PROJEKT

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

Previazané s balíkom KPB1 - Návrh virt. riešenia

Previazané s výstupom V2: zoznam definovaných kritérií;

Obsah

1 Úvod ... 3
2 Metodika hodnotenia ... 3
2.1 Hodnotiace kritéria pre výber open source riešenia ... 3
2.2 Počet hodnotiacich kritérií ... 3
2.3 Podmienky pre výber kandidátnych riešení ... 4
2.4 Kategórie hodnotiacich kritérií ... 4
2.5 Váhovanie kritérií a ich význam ... 5
2.6 Príklady z podobných projektov a porovnaní ... 6
2.7 Zhrnutie ... 7
3 Stanovenie porovnávacích kritérií pre výber cloudovej platformy ... 7
3.1 Funkčné kritériá ... 7
3.1.1 K1: Podpora IaaS funkcionality (váha: 5) ... 7
3.1.2 K2: Modularita a architektúra (váha: 4) ... 7
3.1.3 K3: Podpora orchestrácie a automatizácie (váha: 4) ... 8
3.2 Technické kritériá ... 8
3.2.1 K4: Výkonnosť a škálovateľnosť (váha: 5) ... 8
3.2.2 K5: Spoľahlivosť a stabilita (váha: 4) ... 9
3.2.3 K6: Súlad so štandardmi a interoperabilita (váha: 4) ... 9
3.3 Prevádzkové kritériá ... 10
3.3.1 K7: Náročnosť nasadenia a správy (váha: 3) ... 10
3.3.2 K8: Podpora, dostupnosť dokumentácie a komunita (váha: 4) ... 10
3.4 Bezpečnostné kritériá ... 11
3.4.1 K9: Autentifikácia a riadenie prístupov (váha: 5) ... 11
3.4.2 K10: Izolácia tenantov a ochrana dát (váha: 5) ... 11
3.4.3 K11: Sieťová/monitorovacia integrácia (váha 3) ... 11
3.5 Metodika hodnotenia ... 12
3.6 Návrh hodnotiacej matice ... 13
4 Návrh hodnotiacej tabuľky pre výber cloudovej platformy ... 13
Záver ... 14
Zoznam zdrojov ... 14

1 ÚVOD

Multitenantné operačné centrum kybernetickej bezpečnosti, riešené ako otvorená cloudová služba s prvkami strojového učenia, vyžaduje starostlivý výber technologickej platformy. Keďže projekt zahŕňa návrh komplexnej virtualizačnej platformy a jej inteligentného monitoringu, jedným z prvých krokov je stanovenie porovnávacích kritérií pre výber vhodného riešenia. Medzi základné úlohy pracovného balíka KPB1 patrí práve definovanie kritérií, analýza dostupných riešení a výber open-source platformy. Dôkladne nastavené kritériá umožnia objektívne porovnať alternatívy a vybrať riešenie najlepšie vyhovujúce požiadavkám projektu. Tým sa eliminuje náhodné alebo emocionálne rozhodovanie – kvantifikované hodnotenie pomáha odstrániť subjektívne dohady z procesu rozhodovania.

Výber porovnávacích kritérií je kritický, pretože určuje aspekty riešenia ktoré sú dôležité. V kontexte cloudovej platformy pre bezpečnostné centrum je potrebné zohľadniť široké spektrum faktorov od funkčnej stránky (ponúkané služby, integrácia), cez technické parametre (výkon, škálovateľnosť, spoľahlivosť), prevádzkové hľadiská (náklady, podpora, správa) až po bezpečnostné požiadavky (funkcie zabezpečenia, súlad so štandardmi). Podľa technologických odporúčaní a praxe patria medzi kľúčové kritériá pri výbere cloudového riešenia napríklad bezpečnosť, spoľahlivosť, výkon, škálovateľnosť či cena. Definovanie týchto kritérií a stanovenie ich významnosti (váh) zabezpečí, že následné hodnotenie dostupných platforiem bude systematické a obhájiteľné.

2 METODIKA HODNOTENIA

2.1 HODNOTIACE KRITÉRIA PRE VÝBER OPEN SOURCE RIEŠENIA

Pri porovnávaní open-source riešení pre privátny cloud v akademickom alebo výskumnom prostredí je dôležité zvoliť primeraný počet hodnotiacich kritérií, rozdeliť ich do prehľadných kategórií a priradiť im váhy podľa dôležitosti. Kritériá musia pokryť všetky relevantné oblasti (funkčné, technické, prevádzkové, bezpečnostné atď.), ale zároveň ich nesmie byť priveľa, aby boli realisticky zvládnuteľné na hodnotenie v rámci pilotného projektu. Nižšie uvádzame odporúčaný rozsah kritérií, návrh kategorizácie, prístup k váhovaniu a príklady z podobných projektov

2.2 POČET HODNOTIACICH KRITÉRIÍ

Pre účely objektívneho porovnania odporúčame zvoliť **mierny počet kritérií**, typicky v rozpätí **približne 5 až 15**. Literatúra ukazuje veľké rozpätie prístupov – existujú veľmi podrobné porovnania so stovkou detailných kritérií (rozdelených do viacerých kategórií) [1], no na druhej strane niektoré štúdie si vystačili s niekoľkými kľúčovými kritériami (napríklad ~5–10) pokrývajúcimi najdôležitejšie oblasti [2]. Približne **8–12 kritérií predstavuje praktický kompromis**: pokrývajú podstatné funkcie a vlastnosti cloud platformy, ale tím v akademickom pilotnom projekte ich ešte vie spoľahlivo vyhodnotiť v dostupnom čase. Pri menšom počte kritérií hrozí, že niektoré aspekty riešení ostanú nepostihnuté, kým pri priveľkom počte (desiatky kritérií) sa hodnotenie stáva príliš zložitým a časovo náročným. Preto je vhodné najskôr identifikovať všetky potenciálne faktory a následne ich zúžiť na najdôležitejšie a neprekrývajúce sa kritériá (t.j. odstrániť duplicitné alebo marginálne faktory) [3].

