PROJEKT

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

V12 Technologická 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. Application Viewpoints 4
3. Technologická architektúra 8
1.2. Návrh technologickej architektúry 8
1.1.1. Technology Viewpoint CTI 9
1.1.2. Technology Viewpoint EDR/XDR 19
1.1.3. Technology Viewpoint INNOSOC Common 24
1.1.4. Technology Viewpoint Inventarizacia aktiv 27
1.1.5. Technology Viewpoint Kubernetes 31
1.1.6. Technology Viewpoint OpenStack 55
1.1.7. Technology Viewpoint OpenStack External 61
1.1.8. Technology Viewpoint Reportovanie 62
1.1.9. Technology Viewpoint SIEM 65
1.1.10. Technology Viewpoint Skener zraniteľností 69
1.1.11. Technology Viewpoint SOAR 73
1.1.12. Technology Viewpoint Tiketovací systém/ Evidencia a správa incidentov 79
1.1.13. Technology Viewpoint Znalostný portál pre SOC tím 83

ÚVOD

Zámerom projektu je vyvinúť technologicky moderné, otvorené a škálovateľné riešenie, ktoré bude schopné podporiť organizácie v efektívnom zvládaní kybernetických hrozieb.

1. APLIKAČNÁ ARCHITEKTÚRA

Aplikačná architektúra riešenia predstavuje logický návrh aplikačných služieb, komponentov a ich vzájomných väzieb, ktoré zabezpečujú funkcionalitu navrhovanej platformy SOCaaS. Jej účelom je poskytnúť ucelený pohľad na aplikačnú vrstvu riešenia, a to najmä z hľadiska rozdelenia zodpovedností medzi jednotlivé komponenty, ich funkčného zamerania a spôsobu, akým spoločne podporujú hlavné procesy bezpečnostného dohľadu, detekcie, vyhodnocovania a riešenia bezpečnostných udalostí a incidentov. Architektúra vychádza z modelu spracovaného v nástroji EA, pričom popisy jednotlivých objektov sú odvodené z poznámok priradených k modelovaným prvkom.

Navrhovaná aplikačná architektúra reflektuje charakter riešenia ako multitenantnej služby operačného centra kybernetickej bezpečnosti. Z pohľadu aplikačnej vrstvy pokrýva najmä oblasti zberu a korelácie bezpečnostných udalostí, automatizácie reakcie, správy incidentov, threat intelligence, správy aktív, riadenia zraniteľností, reportovania a podpory znalostného manažmentu SOC tímu. Takto definovaná aplikačná vrstva súčasne vytvára predpoklad pre podporu kľúčových prípadov použitia, ako sú monitorovanie bezpečnostných udalostí, správa detekčných pravidiel, eskalácia a riešenie incidentov, správa threat intelligence, správa aktív, riadenie zraniteľností, export reportov a správa používateľov, rolí a organizácií v rámci SOCaaS platformy.

Aplikačná architektúra je v dokumente prezentovaná ako vysokonávrhový zoznam aplikačných komponentov riešenia. Diagram aplikačných pohľadov zobrazuje hlavné komponenty, ktoré spolu tvoria funkčný základ platformy. Z dostupného modelu vyplýva, že jadro riešenia tvoria najmä komponenty SIEM, SOAR, CTI, EDR/XDR, analytický a automatizačný engine, evidencia a správa incidentov, tiketovací systém, manažovanie kybernetických bezpečnostných incidentov, inventarizácia aktív, skener zraniteľností, reportovanie a znalostný portál pre SOC tím. Diagram tak nepredstavuje detailný návrh interných integračných tokov, ale predovšetkým prehľad hlavných aplikačných stavebných blokov riešenia.

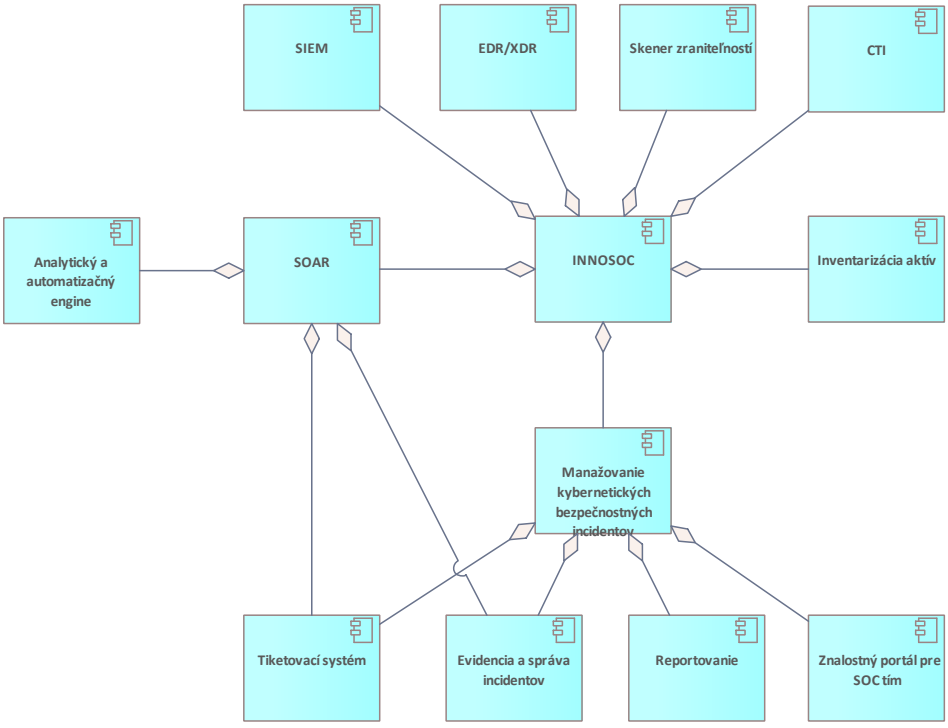
Z funkčného hľadiska možno jednotlivé aplikačné komponenty rozdeliť do viacerých logických skupín. Prvú skupinu tvoria komponenty orientované na zber, analýzu a detekciu, teda najmä SIEM, EDR/XDR, CTI a analytický a automatizačný engine. Tieto komponenty zabezpečujú príjem a spracovanie bezpečnostných dát, ich obohacovanie o kontext hrozieb, koreláciu udalostí a identifikáciu anomálií alebo podozrivých stavov. Druhú skupinu predstavujú komponenty orientované na reakciu a riadenie životného cyklu incidentu, predovšetkým SOAR, evidencia a správa incidentov, tiketovací systém a manažovanie kybernetických bezpečnostných incidentov. Ich úlohou je umožniť systematickú evidenciu, koordináciu, automatizáciu a riadenie reakcie na incidenty od ich vzniku až po uzatvorenie.

Ďalšiu oblasť aplikačnej architektúry tvoria podporné a kontextové komponenty, najmä inventarizácia aktív, skener zraniteľností, reportovanie a znalostný portál pre SOC tím. Inventarizácia aktív poskytuje prehľad o spravovaných zariadeniach, systémoch a zdrojoch, čím vytvára základný kontext pre monitoring a hodnotenie dopadov incidentov. Skener zraniteľností podporuje proaktívny prístup k bezpečnosti a poskytuje vstupy pre prioritizáciu nápravných opatrení. Reportovanie zabezpečuje agregáciu, vizualizáciu a distribúciu bezpečnostných informácií rôznym cieľovým skupinám. Znalostný portál slúži ako centrálne miesto pre uchovávanie playbookov, analytických postupov, odporúčaní a skúseností z riešenia incidentov.

Osobitné miesto v aplikačnej architektúre má analytický a automatizačný engine, ktorý podľa popisu v modeli kombinuje analýzu dát a automatizáciu rozhodovacích alebo operačných procesov. V kontexte riešenia ide o komponent podporujúci spracovanie vstupných dát, aplikovanie analytických pravidiel alebo modelov a následné vykonávanie automatizovaných reakcií prostredníctvom integrovaných nástrojov a rozhraní. Tento prvok je funkčne previazaný s cieľom riešenia využívať prvky automatizácie a metódy strojového učenia pri detekcii a vyhodnocovaní bezpečnostných udalostí.

Z pohľadu celkovej architektúry riešenia aplikačná vrstva vytvára premostenie medzi biznis vrstvou a technologickou vrstvou. Na jednej strane nadväzuje na definované služby a prípady použitia, na druhej strane vytvára základ pre následný technologický návrh konkrétnych platforiem a nástrojov. Jej význam spočíva v tom, že pomenúva hlavné aplikačné zodpovednosti riešenia a vytvára štruktúrovaný rámec pre implementáciu, integráciu a ďalší rozvoj jednotlivých funkčných oblastí platformy SOCaaS.

1.1. Application Viewpoints



Obrázok 1: Application Viewpoints Components

Diagram predstavuje HL zoznam aplikačných komponentov riešenia.

Popis používaných prvkov:

Analytický a automatizačný engine

Analytický a automatizačný engine je softvérová komponenta alebo služba, ktorá kombinuje analýzu dát a automatizáciu rozhodovacích alebo operačných procesov s cieľom zvýšiť efektivitu, presnosť a rýchlosť reakcie systému. V kontexte kybernetickej bezpečnosti alebo IT prevádzky tento engine spracúva vstupné dáta (napr. logy, udalosti, metriky), aplikuje analytické pravidlá alebo modely (napr. detekciu anomálií, koreláciu), a následne vykonáva automatizované reakcie alebo akcie prostredníctvom integrovaných nástrojov a API rozhraní.

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 viaczákaznáckej 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

Predstavuje komplexný agregovaný komponent.

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.

2. TECHNOLOGICKÁ ARCHITEKTÚRA

Technologická architektúra predstavuje štruktúrovaný návrh technologických komponentov, ich vzájomných väzieb a spôsobu integrácie do celkového ekosystému organizácie. Zahŕňa definovanie softvérových vrstiev, komunikačných protokolov, bezpečnostných mechanizmov a prevádzkových procesov. Jej cieľom je zabezpečiť optimálne fungovanie systému, jeho škálovateľnosť, interoperabilitu a schopnosť reagovať na meniace sa požiadavky biznisu a regulačného prostredia.

Projekt reaguje na potreby najmä malých a stredných organizácií, ktoré často nedisponujú dostatočnými odbornými kapacitami ani rozpočtom na vybudovanie vlastného bezpečnostného centra. Navrhované riešenie poskytuje centralizovanú správu, automatizovanú detekciu a reakciu na incidenty, monitoring a reporting, čím znižuje riziko kybernetických útokov a zvyšuje úroveň compliance.

1.2. Návrh technologickej architektúry

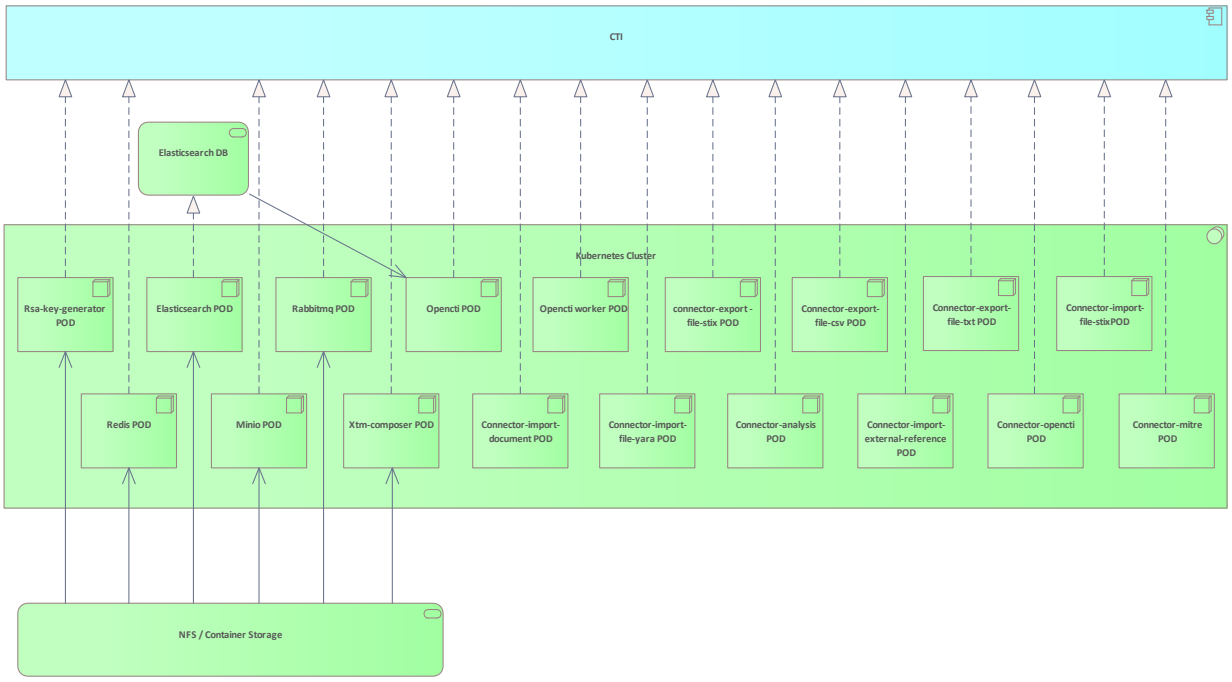
Technologická architektúra určuje spôsob nasadenia, prevádzky a vzájomného prepojenia jednotlivých technických komponentov, vrátane kontajnerizovaných služieb, dátových úložísk, sieťových vrstiev a nástrojov na orchestráciu. Je navrhnutá s dôrazom na modularitu, škálovateľnosť, dostupnosť a bezpečnosť, pričom zohľadňuje požiadavky kladené na multitenantné prevádzkové prostredie.

V tejto časti sú rozpracované konkrétne technologické prvky – ako sú Kubernetes klastre, databázové služby, CI/CD nástroje, kontajnerové registre, proxy vrstvy a zabezpečovacie mechanizmy – a ich väzby na aplikačné komponenty. Podkapitola zároveň poskytuje kontext pre ďalšie technické špecifikácie riešenia vrátane architektúrnych pohľadov, ktoré mapujú funkčné celky ako CTI, EDR, SOAR, inventarizáciu aktív, ako aj zber a analýzu dát. Návrh technologickej architektúry tak vytvára spoľahlivý a dobre riaditeľný základ pre realizáciu celého riešenia v súlade s definovanými biznis cieľmi.

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.

1.1.1. Technology Viewpoint CTI



Obrázok 2: 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 viaczákaznickej 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

Technologická služba NoSQL Elasticsearch databázy je výkonný a distribuovaný systém určený na indexovanie, vyhľadávanie a analýzu dát v reálnom čase, založený na dokumentovo orientovanom modeli. Využíva schému JSON dokumentov, podporuje horizontálne škálovanie, vysokú dostupnosť a je optimalizovaný na spracovanie veľkých objemov nestruktúrovaných alebo semištruktúrovaných údajov, ako sú logy, metriky alebo aplikačné záznamy.

Elasticsearch POD

POD Elasticsearch pre NoSQL databázu je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje Elasticsearch node ako súčasť distribuovaného clustra NoSQL databázy. Tento POD zabezpečuje indexovanie, vyhľadávanie a ukladanie dokumentovo orientovaných dát, pričom umožňuje horizontálne škálovanie, vysokú dostupnosť a efektívne spracovanie veľkých objemov nestruktúrovaných informácií v reálnom čase.

Connector-analysis POD

POD connector-analysis je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje analytický konektor pre OpenCTI, určený na automatizované spracovanie, analýzu a obohacovanie spravodajských informácií o hrozbách. Tento POD prijíma vstupné dáta z OpenCTI, vykonáva nad nimi analytické operácie (napr. reputačné overenie, spracovanie IoC alebo koreláciu entít) a výsledky vracia späť do systému na ďalšiu spravodajskú činnosť a rozhodovanie.

Connector-export-file-csv POD

POD connector-export-file-csv je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje exportný konektor pre OpenCTI, určený na generovanie a ukladanie dát vo formáte CSV (Comma-Separated Values). Tento POD umožňuje automatizovaný export spravodajských informácií, ako sú indikátory hrozieb, útokové techniky alebo aktéri, do CSV súborov, čím podporuje ich jednoduchú integráciu s externými systémami, reporting alebo manuálnu analýzu.

Connector-export-file-stix POD

POD connector-export-file-stix je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI určený na export dát do STIX formátu (Structured Threat Information Expression). Tento POD umožňuje automatizované generovanie a ukladanie hrozbových informácií vo formáte STIX 2.1, čím podporuje štandardizované zdieľanie kyberneticko-bezpečnostných dát s inými systémami, partnermi alebo komunitami.

Connector-export-file-txt POD

POD connector-export-file-txt je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje exportný konektor pre OpenCTI, určený na generovanie textových súborov (TXT) obsahujúcich vybrané hrozbové informácie. Tento POD umožňuje automatizovaný export indikátorov kompromitácie (IoC) a ďalších CTI dát vo forme jednoduchého, čitateľného textového výstupu pre ďalšie použitie v externých systémoch, nástrojoch alebo manuálnych procesoch.

Connector-import-document POD

POD connector-import-document je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI, určený na automatizovaný import dokumentov obsahujúcich spravodajské alebo bezpečnostné informácie. Tento POD spracúva súbory vo formátoch ako PDF, DOCX alebo TXT, extrahuje z nich relevantné dáta a následne ich importuje do platformy OpenCTI ako štruktúrované objekty na ďalšiu analýzu a koreláciu.

Connector-import-external-reference POD

POD connector-import-external-reference je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI zameraný na import externých referencií z verejných alebo súkromných zdrojov hrozbových informácií. Tento POD pravidelne načítava metadáta a odkazy na správy, články alebo analytické dokumenty, prevádza ich na štruktúrované objekty CTI (Cyber Threat Intelligence) a integruje ich do OpenCTI na účely korelácie a analytického obohacovania hrozbového profilu.

Connector-import-file-stixPOD

POD connector-import-file-stix je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje importný konektor pre OpenCTI, zameraný na načítanie a spracovanie súborov vo formáte STIX (Structured Threat Information Expression). Tento POD automatizovane importuje hrozbové informácie zo STIX 2.0/2.1 súborov do OpenCTI, kde sú následne

transformované na štruktúrované CTI objekty a integrované do existujúcich dát pre účely korelácie, vizualizácie a spravodajskej analýzy.

Connector-import-file-yara POD

POD connector-import-file-yara je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI zameraný na import YARA súborov – pravidiel používaných na detekciu malvéru a hrozieb. Tento POD automaticky načítava YARA súbory z definovaného úložiska, analyzuje ich obsah a prevádza ich na štruktúrované hrozbové objekty, ktoré následne importuje do OpenCTI na účely správy a korelácie spravodajských informácií.

Connector-mitre POD

POD connector-mitre je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI určený na automatizovaný import dát z MITRE ATT&CK frameworku. Tento POD pravidelne sťahuje a synchronizuje oficiálne taktiky, techniky, procedúry (TTPs), skupiny, softvér a kampane z MITRE databázy a následne ich transformuje do štruktúrovaných CTI objektov v OpenCTI, čím podporuje presnú a aktuálnu analýzu kybernetických hrozieb.

