PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené ako otvorená cloudová služba s prvkami strojového učenia

V13 DNR - Detailný návrh riešenia spolu s prílohami

KPB4 – Architektúra riešenia

typ – dokumentácia

mesiac odovzdania – M22

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1 Použité skratky a pojmy 7

2 Manažérske zhrnutie 11

2.1 Zámer riešenia 11
2.2 Ciele riešenia 11
2.3 Merateľné a výkonnostné ukazovatele (KPI) 11
2.4 Rozsah riešenia 11
2.5 Mimo rozsah projektu 11
2.6 Stručný popis navrhovaného riešenia 11
2.7 Sumarizácia výstupu M-06 navrhovaného riešenia 11
2.7.1 Prehľad koncových služieb – budúci stav 11
2.7.2 Rozsah informačných systémov – budúci stav 12
2.7.3 Prehľad plánovaných integrácií ISVS na nadrezortné ISVS – spoločné moduly podľa zákona č. 305/2013 e-Governmente – budúci stav 12
2.7.4 Prehľad plánovaného využívania iných ISVS (integrácie) – budúci stav 12
2.7.5 Aplikačné služby pre realizáciu koncových služieb – budúci stav 13
2.7.6 Aplikačné služby na integráciu – budúci stav 13

3 Analýza požiadaviek 13

3.1 Postup analýzy požiadaviek 14
3.2 Používateľský prieskum 14
3.3 Motivačná architektúra 14
3.4 Motivation Viewpoints 15
3.5 Katalóg požiadaviek a jeho mapovanie na návrh ich riešenia 15
3.6 Legislatíva, smernice a metodické materiály zohľadnené v riešení 16
3.7 Akceptačné kritéria 16

4 Biznis architektúra 16

4.1 Business Viewpoints 16
4.1.1 Detekcia a korelácia bezpečnostných udalostí (SIEM) - biznis realizácia služby 16
4.1.2 Riadenie automatizácie reakcie (SOAR) – biznis realizácia služby 16
4.1.3 Riadenie reakcie na hrozby (EDR/XDR) - biznis realizácia služby 16
4.1.4 Monitorovanie zraniteľností – biznis realizácia služby 16
4.1.5 Správa spravodajstva o hrozbách (CTI) - biznis realizácia služby 16
4.1.6 Inventarizácia aktív – biznis pohľad 17
4.1.7 Manažovanie kybernetických bezpečnostných incidentov – biznis realizácia služby 17
4.1.8 Riadenie reportovania bezpečnosti - biznis realizácia služby 17

4.1.9 Riadenie znalostného portálu pre SOC tím - biznis realizácia služby 17
4.2 Biznis architektúra 17
4.3 Business Viewpoints 17
4.3.1 Detekcia a korelácia bezpečnostných udalostí (SIEM) - biznis realizácia služby 17
4.3.2 Riadenie automatizácie reakcie (SOAR) – biznis realizácia služby 22
4.3.3 Riadenie reakcie na hrozby (EDR/XDR) - biznis realizácia služby 28
4.3.4 Monitorovanie zraniteľností – biznis realizácia služby 34
4.3.5 Správa spravodajstva o hrozbách (CTI) - biznis realizácia služby 39
4.3.6 Inventarizácia aktív – biznis pohľad 45
4.3.7 Manažovanie kybernetických bezpečnostných incidentov – biznis realizácia služby 49
4.3.8 Riadenie reportovania bezpečnosti - biznis realizácia služby 53
4.3.9 Riadenie znalostného portálu pre SOC tím - biznis realizácia služby 59
4.4 BPMN - Biznis procesný model 64
4.5 Prípady použitia 64
4.5.1 Aktéri 64
4.5.2 Všeobecné prípady použitia 68
4.5.2.1 Prípady použitia diagramy 68
4.5.2.2 UC_00 - Inicializácia a konfigurácia SOCaaS 69
4.5.2.3 UC_01 - Monitorovať bezpečnostné udalosti 76
4.5.2.4 UC_02 - Vizualizovať a reportovať bezpečnostné údaje 82
4.5.2.5 UC_03 - Spravovať detekčné a korelačné pravidlá 90
4.5.2.6 UC_04 – Upozorniť a eskalovať bezpečnostný incident 94
4.5.2.7 UC_05 – Riešiť a uzatvoriť bezpečnostný incident 96
4.5.2.8 UC_06 – Vyhodnotiť incidenty a zlepšiť detekciu aj povedomie 103
4.5.2.9 UC_07 – Automatizovať reakciu na incident 107
4.5.2.10 UC_08 – Proaktívne hľadanie hrozieb 110
4.5.2.11 UC_09 – Spravovať Threat Intelligence a indikátory kompromitácie 113
4.5.2.12 UC_10 – Riadiť súlad, metriky a manažérsky reporting 116
4.5.2.13 UC_11 – Spravovať aktíva a prostredie zákazníka 123
4.5.2.14 UC_12 – Riadiť zraniteľnosti a bezpečnostné nálezy 125
4.5.2.15 .. UC_13 – Navrhnúť a udržiavať bezpečnostnú architektúru SOCaaS prostredia zákazníka 128
4.5.2.16 UC_14 – Pracovať s portálom zákazníka a spolupracovať 133
4.5.2.17 UC_15 – Spravovať prevádzku SOCaaS platformy 143
4.5.2.18 UC_16 – Prispôsobiť reporty, exporty a dokumenty potrebám organizácie 146
4.5.2.19 UC_17 – Spravovať používateľov a roly v SOCaaS platforme 149
4.5.2.20 UC_18 – Spravovať organizácie, tímy a štruktúru prípadov 152

4.5.2.21UC_19 – Riadiť uchovávanie, ochranu a auditovanie dát SOCaaS 155
4.5.2.22 ..... UC_20 – Spravovať znalostnú bázu a knižnicu playbookov 158
4.5.2.23UC_21 – Spravovať a vyhodnocovať modely strojového učenia pre detekciu incidentov 166
4.5.2.24UC_22 – Spravovať a nasadzovať detekčné balíčky a pravidlá 170
4.5.2.25UC_23 – Spravovať a prevádzkovať skenovanie zraniteľností 174
4.5.2.26UC_24 – Orchestrácia integrácií medzi SOCaaS a externými systémami 177
4.5.2.27UC_25 – Spravovať threat intelligence (CTI) a IOC lifecycle 180
4.5.2.28UC_26 – Konfigurovať plánovanie a export reportov 190
4.5.2.29UC_27 – Spravovať bezpečnostný stav a vzťahy aktív 193
4.5.2.30UC_28 – Nasadiť a udržiavať SOCaaS v rôznych prostrediach 196
4.5.2.31UC_29 – Vysvetliť a analyzovať anomálie detegované ML modelmi 199
4.5.2.32UC_30 – Spravovať endpoint detekciu a reakciu (EDR) v rámci SOCaaS 202
4.5.2.33UC_31 – Poskytovať pracovný priestor pre manuálnu analýzu hrozieb (CTI workspace) 211
4.5.2.34UC_32 – Monitorovať skenovanie zraniteľností a synchronizovať stav súvisiacich incidentov 213
4.6 Biznis architektúra 216
4.7 Business Viewpoints 216
4.7.1 Detekcia a korelácia bezpečnostných udalostí (SIEM) - biznis realizácia služby 216
4.7.2 Riadenie automatizácie reakcie (SOAR) – biznis realizácia služby 217
4.7.3 Riadenie reakcie na hrozby (EDR/XDR) - biznis realizácia služby 217
4.7.4 Monitorovanie zraniteľností – biznis realizácia služby 217
4.7.5 Správa spravodajstva o hrozbách (CTI) - biznis realizácia služby 217
4.7.6 Inventarizácia aktív – biznis pohľad 217
4.7.7 Manažovanie kybernetických bezpečnostných incidentov – biznis realizácia služby 217
4.7.8 Riadenie reportovania bezpečnosti - biznis realizácia služby 217
4.7.9 Riadenie znalostného portálu pre SOC tím - biznis realizácia služby 217
4.7.10 Identifikácia vlastníkov dizajnu koncových služieb (UX) 217
4.7.11 Špecifikácia potrieb koncového zákazníka 217
4.7.12 Návrh prototypov používateľského rozhrania 218
4.7.13 Návrh vizuálov obrazoviek 218
5 Dátová architektúra 218
6 Aplikačná architektúra 219
6.1 Aplikačná architektúra 219

6.2 Aplication Viewpoints ... 219
6.3 Návrh riešenia dizajnu aplikačných služieb ... 223
6.3.1 Existujúce aplikačné rozhrania ... 223
6.3.2 Zanikajúce aplikačné rozhrania ... 224
6.3.3 Nové aplikačné rozhrania ... 224
6.4 Integrácie medzi systémami ... 224
6.4.1 Zoznam existujúcich integrácií bez zmeny ... 224
6.4.2 Zoznam a popis navrhovaných integrácií ... 224
6.4.3 Zoznam a popis požadovaných integračných rozhraní ... 224
6.4.4 Návrh poskytovaných aplikačných rozhraní systému (modulu) ... 224

7 Technologická architektúra ... 224
7.1 Návrh technologickej architektúry ... 225
7.1.1 Technology Viewpoint CTI ... 225
7.1.2 Technology Viewpoint EDR/XDR ... 232
7.1.3 Technology Viewpoint INNOSOC Common ... 237
7.1.4 Technology Viewpoint Inventarizacia aktiv ... 239
7.1.5 Technology Viewpoint Kubernetes ... 243
7.1.6 Technology Viewpoint OpenStack ... 266
7.1.7 Technology Viewpoint Reportovanie ... 271
7.1.8 Technology Viewpoint SIEM ... 274
7.1.9 Technology Viewpoint Skener zraniteľností ... 278
7.1.10 Technology Viewpoint SOAR ... 281
7.1.11 Technology Viewpoint Tiketovací sytém / Evidencia a správa incidentov ... 287
7.1.12 Technology Viewpoint Znalostný portál pre SOC tím ... 292
7.2 Technologické komponenty riešenia a ich vzťah k aplikačným komponentom 295
7.2.1 Správa prístupov, účtov a kľúčov prevádzkových prostredí ... 295
7.2.2 Kontajnerizácia a orchestrácia cloudových služieb ... 295
7.2.3 Špecifikácia využitia služieb vládneho cloudu ... 296
7.3 Popis testovacieho prostredia ... 296
7.4 Popis produkčného prostredia ... 296

8 Požiadavky na úrovne služieb (SLA) a výkonnosť ... 296

9 Softvérové licencie a zdrojové kódy ... 296

10 Zabezpečenie dostupnost, zálohovanie a obnova riešenia ... 297
10.1 Zabezpečenie dostupnosti ... 297
10.2 Zálohovanie ... 298
10.3 Obnova riešenia ... 298

11 Bezpečnosť - riešenie požiadaviek na bezpečnosť 298

12 Migrácia dát 303

12.1 Postup vykonania migrácie dát 303

12.2 Overenie migrácie dát 303

13 Harmonogram realizácie a nasadenia, závislosti 303

13.1 Fázy projektu a časový harmonogram - konsolidovaný prehľad 303

13.2 Závislosti a návrh riešenia 304

13.3 Požiadavky na fázy Testovanie a Nasadenie do produkcie 304

14 Otvorené otázky 304

15 Prílohy 304

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

;	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

;	POPIS
	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	aaS	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

3.4 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 Business Viewpoints

4.1.1 Detekcia a korelácia bezpečnostných udalostí (SIEM) - biznis realizácia služby

4.1.2 Riadenie automatizácie reakcie (SOAR) – biznis realizácia služby

4.1.3 Riadenie reakcie na hrozby (EDR/XDR) - biznis realizácia služby

4.1.4 Monitorovanie zraniteľností – biznis realizácia služby

4.1.5 Správa spravodajstva o hrozbách (CTI) - biznis realizácia služby

4.1.6 Inventarizácia aktív – biznis pohľad

4.1.7 Manažovanie kybernetických bezpečnostných incidentov – biznis realizácia služby

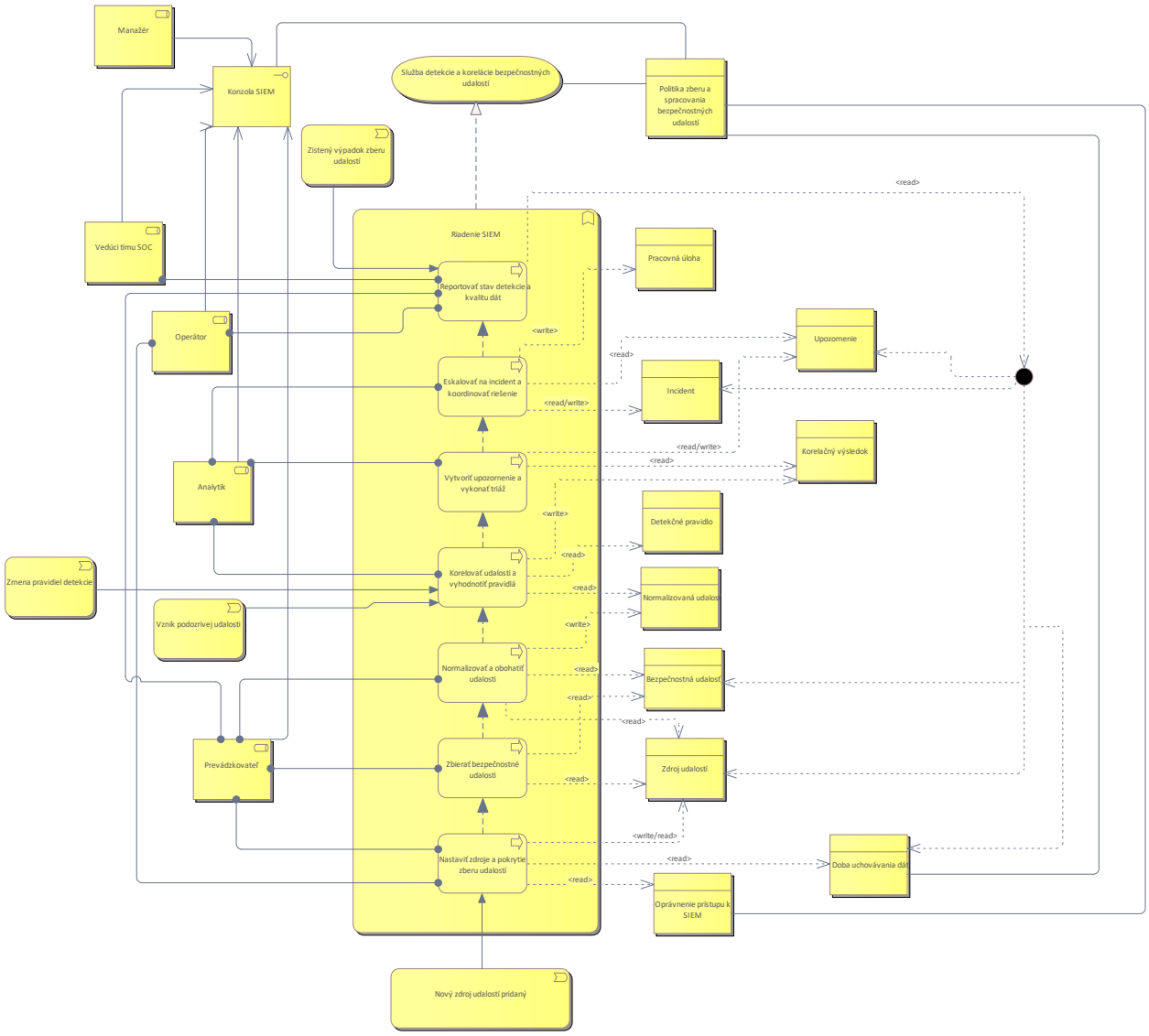
4.1.8 Riadenie reportovania bezpečnosti - biznis realizácia služby

4.1.9 Riadenie znalostného portálu pre SOC tím - biznis realizácia služby

4.2 Biznis architektúra

4.3 Business Viewpoints

4.3.1 Detekcia a korelácia bezpečnostných udalostí (SIEM) - biznis realizácia služby



Obrázok 2 : Detekcia a korelácia bezpečnostných udalostí (SIEM) - biznis realizácia služby

Diagram popisuje riadenie zberu bezpečnostných udalostí zo systémov zákazníka, ich spracovanie, normalizáciu, koreláciu podľa detekčných pravidiel a tvorbu upozornení pre triáž a eskaláciu. Zahŕňa roly, politiku spracovania, konzolu SIEM, biznis udalosti ako spúšťače a prístup procesov k biznis objektom cez číta, zapisuje, aktualizuje.

Popis používaných prvkov:

Nový zdroj udalostí pridaný - BusinessEvent

Udalosť nastane, keď zákazník pridá nový systém alebo službu, ktorá má odovzdávať udalosti do detekcie. Vyžaduje doplnenie pokrytia zberu a kontrolu kvality prijatých dát. Znižuje riziko slepých miest v monitorovaní.

Riadenie SIEM - BusinessFunction

Biznis funkcia zastrešuje zber udalostí, spracovanie a koreláciu dát, tvorbu upozornení, triáž a eskaláciu. Zabezpečuje, že detekcia je konzistentná naprieč zákazníkmi a že zmeny pravidiel sú riadené. Funkcia vytvára podmienky na rýchlu reakciu a spätnú dohľadateľnosť.

Služba detekcie a korelácie bezpečnostných udalostí - BusinessService

Služba zabezpečuje zber bezpečnostných udalostí zo systémov zákazníka, ich spracovanie a vyhodnotenie podľa detekčných pravidiel. Výstupom sú upozornenia pripravené na triáž a prípadnú eskaláciu. Služba je navrhnutá tak, aby bola dohľadateľná, merateľná a oddelená pre každého zákazníka.

Vznik podozrivej udalosti - BusinessEvent

Udalosť vyjadruje zachytenie anomálie alebo vzoru správania, ktorý môže signalizovať útok. Spúšťa koreláciu a následnú triáž, aby sa potvrdil alebo vyvrátil bezpečnostný dopad. Podporuje rýchle zachytenie incidentov.

Zistený výpadok zberu udalostí - BusinessEvent

Udalosť nastane, keď sa preruší prísun udalostí z jedného alebo viacerých zdrojov. Spúšťa overenie dostupnosti zdrojov a nápravné kroky na obnovenie zberu. Minimalizuje obdobie, v ktorom detekcia pracuje s neúplnými dátami.

Zmena pravidiel detekcie - BusinessEvent

Udalosť vyjadruje zmenu logiky pravidiel, prahov alebo podmienok korelácie. Spúšťa kontrolu vplyvu na falošné upozornenia a na pokrytie hrozieb. Umožňuje riadené zmeny a spätné overenie rozhodnutí.

Analytik - BusinessRole

Vykonáva triáž upozornení, overuje kontext a rozhoduje o eskalácii na incident. Používa konzolu na analýzu udalostí, časových línií a súvislostí. Zaznamenáva výsledok posúdenia a pripravuje podklady pre nápravné kroky.

Bezpečnostná udalosť - BusinessObject

Objekt predstavuje jednotlivý záznam aktivity, ktorý môže mať bezpečnostný význam. Obsahuje čas, pôvod, cieľ a údaje potrebné na ďalšie spracovanie. Je základným vstupom pre normalizáciu a koreláciu.

Detekčné pravidlo - BusinessObject

Objekt definuje podmienky, pri ktorých sa z udalostí vytvorí upozornenie alebo korelačný výsledok. Obsahuje logiku vyhodnotenia, prahy a očakávaný výstup pre triáž. Je riadený zmenami, aby sa dalo spätne overiť, prečo vznikol výsledok.

Doba uchovávania dát - BusinessObject

Objekt určuje, ako dlho sa uchovávajú udalosti, korelačné výsledky a upozornenia pre potreby spätnej analýzy a auditu. Zohľadňuje požiadavky na ochranu údajov a prevádzkové možnosti. Podporuje dohľadateľnosť a porovnanie trendov v čase.

Incident - BusinessObject

Objekt sa používa, keď upozornenie vyžaduje koordinované riešenie, evidenciu krokov a uzavretie s výsledkom. Umožňuje priradiť zodpovednosť, stav, dopad a súvisiace pracovné úlohy. Prepojenie na výstupy podporuje audit a spätnú analýzu.

Korelačný výsledok - BusinessObject

Objekt spája viac udalostí do jednej interpretácie s vysvetlením splnených podmienok. Zachytáva, ktoré pravidlá a údaje boli rozhodujúce pre závažnosť. Slúži ako podklad pre triáž a pre spätné overenie.

Manažér - BusinessRole

Používa výstupy na prehľad o rizikách, trendoch a stave detekcie. Vyžaduje zrozumiteľné zhrnutie dopadov a priorít riešenia. Podporuje rozhodovanie o zmenách pokrytia, kapacít a požiadavkách na zákazníka.

Normalizovaná udalosť - BusinessObject

Objekt je udalosť po prevode do jednotnej štruktúry a po doplnení kontextu. Umožňuje porovnanie naprieč zdrojmi a znižuje chyby spôsobené rozdielnymi formátmi. Obsahuje priradenie zákazníka a súvisiacich aktív.

Operátor - BusinessRole

Zabezpečuje prevádzkovú koordináciu a dohľad nad dodržiavaním nastavení a dohôd. Sleduje stav spracovania, dostupnosť výstupov a rieši bežné prevádzkové požiadavky. Podporuje eskaláciu pri zhoršení kvality alebo dostupnosti.

Oprávnenie prístupu k SIEM - BusinessObject

Objekt definuje, kto môže vidieť udalosti, upozornenia a exporty podľa roly a zákazníka. Zabraňuje miešaniu dát medzi zákazníkmi a znižuje riziko úniku informácií. Používa sa pri každom prístupe cez konzolu a je viazaný na politiku.

Politika zberu a spracovania bezpečnostných udalostí - Contract

Politika určuje, ktoré zdroje sa zbierajú, ako sa spracúvajú a aké minimálne požiadavky platia na kvalitu a úplnosť dát. Definuje pravidlá prístupu, označenie zákazníka a pravidlá uchovávania údajov. Zabezpečuje jednotný postup naprieč zákazníkmi a obhájiteľnosť pri audite.

Pracovná úloha - BusinessObject

Objekt predstavuje úlohu na nápravu alebo zlepšenie, ktorá vzniká z incidentu alebo z potreby úprav detekcie. Umožňuje sledovať termín, zodpovednosť, stav a výsledok realizácie. Zabezpečuje, že odporúčania sa premenia na vykonané kroky.

Prevádzkovateľ - BusinessRole

Zodpovedá za technické pokrytie zberu udalostí, dostupnosť spracovania dát a stabilitu prevádzky. Sleduje stav zdrojov, rieši výpadky a nastavuje základné parametre spracovania. Zabezpečuje, že dáta prichádzajú v požadovanej kvalite a v požadovanom čase.

Upozornenie - BusinessObject

Objekt vyjadruje zistenie, ktoré vyžaduje posúdenie analytikom a prípadné ďalšie kroky. Obsahuje závažnosť, dotknuté aktíva a odkazy na súvisiace udalosti. Umožňuje evidovať stav triáže a výsledok posúdenia.

Vedúci tímu SOC - BusinessRole

Riadi kvalitu detekcie a nastavuje smerovanie zlepšovania pravidiel a procesov. Schvaľuje zásadné zmeny, ktoré ovplyvňujú počet upozornení alebo pokrytie hrozieb. Dohliada na konzistentnosť práce tímu a na dohľadateľnosť rozhodnutí.

Zdroj udalostí - BusinessObject

Objekt reprezentuje systém, zariadenie alebo službu, ktorá produkuje bezpečnostné udalosti. Nesie informácie o type, vlastníctve, kritickosti a priradení k zákazníkovi. Umožňuje riadiť pokrytie zberu a identifikovať chýbajúce časti infraštruktúry.

<read> - Junction

Konzola SIEM - BusinessInterface

Rozhranie poskytuje jednotné miesto na prácu s upozorneniami, výsledkami korelácie a stavom zberu udalostí. Umožňuje filtrovanie podľa zákazníka, času, závažnosti a dotknutých aktív. Podporuje spätné overenie tým, že zobrazuje väzby na incidenty a pracovné úlohy.

Eskalovať na incident a koordinovať riešenie - BusinessProcess

Proces zabezpečí vznik incidentu, keď upozornenie vyžaduje koordinované riešenie a

evidenciu krokov. Priraďuje zodpovednosť, stav a vytvára pracovné úlohy pre nápravné opatrenia. Podporuje dohľadateľnosť riešenia a spätné overenie.

Korelovať udalosti a vyhodnotiť pravidlá - BusinessProcess

Proces spája súvisiace udalosti do významových celkov a vyhodnocuje detekčné pravidlá. Vytvára vysvetlenie, prečo bol splnený vzor a ktoré podmienky boli rozhodujúce. Znižuje zahltenie tým, že zoskupuje udalosti do interpretovateľných výsledkov.

Nastaviť zdroje a pokrytie zberu udalostí - BusinessProcess

Proces určuje, ktoré systémy a služby majú odovzdávať udalosti a aké typy udalostí sú potrebné pre detekciu. Zabezpečuje označenie zákazníka, mapovanie aktív a minimálne požiadavky na časové zosúladenie. Výstupom je stabilné pokrytie zberu bez slepých miest.

Normalizovať a obohatiť udalosti - BusinessProcess

Proces prevádza udalosti do jednotnej štruktúry a dopĺňa kontext potrebný na koreláciu. Priraďuje zákazníka, aktívum, kritickosť a ďalšie atribúty, ktoré znižujú chybovosť vyhodnocovania. Zabezpečuje porovnateľnosť udalostí naprieč rôznymi zdrojmi.

Reportovať stav detekcie a kvalitu dát - BusinessProcess

Proces hodnotí úplnosť zberu, kvalitu spracovania a stabilitu počtu upozornení v čase. Identifikuje výpadky zdrojov, nárast šumu a potrebu úprav pravidiel alebo pokrytia. Výstupy sa používajú na plánovanie zlepšení a na kontrolu služby.

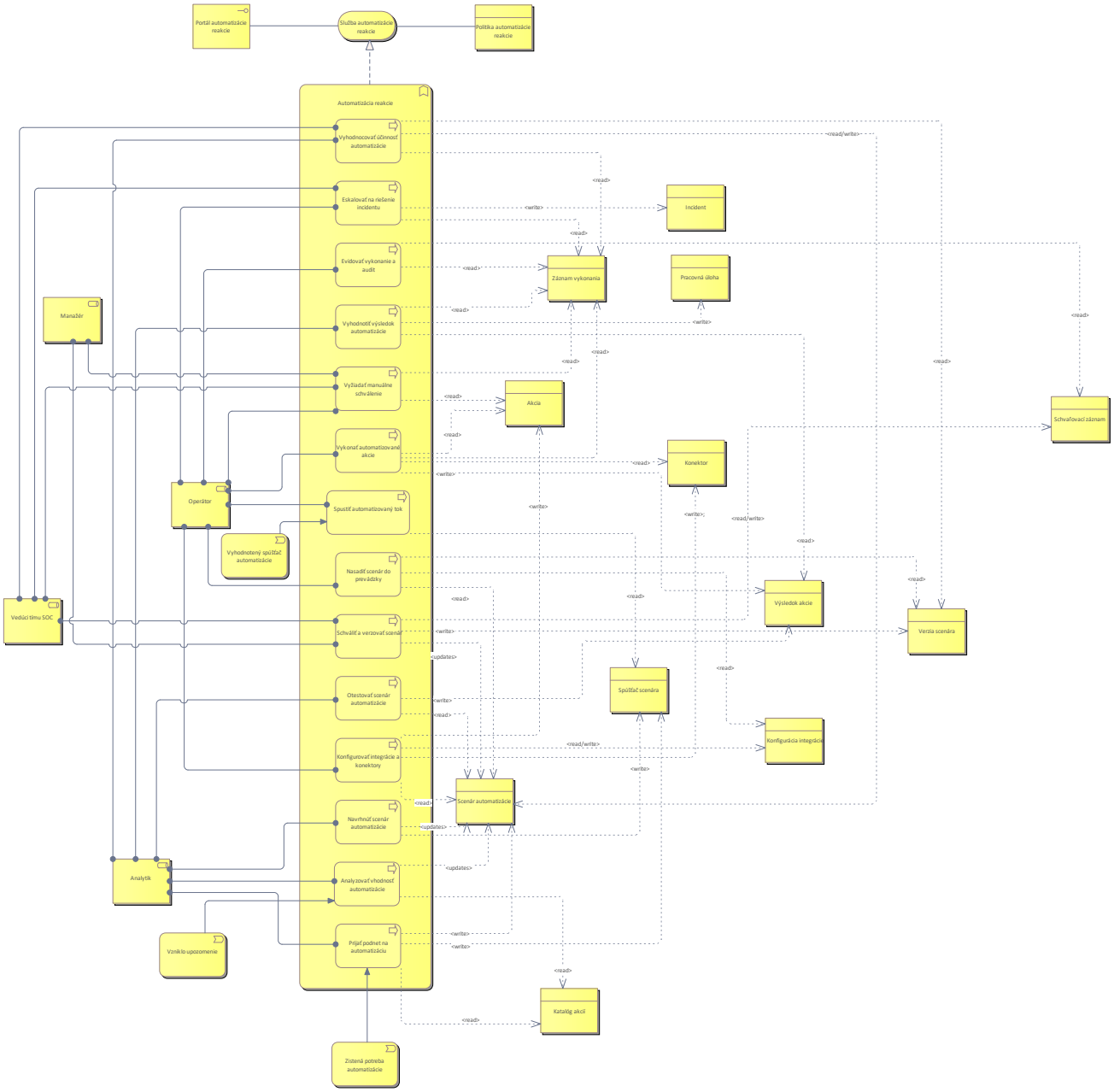
Vytvoriť upozornenie a vykonať triáž - BusinessProcess

Proces vytvára upozornenie z korelačného výsledku a posudzuje jeho relevantnosť. Dopĺňa závažnosť, kontext a prvotné odporúčanie ďalších krokov. Cieľom je rýchlo odlíšiť falošné upozornenia od reálnych hrozieb.

Zbierať bezpečnostné udalosti - BusinessProcess

Proces zabezpečuje prijatie udalostí zo zdrojov a ich doručenie do spracovania. Sleduje dostupnosť, oneskorenie a základné chyby prenosu. Cieľom je, aby udalosti prichádzali úplne, včas a bez poškodenia.

4.3.2 Riadenie automatizácie reakcie (SOAR) – biznis realizácia služby



Obrázok 3 : Riadenie automatizácie reakcie (SOAR) – biznis realizácia služby

Diagram popisuje biznis realizáciu služby automatizácie reakcie na bezpečnostné udalosti a incidenty v SOCaaS. Zachytáva procesy od prijatia podnetu, návrhu scenára a konfigurácie integrácií až po schválenie, verzovanie a nasadenie scenára do prevádzky. V prevádzkovej časti modeluje spúšťanie automatizovaných tokov, vykonávanie akcií, vyhodnotenie výsledku a evidenciu vykonania pre audit. Diagram zahŕňa roly Analytik, Operátor, Vedúci tímu SOC a Manažér spolu s ich zodpovednosťami v životnom cykle automatizácie. Súčasťou sú aj spúšťacie udalosti, biznis objekty scenárov, spúšťačov, integrácií a záznamov vykonania, vrátane prístupov procesov k objektom cez číta, zapisuje a aktualizuje.

Popis používaných prvkov:

Automatizácia reakcie - BusinessFunction

Funkcia zabezpečuje orkestráciu krokov reakcie a vykonanie automatizovaných akcií naprieč integrovanými nástrojmi. Zastrešuje správu scenárov, spúšťačov, integrácií a riadenie vykonania tokov.

Služba automatizácie reakcie - BusinessService

Služba zabezpečuje automatizované vykonanie reakčných krokov pri bezpečnostných udalostiach a incidentoch. Umožňuje spúšťanie scenárov, koordináciu manuálnych potvrdení a evidenciu výsledkov vykonaných akcií.

Vyhodnotený spúšťač automatizácie - BusinessEvent

Udalosť potvrdzuje, že pre konkrétny scenár sú splnené podmienky spustenia podľa definovaného spúšťača. Zabezpečuje, že automatizovaný tok sa spúšťa konzistentne a dohľadateľne. Spúšťa proces spustenia automatizovaného toku.

Vzniklo upozornenie - BusinessEvent

Udalosť vzniká pri vytvorení nového upozornenia v detekčnom alebo monitorovacom procese. Signalizuje, že existuje konkrétny prípad, ktorý je možné posúdiť z hľadiska automatizácie reakcie. Spúšťa proces analýzy vhodnosti automatizácie.

Zistená potreba automatizácie - BusinessEvent

Udalosť vzniká na základe opakujúcej sa manuálnej činnosti, zistenia z prevádzky alebo požiadavky na zrýchlenie reakcie. Vyjadruje potrebu vytvoriť nový scenár alebo upraviť existujúci. Spúšťa proces prijatia podnetu na automatizáciu.

Akcia - BusinessObject

Objekt reprezentuje konkrétny krok scenára vykonávaný v integrovanom nástroji. Obsahuje parametre, podmienky vykonania a očakávaný výsledok.

Analytik - BusinessRole

Rola navrhuje a ladí scenáre automatizácie a definuje spúšťače podľa detekčných požiadaviek. Vyhodnocuje výsledky tokov a rozhoduje o eskalácii pri zlyhaní alebo nejednoznačnom výsledku.

Incident - BusinessObject

Objekt reprezentuje bezpečnostný incident riešený koordinovane v SOC. Slúži ako nadradený záznam pre eskalované prípady a súvisiace úlohy.

Katalóg akcií - BusinessObject

Objekt predstavuje zoznam dostupných typov akcií, ktoré je možné vykonávať automatizovane. Pomáha zabezpečiť jednotné používanie a obmedzenia podľa politiky.

Konektor - BusinessObject

Objekt reprezentuje prepojenie na externý nástroj alebo službu potrebnú pre vykonanie akcií. Eviduje typ konektora, stav a použité prístupové údaje.

Konfigurácia integrácie - BusinessObject

Objekt obsahuje nastavenia, mapovania a parametre pre konkrétnu integráciu. Umožňuje riadenie zmien a kontrolu kompatibility pri aktualizáciách.

Manažér - BusinessRole

Rola stanovuje priority a limity automatizácie pri významnom dopade na biznis a prevádzku zákazníka. Schvaľuje výnimky a rozhoduje o eskalácii pri kritických udalostiach.

Operátor - BusinessRole

Rola dohliada na prevádzku automatizácie a zabezpečuje správne fungovanie integrácií a tokov. Vykonáva zásahy pri zlyhaní automatizácie a potvrdzuje kroky, ktoré vyžadujú manuálne schválenie.

Politika automatizácie reakcie - Contract

Politika definuje pravidlá, kedy je možné vykonať automatizovaný zásah a kedy je potrebné manuálne schválenie. Určuje povolené typy akcií, rozsah oprávnení a požiadavky na auditnú evidenciu.

Pracovná úloha - BusinessObject

Objekt predstavuje priradenú úlohu pre človeka vtedy, keď automatizácia vyžaduje manuálnu činnosť. Umožňuje sledovať stav, zodpovednosť a termíny.

Scenár automatizácie - BusinessObject

Objekt reprezentuje definíciu automatizovaného toku vrátane krokov, podmienok a väzieb na integrácie. Obsahuje aj informácie o schválení a stave nasadenia.

Schvaľovací záznam - BusinessObject

Objekt eviduje manuálne schválenia a odmietnutia krokov, ktoré to vyžadujú. Obsahuje kto schválil, kedy a za akých podmienok.

Spúšťač scenára - BusinessObject

Objekt definuje podmienky, za ktorých sa scenár spustí automaticky alebo manuálne. Obsahuje väzby na zdroj udalosti a prahové hodnoty.

Vedúci tímu SOC - BusinessRole

Rola schvaľuje scenáre s vyšším dopadom a nastavuje pravidlá používania automatizácie v praxi. Zodpovedá za to, aby automatizované zásahy boli v súlade s politikou a prevádzkovými obmedzeniami.

Verzia scenára - BusinessObject

Objekt zachytáva konkrétnu schválenú verziu scenára a jej parametre. Umožňuje spätnú dohľadateľnosť zmien a riadené nasadenie do prevádzky.

Výsledok akcie - BusinessObject

Objekt obsahuje výsledok vykonania konkrétnej akcie vrátane návratového stavu a chybových hlásení. Umožňuje rozhodovanie o pokračovaní toku alebo eskalácii.

Záznam vykonania - BusinessObject

Objekt zachytáva priebeh spustenia scenára vrátane času, vstupných údajov a stavu. Slúži na audit a vyhodnocovanie úspešnosti automatizácie.

Portál automatizácie reakcie - BusinessInterface

Rozhranie poskytuje prístup k správe scenárov, spúšťačov a integrácií. Umožňuje spúšťať a sledovať automatizované toky a zobrazuje záznamy o vykonaní a výsledkoch.

Analyzovať vhodnosť automatizácie - BusinessProcess

Proces posudzuje, či je daný prípad vhodný na automatizáciu a aký je rizikový dopad. Výsledkom je rozhodnutie pokračovať návrhom scenára alebo podnet zamietnuť.

Eskalovať na riešenie incidentu - BusinessProcess

Proces odovzdá prípad do riadenia bezpečnostných incidentov, ak automatizácia nestačí alebo ide o závažný stav. Zabezpečí vytvorenie incidentu a priradenie zodpovedností.

Evidovať vykonanie a audit - BusinessProcess

Proces doplní záznam o vykonaní o potrebné údaje pre audit a dohľadateľnosť. Zabezpečí prepojenie na upozornenie alebo incident a uzavrie tok.

Konfigurovať integrácie a konektory - BusinessProcess

Proces pripravuje prepojenia na nástroje a služby potrebné pre vykonanie akcií. Zahŕňa nastavenie prístupov, parametrov a kontrolu dostupnosti integrácií.

Nasadiť scenár do prevádzky - BusinessProcess

Proces aktivuje schválenú verziu scenára a nastaví jeho spúšťanie v prevádzkovom prostredí. Zabezpečuje, aby scenár používal správne integrácie a oprávnenia.

Navrhnúť scenár automatizácie - BusinessProcess

Proces definuje kroky scenára, spúšťače, podmienky a potrebné integrácie. Zohľadňuje politiku automatizácie a požiadavky na schválenie.

Otestovať scenár automatizácie - BusinessProcess

Proces overuje správnosť krokov scenára na testovacích dátach alebo riadenom prípade. Výsledkom je potvrdenie pripravenosti alebo úpravy scenára.

Prijať podnet na automatizáciu - BusinessProcess

Proces prijíma podnet na vytvorenie alebo úpravu automatizovaného toku z praxe SOC alebo zo zistených problémov. Zabezpečuje základnú evidenciu účelu a očakávaného prínosu.

Schváliť a verzovať scenár - BusinessProcess

Proces zabezpečuje formálne schválenie scenára podľa dopadu a následné vytvorenie verzie. Uchováva stopu schválenia a podmienky nasadenia do prevádzky.

Spustiť automatizovaný tok - BusinessProcess

Proces spúšťa vykonanie scenára na základe spúšťača alebo manuálneho pokynu. Inicializuje záznam vykonania a priradí kontext prípadu.

Vyhodnocovať účinnosť automatizácie - BusinessProcess

Proces sleduje metriky úspešnosti, časové úspory a chybovosť automatizovaných tokov. Výstupom sú odporúčania na úpravy scenárov a politík.

Vyhodnotiť výsledok automatizácie - BusinessProcess

Proces vyhodnotí, či automatizovaný tok dosiahol očakávaný výsledok a či je potrebná ďalšia činnosť. Pri potrebe ďalších krokov vytvorí pracovnú úlohu alebo pripraví eskaláciu.

Vykonať automatizované akcie - BusinessProcess

Proces vykonáva jednotlivé akcie scenára cez integrované nástroje a služby. Pri každom kroku zaznamená výsledok a prípadné chyby.

Vyžiadať manuálne schválenie - BusinessProcess

Proces vyžaduje potvrdenie človekom pre kroky, ktoré majú vyšší dopad alebo to vyžaduje politika. Po

schválení pokračuje v toku alebo ho ukončí.

4.3.3 Riadenie reakcie na hrozby (EDR/XDR) - biznis realizácia služby

Obrázok 4 : Riadenie reakcie na hrozby (EDR/XDR) - biznis realizácia služby

Diagram popisuje poskytovanie a riadenie detekcie a reakcie na hrozby na koncových staniciach a v rozšírených zdrojoch telemetrie zákazníka. Zachytáva procesy nasadenia a správy agentov a zdrojov dát, zber a obohatenie telemetrie, detekciu podozrivého správania, vyhodnocovanie a triáž upozornení, izoláciu alebo obmedzenie kompromitovaných zariadení a odovzdanie incidentu na eskaláciu. Súčasťou sú roly SOC analytik, Operátor a Manažér, pravidlá reakcií a evidencia zásahov a výsledkov.

Popis používaných prvkov:

Incident eskalovaný - BusinessEvent

Udalosť vzniká pri odovzdaní prípadu do procesu riadenia bezpečnostných incidentov. Spúšťa ďalšie kroky vyšetrovania a koordinácie riešenia.

Požiadavka na registráciu koncovej stanice - BusinessEvent

Udalosť vzniká pri onboardingu zákazníka alebo pri pridaní novej koncovej stanice do rozsahu monitorovania. Vyjadruje potrebu zaviesť zariadenie do evidencie a pripraviť ho na zber telemetrie. Spúšťa proces registrácie zdrojov telemetrie.

Reakcia na hrozby - BusinessFunction

Funkcia zabezpečuje koordináciu zberu telemetrie, detekcie, vyhodnotenia a reakcie na hrozby. Zastrešuje procesy práce s upozorneniami a evidenciou zásahov.

Schválený zásah - BusinessEvent

Udalosť vzniká po schválení reakčného opatrenia zodpovednou rolou. Spúšťa vykonanie reakcie a následné overenie výsledku.

Služba reakcie na hrozby - BusinessService

Služba zabezpečuje detekciu a vykonanie reakčných opatrení pri podozrivom správaní na koncových staniciach zákazníka. Podporuje triáž upozornení a odovzdanie potvrdených prípadov na riešenie incidentu.

Vytvorené upozornenie - BusinessEvent

Udalosť signalizuje, že systém vytvoril nové upozornenie na hrozbu s priradenou prioritou. Spúšťa triáž a vyhodnotenie upozornenia.

Zachytená podozrivá aktivita - BusinessEvent

Udalosť vzniká pri identifikovaní podozrivého správania v telemetrii koncovej stanice. Spúšťa proces detekcie a

následnú tvorbu upozornenia.

Zásah vykonaný - BusinessEvent

Udalosť potvrdzuje, že reakčné opatrenie bolo vykonané a je evidované. Spúšťa overenie účinnosti zásahu a uzavretie upozornenia alebo eskaláciu.

Analytik - BusinessRole

Rola vykonáva triáž upozornení a posudzuje závažnosť zistení. Rozhoduje o eskalácii a navrhuje vhodné reakčné opatrenia.

Detekčné pravidlo - BusinessObject

Objekt definuje podmienky, podľa ktorých sa vyhodnocuje podozrivé správanie. Umožňuje evidovať verziu, prioritu a rozsah použitia pravidla.

Detekčný výsledok - BusinessObject

Objekt reprezentuje výsledok vyhodnotenia telemetrie podľa pravidla. Obsahuje zistené indikátory, skóre závažnosti a odkaz na súvisiace dáta.

Incident - BusinessObject

Objekt reprezentuje potvrdený bezpečnostný incident, ktorý vyžaduje koordinované riešenie. Uchováva prepojenia na upozornenia, zásahy a pracovné úlohy.

Koncová stanica - BusinessObject

Objekt reprezentuje zariadenie zákazníka, na ktorom sa zbiera telemetria a vykonávajú zásahy. Obsahuje identifikátory, vlastníka a prevádzkové atribúty potrebné pre reakciu.

Obohatená telemetria - BusinessObject

Objekt predstavuje telemetriu doplnenú o kontext a klasifikáciu. Zvyšuje použiteľnosť dát pre detekciu a znižuje nejednoznačnosť pri triáži.

Operátor - BusinessRole

Rola vykonáva schválené reakčné opatrenia a dohliada na ich realizáciu. Zabezpečuje komunikáciu so zákazníkom pri zásahoch, ktoré ovplyvňujú prevádzku.

Oprávnenia reakcie - BusinessObject

Objekt definuje prístupové práva a rozsah povolených zásahov pre jednotlivé roly. Zabezpečuje, aby sa reakcie vykonávali v súlade s politikou.

Politika reakcie na hrozby - Contract

Politika definuje povolené reakčné opatrenia, úrovne zásahu a zodpovednosti rolí. Určuje podmienky izolácie zariadenia a pravidlá obnovy do prevádzky.

Pracovná úloha - BusinessObject

Objekt predstavuje priradenú úlohu v SOC tíme súvisiacu s reakciou na hrozbu. Umožňuje sledovať stav, zodpovednosť a termíny.

Reakčné opatrenie - BusinessObject

Objekt popisuje navrhnutý zásah a jeho parametre. Umožňuje evidovať schválenie, dôvody a očakávaný dopad na prevádzku.

Stav izolácie zariadenia - BusinessObject

Objekt eviduje aktuálny stav obmedzenia zariadenia a podmienky návratu do prevádzky. Pomáha riadiť riziko a koordinovať obnovu.

Telemetria koncovej stanice - BusinessObject

Objekt obsahuje technické záznamy a udalosti zo zariadenia, ktoré slúžia na detekciu hrozieb. Zahŕňa časové údaje, zdroj a základné kategórie udalostí.

Upozornenie na hrozbu - BusinessObject

Objekt predstavuje záznam o podozrivom správaní pripravený na triáž. Nesie prioritu, stav spracovania a prepojenie na detekčný výsledok.

Vedúci tímu SOC - BusinessRole

Rola schvaľuje zásahy s vyšším dopadom a riadi postup riešenia pri opakovaných alebo rozsiahlych hrozbách. Zodpovedá za dodržiavanie politiky reakcie na hrozby.

Záznam zásahu - BusinessObject

Objekt zachytáva priebeh vykonaných krokov a ich výsledky. Slúži na audit, spätnú dohľadateľnosť a vyhodnocovanie kvality reakcií.

Zberový komponent - BusinessObject

Objekt reprezentuje nasadený komponent, ktorý zbiera a odosiela telemetriu z koncovej stanice. Umožňuje evidovať verziu, stav a konfiguráciu zberu.

Konzola reakcie na hrozby - BusinessInterface

Rozhranie poskytuje jednotné miesto na prehľad telemetrie, upozornení a stavov zariadení.

Umožňuje spúšťať reakčné kroky a evidovať výsledky zásahov.

Detegovať podozrivé správanie - BusinessProcess

Proces vyhodnocuje obohatenú telemetriu podľa detekčných pravidiel a identifikuje podozrivé aktivity. Pri zistení vytvára podklady pre generovanie upozornenia.

Eskalovať na riešenie incidentu - BusinessProcess

Proces odovzdáva potvrdenú hrozbu do riadenia bezpečnostného incidentu. Zabezpečuje vytvorenie incidentu a prepojenie na súvisiace záznamy.

Nasadiť a udržiavať zberové komponenty - BusinessProcess

Proces rieši nasadenie a priebežnú údržbu zberových komponentov na koncových staniciach. Zahŕňa aktualizácie, kontrolu stavu a riešenie chýb zberu.

Navrhnúť reakčné opatrenie - BusinessProcess

Proces vyberá vhodný typ reakcie podľa politiky a kontextu hrozby. Zohľadňuje dopad na prevádzku a potrebu schválenia.

Obohatiť a klasifikovať telemetriu - BusinessProcess

Proces dopĺňa telemetriu o kontext, klasifikáciu a súvisiace informácie. Pripravuje dáta tak, aby boli použiteľné pre detekciu a vyhodnotenie.

Overiť výsledok zásahu - BusinessProcess

Proces overuje, či zásah odstránil alebo obmedzil hrozbu a či sa zariadenie správa očakávane. Pri neúspechu spúšťa doplňujúce kroky alebo eskaláciu.

Schváliť reakčné opatrenie - BusinessProcess

Proces zabezpečuje schválenie reakcie podľa úrovne dopadu a zodpovednosti rolí. Výsledkom je povolenie vykonania alebo požiadavka na úpravu návrhu.

Vyhodnotiť a triážovať upozornenie - BusinessProcess

Proces posudzuje relevantnosť upozornenia, vylučuje falošné poplachy a určuje ďalší postup. Výsledkom je potvrdenie hrozby, uzavretie upozornenia alebo eskalácia.

Vykonať reakčné opatrenie - BusinessProcess

Proces vykonáva zvolený zásah na koncovej stanici alebo v súvisiacich systémoch. Zahŕňa izoláciu zariadenia, obmedzenie komunikácie alebo zastavenie škodlivého procesu.

Vytvoriť upozornenie na hrozbu - BusinessProcess

Proces vytvára upozornenie na základe detekčného výsledku a priraďuje mu prioritu. Zabezpečuje, aby upozornenie obsahovalo potrebné údaje pre triáž.

Zaregistrovať zdroje telemetrie - BusinessProcess

Proces zabezpečuje evidenciu koncových staníc a pripojených zdrojov, z ktorých sa zbiera telemetria. Nastavuje základné parametre zberu a overuje dostupnosť dát.

Zbierať telemetriu z koncových staníc - BusinessProcess

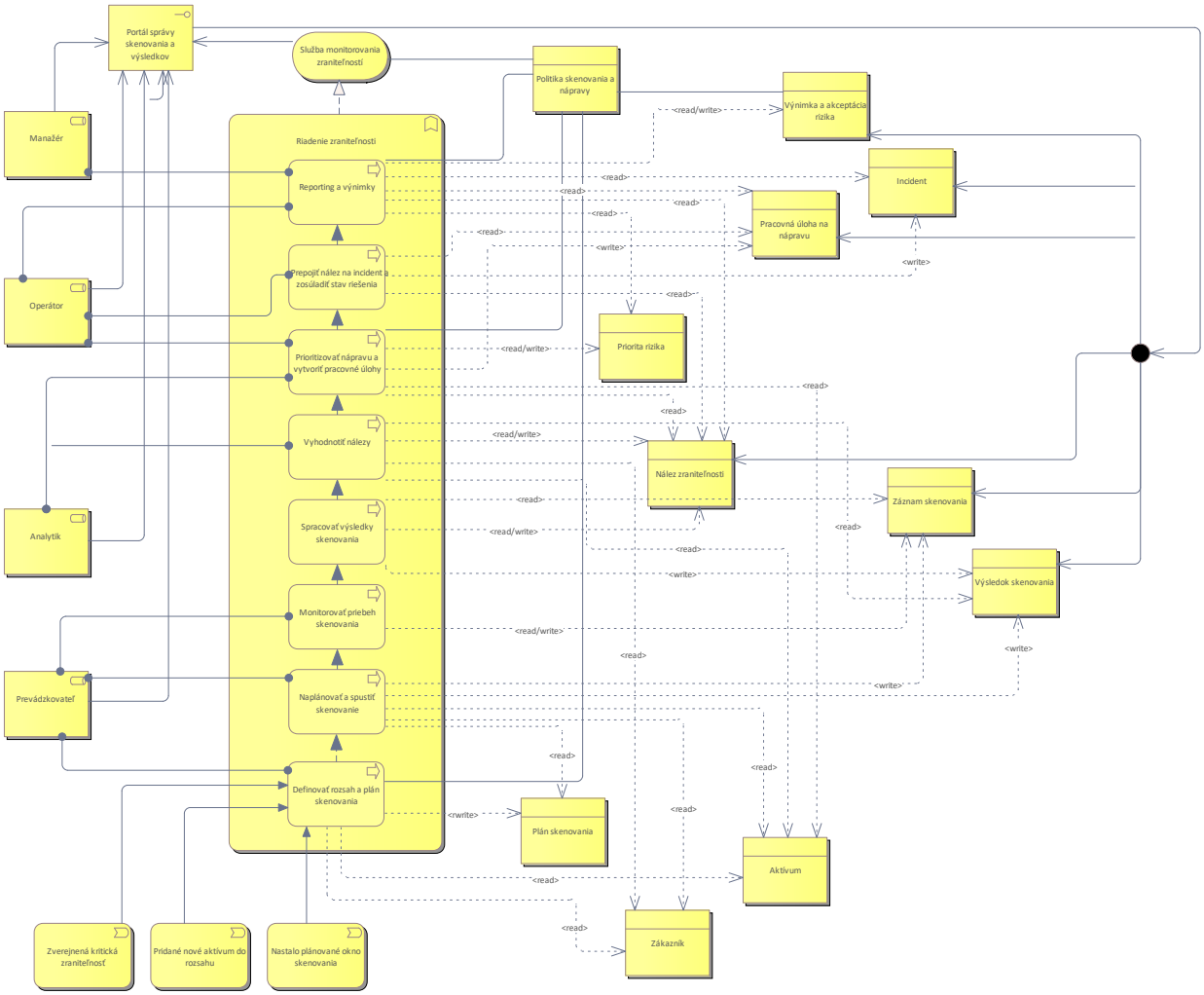
Proces zhromažďuje udalosti a technické záznamy z koncových staníc podľa nastavených pravidiel. Zabezpečuje ich doručenie do konzoly a základnú kontrolu kvality.

Zdokumentovať zásah a uzavrieť upozornenie - BusinessProcess

Proces vytvára záznam o vykonaných krokoch, výsledkoch a odporúčaniach. Upozornenie uzatvára alebo ho viaže na incident, ak pokračuje vyšetrovanie.

4.3.4 Monitorovanie zraniteľností – biznis realizácia služby

Zabezpečuje plánovanie a vykonávanie skenov, validáciu nálezov, hodnotenie rizika, priorizáciu nápravy, ticketovanie a reporting naprieč tenantmi.



Obrázok 5 : Monitorovanie zraniteľností – biznis realizácia služby

Diagram zobrazuje biznis službu monitorovania zraniteľností v prostredí SOCaaS a jej realizáciu prostredníctvom procesov, rolí a spracúvaných informácií. Tok pokrýva definovanie rozsahu a plánu skenovania, spustenie a monitorovanie priebehu, spracovanie a vyhodnotenie výsledkov, priorizáciu nápravy, prepojenie nálezov na incidenty a uzatváranie cyklu cez reporting a výnimky. Model zvýrazňuje viac zákazníkov a oddelenie údajov podľa zákazníka, dohľadateľnosť cez záznam skenovania a prepojenie na pracovné úlohy a incidenty. Súčasťou je aj portál ako biznis rozhranie služby a politika skenovania a nápravy ako zmluvný rámec, pričom udalosti spúšťajú kľúčové procesy podľa plánu, zmien v rozsahu alebo vzniku kritických zistení.

Popis používaných prvkov:

Nastalo plánované okno skenovania - BusinessEvent

Spúšťa plánované spustenie skenovania.

Pridané nové aktívum do rozsahu - BusinessEvent

Spúšťa úpravu rozsahu a často aj mimoriadne spustenie skenovania.

Riadenie zraniteľnosti - BusinessFunction

Zastrešuje schopnosť SOCaaS riadiť zraniteľnosti od definovania rozsahu, cez kontrolu priebehu skenovania, vyhodnotenie a priorizáciu nálezov až po riadenie nápravy, výnimky a uzatvorenie cyklu vrátane zosúladenia stavu súvisiacich incidentov.

Služba monitorovania zraniteľností - BusinessService

Poskytuje plánovanie a vykonávanie skenov, spracovanie výsledkov, vyhodnocovanie nálezov, priorizáciu nápravy, riadenie nápravných úloh, reporting a prepojenie nálezov na incidenty naprieč zákazníkmi.

Zverejnená kritická zraniteľnosť - BusinessEvent

Spúšťa mimoriadnu priorizáciu a často aj mimoriadne skenovanie.

Aktívum - BusinessObject

Cieľ skenovania, ku ktorému sa viažu výsledky a nálezy, umožňuje určiť, aké služby a procesy by boli zasiahnuté pri zneužití zraniteľnosti a podľa toho nastaviť prioritu nápravy.

Analytik - BusinessRole

Validuje nálezy, dopĺňa kontext podľa aktív a väzieb, vyhodnocuje dopad a rozhoduje o postupe.

Incident - BusinessObject

Formálny záznam prípadu, ktorý sa používa vtedy, keď zraniteľnosť vyžaduje incidentové riadenie, koordináciu a komunikáciu podľa pravidiel SOC. Zahŕňa závažnosť, stav, časovú os, zodpovednosti a súvisiace dôkazy a dopady. Je prepojený na nálezy a pracovné úlohy, aby bol priebeh riešenia jednotný a auditovateľný.

Manažér - BusinessRole

Schvaľuje výnimky a akceptáciu rizika, rieši konflikty priorít, sleduje trendy a záväzky voči zákazníkovi.

Nález zraniteľnosti - BusinessObject

Záznam o konkrétnej zraniteľnosti priradenej k aktívu, vrátane identifikátora, závažnosti a stavu spracovania. Nesie kontext potrebný na rozhodnutie, napríklad exponovanosť, dotknutú verziu, dôkaz zistenia a referenciu na výsledok skenu. Umožňuje sledovať životný cyklus nálezu od zistenia po uzatvorenie alebo výnimku.

Operátor - BusinessRole

Zabezpečuje operatívne riadenie nápravy, zakladá a sleduje pracovné úlohy, dohliada na termíny a stav spracovania.

Plán skenovania - BusinessObject

Rozsah, periodicita, okná skenovania, pravidlá spustenia a spracovania.

Politika skenovania a nápravy - Contract

Definuje pravidlá, ktoré musí služba dodržiavať, napríklad periodicitu skenovania, povolené časové okná a požiadavky na pokrytie aktív. Určuje termíny nápravy podľa závažnosti a priority rizika, eskalačné prahy a spôsob sledovania plnenia záväzkov. Zároveň stanovuje postup pre výnimky a akceptáciu rizika vrátane schvaľovania a platnosti, a minimálne požiadavky na reporting a auditovateľnosť.

Pracovná úloha na nápravu - BusinessObject

Pracovná položka, ktorá priraďuje zodpovednosť za opravu, termíny a stav riešenia konkrétneho nálezu alebo skupiny nálezov. Udržiava históriu krokov, komentáre a prepojenie na aktívum, nález a prioritu rizika. Umožňuje operatívne sledovanie plnenia a eskalácie pri omeškaní.

Prevádzkovateľ - BusinessRole

Zodpovedá za nastavenie rozsahu skenovania, pravidiel, okien skenovania, kvality vstupných údajov a prevádzkovej pripravenosti procesu.

Priorita rizika - BusinessObject

Vyjadruje poradie riešenia nálezu na základe kombinácie závažnosti zistenia, kritickosti aktíva a očakávaného dopadu na služby zákazníka. Premieňa technické zistenie na praktickú prioritu pre nápravu a eskalácie. Slúži na nastavenie termínov, SLA a plánovania kapacít.

Výnimka a akceptácia rizika - BusinessObject

Zdokumentované rozhodnutie odložiť alebo nevykonať nápravu, vrátane dôvodu, rozsahu, platnosti a schvaľovateľa. Definuje kompenzačné opatrenia alebo podmienky, za ktorých je riziko dočasne prijateľné. Umožňuje audit a kontrolu, aby výnimky nezostali otvorené bez dohľadu.

Výsledok skenovania - BusinessObject

Konkrétne vykonanie skenu v určitom čase s jednoznačným identifikátorom, stavom a rozsahom. Obsahuje informácie o tom, kto sken spustil, podľa akého plánu prebehol a či skončil úspešne alebo s chybou. Slúži na dohľadateľnosť, audit a vysvetlenie, prečo niektoré aktíva nemali aktuálne výsledky. Súhrn výstupov skenu vrátane metadát, ako je rozsah, čas, použitý profil a pokrytie aktív. Obsahuje zoznam zistení, ich parametre a väzbu na konkrétne aktíva a zákazníka. Je to vstup pre validáciu nálezov, priorizáciu a ďalšie rozhodovanie.

Zákazník - BusinessObject

Určuje vlastníctvo údajov, pravidiel a výstupov, zabezpečuje oddelenie medzi zákazníkmi.

Záznam skenovania - BusinessObject

Obsahuje stav priebehu skenovania a prevádzkové informácie o behu, napríklad začiatok, koniec, priebežný stav a prípadné chyby. Umožňuje sledovať, ktoré časti rozsahu boli naozaj spracované a ktoré zlyhali alebo boli preskočené. Slúži na dohľadateľnosť, riešenie problémov so skenovaním a podporuje auditovateľnosť procesu.

Junction - Junction

Portál správy skenovania a výsledkov - BusinessInterface

Slúži ako jednotné miesto, kde SOC a zákazník vidia stav skenovania, pokrytie aktív a aktuálne výsledky. Umožňuje filtrovanie a vyhľadávanie nálezov, sledovanie priebehu nápravných úloh a prepojenie nálezov na incidenty, aby bola viditeľná súvislosť medzi skenom a riešením. Zabezpečuje konzistentný pohľad naprieč zákazníkmi s oddelením údajov podľa zákazníka a podporuje exporty a reporty pre audit.

Definovať rozsah a plán skenovania - BusinessProcess

Definuje čo sa skenuje, ako často sa skenuje, v akých oknách, aké sú pravidlá vyhodnotenia a zodpovednosti podľa zákazníka.

Monitorovať priebeh skenovania - BusinessProcess

Poskytuje operatívny prehľad stavu skenov, chýb, prebiehajúcich a dokončených behov.

Naplánovať a spustiť skenovanie - BusinessProcess

Realizuje plánované spustenia a umožňuje mimoriadne spustenie pri zmene rozsahu alebo zvýšenej hrozbe.

Prepojiť nález na incident a zosúladiť stav riešenia - BusinessProcess

Zabezpečí viditeľnosť nálezov, ktoré sú riešené ako incidenty, a udržiava jednotný stav súvisiacich incidentov.

Prioritizovať nápravu a vytvoriť pracovné úlohy - BusinessProcess

Určí prioritu riešenia a vytvorí pracovné úlohy na opravu, nastaví termíny a zodpovednosti.

Reporting a výnimky - BusinessProcess

Vytvára reporty, eviduje výnimky, akceptáciu rizika a uzatvára cyklus riadenia zraniteľností.

