Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Uživatelská behaviorální analýza pro systémy SIEM

Diplomová práce

Autor: Bc. Jan Nedbal
Studijní obor: Informační management

Vedoucí práce: Mgr. Josef Horálek Ph.D.

Odborný konzultant: Ing. Lukáš Vízner, Autocont a.s.

Hradec Králové Září 2018

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 3.10.2018 Bc. Jan Nedbal

Poděkování:

Děkuji vedoucímu diplomové práce Mgr. Josef Horálek Ph.D. za metodické vedení práce a Ing. Lukáš Vízner za cenné rady při implementaci.

Anotace

Nebezpečí krádeže a zneužití informací je v dnešní době běžnou záležitostí, o to více to platí pro kybernetické prostředí. V případě, že organizace vlastní a používá software jako je IDS nebo komplexnější SIEM monitorující aktivitu a s ní spojené hrozby, které přicházejí z venčí, a snaží se proniknout do infrastruktury, mohlo by se zdát, že má takřka vyhráno. V dnešním světě je stejně tak kritické nasazení software monitorující aktivitu uvnitř sítě. Predikce a analýza lidského chování je ale velmi obtížná a z toho pramení i značná problematika pro zvolení optimálních nástrojů. Jedním z účinných nástrojů pro tyto účely je modul uživatelské behaviorální analýzy, který je nadstavbovým produktem pro některé z nabízených SIEM systémů. Díky užití strojového učení je schopen se stále učit a snáze odhadnout změny nebo problémy v infrastruktuře.

Tato diplomová práce má jako hlavní cíl představení principů a možností užití uživatelské behaviorální analýzy v systémech SIEM. První kapitola je věnována bezpečnosti, standardům ISO a vymezení legislativního rámce ČR pro tuto problematiku. Druhá kapitola pojednává o detailním definování systémů SIEM, jejich funkcionalitě a logické stavbě. Třetí kapitola přibližuje konkrétní SIEM aplikace, které jsou zkoumány v praktické částí práce – IBM Security QRadar SIEM a AlienVault OSSIM/ USM. Kapitola čtvrtá obsahuje komparaci obou zvolených SIEM aplikací. Pátá kapitola přibližuje principy uživatelské behaviorální analýzy a strojového učení. Kapitola šestá představuje konkrétní implementace SIEM a s tím spojené UBA moduly. Kapitola sedmá se věnuje shrnutí poznatků práce. Závěrečná práce je věnována doporučení a celkovým závěrům.

Annotation

Title: User behavior analytics in the SIEM systems

In today's society, the potential for theft or misuse of an organization's precious information is a constant threat that increases exponentially in the cyber world. Some organizations are already using software such as IDS or the more complex SIEM, monitoring activity and threats coming from the outside of the infrastructure. Unfortunately, under the current circumstances this is simply not enough. Developing the software's ability to predict and analyze the behavior in the infrastructure is just as important as monitoring incoming traffic. For prediction and analysis, there are several applications able to identify possible threats. I've chosen the module for user behavioral analysis which is integrated for some of the available SIEM systems. This module is able to use machine learning principles in order to deliver the sharpest predictions for the user's behavior and communication within the intranet and is constantly learning new behavioral patterns as the user changes. The purpose of this master's thesis is to introduce the principles of user behavioral analysis and its uses. The first chapter explains the whole security content valid for the context of security information as well as the "Law of cyber security." The second chapter acts as a deep scope into the functionality of the SIEM systems and the logical syntax it has. The third chapter describes the concrete SIEM applications, which are lately used for the purposes of implementation of UBA. The fourth chapter delves into comparing the IBM Security QRadar SIEM and AlienVault OSSIM/ USM. The fifth chapter defines the principles of user behavior analysis, and machine learning. The sixth chapter introduces the implementation of the SIEM, its UBA modules and presents both defined and custom use cases. The seventh chapter serves as a summary of the first six chapters. The final chapter is dedicated to the recommendations

Obsah

1 Úvod ... 1
2 Cíl práce ... 3
2.1 Bezpečnost ... 3
2.1.1 Informační bezpečnost ... 5
2.1.2 Kybernetická bezpečnost ... 6
2.2 Standardy ISO ... 7
2.2.1 ISO 27000 – Overview and Vocabulary ... 8
2.2.2 ISO 27001 (Information security management systems) ... 9
2.2.3 ISO/IEC 27002 (Information technology and security techniques) ... 12
2.2.4 ISO/IEC 27003 (Information security management systém and implementation guidance) ... 13
2.2.5 ISO/IEC 27004 Measurement ... 13
2.3 Zákon o kybernetické bezpečnosti ... 14
3 Security Information and Event management ... 18
3.1 Log management ... 19
3.2 IT Regulatory Compliance ... 20
3.3 Event Correlation ... 20
3.4 Architektura SIEM ... 21
3.4.1 Source device ... 22
3.4.2 Log collection ... 22
3.4.3 Normalization and parsing of logs ... 24
3.4.4 Rule engine and correlation engine ... 24
3.4.5 Log storage ... 25
3.4.6 Monitoring ... 26
4 IBM Security QRadar SIEM ... 28
4.1 Architektura IBM Security QRadar SIEM ... 28
5 AlienVault OSSIM ... 31
6 Porovnání QRadar a AlienVault ... 34
6.1.1 QRadar ... 35
6.1.2 AlienVault ... 37
6.1.3 Komparace funkcionality QRadar a AlienVault ... 39
7 Uživatelská behaviorální analýza ... 41

7.1 Strojové učení 44
8 Metodika zpracování 45
8.1 Instalace SIEM aplikací 46
8.1.1 Instalace IBM Security QRadar SIEM 46
8.1.2 Princip kolekce dat o uživatelích v UBA QRadaru 48
8.1.3 Instalace AlienVault OSSIM 54
8.2 Užití modulu uživatelské behaviorální analýzy na vestavěném Use case 57
8.2.1 Vlastní Use case – login failure 64
8.2.2 Vlastní Use Case – uživatelská změna na serveru 66
9 Zhodnocení praktické části (shrnutí výsledků) 70
10 Závěry a doporučení 71
11 Seznam použité literatury 73

Seznam obrázků

Obrázek 1 - Maslowova pyramida potřeb, převzato (Salado & Nilchiani, 2013) 3

Obrázek 2 - Přehled ISO 27k family, převzato a upraveno (ISO/IEC 27001, 2018) .. 9

Obrázek 3 -PDCA cyklus pro ISMS, převzato a upraveno (ISO/IEC 27001, 2018) ...10

Obrázek 4 - Blokové schéma, převzato (NÚKIB, 2018) 15

Obrázek 5 - Architektura SIEM, převzato a upraveno (Miller, 2011).....18

Obrázek 6- Proces zpracování událostí v SIEM, převzato a upraveno (Miller, 2011) 21

Obrázek 7 - Podoba raw logu generovaného zdrojovým zařízením, vlastní zpracování 22

Obrázek 8- Grafické znázornění pravidla autentizace, převzato a upraveno (Vízner, 2011) 25

Obrázek 9 – Grafický interface QRadar, vlastní zpracování (2018).....27

Obrázek 10 - QRadar architektura, převzato a upraveno (IBM corp., 2018) 29

Obrázek 11- QRadar console, vlastní zpracování (2018).....30

Obrázek 12- USM appliance, převzato a upraveno (AlienVault, 2018) 31

Obrázek 13- AlienVault architektura, převzato a upraveno (AlienVault, 2018).....33

Obrázek 14 -QRadar – instalace, vlastní zpracování.....46

Obrázek 15 - QRadar – web konzole, vlastní zpracování.....47

Obrázek 16 - QRadar – proces sběru dat UBA, převzato a upraveno (IBM corp., 2018) 48

Obrázek 17 -QRadar UBA – GUI 1, vlastní zpracování.....49

Obrázek 18 - QRadarUBA – GUI2, vlastní zpracování.....49

Obrázek 19 - QRadar UBA nastavení přes GUI, vlastní zpracování.....50

Obrázek 20 - QRadar – ML app – User analytics, vlastní zpracování.....51

Obrázek 21 - QRadar – ML app – User activity by category, vlastní zpracování.....52

Obrázek 22 - QRadar – ML app – Risk posture, vlastní zpracování.....53

Obrázek 23 - QRadar – ML app – Activity distribution, vlastní zpracování 53

Obrázek 24 - QRadar – ML app – Peer Group, vlastní zpracování 53

Obrázek 25 - AlienVault OSSIM instalace, vlastní zpracování 54

Obrázek 26 - AlienVault OSSIM – web konzole, vlastní zpracování 55
Obrázek 27 - Konverzace s AlienVault SW expertem, vlastní zpracování 55
Obrázek 28 - GUI AlienVault OSSIM – Netflow, vlastní zpracování 56
Obrázek 29 - Use case – prvotní skóre, vlastní zpracování 58
Obrázek 30- Use case – časová osa rizikových aktivit, vlastní zpracování 58
Obrázek 31 - Use case – prvotní spider graf, vlastní zpracování 59
Obrázek 32 -Zasílání událostí pomocí logrun skriptu, vlastní zpracování 59
Obrázek 33 - Use case – změna v aktivitách, vlastní zpracování 60
Obrázek 34 - Nebezpečné IP adresy – IBM X-force, vlastní zpracování 60
Obrázek 35 - Use case, nárůst skóre a dashboard, vlastní zpracování 61
Obrázek 36 - Use case – seznam spuštěných pravidel, vlastní zpracování 61
Obrázek 37 - Use case – překročení limitu pro generování offense, vlastní zpracování 62
Obrázek 38 - Use case – rozpis rizikových aktivit uživatele, vlastní zpracování 62
Obrázek 39 -Use case, modifikace spider grafu – zvýšení aktivity, vlastní zpracování 63
Obrázek 40 - Use Case – generování offense, UBA modul, vlastní zpracování 63
Obrázek 41 - Use case – generování offense, prostředí QRadaru, vlastní zpracování 63
Obrázek 42 - Use case – vytvořené pravidlo pro monitoring login failure, vlastní zpracování 64
Obrázek 43 -Use case, nárůst skóre uživatele, vlastní zpracování 65
Obrázek 44 - Use case – rozpis rizikových aktivit uživatele, vlastní zpracování 65
Obrázek 45 - Use Case – generování offense, UBA modul, vlastní zpracování 65
Obrázek 46 - Use case – vytvořené pravidlo pro sledování změny na serveru, vlastní zpracování 66
Obrázek 47 - Use Case – přidání uživatele do skupiny doménových administrátorů, vlastní zpracování 67
Obrázek 48 - Use case – změna uživatelského skóre po spuštění pravidla, vlastní zpracování 67
Obrázek 49 - Use case – generování bezpečnostního incidentu po spuštění pravidla, vlastní zpracování 68

Obrázek 50 - Use case – seznam podezřelých aktivit, vlastní zpracování 68

Obrázek 51 - Use case – spider graf po spuštění group pravidla, vlastní zpracování 69

Obrázek 52 - Use case – historie bezpečnostních incidentů, vlastní zpracování.....69

Seznam tabulek

Tabulka 1 - System requirements QRadar, vlastní zpracování.....35

Tabulka 2 - System requirements – AlienVault, převzato a upraveno (AlienVault 2018) 37

1 Úvod

Bezpečnost v prostředí internetu a s ním spojenými informačními systémy je tématem, kterému je přikládána stále větší důležitost. Dle některých zdrojů je kybernetický útok třetí nejčastější hrozbou, hned po zemětřesení a jiných extrémních klimatických jevech. Pokud je organizace schopna se úspěšně chránit před útoky vedené zvenčí, má napůl vyhráno. Mnohdy je ale stejně tak důležité mít síťovou infrastrukturu zabezpečenou jak proti útokům z venku, tak proti těm zevnitř. Technologie SIEM je schopná sbírat data ze všech zdrojových zařízení v intranetu a díky analýze v reálném čase je schopna redukovat šanci vzniku potencionálního bezpečnostního incidentu na minimum. Avšak v případech, kdy se jedná o nebezpečné chování uvnitř infrastruktury, je nutné, aby byla funkcionalita těchto analytických prvků posunuta na další úroveň. Jedním z možných řešení je aplikování principů uživatelské behaviorální analýzy. Tyto principy řeší uživatelské interakce a komunikaci uvnitř infrastruktury. Představený modul UBA je schopen vytvořit jakýsi vzorek normálního chování a posléze definovat odchylky, které mohou poukazovat na hrozbu uvnitř sítě.

V rámci mého působení ve firmě Autocont a.s. mi byla nabídnuta možnost pokračovat v problematice SIEM systémů a definování pokročilých modulů, které nabízí. Téma jsem přijal, jelikož jsem se problematikou SIEM systémů zaobíral i ve své bakalářské práci, a je to hlavní náplní mé práce ve firmě.

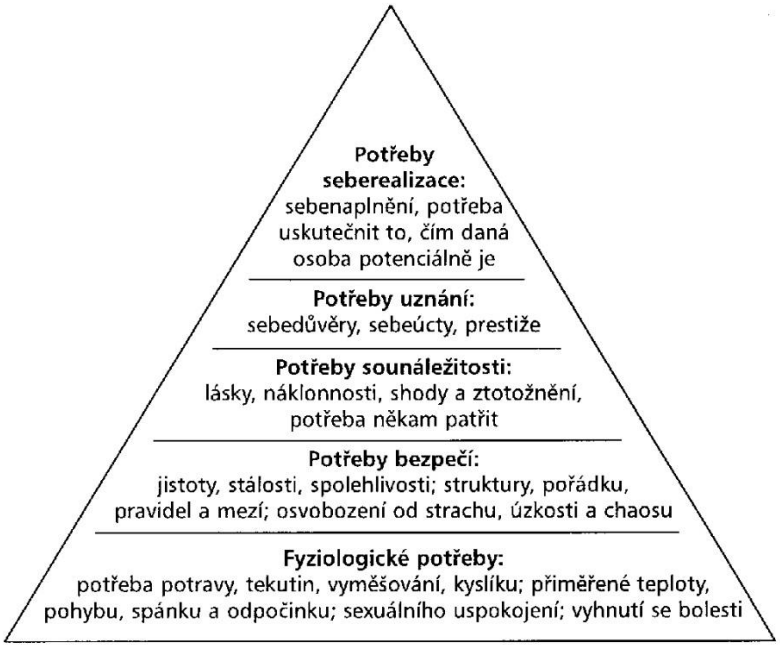
Hlavním cílem práce je definovat použití principů uživatelské behaviorální analýzy a tuto skutečnost demonstrovat na konkrétních zvolených SIEM aplikacích a rovněž komparace těchto modulů mezi sebou z hlediska jejich funkcionality. Samotná práce je rozdělena do 10 kapitol včetně úvodu a závěru. Úvodní část přibližuje problematiku SIEM systémů, uživatelské behaviorální analýzy a také pojednává o struktuře a cílech diplomové práce. První kapitola je věnovaná bezpečnosti a [i]legislativním restrikcím vyplývajícím z aktualizované vyhlášky Zákona o kybernetické bezpečnosti. Kromě zákona jsou zde definovány také standardy ISO 27 000, které úzce souvisí s SIEM systémy. Druhá kapitola je věnovaná bližšímu seznámení s logickou strukturou a funkcionalitou SIEM systémů. Třetí a čtvrtá kapitola jsou věnovaný konkrétním SIEM aplikacím, které byly vybrány pro pozdější implementaci a demonstrování principů UBA a s ním spojenými use case. Pátá kapitola představuje komparaci mezi vybranými SIEM aplikacemi – IBM Security QRadar SIEM a AlienVault USM/OSSIM, a to dle přesně definovaných parametrů. Šestá kapitola definuje funkcionalitu uživatelské behaviorální analýzy a s ní spojenou metodou strojového učení. Sedmá kapitola obsahuje poznatky z implementace a zavádění UBA modulu pro SIEM aplikace. V kapitole osmé jsou shrnuty poznatky z práce. Poslední je závěrečná část pojednávající o dosažených cílech a možnostech pro další výzkum.

Diplomová práce obsahuje řadu cizích pojmů, které se často obtížně předkládají do češtiny z důvodu absence adekvátních překladů. Tyto pojmy jsou z pravidla vysvětleny přímo v textu práce.

2 Cíl práce

2.1 Bezpečnost

Bezpečnost je všudypřítomným faktorem, který lidstvo provází od jeho počátků. ejí důležitost můžeme nalézt i v Maslowově pyramidě potřeb (Salado, Nilchiani, 2013) kde bezpečnost figuruje hned v dalším stupni po uspokojení bazálních potřeb jako je potřeba jíst či pít. Nyní pokud je opomenut základní faktor potřeby bezpečí a přesuneme se na časové ose do přítomnosti, představuje otázka bezpečnosti stále důležitější téma a jeho významnost má s přechodem do informační společnosti gradující tendenci. Smutnou pravdou však je, že většina organizací faktor bezpečnosti ve své infrastruktuře značně podceňuje, což může mít dopad na potencionálních ztrátách informací a dat, pokud bude na takovou infrastrukturu útok skutečně podniknut.



Obrázek 1 - Maslowova pyramida potřeb, převzato (Salado & Nilchiani, 2013)

Než bude přistoupeno ke konkrétním aspektům bezpečnosti a jejich klasifikaci, je nutné nejprve definovat, co to bezpečnost je. Bezpečnost lze definovat vícero způsoby, nicméně z obecné sémantické definice lze vyvodit, že bezpečnost je stav, kdy nehrozí žádné nebezpečí, není mu nikdo vystaven nebo je mu poskytnuta ochrana před nebezpečím, či je nepochybný zaručený a důvěryhodný. *(Mareš, 2017*)

Z dílčí definice lze usoudit, že vymezení bezpečnosti je prováděno v negativním smyslu, tudíž lze očekávat přítomnost negativních vlivů nebo něčeho, co bezpečný stav narušuje.

Jak již bylo zmíněno, bezpečnost je nutné klasifikovat dle segmentu užití – mnohdy je termín „bezpečnost“ nahrazován anglickým ekvivalentem „security and safety,“ tato skutečnost je přisuzována absenci diferenciace mezi těmito dvěma pojmy (ve slovnících je jeden definován druhým).

Nyní bude definována klasifikace bezpečnosti, jejichž název se mnohdy odvíjí od jejího charakteru, tak jak je definován dle Zemanovy definice bezpečnosti. *(Zeman, 2002)*

- Vojenská,
- ekonomická,
- ekologická,
- sociální,
- lidská,
- informační,
- kybernetická…

V rámci této práce není nutné vymezovat všechna zmíněná odvětví, ve kterých lze na pojem bezpečnosti narazit. Mnohdy lze bez předchozího definování odhadnout, čím se daná oblast zabývá, a od čeho člověka nebo jinou instituci chrání.

Pro kontext práce jsou klíčové dvě poslední vymezené sféry bezpečnosti – informační a kybernetická. Tyto dvě oblasti budou nyní blíže specifikovány, aby bylo možné později porozumět celkové problematice vytyčené v práci.