2.3 PODMIENKY PRE VÝBER KANDIDÁTNYCH RIEŠENÍ

Pri výbere kandidátnych cloudových platforiem na porovnanie v ďalšej fáze projektu boli stanovené tieto základné výberové podmienky:

- Platforma musí byť **open-source**, dostupná pod slobodnou licenciou a bez povinnosti viazania sa na konkrétneho komerčného dodávateľa,
- Musí byť **nasaditeľná on-premise**, s možnosťou prevádzky v prostredí akademickej inštitúcie alebo interného datacentra.

Cieľom je nájsť riešenia, ktoré poskytujú IaaS (Infrastructure as a Service) funkcionalitu, umožňujú multitenantné prostredie a sú dostatočne robustné pre bezpečnostné operácie, ideálne s otvoreným zdrojovým kódom alebo aspoň s flexibilnou licenčnou politikou pre akademickú sféru.

2.4 KATEGÓRIE HODNOTIACICH KRITÉRIÍ

Aby porovnanie bolo prehľadné, kritériá je vhodné rozdeliť do tematických kategórií. V kontexte IaaS platforiem pre privátny cloud (najmä s ohľadom na akademické/výskumné využitie a kyberbezpečnosť) sa často používajú nasledujúce kategórie:

- **Funkčné kritériá**: Hodnotia **funkcionalitu a vlastnosti** platformy. Sem patrí napríklad podpora rôznych hypervízorov a technológií virtualizácie, typy podporovaných úložísk a sietí, dostupné API a integrácie, podpora multi-tenancy (oddelenie viacerých projektov/užívateľov), orchestrácia a automatizácia, škálovateľnosť systému či pokročilé funkcie (napr. autoscaling, monitoring). Cieľom je zistiť, aké **služby a možnosti** každá platforma ponúka a do akej miery vyhovujú potrebám projektu. Tieto kritériá odpovedajú na otázku, **čo platforma dokáže poskytnúť** z hľadiska funkcionality.
- **Technické kritériá:** Sledujú **technickú architektúru a požiadavky** riešenia. Patria sem kritériá ako celková architektúra systému (modulárnosť, komponenty), kompatibilita s existujúcou infraštruktúrou a podporovaným hardvérom, podporované operačné systémy a databázy, výkonnosť a efektivita (napr. koľko zdrojov systém spotrebuje, aké sú limity pri počte VM, rýchlosti siete a pod.), škálovateľnosť (ako dobre systém rastie so zvyšujúcou sa záťažou), robustnosť a spoľahlivosť (odolnosť voči zlyhaniam, dostupnosť), či interoperabilita a kompatibilita so štandardmi. Môžeme sem zaradiť aj informácie o technológiách, na ktorých je platforma postavená (napr. použitý programovací jazyk, databázový backend), keďže to môže ovplyvniť napr. nároky na znalosti personálu [2]. Tieto kritériá hodnotia technické predpoklady platformy a odpovedajú na otázku, **ako platforma funguje a aké nároky kladie.**
- **Prevádzkové (organizačné) kritériá**: Zameriavajú sa na **prevádzku, správu a podporu platformy** v reálnom prostredí. Tu patrí náročnosť inštalácie a konfigurácie, jednoduchosť údržby, kvalita dokumentácie a dostupnosť zdrojov na učenie, veľkosť a aktivita používateľskej komunity, dostupná podpora (komunitná či komerčná) a jej kvalita, frekvencia aktualizácií a vývojového cyklu, zrelosť projektu (či ide o overenú technológiu alebo novinku), prípadne požiadavky na licencie (všetky menované riešenia sú open-source, ale môžu existovať voliteľné platené podporné služby). V akademickom prostredí, kde môže byť tím správcov malý, sú dôležité kritériá ako **jednoduchosť nasadenia a automatizácia** (aby systém nevyžadoval neúmerné úsilie na administráciu). Taktiež sem môžeme zaradiť náklady na prevádzku – hoci softvér je open-source, treba zvážiť nepriamu cenu: potrebný hardvér, čas na správu, školenie personálu, prípadne podporu. Prevádzkové kritériá teda hodnotia praktickú

využiteľnosť platformy v konkrétnych podmienkach (odpovedajú na otázku, **ako náročné je platformu nasadiť a prevádzkovať**).

- **Bezpečnostné kritériá**: V prostredí kybernetickej bezpečnosti ide o kľúčovú kategóriu. Posudzuje **bezpečnostné vlastnosti a mechanizmy** platformy. Patrí sem spôsob autentifikácie a autorizácie (podpora integrácie s LDAP/AD, jemne granulované riadenie prístupu, podpora viacfaktorovej autentifikácie), izolácia medzi tenantmi a virtuálnymi strojmi (napr. sieťová izolácia, oddelenie zdrojov), podpora šifrovania (dát v úložisku, komunikácie), dostupnosť auditných logov a monitoringu bezpečnosti, možnosť nastavenia bezpečnostných politík (firewally, bezpečnostné skupiny), a zhoda s priemyselnými štandardmi alebo osvedčenými postupmi. Napríklad, či platforma umožňuje splniť kontrolné opatrenia podľa noriem ako ISO/IEC 27001 v kontexte cloudu. V akademickom SOC-as-a-Service projekte je dôležité aj to, ako platforma podporuje integráciu bezpečnostných nástrojov (IDS/IPS, SIEM systémy) a či obsahuje funkcionality ako role-based access control (RBAC) pre oddelenie povinností. Bezpečnostné kritériá hodnotia, **ako dobre je platforma chránená** a čo ponúka na zabezpečenie spravovaných systémov a dát.

