PROJEKT

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

V12 Biznis architektúra

KPB4 – Architektúra riešenia

typ – dokumentácia

mesiac odovzdania – M22

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

ÚRAD VLÁDY
SLOVENSKEJ REPUBLIKY

Obsah

1. Úvod 3
2. Aplikačná architektúra 3
1.1. Aplication Viewpoints DELETE OLD 7
3. technologická architektúra 14
1.2. Technology Viewpoint Inventarizacia aktiv 14
1.3. Technology Viewpoint Kubernetes 17
1.4. Technology Viewpoint OpenStack 32
1.5. Technology Viewpoint Reportovanie 35
1.6. Technology Viewpoint Tiketovací sytém / Evidencia a správa incidentov 38
1.7. Technology Viewpoint Znalostný portál pre SOC tím 41
4. Záver 44

1. ÚVOD

Zámerom projektu je vyvinúť technologicky moderné, otvorené a škálovateľné riešenie, ktoré bude schopné podporiť organizácie v efektívnom zvládaní kybernetických hrozieb. Projekt reaguje na potreby najmä malých a stredných organizácií, ktoré často nedisponujú dostatočnými odbornými kapacitami ani rozpočtom na vybudovanie vlastného bezpečnostného centra. Tento dokument popisuje fyzickú architektúru 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.

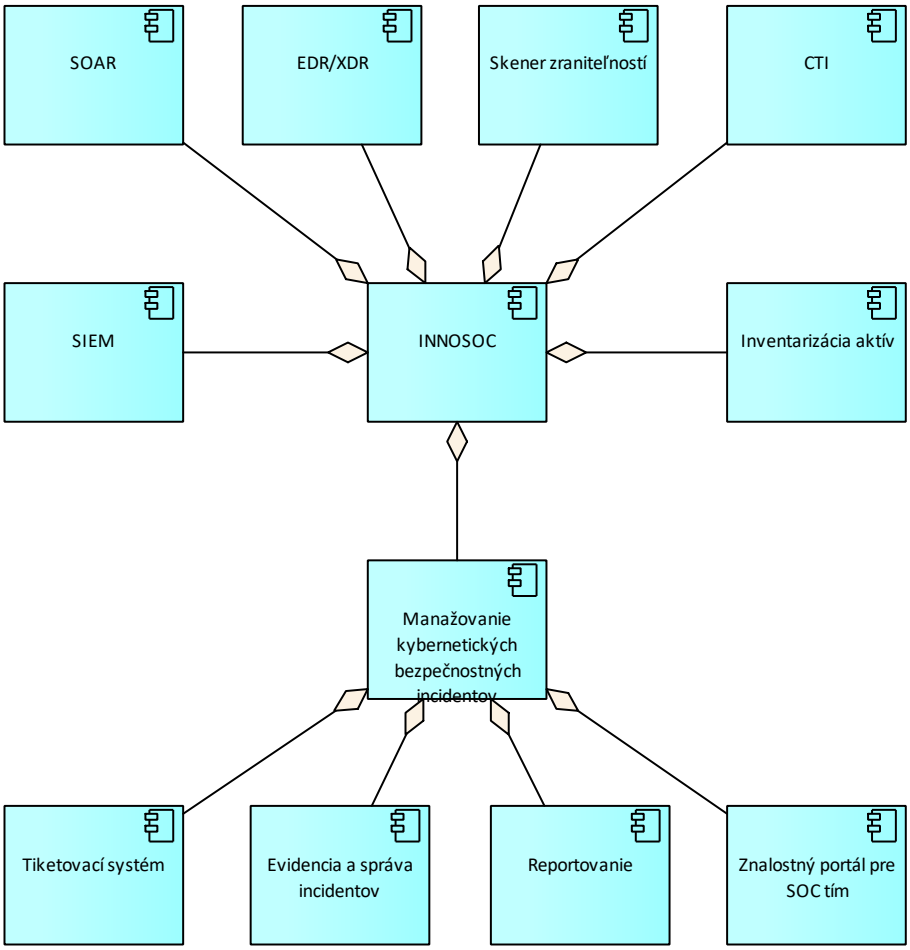
2. APLIKAČNÁ ARCHITEKTÚRA

Aplikačná architektúra modulu CNM je kompletne namodelovaná v nástroji Sparx Enterprise Architect (EA) v notácii Archimate 3.0.

V nasledujúcej kapitole je zobrazený diagram aplikačnej architektúry s popismi objektov, ktoré boli vygenerované z EA, ako výstup.

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

Nakoľko je výstup pre modelovanie aplikačnej architektúry DNR generovaný z EA, v prípade, že je daný objekt aplikačnej architektúry použitý viackrát, jeho popis je identický.



Obrázok 1 : Aplication Viewpoints Components

Diagram predstavuje HL zoznam komponentov riešenia.

Popis používaných prvkov:

CTI

CTI (Cyber Threat Intelligence) predstavuje kľúčový stavebný prvok SOCaaS architektúry, pretože poskytuje schopnosť obohacovať detekčné pravidlá, korelačné mechanizmy a playbooky o externé informácie o hrozbách – vrátane IOC, TTP, profilovania útočníkov, kampaní a súvisiacich zraniteľností. V prostredí viaczákaznícke služby SOCaaS zohráva úlohu pri:
• Distribúcii a správe threat feedov naprieč tenantmi,
• Automatickom obohacovaní SIEM a EDR dát o známe hrozby,
• Vytváraní časových línií útokov a priraďovaní k MITRE ATT&CK technikám,
• Podpore procesov threat huntingu a forenznej analýzy,
• Prioritizácii incidentov podľa kontextu hrozieb.
Pre návrh riešenia boli zvolené open-source platformy, ktoré pokrývajú rôzne aspekty CTI – od zberu IOC cez vizualizáciu, až po STIX/TAXII kompatibilitu.

EDR/XDR

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

mailových systémov a iných vrstiev.

Evidencia a správa incidentov

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

INNOSOC

Inventarizácia aktív

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

Manažovanie kybernetických bezpečnostných incidentov

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

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

Reportovanie

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

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

SIEM

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

Skener zraniteľností

Skener zraniteľností je základným stavebným kameňom pre zabezpečenie proaktívneho prístupu v SOCaaS architektúre. Umožňuje pravidelne identifikovať slabé miesta v infraštruktúre, hodnotiť stav aktualizácií, konfigurácií a nastavení, a poskytovať informácie pre ďalšiu prioritizáciu a

plánovanie nápravných opatrení. Výstupy skenera sú často zdrojom pre SOAR systémy, SLA metriky, reporting ako aj pre hodnotenie bezpečnostnej úrovne klienta.

SOAR

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

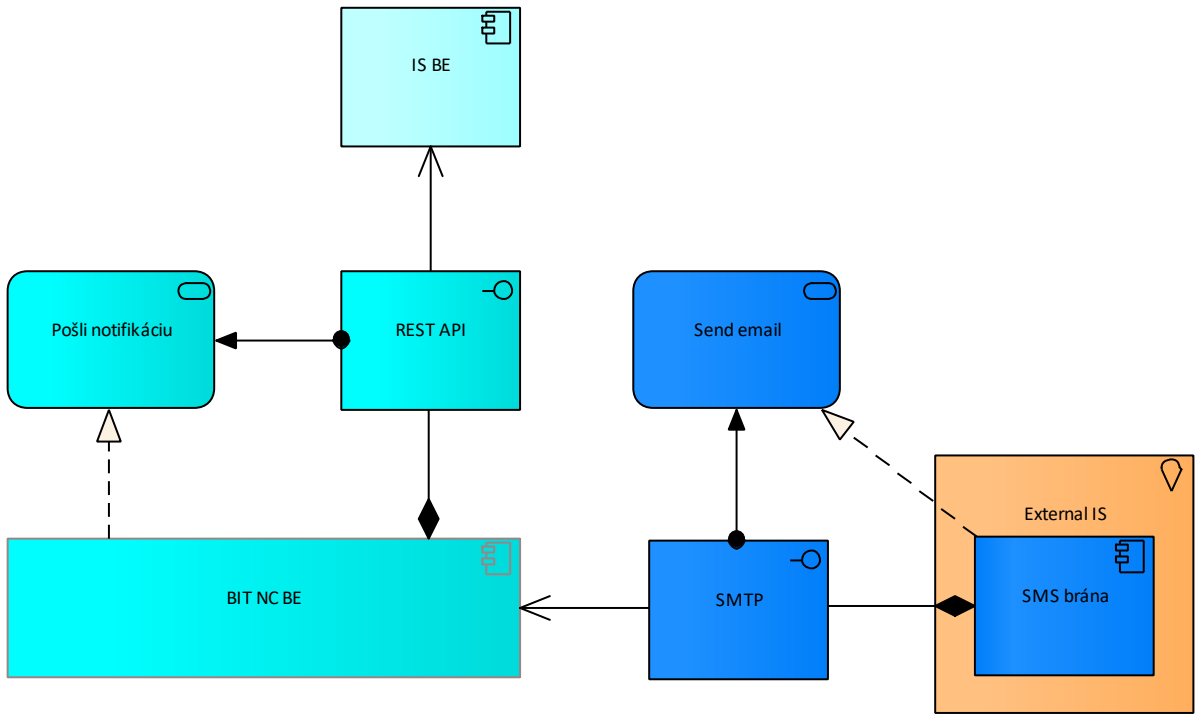
Tiketovací systém

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

Znalostný portál pre SOC tím

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

1.1. Aplication Viewpoints DELETE OLD



Obrázok 2 : Application Cooperation Viewpoint Empire and BIT NC

Diagram predstavuje integráciu IS BE na služby zasielania notifikácií modulu BIT NC pomocou REST API a integráciu BIT NC na Mailový server pomocou SMTP a jeho služby zasielania emailov.

Popis používaných prvkov:

Pošli notifikáciu
Predstavuje HTTP POST, GET, PUT a DELETE metódy služby pre zaslanie notifikácie.

Send email
Služba na poslanie emailu.

External IS
Externé informačné systémy.

BIT NC BE
BIT NC BE predstavuje BE modul BIT Notify Center, ktorý zabezpečuje centrálnu správu notifikácií s príslušným BIT NC FE.

IS BE
Hlavný BE komponent IS, ktorý využíva služby NFQES Enterprise IAM a BIT NC a poskytuje rozhranie pre IS FE modul.