(Zeman, 2002, str. 11)

2.1.1 Informační bezpečnost

Citlivé informace musí být bezpečně uchovány, nesmí být změněny, přesunuty nebo upravovány bez povolení. Informační bezpečnost je vytvořena tak, aby byla schopná zvládat rizika vycházející z analýzy rizik. Ve světě informací může být rizikem či hrozbou takřka cokoliv. Zmíněná bezpečnost se snaží chránit důvěrnost (confidentiality), integritu a dostupnost (availability) informací a systémových dat, před těmi, který by k nim neměli mít přístup nebo s nimi mají nekalé úmysly. Princip výše zmíněné ochrany je často adresován jako CIA Triad of information security *(Dardick, 2010)*. Bohužel brzy přestala tato triáda být v komplexní problematice bezpečnosti informací dostačující, tudíž bylo nutné rozšířitdefinici o další nezbytné atributy, z čehož se posléze vyvinul tzv. Parker hexad *(Dardick, 2010)*, který kromě již zmíněných obsahuje navíc ještě vlastnictví (possession), autentičnost (authenticity) a prospěšnost (utility).

Nyní budou definovány dílčí principy Parker hexad.

- Confidentiality,
    - Potvrzení o přístupy k informacím pouze pro ty, kteří k nim mají mít přístup.
- integrity,
    - Zaručená ucelenost všech metod a principů v každém okamžiku.
- availability,
    - Míra, s jakou jsou obsažené informace dostupné a zároveň relevantní.
- posession,
    - Řeší, jakým způsobem je zajištěno definování vlastnictví.
- authenticity,
    - Atribut zaobírající se kvalitou autentičnosti nebo vytvořená autorita pro rozhodování v procesu autentity informací a dat.
- utility.
    - Občas také nazývána jako relevance – vhodnost a použitelnost daných informací nebo dat.

(Dardick, 2010, s. 6-65)

2.1.2 Kybernetická bezpečnost

Definování kybernetické bezpečnosti nelze provést zcela jednoznačně, ba co víc, spousty současných publikací užívají pojmu „cyber security“ v kontextu značné similarity s „information security.“ Je pravda, že pro většinu incidentů z prostředí kybernetické bezpečnosti to platí, stejně jako lze aplikovat principy „CIA“ na většinu jejich incidentů.

Jednou z definic může být ta, jak je vysvětlena dle Merriam-Webster: „*measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack*.” *(Merriam-Webster, 2018)* Rozdílnou interpretaci pak představuje definice od ITU (International Telecomunications Union): kybernetická bezpečnost je kolekcí nástrojů, politik, bezpečnostních konceptů, přístupů risk managementu, preventivních akcí, tréninku, best practise a v neposlední řadě technologiemi, které lze použít pro ochranu kybernetického prostředí a důležitých uživatelských či firemních dat a informací.

Z výše zmíněných definic jasně vyplývá vzrůstající důležitost řešení problematiky asociované s kybernetickou bezpečností. Tuto skutečnost podporuje i následující fakt zmíněný autory von Solms a van Niekerk v článku *From information security to cyber security*. *(Von Solms a Van Niekerk, 2013)* Velká Británie stanovila kybernetickou bezpečnost jako jednu z nejvyšších priorit a vyčlenila více než 650 milionů liber na program věnující se kybernetické bezpečnosti včetně asociovaných hrozeb.

Základní principy kybernetické bezpečnosti jsou definovány stejným způsobem, jako je tomu u informační bezpečnosti tzn. *Confidentiality, availability, integrity*. Jak již ale bylo zmíněno dříve, nejedná se o synonyma. Rozdíl lze vysledovat na tom, co by měla daná bezpečnost chránit. Vždy se jedná o ochranu aktiva (cenné komodity), nicméně v případě informační bezpečnosti je definice ochrany aktiva zahrnuta napříč všemi aspekty informace samotné. Ochrana v kontextu informační bezpečnosti se nevztahuje pouze na technologie, ICT infrastrukturu nebo informace, které nejsou pomocí informačních technologií zaznamenávány nebo zpracovány. Naproti tomu kybernetická bezpečnost má za úkol chránit konkrétní osobu, zájmy celé společnosti nebo kritickou národní infrastrukturu. V podstatě se dá říct, že v tomto případě do této problematiky spadá kdokoliv nebo jakýkoliv *asset* (aktivum), dosažitelné v kyber prostoru. *(Von Solms a Van Niekerk, 2013 & Rowe, Lunt & Ekstrom, 2011)*

Z toho důvodu lze usoudit, že kybernetická bezpečnost není analogií informační bezpečnosti. Především z důvodu nutné ochrany nejen assetů, nicméně i kyber prostoru jako takového.

Při definování jednotlivých druhů bezpečnosti nelze zapomenout na standardy ISO, které se danou problematikou hluboce zaobírají, především pak standardy ISO 27k family. Tyto standardy budou v další části práce zmíněny a definovány.

2.2 Standardy ISO

Než bude přistoupeno k definování jednotlivých druhů standardů relevantních pro kontext informační bezpečnosti, budou nejprve objasněna základní terminologie.

ISO (*International organization for standardization)* – je mezinárodní organizací zabývající se standardizací a vytvářením norem. Sdružuje experty napříč celým světem a čítá 162 národních certifikačních autorit. Jejím hlavním úkolem je sdílení znalostí a na základě nich vytvářet mezinárodní normy, představující doporučené řešení pro různou problematiku. (About ISO, 2017)

IEC (*International Electrotechnical Commission)* – jinak známá jako mezinárodní elektrotechnická komise, je organizací publikující mezinárodní standardy pro elektrické a elektronické produkty, systémy a služby. Její publikace slouží jako základ pro mezinárodní standardizaci a rovněž jako v případě standardů ISO slouží jako určitá záruka kvality, pokud jej organizace vlastní. Komise IEC úzce spolupracuje s ISO a také s ITU (*International Telecommunication Union*) především z důvodu zamezení redundancím nebo duplicitních standardů. (About IEC, 2017)

Standard ISO je sdružením doporučení a best practises, které pomáhají optimálním způsobem řešit problematiku týkající se produktů, služeb nebo systémů za účelem dodržet určitou úroveň kvality, bezpečnosti a efektivnosti. Hlavní výhodou využití ISO standardů je jeho výpovědní hodnota. V případě, že daná organizace vlastní výše zmíněné standardy, lze předpokládat, že se jedná o důvěryhodnou firmu, neboť jsou jeho produkty, služby nebo firemní procesy optimalizovány. Zatím bylo vydáno 21989 standardů a s tím souvisejících dokumentů. (About ISO, 2017)**Standardy ISO 27000 family**

Sdružení standardů ISO v rámci rodiny 27000 je nejdůležitějším souhrnem v kontextu s řešením bezpečnosti informací. V minulosti byly užívány standardy BS 7799 a ISO 17799, které jsou v současné době nahrazeny výše zmíněným.

V následující části práce budou definovány základní charakteristiky jednotlivých standardů rodiny ISO 27000.

2.2.1 ISO 27000 – Overview and Vocabulary

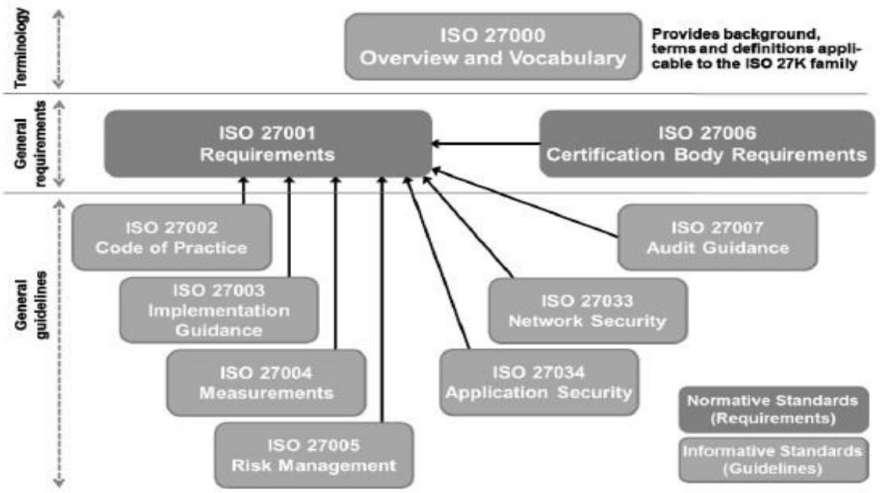
Mezinárodní standardy pro management systémů zprostředkovávají model, díky kterému je možné efektivně nastavit, operovat a řídit systém. Tento model začleňuje klíčové postupy a charakteristiky, které byly vyzkoumány a odsouhlaseny experty, kteří jsou součástí dříve zmíněných „ISO bodies.“ Pro oblast informační bezpečnosti je v rámci ISO definován velmi důležitý pojem, resp. rámec kroků, vedoucí k optimalizované podobě informačního procesu. Pojem **ISMS** (Information Security Management Systém) je zmiňován napříč všemi standardy ISO 27k family. S jeho pomocí lze vytvořit a implementovat rámec, který bude účinným způsobem spravovat důležité assety v rámci firemní infrastruktury.

Následuje výčet Standardů ISO, jinak nazývaných také jako ISMS standardy:

- ISO/IEC 27000, Information security management systems — Overview and vocabulary
- ISO/IEC 27001, Information security management systems — Requirements
- ISO/IEC 27002, Code of practice for information security controls
- ISO/IEC 27003, Information security management system implementation guidance
- ISO/IEC 27004, Information security management — Measurement
- ISO/IEC 27005, Information security risk management
- ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing
- ISO/IEC TR 27008, Guidelines for auditors on information security controls
- ISO/IEC 27009, Sector-specific application of ISO/IEC 27001 — Requirements
- ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000‑1
- ISO/IEC 27014, Governance of information security
- ISO/IEC TR 27015, Information security management guidelines for financial services
- ISO/IEC TR 27016, Information security management — Organizational economics
- ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- ISO/IEC 27018, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27019, Information security management guidelines based on ISO/IEC 27002 for proces control systems specific to the energy utility industry

(ISO/IEC 27000, 2018)



Obrázek 2 - Přehled ISO 27k family, převzato a upraveno (ISO/IEC 27001, 2018)

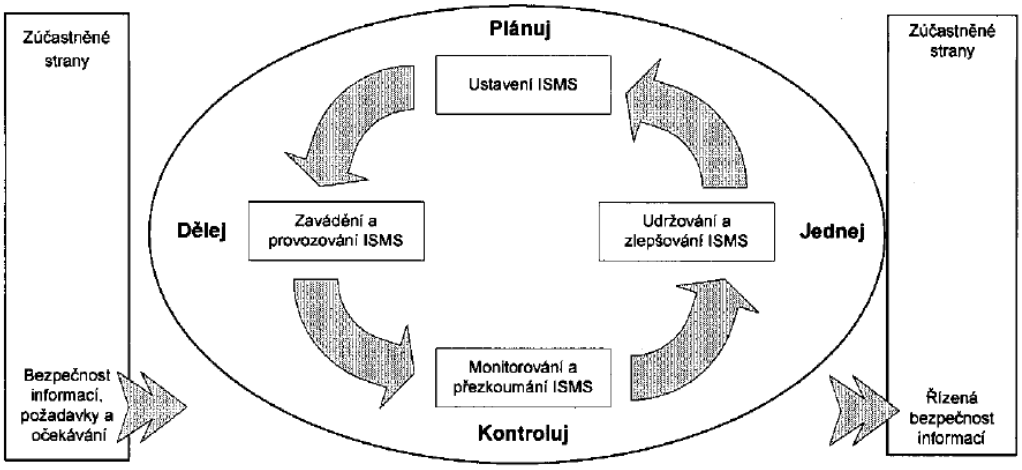
Pro účely této práce jsou důležité především standardy ISO 27001, ISO 27 002, ISO 27 003 a ISO 27 004. Tyto standardy jsou rovněž klíčové v kontextu Zákona o kybernetické bezpečnosti (181/2014 Sb.) a vyhlášky o kybernetické bezpečnosti 82/2018 Sb., který bude definován v následující části práce.

2.2.2 ISO 27001 (Information security management systems)

Mezinárodní norma má primárně poskytovat podporu pro ustavení, zavádění, provozování, monitorování, udržování a zlepšování **systému managementu bezpečnosti informací** (Information Security Management Systém či ISMS). Akceptace ISMS jakožto strategické rozhodnutí je podmíněno cíli, potřebami organizace, používanými procesy, velikostí a strukturou organizace a požadavky na bezpečnost.

Norma ISO/IEC 27001 poskytuje celistvý model pro zavedení principů popsaných také ve směrnici OECD, upravující hodnocení rizik, navržení a implementaci bezpečnostních principů, management bezpečnosti a opětovné hodnocení bezpečnosti. Aplikace ISMS je klíčová pro kontext definování požadavků pro ISMS, vytváří přímou podporu a rovněž cílené vedení za účelem vzniku, implementace a kontinuálního zlepšování ISMS.

Principy ISMS vychází z tzv. PDCA modelu (Plan-Do-Check-Act), který může být souhrnně aplikován na všechny procesy ISMS.



Obrázek 3 -PDCA cyklus pro ISMS, převzato a upraveno (ISO/IEC 27001, 2018)

- **Plánování (ustavení ISMS)**

Je nutné definovat politiky ISMS, cíle, procesy a postupy asociované s managementem rizik a zlepšováním bezpečnosti informací takovým způsobem, aby bylo v dostatečné míře zajištěno plnění v souladu s celkovou politikou a cíli organizace.

- **Implementace a provozování ISMS**

Zavádění a využívání politiky ISMS, jejich opatření, procesů a postupů.

- **Monitorování a přezkoumání ISMS**

Proces explorace, který posuzuje kvalitu zavedení ISMS oproti již definovaným cílům a politice organizace. Součástí je i reportování dosažených výsledků vedení organizace k přezkoumání.

- **Udržování a zlepšování ISMS**

Akceptování opatření k napravení a preventivním opatření, které jsou založeny na výsledcích interního auditu ISMS, přezkoumání systému řízení vedením organizace a snaha o proces kontinuálního a efektivního zlepšování ISMS.

Jelikož je tento standard klíčový pro kontext práce, bude nyní podrobněji definován.

Ustavení ISMS je podmíněno **definováním rozsahu a hranic**, které závisejí na konkrétních požadavků a rysů činnosti společnosti, její struktury, technologické vybavenosti, lokality nebo vlastněných aktiv. Tyto hranice jsou stěžejní pro další krok, ve kterém je stanovena politika ISMS, mimo jiné obsahující rámec ustanovující směr řízení, zásady činností asociované s informační bezpečností. Politika rovněž musí brát v potaz požadavky kladené organizací, veškerá legislativní restrikce nebo požadavky regulatorní povahy a rovněž je nutné vytvořit vazby na stěžejní části strukturu organizace a její risk management.

Management rizik je v kontextu implementace ISMS klíčový, z toho důvodu je nutné, aby byl jednoznačně určen přístup organizace k této problematice. V prvé řadě zvolit vhodnou metodiku pro evaluaci rizik, vytvořit kriteriální atributy pro schválení rizik a určit, jaké jsou jejich úrovně. Je nutné, aby bylo možné danou metodiku v budoucnu porovnávat a také opakovat na různé procesy.

Po definování nezbytných politik je dalším logickým krokem **implementace a provozování ISMS.** V tomto bodě je již formulován základní rámec včetně politik managementu rizik a bezpečnosti informací jako takových, nyní budou vysloveny konkrétní plány, jak zvládat konkrétní druhy výskytu rizik v dané organizaci. Podle odsouhlasených plánů je pak celý podnik, v kontextu ISMS, řízen. Velmi důležitým faktorem je rovněž zvyšování povědomí o dané problematice, vedení školení a zavedení postupů nebo preemptivních procesů pro včasnou detekci a reakci na bezpečnostní události nebo reagování na bezpečnostní incidenty.

Nyní jsou již veškeré nezbytné procesy implementovány, nicméně v rámci ISMS principů opírajících se o již zmíněný PDCA cyklus, je pro zajištění kontinuálního zlepšování nutné systém **monitorovat a revalidovat** již implementovaný systém, aby byla zajištěna jeho aktuálnost. Monitorování a přezkoumání ISMS je klíčové hned z několika hledisek, tím nejvíce transparentním je včasná detekce zpracování, identifikace procentuálního zastoupení úspěšného zamezení bezpečnostních hrozeb a vzniku bezpečnostních incidentů nebo validace správné funkcionality. Přezkoumávání implementace a jejich stěžejních částí je klíčové pro definování nedostatků a možných vylepšení pro další „run.“ V kontextu monitoringu a validace je rovněž stěžejní provádění interních auditů ISMS v předem definovaných intervalech a výstupy těchto měření a zjištění důkladně zaznamenat pro budoucí využití.

Poslední fází dle PDCA cyklu je v kontextu ISMS jeho **udržování a zlepšování**. Tato fáze se týká především optimálního managementu změn na základě zjištěných nedostatků v předchozí fázi monitoringu. Rovněž je nutné provádět činnosti preventivní povahy a stále projednávat činnosti a návrhy na optimalizaci pro zvyšování až na stanovenou úroveň. Tato fáze obsahuje definování zodpovědnosti a garance naplnění stanovených požadavků a předpokládaných cílů.

Za předpokladu, že jsou dodrženy všechny stěžejní postupy v rámci procesu zavádění ISMS, je možné očekávat zlepšení v oblastech:

- zvýšení bezpečnostních aspektů organizace a garanci optimální výše ochrany od začátku procesu,
- porozumění problematice z hlediska restriktivní legislativy a jejího správného aplikování,
- užití strukturovaného holistického rámce pro adekvátní zhodnocení bezpečnostních rizik pro důležité organizační assety a jejich následné monitorování pro optimalizování efektivity.

(ISO/IEC 27001, 2013)

Pro dostatečné porozumění problematiky je nutné definovat také další standardy z rodiny 27 000. Tyto standardy jsou stěžejní pro správnou implementaci bezpečnostního řešení. Dodefinovány budou standardy, které se přímo týkají Zákona o kybernetické bezpečnosti, který je nedílnou součástí této práce.

Na rozdíl, od již zmíněného standardu ISO/IEC 27001 jsou však některé spíše doporučujícího charakteru.

2.2.3 ISO/IEC 27002 (Information technology and security techniques)

Tento mezinárodní standard je vytvořen pro organizace, které jej mohou použít jako dokument poskytující návod během implementace kontrolních procesů asociovaných s ISMS, zmíněném ve standardu ISO/IEC 27001. Standard je možné použít pro jakýkoliv druh organizace, ať už v ziskovém či neziskovém prostoru, pro různě veliké organizace. Standard se zabývá především výběrem adekvátních bezpečnostních kontrol, které budou stěžejní pro implementaci ISMS.

