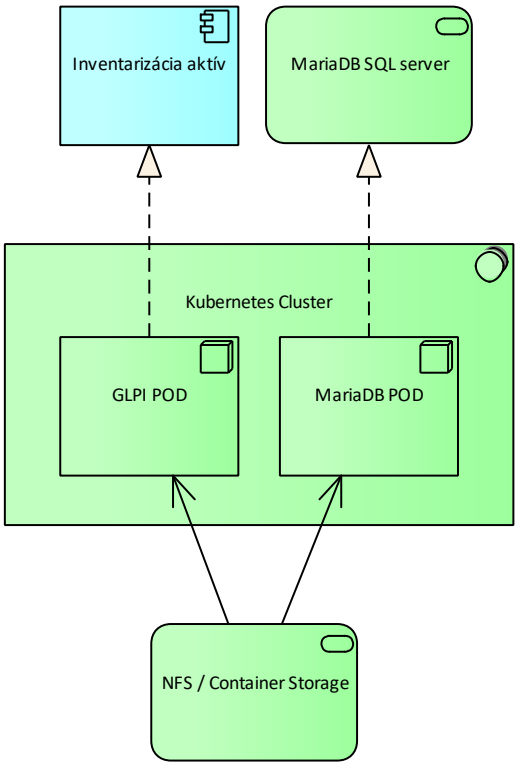
1. Technologická architektúra

Technologická architektúra

Technology Viewpoint INNOSOC Common

Technology Viewpoint Inventarizacia aktiv



Obrázok 1 : 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.

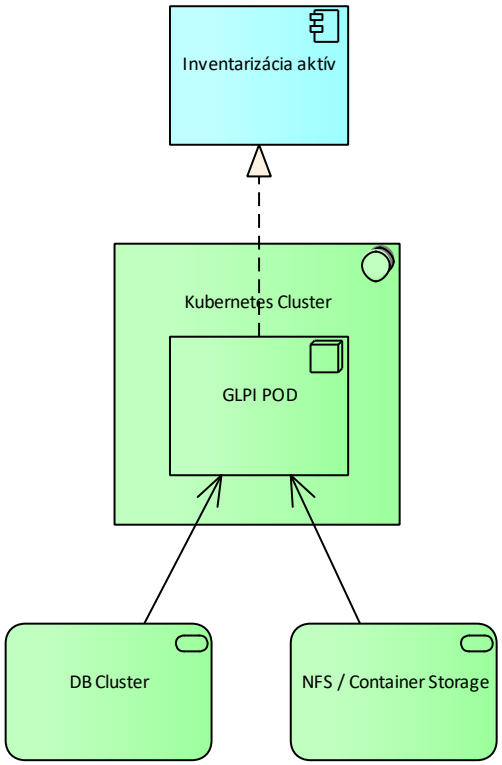
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

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 2 : 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.

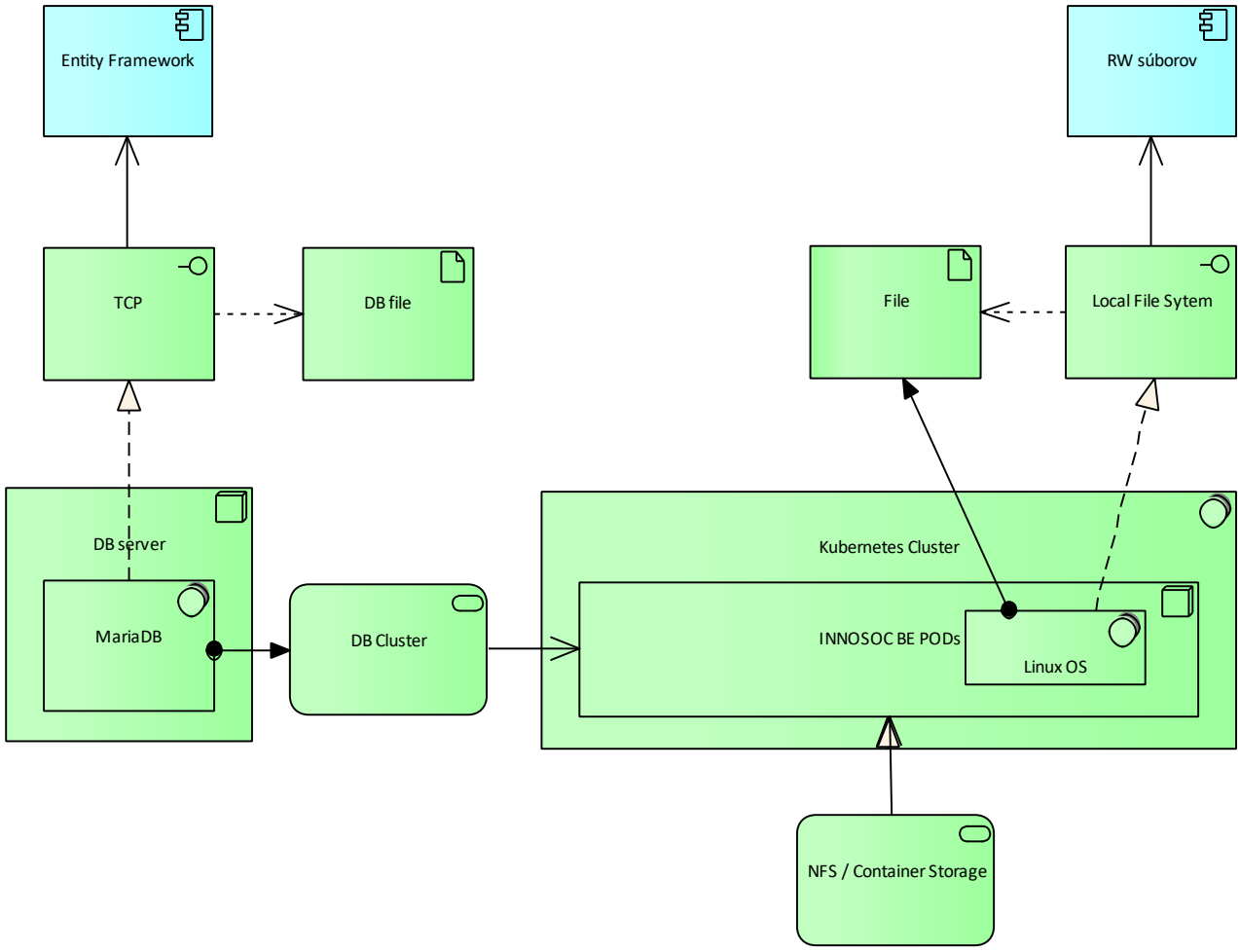
DB Cluster
Predstavuje službu clustrovanej relačnej databázy

