VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OD TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINNESS AND MANAGEMENT

ÚSTAV INFORMATIKY
ISTITUTE OD INFORMATICS

Návrh dílčí části systému pro monitoring bezpečnostních incidentů

Design of a part of the system for monitoring security incidents

DIPLOMOVÁ PRÁCE
DIPLOMA THESIS

AUTOR PRÁCE Bc. Michael Koch
AUTHOR

VEDOUCÍ PRÁCE Ing. Lukáš Novák, Ph.D.
SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Michael Koch**
Vedoucí práce:	**Ing. Lukáš Novák, Ph.D.**
Akademický rok:	2022/23
Studijní program:	Informační management

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh dílčí části systému pro monitoring bezpečnostních incidentů

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení, přínos návrhů řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem je analyzovat stávající stav informačního systému vybrané organizace a jeho efektivnosti, posoudit tento stav a na základě firemní strategie připravit alternativní možnosti nového informačního systému včetně posouzení variant a návrhu optimální.

Základní literární prameny:

BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 3. aktualiz. a dopl. vyd. Praha: Grada, 2012. 323 s. ISBN 978-80-247-4307-3.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2. přeprac. a aktualiz. vyd. Praha: Grada, 2009. 496 s. ISBN 978-80-247-2615-1.

MOLNÁR, Zdeněk. Efektivnost informačních systémů. 2. rozš. vyd. Praha: Ikar, 2000. 178 s. ISBN 80-247-0087-5.

SCHWALBE, Kathy. Řízení projektů v IT. Brno: Computer Press, 2007. 720 s. ISBN 978-80-251-1526-8.

SODOMKA, Petr a Hana KLČOVÁ. Informační systémy v podnikové praxi. 2. aktualiz. a rozš. vyd. Brno: Computer Press, 2010. 501 s. ISBN 978-80-251-2878-7.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2022/23

V Brně dne 5.2.2023

L. S.

Doc. Ing. Miloš Koch, CSc. Garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Diplomová práce se zabývá implementací dílčí části informačního systému pro analýzu bezpečnostních incidentů v rámci firmy PwC. Systém slouží pro doplnění současného řešení, které zaostává vůči budoucím a stávajícím požadavkům. V první části jsou popsána teoretická východiska k pochopení konceptu práce a použité technologie, které byly použity v rámci implementace systému. Navazující kapitola obsahuje analýzu současného stavu existujícího systému. Na jakém principu pracuje a nedostatky, jež zapříčinily nutnost implementace nového řešení. Třetí kapitola se věnuje samotnému návrhu a realizaci nového řešení. V poslední části práce je provedeno ekonomické zhodnocení nákladů a přínosů řešení.

Abstract

The thesis focuses on the implementation of a part of the information system for security incident analysis within PwC. The system serves to complement the current solution, which lags behind future and existing requirements. The first part describes the theoretical background to understand the concept of the thesis and the technologies used in the implementation of the system. The following section contains an analysis of the current state of the existing system. The principle on which it works and the shortcomings that caused the necessity to implement a new solution. The third chapter deals with the actual design and implementation of the new solution. In the last part of the thesis an economic evaluation of the costs and benefits of the solution is made.

Key words

System design, cloud, SIEM, Grafana

Klíčová slova

Návrh systému, cloud, SIEM, Grafana

Bibliografická citace

KOCH, Michael. Návrh dílčí části systému pro monitoring bezpečnostních incidentů. Brno, 2023. Dostupné také z: https://www.vut.cz/studenti/zav-prace/detail/148417. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Lukáš Novák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 14. května 2023

……

podpis studenta

OBSAH

ÚVOD

V současném digitálním světě je riziko kybernetických útoků vyšší než kdykoliv v minulosti. Tento trend je zčásti způsoben současnou politickou situací, která přispěla ke zvýšenému využívání a dostupnosti nástrojů pro narušení kybernetické bezpečnosti. V únoru 2022 upozornil na tuto skutečnost i Národní úřad kybernetické bezpečnosti, který vydal oficiální prohlášení s varováním ohledně nejčastěji používaných kybernetických útoků (50). V důsledku toho musí mnohé firmy pravidelně čelit různým druhům útoků a je nezbytné, aby byly schopny se chránit a shromažďovat co nejvíce údajů o potenciálních hrozbách.

Pro efektivní obranu proti kybernetickým útokům je důležité sledovat aktuální trendy v oblasti kybernetické bezpečnosti a průběžně aktualizovat své bezpečnostní politiky a postupy. Firmy by měly investovat do výzkumu a vývoje nových technologií a nástrojů, které jim umožní lépe chránit své systémy a data. Zároveň by měly zaměstnancům poskytovat pravidelná školení a vzdělávání v oblasti kybernetické bezpečnosti, aby byli schopni rozpoznávat potenciální hrozby a jednat v souladu s interními bezpečnostními pokyny.

I přes sebelepší školení se může stát, že útočník prolomí obranu organizace a ohrozí tak data, firemní procesy nebo nasadí špionážní software. Pokud útočník dokáže využít zranitelnosti aktiva, je již na prevenci pozdě a nastupuje analytik z kyberbezpečnostního týmu, který musí hrozbu identifikovat, zneškodnit a zaznamenat dopady. Aby byl schopen provést všechny tyto kroky, je nezbytné mít k dispozici informace o průlomu zabezpečení organizace. K tomu slouží SIEM (Security Information and Event Management) systém, který shromažďuje, analyzuje a koriguje data z různých zdrojů v organizaci, aby poskytl přehled o bezpečnostních hrozbách a událostech v reálném čase. SIEM pomáhá analytikovi rychle identifikovat potenciální útoky a reagovat na ně účinně, čímž minimalizuje dopady na organizaci.

Tato diplomová práce se zabývá implementací části informačního systému, která má poskytovat přehled o zaznamenaných kybernetických útocích a umožnit klientům získat zpětnou vazbu ohledně stavu zabezpečení systému. Cílem práce je navrhnout a implementovat řešení, které bude efektivně zpracovávat data o útocích, analyzovat jejich povahu a závažnost a poskytovat uživatelům snadno srozumitelné informace a doporučení k dalšímu zlepšení zabezpečení.

CÍLE PRÁCE

Hlavním cílem diplomové práce bylo nasazení nové části informačního systému pro a analýzu bezpečnostních incidentů v rámci společnosti PwC.

Informační systém funguje v cloudovém prostředí Microsoft Azure pod názvem Microsoft Sentinel. Jde o SIEM systém, jehož hlavní úkol spočívá v zachycení a identifikaci bezpečnostních hrozeb. Data shromážděná během kybernetických incidentů jsou následně vyhodnocována a uložena v Azure komponentě zvané Azure Log Analytics Workspace. Zde jsou data zpracovávána a analyzována pomocí jazyka KQL. Poté jsou data zobrazena v rámci Sentinelu prostřednictvím dalšího nástroje, Azure Workbooks, který slouží k vizualizaci dat.

Nevýhodou tohoto řešení je nutnost přístupu k Workbooks, což vyžaduje, aby se každý uživatel nejprve autentizoval a autorizoval do cloudového prostředí, a teprve poté mohl vyhodnocovat incidenty na základě dat z přednastavených grafů. I když lze tento problém řešit správou práv a uživatelů v Azure, jedná se o neefektivní řešení z hlediska potenciálního počtu uživatelů s přístupem do cloudu, ačkoliv v omezené podobě. Tito uživatelé by představovali určité bezpečnostní riziko.

Microsoft Azure Sentinel poskytuje širokou škálu funkcí a možností pro správu a analýzu bezpečnostních incidentů. Přestože jeho pokročilé funkce mohou být užitečné, komplexnost nástroje přináší nevýhodu v jeho náročnosti na správu, kdy je zapotřebí tým odborníků pro jeho modifikaci.

Další nevýhodou je nedostatek vizualizačních prvků v rámci Workbooks, což ztěžuje analytikům získat komplexní přehled o identifikovaných incidentech. Kromě toho je i tvorba grafů v nativním prostředí Sentinelu časově náročná, jelikož prostředí není uživatelsky přívětivé.

Negativním faktorem tohoto řešení je i ze strany uživatelů, kdy by museli projít základním školením pro práci s Azurem. Vzhledem k tomu, že systém má mířit na širší typy uživatelů, technické znalosti by měli být pouze v rámci datové analýzy.

Cílem této práce je implementace systému pro vizualizaci dat, konkrétně Grafany, který umožňuje uživatelům vytvářet různé typy grafů v jednoduchém a organizovaném prostředí, speciálně navrženém pro analýzu dat. Systém navíc poskytuje vlastní nástroje pro správu přístupových práv, což eliminuje potřebu administrace uživatelů s přístupem k cloudovému prostředí.

V rámci práce bylo nezbytné provést nasazení vlastního virtuálního serveru s operačním systémem Ubuntu, jeho konfiguraci a následnou implementaci Grafany. Dále bylo nutné zajistit konektivitu mezi Grafanou a cloudovým prostředím a poté vytvořit samotné Dashboards s grafy.

Všechny stanovené cíle byly úspěšně dosaženy a postup jejich řešení je detailně popsán v části "Vlastní řešení".

1 TEORETICKÁ VÝCHODISKA PRÁCE

V této části práce budou popsány teoretické základy práce, na jakých technologiích je stavěna a základní pojmy, které je potřeba definovat pro plné pochopení práce.

1.1 ZÁKLADNÍ POJMY

1.1.1 Data

„V kontextu informačních systémů jsou data základní jednotkou informací, která může být uložena, zpracována a přenášena mezi různými komponentami systému“ (1, s.120). Jedná se tedy o základní stavební kámen pro libovolný informační systém, jenž jsou poté následně zpracovány dále.

„Data mohou být ve formě textu, čísel, obrázků, zvuku či jiných formátů, a slouží jako základ pro generování užitečných informací a znalostí“ (2, s.60).

V kontextu teorie informací a datové analýzy dochází často k záměně pojmů "data" a "informace". Představme si, že je zaznamenáno číslo 150. Izolovaně tento údaj není možné jednoznačně interpretovat. Může představovat množství položek, stav bankovního účtu, evidenční číslo či unikátní identifikátor. V takovém případě se jedná o data. Avšak pokud by bylo číslo 150 umístěno do sloupce s názvem "počet bodů", získává pro příjemce kontext a stává se informací, kterou lze interpretovat.

Na základě této informace může příjemce dále rozvíjet svou znalost. Předpokládejme, že počet bodů je hodnocení z testu, ve kterém je minimální hranice úspěchu stanovena na 100 bodů. V tomto kontextu příjemce získává znalost o úspěšném absolvování testu. Tento příklad ukazuje, jak se data mění v informace a následně ve znalost díky kontextu a interpretaci.

Na základě práce s daty je možné jejich klasifikace na tři základní typy:

<u>Nestrukturovaná data</u> – Jedná se o obrázky, audiovizuální soubory či aplikační logy. Tyto datové typy nelze uchovávat v klasickém RDBMS (relational database management system) a z historického hlediska bylo velmi obtížné jejich zpracování, které se v dnešní době zlepšilo na základě aplikace umělé inteligence a strojového učení.

<u>Strukturovaná</u> – data, která jsou uložena v jednoznačně identifikovaném formátu, většinou popsaném datovém modelu nebo schématu. Typickým příkladem jsou uložená data v relačním databázovém modelu s přesně popsanou hiearchií jednotlivých elementů. Strukturovaná data jsou velmi vážená, protože způsob jejich uložení zajištuje jednoduchou

interpretaci, hledání a vytváření komplexních analýz. Dalším typem, jenž je možné běžné potkat je kupříkladu excel, XML nebo soubor ve formátu JSON.

Polostrukturovaná – určitá kombinace předchozích typů dat. Jedná se o typ, jenž je má určitou úroveň organizace ale nelze jednoduše popsat pomocí datového modelu. Klasickým příkladem může být JSON zachycující záznamy o logách systému. (3,4)

1.1.2 Informační systém

„*Podnikový informační systém vytvářejí lidé, kteří prostřednictvím dostupných technologických prostředků a stanovené metodologie zpracovávají podniková data a vytvářejí z nich informační a znalostní bázi organizace sloužící k řízení podnikových procesů, manažerského rozhodování a správě podnikové agendy*“ (5, s.44)

Hlavní myšlenkou informačního systému by tedy neměl být pouze hardware a software, ale právě sociální aspekt. Jeho hlavním účelem je podporovat činnost organizace, usnadnit rozhodování a řízení, zlepšovat efektivitu a poskytovat uživatelům potřebné informace a nástroje. Informační systémy mohou být v různých formách, od manuálních, papírových systémů až po pokročilé počítačové aplikace a síťové infrastruktury. (30,31)

1.1.3 Klasifikace informačních systémů

Ve firmě lze identifikovat několik organizačních úrovní, které vyžadují specifické metody zpracování informací nebo určitý druh informací. Tyto úrovně zahrnují strategickou, řídící, znalostní a provozní úroveň. Žádná z těchto úrovní nemůže samostatně poskytnout veškeré informace, které management potřebuje pro efektivní řízení. Na druhou stranu, žádná z těchto úrovní nepředstavuje nezávislou, ucelenou jednotku, která by vyžadovala samostatný informační systém.

Proto je často používaná klasifikace, která rozlišuje provozní, znalostní, řídící a strategické informační systémy, založena na teoretickém pohledu na fungování podniku. Hlavním účelem této klasifikace je popsat hodnotu automatizovaného zpracování informací pro zaměstnance na jednotlivých organizačních úrovních.

Provozní úroveň - Tato úroveň vyžaduje zpracování informací souvisejících s běžnými podnikovými činnostmi, jako je realizace výrobních zakázek, nákupy a prodeje, příjem plateb a výplaty atd. Informační systémy na provozní úrovni se zaměřují na řízení každodenních činností a monitorují tok transakcí v rámci organizací, což se často označuje jako transakční nebo provozní systémy. „*Tyto systémy poskytují odpovědi na otázky, jako jsou: Máme*

dostatek komponent na skladě pro montáž zakázky? Proběhla poslední finanční transakce s naším hlavním dodavatelem? Byly všechny dokončené zakázky doručeny na místa určení? Z těchto otázek vyplývá, že informační systémy na provozní úrovni musí poskytovat přesné, aktuální a snadno dostupné informace." (5, s.73). Typickými uživateli těchto informací jsou účetní, provozní pracovníci nebo operátoři dispečinku, kteří pracují s klientskými stanicemi.

Provozní informační systémy jsou klíčové pro efektivní fungování organizace, protože umožňují rychlé a správné rozhodování v běžných situacích. Díky těmto systémům je možné snížit provozní náklady, zlepšit řízení zásob a zvýšit efektivitu pracovníků. Je důležité, aby byly tyto informační systémy navrženy tak, aby byly snadno použitelné a přizpůsobitelné různým potřebám organizace.

Znalostní úroveň – Mimo klientských aplikací podnikového informačního systému (ERP, CRM) jsou na této úrovni zahrnuty i běžné programy používané pro kancelářské potřeby a groupware. Tyto aplikace podporují růst znalostní báze organizace a řídí především tok dokumentů. Odpovídají na otázky, jako jsou: „*Jak reagují zákazníci ve firemní korespondenci na kvalitu naší produkce? Jaké jsou výsledky z posledních schůzek s našimi dodavateli? Jaké jsou aktuální údaje o hospodaření podniku?*" (5, s.73). Informace poskytované těmito aplikacemi představují potenciální znalosti, které se společně s pracovníky podílejí na vytváření zkušeností v provozu podniku. Typickými uživateli aplikací jsou manažeři a technicko-hospodářští pracovníci na všech úrovních.

Znalostní úroveň informačních systémů hraje klíčovou roli ve vytváření konkurenční výhody organizace. Znalostní systémy podporují spolupráci mezi zaměstnanci, sdílení informací a analýzu dat. Vytváření a udržování takových systémů může organizaci poskytnout výhodu v oblasti inovací a rychlosti reakce na změny trhu.

Řídící úroveň - Řídící úroveň informačních systémů je důležitá pro střední a vrcholový management, jelikož poskytuje informace pro administrativní úkoly a podporu rozhodování. Tato úroveň využívá reportingu, který generuje souhrnné výstupy z požadovaných oblastí, například ekonomické výsledky obchodní činnosti. Reporty bývají pravidelně aktualizovány, například týdně.

Klíčovou součástí řídící úrovně jsou také reporty pro nerutinní rozhodování, jako jsou analýzy "co se stane, když". Tyto analýzy umožňují manažerům získat odpovědi na otázky, jako například optimalizace kapacity produkce při zvýšení objemu o 30 %.

V rámci řídící úrovně informačních systémů je také důležité zdůraznit význam flexibilního a efektivního plánování, které umožňuje organizaci rychle reagovat na změny trhu nebo interních podmínek.

Strategická úroveň - informační systémy na této úrovni pomáhají vrcholovému managementu identifikovat dlouhodobé trendy v rámci i mimo organizaci. Hlavním úkolem je odhalit předpokládané změny a zjistit, zda a jak je firma schopna reagovat. Typické otázky, na které strategické informační systémy odpovídají, zahrnují: Jaké jsou dlouhodobé trendy nákladů na produkci v sektoru a jak souvisejí s náklady naší firmy? Jaká úroveň výkonnosti podnikových procesů bude požadována ve vztazích dodavatelů a odběratelů za dva roky?

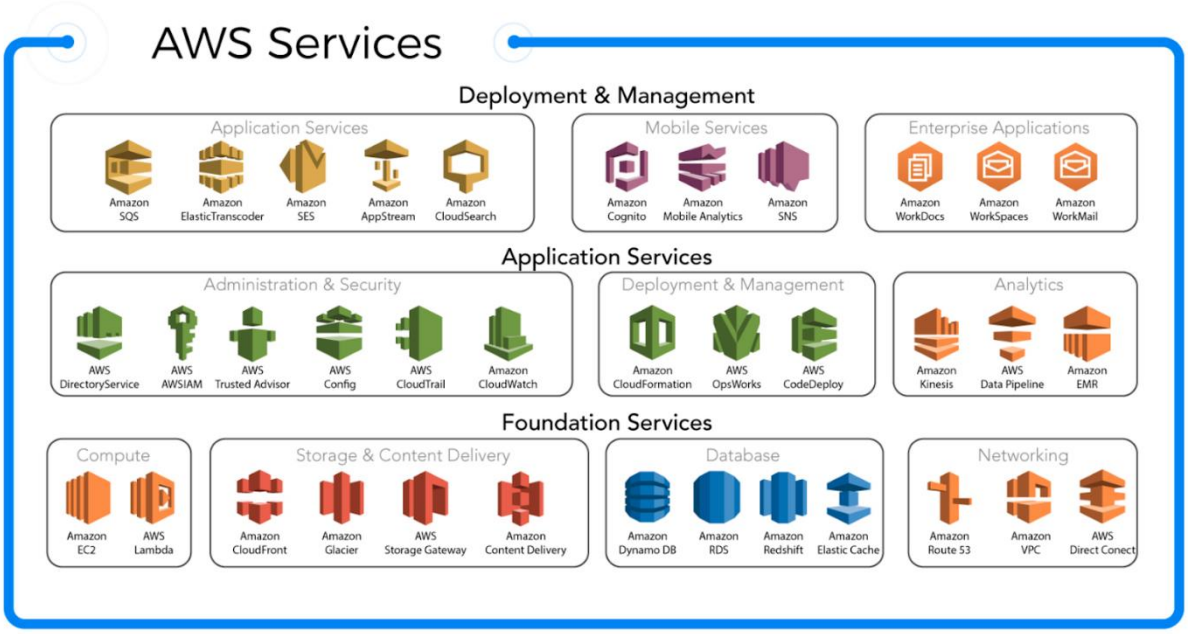
Dále se tyto systémy zaměřují na analýzu konkurence, identifikaci nových trhů a příležitostí pro růst, posuzování rizik spojených s rozvojem nových produktů nebo služeb a sledování technologických trendů, které mohou ovlivnit podnikání. Strategické informační systémy tedy nejen poskytují informace o aktuálním stavu, ale také umožňují vrcholovému managementu plánovat budoucnost a udržet konkurenceschopnost firmy na trhu. (5, 32, 33)

1.1.4 Cloud

Tento pojem není přesně specifikovaný, ale každý informační zdroj ho interpretuje svým vlastním způsobem. Obecně se pod cloudem dá představit síť spojených vzdálených serverů ve stejné síti. Tato síť nabízí uživatelům své služby (kupříkladu hostování webových stránek, poskytování virtuálních počítačů atd.). Podle typu cloudů se rozlišuje i přístup a používání jeho služeb. Této části se podrobně věnuje kapitola 1.1.3 Cloud computing. (6)

Existuje mnoho providerů cloudu, ale dle rozdělení na základě tržního segmentu lze identifikovat následující hlavní poskytovatele cloudových služeb:

AWS – nejznámější poskytovatel cloudových služeb, kdy pokrývá až 32% podílu na trhu. Jeho služby v této oblasti začali od roku 2002 pro své vlastní interní účely. Od roku 2006 pak začala nabízet k pronajmutí virtuální stroje. Jako první ukázala světu nejvíc rozšířený obchodní model používaný ve spojitosti s cloudovými službami – pay as you go, který je rozepsán v kapitole 1.1.3 Cloud computing.



Obrázek 1 Portfolio nejvíce používaných cloudových služeb AWS

(Zdroj: 14)

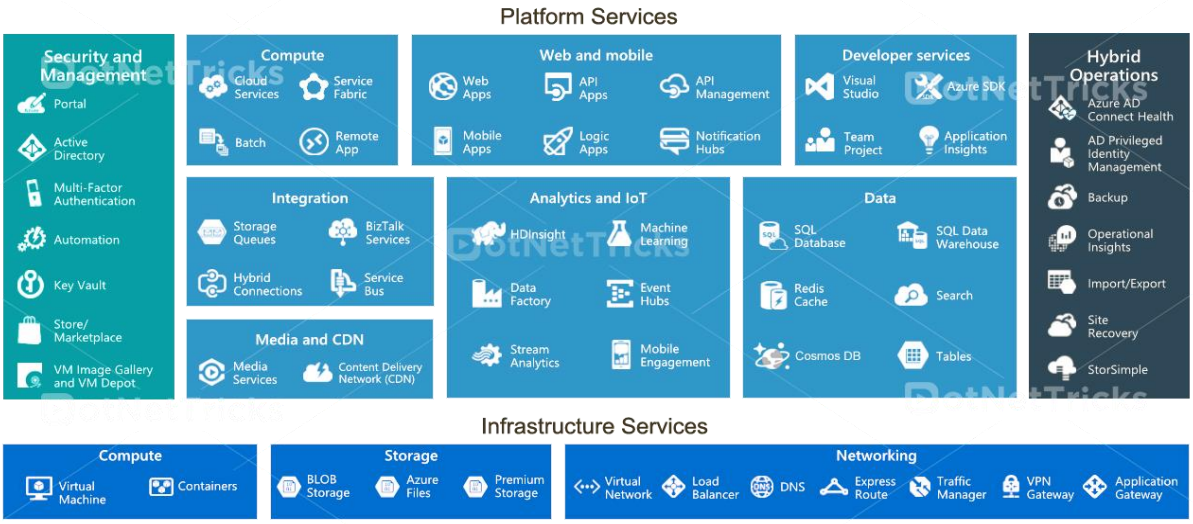
Azure – vytvořen společností Microsoft. Prosadila se jako významná platforma cloud computingu a zaujímá druhé místo v oblasti infrastruktury jako služby (IaaS) a platformy jako služby (PaaS) hned po svém největším konkurentovi na trhu AWS.

V polovině roku 2000 byla služba Microsoft Azure zahájena pod kódovým označením Project Red Dog s cílem dohnat již spuštěnou službu cloud computingu společnosti Amazon. Na konferenci Microsoft Professional Developers Conference v roce 2008 společnost oznámila vytvoření služby Windows Azure, dva roky poté, co společnost AWS představila svou službu Simple Storage Service.

Zpočátku se služba Azure setkala se smíšenými ohlasy, ale Microsoft její služby průběžně vylepšoval a rozšiřoval podporu pro různé programovací jazyky, frameworky a operační systémy včetně Linuxu. V roce 2014 byl systém Windows Azure přejmenován na Microsoft Azure.

Azure nabízí rozsáhlý výběr cloudových služeb rozdělených do čtrnácti sekcí, mezi něž patří výpočetní služby, sítě, úložiště, web + mobilní zařízení, kontejnery, databáze, datová analýza, umělá inteligence a kognitivní služby, internet věcí, a, vývojářské nástroje, monitorování + správa, Microsoft Azure Stack a další. Příklady služeb lze vidět na přiloženém obrázku 2

Mezi hlavní výhody Azure patří bezproblémová integrace se softwarem společnosti Microsoft, zaměření na hybridní výpočetní systémy s Azure Stack, možnosti zabezpečení a dodržování předpisů a živý ekosystém partnerství se společnostmi jako Red Hat, Canonical a Citrix. (7,8)



Obrázek 2 Portfolio nejvíce používaných cloudových služeb Azure

(Zdroj: 15)

Platforma Google Cloud Platform (GCP) se stala jedním z nejlepších dodavatelů veřejných cloudů na světě a připojila se k "velké trojce" Amazon Web Services (AWS) a Microsoft Azure. Cesta GCP začala předběžným vydáním App Engine v dubnu 2008, vývojářského nástroje platformy jako služby (PaaS), který byl navržen tak, aby usnadnil vytváření a škálování webových aplikací na infrastruktuře společnosti Google. Po obdržení zpětné vazby a provedení vylepšení společnost Google v listopadu 2011 oficiálně uvedla App Engine na trh, čímž zahájila éru Google Cloud Platform.

V průběhu uplynulých deseti let GCP rozšířil své služby pod hlavičkou Google Cloud Platform a uspokojil potřeby vývojářů i firem. Odborné znalosti společnosti Google v oblasti provozování datových center a její zdatnost v oblasti analytiky, umělé inteligence a strojového učení jí umožnily poskytovat řadu specializovaných nástrojů a služeb. GCP organizuje své cloudové služby do devíti kategorií: Výpočet, úložiště a databáze, sítě, velká data, internet věcí, strojové učení, identita a zabezpečení, nástroje pro správu a nástroje pro vývojáře.

GCP si získal oblibu u předních společností, jako jsou Snapchat, Airbnb, Zillow, Bloomberg a PayPal, a to z několika důvodů:

Bezpečnost: Model zabezpečení společnosti Google poskytuje škálovatelnou infrastrukturu a inovativní funkce, které organizacím pomáhají udržovat bezpečnost a shodu s předpisy“

Podpora: GCP nabízí všem zákazníkům bezplatnou základní podporu s možností upgradu na prémiovou podporu pro lepší přístup k technikům podpory.

Reputace: GCP je v souladu s pravidly pro poskytování služeb: Díky své zavedené pověsti v technologickém průmyslu je společnost Google důvěryhodnou volbou pro cloudové služby.

Flexibilita: Brian Stevens, technický ředitel Google Cloud, zdůrazňuje, že společnost se snaží o otevřenost a interoperabilitu, což uživatelům zajišťuje flexibilitu.

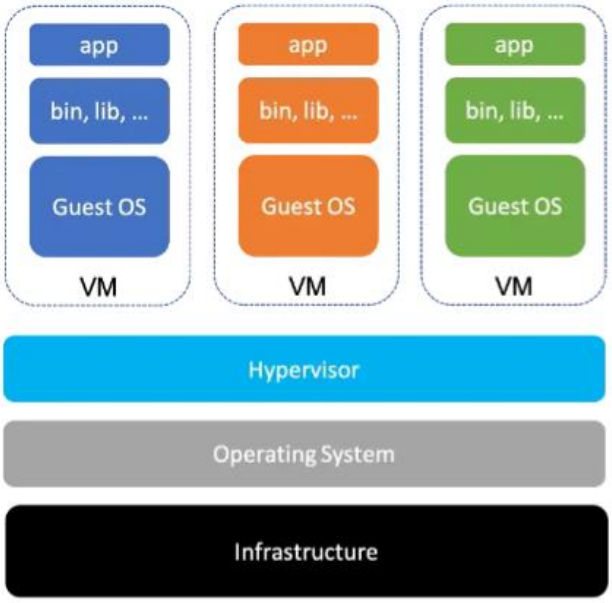
Analytika: Silná stránka společnosti Google v oblasti analýzy a zpracování dat je hnacím motorem nabídky cloudových služeb.

Společnost Google je hrdá na své ceny vstřícné k zákazníkům a tvrdí, že jsou u mnoha výpočetních zátěží v průměru o 60 % levnější než u jiných poskytovatelů cloudových služeb. Díky svému závazku k cenové dostupnosti a specializovaným službám se platforma Google Cloud Platform stala oblíbenou volbou mezi vývojáři a podniky po celém světě.