„ISO/IEC 27002 is a code of practice – a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information. Organizations that adopt ISO/IEC 27002 must assess their own information security risks, clarify their control objectives and apply suitable controls (or indeed other forms of risk treatment) using the standard for guidance.“

(ISO/IEC 27002, 2013)

Z citace týkající se definování standardu tak, jak je zapsána na oficiálních stránkách, je zřejmé jasné vymezení a rozdíl mezi standardy 27001 a 27002. Standard ISO/IEC 27002 je svou povahou často nazýván také jako guideline, neboť není tak striktní v procesu výběru vhodných nástrojů, jako je tomu u ISO/IEC 27001, a plní spíše podpůrnou funkci.

Norma se opírá o principy CIA triády, která byla definována již v kapitole věnující se informační bezpečnosti.

(ISO/IEC 27002, 2013)

2.2.4 ISO/IEC 27003 (Information security management systém and implementation guidance)

Standard ISO/IEC 27003 je, jako všechny standardy z 27k family, úzce spjatý s implementací ISMS a často se odkazuje na standardy ISO/IEC 27000 a ISO/IEC 27001. Jako v předchozím případě, i zde se standard snaží spíše navrhnout doporučení, možnosti a povolení, účelem dokumentu není poskytnutí celkového vedení jako v případě ISO/IEC 27001. Spíše, než na samotnou implementaci je tento standard navržen jako pomoc pro optimalizaci managementu a monitoringu probíhající již po úspěšné implementaci ISMS. Kromě již zmíněných je rovněž zaměřen na správné pojetí PDCA cyklu a s ním spjaté klíčové atributy jako jsou:

- plánování procesu zavedení ISMS
- management rizik v kontextu informační bezpečnosti, hledání optimalizací a jejich aplikace nebo definice potřebných požadavků pro naplnění podstaty standardu
- akceptování a autorizace navrhnutých zlepšení pro pokročení v zavádění ISMS

(ISO/IEC 27003, 2017)

2.2.5 ISO/IEC 27004 Measurement

Standard ISO/IEC 27004 je vytvořen se záměrem pomoci organizacím adekvátním způsobem zhodnotit stav informační bezpečnosti a posoudit efektivitu systému spravujícím informační bezpečnost v organizaci. Jeho účelem je nalezení optimálních **metrik**, díky kterým bude možné naplnit požadavky stanovené v ISO/IEC 27001. Obsahem standardu je mimo jiné:

- monitoring a měření výkonnostních aspektů bezpečnosti informací
- monitoring a měření efektivity ISMS včetně s ním asociovaných procesů a kontrol
- analýza a zhodnocení výsledků monitorování a měření

(ISO/IEC 27004, 2017)

Po zdárném definování potřebných standardů bude nyní definován Zákon o kybernetické bezpečnosti, který významně ovlivnil celý koncept vnímání informační bezpečnosti u nás.

2.3 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti (181/2014 Sb.) vešel v platnost na začátku roku 2015. Svou podstatou podporuje implementování principů informační bezpečnosti, ISO 27k, a tudíž i SIEM systému. Implementace by měla probíhat v souladu s řízením organizace a tak, aby nedocházelo ke střetu mezi legislativními požadavky a primárními cíli organizace. Povinné zavedení principů definovaných v zákoně jsou předepisovány pro kritickou informační infrastrukturu, ta je dle Wolters Kluwer definována jako *„prvek nebo systém prvků kritické infrastruktury v odvětví komunikačních a informačních systémů v oblasti kybernetické bezpečnosti.“* Povinnost vzniká každé organizaci spadající pod zákony č. 127/2005 Sb. (Zákon o elektronických komunikacích), č. 240/200 Sb. (Krizový zákon) a č. 317 (Odvětví veřejné správy).

(Krčmář, 2013; Wolters Kluwer ČR, 2014)

ZKB je regulačním legislativním nástrojem v oblasti bezpečnosti informačních technologií.

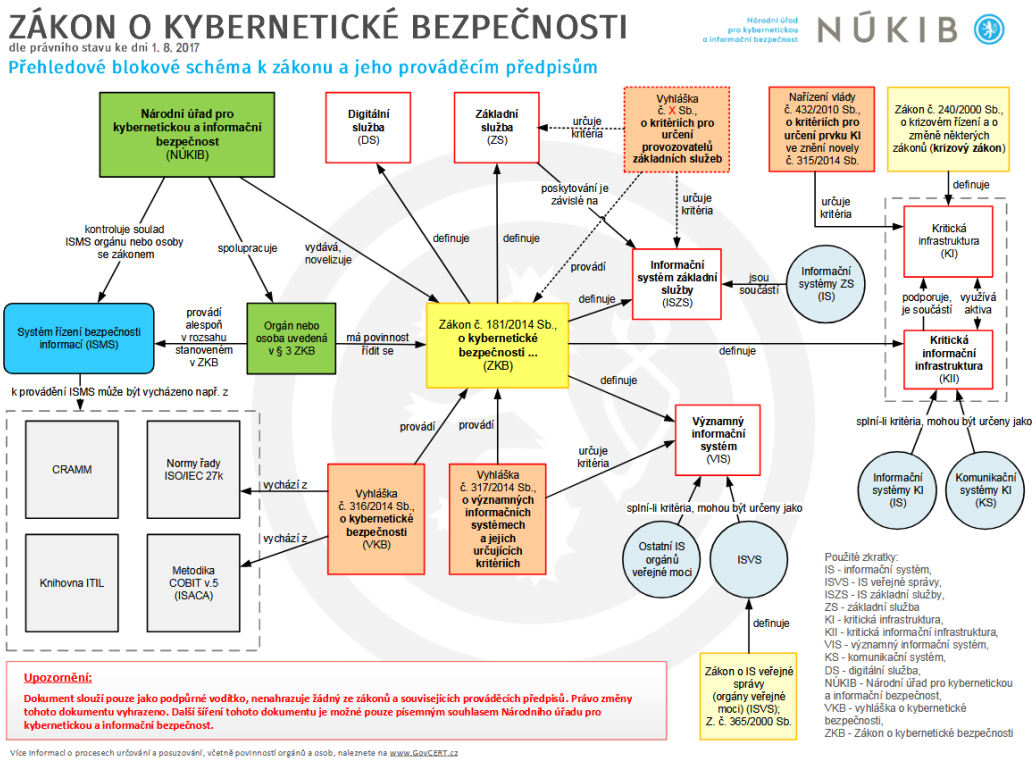
Zákon prošel v roce 2017 novelizací, která se týkala především:

- zavádění nových institutů,
- zavedení nových povinných orgánů a osob,
- nové úpravy povinností při uzavírání smluv mezi orgány veřejné moci a poskytovateli cloud computingu,
- novou informační povinnost pro povinné orgány a osoby,
- rozšíření povinností při bezpečnostních událostech a incidentech,
- rozšíření pravomocí národního a vládního CERT,
- zřízení nového ústředního orgánu – NÚKIB.

Jak je vidět z předchozího přehledu o změnách v zákoně, veškerými procesy týkající se kybernetické a informační bezpečnosti na území České republiky se zabývá tzv. **NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost)**. Tento úřad vznikl v roce 2017 na základě zákona č. 205/2017 Sb. v kontextu změn zákona č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti). Hlavními činnostmi tohoto správního orgánu pro kybernetickou bezpečnost jsou:

- příprava bezpečnostních standardů,
- zvyšování povědomí o oblasti kybernetické bezpečnosti,
- výzkum a s tím spojený vývoj v oblasti kybernetické bezpečnosti,
- ochrana informací citlivé povahy z oblasti informačních komunikačních systémů,
- ochrana kryptografická,
- provoz vládního CERT a spolupráce s ostatními CERT týmy.

(NÚKIB, 2018)



Obrázek 4 - Blokové schéma, převzato (NÚKIB, 2018)

V současné době probíhá jednání o nové vyhlášce o kybernetické bezpečnosti, ta byla naposledy projednávána 19.1.2018. Tato vyhláška zatím ještě nenabyla legislativní úpravou a je možné, že se bude ve své finální podobě trochu lišit, nicméně je už teď jasné, že změna se bude především týkat níže uvedených oblastí:

- obsah a strukturu bezpečnostní dokumentace,
- obsah bezpečnostních opatření, rozsah jejich zavedení,
- typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
- náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů a jeho formu a
- způsob likvidace dat, provozních údajů, informací a jejich kopií.

(NÚKIB, 2018)

V tomto kontextu je pro tuto práci klíčová problematika zaznamenána především v hlavě 2, § 11 - §14. Tyto paragrafy blíže specifikují řízení změn, řízení přístupu, vývoj s údržbou a zvládání kybernetických bezpečnostních událostí a incidentů. Všechny zmíněné oblasti lze vyřešit vhodnou implementací SIEM technologie. Jednotlivé paragrafy z hlavy 2 budou nyní blíže rozebrány.

Řízení změn

Paragraf předepisuje povinnost zavedení bezpečnostních opatření pro management změn u informačního a komunikačního systému. Je nutné zabezpečit manipulaci s informacemi o řízení systémů, analýzách rizik, up-to-date bezpečnostní politiku a dokumentaci, testování optimálního nastavení systémů, zálohování změn pro obnovu dat v případě problému. Paragraf dále specifikuje proces rozhodování pro penetrační testování zmíněných systémů a další postup v případě zjištění nedostatků.

Řízení přístupu

Řízení přístupu je specifikováno povinností pro zodpovědnou osobu nebo orgán přijmout opatření zajišťující omezení přístupu k citlivým údajům, zejména takových, která slouží pro účely autorizace a autentizace. Dále je předepisována povinnost řídit přístup na základě skupin a rolí, užití jedinečného identifikátoru pro přístup do systému (dohlížet na dodržování autentizačních postupů u zaměstnanců), omezení privilegií na nejvyšší možnou mez nezbytnou k provádění pracovních úkonů, zavedení bezpečnostních opatření pro všechny přístroje přistupujících do prostředí informačního nebo komunikačního systému a v neposledním případě přezkoumávání nastavení přístupové politiky v pevně daných časových intervalech. V případě zjištění porušení stanovených pravidel je nutné zakročit a učinit rázné kroky v podobě odebrání přístupových práv nebo rekonfiguraci bezpečnostní politiky. Veškeré provedené kroky, tj. přidělení a odebrání přístupových práv musí být v souladu se zákonem, zaznamenáno pro účely pozdější analýzy.

Akvizice, vývoj a údržba

Tento paragraf je svou podstatou seznamem povinných položek, které je potřeba dodržet v rámci kontinuálního zlepšování a údržby pro komunikační a informační systémy. Mimo jiné specifikuje povinnost řídit rizika dle postupů definovaných v zákoně, řízení změn a stanovení optimálních bezpečnostních požadavků, které jsou do procesu vývoje a údržby zahrnuty. V rámci vývoje je nutné zajistit bezpečnost také pro testovací data a testovat v bezpečném prostředí., a v případě kdy se jedná o testování jakékoliv významné změny, bude tato změna nejdřív otestována, než bude nasazena do provozu.

Zvládání kybernetických bezpečnostních událostí a incidentů

Paragraf předepisuje implementaci bezpečnostního zařízení dle požadavků stanovených v zákoně:

- zavedení systémů pro detekci a vyhodnocování kybernetických bezpečnostních událostí a incidentů,
- definuje odpovědnost a postupy pro průběžnou detekci a pro zvládání kybernetických incidentů,
- předepisuje postupy pro identifikaci, sběr, získání a uchování dat esenciálních pro kvalitní analýzu bezpečnostního incidentu,
- zajistí detekci bezpečnostních událostí a v případě výskytu předepisuje způsob manipulace dále v zákoně,
- přikazuje včasné nahlašování bezpečnostních událostí lidem, kteří přijdou s touto problematikou do styku,
- vytváří povinnost pro posuzování bezpečnostních událostí dle stanovených postupů a nutnost rozhodování o jejich transformaci na bezpečnostní incidenty,
- zajištění preventivních opatření pro odvrácení nebo zmírnění bezpečnostního incidentu,
- zaznamenává veškeré bezpečnostní incidenty,
- provedení diagnostiky daného kybernetického bezpečnostního incidentu a vyhodnotí účinnost jeho vyřešení, případně stanoví oblasti, které je nutné zlepšit pro zamezení opakování bezpečnostního incidentu.

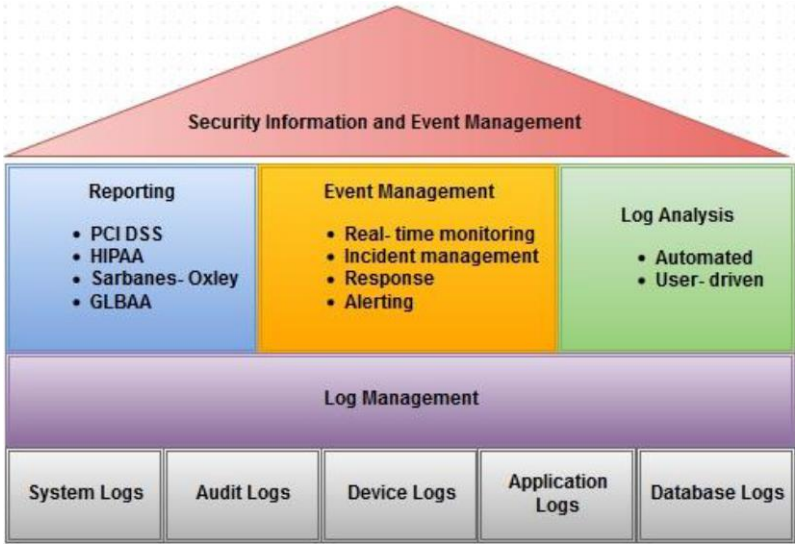
Zvládání bezpečnostních událostí a incidentů je svou povahou nejblíže k SIEM tématice. Ve výše zmíněných bodech definovaných tímto paragrafem lze jasně vidět principy, které jsou v SIEM systémech používány. Tyto principy budou nyní definovány, aby byla zřejmá nutnost použití této technologie.

3 Security Information and Event management

Po definování nezbytných náležitostí týkající se standardů spravujících informační bezpečnost a zákonu implementovaném pro správu kritické infrastruktury státu, budou nyní objasněny dílčí principy SIEM (Security Information and Event management).

Technologie SIEM byla již zmíněna v kontextu ISO standardů 27000, který se jeho optimalizací a funkcionalitou zabývá. SIEM je díky svým funkcím rovněž doporučen v rámci Zákona o kybernetické bezpečnosti. Jeho důležitost vzrůstá především z důvodu nutnosti ochrany informací nejen velkých organizací. Bezpečnostní management událostí a informací je řešením na vzrůstající počet heterogenních a stále komplexnějších prostředí a technologií. Pokud je vzat v potaz fakt, že tyto technologie budou monitorovány a bude proveden sběr informací jejich chování, výsledná data budou svou různorodostí, množstvím a povahou při nejmenším velmi obtížně použitelné pro další analýzu.

SIEM technologie se svým užitím řadí k poměrně novým technologiím, přesto jsou její principy známy již delší dobu, i když v diferenciované podobě. Před vznikem samotného SIEMu zde byly technologie SIM (Security Information Management) a SEM (Security event management). V obou případech se jednalo o management citlivých informací nebo událostí generovaných koncovými zařízeními. S tím, jak se technologie, infrastruktury a systémy stávaly složitějšími, bylo nutné zvýšit funkcionalitu a celkovou komplexnost technologie. Absence těchto vlastností byla vyřešena sloučením dvou technologií.



Obrázek 5 - Architektura SIEM, převzato a upraveno (Miller, 2011)

SIEM technologie využívá specifického postupu a principů při zpracovávání přijímaných dat. Tyto principy budou nyní definovány.

- Log management
- IT regulatory compliance
- Event correlation
- Active response
- Endpoint security

(Miller, 2011)

3.1 Log management

Management logovacích záznamů v SIEM systému je iniciován konfigurací datových uzlů v IT infrastruktuře/ systému. Čím lépe je mapování infrastruktury rozmístěno – jsou monitorovány kritické uzly, tím přesnější je obraz, který je získán z relevantních událostí aplikací (logů). Události jsou zasílány do centralizované databáze, která je spravována SIEM aplikací. SIEM aplikace databáze nejprve rozřadí pomocí parseru a znormalizuje je. Data zasílaná do databáze jsou, jak již bylo zmíněno, vysoce heterogenní a je jich obrovské množství. Koncová zařízení mohou být počítače běžící na různých operačních systémech – Linux, UNIX, Windows. Jiná zařízení mohou představovat switche, firewally, systémy na detekování vniknutí (IDS), systémy zajišťující vzdálený přístup, nebo proxy servery. Tyto rozličné systémy pocházejí od různých druhů výrobců, což se bohužel často promítá v syntaxi a stavbě logů. Řešení je závislé na konkrétním druhu koncového zařízení, ať už se jedná o užití syslogových klientů, které budou zasílat informace nebo je možné využít již předdefinované parsery, případně customizovaný syslog klient software, který je nabízen od SIEM výrobce.

Po úspěšných prvotních krocích jsou události uschovány pro další potřeby v budoucnu. SIEM je schopen události organizovat, ukládat, obnovovat a archivovat pro splnění auditních požadavků společnosti. Kromě již zmíněných funkcí, jsou data také používána pro potřeby analýzy. SIEM se pyšní takřka real-time analýzou událostí a data miningem zkoumajícím celkové zdraví a bezpečnostní status infrastruktury. Čím více koncových zařízení bude zasílat své události do SIEM systému, tím kompletnější a přesnější bude obraz vypovídající o stavu firemní síťové infrastruktury.

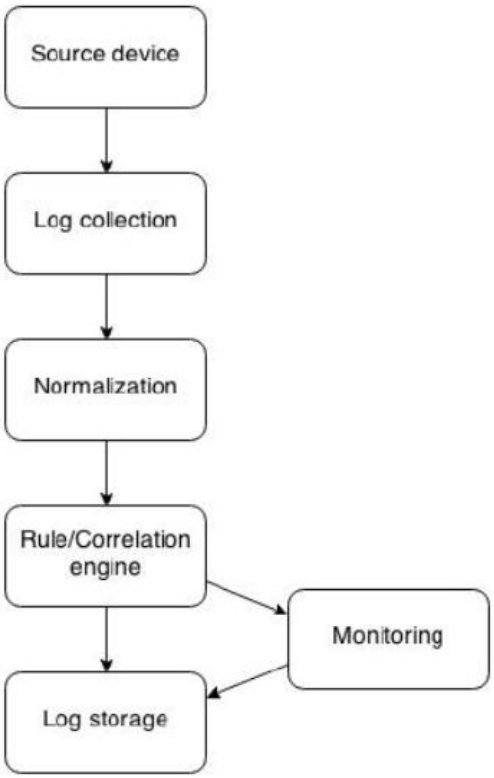
3.2 IT Regulatory Compliance

Poté, co jsou všechny důležitá koncová zařízení síťové infrastruktury napojena a zasílají své logovací záznamy, je nutné vytvořit set pravidel a filtrů. Pravidla jsou typu boolean a zastávají funkci kontroly. Kontrolují přicházející události, zda neobsahují informaci vymykající se normálu. Pokud je zjištěno porušení pravidel v oblasti identifikace OS, autentizace, aktualizace IDS systémů, nesrovnalosti s obvyklým časem nebo geografickou polohou uživatele, to vše může být podnětem k dalšímu prošetření. Spuštění pravidla je ve většině případů vytvořením offense (bezpečnostního incidentu). Vytvoření filtrů je možné vícero způsoby. V první řadě je možné si zakoupit výrobcem již předdefinovanou řadu filtrů, jedná se zejména o filtraci dle nejčastěji užívaných atributů, které logy obsahují tzn. uživatelské jméno, zdroj logovacích záznamů, zdrojová nebo cílová IP adresa, zdrojový nebo cílový port, použitý protokol, … V případě, že je nutné vytvořit filtry specifičtější povahy, odvíjí se povaha filtru zejména podle dané problematiky. V neposlední řadě obsahují SIEM systémy také system reporting, který je důležitý především v kontextu auditingu a validace úrovně řešení.