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

Kubernetes Cluster
Predstavuje Kubernetes Cluster

GLPI POD
Predstavuje POD GLPI pre invertarizáckiu aktív.

Technology Viewpoint Kubernetes



Obrázok 3 : Technology Usage Viewpoint CNM BE, DB and File System

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

Popis používaných prvkov:

DB Cluster
Predstavuje službu clustrovanej relačnej databázy

NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

DB file
DB file - súbor reprezentujúci databázový súbor MariaDB

DB server
Predstavuje MariaDB server

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

Entity Framework
Predstavuje aplikačný modul Entity Framework

RW súborov
Predstavuje modul RW nad súbormi

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

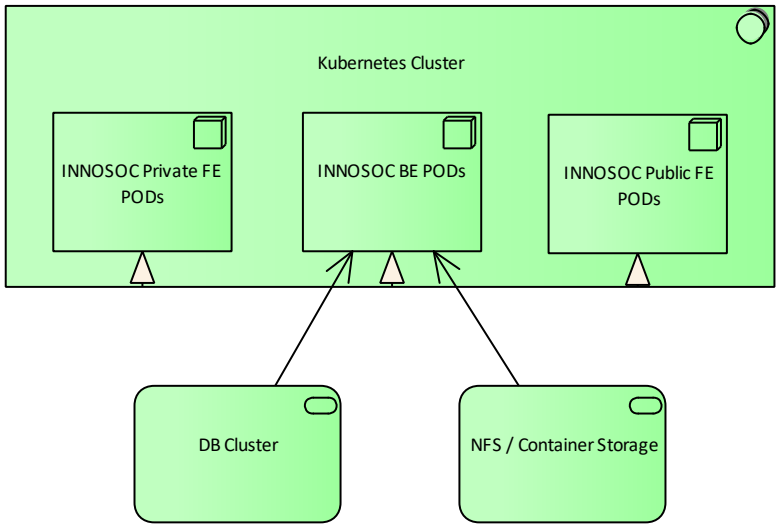
TCP
Predstavuje client server komunikáciu pomocou TCP protokolu

Kubernetes Cluster
Predstavuje Kubernetes Cluster

INNOSOC BE PODs
Predstavuje PODy CNM BE

Linux OS

MariaDB
Predstavuje MariaDB relačnú databázu



Obrázok 4 : 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

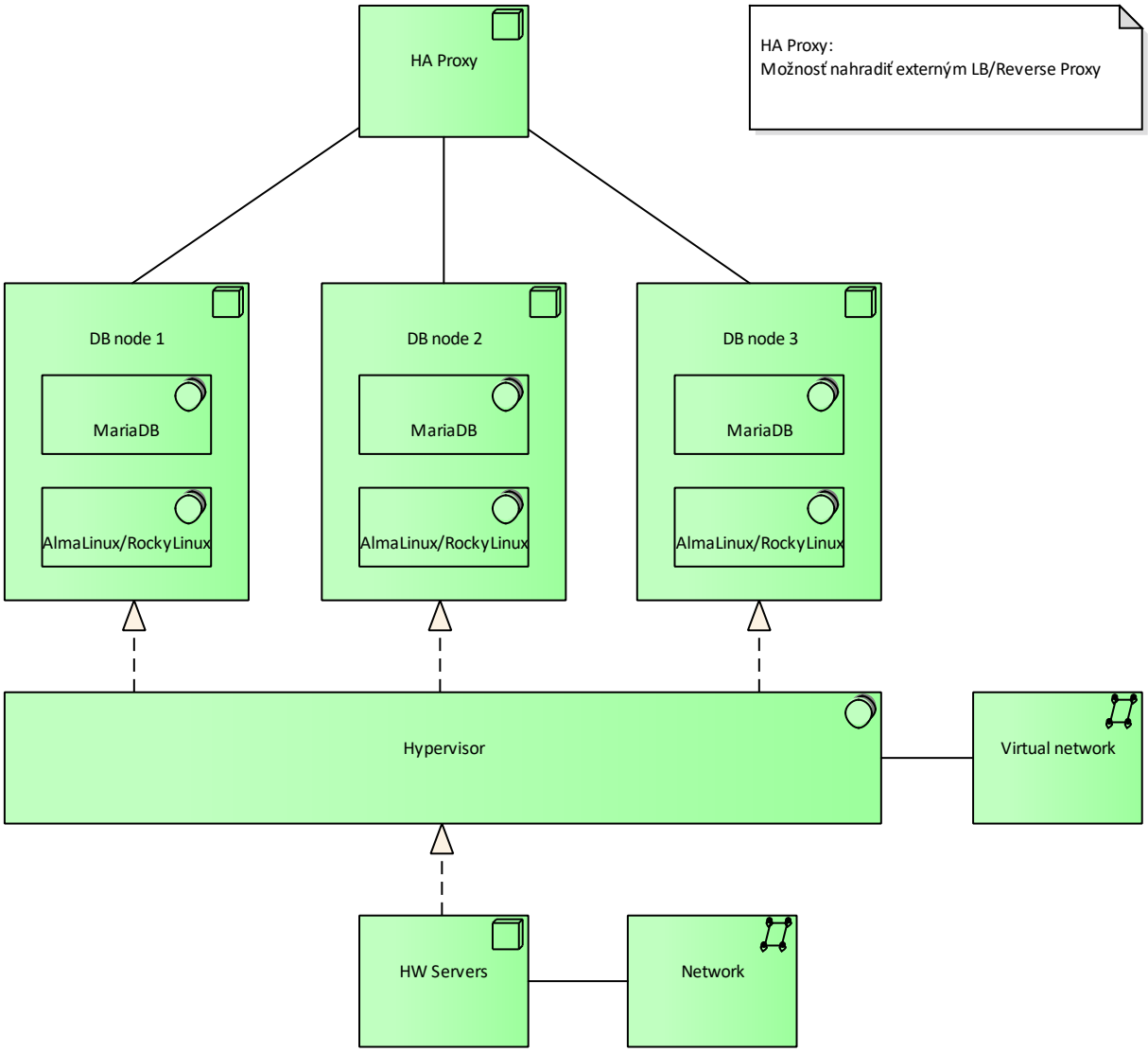
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

