ANALYTICS DATA FACTORY

NEODATA

FRAUD DETECTION SYSTEM

BY NEODATA

PŘEDSTAVENÍ SPOLEČNOSTI ANALYTICS DATA FACTORY

Analytics Data Factory působí na českém trhu od roku 2015 jako dodavatel a správce řešení postavených na analytických technologiích společnosti SAS včetně veškerého navazujícího ekosystému, jako je hardware, operační systémy, databáze, vývojový a verzovací software, messaging infrastruktura nebo big data platformy. Analytics Data Factory se primárně specializuje na oblasti, ve kterých dle referencí poskytuje služby na špičkové úrovni. Jedná se především o analýzu dat v reálném čase, a to například v oblastech aktivního řízení vztahu se zákazníky (CRM), prevence vzniku podvodů, zpracování signálů a rozpoznávání obrazu nebo pokročilé analytiky na velkých a streamovaných datech. Mezi klienty patří Komerční banka, Česká podnikatelská pojišťovna, pojišťovna Kooperativa, Home Credit, a další.

ADF je držitel certifikátu TISAX® třetího stupně a ISO. Norma, garantuje schopnost chránit citlivé informace partnerů a zákazníků v oblasti kritické infrastruktury a automotive. V roce 2022 bylo ADF úspěšně certifikováno dle normy ČSN EN ISO/EIC 27001:2014 v oboru implementace a rozvoji IT systémů.

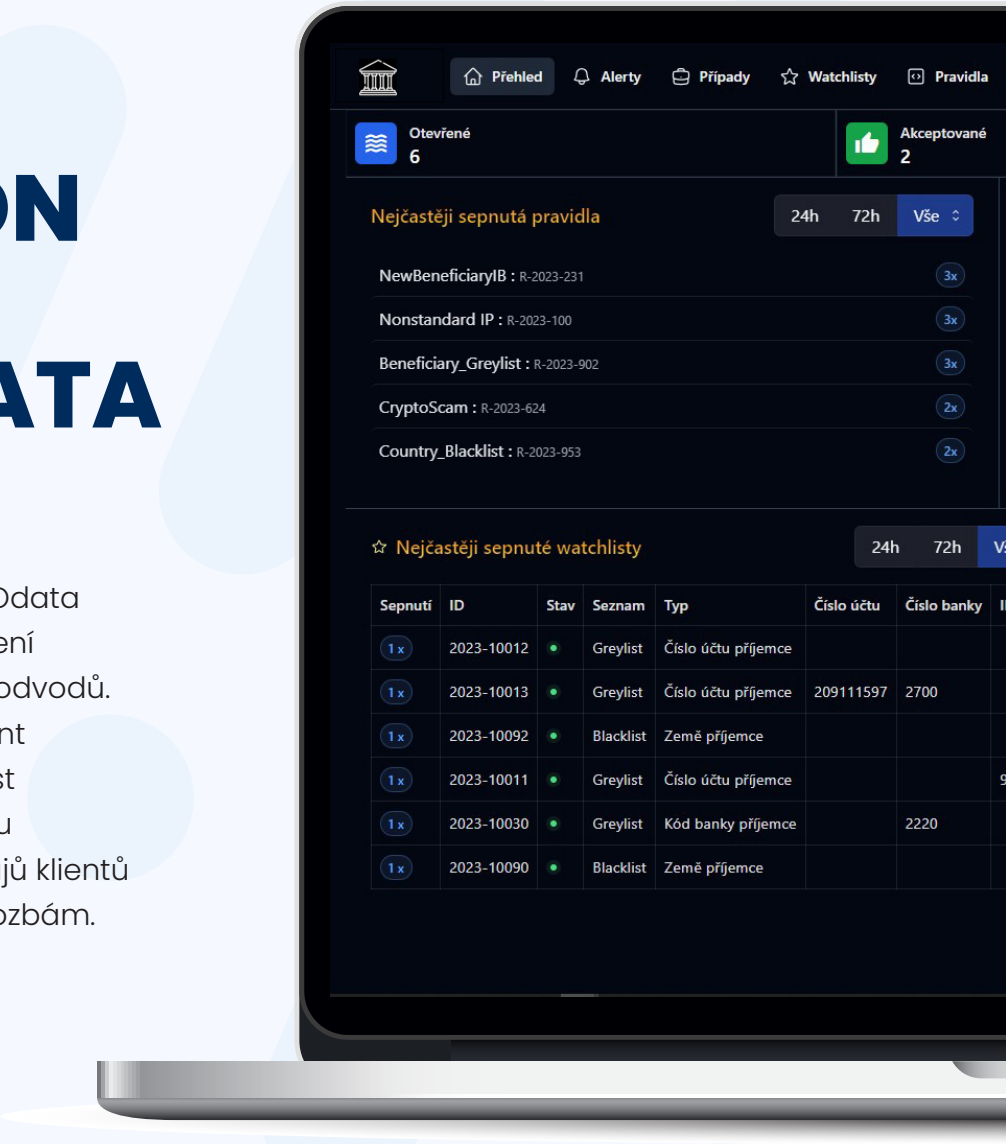
Společnost spolupracuje s významnými českými a zahraničními technologickými partnery jako je Oracle, Dell, VMware, RedHat, Diebold Nixdorf. ADF je zlatým partnerem SASu, jehož technologiím vdechuje život již od samotného vzniku společnosti.