3.3 Event Correlation

Korelace událostí obdržených do systému SIEM je přidanou hodnotou, díky které je SIEM technologie tak žádaná a efektivní. Proces korelace událostí je do jisté míry procesem učení, díky kterému bude systém schopen rozpoznávat potencionální hrozby, přičemž je schopen vzít v potaz rozličnou škálu proměnných. Vzniklý problém ve firemní nebo kritické infrastruktuře může být způsoben x činiteli, a je mnohdy velmi obtížné zohlednit všechny faktory přispívající k této skutečnosti. Korelační engine SIEM je schopen prošetřit, zvážit a korelovat i události, které nemají na první pohled přímou souvislost s problémem, nicméně mohou říci a objasnit další skutečnosti o stavu zdraví síťové infrastruktury. Bude stanoveno několik hypotéz vysvětlující problém v infrastruktuře. Dalším krokem je již lidský faktor, který vybere nejlepší možnou variantu na základě dostupných informací a skutečností.

Po definování dílčích částí SIEM bude nyní blíže přiblížen celý proces zpracování dat a architektura SIEM.



Obrázek 6- Proces zpracování událostí v SIEM, převzato a upraveno (Miller, 2011)

3.4 Architektura SIEM

Jak je možné vidět na přiloženém schématu, SIEM užívá při procesu zpracování událostí vícero nástrojů. Všechny součásti celku musí bezchybně kooperovat, jinak dochází k chybám a pádu celého systému. Je nutné zmínit, že komplexnost řešení se liší velikostí a složitostí od implementace k implementaci. Některá zavedení mohou obsahovat i další součásti věnující se forenzním analýzám nebo korelacím, avšak níže zmíněné součásti musí být přítomny a správně nadefinovány v každé implementaci, jsou sice schopny pracovat samostatně, nicméně SIEM jako celek nebude fungovat dle očekávání.

- Source Device (zdrojová zařízení
- Log Collection (kolekce logovacích událostí)
- Parsing Normalization
- Rule engine
- Correlation engine
- Log storage
- Monitoring and event retrieval

3.4.1 Source device

Pod pojmem zdrojového zařízení si lze představit cokoliv, co zasílá informace o svých aktivitách do SIEM systému. Níže jsou zmíněny některá zdrojová zařízení, která bývají často součástí firemní infrastruktury:

- routery,
- switche,
- firewally,
- appliance,
- aplikace,
- operační systémy.

Napojení zdrojových zařízení je esenciální pro adekvátní výstup v SIEM systému, v případě absence nebude SIEM schopen analyzovat, co se děje v síťové infrastruktuře a nebude možné predikovat, reagovat a zabránit vzniku bezpečnostních událostí a bezpečnostního incidentu. Objem dat, který je generován ve firemní infrastruktuře, je obrovský. Takřka každé kliknutí myší v prostředí webového prohlížeče iniciuje transport datových packetů uvnitř i vně sítě. Veškerá tato komunikace musí být správně zachycena a zasílána do SIEM aplikace, která bude schopná generovat relevantní výstupy týkající se zdraví systému.

Na druhou stranu, pokud bude monitorována každá součást systému, může se nalezení problému rovnat hledání jehly v kupě sena. Z toho důvodu je nutné definovat důležitost jednotlivých zdrojů na základě důležitosti, kterou v infrastruktuře hrají a jak často zasílají své informace do SIEM aplikace. Výše zmíněné je kritické pro vytvoření optimálního prostředí pro real-time analýzu, kterou SIEM používá.

<13>Jun 12 15:51:51 10.146.184.171 AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.2.7.20 Source=Microsoft-Windows-Security-Auditing Computer=SRV01.dom01.poj OriginatingComputer=10.146.184.171 User= Domain= EventID=4624 EventIDCode=4624 EventType=8 EventCategory=0 RecordNumber=1207166006 TimeGenerated=1528811509 TimeWritten=1528811509 Level=Log Always Keywords=Audit Success Task=SE_ADT_LOGON_LOGON Opcode=Info Message=An account was successfully logged on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: DOM01\[redacted] Account Name: [redacted] Account Domain: DOM01 Logon ID: 0x646dc990 Logon GUID: {9F65BEA4-12DE-5C3D-3548-71DFE061A440} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: 10.146.193.63 Source Port: 54104 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about t

Obrázek 7 - Podoba raw logu generovaného zdrojovým zařízením, vlastní zpracování

3.4.2 Log collection

Kolekce událostí je krokem, kdy jsou data, týkající se povědomí o infrastruktuře, transportovány do SIEM aplikace pro vyhodnocení. Přenos se týká všech zařízení, která jsou na SIEM napojena, proto je stěžejním krokem definovat pouze ty, které jsou pro zjištění stavu infrastruktury stěžejní. V kontextu způsobu přenosu existuje několik možných variant v závislosti na druhu SIEM systému, nicméně těmi nejužívanějšími a nejzákladnějšími jsou metody *push* a *pull*. Každá z těchto metod má své výhody a nevýhody, ty budou nyní blíže definovány.

3.4.2.1 Push metoda

Metoda push je metodou, která se vyznačuje především snadným konfigurováním v SIEM systému. V zásadě stačí definovat koncový přijímač, na který se posléze odkazuje zdrojové zařízení, aby do něj mohlo zasílat logovací události. Dobrým příkladem je například užití syslogu pro zasílání informací. Je definována IP adresa a DNS syslog přijímače, který v tomto případě je napojen nebo je součástí SIEMu. SIEM jako takový není v procesu získávání logovacích událostí zapojen, koncové zařízení samo zasílá tyto data do systému nebo aplikace. Absence participace SIEM skýtá jistá nebezpečí – značnou nevýhodou push metody je, že pro transport dat je většinou užit UDP protokol, u které je možné, že ne všechny datové packety dorazí do cílové destinace. V případě nedostatečně definované autorizační politiky je možné, že v případě kybernetického útoku dojde k přepsání nebo nahrazení některých informací, za účelem zkreslit pohled na systémové zdraví. Tzv. man in the middle je technikou, která se pro falsifikaci datových packetů hojně používá. K prevenci před těmito útoky je nutné znát, jaká zdrojová zařízení jsou v infrastruktuře zastoupena a jaké generují záznamy.

3.4.2.2 Pull metoda

Metoda pull se od již zmíněné push liší především v tom, že samotný proces získávání logovacích záznamů je iniciován samotným SIEM systémem. SIEM zašle dotaz na koncové zařízení, ze kterého jsou posléze transferována data do systému. Nevýhodou této metody je možná ztráta schopnosti real-time analýzy. Záznamy lze z koncových zařízení vytahovat v intervalech, které se nastaví, avšak v případě příliš dlouhé prodlevy nebudou informace o infrastruktuře aktuální. Eliminaci by mohlo představit adekvátní nastavení spouštění pull mechanismu na každých pár vteřin.

Po definování metod kolekce budou nyní přiblíženy principy kolekce v rámci přednastavených politik a kolekce nestandardních typů logů.

Z důvodu existence obrovského množství koncových zařízení je několik způsobů, jak přimět SIEM, aby správně četl logovací záznamy z koncových zařízení. Tím nejjednodušším je existence již výrobcem předdefinovanými metodami pro většinu známých zařízení a software (Oracle, Linux, Windows …), bohužel, ne vždy existuje snadné řešení. V případě, že je pracováno s něčím, co ještě SIEM nezná, jsou dvě možnosti. Je možné užití sekundární aplikace, která transformuje výstup na něco, co je SIEM schopen přečíst – jako v případě užití syslogových aplikací, nebo je nutné vytvořit novou definici, podle které budou důležité informace od neznámého koncového zařízení přijímány. Druhá zmíněná metoda bude nyní blíže specifikována.

Vytvoření sběrové metody na míru konkrétní aplikaci nebo zařízení je procesem, který je mnohdy na delší dobu, než by se mohlo zdát. V první řadě je nutné

prozkoumat syntaxi, v jaké jsou logovací záznamy zasílány a také, zda si udrží jednotnou formu po celou dobu zasílání. Pokud je splněna homogenní podoba formátování, přichází na řadu vytvoření regulárních výrazů, které budou součástí parserové extenze. Extenze musí být nadefinována přesně na atributy, které je potřeba ze zdroje logů získat, čím více takovýchto atributů v záznamu je, tím horší je správně nadefinovat parser. Proces parsování logů je předmětem další části práce.

Jak lze vidět výše, jak metoda push, tak pull mají svá nesporná pozitiva při správném užití. V praxi se systém setkává s nespočtem různých koncových zařízení, z toho důvodu se pro sběr většinou používá kombinace vícero metod dohromady v závislosti na druhu koncového zařízení, frekvencí, s jakou je nutné z něj získávat nebo generovat informace a objemem dat, jaký bude do SIEM systému zasílat.

3.4.3 Normalization and parsing of logs

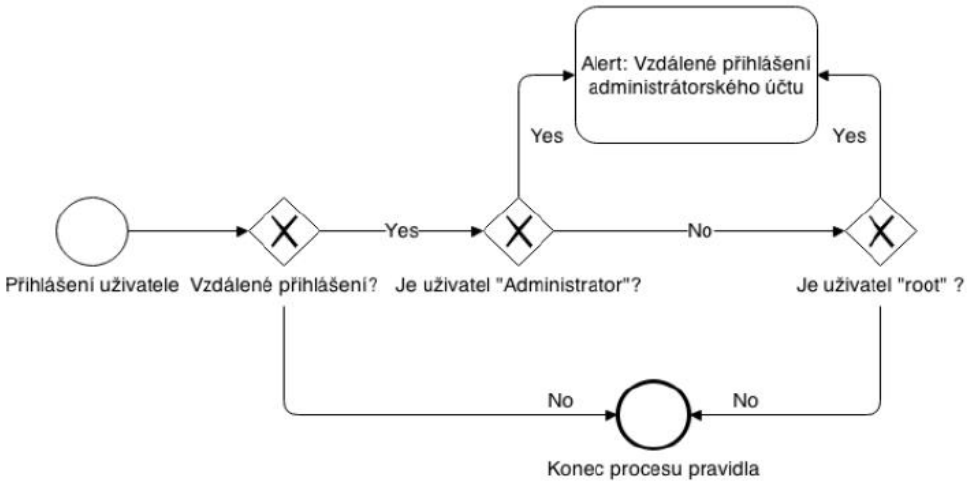
V tomto okamžiku už jsou koncová zařízení napojena na SIEM aplikaci, do které zasílají své logovací záznamy. Nicméně problém spočívá v syrovém naturálním stavu záznamů, které SIEM neumí přečíst. Z toho důvodu je užit proces, při kterém jsou všechny příchozí záznamy převedeny na jednotný formát, tento proces se nazývá normalizace. Během normalizování je mimo jiné možné použít již zmíněný parser, který ze záznamu dokáže vyfiltrovat pouze důležité atributy a informace, které jsou stěžejní pro zvýšení povědomí o síťové infrastruktuře.

3.4.4 Rule engine and correlation engine

Efektivita analýzy logů z koncových zařízení je do jisté míry závislá na každé ze stěžejních součástí SIEM. Tento engine pod sebou združuje funkcionalitu korelačních procesů – tyto procesy fungují na bázi pravidel. Korelační procesy jsou jedním z prvlů, který posouvá analýzu a predikci na další úroveň. **Korelační stroj** je totiž schopen vzít v potaz desítky atributů a vyvozovat díky tomu přesnější predikce během bezpečnostních událostí a incidentů. Informace pro korelační analýzu pocházejí z normalizovaných dat, kterými je SIEM plněn. Mimo zkoumání širšího kontextu problému je korelační stroj schopen také poměrně dobré redukce false positive, zejména díky srovnávání tolika atributů. Korelační stroj se opírá o definovaný **ruleset pravidel**, který rovněž usnadňuje manipulaci s příchozími záznamy. Pravidla jsou definována jakožto „what – if“ podmínky s datovým typem boolean. Konkrétní typ pravidel se liší v závislosti na prostředí, ve kterém je SIEM zprovozněn. Pravidla mohou být jednoduchá nebo komplexnější, dle potřeby a mohou do sebe vnořovat další pravidla s nimi asociované. V případě naplnění podmínky je možné v rámci SIEM aplikace nadefinovat rozdílné spektrum odezvy. Spuštění pravidla je důvodem pro otevření tzv. offense (bezpečnostního incidentu), které je pak nutné prošetřit

pomocí již zmíněného korelačního stroje a rovněž také konzultantem spravující prostředí SIEM.

Funkcionalita korelačního stroje a nastavení pravidel bude demonstrováno na přiloženém schématu představující postup při přihlašování přes účet s administrátorskými pravomocemi.



Obrázek 8- Grafické znázornění pravidla autentizace, převzato a upraveno (Vízner, 2011)

3.4.5 Log storage

Log storage je prvek SIEM, který je nezbytnou součástí architektury. Při množství, s jakým jsou generovány objemy dat je nutné, aby byla tato data někde skladována a mohla být použita pro pozdější využití. Úložiště však kromě přijatých logovacích záznamů ukládá také operace týkající se transakcí nebo systémové povahy. Uložené záznamy slouží pro účely interního auditu (dodržení politiky o povinné délce uchování dat) a analýz při výskytu bezpečnostní události či incidentu.

SIEM je schopen uchovávat příchozí záznamy třemi níže rozvedenými způsoby:

- Database
- Flat text file
- Binary file

Nejvíce využívaným způsobem pro ukládání dat v SIEM je jednoznačně **databáze**. Z pravidla jsou užívány klasické druhy databázových platforem jako je Microsoft SQL, Oracle nebo MySQL. Největší výhoda užití databáze tkví

v relativně jednoduché interakci a zpětného vytažení uložených dat z databáze pro účely analýz. Výkonnostní parametry jako je rychlost přístupu nebo vyhledávání v databázi se pak odvíjí od kvality hardwarových komponentů, které jsou v implementaci užity.

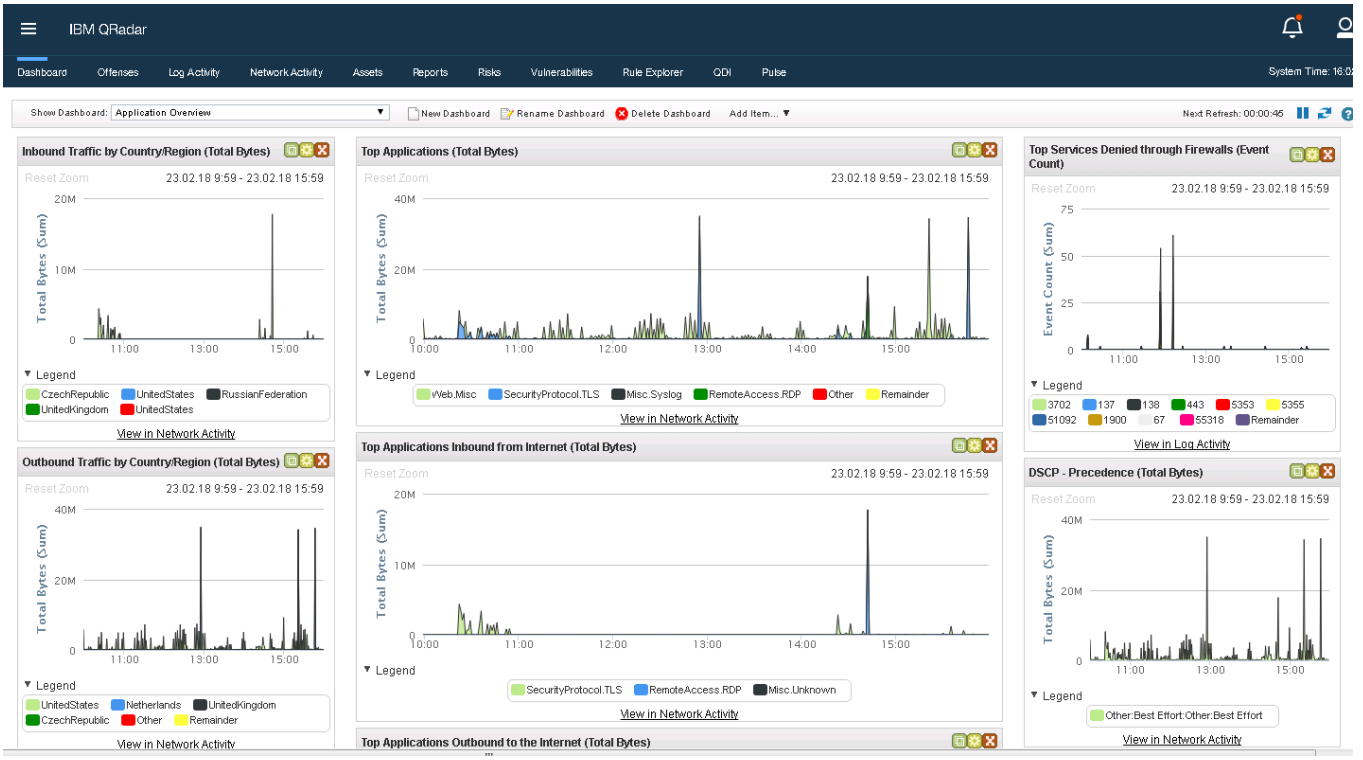
Druhý zmíněný způsob, **flat text file**, je v podstatě textový soubor, který je převeden do formátu, který je více „user-friendly.“Jednotlivé informace jsou odděleny nějakým druhem parseru, ať už se jedná o čárku, středník nebo tečku. Čitelnost patří k nesporným výhodám této metody, nicméně tato metoda má i své nevýhody. Za tu největší by se dala považovat nemožnost scalování pro větší infrastrukturu, rovněž je logické, že s přibývajícím množstvím dat se bude přímou úměrou zvyšovat reakční čas při čtení nebo zápisu dat do souboru a bezpečnost souborů je v porovnání s databází také výrazně nižší.