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 5 : 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

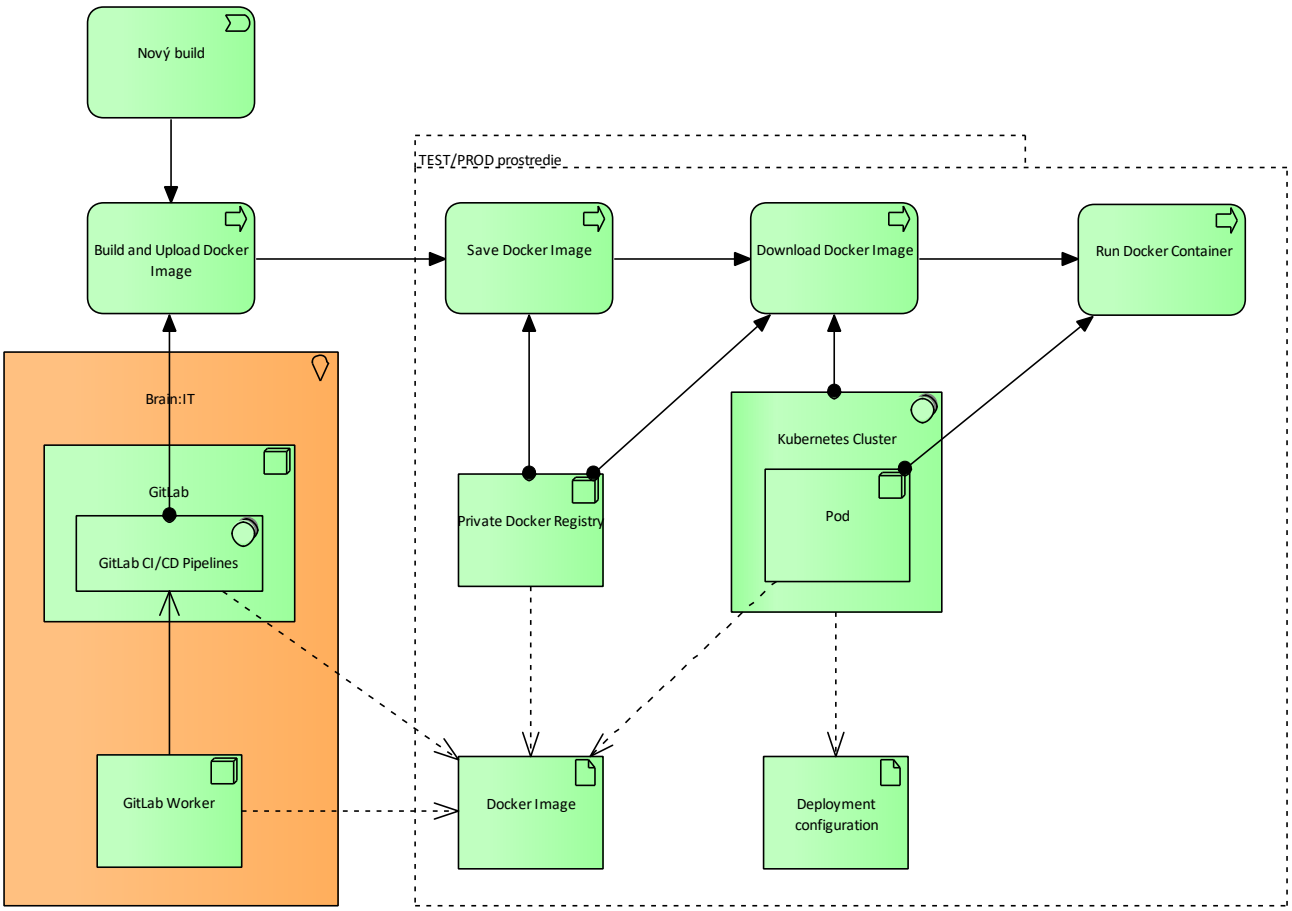
MariaDB
Predstavuje MariaDB relačnú databázu

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 6 : 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.