Partnerstvím s Českou asociací umělé inteligence ADF posílilo svou pozici v oblasti umělé inteligence a datové analýzy s cílem přispět k inovacím a etickému rozvoji AI nejen v České republice. Mezi další cíle spolupráce patří realizace školení a workshopů v oblastech Deep Fake a ACTu AI.

PUBLIC

FRAUD DETECTION SYSTEM BY NEODATA

Fraud Detection System by NEOdata (FDS) je moderní real-time řešení v oblasti detekce platebních podvodů. Navrženo pro bankovní segment s důrazem na přesnost, rychlost a spolehlivost, zajišťuje ochranu transakcí a přihlašovacích údajů klientů proti neustále se vyvíjejícím hrozbám.



KLÍČOVÉ VÝHODY ŘEŠENÍ FRAUD DETECTION SYSTEM BY NEODATA

Neustálá detekce pokročilých platebních a AML podvodů v reálném čase. Řešení FDS usnadňuje vytvoření strategie proti podvodům v rámci jediné platformy a poskytuje investigátorům rychlost a plynulost práce. Zároveň přispívá k prevenci finanční kriminality pro digitální éru.

Pokrytí všech digitálních kanálů plateb a přihlášení. Zpracování karetních i platebních příkazů, autentizací, challenge metod a step-up metod, PSD operací, nefinančních transakcí. Zajišťuje real-time zpracování příchozích i odchozích plateb.

Navrženo pro jednoduchou a rychlou implementaci pokročilých pravidel skóringu pomocí AI mikro-modulů. Řešení nabízí pokročilý hybridní model detekce, který spojuje uživatelsky definovaná pravidla s automaticky se adaptujícími pravidly založenými na AI.

Kompletní auditní stopa a řízení rolí. Komplexní statistiky relace pro forenzní analýzu s podporou dedikovaného týmu. Zajišťujte úplnou transparentnost pro ulehčení dohledu regulačních orgánů.