Connector-opencti POD

POD connector-opencti je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje hlavný konektor OpenCTI, zabezpečujúci obojsmernú komunikáciu medzi OpenCTI platformou a jednotlivými konektormi. Tento POD slúži ako middleware, ktorý registruje konektory, koordinuje ich činnosť a zabezpečuje výmenu dát prostredníctvom OpenCTI API a message brokeru (napr. RabbitMQ), čím umožňuje škálovateľné, modulárne a efektívne spracovanie kyberneticko-bezpečnostných informácií.

Minio POD

POD MinIO je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje službu MinIO – vysoko výkonný, škálovateľný a kompatibilný objektový storage systém typu S3. Tento POD poskytuje úložisko pre neštruktúrované dáta, ako sú logy, zálohy, multimediálne súbory či výstupy analytických nástrojov, pričom podporuje vysokú dostupnosť, replikáciu a integráciu s modernými cloud-native aplikáciami.

Opencti POD

OpenCTI POD je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje platformu OpenCTI (Open Cyber Threat Intelligence) – open-source riešenie na správu, analýzu a koreláciu kybernetických hrozieb a spravodajských informácií (Threat Intelligence). Tento POD poskytuje centrálny uzol na zhromažďovanie, vizualizáciu a prepájanie informácií o hrozbách, vrátane entít ako TTPs (tactics, techniques, procedures), indikátorov kompromitácie (IoC) či aktérov hrozieb, a podporuje integráciu s ďalšími bezpečnostnými nástrojmi cez API.

Opencti worker POD

POD OpenCTI Worker je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá vykonáva asynchrónne spracovanie úloh a dátových operácií v rámci platformy OpenCTI. Tento POD zabezpečuje indexovanie, transformáciu, koreláciu a obohacovanie kybernetickobezpečnostných informácií, pričom úzko spolupracuje s hlavným OpenCTI serverom a konektormi na zabezpečenie plynulej dátovej integrácie a výpočtovej distribúcie.

Rabbitmq POD

POD RabbitMQ je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje RabbitMQ server – spoľahlivý a rozšírený message broker implementujúci protokoly ako AMQP, MQTT alebo STOMP. Tento POD zabezpečuje asynchrónnu komunikáciu a výmenu správ medzi službami a komponentmi systému, čím podporuje škálovateľnosť, odolnosť a efektívne spracovanie úloh v distribuovaných aplikáciách.

Redis POD

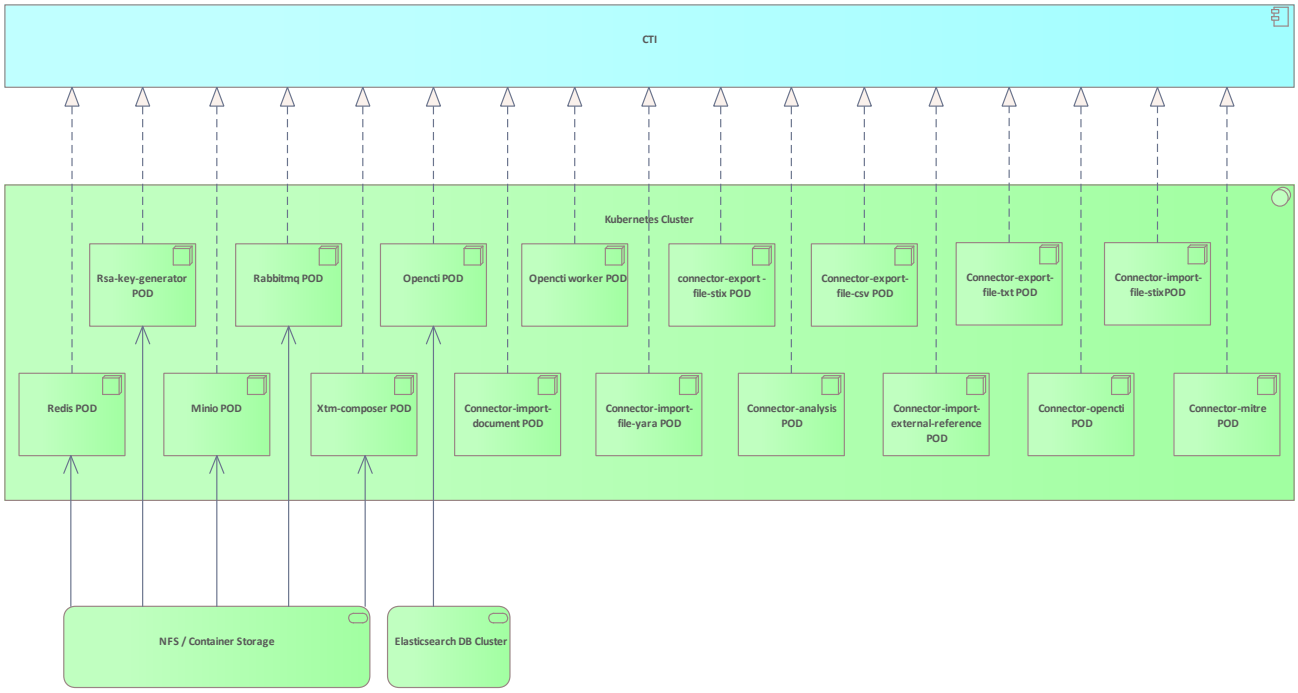
POD redis je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje Redis server – vysoko výkonnú in-memory NoSQL databázu typu key-value. Tento POD slúži na rýchle ukladanie, čítanie a manipuláciu s dočasnými alebo pretrvávajúcimi dátami, často využívanými na caching, frontovanie správ, ukladanie relácií a zdieľanie stavov medzi mikroservisami.

Rsa-key-generator POD

POD rsa-key-generator je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá slúži na generovanie RSA kľúčových párov pre potreby šifrovania, digitálneho podpisovania alebo zabezpečenej komunikácie. Tento POD zabezpečuje automatizované a bezpečné vytváranie kryptografických kľúčov, ktoré môžu byť následne použité inými službami v rámci infraštruktúry, napríklad na TLS certifikáty, GPG podpisy alebo autentifikáciu.

Xtm-composer POD

POD xtm-composer je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje službu XTM Composer – komponentu určenú na kompozíciu a generovanie dátových alebo bezpečnostných výstupov v rámci väčšieho systému, často súvisiaceho so správou kybernetickej bezpečnosti alebo automatizovaným reportovaním. Tento POD zabezpečuje spracovanie vstupných údajov, ich transformáciu a výstup vo vopred definovanom formáte, pričom môže spolupracovať s ďalšími komponentmi ako databázy, analytické nástroje alebo API brány.



Obrázok 3: 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 viaczákaznickej 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

Technologická služba NoSQL Elasticsearch databázy vo forme clustra predstavuje viacuzlové distribuované riešenie, kde jednotlivé uzly (nodes) spolupracujú na uložení, indexovaní a vyhľadávaní dokumentovo orientovaných dát. Každý uzol v klastri plní špecifickú úlohu (napr. master, data alebo ingest node), čo umožňuje horizontálne škálovanie, vysokú dostupnosť a odolnosť voči výpadkom, pričom systém ako celok zabezpečuje spracovanie veľkého objemu dát v reálnom čase.

Connector-analysis POD

POD connector-analysis je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje analytický konektor pre OpenCTI, určený na automatizované spracovanie, analýzu a obohacovanie spravodajských informácií o hrozbách. Tento POD prijíma vstupné dáta z OpenCTI, vykonáva nad nimi analytické operácie (napr. reputačné overenie, spracovanie IoC alebo koreláciu entít) a výsledky vracia späť do systému na ďalšiu spravodajskú činnosť a rozhodovanie.

Connector-export-file-csv POD

POD connector-export-file-csv je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje exportný konektor pre OpenCTI, určený na generovanie a ukladanie dát vo formáte CSV (Comma-Separated Values). Tento POD umožňuje automatizovaný export spravodajských informácií, ako sú indikátory hrozieb, útokové techniky alebo aktéri, do CSV súborov, čím podporuje ich jednoduchú integráciu s externými systémami, reporting alebo manuálnu analýzu.

Connector-export-file-stix POD

POD connector-export-file-stix je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI určený na export dát do STIX formátu (Structured Threat Information Expression). Tento POD umožňuje automatizované generovanie a ukladanie hrozbových informácií vo formáte STIX 2.1, čím podporuje štandardizované zdieľanie kyberneticko-bezpečnostných dát s inými systémami, partnermi alebo komunitami.

Connector-export-file-txt POD

POD connector-export-file-txt je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje exportný konektor pre OpenCTI, určený na generovanie textových súborov (TXT) obsahujúcich vybrané hrozbové informácie. Tento POD umožňuje automatizovaný export indikátorov kompromitácie (IoC) a ďalších CTI dát vo forme jednoduchého, čitateľného textového výstupu pre ďalšie použitie v externých systémoch, nástrojoch alebo manuálnych procesoch.

Connector-import-document POD

POD connector-import-document je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI, určený na automatizovaný import dokumentov obsahujúcich spravodajské alebo bezpečnostné informácie. Tento POD spracúva súbory vo formátoch ako PDF, DOCX alebo TXT, extrahuje z nich relevantné dáta a následne ich importuje do platformy OpenCTI ako štruktúrované objekty na ďalšiu analýzu a koreláciu.

Connector-import-external-reference POD

POD connector-import-external-reference je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI zameraný na import externých referencií z verejných alebo súkromných zdrojov hrozbových informácií. Tento POD pravidelne načítava metadáta a odkazy na správy, články alebo analytické dokumenty, prevádza ich na štruktúrované objekty CTI (Cyber Threat Intelligence) a integruje ich do OpenCTI na účely korelácie a analytického obohacovania hrozbového profilu.

Connector-import-file-stixPOD

POD connector-import-file-stix je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje importný konektor pre OpenCTI, zameraný na načítanie a spracovanie súborov vo formáte STIX (Structured Threat Information Expression). Tento POD automatizovane importuje hrozbové informácie zo STIX 2.0/2.1 súborov do OpenCTI, kde sú následne transformované na štruktúrované CTI objekty a integrované do existujúcich dát pre účely korelácie, vizualizácie a spravodajskej analýzy.

Connector-import-file-yara POD

POD connector-import-file-yara je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI zameraný na import YARA súborov – pravidiel používaných na detekciu malvéru a hrozieb. Tento POD automaticky načítava YARA súbory z definovaného úložiska, analyzuje ich obsah a prevádza ich na štruktúrované hrozbové objekty, ktoré následne importuje do OpenCTI na účely správy a korelácie spravodajských informácií.

Connector-mitre POD

POD connector-mitre je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje konektor pre OpenCTI určený na automatizovaný import dát z MITRE ATT&CK frameworku. Tento POD pravidelne sťahuje a synchronizuje oficiálne taktiky, techniky, procedúry (TTPs), skupiny, softvér a kampane z MITRE databázy a následne ich transformuje

do štruktúrovaných CTI objektov v OpenCTI, čím podporuje presnú a aktuálnu analýzu kybernetických hrozieb.

Connector-opencti POD

POD connector-opencti je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje hlavný konektor OpenCTI, zabezpečujúci obojsmernú komunikáciu medzi OpenCTI platformou a jednotlivými konektormi. Tento POD slúži ako middleware, ktorý registruje konektory, koordinuje ich činnosť a zabezpečuje výmenu dát prostredníctvom OpenCTI API a message brokeru (napr. RabbitMQ), čím umožňuje škálovateľné, modulárne a efektívne spracovanie kyberneticko-bezpečnostných informácií.

Minio POD

POD MinIO je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje službu MinIO – vysoko výkonný, škálovateľný a kompatibilný objektový storage systém typu S3. Tento POD poskytuje úložisko pre neštruktúrované dáta, ako sú logy, zálohy, multimediálne súbory či výstupy analytických nástrojov, pričom podporuje vysokú dostupnosť, replikáciu a integráciu s modernými cloud-native aplikáciami.

Opencti POD

OpenCTI POD je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje platformu OpenCTI (Open Cyber Threat Intelligence) – open-source riešenie na správu, analýzu a koreláciu kybernetických hrozieb a spravodajských informácií (Threat Intelligence). Tento POD poskytuje centrálny uzol na zhromažďovanie, vizualizáciu a prepájanie informácií o hrozbách, vrátane entít ako TTPs (tactics, techniques, procedures), indikátorov kompromitácie (IoC) či aktérov hrozieb, a podporuje integráciu s ďalšími bezpečnostnými nástrojmi cez API.

Opencti worker POD

POD OpenCTI Worker je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá vykonáva asynchrónne spracovanie úloh a dátových operácií v rámci platformy OpenCTI. Tento POD zabezpečuje indexovanie, transformáciu, koreláciu a obohacovanie kyberneticko-bezpečnostných informácií, pričom úzko spolupracuje s hlavným OpenCTI serverom a konektormi na zabezpečenie plynulej dátovej integrácie a výpočtovej distribúcie.

Rabbitmq POD

POD RabbitMQ je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje RabbitMQ server – spoľahlivý a rozšírený message broker implementujúci protokoly ako AMQP, MQTT alebo STOMP. Tento POD zabezpečuje asynchrónnu komunikáciu a výmenu správ medzi službami a komponentmi systému, čím podporuje škálovateľnosť, odolnosť a efektívne spracovanie úloh v distribuovaných aplikáciách.

Redis POD

POD redis je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje Redis server – vysoko výkonnú in-memory NoSQL databázu typu key-value. Tento POD slúži na rýchle ukladanie, čítanie a manipuláciu s dočasnými alebo pretrvávajúcimi dátami, často využívanými na caching, frontovanie správ, ukladanie relácií a zdieľanie stavov medzi mikroservisami.

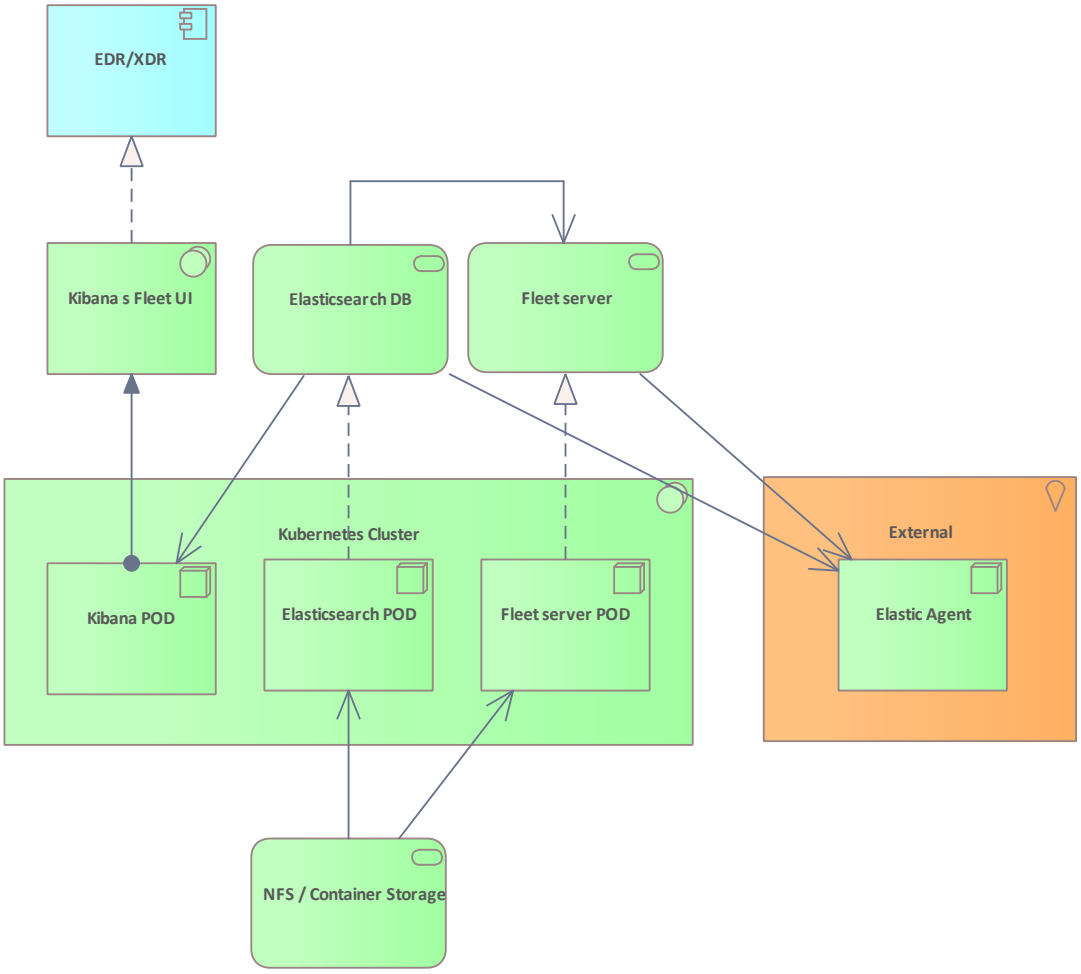
Rsa-key-generator POD

POD rsa-key-generator je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá slúži na generovanie RSA kľúčových párov pre potreby šifrovania, digitálneho podpisovania alebo zabezpečenej komunikácie. Tento POD zabezpečuje automatizované a bezpečné vytváranie kryptografických kľúčov, ktoré môžu byť následne použité inými službami v rámci infraštruktúry, napríklad na TLS certifikáty, GPG podpisy alebo autentifikáciu.

Xtm-composer POD

POD xtm-composer je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje službu XTM Composer – komponentu určenú na kompozíciu a generovanie dátových alebo bezpečnostných výstupov v rámci väčšieho systému, často súvisiaceho so správou kybernetickej bezpečnosti alebo automatizovaným reportovaním. Tento POD zabezpečuje spracovanie vstupných údajov, ich transformáciu a výstup vo vopred definovanom formáte, pričom môže spolupracovať s ďalšími komponentmi ako databázy, analytické nástroje alebo API brány.

1.1.2. Technology Viewpoint EDR/XDR



Obrázok 4: 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

Technologická služba NoSQL Elasticsearch databázy je výkonný a distribuovaný systém určený na indexovanie, vyhľadávanie a analýzu dát v reálnom čase, založený na dokumentovo orientovanom modeli. Využíva schému JSON dokumentov, podporuje horizontálne škálovanie, vysokú dostupnosť a je optimalizovaný na spracovanie veľkých objemov nestruktúrovaných alebo semištruktúrovaných údajov, ako sú logy, metriky alebo aplikačné záznamy.

Elasticsearch POD

POD Elasticsearch pre NoSQL databázu je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje Elasticsearch node ako súčasť distribuovaného clustra NoSQL databázy. Tento POD zabezpečuje indexovanie, vyhľadávanie a ukladanie dokumentovo orientovaných dát, pričom umožňuje horizontálne škálovanie, vysokú dostupnosť a efektívne spracovanie veľkých objemov nestruktúrovaných informácií v reálnom čase.

External

Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

Kibana POD

POD Kibana pre SIEM je kontajnerová inštancia nasadená v Kubernetes clustri, ktorá poskytuje grafické používateľské rozhranie pre vizualizáciu a analýzu bezpečnostných údajov zhromaždených v Elasticsearch. Slúži ako frontend komponent pre SIEM (Security Information and Event Management) riešenie, umožňujúci interaktívne monitorovanie, koreláciu udalostí, tvorbu dashboardov a detekciu bezpečnostných incidentov v reálnom čase.

