Bezpečnostní monitoring uživatelů v informačních systémech

Petr Liška

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Petr Liška**
Osobní číslo:	**A18190**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnostní monitoring uživatelů v informačních systémech**
Téma práce anglicky:	**The Security Monitoring of Users in Information Systems**

Zásady pro vypracování

1. Popište základní koncept informační bezpečnosti ve společnosti.
2. Zhodnoťte možný přínos sběru a vyhodnocování logů pro zvýšení informační bezpečnosti ve společnosti.
3. Stanovte předpoklady pro nasazení nástrojů pro sběr a vyhodnocování logů, detekování a vyhodnocování anomálií chování uživatelů.
4. Vytvořte plán nasazení konkrétních nástrojů.
5. Vytvořte korelační pravidla pro detekování závadného chování uživatelů.

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

Seznam doporučené literatury:

1. BOLLINGER, Jeff, Brandon ENRIGHT a Matthew VALITES. *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan*. Sebastopol: O'Reilly Media, 2015. ISBN 978-1-491-94940-5
2. DRASTICH, Martin. *Systém managementu bezpečnosti informací*. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9
3. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8
4. MURDOCH, Don. *Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases Notes from the Field (V1.02): A condensed field guide for the Security Operations team*. CreateSpace Independent Publishing, 2019. ISBN 978-1091493896
5. MILLER, David, Shon HARRIS, Allen HARPER, Stephen VANDYKE a Chris BLASK. *Security information and event management (SIEM) implementation*. New York: McGraw-Hill, c2011. ISBN 978-0-07-170109-9

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

Datum zadání bakalářské práce: **15. ledna 2021**
Termín odevzdání bakalářské práce: **19. května 2021**

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

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

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.

V Brně, dne 8. 5. 2021

Petr Liška v.r.
podpis studenta

ABSTRAKT

Tato práce se zabývá nasazením systému pro sběr a vyhodnocování logů z informačních systémů, doplněným systémem pro detekování a vyhodnocování anomálií chování uživatelů. Teoretická část práce se zaměřuje na seznámení s problematikou bezpečnostního monitoringu uživatelů, s technickými prostředky pro zajištění detekce událostí v informačních systémech, srovnáním jejich možností a posouzením jejich využití v rámci řízení informační bezpečnosti ve firmě. Práce dále detailněji popisuje jednotlivé částí systému pro sběr a vyhodnocování logů. Hlavním cílem práce je vytvoření postupu nasazení nástroje IBM QRadar Security Information and Event Management a jeho součástí, včetně rozšíření User Behavior Analytics, čemuž je věnována její praktická část. Tato část rovněž představuje praktické příklady korelačních pravidel pro různé případy užití.

Klíčová slova: SIEM, QRadar, UBA, sběr logů, vyhodnocování událostí, bezpečnostní monitoring, analýza chování, korelace

ABSTRACT

This thesis deals with the deployment of a system for collecting and evaluating logs from information systems, supplemented by a system for detecting and evaluating user behaviour anomalies. The theoretical part of the thesis focuses on introducing the security monitoring of users, with technical means for ensuring the detection of events in information systems, comparing their capabilities and assessing their use in information security management in the company. The thesis also describes in detail the individual parts of the system for collecting and evaluating logs. The main objective of the thesis is to create a procedure for deploying the IBM QRadar Security Information and Event Management tool and its components, including the User Behavior Analytics extension, to which the practical part of the thesis is devoted. This part also presents practical examples of correlation rules for different use cases.

Keywords: SIEM, QRadar, UBA, log collection, event evaluation, security monitoring, behavioural analysis, correlation

Rád bych poděkoval za cenné rady a podněty vedoucímu mé bakalářské práce prof. Mgr. Romanu Jaškovi, Ph.D., DBA, dále mému kolegovi Ing. Jiřímu Malečkovi za přínosné odborné připomínky a v neposlední řadě mé rodině za trpělivost a podporu při studiu.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Vlivem rychlého rozvoje informačních technologií, zvyšování výpočetního výkonu a dostupnosti připojení k internetu, se stále více pracovních i všedních činností člověka odehrává v kybernetickém prostoru. Tento fakt ještě umocnil sociální distanc obyvatel způsobený pandemií koronaviru SARS-CoV-2 z jara roku 2020, kdy došlo k urychlení „elektronizace“ dalších lidských činností a oblastí života (školství, státní správa, maloobchod…). Tomuto trendu se velice rychle přizpůsobily i pachatelé kriminálních činů. Počet a závažnost kybernetických hrozeb se zvyšuje a obrana proti nim v mnoha případech zaostává.

Pro podniky a organizace všeho druhu a velikosti (společnost) je tak v současnosti zcela zásadní osvojit si schopnost obrany proti kybernetickým hrozbám a zabránit úniku citlivých informací, ztrátě dat či dokonce zastavení své činnosti. Je potřeba si uvědomit, že bezpečnostní hrozby nepůsobí na společnost pouze zvenčí, ale i z řad vlastních zaměstnanců a tomu přizpůsobit strategii budování informační bezpečnosti. K dosažení uspokojivé úrovně ochrany informačních aktiv společnosti je nutné vyvinout nemalé úsilí a přijmout řadu organizačních, procesních a technických opatření.

Jedním z významných technických opatření je využití systému pro sběr a vyhodnocování logů z informačních systémů (IS). Správným nasazením vhodného nástroje a jeho efektivním používáním, získá společnost mocný prostředek pro sledování událostí v jeho informačních systémech a přehled o tom, jak je zacházeno s jeho informačními aktivy. Takovým nástrojem je Security Information and Event Management system (SIEM).

Cílem této práce je poskytnout ucelený postup pro nasazení konkrétního nástroje SIEM a tvorbu korelačních pravidel pro účely bezpečnostního monitoringu uživatelů. Nezbytným předpokladem pro dosažení tohoto cíle je uvést čtenáře do problematiky informační bezpečnosti, seznámit jej s vhodnými technickými prostředky pro monitoring událostí a chování uživatelů v informačních systémech.

Moji motivací pro výběr daného tématu je skutečnost, že se jako specialista IT bezpečnosti touto problematikou zabývám již řadu let, a to v komerčních společnostech střední velikosti, v oborech finančnictví a pojišťovnictví. Mohu tedy v této práci uplatnit své znalosti a praktické zkušenosti. Výsledná práce tak může být přínosem pro osoby odpovědné za informační bezpečnost ve společnostech, kde zvažují pořízení a nasazení nástroje SIEM.

V praktické části práce jsou, se svolením manažera IT bezpečnosti, použity anonymizované a upravené snímky obrazovky z nástroje IBM QRadar SIEM a jeho rozšíření, za jejichž správu jsem ve společnosti spoluzodpovědný.

Z důvodu lepšího praktického uplatnění informací obsažených v této práci, je často v závorkách uváděn zažitý nebo přejatý anglický výraz použitého termínu nebo jeho zkratka.

I. TEORETICKÁ ČÁST

1 STRUČNÝ ÚVOD DO INFORMAČNÍ BEZPEČNOSTI

Informační bezpečnost je pojem, který je v dnešní době stále více skloňován, ale mnoho lidí jej nedokáže dostatečně definovat. Zjednodušeně se dá říct, že základním úkolem informační bezpečnosti je ochrana informace. Ta může být přítomna ve fyzické či virtuální podobě, nezáleží na jakém nosiči je uchována. Úvodní kapitola práce seznamuje se základy informační bezpečnosti a vysvětluje její význam z několika pohledů.

1.1 Základní pojmy informační bezpečnosti

- **informace**: podle jedné z definic to *„jsou údaje, které byly zpracovány do podoby užitečné pro příjemce“* [1],
- **informační bezpečnost**: můžeme vyjádřit jako *„Vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám.“* [2],
- **aktivum**: vše, co má pro společnost jakoukoliv hodnotu a co je třeba chránit. V informační bezpečnosti se pak jedná o prvek informačního systému (hardwarové komponenty, datové struktury, data, obslužný personál atd.),
- **hrozba**: událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti aktiva,
- **zranitelnost**: slabina aktiva, která může být zneužita hrozbou.

1.2 Základní pilíře ochrany informací

Základní princip ochrany informací, který je také nazýván „CIA triad“, stojí na třech pilířích. Informační bezpečnost má za úkol zajistit důvěrnost (Confidentality), integritu (Integrity) a dostupnost (Availability) informačních aktiv (Obr. 1):

- **důvěrnost**: je nutné chránit aktiva proti neautorizovanému vyzrazení. Tzn. potřebu zajistit, aby informace byla přístupná pouze tomu, komu bylo uděleno oprávnění k ní přistupovat.
- **integrita**: je nutné chránit aktiva před neautorizovanou nebo náhodnou modifikací. Tzn. potřebu znemožnit neoprávněnou manipulaci s informací a zajistit její správnost a úplnost,
- **dostupnost**: je třeba zajistit aby informace byla vždy dostupná pro uživatele ve chvíli, kdy ji potřebuje. [3]

Obrázek 1 Pilíře informační bezpečnosti [4]

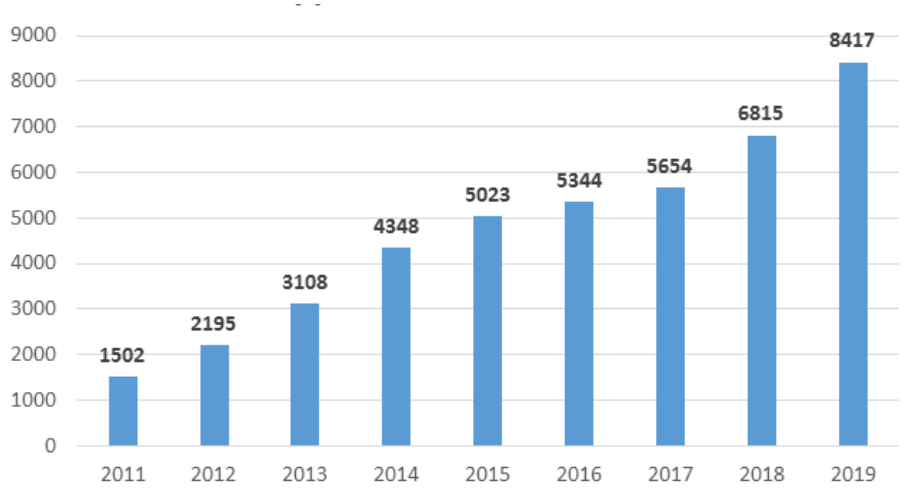
1.3 Kybernetická bezpečnost

Pojem kybernetická bezpečnost není pevně stanoven. Jedná o podmnožinu bezpečnosti, která má podobný cíl a principy k zajištění ochrany, jako informační bezpečnost. Informační bezpečnost vyjadřuje vztah k ochraně informací obecně. Kybernetická bezpečnost je však více zaměřena na ochranu informačních a komunikačních technologií (ICT), aplikací, dat uživatelů a jejich schopnost odolávat kybernetickým hrozbám. [5]

1.3.1 Stav kybernetické bezpečnosti v ČR

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) ve své zprávě o stavu kybernetické bezpečnosti v ČR za rok 2019 uvádí skutečnost, že každým rokem stoupá počet kybernetických útoků a roste i jejich závažnost. [6]

Dle policejních statistik (Obr. 2) je možné sledovat setrvalý růst kriminálních činů spáchaných v kyberprostoru. V roce 2019 to bylo celkem 8 417 trestných činů, což je přibližně 23,5% meziroční nárůst. [7]



Obrázek 2 Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu 2011–2019 [7]

1.4 Legislativa

Informační bezpečnost je významná ve vztahu k mnoha činnostem celé společnosti, jež upravují právní předpisy. Příkladem může být ochrana soukromí, kterou se zabývá Listina základních práv a svobod (články 7, 10, 13) [8], trestní zákoník (§180-183) [9], občanský zákoník (§84-90) [10], nařízení Evropského parlamentu a Rady (EU) 2016/679 GDPR (zkráceně) [11] a další. Nejčastěji zmiňovanými zákony či nařízeními v souvislosti s informační / kybernetickou bezpečností jsou:

181/2014 sb. Zákon o kybernetické bezpečnosti: cílem zákona je stanovit potřebnou úroveň ochrany kritické informační infrastruktury a významných informačních systémů tak, aby byla nedošlo k ohrožení zájmů České republiky. Cílem je také zlepšení detekce kybernetických bezpečnostních incidentů, zavedení jejich hlášení a vytvoření systému pro jejich zvládání. Související prováděcí předpis 82/2018 Sb. pak doplňuje konkrétní opatření vycházející z ISMS a další potřebné náležitosti, [12] [13]

(EU) 2016/679 GDPR: je obecné nařízení Evropského parlamentu a Rady EU o ochraně osobních údajů. Má za cíl zamezit neoprávněnému zacházení s daty občanů EU, zajistit aby nebylo nakládáno s osobními údaji občanů bez jejich vědomí a způsobem, s kterým předem nesouhlasí. Pro případ porušení nařízení jsou stanoveny vysoké sankce. Nařízení také stanoví nové povinnosti pro společnosti určitého typu nebo velikosti, které nakládají s osobními údaji, jako je jmenování pověřence pro ochranu osobních údajů (DPO) nebo vypracování posouzení vlivu na ochranu osobních údajů (DPIA). [14]

Vydáním nařízení (EU) 2016/679 GDPR a jeho adaptačního zákona 110/2019 sb. byl zrušen do té doby platný zákon 101/2000 sb. o ochraně osobních údajů,

ePrivacy Regulation: je připravované nařízení EU o soukromí a elektronických komunikacích, které bude doplňovat GDPR. Na rozdíl od GDPR, které je obecným nařízením, ePrivacy bude zaměřené konkrétněji na ochranu soukromí v elektronických komunikacích, vč. služeb typu Skype, WhatsApp nebo volání přes internet (VoIP). Chráněný bude nejen přenášený obsah, ale i jeho metadata. Ačkoliv mělo ePrivacy původně vejít v platnost současně s GDPR, je stále pouze ve formě návrhu a jeho přijetí je stále odkládáno. [15]

Dílčí závěr: ochrana před kybernetickými hrozbami získává každým rokem na významu a je třeba se jí věnovat na všech úrovních. Od jednotlivců – uživatelů ICT, v zájmu ochrany soukromí, až po státní institute, v rámci ochrany národní bezpečnosti. K naplnění ochrany informační bezpečnosti přispívá také legislativa České republiky a Evropské unie.

2 ZÁKLADNÍ KONCEPT INFORMAČNÍ BEZPEČNOSTI

Každá společnost, využívající informační technologie, potřebuje pro zachování své činnosti implementovat opatření k zajištění informační bezpečnosti. Velikost a typ společnosti bude mít vliv pouze na to, jaké úsilí a kolik prostředků bude potřeba vynaložit pro přijetí efektivních opatření. Společnost si pro dosažení požadovaného cíle musí vytvořit vlastní koncept informační bezpečnosti nebo implementovat již existující. Jedním z prověřených způsobů je implementace systému řízení a bezpečnostní politiky informací dle ISMS.

2.1 Systém řízení bezpečnosti informací

ISO/IEC 27001 – Information Security Management Systems (ISMS), který se do češtiny překládá jako Systém řízení bezpečnosti informací, je celosvětově uznávaný standard pro řízení bezpečnosti v informačních technologiích. ISO/IEC 27001 je součástí souboru norem ISO/IEC 27000, z nichž základními jsou:

- ISO/IEC 27000 - Přehled a slovník,
- ISO/IEC 27001 - Požadavky na ISMS,
- ISO/IEC 27002 - Soubor postupů pro opatření bezpečnosti informací,
- ISO/IEC 27003 - Pokyny,
- ISO/IEC 27004 - Monitorování, měření, analýza a hodnocení,
- ISO/IEC 27005 - Řízení rizik bezpečnosti informací. [16]

ISO/IEC 27xxx čítá celkem padesát norem zabývajících se bezpečnostními technikami v informačních technologiích.

Při zavádění systému řízení bezpečnosti informací jsou stěžejní: **ISO/IEC 27001**, který stanovuje soubor opatření vedoucích k zajištění informační bezpečnosti a **ISO/IEC 27002**, obsahující postupy pro řízení informační bezpečnosti, vycházející ze zkušeností.

Cílem pro zavedení řízení bezpečnosti informací nemusí být nutně příprava na certifikaci organizace dle této normy, ale poslouží jako velmi dobrý návod pro implementaci všech potřebných opatření v rámci budování informační bezpečnosti ve společnosti.

2.2 Bezpečnostní politika informací

Na počátku realizace informační bezpečnosti ve společnosti je ustanovení bezpečnostní politiky informací (BPI). Jednoduchou definici BPI nabízí vyhláška č. 82/2018 Sb., § 2 písm.

c) (zkráceně vyhláška o kybernetické bezpečnosti) – bezpečnostní politikou se rozumí *„soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv“* [13].

Pro vytvoření BPI se nabízí využití normy ISO/IEC 27002, která pro tento účel poskytuje seznam ověřených postupů. Jednotlivá doporučení, kterých je 114 rozděluje do 14 oblastí (Obr. 3). [17]

Obrázek 3 Oblasti bezpečnosti informací, upraveno z: [17]

BPI krom samotných opatření stanovuje také účel, pro který byla politika vytvořena, jakých cílů má být dosaženo a jakými prostředky:

- **účel**: BPI stanovuje základní rámec systému řízení bezpečnosti informací, vymezuje základní pravomoci, odpovědnosti a definuje zásady systému řízení bezpečnosti informací společnosti,
- **cíl**: cílem bezpečnosti informací je zajistit jejich důvěrnost, integritu a dostupnost,
- **strategie**: základem prosazení bezpečnosti informací je realizace a prosazení systému řízení informací ve všech oblastech bezpečnosti, jak je popsáno dále,
- **odpovědnost**: jsou stanoveny odpovědnosti za bezpečnost informací. Vedení společnosti musí vyjadřovat vůli a podporu při prosazování informační bezpečnosti, vč. zajištění personálních zdrojů a rozpočtových prostředků. Vedení společnosti

deleguje odpovědnosti na jednotlivé role, jako je manažer IT bezpečnosti, bezpečnostní výbor a stanovuje práva a povinnosti pro zaměstnance.

2.2.1 Oblasti bezpečnostní politiky informací a jejich cíle

Následující výčet oblastí s jejich cíli a příklady opatření vychází z ISMS, je však upraven dle vlastních praktických zkušenosti při zavádění informační bezpečnosti ve společnosti, vytváření BPI a navazující předpisové základny:

- **řízení aktiv**: cílem je nastavit a udržovat přiměřenou ochranu aktiv a zajistit odpovídající úroveň ochrany informací společnosti. Příkladem opatření je zavedení evidence aktiv nebo klasifikace informací,
- **hodnocení rizik**: cílem je zajištění bezpečnostních opatření pro klíčové procesy ve společnosti na základě opatření vzešlých z analýzy rizik. Analýza rizik je jednou z nejdůležitějších fází řízení rizik. Měla by odpovědět na otázku, jaké hrozby působí na společnost, jak jsou aktiva působením hrozeb zranitelná, jaká je pravděpodobnost, že bude některá hrozba vůči aktivu naplněna a jaký by to mohlo mít dopad na společnost,
- **organizace bezpečnosti informací**: cílem je zajištění řízení bezpečnosti informací ve společnosti pro interní zaměstnance a externí subjekty. Tzn. například zavedení předpisové základny, implementace bezpečnosti informací nebo stanovení podmínek přístupu pro externí subjekty,
- **bezpečnost lidských zdrojů**: cílem je zajistit aby všichni zaměstnanci i smluvní strany byly seznámeni se svými povinnostmi a odpovědnostmi, byli si vědomi bezpečnostních hrozeb a byli připravení se podílet na dodržování BPI tak, aby bylo sníženo riziko lidské chyby, krádeže, podvodu či zneužití prostředků společnosti. To lze dosáhnou např. stanovením odpovědností zaměstnanců nebo školením v oblasti informační bezpečnosti,
- **fyzická bezpečnost a bezpečnost prostředí**: cílem je zabezpečit fyzickou ochranu prostor, zamezit neautorizovanému fyzickému přístupu do vymezených oblastí a předcházet tak poškození, krádeži, kompromitaci aktiv společnosti a zamezení přerušení její činnosti. Požadovaného cíle dosáhneme zavedením fyzické bezpečnosti v rámci režimových opatření, kontroly vstupu, či fyzickou ochranu kritických aktiv společnosti,

- **řízení přístupu**: cílem je řídit oprávněný přístup k informacím, předcházet neoprávněnému přístupu, vyzrazení nebo krádeži informací, neautorizovanému přístupu k prostředkům pro zpracování informací, síťovým prostředkům a operačním systémům aby nedocházelo ke snižování bezpečnosti. V této oblasti je třeba implementovat mnohá opatření, zejména taková, která zajísti soulad s principy řízení oprávnění. Např. princip nejnižších oprávnění, neslučitelnosti rolí, nesdílených přístupů, schvalování oprávnění, vícefaktorové autentizace atd.,
- **řízení komunikací a řízení provozu**: cílem je zajistit správný a bezpečný provoz informačních systémů a infrastruktury, minimalizovat riziko jejich selhání, zajistit důvěrnost, dostupnost a integritu informací a zjistit úroveň dodávaných služeb. Opatřeními jsou např. zavedení provozních postupů, ochrana proti škodlivým kódům, strategie zálohování nebo monitoring bezpečnostních a provozních událostí v počítačové síti,
- **akvizice, vývoj a údržba informačních systémů**: cílem je zajistit bezpečnost nově pořizovaných informačních systémů, vývoje a údržby programového vybavení, ochránit důvěrnost, autentičnost a integritu informací s pomocí kryptografických prostředků a snižovat riziko hrozeb plynoucích ze zveřejněných technických zranitelností. K dosažení cíle je třeba implementovat např. postupy pro řízení změn (change management), zavedení řízení technických zranitelností (vulnerability management), prioritizování a zvládání rizik (patch management), či zavedení kryptografických opatření,
- **řízení kontinuity činností**: cílem je zajistit nepřetržitý provozní chod společnosti v případě katastrofy nebo vlivem vážného selhání informačních systémů, zajistit ochranu kritických procesů a neprodlené obnovení všech činností. Pro dosažení cíle je nutné vytvořit plán kontinuity činností (Business Continuity Plan),
- **zvládání bezpečnostních incidentů**: cílem je zajistit včasné hlášení bezpečnostních událostí, incidentů, zjištěných slabin informačních systémů a adekvátní reakci vedoucí ke zjištění příčiny a provedení nápravy bránící jejich opakování. Opatřením je zavedení procesu pro hlášení, zaznamenávání, šetření událostí a incidentů, s následnou implementací nápravných opatření (incident management),
- **soulad opatření s regulatorními a legislativními požadavky**: cílem je vyvarovat se porušení zákonných nebo smluvních norem a povinností, regulatorních

požadavků, občanského a trestního práva. Je třeba implementovat taková opatření, která zajistí soulad se všemi právními a jinými předpisy.

Dílčí závěr: bezpečnostní politika informací přizpůsobená podmínkám společnosti, pro kterou je tvořena, je vhodným prostředkem pro naplnění koncepce informační bezpečnosti. Zajištění principů informační bezpečnosti, tedy důvěrnosti, integrity a dostupnosti, nemusí být nezbytně podmíněno certifikací dle normy ISO 27001.

3 BEZPEČNOSTNÍ MONITORING UŽIVATELŮ

Od roku 2018 vzrostl počet incidentů zapříčiněných uvnitř společnosti o 47 %, jak dokládá průzkum společnosti The Ponemon Institute z roku 2020. Nejčastější hrozbou nebyl malware, jak by se dalo předpokládat, ale nedbalý zaměstnanec nebo kontraktor (Obr. 4). [18]

Obrázek 4 Nejčastější příčiny incidentů uvnitř společnosti, upraveno z: [18]

To dokládá oprávněnost potřeby bezpečnostního monitoringu uživatelů v informačních systémech. Osvědčeným postupem k zajištění sledování a vyhodnocování aktivit uživatele je získávání záznamů o událostech z IS.

Často se lze setkat s případy, kdy jsou hromaděny záznamy událostí všech systémů a aplikací, které to umožňují. A to pro případ jejich budoucí potřeby, pro vyšetřování možných incidentů. Dopředu ale nikdy nevíme, které záznamy budou pro vyšetřování užitečné. Neadekvátní množství záznamů ztěžuje investigaci a odvádí pozornost specialisty IT bezpečnosti od nalezení podstatného. Také záznamy, které neobsahují žádný relevantní bezpečnostní obsah pouze zabírají diskové úložiště a zbytečně zvyšují výpočetní výkony systémů, které s nimi pracují. [19]

Následující odstavce kapitoly odpovídají na otázku, jaké záznamy událostí jsou pro bezpečnostní monitoring užitečné a měly by být sbírány. Jejich sběr a vyhodnocování zároveň poskytne potřebnou kontrolu nad naplňováním stanovené BPI, viz kapitola *2.2.1 Oblasti bezpečnostní politiky informací a jejich cíle*.

3.1 Uživatelé

Bezpečnostní monitoring je zaměřen z větší části na aktivity uživatelů, ať už zaměstnanců společnosti nebo osob zvenčí. Při prevenci nebo šetření incidentu můžou mít události o aktivitě uživatele různý kontext. Uživatel může být obětí útoku, může být jeho původce nebo může sloužit i jako nevědomý prostředník. Příčina události vedoucí k incidentu může být úmyslná nebo se může jednat o chybu. První část sběru záznamů je zaměřena přímo na události o uživateli.

3.1.1 Ověření identity

Prvním předpokladem pro úspěšný monitoring uživatelů a případné šetření incidentů, je znát identitu původce zaznamenané události a průběh jeho ověření. Systémy pro ověření identity (autentizace) a přístupu (autorizace), jejichž záznamy je nezbytné získávat jsou např:

- **Active Directory** (AD): adresářová služba integrovaná s řadičem domény od výrobce Microsoft, implementující Lightweight Directory Access Protocol (LDAP),
- **OpenLDAP**: volně šiřitelná implementace protokolu LDAP pro operační systémy různých výrobců,
- **Remote Authentication Dial In User Service** (RADUIS): AAA (authentication, authorization, accounting) protokol využívaný pro ověření uživatele v síti,
- **systémy pro vícefaktorové ověření** (MFA): k ověření uživatele je použito více způsobů ověření v jednom sledu. Např. jméno a heslo + jednorázový kód zaslaný na zařízení uživatele.

3.1.2 Řízení přístupu

Přístupy uživatelů do systému by měly být řízeny na základě přidělených rolí – role-based access control (RBAC). Přidělení rolí uživatelům lze provést ručně, např. na základě požadavku zaslaného IT podpoře, lepším způsobem je pak využití systému pro správu identit (IDM). Hlavním úkolem IDM je automatizovat následující procesy:

- správa identity uživatele,
- žádost uživatelů o přidělení rolí,
- schválení žádostí odpovědnou osobou, případě více osobami,
- přidělení a rolí uživatelům na základě schválené žádosti a jejich evidenci,
- aplikování členství na základě rolí v napojených systémech,
- odebírání rolí při ukončení pracovního vztahu,

- kontrolu přidělených rolí,
- auditování celého procesu.

3.1.3 Koncové stanice

Koncové stanice uživatele mohou být fyzické (pracovní stanice, notebook…) nebo virtuální (virtuální desktop / stanice). Bez ohledu na formu je potřeba aby měl správce o stanici kompletní přehled. K tomu slouží různé centrálně spravované nástroje, jejichž klientská část je instalovaná na koncové stanici, a které zároveň poskytují hodnotné záznamy událostí:

- **antivirový software** (AV),
- **management zranitelností** (vulnerability management): nástroj pro zjišťování zranitelností operačního systému (OS) a instalovaného software (SW),
- **management oprav** (patch management): nástroj pro nápravu zjištěných zranitelností OS a SW,
- **systémový management** (systems management): nástroj pro inventarizaci hardware (HW) i SW na stanici a pro jeho správu.

3.1.4 Klasifikace a ochrana informací

Je nezbytné sbírat záznamy nejen o uživateli a jeho stanici, ale i o celém toku informací, se kterými uživatel pracuje. K tomu slouží nástroje pro klasifikaci informací a jejich ochranu:

- **klasifikace informací**: abychom mohli sledovat tok informací, musíme ji nejprve označit příslušným stupněm ochrany. Klasifikační stupně a způsob, jak s informacemi určitého klasifikačního stupně může být zacházeno, si určuje každá organizace dle potřeby. Zpravidla to bývají klasifikace informací typu: veřejné, interní, chráněné a přísně chráněné. Klasifikaci provádí uživatel ručně, nebo je prováděna automaticky nástrojem na základě definovaných pravidel,
- **ochrana informací**: o ochranu klasifikovaných informací se stará systém prevence ztráty dat (DLP). Tento systém kontroluje na více úrovních (na stanici, v síti, na sdíleném úložišti, na rozhraní sítě…) zacházení se soubory, které jsou označeny některým z klasifikačních stupňů. Nedovolí např. odeslání dokumentu označeného „interní“ do veřejné internetové služby nebo otevřít přísně chráněný dokument uživateli, kterému nebyl přímo určen.

3.1.5 Analýza chování

Všechny aktivity uživatele, zaznamenané jednotlivými systémy, vytváří celkový pohled na jeho chování. Nástroje pro analýzu chování uživatele (UBA) dokáží v záznamech vyhledávat významné události, vzájemně je korelovat a za pomoci strojového učení vytvářet profil chování každého uživatele v síti. Pakliže nástroj zaznamená v chování uživatele odchylku oproti naučenému vzoru, upozorní na to zvýšením jeho rizikového skóre. UBA je na jednu stranu konzumentem záznamů z jednotlivých systémů, na straně druhé generuje další nové, vysoce hodnotné záznamy na základě provedených analýz. O nástroji UBA dále pojednávají kapitoly v praktické části práce.

3.2 Infrastruktura

Uživatelé a jejich koncově stanice jsou součástí podnikové informační a komunikační infrastruktury. Pro výměnu a ukládání dat využívají řadu síťových prostředků a serverů, které o této činnosti poskytují důležité auditní záznamy. Neméně důležité je sbírat záznamy o událostech, které vznikly vlivem správy těchto prostředků administrátory.

3.2.1 Servery a datová úložiště

Servery zajišťují řadu procesů, které jsou pro fungování společnosti kriticky důležité. Je nutností mít k dispozici veškeré záznamy o událostech, které vznikají při přístupu k OS serveru a jeho konfiguraci. Další důležité záznamy poskytují databázové servery, virtualizační platformy, datová úložiště, zálohovací nástroje a další SW využívající výpočetního výkonu serverů.

3.2.2 Sítě a síťové služby

Dalšími kritickými systémy z pohledu chodu společnosti a sběru auditních záznamů jsou veškeré síťové prvky a služby. Každé provedené nastavení na switchi, routeru či firewallu může mít vliv na bezpečnost dat, které sítí procházejí. Proto o veškerých konfiguračních změnách musí existovat podrobný záznam. Ze síťového provozu a auditních záznamů síťových prvků a služeb, můžeme také získat velice důležité informace o aktivitách uživatelů:

- **switche a přístupové body bezdrátové sítě**: autentizace a připojení uživatelů k síti, množství přenesených dat, pokusy o neoprávněný přístup k síti, podezřelé síťové aktivity,

- **firewall**: komunikace uživatelů do externích sítí a internetu, případně mezi jednotlivými interními sítěmi. Komunikace z internetu do vnitřní sítě, objemy přenesených dat, informace o zdrojích a cílech komunikace a mnoho dalšího. V případě, že je firewall vybaven pokročilými funkcemi pro monitorování a vyhodnocování síťového provozu (UTM funkce), poskytují nám jeho záznamy také cenné informace, například o možných síťových útocích, závadné komunikaci uživatelů na podezřelé nebo zakázané webové stránky v internetu, používání nepovolených aplikací, pokusech o průnik malware na koncové stanice a servery atd.,
- **základní síťové služby DNS a DHCP**: tyto základní síťové služby (protokoly) poskytuje systém pro převod doménových jmen na IP adresy (DNS) a systém pro přidělování IP adres zařízením v síti (DHCP). Ať už jsou tyto systémy implementovány na serveru nebo aktivním síťovém prvku, poskytují velice důležité záznamy, které je potřeba sbírat,
- **virtuální privátní síť** (VPN): záznamy o vzdáleném připojení uživatelů do vnitřní sítě společnosti a o vzájemném propojení celých sítích v oddělených lokalitách.