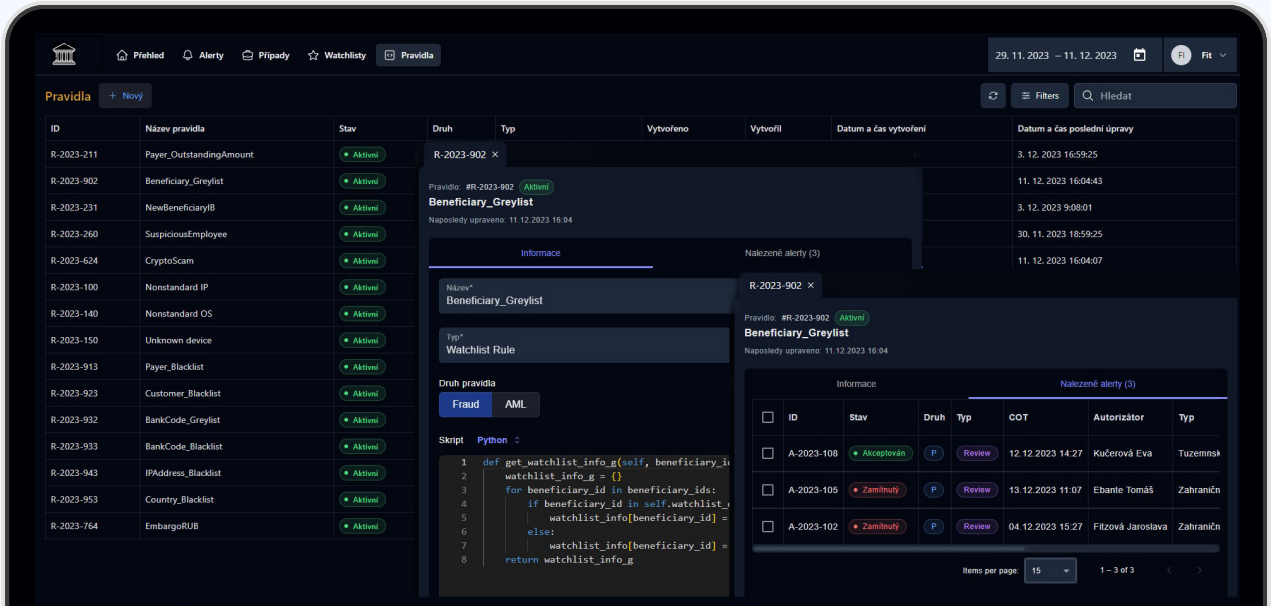
FUNKČNÍ MOŽNOSTI ŘEŠENÍ

Optimalizovaný 360° Frontend se všemi daty pro investigaci včetně funkce automatického globálního propojení a mapování entit. Ivestigátoři již nemusejí překlikávat do jiných systémů – všechna potřebná data mají k dispozici v přehledné podobě:

- klienti, zaměstnaneci banky, transakce
- watchlisty, pravidla
- alerty, případy
- uživatelé (aplikace)

Řízení watchlistů all-in-one:

- podporované typy watchlistingu (čísla účtů, klienti, banky, země, PSD třetí strany, IP Adresy)
- přehledná statistika nejčastějších sepnutých watchlistů
- one-click propojení a navigace na související alerty a pravidla

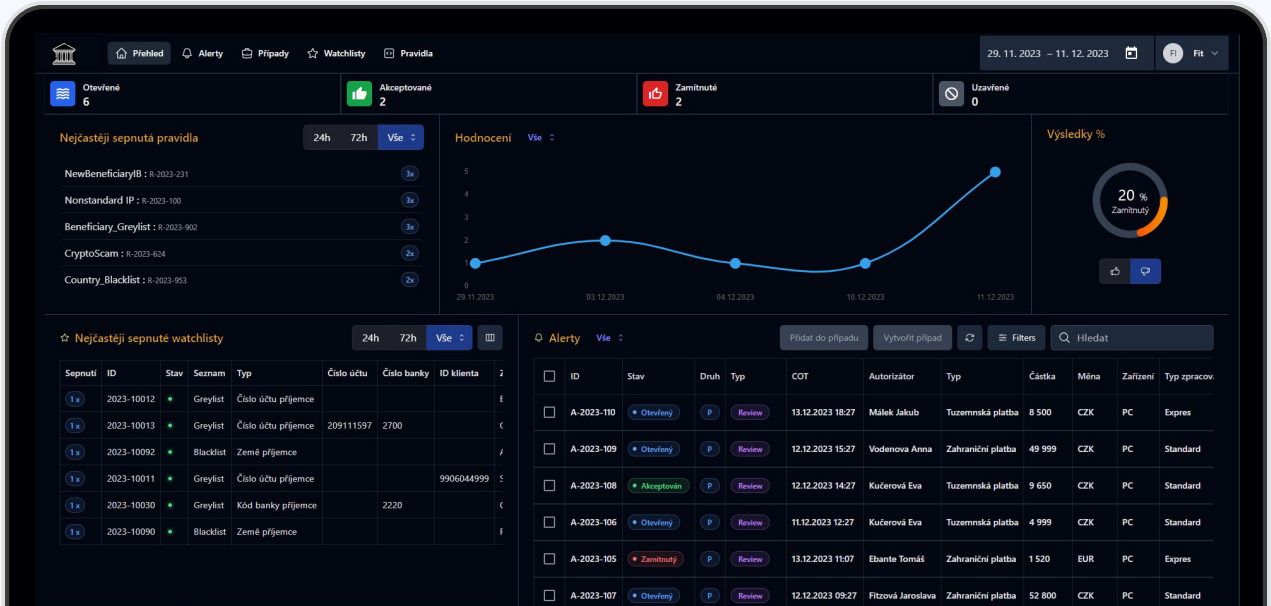


Řízení alertů a případů all-in-one:

- generování, řízení toku a obohacování dat alertů
- řízení investigace a front pro real-time platební, AML a karetní podvody
- dynamické přiřazení alertů do případu
- možnost vícevrstvých komentářů s přílohou