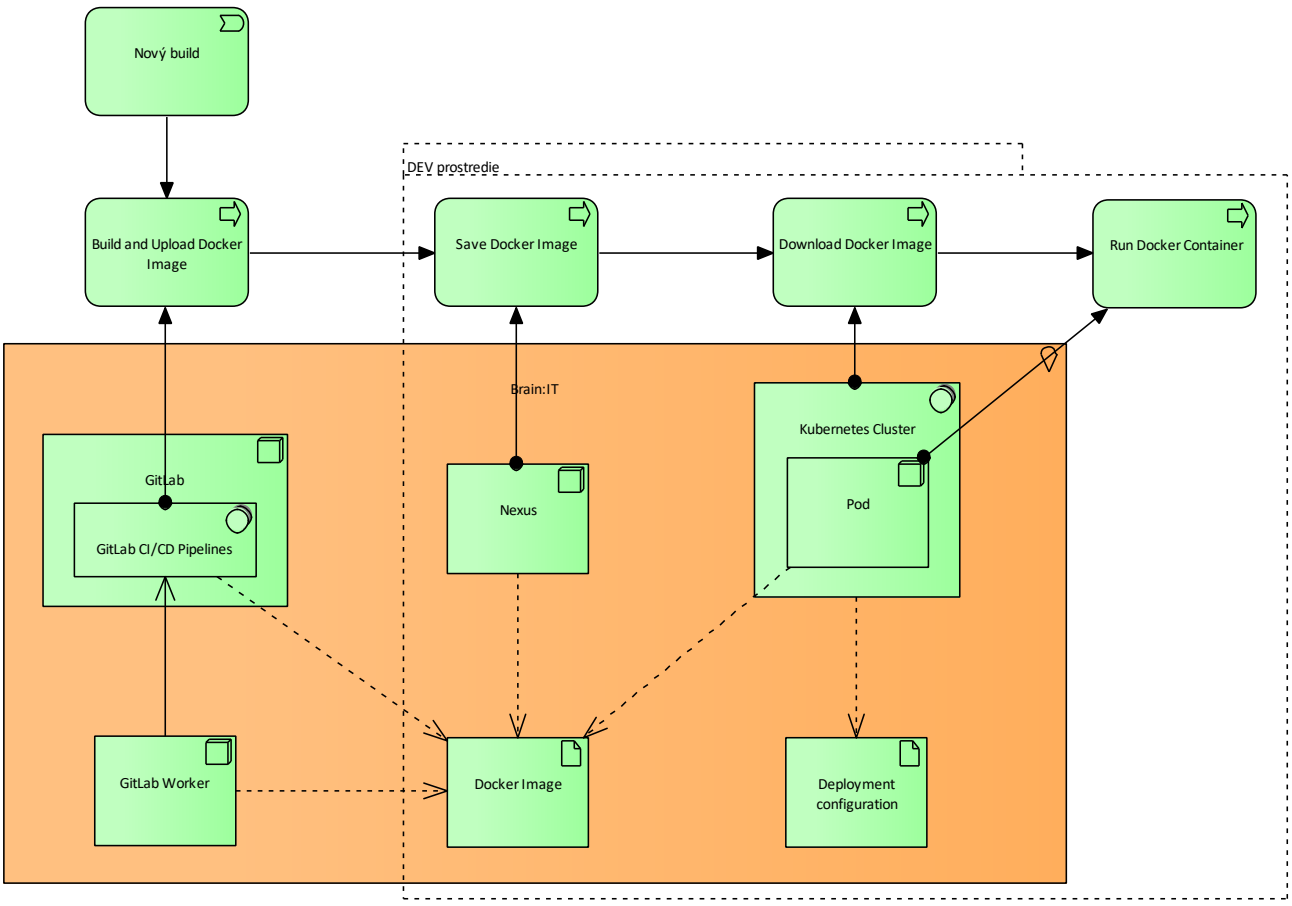
GitLab
Predstavuje inštanciu GitLab.

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 7 : 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.

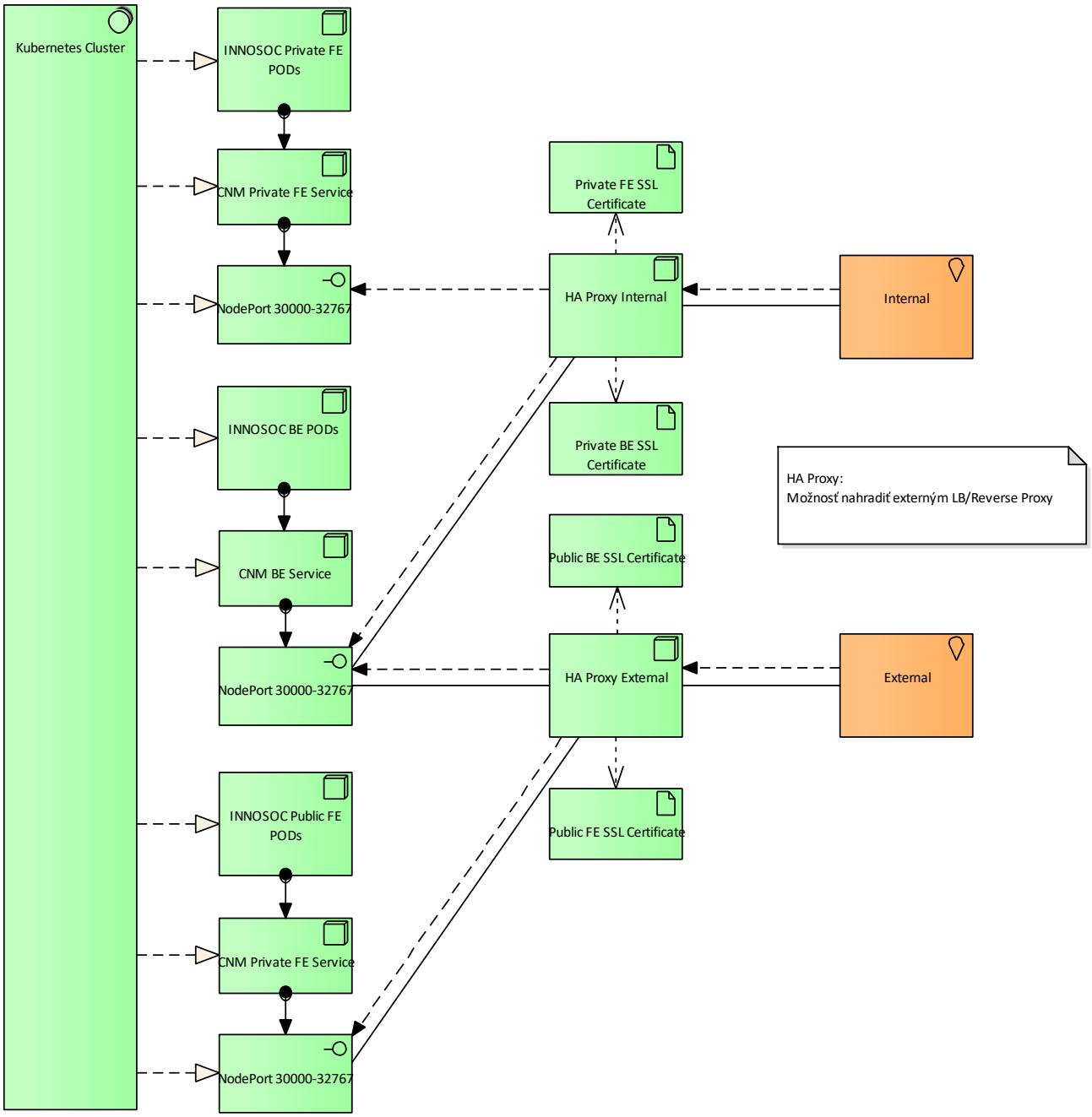
GitLab Worker
Predstavuje insštanciu GitLab Worker