Vzhledem k tomu, že se Google Cloud Platform nadále vyvíjí a rozšiřuje své služby, zůstává na trhu veřejných cloudů silným konkurentem. Její zaměření na uspokojování potřeb vývojářů spolu s odbornými znalostmi v oblasti velkých dat, analytiky, umělé inteligence a strojového učení staví GCP do pozice přední volby pro podniky a vývojáře, kteří chtějí využít výkon cloudu. (9, 10)

1.1.5 Virtualizace

V případě, kdy je zapotřebí provozovat na jediném zařízení – kupříkladu serveru či počítači více operačních systémů, ať už z důvodu kompatibility programů nebo zefektivnění infrastruktury, kdy je potřeba docílit využití zdroje na plnou kapacitu, je možné využít „virtualizaci“. Systém, který je nainstalován tímto způsobem se nazývá „virtuálním strojem“, kdy tento název plnohodnotně vystihuje koncept. Stejně jako nevirtuální stroj, disponuje vlastním operační systém s vším, co k němu patří – licencí, kernelem atd.



Obrázek 3 Základní části virtualizace

(Zdroj: 16)

Aby na hlavním zařízení mohl fungovat virtuální stroj, je zapotřebí funkční „hypervisor“, pomocí kterého tyto stroje řídí. Virtualizace se stala populární především díky svým přínosům, jak pro technickou část publika – kdy tak i pro management firem, protože představuje optimalizaci nákladů na pořízení a údržbu nových strojů, které mohou běžet na jediném zařízení. (11,12)

Hlavními přínosy virtualizace tedy jsou:

Snížení nákladů firmy – pomocí virtualizace lze provozovat více virtuálních počítačů na jednom fyzickém serveru, čímž se snižuje potřeba dalšího hardwaru. Tato konsolidace snižuje kapitálové výdaje spojené s nákupem, nasazením a údržbou více serverů.

Snížení spotřeby energie – zvlášt v době energetické krize je potřeba co nejvíc šetřit energií. Byť se tato úspora může zdát zanedbatelná, firemní servery jsou často jedním z největších spotřebitelů energie.

Zvýšení možností pro vývoj – oddělení pro vývoj softwaru může těžit z oddělené infrastruktury, kdy může testovat software na virtuálním stroji, aniž by ohrozil chod ostatních využívaných, například v produkci. (11,12,13)

1.1.6 Cloud computing

V češtině volně přeložitelné jako cloudové služby je koncept, kdy uživatel přistupuje vzdáleně ke cloudu. Zde má možnost využívat možností, které mu cloud nabízí. Ty se liší podle typu cloudu, jenž se obecně dělí na veřejné, soukromé „on-premise“ či hybridní variantu. Nejvíce populární a dostupné jsou veřejné, tento typ je volně dostupný pro všechny možné varianty uživatelů.

Zaregistrovat se může běžný uživatel, který si přeje vyzkoušet si cloudové nástroje, mnozí provideři cloudových služeb pak dávají i určitý kredit nebo časově omezenou nabídku využití jinak placených služeb. Příkladem může být Azure subscriptions pro studenty, kdy společnost Microsoft v zájmu rozšíření povědomí o svém produktu nabízí 100 dolarové kredity a několik prémiových služeb zdarma na 12 měsíců. Dalším typem zákazníků, na něž se většina poskytovatelů cloudových služeb (dále „poskytovatelé“) snaží co nejvíc zaměřit jsou firmy.

Pro ně je určena i speciální podpora buď ze strany poskytovatele nebo přes verifikované partnera. Poslední potenciální skupinou klientů se zejména v poslední době stávají státní aparáty. Zde musejí poskytovatelé především cílit na bezpečnost podle platných legislativ dané země. Kvůli tomu je i vyhrazená samostatná platforma pro státní aparáty, v Azure se například jedná o Azure government.

Služby cloudu se liší podle konkrétního poskytovatele, ale obecně se dělí na 3 hlavní kategorie – Iaas, Paas a Saas. (17,18)

Iaas (Infrastructure as service) – do této skupiny lze řadit veškeré prvky spojené s infrastrukturou organizace. Lze sem tedy zařadit veškerý výpočetní výkon – úložiště, síť či virtualizace. Hlavním přínosem této skupiny je jeho škálovatelnost, kterou lze vysvětlit následovně. Považme, že existuje firma, která chce rozšířit svoji infrastrukturu o server pro zvýšení kapacit svých nabízených služeb. Firma, která by neměla přístup ke cloudovým službám by musela identifikovat předpokládaný výpočetní výkon, který server bude potřebovat a podle toho zajistit jeho koupi s požadovanými parametry na operační výkon, velikost disku, paměti atd. Krom těchto původních nákladů na pořízení pak lze očekávat náklady spojené se samotnou údržbou serveru – zajištění serverovny a její ochranu, cenu za elektřinu, náhrady vadných dílů atd. Po vyřízení výše popsaných nákladů by pak firma disponovala svým vlastním serverem, na kterém by úspěšně mohla spouštět další služby svým zákazníkům, ovšem co se stane, pokud služby budou natolik úspěšné, že výpočetní výkon serveru již nebude dostatečný na vyřízení všech klientských požadavků. Společnost by pravděpodobně aplikovala stejný postup jako při nákupu prvního serveru, kdy by mohla přijít o potenciální klienty, než nově objednaný výpočetní výkon dorazí. Pokud by ale stejná společnost měla přístup ke cloudu, mohla by kdykoliv zvýšit výpočetní výkon v rámci pár minut kliknutím na změnu velikosti serveru. Škálovatelnost tak zajištuje změny velikosti serverů podle aktuální situace, kdy tato vlastnost benefituje především v případech, kdy klient neví finální potřebný výkon virtuálního stroje a potřebuje možnost ho změnit v řádech několika minut. V prostředí Azure lze vidět změnu v nastavení virtuálního stroje na níže přiloženém obrázku

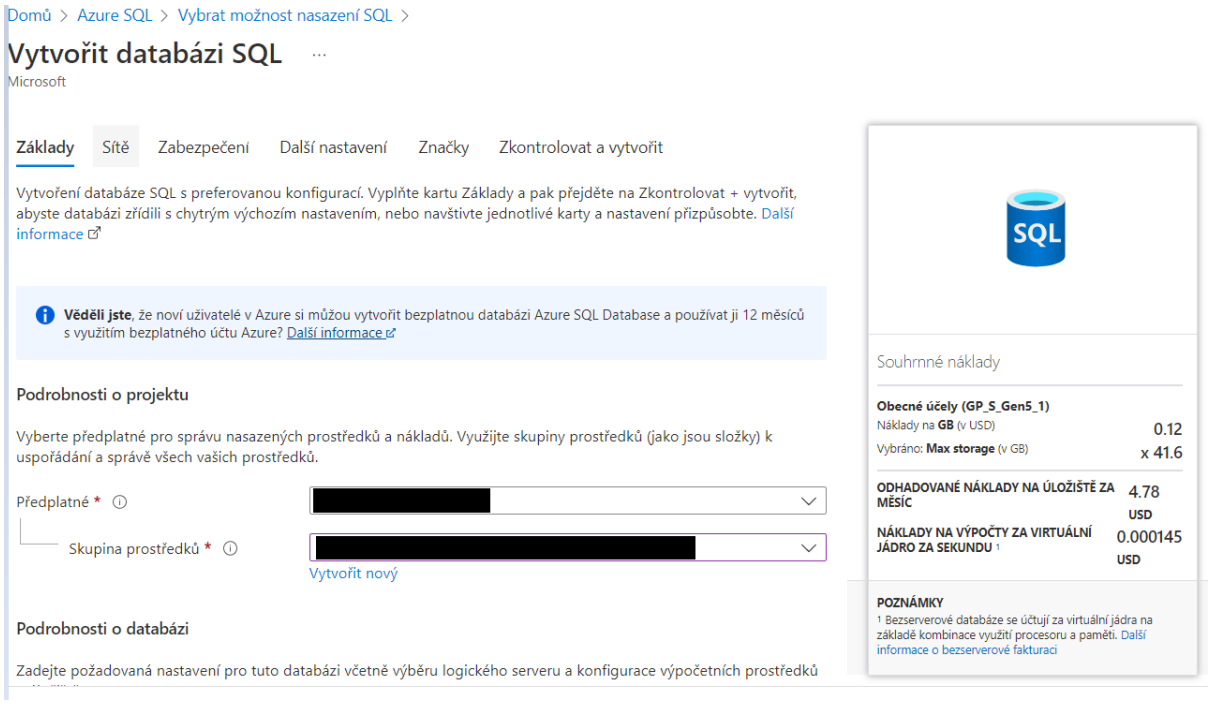
Velikost virtuálního ...	Typ	vCPU	RAM (GiB)	Datové disky	Maximální počet ...	Dočasné úložiště (GiB)	Disk úrovně
Nejvíce používané uživateli Azure	Velikosti, které uživatelé v Azure používají nejvíce						
D-Series v5	Velikosti řady D nejnovější generace doporučené pro obecné účely						
D-Series v4	Velikosti řady D 4. generace pro obecné účely						
B-Series	Ideální pro úlohy, které nevyžadují nepřetržitě celý výkon procesoru.						
DC-Series	Navrženo pro ochranu důvěrnosti a integrity kódu a dat pro úlohy pro obecné účely						
E-Series v5	Velikosti řady E nejnovější generace pro požadavky na velkou paměť						
E-Series v4	Velikosti řady E 4. generace pro požadavky na velkou paměť						
F-Series v2	Až 2× vyšší výkon pro úlohy zpracování vektorů						
L-Series	Vysoká propustnost, nízká latence a přímé mapování na místní úložiště NVMe						
D-Series v3	Velikosti řady D 3. generace pro obecné účely						

Obrázek 4 Typy virtuálních strojů

(Zdroj: 22)

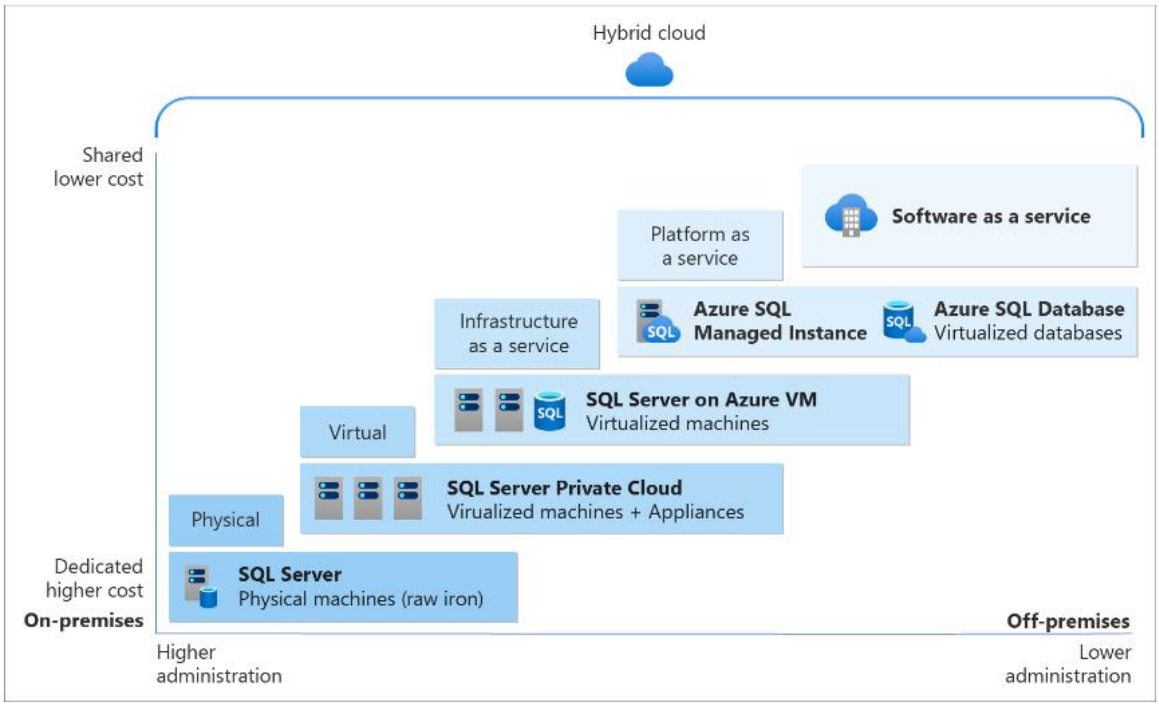
Krom této přínosné vlastnosti IAAS nabízí několik dalších výhod. Zejména zvýšenou bezpečnost nad infrastrukturou, které bychom nad našimi servery nebyli schopni zavést v tak stejné míře jako u poskytovatele cloudových služeb.

PaaS (Platform as a service), kategorie klíčová zejména pro developery v rámci cloudových služeb. Platforma umožnuje vytvářet, testovat a nasazovat aplikace bez nutnosti správy infrastruktury. Právě výše popsaný důvod vede k daleko rychlejší vývoji cloudových aplikací, kdy vývojáři mohou od začátku pracovat na samotném kódu než ztrácet čas nasazováním a administrací infrastruktury. Velký přínosem je kromě rychlosti i cena ušetřená za náklady spjaté s nasazováním aplikací. Vývojáři nepotřebují investovat peníze do hardwaru, který jim poskytuje poskytovatel cloudových služeb, stejně tak pro vývoj aplikací je zde klíčová škálovatelnost – možnost změny výpočetní výkon podle nároků programu. PasS poskytuje velké množství aplikací, které se navzájem dají spojit. Pokud by vývojář například potřeboval vytvořit SQL databázi pro svoji aplikaci, v klasickém řešení by musel implementovat SQL server s jeho vlastní správou. V Azure má možnost nasazení databázového serveru a vytvoření tabulek, do kterých budou zapisovány data pouze v pár krocích, s možností nastavení sítě a zabezpečení – opětovně ušetřený čas, který by jinak musel být vynaložen na „manuální“ konfiguraci firewallů a portů v CLI.



Obrázek 5 SQL databáze

(Zdroj: 22)



Obrázek 6 SQL server z pohledu možností virtualizace

(Zdroj: 23)

Navzdory všem výhodám pramenících z Paas i tato kategorie má své nevýhody. Podle potřeb a nároků programátorů nemusí být Paas nejvhodnější prostředí pro vývoj aplikace z důvodu omezení nastavení infrastruktury. Zatímco vlastní server by poskytoval největší možnost modifikaci všech dostupných možností pro vývoj aplikace, PaaS je omezen co se týče vrstev infrastruktury (Runtime, middleware atd.) a umožnuje pouze pracovat s daty a aplikacemi. Podrobný obrázek lze najít na Obrázku 7, kde jsou znázorněny vrstvy přístupu jednotlivých kategorií IaaS PaaS SaaS.. (19)

Poslední kategorií je SaaS (Software as a Service) - V této kategorii se vývojáři nesnaží vytvořit vlastní aplikaci nebo nasadit hostovaný server, ale aplikace samotná je již vytvořena třetí stranou a na koncovém uživateli cloudových služeb ji zbývá jenom spravovat. V době zpracování této práce nabývá řešení velké popularity, kdy se zvyšuje počet aplikací nabízených ve formě SaaS v prostředí cloudových poskytovatelů.

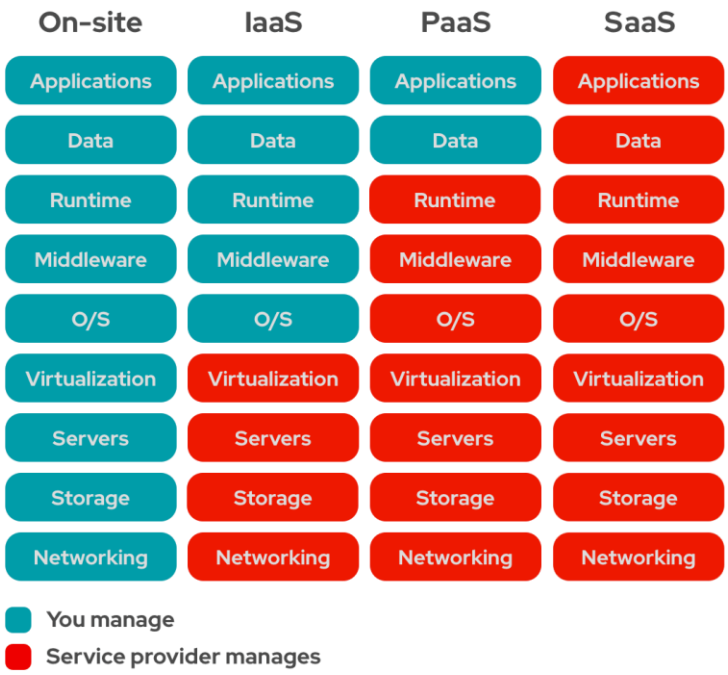
Velkou výhodou je omezení potřeby SW a HW vývoje z hlediska koncového uživatele. Tato část odpovědnosti se předává na poskytovatele aplikace. Zbytek – konfigurace, administrace a správu aplikace pak zařizuje zákazník. I přesto je toto řešení ekonomicky velmi výhodné, je-li vzat v potaz průměrná doba a cena spjatá s variantou vlastního vývoje. V případě času se

jedná až o desítky hodin ušetřeného času, kdy lze začít vykonávat všechny procesy spjaté se sass aplikací. Za další benefity lze považovat zvýšenou bezpečnost aplikace prostřednictvím aktualizací na pravidelné bázi, které mimo jiné přináší i lepší a kvalitnější obsah.

I v této kategorii se každopádně najdou rizika, se kterými se musí koncový zákazník obeznámit pro objektivní zhodnocení pronajmutí SaaS licence. V určitém případě výše popsané benefity mohou být ošemetné – v případě pronajmutí již hotové aplikace může nastat případ, kdy se objeví chyba na straně dodavatele, ať už se jedná o nedostupnost v případě poruchy infrastruktury nebo softwarové chyby, znemožňující práci nebo ovlivňující současné výsledky práce. Zde se objevuje problém i s verzováním, kdy nově vydaná verze bude automaticky nainstalována pro všechny.

V rámci práce je zaměřena podstatná část práce na právě takovou službu – Microsoft Sentinel, jež je podrobně popsán v kapitole 1.2.1 Microsoft Sentinel

Pro přehlednější porovnání jednotlivých částí, za jež je zodpovědný koncový zákazník či poskytovatel služeb v rámci IaaS, PaaS a SaaS lze vidět na následujícím obrázku.



Obrázek 7 Detailní porovnání vrstev IaaS, PaaS, SaaS

(Zdroj: 24)

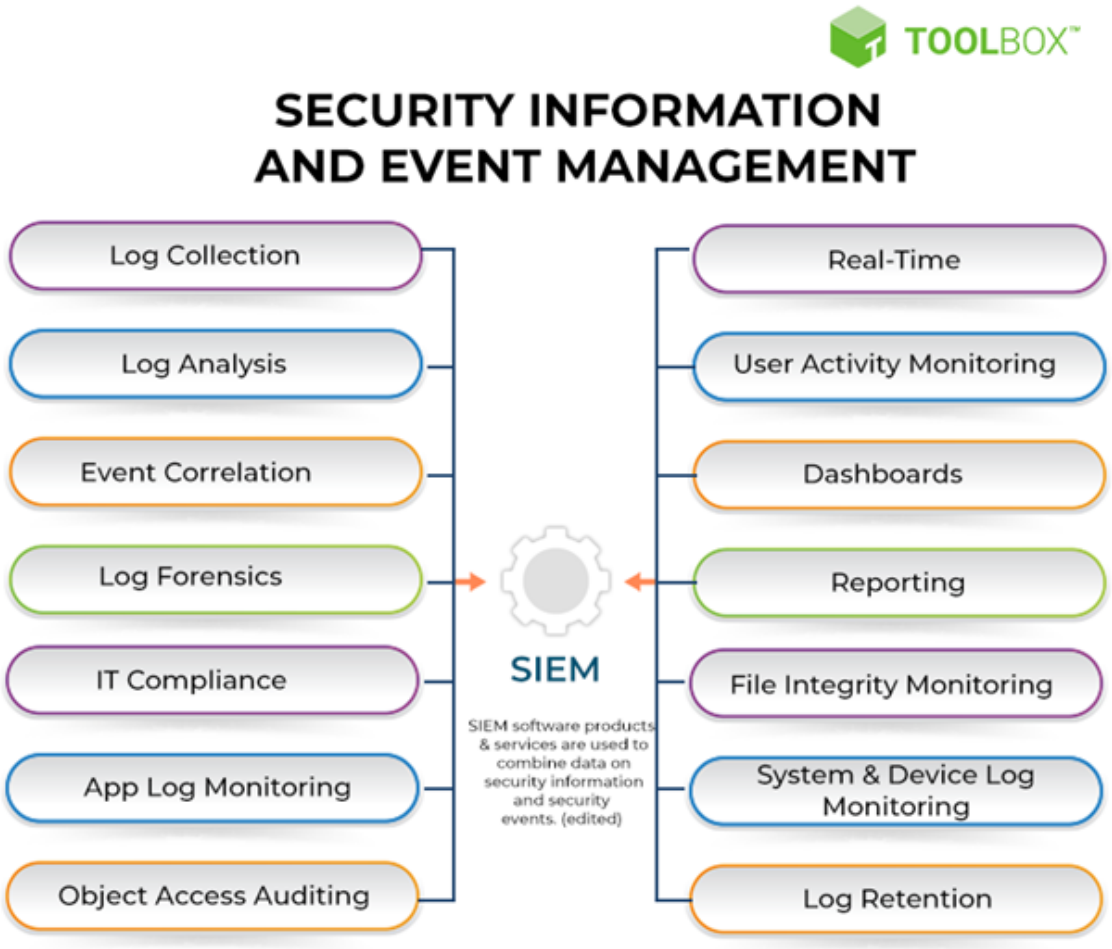
Za jednotlivé služby se účtují podle dvou ekonomických modelů CostEx a OpEx. OpEx neboli Operation Expense je pravidelná platba za používání určité služby, kdy si ji v podstatě pronajímáme, příkladem může být roční platba za licenci k programu a v případě cloudové problematiky do této kategorie spadá virtuální stroj, za který si poskytovatel účtuje hodinové poplatky jeho provozování v závislosti na procesním a operačním výkonu. Model se označuje i jako „pay as you go“. (20,21,25)

1.1.7 SIEM

SIEM, neboli Security Information and Event Management, je pro organizace klíčová technologie, jejímž cílem je centralizovat data protokolů, bezpečnostní výstrahy a události pro monitorování a analýzu zabezpečení v reálném čase. Kombinuje dvě části SEM (Security Event Management) jenž se soustředí na získávání logů, událostí a řízení incidentů. SIM (Security Information Management) slouží pro detailní analýzu a monitoring sesbíraných údajů ze SEM.

Bezpečnostní operační centra (SOC) se spoléhají na software SIEM, aby zvýšily přehled o svém IT prostředí, reagovaly na kybernetické útoky a narušení dat a udržovaly soulad s místními zákony. (26,27,28)

Na níže zobrazeném obrázku lze vidět základní funkce, jenž patří do kompetence SIEM systému



Obrázek 8 Možnosti SIEM systému

(Zdroj: 28)

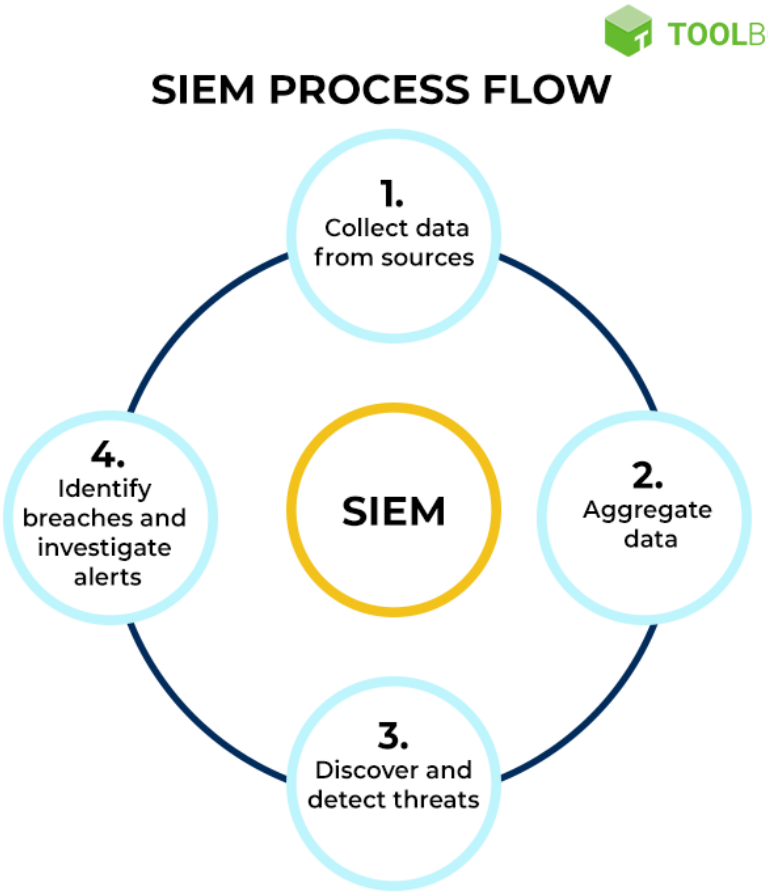
Obecná architektura SIEM by měla splňovat následující body:

- Správu protokolů: Architektura by měla být zodpovědná za sběr dat, správu dat a jejich předchozí uchovávání a shromažďování data jak o událostech, tak i kontextová data z nainstalovaných služeb, zařízení, síťových protokolů, protokolů pro ukládání a protokolů pro streamování.
- Normalizaci protokolu: Tento proces zahrnuje filtrování a odstraňování irelevantních nebo nežádoucích dat ze shromážděných informací a uchovávání pouze relevantních dat pro budoucí analýzu.
- Zdroje protokolů: Logy lze získávat z různých systémů, jako jsou síťové aplikace, bezpečnostní systémy nebo cloudové systémy, se zaměřením na zdroje dat a jejich přenos.

- Hostování SIEM: Systémy SIEM mohou být hostovány pomocí modelů selfhost, cloud-host nebo hybrid-host. Na základě dostupných protokolů identifikují a hlásí nepravidelné nebo škodlivé aktivity.
- Monitorování v reálném čase: Systémy SIEM poskytují řešení pro monitorování v reálném čase, které odhaluje škodlivé útoky, identifikují jejich původ, předpovídají hrozby a přijímají potřebná opatření, aby se zabránilo případnému úniku dat.

Univerzální princip, na kterém operuje každý SIEM se dá popsat do několika bodů. V prvním kroku je potřeba sesbírat veškerá data z monitorovaných zařízení. Sběr dat může probíhat dvěma způsoby. Prvním z nich je automatizovaný způsob, kdy se pomocí nainstalovaného logovacího agenta extrahují potřebné informace, často ve formátu syslog. Druhým způsobem je sběr dat v reálném čase prostřednictvím streamovacích protokolů.

V dalším kroku je nutné získaná data zpracovat a agregovat do funkčního a použitelného formátu. Při správě dat je třeba dbát na obecné požadavky, jako je důkladné zabezpečení datových úložišť, ať už ve formě cloudu či on-premise řešení. Dále je důležitá strukturalizace dat na základě relevance a priority. Nejdůležitější data monitorovaná v reálném čase by měla být uložena v úložišti s vysokým výkonem, zatímco "studená" data určená pro archivaci a pozdější analýzu by měla být umístěna na úložiště s nižšími náklady. (28,29)



Obrázek 9 Cyklus SIEM systému

(Zdroj: 28)

V dalším kroku dochází k analýze dat pro zjištění potencionálních hrozeb. V této fázi se SIEM zaměřuje na identifikaci potenciálních hrozeb a zranitelností v síti organizace. Systém na základě získaných dat vytváří komplexní přehled o stavu sítě. Na shromážděná data se pak aplikují pokročilé analytické nástroje, jako je strojové učení a korelační pravidla, které identifikují vzory nebo anomálie, jež by mohly znamenat bezpečnostní hrozbu.

Po zjištění potenciální hrozby nebo zranitelnosti přechází systém SIEM do fáze identifikace a vyšetřování. Tento proces zahrnuje určení povahy a rozsahu bezpečnostního incidentu a posouzení jeho potenciálního dopadu na organizaci. Cílem je rychle identifikovat a ověřit narušení bezpečnosti, aby se minimalizovaly škody a zahájila vhodná odezva.

Proces identifikace narušení a vyšetřování výstrah zahrnuje:

- Stanovení priorit výstrah na základě jejich závažnosti, potenciálního dopadu a dalších relevantních faktorů s cílem zaměřit se na nejkritičtější incidenty.