Posledním způsobem ukládání záznamů je do souborů užívající **binární formát**, který je na rozdíl od jiných druhů textových souborů pro uživatele nečitelný, díky čemuž má tato varianta lepší bezpečnostní aspekt. Kromě toho je užíván při přenosu (zpravidla protokol TCP) kontrolní součty, které díky zpětné kontrole již zmíněný bezpečnostní aspekt ještě umocňují.

3.4.6 Monitoring

Je finální částí v anatomii SIEM, přičemž se jedná o metodu interakce se záznamy, které jsou uložené v SIEM systému. V momentě, kdy jsou záznamy normalizovány a procesovány, je nutné udělat něco užitečné s informativními výstupy, které jsou z logů získány. Součástí SIEM technologie je také uživatelský interface, ve kterém je možné vizuálně interagovat se získanými daty. Díky sloučení informací ze všech připojených koncových zařízení je mnohem lehčí analyzovat data nebo vytvářet ruleset aplikovatelný na různé části infrastruktury dle potřeby.

(Miller, 2011, s. 86-92)



Obrázek 9 – Grafický interface QRadar, vlastní zpracování (2018)

Po detailním definování SIEM principů a funkcionality jeho architektury budou nyní zmíněny konkrétní SIEM aplikace, které budou součástí případových studií v praktické části práce. Pro účely práce byly vybrány níže zmíněné SIEM aplikace:

- IBM Security QRadar SIEM
- AlienVault OSSIM

Tyto aplikace byly vybrány na základě vyhovujících kritérií v oblasti škálovatelnosti, výkonu, a především z důvodu aplikace principů *user behavior analysis* (behaviorální analýzy), která jakožto modulární součást těchto SIEM aplikací bude stěžejním pilířem této práce. Jako další kritérium pro zvolení lze zmínit také vysoké skóre v Gartnerově magickém čtyřúhelníku pro problematiku SIEM. QRadar byl zvolen jako nejlepší volba již několik let za sebou a kvalitativní skóre AlienVaultu rovněž každým rokem stoupá. Posledním kritériem bylo vytvoření kontrastu mezi komerčním a open-source SIEM řešením a korelovat kvalitu jejích funkcionality.

4 IBM Security QRadar SIEM

IBM Security QRadar SIEM je komerčním SIEM řešením distribuované firmou IBM. Předchozím distributorem byla firma Q1 Labs. IBM integrovala QRadar do svého portfolia, což přineslo zvýšení funkcionality v rámci propojení s dalšími dílčími systémy, zvýšení škálovatelnosti řešení.

QRadar běží na operačním systému Red hat enterprise Linux 7 64 bit. Aktuálně se používá QRadar verze 7.3.1.

Samozřejmostí řešení je vysoká škálovatelnost implementace, ať už se jedná o nasazení fyzických či virtuálních appliance, rozličné škály dostupného hardware nebo rozdělení infrastruktury na více lokací.

Pro účel práce není zcela stěžejní definovat konkrétní implementace QRadaru nebo užité appliance, z toho důvodu bude pouze zmíněna architektura a výkonnostní aspekty mající vliv na optimální fungování modulu uživatelské analýzy, který bude součástí praktické části práce.

V případě zájmu o konkrétní implementace je možné nahlédnout do bakalářské práce, která je nepřímým předchůdcem této práce.

4.1 Architektura IBM Security QRadar SIEM

Pro větší přehlednost je architektura QRadaru rozdělena na nezbytné a volitelné logické prvky. Nezbytné logické prvky jsou nenahraditelné pro optimální funkčnost, kdežto volitelně nasaditelné prvky jsou schopny zvýšit funkcionalitu konkrétních součástí systému nebo zrychlit jejich procesování.

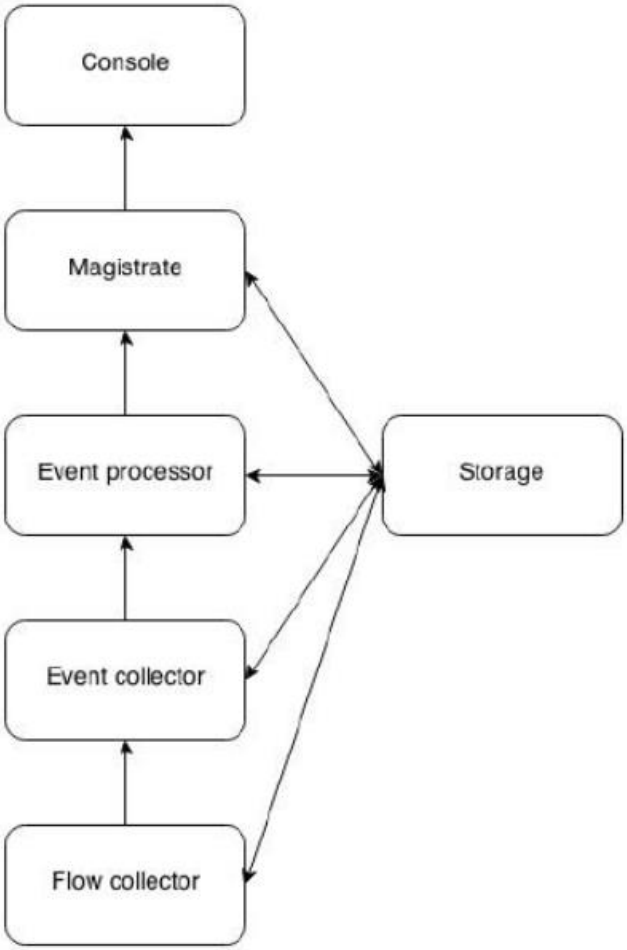
Nezbytné logické prvky

- Event collector,
- flow collector,
- event processor,
- flow processor,
- QRadar console,
- magistrate.

Volitelně využitelné logické prvky

- Risk manager,
- Incident forensis,
- Packet capture,
- Vulnerability manager,
- Anomaly detection,
- User behavioral analysis (machine learning add-on)
- Data Node

Následuje grafické znázornění logické struktury pro lepší porozumění procesu zpracování dat v prostředí IBM Security QRadar SIEM.



Obrázek 10 - QRadar architektura, převzato a upraveno (IBM corp., 2018)

Pod pojmem **flow collector** si lze představit komponentu sbírající datový tok z infrastruktury, datové packety, které jsou sbírány, představují komunikaci nebo kooperaci portů a IP adres komunikující pomocí konkrétního protokolu (TCP/UDP, SFTP, …). V závislosti na konkrétním druhu kolektoru je pak tato část schopna rozpoznávat identitu datových packetů až do 4. nebo i 7. ISO/OSI vrstvy. Tento proces je důležitý pro tvorbu QRadar assetů a zvyšování povědomí o původu komunikace v síti. Kolektory jsou rovněž schopny sbírat informace mimo infrastrukturu.

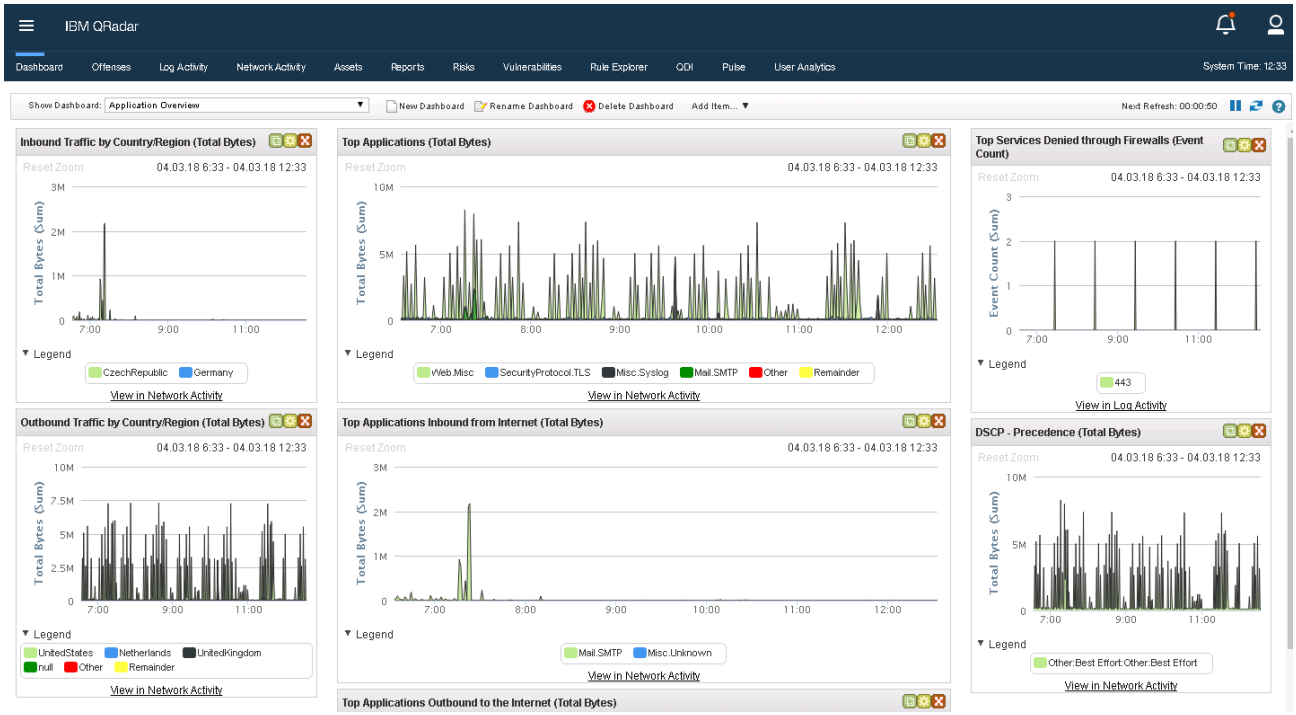
Event collector plní funkci kolekce logů ze zdrojových zařízení ať už lokálních nebo vzdálených. Obdržené události jsou pak podrobeny procesu normalizace, jak již bylo nastíněno v předchozí kapitole. V případě, že se jedná o známou událost, je k ní přiřazen QRadar Identifier (QID), tento způsob mapování a sdružování kontextově homogenních událostí je schopen významně šetřit výkon

a zmenší nutné procesování na optimální výši. Takto definované události jsou předány event processoru.

Hlavní úlohou **event processoru** je zpracování událostí, která jsou sbírána kolektory implementovaných do síťové infrastruktury podniku. Processor obdrží již normalizované události z koncových zařízení, které podrobí analýze dle definovaných rulesetů a podmínek. Poté je provedena korelace a interpretace získaného výstupu z analýz a informace předány dále do Magistrate. Kromě výše zmíněné funguje event processor také jako úložiště dat, čímž do jisté míry substituuje funkci volitelně využitelného prvku Data Node.

Magistrate je konzolovou službou QRadaru obsahující stěžejní procesy implementovaných komponentů. Kromě prezentování reportů, flow a event analýz nebo alternací pohledů je jejím hlavním úkolem procesování událostí přes vytvořená pravidla. V případě splnění podmínky definované v pravidlech, magistrate generuje adekvátní reakci. Reakci je možné nastavit při vytváření konkrétních pravidel. Nejčastější odezvu představuje vznik bezpečnostního incidentu (offense). Tento incident je posléze nutné prošetřit.

Komponenta **QRadar console** představuje uživatelské rozhraní pro všechny implementované komponentu QRadaru v infrastruktuře. Níže je vidět, že kromě grafického znázornění datového toku nebo přijatých událostí je v dalších záložkách možné spravovat více specializované procesy jako je Risk či Vulnerability manager nebo User analytics.



Obrázek 11- QRadar console, vlastní zpracování (2018)

(IBM Security QRadar SIEM, 2018)

5 AlienVault OSSIM

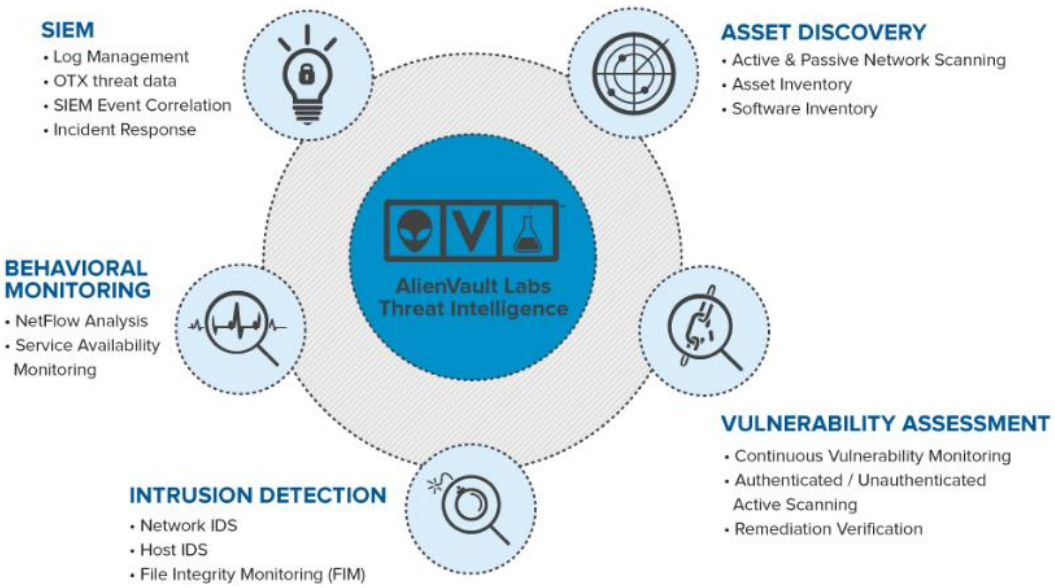
AlienVault OSSIM je open-source SIEM systém od firmy AlienVault. Kromě své open-source verze nabízí rovněž placenou verzi Unified Security Management (USM), která má oproti OSSIM navíc některé pokročilé funkce detekce hrozeb, odpovědi na incidenty nebo managementu logů v rámci jednoho sdruženého systému.

AlienVault disponuje také vlastním volně stažitelným softwarem na sdružování informací a dat o bezpečnostních hrozbách, zvaným Open Threat Exchange (OTX). OTX je schopné procesovat přirozený jazyk a také uplatňuje principy machine learningu.

Pro účely práce bude užita dokumentace pro USM, a to především z důvodu většího počtu informací a konkrétních dat než u open source verze OSSIM. Je předpokládána shoda v užitých komponentech i architektuře.

AlienVault ve svém incident response využívá princip tzv. kill chain, který umožňuje rychlou identifikaci vážnosti hrozby, jejího cíle a zvolení vhodné strategie pro specifikaci.

Nyní bude prezentována logická struktura USM se všemi nezbytnými prvky.



Obrázek 12- USM appliance, převzato a upraveno (AlienVault, 2018)

Dle přiloženého schématu bude definována kompletní funkcionalita AlienVault USM. Funkční appliance USM mimo jiné obsahuje:

- SIEM,
- Asset Discovery,
- Vulnerability assessment,
- Intrusion detection,
- Behavioral monitoring.

SIEM kombinuje sběr a korelaci logů ze zdrojových zařízení za účelem nalezení potenciálně nebezpečné situace v síťové infrastruktuře podniku. Tato součást bude více přiblížena později.

Asset Discovery užívá pasivních nástrojů, jako je např. pasivní service discovery nebo pasivní fingerprinting operačního systému. Objevování assetů je stěžejní součástí bezpečnostních principů řešení, neboť je užíváno pro zvýšení povědomí o doplňujících informací, které mohou být v případě incidentu velmi užitečné.

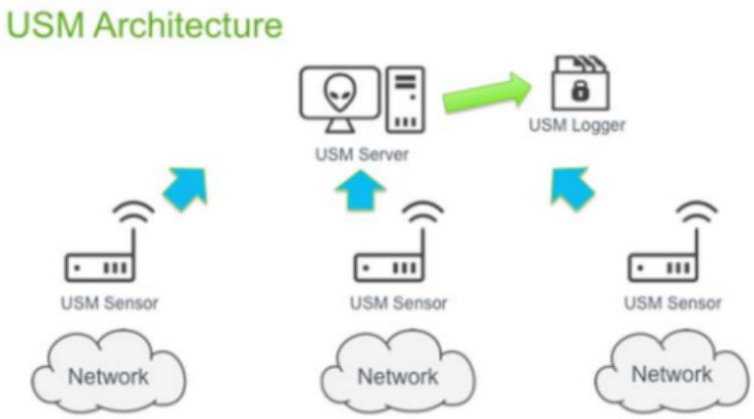
Vulnerability assessment je součást USM, zajišťující identifikaci zranitelnosti pomocí procesu komparace nainstalovaného software na zařízeních a známých zranitelností. Skenování lze provádět s i bez administrátorských privilegií, nicméně s plným administrátorským přístupem je šance na zjištění vulnerabilit vyšší.

Intrusion detection monitoruje síťovou komunikace z důvodu možného výskytu škodlivé aktivity, provádí také monitoring logovacích záznamů a v neposlední řadě i uživatelskou aktivitu v síti. V appliance USM je IDS rozděleno na detekci aktivit asociovaných s hostem (HIDS) a detekci aktivit asociovaných se síťovými komponentami (NIDS). HIDS je používáno pro detekci problémů na koncových zařízení (monitorování datové integrity, rootkit a kontrola registru). NIDS je zaměřeno na analýzu síťového toku a potenciální škodlivou aktivitu.

Behavioral monitoring se specializuje na vizualizaci provozních vzorů a datových toků, které jsou užity pro detekci anomálií a mohou poukazovat na porušení bezpečnostních politik. Data pro analýzu a behaviorální monitoring jsou získány ze síťových zařízení, datového toku a assetů.

Architektura USM v kontextu SIEM a její způsob zpracování událostí je do určité míry podobný tomu, jakým způsobem je zpracovává QRadar, nicméně lze z níže přiloženého schématu vidět podstatné zjednodušení a snížení počtu komponent v appliance. USM architektura obsahuje tyto komponenty:

- Appliance sensor,
- Appliance server,
- Apliance logger.



Obrázek 13- AlienVault architektura, převzato a upraveno (AlienVault, 2018)

Appliance sensor – komponenta primárně se zabývající kolekcí událostí ze zdrojových zařízení. Je možné ji nasadit přímo do infrastruktury nebo na periferie pro kontrolu příchozí a odchozí komunikace. Přijaté události normalizuje a zasílá je do appliance serveru.

Appliance Server – hlavní funkcionalita appliance serveru spočívá v agregování a korelaci informací z normalizovaných událostí zaslaných appliance sensorem. V tomto okamžiku je již možné vidět přijaté události v uživatelském rozhraní USM. Je možné provádět analýzu, management logů, reporting, vytváření politik a korelačních pravidel nebo prošetření potenciálních bezpečnostních incidentů.