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 8 : 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

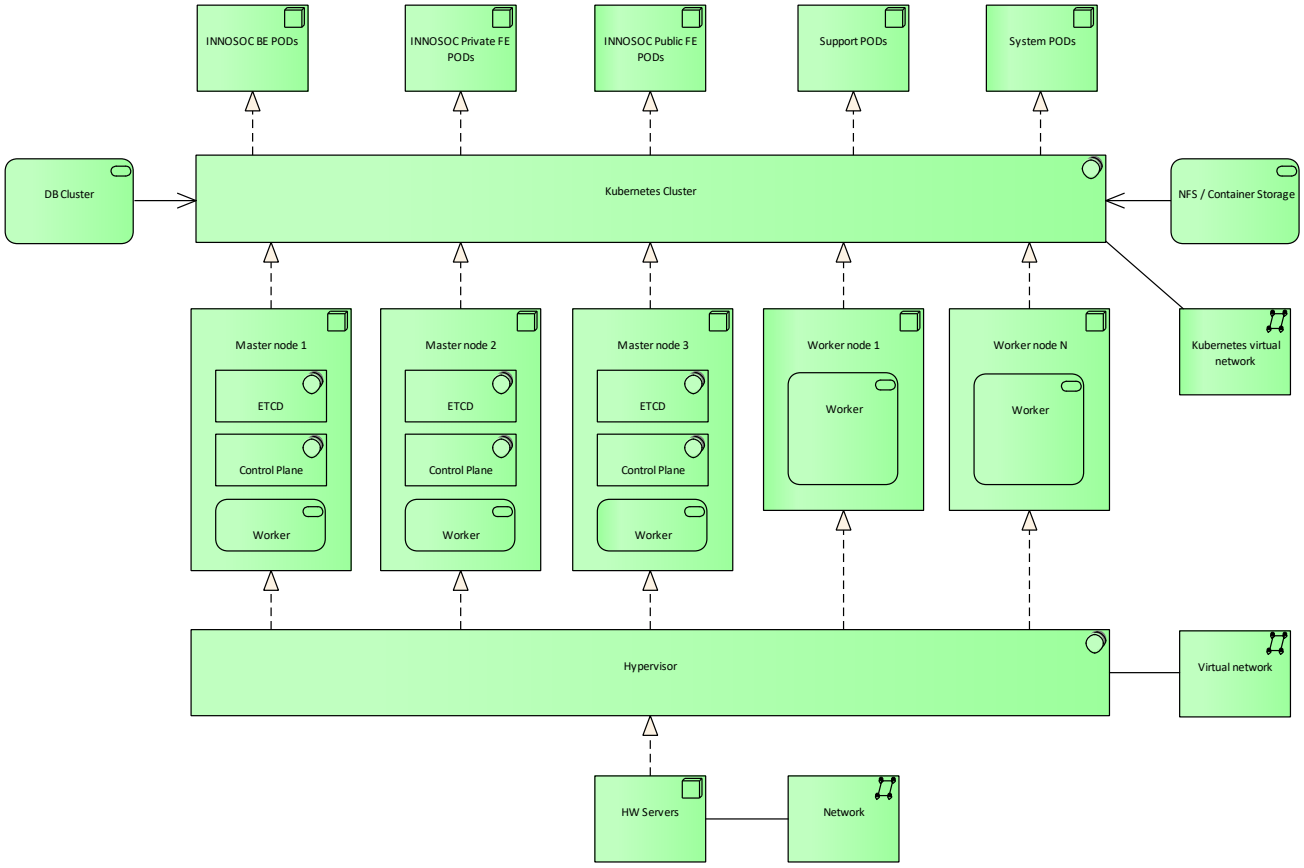
Note
HA Proxy:
Možnosť nahradiť externým LB/Reverse Proxy

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 9 : 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