Fleet server

Technologická služba Fleet Server je centrálny komponent Elastic Stacku, ktorý slúži na správu, koordináciu a zabezpečenú komunikáciu Elastic Agentov nasadených v rôznych systémoch. Fleet Server sprostredkúva konfigurácie, aktualizácie a príkazy z Kibana Fleet UI k jednotlivým agentom, čím umožňuje centralizovanú správu zberu logov, metrík a bezpečnostných údajov v rámci veľkých distribuovaných prostredí.

Elastic Agent

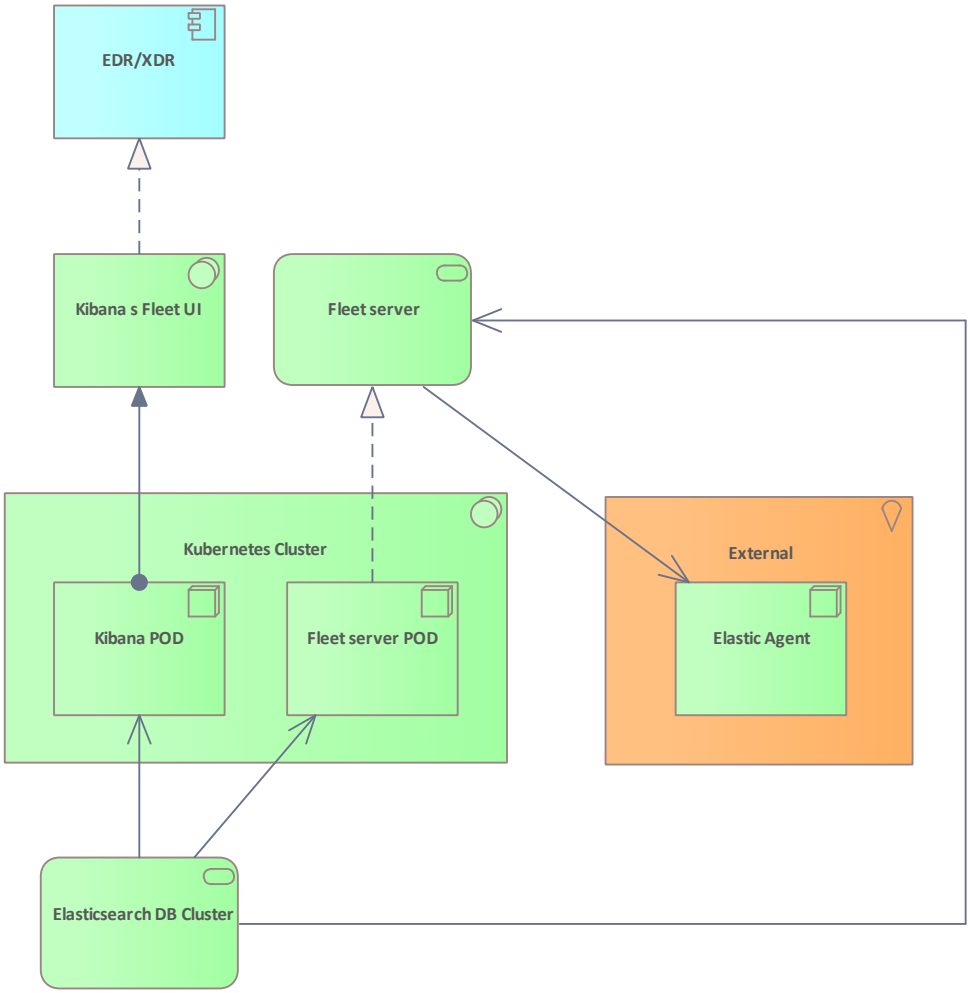
Predstavuje inštanciu Elastic Agent pre monitoring a spracovanie logov a ich zapísanie do Elasticsearch a ochranu hosta pred bezpečnostnými hrozbami.

Fleet server POD

POD Elasticsearch pre NoSQL databázu je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje Elasticsearch node ako súčasť distribuovaného vyhľadávacieho a indexovacieho systému. Tento POD zabezpečuje ukladanie, vyhľadávanie a analýzu dokumentovo orientovaných dát v reálnom čase, s podporou horizontálneho škálovania, vysokej dostupnosti a integrácie s ďalšími nástrojmi v dátovo-analytickom alebo bezpečnostnom ekosystéme.

Kibana s Fleet UI

Kibana s Fleet UI je rozšírené webové rozhranie nástroja Kibana, ktoré poskytuje centralizovanú správu agentov a dátových integrácií v rámci Elastic Stacku. Fleet UI umožňuje jednoduché nasadzovanie, konfiguráciu a monitoring Elastic Agentov, čím zjednodušuje zber logov, metrík a bezpečnostných údajov z rôznych systémov a ich následnú vizualizáciu a analýzu v Kibane.



Obrázok 5: 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

Technologická služba NoSQL Elasticsearch databázy vo forme clustra predstavuje viacuzlové distribuované riešenie, kde jednotlivé uzly (nodes) spolupracujú na uložení, indexovaní a vyhľadávaní dokumentovo orientovaných dát. Každý uzol v klastri plní špecifickú úlohu (napr. master, data alebo ingest node), čo umožňuje horizontálne škálovanie, vysokú dostupnosť a odolnosť voči výpadkom, pričom systém ako celok zabezpečuje spracovanie veľkého objemu dát v reálnom čase.

External

Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

Kibana POD

POD Kibana pre SIEM je kontajnerová inštancia nasadená v Kubernetes clustri, ktorá poskytuje grafické používateľské rozhranie pre vizualizáciu a analýzu bezpečnostných údajov zhromaždených v Elasticsearch. Slúži ako frontend komponent pre SIEM (Security Information and Event Management) riešenie, umožňujúci interaktívne monitorovanie, koreláciu udalostí, tvorbu dashboardov a detekciu bezpečnostných incidentov v reálnom čase.

Fleet server

Technologická služba Fleet Server je centrálny komponent Elastic Stacku, ktorý slúži na správu, koordináciu a zabezpečenú komunikáciu Elastic Agentov nasadených v rôznych systémoch. Fleet Server sprostredkúva konfigurácie, aktualizácie a príkazy z Kibana Fleet UI k jednotlivým agentom, čím umožňuje centralizovanú správu zberu logov, metrík a bezpečnostných údajov v rámci veľkých distribuovaných prostredí.

Elastic Agent

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

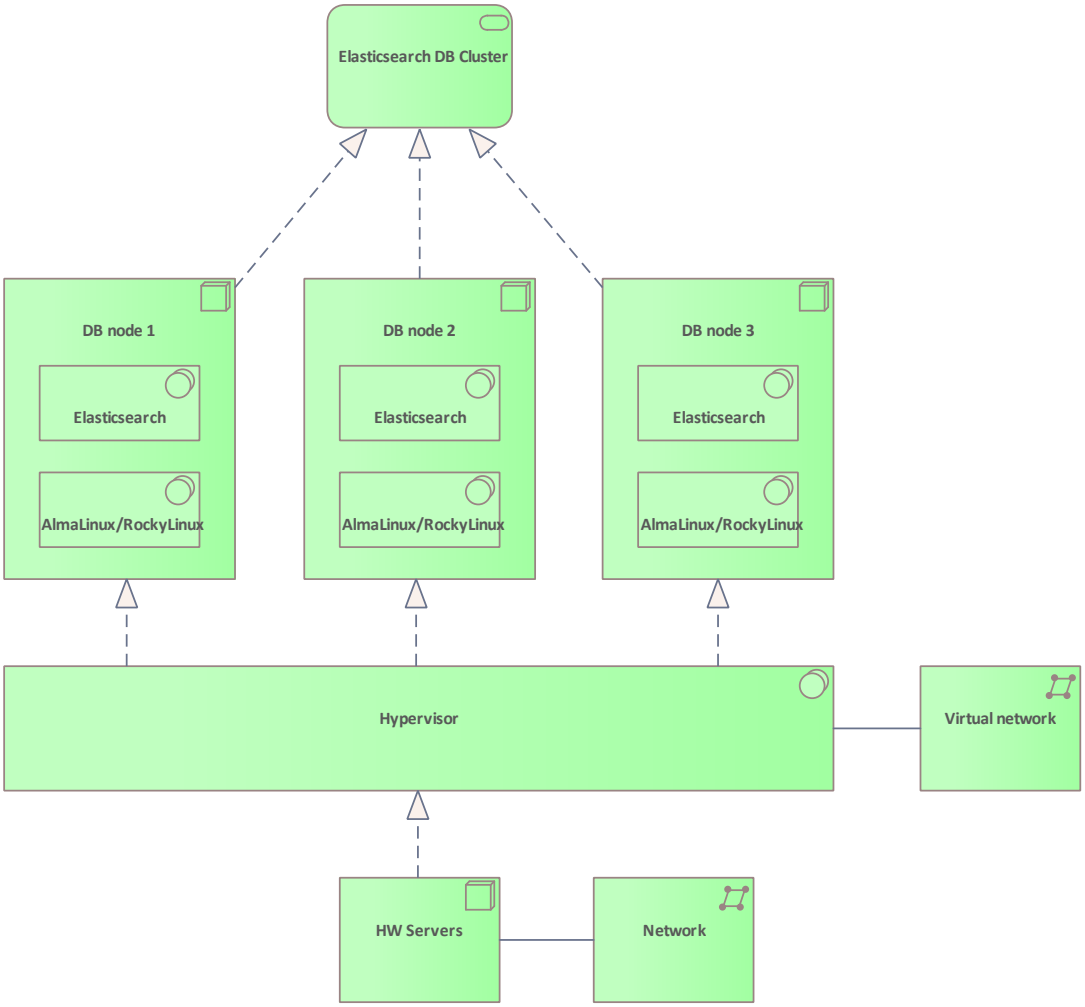
Fleet server POD

POD Elasticsearch pre NoSQL databázu je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje Elasticsearch node ako súčasť distribuovaného vyhľadávacieho a indexovacieho systému. Tento POD zabezpečuje ukladanie, vyhľadávanie a analýzu dokumentovo orientovaných dát v reálnom čase, s podporou horizontálneho škálovania, vysokej dostupnosti a integrácie s ďalšími nástrojmi v dátovo-analytickom alebo bezpečnostnom ekosystéme.

Kibana s Fleet UI

Kibana s Fleet UI je rozšírené webové rozhranie nástroja Kibana, ktoré poskytuje centralizovanú správu agentov a dátových integrácií v rámci Elastic Stacku. Fleet UI umožňuje jednoduché nasadzovanie, konfiguráciu a monitoring Elastic Agentov, čím zjednodušuje zber logov, metrík a bezpečnostných údajov z rôznych systémov a ich následnú vizualizáciu a analýzu v Kibane.

1.1.3. Technology Viewpoint INNOSOC Common



Obrázok 6 : Technology Viewpoint DB Cluster

Diagram znázorňuje technologickú architektúru PostgreSQL Clustra.

Popis používaných prvkov:

DB node 1

Predstavuje Node 1 Elasticsearch Clustra. Node Elasticsearch Clustra je jednotlivá inštancia Elasticsearch, ktorá je súčasťou distribuovaného clustra a plní jednu alebo viac

špecifických úloh, ako napríklad správa dát, indexovanie alebo koordinácia požiadaviek. Každý node komunikuje s ostatnými uzlami v clustri, pričom spoločne zabezpečujú škálovateľnosť, vysokú dostupnosť a paralelné spracovanie dotazov a operácií nad veľkými objemami dát.

DB node 2

Predstavuje Node 2 Elasticsearch Clustra. Node Elasticsearch Clustra je jednotlivá inštancia Elasticsearch, ktorá je súčasťou distribuovaného clustra a plní jednu alebo viac špecifických úloh, ako napríklad správa dát, indexovanie alebo koordinácia požiadaviek. Každý node komunikuje s ostatnými uzlami v clustri, pričom spoločne zabezpečujú škálovateľnosť, vysokú dostupnosť a paralelné spracovanie dotazov a operácií nad veľkými objemami dát.

DB node 3

Predstavuje Node 3 Elasticsearch Clustra. Node Elasticsearch Clustra je jednotlivá inštancia Elasticsearch, ktorá je súčasťou distribuovaného clustra a plní jednu alebo viac špecifických úloh, ako napríklad správa dát, indexovanie alebo koordinácia požiadaviek. Každý node komunikuje s ostatnými uzlami v clustri, pričom spoločne zabezpečujú škálovateľnosť, vysokú dostupnosť a paralelné spracovanie dotazov a operácií nad veľkými objemami dát.

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. AlmaLinux a RockyLinux sú open-source Linuxové distribúcie založené na Red Hat Enterprise Linux (RHEL), ktoré poskytujú plne binárne kompatibilné alternatívy k RHEL bez licenčných obmedzení. Sú navrhnuté pre stabilné, bezpečné a dlhodobo podporované serverové prostredia, a často sa využívajú v podnikových, cloudových a dátových centrách ako náhrada za CentOS po jeho ukončení ako downstream projektu.

Elasticsearch

Predstavuje Elasticsearch NoSQL databázu. Elasticsearch je vysoko výkonná, distribuovaná NoSQL databáza, navrhnutá na indexovanie, fulltextové vyhľadávanie a analýzu veľkého objemu dát v reálnom čase. Využíva dokumentovo orientovaný model na báze JSON, podporuje horizontálne škálovanie, vysokú dostupnosť a je široko používaná v oblastiach ako log management, monitorovanie, bezpečnostná analytika a business intelligence.

AlmaLinux/RockyLinux

Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux. AlmaLinux a RockyLinux sú open-source Linuxové distribúcie založené na Red Hat Enterprise Linux (RHEL), ktoré poskytujú plne binárne kompatibilné alternatívy k RHEL bez licenčných obmedzení. Sú navrhnuté pre stabilné, bezpečné a dlhodobo podporované serverové prostredia, a často sa využívajú v podnikových, cloudových a dátových centrách ako náhrada za CentOS po jeho ukončení ako downstream projektu.

Elasticsearch

Predstavuje Elasticsearch NoSQL databázu. Elasticsearch je vysoko výkonná, distribuovaná NoSQL databáza, navrhnutá na indexovanie, fulltextové vyhľadávanie a analýzu veľkého objemu dát v reálnom čase. Využíva dokumentovo orientovaný model na báze JSON, podporuje horizontálne škálovanie, vysokú dostupnosť a je široko používaná v oblastiach ako log management, monitorovanie, bezpečnostná analytika a business intelligence.

AlmaLinux/RockyLinux

Predstavuje Linuxovú distibúciu AlmaLinux/RockyLinux. AlmaLinux a RockyLinux sú open-source Linuxové distribúcie založené na Red Hat Enterprise Linux (RHEL), ktoré poskytujú plne binárne kompatibilné alternatívy k RHEL bez licenčných obmedzení. Sú navrhnuté pre stabilné, bezpečné a dlhodobo podporované serverové prostredia, a často sa

využívajú v podnikových, cloudových a dátových centrách ako náhrada za CentOS po jeho ukončení ako downstream projektu.

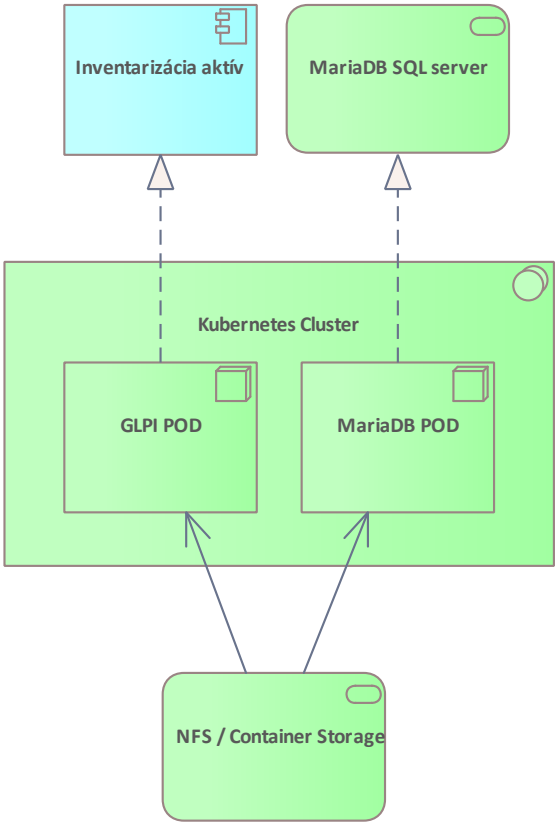
Elasticsearch

Predstavuje Elasticsearch NoSQL databázu. Elasticsearch je vysoko výkonná, distribuovaná NoSQL databáza, navrhnutá na indexovanie, fulltextové vyhľadávanie a analýzu veľkého objemu dát v reálnom čase. Využíva dokumentovo orientovaný model na báze JSON, podporuje horizontálne škálovanie, vysokú dostupnosť a je široko používaná v oblastiach ako log management, monitorovanie, bezpečnostná analytika a business intelligence.

Elasticsearch DB Cluster

Technologická služba NoSQL Elasticsearch databázy vo forme clustra predstavuje viacuzlové distribuované riešenie, kde jednotlivé uzly (nodes) spolupracujú na uložení, indexovaní a vyhľadávaní dokumentovo orientovaných dát. Každý uzol v klastri plní špecifickú úlohu (napr. master, data alebo ingest node), čo umožňuje horizontálne škálovanie, vysokú dostupnosť a odolnosť voči výpadkom, pričom systém ako celok zabezpečuje spracovanie veľkého objemu dát v reálnom čase.

1.1.4. Technology Viewpoint Inventarizacia aktiv



Obrázok 7: 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.

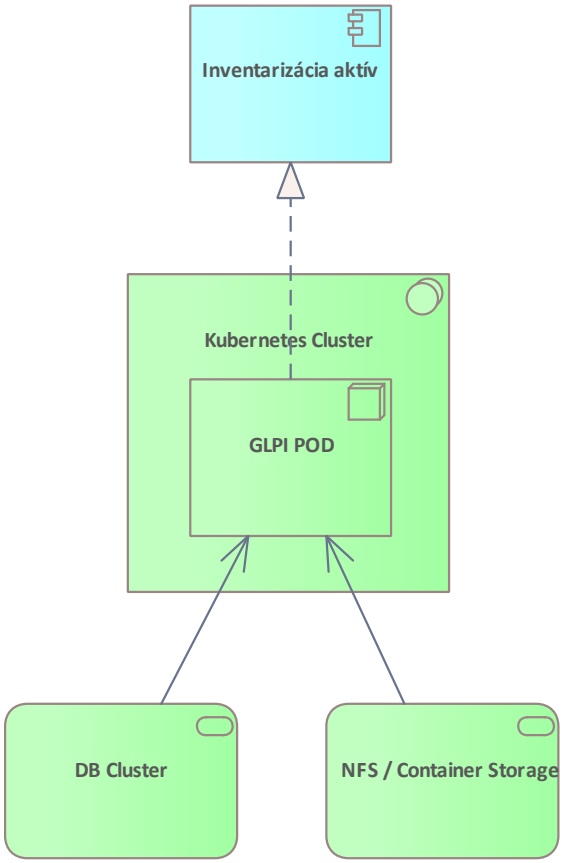
GLPI POD

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 8: 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.