Analýza skóringu a pravidel:

- využívá nejnovější trendy ve streamované analytice a umožňuje korelovat související toky dat v reálném čase
- vizualizace skrytých vztahů mezi transakcemi, klienty a účty
- práce s kalkulovanými prediktory a indikátory detekce anomálií
- detekce i komplexních typologií
- možnosti napojení na externí registry, seznamy účtů pro automatické vytvoření nového pravidla (skupiny pravidel)



BENEFITY FRAUD DETECTION SYSTEM BY NEODATA

All in one řešení formou služby

- Zákazník se nemusí o nic starat (SW, HW, licence, implementace, provoz a interní zdroje).

Rychlá implementace

- V řádu týdnů.

Zkušenosti a reference

- Špička v oboru na FRAUD řešení.
- Úspěšná implementaci a více než sedmiletý provoz v KB.

Odezva v řádu milisekund

- Řešení je postaveno na nejmodernější infrastruktuře s výkonem, který je schopen zajistit odezvy v řádu milisekund.
- Support 24/7
- SLA 99,99 %

DOPLŇKOVÉ SLUŽBY FRAUD DETECTION SYSTEM BY NEODATA

ADF má virtuální investigativní tým, který testuje podvody/hrozby, identifikuje nové podvodné scénáře či nežádoucí entity včetně možnosti rozpoznání bílých koňů nebo detekce podvodných skupin.

Pro tyto aktivity je využíván Deep learning, které trénuje umělé neuronové sítě tak, aby byly schopny vykonávat specifické úkoly.

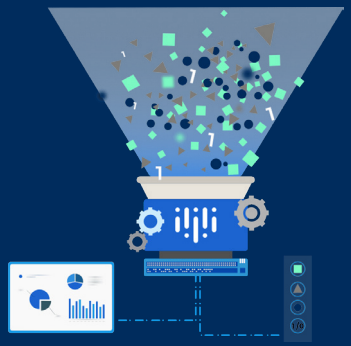
Kalibrace a fine-tuning neuronových sítí zajišťují, aby pravděpodobnosti predikcí byly spolehlivé a interpretovatelné, zároveň se lépe specializovaly na konkrétní úlohu či data a dosažení optimální výkonnosti neuronových sítí v rámci konkrétních aplikací a úloh v oblasti umělé inteligence.

Školení zaměstnanců banky v oblastech nových podvodných technik a způsobů. Realizace workshopů zaměřených na analytiku, fraud, security.

Pomoc při vytváření pozitivního povědomí mezi zaměstnanci a zákazníky o významu bezpečnosti a prevence podvodů.

Pravidelné kontroly a audity systému FDS k zajištění jeho účinnosti a shody s nejnovějšími bezpečnostními normami.

Udržitelné IT – zvyšování efektivity a snižování nákladů. Podpora recyklace starého hardware, minimalizace odpadu v průběhu životního cyklu zařízení.



ESG A FRAUD DETECTION SYSTEM BY NEODATA

Environmentální Aspekty
Fraud Detection System je navržen tak, aby minimalizoval ekologickou stopu. Systém využívá technologie a optimalizované algoritmy, které snižují potřebu fyzických serverů a tím i spotřebu energie. Zároveň je podporována iniciativa pro zelené bankovnictví, například snižováním papírového odpadu prostřednictvím digitálního zpracování transakcí.

Sociální Aspekty
Bezpečnost a ochrana klientů jsou nejvyšší prioritou. Fraud Detection System přispívá k ochraně osobních a finančních údajů klientů banky, což posiluje důvěru a sociální odpovědnost banky. Tímto způsobem je podporována transparentnost a etické jednání v celém finančním sektoru.

Governance Aspekty
Řešení bylo navrženo s důrazem na dodržování nejpřísnějších standardů v oblasti řízení a compliance. Nabízí podrobné auditové stopy a dodržuje přísné protokoly pro zabezpečení dat, což bankám umožňuje efektivně řídit rizika a dodržovat regulativní požadavky.

V rámci firemního závazku k dodržování principů ESG (Environmentální, Sociální a Governance) je chápana důležitost integrování těchto aspektů do produktů, řešení a služeb. Fraud Detection System by NEOdata byl vyvinut s myšlenkou podpory udržitelného a etického bankovnictví, které je v souladu s ESG zásadami.