Uvedené kategórie možno prispôsobiť podľa konkrétnych potrieb. Napríklad niektoré metodiky uvádzajú **kategóriu podpory** samostatne (t.j. komunita, dokumentácia a podpora ako samostatná oblasť), prípadne zaraďujú finančné či legislatívne aspekty. Pre účely výskumného/pilotného projektu v akademickej sfére však vyššie uvedené štyri oblasti (funkčné, technické, prevádzkové, bezpečnostné) typicky pokryjú hlavné kritériá. Dôležité je, aby každá kategória mala aspoň niekoľko (napr. 2–5) konkrétnych kritérií, na základe ktorých bude možné hodnotiť daný aspekt. Tým vznikne vyvážená **matica porovnania**, ktorú je možné prezentovať aj vo forme tabuľky – riadky predstavujú kritériá (zoskupené podľa kategórií) a stĺpce jednotlivé porovnávané platformy.

2.5 VÁHOVANIE KRITÉRIÍ A ICH VÝZNAM

Pri **viackriteriálnom rozhodovaní** je vhodné jednotlivým kritériám prideliť **váhy** podľa ich relatívnej dôležitosti pre daný projekt. Odporúča sa a aj my použijeme jednoduchú stupnicu, napríklad **1 až 5**, kde 1 znamená nízku dôležitosť a 5 kľúčovú kritickú dôležitosť. **Význam váhy** spočíva v tom, že kritériá s vyššou váhou budú mať väčší vplyv na celkové hodnotenie platformy.

Postup bude taký, že **každú platformu ohodnotíme** v každom kritériu (napríklad bodmi 1–5 alebo slovne: vynikajúca, priemerná, slabá), a následne tieto **hodnoty vynásobíme váhou** daného kritéria. Tým získame **vážené skóre** pre každú platformu. Po sčítaní vážených skóre cez všetky kritériá dostaneme celkové poradie platforiem. Takýto prístup zabezpečí, že platforma, ktorá exceluje v kriticky dôležitých oblastiach, dosiahne lepšie celkové hodnotenie než tá, ktorá má možno viac slabších „nice-to-have“ funkcií. Váhy tak pomáhajú **formalizovať rozhodovanie** – umožňujú napríklad vytvoriť scenár „bezpečnostne orientovaný“ vs. „výkonovo orientovaný“ a podobne. V akademickom prostredí sa dá použiť aj formálnejšia metóda, napríklad analytický hierarchický proces (AHP), ktorá pomocou párového porovnávania kritérií určí váhy konzistentne [4]. Vo väčšine prípadov však postačí jednoduché ohodnotenie váhami 1–5. **Dôležité je zdôvodniť pridelené váhy** – napr. ak má bezpečnosť váhu 5, explicitne uviesť, že ide o projekt zameraný na kyberbezpečnosť, kde je ochrana dát prvoradá.

2.6 PRÍKLADY Z PODOBNÝCH PROJEKTOV A POROVNANÍ

Existuje viacero **štúdií a projektov**, ktoré sa zaoberali porovnaním open-source cloud platforiem, z ktorých možno čerpať inšpiráciu pre voľbu kritérií a metodiku hodnotenia:

- **Akademické porovnania:** Rozsiahla štúdia vykonaná [5] navrhla až **100 detailných kritérií** na porovnávanie open-source IaaS platforiem, pričom ich rozdelila do **6 hlavných kategórií**: virtualizácia, úložisko, sieť, správa, bezpečnosť a podpora [1]. Táto práca zdôrazňuje potrebu komplexného pohľadu – napríklad že popri základných IaaS vlastnostiach treba hodnotiť aj bezpečnosť a úroveň podpory. Iný akademický prístup použil **užší výber ~9 kritérií**, medzi ktoré zaradil napríklad architektúru systému, použitý programovací jazyk, podporované typy cloudových nasadení a hypervízorov, používateľské rozhranie, licencovanie, **robustnosť**, **interoperabilitu**, **bezpečnosť** a kompatibilitu. Ďalší autori sa zamerali iba na určité aspekty – napríklad Steinmetz et al. porovnávali OpenStack a Eucalyptus výlučne z hľadiska **výkonnosti** (časy štartu inštancií, sieťová priepustnosť, atď.) [2]. Tieto príklady ukazujú, že výber kritérií závisí od zamerania projektu – či už ide o komplexné porovnanie všetkých funkcií, alebo hĺbkovú analýzu špecifickej oblasti.
- **Diplomové a výskumné projekty:** V rámci akademických prác sa často využíva kombinácia kvantitatívnych a kvalitatívnych kritérií. Napríklad nedávny výskum na University of Twente vyvinul rámec hodnotenia IaaS poskytovateľov pomocou **6 hlavných kritérií** (Dostupnosť, Výkon, Škálovateľnosť, Spoľahlivosť, Bezpečnosť, Nákladová efektívnosť), pričom každé z nich malo ešte podkritériá mapujúce sa na konkrétne metriky (napr. v kategórii výkon sledovali výkon CPU, diskové I/O, sieťovú latenciu atď.). Aj keď tento konkrétny príklad sa zameriaval na verejné cloudy, metodika je poučná – využili váhy pre kritériá a scenáre, aby výsledné hodnotenie odrážalo priority (napr. scenár citlivý na bezpečnosť vs. na cenu) [4]. Podobný prístup sa dá aplikovať pri výbere privátnej cloud platformy: definovať si hlavné oblasti a ku každej viacero metrík. Iná diplomová práca alebo pilotný projekt môže mať napríklad kritériá ako *podpora kontajnerizácie* či *integrácia so špecifickými bezpečnostnými nástrojmi*, ak sú relevantné – dôležité je, že ich počet zostane zvládnuteľný a každé kritérium bude možné reálne zmerať alebo posúdiť.
- **Priemyselné odporúčania:** V priemyselnej praxi pri výbere cloudového riešenia existujú rôzne checklisty a best practices. Napríklad porovnávacie články od cloudových konzultačných firiem často radia hodnotiť **škálovateľnosť vs. robustnosť vs. podporu** atď., a odporúčajú **prispôsobiť váhy kategórií** podľa potrieb organizácie. Tiež existujú otvorené metodiky ako OSS-PAL či QSOS pre hodnotenie open-source softvéru, ktoré zdôrazňujú nutnosť hodnotiť nielen funkcionalitu, ale aj **kvalitu komunity a bezpečnosť**. Pri výbere IaaS pre SOC-as-a-Service by priemyselné štandardy (napr. CSA – Cloud Security Alliance kontrolné zoznamy) napovedali zahrnúť **kontroly bezpečnosti** a **riadenia rizík** ako kritériá. Napokon, normy ako ISO/IEC 27017 (bezpečnostné kontroly pre cloud) či referenčné architektúry (napr. NIST pre cloud) môžu poslúžiť ako zdroj pre vytvorenie bezpečnostných a prevádzkových kritérií, aby zvolená platforma vyhovovala požadovanej úrovni zabezpečenia.