3.3 Aplikace

Byznysové aplikace, aplikace řízení vztahu se zákazníky (CRM), aplikace pro řízení projektů, pro týmovou spolupráci, a mnohé další, obsahují cenná data společnosti, od strategických rozhodnutí až po osobní data klientů. Aplikace generují velké množství záznamů pro provozní účely, pro bezpečnostní monitoring uživatelů však nejsou jako celek vhodné. Oblasti zájmu pro bezpečnostní monitoring uživatelů v aplikacích jsou následující.

3.3.1 Řízení přístupu a správa

Z bezpečnostního pohledu je potřeba zaznamenávat události správce uživatelů (user management) aplikace. Jedná se o přístupové záznamy (udělení / odebrání přístupu, přihlášení, odhlášení uživatele) a záznamy o přidělení nebo odebrání rolí uživateli (získání oprávnění pro různé funkce aplikace nebo k určitým informacím).

3.3.2 Uživatelské operace

V případě, že aplikace umožňuje uživateli přístup k osobním údajům osob (klienti, zaměstnanci…) nebo k jiným pro společnost citlivým údajům, musí aplikace poskytovat přehled o tom, jak s takovými údaji bylo nakládáno. Zaznamenány musí být např. události

o přístupu k údajům, jejich procházení, tisku, exportu, úpravě, smazání atd. V případě osobních údajů tento požadavek vychází také z GDPR.

3.3.3 Aplikační programovatelné rozhraní

V předchozích odstavcích byl popsán přístup uživatelů k datům přes grafické rozhraní aplikace (GUI). Stejné požadavky na monitoring platí i pro ostatní způsoby přístupu. Jednou z často využívaných možnosti přístupu je aplikační programovatelné rozhraní (API).

3.4 Fyzická ochrana

Důležitou oblastí informační bezpečnosti je i fyzická ochrana. Elektronické bezpečnostní systémy poskytují záznamy, které lze efektivně korelovat se záznamy z informačních systémů nebo vzájemně mezi sebou:

přístupový systém (ACS): záznamy o přístupu osob do objektu, vymezených oblastí (technické místnosti, serverovny…), přítomnosti na pracovišti, průchodu a to včetně časů. Podezřelou událostí může být například přístup do IS z vnitřní sítě, zaznamenaný po odchodu zaměstnance z pracoviště,

dohledové videosystémy pro použití v bezpečnostních aplikacích (VSS): záznamy o detekci pohybu v obraze, přemístění sledovaného objektu, rozpoznání tváře, registrační značky automobilu, detekce sabotáže atd.,

poplachový zabezpečovací a tísňový systém (PZTS): jedná se především o záznamy o zastřežení / odstřežení, spuštění poplachu a pohybu osob v zónách,

sledování prostředí: záznamy, které neshromažďují události o činnosti uživatele, ale o ochraně jejich prostředí. Jmenovat můžeme elektrickou požární signalizaci, nebo pro ochranu kritických aktiv – klimatizaci serverovny.

Dílčí závěr: z uvedené statistiky je zřejmé, že monitoring chování uživatelů v informačních systémech je nezbytný. Získávání záznamů událostí o činnostech uživatelů, jak bylo popsáno, zajistí dostatek znalostí pro jejich vyhodnocování ve specializovaných nástrojích.

4 TECHNICKÉ PROSTŘEDKY

V předchozí kapitole byly vyjmenovány oblasti zájmu bezpečnostního monitoringu uživatelů. Události nebo stavy popsaných systémů a aplikací je potřeba centralizovaně shromažďovat, ukládat, vyhodnocovat, reportovat, zobrazovat či jinak zpracovávat. K tomu jsou určeny nástroje, jejichž funkci a zaměření popisují následující podkapitoly.

4.1 Nástroje pro sběr a vyhodnocování logů – SIEM

SIEM je zkratkou pro Security Information and Event Management. Účelem SIEM je:

- shromažďovat záznamy událostí z relevantních zdrojů (informační systémy, aplikace, prvky síťové infrastruktury), ukládat je do databáze, normalizovat jejich obsah, umožnit jejich prohledávání, analýzu a reporting = **log management**,
- vytváření vztahů mezi událostmi z jednoho nebo více systémů a dalšími okolnostmi nebo vlastnostmi prostředí = **korelace událostí**. Korelace přidávají k log managementu inteligenci v podobě pravidel, které umožňují vytvářet rozhodovací procesy pro správné vyhodnocování událostí,
- na základě funkcí log managementu a korelace událostí, SIEM v reálném čase reaguje a vytváří výstrahy, které jsou následně zpracovávány specialisty IT bezpečnosti = **aktivní odezva**. Výstrahy můžou mít různou formu, dle jejich kritičnosti. Mohou být zasílány okamžitě prostředky elektronické komunikace zodpovědným osobám, mohou být zobrazovány na „dashboard“ operačního střediska bezpečnosti (SOC) nebo např. vytvářet záznamy v incident managementu společnosti. [20]

4.1.1 Přínos SIEM pro společnost

Přínosy SIEM pro společnost jsou proaktivní a reaktivní vyhodnocování hrozeb a incidentů, vyhodnocování požadavků stanovených v BPI, sledování dodržování předpisů, zajištění zákonných a normativních požadavků. SIEM se podílí na bezpečnostním monitorování uživatelů a kontrole koncových stanic a infrastruktury. Umožňuje pracovníkům IT bezpečnosti realizovat a zefektivňovat jejich každodenní činnosti při zajišťování informační bezpečnosti ve společnosti. Možnosti SIEM lze dále rozšiřovat dle potřeb společnosti. Jeho rozhodovací schopnosti lze např. vylepšit umělou inteligencí na principu strojového učení nebo jej propojit s dalšími bezpečnostními nástroji. SIEM je přínosem také pro pracovníky provozního IT – administrátory, technickou podporu a další, kteří mohou těžit

z centralizovaného přístupu k logům všech stěžejních informačních systémů. Reportovací schopnosti SIEM lze dále využít pro potřebu všech oddělení společnosti.

4.1.2 Základy SIEM a pojmy

V další části práce se v souvislosti se SIEM setkáme s řadou pojmů, které je nezbytné vysvětlit:

log: v předchozích kapitolách práce byl používán ekvivalentní termín **záznam událostí**. Jedná se o informace, které systém (aplikace, zařízení…) generuje a které vypovídají o jeho činnosti. Log může mít různou formu podle zdroje, ze kterého je generován nebo podle jeho určení. Typickým logem pro potřeby informační bezpečnosti je auditní záznam (audit trail), který obsahuje informace potřebné pro analýzu bezpečnostních událostí. Transakční log obsahuje informace užitečné z bezpečnostního, ale i provozního hlediska. Jedná se o záznam všech operací (transakcí), např. při práci s databází. Existují další typy logů, které jsou svým obsahem a detailem vhodnější více pro pracovníky aplikační podpory nebo podpory provozních systémů (debug log, aplikační log…), [21]

událost (event): jedná se o konkrétní záznam logu, který má nějaký kontext, má pro nás vypovídající hodnotu a často nese s sebou i informaci o své důležitosti (kritický, varovný, informační atd.). Příklady události:

- uživatel byl přihlášen do systému,
- disková kvóta dosáhla prahové hodnoty,
- uživatelský účet byl uzamčen, [21]

výstraha (alert): pokud událost nebo jejich sled dosáhne předem definované úrovně nebo významu, je vyvolán poplach nebo je zaslána notifikace k okamžité reakci a zahájení investigace. Alert je indikátorem možného incidentu. Ne každý vyvolaný alert musí být nutně incidentem a naopak ne vždy může být incident označen alertem. Rozeznáváme tyto kategorie alertu:

- falešná pozitivita (false positive): parametry pravidla určující vznik alertu jsou nastavena tak, že mohou v určitých případech reagovat i na události generované legitimním provozem systému. V takovém případě se jedná o falešně pozitivní nález a pravidlo je nutné upravit,
- skutečná pozitivita: (true positive): v případě, že pravidlo pro vznik alertu je nastaveno správně a správně reaguje na události, jedná se o skutečnou pozitivitu,

tedy potvrzení incidentu. Čím je poměr skutečně pozitivních alertů k falešně negativním vyšší, tím lépe máme nastavený systém pro detekci. V ideálním případě by mělo být 100 % alertů skutečně pozitivních,

- falešná negativita (false negative): by neměla nikdy nastat. Jedná se o případ, kdy nastavené pravidlo neidentifikuje událost značící skutečný incident. Existující falešná negativita je selháním bezpečnostního systému. Falešná negativita může vzniknout např. laděním pravidla, které způsobuje vysoký počet falešně pozitivních alertů. Proto je potřeba každou úpravu pravidla řádně otestovat,
- skutečná negativita (true negative): pokud nevznikne žádný incident, nezareaguje žádné pravidlo a není vytvořen žádný alert. Jedná se o stav relativní bezpečnosti (buď jsou hrozby / zranitelnosti minimalizovány nebo nedochází ke zneužívání zranitelností hrozbami), [21]

incident: je událost nebo řada událostí, u které došlo k narušení nebo bezprostřední hrozbě narušení bezpečnosti informací nebo zásad zabezpečení ICT. S každým incidentem musí být zacházeno dle incident managementu, který společnost stanovila. Základem je, aby byl každý incident identifikován, zaznamenán, analyzován, klasifikován a aby bylo realizováno opatření s cílem minimalizovat dopady incidentu na informační bezpečnost a jeho budoucí opakování,

zdroj logů (logsource – LS): jedná se o systém, aplikaci nebo jiný prvek ICT, který generuje logy. V souvislosti s nástrojem SIEM se jedná o konfigurační záznam, který definuje zdroj, typ a formát přijímaných logů,

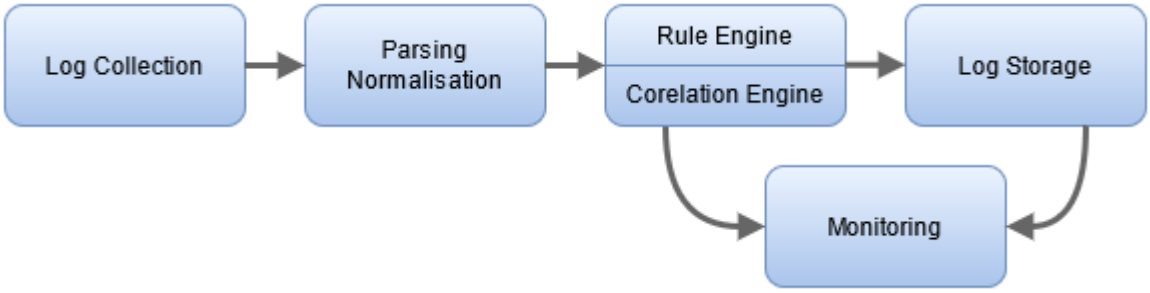
EPS: je zkratkou výrazu events per second, tedy počet událostí za vteřinu. Údaj o počtu EPS generovaných zdrojem logů je důležitý pro plánování kapacity a výkonu SIEM,

síťový tok (netflow, flow): v souvislosti se SIEM hovoříme především o zpracování událostí. Moderní nástroje SIEM umí přijímat a zpracovávat také flow a pracovat s nimi v rámci korelačních pravidel. Flow data jsou vytvářena síťovými zařízeními, jako jsou switche, firewally a routery. Poskytují informace o síťové komunikaci mezi dvěma koncovými body. Neobsahují obsah komunikace, ale pouze metadata (např. IP adresy zdroje a cíle, komunikační porty, trvání komunikace, počet přenesených packetů a bitů…). Výrobci implementují flow různým způsobem. Příkladem je NetFlow (Cisco), IPFIX (RFC 3954 na základě NetFlow) nebo sFlow (sFlow.org). [22]

FPS: je zkratkou pro flow per second. FPS je ekvivalentem k EPS, ale pro vyjádření množství síťových toků za vteřinu.

4.1.3 Architektura SIEM

Architektura SIEM vychází z jeho účelu, jak bylo popsáno v úvodu kapitoly *4.1 Nástroje pro sběr a vyhodnocování logů – SIEM* a jak je znázorněno ve funkčním schématu (Obr. 5).



Obrázek 5 Funkční schéma nástroje SIEM, upraveno z: [23]

Základní součásti nástroje SIEM jsou:

- **Log Collection**: modul zodpovědný za příjem logů z jejich zdroje. Specifika příjmu logů jsou podrobně popsána v kapitole *6. Technické předpoklady pro nasazení SIEM*,
- **Parsing Normalization**: logy přijaté z různých zdrojů mají rozličný formát a bez další úpravy nejsou pro SIEM použitelné. Normalizace logů, za využití syntaktické analýzy, přeformátuje původní log do podoby srozumitelné pro SIEM a tak, aby byl výsledný formát shodný pro všechny typy logů,
- **Rule Engine**: normalizované logy zpracovává rule engine, který jejich obsah porovnává s podmínkami určenými pravidly. Pokud testovací podmínky pravidla souhlasí s parametry logu, vytvoří se alert,
- **Correlation Engine**: umožňuje porovnávat standardní události z různých zdrojů a slučovat je do jedné korelované události. Jednotlivé události z různých zdrojů, analyzované samostatně, nemusí indikovat žádný problém. Jejich vzájemná korelace vytvoří nový kontext událostí, který může značit incident,
- **Log storage**: normalizované logy a korelované události jsou ukládány do databáze, což umožňuje jejich další efektivní využití,
- **Monitoring**: SIEM obsahuje grafické uživatelské rozhraní, umožňující obsluze pracovat s uloženými normalizovanými logy a poskytovanými informacemi.

Vyšetřování incidentů je tak centralizované do jednoho místa a není potřeba složitě prohledávat nezpracované logy v místě jejich vzniku. [24]

4.2 Nástroje pro analýzu síťového provozu

Informaci o tom, co se děje v systémech a aplikacích nám poskytují logy, jak bylo vysvětleno v předchozích kapitolách. Logy jsou generovány i aktivními síťovými prvky, poskytují však omezené informace o tom, co se děje v síti. K provádění analýzy síťového provozu, ať už z důvodu bezpečnostního nebo provozního monitoringu, potřebujeme specializované nástroje. Takové nástroje jsou vhodným a mnohdy nezbytným doplněním SIEM.

4.2.1 Možnosti analýzy síťového provozu

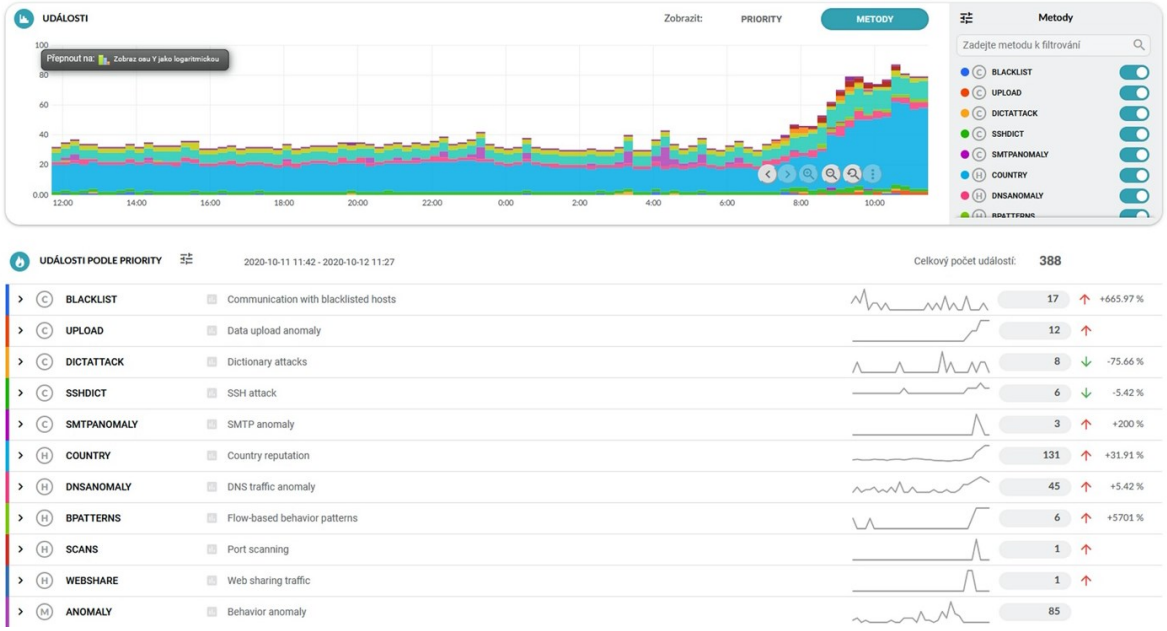
Záchyt packetů (packet capture): nejjednodušší možností, jak provádět analýzu síťového provozu, je použít nástroj pro záchyt packetů, který vytvoří kompletní obraz veškeré komunikace v síti. Vytvořený záznam lze zpětně procházet po jednotlivých packetech. Takovými nástroji jsou např. tcpdump pro Linuxové OS nebo Wireshark pro Windows a macOS. Tento způsob je velice neefektivní a má uplatnění pouze v rámci forenzní analýzy síťového problému.

Systémy pro detekci a prevenci narušení (IDS / IPS): jsou nástroje, které na základě signatur (otisky známých technik útoků) detekují (IDS) nebo i zamezují (IPS) průnik útočníka do chráněné sítě a na koncová zařízení. V současné době jsou IPS systémy často integrovány do firewallu.

Monitoring síťového provozu na bázi síťových toků: jedná se o pokročilý způsob analýzy síťového provozu. Nástroj neprochází celý obsah zachycených packetů síťové komunikace, ale pouze její flow. Získané flow spojuje a vytváří komplexní představu o celé síťové komunikaci mezi jejím zdrojem a cílem. Nástroj získaná data agreguje a prezentuje síťovým analytikům v grafickém rozhraní.

Systémy detekce anomálií a analýzy chování sítě (NBAD): přidává k monitoringu síťového flow inteligenci na základě strojového učení. NBAD systém v reálném čase monitoruje síťový provoz a reaguje na neobvyklé síťové anomálie. Anomálie v síti neurčuje na základě signatur, ale porovnáním s běžným nebo naučeným chováním sítě. Tímto způsobem dokáže identifikovat hrozby, které nezachytí jiné konvenční bezpečnostní systémy a je vhodným nástrojem k detekci nežádoucích aktivit uživatelů. [25]

Výsledky detekce jsou prezentovány přehlednou formou (Obr. 6), což umožňuje efektivní práci při investigaci. Detekované události můžou být přeposílány do SIEM k obohacení jeho možností korelace.



Obrázek 6 grafické rozhraní NBAD nástroje Flowmon ADS (vlastní)

4.3 Nástroje pro sledování stavu infrastruktury

Je třeba krátce pojednat i o monitoringu stavu infrastruktury využitím protokolu SNMP (Simple Network Management Protocol). SNMP je využíván pro účely nepřetržitého, automatizovaného monitoringu „zdraví“ serverů (vytížení procesoru, využití operační paměti, datového úložiště…), spuštěných služeb, vytížení sítě a dalších provozních záležitostí. Nástroj k monitorování stavu infrastruktury napomáhá k včasné identifikaci narušení jednoho z pilířů informační bezpečnosti – dostupnosti.

4.4 SOC

Závěrem kapitoly je třeba zmínit Security Operations Center (SOC), což je dle jedné z definic *„centralizovaný tým v rámci jedné organizace, který monitoruje prostředí informačních technologií z hlediska zranitelností, autorizovaných aktivit, přijatelného*

použití/porušení zásad/procedur, průniků do sítě a ze sítě a poskytuje přímou podporu procesu reakce na kybernetické incidenty.“ [1] [26]

Jedná se tedy o organizační útvar společnosti, který k zajištění své pracovní činnosti využívá více vzájemně se doplňujících technických prostředků, z nichž ty nejzásadnější byly popsány v této kapitole.

Dílčí závěr: pakliže víme, jaké události k zajištění bezpečnostního monitoringu uživatelů je užitečné získávat a známe technické prostředky pro jejich zpracování, lze přejít k návrhu konkrétního řešení. Prvním krokem k dosažení požadovaného cíle je nasazení nástroje SIEM.

[1] A centralized team in a single organization that monitors the information technology environment for vulnerabilities, authorized activity, acceptable use/policy/procedure violations, intrusions into and out of the network, and provides direct support of the cyber incident response process.

5 ORGANIZAČNÍ PŘEDPOKLADY PRO NASAZENÍ SIEM

Před hodnocením technické způsobilosti nasazení SIEM je třeba zvážit a zajistit i mnoho organizačních a procesních náležitostí. Ve společnosti musí být vytvořeno vhodné prostředí pro jeho provoz.

Nestačí disponovat pouze daty ze zdrojových systémů, ale potřebujeme mít informace o celé organizaci a jejich obchodních procesech. Je třeba začít inventarizací hlavních obchodních procesů organizace s jejími vlastníky a pokračovat aplikacemi, které jsou pro tyto procesy použity. Od aplikací se dostaneme k serverům, které zajišťují jejich provoz a k další infrastruktuře. [27]

Organizační předpoklady můžeme shrnout do následujících oblastí.

5.1 Předpisová základna

Potřeba získávat logy z aplikací a systémů zvyšuje technické požadavky na jejich pořízení či vývoj a následnou údržbu. Pokud nejsou požadavky na logování stanoveny již ve výběrovém řízení na nový systém, lze je zpětně jen těžko vyžadovat a ve většině případů je to i nemožné. Musí tedy být obecně zakotveny v BPI a dále detailněji rozpracovány v navazujících směrnicích společnosti.

5.2 Personální zajištění

Informační aktiva se v čase neustále mění, přibývají nová a jiná zanikají s tím, jak se mění obchodní procesy nebo vyvíjí nové technologie. Proto samotný nástroj SIEM, i když se v počátku správně implementuje, nebude plnit svoji funkci bez neustálého a nikdy nekončícího procesu rozvoje a údržby.

Dle velikosti společnosti je nezbytné pro rozvoj a údržbu SIEM zajistit dostatečný počet specialistů IT bezpečnosti na trhu práce. Starost o SIEM musí být jejich hlavní pracovní náplní a musí mít pro tuto činnost pevně vyhrazený čas.

Při rozvoji SIEM je důležité reagovat na nové hrozby a specialisté musí mít aktualizované znalosti pro jejich identifikaci a obranu proti nim. Z toho důvodu je potřebné dbát na jejich profesní rozvoj vhodnými školeními.

5.3 Zajištění finančních zdrojů

V celém životním cyklu SIEM musí být zajištěno jeho financování. Kromě investičních nákladů na pořízení a nákladů na personální zajištění (potřebný počet FTE), musí být součástí rozpočtu na každý rok i částka věnovaná na údržbu a podporu.

5.4 Spolupráce

Dobrá spolupráce se všemi odděleními napříč organizační strukturou je klíčová. Zásadní je pak bezproblémová a velice úzká spolupráce s provozním IT, které zajišťuje většinu technických předpokladů pro provoz SIEM.

Stěžejní je podpora vedení společnosti, které pořízení SIEM identifikuje jako jeden z prostředků k zajištění svých strategických cílů v oblasti ochrany informačních aktiv.

5.5 Seznam informačních aktiv

Jak bylo nastíněno v úvodu kapitoly, je třeba zmapovat jednotlivé obchodní procesy společnosti, na základě kterých je vytvořen seznam informačních aktiv. U každého aktiva stanovíme co a v jakém rozsahu chceme auditovat. Dalším vhodným zdrojem pro získání seznamu aktiv je analýza rizik, ale můžeme čerpat i z dalších zdrojů, jako jsou aplikační katalog, mapa síťové topologie, CMDB, informace z admin konzolí pro virtualizaci serverů, síťové kontroléry, síťové skeny atd.

Dílčí závěr: bez zajištění vhodného prostředí pro nasazení nástroje SIEM, a to ve všech ohledech uvedených v jednotlivých podkapitolách, nelze předpokládat jeho úspěšné nasazení a následný provoz.

6 TECHNICKÉ PŘEDPOKLADY PRO NASAZENÍ SIEM

Technických předpokladů může být celá řada v závislosti na charakteru a velikosti společnosti a na její technické vybavenosti. V následujících odstavcích jsou popsány technické požadavky platné pro lokální společnost střední velikosti, avšak dají se s různými modifikacemi přenést na libovolnou společnost.

Jak již bylo řečeno v kapitole *4.1.4 Základní princip SIEM*, základem fungování nástroje SIEM je získávání logů. Základní otázky při přípravě jeho nasazení, které je třeba zodpovědět, tedy jsou:

- **jak dlouho potřebujeme uchovávat logy?** Během základní konfigurace, při implementaci zvoleného řešení, budeme muset nastavit tzv. retenci logů – po jak dlouhé době budou data smazána. Jedním z kritérií (dle oboru podnikání) bývají regulatorní nebo legislativní požadavky (např. požadavky ČNB nebo zákon o kybernetické bezpečnosti),
- **kolik informací budeme chtít z logu získávat?** I v malých síťových prostředích může být generováno tolik auditních záznamů, že to může přehltit dostupné datové úložiště. Při nastavení nejvyšší úrovně logování na síťových prvcích mohou tyto generovat v malých sítích i miliony událostí denně a v těch korporátních i miliardy. Bude třeba zvolit vhodný poměr mezi množstvím informací, které potřebujeme, zvolenou retencí logů a kapacitou úložiště,
- **jaký druh logů požadujeme uchovávat?** Potřebujeme zhodnotit a zvolit, které informace jsou pro naše SIEM řešení nezbytné. Teoreticky může logy generovat každé síťové zařízení, server i pracovní stanice, vč. všech instalovaných aplikací. [28]

Odpovědět na tyto otázky není jednoduché a zároveň jsou zcela zásadní pro plánování nasazení SIEM řešení.

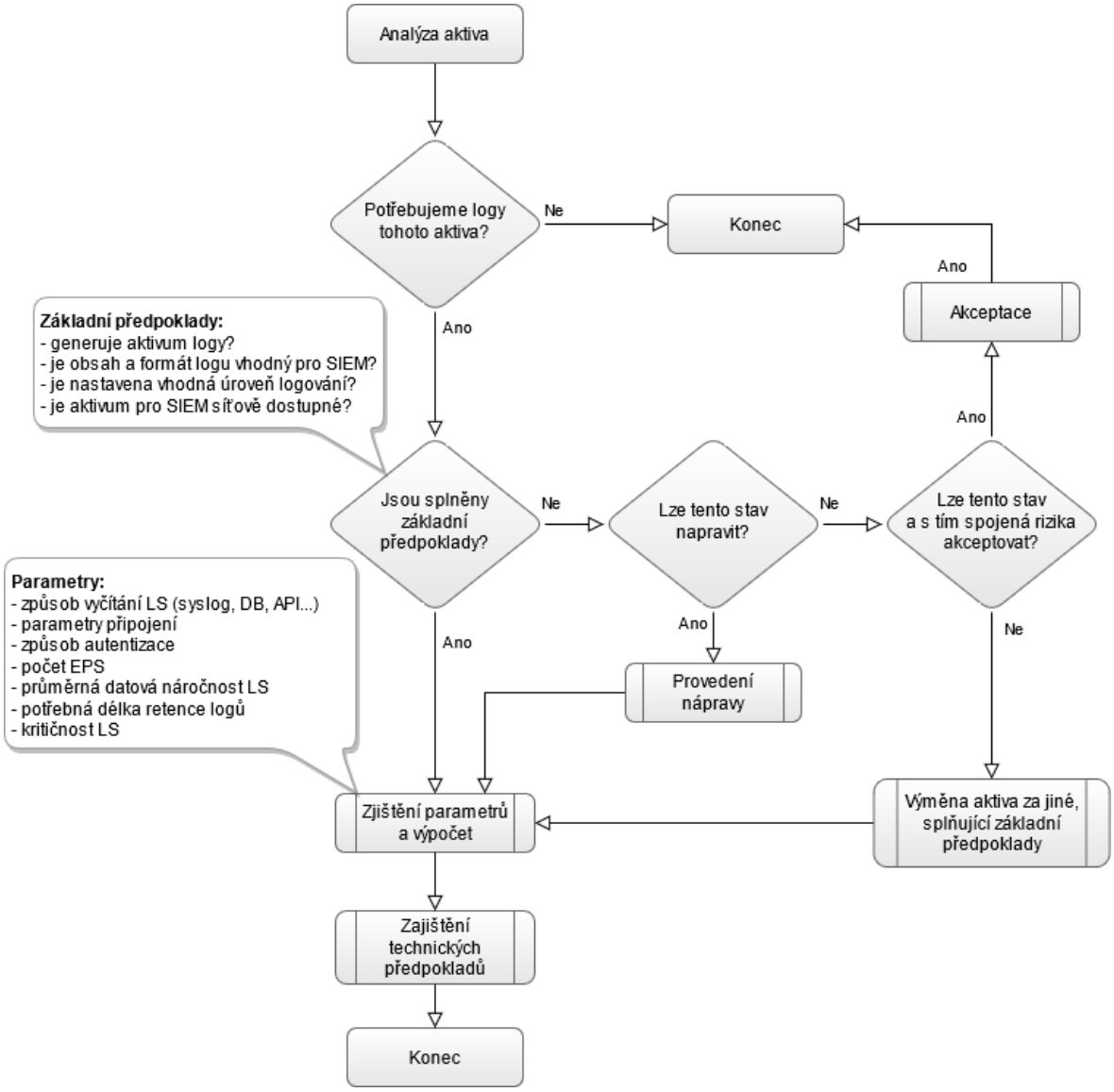
6.1 Analýza aktiv

Dle kapitoly *5.5 Seznam informačních aktiv* bychom měli mít k dispozici seznam všech informačních aktiv ve společnosti. Tento seznam je třeba rozšířit o další položky:

- generuje aktivum logy?
- je obsah a formát logu vhodný pro SIEM?
- je aktivum pro SIEM síťově dostupné?

- způsob vyčítání logů,
- parametry připojení k logům,
- způsob autentizace ke zdroji logů,
- počet generovaných událostí za vteřinu (EPS),
- průměrná datová náročnost LS,
- potřebná délka retence logů,
- kritičnost LS.

Postupovat můžeme dle diagramu (Obr. 7) a následujících podkapitol.



Obrázek 7 Diagram analýzy aktiv (vlastní)

6.2 Formát logu

Správně formátovaný log je nezbytným předpokladem pro jeho automatizované zpracování nástrojem SIEM. Správná struktura zajistí možnost získání informací uložených v logu a jejich další zpracování. Ideální je stav, kdy je jedna konkrétní událost, se všemi potřebnými informacemi, uložena jako jeden řádek logu. Jednotlivé události jsou od sebe odděleny řádkováním. V některých případech toto nelze zajistit – jedná se o tzv. víceřádkové logy. V těchto případech musí všechny řádky stejné události obsahovat jedinečný identifikátor, aby se daly vzájemně propojit v celistvou informaci.

Jednotlivé údaje musí být pro SIEM od sebe vzájemně rozeznatelné. Toho lze dosáhnout kombinací oddělovače, identifikátoru položky, uzavřením speciálním symbolem apod., jak je vidět na příkladu – zalomený jeden řádek logu (Obr. 8).

```
<189>date=2021-02-23 time=01:13:56 devname="FW-BRNO"
devid="GX5DR8581988270" eventtime=1614039236688671286 tz="+0100"
logid="0000000015" type="traffic" subtype="forward" level="notice"
srcip=10.9.8.115 srcport=64780 srcintf="USR" srcintfrole="lan"
dstip=52.96.35.14 dstport=443 dstintf="INET" dstintfrole="wan"
srccountry="Reserved" dstcountry="Netherlands" sessionid=1284624483
proto=6 action="start" policyid=142 policytype="policy"
policyname="INET access" user="JAN.NOVAK" service="HTTPS"
```

Obrázek 8: Ukázka jedné události logu firewallu (vlastní)

Z důvodu správné normalizace a parsování hodnot z logu je doporučeno používat anglickou jazykovou verzi logování. Např. OS Microsoft Windows pojmenovává atributy v logu dle jazyku nastaveného pro uživatelské prostředí. U serverových edicí je tedy vhodné používat anglické uživatelské prostředí (a to nejen z důvodu logování, ale i přehlednější správy samotného systému).

