Bezpečnostní monitoring a automatizovaný návrh nasazení SIEM v informačních systémech

Jan Fojtík

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jan Fojtik**
Osobní číslo:	**A21699**
Studijní program:	**B0613A140020 Softwarové inženýrství**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnostní monitoring a automatizovaný návrh nasazení SIEM v informačních systémech**
Téma práce anglicky:	**Security Monitoring and Automated Design of SIEM Deployment in Information System**

Zásady pro vypracování

1. Proveďte literární rešerši spojenou s tématem práce.
2. Navrhněte vhodný postup pro implementaci konkrétního nástroje SIEM a vytvoření korelačních pravidel pro bezpečnostní monitoring uživatelů.
3. Imlementujte ve vhodném prostředí a demonstrujte automatizaci jednotlivé části systému.
4. Ověřte funkčnost nástroje.
5. Vyhodnoťte projekt a jeho skutečné přínosy.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. IBM, 2022. *IBM QRadar documentation*. Online. IBM. Dostupné z: https://www.ibm.com/docs/en/qsip/7.5?topic=SS42VS_7.5/com.ibm.qradar.doc/c_pdf_launch.htm. [cit. 2023-11-13].
2. MICROSOFT, 2023. *What is SIEM*. Online. Https://www.microsoft.com. Dostupné z: https://www.microsoft.com/en/security/business/security-101/what-is-siem. [cit. 2023-12-07].
3. ROCHFORD, Oliver a KAVANAGH, Kelly M. Critical Capabilities for Security Information and Event Management. Online. S. 1-16. Dostupné z: https://solutionsreview.com/dl/Gartner_Critical_Capabilities_SIEM_2015_LRDL2.pdf. [cit. 2023-11-13].
4. *The Anatomy of a Modern SIEM*, 2023. Online. Securonix. Dostupné z: https://www.securonix.com/blog/the-anatomy-of-a-modern-siem/. [cit. 2023-12-07].
5. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů, 2014. In: *181/2014*. Dostupné z: https://www.govcert.cz/download/legislativa/2020/2020-02-01_novelizace_zneni_zakona_181_2014_final.pdf. [cit. 2023-12-07].

Vedoucí bakalářské práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **5. listopadu 2023**
Termín odevzdání bakalářské práce: **13. května 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.
- Že při tvorbě této práce jsem použil/a nástroj generativního modelu AI [OpenAI GPT-4-turbo-preview; https://platform.openai.com/] za účelem stylistiky. Po použití tohoto nástroje jsem provedl/a kontrolu obsahu a přebírám za něj plnou zodpovědnost. Při používání nástrojů AI je důležité také rozlišovat, zda jejich využití ovlivnilo samotný obsah předkládané práce

Ve Zlíně, dne …….

podpis studenta

ABSTRAKT

Tato práce se zabývá implementací systému pro sběr a analýzu protokolů v oblasti kybernetické bezpečnosti se zaměřením na detekci neobvyklých vzorců chování uživatelů. Začíná přehledem klíčových konceptů kybernetické bezpečnosti. Jádro studie podrobně popisuje nasazení systému IBM QRadar s důrazem na automatizaci jeho jednotlivých segmentů. Práce propojuje teoretické poznatky s praktickým využitím při zvyšování podnikové bezpečnosti.

Klíčová slova: Kybernetická bezpečnost, SIEM, detekce událostí, sběr logů, korelační pravidla

ABSTRACT

This thesis explores the implementation of a system for log collection and analysis in cybersecurity, focusing on detecting unusual user behavior patterns. It begins with an overview of key cybersecurity concepts, followed by a comparative analysis of technical tools for event detection in information systems. The core of the study details the deployment of the IBM QRadar system, emphasizing the automation of its various segments. This work bridges theoretical knowledge with practical application in enhancing corporate security.

Keywords: Cybersecurity, SIEM, Event Detection, Log Collection, Correlation rules.

Rád bych poděkoval touto cestou vedoucímu práce prof. Mgr. Roman Jašek. Ph.D., DBA za cenné rady a čas, který mi při vypracování bakalářské práce věnoval a děkuji kolegům z ARICOMY za věcné poznatky. Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V současnosti, kdy se informační technologie stávají stále více integrovanou součástí každodenního života a podnikání, roste také význam kybernetické bezpečnosti a s ním i důležitost zabezpečení firemních dat. S nárustem a frekvencí sofistikovaných kybernetických útoků se stává ochrana informačních systémů před potenciálními hrozbami jednou z nejdůležitějších priorit organizací, pro které data představují firemní zlato. Pro společnosti a organizace různých velikosti je zabezpečení dat základní myšlenkou a měla by hrát důležitou roli při stavbě architektury IT prostředí.

Tento růst kybernetické bezpečnosti se odráží i v kontinuálním zvyšování nároku na monitorovací systémy a nástroje pro detekci hrozeb. V této souvislosti se objevuje ověřený koncept Security Information and Event Management (SIEM), který představuje komplexní přístup ke správě bezpečnostních informací a událostí. SIEM systémy umožňují organizacím sledovat, analyzovat, spravovat a v neposlední řadě taky reagovat na bezpečnostní hrozby v reálném čase, což je zásadní pro ochranu citlivých dat.

Přestože je nasazení SIEM řešení klíčové pro moderní bezpečnostní strategie, mnoho organizací čelí výzvám spojeným s jejich efektivním využití. Tyto výzvy zahrnují složité konfigurace, správu a automatizaci, ale především integraci s existujícími bezpečnostními systémy a zařízeními, které systém efektivně filtruje a analyzuje velké množství dat, aby identifikoval skutečné hrozby. Jelikož kybernetické hrozby neustále evolvují, tak kromě technických aspektů SIEM vyžaduje rozvoj lidských zdrojů, včetně školení a rozvoje dovednosti bezpečnostních týmu, které budou s těmito systémy pracovat. Tento proces nejenže zahrnuje technické upgrady, ale i neustálé vzdělávání a informovanost zaměstnanců o nových hrozbách a nejlepších praktikách.

Hlavním cílem této práce je poskytnout fundamentální informace a komplexní postup pro implementaci SIEM nástroje a vytvoření korelačních pravidel zaměřených na bezpečnostní monitorování uživatelské aktivity. Zásadním krokem k dosažení tohoto cíle je zasvětit čtenáře do informační bezpečnosti a představené odpovídajících technologických řešení.

Mým hlavním důvodem pro výběr tohoto tématu je zkušenost získána během mého působení ve společnosti ARICOMY, kde jsem se podílel na implementaci SIEM řešení pro společnosti a státní orgány. V praktické části jsou se svolením manažera Ing. Leoše Stránského použity anonymizované a upravené snímky z IBM QRadar SIEM za jejíchž správu jsem zodpovědný. Práce má za cil reflektovat mé zkušenosti a nabídnout praktické návody a postupy

pro efektivní nasazení SIEM řešení, což může být prospěšné pro osoby zodpovědné za informační bezpečnosti.

I. TEORETICKÁ ČÁST

1 ÚVOD DO INFORMAČNÍ BEZPEČNOSTI

V dnešní digitálně propojené době je informační bezpečnost nezbytná pro ochranu důležitých dat a udržení důvěry v technologických systémech. Tato kapitola slouží jako úvod do základních principů informační bezpečnosti, jejího významu a výzev, se kterými se potýkáme v současné době. Ve světě, kde se stále více osobních, firemních a státních dat přesouvá do digitálního prostoru, význam bezpečnosti informací výrazně roste. Zajištění ochrany těchto dat před neoprávněným přístupem, únikem informací, zneužitím nebo poškozením je klíčové nejen pro jednotlivé uživatele, ale především pro organizace a instituce, pro které mohou být důsledky bezpečnostních incidentů zničující.

1.1 Základní pojmy a principy informační bezpečnosti

Informační bezpečnost, často označovaná jako InfoSec, se zabývá ochranou informací ve všech jejích formách, ať už digitálních nebo analogových, proti nepovolenému přístupu, zneužití, zveřejnění, narušení, změně, inspekci, záznamu nebo zničení. InfoSec je zásadní pro zachování důvěrnosti, integrity a dostupnosti informací. Důvěrnost znamená, že informace jsou dostupné jen osobám, které mají k přístupu oprávnění; integrita znamená zachování přesnosti a úplnosti informací; a dostupnost zajišťuje, že informace jsou přístupné oprávněným uživatelům, když jsou potřeba [1]

Na druhé straně, kybernetická bezpečnost, většinou označováná jako IT bezpečnost, která se specificky soustředí na ochranu digitálních informační a zajišťuje bezpečnost IT infrastruktury před kybernetickými hrozbami, jako jsou malware, ransomware, phishing a další útoky. Zahrnuje technologie, procesy a mechanismy, které jsou navrhnuty k bezpečnosti systému, dat a neoprávněného přístupu. [2]

1.2 Základní prvky ochrany informací

Základními pilíři informační bezpečnosti, často označovanými jako 'CIA triáda', jsou integrita (Integrity), důvěrnost (Confidentiality) a dostupnost (Availability). Tyto tři prvky tvoří základní rámec, na kterém stojí všechny bezpečnostní politiky a postupy.

Integrita informací znamená, že data zůstávají přesná, uplná a nezměněná během celého životního cyklu – od vytvoření, skrz uložení a přenos, až po zpracování. Jakákoli neautorizovaná změna dat, ať už úmyslná nebo náhodná, může vést k finančním ztrátám, poškození reputace či jinému negativnímu dopadu.[3]

1.2.1 Způsoby ochrany integrity

- Kontrolní součty a hashovací funkce se používají k ověření, že data nebyla změněna od okamžiku svého vytvoření nebo posledního ověření.
- Digitální podpisy poskytují mechanismus pro ověření původu a integrity dokumentů nebo zpráv.
- Správa verzí a auditní záznamy umožňují sledovat historii změn a identifikovat neoprávněné nebo nežádoucí změny.

Důvěrnost se týká ochrany informací před neoprávněným přístupem nebo zveřejněním. Zajištění důvěrnosti zahrnuje aplikaci kontrol, jako jsou šifrování, autentizace a řízení přístupu, aby byly informace přístupné pouze těm, kteří mají k nim mít přístup.

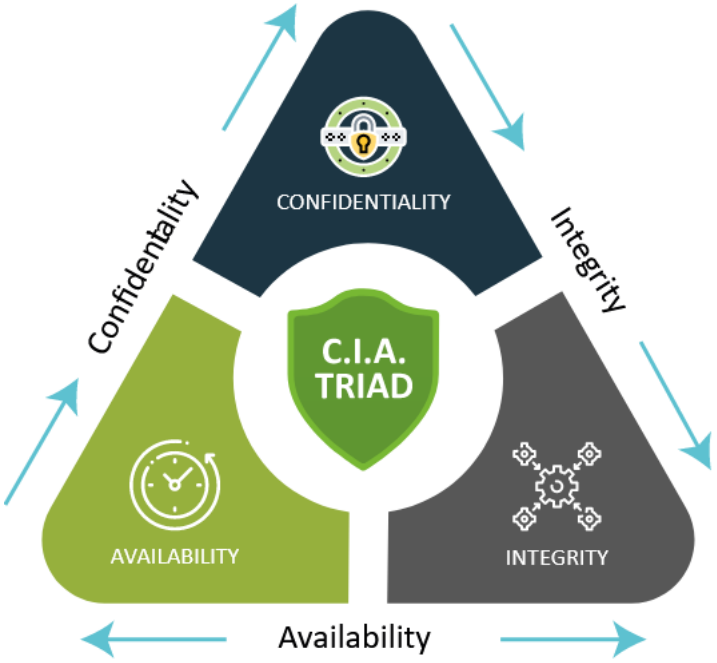
1.2.2 Způsoby ochrany důvěrnosti

- Šifrování chrání data před neoprávněným přístupem tím, že je převádí do podoby, kterou lze dešifrovat pouze s odpovídajícím klíčem, např. asynchronní klíče.
- Autentizační mechanismy, jako jsou hesla, biometrie nebo více faktorová autentizace zajištují, že přístup mají pouze ověřené osoby
- Řízení přístupu a politika oprávnění omezují přístupy k informacím pouze na nezbytnou skupinu potřebnou pro splnění pracovních úkolu

Dostupnost se zaměřuje na zajištění, že informace a systémy jsou dostupné oprávněným uživatelům, kdykoli jsou potřeba. To zahrnuje ochranu proti DoS (Denial of Service) útokům, zajištění redundance systémů a implementaci efektivního plánování obnovy po havárii.

1.2.3 Způsoby ochrany dostupnosti

- Redundance systému a vyvažování zátěže zajištují, že v případě selhání jednoho systému převezme jiný systém jeho funkci (High Availability).
- Plány obnovy po havárii a zálohování dat jsou esenciální pro rychlou obnovu systému a dat po výpadku či útoku.
- Ochrana proti DoS útokům zahrnuje monitorování síťového provozu a filtraci, aby se zabránilo nebo minimalizovaly dopady jednotlivých útoků, které jsou zaměřeny na přerušení služeb. [4]



Obrázek 1 – Klíčové komponenty informační bezpečnosti

Výzvy v oblasti informační bezpečnosti neustále rostou s rozvojem nových technologií a narůstajícím počtem kybernetických hrozeb. Kybernetické útoky, jako jsou malware, ransomware, phishing a další se stávají sofistikovanějšími a cílenějšími. V důsledku toho se organizace musí neustále adaptovat a vylepšovat své bezpečnostní strategie a protokoly, aby se vyrovnaly s těmito hrozbami. V tomto kontextu hrají SIEM systémy klíčovou roli. Tyto systémy umožňují organizacím shromažďovat, analyzovat a reagovat na logy a analyzovat bezpečnostní události z různých zdrojů v reálném čase, což je nezbytné pro rychlou identifikaci a řešení bezpečnostních incidentů. Efektivní implementace a správa SIEM systému je proto zásadní pro moderní strategie kybernetické bezpečnosti. V následujících kapitolách se podrobněji zaměříme na různorodost jednotlivých kybernetických útoků a jejích charakteristiku.

2 BEZPEČNOST V KYBERPROSTORU

Bezpečnost v kyberprostoru se stává zásadní součásti ochrany informací v digitálním věku. Kyberprostor, představuje virtuální prostředí, v němž lidé a technologie interagují se systémy a sítěmi. Tato interakce přestavuje jisté pohodlní a inovace, ale přináší také různá rizika a potřebné opatření před nežádoucími aktivitami. Rizika plynoucí z kybernetických hrozeb se neustále vyvíjí. Kybernetická bezpečnost zahrnuje širokou škálu postupů a technologií určených k ochraně digitálních systémů, sítí a dat před neoprávněným přístupem, útoky a poškozením. Patří sem ochrana osobních údajů, duševního vlastnictví, počítačových systémů a kritické informační infrastruktury. S rostoucím využíváním cloudových služeb, mobilních zařízení a internetu věcí (IoT) roste i složitost kybernetické bezpečnosti. Účinná kybernetická bezpečnost vyžaduje nejen technologická řešení, ale také silnou bezpečnostní kulturu, pravidelné školení zaměstnanců a spolupráci na všech úrovních organizace. Jedná se o kontinuální proces, který zahrnuje prevenci, detekci, reakci a obnovu po bezpečnostních incidentech.

2.1.1 Stav kybernetické bezpečnosti ve světě

Nejnovější studie kybernetické bezpečnosti ukazuje, že mnoho organizací využívá kybernetickou bezpečnost jako klíčový diferenciátor pro dosažení lepších obchodních výsledků. Ty společnosti, které efektivně sladily své programy kybernetické bezpečnosti s obchodními cíli a inovačními strategiemi, mají o 18 % vyšší pravděpodobnost zvýšení příjmů, většího podílu na trhu a větší spokojenosti zákazníků. Integrace kybernetické bezpečnosti do obchodních operací může zahrnovat různé aspekty, jako je ochrana značky, ochrana před finanční ztrátou způsobená útoky a vytváření důvěry u zákazníka tím, že se prezentují jako důvěryhodná a zabezpečená firma. Tato důvěra je stále více ceněna, obzvlášť ve světle nedávných incidentů týkajících se úniků dat a porušení soukromí.

2.1.2 Statistiky a nejčastější typy kybernetických hrozeb

Analýza a výroční zpráva o kybernetické bezpečnosti ve světě poukázala na čtyři nejčastější typy kybernetických hrozeb – Cryptomining, Phising, Trojan a Ransomware a další. Lidský faktor je příčinou přibližně 74 % všech porušení kybernetické bezpečnosti. Průměrné náklady na nápravu v roce 2023 činily 4,45 milionu dolarů, což je největší průměr v historii. Průměrný životní cyklus narušení bezpečnosti je 277 dní od identifikace po zvládnutí. Pravděpodobnost, že bude v USA odhalen a stíhán subjekt páchající kybernetickou trestnou

činnost se odhaduje na přibližně 0,05 %. Kybernetická únava neboli apatie k proaktivní obraně proti kybernetickým útokům postihuje až 42% společnosti. Od začátku rusko-ukrajinské války v roce 2022 zaznamenalo 97 % organizací nárust kybernetických hrozeb. LinkedIn zažil v roce 2021 rozsáhlé porušení bezpečnosti, při kterém byly odhaleny osobní informace 700 milionů uživatelů, tedy přibližně 93% všech členů LinkedIn. Jediné heslo umožnilo hackerům proniknout do Colonial Pipeline Company v roce 2021 s ransomwarovým útokem, který způsobil nedostatek paliva po celých spojených státech. Společnost JBS, zpracovatel masa se stal obětí ransomwarového útoku, který zastavil provoz závodu na zpracování hovězího a drůbežího masa na čtyřech kontinentech. [5]

V následujících řádcích si představíme jednotlivé typy kybernetických útoků.

2.1.3 Útoky pomocí sociálního inženýrství

Tato metoda se soustředí na techniku, při které dochází k manipulaci jednotlivců za účelem získání citlivých informací nebo přístupu k datům často s cílem finančního zisku. Většinou to zahrnuje podvodná technika jménem phising, která je používána k získání citlivých údajů (hesla, údaje z kreditních karet) od obětí útoků.