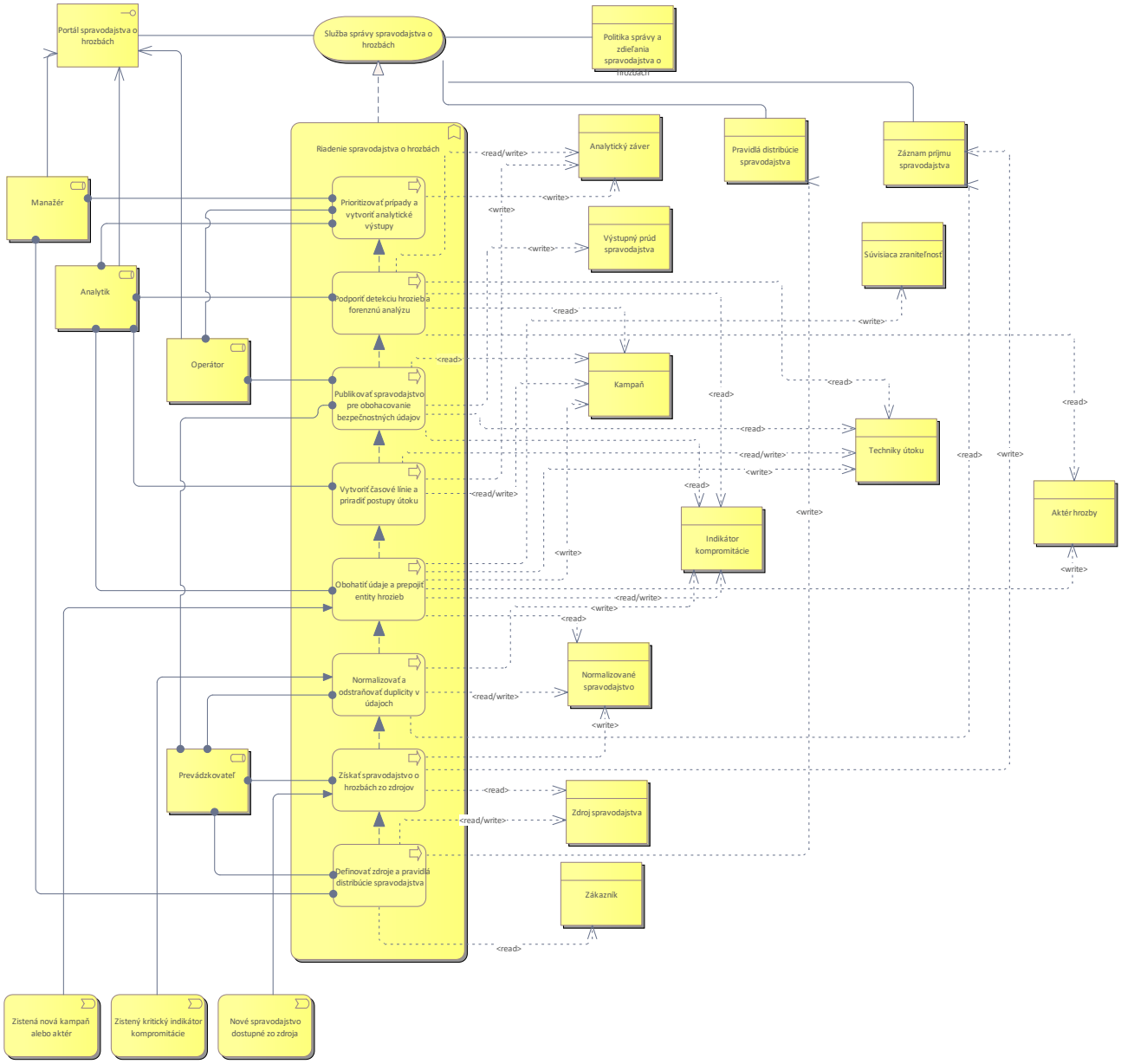
Spracovať výsledky skenovania - BusinessProcess

Zbiera a normalizuje výsledky, zabezpečuje dohľadateľnosť a priradenie výsledkov k správnym aktívam a zákazníkovi.

Vyhodnotiť nálezy - BusinessProcess

Overuje relevantnosť nálezov, odfiltruje falošné nálezy, dopĺňa kritickosť a dopad podľa aktív a ich väzieb.

4.3.5 Správa spravodajstva o hrozbách (CTI) - biznis realizácia služby



Obrázok 6 : Správa spravodajstva o hrozbách (CTI) - biznis realizácia služby

Diagram popisuje, ako sa v prostredí SOCaaS spravodajstvo o hrozbách prijíma zo zdrojov, eviduje cez záznam príjmu a následne sa prevádza na normalizované spravodajstvo. Z neho sa odvodzujú indikátory kompromitácie a dopĺňa sa kontext formou kampane, aktéra hrozby, techník útoku a súvisiacich zraniteľností, aby boli výstupy interpretovateľné a obhájiteľné. Pravidlá distribúcie riadené politikou určujú, aký výstupný prúd spravodajstva sa poskytne zákazníkovi a analytický záver sumarizuje hlavné zistenia a odporúčania pre prax.

Popis používaných prvkov:

Nové spravodajstvo dostupné zo zdroja - BusinessEvent

Udalosť signalizuje dostupnosť nových údajov a spúšťa ich príjem a spracovanie. Môže byť pravidelná podľa harmonogramu alebo mimoriadna pri rýchlej zmene hrozbovej situácie. Je dôležitá pre udržiavanie aktuálnosti výstupov a pre rýchle obohatenie prevádzkových údajov.

Riadenie spravodajstva o hrozbách - BusinessFunction

Funkcia pokrýva celý životný cyklus spravodajstva o hrozbách od výberu zdrojov až po publikovanie použiteľných výstupov. Zabezpečuje kvalitu, aktuálnosť, odstránenie duplicít a vytváranie vzťahov medzi entitami hrozieb pre lepšiu interpretáciu. Funkcia podporuje obohacovanie detekcií, lov hrozieb, forenznú analýzu a rozhodovanie o závažnosti a priorite.

Služba správy spravodajstva o hrozbách - BusinessService

Služba zabezpečuje spracovanie externých a interných informácií o hrozbách tak, aby boli použiteľné pre bezpečnostné operácie. Výstupy sú pripravené na obohacovanie bezpečnostných údajov, podporu vyšetrovania a zmysluplné určovanie priority prípadov. Služba je navrhnutá pre prostredie s viacerými zákazníkmi a udržiava oddelenie údajov a pravidiel podľa zákazníka.

Zistená nová kampaň alebo aktér - BusinessEvent

Udalosť vzniká pri identifikovaní nových súvislostí, ktoré vyžadujú prepojenie entít a doplnenie kontextu. Spúšťa kroky na tvorbu časovej línie a na aktualizáciu vzťahov medzi indikátormi, kampaňami a postupmi útoku. Pomáha zachytiť zmenu charakteru hrozby a zlepšiť interpretáciu zistení.

Zistený kritický indikátor kompromitácie - BusinessEvent

Udalosť signalizuje, že sa objavil indikátor s vysokou dôležitosťou, ktorý si vyžaduje rýchle použitie v prevádzke. Typicky vedie k okamžitému publikovaniu výstupov a k podpore lovu hrozieb a priorizácie prípadov. Zabezpečuje, že kritické informácie sa nestratia v objeme údajov a budú spracované s vyššou naliehavosťou.

Aktér hrozby - BusinessObject

Popisuje útočníka alebo skupinu a poskytuje kontext o motivácii, typických cieľoch a preferovaných postupoch. Umožňuje spojiť jednotlivé zistenia do uceleného obrazu a odlíšiť náhodnú aktivitu od koordinovanej kampane. Podporuje rozhodovanie o priorite a forme reakcie, najmä keď sa objavia opakované vzorce správania.

Analytický záver - BusinessObject

Predstavuje zhrnutie a interpretáciu spravodajstva pre konkrétny účel, napríklad odporúčané kroky alebo hodnotenie rizika. Spája technické údaje s kontextom, aby sa dali priamo použiť pri rozhodovaní a komunikácii so zákazníkom. Zabezpečuje, že výstupy sú konzistentné, obhájiteľné a vysvetliteľné aj pri spätnej kontrole.

Analytik - BusinessRole

Posudzuje relevantnosť spravodajstva pre konkrétne prostredie zákazníka a dopĺňa kontext potrebný na rozhodovanie. Vytvára prepojenia medzi indikátormi, kampaňami, aktérmi a postupmi útoku a pripravuje analytické závery. Používa spravodajstvo pri love hrozieb a pri vyšetrovaní, aby sa zrýchlilo pochopenie priebehu a dopadu udalostí.

Indikátor kompromitácie - BusinessObject

Predstavuje konkrétny identifikátor hrozby, ktorý sa dá vyhľadávať v bezpečnostných údajoch a použiť na obohatenie detekcie. Obsahuje typ indikátora, úroveň dôveryhodnosti, časovú platnosť a súvislosti s ďalšími entitami, aby sa dal správne interpretovať. Pri kritických indikátoroch umožňuje rýchlu operatívnu reakciu a zníženie času do zachytenia hrozby.

Kampaň - BusinessObject

Zoskupuje súvisiace udalosti a aktivity do jedného celku, aby bolo možné sledovať vývoj hrozby v čase. Prepája indikátory, aktérov a použité postupy útoku a tým vytvára kontext pre vyšetrovanie a lov hrozieb. Pomáha identifikovať opakujúce sa scenáre a zhodnotiť, či sa hrozba týka viacerých zákazníkov alebo len konkrétneho prostredia.

Manažér - BusinessRole

Schvaľuje pravidlá zdieľania a priority spracovania spravodajstva podľa potrieb zákazníkov a rizika. Sleduje prínos spravodajstva, požiadavky na reportovanie a dohliada na to, aby procesy podporovali merateľné zlepšenie. Rozhoduje v citlivých situáciách, napríklad pri významných kampaniach, ktoré vyžadujú jasnú komunikáciu dopadu.

Normalizované spravodajstvo - BusinessObject

Predstavuje konsolidované údaje po čistení a zjednotení štruktúry, pripravené na vyhľadávanie a prepojenia. Obsahuje minimálne požadované polia a jednotné typy údajov, aby sa dali spoľahlivo spracúvať ďalšími procesmi. Znižuje šum a vytvára stabilný základ pre obohacovanie a publikovanie výstupov.

Operátor - BusinessRole

Zabezpečuje operatívne používanie výstupov spravodajstva v každodennej prevádzke a dohliada na dodanie výstupov včas. Sleduje stav publikovania, rieši praktické otázky distribúcie a koordinuje reakcie pri výskyte kritických indikátorov. Podporuje prepojenie spravodajstva s riešením prípadov tak, aby boli výstupy dostupné tam, kde sa s nimi pracuje.

Politika správy a zdieľania spravodajstva o hrozbách - Contract

Politika stanovuje pravidlá výberu zdrojov, minimálne požiadavky na kvalitu, periodicitu spracovania a uchovávanie údajov. Definuje obmedzenia zdieľania medzi zákazníkmi, postupy pre citlivé informácie a požiadavky na dohľadateľnosť a audit. Zabezpečuje, že spravodajstvo je spravované konzistentne, predvídateľne a v súlade s dohodnutými očakávaniami.

Pravidlá distribúcie spravodajstva - BusinessObject

Definuje, ktoré výstupy sa poskytujú ktorým zákazníkom a aké obmedzenia platia pre zdieľanie. Obsahuje pravidlá izolácie, povolené formy publikovania a podmienky sprístupnenia citlivých informácií. Je základom pre konzistentnú a auditovateľnú distribúciu spravodajstva v prostredí viacerých zákazníkov.

Prevádzkovateľ - BusinessRole

Zodpovedá za spoľahlivý príjem a spracovanie zdrojov spravodajstva, nastavenie harmonogramov a kontrolu dostupnosti. Rieši prevádzkové zlyhania spracovania, sleduje kapacitu a zabezpečuje, aby spracovanie bežalo podľaальян definovaných pravidiel. Dohliada aj na technickú kvalitu údajov, aby boli výstupy konzistentné a použiteľné naprieč zákazníkmi.

Súvisiaca zraniteľnosť - BusinessObject

Predstavuje zraniteľnosť, ktorú môže hrozba zneužívať alebo na ktorú sa viaže konkrétny indikátor, aktér alebo kampaň. Umožňuje posúdiť naliehavosť nápravy podľa kontextu hrozby, nie iba podľa všeobecnej závažnosti. Podporuje koordináciu medzi spravodajstvom o hrozbách a procesmi riadenia zraniteľností, aby sa opravovali najrizikovejšie miesta.

Techniky útoku - BusinessObject

Reprezentujú popísané spôsoby, ktorými útočník postupuje pri prieniku, pohybe v prostredí a dosiahnutí cieľa. Slúžia na mapovanie zistení na známe postupy, aby sa dali porovnať s predchádzajúcimi prípadmi a lepšie vysvetliť súvislosti. Umožňujú aj plánovať preventívne opatrenia a cielenejšie vyhľadávanie podozrivých prejavov v dátach.

Výstupný prúd spravodajstva - BusinessObject

Obsahuje publikované výstupy určené na obohacovanie bezpečnostných údajov a podporu vyšetrovania v prevádzke. Je cielený podľa zákazníka a pravidiel distribúcie a obsahuje len údaje, ktoré sú povolené a relevantné. Podporuje automatizované používanie spravodajstva a znižuje čas potrebný na manuálne obohacovanie.

Zákazník - BusinessObject

Reprezentuje organizáciu, pre ktorú sa spravodajstvo o hrozbách spracúva a distribuuje. Nesie požiadavky na rozsah, citlivosť a spôsob poskytovania výstupov, aby boli použiteľné pre jej prostredie. Slúži aj na oddelenie údajov a na priradenie pravidiel, ktoré určujú čo sa smie zdieľať a komu.

Záznam príjmu spravodajstva - BusinessObject

Zachytáva fakt, že spravodajstvo bolo prijaté, vrátane času, zdroja, rozsahu a výsledku spracovania. Umožňuje dohľadateľnosť pri spätnom overovaní, prečo sa určitý údaj objavil alebo neobjavil vo výstupoch a kedy bol naposledy aktualizovaný. Je dôležitý aj pre audit a riešenie chýb pri výpadkoch zdrojov alebo pri nekonzistentných dátach.

Zdroj spravodajstva - BusinessObject

Eviduje pôvod spravodajstva, parametre spracovania, periodicitu a očakávanú kvalitu údajov. Obsahuje informácie potrebné na kontrolu dôveryhodnosti a na riadenie toho, čo sa prijíma a ako sa to spracúva. Umožňuje dohľad nad dostupnosťou zdrojov a nad zmenami, ktoré môžu ovplyvniť kvalitu výstupov.

Portál spravodajstva o hrozbách - BusinessInterface

Rozhranie poskytuje prehľad entít hrozieb, ich väzieb a dostupných výstupov pre jednotlivých zákazníkov. Umožňuje vyhľadávanie, filtrovanie a rýchle zobrazenie kontextu indikátorov, kampaní a postupov útoku. Podporuje dohľadateľnosť tým, že zobrazuje pôvod údajov, stav spracovania a históriu zmien výstupov.

Definovať zdroje a pravidlá distribúcie spravodajstva - BusinessProcess

Proces určuje, ktoré zdroje spravodajstva sa používajú, aké majú požiadavky na kvalitu a ako často sa majú spracúvať. Nastavuje pravidlá distribúcie podľa zákazníka a definuje obmedzenia zdieľania tak, aby sa zachovalo oddelenie údajov. Výstupom je jasný rámec, podľa ktorého sa spravodajstvo prijíma, spracúva a poskytuje ďalej.

Normalizovať a odstraňovať duplicity v údajoch - BusinessProcess

Proces prevádza prijaté údaje do jednotnej štruktúry a odstraňuje duplicity a nekvalitné záznamy. Zabezpečuje konzistentné pomenovanie, jednotné typy údajov a minimálnu úroveň povinných polí pre ďalšie použitie. Výstup znižuje šum, zlepšuje vyhľadávanie a pripravuje údaje na prepojenia a koreláciu.

Obohatiť údaje a prepojiť entity hrozieb - BusinessProcess

Proces dopĺňa kontext k indikátorom a vytvára väzby medzi indikátormi, aktérmi, kampaňami, postupmi útoku a súvisiacimi zraniteľnosťami. Cieľom je, aby spravodajstvo nevystupovalo ako izolované položky, ale ako prepojený obraz hrozby s vysvetlením súvislostí. Tento krok výrazne zvyšuje použiteľnosť pri vyšetrovaní, love hrozieb a pri rozhodovaní o priorite.

Podporiť detekciu hrozieb a forenznú analýzu - BusinessProcess

Proces používa spravodajstvo na vytváranie hypotéz, vyhľadávanie súvislostí a vysvetľovanie nálezov v rámci vyšetrovania. Analytikom poskytuje prepojené entity, časové línie a kontext, aby bolo možné rýchlejšie určiť rozsah a dopad. Výstupy z procesu sa používajú aj ako podklady pre rozhodnutia o ďalších krokoch a pre komunikáciu so zákazníkom.

Prioritizovať prípady a vytvoriť analytické výstupy - BusinessProcess

Proces využíva kontext hrozieb na určenie priority prípadov a odporúčaných krokov pre riešenie. Vytvára analytické závery a zhrnutia, ktoré prepájajú technické zistenia s dopadom na služby a riziko zákazníka. Výstupom sú jasné odporúčania a podklady pre reportovanie, rozhodovanie a riadenie reakcie.

Publikovať spravodajstvo pre obohacovanie bezpečnostných údajov - BusinessProcess

Proces pripraví výstupné prúdy spravodajstva a zabezpečí ich dostupnosť podľa pravidiel distribúcie pre jednotlivých zákazníkov. Publikovanie je zamerané na rýchle použitie v detekcii a vyšetrovaní, aby sa známe hrozby dali identifikovať v dátach čo najskôr. Proces zároveň kontroluje, že publikované výstupy spĺňajú kvalitatívne požiadavky a sú auditovateľné.

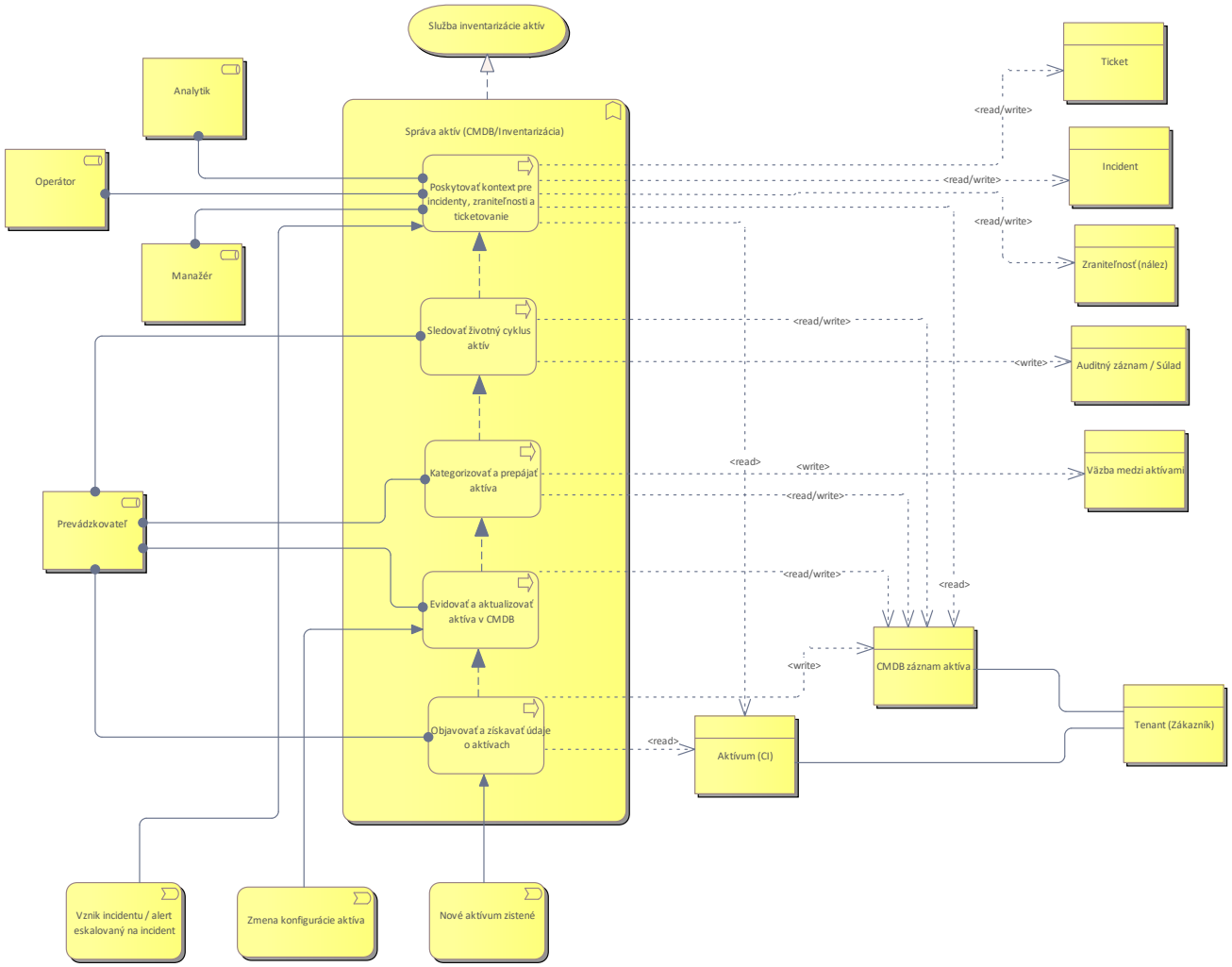
Vytvoriť časové línie a priradiť postupy útoku - BusinessProcess

Proces skladá informácie do časovej línie a zobrazuje vývoj kampaní a aktivít v čase. Priraďuje typické postupy útoku, aby sa dali porovnať aktuálne zistenia s už známymi vzorcami správania. Výstup pomáha pochopiť priebeh udalostí a podporuje formulovanie hypotéz pri love hrozieb.

Získať spravodajstvo o hrozbách zo zdrojov - BusinessProcess

Proces zabezpečuje príjem spravodajstva z externých a interných zdrojov vrátane metadát o pôvode a čase prijatia. Vytvára záznamy o prijatí, aby bola dohľadateľná úplnosť a priebeh spracovania a aby sa dali riešiť výpadky alebo chyby. Cieľom je konzistentný vstup pre ďalšie spracovanie bez ohľadu na rozdielne formáty zdrojov.

4.3.6 Inventarizácia aktív – biznis pohľad



Obrázok 7 : Inventarizácia aktív – biznis pohľad

Biznis pohľad na službu inventarizácie aktív v SOCaaS a jej realizáciu procesmi. Diagram ukazuje, ako sa údaje o aktívach získavajú, evidujú v CMDB, kategorizujú a prepájajú, ako sa sleduje životný cyklus a auditovateľnosť, a ako sa následne tieto informácie používajú na kontextualizáciu incidentov, zraniteľností a ticketovania. Zároveň zachytáva roly zodpovedné za udržiavanie kvality evidencie a využívanie kontextu naprieč tenantmi (zákazníkmi).

Popis používaných prvkov:

Nové aktívum zistené - BusinessEvent

Služba inventarizácie aktív - BusinessService

Centralizovaná evidencia a správa aktív naprieč tenantmi. Podporuje kategorizáciu, väzby, sledovanie bezpečnostného stavu a životného cyklu. Poskytuje kontext pre zraniteľnosti, incidenty, ticketovanie, audit a regulácie.

Správa aktív (CMDB/Inventarizácia) - BusinessFunction

Vznik incidentu / alert eskalovaný na incident - BusinessEvent

Zmena konfigurácie aktíva - BusinessEvent

Aktívum (CI)

- BusinessObject

Zariadenie/systém/aplikácia/virtuálny alebo cloudový zdroj.

Analytik - BusinessRole

Využíva evidenciu aktív na kontextualizáciu incidentov, analýzu dopadu a priorít.

Auditný záznam / Súlad - BusinessObject

Dôkaz o stave a zmenách aktív pre audit a regulácie.

CMDB záznam aktíva

- BusinessObject

Atribúty aktíva, tenant, kritickosť, stav, história zmien.

Incident

- BusinessObject

Bezpečnostný incident kontextualizovaný evidenciou aktív.

Manažér - BusinessRole

Využíva evidenciu aktív pre audit, plánovanie obnovy, compliance a reporting.

Operátor - BusinessRole

Pracuje s ticketmi a SLA; využíva informácie o aktívach na operatívne riešenie a eskalácie.

Prevádzkovateľ - BusinessRole

Zodpovedá za kvalitu a aktuálnosť evidencie aktív, kategorizáciu, správu životného cyklu a zber údajov.

Tenant (Zákazník) - BusinessObject

Ticket

- BusinessObject

Pracovná položka na riešenie; viazaná na aktívum/incident/SLA.

Väzba medzi aktívami

- BusinessObject

Závislosti a prepojenia (topológia, service-to-component, sieťové väzby).

Zraniteľnosť (nález)

- BusinessObject

Nález viazaný na aktívum; vstup pre prioritu a dopad.

Evidovať a aktualizovať aktíva v CMDB - BusinessProcess

Udržiavanie záznamov aktív (identita, typ, vlastník/tenant, kritickosť, stav).

Kategorizovať a prepájať aktíva - BusinessProcess

Tagovanie a tvorba väzieb medzi aktívami (závislosti, topológia, vzťahy).

Objavovať a získavať údaje o aktívach - BusinessProcess

Získavanie údajov o zariadeniach, systémoch, aplikáciách a cloudových zdrojoch; cieľom je úplnosť a aktuálnosť.

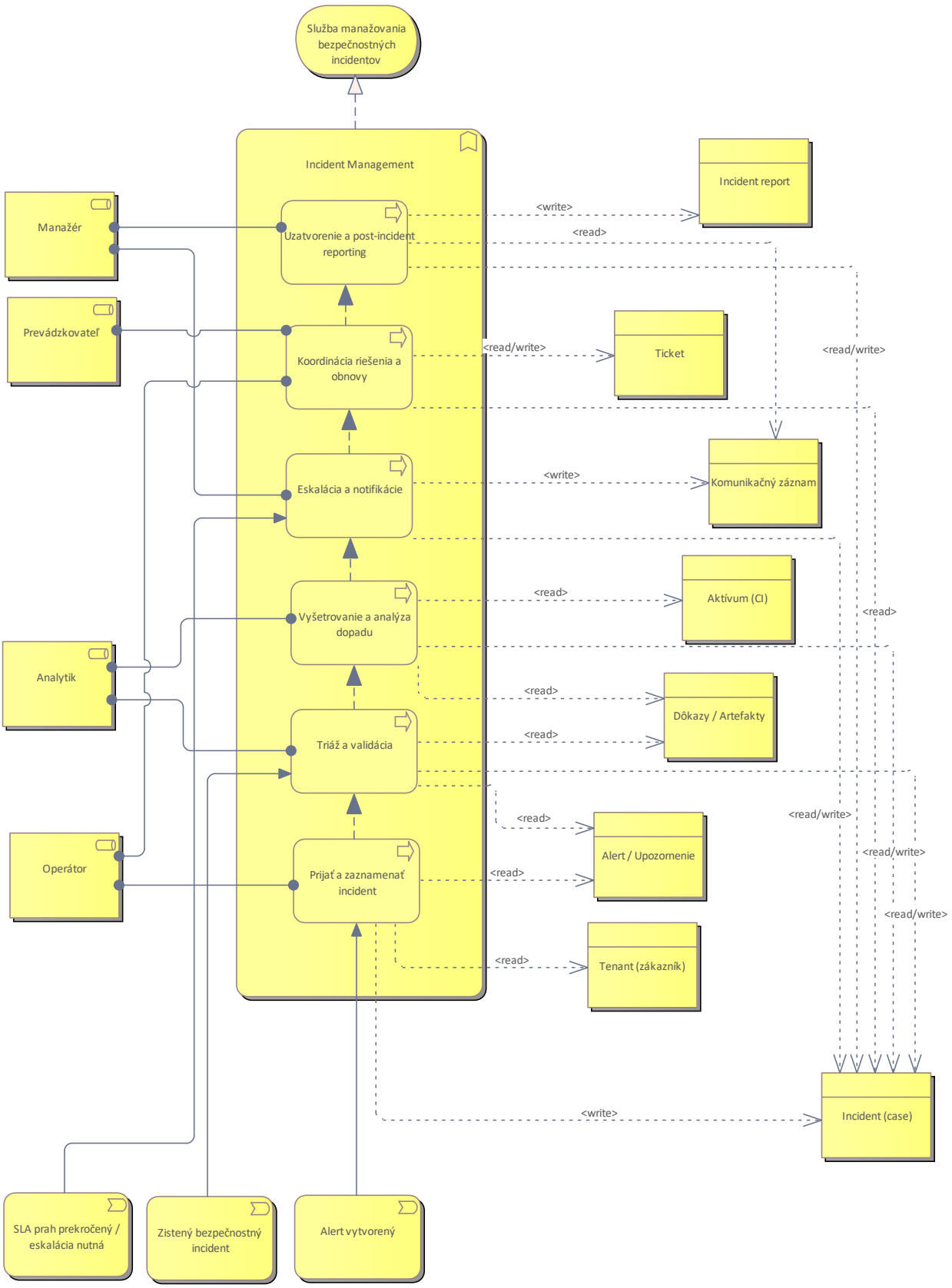
Poskytovať kontext pre incidenty, zraniteľnosti a ticketovanie - BusinessProcess

Kontextualizácia incidentov, analýza dopadu a priorít, podpora efektívneho ticketovania.

Sledovať životný cyklus aktív - BusinessProcess

Stavové prechody, história zmien, plánovanie obnovy, auditovateľnosť.

4.3.7 Manažovanie kybernetických bezpečnostných incidentov – biznis realizácia služby


Služba manažovania bezpečnostných incidentov
Incident Management
Uzatvorenie a post-incident reporting
Koordinácia riešenia a obnovy
Eskalácia a notifikácie
Vyšetrovanie a analýza dopadu
Triáž a validácia
Prijať a zaznamenať incident
Manažér
Prevádzkovateľ
Analytik
Operátor
SLA prah prekročený / eskalácia nutná
Zistený bezpečnostný incident
Alert vytvorený
Incident report
Ticket
Komunikačný záznam
Aktívum (CI)
Dôkazy / Artefakty
Alert / Upozornenie
Tenant (zákazník)
Incident (case)
<write>
<read>
<read/write>

Obrázok 8 : Manažovanie kybernetických bezpečnostných incidentov – biznis realizácia služby

Biznis pohľad na službu manažovania bezpečnostných incidentov v SOCaaS a jej end-to-end tok. Diagram zobrazuje zodpovedné roly a hlavné procesy od prijatia a triáže, cez vyšetrovanie a eskaláciu až po koordináciu riešenia a uzatvorenie s post-incident reportingom. Súčasťou je aj práca s kľúčovými biznis objektmi (incident/case, alert, ticket, dôkazy, komunikačný záznam, report) a ich väzba na tenanta, aby bol proces riadenia incidentov konzistentný a auditovateľný.

Popis používaných prvkov:

Alert vytvorený - BusinessEvent

Incident Management - BusinessFunction

Biznis schopnosť SOC tímu riadiť bezpečnostné incidenty end-to-end vrátane evidencie, eskalácie, koordinácie a post-incident aktivít.

SLA prah prekročený / eskalácia nutná - BusinessEvent

Služba manažovania bezpečnostných incidentov - BusinessService

Zabezpečuje triáž, vyšetrovanie, eskaláciu, koordináciu riešenia, uzatvorenie incidentu a reporting naprieč tenantmi (zákazníkmi).

Zistený bezpečnostný incident - BusinessEvent

Aktívum (CI) - BusinessObject

Dotknuté aktívum alebo služba v prostredí zákazníka.

Alert / Upozornenie - BusinessObject

Vstupný signál, ktorý môže viesť k incidentu (triáž rozhoduje).

Analytik - BusinessRole

Triáž, vyšetrovanie, obohatenie incidentu o kontext, návrh ďalších krokov.

Dôkazy / Artefakty - BusinessObject

Logy, indikátory, výstupy analýzy potrebné pre vyšetrovanie a audit.

Incident (case) - BusinessObject

Hlavný záznam prípadu – stav, závažnosť, časová os, zodpovednosti.

Incident report - BusinessObject

Záverečný report + odporúčania/lessons learned.

Komunikačný záznam - BusinessObject

Záznam notifikácií a komunikácie (kto, kedy, čo bolo oznámené).

Manažér - BusinessRole

Rozhodnutia pri eskalácii, schválenia, komunikácia na úrovni manažmentu, reporting.

Operátor - BusinessRole

Operatívna koordinácia, komunikácia, ticketing, SLA dohľad, vykonanie rutinných akcií.

Prevádzkovateľ - BusinessRole

Podpora platformy a kvality dát; pri incidente pomáha odstrániť technické prekážky (napr. chýbajúce logy, integrácie).

Tenant (zákazník) - BusinessObject

Oddelenie dát a zodpovedností podľa zákazníka.

Ticket - BusinessObject

Pracovná položka na realizáciu nápravných krokov a sledovanie SLA.

Eskalácia a notifikácie - BusinessProcess

Eskalovať podľa SLA a kritickosti; informovať správne kontakty u zákazníka a interné roly.

Koordinácia riešenia a obnovy - BusinessProcess

Riadenie krokov nápravy, sledovanie stavu, komunikácia, priebežné aktualizácie.

Prijať a zaznamenať incident - BusinessProcess

Vznik evidencie prípadu (case) a základných údajov, priradenie tenanta, kategórie, priority.

Triáž a validácia - BusinessProcess

Overiť relevantnosť, odstrániť false positive, určiť závažnosť a ďalší postup.

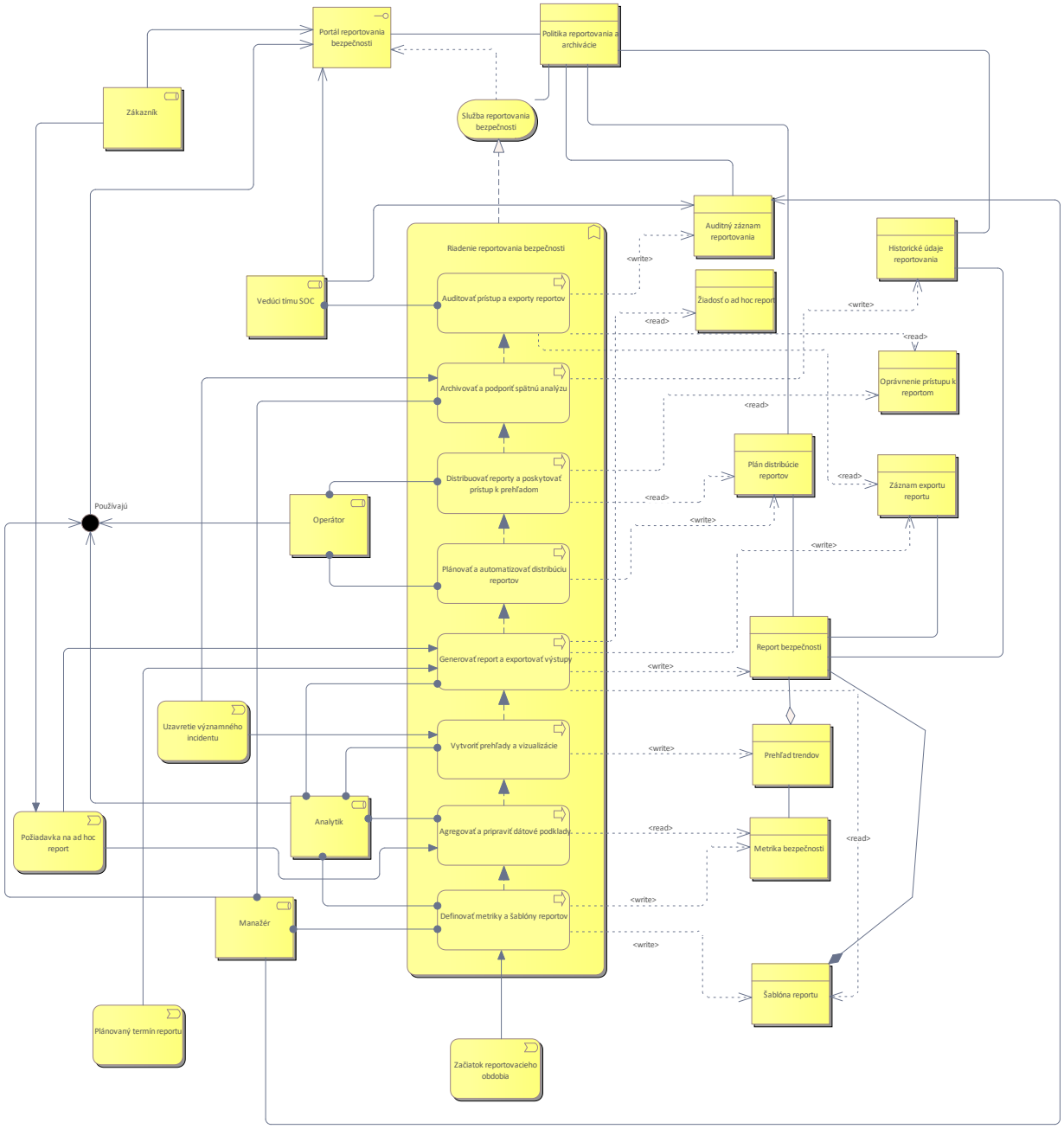
Uzatvorenie a post-incident reporting - BusinessProcess

Záver incidentu, lessons learned, reporty, odporúčania, auditovateľná stopa.

Vyšetrovanie a analýza dopadu - BusinessProcess

Zistenie príčiny, rozsahu, dotknutých aktív a služby; návrh mitigácie.

4.3.8 Riadenie reportovania bezpečnosti - biznis realizácia služby



Obrázok 9 : Riadenie reportovania bezpečnosti - biznis realizácia služby

Diagram popisuje, ako sa v SOCaaS službe riadi reportovanie bezpečnosti od spúšťacích udalostí až po tvorbu výstupov, ich distribúciu, archiváciu a audit. Biznis funkcia združuje procesy, ktoré definujú metriky a šablóny, pripravia dátové podklady, vytvoria vizualizácie, vygenerujú report a zabezpečia jeho doručenie podľa plánov a oprávnení. Roly analytik, operátor, vedúci tímu SOC a manažér majú rozdelené zodpovednosti tak, aby boli výstupy konzistentné, dohľadateľné a použiteľné pre zákazníka aj interné riadenie.

Popis používaných prvkov:

Plánovaný termín reportu - BusinessEvent

Udalosť vyjadruje pravidelný cyklus reportovania podľa plánu distribúcie a spúšťa prípravu a generovanie výstupov. Zabezpečuje, že reporty vznikajú konzistentne a včas pre dohodnuté obdobia a adresátov. Pomáha udržať predvídateľnosť a znižuje závislosť na manuálnej iniciácii.

Požiadavka na ad hoc report - BusinessEvent

Udalosť vzniká, keď zákazník alebo manažment potrebuje mimoriadny výstup pre konkrétnu situáciu. Spúšťa proces prípravy dát a generovania reportu s presne definovaným rozsahom a úrovňou detailu. Podporuje rýchlu reakciu pri incidentoch, auditoch alebo pri rozhodovaní o nápravných krokoch. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou informovaného rozhodovania, dohľadateľnosti a poskytovania výstupov pre zodpovedné roly.

Riadenie reportovania bezpečnosti - BusinessFunction

Funkcia riadi celý životný cyklus reportov od definovania metrík a šablón až po publikovanie, plánovanie distribúcie a archiváciu výstupov. Zabezpečuje, že reporty sú konzistentné, porovnateľné v čase a prispôsobené úrovni detailu od technických prehľadov až po strategické zhrnutia. Funkcia podporuje dohľadateľnosť exportov a riadenie prístupov tak, aby reportovanie bolo bezpečné aj v prostredí viacerých zákazníkov. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou informovaného rozhodovania, dohľadateľnosti a poskytovania výstupov pre zodpovedné roly.

Služba reportovania bezpečnosti - BusinessService

Služba zabezpečuje agregáciu, vizualizáciu a distribúciu bezpečnostných informácií pre rôzne cieľové skupiny v prostredí viacerých zákazníkov. Poskytuje pravidelné aj ad hoc výstupy o incidentoch, výstrahách, výkonnosti opatrení a plnení dohôd o úrovni služieb, aby podporila rozhodovanie a zodpovednosť. Služba udržiava históriu, umožňuje spätnú analýzu a podporuje audit a súlad s požiadavkami regulácií. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou informovaného rozhodovania, dohľadateľnosti a poskytovania výstupov pre zodpovedné roly.

Uzavretie významného incidentu - BusinessEvent

Udalosť signalizuje, že incident bol vyriešený a je pripravený na zhrnutie, poučenia a zhodnotenie dopadu v reportoch. Spúšťa aktualizáciu metrík, trendov a prípadne prípravu výstupu pre vedenie alebo zákazníka. Zlepšuje zodpovednosť tým, že výsledok riešenia je zachytený aj v historických výstupoch. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou informovaného rozhodovania, dohľadateľnosti a poskytovania výstupov pre zodpovedné roly.

Začiatok reportovacieho obdobia - BusinessEvent

Udalosť označuje začiatok nového dohodnutého obdobia pre reportovanie, napríklad týždeň, mesiac alebo štvrťrok. Spúšťa overenie platnosti metrík a šablón a následne prípravu údajov tak, aby boli výstupy konzistentné a porovnateľné v čase. V prostredí viacerých zákazníkov zároveň

potvrdzuje, pre ktorých zákazníkov a v akom rozsahu sa daný reportovací cyklus vykoná.

Analytik - BusinessRole

Pripravuje technický obsah reportov, interpretuje trendy a vysvetľuje príčiny zmien v metrikách a výstrahách. Používa reporty na prioritizáciu práce, hodnotenie účinnosti detekcie a podporu vyšetrovania incidentov. Dohliada na kvalitu dátových podkladov a dopĺňa komentáre k zisteniam, ktoré sú dôležité pre rozhodovanie.

Auditný záznam reportovania - BusinessObject

Záznam o prístupe k reportom a o vytváraní exportov, ktorý obsahuje kto, kedy, z akého dôvodu a v akom rozsahu pracoval s výstupmi. Umožňuje spätné overenie oprávnenosti prístupov, vyšetrovanie sporov a preukázanie dohľadateľnosti činností. V prostredí viacerých zákazníkov sa eviduje aj priradenie k zákazníkovi a k reportovaciemu obdobiu.

Historické údaje reportovania - BusinessObject

Predstavujú archivované výstupy a podklady, ktoré umožňujú spätnú analýzu trendov a overenie rozhodnutí. Udržiavajú konzistentné časové rady a kontext, aby bolo možné porovnávať účinnosť opatrení v dlhšom horizonte. Slúžia aj na audit a na preukázanie súladu s požiadavkami na uchovávanie záznamov.

Manažér - BusinessRole

Používa strategické zhrnutia na rozhodovanie o prioritách, investíciách a zodpovednosti za bezpečnostné opatrenia. Vyžaduje auditovateľnosť a zrozumiteľnosť výstupov, aby sa dali obhájiť voči internému auditu alebo regulátorovi. Schvaľuje pravidlá reportovania, archivácie a prístupu k citlivým informáciám v prostredí viacerých zákazníkov.

Metrika bezpečnosti - BusinessObject

Predstavuje definovanú hodnotu používanú na meranie stavu bezpečnosti, napríklad počty incidentov, výstrah alebo časové ukazovatele riešenia. Obsahuje metodiku výpočtu, časové okno a priradenie k zákazníkovi, aby boli výsledky porovnateľné a interpretovateľné. Slúži ako základ pre prehľady trendov, hodnotenie výkonnosti a plnenie dohôd o úrovni služieb.

Operátor - BusinessRole

Zabezpečuje operatívnu distribúciu reportov, kontroluje dostupnosť výstupov a rieši praktické požiadavky na exporty. Sleduje plánované cykly reportov, dohliada na doručenie správnym adresátom a eviduje výpadky alebo chyby exportu. Pomáha s udržiavaním reportovacích prehľadov tak, aby boli vždy pripravené pre analytikov a manažment.

Oprávnenie prístupu k reportom - BusinessObject

Reprezentuje pravidlá, ktoré určujú, kto môže vidieť konkrétne prehľady, exportovať reporty alebo meniť šablóny. V prostredí viacerých zákazníkov zabezpečuje oddelenie údajov a obmedzuje prístup na základe roly a zákazníka. Podporuje bezpečnú distribúciu a minimalizuje riziko úniku citlivých

informácií.

Plán distribúcie reportov - BusinessObject

Obsahuje harmonogramy, adresátov a pravidlá doručovania reportov pre jednotlivé roly a zákazníkov. Zohľadňuje citlivosť údajov a oprávnenia, aby sa informácie šírili len v rozsahu, ktorý je povolený. Podporuje automatizáciu a znižuje riziko oneskorení alebo nesprávneho doručenia.

Politika reportovania a archivácie - Contract

Politika definuje rozsah reportovania, periodicitu výstupov, minimálne metriky a pravidlá pre úroveň detailu pre rôzne cieľové skupiny. Upravuje uchovávanie historických údajov, požiadavky na dohľadateľnosť exportov a pravidlá prístupu k citlivým informáciám. Zabezpečuje, že reportovanie je konzistentné, auditovateľné a v súlade s internými a regulačnými požiadavkami. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou informovaného rozhodovania, dohľadateľnosti a poskytovania výstupov pre zodpovedné roly.

Prehľad trendov - BusinessObject

Zobrazuje vývoj vybraných metrík v čase a umožňuje identifikovať odchýlky, zhoršenie alebo zlepšenie situácie. Podporuje porovnávanie období a vysvetlenie príčin zmien na základe udalostí, zásahov a úprav konfigurácie. Používa sa pri plánovaní opatrení, hodnotení účinnosti a pri komunikácii s vedením a zákazníkom.

Report bezpečnosti - BusinessObject

Je výsledný výstup reportovania za definované obdobie alebo pre konkrétnu ad hoc potrebu. Obsahuje zhrnutia incidentov, výstrah, plnenia dohôd o úrovni služieb a odporúčania podľa zistených trendov. Slúži na rozhodovanie, audit, komunikáciu so zákazníkom a preukázanie zodpovednosti. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou informovaného rozhodovania, dohľadateľnosti a poskytovania výstupov pre zodpovedné roly.

Šablóna reportu - BusinessObject

Definuje štruktúru reportu, rozsah obsahu, úroveň detailu a spôsob prezentácie pre konkrétnu cieľovú skupinu. Zabezpečuje konzistentnosť výstupov naprieč obdobiami a znižuje riziko, že sa dôležité informácie vynechajú. Obsahuje aj pravidlá označenia obdobia, verzie a povinné komentáre k interpretácii.

Vedúci tímu SOC - BusinessRole

Využíva reporty na riadenie výkonu tímu, kontrolu plnenia dohôd o úrovni služieb a identifikáciu slabých miest procesov. Schvaľuje šablóny reportov a úroveň detailu pre jednotlivé cieľové skupiny, aby výstupy zodpovedali potrebám. Koordinuje zlepšovacie opatrenia na základe trendov a opakujúcich sa príčin incidentov.

Zákazník - BusinessRole

Prijíma vybrané reporty a prehľady podľa dohodnutého rozsahu a úrovne detailu. Používa výstupy na kontrolu stavu

bezpečnosti, plnenia dohôd o úrovni služieb a na rozhodovanie o nápravných krokoch. Môže žiadať ad hoc reporty pri významných udalostiach alebo pri potrebe preukázania súladu s auditnými požiadavkami.

Záznam exportu reportu - BusinessObject

Eviduje vytvorenie a odovzdanie exportu reportu vrátane času, používateľa, šablóny a rozsahu údajov. Umožňuje spätné overenie, kto vytvoril výstup, a podporuje vyšetrovanie sporov alebo podozrivých aktivít. Je dôležitý pre audit a pre požiadavky na dohľadateľnosť v regulovaných prostrediach.

Žiadosť o ad hoc report - BusinessObject

Zachytáva požiadavku na mimoriadny výstup mimo pravidelného cyklu, napríklad pri významnej udalosti alebo pri audite. Obsahuje rozsah, cieľovú skupinu, časové obdobie a očakávanú úroveň detailu, aby sa report pripravil správne. Podporuje priorizáciu práce a dohľadateľnosť, prečo bol report vytvorený a komu bol určený.

Používajú - Junction

Portál reportovania bezpečnosti - BusinessInterface

Rozhranie poskytuje prístup k prehľadom, vizualizáciám a exportom reportov podľa roly a priradenia k zákazníkovi. Umožňuje filtrovanie, porovnávanie období a zobrazenie kontextu metrík, aby používatelia rozumeli príčinám zmien. Podporuje dohľadateľnosť tým, že sprístupňuje aj informácie o šablónach, verziách a histórii exportov. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou informovaného rozhodovania, dohľadateľnosti a poskytovania výstupov pre zodpovedné roly.

Agregovať a pripraviť dátové podklady - BusinessProcess

Proces zhromažďuje údaje z bezpečnostných zdrojov a pripravuje ich do podoby vhodnej na vizualizáciu a výpočet metrík. Zabezpečuje konzistentnosť časových okien, normalizáciu polí a kontrolu kvality, aby výstupy neboli skreslené. V prostredí viacerých zákazníkov udržiava oddelenie dát a správne priradenie podkladov k zákazníkovi.

Archivovať a podporiť spätnú analýzu - BusinessProcess

Proces uchováva historické reporty a podkladové údaje tak, aby sa dali spätne overiť trendy, rozhodnutia a súlad s požiadavkami. Umožňuje porovnávať obdobia, hľadať opakujúce sa príčiny incidentov a vyhodnocovať účinnosť bezpečnostných opatrení. Archivácia podporuje audit a zodpovednosť tým, že výstupy zostávajú dohľadateľné a nemenné.

Auditovať prístup a exporty reportov - BusinessProcess

Proces eviduje prístupy k reportom, spustenia exportov a významné zmeny šablón alebo oprávnení. Podporuje vyšetrovanie neoprávnených prístupov a umožňuje preukázať, kto pracoval s citlivými

informáciami. Je dôležitý pre viacúrovňové tímy a pre požiadavky regulácií, ktoré vyžadujú spätnú verifikáciu činností.

Definovať metriky a šablóny reportov - BusinessProcess

Proces stanoví, ktoré metriky sa sledujú, ako sa počítajú a aké šablóny výstupov sa používajú pre jednotlivé cieľové skupiny. Zohľadňuje technický pohľad pre analytikov aj strategické zhrnutia pre vedenie a zákazníka, aby bol obsah primeraný. Výsledkom je jednotný rámec, ktorý umožňuje porovnávanie v čase a znižuje riziko nejednoznačnej interpretácie.

Distribuovať reporty a poskytovať prístup k prehľadom - BusinessProcess

Proces doručí reporty a sprístupní interaktívne prehľady cez reportovací portál podľa pravidiel prístupu. Podporuje ad hoc žiadosti, keď je potrebné rýchlo pripraviť pohľad na konkrétnu udalosť alebo obdobie. Zabezpečuje, že používatelia vidia len údaje priradené k ich roli a zákazníkovi.

Generovať report a exportovať výstupy - BusinessProcess

Proces vytvára reporty vo formátoch vhodných na distribúciu a archiváciu, napríklad tabuľkové výstupy a dokumentové zostavy. Zabezpečuje konzistentné označenie obdobia, zdrojov a verzie šablóny, aby bol report dohľadateľný aj po čase. Pri exporte vytvára záznam, ktorý podporuje audit a vysvetlenie, kto a kedy výstup vytvoril.

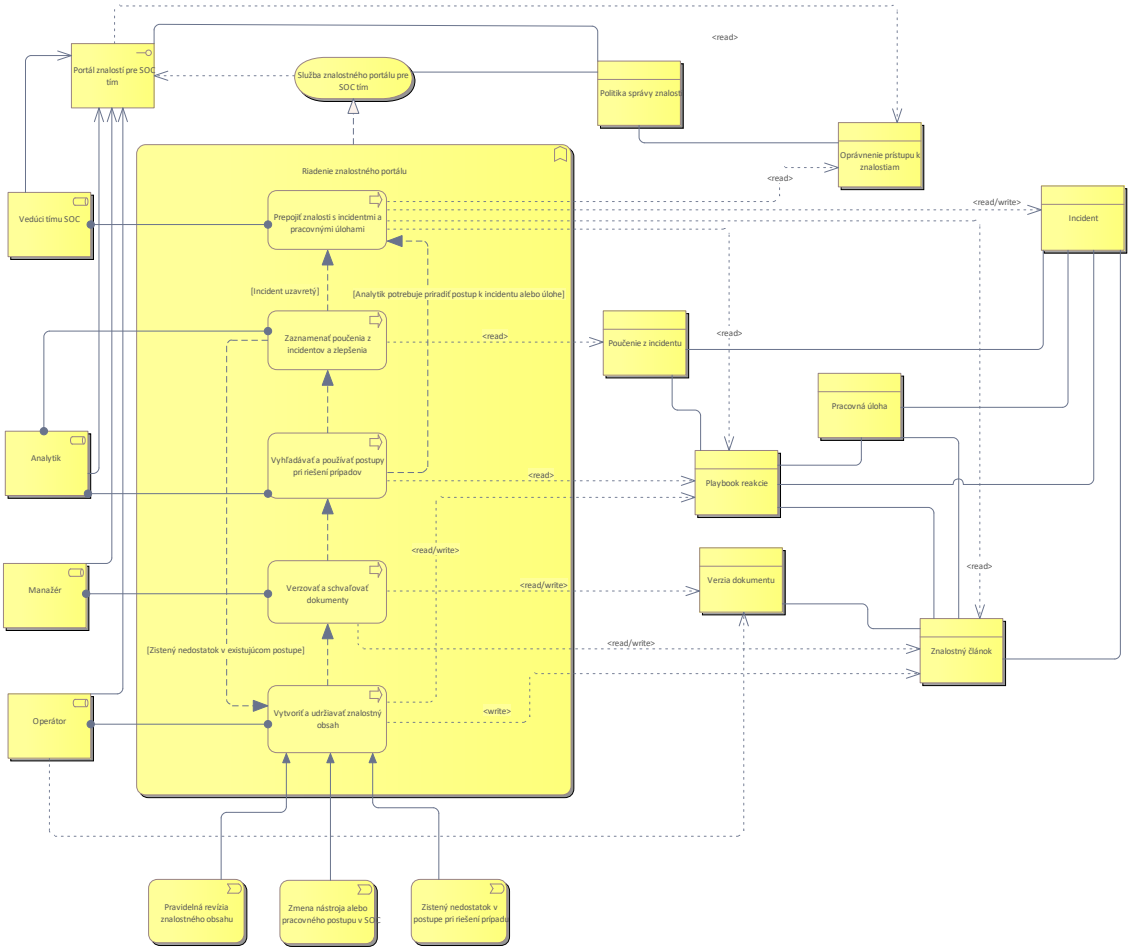
Plánovať a automatizovať distribúciu reportov - BusinessProcess

Proces nastavuje harmonogramy pravidelných výstupov a pravidlá doručovania pre jednotlivé cieľové skupiny a zákazníkov. Zohľadňuje citlivosť údajov a oprávnenia, aby sa výstupy dostali len k správnym adresátom. Znižuje manuálnu prácu tímu a zabezpečuje, že reportovanie prebieha konzistentne podľa dohôd.

Vytvoriť prehľady a vizualizácie - BusinessProcess

Proces vytvára prehľady trendov v čase, súhrny výstrah a incidentov a pohľady na plnenie dohôd o úrovni služieb. Vizualizácie sú navrhnuté tak, aby umožnili rýchle filtrovanie, porovnávanie období a identifikáciu odchýlok. Výstupy sú pripravené pre technické aj manažérske použitie a podporujú rozhodovanie na základe faktov.

4.3.9 Riadenie znalostného portálu pre SOC tím - biznis realizácia služby



Obrázok 10 : Riadenie znalostného portálu pre SOC tím - biznis realizácia služby

Diagram zachytáva, ako SOCaaS buduje a udržiava znalosti potrebné na konzistentnú reakciu na incidenty. Ukazuje zodpovednosti rolí pri tvorbe obsahu, schvaľovaní, vyhľadávaní postupov a zaznamenávaní poučení z incidentov, vrátane riadenia prístupov a väzieb na incidenty a pracovné úlohy. Cieľom je, aby postupy boli dohľadateľné, verziované, kontrolované a okamžite použiteľné pri riešení prípadov.

Popis používaných prvkov:

Riadenie znalostného portálu - BusinessFunction

Funkcia riadi tvorbu, schvaľovanie, verzovanie a publikovanie znalostného obsahu tak, aby bol aktuálny a použiteľný v praxi. Zabezpečuje štruktúru obsahu, vyhľadateľnosť, prepojenie na incidenty a dohľadateľnosť zmien pre audit a spätné učenie. Podporuje integráciu s ďalšími nástrojmi SOC, aby sa znalosti prirodzene používali pri riešení prípadov. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou jednotných postupov, dohľadateľnosti rozhodnutí a kolektívneho učenia z incidentov.

Služba znalostného portálu pre SOC tím - BusinessService

Služba poskytuje centrálne miesto na uchovávanie a zdieľanie playbookov, postupov, odporúčaní a poučení z incidentov. Zvyšuje konzistentnosť reakcie, skracuje čas zaškolenia nových členov a podporuje štandardizáciu metodík a procesov. V prostredí viacerých zákazníkov zabezpečuje oprávnenia, históriu zmien, verzovanie a prepojenie na incidenty a pracovné úlohy. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou jednotných postupov, dohľadateľnosti rozhodnutí a kolektívneho učenia z incidentov.

Manažér - BusinessRole

Manažér schvaľuje obsah, ktorý má dopad na pravidlá, zodpovednosti, eskalácie alebo požiadavky na zákazníka. Kontroluje súlad s internými politikami, auditnými požiadavkami a záväzkami voči zákazníkovi. Je vhodný najmä pre obsah s vyššou úrovňou formálnosti.

Operátor - BusinessRole

Operátor dopĺňa znalostnú bázu o prevádzkové postupy, konfigurácie a rutinné kroky, ktoré zabezpečujú opakovateľnosť. Aktualizuje návody pri zmenách nástrojov a pracovných postupov a dbá na to, aby boli kroky vykonateľné v praxi. Je vhodný najmä pre obsah typu postupy a návody, nie pre analytické interpretácie.

Oprávnenie prístupu k znalostiam - BusinessObject

Definuje kto môže obsah čítať, upravovať alebo schvaľovať a v akom rozsahu. Zabezpečuje, že citlivé poznatky sú dostupné len oprávneným rolám a že v prostredí viacerých zákazníkov nedochádza k nežiaducej viditeľnosti. Podporuje kontrolu prístupov a dohľadateľnosť, kto s obsahom pracoval.

Playbook reakcie - BusinessObject

Je praktický postup krok za krokom pre typické situácie, napríklad pri malvéri, úniku údajov alebo podozrivej komunikácii. Zabezpečuje konzistentnosť reakcie, minimalizuje improvizáciu a urýchľuje rozhodovanie v čase tlaku. Obsahuje kontrolné body, ktoré pomáhajú preukázať správny postup pri audite a spätnej kontrole. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou jednotných postupov, dohľadateľnosti rozhodnutí a kolektívneho učenia z incidentov.

Politika správy znalostí - Contract

Politika definuje štruktúru obsahu, pravidlá tvorby, schvaľovania a verzovania dokumentov a minimálne požiadavky na kvalitu. Upravuje oprávnenia, prístup k citlivým poznatkom, archiváciu a spôsob prepojenia na incidenty a pracovné úlohy. Zabezpečuje, že znalosti sú konzistentné, auditovateľné a dlhodobo udržiavateľné v prostredí viacerých zákazníkov. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou jednotných postupov, dohľadateľnosti rozhodnutí a kolektívneho učenia z incidentov.

Poučenie z incidentu - BusinessObject

Zaznamenáva čo fungovalo, čo zlyhalo a aké zlepšenia treba urobiť po vyriešení incidentu. Premieta sa do úprav playbookov, šablón a nastavení, aby sa rovnaké chyby neopakovali. Je dôležité pre

budovanie tímových znalostí a pre dlhodobé zvyšovanie efektivity reakcie. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou jednotných postupov, dohľadateľnosti rozhodnutí a kolektívneho učenia z incidentov.

Verzia dokumentu - BusinessObject

Predstavuje konkrétny stav dokumentu v čase vrátane autora, dátumu a zoznamu zmien. Umožňuje vrátiť sa k predchádzajúcemu obsahu a vysvetliť, prečo došlo k úprave postupu alebo odporúčania. Podporuje audit a znižuje riziko, že sa bude používať neaktuálny alebo neschválený obsah.

Znalostný článok - BusinessObject

Predstavuje samostatný dokument so štruktúrovaným obsahom, ktorý opisuje tému, postup alebo odporúčanie. Obsahuje popis problému, kroky riešenia, podmienky použitia a odkazy na súvisiace zdroje a incidenty. Je verzovaný a riadený oprávneniami, aby sa zachovala kvalita a dohľadateľnosť zmien.

Portál znalostí pre SOC tím - BusinessInterface

Rozhranie poskytuje prístup k dokumentom, playbookom a poučeniam a umožňuje vyhľadávanie podľa tém, incidentov a techník útoku. Podporuje prácu s verziami, komentármi a väzbami na incidenty a úlohy, aby sa znalosti dali použiť priamo v prevádzke. Zabezpečuje riadenie prístupov a zobrazuje históriu zmien pre dohľadateľnosť. Súvis s UC_04 Upozorniť a eskalovať bezpečnostný incident podporou jednotných postupov, dohľadateľnosti rozhodnutí a kolektívneho učenia z incidentov.

Prepojiť znalosti s incidentmi a pracovnými úlohami - BusinessProcess

Proces vytvára väzby medzi dokumentmi, incidentmi a úlohami tak, aby sa pri riešení prípadov používal správny postup. Umožňuje rýchlo pochopiť, ktorý postup bol použitý a aký mal výsledok, čo podporuje audit a spätné overovanie. Znižuje duplicitnú dokumentáciu tým, že obsah sa zdieľa cez odkazy a nie opakovaným kopírovaním.