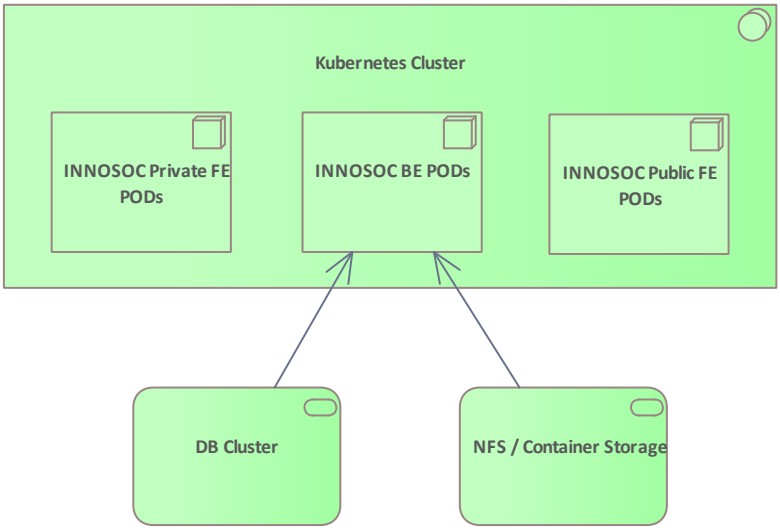
Kubernetes Cluster

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.

1.1.5. Technology Viewpoint Kubernetes



Obrázok 9: Technology Usage Viewpoint 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

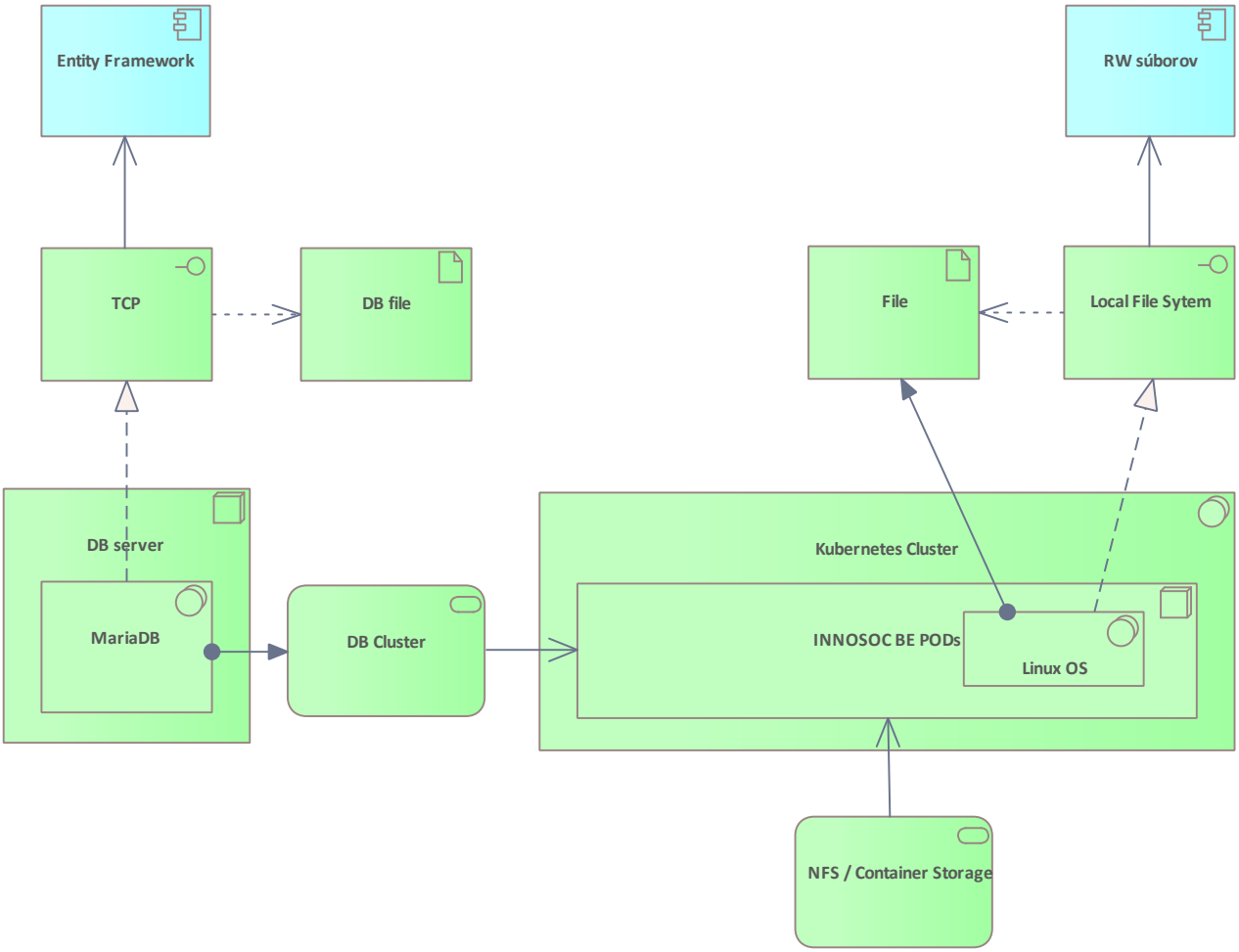
Predstavuje PODy BE. PODy BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému, ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu architektúry, ktorá zaisťuje spracovanie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

INNOSOC Private FE PODs

PODy FE Private predstavujú izolované a modulárne jednotky nasadenia frontendových komponentov systému 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 FE Public predstavujú výpočtové jednotky nasadenia frontendových komponentov systému vo 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 službám bez nutnosti lokálnej inštalácie alebo privátnej infraštruktúry.



Obrázok 10: Technology Usage Viewpoint BE, DB and File System

Diagram repezentuje a bližšie popisuje využívanie perzistentnej vrstvy pre potreby BIT NC a 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 BE. PODy BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému, ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu architektúry, ktorá zaisťuje spracovanie dát, business logiku, transakcie, API služby a interakciu s databázou a sieťovými entitami (core network functions).

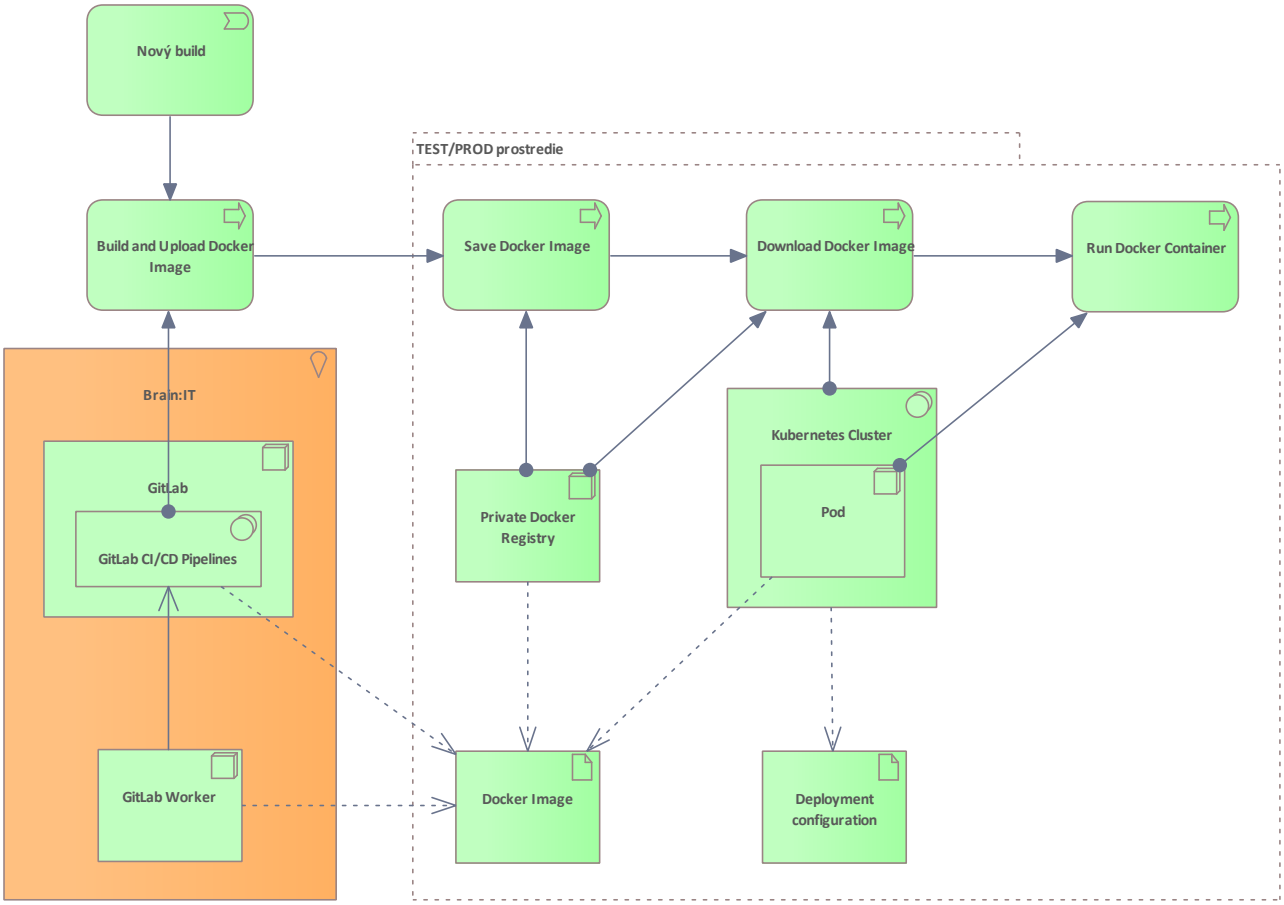
Linux OS

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 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 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

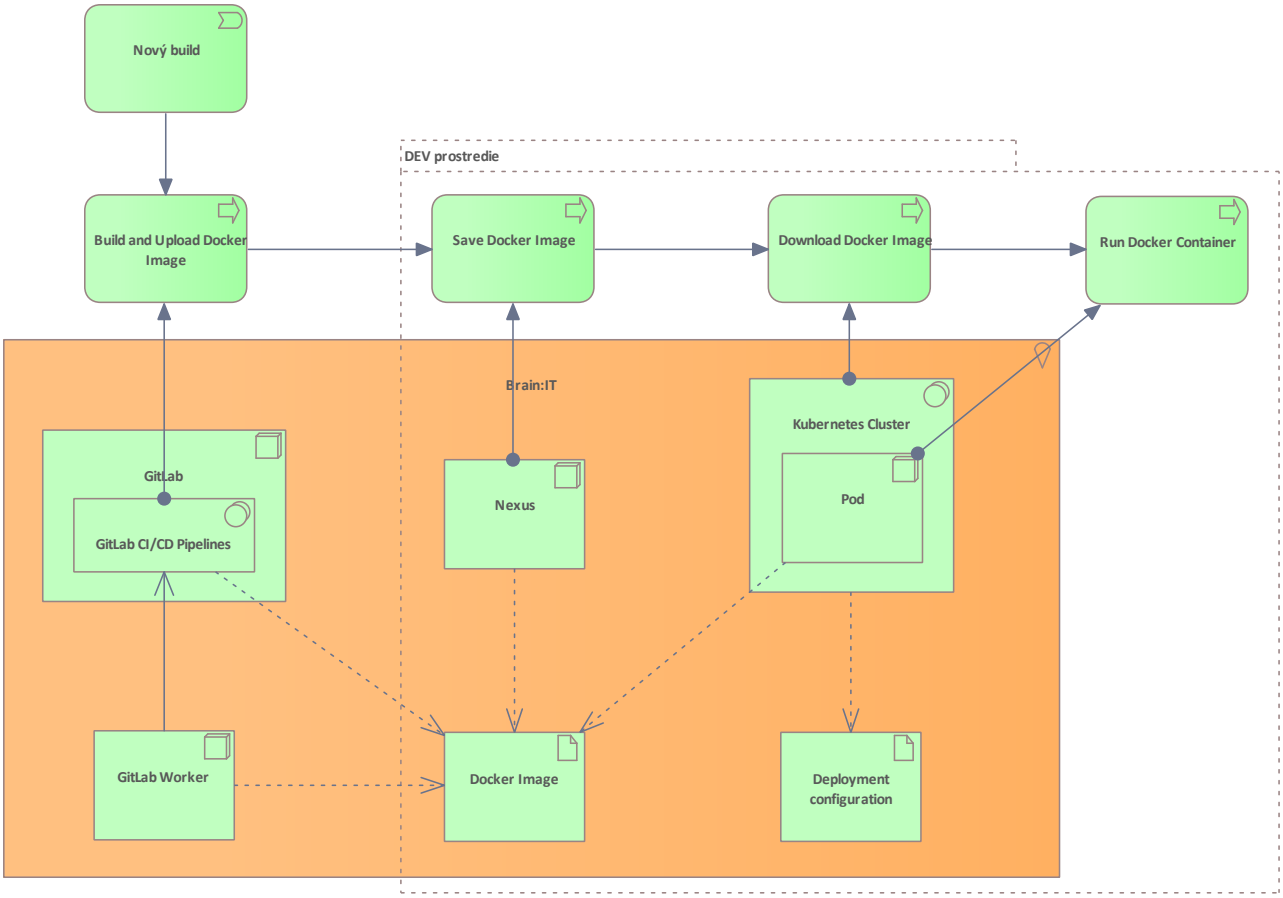
Predstavuje Kubernetes Cluster. Kubernetes Cluster je distribuované výpočtové prostredie, ktoré slúži na orchestráciu kontajnerizovaných aplikácií. Zabezpečuje nasadzovanie, škálovanie, monitorovanie, aktualizáciu a správu kontajnerov (najčastejšie Docker alebo kompatibilné OCI kontajnery) naprieč skupinou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

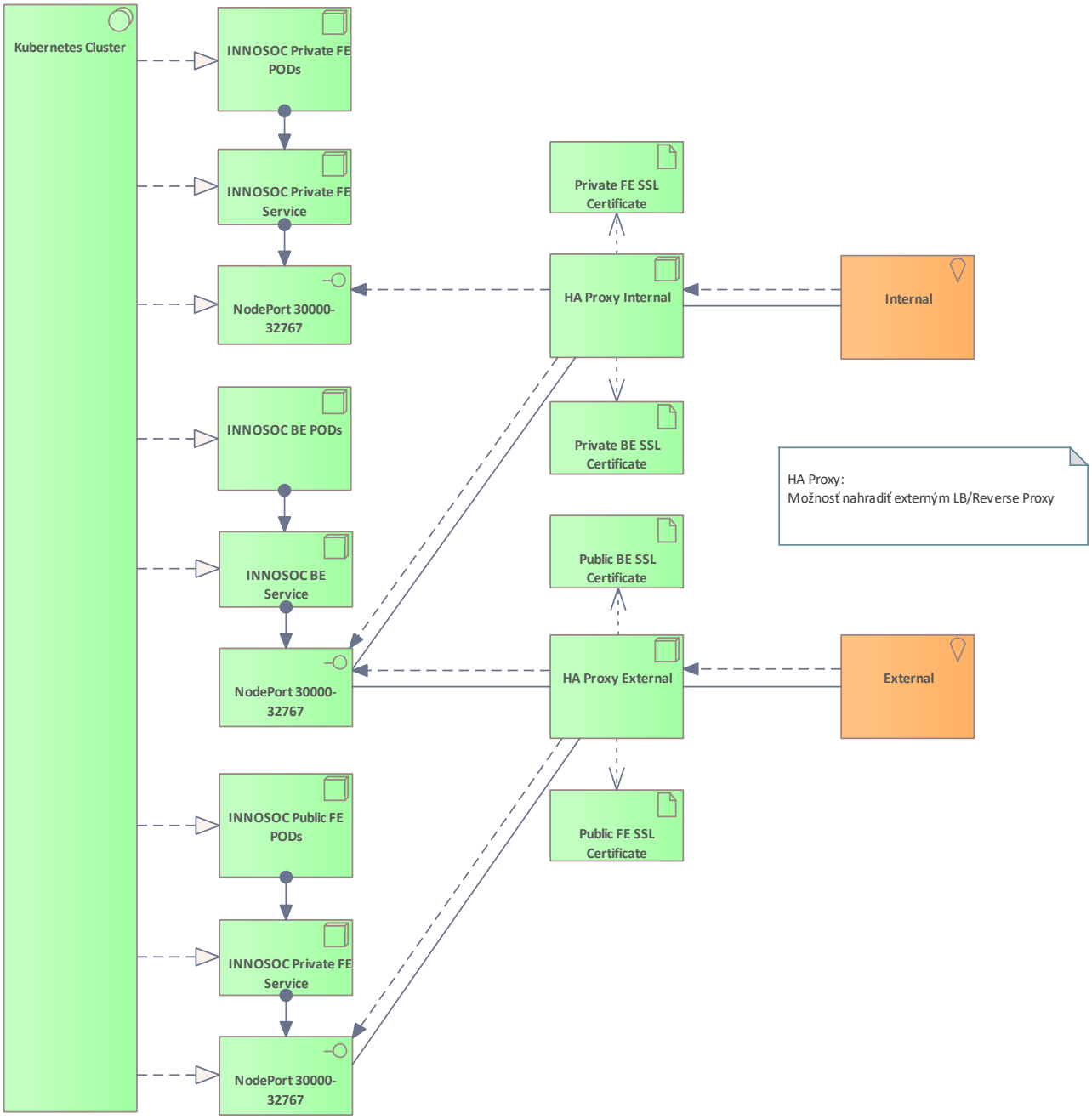
Predstavuje private Docker Registry. Private Docker Registry je súkromné úložisko pre Docker imagy, ktoré umožňuje organizáciám bezpečne ukladať a spravovať kontajnerové obrazy mimo verejných služieb ako Docker Hub. Poskytuje kontrolu nad prístupom, verziami a distribúciou image-ov, a je často integrovaný 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 13: 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