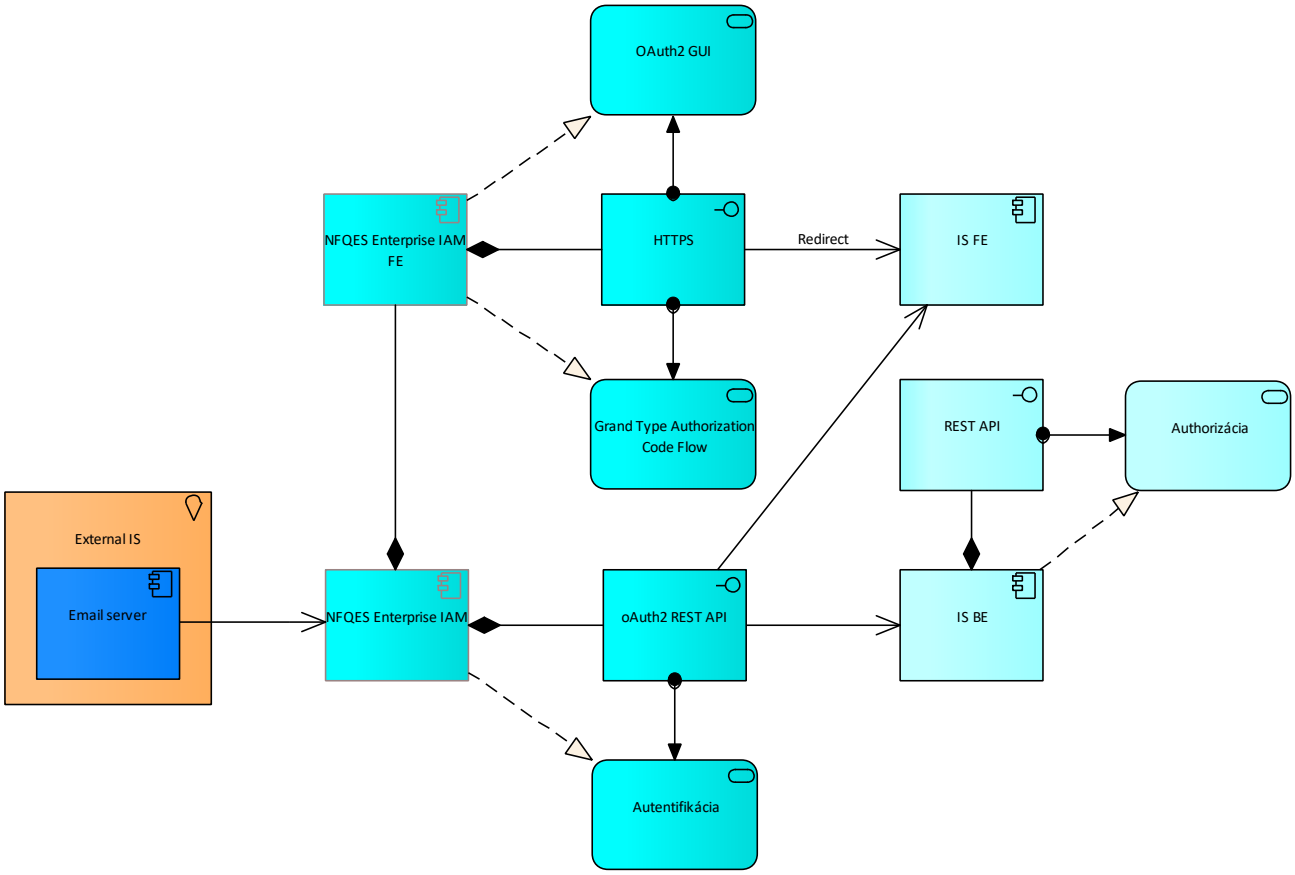
REST

API

Predstavuje REST API modulu BIT NC.

SMTP
SMTP služba Mailového servera. Port 587 pre Secure SMTP, prípadne 465 a v prípade interného Mailového servera možný aj port 25 (neodporúča sa).

SMS brána
Predstavuje Emailový server pripojený pomocou mena a hesla cez SMTP.



Obrázok 3 : Application Cooperation Viewpoint IS and BIT IAM

Diagram predstavuje vzájomnú integráciu medzi budovaným IS a existujúcim modulom NFQES Enterprise IAM.

Popis používaných prvkov:

Autentifikácia
Predstavuje HTTP POST, GET, PUT a DELETE metódy služby pre Authentifikáciu.

Authorizácia
Predstavuje aplikačnú službu autorizácie.

Grand Type Authorization Code Flow
Grand Type - Authorization Code Flow.
Poznámka - Druhý flow ktorý neimpelmentujeme je Pasword Flow (Prihalasovanie priamo z apky - nesmie újsť klient id a password).

OAuth2 GUI
Predstavuje HTTP stránky NFQES Enterprise IAM.

External IS
Externé informačné systémy.

IS BE
Hlavný BE komponent IS, ktorý využíva služby NFQES Enterprise IAM a BIT NC a poskytuje rozhranie pre IS FE modul.

IS FE
Hlavný FE komponent IS, ktorý využíva služby IS BE a NFQES Enterprise IAM.

NFQES Enterprise IAM
NFQES Enterprise IAM predstavuje modul BIT Identity Access Management, ktorý zabezpečuje autentifikáciu a správu rolí s príslušným NFQES Enterprise IAM FE.

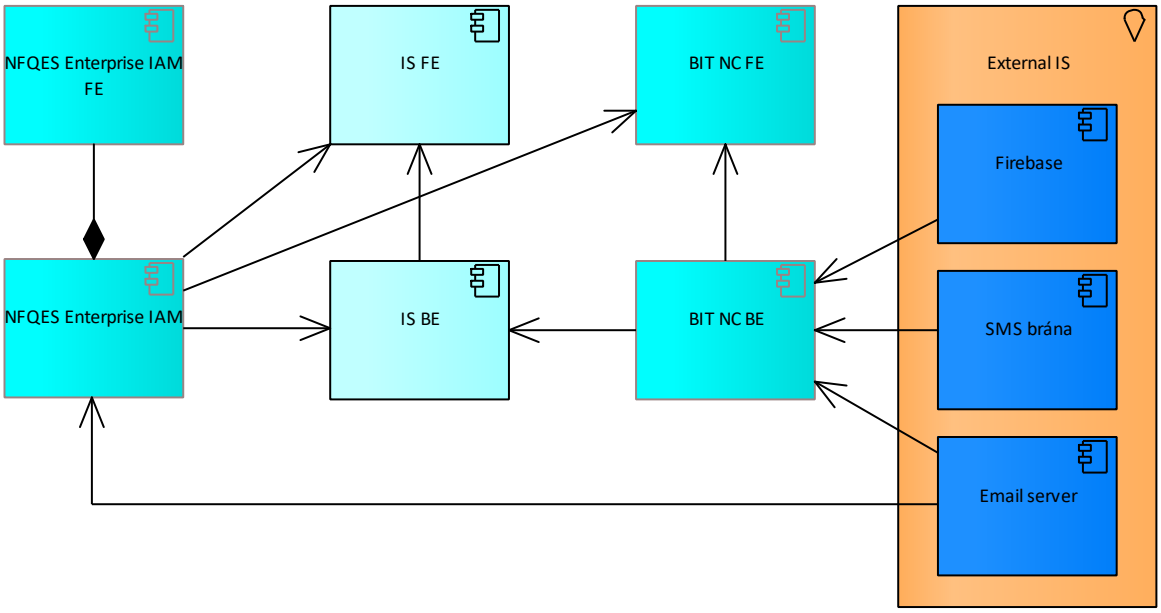
NFQES Enterprise IAM FE
IAM FE predstavuje FE submodul NFQES Enterprise IAM FE modulu, ktorý zabezpečuje základné obrazovky potrebné pre flow autentifikácie.

HTTPS
Predstavuje HTTPS interface modulu NFQES Enterprise IAM.

oAuth2 REST API
Predstavuje oAuth2 REST API modulu NFQES Enterprise IAM.

REST API
Predstavuje REST API modulu IS BE.

Email server
Predstavuje účtovný program, do ktorého sa budú importovať v dohodnutom formáte dáta. Jedná a o procesnú intergáciu.



Obrázok 4 : Application Structure Viewpoint

Diagram predstavuje High Level architektonickú schému prepojenia komponentov.

Popis používaných prvkov:

External IS
Externé informačné systémy.

BIT NC BE
BIT NC BE predstavuje BE modul BIT Notify Center, ktorý zabezpečuje centrálnu správu notifikácií s príslušným BIT NC FE.

BIT NC FE
BIT NC FE predstavuje samostatný FE modul využívajúci modul BIT NC.

IS BE
Hlavný BE komponent IS, ktorý využíva služby NFQES Enterprise IAM a BIT NC a poskytuje rozhranie pre IS FE modul.

IS FE
Hlavný FE komponent IS, ktorý využíva služby IS BE a NFQES Enterprise IAM.

NFQES Enterprise IAM
NFQES Enterprise IAM predstavuje modul BIT Identity Access Management, ktorý zabezpečuje autentifikáciu a správu rolí s príslušným NFQES Enterprise IAM FE.

NFQES Enterprise IAM FE
IAM FE predstavuje FE submodul NFQES Enterprise IAM FE modulu, ktorý zabezpečuje základné obrazovky potrebné pre flow autentifikácie.