Verzovať a schvaľovať dokumenty - BusinessProcess

Proces spravuje verzie dokumentov, eviduje zmeny a umožňuje schvaľovací postup pred publikovaním. Zvyšuje dôveryhodnosť obsahu tým, že každá zmena má autora, dôvod a je dohľadateľná aj po čase. Podporuje audit a umožňuje návrat k predchádzajúcim verziám pri sporoch alebo pri potrebe porovnania.

Vyhľadávať a používať postupy pri riešení prípadov - BusinessProcess

Proces umožňuje rýchlo nájsť relevantný playbook alebo návod podľa typu incidentu, indikátora alebo použitej techniky útoku. Podporuje konzistentný postup pri reakcii a znižuje riziko vynechania dôležitých krokov v časovej tiesni. Znalosti sa používajú priamo pri práci s incidentmi a výsledok sa môže spätne doplniť do obsahu.

Vytvoriť a udržiavať znalostný obsah - BusinessProcess

Proces zahŕňa tvorbu dokumentov, playbookov a odporúčaní a ich priebežnú aktualizáciu podľa vývoja hrozieb a nástrojov. Zabezpečuje, že znalosti sú zachytené v štruktúrovanej podobe a sú dostupné pre celý tím bez závislosti na konkrétnych osobách. Obsah sa dopĺňa aj o praktické poznámky a príklady, aby bol použiteľný v reálnych situáciách.

Zaznamenať poučenia z incidentov a zlepšenia - BusinessProcess

Proces zachytáva poučenia z ukončených incidentov a premieňa ich na konkrétne úpravy playbookov, odporúčaní a postupov. Zabezpečuje, že tím sa kolektívne učí a že poznatky sú dostupné aj pre nových členov. Pomáha zvyšovať kvalitu reakcie v čase a znižovať opakovanie rovnakých chýb.

Pravidelná revízia znalostného obsahu - BusinessEvent

Udalosť vyjadruje plánovaný moment, keď sa kontroluje aktuálnosť článkov a playbookov podľa dohodnutého cyklu. Spúšťa prechádzanie obsahu, identifikáciu neaktuálnych postupov a prípravu zmien na schválenie. Pomáha predchádzať tomu, aby tím používal zastarané návody pri riešení prípadov.

Zistený nedostatok v postupe pri riešení prípadu - BusinessEvent

Udalosť vzniká, keď analytik počas riešenia zistí, že existujúci postup je neúplný, nejasný alebo nepokrýva konkrétnu situáciu. Spúšťa doplnenie obsahu a jeho následné schválenie, aby sa zistenie premietlo do štandardizovaného postupu. Podporuje kontinuálne zlepšovanie bez čakania na veľké revízne cykly.

Zmena nástroja alebo pracovného postupu v SOC - BusinessEvent

Udalosť nastáva pri úprave nástrojov, pracovných tokov alebo zodpovedností, ktorá mení spôsob riešenia prípadov. Spúšťa aktualizáciu súvisiacich článkov a playbookov tak, aby zodpovedali reálnej prevádzke. Znižuje riziko chýb spôsobených nesúladom medzi dokumentáciou a praxou.

Analytik - BusinessRole

Používa portál znalostí pri riešení prípadov a vyhľadáva schválené postupy. Zodpovedá za to, že sa v praxi používajú aktuálne verzie a že sa odchýlky alebo nové zistenia vrátia späť do znalostnej bázy. Podieľa sa na zaznamenávaní poučení po uzavretí incidentov.

Incident - BusinessObject

Záznam bezpečnostnej udalosti, ktorá vyžaduje koordinované riešenie, evidenciu krokov a uzavretie s výsledkom. Slúži ako kotva pre prepojenie na použité postupy, relevantné články a poučenia, aby bolo možné spätne obhájiť priebeh riešenia. Podporuje audit a zodpovednosť v prostredí viacerých zákazníkov.

Pracovná úloha - BusinessObject

Záznam úlohy, ktorá vzniká pri náprave, doplnení dôkazov alebo pri implementácii odporúčaní zo znalostného obsahu. Umožňuje sledovať stav, termíny, zodpovednosť a výsledok, aby sa zlepšenia realizovali a nezostali iba v dokumentácii. Prepojenie na znalosti zabezpečí, že úloha má jasný postup a očakávaný výstup.

Vedúci tímu SOC - BusinessRole

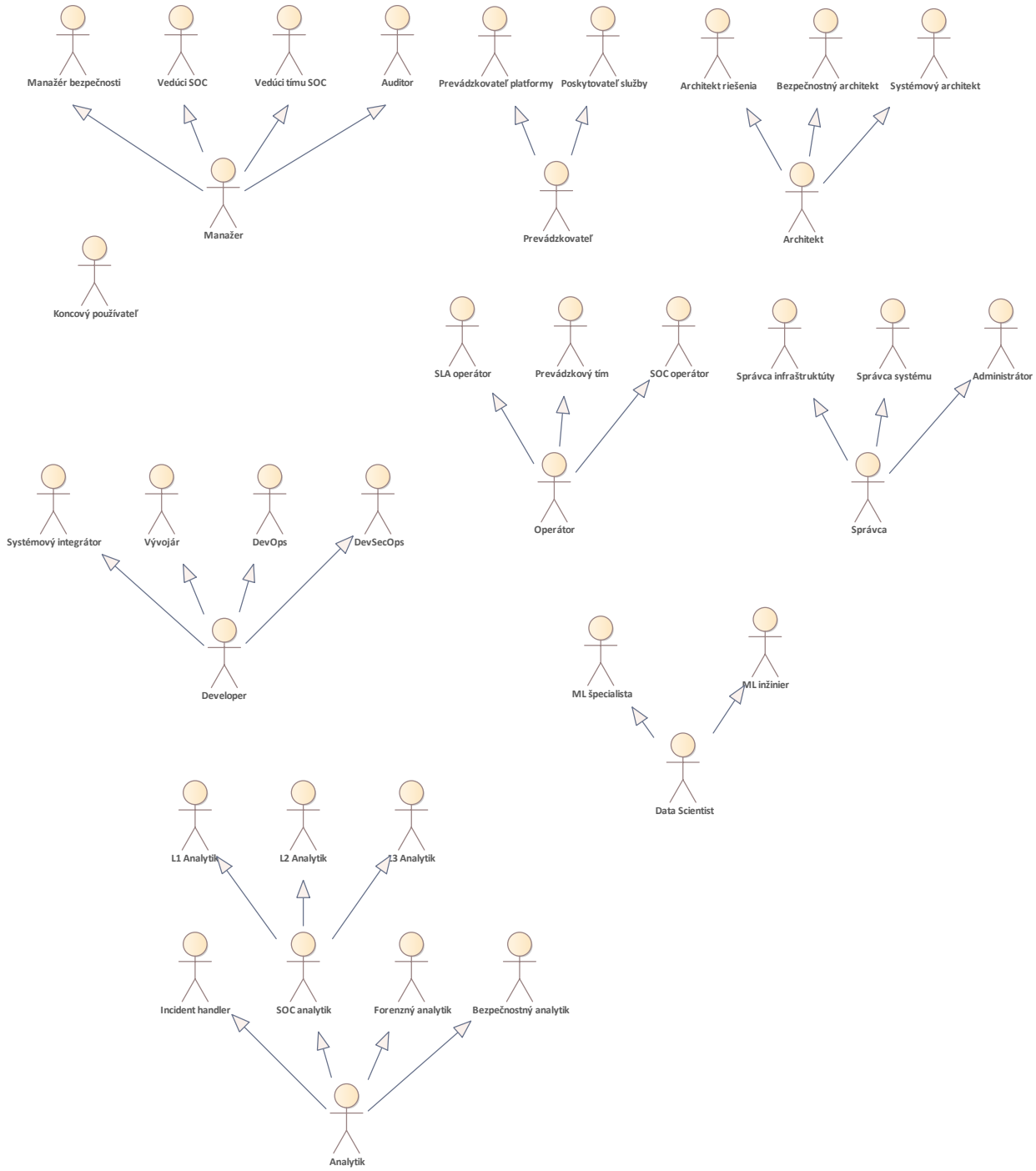
Zabezpečuje, že znalosti sú používané konzistentne a že sa poučenia z incidentov premietajú do postupov. Riadi prepojenia medzi incidentmi, pracovnými úlohami a relevantným obsahom, aby bola dohľadateľná metodika riešenia. Dohliada na kvalitu, úplnosť a dodržiavanie politiky správy znalostí.

4.4 BPMN - Biznis procesný model

4.5 Prípady použitia

V nasledujúcej kapitole sú uvedené jednotlivé používateľské scenáre.

4.5.1 Aktéri



Obrázok 11 : Aktéri

Názov aktéra/roly	Popis

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 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.

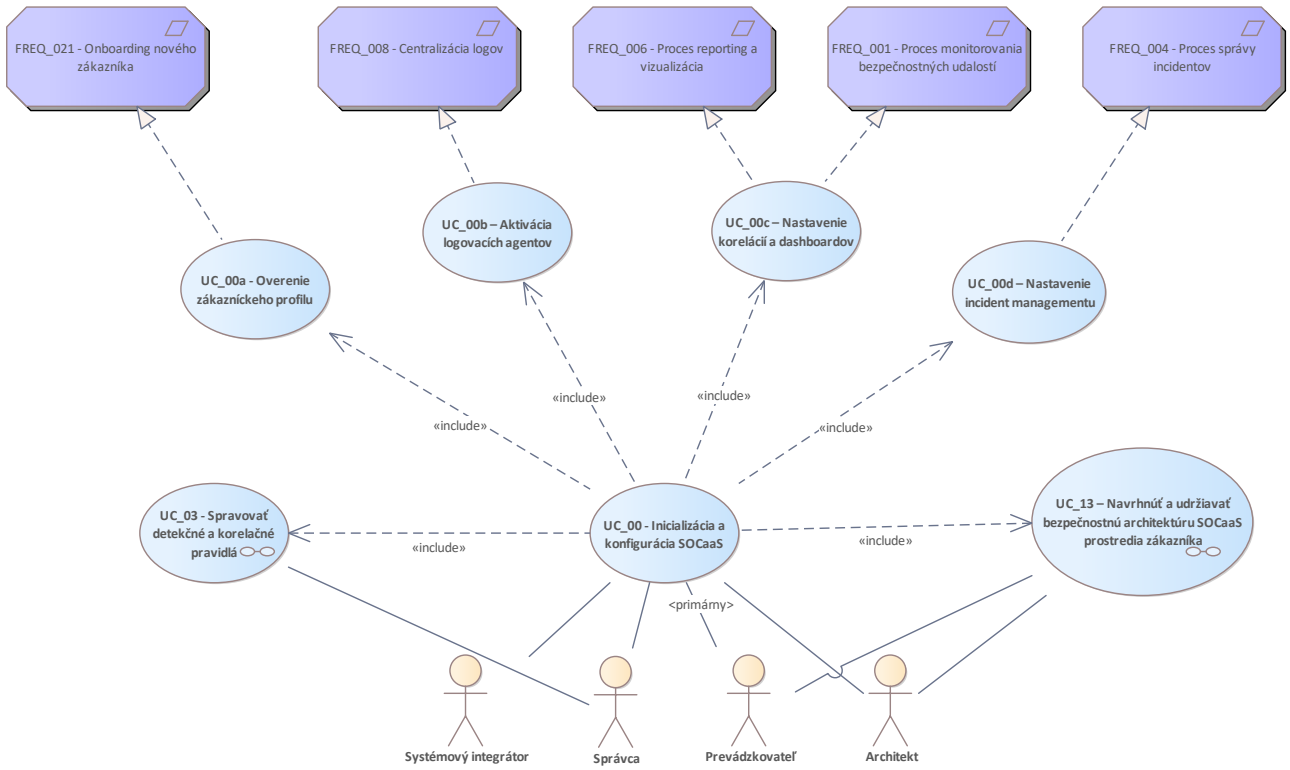
Názov aktéra/roly	Popis
Forenzný analytik	Zodpovedá za oblasti ako sú: voliteľné rozšírenia a EDR/XDR.
Incident handler	Zodpovedá za oblasti ako sú: SOAR a Evidencia a správaincidentov.
Incident Handler	
Koncový používateľ	Zodpovedá za oblasti ako sú: Vizualizácia dát.
L1 Analytik	
L2 Analytik	
L3 Analytik	
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.

Názov aktéra/roly	Popis
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 Aministratíva 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.

4.5.2 Všeobecné prípady použitia

4.5.2.1 Prípady použitia diagramy

4.5.2.2 UC_00 - Inicializácia a konfigurácia SOCaaS



Obrázok 12 : 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	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.
Výstupná podmienka	Logy zo všetkých povinných zdrojov obsahujú povinné polia pre detekciu.

Basic Path	Basic Path

Krok	Aktivita
1	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.

ALT_00_01 – Neúplný profil zákazníka	Alternate

Krok	Aktivita
1	Systém zistí chýbajúce údaje.
2	Upozorní architekta na doplnenie.
3	Proces pokračuje po doplnení informácií.

ALT_00_02 – 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.

Naviazané funkčné požiadavky	
UC_03 - Spravovať detekčné a korelačné pravidlá	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).
UC_00b – Aktivácia logovacích agentov	Systém aktivuje logovacích agentov zákazníka pre odosielanie logov do SOCaaS.
UC_13 – Navrhnúť a udržiavať bezpečnostnú architektúru SOCaaS prostredia zákazníka	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), a zoznam povinných log zdrojov a typov logov ktorý slúži ako podklad pre onboarding (UC_00), monitoring (UC_01), správu aktív (UC_11), zraniteľností (UC_12) a automatizáciu (UC_07).
UC_00c – Nastavenie korelácií a dashboardov	Systém vytvorí preddefinované korelačné pravidlá a dashboardy pre monitoring bezpečnostných udalostí.
UC_00a - Overenie zákazníckeho profilu	Systém overí, či zákaznícky tenant obsahuje všetky povinné údaje (identifikačné, technické, integračné).
UC_00d – Nastavenie incident managementu	Systém aktivuje workflow pre správu incidentov a priradenia rolí.

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.
4	Overenie je úspešné.

ALT_00a_01 – Neúplné údaje	Alternate

Krok	Aktivita
1	Systém vyžiada doplnenie chýbajúcich údajov

ALT_00a_02 – Tenantu chýba technická konfigurácia	Alternate

Krok	Aktivita
1	Systém zastaví proces a upozorní správcu.

Naviazané funkčné požiadavky	
FREQ_021 - Onboarding nového zákazníka	Riešenie musí zabezpečiť onboarding nového zákazníka, kde prebieha integrácia jeho infraštruktúry do multitenantného prostredia SOCaaS. To zahŕňa: • nastavenie logovacieho agenta • konfiguráciu korelačných pravidiel • vytvorenie separovaných dashboardov • nastavenie incident managementu pre zákazníka
UC_00a - Overenie zákazníckeho profilu	Systém overí, či zákaznícky tenant obsahuje všetky povinné údaje (identifikačné, technické, integračné).
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.	
ALT_00b_01 – Agent neodpovedá		Alternate
Krok	Aktivita	
1	Systém oznámi chybu, pokračuje neskôr.	
ALT_00b_02 – Chybné API kľúče		Alternate
Krok	Aktivita	
1	Systém vyžiada opätovné nahratie kľúčov.	

Naviazané funkčné požiadavky	
FREQ_008 - Centralizácia logov	Riešenie musí zabezpečiť zber a centralizáciu logov zo systémov, sietí, koncových bodov a aplikácií.
UC_00b – Aktivácia logovacích agentov	Systém aktivuje logovacích agentov zákazníka pre odosielanie logov do SOCaaS.
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.

ALT_00c_02 – Dashboard sa nedá vytvoriť	Alternate

Krok	Aktivita
1	Systém vytvorí len minimálnu verziu. (poslednú spustiteľnú)

ALT_00c_01 – Korelačné pravidlo je neplatné	Alternate

Krok	Aktivita
1	Systém ho preskočí a nahlási chybu.

Naviazané funkčné požiadavky	
FREQ_006 - Proces reporting a vizualizácia	Zabezpečiť proces reporting a vizualizácia – zabezpečuje pravidelný výstup pre manažment, audítorov a SOC analytikov.
FREQ_001 - Proces monitorovania bezpečnostných udalostí	Zabezpečiť proces monitorovania bezpečnostných udalostí – zabezpečuje zber a sledovanie logov, metrických údajov a alertov zo všetkých integrovaných systémov.

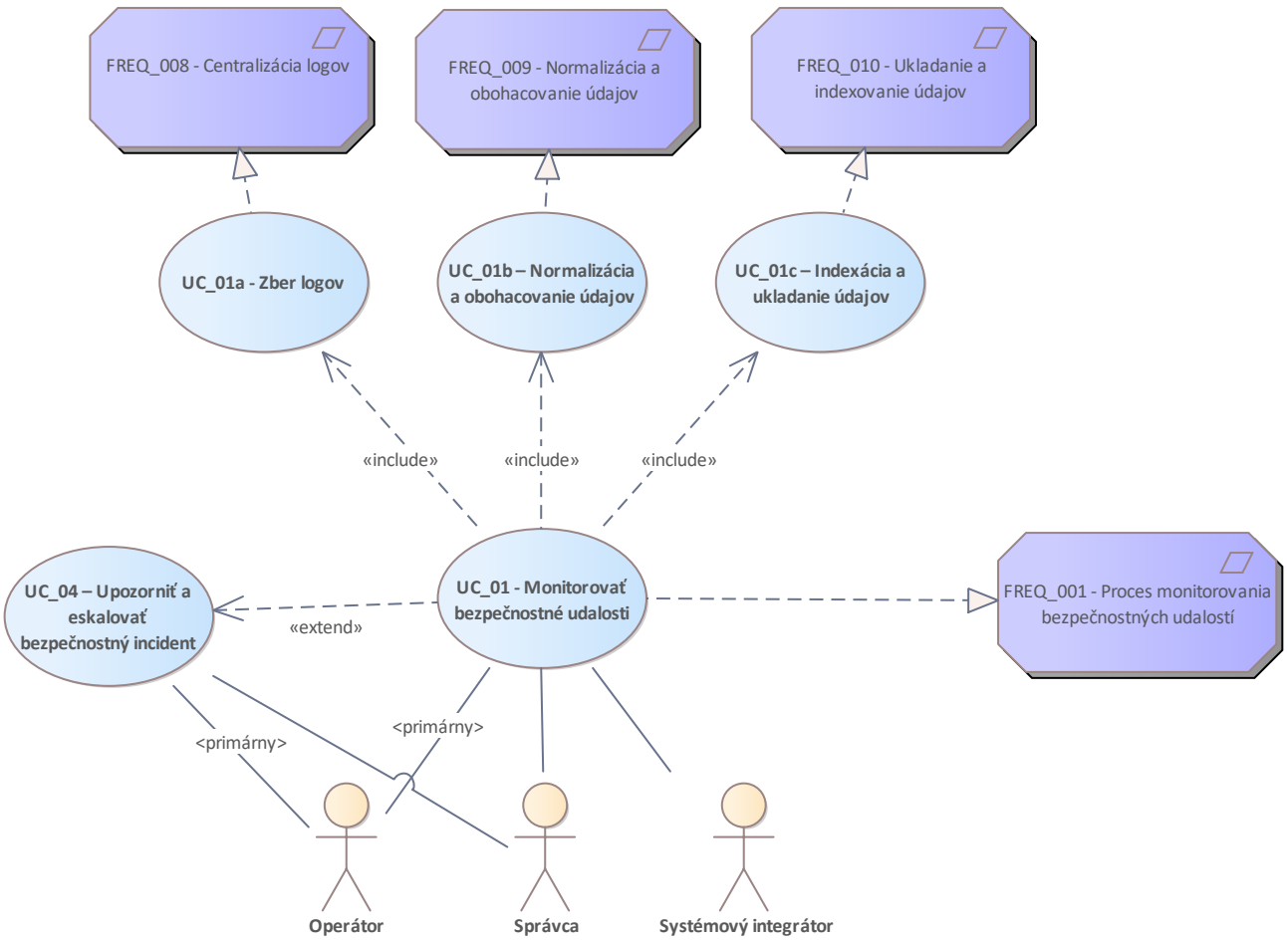
UC_00c – Nastavenie korelácií a dashboardov	Systém vytvorí preddefinované korelačné pravidlá a dashboardy pre monitoring bezpečnostných udalostí.
Prípad použitia	UC_00d – Nastavenie incident managementu
Cieľ	Systém aktivuje workflow pre správu incidentov a priradenia rolí.

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).	
ALT_00d_01 – Neexistujú roly používateľov		Alternate
Krok	Aktivita	
1	Systém zastaví workflow a požiada správcu o pridanie rolí.	
ALT_00d_02 – Ticketing modul je nedostupný		Alternate
Krok	Aktivita	
1	Systém aktivuje len základný SOAR fallback.	

Naviazané funkčné požiadavky	
FREQ_004 - Proces správy incidentov	Zabezpečiť proces správy incidentov – zahŕňa evidenciu, klasifikáciu, priraďovanie priorít, dokumentovanie a uzatváranie incidentov.
UC_00d – Nastavenie incident managementu	Systém aktivuje workflow pre správu incidentov a priradenia rolí.

4.5.2.3 UC_01 - Monitorovať bezpečnostné udalosti



Obrázok 13 : 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_04 - Upozorniť a eskalovať bezpečnostný incident.
9	Use Case končí – monitoring pokračuje ďalej.

ALT_01_01 – 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.

ALT_01_02 – 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.	
Naviazané funkčné požiadavky		
UC_01c – Indexácia a ukladanie údajov	Use case sa stará o uloženie normalizovaných bezpečnostných udalostí do úložiska a ich indexáciu pre rýchle vyhľadávanie a korelačné mechanizmy.	
UC_04 – Upozorniť a eskalovať bezpečnostný incident	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	
UC_01b – Normalizácia a obohacovanie údajov	Use case zabezpečuje normalizáciu logov do jednotného formátu a obohacovanie informáciami z CTI, asset databázy alebo užívateľských údajov.	
UC_01a - Zber logov	Zabezpečuje technický príjem logovacích dát zo systémov, aplikácií, zariadení a zdrojov do SIEM platformy. Je základom monitorovacieho procesu.	
FREQ_001 - Proces monitorovania bezpečnostných udalostí	Zabezpečiť proces monitorovania bezpečnostných udalostí – zabezpečuje zber a sledovanie logov, metrických údajov a alertov zo všetkých integrovaných systémov.	
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.	
ALT_01a_01 – Logy sa nedoručujú		Alternate
Krok	Aktivita	
1	SOCaaS nezaznamená žiadne dáta zo zdroja.	
2	Systém vytvorí „Missing logs“ upozornenie.	
3	Správca dostane notifikáciu.	
ALT_01a_02 – 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.	
Naviazané funkčné požiadavky		
FREQ_008 - Centralizácia logov	Riešenie musí zabezpečiť zber a centralizáciu logov zo systémov, sietí, koncových bodov a aplikácií.	
UC_01a - Zber logov	Zabezpečuje technický príjem logovacích dát zo systémov, aplikácií, zariadení a zdrojov do SIEM platformy. Je základom monitorovacieho procesu.	
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.

ALT_01a_01 – Neznámy typ logu	Alternate

Krok	Aktivita
1	Systém použije fallback normalizačný profil.

ALT_01a_02 – Chýba CTI feed	Alternate

Krok	Aktivita
1	Systém vykoná normalizáciu bez obohatenia a označí event ako „unenriched“.

Naviazané funkčné požiadavky	
FREQ_009 - Normalizácia a obohacovanie údajov	Riešenie musí zabezpečiť normalizáciu a obohacovanie údajov.
UC_01b – Normalizácia a obohacovanie údajov	Use case zabezpečuje normalizáciu logov do jednotného formátu a obohacovanie informáciami z CTI, asset databázy alebo užívateľských údajov.
Prípad použitia	UC_01c – Indexácia a ukladanie údajov

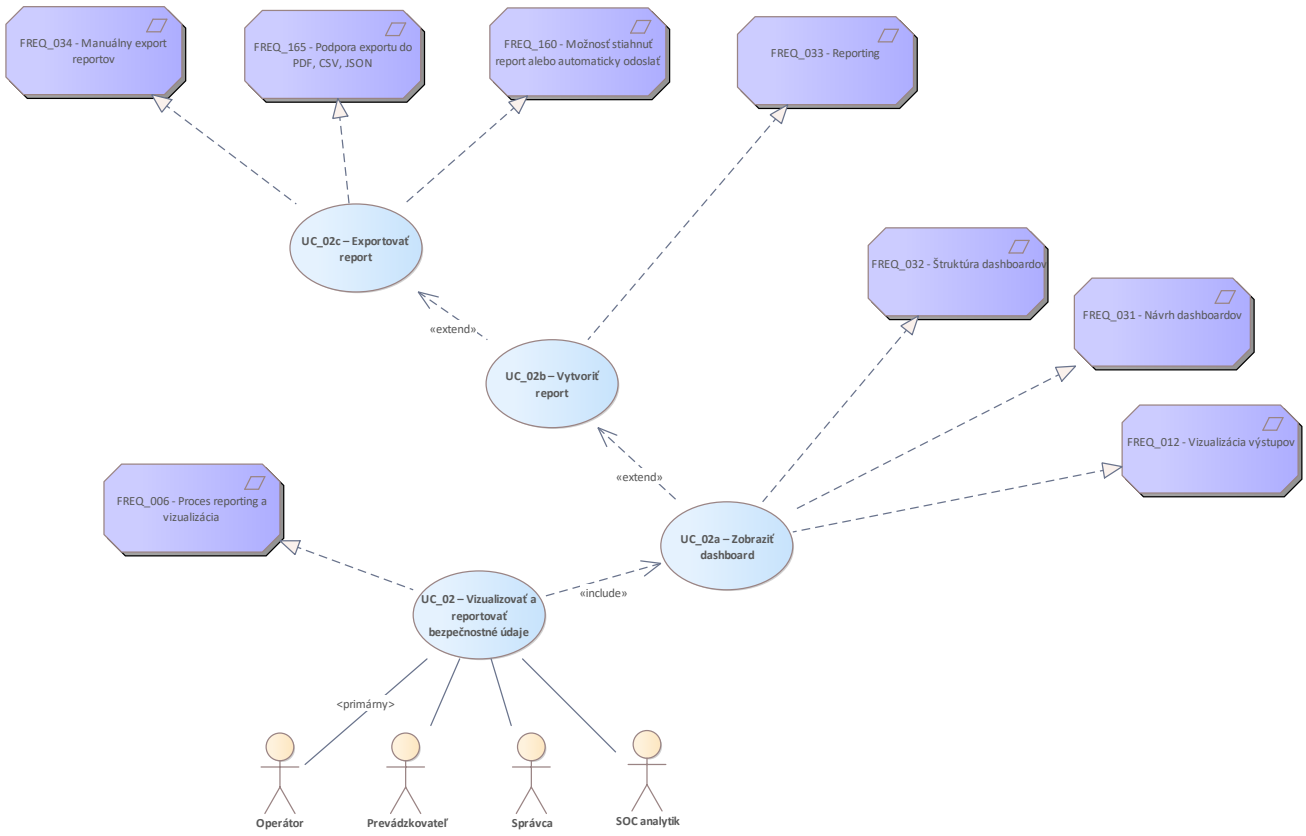
Cieľ	Use case sa stará o uloženie normalizovaných bezpečnostných udalostí do úložiska a ich indexáciu pre rýchle vyhľadávanie a korelačné mechanizmy.

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.	
ALT_01c_01 – Úložisko nedostupné		Alternate
Krok	Aktivita	
1	Systém uloží dáta do bufferu a vytvorí alert.	
ALT_01c_02 – Vyčerpanie úložného priestoru		Alternate
Krok	Aktivita	
1	Systém aktivuje cleanup alebo alertuje prevádzku.	
Naviazané funkčné požiadavky		
FREQ_010 - Ukladanie a indexovanie údajov	Riešenie musí zabezpečiť ukladanie, indexovanie a uchovávanie údajov.	

UC_01c – Indexácia a ukladanie údajov	Use case sa stará o uloženie normalizovaných bezpečnostných udalostí do úložiska a ich indexáciu pre rýchle vyhľadávanie a korelačné mechanizmy.

4.5.2.4 UC_02 - Vizualizovať a reportovať bezpečnostné údaje



Obrázok 14 : 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).

ALT_02_01 – Nedostupné dáta	Alternate

Krok	Aktivita
1	Dashboard vráti prázdny dataset.
2	Systém zobrazí varovanie.
3	Operátor a Prevádzkovateľ môže zmeniť filtračné kritériá.

ALT_02_02 – Chybné oprávnenia	Alternate

Krok	Aktivita

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

ALT_02_03 – Generovanie reportu zlyhalo	Alternate

K rok	Aktivita
1	Zobrazí chybové hlásenie.
2	Uloží chybu do audit logu.
3	Aktér (napr. Prevádzkovateľ) otvorí dashboard mimo jeho tenantu.

Naviazané funkčné požiadavky	
UC_02a – Zobraziť dashboard	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.
FREQ_006 - Proces reporting a vizualizácia	Zabezpečiť proces reporting a vizualizácia – zabezpečuje pravidelný výstup pre manažment, audítorov a SOC analytikov.
UC_02 – Vizualizovať a reportovať bezpečnostné údaje	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.
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_02a_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.	
ALT_02a_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.	
Naviazané funkčné požiadavky		
FREQ_012 - Vizualizácia výstupov	Riešenie musí zabezpečiť vizualizáciu výstupov	

FREQ_031 - Návrh dashboardov	Riešenie musí zabezpečiť návrh dashboardov. Pre udržanie prehľadnosti budú dashboardy v rámci SOCaaS rozdelené podľa funkčných vrstiev nasledovne: 1. Globálne prehľady (SOC Overview) Určené pre manažment a SLA reporting – zahŕňajú denné/měsíčné štatistiky incidentov, typy hrozieb, top 10 IP adries, krajiny pôvodu útokov, čas vyriešenia ticketov. 2. Alert monitoring dashboardy Zamerané na operatívny monitoring – zobrazujú nové alerty, rozdelenie podľa severity (Critical, High, Medium), časové trendy, a korelácie medzi viacerými zdrojmi. 3. Tematické dashboardy Pokrývajú špecifické oblasti: • EDR aktivity: zaznamenané súbory, procesy, pokusy o exekúciu škodlivého kódu. • Zraniteľnosti a skeny: výsledky z Greenbone alebo OpenSCAP. • Firewall a sieťové logy: prístupy, porty, odhalené scanningové aktivity. 4. Detailné analytické dashboardy – Slúžia pre L2 analytikov a threat hunting. Obsahujú heatmapy, časové rezy, distribúcie podľa hodín, krajín, ASN, výskyt IOC a podobne. 5. Ad-hoc a incident-specific dashboardy – Vznikajú počas vyšetrovania konkrétneho prípadu, kde si analytik zostaví vlastnú vizualizáciu na základe dát z Elasticsearch.
UC_02b – Vytvoriť report	Používateľ vytvorí jednorazový report alebo uloží reportovaciu šablónu založenú na dátach z dashboardov alebo udalostí.
FREQ_032 - Štruktúra dashboardov	Riešenie musí zabezpečiť štruktúru dashboardov ako sú dashboardy zostavené z jednotlivých panelov, ktoré môžu obsahovať grafy, tabuľky, heatmapy, distribučné histogramy, metriky alebo mapy. Každý dashboard v rámci SOCaaS je navrhnutý ako kompozícia týchto vizualizácií zameraná na konkrétny aspekt monitorovania alebo analýzy. Prehľad systémovej bezpečnosti Korelačné a incidentové dashboardy Vizualizácia sieťovej prevádzky a prístupov Monitorovanie autentifikácií a správania používateľov Integrovaný prehľad pre SOC analytika

UC_02a – Zobraziť dashboard	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.
UC_02a – Zobraziť dashboard	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.
UC_02a – Zobraziť dashboard	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.
UC_02a – Zobraziť dashboard	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.
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_02b_02 – Nedostupné dáta pre report	Alternate

K rok	Aktivita
1	Systém zobrazí hlásenie „Dáta pre vybrané obdobie nie sú dostupné“.
2	Operátor, Prevádkovateľ alebo Správca zvolí iné obdobie.

ALT_02b_01 – Nevalidný parameter reportu	Alternate

K rok	Aktivita
1	Systém zistí chýbajúci parameter (časové obdobie, zdroj dát...).
2	Zobrazí chybu a vyžiada doplnenie.

Naviazané funkčné požiadavky	
FREQ_033 - Reporting	Riešenie musí zabezpečiť reporting. Reporting v SOCaaS bude plniť niekoľko základných cieľov: • Prevádzkový prehľad – zobrazenie stavu systémov, počtu incidentov, aktivity agentov. • Bezpečnostný reporting – výstupy o detekovaných hrozbách, typoch útokov, trendoch. • Compliance reporting – reporty podľa regulatórnych požiadaviek (napr. GDPR, NIS2). • Manažérsky reporting – agregované štatistiky a ukazovatele pre vedenie organizácie. • Zákaznícky reporting – individuálne prehľady pre jednotlivých klientov multitenantného SOCaaS.
UC_02c – Exportovať report	Používateľ exportuje existujúci report do PDF, CSV, JSON alebo PNG a môže ho odoslať emailom alebo webhookom.
UC_02b – Vytvoriť report	Používateľ vytvorí jednorazový report alebo uloží reportovaciu šablónu založenú na dátach z dashboardov alebo udalostí.

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_02c_02 – Nedostatočné oprávnenia	Alternate

Krok	Aktivita
1	Systém zobrazí „Access Denied“.
2	Ponúkne požiadať o prístup.

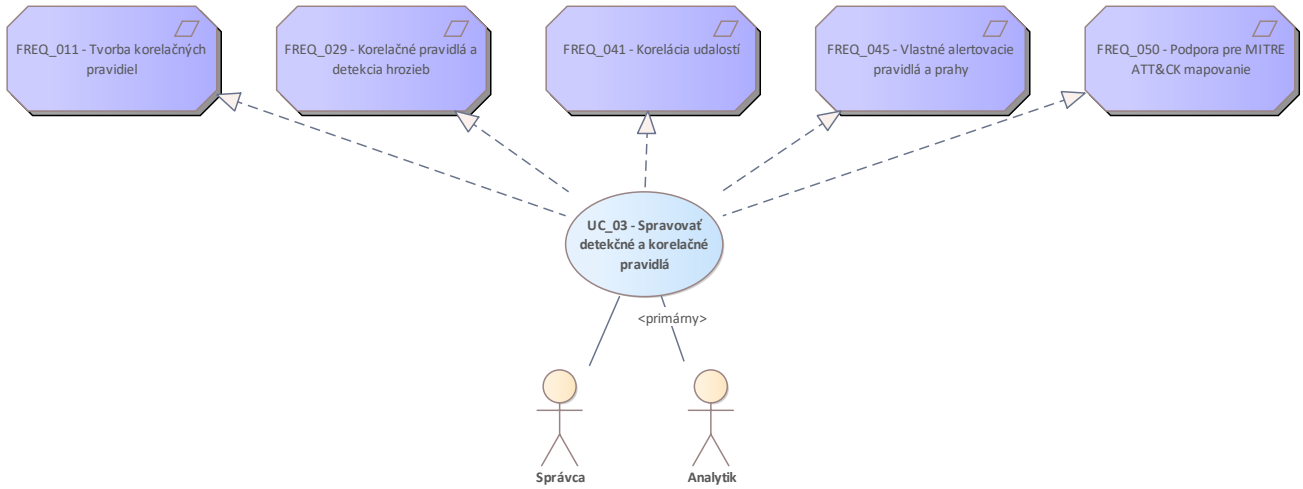
ALT_02c_01 – Export zlyhá (timeout, veľký dataset)	Alternate

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

Naviazané funkčné požiadavky	
FREQ_160 - Možnosť stiahnuť report alebo automaticky odoslať	Exportovanie reportov manuálne alebo ich plánovaná automatická distribúcia. Možnosť stiahnuť report alebo automaticky odoslať (e-mail, webhook)

FREQ_034 - Manuálny export reportov	Riešenie musí zabezpečiť manuálny export reportov. Reporty bude možné exportovať ako: • PDF dokument – generovaný snapshot aktuálneho dashboardu. • PNG obraz – statické obrázky jednotlivých vizualizácií. • CSV súbory – surové dáta z tabuliek a dátových polí. • JSON – pre automatizovanú analýzu a ďalšie spracovanie.
FREQ_165 - Podpora exportu do PDF, CSV, JSON	Možnosť exportovať reporty do rôznych bežných formátov. Podpora exportu do PDF, CSV, JSON
UC_02c – Exportovať report	Používateľ exportuje existujúci report do PDF, CSV, JSON alebo PNG a môže ho odoslať emailom alebo webhookom.

4.5.2.5 UC_03 - Spravovať detekčné a korelačné pravidlá



Obrázok 15 : 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_03_01 – Pravidlo sa testuje na historických dátach (debugging)	Alternate

K rok	Aktivita
1	Analytik použije nástroj na testovanie pravidiel voči historickým logom.
2	Výsledky sa zobrazia, pravidlo sa následne upraví alebo schváli.

ALT_03_02 – Pravidlo sa vytvorí cez no-code rozhranie	Alternate

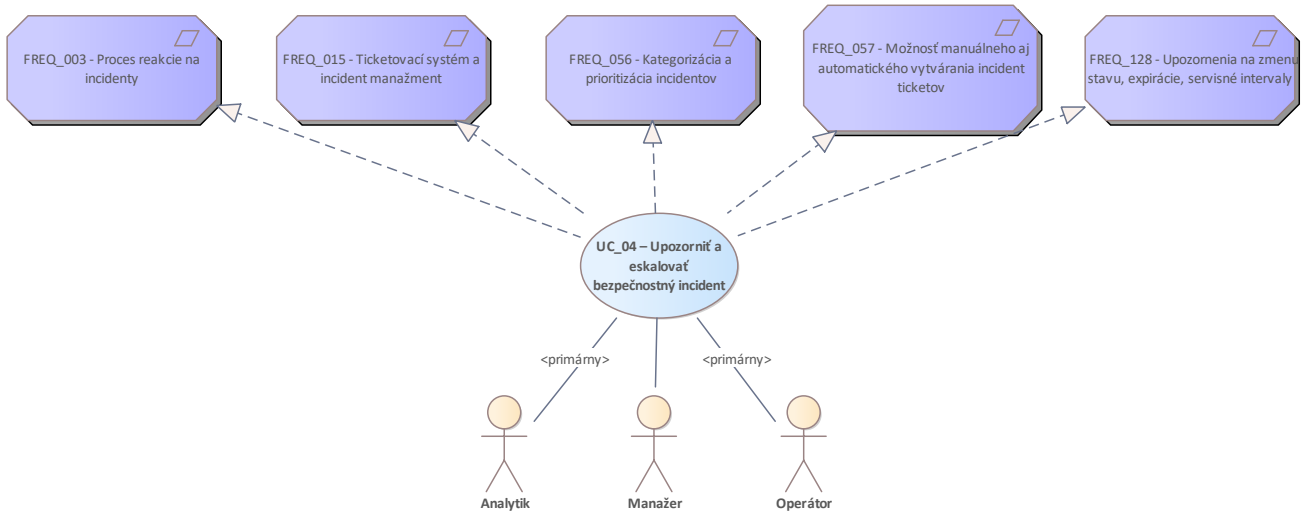
K rok	Aktivita
1	Analytik použije vizuálne rozhranie (drag & drop) na vytvorenie podmienok bez písania syntaxe.
2	Platforma automaticky vytvorí podkladový kód pravidla.

Naviazané funkčné požiadavky	
FREQ_041 - Korelácia udalostí	Možnosť prepájať súvisiace udalosti pomocou korelačných pravidiel. Korelácia udalostí (preddefinované a vlastné pravidlá)
FREQ_011 - Tvorba korelačných pravidiel	Riešenie musí zabezpečiť tvorbu korelačných pravidiel a alertov
FREQ_050 - Podpora pre MITRE ATT&CK mapovanie	Schopnosť mapovať detekcie na taktiky a techniky podľa MITRE ATT&CK. Podpora pre MITRE ATT&CK mapovanie

FREQ_029 - Korelačné pravidlá a detekcia hrozieb	Riešenie musí zabezpečiť korelačné pravidlá a detekcia hrozieb. • Alerty na základné IOC – porovnanie s databázou známych indikátorov (IP, URL, hash). • Anomálne správanie používateľov – napr. viacnásobné neúspešné prihlásenie v krátkom čase, login z nového geografického regiónu. • Neštandardné sieťové komunikácie – napr. DNS dotazy na dynamicky generované domény (DGA), odchýlky v čase a objeme dát. • Aktivity s administratívnymi právami – napr. pridanie používateľa do skupiny „Administrators“, zmeny ACL, spustenie netsh, powershell. • Reťazenie udalostí – korelácia medzi viacerými logmi v čase: napr. login ? súborový prenos ? spustenie škodlivého procesu. Tieto pravidlá budú spravované, kde možno: • sledovať detekčné alerty, • nastavovať prahové hodnoty (thresholds), • konfigurovať výnimky a ignorované hodnoty (exceptions), • exportovať a importovať pravidlá ako JSON objekty.
FREQ_045 - Vlastné alertovacie pravidlá a prahy	Schopnosť definovať vlastné pravidlá a podmienky pre generovanie alertov. Vlastné alertovacie pravidlá a prahy
UC_03 - Spravovať detekčné a korelačné pravidlá	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).
UC_03 - Spravovať detekčné a korelačné pravidlá	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).

UC_03 - Spravovať detekčné a korelačné pravidlá	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).

4.5.2.6 UC_04 – Upozorniť a eskalovať bezpečnostný incident



Obrázok 16 : 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

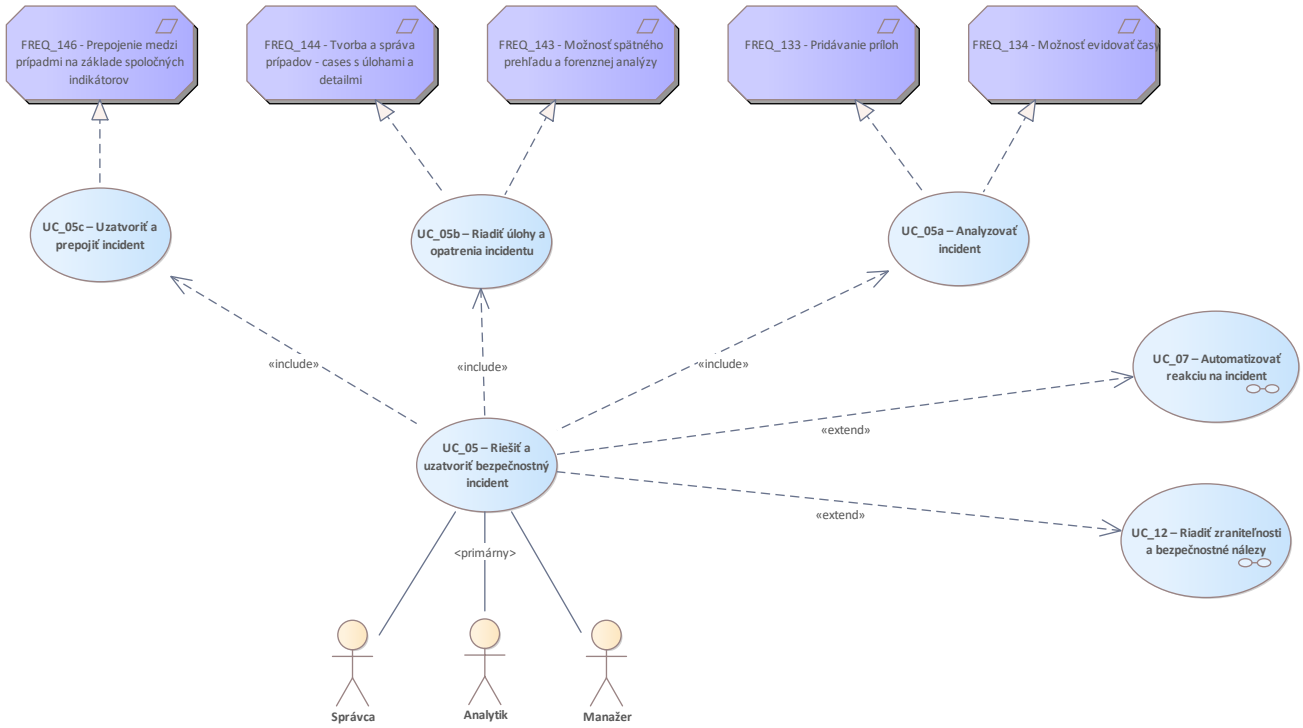
Krok	Aktivita
1	Vznik alebo zmena incidentu
2	Vyhodnotenie notifikačnej politiky
3	Výber primárnych príjemcov
4	Generovanie notifikačnej správy
5	Odoslanie notifikácie primárnymi kanálmi
6	Čakanie na potvrdenie (acknowledgement)
7	Potvrdenie incidentu Analytikom/Operátorom
8	Zastavenie ďalšej eskalácie
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).	
Naviazané funkčné požiadavky		
FREQ_003 - Proces reakcie na incidenty	Zabezpečiť proces reakcie na incidenty – definuje spôsob, akým tím reaguje na identifikované incidenty. Zahŕňa eskaláciu, priradenie zodpovednosti, vykonanie opatrení, ako aj komunikáciu so zasiahnutými stranami.	
FREQ_015 - Ticketovací systém a incident manažment	Riešenie musí zabezpečiť ticketovací a incident manažment systém poskytne workflow pre riešenie incidentov, eskaláciu, audit a sledovanie riešenia.	
FREQ_128 - Upozornenia na zmenu stavu, expirácie, servisné intervaly	Automatické notifikácie pri zmene stavu alebo potrebe servisného zásahu. Upozornenia na zmenu stavu, expirácie, servisné intervaly	
FREQ_057 - Možnosť manuálneho aj automatického vytvárania incident ticketov	Podpora ručného aj automatického vytvárania incident ticketov zo vstupných údajov. Možnosť manuálneho aj automatického vytvárania incident ticketov	
FREQ_056 - Kategorizácia a prioritizácia incidentov	Možnosť triediť incidenty podľa závažnosti, typu, kategórie a dôležitosti. Kategorizácia a prioritizácia incidentov	
UC_04 – Upozorniť a eskalovať bezpečnostný incident	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	

4.5.2.7 UC_05 – Riešiť a uzatvoriť bezpečnostný incident



Obrázok 17 : 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.
Naviazané funkčné požiadavky	
UC_05a – Analyzovať incident	Analytik detailne preskúma incident – pozrie si časovú os udalostí, logy, IOC, doplní dôkazy a vytvorí ucelený obraz o príčine a rozsahu incidentu.
UC_05b – Riadiť úlohy a opatrenia incidentu	Analytik a Správca vytvárajú, priraďujú a sledujú úlohy, ktoré predstavujú konkrétne nápravné alebo preventívne opatrenia súvisiace s incidentom.
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.
UC_05c – Uzatvoriť a prepojiť incident	Po vykonaní nápravných opatrení Analytik (príp. Manažér) rozhodne o finálnom stave incidentu, zdokumentuje záver a prepojí incident s inými súvisiacimi prípadmi.
UC_07 – Automatizovať reakciu na incident	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.
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.

Naviazané funkčné požiadavky	
FREQ_134 - Možnosť evidovať časy	Sledovanie a evidencia časových údajov pre celý životný cyklus ticketu. Možnosť evidovať časy (vytvorenie, aktualizácia, eskalácia, uzavretie)

FREQ_133 - Pridávanie príloh	Možnosť pridávať prílohy ako logy, snímky obrazovky a iné dôkazy. Pridávanie príloh (logy, dôkazy, screenshoty, výpisy z nástrojov)
UC_05a – Analyzovať incident	Analytik detailne preskúma incident – pozrie si časovú os udalostí, logy, IOC, doplní dôkazy a vytvorí ucelený obraz o príčine a rozsahu incidentu.
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

K rok	Aktivita
1	Správca aktualizuje termín a dôvod v úlohe; Analytik podľa potreby upraví prioritu incidentu alebo informuje Manažéra.

Naviazané funkčné požiadavky	
FREQ_143 - Možnosť spätného prehľadu a forenznej analýzy	Schopnosť spätne analyzovať priebeh a históriu incidentov. Možnosť spätného prehľadu a forenznej analýzy
FREQ_144 - Tvorba a správa prípadov - cases s úlohami a detailmi	Možnosť vytvárať incidenty ako prípady s úlohami, popisom a atribútmi. Tvorba a správa prípadov (cases) s úlohami a detailmi
UC_05b – Riadiť úlohy a opatrenia incidentu	Analytik a Správca vytvárajú, priraďujú a sledujú úlohy, ktoré predstavujú konkrétne nápravné alebo preventívne opatrenia súvisiace s incidentom.

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

K rok	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

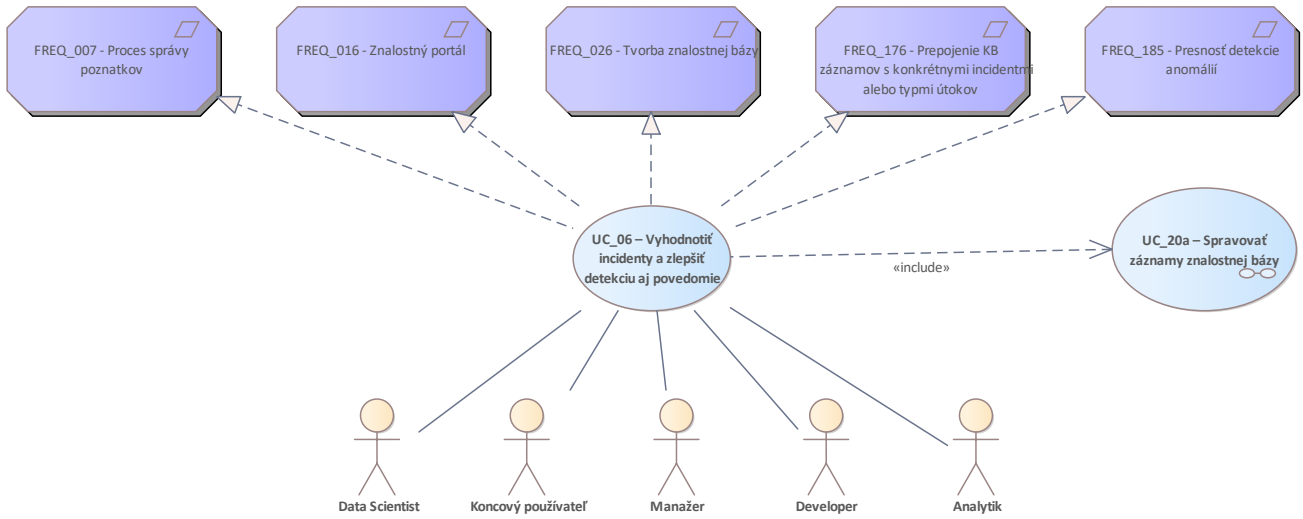
K rok	
	Aktivita
1	Počas kontroly Analytik zistí nové podozrivé udalosti; incident ponechá otvorený, vytvorí nové úlohy a vráti sa späť k UC_05a/05b.

ALT_02 – Incident je súčasťou rozsiahlej kampane	Alternate

K rok	
	Aktivita
1	Analytik identifikuje, že incident patrí do väčšej kampane; nastaví ho ako podriadený k nadradenému prípadu a upraví záverečné zhrnutie.

Naviazané funkčné požiadavky	
FREQ_146 - Prepojenie medzi prípadmi na základe spoločných indikátorov	Automatická alebo manuálna identifikácia súvisiacich incidentov. Prepojenie medzi prípadmi na základe spoločných indikátorov
UC_05c – Uzatvoriť a prepojiť incident	Po vykonaní nápravných opatrení Analytik (príp. Manažér) rozhodne o finálnom stave incidentu, zdokumentuje záver a prepojí incident s inými súvisiacimi prípadmi.

4.5.2.8 UC_06 – Vyhodnotiť incidenty a zlepšiť detekciu aj povedomie



Obrázok 18 : 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

K rok	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.

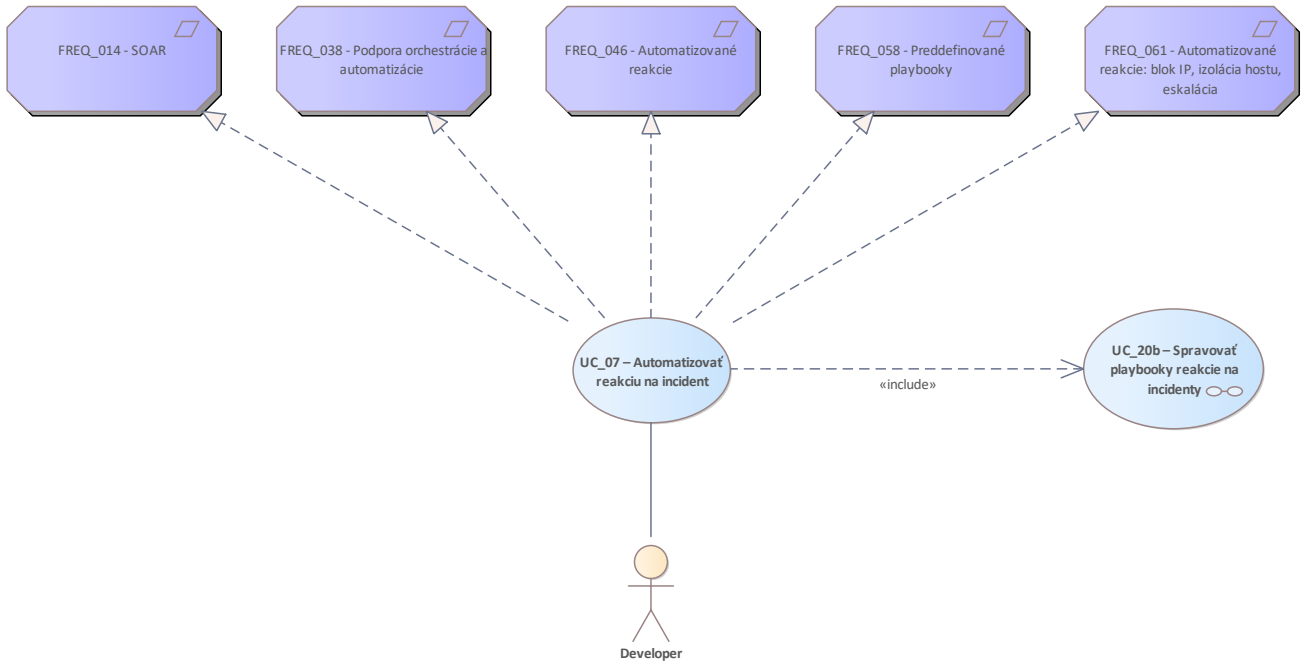
ALT_03 – Identifikovaná potreba cieleneho školenia zamestnancov	Alternate

K rok	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.

Naviazané funkčné požiadavky	
FREQ_026 - Tvorba znalostnej bázy	Riešenie musí zabezpečiť tvorbu znalostnej bázy. Každý incident alebo nový typ hrozby sa bude dokumentovať formou: • incident summary + lessons learned • zápis v znalostnom portáli • kategorizácia podľa MITRE ATT&CK a dátumov
UC_20a – Spravovať záznamy znalostnej bázy	UC_20a detailne rieši životný cyklus KB článkov – vytváranie, úpravy, štruktúru, tagovanie a väzbu na incidenty.
FREQ_007 - Proces správy poznatkov	Zabezpečiť proces správy poznatkov – zabezpečuje udržiavanie znalostnej bázy playbookov, dokumentácie a odporúčaných reakcií.
FREQ_176 - Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov	Možnosť prepojenia znalostných článkov s konkrétnymi typmi útokov a incidentmi v iných nástrojoch. Prepojenie KB záznamov s konkrétnymi incidentmi alebo typmi útokov

UC_20 – Spravovať znalostnú bázu a knižnicu playbookov	UC_20 rieši, aby mal SOC centrálne a riadene: znalostnú bázu (KB) – články, návody, lessons learned, postupy, knižnicu playbookov – manuálne aj automatizované reakčné postupy, proces schvaľovania, verzovania a publikovania tohto obsahu.
FREQ_185 - Presnosť detekcie anomálií	Riešenie musí zabezpečiť vyhodnotenie presnosti detekcie anomálií (Precision, Recall, F1). Ako presne algoritmus deteguje anomálie bez ohľadu na triedu. Vyhodnotenie celkovej presnosti pomocou metrík ako Precision, Recall, F1-score alebo AUC-ROC.
FREQ_016 - Znalostný portál	Riešenie musí zabezpečiť znalostný portál, ktoré bude podporovať reakčné procesy zdieľaním playbookov, interných politík a návodov.

4.5.2.9 UC_07 – Automatizovať reakciu na incident



Obrázok 19 : 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

K rok	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

K rok	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.

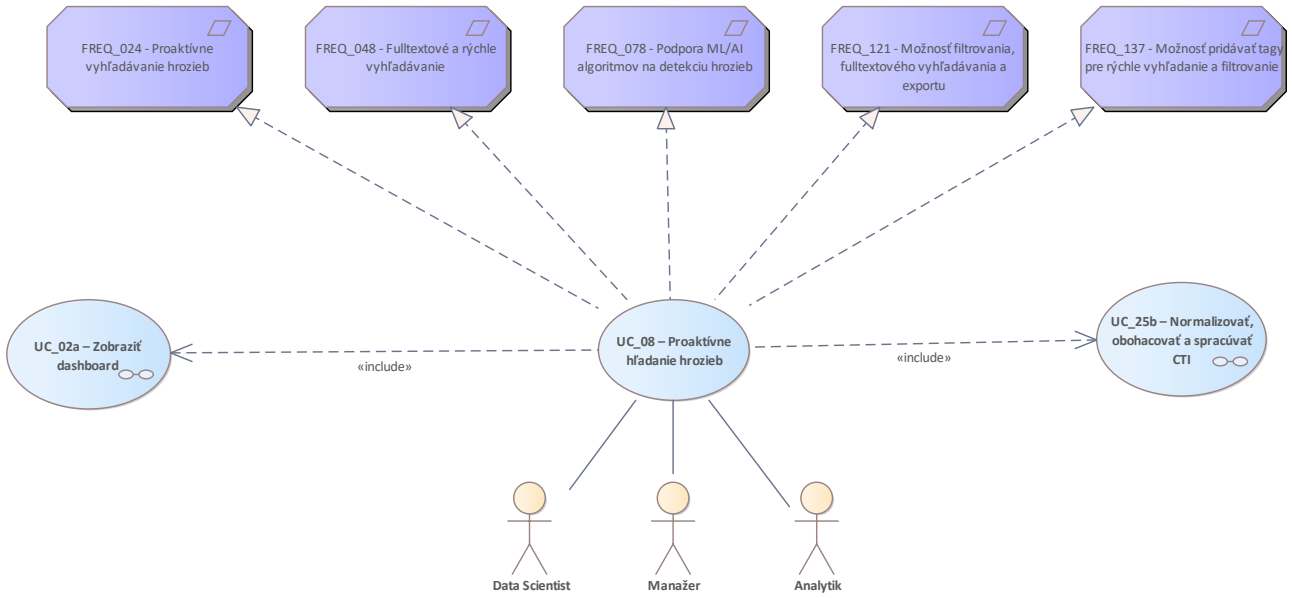
ALT_03 – Playbook sa spustí iba v simulačnom režime	Alternate

K rok	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.

Naviazané funkčné požiadavky	
FREQ_014 - SOAR	Riešenie musí zabezpečiť SOAR a bude slúžiť na automatizáciu reakčných scenárov, spracovanie alertov do prípadov a ich analýzu.

UC_20 – Spravovať znalostnú bázu a knižnicu playbookov	UC_20 rieši, aby mal SOC centrálne a riadene: znalostnú bázu (KB) – články, návody, lessons learned, postupy, knižnicu playbookov – manuálne aj automatizované reakčné postupy, proces schvaľovania, verzovania a publikovania tohto obsahu.
UC_20b – Spravovať playbooky reakcie na incidenty	UC_20b rieši návrh, úpravu a údržbu playbookov, ktoré SOC využíva pri automatizovanej alebo poloautomatizovanej reakcii (UC_07).
FREQ_046 - Automatizované reakcie	Možnosť spustiť reakciu (blokovanie, izolácia, notifikácia) automaticky. Automatizované reakcie (napr. blokovanie IP, integrácia SOAR)
FREQ_038 - Podpora orchestrácie a automatizácie	Riešenie má podporovať nástroje ako Heat (OpenStack orchestration), Terraform (infrastructure as code), Ansible (automatizácia) alebo Kubernetes Operator pre efektívnu správu a nasadzovanie komplexných infraštruktúrnych scénarov. Táto schopnosť umožní rýchle škálovanie služieb, automatizované rozbaľovanie prostredí, opakovateľné testovanie aj zotavenie pri výpadkoch. V prostredí SOC, kde sa často menia požiadavky a topológia siete, je orchestrácia nevyhnutná pre zabezpečenie flexibility, udržateľnosti a prevádzkovej efektivity.
FREQ_061 - Automatizované reakcie: blok IP, izolácia hostu, eskalácia	Schopnosť automaticky vykonať reakcie ako blokovanie, izolácia či upozornenie. Automatizované reakcie: blok IP, izolácia hostu, eskalácia
FREQ_058 - Preddefinované playbooky	Dostupnosť základných reakčných scenárov a automatizácií vopred pripravených v nástroji. Preddefinované playbooky
UC_07 – Automatizovať reakciu na incident	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.