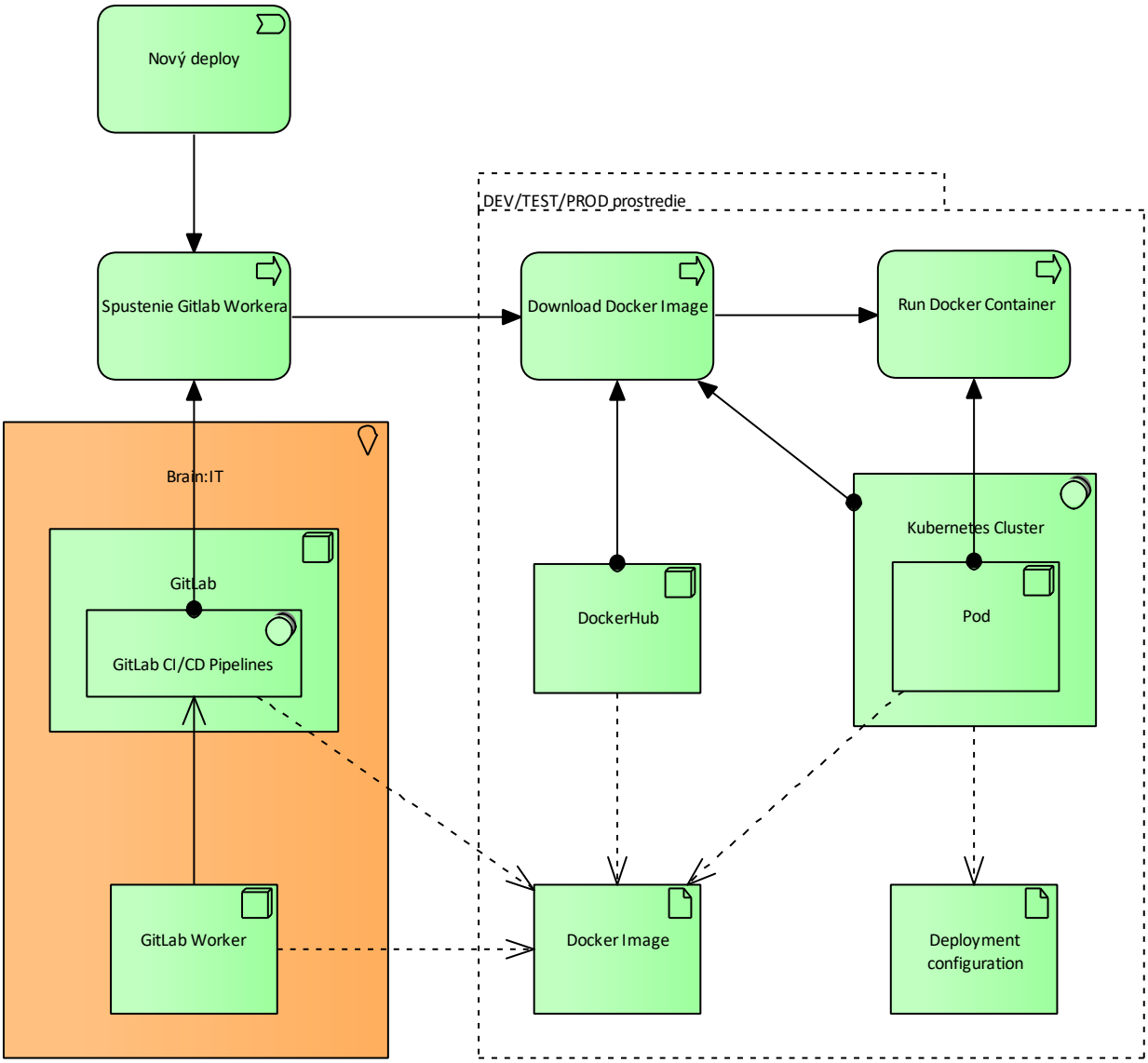
Worker

Control Plane
Predstavuje Control Plane pre správu Kubernetes Clustra

ETCD
Predstavuje ETCD databázu

Worker

Worker



Obrázok 10 : 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.

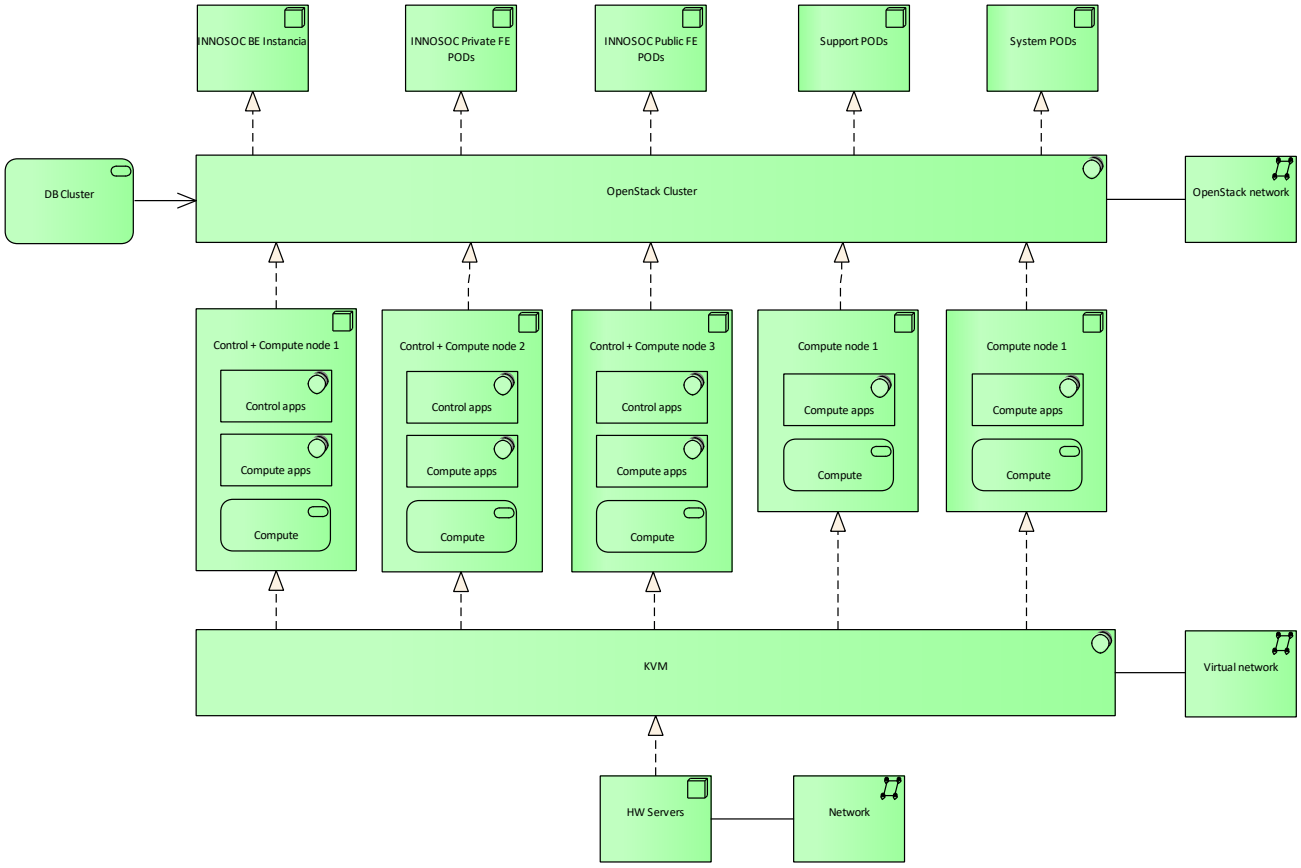
GitLab Worker
Predstavuje insštanciu GitLab Worker

