Detailný návrh riešenia

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	
Názov projektu	
Zodpovedná osoba za projekt	
Realizátor projektu	
Vlastník projektu	
Dodávateľ	
PM Dodávateľa	

Schvaľovanie dokumentu

Položka	Meno apriezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval					

História dokumentu

Verzia	Dátum	Zmeny	Meno
R2v0.3	*30.05.2025*		

Obsah

1 Použité skratky a pojmy 5

2 Manažérske zhrnutie 6

2.1 Zámer riešenia 6

2.2 Ciele riešenia 6

2.3 Merateľné a výkonnostné ukazovatele (KPI) 6

2.4 Rozsah riešenia 6

2.5 Mimo rozsah projektu 7

2.6 Stručný popis navrhovaného riešenia 7

2.7 Sumarizácia výstupu M-06 navrhovaného riešenia 7

2.7.1 Prehľad koncových služieb – budúci stav 7

2.7.2 Rozsah informačných systémov – budúci stav 7

2.7.3 Prehľad plánovaných integrácií ISVS na nadrezortné ISVS – spoločné moduly podľa zákona č. 305/2013 e-Governmente – budúci stav 7

2.7.4 Prehľad plánovaného využívania iných ISVS (integrácie) – budúci stav 7

2.7.5 Aplikačné služby pre realizáciu koncových služieb – budúci stav 8

2.7.6 Aplikačné služby na integráciu – budúci stav 8

3 Analýza požiadaviek 8

3.1 Postup analýzy požiadaviek 8

3.2 Používateľský prieskum 9

3.3 Motivačná architektúra 9

3.3.1 9

3.4 Motivation Viewpoints 9

3.5 Katalóg požiadaviek a jeho mapovanie na návrh ich riešenia 10

3.6 Legislatíva, smernice a metodické materiály zohľadnené v riešení 11

3.7 Akceptačné kritéria 11

4 Biznis architektúra 11

4.1 Biznis architektúra 11

4.2 BPMN - Biznis procesný model 11

4.3 Prípady použitia 11

4.3.1 Aktéri 11

4.3.2 Všeobecné prípady použitia 14

4.3.2.1 Prípady použitia diagramy ..... **Chyba! Záložka nie je definovaná.**

4.3.2.2 UC_00 - Inicializácia a konfigurácia SOCaaS ..... **Chyba! Záložka nie je definovaná.**

4.3.2.3 UC_01 - Monitorovať bezpečnostné udalosti ..... **Chyba! Záložka nie je definovaná.**

4.3.2.4 UC_02 - Vizualizovať a reportovať bezpečnostné údaje ..... **Chyba! Záložka nie je definovaná.**

4.3.2.5 UC_03 - Spravovať detekčné a korelačné pravidlá 25

4.3.2.6 UC_04 – Upozorniť a eskalovať bezpečnostný incident 26

4.3.2.7 UC_05 – Riešiť a uzatvoriť bezpečnostný incident 28

4.3.2.8 UC_06 – Vyhodnotiť incidenty a zlepšiť detekciu aj povedomie 31

4.3.2.9 UC_07 – Automatizovať reakciu na incident 32

4.3.2.10 UC_08 – Proaktívne hľadanie hrozieb 34

4.3.2.11 UC_09 – Spravovať Threat Intelligence a indikátory kompromitácie 35

4.3.2.12 UC_10 – Riadiť súlad, metriky a manažérsky reporting 37

4.3.2.13 UC_11 – Spravovať aktíva a prostredie zákazníka 40

4.3.2.14 UC_12 – Riadiť zraniteľnosti a bezpečnostné nálezy 41

4.3.2.15 UC_13 – Navrhnúť a udržiavať bezpečnostnú architektúru SOCaaS prostredia zákazníka 43

4.3.2.16 UC_14 – Portál zákazníka a spolupráca 45

4.3.2.17 UC_15 – Spravovať prevádzku SOCaaS platformy 48
4.3.2.18 UC_16 – Prispôsobiť reporty, exporty a dokumenty potrebám organizácie 50
4.3.2.19 UC_17 – Spravovať používateľov a roly v SOCaaS platforme 51
4.4 Biznis architektúra 53
4.4.1 Identifikácia vlastníkov dizajnu koncových služieb (UX) 53
4.4.2 Špecifikácia potrieb koncového zákazníka 53
4.4.3 Návrh prototypov používateľského rozhrania 53
4.4.4 Návrh vizuálov obrazoviek 54
5 Dátová architektúra 54
6 Aplikačná architektúra 54
6.1 Aplikačná architektúra 54
6.2 Aplication Viewpoints 54
6.3 Návrh riešenia dizajnu aplikačných služieb 57
6.3.1 Existujúce aplikačné rozhrania 57
6.3.2 Zanikajúce aplikačné rozhrania 57
6.3.3 Nové aplikačné rozhrania 57
6.4 Integrácie medzi systémami 57
6.4.1 Zoznam existujúcich integrácií bez zmeny 57
6.4.2 Zoznam a popis navrhovaných integrácií 57
6.4.3 Zoznam a popis požadovaných integračných rozhraní 57
6.4.4 Návrh poskytovaných aplikačných rozhraní systému (modulu) 57
7 Technologická architektúra 57
7.1 Technologická architektúra 58
7.2 Technology Viewpoint INNOSOC Common 58
7.3 Technology Viewpoint Inventarizacia aktiv 58
7.4 Technology Viewpoint Kubernetes 60
7.5 Technology Viewpoint OpenStack 73
7.6 Technology Viewpoint OpenStack External 75
7.7 Technology Viewpoint Reportovanie 75
7.8 Technology Viewpoint Skener zraniteľností 78
7.9 Technology Viewpoint Tiketovací sytém / Evidencia a správa incidentov 78
7.10 Technology Viewpoint Znalostný portál pre SOC tím 81
7.11 Technologické komponenty riešenia a ich vzťah k aplikačným komponentom 83
7.11.1 Správa prístupov, účtov a kľúčov prevádzkových prostredí 83
7.11.2 Kontajnerizácia a orchestrácia cloudových služieb 83
7.11.3 Špecifikácia využitia služieb vládneho cloudu 83
7.12 Popis testovacieho prostredia 83
7.13 Popis produkčného prostredia 83
8 Požiadavky na úrovne služieb (SLA) a výkonnosť 83
9 Softvérové licencie a zdrojové kódy 83
10 Zabezpečenie dostupnost, zálohovanie a obnova riešenia 84
10.1 Zabezpečenie dostupnosti 84
10.2 Zálohovanie 85
10.3 Obnova riešenia 85
11 Bezpečnosť - riešenie požiadaviek na bezpečnosť 85
12 Migrácia dát 88
12.1 Postup vykonania migrácie dát 88
12.2 Overenie migrácie dát 88

13 Harmonogram realizácie a nasadenia, závislosti 88
13.1 Fázy projektu a časový harmonogram - konsolidovaný prehľad 88
13.2 Závislosti a návrh riešenia 88
13.3 Požiadavky na fázy Testovanie a Nasadenie do produkcie 88
14 Otvorené otázky 88
15 Prílohy 88

1 Použité skratky a pojmy

SKRATKA	POPIS
API	Application Programming Interface (Programové rozhranie aplikácie)
API GW	Modul procesnej integrácie a integrácie údajov - prístupová časť
CEP	Modul centrálnej elektronickej podateľne ÚPVS
CI/CD	Continuous integration/Continuous deployment – séria krokov pre správne nasadenie softvéru - Kontinuálna integrácia adodávka
CUET	Centrálna úradná elektronická tabuľa
e-Government	Electronical Government, elektronizácia verejnej správy
eDesk	Modul elektronických komunikačných schránok ÚPVS
eForm	Modul elektronických formulárov ÚPVS
G2G	Modul procesnej integrácie a integrácie údajov - komunikačná časť
GDPR	General Data Protection Regulation
GovNET	Zabezpečená štátna sieť spravovaná Národnou agentúrou pre sieťové a elektronické systémy. / Nadrezortná informačná sieť verejnej správy
GUI	Grafické používateľské rozhranie (Graphical user interface)
IAM	Identity Access Management - Správa identity používateľa. / Autentifikačný Modul v rámci ÚPVS
IDSK	Súbor pravidiel tvorby obsahu a funkčnosti elektronických služieb v súlade s potrebami používateľov.
KAV	Konsolidovaná analytická vrstva
MIRRI	Ministerstvo investícií, regionálneho rozvoja ainformatizácie
MoSCoW	M - Must have, S - Should have, C - Could have, W - Won't have. Technika na určovanie priorít požiadaviek v rámci projektového riadenia a vývoja software
NASES	Národná agentúra pre sieťové aelektronické služby
OVM	Orgán verejnej moci - štátny orgán, orgán územnej samosprávy, verejnoprávna inštitúcia, orgán záujmovej samosprávy a fyzická osoba alebo právnická osoba, ktorým zákon zveril výkon verejnej moci
PO/FO	Právnická osoba/Fyzická osoba
SkTalk/Sk-Talk	Štandard pre komunikáciu prostredníctvom ÚPVS podľa § 11 písm. g) Vyhlášky č. 78/2020 Z. z.
SLA	Service Layer/Level Agreement - Dohoda o úrovni/ parametroch / kvalite poskytovania služby
SvM	Slovensko vmobile
PROD	Produkčné prostredie
UAT	Testovacie prostredie
UIR	Univerzálne integračné rozhranie – asynchrónne rozhranie na príjem a odosielanie správ z a do ÚPVS
USR	Univerzálne synchrónne rozhranie pre sprístupnenie ostatných synchrónnych služieb modulov ÚPVS – zpohľadu poskytovateľa služieb ide orozhranie externej zbernice
ÚPVS	Ústrednýportál verejnej správy, ústredný portál
XML	Extensible Markup Language
WSDL	Web Services Description Language
ZEP/KEP	Zaručený elektronický podpis / Kvalifikovaný elektronický podpis
ŽS	Životná situácia

POJEM/REFERENCIA	POPIS
ArchiMate	Štandardizovaný modelovací jazyk, ktorý sa používa primárne na zobrazenie, popis anáslednú analýzu podnikovej architektúry.
Autentifikácia	Proces identifikácie a overenia identity používateľa, žiadajúceho oslužbu alebo zdroj, v informačnom systéme.
Autorizácia	Predstavuje overenie oprávnenia osôb, či objektov na prácu s dátami.
Dokumentácia ke-Notify	Na Partner Framework Portal (PFP) sa nachádza dokumentácia kmodulu e-Notify ÚPVS pre integračných partnerov, prístup do PFP portálu je umožnený na požiadanie.
Integračný manuál ke-Notify	Integračný manuál na e-Notify spopisom služieb vaktuálnej verzii na PFP portáli eNOTIFY - Všetky dokumenty (gov.sk) (gov.sk)
KAV	KAV - Konsolidovaná analytická vrstva | Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (gov.sk)
MetaIS/METAIS	Centrálny metainformačný systém verejnej správy
Notifikácia	Notifikácia je informačný signál alebo správa, ktorá je posielaná používateľovi s cieľom upozorniť ho na nejakú udalosť, aktivitu alebo potrebu zasiahnutia.
eGOV,e-Government	Electronical Government, elektronizácia verejnej správy
OpenID Connect (OIDC), OAuth2	RFC 6749 (The OAuth 2.0 Authorization Framework), štandard pre autentifikáciu a určenie rozsahu oprávnení pri použití protokolu REST podľa Vyhlášky o štandardoch 78/2020, §11, písm. i)
Pravidlá publikovania elektronických služieb	Pravidlápublikovania elektronických služiebdo multikanálového prostredia verejnej správy https://mirri.gov.sk/wp-content/uploads/2018/10/Pravidla_Publikovania_Sluzieb_v1_0-1.pdf
Representational State Transfer (REST)	Protokol sieťovej komunikácie pri poskytovaní elektronických služieb potrebných na spracovanie elektronických podaní alebo úspešné vyplnenie a prípravu elektronického podania prostredníctvom modulu procesnej integrácie a integrácie údajov podľa Vyhlášky o štandardoch 78/2020, §11, písm. a)
Spätná kompatibilita	Vtechnickej praxi, vlastnosť produktu, spočívajúca v tom, že produkt dokáže nahradiť svojho predchodcu tak, že je naďalej schopný spolupracovať s produktami, ktoré boli vytvorené pre tento starší produkt. Novší produkt teda dokáže plnohodnotne nahradiť svojho predchodcu.
ŽS	Prioritné životné situácie | Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (gov.sk)

2 Manažérske zhrnutie

2.1 Zámer riešenia

2.2 Ciele riešenia

2.3 Merateľné a výkonnostné ukazovatele (KPI)

2.4 Rozsah riešenia

2.5 Mimo rozsah projektu

2.6 Stručný popis navrhovaného riešenia

2.7 Sumarizácia výstupu M-06 navrhovaného riešenia

2.7.1 Prehľad koncových služieb – budúci stav

Kód KS (z MetaIS)	Názov KS	Používateľ KS (G2C/G2B/G2G/G2A)	Životná situácia (+ kód zMetaIS)	Úroveň elektronizácie KS

Tabuľka 1 Prehľad koncových služieb – budúci stav

2.7.2 Rozsah informačných systémov – budúci stav

Kód ISVS (z MetaIS)	Názov ISVS	Modul ISVS (zaškrtnite ak ISVS je modulom)	Stav IS VS	Typ IS VS	Kód nadradeného ISVS (vprípade zaškrtnutého checkboxu pre modul ISVS)

Tabuľka 2 Rozsah informačných systémov – budúci stav

2.7.3 Prehľad plánovaných integrácií ISVS na nadrezortné ISVS – spoločné moduly podľa zákona č. 305/2013 e-Governmente – budúci stav

Kód IS	Názov ISVS	Spoločné moduly podľa zákona č. 305/2013 e-Governmente

Tabuľka 3 Prehľad plánovaných integrácií ISVS na nadrezortné ISVS

2.7.4 Prehľad plánovaného využívania iných ISVS (integrácie) – budúci stav

Kód ISVS *(z MetaIS)*	Názov ISVS	Kód integrovaného ISVS *(z MetaIS)*	Názov integrovaného ISVS

Tabuľka 4 Prehľad plánovaného využívania iných ISVS (integrácie)

2.7.5 Aplikačné služby pre realizáciu koncových služieb – budúci stav

Kód AS *(zMetaIS)*	Názov AS	ISVS/modul ISVS *(kód zMetaIS)*	Aplikačná služba realizuje KS *(kód KS zMetaIS)*

Tabuľka 5 Aplikačné služby pre realizáciu koncových služieb

2.7.6 Aplikačné služby na integráciu – budúci stav

AS (Kód MetaIS)	Názov AS	Realizuje ISVS (kód MetaIS)	Poskytujúca alebo Konzumujúca	Integrácia cez CAMP	Integrácia sIS tretích strán	SaaS	Integrácia na AS poskytovateľa (kód MetaIS)

Tabuľka 6 Aplikačné služby na integráciu

3 Analýza požiadaviek

3.1 Postup analýzy požiadaviek

Pri vývoji architektúry je v rámci tohoto projektu použitý rámec TOGAF a jazyk Archimate. Využívanie komponentov rámca TOGAF bolo pre účely tohoto projektu prispôsobené. Z rámca bola predovšetkým prevzatá časť metódy pre vývoj architektúry (Architecture Development Method) týkajúca sa vývoja architektúry vo všetkých štyroch architektonických doménach. Metóda pre vývoj architektúry predstavuje proces s doporučenými krokmi a aktivitami. Aj keď je ADM často spájaný s iteratívnymi a agilnými prístupmi, s ohľadom na ciele a charakter tohto projektu bola prispôsobená metodike Waterfall, ktorá je sekvenčná a lineárna.

Projekt je vyvíjaný v jednotlivých na seba nadväzujúcich fázach.

Vrámci prvej fázy sa realizuje analýza požiadaviek, ktoré definujú očakávania používateľov azainteresovaných strán.

Počas druhej fázy sa požiadavky transformujú do návrhu architektúry systému, ktorý definuje ako bude systém fungovať. Návrh prebieha vdvoch úrovniach. High level návrh rozhoduje o celkovej štruktúre systému, ako sú hlavné komponenty a spôsob ich vzájomného prepojenia. Detailná špecifikácia podrobnejšie popisuje každý modul alebo komponent, vrátane dátových modelov, algoritmov, rozhraní alogických tokov. Tento návrh je podrobený schváleniu, aby sa zabezpečilo, že spĺňa požiadavky a rešpektuje technologické, finančné a legislatívne obmedzenia.

Po jeho pripomienkovaní aschválení začína fáza implementácie. Počas nej sa implementujú jednotlivé moduly systému podľa špecifikácie, pri písaní kódu sa uplatňujú štandardy kvality a bezpečnosti. Priebežné testovanie každého modulu zabezpečí UNIT testovanie. Fáza implementácie prebehne vdvoch krokoch. Vprvom kroku sa nasadí verzia aplikácie obsahujúca funkčnosť, ktorá pokrýva stanovené funkčné požiadavky avykoná sa kontrola aschválenie prvej fázy implementácie. Vdruhom kroku sa vykoná implementácia ostávajúcej funkčnosti aintegrácia na existujúce moduly.

Ďalšia fáza zabezpečí otestovanie systému. Overí sa, že všetky komponenty spolupracujú správne a že systém ako celok plní požiadavky definované v úvodnej fáze.

Po úspešnom testovaní sa systém nasadzuje do produkčného prostredia. Tento proces zahŕňa inštaláciu softvéru a konfiguráciu prostredia. Súčasťou tejto fázy je aj školenie používateľov, aby vedeli systém efektívne využívať.

Po nasadení sa systém monitoruje a priebežne sa aktualizuje podľa potrieb používateľov a technologických zmien. Údržba zahŕňa opravu chýb, implementáciu nových funkcií a optimalizáciu výkonu. Proces údržby musí rešpektovať všetky legislatívne požiadavky, napríklad zabezpečenie ochrany osobných údajov a kybernetickú bezpečnosť.

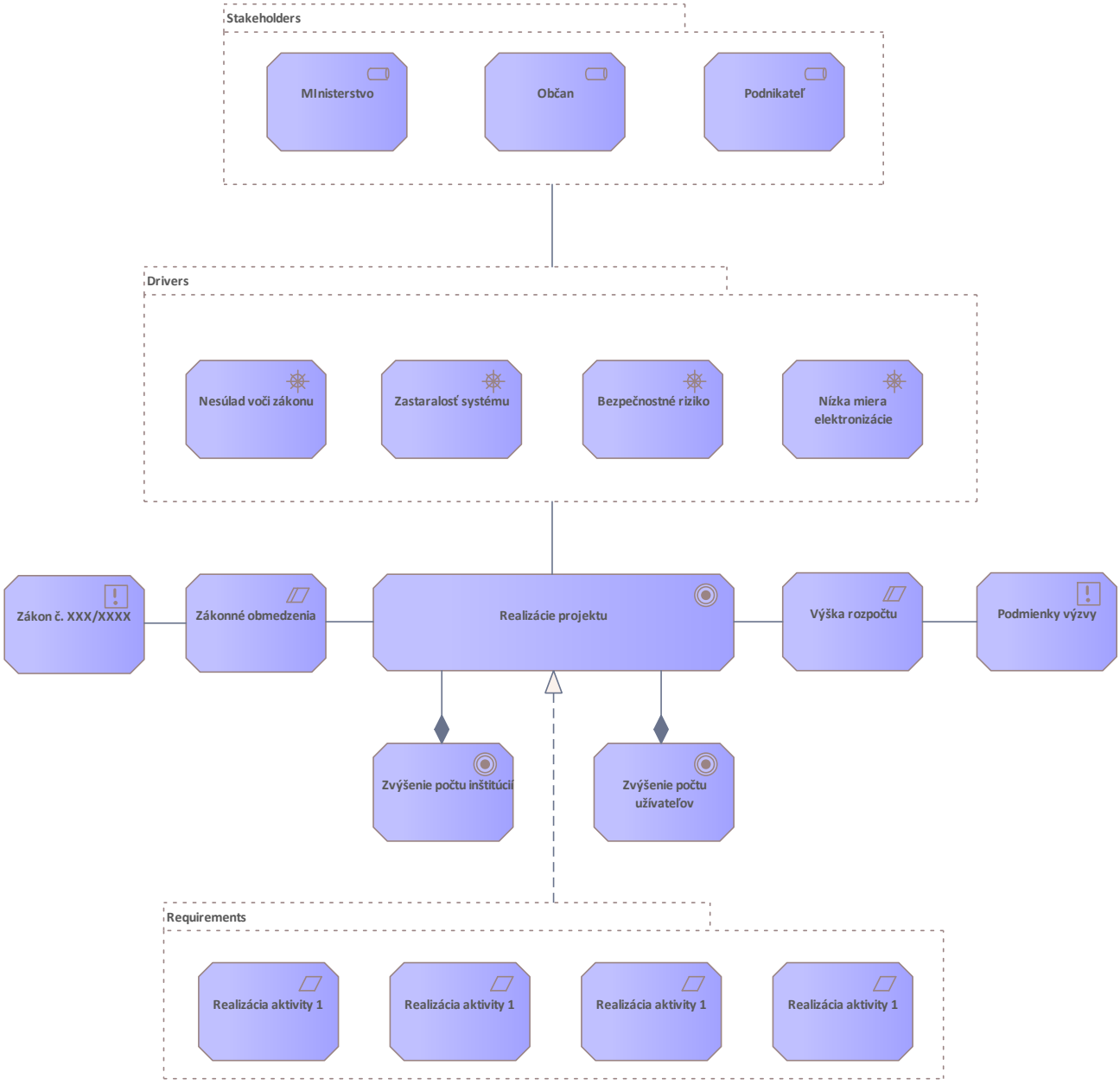
Pre dizajn vyvíjaných aplikačných komponentov je použitý nástroj Enterprise Architect.

3.2 Používateľský prieskum

3.3 Motivačná architektúra

3.3.1

3.4 Motivation Viewpoints



Obrázok 1 : Motivation Viewpoint

3.5 Katalóg požiadaviek a jeho mapovanie na návrh ich riešenia

Katalóg požiadaviek je definovaný ako príloha tohto dokumentu. Návrh riešenia požiadaviek je obsahom tohto dokumentu a je detailne popísaný v nasledujúcich kapitolách. Na základe katalógu požiadaviek vznikol dokument Plán testov, ktorý bude podkladom pre akceptáciu pri UAT testoch. Rozsah a plán testov je definovaný v dokumente Testovacia stratégia a zahŕňa:

- Funkčné testovanie (FAT) – na strane dodávateľa
- Systémové a integračné testovanie (dodávateľ, NASES môže byť účastný)
- Záťažové a výkonnostné testovanie
- Bezpečnostné testovanie
- Používateľské testy funkčného používateľského rozhrania (UX) a testovanie prístupnosti (nemusí byť povinné)
- Užívateľské akceptačné testovanie (UAT) – na strane objednávateľa / prijímateľa

Súčasťou bezpečnostných testov budú penetračné testy, z ktorých bude vytvorený formálny report.

Súhrn mapovanie požiadaviek na prípady použitia a objekty architektúry:

3.6 Legislatíva, smernice a metodické materiály zohľadnené v riešení

3.7 Akceptačné kritéria

4 Biznis architektúra

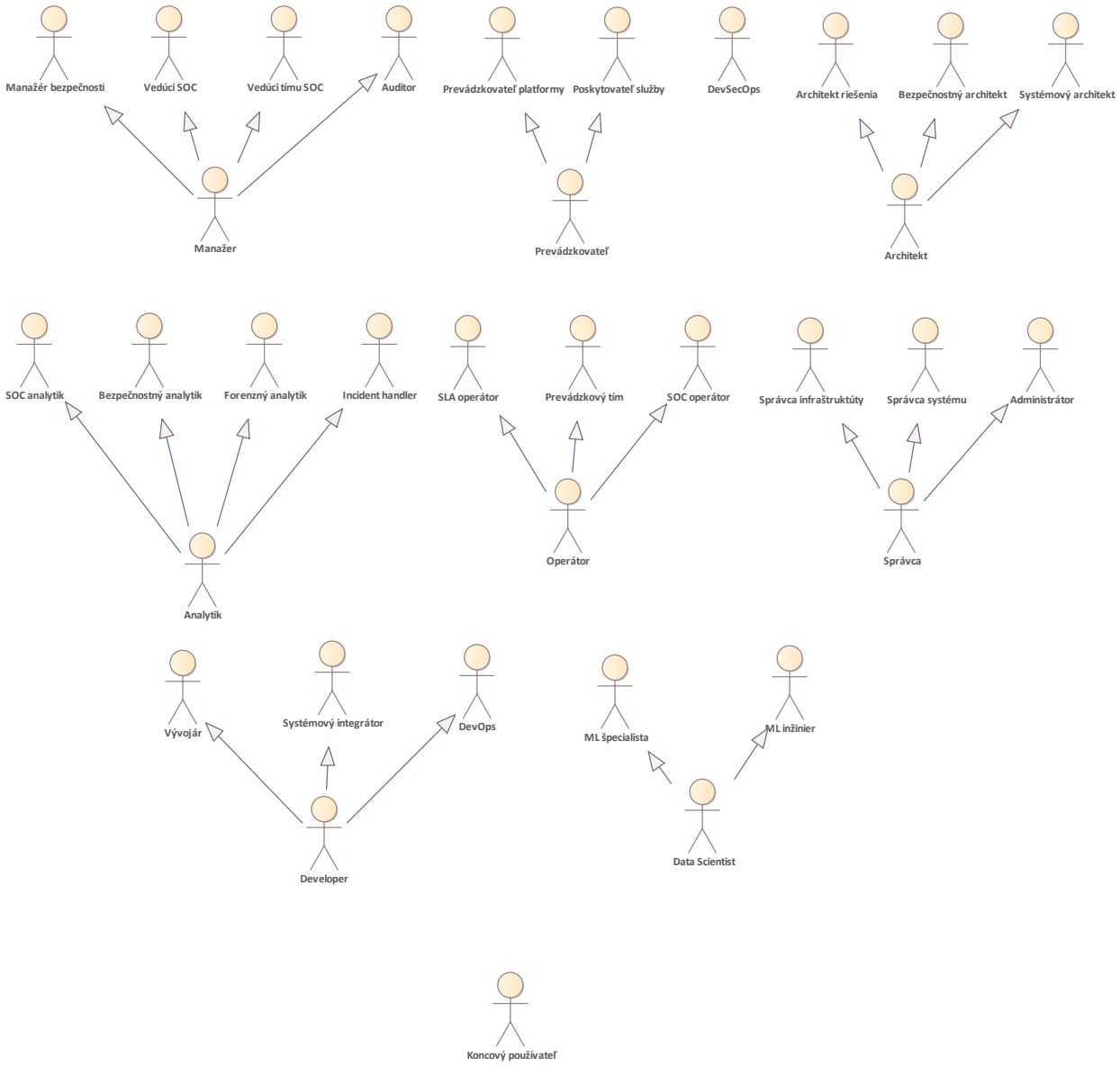
4.1 Biznis architektúra

4.2 BPMN - Biznis procesný model

4.3 Prípady použitia

V nasledujúcej kapitole sú uvedené jednotlivé používateľské scenáre.

4.3.1 Aktéri



Obrázok 2 : Aktéri

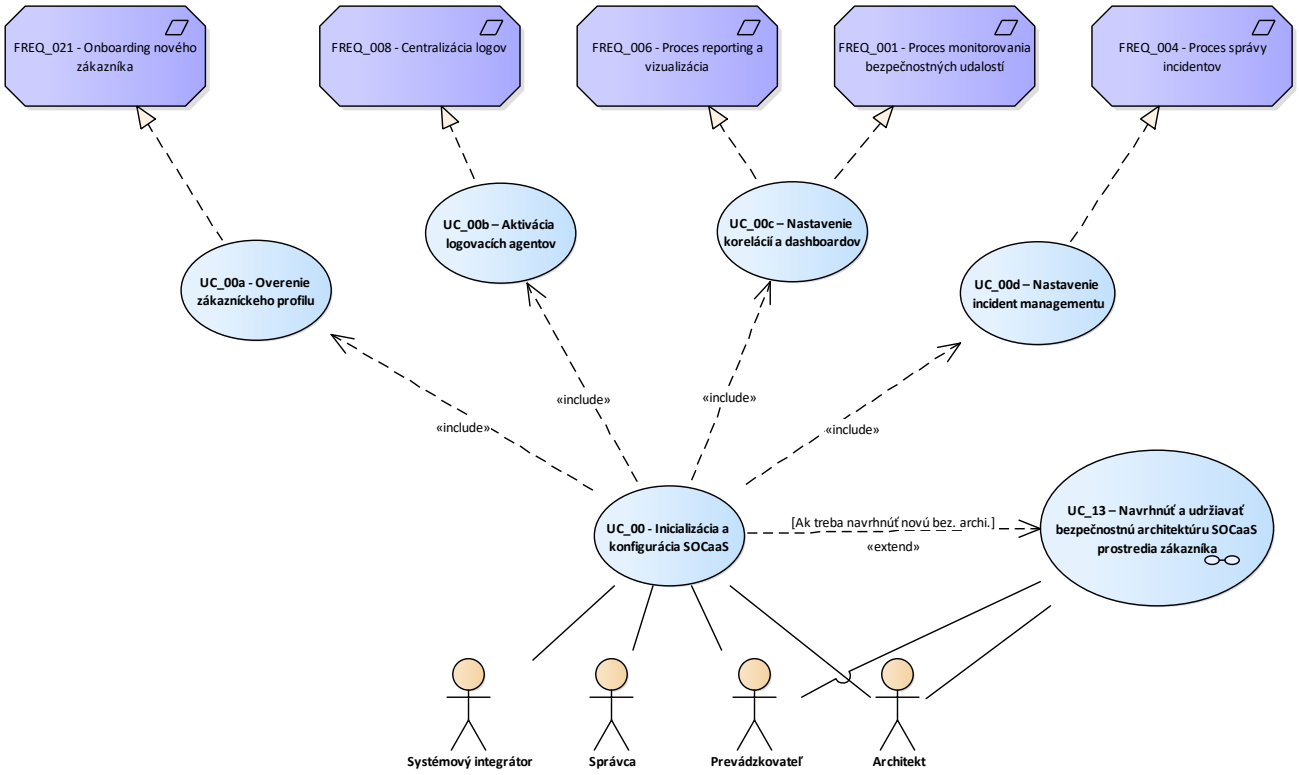
Názov aktéra/roly	**Popis**
Administrátor	Zodpovedá za: SIEM, spracovanie logov, vizualizácia dát, alertovanie, EDR/XDR, asset management, skener zraniteľnosti a zdroje bezpečnostných údajov.
Analytik	Zodpovedá za oblasti ako sú: Spracovanie logov, SOAR, Detekcia pomocou ML, Vizualizácia dát, Alertovanie, EDR/XDR, Asset management, Skener zraniteľnosti, knowledge base, Evidencia a správa incidentov a Reportovanie.
Architekt	Zodpovedá za oblasti ako sú: Detekcia pomocou ML a EDR/XDR.
Architekt riešenia	Zodpovedá za oblasti ako sú: SIEM a Spracovanie logov.
Auditor	Zodpovedá za oblasti ako sú: SIEM, SOAR, Asset management, Evidencia a správa incidentov, Reportovanie, Voliteľné rozšírenia, Administratíva systému, CTI a Alertovanie.
Bezpečnostný analytik	Zodpovedá za oblasti ako sú: SIEM, Spracovanie logov, SOAR, Detekcia pomocou ML, Vizualizácia dát, Alertovanie, EDR/XDR, CTI, Asset management, Skener

Názov aktéra/roly	Popis
	zraniteľnosti, Zdroje bezpečnostntných údajov, Knowledge base, Ticketing a Evidencia a správa incidentov.
Bezpečnostný architekt	Zodpovedá za oblasti ako sú: SIEM, SOAR, Detekcia pomocou ML, Vizualizácia dát, EDR/XDR, Zdroje bezpečných údajov, Knowledge base, Evidencia a správa incidentov a Administratíva systému.
Data Scientist	Zodpovedá za oblasti ako sú: detekcia pomocou ML.
Developer	Developer je základná rola orientovaná na návrh, vývoj, úpravu a údržbu softvéru, skriptov a integračných riešení. Zameriava sa na implementáciu logiky, automatizáciu procesov a technickú podporu vývoja.
DevOps	Zodpovedá za oblasti ako sú: SIEM, Spracovanie logov, Detekcia pomocou ML, Skener zraniteľnosti, Zdroje bezpečnostných údajov, Administratíva systému a Voliteľné rozšírenia.
DevSecOps	Zodpovedá za oblasti ako sú: SOAR, CTI, Skener zraniteľnosti a administratíva systému.
Forenzný analytik	Zodpovedá za oblasti ako sú: voliteľné rozšírenia a EDR/XDR.
Incident handler	Zodpovedá za oblasti ako sú: SOAR a Evidencia a správaincidentov.
Koncový používateľ	Zodpovedá za oblasti ako sú: Vizualizácia dát.
Manažer	Zodpovedá za oblasti ako sú: SIEM, Detekcia pomocou ML, vizualizácia dát, alertovanie, Asset management, skener zraniteľnosti, knowledge base, Ticketing, Reportovanie a Voliteľné rozšírenia.
Manažér bezpečnosti	Zodpovedá za oblasti ako sú: SIEM, SOAR, Detekcia pomocou ML, Vizualizácia dát, Alertovanie, EDR/XDR, CTI, Asset management, Skener zraniteľnosti, Ticketing, Evidencia a správa incidentov, Reportovanie, Asministratíva systému a Voliteľné rozšírenia.
ML inžinier	Zodpovedá za oblasti ako sú: detekcia pomocou ML.
ML špecialista	Zodpovedá za oblasti ako sú: detekcia pomocou ML a EDR/XDR.
Operátor	Zodpovedá za oblasti ako sú: alertovanie, EDR/XDR, CTI, asset management, skener zraniteľnosti, zdroje bezpečnostných údajov, knowledge base, ticketing a administratíva systému.
Poskytovateľ služby	Zodpovedá za oblasti ako sú: SIEM.
Prevádzkovateľ	Zodpovedá za oblasti ako sú: vizualizácia dát.
Prevádzkovateľ platformy	Zodpovedá za oblasti ako sú: SIEM.
Prevádzkový tím	Zodpovedá za oblasti ako sú: alertovanie a voliteľné rozšírenia.
SLA operátor	Zodpovedá za oblasti ako sú: alertovanie.
SOC analytik	Zodpovedá za oblasti ako sú: EDR/XDR, CTI, evidencia a správa incidentov, reportovanie a voliteľné rozšírenia.
SOC operátor	Zodpovedá za oblasti ako sú: alertovanie, EDR/XDR, knowledge base a ticketing.
Správca	Správca je základná technická rola zodpovedná za prevádzku, údržbu a fungovanie IT infraštruktúry a systémov. Zastrešuje kompetencie od infraštruktúry, cez správu systémov, až po administráciu konfigurácií.
Správca infraštruktúty	Zodpovedá za oblasti ako sú: Spracovanie logov, Asset management a Administratíva systému.
Správca systému	Zodpovedá za oblasti ako sú: SOAR, Vizualizácia dát, alertovanie, EDR/XDR, Asset management, Skener zraniteľností, Zdroje bezpečnostných údajov, Knowledge base, Ticketing, Evidencia a správa incidentov, Reportovanie a Administratíva systémuvizualizácia dát.
Systémový architekt	Zodpovedá za oblasti ako sú: SIEM, Spracovanie logov, SOAR, Detekcia pomocou ML, Skener zraniteľnosti a

Názov aktéra/roly	Popis
	Administratíva systému.
Systémový integrátor	Zodpovedá za oblasti ako sú: SIEM, Spracovanie logov, SOAR, Detekcia pomocou ML, Vizualizácia dát, Alertovanie, EDR/XDR, CTI, Asset management, Skener zraniteľnosti, Zdroje bezpečnostných údajov, Knowedge base, Ticketing a Evidencia a správa incidentov.
Vedúci SOC	Zodpovedá za oblasti ako sú: alertovanie.
Vedúci tímu SOC	Zodpovedá za oblasti ako sú: vizualizácia dát.
Vývojár	Zodpovedá za oblasti ako sú: SIEM, SOAR, Detekcia pomocou ML a Zdroje bezpečnostných údajov.