4.5.2.10 UC_08 – Proaktívne hľadanie hrozieb



Obrázok 20 : 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

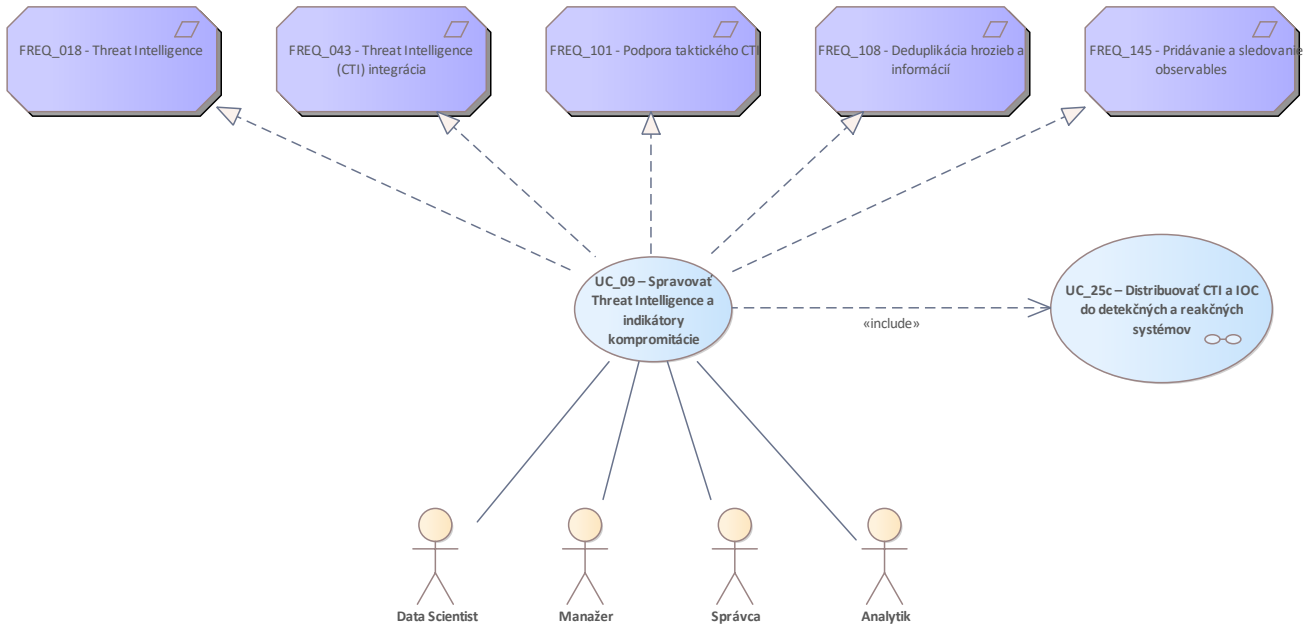
Krok	Aktivita
1	Hunting identifikuje viaceré súvisiace nálezy, ktoré naznačujú rozsiahlejší útok; Analytik vytvorí nadradený incident/kampaň, priradí k nemu všetky súvisiace nálezy a incidenty a informuje Manažéra o potrebe zvýšenej pozornosti.

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.
Naviazané funkčné požiadavky	
FREQ_121 - Možnosť filtrovania, fulltextového vyhľadávania a exportu	Efektívna práca s údajmi – vyhľadávanie podľa rôznych parametrov a exportovanie údajov. Možnosť filtrovania, fulltextového vyhľadávania a exportu
UC_02a – Zobraziť dashboard	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.
FREQ_024 - Proaktívne vyhľadávanie hrozieb	Riešenie musí zabezpečiť proaktívne vyhľadávanie hrozieb (Threat Hunting). Používajú sa pokročilé dotazy, často doplnené o: • CTI dáta • manuálnu analýzu v prípade podozrivých entít • výsledky sú dokumentované ako playbooky
UC_25c – Distribuovať CTI a IOC do detekčných a reakčných systémov	UC_25c rieši push CTI do zvyšku ekosystému: preposielanie IOC do SIEM/IDS/EDR/firewallov, využitie CTI v detekcii, playbookoch a incidentoch,
FREQ_137 - Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie	Použitie tagov na uľahčenie vyhľadávania a kategorizácie. Možnosť pridávať tagy pre rýchle vyhľadanie a filtrovanie
FREQ_078 - Podpora ML/AI algoritmov na detekciu hrozieb	Využitie algoritmov umelej inteligencie na detekciu anomálií a hrozieb. Podpora ML/AI algoritmov na detekciu hrozieb
FREQ_048 - Fulltextové a rýchle vyhľadávanie	Schopnosť vyhľadávať v logoch cez operátory, tagy, filtre. Fulltextové a rýchle vyhľadávanie
UC_25b – Normalizovať, obohacovať a spracúvať CTI	UC_25b rieši pipeline spracovania CTI: normalizáciu rôznych formátov na jednotný model, obohacovanie IOC a artefaktov z externých služieb, workflow pre automatické/poloautomatické spracovanie CTI.

4.5.2.11 UC_09 – Spravovať Threat Intelligence a indikátory kompromitácie



Obrázok 21 : 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.	

Naviazané funkčné požiadavky	
FREQ_101 - Podpora taktického CTI	Práca s indikátormi kompromitácie (IOC) a ich evidencia, spracovanie, distribúcia. Podpora taktického CTI (IOC, IP, hash, URL, domény)
FREQ_108 - Deduplikácia hrozieb a informácií	Odstraňovanie redundantných IOC a indikátorov. Deduplikácia hrozieb a informácií
FREQ_145 - Pridávanie a sledovanie observables	Možnosť sledovať IOC ako súčasť prípadu. Pridávanie a sledovanie observables (IP, domény, URL, hash hodnoty)
FREQ_018 - Threat Intelligence	Riešenie musí zabezpečiť Threat Intelligence. Procesy CTI (Cyber Threat Intelligence) umožňujú obohacovanie incidentov o známe hrozby, TTPs a IOCs
UC_25c – Distribuovať CTI a IOC do detekčných a reakčných systémov	UC_25c rieši push CTI do zvyšku ekosystému: preposielanie IOC do SIEM/IDS/EDR/firewallov, využitie CTI v detekcii, playbookoch a incidentoch,
FREQ_043 - Threat Intelligence (CTI) integrácia	Integrácia so zdrojmi hrozieb (IOC, TTP), automatické obohacovanie údajov. Threat Intelligence (CTI) integrácia

4.5.2.12 UC_10 – Riadiť súlad, metriky a manažérsky reporting

Obrázok 22 : 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

K rok	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

K rok	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).

Naviazané funkčné požiadavky	
UC_10a – Sledovať KPI a SLA bezpečnostných služieb	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.
FREQ_098 - Politiky súladu s normami	Možnosť hodnotiť zraniteľnosti vo vzťahu k štandardom. Politiky súladu s normami (napr. GDPR, ISO, CIS, BSI...)
FREQ_157 - Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov	Umožňuje získať úplný časový priebeh incidentu. Zabezpečenie spätnej dohľadateľnosti a analýzy incidentov
FREQ_020 - Reporting a spätná analýza	Riešenie musí zabezpečiť reporting a spätnú analýzu.
UC_10b – Tvorba a plánovanie manažérskych a compliance reportov	UC_10b rieši praktickú prácu s reportami pre manažment a audity: tvorbu, konfiguráciu obsahu, plánovanie pravidelných reportov a ich jednorazové generovanie.

UC_10c – Spravovať prístup, audit a archiváciu reportov	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.
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.

Naviazané funkčné požiadavky	
FREQ_073 - Zber systémových metrík, procesov a správania	Monitorovanie systémového správania a metrík ako CPU, pamäť, služby a procesy. Zber systémových metrík, procesov a správania
FREQ_159 - Vytvorenie základného prehľadu stavu bezpečnosti a incidentov	Možnosť vytvárať zhrnutia stavu bezpečnosti, incidentov a aktivity systému. Vytvorenie základného prehľadu stavu bezpečnosti a incidentov
UC_02a – Zobraziť dashboard	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.
UC_10a – Sledovať KPI a SLA bezpečnostných služieb	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.

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

K rok	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

K rok	Aktivita
1	Pri generovaní reportu systém upozorní, že niektoré časti budú neúplné; používateľ sa môže rozhodnúť report aj tak vygenerovať alebo upraviť rozsah.

Naviazané funkčné požiadavky	
FREQ_025 - Tvorba reportov a dashboardov	Riešenie musí zabezpečiť tvorbu reportov a dashboardov. Pre manažment a zákazníkov budú pravidelne generované: • prehľady incidentov • vizualizácie z metrík a ticketingu • exporty pre audit a SLA reporting
FREQ_162 - Plánovanie pravidelných reportov	Možnosť nastaviť generovanie reportov na základe harmonogramu. Plánovanie pravidelných (napr. denných, týždenných) reportov
UC_02a – Zobraziť dashboard	Používateľ otvorí dashboard, ktorý vizualizuje bezpečnostné udalosti, metriky a stavy systému v reálnom čase.
FREQ_161 - Možnosť výberu obsahu reportu – časové obdobie, typy incidentov	Možnosť filtrovať obsah reportu podľa času, typu alebo zdrojových údajov. Možnosť výberu obsahu reportu – časové obdobie, typy incidentov
UC_10b – Tvorba a plánovanie manažérskych a compliance reportov	UC_10b rieši praktickú prácu s reportami pre manažment a audity: tvorbu, konfiguráciu obsahu, plánovanie pravidelných reportov a ich jednorazové generovanie.

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.

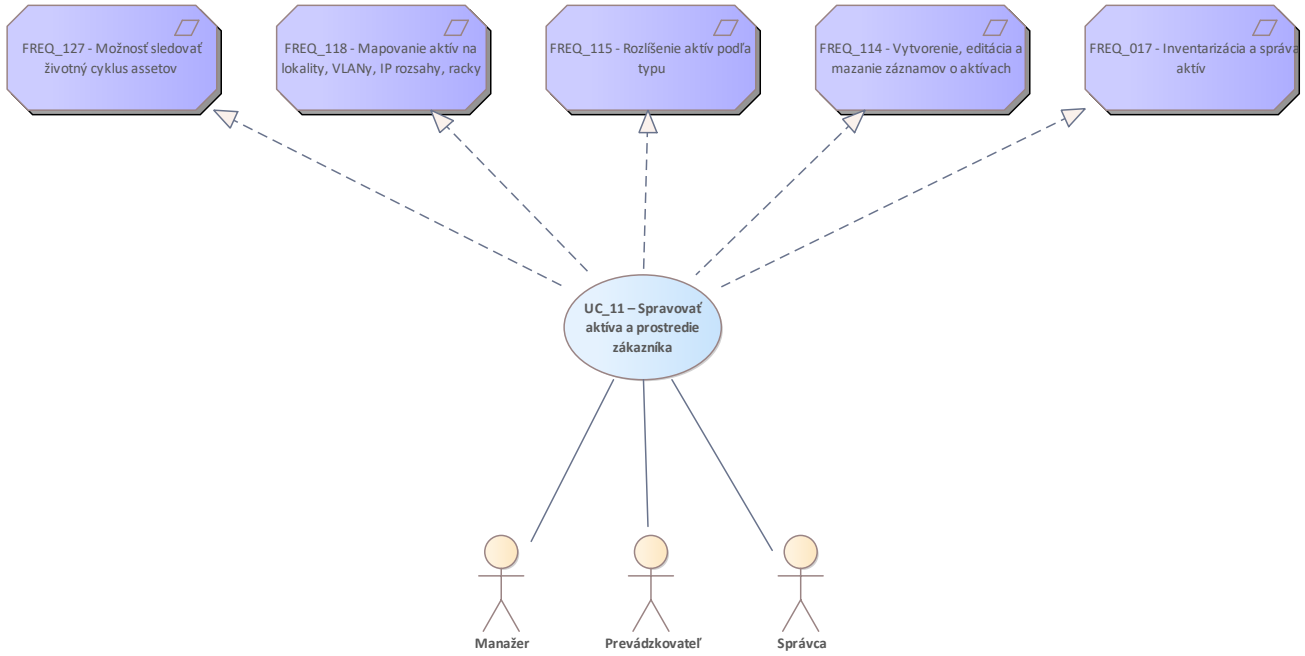
ALT_01 – Pokus o prístup k reportu bez oprávnenia	Alternate

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.

Naviazané funkčné požiadavky	
FREQ_066 - RBAC a audit trail	Riadenie prístupov na základe rolí a logovanie zmien v systéme. RBAC a audit trail
FREQ_170 - Možnosť archivácie vygenerovaných reportov	Možnosť uchovávať reporty pre spätnú analýzu a audit. Možnosť archivácie vygenerovaných reportov
FREQ_171 - Možnosť obmedziť prístup k reportom podľa rolí - RBAC	Prístup k reportom riadený rolami a oprávneniami. Možnosť obmedziť prístup k reportom podľa rolí (RBAC)

UC_10c – Spravovať prístup, audit a archiváciu reportov	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.

4.5.2.13 UC_11 – Spravovať aktíva a prostredie zákazníka



Obrázok 23 : 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).
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.

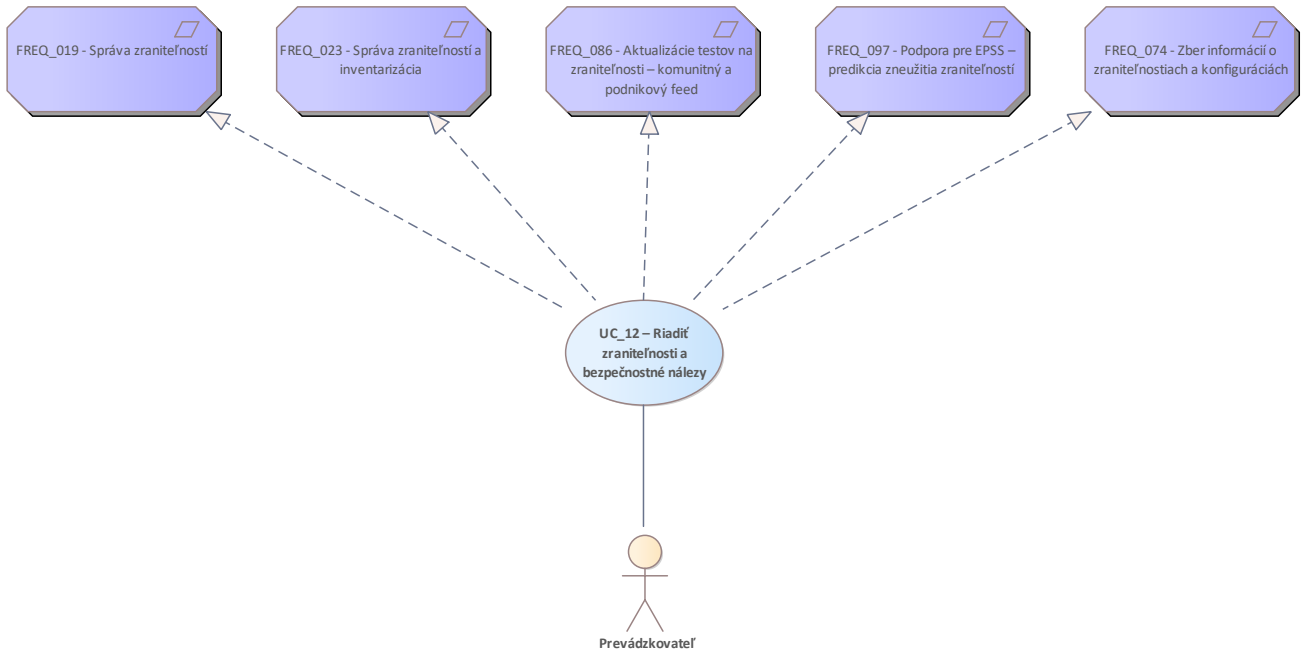
ALT_11_02 – Detegovaný duplikát aktíva		Alternate
Krok	Aktivita	
1	Pri ukladaní nového aktíva systém zistí, že už existuje záznam s rovnakými kľúčovými identifikátormi (napr. IP/hostname); používateľ dostane možnosť buď aktualizovať existujúci záznam, alebo vytvoriť samostatné aktívum s odôvodnením.	
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.	
Naviazané funkčné požiadavky		
FREQ_127 - Možnosť sledovať životný cyklus assetov	Správa jednotlivých fáz životnosti aktíva – od zaradenia po vyradenie. Možnosť sledovať životný cyklus assetov (nasadenie – vyradenie)	
FREQ_115 - Rozlíšenie aktív podľa typu	Možnosť rozlišovať typy aktív pre lepšiu organizáciu a správu. Rozlíšenie aktív podľa typu – hardvér, softvér, virtuálne, cloudové	
FREQ_118 - Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	Schopnosť mapovať fyzické a logické umiestnenie aktív v sieti. Mapovanie aktív na lokality, VLANy, IP rozsahy, racky	
FREQ_017 - Inventarizácia a správa aktív	Riešenie musí zabezpečiť inventarizáciu a správu aktív. Správa IT aktív je kľúčová pre mapovanie dopadov hrozieb.	
FREQ_114 - Vytvorenie, editácia a mazanie záznamov o aktívach	Schopnosť systému evidovať, upravovať a mazať informácie o jednotlivých aktívach. Vytvorenie, editácia a mazanie záznamov o aktívach	

4.5.2.14 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 24 : 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

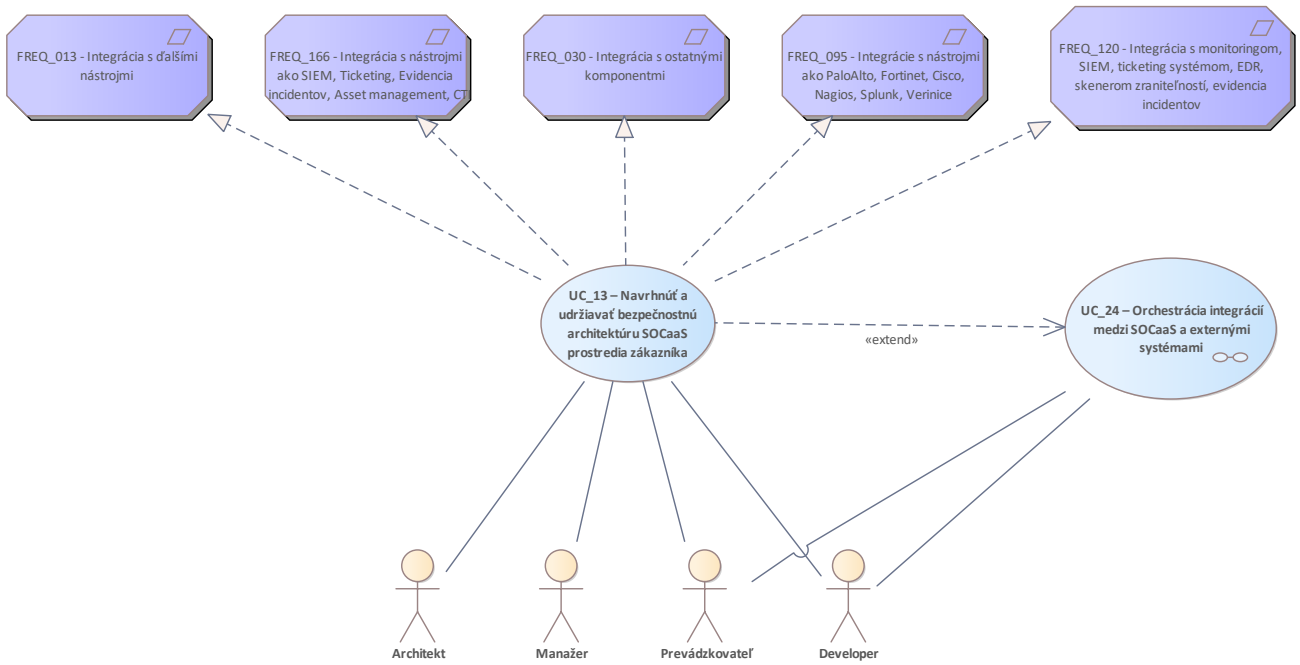
Krok	Aktivita
1	Správca zistí, že zraniteľnosť nie je možné opraviť (technické limity, vendor patch neexistuje, vysoký dopad na prevádzku); Manažér po diskusii rozhodne, či sa riziko dočasne akceptuje, alebo sa zavedú kompenzačné opatrenia (network segmentácia, zvýšený monitoring). Stav zraniteľnosti 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.	
Naviazané funkčné požiadavky		
FREQ_097 - Podpora pre EPSS – predikcia zneužitia zraniteľností	Využitie modelov pravdepodobnosti zneužitia zraniteľnosti. Podpora pre EPSS – predikcia zneužitia zraniteľností	
FREQ_023 - Správa zraniteľností a inventarizácia	Riešenie musí zabezpečiť správu zraniteľností a inventarizáciu. Pravidelné skeny majú byť prepojené s CMDB. • Assety sú aktualizované na základe detekcie • incidenty viazané na zraniteľnosti sú prepájané do manažment systému	
FREQ_086 - Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed	Frekvencia a rozsah aktualizácií detekčných vzorov. Aktualizácie testov na zraniteľnosti – komunitný a podnikový feed	
FREQ_019 - Správa zraniteľností	Riešenie musí zabezpečiť správu zraniteľností.	
FREQ_074 - Zber informácií o zraniteľnostiach a konfiguráciách	Získavanie informácií o zraniteľnostiach z konfiguračných údajov a porovnanie s databázami CVE. Zber informácií o zraniteľnostiach a konfiguráciách	
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.	

4.5.2.15 UC_13 – Navrhnúť a udržiavať bezpečnostnú architektúru SOCaaS prostredia zákazníka



Obrázok 25 : 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), a zoznam povinných log zdrojov a typov logov 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.
Výstupná podmienka	Je definovaný a zdokumentovaný zoznam povinných log zdrojov a typov logov pre onboarding zákazníka do SOCaaS (vrátane minimálne potrebných polí pre detekciu hrozieb).

Basic Path	Basic Path

Krok	Aktivita
1	Zber požiadaviek a vstupov

2	Analýza existujúcej architektúry zákazníka
3	Návrh dátových tokov a integračných patternov vrátane identifikácie povinných log zdrojov a typov logov
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

K rok	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

K rok	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

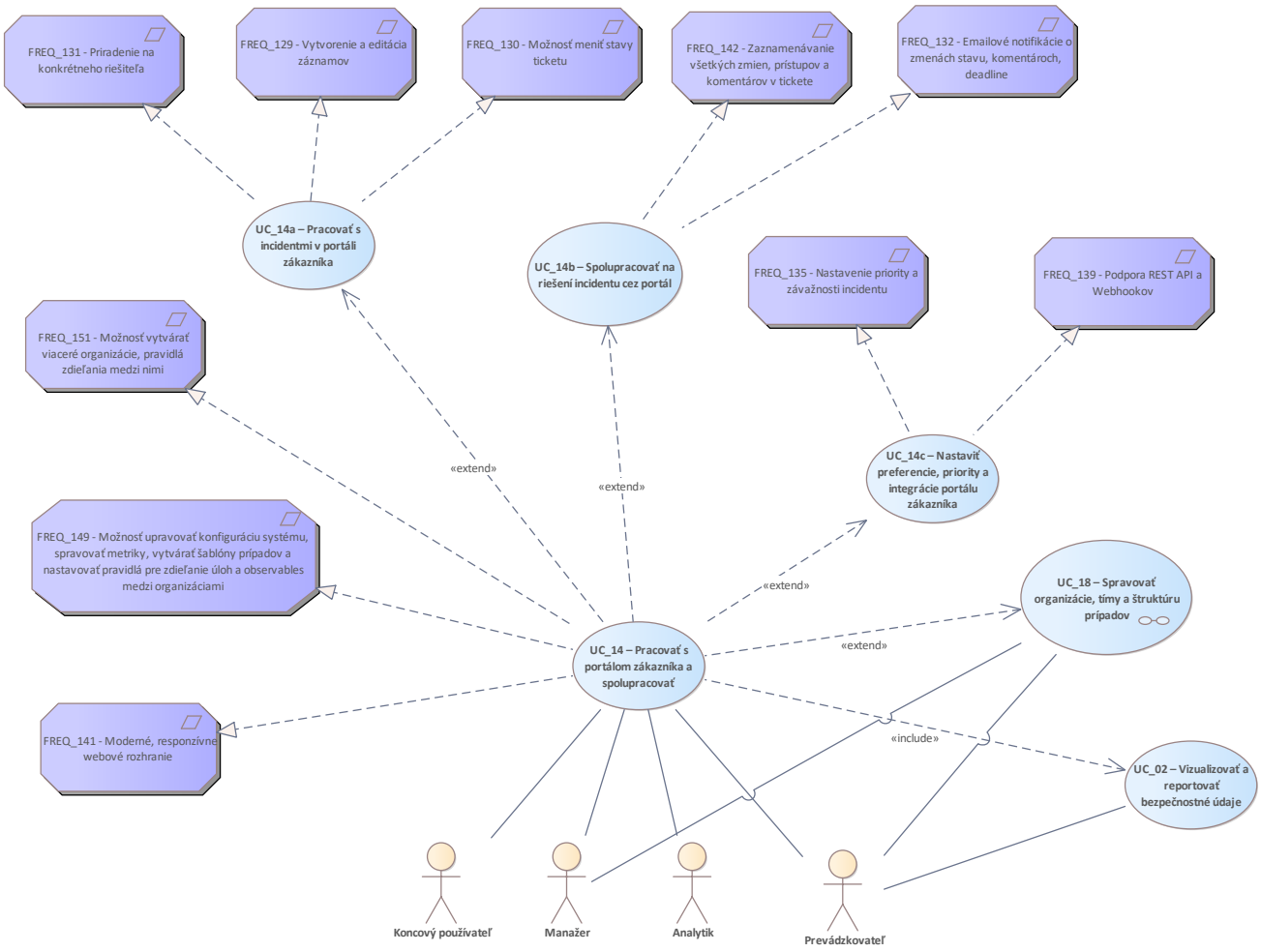
K rok	Aktivita
1	Pri posúdení návrhu sa zistí, že navrhované riešenie nevyhovuje (príliš veľké latencie, neakceptovateľné riziká, nedostatočné škálovanie); návrh sa vráti Architektovi na prepracovanie a až po zapracovaní pripomienok je znovu predložený na schválenie.

Naviazané funkčné požiadavky

FREQ_120 - Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov	Možnosť prepojenia s ďalšími nástrojmi SOC pre automatizáciu a zdieľanie údajov. Integrácia s monitoringom, SIEM, ticketing systémom, EDR, skenerom zraniteľností, evidencia incidentov
UC_24 – Orchestrácia integrácií medzi SOCaaS a externými systémami	UC_24 rieši technickú a procesnú orchestráciu integrácií medzi SOCaaS a ďalšími systémami: SIEM, SOAR, CTI, ticketing, komunikačné nástroje, firewall, EDR, API integrácie, webhooky, plug-iny a konektory, jednotné riadenie dátových tokov a akcií naprieč týmito systémami. Cieľom je, aby incident response, automatizácia (UC_07) a správa incidentov fungovali ako jeden prepojený ekosystém, nie ako izolované nástroje.
FREQ_013 - Integrácia s ďalšími nástrojmi	Riešenie musí zabezpečiť integráciu s ďalšími nástrojmi
FREQ_030 - Integrácia s ostatnými komponentmi	Riešenie musí zabezpečiť integráciu s ostatnými komponentmi. Prepojenie so zdrojmi dát Integrácia s nástrojmi incident managementu a SOAR Znalostná databáza a playbooky
FREQ_166 - Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI	Možnosť zbierať údaje z iných systémov a vytvárať prepojené reporty. Integrácia s nástrojmi ako SIEM, Ticketing, Evidencia incidentov, Asset management, CTI, ...
FREQ_095 - Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	Možnosť prepojenia s ďalšími bezpečnostnými a IT systémami. Integrácie s nástrojmi ako PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice

UC_13 – Navrhnúť a udržiavať bezpečnostnú architektúru SOCaaS prostredia zákazníka	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), a zoznam povinných log zdrojov a typov logov ktorý slúži ako podklad pre onboarding (UC_00), monitoring (UC_01), správu aktív (UC_11), zraniteľností (UC_12) a automatizáciu (UC_07).

4.5.2.16 UC_14 – Pracovať s portálom zákazníka a spolupracovať



Obrázok 26 : 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. „Manažér bezpečnosti“).
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).
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

K rok	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

K rok	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.

Naviazané funkčné požiadavky

UC_14a – Pracovať s incidentmi v portáli zákazníka	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).
FREQ_149 - Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami	Možnosť prispôsobiť platformu podľa potrieb organizácie. Možnosť upravovať konfiguráciu systému, spravovať metriky, vytvárať šablóny prípadov a nastavovať pravidlá pre zdieľanie úloh a observables medzi organizáciami?
UC_14c – Nastaviť preferencie, priority a integrácie portálu zákazníka	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).
FREQ_151 - Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi	Schopnosť prevádzkovať systém pre viac entít súčasne. Možnosť vytvárať viaceré organizácie, pravidlá zdieľania medzi nimi
UC_02 – Vizualizovať a reportovať bezpečnostné údaje	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.

UC_18 – Spravovať organizácie, tímy a štruktúru prípadov	UC_18 rieši administráciu organizácií/tenantov a spôsob, akým sa incidenty/prípady v rámci nich štruktúrujú: založenie a úprava organizácií / tímov, nastavenie kategórií, typov a vlastníkov prípadov, definovanie šablón incidentov a spôsobu ich zdieľania medzi tímami a externými partnermi. Stojí na UC_17 (používatelia a roly) a UC_14 (portál zákazníka) a dopĺňa ich o „organizačno-procesnú“ vrstvu.
UC_14b – Spolupracovať na riešení incidentu cez portál	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.
FREQ_141 - Moderné, responzívne webové rozhranie	Moderný a responzívny dizajn pre pohodlné používanie. Moderné, responzívne webové rozhranie
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“ , ...).
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.

Naviazané funkčné požiadavky	
FREQ_130 - Možnosť meniť stavy ticketu	Schopnosť prepínať medzi rôznymi stavmi ticketu počas jeho životného cyklu. Možnosť meniť stavy ticketu (napr. Nový, V riešení, Uzavretý, Odložený)
FREQ_131 - Priradenie na konkrétneho riešiteľa	Priradenie ticketov na konkrétnych riešiteľov vrátane eskalácie podľa úrovne. Priradenie na konkrétneho riešiteľa (L1 analytik, eskalácia L2/L3)
FREQ_129 - Vytvorenie a editácia záznamov	Základná funkcionalita ticketovacieho systému – vytváranie, editovanie a mazanie ticketov. Vytvorenie a editácia záznamov (ticketov)
UC_14a – Pracovať s incidentmi v portáli zákazníka	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).

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

Naviazané funkčné požiadavky	
FREQ_132 - Emailové notifikácie o zmenách stavu, komentároch, deadline	Automatické emailové notifikácie o zmene stavu, komentároch, deadline. Emailové notifikácie o zmenách stavu, komentároch, deadline
FREQ_142 - Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete	Zaznamenávanie všetkých akcií, zmien a komentárov v tickete. Zaznamenávanie všetkých zmien, prístupov a komentárov v tickete
UC_14b – Spolupracovať na riešení incidentu cez portál	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.

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

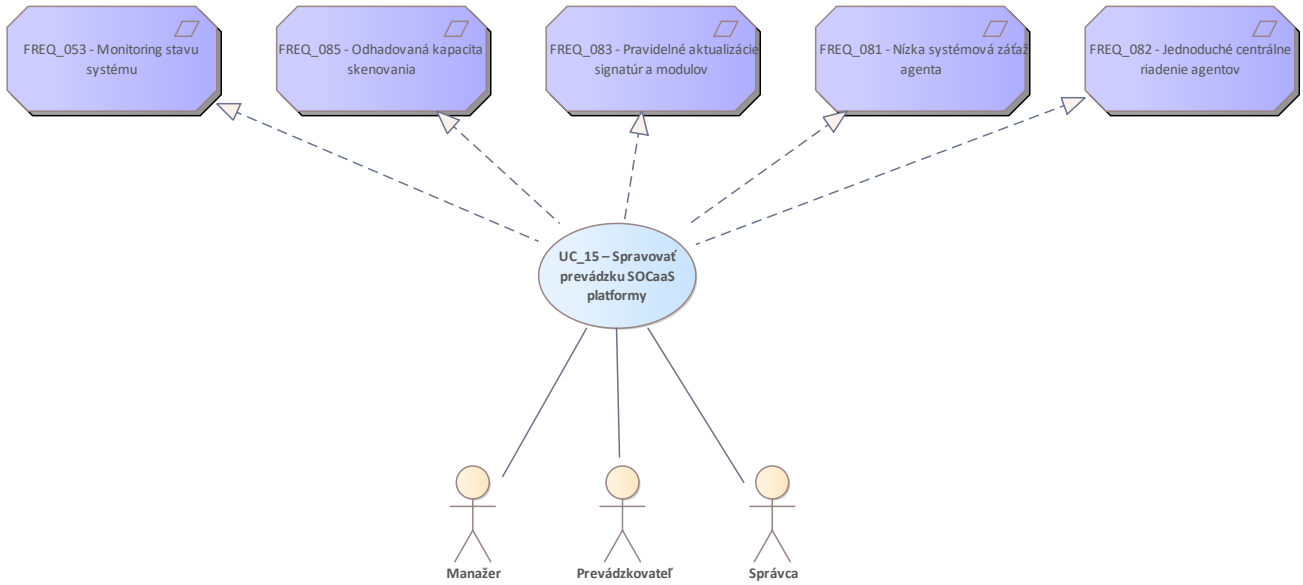
Krok	Aktivita
1	Manažér v portáli otvorí sekciu „Nastavenia organizácie“.
2	V časti „Incidenty“ nastaví mapovanie priorít/závažnosti (napr. ako sa majú SOC priority premietať do interných priorít zákazníka).
3	V časti „Integrácie“ zadá koncové URL pre Webhooky alebo API tokeny pre napojenie na interný 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.
Naviazané funkčné požiadavky	
FREQ_135 - Nastavenie priority a závažnosti incidentu	Nastavenie úrovne priority a závažnosti ticketu pre lepšie plánovanie. Nastavenie priority a závažnosti incidentu
FREQ_139 - Podpora REST API a Webhookov	Podpora pre rozhrania REST API a Webhooky na komunikáciu s inými systémami. Podpora REST API a Webhookov
UC_14c – Nastaviť preferencie, priority a integrácie portálu zákazníka	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).

4.5.2.17 UC_15 – Spravovať prevádzku SOCaaS platformy



Obrázok 27 : 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

rok	K	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.

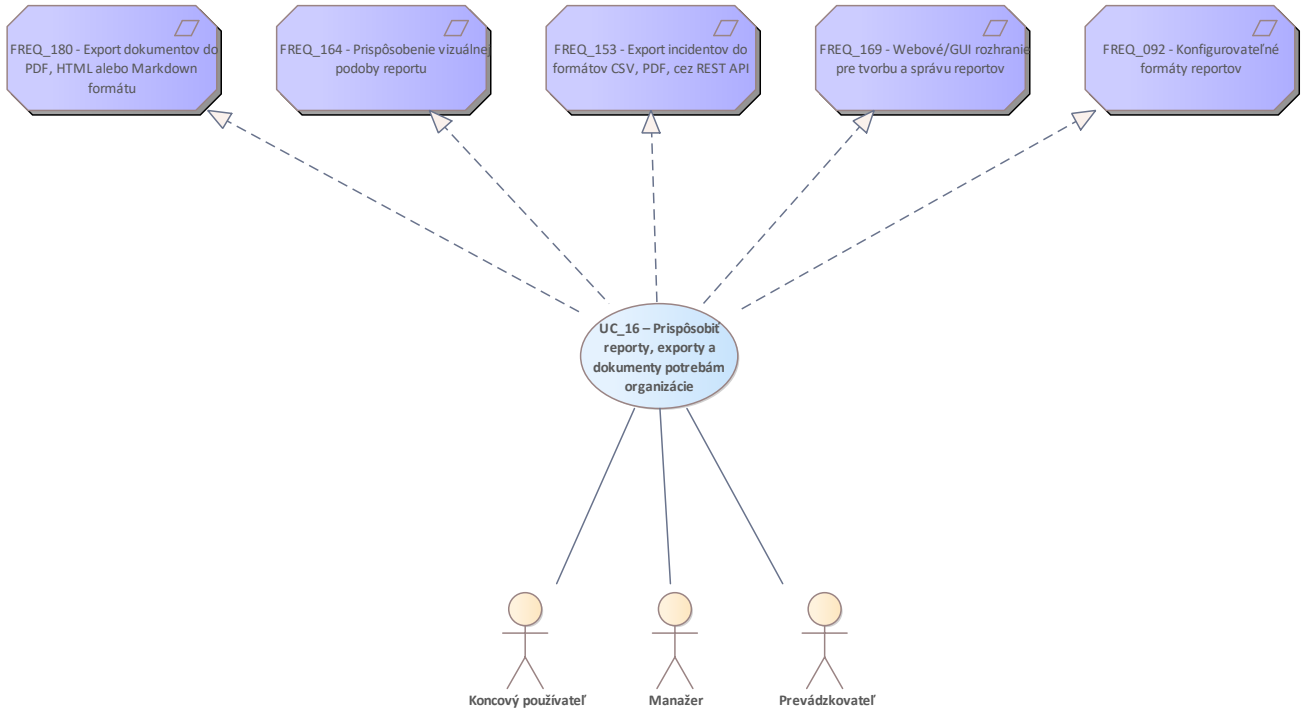
ALT_15_02 – Zlyhanie aktualizácie signatúr alebo modulov	Alternate

rok	K	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.

Naviazané funkčné požiadavky	
FREQ_081 - Nízka systémová záťaž agenta	Agent má nízky vplyv na výkon systému, čo umožňuje nasadenie vo veľkej škále. Nízka systémová záťaž agenta
FREQ_083 - Pravidelné aktualizácie signatúr a modulov	Pravidelné aktualizácie databáz hrozieb, signatúr a detekčných pravidiel. Pravidelné aktualizácie signatúr a modulov
FREQ_082 - Jednoduché centrálne riadenie agentov	Centrálna konzola na správu, konfiguráciu a dohľad nad všetkými agentmi. Jednoduché centrálne riadenie agentov

FREQ_053 - Monitoring stavu systému	Sledovanie výkonu, dostupnosti a funkčnosti systému. Monitoring stavu systému (healthcheck)
FREQ_085 - Odhadovaná kapacita skenovania	Schopnosť nástroja efektívne skenovať veľké siete. Odhadovaná kapacita skenovania (napríklad min. 100 IP/24h)

4.5.2.18 UC_16 – Prispôsobiť reporty, exporty a dokumenty potrebám organizácie



Obrázok 28 : 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

K rok	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

K rok	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.

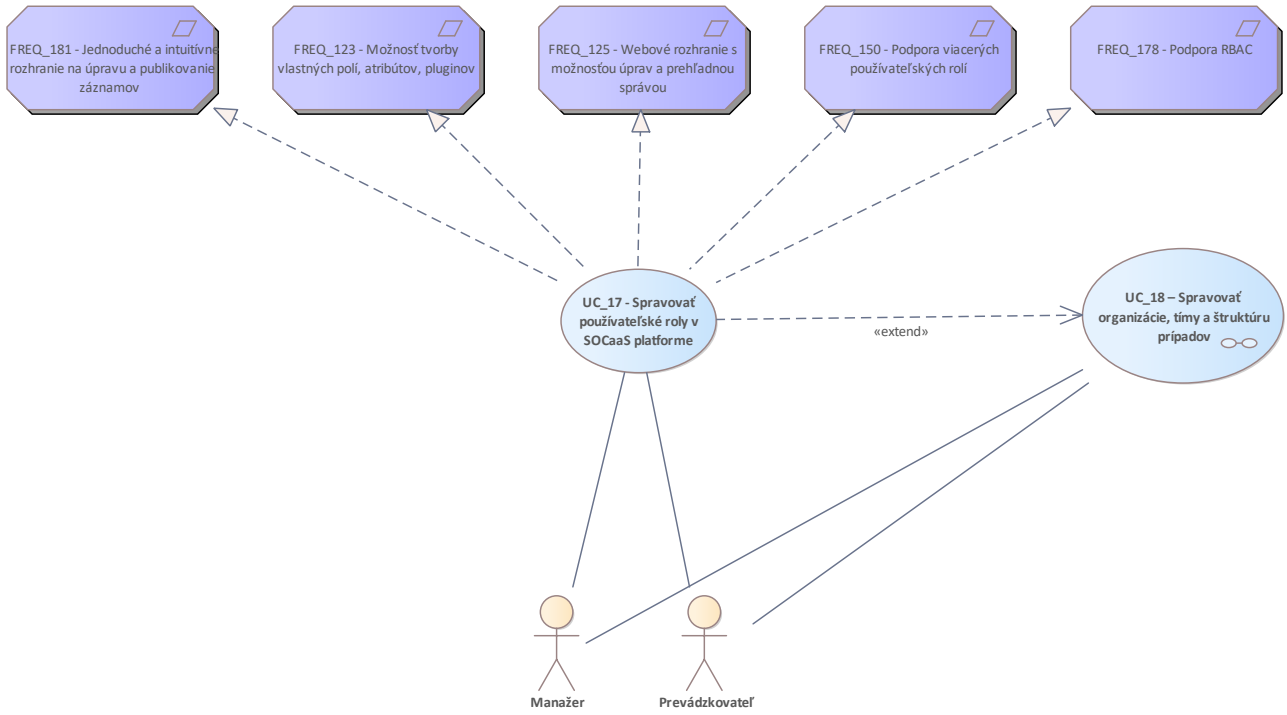
ALT_16_03 – Zmena firemnej identity	Alternate

K rok	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.

Naviazané funkčné požiadavky	
FREQ_180 - Export dokumentov do PDF, HTML alebo Markdown formátu	Možnosť exportu dokumentov na offline použitie alebo publikovanie. Export dokumentov do PDF, HTML alebo Markdown formátu
FREQ_092 - Konfigurovateľné formáty reportov	Flexibilita výstupov pre ďalšie spracovanie. Konfigurovateľné formáty reportov (napr. CSV, XML, PDF)
FREQ_169 - Webové/GUI rozhranie pre tvorbu a správu reportov	Používateľsky prívetivé rozhranie pre návrh, úpravu a správu reportov. Webové/GUI rozhranie pre tvorbu a správu reportov

FREQ_153 - Export incidentov do formátov CSV, PDF, cez REST API	Export dát pre dokumentáciu alebo reportovanie. Export incidentov do formátov CSV, PDF, cez REST API
FREQ_164 - Prispôsobenie vizuálnej podoby reportu	Možnosť upraviť vzhľad reportu podľa firemnej identity. Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie)

4.5.2.19 UC_17 – Spravovať používateľov a roly v SOCaaS platforme



Obrázok 29 : UC_17 – Spravovať používateľov a roly v SOCaaS platforme

Prípad použitia	UC_17 - Spravovať používateľské roly v SOCaaS platforme

Cieľ	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.

Vstupná podmienka	SOCaaS platforma beží a má prístupné administrátorské webové rozhranie.
Vstupná podmienka	Aktuálne prihlásený používateľ má administrátorské oprávnenia na správu účtov a rolí.
Výstupná podmienka	Vytvorené, upravené alebo deaktivované používateľské účty sú uložené v systéme.
Výstupná podmienka	Používateľom sú priradené vhodné roly podľa RBAC modelu.
Výstupná podmienka	Prípadné vlastné atribúty/metadata sú nastavené a použiteľné v ďalších častiach systému.

Basic Path	Basic Path

Krok	Aktivita
1	Prevádzkovateľ sa prihlási do administrátorského webového rozhrania.
2	Otvorí sekciu „Používatelia a roly“.
3	Vyberie, či chce vytvoriť nového používateľa alebo upraviť existujúci účet.
4	Pri vytváraní účtu zadá základné údaje (meno, kontakty, identifikátor účtu) a vyberie jednu alebo viac používateľských rolí (napr. SOC analytik, Manažér, Zákazník, Auditor).
5	Podľa potreby doplní vlastné polia/atribúty (napr. príslušnosť k organizácii, úroveň oprávnenia, špeciálne tagy).
6	Systém uloží zmeny a zobrazí používateľa v prehľadnom zozname; rozhranie umožní filtrovanie a vyhľadávanie podľa mena, roly a ďalších atribútov.

7	Prevádzkovateľ môže účet deaktivovať alebo zmeniť roly, ak sa zmení zodpovednosť používateľa.

ALT_17_01 – Pokus o zmenu, na ktorú používateľ nemá oprávnenie	Alternate

K rok	Aktivita
1	Používateľ bez administrátorských práv sa pokúsi upraviť účty alebo roly; systém zmenu odmietne a zobrazí informáciu, že nemá dostatočné oprávnenie.

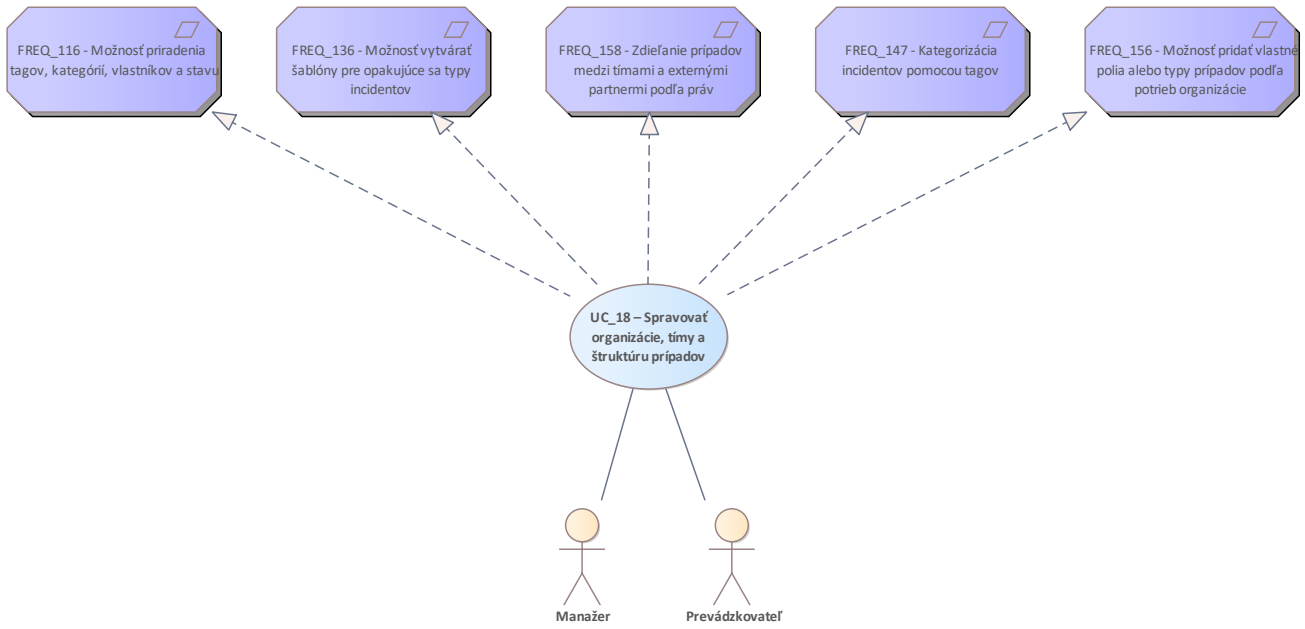
ALT_17_02 – Neplatná kombinácia rolí	Alternate

K rok	Aktivita
1	Pri ukladaní účtu systém zistí, že zvolená kombinácia rolí je v rozpore s RBAC politikou (napr. konflikt záujmov); administrátor dostane informáciu a musí upraviť zvolené roly.

Naviazané funkčné požiadavky	
FREQ_092 - Konfigurovateľné formáty reportov	Flexibilita výstupov pre ďalšie spracovanie. Konfigurovateľné formáty reportov (napr. CSV, XML, PDF)
FREQ_125 - Webové rozhranie s možnosťou úprav a prehľadnou správou	Používateľsky prívetivé GUI pre správu assetov. Webové rozhranie s možnosťou úprav a prehľadnou správou
FREQ_150 - Podpora viacerých používateľských rolí	Podpora RBAC pre rôzne roly. Podpora viacerých používateľských rolí – minimálne analytik a administrátor
FREQ_153 - Export incidentov do formátov CSV, PDF, cez REST API	Export dát pre dokumentáciu alebo reportovanie. Export incidentov do formátov CSV, PDF, cez REST API
FREQ_123 - Možnosť tvorby vlastných polí, atribútov, pluginov	Užívateľská flexibilita pre prispôsobenie systému vlastným potrebám. Možnosť tvorby vlastných polí, atribútov, pluginov (napr. NetBox/Django)
FREQ_169 - Webové/GUI rozhranie pre tvorbu a správu reportov	Používateľsky prívetivé rozhranie pre návrh, úpravu a správu reportov. Webové/GUI rozhranie pre tvorbu a správu reportov
FREQ_178 - Podpora RBAC	Riadenie prístupu podľa používateľských rolí. Podpora RBAC – rôzne úrovne prístupu pre čítanie, editáciu, schvaľovanie
FREQ_164 - Prispôsobenie vizuálnej podoby reportu	Možnosť upraviť vzhľad reportu podľa firemnej identity. Prispôsobenie vizuálnej podoby reportu (logo, farby, záhlavie)

FREQ_180 - Export dokumentov do PDF, HTML alebo Markdown formátu	Možnosť exportu dokumentov na offline použitie alebo publikovanie. Export dokumentov do PDF, HTML alebo Markdown formátu
FREQ_181 - Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov	Používateľsky prívetivé GUI pre správu znalostí. Jednoduché a intuitívne rozhranie na úpravu a publikovanie záznamov
UC_18 – Spravovať organizácie, tímy a štruktúru prípadov	UC_18 rieši administráciu organizácií/tenantov a spôsob, akým sa incidenty/prípady v rámci nich štruktúrujú: založenie a úprava organizácií / tímov, nastavenie kategórií, typov a vlastníkov prípadov, definovanie šablón incidentov a spôsobu ich zdieľania medzi tímami a externými partnermi. Stojí na UC_17 (používatelia a roly) a UC_14 (portál zákazníka) a dopĺňa ich o „organizačno-procesnú“ vrstvu.

4.5.2.20 UC_18 – Spravovať organizácie, tímy a štruktúru prípadov



Obrázok 30 : UC_18 – Spravovať organizácie, tímy a štruktúru prípadov

Prípad použitia	UC_18 – Spravovať organizácie, tímy a štruktúru prípadov
Cieľ	UC_18 rieši administráciu organizácií/tenantov a spôsob, akým sa incidenty/prípady v rámci nich štruktúrujú: založenie a úprava organizácií / tímov, nastavenie kategórií, typov a vlastníkov prípadov, definovanie šablón incidentov a spôsobu ich zdieľania medzi tímami a externými partnermi. Stojí na UC_17 (používatelia a roly) a UC_14 (portál zákazníka) a dopĺňa ich o „organizačno-procesnú“ vrstvu.

Vstupná podmienka	Používateľ je prihlásený a má oprávnenia na správu organizácií/štruktúry prípadov.
Vstupná podmienka	SOCaaS má vytvorených aspoň pár používateľov (UC_17) a minimálne jednu organizáciu/tenant (UC_14).
Výstupná podmienka	Organizácie/ tímy majú nastavenú štruktúru prípadov (typy, kategórie, vlastníci).
Výstupná podmienka	Sú definované šablóny pre opakujúce sa incidenty a spôsob ich zdieľania medzi tímami/partnermi.
Výstupná podmienka	Incidenty je možné jednoznačne priradiť k organizácii, tímu, kategórii a vlastníkovi.

Basic Path		Basic Path
Krok	Aktivita	
1	Manažér alebo Prevádzkovateľ otvorí v administrácii sekciu „Organizácie a prípady“.	
2	Vyberie existujúcu organizáciu (tenant) alebo vytvorí novú a priradí k nej tímy (napr. „SOC L1“, „SOC L2“, „IT zákazníka“).	
3	Pre organizáciu nastaví typy prípadov/incidentov (napr. „Phishing“, „Malware“, „Politika“, „Vuln nález“) a základné kategórie.	

4	Pre jednotlivé typy incidentov vytvorí šablóny – predvyplnené polia, odporúčané položky, požadované informácie.
5	K typom incidentov a šablónam priradí vlastníkov, tagy a kategórie (napr. „kritické“, „regulačné“, „interné“), aby bolo možné nad nimi filtrovať a reportovať.
6	Nastaví, ktoré tímy a prípadne externí partneri môžu dané prípady vidieť a upravovať (zdieľanie medzi tímami podľa práv).Nastaví, ktoré tímy a prípadne externí partneri môžu dané prípady vidieť a upravovať (zdieľanie medzi tímami podľa práv).
7	Systém uloží štruktúru organizácie, šablóny a pravidlá zdieľania; nové incidenty sa vytvárajú podľa týchto nastavení.

ALT_18_01 – Vytvorenie vlastného typu prípadu pre konkrétnu organizáciu	Alternate

K rok	Aktivita
1	Organizácia má špecifický typ prípadu (napr. „Compliance nález“), ktorý neexistuje v globálnej schéme; Manažér pridá nový typ prípadu len pre túto organizáciu a vytvorí k nemu vlastnú šablónu.

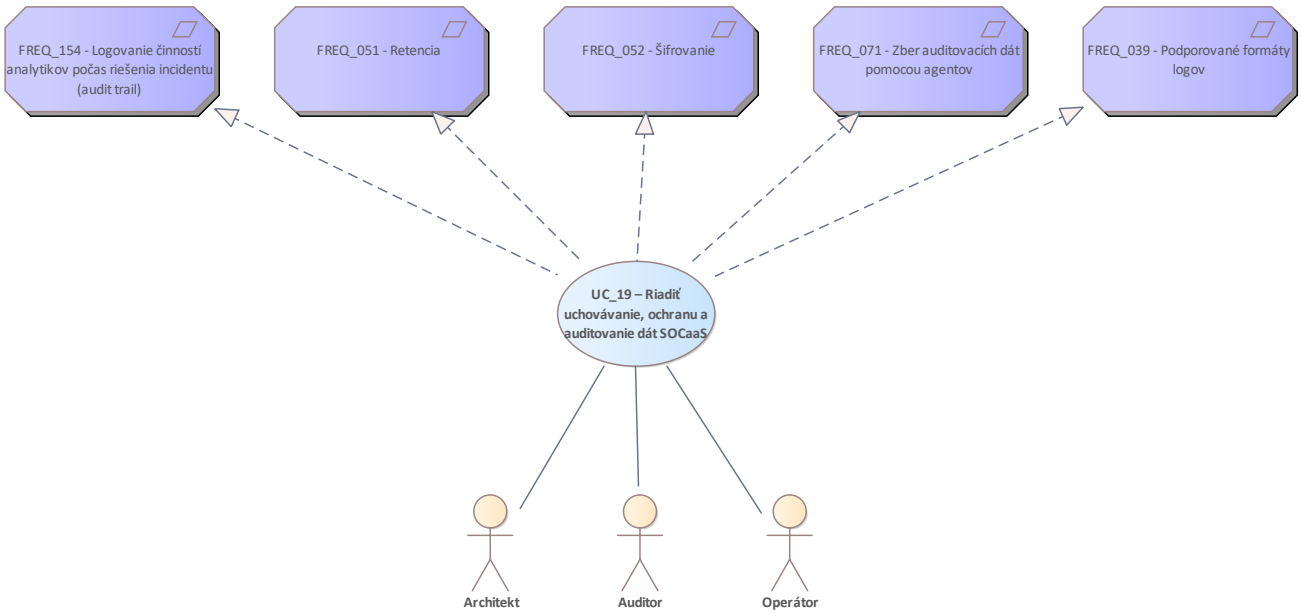
ALT_18_02 – Obmedzenie zdieľania prípadov s externým partnerom	Alternate

K rok	Aktivita
1	Pôvodne sú prípady zdieľané s externým dodávateľom; Manažér rozhodne, že niektoré kategórie (napr. HR incidenty) sa zdieľať nebudú a upraví pravidlá zdieľania tak, aby tieto prípady boli prístupné len interným tímom.

Naviazané funkčné požiadavky	
FREQ_156 - Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie	Možnosť rozšíriť schému incidentu. Možnosť pridať vlastné polia alebo typy prípadov podľa potrieb organizácie
FREQ_116 - Možnosť priradenia tagov, kategórií, vlastníkov a stavu	Pridávanie metadát pre efektívne triedenie a správu aktív. Možnosť priradenia tagov, kategórií, vlastníkov a stavu (napr. aktívne, v údržbe, vyradené)
FREQ_147 - Kategorizácia incidentov pomocou tagov	Možnosť kategorizovať incidenty pomocou štítkov/tagov. Kategorizácia incidentov pomocou tagov
FREQ_136 - Možnosť vytvárať šablóny pre opakujúce sa typy incidentov	Tvorba šablón pre rýchle zadávanie často sa opakujúcich incidentov. Možnosť vytvárať šablóny pre opakujúce sa typy incidentov

FREQ_158 - Zdieľanie prípadov medzi tímami a externými partnermi podľa práv	Podpora riadeného zdieľania prípadov. Zdieľanie prípadov medzi tímami a externými partnermi podľa práv
UC_18 – Spravovať organizácie, tímy a štruktúru prípadov	UC_18 rieši administráciu organizácií/tenantov a spôsob, akým sa incidenty/prípady v rámci nich štruktúrujú: založenie a úprava organizácií / tímov, nastavenie kategórií, typov a vlastníkov prípadov, definovanie šablón incidentov a spôsobu ich zdieľania medzi tímami a externými partnermi. Stojí na UC_17 (používatelia a roly) a UC_14 (portál zákazníka) a dopĺňa ich o „organizačno-procesnú“ vrstvu.
UC_18 – Spravovať organizácie, tímy a štruktúru prípadov	UC_18 rieši administráciu organizácií/tenantov a spôsob, akým sa incidenty/prípady v rámci nich štruktúrujú: založenie a úprava organizácií / tímov, nastavenie kategórií, typov a vlastníkov prípadov, definovanie šablón incidentov a spôsobu ich zdieľania medzi tímami a externými partnermi. Stojí na UC_17 (používatelia a roly) a UC_14 (portál zákazníka) a dopĺňa ich o „organizačno-procesnú“ vrstvu.

4.5.2.21 UC_19 – Riadiť uchovávanie, ochranu a auditovanie dát SOCaaS



Obrázok 31 : UC_19 – Riadiť uchovávanie, ochranu a auditovanie dát SOCaaS

Prípad použitia	UC_19 – Riadiť uchovávanie, ochranu a auditovanie dát SOCaaS
Cieľ	UC_19 rieši správu dát v SOCaaS z pohľadu platformy: kde a ako sa logy ukladajú, indexujú a uchovávajú, aké retenčné politiky platia pre jednotlivé zdroje logov, ako sú logy chránené a šifrované, ako sa vedú auditovacie záznamy o aktivitách používateľov a analytikov. Cieľom je, aby SOCaaS spĺňal požiadavky na bezpečné ukladanie a auditovateľnosť dát, a zároveň podporoval forenznú analýzu.

Vstupná podmienka	SOCaaS platforma je v prevádzke (UC_15) a prijíma logy z rôznych zdrojov (UC_01).
Vstupná podmienka	Existuje úložisko logov / dát (SIEM / data lake), ktoré podporuje konfiguráciu retencie a šifrovania.
Vstupná podmienka	Je definovaná aspoň základná politika uchovávania a bezpečnosti logov (napr. podľa typu logu alebo regulácie).
Výstupná podmienka	Pre logy/dáta sú nastavené retenčné politiky podľa zdroja a dôležitosti.
Výstupná podmienka	Logy sú chránené pri prenose aj uložení (nastavené šifrovanie).
Výstupná podmienka	Aktivity používateľov a analytikov sú auditované, aby bolo možné vykonať forenznú analýzu a dohľadať, kto čo robil.

Basic Path	Basic Path

Krok	Aktivita
1	Návrh architektúry ukladania a retencie
2	Nastavenie retenčných politík podľa zdroja a dôležitosti
3	Zapnutie a overenie šifrovania logov
4	Konfigurácia zberu auditovacích záznamov
5	Monitorovanie stavu uchovávania a audit trailu
6	Vyhodnocovanie požiadaviek auditorov
7	Úprava politík na základe zistení

ALT_19_01 – Nedostatočná kapacita pre nastavenú retenciu	Alternate

Krok	Aktivita
1	Pri dlhších retenčných dobách Operátor zistí, že úložisko nemá dostatočnú kapacitu; spoločne s Architektom buď upravia retenciu (napr. rozdielne podľa typu logu), alebo navrhnú rozšírenie úložiska.

ALT_19_02 – Požiadavka audítora na dlhšiu retenciu	Alternate

Krok	Aktivita

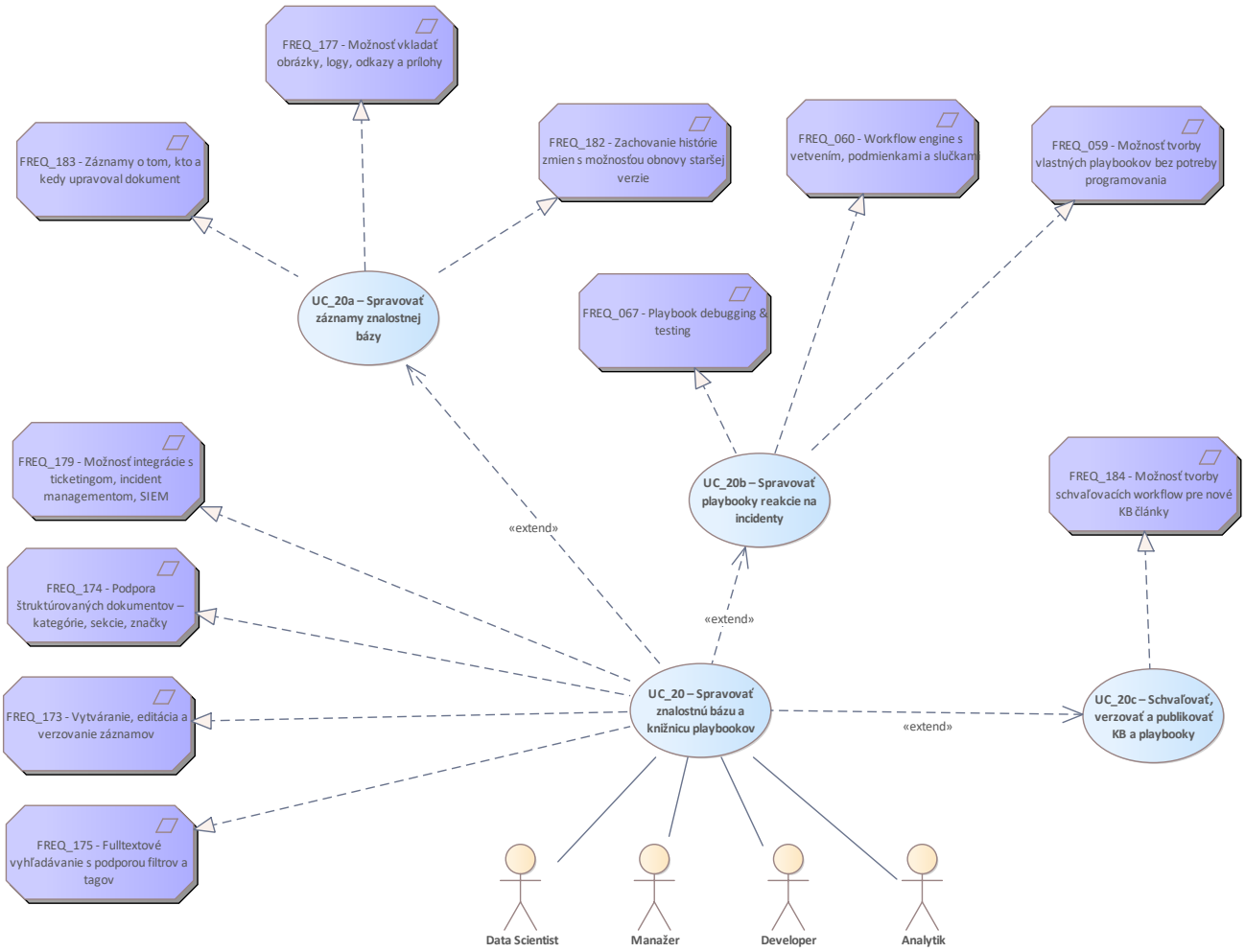
1	Auditor alebo regulátor požaduje dlhšiu retenciu pre konkrétny typ logov (napr. prihlasovacie logy); Architekt a Operátor upravia príslušnú retenčnú politiku a zaznamenajú zmenu ako súčasť compliance dokumentácie.