Fraud Detection System by NEOdata plně reflektuje zásady ESG, které jsou klíčové pro moderní bankovnictví. Technologie přispívá k efektivní detekci podvodů, ale také posiluje environmentální, sociální a governance standardy našich zákazníků. Tento integrovaný přístup pomáhá bankám budovat udržitelné, transparentní a etické finanční prostředí.

TECHNICKÉ SPECIFIKACE FRAUD DETECTION SYSTEM BY NEODATA

Udržitelný rozvoj pomocí on-demand infrastruktury a dynamického škálování

On-Demand infrastruktura:

- Řešení je postaveno tak, že umožňuje dynamickou alokaci zdrojů podle aktuální potřeby. Využívá služby VMware Tanzu pro zajištění vysoké dostupnosti a flexibilní škálovatelnosti.
- Pro rychlé nasazení a správu aplikačních prostředí řešení využívá kontejnerizace a orchestrace kontejnerů.

Dynamické škálování:

- FDS řešení je implementováno včetně automatického škálování, které reaguje na změny zatížení systému. To zahrnuje vertikální škálování pro zvýšení výkonu existujících instancí a horizontální škálování pro přidání dalších instancí.
- Díky škálování a on-demand přístupu se jedná o udržitelné řešení, které umožňuje plnit společné ESG cíle.

Optimalizované CI/CD nasazování pomocí Helm v souladu s DevSecOps a GitOps

CI/CD pipeline:

- Využívá nástrojů jako Jenkins, GitLab CI/CD nebo GitHub Actions pro automatizaci procesu integrace (CI) a nasazování (CD). Tato pipeline zahrnuje automatické testování kódu, sestavení a nasazení.
- Integrace skriptů Helm do pipeline pro správu a nasazení aplikací v Kubernetes.

Helm pro správu nasazení:

- Helm se používá jako správce balíčků pro Kubernetes. Umožňuje definovat, instalovat a aktualizovat Kubernetes aplikace.
- Vytváření Helm grafů pro popis a verzi aplikací, což zjednodušuje aktualizace a rollbacks

DevSecOps integrace:

- Začlenění bezpečnostních prvků do CI/CD pipeline, včetně statické a dynamické analýzy kódu, skenování zranitelností v závislostech a kontejnerech.
- Pro zajištění bezpečnosti každého nasazení řešení využívá automatizované bezpečnostní kontroly.

GitOps procesy:

- Použití Gitu jako jediného single source of truth pro infrastrukturní kód i konfiguraci aplikace. Změny v infrastruktuře a aplikacích jsou spravovány prostřednictvím pull requestů a code reviews.
- Automatické nasazení změn, které jsou schváleny a sloučeny do hlavní větve repozitáře.

Monitoring a zpětná vazba:

- V rámci řešení jsou implementovány monitorovací a logovací nástroje jako Prometheus, Zabbix, Grafana, a ELK stack pro sledování zdraví aplikací a infrastruktury.
- Pro zajištění okamžité reakce na problémy a optimalizaci procesů jsou nastaveny upozornění a zpětnovazební smyčky.

Zabezpečení pomocí TLS 1.3

Implementace TLS 1.3:

- Řešení je postaveno na TLS 1.3, nejnovější verze protokolu TLS, která nabízí vylepšené zabezpečení a výkon.
- Konfigurace serverů pro vynucení použití TLS 1.3 pro všechnu šifrovanou komunikaci. Odstranění podpory pro starší a méně bezpečné verze protokolů TLS/SSL.

Optimalizace a konfigurace:

- Nastavení preferovaných šifer s důrazem na ty, které poskytují nejvyšší úroveň bezpečnosti a zároveň efektivní výkon.
- Konfigurace Perfect Forward Secrecy (PFS) pro zajištění, že i v případě kompromitace soukromého klíče zůstanou dřívější komunikace bezpečné.

Vysoká dostupnost a škálování na tisíce plateb/vteřinu

Architektura pro vysokou dostupnost:

- Je používáno více replikovaných serverů a služeb rozložených přes různé geografické oblasti a datacentra, zajišťující kontinuální dostupnost služby i v případě výpadku v jedné lokalitě.

Analytics Data Factory s.r.o.
Masarykovo náměstí 1544
Pardubice - Zelené Předměstí 530 02

info@byadf.cz
730 590 826

@analytics_data_factory

@analyticsdatafactoryadf1216

/analytics-data-factory-s.r.o.

www.byadf.cz

www.neodatabyadf.cz

www.foodsave.cz