4.3.2 Všeobecné prípady použitia

4.3.2.1.1 UC_00 - Inicializácia a konfigurácia SOCaaS



Obrázok 3 : UC_00 - Inicializácia a konfigurácia SOCaaS

Prípad použitia	UC_00 - Inicializácia a konfigurácia SOCaaS
Cieľ	Use case popisuje prvotnú inicializáciu a nastavenie SOCaaS pre nového zákazníka. Zahŕňa aktiváciu logovacích zdrojov, nastavenie integračných bodov, dashboardov a základných bezpečnostných procesov.
Vstupná podmienka	Zákazník má vytvorený tenant.
Vstupná podmienka	SOC architekt má konfiguračné oprávnenia.
Vstupná podmienka	Základná sieťová konektivita je dostupná.
Výstupná podmienka	SOCaaS je úspešne inicializovaný a pripravený na monitorovanie a detekciu.
Výstupná podmienka	Aktivované sú základné moduly: logovanie, SIEM korelácie, dashboardy, incident management.
Basic Path	Basic Path

Krok	Aktivita
1	SOC architekt spustí proces inicializácie pre nového zákazníka.
2	Systém načíta profil zákazníka a pripraví konfiguračné rozhranie.
3	Architekt zvolí moduly, ktoré sa majú aktivovať (SIEM, SOAR, CTI, Ticketing).
4	Systém vykoná inicializačné úkony (registrácia zdrojov, aktivácia agentov, vytváranie dashboardov).
5	Architekt potvrdí konfiguráciu.
6	Systém uloží konfiguráciu a oznámi úspešné dokončenie.

ALT01 – Neúplný profil zákazníka	Alternate
Krok	**Aktivita**
1	Systém zistí chýbajúce údaje.
2	Upozorní architekta na doplnenie.
3	Proces pokračuje po doplnení informácií.

ALT02 – Nedostupné logovacie zdroje / infra	Alternate
Krok	**Aktivita**
1	Systém nedokáže nadviazať spojenie s logovacím agentom alebo API zákazníka.
2	Zobrazí chybu a ponúkne možnosť opakovať, alebo preskočiť modul.
3	Proces pokračuje s obmedzenou funkcionalitou.

Prípad použitia	UC_00a - Overenie zákazníckeho profilu
Cieľ	Systém overí, či zákaznícky tenant obsahuje všetky povinné údaje (identifikačné, technické, integračné).
Vstupná podmienka	Tenant existuje v systéme.
Výstupná podmienka	Profil zákazníka je potvrdený ako kompletný.
Basic Path	Basic Path
Krok	**Aktivita**
1	Prevádzkovateľ platformy spustí overenie profilu.
2	Systém načíta údaje zákazníka.
3	Systém skontroluje povinné polia. Systém skontroluje povinné polia.
4	Overenie je úspešné.

ALT01 – Neúplné údaje	Alternate
Krok	**Aktivita**

1	systém vyžiada doplnenie.

ALT02 – Tenantu chýba technická konfigurácia	Alternate
Krok	**Aktivita**
1	systém zastaví proces a upozorní správcu.

Prípad použitia	UC_00b – Aktivácia logovacích agentov
Cieľ	Systém aktivuje logovacích agentov zákazníka pre odosielanie logov do SOCaaS.
Vstupná podmienka	Zákaznícke systémy sú dostupné.
Vstupná podmienka	Komunikačné kanály sú otvorené.
Výstupná podmienka	Logovacie agenty sú aktívne a odosielajú dáta.
Basic Path	Basic Path
Krok	**Aktivita**
1	Prevádzkovateľ platformy spustí aktiváciu.
2	Systém kontaktuje logovacích agentov.
3	Overí sa dostupnosť API a certifikátov.
4	Agenti sú aktivovaní.

ALT01 – Agent neodpovedá	Alternate
Krok	**Aktivita**
1	systém oznámi chybu, pokračuje neskôr.

ALT02 – Chybné API kľúče	Alternate
Krok	**Aktivita**
1	vyžaduje sa opätovné nahratie kľúčov.

Prípad použitia	UC_00c – Nastavenie korelácií a dashboardov
Cieľ	Systém vytvorí preddefinované korelačné pravidlá a dashboardy pre monitoring bezpečnostných udalostí.
Vstupná podmienka	SIEM modul je aktívny.
Vstupná podmienka	Logy prichádzajú do systému.
Výstupná podmienka	Korelačné pravidlá a dashboardy sú nakonfigurované.
Basic Path	Basic Path
Krok	**Aktivita**
1	Prevádzkovateľ platformy spustí nastavenie.
2	Systém načíta template korelácií.

3	Systém vytvorí dashboardy pre monitorovanie.
4	Konfigurácia je uložená.

ALT01 – Korelačné pravidlo je neplatné	Alternate
Krok	**Aktivita**
1	systém ho preskočí a nahlási chybu.

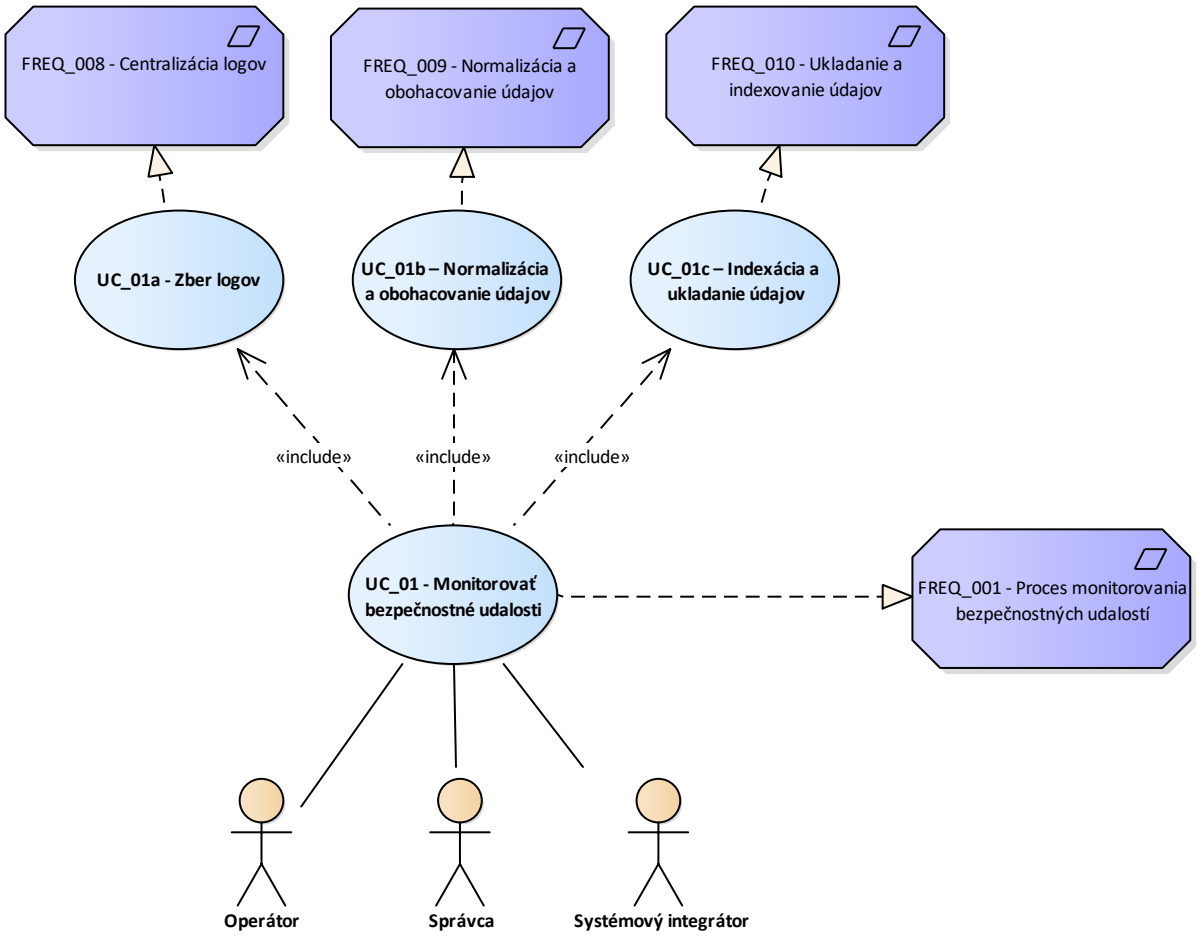
ALT02 – Dashboard sa nedá vytvoriť	Alternate
Krok	**Aktivita**
1	systém vytvorí len minimálnu verziu.

Prípad použitia	UC_00d – Nastavenie incident managementu
Cieľ	Systém aktivuje workflow pre správu incidentov a priradenia rolí.
Vstupná podmienka	Ticketing alebo SOAR modul je inicializovaný.
Výstupná podmienka	Incident lifecycle (triage → analýza → uzavretie) je pripravený.
Basic Path	Basic Path
Krok	**Aktivita**
1	Prevádzkovateľ platformy spustí konfiguráciu.
2	Systém načíta workflow šablóny.
3	Systém vytvorí incidentné kategórie a priority.
4	Priradí roly (Analytik, Operátor, Manažér).

ALT01 – Neexistujú roly používateľov	Alternate
Krok	**Aktivita**
1	systém zastaví workflow a požiada správcu o pridanie rolí.

ALT02 – Ticketing modul je nedostupný	Alternate
Krok	**Aktivita**
1	systém aktivuje len základný SOAR fallback.

4.3.2.1.2 UC_01 - Monitorovať bezpečnostné udalosti



Obrázok 4 : UC_01 Monitorovať bezpečnostné udalosti

Prípad použitia	UC_01 - Monitorovať bezpečnostné udalosti
Cieľ	Use case opisuje nepretržité monitorovanie bezpečnostných udalostí v rámci SOCaaS. Zahŕňa zber udalostí, ich normalizáciu, obohacovanie a prípravu alertov pre následný proces detekcie incidentov.
Vstupná podmienka	Logovacie agenty sú aktívne.
Vstupná podmienka	SIEM modul SOCaaS je funkčný.
Vstupná podmienka	UC_00 (inicializácia) bol úspešne dokončený.
Výstupná podmienka	Udalosti sú spracované a posunuté do procesu detekcie incidentov.
Výstupná podmienka	Alerty sú zobrazené operátorovi.
Výstupná podmienka	Monitoring beží v reálnom čase.

Basic Path	Basic Path

Krok	**Aktivita**
1	Operátor sleduje riadiaci dashboard v SOCaaS.
2	UC_01a: Systém prijíma udalosti z logovacích zdrojov.
3	UC_01b: Systém normalizuje a obohacuje dáta.
4	UC_01c: Systém ukladané údaje indexuje pre rýchle vyhľadávanie.

5	SOCaaS generuje alerty na základe korelačných pravidiel.
6	Operátor vidí výsledné bezpečnostné udalosti.
7	Use case končí, monitoring pokračuje bez obmedzenia. Operátor vyhodnotí alert.
8	Ak je kritický → aktivuje UC_01x Eskalácia incidentu.
9	Use Case končí – monitoring pokračuje ďalej.

ALT01 – Nedostupné logy alebo agenti	Exception
Krok	**Aktivita**
1	SOCaaS nedostáva dáta zo zdroja.
2	Systém vytvorí „Missing logs“ alert.
3	Správca je upozornený a môže problém manuálne vyriešiť.

ALT02 – Preťažený SIEM alebo pipeline	Exception
Krok	**Aktivita**
1	SOCaaS nestíha spracovávať prúd udalostí.
2	Systém zapne ochranné mechanizmy (rate-limiting, buffering).
3	Operátor je upozornený o riziku straty udalostí.

Prípad použitia	UC_01a - Zber logov
Cieľ	Zabezpečuje technický príjem logovacích dát zo systémov, aplikácií, zariadení a zdrojov do SIEM platformy. Je základom monitorovacieho procesu.
Vstupná podmienka	Komunikačný kanál medzi systémom a agentom je funkčný.
Vstupná podmienka	Logovací agent je aktívny.
Výstupná podmienka	Logy sú pripravené na ďalší krok – normalizáciu.
Výstupná podmienka	SOCaaS prijal nové logy.
Basic Path	Basic Path
Krok	**Aktivita**
1	Logovací agent odosiela bezpečnostné udalosti.
2	SOCaaS prijme dáta.
3	Overí sa formát a integrita logov.
4	Logy sú odovzdané do procesu normalizácie.

ALT01 – Logy sa nedoručujú	Alternate
Krok	**Aktivita**

1	SOCaaS nezaznamená žiadne dáta zo zdroja.
2	Systém vytvorí „Missing logs“ upozornenie.
3	Správca dostane notifikáciu.

ALT02 – Nevalidný formát logu	Alternate
Krok	**Aktivita**
1	Log má chybný formát alebo chýbajúce polia.
2	SOCaaS ho odmietne a uloží do quarantine bufferu.
3	Notifikácia sa pošle integrátorovi.

Prípad použitia	UC_01b – Normalizácia a obohacovanie údajov
Cieľ	Use case zabezpečuje normalizáciu logov do jednotného formátu a obohacovanie informáciami z CTI, asset databázy alebo užívateľských údajov.
Vstupná podmienka	Existuje konfigurácia normalizačných pravidiel.
Vstupná podmienka	UC_01a (zber logov) bol úspešný.
Výstupná podmienka	Log je normalizovaný a obohatený.
Výstupná podmienka	Dáta sú pripravené na uloženie a indexáciu.

Basic Path	Basic Path
Krok	**Aktivita**
1	SOCaaS načíta prijaté logy.
2	Použije sa normalizačný profil podľa typu zdroja.
3	Obohatenie dát (IP reputácia, hostname, používateľ).
4	Výsledný event je pripravený pre indexáciu.

ALT01 – Neznámy typ logu	Alternate
Krok	**Aktivita**
1	systém použije fallback normalizačný profil.

ALT02 – Chýba CTI feed	Alternate
Krok	**Aktivita**
1	systém vykoná normalizáciu bez obohatenia a označí event ako „unenriched“.

Prípad použitia	UC_01c – Indexácia a ukladanie údajov
Cieľ	Use case sa stará o uloženie normalizovaných bezpečnostných udalostí do úložiska a ich indexáciu pre rýchle vyhľadávanie a korelačné mechanizmy.
Vstupná podmienka	Normalizácia dát (UC_01b) je dokončená.
Vstupná podmienka	Úložisko a cluster sú dostupné.

Výstupná podmienka	Udalosti sú uložené v SIEM databáze.
Výstupná podmienka	Indexy sú pripravené pre query systémy.

Basic Path	Basic Path

Krok	**Aktivita**
1	Systém prevezme normalizované dáta.
2	Zapíše ich do úložiska (DB alebo distrib. index).
3	Vytvorí/aktualizuje indexy.
4	Event je k dispozícii pre korelačné pravidlá.

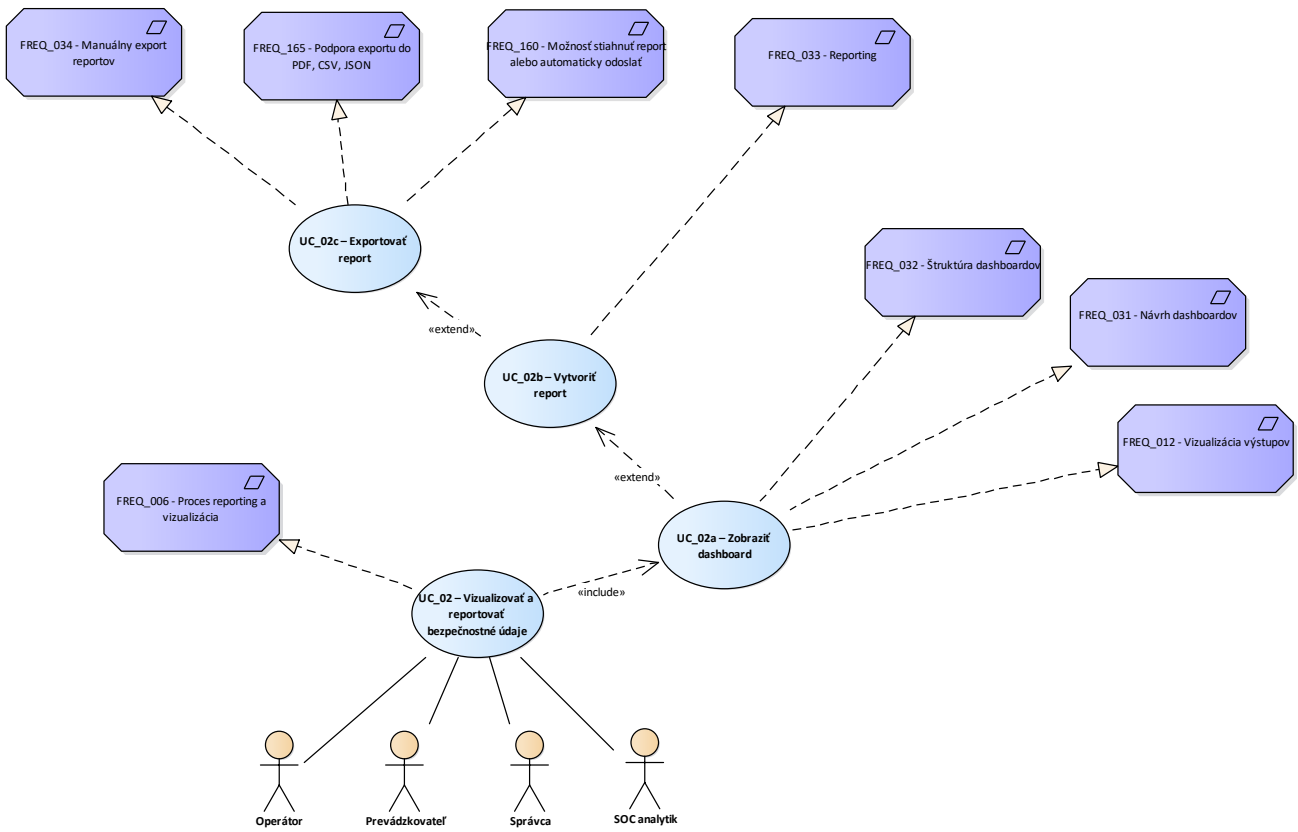
ALT01 – Úložisko nedostupné	Alternate

Krok	**Aktivita**
1	Systém uloží dáta do bufferu a vytvorí alert.

ALT02 – Vyčerpanie úložného priestoru	Alternate

Krok	**Aktivita**
1	Systém aktivuje cleanup alebo alertuje prevádzku.

4.3.2.1.3 UC_02 - Vizualizovať a reportovať bezpečnostné údaje



Obrázok 5 : UC_02 - Vizualizovať a reportovať bezpečnostné údaje

Prípad použitia	UC_02 – Vizualizovať a reportovať bezpečnostné údaje
Cieľ	Systém umožňuje SOC operátorom a správcovi zobrazovať bezpečnostné udalosti pomocou dashboardov, filtrov, grafov a tabuľkových výstupov. Umožňuje tiež generovanie reportov a export dát pre manažment, audit alebo zákazníkov.
Vstupná podmienka	Dashboardy sú definované v konfigurácii (UC_00c).
Vstupná podmienka	UC_01c – Dáta sú indexované a dostupné pre vizualizáciu.
Vstupná podmienka	UC_01 – Monitorovanie beží a poskytuje dáta.
Výstupná podmienka	Aktivita je zaznamenaná v audit logu.
Výstupná podmienka	Report bol vygenerovaný alebo exportovaný (ak bolo iniciované).
Výstupná podmienka	Používateľ vidí aktualizované vizualizácie.

Basic Path	Basic Path

Krok	**Aktivita**
1	Aktér otvorí modul „Vizualizácia a reporting“.
2	Systém načíta dostupné dashboardy a reporty podľa role aktéra.
3	Aktér otvorí dashboard → systém zobrazí grafy, metriky, tabuľky.
4	Aktér môže aplikovať filtre (čas, typ udalosti, zdroj).
5	Aktér môže kliknúť na „Vytvoriť report“.
6	Systém zostaví report podľa vybraného formátu a šablóny.
7	Aktér môže použiť funkciu „Exportovať report“ (PDF, CSV, JSON).

ALT01 – Nedostupné dáta	Alternate

Krok	**Aktivita**
1	Dashboard vráti prázdny dataset.
2	Systém zobrazí varovanie.
3	Aktér môže zmeniť filtračné kritériá.

ALT02 – Chybné oprávnenia	Alternate

Krok	**Aktivita**
1	Aktér (napr. Prevádzkovateľ) otvorí dashboard mimo jeho tenantu.
2	Systém zobrazí chybu „Nedostatočné oprávnenia“.

ALT03 – Generovanie reportu zlyhalo	Alternate

Krok	**Aktivita**
1	Zobrazí chybové hlásenie.
2	Uloží chybu do audit logu.

3	Aktér (napr. Prevádzkovateľ) otvorí dashboard mimo jeho tenantu.

Prípad použitia	UC_02a – Zobraziť dashboard
Cieľ	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.
Vstupná podmienka	Systém je inicializovaný a nakonfigurovaný (UC_00).
Vstupná podmienka	Všetky zdroje logov sú aktívne a dáta sú prijímané (UC_01).
Vstupná podmienka	Používateľ je autentifikovaný a má rolu umožňujúcu zobrazenie dashboardov.
Výstupná podmienka	Dashboard bol zobrazený s aktuálnymi dátami.
Výstupná podmienka	Používateľ môže filtre, pohľady alebo sekcie uložiť (ak má oprávnenie).

Basic Path	Basic Path
Krok	**Aktivita**
1	Aktér otvorí modul Dashboardov.
2	Systém načíta dostupné dashboardy podľa roly.
3	Aktér vyberie dashboard na zobrazenie.
4	Systém načíta a zrenderuje vizualizácie (grafy, heatmapy, tabuľky).
5	Systém aktualizuje vizualizácie v reálnom čase alebo v definovaných intervaloch.

ALT_01 – Nenačítajú sa dáta	Alternate
Krok	**Aktivita**
1	Systém zistí nedostupnosť zdrojov.
2	Namiesto grafov zobrazí správu: „Dáta nie sú dostupné.“
3	Ponúkne obnoviť alebo prepnúť zdroj.

ALT_02 – Používateľ nemá oprávnenie na konkrétny dashboard	Alternate
Krok	**Aktivita**
1	Systém skryje dashboard alebo zobrazí „Access Denied“.
2	Aktér musí požiadať administrátora o prístup.

Prípad použitia	UC_02b – Vytvoriť report
Cieľ	Používateľ vytvorí jednorazový report alebo uloží reportovaciu šablónu založenú na dátach z dashboardov alebo udalostí.
Vstupná podmienka	Dashboardy sú dostupné a dáta sú indexované (UC_01).
Vstupná podmienka	Používateľ má oprávnenie „Create Report“.
Výstupná podmienka	Report je uložený v systéme.
Výstupná podmienka	Môže byť zobrazený, upravený alebo exportovaný (UC_02c).

Basic Path	Basic Path
Krok	**Aktivita**
1	Aktér otvorí modul Reportov.
2	Zvolí „Vytvoriť nový report“.
3	Vyberie: typ reportu, časový rozsah, šablónu alebo vlastný dizajn.
4	Systém načíta potrebné dáta.
5	Používateľ potvrdí generovanie.
6	Systém vygeneruje report a uloží ho do databázy reportov.

ALT_01 – Nevalidný parameter reportu	Alternate
Krok	**Aktivita**
1	Systém zistí chýbajúci parameter (časové obdobie, zdroj dát...).
2	Zobrazí chybu a vyžiada doplnenie.

ALT_02 – Nedostupné dáta pre report	Alternate
Krok	**Aktivita**
1	Systém zobrazí hlásenie „Dáta pre vybrané obdobie nie sú dostupné“.
2	Aktér zvolí iné obdobie.

Prípad použitia	UC_02c – Exportovať report
Cieľ	Používateľ exportuje existujúci report do PDF, CSV, JSON alebo PNG a môže ho odoslať emailom alebo webhookom.
Vstupná podmienka	Existuje vygenerovaný report (UC_02b).
Vstupná podmienka	Používateľ má práva „Export Report“.
Výstupná podmienka	Systém vytvoril súbor vo zvolenom formáte.
Výstupná podmienka	Súbor bol stiahnutý alebo odoslaný na externý endpoint.

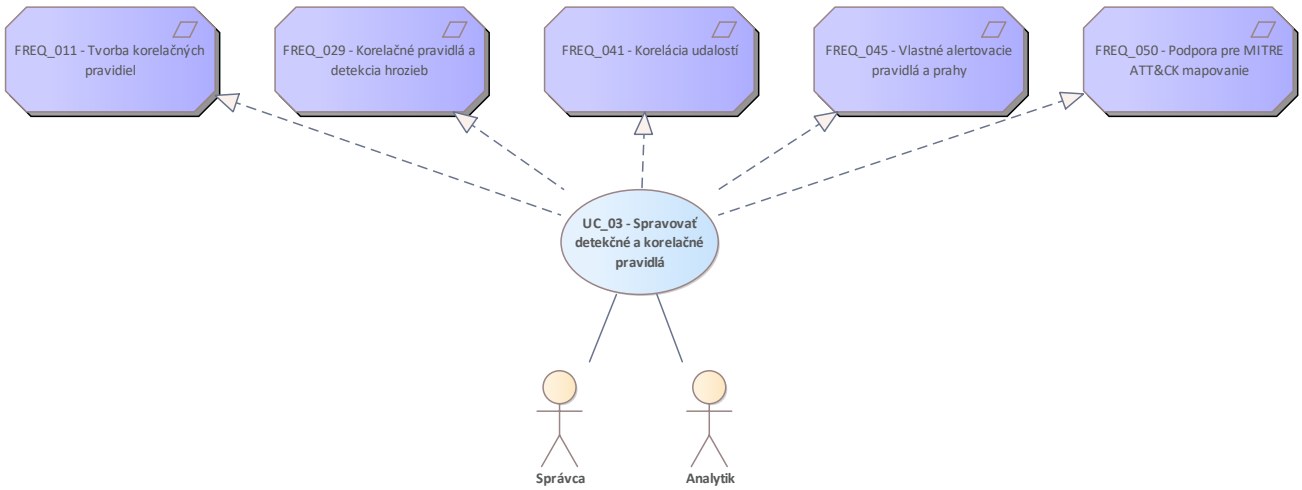
Basic Path	Basic Path
Krok	**Aktivita**
1	Používateľ otvorí detail reportu.
2	Zvolí možnosť Exportovať.
3	Vyberie formát (PDF/CSV/JSON/PNG).
4	Systém vygeneruje export.
5	Súbor sa stiahne alebo odošle podľa nastavenia.

ALT_01 – Export zlyhá (timeout, veľký dataset)	Alternate

Krok	Aktivita
1	Systém oznámi chybu exportu.
2	Ponúkne offline export alebo rozdelenie dát.

ALT_02 – Nedostatočné oprávnenia	Alternate
Krok	**Aktivita**
1	Systém zobrazí „Access Denied“.
2	Ponúkne požiadať o prístup.