ALT_19_03 – Incident s kompromitáciou úložiska logov	Alternate

K rok	Aktivita
1	Zistí sa incident súvisiaci s prístupom k úložisku logov; audit trail umožní určiť, kto a kedy pristupoval k dátam. Architekt a Operátor na základe zistení sprísnia šifrovanie, prístupové práva alebo segmentáciu úložiska.

Naviazané funkčné požiadavky	
FREQ_154 - Logovanie činností analytikov počas riešenia incidentu (audit trail)	Evidencia činností pre forenznú analýzu. Logovanie činností analytikov počas riešenia incidentu (audit trail)
FREQ_039 - Podporované formáty logov	Schopnosť SIEM prijímať a spracovávať logy v rôznych štandardizovaných formátoch. Podporované formáty logov (syslog, JSON, CSV, CEF, LEEF...)
FREQ_052 - Šifrovanie	Ochrana logov pred neoprávneným prístupom pri prenose a ukladaní. Šifrovanie (pri prenose aj uložení)
FREQ_071 - Zber auditovacích dát pomocou agentov	Zber auditovacích záznamov o aktivitách používateľov, procesoch a systéme cez agenta. Zber auditovacích dát pomocou agentov
FREQ_051 - Retencia	Schopnosť nastaviť retenčné politiky logov podľa zdroja a dôležitosti. Retencia (flexibilná, podľa typu logu)

4.5.2.22 UC_20 – Spravovať znalostnú bázu a knižnicu playbookov



Obrázok 32 : UC_20 – Spravovať znalostnú bázu a knižnicu playbookov

Prípad použitia	UC_20 – Spravovať znalostnú bázu a knižnicu playbookov

Cieľ	UC_20 rieši, aby mal SOC centrálne a riadene: znalostnú bázu (KB) – články, návody, lessons learned, postupy, knižnicu playbookov – manuálne aj automatizované reakčné postupy, proces schvaľovania, verzovania a publikovania tohto obsahu.

Vstupná podmienka	Existuje modul pre knowledge base a playbooky dostupný pre Analytika a Manažéra.
Vstupná podmienka	Sú definované roly a práva na tvorbu, úpravu a schvaľovanie obsahu.
Vstupná podmienka	V systéme už existujú aspoň základné KB články alebo playbooky (napr. inicializačný set).
Výstupná podmienka	Znalostná báza obsahuje aktuálne, verzované a kategorizované záznamy.
Výstupná podmienka	Knižnica playbookov obsahuje publikované a použiteľné playbooky naviazané na typy incidentov.
Výstupná podmienka	Každý záznam má dohľadateľnú históriu a informáciu, kto ho vytvoril a schválil.

Basic Path	Basic Path

Krok	Aktivita
1	Analytik otvorí modul „Znalostná báza a playbooky“ a zvolí, či chce pracovať s KB alebo playbookmi.
2	Analytik vytvorí nový záznam alebo otvorí existujúci a doplní obsah podľa aktuálnych poznatkov z incidentov, TI alebo huntovania.
3	Analytik priradí záznam k typom incidentov, kategóriám a tagom, aby bol jednoducho vyhľadateľný v iných UC.
4	Analytik uloží záznam ako draft a odošle ho na schválenie Manažérovi alebo vlastníkovi oblasti.
5	Manažér skontroluje obsah, porovná zmeny s predchádzajúcou verziou a rozhodne o schválení alebo vrátení na úpravu.
6	Po schválení systém označí novú verziu ako platnú a starú verziu presunie do histórie so záznamom o dátume a autorovi zmeny.

7	Platný záznam je sprístupnený v relevantných častiach systému (napr. v detaile incidentu, v playbook engine, v portáli zákazníka).
8	Systém zaznamená všetky operácie nad záznamom (vytvorenie, úpravy, schválenie) pre audit a forenznú analýzu.

ALT_20_01 – Záznam je vrátený na dopracovanie	Alternate

K rok	Aktivita
1	Manažér neodsúhlasí navrhovaný obsah, pridá komentár s pripomienkami a záznam sa vráti Analytikovi do stavu draft.

ALT_20_02 – Záznam je označený ako zastaraný	Alternate

K rok	Aktivita
1	Manažér alebo Analytik zistí, že obsah už neplatí; zmení stav na „archivovaný“ a systém ho prestane ponúkať ako aktívne odporúčanie, no zostane dostupný v histórii.

Naviazané funkčné požiadavky	
UC_20a – Spravovať záznamy znalostnej bázy	UC_20a detailne rieši životný cyklus KB článkov – vytváranie, úpravy, štruktúru, tagovanie a väzbu na incidenty.
FREQ_179 - Možnosť integrácie s ticketingom, incident managementom, SIEM	Prepojenie KB s inými systémami pre efektívnejšie používanie obsahu. Možnosť integrácie s ticketingom, incident managementom, SIEM
UC_20c – Schvaľovať, verzovať a publikovať KB a playbooky	UC_20c rieši governance vrstvu nad KB a playbookmi – schvaľovanie, verzovanie, audit zmien a workflow schválení.
FREQ_140 - Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	Možnosť exportovať tickety pre účely archivácie alebo reportingu. Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting
FREQ_175 - Fulltextové vyhľadávanie s podporou filtrov a tagov	Vyhľadávanie v KB s možnosťou filtrovania podľa tagov, kategórií a obsahu. Fulltextové vyhľadávanie s podporou filtrov a tagov
FREQ_173 - Vytváranie, editácia a verzovanie záznamov	Možnosť vytvárať, upravovať a sledovať verzie dokumentov s históriou zmien. Vytváranie, editácia a verzovanie záznamov (návody, playbooky, FAQ)

UC_20b – Spravovať playbooky reakcie na incidenty	UC_20b rieši návrh, úpravu a údržbu playbookov, ktoré SOC využíva pri automatizovanej alebo poloautomatizovanej reakcii (UC_07).
FREQ_174 - Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky	Organizácia KB dokumentov podľa štruktúrovaných pravidiel (kategórie, tagy, sekcie). Podpora štruktúrovaných dokumentov – kategórie, sekcie, značky (tags)
UC_20 – Spravovať znalostnú bázu a knižnicu playbookov	UC_20 rieši, aby mal SOC centrálne a riadene: znalostnú bázu (KB) – články, návody, lessons learned, postupy, knižnicu playbookov – manuálne aj automatizované reakčné postupy, proces schvaľovania, verzovania a publikovania tohto obsahu.
UC_20 – Spravovať znalostnú bázu a knižnicu playbookov	UC_20 rieši, aby mal SOC centrálne a riadene: znalostnú bázu (KB) – články, návody, lessons learned, postupy, knižnicu playbookov – manuálne aj automatizované reakčné postupy, proces schvaľovania, verzovania a publikovania tohto obsahu.
Prípad použitia	UC_20a – Spravovať záznamy znalostnej bázy
Cieľ	UC_20a detailne rieši životný cyklus KB článkov – vytváranie, úpravy, štruktúru, tagovanie a väzbu na incidenty.

Vstupná podmienka	Platí preconditions z UC_20.
Vstupná podmienka	Používateľ má oprávnenie editovať KB záznamy.
Výstupná podmienka	KB obsahuje aktuálne, štruktúrované články s bohatým obsahom, históriou zmien a audit trailom.

Basic Path		Basic Path
K rok	Aktivita	
1	Analytik otvorí v module „Znalostná báza“ zoznam KB článkov.	
2	Analytik vytvorí nový KB článok alebo otvorí existujúci záznam na úpravu.	
3	Analytik upraví obsah článku, doplní štruktúru (sekcie, podsekcie), tagy a kategórie.	
4	Analytik vloží relevantné prílohy, logy alebo snímky obrazovky, ktoré pomáhajú pri riešení podobných incidentov.	
5	Analytik uloží záznam, systém zaznamená autora a čas zmeny a podľa potreby ho odošle na schválenie.	
ALT_20a_01 - Zlúčenie dvoch príbuzných KB záznamov		Alternate
K rok	Aktivita	
1	Analytik identifikuje dva veľmi podobné články v znalostnej báze, vytvorí jeden konsolidovaný záznam a pôvodné články označí ako archivované s odkazom na nový konsolidovaný článok.	
ALT_20a_02 - Pokus o úpravu bez dostatočných oprávnení		Alternate
K rok	Aktivita	
1	Používateľ s read-only prístupom sa pokúsi upraviť KB článok, systém mu zmenu nedovolí, zobrazí informáciu o nedostatočných oprávneniach a ponechá záznam bez zmeny.	
Naviazané funkčné požiadavky		
FREQ_183 - Záznamy o tom, kto a kedy upravoval dokument	Audit trail zmien dokumentov s informáciou o autoroch a čase. Záznamy o tom, kto a kedy upravoval dokument	
FREQ_177 - Možnosť vkladať obrázky, logy, odkazy a prílohy	Schopnosť obohatiť dokumenty o multimediálny alebo dátový obsah. Možnosť vkladať obrázky, logy, odkazy a prílohy	
FREQ_182 - Zachovanie histórie zmien s možnosťou obnovy staršej verzie	Sledovanie a archivácia zmien pre každý dokument. Zachovanie histórie zmien s možnosťou obnovy staršej verzie	

UC_20a – Spravovať záznamy znalostnej bázy	UC_20a detailne rieši životný cyklus KB článkov – vytváranie, úpravy, štruktúru, tagovanie a väzbu na incidenty.
UC_20a – Spravovať záznamy znalostnej bázy	UC_20a detailne rieši životný cyklus KB článkov – vytváranie, úpravy, štruktúru, tagovanie a väzbu na incidenty.
Prípad použitia	UC_20b – Spravovať playbooky reakcie na incidenty
Cieľ	UC_20b rieši návrh, úpravu a údržbu playbookov, ktoré SOC využíva pri automatizovanej alebo poloautomatizovanej reakcii (UC_07).

Vstupná podmienka	V systéme je dostupný workflow/playbook engine.
Vstupná podmienka	Používateľ má oprávnenie vytvárať a meniť playbooky.
Výstupná podmienka	Playbooky majú definované kroky, vetvenie a integračné body a sú otestované pred nasadením do produkcie.

Basic Path	Basic Path

Krok	Aktivita
1	Analytik alebo Developer otvorí sekciu „Playbooky“ v SOCaaS rozhraní.
2	Používateľ založí nový playbook alebo otvorí existujúci na úpravu.
3	V grafickom editore definuje jednotlivé kroky playbooku, ich poradie, vetvenie a podmienky vykonania.
4	Ku krokom priradí integračné akcie (napr. volať API firewallu, EDR, ticketingu) a nastaví potrebné parametre.
5	Používateľ spustí test playbooku v debug/simulačnom režime a overí, že kroky prebiehajú podľa očakávaní.
6	Po úspešnom teste odošle playbook na schválenie Manažérovi a po schválení je označený ako „produkčný“ pre UC_07.

ALT_20b_01 - Playbook neprejde testom v simulačnom režime	Alternate

Krok	Aktivita
1	Po spustení testu playbooku v simulačnom režime systém zistí chybu v niektorom kroku alebo chýbajúce parametre, test skončí s chybou a playbook zostane v stave draft, kým ho Analytik alebo Developer neupravia.

ALT_20b_02 - Uloženie playbooku s neúplnou konfiguráciou		Alternate
K rok	Aktivita	
1	Používateľ sa pokúsi uložiť playbook, v ktorom chýbajú povinné polia alebo nie sú nakonfigurované všetky integračné kroky, systém ukladanie odmietne a zvýrazní chýbajúce alebo neplatné nastavenia.	
Naviazané funkčné požiadavky		
FREQ_059 - Možnosť tvorby vlastných playbookov bez potreby programovania	Schopnosť tvoriť a spravovať playbooky pomocou vizuálneho rozhrania bez nutnosti kódovania. Možnosť tvorby vlastných playbookov bez potreby programovania	
FREQ_067 - Playbook debugging & testing	Možnosť testovať a ladiť playbooky pred ich ostrým nasadením. Playbook debugging & testing	
FREQ_060 - Workflow engine s vetvením, podmienkami a slučkami	Možnosť definovať komplexné logiky v playbookoch pomocou rozhodovacích bodov. Workflow engine s vetvením, podmienkami a slučkami	
UC_20b – Spravovať playbooky reakcie na incidenty	UC_20b rieši návrh, úpravu a údržbu playbookov, ktoré SOC využíva pri automatizovanej alebo poloautomatizovanej reakcii (UC_07).	
UC_20b – Spravovať playbooky reakcie na incidenty	UC_20b rieši návrh, úpravu a údržbu playbookov, ktoré SOC využíva pri automatizovanej alebo poloautomatizovanej reakcii (UC_07).	
Prípad použitia	UC_20c – Schvaľovať, verzovať a publikovať KB a playbooky	
Cieľ	UC_20c rieši governance vrstvu nad KB a playbookmi – schvaľovanie, verzovanie, audit zmien a workflow schválení.	

Vstupná podmienka	Existujú drafty alebo upravené verzie KB článkov a playbookov (UC_20a, UC_20b).	
Vstupná podmienka	Manažér má oprávnenie schvaľovať a publikovať obsah.	
Výstupná podmienka	Každý záznam má stav (draft, v schvaľovaní, publikovaný, archivovaný) a sledovanú históriu zmien a autorov.	
Basic Path		Basic Path
K rok	Aktivita	
1	Manažér otvorí zoznam KB článkov a playbookov, ktoré čakajú na schválenie.	

2	Manažér vyberie konkrétny záznam a zobrazí si aktuálnu verziu spolu s prehľadom zmien oproti predchádzajúcej verzii.
3	Manažér rozhodne, či záznam schváli, vráti na dopracovanie alebo označí na archiváciu.
4	Pri schválení systém nastaví novú verziu ako platnú, staršiu verziu presunie do histórie a zaznamená dátum a autora schválenia.
5	Systém podľa nastaveného workflow informuje relevantných používateľov, že nový článok alebo playbook je publikovaný a dostupný na použitie.

ALT_20c_01 - Zistená chyba v obsahu po publikovaní	Alternate

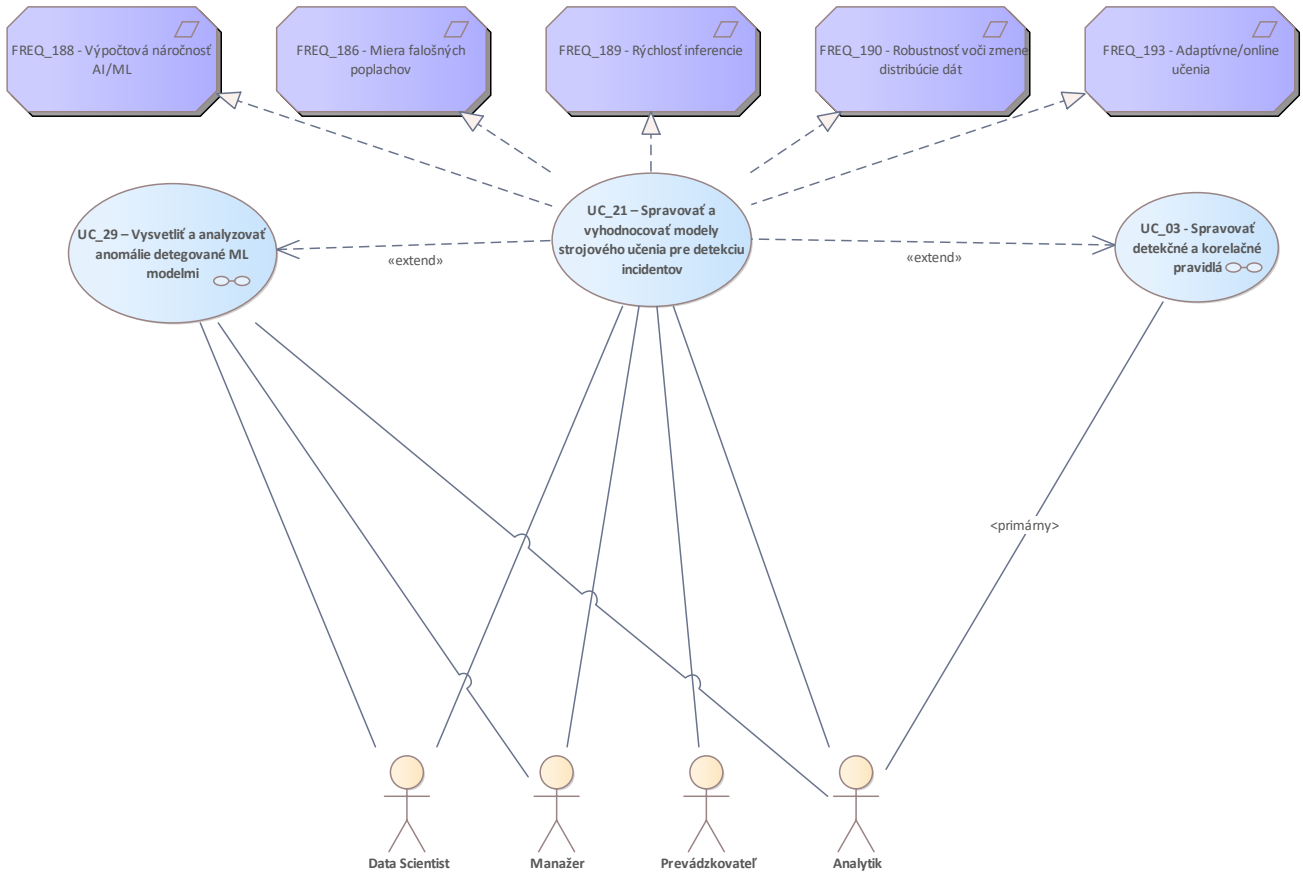
K rok	Aktivita
1	Po publikovaní novej verzie KB článku alebo playbooku si Analytik všimne faktickú chybu, vytvorí opravnú verziu, odošle ju na zrýchlené schválenie a po schválení sa opravná verzia stane platnou.

ALT_20c_02 - Primárny schvaľovateľ nie je dostupný	Alternate

K rok	Aktivita
1	Záznam čaká na schválenie, ale primárny Manažér je dlhodobo nedostupný, systém po uplynutí definovaného času ponúkne schválenie náhradnému schvaľovateľovi podľa nastaveného schvaľovacieho workflow.

Naviazané funkčné požiadavky	
FREQ_184 - Možnosť tvorby schvaľovacích workflow pre nové KB články	Procesy schvaľovania pre publikáciu nových článkov. Možnosť tvorby schvaľovacích workflow pre nové KB články
UC_20c – Schvaľovať, verzovať a publikovať KB a playbooky	UC_20c rieši governance vrstvu nad KB a playbookmi – schvaľovanie, verzovanie, audit zmien a workflow schválení.

4.5.2.23 UC_21 – Spravovať a vyhodnocovať modely strojového učenia pre detekciu incidentov



Obrázok 33 : UC_21 – Spravovať a vyhodnocovať modely strojového učenia pre detekciu incidentov

Prípad použitia	UC_21 – Spravovať a vyhodnocovať modely strojového učenia pre detekciu incidentov

Cieľ	UC_21 rieši životný cyklus ML modelov, ktoré používame na detekciu incidentov a anomálií v SOCaaS: návrh a trénovanie modelov, meranie kvality (FP/FN, presnosť, rýchlosť), robustnosť voči zmene dát, adaptívne/online učenie pri bežiacom systéme.

Vstupná podmienka	SOCaaS má komponent(y) detekcie postavené na ML (anomálie, klasifikátory, scoring).
Vstupná podmienka	Sú dostupné historické dáta/logy na tréning a testovanie modelov.
Vstupná podmienka	Sú nastavené základné metriky kvality, ktoré chceme dosiahnuť (napr. limit na FP/FN).
Výstupná podmienka	ML modely majú vyhodnotenú kvalitu (FP/FN, rýchlosť, robustnosť) a sú buď nasadené, alebo zamietnuté.
Výstupná podmienka	Systém vie reagovať na zmenu dát (drift) pomocou opätovného tréningu alebo online učenia.
Výstupná podmienka	Sú evidované výsledky hodnotenia modelov pre ďalšie rozhodovanie a audit.

Basic Path	Basic Path

Krok	Aktivita
1	Data Scientist vyberie dátový set (historické logy, incidenty) ako podklad pre tréning alebo testovanie modelu.
2	Data Scientist natrénuje nový model alebo upraví existujúci model na základe aktuálnych požiadaviek na detekciu.
3	Systém vyhodnotí kvalitu modelu na validačnom sete vrátane metriky falošných poplachov a nezachytených incidentov (FP/FN).
4	Systém vyhodnotí výpočtovú náročnosť modelu počas tréningu (CPU, GPU, RAM, čas trénovania) a porovná ju s dostupnými zdrojmi.
5	Systém zmeria rýchlosť inferencie modelu – čas potrebný na spracovanie nových udalostí v podmienkach blízkych reálnej prevádzke.

6	Data Scientist vyhodnotí robustnosť modelu voči zmene distribúcie dát (napr. nové typy logov, zmeny vzorcov správania) a dopad na kvalitu detekcie
7	Ak model spĺňa požadované metriky, Manažér schváli jeho nasadenie do produkcie, Prevádzkovateľ zabezpečí nasadenie modelu v detekčnom engine.
8	Po nasadení systém priebežne zbiera spätnú väzbu z reálnej prevádzky (skutočné FP/FN) a pripravuje podklady pre ďalšie ladnie alebo adaptívne učenie.

ALT_21_02 – Model je príliš pomalý pre reálny čas	Alternate

K rok	Aktivita
1	Test inferencie ukáže, že model nedokáže spracovať prichádzajúce dáta v požadovanom čase; Data Scientist zvolí efektívnejšiu architektúru, zjednoduší model alebo navrhne offloading na iné prostredie (napr. dedikovaný GPU server).

ALT_21_03 – Objaví sa výrazný dátový drift po nasadení	Alternate

K rok	Aktivita
1	Po čase sa zistí, že nové typy udalostí alebo správania znížili kvalitu detekcie; systém upozorní na drift, Data Scientist pripraví aktualizovaný tréningový set a spustí adaptívne/online učenie, aby model reflektoval nové dáta.

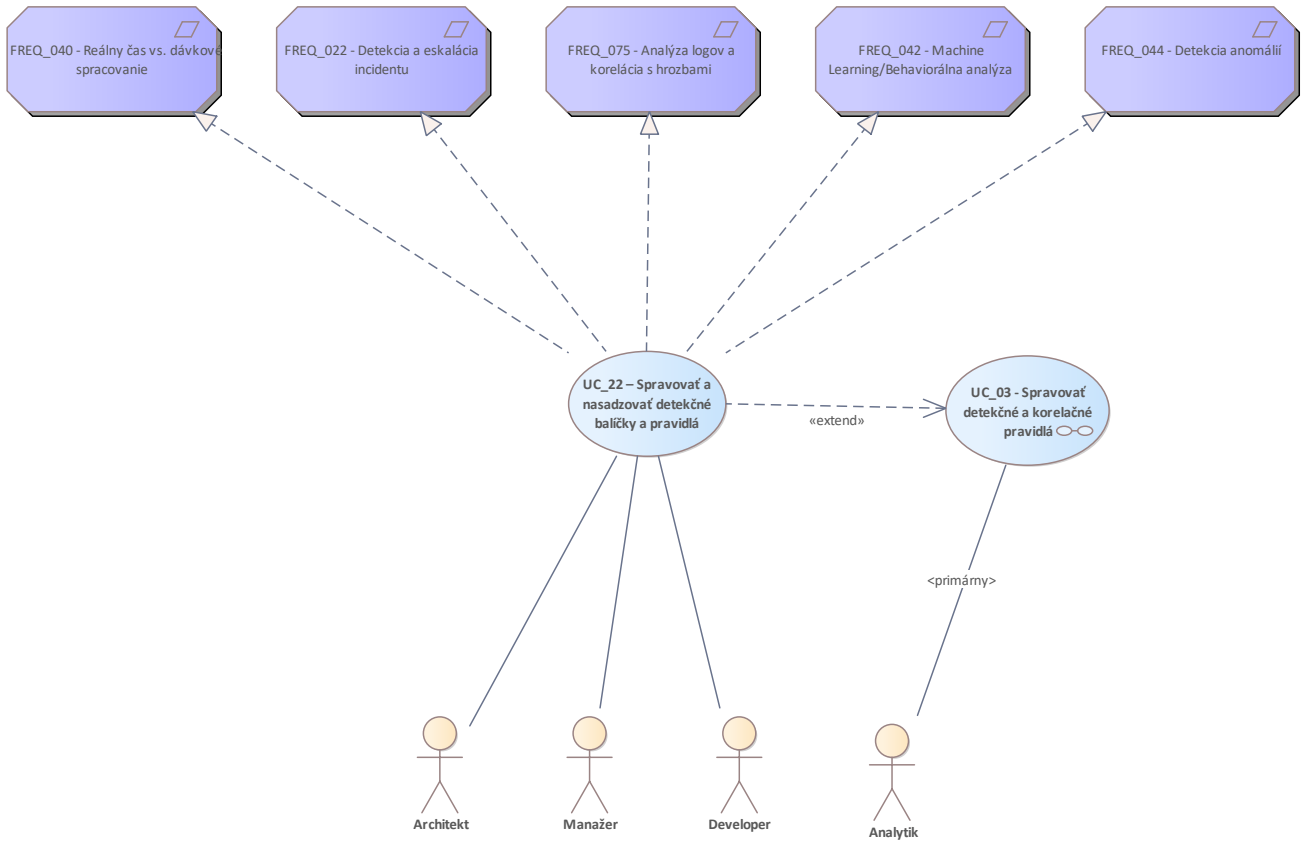
ALT_21_01 – Model má príliš vysoký počet falošných poplachov (FP)	Alternate

K rok	Aktivita
1	Po vyhodnotení sa ukáže, že model generuje neakceptovateľne veľa FP; Data Scientist upraví architektúru, hyperparametre alebo prahové hodnoty a proces tréningu a hodnotenia zopakuje, kým sa nedosiahne prijateľná úroveň.

Naviazané funkčné požiadavky	
FREQ_193 - Adaptívne/online učenia	Riešenie musí mať možnosť adaptívneho/online učenia. Podpora aktualizácie modelu počas prevádzky bez retrénovania. Schopnosť aktualizovať model bez nutnosti úplného retrénovania, napr. pomocou online learningu.
FREQ_186 - Miera falošných poplachov	Riešenie musí zabezpečiť vyhodnotenie miery falošných poplachov (False Positives/Negatives). Ako často algoritmus generuje falošné pozitíva/negatíva. Zníženie miery falošných poplachov je kľúčové pre použiteľnosť v SOC. Ideálne modely majú veľmi nízky počet FP/FN.

UC_29 – Vysvetliť a analyzovať anomálie detegované ML modelmi	UC_29 rieši, aby SOCaaS vedel zrozumiteľne vysvetliť anomálie detegované modelmi strojového učenia: zobraziť kontext dátového toku (logy, metriky, sieťové toky), ukázať časový priebeh signálov, ktoré viedli k anomálii, pracovať s unsupervised modelmi (bez labelov), a dať analytikovi interpretáciu „prečo to model označil“.
FREQ_188 - Výpočtová náročnosť AI/ML	Riešenie musí byť škálovateľné pre výpočtová náročnosť (CPU/GPU, pamäť). Zdroje požadované na trénovanie a inferenciu modelu. Rôzna záťaž na výpočtové zdroje vrátane náročnosti na GPU, RAM a trvanie trénovania.
UC_03 - Spravovať detekčné a korelačné pravidlá	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).
FREQ_190 - Robustnosť voči zmene distribúcie dát	Riešenie musí zabezpečiť robustnosť voči zmene distribúcie dát (drift, noise). Odolnosť voči šumu, zmenám v dátach alebo útokomModel musí byť odolný voči neočakávaným zmenám, fluktuáciám alebo noise, inak prestane fungovať správne.
FREQ_189 - Rýchlosť inferencie	Riešenie musí zabezpečiť vyhodnotenie rýchlosti inferencie (čas detekcie). Rýchlosť odozvy pri detekcii. Ako rýchlo dokáže model poskytnúť výsledok na nové dáta. Kritické pre nasadenie v reálnom čase.

4.5.2.24 UC_22 – Spravovať a nasadzovať detekčné balíčky a pravidlá



Obrázok 34 : UC_22 – Spravovať a nasadzovať detekčné balíčky a pravidlá

Prípad použitia	UC_22 – Spravovať a nasadzovať detekčné balíčky a pravidlá

Cieľ	UC_22 rieši životný cyklus detekčného obsahu (pravidlá, korelačné pravidlá, signatúry, „content packy“) v SOCaaS: návrh a úpravu detekčných pravidiel a balíčkov, testovanie na historických alebo syntetických dátach, riadené nasadenie do produkcie, vrátane možnosti rollbacku, obmedzené nasadenie pre vybraných tenantov/zákazníkov. UC_22 nerieši samotný runtime detekcie (to je v UC_03), ale proces návrhu, testovania a riadeného nasadzovania detekčných pravidiel a balíčkov do enginu.

Vstupná podmienka	Existuje detekčný engine (UC_03), ktorý podporuje konfiguráciu pravidiel/balíčkov.
Vstupná podmienka	Platforma má mechanizmus na testovanie pravidiel (oddelené testovacie prostredie alebo test mód).
Vstupná podmienka	Sú definované roly a kompetencie, kto môže vytvárať/upravovať, a kto musí schvaľovať detekčné pravidlá.
Výstupná podmienka	Nové alebo upravené detekčné pravidlá sú otestované, schválené a nasadené do produkcie alebo zamietnuté.
Výstupná podmienka	Zmeny pravidiel sú verzované, auditovateľné a v prípade problémov je možné vrátiť sa k predchádzajúcej verzii.

Basic Path		Basic Path
Krok	Aktivita	
1	Analytik otvorí modul „Detekčné pravidlá a balíčky“ a zobrazí zoznam existujúcich pravidiel.	
2	Analytik vytvorí nové pravidlo alebo upraví existujúce, definuje podmienky, prahové hodnoty a mapovanie na typ incidentu.	
3	Analytik uloží zmenu ako návrh (draft) a spustí test pravidla na historických alebo syntetických dátach v testovacom režime.	
4	Systém vyhodnotí výsledky testu – počet zásahov, potenciálne falošné poplachy a dopad na existujúcu detekciu.	
5	Analytik na základe výsledkov testov prípadne upraví pravidlo a test zopakuje, kým nedosiahne akceptovateľné správanie.	

6	Analytik odošle pravidlo na schválenie Manažérovi alebo definovanému ownerovi detekčného obsahu.
7	Manažér zhodnotí dopad pravidla (najmä na počet alertov, typy hrozieb a dotknutých zákazníkov/tenantov) a rozhodne o schválení alebo vrátení na úpravu.
8	Po schválení Developer / DevSecOps spustí nasadenie pravidla do produkcie, prípadne len pre vybrané tenanty alebo v obmedzenom („canary“) režime.
9	Systém zaznamená všetky zmeny (verziu pravidla, autora, schvaľovateľa, čas nasadenia) a monitoruje dopady na alerty a výkon.

ALT_22_01 – Test pravidla odhalí extrémne veľa zásahov	Alternate

K rok	Aktivita
1	Analytik po kroku 4 zistí, že pravidlo by generovalo neprimerané množstvo alertov; pravidlo upraví (sprísnenie podmienok, doplnenie filtrov) a test zopakuje, kým nedosiahne prijateľný počet zásahov.

ALT_22_02 – Nasadené pravidlo negatívne ovplyvní produkciu	Alternate

K rok	Aktivita
1	Po nasadení v kroku 8 systém zistí výrazný nárast počtu alertov, latencie alebo chýb; Prevádzkovateľ alebo DevSecOps iniciuje návrat k predchádzajúcej verzii pravidiel a nové pravidlo sa označí ako „vyžaduje úpravu/test“.

ALT_22_03 – Pravidlo sa má nasadiť len pre vybraných zákazníkov	Alternate

K rok	Aktivita
1	Pri schvaľovaní v kroku 7 Manažér rozhodne, že pravidlo je relevantné len pre určitý typ zákazníka (napr. konkrétny sektor alebo tenant); pri nasadzovaní sa zvolí len podmnožina tenantov, na ktorých sa pravidlo aplikuje

Naviazané funkčné požiadavky	
FREQ_040 - Reálny čas vs. dávkové spracovanie	Schopnosť spracovávať logy v reálnom čase (streaming) alebo len v dávkach. Reálny čas vs. dávkové spracovanie
FREQ_044 - Detekcia anomálií	Detekcia neštandardného správania alebo odchýlok od očakávaného správania. Detekcia anomálií

FREQ_075 - Analýza logov a korelácia s hrozbami	Analýza logov s cieľom detekcie korelovaných udalostí a potenciálnych hrozieb. Analýza logov a korelácia s hrozbami
FREQ_042 - Machine Learning/Behaviorálna analýza	Schopnosť SIEM systému detegovať anomálie pomocou strojového učenia. Machine Learning/Behaviorálna analýza
FREQ_022 - Detekcia a eskalácia incidentu	Riešenie musí zabezpečiť detekciu a eskalácia incidentu. V prostredí musia byť nakonfigurované pravidlá na detekciu anomálií a známych hrozieb. Po detekcii: • sa generuje alert • alert sa automaticky transformuje na incident • Zammad zabezpečuje ticket pre L1 tím a podporu eskalácie, • tím vyhodnotí observables a využije obohatenie
UC_03 - Spravovať detekčné a korelačné pravidlá	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).

4.5.2.25 UC_23 – Spravovať a prevádzkovať skenovanie zraniteľností

Obrázok 35 : UC_23 – Spravovať a prevádzkovať skenovanie zraniteľností

Prípad použitia	UC_23 – Spravovať a prevádzkovať skenovanie zraniteľností
Cieľ	UC_23 rieši prevádzku a správu skenovania zraniteľností v rámci SOCaaS: plánovanie a spúšťanie skenov, priradenie skenov na aktíva a siete, technickú architektúru skenovania (master/senzor), integráciu nálezov do ticketov a do procesu správy zraniteľností (UC_12).

Vstupná podmienka	Sú známe aspoň základné aktíva a rozsahy sietí (UC_11) určené na skenovanie.
Vstupná podmienka	V prostredí je nasadený nástroj na skenovanie zraniteľností (on-prem, VM alebo SaaS).
Vstupná podmienka	Správca a Prevádzkovateľ majú oprávnenia konfigurovať skenery a plánovať skenovanie.
Výstupná podmienka	Skenovanie zraniteľností pre vybrané rozsahy prebehlo podľa plánu alebo na požiadanie.
Výstupná podmienka	Nálezy sú obohatené o CPE/CVE a CVSS skóre a sú dostupné pre UC_12.
Výstupná podmienka	Relevantné nálezy sú exportované alebo prepojené do ticketov na nápravu.

Basic Path	Basic Path

Krok	Aktivita
1	Prevádzkovateľ alebo Správca otvorí modul „Skenovanie zraniteľností“ a zobrazí prehľad existujúcich skenovacích profilov.

2	Prevádzkovateľ vyberie rozsahy (IP, siete, skupiny aktív) a zvolí typ skenu (plný, rýchly, autentifikovaný).
3	Prevádzkovateľ naplánuje pravidelné spúšťanie skenov (napr. týždenne v noci) alebo spustí jednorazový ad-hoc sken.Prevádzkovateľ naplánuje pravidelné spúšťanie skenov (napr. týždenne v noci) alebo spustí jednorazový ad-hoc sken.
4	Systém priradí skeny k dostupným skenovacím uzlom podľa architektúry (master/senzor) a optimalizuje rozloženie záťaže.Systém priradí skeny k dostupným skenovacím uzlom podľa architektúry (master/senzor) a optimalizuje rozloženie záťaže.
5	Po dokončení skenu systém spracuje výsledky, priradí zraniteľnostiam CPE/CVE identifikátory a vypočíta CVSS skóre.Po dokončení skenu systém spracuje výsledky, priradí zraniteľnostiam CPE/CVE identifikátory a vypočíta CVSS skóre.
6	Analytik alebo Správca si zobrazí výsledky skenovania, filtruje nálezy podľa závažnosti a rozsahu a označí tie, ktoré majú byť riešené.Analytik alebo Správca si zobrazí výsledky skenovania, filtruje nálezy podľa závažnosti a rozsahu a označí tie, ktoré majú byť riešené.
7	Systém vytvorí alebo aktualizuje tikety na nápravu v integrovanom ticketovacom systéme alebo exportuje nálezy vo zvolenom formáte pre ďalšie spracovanie.

ALT_23_01 – Skenovanie nie je možné dokončiť na časti infraštruktúry	Alternate

K rok	Aktivita
1	Počas skenu nie sú niektoré systémy dostupné alebo sú blokované firewallom; systém tieto časti označí ako „neskenované“, Prevádzkovateľ dostane informáciu a môže naplánovať náhradný sken s upravenou konfiguráciou alebo v inom časovom okne.

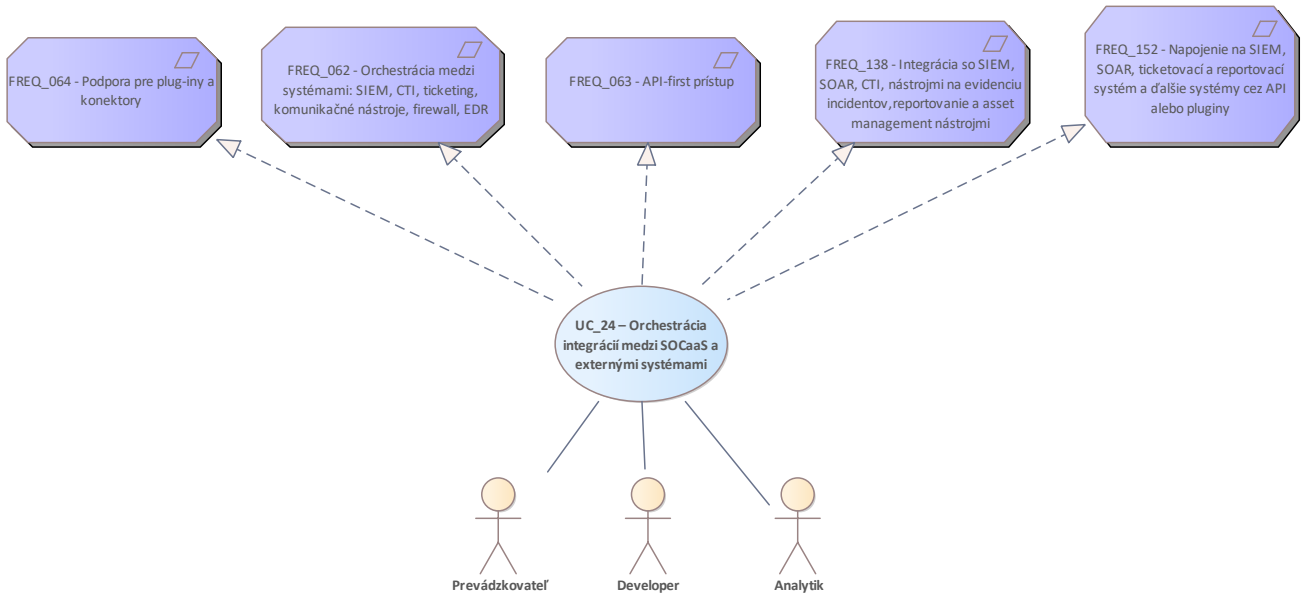
ALT_23_02 – Preťaženie skenovacej infraštruktúry	Alternate

K rok	Aktivita
1	Po spustení viacerých skenov naraz systém zistí nadmernú záťaž skenovacích uzlov; skeny sú zoradené do fronty alebo rozdelené v čase tak, aby neprekročili povolené limity, a Prevádzkovateľ je upozornený, že je vhodné posilniť architektúru skenovania.

Naviazané funkčné požiadavky

FREQ_087 - Podpora CPE, CVE identifikátorov	Možnosť identifikácie zraniteľností podľa štandardizovaných identifikátorov. Podpora CPE, CVE identifikátorov
FREQ_096 - Podpora pre CVSS 4.0	Podpora najnovšej verzie skórovacieho systému CVSS. Podpora pre CVSS 4.0
FREQ_090 - Podpora plánovania úloh a alertov	Možnosť automatizovať opakované úlohy a generovanie upozornení. Podpora plánovania úloh a alertov (voliteľné)
FREQ_091 - Tikety na nápravu – integrácia alebo export	Možnosť exportovať nálezy do ticketovacieho systému alebo CSV, JSON, PDF. Tikety na nápravu – integrácia alebo export
FREQ_094 - Architektúra skenovania	Škálovateľnosť a prispôsobenie distribúcie skenov. Architektúra skenovania (monolitická alebo master/senzor)

4.5.2.26 UC_24 – Orchestrácia integrácií medzi SOCaaS a externými systémami



Obrázok 36 : UC_24 – Orchestrácia integrácií medzi SOCaaS a externými systémami

Prípad použitia	UC_24 – Orchestrácia integrácií medzi SOCaaS a externými systémami

Cieľ	UC_24 rieši technickú a procesnú orchestráciu integrácií medzi SOCaaS a ďalšími systémami: SIEM, SOAR, CTI, ticketing, komunikačné nástroje, firewall, EDR, API integrácie, webhooky, plug-iny a konektory, jednotné riadenie dátových tokov a akcií naprieč týmito systémami. Cieľom je, aby incident response, automatizácia (UC_07) a správa incidentov fungovali ako jeden prepojený ekosystém, nie ako izolované nástroje.

Vstupná podmienka	Architektúra integrácií zákazníka a SOCaaS je navrhnutá (UC_13) a existuje aspoň základné napojenie na SIEM/SOAR/ticketing.
Vstupná podmienka	SOCaaS platforma podporuje REST API, webhooky a plug-in/konektorový mechanizmus.
Vstupná podmienka	Prevádzkovateľ a Developer majú oprávnenia konfigurovať integrácie a orchestrácie medzi systémami.
Výstupná podmienka	Definované integračné väzby a flow medzi SOCaaS, SIEM, SOAR, CTI, ticketingom, firewallmi, EDR a ďalšími systémami sú aktívne a monitorované.
Výstupná podmienka	Incidenty a udalosti sú konzistentne synchronizované medzi systémami (stav, ID, odkazy).
Výstupná podmienka	Je k dispozícii audit a prehľad, ktoré integračné kanály sú aktívne, aké akcie spúšťajú a ako zlyhávajú.

Basic Path		Basic Path
Krok	Aktivita	
1	Prevádzkovateľ otvorí modul „Integrácie a orchestrácia“ a zobrazí prehľad existujúcich integračných väzieb (SIEM, SOAR, CTI, ticketing, EDR, firewall, komunikačné nástroje).	
2	Developer alebo Prevádzkovateľ vytvorí novú integračnú väzbu alebo upraví existujúcu, zvolí cieľový systém (napr. ticketovací systém, CTI, firewall) a typ integrácie (API, webhook, plug-in).	
3	Používateľ nakonfiguruje autentifikáciu, endpointy, formáty dát a mapovanie polí medzi SOCaaS a cieľovým systémom.	

4	Používateľ definuje, ktoré udalosti v SOCaaS majú spúšťať akcie v externých systémoch (napr. vytvorenie incidentu → vytvor ticket, zmena stavu incidentu → aktualizuj ticket, IOC z TI → aktualizuj blokovací zoznam vo firewalle).
5	Systém uloží konfiguráciu a umožní spustiť test integračnej väzby na malom vzorku dát alebo testovacom incidente.
6	Po úspešnom teste Prevádzkovateľ aktivuje integračnú väzbu a nastaví, či sa má aplikovať globálne alebo len pre vybraných zákazníkov/tenantov.
7	SOCaaS v reálnej prevádzke začína využívať nastavenú orchestráciu – generuje webhooky, volá API alebo spúšťa plug-iny podľa definovaných pravidiel a mapovaní.
8	Systém priebežne loguje úspešné a neúspešné integračné volania, zobrazuje štatistiky a upozorňuje Prevádzkovateľa na chyby alebo výpadky integračných kanálov.

ALT_24_01 – Zlyhanie integračného volania	Alternate

K rok	Aktivita
1	Počas testu alebo produkčného volania API/webhooku externý systém vráti chybu alebo nie je dostupný; SOCaaS záznam označí ako neúspešný, uloží detail chyby a podľa nastavenia buď zopakuje volanie s retry politikou, alebo vytvorí interný incident/prehlásenie pre Prevádzkovateľa.

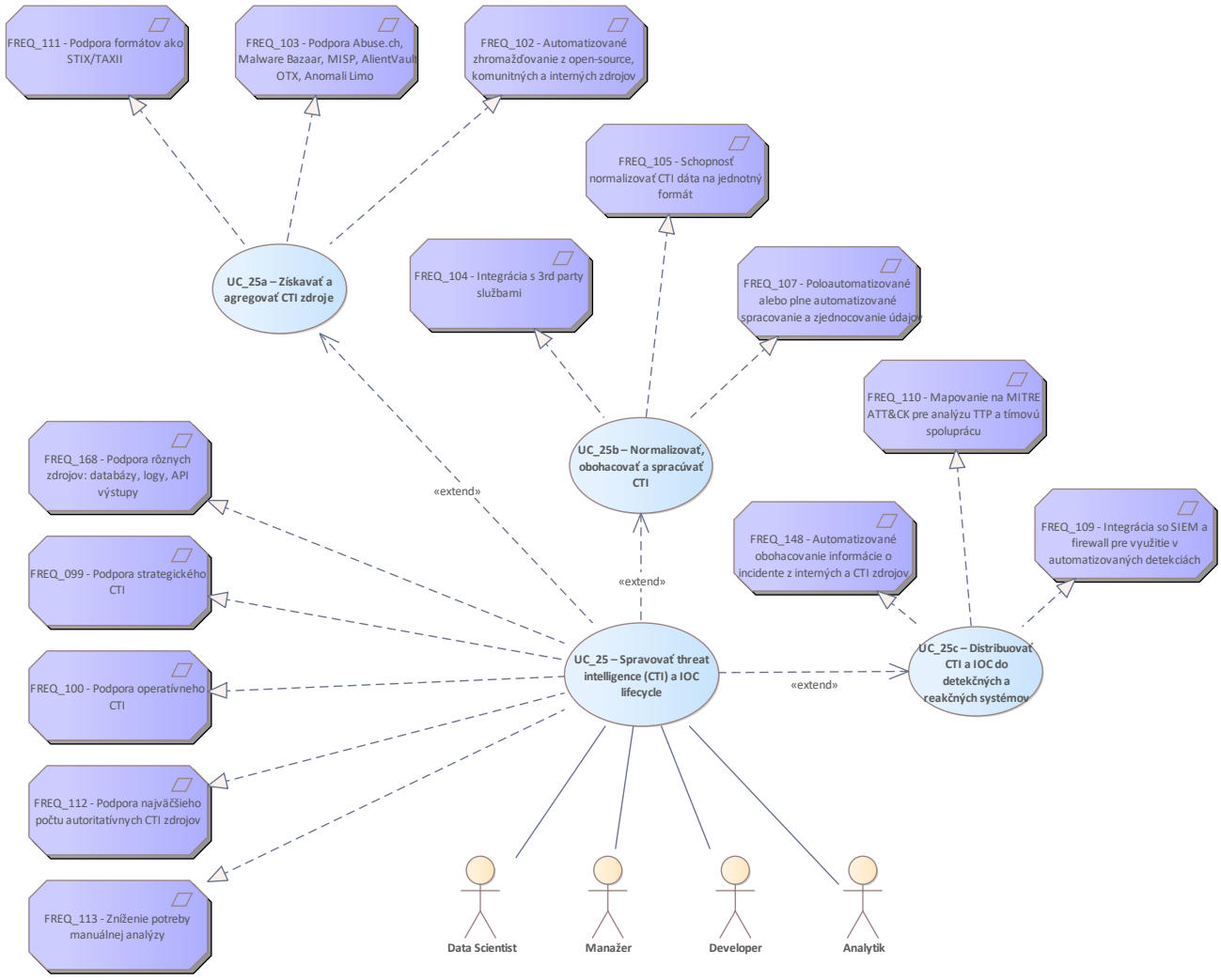
ALT_24_02 – Konflikt pri mapovaní dát medzi systémami	Alternate

K rok	Aktivita
1	Pri nastavovaní mapovania polí medzi SOCaaS a externým systémom sa zistí, že niektoré povinné polia v cieľovom systéme nie je možné jednoznačne vyplniť z dát SOCaaS; Prevádzkovateľ musí doplniť transformáciu, default hodnoty alebo obmedziť typ udalostí, pre ktoré sa integrácia používa.

Naviazané funkčné požiadavky	
FREQ_062 - Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR	Prepojenie a výmena dát s inými systémami v rámci incident response procesu. Orchestrácia medzi systémami: SIEM, CTI, ticketing, komunikačné nástroje, firewall, EDR
FREQ_063 - API-first prístup	Prístupnosť funkcií nástroja cez API a podpora webhookov na notifikácie a interakcie. API-first prístup (REST, Webhooky)

FREQ_138 - Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi	Integrácia s inými bezpečnostnými nástrojmi na automatizáciu a workflow. Integrácia so SIEM, SOAR, CTI, nástrojmi na evidenciu incidentov,reportovanie a asset management nástrojmi
FREQ_152 - Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy	Možnosť obojsmernej výmeny dát. Napojenie na SIEM, SOAR, ticketovací a reportovací systém a ďalšie systémy cez API alebo pluginy
FREQ_064 - Podpora pre plug-iny a konektory	Schopnosť rozšírenia funkcionality nástroja cez moduly alebo konektory. Podpora pre plug-iny a konektory
UC_24 – Orchestrácia integrácií medzi SOCaaS a externými systémami	UC_24 rieši technickú a procesnú orchestráciu integrácií medzi SOCaaS a ďalšími systémami: SIEM, SOAR, CTI, ticketing, komunikačné nástroje, firewall, EDR, API integrácie, webhooky, plug-iny a konektory, jednotné riadenie dátových tokov a akcií naprieč týmito systémami. Cieľom je, aby incident response, automatizácia (UC_07) a správa incidentov fungovali ako jeden prepojený ekosystém, nie ako izolované nástroje.

4.5.2.27 UC_25 – Spravovať threat intelligence (CTI) a IOC lifecycle



Obrázok 37 : UC_25 – Spravovať threat intelligence (CTI) a IOC lifecycle

Prípad použitia	UC_25 – Spravovať threat intelligence (CTI) a IOC lifecycle

Cieľ	UC_25 rieši kompletný lifecycle CTI v SOCaaS: získavanie CTI z rôznych zdrojov (feeds, MISP, open-source, vendor), normalizáciu, obohacovanie a prioritizáciu CTI dát, distribúciu IOC/TTP do detekcie (SIEM, EDR, firewall, SOAR) a do incidentov.

Vstupná podmienka	SOCaaS má modul CTI (alebo je integrovaný s externým CTI nástrojom).
Vstupná podmienka	Sú definované CTI zdroje (komunitné, komerčné, interné) a základná politika, ktoré zdroje sú „trusted“.
Vstupná podmienka	Detekčné systémy (SIEM, EDR, firewall, IDS, SOAR) podporujú príjem IOC/TTP z CTI.
Výstupná podmienka	CTI dáta sú systematicky zbierané, normalizované, obohatené a agregované.
Výstupná podmienka	Hrozby sú prioritizované a z relevantných IOC/TTP sú vytvorené podklady pre detekciu, hunting a incidenty.
Výstupná podmienka	IOC/TTP sú distribuované do detekčných systémov a incident managementu konzistentným spôsobom (s audit trailom).

Basic Path	Basic Path

Krok	Aktivita
1	Analytik otvorí modul „Threat Intelligence“ a zobrazí prehľad aktívnych CTI zdrojov a posledných aktualizácií.
2	Systém periodicky alebo na požiadanie stiahne nové CTI dáta zo všetkých nakonfigurovaných zdrojov (open-source, komunitné, vendor, interné).Systém periodicky alebo na požiadanie stiahne nové CTI dáta zo všetkých nakonfigurovaných zdrojov (open-source, komunitné, vendor, interné).
3	CTI pipeline dáta normalizuje, obohacuje a agreguje – spája IOC, dopĺňa kontext, spája s historickými incidentmi a logmi.
4	Data Scientist definuje alebo upraví pravidlá pre scoring, prioritu a kategorizáciu hrozieb (kritickosť, relevantnosť pre konkrétnych zákazníkov).
5	Systém na základe scoringu automaticky identifikuje najrelevantnejšie hrozby a IOC, ktoré majú byť použité v detekcii, huntingu a incidentoch.

6	CTI modul vytvorí pre vybrané IOC/TTP výstupy pre detekciu (napr. block listy, SIEM pravidlá, hunting queries) a pripraví ich na distribúciu do pripojených systémov.
7	Analytik má v incidentoch a hunting nástrojoch k dispozícii obohatené CTI – vidí kampane, TTP, skupiny a súvisiace IOC.
8	Systém priebežne zaznamenáva, ktoré CTI zdroje a IOC/TTP boli použité v reálnych incidentoch a hunting prípadoch a tieto informácie používa na ďalšie dolaďovanie scoringu a relevancie.

ALT_25_01 – CTI zdroj prestane byť dôveryhodný alebo dostupný	Alternate

K rok	Aktivita
1	Po čase sa ukáže, že konkrétny CTI zdroj má nekvalitné alebo duplicitné dáta, prípadne je dlhodobo nedostupný; Manažér alebo CTI špecialista zdroj deaktivuje, prípadne zníži jeho váhu v scoringu.

ALT_25_02 – Prebytok CTI a zahltenie analytikov	Alternate

K rok	Aktivita
1	Systém deteguje, že množstvo nových IOC/hrozieb výrazne prevyšuje kapacitu analytikov; CTI špecialista upraví scoring, filtre a prahy tak, aby sa do popredia dostali len najrelevantnejšie hrozby (napr. podľa sektora, geolokácie, expozície aktív).

ALT_25_03 – Nesúlad CTI medzi zákazníkmi/tenantmi	Alternate

K rok	Aktivita
1	Niektorý IOC je relevantný len pre konkrétneho zákazníka (napr. podľa jeho technológií alebo geografie); systém podporuje per-tenant filtráciu CTI, takže IOC/TTP sa distribuujú len tým zákazníkom, ktorých sa týkajú.

Naviazané funkčné požiadavky	
FREQ_112 - Podpora najväčšieho počtu autoritatívnych CTI zdrojov	Rozsiahly výber komunitných, verejných a platených zdrojov. Podpora najväčšieho počtu autoritatívnych CTI zdrojov
FREQ_168 - Podpora rôznych zdrojov: databázy, logy, API výstupy	Schopnosť agregovať dáta z viacerých technických a analytických zdrojov. Podpora rôznych zdrojov: databázy, logy, API výstupy

UC_25b – Normalizovať, obohacovať a spracúvať CTI	UC_25b rieši pipeline spracovania CTI: normalizáciu rôznych formátov na jednotný model, obohacovanie IOC a artefaktov z externých služieb, workflow pre automatické/poloautomatické spracovanie CTI.
UC_25a – Získavať a agregovať CTI zdroje	UC_25a rieši ingest a napojenie CTI zdrojov: definovanie zdrojov (feeds, MISP, API, vendor portály), automatizované sťahovanie, použitie štandardizovaných formátov.
FREQ_099 - Podpora strategického CTI	Získavanie a analýza informácií o dlhodobých trendoch, dopadoch útokov a strategických odporúčaniach. Podpora strategického CTI (správy, analýzy dopadu, trendy útokov)
FREQ_113 - Zníženie potreby manuálnej analýzy	Zautomatizovanie a prioritizácia hrozieb tak, aby sa analytici venovali len relevantným. Zníženie potreby manuálnej analýzy – šetrenie času analytikov
FREQ_100 - Podpora operatívneho CTI	Schopnosť mapovať techniky, taktiky a procedúry (TTP), identifikovať útočnícke skupiny a ich správanie. Podpora operatívneho CTI (TTP, profilovanie skupín)
UC_25c – Distribuovať CTI a IOC do detekčných a reakčných systémov	UC_25c rieši push CTI do zvyšku ekosystému: preposielanie IOC do SIEM/IDS/EDR/firewallov, využitie CTI v detekcii, playbookoch a incidentoch,
Prípad použitia	UC_25a – Získavať a agregovať CTI zdroje

Cieľ	UC_25a rieši ingest a napojenie CTI zdrojov: definovanie zdrojov (feeds, MISP, API, vendor portály), automatizované sťahovanie, použitie štandardizovaných formátov.

Vstupná podmienka	CTI modul je dostupný v SOCaaS.
Vstupná podmienka	Sú známe CTI zdroje, ku ktorým máme prístup (API kľúče, URL, autentifikácia).
Výstupná podmienka	Zdroje CTI sú nakonfigurované, aktivované a pravidelne sťahujú nové dáta v podporovaných formátoch.

Basic Path	Basic Path

Krok	Aktivita
1	Developer otvorí sekciu „CTI zdroje“ a zobrazí zoznam existujúcich zdrojov.
2	Developer pridá nový zdroj CTI (feed, MISP, vendor API) a zadá potrebné prístupové údaje.
3	Konfiguruje interval sťahovania (periodický, na požiadanie) a typ dát (IOC, TTP, kampane, reporty).
4	Systém otestuje pripojenie, stiahne vzorku dát a overí formát a konzistenciu.
5	Po úspešnom teste je zdroj označený ako aktívny a zapojený do pravidelného CTI ingestu.

ALT_25a_01 – Chyba pri pripojení k CTI zdroju	Alternate

Krok	Aktivita
1	Test v kroku 4 zlyhá (chybný API kľúč, expired token, nedostupný endpoint); systém zobrazí chybu, deaktivuje zdroj a ponechá ho v stave „vyžaduje opravu konfigurácie“.

ALT_25a_02 – Limit alebo kvóty na CTI zdroji		Alternate
K rok	Aktivita	
1	CTI zdroj má obmedzený počet požiadaviek za deň; systém upraví interval sťahovania tak, aby sa kvóty neprekračovali, a upozorní SOC analytika	
Naviazané funkčné požiadavky		
FREQ_103 - Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	Pripravené konektory alebo integrácie pre známe CTI zdroje. Podpora Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	
FREQ_102 - Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	Automatické sťahovanie dát z rôznych zdrojov (napr. GitHub, feeds, MISP, API systémy). Automatizované zhromažďovanie z open-source, komunitných a interných zdrojov	
FREQ_111 - Podpora formátov ako STIX/TAXII	Použitie štandardizovaných formátov pre výmenu CTI dát. Podpora formátov ako STIX/TAXII	
UC_25a – Získavať a agregovať CTI zdroje	UC_25a rieši ingest a napojenie CTI zdrojov: definovanie zdrojov (feeds, MISP, API, vendor portály), automatizované sťahovanie, použitie štandardizovaných formátov.	
Prípad použitia	UC_25b – Normalizovať, obohacovať a spracúvať CTI	
Cieľ	UC_25b rieši pipeline spracovania CTI: normalizáciu rôznych formátov na jednotný model, obohacovanie IOC a artefaktov z externých služieb, workflow pre automatické/poloautomatické spracovanie CTI.	

Vstupná podmienka	CTI dáta sú stiahnuté zo zdrojov (UC_25a).
Vstupná podmienka	Sú nakonfigurované integračné služby na obohatenie (VirusTotal, Shodan, …).
Výstupná podmienka	CTI dáta sú v jednotnom formáte, obohatené a preverené, pripravené na scoring a distribúciu.

Basic Path	Basic Path

Krok	Aktivita
1	Systém prijme nové CTI dáta zo zdrojov a uloží ich do bufferu na spracovanie.
2	CTI pipeline transformuje rôzne formáty do jednotného štruktúrovaného modelu (IOC, TTP, kampane, meta).
3	Pre každý IOC alebo relevantný artefakt pipeline voliteľne vykoná obohatenie cez externé služby (VirusTotal, Shodan, DomainTools, …).
4	Workflow engine aplikuje definované kroky spracovania – deduplikáciu, filtrovanie, first-seen/last-seen logiku a technické validácie.
5	Výsledné CTI záznamy sú uložené v jednotnej podobe a označené stavom (nové, spracované, nepotvrdené, vyradené).

ALT_25b_01 – Externé obohatenie je dočasne nedostupné	Alternate

Krok	Aktivita
1	Pri kroku 3 niektorá externá služba (napr. VirusTotal) neodpovie včas; systém označí stav obohatenia ako „pending“ a naplánuje opakovaný pokus neskôr bez blokovania celého pipeline.

ALT_25b_02 – Konflikt pri normalizácii CTI dát	Alternate

Krok	Aktivita
1	Rôzne zdroje poskytnú pre rovnaký IOC konfliktné informácie; pipeline označí záznam na manuálnu revíziu CTI špecialistom, ktorý vyberie alebo skombinuje správne hodnoty.