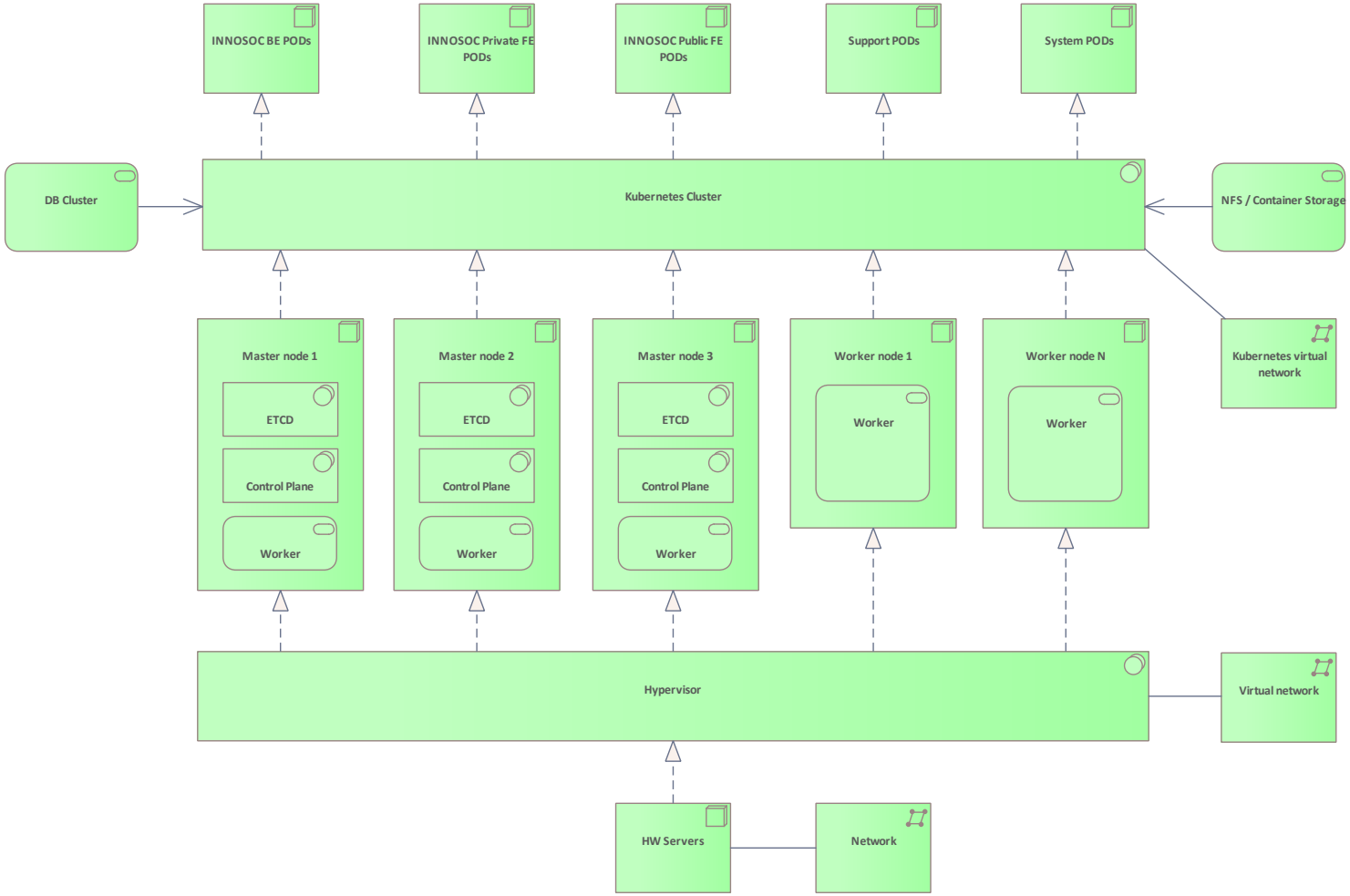
Predstavuje PODy BE. PODy BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému, ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu architektúry, ktorá zaisťuje spracovanie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

INNOSOC Private FE PODs

PODy FE Private predstavujú izolované a modulárne jednotky nasadenia frontendových komponentov systému 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 FE Public predstavujú výpočtové jednotky nasadenia frontendových komponentov systému vo 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 službám bez nutnosti lokálnej inštalácie alebo privátnej infraštruktúry.



Obrázok 14: 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 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 3

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.

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. 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.

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 BE. PODy BE označujú kontajnerové inštancie backendových služieb (BE – Backend) systému, ktoré sú nasadené v distribuovanom prostredí, typicky v Kubernetes clustri alebo inej kontajnerovej orchestrácii. Tieto PODy tvoria serverovú (logickú) vrstvu 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 FE Private predstavujú izolované a modulárne jednotky nasadenia frontendových komponentov systému 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 FE Public predstavujú výpočtové jednotky nasadenia frontendových komponentov systému vo 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 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. 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. 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

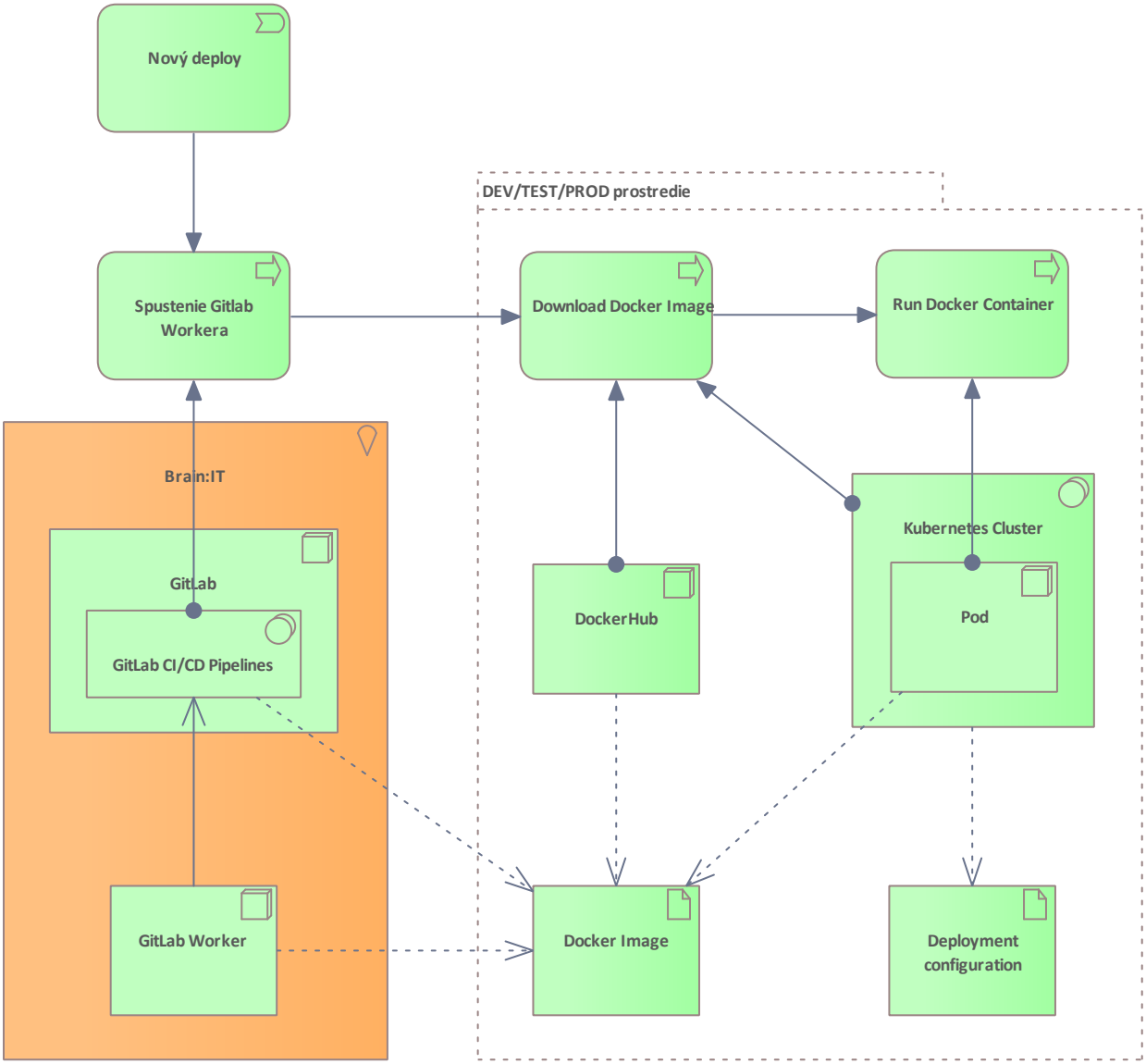
Predstavuje ETCD databázu. ETCD databáza je distribuovaná, vysoko dostupná kľúč-hodnota databáza, navrhnutá pre ukladanie konfiguračných dát a metadát v reálnom čase. Je základnou súčasťou Kubernetes, kde slúži ako centrálne úložisko stavov clustra, vrátane informácií o pods, konfiguráciách, secret-och a ďalších objektoch. Vďaka mechanizmu konsenzu Raft zabezpečuje spoľahlivosť, konzistenciu a odolnosť voči výpadkom v distribuovaných systémoch.

Worker

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

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.



Obrázok 15: 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.

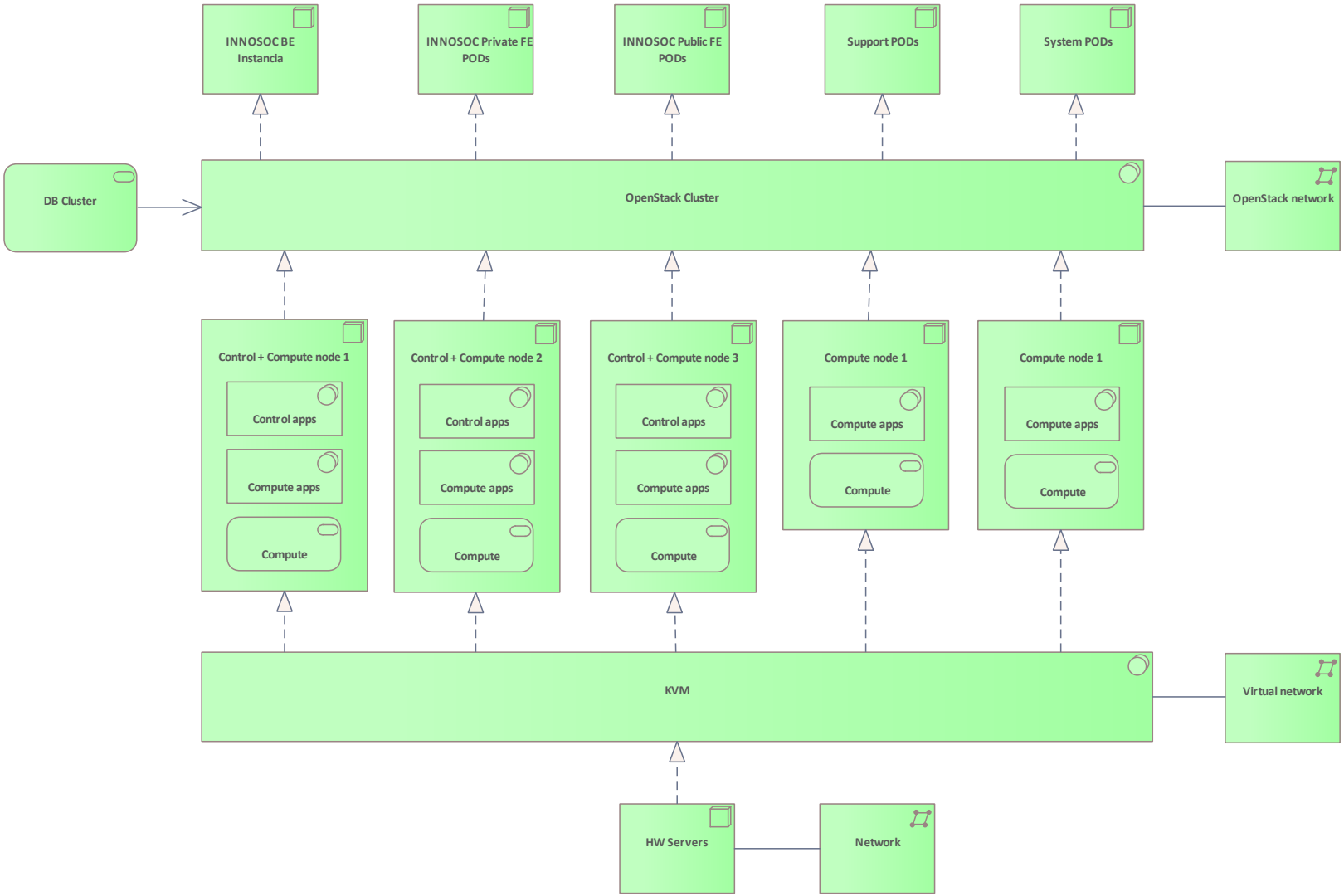
GitLab CI/CD Pipelines

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

1.1.6. Technology Viewpoint OpenStack



Obrázok 16: Technology Viewpoint OpenStack Cluster

Popis používaných prvkov:

DB Cluster

Predstavuje službu clustrovanej relačnej databázy. Služba clustrovanej relačnej databázy predstavuje viacuzlové databázové riešenie, kde sú dáta rozdelené alebo replikované medzi viaceré databázové nody za účelom zabezpečenia vysokej dostupnosti, škálovateľnosti a odolnosti voči výpadkom. Každý uzol v klastri môže slúžiť ako aktívny alebo pasívny člen, v závislosti od použitého režimu. Tento typ databázovej architektúry sa využíva v podnikových systémoch, kde je kritická konzistencia dát, výkon pri záťaži a nepretržitá dostupnosť.

Compute node 1

Predstavuje Compute node OpenStack Clustra. Compute node v OpenStack clustri je výpočtový uzol zodpovedný za spúšťanie a správu virtuálnych strojov (VM) pomocou služby Nova Compute. Prijíma pokyny z Control nodu a poskytuje fyzické alebo virtuálne zdroje ako CPU, RAM a disk pre jednotlivé inštancie, čím tvorí základ výpočtovej kapacity clustra.

Compute node 1

Predstavuje Compute node OpenStack Clustra. Compute node v OpenStack clustri je výpočtový uzol zodpovedný za spúšťanie a správu virtuálnych strojov (VM) pomocou služby Nova Compute. Prijíma pokyny z Control nodu a poskytuje fyzické alebo virtuálne zdroje ako CPU, RAM a disk pre jednotlivé inštancie, čím tvorí základ výpočtovej kapacity clustra.

Control + Compute node 1

Control a Compute node v OpenStack clustri sú základné typy uzlov, ktoré spolu zabezpečujú riadenie a prevádzku cloudového prostredia. Control node obsahuje centrálne služby ako API servery, plánovače (Scheduler), databázu, message broker a autentifikáciu, čím riadi orchestráciu, správu zdrojov a komunikáciu v rámci clustra. Compute node 1 poskytuje výpočtové kapacity pre spúšťanie virtuálnych strojov (VM) a zabezpečuje ich lokálnu správu pomocou komponentu Nova Compute, podľa inštrukcií z Control nodu.

Control + Compute node 2

Control a Compute node v OpenStack clustri sú základné typy uzlov, ktoré spolu zabezpečujú riadenie a prevádzku cloudového prostredia. Control node obsahuje centrálne služby ako API servery, plánovače (Scheduler), databázu, message broker a autentifikáciu, čím riadi orchestráciu, správu zdrojov a komunikáciu v rámci clustra. Compute node 2 poskytuje výpočtové kapacity pre spúšťanie virtuálnych strojov (VM) a zabezpečuje ich lokálnu správu pomocou komponentu Nova Compute, podľa inštrukcií z Control nodu.

Control + Compute node 3

Control a Compute node v OpenStack clustri sú základné typy uzlov, ktoré spolu zabezpečujú riadenie a prevádzku cloudového prostredia. Control node obsahuje centrálne služby ako API servery, plánovače (Scheduler), databázu, message broker a autentifikáciu, čím riadi orchestráciu, správu zdrojov a komunikáciu v rámci clustra. Compute node 3

poskytuje výpočtové kapacity pre spúšťanie virtuálnych strojov (VM) a zabezpečuje ich lokálnu správu pomocou komponentu Nova Compute, podľa inštrukcií z Control nodu.

HW Servers

HW serverová infraštruktúra je fyzický základ IT prostredia, zahŕňajúci výpočtové servery, úložiská, sieťové prvky, napájacie zdroje a podporné zariadenia, ktoré spoločne poskytujú potrebný výkon, dostupnosť a konektivitu pre prevádzku informačných systémov. Táto infraštruktúra tvorí platformu pre virtualizáciu, cloudové služby, databázy a aplikačné workloady v podnikových aj dátových centrách.

KVM

KVM (Kernel-based Virtual Machine) je hypervisor 1. typu, ktorý je integrovaný priamo do linuxového jadra a umožňuje bežať viaceré virtuálne stroje s plnou izoláciou na fyzickom serveri. Využíva hardvérovú virtualizáciu a poskytuje vysoký výkon, stabilitu a efektivitu, čím je vhodný pre produkčné a cloudové prostredia ako OpenStack.

Network

Predstavuje sieť/subsieť HW infraštruktúry. Sieť alebo podsieť HW infraštruktúry predstavuje fyzické a logické prepojenie medzi servermi, úložiskami, sieťovými zariadeniami a ďalšími komponentmi v rámci dátového centra. Slúži na zabezpečenie prenosu dát, segregáciu prevádzky a na riadenie komunikácie pomocou smerovačov, prepínačov, VLAN a bezpečnostných pravidiel.

OpenStack Cluster

Predstavuje OpenStack cluster, ktorý je distribuovaným cloudovým prostredím, ktoré pozostáva z viacerých fyzických alebo virtuálnych uzlov, spoločne prevádzkujúcich jednotlivé služby OpenStacku ako výpočtové (Nova), sieťové (Neutron), úložiskové (Cinder, Swift) a riadiace komponenty. Tento klaster umožňuje organizáciám budovať súkromný alebo hybridný cloud s podporou automatizovaného provisioningu, správy zdrojov a škálovateľnej viacnájomnej architektúry.

OpenStack network

Sieť a podsiete OpenStack clustra slúžia na logické a fyzické oddelenie rôznych typov komunikácie v rámci cloudovej infraštruktúry, pričom každá plní špecifickú úlohu. Corporate network zabezpečuje prepojenie OpenStack prostredia s podnikovou infraštruktúrou, OpenStack Tenant Data Network poskytuje sieťovú konektivitu pre virtuálne inštancie jednotlivých tenantov, a OpenStack Internal Admin / API Subnet je vyhradená pre internú komunikáciu medzi komponentmi clustra, vrátane API volaní, databázovej replikácie a správy služby.

Support PODs

Predstavuje PODy podporných služieb. PODy podporných služieb sú kontajnerové jednotky, ktoré zabezpečujú nefunkčné, infraštruktúrne alebo prevádzkové funkcie potrebné pre

chod aplikačného systému, ako sú monitoring, logovanie, autentifikácia či konfigurácia. Tieto služby bežia nezávisle od aplikačných PODov a podporujú stabilitu, bezpečnosť a správu celého prostredia.

System PODs

Predstavuje PODy systémových služieb. PODy systémových služieb sú základné kontajnerové jednotky, ktoré zabezpečujú kľúčové funkcionality Kubernetes clustra a jeho infraštruktúry, ako sú sieťová konektivita, DNS, plánovanie workloadov či riadenie prístupu. Typicky zahŕňajú komponenty ako CoreDNS, kube-proxy, metrics-server alebo ďalšie systémové operátory potrebné pre správnu funkciu prostredia. Tieto PODy sú kritické pre stabilitu a prevádzkyschopnosť platformy a bežia na úrovni systémových namespaces mimo aplikačnej vrstvy.