2.1.4 Phishing

Jedná se o pokus krádeže citlivých informací, obvykle v podobě uživatelských jmen, čísel kreditních karet, hesel, informací o bankovních účtech nebo jiných citlivých údajích s cílem prodat nebo využít ukradené informace. Útočník se označuje za důvěryhodný zdroj a lákavou žádosti láka oběť, aby ji oklamal, podobně jako rybář používá návnadu k chycení ryby. Mezi nejčastější formy, při kterých útočnici rozesílají e-maily, které vypadají, jako by pocházely z legitimních společností a institucí, jako jsou banky, sociální sítě anebo e-commerce platformy. E-mail obvykle obsahuje odkaz vedoucí na falešnou webovou stránku, kde se obětí žádá o zadaní osobních údajů. [6]

2.1.5 SQL Injection

Je sofistikovaná a nebezpečná technika, která zneužívá zranitelnosti mezi webovou aplikací a její databázi. Útočník využívá neověřené vstupní hodnoty na webové stránce, například ve formulářích pro přihlášení, vyhledávací políčka nebo URL parametrech. Útočník využívá neověřené nebo nedostatečně filtrované vstupní hodnoty na webové stránce. Filtrovaní vstupních hodnot je proces, při kterém dochází k tomu, že data zadaná do webové aplikace (například přes formuláře webových stránek) jsou před jejich dalším zpracováním nebo

uložením do databáze kontrolována a upravená tak, aby byla odstraněna nebo neutralizovaná potenciálně škodlivá data. Útočník zadá SQL škodlivý kód do vstupního pole na webové stránce, který mu umožní manipulovat data v databázi, získat neoprávněné přístupy do různých oblastí, získat nebo mazat citlivé informace. [7]

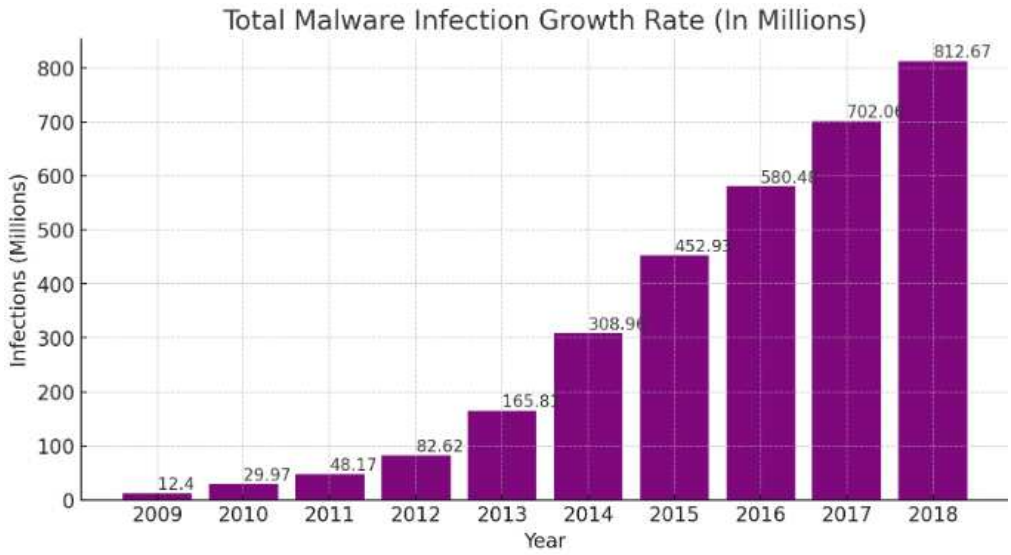
2.1.6 Cross-Site-Scripting (XSS)

Je typ útoku, při kterém útočníci vkládají škodlivý script do obsahu webových stránek, které jsou za normálních okolností důvěryhodné a legitimní. Script je poté spouštěn v prohlížeči v momentě, kdy oběť nic netuší při návštěvě ovlivněné webovou stránku. Tyto útoky jsou obzvláště nebezpečné, protože mohou vést k odcizení cookies, session tokenů nebo jiných citlivých informací uložených v prohlížeči oběti, což útočníkům umožňuje obcházet kontrolní mechanismy autentizace a získat neautorizovaný přístup k uživatelským účtům. XSS může nabývat několika forem, z nichž každá představuje jinou specifickou hrozbu pro bezpečnost webových stránek a uživatelů. První typ je odrážený (Reflected), který se odehrává, když útočník láka oběť na škodlivých odkaz, jenž po kliknutí odesílá škodlivý script na zranitelnou webovou stránku. Tato stránka následně script zpracuje a vrátí ho ve formě odpovědi zpět prohlížeči oběti, kde je script aktivován. Druhý typ je uložený (Stored) XSS a ten spočívá v trvalém uložením škodlivého scriptu na serveru, často v databázích, fórech nebo komentářích, odkud je při návštěvě ovlivněné stránky script spuštěn v prohlížeči uživatele. DOM – Based XSS představuje posledních typ kybernetického útoku, při kterém útočník vkládá nebo upravuje JavaScript kód na webové stránce prostřednictvím manipulace DOM struktury stránky, aniž by bylo potřeba odesílat škodlivý kód na server. Tento útok probíhá na straně klienta, kdy škodlivý script je aktivován v prohlížeči uživatele. Nejběžnější zdrojem je adresa URL, na kterou se obvykle přistupuje pomocí objektu Windows location. [8]

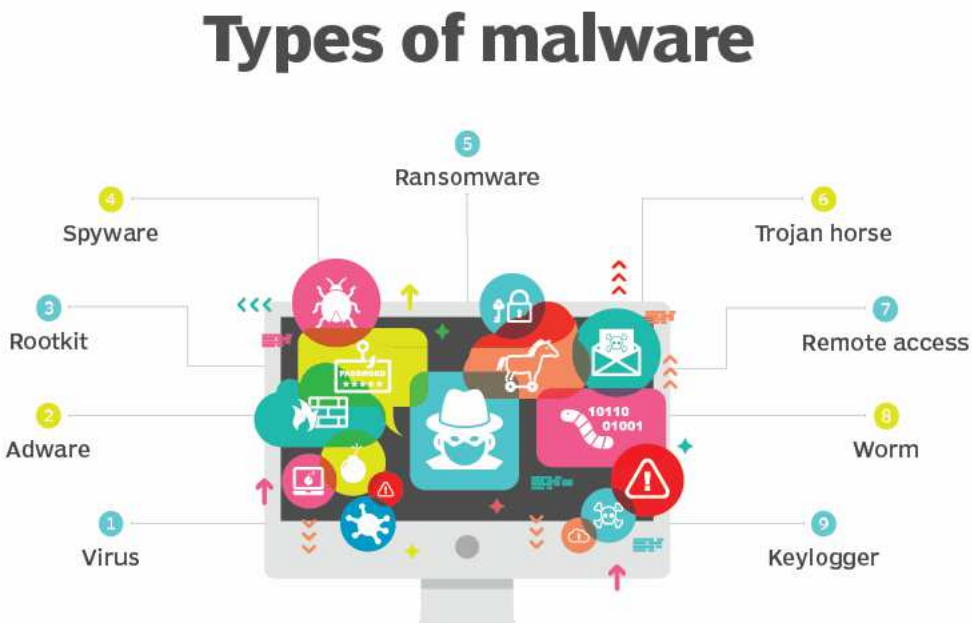
2.1.7 Malware

Je označení pro škodlivý software (složení z anglických slov malicious software), který umožní pachateli poškodit anebo narušit funkcionalitu jednoho nebo více po-čítačů, serverů či počítačových sítí. Mezi různé formy škodlivého softwaru patří ransomware, spyware, trojské koně, viry, červy a DDoS útoky (kde jsou kompromitovány jiné zařízení pro provedení útoků). Ačkoliv malware většinou nemůže způsobit fyzické poškození jednotlivých komponentů počítače, je schopen odcizit, zašifrovat anebo odstranit data, může taky změnit základní funkce PC anebo špehovat Vaši aktivitu bez Vašeho vědomí a svolení. Je schopen

také spouštět jisté operace na pozadí pomocí příkazového řádku a tím se stát obtížně detekovaným a neviditelným. [9]



Obrázek 2 – Tempo růstu útoku pomocí Malware



Obrázek 3 – Druhy Malware

2.1.8 Spyware

Je druh škodlivého softwaru určen pro špehování. Do zařízení se instaluje neoprávněně bez vědomí uživatelů a působí jako „špión“. Tajně shromažďuje data a poté je posílá

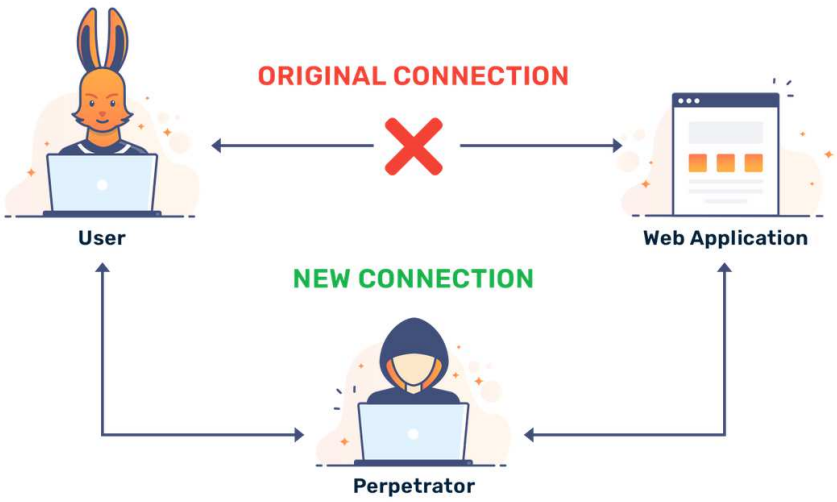
kyberzločinci, který tyto informace využije ve svůj prospěch, například pro marketingové účely anebo tyto informace dále využije k dalšímu kybernetickému útoku. Jeho nenápadná povaha a schopnost se skrýt v legitimních aplikacích dělá z něj velice nebezpečnou hrozbu.[10]

2.1.9 Ransomware

Je forma malware, který zakóduje data na PC nebo zablokuje uživatelům přístup k jejich souborům, čímž je v podstatě stávají „rukojmí“ pro útočníka. Pro odemčení či dešifrování těchto dat obvykle vyžaduje útočník výkupné a chce na dané akci vydělat. V období pandemie COVID – 19 došlo k výraznému nárustu těchto kybernetických incidentů.[11]

2.1.10 Man-in-the-middle

Útok tohoto typu vyžaduje, aby se útočník postavil mezi dvě komunikující strany a předával jim zprávy, zatímco strany věří, že spolu komunikují napřímo a bezpečně. Útočník pak může sledovat a případně měnit obsah zpráv. Tento koncept se neomezuje pouze na počítačovou bezpečnost, podobné útoky existovaly ve fyzickém světě dávno předtím, než byly vynaleznuty počítače.[12]



Obrázek 3 – Man in the middle

2.1.11 DoS a DDoS

Útok DoS (Denial-of-service) zaplaví server provozem a z nedostupní web nebo server. Distribuovaný útok typu DDoS (Denial-of-service) je útok DoS, který využívá více počítačů

nebo strojů k zaplavení cíleného zdroje. Oba typy útoků přetěžují server nebo webovou aplikací s cílem přerušit služby. Protože je server zahlcen větším počtem paketů TCP/UDP (Transmission Control Protocol / User Datagram Protocol), než dokáže zpracovat, může dojít k jeho zhroucení, poškození dat a nesprávnému přesměrování či dokonce vyčerpání zdrojů, které mohou paralyzovat systém.[13]

2.2 Technologie SIEM

IBM Security QRadar SIEM (dále též QRadar SIEM) automaticky sbírá, archivuje a analyzuje data zahrnující logy bezpečnostní povahy napříč celou IT i OT infrastrukturou. Systém je schopen přijímat protokoly síťových toků (Netflow, sFlow, IPFIX, JFlow apod.). Logovací události jsou přijímány z různých oblastí infrastruktury od operačních systémů, přes síťová zařízení, middleware až po aplikační logy, SCADA systémy nebo vyspělá PLC. Zprávy různých formátů jsou po příjmu tzv. normalizovány do jednotné podoby. V normalizovaném formátu dochází k dalšímu zpracování událostí v korelačním systému SIEM. Za pomoci definovaných korelačních pravidel v systému jsou data automaticky vyhodnocována téměř v reálném čase. V případě podezřelého nálezu může být výstupem tzv. Offense, tedy bezpečnostní událost (tiket) k prověření lidským operátorem nebo nástroji umělé inteligence. Uživatelé mohou, v souladu s nastavenými oprávněními, logovací události a záznamy o síťových tocích v systému filtrovat a efektivně vyhledávat požadované informace. I za pomocí automaticky generovaných reportů mají pracovníci IT/OT oddělení i bezpečnostní pracovníci aktuální přehled o potenciálních i skutečných anomáliích, hrozbách a bezpečnostních událostech monitorovaného prostředí. [14]

2.2.1 Klíčové vlastnosti systému QRadar SIEM

Klíčovou vlastností QRadaru SIEM je jeho využitelnost a efektivita. Systém lze tvořit v distribuované vícevrstvé architektuře, která reflektuje geografické, bezpečnostní a výpočetní požadavky. QRadar dokáže zpracovávat od stovek událostí za sekundu až po 40 000 nebo více událostí za sekundu (EPS) na jednom zařízení. QRadar může zpracovávat od 15 tisíc síťových toků za minutu až po více než jeden milion síťových toků za minutu (FPM). QRadar umožňuje získávat data ze stovek až několika tisíců unikátních zdrojů logů. Interní úložiště má kapacitu od několika TB až po desítky TB efektivní kapacity v uspořádání RAID 5, 6 nebo 10. Jiná uspořádání RAID nejsou výrobcem doporučena. Pokud jde o schéma RAID, výrobce doporučuje RAID10 a RAID5 pro zařízení s kapacitou úložiště do 10TB,

nad tuto kapacitu doporučuje RAID6. K dispozici je clusterova HA konfigurace, která zajišťuje vysokou dostupnost a nepřetržitou funkcí na úrovní kolektorů, procesorů a centrálních konzolí.[14]

2.2.2 Přednosti systému QRadar SIEM

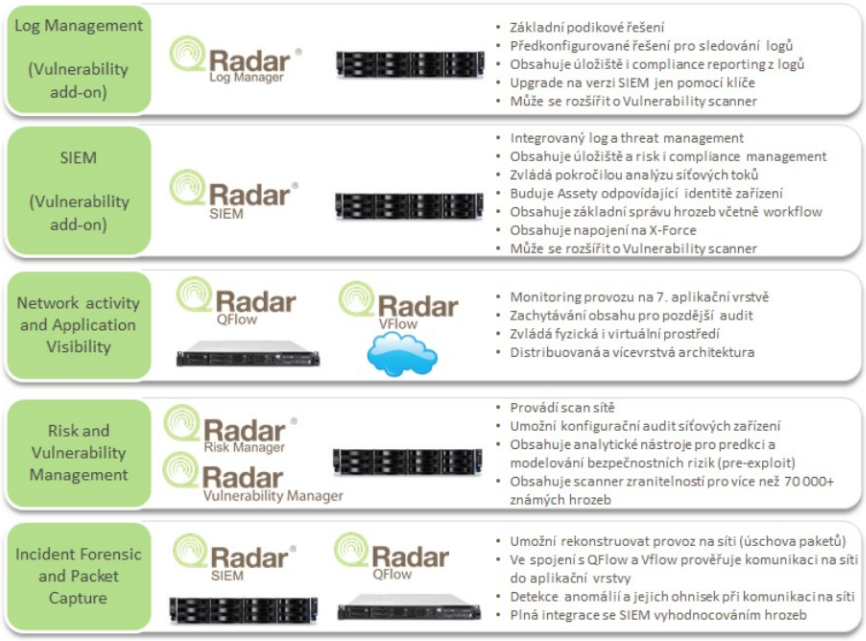
Je nezbytné, aby organizace disponovaly nástroji pro efektivní vyhodnocování zranitelností v reálném čase. To zahrnuje schopnost generovat sady reportů, které podávají přesný obraz o stávající bezpečnostní situaci, ale také plně odpovídají regulačním nařízením a standardům. Klíčovým aspektem v tomto procesu je použití interaktivních grafických vizualizací, které umožnují analýzu provozu a identifikaci zranitelnosti. Systémy pro správu bezpečnostních informací a události nabízí velké množství korelačních funkcí, přímé napojení na zpracování protokolů Netflow a IPFix, jakož i přímé napojení na aktivní prvky sítě, včetně firewallu a routerů. Tyto systémy jsou rovněž připojeny k logům standardních operačních systému a databází, což umožňuje komplexní přehled o systému. Dalším klíčem k úspěchu je plně škálovatelná infrastruktura pro distribuované nasazení a plná nezávislost funkcí pro jednotlivé komponenty, včetně self-monitoringu. Napojení na službu X-Force Exchange zajištuje kompletní přehled o celosvětových hrozbách a kompletní analýzu dané IP adresy, která poskytuje přehled o jejích atributech.

