálmódosításokra és az új szabályok élesítésére.

I_15	A felhasználói felület tartalmazzon egy keresési funkciót, amely lehetővé teszi a naplózott események szűrését és keresését dátum, felhasználó vagy szabály azonosító alapján.
I_16	A rendszernek biztosítania kell a felhasználók számára a könnyen használható hibajegyzrendszert, ahol gyorsan bejelenthetők a rendszerproblémák és kérdések, valamint azok nyomon követhetők legyenek.

3.8 Biztonság

Mivel a rendszer rengeteg bizalmas jellegű adattal dolgozik, nagyon fontos, hogy minden adatunkat és a teljes működést is erős védelemmel lássuk el.

Azonosító	Leírás
B_01	Mivel nem akarjuk, hogy a felhasználó kiiktathassa a védelmünket, a rendszernek operációs rendszer szinten kell működnie, ezzel biztosítva az ellenőrzések áthidalhatatlanságát.
B_02	A rendszer által naplózott adatokhoz csak az erre jogosult személyek férhetnek hozzá
B_03	Minden tárolt adatot titkosítással kell ellátnunk
B_04	A rendszernek képesnek kell lennie a biztonsági frissítések automatikus alkalmazására, hogy minimalizálja a sebezhetőségek kihasználásának lehetőségét
B_05	A rendszernek rendelkeznie kell behatolásérzékelő mechanizmusokkal, amelyek figyelik a gyanús tevékenységeket és azonnal riasztást generálnak
B_06	A rendszernek biztosítania kell a felhasználói tevékenységek auditálhatóságát, hogy visszakövethető legyen minden adatmozgás és szabálmódosítás
B_07	A rendszernek integrálhatónak kell lennie a meglévő biztonsági infrastruktúrával, beleértve a tűzfalakat és a behatolásmegelőző rendszereket, hogy átfogó védelmet nyújtson
B_08	A rendszernek támogatnia kell a többlépcsős hitelesítést a kritikus adminisztrátori funkciók eléréséhez, hogy növelje a hozzáférés biztonságát
B_09	A rendszernek támogatnia kell a felhőalapú szolgáltatásokkal való integrációt, miközben biztosítja a titkosított adatátvitelt és tárolást
B_10	A rendszernek rendelkeznie kell a felhőalapú környezetekben történő hozzáférés-szabályozási mechanizmusokkal, hogy csak az arra jogosult felhasználók férhessenek hozzá a bizalmas adatokhoz
B_11	A rendszernek képesnek kell lennie a felhőszolgáltatók által biztosított biztonsági naplók integrálására és elemzésére, hogy azonosíthassa a potenciális biztonsági incidenseket
B_12	Minden kritikus művelet előtt többlépcsős hitelesítés legyen kötelező.

B_13	A rendszernek biztosítania kell, hogy az összes naplózott adat megfeleljen a releváns adatvédelmi szabványoknak és törvényeknek, mint például a GDPR vagy a CCPA.
B_14	A naplózott adatok hash alapú aláírással kerülnek archiválásra, hogy azok megváltoztatása észlelhető és ezzel megakadályozható legyen.
B_15	A többlépcsős hitelesítésnek személyre szabhatónak kell lennie, hogy az illeszkedjen a létező rendszer folyamatához.
B_16	A rendszernek támogatnia kell a biometrikus azonosítást, például ujjlenyomat vagy arcfelismerés alapú hitelesítést kritikus műveletek elvégzéséhez.
B_17	A rendszernek figyelnie kell a nem szokványos adatforgalmat, például nagyszámú egyidejű adatátviteli próbálkozást, és ezeket potenciális fenyegetésként kell kezelnie.

3.9 Skálázhatóság

A rendszer skálázhatósága elengedhetetlen, mivel a vállalat, és az adatfolyamok száma folyamatosan növekszik. Fontos, hogy a rendszer rugalmasan alkalmazkodjon a nagyvállalati környezethez, esetleges változásai mellett is megbízhatóan működjön.

Azonosító	Leírás
S_01	A rendszernek képesnek kell lennie nagy adatmennyiségek kezelésére
S_02	A rendszert moduláris és skálázható architektúrával kell kialakítani, hogy a jövőbeni bővítések és funkciófejlesztések minimális átalakítással, könnyen megvalósíthatók legyenek.
S_03	A rendszer modulárisra kell tenni, így például könnyen hozzáadhatunk majd új csatornákat
S_04	A rendszernek képesnek kell lennie a terhelés dinamikus kezelésére, hogy a csúcsidőszakokban is megfelelően működjön, és ne okozzon fennakadásokat a szervezet működésében
S_05	A rendszernek támogatnia kell a több telephelyes működést, hogy a különböző földrajzi helyszíneken lévő felhasználók is zökkenőmentesen használhassák
S_06	A rendszernek rugalmasan kell kezelnie a felhasználói bázis növekedését, beleértve az új alkalmazottak gyors integrálását és a felhasználói szerepkörök dinamikus kezelését
S_07	A rendszernek biztosítania kell a skálázhatóságot a technológiai infrastruktúra szintjén is, lehetővé téve a szerverkapacitás és a hálózati erőforrások bővítését a növekvő igények kielégítésére
S_08	A rendszernek támogatnia kell a konténerizációs technológiákat (pl. Docker, Kubernetes), hogy könnyen telepíthető és skálázható legyen különböző környezetekben