Virtual network

Predstavuje virtuálnu sieť/subsieť Hypervisora. Virtuálna sieť alebo podsieť hypervisora je logická sieťová vrstva, ktorá umožňuje komunikáciu medzi virtuálnymi strojmi navzájom, s hostiteľom alebo s externou sieťou. V rámci tejto siete hypervisor vytvára a spravuje virtuálne switche, bridge alebo NAT rozhrania, čím zabezpečuje flexibilné smerovanie, izoláciu a riadenie sieťovej prevádzky medzi VM a fyzickou infraštruktúrou.

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 FE Private. PODy FE Private sú izolované kontajnerové jednotky nasadenia frontendovej vrstvy systému, ktoré sú prevádzkované v privátnom prostredí zákazníka, napríklad on-premise alebo v privátnom cloude. Tieto PODy zabezpečujú bezpečné a oddelené sprístupnenie používateľského rozhrania, pričom sú integrované s lokálnou infraštruktúrou, autentifikáciou a sieťovými politikami zákazníka.

INNOSOC Public FE PODs

Predstavuje PODy FE Public. PODy FE Public sú kontajnerové jednotky nasadenia frontendovej vrstvy systému, ktoré sú prevádzkované v verejne dostupnom cloudovom prostredí a prístupné cez internet. Slúžia na poskytovanie používateľského rozhrania pre viacerých klientov (multitenancy), pričom využívajú centralizovanú správu, zabezpečený prístup a škálovateľnú cloudovú infraštruktúru.

Compute

Rola a služba Compute nodu v OpenStack clustri spočíva v poskytovaní výpočtových zdrojov pre spúšťanie virtuálnych inštancií prostredníctvom komponentu Nova Compute. Tento uzol je zodpovedný za správu životného cyklu VM, alokáciu CPU, pamäte a diskového priestoru, a komunikuje s riadiacimi službami na základe požiadaviek používateľov alebo orchestrace.

Compute apps

Predstavuje súbor Compute aplikácií. Súbor Compute aplikácií predstavuje skupinu softvérových komponentov, ktoré zabezpečujú výpočtové operácie a správu výpočtových zdrojov v rámci cloudovej alebo virtualizovanej infraštruktúry. Zahŕňa aplikácie zodpovedné za nasadzovanie, správu, škálovanie a monitorovanie virtuálnych strojov alebo kontajnerov, pričom úzko spolupracujú so sieťovou, úložiskovou a orchestračnou vrstvou systému.

Control apps

Súbor aplikácií pre Control node predstavuje kľúčové softvérové komponenty, ktoré riadia a koordinujú činnosť celého clustra v prostredí OpenStack alebo Kubernetes. Tento súbor zahŕňa služby ako API servery, plánovače, manažéry stavov (controller managers), databázové služby, autentifikačné mechanizmy a ďalšie systémové aplikácie potrebné na orchestráciu, monitorovanie a správu životného cyklu workloadov a infraštruktúry.

Compute

Rola a služba Compute nodu v OpenStack clustri spočíva v poskytovaní výpočtových zdrojov pre spúšťanie virtuálnych inštancií prostredníctvom komponentu Nova Compute. Tento uzol je zodpovedný za správu životného cyklu VM, alokáciu CPU, pamäte a diskového priestoru, a komunikuje s riadiacimi službami na základe požiadaviek používateľov alebo orchestrace.

Compute apps

Predstavuje súbor Compute aplikácií. Súbor Compute aplikácií predstavuje skupinu softvérových komponentov, ktoré zabezpečujú výpočtové operácie a správu výpočtových zdrojov v rámci cloudovej alebo virtualizovanej infraštruktúry. Zahŕňa aplikácie zodpovedné za nasadzovanie, správu, škálovanie a monitorovanie virtuálnych strojov alebo kontajnerov, pričom úzko spolupracujú so sieťovou, úložiskovou a orchestračnou vrstvou systému.

Compute

Rola a služba Compute nodu v OpenStack clustri spočíva v poskytovaní výpočtových zdrojov pre spúšťanie virtuálnych inštancií prostredníctvom komponentu Nova Compute. Tento uzol je zodpovedný za správu životného cyklu VM, alokáciu CPU, pamäte a diskového priestoru, a komunikuje s riadiacimi službami na základe požiadaviek používateľov alebo orchestrace.

Compute apps

Predstavuje súbor Compute aplikácií. Súbor Compute aplikácií predstavuje skupinu softvérových komponentov, ktoré zabezpečujú výpočtové operácie a správu výpočtových zdrojov v rámci cloudovej alebo virtualizovanej infraštruktúry. Zahŕňa aplikácie zodpovedné za nasadzovanie, správu, škálovanie a monitorovanie virtuálnych strojov alebo kontajnerov, pričom úzko spolupracujú so sieťovou, úložiskovou a orchestračnou vrstvou systému.

Control apps

Súbor aplikácií pre Control node predstavuje kľúčové softvérové komponenty, ktoré riadia a koordinujú činnosť celého clustra v prostredí OpenStack alebo Kubernetes. Tento súbor zahŕňa služby ako API servery, plánovače, manažéry stavov (controller managers), databázové služby, autentifikačné mechanizmy a ďalšie systémové aplikácie potrebné na orchestráciu, monitorovanie a správu životného cyklu workloadov a infraštruktúry.

Compute

Rola a služba Compute nodu v OpenStack clustri spočíva v poskytovaní výpočtových zdrojov pre spúšťanie virtuálnych inštancií prostredníctvom komponentu Nova Compute. Tento uzol je zodpovedný za správu životného cyklu VM, alokáciu CPU, pamäte a diskového priestoru, a komunikuje s riadiacimi službami na základe požiadaviek používateľov alebo orchestrace.

Compute apps

Predstavuje súbor Compute aplikácií. Súbor Compute aplikácií predstavuje skupinu softvérových komponentov, ktoré zabezpečujú výpočtové operácie a správu výpočtových zdrojov v rámci cloudovej alebo virtualizovanej infraštruktúry. Zahŕňa aplikácie zodpovedné za nasadzovanie, správu, škálovanie a monitorovanie virtuálnych strojov alebo kontajnerov, pričom úzko spolupracujú so sieťovou, úložiskovou a orchestračnou vrstvou systému.

Control apps

Súbor aplikácií pre Control node predstavuje kľúčové softvérové komponenty, ktoré riadia a koordinujú činnosť celého clustra v prostredí OpenStack alebo Kubernetes. Tento súbor zahŕňa služby ako API servery, plánovače, manažéry stavov (controller managers), databázové služby, autentifikačné mechanizmy a ďalšie systémové aplikácie potrebné na orchestráciu, monitorovanie a správu životného cyklu workloadov a infraštruktúry.

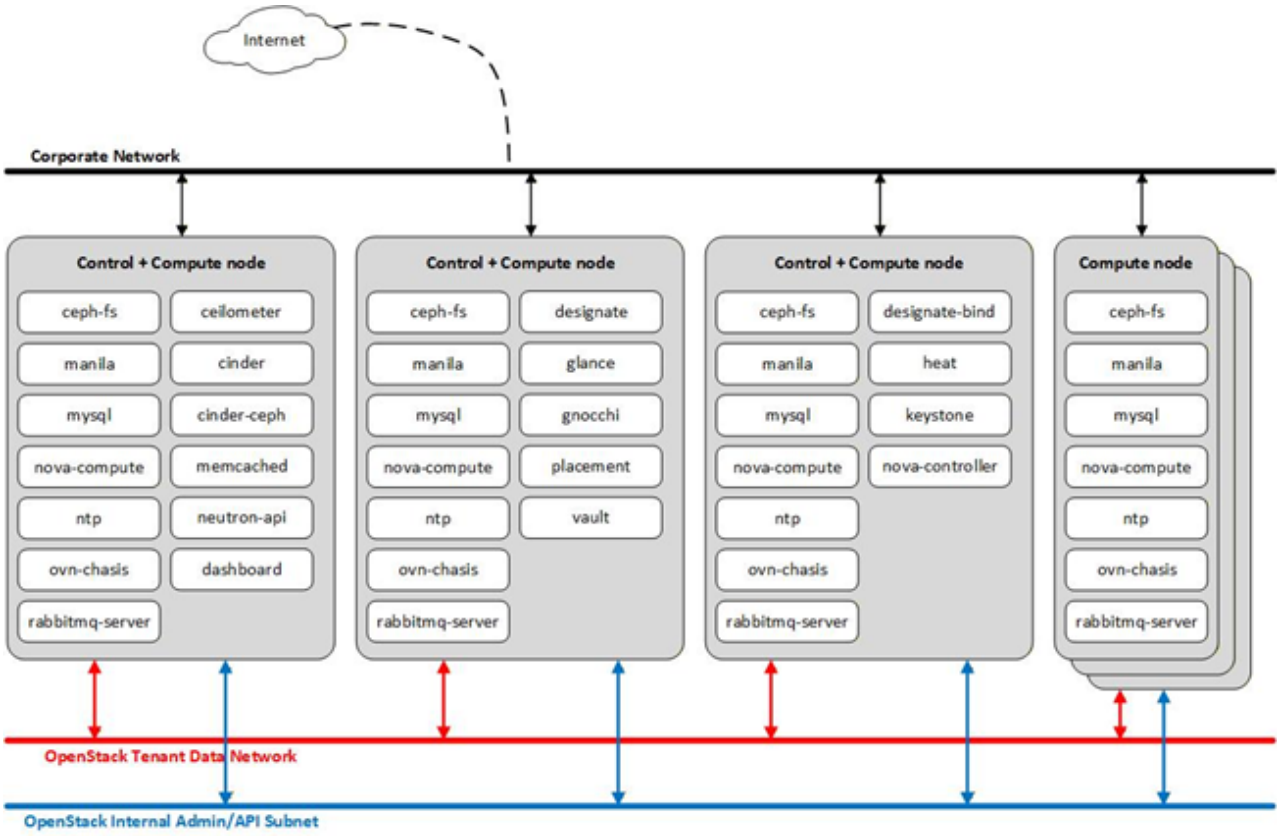
Compute

Rola a služba Compute nodu v OpenStack clustri spočíva v poskytovaní výpočtových zdrojov pre spúšťanie virtuálnych inštancií prostredníctvom komponentu Nova Compute. Tento uzol je zodpovedný za správu životného cyklu VM, alokáciu CPU, pamäte a diskového priestoru, a komunikuje s riadiacimi službami na základe požiadaviek používateľov alebo orchestrace.

Compute apps

Predstavuje súbor Compute aplikácií. Súbor Compute aplikácií predstavuje skupinu softvérových komponentov, ktoré zabezpečujú výpočtové operácie a správu výpočtových zdrojov v rámci cloudovej alebo virtualizovanej infraštruktúry. Zahŕňa aplikácie zodpovedné za nasadzovanie, správu, škálovanie a monitorovanie virtuálnych strojov alebo kontajnerov, pričom úzko spolupracujú so sieťovou, úložiskovou a orchestračnou vrstvou systému.

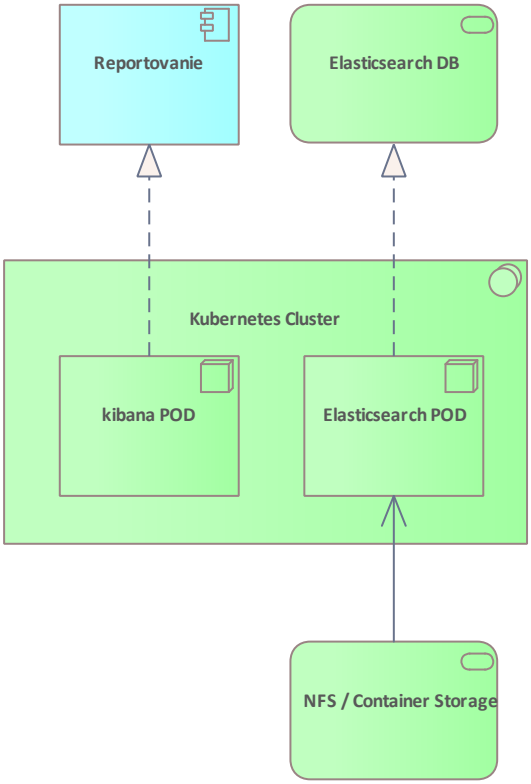
1.1.7. Technology Viewpoint OpenStack External



Obrázok1.png

Obrázok 17: Technology Viewpoint OpenStack External

1.1.8. Technology Viewpoint Reportovanie



Obrázok 18: 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

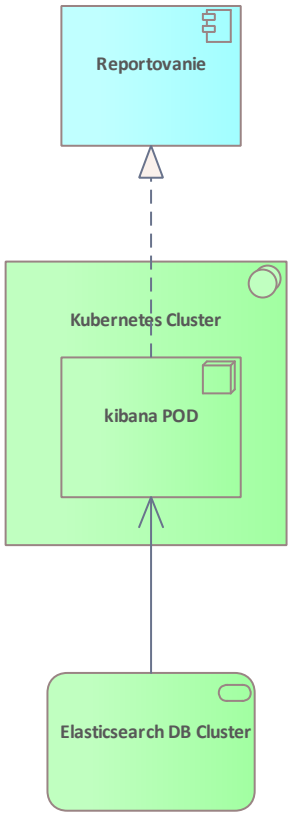
Technologická služba NoSQL Elasticsearch databázy je distribuovaný systém na fulltextové vyhľadávanie, indexovanie a analýzu dát, ktorý funguje na báze dokumentovo orientovaného modelu. Umožňuje efektívne spracovanie veľkého množstva nestruktúrovaných alebo semištruktúrovaných údajov v reálnom čase, pričom je optimalizovaný pre horizontálne škálovanie, vysokú dostupnosť a výkonnú analytiku nad logmi, metrikami alebo aplikačnými dátami.

Elasticsearch POD

Predstavuje POD Elasticsearch pre NoSQL databázu, ktorá je kontajnerovou jednotkou nasadenou v Kubernetes clustri, ktorá hostuje Elasticsearch node ako súčasť distribuovanej, dokumentovo orientovanej NoSQL databázy. Tento POD zabezpečuje indexovanie, vyhľadávanie a ukladanie nestruktúrovaných alebo semištruktúrovaných dát, pričom je navrhnutý pre horizontálne škálovanie, vysokú dostupnosť a rýchlu odozvu pri práci s veľkým objemom dát.

Kibana POD

POD Kibana pre reportovanie je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje webovú aplikáciu Kibana určenú na vizualizáciu a analýzu dát uložených v Elasticsearch. Tento POD poskytuje grafické používateľské rozhranie na tvorbu dashboardov, reportov a interaktívnych prehľadov, čím umožňuje používateľom efektívne monitorovať, analyzovať a interpretovať prevádzkové a logovacie dáta v reálnom čase.



Obrázok 19: 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.

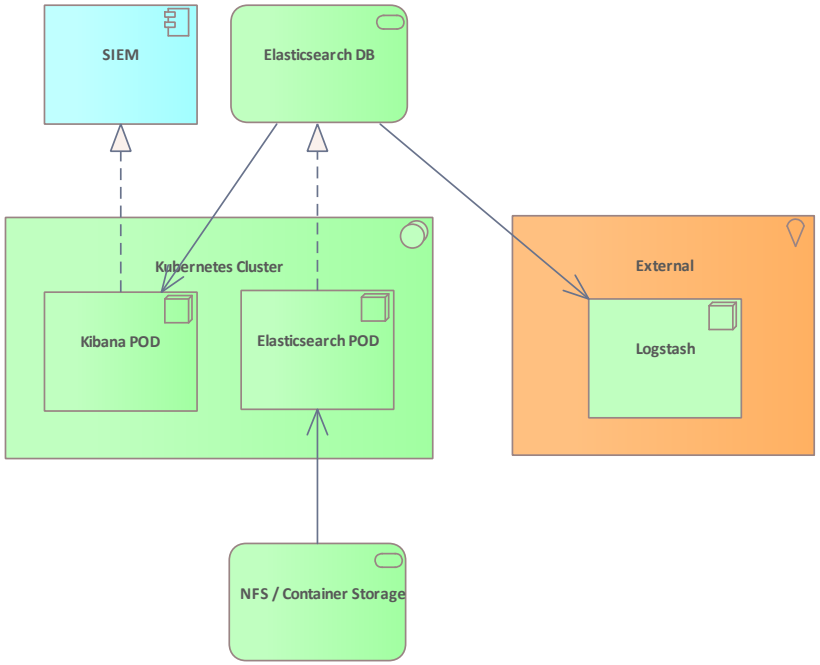
Elasticsearch DB Cluster

Technologická služba NoSQL Elasticsearch databázy vo forme clustra predstavuje viacuzlové distribuované riešenie, kde jednotlivé uzly (nodes) spolupracujú na uložení, indexovaní a vyhľadávaní dokumentovo orientovaných dát. Každý uzol v klastri plní špecifickú úlohu (napr. master, data alebo ingest node), čo umožňuje horizontálne škálovanie, vysokú dostupnosť a odolnosť voči výpadkom, pričom systém ako celok zabezpečuje spracovanie veľkého objemu dát v reálnom čase.

Kibana POD

POD Kibana pre reportovanie je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje webovú aplikáciu Kibana určenú na vizualizáciu a analýzu dát uložených v Elasticsearch. Tento POD poskytuje grafické používateľské rozhranie na tvorbu dashboardov, reportov a interaktívnych prehľadov, čím umožňuje používateľom efektívne monitorovať, analyzovať a interpretovať prevádzkové a logovacie dáta v reálnom čase.

1.1.9. Technology Viewpoint SIEM



Obrázok 20: 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

Technologická služba NoSQL Elasticsearch databázy je výkonný a distribuovaný systém určený na indexovanie, vyhľadávanie a analýzu dát v reálnom čase, založený na dokumentovo orientovanom modeli. Využíva schému JSON dokumentov, podporuje horizontálne škálovanie, vysokú dostupnosť a je optimalizovaný na spracovanie veľkých objemov nestruktúrovaných alebo semištruktúrovaných údajov, ako sú logy, metriky alebo aplikačné záznamy.

Elasticsearch POD

POD Elasticsearch pre NoSQL databázu je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje Elasticsearch node ako súčasť distribuovaného clustra NoSQL databázy. Tento POD zabezpečuje indexovanie, vyhľadávanie a ukladanie dokumentovo orientovaných dát, pričom umožňuje horizontálne škálovanie, vysokú dostupnosť a efektívne spracovanie veľkých objemov nestruktúrovaných informácií v reálnom čase.