2.2.3 High – Availability

V případě selhání hardwaru nebo sítě může QRadar pokračovat ve shromažďovaní, ukládání a zpracování dat o událostech a tocích pomocí zařízení s vysokou dostupností (HA). Aby QRadar umožnil HA, propojí primárního hostitele HA se sekundárním hostitelem HA a vytvoří se cluster HA. Pokud dojde k selhání primárního hostitele, sekundarní hostitel převezme řízení a má stejným přístup k datům jako primární a pomocí synchronizace dat se dostane do stejného stavu. Je možné použít HA na hardwaru nebo na virtuálním zařízením, ale HA není podporován v cloudovým prostředí.[19]

2.3 ROZSAH TECHNOLOGIE IBM SECURITY QRADAR

IBM poskytuje v rámci svého portfolia QRadaru několik typu software. SW lze provozovat na straně zákazníka, a to ve formě virtuálního nebo fyzického serveru. QRadar lze provozovat buď jako rozšíření v rámci stávajícího HW (fyzický či virtuální) nebo samostatně na novém HW (fyzickém či virtuálním) serveru. Moduly QRadaru lze alternativně provozovat v Cloud prostředí IBM. Základní řadu typu uvádí následující obrázek:



Obrázek 4 – Souhrn softwarových modulů IBM QRadar

2.3.1 Modul QRadar Log Manager

Modul QRadar Log Manager poskytuje komplexní řešení pro centralizované spravování logů, zahrnující sběr dat z rozmanitých síťových a bezpečnostních zařízení jako jsou routery, switche, firewally, VPN, systémy pro detekci a prevenci průniku (IPS/IDS), antivirové programy, koncová zařízení, servery, databáze, emailové a webové aplikace, stejně jako proprietární aplikace klientů. QRadar Log Manager normalizuje a agreguje všechny zaznamenané události. Speciálně upravený nástroj pro aplikaci pravidel vyhodnocuje každou přijatou událost v reálném čase, přiřazuje ji hodnotící atributy podle závažnosti, důvěryhodnosti a relevance a aktivuje odpovídající reakci, ať už prostřednictvím emailové notifikace, výstrahy na dashboardu, nebo zařazením události do sady podobných aktivit pro budoucí podrobnější analýzu nebo kontinuální vylepšování vyhodnocovacího procesu. S licenčním klíčem je možné expandovat jednotné nebo distribuované instalace, provádět upgrade EPS, přecházet na verzi SIEM, nebo aktivovat funkce skeneru zranitelností.[15]

2.3.2 IBM QRadar User Behavior Analytics

IBM QRadar User Behavior Analytics pro analýzu uživatelského chování a detekci anomálií a hrozeb s vizualizací dat v dedikované záložce systém.[15]

2.3.3 QRadar Network Insights

Jedná se o posílení schopnosti QRadar v oblasti analýzy dat v síťové komunikaci. Jde především o hlubší analýzu datových rámců (paketů) pohybujících se v síti. QNI sonda je dedikovaný fyzický nebo virtuální server, do kterého je zrcadlen síťový provoz (TAP/SPAN mirror port). Obsah paketů je předáván do systému IBM Security QRadar SIEM, kde je možné data podrobit korelaci.[15]

2.3.4 Modul Incident Forensic and Packet Capture

Nástroj umožňující zachytávání a analýzu síťových paketů v reálném čase. Díky speciálně vyvinutým síťovým kartám, které jsou nezbytné pro zachycení dat přímo ze síťového provozu, je nutné tento modul pořídit jako hardwarové zařízení přímo od společnosti IBM. Uložená síťová data pak modul využívá pro detailní forenzní vyšetřování a analýzu bezpečnostních incidentů, což usnadňuje identifikaci a návrh opatření pro odstranění zjištěných bezpečnostních rizik. Modul Incident Forensic lze instalovat na libovolný kompatibilní server nebo vytvořit jeho virtuální instanci. Mezi jednotlivými systémy pro zachytávání paketů a systémem Incident Forensic je doporučené maximální poměrové rozložení 5:1, což zajišťuje efektivní zpracování a analýzu dat bez přetížení systému.[15]

2.3.5 QRadar Vulnerability and Risk Manager

Jednotlivá instalace je určena pro propojení systému QRadar s vybranými externími službami pro skenování zranitelností, jako jsou Nessus, Qualys a Rapid7. Tato licence umožňuje systému začlenit informace o zranitelnostech do hodnocení různých bezpečnostních scénářů díky předem připraveným konektorům k těmto skenerům.[15]

2.3.6 Modul IBM QRadar Advisor with Watson a přidružený Watson Starter Pack

Poskytuje možnost sdílet data analyzovaná v rámci IBM Security QRadar SIEM s cloudovou službou Watson for Cyber Security. Využitím pokročilé kognitivní analýzy Watson dokáže identifikovat souvislosti mezi bezpečnostními informacemi, čímž zkracuje dobu potřebnou k vyšetření narušení bezpečnosti. Výsledky jsou prezentovány ve vizuální formě s doprovodným textovým vysvětlením a doporučeními. Tento modul je nabízen jako služba od IBM a jeho licencování se odvíjí od počtu zpracovaných událostí za sekundu (EPS) v systému QRadar. Implementace služby vyžaduje, aby systém QRadar prošel validací skrze plugin z X-Force App Exchange a byl certifikován pro integraci s Watsonem. Poté je možné specifické bezpečnostní incidenty předat k analýze Watsonovi.[15]

2.3.7 IBM Security QRadar SOAR (Resilient)

Představuje specializovanou platformu pro orchestraci bezpečnostních odpovědí, automatizaci a reakci, která umožňuje organizacím efektivně shromažďovat informace o bezpečnostních hrozbách a reagovat na incidenty podle předem stanovených procedur (tzv. playbooks) s minimálním nebo bez lidského zásahu, v souladu s platnými právními a regulačními standardy. Hlavním cílem této platformy je zvýšení efektivity operací v oblasti fyzické i kybernetické bezpečnosti.[15]

3 BEZPEČNOSTNÍ MONITORING UŽIVATELŮ A JEHO SÍLA V KYBERNETICKÉ OBRANĚ.

Monitorování uživatelů je proces sběrů informací, analýzy a vyhodnocování uživatelských aktivit. S rostoucí komplexností kybernetických hrozeb se stává bezpečnostní monitoring nejen doplňkem pro organizace, ale také zásadním prvkem obrany proti vnějším a vnitřním hrozbám v organizaci. Monitoring uživatelů nám pomáhá identifikovat neobvyklé chování, které mohou být signálem kybernetického útoku. Jedním z prvních prvků v infrastruktuře kybernetické bezpečnosti, který může zachytit pokus o zpronevěru dat, je SIEM. Tato technologie slouží, jako centrální bod pro analýzu informací. Díky pokročilým analytickým schopnostem a využití strojového učení může SIEM rychle identifikovat anomálie v chování uživatelů nebo aplikací, které by mohly naznačovat pokus o neoprávněný přístup nebo exfiltraci dat. Integrace monitoringu uživatelů do systému SIEM poskytuje organizacím významnou obrannou schopnost a rychlý přístup k nápravám při útocích. [15]

Obrázek 5 – Hlavní příčiny vzniků incidentů v organizacích

3.1 SOC (Security Operations Center)

Bezpečnostní operační centrum je centralizována funkce v rámci organizace, která využívá lidi, procesy a technologie k nepřetržitému monitorování a zlepšování bezpečnostního

postavení organizace a zároveň k prevenci, odhalování, analýze a reakci na kybernetické bezpečnostní incidenty. SOC funguje jako centrum nebo centrální velitelské stanoviště, které přijímá telemetrii z celé IT infrastruktury organizace, včetně jejich sítí, zařízení, přístrojů a informačních úložišť, ať už se tato aktiva nacházejí kdekoli. Šíření pokročilých hrozeb klade důraz na shromažďování souvislostí z různých zdrojů.

SOC je v podstatě korelačním bodem pro každou událost zaznamenanou v rámci organizace, která je monitorována. Pro každou z těchto událostí musí SOC rozhodnout, jakým způsobem budou spravovány a jak se na ně bude reagovat. Úkolem týmu bezpečnostních operací a často i centra bezpečnostních operací (SOC) je nepřetržitě monitorovat, odhalovat, vyšetřovat a reagovat na kybernetické hrozby.

Týmy bezpečnostních operací mají za úkol monitorovat a chránit mnoho aktiv, jako je duševní vlastnictví, personální údaje, obchodní systémy a integrita značky. Jako implementační složka celkového rámce kybernetické bezpečnosti organizace fungují týmy bezpečnostních operací jako ústřední bod spolupráce. Ačkoli je každá organizace jiná, určité základní schopnosti a osvědčené postupy bezpečnostních operací dnes představují náležitou péči.

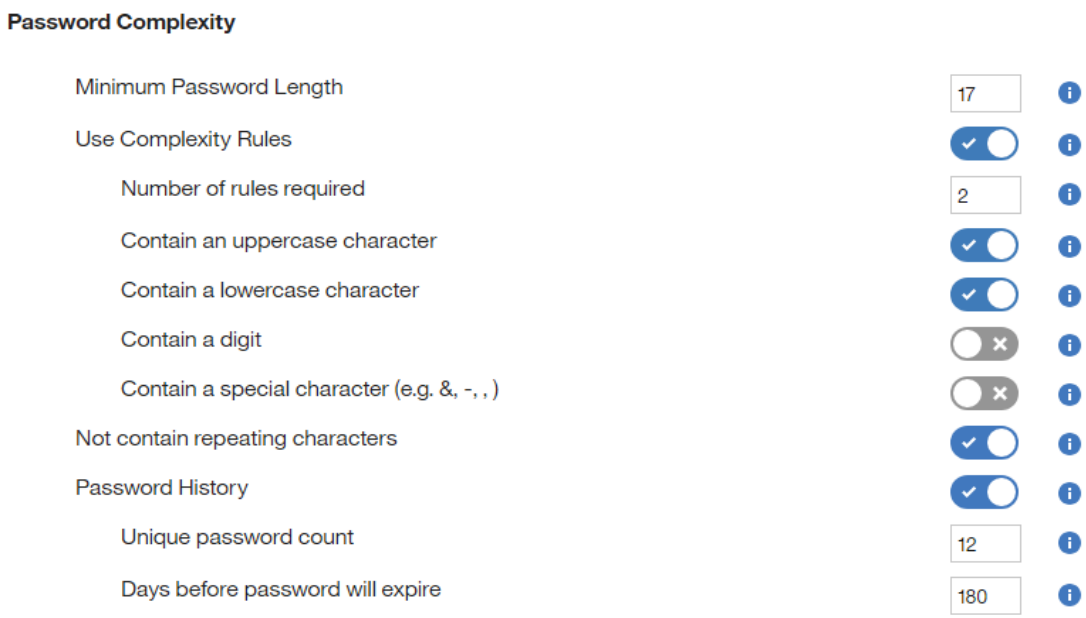
Rozumný proces správy hrozeb začíná plánem a zahrnuje zjišťování (včetně výpočtu základní linie na podporu detekce anomálií, normalizace a korelace), třídění (na základě rizika a hodnoty aktiv), analýzu a stanovení rozsahu (včetně opakovaného vyšetřování). Procesy řízení hrozeb předávají prioritizované a charakterizované případy do programů reakce na incidenty. Dobře definovaný plán reakce je naprosto klíčový pro zvládnutí hrozby nebo minimalizaci škod způsobených únikem dat. [16]

3.2 Monitoring uživatelů

Monitoring uživatelů se zaměřuje na aktivitu jednotlivých uživatelů v interní sítí. Při vyšetřování incidentů se může odehrávat několik scénářů, které musíme při vyšetřování incidentů brát v potaz. V rámci vyšetřování incidentů je klíčové pochopení a identifikace rozlišných scénářů, které mohou signalizovat bezpečnostní problémy nebo pokusy o zneužití systémových zdrojů.

3.2.1 Autentizace a autorizace uživatelů

Pro autentizaci uživatelů do webového prostředí je využit modul LDAP, který je nastaven vůči Active Directory. Definovaní uživatelé využívají pro přihlášení do systému svá doménová jména a hesla. V případě výpadku konektivity s doménovým kontrolérem je možnost zachovat přihlášení uživatele s administrátorskými právy do systému QRadaru pomocí lokálního ověření. Nastavení politiky hesel je zachyceno na obrázku. Tato politika je aplikována pro uživatele, kteří mají povoleno lokální přihlašovaní, pro případ výpadku s AD. [16]



Obrázek 6 – Politika hesel

3.2.2 Role

Bezpečnostní profily a role definují, jaké informace (logy, flow) ze systému mohou jednotliví uživatelé zobrazit. Pomocí rolí můžeme poté určit, jaké funkce a záložky mohou uživatelé používat. (Offenses, záložka logů, flows, pulse apod.) V systému jsou před definované jednotlivé role.

- Admin – se stará o kompletní fungování QRadaru a má plná práva. Přístup do záložek je modifikovatelný, ale většinou se jedná o kompletní práva k systému.
- Operátoři – má kompletní přístup k funkcím systému QRadar bez možností administrace. (Dashboard. Offenses, Log Activity, Network Activity, Assets, Reports a Pulse). [17]

3.3 Koncové stanice

Termín „koncové stanice“ zahrnují různé typy zařízení v síťovém prostředí. Patří sem jednotlivé počítače zaměstnanců, ale taky i servery nebo virtuální počítače a stanice. Každý z těchto zařízení představuje bod, kde uživatelé přistupují k síťovým službám. Správou koncových stanic se tedy rozumí většinou IT outsourcingové služby, kde poskytoval těchto služeb má odpovědnost za stabilní fungováváni spravovaných stanic.

II. PRAKTICKÁ ČÁST

4 VOLBA PROSTŘEDÍ

Tato kapitola se zaměřuje na volbu prostředí pro nasazení systému SIEM s využitím IBM QRadar. Prostředí bude optimalizováno tak, aby odpovídalo specifikacím a požadavkům středně velké společnosti, se zvláštním důrazem na bezpečnost, efektivitu a škalovatelnost a autotomatizaci základních procesů. Budeme implementovat a nastavovat QRadar a jeho základní konfiguraci a představíme si jednotlivá korelační pravidla specifická pro detekci neobvyklých vzorců chování uživatelů, jak bylo zmíněno v teoretické části a tíženým výsledkem bude uvést QRadaru do ostrého provozu.

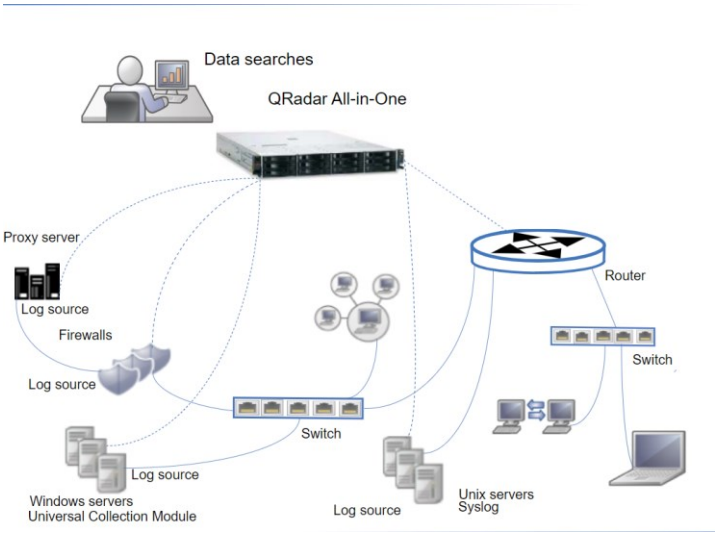
4.1 Analýza prostředí

Architektura SIEM bude založena na konzoli typu „All-in-One“, která je implementována ve virtuálním prostředí. Tato centrální konzole bude zodpovědná za sběr událostí a síťových toků ze systémů v rámci vytvořeného testovacího prostředí pro účely bakalářské práce. Pro integraci logovacích událostí Windows serverů bude využita kombinace Wincollect a technologie od společnosti Microsoft tzv. Windows Event Forwarding. V případě potřeby je možné na server windows, instalovat lokálního agenta, který sbírá logy z OS, tak i lokálních file systému. Lokální agenti zasílají logovací události protokolem Syslog. Autentizace do systému bude zajištěna pomocí Active Directory. Uživatelé se do systému přihlašují pomocí stávajících doménových účtů. Autorizace a udělení práv bude realizováno přímo v systému QRadar. Systém SIEM bude napojen přes internet do externí databáze IBM X-Force Threat Intelligence a bude schopen načítat bezpečnostní informace pomocí standardu STIX/TAXII z externího zdroje v případě potřeby.

4.2 QRadar All-in-One

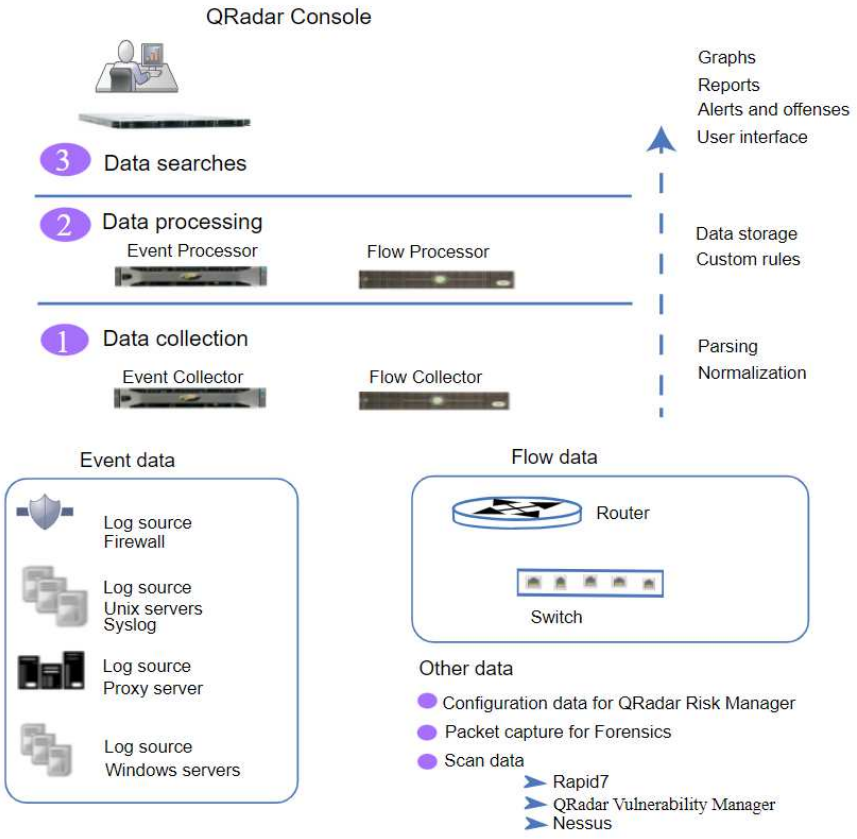
Architektura IBM QRadar umožňuje nasazení různých velikostí a topologii – od nasazení jednoho hostitele, kde všechny softwarové komponenty běží na jednom systému, až po více hostitelů, kde zařízení, jako kolektory události, kolektory toků, datové uzly a aplikace mají specifickou roli. Primárně se chci fokusovat v této bakalářské práci na nasazení, automatizaci a popis a jednotlivých zařízení All-in-One pro středně velkou společnost. Před plánovaním nasazení je dobré si položit tyto otázky. Jak společnost využívá internet? Odesílá se více dat, než kolik stahujeme? Zvýšené využívání může zvýšit vystavení potenciálním bezpečnostním problémům. Kolik události za sekundu (EPS) a toků za minutu (FPM)

potřebujeme monitorovat. Požadavky na kapacitu licencí EPS a FPM se s rostoucím počtem zvyšují. S výkonem exponenciálně rostou i požadavky na retenci dat, a proto musíme vzít v úvahu i dostatečnou kapacitu úložiště.[20]



Obrázek 7 – Architektura All-in-One

4.3 Architektura QRadar



Obrázek 8 – Architektura QRadar

4.3.1 Sběr dat

Sběr dat je první vrstvou, kde se z Vaší sítě shromažďují data, jako jsou události nebo toky. Zařízení All-in-One lze použit ke sběru dat přímo ze sítě nebo můžeme použít kolektory, jako jsou QRadar Event Collectors nebo QRadar QFlow Collectors pro sběr dat o událostech nebo tocích. Data jsou před předaním do další vrstvy zpracována a normalizována. Když jsou nezpracována data analyzována, jsou normalizovaná, aby byla prezentována ve strukturovaném a použitelném formátu. [17]

4.3.1.1 Event data

Data událostí představují události, ke kterým dochází v určitém okamžiku v prostředí uživatele, jako je přihlášení uživatele, připojení VPN, odmítnutí brány firewall, připojení proxy a jakékoli další události o kterých chce mít správce informace.[17]

4.3.1.2 Flow data

Data toku jsou informace o síťové aktivitě nebo informace o relaci mezi dvěma hostiteli v síti, které QRadar převádí do záznamů toku. QRadar překládá nebo normalizuje nezpracovaná data na IP adresy, porty, počty bajtů a paketů a další informace do záznamů toku, které efektivně představují relaci mezi dvěma hostiteli. Kromě shromažďování informací o toku pomocí Flow Collector je k dispozici úplné zachycení paketů s komponentou QRadar Incident Forensics.[17]

4.3.2 Zpracovaní dat

Po shromáždění dat následuje druhá vrstva neboli vrstva zpracování dat, kde jsou data o událostech a tocích prohnána přes nástroj CRE (Custom Rules Engine), který generuje Offense výstrahy a poté jsou data zapsána do úložiště. Data událostí a data toků lze zpracovávat pomocí zařízení All-in-One, aniž by bylo nutné přidávat procesory událostí nebo procesory toků. Pokud je kapacita zpracování zařízení All-in-One překročena, může být nutné přidat procesory událostí, procesory toků nebo jiné zařízení pro zpracování, které zvládne další požadavky. Můžete také potřebovat větší kapacitu úložiště, což lze řešit přidáním datových uzlů.