4.3.2.2 UC_03 - Spravovať detekčné a korelačné pravidlá



Obrázok 6 : UC_03 - Spravovať detekčné a korelačné pravidlá

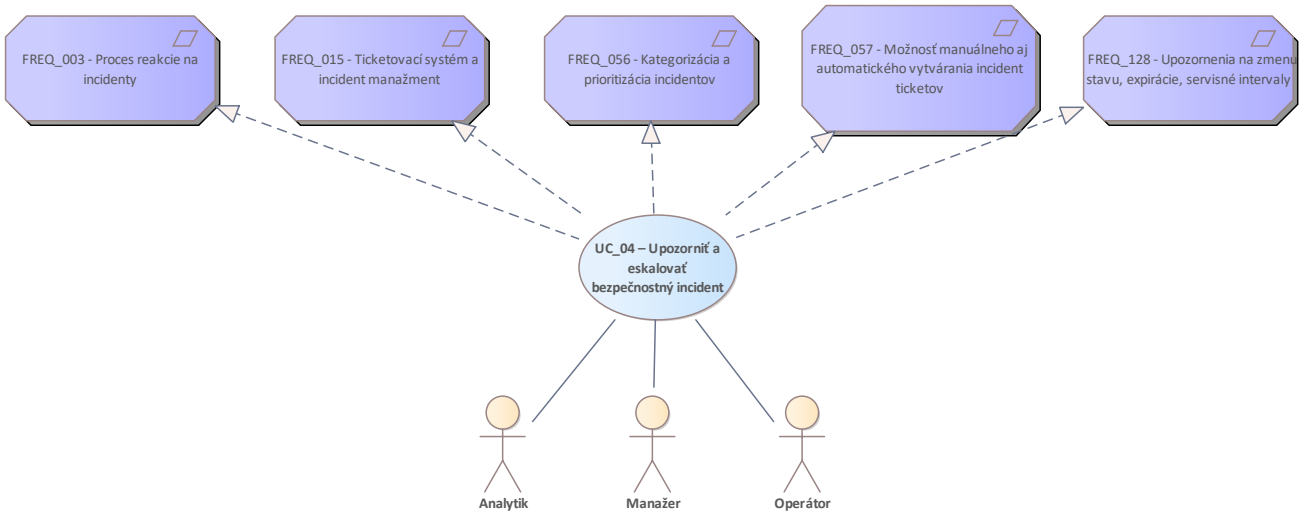
Prípad použitia	UC_03 - Spravovať detekčné a korelačné pravidlá
Cieľ	Tento use case pokrýva aktivity analytikov a správcov pri tvorbe, správe a údržbe detekčných a korelačných pravidiel v prostredí SOCaaS. Tieto pravidlá umožňujú detekciu bezpečnostných hrozieb na základe IOC, behaviorálnych anomálií, reťazenia udalostí alebo prahových hodnôt. Use case sa zameriava výlučne na proces správy pravidiel – ich definovanie, ladenie, klasifikáciu a mapovanie na bezpečnostné rámce (napr. MITRE ATT&CK).
Vstupná podmienka	Aktéri majú prístup do administračného rozhrania na tvorbu pravidiel.
Vstupná podmienka	Systém podporuje definovanie, správu a verzovanie detekčných pravidiel.
Výstupná podmienka	Nové pravidlo je vytvorené alebo existujúce pravidlo je upravené, deaktivované alebo vymazané.
Výstupná podmienka	Pravidlo je verzované, validované a pripravené na nasadenie do produkčného prostredia.
Výstupná podmienka	Pravidlo je dostupné na vyhodnocovanie bezpečnostných udalostí (UC_04).
Basic Path	Basic Path

Krok	Aktivita
1	Analytik alebo správca otvorí rozhranie pre správu detekčných pravidiel.
2	Vytvorí nové pravidlo alebo vyhľadá existujúce.
3	Definuje podmienky: typ udalosti, IOC/indikátor, frekvencia výskytu, zdrojové/destinované entity,
4	Priradí pravidlu závažnosť, typ hrozby a MITRE ATT&CK kategóriu.
5	Pravidlo je uložené a verzované.
6	Môže byť validované na historických dátach alebo označené ako aktívne.
7	Pravidlo sa začne používať pri vyhodnocovaní udalostí (UC_04).

ALT_1 – Pravidlo sa testuje na historických dátach (debugging)	Alternate
Krok	**Aktivita**
1	Analytik použije nástroj na testovanie pravidiel voči historickým logom.
2	Výsledky sa zobrazia, pravidlo sa následne upraví alebo schváli.

ALT_2 – Pravidlo sa vytvorí cez no-code rozhranie	Alternate
Krok	**Aktivita**
1	Analytik použije vizuálne rozhranie (drag & drop) na vytvorenie podmienok bez písania syntaxe.
2	Platforma automaticky vytvorí podkladový kód pravidla.

4.3.2.3 UC_04 – Upozorniť a eskalovať bezpečnostný incident



Obrázok 7 : UC_04 – Upozorniť a eskalovať bezpečnostný incident

Prípad použitia	UC_04 – Upozorniť a eskalovať bezpečnostný incident
Cieľ	Po tom, ako systém deteguje a založí bezpečnostný incident (UC_01, UC_03), je cieľom UC_04 zabezpečiť, aby sa o ňom včas dozvedol správny človek (1st level), aby incident niekto prevzal a aby sa pri nečinnosti alebo zhoršení závažnosti incident automaticky posunul na vyššiu úroveň
Vstupná podmienka	Existuje incident – incident bol vytvorený a má priradenú kategóriu a závažnosť
Vstupná podmienka	Sú nastavené notifikačné a eskalačné politiky
Vstupná podmienka	Sú známe kontaktné kanály a on-call rozpis
Výstupná podmienka	Relevantný príjemca bol notifikovaný
Výstupná podmienka	Incident má zaznamenanú históriu notifikácií/escalácií
Výstupná podmienka	V prípade nečinnosti prebehla eskalácia podľa SLA

Basic Path	Basic Path

Krok	**Aktivita**
1	Vznik alebo zmena incidentu
2	Vyhodnotenie notifikačnej politiky
3	Výber primárnych príjemcov
4	Generovanie notifikačnej správy
5	Odoslanie notifikácie primárnymi kanálmi
6	Čakanie na potvrdenie (acknowledgement)
7	Potvrdenie incidentu Analytikom/Operátorom
8	Zastavenie ďalšej eskalácie
9	Aktualizácia histórie incidentu

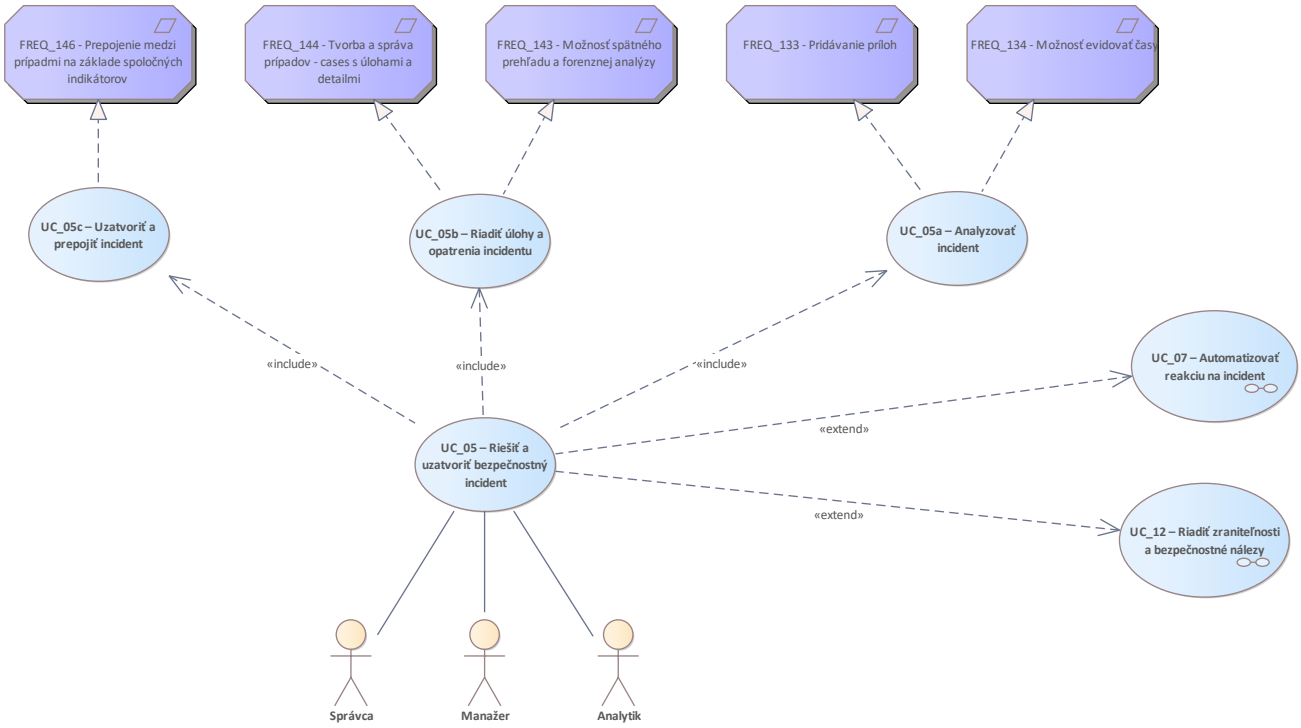
ALT_01 – Zlyhanie primárneho notifikačného kanála	Alternate

Krok	**Aktivita**
1	Odoslanie notifikácie zlyhá (napr. e-mail server nedostupný).
2	Systém automaticky vyskúša alternatívny kanál (napr. SMS, iný mailový gateway, chat).
3	Do histórie incidentu sa zaznamená neúspešný pokus aj následný fallback.
4	Ak všetky kanály zlyhajú, incident dostane príznak „notifikácia neúspešná“ a systém automaticky vytvorí interný ticket pre správcu infraštruktúry.

ALT_02 - Incident nie je v SLA čase potvrdený - eskalácia	Alternate

Krok	**Aktivita**
1	Po uplynutí SLA intervalu nedošlo k potvrdeniu incidentu.
2	Systém automaticky eskaluje incident na vyššiu úroveň (Manažér, Vedúci SOC): zvýšenie priority / závažnosti incidentu, odoslanie eskalačnej notifikácie Manažérovi cez jeho preferované kanály.
3	Do histórie incidentu sa pridá záznam o neprevzatí v SLA a o vykonanej eskalácii.
4	Voliteľne sa spustí ďalší playbook (napr. čiastočné automatizované opatrenia, predpripravené akcie).

4.3.2.4 UC_05 – Riešiť a uzatvoriť bezpečnostný incident



Obrázok 8 : UC_05 – Riešiť a uzatvoriť bezpečnostný incident

Prípad použitia	UC_05 – Riešiť a uzatvoriť bezpečnostný incident
Cieľ	Po detekcii incidentu a odoslaní upozornení (UC_01, UC_03, UC_04) tento UC pokrýva celý proces riešenia incidentu – od prevzatia, analýzy a realizácie nápravných opatrení až po uzatvorenie incidentu a kompletné zdokumentovanie jeho priebehu (časová os, dôkazy, prepojené prípady). Výsledkom je incident, ktorý má jasného vlastníka, realizované kroky, zaznamenané časy a pripravené podklady pre prípadné „poučenie“
Vstupná podmienka	Incident je založený a notifikovaný
Vstupná podmienka	Incident má priradeného vlastníka / tím
Vstupná podmienka	Dostupné sú relevantné dáta a logy
Výstupná podmienka	Incident má zdokumentovaný priebeh a výsledok
Výstupná podmienka	Bol vykonaný dohodnutý súbor nápravných opatrení
Výstupná podmienka	Incident je uzatvorený alebo preklasifikovaný

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevzatie incidentu Analytikom
2	Zber a doplnenie dôkazov
3	Analýza a identifikácia príčin
4	Návrh nápravných opatrení

5	Realizácia opatrení Správcom
6	Sledovanie časov a priebehu riešenia
7	Kontrola a schválenie výsledku
8	Uzatvorenie incidentu
9	Príprava podkladov pre poučenie

ALT_ 01 – Incident je vyhodnotený ako false positive	Alternate
Krok	**Aktivita**
1	Po analýze Analytik zistí, že incident nevznikol (nesprávna korelácia, testovací traffic).
2	Analytik aktualizuje incident na stav „false positive“ a stručne zdokumentuje dôvod.
3	Incident je uzatvorený, ale zostáva v histórii vrátane dôkazov – neskôr môže byť použitý na úpravu detekčných pravidiel

ALT_02 – Nápravné opatrenia nie je možné okamžite realizovať	Alternate
Krok	**Aktivita**
1	Správca zistí, že navrhované opatrenie má vysoký dopad na prevádzku (napr. odstavenie kritickej služby).
2	V incidente vytvorí plánované úlohy s termínmi a komentármi, prípadne žiadosť o schválenie Manažérovi.
3	Incident zostáva v stave „otvorený – čaká na plánované opatrenia“ s evidovanými časmi a rizikom.

Prípad použitia	UC_05a – Analyzovať incident
Cieľ	Analytik detailne preskúma incident – pozrie si časovú os udalostí, logy, IOC, doplní dôkazy a vytvorí ucelený obraz o príčine a rozsahu incidentu.
Vstupná podmienka	Incident je založený a priradený Analytikovi.
Vstupná podmienka	K incidentu sú dostupné základné logy a udalosti z monitorovacieho systému.
Výstupná podmienka	Incident obsahuje doplnené dôkazy (logy, prílohy, IOC).
Výstupná podmienka	Je popísaná predbežná príčina incidentu a rozsah dopadu.

Basic Path	Basic Path
Krok	**Aktivita**
1	Analytik otvorí detail incidentu.
2	Zobrazí si časovú os súvisiacich udalostí a logov.
3	Identifikuje podozrivé udalosti a indikátory kompromitácie.
4	Stiahne alebo si vyžiada doplňujúce logy/prílohy a pripojí ich k incidentu.
5	Na základe zhromaždených dát popíše predbežnú príčinu a rozsah incidentu.
6	Aktualizuje prioritu incidentu, ak je to potrebné.

ALT_01 – Nedostupné alebo neúplné logy	Alternate
Krok	**Aktivita**
1	Analytik zistí, že logy sú neúplné alebo chýbajú; v incidente založí úlohu pre Správcu na nápravu (dopnutie logovania, export zo zdrojového systému) a ďalej pracuje s tým, čo má k dispozícii.

ALT_02 – Incident sa ukáže ako false positive	Alternate
Krok	**Aktivita**
1	Analytik po analýze vyhodnotí, že nejde o skutočný incident; incident označí ako „false positive“, stručne zdokumentuje dôvod a UC_05 sa ukončí.

Prípad použitia	UC_05b – Riadiť úlohy a opatrenia incidentu
Cieľ	Analytik a Správca vytvárajú, priraďujú a sledujú úlohy, ktoré predstavujú konkrétne nápravné alebo preventívne opatrenia súvisiace s incidentom.
Vstupná podmienka	K incidentu existuje základná analýza (UC_05a).
Vstupná podmienka	Je jasné, aké systémy alebo služby incident ovplyvňuje.
Výstupná podmienka	Incident má vytvorený zoznam úloh s priradenými zodpovednými osobami a termínmi.
Výstupná podmienka	Stav jednotlivých úloh odráža reálny priebeh riešenia (plánované, v riešení, hotové).
Basic Path	Basic Path
Krok	**Aktivita**
1	Analytik na základe analýzy navrhne konkrétne nápravné opatrenia.
2	V incidente vytvorí úlohy a priradí ich konkrétnym Správcom alebo tímom.
3	Ku každej úlohe nastaví prioritu a termín.
4	Správcovia priebežne aktualizujú stav úloh podľa realizácie opatrení.
5	Systém zaznamenáva časy vytvorenia, začiatku a dokončenia úloh.
6	Analytik sleduje stav úloh a podľa potreby pripomína alebo eskaluje oneskorené úlohy.
7	Po dokončení kľúčových úloh aktualizuje Analytik stav incidentu.

ALT_01 – Úloha má vysoký dopad na prevádzku	Alternate
Krok	**Aktivita**
1	Správca zistí, že navrhované opatrenie môže spôsobiť výpadok; úlohu označí ako „vyžaduje schválenie“ a Manažér ju schváli alebo zamietne s komentárom.

ALT_02 – Úloha nie je realizovateľná v plánovanom termíne	Alternate
Krok	**Aktivita**
1	Správca aktualizuje termín a dôvod v úlohe; Analytik podľa potreby upraví prioritu incidentu alebo informuje Manažéra.

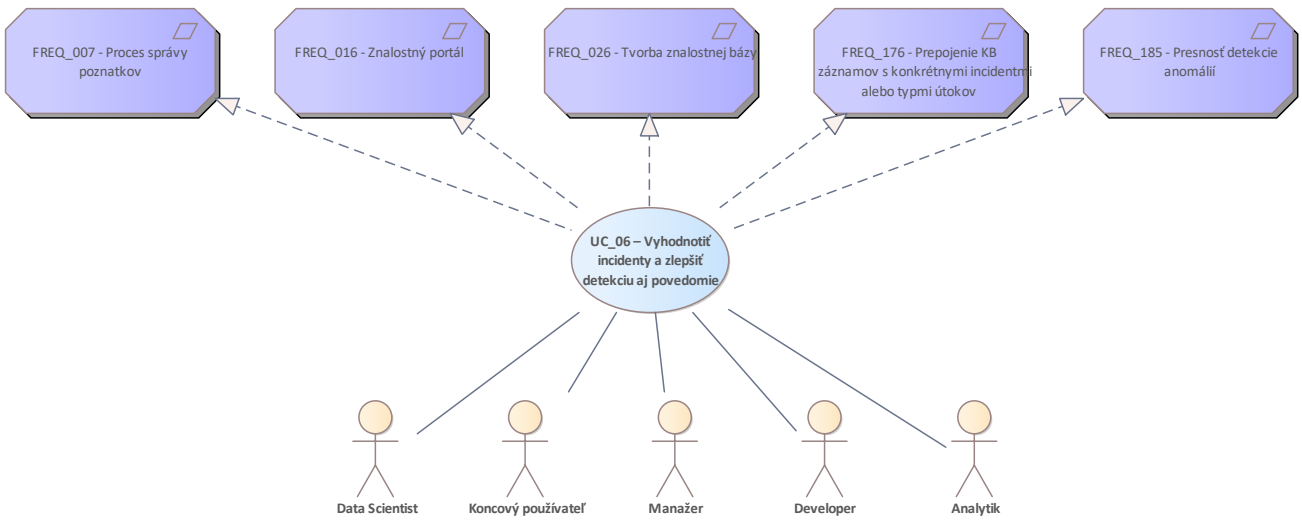
Prípad použitia	UC_05c – Uzatvoriť a prepojiť incident
Cieľ	Po vykonaní nápravných opatrení Analytik (príp. Manažér) rozhodne o finálnom stave incidentu, zdokumentuje záver a prepojí incident s inými súvisiacimi prípadmi.
Vstupná podmienka	Kľúčové úlohy incidentu sú dokončené alebo je rozhodnuté o akceptovaní zostávajúceho rizika.
Vstupná podmienka	Monitoring neukazuje pretrvávajúce indikátory útoku alebo je ich výskyt vysvetlený.
Výstupná podmienka	Incident je v jednom z finálnych stavov (uzatvorený, false positive, akceptované riziko, súčasť kampane).
Výstupná podmienka	Incident je prepojený s ďalšími relevantnými incidentmi/prípadmi alebo kampaňami, ak existujú.
Basic Path	Basic Path

Krok	Aktivita
1	Analytik skontroluje, že všetky dôležité úlohy sú dokončené a systémy sú stabilné.
2	Overí v monitoringu, že sa neobjavujú nové súvisiace udalosti.
3	Ak je incident súčasťou širšej kampane, vyhľadá a prepojí súvisiace incidenty.
4	Vyplní záverečné zhrnutie: príčina, dopad, vykonané opatrenia.
5	Nastaví finálny stav incidentu (napr. „uzatvorený“).
6	Pri kritických incidentoch požiada Manažéra o schválenie uzatvorenia.
7	Incident sa presunie do archívu a je pripravený pre proces „lessons learned“.

ALT_01 – Zistené nové súvisiace udalosti pri uzatváraní	Alternate
Krok	**Aktivita**
1	Počas kontroly Analytik zistí nové podozrivé udalosti; incident ponechá otvorený, vytvorí nové úlohy a vráti sa späť k UC_05a/05b.

ALT_02 – Incident je súčasťou rozsiahlej kampane	Alternate
Krok	**Aktivita**
1	Analytik identifikuje, že incident patrí do väčšej kampane; nastaví ho ako podriadený k nadradenému prípadu a upraví záverečné zhrnutie.

4.3.2.5 UC_06 – Vyhodnotiť incidenty a zlepšiť detekciu aj povedomie



Obrázok 9 : UC_06 – Vyhodnotiť incidenty a zlepšiť detekciu aj povedomiel

Prípad použitia	UC_06 – Vyhodnotiť incidenty a zlepšiť detekciu aj povedomie
Cieľ	Po vyriešení a uzatvorení incidentu (UC_05) tento UC zabezpečuje, aby sa z incidentu systém aj ľudia poučili: incident sa zhodnotí (post-incident / post-mortem), zistenia sa premietnu do úprav detekčných pravidiel a ML modelov,

	pripraví sa alebo aktualizuje školenie / usmernenie pre zamestnancov.
Vstupná podmienka	Incident je uzatvorený
Vstupná podmienka	Sú dostupné údaje o incidente
Vstupná podmienka	Existuje aspoň základný proces „lessons learned“
Výstupná podmienka	Incident má spracovaný záznam „lessons learned“
Výstupná podmienka	Sú navrhnuté alebo vykonané úpravy detekcie/ML
Výstupná podmienka	Je pripravené alebo aktualizované školenie / guidance pre používateľov

Basic Path	Basic Path

Krok	**Aktivita**
1	Výber incidentov na vyhodnotenie
2	Príprava podkladov na vyhodnotenie
3	Post-incident meeting / hodnotenie
4	Zápis lessons learned a odporúčaní
5	Návrh úprav detekcie a ML modelov
6	Tím vyhodnotí, ako incident ovplyvňuje presnosť detekcie (napr. počet false positive/false negative, vhodnosť prahov, správanie modelu pri anomáliách) a tieto zistenia zahrnie do návrhu úprav.
7	Záznam v znalostnej báze je prelinkovaný s konkrétnym incidentom (resp. typom útoku), aby sa dal pri podobných prípadoch rýchlo nájsť.
8	Výstupy sú uložené v znalostnom portáli / knowledge base a komunikované relevantným ľuďom.
9	Schvaľovanie a plánovanie nasadenia zmien
10	Príprava školenia / awareness materiálov
11	Distribúcia poznatkov
12	Záver UC

ALT_01 – Nedostatok dát na kvalitné vyhodnotenie	Alternate

Krok	**Aktivita**
1	Pri analýze sa ukáže, že nie sú dostupné všetky potrebné logy alebo historické údaje; tím síce spraví základné lessons learned, ale zároveň vytvorí úlohy na zlepšenie logovania a zberu dát do budúcna.

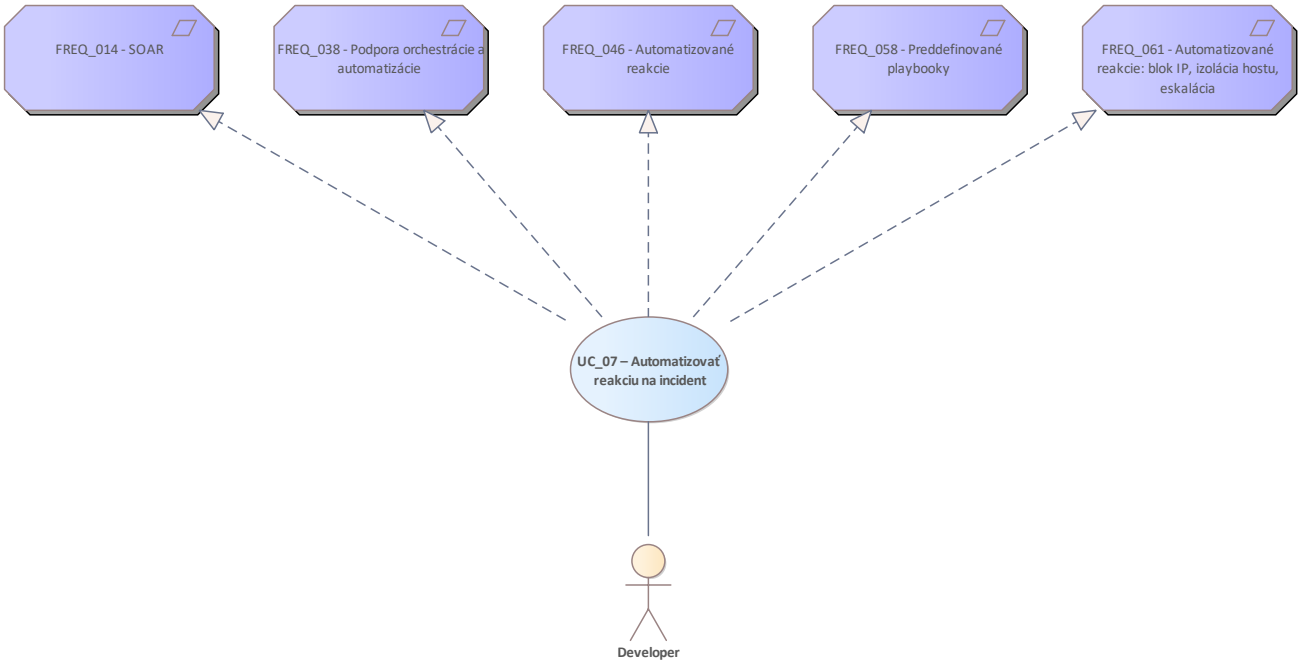
ALT_02 – Návrh úprav detekcie/ML sa zamietne	Alternate

Krok	**Aktivita**
1	Data Scientist alebo Developer pripravia návrh zmien, ale Manažér ich na základe rizík alebo nákladov neschváli; odporúčania sa uložia v knowledge base a zmeny sa prípadne prehodnotia neskôr.

ALT_03 – Identifikovaná potreba cieleneho školenia zamestnancov	Alternate

Krok	**Aktivita**
1	Z vyhodnotenia vyplynie, že hlavnou slabinou boli ľudské chyby alebo neznalosť; Manažér rozhodne o príprave alebo úprave konkrétneho školenia, ktoré je priradené vybranej skupine používateľov.

4.3.2.6 UC_07 – Automatizovať reakciu na incident



Obrázok 10 : UC_07 – Automatizovať reakciu na incident

Prípad použitia	UC_07 – Automatizovať reakciu na incident
Cieľ	UC_07 rieši situáciu, keď je incident už detegovaný a v riešení (UC_05), ale namiesto čisto manuálnych krokov sa použijú automatizované alebo poloautomatizované playbooky. Systém na základe typu incidentu a TTP navrhne vhodné playbooky, orchestruje technické zásahy (blokovanie, izolácia, vypnutie účtu, ticketing) a všetko auditne zaznamená.
Vstupná podmienka	Incident je v stave „v riešení“
Vstupná podmienka	Pre daný typ incidentu existujú dostupné playbooky
Vstupná podmienka	Sú funkčné integrácie na cieľové systémy
Výstupná podmienka	Vybrané playbooky boli vykonané (auto / semi-auto)
Výstupná podmienka	Všetky automatizované zásahy sú auditne zaznamenané v incidente
Výstupná podmienka	Incident je v stave, ktorý odráža výsledok automatizovanej reakcie
Basic Path	Basic Path

Krok	**Aktivita**
1	Analytik otvorí incident v stave „v riešení“ a systém mu zobrazí zoznam navrhnutých playbookov podľa typu incidentu a použitých techník.
2	Analytik vyberie vhodný playbook a zvolí režim vykonania (napr. simulácia, poloautomatický režim, plne automatický pri nízkom riziku).
3	Systém zobrazí prehľad plánovaných krokov playbooku (napr. blok IP, izolácia endpointu, zakázanie účtu, vytvorenie ticketu).
4	Pri poloautomatickom režime systém pred vykonaním každého kroku vyžiada od Analytika potvrdenie alebo preskočenie kroku.
5	Systém postupne vykonáva schválené kroky cez integrácie na cieľové systémy a priebežne zaznamenáva stav (úspech/zlyhanie).
6	Po skončení playbooku systém zhrnie výsledok: ktoré akcie prebehli úspešne, čo zlyhalo a kde je treba manuálny zásah.
7	Výsledky vykonaných akcií a časová os playbooku sa uložia do incidentu ako súčasť histórie riešenia.

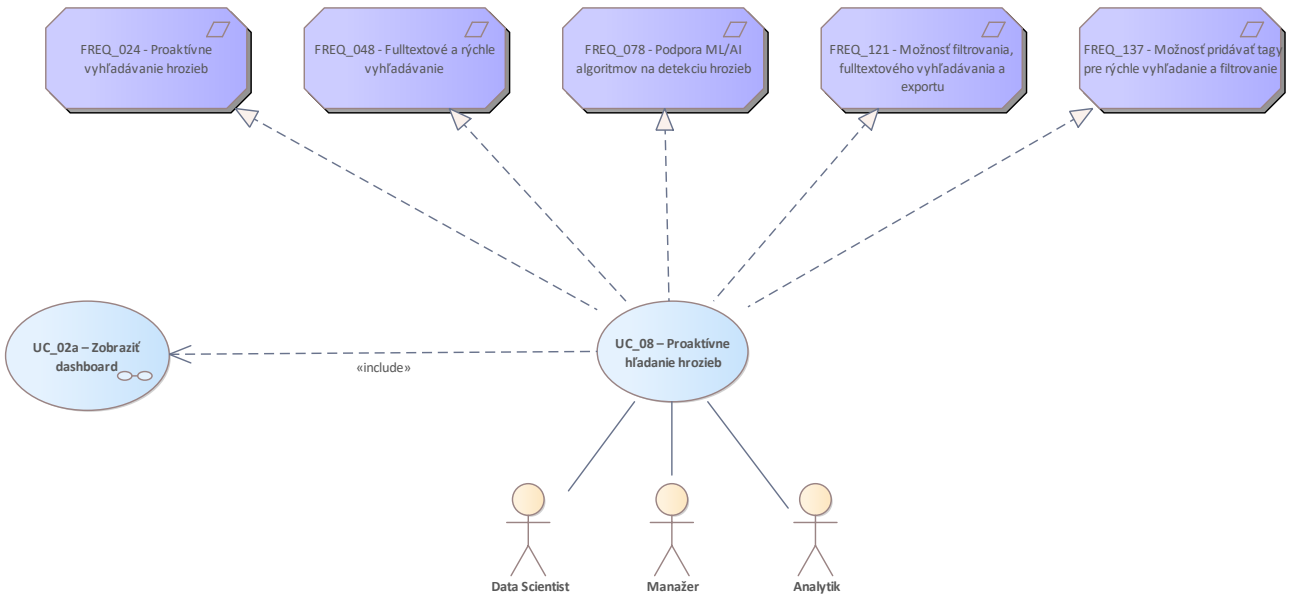
8	Analytik na základe výsledku aktualizuje stav incidentu (napr. containment hotový, čaká sa na monitoring, čaká sa na ďalšie úlohy podľa UC_05).
9	Incident pokračuje ďalej v UC_05 (detailná analýza, doplnenie úloh, uzatvorenie).

ALT_01 – Nenašiel sa vhodný playbook	Alternate
Krok	**Aktivita**
1	Systém nedokáže priradiť žiaden relevantný playbook k danému incidentu; Analytik pokračuje v riešení incidentu manuálne podľa UC_05 a incident označí ako kandidáta na vytvorenie nového playbooku v budúcnosti.

ALT_02 – Kritický krok playbooku zlyhá	Alternate
Krok	**Aktivita**
1	Pri vykonávaní automatizovaného kroku (napr. blokovanie na firewalle) dôjde k chybe; systém krok označí ako neúspešný, zaznamená detail chyby a Analytik sa rozhodne, či krok zopakuje, nahradí ho iným opatrením alebo priradí manuálnu úlohu Správcovi.

ALT_03 – Playbook sa spustí iba v simulačnom režime	Alternate
Krok	**Aktivita**
1	Na základe politiky Manažéra sú vybrané playbooky povolené len v režime simulácie; Analytik spustí simuláciu, systém zobrazí, aké akcie by boli vykonané a aký by bol dopad, a až následne Analytik rozhodne, ktoré z nich sa vykonajú manuálne alebo formou čiastočnej automatizácie.

4.3.2.7 UC_08 – Proaktívne hľadanie hrozieb



Obrázok 11 : UC_08 – Proaktívne hľadanie hrozieb

Prípad použitia	UC_08 – Proaktívne hľadanie hrozieb
Cieľ	UC_08 rieši proaktívne hľadanie hrozieb v historických a aktuálnych dátach mimo bežných alertov. Analytik cieľavedome hľadá podozrivé vzory správania (TTP, IOC), ktoré doteraz nevyvolali incident ani upozornenie, ukladá si huntingové scenáre a z nálezov vie priamo

	zakladať nové incidenty.
Vstupná podmienka	Sú k dispozícii historické a aktuálne logy/telemetria
Vstupná podmienka	Existuje aspoň základná sada huntingových dopytov alebo scenárov
Vstupná podmienka	Analytik má prístup k dashboardom a nástrojom na ad-hoc dotazy
Výstupná podmienka	Prebehol aspoň jeden huntingový beh
Výstupná podmienka	Nálezy sú zdokumentované a prepojené na incidenty alebo knowledge base
Výstupná podmienka	Huntingové scenáre sú uložené pre opakované použitie

Basic Path	Basic Path

Krok	**Aktivita**
1	Výber huntingového cieľa
2	Otvorenie huntingového pracovného priestoru
3	Tvorba alebo výber dopytu / scenára
4	Spustenie hunting behu nad dátami
5	Analýza nálezov
6	Prevod nálezov na incidenty alebo obohatenie existujúcich incidentov
7	Uloženie huntingového scenára
8	Dokumentácia výsledkov
9	Plánovanie opakovaného huntovania

ALT_01 – Hunting neodhalí nič významné	Alternate

Krok	**Aktivita**
1	Huntingový dopyt nevráti žiadne podozrivé nálezy alebo všetky nálezy sú po kontrole legitímne; Analytik záznam o huntingu uloží ako „bez významných zistení“ a môže upraviť dopyt pre budúce použitie.