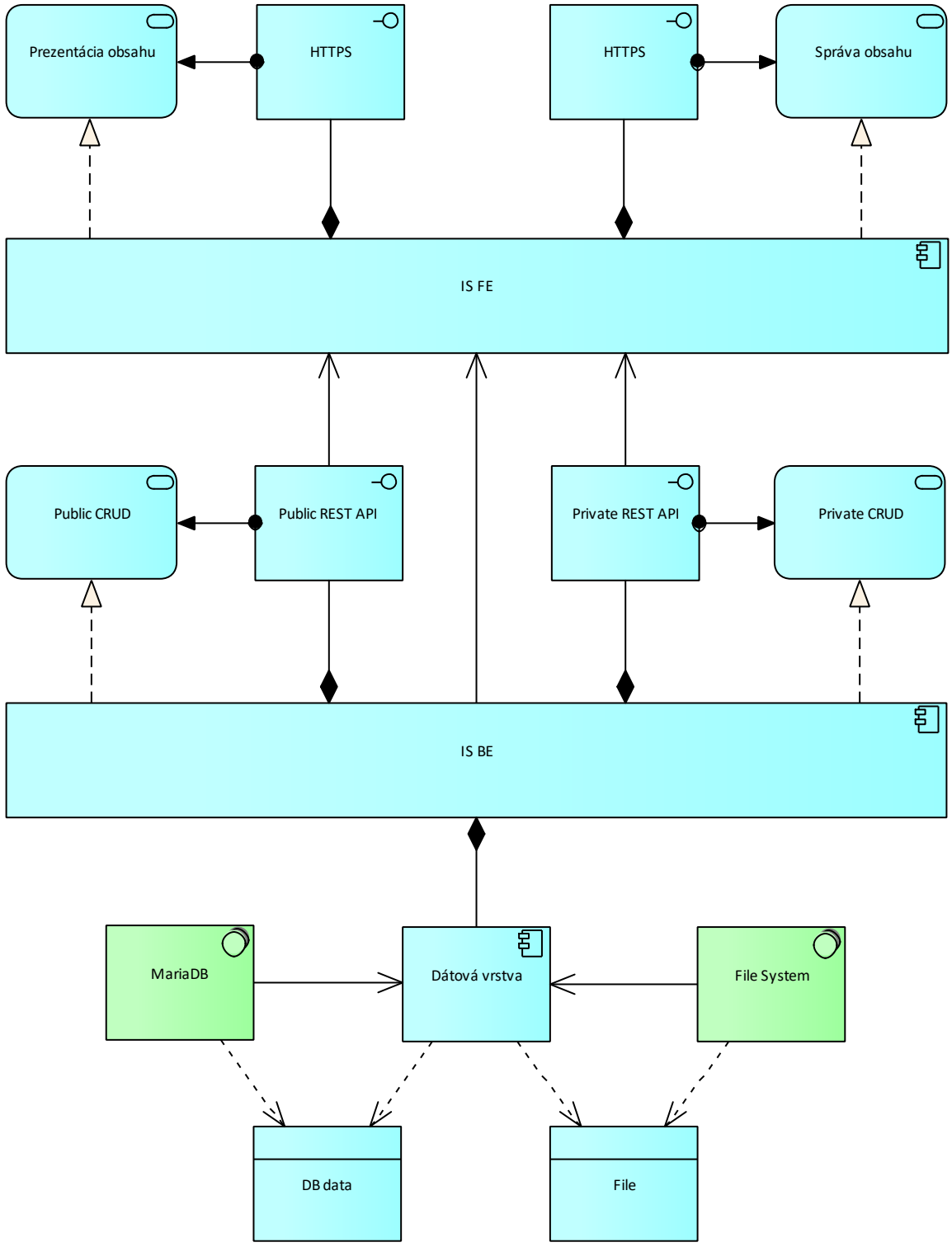
Email server
Predstavuje účtovný program, do ktorého sa budú importovať v dohodnutom formáte dáta. Jedná a o procesnú intergáciu.

Firebase

Predstavuje účtovný program, do ktorého sa budú importovať v dohodnutom formáte dáta. Jedná a o procesnú intergáciu.

SMS brána

Predstavuje Emailový server pripojený pomocou mena a hesla cez SMTP.



Obrázok 5 : Implementation and Deployment Viewpoint with bussines objects - Empire

Diagram predstavuje Aplikačnú architektúru IS a jeho vzájomné prepojenie pomocou REAST API rozhraní. Zároveň znázorňuje aj využívanie perzistentnej vrstvy v podobe relačnej SQL databázy MariaDB a File systému.

Popis

používaných prvkov:

Prezentácia obsahu
Predstavuje aplikačnú službu prezentácie obsahu.

Private CRUD
Predstavuje private HTTP POST, GET, PUT a DELETE metódy služby.

Public CRUD
Predstavuje public HTTP POST, GET, PUT a DELETE metódy služby.

Správa obsahu
Predstavuje aplikačnú službu správy obsahu.

DB data
Predstavuje databázové dáta.

File
Štandardný súbor reprezentujúci akékoľvek potrebné dáta ako obrázky, dokumenty a iné.

File System
Lokálny súborový systém pre štandardnú prácu so súbormi.

MariaDB
Relačná SQL databáza poskytujúca perzistentnú vrstvu pre dáta okrem súborov.

Dátová vrstva
Predstavuje komponent Empire BE modulu, ktorý zabezpečuje operácie nad perzistentnou vrstvou v podobe File systému, databázy a prípadne iné.

IS BE
Hlavný BE komponent IS, ktorý využíva služby NFQES Enterprise IAM a BIT NC a poskytuje rozhranie pre IS FE modul.

IS FE
Hlavný FE komponent IS, ktorý využíva služby IS BE a NFQES Enterprise IAM.

HTTPS
Predstavuje HTTPS rozhranie pre prístup k obsahu.

HTTPS
Predstavuje HTTPS rozhranie pre správu obsahu.

Private REST API
Predstavuje private REST API modulu WCM.

Public REST API
Predstavuje public REST API modulu WCM.

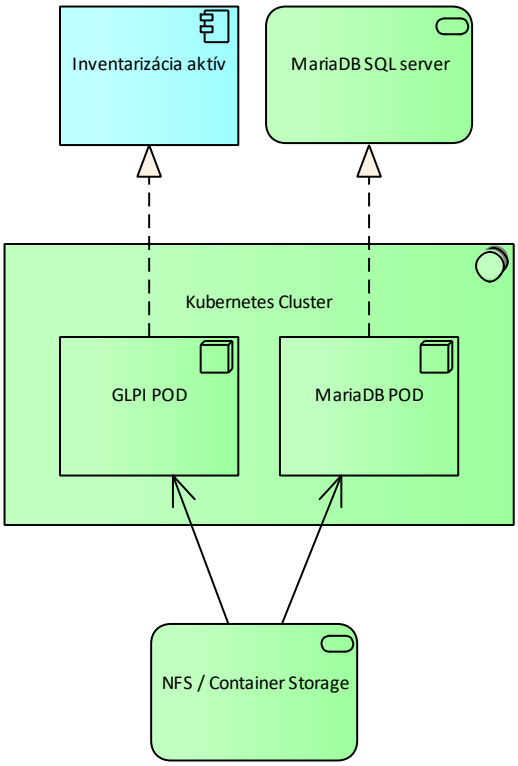
3. TECHNOLOGICKÁ ARCHITEKTÚRA

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.

1.2. Technology Viewpoint Inventarizacia aktiv



Obrázok 6 : Technology Usage Viewpoint Inventarizacia aktiv alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Alt 1

predstavuje využitie Databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou SQL servera.

Popis používaných prvkov:

Inventarizácia aktív

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

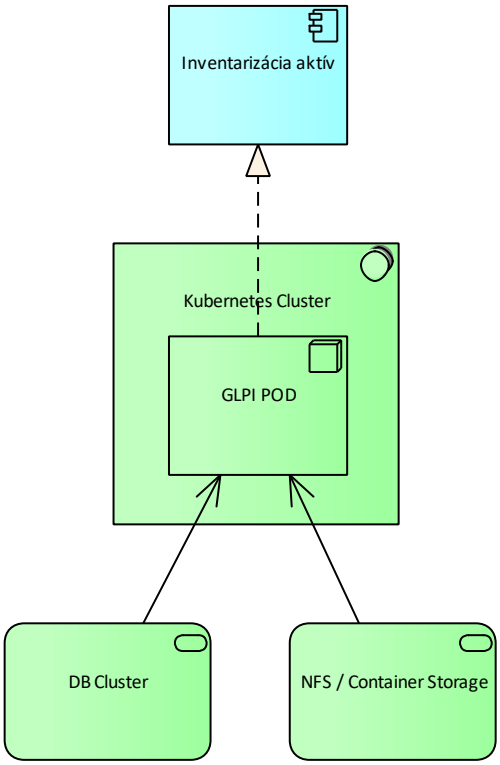
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

MariaDB SQL server
Predstavuje technologickú službu relačnej MariaDB SLQ databázy.

GLPI POD
Predstavuje POD GLPI pre invertarizáckiu aktív.

MariaDB POD
Predstavuje POD MariaDB pre relačnú SQL DB.



Obrázok 7 : Technology Usage Viewpoint Inventarizacia aktiv alt 2

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

Popis používaných prvkov:

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

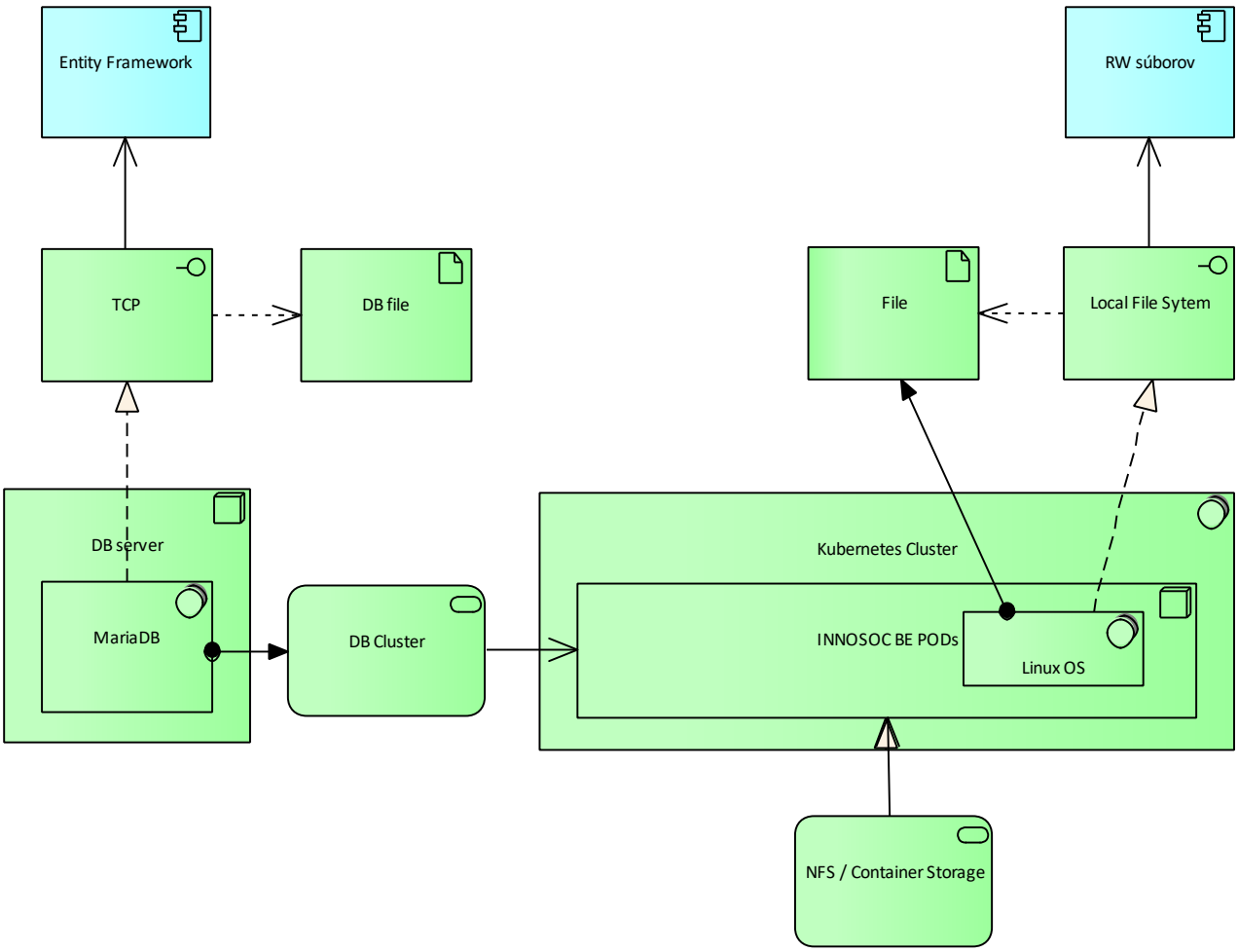
DB Cluster
Predstavuje službu clustrovanej relačnej databázy

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

GLPI POD
Predstavuje POD GLPI pre invertarizáckiu aktív.

1.3. Technology Viewpoint Kubernetes



Obrázok 8 : Technology Usage Viewpoint CNM BE, DB and File System

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

Popis používaných prvkov:

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

file

DB file - súbor reprezentujúci databázový súbor MariaDB

DB server
Predstavuje MariaDB server

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

Entity Framework
Predstavuje aplikačný modul Entity Framework

RW súborov
Predstavuje modul RW nad súbormi

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

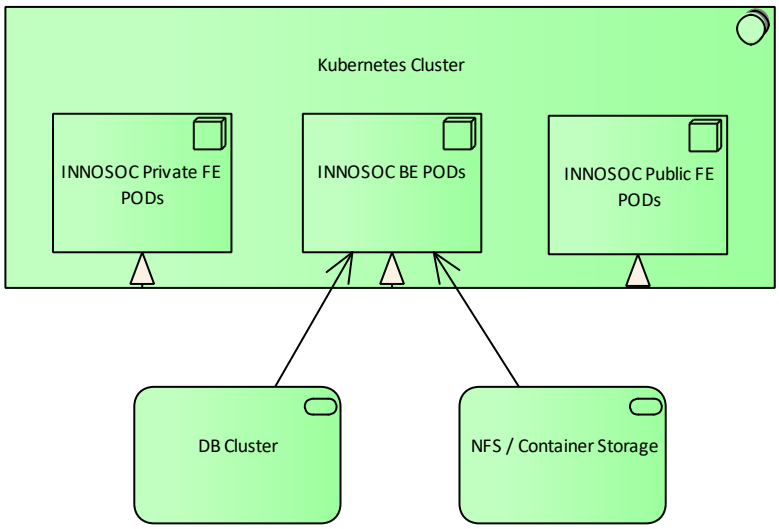
TCP
Predstavuje client server komunikáciu pomocou TCP protokolu

Kubernetes Cluster
Predstavuje Kubernetes Cluster

INNOSOC BE PODs
Predstavuje PODy CNM BE

Linux OS

MariaDB
Predstavuje MariaDB relačnú databázu



Obrázok 9 : Technology Usage Viewpoint CNM and Containers maping

Diagram znázorňuje priradenie jednotlivých PODov k prislúchajúcim aplikačným komponentom.

Popis používaných prvkov:

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

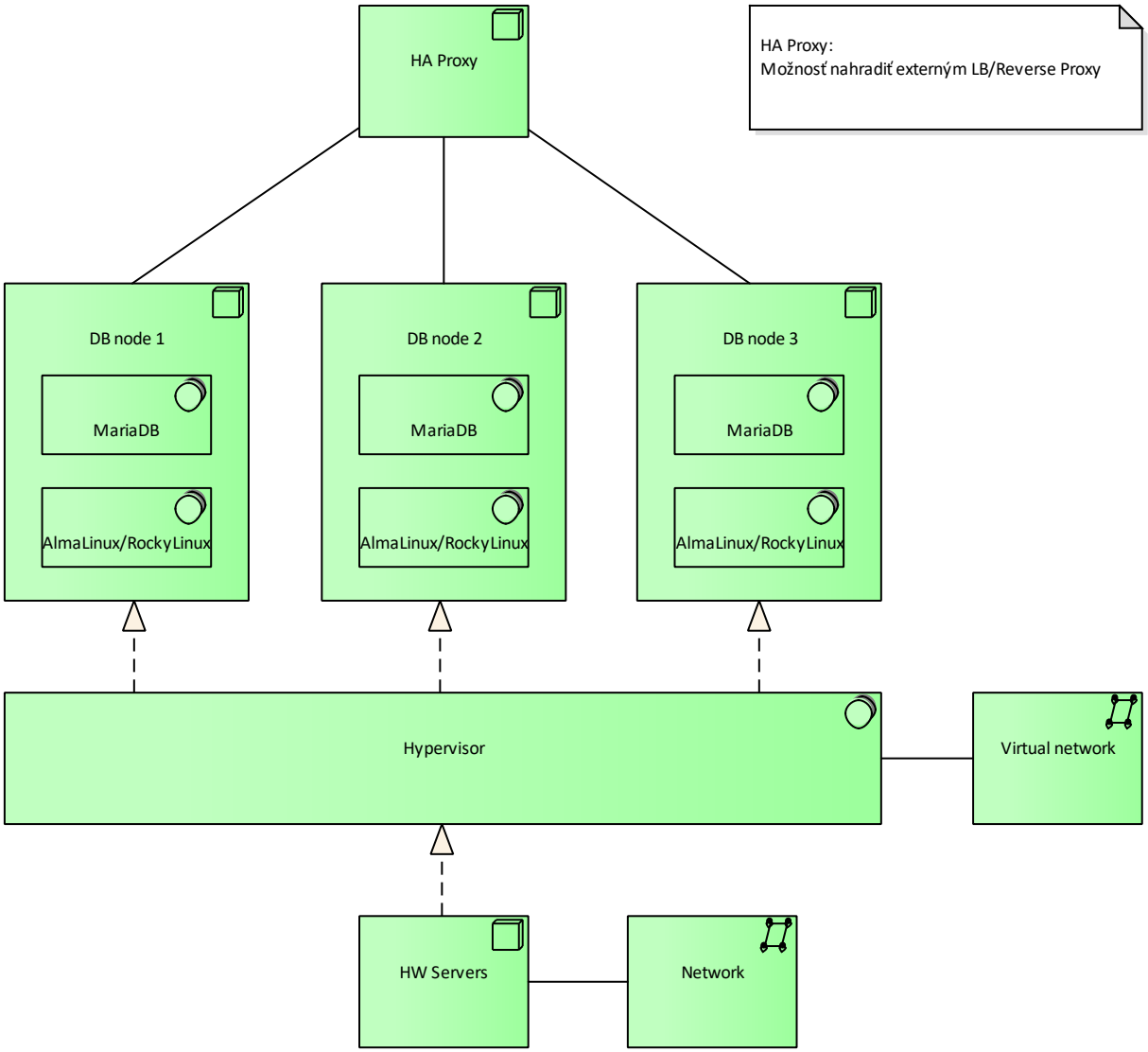
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

INNOSOC BE PODs
Predstavuje PODy CNM BE

INNOSOC Private FE PODs
Predstavuje PODy CNM FE Private

INNOSOC Public FE PODs
Predstavuje PODy CNM FE Public



Obrázok 10 : Technology Viewpoint DB Cluster

Diagram znázorňuje technologickú architektúru PostgreSQL Clustra.

Popis používaných prvkov:

DB node 1
Predstavuje Node 2 MariaDB Galera Clustra

DB node 2
Predstavuje Node 2 MariaDB Galera Clustra

DB node 3
Predstavuje Node 3 MariaDB Galera Clustra

HA Proxy
Predstavuje Internú reverse proxy postavenú na HA Proxy

HW Servers

Predstavuje HW serverovú infraštruktúru

Hypervisor
Predstavuje Hypervisor 1. alebo 2. typu

Network
Predstavuje sieť/subsieť HW infraštruktúry

Virtual network
Predstavuje virtuálnu sieť/subsieť Hypervisora

Note
HA Proxy:
Možnosť nahradiť externým LB/Reverse Proxy

AlmaLinux/RockyLinux
Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

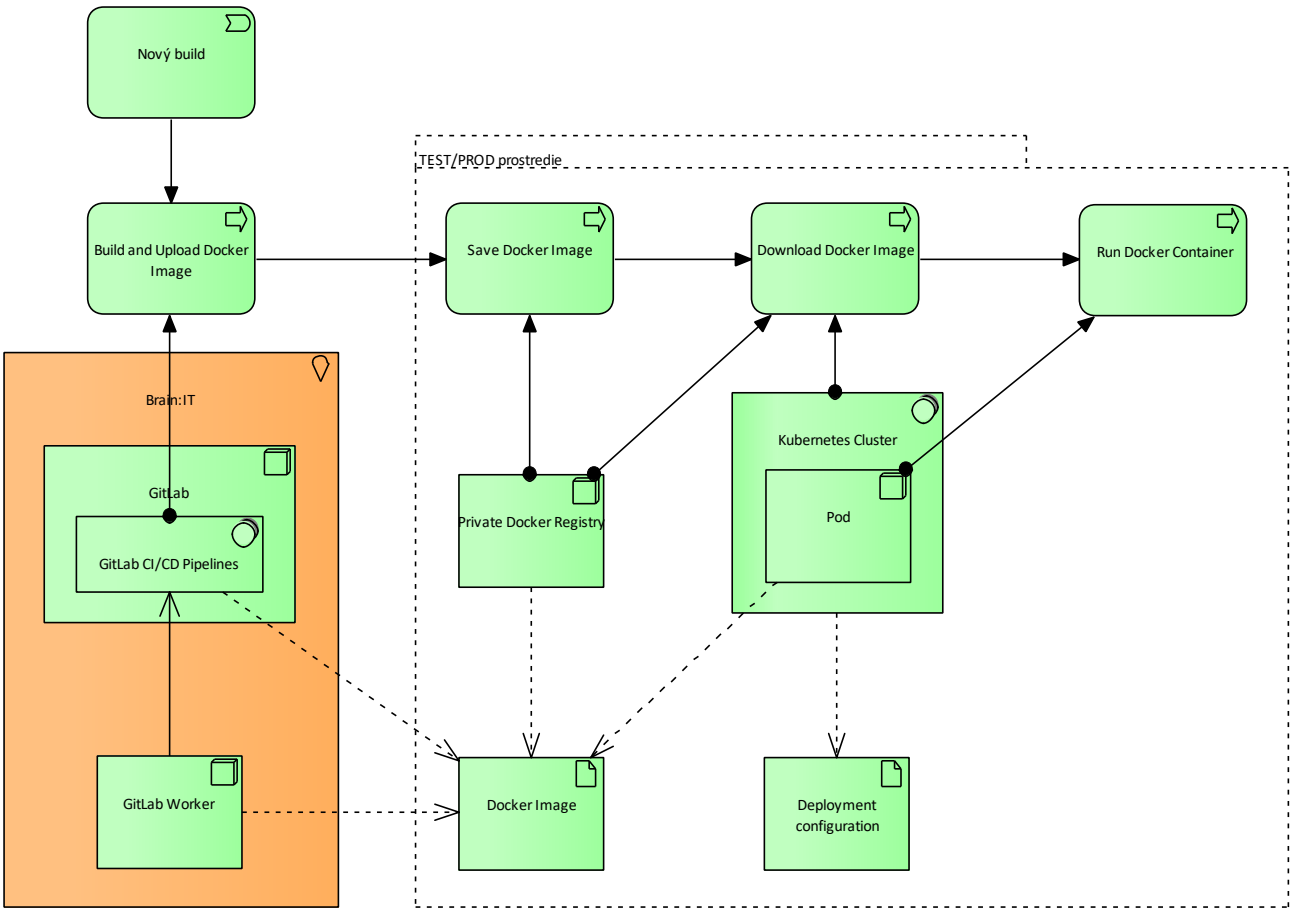
MariaDB
Predstavuje MariaDB relačnú databázu

AlmaLinux/RockyLinux
Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

MariaDB
Predstavuje MariaDB relačnú databázu

AlmaLinux/RockyLinux
Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux

MariaDB
Predstavuje MariaDB relačnú databázu



Obrázok 11 : Technology Viewpoint Development CI/CD TEST/PROD

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

Popis používaných prvkov:

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

Download Docker Image
Proces uloženie Docker Image do Docker Registry

Nový build
Spustenie nového build procesu

Run Docker Container
Proces spustenia Docker Containera

Save Docker Image
Proces uloženie Docker Image do Docker Registry

TEST/PROD prostredie
Predstavuje interné DEV a TEST prostredie

Brain:IT
Lokalita Brain:IT

Private Docker Registry
Predstavuje private Docker Registry

Deployment configuration
Reprezentácia Kubernetes Deployment artifaktu.

Docker Image
Reprezentácia Docker Image artifaktu.

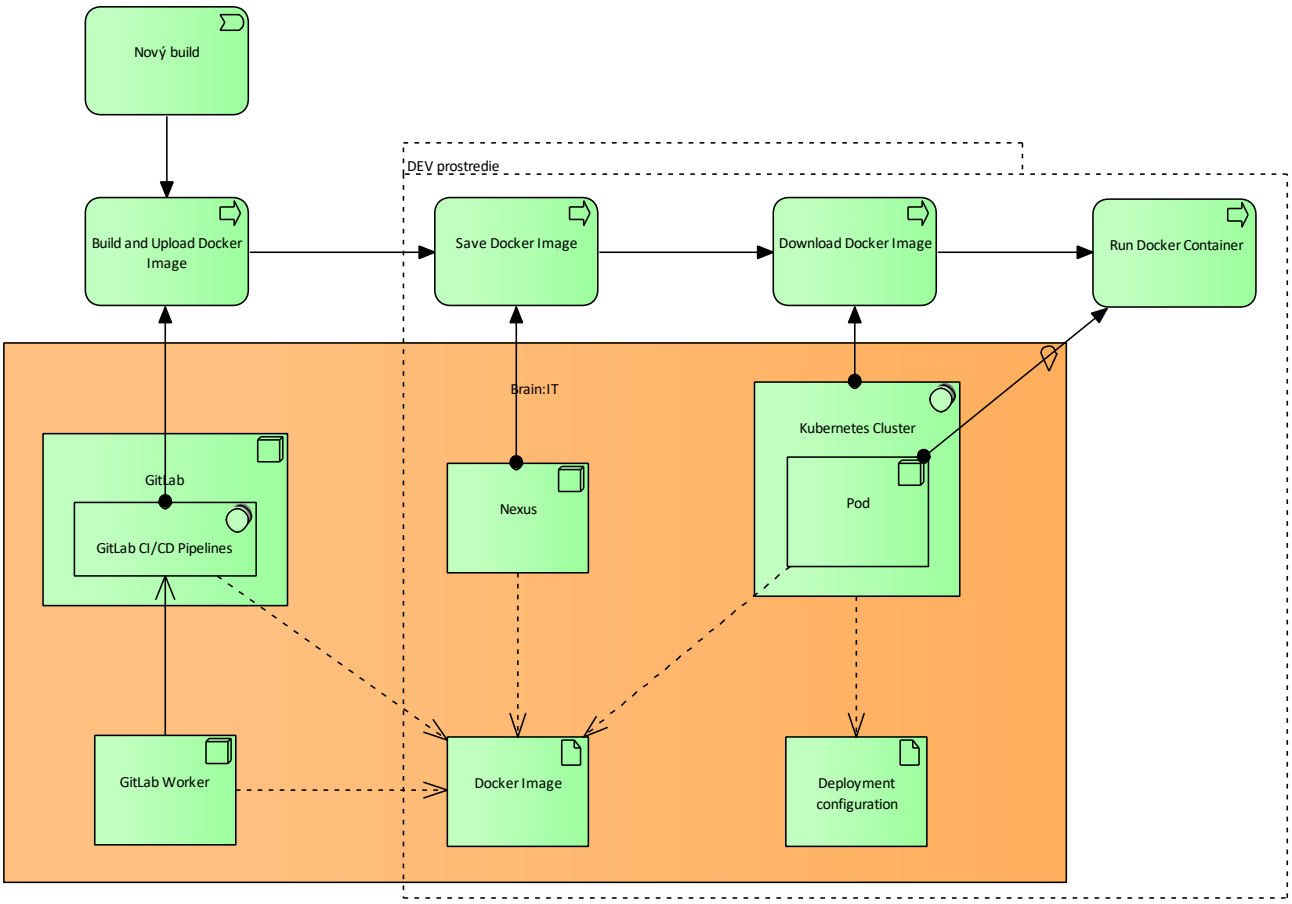
GitLab
Predstavuje inštanciu GitLab.

GitLab Worker
Predstavuje insštanciu GitLab Worker

Kubernetes Cluster
Predstavuje Kubernetes Cluster

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

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



Obrázok 12 : Technology Viewpoint Developmnent CI/CD DEV

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

Popis používaných prvkov:

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

Download Docker Image
Proces uloženie Docker Image do Docker Registry

Nový build
Spustenie nového build procesu

Run Docker Container
Proces spustenia Docker Containera

Save Docker Image
Proces uloženie Docker Image do Docker Registry

DEV prostredie
Predstavuje interné DEV a TEST prostredie

Brain:IT
Lokalita Brain:IT

Deployment configuration
Reprezentácia Kubernetes Deployment artifaktu.

Docker Image
Reprezentácia Docker Image artifaktu.

GitLab
Predstavuje inštanciu GitLab.