2.7 ZHRNUTIE

Pre náš projekt vyberieme približne 5–15 najrelevantnejších kritérií, rozdelených do zmysluplných kategórií (napr. funkčné, technické, prevádzkové a bezpečnostné). Každému kritériu priradíme váhu podľa jeho významu pre projekt, aby výsledné porovnanie odrážalo vaše priority. Tento prístup umožní vytvoriť prehľadnú **tabuľkovú komparáciu** platforiem (OpenStack, CloudStack, OpenNebula, Proxmox, prípadne iných), kde bude jasne vidieť silné a slabé stránky jednotlivých riešení. Postup je v súlade s osvedčenými postupmi z literatúry – od veľmi podrobných akademických analýz až po praktické odporúčania – a je **prispôsobený kontextu výskumného projektu** zameraného na budovanie SOC-as-a-Service. Takéto porovnanie by malo významne uľahčiť **rozhodnutie**, ktorá platforma najlepšie vyhovuje stanoveným požiadavkám.

3 STANOVENIE POROVNÁVACÍCH KRITÉRIÍ PRE VÝBER CLOUDOVEJ PLATFORMY

Kapitola predstavuje kategórie a konkrétne kritériá, ktoré boli navrhnuté pre porovnanie kandidátnych cloudových platforiem v projekte. Pre každé kritérium je uvedené zdôvodnenie jeho významu a priradená váha na škále 1–5 (kde 5 označuje najvyššiu dôležitosť). Následne je opísaná metodika hodnotenia – spôsob bodovania alternatív podľa kritérií, použitie váh pri výpočte celkových skóre a postup rozhodovania na základe výsledkov. Súčasťou dokumentu je aj návrh hodnotiacej matice, ktorá prehľadne zobrazuje kritériá, ich váhy a bodové hodnotenie. V závere zhrnieme prínosy navrhnutého systému hodnotenia a ukážeme, ako jeho aplikácia umožní výber vhodnej platformy pre daný projekt.

3.1 FUNKČNÉ KRITÉRIÁ

3.1.1 K1: Podpora IaaS funkcionality (váha: 5)

Odôvodnenie: Projekt vyžaduje plnú funkcionalitu IaaS – správu virtuálnych strojov (VM), diskov, sietí, obrazov, snapshotov a samostatných zdrojov. Platforma musí podporovať vytváranie a správu rôznych typov inštancií, umožniť priradenie zdrojov podľa potreby tenantov a zároveň ponúknuť robustné API rozhranie pre programovateľný prístup. Schopnosť poskytovať kompletnú IaaS funkcionalitu je kľúčová pre zabezpečenie pružného a spoľahlivého prevádzkovania SOC ako služby.

Odporúčanie pre hodnotenie:

- 5 bodov: Podpora kompletných IaaS funkcií (VM, siete, disky, snapshoty), silné API rozhrania, potvrdené referencie.
- 3 body: Väčšina základných funkcií IaaS dostupná, API s určitými limitmi.
- 1 bod: Obmedzená funkcionalita IaaS, slabá alebo žiadna API podpora.

3.1.2 K2: Modularita a architektúra (váha: 4)

Odôvodnenie: Modularita architektúry zásadne ovplyvňuje rozšíriteľnosť a škálovateľnosť riešenia. Platforma, ktorá je rozdelená do samostatných komponentov (napr. Nova – compute, Neutron – networking, Cinder – block storage), umožňuje nezávislé nasadzovanie, ladenie a výmenu modulov podľa potrieb. Taktiež je výhodné, ak platforma podporuje modernú architektúru mikroslužieb, pluginy, kontajnerizáciu a orchestračné vrstvy. Vyššia modularita zároveň znižuje riziko výpadku celého systému pri poruche jednej služby.

Odporúčanie pre hodnotenie:

- **5 bodov:** Vysoká modularita, mikroslužby, samostatne nasaditeľné komponenty, jasná integrácia pluginov.
- **3 body:** Modulárnosť je čiastočná, niektoré komponenty sú navzájom závislé.
- **1 bod:** Monolitická architektúra, obmedzené možnosti úprav alebo výmeny komponentov.