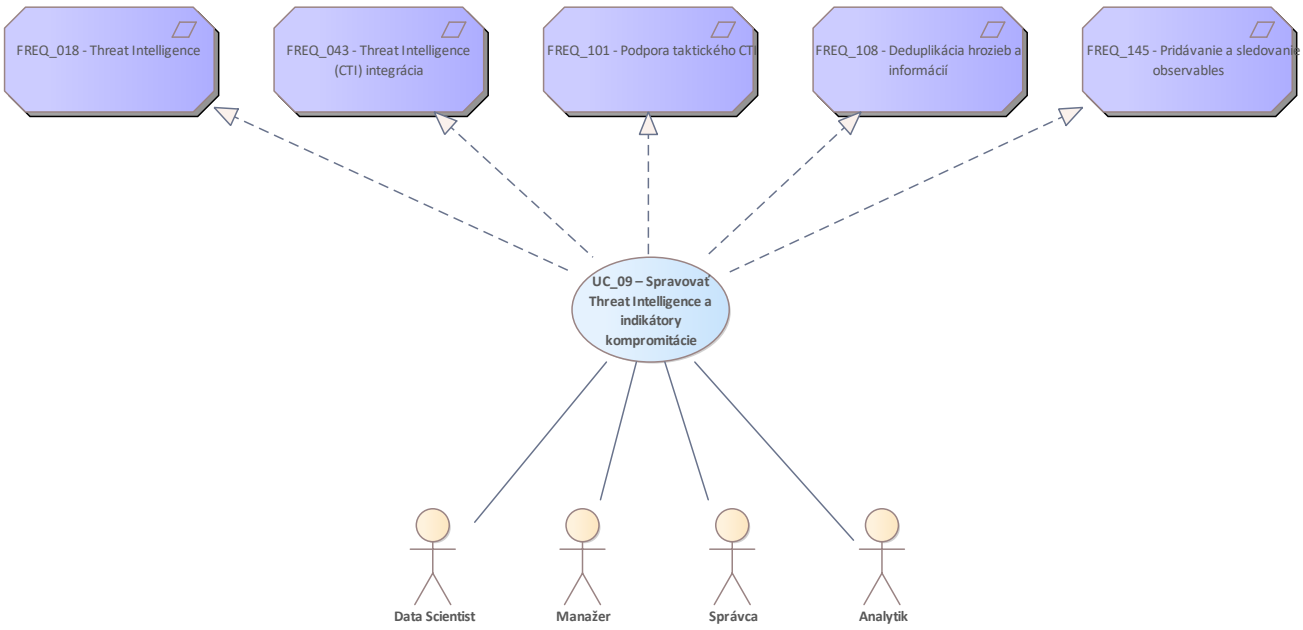
ALT_02 – Hunting odhalí rozsiahlu kampaň	Alternate

Krok	**Aktivita**
1	Hunting identifikuje viaceré súvisiace nálezy, ktoré naznačujú rozsiahlejší útok; Analytik vytvorí nadradený incident/kampaň, priradí k nemu všetky súvisiace nálezy a incidenty a informuje Manažéra o potrebe zvýšenej pozornosti.

ALT_03 – Dopyt je príliš náročný alebo pomalý	Alternate

Krok	**Aktivita**
1	Spustený huntingový dopyt prechádza nad veľkým objemom dát a systémy ho vyhodnotia ako príliš náročný; systém upozorní Analytika, dopyt zastaví alebo obmedzí a ponúkne možnosť upraviť časový rozsah alebo granularitu.

4.3.2.8 UC_09 – Spravovať Threat Intelligence a indikátory kompromitácie



Obrázok 12 : UC_09 – Spravovať Threat Intelligence a indikátory kompromitácie

Prípad použitia	UC_09 – Spravovať Threat Intelligence a indikátory kompromitácie
Cieľ	UC_09 rieši správu Threat Intelligence: prijímanie a integráciu CTI feedov, prácu s indikátormi kompromitácie (IOC), ich deduplikáciu a sledovanie v čase. Cieľom je, aby SOC vedel centrálne spravovať hrozby, obohacovať incidenty a logy o TI informácie a mať poriadok v observables.
Vstupná podmienka	Existujú dostupné TI zdroje
Vstupná podmienka	Sú nakonfigurované integrácie na TI zdroje
Vstupná podmienka	Systém má úložisko pre TI a IOC
Výstupná podmienka	TI dáta sú načítané, normalizované a uložené
Výstupná podmienka	Redundantné alebo konfliktné IOC sú deduplikované alebo zlúčené
Výstupná podmienka	IOC/observables sú prepojené s incidentmi, prípadmi alebo aktívami a majú sledovateľnú históriu

Basic Path	Basic Path

Krok	**Aktivita**
1	Načítanie TI z externých zdrojov
2	Normalizácia a uloženie TI
3	Deduplikácia a zlúčenie IOC
4	Správa životného cyklu IOCSpráva životného cyklu IOC
5	Prepojenie IOC na incidenty a prípady
6	Zverejnenie TI pre ostatné časti systému
7	Monitoring kvality TI

ALT_01 – Zlyhanie alebo nedostupnosť TI zdroja	Alternate

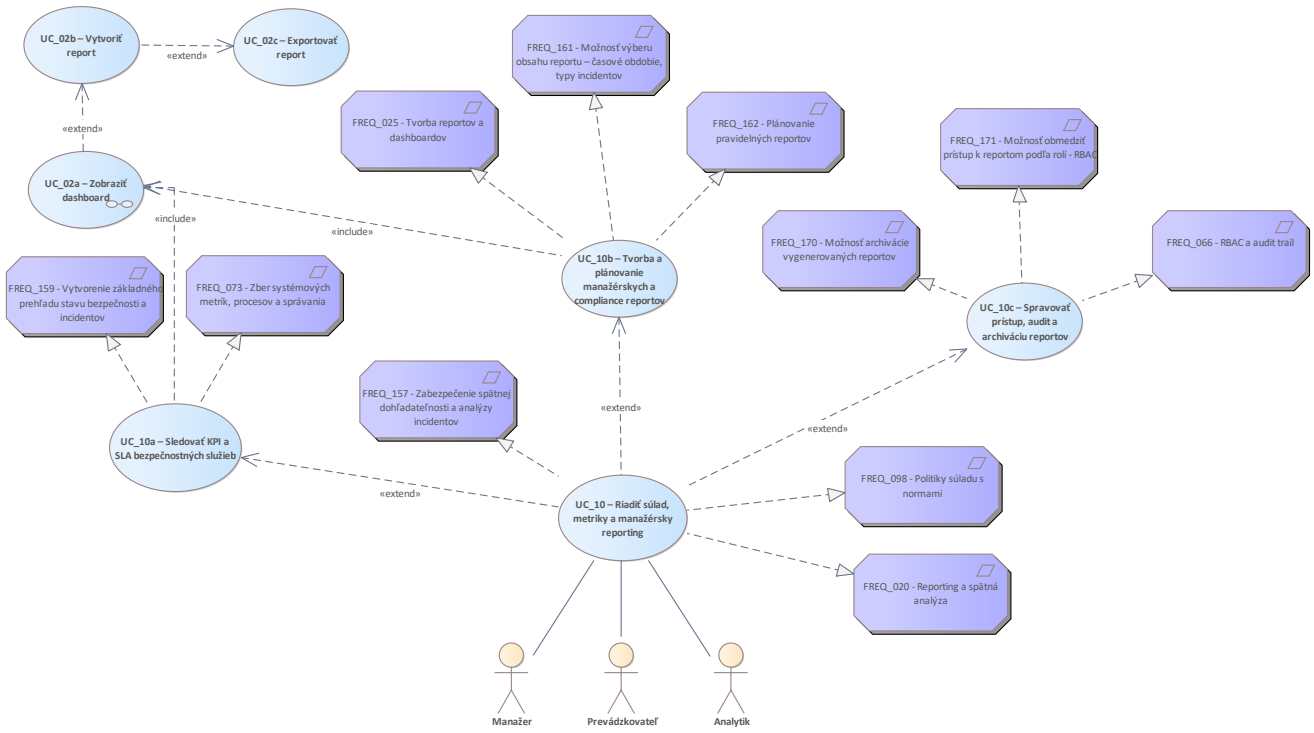
Krok	**Aktivita**

1	Pri načítaní TI je zdroj dočasne nedostupný alebo vracia chyby; systém zaznamená incident na integráciu, použije poslednú platnú sadu IOC a upozorní Správcu na problém.

ALT_02 – Konfliktné informácie o tej istej hrozbe	Alternate
Krok	**Aktivita**
1	Viacero TI zdrojov poskytne rozdielne alebo protichodné informácie o rovnakom IOC; systém uchová všetky varianty so zdrojmi, označí IOC ako konfliktné a nechá na Analytikovi, aby vybral dôveryhodnejší zdroj.

ALT_03 – IOC je vyhodnotený ako neaktuálny alebo nespoľahlivý	Alternate
Krok	**Aktivita**
1	Analytik zistí, že daný IOC už nie je relevantný alebo bol označený ako omyl; zmení jeho stav na neaktívny, pridá komentár a systém zabezpečí, aby sa ďalej nepoužíval v nových detekciách.

4.3.2.9 UC_10 – Riadiť súlad, metriky a manažérsky reporting



Obrázok 13 : UC_10 – Riadiť súlad, metriky a manažérsky reporting

Prípad použitia	UC_10 – Riadiť súlad, metriky a manažérsky reporting
Cieľ	UC_10 rieši “vrchné poschodie” SOCaaS – aby mal manažment a audítori prehľad: ako sa SOCu darí (KPI, SLA, trend incidentov), či je systém v súlade s normami/predpismi, či sú všetky dôležité veci dohľadateľné spätne cez reporty, logy a audity.
Vstupná podmienka	Systém dlhodobo zbiera dáta o incidentoch, reakciách, playbookoch a TI
Vstupná podmienka	Existujú definované metriky/KPI a SLA
Vstupná podmienka	Je nastavená aspoň základná politika súladu (normy, interné smernice)

Výstupná podmienka	Manažér a Auditor majú k dispozícii prehľadné metriky a reporty o stave bezpečnosti a SOC služieb
Výstupná podmienka	Identifikované problémy v KPI/SLA alebo súlade sú zaznamenané a majú priradené odporúčania/opatrenia
Výstupná podmienka	Vytvorené reporty sú archivované a dohľadateľné pre budúce audity

Basic Path	Basic Path

Krok	**Aktivita**
1	Manažér otvorí manažérsky prehľad SOC
2	Výber oblasti záujmu
3	Zobrazenie agregovaných metrík a trendov
4	Identifikácia odchýlok alebo problémov
5	Detailný drill-down
6	Zadanie požiadavky na report / analýzu
7	Zaznamenanie zistení a odporúčaní
8	Prepojenie na opatrenia

ALT_01 – Nedostupné alebo neúplné metriky	Alternate

Krok	**Aktivita**
1	Pri zobrazení manažérskeho prehľadu systém indikuje, že niektoré metriky nie je možné spoľahlivo vypočítať (chýbajúce dáta, neúplné logy); Manažér dostane informáciu, ktoré časti sú neúplné a môže vyžiadať nápravu.

ALT_02 – Identifikované porušenie SLA alebo normy	Alternate

Krok	**Aktivita**
1	Z metrík a reportov vyplynie, že boli porušené SLA alebo požiadavky normy; Manažér zaregistruje zistenie ako oficiálny nález a spustí interné opatrenia (napr. incident kvality služby, korekčné opatrenia).

Prípad použitia	UC_10a – Sledovať KPI a SLA bezpečnostných služieb
Cieľ	UC_10a rozširuje UC_10 o detailné sledovanie KPI, SLA a celkového stavu bezpečnosti. Manažér, Auditor alebo Prevádzkovateľ si v dashboardoch pozrú trendové grafy, prehľady podľa tímov/zákazníkov a celkový „zdravotný stav“ SOCaaS.
Vstupná podmienka	Z UC_10 – manažérsky prehľad je dostupný.
Vstupná podmienka	Sú definované KPI a SLA (napr. MTTR, MTTD, % incidentov v SLA).
Výstupná podmienka	Identifikované odchýlky v KPI/SLA sú zdokumentované.
Výstupná podmienka	Manažér má prehľad o tom, ktoré oblasti/tímy/zákazníci vyžadujú pozornosť.

Basic Path	Basic Path

Krok	**Aktivita**
1	Manažér si v UC_10 zvolí oblasť „KPI a SLA“.
2	Systém zobrazí dashboard s KPI a SLA (include UC_02a – Zobraziť dashboard).
3	Manažér filtruje metriky podľa obdobia, tímu, typu incidentu alebo zákazníka.
4	Systém zobrazuje trendové grafy, priemery, percentá plnenia SLA a porovnania s cieľovými hodnotami.

5	Manažér identifikuje problémy (napr. konkrétny tím má dlhé časy reakcie) a označí ich na detailnej analýzy alebo nápravné opatrenia.

ALT_10a_01 – KPI alebo SLA nie sú ešte definované	Alternate
Krok	**Aktivita**
1	Pri pokuse o zobrazenie KPI/SLA systém označí, že nie sú nakonfigurované; Manažér dostane odporúčanie definovať metriky a priradené zdroje dát.

Prípad použitia	UC_10b – Tvorba a plánovanie manažérskych a compliance reportov
Cieľ	UC_10b rieši praktickú prácu s reportami pre manažment a audity: tvorbu, konfiguráciu obsahu, plánovanie pravidelných reportov a ich jednorazové generovanie.
Vstupná podmienka	Systém má k dispozícii agregované dáta z ostatných UC (incidenty, TI, playbooky, KPI).
Vstupná podmienka	Užívateľ má dostatočné oprávnenia na tvorbu reportov.
Výstupná podmienka	Vznikajú šablóny reportov pre manažment/regulátora.
Výstupná podmienka	Sú nastavené pravidelné aj ad-hoc reporty podľa potrieb.

Basic Path	Basic Path
Krok	**Aktivita**
1	Manažér alebo Auditor otvorí sekciu „Reporty“ v rámci UC_10.
2	Zvolí typ reportu (manažérsky prehľad, incident overview, compliance report).
3	Systém umožní nakonfigurovať obsah reportu – výber metrik, časového obdobia, filtrov.
4	Používateľ si zvolí, či ide o jednorazový report, alebo pravidelný (denný/týždenný/mesačný).
5	Pri generovaní reportu systém využije UC_02b (Vytvoriť report) a UC_02c (Exportovať report) – PDF/CSV/…
6	Vygenerovaný report sa uloží a je dostupný v archíve reportov.

ALT_01 – Nekompletný report z dôvodu chýbajúcich dát	Alternate
Krok	**Aktivita**
1	Pri generovaní reportu systém upozorní, že niektoré časti budú neúplné; používateľ sa môže rozhodnúť report aj tak vygenerovať alebo upraviť rozsah.

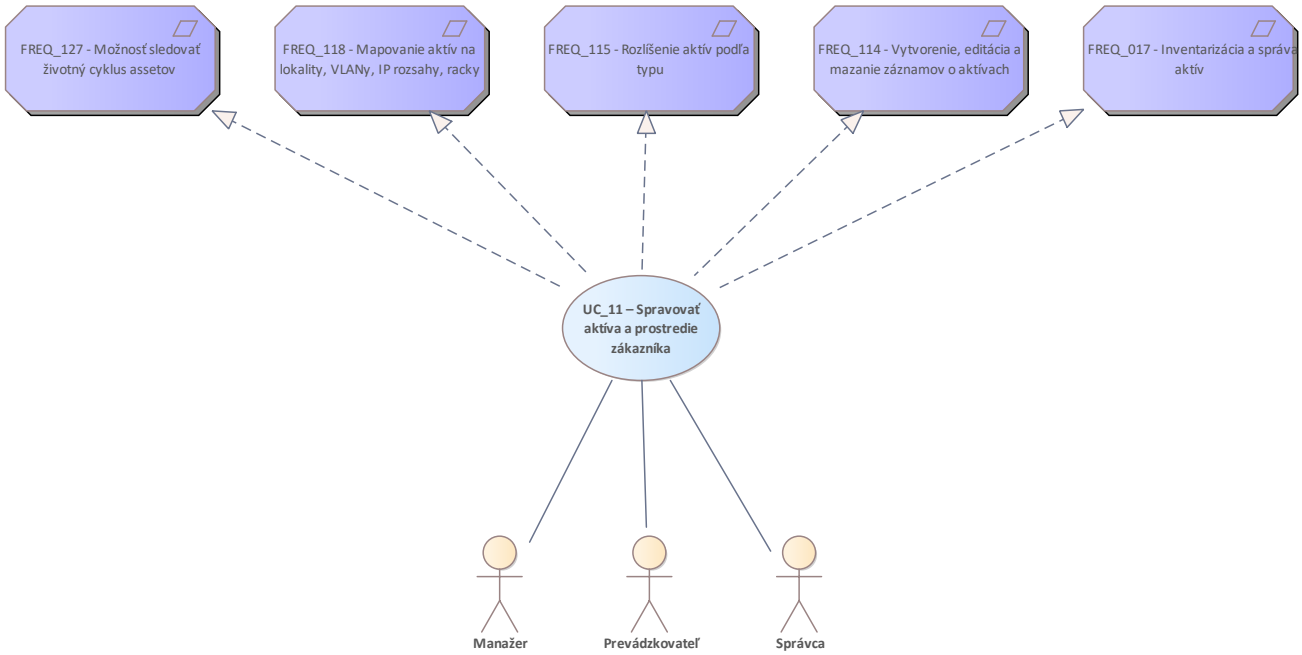
Prípad použitia	UC_10c – Spravovať prístup, audit a archiváciu reportov
Cieľ	UC_10c rieši bezpečnostnú a auditnú stránku reportovania: kto čo vidí, kto čo sprístupnil, či sú reporty archivované a či je možné rekonštruovať, kto mal aké údaje k dispozícii.
Vstupná podmienka	V systéme existujú vygenerované reporty (UC_10b).
Vstupná podmienka	Sú definované roly a prístupové politiky (RBAC).
Výstupná podmienka	Prístup k reportom je obmedzený podľa rolí a zodpovedností.
Výstupná podmienka	Existuje auditná stopa, kto a kedy s reportami pracoval.
Výstupná podmienka	Dôležité reporty sú archivované pre potreby budúcich auditov.

Basic Path	Basic Path
Krok	**Aktivita**

1	Manažér alebo Auditor otvorí správu reportov a prístupov.
2	Pre jednotlivé typy reportov nastaví, ktoré roly alebo konkrétni používatelia k nim majú prístup.
3	Systém aplikuje RBAC pri zobrazovaní a sťahovaní reportov.
4	Pri každom zobrazení, stiahnutí alebo zmene nastavení prístupu systém zapisuje udalosť do audit trail.
5	Staršie reporty sú automaticky alebo manuálne archivované, aby boli dostupné pre audit, ale nepreťažovali bežné rozhranie.

ALT_01 – Pokus o prístup k reportu bez oprávnenia	Alternate
Krok	**Aktivita**
1	Používateľ sa pokúsi otvoriť report, na ktorý nemá rolu; systém prístup odmietne, udalosť zaznamená do audit trail a môže upozorniť Manažéra alebo Auditora.

4.3.2.10 UC_11 – Spravovať aktíva a prostredie zákazníka



Obrázok 14 : UC_11 – Spravovať aktíva a prostredie zákazníka

Prípad použitia	UC_11 – Spravovať aktíva a prostredie zákazníka
Cieľ	Cieľom UC_11 je, aby SOCaaS poznal, čo vlastne chráni – všetky relevantné aktíva zákazníka (servery, aplikácie, siete, cloud služby...) a ich vzťahy. Umožňuje evidovať aktíva, rozlišovať ich typy, mapovať ich na lokality/VLAN/IP a sledovať ich životný cyklus, aby sa incidenty, hrozby a zraniteľnosti dali viazať na konkrétne časti prostredia.
Vstupná podmienka	Zákazník je onboardnutý v systéme (UC_00) a má vytvorený základný profil.
Vstupná podmienka	Systém má k dispozícii modul / sekciu pre evidenciu aktív.
Vstupná podmienka	Existuje aspoň základný zoznam systémov/služieb, ktoré treba zaradiť do inventára.
Výstupná podmienka	Aktíva zákazníka sú zaevidované v systéme s typom, umiestnením a základnými vlastnosťami.
Výstupná podmienka	Každé aktívum má jednoznačný identifikátor a je možné ho použiť v incidentoch, TI, vuln mgmt a reportoch.

Výstupná podmienka	Zmeny v aktívach (pridanie, úprava, vyradenie) sú evidované a životný cyklus je sledovateľný.

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevádzkovateľ otvorí modul „Aktíva“ pre konkrétneho zákazníka.
2	Vytvorí nový záznam o aktíve a zadá jeho základné údaje (názov, popis, vlastník, kritickosť).Vytvorí nový záznam o aktíve a zadá jeho základné údaje (názov, popis, vlastník, kritickosť).
3	Zvolí typ aktíva (napr. server, aplikácia, cloud služba, sieťový prvok) podľa preddefinovaných kategórií.
4	Správca doplní technické údaje – IP adresy, hostname, prostredie (prod/test/dev).
5	Systém umožní namapovať aktívum na konkrétnu lokalitu, VLAN, IP rozsah alebo rack.
6	Prevádzkovateľ nastaví stav aktíva v životnom cykle (napr. „v prevádzke“, „v nasadzovaní“, „vyradené“).
7	Systém uloží záznam o aktíve a sprístupní ho ostatným modulom (incident mgmt, TI, vuln mgmt, reporting).
8	Pri ďalšej zmene (upgrade, migrácia, vyradenie) Správca aktualizuje záznam o aktíve a systém zaznamená zmenu v histórii.

ALT_11_01 – Import aktív z externého CMDB	Alternate

Krok	**Aktivita**
1	Namiesto ručného vytvárania záznamov Prevádzkovateľ zvolí import z externého CMDB alebo inventarizačného nástroja; systém načíta zoznam aktív, zobrazí náhľad a umožní ich hromadné uloženie alebo spárovanie s existujúcimi záznamami.

ALT_11_02 – Detegovaný duplikát aktíva	Alternate

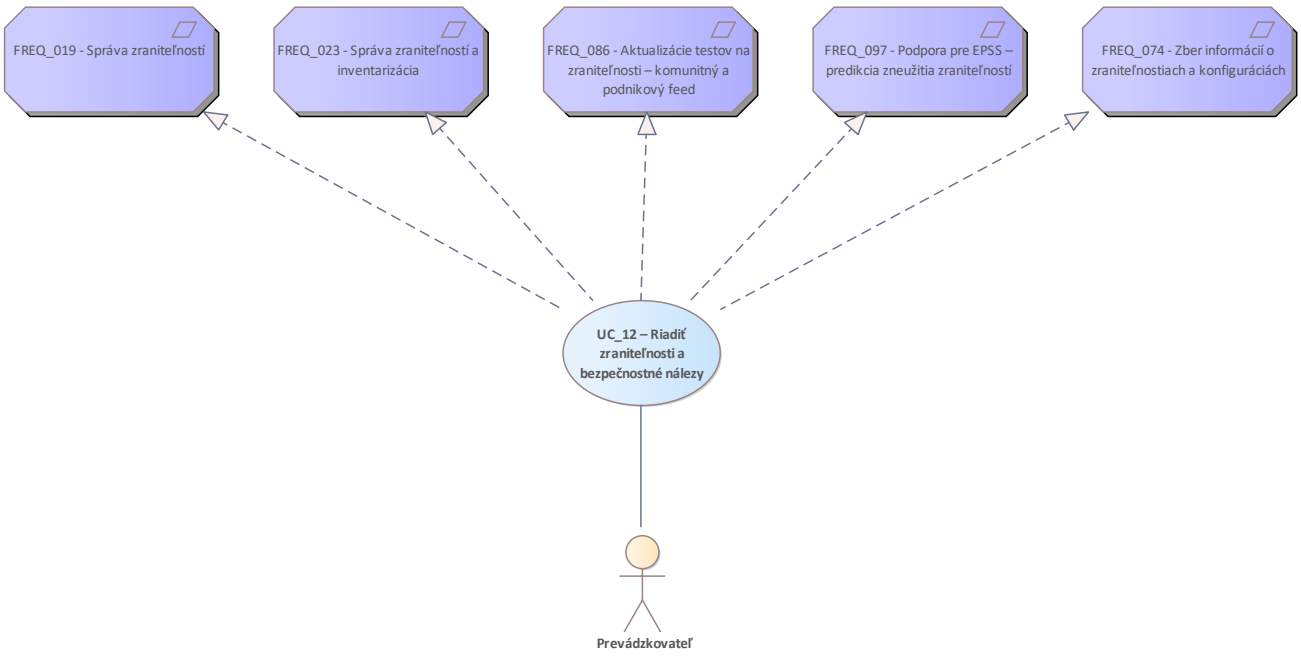
Krok	**Aktivita**
1	Pri ukladaní nového aktíva systém zistí, že už existuje záznam s rovnakými kľúčovými identifikátormi (napr. IP/hostname); používateľ dostane možnosť buď aktualizovať existujúci záznam, alebo vytvoriť samostatné aktívum s odôvodnením.

ALT_11_03 – Zmena kritickosti aktíva	Alternate

Krok	**Aktivita**
1	Manažér rozhodne, že aktívum má vyššiu/nižšiu kritickosť; upraví hodnotu v zázname aktíva a systém označí súvisiace incidenty a zraniteľnosti, ktorých priorita sa môže týmto rozhodnutím zmeniť.

4.3.2.11 UC_12 – Riadiť zraniteľnosti a bezpečnostné nálezy

UC_12 pokrýva vulnerability management v SOCaaS:
od prijatia výstupov zo skenerov zraniteľností, cez ich priradenie na konkrétne aktíva (UC_11), prioritizáciu podľa rizika, až po plánovanie a sledovanie nápravných opatrení.
Cieľom je mať ucelený prehľad o tom, kde sme deraví, čo je najdôležitejšie opraviť a v akom čase.



Obrázok 15 : UC_12 – Riadiť zraniteľnosti a bezpečnostné nálezy

Prípad použitia	UC_12 – Riadiť zraniteľnosti a bezpečnostné nálezy
Cieľ	UC_12 pokrýva vulnerability management v SOCaaS: od prijatia výstupov zo skenerov zraniteľností, cez ich priradenie na konkrétne aktíva (UC_11), prioritizáciu podľa rizika, až po plánovanie a sledovanie nápravných opatrení. Cieľom je mať ucelený prehľad o tom, kde sme deraví, čo je najdôležitejšie opraviť a v akom čase.
Vstupná podmienka	Existujú výsledky skenovania zraniteľností alebo iné bezpečnostné nálezy
Vstupná podmienka	Aktíva sú zaevidované v systéme
Vstupná podmienka	Je definovaná základná politika priorizácie zraniteľností
Výstupná podmienka	Zraniteľnosti sú zaevidované a priradené ku konkrétnym aktívam.
Výstupná podmienka	Každá zraniteľnosť má určenú prioritu a plánovaný spôsob remediation.
Výstupná podmienka	Stav riešenia (neopravené / v riešení / opravené / akceptované riziko) je sledovaný a dohľadateľný.

Basic Path	Basic Path

Krok	**Aktivita**
1	Import alebo zadanie zraniteľností
2	Normalizácia a zoskupenie nálezov
3	Priradenie zraniteľností na aktíva
4	Výpočet a nastavenie priority zraniteľnostíVýpočet a nastavenie priority zraniteľností
5	Vytvorenie remediation plánu
6	Realizácia nápravných opatrení
7	Re-scan alebo overenie stavu
8	Aktualizácia stavu zraniteľností

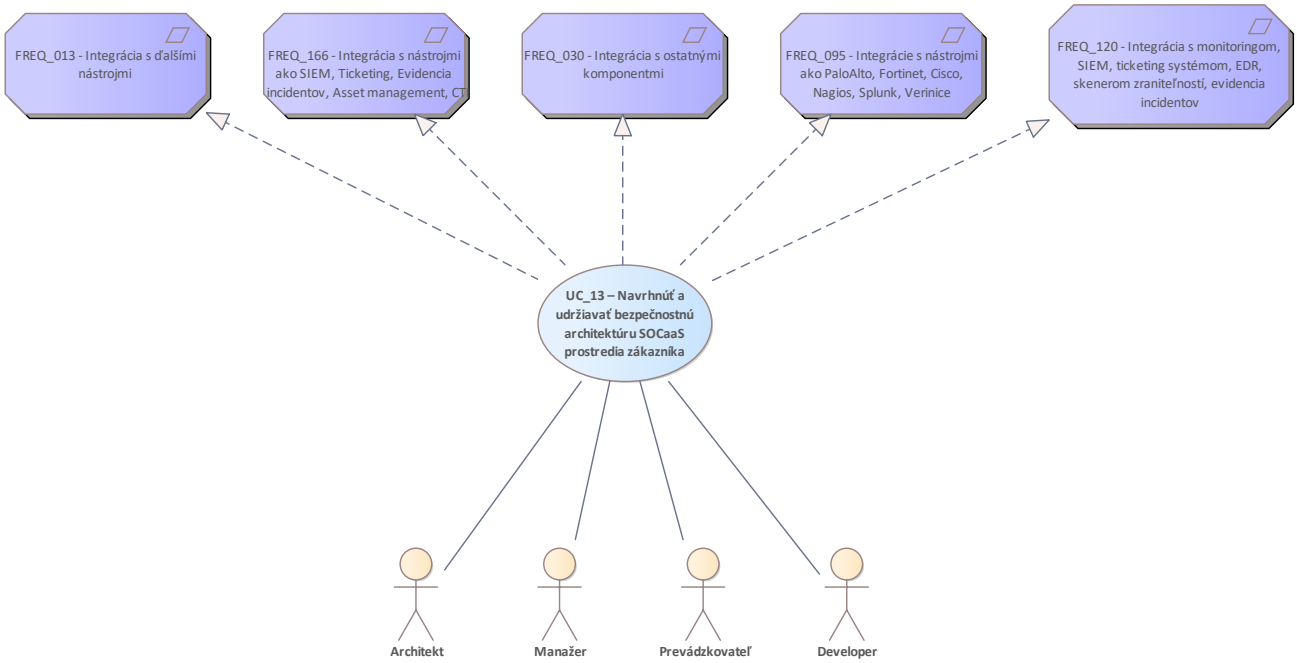
9	Reporting a prepojenie s incidentmi

ALT_12_01 – Zraniteľnosť nie je možné opraviť v požadovanom čase	Alternate
Krok	**Aktivita**
1	Správca zistí, že zraniteľnosť nie je možné opraviť (technické limity, vendor patch neexistuje, vysoký dopad na prevádzku); Manažér po diskusii rozhodne, či sa riziko dočasne akceptuje, alebo sa zavedú kompenzačné opatrenia (network segmentácia, zvýšený monitoring). Stav zraniteľnosti sa nastaví na „akceptované riziko“ alebo „kompenzované“.

ALT_12_02 – Detegovaný duplicitný alebo obsolete nález	Alternate
Krok	**Aktivita**
1	Pri importovaní výsledkov skenu systém zistí, že rovnaká zraniteľnosť bola už zaevidovaná a medzičasom označená ako opravená/irrelevantná; nález sa označí ako duplicitný alebo obsolete, pričom sa uchová referenčný záznam pre audit.

ALT_12_03 – Zraniteľnosť vedie k otvoreniu incidentu	Alternate
Krok	**Aktivita**
1	Analytik vyhodnotí konkrétnu zraniteľnosť (napr. kritickú, aktívne exploitovanú) ako akútnu hrozbu; založí k nej bezpečnostný incident, ktorý sa začne riešiť podľa UC_05, pričom UC_12 sa používa na sledovanie dlhodobej remediation.