S_09	A rendszernek képesnek kell lennie a felhőalapú adatbázisok és tárolási megoldások használatára a nagy mennyiségű adat hatékony kezeléséhez
S_10	A rendszernek biztosítani kell a felhőszolgáltatók (pl. AWS, Azure, Google Cloud) által nyújtott skálázási és terheléelosztási megoldások integrációját
S_11	A rendszernek dinamikusan bővíthető kell legyen különböző időzónákhoz igazított működéshez, amely figyelembe veszi a globális vállalatok igényeit.

3.10 Teljesítmény és megbízhatóság

A teljesítmény és megbízhatóság garantálása kulcsfontosságú egy DLP rendszer folyamatos, hatékony és zökkenőmentes működéséhez. Figyelembe kell venni a különböző mértékű terheléseket és adatmennyiségeket, illetve a kritikus körülményeket ahhoz, hogy biztosítani lehessen a hibamentes adatkezelést és a pontos riasztásokat.

Azonosító	Leírás
T_01	A rendszernek képesnek kell lennie a kimenő adatforgalom valós idejű feldolgozására, hogy azonnali blokkolást és riasztást biztosítson, miközben az átfutási idő nem haladhatja meg a 200 milliszekundumot üzenetenként.
T_02	A rendszernek tartalmaznia kell egy teljesítménymonitorozó modult, amely folyamatosan nyomon követi a rendszer terhelését, az átlagos válaszidőt és a kritikus erőforrások (CPU, memória, hálózati sávszélesség) használatát.
T_03	A rendszernek automatikusan el kell indítania egy helyreállítási folyamatot minden kritikus hiba esetén, biztosítva, hogy a szolgáltatás 99,9%-os rendelkezésre állást érjen el.
T_04	A rendszernek képesnek kell lennie a terheléelosztásra, így nagy adatforgalom esetén dinamikusan osztja el a terhelést több szerver vagy folyamat között a stabil működés érdekében.
T_05	A rendszernek redundanciával kell rendelkeznie, hogy az egyes komponensek meghibásodása ne eredményezzen adatvesztést vagy szolgáltatáskimaradást.
T_06	A rendszernek támogatnia kell a teljesítményadatok exportálását külső monitorozó eszközök (pl. Prometheus, Grafana) számára, hogy ezekkel valós idejű riportok készülhessenek.
T_07	A rendszernek tartalmaznia kell egy figyelmeztetési rendszert, amely automatikusan értesíti az adminisztrátorokat, ha a teljesítménykritériumok (pl. válaszidő, terhelés) meghaladják az előre meghatározott határértékeket.
T_08	A rendszernek meg kell őriznie a naplózott adatokat és a konfigurációs beállításokat a helyreállítási folyamat során, hogy az újraindulás után minden adat és beállítás elérhető maradjon.

T_09	A rendszernek képesnek kell lennie a kritikus adatfolyamok prioritásának automatikus meghatározására és kezelésére túlterhelés esetén, biztosítva a legfontosabb funkciók folytonosságát.
------	---

3.11 Tesztelési terv

A rendszer tesztelése kritikus fontosságú a DLP rendszer megbízhatóságának és hatékonyságának biztosítása érdekében. A tesztelési terv az alábbi területeket foglalja magában:

Azonosító	Leírás
TE_01	A rendszer tesztelési tervének tartalmaznia kell a funkcionális, teljesítmény- és biztonsági tesztek. Minden tesztelési szakaszt dokumentálni kell, és az eredményeket naplózni kell auditálás céljából.
TE_02	Funkcionális tesztelés során: <ul style="list-style-type: none"> • Ellenőrizni kell az egyszerű szabályok helyes működését (pl. regex). • Az AI vezérelte szabályok helyességét szimulált adatokkal. • Fájltypus-alapú szűrés tesztelése különböző formátumokkal (PDF, ZIP, kép).
TE_03	Teljesítménytesztelés céljai: <ul style="list-style-type: none"> • Ellenőrizni kell, hogy a rendszer képes a 200 ms/üzenet átfutási időre nagy adatforgalom esetén. • Szimulált csúcsidőszakokban biztosítani kell a terhelés megfelelő elosztását.
TE_04	Biztonsági tesztelés során: <ul style="list-style-type: none"> • Szimulált behatolási tesztek végrehajtása (pl. brute force támadások). • Az adattitkosítás helyességének vizsgálata (AES-256 alkalmazása).
TE_05	Sandbox környezet biztosítása az adminisztrátorok számára, ahol: <ul style="list-style-type: none"> • Új szabályok tesztelése történhet az éles rendszer befolyásolása nélkül. • A sandbox izolált működése biztosított legyen minden szinten.
TE_06	Minden tesztelés után automatikus jelentéskészítés, amely tartalmazza az összes észlelt hibát, a javításokat és az elvégzett tesztek. A jelentések feleljenek meg a GDPR előírásainak.
TE_7	Képesség tesztelés: <ul style="list-style-type: none"> • A rendszer képes legyen a nagy adatmennyiségek és a magas felhasználói terhelés kezelésére.