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

Technology Viewpoint OpenStack



Obrázok 11 : 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

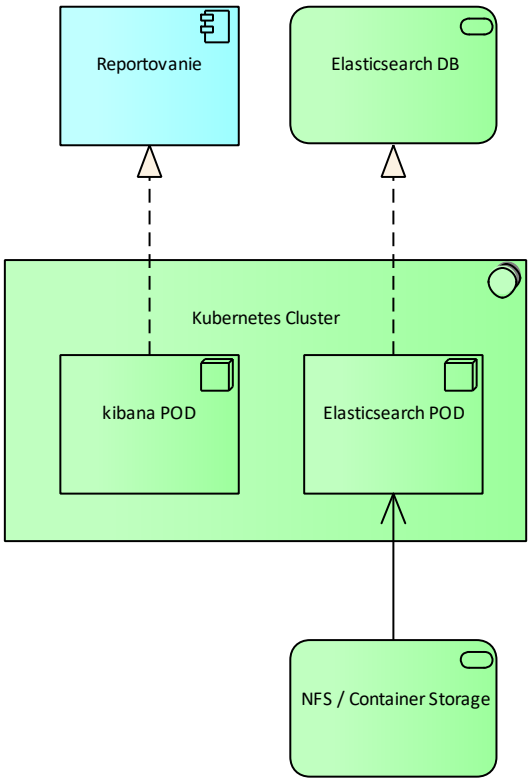
Control apps
Predstavuje súbor aplikácií pre Control node potrebných pre správu clustra

Compute
Predstavuje rolu a službu Compute nodu

Compute apps
Predstavuje súbor Compute aplikácií

Technology Viewpoint OpenStack External

Technology Viewpoint Reportovanie



Obrázok 12 : 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.

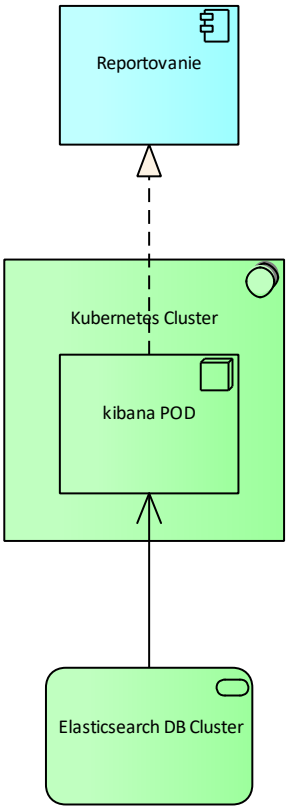
NFS / Container Storage
Predstavuje službu NFS alebo iného Container Storage

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 13 : 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.

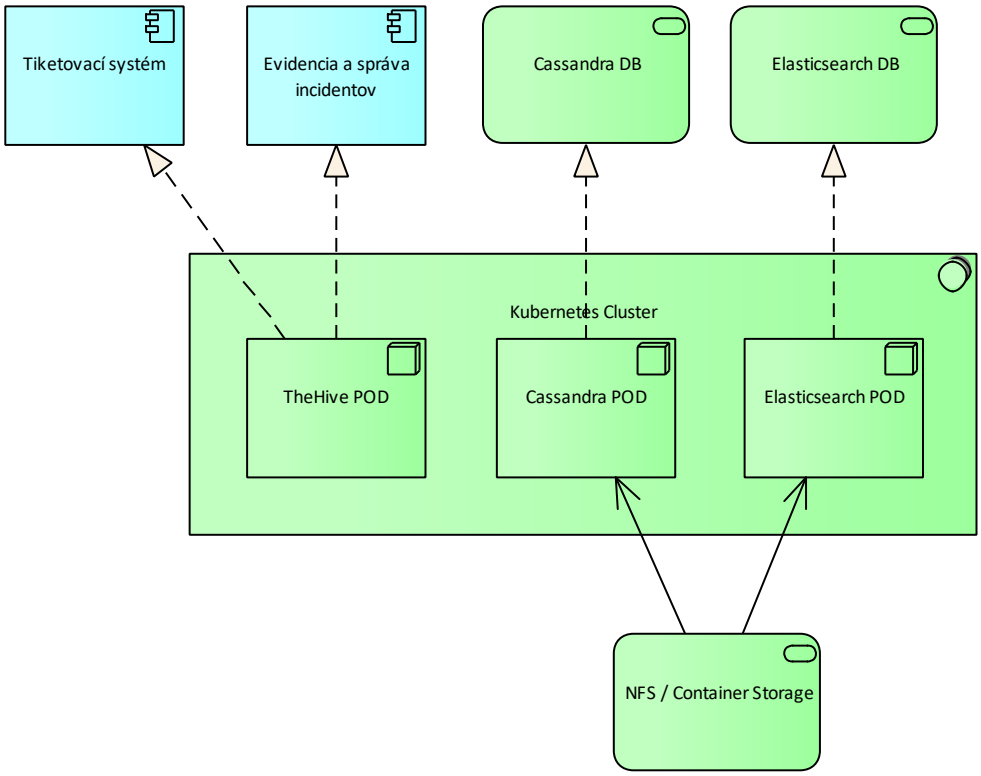
Kubernetes Cluster
Predstavuje Kubernetes Cluster