3.1.3 K3: Podpora orchestrácie a automatizácie (váha: 4)

Odôvodnenie: Platforma by mala podporovať nástroje ako Heat (OpenStack orchestration), Terraform (infrastructure as code), Ansible (automatizácia) alebo Kubernetes Operator pre efektívnu správu a nasadzovanie komplexných infraštruktúrnych scénarov. Táto schopnosť umožní rýchle škálovanie služieb, automatizované rozbaľovanie prostredí, opakovateľné testovanie aj zotavenie pri výpadkoch. V prostredí SOC, kde sa často menia požiadavky a topológia siete, je orchestrácia nevyhnutná pre zabezpečenie flexibility, udržateľnosti a prevádzkovej efektivity.

Odporúčanie pre hodnotenie:

- 5 bodov: Výborná podpora (Heat, Terraform, Ansible, Kubernetes), automatizácia robustná a flexibilná.
- 3 body: Základná orchestrácia dostupná, čiastočné limity v podpore nástrojov.
- 1 bod: Veľmi obmedzená alebo žiadna automatizácia, slabá integrácia s populárnymi nástrojmi.

3.2 TECHNICKÉ KRITÉRIÁ

3.2.1 K4: Výkonnosť a škálovateľnosť (váha: 5)

Odôvodnenie: Hodnotí sa, ako efektívne dokáže riešenie využívať zdroje, aké má limity z hľadiska počtu VM, kontajnerov či tenantov, a aké mechanizmy automatického škálovania podporuje. Dôležitá je aj latencia a celkový výkon pri spracovaní údajov, najmä v reálnom čase pre účely monitoringu bezpečnostných udalostí. Riešenie musí byť schopné rásť s počtom VM, tenantov a služieb. Hodnotí sa horizontálna a vertikálna škálovateľnosť. V podmienkach projektu potrebujeme platformu, ktorá dokáže rásť spolu s počtom klientov SOC služby a objemom spracovávaných dát.

Preto tomuto kritériu prislúcha **váha 5** – maximálna dôležitosť, keďže nedostatočná výkonnosť alebo obmedzené škálovanie by predstavovali zásadné riziko.

Odporúčanie pre hodnotenie:

- 5 bodov: Vynikajúca škálovateľnosť, potvrdená schopnosť obslúžiť stovky VM, horizontálne a vertikálne škálovanie.
- 3 body: Primeraná škálovateľnosť s istými obmedzeniami (desiatky VM bez výrazného poklesu výkonu).
- 1 bod: Slabý výkon, výrazné škálovacie limity už pri nízkom počte VM.

3.2.2 K5: Spoľahlivosť a stabilita (váha: 4)

Odôvodnenie: Posudzujeme mieru vyzretosti platformy, jej stabilitu v produkčnej prevádzke a dostupnosť mechanizmov pre vysoko dostupné nasadenie. Kritérium zahŕňa úroveň otestovania a odladenia softvéru a možnosť nasadiť komponenty redundantne (HA – High Availability). V prostredí bezpečnostného centra je dôležité minimalizovať prestoje a zaistiť nepretržitú dostupnosť služby. Pri hodnotení cloudových služieb sa odporúča dôkladne preskúmať minulú výkonnosť, spokojnosť zákazníkov a zvládanie neplánovaných výpadkov. Rovnako porovnávame SLA (Service Level Agreement) ak sú k dispozícii – hoci v prípade open-source platformy ide skôr o interné garancie, dostupnosť podpory atď.

Keďže spoľahlivosť priamo ovplyvňuje kvalitu poskytovanej SOC služby, má toto kritérium **váhu 4** (vyššia dôležitosť).

Odporúčanie pre hodnotenie:

- 5 bodov: Bez vážnych výpadkov, spoľahlivé referencie v produkcii, podpora HA nasadenia.
- 3 body: Občasné menšie výpadky, čiastočná podpora HA.
- 1 bod: Časté alebo významné výpadky, žiadna podpora HA.

3.2.3 K6: Súlad so štandardmi a interoperabilita (váha: 4)

Odôvodnenie: Z technického hľadiska je významné, či platforma podporuje otvorené štandardy a bežné technológie, čo podmieňuje jej interoperabilitu s inými systémami. Riešenie by malo byť kompatibilné s populárnymi hypervízormi, sieťovými protokolmi, úložiskovými technológiami a rozhraniami pre správu (napr. OpenStack API je de facto štandard pre open-source cloudy). Široká podpora štandardov zároveň uľahčuje integráciu a minimalizuje riziko proprietárnych obmedzení. Posudzujeme tiež dostupnosť certifikácií alebo referencií – napríklad či platforma vychádza z osvedčených open-source projektov podporovaných veľkou komunitou. Ako naznačujú postupy hodnotenia cloudových poskytovateľov, dodržiavanie priemyselných štandardov a osvedčení (napr. ISO 27001 v bezpečnosti) je významným kritériom výberu. V našom projekte interoperabilita umožní v budúcnosti prepojenie viacerých cloudových prostredí a integráciu ďalších komponentov.

Je tiež dôležité, aby platforma obsahovala nástroje na implementáciu požadovaných opatrení (napr. logovanie, šifrovanie, prístupové kontroly) a aby komunita/dodávatelia poskytovali usmernenia pre súlad s predpismi. Súlad s reguláciami ovplyvní prijateľnosť riešenia v produkcii – napríklad pre dáta verejnej správy by platforma mala podporovať nasadenie v súlade so zákonom o ochrane osobných údajov (GDPR). Vzhľadom na charakter plánovaného SOC riešenia (ktoré môže spracúvať citlivé bezpečnostné údaje klientov) považujeme toto kritérium za veľmi významné a priraďujeme mu váhu 4.