Naviazané funkčné požiadavky

FREQ_104 - Integrácia s 3rd party službami	Schopnosť obohacovať IOC a ďalšie artefakty pomocou externých služieb. Integrácia s 3rd party službami ako VirusTotal, Shodan, DomainTools, URLScan.io
FREQ_105 - Schopnosť normalizovať CTI dáta na jednotný formát	Konsolidácia dát z rôznych formátov do štruktúrovaného jednotného výstupu. Schopnosť normalizovať CTI dáta na jednotný formát
FREQ_107 - Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov	Možnosť workflow pre spracovanie dát bez potreby manuálnych zásahov. Poloautomatizované alebo plne automatizované spracovanie a zjednocovanie údajov
UC_25b – Normalizovať, obohacovať a spracúvať CTI	UC_25b rieši pipeline spracovania CTI: normalizáciu rôznych formátov na jednotný model, obohacovanie IOC a artefaktov z externých služieb, workflow pre automatické/poloautomatické spracovanie CTI.
UC_25b – Normalizovať, obohacovať a spracúvať CTI	UC_25b rieši pipeline spracovania CTI: normalizáciu rôznych formátov na jednotný model, obohacovanie IOC a artefaktov z externých služieb, workflow pre automatické/poloautomatické spracovanie CTI.
Prípad použitia	UC_25c – Distribuovať CTI a IOC do detekčných a reakčných systémov
Cieľ	UC_25c rieši push CTI do zvyšku ekosystému: preposielanie IOC do SIEM/IDS/EDR/firewallov, využitie CTI v detekcii, playbookoch a incidentoch,

Vstupná podmienka	CTI dáta sú spracované a prioritizované (UC_25, UC_25b).
Vstupná podmienka	Existujú integračné väzby na detekčné systémy (UC_24).

Výstupná podmienka	Relevantné IOC/TTP sú nasadené v detekčných systémoch.
Výstupná podmienka	Incidenty a hunting prípady sú obohatené CTI metadátami.

Basic Path	Basic Path

Krok	Aktivita
1	CTI modul vyberie IOC/TTP, ktoré sú označené ako „relevantné na distribúciu“ podľa scoringu a politiky.
2	Developer vyberie, do ktorých detekčných systémov sa majú IOC/TTP distribuovať (SIEM, IDS/IPS, EDR, firewall, SOAR).
3	Systém vygeneruje výstupné artefakty (block listy, SIEM pravidlá, feedy) a odošle ich cez integračné kanály (API, plug-in, CTI rozhranie).
4	Detekčné systémy začnú používať nové IOC/TTP pri detekcii; CTI modul sleduje úspešnosť a spôsob použitia v reálnych incidentoch.
5	Pri vzniku incidentu SOCaaS incident automaticky obohatí informáciami z CTI – prepojí IOC, TTP a MITRE ATT&CK techniky.

ALT_25c_01 – Detekčný systém neprijme niektoré IOC	Alternate

Krok	Aktivita
1	Pri distribúcii v kroku 3 SIEM alebo firewall odmietne časť IOC (napr. kvôli formátu alebo limitu); systém tieto záznamy označí ako „neaplikované“ a ponúkne CTI špecialistovi možnosť úpravy formátu alebo rozsahu.

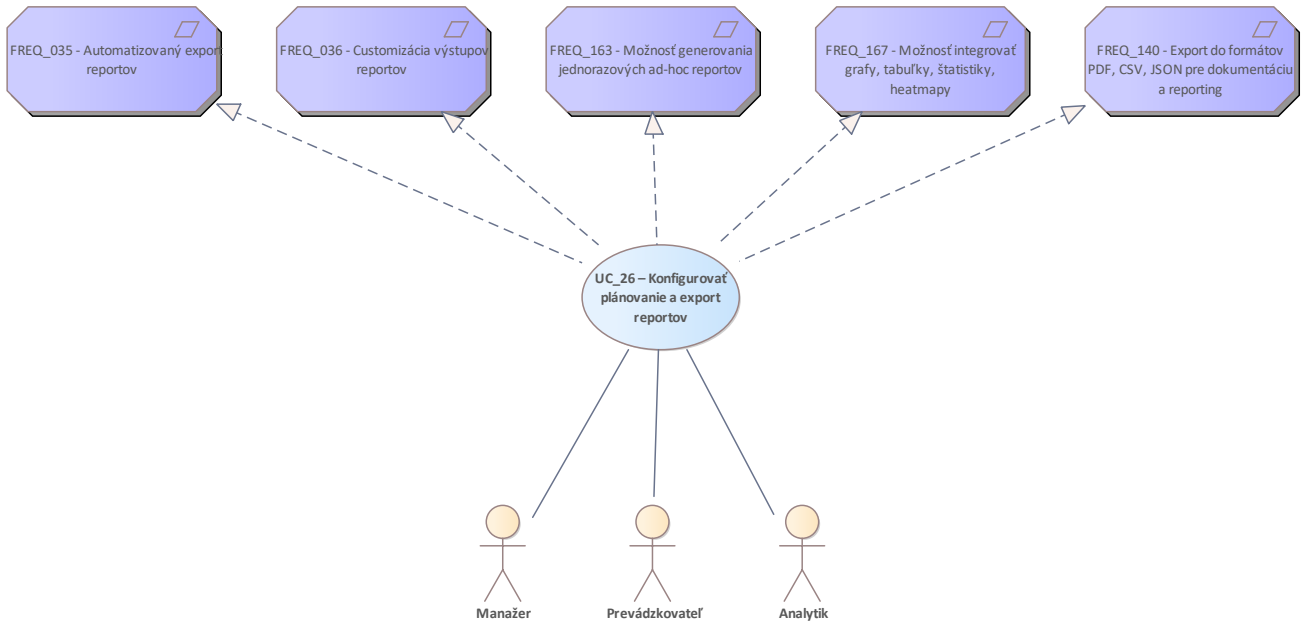
ALT_25c_02 – IOC je po čase označený ako false positive alebo nerelevantný	Alternate

Krok	Aktivita
1	Na základe spätnej väzby z incidentov sa zistí, že niektoré IOC spôsobujú spam v detekcii; CTI modul tieto IOC stiahne z distribúcie a upraví scoring/politiku, aby sa podobné hrozby v budúcnosti hodnotili inak.

Naviazané funkčné požiadavky	
FREQ_110 - Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu	Spájanie incidentov, IOC a TTP s ATT&CK frameworkom. Mapovanie na MITRE ATT&CK pre analýzu TTP a tímovú spoluprácu

FREQ_109 - Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách	Preposielanie IOC a dát priamo do detekčných systémov (SIEM, IDS, firewall). Integrácia so SIEM a firewall pre využitie v automatizovaných detekciách
FREQ_148 - Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov	Integrácia na obohatenie IOC a metadát z CTI alebo iných systémov. Automatizované obohacovanie informácie o incidente z interných a CTI zdrojov
UC_25c – Distribuovať CTI a IOC do detekčných a reakčných systémov	UC_25c rieši push CTI do zvyšku ekosystému: preposielanie IOC do SIEM/IDS/EDR/firewallov, využitie CTI v detekcii, playbookoch a incidentoch,
UC_25c – Distribuovať CTI a IOC do detekčných a reakčných systémov	UC_25c rieši push CTI do zvyšku ekosystému: preposielanie IOC do SIEM/IDS/EDR/firewallov, využitie CTI v detekcii, playbookoch a incidentoch,
UC_25c – Distribuovať CTI a IOC do detekčných a reakčných systémov	UC_25c rieši push CTI do zvyšku ekosystému: preposielanie IOC do SIEM/IDS/EDR/firewallov, využitie CTI v detekcii, playbookoch a incidentoch,

4.5.2.28 UC_26 – Konfigurovať plánovanie a export reportov



Obrázok 38 : UC_26 – Konfigurovať plánovanie a export reportov

Prípad použitia	UC_26 – Konfigurovať plánovanie a export reportov
Cieľ	UC_26 rieši praktickú správu reportov v SOCaaS: nastavenie automatického generovania a distribúcie reportov, customizáciu obsahu a vzhľadu reportov, generovanie jednorazových ad-hoc reportov pre manažérov alebo audit.

Vstupná podmienka	V systéme existuje modul reportovania (UC_10) s definovanými typmi reportov (incidenty, SLA, KPI…).
Vstupná podmienka	Sú nakonfigurované kanály distribúcie (minimálne e-mail, ideálne aj webhook/integračné endpointy).
Výstupná podmienka	Pre jednotlivé typy reportov sú nastavené harmonogramy generovania, príjemcovia a formáty exportu.

Výstupná podmienka	Používatelia vedia generovať jednorazové ad-hoc reporty mimo harmonogramu.
Výstupná podmienka	Reporty obsahujú zvolené metriky, grafy a vizualizácie v požadovanom dizajne.

Basic Path	Basic Path

Krok	Aktivita
1	Manažér alebo Prevádzkovateľ otvorí modul „Reporty a export“ a zobrazí dostupné typy reportov.
2	Používateľ vyberie konkrétny typ reportu a zvolí, ktoré metriky, časové rozsahy a sekcie majú byť v reporte zahrnuté.
3	Používateľ nakonfiguruje harmonogram generovania reportu (denne, týždenne, mesačne) a zoznam príjemcov alebo cieľových endpointov.
4	Používateľ upraví vzhľad reportu – logo organizácie, záhlavie, poznámky, prípadne štruktúru sekcií.
5	Používateľ zvolí formát exportu (PDF, CSV, JSON) a spôsob doručenia (e-mail, webhook, uloženie do úložiska).
6	Systém v definovaných časoch automaticky vygeneruje report, doplní vybrané grafy, tabuľky a štatistiky a odošle ho na zvolené kanály.
7	Systém uchováva históriu vygenerovaných reportov, aby bolo možné ich spätne stiahnuť alebo použiť ako podklad pre audit.

ALT_26_01 – Vytvorenie jednorazového ad-hoc reportu	Alternate

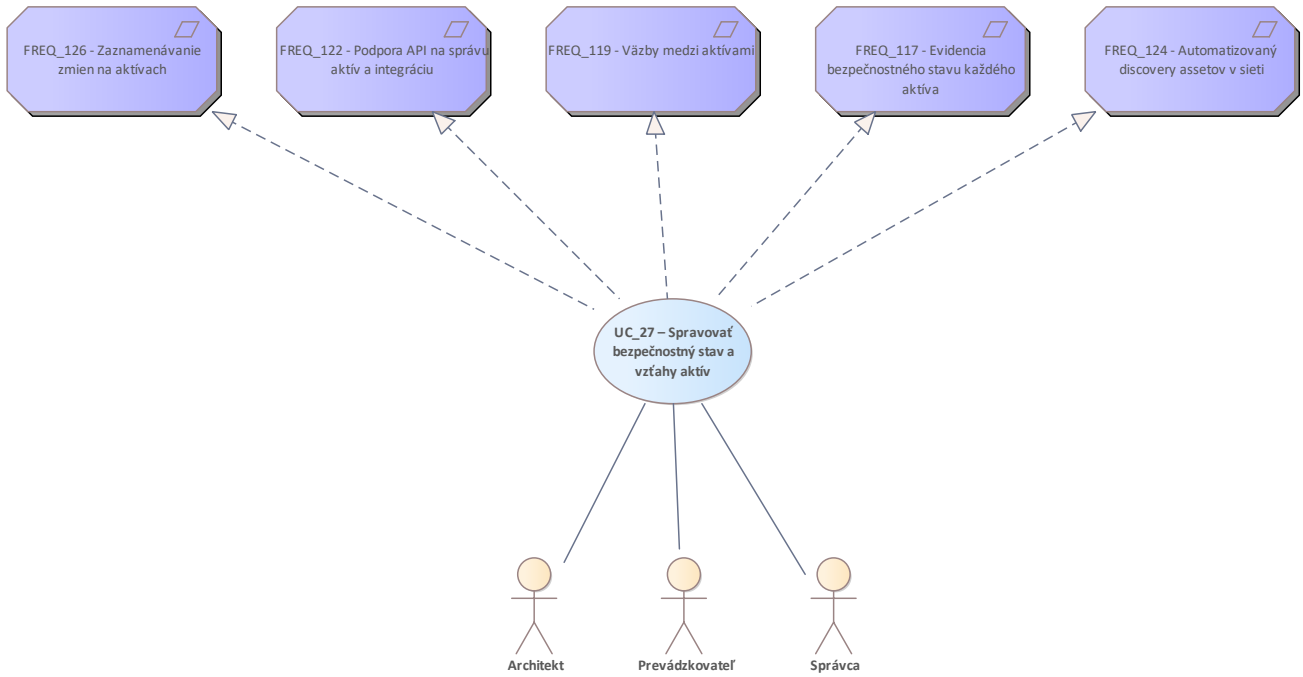
Krok	Aktivita
1	Manažér potrebuje mimoriadny report mimo plánovaného cyklu; v module zvolí typ reportu, nastaví filtre a časové obdobie a spustí jednorazové generovanie, pričom systém vygeneruje report len raz bez zmeny existujúcich harmonogramov.

ALT_26_02 – Neúspešné doručenie automaticky generovaného reportu	Alternate

Krok	Aktivita

1	Pri pravidelnom exporte reportu dôjde k chybe pri odoslaní e-mailu alebo webhooku; systém report uloží, označí distribúciu ako neúspešnú a upozorní Prevádzkovateľa, ktorý môže doručenie zopakovať alebo upraviť cieľové adresy.
Naviazané funkčné požiadavky	
FREQ_036 - Customizácia výstupov reportov	Riešenie musí zabezpečiť customizácia výstupov reportov. Bude obsahovať: • Možnosť výberu metrík, polí, časových rozsahov • Personalizácia dizajnu – logá, záhlavie, farebná schéma • Zaradenie vysvetliviek, poznámok a kontextuálneho komentára
FREQ_167 - Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy	Vizualizácia dát priamo v reportoch rôznymi formami. Možnosť integrovať grafy, tabuľky, štatistiky, heatmapy
FREQ_163 - Možnosť generovania jednorazových ad-hoc reportov	Tvorba reportov mimo pravidelného harmonogramu podľa potreby. Možnosť generovania jednorazových ad-hoc reportov
FREQ_035 - Automatizovaný export reportov	Riešenie musí zabezpečiť automatizovaný export reportov. Reporty bude možné exportovať automatizovane: • Periodické reporty – denne, týždenne alebo mesačne generované a distribuované výstupy. • Distribúcia cez e-mail alebo webhook – reporty môžu byť automaticky odoslané na určené adresy alebo endpointy. • Podpora pre templaty a vlastné filtre – možnosť nastaviť podmienky, výbery časových období a formáty podľa potrieb.
FREQ_140 - Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting	Možnosť exportovať tickety pre účely archivácie alebo reportingu. Export do formátov PDF, CSV, JSON pre dokumentáciu a reporting

4.5.2.29 UC_27 – Spravovať bezpečnostný stav a vzťahy aktív



Obrázok 39 : UC_27 – Spravovať bezpečnostný stav a vzťahy aktív

Prípad použitia	UC_27 – Spravovať bezpečnostný stav a vzťahy aktív
Cieľ	UC_27 rozširuje asset management o „smart CMDB“: eviduje bezpečnostný stav každého aktíva (patch level, zraniteľnosti, posledné zmeny), zobrazuje a spravuje väzby medzi aktívami (server–služba–aplikácia), využíva automatizovaný discovery a API integrácie, vedie audit zmien na aktívach.

Vstupná podmienka	Základný inventár aktív je založený (UC_11) – existujú aspoň kľúčové servery, siete, aplikácie.
Vstupná podmienka	Sú k dispozícii zdroje dát pre discovery (skeny, CMDB, cloud API…).
Vstupná podmienka	Používatelia majú definované roly pre čítanie/úpravu aktív.
Výstupná podmienka	Pre každé aktívum je evidovaný aktuálny bezpečnostný stav (verzie, patch úroveň, zraniteľnosti).
Výstupná podmienka	Medzi aktívami sú definované väzby (topológia / závislosti).
Výstupná podmienka	Zmeny na aktívach sú auditovateľné (kto, čo, kedy) a dostupné pre forenznú a prevádzkovú analýzu.

Basic Path	Basic Path

Krok	Aktivita
1	Správca alebo Prevádzkovateľ otvorí modul „Aktíva“ a zobrazí prehľad aktív s ich aktuálnym bezpečnostným stavom.
2	Prevádzkovateľ nakonfiguruje automatizovaný discovery (napr. sieťové skenovanie, cloud API, integrácia s CMDB) pre vybrané segmenty prostredia.
3	Systém spustí discovery a identifikuje nové alebo zmenené aktíva, pričom ich porovná s existujúcim inventárom.
4	Správca skontroluje novo nájdené alebo zmenené aktíva, priradí ich do správnych kategórií a podľa potreby upraví detaily (vlastník, kritickosť, lokalita).
5	Správca alebo Architekt doplní alebo upraví väzby medzi aktívami (napr. server → služba → aplikácia → databáza), aby odrážali skutočné závislosti.
6	Systém automaticky aktualizuje bezpečnostný stav aktív na základe vstupov zo skenovania, patch managementu alebo iných integračných zdrojov.
7	Každá zmena na aktíve (parametre, stav, väzby) sa uloží s informáciou o autorovi a čase zmeny, aby bolo možné neskôr analyzovať históriu.

ALT_27_01 – Konflikt medzi discovery a existujúcim inventárom	Alternate

Krok	Aktivita
1	Discovery nájde aktívum, ktoré už v inventári existuje, ale s iným označením alebo parametrami; systém označí konflikt, Správca vyberie, či záznam zlúči, prepíše, alebo ponechá ako nové aktívum.

ALT_27_02 – Zlyhanie automatizovaného discovery		Alternate
K rok	Aktivita	
1	Discovery úloha zlyhá (chybná autentifikácia, nedostupná sieť, chýbajúce oprávnenia); systém discovery zastaví, zaznamená detaily chyby a informuje Prevádzkovateľa, aby mohol upraviť konfiguráciu alebo spustiť discovery znovu.	
Naviazané funkčné požiadavky		
FREQ_124 - Automatizovaný discovery assetov v sieti	Automatizovaný zber a aktualizácia údajov o aktívach zo siete a iných systémov. Automatizovaný discovery assetov v sieti (napr. SNMP, nmap, API z iných systémov)	
FREQ_119 - Väzby medzi aktívami	Možnosť vizualizovať a spravovať prepojenia medzi komponentmi infraštruktúry. Väzby medzi aktívami (napr. server – služba – aplikácia)	
FREQ_126 - Zaznamenávanie zmien na aktívach	Auditovateľnosť všetkých zmien pre forenznú a prevádzkovú transparentnosť. Zaznamenávanie zmien na aktívach (kto, kedy, čo zmenil)	
FREQ_122 - Podpora API na správu aktív a integráciu	Možnosť spravovať a aktualizovať údaje o aktívach pomocou API. Podpora API (REST, GraphQL) na správu aktív a integráciu	
FREQ_117 - Evidencia bezpečnostného stavu každého aktíva	Ukladanie informácií o zraniteľnostiach, patch úrovni a aktualizáciách systému. Evidencia bezpečnostného stavu každého aktíva (napr. OS verzie, posledná aktualizácia)	

4.5.2.30 UC_28 – Nasadiť a udržiavať SOCaaS v rôznych prostrediach

Obrázok 40 : UC_28 – Nasadiť a udržiavať SOCaaS v rôznych prostrediach

Prípad použitia	UC_28 – Nasadiť a udržiavať SOCaaS v rôznych prostrediach
Cieľ	UC_28 rieši nasadenie a technickú prevádzku SOCaaS platformy v rôznych prostrediach: on-premise u zákazníka, v cloude, hybridne, ako vlastné IaaS prostredie pre SOCaaS, s jasnými pravidlami údržby, aktualizácií a monitoringu, vrátane použitia open-source/bezplatnej edície ako základnej platformy. Je to technicko-prevádzkový UC, ktorý rozširuje prevádzku platformy (napr. UC o prevádzke SOCaaS) o multi-deployment / IaaS pohľad.

Vstupná podmienka	Architektúra SOCaaS riešenia je navrhnutá (topológia, moduly, integračné body).
Vstupná podmienka	Je k dispozícii infraštruktúra (on-prem, cloud alebo IaaS), v ktorej sa dá SOCaaS nasadiť.
Vstupná podmienka	Prevádzkovateľ má definované procesy na monitoring, údržbu a aktualizácie komponentov.
Výstupná podmienka	SOCaaS je nasadený v zvolenom prostredí (on-prem/cloud/hybrid/IaaS) a je monitorovaný.
Výstupná podmienka	Sú nastavené pravidlá údržby, aktualizácií a testovania zmien v samostatnom prostredí.
Výstupná podmienka	Platforma je pripravená škálovať sa podľa potrieb tenantov / zákazníkov.
Basic Path	Basic Path

K rok	Aktivita
1	Architekt spolu s Prevádzkovateľom rozhodne, či bude SOCaaS nasadený on-premise, v cloude alebo v hybridnom modeli.
2	Prevádzkovateľ pripraví cieľové prostredie – vytvorí potrebné virtuálne stroje, siete, úložiská a ďalšie zdroje v IaaS.
3	Prevádzkovateľ nainštaluje alebo nasadí SOCaaS komponenty v zvolenej forme (napr. VM, Docker kontajnery, cloud/SaaS inštancia).
4	Prevádzkovateľ nastaví centralizovaný monitoring funkčnosti modulov (zber metrik, health-checks, logovanie stavu).
5	Prevádzkovateľ vytvorí testovacie prostredie alebo staging inštanciu, kde sa budú overovať aktualizácie a zmeny konfigurácie.
6	Prevádzkovateľ definuje pravidlá údržby a aktualizácií – okná údržby, poradie nasadzovania zmien a postup rollbacku.
7	Správca alebo Prevádzkovateľ priebežne monitoruje stav nasadenia a podľa potreby pridáva ďalšie zdroje (VM, storage, sieťové prvky) na zabezpečenie výkonu a dostupnosti.

ALT_28_01 – Potreba zmeniť model nasadenia (on-prem → cloud alebo hybrid)	Alternate

K rok	Aktivita
1	Na základe rastu alebo požiadaviek zákazníka sa ukáže, že pôvodné on-prem nasadenie už nevyhovuje; Architekt navrhne prechod na cloud alebo hybridný model, Prevádzkovateľ pripraví nové prostredie a postupný presun komponentov tak, aby zostala zachovaná dostupnosť služby.

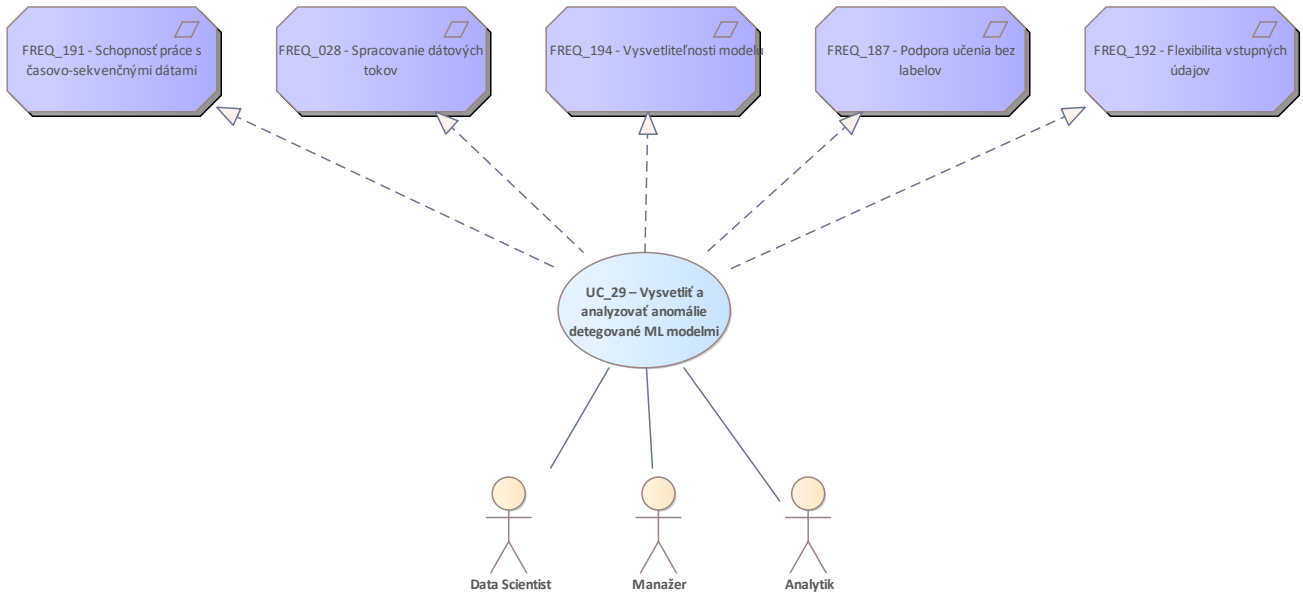
ALT_28_02 – Aktualizácia spôsobí problémy v produkčnom prostredí	Alternate

K rok	Aktivita
1	Po nasadení aktualizácie podľa krokov 5–6 sa zistí, že niektorý modul nefunguje správne; Prevádzkovateľ použije pripravený rollback postup, vráti sa na predošlú verziu a aktualizáciu najprv opraví a otestuje v staging prostredí pred ďalším pokusom.

Naviazané funkčné požiadavky	
FREQ_084 - Bezplatná verzia, open-source riešenie s možnosťou rozšírenia	Dostupnosť základnej funkcionality bez licencie a možnosť rozšírenia. Bezplatná verzia, open-source riešenie s možnosťou rozšírenia

FREQ_069 - Možnosti nasadenia: on-prem, cloud, hybrid	Možnosť nasadenia riešenia v rôznych prostrediach vrátane lokálneho, cloudového alebo hybridného modelu. Možnosti nasadenia: on-prem, cloud, hybrid
FREQ_037 - Podpora IaaS funkcionality	Riešenie vyžaduje plnú funkcionalitu IaaS – správu virtuálnych strojov (VM), diskov, sietí, obrazov, snapshotov a samostatných zdrojov. Platforma musí podporovať vytváranie a správu rôznych typov inštancií, umožniť priradenie zdrojov podľa potreby tenantov a zároveň ponúknuť robustné API rozhranie pre programovateľný prístup. Schopnosť poskytovať kompletnú IaaS funkcionalitu je kľúčová pre zabezpečenie pružného a spoľahlivého prevádzkovania SOC ako služby.
FREQ_093 - Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker	Flexibilita inštalácie do rôznych prostredí. Možnosti nasadenia: on-premise, cloud/SaaS, VM, Docker
FREQ_027 - Údržba a aktualizácia systému	Riešenie musí zabezpečiť údržbu a aktualizáciu systému. Prevádzkový tím musí mať stanovené: • pravidlá pre aktualizácie komponentov • testovacie prostredie na overenie zmien • centralizovaný monitoring funkčnosti všetkých modulov

4.5.2.31 UC_29 – Vysvetliť a analyzovať anomálie detegované ML modelmi



Obrázok 41 : UC_29 – Vysvetliť a analyzovať anomálie detegované ML modelmi

Prípad použitia	UC_29 – Vysvetliť a analyzovať anomálie detegované ML modelmi
Cieľ	UC_29 rieši, aby SOCaaS vedel zrozumiteľne vysvetliť anomálie detegované modelmi strojového učenia: zobraziť kontext dátového toku (logy, metriky, sieťové toky), ukázať časový priebeh signálov, ktoré viedli k anomálii, pracovať s unsupervised modelmi (bez labelov), a dať analytikovi interpretáciu „prečo to model označil“.

Vstupná podmienka	V SOCaaS sú nasadené ML modely na detekciu anomálií (UC_21) a generujú anomálne udalosti/alerty.
Vstupná podmienka	Dátové toky (logy, metriky, sieťové toky) sú spracovávané cez pipeline – validované, normalizované, obohatené a ukladané.
Vstupná podmienka	Používateľ (Analytik, Data Scientist) má prístup k modulu „ML anomálie a vysvetlenia“.
Výstupná podmienka	Pre vybranú anomáliu existuje vysvetlenie detekcie – v čase, nad relevantnými vstupmi a s textovým komentárom.
Výstupná podmienka	Analytik môže označiť výstup modelu (TP/FP) a doplniť komentár, ktorý sa využije ako spätná väzba pre modely.

Basic Path	Basic Path

Krok	Aktivita
1	Analytik otvorí modul „ML anomálie“ a vyberie konkrétnu anomáliu alebo incident, ktorý bol detegovaný ML modelom.
2	Systém načíta z dátového pipeline všetky súvisiace udalosti – logy, metriky a sieťové toky – ktoré prešli validáciou, normalizáciou, obohatením a boli priradené do správnych indexov a časových pečiatok.
3	Systém identifikuje, ktorý ML model anomáliu detegoval (supervised/unsupervised) a načíta jeho výstupy (skóre, prípadne členstvo v klustri).

4	Analytik spustí funkciu „vysvetliť detekciu“ a systém vygeneruje vysvetlenie – kľúčové signály, časové úseky a vlastnosti, ktoré najviac prispeli k rozhodnutiu modelu.
5	Systém zobrazí časový priebeh vybraných metrík a logových udalostí (time series) s vyznačením intervalu, v ktorom bola anomália detegovaná.
6	Systém zobrazí rozklad vstupov podľa typu (logy, metriky, tokové dáta) a ukáže, ktoré skupiny vstupov najviac ovplyvnili detekciu, vrátane prípadu, keď pochádzajú z rôznych zdrojov.
7	Analytik doplní vlastnú interpretáciu, označí detekciu ako „true positive“, „false positive“ alebo „nejasné“ a uloží spätnú väzbu; Data Scientist môže tieto označenia neskôr využiť pri dolaďovaní (aj unsupervised) modelov.

ALT_29_01 – Nedostatočné dáta na vysvetlenie anomálie	Alternate

K rok	Aktivita
1	Pri pokuse o vysvetlenie systém zistí, že v zvolenom časovom úseku chýbajú niektoré logy alebo metriky (dáta neboli uložené alebo spracované); systém upozorní analytika na obmedzené vysvetlenie, zobrazí len dostupné dáta a označí vysvetlenie ako „neúplné“.

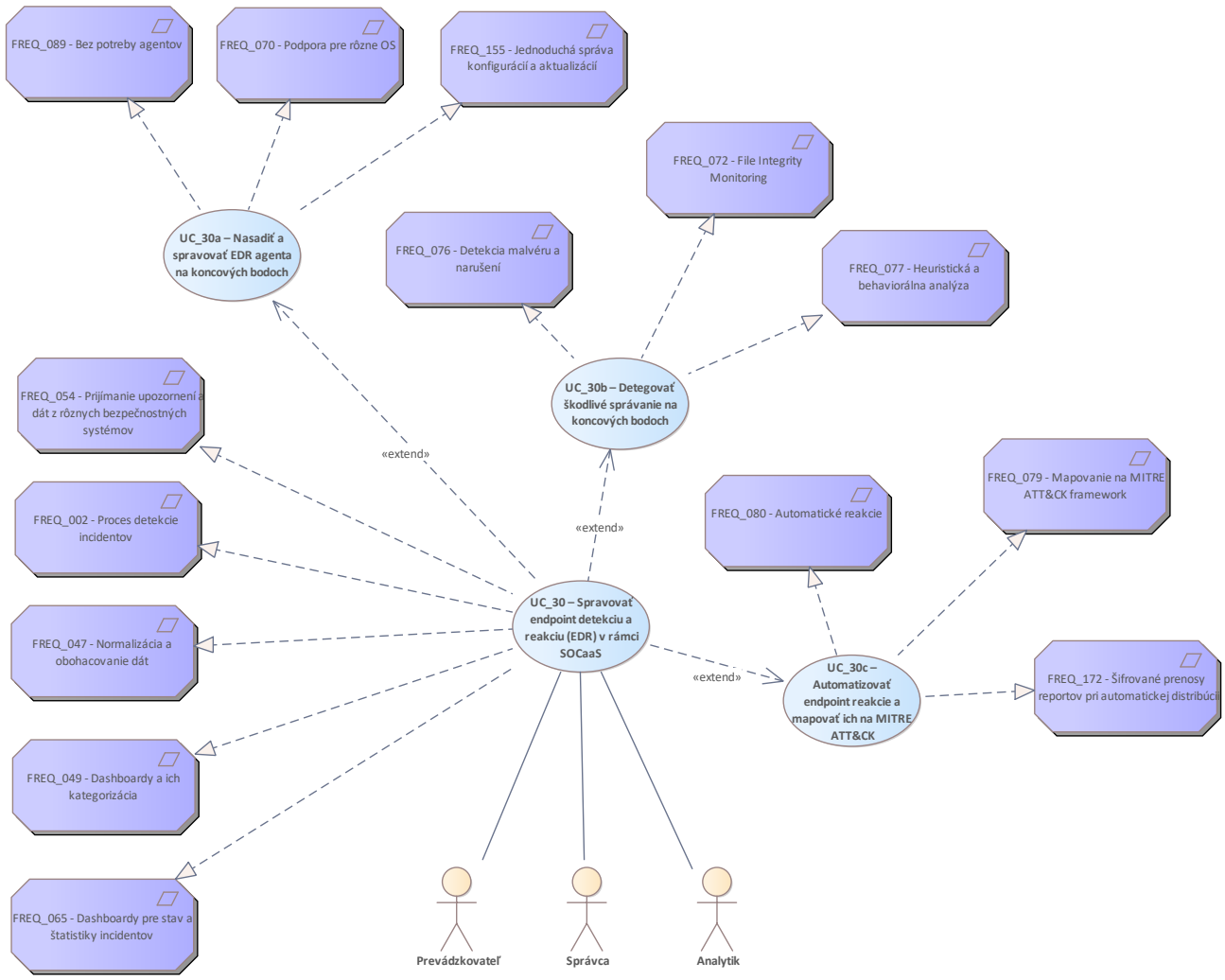
ALT_29_02 – Analytik pretrénuje dôveru v konkrétny model	Alternate

K rok	Aktivita
1	Analytik opakovane označí detegované anomálie z jedného modelu ako „false positive“; systém túto spätnú väzbu agreguje a zobrazí Data Scientistovi odporúčanie pre revíziu modelu (prípadne jeho nahradenie iným typom, vrátane zmeny prahu alebo architektúry).

Naviazané funkčné požiadavky	
FREQ_194 - Vysvetliteľnosti modelu	Riešenie musí mať vysvetliteľný model (interpretability). Možnosť vysvetliť výstup detekcie analytikovi. Možnosť poskytnúť analytikovi zrozumiteľné vysvetlenie, prečo bola anomália detegovaná.
FREQ_191 - Schopnosť práce s časovo-sekvenčnými dátami	Riešenie musí byť schopné práce s časovo-sekvenčnými dátami. Vhodnosť pre dáta s časovým vývojom (napr. logy, sieťová prevádzka). Schopnosť zachytiť dočasné vzory a anomálie v časových radoch. Výhodou sú architektúry ako LSTM, Transformer.

FREQ_192 - Flexibilita vstupných údajov	Riešenie musí byť schopné zabezpečiť flexibilitu vstupných údajov (logy, metriky, tokové dáta). Koľko typov dát model zvládne bez potreby úpravy architektúry. Model musí vedieť pracovať so štruktúrovanými i neštruktúrovanými vstupmi – logy, metriky, sieťové toky.
FREQ_028 - Spracovanie dátových tokov	Riešenie musí zabezpečiť spracovanie dátových tokov. Hlavné úlohy spracovania dátových tokov sú: • Príjem logov a udalostí z viacerých heterogénnych zdrojov • Validácia, normalizácia a obohatenie dát • Priradenie časových pečiatok, identifikátorov a kategórií udalostí • Presmerovanie dát do vhodných indexov pre efektívnu analýzu • Odfiltrovanie redudantných alebo irelevantných údajov • Implementácia pipeline pravidiel a spracovateľských modulov
FREQ_187 - Podpora učenia bez labelov	Riešenie musí zabezpečiť podporu učenia bez labelov (unsupervised). Schopnosť učiť sa zo vstupných dát bez potreby anotácií. Nie všetky modely vyžadujú označené dáta. Unsupervised modely sú výhodné najmä pri veľkých množstvách nelabelovaných údajov.
UC_29 – Vysvetliť a analyzovať anomálie detegované ML modelmi	UC_29 rieši, aby SOCaaS vedel zrozumiteľne vysvetliť anomálie detegované modelmi strojového učenia: zobraziť kontext dátového toku (logy, metriky, sieťové toky), ukázať časový priebeh signálov, ktoré viedli k anomálii, pracovať s unsupervised modelmi (bez labelov), a dať analytikovi interpretáciu „prečo to model označil“.

4.5.2.32 UC_30 – Spravovať endpoint detekciu a reakciu (EDR) v rámci SOCaaS



Obrázok 42 : UC_30 – Spravovať endpoint detekciu a reakciu (EDR) v rámci SOCaaS

Prípad použitia	UC_30 – Spravovať endpoint detekciu a reakciu (EDR) v rámci SOCaaS

Cieľ	UC_30 rieši, ako SOCaaS centrálne riadi EDR/XDR vrstvu: prijíma alerty a logy z EDR/antivírus/OS nástrojov, normalizuje a obohacuje ich, zobrazuje stav incidentov na dashboardoch, napája ich na celkový proces detekcie incidentov (UC_03) a reakcie (UC_07).

Vstupná podmienka	Na koncových bodoch zákazníka je nasadený EDR/AV/host-based senzor (alebo integračný agent).
Vstupná podmienka	SOCaaS má integračné konektory na zber logov a alertov z EDR a ďalších bezpečnostných nástrojov.
Vstupná podmienka	Sú definované základné korelačné pravidlá a heuristiky pre detekciu endpointových incidentov.
Výstupná podmienka	Alerty a logy z endpoint nástrojov sú prijaté, normalizované a obohatené a využité v detekcii incidentov.
Výstupná podmienka	Stav endpoint incidentov je prehľadne zobrazovaný na dashboardoch pre analytikov a manažment.
Výstupná podmienka	Endpoint incidenty sú napojené na automatizované reakcie (UC_07), ak je to povolené politikou.

Basic Path	Basic Path

Krok	Aktivita
1	Prevádzkovateľ nakonfiguruje integráciu EDR/AV nástroja so SOCaaS a definuje, ktoré typy alertov a logov sa majú odosielať.
2	Systém prijíma alerty a dáta z rôznych bezpečnostných nástrojov (EDR, AV, OS logy) a zaraďuje ich do jednotného pipeline spracovania.
3	Pipeline transformuje rôzne logy z endpointov do jednotného formátu, dopĺňa WHOIS/GEOIP a ďalší kontext a ukladá ich do vhodných indexov pre koreláciu.
4	Detekčný engine (UC_03) používa normalizované endpoint dáta v korelačných pravidlách a heuristike na identifikáciu potenciálnych incidentov.
5	Keď vznikne incident s pôvodom na koncovom bode, systém ho zobrazí na dashboardoch spolu s kontextom (host, používateľ, typ hrozby, časová os).

6	Analytik pracuje s endpoint incidentom priamo v SOCaaS – filtruje, triedi, drill-down do detailu logov a obohatenia, prípadne manuálne eskaluje alebo uzatvára.
7	Ak je pre daný typ incidentu definovaný playbook, SOCaaS vyvolá UC_07 a ponúkne automatizované alebo poloautomatizované reakcie (izolácia, karanténa, blokovanie).

ALT_30_01 – Neúplná alebo chybná integrácia EDR	Alternate

K rok	Aktivita
1	EDR nástroj neodosiela všetky očakávané typy alertov alebo logov; systém upozorní Prevádzkovateľa, že z daného zdroja prichádzajú len čiastkové údaje, a odporučí skontrolovať konfiguráciu alebo oprávnenia.

ALT_30_02 – Prebytok endpoint alertov (alert fatigue)	Alternate

K rok	Aktivita
1	Po napojení EDR príde extrémne veľké množstvo alertov nízkej závažnosti; Analytik a Prevádzkovateľ upravia filtre, korelačné pravidlá a prahy tak, aby sa na dashboardoch zobrazovali len relevantné incidenty a zvyšok zostal ako nízko-prioritné udalosti v pozadí.

Naviazané funkčné požiadavky	
FREQ_049 - Dashboardy a ich kategorizácia	Vizualizácia údajov pomocou grafov, filtrov a widgetov. Dashboardy (vrátane interaktívnych) a ich kategorizácia
UC_30c – Automatizovať endpoint reakcie a mapovať ich na MITRE ATT&CK	UC_30c rieši automatizované/poloautomatizované reakcie na endpoint incidenty a ich mapovanie na MITRE ATT&CK: izolácia zariadenia, karanténa súboru, blokovanie procesov, prepojenie so SOAR playbookmi, bezpečný prenos forenzných dát a reportov.
FREQ_065 - Dashboardy pre stav a štatistiky incidentov	Prehľadné zobrazenie stavu systému a prebiehajúcich incidentov. Dashboardy pre stav a štatistiky incidentov

UC_30b – Detegovať škodlivé správanie na koncových bodoch	UC_30b rieši samotnú detekciu malvéru, narušení a podozrivého správania na endpointoch: FIM (File Integrity Monitoring), detekciu malvéru, heuristickú/behaviorálnu analýzu.
UC_30a – Nasadiť a spravovať EDR agenta na koncových bodoch	UC_30a rieši nasadenie a životný cyklus EDR agenta / senzora: inštaláciu na rôzne OS, aktualizácie a konfiguráciu, prípadne využitie agentless režimu tam, kde agent nie je možný
FREQ_002 - Proces detekcie incidentov	Zabezpečiť proces detekcie incidentov – je zodpovedný za identifikáciu anomálií, vzorcov útokov a iných hrozieb prostredníctvom korelačných pravidiel a heuristických mechanizmov.
FREQ_047 - Normalizácia a obohacovanie dát	Transformácia rôznych logov do jednotného formátu a ich rozšírenie (napr. WHOIS, GEOIP). Normalizácia a obohacovanie dát
FREQ_054 - Prijímanie upozornení a dát z rôznych bezpečnostných systémov	Schopnosť prijímať alerty a dáta z rôznych bezpečnostných zdrojov (SIEM, EDR, CTI...). Prijímanie upozornení a dát z rôznych bezpečnostných systémov

Prípad použitia	UC_30a – Nasadiť a spravovať EDR agenta na koncových bodoch
Cieľ	UC_30a rieši nasadenie a životný cyklus EDR agenta / senzora: inštaláciu na rôzne OS, aktualizácie a konfiguráciu, prípadne využitie agentless režimu tam, kde agent nie je možný

Vstupná podmienka	Je vybraný EDR/endpoint nástroj, ktorý bude použitý v SOCaaS.
Vstupná podmienka	Sú k dispozícii zoznamy koncových bodov a ich OS.
Výstupná podmienka	EDR agent je nasadený alebo nakonfigurovaný (aj v agentless režime) na relevantných koncových bodoch.
Výstupná podmienka	Konfigurácie a aktualizácie agentov sa spravujú centrálne bez zásahov do kódu.

Basic Path	Basic Path

Krok	Aktivita
1	Správca získa prehľad koncových bodov a ich operačných systémov, ktoré majú byť monitorované.
2	Prevádzkovateľ pripraví inštalačné balíčky alebo politiky pre nasadenie EDR agenta na podporované OS.
3	Správca nasadí agenta (alebo nakonfiguruje agentless pripojenie) na vybrané koncové body podľa politiky zákazníka.
4	Prevádzkovateľ centrálne nastaví konfiguráciu agentov – aké logy zbierať, aké moduly sú aktívne a ako často odosielať dáta.
5	Systém zabezpečí distribúciu aktualizácií agentov a konfigurácií bez potreby meniť kód alebo manuálne zasahovať na každom zariadení.

ALT_30a_01 - Agent nie je možné nainštalovať	Alternate

Krok	Aktivita
1	Na niektoré zariadenia (napr. špeciálne servery, OT zariadenia) nie je možné agenta nainštalovať; Prevádzkovateľ aktivuje agentless režim (napr. zber logov cez syslog, WMI, API) a označí tieto zariadenia v systéme ako „agentless“.

Naviazané funkčné požiadavky	
FREQ_070 - Podpora pre rôzne OS	Podpora pre inštaláciu a beh agenta na rôznych operačných systémoch. Podpora pre rôzne OS (Windows, Linux, macOS)
FREQ_155 - Jednoduchá správa konfigurácií a aktualizácií	Schopnosť spravovať platformu bez potreby zásahu do kódu. Jednoduchá správa konfigurácií a aktualizácií
FREQ_089 - Bez potreby agentov	Možnosť realizovať skeny bez nutnosti inštalovať agenta na zariadenia. Bez potreby agentov (agentless)

UC_30a – Nasadiť a spravovať EDR agenta na koncových bodoch	UC_30a rieši nasadenie a životný cyklus EDR agenta / senzora: inštaláciu na rôzne OS, aktualizácie a konfiguráciu, prípadne využitie agentless režimu tam, kde agent nie je možný
Prípad použitia	UC_30b – Detegovať škodlivé správanie na koncových bodoch
Cieľ	UC_30b rieši samotnú detekciu malvéru, narušení a podozrivého správania na endpointoch: FIM (File Integrity Monitoring), detekciu malvéru, heuristickú/behaviorálnu analýzu.

Vstupná podmienka	Na koncových bodoch beží EDR/agent (UC_30a).
Vstupná podmienka	Sú definované politiky, ktoré typy správania sa majú považovať za podozrivé.
Výstupná podmienka	Podozrivé správanie (malvér, narušenia, FIM udalosti) je detegované a mapované na incidenty v SOCaaS.

Basic Path	Basic Path

Krok	Aktivita
1	EDR agent monitoruje zmeny súborov, procesov a systémových volaní na koncovom bode.
2	Pri podozrivej zmene súboru (napr. systémový binár, kritická konfigurácia) vytvorí FIM udalosť a odošle ju do SOCaaS.
3	EDR engine analyzuje správanie procesov a pamäte, aby identifikoval znaky malvéru alebo narušenia bezpečnosti.

4	Heuristické a behaviorálne pravidlá (prípadne modely) vyhodnotia kombináciu udalostí a určia, či ide o podozrivú aktivitu.
5	Pri prekročení prahov alebo zodpovedajúcom vzore EDR vytvorí alert, ktorý je následne spracovaný v UC_30/UC_03 ako incident alebo kandidát na incident.

ALT_30b_01 - Podozrivé správanie bez jednoznačného verdiktu	Alternate

K rok	Aktivita
1	Heuristika vyhodnotí aktivitu ako podozrivú, ale nie dostatočne silnú na automatickú klasifikáciu; EDR odošle „low confidence“ alert, ktorý je na dashboarde zobrazený ako nízko prioritná udalosť na manuálne posúdenie analytikom.

Naviazané funkčné požiadavky	
FREQ_077 - Heuristická a behaviorálna analýza	Založenie detekcie na správaní a heuristike namiesto len signatúr. Heuristická a behaviorálna analýza
FREQ_072 - File Integrity Monitoring	Detekcia zmeny súborov v reálnom čase pre účely forenznej analýzy a integrity. File Integrity Monitoring (FIM)
FREQ_076 - Detekcia malvéru a narušení	Identifikácia škodlivého softvéru a incidentov narušenia bezpečnosti. Detekcia malvéru a narušení
UC_30b – Detegovať škodlivé správanie na koncových bodoch	UC_30b rieši samotnú detekciu malvéru, narušení a podozrivého správania na endpointoch: FIM (File Integrity Monitoring), detekciu malvéru, heuristickú/behaviorálnu analýzu.

Prípad použitia	UC_30c – Automatizovať endpoint reakcie a mapovať ich na MITRE ATT&CK
Cieľ	UC_30c rieši automatizované/poloautomatizované reakcie na endpoint incidenty a ich mapovanie na MITRE ATT&CK: izolácia zariadenia, karanténa súboru, blokovanie procesov, prepojenie so SOAR playbookmi, bezpečný prenos forenzných dát a reportov.

Vstupná podmienka	Pre endpoint typy incidentov sú definované playbooky reakcie (UC_07).
Vstupná podmienka	EDR nástroj podporuje automatické akcie na koncových bodoch (izolácia, karanténa, blokovanie).
Vstupná podmienka	SOCaaS má mapovanie aktivít na MITRE ATT&CK.
Výstupná podmienka	Endpoint incidenty sú mapované na ATT&CK TTP a použité v reportoch a CTI.
Výstupná podmienka	Automatizované reakcie sú vykonané bezpečne a auditovateľne, vrátane bezpečného prenosu reportov a forenzných dát.

Basic Path	Basic Path

Krok	Aktivita
1	Analytik alebo systém identifikuje endpoint incident, pri ktorom je vhodná automatizovaná reakcia (napr. malvér na koncovej stanici).
2	SOCaaS priradí incidentu relevantné MITRE ATT&CK techniky a zobrazuje ich v detaile incidentu.
3	Analytik spustí playbook alebo systém automaticky vyhodnotí podmienky a vykoná akciu (izolácia zariadenia, karanténa súboru, zablokovanie procesu).
4	EDR odošle potvrdenie o výsledku akcie späť do SOCaaS, kde sa aktualizuje stav incidentu a zaznamenajú sa vykonané kroky.
5	Systém vygeneruje súhrnný report o priebehu incidentu a vykonaných reakciách a bezpečne ho odošle cez šifrovaný kanál (napr. manažérovi alebo zákazníkovi).

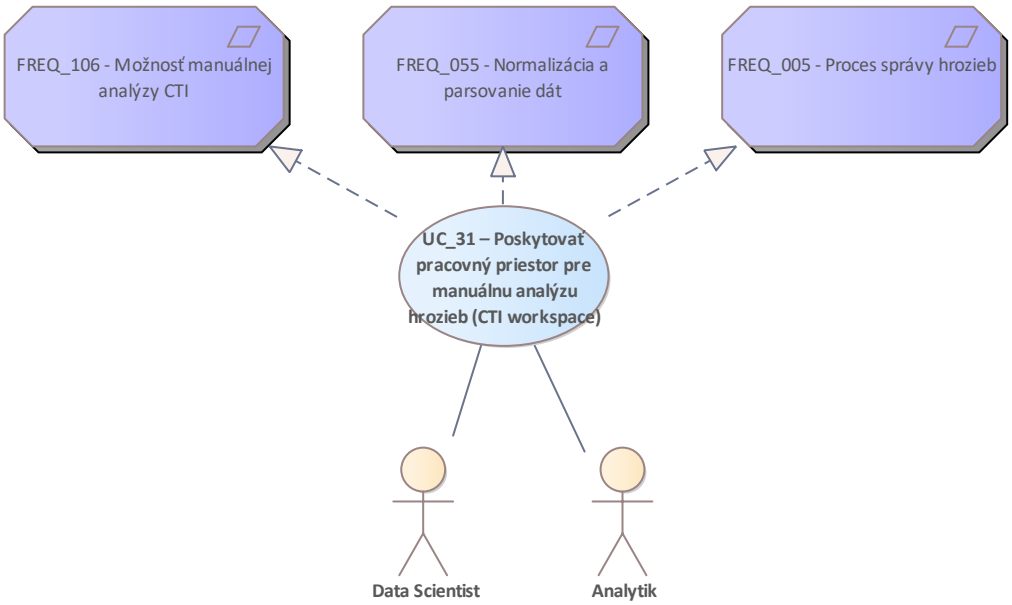
ALT_30c_01 - Automatizovaná reakcia je zablokovaná politikou	Alternate

Krok	Aktivita
1	Manažér nastavil politiku, že na kritických serveroch nie je dovolená plne automatická izolácia; pri takom incidente SOCaaS ponúkne len „poloautomatickú“ akciu vyžadujúcu explicitné potvrdenie analytikom.

Naviazané funkčné požiadavky	
FREQ_172 - Šifrované prenosy reportov pri automatickej distribúcii	Bezpečný prenos citlivých dát cez šifrované kanály. Šifrované prenosy reportov pri automatickej distribúcii
FREQ_079 - Mapovanie na MITRE ATT&CK framework	Zaradenie detegovaných aktivít a techník do rámca MITRE ATT&CK pre účely TTP analýz. Mapovanie na MITRE ATT&CK framework

FREQ_080 - Automatické reakcie	Automatická reakcia na incidenty, ako je izolácia koncového bodu alebo karanténa súborov. Automatické reakcie (napr. izolácia zariadenia, karanténa súboru)
UC_30c – Automatizovať endpoint reakcie a mapovať ich na MITRE ATT&CK	UC_30c rieši automatizované/poloautomatizované reakcie na endpoint incidenty a ich mapovanie na MITRE ATT&CK: izolácia zariadenia, karanténa súboru, blokovanie procesov, prepojenie so SOAR playbookmi, bezpečný prenos forenzných dát a reportov.

4.5.2.33 UC_31 – Poskytovať pracovný priestor pre manuálnu analýzu hrozieb (CTI workspace)



Obrázok 43 : UC_31 – Poskytovať pracovný priestor pre manuálnu analýzu hrozieb (CTI workspace)

Prípad použitia	UC_31 – Poskytovať pracovný priestor pre manuálnu analýzu hrozieb (CTI workspace)
Cieľ	UC_31 rieši, aby SOCaaS poskytoval dedikovaný pracovný priestor pre manuálnu analýzu hrozieb (CTI): analytik si vie otvoriť konkrétnu hrozbu, IOC alebo kampaň, vidí znormalizované dáta z viacerých CTI zdrojov, má nástroje na ručné skúmanie, filtrovanie a dopĺňanie komentárov.

Vstupná podmienka	CTI pipeline je funkčná (UC_25) – CTI dáta sú stiahnuté a technicky spracované.
Vstupná podmienka	Používateľ má rolu, ktorá mu umožňuje pracovať s CTI dátami (čítanie, komentáre, označenia).
Výstupná podmienka	Pre vybrané hrozby / IOC existujú ručne doplnené analýzy a komentáre od analytika.
Výstupná podmienka	Výsledky manuálnej analýzy sú uložené tak, aby ich bolo možné použiť v incidentoch, hunting prípadoch a ďalšom CTI spracovaní.

Basic Path	Basic Path

Krok	Aktivita
1	Analytik otvorí modul „CTI workspace“ a vyhľadá hrozbu, IOC alebo kampaň, ktorú chce analyzovať.
2	Systém načíta z CTI úložísk všetky dostupné informácie o danej hrozbe – IOC, popisy, zdrojové feedy – a zobrazí ich v jednotnom, normalizovanom formáte.
3	Analytik použije dostupné nástroje (filtrovanie, pivotovanie na IOC, prepojenie na incidenty a logy) na ručné preskúmanie dát a kontextu hrozby.
4	Analytik doplní vlastné komentáre, hodnotenie relevancie, odporúčania a prípadne označí hrozbu pre konkrétnych zákazníkov/segmenty.
5	Systém uloží výsledok manuálnej analýzy ako súčasť CTI záznamu a sprístupní ho v súvisiacich incidentoch, hunting prípadoch a reportoch.

ALT_31_01 – CTI dáta pre hrozbu sú neúplné alebo nekonzistentné	Alternate

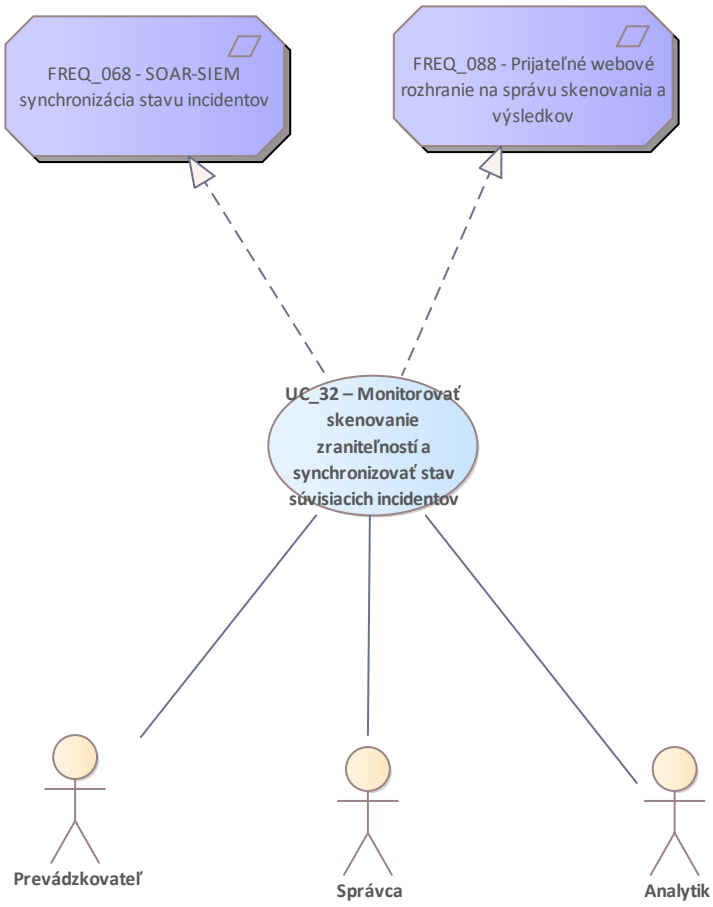
K rok	Aktivita
1	Analytik v kroku 2 zistí, že informácie o hrozbe z rôznych zdrojov si odporujú alebo sú neúplné; označí záznam ako „vyžaduje doplnenie“, doplní manuálne poznámky a CTI špecialista neskôr upraví zdroje alebo scoring.

ALT_31_02 – Analytik otvorí CTI workspace priamo z incidentu	Alternate

K rok	Aktivita
1	Pri vyšetrovaní incidentu v UC_06 klikne na prepojenú hrozbu/IOC; systém otvorí CTI workspace už predfiltrovaný na relevantné IOC a kampaň, aby analytik nemusel manuálne vyhľadávať.

Naviazané funkčné požiadavky	
FREQ_005 - Proces správy hrozieb	Zabezpečiť proces správy hrozieb (Threat Intelligence) – umožňuje systematickú prácu s informáciami o hrozbách.
FREQ_055 - Normalizácia a parsovanie dát	Transformácia vstupných dát do štandardizovaného formátu pre ďalšie spracovanie. Normalizácia a parsovanie dát
FREQ_106 - Možnosť manuálnej analýzy CTI	Rozhranie a nástroje pre bezpečnostných analytikov na ručné skúmanie dát. Možnosť manuálnej analýzy CTI

4.5.2.34 UC_32 – Monitorovať skenovanie zraniteľností a synchronizovať stav súvisiacich incidentov



Obrázok 44 : UC_32 – Monitorovať skenovanie zraniteľností a synchronizovať stav súvisiacich incidentov

Prípad použitia	UC_32 – Monitorovať skenovanie zraniteľností a synchronizovať stav súvisiacich incidentov

Cieľ	UC_32 rieši operatívny pohľad na skenovanie zraniteľností a súvisiace incidenty: poskytuje webové rozhranie na správu skenov a výsledkov (nad funkciami z UC_23), zobrazuje, ktoré nálezy boli už prekonvertované na incidenty, a zabezpečuje synchronizáciu stavu incidentov medzi SIEM a SOAR, aby mali analytici všade konzistentný stav.

Vstupná podmienka	Skenovanie zraniteľností je technicky nastavené a beží podľa UC_23.
Vstupná podmienka	Existuje integračné napojenie medzi SIEM a SOAR (podľa UC_24).
Vstupná podmienka	Používateľ má oprávnenie pristupovať k modulu „Skenovanie a incidenty“.
Výstupná podmienka	Používatelia majú k dispozícii prehľadné webové rozhranie, cez ktoré vidia skeny, ich stav a výsledky.
Výstupná podmienka	Nálezy zo skenovania, ktoré sú spracované ako incidenty, majú synchronizovaný stav medzi SIEM a SOAR (napr. „open / in progress / resolved“).

Basic Path	Basic Path

Krok	Aktivita
1	Analytik alebo Správca otvorí modul „Skenovanie a incidenty“ vo webovom rozhraní SOCaaS a vidí prehľad spustených a plánovaných skenov.
2	Používateľ si vyberie konkrétny sken a zobrazí detail – rozsah, čas spustenia, stav, počet nájdených zraniteľností a základné štatistiky.
3	V tom istom rozhraní si používateľ zobrazí zoznam nálezov skenovania, pričom každý nález je prepojený na svoj aktuálny stav (nový, v riešení, uzatvorený) a informáciu, či k nemu už existuje incident v SIEM/SOAR.
4	Systém zobrazuje, pre ktoré nálezy bol vytvorený incident v SOAR a automaticky overuje, aký stav má tento incident v SIEM (napr. „open“, „assigned“, „resolved“).
5	Pri zmene stavu incidentu v SOAR (napr. po vykonaní playbooku) modul UC_32 cez integračnú vrstvu aktualizuje stav incidentu aj v SIEM, aby mali analytici a manažment všade konzistentnú informáciu.

6	Analytik môže z GUI filtrovať nálezy podľa stavu incidentu (napr. „kritické nálezy bez incidentu“ alebo „incidenty v riešení“) a tým prioritizovať ďalšie kroky.
ALT_32_01 – Incident v SOAR existuje, ale SIEM stav nepozná	Alternate
K rok	Aktivita
1	Pri kroku 4 systém zistí, že v SOAR existuje incident nad konkrétnym nálezom, ale v SIEM sa nenachádza korešpondujúci záznam (napr. integračná chyba alebo historický incident); systém nález označí ako „nekonzistentný“ a upozorní Prevádzkovateľa, aby skontroloval integračné pravidlá alebo manuálne zarovnal incidenty.
ALT_32_02 – Webové rozhranie nedokáže zobraziť časť skenov alebo výsledkov	Alternate
K rok	Aktivita
1	Pri načítaní prehľadu v kroku 1 alebo 2 dôjde k chybe v API (napr. skener nedostupný); UI zobrazí upozornenie, ktoré skeny/výsledky sa nepodarilo načítať, a ponechá zvyšok prehľadu funkčný, pričom umožní neskoršie obnovenie zobrazenia.
Naviazané funkčné požiadavky	
FREQ_088 - Prijateľné webové rozhranie na správu skenovania a výsledkov	Použiteľnosť GUI pre správu skenov a výsledkov. Prijateľné webové rozhranie na správu skenovania a výsledkov
FREQ_068 - SOAR-SIEM synchronizácia stavu incidentov	Prepojenie stavu incidentov medzi SIEM a SOAR pre aktuálnu viditeľnosť. SOAR-SIEM synchronizácia stavu incidentov

4.6 Biznis architektúra

4.7 Business Viewpoints

4.7.1 Detekcia a korelácia bezpečnostných udalostí (SIEM) - biznis realizácia služby

4.7.2 Riadenie automatizácie reakcie (SOAR) – biznis realizácia služby

4.7.3 Riadenie reakcie na hrozby (EDR/XDR) - biznis realizácia služby

4.7.4 Monitorovanie zraniteľností – biznis realizácia služby

4.7.5 Správa spravodajstva o hrozbách (CTI) - biznis realizácia služby

4.7.6 Inventarizácia aktív – biznis pohľad

4.7.7 Manažovanie kybernetických bezpečnostných incidentov – biznis realizácia služby

4.7.8 Riadenie reportovania bezpečnosti - biznis realizácia služby

4.7.9 Riadenie znalostného portálu pre SOC tím - biznis realizácia služby

4.7.10 Identifikácia vlastníkov dizajnu koncových služieb (UX)

Meno apriezvisko	Pracovné zaradenie	Telefón	E-mail

Tabuľka 7 : Identifikácia vlastníkov dizajnu koncových služieb (UX)

4.7.11 Špecifikácia potrieb koncového zákazníka

P opis potreby používateľa	Refer encia na výskum, z ktorej potreba plynie	Ná vrh riešenia potreby	K vantita	Do pad na zákaznícku skúsenosť	Tech nická náročnosť	Biz nis prínos	Pri orita

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.