Struktura logů může být dle jejich zdroje velice rozličná, což znesnadňuje jejich normalizaci na vstupu do SIEM. Určitá pravidla zápisu jsou použita i u protokolu syslog, který byl původně vytvořen před mnoha lety v rámci implementace TCP/IP v OS BSD a byl následně převzat dalšími OS a implementován do mnoha síťových zařízení [29]. Později byl také popsán v doporučeních RFC 3164 [29] a dále rozšířen v RFC 5424 [30]. Pro jednoduchou normalizaci logů je syslog ve své původní formě nedostačující a proto někteří výrobci SIEM vytvořili pro svá řešení standardizovaný formát, viz dále.

6.2.1 Obsah logu

Každý auditní záznam, aby byl vypovídající, by měl obsahovat následující informace:

- **datum a čas události**:
  - kdy došlo k události,
  - kdy došlo k záznamu události – tuto informaci přidává SIEM při přijetí záznamu logu.
    Tyto dva časy se často liší,
- **původce události**:
  - jednoznačný identifikátor původce události (účet uživatele, systému, technického účtu),
  - název aplikace, služby, instance databáze, kde událost vznikla – může být zaznamenáno původcem události nebo je tato informace převzata z názvu LS v SIEM,
- **místo vzniku události**:
  - zdrojová IP adresa, kterou měl v době události její původce (např. IP adresa počítače uživatele či správce),
  - cílová IP adresa v případě některých síťových zařízení, kdy komunikace probíhá mezi dvěma a více stranami,
- **událost nebo provedená operace**:
  - popis události, který vystihuje co uživatel nebo proces provedl,
  - provedené změny, či jiný obsah – může se lišit v závislosti na druhu logu,
- **podmínky události**:
  - úspěch či neúspěch provedené události, případně její kritičnost. [31]

6.2.2 CEF

Společnost ArcSight (dnes Micro Focus) pro svůj stejnojmenný produkt vytvořila Common Event Format (CEF). Tento formát zobecnil a rozšířil se mezi výrobci, jejichž zařízení umožňuje zasílání událostí syslogem. Struktura hlavičky záznamu je popsána níže (Obr. 9).

```
Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device
Version|Device Event Class ID|Name|Severity|[Extension]
```

Obrázek 9 Hlavička CEF [32]

Za CEF hlavičkou následují jednotlivé atributy události, které mají jednoznačné identifikátory a způsob zápisu. Kompletní popis CEF se všemi parametry je ke stažení na webu výrobce [32]. Na následujícím příkladu je vidět celý záznam události (Obr. 10).

```
Sep 19 08:26:10 host CEF:0|Security|threatmanager|1.0|100|worm successfully
stopped|10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

Obrázek 10 Příklad CEF [32]

6.2.3 LEEF

Společnost Q1 Labs (dnes IBM) pro QRadar SIEM vytvořila vlastní Log Event Extended Format. V dnešní době lze v nastavení logování mnoha zařízení vybrat krom CEF formátu i LEEF. Jak je vidět na následujícím příkladu hlavičky LEEF (Obr. 11), je způsobem zápisu podobný CEF.

```
LEEF:Version|Vendor|Product|Version|EventID|
LEEF:1.0|Microsoft|MSExchange|4.0 SP1|15345|
LEEF:2.0|Lancope|StealthWatch|1.0|41|^|
```

Obrázek 11 Hlavička LEEF s příklady [33]

Za hlavičkou opět následují informace v daném formátu a jsou použity předdefinované atributy (Obr. 12), jejichž seznam je k dispozici dokumentace výrobce [33].

```
key=value<tab>key=value<tab>key=value<tab>key=value<tab>.
src=192.0.2.0 dst=172.50.123.1 sev=5 cat=anomaly srcPort=81 dstPort=21 usrName=joe.black
```

Obrázek 12 Příklad payloadu LEEF formátu [33]

6.3 Způsob vyčítání LS

Logy můžeme ze zdroje získávat různými způsoby. Každý takový způsob má své výhody a nevýhody, které jsou dále popsány.

V obecném pohledu však můžeme říci, že logy lze získávat metodami:

- **push**: tato metoda je jednoduchá na nastavení a zajišťuje on-line přísun logů do SIEM. Na LS nastavíme pouze kam a jak má zprávy zasílat (IP adresa nebo DNS jméno SIEM a parametry připojení). Pro zahájení přenosu není potřeba žádná přímá interakce se SIEM, iniciátorem je zařízení, které generuje logy. Typickým zástupcem této metody je syslog. Nevýhodou je zabezpečení přenosu a možnost ztráty logů, viz kapitola o syslog protokolu,
- **pull**: na rozdíl od push metody je zde iniciátorem přenosu zpráv SIEM. Pro získání logů z jejich zdroje musí existovat předem připravená konfigurace. SIEM se za použití technického účtu a hesla přihlásí k LS a sám si řídí vyčítání událostí.

Výhodou je tedy plná kontrola nad získáváním logů. Při dočasné nedostupnosti LS nepřijdeme o žádné události, protože SIEM si „pamatuje“, které události vyčetl naposled a po obnově spojení si zpětně dočte zbytek. Také (na rozdíl od syslogu) je přenos informací zpravidla šifrován. Nevýhodou je vyčítání logů v dávkách, v časových intervalech – události ze zdroje neplynou v proudu on-line. [23]
Mezi pull metody patří všechny ostatní popsané způsoby připojení níže.

6.3.1 Syslog protokol

Syslog protokol pro zasílání událostí logu používá většina síťových zařízení, jako jsou firewally, switche, routery a dále ve velké míře OS na jádře Linux / UNIX. V menší míře je syslog implementován i do některých síťových aplikací. Syslog má v síťové komunikaci vyhrazeno číslo portu 514 (Tab. 1) a data mohou být přenášeny protokoly TCP nebo UDP [34]. Zda budeme data přenášet pomocí TCP nebo UDP závisí na dvou faktorech:

- **na velikosti generovaných zpráv**: z principu fungování UDP protokolu a jak je popsáno v RFC 5426 [35] musí vždy UDP datagram obsahovat jednu syslog zprávu. Vzhledem k běžné maximální velikosti přenosové jednotky (MTU) 1500 bytů je pak maximální velikost syslogové zprávy zasílané pomocí UDP protokolu 1024 bytů [29]. Pokud potřebujeme přenášet další zprávy, musíme použít protokol TCP,
- **na potřebě zabezpečení zpráv**: u zpráv přenášených UDP protokolem není na rozdíl od TCP zajištěno, že dorazí do cíle. Je-li v síti nebo v cíli doručení nějaký problém způsobující nedostupnost služby, zprávy budou nenávratně ztraceny a nebude o tom vytvořen žádný záznam. Při použití TCP můžeme navíc zabezpečit přenášená data šifrováním prostřednictvím TLS protokolu a zabezpečit tak jejich důvěrnost.

Tabulka 1 Syslog - FW prostupy, data čerpána z: [34]

Zdroj	Cíl	Port	Protokol
LS	SIEM	514, 6514 (TLS)	TCP, UDP

6.3.2 Databázové připojení

Získávání událostí z databází (DB) můžeme rozdělit na dvě části:

- **audit DB**: jedná se o události generované samotným provozem DB. Např. přihlášení uživatelů a správců přímo k DB, úpravy schématu, vytváření / mazání tabulek, nastavování oprávnění, spouštění SQL dotazů atd.,

- **logy aplikací uložené v DB**: aplikace, které pro ukládání dat používají DB, většinou do stejné databáze ukládají i své provozní / bezpečnostní logy. Tabulka nebo upravený pohled na tabulku s logy můžeme použít jako vstup pro SIEM.

SIEM disponuje řadou předpřipravených konektorů pro vyčítání událostí z databází různých výrobců. Pro připojení k DB potřebujeme znát číslo TCP portu (liší se dle výrobce, instance) a technický účet s heslem s oprávněním číst tabulky s logy. V tabulce (Tab. 2) jsou uvedeny čísla výchozích portů pro nejpoužívanější databáze.

Tabulka 2 Databáze - FW prostupy, data čerpána z: [36]

Zdroj	**Cíl**	**Port**	**Protokol**
SIEM	MS SQL Databáze	1433	TCP
	Postgres	5432	
	MySQL	3306	
	Oracle	1521	

6.3.3 Web API připojení

API je zkratkou pro aplikační programovatelné rozhraní. Umožňuje jednoduchým způsobem aplikaci komunikovat s jinými aplikacemi nebo službami, bez potřeby znalosti jejich implementace. S rozvojem webových aplikací byly vyvinuty specifikace protokolu ve snaze standardizovat výměnu informací. Příkladem je protokol SOAP. Dalším příkladem je REST, který však není standardizovaný a jeho implementace se různí. [37]

API je vhodné pro vyčítání auditních záznamů z aplikací nejen uvnitř sítě společnosti, ale i (a především) z cloudových aplikací na internetu, kde je to často jediná možnost. SIEM disponuje možností se k API připojit a potřebné informace získat. Pro připojení k API je využíváno standardního HTTPS protokolu (HTTP protocol over TLS/SSL) na TCP portu 443 [34] (Tab. 3). Pro připojení musí SIEM znát technický účet a heslo (nebo token) s oprávněním se k API připojit a také strukturu API, ke kterému se připojuje (URL koncového bodu, metody, parametry).

Tabulka 3 API - FW prostupy, data čerpána z: [34]

Zdroj	Cíl	Port	Protokol
SIEM	API	443	TCP

6.3.4 Vyčítání souboru

Další možností získávání logů je jejich včítání z textových souborů, které ukládá zdrojový systém nebo aplikace na pevný disk nebo síťové úložiště. Přístup k souborům umožňuje použití některého ze síťových protokolů pro práci se soubory, jako jsou např. SMB / SAMBA, SFTP jejichž čísla portů jsou uvedena v tabulce níže (Tab. 4). Uvedené protokoly také zajišťují šifrovaný přenos informací (SMB od verze 3 [38]).

Tento způsob vyčítání má několik úskalí a tím největším je zajištění správné rotace souborů v místě jejich uložení. Systém, který loguje události, zapisuje do souboru informace postupně a má nastavena pravidla, kdy má soubor uzavřít a vytvořit nový. Předchozí soubor může např. přejmenovat, archivovat, přesunout do jiné složky nebo smazat. Nevhodným nastavením rotace může dojít ke ztrátě událostí, které si SIEM nestihne vyčíst – mezi dvěma intervaly, kdy se SIEM k LS připojuje, dojde k „odrotování“ souboru.

Vyčítání souborů se používá např. pro logy služeb DHCP a DNS v rámci MS Windows Serveru.

Tabulka 4 Souborové protokoly – FW prostupy, data čerpána z: [34]

Zdroj	Cíl	Port	Protokol
SIEM	SMB / SAMBA	445	TCP
	SFTP (SSH)	22	TCP

6.3.5 Kolektor

Kolektorem se v této kapitole rozumí specializované zařízení, server nebo aplikace, která je součástí řešení SIEM, ale funguje odděleně a je určena pro sběr logů určitého druhu a jejich následné předání ke zpracování. Příkladem může být kolektor pro vyčítání logů z Windows Event Logu. Kolektor se může k LS připojovat vzdáleně nebo může být nainstalován přímo

v zařízení, kde se logy generují. Z popsaného důvodu nelze obecně určit jeho požadavky na připojení ani autentizaci. Ty je třeba řešit individuálně před jeho nasazením.

6.4 Požadavky na připojení a autentizaci

Z předchozí kapitoly vyplývá potřeba připravit prostupy na firewallu v síti společnosti a připravit technické účty. V této kapitole jsou požadavky blíže popsány a přidány další, nezbytné pro správné fungování SIEM.

Požadavky pro zajištění komunikace SIEM v síti jsou následující:

- **IP adresy**: pro jednotlivé servery, datová úložiště a zařízení, které jsou součástí SIEM řešení,
- **VLAN**: síťovou topologii je potřeba rozšířit o VLAN vyhrazenou pro SIEM řešení, které bude zakončená na firewallu. To zaručí bezpečné oddělení od ostatních zařízení v síti,
- **DHCP**: pro VLAN, kde bude SIEM řešení umístěno musí být dostupná služba přidělování IP adres serverem DHCP,
- **DNS**: v síti musí být dostupný DNS server pro překlad názvů,
- **NTP**: synchronizace času všech součástí SIEM je nezbytná. Všechna zařízení v síti společnosti musí mít naprosto shodný čas,
- **SMTP**: SIEM bude zasílat e-mailová upozornění, reporty a notifikace, musí mít tedy k dispozici SMTP server a oprávnění přes něj zasílat e-maily,
- **LDAP**: pro autentizaci uživatelů a správců do konzole a na další servery řešení SIEM je vhodné použít některou z adresářových služeb,
- **SMNP**: pro monitoring běhu služeb SIEM, v nástroji pro sledování stavu infrastruktury,
- **VPN**: v případě, že bude SIEM vyčítat logy z dalších lokalit nebo geograficky oddělených datacenter společnosti, musí být mezi nimi vybudováno VPN spojení,
- **síťové prostupy**: na firewallech společnosti musí být vybudovány pro SIEM prostupy tak, aby měl SIEM síťový přístup na všechny výše uvedené služby, a dále do všech VLAN a do internetu odkud vyčítá logy (viz tabulky k jednotlivými typům připojení v předchozí kapitole). A naopak aby byl SIEM přístupný pro všechny LS, které zasílají logy metodou push. SIEM potřebuje dále přístup do internetu z důvodu aktualizace svých komponent a kvůli přístupu do specializovaných databází (např. seznamy nebezpečných internetových adres).

6.4.1 Adresářová služba

Správci aplikací a systémů musí připravit sadu technických účtů, skupin zabezpečení a rolí. Pro tyto účely je vhodné využít adresářovou službu s implementovaným protokolem LDAP, např. MS Active Directory nebo OpenDJ. Zajistit je třeba:

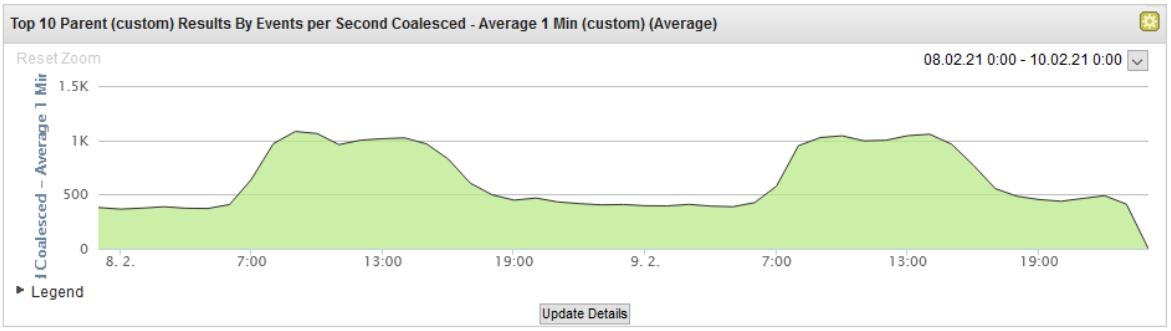
- technické účty pro LS, kde je použita metoda pull pro získávání logů,
- technické účty pro služby uvedené v předchozím odstavci (připojení SIEM k adresářové službě, SMTP serveru),
- skupiny zabezpečení v adresářové službě, na které budou navázány role řídící přístup a oprávnění k jednotlivým částem SIEM řešení.

6.4.2 Certifikační autorita

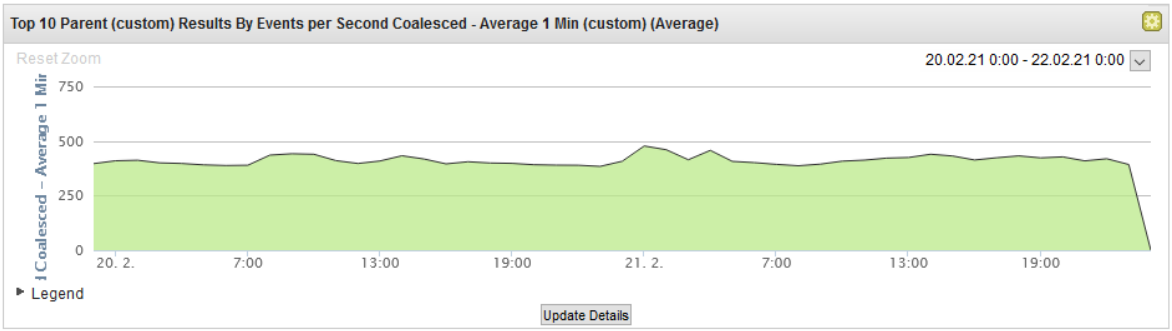
Pokud má SIEM konzole uživatelské rozhraní tvořené webovou aplikací, musí být přístup uživatelů k ní důvěryhodný. Na webový server je potřeba vystavit certifikát podepsaný certifikační autoritou (CA), které uživatelé v síti důvěřují. Může se jednat o interní CA nebo veřejně uznávanou.

6.5 Zajištění výkonu a kapacity

Pro dokončení analýzy aktiv musíme u každého LS určit průměrnou hodnotu EPS a objem generovaných dat. EPS se u většiny logů mění během dne zároveň s pracovní dobou, směnami, sezónou a jinými faktory závislými na aktivitě zaměstnanců, zákazníků nebo třeba studentů v případě škol, jak je vidět na následujících příkladech (Obr. 13 a 14).



Obrázek 13 Graf EPS – 2 pracovní dny (vlastní)



Obrázek 14 Graf EPS – 2 nepracovní dny (vlastní)

6.5.1 Odhad EPS a objemu dat LS

Pokud nelze požadované údaje o EPS a objemu dat získat přímo z managementu aplikace / systému, který log generuje, je třeba tyto hodnoty odhadnout výpočtem. K tomu potřebujeme získat textový soubor s logy za 24 h jednoho běžného pracovního a jednoho nepracovního dne. Výpočet provedeme jednoduchým způsobem (Rov. 1).

$$EPS = \frac{E_w + E_n}{172800} \tag{1}$$

Kde: EPS = počet událostí za vteřinu, E_w = počet událostí (řádků) souboru logu z běžného pracovního dne, E_n = počet událostí souboru logu z běžného nepracovního dne, číselná hodnota představuje počet vteřin za dva dny.

Objem dat můžeme stanovit pomocí průměrné denní velikosti datového souboru s logy (datová náročnost) vynásobené požadovanou dobou retence logu (Rov. 2).

$$DV = R \cdot \frac{S_w + S_n}{2} \tag{2}$$

Kde: DV = objem dat [MB], S_w = velikost datového souboru s logy z běžného pracovního dne [MB], S_n = velikost datového souboru s logy z běžného nepracovního dne [MB], R = požadovaná retence logů ve dnech.

Získané hodnoty objemu dat jsou pouze odhadem a skutečné nároky na kapacitu datového úložiště se budou lišit. Události na vstupu SIEM budou mít jinou velikost, než jakou budou mít po normalizaci, uložení do databáze a případně indexaci.

Hodnoty EPS jednotlivých LS i objemy dat nakonec sečteme, čímž získáme potřebné informace pro návrh celého řešení. Musíme však počítat s tím, že během provozu SIEM přibývají v infrastruktuře další nové systémy a aplikace, jejichž logy budeme chtít do SIEM

postupně přidávat. Proto k celkovým nárokům na EPS a úložiště přičteme dostatečnou rezervu. Celé řešení je třeba plánovat tak, aby jej bylo možné v budoucnu dále rozšiřovat. Pokud je požadováno zasílat do SIEM ke zpracování i síťové flow, je třeba s tím při plánování kapacity počítat.

6.5.2 Způsob provozu a požadavky na výkon

Celé SIEM řešení (nebo jeho časti) můžeme provozovat ve virtualizovaném prostředí, nebo na hardwarovém prostředku. Každá varianta má své výhody a nevýhody. V případě velkého řešení v prostředí s velkým počtem LS a vysokým EPS se již virtualizace nemusí vyplatit (z důvodu vysokých nároků na výkon, především na velikost dostupné paměti) a SIEM bude efektivnější provozovat na dedikovaném hardware. V případě menšího řešení (cca do 1000 EPS), jej lze s výhodou virtualizovat (lepší správa prostředků, dynamické přidělování výkonu…). Při rozhodování je nutné řídit se doporučeními a stanovenými požadavky výrobcem konkrétního SIEM nástroje. Pro příklad IBM v závislosti na EPS stanovuje pro každou virtualizovanou komponentu minimální a doporučené výkonové požadavky [39] nebo nabízí vlastní HW, kde jsou stanoveny výkonové limity [40].

6.5.3 Zálohování a vysoká dostupnost

SIEM je pro společnost cenné aktivum, které je nutno důsledně chránit a zabezpečit dostupnost, integritu a důvěrnost uložených informací. Základem je zabezpečit především:

- vysokou dostupnost pro nepřerušovaný příjem a zpracování logů, pro zasílání upozornění a reportů a pro práci specialistů IT bezpečnosti s grafickým rozhraním,
- důvěrnost dat dostupných v SIEM šifrováním a řízením přístupu,
- zálohovaní konfigurace i dat na externí úložiště pro případ mimořádných událostí. Úložiště záloh by mělo být v geograficky odlišném místě, než je SIEM a platí pro něj stejné zásady zabezpečení dat,
- proaktivní dohled celého řešení z důvodu okamžité reakce při selhání některé ze součástí.

Dílčí závěr: důkladná analýza a příprava technických předpokladů, nám umožní doplnit projektový plán pro nasazení SIEM o technické detaily a pomůže stanovit dílčí úkoly pro jednotlivé realizační týmy.

II. PRAKTICKÁ ČÁST

7 PLÁN NASAZENÍ SIEM

Cílem této kapitoly je sestavit plán nasazení SIEM řešení tak, aby mohl být podkladem pro vytvoření projektu. Plán lze rozdělit do tří hlavních částí – příprava, ověření konceptu, neboli Proof of Concept (PoC) a uvedení do provozu. Plán je vhodné přenést do některého specializovaného nástroje pro řízení projektu.

7.1 Příprava

Všechny tři části plánu jsou stejně významné, avšak přípravě musíme věnovat zvláštní pozornost. Příprava zásadním způsobem ovlivní celý zbytek plánu.

7.1.1 Kontrolní seznam

Kontrolní seznam přímo vychází z kapitol *5 Organizační předpoklady pro nasazení SIEM* a *6 Technické předpoklady pro nasazení SIEM*. Organizační i technické předpoklady je třeba strukturovat do tabulky a bod po bodu odsouhlasit připravenost. V případě zjištění nedostatku tento napravit. Příklad takové tabulky – kontrolního seznamu je uveden v příloze *P I: Kontrolní seznam přípravy pro nasazení*. Tabulku je možné interpretovat jako dílčí úkoly v nástroji pro řízení projektů.

7.1.2 Výběr SIEM

První otázkou často bývá, zda můžeme použít nějaký open source nástroj, který je ke stažení a použití zdarma. Přesto, že existují různé open source nástroje, ze kterých by šlo poskládat SIEM řešení, musíme si položit otázku, kolik by bylo potřeba času se tomu věnovat a jaké by to neslo náklady. Do nákladů je třeba započítat i náklady na vytvoření podrobné dokumentace, aby se v budoucnu, v případě potřeby, dalo celé řešení předat dalším zaměstnancům. Výsledné celkové náklady na vlastnictví (TCO) open source řešení by mohly být vyšší, než náklady na komerční řešení. Výrobci komerčních řešení nabízejí své produkty s výhodou tak, že je možné nejdříve pořídit SIEM v základní konfiguraci a následně jej rozšiřovat o další komponenty [41].

Při výběru komerčního řešení se můžeme řídit praktickými doporučeními specialistů IT bezpečnosti, odbornými rešeršemi z dostupných zdrojů nebo třeba doporučením společností Gartner, který pro různé IT oblasti vytváří report a tzv. Gartner Magic Quadrant (Obr. 15).

Obrázek 15 2020 Gartner Magic Quadrant for SIEM [42]

7.1.3 Vytvoření zadání a vyhodnocení

Abychom mohli objektivně zhodnotit, které z nabízených řešení splňuje nejvíce našich požadavků a očekávání, je třeba vytvořit kritéria výběru a stanovit jejich váhy. V rámci výběru je důležité zhodnotit i pořizovací cenu a celkové náklady na vlastnictví. Dalším krokem je vytvoření zadání pro výběrové řízení a oslovení dodavatelů jednotlivých SIEM řešení. V zadání by neměly chybět požadavky na způsobilost dodavatele, požadovanou podporu, údržbu a zajištění školení. Ze zadání musí být také zřejmé, jaké máme nároky na výkon (EPS, FPS).

Informace získané od dodavatelů přeneseme do tabulky, viz příklad v příloze *P II: Zadání pro hodnocení výběru SIEM* a provedeme vyhodnocení.

7.2 Proof of Concept

Účelem Proof of Concept (PoC) je ověřit, že vybrané řešení splňuje naše očekávání i v praxi. Někteří výrobci pro účely PoC disponují potřebným HW vybavením i licencemi s omezenou platností, které mohou zákazníkovi prostřednictvím zvoleného dodavatele zapůjčit.

7.2.1 Konfigurace SIEM

V rámci PoC je provedena konfigurace celého řešení v prostředí společnosti a v rozsahu potřebném pro ověření všech funkcí a postupů. Postup konfigurace vybraného SIEM řešení je v jednotlivých detailech popsán v kapitole *9 Nasazení řešení IBM QRadar SIEM*.

7.2.2 Vyhodnocení PoC a pořízení

Obsahem hodnocení PoC může být např.:

- ověření splnění všech výběrových kritérií ze zadání,
- ověření naplnění očekávání prostřednictvím vytvoření a ověření příkladových případů užití (modelové situace, korelace událostí, reakce na incidenty…),
- ověření funkčnosti získávání a normalizace logů z aktiv, vyhodnocených jako kritické,
- hodnocení práce s uživatelským rozhraním,
- penetrační test jednotlivých částí řešení,
- test odolnosti proti neočekávaným situacím (výpadek připojení k LS, restart služeb, zaplnění disku, překročení licence EPS…).

Pokud je PoC úspěšný, provedeme akceptaci řešení z technického pohledu. Výsledek PoC zdokumentujeme a společně s indikativní cenovou nabídkou představíme vedení společnosti. Není třeba rozvádět následující proces výběrového řízení dodavatele vybraného SIEM řešení, na jehož konci by mělo být schválení vedením společnosti, pořízení a zahrnutí do rozpočtu na následující období.

7.3 Uvedení do provozu

PoC lze většinou přímo převést do produkčního užívaní, není tak nutné provádět celou konfiguraci od začátku. To zajistí plynulý přechod do produkčního provozu.

Před začátkem produkčního užívaní SIEM je důležité:

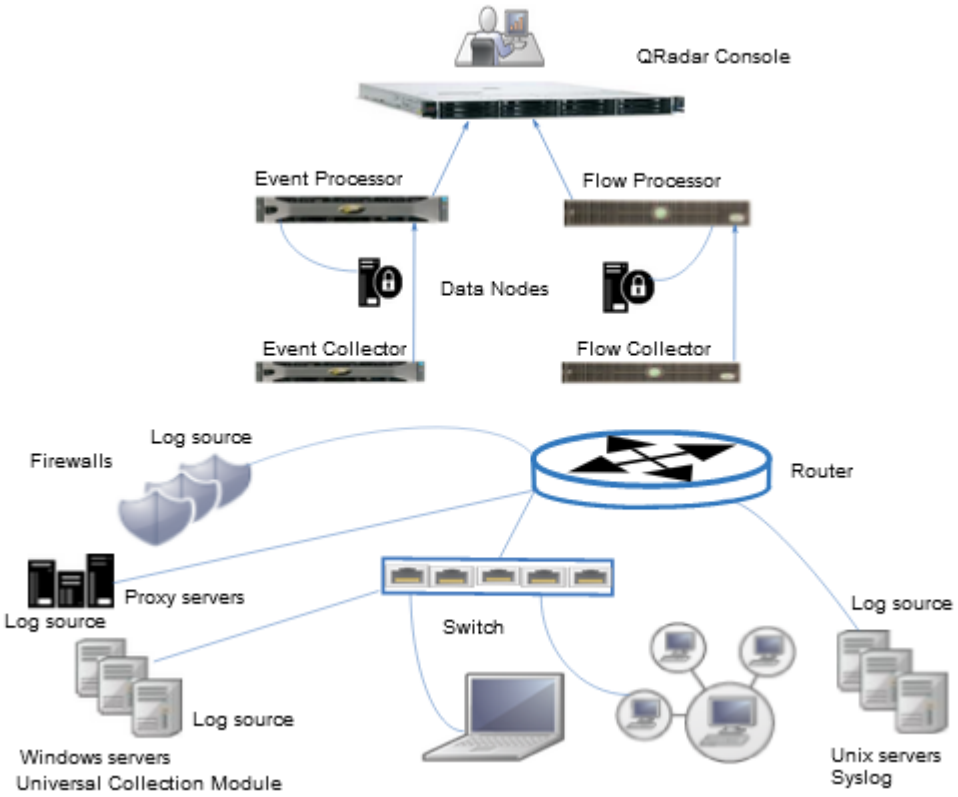
- stanovit odpovědnosti za jednotlivé činnosti (vyhodnocování událostí, pravidelná údržba, rozvoj, reporting…),
- stanovit denní pracovní postupy (co a jak často se vyhodnocuje),
- vytvořit postupy pro navazující činnosti, např. provázání s incident managementem,
- provést potřebná školení.

8 POPIS ŘEŠENÍ IBM QRADAR SIEM

Následující kapitola popisuje řešení IBM QRadar SIEM v rozsahu potřebném pro tuto práci. QRadar byl vybrán z důvodu jeho velké uživatelské základny, vhodného použití pro velké i středně velké společnosti a v neposlední řádě i pro jeho vynikající hodnocení poradenskými společnostmi, jako např. Gartner, kde je v Gartner Magic Quadrantu zařazen mezi lídry na trhu (Obr. 15) [42].

Dalším důvodem jsou mé osobní praktické zkušenosti z implementace a rozvoje tohoto SIEM řešení a přístup k technologii v rámci svého zaměstnání.

QRadar poskytuje robustní řešení pro velké organizace, kdy je pro každou funkci vyhrazený samostatný server (Obr. 16), ale i řešení pro středně velké společnosti ve variantě All-in-One QRadar appliance, kdy všechny funkce běží na jednom serveru. [43]

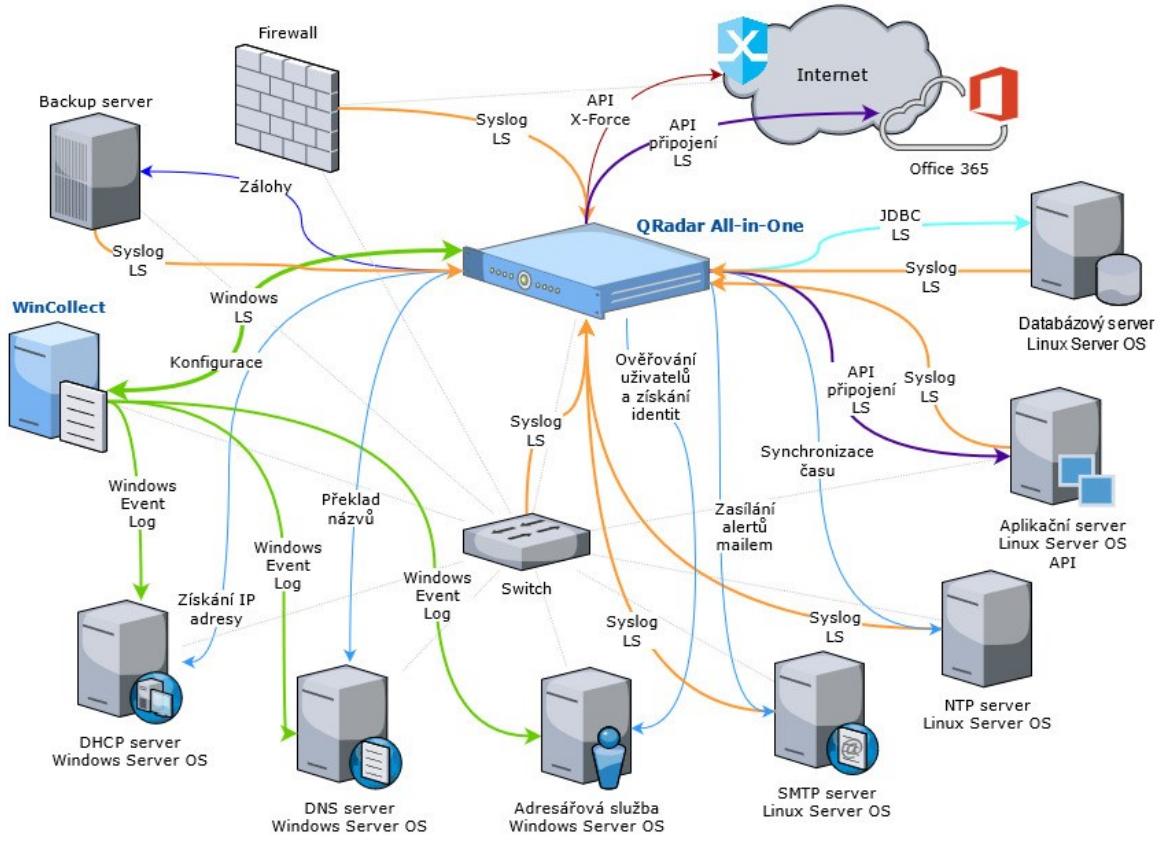


Obrázek 16 Komponenty QRadaru pro události a flow [43]

8.1 Schéma řešení

Pro potřeby práce bude v této i všech následujících kapitolách využito QRadaru ve variantě All-in-One, doplněného o WinCollect server pro získávání logů z MS Windows OS

a síťového zálohovacího zařízení. Ve schématu (Obr. 17) je znázorněno napojení QRadaru na základní služby sítě, adresářovou službu, poštovní server a zároveň příklad připojení k různým typům LS. Šipkami je znázorněn směr navazování síťové komunikace.



Obrázek 17 QRadar All-in-One schéma (vlastní)

QRadar umožňuje přijímat a korelovat i síťové flow (Netflow, IPFIX), avšak pro účely praktické části práce tato možnost nebude využita. Pro zpracování síťového flow existují na trhu specializované nástroje, kdy je vhodnější do SIEM (např. z důvodu licenčního omezení FPS) přeposílat formou událostí již zpracované výsledky analýzy z těchto nástrojů a dále je korelovat.

8.2 QRadar All-in-One

Maximální kapacita QRadaru provozovaného ve variantě All-in-one závisí pouze na zakoupené licenci a HW specifikaci zařízení. IBM nabízí vlastní zařízení v několika variantách, jejichž maximální kapacita zpracovaných událostí je (dle specifikace IBM) do 5000 EPS u nejméně výkonného zařízení (QRadar 3105), až do 30 000 EPS u nejvýkonnějšího zařízení (QRadar 3128). Přičemž středně velké výrobní společnosti do 1000 zaměstnanců může dostačovat i ta nejméně výkonná varianta. [44]

All-in-one variantu je možné rozšířit jak z pohledu získávání událostí a flow ze vzdálených destinací (přídavné kolektory událostí a flow), tak z pohledu rozšíření výkonu (přídavné procesory událostí a flow). QRadar lze provozovat i na vlastním HW nebo ve virtualizaci.

8.2.1 Specifikace zvoleného řešení

Popisované řešení je a veškeré praktické postupy jsou prováděny na zařízení:

- IBM QRadar SIEM All-in-One Virtual 3199,
- licence 2500 EPS, 15k FPM,
- WinCollect kolektor,
- rozšíření IBM User Behavior Analytics for QRadar,
- rozšíření IBM X-Force Exchange,
- rozšíření Backup app [45],
- další rozšíření.

8.2.2 Komponenty systému

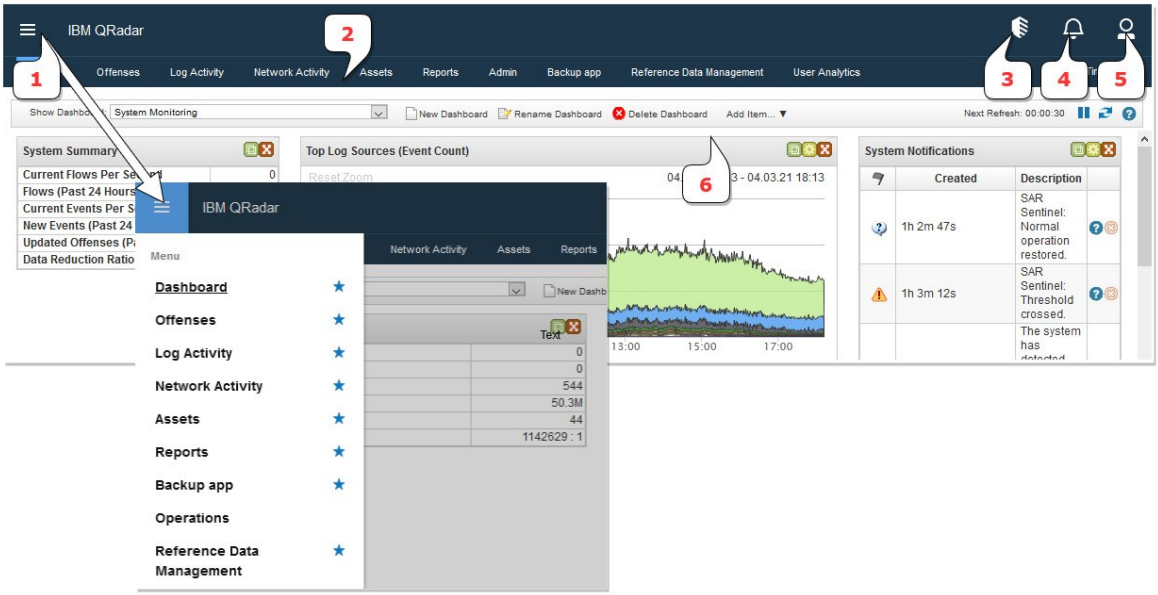
Základními komponentami, které jsou v případě zvolené All-in-one varianty integrované v jednom zařízení, jsou:

- **QRadar Console**: poskytuje grafické uživatelské rozhraní pro práci a administraci celého řešení,
- **QRadar Event Collector**: kolektor sbírá události ze všech LS a provádí jejich normalizaci pro další použití. Normalizované události přeposílá do procesoru událostí. Kolektor má na starosti kontrolu licence, zda nedochází k překračování EPS. Pokud k překročení dojde, ponechá si události ve vyrovnávací paměti a zpracuje je až ve chvíli, kdy hodnota EPS poklesne zpět do vymezených hodnot. Pokud vyrovnávací paměť přeteče, události jsou zahozeny,
- **QRadar Event Processor**: procesor zpracovává události pomocí vytvořených pravidel. Pokud některá událost způsobí sepnutí pravidla, vykoná procesor definovanou akci. Zároveň je procesor zodpovědný za předávání událostí v reálném čase do konzole a jejich ukládání do databáze,
- **QRadar QFlow Collector**: flow kolektor přijímá síťový provoz ze zrcadlených portů na switchi, TAP adaptérů nebo přímo flow z externích zdrojů. Připravený síťový flow přeposílá do flow procesoru. Flow kolektor je také zodpovědný za kontrolu nepřekročení FPS licence, deduplikaci flow z více zdrojů a jejich párování,

- **QRadar Flow Processor**: podobně jako v procesoru událostí jsou síťová flow porovnávána vůči pravidlům a při sepnutí je vyvolána definovaná akce. Procesor také ukládá flow do databáze. [46]

8.2.3 Popis grafického rozhraní a jeho funkcí

Grafické rozhraní QRadaru je realizované formou webové aplikace. Webový server je součástí QRadar Console a jeho služba běží nezávisle na ostatních komponentách.



Obrázek 18 Webová konzole QRadar (vlastní)

Na obrázku je znázorněno členění grafického rozhraní (Obr. 18), kde:

- **1** – hlavní nabídka: po rozkliknutí obsahuje veškeré položky nabídky, všech základních funkcí, rozšíření, administrace a dalších informací,
- **2** – rychlá nabídka: lze zobrazit položky z hlavní nabídky, volitelně dle preferencí každého uživatele,
- **3** – IBM QRadar Assistant (rozšíření),
- **4** – notifikace: zobrazuje informační, varovné a kritické události o stavu QRadaru, jako je překročení EPS, vysoké vytížení CPU, docházející místo na interním úložišti a další,
- **5** – uživatelská nastavení a odhlášení,
- **6** – pracovní plocha: na obrázku funkce dashboardu.

Základní funkce konzole, které se nachází v jednotlivých záložkách jsou:

- **Dashboard**: plně uživatelsky přizpůsobitelný a personifikovaný dashboard. Lze přidávat grafy, notifikace a statistiky z různých modulů a rozšíření. Umožňuje sledovat nejen stav systému, aktuální výstrahy a informace, ale i trendy v čase,
- **Offenses**: slouží pro práci s tzv. offensemi, které jsou výsledkem sepnutí předdefinovaných pravidel. Offense můžeme přirovnat k incidentům. Hlavní činností v této záložce je vytváření pravidel a následné vyšetřování offensí,
- **Log Activity**: slouží pro práci s logy. Pomocí filtrů můžeme vyhledávat události uložené v databázi nebo je zobrazovat v reálném čase, jak přicházejí z Event Processoru. V této záložce lze také v DSM editoru vytvářet definice pro nové LS, nebo exportovat či ukládat výsledky hledání, spouštět historické korelace a mnoho dalšího,
- **Network Activity**: obdoba Log Activity, ale pro síťové flow,
- **Assets**: jedná se o seznam aktiv, který napomáhá ztotožňovat uživatele s událostmi, které sebou přímo nenesou informaci o identitě. Každý profil aktiva obsahuje informace, které doplňuje automaticky z událostí z různých LS, např. IP adresa, MAC adresa, název zařízení (host name), uživatelské jméno a další. Profily aktiv se dají vytvářet i ručně nebo mohou vznikat na základě skenu zranitelností. QRadar lze o skener zranitelností rozšířit dokoupením licence nebo propojit s již existujícím skenerem třetí strany. V případě použití skeneru jsou profily aktiv doplněny i o informace o zranitelnostech zařízení,
- **Reports**: slouží pro vytváření reportů, které lze spouštět ručně nebo naplánovat jejích automatické opakované spouštění a rozesílání,
- **Admin**: administrátorská část celého systému.

8.3 Zdroje logů – Logsource

Zdroj logů, neboli Logsource (LS) byl již obecně vysvětlen v teoretické části v kapitole *4.1 Nástroje pro sběr a vyhodnocování logů – SIEM*. LS se v QRadaru spravují v části administrace v nástroji IBM QRadar Log Source Management. Kromě vytváření nových LS a jejich úprav, slouží nástroj i k zobrazení detailních informací o každém LS (např. průměrná hodnota EPS, datum poslední zaslané události, typ a popis LS…) a o jejich aktuálním stavu.

8.3.1 DSM a LSX

Události z LS přicházejí do Event Collectoru QRadaru, jehož hlavním úkolem je provést jejich normalizaci a vyparsování hodnot:

Normalizace: aby bylo možné události normalizovat, QRadar musí znát jejich strukturu, musí rozpoznat jednotlivé události, jejich atributy a správně doplnit hodnoty. Tato znalost se QRadaru předává ve formě modulů – DSM (Device Support Module). DSM je malá aplikace, která obsahuje vzory konkrétních LS. QRadar obsahuje několik set předpřipravených DSM pro LS různých zařízení, systémů a aplikací rozličných výrobců [47]. Pokud potřebujeme přidat nový LS, pro který neexistuje DSM, můžeme si jej vytvořit sami v DSM editoru. Může se stát, že DSM pro požadovaný LS existuje, ale nerozpoznává všechny existující události. V takovém případě lze v QRadaru DSM doplnit rozšířením LSX (Log Source Extension). LSX je XML dokument, který se aplikuje na log source a doplňuje nebo může i přepsat DSM.

Parsování: syntaxe pro parsování je součástí DSM a LSX, nemusí být ale kompletní pro všechny atributy obsažené v události. Následující příklad (Obr. 19) znázorňuje konkrétní událost – povolený prostup na firewallu zařízení FortiGate, výrobce Fortinet. Tučně zvýrazněné jsou vyparsované atributy v rámci DSM. Níže v tabulce (Tab. 5) jsou uvedeny v levém sloupci názvy normalizovaných položek QRadaru a v pravém sloupci původní názvy atributů ze surových dat události (payload) zdrojového zařízení.