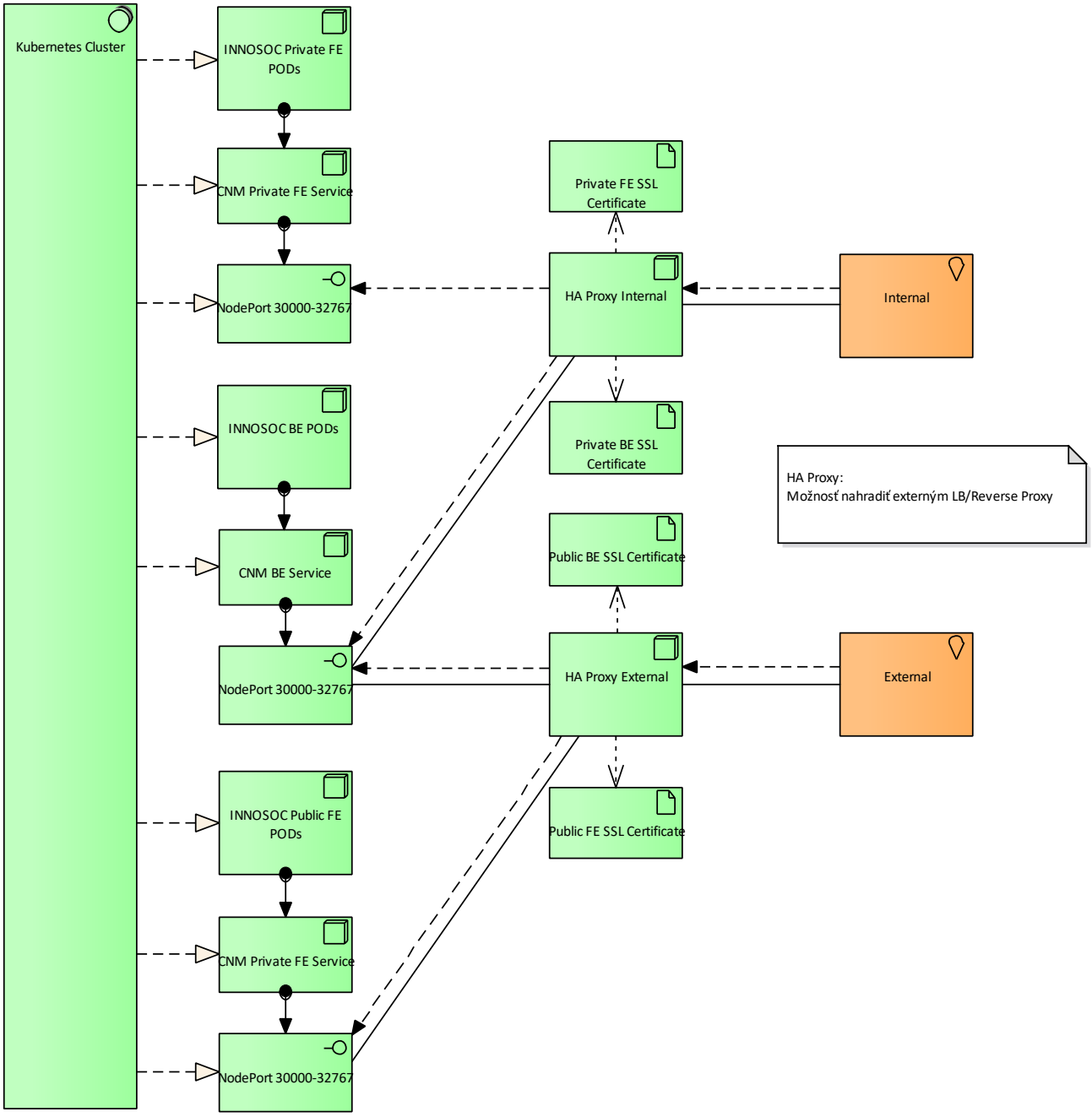
GitLab Worker
Predstavuje insštanciu GitLab Worker

Kubernetes Cluster
Predstavuje Kubernetes Cluster

Nexus
Predstavuje private Docker Registry

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

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



Obrázok 13 : Technology Viewpoint Interconnect

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

Popis používaných prvkov:

CNM BE Service
Predstavuje CNM BE Service

CNM Private FE Service
Predstavuje CNM FE Private Service

CNM Private FE Service
Predstavuje CNM FE Private Service

External
Predstavuje externé prostredie Internet

HA Proxy External
Predstavuje Externú reverse proxy postavenej na HA Proxy

HA Proxy Internal
Predstavuje Internú reverse proxy postavenej na HA Proxy

Internal
Predstavuje interné prostrednie BRAIN:IT

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

Private FE SSL Certificate
Predstavuje validný SSL certifikát pre potreby HTTPS

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

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

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

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

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

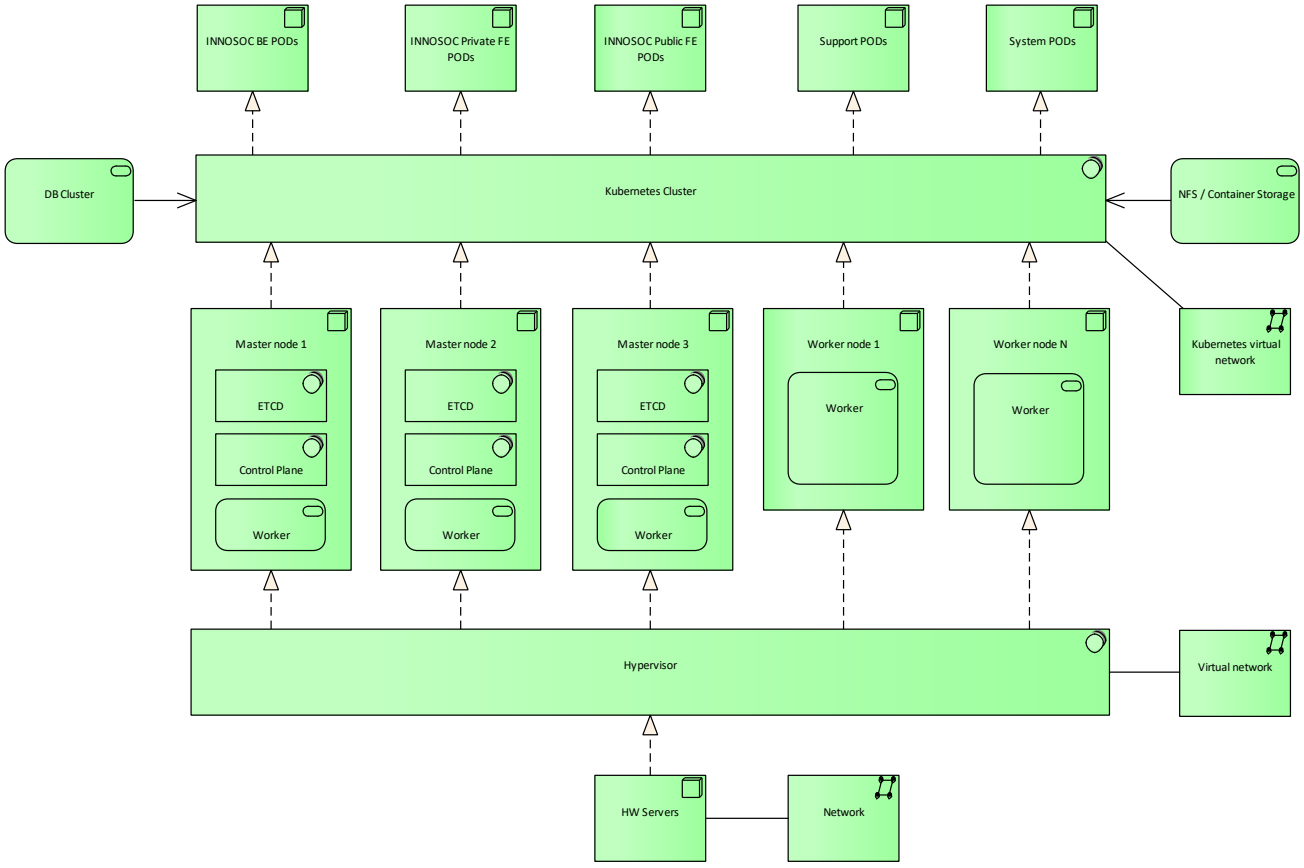
Note
HA Proxy: Možnosť nahradiť externým LB/Reverse Proxy

Kubernetes Cluster
Predstavuje Kubernetes Cluster

INNOSOC BE PODs
Predstavuje PODy CNM BE

INNOSOC Private FE PODs
Predstavuje PODy CNM FE Private

INNOSOC Public FE PODs
Predstavuje PODy CNM FE Public



Obrázok 14 : Technology Viewpoint Kubernetes Cluster

Predstavuje rolu a službu Worker nodu .

Popis používaných prvkov:

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

HW Servers
Predstavuje HW serverovú infraštruktúru

Hypervisor
Predstavuje Hypervisor 1. alebo 2. typu

Kubernetes virtual network
Predstavuje virtuálnu sieť/subsieť Kubernetes Clustra

Master node 1
Predstavuje Master node Kubernetes Clustra

Master node 2
Predstavuje Master node Kubernetes Clustra

Master node 3
Predstavuje Master node Kubernetes Clustra

Network
Predstavuje sieť/subsieť HW infraštruktúry

Support PODs
Predstavuje PODy podporných služieb

System PODs
Predstavuje PODy systémových služieb

Virtual network
Predstavuje virtuálnu sieť/subsieť Hypervisora

Worker node 1
Predstavuje Worker node Kubernetes Clustra

Worker node N
Predstavuje Worker node Kubernetes Clustra

Kubernetes Cluster
Predstavuje Kubernetes Cluster

INNOSOC BE PODs
Predstavuje PODy CNM BE

INNOSOC Private FE PODs
Predstavuje PODy CNM FE Private

INNOSOC Public FE PODs
Predstavuje PODy CNM FE Public

Worker
Predstavuje rolu a službu Worker nodu

Control Plane
Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD
Predstavuje ETCD databázu

Worker
Predstavuje rolu a službu Worker nodu

Control Plane
Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD
Predstavuje ETCD databázu