4.7.12 Návrh prototypov používateľského rozhrania

4.7.13 Návrh vizuálov obrazoviek

5 DÁTOVÁ ARCHITEKTÚRA

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

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.

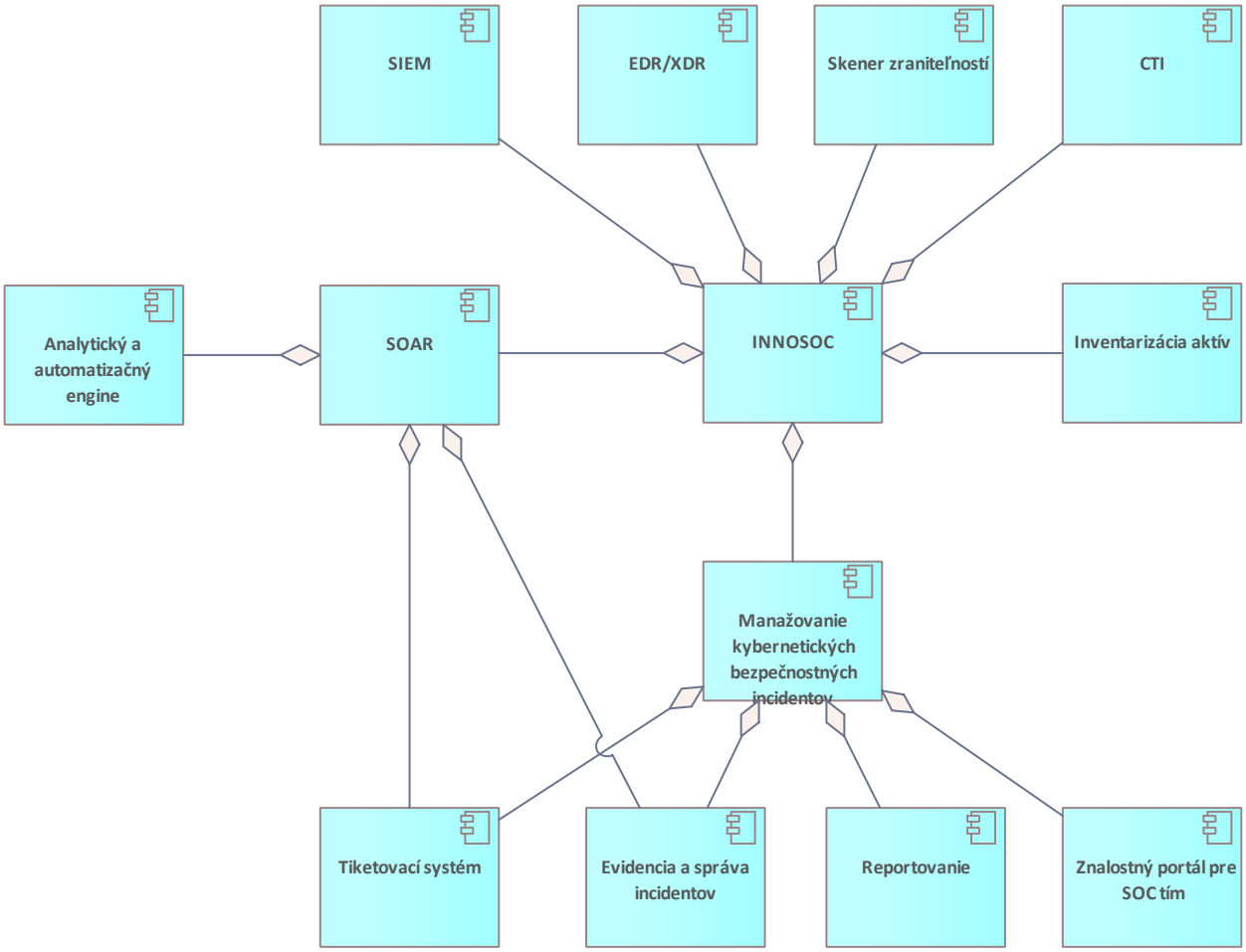
Vnasledujúcej kapitole je zobrazený diagram aplikačnej architektúry spopismi objektov, ktoré boli vygenerované zEA, ako výstup.

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 45 : Aplication Viewpoints Components

Diagram predstavuje HL zoznam aplikačných komponentov riešenia.

Popis používaných prvkov:

Analytický a automatizačný engine

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.

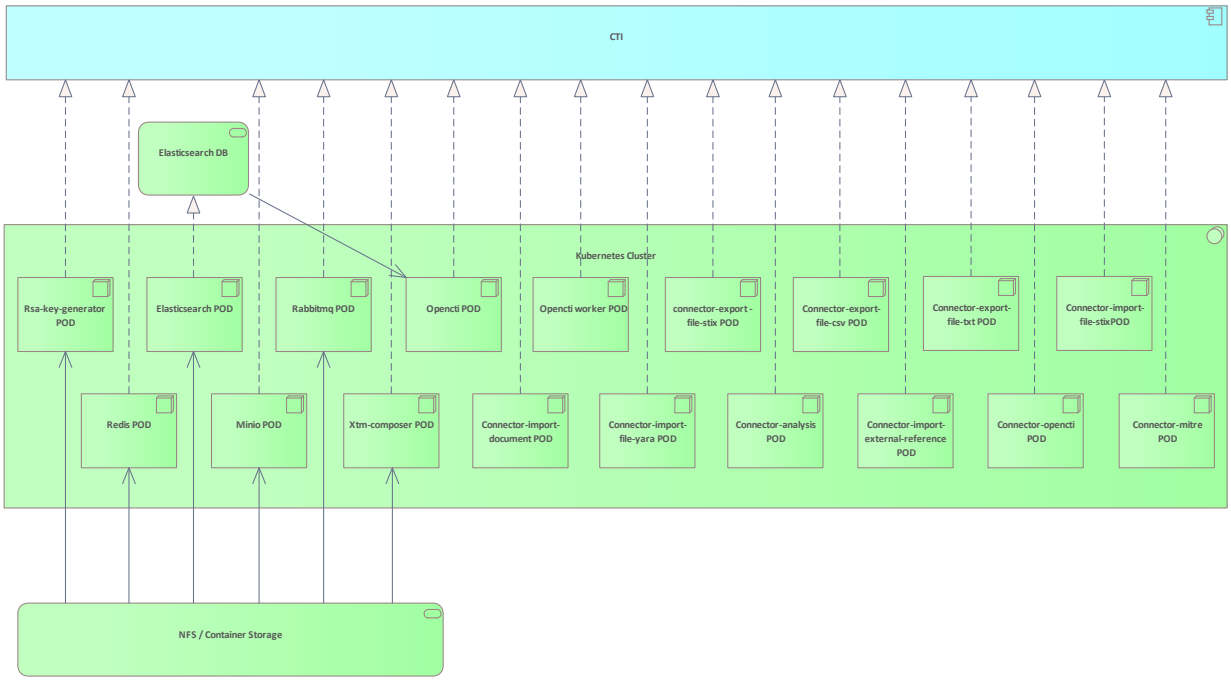
Navrhovaná prevádzka je plánovaná na dvoch identických prostrediach líšiacimi sa len množstvom a typom zdrojov:

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 Návrh technologickej architektúry

7.1.1 Technology Viewpoint CTI



Obrázok 46 : Technology Usage Viewpoint CTI 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 Elasticsearch.

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.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB

Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

Connector-analysis POD

Predstavuje POD connector-analysis.

Connector-export- file-csv POD

Predstavuje POD connector-export-file-csv.

connector-export -file-stix POD

Predstavuje POD connector-export-file-stix.

Connector-export- file-txt POD

Predstavuje POD connector-export-file-txt.

Connector-import- document POD

Predstavuje POD connector-import-document.

Connector-import- external-reference POD

Predstavuje POD connector-import-external-reference.

Connector-import- file-stixPOD

Predstavuje POD connector-import-file-stix.

Connector-import- file-yara POD

Predstavuje POD connector-import-file-yara.

Connector-mitre POD

Predstavuje POD connector-mitre.

Connector-opencti POD

Predstavuje POD connector-opencti.

Minio POD

Predstavuje POD minio.

Opencti POD

Predstavuje POD minio.

Opencti worker POD

Predstavuje POD Opencti worker.

Rabbitmq POD

Predstavuje POD rabbitmq.

Redis POD

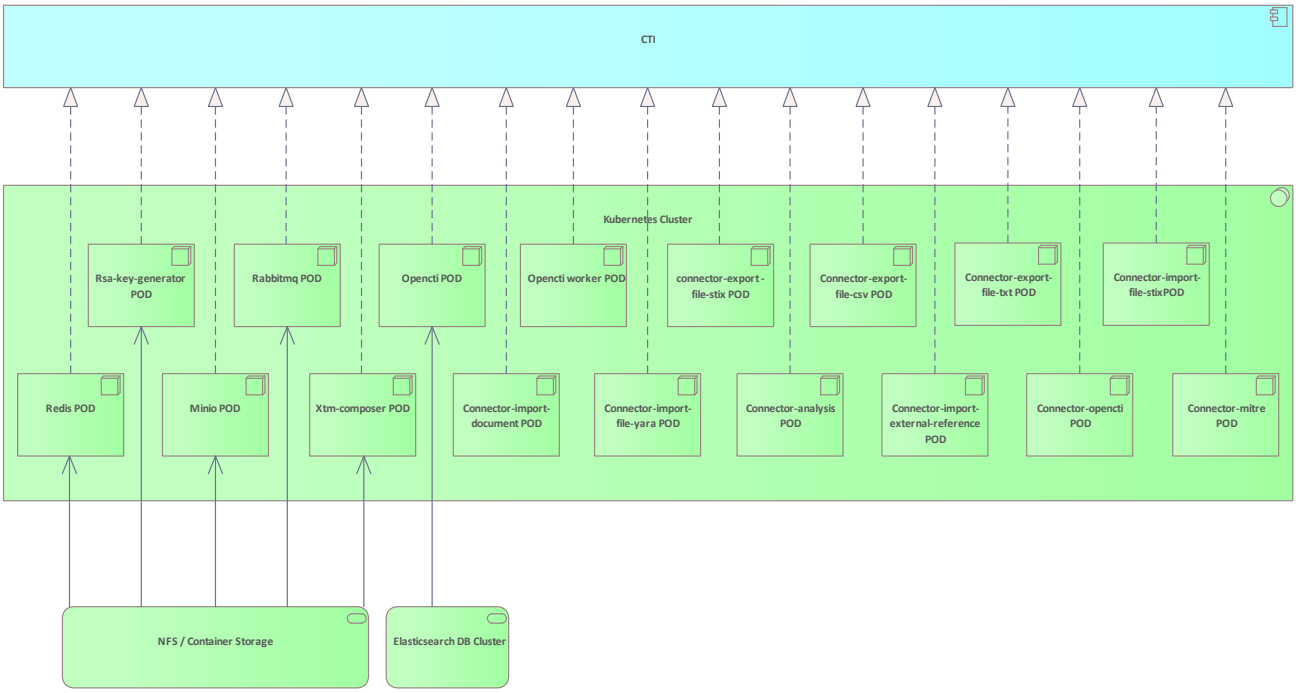
Predstavuje POD redis.

Rsa-key-generator POD

Predstavuje POD rsa-key-generator.

Xtm-composer POD

Predstavuje POD xtm-composer.



Obrázok 47 : Technology Usage Viewpoint CTI 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:

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.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

Connector-analysis POD

Predstavuje POD connector-analysis.

Connector-export- file-csv POD

Predstavuje POD connector-export-file-csv.

connector-export -file-stix POD

Predstavuje POD connector-export-file-stix.

Connector-export- file-txt POD

Predstavuje POD connector-export-file-txt.

Connector-import- document POD

Predstavuje POD connector-import-document.

Connector-import- external-reference POD

Predstavuje POD connector-import-external-reference.

Connector-import- file-stixPOD

Predstavuje POD connector-import-file-stix.

Connector-import- file-yara POD

Predstavuje POD connector-import-file-yara.

Connector-mitre POD

Predstavuje POD connector-mitre.

Connector-opencti POD

Predstavuje POD connector-opencti.

Minio POD

Predstavuje POD minio.

Opencti POD

Predstavuje POD minio.

Opencti worker POD

Predstavuje POD Opencti worker.

Rabbitmq POD

Predstavuje POD rabbitmq.

Redis POD

Predstavuje POD redis.

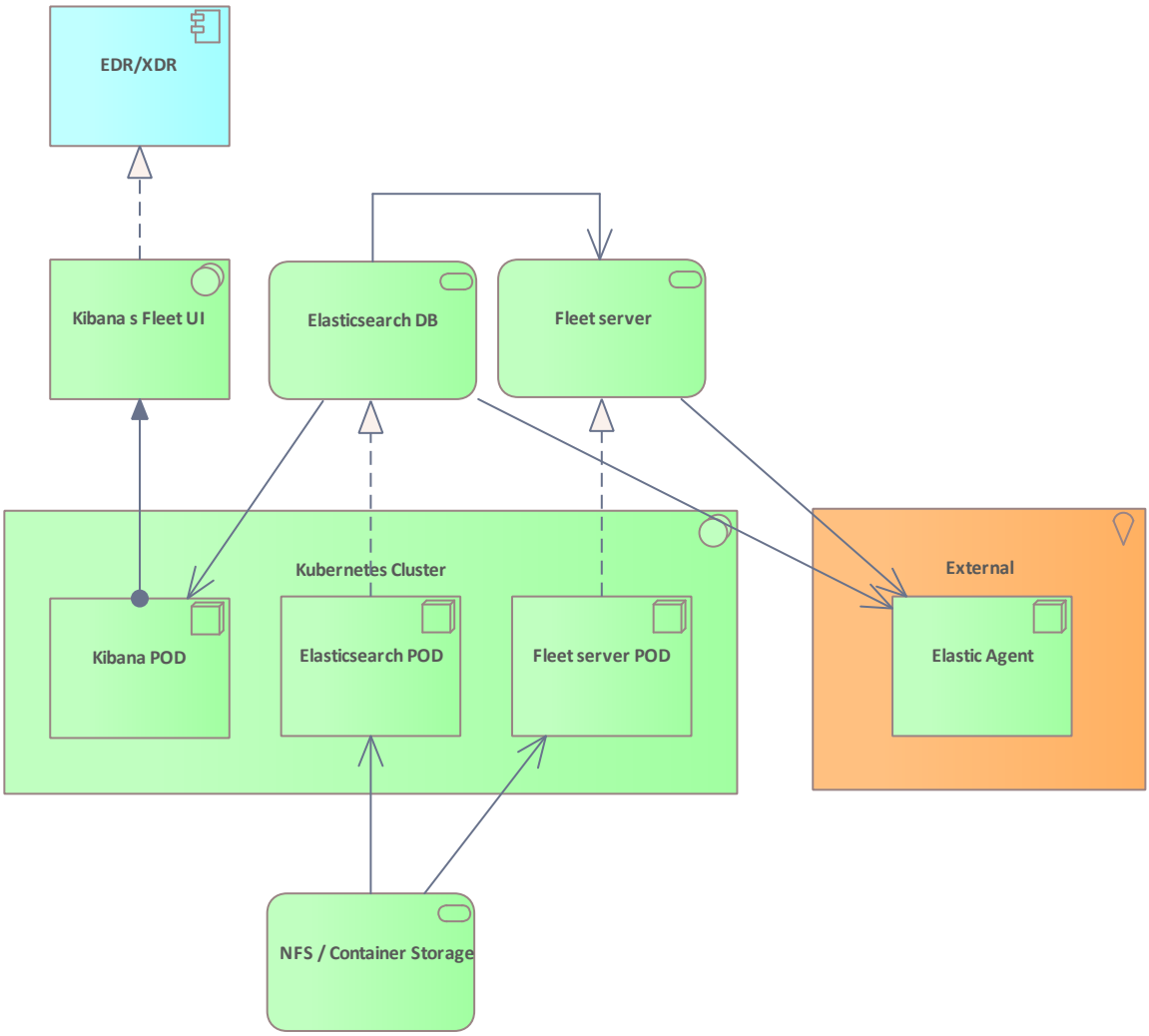
Rsa-key-generator POD

Predstavuje POD rsa-key-generator.

Xtm-composer POD

Predstavuje POD xtm-composer.

7.1.2 Technology Viewpoint EDR/XDR



Obrázok 48 : Technology Usage Viewpoint EDR/XDR 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 Elasticsearch.

Popis používaných prvkov:

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.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB

Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

External

Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

Kibana POD

Predstavuje POD Kibana pre SIEM.

Fleet server

Predstavuje technologickú službu Fleet server pre správu Elastic agents.

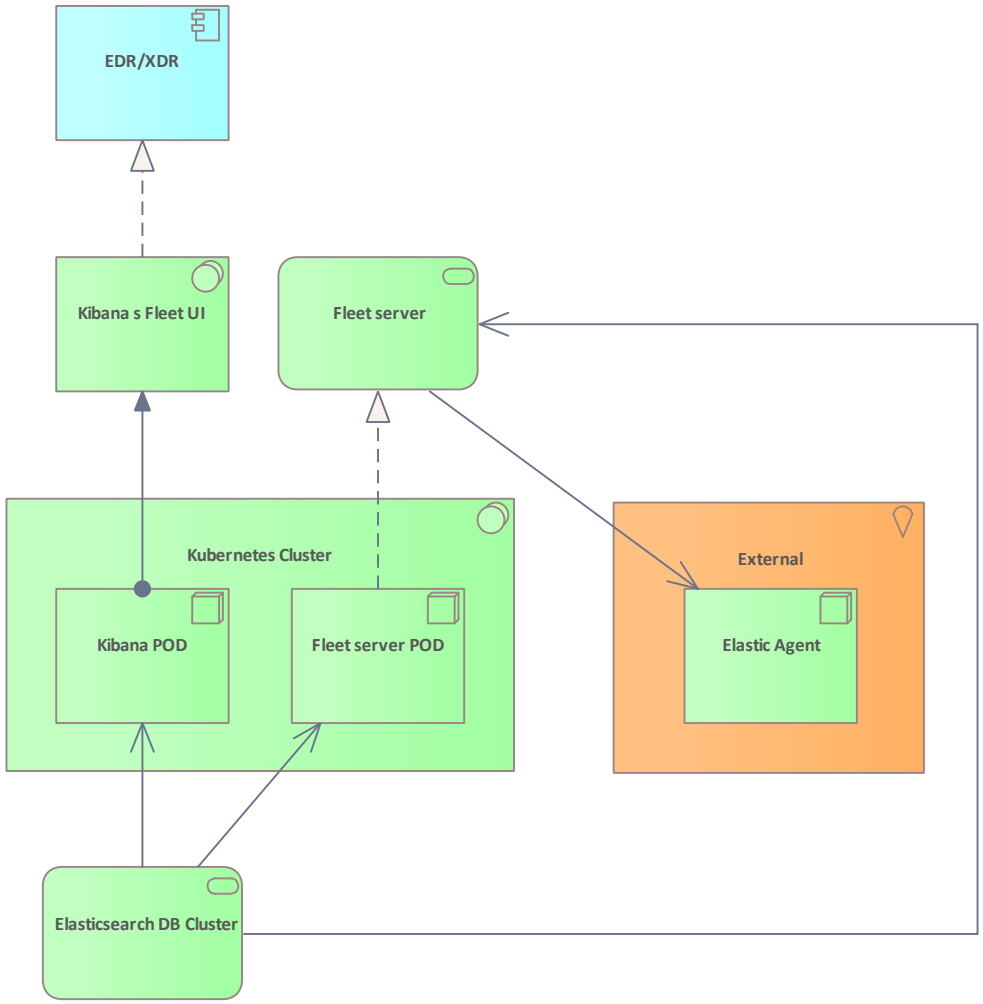
Elastic Agent

Predstavuje inštanciu Elastic Agent pre monitoring a spracovanie logov a ich zapísanie do Elasticsearch a ochranu hosta pred bezpečnostnými hrozbami.

Fleet server POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

Kibana s Fleet UI



Obrázok 49 : Technology Usage Viewpoint EDR/XDR 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:

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.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

External

Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

Kibana POD

Predstavuje POD Kibana pre SIEM.

Fleet server

Predstavuje technologickú službu Fleet server pre správu Elastic agents.

Elastic Agent

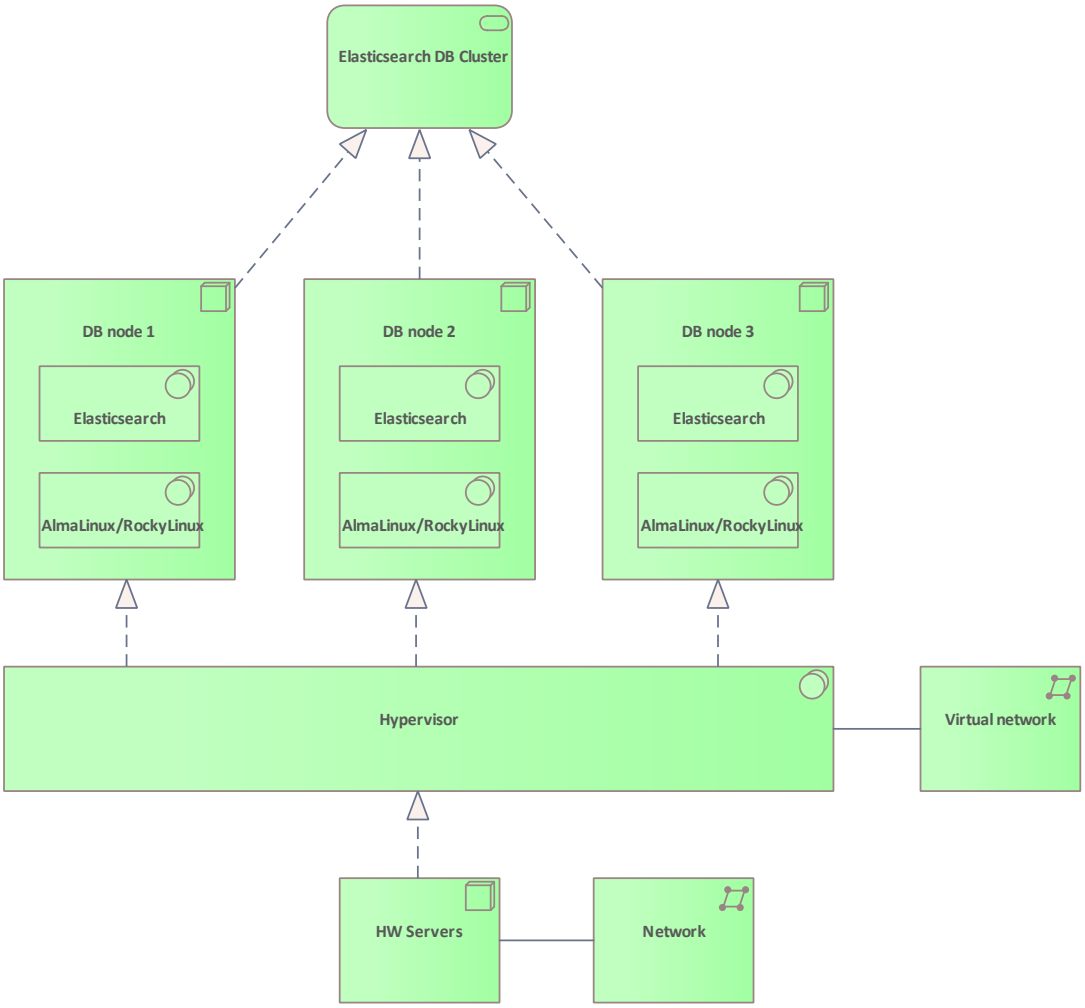
Predstavuje inštanciu Elastic Agent pre monitoring a spracovanie logov a ich zapísanie do Elasticsearch a ochranu hosta pred bezpečnostnými hrozbami.

Fleet server POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

Kibana s Fleet UI

7.1.3 Technology Viewpoint INNOSOC Common



Obrázok 50 : Technology Viewpoint DB Cluster

Diagram znázorňuje technologickú architektúru PostgreSQL Clustra.

Popis používaných prvkov:

DB node 1

Predstavuje Node 1 Elasticsearch Clustra.

DB node 2

Predstavuje Node 2 Elasticsearch Clustra.

DB node 3

Predstavuje Node 3 Elasticsearch Clustra.

HW Servers

Predstavuje HW serverovú infraštruktúru. HW serverová infraštruktúra predstavuje fyzické výpočtové a sieťové vybavenie, ktoré tvorí základ pre prevádzku IT systémov, vrátane serverov, úložísk, prepínačov, smerovačov a záložných zdrojov napájania. Táto infraštruktúra je nasadzovaná buď on-premise alebo ako súčasť cloudovej platformy, a poskytuje výpočtový výkon, dostupnosť a konektivitu pre virtualizované aj nevirtualizované prostredia.

Hypervisor

Predstavuje Hypervisor 1. alebo 2. typu. Hypervisor 1. typu, známy aj ako "bare-metal" hypervisor, beží priamo na fyzickom hardvéri bez operačného systému, čím poskytuje vysoký výkon a efektivitu virtualizácie; príkladmi sú VMware ESXi, Microsoft Hyper-V (core) alebo Xen. Tento typ hypervisora je určený najmä pre dátové centrá a enterprise prostredia, kde sa kladie dôraz na výkon, stabilitu a bezpečnosť.

Hypervisor 2. typu, nazývaný aj "hostovaný" hypervisor, beží nad existujúcim operačným systémom ako aplikácia, a tým zdieľa systémové zdroje s hostiteľom; príklady zahŕňajú VMware Workstation alebo Oracle VirtualBox. Hoci je jednoduchší na inštaláciu a vhodný na vývoj alebo testovanie, jeho výkon a izolácia sú nižšie v porovnaní s typom 1.

Network

Predstavuje sieť/subsieť HW infraštruktúry. Sieť alebo podsieť HW infraštruktúry je fyzická a logická vrstva prepojenia serverov, úložísk a sieťových zariadení, ktorá zabezpečuje prenos dát, komunikáciu a prístup k službám v rámci dátového centra.

Virtual network

Predstavuje virtuálnu sieť/subsieť Hypervisora. Virtuálna sieť alebo podsieť Hypervisora je logická sieťová infraštruktúra, ktorú hypervisor vytvára na účely prepojenia virtuálnych strojov (VM) medzi sebou, s hostiteľským systémom alebo s vonkajšou sieťou. Umožňuje definovanie virtuálnych switchov, NAT, bridged alebo internal networking režimov, čím poskytuje flexibilitu v izolácii, komunikácii a routovaní dát medzi VM a fyzickým sieťovým prostredím.

AlmaLinux/RockyLinux

Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

Elasticsearch

Predstavuje Elasticsearch NoSQL databázu.

AlmaLinux/RockyLinux

Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

Elasticsearch

Predstavuje Elasticsearch NoSQL databázu.

AlmaLinux/RockyLinux

Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

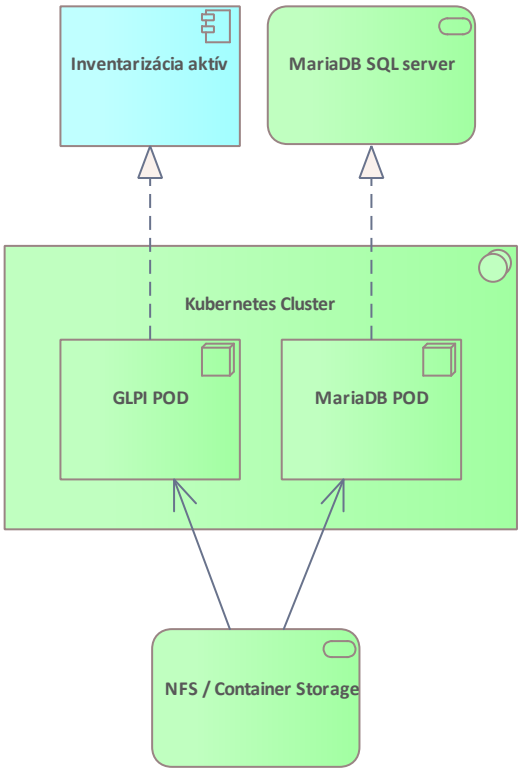
Elasticsearch

Predstavuje Elasticsearch NoSQL databázu.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

7.1.4 Technology Viewpoint Inventarizacia aktiv



Obrázok 51 : 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. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

MariaDB SQL server

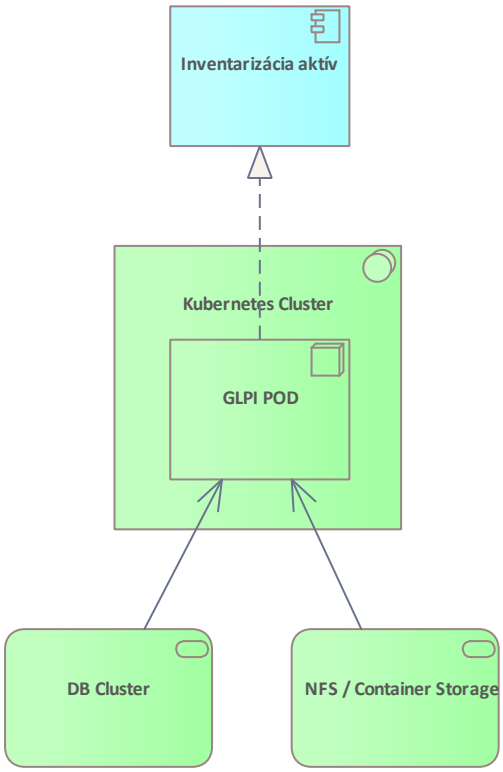
Predstavuje technologickú službu relačnej MariaDB SLQ databázy. Technologická služba v oblasti databázových systémov označuje softvérový komponent alebo platformu, ktorá poskytuje konzistentné, riadené a škálovateľné prostredie pre ukladanie, manipuláciu a správu štruktúrovaných údajov. V prípade relačnej databázy MariaDB, ide o platformovo nezávislú databázovú službu, ktorá sprístupňuje relačný model pomocou SQL (Structured Query Language) prostredníctvom konzistentného a transakčne bezpečného aplikačného rozhrania.

GLPI POD

Predstavuje POD GLPI pre invertarizáckiu aktív. GLPI (Gestionnaire Libre de Parc Informatique) je open-source systém pre správu IT služieb (ITSM), ktorý ponúka funkcionality ako správa IT aktív (hardware, software), incident management, service request management, správa zásob a používateľov a CMDB (Configuration Management Database). POD (Point Of Deployment) v kontexte GLPI predstavuje modulárne a distribuované nasadenie GLPI komponentov na viacerých miestach alebo lokalitách, pričom každé POD pôsobí ako lokálny uzol pre zber, aktualizáciu a správu IT aktív.

MariaDB POD

Predstavuje POD MariaDB pre relačnú SQL DB. MariaDB je pokročilý open-source relačný databázový systém (RDBMS), ktorý vznikol ako fork MySQL. Dodržiava štandard SQL (Structured Query Language) a poskytuje výkonné nástroje na správu a manipuláciu s relačnými údajmi. MariaDB podporuje klasickú ACID architektúru (Atomicita, Konzistencia, Izolácia, Trvácnosť) a MVCC (Multiversion Concurrency Control) pre bezpečné a konzistentné databázové transakcie.



Obrázok 52 : 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. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

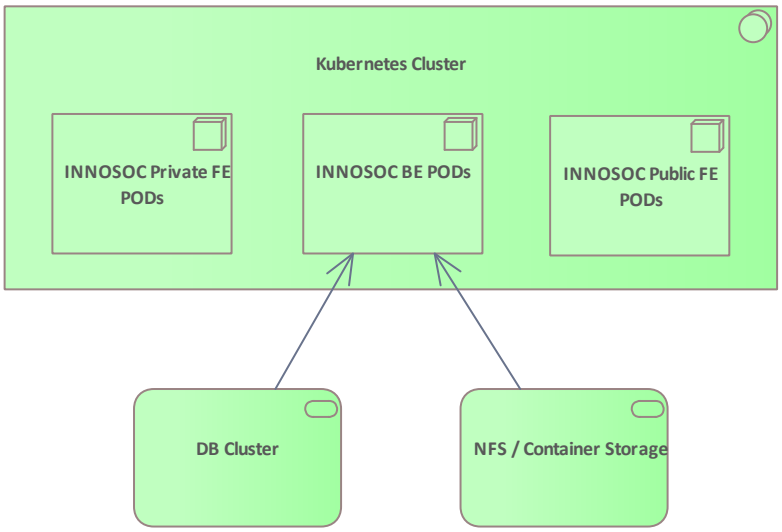
Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

GLPI POD

Predstavuje POD GLPI pre invertarizáckiu aktív. GLPI (Gestionnaire Libre de Parc Informatique) je open-source systém pre správu IT služieb (ITSM), ktorý ponúka funkcionality ako správa IT aktív (hardware, software), incident management, service request management, správa zásob a používateľov a CMDB (Configuration Management Database). POD (Point Of Deployment) v kontexte GLPI predstavuje modulárne a distribuované nasadenie GLPI komponentov na viacerých miestach alebo lokalitách, pričom každé POD pôsobí ako lokálny uzol pre zber, aktualizáciu a správu IT aktív.

7.1.5 Technology Viewpoint Kubernetes



Obrázok 53 : 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. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI

kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

INNOSOC BE PODs

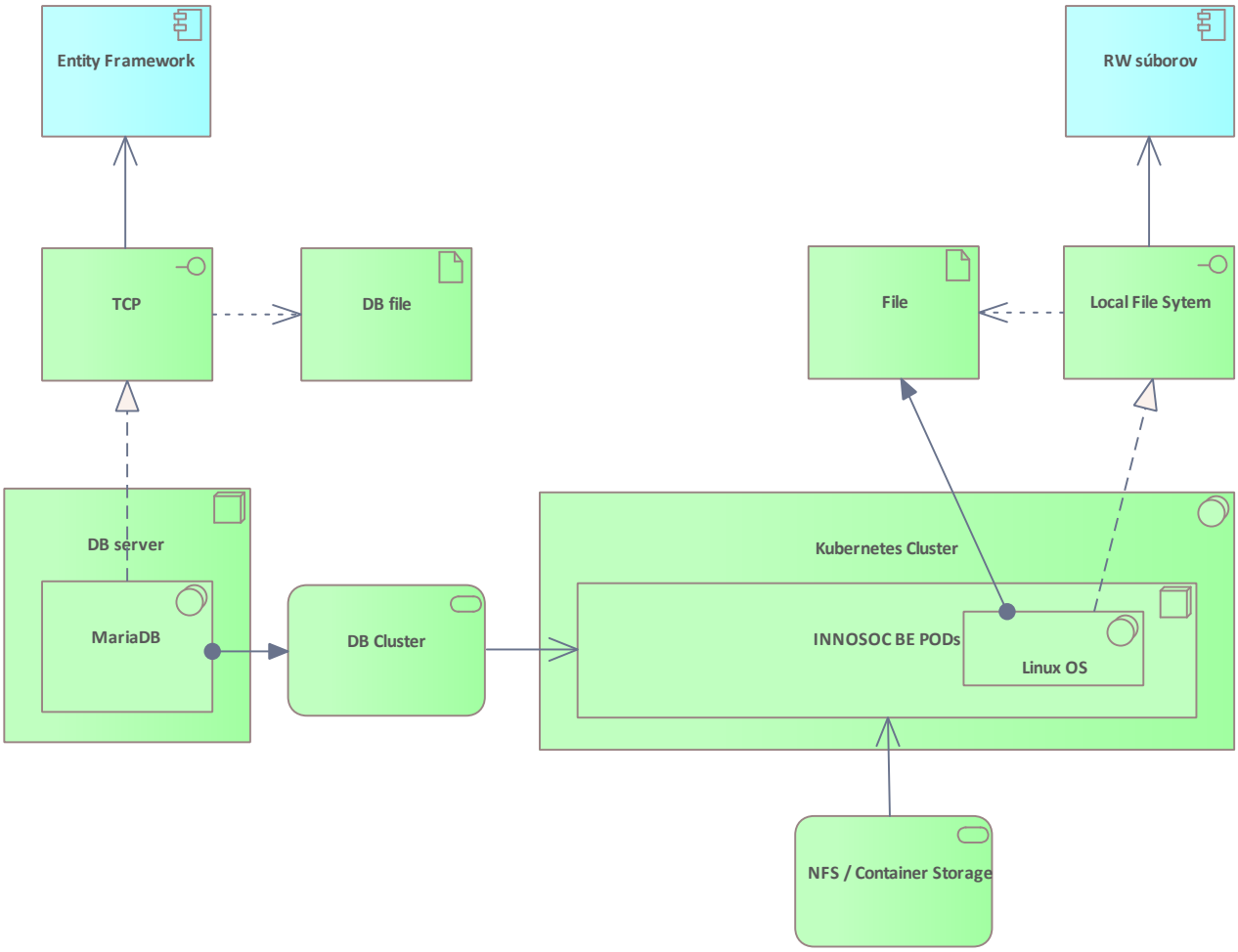
Predstavuje PODy CNM BE. PODy CNM BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému Core Network Management (CNM), ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu CNM architektúry, ktorá zaisťuje spracovanie dát, business logiku, transakcie, API služby a interakciu s databázou a sieťovými entitami (core network functions).

INNOSOC Private FE PODs

PODy CNM FE Private predstavujú izolované a modulárne jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v privátnom prostredí zákazníka. Ide o architektonický prvok vychádzajúci z princípov kontajnerizácie a mikroservisnej architektúry, kde každý POD obsahuje samostatne nasaditeľné prvky prezentačnej vrstvy (FE – frontend), ako sú webové aplikácie, Single Page Applications (SPA), či UI moduly.

INNOSOC Public FE PODs

PODy CNM FE Public predstavujú výpočtové jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v verejne dostupnom cloudovom alebo hybridnom prostredí, ktoré je spravované poskytovateľom služby alebo centralizovanou infraštruktúrou organizácie. V rámci tejto architektúry sú frontendové komponenty – typicky Single Page Applications (SPA) alebo webové rozhrania – prevádzkované ako súčasť viacnájomného (multi-tenant) systému, dostupného cez verejnú sieť (internet), pričom komunikácia a prístup sú riadené prísnymi bezpečnostnými politikami. Tieto PODy fungujú ako izolované deploymenty v rámci centralizovaného cloudu (napr. Microsoft Azure, AWS, GCP), prípadne v spravovanom Kubernetes clustri. Ich cieľom je zabezpečiť škálovateľné, vysoko dostupné a jednoducho aktualizovateľné rozhranie pre koncových používateľov alebo zákazníkov, ktorí pristupujú k CNM službám bez nutnosti lokálnej inštalácie alebo privátnej infraštruktúry.



Obrázok 54 : 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. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

DB file

DB file - súbor reprezentujúci databázový súbor MariaDB. DB file (database file) v kontexte systému MariaDB predstavuje fyzický súbor na úložisku, ktorý reprezentuje perzistentnú dátovú štruktúru databázy. Tento súbor obsahuje samotné dáta, metadáta, indexy, transakčné logy alebo systémové štruktúry používané databázovým enginom (najčastejšie InnoDB alebo MyISAM) na správu relačných dát.

DB server

Predstavuje MariaDB server. MariaDB Server je relačný databázový serverový systém (RDBMS) typu open-source, určený na správu, uchovávanie a manipuláciu s štruktúrovanými údajmi. Je kompatibilný s MySQL (jeho pôvodný fork), využíva jazyk SQL a je optimalizovaný pre výkon, bezpečnosť, transakčnosť a škálovateľnosť.

File

File - súbor je základná jednotka ukladania dát v súborovom systéme, ktorá reprezentuje štruktúrované alebo neštruktúrované dáta ako prílohy, obrázky, dokumenty, multimédiá a iné digitálne objekty. Súbor obsahuje metadáta (napr. názov, typ, veľkosť, časové značky, prístupové práva) a binárny alebo textový obsah, ktorý je interpretovaný podľa MIME typu alebo prípony.

Entity Framework

Aplikačný modul Entity Framework (EF) predstavuje logickú softvérovú vrstvu v aplikácii, ktorá využíva technológiu Entity Framework na objektovo-relačné mapovanie (ORM) medzi databázou a objektmi programovacieho jazyka (najčastejšie C# v .NET ekosystéme). Tento modul zabezpečuje, že aplikácia môže pracovať s databázovými tabuľkami ako s objektami a kolekciami tried, pričom všetky CRUD operácie (Create, Read, Update, Delete) sú automaticky prekladané na SQL príkazy.

RW súborov

Modul RW nad súbormi predstavuje softvérovú komponentu alebo logickú vrstvu, ktorá zabezpečuje čítanie (Read) a zápis (Write) údajov do súborov v rámci súborového systému. Tento modul slúži ako abstrakcia medzi aplikačnou logikou a fyzickým úložiskom, pričom využíva štandardné systémové rozhrania operačného systému na manipuláciu so súbormi (napr. POSIX API alebo abstraktné I/O knižnice).

Local File Sytem

Lokálny súborový systém poskytujúci prácu so súbormi realizovaný operačným systémom pod ktorým je

spúšťaný BE modul. Tento súborový systém umožňuje nízkolatenčný prístup k súborom, typicky prostredníctvom štandardných POSIX operácií a je viazaný na konkrétny fyzický alebo virtuálny uzol. V kontajnerizovaných prostrediach (napr. Kubernetes) je tento typ úložiska obvykle reprezentovaný typom hostPath alebo emptyDir, čím sa viaže na konkrétny uzol a stráca perzistenciu pri reštarte alebo presune PODu. Lokálny súborový systém je vhodný pre dočasné, vysokovýkonné operácie (napr. cache, scratch space), ale nie je určený na trvalé alebo zdieľané ukladanie dát, keďže neumožňuje nezávislé zotavenie dát po výpadku alebo škálovanie medzi uzlami.

TCP

Predstavuje client server komunikáciu pomocou TCP protokolu. Client-server komunikácia cez TCP (Transmission Control Protocol) je spôsob výmeny dát medzi dvoma entitami v počítačovej sieti, kde klient iniciuje spojenie a server pasívne čaká na pripojenie. Prenos je realizovaný prostredníctvom TCP protokolu – transportného protokolu vrstvy 4 (transport layer) modelu OSI, ktorý poskytuje spoľahlivý, riadený a orientovaný prenos dát cez sieť.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

INNOSOC BE PODs

Predstavuje PODy CNM BE. PODy CNM BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému Core Network Management (CNM), ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu CNM architektúry, ktorá zaisťuje spracovanie dát, business logiku, transakcie, API služby a interakciu s databázou a sieťovými entitami (core network functions).

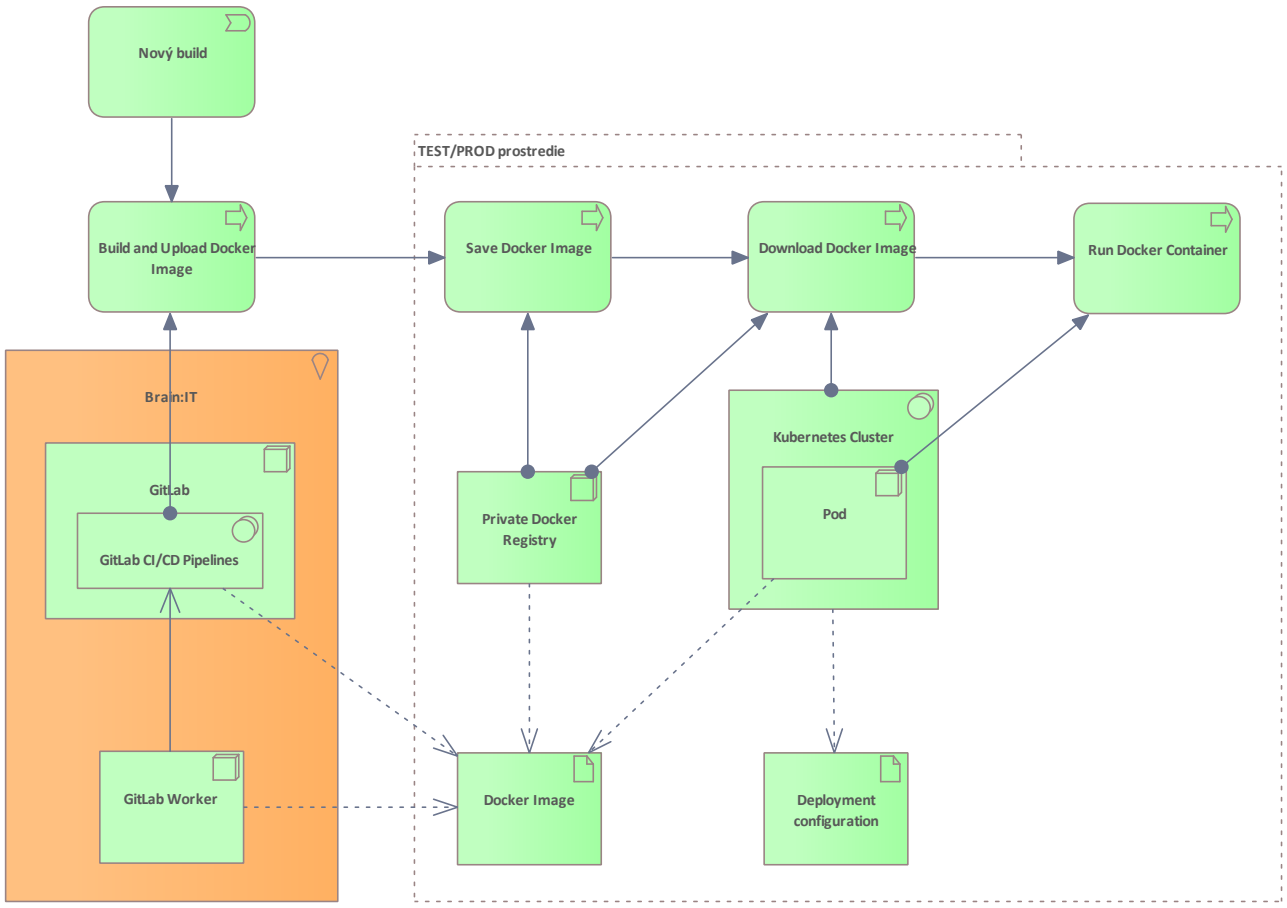
Linux OS

Linux je viacúlohový, viacpoužívateľský, unixovo kompatibilný operačný systém (OS) postavený na monolitickom jadre, vyvíjaný ako open-source softvér. Vyznačuje sa modulárnou architektúrou, vysokou prispôsobiteľnosťou a je používaný v serveroch, desktopoch, mobilných zariadeniach, embedded systémoch a superpočítačoch. Linux je technicky softvérová vrstva medzi hardvérom a používateľskými aplikáciami, ktorá zabezpečuje správu procesov, pamäte, súborových systémov, zariadení a sieťovej komunikácie.

MariaDB

Predstavuje MariaDB relačnú databázu. MariaDB predstavuje relačnú databázu (Relational Database Management System – RDBMS). V zmysle formálnej definície je MariaDB databázový systém, ktorý: pracuje s relačným modelom (údaje sú organizované do tabuliek, stĺpcov a riadkov), používa jazyk SQL (Structured Query Language) na manipuláciu a dotazovanie dát, zabezpečuje integritu
údajov

pomocou primárnych a cudzích kľúčov a implementuje ACID vlastnosti prostredníctvom svojich storage enginov.



Obrázok 55 : 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 s následným nahratím Docker Image do Docker Registry je štandardný krok, ktorý

zabezpečuje automatizované zostavenie aplikačného kontajnera, jeho označenie a publikovanie do centralizovaného repozitára, odkiaľ môže byť nasadený do vývojových, testovacích alebo produkčných prostredí.

Download Docker Image

Uloženie Docker image do Docker Registry začína vytvorením image z Dockerfile pomocou príkazu docker build. Následne sa image označí podľa názvu a verzie cieľového registry. Po autentifikácii sa image nahrá príkazom docker push a stáva sa dostupným pre ďalšie nasadenie.

Nový build

Spustenie nového build procesu predstavuje inicializáciu a konfiguráciu automatizovaného reťazca úloh, ktorého cieľom je zostavenie, testovanie a príprava softvérového artefaktu na ďalšie spracovanie alebo nasadenie.

Run Docker Container

Spustenie Docker kontajnera začína stiahnutím alebo výberom existujúceho Docker image, z ktorého sa vytvorí inštancia aplikácie. Kontajner sa spúšťa príkazom docker run, kde možno definovať parametre ako porty, volume mounty, premenné prostredia či sieťové nastavenia. Po spustení beží kontajner ako izolovaný proces, pripravený na komunikáciu so službami alebo používateľom.

Save Docker Image

Proces uloženia Docker image do Docker Registry zahŕňa vytvorenie image pomocou príkazu docker build, jeho označenie s cieľovou adresou registry a verziou. Následne prebehne autentifikácia do registry a samotný upload cez príkaz docker push. Výsledkom je, že image je uložený v centrálnom repozitári, odkiaľ ho možno nasadiť do ľubovoľného prostredia.

TEST/PROD prostredie

Predstavuje interné DEV a TEST prostredie

Brain:IT

Lokalita Brain:IT

Private Docker Registry

Predstavuje private Docker Registry, Private Docker Registry je súkromný repozitár, v ktorom organizácia bezpečne ukladá a spravuje vlastné Docker imagy mimo verejných registry ako Docker Hub. Umožňuje plnú kontrolu nad prístupom, verziovaním, retention politikami a bezpečnostným skenovaním kontajnerov.

Deployment configuration

Reprezentácia Kubernetes Deployment artifaktu. Kubernetes Deployment artefakt je

konfiguračný súbor, ktorý definuje želaný stav nasadenia aplikácie v Kubernetes klustri – vrátane počtu replík, Docker imagu, portov a stratégií aktualizácie. Tento artefakt slúži ako vstup pre kubectl alebo CI/CD pipeline, ktoré ho aplikujú do klastru na zabezpečenie deklaratívneho a opakovateľného nasadenia.

Docker Image

Reprezentácia Docker Image artifaktu, Docker Image ako artefakt je výsledný balík aplikácie zostavený počas build procesu, ktorý obsahuje všetky potrebné vrstvy, závislosti a konfiguráciu na spustenie v kontajnerovom prostredí. Tento artefakt sa ukladá do Docker Registry, odkiaľ môže byť opakovane použitý na nasadenie v rôznych prostrediach.

GitLab

Predstavuje inštaláciu GitLab. Inštancia GitLab predstavuje samostatné nasadenie platformy GitLab, ktoré môže bežať ako cloudová služba (GitLab.com) alebo ako self-managed verzia na vlastnej infraštruktúre. Obsahuje všetky komponenty potrebné na správu repozitárov, CI/CD pipeline, issue tracking a DevOps workflow v jednom integrovanom prostredí. V rámci organizácie umožňuje úplnú kontrolu nad projektmi, používateľmi, bezpečnosťou a prístupovými právami.

GitLab Worker

Predstavuje insštanciu GitLab Worker, inštancia GitLab Worker (nazývaná aj GitLab Runner) je samostatná služba, ktorá vykonáva úlohy definované v CI/CD pipeline, ako je build, testovanie alebo nasadenie aplikácií. Beží na vyhradenom prostredí (Kubernetes) a komunikuje s centrálnym GitLab serverom, kde prijíma joby na spracovanie.

Kubernetes Cluster

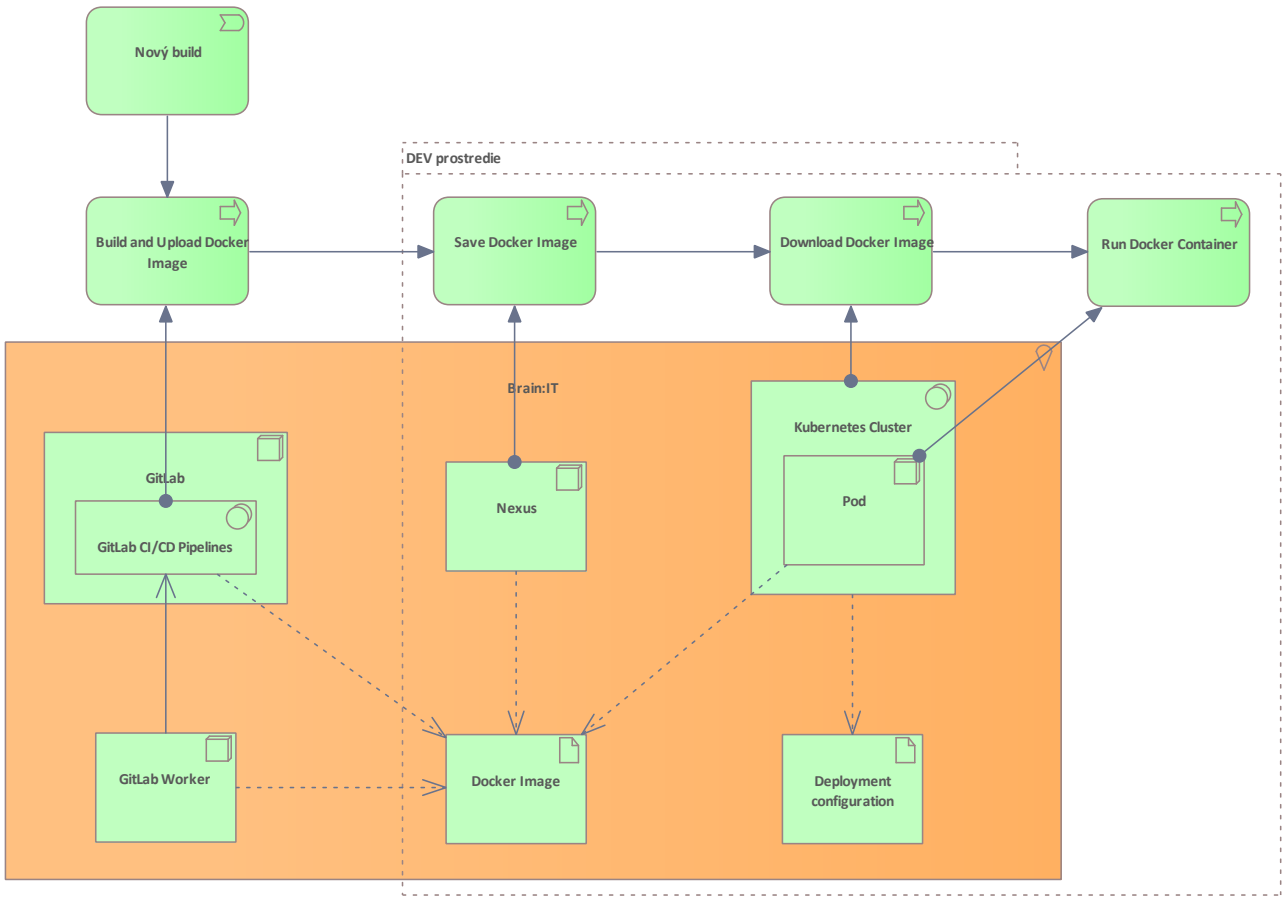
Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

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 56 : 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 s následným nahratím Docker Image do Docker Registry je štandardný krok, ktorý zabezpečuje automatizované zostavenie aplikačného kontajnera, jeho označenie a publikovanie do centralizovaného repozitára, odkiaľ môže byť nasadený do vývojových, testovacích alebo produkčných prostredí.

Download Docker Image

Uloženie Docker image do Docker Registry začína vytvorením image z Dockerfile pomocou príkazu docker build. Následne sa image označí podľa názvu a verzie cieľového registry. Po

autentifikácii sa image nahrá príkazom docker push a stáva sa dostupným pre ďalšie nasadenie.

Nový build

Spustenie nového build procesu predstavuje inicializáciu a konfiguráciu automatizovaného reťazca úloh, ktorého cieľom je zostavenie, testovanie a príprava softvérového artefaktu na ďalšie spracovanie alebo nasadenie.

Run Docker Container

Spustenie Docker kontajnera začína stiahnutím alebo výberom existujúceho Docker image, z ktorého sa vytvorí inštancia aplikácie. Kontajner sa spúšťa príkazom docker run, kde možno definovať parametre ako porty, volume mounty, premenné prostredia či sieťové nastavenia. Po spustení beží kontajner ako izolovaný proces, pripravený na komunikáciu so službami alebo používateľom.

Save Docker Image

Proces uloženia Docker image do Docker Registry zahŕňa vytvorenie image pomocou príkazu docker build, jeho označenie s cieľovou adresou registry a verziou. Následne prebehne autentifikácia do registry a samotný upload cez príkaz docker push. Výsledkom je, že image je uložený v centrálnom repozitári, odkiaľ ho možno nasadiť do ľubovoľného prostredia.

DEV prostredie

Predstavuje interné DEV a TEST prostredie

Brain:IT

Lokalita Brain:IT

Deployment configuration

Reprezentácia Kubernetes Deployment artifaktu. Kubernetes Deployment artefakt je konfiguračný súbor, ktorý definuje želaný stav nasadenia aplikácie v Kubernetes klustri – vrátane počtu replík, Docker imagu, portov a stratégií aktualizácie. Tento artefakt slúži ako vstup pre kubectl alebo CI/CD pipeline, ktoré ho aplikujú do klastru na zabezpečenie deklaratívneho a opakovateľného nasadenia.

Docker Image

Reprezentácia Docker Image artifaktu, Docker Image ako artefakt je výsledný balík aplikácie zostavený počas build procesu, ktorý obsahuje všetky potrebné vrstvy, závislosti a konfiguráciu na spustenie v kontajnerovom prostredí. Tento artefakt sa ukladá do Docker Registry, odkiaľ môže byť opakovane použitý na nasadenie v rôznych prostrediach.

GitLab

Predstavuje inštaláciu GitLab. Inštancia GitLab predstavuje samostatné nasadenie platformy GitLab, ktoré môže

bežať ako cloudová služba (GitLab.com) alebo ako self-managed verzia na vlastnej infraštruktúre. Obsahuje všetky komponenty potrebné na správu repozitárov, CI/CD pipeline, issue tracking a DevOps workflow v jednom integrovanom prostredí. V rámci organizácie umožňuje úplnú kontrolu nad projektmi, používateľmi, bezpečnosťou a prístupovými právami.

GitLab Worker

Predstavuje insštanciu GitLab Worker, inštancia GitLab Worker (nazývaná aj GitLab Runner) je samostatná služba, ktorá vykonáva úlohy definované v CI/CD pipeline, ako je build, testovanie alebo nasadenie aplikácií. Beží na vyhradenom prostredí (Kubernetes) a komunikuje s centrálnym GitLab serverom, kde prijíma joby na spracovanie.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Nexus

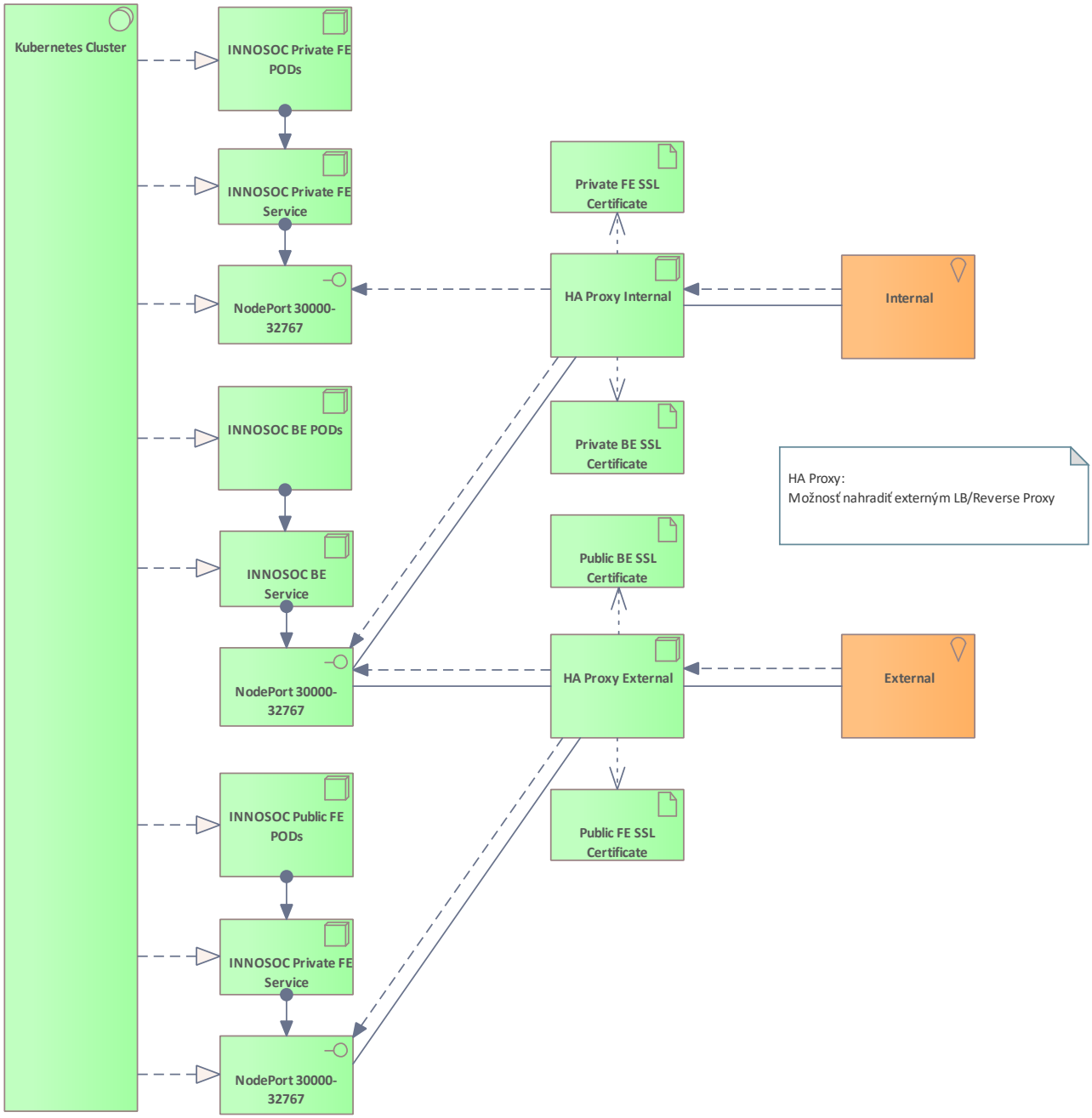
Predstavuje private Docker Registry. Private Docker Registry je súkromné úložisko pre Docker imagy, ktoré umožňuje organizáciám bezpečne ukladať a spravovať kontajnerové obrazy mimo verejných služieb ako Docker Hub. Poskytuje kontrolu nad prístupom, verziami a distribúciou image-ov, a je často integrovaný s CI/CD pipeline pre automatizované buildy a nasadenia.