External

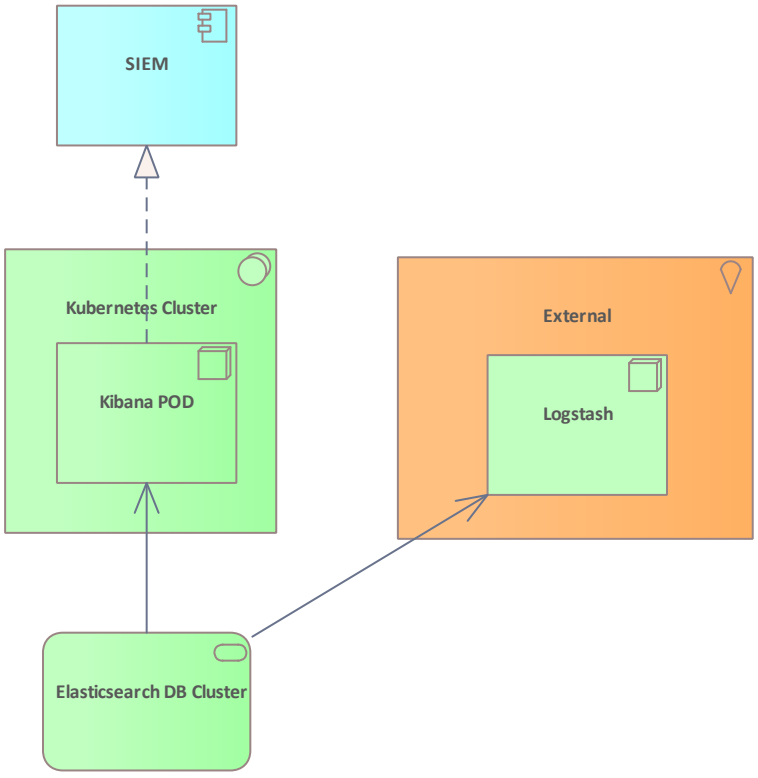
Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

Kibana POD

POD Kibana pre SIEM je kontajnerová inštancia nasadená v Kubernetes clustri, ktorá poskytuje grafické používateľské rozhranie pre vizualizáciu a analýzu bezpečnostných údajov zhromaždených v Elasticsearch. Slúži ako frontend komponent pre SIEM (Security Information and Event Management) riešenie, umožňujúci interaktívne monitorovanie, koreláciu udalostí, tvorbu dashboardov a detekciu bezpečnostných incidentov v reálnom čase.

Logstash

Inštancia Logstash pre spracovanie logov je dátový procesor nasadený ako samostatná služba alebo kontajner, ktorý zhromažďuje, transformuje a smeruje logovacie dáta z rôznych zdrojov. V rámci pipeline zabezpečuje parsovanie, obohatenie a filtrovanie údajov, ktoré následne zapisuje do Elasticsearch, čím umožňuje centralizované, efektívne a štruktúrované ukladanie logov pre ďalšiu analýzu.



Obrázok 21: 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

Technologická služba NoSQL Elasticsearch databázy vo forme clustra predstavuje viacuzlové distribuované riešenie, kde jednotlivé uzly (nodes) spolupracujú na uložení, indexovaní a vyhľadávaní dokumentovo orientovaných dát. Každý uzol v klastri plní špecifickú úlohu (napr. master, data alebo ingest node), čo umožňuje horizontálne škálovanie, vysokú dostupnosť a odolnosť voči výpadkom, pričom systém ako celok zabezpečuje spracovanie veľkého objemu dát v reálnom čase.

External

Predstavuje fyzické umiestnenie u klienta a teda mimo prostredia INNOSOC.

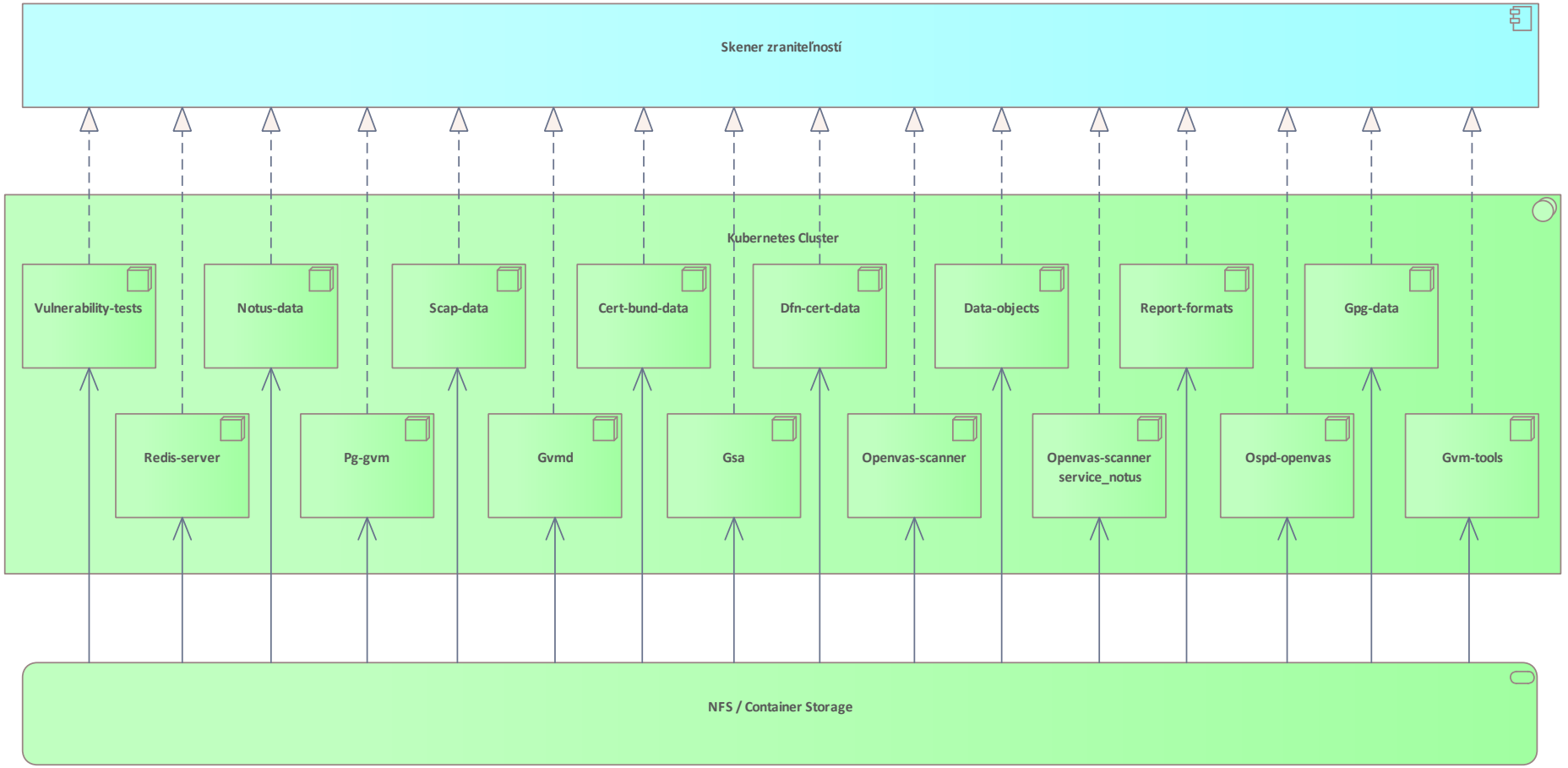
Kibana POD

POD Kibana pre SIEM je kontajnerová inštancia nasadená v Kubernetes clustri, ktorá poskytuje grafické používateľské rozhranie pre vizualizáciu a analýzu bezpečnostných údajov zhromaždených v Elasticsearch. Slúži ako frontend komponent pre SIEM (Security Information and Event Management) riešenie, umožňujúci interaktívne monitorovanie, koreláciu udalostí, tvorbu dashboardov a detekciu bezpečnostných incidentov v reálnom čase.

Logstash

Inštancia Logstash pre spracovanie logov je dátový procesor nasadený ako samostatná služba alebo kontajner, ktorý zhromažďuje, transformuje a smeruje logovacie dáta z rôznych zdrojov. V rámci pipeline zabezpečuje parsovanie, obohatenie a filtrovanie údajov, ktoré následne zapisuje do Elasticsearch, čím umožňuje centralizované, efektívne a štruktúrované ukladanie logov pre ďalšiu analýzu.

1.1.10. Technology Viewpoint Skener zraniteľností



Obrázok 22: 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

POD cert-bund-data je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá poskytuje aktualizované bezpečnostné informácie a varovania z oficiálnych zdrojov. Tento POD distribuuje dáta o hrozbách, zraniteľnostiach a odporúčaniach, ktoré sú využívané bezpečnostnými nástrojmi na zlepšenie detekcie a reakcie na aktuálne kybernetické riziká.

Data-objects

POD data-objects je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá slúži na uchovávanie a poskytovanie štruktúrovaných dátových objektov využívaných v rámci bezpečnostného ekosystému, ako sú definície zraniteľností, konfigurácií alebo analytických pravidiel. Tento POD zabezpečuje centralizovaný prístup k referenčným dátam pre ostatné komponenty systému, čím podporuje konzistenciu a aktuálnosť informácií v procesoch detekcie a hodnotenia bezpečnostných hrozieb.

Dfn-cert-data

POD dfn-cert-data je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá slúži na distribúciu bezpečnostných informácií a varovaní. Tento POD poskytuje aktuálne dáta o kybernetických hrozbách, zraniteľnostiach a odporúčaniach, ktoré sú využívané bezpečnostnými nástrojmi na zlepšenie detekčných schopností a rýchlejšiu reakciu na incidenty.

Gpg-data

POD gpg-data je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá poskytuje GPG (GNU Privacy Guard) kľúče a súvisiace dáta potrebné na overovanie podpisov aktualizačných balíkov a bezpečnostných dát v ekosystéme Greenbone Vulnerability Management (GVM). Tento POD zabezpečuje integritu a dôveryhodnosť prenášaných bezpečnostných informácií, ako sú zraniteľnostné databázy, reportovacie formáty či konfiguračné súbory.

Gsa

POD gsa je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje komponent Greenbone Security Assistant (GSA) – webové používateľské rozhranie pre prácu s Greenbone Vulnerability Management (GVM) systémom. Tento POD poskytuje prístup k funkciám zraniteľnostného skenovania cez prehliadač, vrátane správy používateľov, plánovania skenov, zobrazenia výsledkov a konfigurácie celého bezpečnostného prostredia.

Gvmd

POD gvmd je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje komponent Greenbone Vulnerability Management Daemon (gvmd) – centrálnu riadiacu službu pre nástroj GVM/OpenVAS. Tento POD zabezpečuje správu používateľov, plánovanie a spúšťanie skenov, spracovanie výsledkov a komunikáciu s databázou a ďalšími službami, čím tvorí jadro zraniteľnostného skenovacieho systému.

Gvm-tools

POD gvm-tools je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá obsahuje nástroje GVM-Tools – klientské utility pre automatizovanú správu a interakciu so systémom Greenbone Vulnerability Management (GVM). Tento POD umožňuje vykonávanie príkazov, skriptovanie úloh, plánovanie skenov a extrakciu výsledkov prostredníctvom XML alebo GMP (Greenbone Management Protocol), čím podporuje integráciu GVM do väčších bezpečnostných a orchestračných workflowov.

Notus-data

POD notus-data je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá poskytuje dáta a aktualizácie pre detekčné mechanizmy zraniteľností, najmä v kontexte nástroja Greenbone/OpenVAS. Tento POD distribuuje štruktúrované informácie o známych zraniteľnostiach vo formáte JSON, ktoré sú využívané inými komponentmi na precízne a aktuálne testovanie systémov na bezpečnostné slabiny.

Openvas-scanner

POD openvas-scanner je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje komponent OpenVAS (Open Vulnerability Assessment System) – výkonný skenovací engine pre zraniteľnostné testovanie. Tento POD vykonáva aktívne skenovanie cieľových systémov, analyzuje ich bezpečnostné slabiny na základe aktualizovaných podpisov a komunikuje s centrálnym gvmd daemonom na zaznamenanie a spracovanie výsledkov skenov.

Openvas-scanner service_notus

Predstavuje POD openvas-scanner service_notus. POD openvas-scanner service_notus je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá rozširuje funkčnosť OpenVAS skenovacieho enginu o integráciu so službou Notus. Táto služba umožňuje bezagentové a rýchle testovanie zraniteľností na základe dát z Notus databázy bez potreby priameho sieťového prístupu ku všetkým cieľom. POD kombinuje výkonnosť aktívneho skenovania s dynamickou detekciou známych zraniteľností, čím zvyšuje presnosť a efektivitu bezpečnostných analýz.notus.

Ospd-openvas

POD ospd-openvas je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje komponent OSPd (Open Scanner Protocol daemon) pre integráciu OpenVAS skenera s riadiacim systémom gvmd v rámci Greenbone Vulnerability Management. Tento POD zabezpečuje štandardizovanú komunikáciu medzi gvmd a OpenVAS, spracováva požiadavky na skenovanie, riadi ich vykonanie a odosiela výsledky späť na centrálne spracovanie, čím umožňuje škálovateľnú a efektívnu orchestráciu zraniteľnostných skenov.

Pg-gvm

POD pg-gvm je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje PostgreSQL databázu prispôsobenú pre Greenbone Vulnerability Management (GVM). Tento POD slúži ako centrálne úložisko pre všetky dáta o zraniteľnostiach, skenoch, výsledkoch a konfiguráciách, ktoré sú generované a spravované nástrojmi GVM/OpenVAS v rámci bezpečnostného ekosystému.

Redis-server

POD redis-server je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje inštanciu Redis – vysoko výkonnú in-memory NoSQL databázu. Tento POD poskytuje dočasné alebo trvalo uložené kľúč-hodnota dáta pre rýchly prístup, caching, frontovanie správ alebo zdieľanie stavov medzi aplikáciami v rámci distribuovaného systému.

Report-formats

Predstavuje POD report-formats. POD report-formats je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá poskytuje a spravuje šablóny a formáty výstupných reportov v rámci systému Greenbone Vulnerability Management (GVM). Tento POD umožňuje generovanie výsledkov skenov v rôznych štandardizovaných formátoch, čím podporuje

automatizované reportovanie, archiváciu a zdieľanie zistení s rôznymi zainteresovanými stranami.

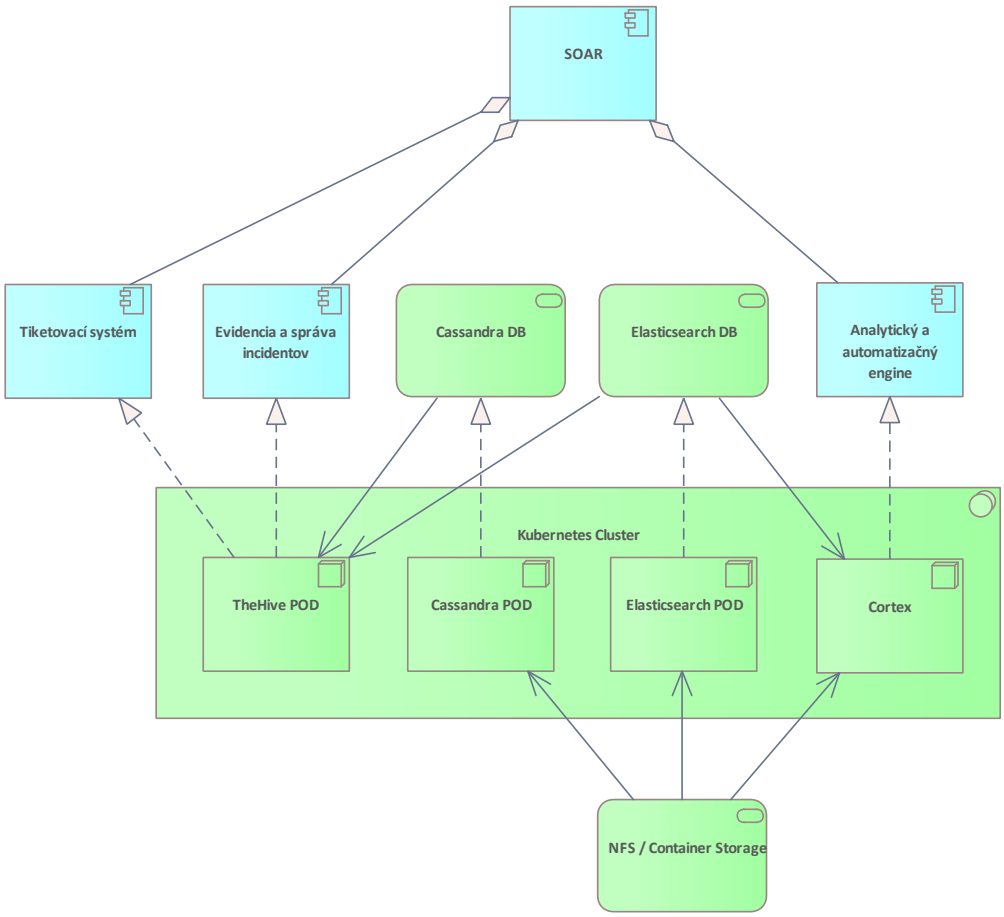
Scap-data

POD scap-data je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá poskytuje štruktúrované bezpečnostné dátové balíky vo formáte SCAP (Security Content Automation Protocol). Tieto dáta obsahujú štandardizované informácie o bezpečnostných konfiguráciách, zraniteľnostiach a politikách, ktoré sú následne využívané nástrojmi na compliance audit, zhodu s bezpečnostnými normami a automatizované hodnotenie systémov.

Vulnerability-tests

POD vulnerability-tests je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá vykonáva automatizované testy zraniteľností voči cieľovým systémom, službám alebo kontajnerom. Tento POD využíva bezpečnostné skenery alebo nástroje na analýzu a slúži na detekciu známych slabín, hodnotenie rizík a generovanie výstupov pre ďalšie spracovanie v rámci bezpečnostného cyklu.

1.1.11. Technology Viewpoint SOAR



Obrázok 23: 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

Analytický a automatizačný engine je softvérová komponenta alebo služba, ktorá kombinuje analýzu dát a automatizáciu rozhodovacích alebo operačných procesov s cieľom zvýšiť efektivitu, presnosť a rýchlosť reakcie systému. V kontexte kybernetickej bezpečnosti alebo IT prevádzky tento engine spracúva vstupné dáta (napr. logy, udalosti, metriky), aplikuje analytické pravidlá alebo modely (napr. detekciu anomálií, koreláciu), a následne vykonáva automatizované reakcie alebo akcie prostredníctvom integrovaných nástrojov a API rozhraní.

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

Technologická služba NoSQL Cassandra databázy je distribuovaný databázový systém navrhnutý na ukladanie veľkého objemu štruktúrovaných dát s dôrazom na vysokú dostupnosť, škálovateľnosť a odolnosť voči výpadkom. Využíva masterless architektúru s replikáciou dát naprieč uzlami, čo umožňuje rýchly zápis aj čítanie v geograficky distribuovanom prostredí bez výpadkov jedného bodu (single point of failure).

Elasticsearch DB

Technologická služba NoSQL Elasticsearch databázy je výkonný a distribuovaný systém určený na indexovanie, vyhľadávanie a analýzu dát v reálnom čase, založený na dokumentovo orientovanom modeli. Využíva schému JSON dokumentov, podporuje horizontálne škálovanie, vysokú dostupnosť a je optimalizovaný na spracovanie veľkých objemov nestruktúrovaných alebo semištruktúrovaných údajov, ako sú logy, metriky alebo aplikačné záznamy.

Cassandra POD

POD Apache Cassandra pre NoSQL databázu je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje Cassandra node ako súčasť distribuovaného NoSQL clustra. Tento POD zabezpečuje škálovateľné, vysoko dostupné a odolné ukladanie štruktúrovaných dát s dôrazom na rýchly zápis a čítanie v prostredí s veľkým objemom údajov a vysokou redundanciou.