Appliance logger představuje databázi, do které je možné bezpečně uchovávat příchozí události., např. pro forenzní analýzu nebo z důvodu auditních požadavků společnosti.

(AlienVault, 2018)

6 Porovnání QRadar a AlienVault

Pro komparaci výše definovaných SIEM aplikací je vytvořeno kvantifikační srovnání, které blíže specifikuje klíčové vlastnosti a požadovanou funkcionalitu. Pro účely samotné práce jsou v kontextu implementace SIEM a UBA stěžejní níže zmíněné atributy:

- Application monitoring,
- Analytics,
- Deployment/ Support Simplicity,
- Data and User Monitoring,
- Real-time monitoring,
- Threat inteligence,
- Behavior profiling,
- Log management and reporting,
- Licensing

Nutno zmínit, že pro účely porovnávání jsou z části užity stěžejní atributy tak, jak jsou definovány v rámci Gartnerova *Critical capability* pro SIEM. *(Kavanagh a Rochfold, 2015)*

Nyní budou obě SIEM aplikace porovnány podle výše zmíněného seznamu, a kromě toho také uvedeny základní informace týkající se konkrétního SIEM řešení.

6.1.1 QRadar

Platforma IBM Security QRadaru obsahuje mimo SIEM aplikace také log manager, manager zranitelností, manager rizik, kolektory pro Vflow a Qflow, a Forenzi incidentů. Může být deployován jako fyzická nebo virtuální appliance, případně SaaS nebo IaaS. Komponenty QRadaru je možné napojit hromadně v rámci all-in-one řešení nebo škálovat pomocí užití samostatných appliance pro rozdílnou funkcionalitu.

Tabulka 1 - System requirements QRadar, vlastní zpracování

	QRadar All-in-one a QRadar Log Manager Appliances	
min. RAM(GB)	32 - 128 dle EPS a FPM	
Úložiště - QRadar(GB)	256 u nižší verze; nutno počítat s trojnásobným navýšením pro optimalizaci výkonu	
Úložiště - dle počtu užívaných IP adres / zdrojových konfigurací (GB)	50000 IP adres	300000 IP adres/ 10000 konfiguračních zdrojů
	500	1000
Počet jader a odpovídající výkon	All-in-one virtual 3199 lowest perf.	All-in-one virtual 3199 highest perf.
	4	56
	500 EPS, 25000 FPM	30000 EPS, 1200000 FPM
Virtuální prostředí	VMWare ESXi 5.0 a pozdější; Hyper-V v3.0 a pozdější; Windows server 2008 SP2 a pozdější	

Real-time monitoring

Technologie QRadaru je schopna takřka realtime analýzy dat na bázi integrovaného pohledu dané infrastrukturu za použití sběru logů událostí ze zdrojových zařízení. V kombinaci s NetFlow, zachytáváním packetů, sběrem datových aktiv – assetů (pokročilé informace o původu dat) je schopen rozpoznání bezpečnostního incidentu včas.

Threat intelligence, je službou automatické aktualizace databáze služeb, které zaznamenávají nejnovější bezpečnostní hrozby (botnet, darknet, anonymní proxy, nejčastěji napadané porty, …) Jako bonus IBM poskytuje integraci s tzv.“X-Force IP Reputation,“ což zajišťuje zvýšení povědomí o konkrétní hrozbě v reálném čase.

Behavior profiling

Principy behaviorální uživatelské analýzy je možné aplikovat na všechna podporovaná zdrojová zařízení, tj. události a datový tok. Je možné jej použít v reálném čase nebo i v rámci historických dat. Princip UBA je založen na korelaci předem definovaných pravidel. QRadar rovněž určuje základní chování pro assety, uživatele, aplikace a u v případě zaznamenané odchylky spouští varovnou sekvenci.

Data and User monitoring je předdefinovaným, na uživatele orientovaným reportingem aktivit a náhledů v rámci konzole, aby bylo možné kontrolovat uživatelskou autentizaci v reálném čase. Nadstavbou nad klasickou integraci s AD nebo ostatními síťovými autentizačními zařízení, je QRadar schopen integrovat také IAM technologie, CA technologie a další. Data monitoring je přímo monitorován přes databázové logy a interagován s databázemi třetích stran jako je Imperva, McAfee nebo IBM InfoSphere.

Application monitoring

Monitorování aplikací je zprostředkováno přes různé druhy aplikací, ať už týkající se firewallu pro webové aplikace, technologií pro webové servery, podpory pro SaaS aplikace, SAP auditní logy nebo monitoring chování sítě pomocí užití QFlow sensorů.

Analytics

Analytické nástroje jsou přímo podporovány z QRadaru, přičemž se porovnávají real-time příchozí události a datové toky proti již uloženým historickým datům. Pro samotnou analýzy je možné využití dvou způsobů, prvním je InfoSphere a BigInsights, což je komerční IBM řešení Hadoop, a druhé jsou technologie pro analýzu a vizualizaci dat InfoSphere Bigsheets a i2 Intelligence analysis.

Log management a reporting

Management logů a reporting je dostupný v rámci funkcionality SIEM appliance, jako specializovaná funkce v deploymentu nebo jako samostatná schopnost přes QRadar Log Manager appliance. QRadar má v rámci svého licencování velké množství předdefinovaných reportů, které pokrývají většinu požadavků. Tyto reporty mohou být obohaceny o informace z Risk manageru nebo reportu zranitelností z Vulnerability manageru.

Deployment/ Support Simplicity

V rámci dostupných zpětných vazeb od zákazníků, se dá říci, že daná technologie je relativně snadno implementovatelná a dostupná v široké škále nasazení.

Licensing

Každý nasazený QRadar je v určitém slova smyslu plnou verzí, jednotlivá funkcionalita a rovněž výkonnost řešení se zpřístupňuje v rámci jednotlivých licencí, u kterých je stěžejním výkonnostním atributem především **EPS** (Events per second) a **FPM** (Flows per minute). Jedná se dvě jednotky, které determinují potřebný výkon pro danou infrastrukturu.

6.1.2 AlienVault

Bezpečnostní software AlienVaultu a jeho appliance nabízejí kromě SIEMu také posouzení zranitelností, NetFlow, detekci vniknutí do sítě či hosta, monitoring datové integrity. Komerční verze AlienVaultu – USM pak posouvá funkcionalitu opensource verze OSSIM dále. Obsahuje pokročilé principy škálovatelnosti, správy logů, konsolidovaných administrací, reportingu a jiné. USM je možné nasadit jakožto fyzickou či virtuální appliance a stejně tak i pro Amazon EC2 (Amazon Elastic Compute Cloud).

Tabulka 2 - System requirements – AlienVault, převzato a upraveno (AlienVault 2018)

	USM Appliance All-in-One		Remote sensor		USM Appliance Standartní		
	1TB	500GB	1TB	250GB	Server	Logger	Sensor
Počet jader	8		4		8		
RAM (GB)	16		8		24		
Úložiště (TB)	1	0,5	1	0,25	1,2	1,8	1,2
Virtuální prostředí	VMWare ESXi 4.x, 5.x, 6.x; Hyper-V v3.0+ (Windows Server 2008 SP2 a pozdější						

Real-time monitoring

AlienVault korelační stroj je schopen real-time monitoringu a korelace, přičemž užívá předdefinovaných korelačních pravidel, která jsou primárně stanovena pro senzorická data IDS.

Threat Intelligence

AlienVault nabízí obsah Threat intelligence v rámci své komerční verze, která je založená na několika open-source a komerčních hrozbách a také na obsahu

generovaném tzv. AlienVault Labs, který dodává aktualizace podpisů, zranitelností, korelačních pravidel nebo dat nezbytných pro řešení odezvy na incident (*incident response*). Kromě toho také zaštiťuje služby sdílející informace o reputaci IP adres a URL.

Behavior Profiling

Statistická analýza je aplikovaná na základě asi 50 parametrů a je založena na Holt-Wintersově exponenciálním vyhlazovacím algoritmu, který je schopen detekovat odchylky od výchozích hodnoty a outliery. Tato schopnost doplňuje proces korelace pomocí pravidel.

Data and User Monitoring

Speciální komponenta AlienVaultu, tzv. identity manager, umožňuje integraci monitoringu s identitním obsahem. Je možné monitorovat Active direktory a rovněž Lightweight Directory Access Protocol (LDAP). Lokální změny týkající se uživatelů je možné sledovat pomocí agenta IDS na hostu. AlienVault neumožňuje integraci s DLP (data loss prevention) nebo FIM(Forefront Indentity manager) produkty třetích stran. Co se týče dat, AlienVault užívá open-source Nagios pro primární monitoring DBMS (database management systém) a s nimi asociovanými službami.

Application Monitoring

Monitoring aplikací probíhá v integraci s webovou aplikací firewallu a technologie webových serverů, a kromě toho primárně pomocí open-source aplikací. Systémy jako je ERP, governance nebo GRC nemají dostatečnou podporu.

Analytics

Strukturovaná analýza a vyhledávání jsou prováděny přes investigační panel v primární konzoli a přes panel obsahující surové události. Surové příchozí události jsou korelovány s těmi, které jsou uloženy v datovém úložišti.

Log Management and Reporting

Schopnosti správy logů jsou zprostředkovány jakožto funkce v rámci logovací komponenty. Reporting je zprostředkován v rámci grafického interface.

Deployment/ Support Simplicity

AlienVault obsahuje instalační wizardy a dashboardy jakožto podporu pro prvotní nasazení, konfiguraci a správu senzorů a kontrolerů. Rovněž obsahuje aktualizace pro signatury senzorů, korelační pravidla, reporty a šablony pro incident response. Chybí zde integrace s externími adresáři pro workflow.

Licensing

AlienVault je dostupný ve dvou verzích. První open-source verze je zdarma, obsahuje však pouze základní SIEM a IDS funkcionalitu a není škálovatelná.

Komerční verzi USM lze škálovat a jak již bylo zvýšeno výše, obsahuje rozpracovanější verzi funkcionality OSSIM (log management, user behavior analysis, přístup do databáze aktualizace zranitelností, …).

(Kavanagh a Rochfold, 2015, s. 3-16)

6.1.3 Komparace funkcionality QRadar a AlienVault

U AlienVaultu lze konstatovat významné rozdíly v architektuře i přístupu k jednotlivým modulům v porovnání s architekturou QRadaru. Zatímco QRadar má všechny moduly přístupné v rámci svého webového rozhraní, v případě AlienVaultu USM se jedná o součásti, které jsou schopny do jisté míry pracovat i nezávisle na funkcionalitě ostatních.

Platforma AlienVaultu USM je vhodná pro organizaci, která potřebuje široký rámec integrovaných bezpečnostních funkcí za relativně nízkou cenu, v porovnání s ostatními komerčními řešeními, a primárně pro organizace, kterým nevadí platit za komercializované verze produktů založených na open source. Základní funkcionalita SIEM je zde zpracována relativně dobře, nicméně mnohdy chybí možnost užití aplikací a software třetích stran nebo např. analýza v rámci historické korelace či pokročilé principy uživatelské behaviorální analýzy.

Hlavní výhodou QRadaru je především jeho škálovatelnost a široké variace možných nasazení případů užití pro menší, ale i velké firmy. K tomu všemu QRadar podporuje bezpečnostně orientované modely, které profitují z analýzy síťové infrastruktury, detekce hrozeb a uživatelské i aplikační behaviorální analýzy. QRadar sice nemá žádnou bezplatnou verzi, to, co je však schopen nabídnout při zakoupení licence dalece převyšuje základní funkcionalitu AlienVaultu USM, např. moduly věnující se forenznímu vyšetřování, techniky pro zjištění packet rupture, historická korelace nebo principy machine learningu (IBM Watson).

Největším zklamáním v případě AlienVaultu je však neefektivita ukládání logů, resp. absence databázového systému, který by nebyl zbytečně složitý. AlienVault pro své logování používá ne zcela jednoduchého databázového systému (Nagios), což sice občas vede k rychlejšímu vyhledávání či jiným selektivním operacím, nicméně má neblahý vliv na nároky úložiště. Již nyní je nutné pro takřka každou implementaci nasazovat nejvyšší možné appliance, aby byl AlienVault schopen plynulého chodu. Z jejich dokumentace vyplývá, že jsou schopni pokrýt pro auditivní požadavky až 200 000 000 logů, což je bohužel, u některých větších nasazení počet logů, který je uložen za den. Z legislativního rámce České republiky, dle starší verze vyhlášky o kybernetické bezpečnosti je nutné auditovat alespoň 6 měsíců pro všechny organizace spadající do tzv. kritické infrastruktury. NÚKIB však nyní podle aktualizované vyhlášky předepisuje pro osoby uvedené v § 3 písm. c), d) a f) prodloužení auditu na 18 měsíců, pro

osoby uvedené v § 3 písm. e) zákona uchovává záznamy událostí zaznamenaných podle odstavce 2 nejméně po dobu 12 měsíců. *(NÚKIB, 2018)* Vzhledem k tomu, že dříve byly implementace nasazovány pro audit po třech měsících, byly i tak výkonnostní parametry zanedbatelné. Pro nároky tříměsíčního auditu by musel deployment generovat 26EPS, což je cifra, kterou nelze vidět ani u velmi malých nasazení. V momentě, kdy je nutností alespoň půl roku už není AlienVault schopen efektivně pokrýt auditivní nároky na něj kladené, aniž by došlo k velkému navyšování kapacity úložišť. Někdo by mohl namítat, že by možným řešením mohlo být monitorování pouze těch nejdůležitějších logů, což by však zapříčinilo ztrátu komplexnosti a preciznosti analýzy a zároveň by to bylo v rozporu s legislativou pro auditní logování.
Naproti tomu QRadar pro své primární logování užívá jednoduché Ariel databáze, ačkoliv IBM ve svém portfoliu disponuje jedním z nejlepších databázových systému IBM DB2. Zjevně jsou si vědomi, jakým tempem by narůstaly nároky na logování a celou appliance, pokud by se pokusili integrovat tento funkcionalitou mnohem komplexnější a robustnější databázový systém.

Po definování software, který bude užit pro účely praktické části práce je ještě nutné definovat principy behaviorální analýzy, se kterým bude primárně pracováno. Oba SIEM systémy jsou schopny do svých appliance integrovat principy machine learningu, který do budoucna představuje vysoký potenciál, z toho důvodu zde bude rovněž blíže rozebrán.

7 Uživatelská behaviorální analýza

Než budou definovány principy UBA, která je užita v praktické části práce, je nejprve nutné pokrýt obecné teoretické principy a východiska této metody.

Behaviorální analýza je disciplínou zabývající se experimentálním zkoumáním chování testovaných subjektů. Jedná se o vědeckou metodu založenou na principech **behaviorismu**. Tento přístup vychází z předpokladu možnosti zkoumání chování, aniž by bylo nutné znát vnitřní duševní stav testovaného organismu. Hlavním zkoumaným procesem je proces adaptace na prostředí nebo podnět.

Jak bylo zmíněno Americkou psychologickou asociací, je možná aplikace principů dle tří částí:

- experimentální investigace chování,
- pomocí aplikované behaviorální analýzy,
- konceptuální analýza chování.

(Cherry, 2018)

Pro kontext práce není tolik přínosná experimentální analýza, z toho důvodu budou definovány především metody aplikované behaviorální analýzy.

Aplikovaná behaviorální analýza se soustředí na aplikaci technik založených na principech učení a má za úkol změnit chování cílového subjektu. V dřívější době byla tato metoda rovněž nazývána „behaviorální modifikací," nicméně tento přístup neobsahoval vysvětlení relevantních interakcí mezi prostředím a chováním. Naproti tomu ABA se snaží o změnu iniciací a vytvořením funkčního vztahu mezi cílovým chováním a prostředím. Kromě toho se ABA principy snaží vyhledávat a vyvíjet sociálně akceptovatelné alternativy pro hraniční chování.

I když se ABA používá v rozličné škále problémů jako je intervenování chování u dětí s autismem, změna chování násilného chování nebo prevence HIV, stěžejním pro tuto práci je uživatelská behaviorální analýza a její konkrétní druhy užití.

Uživatelská behaviorální analýza je pojmem, který pod sebe sdružuje sledování, sběr a přiřazování uživatelských dat a aktivit v rámci jejich komunikace v prostředí sítě. Ačkoliv byla UBA vyvinuta primárně pro užití v marketingu pro predikci nákupního chování zákazníků, nyní je hojně užívána především v prostředí kybernetické bezpečnosti. Svou povahou se jedná o proces detekce hrozeb u uživatelů uvnitř infrastruktury. UBA hledá vzorce chování, na které jsou posléze aplikovány statistické analýzy a algoritmy, aby bylo možné detekovat chování, které se proti tomu standardnímu chování vymyká.

V dnešní době je hlavní problém ve skutečnosti, v jakých objemech data přichází do systému. V případě, že jsou generována terabyty dat denně, je velmi těžké indentifikovat relevatní data pro detekci podezřelé aktivity. Přesně z toho důvodu

jsou principy behaviorální analýzy tak efektivní, neboť se soustředí především na uživatelskou interakci, nikoliv na to, aby podezřelou událost v záplavě příchozího datového toku.

Jak zmiňuje E. Siegel, společnosti jako je Netflix, Facebook nebo Paypal jsou schopny predikovat na základě předešlých interakcí, co by uživatel viděl rád přiště nebo jaké zboží má největší šanci na koupi vzhledem k jeho nákupní historii. *(What is UBA used for, 2018 & Siegel, 2013)*

Na základě těchto principů vytvořil Gartner kategorii nazvanou **user and entity behavior analytics** (UEBA). UEBA se zaměřuje především na prevenci před krádeží nebo rozpadem sítě v případě, kdy dojde k prolomení uživatelovy autentizace a pod jeho jménem v síti operuje mallware či hacker.

Pro účely odhalení těchto případů užívá UEBA tří hlavních komponentů:

- **Data analytics**
  - UEBA aplikace identifikuje uživatelské a entitní chování, pro vytvoření zdrojových skupin a profilů. Po založení základního chování a jeho parametrů, používá statistických modelů a pravidel za účelem komparace příchozích transakcí u existujících modelů.
- **Data integration**
  - Flexibilní UEBA aplikace jsou schopny integrovat informace na strukturální i nestrukturální úrovni do již existujícího systému monitorujícího bezpečnost. Informace mimo jiné obsahují také logy ze SIEM systémů, data z datového toku a zachycených datových packetů.
- **Data presentation and Visualization**
  - Aplikace prezentuje výsledky efektivním způsobem tak, aby bylo jednoduché ve výstupech analýzy číst a snadno rozpoznat vzorce chování, které jsou spojeny s neautorizovanou činností.

(Gartner.com 2015; Searchsecurity.techtarget.com 2015)

Občas je možné vidět záměnu pojmů síťové analýzy a uživatelské behaviorální analýzy. Z toho důvodu bude definována rovněž síťová uživatelská analýza a demonstrovány rozdíly v užití.