```
<185>date=2020-09-10 time=05:01:35 logid="0000000013"
type="traffic" subtype="forward" level="notice" vd="root"
eventtime=1599739296076496743 tz="-0700" srcip=192.168.14.111
srcport=54923 srcintf="internal" srcintfrole="lan"
dstip=192.168.14.112 dstport=80 dstintf="wan1" dstintfrole="wan"
srccountry="Reserved" dstcountry="Test Country" sessionid=53159
proto=6 action="close" policyid=1 policytype="policy"
poluuid="a9b81e06-c6a0-51e8-e434-a05c75d5ad74"
policyname="Internet_Access" service="HTTP" trandisp="snat"
transip=172.16.72.26 transport=54923 appid=17735
app="Facebook_Apps" appcat="Social.Media" apprisk="medium"
applist="default" duration=187 sentbyte=2333 rcvdbyte=2585
sentpkt=42 rcvdpkt=42 vwlid=6 vwlservice="Facebook-Instagram"
vwlquality="Seq_num(1 wan1), alive, sla(0x1), cfg_order(0),
cost(10), selected" utmaction="allow" countapp=1 sentdelta=1092
rcvddelta=780 utmref=65515-3302
```

Obrázek 19 DSM – příklad parsování FW události [48]

Tabulka 5 DSM - příklad normalizace FW události [48]

QRadar field name	Highlighted payload field name
Event ID	utmaction
Source IP	srcip
Source Port	srcport
Destination IP	dstip
Destination Port	dstport
Pre NAT Source IP	srcip
Pre NAT Source Port	srcport
Post NAT Source IP	transip
Post NAT Source Port	transport
Protocol	proto
Policy	policyid
Duration Seconds	duration
Device Time	date + time

Jak je vidět z příkladu, z payloadu nejsou vyparsovány všechny atributy události. Chceme-li při vyhledávání v Log Activity použít filtr nad vyhledáváním, který nám např. omezí oblast hledání jen na události FW prostupu dle kategorie aplikace, potřebujeme vyparsovat z payloadu také atribut „appcat“. K tomu slouží funkce v administraci pro vytváření vlastních položek (Custom Event Properties).

8.4 WinCollect agent

Specifickými zdroji logu jsou operační systémy MS Windows. Získávat logy z koncových stanic z OS Windows až na výjimky není potřeba. Naopak logy OS Windows Server (pokud se ve společnosti používají) jsou pro vyhodnocování událostí nezbytné. Windows ukládají své logy na disk do souboru ve speciálním formátu, který není přímo čitelný a nedá se jeho obsah bez instalace nástrojů třetích stran jednoduše zasílat např. syslogem. Přímo v OS lze

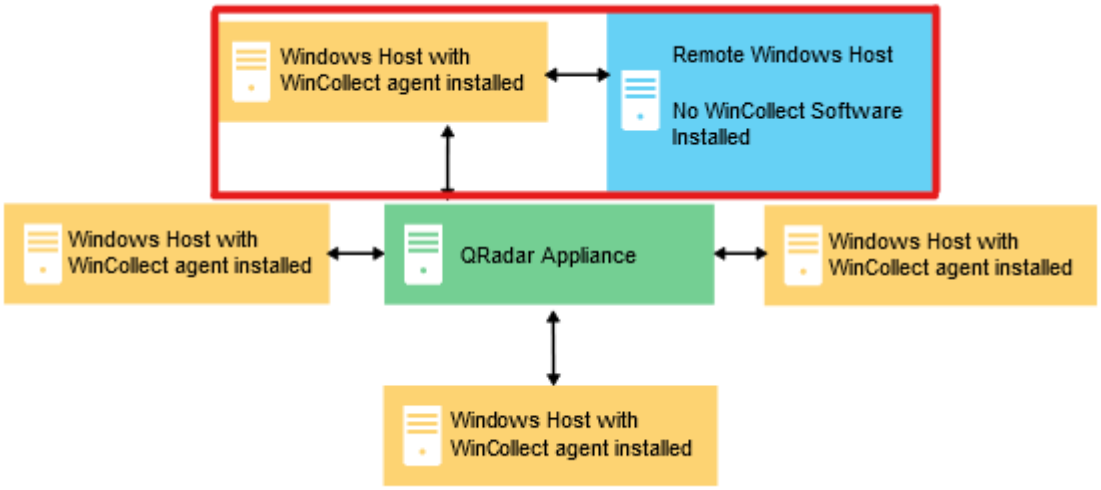
logy číst nativní aplikací Event Viewer, vzdáleně lze k logům přistupovat prostřednictvím Windows Event Log API [49].

8.4.1 WinCollect – způsoby nasazení

WinCollect agent je aplikace, která získává logy z OS Windows přes API a následně je zasílá syslogem do QRadaru. Pro koncové stanice i servery funguje stejný princip, dále však bude uvažován pouze Windows Server. Instalovat a provozovat WinCollect lze dvěma způsoby:

- přímo na jednotlivých serverech, z kterých chceme logy získávat. Z každého serveru jsou logy samostatně zasílány přímo do QRadaru,
- na speciálním serveru – kolektoru, který vzdáleně vyčítá logy ze všech požadovaných serverů. Na koncových serverech není WinCollect potřeba instalovat. Kolektor pak logy získané ze všech serverů přeposílá hromadně do QRadaru [50].

WinCollect může být přímo spravován z QRadar Console nebo může fungovat samostatně a nezávisle [50]. Pro účely této práce bude WinCollect spravován QRadarem, jak je vyznačeno níže (Obr. 20).



Obrázek 20 WinCollect spravován QRadarem, upraveno z: [50]

8.5 User Behavior Analytics

„Aplikace User Behavior Analytics pro QRadar (UBA) je nástroj pro detekování hrozeb plynoucích od interních pracovníků vaší organizace. Je postavena na vrcholu aplikačního rámce, tak aby za použití stávajících dat QRadaru vytvářela nový pohled na uživatele

a rizika. UBA přináší do QRadaru dvě hlavní funkce: profilování rizika a sjednocené identity uživatele.“ [2] [51]

UBA pracuje s logy QRadaru, avšak zcela nezávisle. Má vlastní konfiguraci, grafické uživatelské rozhraní i databázi. Jak je znázorněno ve funkčním schématu Příloha *P III: Funkční schéma rozšíření UBA* [52], pravidla v QRadaru (vytvořena automaticky při instalaci doplňku UBA) při sepnutí nad logy z různých LS vytvářejí speciální „sense“ události a offense, které obsahují rizikové skóre a další potřebné informace důležité pro UBA.

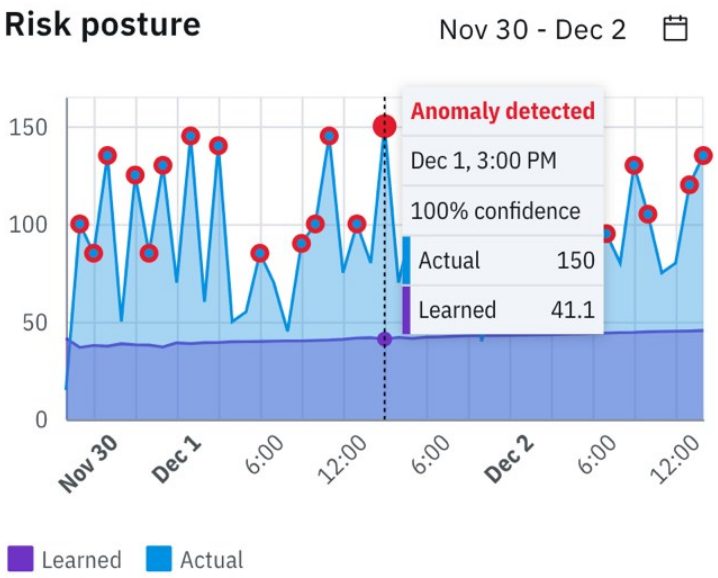
Profilování rizika uživatele: UBA informace ze „sense“ událostí přiřazuje k profilu uživatele ve své databázi. Agreguje rizikové skóre jednotlivých událostí a vytváří celkové rizikové skóre uživatele. Výsledky zobrazuje v grafickém rozhraní aplikace a zároveň jsou ukládány do databáze QRadaru jako události nebo offense (při překročení prahu rizikového skóre). UBA je tedy pro QRadar další LS.

Rizikové skóre uživatele se zvyšuje každou novou událostí, která je z QRadaru přijata a přiřazena uživateli. Rizikové skóre klesá postupně s časem, kdy nebyla pro uživatele detekována žádná další nová riziková událost.

Strojové učení: UBA lze rozšířit o analytický modul využívající strojového učení (Machine learning, dále ML). ML modul rozšiřuje možnosti profilování chování uživatelů v čase, na základě řady předpřipravených modelů. Např. model „Access activity“ sleduje všechny přístupy uživatele v rámci sítě a do informačních systémů (IS), a pro každou hodinu vytváří jeho model chování. Pokud se v budoucnu chování uživatele odchýlí od naučeného modelu, vytvoří se „sense“ událost, které zvýší celkové rizikové skóre uživatele.

Níže je na příkladu znázorněn graf metody „Risk posture“, která sleduje změnu celkové rizikovosti chování uživatele (Obr. 21). Fialovou barvou je zobrazené naučené chování uživatele v průběhu několika dní a světle modrou barvou aktuální chování uživatele. Vrcholy odchylek jsou označeny jako detekované anomálie – odchylky rizikovosti.

[2] The User Behavior Analytics for QRadar (UBA) app is a tool for detecting insider threats in your organization. It is built on top of the app framework to use existing data in your QRadar to generate new insights around users and risk. UBA adds two major functions to QRadar: risk profiling and unified user identities. (Vlastní překlad)



Obrázek 21 Příklad grafu metody Risk posture [53]

Sjednocení identity uživatele:

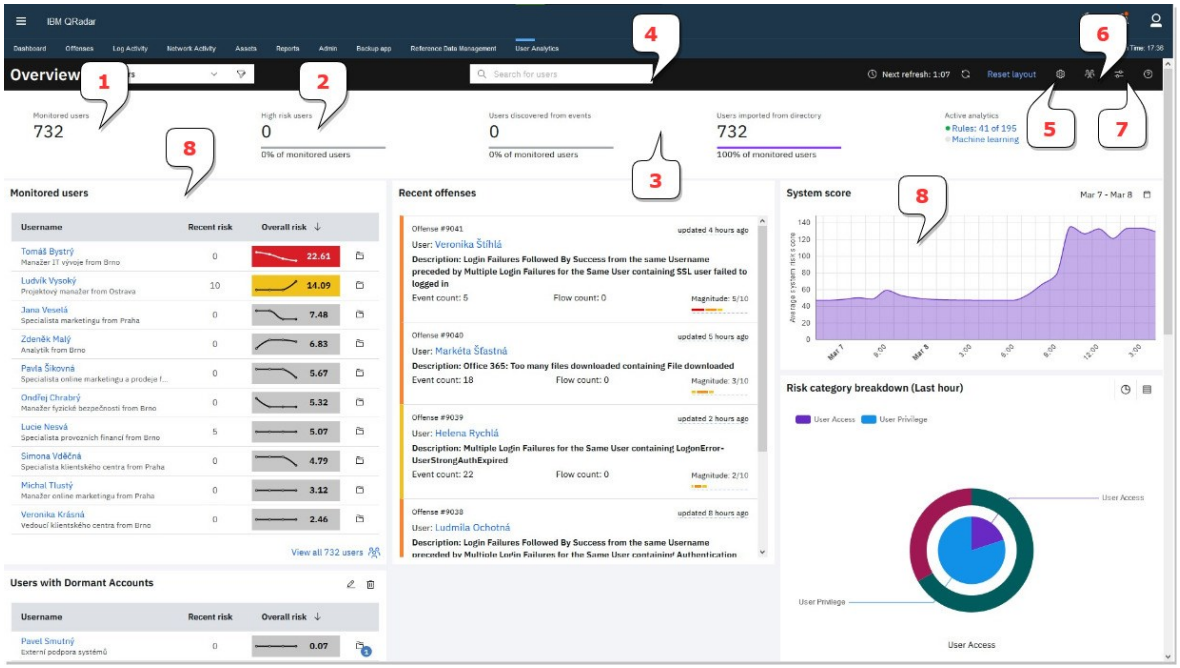
Uživatel často používá pro autentizaci do různých IS více identifikátorů. Např. ověření uživatele do IS vůči Active Directory může být provedeno za použití přihlašovacího údaje v různém tvaru:

- sAMAccountName,
- NetbiosName\sAMAccountName,
- sAMAccountName@dnsRoot,
- sAMAccountName@uPNSuffixes (uPNSuffixes může být více v jedné doméně).

V dalších IS může být pro autentizaci uživatele použita úplně jiná adresářová služba, kde má uživatel jiný tvar identifikátoru nebo může být řízení přístupu řešeno lokálně. UBA dokáže z logů různých LS vyčíst všechny tvary identifikátoru a přiřadit je jednomu konkrétnímu uživatelskému profilu.

8.5.1 Popis grafického rozhraní

Grafické uživatelské rozhraní UBA je stejně jako ostatní části QRadaru a doplňků vyvedeno webovou aplikací.



Obrázek 22 Rozšíření UBA – přehled (vlastní)

Na obrázku je znázorněno členění grafického rozhraní (Obr. 22), kde:

- **1** – počet monitorovaných uživatelů celkem,
- **2** – počet rizikových uživatelů,
- **3** – počet detekovaných a importovaných uživatelů,
- **4** – vyhledávací pole uživatelů,
- **5** – nastavení aplikace,
- **6** – nastavení importu uživatelů,
- **7** – nastavení a ladění pravidel,
- **8** – pracovní plocha: nastavitelné moduly aplikace.

8.6 Rozšíření

QRadar je možné rozšiřovat aplikacemi a doplňky, které se integrují do jeho webového grafického rozhraní. Rozšíření jsou stovky, od vývojářů IBM i třetích stran. Existují dvě základní metody získání a instalace vybraného doplňku:

- ruční stažení z IBM X-Force Exchange a instalace funkcí Extensions Management v administraci QRadaru,
- pomocí rozšíření IBM QRadar Assistant.

Dále popsaná rozšíření jsou těmi základními, které jsou zmiňovány v této práci.

8.6.1 IBM X-Force Exchange

X-Force Exchange je cloudová webová platforma určena pro odborníky zabývající se IT bezpečností. Jedná se o webovou aplikaci, která poskytuje aktuální informace o globálních bezpečnostních hrozbách a mnoho dalšího obsahu. Informace z X-Force Exchange lze získávat také automatizovaně prostřednictvím API. **App Exchange** je stránka webu, která obsahuje informace o všech rozšířeních QRadaru, umožňuje jejich stažení manuálně nebo rozšířením QRadar Assistant. Většina informací v X-Force Exchange je veřejně dostupná, připojení na API, stahování rozšíření QRadaru a některé další funkce vyžadují registraci. Některé funkce a přístup k vybraným informacím je k dispozici pouze na základě předplatného.

8.6.2 IBM QRadar Assistant

IBM QRadar Assistant zprostředkovává aktualizované informace o QRadaru, návody, doporučení a novinky z různých zdrojů výrobce:

- X-Force Exchange,
- IBM Learning Academy (školící centrum),
- stránky podpory produktu,
- komunitní fórum,
- YouTube kanál a další zdroje.

Další funkcí je možnost instalovat a spravovat rozšíření, jak již bylo zmíněno.

8.6.3 IBM QRadar Threat Intelligence

Rozšíření, které umožňuje získávat znalosti o hrozbách z informačních kanálů X-Force Exchange a ukládat je do datových struktur QRadaru. Může se jednat např. o URL phishingových stránek, IP adresy botnet počítačů apod.

8.6.4 IBM QRadar Pulse

Jedná se o užitečné rozšíření pro specialisty SOC. Na několika dashboardech je v reálném čase vizualizován celkový přehled o stavu QRadaru, aktuálních hrozbách působících na síť, přehled o offensích a další informace.

8.6.5 Backup app

Nativní zálohování QRadaru má omezené možnosti ukládání souborů záloh na vzdálená úložiště. Backup App efektivně monitoruje zálohovací proces a umožňuje přenášet kopie záloh různými protokoly (Samba, SFTP, SCP) a na různá datová úložiště v síti.

Dílčí závěr: kapitola v dostatečném detailu popisuje princip fungování nástroje IBM QRadar SIEM ve verzi All-in-One Virtual 3199, představuje jeho jednotlivé komponenty a doporučená rozšíření. Specialisté IT bezpečnosti si tak mohou utvořit představu o možnostech, které vybrané řešení nabízí a jak by jeho nasazení ve společnosti mohlo přispět k zajištění informační bezpečnosti.

9 NASAZENÍ ŘEŠENÍ IBM QRADAR SIEM

Cílem kapitoly je popsat nasazení a konfiguraci QRadar SIEM v jeho hlavních bodech se zaměřením na správnou konfiguraci LS na straně monitorovaného systému i QRadaru a s důrazem na osvědčené postupy. Kompletní popis konfigurace všech částí řešení by svým rozsahem výrazně přesahoval možnosti této práce.

V práci bude u pojmenování různých hodnot nastavení a pravidel používán prefix **BP** (bakalářská práce).

9.1 Přípravná fáze

Prvním krokem je zajistit všechny předpoklady pro nasazení QRadaru, jak je popsáno v kapitole *6 Technické předpoklady pro nasazení SIEM*. V podkapitolách je upřesněno konkrétní zjednodušené nastavení modelové instalace.

Po přípravné fázi následuje vlastní instalace binárních souborů aplikace na připravený virtuální systém formou průvodce, který zde není třeba popisovat. Součástí průvodce instalací je i zadání IP adresy serveru, FQDN a SMTP serveru pro odesílání e-mailových zpráv.

9.1.1 Příprava sítě

Pro modelový příklad budou použity parametry prostředků v síti dle přílohy *P IV: Modelová tabulka síťových prostředků*. Předpokládá se, že v reálném nasazení je u všech kritických prvků zajištěna vysoká dostupnost a řešení se rozprostírá ve více lokalitách, což znásobuje potřebný počet IP adres. V modelové situaci je použita vždy jen jedna IP adresa pro konkrétní zařízení / službu, což bude pro demonstraci postupů v této práci dostačující.

Síťové prostupy z VLAN určené pro SIEM a další bezpečnostní nástroje jsou nastaveny následovně (Tab. 6).

Tabulka 6 Síťové prostupy pro QRadar a WinCollect, data čerpána z: [34], [54]

Popis	**Zdroj**	**Cíl**	**Port**
QRadar -> DC, LDAPS pro bind do AD, DNS dotazy	10.0.50.1/32	10.0.20.1/32	TCP 636 TCP/UDP 53

Popis	Zdroj	Cíl	Port
QRadar -> SMTP pro zasílání e-mailů	10.0.50.1/32	10.0.20.3/32	TCP 25
QRadar -> NTP pro synchronizaci času	10.0.50.1/32	10.0.20.4/32	UDP 123
QRadar -> internet pro vyčítání logů z API cloudu a připojení k API X-Force Exchange	10.0.50.1/32	Internet	TCP 443
QRadar -> LS pull metoda viz tabulky v kapitole *6.3 Způsob vyčítání LS*	10.0.50.1/32	10.0.20.0/24 10.0.30.0/24 10.0.40.0/24	TCP 443, 445, 5432
WinCollect – LS MS Windows OS	10.0.50.2/32	10.0.20.0/24 10.0.30.0/24	TCP 135, 139, 445, 49152–65535 UDP 137, 138
LS push metoda -> QRadar	10.0.10.0/24 10.0.20.0/24 10.0.30.0/24 10.0.40.0/24 10.0.100.0/24	10.0.50.1/32	TCP/UDP 514
Uživatelé -> QRadar, web GUI	10.0.60.0/23 10.0.70.0/23	10.0.50.1/32	TCP 443
Pracovníci IT bezpečnosti / SOC -> Bezpečnostní servery	10.0.60.0/23 10.0.70.0/23 + identita	10.0.50.0/24	TCP 22, 443, 445, 3389, ICMP
Monitorovací nástroj (SNMP)	10.0.20.6/32	10.0.50.1/32	TCP 10161

Poznámky:

- dostupnost DHCP pro získání IP adresy zajišťuje funkce DHCP relay,
- QRadar, WinCollect a datové úložiště pro zálohy QRadaru jsou ve stejné VLAN.

9.1.2 Příprava účtů

QRadar bude používat následující technické účty (Tab. 7), které budou zavedeny v AD.

Tabulka 7 Technické účty pro QRadar

Název	Účel
qradar_ad_bind	Dotazy do AD pro ověření uživatele ve vlastním uživatelském managementu a pro import uživatelů do nástroje UBA.
qradar_ls_ro	Účet pro vyčítání LS metodou pull.
qradar_wc_ro	Účet pro vyčítání LS prostřednictvím WinCollectu.

9.1.3 Příprava virtualizace

Virtualizované HW nároky zvoleného řešení byly stanoveny následovně (Tab. 8).

Tabulka 8 QRadar – stanovené HW nároky

Parametr	Hodnota
CPU	2 x 9 jader
Paměť RAM	128 GB
Pevný disk 1 (OS, aplikace a služby)	300 GB, SSD úložiště, RAID 10
Pevný disk 2 (databáze)	6 TB, SAS úložiště, RAID 6
Síťové připojení	1x připojení k distribuovanému switchi
Vysoká dostupnost	vSphere High Availability

9.2 Základní konfigurace

V prvním kroku konfigurace, po instalaci QRadar aplikace na serveru, je třeba provést základní nastavení systému.

9.2.1 Vytvoření uživatelských rolí a bezpečnostních profilů

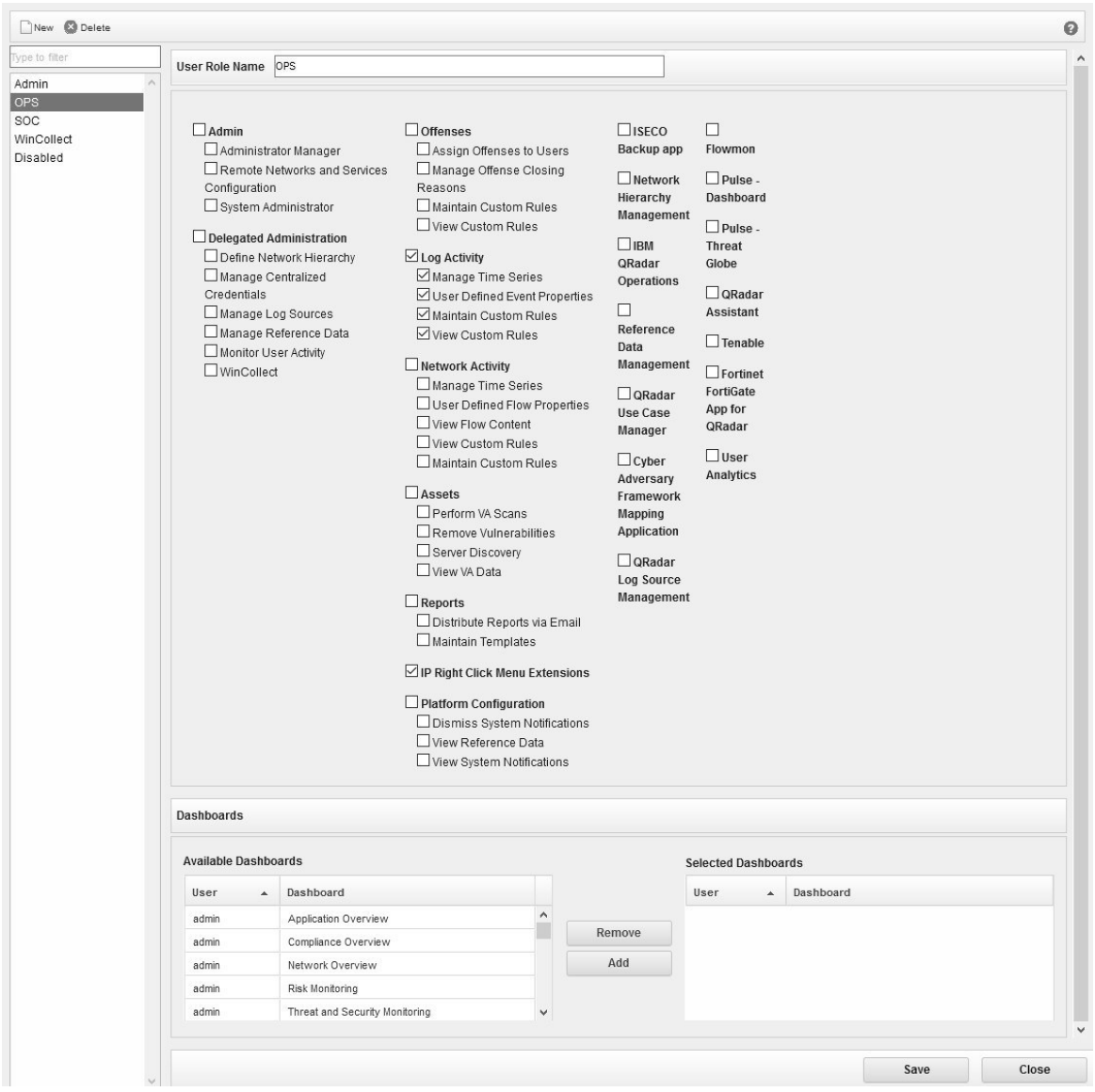
Ve výchozím nastavení obsahuje uživatelský management pouze účet správce (Admin) s nejvyšším oprávněním (Admin) a neomezeným profilem (All). Protože QRadar může sloužit nejen pro potřeby specialistů IT bezpečnosti, SOC, ale i pro IT administrátory, je

vhodné vytvořit více uživatelských rolí a bezpečnostních profilů. Nastavení se provádí v administraci QRadaru: *Menu* > *Admin*.

User Roles: uživatelské role slouží k definování oprávnění pro jednotlivé funkce QRadaru. Pro správce SIEM je vhodná výchozí role Admin. Byly vytvořeny další dvě role pro specialisty SOC a administrátory provozních systémů:

- **SOC**: všechny funkce a dashboardy, kromě administrace,
- **OPS**: pouze přístup k logům, kontextovým nabídkám.

Na příkladu nastavení role OPS jsou vidět všechny možnosti nastavení oprávnění (Obr. 23).



Obrázek 23 QRadar - User Role (vlastní)

Role WinCollect a Disabled jsou stejně jako Admin výchozí role, jejichž funkce bude popsána dále.

Security Profiles: bezpečnostní profily omezují přístup uživatelů k vybraným logům. Omezení se dá aplikovat dle jednotlivých LS či skupin LS, dle zdrojových a cílových sítí nebo v kombinaci. Pro administrátory provozních systémů je vhodné vytvořit profily, které umožní přístup pouze k provozním logům systémů, které spravují.

9.2.2 Připojení k adresářové službě

Přístup do všech aplikací a systémů je vhodné ověřovat vůči některé adresářové službě. Zvolena byla adresářová služba Active Directory (AD), ktera je součástí řadiče domény, kterou jsem zvolil pro test – **bp-test.cz** (tato doména není registrována a je použita pouze v lokální síti pro účely této práce). V AD byly vytvořeny následující objekty.

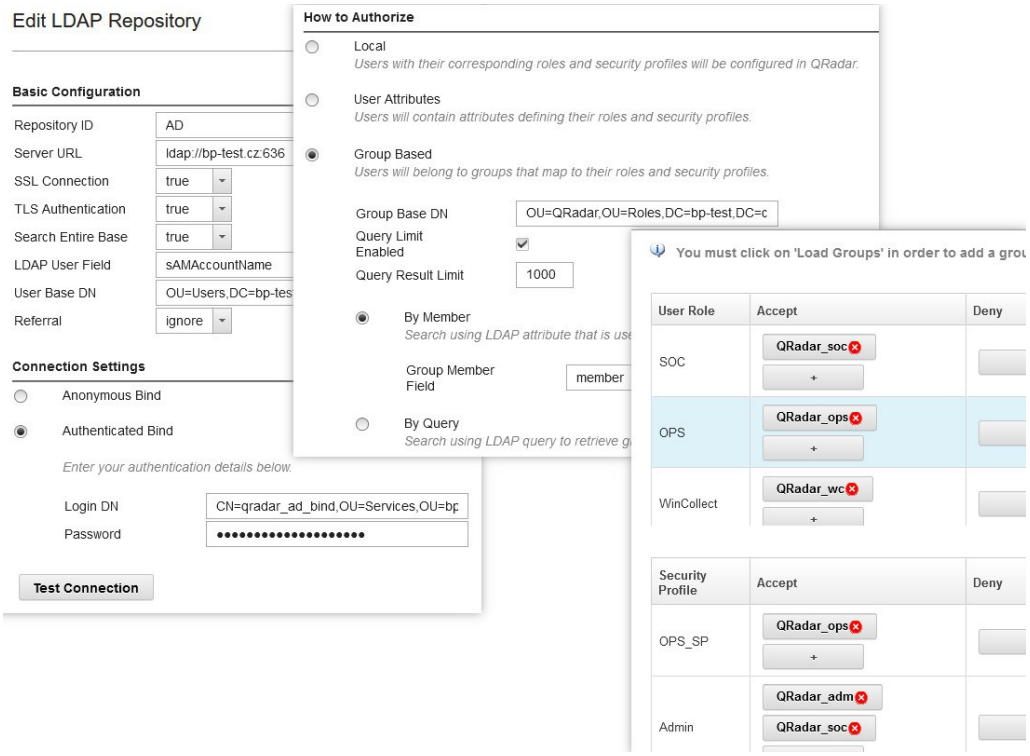
Organizační jednotka:

- OU=QRadar,OU=Roles,DC=bp-test,DC=cz.

Skupiny zabezpečení:

- CN=QRadar_adm,OU=QRadar,OU=Roles,DC=bp-test,DC=cz,
  slouží pro specialisty IT bezpečnosti, kteří spravují SIEM,
- CN=QRadar_soc,OU=QRadar,OU=Roles,DC=bp-test,DC=cz,
  slouží pro specialisty IT bezpečnosti, kteří obsluhují SIEM,
- CN=QRadar_ops,OU=QRadar,OU=Roles,DC=bp-test,DC=cz,
  slouží pro administrátory provozních systémů,
- CN=QRadar_disabled,OU=QRadar,OU=Roles,DC=bp-test,DC=cz,
  technická skupina pro potřeby QRadaru,
- CN=QRadar_wc,OU=QRadar,OU=Roles,DC=bp-test,DC=cz,
  technická skupina pro potřeby QRadaru.

Konfigurace autentizace se provádí v administraci QRadaru: *Menu > Admin > System Configuration > User Management > Authentication > Authentication Module Settings*. Po přepnutí volby ze *System Authentication* na *LDAP* umožníme konfiguraci ověření vůči AD zabezpečeným protokolem LDAPS (Obr 24). Funkčnost připojení k AD provedeme tlačítkem *Test Connection* a následně provedeme načtení skupin vytvořených v AD tlačítkem *Load Groups*. Ve zobrazené tabulce provedeme spárování rolí a profilů v QRadaru se skupinami zabezpečení v AD.



Obrázek 24 QRadar – autentizace (vlastní)

9.2.3 Nastavení SMTP

Z QRadaru budeme chtít odesílat upozornění e-mailem, jako odezvu na sepnutá pravidla nebo zasílat naplánované reporty. FQDN a port SMTP serveru se zadává v administraci: *Admin > System Configuration > System and License Management > View and Manage System* (kontextová nabídka) > *Email Server*. Hodnota bude ve tvaru: smtp.bc-test.cz:25. Adresa odesílatele se nastavuje na jiném místě administrace: *Admin > System Configuration > System Settings > Alert Email From Address*.

9.2.4 Přiřazení licence

Jedna z položek ceny QRadar SIEM je licence za počet EPS a FPS. Zakoupená licence je poskytnuta formou licenčního klíče. Jedná se o zašifrovaný soubor s příponou .key. Licenční klíč vložíme do QRadaru v administraci: *Admin > System Configuration > System and License Management > Upload License*. následně je nutné v nabídce: *License Pool management* alokovat EPS a FPS mezi jednotlivé hostitele SIEM řešení. V případě QRadar All-in-One existuje pouze jeden hostitel, tedy alokujeme na něj veškeré licenční prostředky.

9.2.5 Nastavení retence logu

Dle kapitoly *6.1 Analýza aktiv* bychom měli mít ke každému LS informaci o jeho retenci. Tedy znalost, jak dlouho chceme logy uchovat. V QRadaru lze nastavit výchozí retenci pro všechny logy a u vybraných logů nastavit individuální hodnoty. Kromě výchozího nastavení je k dispozici dalších deset, pro které lze nastavit různé politiky. Nastavení se provádí v administraci: *Admin* > *Data Sources* > *Event Retention*. U každé politiky je následující nastavení:

- **Keep data placed in this bucket for**: celková zaručená doba zachování logů,
- **Allow data in this bucket to be compressed**: po jaké době se mají logy v databázi začít komprimovat. Toto nastavení má vliv na rychlost prohledávání logů. Prohledávání nekomprimovaných logů je rychlejší,
- **Delete data in this bucket**: volíme, zda chceme aby byly logy po nastavené době ihned smazány nebo se začaly mazat až ve chvíli nedostatku místa na disku,
- **Current Filters** (není u výchozího nastavení): zde definujeme filtr, na které logy se má politika aplikovat.

Každá retenční politika zajistí ukládání dat do jiného souboru. To lze s výhodou využít např. při požadavku na rozdílnou archivaci dat pro určité typy logů (např. legislativní důvody).

Politiky se zpracovávají postupně z vrchu dolů. Bylo provedeno následující nastavení (Obr. 25).

Order	Name	Retention	Compression	Deletion Policy	Filters	Distribution	Enabled	Creation Date	Modification ...
1	Business apps [ID: 1]	2 years	After 1 month	Immediately ...	Log Source is BssApp| ba.bp-test.cz @ 10.0.2...	0%	true	3. 1. 2021 10:...	3. 1. 2021 10:...
2	Exchange MSGTR [I...	2 years	After 1 week	Immediately ...	Log Source Type is Microsoft Office 365 Mess...	<1%	true	3. 1. 2021 10:...	3. 1. 2021 10:...
3	PROD DB [ID: 3]	2 years	After 1 week	Immediately ...	Log Source is DB PROD | db.bc-test.cz @ 10....	<1%	true	3. 1. 2021 10:...	3. 1. 2021 10:...
4				Immediately ...		0%	false		
5				Immediately ...		0%	false		
6				Immediately ...		0%	false		
7				Immediately ...		0%	false		
8				Immediately ...		0%	false		
9				Immediately ...		0%	false		
10				Immediately ...		0%	false		
	[DEFAULT]	**1 year**		**Immediately ...**		**99%**		**6. 9. 2020 10:...**	**16. 9. 2020 1...**

Obrázek 25 QRadar - nastavení retence logů (vlastní)

V databázi QRadaru jsou uloženy nejen zpracované události, ale i různá metadata. Např. pro urychlení vyhledávání lze nastavit indexaci zvolených atributů. Ukládají se i výsledky hledání, akumulovaná data pro reporty, grafy a samozřejmě vytvořené offense. Retenci těchto metadat nastavíme v administraci: *Admin* > *System Configuration* > *System Settings* > *Database Settings* a *Ariel Database Settings*.

9.2.6 Nastavení zálohování

SIEM je aktivum s vysokou hodnotou, což je nutné zohlednit i při jeho zálohování. V SIEM jsou zpravidla uchovávány logy mnohem déle, než v systémech, které je generují. Strategie zálohování musí být tedy vhodně navrhnuta také s ohledem na velikost dat. Strategie zálohováni pro QRadar byla navrhnuta následovně (Tab. 9):

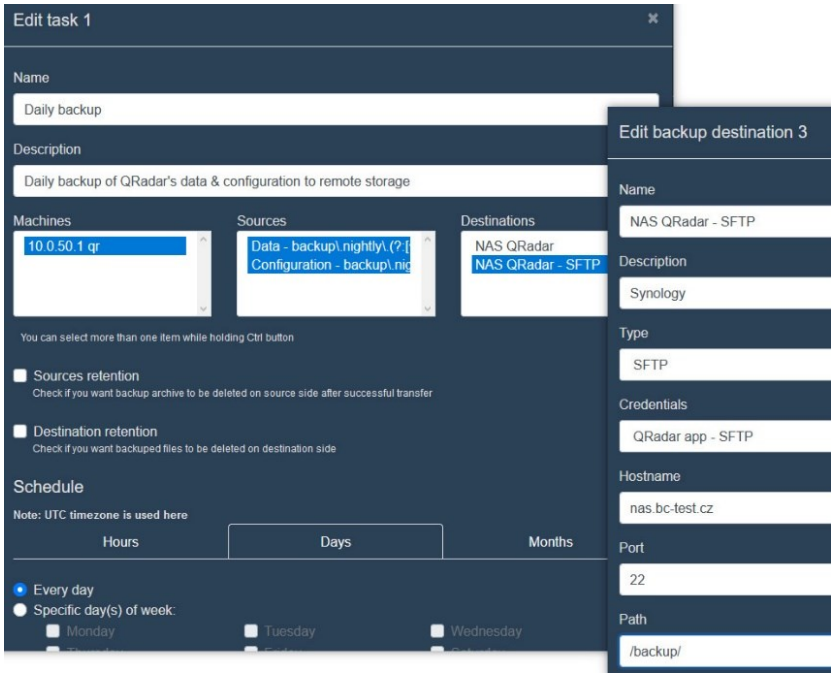
Tabulka 9 QRadar - strategie zálohování

Č.	**Typ**	**Obsah**	**Umístění**	**Popis**	**Plán**	**Retence**
1	Plná záloha	Data Konfigurace	Místní diskové úložiště	Pro rychlé obnovení	Denně	7 dní
2	Plná záloha	Data Konfigurace	Vzdálené síťové úložiště	Dlouhodobé uložení (roky)	Denně	Při 90% zaplnění
3	Obraz VM	Obraz celého zařízení Konfigurace VM	Diskové úložiště zálohovacího serveru	Pro rychlé obnovení celého zařízení	Týdně	1 měsíc
4	Obraz VM	Obraz celého zařízení Konfigurace VM	Pásková jednotka	Uchování na páskách v trezoru mimo objekt	Týdně	14 dní

Nastavení zálohování č. 1 se provádí v administraci QRadaru: *Admin > System Configuration > Backup and Recovery*. Kromě cesty k datovému úložišti pro zálohy a retence lze zvolit:

- co chceme zálohovat (konfiguraci, data),
- co mají obsahovat data zálohy (události, síťové flow) a to u každého hostitele,
- časový limit pro zálohy a prioritu procesu zálohování.

Zálohování č. 2 je nastaveno za použití rozšíření Backup app (Obr. 26), které má široké konfigurační možnosti.



Obrázek 26 QRadar – zálohování (vlastní)

9.2.7 Připojení WinCollectu

Jak již bylo zmíněno, WinCollect bude spravován přímo QRadarem. Vzhledem k tomu, že WinCollect i QRadar budou umístěny ve stejné VLAN, není třeba vytvářet žádné síťové prostupy na firewallu. HW nároky na instalaci serveru pro WinCollect nejsou velké a odvíjejí se opět především od počtu přijímaných EPS. V navrhnutém řešení byl vytvořen virtuální server s následujícími parametry (Tab. 10).

Tabulka 10 WinCollect - stanovené HW nároky

Parametr	**Hodnota**
CPU	8 jader
Paměť RAM	8 GB
Pevný disk 1 (OS, aplikace a služby)	80 GB, SSD úložiště, RAID 10
Síťové připojení	1x připojení k distribuovanému switchi
Vysoká dostupnost	vSphere High Availability
OS	MS Windows Server 2019 Datacenter

Prvním krokem je instalace podpory WinCollectu do uživatelského rozhraní QRadaru, nahráním, připojením (mount) balíčku typu SFS a spuštěním instalátoru. Tento proces je detailně popsán v dokumentaci IBM [55]. Po dokončení instalačního procesu bude v GUI v administraci dostupná položka pro konfiguraci WinCollectu.

Dalším krokem je spuštění binárního instalačního souboru (WinCollect Agent.exe), na připraveném virtuálním serveru. Je třeba v několika krocích zadat potřebné údaje, především IP QRadaru a port, kam se mají přeposílat logy stažené z jednotlivých Windows LS a autentizační token pro komunikaci s QRadarem. Autentizační token se vytváří v administraci QRadaru: *Admin* > *System Configuration* > *User Management* >*Authorized Services* > *Add Authorized Service*. V poli *User Role* musí být nastavena hodnoto WinCollect a v poli *Security Profile* hodnota Admin. Token lze po vytvoření vyzvednout po vybrání řádku v hlavním okně tohoto nastavení (Obr. 27).

Add Authorized Service | Delete Authorized Service | Edit Authorized Service Name | Selected Token: 32db8954-6844-0237-4c11-45a5de6f67bb

Service Name	Authorized By	Authentication Token	User Role	Security Profile	Created	Expires
UBA	tomas.dobry	9875ccd5-2302-fff9-9...	Admin	Admin	6. 5. 2020 11:22:14	Permanent
WinCollect	admin	32db8954-6844-0237...	WinCollect	Admin	5. 9. 2019 19:47:17	Permanent
ISECO Backup App	admin	458d5bc2-297a-1451...	Admin	Admin	10. 9. 2019 16:13:08	Permanent
QRadar Assistant	jan.chytry	778a90ee-5cc5-0398-...	Admin	Admin	22. 10. 2019 15:18:37	Permanent
QRadar Use Case Ma...	tomas.dobry	99841caa-d4ee-1719-...	Admin	Admin	12. 12. 2019 10:12:17	Permanent

Obrázek 27 QRadar - autentizční tokeny, anonymizováno (vlastní)

Po instalaci WinCollect Agenta jej QRadar automaticky detekuje. Kontrolu provedeme v administraci: *Admin* > *Data Sources* > *WinCollect*. V této nabídce můžeme upravit konfiguraci, např. interval pro zasílání konfigurace nebo povolení automatických aktualizací agenta.