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 57 : Technology Viewpoint Interconnect

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

Popis používaných prvkov:

External

Predstavuje externé prostredie Internet

HA Proxy External

Predstavuje Externú reverse proxy postavenej na HA Proxy. Externá reverse proxy postavená na HAProxy je sprostredkovateľská vrstva, ktorá sa nachádza na hranici siete a slúži na prijímanie požiadaviek z internetu, ktoré následne presmerováva na interné backend služby. HAProxy v tejto úlohe zabezpečuje TLS termináciu, load balancing, ochranu cez ACL pravidlá, a tiež možnosť filtrovania alebo prepúšťania prevádzky na základe definovaných bezpečnostných politík. Táto architektúra zvyšuje bezpečnosť, škálovateľnosť a dostupnosť verejne prístupných služieb, pričom oddeľuje externú vrstvu od vnútornej infraštruktúry.

HA Proxy Internal

Predstavuje Internú reverse proxy postavenej na HA Proxy. Interná reverse proxy postavená na HAProxy je sprostredkovateľská služba, ktorá prijíma prichádzajúce požiadavky v rámci internej siete a presmerováva ich na príslušné backend služby podľa konfigurovaných pravidiel. HAProxy v tomto prípade zabezpečuje load balancing, TLS termináciu, health checking a možnosť centrálne riadiť tok dát medzi mikroslužbami alebo internými aplikáciami.

INNOSOC BE Service

Predstavuje INNOSOC BE Service. Beží ako súčasť predkonfigurovaného PODu, často vo forme kontajnera alebo virtuálneho stroja, a aktualizuje sa cez riadený CI/CD proces.

INNOSOC Private FE Service

Predstavuje INNOSOC FE Private Service. Beží ako súčasť predkonfigurovaného PODu, často vo forme kontajnera alebo virtuálneho stroja, a aktualizuje sa cez riadený CI/CD proces.

INNOSOC Private FE Service

Predstavuje INNOSOC FE Public Service. Beží ako súčasť predkonfigurovaného PODu, často vo forme kontajnera alebo virtuálneho stroja, a aktualizuje sa cez riadený CI/CD proces.

Internal

Predstavuje interné prostrednie BRAIN:IT

Private BE SSL Certificate

Predstavuje validný Private SSL certifikát pre potreby HTTPS. Validný BE SSL certifikát pre potreby HTTPS je bezpečnostný certifikát nainštalovaný na backendovej (BE) vrstve systému, ktorý umožňuje šifrovanú a autentifikovanú komunikáciu medzi službami alebo medzi frontendom a backendom. Certifikát musí byť vydaný dôveryhodnou certifikačnou autoritou (CA) alebo internou PKI infraštruktúrou a zabezpečovať integritu a dôvernosť dát prenášaných cez HTTPS.

Private FE SSL Certificate

Predstavuje validný SSL certifikát pre potreby HTTPS. Validný FE SSL certifikát pre potreby HTTPS je dôveryhodný digitálny certifikát, nainštalovaný na frontendovej (FE) vrstve aplikácie, ktorý zabezpečuje šifrovanú komunikáciu medzi používateľským prehliadačom a frontend serverom. Tento certifikát musí byť vydaný akreditovanou certifikačnou autoritou (CA), byť platný pre konkrétnu doménu a nesmie byť expirovaný ani neplatný.

Public BE SSL Certificate

Predstavuje validný Public SSL certifikát pre potreby HTTPS. Validný BE Public SSL certifikát pre potreby HTTPS je certifikát nainštalovaný na backendovej službe, ktorá je dostupná z verejnej siete, a slúži na zabezpečenie šifrovanej a overenej komunikácie cez HTTPS. Musí byť vydaný dôveryhodnou verejnou certifikačnou autoritou (CA), byť platný pre konkrétnu verejnú doménu a spĺňať bezpečnostné štandardy.

Public FE SSL Certificate

Predstavuje validný Public SSL certifikát pre potreby HTTPS. Validný FE Public SSL certifikát pre potreby HTTPS je dôveryhodný certifikát nainštalovaný na frontendovej vrstve aplikácie, ktorá je verejne dostupná cez internet, a zabezpečuje šifrovanú komunikáciu medzi klientským prehliadačom a frontend serverom. Musí byť vydaný verejnou certifikačnou autoritou (CA), byť platný pre danú doménu a nesmie byť expirovaný ani zneplatnený, aby bol akceptovaný modernými prehliadačmi.

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. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo

umožňuje automatizované riadenie životného cyklu aplikácií.

INNOSOC BE PODs

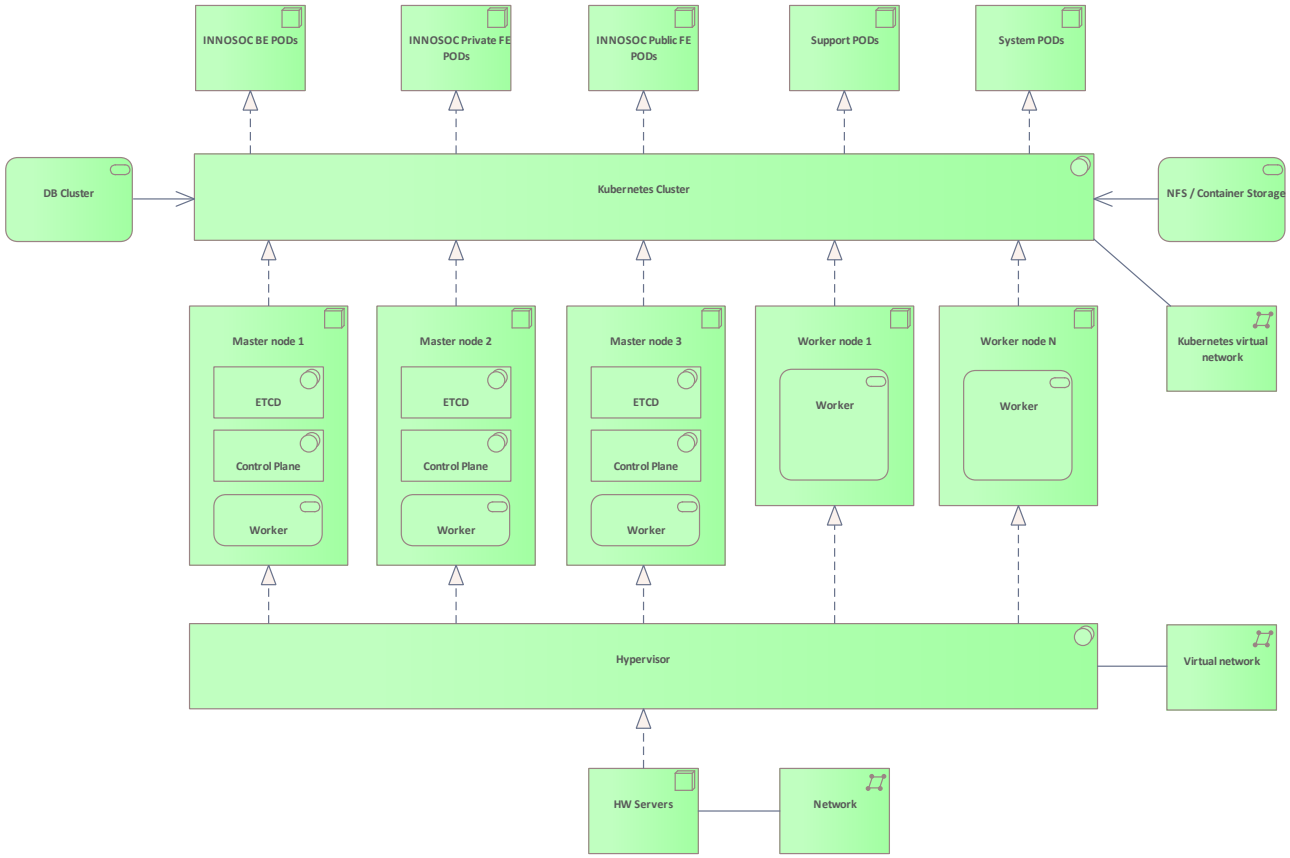
Predstavuje PODy CNM BE. PODy CNM BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému Core Network Management (CNM), ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu CNM architektúry, ktorá zaisťuje spracovanie dát, business logiku, transakcie, API služby a interakciu s databázou a sieťovými entitami (core network functions).

INNOSOC Private FE PODs

PODy CNM FE Private predstavujú izolované a modulárne jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v privátnom prostredí zákazníka. Ide o architektonický prvok vychádzajúci z princípov kontajnerizácie a mikroservisnej architektúry, kde každý POD obsahuje samostatne nasaditeľné prvky prezentačnej vrstvy (FE – frontend), ako sú webové aplikácie, Single Page Applications (SPA), či UI moduly.

INNOSOC Public FE PODs

PODy CNM FE Public predstavujú výpočtové jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v verejne dostupnom cloudovom alebo hybridnom prostredí, ktoré je spravované poskytovateľom služby alebo centralizovanou infraštruktúrou organizácie. V rámci tejto architektúry sú frontendové komponenty – typicky Single Page Applications (SPA) alebo webové rozhrania – prevádzkované ako súčasť viacnájomného (multi-tenant) systému, dostupného cez verejnú sieť (internet), pričom komunikácia a prístup sú riadené prísnymi bezpečnostnými politikami. Tieto PODy fungujú ako izolované deploymenty v rámci centralizovaného cloudu (napr. Microsoft Azure, AWS, GCP), prípadne v spravovanom Kubernetes clustri. Ich cieľom je zabezpečiť škálovateľné, vysoko dostupné a jednoducho aktualizovateľné rozhranie pre koncových používateľov alebo zákazníkov, ktorí pristupujú k CNM službám bez nutnosti lokálnej inštalácie alebo privátnej infraštruktúry.



Obrázok 58 : Technology Viewpoint Kubernetes Cluster

Predstavuje rolu a službu Worker nodu .

Popis používaných prvkov:

DB Cluster

Predstavuje službu clustrovanej relačnej databázy. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby

poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

HW Servers

Predstavuje HW serverovú infraštruktúru. HW serverová infraštruktúra predstavuje fyzické výpočtové a sieťové vybavenie, ktoré tvorí základ pre prevádzku IT systémov, vrátane serverov, úložísk, prepínačov, smerovačov a záložných zdrojov napájania. Táto infraštruktúra je nasadzovaná buď on-premise alebo ako súčasť cloudovej platformy, a poskytuje výpočtový výkon, dostupnosť a konektivitu pre virtualizované aj nevirtualizované prostredia.

Hypervisor

Predstavuje Hypervisor 1. alebo 2. typu. Hypervisor 1. typu, známy aj ako "bare-metal" hypervisor, beží priamo na fyzickom hardvéri bez operačného systému, čím poskytuje vysoký výkon a efektivitu virtualizácie; príkladmi sú VMware ESXi, Microsoft Hyper-V (core) alebo Xen. Tento typ hypervisora je určený najmä pre dátové centrá a enterprise prostredia, kde sa kladie dôraz na výkon, stabilitu a bezpečnosť.

Hypervisor 2. typu, nazývaný aj "hostovaný" hypervisor, beží nad existujúcim operačným systémom ako aplikácia, a tým zdieľa systémové zdroje s hostiteľom; príklady zahŕňajú VMware Workstation alebo Oracle VirtualBox. Hoci je jednoduchší na inštaláciu a vhodný na vývoj alebo testovanie, jeho výkon a izolácia sú nižšie v porovnaní s typom 1.

Kubernetes virtual network

Predstavuje virtuálnu sieť/subsieť Kubernetes Clustra. Virtuálna sieť alebo podsieť v Kubernetes clustri je logická sieťová architektúra, ktorá umožňuje komunikáciu medzi podmi, službami a ďalšími komponentmi v klastri bez nutnosti NAT. Každý pod dostáva vlastnú IP adresu v rámci tejto siete, čo zabezpečuje predvídateľnú a plne routovateľnú konektivitu v súlade s princípom "každý pod môže komunikovať s každým iným podom".

Master node 1

Predstavuje Master node Kubernetes Clustra. Master node v Kubernetes clustri je riadiaci uzol, ktorý hostuje komponenty Control Plane, zodpovedné za globálne rozhodovanie, plánovanie workloadov a udržiavanie stavu clustra. Obsahuje kľúčové služby ako kube-apiserver, ETCD databázu, scheduler a controller-managery, ktoré spolu zabezpečujú orchestráciu a správu všetkých Worker nodov a podov.

Master node 2

Predstavuje Master node Kubernetes Clustra

Master node 3

Predstavuje Master node Kubernetes Clustra

Network

Predstavuje sieť/subsieť HW infraštruktúry. Sieť alebo podsieť HW infraštruktúry je fyzická a logická vrstva prepojenia serverov, úložísk a sieťových zariadení, ktorá zabezpečuje prenos dát, komunikáciu a prístup k službám v rámci dátového centra.

Support PODs

Predstavuje PODy podporných služieb. PODy podporných služieb predstavujú kontajnerové alebo virtuálne jednotky nasadenia, ktoré zabezpečujú neaplikačné funkcie potrebné na chod a správu hlavného systému, ako sú monitoring, logging, autentifikácia či konfigurácia. Tieto služby typicky fungujú ako infrastrukturné komponenty a sú nasadené paralelne s aplikačnými PODmi v rámci rovnakého clustra alebo prostredia.

System PODs

Predstavuje PODy systémových služieb. PODy systémových služieb sú nasadené komponenty v kontajnerizovanom prostredí, ktoré zabezpečujú základnú funkcionalitu a operácie potrebné pre správnu činnosť celej platformy alebo clustra, ako je networking, DNS, storage či orchestrácia. Tieto služby zvyčajne tvoria súčasť základnej infraštruktúry Kubernetes alebo iného orchestrátora a fungujú nezávisle od aplikačných a podporných PODov, pričom zabezpečujú stabilitu a prevádzkyschopnosť systému.

Virtual network

Predstavuje virtuálnu sieť/subsieť Hypervisora. Virtuálna sieť alebo podsieť Hypervisora je logická sieťová infraštruktúra, ktorú hypervisor vytvára na účely prepojenia virtuálnych strojov (VM) medzi sebou, s hostiteľským systémom alebo s vonkajšou sieťou. Umožňuje definovanie virtuálnych switchov, NAT, bridged alebo internal networking režimov, čím poskytuje flexibilitu v izolácii, komunikácii a routovaní dát medzi VM a fyzickým sieťovým prostredím.

Worker node 1

Predstavuje Worker node Kubernetes Clustra. Worker node v Kubernetes clustri je výpočtový uzol, na ktorom sú nasadzované a spúšťané aplikačné Pody, teda reálne workloady systému. Obsahuje základné komponenty ako kubelet, kube-proxy a container runtime (napr. containerd), ktoré zabezpečujú komunikáciu s Control Plane a správne vykonávanie priradených úloh.

Worker node N

Predstavuje Worker node Kubernetes Clustra

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

INNOSOC BE PODs

Predstavuje PODy CNM BE. PODy CNM BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému Core Network Management (CNM), ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu CNM architektúry, ktorá zaisťuje spracovanie dát, business logiku, transakcie, API služby a interakciu s databázou a sieťovými entitami (core network functions).

INNOSOC Private FE PODs

PODy CNM FE Private predstavujú izolované a modulárne jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v privátnom prostredí zákazníka. Ide o architektonický prvok vychádzajúci z princípov kontajnerizácie a mikroservisnej architektúry, kde každý POD obsahuje samostatne nasaditeľné prvky prezentačnej vrstvy (FE – frontend), ako sú webové aplikácie, Single Page Applications (SPA), či UI moduly.

INNOSOC Public FE PODs

PODy CNM FE Public predstavujú výpočtové jednotky nasadenia frontendových komponentov systému Customer Network Management (CNM) v verejne dostupnom cloudovom alebo hybridnom prostredí, ktoré je spravované poskytovateľom služby alebo centralizovanou infraštruktúrou organizácie. V rámci tejto architektúry sú frontendové komponenty – typicky Single Page Applications (SPA) alebo webové rozhrania – prevádzkované ako súčasť viacnájomného (multi-tenant) systému, dostupného cez verejnú sieť (internet), pričom komunikácia a prístup sú riadené prísnymi bezpečnostnými politikami. Tieto PODy fungujú ako izolované deploymenty v rámci centralizovaného cloudu (napr. Microsoft Azure, AWS, GCP), prípadne v spravovanom Kubernetes clustri. Ich cieľom je zabezpečiť škálovateľné, vysoko dostupné a jednoducho aktualizovateľné rozhranie pre koncových používateľov alebo zákazníkov, ktorí pristupujú k CNM službám bez nutnosti lokálnej inštalácie alebo privátnej infraštruktúry.

Worker

Predstavuje rolu a službu Worker nodu. Rola a služba Worker nodu v Kubernetes spočíva v hostovaní a spúšťaní aplikačných podov, pričom zabezpečuje vykonávanie workloadov na základe pokynov z Control Plane.

Control Plane

Predstavuje Control Plane pre správu Kubernetes Clustra. Control Plane pre správu Kubernetes clustra je centrálna riadiaca vrstva, ktorá zabezpečuje globálnu orchestráciu, plánovanie a správu všetkých komponentov v klastri. Obsahuje kľúčové služby ako kube-apiserver, ETCD databáza, kube-scheduler, kube-controller-manager a prípadne cloud-controller-manager. Control Plane rozhoduje, kde a ako budú aplikácie bežať, monitoruje ich stav a zaručuje, že požadovaný stav (deklarovaný používateľom) zodpovedá aktuálnemu stavu clustra.

ETCD

Predstavuje ETCD databázu. ETCD databáza je distribuovaná, vysoko dostupná kľúč-hodnota databáza, navrhnutá pre ukladanie konfiguračných dát a metadát v reálnom čase. Je základnou súčasťou Kubernetes, kde slúži ako centrálne úložisko stavov clustra, vrátane informácií o pods,

konfiguráciách, secret-och a ďalších objektoch. Vďaka mechanizmu konsenzu Raft zabezpečuje spoľahlivosť, konzistenciu a odolnosť voči výpadkom v distribuovaných systémoch.

Worker

Predstavuje rolu a službu Worker nodu

Control Plane

Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD

Predstavuje ETCD databázu

Worker

Control Plane

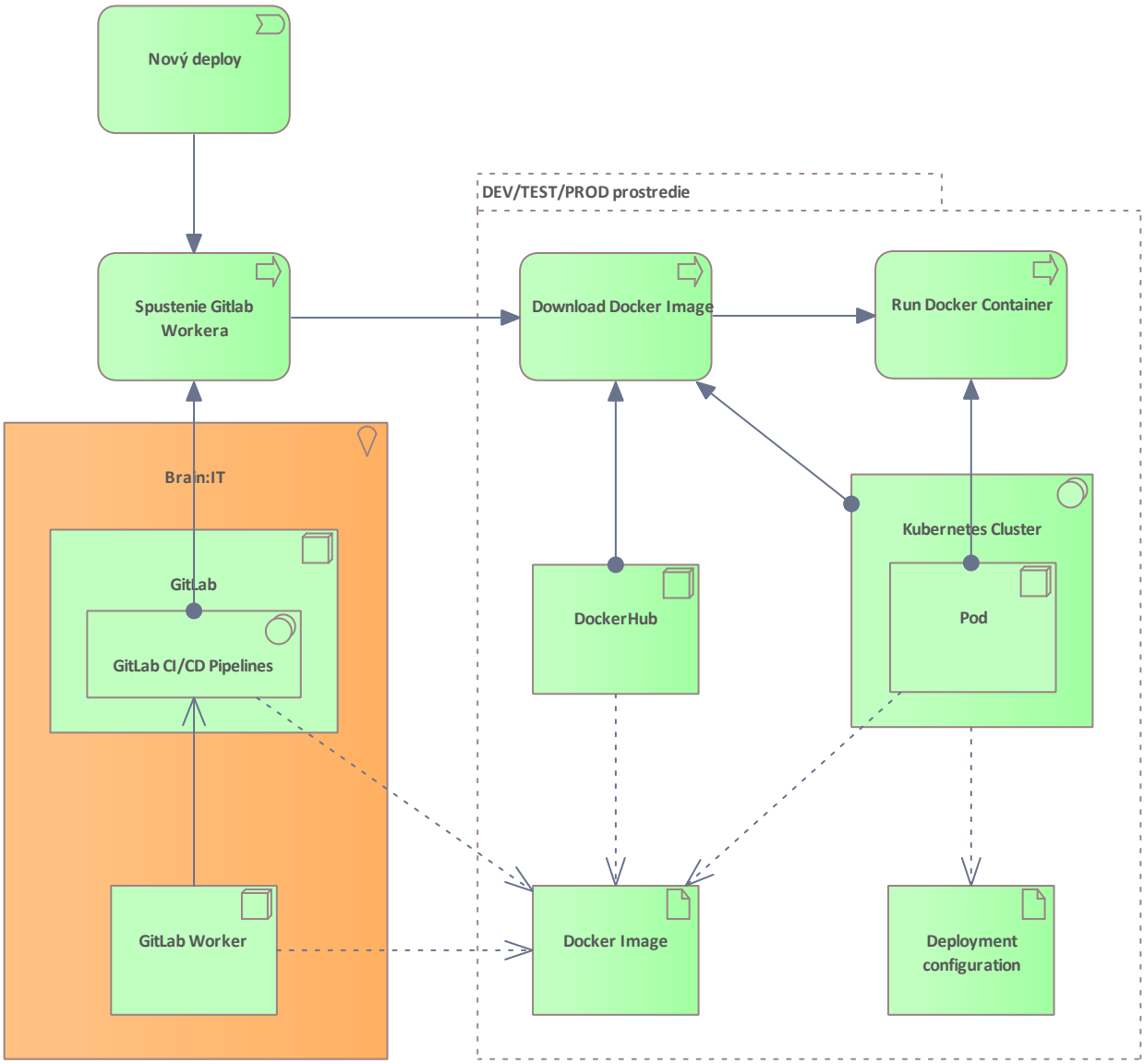
Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD

Predstavuje ETCD databázu

Worker

Worker



Obrázok 59 : Technology Viewpoint standard CI/CD DEV/TEST/PROD

Popis používaných prvkov:

Download Docker Image

Uloženie Docker image do Docker Registry začína vytvorením image z Dockerfile pomocou príkazu docker build. Následne sa image označí podľa názvu a verzie cieľového registry. Po autentifikácii sa image nahrá príkazom docker push a stáva sa dostupným pre ďalšie nasadenie.

Nový deploy

Spustenie nového deploy procesu je akcia, pri ktorej sa nová verzia aplikácie alebo služby automatizovane nasadí do cieľového prostredia na základe definovanej CI/CD pipeline.

Run Docker Container

Spustenie Docker kontajnera začína stiahnutím alebo výberom existujúceho Docker image, z ktorého sa vytvorí inštancia aplikácie. Kontajner sa spúšťa príkazom docker run, kde možno definovať parametre ako porty, volume mounty, premenné prostredia či sieťové nastavenia. Po spustení beží kontajner ako izolovaný proces, pripravený na komunikáciu so službami alebo používateľom.

Spustenie Gitlab Workera

Proces spustenia GitLab Workera pre nasadenie novej verzie balíka začína prijatím jobu z CI/CD pipeline definovanej v .gitlab-ci.yml, ktorý obsahuje kroky pre deployment. Worker následne vykoná inštrukcie ako sťahovanie artefaktu, pripojenie na cieľové prostredie a nasadenie novej verzie aplikácie, pričom celý priebeh je logovaný a spätne sledovateľný.

DEV/TEST/PROD prostredie

Predstavuje interné DEV a TEST prostredie

Brain:IT

Lokalita Brain:IT

DockerHub

Predstavuje verejný Docker Registry DockerHub. DockerHub je verejný Docker Registry poskytovaný spoločnosťou Docker Inc., ktorý umožňuje vývojárom zdieľať, ukladať a sťahovať kontajnerové image prostredníctvom cloudovej platformy. Podporuje verejné aj súkromné repozitáre, verziovanie image-ov, automatické buildy a integráciu s CI/CD nástrojmi.

Deployment configuration

Reprezentácia Kubernetes Deployment artifaktu. Kubernetes Deployment artefakt je konfiguračný súbor, ktorý definuje želaný stav nasadenia aplikácie v Kubernetes klustri – vrátane počtu replík, Docker imagu, portov a stratégií aktualizácie. Tento artefakt slúži ako vstup pre kubectl alebo CI/CD pipeline, ktoré ho aplikujú do klastru na zabezpečenie deklaratívneho a opakovateľného nasadenia.

Docker Image

Reprezentácia Docker Image artifaktu, Docker Image ako artefakt je výsledný balík aplikácie zostavený počas build procesu, ktorý obsahuje všetky potrebné vrstvy, závislosti a konfiguráciu na spustenie v kontajnerovom prostredí. Tento artefakt sa ukladá do Docker Registry, odkiaľ môže byť opakovane použitý na nasadenie v rôznych prostrediach.

GitLab

Predstavuje inštaláciu GitLab. Inštancia GitLab predstavuje samostatné nasadenie platformy GitLab, ktoré môže bežať ako cloudová služba (GitLab.com) alebo ako self-managed verzia na vlastnej infraštruktúre. Obsahuje všetky komponenty potrebné na správu repozitárov, CI/CD pipeline, issue tracking a DevOps workflow v jednom integrovanom prostredí. V rámci organizácie umožňuje úplnú kontrolu nad projektmi, používateľmi, bezpečnosťou a prístupovými právami.

GitLab Worker

Predstavuje insštanciu GitLab Worker, inštancia GitLab Worker (nazývaná aj GitLab Runner) je samostatná služba, ktorá vykonáva úlohy definované v CI/CD pipeline, ako je build, testovanie alebo nasadenie aplikácií. Beží na vyhradenom prostredí (Kubernetes) a komunikuje s centrálnym GitLab serverom, kde prijíma joby na spracovanie.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

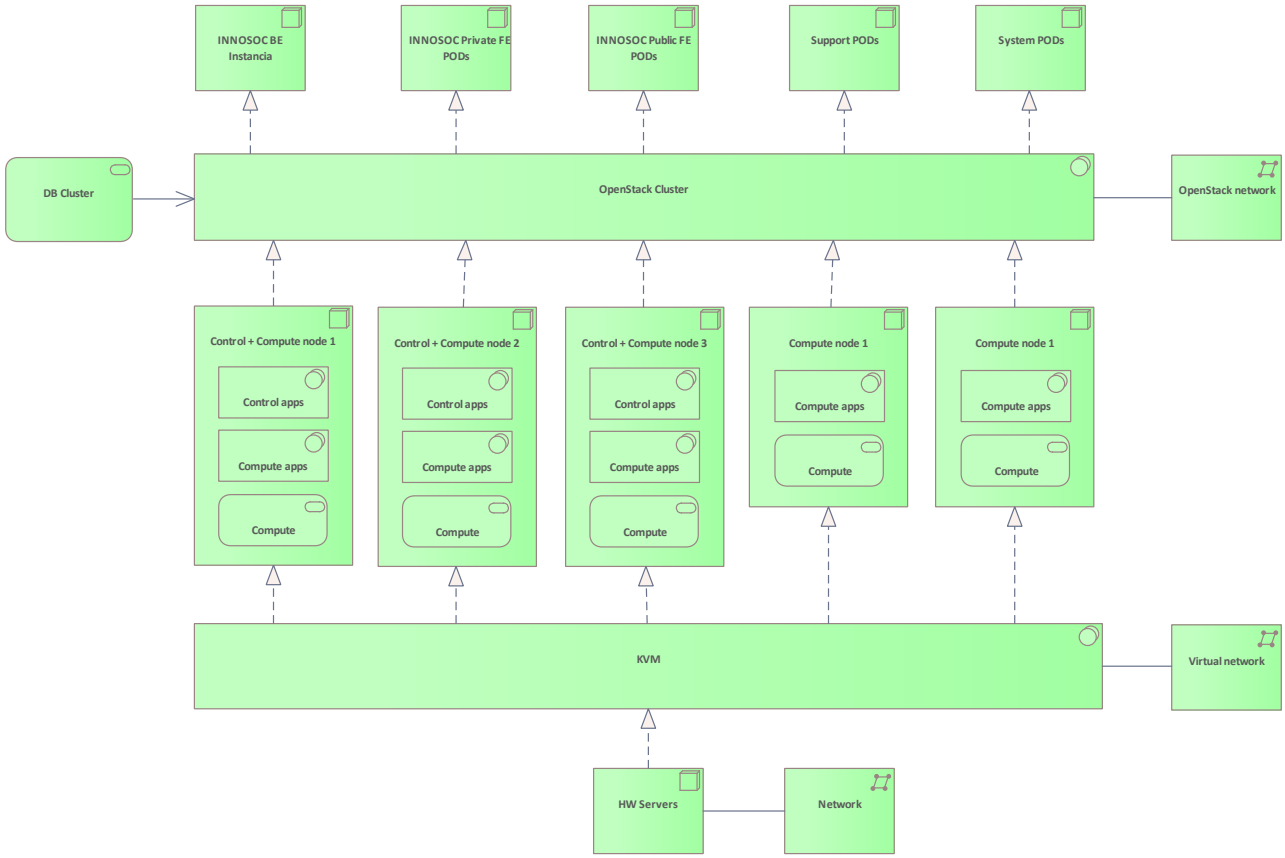
GitLab CI/CD Pipelines

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

7.1.6 Technology Viewpoint OpenStack



Obrázok 60 : 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. Inštancia OpenStacku vo forme VM alebo kontajnera predstavuje virtuálny výpočtový zdroj (compute instance), ktorý je nasadený v rámci cloudovej platformy OpenStack prostredníctvom komponentu Nova. Môže ísť o klasickú virtuálnu mašinu (VM) alebo o ľahšiu kontajnerovú inštanciu, v závislosti od použitého hypervisora a integrácie s kontajnerizačnými technológiami ako Kubernetes alebo Docker.

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

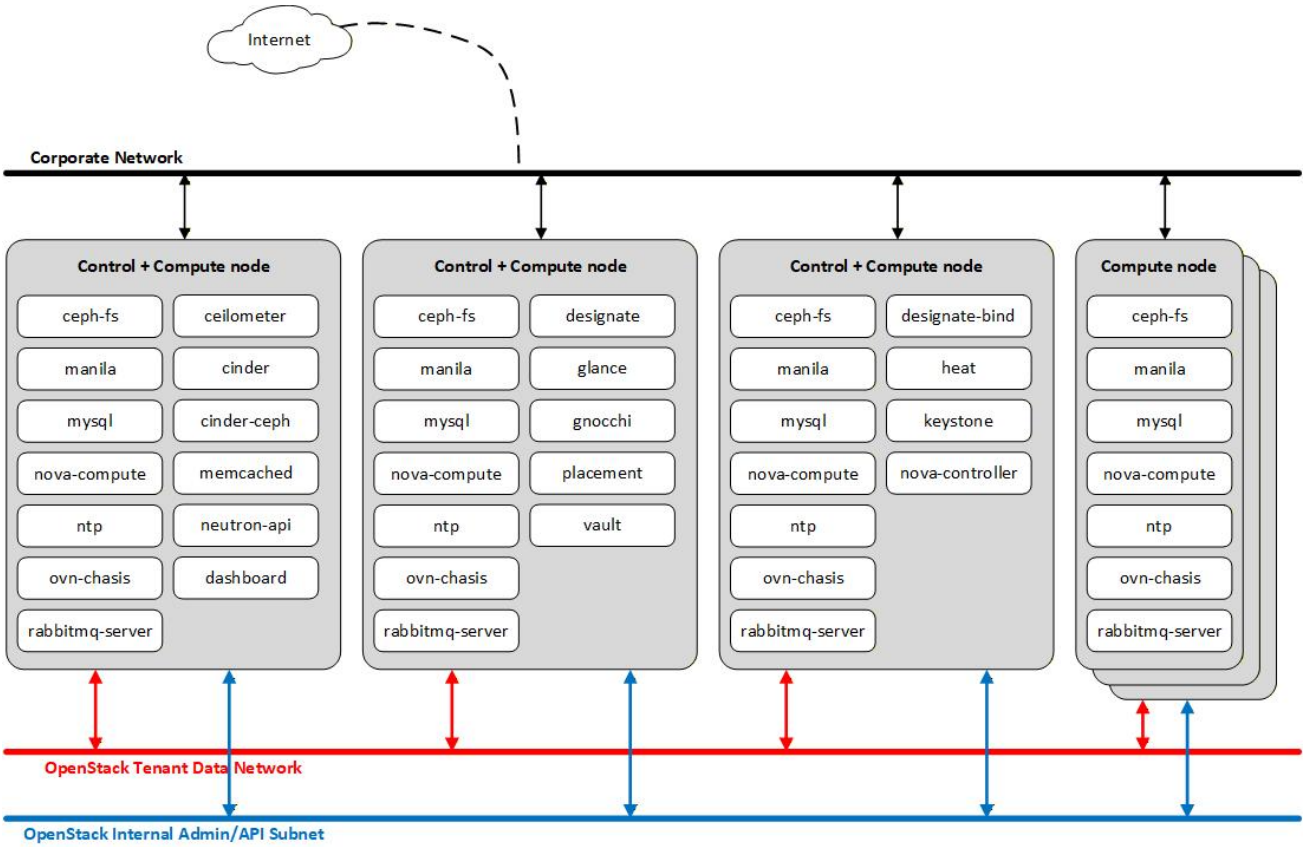
Predstavuje súbor aplikácií pre Control node potrebných pre správu clustra

Compute

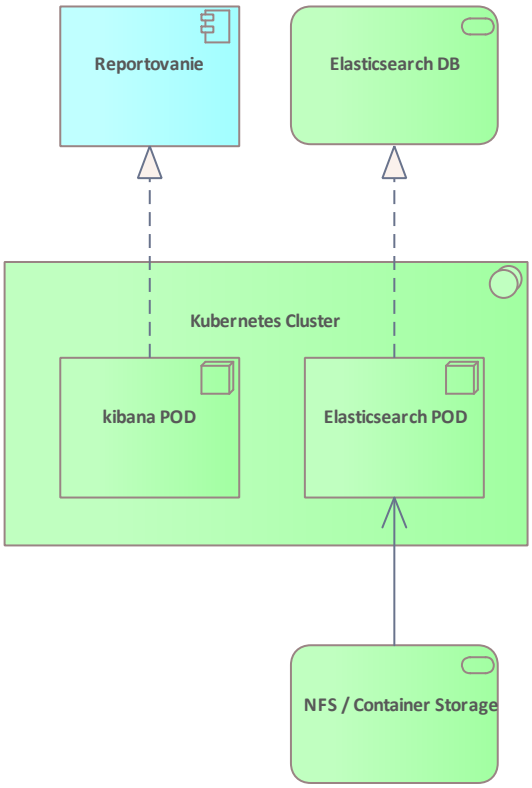
Predstavuje rolu a službu Compute nodu

Compute apps

Predstavuje súbor Compute aplikácií



7.1.7 Technology Viewpoint Reportovanie



Obrázok 61 : 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. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB

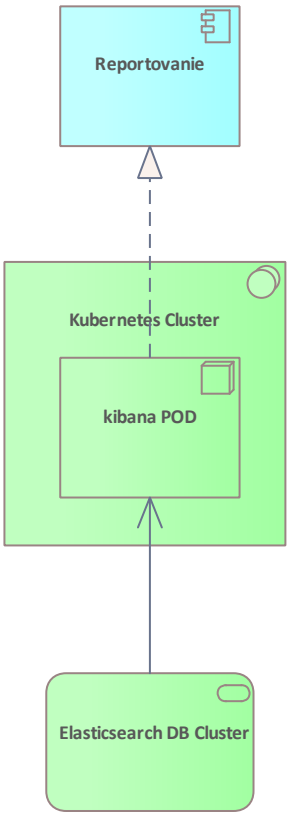
Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

kibana POD

Predstavuje POD Kibana pre Reportovanie.



Obrázok 62 : 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. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

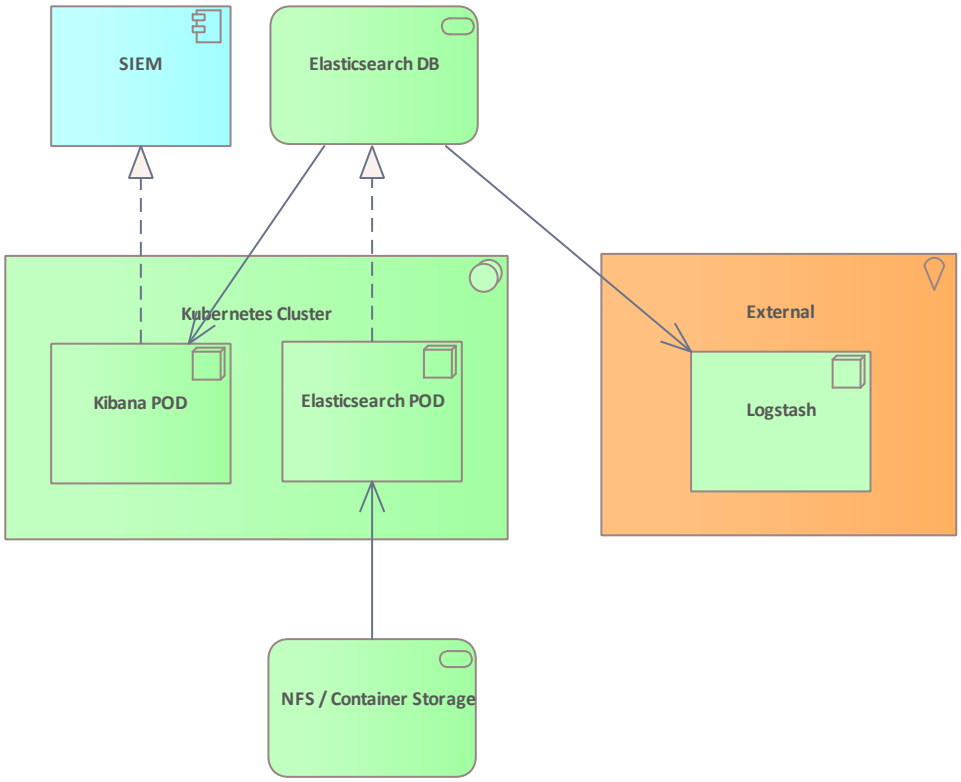
Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

kibana POD

Predstavuje POD Kibana pre Reportovanie.

7.1.8 Technology Viewpoint SIEM



Obrázok 63 : Technology Usage Viewpoint SIEM 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 Elasticsearch.

Popis používaných prvkov:

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.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB

Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

External

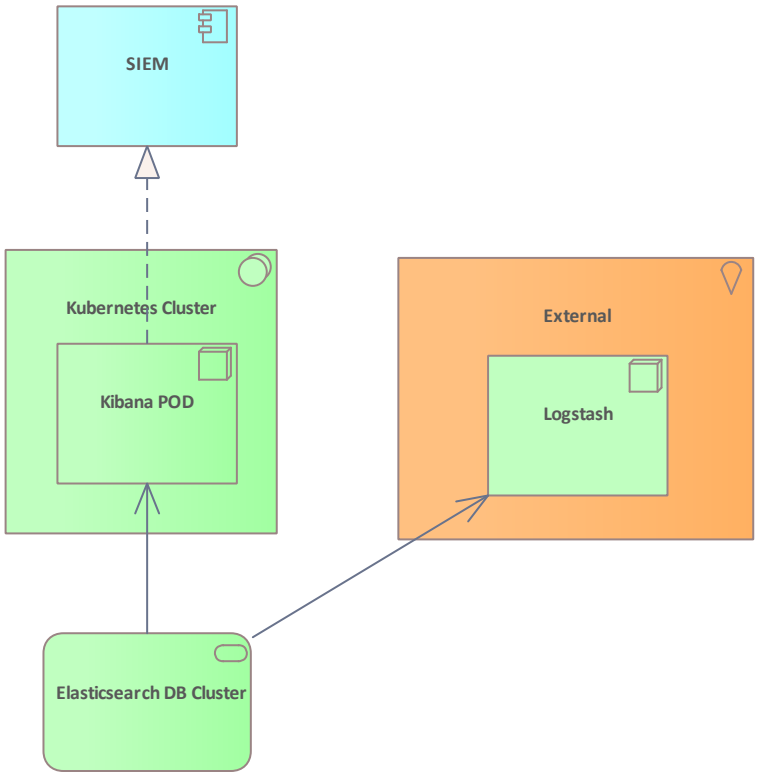
Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

Kibana POD

Predstavuje POD Kibana pre SIEM.

Logstash

Predstavuje inštanciu Logstashg pre spracovanie logov a ich zapísanie do Elasticsearch.



Obrázok 64 : Technology Usage Viewpoint SIEM 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:

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.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

External

Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

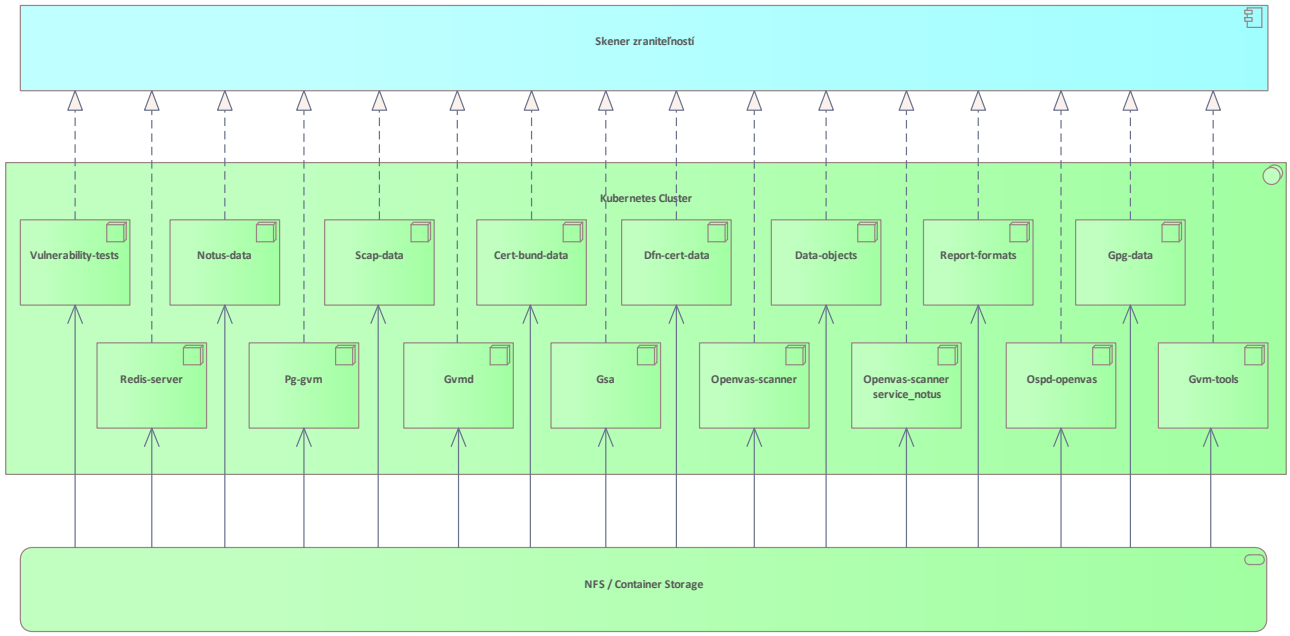
Kibana POD

Predstavuje POD Kibana pre SIEM.

Logstash

Predstavuje inštanciu Logstashg pre spracovanie logov a ich zapísanie do Elasticsearch.

7.1.9 Technology Viewpoint Skener zraniteľností



Obrázok 65 : Technology Usage Viewpoint Skener zraniteľností

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Popis používaných prvkov:

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.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Cert-bund-data

Predstavuje POD cert-bund-data.

Data-objects

Predstavuje POD data-objects.

Dfn-cert-data

Predstavuje POD dfn-cert-data.

Gpg-data

Predstavuje POD gpg-data.

Gsa

Predstavuje POD gsa.

Gvmd

Predstavuje POD gvmd.

Gvm-tools

Predstavuje POD gvm-tools.

Notus-data

Predstavuje POD notus-data.

Openvas-scanner

Predstavuje POD openvas-scanner.

Openvas-scanner service_notus

Predstavuje POD openvas-scanner service_notus.

Ospd-openvas

Predstavuje POD ospd-openvas.

Pg-gvm

Predstavuje POD pg-gvm.

Redis-server

Predstavuje POD redis-server.

Report-formats

Predstavuje POD report-formats.

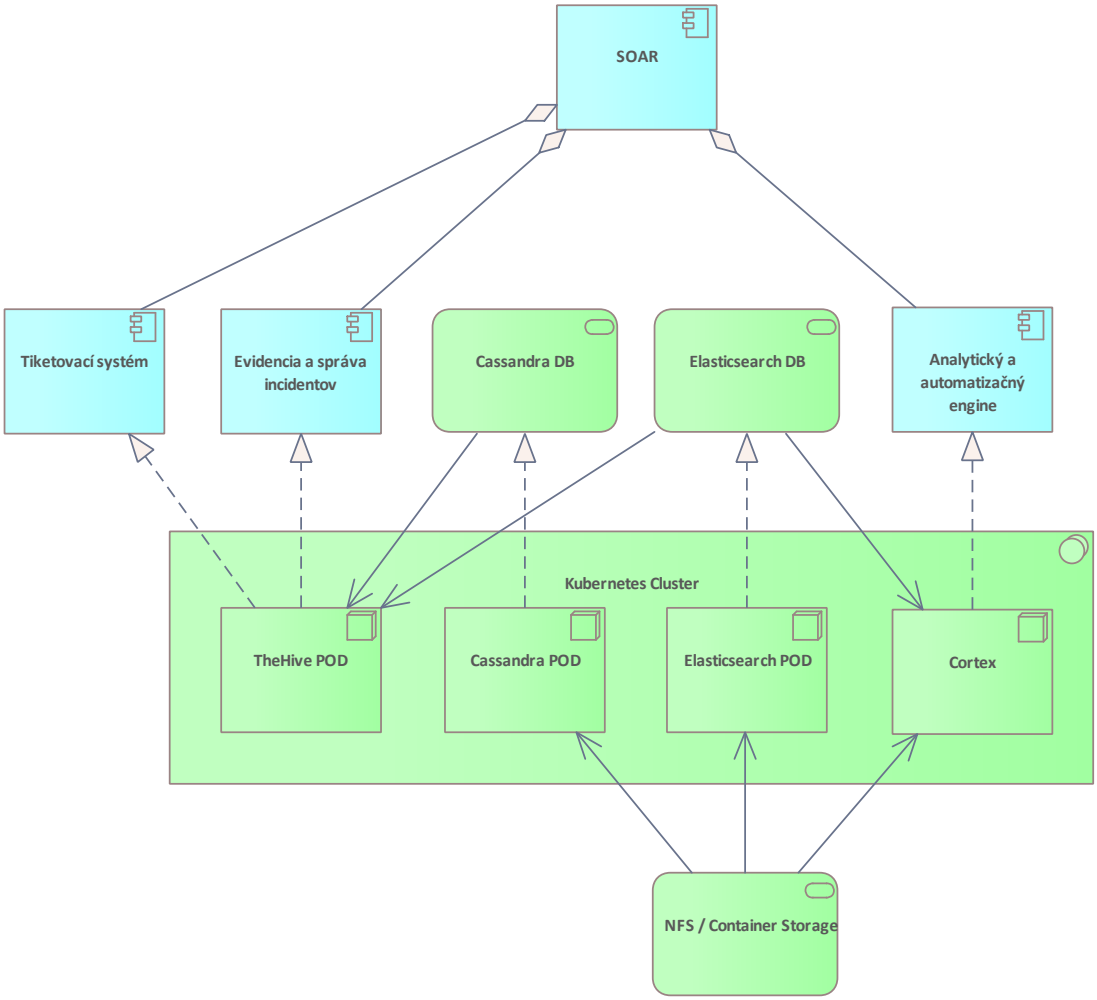
Scap-data

Predstavuje POD scap-data.

Vulnerability-tests

Predstavuje POD vulnerability-tests.

7.1.10 Technology Viewpoint SOAR



Obrázok 66 : Technology Usage Viewpoint SOAR 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:

Analytický a automatizačný engine

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.

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.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

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

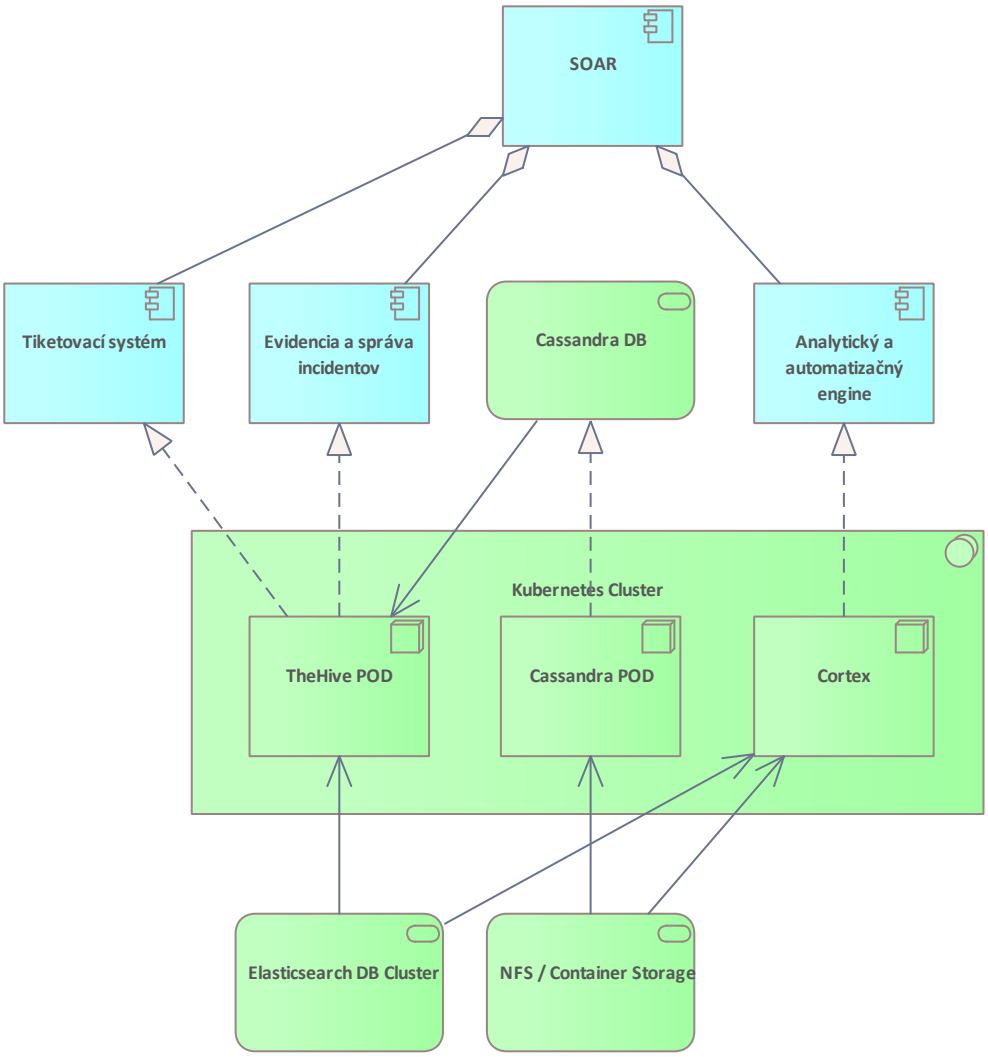
Predstavuje POD Elasticsearch pre NoSQL databázu.

TheHive POD

Predstavuje POD TheHive pre invertarizáckiu aktív.

Cortex

Predstavuje POD Cortex pre SOAR.



Obrázok 67 : Technology Usage Viewpoint SOAR 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.

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.

NFS / Container Storage

Predstavuje službu NFS alebo iného Container Storage. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

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.

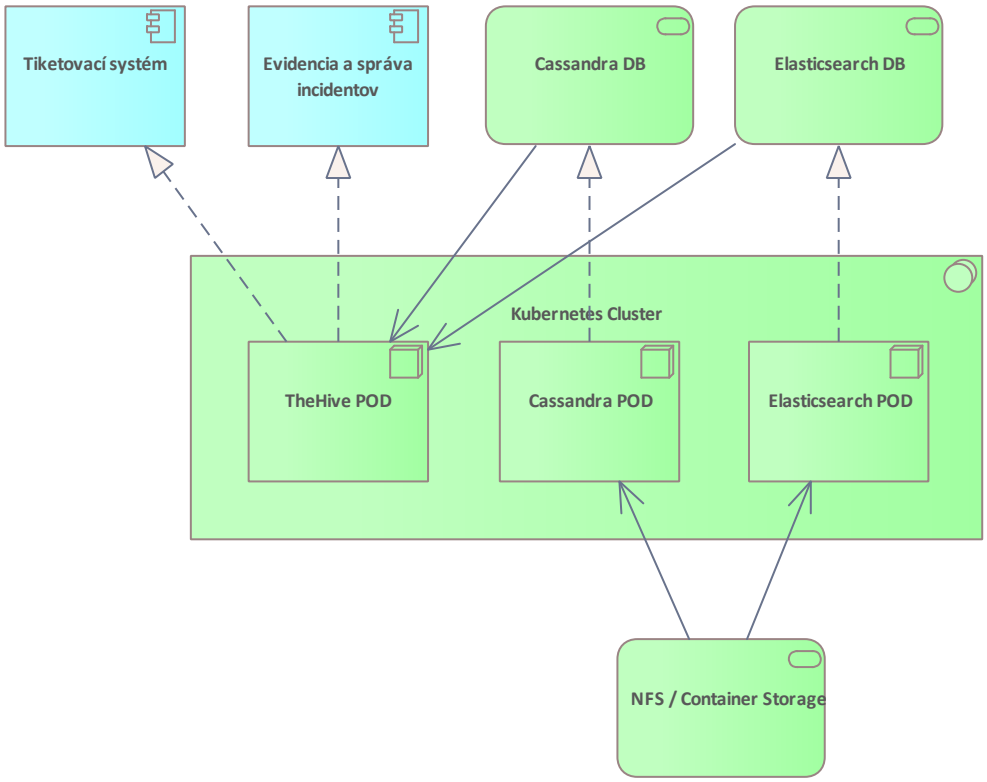
TheHive POD

Predstavuje POD TheHive pre invertarizáckiu aktív.

Cortex

Predstavuje POD Cortex pre SOAR.

7.1.11 Technology Viewpoint Tiketovací sytém / Evidencia a správa incidentov



Obrázok 68 : 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. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Cassandra DB

Predstavuje technologickú službu NoSQL Cassandra databázy.

Elasticsearch DB

Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Cassandra POD

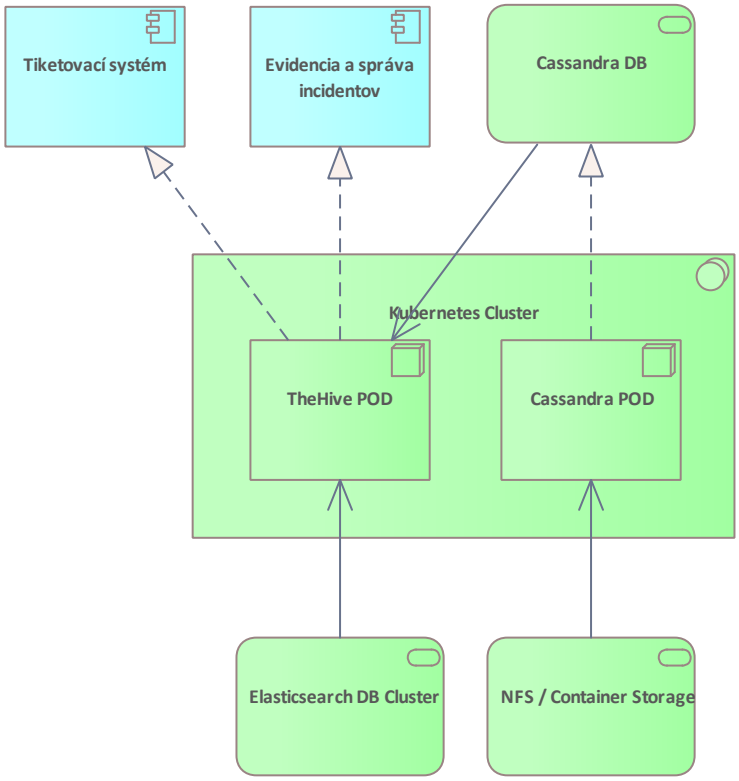
Predstavuje POD Apache Cassandra pre NoSQL databázu.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

TheHive POD

Predstavuje POD TheHive pre invertarizáckiu aktív.



Obrázok 69 : 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. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Cassandra DB

Predstavuje technologickú službu NoSQL Cassandra databázy.

Elasticsearch DB Cluster

Predstavuje technologickú službu NoSQL Elasticsearch databázy vo forme Clustra.

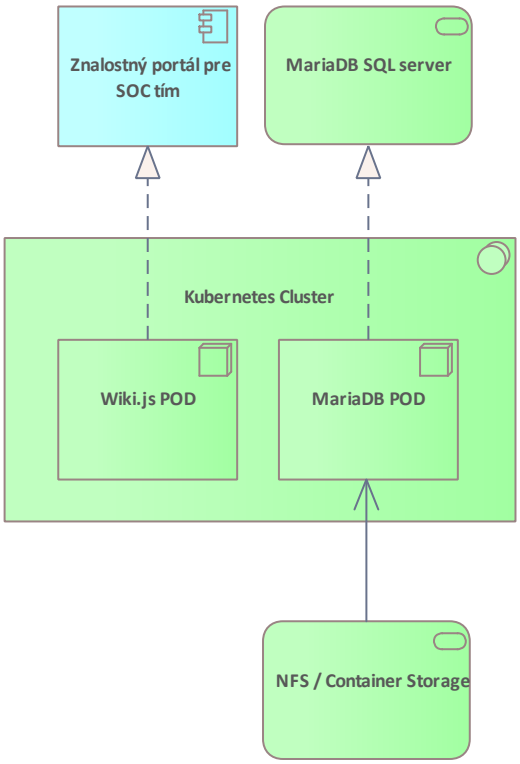
Cassandra POD

Predstavuje POD Apache Cassandra pre NoSQL databázu.

TheHive POD

Predstavuje POD TheHive pre invertarizáckiu aktív.

7.1.12 Technology Viewpoint Znalostný portál pre SOC tím



Obrázok 70 : 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. NFS (Network File System) je sieťový súborový protokol vrstvy aplikačného modelu OSI, ktorý umožňuje vzdialený prístup ku súborovým systémom cez sieť. Je to jedna z najbežnejších foriem zdieľaného úložiska (shared storage) v kontajnerizovaných prostrediach, ako napr. Kubernetes, kde je implementovaný ako PersistentVolume (PV) typ. V širšom zmysle, container storage označuje mechanizmy a služby poskytujúce úložný priestor pre kontajnery, ktoré potrebujú perzistentné alebo zdieľané dáta medzi reštartmi či medzi uzlami klastra.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

MariaDB SQL server

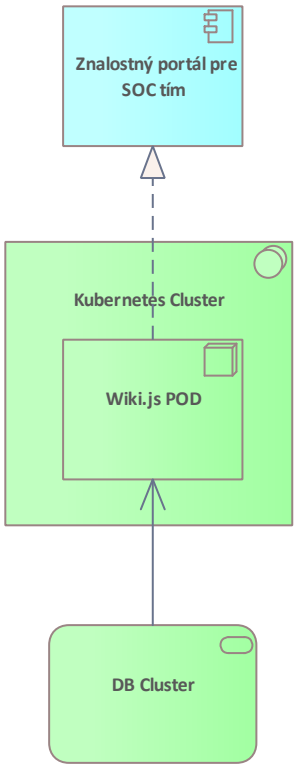
Predstavuje technologickú službu relačnej MariaDB SLQ databázy.

MariaDB POD

Predstavuje POD MariaDB pre relačnú SQL DB.

Wiki.js POD

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



Obrázok 71 : 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. Služba clustrovanej relačnej databázy je distribuovaný databázový systém, ktorý poskytuje služby relačnej databázy prostredníctvom viacerých prepojených databázových uzlov (clustrov), čím zabezpečuje vysokú dostupnosť, škálovateľnosť, redundanciu a odolnosť voči poruchám.

Kubernetes Cluster

Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou fyzických alebo virtuálnych serverov.V klustri Kubernetes sú výpočtové zdroje (CPU, pamäť, storage, sieť) abstrahované a spravované ako jednotný systém, čo umožňuje automatizované riadenie životného cyklu aplikácií.

Wiki.js POD

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

7.2 Technologické komponenty riešenia a ich vzťah k aplikačným komponentom

7.2.1 Správa prístupov, účtov a kľúčov prevádzkových prostredí

7.2.2 Kontajnerizácia a orchestrácia cloudových služieb

7.2.3 Špecifikácia využitia služieb vládneho cloudu

7.3 Popis testovacieho prostredia

Uvedený v kapitole 7.1.

7.4 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:

. 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:

Vysoká dostupnosť systému použitím softvérového clustrovania. Tým je zabezpečený rýchly a od obsluhy nezávislý nábeh systému po hardvérovej alebo softvérovej havárii, prípadne poruche systému.

Cyklické (a automatické) zálohovanie dát (logy systémov, aplikačné dáta, samotné aplikácie...). Týmto ochraňujeme systém proti prípadnej strate cenných dát.

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.

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.

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