- Provedení podrobné analýzy incidentu, včetně postižených systémů, potenciálních vstupních bodů a rozsahu narušení.
- Shromažďování dalších souvislostí a informací z různých zdrojů, jako je inventář prostředků, údaje o zranitelnostech a aktivita uživatelů, aby bylo možné lépe porozumět incidentu.
- Ověřování výstrah porovnáváním se známými falešnými poplachy, historickými daty a informacemi o hrozbách, aby se minimalizovaly falešné poplachy a zajistila přesnost.
- Spolupráce s bezpečnostními týmy, analytiky a dalšími zúčastněnými stranami s cílem sdílet informace, shromažďovat poznatky a koordinovat reakci na incident. (28,29)

1.2 POUŽITÉ TECHNOLOGIE

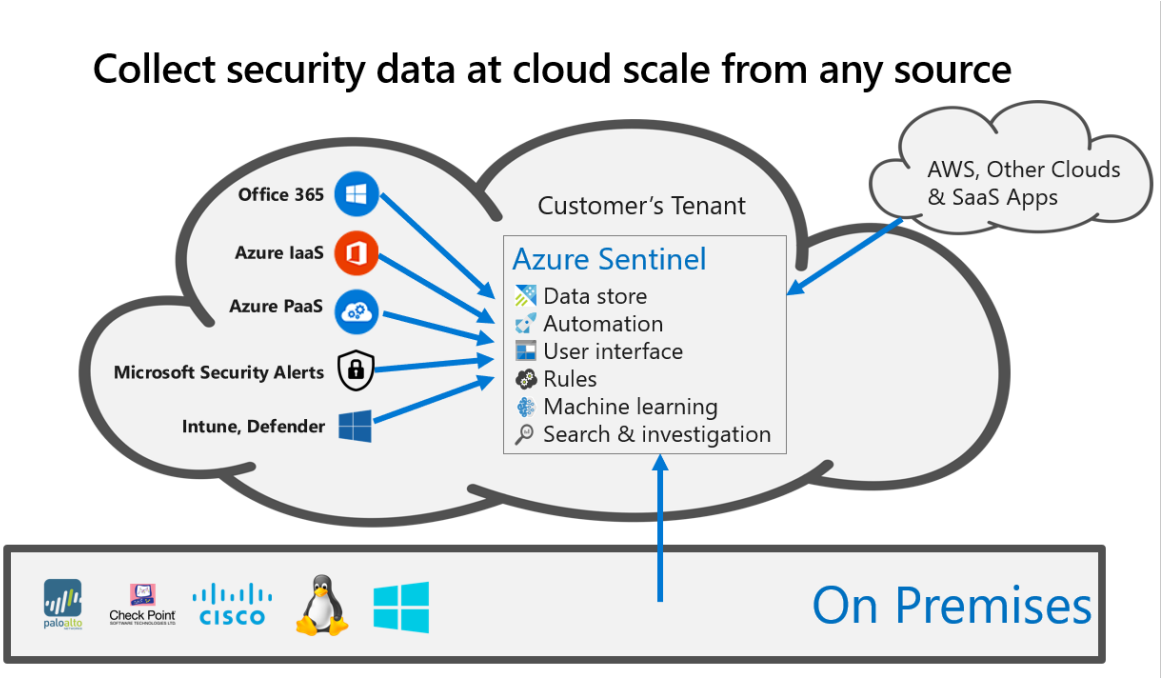
Nástin technologií, jež byly použity v rámci práce byly nastíněny v kapitole Cíle práce. Práce slouží ke spojení starého informačního systému s nově přidaným (Grafanou) k tomu je zapotřebí se seznámit, jak s technologiemi, na kterých funguje současný systém, tak i nově implementovaný.

1.2.1 Microsoft Sentinel

K zajištění potřebným dohledem nad reportováním kyberbezpečnostních hrozeb je v dnešní době dodáváno mnoho systémů, podle ceny, provedení, množství dostupných služeb a optimalizace. Společnosti se také snaží stále více přecházet do cloudu nebo delegují pouze určitou část svých služeb a vytváří takzvané „hybridní“ modely, kdy část systému běží na on premise řešení a nová v cloudu. V diplomové práci se použil System Information Event Management – zkráceně S.I.E.M systém, jenž funguje pouze v cloudovém prostředí Microsoft Azure. Můžeme ho nalézt jako produkt Microsoftu pod názvem Microsoft Sentinel. Veřejnosti se Sentinel představil v roce 2019, kdy uživatelům nabídl systém spojující umělou intelligence a možnosti platformy Azure, sám Microsoft při zahájení uvedl “*Začátkem tohoto týdne jsme oznámili, že služba Azure Sentinel je nyní všeobecně dostupná. To představuje důležitý milník na naší cestě k nové definici správy bezpečnostních informací a událostí (SIEM) pro éru cloudu.*” (34) Samotný potenciál Sentinelu si všimly i technologické společnosti, zejména pak Forrester, jež vydal hodnocení SIEM služeb mezi krom Sentinelu nechyběli ani ty nejlépe hodnocené jako Splunk či IBM Security a kde se Azure sentinel umístil jako nejlepší z pohledu strategie. (34, 35)

Nástroj se skládá z několika komponentů, které zajištují funkční prostředí pro detekování hrozeb a útoků v kybernetickém prostředí

Prvním jsou datové zdroje. Azure Sentinel nabízí enormního množství datových zdrojů ať ze samotného cloudového prostředí – Azure IaaS, PaaS platforem či Office nebo on-premise.



Obrázek 10 Proces sbírání logů

(Zdroj: 39)

Obecně se pro sbírání dat používá několik metod:

- Microsoft monitoring agent – součást Azure systému, umožnuje sbírat telemetrii z operační systém windows a linux či dalších aplikací jako windows firewall
- Remote connection - Datové konektory pro vzdálené připojení usnadňují sběr dat ze vzdálených zařízení a systémů, jako jsou firewally a síťová zařízení. Tyto konektory obvykle používají k přenosu dat protokolů do Azure Sentinel protokoly jako Syslog a Common Event Format (CEF). Mezi příklady zdrojů dat vzdálených připojení patří Cisco ASA, Fortinet FortiGate a firewally Palo Alto Networks.
- Cloud connection - Datové konektory pro připojení ke cloudu jsou určeny ke shromažďování a přijímání dat z různých cloudových služeb a aplikací. Tyto konektory používají rozhraní API k bezpečné komunikaci s poskytovateli cloudových služeb a k přenosu dat protokolů a událostí do služby Azure Sentinel. Mezi příklady zdrojů dat cloudového připojení patří Amazon Web Services (AWS), Microsoft 365 Defender a Google Workspace.
- Cloud native connection - Datové konektory nativního připojení ke cloudu jsou navrženy speciálně pro služby Microsoft Azure. Tyto konektory jsou optimalizovány pro bezproblémovou integraci se službami Azure a mohou automaticky přijímat protokoly a události z různých zdrojů Azure. Mezi příklady datových zdrojů nativního

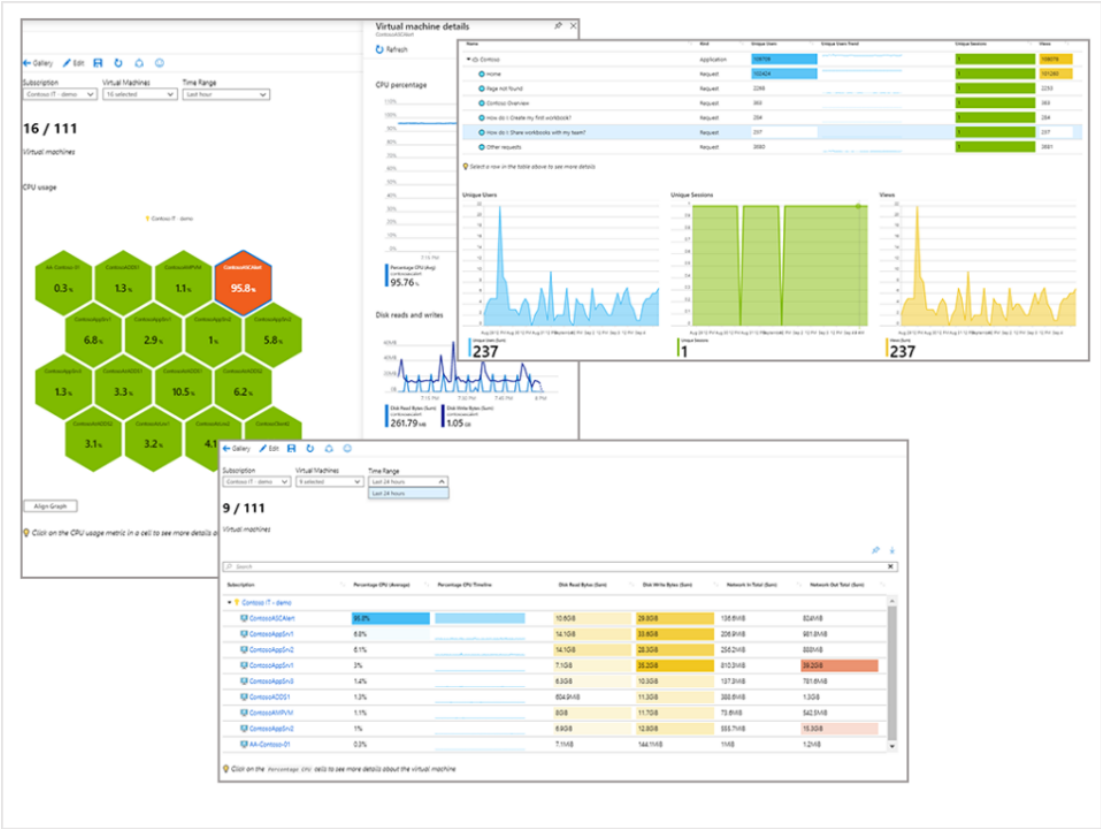
připojení ke cloudu patří Azure Active Directory, Azure Security Center a Azure Firewall.

- Custom connection - Datové konektory vlastního připojení umožňují organizacím vytvářet vlastní datové konektory pro příjem dat ze zdrojů, které nejsou podporovány vestavěnými konektory Azure Sentinel. Může se jednat o proprietární systémy, aplikace nebo zařízení IoT. Vlastní konektory obvykle zahrnují psaní skriptů nebo použití funkcí Azure Functions a Logic Apps k přijímání dat do Azure Sentinel. To poskytuje flexibilitu při plnění specifických obchodních požadavků a integraci jedinečných zdrojů dat pro analýzu a detekci hrozeb.

Po zajištění dostupnosti a přístupu k datům je možné přistoupit k jejich zpracování a vizualizaci. Za tímto účelem nabízí Azure Sentinel komponentu nazvanou Workbooks, jedná se o interaktivní ovládací panely, které kombinují vizualizace dat, dotazy a uživatelské vstupy a poskytují komplexní a přizpůsobitelný pohled na kyberbezpečností situace sledovaného prostředí. Jsou postaveny na službě Azure Monitor Workbooks, která uživatelům umožňuje vytvářet vlastní interaktivní sestavy a vizualizace s využitím dat z různých zdrojů. Azure Sentinel Workbooks čerpají z právě výše popsaných zdrojů dat, které zpracovávají na základě jazyka KQL, jenž je podrobně popsán v 1.2.4 KQL.

Mezi výhody Workbooků lze zařadit automatizaci a propojení s platformou Azure, kdy lze napojit Azure logic apps a tak zefektivnit procesy svázané s hledáním incidentů.

Mezi nevýhody lze zařadit omezenost vizualizací a nepřívětivá práce s nastavením designu celého dashboardu, kdy je Azure značně limitován. (35, 36)



Obrázek 11 Vizualizace grafů v Sentinelu

(Zdroj: 40)

Významnou součástí Sentinelu jsou i analytická pravidla pro detekování hrozeb. Ve chvíli, kdy se napojí datový konektor je zapotřebí zautomatizovat dohled nad hlídanými daty. Analytická pravidla vytvořená pro tento účel se dají vytvořit přes již zhotovené šablony nabízené zdarma Sentinelem. Dají se rovněž vytvořit i manuálně nakonfigurovat na základě našich požadavků a kritérií. Stejně jako Workbooks i zde je pro tvorbu pravidel využit jazyk KQL, jenž je popsán v kapitole 1.2.4 KQL. Pro analyzování hrozeb jsou plně k dispozici různé varianty strojového učení, ať ve formě předpřipravených algoritmů strojového učení pro různé případy použití, jako je detekce vzácných nebo neobvyklých procesů, identifikace podezřelých vzorů ověřování a dalších nebo vlastní verzí pro specifické potřeby organizace. (36,38)

21
Active rules

Rules by severity

High (5) | Medium (16) | Low (0) | Informational (0)

Active rules | Rule templates

Search | Severity : All | Rule Type : All | Status : All | Tactics : All | Techniques : All

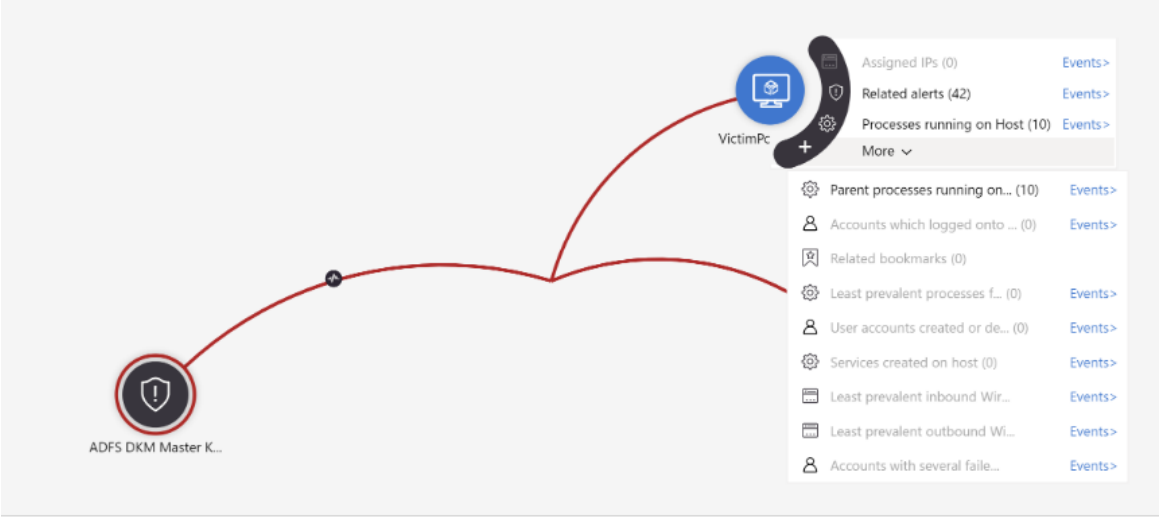
SEVERITY	NAME	RULE TYPE	DATA SOURCES	TACTICS
Medium	Suspicious number of resource creation or deplo...	Scheduled	Azure Activity	Impact
Medium	High Number of Urgent Vulnerabilities Detected	Scheduled	Qualys Vulnerability Management ...	Initial Access
Medium	Suspicious application consent similar to PwnAuth	Scheduled	Azure Active Directory	
Medium	User account enabled and disabled within 10 mins	Scheduled	Security Events	
Medium	Malware in the recycle bin	Scheduled	Security Events	Defense Evasion
Medium	TI map IP entity to GitHub_CL	Scheduled	Threat Intelligence Platform... +1	Impact
Medium	SharePointFileOperation via previously unseen IPs	Scheduled	Office 365	Exfiltration
Medium	Multiple users email forwarded to same destinati...	Scheduled	Office 365	
Medium	Port Scan Detected	Scheduled	Sophos XG Firewall (Preview)	Discovery
Medium	User account created and deleted within 10 mins	Scheduled	Security Events	
Medium	Potential Password Spray Attack	Scheduled	Okta Single Sign-On (Preview)	Credential Access

Obrázek 12 Prostředí pravidel pro identifikování incidentů

(Zdroj: 40)

Pro identifikace incidentu lze podrobně prozkoumat vlastnosti a příčiny jeho vzniku. Za tímto účelem existuje v Sentinelu vlastní část Investigate. Zde, lze z grafického zpracování incidentu vyčíst rozsah a hlavní příčinu pomocí korelace dat svázaných s incidentem.

Veškeré informace spojené s identifikací incidentu lze jednoduše identifikovat v grafickém prostředí. Prostředí nabízí analytikovi automaticky generované otázky vytvořené specialisty v oboru. (37)



Obrázek 13 Grafické prostředí pro identifikaci incidentu

(Zdroj: 37)

1.2.2 Azure VM

Virtuální počítače Azure (VM) jsou základní součástí nabídky infrastruktury jako služby (IaaS) Microsoft Azure, která umožňuje firmám a vývojářům nasazovat a spravovat virtuální počítače v plně spravovaném, bezpečném a škálovatelném cloudovém prostředí.

Virtuální počítače Azure jsou virtualizované výpočetní prostředky hostované v globální infrastruktuře datových center Microsoft Azure. Nabízejí uživatelům flexibilní, nákladově efektivní a snadno škálovatelné řešení pro provoz aplikací a služeb v cloudu bez nutnosti nákupu a údržby fyzického hardwaru. Virtuální počítače Azure podporují širokou škálu operačních systémů, včetně systémů Windows, Linux a dalších platforem s otevřeným zdrojovým kódem, a lze je přizpůsobit různým hardwarovým konfiguracím tak, aby splňovaly konkrétní požadavky.

Popularita a výhody pramenící z IaaS se dají rozdělit následovně:

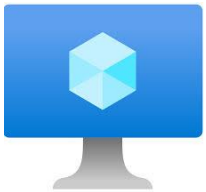
Škálovatelnost – Jednou z hlavních výhod virtuálních počítačů Azure je jejich škálovatelnost. Virtuální počítače lze rychle poskytovat nebo odebírat podle potřeby, což podnikům umožňuje reagovat na měnící se pracovní zátěž a poptávku. Virtuální počítače Azure lze také automaticky škálovat, čímž se počet instancí virtuálních počítačů automaticky upravuje na základě předem definovaných pravidel a metrik. Tato výhoda byla rozepsána již v Kapitole 1.1.6 Cloud computing

Vysoká dostupnost a spolehlivost – virtuální počítače Azure jsou navrženy s ohledem na vysokou dostupnost a spolehlivost. Oba termíny společnost Microsoft ve své oficiální dokumentaci pro Azure označuje následovně: “Spolehlivost se skládá ze dvou principů: odolnosti a dostupnosti. Cílem odolnosti je vrátit aplikaci do plně funkčního stavu po selhání. Cílem dostupnosti je poskytnout uživatelům konzistentní přístup k aplikaci nebo úloze podle potřeb“. (41) Tím že jsou virtuální počítače hostovány na redundantním hardwaru a síťové infrastruktuře, zajišťuje, že zůstanou v provozu i v případě selhání hardwaru. Kromě toho lze virtuální počítače Azure nasadit ve více datových centrech nebo regionech, což zajišťuje geografickou redundanci a dále zvyšuje odolnost aplikací a služeb.

Zabezpečení - ochrana virtuálních počítačů představuje pro Azure nejvyšší prioritou a obsahuje řadu vestavěných funkcí, které chrání virtuální počítače a jejich data před potenciálními hrozbami. Mezi tyto funkce patří např:

- Azure Security Center: Centrum zabezpečení Azure: Monitoruje virtuální počítače z hlediska potenciálních bezpečnostních zranitelností a poskytuje doporučení pro zlepšení zabezpečení.
- Brána Azure Firewall: Zajišťuje zabezpečení na úrovni sítě filtrováním provozu na základě IP adres, portů a protokolů.
- Skupiny zabezpečení sítě (NSG): Umožňují jemnou kontrolu nad příchozím a odchozím síťovým provozem do virtuálních počítačů.
- Šifrování disků Azure: Šifrování disků virtuálních počítačů pomocí standardních šifrovacích algoritmů pro ochranu dat v klidovém stavu.
- Azure Private Link: Poskytuje bezpečné, soukromé připojení mezi virtuálními počítači a dalšími službami Azure.

Další výhodou získanou v hostingu v cloudovém prostředí je rozsáhlý ekosystém cloudových služeb, které se mezi sebou mohou propojovat a mohli tak spolupracovat s dalšími službami jako je Azure Active Directory (Azure AD), Azure Managed Identities, Azure Storage a Azure SQL Database. Tato integrace umožňuje uživatelům vytvářet komplexní, víceúrovňové aplikace a služby, které využívají celou škálu možností Azure. (41)



Obrázek 14 Logo VM v portálu Azure

(Zdroj: 41)

1.2.3 Azure managed identities

Azure Managed Identities (AMI) je funkce poskytovaná službou Microsoft Azure, která zjednodušuje proces správy a zabezpečení přístupu k různým službám a prostředkům Azure. Je součástí služby Azure Active Directory (Azure AD) a nabízí automatický, bezproblémový a bezpečný způsob správy identit služeb, díky němuž vývojáři nemusí spravovat pověření ručně. Spravované identity existují proto, aby řešily problémy spojené se správou identit služeb a ověřováním, zejména v rozsáhlých a složitých cloudových prostředích.

Používají se v různých službách Azure, jako jsou virtuální počítače, služby App Services, funkce Azure Functions a instance kontejnerů, k bezpečnému přístupu k dalším zdrojům Azure, jako jsou úložiště Azure Storage, Azure SQL a trezor klíčů Azure Key Vault.

Přiřazením spravované identity prostředku Azure udělíte tomuto prostředku jedinečnou identitu v Azure AD, kterou lze použít k ověřování a autorizaci přístupu k dalším prostředkům v rámci předplatného Azure.

Obecně dělíme 2 typy přiřazených identit:

- Spravovaná identita přiřazená systémem:
  Tyto identity jsou automaticky vytvořeny a vázány na konkrétní prostředek Azure, například virtuální počítač nebo funkci Azure. Při odstranění prostředku se odstraní i přidružená spravovaná identita.
- Spravovaná identita přiřazená uživatelem:
  Na rozdíl od spravovaných identit jsou vytvářeny nezávisle na konkrétním prostředku Azure a mohou být přiřazeny k více prostředkům. To umožňuje sdílení spravované identity napříč různými zdroji a poskytuje flexibilnější a granulárnější přístup k řízení přístupu.

Nabízené řešení tak odstraňuje potřebu spravovat a ukládat autentizační údaje, jako jsou uživatelská jména, hesla nebo tajné klíče, v rámci aplikací. Azure se stará o celý životní cyklus těchto identit, včetně vytváření, mazání a automatických udílení pověření. Pomocí spravovaných identit snižujete riziko úniku pověření a minimalizujete plochu pro útoky.

Velmi vhodným aspektem je nativní podpora IAM různými službami Azure, kdy lze je snadno integrovat se službou Azure Role-Based Access Control (RBAC) pro správu přístupových oprávnění.:

Delegováním správy identit služeb na Azure se organizace mohou soustředit na zabezpečení svých aplikací a dat a zároveň snížit administrativní režii spojenou se správou pověření.

V kontextu diplomové práce se Azure managed identity používá pro zajištění přístupu mezi nově implementovaným SIEM systémem na bázi Grafany a Azure Sentinelem, jenž je primárním systémem pro monitoring incidentů. (42)

Obrázek 15 Logo Managed Identity v portálu Azure

(Zdroj: 42)

1.2.4 KQL

Microsoft popisuje KQL následovně: „Jazyk Kusto Query Language je výkonný nástroj pro zkoumání vašich dat a odhalování vzorů, identifikaci anomálií a okrajových hodnot, vytváření statistických modelů a další.“

Jazyk Kusto Query Language (KQL) je výkonný dotazovací jazyk určený pro vytváření dotazu nad velkými datovými sadami a používá se především s aplikacemi Azure Data Explorer, Azure Log Analytics a Azure Application Insights. Byl vytvořen v roce 2014 jako součást již zmíněného produktu Microsoftu Azure Data s cílem řešit problémy, kterým organizace čelí při zpracování velkého množství dat generovaných moderními aplikacemi, zařízeními internetu věcí a webovými službami. S rychlým nárůstem objemu, rozmanitosti a rychlosti dat se tradiční dotazovací jazyky a techniky zpracování dat staly méně efektivními při poskytování včasných a relevantních informací. Jazyk KQL je navržen tak, aby tato omezení překonal tím, že nabízí výraznější, efektivnější způsob zkoumání a analýzy dat.

Syntaxe jazyka KQL vychází z celosvětově známého jazyka SQL (Structured Query Language) skládá z řady příkazů, přičemž každý příkaz pracuje s výstupem předchozího příkazu. K oddělení příkazů se používá symbol roury (|) a každý příkaz obvykle obsahuje sloveso následované sadou argumentů. Mezi běžné operátory jazyka KQL patří:

„|“: Operátor pipe se používá k předání výstupu jednoho příkazu dalšímu příkazu v dotazu.

„==“: Operátor rovnosti, který se používá k porovnání dvou hodnot.

„!=“: Operátor nerovnosti, který se používá pro porovnání dvou hodnot.

„>“ a <: Operátory větší než a menší než se používají k porovnávání hodnot.

„>=“ a <=: Operátory větší nebo rovno a menší nebo rovno, používané pro porovnávání hodnot.

„and“ a „or“: Logické operátory používané ke kombinování výrazů.

„in“ a „!in“: Operátory příslušnosti k množině, které se používají ke kontrole, zda hodnota existuje nebo neexistuje v množině.

Chceme-li vytvářet komplexnější dotazy, KQL disponuje funkcemi pro pokročilejší manipulaci s daty:

project: Vybere konkrétní sloupce ze vstupních dat.

extend: Přidá ke vstupním datům nové vypočtené sloupce.

summarize: Seskupí data podle zadaných sloupců a provede agregační funkce.

where: Filtruje data na základě zadané podmínky.

join: slouží ke spojení dat: Spojí data ze dvou tabulek na základě společného sloupce.

top: Vrátí N nejlepších záznamů na základě zadaného pořadí.

take: Omezí výstup na zadaný počet záznamů.

Potřeba jazyka KQL v oblasti kybernetické bezpečnosti vyplývá z rostoucí složitosti a sofistikovanosti kybernetických hrozeb. Bezpečnostní odborníci musí procházet obrovské množství dat protokolů, výstrah a telemetrických informací, aby identifikovali potenciální narušení bezpečnosti a zranitelnosti. Jazyk KQL umožňuje bezpečnostním analytikům psát složité dotazy, filtrovat a agregovat data a odhalovat skryté vzorce, které mohou znamenat kybernetický útok nebo bezpečnostní problém.

Jednoduchost a objem zvládání enormního počtu dat patří bezesporu mezi hlavní výhody jazyka KQL. Mimo jiné analytici v bezpečnostních operačních centrech (SOC) těží i z několika dalších benefitů. Jedním je i vestavěná podpora časových funkcí, které vám pomohou efektivně agregovat, manipulovat a analyzovat časová data jako je například range nebo timestamp. Velmi výrazným přínosem je již zmíněna podpora ekosystému Azure, kdy mohou specialisté využívat dalších prvků IaaS, PaaS a SaaS k rozšiřování systémů či zlepšování stávajích bezpečnostních řešení. (43)

Obrázek 16 Logo Kusto Log Analytics v portálu Azure

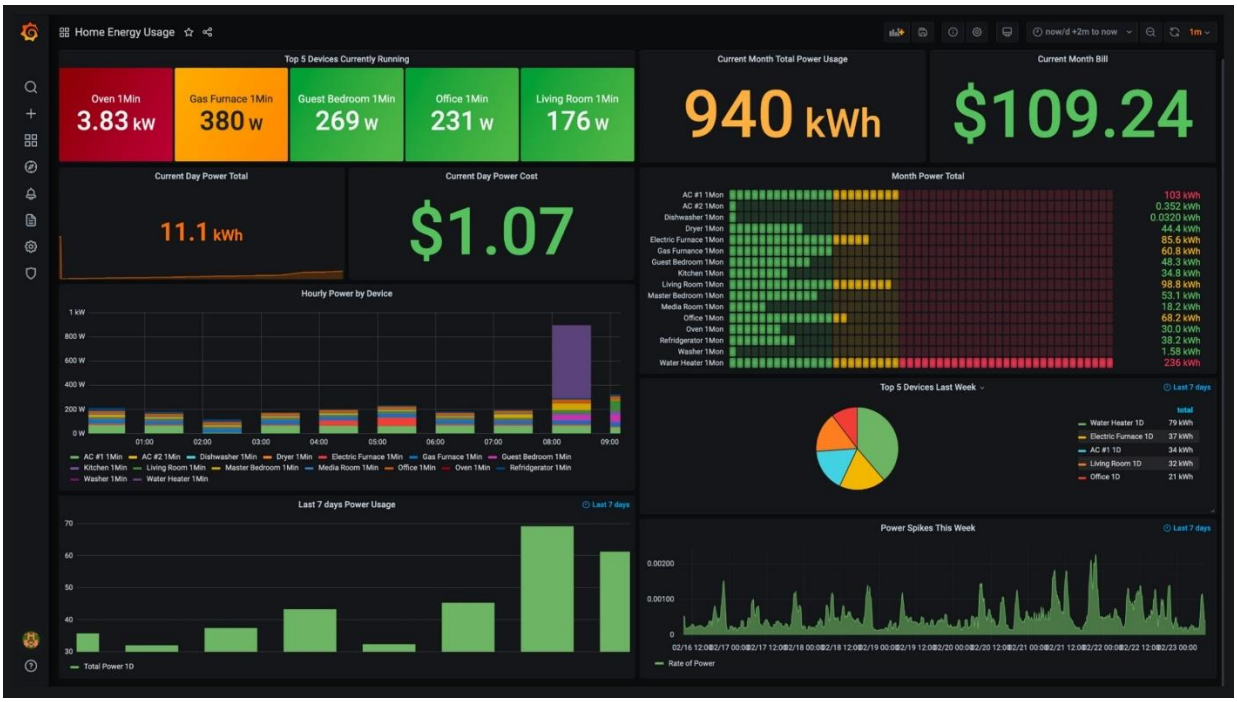
(Zdroj: 43)

1.2.5 Grafana

Grafana je open-source nástroj pro vizualizaci a monitorování dat, který uživatelům umožňuje vytvářet interaktivní panely pro sledování a analýzu různých typů dat v reálném čase. Je hojně využíván inženýry, správci a datovými nadšenci ke sledování, zkoumání a analýze dat z nejrůznějších zdrojů. Grafana je vysoce přizpůsobitelná a podporuje více zdrojů dat, což z ní činí atraktivní řešení pro různé případy použití.