4.3.2.12 UC_13 – Navrhnúť a udržiavať bezpečnostnú architektúru SOCaaS prostredia zákazníka



Obrázok 16 : UC_13 – Navrhnúť a udržiavať bezpečnostnú architektúru SOCaaS prostredia zákazníka

Prípad použitia	UC_13 – Navrhnúť a udržiavať bezpečnostnú architektúru SOCaaS prostredia zákazníka
Cieľ	UC_13 rieši návrh a priebežnú údržbu technickej a bezpečnostnej architektúry pre konkrétneho zákazníka:

	ako je zákazník napojený na SOCaaS, aké systémy, zóny a logovacie zdroje sa integrujú, akými kanálmi tečú dáta (agent, syslog, API, VPN, peering…), ako sú prepojené SIEM, SOAR, TI, ticketing, EDR, vuln skenery, asset mgmt. Výstupom je schválený a udržiavaný architektonický návrh (topológia, integračné body, dátové toky), ktorý slúži ako podklad pre onboarding (UC_00), monitoring (UC_01), správu aktív (UC_11), zraniteľností (UC_12) a automatizáciu (UC_07).
Vstupná podmienka	So zákazníkom je dohodnutá spolupráca a sú známe základné požiadavky (rozsah, regulácie, kritickosť služieb).
Vstupná podmienka	Zákazník poskytol potrebný prehľad o svojom prostredí (aspoň high-level architektúra, typy systémov, siete).
Vstupná podmienka	SOCaaS platforma má k dispozícii integračné možnosti (konektory, API, agenti, sieťové cesty), ktoré je možné použiť.
Výstupná podmienka	Existuje zdokumentovaný a schválený architektonický návrh napojenia prostredia zákazníka na SOCaaS (topológia, integračné body, tok dát).
Výstupná podmienka	Sú definované integračné kanály (aký systém → akým spôsobom → do ktorého modulu SOCaaS).
Výstupná podmienka	Zmeny v architektúre sú sledovateľné (verzie, kto schválil, kedy) a použiteľné ako vstup pre onboarding a prevádzku.

Basic Path	Basic Path

Krok	**Aktivita**
1	Zber požiadaviek a vstupov
2	Analýza existujúcej architektúry zákazníka
3	Návrh dátových tokov a integračných patternovNávrh dátových tokov a integračných patternov
4	Návrh integrácií s nástrojmi zákazníka
5	Posúdenie bezpečnostných princípov a rizík
6	Schválenie architektonického návrhu
7	Odoslanie návrhu do realizácie
8	Priebežná údržba architektúry

ALT_13_01 – Obmedzenia na strane zákazníka (sieť, bezpečnostné politiky)	Alternate

Krok	**Aktivita**
1	Počas návrhu sa zistí, že zákazník má obmedzenia (napr. nemožno otvoriť nové porty, využiť agenta alebo VPN); Architekt upraví návrh tak, aby využíval alternatívne integračné patterny alebo zúžený rozsah monitoringu a zmeny znovu predloží na schválenie.

ALT_13_02 – Zmeny v prostredí zákazníka po nasadení	Alternate

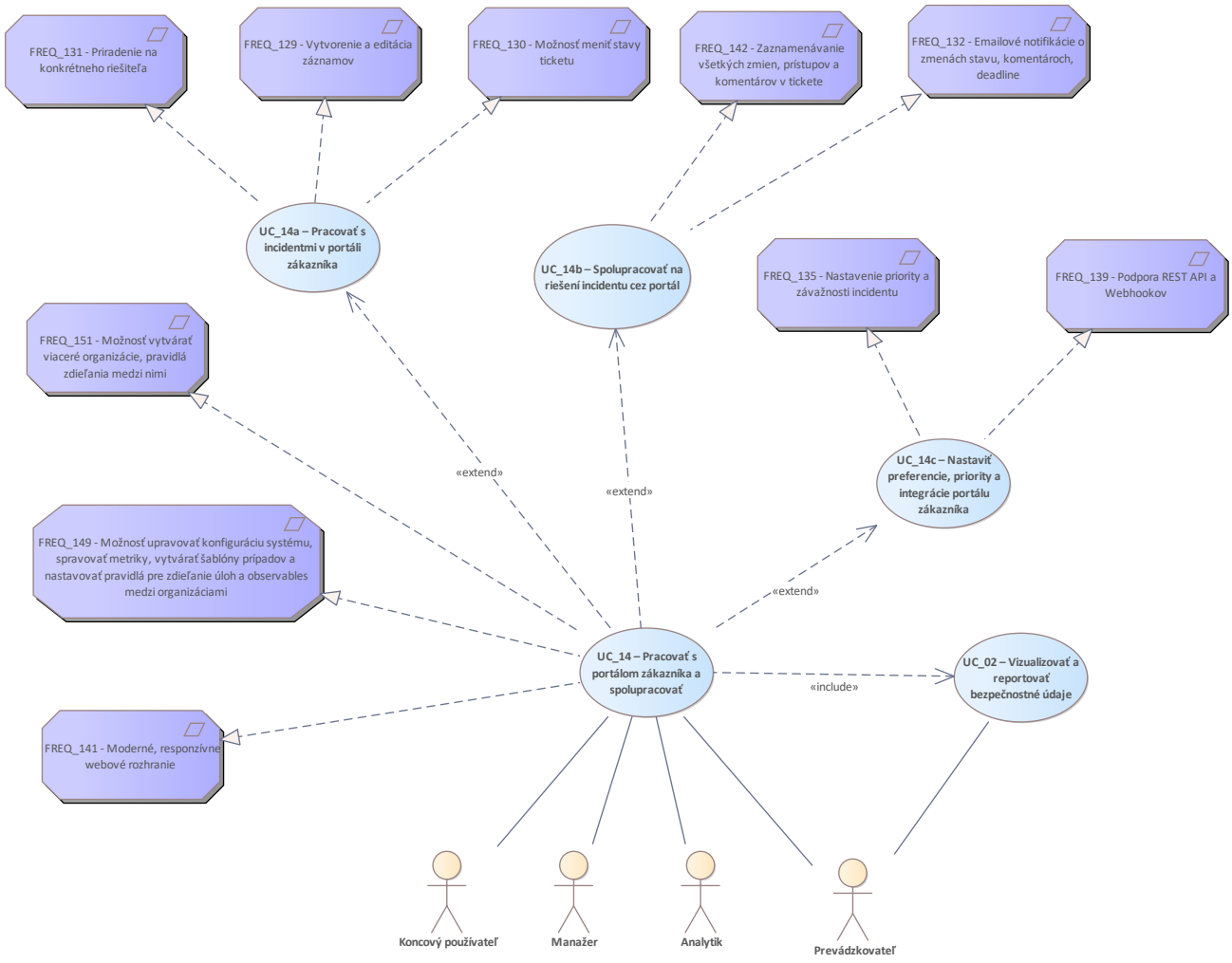
Krok	**Aktivita**
1	Počase zákazník pridá nové systémy, migruje do cloudu alebo zmení topológiu; Architekt vytvorí revíziu architektonického návrhu, doplní nové integračné body a Prevádzkovateľ naplánuje a vykoná potrebné zmeny v konfigurácii SOCaaS.

ALT_13_03 – Návrh neprejde bezpečnostným alebo výkonnostným posúdením	Alternate

Krok	**Aktivita**
1	Pri posúdení návrhu sa zistí, že navrhované riešenie nevyhovuje (príliš veľké latencie, neakceptovateľné riziká, nedostatočné škálovanie); návrh sa vráti Architektovi na prepracovanie a

	až po zapracovaní pripomienok je znovu predložený na schválenie.

4.3.2.13 UC_14 – Portál zákazníka a spolupráca



Obrázok 17 : UC_14 – Pracovať s portálom zákazníka a spolupracovať

Prípad použitia	UC_14 – Pracovať s portálom zákazníka a spolupracovať
Cieľ	UC_14 rieši pohľad zákazníka na SOCaaS – cez webový portál, kde: vidí svoje incidenty, KPI, reporty a aktíva, vie spolupracovať so SOC (komentáre, prílohy, schvaľovanie opatrení), môže si prispôsobiť portál pre viac organizácií/jednotiek. Portál je moderné, responzívne webové rozhranie, multi-tenant, a podporuje aj pokročilejšie nastavenia (šablóny, zdieľanie, integračné hooky v pod-UC).
Vstupná podmienka	Zákazník je onboardnutý (UC_00) a má vytvorenú aspoň jednu organizáciu / tenant.
Vstupná podmienka	Pre používateľov sú vytvorené účty a priradené roly (napr. „Customer security officer“).
Vstupná podmienka	Portál je dostupný cez zabezpečené webové rozhranie (HTTPS, SSO/Federácia ak treba).

Výstupná podmienka	Používateľ má cez portál prehľad o svojich incidentoch, KPI a aktívach.
Výstupná podmienka	Je možné spolupracovať s SOC priamo v kontexte incidentov (komentáre, prílohy, schvaľovanie).Je možné spolupracovať s SOC priamo v kontexte incidentov (komentáre, prílohy, schvaľovanie).
Výstupná podmienka	Portál rešpektuje multi-tenant model – dáta sú oddelené medzi organizáciami a nastavenia sú prispôsobené potrebám konkrétnej organizácie.

Basic Path	Basic Path

Krok	**Aktivita**
1	Koncový používateľ sa prihlási do portálu zákazníka (SSO / meno + heslo / MFA podľa politiky).
2	Systém zobrazí úvodný prehľad – dashboard so stavom incidentov, základnými KPI a upozorneniami
3	Používateľ si vyberie organizáciu/tenant, za ktorú chce pracovať (ak ich má viac).
4	V menu si zvolí, či chce riešiť incidenty, pozrieť reporty, alebo spravovať nastavenia a notifikácie.V menu si zvolí, či chce riešiť incidenty, pozrieť reporty, alebo spravovať nastavenia a notifikácie.
5	Pri výbere „Incidenty“ sa zobrazí zoznam incidentov/ticketov pre danú organizáciu; používateľ sa môže prekliknúť na detail
6	Pri výbere „Reporty“ si môže pozrieť alebo stiahnuť manažérske reporty, ktoré sú pre jeho organizáciu dostupné
7	Pri výbere „Nastavenia“ môže používateľ (podľa roly) meniť notifikácie, preferencie a organizačné nastavenia portálu
8	Systém všetky interakcie (prístup k incidentom, komentáre, zmeny v nastaveniach) auditne zaznamenáva a zabezpečuje, aby boli viditeľné len v rámci danej organizácie.

ALT_14_01 – Používateľ nemá priradenú žiadnu organizáciu	Alternate

Krok	**Aktivita**
1	Po prihlásení systém zistí, že účet nie je naviazaný na žiadnu organizáciu; zobrazí informáciu o chýbajúcom priradení a odporučí kontaktovať Prevádzkovateľa alebo Manažéra.

ALT_14_02 – Obmedzené zobrazenie podľa roly	Alternate

Krok	**Aktivita**
1	Používateľ má len rolu s obmedzenými právami (napr. „read-only“); portál skryje niektoré akčné prvky (editácia, schvaľovanie) a umožní iba prezeranie incidentov a reportov.

Prípad použitia	UC_14a – Pracovať s incidentmi v portáli zákazníka
Cieľ	UC_14a rozširuje UC_14 o konkrétnu prácu s incidentmi/ticketmi z pohľadu zákazníka: vidieť zoznam incidentov, otvoriť detail, vytvoriť nový „ticket“ alebo doplniť informácie, meniť stavy (Nový, V riešení, Uzavretý, Odložený), cieľovo smerovať incident na správneho riešiteľa (L1/L2/L3, konkrétny tím).
Vstupná podmienka	Platí precondition z UC_14 – používateľ je prihlásený a má organizáciu.
Vstupná podmienka	Používateľ má rolu, ktorá umožňuje pracovať s incidentmi (nie len read-only).
Výstupná podmienka	Incidenty/tickety sú vytvorené alebo aktualizované podľa akcií zákazníka.
Výstupná podmienka	Incident má nastavený aktuálny stav a priradeného riešiteľa.

Basic Path	Basic Path

Krok	Aktivita
1	Používateľ v portáli otvorí sekciu „Incidenty / Tickety“.
2	Systém zobrazí zoznam incidentov s filtrom podľa stavu, typu, priority alebo obdobia.
3	Používateľ vyberie konkrétny incident a otvorí jeho detail.
4	V detaile incidentu môže doplniť informácie (opis, dopady, kontaktnú osobu) alebo zmeniť stav incidentu (napr. z „Nový“ na „V riešení“).
5	Používateľ môže priradiť incident konkrétnemu riešiteľovi alebo tímu (napr. „SOC L1“, „SOC L2“, „interný IT zákazníka“).
6	Systém zmeny uloží, aktualizuje zobrazenie v portáli a sprístupní ich SOC analytikom.

ALT_14a_01 – Používateľ chce vytvoriť nový incident/ticket	Alternate

Krok	Aktivita
1	Používateľ klikne na „Vytvoriť incident/ticket“, vyplní formulár (popis, kritickosť, dotknuté systémy) a odošle ho; systém vytvorí nový záznam a priradí ho do frontu SOC.

ALT_14a_02 – Zmena stavu nie je povolená	Alternate

Krok	Aktivita
1	Používateľ sa pokúsi zmeniť stav incidentu, na ktorý nemá oprávnenie (napr. uzatvoriť incident, ktorý môže uzatvoriť len SOC); systém zmenu odmietne a zobrazí informáciu o nedostatočných právach.

Prípad použitia	UC_14b – Spolupracovať na riešení incidentu cez portál
Cieľ	UC_14b rozširuje UC_14 o kolaboračnú vrstvu pri riešení incidentu: komentáre medzi zákazníkom a SOC, emailové notifikácie o zmenách stavu, komentároch a deadlinoch, auditná stopa všetkých zmien a prístupov v tickete.
Vstupná podmienka	Incident existuje a je dostupný v portáli (UC_14a).
Vstupná podmienka	Používateľ má oprávnenie vidieť a komentovať daný incident.
Výstupná podmienka	K incidentu sú pridané komentáre a/alebo prípadné zmeny stavu iniciované zákazníkom.
Výstupná podmienka	Všetky zmeny a prístupy sú auditne zaznamenané; príslušné strany dostávajú notifikácie.

Basic Path	Basic Path

Krok	Aktivita
1	Používateľ otvorí detail incidentu v portáli.Používateľ otvorí detail incidentu v portáli.
2	Systém uloží komentár, zaznamená, kto a kedy ho pridal.
3	Systém uloží komentár, zaznamená, kto a kedy ho pridal.
4	Systém odošle emailové notifikácie relevantným stranám (Analytik, ďalší zástupcovia zákazníka) o novom komentári alebo zmene stavu.
5	Analytik odpovie cez svoj nástroj; odpoveď sa synchronizuje do portálu a zobrazí sa zákazníkovi ako ďalší komentár.
6	V histórii incidentu je možné spätne vidieť všetky komentáre, zmeny stavu a prístupy.

ALT_14b_01 – Notifikácie sú pre konkrétneho používateľa vypnuté	Alternate

Prípad použitia	UC_14c – Nastaviť preferencie, priority a integrácie portálu zákazníka
Cieľ	UC_14c rozširuje UC_14 o konfiguračnú časť pre zákazníka: nastavenie priorít a závažnosti incidentov z pohľadu zákazníka, nastavenie integračných kanálov (REST API / Webhooky) pre napojenie portálu na interné nástroje zákazníka (ticketing, chat, ITSM).
Vstupná podmienka	Používateľ má rolu s právom meniť nastavenia portálu pre svoju organizáciu.
Vstupná podmienka	Pre organizáciu sú definované aspoň základné priority a kategórie incidentov.
Výstupná podmienka	Sú definované preferované priority/závažnosti incidentov pre danú organizáciu.
Výstupná podmienka	Sú nakonfigurované (ak treba) integračné kanály – napr. Webhooky pre notifikácie do interného ticketingu.

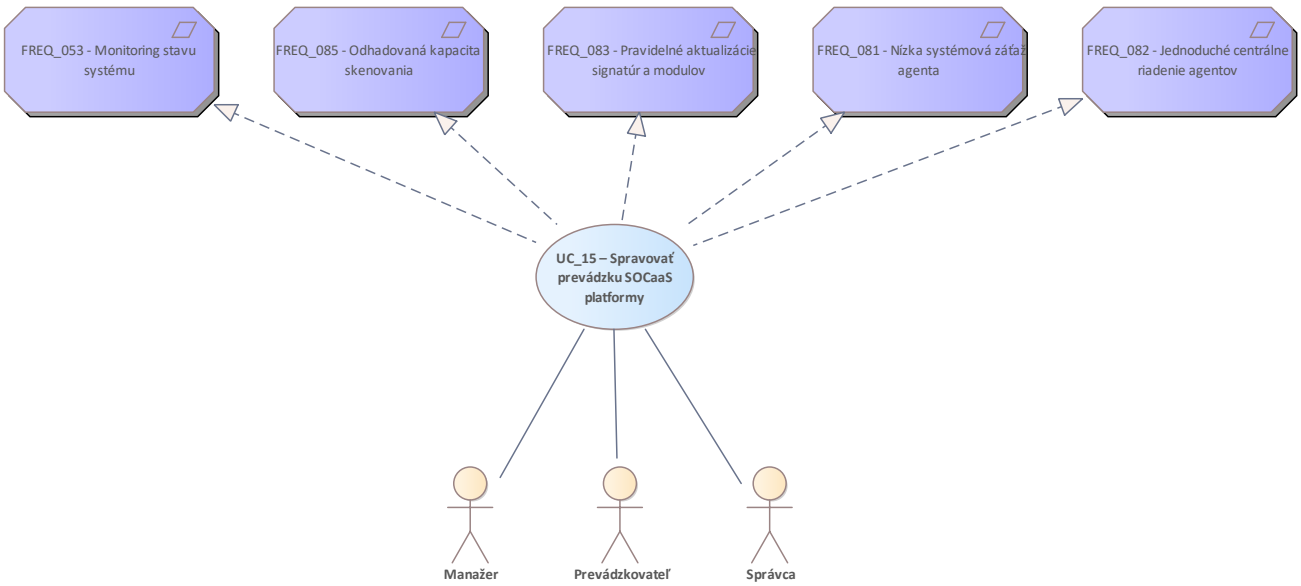
Basic Path	Basic Path

Krok	**Aktivita**
1	Manažér v portáli otvorí sekciu „Nastavenia organizácie“.
2	V časti „Incidenty“ nastaví mapovanie priorít/závažnosti (napr. ako sa majú SOC priority premietať do interných priorít zákazníka).
3	V časti „Integrácie“ zadá koncové URL pre Webhooky alebo API tokeny pre napojenie na interný ticketovací/ITSM systém.
4	Systém overí základnú konektivitu a uloží nastavenia.
5	Pri ďalších zmenách stavu incidentu alebo pri nových incidentoch systém podľa nastavení posiela notifikácie cez REST API / Webhooky do systémov zákazníka.

ALT_14c_01 – Neplatné alebo nedostupné integračné rozhranie	Alternate

Krok	**Aktivita**
1	Pri uložení nastavení integrácie testovací request zlyhá (timeout, 4xx, 5xx); systém na to upozorní Manažéra a integráciu uloží buď ako neaktívnu, alebo vyžaduje opravu parametrov.

4.3.2.14 UC_15 – Spravovať prevádzku SOCaaS platformy



Obrázok 18 : UC_15 – Spravovať prevádzku SOCaaS platformy

Prípad použitia	UC_15 – Spravovať prevádzku SOCaaS platformy
Cieľ	UC_15 rieši technickú prevádzku SOCaaS platformy tak, aby: bola stabilná, výkonná a dostupná, agenty a senzory nezaťažovali zbytočne prostredie zákazníka, sa platforma priebežne aktualizovala (signatúry, moduly), bola pod kontrolou kapacita spracovania/skenovania. Cieľom je, aby SOCaaS bežal spoľahlivo, vedel zvládnuť očakávaný objem dát a neohrozoval výkon systémov zákazníka.
Vstupná podmienka	SOCaaS platforma je nasadená v produkčnom prostredí (on-prem/cloud/SaaS).
Vstupná podmienka	Existujú monitorovacie nástroje a mechanizmy na sledovanie stavu platformy a agentov.
Vstupná podmienka	Sú definované základné prevádzkové parametre – akceptovateľná záťaž, kapacita spracovania, časy údržby.
Výstupná podmienka	Stav platformy a nasadených agentov je priebežne monitorovaný a známy Prevádzkovateľovi.
Výstupná podmienka	Aktualizácie signatúr a modulov sú vykonávané riadeným spôsobom a bez výrazného výpadku služby.
Výstupná podmienka	Kapacita spracovania/skenovania je plánovaná a Prevádzkovateľ vie identifikovať potrebu rozšírenia alebo optimalizácie.

Basic Path	Basic Path

Krok	**Aktivita**
1	Prevádzkovateľ sleduje stav SOCaaS platformy v prevádzkovom prehľade (dostupnosť komponentov, fronty, latencie, chybovosť).
2	Systém priebežne monitoruje stav nasadených agentov u zákazníkov – dostupnosť, verziu, záťaž na CPU/RAM.
3	Pri náraste počtu zákazníkov alebo objemu dát Prevádzkovateľ vyhodnotí kapacitu spracovania/skenovania a porovná ju s očakávaným rastom.
4	Na základe politiky aktualizácií naplánuje Prevádzkovateľ pravidelné aktualizácie signatúr a modulov (napr. mimo špičky), aby minimalizoval dopad na výkon.
5	Systém vykoná aktualizácie a overí, či sú agenty a komponenty po aktualizácii funkčné a reportujú v očakávanom rozsahu.
6	Prevádzkovateľ v prípade potreby upraví konfiguráciu agentov (odhady frekvencie skenovania, úroveň detailu, limity záťaže), aby nepreťažovali systémy zákazníkov.
7	Všetky prevádzkové zásahy (aktualizácie, zmeny konfigurácie, zásahy do kapacity) sú zaznamenané pre potreby auditu a diagnostiky.

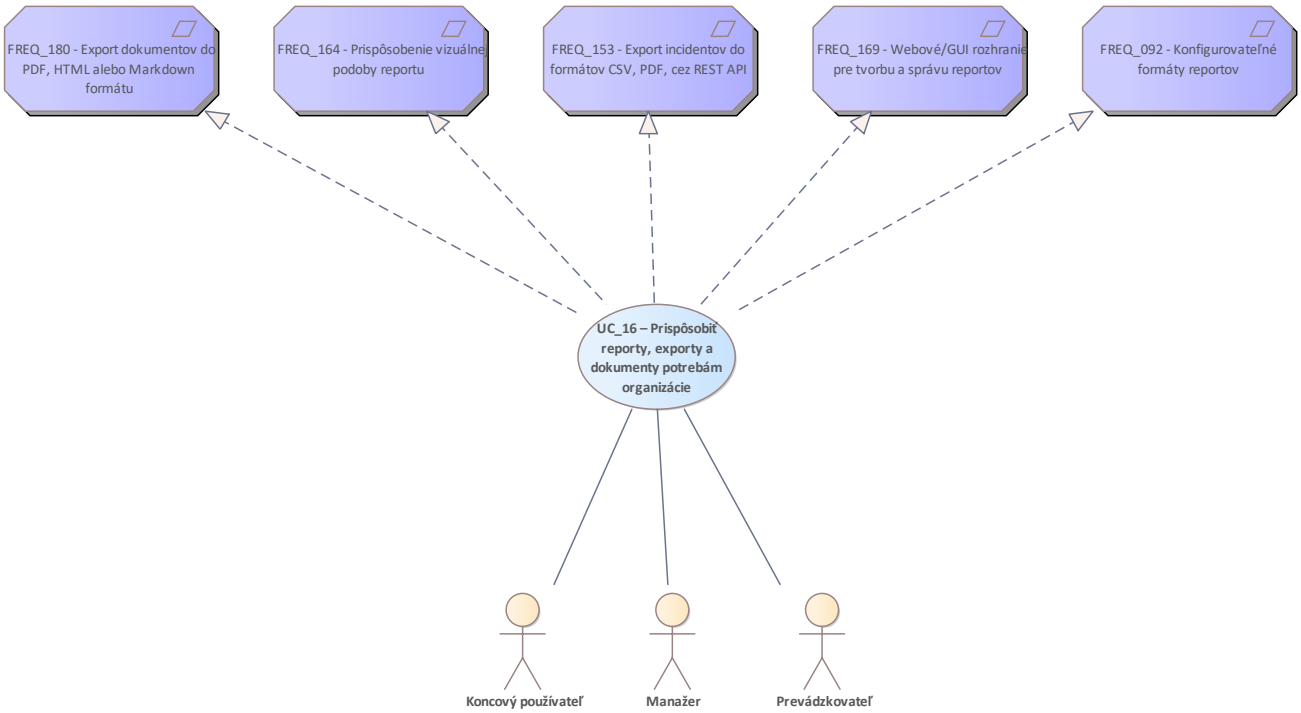
ALT_15_01 – Zistené preťaženie agentov alebo platformy	Alternate

Krok	**Aktivita**
1	Monitoring ukáže, že agenti alebo samotná platforma nadmerne zaťažujú systém (CPU, RAM, disk, sieť); Prevádzkovateľ upraví konfiguráciu (frekvenciu skenovania, rozsah dát), prípadne navrhne rozšírenie kapacity alebo optimalizáciu nasadenia.

ALT_15_02 – Zlyhanie aktualizácie signatúr alebo modulov	Alternate

Krok	**Aktivita**
1	Po spustení aktualizácie sa zistí, že časť agentov alebo komponentov aktualizáciu nedokončila alebo prestala reportovať; Prevádzkovateľ identifikuje dotknuté systémy, vráti ich na poslednú stabilnú verziu alebo zopakuje aktualizáciu s upravenými parametrami.

4.3.2.15 UC_16 – Prispôsobiť reporty, exporty a dokumenty potrebám organizácie



Obrázok 19 : UC_16 – Prispôsobiť reporty, exporty a dokumenty potrebám organizácie

Prípad použitia	UC_16 – Prispôsobiť reporty, exporty a dokumenty potrebám organizácie
Cieľ	UC_16 rieši konfiguráciu podoby výstupov zo SOCaaS: vzhľad reportov podľa firemnej identity (logo, farby, záhlavie), formáty exportov (CSV, XML, PDF, HTML, Markdown), export incidentov a dokumentov pre ďalšie spracovanie alebo archiváciu. Nadväzuje na UC_10b (ktorý rieši obsah a plánovanie reportov) tým, že umožňuje detailné nastavenie prezentácie a exportu, aby výstupy zapadli do prostredia zákazníka a do jeho nástrojov.
Vstupná podmienka	Existujú definované reporty a dokumenty, ktoré je možné generovať (UC_10b, UC_02b).
Vstupná podmienka	Používateľ má rolu, ktorá mu umožňuje meniť vzhľad a exportné nastavenia reportov/dokumentov.
Vstupná podmienka	SOCaaS platforma podporuje viac formátov exportu a základné šablóny vzhľadu.
Výstupná podmienka	Sú definované šablóny vzhľadu reportov pre jednotlivé organizácie (logo, farby, záhlavie).
Výstupná podmienka	Pre konkrétne typy reportov/incitentov sú nastavené preferované exportné formáty.
Výstupná podmienka	Používatelia vedia exportovať reporty, incidenty a dokumenty v požadovaných formátoch pre ďalšie spracovanie alebo archiváciu.
Basic Path	Basic Path
Krok	**Aktivita**

1	Manažér alebo Auditor otvorí v portáli sekciu „Nastavenie reportov a exportov“.
2	Vyberie typ výstupu, ktorý chce prispôsobiť (napr. „manažérsky report“, „incident overview“, „knowledge dokument“).
3	V časti Vzhľad zvolí alebo upraví šablónu:
4	V časti Formáty exportu zvolí, v akých formátoch má byť report/dokument dostupný (napr. CSV a PDF; pre dokumenty aj HTML/Markdown).
5	Používateľ si zobrazí náhľad reportu s novým vzhľadom a formátom, skontroluje rozloženie a čitateľnosť.
6	Po potvrdení systém uloží šablónu vzhľadu a preferované exportné formáty pre daný typ reportu/dokumentu.
7	Pri ďalšom generovaní reportu alebo pri zobrazení incidentu systém umožní priamo vybrať jeden z nakonfigurovaných exportov (napr. „Stiahnuť ako PDF“, „Export do CSV“, „Export dokumentu do HTML“).
8	Exportované súbory môžu byť stiahnuté používateľom alebo odoslané do ďalších systémov (napr. cez REST API), podľa nastavení organizácie.

ALT_16_01 – Požadovaný exportný formát nie je podporovaný	Alternate
Krok	**Aktivita**
1	Používateľ sa pokúsi nastaviť formát, ktorý platforma nepodporuje; systém ho na to upozorní a ponúkne dostupné alternatívy (napr. CSV namiesto XLSX, PDF namiesto DOCX).

ALT_16_02 – Chyba pri exporte veľkého objemu dát	Alternate
Krok	**Aktivita**
1	Pri exporte reportu s veľkým počtom záznamov dôjde k prekročeniu limitu alebo timeoutu; systém export preruší, informuje používateľa a ponúkne zúženie rozsahu (kratšie obdobie, filtrované dáta) alebo asynchrónny export.

ALT_16_03 – Zmena firemnej identity	Alternate
Krok	**Aktivita**
1	Organizácia zmení logo alebo korporátne farby; Manažér otvorí nastavenia vzhľadu, upraví šablónu (logo, farby) a po uložení budú všetky novovygenerované reporty používať novú identitu, pričom staršie reporty zostanú v pôvodnej podobe.

4.3.2.16 UC_17 – Spravovať používateľov a roly v SOCaaS platforme

UC_17 rieši administráciu používateľov a rolí v rámci SOCaaS:

vytváranie a úpravu účtov,

priraďovanie rolí (SOC, zákazník, auditor…),

nastavenie prístupov cez RBAC,

prípadné doplnenie vlastných atribútov.

Je to systémový/administrátorský UC, ktorý podporuje všetky ostatné UC tým, že určuje, kto čo v platforme môže vidieť a robiť.

Obrázok 20 : UC_16 – Prispôsobiť reporty, exporty a dokumenty potrebám organizácie

Prípad použitia	UC_16 – Prispôsobiť reporty, exporty a dokumenty potrebám organizácie
Cieľ	UC_16 rieši konfiguráciu podoby výstupov zo SOCaaS: vzhľad reportov podľa firemnej identity (logo, farby, záhlavie), formáty exportov (CSV, XML, PDF, HTML, Markdown), export incidentov a dokumentov pre ďalšie spracovanie alebo archiváciu. Nadväzuje na UC_10b (ktorý rieši obsah a plánovanie reportov) tým, že umožňuje detailné nastavenie prezentácie a exportu, aby výstupy zapadli do prostredia zákazníka a do jeho nástrojov.
Vstupná podmienka	Existujú definované reporty a dokumenty, ktoré je možné generovať (UC_10b, UC_02b).
Vstupná podmienka	Používateľ má rolu, ktorá mu umožňuje meniť vzhľad a exportné nastavenia reportov/dokumentov.
Vstupná podmienka	SOCaaS platforma podporuje viac formátov exportu a základné šablóny vzhľadu.
Výstupná podmienka	Sú definované šablóny vzhľadu reportov pre jednotlivé organizácie (logo, farby, záhlavie).
Výstupná podmienka	Pre konkrétne typy reportov/incitentov sú nastavené preferované exportné formáty.
Výstupná podmienka	Používatelia vedia exportovať reporty, incidenty a dokumenty v požadovaných formátoch pre ďalšie spracovanie alebo archiváciu.

Basic Path	Basic Path

Krok	**Aktivita**
1	Manažér alebo Auditor otvorí v portáli sekciu „Nastavenie reportov a exportov“.
2	Vyberie typ výstupu, ktorý chce prispôsobiť (napr. „manažérsky report“, „incident overview“, „knowledge dokument“).
3	V časti Vzhľad zvolí alebo upraví šablónu:
4	V časti Formáty exportu zvolí, v akých formátoch má byť report/dokument dostupný (napr. CSV a PDF; pre dokumenty aj HTML/Markdown).
5	Používateľ si zobrazí náhľad reportu s novým vzhľadom a formátom, skontroluje rozloženie a čitateľnosť.
6	Po potvrdení systém uloží šablónu vzhľadu a preferované exportné formáty pre daný typ reportu/dokumentu.
7	Pri ďalšom generovaní reportu alebo pri zobrazení incidentu systém umožní priamo vybrať jeden z nakonfigurovaných exportov (napr. „Stiahnuť ako PDF“, „Export do CSV“, „Export dokumentu do HTML“).
8	Exportované súbory môžu byť stiahnuté používateľom alebo odoslané do ďalších systémov (napr. cez REST API), podľa nastavení organizácie.

ALT_16_01 – Požadovaný exportný formát nie je podporovaný	Alternate

Krok	**Aktivita**
1	Používateľ sa pokúsi nastaviť formát, ktorý platforma nepodporuje; systém ho na to upozorní a ponúkne dostupné alternatívy (napr. CSV namiesto XLSX, PDF namiesto DOCX).