4.3.3 Vyhledávání dat

Ve třetí nejvyšší vrstvě systému QRadar jsou data dostupná uživatelům pro vyhledávání, hlášení a upozornění pro následné vyšetřování incidentů. Uživatelé mohou prostřednictvím GUI QRadaru spravovat bezpečnostní přestupky pro svou síť a tím mít relevantní zdroje dat pro zpracování. V zařízení All-in-One jsou všechna data shromažďována, zpracovávána a uchovávána přímo na zařízení All-in-One.

4.3.4 Metody sběru dat

Systém IBM QRadar umožňuje několik způsobu pro sběr logovacích událostí a síťových toků. Hlavní rozdíl mezi technologiemi sběru je způsob doručení. Při využití push metody jsou data automaticky odesílaná na servery SIEM bez zásahu do procesu doručení. Naopak pull metody iniciují servery SIEM komunikaci a data jsou z těchto serveru dynamicky vyčítána.[19]

4.3.4.1 Push metoda

Pro metodu Push je nejčastěji využívanou metodou Syslog. Z důvodu širokého rozšíření, snadné konfigurace, nízké zátěží pro logovací zdroj, možnosti zasílání přes UDP i TCP.

- TCP/UDP Syslog
- Multiline TCP/UDP Syslog
- HTTP Receiver
- SNMP
- Lokální agent Wincollect (Syslog)
- Tail2Syslog (script pro monitoring vlastního souboru na Linux – syslog)
- JFlow
- SFlow
- Netflow v.1/v.5/v.7/v.9
- IPFIX
- SFlow v.2/v.4/v.5

4.3.4.2 Pull metoda

V případě metody Pull je využíváno více protokolů dle možností zdroje.

- JDBC
- FTP
- FTPS
- SFTP
- SCP
- REST API
- SMB
- Vlastní script

4.3.4.3 Podporované / Nepodporované logovací zdroje

Korelační engine, který je zodpovědný za testování logovacích událostí a flow pracuje s normalizovanými událostmi. Filtrování a vyhledávání dat v systému probíhá primárně prostřednictvím normalizovaných polí. Normalizace je proces, při kterém se původní data (raw data) převádějí do standardizovaného formátu, který je konzistentní bez ohledu na způsob přenosu. Je to nezbytné, protože formáty a obsah logů se mohou značně lišit, protože neexistuje univerzální standard. Protokoly síťových toků však tuto potřebu nemají, protože obsahová pole jsou standardizována.[20]

Log záznam kritické IBM ISIM 6.0:

```
[3.3.24 17:18:57:126 SE?] 00000043 LTPAServerObj E SECJ0369E: Authentication failed when using LTPA.
The exception is Password check failed for user: itim manager.

[3.3.24 17:18:57:151 SE?] 00000043 FormLoginExte E SECJ0118E: Authentication error during authentica-
tion for user itim manager
```

Log záznam Cisco routeru:

```
1252: *Dec 03 19:13:37.011: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: root] [Source: 10.10.10.2]
[localport: 23] [Reason: Login Authentication Failed - BadPassword] at 19:13:36 CST Thu Dec 03 2013
```

Normalizovaná logovací událost je v systému definována těmito poli:

- **Event Name** – jméno události,
- **Log Source** – logovací zdroj (zdroj dat),
- **Event Count** – počet událostí,

- **Time** – datum a čas příjmu události,
- **Low Level Category** – zařazení události do kategorie,
- **Source IP** – zdrojová IP adresa vztahující se k události,
- **Source Port** – zdrojový port související s událostí,
- **Destination IP** – IP adresa destinace spojená s událostí,
- **Destination Port** – cílový port spojený s událostí,
- **Username** – uživatel spojený s událostí,
- **Magnitude** – výpočet celkové závažnosti události.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
User Login Failure t...	web portal	1	11/20/14, 1:16:15 PM	User Login Failure	91.200.12.41	0	172.17.1.20	0	uoqdvyqgt	
User Login Failure t...	web portal	1	11/20/14, 12:49:01 PM	User Login Failure	91.207.6.118	0	172.17.1.20	0	cvetonqci	
User Login Failure t...	web portal	1	11/20/14, 12:33:54 PM	User Login Failure	91.200.12.41	0	172.17.1.20	0	ayimefftd	

Obrázek 9 – Normalizována logovací událost

Předpis, který určuje, jak bude zpráva normalizována, se nazývá DSM parser. Systém IBM Security QRadar SIEM obsahuje předinstalované DSM parsery společnostní IBM. Po napojení systém tedy rozumí obsahu logovacích událostí. Takové zdroje, ke kterým jsou v systému dostupné DSM parsery, se nazývají podporované. Pro nepodporované zdroje musí být DSM parser vytvořen manuálně. Seznam aktuálně podporovaných zdrojů je v době psaní dokumentu dostupný na oficiálních stránkách IBM. [20]

4.4 Doporučení pro logování

Tato kapitola stanovuje doporučení pro logování informačních systémů, aplikací a dalších prvků infrastruktury. Cílem je zajistit, aby logovací události posílané do systému IBM Security QRadar SIEM byly zpracovatelné a relevantní. Pokud je třeba nastavit úroveň logování, doporučuje se použít úroveň "Informational", pokud není uvedeno jinak. Kapitola uvádí obecná doporučení pro konfiguraci a vývoj logování, která jsou určena především pro dodavatele informačních systémů a aplikací. Stejné principy lze ale použít i na jiné vrstvy informační architektury.[21]

4.4.1 Doporučený obsah logovacích událostí a síťových toků

Logovací události by měly zahrnovat informace z následujícího seznamu, který vychází z vyhlášky č. 82/2018 Sb. zákona o kybernetické bezpečnosti:

- Přihlašování a odhlašování všech účtů, včetně neúspěšných pokusů.
- Činnosti prováděné administrátory.
- Úspěšná i neúspěšná manipulace s účty, oprávněními a právy.

- Neprovedené akce kvůli nedostatku přístupových práv a oprávnění.
- Činnosti uživatelů, které mohou ovlivnit bezpečnost informačních systémů.
- Zahájení a ukončení technických aktivit.
- Kritická i chybová hlášení technických zařízení.

Kromě těchto údajů by logovací události měly obsahovat následující atributy, pokud jsou pro daný zdroj a typ události relevantní:

- Identifikátor události (typ činnosti).
- Výsledek činnosti (úspěšná nebo neúspěšná).
- Datum a čas (ve formátu DD-MM-RRRR HH:MM:SS).
- Jednoznačná síťová identifikace zařízení (IP adresa zdroje).
- Jednoznačná identifikace uživatelského účtu [21]

4.4.2 Způsob záznamu a doručení logovacích událostí a síťových toků

Systém IBM Security QRadar SIEM podporuje různé protokoly a standardy pro příjem logovacích událostí. Pro přenos dat by měl být zvolen vhodný protokol. Zde jsou doporučení pro některé oblasti.

4.4.2.1 UNIX/Linux OS

Nejčastěji se používá protokol Syslog kvůli jeho rozšíření a snadné implementaci. Nabízí velice jednoduchou integraci, která zahrnuje úpravu jednoho konfiguračního souboru.

4.4.2.2 Microsoft Windows

Windows ukládá logy do tzv. EventLog (Security, System, Application atd.). Pro přístup k těmto logům využívá IBM Security QRadar technologii WinCollect, která umožňuje vzdálený nebo lokální sběr dat. Při použití lokálního WinCollect agenta se logy v reálném čase odesílají přímo do SIEM. Vzdálené vyčítání pomocí MSRPC umožňuje spravovat logy centrálně, ale vyžaduje více portů a nabízí nižší výkon.

4.4.2.3 Windows Event Forwarding:

Umožňuje centrální správu logů pomocí GPO, bez nutnosti instalace agenta. Není nutný žádný účet a pro provoz stačí jeden port. Centrální správa pomocí politik GPO. Administrátor SIEM se dozví o existenci nového stroje (události v generickým LS). Toto elegantní řešení je velice jednoduché na správu a zároveň je vybaveno šifrovaným a autentizovaným

přenosem mezi serverem a WEC kolektorem. Nicméně toto řešení má i své nevýhody. Konfigurace vyčítání není prováděna v QRadaru, ale na centrálním WEC serveru. Je důležité myslet na rozložení zátěže (cca 5000 EPS na WEC). Není možné vyčítat lokální soubory (v takových případech je nutný agent). [19]

4.5 Plán konfigurace

Výkonnostní parametry systému (trvalé toky):

- 1 100 EPS (korelační engine)
- 15 000 FPM

Architektura SIEM bude založena na konceptu „All-in-One konzole“, která bude nainstalována ve virtuálním prostředí. Tato centrální konzole bude zodpovědná za sběr událostí a síťových toků z různých systémů. Instalace IBM QRadar bude realizována s využitím zákaznického prostředí klienta, aby bylo možně efektivně interagovat se zdroji dat a přizpůsobit sběr a analýzu specifickým potřebám klienta.

Pro integraci logovacích událostí Windows serverů bude použita kombinace technologie IBM WinCollect a nástroje Windows Event Forwarding od společnosti Microsoft. Pokud bude potřeba, nainstaluji lokální WinCollect agenta přímo na Windows servery. Tento agent umožní sběr logů nejen z operačního systému, ale také z lokálních souborů v rámci souborového systému. Lokální agenti budou odesílat logovací události protokolem Syslog. Pro účely korelačních pravidel a autentizace bude vytvořeno propojení s doménovým kontrolerem. Autentizace do systému bude probíhat přes Active Directory, což umožní uživatelům přihlašovat se pomocí stávajících doménových účtů. Autorizace a udělování práv se budou spravovat přímo v systému QRadar. SIEM bude připojen přes internet k externí databázi IBM X-Force Threat Intelligence a v případě potřeby načte bezpečnostní informace pomocí standardu STIX/TAXII z externích zdrojů.

4.5.1 Výpočet odhadu diskového prostoru úložiště logů

QRadar Deployment (Events + Flows)	User / External Storage
Available storage in TB	**6**
Storage in Bytes	6 597 069 766 656
85% disk allowed utilization	5 607 509 301 658
Storage for Days uncompressed	500 328 360 000
Remaining for compressed data	5 107 180 941 658
Uncompressed / Raw Days	7
Compressed / Normalized Days	357
Total Storage in days	**364**

Tabulka 1 - Výpočet odhadu

4.5.2 Výpočet odhadu počtu EPS a FPM

Výpočet očekávaného počtu EPS a FPM v prostředí Zadavatele je založen na základě kvalifikovaného odhadu metrik jednotlivých technologií a kalkulátoru IBM.

	Device Type	Qty.	EPS Factor	EPS Rate
Event Sources	Windows General Purpose Servers	80	2	160
	UNIX / Linux General Purpose Servers	13	1	13
	Windows Active Directory Servers	2	30	60
	RADIUS/LDAP serevrs	1	5	5
	DNS / DHCP Servers	2	20	40
	Windows Fileservers	1	30	30
	Antivirus, Anti-Malware Servers	1	20	20
	Database Servers	10	10	100
	WEB and Mail servers	5	20	100
	Terminal (Jump) server	1	5	5

	Proxy Servers	1	25	25
	Large Firewalls	2	150	300
	Small Firewalls	0	25	0
	IDS, IPS, DAM, NAC and DLP	1	5	5
	VPN concentrators	1	5	5
	WiFi controlers	1	5	5
	Routers and Switches	30	0,25	8
	Server management cards (iDrac. iLo)	11	0,25	3
	Managed UPS	0	1	0
	ESXi, Hyper-V or other hyperviz. hosts	3	10	30
	Významný informační systém	0	5	0
	Koncová PC a NTB	0	0,5	0
				0
Additio-nal Event Sources	AD users	300	0,1	30
	MS O365 users	300	0,1	30
				0
				0
	Total Log Sources	**166**	**Total EPS License**	**973**

Tabulka 2 – Výpočet EPS

Závěr: Licence 1 100 EPS by měla dostačovat

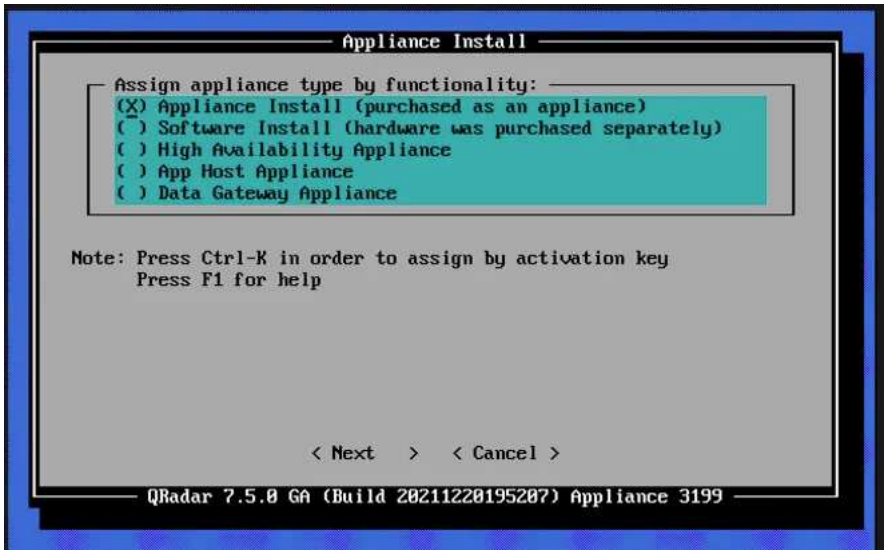
	Device Type	**Qty.**	**Flow Factor**	**Flow Rate**
Flow Sources	Total Workstations on Network	300	15	4 500
	Total Servers on Network	95	150	14 250
	Total FPM License			**18 750**

Tabulka 3 – Výpočet FPM

Závěr: Licence 15 000 nebude dostatečnou a v budoucnu se bude muset uvažovat o jejím rozšíření.

4.5.3 Instalace IBM Security QRadar

IBM QRadar je dostupný v ISO verzi, bežící na OS Linux CentOS. Připojíme ISO tedy k virtuální diskové jednotce a zapneme instalaci.



Obrázek 10 – Instalace QRadaru

4.5.4 Diskový oddíl

RHEL má doporučený průvodce rozdělením diskových oddílu, který umožňuje optimalizovat výkon a zapezpečení systému.

- /boot: Oddíl je určen pro bootovací informace a jádro systému.
- /boot/efi: Malý oddíl, který je využíván v systémech UEFI.
- /recovery: Oddíl určený pro nástroje a data potřebna k obnově systému.
- /var: Oddíl pro ukládání proměnlivých dat jako jsou systémové logy, emailové fronty a další.
- /var/log: Oddíl speciálně pro systémové logy, které pomáhají v diagnostice a monitoringu systému.
- /var/log/audit: Oddíl pro logy auditu, uchovávající záznamy o bezpečnostních událostech a jiné auditní informace.
- /opt: Oddíl pro instalaci volitelných aplikací, slouží jako místo pro softwarové balíčky třetích stran.
- /home: Oddíl pro osobní uživatelské soubory a nastavení, kde každý uživatel má svůj vlastní pododdíl.
- /storetemp: Oddíl pro dočasně ukládané soubory a data, která nejsou nezbytně nutná pro běžný chod systému.
- /tmp: Oddíl pro dočasné soubory vytvořené aplikacemi a systémem, obvykle vyčištěný při restartu.
- swap: Virtuální paměťový oddíl používaný pro zvýšení množství dostupné RAM, přesouvající data mezi fyzickou pamětí a diskem.
- /: Kořenový oddíl obsahující operační systém, všechny aplikace a hlavní systémové soubory.
- /store: Hlavní úložný oddíl pro dlouhodobé skladování dat a aplikací, využívá většinu zbylého prostoru na disku.
- /transient: Oddíl pro krátkodobé skladování dat, která se mohou často měnit nebo jsou dočasně potřebná.