Grafana nabízí řadu možností vizualizace, které jsou uspořádány do panelů, z nichž lze sestavit vlastní ovládací panely. Tyto panely mohou zobrazovat různé typy grafů, protokolů a upozornění podle zdroje dat přiřazeného k panelu. Uživatelé mohou také navrhovat a přidávat vlastní panely pomocí pluginů, díky open-source povaze Grafany.

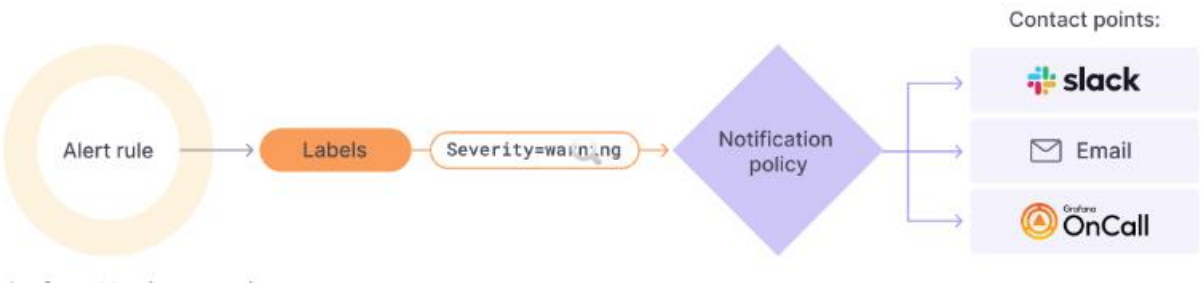
Na základě různých panelů dokáže vizualizovat složité datové sady ve snadno srozumitelné podobě. To je důležité zejména v dnešním světě založeném na datech, kde se denně generují a analyzují obrovská množství. Vizualizace umožňuje uživatelům rychle identifikovat vzory, trendy a anomálie v datech.



Obrázek 17 Dashboard v Grafaně

(Zdroj: 44)

Další důležitou funkcí Grafany je nativní možnost upozornění Grafany, která je klíčová pro udržení zdravých systémů a snížení prostojů. Software nabízí vestavěnou podporu pro širokou škálu oznamovacích kanálů, jako je e-mail, Slack a PagerDuty. Uživatelé mohou vytvářet a konfigurovat pravidla upozornění, která slouží jako spouštěče oznámení, a zajistit tak, aby byli informováni, když se něco pokazí nebo když je porušeno nějaké pravidlo.



Obrázek 18 Proces upozornění v Grafaně

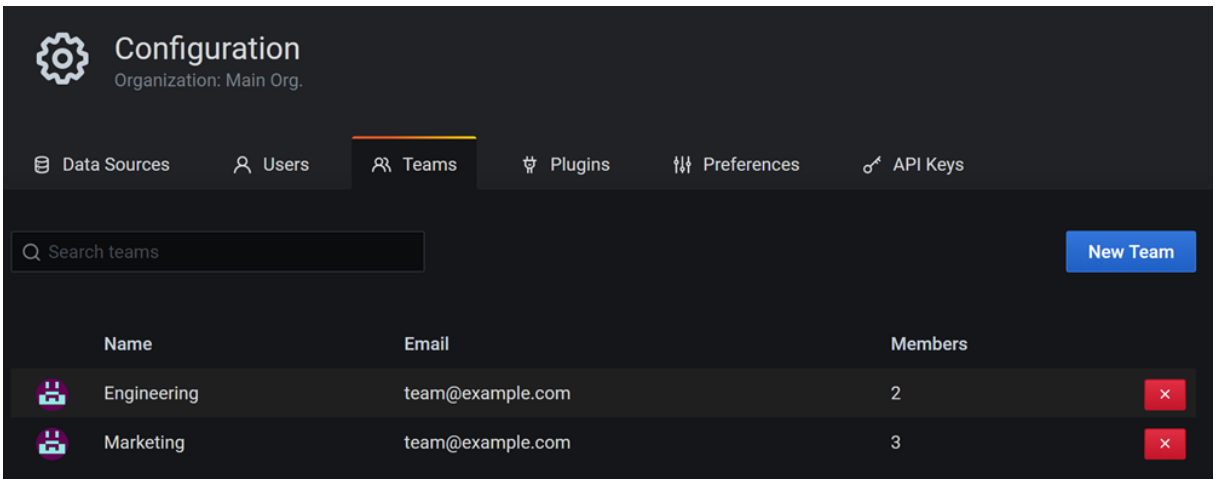
(Zdroj: 46)

Grafana umožňuje uživatelům anotovat grafy, což představuje efektivní způsob, jak označit důležité body nebo události pro budoucí použití nebo jak nabídnout kontext ostatním členům týmu. Anotace fungují jako digitální samolepicí poznámky umístěné přímo na grafu, což zefektivňuje komunikaci a sdílení znalostí.

Obrázek 19 Možnosti anotace v grafu

(Zdroj: 47)

Pro správu uživatelů Grafana nabízí pokročilou administrativní sekci. Ta je rozdělena na část Users, kde se vyskytuje kompletní seznam uživatelů s jejich právy a případně do jaké organizace patří. Krom informativní části zde může administrátor grafany přidat nového uživatele, smazat či zablokovat existujícího nebo modifikovat jeho údaje. V další části Teams lze vytvářet organizační skupiny, urychlující sdílení a přístupy uživatelů k jednotlivým dashboardům a grafům. Administrátor potřebuje pro vytvoření týmu pouze zadat jméno a libovolnou emailovou adresu. V týmu lze pak přidávat či odebírat členy podle uvážení vlastníka skupiny a přidávat oprávnění. Pro přístup týmu k dashboardu je možné přiřadit samotný tým k přístupu ke složce, kde je umístěn. Přiřazením celých týmů namísto jednotlivých členů se dodržuje jasná a organizovaná struktura práv napříč týmy.



Obrázek 20 Team management

(Zdroj: 48)

Open-source Grafany, podporovaný nadšenou a aktivní komunitou, nabízí uživatelům značné výhody. Patří mezi ně flexibilita při vytváření a publikování vlastních zásuvných modulů nebo využívání zásuvných modulů vyvinutých jinými uživateli. Instalace těchto zásuvných modulů je obvykle jednoduchá a zahrnuje stažení zdrojového kódu a jeho ruční spuštění.

To, že se jedná o otevřený zdrojový kód, má však i své nevýhody. Uživatelé například musí udržovat své instance Grafana a provádět aktualizace ručně. (45)

2 ANALÝZA SOUČASNÉ SITUACE

Tato kapitola bude věnována uvedení čtenáře do kontextu současné situace a identifikovaní nedostatků, kvůli kterým bylo nutno zavést nové řešení uvedené v kapitole Vlastní řešení.

2.1 Představení společnosti

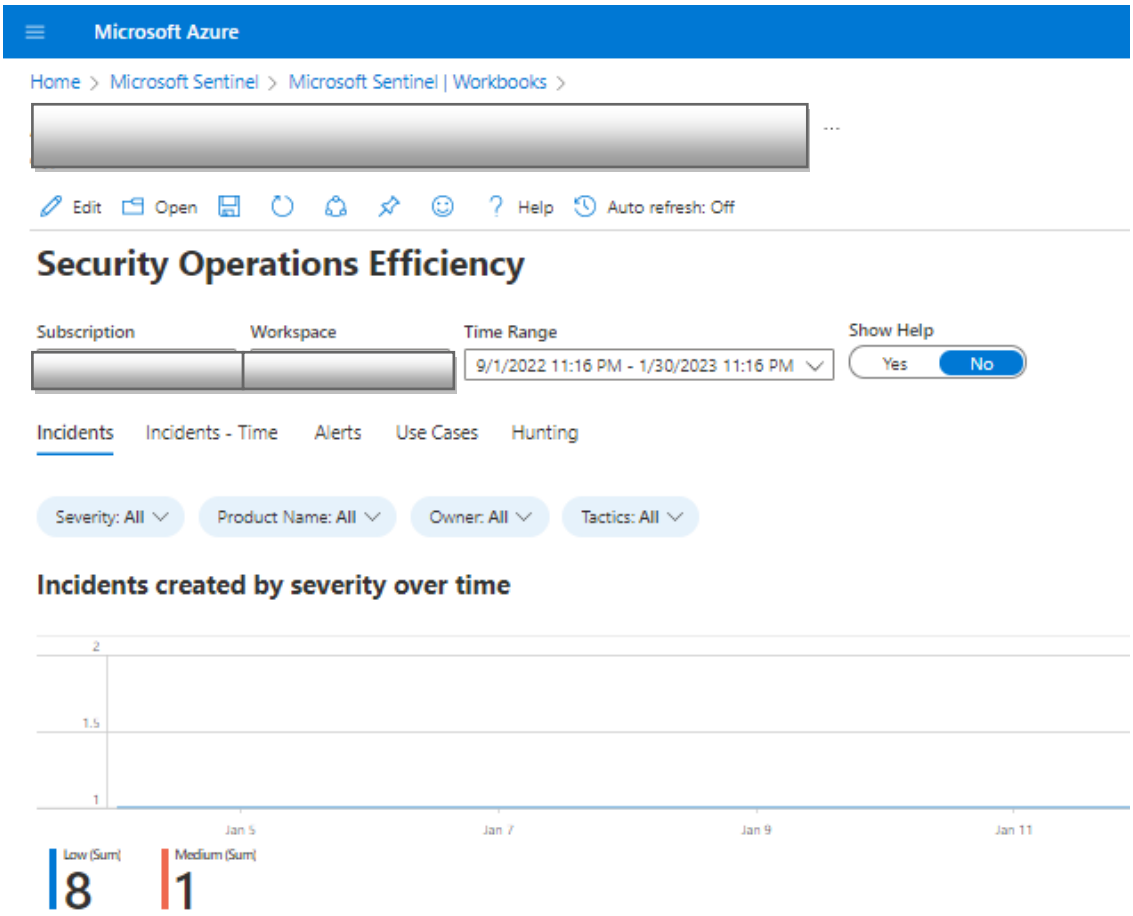
Systém, pro který je navrhnuto současné i budoucí řešení vlastní společnost PwC. Jedná se o jednu z největších globálních konzultačních společností a patří do takzvané „velké čtyřky“ – skupin 4 firem, které se zaměřují především na poradenské služby v oblasti financí, účetnictví a nově i informačních technologií. Jmenovitě zde spadají – PwC, Deloitte, KPMG, EY. Byť je PwC velmi často spojovány právě s výše zmíněným finančním poradenstvím v poslední době se více zaměřil na služby v oblasti informačních technologií. V oblasti datového řízení dodává služby v podobě zavedení komplexních BI reportů, návrhů řízení a zavádění business inteligence v rámci společností napříč různými sektory, či detailní analýza dat za pomoci implementování machine learning řešení. Krom specializací na data se zaměřuje i na jiné odvětví – za zmínku stojí služby spojené s informačním systémem SAP, jeho optimalizaci a transformaci. Práce spadá do kategorie kybernetické bezpečnosti konkrétně pod oddělení Cyber resilience, jehož hlavními procesy jsou kupříkladu „Návrh, realizace případně audit zabezpečených IS/IT systémů a aplikací prostřednictvím Secure SDLC v DevOps a tradičních prostředí“ či „Návrh, realizace a případně audit cloudového prostředí vaší organizace, včetně konkrétních řešení na platformě Azure/AWS/Google“ (49) Do této skupiny spadá i problematika řešená v rámci diplomové práce, kdy je vyvíjeno cloudové řešení SIEM v prostředí Azure.

Obrázek 21 Logo PwC

(Zdroj: 49)

2.1.1 Současný systém

Pro nynější řešení, jak již bylo zmíněno v Cíli práce je systém navržený a postavený pouze v cloudové podobě – či-li jediný centralizovaný systém, kam je potřeba se přihlásit pro monitorování a řízení hrozeb identifikovaných cloudovým systémem Microsoft Sentinel. Tento systém je momentálně postaven na developerské úrovni – tedy stále se vyvíjí, upravuje a mění. Rozlišujeme 2 typy uživatelů – developera a analytika. Developerovou povinností je vývoj systému, návrhy úprav řešení na základě možných budoucích požadavků, podle toho má i adekvátní oprávnění a přístupy. Analytik zodpovídá za monitorování a řešení incidentů v SIEMu, aby tuto činnost mohl vykonávat je nutné mu zajistit odpovídající přístup ke Sentinelu a především podsystému Workbooks, jenž je ústřední části současného systému. Diplomová práce se soustředí právě na tento podsystém, se kterým analytik nejvíce pracuje. V následující části bude představeno, jak současné řešení vypadá, z jakých částí se skládá a jeho nedostatky, kvůli kterým vzniklo řešení představené v kapitole Vlastní řešení.



a

Obrázek 22 Rozhraní workbooku v Sentinelu

(Zdroj: Vlastní zpracování)

Po přihlášení se analytikovi naskytne pohled na následující systém, jenž je zobrazen na obrázku výše. Lze vidět stránku s názvem „Security Operations Efficiency“ a celkově několik grafů rozdělené do 4 kategorií podle logického uskupení, seřazené od kriticky důležitých až po více informativní. Každý graf, který se zde nachází interpretuje data z tabulky SecurityIncident v kategorii logů Sentinelu, jejichž princip je blíže popsán v kapitole 1.2.1 Microsoft Sentinel. Tabulka je tvořena několika následujícími parametry:

- **TimeGenerated** – přesný čas, kdy došlo k zachycení incidentu, data jsou generovány ve formátu UTC – čili DD/MM/YYYY hh:mm:sss AM/PM např. 1/26/2023, 8:19:07.915 PM. Slouží pro identifikování přesného času, kdy došlo k incidentu a tudíž pochopení časového průběhu událostí.

- **IncidentName** – vygenerované unikátní označení incidentu, tvořený směsicí čísel a písmen znázorněné na následujícím příkladu: f11223f1-1f91-2214-8f54-5311770cecb2

- **Title** – Přesný název typu útoku, jenž byl zaznamenán – nejběžnější sledované kategorie v rámci práce jsou *Traffic detected from IP addresses recommended for blocking* a *Unfamiliar sign-in properties involving one user*, monitorující činnost IP adres jenž byly zahrnuty do listu zablokovaných IP adres či podezřelé přihlášení uživatele, způsobené pokusem přihlásit se do systému z IP adresy, které nepatří jeho obvyklé lokalitě a mohlo by se jednat o pokus infiltrace útočníka z jiné geolokace. Název slouží k rychlému sdělení hlavních informací o incidentu zúčastněným stranám a členům týmu.

- **Description** – detailní informace popisující typ útoku. Na výše uváděném útoku *Traffic detected from IP addresses recommended for blockin* systém poskytuje následující detaily - *Defender for Cloud detected inbound traffic from IP addresses that are recommended to be blocked. This typically occurs when this IP address doesn't communicate regularly with this resource. Alternatively, the IP address has been flagged as malicious by Microsoft's threat intelligence sources.* Tento atribut tak pomáhá analytikům rychleji pochopit incident, kdy každá minuta hraje roli.

- **Severity** – parametr pro určení míry závažnosti identifikované hrozby. Současné řešení ji vyhodnocuje do 4 kategorií. První, nejméně závažná nese název Informational. Jak z názvu vyplývá, slouží pouze pro analytické a testovací účely v rámci vývoje platformy a nepředstavuje závažnou hrozbu. Druhá, označená jako *low*, řadí hrozbu do méně závažných rizik. V této kategorii je nutno prověřit operátorem SIEMu validace rizika na základě kyberbezpečnostních standardů. Středně vysoké hrozby systém identifikuje třetí kategorií nazvaná *medium,* kdy riziko představuje určitý dopad pro společnost, pokud nebude včas validováno operátorem SIEMu. Poslední kategorie *High* představuje nejvyšší úroveň rizika pro bezpečnost organizace, s velmi zavážnými následky v případě nezachycení či špatného posouzení incidentu. Rozdělení podle výše zmíněných kategorií dává analytikům informaci o určení priorit a zajištění tak adekvátní rozdělení práce mezi analytiky.

- **Owner** – identifikuje osobu či pracovní skupinu zodpovědnou za prověření bezpečnostního incidentu. Jedná se o volitelný parametr, který se v současném stavu systému nemusí doplňovat.

- **ProviderName –** Tento atribut představuje název zdroje nebo služby, která incident vyvolala. Může se jednat o integrované bezpečnostní řešení, jako je Azure Sentinel, aplikaci třetí strany nebo interní bezpečnostní systém. Název providera pomáhá pochopit zdroj incidentu a koordinovat úsilí o reakci napříč různými bezpečnostními systémy a nástroji

- **ProviderIncidentId -** Jedná se o jedinečný identifikátor přidělený poskytovatelem zabezpečení pro každý incident. Tento identifikátor pomáhá při sledování a korelaci incidentů v různých systémech a u různých poskytovatelů.

- **FirstActivityTime –** Přesný čas ve formátu DD/MM/YYYY hh:mm:sss AM/PM, kdy byla identifikována podezřelá aktivita

- **LastActivityTime –** Přesný čas ve formátu DD/MM/YYYY hh:mm:sss AM/PM, kdy byla identifikována podezřelá aktivita

- **IncidentNumber -** Tento atribut označuje automaticky generované číslo přidělené každému bezpečnostnímu incidentu v organizaci. Pomáhá při organizaci a odkazování na incidenty pro snadnější správu a analýzu.

- **RelatedAnalyticalRulesIds -** Tento atribut obsahuje seznam ID analytických pravidel, která jsou spojena s bezpečnostním incidentem. Tato pravidla pomáhají při identifikaci a analýze konkrétních bezpečnostních událostí nebo vzorců, které incident vyvolaly.

- **Comments -** Tento atribut obsahuje jakékoli další poznámky, postřehy nebo souvislosti, které členové bezpečnostního týmu nebo analytici k incidentu poskytli. Tyto poznámky mohou pomoci při dalším vyšetřování a nápravě**.**

- **Tasks -** Tento atribut obsahuje seznam úkolů nebo akcí, které byly zadány nebo dokončeny v rámci procesu reakce na incident. Tyto úkoly mohou zahrnovat kroky vyšetřování, opatření k omezení šíření nebo úsilí o nápravu.

- **Labels** - Tento atribut obsahuje štítky, které jsou spojeny s bezpečnostním incidentem. Štítky lze použít ke kategorizaci incidentů na základě jejich závažnosti, typu nebo jiných relevantních kritérií pro snadnější filtrování a analýzu.

- **IncidentURl –** odkaz na incident v sentinelu, po jehož rozkliknutí lze zobrazit veškeré spojené detaily, v případě že uživatel má nastavená oprávnění

- **AdditonalData –** atribut obsahuje doplňující informace týkající se bezpečnostního incidentu, které mohou být užitečné pro účely analýzy.

- **ModifiedBy –** slouží pro zaznamenání jména nebo identifikátoru uživatele, který naposledy upravil podrobnosti incidentu. Tato informace je užitečná pro sledování změn a udržování auditní stopy procesu reakce na incident.

- **Type** – označuje kategorii bezpečnostního incidentu, například malware, phishing nebo neoprávněný přístup. Kategorizace incidentů podle typu pomáhá při určování priorit reakce a analýze bezpečnostních trendů.

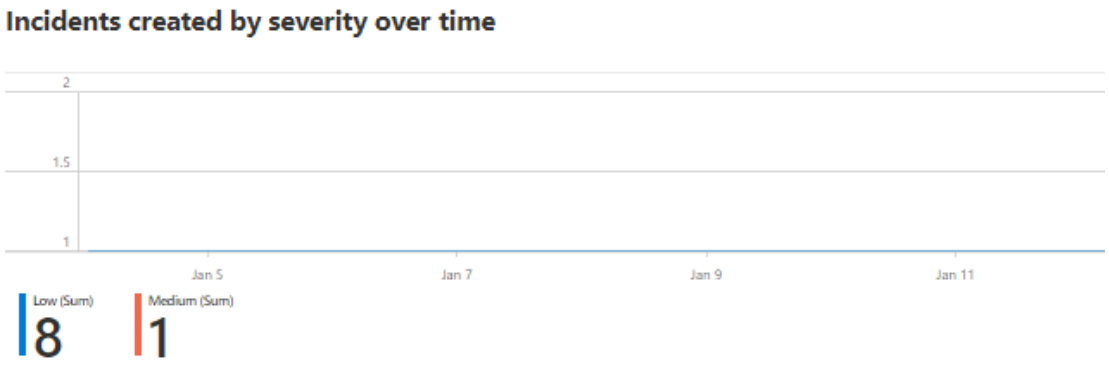
- **TenantID** - jedinečný identifikátor organizace. Pomáhá při korelaci incidentů a dat napříč více organizacemi

- **SourceSystem** - Tento atribut určuje systém nebo aplikaci, ze které byl bezpečnostní incident vytvořen nebo zjištěn. Tato informace je zásadní pro pochopení původu incidentu a potenciálního rozsahu jeho dopadu.

Všech výše popsaných 22 parametrů nejsou v rámci jednotlivých grafů interpretovány, protože některé slouží pouze pro technické a budoucí účely, které potřebují být zaznamenány, nikoliv zobrazeny koncové uživateli. Všechny výsledné vizualizace jsou spravovány ve 4 skupinách Incidents, Incidents-time, Alerts, Use Cases, Hunting

Všechny kategorie krom první jsou zatím ve vývojářské fázi a proto se rámec práce soustředí pouze na Incidents, jenž je specializovaná výhradně na identifikované incidenty. V této kategorii se nachází celkem 8 grafů. Jenž se dají popsat následovně:

- **Incidents created by severity over time**
  Počáteční se zaměřuje na rozdělení incidentů podle parametru *severity* tedy míry závažnosti identifikovaného incidentu a datem, kdy byly nalezeny systémem. Vzniká tak přehledný graf, jež je přiložený níže. Osa X reprezentuje časovou osu, osa Y pak počet incidentů. Jednotlivé linie zobrazené v grafu se liší barvou podle míry „severity“

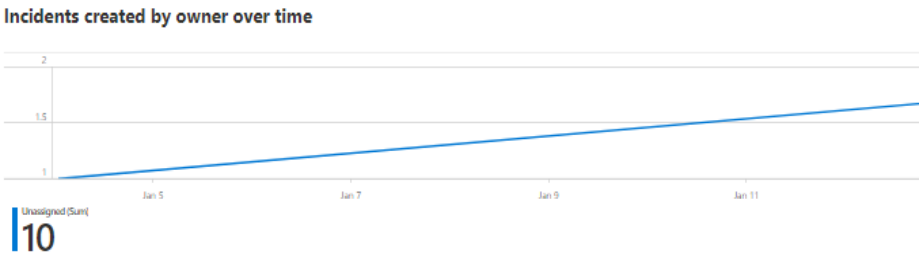


Obrázek 23 Incidents created by severity over time graf

(Zdroj: Vlastní zpracování)

- **Incidents created by owner over time**

  Graf obdobný předcházejícímu, s tím rozdílem že identifikuje jednotlivé osoby zodpovědné za řešení incidentu

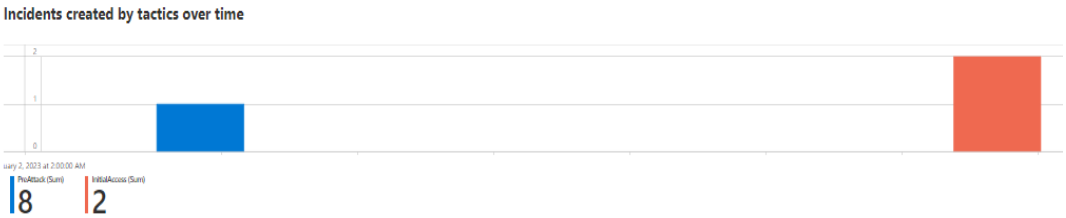


Obrázek 24 Incidents created by owner over time graf

(Zdroj: Vlastní zpracování)

- **Incidents created by tactics over time**

  V tomto případě se graf odlišuje svou formou. Aktuálně vytvořený graf je ve formě sloupcového grafu, na rozdíl od dřívějších, které měly tvar spojnicového grafu. Osy zůstávají zachovány, avšak s odlišností, že graf posuzuje uplatněnou taktiku útoku.



Obrázek 25 Incidents created by tactics over time graf

(Zdroj: Vlastní zpracování)

- **Incidents created by tags over time**

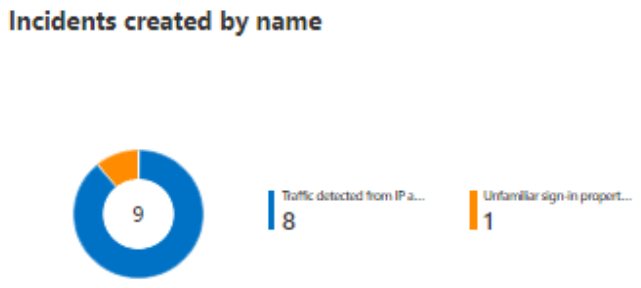
  Graf je vytvořen ve stejném formátu jako předcházející. Modifikací je pouze změna trasované hodnoty, kdy se monitoruje incident na základě tagu.

Obrázek 26 Incidents created by tags over time graf

(Zdroj: Vlastní zpracování)

- **Incidents created by name**

  Tato vizualizace, která se zaměřuje na detailní identifikaci incidentů je na rozdíl od předcházejících propojena s tabulkou. Na níže uvedeném obrázku lze vidět graf v základním tvaru v literatuře velmi často zván jako „výsečový graf“ nebo i „koláčový“



Obrázek 27 Incidents created by name graf

(Zdroj: Vlastní zpracování)

Pro získání více informací o incidentech lze nahlédnout do tabulky přiložené pod grafem. Tabulka udává – název incidentu, vážnost, zda se jedná o nový či dlouho otevřený, kolikrát byl již identifikován, bližší popis útoku, taktika, url adresa provázaná s incidentem a subsystém jež útok zaregistroval

Details for the workspace, count of: 8 Incidents during 8/1/2022 7:28 PM - 2/2/2023 7:28 PM

Search

IncidentNumber	Severity	Status	AlertCount	Owner	Title	Tactics	IncidentUrl
1576	Low	New	1		Traffic detected from IP addresses recommended for bloc...	["PreAttack"]	Open Incident in Azure Sentinel
1575	Low	New	1		Traffic detected from IP addresses recommended for bloc...	["PreAttack"]	Open Incident in Azure Sentinel
1574	Low	New	1		Traffic detected from IP addresses recommended for bloc...	["PreAttack"]	Open Incident in Azure Sentinel
1573	Low	New	1		Traffic detected from IP addresses recommended for bloc...	["PreAttack"]	Open Incident in Azure Sentinel
1572	Low	New	1		Traffic detected from IP addresses recommended for bloc...	["PreAttack"]	Open Incident in Azure Sentinel
1571	Low	New	1		Traffic detected from IP addresses recommended for bloc...	["PreAttack"]	Open Incident in Azure Sentinel
1570	Low	New	1		Traffic detected from IP addresses recommended for bloc...	["PreAttack"]	Open Incident in Azure Sentinel
1568	Low	New	1		Traffic detected from IP addresses recommended for bloc...	["PreAttack"]	Open Incident in Azure Sentinel

Obrázek 28 Tabulka s detaily incidentů

(Zdroj: Vlastní zpracování)

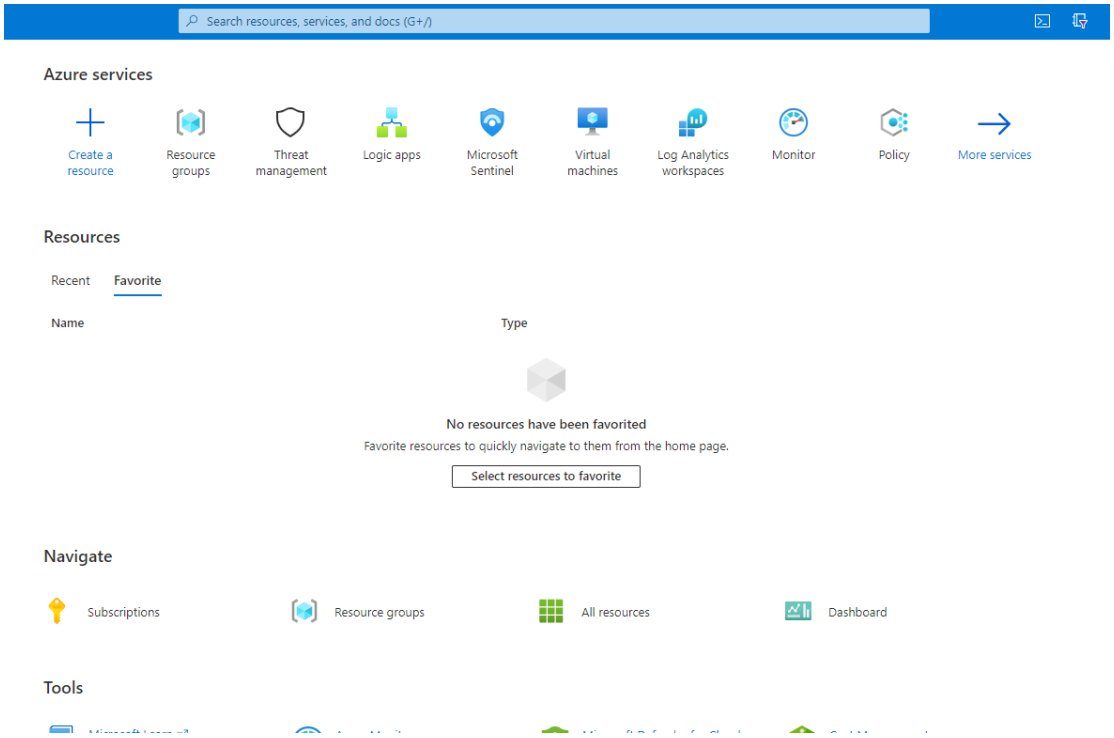
- **Long term incidents**

  Kategorie Incidents je zakončena tabulkou long term incidents, která mapuje dlouhodobě otevřené případy nahlášených útoků. Tabulka obsahuje stejné sloupce jako předcházející krom nově případných URL k forenzní analýze.