ALT_16_02 – Chyba pri exporte veľkého objemu dát	Alternate

Krok	**Aktivita**
1	Pri exporte reportu s veľkým počtom záznamov dôjde k prekročeniu limitu alebo timeoutu; systém export preruší, informuje používateľa a ponúkne zúženie rozsahu (kratšie obdobie, filtrované dáta) alebo asynchrónny export.

ALT_16_03 – Zmena firemnej identity	Alternate

Krok	**Aktivita**

1	Organizácia zmení logo alebo korporátne farby; Manažér otvorí nastavenia vzhľadu, upraví šablónu (logo, farby) a po uložení budú všetky novovygenerované reporty používať novú identitu, pričom staršie reporty zostanú v pôvodnej podobe.

4.4 Biznis architektúra

4.4.1 Identifikácia vlastníkov dizajnu koncových služieb (UX)

Meno apriezvisko	Pracovné zaradenie	Telefón	E-mail

Tabuľka 7 : Identifikácia vlastníkov dizajnu koncových služieb (UX)

4.4.2 Špecifikácia potrieb koncového zákazníka

Popis potreby používateľa	Referencia na výskum, z ktorej potreba plynie	Návrh riešenia potreby	Kvantita	Dopad na zákaznícku skúsenosť	Technická náročnosť	Biznis prínos	Priorita

Tabuľka 8 : Špecifikácia používateľských potrieb

Vysvetlenie k **Chyba! Neznámy argument prepínača.** (bunky v tabuľke zľava doprava):

- Popis potreby používateľa: je zápis konkrétnej potreby používateľa v prvej osobe, ktorý nepopisuje riešenie.
- Referencia na výskum, z ktorej potreba plynie: popisuje konkrétne rozhovory s respondentami, kde bola požiadavka vyslovená.
- Návrh riešenia potreby: je jedno z možných riešení, ktoré bolo kvantitatívne validované.
- Kvantita: výstup z dotazníka, kde používatelia hodnotili návrh riešenia potreby na škále od 1 po 10, kde 1 je "Nie je to pre mňa dôležité" a 10 je "Je to pre mňa veľmi dôležité."
- Dopad na zákaznícku skúsenosť: je určená kombináciou kvalitatívnych a kvantitatívnych informácii z výskumu a je určená na stupnici MoSCoW[1].
- Technická náročnosť je vstupom od technického riešiteľa.
- Biznis prínos je vstupom od biznis zadávateľa.
- Priorita je výsledná dôležitosť implementácie tohto riešenia po zvážení stĺpcov Dopad na zákaznícku skúsenosť, Technická náročnosť a Biznis prínos.

4.4.3 Návrh prototypov používateľského rozhrania

[1] https://en.wikipedia.org/wiki/MoSCoW_method

4.4.4 Návrh vizuálov obrazoviek

5 Dátová architektúra

Nasledujúce kapitoly popisujú návrh entít perzistentnej vrstvy modulu.
Každá entita obsahuje:

- Definíciu entity
- Zoznam základných atribútov
- Názov atribútu
- Dátový typ
- Povinnosť – atribút musí byť naplnený (not null)
- Popis – vysvetlenie čo atribút vyjadruje, ak to z názvu nie je zrejmé, prípadne popis validácie

6 Aplikačná architektúra

Aplikačná architektúra modulu CNM je kompletne namodelovaná vnástroji Sparx Enterprise Architect (EA) vnotácii Archimate 3.0.

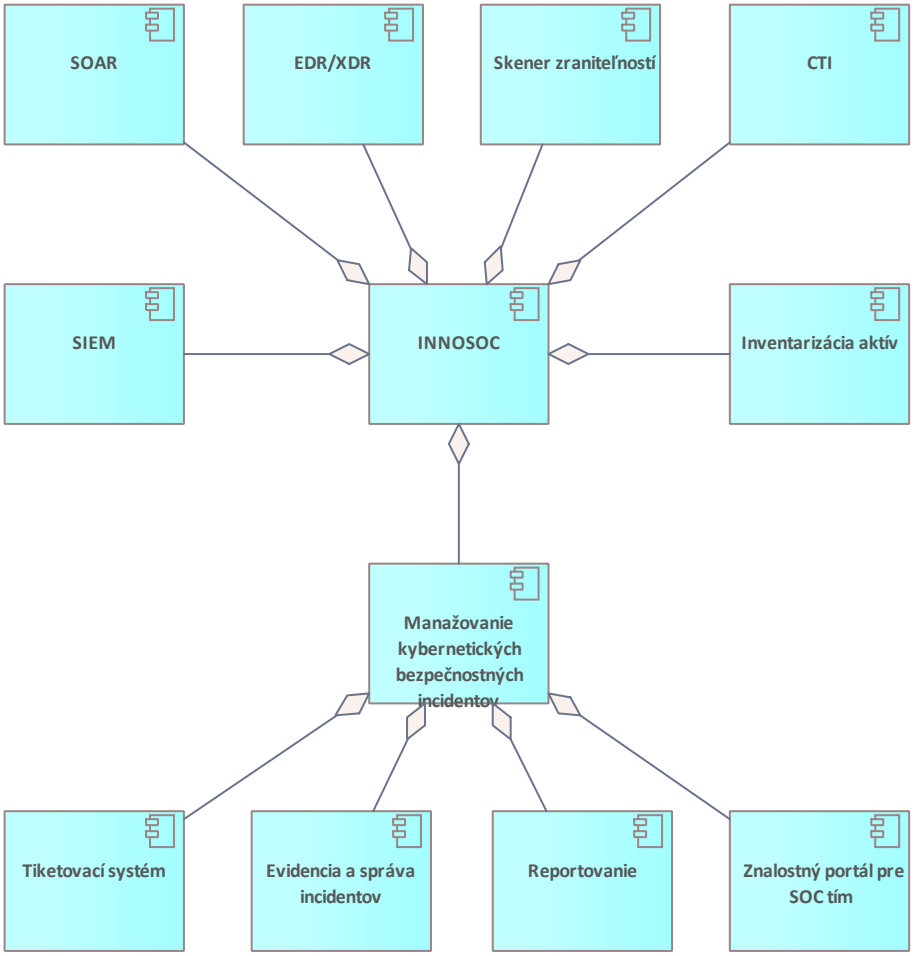
Vnasledujúcej kapitole je zobrazený diagram aplikačnej architektúry spopismi objektov, ktoré boli vygenerované zEA, ako výstup.

Všetky popisy objektov aplikačnej architektúry ako aplikačné služby, aplikačné komponenty, funkčné komponenty a dátové objekty sú súčasťou modelu vEA, zaznamenané v„Popise" objektu (note).

Nakoľko je výstup pre modelovanie aplikačnej architektúry DNR generovaný zEA, vprípade, že je daný objekt aplikačnej architektúry použitý viackrát, jeho popis je identický.

6.1 Aplikačná architektúra

6.2 Aplication Viewpoints



Obrázok 21 : Aplication Viewpoints Components

Diagram predstavuje HL zoznam komponentov riešenia.

Popis používaných prvkov:

CTI

CTI (Cyber Threat Intelligence) predstavuje kľúčový stavebný prvok SOCaaS architektúry, pretože poskytuje schopnosť obohacovať detekčné pravidlá, korelačné mechanizmy a playbooky o externé informácie o hrozbách – vrátane IOC, TTP, profilovania útočníkov, kampaní a súvisiacich zraniteľností. V prostredí viaczákaznícke služby SOCaaS zohráva úlohu pri:

• Distribúcii a správe threat feedov naprieč tenantmi,
• Automatickom obohacovaní SIEM a EDR dát o známe hrozby,
• Vytváraní časových línií útokov a priraďovaní k MITRE ATT&CK technikám,
• Podpore procesov threat huntingu a forenznej analýzy,
• Prioritizácii incidentov podľa kontextu hrozieb.

Pre návrh riešenia boli zvolené open-source platformy, ktoré pokrývajú rôzne aspekty CTI – od zberu IOC cez vizualizáciu, až po STIX/TAXII kompatibilitu.

EDR/XDR

EDR (Endpoint Detection and Response) a XDR (Extended Detection and Response) predstavujú základné technologické piliere pre detekciu hrozieb na úrovni koncových zariadení. V prostredí SOCaaS slúžia na zber, koreláciu a reakciu na udalosti, ktoré by inak unikli tradičným perimeterovým detekciám. XDR rozširuje koncept EDR o schopnosť integrovať dáta zo sietí, cloudov, e-mailových systémov a iných vrstiev.

Evidencia a správa incidentov

Evidencia a správa incidentov je jadrovým prvkom každej bezpečnostnej prevádzky (SOC). Tento podkomponent zaisťuje systematickú dokumentáciu, sledovanie a manažovanie bezpečnostných udalostí a incidentov v priebehu ich životného cyklu – od detekcie cez analýzu až po uzavretie. Kvalitný systém evidencie musí umožniť tímom koordinovane spolupracovať, dokumentovať kroky, evidovať súvisiace artefakty (observables) a prepojiť incidenty

s relevantnými hrozbami, systémami alebo historickými prípadmi. V ideálnom prípade podporuje aj pokročilé obohacovanie údajov, audit, multitenantnosť a možnosť spätného skúmania incidentov.

INNOSOC

Inventarizácia aktív

Inventarizácia aktív je základným pilierom každého bezpečnostného riešenia. Umožňuje SOC tímu získať prehľad o všetkých zariadeniach, systémových entitách, aplikáciách a virtuálnych či cloudových zdrojoch, ktoré tvoria infraštruktúru organizácie. V prostredí SOCaaS zohráva ešte významnejšiu úlohu, pretože umožňuje centralizovanú správu, kategorizáciu, monitorovanie a sledovanie bezpečnostného stavu infraštruktúry naprieč rôznymi zákazníkmi.

Manažovanie kybernetických bezpečnostných incidentov

Efektívne riešenie kybernetických incidentov je kľúčovým pilierom SOCaaS architektúry. Nezahŕňa len samotné zaznamenanie udalostí, ale komplexný cyklus ich evidencie, manažmentu, reakcie, reportovania a uchovávania znalostí. Pre SOC tím je zásadné, aby boli incidenty riadené systémovo, s dôrazom na trasovateľnosť, analytickú prácu, koordináciu a znalostnú podporu. Efektívna a koordinovaná reakcia na bezpečnostné incidenty je nevyhnutným pilierom každého SOCaaS riešenia. V rámci architektúry INNOSOC boli identifikované štyri podkomponenty, ktoré spoločne tvoria integrovaný systém na správu, evidenciu, dokumentáciu a riešenie incidentov:

1. Tiketovací systém
2. Evidencia a správa incidentov
3. Reportovanie
4. Znalostný portál pre SOC tím

Reportovanie

Komponent reportovania v rámci SOCaaS architektúry slúži ako centrálny prostriedok na agregáciu, vizualizáciu a distribúciu bezpečnostných informácií. Jeho úlohou je zabezpečiť pravidelné aj ad-hoc výstupy o stave kybernetickej bezpečnosti pre rôzne cieľové skupiny – od SOC analytikov, cez vedúcich tímov, až po vedenie organizácie alebo klientov. Takýto reportovací systém musí pokrývať:

• Generovanie metriky incidentov, výstrah, SLA a KPIs,
• Prehľady trendov v čase a hodnotenie výkonnosti bezpečnostných opatrení,
• Prispôsobenie obsahu podľa úrovne detailu (technické vs. strategické),
• Automatizáciu a plánovanie distribúcie výstupov,
• Spätnú analýzu a archiváciu historických údajov.

SIEM

SIEM je srdcom SOCaaS riešenia. Zabezpečuje agregáciu, spracovanie, koreláciu a analýzu bezpečnostných udalostí z rôznych zdrojov, v reálnom čase. Umožňuje analytikom identifikovať anomálie, generovať upozornenia a eskalovať incidenty, pričom zvyšuje viditeľnosť nad infraštruktúrou klienta.

Skener zraniteľností

Skener zraniteľností je základným stavebným kameňom pre zabezpečenie proaktívneho prístupu v SOCaaS architektúre. Umožňuje pravidelne identifikovať slabé miesta v infraštruktúre, hodnotiť stav aktualizácií, konfigurácií a nastavení, a poskytovať informácie pre ďalšiu prioritizáciu a plánovanie nápravných opatrení. Výstupy skenera sú často zdrojom pre SOAR systémy, SLA metriky, reporting ako aj pre hodnotenie bezpečnostnej úrovne klienta.

SOAR

SOAR (Security Orchestration, Automation and Response) je komponent zodpovedný za automatizáciu reakcií na incidenty, orchestráciu bezpečnostných nástrojov a podporu rozhodovania analytikov. V SOCaaS predstavuje základnú zložku umožňujúcu škálovanie reakčných kapacít bez nutnosti zvyšovať počet personálu. Je nevyhnutný najmä pri spracovaní veľkého množstva alertov, kde znižuje MTTR a MTTC metriky.

Tiketovací systém

Tiketovací systém slúži ako ústredný komunikačný a organizačný kanál pre správu bezpečnostných incidentov počas ich celého životného cyklu. Umožňuje vytváranie, priraďovanie a sledovanie úloh a komunikáciu medzi analytikmi, pričom podporuje audit, SLA monitoring, eskaláciu a notifikácie.

Znalostný portál pre SOC tím

Znalostný portál pre SOC tím je dôležitým stavebným kameňom každého moderného bezpečnostného operačného centra. Slúži ako centrálny repozitár know-how, playbookov, postupov, odporúčaní, analytických návodov a často aj historických lekcií (lessons learned) z incidentov. Znalostný portál:

• Zvyšuje efektivitu a konzistentnosť reakcie na incidenty,
• Umožňuje rýchle zaškolenie nových členov tímu,

• Podporuje štandardizáciu procesov a metodík,
• Umožňuje tímu uchovávať a zdieľať overené postupy a vlastné analytické skúsenosti,
• Posilňuje schopnosť kolektívne sa učiť z incidentov a budovať interné "threat intel" vedomosti.

6.3 Návrh riešenia dizajnu aplikačných služieb

6.3.1 Existujúce aplikačné rozhrania

Projekt CNM ráta so zachovaním služieb modulu eNotify - SendNotification, SendNotificationUsingTemplate. Pre tento účel vznikne služba LegacyService, ktorá implementuje rozhranie prijímajúce asynchrónne správy v štruktúre requestov SendNotification a SendNotificationUsingTemplate. Detailnejší popis je uvedený v nasledujúcej podkapitole.

6.3.2 Zanikajúce aplikačné rozhrania

6.3.3 Nové aplikačné rozhrania

6.4 Integrácie medzi systémami

6.4.1 Zoznam existujúcich integrácií bez zmeny

6.4.2 Zoznam a popis navrhovaných integrácií

6.4.3 Zoznam a popis požadovaných integračných rozhraní

6.4.4 Návrh poskytovaných aplikačných rozhraní systému (modulu)

7 Technologická architektúra

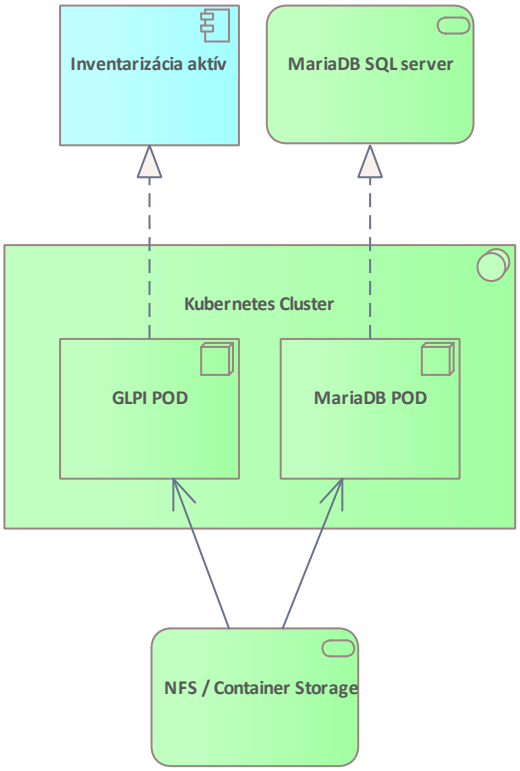
Kapitola popisuje fyzickú architektúra a definuje požiadavky pre testovacie a produkčné prostredie.

Navrhovaná prevádzka je plánovaná na dvoch identických prostrediach líšiacimi sa len množstvom a typom zdrojov:
· **PROD** prostredie – prevádzkové prostredie s reálnymi dátami a prevádzkou verejného portálu.
· **TEST** prostredie – testovacie, školiace, pred produkčné prostredie. Celé TEST prostredie je dostupné prostredníctvom VPN pre privilegovaných používateľov.

7.1 Technologická architektúra

7.2 Technology Viewpoint INNOSOC Common

7.3 Technology Viewpoint Inventarizacia aktiv



Obrázok 22 : Technology Usage Viewpoint Inventarizacia aktiv alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom. Alt 1 predstavuje využitie Databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou SQL servera.

Popis používaných prvkov:

Inventarizácia aktív

Inventarizácia aktív je základným pilierom každého bezpečnostného riešenia. Umožňuje SOC tímu získať prehľad o všetkých zariadeniach, systémových entitách, aplikáciách a virtuálnych či cloudových zdrojoch, ktoré tvoria infraštruktúru organizácie. V prostredí SOCaaS zohráva ešte významnejšiu úlohu, pretože umožňuje centralizovanú správu, kategorizáciu, monitorovanie a sledovanie bezpečnostného stavu infraštruktúry naprieč rôznymi zákazníkmi.

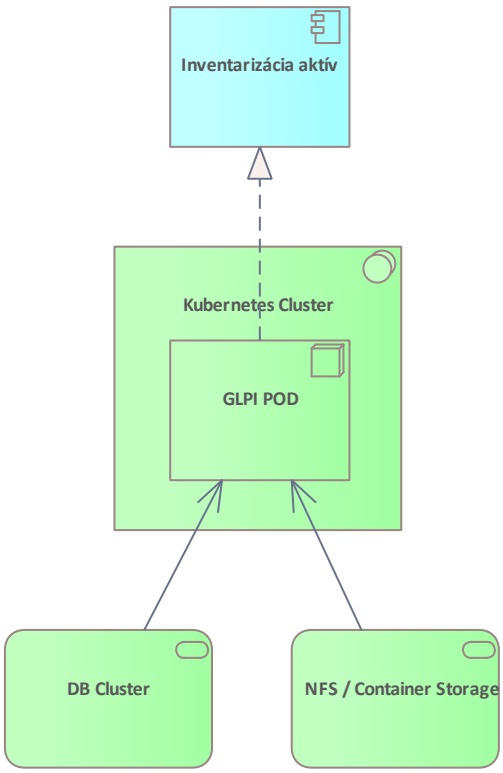
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

MariaDB SQL server
Predstavuje technologickú službu relačnej MariaDB SLQ databázy.

GLPI POD
Predstavuje POD GLPI pre invertarizáckiu aktív.

MariaDB POD
Predstavuje POD MariaDB pre relačnú SQL DB.



Obrázok 23 : Technology Usage Viewpoint Inventarizacia aktiv alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.
Alt 2 predstavuje využitie Databázy priamo vo forme centralizovaného DB Clustra.

Popis používaných prvkov:

Inventarizácia aktív

Inventarizácia aktív je základným pilierom každého bezpečnostného riešenia. Umožňuje SOC tímu získať prehľad o všetkých zariadeniach, systémových entitách, aplikáciách a virtuálnych či cloudových zdrojoch, ktoré tvoria infraštruktúru organizácie. V prostredí SOCaaS zohráva ešte významnejšiu úlohu, pretože umožňuje centralizovanú správu, kategorizáciu, monitorovanie a sledovanie bezpečnostného stavu infraštruktúry naprieč rôznymi zákazníkmi.

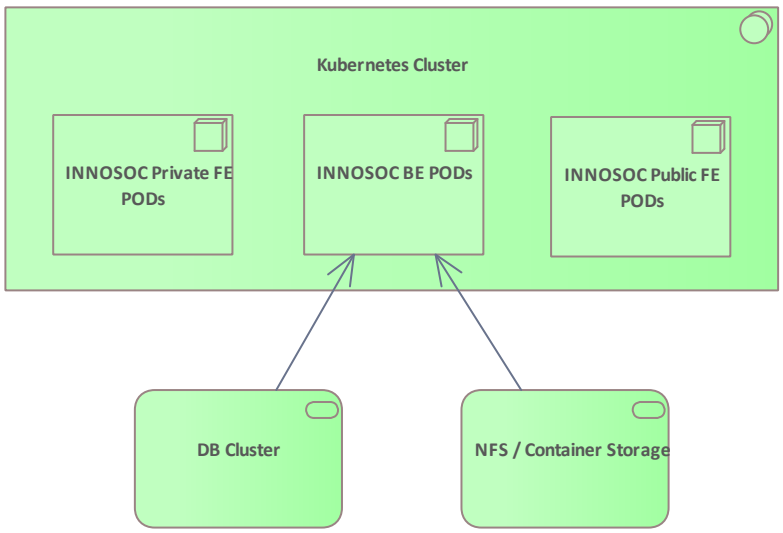
DB Cluster
Predstavuje službu clustrovanej relačnej databázy

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

GLPI POD
Predstavuje POD GLPI pre invertarizáckiu aktív.

7.4 Technology Viewpoint Kubernetes



Obrázok 24 : Technology Usage Viewpoint CNM and Containers maping

Diagram znázorňuje priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Popis používaných prvkov:

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

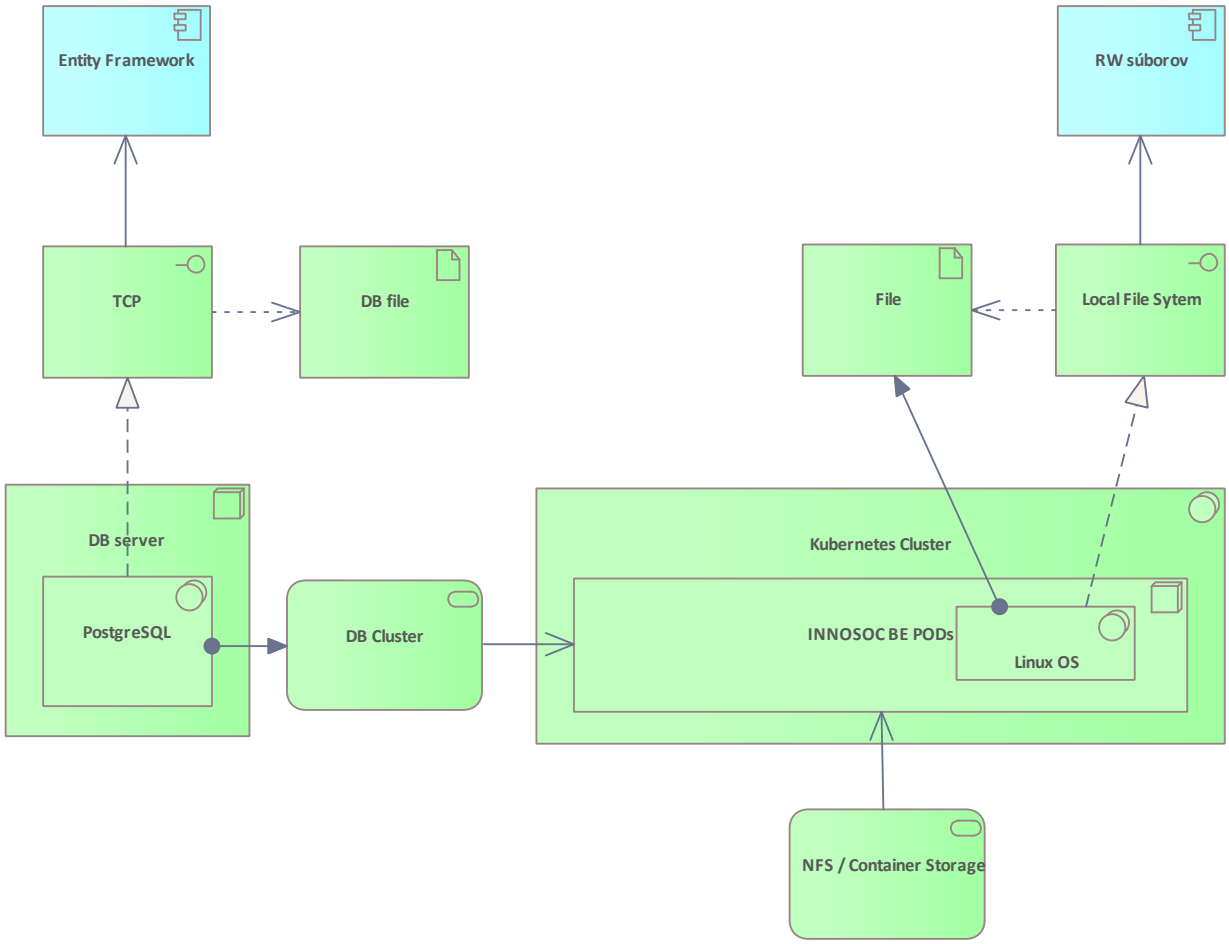
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

INNOSOC BE PODs
Predstavuje PODy CNM BE

INNOSOC Private FE PODs
Predstavuje PODy CNM FE Private

INNOSOC Public FE PODs
Predstavuje PODy CNM FE Public



Obrázok 25 : Technology Usage Viewpoint CNM BE, DB and File System

Diagram repezentuje a bližšie popisuje využívanie perzistentnej vrstvy pre potreby BIT NC a CNM BE modulu a pomocou jeho komponentu Dátovej vrstvy ktorý zabezpečuje prácu s PostgreSQL a Local File System.

Popis používaných prvkov:

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

DB file
DB file - súbor reprezentujúci databázový súbor MariaDB

DB server
Predstavuje MariaDB server

File
File - súbor reprezentujúci dáta ako prílohy, obrázky, dokumenty a iné

Entity Framework
Predstavuje aplikačný modul Entity Framework

RW súborov
Predstavuje modul RW nad súbormi

Local File Sytem
Lokálny súborový systém poskytujúci prácu so súbormi realizovaný operačným systémom pod ktorým je spúšťaný BE modul

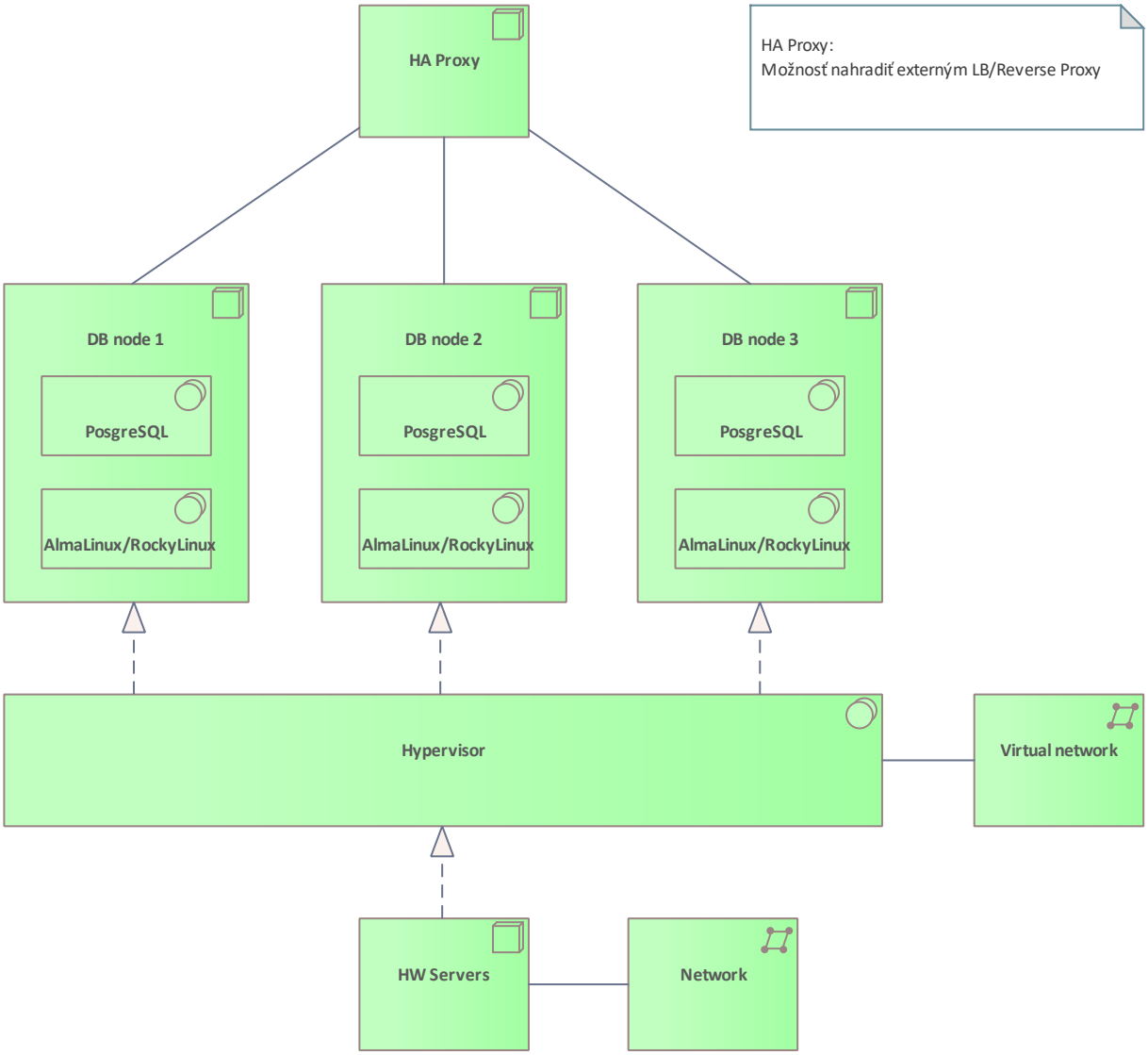
TCP
Predstavuje client server komunikáciu pomocou TCP protokolu

Kubernetes Cluster
Predstavuje Kubernetes Cluster

INNOSOC BE PODs
Predstavuje PODy CNM BE

Linux OS

PostgreSQL
Predstavuje PostgreSQL relačnú databázu



Obrázok 26 : Technology Viewpoint DB Cluster

Diagram znázorňuje technologickú architektúru PostgreSQL Clustra.