Elasticsearch POD

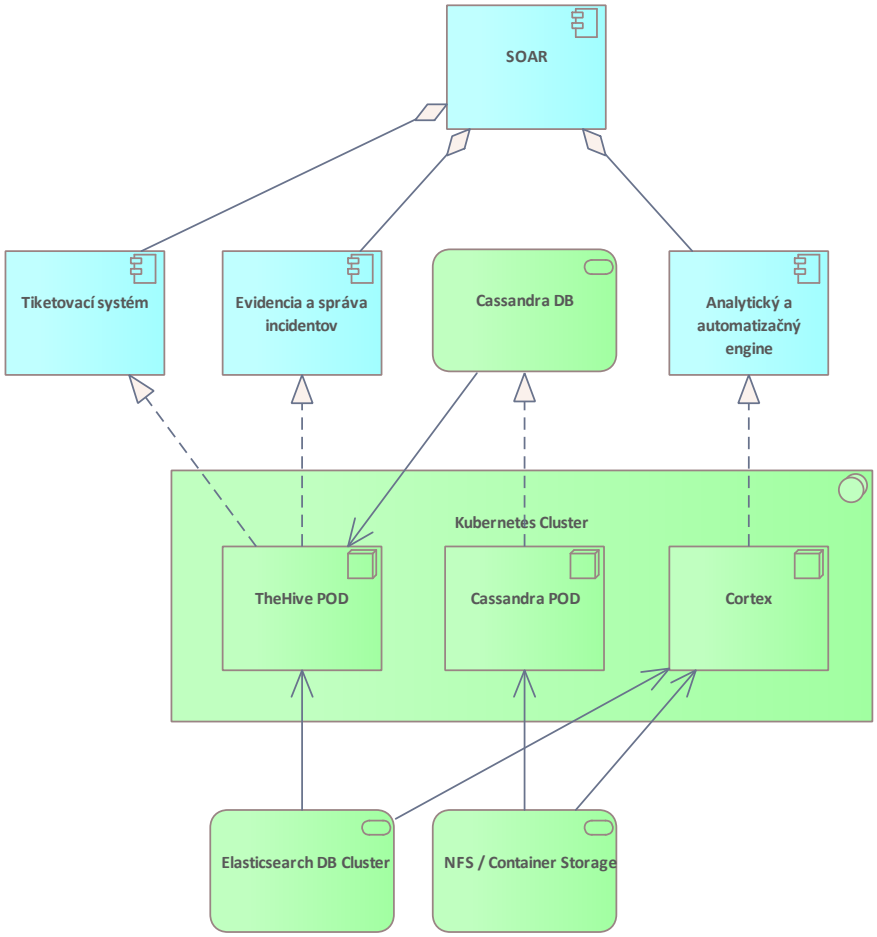
POD Elasticsearch pre NoSQL databázu je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje Elasticsearch node ako súčasť distribuovaného clustra NoSQL databázy. Tento POD zabezpečuje indexovanie, vyhľadávanie a ukladanie dokumentovo orientovaných dát, pričom umožňuje horizontálne škálovanie, vysokú dostupnosť a efektívne spracovanie veľkých objemov nestruktúrovaných informácií v reálnom čase.

TheHive POD

POD TheHive pre inventarizáciu aktív je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje aplikáciu TheHive – open-source platformu na správu bezpečnostných incidentov a digitálnych aktív. Tento POD umožňuje centralizované zhromažďovanie, kategorizáciu a analýzu aktív, ich väzbu na incidenty a podporu kolaboratívneho vyšetrovania v rámci tímov kybernetickej bezpečnosti.

Cortex

Predstavuje POD Cortex pre SOAR. POD Cortex pre SOAR je kontajnerová jednotka nasadená v Kubernetes prostredí, ktorá hostuje službu Cortex ako súčasť SOAR riešenia. Tento POD umožňuje automatizované spúšťanie analytických modulov (analyzers) a reakčných akcií (responders) na základe bezpečnostných incidentov, čím zefektívňuje detekciu hrozieb, reakciu na incidenty a integráciu s ďalšími bezpečnostnými nástrojmi.



Obrázok 24: 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:

Analytický a automatizačný engine

Analytický a automatizačný engine je softvérová komponenta alebo služba, ktorá kombinuje analýzu dát a automatizáciu rozhodovacích alebo operačných procesov s cieľom zvýšiť efektivitu, presnosť a rýchlosť reakcie systému. V kontexte kybernetickej bezpečnosti alebo IT prevádzky tento engine spracúva vstupné dáta (napr. logy, udalosti, metriky), aplikuje analytické pravidlá alebo modely (napr. detekciu anomálií, koreláciu), a následne vykonáva automatizované reakcie alebo akcie prostredníctvom integrovaných nástrojov a API rozhraní.

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

Technologická služba NoSQL Cassandra databázy je distribuovaný databázový systém navrhnutý na ukladanie veľkého objemu štruktúrovaných dát s dôrazom na vysokú dostupnosť, škálovateľnosť a odolnosť voči výpadkom. Využíva masterless architektúru s replikáciou dát naprieč uzlami, čo umožňuje rýchly zápis aj čítanie v geograficky distribuovanom prostredí bez výpadkov jedného bodu (single point of failure).

Elasticsearch DB Cluster

Technologická služba NoSQL Elasticsearch databázy vo forme clustra predstavuje viacuzlové distribuované riešenie, kde jednotlivé uzly (nodes) spolupracujú na uložení, indexovaní a vyhľadávaní dokumentovo orientovaných dát. Každý uzol v klastri plní špecifickú úlohu (napr. master, data alebo ingest node), čo umožňuje horizontálne škálovanie, vysokú dostupnosť a odolnosť voči výpadkom, pričom systém ako celok zabezpečuje spracovanie veľkého objemu dát v reálnom čase.

Cassandra POD

POD Apache Cassandra pre NoSQL databázu je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje Cassandra node ako súčasť distribuovaného NoSQL clustra. Tento POD zabezpečuje škálovateľné, vysoko dostupné a odolné ukladanie štruktúrovaných dát s dôrazom na rýchly zápis a čítanie v prostredí s veľkým objemom údajov a vysokou redundanciou.

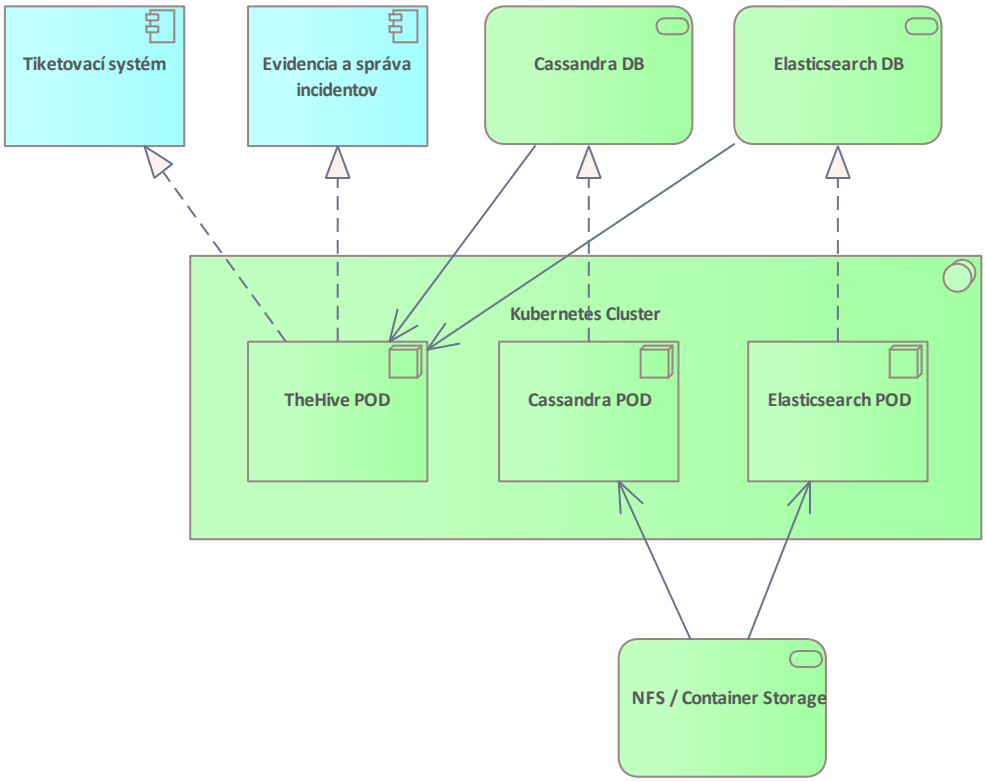
TheHive POD

POD TheHive pre inventarizáciu aktív je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje aplikáciu TheHive – open-source platformu na správu bezpečnostných incidentov a digitálnych aktív. Tento POD umožňuje centralizované zhromažďovanie, kategorizáciu a analýzu aktív, ich väzbu na incidenty a podporu kolaboratívneho vyšetrovania v rámci tímov kybernetickej bezpečnosti.

Cortex

Predstavuje POD Cortex pre SOAR. POD Cortex pre SOAR je kontajnerová jednotka nasadená v Kubernetes prostredí, ktorá hostuje službu Cortex ako súčasť SOAR riešenia. Tento POD umožňuje automatizované spúšťanie analytických modulov (analyzers) a reakčných akcií (responders) na základe bezpečnostných incidentov, čím zefektívňuje detekciu hrozieb, reakciu na incidenty a integráciu s ďalšími bezpečnostnými nástrojmi.

1.1.12. Technology Viewpoint Tiketovací systém / Evidencia a správa incidentov



Obrázok 25: 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

Technologická služba NoSQL Cassandra databázy je distribuovaný databázový systém navrhnutý na ukladanie veľkého objemu štruktúrovaných dát s dôrazom na vysokú dostupnosť, škálovateľnosť a odolnosť voči výpadkom. Využíva masterless architektúru s replikáciou dát naprieč uzlami, čo umožňuje rýchly zápis aj čítanie v geograficky distribuovanom prostredí bez výpadkov jedného bodu (single point of failure).

Elasticsearch DB

Technologická služba NoSQL Elasticsearch databázy je výkonný a distribuovaný systém určený na indexovanie, vyhľadávanie a analýzu dát v reálnom čase, založený na dokumentovo orientovanom modeli. Využíva schému JSON dokumentov, podporuje horizontálne škálovanie, vysokú dostupnosť a je optimalizovaný na spracovanie veľkých objemov nestruktúrovaných alebo semištruktúrovaných údajov, ako sú logy, metriky alebo aplikačné záznamy.

Cassandra POD

POD Apache Cassandra pre NoSQL databázu je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje Cassandra node ako súčasť distribuovaného NoSQL clustra. Tento POD zabezpečuje škálovateľné, vysoko dostupné a odolné ukladanie štruktúrovaných dát s dôrazom na rýchly zápis a čítanie v prostredí s veľkým objemom údajov

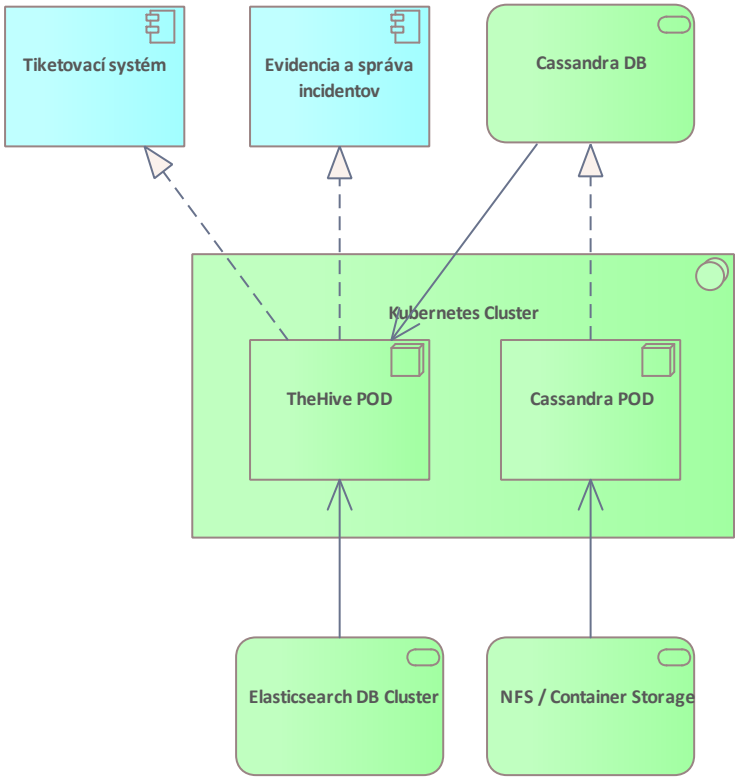
a vysokou redundanciou.

Elasticsearch POD

POD Elasticsearch pre NoSQL databázu je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje Elasticsearch node ako súčasť distribuovaného clustra NoSQL databázy. Tento POD zabezpečuje indexovanie, vyhľadávanie a ukladanie dokumentovo orientovaných dát, pričom umožňuje horizontálne škálovanie, vysokú dostupnosť a efektívne spracovanie veľkých objemov nestruktúrovaných informácií v reálnom čase.

TheHive POD

POD TheHive pre inventarizáciu aktív je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje aplikáciu TheHive – open-source platformu na správu bezpečnostných incidentov a digitálnych aktív. Tento POD umožňuje centralizované zhromažďovanie, kategorizáciu a analýzu aktív, ich väzbu na incidenty a podporu kolaboratívneho vyšetrovania v rámci tímov kybernetickej bezpečnosti.



Obrázok 26: 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

Technologická služba NoSQL Cassandra databázy je distribuovaný databázový systém navrhnutý na ukladanie veľkého objemu štruktúrovaných dát s dôrazom na vysokú dostupnosť, škálovateľnosť a odolnosť voči výpadkom. Využíva masterless architektúru s replikáciou dát

naprieč uzlami, čo umožňuje rýchly zápis aj čítanie v geograficky distribuovanom prostredí bez výpadkov jedného bodu (single point of failure).

Elasticsearch DB Cluster

Technologická služba NoSQL Elasticsearch databázy vo forme clustra predstavuje viacuzlové distribuované riešenie, kde jednotlivé uzly (nodes) spolupracujú na uložení, indexovaní a vyhľadávaní dokumentovo orientovaných dát. Každý uzol v klastri plní špecifickú úlohu (napr. master, data alebo ingest node), čo umožňuje horizontálne škálovanie, vysokú dostupnosť a odolnosť voči výpadkom, pričom systém ako celok zabezpečuje spracovanie veľkého objemu dát v reálnom čase.

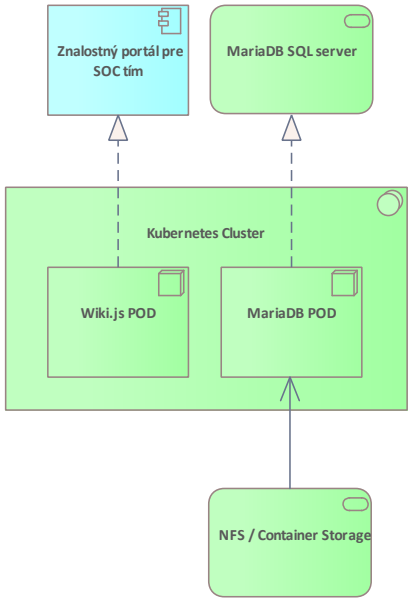
Cassandra POD

POD Apache Cassandra pre NoSQL databázu je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje Cassandra node ako súčasť distribuovaného NoSQL clustra. Tento POD zabezpečuje škálovateľné, vysoko dostupné a odolné ukladanie štruktúrovaných dát s dôrazom na rýchly zápis a čítanie v prostredí s veľkým objemom údajov a vysokou redundanciou.

TheHive POD

POD TheHive pre inventarizáciu aktív je kontajnerová inštancia nasadená v Kubernetes prostredí, ktorá hostuje aplikáciu TheHive – open-source platformu na správu bezpečnostných incidentov a digitálnych aktív. Tento POD umožňuje centralizované zhromažďovanie, kategorizáciu a analýzu aktív, ich väzbu na incidenty a podporu kolaboratívneho vyšetrovania v rámci tímov kybernetickej bezpečnosti.

1.1.13. Technology Viewpoint Znalostný portál pre SOC tím



Obrázok 27: 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

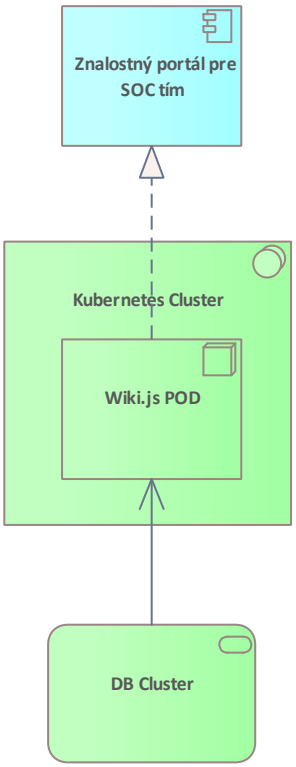
Technologická služba relačnej databázy MariaDB je výkonný a škálovateľný relačný databázový systém postavený na architektúre SQL, ktorý slúži na trvalé ukladanie, správu a dotazovanie štruktúrovaných dát pomocou relačných tabuliek. MariaDB podporuje transakčnosť, referenčnú integritu, replikáciu a vysokú dostupnosť, čím je vhodná pre nasadenie v kritických podnikových aplikáciách, kde sú dôležité výkon, spoľahlivosť a bezpečnosť spracovania údajov.

MariaDB POD

POD MariaDB pre relačnú SQL databázu je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje databázový server MariaDB – výkonný open-source relačný databázový systém kompatibilný s MySQL. Tento POD poskytuje trvalo uložené, štruktúrované dáta pre aplikácie alebo služby, podporuje transakcie, integritu údajov a umožňuje horizontálne alebo vertikálne škálovanie v rámci cloudovej infraštruktúry.

Wiki.js POD

POD Wiki.js pre Znalostný portál pre SOC tím je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje aplikáciu Wiki.js – moderný a výkonný systém na správu dokumentácie a znalostí. Tento POD slúži ako centrálny znalostný portál pre tím kybernetickej bezpečnosti (SOC), kde sa ukladajú, spravujú a zdieľajú informácie o postupoch, incidentoch, analýzach a interných procesoch s dôrazom na bezpečnosť, auditovateľnosť a prístupové práva.



Obrázok 28: 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

POD Wiki.js pre Znalostný portál pre SOC tím je kontajnerová jednotka nasadená v Kubernetes clustri, ktorá hostuje aplikáciu Wiki.js – moderný a výkonný systém na správu dokumentácie a znalostí. Tento POD slúži ako centrálny znalostný portál pre tím kybernetickej bezpečnosti (SOC), kde sa ukladajú, spravujú a zdieľajú informácie o postupoch, incidentoch, analýzach a interných procesoch s dôrazom na bezpečnosť, auditovateľnosť a prístupové práva.