9.2.8 Další konfigurace

Pro lepší přehled, členění a práci s aktivy je dobré vytvořit v QRadaru hierarchii sítí a skupiny LS. Je na každém, do jakých logických bloků členění provede. Osvědčeným postupem je sítě členit dle adres sítí a podsítí. Skupiny by měly mít možnost shlukovat LS např, dle jejich klasifikace (test / produkce / vývoj) a funkce (operační systémy / aplikace / aktivní prvky a jejich podkategorie). Nastavení se provádí v administraci: *Admin* > *System Configuration* > *Network Hierarchy* (sítě) a *Admin* > *Data Sources* > *Log Source Groups* (skupiny LS).

9.3 Konfigurace LS

Konfigurace zdrojů logů pro příjem událostí do QRadaru je stěžejní část konfigurace, a to nejen v počáteční fázi nasazení SIEM, ale i v průběhu celé jeho životnosti. Jak již bylo popsáno, QRadar poskytuje stovky předpřipravených DSM pro různé druhy systémů a aplikací. V následujících příkladech bude popsána konfigurace nejčastěji připojovaných LS. V QRadaru se konfigurace provádí v administraci: *Admin > Data Sources > Log Sources* nebo přímo spuštěním aplikace IBM QRadar Log Source Management.

Obecně lze u každého LS v QRadaru v závislosti na jeho typu nastavit:

- **Name**: dle názvu lze LS vyhledávat při různých činnostech v QRadaru, dle osvědčených postupů je dobré v názvu uvést kromě obecného názvu i název hostitele a IP adresu. Příklad názvu: Core switch – sw.bc-test.cz @ 10.0.10.2,
- **Description**: vyhledávání funguje i na toto pole. Můžeme zde uvést detailnější popis zdroje logu,
- **Log Source Type**: typ LS. Odpovídá DSM pro konkrétní typ logů a ovlivňuje další pole nastavení,
- **Protocol Type**: každý typ LS může mít více možností, jakým způsobem bude do QRadaru přijímán. Např. syslogem, přes WinCollect nebo vyčítáním ze souboru,
- **Enabled**: během času vznikají nové zdroje logů a jiné naopak zanikají. Osvědčeným postupem je LS neodstraňovat, ale pouze je v konfiguraci vypnout,
- **Groups**: pokud jsme si pro LS vytvořili skupiny, zde je můžeme přiřadit,
- **Extension**: slouží pro výběr LSX, viz kapitola *8.3.1 DSM a LSX*,
- **Language**: doporučuji ponechat anglický jazyk,
- **Target Event Collector**: pokud bychom měli více kolektorů, tímto nastavením určíme, který bude logy ze zdrojového systému přijímat,
- **Credibility**: je jedním ze vstupů pro výpočet závažnosti při generování offensí,
- **Coalescing Events**: důležitý parametr, který může snížit velikost ukládaných dat v databázi. Pokud je tato volba zapnutá, bude QRadar v případě, že přijde ze zdroje více stejných událostí v krátkém čase, ukládat pouze jednu a zapíše jejich počet. U důležitých LS je užitečné tuto volbu vypnout,
- **Store Event Payloads**: určuje, zda bude do databáze ukládán celý payload příchozí události nebo jen vyparsované hodnoty. Z praktických zkušeností se dá tvrdit, že payload je ve většině případů při vyšetřování bezpečnostních událostí potřeba,

- **Log Source Identifier**: identifikátor, dle kterého QRadar rozpoznává, kterému LS má příchozí události přiřadit. Zpravidla se jedná o IP adresu nebo název hostitele, ze kterého události přicházejí.

Ostatní nastavení se mění dle zvolené kombinace Log Source Type a Protocol Type. V příkladech jsou použity hodnoty a nastavení dle přílohy *P IV: Modelová tabulka síťových prostředků*.

9.3.1 Linux OS

Konfigurace na straně zdroje logů: V závislosti na použitém Linux OS je provedena konfigurace syslogu:

- úprava konfiguračního souboru syslogu v cestě: /etc/rsyslog.conf,
- zapsání hodnoty: authpriv.* @@qr.bc-test.cz:514, pro zasílání do QRadaru.

Konfigurace na straně QRadaru: syslog LS je typu pull. Tzn. po konfiguraci na straně zdroje logů QRadar automaticky detekuje příchozí logy a vytvoří pro něj LS. Jeho název v aplikaci Log Source Management bude např.: LinuxServer @ mon.bc-test.cz. V případě Linux OS bude veškeré nastavení automaticky detekováno a nastaveno. Bude třeba pouze upravit název a popis LS, dle zvolené konvence, případně upravit další parametry:

- **Name**: Linux - mon.bc-test.cz @ 10.0.20.6.

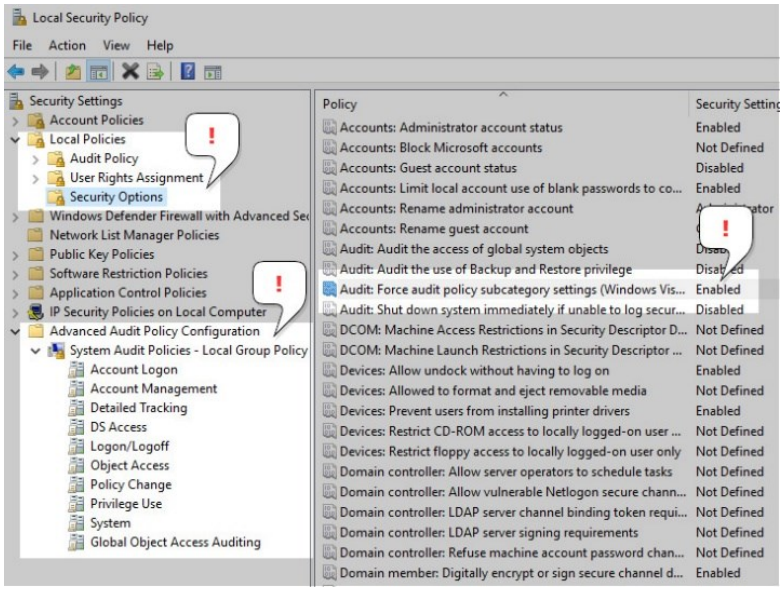
9.3.2 Windows OS

Konfigurace na straně zdroje logů: ve Windows je potřeba povolit a nastavit (nejlépe využitím skupinových politik – GPO, hromadně na všech monitorovaných serverech) politiky pro generování událostí. Nastavení logování je v systému Windows velice podrobné a může se lišit pro různé funkce serverů. Jiná politika bude např. pro doménový řadič a pro souborový server.

Od verze Windows Server 2008 dále je v politice využito nastavení v uzlu s názvem: *Advanced Audit Policy Configuration*. Aby na toto nastavení byl brán zřetel, musí být povolena politika: *Audit: Force audit policy subcategory settings* (Obr. 28).

Logování operačního systému Windows lze povýšit na vyšší úroveň instalací nástroje Sysmon, který je součástí Windows Sysinternals „z dílny“ Marka Russinoviche, CTO společnosti Microsoft. Tento nástroj poskytuje detailní informace o všech spouštěných procesech, síťových připojeních a operacích se soubory. Události jsou zapisovány do

Windows event logu [56]. IBM Sysmon přímo podporuje a na IBM X-Force Exchange poskytuje ke stažení QRadar Content Extension for Sysmon, což je rozšiřující balíček nastavení a pravidel pro QRadar [57].



Obrázek 28 Windows – auditní politiky (vlastní)

Na serveru je dále třeba nastavit účet pro vyčítání Event Logu:

- **účet**: qradar_wc_ro@bc-test.cz,
- **členem lokální skupiny**: Event Log Readers.

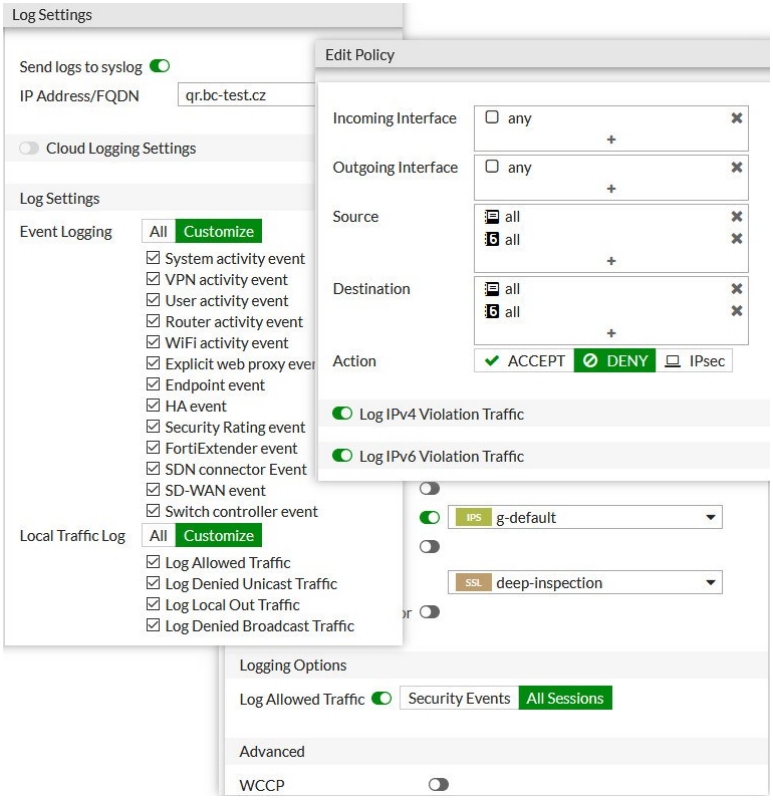
Konfigurace na straně QRadaru: jedná se o speciální typ push LS, je tedy třeba v QRadar Log Source Management nejprve vytvořit konfiguraci. V poli *Log Source Type* vybereme položku: Microsoft Windows Security Event Log a v poli *Protocol Type*: WinCollect. V konfiguraci protokolu je potřeba mimo jiné definovat následující specifické parametry:

- **Domain / User Name / Password**: údaje nutné pro autentizaci na systému, z kterého chceme vyčítat logy. Naše zvolené uživatelské jméno: qradar_wc_ro a doména: bc-test.cz,
- **Polling Interval** (ms): interval pro vyčítání logů,
- **Event Log Poll Protocol**: výběrem MSEVEN6 získáme z logu více informací,
- **Standard Log Types**: zapnutím jednotlivých voleb určíme, které logy chceme vyčítat. Ve většině případů se zapíná pouze volba Security,
- **XPath Query**: definováním XPath můžeme vybírat pouze části logů, které nás zajímají a které budeme vyčítat. XPath dotaz se zasílá zdrojovému systému. Používá se také v souvislosti se Sysmonem,

- **Log Filter (Type)**: sada nastavení, kterými je možné filtrovat vyčtené události, před jejich zpracováním,
- **Event Types**: zapnutím jednotlivých voleb zvolíme úroveň kritičnosti logů, které chceme vyčítat,
- **WinCollect Agent**: vybereme WinCollect agenta, který má logy ze zdrojového systému vyčítat.

9.3.3 FW log

Konfigurace na straně zdroje logů: většina síťových prvků vč. firewallů zasílá logy prostřednictvím syslogu. Na straně firewallu tedy stačí zadat IP adresu nebo FQDN QRadaru a v nastavení upravit úroveň logování nebo vybrat jednotlivé typy logů. Politiku logování FW je třeba vhodně navrhnout a nastavit pro jednotlivá FW pravidla, vč. výchozího (Obr. 29).



Obrázek 29 Firewall – příklad nastavení logování (vlastní)

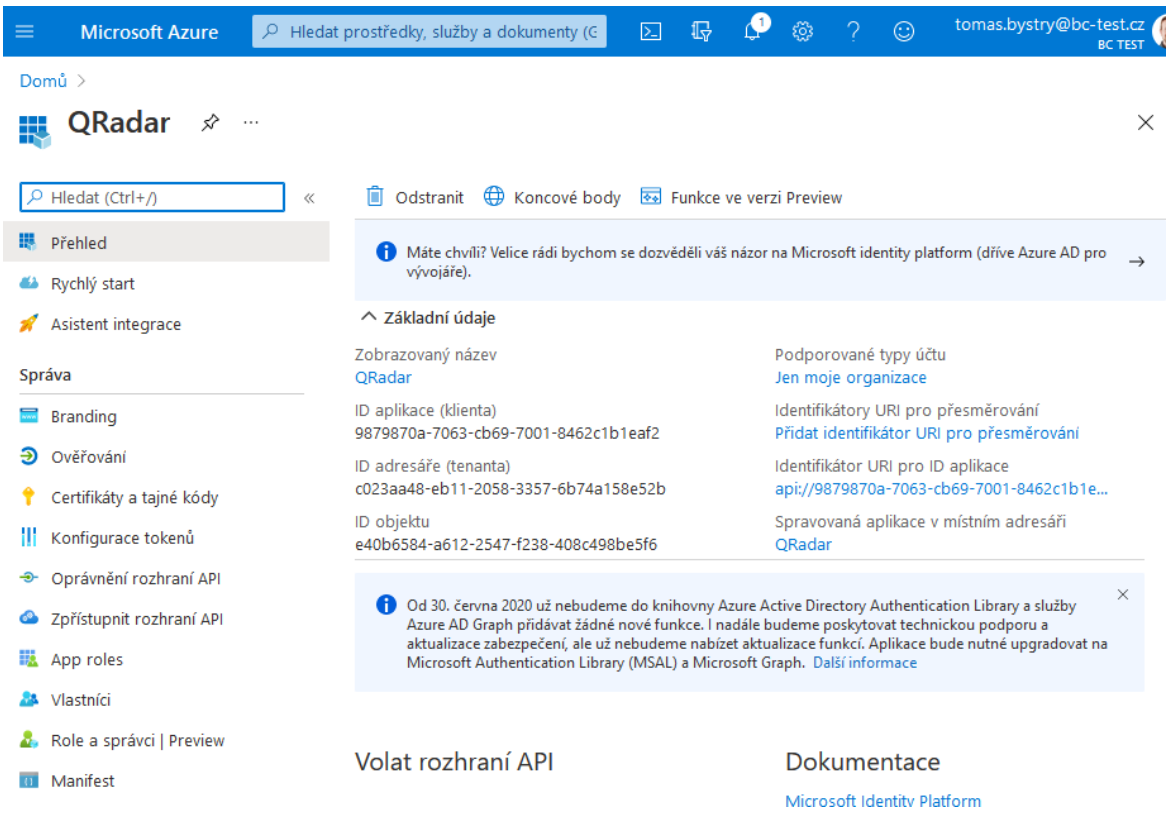
Konfigurace na straně QRadaru: platí to stejné, jako pro ostatní syslog LS. Pokud má QRadar k dispozici DSM pro daný firewall, ale byl špatně detekovaný, upravíme nastavení a zvolíme správný *Log Source Type*. V našem případě: Fortinet FortiGate Security Gateway.

9.3.4 Cloud – Office 365

Pro ukázku nastavení vyčítání logů za použití API byl vybrán MS Office 365, který je ve velké míře používán společnostmi všech velikostí a oborů. Nezřídka zaměstnanci tráví většinu svého času právě používáním služeb a aplikací v rámci balíku Office 365.

Konfigurace na straně zdroje logů: logy lze získávat připojením na Office 365 Management API. K připojení musíme znát ID aplikace, ID tenanta a tajemství (client secret). Obecný postup je následující:

- kontrola nebo zapnutí auditování v administraci Office 365, konkrétně v: *Compliance centre* > *Search* > *Audit log search*,
- registrace nové aplikace v Azure Active Directory,
- získání všech ID a tajemství (Obr. 30),
- přidání oprávnění číst události (ActivityFeed.Read, ActivityReports.Read…).



Obrázek 30 Azure AD – registrace aplikace v API (vlastní)

Konfigurace na straně QRadaru: vytvořit nový LS typu Microsoft Office 365, *Protocol Type*: Office 365 REST API a v nastavení protokolu doplnit údaje získané z Azure AD:

- **Client ID**: 9879870a-7063-cb69-7001-8462c1b1eaf2,
- **Client Secret**: tajný kód klienta,

- **Tenant ID**: c023aa48-eb11-2058-3357-6b74a158e52b.

V části nastavení *Event Filter* lze vybrat, které logy Office 365 chceme přijímat. V nabídce na první pohled chybí logy pro trasování zpráv elektronické pošty. Office 365 REST API tyto logy neposkytuje, je nutné je získávat z Message Trace API, které funguje samostatně. V QRadaru se jedná o *Log Source Type*: Microsoft Office 365 Message Trace.

9.3.5 DHCP

Jedním z LS, které je nutné vyčítat přímo ze souboru uloženého na disku, je MS DHCP Server.

Konfigurace na straně zdroje logů: na serveru se logy IPv4 DHCP nacházejí obvykle v cestě:

- **IPv4 DHCP**: %WINDIR%\system32\dhcp\DhcpSrvLog-<zkratka dne>.log,
- **IPv6 DHCP**: %WINDIR%\system32\dhcp\DhcpV6SrvLog-<zkratka dne>.log.

Složku s logy je nutné nasdílet účtu určenému pro vyčítání. Můžeme použít stejný účet, jako v případě WinCollectu:

- **účet**: qradar_wc_ro@bc-test.cz,
- **oprávnění**: jen pro čtení.

Konfigurace na straně QRadaru: k DHCP serveru se budeme připojovat napřímo, tomu odpovídá nastavení:

- **Name**: DHCP – dhcp.bc-test.cz @ 10.0.20.2,
- **Log Source Type**: Microsoft DHCP Server,
- **Protocol Type**: Microsoft DHCP Server,
- **Log Source Identifier a Server Address**: dhcp.bc-test.cz,
- **Domain**: bc-test.cz,
- **Username**: qradar_wc_ro,
- **Folder Path**: název sdílené složky.

Ostatní hodnoty mohou zůstat ve výchozím nastavení.

9.3.6 Databáze

Konfigurace na straně zdroje logů: konfigurace závisí na typu databázového serveru a na jeho nastavení. Zde uvedený příklad bude demonstrovat nastaveni auditu PostgreSQL

databáze (audit trail) a zasílání událostí syslogem. Pro detailnější logování je použito open source rozšíření pgAudit a Session Audit Logging.

Po instalaci rozšíření lze nastavit logování globálně nebo např. nad systémem, databází či rolí. Například:

- **globálně**: set pgaudit.log = 'all, -misc'; – nastaví logování všech operací, kromě misc,
- **konkrétně**: alter database businessapp_main set pgaudit.log = 'ROLE,DDL'; – nastaví logování nad rolemi (grant, revoke, create role…).

Veškeré možnosti nastavení jsou popsány v dokumentaci autorů rozšíření [58]. Zasílání logů syslogem zajistíme:

- úpravou parametru: log_destination = 'stderr,syslog' v souboru postgresql.conf pro zasílání logů i do syslogu,
- úpravou konfiguračního souboru syslogu v cestě: /etc/rsyslog.d/postgresql.conf,
- zapsáním hodnoty: local0.* @@ qr.bc-test.cz:514, pro zasílání syslogu do QRadaru.

Konfigurace na straně zdroje logů: platí to stejné, jako pro ostatní syslog LS. Pokud byl špatně detekovaný typ LS, upravíme nastavení a zvolíme správný *Log Source Type*. V tomto případě: PostgreSQL Audit Trail.

9.4 UBA

Instalaci UBA provedeme v aplikaci QRadar Assistant. Instalace obsahuje krom vlastní aplikace i velké množství obsahu, jako jsou již vytvořená pravidla, referenční data, uložená vyhledávání a také vlastní LS. Aplikaci tedy zbývá dodat identity uživatelů a nakonfigurovat jednotlivé metody pro profilování chování uživatele.

9.4.1 Připojení k adresářové službě

Nastavení zahájíme tlačítkem *User Import* > *Add*. Uživatelské identity můžeme získat jednorázově importem z referenční tabulky v databázi QRadaru, z CSV souboru nebo můžeme provést připojení k LDAP / AD adresáři. Z důvodu automatického importu nových uživatelů a synchronizace změn atributů byla zvolena poslední z možností. V konfiguraci byl nastaven LDAP filtr tak aby byly importovány pouze aktivní uživatelské a technické účty (Obr. 31).

Obrázek 31 UBA - LDAP konfigurace (vlastní)

Po provedení testu připojení byl na další stránce nastaven interval importu účtů na každých 12 hodin a limit importovaných uživatelů na 1000.

Tlačítkem *Tuning* upravíme nastavení:

- **User coalescing**: všechny atributy, které mohou identifikovat uživatele na základě různých formátů zápisu jeho uživatelského jména, jak bylo popsáno v kapitole *8.5 User Behavior Analytics*,
- **Display fields**: spárování atributů uživatelů mezi aplikací UBA a adresářovou službou (Obr. 32).

Obrázek 32 UBA - párování atributů (vlastní)

9.4.2 Konfigurace metod

Před konfigurací metod můžeme upravit výchozí hodnoty globální konfigurace – tlačítko *UBA Settings*. Lze např. nastavit, zda chceme vyhodnocovat chování pouze těch uživatelů, které jsme importovali nebo všech, které UBA dokáže vyčíst z logů. Dalšími hodnotami můžeme ovlivnit způsob, jakým se počítá rizikové skóre, různé limity a prahové úrovně.

Zapnutím jednotlivých metod určujeme, které případy chování uživatelů chceme sledovat a vyhodnocovat. V instalované verzi UBA (4.0.1) je 195 metod pro různé případy. Metody jsou řešeny pomocí pravidel v QRadaru.

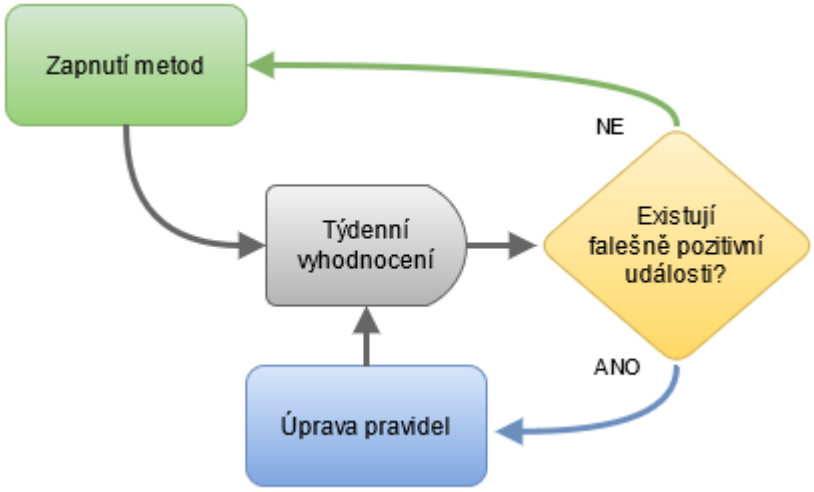
Příklady metod:

- **UBA: Failed Access to Critical Assets**: metoda detekuje chybné pokusy o přihlášení do systémů, které jsou nastaveny jako kritické. Kritické systémy je potřeba vydefinovat jejich IP adresami. Toto chování může značit pokus o zneužití cizí identity pro přístup do systému s citlivými daty, případně jejich odcizení,
- **UBA: User Account Created and Deleted in a Short Period of Time**: metoda sleduje, zda došlo během jednoho dne k vytvoření účtu uživatele a jeho následné smazání. Takovéto chování může indikovat pokus privilegovaného uživatele (administrátor systému) o zastření podvodné aktivity uměle vytvořenou identitou,
- **UBA: Ransomware Behavior Detected**: tato metoda se snaží identifikovat chování typické pro Ransomware. Je zaměřena na logy OS Windows a sepne ve chvíli, kdy je zaznamenáno nejméně 500 přístupů k různým objektům na disku během 1 minuty a stejným uživatelským jménem a procesem.

Obrázek 33 UBA - ladění metod (vlastní)

Každou metodu lze individuálně zapnout, nastavit přírůstek skóre a lze i upravit logiku pravidla dle vlastních představ (Obr. 33). Nastavení provedeme tlačítkem *Rules and Tuning*.

Nelze zapnout všechna pravidla najednou a čekat, že se okamžitě dostaví kýžený výsledek v podobě dokonalého profilování uživatelů a hodnocení jejich rizikovosti. Naopak je nutné postupovat v cyklech (Obr. 34), dokud nejsou zapnuta všechna pravidla, která dávají ve spravovaném prostředí smysl.



Obrázek 34 UBA - cyklus ladění metod (vlastní)

Jakmile je ukončeno nastavení metod a ladění pravidel, lze nainstalovat a zapnout strojové učení. V opačném případě by došlo k nesprávnému naučení normálního chování uživatelů (stanovení „base line“) a UBA by neposkytovala relevantní informace. Celý proces od instalace aplikace UBA až po zapnutí strojového učení může trvat i několik měsíců.

Dílčí závěr: na modelovém příkladu je ukázaná konfigurace základních částí nástroje QRadar a jeho rozšíření. V ukázkách konfigurace jsou představeny konkrétní postupy vycházející z osvědčené praxe, což by mělo přispět k efektivnějšímu postupu při nasazování tohoto nástroje.

10 DETEKCE NEŽÁDOUCÍCH AKTIVIT UŽIVATELŮ

V následující kapitole bude na praktických příkladech popsán postup vytváření korelačních pravidel pro detekci nežádoucích aktivit uživatelů v QRadar SIEM, šetření souvisejících offensí a vyhodnocování rizikovosti uživatelů v UBA. Veškeré výstupy jsou anonymizovány.

10.1 Tvorba pravidel a vyhodnocení událostí

QRadar je po instalaci vybaven stovkami předpřipravených pravidel pro detekci širokého spektra nežádoucích aktivit. Další pravidla lze získat:

- vytvořením vlastních pravidel,
- stažením a instalací specializovaného rozšíření obsahu (např. sada obsahu zaměřena na logy Office 365 nebo na práci se Sysmon logy),
- stažením a instalací aplikačního rozšíření, které pro svůj chod vyžaduje další obsah, vč. pravidel (např. UBA).

V následujících příkladech bude popsán proces vytváření vlastních pravidel.

10.1.1 Základní pojmy při vytváření pravidel

Pravidla (Rules) jsou tvořena kombinací podmínek (Rule Tests), které testují vlastnosti událostí, síťových flow, offensí, stavebních bloků (Building Blocks), časových sousledností, počítadel, referenčních dat a dalších znalostí QRadaru. V pravidlech je definována odezva (rule response) pro případ, kdy jsou podmínky splněny (pravidlo sepne).

Stavební bloky (BB) mají stejné možnosti tvorby jako pravidla, avšak oproti pravidlům neobsahují žádné nastavení pro definici odezvy na sepnutí.

Referenční data jsou datové struktury, do kterých je možné ukládat informace a následně s nimi pracovat v pravidlech. Informace do referenčních dat lze vkládat ručně, importem, aplikačním rozšířením, nebo z událostí v rámci odezvy pravidla na sepnutí. Referenčních dat je několik typů, od jednoduchého seznamu hodnot (reference set) až po datovou strukturu za použití více klíčů (reference table). V práci nebudou názvy typů referenčních dat překládány.

Offense vznikají sepnutím pravidla, jsou tedy jednou z možných odezev na pozitivní vyhodnocení podmínek. Offense jsou předmětem investigace specialistů IT bezpečnosti. Po vyšetření jsou offense klasifikovány a uzavírány. Pozitivní nálezy bývají vstupem pro incident management.

10.1.2 Reakce na sepnutá pravidla (Rule Response)

U každého pravidla lze nastavit akci, která se má provést, jestliže byly splněny všechny zadané podmínky.

Rule Action: nastavuje, co se má provést s událostí, která pravidlo spustila:

- Severity: upravuje hodnotu závažnosti události,
- Credibility: upravuje hodnotu důvěryhodnosti události,
- Relevance: upravuje hodnotu dopadu události,
- Ensure the detected event is part of an offense: zajistí aby událost byla přiřazena k offensi,
- Annotate event: přidá do události popisek,
- Bypass further rule correlation event: zakáže korelaci události v dalších pravidlech.

Rule Response: určuje, jaká akce se má vyvolat:

- Dispatch New Event: vytvořit novou událost se zadanými parametry. Touto volbou lze také podrobně nastavit vytvoření offense,
- Email: vytvoří e-mailové upozornění s definovanou šablonou, které je okamžitě zasláno uvedeným příjemcům,
- SNMP Trap, Send to Local Syslog, Send to Forwarding Destinations, Notify: zaslání vytvořené události různými kanály příjemci,
- Add to / Remove from Reference Set / Data: umožňuje uložit / vymazat zvolené atributy události do / z datových struktur QRadaru,
- Execute Custom Action: touto volbou lze spustit jakýkoliv předem připravený kód (např. Perl, Python, Shell skript).

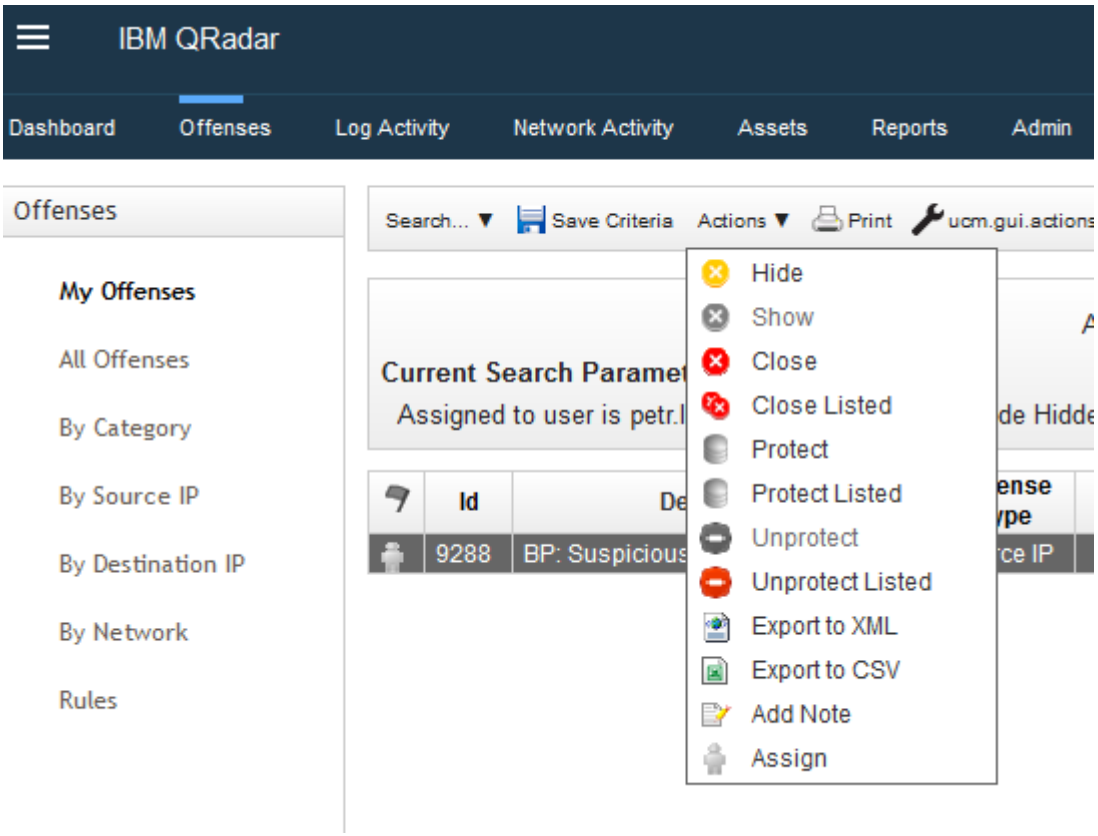
Response Limiter: umožní omezit vícenásobné sepnutí pravidla zadanými parametry.

10.1.3 Šetření offensí

Pakliže jsou splněny všechny podmínky pravidla a v sekci Rule Response je nastavena akce pro vytvoření offense, objeví se v nabídce *Offenses > All Offenses*. Zde se offense ukládají a agregují. Pokud pravidlo spíná opakovaně, nevytvářejí se po každé nové záznamy, ale pouze se aktualizuje již vytvořené offense. Každá offense obsahuje všechny potřebné údaje k jejímu prošetření, jako jsou IP adresy jejího původce a cíle, uživatelské jméno původce, popis offense a především všechny související události, které způsobily sepnutí pravidla.

Postup šetření: osvědčeným postupem je šetřit událost v následujících krocích:

- přiřazení (Assign, Obr. 35) offense vyšetřovateli (specialista IT bezpečnosti, SOC specialista),
- zobrazení detailu offense, seznámení se s podrobnostmi a proklikem zobrazení relevantních událostí v Log Activiti okně. Dalším filtrováním událostí a jejich detailů shromáždit dostatek informací pro vyhodnocení offense,
- během šetření lze k offensi přidávat další poznámky (Add Note, Obr. 35),
- šetření končí uzavřením offense (Close, Obr. 35). Při uzavírání je povinné zvolit důvod jejího uzavření z rozbalovacího seznamu. Základní tři důvody jsou: **False-Positive** (sepnutí pravidla neodpovídá jejímu význam – pravidlo je vhodné upravit), **Non-Issue** (pravidlo sepnulo správně, ale nejedná se o bezpečnostní událost), **Policy Violation** (byla potvrzena bezpečnostní událost). Důvody uzavření offensí lze konfigurovat a přizpůsobit je např. dle požadavků Kybernetického zákona,
- pokud byla offense potvrzena (jedná se o bezpečnostní událost), následuje další vyšetřování v rámci řízení bezpečnostních incidentů.



Obrázek 35 Práce s offensí (vlastní)

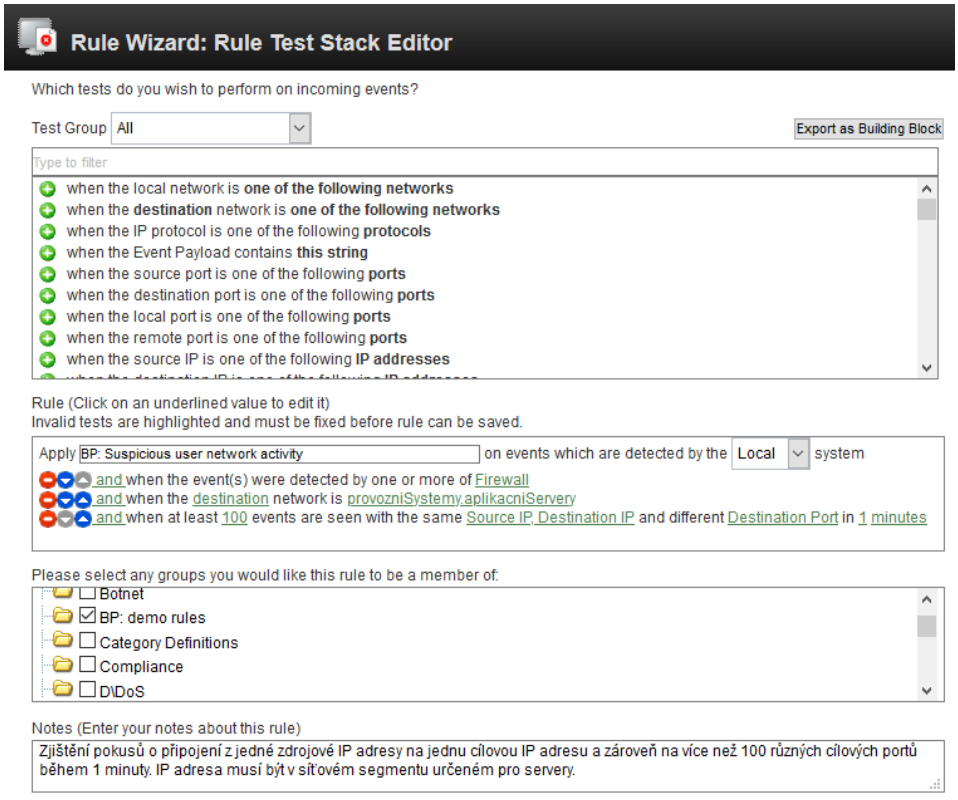
Dalšími možnostmi práce s offensemi jsou např. jejich export pro další zpracování, ochrana před smazáním (dle nastavené retence) nebo její skrytí ze seznamu.

10.1.4 Detekce nežádoucí síťové aktivity uživatele

Cíl: detekovat chování uživatele na síti, které neodpovídá běžnému provozu. Může se jednat např. o cílené zjišťování otevřených portů na vybraném serveru za účelem hledání možné zranitelnosti v některé ze spuštěných služeb. Taková aktivita může záměrně pocházet přímo od uživatele, který má povolený přístup k síti, ale také se může jednat o činnost útočníka prostřednictvím úspěšně napadeného počítače v síti, který získal pod svoji kontrolu.

Metoda: využijeme logu firewallu a znalosti síťové segmentace. Můžeme předpokládat, že útočník bude zkoušet prověřit služby na serverech, jejichž čísla portů protokolu TCP/IP jsou registrovány pro nejčastěji používané síťové služby. Budeme tedy zjišťovat pokusy o připojení z jedné zdrojové IP adresy na jednu cílovou IP adresu a zároveň na více než 100 různých cílových portů během 1 minuty. Cílová IP adresa musí být v síťovém segmentu určeném pro servery.

Konfigurace: pravidla **BP: Suspicious user network aktivity** (osvědčeným postupem je všechny názvy uvádět v anglickém znění). V rámci ukázky prvního případu užití bude popsán celý průběh konfigurace. Vytváření pravidel pro události se provádí pomocí průvodce v nabídce *Offenses* > *Rules* > *Actions* > *New Event Rule* > *Events*.



Obrázek 36 Vytváření pravidla (vlastní)

V horní části konfiguračního okna (Obr. 36) je výčet testů, které můžeme zvolit a upravit pro podmínku pravidla. Střední část slouží pro pojmenování pravidla a definici podmínky. Mezi jednotlivými testy v podmínce je vždy logický operand AND nebo NOT. Kliknutím na zvýrazněnou část testu zadáváme jeho parametry. Ve spodní části můžeme pravidlo kategorizovat a přidat jeho popis. Vytvořené pravidlo můžeme exportovat jako stavební blok (tlačítko *Export as Building Block*).

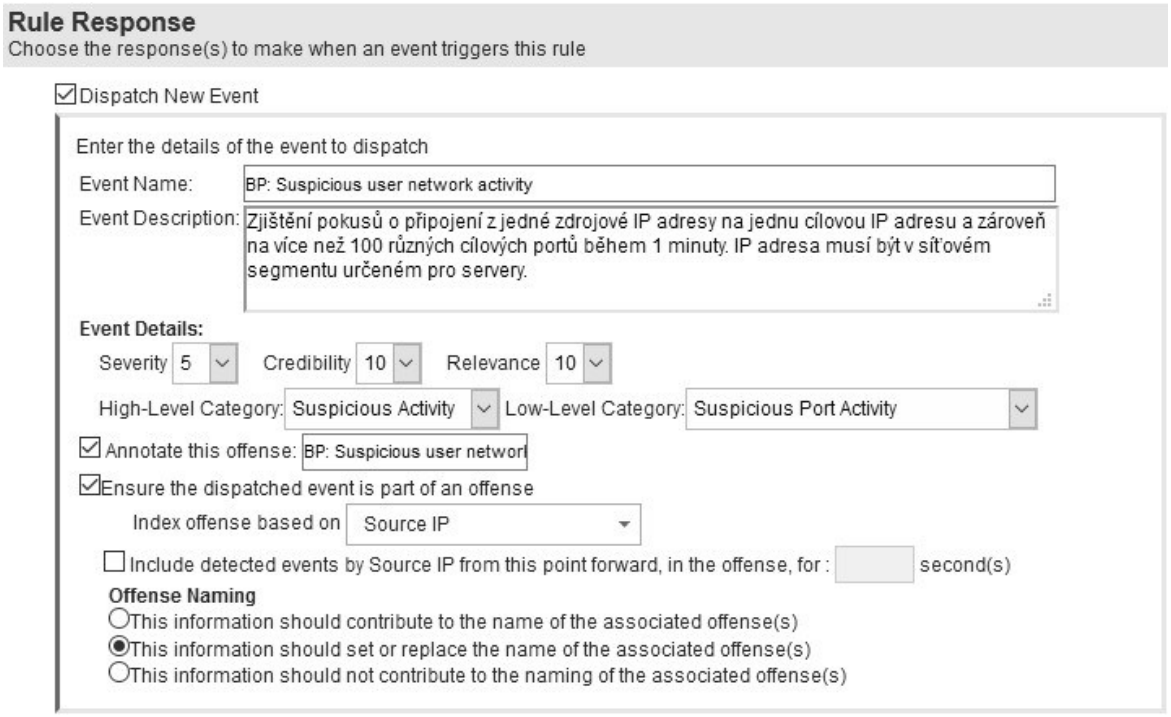
V konfiguraci podmínky pro pravidlo na detekci nežádoucí síťové aktivity byly použity tři testy s následujícím nastavením:

- **and** when the event(s) were detected by one or more of **Firewall**. (Firewall je námi předem definovaná skupina LS, do které jsou přiřazeny všechny firewally),
- **and** when the destination network is **provozniSystemy.aplikacniServery** (provozniSyst… je námi předem definovaná pojmenovaná síť v *Network Hierarchy*),
- **and** when at least **100** events are seen with the same **Source IP, Destination IP** and different **Destination Port** in **1** minutes.

Další strana průvodce slouží k nastavení reakce na sepnutí pravidla, jak bylo popsáno v kapitole *10.1.2 Reakce na sepnutá pravidla*. V části Rule Action byla vybrána volba, která zajistí přidání událostí zodpovědných za sepnutí pravidla do offense (Obr. 37).

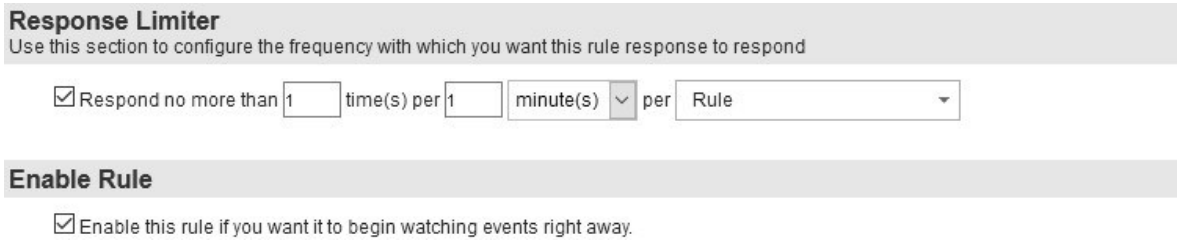
Obrázek 37 Reakce na sepnutí – Rule Action (vlastní)

V části Rule Response (Obr. 38) bylo nastaveno vytvoření nové události (její pojmenování a popis), hodnoty Severity, Credibility a Relevance, určení kategorií události, vytvoření a pojmenování offense, přidání nové události do offense a určení, jak má být vytvořen název offense.



Obrázek 38 Reakce na sepnutí – Rule Response (vlastní)

Response Limiter (Obr. 39) byl nastaven tak aby se v případě pokračující události vytvořila vždy jen jedna offense do minuty. V závěru nastavení byla zapnuta volba pro okamžité zapnutí pravidla.



Obrázek 39 Reakce na sepnutí – Response Limiter (vlastní)

Simulace útoku: byla provedena nástrojem **Nmap** z příkazového řádku OS Windows. Zadaný parametr **F** určuje provedení skenu 100 nejběžnějších portů v každém protokolu. Parametr **T4** určuje použití agresivní šablony časování [59]. Skener nalezl několik otevřených portů služeb (Obr. 40), které mohou obsahovat zranitelnosti.