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

kibana POD
Predstavuje POD Kibana pre Reportovanie.

Technology Viewpoint Skener zraniteľností

Technology Viewpoint Tiketovací sytém / Evidencia a správa incidentov



Obrázok 14 : 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

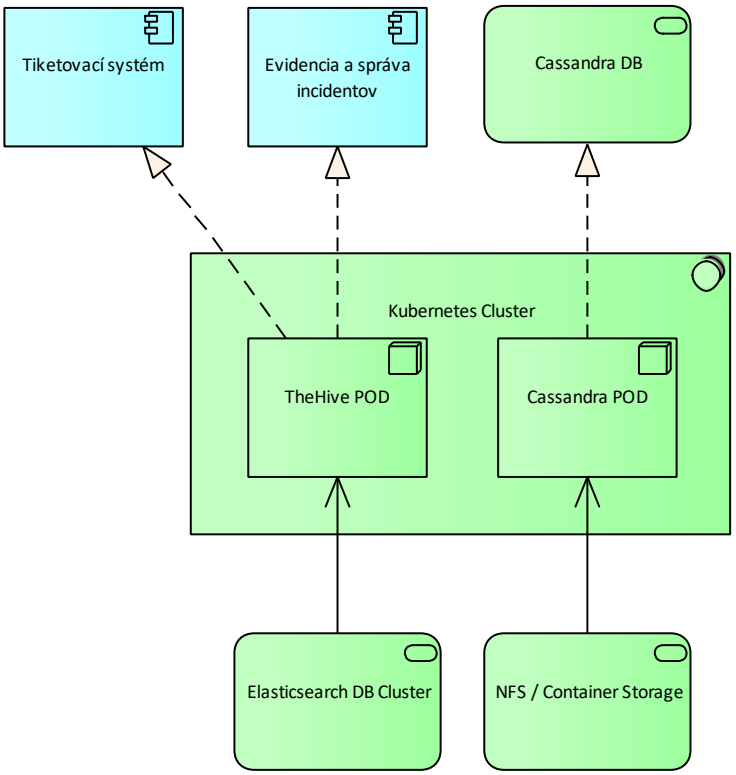
Predstavuje POD Apache Cassandra pre NoSQL databázu.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu.

TheHive POD

Predstavuje POD TheHive pre invertarizáckiu aktív.



Obrázok 15 : 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

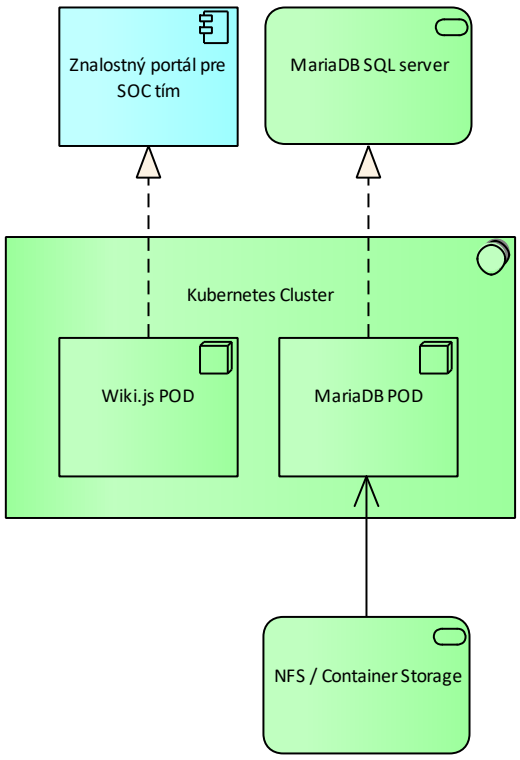
Cassandra DB
Predstavuje technologickú službu NoSQL Cassandra databázy.

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.

Technology Viewpoint Znalostný portál pre SOC tím



Obrázok 16 : 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

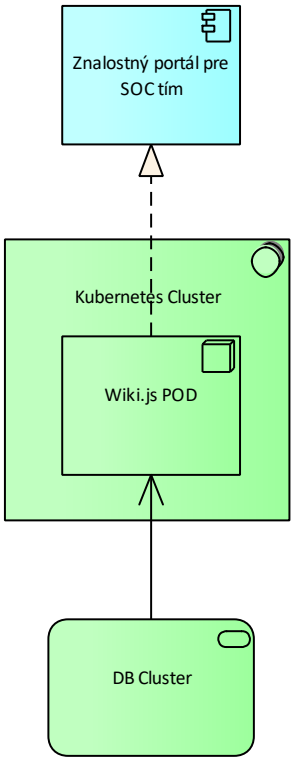
Predstavuje technologickú službu relačnej MariaDB SLQ databázy.

MariaDB POD

Predstavuje POD MariaDB pre relačnú SQL DB.

Wiki.js POD

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



Obrázok 17 : 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.