2.1.2 Nedostatky současného řešení

Byť by se řešení mohlo zdát vhodné pro developerskou fázi, pro produkční a klientské potřeby stávající řešení není vyhovující z několika následujících důvodů:

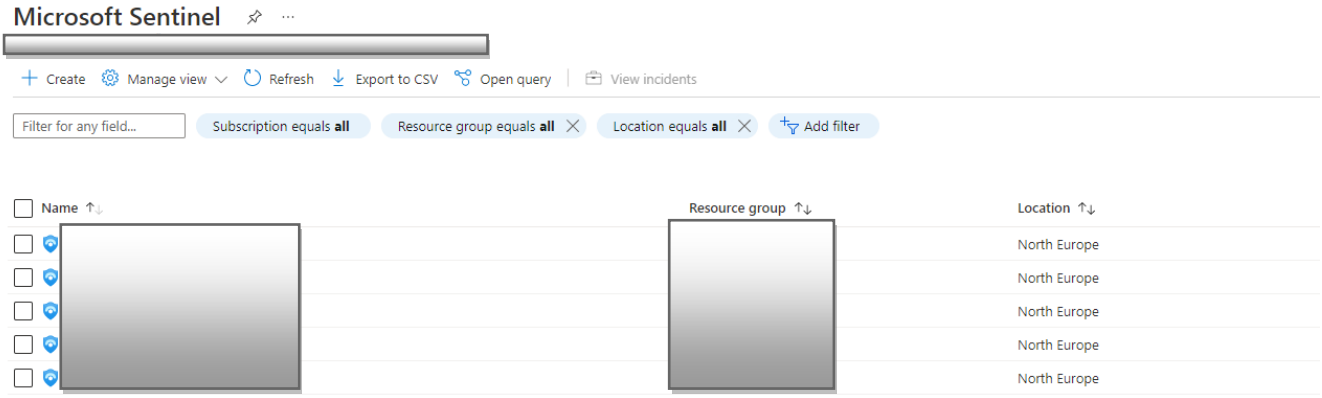
- Komplexnost Sentinelu – analytik má možnost podívat se na výsledky analýz pouze za předpokladu, že se úspěšně přihlásí do cloudu. Poté se musí zorientovat na hlavní stránce Azure, kde, jak lze vidět na obrázku 29 může být prvotní dojem matoucí a zabere určitý čas pro uživatele než se zorientuje ve službách a prostředí cloudového prostředí.



Obrázek 29 Úvodní menu Sentinelu

(Zdroj: Vlastní zpracování)

Poté musí přejít do prostředí SaaS aplikace Microsoft Sentinel, kde je potřeba zvolit správnou monitorovací skupiny – opětovně, pokud je v sentinelu více skupin a uživatel má přístup do každé z nich, nastává administrativní komplikace a nahrává chybovosti uživatele s prací v naprosto jiné skupině nebo nežádoucí modifikací v prvku alternativní skupiny, než byla cílová.

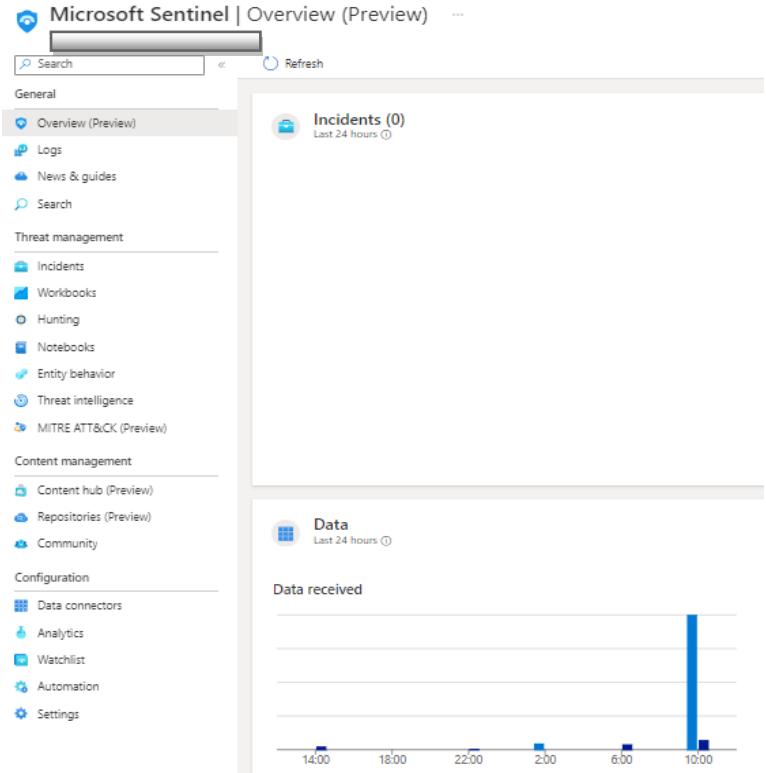


Obrázek 30 Skupiny v Sentinelu

(Zdroj: Vlastní zpracování)

Po jejím zvolení se uživateli nabízí široká nabídka možností, ke kterým má přístup rozdělené do 4 základních kategorií General, Threat management, Content management, Configuration, které jsou blíže rozepsány v kapitole 1.2.1. Microsoft Sentinel.

K potřebným datům je potřeba vybrat záložku Workbooks a vybrat potřebný Workbook, obsahující veškeré grafy.



Obrázek 31 Možnosti v Sentinelu

(Zdroj: Vlastní zpracování)

Jak bylo zmíněno v teoretických východiskách, Sentinel je velmi komplexní program, který dokáže detailně analyzovat incidenty. V praxi se však může stát, že tato komplexnost představuje problém, zejména v organizacích, které nejsou obeznámené s tímto nástrojem.

- Technická neznalost – pro práci s libovolným cloudovým prostředím je potřeba disponovat aspoň základními technickými dovednostmi, jak již bylo zmíněno v předchozím problému, uživatel se může velmi snadno splést v důsledku chybně vybraných zdrojových dat, neznalosti poskytovaných služeb či případně nežádoucí modifikací dat nebo již zhotovené instance.

- IAM – povinnost monitorovat uživatele v cloudu – další nevýhodou, kterou představuje jednotný systém v cloudu je nutnost administrace všech účtů odpovědných osob s přístupovými právy. Vytváření, správa a sledování přístupových oprávnění pro různé uživatele, skupiny a v případě nutnosti zapojení třetí strany je složité a zdlouhavé. V rámci kyberbezpečnosti je vždy důležité dávat uživatelům pouze ty práva a přístupy, které nezbytně potřebují k výkonu své práce, na základě faktu, že nezanedbatelná část útoků ať z pohledu odcizení dat, narušení firemních procesů či nasazení špionážních programů stojí právě bývalý nebo současný zaměstnanec, často nazývaný „Insider“

- Problémy kooperací s třetí stranou – nedostatek velmi propojený s předcházejícím. Mnoho společností spoléhá krom vlastních vývojářů, analytiků nebo datových vědců i na externí dodavatele. V tomto případě je důležité přistupovat s důslednou obezřetnostní. Po předání přístupů třetí straně je potřeba monitorovat přesný počet účastníků s právy. Důležité je zjistit, zda poskytnuté účty byly využity, v praxi byly evidovány případy vytvoření účtů externí firmě, které následně nebyly aktivovány, tím zůstala možnost potencionálního zneužití poskytnutých přihlašovacích údajů, s výchozím heslem a přihlašovacím jménem poskytnutý organizací.

- Limitovaná nabídka vizualizací – Posunování a přeskládávání dílčích grafů, tabulek či objektů v rámci worksheetu je velice pracné z hlediska stylizace, kdy se musí vývojář ručně nastavovat padding a margin pro zajištění mezer mezi jednotlivými prvky. Dále Azure Workbooks neobsahuje velké množství různých typů grafů, které by dokázali zajistit komplexní přehled a vizualizaci nad daty v Sentinelu. Byť se Microsoft snaží

produkt stále vyvíjet a vylepšovat, alternativní systémy disponují širší škálou objektů pro zobrazení dat – kupříkladu heatmapa .

- Integrace s dalšími monitorovacími nástroji: Organizace používá více monitorovacích nástrojů pro různé aspekty své IT infrastruktury, což vede k roztříštěnému pohledu na stav zabezpečení. Potřebují řešení, které dokáže konsolidovat data z různých zdrojů a poskytnout jednotný pohled na jejich bezpečnostní prostředí.

- Omezená podpora pro některé zdroje dat: Ačkoli Azure Sentinel podporuje mnoho zdrojů dat, může být jeho podpora pro některé specifické nebo proprietární systémy omezená. V takových případech je třeba vytvořit vlastní konektory nebo integrace, což může být časově náročné a nákladné.

V této kapitole bylo představeno současné řešení – jeho řešení v cloudové podobě, funkčnost a nedostatky, které vedli k vytvoření alternativního systému¨, jenž je blíže popsán v kapitole Vlastní řešení.

3 VLASTNÍ ŘEŠENÍ

Kvůli důvodům uvedeném v kapitole Analýzy současné situace bylo rozhodnuto o vytvoření alternativního systému pro monitorování bezpečnostních incidentů, které by sloužilo pouze pro analytické účely. Po analyzování datových zdrojů a požadavku managementu na systém byly zhotoveny 2 alternativní řešení

3.1 PowerBi řešení

Původní návrh pro splnění cíle práce spočíval ve vývoji systému založeném na platformě PowerBI. Avšak během realizace projektu se objevilo několik problémů. Hlavním problémem se ukázaly být licence – i když PowerBI je poskytován společností Microsoft "zdarma", je pro sdílení vytvořených dashboardů nutné mít placenou verzi Pro nebo Premium, v závislosti na SLA sjednaném mezi Microsoftem a společností implementující business intelligence systém. Navíc, vzhledem k tomu, že řešení mělo být realizováno v cloudové podobě, by náklady vzrostly o poplatky za SaaS službu PowerBI. S ohledem na to, že nově realizovaný systém měl být co nejméně nákladný, nejlépe postavený na open-source řešení, byl tento návrh architektury zamítnut.

Dalším problémem, který představoval obtíže jak z technického, tak z nákladového hlediska, byl požadavek na dodatečný virtuální SQL server, který je nezbytný při propojování SQL databáze s PowerBI on-premise serverem. Tato nutnost zvyšovala komplexnost a náklady celkového řešení.

3.2 Grafana řešení

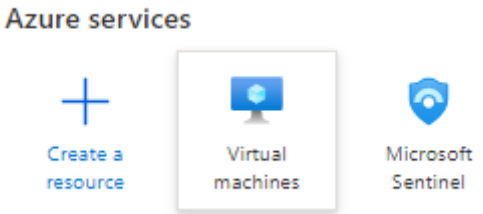
Po zvážení různých alternativ byl pro dosažení cílů stanovených managementem nakonec zvolen vizualizační nástroj Grafana, který je podrobněji popsán v kapitole Použité technologie. Grafana byla vybrána jako plnohodnotné řešení pro naplnění cílů práce, a to zejména díky architektuře založené na open-source řešení, možnosti integrace s cloudovými službami Azure a škálovatelnosti podle množství přicházejících dat do Grafany.

Při zahájení projektu bylo zvažováno využití SaaS alternativy, podobně jako v předchozím případě s PowerBI. Avšak v tomto případě náklady přesahovaly potenciální zhodnocení projektu, což vedlo k rozhodnutí vytvořit řešení na úrovni IaaS. To zahrnovalo vytvoření virtuálního serveru s operačním systémem Ubuntu, který bude hostit Grafanu. K tomu byla přidána konfigurace serveru, jako je instalace Grafany přes CLI, nastavení DNS a SSL certifikátu, propojení Grafany s cloudovým prostředím a příprava dashboardů.

V následujících kapitolách bude podrobně vysvětleno kompletní nasazení tohoto systému, které zahrnuje kroky od vytvoření virtuálního serveru až po finální konfiguraci Grafany a její integraci s cloudovým prostředím. Tímto způsobem bude demonstrováno, jak bylo dosaženo cílů stanovených managementem, a představena efektivita zvoleného řešení pro vizualizaci dat.

3.2.1 Inicializace serveru

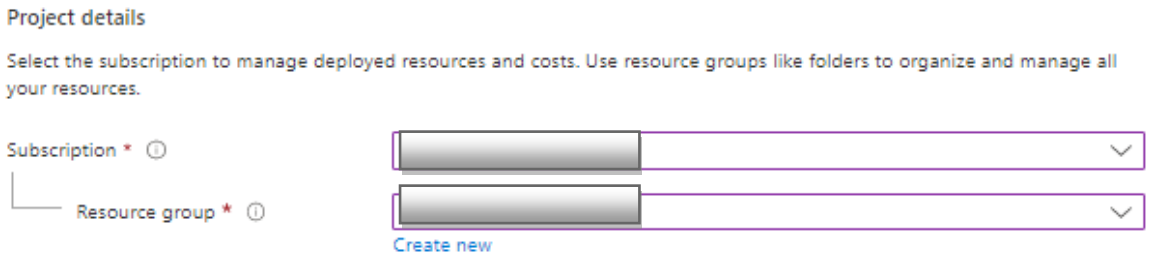
Prvním krokem při vytváření systémové architektury bylo nasazení virtuálního stroje v Azure cloudu. Toho lze dosáhnout vyhledáním služby "Virtual machines" a následně výběrem možnosti "Create virtual machine hosted by cloud". Poté je možné nastavit jednotlivé parametry potřebné pro inicializaci serveru.



Obrázek 32 Služba Virtual machines v Azure

(Zdroj: Vlastní zpracování)

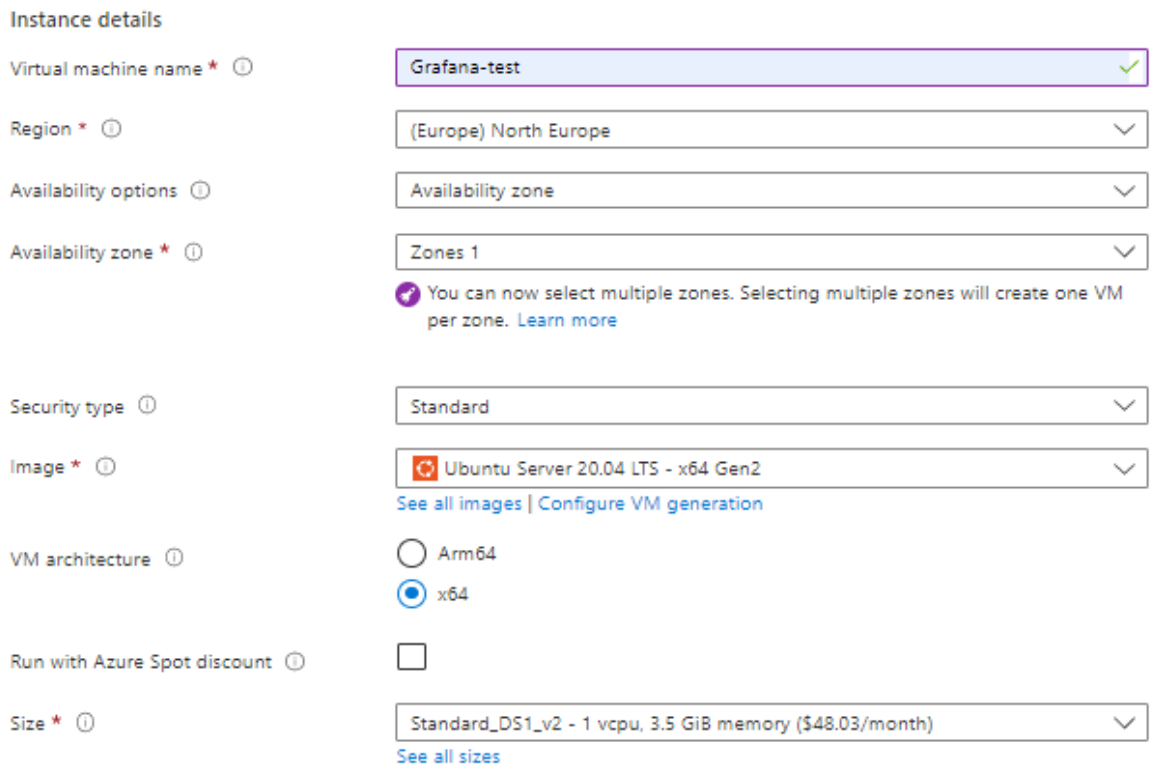
Parametry jsou rozdělené do celkově 8 skupin a několika podskupin s rozdílným počtem pro každou skupinu. V první skupině "Basics“ se nachází 4 podskupiny. Pro podskupinu "Project details“ je nutné zvolit subscription nebo-li předplatné, ze kterého budou účtovány poplatky a skupinu zdrojů, do které bude server umístěn



Obrázek 33 Zvolení předplatného a skupiny prostředků

(Zdroj: Vlastní zpracování)

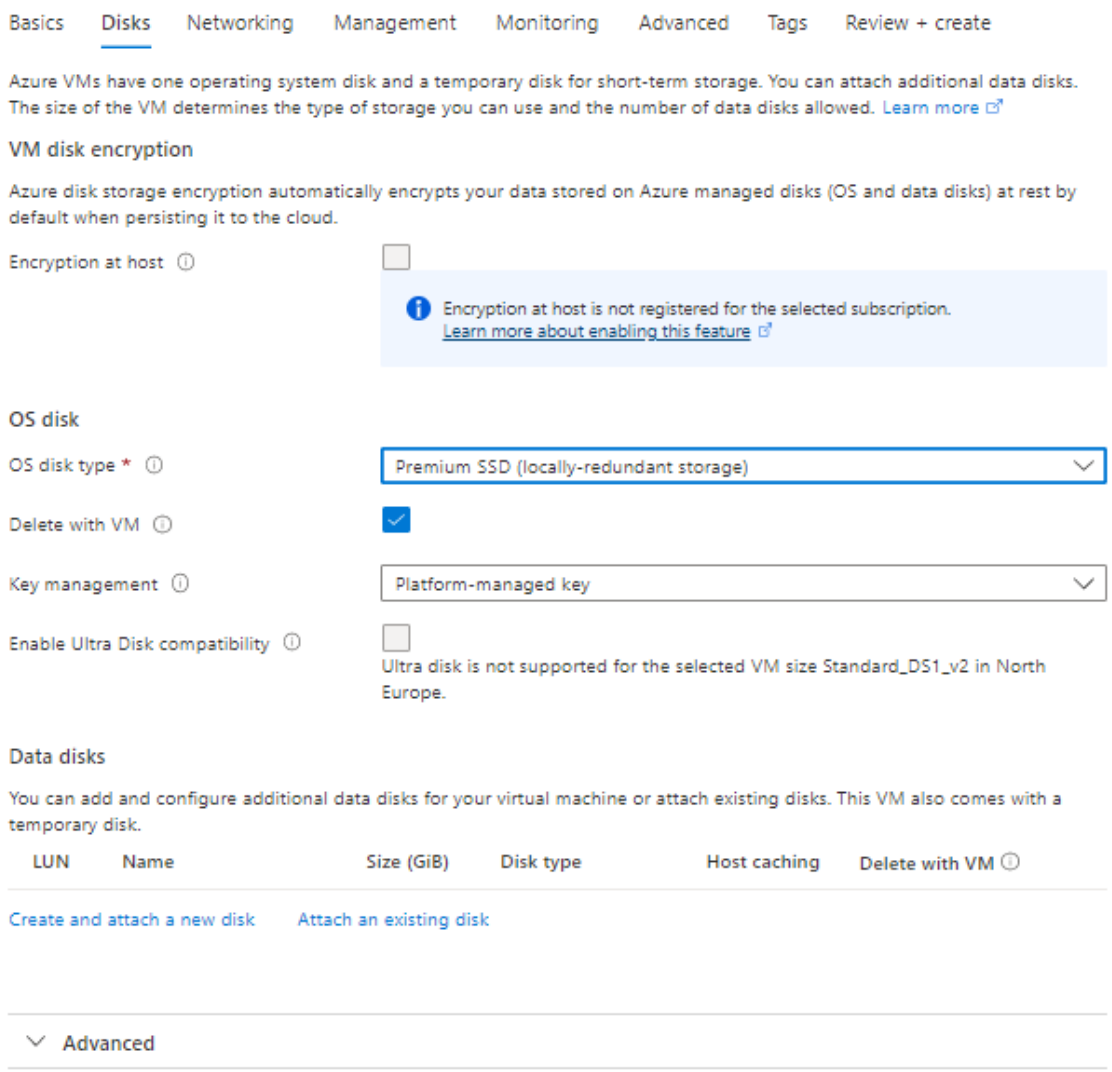
V další podskupině "Instance detail“ se zvolí název serveru, v rámci diplomové práce byl vyplněn pracovní název "Grafana-test“ a region určující lokaci virtuálního stroje a dostupnost v případě výpadku datového centra. Jako poslední se zvolil typ operačního systému a velikost výpočetního výkonu.



Obrázek 34 Podrobnosti vytváření VM

(Zdroj: Vlastní zpracování)

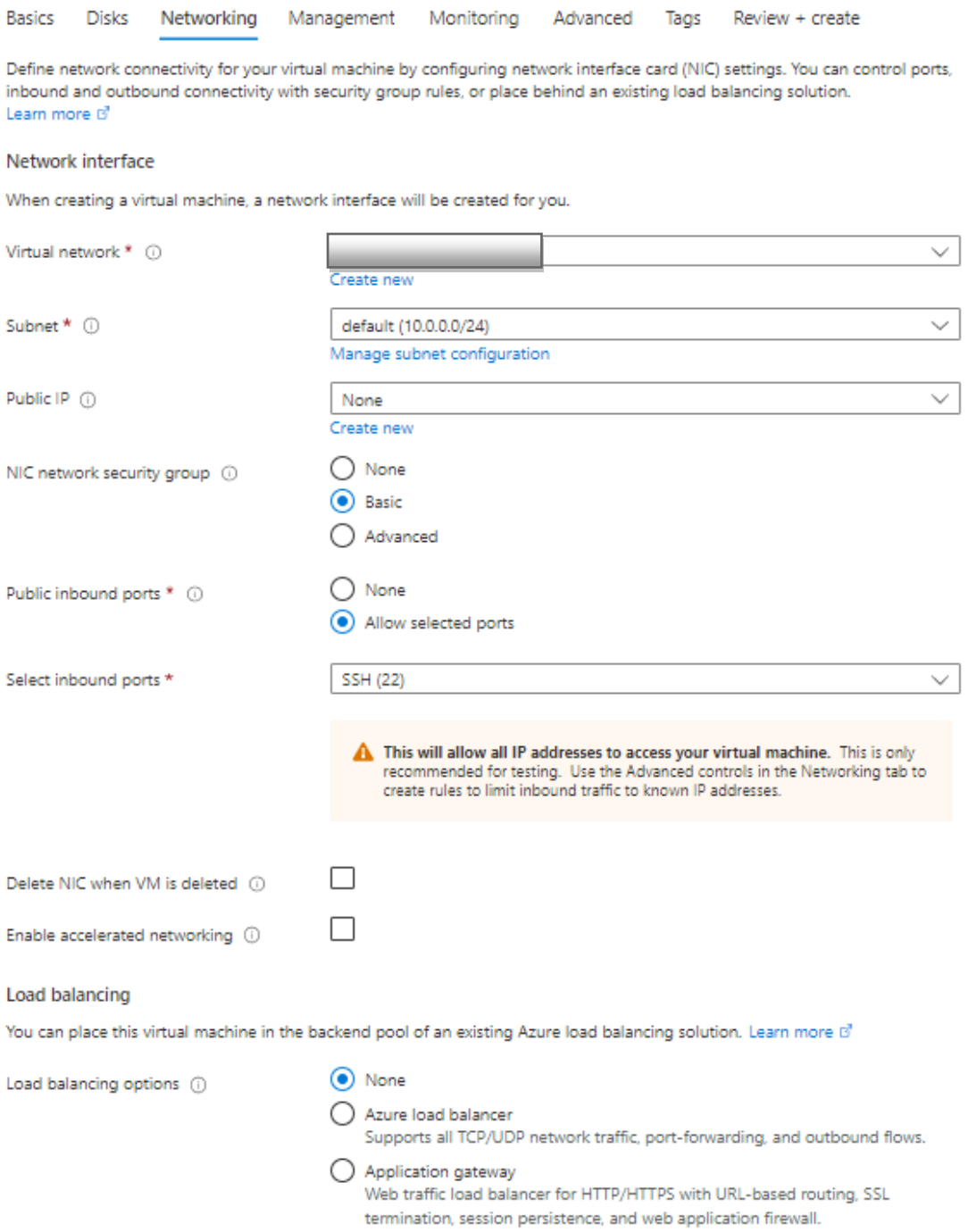
Následující skupina “Disks“ se zaměřuje na podrobnosti datového úložiště implementované VM. V Podsekci VM je nutné zvolit typ disku Premium SSD, jenž poskytuje vícenásobný výkon oproti typu standard HDD, zbylé možnosti není nutné nastavovat a lze je ponechat výchozím hodnotám.



Obrázek 35 Alokace disku

(Zdroj: Vlastní zpracování)

Pro skupinu Networking je potřeba nastavit v podsekci “Virtual network“ a “Subnet“ síť, ve které bude Grafana operovat, pro testovací účely necháme otevřený port 22, který v dalších kapitolách nabývá na důležitosti pro konfiguraci zařízení.



Obrázek 36 Nastavení síťové konfigurace

(Zdroj: Vlastní zpracování)

Sekce management se zaměřuje na bližší možnosti pro získání kontroly na virtuálním strojem. Celkově se zde nachází 5 prvků.

Microsoft Defender for Cloud – zhodnocení, zda VM bude zařazena do bezpečnostního programu

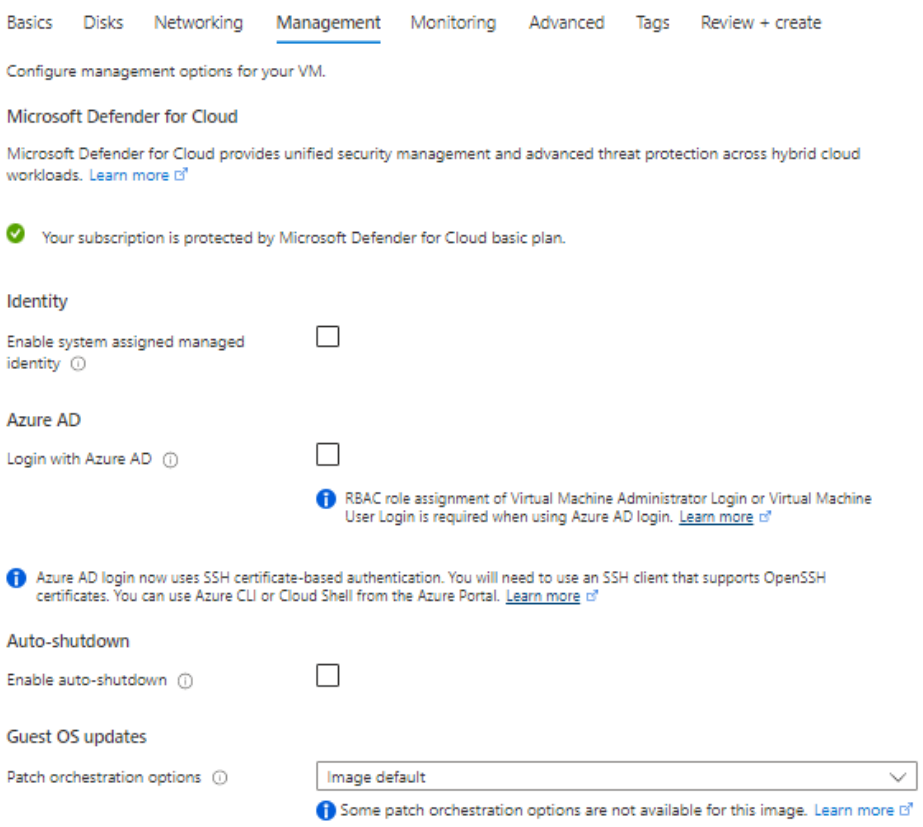
Identity – Systémem přiřazená spravovaná identita, pro jednotnou autentizaci napříč službami Azure.