```
C:\Users\karel.spatny>nmap -T4 -F 10.0.30.1
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-17 19:55 Střední Evropa
Nmap scan report for fs.bc-test.cz (10.0.30.1)
Host is up (0.018s latency).
Not shown: 93 filtered ports
PORT     STATE  SERVICE
113/tcp  closed ident
135/tcp  open   msrpc
445/tcp  open   microsoft-ds
2000/tcp open   cisco-sccp
3389/tcp open   ms-wbt-server
5060/tcp open   sip
5666/tcp open   nrpe

Nmap done: 1 IP address (1 host up) scanned in 33.76 seconds

C:\Users\karel.spatny>
```

Obrázek 40 Nmap - skenování portů (vlastní)

Na provedenou simulaci zareagovalo pravidlo sepnutím a vytvořením offense ID 9288 (Obr. 41).

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users
9288	BP: Suspicious user network activity	Source IP	10.70.0.100		10.70.0.100	10.0.30.1	karel.spatny

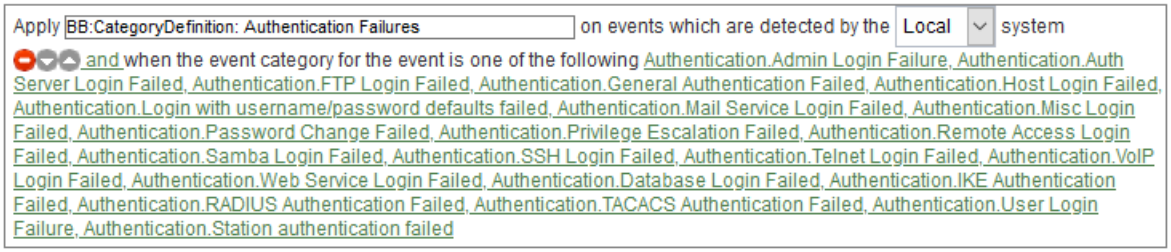
Obrázek 41 Offense ID 9288 (vlastní)

10.1.5 Detekce pokusu o prolomení hesla

Cíl: detekovat pokus o prolomení hesla na libovolnému systému nebo do aplikace, které nemají implementovanou ochranu proti útoky typu „brute force“ (útok hrubou silou). Požadavek na detekci nežádoucí aktivity tohoto typu je bez ohledu na to, zda byl útok úspěšný.

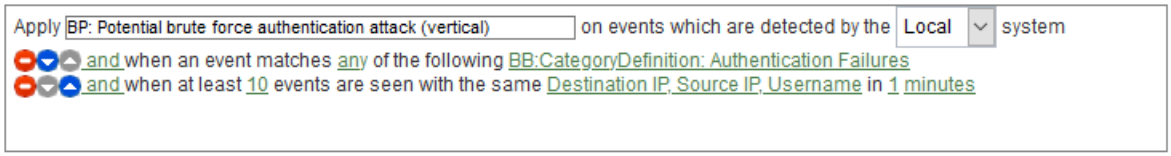
Metoda: využijeme faktu, že logy ze všech LS máme normalizované a jednotlivé události jsou zařazeny do kategorií. Testovací podmínka v pravidle bude reagovat na kteroukoliv událost v kategorii **Authentication** a kteroukoliv podkategorii typu **failed**. Podkategorií typu failed je 22. Abychom je nemuseli v podmínce všechny vyjmenovávat, využijeme již existujícího systémového stavebního bloku s názvem **BB:CategoryDefinition: Authentication Failures** (Obr. 42). Předpokládejme, že útočník zná přihlašovací jméno (často bývá přihlašovací jméno e-mailová adresa nebo její část) a bude zkoušet odhadnout heslo opakovaným zadáváním (nebo automatizovaně pomocí skriptu slovníkovou metodou). Jedná se tedy o vertikální typ útoku. Nastavíme test v podmínce na minimálně 10 opakování pokusu během 1 minuty (pokud bychom chtěli detekovat pouze automatizovaný útok, zvýšíme počet pokusů a snížíme dobu opakování).

Následně vytvoříme ještě druhé pravidlo, které sepne v případě, že po sepnutí prvního pravidla bude do 5 minut detekováno úspěšné přihlášení ze stejné zdrojové IP adresy na stejnou cílovou IP adresu a se stejným přihlašovacím jménem (využijeme řetězení pravidel). To by mohlo značit úspěšné prolomení hesla.

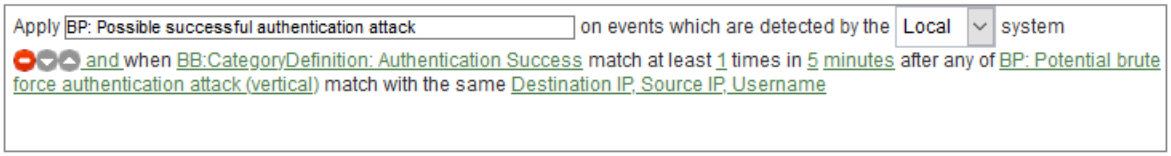


Obrázek 42 Stavební blok – Auth. Failures (vlastní)

Konfigurace: pravidel **BP: Potential brute force authentication attack (vertical)** (Obr. 43) a **BP: Possible successful authentication attack** (Obr. 44) s použitím BB a řetězení pravidel.



Obrázek 43 Pravidlo – detekce neúspěšných přihlášení (vlastní)



Obrázek 44 Pravidlo – detekce možného prolomení hesla (vlastní)

V druhém pravidle byl použit systémový stavební blok s názvem **BB:CategoryDefinition: Authentication Success**.

Simulace útoku: byla provedena z běžné linuxové konzole uživatele (Obr. 45), simulováním neúspěšného SSH přihlášení na vzdálenou konzoli linuxového serveru. Po více neúspěšných přihlášeních bylo poslední přihlášení úspěšné – heslo bylo útočníkem „uhádnuto“.

Na provedenou simulaci zareagovalo pravidlo sepnutím a vytvořením offensí ID 9299 a 9300 (Obr. 46). Druhé pravidlo, reagující na následné úspěšné přihlášení, spustilo nastavenou odezvu pro okamžité zaslání e-mailového upozornění odpovědné osobě (Obr. 47).