Odporúčanie pre hodnotenie:

- **5 bodov:** Plná kompatibilita s otvorenými štandardmi, certifikácie (ISO 27001, GDPR compliant), aktívna interoperabilita.
- **3 body:** Čiastočná kompatibilita a interoperabilita, niektoré štandardy nie sú úplne pokryté.
- **1 bod:** Obmedzená alebo žiadna kompatibilita, problémy s interoperabilitou.

3.3 PREVÁDZKOVÉ KRITÉRIÁ

3.3.1 K7: Náročnosť nasadenia a správy (váha: 3)

Odôvodnenie: Toto kritérium posudzuje, aké úsilie a zdroje bude potrebné vynaložiť na inicializáciu platformy a jej následnú správu. Vstupuje sem zložitosť inštalácie (počet a komplikovanosť krokov pri nasadzovaní celého prostredia), požiadavky na odborné znalosti personálu, čas potrebný na plné sprevádzkovanie, ale aj prehľadnosť údržby (aktualizácie, upgrady, škálovanie). Napríklad niektoré open-source platformy sú vysoko konfigurovateľné, ale môžu byť komplexné na nasadenie, čo si vyžaduje skúsený tím alebo využitie automatizačných nástrojov (napr. Ansible skripty a pod.). Z prevádzkového hľadiska hodnotíme aj to, či riešenie prináša funkcionality uľahčujúce správu – napr. self-healing, monitoring, jednoduché rozšírenie klasteru apod. Cieľom je zvoliť platformu, ktorej prevádzka nebude pre organizáciu neúmernou záťažou.

Tomuto kritériu dávame **váhu 3** (stredná dôležitosť), vzhľadom na to, že niektoré dodatočné úsilie pri open-source riešení je akceptovateľné, pokiaľ ostatné prínosy prevažujú.

Odporúčanie pre hodnotenie:

- 5 bodov: Jednoduché nasadenie, jasná dokumentácia, minimálne požiadavky na správu, silná automatizácia.
- 3 body: Mierne komplexnejšie nasadenie, zvládnuteľné s dostupnými nástrojmi a dokumentáciou.
- 1 bod: Zložitá inštalácia, náročná administrácia, nedostatočná dokumentácia.

3.3.2 K8: Podpora, dostupnosť dokumentácie a komunita (váha: 4)

Odôvodnenie: Úroveň dostupnej podpory pre danú platformu výrazne ovplyvňuje jej praktickú použiteľnosť. Pri komerčných riešeniach sledujeme kvalitu technickej podpory dodávateľa (dostupnosť 24/7, SLA pre riešenie incidentov). Pri open-source riešeniach je dôležitá veľkosť a aktivita komunity – počet prispievateľov, frekvencia vydávania nových verzií a opráv chýb, dostupnosť dokumentácie a znalostnej bázy. Silná komunita a podpora od veľkých IT firiem sú zárukou dlhodobej udržateľnosti projektu. Hodnotí sa aj existencia školení, certifikácií alebo konzultačných služieb pre danú platformu. Podľa skúseností môžu menší poskytovatelia ponúkať osobnejšiu podporu, kým väčší hráči majú rozsiahlejšie zdroje podpory, avšak často za príplatok. Keďže v našom prípade uvažujeme open-source platformu, kritérium sa sústreďuje na komunitnú podporu a ekosystém okolo nej. Hodnotí sa vývojová aktivita projektu, frekvencia aktualizácií

Priraďujeme mu **váhu 4**, keďže dostupnosť odbornej podpory a aktívny vývoj sú pre úspech projektu veľmi dôležité.

Odporúčanie pre hodnotenie:

- **5 bodov:** Aktívna komunita, bohatá dokumentácia, pravidelné aktualizácie a profesionálna podpora.
- **3 body:** Priemerná komunita, základná dokumentácia, pomalšie aktualizácie.
- **1 bod:** Slabá alebo neexistujúca komunita, zastaraná dokumentácia, minimálna podpora.

3.4 BEZPEČNOSTNÉ KRITÉRIÁ

3.4.1 K9: Autentifikácia a riadenie prístupov (váha: 5)

Odôvodnenie: Platforma by mala obsahovať zabudované bezpečnostné prvky potrebné na ochranu infraštruktúry a dát v prostredí SOC. Sem patrí napríklad podpora pre viacúrovňovú autentifikáciu a autorizáciu užívateľov, možnosť šifrovania dát (v úložiskách, prenosoch), logovanie a auditovanie udalostí či automatizované bezpečnostné politiky. Pri open-source riešení posudzujeme, aké bezpečnostné moduly ponúka a či spĺňa moderné bezpečnostné postupy (pravidelné bezpečnostné aktualizácie, možnosti hardeningu).

Vzhľadom na povahu projektu (kyberbezpečnosť) ide o **kritické** kritérium s váhou **5**. Platforma, ktorá by nevedela zabezpečiť dáta a systémy na adekvátnej úrovni, nemôže byť považovaná za vhodnú.

Odporúčanie pre hodnotenie:

- 5 bodov: Pokročilá viacúrovňová autentifikácia, robustné riadenie prístupov, úplná podpora logovania a auditu.
- 3 body: Základná autentifikácia a riadenie prístupov, limitované možnosti auditovania.
- 1 bod: Slabá bezpečnosť autentifikácie, minimálne možnosti auditu.