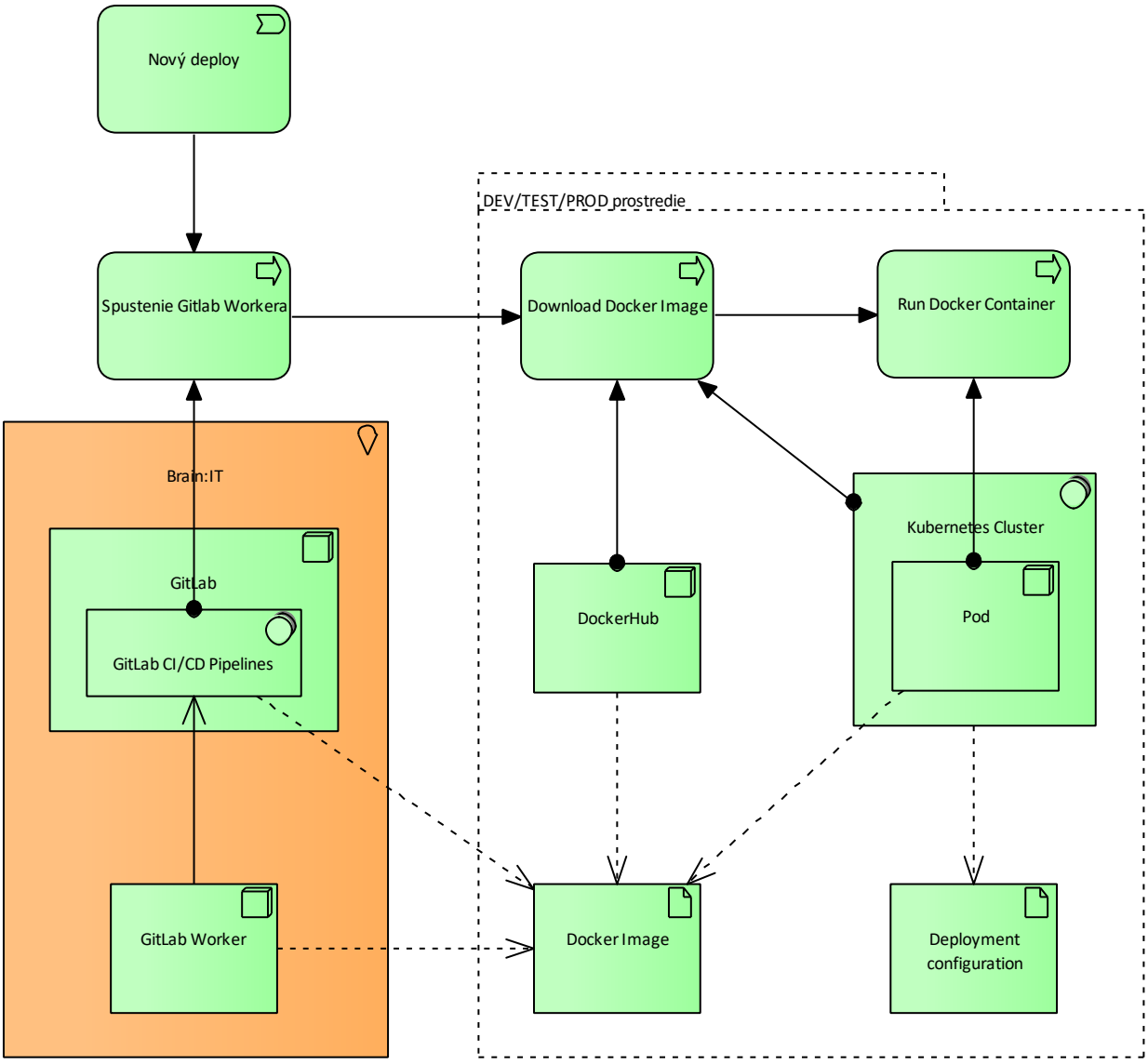
Worker

Control Plane
Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD
Predstavuje ETCD databázu

Worker

Worker



Obrázok 15 : Technology Viewpoint standard CI/CD DEV/TEST/PROD

Popis používaných prvkov:

Download Docker Image
Proces uloženie Docker Image do Docker Registry

Nový deploy
Spustenie nového deploy procesu

Run Docker Container
Proces spustenia Docker Containera

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

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

Brain:IT
Lokalita Brain:IT

DockerHub
Predstavuje verejný Docker Registry DockerHub

Deployment configuration
Reprezentácia Kubernetes Deployment artifaktu.

Docker Image
Reprezentácia Docker Image artifaktu.

GitLab
Predstavuje inštanciu GitLab.

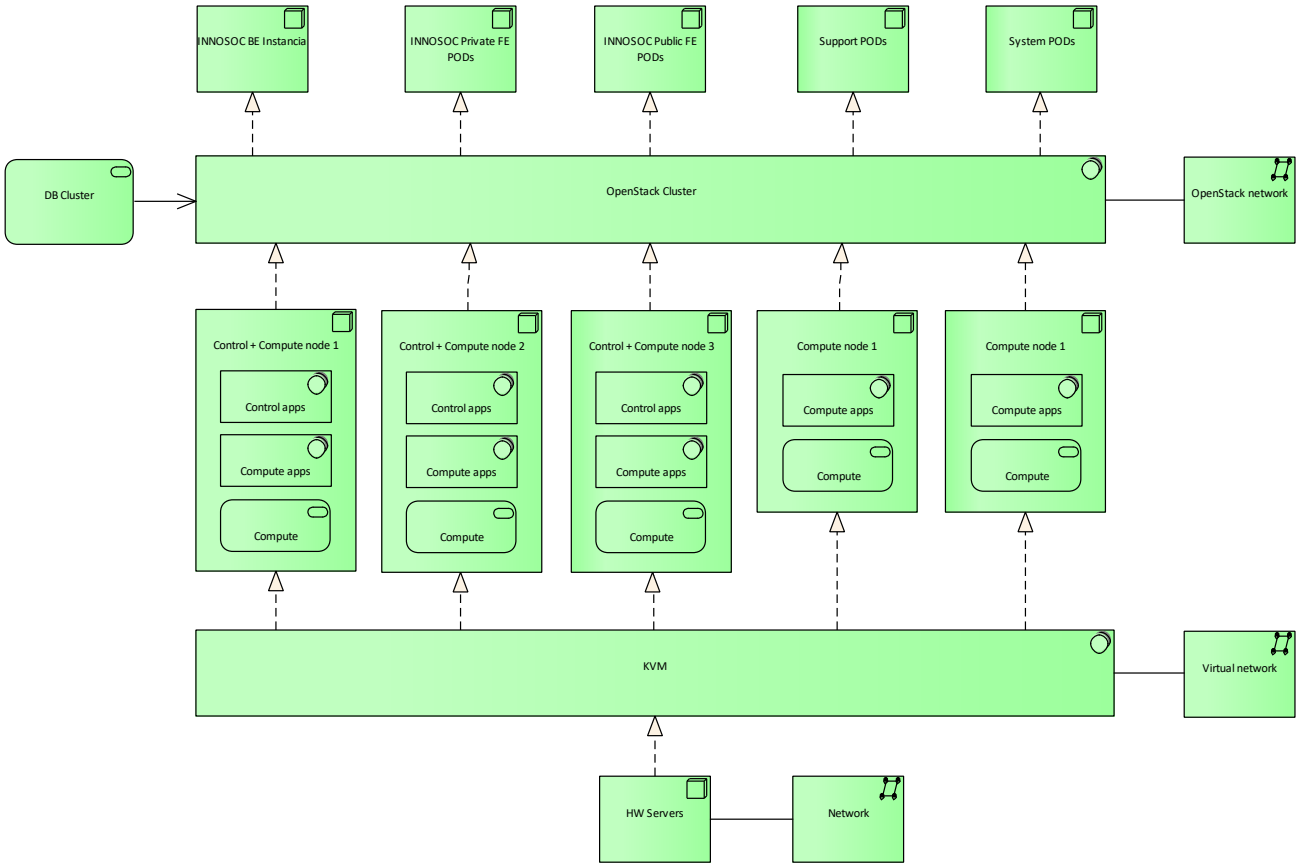
GitLab Worker
Predstavuje insštanciu GitLab Worker

Kubernetes Cluster
Predstavuje Kubernetes Cluster

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

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

1.4. Technology Viewpoint OpenStack



Obrázok 16 : Technology Viewpoint OpenStack Cluster

Popis používaných prvkov:

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

Compute node 1
Predstavuje Compute node OpenStack Clustra

Compute node 1
Predstavuje Compute node OpenStack Clustra

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

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

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

HW Servers
Predstavuje HW serverovú infraštruktúru

KVM
Predstavuje KVM Hypervisor 1. typu.

Network
Predstavuje sieť/subsieť HW infraštruktúry

OpenStack Cluster
Predstavuje OpenStack Cluster

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

Support PODs
Predstavuje PODy podporných služieb

System PODs
Predstavuje PODy systémových služieb

Virtual network
Predstavuje virtuálnu sieť/subsieť Hypervisora

INNOSOC BE Instancia
Predstavuje inštanciu OpenStacku VM alebo kontajner

INNOSOC Private FE PODs
Predstavuje PODy CNM FE Private

INNOSOC Public FE PODs
Predstavuje PODy CNM FE Public

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

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

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

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

Compute
Predstavuje rolu a službu Compute nodu

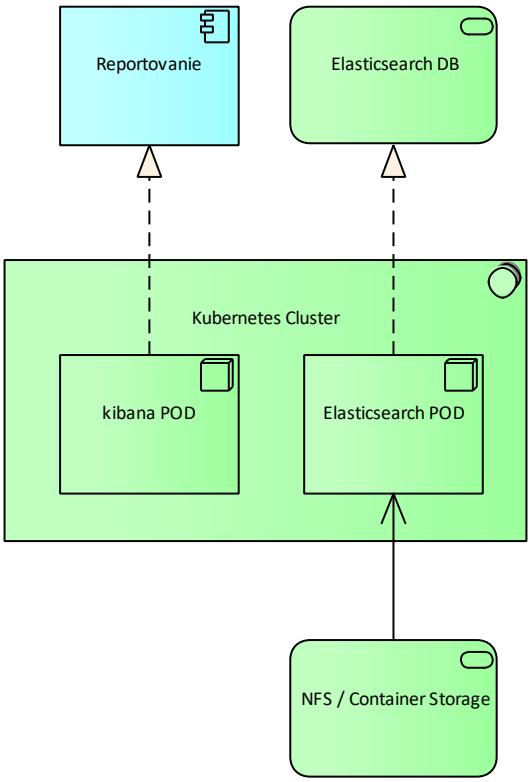
Compute apps
Predstavuje súbor Compute aplikácií

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

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

1.5. Technology Viewpoint Reportovanie



Obrázok 17 : Technology Usage Viewpoint Reportovanie alt 1

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

Popis používaných prvkov:

Reportovanie
Komponent reportovania v rámci SOCaaS architektúry slúži ako centrálny prostriedok na agregáciu, vizualizáciu a distribúciu bezpečnostných informácií. Jeho úlohou je zabezpečiť pravidelné aj ad-hoc výstupy o stave kybernetickej bezpečnosti pre rôzne cieľové skupiny – od SOC analytikov, cez

vedúcich tímov, až po vedenie organizácie alebo klientov. Takýto reportovací systém musí pokrývať:
• Generovanie metriky incidentov, výstrah, SLA a KPIs,
• Prehľady trendov v čase a hodnotenie výkonnosti bezpečnostných opatrení,
• Prispôsobenie obsahu podľa úrovne detailu (technické vs. strategické),
• Automatizáciu a plánovanie distribúcie výstupov,
• Spätnú analýzu a archiváciu historických údajov.