```
karel@ntb:~$ ssh karelspatny@10.0.20.4
karelspatny@10.0.20.4's password:
Permission denied, please try again.
karelspatny@10.0.20.4's password:
Permission denied, please try again.
karelspatny@10.0.20.4's password:
karelspatny@10.0.20.4: Permission denied (publickey,gssapi-keyex,gssapi-with-mi
karel@ntb:~$ ssh karelspatny@10.0.20.4
karelspatny@10.0.20.4's password:
Permission denied, please try again.
karelspatny@10.0.20.4's password:
Permission denied, please try again.
karelspatny@10.0.20.4's password:
karelspatny@10.0.20.4: Permission denied (publickey,gssapi-keyex,gssapi-with-mi
karel@ntb:~$ ssh karelspatny@10.0.20.4
karelspatny@10.0.20.4's password:
Permission denied, please try again.
karelspatny@10.0.20.4's password:
Permission denied, please try again.
karelspatny@10.0.20.4's password:
karelspatny@10.0.20.4: Permission denied (publickey,gssapi-keyex,gssapi-with-mi
karel@ntb:~$ ssh karelspatny@10.0.20.4
karelspatny@10.0.20.4's password:
Permission denied, please try again.
karelspatny@10.0.20.4's password:
Last failed login: Sun Apr 18 22:31:22 CEST 2021 from 10.0.70.100 on ssh:notty
There were 10 failed login attempts since the last successful login.
Last login: Sun Apr 18 22:08:50 2021 from 10.0.70.100
[karelspatny@ntp ~]$
```

Obrázek 45 Linux konzole – uhádnutí hesla (vlastní)

Id	Description	Offense Type	Offense Source	Magn	Source IPs	Destination IPs	Users
9300	BP: Possible successful authentication attack	Source IP	10.0.70.100		10.0.70.100	ntp.bc-test.cz	karelspatny
9299	BP: Potential brute force authentication attack (vertical)	Username	karelspatny		10.0.70.100	ntp.bc-test.cz	karelspatny

Obrázek 46 Offense ID 9299 a 9300 (vlastní)

-----Original Message-----
From: qradar@bc-test.cz < qradar@bc-test.cz>
Sent: Sunday, April 18, 2021 10:31 PM
To: Tomáš Bystrý <bystry@bc-test.cz>
Subject: BP: Possible successful authentication attack Fired

The following is an automated response sent to you by the QRadar event custom rules engine:

Apr 18, 2021 10:31:10 PM CEST

Rule Name:	BP: Possible successful authentication attack
Rule Description:	Zjištění neúspěšných přihlášení následované úspěšným přihlášením ze stejné zdrojové IP adresy na jednu cílovou IP adresu pod stejným přihlašovacím jménem během 5 minut
Source IP:	10.0.70.100
Source Port:	3355
Source Username:	karelspatny
Source Network:	uzivatele.vpn
Destination IP:	10.0.20.4
Destination Port:	0
Destination Network:	provozniSystemy.provozniServery
Protocol:	other(255)
QID:	44250019
Event Name:	Accepted Password for User
Event Description:	Accepted Password for User
Category:	Host login Succeeded
Log Source ID:	370
Log Source Name:	Linux - ntp.bc-test.cz @ 10.0.20.4
Payload:	<86>Apr 18 22:21:31 ntp sshd[26394]: Accepted password for karelspatny from 10.0.70.100 port 3355 ssh2

Obrázek 47 E-mailový alert – uhodnutí hesla (vlastní)

10.1.6 Zneužití technického účtu

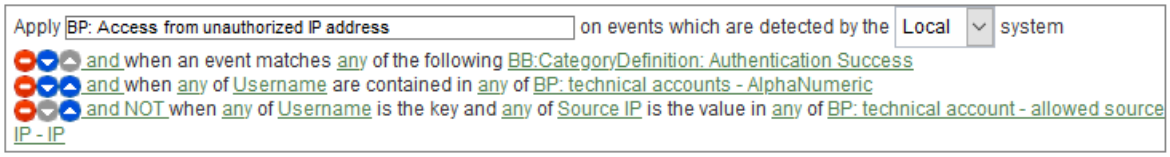
Cíl: detekovat zneužití technického účtu uživatelem, který má znalost jeho hesla a snaží se tak maskovat svoji identitu při páchání nežádoucích aktivit. Útočník může být např. nespokojeným zaměstnancem, který má na starost správu některého systému.

Metoda: budeme detekovat přihlášení použitím technických účtů z IP adres, které nekorespondují s očekávanou síťovou aktivitou. Tedy. z IP adres, které nejsou pro dané technické účty vyhrazené. V testovacích podmínkách využijeme referenční data uložená v databázi QRadaru. Použijeme datovou strukturu **reference set** s uloženými názvy monitorovaných technických účtů a **reference map of sets**, kde klíčem bude přihlašovací jméno technického účtu a hodnotou zdrojová IP adresa, ze které je povoleno účtu přistupovat k cílovému systému / aplikaci.

Konfigurace: v prvním kroku byly pro použití v pravidle **BP: Access from unauthorized IP address** vytvořeny dvě datové struktury v *Reference Data Management* > *Reference Set* a *Reference Map of Sets* > *Create New*:

- **BP: technical accounts** s názvy všech používaných technických účtů (reference set),
- **BP: technical account – allowed source IP**, ve které jsme definovali, že účet s názvem **qradar** lze použít pouze z IP adresy QRadaaru **10.0.50.1** (reference map of sets).

Následuje konfigurace pravidla (Obr. 48).



Obrázek 48 Pravidlo – detekce neautorizovaného přístupu (vlastní)

Simulace útoku: byla provedena prostým přihlášením na webové rozhraní síťového úložiště z IP adresy uživatele připojeného do sítě VPN a jménem technického účtu qradar. Zdrojová IP adresa se neshoduje s IP adresou uloženou v seznamu povolených IP adres. Na provedenou simulaci zareagovalo pravidlo sepnutím a vytvořením offense ID 9301 (Obr. 49).

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users
9301	BP: Access from unauthorized IP address	Source IP	10.0.70.100		10.0.70.100	10.0.50.3	qradar

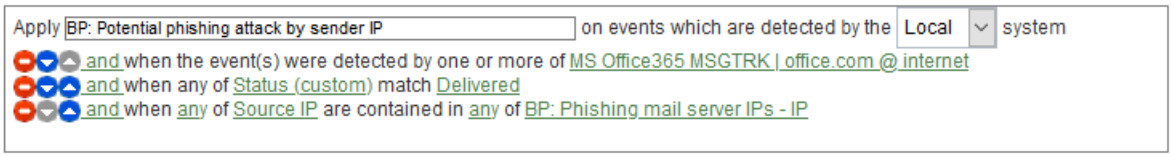
Obrázek 49 Offense ID 93001 (vlastní)

10.1.7 Detekce možného phishingu na uživatele

Cíl: detekovat příchozí phishingový e-mail na základě IP reputační databáze. Obsah databáze lze získávat např. z vláken IBM X-Force Exchange.

Metoda: v pravidle využijeme **Exchange message tracking logs** získaný přes API LS Office 365. Tento log obsahuje záznamy o všech příchozích i odchozích e-mailech společnosti, včetně IP adres odesílajících mail serverů. IP adresu odesílatele porovnáme s reference set datovou strukturou **BP: Phishing mail server IPs**. IP adresy reference set získá z IBM X-Force Exchange, z veřejné kolekce **Phishing & Spam** [60]. reference set můžeme doplnit vlastními položkami. Podmínku doplníme testem, zda byl e-mail doručen uživateli do schránky.

Konfigurace: pravidla **BP: Potential phishing attack by sender IP** (Obr. 50).



Obrázek 50 Pravidlo – detekce phishingu (vlastní)

Simulace útoku: pro simulaci útoku byla použita kopie e-mailu z reálné phishingové kampaně (Obr. 51), zaslána prostřednictvím poštovního serveru s IP adresou uvedenou v reference setu.

Obrázek 51 Phishingový e-mail (vlastní)

Přijaté zpráva způsobila sepnutí pravidla a vytvoření offence ID 9328 (Obr. 52).

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users
9328	BP: Potential phishing attack by sender IP	Source IP	46.28.106.43		46.28.106.43	0.0.0.0	testy@outlook.cz

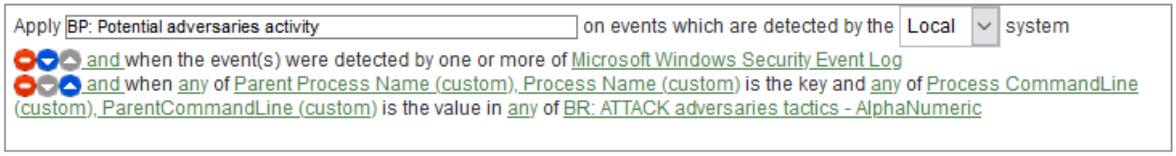
Obrázek 52 Offence ID 9328 (vlastní)

10.1.8 Detekce malware aktivity

Cíl: detekovat malware na základě jeho chování na stanici nebo v síti, nikoliv dle antivirových či IPS signatur. Tento přístup je důležitý zejména pro odhalení tzv. „zero day" útoku (nový útok, doposud neznámý pro detekci konvenčním způsobem).

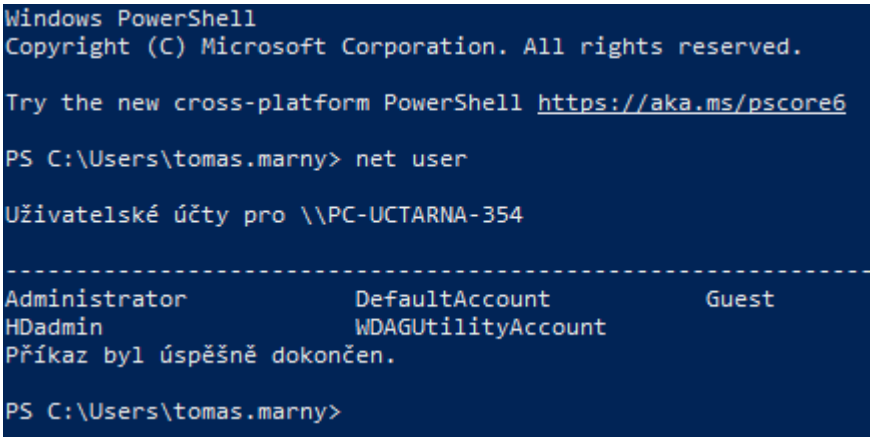
Metoda: pro stanovení metody záchytu malware aktivity bude využito znalostní báze MITRE ATT&CK®, ve které jsou shromážděny, kategorizovány a popsány taktiky využívané útočníky [61]. V tomto případě se bude jednat o detekci aktivity, kterou malware využívá pro hledání dalších obětí v síti, kam by se mohl replikovat. Potřebné informace budeme získávat z logů OS Windows, do kterých bude zapisovat události nástroj Sysmon (viz kapitola *9.3.2 Windows OS*). Podmínka pravidla bude testovat spouštění příkazů **net view, net user, net user /domain, net localgroup, net group /domain** z příkazové řádky na koncové stanici, což neodpovídá běžnému chování uživatele, ale je často využíváno malware [62].

Konfigurace: abychom nemuseli monitorované příkazy na stanici vypisovat přímo do testu pravidla **BP: Potential adversaries activity** a případně je mohli použít i v dalších pravidlech, byl vytvořen reference map of sets **BR: ATTACK adversaries tactics** a do něj vloženy hodnoty příkazu **net** viz minulý odstavec, pod klíčem s názvem procesu **net.exe**. V pravidle testujeme vyparsované hodnoty všech LS typu **Microsoft Windows Security Event Log** proti vytvořenému reference setu (Obr. 53). V odezvě pravidla bylo nastaveno i zaslání e-mailového upozornění odpovědné osobě.



Obrázek 53 Pravidlo - detekce malware aktivity (vlastní)

Simulace útoku: byla provedena v konzoli Windows PowerShell (Obr. 54), zadáním příkazu pro vypsání všech lokálních uživatelů na stanici. Na tuto aktivitu zareagovalo pravidlo sepnutím, vytvořením offense ID 9351 (Obr. 55) a zasláním e-mailu.



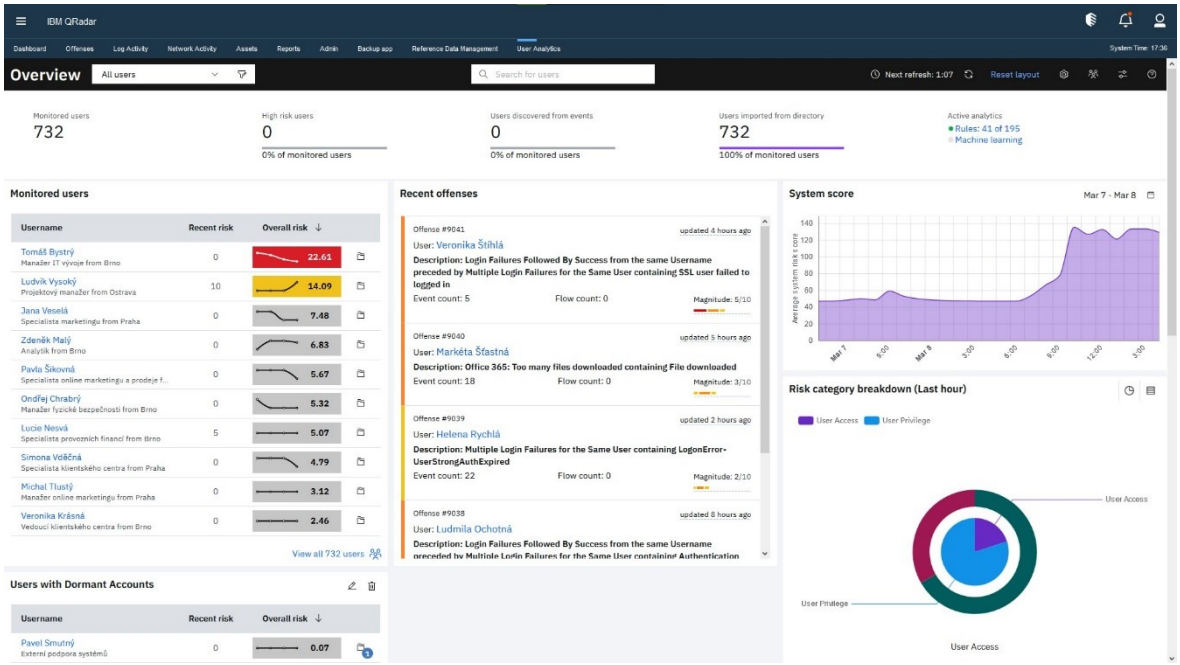
Obrázek 54 PowerShell konzole – malware aktivita (vlastní)

Id	Description	Offense Type	Offense Source	Magr	Source IPs	Destination IPs	Users
9351	BP: Potential adversaries activity	Username	tomas.marny		10.0.70.100	10.0.70.100	tomas.marny

Obrázek 55 Offense ID 9351 (vlastní)

10.2 Analýza chování uživatelů nástrojem UBA (anonymizováno)

UBA poskytuje pohled na rizikovost uživatelů přehlednou grafickou formou. Pracovní plocha UBA je dělena na několik konfigurovatelných modulů (Obr. 56):

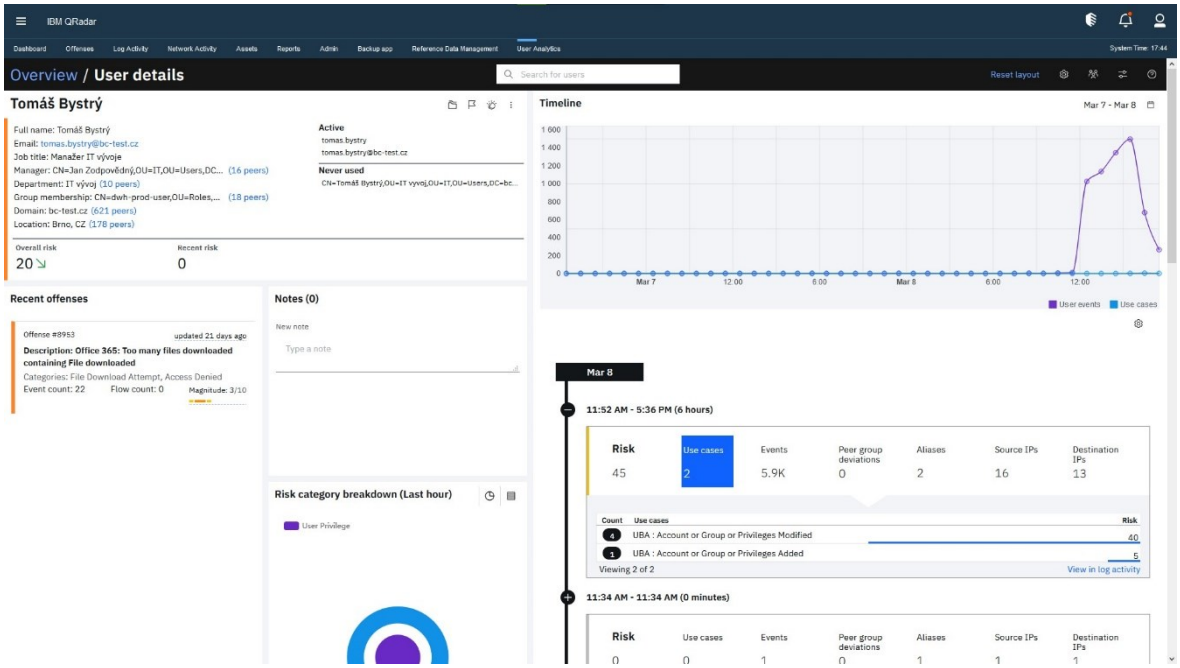


Obrázek 56 UBA – praovní plocha (vlastní)

- **Monitored users**: přehled všech uživatelů s aktuálním a celkovým rizikovým skóre,
- **Recent offences**: přehled nevyřešených offensí dle uživatelů,
- **System score**: celkové rizikové skóre za všechny uživatele a dané období,

- **Risk category breakdown**: graf podílu jednotlivých rizikových kategorií na celkovém skóre za dané období,
- **Watchlist**: uživatelsky definované seznamy, dle různých kritérií,
- **Active investigation**: seznam uživatelů, u kterých právě probíhá šetření.

Analýza začíná výběrem uživatele. Uživatele můžeme v průběhu práce přidávat na seznamy (watchlist), dle vybraných kritérií. Např. můžeme vytvořit seznam uživatelů, kteří často překračují prahovou hodnotu risk skóre nebo seznam uživatelů s privilegovaným oprávněním v systémech (mohou být rizikovější z podstaty své pracovní pozice). Kliknutím na jméno vybraného uživatele zobrazíme jeho detail. Na kartě **User details** (Obr. 57) jsou zobrazeny informace o uživateli načtené např. z Active Directory, jeho skóre a další údaje. V grafu **Timeline** jsou na vodorovné ose zobrazeny události a rizikové případy v čase vztažené k uživateli. Kliknutím na každý bod grafu jsou tyto události zobrazeny v náhledu a lze jejich detail dále zobrazit v QRadar Log Activity.



Obrázek 57 UBA – detail uživatele (vlastní)

Praktický postup analýzy chování uživatele s vysokým skóre je shrnut v následujících bodech:

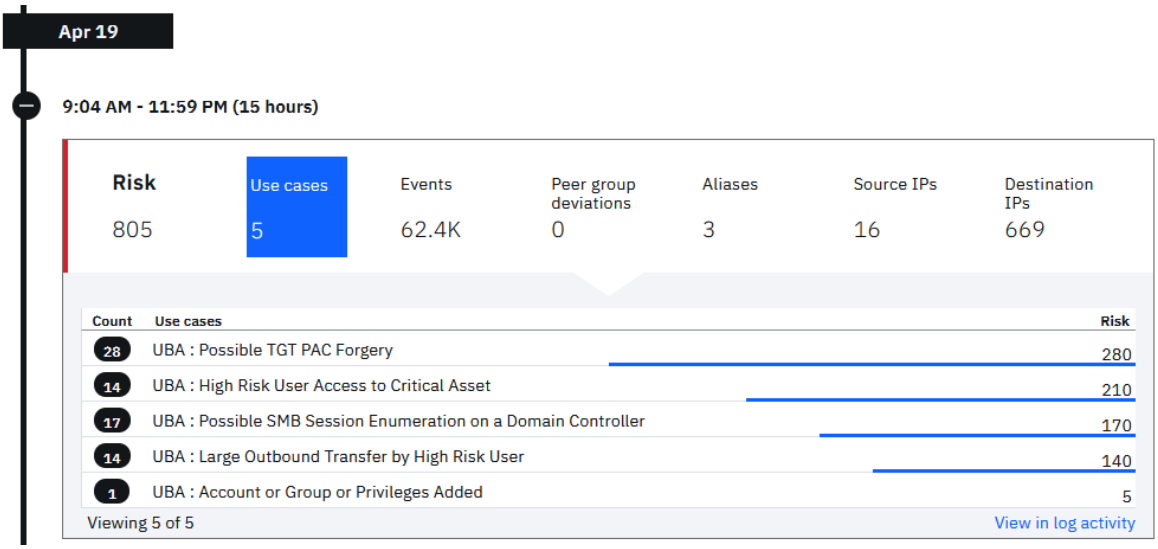
Vyhodnocení časové osy:

- v Timeline ponechat pouze graf Use cases,
- vybrat delší časový úsek zobrazení (např. týden),
- nalézt moment, kdy začalo rizikové skóre stoupat (Obr. 58).

Obrázek 58 UBA – Timeline (vlastní)

Zobrazení rizikových případů:

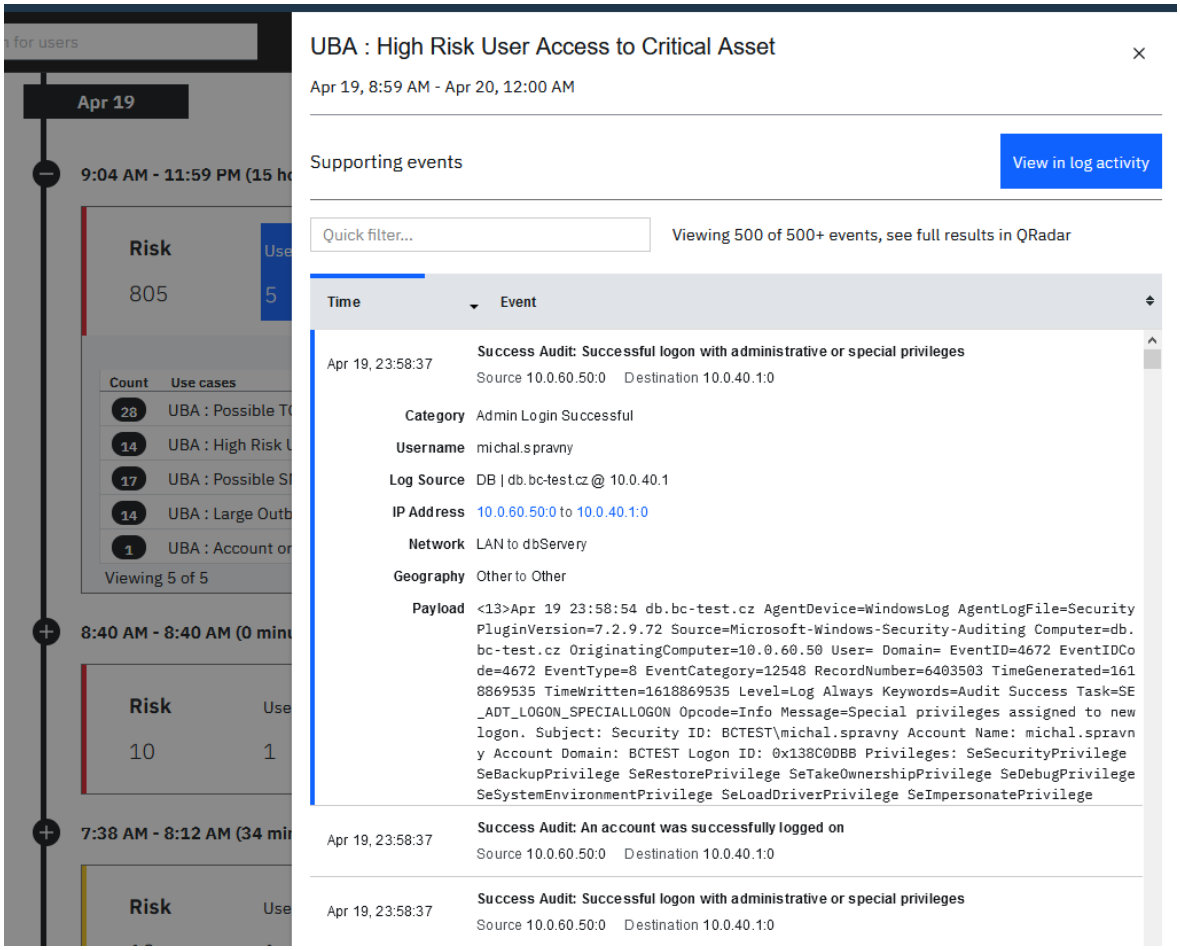
- v časové ose záznamů rizikových případů pod grafem přejít k boxu s vybraným časem,
- kliknutím na box zobrazit případy v daném momentě, agregované dle počtu sepnutí (jedná se o počet sepnutých pravidel, definovaných metodami UBA). Z detailů lze odečíst, jak se jednotlivé metody podílely na rizikovém skóre v daný moment (Obr. 59). Je možné zobrazit daný moment agregovaně např. i podle událostí, zdrojových, či cílových adres.



Obrázek 59 UBA – rizikové případy (vlastní)

Vyhodnocení událostí:

- kliknutím na jednotlivé případy zobrazit konkrétní události, které byly metodou vyhodnoceny jako rizikové. U každé události lze zobrazit její detail (Obr. 60) nebo je možné všechny události zobrazit v QRadar Log Activity.



Obrázek 60 UBA – detail události (vlastní)

Na rozdíl od vyšetřování offensí v QRadaru, nedochází v UBA po dokončení investigace k uzavření konkrétních případů. Analýza chování uživatelů je průběžná činnost, která začíná a končí zároveň s pracovním poměrem zaměstnance. Poznatky z investigace pouze zapisujeme do poznámek v detailu uživatele pro další použití.

Dílčí závěr: na jednotlivých praktických příkladech bylo ukázáno, jak postupovat při vytváření pravidel pro detekci nežádoucích uživatelských aktivit, jak provést následnou investigaci offensí a rizikových uživatelů v rozšíření UBA. Jedná se o základ práce s vybraným nástrojem SIEM, umožňující jeho další rozvoj a zlepšování schopností obsluhy.

ZÁVĚR

V úvodu práce byl představen aktuální stav kybernetické bezpečnosti z pohledu národních autorit. Tento stav se nepřímo odráží v ohrožení informační bezpečnosti ve společnostech. Mnoho vnějších hrozeb působí na nejslabší článek informační bezpečnosti – člověka. Dle legislativy musí být zajištěna ochrana soukromí každé osoby, což platí i pro kybernetický prostor. Aktivity člověka jsou nejen objektem ochrany, ale zároveň mohou působit i jako hrozba. Uvedený průzkum nastiňuje, že člověk působící uvnitř společnosti je nejčastějším zdrojem bezpečnostních incidentů. Zmíněná fakta vyzdvihují potřebu společnosti vytvořit vlastní koncept informační bezpečnosti a zavést odpovídající opatření v souladu s jejími pilíři – zachování důvěrnosti, integrity a dostupnosti informace. Práce ukazuje možnost, jak tuto potřebu naplnit zavedením bezpečnostní politiky informací, která je inspirována systémem řízení bezpečnosti informací dle normy ISO 27001. Naplňování bezpečnostní politiky je třeba neustále ověřovat. Celý koncept práce odráží aplikační požadavky vycházející z legislativy EU a zákonných norem.

Jedním z prostředků zajištění informační bezpečnosti je monitorování chování uživatelů v informačních systémech společnosti. V navazujících kapitolách byly podrobně popsány oblasti zájmu monitoringu a systémy, které poskytují události o uživatelských aktivitách. Představeny byly nástroje vhodné pro monitoring a vyhodnocování aktivit uživatele v informačních systémech, popsány jejich vlastnosti, poskytované možnosti monitoringu a určení použití. Získané informace lze zužitkovat při rozhodování, který způsob monitoringu a jaký typ zařízení je vhodný pro stanovené potřeby společnosti.

Práce se dále věnuje nástroji pro sběr a vyhodnocování událostí – SIEM, který byl zvolen jako ideální pro bezpečnostní monitoring chování uživatelů v informačních systémech. Byla popsána jeho architektura, princip fungování a detailně stanoveny předpoklady pro jeho nasazení ve společnosti. Na základě těchto znalostí byl vytvořen plán jeho nasazení, včetně doporučení pro zadání a vyhodnocení výběrového řízení.

Hlavní část práce se zabývá nasazením vybraného nástroje – IBM QRadar SIEM a jeho rozšíření, především nástroje pro analýzu chování uživatelů UBA. Jednotlivé kapitoly popisují jeho možnosti, způsob zapojení do IT infrastruktury a konkrétní konfiguraci v reálném prostředí. Uvedené informace tvoří ucelený postup pro nastavení stěžejních parametrů tak, aby na jeho konci bylo možné provést spuštění nástroje do produkčního

prostředí. Postup je vytvořen způsobem, který zaručuje přenesení získaných konfiguračních znalostí do jiných prostředí ICT podobného typu.

Závěr práce je věnován praktickým příkladům konfigurace korelačních pravidel. Uvedené příklady demonstrují jejich reálné užití k detekci nežádoucích aktivit uživatelů v IS. Každý příklad popisuje jiný typ detekce a zároveň také využití rozličných možností testovacích podmínek pravidel. Aby byl popis práce se SIEM kompletní, uvádí práce i postup šetření incidentů (offensí), které jsou korelačními pravidly generovány a postup vyhodnocení rizikových událostí v analytickém nástroji UBA.

Práce jako celek dané téma bezpečnostního monitoringu chování uživatelů v informačních systémech pokrývá v dostatečné šíři, od pochopení problematiky tématu až po předání konkrétních znalostí k realizaci vytyčeného cíle. Je ale třeba zdůraznit, že se jedná pouze o jednu z dílčích části, která je součástí integrovaného systému zajištění informační bezpečnosti ve společnosti, a kterou je nutné doplnit dalšími technickými a organizačními opatřeními.

SEZNAM POUŽITÉ LITERATURY

[1] POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

[2] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6. Dostupné také z: https://cybersecurity.cz/data/slovnik_v310.pdf

[3] What is the CIA Triad?: The CIA triad defined, explained, and explored. *Forcepoint | Human-Centric Cybersecurity* [online]. Austin: Forcepoint, 2020 [cit. 2020-11-09]. Dostupné z: https://www.forcepoint.com/cyber-edu/cia-triad

[4] ČERMÁK, Miroslav. CIA: Důvěrnost-Integrita-Dostupnost. *CleverAndSmart Management Consulting* [online]. Dolní Břežany: Ing. Miroslav Čermák, 2020 [cit. 2020-11-08]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/

[5] Kybernetická bezpečnost. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2019, s. 39-45. CZ.NIC. ISBN 978-80-88168-34-8.

[6] Zpráva o stavu kybernetické bezpečnosti ČR - 2019. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: NÚKIB, Brno [cit. 2021-04-24]. Dostupné z: https://nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf

[7] Kyberkriminalita. *Policie České republiky* [online]. Praha: Ministerstvo vnitra Ceske republiky, 2021 [cit. 2021-04-24]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[8] *Usnesení předsednictva České národní rady ze dne 16. prosince 1992: o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky*. In: . ČESKO, 1993, 2/1993, s. 18-19. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22426

[9] *Zákon ze dne 8. ledna 2009: trestní zákoník*. In: . ČESKO, 2009, 40/2009, 393/395. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405

[10] *Zákon ze dne 3. února 2012: občanský zákoník*. In: . ČESKO, 2012, 89/2012, s. 1035. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=24084

[11] *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. In: . EU, 2016, 2016/679. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS

[12] *Zákon ze dne 23. července 2014: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: . ČESKO, 2014, 181/2014. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27231

[13] VYHLÁŠKA ze dne 21. května 2018: o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů*. ČESKO, 2018, částka 43, 82/2018, s. 1122-1163. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38431

[14] Co je GDPR?. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. Praha: Mgr. Eva Škorničková [cit. 2021-04-25]. Dostupné z: https://www.gdpr.cz/gdpr/

[15] EPrivacy. *Deloitte Česká republika* [online]. Praha: Deloitte, 2021 [cit. 2021-04-25]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/risk/articles/eprivacy.html

[16] ŠEFČÍK, Antonín a Barbora KVASNICOVÁ. Sepsali jsme pro vás přehled doposud vydaných norem řady ISO/IEC 27000. *Kybernetická bezpečnost na internetu a zákon | NGSS* [online]. Praha: NEXT GENERATION SECURITY SOLUTIONS s.r.o., 2020 [cit. 2020-11-09]. Dostupné z: https://www.ngss.cz/clanek/46-sepsali-jsme-pro-vas-prehled-doposud-vydanych-norem-rady-iso-iec-27000

[17] ISO 27001 assessment. *UnderDefense CyberSecurity and Incident Response* [online]. New York: UnderDefense [cit. 2021-03-13]. Dostupné z: https://underdefense.com/iso-27001-assessment/

[18] Cost of Insider Threats. *ObserveIT | Insider Threat Software* [online]. Sunnyvale: Proofpoint, 2021 [cit. 2021-03-12]. Dostupné z: https://www.observeit.com/cost-of-insider-threats/

[19] A Data-Centric Approach to Security Monitoring. BOLLINGER, Jeff, Brandon ENRIGHT a Matthew VALITES. *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan*. First Edition. Sebastopol: O'Reilly Media, 2015, s. 50-51. ISBN 978-1-491-94940-5.

[20] What the Heck Is a SIEM Tool?. MILLER, David, Shon HARRIS, Allen HARPER, Stephen VANDYKE a Chris BLASK. *Security information and event management (SIEM) implementation*. New York: McGraw-Hill, 2011, xxvii - xxx. ISBN 978-0-07-170109-9.

[21] Efficient operations. NATHANS, David. *Designing and Building A Security Operations Center*. Waltham: Syngress, 2015, s. 13-21. ISBN 978-0-12-800899-7.

[22] Hustle and NetFlow. BOLLINGER, Jeff, Brandon ENRIGHT a Matthew VALITES. *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan*. First Edition. Sebastopol: O'Reilly Media, 2015, s. 129. ISBN 978-1-491-94940-5.

[23] Log Collection. MILLER, David, Shon HARRIS, Allen HARPER, Stephen VANDYKE a Chris BLASK. *Security information and event management (SIEM) implementation*. New York: McGraw-Hill, 2011, s. 81-82. ISBN 978-0-07-170109-9.

[24] The Anatomy of a SIEM. MILLER, David, Shon HARRIS, Allen HARPER, Stephen VANDYKE a Chris BLASK. *Security information and event management (SIEM) implementation*. New York: McGraw-Hill, 2011, s. 81-91. ISBN 978-0-07-170109-9.

[25] Detekce anomálií & Analýza chování sítě. *Flowmon - Řešení pro řízení výkonnosti a bezpečnosti vaší sítě* [online]. Brno: Flowmon Networks, 2021 [cit. 2021-04-29].

Dostupné z: https://www.flowmon.com/cs/solutions/security-operations/network-behavior-analysis-anomaly-detection

[26] SOC Defined. MURDOCH, Don. *Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases Notes from the Field (V1.02): A condensed field guide for the Security Operations team*. 1.02. CreateSpace Independent Publishing, 2019, s. 15. ISBN 978-1091493896.

[27] Conduct en Environmental Data Inventory Survey (EDIS). MURDOCH, Don. *Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases Notes from the Field (V1.02): A condensed field guide for the Security Operations team*. 1.02. CreateSpace Independent Publishing, 2019, s. 23-24. ISBN 978-1091493896.

[28] Log Management. MILLER, David, Shon HARRIS, Allen HARPER, Stephen VANDYKE a Chris BLASK. *Security information and event management (SIEM) implementation*. New York: McGraw-Hill, 2011, s. 55-63. ISBN 978-0-07-170109-9.

[29] LONVICK, Chris. RFC 3164: The BSD syslog Protocol. *Internet Engineering Task Force* [online]. Wilmington: IETF [cit. 2021-02-23]. Dostupné z: https://tools.ietf.org/html/rfc3164

[30] GERHARDS, Rainer. RFC 5424: The Syslog Protocol. *Internet Engineering Task Force* [online]. Wilmington: IETF [cit. 2021-02-23]. Dostupné z: https://tools.ietf.org/html/rfc5424

[31] Log Record Data Elements. MURDOCH, Don. *Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases Notes from the Field (V1.02): A condensed field guide for the Security Operations team*. 1.02. CreateSpace Independent Publishing, 2019, s. 223-224. ISBN 978-1091493896.

[32] ArcSight Common Event Format (CEF) Implementation Standard. In: *Digital Transformation and Enterprise Software Modernization | Micro Focus* [online]. Newbury: Micro Focus, 2021 [cit. 2021-02-23]. Dostupné z: https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-Common-Event-Format-CEF-Implementation-Standard/ta-p/1645557?attachment-id=68077

[33] IBM QRadar : Log Event Extended Format (LEEF). In: *IBM Knowledge Center - Home of IBM product documentation* [online]. Armonk: IBM [cit. 2021-02-23]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/b_Leef_format_guide.pdf?view=kc

[34] Service Name and Transport Protocol Port Number Registry. *Internet Assigned Numbers Authority* [online]. Los Angeles: Internet Corporation for Assigned Names and Numbers [cit. 2021-02-24]. Dostupné z: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[35] OKMIANSKI, Anton. 5426: Transmission of Syslog Messages over UDP. *Internet Engineering Task Force* [online]. Wilmington: IETF [cit. 2021-02-23]. Dostupné z: https://tools.ietf.org/html/rfc5426

[36] Oracle DB Audit. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/c_DSM_guide_Oracle_DB_Audit_overview.html

[37] What is an API?. *Red Hat - We make open source technologies for the enterprise* [online]. Raleigh: Red Hat, Inc., 2021 [cit. 2021-02-24]. Dostupné z: https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces

[38] SMB security enhancements. *Microsoft Docs* [online]. Redmond: Microsoft Corporation, 2021 [cit. 2021-02-24]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/storage/file-server/smb-security

[39] System requirements for virtual appliances. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_ha_vrt_ap_reqs.html

[40] QRadar M6 appliance overview. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/c_hwg_app_overview_m6.html

[41] The Homegrown SIEM. MILLER, David, Shon HARRIS, Allen HARPER, Stephen VANDYKE a Chris BLASK. *Security information and event management (SIEM) implementation*. New York: McGraw-Hill, 2011, s. 54. ISBN 978-0-07-170109-9.

[42] KAVANAGH, Kelly, Toby BUSSA a Gorka SADOWSKI. *Magic Quadrant for Security Information and Event Management*. Stamford, 2020.

[43] QRadar deployment overview. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/c_qradar_deployment_guide_overview.html

[44] All-in-One deployment. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/c_qradar_deployment_guide_all-in-one.html

[45] ISECO Toolset. *ISECO* [online]. Praha: ISECO [cit. 2021-05-09]. Dostupné z: https://www.iseco.global/Leaf_Iseco_Toolset_2020.pdf

[46] QRadar events and flows. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/c_qradar_deploy_event_and_flow_pipeline.html

[47] QRadar supported DSMs. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/r_supported_dsm_list.html?cp=SS42VS_7.4

[48] Fortinet FortiGate Security Gateway sample event messages. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/c_dsm_guide_fortinet_fortigate_security_gateway_sample_event_msg.html

[49] Service overview and network port requirements for Windows. *Microsoft Docs* [online]. Redmond: Microsoft Corporation, 2021 [cit. 2021-02-24]. Dostupné z: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements

[50] WinCollect overview. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.wincollect.doc/c_wincollect_overview_new.html?cp=SS42VS_7.4

[51] QRadar User Behavior Analytics. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.UBAapp.doc/c_Qapps_UBA_intro.html?cp=SS42VS_7.4

[52] How UBA works. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.UBAapp.doc/c_Qapps_UBA_process.html

[53] UBA dashboard with Machine Learning. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.UBAapp.doc/c_Qapps_UBA_ML_app_db.html

[54] Communication between WinCollect agents and QRadar. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/ com.ibm.wincollect.doc/c_ug_wincollect_comm_event_collector.html

[55] Installing and upgrading the WinCollect application on QRadar appliances. *IBM Knowledge Center* [online]. Armonk: IBM [cit. 2021-02-24]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.wincollect.doc/t_ug_wincollect_install.html

[56] Sysmon - Windows Sysinternals. *Microsoft Docs* [online]. Redmond: Microsoft Corporation, 2021 [cit. 2021-02-24]. Dostupné z: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

[57] IBM QRadar Content Extension for Sysmon. *IBM X-Force Exchange: Research, Collaborate and Act on threat intelligence* [online]. Armonk: IBM, 2021 [cit. 2021-03-28]. Dostupné z: https://exchange.xforce.ibmcloud.com/hub/extension/e41e758e2ab5786173438cd09219a9d0

[58] PgAudit: Open Source PostgreSQL Audit Logging. *GitHub: Where the world builds software* [online]. GitHub, 2021 [cit. 2021-03-29]. Dostupné z: https://github.com/pgaudit/pgaudit/blob/master/README.md

[59] *Nmap: the Network Mapper - Free Security Scanner* [online]. Insecure.Org [cit. 2021-04-18]. Dostupné z: https://nmap.org/

[60] Phishing & Spam. *IBM X-Force Exchange: Research, Collaborate and Act on threat intelligence* [online]. Armonk: IBM, 2021 [cit. 2021-03-28]. Dostupné z: https://exchange.xforce.ibmcloud.com/collection/Phishing-and-Spam-0777fb2ca2d2a93ccc01e1325b206c98

[61] *MITRE ATT&CK®* [online]. McLean: Mitre Corporation, © 2015-2021 [cit. 2021-04-22]. Dostupné z: https://attack.mitre.org/

[62] Remote System Discovery, Technique T1018. *MITRE ATT&CK®* [online]. McLean: Mitre Corporation, © 2015-2021 [cit. 2021-04-22]. Dostupné z: https://attack.mitre.org/techniques/T1018/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA	Authentication, authorization, accounting
ACS	Access Control System
AD	Active Directory
API	Application Programming Interface
AV	Anti-virus
BB	Building block – stavební blokalert
BPI	Bezpečnostní politika informací
BPI	Bezpečnostní politika informací
CA	Certifikační autorita
CEF	Common Event Format
CIA	Confidentiality, integrity, availability
CMDB	Configuration management database
CPU	Central Processing Unit
CSV	Comma-separated values
CTO	Chief technology officer
ČNB	Česká národní banka
DB	Databáze
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DLP	Data loss prevention
DMZ	Demilitarizovaná zóna
DNS	Domain Name System
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer

DSM	Device Support Module
DV	Data volume
EPS	Events Per Second
FQDN	Fully Qualified Domain Name
FTE	Full time equivalent
FW	Firewall
GDPR	General Data Protection Regulation
GPO	Group Policy objects
GUI	Graphic User Interface
GUI	Graphic User Interface
HW	Hardware
ICT	Information and Communication Technologies
ID	Identifikátor
IDM	Identity management
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPS	Intrusion Prevention Systems
IS	Informační systém
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEEF	Log Event Extended Format
LS	Logsource

LSX	Log Source Extension
MAC	Media Access Control
ML	Machine learning
MS	Microsoft
MTU	Maximum transmission unit
NBAD	Network behavior anomaly detection
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém
PoC	Proof of Concept
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RFC	Request for Comments
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SEM	Security Event Management
SFS	SquashFS
SFTP	SSH File Transfer Protocol
SIEM	Security Information and Event Management
SIEM	Security Information and Event Management
SIM	Security Information Management
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol

SNMP	Simple Network Management Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SOC	Security Operation Center
SQL	Structured Query Language
SSD	Solid-state drive
SSH	Secure Shell
SW	Software
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTM	Unified threat management
VLAN	Virtual LAN
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual private network
VSS	Video surveillance system
WLAN	Wireless LAN
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: KONTROLNÍ SEZNAM PŘÍPRAVY PRO NASAZENÍ

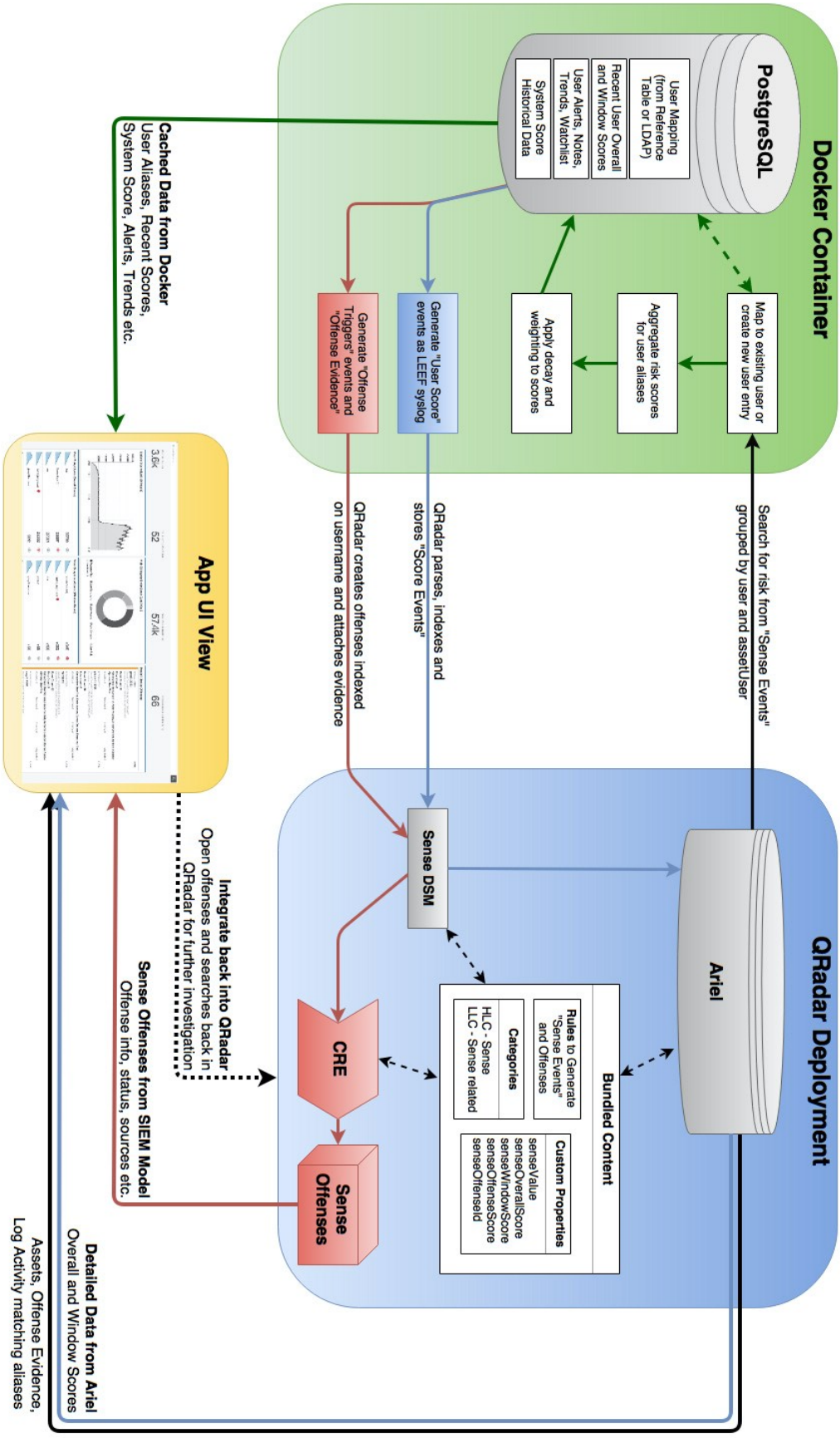
Položka	Termín splnění	Stav %	Číslo ticketu	Vlastník úkolu	Poznámka
Organizační předpoklady					
Představení záměru pořízení SIEM vedení společnosti					
Schválení záměru pořízení SIEM vedením společnosti					
Schválení FTE pro SIEM specialisty vedením společnosti					
Zajištění specialistů IT bezpečnosti interně nebo na trhu práce					
Revize nebo vytvoření předpisové základny pro zajištění logování					
Realizace schůzek s vlastníky obchodních procesů a vytvoření jejich seznamu					
Vytvoření seznamu informačních aktiv, dle jednotlivých obchodních procesů					
Technické předpoklady					
Provedení analýzy aktiv a vytvoření seznamu s parametry všech zdrojů logu					
Vytvoření seznamu technických předpokladů pro nasazení SIEM					
Předání a odsouhlasení technických předpokladů oddělením IT provozu					
Potvrzení připravenosti technických předpolkadů pro PoC					

PŘÍLOHA P II: ZADÁNÍ PRO HODNOCENÍ VÝBĚRU SIEM

Funkce / kritérium	Váha	Výr. 1	V1 %	Výr. 2	V2 %	Výr. 3	V3 %
Plně automatická korelace událostí	10		0		0		0
Více alertů do jedné události z více pravidel (řetězení událostí)	10		0		0		0
Historické korelace	8		0		0		0
Systémové korelace	8		0		0		0
Neomezený počet korelací souběžně	10		0		0		0
Uživatelsky definované akce při sepnutí pravidla	10		0		0		0
Interakce s jinými aplikacemi při sepnutí pravidla (volání API)	5		0		0		0
Alerting	10		0		0		0
Klasifikace incidentů	5		0		0		0
Management incidentů	5		0		0		0
Ladění false positive	8		0		0		0
Ukládání a čtení informací / vlastností z událostí do/z datových struktur	9		0		0		0
Rychlé hledání	10		0		0		0
SQL like hledání	10		0		0		0
Široké možnosti vstupů pro hledání	10		0		0		0
Historické hledání bez omezení	10		0		0		0
Možnost ukládání hledání	10		0		0		0
Možnost ukládání rozvržení výsledku hledání	10		0		0		0
Možnost uložení a exportu výsledku hledání	10		0		0		0
Uživatelsky definované funkce	5		0		0		0
Uživatelsky definované dashboardy	10		0		0		0
Uživatelsky definované reporty	10		0		0		0
Podrobně řízení oprávnění	10		0		0		0
API s dokumentací	8		0		0		0
Analýza chování uživatelů součásti řešení (UBA/UEBA)	10		0		0		0
Nativní práce s Flow součástí řešení	3		0		0		0
Korelační pravidla pro flow	3		0		0		0
Správa zdrojů logu	10		0		0		0
Automatická detekce nových zdrojů logů	8		0		0		0
Neomezený počet zdrojů logů	10		0		0		0
Široká podpora typů zdrojů logů	10		0		0		0
Možnost vytvoření vlastního typu logů	10		0		0		0
Možnost extrahovat vlastnosti z payloadu logu	10		0		0		0
Možnost obohacení logů	9		0		0		0

Funkce / kritérium	Váha	Výr. 1	V1 %	Výr. 2	V2 %	Výr. 3	V3 %
Možnost spojování víceřádkových logů	8		0		0		0
Možnost přeposílání logů	5		0		0		0
Volitelná dostupnost historických logů dle jeho zdroje (retence logů)	8		0		0		0
Správa síťová hierarchie	5		0		0		0
Správa aktiv	5		0		0		0
Podpora zásuvných modulů	10		0		0		0
Práce s identitami	10		0		0		0
Způsob licencování							
On-site řešení	10		0		0		0
Podpora cloudu	10		0		0		0
Agenti na koncových stanicích uživatelů	5		0		0		0
Napojení na kvalitní on-line zpravodajství o hrozbách (threat inteligence)	10		0		0		0
Ochrana proti výpadku	10		0		0		0
Ochrana db proti poškození / úpravě / smazání	10		0		0		0
Intuitivní webové GUI	10		0		0		0
Kompletní audit systému a uživatelů SIEM	10		0		0		0
Možnost interní i externí zálohy systému i logů, vč. jejich zabezpečení	10		0		0		0
Lokální (CZ) expertní podpora s certifikací od dodavatele	10		0		0		0
Monitoring stavu systému	10		0		0		0
Možnost napojení na správu zranitelností	5		0		0		0
Maintanance od výrobce formou předplatného	10		0		0		0
Možnost virtualizace	10		0		0		0
All in one instalace	5		0		0		0
Počet serverů (xxxx EPS, xxxxx FPS)	10		0		0		0
Možnost PoC	10		0		0		0
Cena HW – jednorázově	50		0		0		0
Cena licencí – jednorázově	50		0		0		0
Cena předplatného	100		0		0		0
Cena implementace	50		0		0		0
Cena školení	50		0		0		0
Cena maintenance – 1 rok	100		0		0		0
Cena podpory – 1rok	100		0		0		0
Max. počet bodů	**1000**		**0**		**0**		**0**

PŘÍLOHA P III: FUNKČNÍ SCHÉMA ROZŠÍŘENÍ UBA



PŘÍLOHA P IV: MODELOVÁ TABULKA SÍŤOVÝCH PROSTŘEDKŮ

VLAN ID	Popis	Podsíť	Zařízení	FQDN	IP adresa
10	Síťové prvky	10.0.10.0/24	FW	fw.bc-test.cz	10.0.10.1
	(management)		Core switch	sw.bc-test.cz	10.0.10.2
20	Provozní servery	10.0.20.0/24	DC, AD, DNS	dc.bc-test.cz	10.0.20.1
			DHCP server	dhcp.bc-test.cz	10.0.20.2
			SMTP server	smtp.bc-test.cz	10.0.20.3
			NTP server	ntp.bc-test.cz	10.0.20.4
			Zálohovací server	bk.bc-test.cz	10.0.20.5
			Monitorovací server	mon.bc-test.cz	10.0.20.6
30	Aplikační servery	10.0.30.0/24	Souborový server	fs.bc-test.cz	10.0.30.1
			Business aplikace	ba.bc-test.cz	10.0.30.2
40	Databázové servery	10.0.40.0/24	Databázový server 1	db.bc-test.cz	10.0.40.1
50	Bezpečnostní servery	10.0.50.0/24	QRadar All-in-one	qr.bc-test.cz	10.0.50.1
			WinCollect	wc.bc-test.cz	10.0.50.2
			Síťové datové úložiště	nas.bc-test.cz	10.0.50.3
60	Uživatelé	10.0.60.0/23			
70	Uživatelé VPN	10.0.70.0/23			
80	Hosté WLAN	10.0.80.0/24			
100	DMZ	10.0.100.0/24	Reverzní proxy	rp.bc-test.cz	10.0.100.1