3.4.2 K10: Izolácia tenantov a ochrana dát (váha: 5)

Odôvodnenie: V multitenantnom prostredí je nevyhnutné, aby platforma zaručila striktnú izoláciu medzi jednotlivými zákazníkmi (tenantmi) – ich virtuálne stroje, úložiská a siete musia byť oddelené tak, aby sa zabránilo neoprávnenému prístupu alebo úniku dát medzi tenantmi. Toto kritérium hodnotí architektúru platformy z hľadiska viacvrstvovej bezpečnosti: oddelenie výpočtových zdrojov, sieťová segmentácia, mechanizmy kontroly prístupu a podobne. **Miera izolácie dát medzi tenantmi je zásadným aspektom multitenantných systémov**.

Akákoľvek slabina v izolácii by mohla viesť k bezpečnostným incidentom, preto tomuto kritériu priraďujeme **váhu 5** (veľmi vysoká).

Odporúčanie pre hodnotenie:

- **5 bodov:** Vysoká izolácia tenantov, úplná segmentácia zdrojov, pokročilé mechanizmy ochrany dát.
- **3 body:** Čiastočná izolácia s niektorými limitmi, menej robustné mechanizmy ochrany.
- **1 bod:** Slabá izolácia tenantov, riziko úniku dát, slabá kontrola prístupu.

3.4.3 K11: Sieťová/monitorovacia integrácia (váha 3)

Odôvodnenie: Odôvodnenie: Hodnotí mieru integrácie s nástrojmi pre monitoring a bezpečnostné dohľadové systémy – najmä SIEM, IDS/IPS (napr. Suricata, Snort), ako aj metrické/logovacie nástroje ako Ceilometer, Grafana, Prometheus. Zohľadňuje tiež schopnosť platformy exportovať bezpečnostné udalosti, podporu API/webhookov a možnosti integrácie s externými bezpečnostnými prvkami. Kritérium dopĺňa hodnotenie autentifikácie a izolácie o schopnosť platformy byť súčasťou aktívneho bezpečnostného prostredia.

Odporúčanie pre hodnotenie:

- 5 bodov: Úplná integrácia s nástrojmi (SIEM, IDS/IPS, Grafana, Prometheus), jednoduchá konfigurácia.

- 3 body: Čiastočná integrácia, niektoré dôležité nástroje sú podporované obmedzene.
- 1 bod: Veľmi obmedzená integrácia, problémy s prepojením nástrojov a exportom udalostí.

3.5 METODIKA HODNOTENIA

Každé riešenie bude hodnotené v každom kritériu bodovo na škále **1 až 5**:

Pre objektívny výber najvhodnejšej platformy sme zvolili **viackriteriálny hodnotiaci prístup** založený na bodovom ohodnotení jednotlivých alternatív podľa stanovených kritérií a využití váženého súčtu. Metodika hodnotenia pozostáva z nasledovných krokov:

1. **Definovanie škály bodovania:** Každé kritérium bude hodnotené bodmi od 1 do 5, pričom 1 znamená, že riešenie kritérium spĺňa veľmi slabo alebo vôbec, a 5 znamená vynikajúce splnenie kritéria. Táto škála poskytuje dostatočné rozlíšenie a je zrozumiteľná. Pre konzistentnosť hodnotenia budú stanovené aj slovné opisy pre jednotlivé body (napr. 1 – nedostatočné splnenie, 3 – priemerné splnenie, 5 – výborné splnenie). Všetci hodnotitelia musia používať škálu jednotne.
2. **Priradenie váh kritériám:** Každé kritérium má pridelenú **váhu v rozmedzí 1–5** podľa jeho relatívnej dôležitosti (tieto váhy sú uvedené vyššie pri popise kritérií). Váha vyjadruje, koľkokrát je dané kritérium významnejšie oproti iným. Najkritickejšie faktory (napr. bezpečnosť, kľúčové funkcie, náklady) majú váhu 5, menej dôležité aspekty váhu nižšiu. Váhy sme stanovili expertným odhadom na základe potrieb projektu; v prípade potreby je možné ich spresniť metódami párového porovnávania alebo konsenzom tímu:
   - 5 = vynikajúce splnenie,
   - 4 = plné splnenie,
   - 3 = čiastočné splnenie,
   - 2 = obmedzené splnenie,
   - 1 = minimálne alebo žiadne splnenie.
3. **Bodové ohodnotenie alternatív:** Pre každú uvažovanú alternatívu cloudovej platformy sa vykoná hodnotenie všetkých 11 kritérií na škále 1–5. Hodnotenie bude založené na zisteniach z analýzy (výstup V1) – napr. do akej miery daná platforma poskytuje požadované funkcie, aký má výkon podľa testov či referencií, ako spĺňa bezpečnostné požiadavky atď. Môže ísť o kombináciu meraných údajov (napr. výkonových testov), informácií z dokumentácie a expertného posudku. Každé pridelené bodové hodnotenie bude zdôvodnené, aby bol proces transparentný.
4. **Výpočet váženého skóre:** Následne pre každú alternatívu vypočítame celkové **skóre** ako vážený súčet bodov. Tzn. bodové hodnotenie kritéria sa vynásobí váhou daného kritéria a tieto súčiny sa sčítajú cez všetkých 11 kritérií. Výsledkom je jedno číslo – celkové hodnotenie alternatívy. Tento **vážený hodnotiaci model** je osvedčený nástroj pre viac-kriteriálne rozhodovanie, umožňujúci kvantifikovať mieru, do akej každá možnosť spĺňa celkové požiadavky.
5. **Porovnanie a výber:** Alternatívy sa zoradia podľa dosiahnutého váženého skóre. Najvyššie skóre indikuje platformu, ktorá najlepšie vyhovuje stanoveným kritériám a teda predstavuje optimálnu voľbu. Pri tesných výsledkoch je možné uskutočniť citlivostnú analýzu – napr. skontrolovať vplyv zmien váh na poradie, alebo detailne rozobrať rozdiely v kľúčových kritériách. Výsledkom procesu bude odporúčanie

konkrétnej platformy (v ďalšom výstupe projektu, V3) s odôvodnením na základe dosiahnutých bodov.