Popis používaných prvkov:

DB node 1
Predstavuje Node 2 MariaDB Galera Clustra

DB node 2
Predstavuje Node 2 MariaDB Galera Clustra

DB node 3
Predstavuje Node 3 MariaDB Galera Clustra

HA Proxy
Predstavuje Internú reverse proxy postavenú na HA Proxy

HW Servers
Predstavuje HW serverovú infraštruktúru

Hypervisor
Predstavuje Hypervisor 1. alebo 2. typu

Network

Predstavuje sieť/subsieť HW infraštruktúry

Virtual network
Predstavuje virtuálnu sieť/subsieť Hypervisora

Note
HA Proxy:
Možnosť nahradiť externým LB/Reverse Proxy

AlmaLinux/RockyLinux
Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

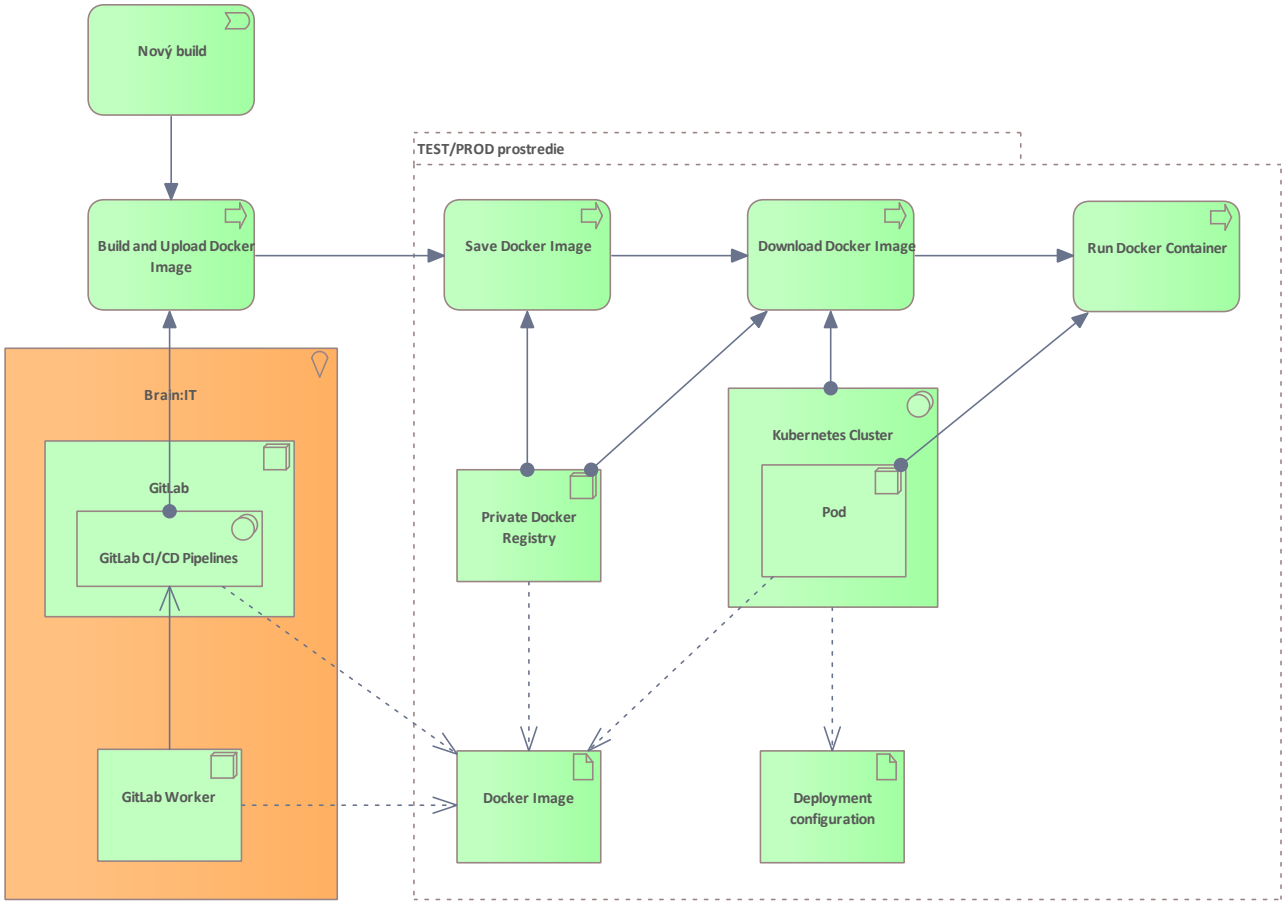
PosgreSQL
Predstavuje PosgreSQL relačnú databázu

AlmaLinux/RockyLinux
Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

PosgreSQL
Predstavuje PosgreSQL relačnú databázu

AlmaLinux/RockyLinux
Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

PosgreSQL
Predstavuje PosgreSQL relačnú databázu



Obrázok 27 : Technology Viewpoint Development CI/CD TEST/PROD

Diagram znázorňuje proces buildu a nasadenia novej verzie balíka v podobe Docker image do TEST/PROD prostredia. Diagram je využitelný pre prípad vlastných balíkov, pre ostatné existujúce sa využíva verejný DockerHub zdroj.

Popis používaných prvkov:

Build and Upload Docker Image
Build proces a nahratie Docker Image do Docker Registry

Download Docker Image
Proces uloženie Docker Image do Docker Registry

Nový build
Spustenie nového build procesu

Run Docker Container
Proces spustenia Docker Containera

Save Docker Image
Proces uloženie Docker Image do Docker Registry

TEST/PROD prostredie
Predstavuje interné DEV a TEST prostredie

Brain:IT
Lokalita Brain:IT

Private Docker Registry
Predstavuje private Docker Registry

Deployment configuration
Reprezentácia Kubernetes Deployment artifaktu.

Docker Image
Reprezentácia Docker Image artifaktu.

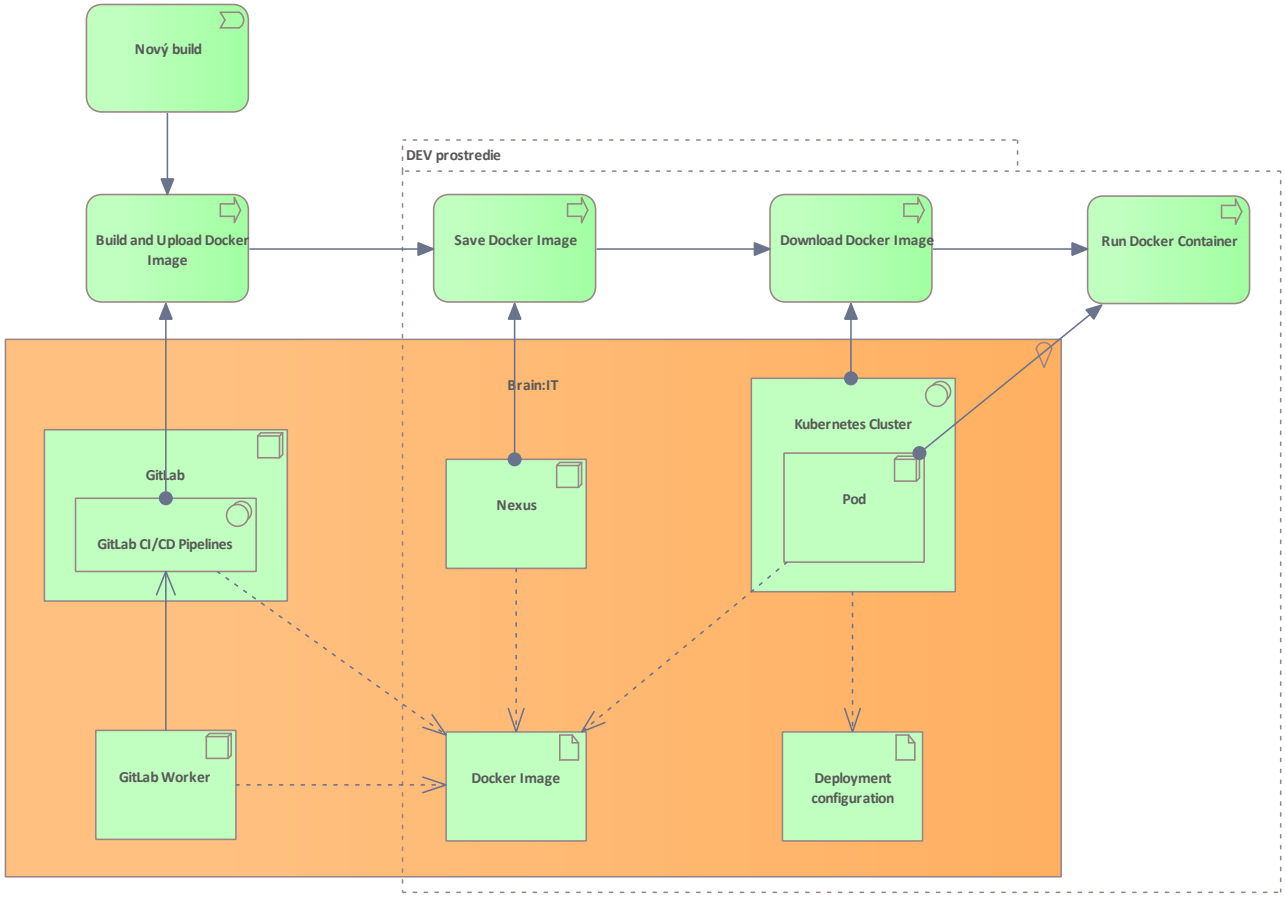
GitLab
Predstavuje inštanciu GitLab.

GitLab Worker
Predstavuje insštanciu GitLab Worker

Kubernetes Cluster
Predstavuje Kubernetes Cluster

GitLab CI/CD Pipelines
GitLab CI/CD Pipelines je séria úloh zabezpečujúca kompiláciu, testy, konfiguráciu, nasadenie a iné v rámci GitLabu.

Pod
Predstavuje inštanciu Podu, v rámci ktorej je spustený nový Docker Image v podobe Docker Containera



Obrázok 28 : Technology Viewpoint Developmnent CI/CD DEV

Diagram znázorňuje proces buildu a nasadenia novej verzie balíka v podobe Docker image do DEV prostredia. Diagram je využitelný pre prípad vlastných balíkov, pre ostatné existujúce sa využíva verejný DockerHub zdroj.

Popis používaných prvkov:

Build and Upload Docker Image
Build proces a nahratie Docker Image do Docker Registry

Download Docker Image
Proces uloženie Docker Image do Docker Registry

Nový build
Spustenie nového build procesu

Run Docker Container
Proces spustenia Docker Containera

Save Docker Image
Proces uloženie Docker Image do Docker Registry

DEV prostredie
Predstavuje interné DEV a TEST prostredie

Brain:IT
Lokalita Brain:IT

Deployment configuration
Reprezentácia Kubernetes Deployment artifaktu.

Docker Image

Reprezentácia Docker Image artifaktu.

GitLab
Predstavuje inštanciu GitLab.

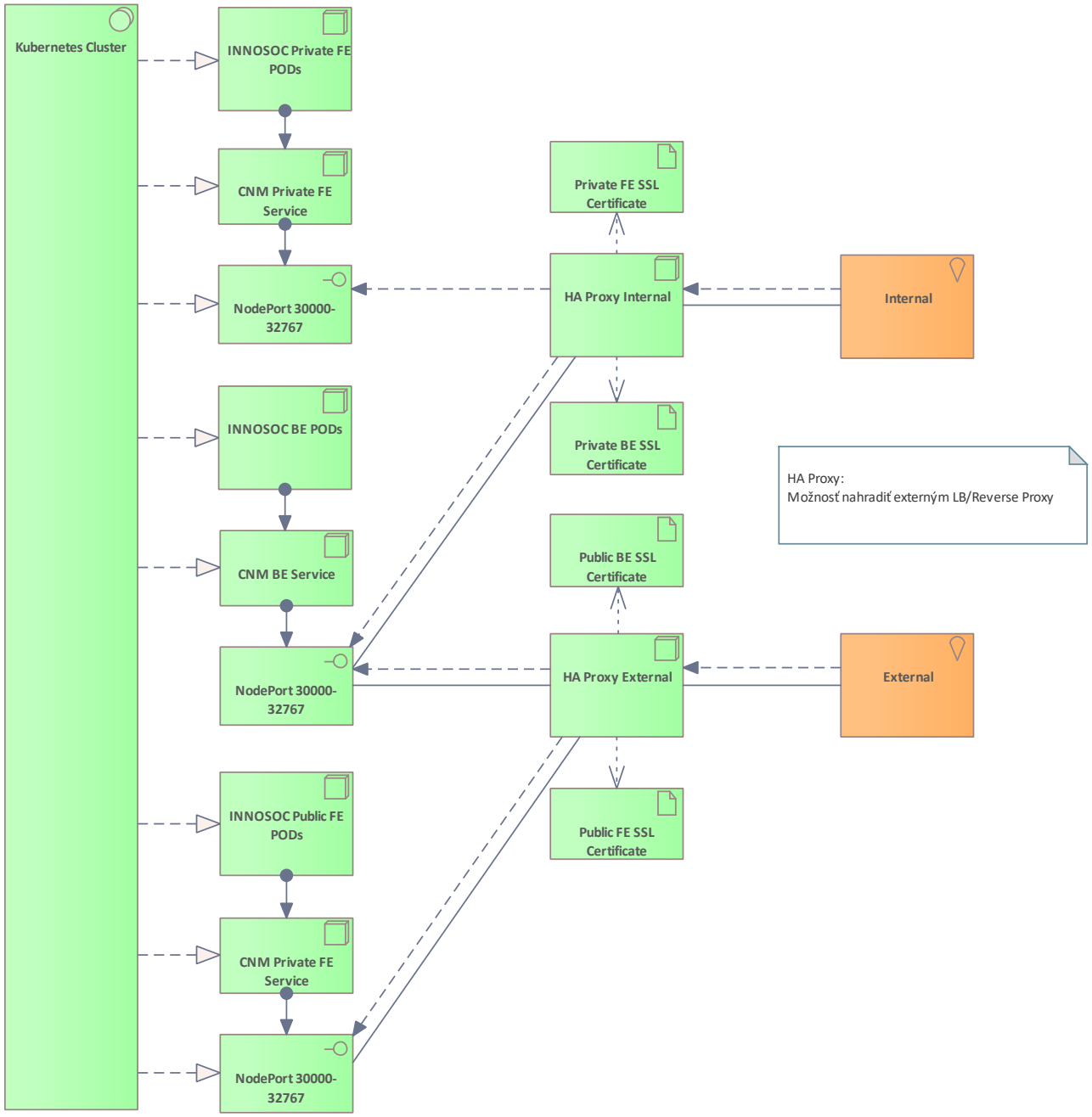
GitLab Worker
Predstavuje insštanciu GitLab Worker

Kubernetes Cluster
Predstavuje Kubernetes Cluster

Nexus
Predstavuje private Docker Registry

GitLab CI/CD Pipelines
GitLab CI/CD Pipelines je séria úloh zabezpečujúca kompiláciu, testy, konfiguráciu, nasadenie a iné v rámci GitLabu.

Pod
Predstavuje inštanciu Podu, v rámci ktorej je spustený nový Docker Image v podobe Docker Containera



Obrázok 29 : Technology Viewpoint Interconnect

Diagram znázorňuje deployment a prepojenie vystavených služieb kubernetes a LB/Reverse Proxy pre dve zóny.

Popis používaných prvkov:

CNM BE Service
Predstavuje CNM BE Service

CNM Private FE Service
Predstavuje CNM FE Private Service

CNM Private FE Service
Predstavuje CNM FE Private Service

External
Predstavuje externé prostredie Internet

HA Proxy External
Predstavuje Externú reverse proxy postavenej na HA Proxy

HA Proxy Internal
Predstavuje Internú reverse proxy postavenej na HA Proxy

Internal
Predstavuje interné prostrednie BRAIN:IT

Private BE SSL Certificate
Predstavuje validný Private SSL certifikát pre potreby HTTPS

Private FE SSL Certificate
Predstavuje validný SSL certifikát pre potreby HTTPS

Public BE SSL Certificate
Predstavuje validný Public SSL certifikát pre potreby HTTPS

Public FE SSL Certificate
Predstavuje validný Public SSL certifikát pre potreby HTTPS

NodePort 30000-32767
Predstavuje smerovanie typu NodePort z rozsahu 30000-32767

NodePort 30000-32767
Predstavuje smerovanie typu NodePort z rozsahu 30000-32767

NodePort 30000-32767
Predstavuje smerovanie typu NodePort z rozsahu 30000-32767

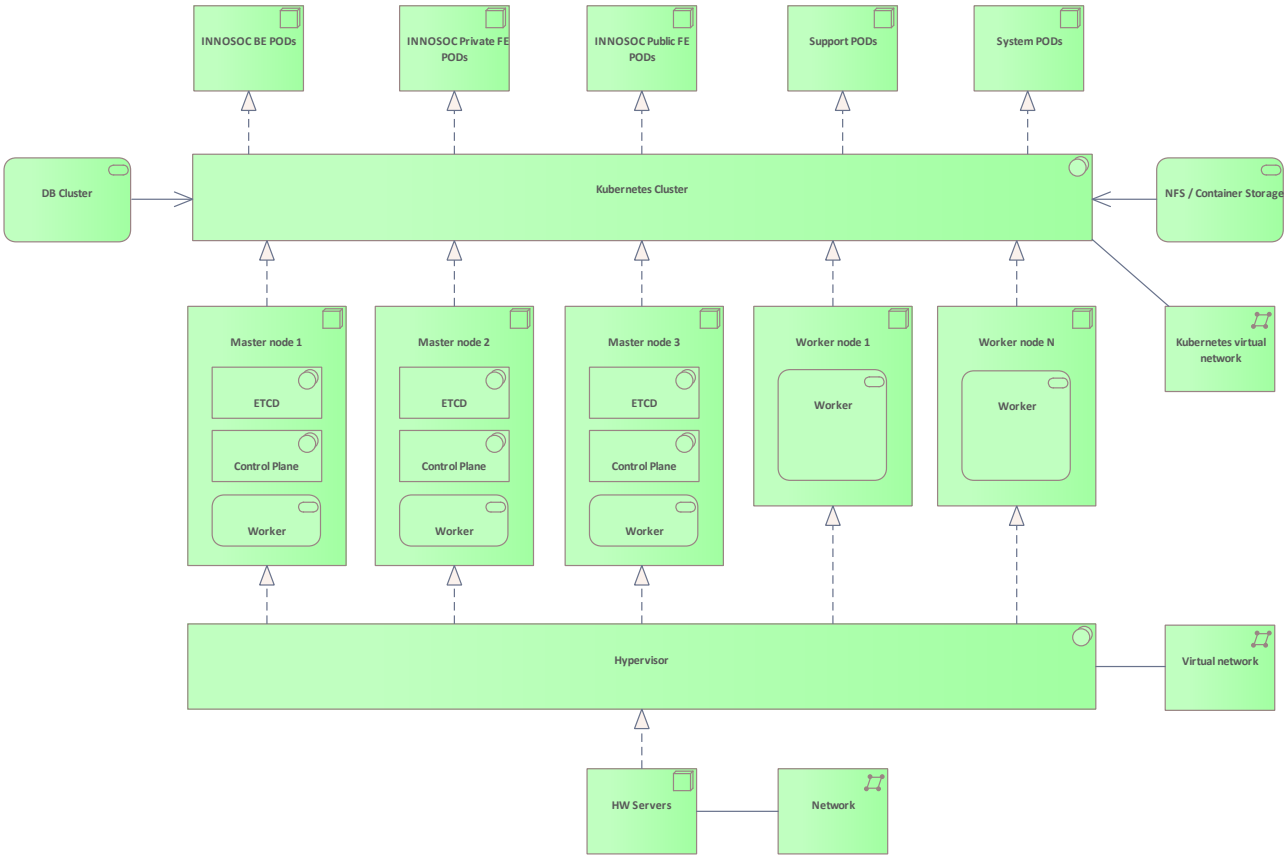
Note
HA Proxy:
Možnosť nahradiť externým LB/Reverse Proxy

Kubernetes Cluster
Predstavuje Kubernetes Cluster

INNOSOC BE PODs
Predstavuje PODy CNM BE

INNOSOC Private FE PODs
Predstavuje PODy CNM FE Private

INNOSOC Public FE PODs
Predstavuje PODy CNM FE Public



Obrázok 30 : Technology Viewpoint Kubernetes Cluster

Predstavuje rolu a službu Worker nodu .

Popis používaných prvkov:

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

HW Servers
Predstavuje HW serverovú infraštruktúru

Hypervisor
Predstavuje Hypervisor 1. alebo 2. typu

Kubernetes virtual network
Predstavuje virtuálnu sieť/subsieť Kubernetes Clustra

Master node 1
Predstavuje Master node Kubernetes Clustra

Master node 2
Predstavuje Master node Kubernetes Clustra

Master node 3
Predstavuje Master node Kubernetes Clustra

Network
Predstavuje sieť/subsieť HW infraštruktúry

Support PODs
Predstavuje PODy podporných služieb

System PODs
Predstavuje PODy systémových služieb

Virtual network
Predstavuje virtuálnu sieť/subsieť Hypervisora

Worker node 1
Predstavuje Worker node Kubernetes Clustra

Worker node N
Predstavuje Worker node Kubernetes Clustra

Kubernetes Cluster
Predstavuje Kubernetes Cluster

INNOSOC BE PODs
Predstavuje PODy CNM BE

INNOSOC Private FE PODs
Predstavuje PODy CNM FE Private

INNOSOC Public FE PODs
Predstavuje PODy CNM FE Public

Worker
Predstavuje rolu a službu Worker nodu

Control Plane
Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD
Predstavuje ETCD databázu

Worker
Predstavuje rolu a službu Worker nodu

Control Plane
Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD
Predstavuje ETCD databázu

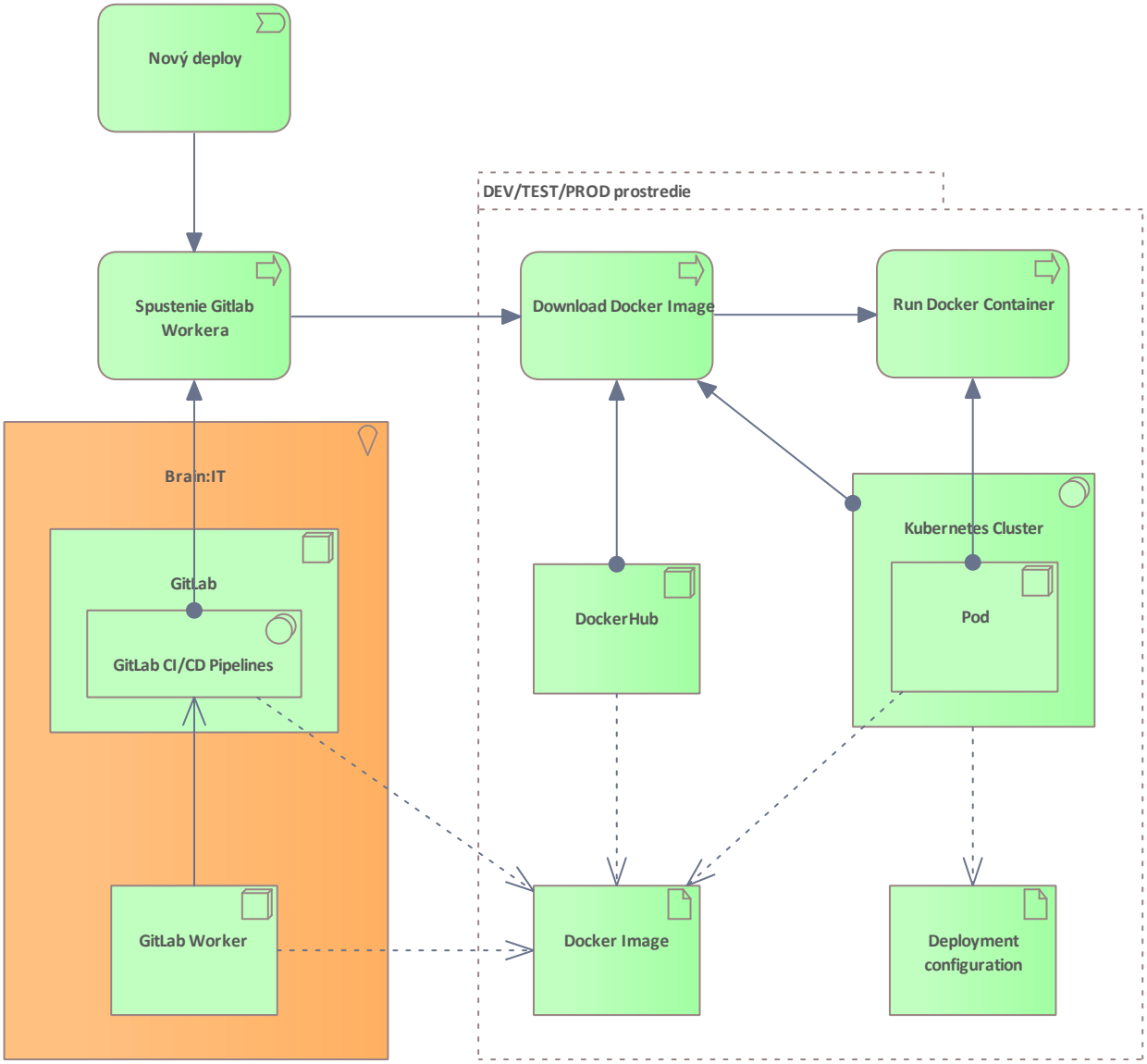
Worker

Control Plane
Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD
Predstavuje ETCD databázu

Worker

Worker



Obrázok 31 : Technology Viewpoint standard CI/CD DEV/TEST/PROD

Popis používaných prvkov:

Download Docker Image
Proces uloženie Docker Image do Docker Registry

Nový deploy
Spustenie nového deploy procesu

Run Docker Container
Proces spustenia Docker Containera

Spustenie Gitlab Workera
proces spustenie Gitlam Workera pre nasadenie novej verzie balíka.

DEV/TEST/PROD prostredie
Predstavuje interné DEV a TEST prostredie

Brain:IT
Lokalita Brain:IT

DockerHub
Predstavuje verejný Docker Registry DockerHub

Deployment configuration
Reprezentácia Kubernetes Deployment artifaktu.

Docker Image
Reprezentácia Docker Image artifaktu.

GitLab
Predstavuje inštanciu GitLab.

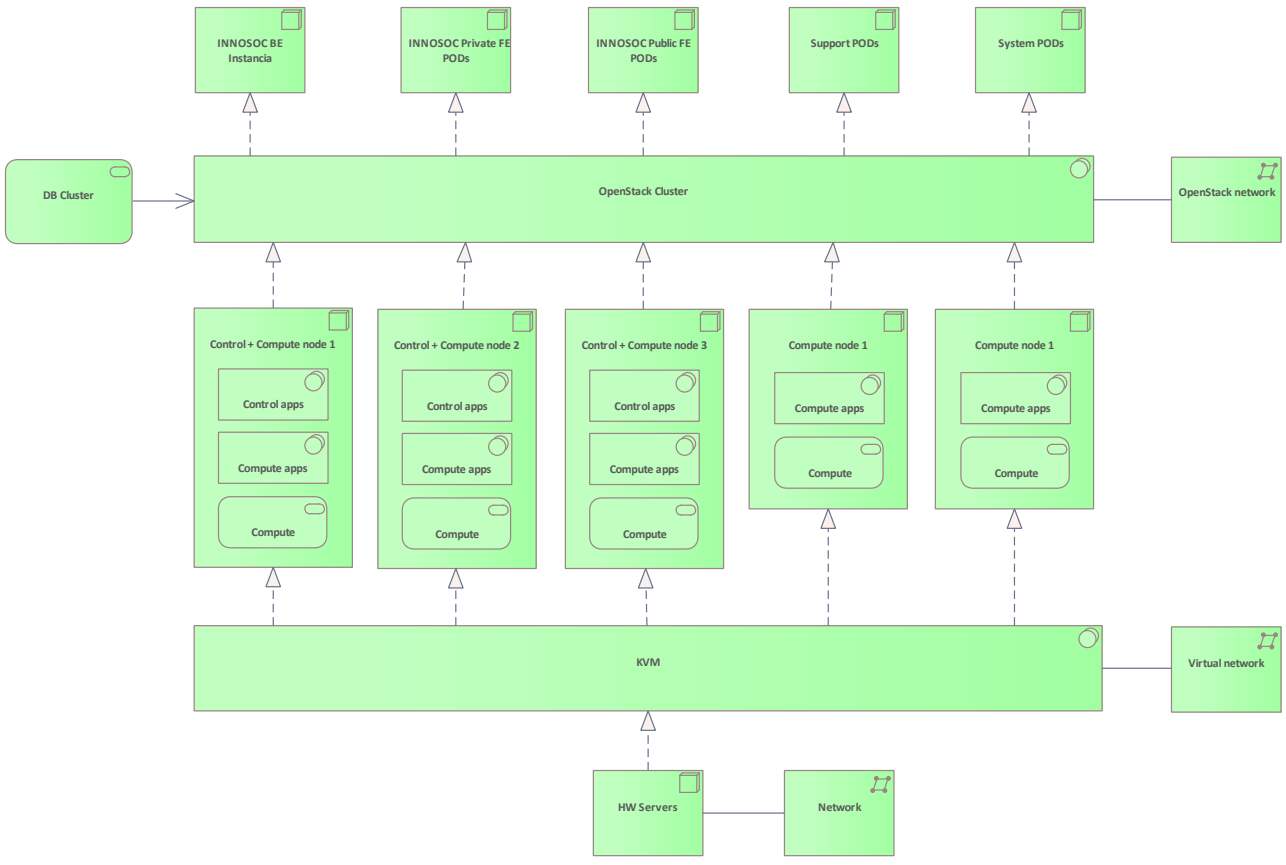
GitLab Worker
Predstavuje insštanciu GitLab Worker

Kubernetes Cluster
Predstavuje Kubernetes Cluster

GitLab CI/CD Pipelines
GitLab CI/CD Pipelines je séria úloh zabezpečujúca kompiláciu, testy, konfiguráciu, nasadenie a iné v rámci GitLabu.

Pod
Predstavuje inštanciu Podu, v rámci ktorej je spustený nový Docker Image v podobe Docker Containera

7.5 Technology Viewpoint OpenStack



Obrázok 32 : Technology Viewpoint OpenStack Cluster

Popis používaných prvkov:

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

Compute node 1
Predstavuje Compute node OpenStack Clustra

Compute node 1
Predstavuje Compute node OpenStack Clustra

Control + Compute node 1
Predstavuje Control a Compute node 1 OpenStack Clustra

Control + Compute node 2
Predstavuje Control a Compute node 2 OpenStack Clustra

Control + Compute node 3
Predstavuje Control a Compute node 3 OpenStack Clustra

HW Servers
Predstavuje HW serverovú infraštruktúru

KVM
Predstavuje KVM Hypervisor 1. typu.

Network
Predstavuje sieť/subsieť HW infraštruktúry

OpenStack Cluster
Predstavuje OpenStack Cluster

OpenStack network
Predstavuje sieť/subsieť OpenStack Clustra, konkrétne:
Corporate network
OpenStack Tenant Data Network
OpenStack Internal Admin / API Subnet

Support PODs
Predstavuje PODy podporných služieb

System PODs
Predstavuje PODy systémových služieb

Virtual network
Predstavuje virtuálnu sieť/subsieť Hypervisora

INNOSOC BE Instancia
Predstavuje inštanciu OpenStacku VM alebo kontajner

INNOSOC Private FE PODs
Predstavuje PODy CNM FE Private

INNOSOC Public FE PODs
Predstavuje PODy CNM FE Public

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

Control apps
Predstavuje súbor aplikácií pre Control node potrebných pre správu clustra

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

Control apps
Predstavuje súbor aplikácií pre Control node potrebných pre správu clustra

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

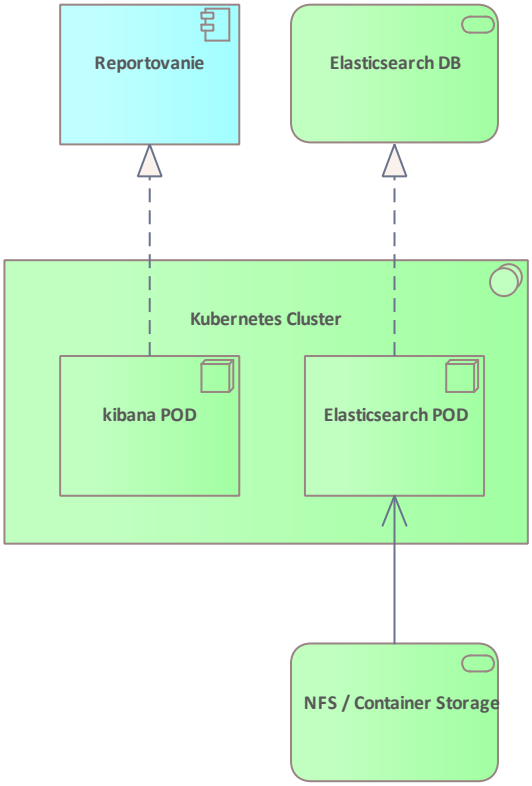
Control apps
Predstavuje súbor aplikácií pre Control node potrebných pre správu clustra

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

7.6 Technology Viewpoint OpenStack External

7.7 Technology Viewpoint Reportovanie



Obrázok 33 : Technology Usage Viewpoint Reportovanie alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom. Alt 1 predstavuje využitie Elasticsearch databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databázy pre Elasticsearch.

Popis používaných prvkov:

Reportovanie
Komponent reportovania v rámci SOCaaS architektúry slúži ako centrálny prostriedok na agregáciu, vizualizáciu a distribúciu bezpečnostných informácií. Jeho úlohou je zabezpečiť pravidelné aj ad-hoc výstupy o stave kybernetickej bezpečnosti pre rôzne cieľové skupiny – od SOC analytikov, cez vedúcich tímov, až po vedenie organizácie alebo klientov. Takýto reportovací systém musí pokrývať:
• Generovanie metriky incidentov, výstrah, SLA a KPIs,
• Prehľady trendov v čase a hodnotenie výkonnosti bezpečnostných opatrení,
• Prispôsobenie obsahu podľa úrovne detailu (technické vs. strategické),
• Automatizáciu a plánovanie distribúcie výstupov,
• Spätnú analýzu a archiváciu historických údajov.