Azure ActiveDirectory – Služba k řízení přístupů uživatelských účtů. Povoluje organizaci spravovat práva napříč prostředky ať jsou nasazené v cloudu nebo on-premise.

Auto-shutdown – možnost pro vypnutí VM automaticky

Guest OS updates – nastavení aktualizace operačního systému

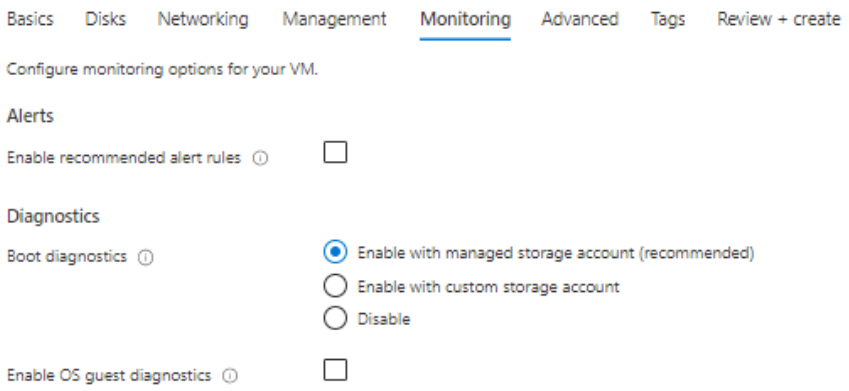
Byť jsou výše zmíněné prvky velmi užitečné v praxi, většina z nich je často placené a proto se i zde ponechají výchozí hodnoty a lze pokračovat v nastavování „Monitoring“



Obrázek 37 Konfigurace Managementu

(Zdroj: Vlastní zpracování)

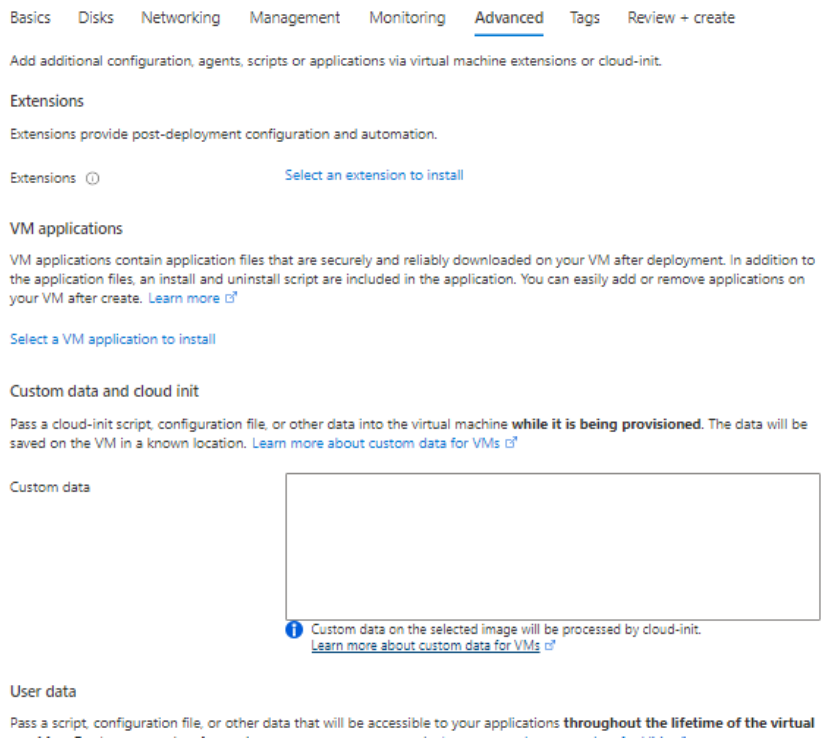
Monitoring sestává se 2 podsekcí. Alerts pro zapnutí upozorňujících správ, které lze specifikovat kupříkladu pro překročení výkonu procesoru nad 90 %, či dostupnosti paměti a Diagnostic, jenž je zaměřena pro konfiguraci logů v případě chybného zavedení operačního systému. I zde ponecháme výchozí hodnoty a pokračujeme na “Advanced“



Obrázek 38 Nastavení Monitoringu

(Zdroj: Vlastní zpracování)

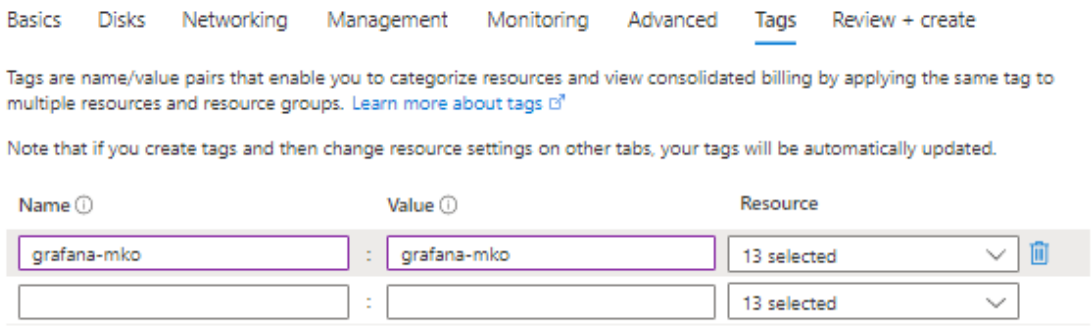
Sekce Advanced se zaměřuje na pokročilé nastavení při nasazování virtuálního stroje. Je tvořena několika dílčími podsekcemi, ale pro potřeby projektu není potřeba konfigurovat ani jednu z nich. I je tedy ponecháme výchozím hodnotám a přepneme na kartu „Tags“.



Obrázek 39 Pokročilé nastavení

(Zdroj: Vlastní zpracování)

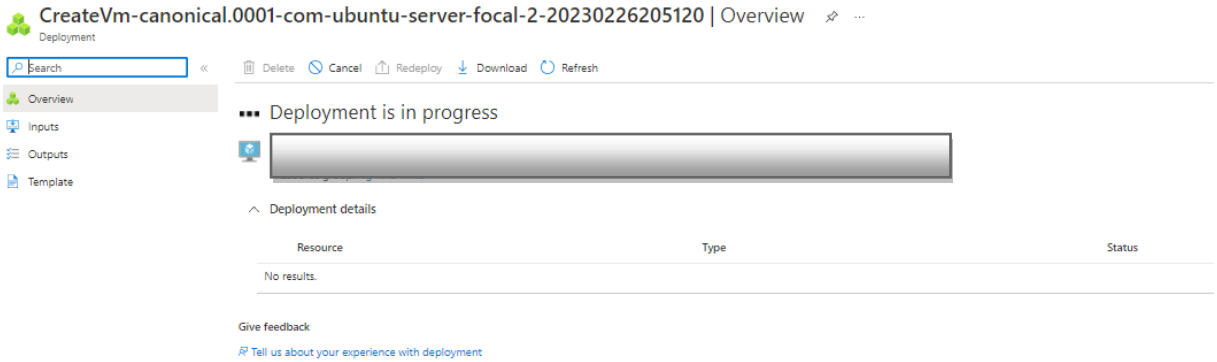
V předposlední sekci Tags je možné nastavit jednotný identifikátor pro všechny nasazované položky v rámci VM – disk, sítové rozhraní atd. Tagy slouží především pro organizace jednotlivých zdrojů napříč skupinami prostředků v celé organizaci. Dalším benefitem je i přehlednější sledování nákladů spjaté se zdroji. V rámci projektu jsou všechny komponenty otagovány pod názvem „mko-grafana“, jak lze vidět na dolním přiloženém obrázku



Obrázek 40 Zvolený tag pro VM

(Zdroj: Vlastní zpracování)

Po potvrzení nasazení virtuálního stroje se Azure Cloud postará o automatické nasazení a konfiguraci zdrojů dle zadaných parametrů. Během několika minut bude virtuální stroj připraven k použití a můžeme začít s jeho další konfigurací a instalací Grafany.

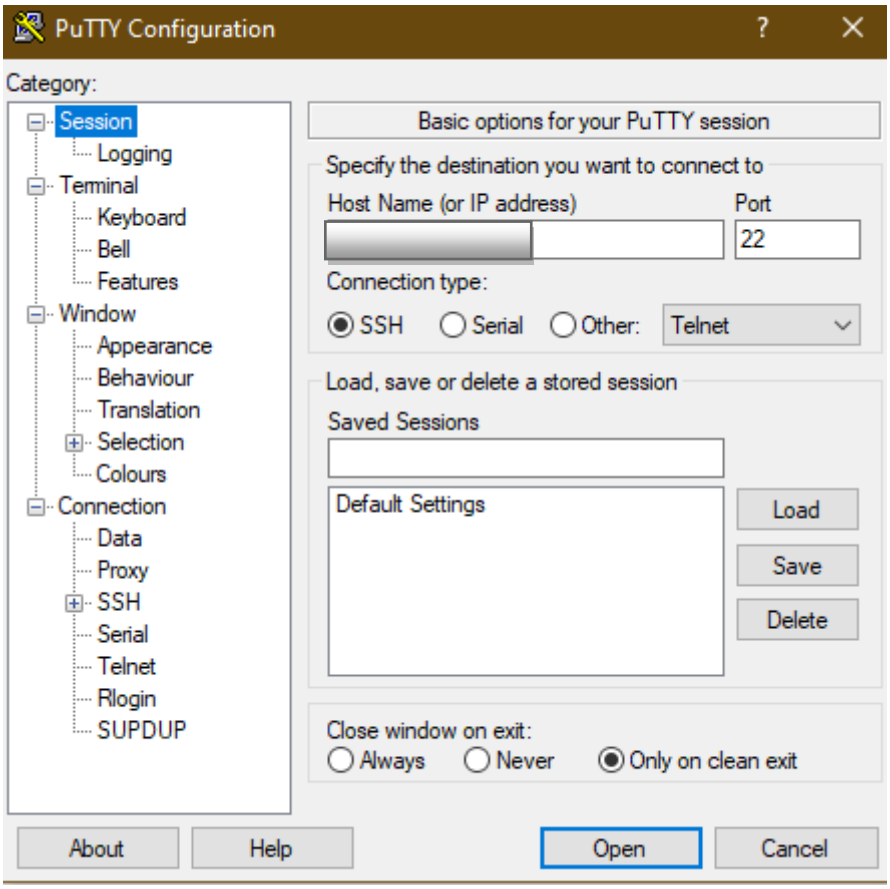


Obrázek 41 Konečné nasazení VM

(Zdroj: Vlastní zpracování)

3.2.2 Instalace Grafany

Dalším krokem po vytvoření serveru je instalace Grafany. Toho je docíleno následujícími kroky. Do spravovaného serveru je nutné se přihlásit přes SSH protokol, operující na portu na 22. Otevřeme tedy nástroj Putty, který je určený pro tento typ operace. Pro autentizaci je nutné zada IP adresu serveru, port 22 a stisknout Open, jak je znázorněno na přiloženém obrázku.



Obrázek 42 Připojení k systému přes PuTTy

(Zdroj: Vlastní zpracování)

Nyní se nacházíme v konzoli, kde vytvoříme instalační soubor grafany pomocí:

```
nano install-grafana.sh
```

Následně zadáme příkazy pro instalaci grafany, které lze vidět na přiloženém obrázku

```
  GNU nano 4.8                    install-grafana.sh
#!/bin/sh
sudo apt install -y software-properties-common

#add grafana to list of allowed software
sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -

sudo apt update && apt install -y grafana
sudo systemctl enable grafana-server.service
sudo systemctl start grafana-server

                              [ Read 10 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line
```

Obrázek 43 Vytvořený instalační soubor

(Zdroj: Vlastní zpracování)

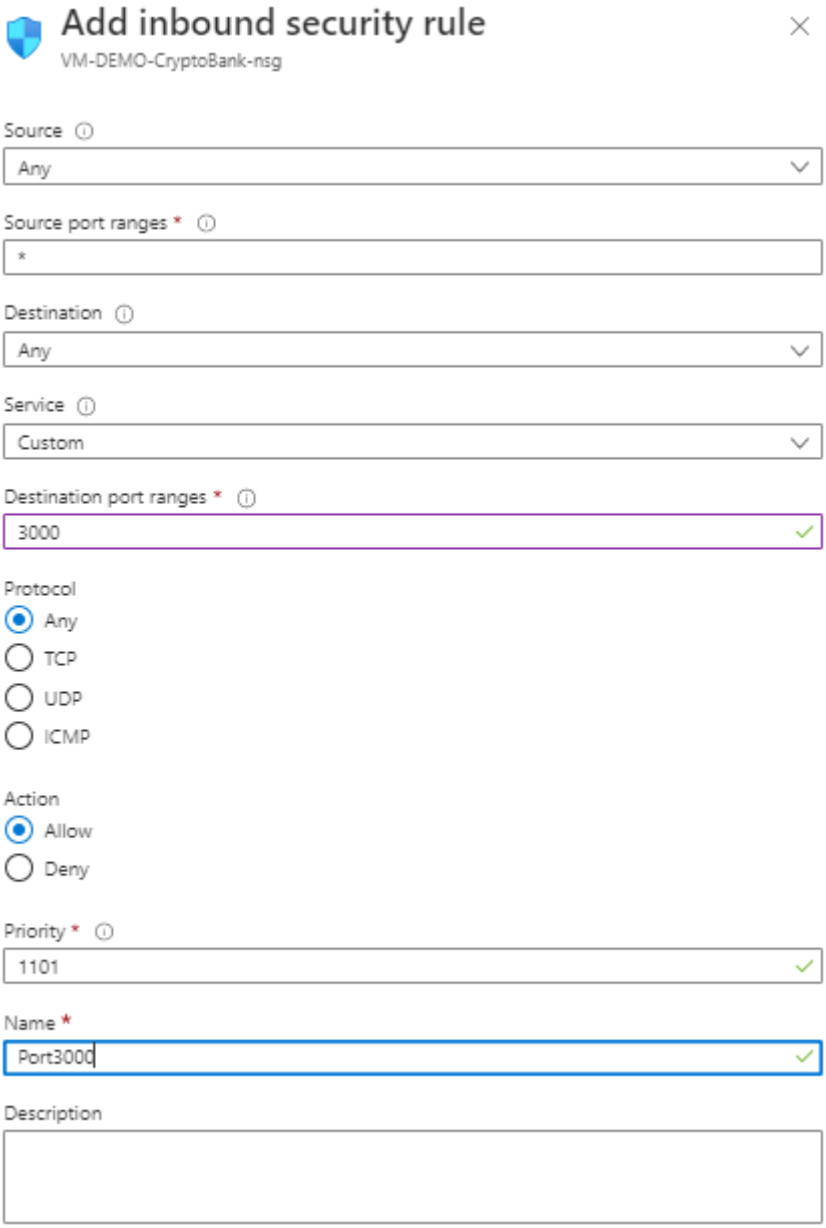
Vytvořený instalační soubor funguje na jednoduchém principu, kdy při svém spuštění stáhne nejnovější verzi Grafany z oficiálního repositáře, poté je nutné soubor udělat spustitelným pomocí:

```
chmod +x install-grafana.sh
```

Následuje pak samotné spuštění:

```
sudo ./install-grafana.sh
```

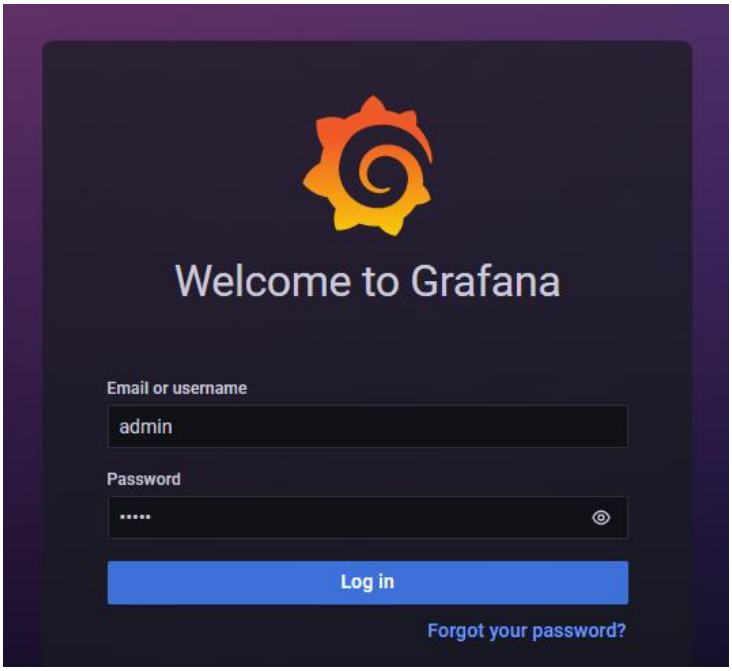
Pro funkčnost aplikace je nutné povolit port 3000. Toho docílíme konfigurací “Add inbound security rule“ v sekci “networking“. Zde dosadíme hodnotu 3000 do pole “Destination port ranges“ a nastavíme jméno Port3000 v poli “Name“



Obrázek 44 Otevření portu 3000

(Zdroj: Vlastní zpracování)

Nyní se lze přihlásit do grafany přes IP adresu s portem 3000 a přihlašovací jméno “admin“ s heslem “admin“



Obrázek 45 Přihlašovací obrazovka Grafany

(Zdroj: Vlastní zpracování)

3.2.3 Nastavení SSL certifikátů

Jak si lze všimnout z předchozí kapitoly Grafana v tomto okamžiku funguje pouze na IP adrese a portu. To z praktického hlediska představuje velmi neintuitivní prostředí, které by bylo pro běžného uživatele krajně nevhodné.

Každá webová stránka v produkčním prostředí a dostupná pro veřejnost má své doménové jméno, např. "google", "seznam", "vut". Azure umožňuje nastavit takové doménové jméno, ale za předpokladu, že by výsledný systém fungoval pouze na starším protokolu HTTP místo novějšího a lépe zabezpečeného HTTPS. Pro tento projekt je využit nástroj LetsEncrypt, který poskytuje certifikát pro šifrování komunikace, s tím, že jeho platnost vyprší po 30 dnech. To řeší nástroj Certbot, který automaticky žádá o obnovení certifikátu bez nutnosti manuálního zásahu.

Nyní je potřeba nastavit SSL certifikát pro nově implementovaný systém. Pro tento projekt bylo stanoveno doménové jméno mkografana.northeurope.cloudapp.azure.com. Po ověření, že toto jméno je volně přístupné a není využíváno jinou webovou stránkou, je třeba nakonfigurovat Grafanu.

V prvním kroku je zapotřebí vytvořit skupinu pro manipulaci s SSL certifikáty:

```
sudo groupadd sslcerts
```

V dalším kroku se vytvoří adresáře jednotlivých certifikátů s modifikací oprávnění

```
sudo mkdir /etc/letsencrypt
sudo mkdir /etc/letsencrypt/archive
sudo mkdir /etc/letsencrypt/live
sudo chown -R root:sslcerts /etc/letsencrypt/
sudo chmod 755 /etc/letsencrypt/archive
sudo chmod 755 /etc/letsencrypt/live
```

Po této úpravě práv zbývá samotná instalace Certbota. Ta je provedena následujícími příkazy

```
sudo apt install -y certbot
sudo certbot certonly –standalone
```

V procesu instalace je zapotřebí poskytnou emailovou adresu, odsouhlasit podmínky použití a zadat požadovanou doménu, jak je ukázáno na obrázku 46

```
Please enter in your domain name(s) (comma and/or space separated)  (Enter 'c'
to cancel): grafana-dokumentace.northeurope.cloudapp.azure.com
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for grafana-dokumentace.northeurope.cloudapp.azure.com
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/grafana-dokumentace.northeurope.cloudapp.azure.com/full
chain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/grafana-dokumentace.northeurope.cloudapp.azure.com/priv
key.pem
   Your cert will expire on 2022-12-28. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
```

Obrázek 46 Podmínky použití LetsEncrypt

(Zdroj: Vlastní zpracování)

Pro dokončení celého procesu je nutné se přihlásit do konfigurace Grafany a změnit doménu a cestu pro nalezení jednotlivých certifikátů vygenerovaných Encryptem, opětovně změnu lze vidět na přiloženém obrázku.

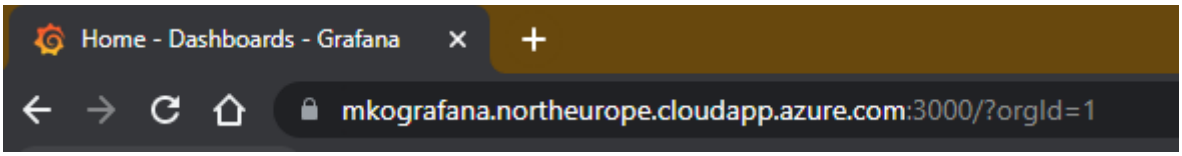
```
  GNU nano 2.9.3                    /etc/grafana/grafana.ini

# Protocol (http, https, h2, socket)
protocol = https

# The ip address to bind to, empty will bind to all interfaces
;http_addr =

# The http port  to use
;http_port = 3000

# The public facing domain name used to access grafana from a browser
domain = mkografana.northeurope.cloudapp.azure.com

# Redirect to correct domain if host header does not match domain
# Prevents DNS rebinding attacks
enforce_domain = true

# The full public facing url you use in browser, used for redirects and emails
# If you use reverse proxy and sub path specify full url (with sub path)
root_url = https://mkografana.northeurope.cloudapp.azure.com

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

```
  GNU nano 2.9.3                    /etc/grafana/grafana.ini                Modified

# Serve Grafana from subpath specified in `root_url` setting. By default it is set to `false` for com$
;serve_from_sub_path = false

# Log web requests
;router_logging = false

# the path relative working path
;static_root_path = public

# enable gzip
;enable_gzip = false

# https certs & key file
cert_file = /etc/letsencrypt/live/mkografana.northeurope.cloudapp.azure.com/fullchain.pem
cert_key = /etc/letsencrypt/live/mkografana.northeurope.cloudapp.azure.com/privkey.pem

# Unix socket path
;socket =

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo
```

Obrázek 47 Upravení doménových jmen v konfiguračním souboru Grafany

(Zdroj: Vlastní zpracování)

Nyní, pokud je zadána adresa mkografana.northeurope.cloudapp.azure.com do prohlížeče, lze vidět že systém funguje na zabezpečeném https doméně s požadovaným doménovým jménem



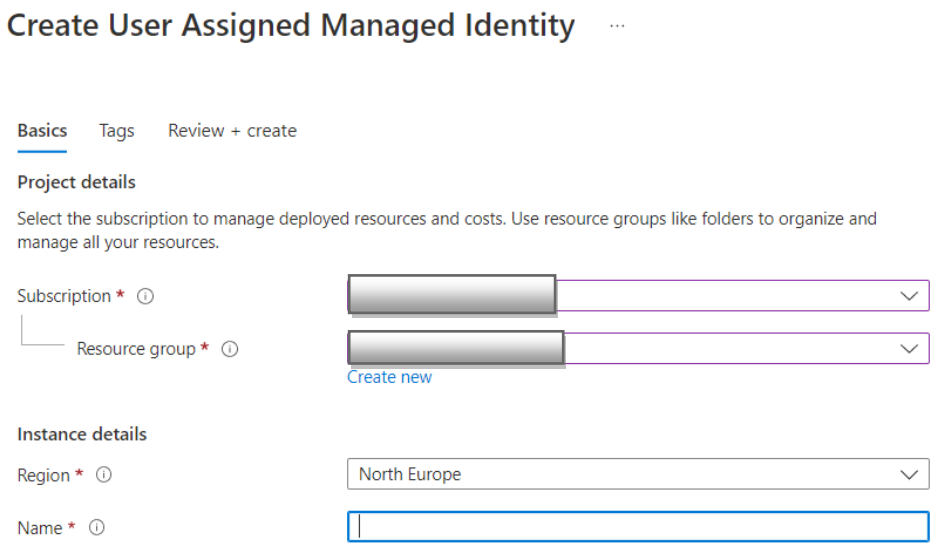
Obrázek 48 Grafana s požadovaným doménovým jménem

(Zdroj: Vlastní zpracování)

3.2.4 Propojení Grafany s Azure

Na základě předchozích dvou podkapitol je systém ve stavu, kdy je implementovaná plně funkční grafana na dostupné webové stránce. Tato podkapitola bude věnována samotnému propojení Grafany s daty ze Sentinelu. Za tímto účelem se využívá služba azure nazvaná Managed Identities, jenž je detailně popsaná v 1.2.3 Azure Managed Identities

V nabídce Azure managed identitites se vybere možnost “Create new“. Zobrazí se okno na obrázku 49



Obrázek 49 User Managed Identities

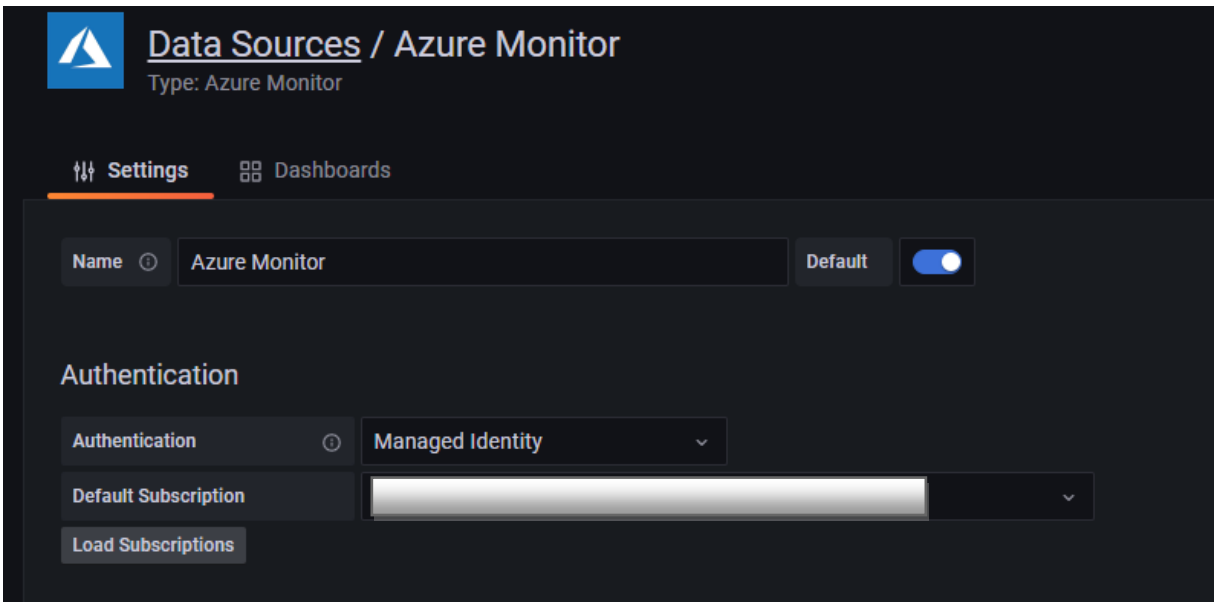
(Zdroj: Vlastní zpracování)

Pak stačí pouze přiřadit jméno a kliknout na “Create“. Nově přidané identitě je nutná přidat potřebná práva pro manipulaci s daty. V tomto konkrétním případě se bude jednat o “Logs analytic reader“, jak lze vidět obrázku 50

Obrázek 50 Propojená VM se Sentinelem

(zdroj: Vlastní zpracování)

Poté je zapotřebí v systému Grafany nastavit datový zdroj jako „Managed Identity“ a vybrat subscription ke které má nastavena práva



Obrázek 51 Připojený datový zdroj s Azure

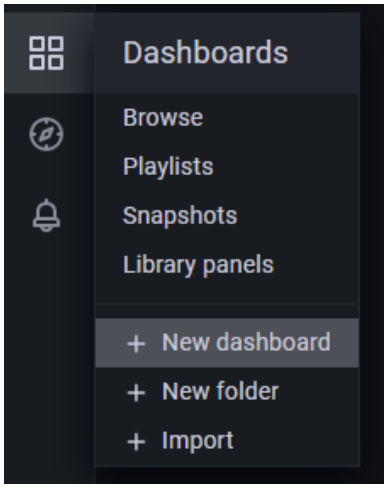
(Zdroj: Vlastní zpracování)

V tomto momentu je Grafana plně propojená s daty z cloudového prostředí a je možné vytvořit informační systém pro plnohodnotnou správu incidentů.

3.2.5 Vytvoření Dashboardu a grafů

Obecnému prostředí Grafany je věnovaná kapitola 1.2.5 Grafana a proto zde bude uveden pouze implementační postup. Nyní je třeba přistoupit k samotnému vytvoření dashboardu, ve kterém budou zachyceny stávající a nově implementované grafy.

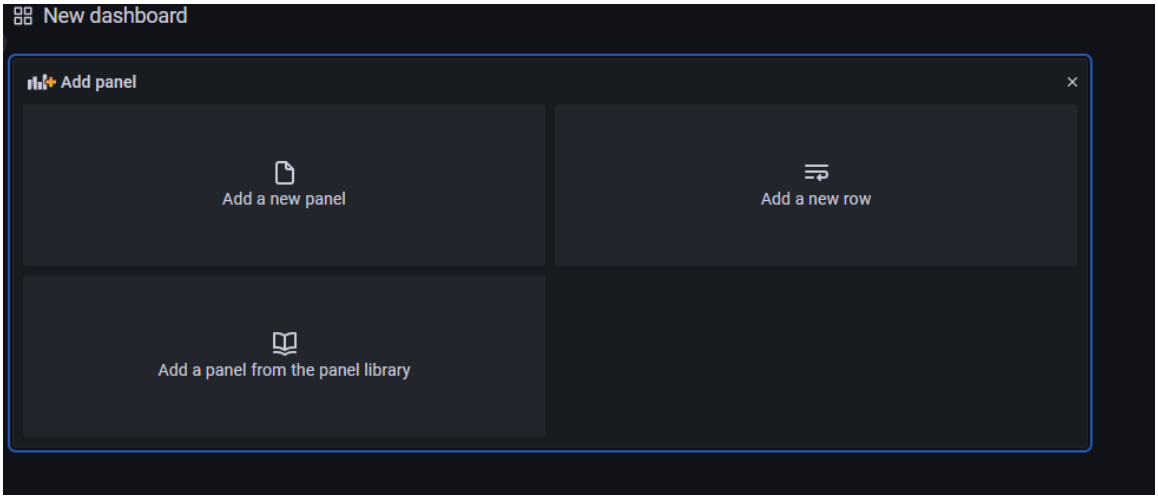
V levé části navigace se pod sekcí Dashboards nachází možnost „New dashboard“, pomocí které se vytvoří dashboard.



Obrázek 52 Menu pro vytvoření dashboardu

(Zdroj: Vlastní zpracování)

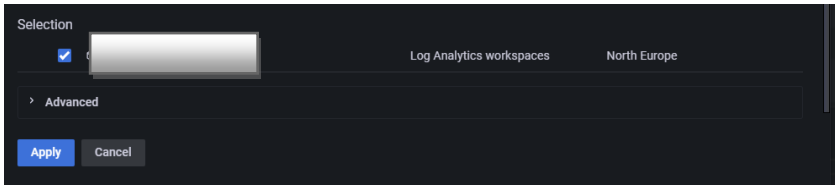
Následně se vytvoří nový dashboard s výchozím názvem „New dashboard“. Nyní lze přistoupit k realizační fázi grafů. V kolonce „Add panel“ jsou 3 různé možnosti. V projektu bude využita pouze jediná varianta „Add a new panel“



Obrázek 53 Přidání panelu

(Zdroj: Vlastní zpracování)

Nyní je třeba vybrat datový zdroj pro graf. Veškerá data budou pramenit z prostředí Azure. Vybereme tedy v sekci „Data source“ možnost „Azure Monitor“. Zvolí se prostředky určené k monitorování a možnost se potvrdí „Apply“, jak je znázorněno na přiloženém obrázku.



Obrázek 54 Vybrání datového zdroje

(Zdroj Vlastní zpracování)

Graf je po dokončení předchozího kroku spojený s analytickou částí určenou pro sbírání logů a lze získávat daty přes jazyk KQL, konkrétně popsaný v části 1.2.4 KQL.

Výše popsaný postup bude aplikovaný na veškeré implementované grafy. Podstatný rozdíl bude představovat kód KQL, jež bude v každém grafu rozdílný.

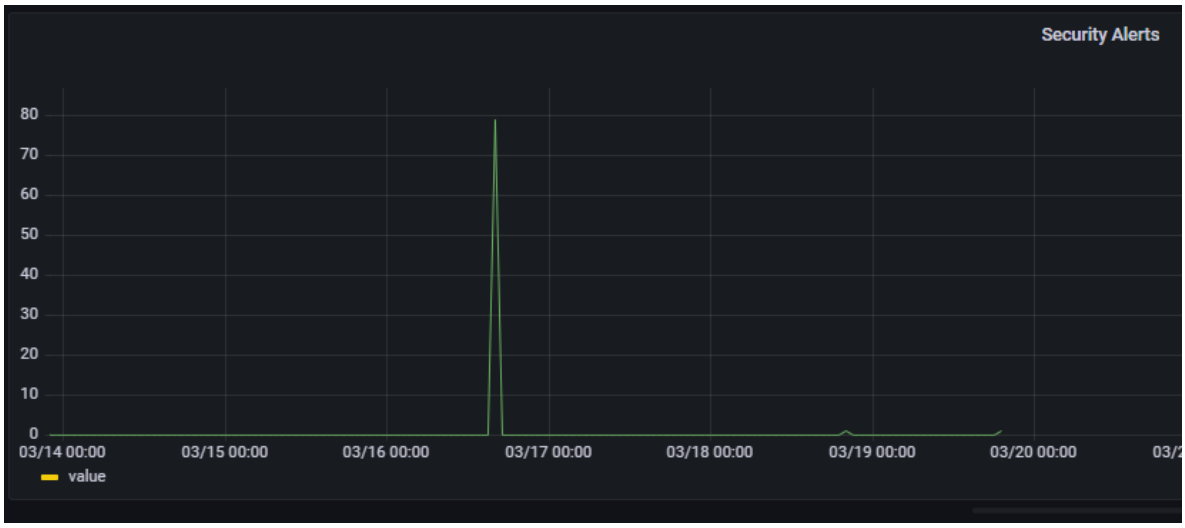
Je nutné se zaměřit na první graf. Ten bude monitorovat identifikované upozornění v průběhu času. Podle výše uvedeného postupu se vytvoří graf a zadá se kód z následujícího obrázku