Uvedený postup zaisťuje, že rozhodnutie bude **transparentné a obhájiteľné**. Všetky vstupy (váhy, bodovania) budú zdokumentované. Prístup je flexibilný – v prípade potreby možno doplniť nové kritériá alebo upraviť váhy a znovu prepočítať skóre. Týmto spôsobom sa minimalizuje riziko nesprávnej voľby a zabezpečí sa, že vybrané riešenie bude zodpovedať definovaným potrebám projektu.

3.6 NÁVRH HODNOTIACEJ MATICE

Pre prehľadné znázornenie hodnotenia slúži nasledujúca hodnotiaca matica (Tabuľka 1). Riadky predstavujú jednotlivé kritériá (rozdelené podľa kategórií) s priradenou váhou. V stĺpci „Bodové hodnotenie (1–5)“ sa budú uvádzať pridelené body pre hodnotenú alternatívu – v procese výberu sa táto tabuľka vyplní pre každú posudzovanú platformu.

4 NÁVRH HODNOTIACEJ TABUĽKY PRE VÝBER CLOUDOVEJ PLATFORMY

Kritérium (Kx)	Váha (1–5)	Hodnotenie (1–5)
K1: Podpora IaaS funkcionality	5	[1 - 5]
K2: Modularita a architektúra	4	[1 - 5]
K3: Orchestrácia a automatizácia	3	[1 - 5]
K4: Výkonnosť a škálovateľnosť	5	[1 - 5]
K5: Spoľahlivosť a stabilita	4	[1 - 5]
K6: Štandardy a interoperabilita	4	[1 - 5]
K7: Náročnosť nasadenia a správy	3	[1 - 5]
K8: Dokumentácia a komunita	4	[1 - 5]
K9: Autentifikácia a prístupy	5	[1 - 5]
K10: Izolácia tenantov a ochrana dát	5	[1 - 5]
K11: Sieťová / monitorovacia integrácia	3	[1 - 5]

V tabuľke sú uvedené aj navrhované váhy pre jednotlivé kritériá (druhá kolónka). Pri hodnotení konkrétnej platformy sa do tretej kolónky zaznačí dosiahnuté bodové hodnotenie 1 až 5. Následne sa vypočíta vážené skóre ako súčet súčinov váh a bodov v každom riadku. Takáto matica pomôže rýchlo identifikovať silné a slabé stránky hodnotených riešení – napríklad je vidieť, ktoré kritériá majú najvyššiu váhu a aké skóre v nich alternatíva získala. Umožní to transparentnú diskusiu o výsledkoch a prípadné doladenie hodnotenia. Matica je navrhnutá univerzálne; v projekte ju plánujeme použiť pre porovnanie viacero open-source platforiem, pričom očakávaným výstupom je víťazné riešenie s najvyšším celkovým skóre.

ZÁVER

Navrhnutý systém porovnávacích kritérií poskytuje systematický rámec pre výber cloudovej platformy pre multitenantné SOC riešenie. V rámci dokumentu sme definovali 11 kľúčových kritérií v štyroch kategóriách – funkčnej, technickej, prevádzkovej a bezpečnostnej. Každé kritérium bolo zdôvodnené s ohľadom na ciele a požiadavky projektu a bola mu pridelená váha vyjadrujúca jeho relatívnu dôležitosť. Tým je zabezpečené, že hodnotenie bude pokrývať všetky relevantné oblasti: od schopností platformy poskytnúť požadované funkcie, cez jej výkon a spoľahlivosť, náklady a podporu, až po robustnosť zabudovaných bezpečnostných mechanizmov.

Takto zostavené kritériá a váhy umožnia objektívne **porovnať alternatívne riešenia**. Pomocou bodovania a váženého súčtu dokážeme kvantifikovať mieru splnenia požiadaviek pre každú posudzovanú platformu. Váhy zabezpečia, že najdôležitejšie oblasti (napr. bezpečnosť, kritické funkcie, náklady) budú mať primeraný vplyv na výsledné skóre. Výberový proces založený na týchto kritériách je transparentný – ku každej známke bude existovať odôvodnenie, a výsledné skóre jasne ukáže, ktorá možnosť najlepšie vyhovuje projektu.

Navrhnutý systém kritérií a hodnotenia výrazne zvyšuje šance, že zvolíme **vhodnú platformu** pre budovanie multitenantného bezpečnostného centra. Umožňuje nám identifikovať riešenie, ktoré najlepšie spĺňa funkčné požiadavky, zapadne do existujúcej infraštruktúry, bude technicky spoľahlivé a škálovateľné, ekonomicky prijateľné a zároveň zaistí vysokú úroveň kybernetickej bezpečnosti. Takáto platforma vytvorí pevný základ pre realizáciu zámerov projektu a dosiahnutie jeho cieľov.

ZOZNAM ZDROJOV

[1] I. Voras, B. Mihaljevič a M. Orlic, „Criteria for Evaluation of Open Source Cloud Computing Solutions,“ rev. *roceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces, Cavtat, Croatia, 2011*.

[2] F. Cocozza, „Cloud Management Platform Selection: A Case Study in a University Setting,“ 2015.

[3] Business analytics review, https://library.fiveable.me/business-analytics/unit-11/multi-criteria-decision-making/study-guide/Xgpbm7FKThBDW6Oe.

[4] G. Chalan, Developing Objective Comparison Evaluation, 2024.

[5] D. Greibler a a ďalší, „Private IaaS Clouds: A Comparative Analysis of OpenNebula, CloudStack and OpenStack,“ Conference: 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), 2016.