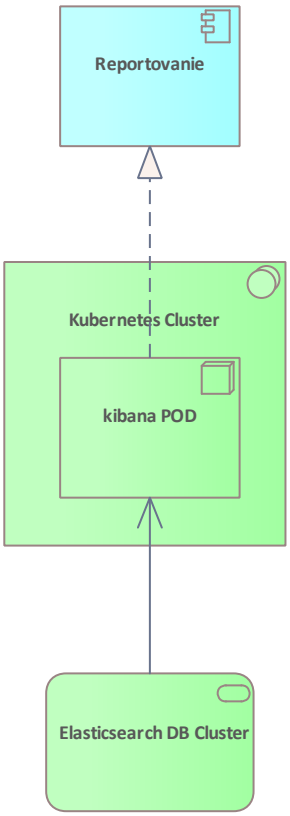
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

Elasticsearch DB
Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD
Predstavuje POD Elasticsearch pre NoSQL databázu.

kibana POD
Predstavuje POD Kibana pre Reportovanie.



Obrázok 34 : Technology Usage Viewpoint Reportovanie alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.
Alt 2 predstavuje využitie Elasticsearch Databázy priamo vo forme centralizovaného DB Clustra.

Popis používaných prvkov:

Reportovanie
Komponent reportovania v rámci SOCaaS architektúry slúži ako centrálny prostriedok na agregáciu, vizualizáciu a distribúciu bezpečnostných informácií. Jeho úlohou je zabezpečiť pravidelné aj ad-hoc výstupy o stave kybernetickej bezpečnosti pre rôzne cieľové skupiny – od SOC analytikov, cez vedúcich tímov, až po vedenie organizácie alebo klientov. Takýto reportovací systém musí pokrývať:
• Generovanie metriky incidentov, výstrah, SLA a KPIs,
• Prehľady trendov v čase a hodnotenie výkonnosti bezpečnostných opatrení,
• Prispôsobenie obsahu podľa úrovne detailu (technické vs. strategické),
• Automatizáciu a plánovanie distribúcie výstupov,

• Spätnú analýzu a archiváciu historických údajov.

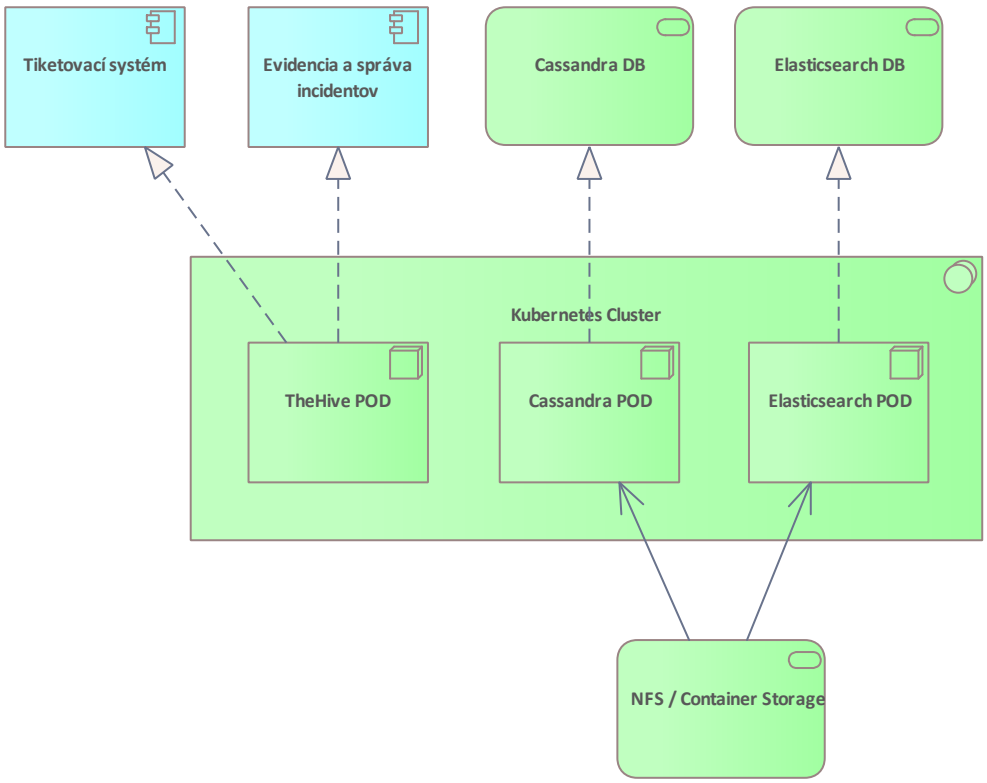
Kubernetes Cluster
Predstavuje Kubernetes Cluster

Elasticsearch DB Cluster
Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

kibana POD
Predstavuje POD Kibana pre Reportovanie.

7.8 Technology Viewpoint Skener zraniteľností

7.9 Technology Viewpoint Tiketovací sytém / Evidencia a správa incidentov



Obrázok 35 : Technology Usage Viewpoint Tiketovací sytém / Evidencia a správa incidentov alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom. Alt 1 predstavuje využitie Elasticsearch databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databáz pre Cassandra a Elasticsearch.

Popis používaných prvkov:

Evidencia a správa incidentov

Evidencia a správa incidentov je jadrovým prvkom každej bezpečnostnej prevádzky (SOC). Tento podkomponent zaisťuje systematickú dokumentáciu, sledovanie a manažovanie bezpečnostných udalostí a incidentov v priebehu ich životného cyklu – od detekcie cez analýzu až po uzavretie. Kvalitný systém evidencie musí umožniť tímom koordinovane spolupracovať, dokumentovať kroky, evidovať súvisiace artefakty (observables) a prepojiť incidenty s relevantnými hrozbami, systémami alebo historickými prípadmi. V ideálnom prípade podporuje aj pokročilé obohacovanie údajov, audit, multitenantnosť a možnosť spätného skúmania incidentov.

Tiketovací systém

Tiketovací systém slúži ako ústredný komunikačný a organizačný kanál pre správu bezpečnostných incidentov počas ich celého životného cyklu. Umožňuje vytváranie, priraďovanie a sledovanie úloh a komunikáciu medzi analytikmi, pričom podporuje audit, SLA monitoring, eskaláciu a notifikácie.

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

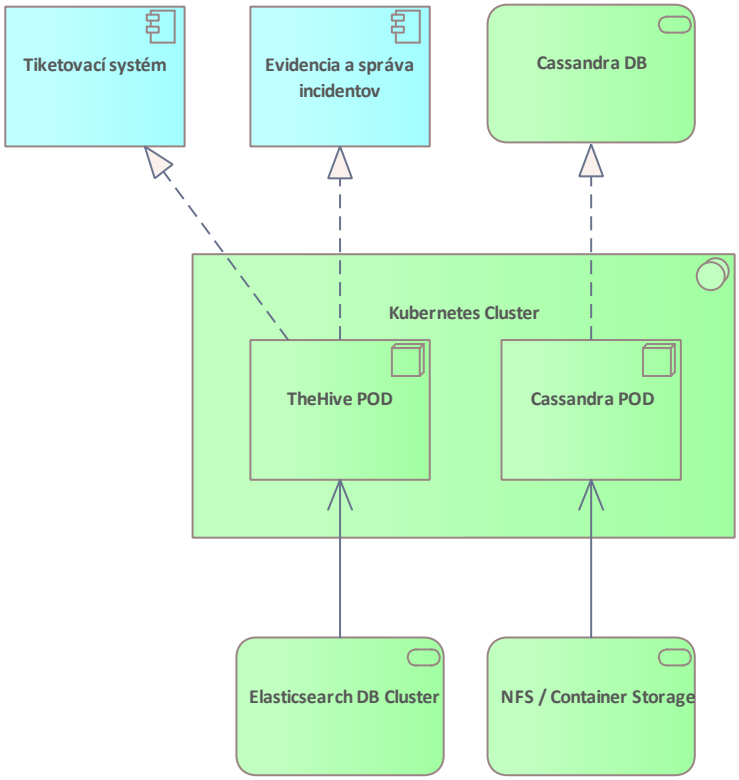
Cassandra DB
Predstavuje technologickú službu NoSQL Cassandra databázy.

Elasticsearch DB
Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Cassandra POD
Predstavuje POD Apache Cassandra pre NoSQL databázu.

Elasticsearch POD
Predstavuje POD Elasticsearch pre NoSQL databázu.

TheHive POD
Predstavuje POD TheHive pre invertarizáckiu aktív.



Obrázok 36 : Technology Usage Viewpoint Tiketovací sytém / Evidencia a správa incidentov alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.
Alt 2 predstavuje využitie Elasticsearch Databázy priamo vo forme centralizovaného DB Clustra. V rámci návrhu sa počíta s kontajnerizovanou verziou NoSQL databázy pre Cassandra.

Popis používaných prvkov:

Evidencia a správa incidentov
Evidencia a správa incidentov je jadrovým prvkom každej bezpečnostnej prevádzky (SOC). Tento podkomponent zaisťuje systematickú dokumentáciu, sledovanie a manažovanie bezpečnostných udalostí a incidentov v priebehu ich životného cyklu – od detekcie cez analýzu až po uzavretie. Kvalitný systém evidencie musí umožniť tímom koordinovane spolupracovať, dokumentovať kroky, evidovať súvisiace artefakty (observables) a prepojiť incidenty s relevantnými hrozbami, systémami alebo historickými prípadmi. V ideálnom prípade podporuje aj pokročilé obohacovanie údajov, audit, multitenantnosť a možnosť spätného skúmania incidentov.

Tiketovací systém
Tiketovací systém slúži ako ústredný komunikačný a organizačný kanál pre správu bezpečnostných incidentov počas ich celého životného cyklu. Umožňuje vytváranie, priraďovanie a sledovanie úloh a komunikáciu medzi analytikmi, pričom podporuje audit, SLA monitoring, eskaláciu a notifikácie.

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

Cassandra DB
Predstavuje technologickú službu NoSQL Cassandra databázy.

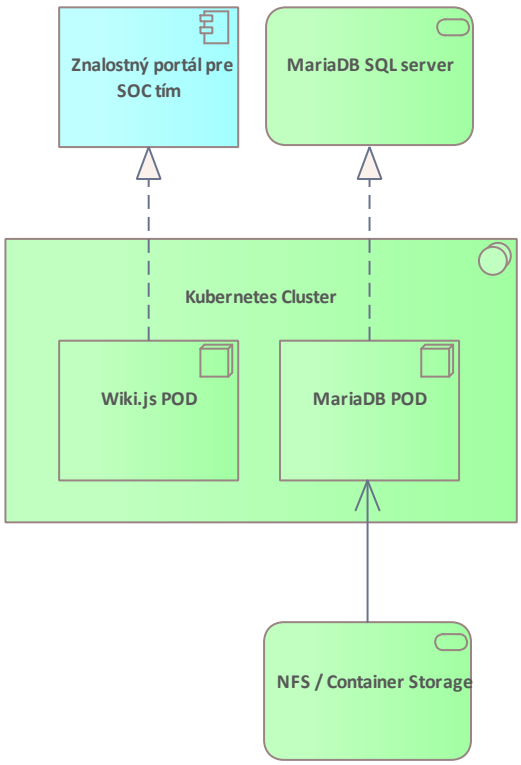
Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

Cassandra POD
Predstavuje POD Apache Cassandra pre NoSQL databázu.

TheHive POD
Predstavuje POD TheHive pre invertarizáckiu aktív.

7.10 Technology Viewpoint Znalostný portál pre SOC tím



Obrázok 37 : Technology Usage Viewpoint Znalostný portál pre SOC tím alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom. Alt 1 predstavuje využitie Databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou SQL servera.

Popis používaných prvkov:

Znalostný portál pre SOC tím
Znalostný portál pre SOC tím je dôležitým stavebným kameňom každého moderného bezpečnostného operačného centra. Slúži ako centrálny repozitár know-how, playbookov, postupov, odporúčaní, analytických návodov a často aj historických lekcií (lessons learned) z incidentov. Znalostný portál:
• Zvyšuje efektivitu a konzistentnosť reakcie na incidenty,
• Umožňuje rýchle zaškolenie nových členov tímu,
• Podporuje štandardizáciu procesov a metodík,

• Umožňuje tímu uchovávať a zdieľať overené postupy a vlastné analytické skúsenosti,
• Posilňuje schopnosť kolektívne sa učiť z incidentov a budovať interné "threat intel" vedomosti.

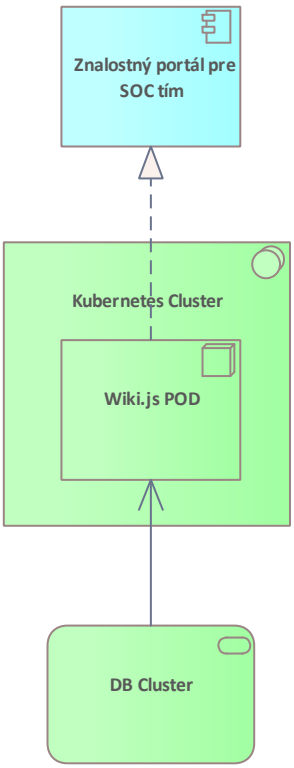
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

MariaDB SQL server
Predstavuje technologickú službu relačnej MariaDB SLQ databázy.

MariaDB POD
Predstavuje POD MariaDB pre relačnú SQL DB.

Wiki.js POD
Predstavuje POD Wiki.js pre Znalostný portál pre SOC tím.



Obrázok 38 : Technology Usage Viewpoint Znalostný portál pre SOC tím alt 2

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.
Alt 2 predstavuje využitie Databázy priamo vo forme centralizovaného DB Clustra.

Popis používaných prvkov:

Znalostný portál pre SOC tím

Znalostný portál pre SOC tím je dôležitým stavebným kameňom každého moderného bezpečnostného operačného centra. Slúži ako centrálny repozitár know-how, playbookov, postupov, odporúčaní, analytických návodov a často aj historických lekcií (lessons learned) z incidentov. Znalostný portál:
• Zvyšuje efektivitu a konzistentnosť reakcie na incidenty,
• Umožňuje rýchle zaškolenie nových členov tímu,
• Podporuje štandardizáciu procesov a metodík,
• Umožňuje tímu uchovávať a zdieľať overené postupy a vlastné analytické skúsenosti,
• Posilňuje schopnosť kolektívne sa učiť z incidentov a budovať interné "threat intel" vedomosti.

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

Kubernetes Cluster
Predstavuje Kubernetes Cluster

Wiki.js POD
Predstavuje POD Wiki.js pre Znalostný portál pre SOC tím.

7.11 Technologické komponenty riešenia a ich vzťah k aplikačným komponentom

7.11.1 Správa prístupov, účtov a kľúčov prevádzkových prostredí

7.11.2 Kontajnerizácia a orchestrácia cloudových služieb

7.11.3 Špecifikácia využitia služieb vládneho cloudu

7.12 Popis testovacieho prostredia

Uvedený v kapitole 7.1.

7.13 Popis produkčného prostredia

Uvedený v kapitole 7.1.

8 Požiadavky na úrovne služieb (SLA) a výkonnosť

9 Softvérové licencie a zdrojové kódy

Zoznam SW licencií, ktoré sa použijú pri vývoji:

P. č.	Názov použitého SW	Typ použitého SW	Licencia k SW
....			

10 Zabezpečenie dostupnost, zálohovanie a obnova riešenia

Popis spôsobu riešenia ZABEZPEČENIE DOSTUPNOSTI Zálohovanie a obnova riešeniaje presne spísaný ariešený vplatnej**Zmluve o poskytovaní služieb podpory a údržby informačného systému**, ktorá naberá účinnosť dňom akceptovania Záverečného akceptačného protokolu dodávaného diela.

10.1 Zabezpečenie dostupnosti

Základným pilierom dostupnosti kritických systémov v cloudovom prostredí je clustering systémov, zabezpečujúci automatický prechod aplikácie na náhradný uzol (virtuálny server) v prípade výpadku primárneho uzla a vykonanie všetkých operácií s tým spojených. Kritické aplikácie alebo sieťové služby realizované vo vysokej dostupnosti (High Availability – HA) systémov pomocou softvérového clustera..., ktorý predstavuje štandard v problematike vysokej dostupnosti.

Spoľahlivosť kritických systémov je realizovaná na dvoch (až štyroch) úrovniach:

1. Vysoká dostupnosť systému použitím softvérového clustrovania. Tým je zabezpečený rýchly a od obsluhy nezávislý nábeh systému po hardvérovej alebo softvérovej havárii, prípadne poruche systému.
2. Cyklické (a automatické) zálohovanie dát (logy systémov, aplikačné dáta, samotné aplikácie...). Týmto ochraňujeme systém proti prípadnej strate cenných dát.
3. Úlohou servisného zásahu je vrátiť systém do pôvodného stavu, opraviť hardvérové alebo sieťové poruchy, ktorých vznikom prestala fungovať časť systému, a tak ho pripraviť na ďalší potenciálny výpadok. V prípade, ak by na výpadky väčšieho charakteru na zabezpečenie fungovania systému nestačila navrhnutá “redundancia” systému, alebo v prípade výpadkov spôsobených zlou obsluhou (chyby administrátorov atď.) je niekedy potrebné sprevádzkovať systémy aj s použitím dátových záloh.
4. Replikácia dát do inej lokality kvôli odolnosti systému (počítačového centra) proti plošným výpadkom, živelným pohromám atď. Túto problematiku však v plnom rozsahu zabezpečuje poskytovateľ cloudového riešenia.

Vytvárané sú zálohy aplikačného prostredia serverov, konfigurácie systému, záznamov o prevádzke aj samotných báz údajov.

Všetky dôležité centrálne komponenty systému a infraštruktúry sú v produkčnej prevádzke nasadené podľa potreby viacnásobne tak, aby zlyhanie žiadneho jedného komponentu neohrozilo zlyhanie alebo nedostupnosť určitých služieb systému.

Všetky interné sieťové rozhrania pracovných staníc sú chránené lokálnym firewallom, majú nastavenú politiku riadenia prístupu so štandardne zablokovanými portami (default deny all) a povolená je komunikácia iba pre určené spojenia podľa komunikačnej matice.

10.2 Zálohovanie

Zálohovať je potrebné PostgreSQL databázu. Nie je potrebné riešiť zálohu súborov.
Spôsob zálohovania a obnova je v kompetencii objednávateľa, odporúčaná frekvencia zálohovania je 1x za 12 hodín s retenčnou politikou jeden týždeň.

10.3 Obnova riešenia

11 Bezpečnosť - riešenie požiadaviek na bezpečnosť

Zásady bezpečného vývoja
Požiadavky stanovené v tomto dokumente musia byť splnené pre všetky komponenty, ktoré sú používané v priebehu vývoja a všetky artefakty, ktoré sa považujú za produkty vývoja.
Systém bude vyvíjaný v súlade s medzinárodne uznávanými odporúčaniami a osvedčenými postupmi v oblasti bezpečného vývoja softvéru. Vývojové aktivity budú reflektovať požiadavky definované v rámci iniciatívy CISA Secure by Design (https://www.cisa.gov/resources-tools/resources/secure-by-design) ako aj metodiky OWASP Developer Guide (https://owasp.org/www-project-developer-guide/release/).

Pod produktami vývoja máme na mysli najmä:
- High-level Design (HLD), Low-level Design (LLD), Entity Relationship Diagram (ERD), procesné diagramy apodobne
- zdrojové kódy softvéru
- spustiteľné programy ktoré sú súčasťou dodávky
- konfigurácie
- databázové schémy
- testovacie sady údajov

Bezpečnostné požiadavky je vhodné rozdeliť do troch častí:
- Požiadavky na vývojové prostredie
- Požiadavky na samotný vyvíjaný produkt – aplikáciu
- Požiadavky na produkčné prostredie, v ktorom je produkt prevádzkovaný.

Cieľom týchto opatrení je znížiť pravdepodobnosť a dopad hrozieb spojených s vývojom a dodávkou softvéru a to predovšetkým:
- zanesenie zraniteľností v dôsledku zlých programátorských techník,
- zanesenie zraniteľností v dôsledku používania nebezpečných a nepodporovaných frameworkov,
- zanesenie nežiadúcej funkcionality do kódu či už v dôsledku nedbalosti alebo úmyselne,
- oneskorenie dodávky z dôvodu výpadku vývojárskych prostredí,
- porušenie zásad ochrany osobných údajov z dôvodu nesprávnej manipulácie s nimi,
- zanesenie zraniteľností z dôvodu nesprávnej konfigurácie prostredí,
- trestnoprávna zodpovednosť v dôsledku porušovania autorských práv,
- únik citlivých údajov, strata citlivých údajov,
- nemožnosť zabezpečiť dôkazný materiál v prípade bezpečnostného incidentu ako vo vývoji tak v prevádzke a podobne.

Počas vývoja projektu je potrebné zamedziť a vyhnúť sa zaneseniu najbežnejších implementačných chýb, zraniteľností arizík na základe dodržiavania bezpečného životného cyklu vývoja, best-practices avhodne zvoleného bezpečnostného štandardu a/alebo metodiky. Pri implementácii navrhovaného riešenia sapočas vývoja softvér verifikuje voči well-known zraniteľnostiam abezpečnostným odporúčaniam, ktoré sú obsahom dodržiavania bezpečného vývoja pre zamedzenie vzniku najčastejších bezpečnostných rizík pre webové aplikácie.

Pod komponentami používanými v priebehu vývoja máme na mysli najmä:
- pracovné stanice používané pri vývoji
- virtualizačné prostredie
- servery používané pri vývoji (vývojové, testovacie)
- sieťové prostredie používané pri vývoji, vrátane domácich sietí
- tlačiarne a ostatné aktívne prvky
- fyzické prostredie v ktorom prebieha vývoj, vrátane domácich kancelárií
- podporné služby používané pri vývoji ako sú komunikačné nástroje (MS Teams, Jira, email...)
- vývojové nástroje (editory, kompilátory)
- vývojové frameworky
- middleware (webservery, proxy servery, aplikačné servery)
- úložiská zdrojových kódov a konfigurácií (github)
- zálohovacie aplikácie/služby/systémy a zálohované dáta

autentizačné mechanizmy (AD, AAD, LDAP, Radius, Kerberos, SAML, cloud access security broker a podobne)

Zabezpečenie vývojového prostredia
Pri vývoji sa dodržujú zásady najlepšej bezpečnostnej praxe vrátane bezpečnej správy, konfigurácie, patchovania a hardeningu pracovných staníc a serverov, antimalvérovej ochrany, segregácie fyzických a logických prostredí, politík pre účty, správy prihlasovacích údajov, bezpečných prihlasovacích postupov, napr. v súlade s ISO/IEC 27001.

Všetky zariadenia používané pri vývoji budú chránené firewallom a to ako na sieťovom perimetri (rozhraní medzi sieťami) tak aj lokálne pomocou host firewallu, ktorý povoľuje len nutné spojenia. V sieťach, v ktorých prebieha vývoj, smú byť zapojené len zariadenia, ktoré sú pre vývoj potrebné.
Koncové stanice, na ktorých prebieha vývoj, nesmú byť prístupné a používané inými osobami. Vprípade počítačov bude zabezpečená avyžadovaná nutnosť mať nastavené automatické uzamykanie obrazovky chránené heslom.
Počítač sa nebude automaticky pripájať k iným wifi sieťam než ku chráneným sieťam používaným pri vývoji. Wifi SSID, v ktorom je pripojený vývojársky počítač, musí mať prístup riadený WPA2 a komplexné heslo, ideálne autentizáciu cez WPA2 Enterprise. V prípade používania fyzickej LAN, je potrebné používať ochranu prístupu.
Všetky zariadenia používané pri vývoji, vrátane OS sieťových a bezpečnostných prvkov (routre, switche, firewally, wifi accesspointy) musia mať nainštalované aktuálne bezpečnostné záplaty a verzia firmvéru musí byť najmenej N-1.

Všetka sieťová komunikácia do internetu a z internetu musí prechádzať zariadením filtrujúcim nebezpečný a škodlivý obsah. Všetka komunikácia z počítačov používaných na vývoj, ktoré sa nachádzajú mimo chránené interné siete (napríklad sú na homeoffice), musí prechádzať cez firemnú VPN bránu kontrolujúcu a filtrujúcu nebezpečný obsah.
Pri vývoji sa bude používať len legálny, podporovaný a aktuálny softvér. Disky všetkých prenosných zariadení musia byť šifrované (notebooky). Je potrebné šifrovať aj disky neprenosných pracovných staníc a serverov, ktoré nie sú umiestnené v dostatočne chránených priestoroch dátových centier a serverovní.

Všetky konfigurácie musia byť chránené proti neautorizovaným zmenám. Všetky zmeny v konfigurácii budú automaticky detegované a reportované.

Na prihlasovanie sa k systémom je povolené používať len osobné účty. Osobné účty používané na bežnú prácu musia byť oddelené od osobných účtov na administráciu. Používanie generických a zdieľaných účtov (root, administrator) je zakázané s výnimkou disaster recovery. Všetky účty musia byť chránené pomocou SSH kľúčov, vo výnimočných prípadoch, ak je to potrebné dostatočne silným heslom alebo frázou s vysokou mierou entropie.
Na všetkých systémoch používaných pre vývoj je povolené inštalovať len minimálnu nutnú množinu softvéru potrebnú pre konkrétnu činnosť.

Všetky testovacie dáta, citlivé dáta, heslá a podobne sa ukladajú na definované miesta.

Manažment koncových používateľov - Samotné práva, či už pre prístup k informáciám, oprávnenia pre prácu s údajmi, ako aj pre prístup k jednotlivým modulom, funkcionalitám budú riadené oprávneniami definovanými v centrálnej správe používateľov a správe identít, tzv. IAM (Identity and Access Management) pomocou oAuth/SAML smožným využitím 2FA na základe čoho sa budú prideľovať jednotlivé používateľské roly.

Zabezpečenie integrity

Validácia všetkých používateľských vstupov a akcií bude vykonávaná na strane servera a pre vhodné operácie aj na strane klienta. Všetky používateľské vstupy musia byť kontrolované na strane servera.
Proces webového servera aj proces backend databázy musí byť konfigurovaný tak, aby bežal pod unikátnym používateľským kontom s limitovanou množinou privilégií.
Webový server bude konfigurovaný tak, aby súbory s webovým obsahom boli procesom prislúchajúcim službe webového servera prístupné iba na čítanie, no nie na zápis (ak si to samotná služba a proces nevyžaduje).

Webový obsah a všetky logy ním vytvárané budú umiestnené na separátnom pevnom disku alebo na inej logickej partícii, ako OS a webový server. Vprípade kontajnerizácie bude spôsob logovania upravený vzmysle danej orchestračnej platformy.
Na zabezpečenie požiadaviek na bezpečnosť spojených s vývojom projektu bude použitý vhodný nástroj poskytujúci priebežnú kontrolu kvality kódu, validáciu bezpečného životného cyklu akontrolu, ktorá odhaľuje chyby, duplikovaný kód a bezpečnostné diery.

Zabezpečenie komunikácie

Všetky komunikačné kanály budú známe a popísané. Jednotlivé komponenty systému budú oddelené podľa vrstiev plniacich špecifickú úlohu.
Základnými vrstvami sú:
· Prístupová vrstva
· Aplikačná vrstva
· Databázová vrstva

Jednotlivé vrstvy budú umiestnené v separátnych, logicky oddelených sieťových segmentoch alebo samostatne spustiteľných blokoch, prípadne pomocou definovaním prístupu na základe prístupových skupín, pričom komunikácia medzi nimi bude umožnená na základe pravidiel firewallu prípadne pravidlami orchestračnej platformy a navyše bude možný monitoring a filtrácia.
Správcovské a monitorovacie rozhrania sieťových prvkov a serverov nie sú prístupné priamo z externej siete, internetu. Správcovské a monitorovacie rozhrania sú prístupné len z vopred špecifikovaných sietí (napr. administrátorská sieť, určená interná sieť).
Webový server bude externe prístupný výlučne prostredníctvom protokolu HTTPS. S ohľadom na best-practices sa k webovému portálu nemá externe pristupovať prostredníctvom HTTP.
Identita webového portálu bude zabezpečená platným, dôveryhodným certifikátom vydaným na doménu, na ktorej je dostupný predmetný portál. Na tieto účely je možné využiť certifikát atechnický certifikát zinternej CA. Webový portál nesmie do externého prostredia používať nedôveryhodné alebo vypršané SSL/TLS certifikáty.
Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti, sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS. Citlivé údaje (zvlášť prihlasovacie údaje) musia byť prenášané výhradne prostredníctvom zašifrovaného kanála.
Webový server bude podporovať TLS 1.2, TLS 1.3 a novšie. Štandardne nebude podporovať staré verzie SSLv2, SSLv3, TLS 1.0 a TLS 1.1, ak nebude vyžadované inak.
Webový server nemá podporovať šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64 bitov. Webový server nesmie podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.
Webová aplikácia bude čo v najväčšej miere zohľadňovať a aplikovať odporúčania na elimináciu well known zraniteľností podľa best practices.
Základná logická topológia riešenia systému je znázornená vrámci fyzickej architektúry.

Riadenie prístupu
Na riadenie prístupu k aplikácií sa využíva IAM, ktorý na základe definovaných oprávnení vcentrálnej správe používateľov na základe oAuth/SAML a prípadne2FA prideľuje používateľské roly.
Riadenie prístupu medzi jednotlivými zónami alebo podsieťami je zabezpečené pomocou firewallov prípadne iným bezpečnostným mechanizmom.

Logovanie systému a zber auditných záznamov
Logovanie a monitorovanie systému bude zabezpečené technológiou dodanou Objednávateľom. Je odporúčanie nastaviť vhodné metriky pre monitorovanie využiteľnosti a kapacity zdrojov pre každé monitorované zariadenie/system.
Monitorovanie a logovanie systému by malo zahŕňať upozornenia, ktoré by mali byť poskytované systémovému administrátorovi v prípadoch ako napríklad: blížiace sa zaplnenie kapacity úložného priestoru, neštandardne vysoká záťaž systému, detegovaná neobvyklá bezpečnostná udalosť.
Logy aauditné záznamy budú obsahovať konkrétne informácie odátume, čase apoužitej časovej zóne, mali by byť prenášané zabezpečeným kanálom agranularita logovania bude zodpovedať požiadavkám danej služby. Uchovávanie logov by malo byť nastavené tak, aby sa predišlo prípadnému zaplneniu logovacieho miesta aneovplyvnilo stabilitu zdrojov.
Logovanie podlieha centrálne definovanej retenčnej politike, ktorá určuje dobu uchovávania jednotlivých typov logovacích záznamov v závislosti od ich charakteru (napr. prevádzkové, bezpečnostné, auditné). Retenčné obdobia budú konfigurovateľné a nastavené v súlade s legislatívnymi požiadavkami a prevádzkovými potrebami Objednávateľa. Odporúčaná retenčná politika dodávateľom pre logovanie je aspoň 1 mesiac a pre auditné logy aspoň rok. Po uplynutí retenčného obdobia budú záznamy automaticky archivované alebo bezpečne zmazané.

Metodika Manažmentu používateľov

Samotné práva, či už pre prístup k informáciám, oprávnenia pre prácu s údajmi, ako aj pre prístup k jednotlivým modulom, funkcionalitám budú riadené oprávneniami definovanými v centrálnej správe používateľov a správe identít, tzv. IAM (Identity and Access Management) pomocou oAuth/SAML sprípadným využitím 2FA na základe čoho sa budú prideľovať jednotlivé používateľské roly. Pomocou IAM bude taktiež zabezpečené definovanie spôsobu akým môžu jednotlivý používatelia narábať so systémom (CRUD operácie).

12 Migrácia dát

V rámci riešenia sa nebude vykonávať migrácia dát.

12.1 Postup vykonania migrácie dát

12.2 Overenie migrácie dát

13 Harmonogram realizácie a nasadenia, závislosti

13.1 Fázy projektu a časový harmonogram - konsolidovaný prehľad

13.2 Závislosti a návrh riešenia

13.3 Požiadavky na fázy Testovanie a Nasadenie do produkcie

Dielo bude realizované ako projekt, ktorý bude riadený v súlade s metodikouPRINCE2. Dodanie riešenia bude prechádzaťzákladnýmiprojektovýmietapamiv zmysle Vyhláškyč.401/2023 oriadení projektov.Výstupy každejetapy budú schvaľované Riadiacim výborom projektu.

14 Otvorené otázky

15 Prílohy

Zoznam príloh DNR:

1. Katalóg požiadaviek amapovanie na ich realizáciu vnavrhovanom riešení
2. Zoznam obrázkov