```
SecurityAlert
| make-series value=count() default=0
    on TimeGenerated
    step 1h
    by ProviderName
| mv-expand TimeGenerated to typeof(datetime), value to typeof(int)
| order by TimeGenerated, ProviderName asc
```

Obrázek 55 Kód k Security alerts

(Zdroj: Vlastní zpracování)

SecurityAlert představuje primární tabulku, která uchovává data o zachycených alertech. Protože graf bude obsahovat časovou osu je nutné ho doplnit o příkaz o „make-series“ s agregační funkcí „count()“, pro zjištění počtu incidentů. Časový údaj pro graf bude vycházet z položky „Time Generated“, tedy přesného času identifikace systémem. Dále se použije operátor „mv-expand“ k rozbalení časové řady do samostatných řádků pro každý datový bod. To umožňuje vykreslit data jako graf, kde osa x představuje čas a osa y počet bezpečnostních alertů. Nakonec se k seřazení dat podle času a názvu poskytovatele použije operátor „order by“.



Obrázek 56 Security Alerts graf

(Zdroj: Vlastní zpracování)

Dalším objektem k vizualizaci bude tabulka obsahující specifikaci jednotlivých incidentů, kde se zobrazí kompletní výpis veškerých parametrů, které lze k incidentům dohledat v databázi. Pro vypsání se tedy použije pouze SecurityIncident.

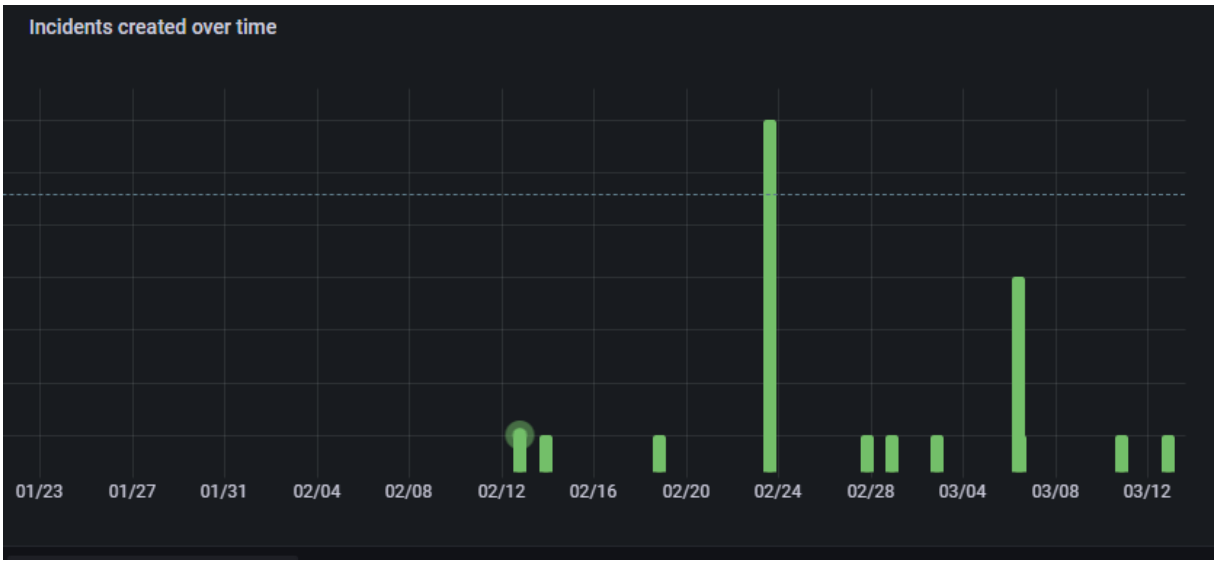
Security Incident

TenantId	TimeGenerated	IncidentName	Title	Description	Severity
bd75d088-ad3e-445...	2023-02-27 20:27:3...	51f93e94-6888-4ba...	Traffic detected fro...	Defender for Cloud ...	Low
bd75d088-ad3e-445...	2023-02-27 20:27:3...	51f93e94-6888-4ba...	Traffic detected fro...	Defender for Cloud ...	Low
bd75d088-ad3e-445...	2023-02-28 22:51:4...	f5d06be8-1522-432...	Traffic detected fro...	Defender for Cloud ...	Low
bd75d088-ad3e-445...	2023-02-28 22:51:5...	f5d06be8-1522-432...	Traffic detected fro...	Defender for Cloud ...	Low
bd75d088-ad3e-445...	2023-03-06 09:52:1...	fbaf5990-3ab5-4f44...	test		Medium
bd75d088-ad3e-445...	2023-03-06 09:52:4...	8071759d-70bd-43...	test		Medium
bd75d088-ad3e-445	2023-03-06 09:52:5	ed76749e-5928-403	test		Medium

Obrázek 57 Security Incident tabulka

(Zdroj: Vlastní zpracování)

Následuje další nově vytvořený graf pro zobrazení všech incidentů, které se objevily za libovolné monitorované období. Uživatel má možnost přizpůsobovat sledované období tlačítkem umístěným v každém grafu.



Obrázek 58 Incidents created over time graf

(Zdroj: Vlastní zpracování)

Byl vytvořen obdobným způsobem jako graf k zobrazení alertů. Nyní si projdeme jednotlivé řádky kódu.

```
SecurityIncident
| summarize arg_max(TimeGenerated, Status, Severity, Owner, AdditionalData,CreatedTime) by IncidentNumber
| extend Tactics = todynamic(AdditionalData.tactics)
| extend Owner_new = todynamic(Owner.assignedTo)
| extend Product = todynamic((parse_json(tostring(AdditionalData.alertProductNames))[0]))
| summarize count() by bin(CreatedTime, 1h)
| project-rename Incidents = count_
```

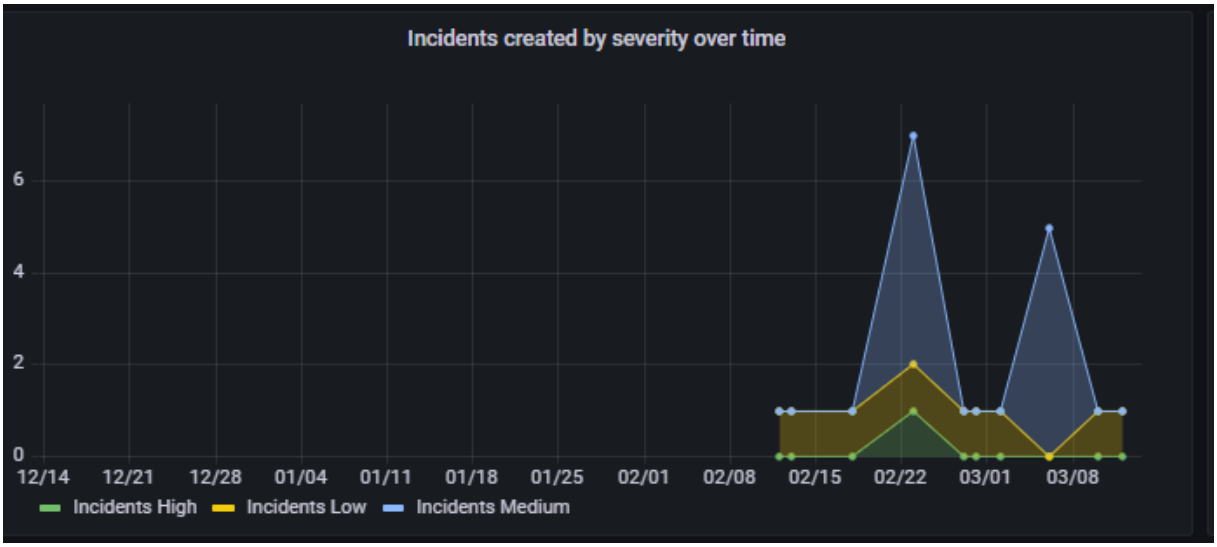
Obrázek 59 KQL kód k Incidents created over time grafu

(Zdroj: Vlastní zpracování)

Opětovně prvním krokem musí být zvolení tabulky, ze které budou brány data. V tomto případě se bude jednat o tabulku SecurityIncident. Následně se seskupí data podle čísla incidentu a vypočítá maximální hodnotu zadaných polí (TimeGenerated, Status, Severity, Owner, AdditionalData, CreatedTime). Ponechá se řádek s maximální hodnotou. V dalším kroku se vytvoří nový sloupec s názvem Tactics převedením pole JSON AdditionalData.tactics na dynamický objekt. To stejné provedeme pro nově vytvořený sloupec Owner_new. Protože všechny data nejsou uložena v jednotlivých sloupcích, ale objevuje se zde Product, jenž je potřeba rozparsovat z existujícího json soubor. Převede se pole JSON AdditionalData.alertProductNames na řetězec, rozebere se zpět na JSON a vezme se první prvek pole. Poté převede výslednou hodnotu na dynamický objekt. Následně se seskupí data podle sloupce CreatedTime s velikostí bin 1 hodina (což znamená, že spočítá

počet incidentů, které se vyskytnou v každé hodině). Poté vypočítá počet incidentů pro každý časový bin. Na závěr se přejmenuje celkově počet incidentů na count_

Další grafy se velmi podobají grafům předchozím až na to, že nový dotaz se zaměřuje na počítání odlišného počtu incidentů podle závažnosti (High, medium, low), zatímco původní dotaz počítá celkový počet incidentů podle hodin.

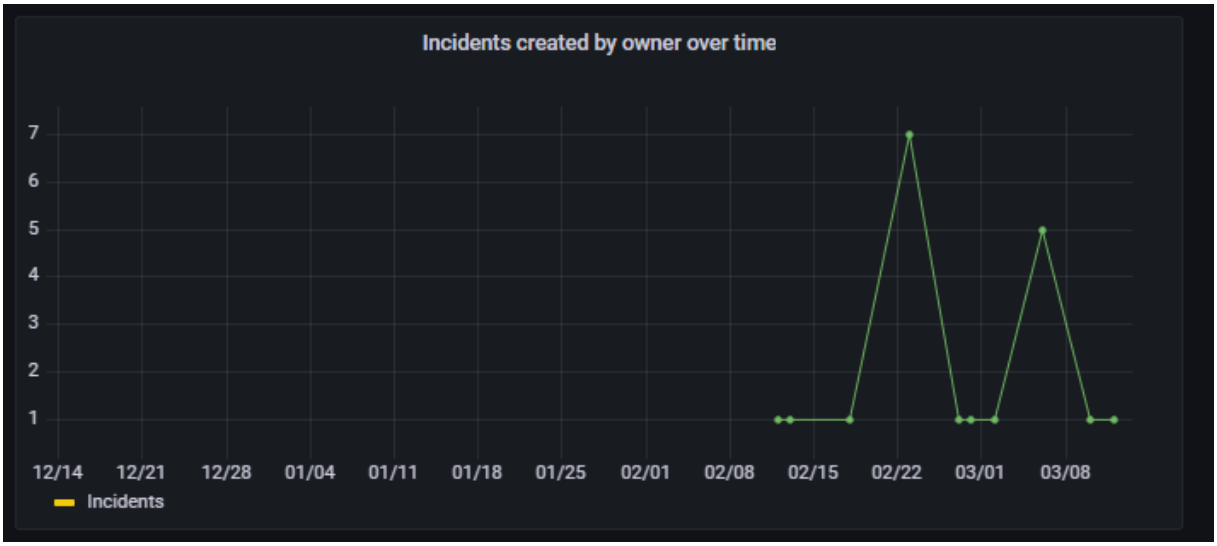


Obrázek 60 Incidents created by severity over time

(Zdroj: Vlastní zpracování)

```
SecurityIncident
| extend Tactics = todynamic(AdditionalData.tactics)
| extend Owner_new = todynamic(Owner.assignedTo)
| extend Product =
todynamic((parse_json(tostring(AdditionalData.alertProductNames))[0]))
| summarize Incidents=dcount(IncidentNumber) by Severity, bin(CreatedTime, 1d)
| order by CreatedTime asc
```

Opětovně další varianta výše popsaného grafu. V tomto případě rozdělená podle vlastníka incidentu.



Obrázek 61 Incidents created by owner over time

(Zdroj: Vlastní zpracování)

```
SecurityIncident
| extend Tactics = todynamic(AdditionalData.tactics)
| extend Owner_new = todynamic(Owner.assignedTo)
| extend Product =
todynamic((parse_json(tostring(AdditionalData.alertProductNames))[0]))
| summarize Incidents=dcount(IncidentNumber) by case(tostring(Owner_new)=="",
"Unassigned",tostring(Owner_new)), bin(CreatedTime, 1d)
| order by CreatedTime desc
```

Poslední graf představuje celkový počet incidentů rozdělených dle závažnosti. Na rozdíl od svých předchůdců nepracuje s časovou osou, ale pouze agreguje data do donutového grafu.

Obrázek 62 Incidents created by severity

(Zdroj: Vlastní zpracování)