Síťová behaviorální analýza (Network Behavior analysis) je soubor technik a procedur, které jsou primárně užívány pro zjištění nestandartní a potenciálně nebezpečné situace v rámci sítě organizace. NBA techniky jsou účinně využívány v bojí proti tzv. APT (Advanced Persistent Threat), ty se na rozdíl od těch běžných liší definováním konkrétního cíle pro útok. Cílem bývá konkrétní osoba nebo firma a útočník je ochoten strávit nemalý čas hledáním informací a dat, které by mu pomohly proniknout do infrastruktury, kam by se pokusil implementovat exploit. Jedním z nejznámějších příkladů útoků je tzv. „zero-day attack." Jak již bylo zmíněno, především v boji proti tomuto druhu hrozeb je užíváno principů síťové behaviorální analýzy. Pro zamezení je nutné užití aplikace s inspekcí packetů a analýzy chování v rámci síťové infrastruktury. Laicky řečeno jsou pomocí Netflow protokolu shromažďovány statistiky a informace o komunikaci vevnitř a na perimetru sítě, přičemž se hledá komunikace, která se svou podstatou vymyká standartním.

Primárním účelem NBA je analýza síťového prostředí firmy a snaha vyhledat potenciálně nebezpečnou komunikaci v rámci sítě, poukazující na malware. Naproti tomu UBA je primárně zacílena na uživatele a jejich podezřelé chování, které by mohlo indikovat pokus o zneužití informací nebo zneužití účtu zaměstnance útočníkem, který byl schopen získat jeho přístupové údaje. *(Čermák, 2012)*

7.1 Strojové učení

Definování strojového učení je datováno do roku 1959, kdy jej poprvé představil A. Samuel v rámci svého naprogramování pro hraní šachů. Nechal program, aby sehrál tisíce her proti sobě samému, přičemž se program postupně učil, jaké kombinace jsou nejoptimálnější pro danou partii, až nakonec Samuela porazil.

Strojové učení je dle stanfordského slovníku definováno jako proces aplikování indukčních algoritmů, které jsou jedním z podpůrných procesů při objevování znalostí. (*Stanford glossary, 1998*)

V širším kontextu lze říci, že proces strojového učení je v zásadě užití algoritmů pro vytvoření modelů, které jsou užity pro lepší predikci a rozhodování, a to vše bez lidského zásahu. (*SAS insights, 2017*) Tato funkcionalita je využívána pro potřeby filtrování emailu, optického rozpoznávání znaků (OCR) nebo při detekci nebezpečného malware nebo vetřelců uvnitř sítě.

Strojové učení může být dále děleno dle dílčích úkonů na následující skupiny:

- **Supervised learning**
  - Počítači jsou prezentovány vstupy, díky kterým si má osvojit jakési obecné pravidlo, které bude mapovat vstupy na výstupy. Ve speciálních případech může být vstup dostupný pouze z části.
- **Semi-supervised learning**
  - Počítači jsou předány pouze nekompletní testovací data, přičemž některé z cílových výstupů také chybí.
- **Active learning**
  - Počítač obdrží pouze předem stanovený trénovací vzorek(znaky), na základě, kterého je nucen optimalizovat svůj výběr, pro které obdrží testové znaky.
- **Reinforcement learning**
  - Trénovací data jsou zde prezentována jakožto odměna nebo trest, která jsou počítači předána pouze zpětně na základě toho, jak se počítač zachová v rámci dynamického prostředí – hraní hry proti soupeři nebo řízení auta.
- **Unsupervised learning**
  - Žádné označené vzorky nejsou učícímu algoritmu prezentovány, což zapříčiní nutnost vyhledání vlastní struktury a také vstupů. Tento druh učení může být užit pro vyhledávání skrytých vzorů v datech.

8 Metodika zpracování

Praktická část diplomové části bude rozdělena do několika částí, aby bylo možné v dostatečné míře rozebrat rozsáhlou problematiku uživatelské behaviorální analýzy pro obě zvolené SIEM aplikace.

První část bude věnovaná instalaci deploymentu pro QRadar a AlienVault OSSIM, implementace UBA modulů a vysvětlení principů UBA a machine learningu v prostředního konkrétní aplikace. V obou případech se bude jednat o virtuální appliance hostované na ESXi VMware vSphere v6.5.

Druhá část definuje užití UBA a strojového učení na předdefinovaných use casech SIEM aplikace.

Třetí část demonstruje užití UBA na vlastních vytvořených use case.

Pro účely této části byly užity data pocházející z reálné implementace z infrastruktury středního podniku operujícího v bankovním sektoru. V případě potřeby bližších informací o tomto nasazení, je možné je nalézt v předchozí závěrečné (bakalářské) práci s názvem: Analýza a návrh nasazení SIEM řešení v prostředí středního podniku (Nedbal, 2016)

Z legislativních důvodů jsou osobní a citlivé údaje z datového zdroje pozměněny, zakryty nebo jinak upraveny. Rovněž není možné je přiložit jako přílohu k práci.

Jedná se o data ze tří zdrojových zařízení (log source), čítajících v součtu více než 1 000 000 logů (záznamů).

- **Fortigate** – 1 000 000 logů, firewall, sběr informací o komunikaci uživatelů v infrastruktuře,
- **Eventlog**- 60 000 logů, active directory server, informace o autentizaci aj.,
- **IBMSense** – 6 000 logů, zdroj sbírající informace v rámci UBA modulu.

Před samotným nahráním do SIEM předcházel proces normalizace, parsování a vytvoření custom log source.

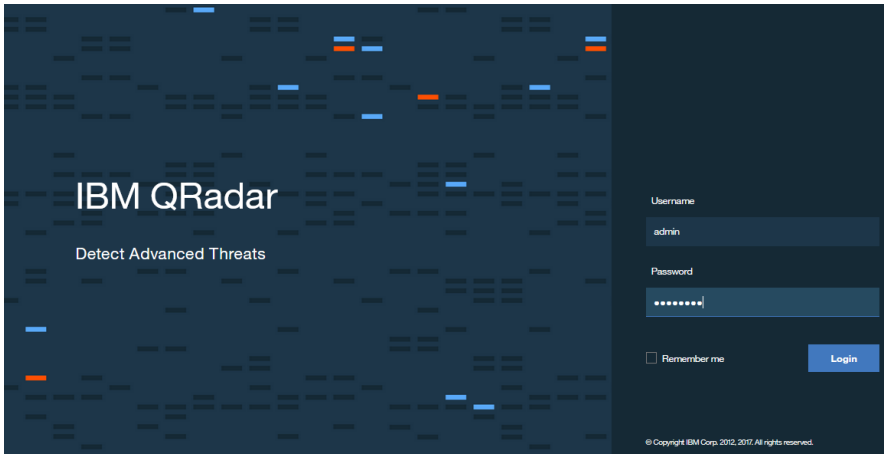
8.1 Instalace SIEM aplikací

8.1.1 Instalace IBM Security QRadar SIEM

IBM Security QRadar SIEM je dostupný jako ISO obraz, běžící na operačním systému Linux CentOS 7. Minimální požadovaná konfigurace pro nasazení a instalaci byla specifikována v předchozí kapitole. Užitá virtuální appliance má definovány tyto parametry: 8 CPU, 24 GB RAM a 380 GB úložiště.

Obrázek 14 -QRadar – instalace, vlastní zpracování

Po spuštění instalačního wizardu je uživatel vyzván k výběru konkrétního typu appliance. V dalších krocích pak vybere, o jaké se jedná řešení (All-in-one, Event collector, Data node, …) a zda jde o vytvoření nového nebo opravu již existujícího řešení. Poté nastaví čas, datum, IP adresu pro konzoli, root heslo, specifikuje doménu, bránu, DNS a další potřebné IP adresy. Po zadání všech nezbytných údajů se instalační proces dokončí a je možné na QRadar přistoupit z dříve definované IP adresy konzole. Po instalaci a příjmu datového toku či událostí už jsou aplikována výchozí korelační pravidla QRadaru.



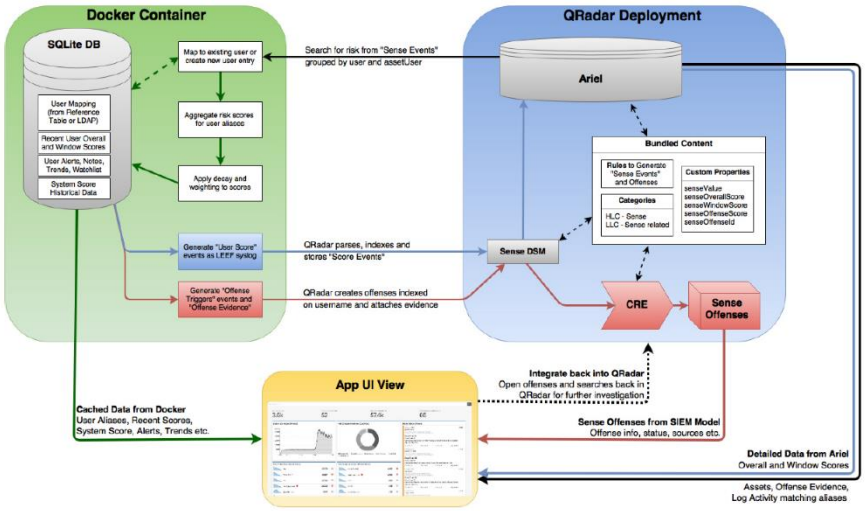
Obrázek 15 - QRadar – web konzole, vlastní zpracování

Po úspěšném nasazení bude přiblížena funkcionalita UBA v rámci QRadaru. QRadar je schopen díky svému UBA modulu, který není instalován v rámci defaultní instalace, z toho důvodu je nutné jej později přidat. Tento modul je možné nainstalovat v rámci Extension managementu z Admin tabu. Přidání modulu je chvilkovou záležitostí, nicméně aby bylo úspěšné, je nutné mít vytvoření log source IBM Sense, který bude akumulovat informace v rámci UBA a po přidání provést plný deploy SIEM aplikace. Nejnovější modul nese verzi 2.8 a pro jeho plnou funkcionalitu je nutné vytvořit v QRadaru autorizační token, který je do modulu zadán, tento token představuje povolení, že má UBA přístup všude, kam je to potřeba.

Samotná definice UBA již byla zmíněna v předchozí kapitole, přičemž definování UBA v prostředí SIEM aplikace se zásadním způsobem neliší. QRadar je schopen monitorování uživatelského chování na základě příchozích událostí ze zdrojů logů. Na základě vestavěných nebo vytvořených use casů a vnitřního algoritmu definuje skóre, které je indikátorem potenciálního nebezpečí ze strany daného uživatele. Kromě toho UBA modul generuje vlastní záznamy, které jsou evidovány pomocí IBM Sense, ten se snaží zlepšit pohled na adekvátní stav skóre UBA jednotlivých uživatelů. Velmi důležitou funkcí modulu je sdružování různých autentizačních údajů pod jméno jednoho uživatele, ten se totiž může v rámci sítě vyskytovat několikrát a v závislosti na užitém software se může jeho uživatelské jméno lišit.

Kromě samotných principů UBA, je QRadar schopen rovněž implementovat pokročilou funkcionalitu machine learningu. Strojové učení v tomto případě znamená, že se modul učí predikovat budoucí chování na základě již zažitých skutečností. Podrobnější definici strojového učení lze nalézt v předchozí kapitole.

8.1.2 Princip kolekce dat o uživatelích v UBA QRadaru



Obrázek 16 - QRadar – proces sběru dat UBA, převzato a upraveno (IBM corp., 2018)

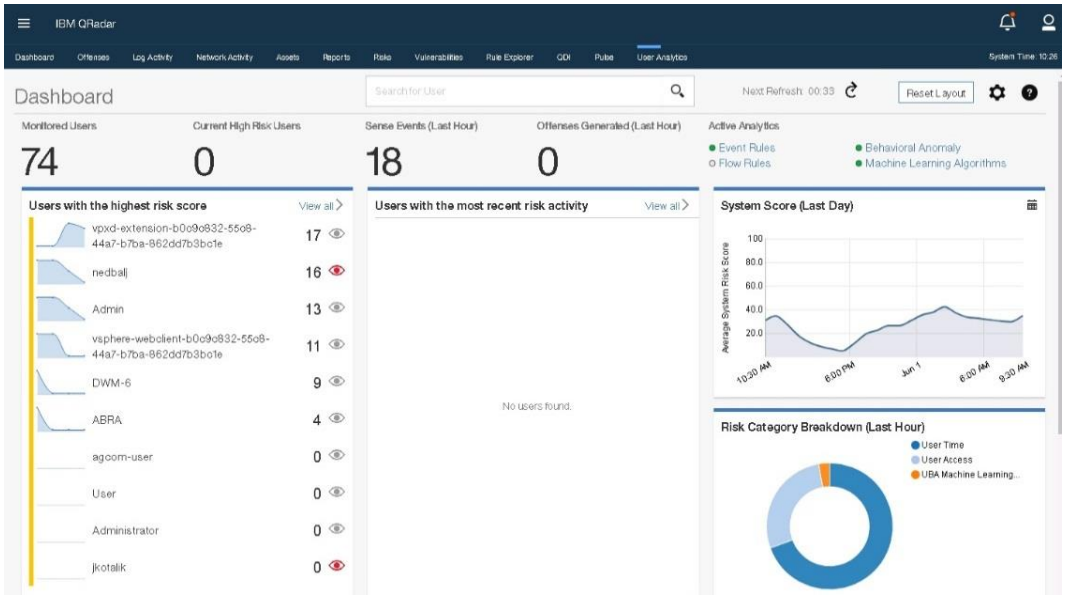
Na schématu výše lze blíže pochopit, jakým způsobem proces kolekce dat o uživatelích v rámci UBA modulu funguje. QRadar přijímá logovací události a datový tok ze zdrojových zařízení. Z těchto logů jsou pomocí pravidel vyhledávány konkrétní události a data, které jsou spouštěčem pro vytvoření dalších událostí pro již zmíněný IBM Sense, který přímo koresponduje s UBA aplikací.

Aby byl proces zdařilý, je nutné, aby měly příchozí události definované uživatelské jméno, doménu nebo jiný identifikační atribut.

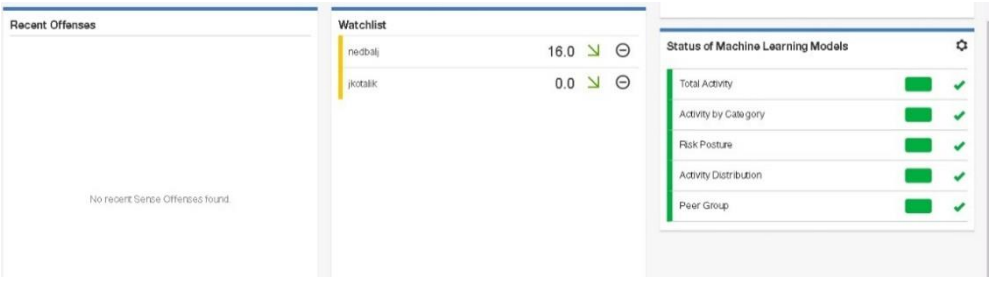
Modul UBA si z událostí zdroje IBM Sense extrahuje atributy „username“ a „senseValue“ (což je definování přírůstku pro skóre), podle kterého upraví konkrétní hodnotu u souvisejícího uživatele.

Hodnota senseValue je definována odlišně pro každé z nastavených pravidel z rulesetu UBA modulu, především v závislosti na závažnosti dané události. Čím více uživatel porušuje pravidla, tím vyšší skóre je připsáno k jeho jménu.

V případě, že uživatel překročí definovanou hranici skóre, UBA modul vytvoří událost, jejíž odezvou bude vytvoření bezpečnostního incidentu (offense) jakožto varování na podezřelé chování. Kromě toho je zároveň uživatel zařazen do skupiny velmi podezřelých uživatelů.



Obrázek 17 -QRadar UBA – GUI 1, vlastní zpracování



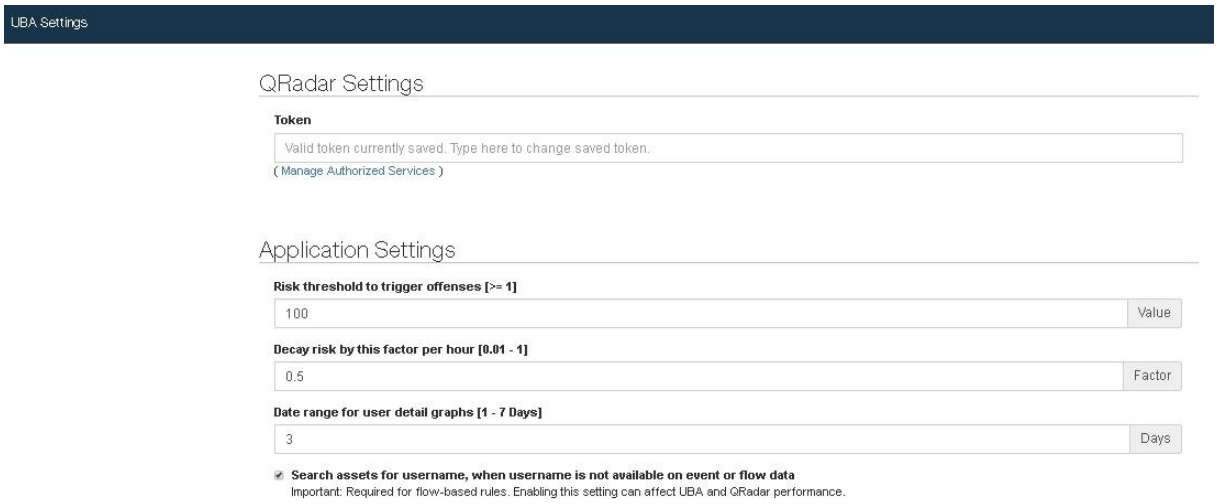
Obrázek 18 - QRadarUBA – GUI2, vlastní zpracování

- **Users with highest risk score** – zobrazuje přehled celkového skóre získaného pro jednotlivé uživatele. V případě velkého počtu monitorovaných se zobrazuje žebříček s prvními 10 místy.
- **Users with recent risk activity** – zobrazuje nejnovější aktivitu uživatelů v kontextu prohřešení se proti definovaným pravidlům.
- **Watchlist** – představuje jistou formu selekce, díky které si lze přehledně zobrazit podezřelé uživatele v systému.
- **System score** – suma skóre, kterého dosáhli uživatelé za určený časový interval. Maximální zobrazená doba je 30 dní.
- **Risk Category Breakdown** – graf zobrazující nejčastější druhy prohřešků za poslední hodinu. Graf lze přiblížit a při prokliknutí je schopen zobrazit konkrétní události od různých uživatelů.
- **Recent Offenses** – představuje seznam nejnovějších bezpečnostních incidentů pro uživatele, kteří se díky své aktivitě dostali nad hranici stanovenou pro spuštění offense.