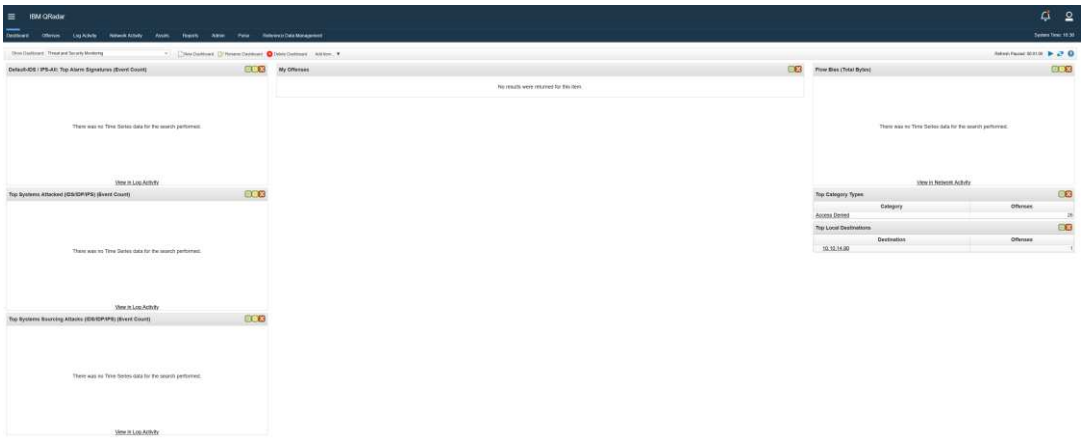
Table 9. Partitioning guide for RHEL

Mount Path	LVM supported?	Exists on Software Installation?	Size
/boot	No	Yes	1 GB
/boot/efi	No	Yes	200 MB
/recovery	No	No	8 GB
/var	Yes	Yes	5 GB
/var/log	Yes	Yes	15 GB
/var/log/audit	Yes	Yes	3 GB
/opt	Yes	Yes	13 GB
/home	Yes	Yes	1 GB
/storetmp	Yes	Yes	15 GB
/tmp	Yes	Yes	3 GB
swap	N/A	Yes	Swap formula: Configure the swap partition size to be 75 per cent of RAM, with a minimum value of 12 GiB and a maximum value of 24 GiB.
/	Yes	Yes	Up to 15 GB
/store	Yes	Yes	80% of remaining space
/transient	Yes	Yes	20% of remaining space

Obrázek 11 – Rozdělení partitions

4.5.5 GUI

Po instalaci vidíme na dané IP adrese, kterou jsme zadali při instalaci výchozí zobrazení QRadaru. Pro zabezpečení komunikace uživatelů s webovou konzolí je důležité nahradit výchozí certifikát IBM certifikátem vlastním. Importovat je možné jak certifikáty vnitřní certifikační autority, tak certifikát vydaný komerčním subjektem. Důležité je, aby certifikát splňoval důležité parametry. Musí být x.509 s PEM kódováním base64, musí mít příponu. cert, .crt, .der nebo .pem a privátní klíč nesmí být zaheslovaný.



Obrázek 12 – Grafická konzole po instalaci

- **Dashboard**: Je centrální místo pro monitorování aktuálního stavu bezpečnostního prostředí. Obsahuje widgety a grafy, které zobrazují různé metriky, jako jsou detekované hrozby, aktivity uživatelů, síťová provozní data a další relevantní bezpečnostní informace. Administrátor si může přizpůsobit dashboard pro zobrazení specifických dat, která jsou pro něho prioritní.
- **Offenses**: Záložka Offenses obsahuje seznam všech bezpečnostních incidentů (offenses), které byly detekovány systémem. Danou Offense je si možno přidělit a zpracovat.
- **Log Activity**: V záložce Log Activity uživatelé mohou prohlížet a analyzovat logy z různých zdrojů. Tyto logy obsahují důležité informace o událostech v síti a na hostitelských strojích, což umožňuje hlubší analýzu a forenzní vyšetřování. Filtry a vyhledávací nástroje umožňují uživatelům efektivně třídit a hledat specifické záznamy.
- **Network Activity**: Network Activity poskytuje uživatelům náhled na síťový provoz a aktivitu. Tato sekce zobrazuje informace o toku dat mezi různými uzly v síti, což může zahrnovat zobrazení portů, IP adres, typů protokolů a množství přenesených dat. To pomáhá identifikovat potenciální bezpečnostní rizika a síťové útoky.
- **Assets**: V záložce Assets jsou uvedeny všechny zařízení a zdroje, které jsou sledovány systémem QRadar. Tato sekce umožňuje správcům zobrazit podrobné informace o každém aktivu, včetně jeho konfigurace, přiřazených zranitelností a historie bezpečnostních událostí spojených s tímto aktivem.
- **Reports**: Reports umožňuje generování různých typů reportů pro dokumentaci a audit bezpečnostního stavu organizace. Uživatelé mohou vytvářet, plánovat a distribuovat přizpůsobené reporty, které poskytují přehled o bezpečnostních trendech, incidentech a provozních metrikách.
- **Admin**: Sekce Admin je určena pro správu systému QRadar. Zde mohou správci konfigurovat systémová nastavení, spravovat uživatelské účty, nastavovat pravidla pro sběr dat a konfigurovat integrace s jinými systémy. To zahrnuje také aktualizace a údržbu systému pro zajištění jeho optimálního výkonu.

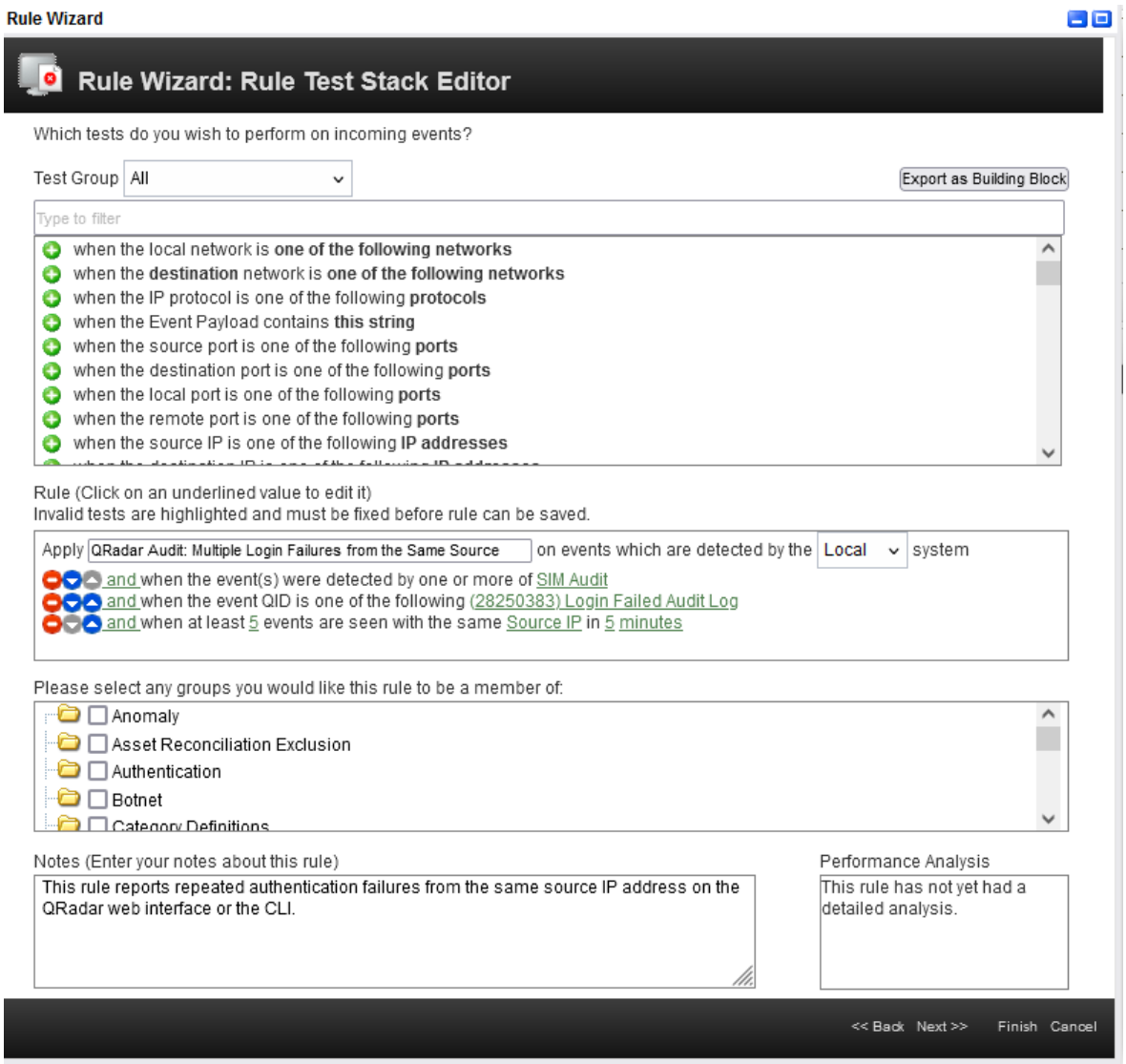
4.6 Vytvoření korelačních pravidel pro monitoring uživatelů

Tato demonstrační část práce se zaměřuje na tvorbu korelačních pravidel pro sledování aktivit uživatelů. Cílem je identifikovat anomální chování, podezřelé přihlašovací pokusy nebo

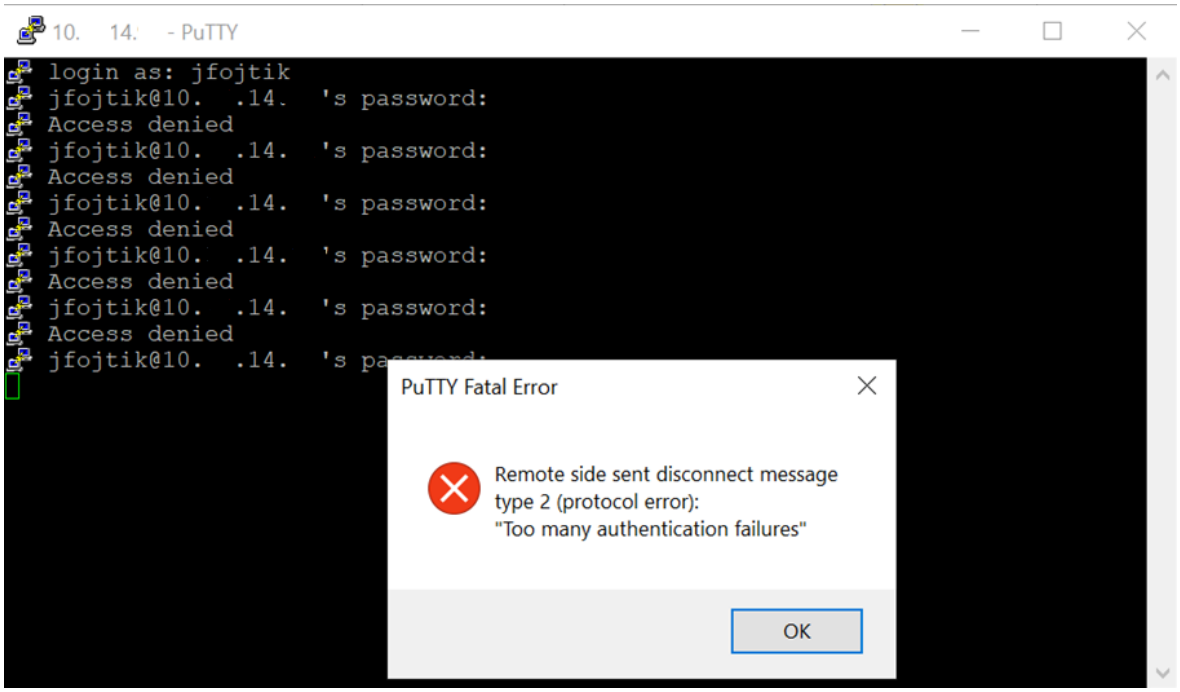
manipulaci s účty, která můžou naznačovat bezpečnostní incidenty. Korelační pravidla jsou navržena tak, aby detekovala neobvyklé aktivity prostřednictvím analýzy logů a síťových toků, čímž umožnuje reagovat okamžitě.

4.6.1 Vícenásobná neúspěšná přihlášení ze stejného zdroje

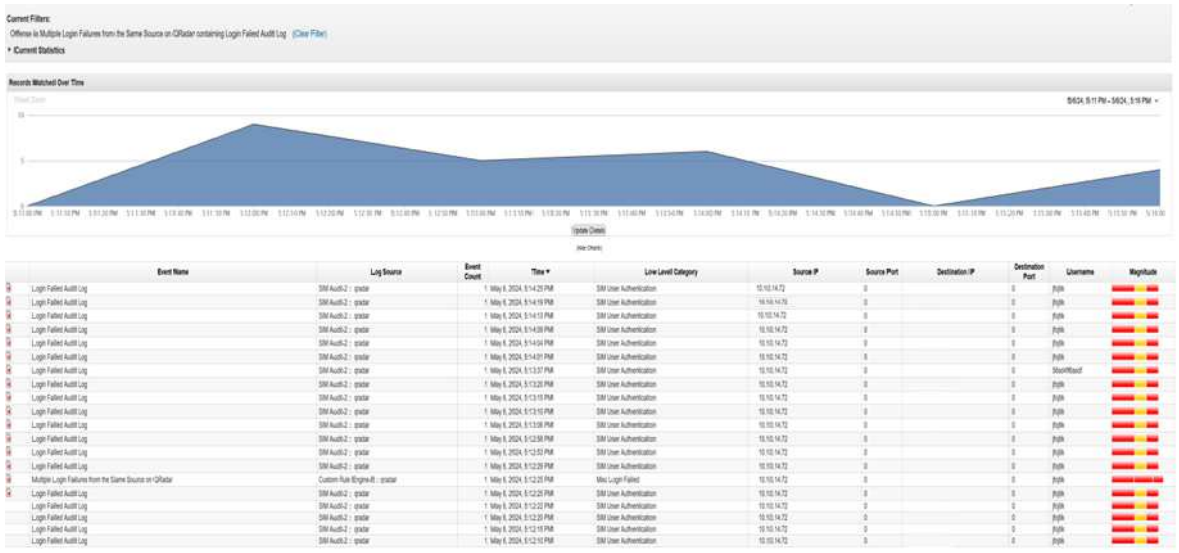
Během 5 minut bude provedeno více jak 10 neúspěšných přihlášení k jednomu Linuxovému serveru pod stejným účtem. První obrázek nám zobrazuje situaci, kdy jsem se pokoušel přihlásit pomocí SSH klienta PuTTy a opakovaně zadával nesprávné heslo. Po několika pokusech se objevuje chybová zpráva „Too many authenticaion failures“, což znamená, že bylo provedeno příliš noho neúspěšných pokusů o autentizaci. Toto je bezpečnostní opatření na straně serveru, které má za cíl zabránit útokům hrubou silou (brute-force attacks), kde útočnici zkouší mnoho kombinací jména a hesla, aby získal neautorizovaný přístup.



Obrázek 13 – Nastavení pravidla Multiple login failures from the same source



Obrázek 14 – Ukázka chybného přihlášení v PuTTy

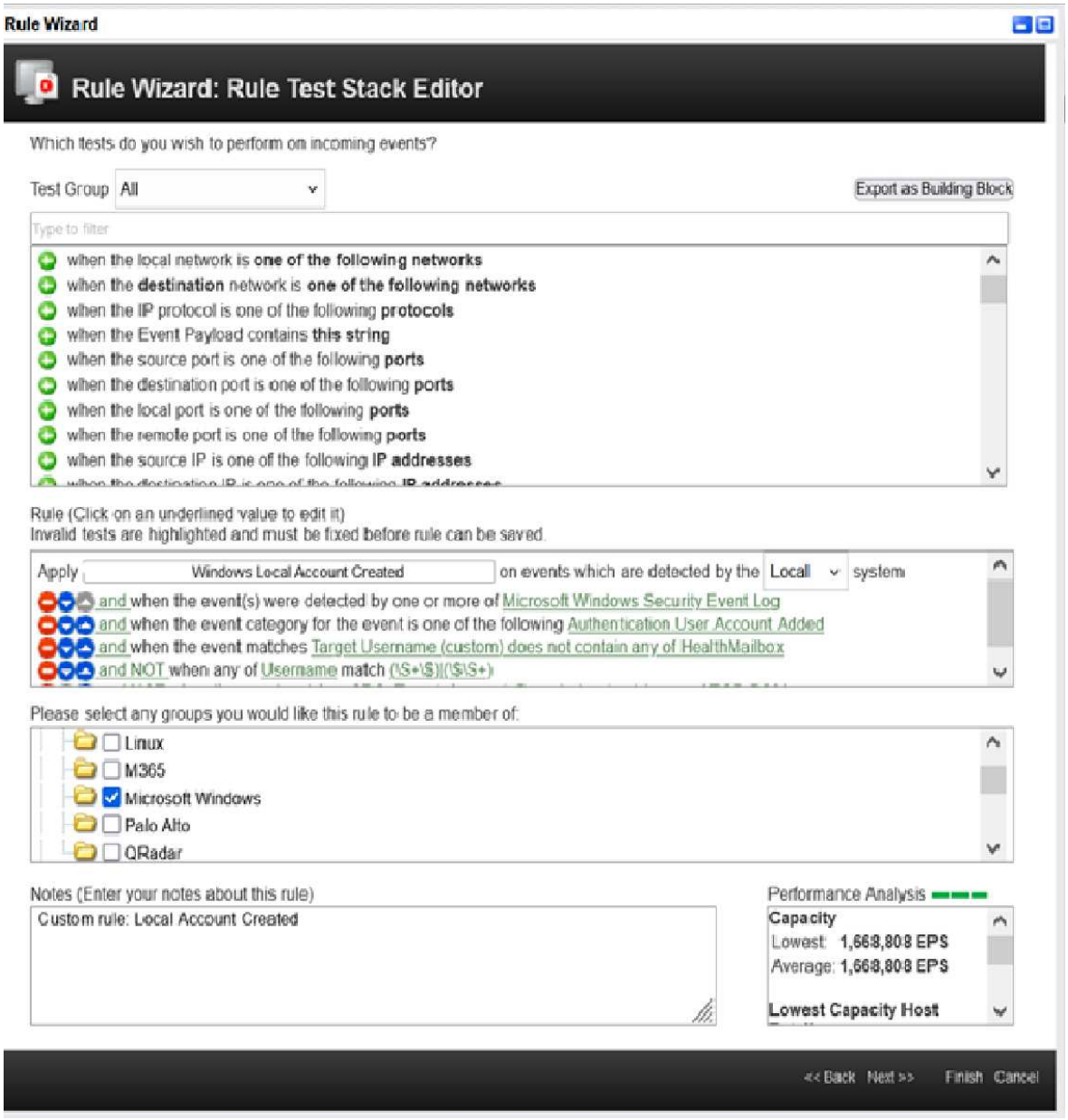


Obrázek 15 – Dashboard offense

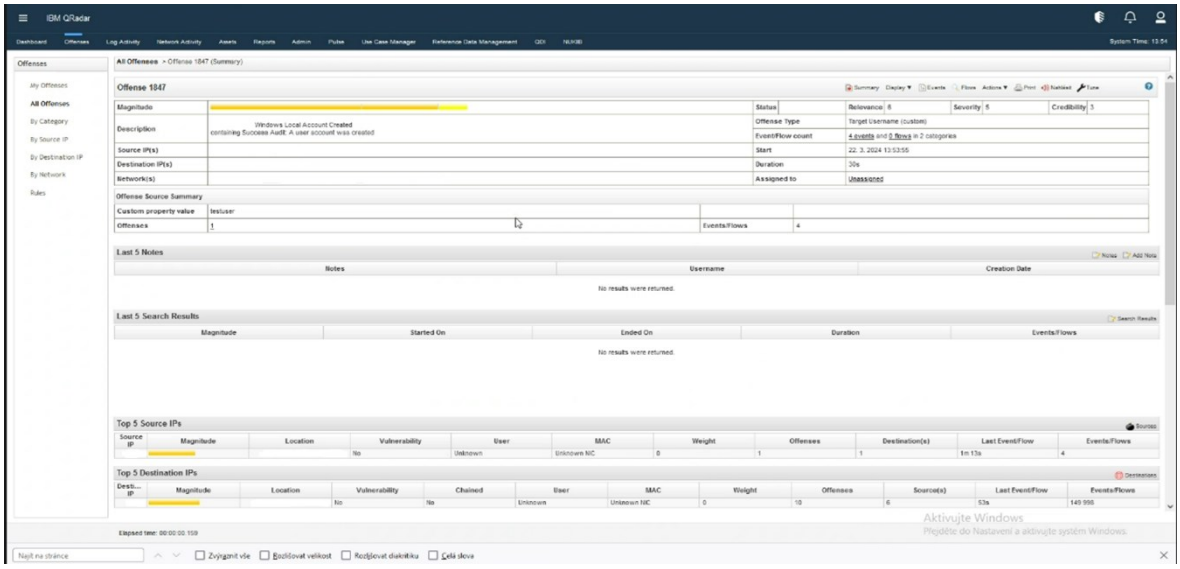
Druhý obrázek nám ukazuje detail vygenerované offense, která v QRadaru na základě neúspěšných přihlášení vznikla. Detaily v tabulce a na grafu naznačují, že dochází k mnohonásobným pokusům o autentizaci v krátkém časovém období, což je typicky znak pokusu o útok hrubou silou nebo možného skriptového útoku. Dashboard slouží, jako nástroj pro sledování bezpečnostních aktivit a pomáhá správcům lépe pochopit vznik dané offense a následovně na ní reagovat.