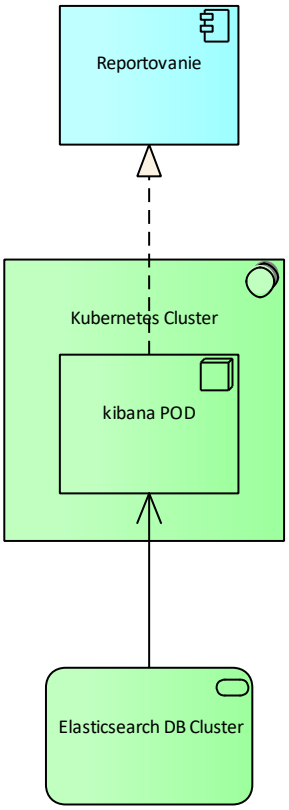
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

Elasticsearch DB
Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Elasticsearch POD
Predstavuje POD Elasticsearch pre NoSQL databázu.

kibana POD
Predstavuje POD Kibana pre Reportovanie.



Obrázok 18 : Technology Usage Viewpoint Reportovanie alt 2

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

Popis používaných prvkov:

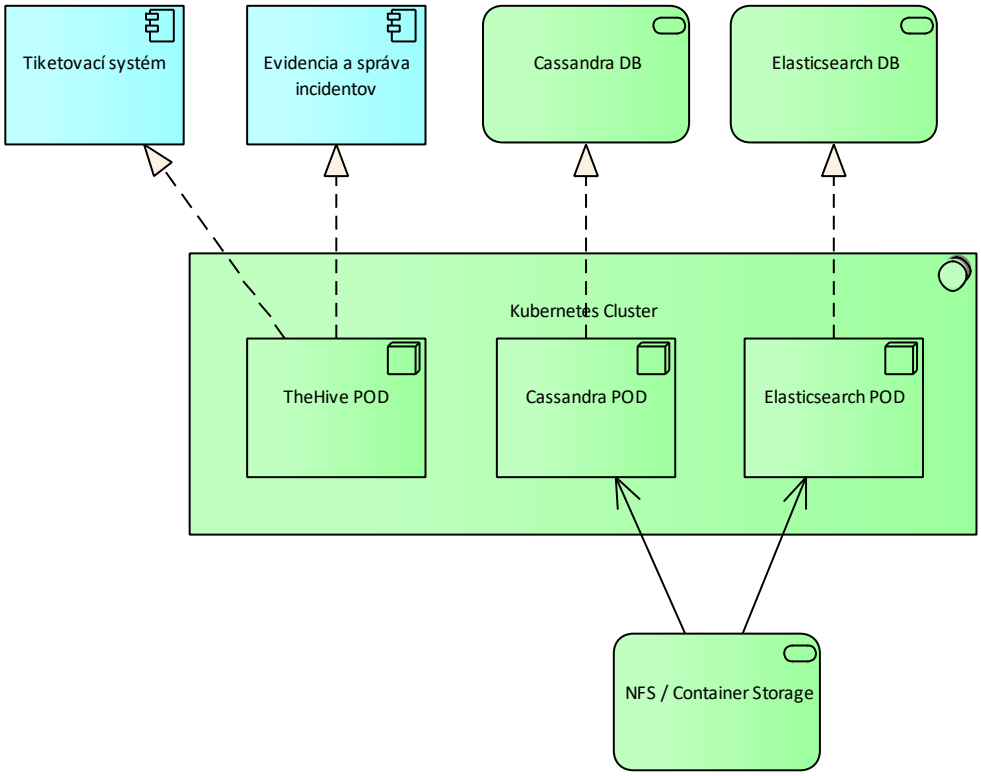
Reportovanie
Komponent reportovania v rámci SOCaaS architektúry slúži ako centrálny prostriedok na agregáciu, vizualizáciu a distribúciu bezpečnostných informácií. Jeho úlohou je zabezpečiť pravidelné aj ad-hoc výstupy o stave kybernetickej bezpečnosti pre rôzne cieľové skupiny – od SOC analytikov, cez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

Kubernetes Cluster
Predstavuje Kubernetes Cluster

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

kibana POD
Predstavuje POD Kibana pre Reportovanie.

1.6. Technology Viewpoint Tiketovací sytém / Evidencia a správa incidentov



Obrázok 19 : Technology Usage Viewpoint Tiketovací sytém / Evidencia a správa incidentov alt 1

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

Popis používaných prvkov:

Evidencia a správa incidentov

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

Tiketovací systém

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

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

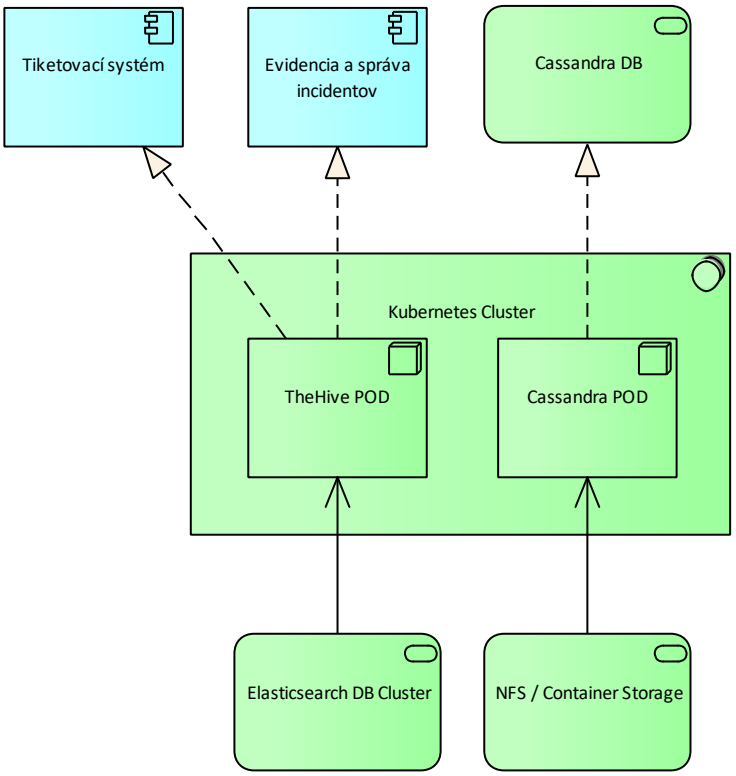
Cassandra DB
Predstavuje technologickú službu NoSQL Cassandra databázy.

Elasticsearch DB
Predstavuje technologickú službu NoSQL Elasticsearch databázy.

Cassandra POD
Predstavuje POD Apache Cassandra pre NoSQL databázu.

Elasticsearch POD
Predstavuje POD Elasticsearch pre NoSQL databázu.

TheHive POD
Predstavuje POD TheHive pre invertarizáckiu aktív.



Obrázok 20 : Technology Usage Viewpoint Tiketovací sytém / Evidencia a správa incidentov alt 2

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

Popis používaných prvkov:

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

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

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

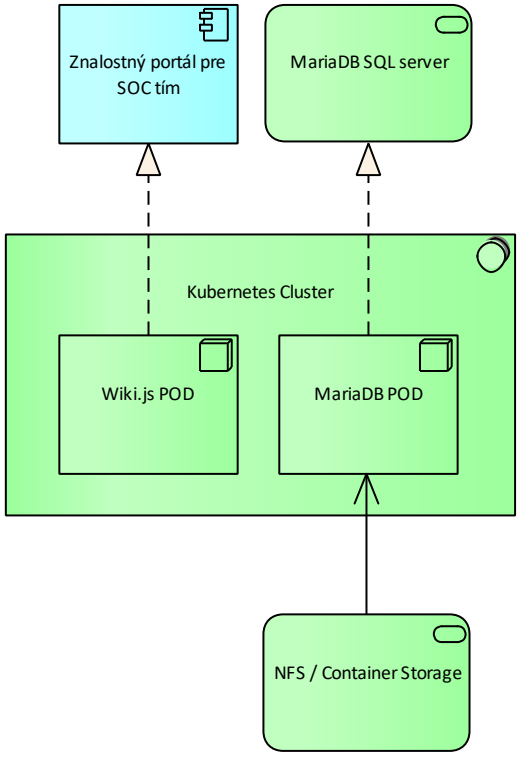
Cassandra DB
Predstavuje technologickú službu NoSQL Cassandra databázy.

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

Cassandra POD
Predstavuje POD Apache Cassandra pre NoSQL databázu.

TheHive POD
Predstavuje POD TheHive pre invertarizáckiu aktív.

1.7. Technology Viewpoint Znalostný portál pre SOC tím



Obrázok 21 : Technology Usage Viewpoint Znalostný portál pre SOC tím alt 1

Diagram znázorňuje zjednodušené priradenie jednotlivých PODov k prislúchajúcim aplikačným

komponentom.
Alt 1 predstavuje využitie Databázy priamo v rámci setupu modulu. V rámci návrhu sa počíta s kontajnerizovanou verziou SQL servera.

Popis používaných prvkov:

Znalostný portál pre SOC tím

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

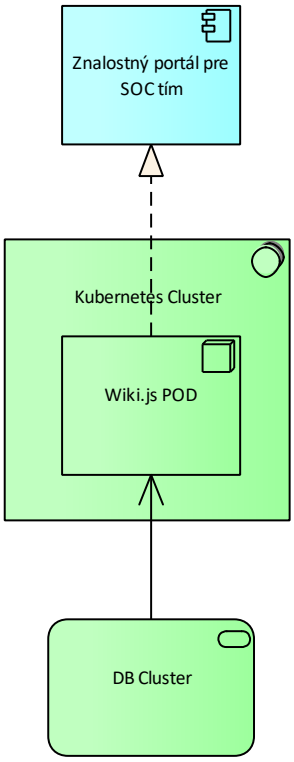
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

MariaDB SQL server
Predstavuje technologickú službu relačnej MariaDB SLQ databázy.

MariaDB POD
Predstavuje POD MariaDB pre relačnú SQL DB.

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



Obrázok 22 : Technology Usage Viewpoint Znalostný portál pre SOC tím alt 2

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

Popis používaných prvkov:

Znalostný portál pre SOC tím

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

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

Kubernetes Cluster
Predstavuje Kubernetes Cluster

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

4. ZÁVER

Navrhované riešenie v rámci projektu INNOSOC sa sústreďuje na vybudovanie multitenantného operačného centra kybernetickej bezpečnosti (SOC), ktoré bude poskytované ako otvorená a flexibilná cloudová služba. Práca konkrétne popisuje používané prvky a ich použitie v rámci technologickej architektúry. Integráciou prvkov automatizácie a pokročilých metód strojového učenia, najmä hlbokých neurónových sietí (DNN), sa zvýši schopnosť systému efektívne detegovať a predikovať anomálie v reálnom čase.