```
SecurityIncident
| summarize arg_max(TimeGenerated,Status, Severity, Owner, AdditionalData) by
IncidentNumber
| extend Tactics = todynamic(AdditionalData.tactics)
| extend Owner_new = todynamic(Owner.assignedTo)
| extend Product =
todynamic((parse_json(tostring(AdditionalData.alertProductNames))[0]))
| summarize dcount(IncidentNumber) by Severity
| order by Severity asc
```

3.2.6 Monitoring

Po zavedení monitorovacího prostředí je potřeba stanovit typy uživatelů, kteří budou mít přístup k jednotlivým ukazatelům. Je důležité zmínit, že výše popsané grafy jsou pouze prvními mezi řadou dalších, které se postupně do systému budou doplňovat v závislosti na dostupnosti personálu společnosti. Proto v této kapitole budou popsány i grafy, které jsou implementované v současném nebo jiném systému a se zavedením do Grafany se do budoucna počítá.

Rozeznáváme následující typy uživatelů:

SOC analytik – hlavní uživatel systému. Jedná se o odborníka, jenž se zaměřuje na monitorování, detekci, analýze a reakci na kybernetické hrozby a bezpečnostní incidenty. Pomocí různých bezpečnostních nástrojů neustále kontrolují možné průniky a identifikovali podezřelou aktivitu. Pokud takový incident analytik provede triáž, což zahrnuje sběr informací, analýzu incidentu a podle závažnosti ho buď vyřeší v podobě izolace napadeného systému nebo odstranění škodlivého prvku. Pokud se jedná o závažný incident, analytik eskaluje incident k vyšší odpovědnosti. Všeobecně se rozlišují 3 prvky úrovní: SOC analytik L1, SOC analytik L2, SOC analytik L3.

- SOC analytik L1: Základní úroveň analytika. Většinou se jedná o začátečníky v oboru, často o absolventy informačních oborů na začátku kariéry v kyberbezpečnosti. Pro tuto úroveň je většinou spojena práce s monitoringem incidentů a firewallů, kategorizují bezpečnostní události na základě rizik a závažnosti a filtrují falešné poplachy. Také pracují na triáži a eskalaci incidentů na vyšší úroveň, pokud je to nutné. Mají přístup pouze k základním grafům pro filtrování a monitoring incidentů, jejichž část byla představena v kapitole 3.2.5.

- SOC analytik L2: Střední úroveň SOC analytika, která zahrnuje odborníky se středně pokročilými znalostmi a zkušenostmi. Provádí hlubší analýzu a vyšetřování incidentů, které byly eskalovány úrovní L1 a používají pokročilé analytické nástroje a techniky pro identifikaci a zjištění rozsahu hrozeb. Koordinují jednotlivé týmy k nápravě incidentů a vytváří metodiky pro zlepšení bezpečnosti organizace, aby k incidentům nedocházelo. Analytici na této úrovni mají krom přístupům ke informačním zdrojům L1 i možnost sledovat eskalaci incidentů přesměrovaných z L1, změny v konfiguraci

systémů a sítě, uživatelských aktivit a přístupových práv.

- SOC analytik L3: Nejvyšší úroveň SOC analytika, zkušení odborníci s hlubokými znalostmi v oblasti kybernetické bezpečnosti. Řeší nejkomplexnější a nejkritičtější bezpečnostní incidenty, které vyžadují vysokou úroveň odborných znalostí a zkušeností. Provádějí pokročilý výzkum hrozeb a vytvářejí strategie pro ochranu proti novým a neznámým hrozbám. Působí jako mentoři a školitelé pro mladší členy týmu a přispívají k vývoji dovedností a znalostí v rámci organizace. Krom přístupu ke grafům L1 a L2 mají navíc přístup ke grafům pokročilých hrozeb, úspěšnosti týmu, četnosti incidentů podle hodin a dalším zmíněných v Tabulce 1 – Použité grafy.

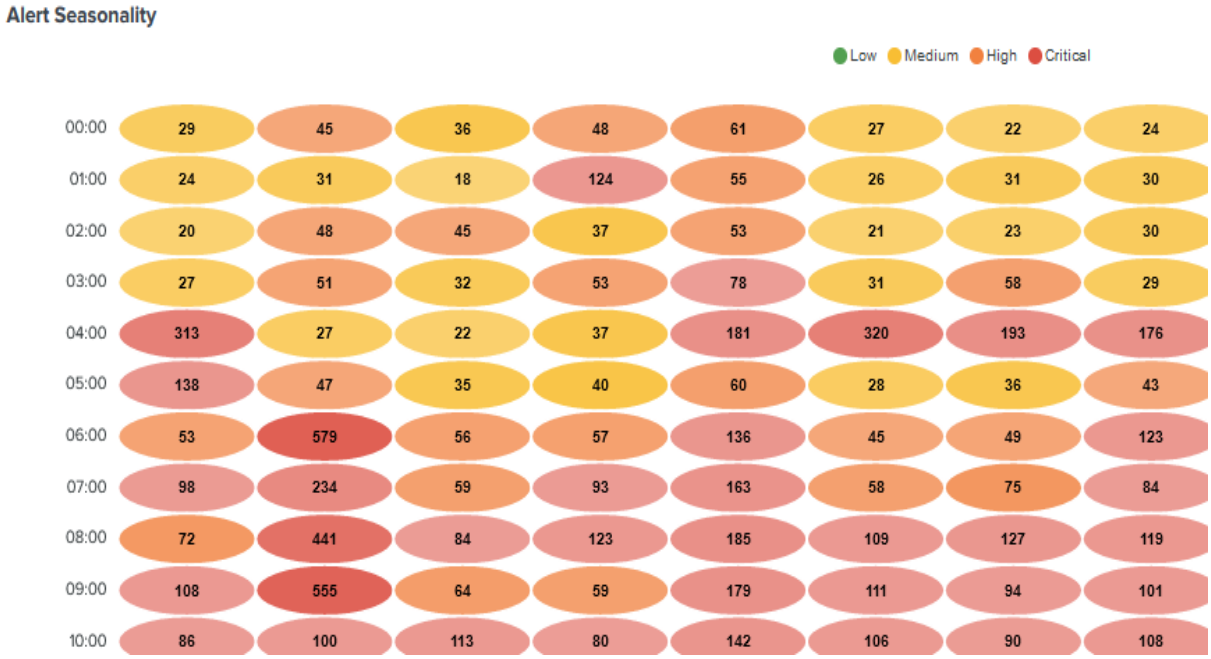
Správce systému – Administrátor zodpovědný za celý systém Grafany, má na starost její údržbu, instalaci nových verzí, nasazením v Azure cloudu a také má práva na stahování případných pluginů, které by zahrnovaly nové vizualizace pro SOC tým. Má přístup ke všem uživatelům, dashboardům, týmům a podle potřeby může udělovat práva.

Manažer – Product owner, kterému byla Grafana dodána pro monitoring bezpečnostních incidentů. Tato skupina má přístup pouze k určitým grafům. Manažeři často nemají odborné znalosti a zkušenosti potřebné k interpretaci a analýze technických detailů prezentovaných v grafu. Přístup ke všem grafům by mohl vést k nedorozuměním nebo nesprávným závěrům.

Konzultant – Slouží jako prostředník mezi klientem a PwC. V případě, že by klient projevil zájem o bezpečnostní SIEM řešení, konzultant zajistí hladký průběh implementace. Shromáždí data od klienta a zanalyzuje jeho současné řešení. Zná velmi dobře systém Grafany, její možnosti z hlediska administrace uživatelů, grafů, dashboardů a podle toho může učinit nabídku klientovi a nabídnou mu řešení šité na míru. Proto stejně jako správce systému má přístup ke všem grafům, s tím rozdílem, že nemůže přidávat, modifikovat či odebírat uživatele a nemá oprávnění na změny infrastruktury v Azure.

Mnohé z grafů, které byly implementovány v kapitole 3.2.5 představují základní úroveň monitoringu, určené především pro analytiky úrovně L1. To je dáno především požadavky společnosti, která si přála pouze implementovat Grafanu a zjistit možné budoucí perspektivy dodávání systémů klientů. V průběhu zpracování diplomové práce bylo vytvořeno několik námětů na grafy pro jednotlivé typy uživatelů. Tyto náměty se získaly na základě požadavků analytiků a její vizualizace se čerpala z různých systémů. Příkladem může být Alert

Seasonality (Obrázek 63) ze systému Splunk, která ukazuje četnost incidentů podle hodin, na jejichž základě kterých se plánují směny v SOC týmu.



Obrázek 63 Alert Seasonality ze systému Splunk

(Zdroj: Vlastní zpracování)

Na základě požadavků tedy byly zpracovány následující grafy a přiřazen typ uživatelů, kteří k nim budou mít přístup.

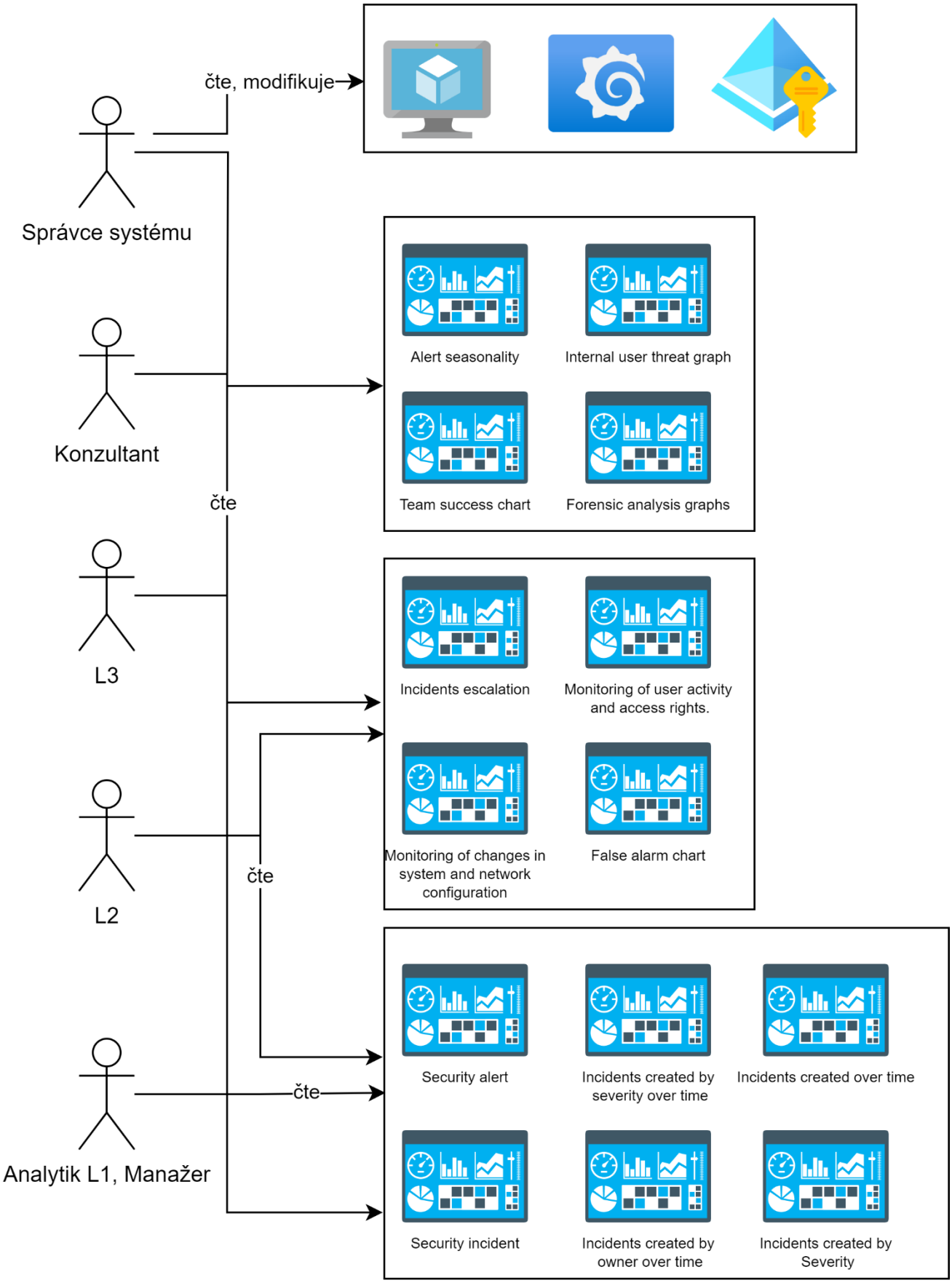
Název grafu	Typ uživatelů	Popis
Security alert	L1, L2, L3, Konzultant, Správce, Manažer	Graf poukazující na bezpečnostní výstrahy zjištěné v síti nebo systémech organizace za určité časové období. Tento graf je navržen tak, aby poskytoval jasný a stručný přehled o bezpečnostních událostech a umožnil analytikům SOC a dalším pracovníkům rychle identifikovat trendy, stanovit priority zdrojů a účinně reagovat na incidenty.
Security incident	L1, L2, L3, Konzultant, Správce, Manažer	Graf pro měření bezpečnostních incidentů, které byly identifikovány, vyšetřeny a zvládnuty v rámci sítě nebo systémů organizace za určité období. Cílem tohoto grafu je poskytnout ucelený přehled o bezpečnostních incidentech, který analytikům SOC, bezpečnostním pracovníkům a vedení umožní rychle rozpoznat vzorce, rozdělit zdroje a zlepšit strategie reakce na incidenty
Incidents created over time	L1, L2, L3, Konzultant, Správce, Manažer	Vizuální znázornění počtu bezpečnostních incidentů vytvořených v síti nebo systémech organizace za určité časové období. Tento graf je navržen tak, aby poskytoval snadno pochopitelný přehled trendů vytváření incidentů.
Incidents created by severity over time	L1, L2, L3, Konzultant, Správce, Manažer	Poskytuje vizuální zobrazení bezpečnostních incidentů vytvořených v síti nebo systémech organizace, roztříděných podle úrovně závažnosti za určité časové období.
Incidents created by owner over time	L1, L2, L3, Konzultant, Správce,	Vizuální zobrazení bezpečnostních incidentů vytvořených v síti nebo systémech organizace, rozdělených do kategorií podle jednotlivce

	Manažer	nebo týmu odpovědného za jejich řešení (vlastníka) za určité časové období.
Incidents created by Severity	L1, L2, L3, Konzultant, Správce, Manažer	Vizuální zobrazení bezpečnostních incidentů vytvořených v síti nebo systémech organizace, rozdělených do kategorií podle úrovně závažnosti.
Incidents escalation	L2, L3, Konzultant, Správce,	Graf je vizuální znázornění bezpečnostních incidentů v síti nebo systémech organizace, které byly eskalovány na vyšší úroveň závažnosti nebo přiřazeny jinému vlastníkovi k dalšímu prošetření a řešení za určité časové období. Tento graf je navržen tak, aby mohl optimalizovat přidělování zdrojů na základě eskalace incidentů.
Monitoring of changes in system and network configuration	L2, L3, Konzultant, Správce,	Graf je vizuální zobrazení změn provedených v konfiguraci systémů a síťových zařízení v rámci síťové infrastruktury organizace za určité časové období.
Monitoring of user activity and access rights.	L2, L3, Konzultant, Správce,	Vizuální zobrazení aktivity uživatelů, včetně požadavků na přístup a udělených oprávnění v rámci sítě, systémů nebo aplikací organizace za určité časové období.
False alarm chart	L2, L3, Konzultant, Správce,	Představuje vizuální znázornění falešných poplachů generovaných bezpečnostními monitorovacími a výstražnými systémy organizace za určité časové období.
Alert seasonality	L3, Konzultant, Správce,	Graf představuje sofistikovanou vizualizaci výskytu incidentů v závislosti na denní hodině. Toto znázornění založené na datech hraje klíčovou roli při rozeznávání časových vzorců v projevech incidentů. Vzhledem k poznatkům získaným z tohoto grafu je analytik SOC 3. úrovně (L3) vybaven pro strategické

		navrhování rozvrhů směn pro tým bezpečnostního operačního střediska (SOC). Toto optimální rozdělení lidských zdrojů přímo odpovídá předpokládanému objemu incidentů, čímž je zajištěno, že připravenost týmu odpovídá očekávanému zatížení incidenty, a tím se zvyšuje celková efektivita a schopnost reakce SOC.
Team success chart	L3, Konzultant, Správce,	Graf slouží pro monitorování úspěšnosti jednotlivých týmů zodpovědných za řešení incidentů. Podle míry úspěšnosti vyřešených bezpečnostních hrozeb má analytik možnost modifikovat týmy a jejich členy, tak aby úspěšnost byla co největší.
Internal user threat graph	L3, Konzultant, Správce,	Graf představuje vizuální znázornění identifikovaných potenciálních hrozeb, podezřelých aktivit nebo porušení, které se týkají interních uživatelů v rámci sítě, systémů nebo aplikací organizace za určité časové období.
Forensic analysis graphs	L3, Konzultant, Správce,	Jedná se o soubor vizuálních zobrazení digitálních forenzních dat získaných ze sítě, systémů nebo aplikací organizace za určité období. Tyto grafy jsou navrženy tak, aby nabízely podrobný a jasný přehled různých forenzních aspektů, jako jsou časové osy událostí, síťový provoz, aktivita souborů, chování uživatelů a další.

Tabulka 1 Návrhy grafů pro SOC tým v Grafaně

(Zdroj: Vlastní zpracování)



Obrázek 64 Use case diagram nového řešení

(Zdroj: Vlastní zpracování)

3.2.7 Budoucí možná rozšíření řešení

Pro zajištění všech budoucích potřeb z perspektivy IT byl v průběhu projektu zjištěn velký počet možností, jejichž integrací do projektu by se zlepšila výkonnost systému nebo její udržitelnost. Zde je uvedeno několik takových, na které by se měla společnost z dlouhodobého pohledu zaměřit a aplikovat aspoň určitou část:

- Provedení podrobné srovnávací analýzy pracovních knihoven Grafana a Azure z hlediska výkonu, škálovatelnosti a sad funkcí, která by organizacím poskytla komplexnější pochopení silných a slabých stránek jednotlivých platforem.
- Prozkoumání možnosti integrace platformy Grafana s dalšími službami Azure, s cílem rozšířit možnosti platformy a zefektivnit pracovní postupy v oblasti bezpečnosti.
- Zkoumání možností vývoje vlastních zásuvných modulů a rozšíření Grafany na základě potřeb analytiků kybernetické bezpečnosti, včetně pokročilých funkcí detekce hrozeb, reakce na incidenty a řízení rizik
- Posouzení možností využití strojového učení a umělé inteligence v rámci Grafana a Azure pro zlepšení prediktivní analýzy, automatické detekce vzorců a odhalování anomálií, což by vedlo ke zlepšení proaktivního řešení problémů a minimalizaci výpadků.
- Analýza zkušeností uživatelů a přizpůsobení Grafana v Azure prostředí s cílem zlepšit uživatelské rozhraní a zjednodušit procesy, které by usnadnily adopci nástroje pro širší spektrum uživatelů s různými úrovněmi odborných znalostí.
- Zkoumání potenciálu Grafana v Azure pro podporu hybridních a více-cloudových prostředí, což by umožnilo organizacím flexibilnější a snadnější migraci mezi různými cloudovými poskytovateli a současně zachovalo integritu dat a soudržnost monitorování.
- Poskytování podrobných školení a vzdělávacích materiálů pro uživatele Grafana v Azure prostředí, které by zahrnovalo nejlepší postupy, tipy a triky pro efektivní využití obou platforem, zlepšení produktivity a zrychlení řešení problémů.
- Zavedení pokročilé automatizace IaaS pomocí nástroje Terraform a Ansible.

3.3 Ekonomické zhodnocení

3.3.1 Přínosy řešení

Prospěšnost informačního systému lze posuzovat různými pohledy. Příklady několika z nich mohou být následující:

Kvalitativní přínosy – tyto přínosy souvisí s kvalitou práce, která je díky informačnímu systému zlepšena. Navrhnuté řešení prokázalo přinos ve zvýšení počtu typů grafů, které byly v původním řešení pouze v omezené podobě. Grafana nabízí širokou škálu možností vizualizace, které jsou vysoce přizpůsobitelné, interaktivní a esteticky přitažlivé. Tato flexibilita umožňuje bezpečnostním analytikům vytvářet komplexnější a přehlednější dashboardy přizpůsobené jejich specifickým potřebám, což v konečném důsledku zlepšuje jejich porozumění podkladovým datům a umožňuje lepší rozhodování. Tím, že se jedná o opensource řešení je i možnost implementace dalších různých grafů a prvků z řad komunity, zároveň se dostává i podpory napříč skalními fanoušky tohoto řešení a to zajišťuje, že platforma zůstává v souladu s nejnovějšími inovacemi v oblasti vizualizace dat a dokáže se přizpůsobit vyvíjejícím se potřebám profesionálů v oblasti kybernetické bezpečnosti.

Strategické přínosy – po aplikaci Grafany pro SOC použití by tento nástroj mohl představovat dlouhodobý benefit pro klienty, jenž by rádi implementovali další prvky opatření z hlediska kyberbezpečnosti. Přínos by mohl jít i do dalších segmentů, které PwC nabízí. Vzhledem k tomu, že nástroj nemusí nutně sloužit jen pro monitorování incidentů, ale má univerzální použití, mohl by se uplatnit pro datovou analýzu klienta nebo sledování vytíženosti infrastruktury v reálném čase. Využitelnost napříč oblastmi je natolik široká, což je zapříčiněno faktem, že každý segment potřebuje určitý program pro sledování dat.

3.3.2 Náklady

V této části budou shrnuty náklady za implementaci systému. Do analýzy jsou započítány MD strávené vývojem a měsíční poplatky nutné za provoz infrastruktury řešení.

Jednotlivé části implementace	Počet MD
Analýza požadavků firmy	2
Analýza Grafany	4
Nasazení serveru hostovaného v Azure	2
Konfigurace serveru	4
Instalace Grafany	1
Konfigurace Grafany na straně server	3
Nastavení DNS a SSL	4
Zavedení Managed Identities	4
Tvorba grafů a dashboardů v Grafaně	4
Testování aplikovatelnosti grafů	10
Tvorba dokumentace	4
Školení	5
Celkem	**47**

Tabulka 2 Ekonomické zhodnocení implementace

(Zdroj: Vlastní zpracování)

Nacenění za jeden MD bylo stanoveno na 2000 Kč. Dojde-li k vynásobení sazby s celkovým počtem MD, konečná suma za projekt činí 94 000 Kč.

Pokud by zadání bylo řešeno externí firmou, kdy průměrná sazba cloudového podle kvalifikovaného odhadu ze interních HR zdrojů firmy pro MD sazby externích dodavatelů činí 4000 Kč, tak by náklady byly dvojnásobné.

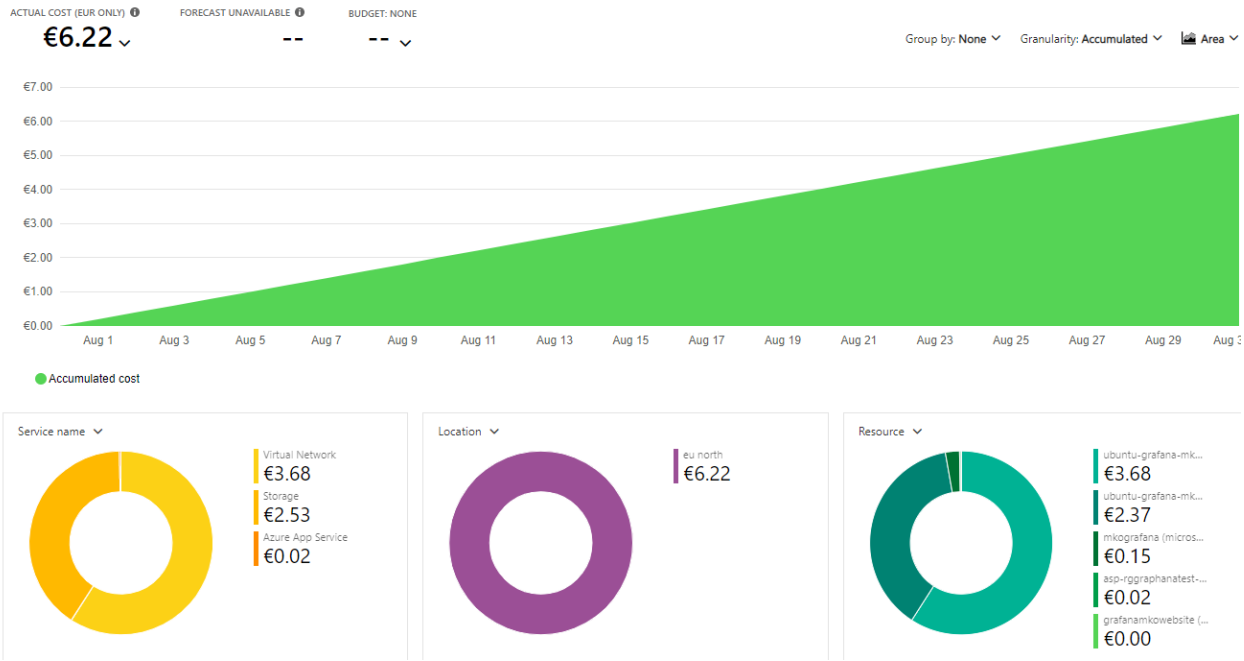
K nákladům je potřeba přidat i měsíční poplatek za Azure VM, na kterém Grafana funguje. Server funguje na instanci DS1 v2 s operační pamětí 3,5 GiB. Předplatné je stanoveno pomocí „pay as you go“. V jehož rámci platíme pouze za hodiny spuštěného VM a úložného místa pro disk. Podle Microsoftu, předpokládaná částka by se pohybovala okolo 53.29 $ za měsíc dle obrázku 65.

Instance	vCPU(s)	RAM	Temporary storage	Pay as you go with AHB
DS1 v2	1	3.5 GiB	7 GiB	$53.2900/month

Obrázek 65 Odhadované měsíční náklady server

(Zdroj: Vlastní zpracování)

Tím, že náklady jsou razantně nižší, než u obvyklých IT projektů je dáno i nákladovou efektivností. Integrace Open source představuje a škálovatelnosti Azure představuje velmi úsporné řešení pro finance.



Obrázek 66 Ekonomické zhodnocení provozu infrastruktury

(Zdroj: Vlastní zpracování)

V případě, že by Grafana byla pouze alokovaná v Azure a nebyla v provozu vychází její údržba pouze na 6,82 $ (6.22 €).

Pokud převedeme výše popsané částky vychází nám provoz infrastruktury na 1 283,64 Kč měsíčně.

Celková cena implementace i se započítáním poplatku na údržbu infrastruktury činí 95 283,64 Kč.

ZÁVĚR

Cílem mé diplomové práce bylo posouzení současného informačního systému pro sledování incidentů (SIEM) společnosti PwC v cloudovém prostředí Azure. Na základě identifikovaných nedostatků byly navrhnuta implementace systému Grafany, která by zjištěné chyby napravila a zajistila nákladově efektivní variantu s bohatou mírou využitelnosti pro firmu napříč všemi divizemi.

Začátek práce se zaměřoval především na teoretická východiska práce, pojmy a i použité technologie, které byly zapotřebí detailně představit kvůli technickému zaměření práce.

Pro představu o aktuální situaci společnosti a důvodech, které přispěly k nutnosti výběru a implementace alternativního SIEM řešení je věnována kapitola Analýza současné situace. Zde je především popsána společnost a slabé stránky současného řešení

Třetí kapitola zahrnuje detailní popis nasazení systému v Azure prostřednictvím IaaS řešení, nasazení a konfiguraci serveru, instalaci Grafany prostřednictvím nástroje Putty a její napojení na cloudový SIEM systém Azure Sentinel. Následuje samotná operace s Grafanou, vytvářením dashboardů a jednotlivých grafů. Každý graf je zaměřený na sledování jiné části monitoringu incidentů, kdy je popsaný i KQL kód, který jednoznačně identifikuje data ze SIEM systému. V této kapitole jsou i nastíněny přínosy řešení, které poskytlo mimo vyřešení stanovených nedostatků v kapitole Analýza současné situace a také budoucí řešení, kudy se nový systém může posouvat a zlepšovat. V závěru kapitoly je zhodnocena ekonomická stránka s naceněným dílčích činností a měsíčních plateb spojené s cloudem.

Systém splnil požadované cíle pro společnost a je již zaveden a implementován v produkčním prostředí PwC.

ZDROJE

(1) Laudon, K. C., & Laudon, J. P. (2016). Management Information Systems: Managing the Digital Firm (14th ed.). Pearson.

(2) Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. MIS Quarterly, 36(4), 1165-1188.

(3) SKLENÁK, Vilém. Data, informace, znalosti a Internet. V Praze: C.H. Beck, 2001. C.H. Beck pro praxi. ISBN 80-7179-409-0.

(4) CONOLLY, Thomas, Carolyn E. BEGG a Richard HOLOWCZAK. Mistrovství - databáze: profesionální průvodce tvorbou efektivních databází. 1. vyd. Brno: Computer Press, 2009. 584 s. ISBN 978-80-251-2328-7.

(5) SODOMKA, Petr a Hana KLČOVÁ. Informační systémy v podnikové praxi. 2. aktualiz. a rozš. vyd. Brno: Computer Press, 2010. 501 s. ISBN 978-80-251-2878-7.

(6) Co je cloud – definice | Microsoft Azure. Object moved [online]. Copyright © Microsoft 2023 [cit. 01.05.2023]. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-the-cloud

(7) What is Microsoft Azure? - An Introduction to Azure. Intensive Project Based Training | DotNetTricks [online]. Copyright © 2023 Dot Net Tricks Innovation Pvt. Ltd. All rights Reserved. The course names and logos are the trademarks of their respective owners. [cit. 01.05.2023]. Dostupné z: https://www.dotnettricks.com/learn/azure/getting-started-with-microsoft-azure-platform

(8) What is AWS (Amazon Web Services) and How Does it Work?. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchaws/definition/Amazon-Web-Services

(9) The History of Google Cloud Platform | A Cloud Guru. World's #1 Digital Cloud Certification Course & Training Provider | A Cloud Guru [online]. Copyright © 2023 Serverless Heroes, Inc. [cit. 11.05.2023]. Dostupné z: https://acloudguru.com/blog/engineering/history-google-cloud-platform

(10) Google Cloud Platform: History Features & Pricing | Datamation. Technology News: Latest IT and Tech Industry News [online]. Copyright © 2023 TechnologyAdvice. All Rights

Reserved [cit. 11.05.2023]. Dostupné z: https://www.datamation.com/cloud/google-cloud-platform/

(11) Virtualization in Cloud Computing and Types – Geeks for Geeks. Dostupné z https://www.geeksforgeeks.org/virtualization-cloud-computing-types/

(12) What is Virtualization, and why is it important in the Cloud? [online]. Copyright © 2023 [cit. 11.05.2023]. Dostupné z: https://www.linkedin.com/pulse/what-virtualization-why-important-cloud-broadus-palmer

(13) Virtualization for Machine Learning [online]. Copyright © 2023 Towards Data Science. Dostupné z https://towardsdatascience.com/virtualization-for-machine-learning-da11b7a59070

(14) AWS Services - Testprep Training Tutorials. Test Prep Training | Practice Exam Questions |Practice Tests for Certifications [online]. Copyright © 2020 TestPrepTraining [cit. 01.05.2023]. Dostupné z: https://www.testpreptraining.com/tutorial/aws-sysops-administrator-associate/aws-services/

(15) What is Microsoft Azure? - An Introduction to Azure. Intensive Project Based Training | DotNetTricks [online]. Copyright © 2023 Dot Net Tricks Innovation Pvt. Ltd. All rights Reserved. The course names and logos are the trademarks of their respective owners. [cit. 01.05.2023]. Dostupné z: https://www.dotnettricks.com/learn/azure/getting-started-with-microsoft-azure-platform

(16) Virtualization for Machine Learning [online]. Copyright © 2021 Misbah Uddin. [cit. 01.05.2023] Dostupné z: https://towardsdatascience.com/virtualization-for-machine-learning-da11b7a59070

(17) What is Cloud Computing? Everything You Need to Know | TechTarget. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing

(18) Cloud Computing for Medium and Small Businesses | Microsoft Azure. Object moved [online]. Copyright © Microsoft 2023 [cit. 01.05.2023]. Dostupné z: https://azure.microsoft.com/en-us/solutions/medium-small-business-cloud-computing/#contact-us

(19) What is PaaS? Platform as a Service Definition and Guide. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchcloudcomputing/definition/Platform-as-a-Service-PaaS

(20) What is SaaS (Software as a Service)? Everything You Need to Know. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchcloudcomputing/definition/Software-as-a-Service

(21) What is SaaS (Software as a Service)? [online]. © Copyright 2023 Salesforce, Inc. All rights reserved. Dostupné z: https://www.salesforce.com/saas/

(22) Microsoft Azure. Microsoft Azure [online]. Dostupné z: https://portal.azure.com

(23) Co je Azure SQL? - Azure SQL | Microsoft Learn. [online]. Copyright © Microsoft 2023 [cit. 01.05.2023]. Dostupné z: https://learn.microsoft.com/cs-cz/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview?view=azuresql

(24) IaaS vs. PaaS vs. SaaS. [online]. Dostupné z: https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas

(25) Ellis, GETHYN. Microsoft Azure IaaS Essentials. USA: Packt Publishing, 2015. ISBN · 178217463X

(26) What is Security Information and Event Management (SIEM)? | IBM. [online]. [cit. 01.05.2023]. Dostupné z: https://www.ibm.com/topics/siem

(27) What Is SIEM and What Are the Benefits?. SIEM + Endpoint Visibility + XDR For SMB | Blumira [online]. Copyright © 2023 Blumira [cit. 08.05.2023]. Dostupné z: https://www.blumira.com/glossary/what-is-siem/

(28) What Is Security Information and Event Management (SIEM)? Definition, Architecture, Operational Process, and Best Practices - Spiceworks. Business and Industry News, Analysis and Expert Insights - Spiceworks [online]. Dostupné z: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/

(29) What is SIEM? | A Definition from TechTarget.com. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

(30) BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 3. aktualiz. a dopl. vyd. Praha: Grada, 2012. 323 s. ISBN 978-80-247-4307-3.

(31) GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2. přeprac. a aktualiz. vyd. Praha: Grada, 2009. 496 s. ISBN 978-80-247-2615-1.

(32) MOLNÁR, Zdeněk. Efektivnost informačních systémů. 2. rozš. vyd. Praha: Ikar, 2000. 178 s. ISBN 80-247-0087-5.

(33) SCHWALBE, Kathy. Řízení projektů v IT. Brno: Computer Press, 2007. 720 s. ISBN 978-80-251- 1526-8.

(34) Azure Sentinel general availability: A modern SIEM reimagined in the cloud | Azure Blog and Updates | Microsoft Azure. Object moved [online]. Copyright © Microsoft 2023 [cit. 08.05.2023]. Dostupné z: https://azure.microsoft.com/en-us/blog/azure-sentinel-general-availability-a-modern-siem-reimagined-in-the-cloud/

(35) Forrester Wave Gives Azure Sentinel A Leader Placement. Accelerating Your Transformation With A Full Spectrum Of Solutions - Infused Innovations [online]. Copyright © 2023 Infused Innovations [cit. 08.05.2023]. Dostupné z: https://www.infusedinnovations.com/blog/secure-intelligent-workplace/forrester-wave-gives-azure-sentinel-a-leader-placement

(36) Microsoft Sentinel Cloud Native SIEM Solution - Brief Overview. Continuous Intelligence with Real Time AI [online]. Dostupné z: https://www.xenonstack.com/blog/azure-sentinel-and-its-components

(37) Investigate incidents with Microsoft Sentinel | Microsoft Learn. [online]. Copyright © Microsoft 2023 [cit. 08.05.2023]. Dostupné z: https://learn.microsoft.com/en-us/azure/sentinel/investigate-cases

(38) BHARDWAJ, Navneet, Abhik BANERJEE a Agniswar ROY. Case Study of Azure and Azure Security Practices. In: Machine Learning Techniques and Analytics for Cloud Security. Hoboken, NJ, USA: John Wiley & Sons, 2021, s. 339-355. ISBN 1119762251.

(39) Categorizing Microsoft alerts across data sources in Azure Sentinel [online]. Copyright © Microsoft 2023 [cit. 08.05.2023]. Dostupné z: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/categorizing-microsoft-alerts-across-data-sources-in-azure/ba-p/1503367

(40) Making your Microsoft Sentinel Workbooks multi-tenant [online]. Copyright © Microsoft 2023 [cit. 08.05.2023]. Dostupné z: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/making-your-microsoft-sentinel-workbooks-multi-tenant-or-multi/ba-p/1402357

(41) Virtual Machines (VMs) for Linux and Windows | Microsoft Azure. Object moved [online]. Copyright © Microsoft 2023 [cit. 10.05.2023]. Dostupné z: https://azure.microsoft.com/en-us/products/virtual-machines

(42) How to add Microsoft Graph API permissions to a Managed Identity - AzToso.com. The cloud is not yet another datacenter - AzToso.com [online]. Copyright © 2023 Aleksandar Stefanov. Powered by [cit. 10.05.2023]. Dostupné z: https://aztoso.com/security/microsoft-graph-permissions-managed-identity/

(43) The Kusto Query Language – Azure Training Series. Azure Training Series [online]. Dostupné z: https://azure-training.com/azure-data-science/the-kusto-query-language/

(44) Grafana | Query, visualize, alerting observability platform. Grafana: The open observability platform | Grafana Labs [online]. Copyright © Grafana Labs [cit. 10.05.2023]. Dostupné z: https://grafana.com/grafana/

(45) SALITURO, Eric. Learn Grafana 7.0: A beginner's guide to getting well versed in analytics, interactive dashboards, and monitoring. USA: Packt Publishing Ltd, 2020. ISBN 1838828311

(46) Alerting | Grafana documentation. Grafana: The open observability platform | Grafana Labs [online]. Copyright © Grafana Labs [cit. 10.05.2023]. Dostupné z: https://grafana.com/docs/grafana/latest/alerting/

(47) Annotate visualizations | Grafana documentation. Grafana: The open observability platform | Grafana Labs [online]. Copyright © Grafana Labs [cit. 10.05.2023]. Dostupné z: https://grafana.com/docs/grafana/latest/dashboards/build-dashboards/annotate-visualizations/

(48) Team management | Grafana documentation. Grafana: The open observability platform | Grafana Labs [online]. Copyright © Grafana Labs [cit. 10.05.2023]. Dostupné z: https://grafana.com/docs/grafana/latest/administration/team-management/

(49) Cyber Resilience. PwC: Building trust for today and tomorrow [online]. Copyright © [cit. 10.05.2023]. Dostupné z: https://www.pwc.com/cz/cs/sluzby/cyberandprivacy/cyber-resilience.html

(50) Národní úřad pro kybernetickou a informační bezpečnost - Upozornění na zvýšené riziko kyberšpionáží či ransomwarových útoků proti České republice. Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka [online]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1796-upozorneni-na-zvysene-riziko-kyberspionazi-ci-ransomwarovych-utoku-proti-ceske-republice/

SEZNAM POUŽITÝCH ZKRATEK

SIEM – System information event management

SIM – System information management

VM – Virtual machine

SOC – Security operation system

PaaS – Platform as a service

SaaS – Software as a service

IAAS – Infrastructure as a services

ERP – Enterprise resource planning

CRM – Customer relationship management

CEF – Common event format

API – Application interface

KQL – Kusto query language

AMI - Azure managed identities

RBAC - Role-based access control

SEZNAM OBRÁZKŮ

SEZNAM TABULEK