4.6.2 Vytvoření nového lokálního účtu

Tato událost je detekována a zaznamenávána, protože vytvoření nového lokálního účtu může být známkou potenciální neautorizované aktivity, zejména pokud je prováděno bez předchozího schválení nebo v rámci atypického chování uživatele. V systémech AD může vytvoření nových účtu bez dodržení správných postupů znamenat bezpečnostní riziko, protože útočníci se často maskují způsobem, že vytvoří nové uživatelské účty, aby získali trvalý přístup ke zdrojům.



Obrázek 16 – Vytvoření pravidla Windows Local Account Created

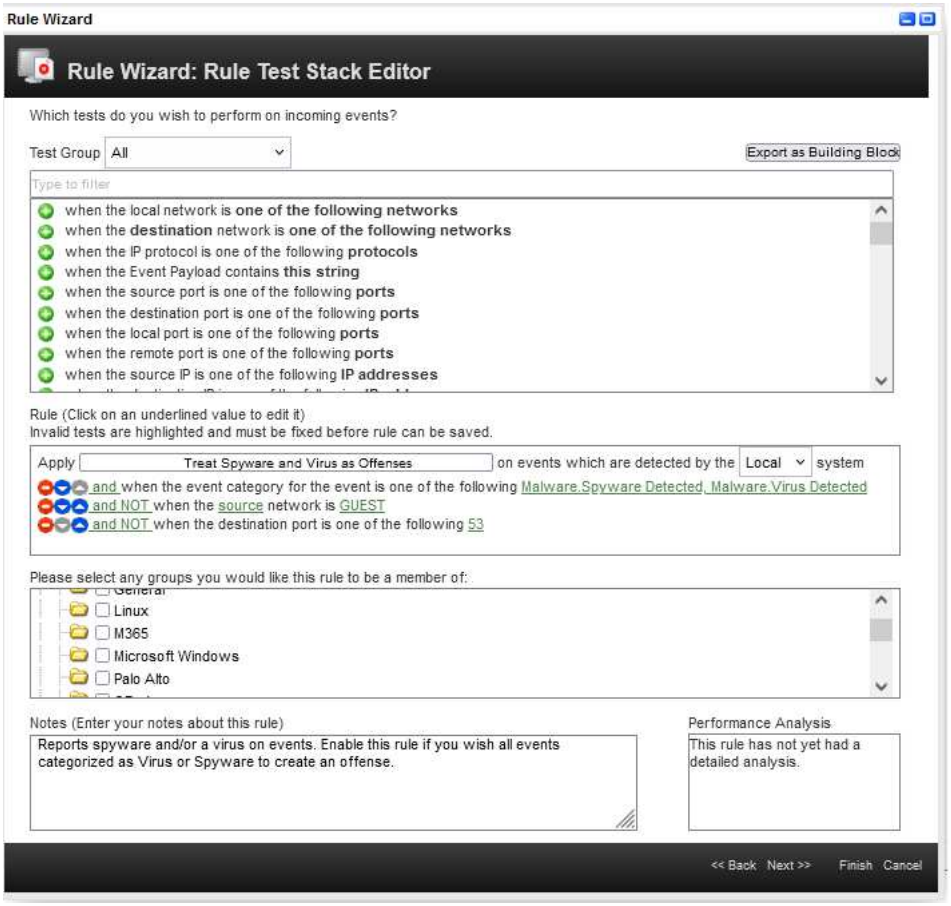


Obrázek 17 – Vygenerování offense – vytvoření nového lokální účtu

4.6.3 Treat Spyware and Virus

Událost odhaluje přítomnost spyware nebo viru v síti, což bylo detekováno antivirovými systémy jako MCAfee a Trellix. Identifikace a klasifikace takových škodlivých softwarů jsou kritické pro zachování bezpečnostní jednotlivých informačních systémů a ochranu dat.

Tento typ události zvyšuje povědomí o bezpečnostních hrozbách a umožňuje rychlou reakci na možné infekce.



Obrázek 18 – Definice pravidla Treat Spyware and Virus

Obrázek 19 – Vygenerování Offense – Treat Spyware and Virus

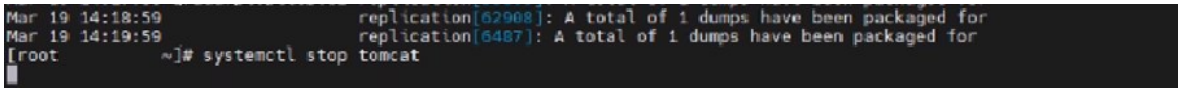
4.6.4 Automatizovány monitoring QRadaru

Monitoring je v systému zajištěn na několika úrovních. Pro demonstraci jsem využil centrální monitoring společnosti Autocont. V systému IBM QRadar je povoleno monitorování pomocí SNMP trapů. SNMP daemon zpřístupní diagnostická data o operačním systému serverů QRadar. K interpretaci dat je použita standardní Linux SNMP template, která je volně dostupná v systému. Na obrázku níže můžeme vidět aktivní status Tomcatu. Pro názornou

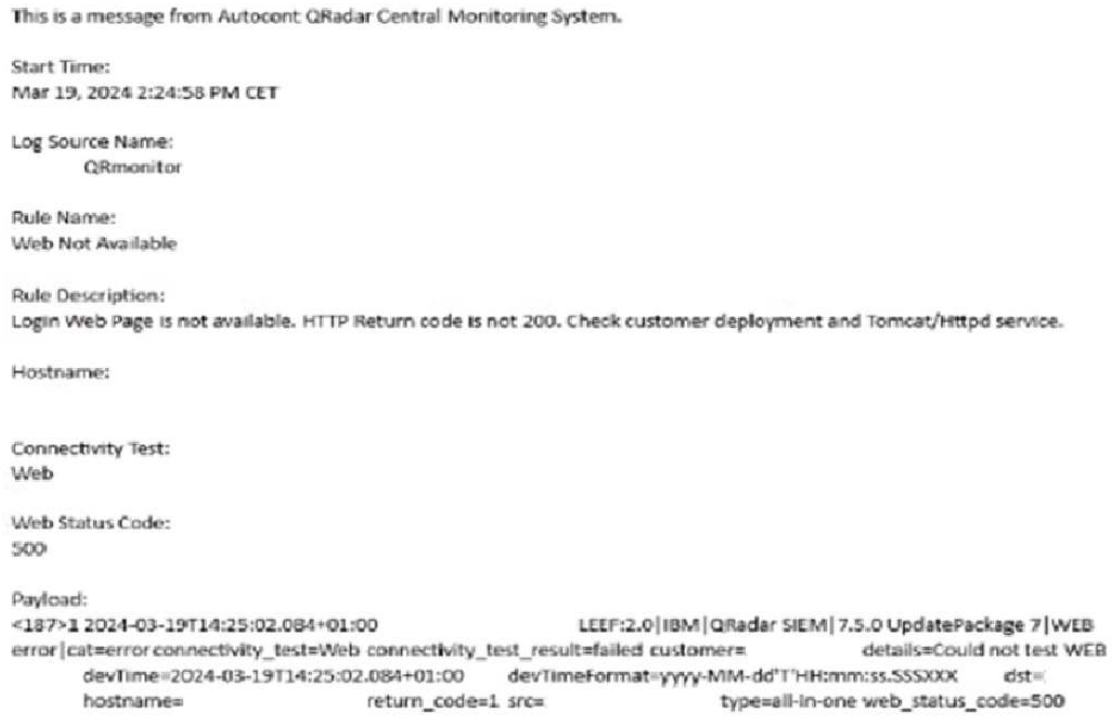
demonstraci a ukázaní funkcionality zastavíme služby a jsme informování skrz email. Pro demonstraci byli některé citlivé informace anonymizovány.

Obrázek 20 – Status Tomcat

4.6.4.1 Zastavení služeb Tomcat



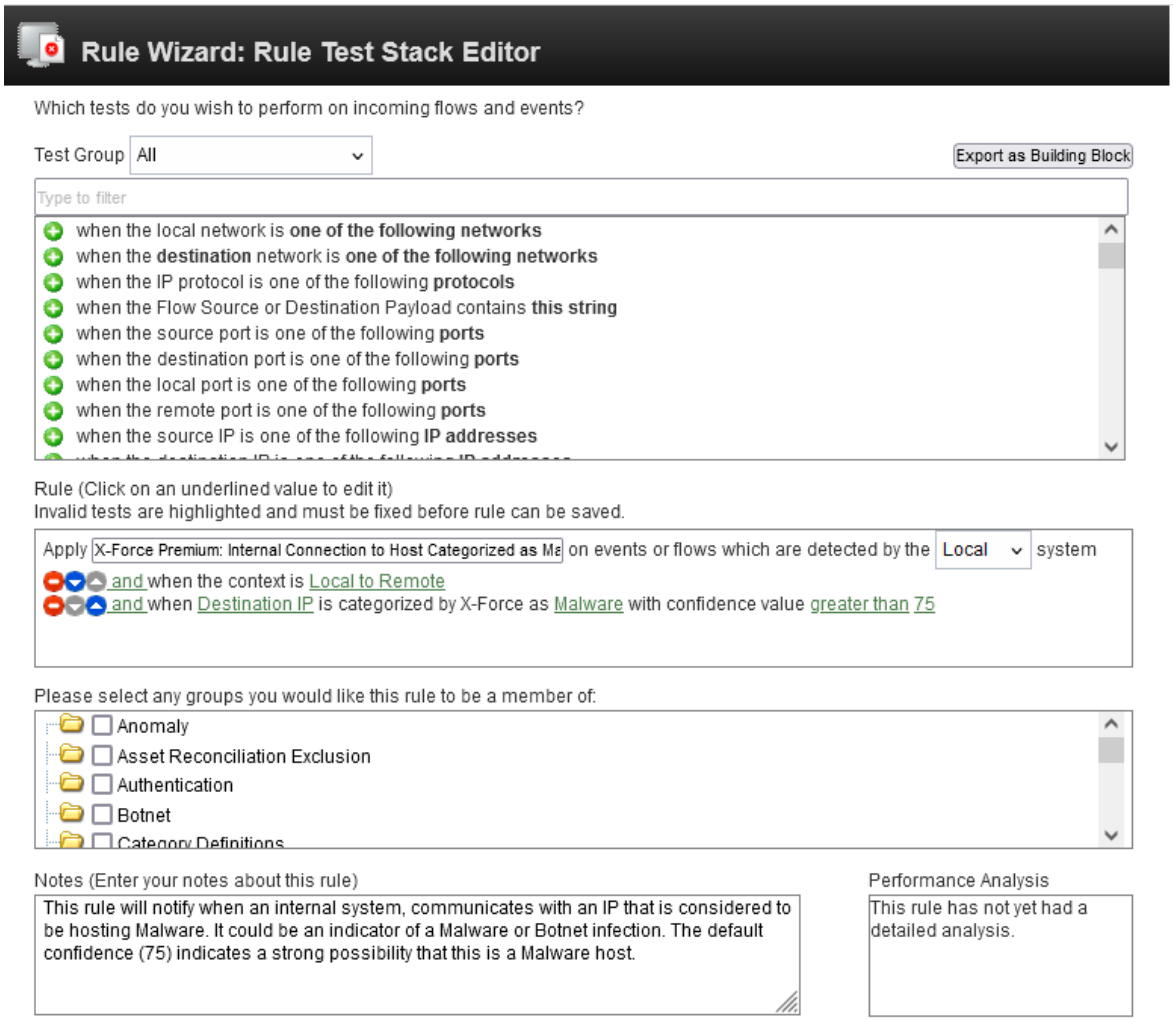
Obrázek 21 – Zastavení služeb



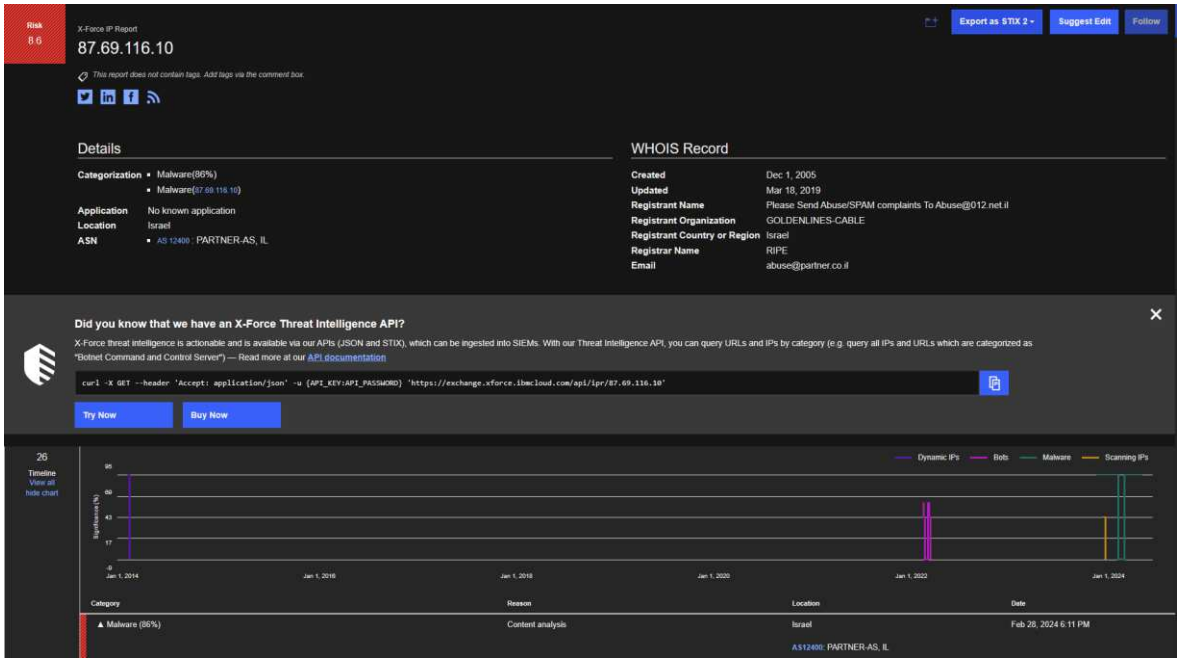
Obrázek 22 – Automatizována notifikace e-mailem

4.6.5 Komunikace s rizikovou IP adresou na černé listině IBM

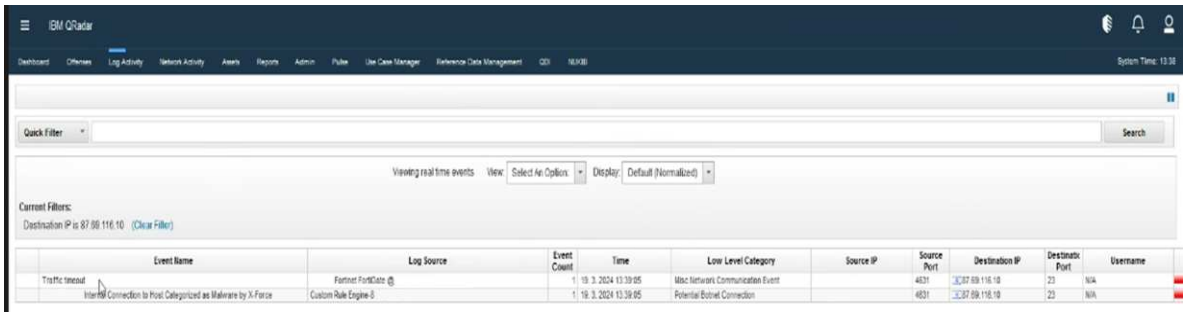
Tato událost značí, že došlo k síťové komunikaci mezi interním systémem a externí IP adresou, která je známa pro svou rizikovost a je zahrnutá na černé listině IBM. IP adresy jsou většinou spojovány s Malwarem, phishingovými akcemi, botnety a jinými škodlivými aktivitami.