	<ul style="list-style-type: none"> • Tesztelni kell a rendszer válaszüdejét és megbízhatóságát, amikor több ezer felhasználó egyidejűleg próbál adatokat küldeni.
TE_8	Különböző platformokon történő tesztelés: A rendszer működésének tesztelése különböző operációs rendszereken (Linux, Windows, MacOS) és mobilplatformokon (Android, iOS).
TE_9	Tesztelni kell, hogy a rendszer pontos és időben történő riasztásokat generál, amikor veszélyes adatküldési próbálkozás történik.
TE_10	A rendszer hosszú távú működésének tesztelés, hogy ellenőrizze a rendszer stabilitását és megbízhatóságát.
TE_11	A felhasználói jogosultságok és szerepkörök tesztelése, hogy biztosítsa, hogy minden felhasználói szerepkör megfelelő hozzáférést kap, és hogy a jogosulatlan hozzáférések blokkolásra kerüljenek.
TE_12	A rendszer végfelhasználói tesztelése, hogy biztosítsa a könnyű használhatóságot és a felhasználói élményt, különös figyelmet fordítva a rendszer kezelőfelületére és a felhasználói visszajelzések integrálására.

3.12 Egyéb

Az alábbi kategóriákhoz tartoznak azok a követelmények, amelyek nem tartoznak szorosan más részterületekhez, de nélkülözhetetlenek a rendszer zökkenőmentes működése érdekében.

Azonosító	Leírás
Eg_01	A rendszer képes kell legyen minden népszerű számítógépes (Linux, Windows, MacOS) és mobilos (Android, iOS) rendszeren helyesen működni
Eg_02	A rendszernek képesnek kell lennie a felhőalapú szolgáltatásokkal való integrációra, hogy a biztonsági funkciók a felhőben tárolt adatokra is kiterjedjenek
Eg_03	A rendszernek kompatibilisnek kell lennie a különböző felhőszolgáltatók (pl. AWS, Azure, Google Cloud) platformjaival, hogy rugalmasan alkalmazható legyen különböző felhőinfrastruktúrákban
Eg_04	A rendszernek lehetőséget kell biztosítania testreszabott riportok készítésére, amelyek a különböző vezetői szintek igényeihez igazíthatók, lehetővé téve a fontos metrikák és teljesítményadatok dinamikus és rugalmas megjelenítését különböző formátumokban (pl. PDF, Excel, stb.).

4 Szójegyzék

- **Bizalmas adat** – Minden olyan adat, ami a nemzeti és nemzetközi törvények értelmében személyesnek, bizalmasnak van feltüntetve, és semmilyen körülmények között nem lehet publikussá tenni
- **Veszélyes adat** – A bizalmas adatok és a saját egyedi szűrőkön fennakadó adatok összessége
- **Blokkolás** – Egy adott elem mozgásának megállítása. A mi esetünkben a kimenő adatforgalom küldés előtti megállítása.
- **Riasztás** – Egy automatikusan generált értesítés, amely figyelmezteti a felelősöket és a hibázó felhasználót a veszélyes adat észlelésére és blokkolására.
- **Naplózás** – Az a folyamat, amely során a rendszer rögzíti a kimenő adatforgalom eseményeit, beleértve a veszélyes adatok észlelését és a kapcsolódó részleteket.
- **Szabály** – Olyan előírás vagy feltétel, amely alapján a rendszer meghatározza, hogy egy adott adatforgalom veszélyes-e, és szükséges-e annak blokkolása.
- **Felhasználói szerepkör** – A felhasználókhöz rendelt jogosultságok és funkciók összessége, amelyek meghatározzák, hogy a felhasználó milyen műveleteket végezhet a rendszerben.
- **Skálázhatóság** – A rendszer azon képessége, hogy hatékonyan kezelje a növekvő adatmennyiséget és felhasználói bázist anélkül, hogy a teljesítmény csökkenne.
- **Integráció** – A rendszer összekapcsolása más meglévő rendszerekkel, például naplózó és riasztó rendszerekkel, hogy zökkenőmentesen működjenek együtt.
- **Felhőalapú szolgáltatások** – Olyan távoli szervereken futó szolgáltatások, amelyek lehetővé teszik az adatok tárolását, kezelését és elemzését a felhőben.