Obrázek 23 – Definice pravidla komunikace na IP adresu označenou za nebezpečnou IBM



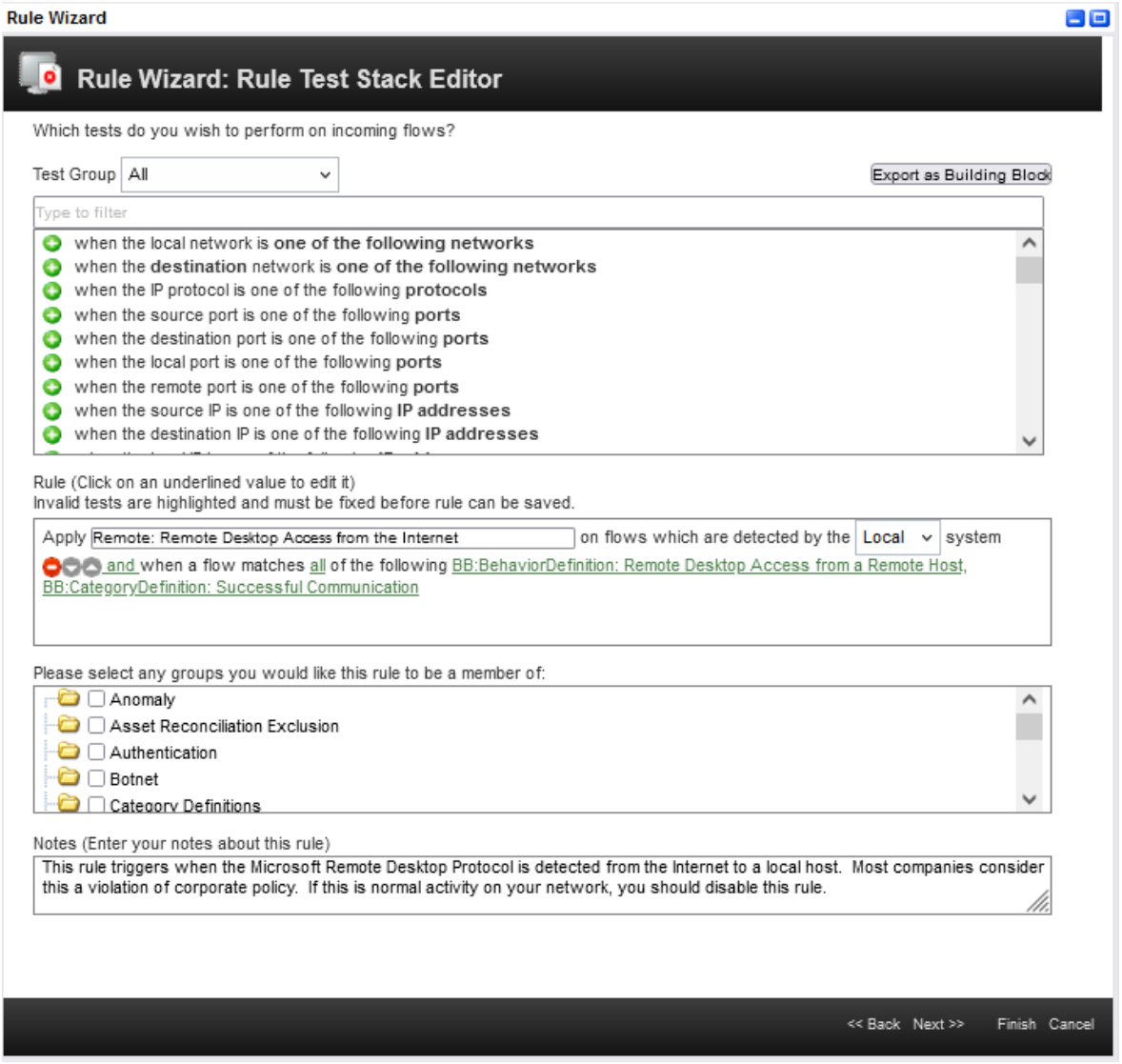
Obrázek 24 – IBM X-Force nebezpečná IP adresa



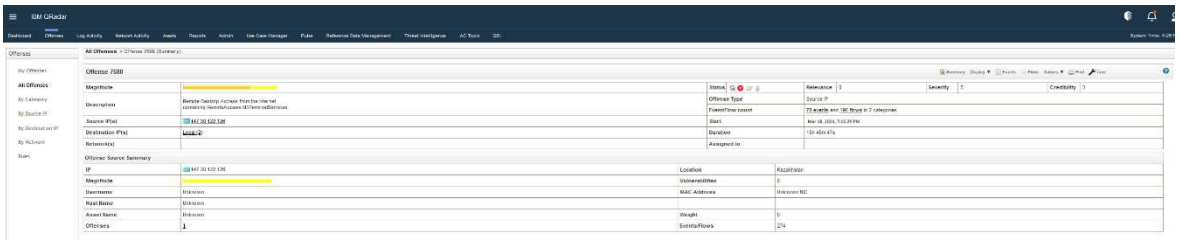
Obrázek 25 – Zobrazení události v Log Activity

4.6.6 Vzdálený přístup desktopu z internetu

Toto pravidlo detekuje pokusy o vzdálené připojení k interním systémům pomocí Microsoft Remote Desktop Protocol (RDP) z externích IP adres, což může znamenat potenciální bezpečnostní riziko. RDP je běžně využíván pro správu serverů a pracovních stanic na dálku, ale když je otevřen přímo z internetu, může se stát cílem útočníků. Pravidlo je navrženo tak, aby upozornilo na neobvyklé nebo neautorizované pokusy o přístup, které by mohly být indikací kompromitace nebo pokusu o neoprávněný přístup.



Obrázek 20 – Definice pravidla Remote Desktop Access from the internet



Obrázek 21 – Vygenerování Offense Remote Desktop Access

4.7 Automatizace QRadaru

V kapitole 4.7.4 Automatizovaný monitoring QRadaru jsme si ukázali pozastavení Tomcatu a následnou předem modifikovanou reakci, která zasílá informativní e-mail správcům, kteří mají instantní přehled. Tomcat je zodpovědný za provoz Java aplikací na webovém serveru, obzvláště ty, které používají Java Servlet a JavaServer Pages (JSP) technologie. Nicméně tohle je jen vrchol ledovce, škálovatelnost a možnosti QRadaru jsou neomezené. Tyto možnosti zlepšují efektivitu operací týmu bezpečnosti, ale také významně snižují možnost lidské chyby a zkracují čas k detekci a řešení hrozeb. Automatizace v QRadaru se může projevovat v mnoha formách, od automatizovaných pravidel pro odezvu, přes integraci s externími tiketovými systémy (např. Jira), po využití playbooku pro standardizované reakce na incidenty.

4.7.1 Automatizované vyčítání Active Directory

V této sekci se věnuji vývoji a implementaci automatizovaného skriptu, jehož úkolem je zefektivnění procesu extrakce uživatelských dat z Active Directory (AD) a jejich následná integrace do systému QRadar. Skript, napsaný v skriptovacím jazyce Bash, je navržen tak, aby automaticky detekoval aktivní hostitelské prostředí kontrolou mountpointu /store. Pokud není mountpoint dostupný, skript se ukončí, což zabraňuje spuštění na neaktivním hostiteli. Dále skript dynamicky načítá přihlašovací údaje pro LDAP z bezpečnostně spravovaného úložiště pomocí utilit secman, což minimalizuje riziko neoprávněného přístupu k citlivým údajům. Po ověření dostupnosti LDAP serveru skript provádí vyhledávání v AD podle specifikovaných parametrů, jako jsou organizační jednotky a uživatelské účty, přičemž výsledky jsou formátovány a ukládány do dočasného souboru. Klíčovým aspektem skriptu je jeho schopnost logovat důležité události během procesu do systémového logu pomocí vlastních syslog zpráv, což umožňuje snadnou auditovatelnost a sledování běhu skriptu. Na závěr, skript využívá nástroje QRadar pro manipulaci s referenčními sadami dat, kde dojde k aktualizaci referenční sady Employee Accounts na základě nejnovějších dat získaných z AD. Tento přístup nejen zvyšuje bezpečnost tím, že udržuje synchronizaci mezi AD a QRadarem, ale také značně snižuje čas a zdroje potřebné pro manuální správu dat, čímž podporuje efektivnější a bezpečnější provoz IT systémů.

4.7.2 Zdrojový kód vyčítání AD

```
#!/bin/bash

# Define constants
SEC_NAME="175.18.24.125"
LDAP_HOSTNAME="AD.BP.server.cz"
LDAP_FILTER="(objectclass=user)"
LDAP_OU="OU=AD,DC=cz,DC=bp,DC=cz"
TEMP_FILE="/opt/scripts/Ldap2RefSets/employees_tmp.csv"
SYSLOG_ID="LDAP2REFSET"
SYSLOG_PORT=514
SYSLOG_SERVER=11.20.0.1
LEEF_HEADER="LEEF:2.0|Employees2ReferenceSet|1.0.0|"
# Load required scripts
source /opt/scripts/BASHFunctions/syslog.sh
# Define functions
get_credentials() {
    LDAP_USER=$(/opt/scripts/secman/secrets_manager get --secret_name $SEC_NAME --user
| tr --delete '\r\n'
    LDAP_USER_PWD=$(/opt/scripts/secman/secrets_manager get --secret_name $SEC_NAME --
password | tr --delete '\r\n')
}
test_connectivity() {
    if nc -z $LDAP_HOSTNAME 636 2>/dev/null; then
        return 0
    else
        return 1
    fi
}
#perform function performs two LDAP searches. The result of these searches are appended
to a temporary file.
perform_search() {
     /opt/scripts/LDAPsearch/ldapsearch -H ldaps://$LDAP_HOSTNAME -D "$LDAP_USER" -w
$LDAP_USER_PWD -o ldif-wrap=no -E pr=1000/noprompt -b "$LDAP_OU" -L -s sub $LDAP_FILTER
sAMAccountName | grep sAMAccountName: | cut -c17- | tr [a-z] [A-Z] >> $TEMP_FILE

    /opt/scripts/LDAPsearch/ldapsearch -H ldaps://$LDAP_HOSTNAME -D "$LDAP_USER" -w
$LDAP_USER_PWD -o ldif-wrap=no -E pr=1000/noprompt -b "$LDAP_OU" -L -s sub $LDAP_FILTER
userPrincipalName | grep userPrincipalName: | cut -c20- | tr [a-z] [A-Z] >> $TEMP_FILE
}

#this functions purges and then loads a reference set named Employee Accounts with the
data in the temporary file.
update_reference_set() {
    /opt/qradar/bin/ReferenceDataUtil.sh purge "Employee Accounts"
    /opt/qradar/bin/ReferenceDataUtil.sh load "Employee Accounts" $TEMP_FILE
}

# Main script
mountpoint -q /store
if [ $? -eq 1 ]; then
    exit 1
fi

get_credentials
if test_connectivity; then
    perform_search
    update_reference_set
else
    echo "Unable to connect to $LDAP_HOSTNAME"
    exit 1
fi
```

Kód 1. Bash script

Tento Bash skript je zodpovědný za interakci s LDAP serverem a k logování pomocí syslogu v systému QRadar. Skript začíná definicí proměnných pro parametry LDAP a syslog zprávy. Obsahuje funkce pro získání přístupových údajů, testování dostupnosti LDAP serveru, vyhledávání v LDAP a aktualizaci referenčních sad. Hlavní část skriptu nejprve ověřuje dostupnost připojovacího bodu /store. Pokud je dostupný, skript načte přihlašovací údaje, testuje připojení k LDAP a v případě úspěchu provádí požadované operace. Při neúspěchu vypíše chybovou zprávu a skript se ukončí. Díky tomu je skript efektivní a bezpečný pro správu dat v systému QRadar.

4.7.3 Zálohování pomocí NFS

NFS je síťový souborový systém, který umožňuje uživatelům na počítačové sítí ukládat a získávat data z centrálního úložiště na síťovém serveru tak, jako by data byla lokální. Tento systém je běžně používán pro zálohování, protože umožňuje efektivní správu a přístup k datům. V první části kódu 2a si deklarujeme proměnné a definujeme cesty a konfigurační parametry, jako je BKUP_DIR, což je adresa a cesta k vzdálenému NFS úložišti. Script také obsahuje cesty k dalším důležitým složkám a konfiguračním souborům, jako jsou APP_BKUP_DIR pro aplikace a LDAP_CONF pro konfiguraci LDAP. Pro logování používá syslog s nastaveními jako SYSLOG_PORT a SYSLOG_HOST a formát zpráv definovaný v LEEF_PREFIX. Dále skript zjišťuje jméno aktuálně přihlášeného uživatele a aktuální čas, které používá pro označení logů.

Hlavní operace zahajuje pokusem o montování NFS úložiště. Pokud je montování úspěšné, skript loguje tuto informaci a pokračuje ve zpracování. V případě selhání montování skript okamžitě loguje chybu a ukončí se, aby zabránil dalšímu zpracování bez přístupu k úložišti. Tímto způsobem skript zajišťuje, že zálohovací proces je pečlivě monitorován a spravován.

Druhá část skriptu se zaměřuje na zálohovací operace a správu dat na NFS úložišti. Nejprve skript získává IP adresu aktuálního zařízení. Používá kombinaci příkazů hostname -I, awk a grep k extrakci a ověření formátu IP adresy. Tento krok je důležitý pro zjištění, zda se skript spustil na primární konzoli, která je definována v proměnné PRIMARY_CONSOLE. Pokud je toto zařízení primární konzole, skript provede další specifické kroky zálohování, které nejsou v ukázce kódu specifikovány, ale byly by zde umístěny.

Následuje pauza, během které skript čeká 2 sekundy, a pak pokračuje ve skutečném zálohování souborů. Vypíše zprávu o zahájení kopírování lokálních zálohových archivů na NFS úložiště. K tomu využívá nástroj rsync s volbami --progress a --times, které zajišťují zobrazení postupu a zachování časových údajů souborů. Skript hledá a synchronizuje soubory s koncovkami .tgz a .tar.gz, které byly modifikovány během posledního dne, z lokálního zálohovacího adresáře do NFS mountpointu. Také synchronizuje specifické aplikace a objemy záloh z adresáře APP_BKUP_DIR.

Na závěr skript loguje prostřednictvím syslogu úspěšné dokončení všech úloh a vypisuje zprávu, že skript skončil. Skript pak končí s návratovým stavem exit 0, což signalizuje úspěšné dokončení bez chyb. Tato část skriptu je klíčová pro zajištění, že všechny zálohy jsou správně synchronizovány a uloženy na vzdálené úložiště, což zvyšuje bezpečnost a dostupnost kritických dat.

```bash
#!/bin/bash
# Backup script for QRadar to a remote location
# Configuration
BKUP_DIR="/store/backup"
NFS_MOUNT="/store/backup/nfs"
REMOTE_NFS="168.39.46.80:/volume1/qradar-nfs"
APP_BKUP_DIR="/store/apps/backup"
BP_PATH="/opt/bakalarka"
SSH_DIR="/root/.ssh"
QR_CONF="/opt/qradar/conf"
LDAP_CONF="/opt/qradar/conf/ldap.properties"
PRIMARY_BKUP_ARCHIVE="/path/to/backup_bp_console_primary.tgz"
SYSLOG_TAG="BACKUP2NFS"
SYSLOG_PORT=514
SYSLOG_HOST=10.10.0.10
LEEF_PREFIX="LEEF:2.0|BP|BACKUP2NFS|1.0.0|"
PRIMARY_CONSOLE=10.10.0.10
BKUP_RETENTION=14

# Import syslog functions
source /opt/bp/scripts/BASHFunctions/syslog.sh

# Get current user and date
CURRENT_USER=$(whoami)
DAY=$(date +%u)
NOW=$(date +"%Y%m%d%H%M%S")
SYSLOG_TIME=$(date +"%Y-%m-%dT%H:%M:%S")

# Log start of script
syslog_message $SYSLOG_HOST $SYSLOG_PORT "local0.info" $SYSLOG_TAG
"$LEEF_PREFIX""INFO|cat=backup  devTime=$(date +"%Y-%m-%dT%H:%M:%S")
devTimeFormat=yyyy-MM-dd'T'HH:mm:ss message=QRadar backup script started."
sleep 2

# Mount remote NFS
mount -t nfs $REMOTE_NFS $NFS_MOUNT

# Check if mount was successful
if mountpoint -q $NFS_MOUNT; then
    mkdir -p $NFS_MOUNT
    syslog_message $SYSLOG_HOST $SYSLOG_PORT "local0.info" $SYSLOG_TAG
"$LEEF_PREFIX""INFO|cat=backup  devTime=$(date +"%Y-%m-%dT%H:%M:%S")
devTimeFormat=yyyy-MM-dd'T'HH:mm:ss message=Mountpoint $NFS_MOUNT mounted."
    echo "BACKUP: INFO: Mountpoint $NFS_MOUNT mounted."
else
    syslog_message $SYSLOG_HOST $SYSLOG_PORT "local0.err" $SYSLOG_TAG
"$LEEF_PREFIX""ERROR|cat=backup devTime=$(date +"%Y-%m-%dT%H:%M:%S")
devTimeFormat=yyyy-MM-dd'T'HH:mm:ss message=Unable to create mountpoint $NFS_MOUNT.
Exit script."
    echo "BACKUP: ERROR: Unable to create mountpoint $NFS_MOUNT. Exit script."
    exit 1
fi

sleep 2
```

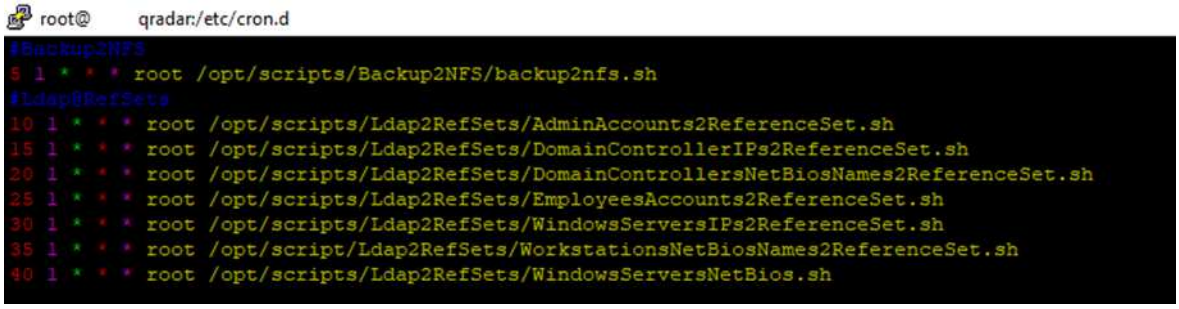
Kód 2a Zálohování NFS

```
sleep 2

# Get IP address
IP_ADDR=$(hostname -I | awk '{print $3}' | grep -E "[ 0-9 ]+.[ 0-9 ]+.[ 0-9 ]+.[ 0-9
]+")

# If on primary console, perform additional backup steps
if [ $IP_ADDR == $PRIMARY_CONSOLE ]; then
    # Additional backup steps here...
fi

sleep 2

# Copy recent backup files to NFS mount
echo "BACKUP: INFO: Copying local backup archives to $NFS_MOUNT"
find $BKUP_DIR -maxdepth 1 -name "*.tgz" -mtime -1 -exec rsync --progress --times "{}"
$NFS_MOUNT \;
find $BKUP_DIR -maxdepth 1 -name "*.tar.gz" -mtime -1 -exec rsync --progress --times "
{}" $NFS_MOUNT \;
rsync --progress --times $APP_BKUP_DIR/backup.apps-volumes.all.*.tgz $NFS_MOUNT

# Log end of script
syslog_message $SYSLOG_HOST $SYSLOG_PORT "local0.info" $SYSLOG_TAG
"$LEEF_PREFIX""INFO|cat=backup  devTime=$(date +"%Y-%m-%dT%H:%M:%S")
devTimeFormat=yyyy-MM-dd'T'HH:mm:ss message=All tasks succussfully finished."

echo "BACKUP: INFO: Scripted finished."
exit 0
```

Kód 2b Zálohování NFS

4.7.3.1 Cron

Je nástroj v operačním systému Unix a Linux k plánování úloh, které mají být spuštěny automaticky v určitých časových interval. Jedná se o daemona, který běží na pozadí a aktivuje plánované úkoly bez nutnosti zásahu uživatele. Úlohy, které cron zpracovává jsou definovány v konfiguračním souboru zvaném crontab, kde každá úloha má specifikovaný čas spuštění a příkaz, který má byt vykonán. Cron umožňuje uživatelům velkou flexibilitu a je schopen plánovat úkoly podle minut, hodin, dnů, měsíců a let. Díky této flexibilitě je ideální pro automatizaci opakujících se úloh, jako je zálohování dat, aktualizace systému a nebo automatické spuštění scriptu, což je přesně případ naší potřeby, který potřebujeme pro přenos dat z AD do referenčních setů v předchozí kapitole.



Obrázek 22 – Nastavení Cronu

4.7.3.2 Syntaxe Cronu

Cron používá specifický formát pro definování, kdy mají být úlohy spuštěny. Formát se skládá z pěti polí oddělených mezerami, přičemž každé pole představuje určitou jednotku času (viz Obrázek 33, který ukazuje příklad nastavení crontabu).

Obrázek 23 – Syntaxe Cronu

5 ZÁVĚR

V úvodu této bakalářské práce byl nastíněn význam efektivního nasazení systémů SIEM pro středně velké společnosti s důrazem na bezpečnost, efektivitu a škálovatelnost informačních systémů. IBM QRadar byl vybrán jako optimální řešení pro tyto účely a byl představen jako komplexní nástroj schopný zajistit zvýšení úrovně kybernetické bezpečnosti a automatizace rutinních procesů. Důraz byl kladen na nutnost ochrany informací ve společnosti, které musí být v souladu s legislativními požadavky a normami EU. QRadar, jakožto nástroj SIEM, umožňuje detailní monitoring a analýzu bezpečnostních událostí, což podporuje zachování důvěrnosti, integrity a dostupnosti citlivých dat.

V průběhu práce byla zdůrazněna potřeba adekvátního sledování chování uživatelů ve firemních informačních systémech. Byla představena implementace a konfigurace systému IBM QRadar SIEM, včetně specifikace jeho architektury. Zároveň bylo ukázáno, jak systém QRadar umožňuje společnosti reagovat na bezpečnostní hrozby v reálném čase prostřednictvím korelačních pravidel a automatického vyhodnocení událostí.

Hlavní část práce představila implementaci korelačních pravidel a analytických nástrojů určených k detekci neobvyklých vzorců chování a potenciálních bezpečnostních incidentů. Tato část zdůrazňuje přínos QRadaru v rámci analýzy a interpretace bezpečnostních dat, což umožňuje společnostem přijmout proaktivní přístup k řízení bezpečnostních rizik. V závěru práce byly představeny praktické příklady konfigurace a využití QRadaru, které demonstrují jeho flexibilitu a široké možnosti přizpůsobení potřebám specifického prostředí.

Tyto příklady ilustrují, jak efektivní nasazení QRadaru může poskytnout cenné náhledy do bezpečnostních operací a významně přispět k zajištění kybernetické odolnosti organizace. Celkově tato práce poskytuje komplexní pohled na implementaci a využití IBM QRadar SIEM jako klíčového nástroje pro zajištění informační bezpečnosti ve středně velké společnosti.

Výsledky ukazují, že QRadar je nejen efektivní v detekci a reakci na bezpečnostní hrozby, ale také podporuje širší integraci bezpečnostních a organizačních opatření do jednotného systému pro zajištění informační bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

[1] Computer Security Principles and Practice, 2018. Online. Computer Security Principles and Practice. S. 1-838. Dostupné z: https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/Computer_Security_Principles_and_Practice_(3rd_Edition).pdf. [cit. 2024-05-12].

[2] ISO. ISO/IEC 27001:2013. Information technology, Security techniques, Information security management systems.

[3] SAP, 2023. Co je to kybernetická bezpečnost? Online. Dostupné z: https://www.sap.com/cz/products/financial-management/what-is-cybersecurity.html. [cit. 2024-05-12].

[4] TECH TARGET, 2023. CIA. Online. Dostupné z: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. [cit. 2024-05-12].

[5] VARONIS, 2024. Cybersecurity Statistics. Online. Dostupné z: https://www.varonis.com/blog/cybersecurity-statistics. [cit. 2024-05-12].

[6] CLOUDFARE, 2023. Phishing Attack. Online. Cloudfare. Dostupné z: https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack/. [cit. 2024-05-12].

[7] OWASP. SQL Injection. Online. OWASP. Dostupné z: https://owasp.org/www-community/attacks/SQL_Injection. [cit. 2024-05-12].

[8] OWASP, 2022. Cross Site Scripting (XSS). Online. OWASP. Dostupné z: https://owasp.org/www-community/attacks/xss/. [cit. 2024-05-12].

[9] Malware attacks types and how to combat them, 2022. Online. Https://imit.com/. Dostupné z: https://imit.com/malware-attacks-types-and-how-to-combat-them/. [cit. 2024-05-12].

[10] OWASP, 2020. Spyware. Online. Https://owasp.org. Dostupné z: https://owasp.org/www-community/attacks/Spyware. [cit. 2024-05-12].

[11] Ransomware Attack: Ransomware Attacks and OWASP Vulnerabilities : Threat to Corporate Giants, 2023. Online. In: LINKEDIN. LinkedIn. Dostupné z: https://www.linkedin.com/pulse/ransomware-attacks-owasp-vulnerabilities-threat-abou-sfeir/. [cit. 2024-05-12].

[12] ENISA EUROPE. Man-In-The-Middle. Online. Https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle. Dostupné z: https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle. [cit. 2024-05-12].

[13] FORTINET. DoS vs DDoS. Online. FORTINET. Https://www.fortinet.com/. Dostupné z: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos. [cit. 2024-05-12].

[14] IBM, 2024. HA Deployment Planning. Online. IBM. Https://ibm.com. Dostupné z: https://www.ibm.com/docs/en/qsip/7.5?topic=deployments-ha-deployment-planning. [cit. 2024-05-12].

[15] IBM, 2023. QRadar. Online. QRadar Architecturen Overview. Dostupné z: https://www.ibm.com/docs/en/qsip/7.4?topic=deployment-qradar-architecture-overview. [cit. 2024-05-12].

[16] CISCO. Cybersecurity threat trends: phishing, crypto top the list. Online. CISCO. Dostupné z: https://learn-cloudsecurity.cisco.com/umbrella-library/2021-cybersecurity-threat-trends-phishing-crypto-top-the-list. [cit. 2024-05-12].

[17] IBM, 2023. QRadar Events and Flows. Online. Https://ibm.com. Dostupné z: https://www.ibm.com/docs/en/qsip/7.5?topic=overview-qradar-events-flows. [cit. 2024-05-12].

[18] IBM, 2024. Management User Roles. Online. IBM. Https://www.ibm.com/. Dostupné z: https://www.ibm.com/docs/en/qradar-on-cloud?topic=management-user-roles. [cit. 2024-05-12].

[19] IBM, 2023. Deployment QRadar Architecture Overview. Online. Https://www.ibm.com/docs/en/qsip/7.5?topic=deployment-qradar-architecture-overview. Dostupné z: https://www.ibm.com/docs/en/qsip/7.5?topic=deployment-qradar-architecture-overview. [cit. 2024-05-12].

[20] IBM, 2024. QRadar Support DSM'S. Online. Https://ibm.com. Dostupné z: https://www.ibm.com/docs/en/dsm?topic=configuration-qradar-supported-dsms. [cit. 2024-05-12].

[21] NUKIB. 82/2018 Sb. zákona o kybernetické bezpečnosti, Sbírka zákonů. 2018. Dostupné také z: https://nukib.gov.cz/download/publikace/legislativa/vkb_82-2018sb.pdf.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Pojem nebo zkratka (CZ)	Význam
API/REST API	API (zkratka pro Application Programming Interface) označuje v informatice rozhraní pro programování aplikací. Tento termín používá softwarové inženýrství. Jde o sbírku procedur, funkcí či tříd nějaké knihovny (ale třeba i jiného programu nebo jádra operačního systému), které může programátor využívat. API určuje, jakým způsobem jsou funkce knihovny volány ze zdrojového kódu programu.
Alerting	Alerting je proces zaslání zprávy technického prvku směrem k člověku.
Autentizace/Authentication	Někdy též autentikace je proces ověření proklamované identity subjektu. Po dokončení autentizace obvykle následuje autorizace, což je souhlas, schválení, umožnění přístupu či provedení konkrétní operace daným subjektem.
Auto Discovery	Funkce systému IBM Security QRadar, která na základě formátu a typu přijatých událostí automaticky vytvoří příslušný Log Source.
Dashboard	Je grafické rozhraní poskytující rychlý a aktuální pohled na klíčové ukazatele relevantních pro takto zavedený systém.
Data Obfuscation	Metoda, kdy při prezentaci osobních údajů v grafické konzoli SIEM systému dochází k jejich anonymizaci.
EPS	Events per Second je počet událostí z logů generovaných za sekundu. V praxi je dobrým přirovnáním: jeden řádek představuje jeden Event. Zároveň se tento ukazatel používá jako licenční metrika v mnoha SIEM řešeních.
EventLog	Je protokol pro záznam programových zpráv na platformě Microsoft Windows. Protokoly událostí jsou zvláštní soubory, do kterých se zaznamenávají významné události v počítači/serveru, jako je přihlášení uživatele do počítače nebo zjištění chyby v programu. Pokaždé, když podobná událost nastane, zaznamená ji operační systém Windows do protokolu událostí.
Event Name	Název logovací události, která je prezentována koncovému uživateli.
Flow Source/ Zdroj Flow	Označení pro zdroj poskytující informace pomocí protokolů síťových toků.
Flow Source Alias	Alias slouží pro rozlišení různých zdrojů informací síťových toků na základě IP adresy.

FPM	Flows per Minute je počet síťových toků za minutu (někdy se též používá jednotka FPS – per Second). Jedná se o počet aktivních síťových relací během jedné minuty. V praxi je dobrým přirovnáním: jedna instance aplikace komunikující po síti představuje jedno Flow. Zároveň se tento ukazatel používá jako licenční metrika v mnoha SIEM řešeních.
FQDN	FQDN je označení pro plně specifikované doménové jméno počítače (zkratka z anglického termínu Fully Qualified Domain Name). Můžeme se ale setkat i s termínem absolutní doménové jméno. FQDN přesně určuje umístění počítače ve stromové struktuře DNS (Domain Name System) včetně uvedení top-level domény a root domény. Příklad: Počítač je označen host jménem (hostname) myhost a je začleněn do domény example.com. Plně specifikované doménové jméno pro tento počítač tedy bude myhost.example.com.
FTP, FTPS, SFTP, SCP	Protokoly pro přenos souborů mezi počítači pomocí počítačové sítě.
IBM Security QRadar	Rodina bezpečnostních produktů společnosti IBM.
Incident	Narušení integrity, důvěrnosti nebo dostupnosti.
Indexace/Indexing	je databázová nebo souborová konstrukce uchovávající metadata, sloužící ke zrychlení vyhledávacích a dotazovacích procesů v databázi nebo na souborovém systému. Indexace pracuje na základě definování unikátní hodnoty jednoho či více sloupců tabulky nebo slouží k optimalizaci fulltextového vyhledávání na souborovém systému.
IPFIX	Na základě protokolu NetFlow v9 vznikl nový IETF standard Internet Protocol Flow Information eXport (IPFIX) – RFC 7011.
JDBC	(Java Database Connectivity) je univerzální aplikační rozhraní pro přístup k relačním databázím.
JFlow	Juniper Flow Monitoring je proprietární modifikace NetFlow protokolu používaná v zařízeních Juniper Networks.
Korelace/Correlation	Schopnost objevit a aplikovat logické asociace mezi různými logovacími událostmi a flow.
Korelační pravidlo/Rule	Je algoritmus uzpůsobený k hledání vzájemné závislosti mezi dvěma či více hodnotami zachycenými v zdroji informace. V kontextu bezpečnosti se jedná o údaje obsažené v lozích nebo síťových flow, které jsou korelovány vzhledem ke kritériu obsaženém v pravidle.

Log Management	Log Management (též LM) je v oblasti bezpečnosti disciplínou, která zahrnuje přístup k práci s velkými objemy počítačem generovaných logů (známých také jako záznamy o auditu, kontrolní záznamy, protokoly událostí atd.). Správa logů obecně zahrnuje: Jejich sběr, centralizovanou agregaci, dlouhodobé uchovávání a archivaci, expiraci, prohledávání a analýzu v nich obsažených informací, či tvorbu přehledů.
Zdroj logovacích událostí /Log Source	Označení pro zdroj logovacích záznamů
Low Level Category	Zařazení logovací události do jedné z příslušných IBM QRadar kategorií
Magnitude	Celková závažnost události vypočítaná pomocí vzorce a dílčích bezpečnostních hodnot
MSRPC	Technologie Microsoft Remote Procedure Call umožňuje bezagentový sběr logovacích záznamů ze systému Microsoft Windows.
NetFlow	NetFlow je otevřený protokol vyvinutý společností Cisco Systems, určený původně jako doplňková služba k Cisco směrovačům. Jeho hlavním účelem je monitorování síťového provozu na základě IP toků, které poskytuje podrobný pohled do provozu na jejich síti v reálném čase. Aktuálně jsou nejrozšířenější verze tohoto protokolu: 5, 9, 10 a standard RFC3954.
Normalizace/Normalizati on	Proces, kdy přicházející „RAW“ logy rozdělíme do databázové věty. Cílem procesu normalizace je jednotné zacházení s původně nestrukturovanými vstupními informacemi.
Offense	Přestupek proti pravidlům generovaný bezpečnostní politikou QRadar. Offense jsou sdruženy na samostatné záložce v grafickém prostředí Konzole QRadaru.
OPSEC/LEA	Typ API společnosti Check Point pro načítání logovacích událostí.
Parser/DSM Parser	Předpis ve formátu XML definující regulárními výrazy význam dat logovacích událostí a flow.
QDI	QRadar Deployment Intelligence – modul monitoringu systému QRadar.
QFLow	Jedná se o proprietární modifikaci NetFlow protokolu od společnosti IBM. Zdrojem QFlow je QRadar sonda. Rozšíření protokolu spočívají v uložení informací až ze sedmé vrstvy ISO/OSI modelu pro přesnější bezpečnostní analýzu QRadar SIEM.
Referenční Data/Reference Set	Logický kontejner obsahující data využitelná v pravidlech v systému IBM Security QRadar.
Reporting	Je systém podnikového vykazování ve formě tabulek a grafů za určité období.

Pull metoda	Způsob načítání dat, kdy je komunikace iniciována na straně systému SIEM.
Push metoda	Způsob načítání dat, kdy systém SIEM neiniciuje komunikaci, ale pouze data přijímá na definovaném portu.
SDEE	Security Device Event Exchange – standard pro načítání logovacích událostí společností Cisco.
Severity	Dílčí závažnost logované události/offense.
SIEM	Security Information and Event Management je software pro agregaci a zpracování informací a událostí souvisejících s bezpečností.
SFlow	NetFlow protokol poskytující samplované (vzorkované, příležitostné) informace o aktuálních Flow. Centrální síťové prvky poskytují z důvodu výkonu informace o síťových tocích právě tímto samplovaným Flow protokolem (verze 5 z 7/2004).
SMB	Server Message Block (SMB), známý také jako Common Internet File System (CIFS), je síťový komunikační protokol aplikační vrstvy, který slouží ke sdílenému přístupu k souborům, tiskárnám, sériovým portům a další komunikaci mezi uzly na síti. Poskytuje také autentizovaný mechanismus pro meziprocesorovou komunikaci. Je využíván hlavně na počítačích s operačními systémy rodiny Windows.
SNMP	Simple Network Management Protocol (SNMP) je součástí sady internetových protokolů. Standardně využívá port 161. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítě, a jejich následné vyhodnocování. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě.
SSH	SSH (Secure Shell) je v informatice označení pro program a zároveň pro zabezpečený komunikační protokol v počítačových sítích, které používají TCP/IP. SSH byl navržen jako náhrada za telnet a další nezabezpečené vzdálené shelly (rlogin, rsh apod.), které posílají heslo v nezabezpečené formě a umožňují tak jeho odposlechnutí při přenosu pomocí počítačové sítě [1]. Šifrování přenášených dat, které SSH poskytuje, slouží k zabezpečení dat při přenosu přes nedůvěryhodnou síť, jako je například Internet.
Syslog	Syslog je standard pro záznam programových zpráv na platformě UNIX/LINUX a v prostředí aktivních síťových prvků. Protokol umožňuje oddělit software generující zprávy od systému, který je ukládá a softwaru, jenž poskytuje reporty a analýzy. Syslog může sloužit v rámci systémovému managementu a bezpečnostnímu auditu jako zdroj informací pro analýzu anebo ladění systému. Díky těmto vlastnostem může syslog sloužit pro integraci logovaných dat mnoha různých systémů.
SZS	Systém základní služby

WinCollect	Technologie systému IBM Security QRadar pro sběr bezpečnostních událostí z event logů operačního systému Microsoft Windows.
WMI	Typ API společnosti Microsoft pro operační sytém Windows (Windows Management Instrumentation).
Zdroj	Zdroj logovacích událostí nebo záznamů síťových toků flow.
Zranitelnost/Vulnerability	Security vulnerability, je úmyslná chyba nebo neúmyslný nedostatek či závada v software obecně nebo ve firmware zařízení komunikační infrastruktury, která může být zneužita potenciálním útočníkem pro škodlivou činnost. Tyto zranitelnosti jsou buď známé a publikované, ale výrobcem ještě neošetřené nebo skryté a neobjevené.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM UKÁZEK KÓDU

PŘÍLOHA P I: NÁZEV PŘÍLOHY

[1] BP-All.zip0020