- **Status of Machine Learning Models** – ukazuje stav modelů definovaných pro účely strojového učení.

Po úvodním představení následuje bližší seznámení s nastavením uživatelské behaviorální analýzy a rovněž strojového učení.

User Behavior Analysis settings



Obrázek 19 - QRadar UBA nastavení přes GUI, vlastní zpracování

- **Token** – představuje verifikační nástroj QRadaru, díky kterému je modulu propůjčena veškerá funkcionalita a přístupová práva v QRadar appliance.
- **Risk treshold to trigger offenses** – je hodnota, která specifikuje hranici pro vytvoření offense, tzn. že uživatel se provinil natolik, že jeho chování je významně v rozporu s definovanými politikami.
- **Decay risk by this factor per hour** – hodnota skóre, o kterou bude uživatelovo skóre sníženo za každou hodinu, pokud nedojde k opětovnému porušení pravidel.
- **Date range for user detail graphics** – týká se datové specifikace pro grafy, které zobrazují uživatelskou aktivitu v kontextu UBA modulu.
- **Search assets for username, when username is not available on event or flow data** – důležitý atribut, který je schopen významně pomoci s dodefinováním událostí. V případě, že není uživatelské jméno přítomno v příchozích událostech, je schopen si modul tyto informace vytáhnout z Assetů(sběr informací o doménách, IP adresách a uživatelích,..). Na druhou stranu je tato možnost v případě časté absence poměrně nákladná na výkon.

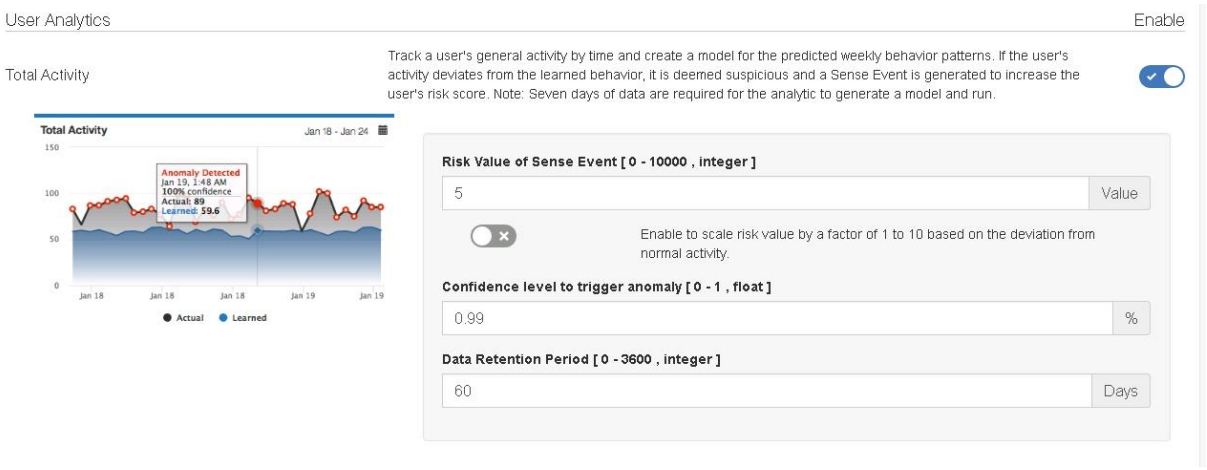
Machine learning

Nyní bude blíže specifikováno grafické rozhraní strojového učení v UBA modulu QRadaru a rovněž jednotlivá funkcionalita v rámci aktivních modulů strojového učení.

Definice strojového učení je pokryta v předchozí kapitole a svou povahou se příliš neliší od funkcionality v rámci QRadaru. Pomocí nahrávání logovacích záznamů do QRadar je ML schopno definovat určitý druh normálního chování, pomocí kterého později predikuje budoucí stav aktivity.

Nutno podotknout, že nadstavba strojového učení není ničím zanedbatelným a svými nároky vysoce zvyšuje nároky celé appliance. V tomto případě není měřitelnou jednotkou EPS nebo FPM ale počet monitorovaných uživatelů. Při monitoringu 2000 nejvíce rizikových uživatelů jsou nároky konzole 64 GB. V případě monitoringu 5000 uživatelů je pak potřebná hodnota dvojnásobná. Kromě toho je rovněž potřeba alespoň 5 GB volná kapacita na úložišti pro aplikace QRadaru. Poslední prerekvizitou je užití verze IBM QRadaru 7.2.8 a vyšší, aktivní UBA modul a rovněž správně definovaný IBM Sense DSM.

Pro všechny níže uvedené modely je nutné mít alespoň **7 dní** dat pro vyhodnocení analytického modelu. V případě absence dat nebude žádný z níže uvedených modelů vygenerován.

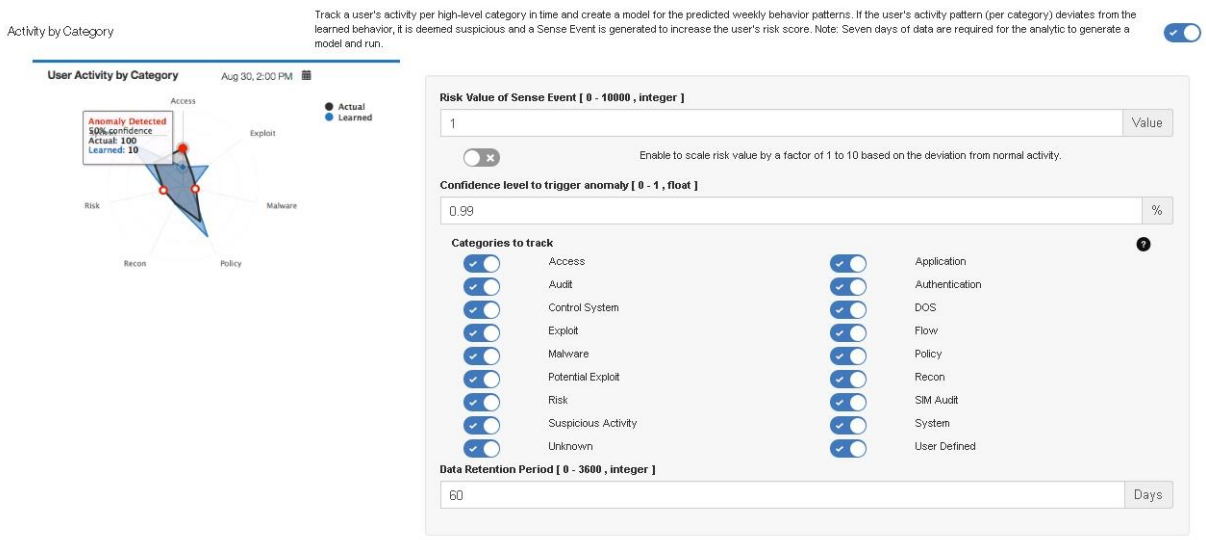


Obrázek 20 - QRadar – ML app – User analytics, vlastní zpracování

Tento model vytváří souhrnný graf pro všechny uživatelské aktivity v rámci týdenních zvyklostí. V případě, že se zde vyskytuje odchylka, je toto chování považováno za potencionálně nebezpečné a je generována událost IBM Sense pro zvýšení skóre v UBA modulu. Odchylkou může být cokoliv, od odlišného času či místa přihlášení, rozdílná IP adresa, opakovaná aktivita, špatné zadání credentials, aj. Míra, s jakou bude skóre zvednuto je definováno v rámci UBA případů užití.

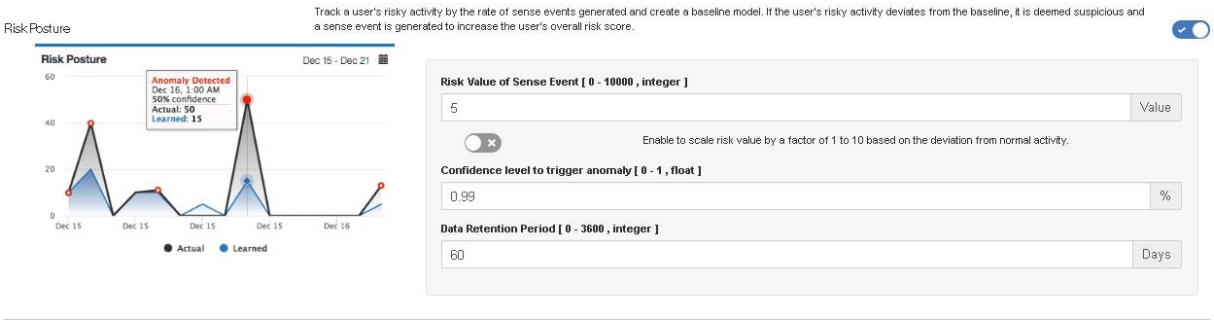
Nyní budou rozebrány atributy modelů, které jsou ve většině případů shodné. Rozdílné atributy budou dodefinovány pro konkrétní model.

- **Risk value of sense event** – představuje hodnotu, jaká bude přičtena k uživatelovi, pokud dojde k příjmu události od IBM Sense log source. Základní hodnota je 5.Kromě toho je také možné zapnout možnost, díky které bude toto skóre násobeno hodnotou v intervalu <1;10> v závislosti na míře odchylky od naučeného chování.
- **Confidence interval to trigger anomaly** – definuje interval spolehlivosti, který musí splňovat algoritmus ML, než bude generován sense event (anomálie).
- **Data retention period** – představuje počet dní, po který budou uchována data modelu. Přednastavená hodnota je 60 dní.



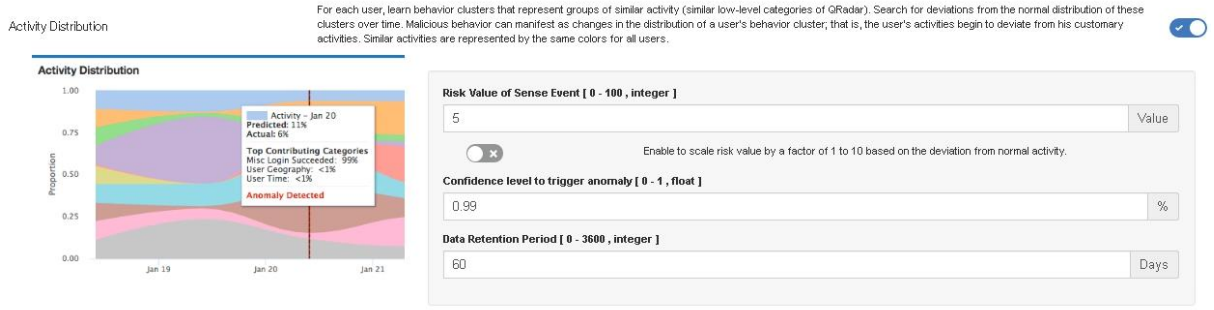
Obrázek 21 - QRadar – ML app – User activity by category, vlastní zpracování

Model zachycuje aktivity generované uživateli a analyzuje je dle kategorií, které jsou promítnuty do tzv. spider grafu (občas také adresován jako polygon-circle graph). Tento graf zobrazuje sumu událostí do jednotlivých kategorií. Lze zde rozlišit celkovou a naučenou hodnotu, o kterou je celek navýšen. Opět jsou sledovány týdenní behaviorální návyky uživatelů. V případě vzniku odchylky je generována událost a připočtena adekvátní hodnota skóre ke sledovanému uživateli.



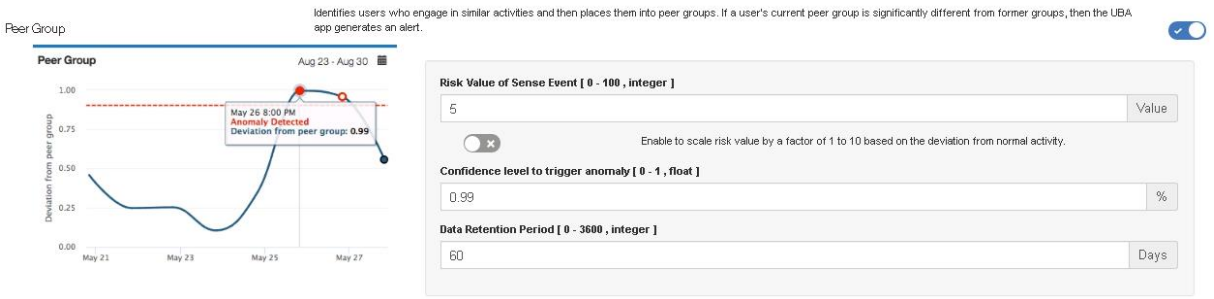
Obrázek 22 - QRadar – ML app – Risk posture, vlastní zpracování

Model sleduje uživatelskou aktivitu dle míry vygenerovaných Sense událostí, pomocí kterých vytváří základní model. V případě odchylky od základního modelu je generována událost.



Obrázek 23 - QRadar – ML app – Activity distribution, vlastní zpracování

Model je schopen definovat shluky chování pro každého uživatele, které jsou posléze sdruženy do tématicky podobných kategorií nižšího druhu. V případě odchylek je možné předefinování modelu pro daného uživatele. Pro všechny uživatele jsou použity shodné barvy.



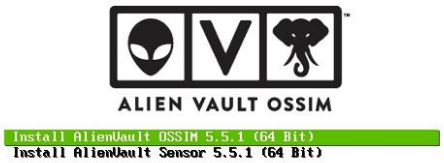
Obrázek 24 - QRadar – ML app – Peer Group, vlastní zpracování

Poslední model rozpoznává uživatele, kteří mají shodné aktivity. Tyto uživatele sdružuje do skupiny, která představuje porovnání pro pozdější chování uživatelů. Pokud je chování příliš odlišné od skupiny, je generována událost a navýšeno skóre v UBA modulu.

8.1.3 Instalace AlienVault OSSIM

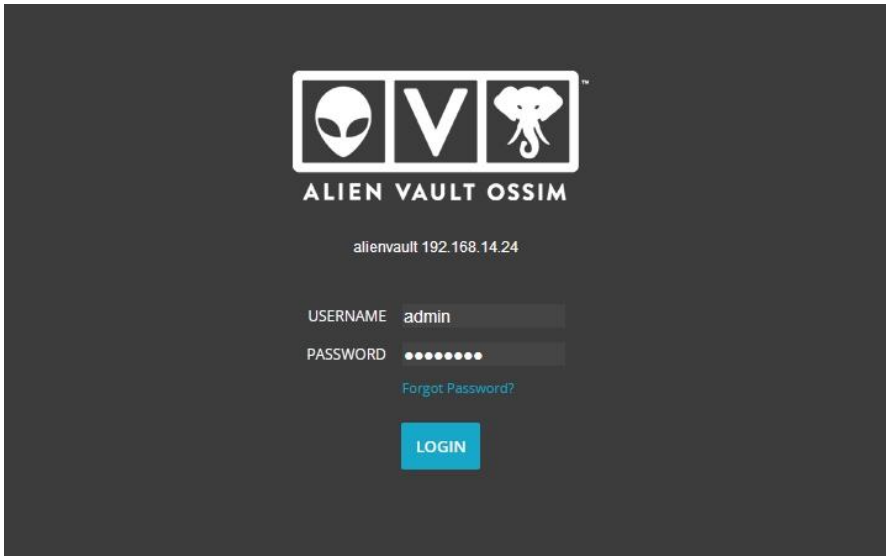
AlienVault OSSIM je dostupný jako ISO obraz, který běží na operačním systému Linux Debian 8.x. Minimální konfigurace pro deployment a instalaci je blíže specifikovaná v kapitole věnující se porovnání SIEM aplikací. Nicméně, konkrétní užité nastavení pro tuto virtuální appliance je 4 CPU, 8 GB RAM a 300 GB úložiště.

Grafický instalátor je schopen provést instalaci Linuxu i veškerých propriet pro AlienVault OSSIM.



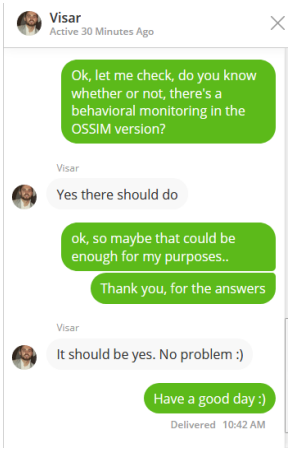
Obrázek 25 - AlienVault OSSIM instalace, vlastní zpracování

V rámci provedení instalačního procesu je administrátor požádán o definování základních konfigurací nutných pro dokončení instalace (IP adresa pro konzoli, …). Po dokončení instalace je umožněn přístup přes definovanou IP adresu do webového rozhraní, kde jsou dokončeny další konfigurační kroky jako je změna hesla, skenování síťové infrastruktury pro nalezení všech zdrojových zařízení. Nalezená zařízení je pak nutné blíže specifikovat, rozlišit jejich druh, operační systém aj. Posledním krokem v rámci prvotní konfigurace je vložení licenčního tokenu pro OTX (Open Threat Exchange), který je nezbytný pro získávání aktuální databáze zranitelností. Poslední částí je automatizované spuštění defaultních korelačních pravidel pro datový tok a události.



Obrázek 26 - AlienVault OSSIM – web konzole, vlastní zpracování

Po úspěšném deploymentu bude nyní blíže definována funkcionalita UBA, která je v rámci AlienVault OSSIM přislíbena. UBA modul byl jednou z podmínek pro implementaci dané SIEM aplikace, z toho důvodu byl nejdříve proveden výzkum, zda je tato funkcionalita obsažena, nicméně neexistují žádné konkrétní manuály pro UBA v AlienVault OSSIM až na výjimku všeobecného pojednání o UBA (https://www.alienvault.com/blogs/security-essentials/user-behavior-analytics-methods-and-best-practices-2). Z toho důvodu proběhla online konverzace (5.7.2018) s jedním z členů Business developmentu, který tuto skutečnost potvrdil.



Obrázek 27 - Konverzace s AlienVault SW expertem, vlastní zpracování

Nicméně po úspěšné implementaci AV bylo zjištěno, že AlienVault neumožňuje využití principů UBA, je schopen pouze základního užití NBA (Network behavior analysis), což je v podstatě základní funkcionalita SIEM řešení, resp. jeho log managementu.

Obrázek 28 - GUI AlienVault OSSIM – Netflow, vlastní zpracování

8.2 Užití modulu uživatelské behaviorální analýzy na vestavěném Use case

Z důvodu zjištění absence UBA modulu pro SIEM aplikaci AlienVault OSSIM, bude tato část věnována pouze případu užití v rámci IBM Security QRadar SIEM.

Modul UBA v QRadaru má desítky již nadefinovaných případů užití, které lze používat takřka na jakoukoliv událost či činnost, která se v síťové infrastruktuře vyskytne. Výstupem této části práce bude poukázat na to, jakým způsobem funguje jeden konkrétní zvolený use case a jak se tato skutečnost promítne do chodu UBA modulu nebo QRadaru jako takového.

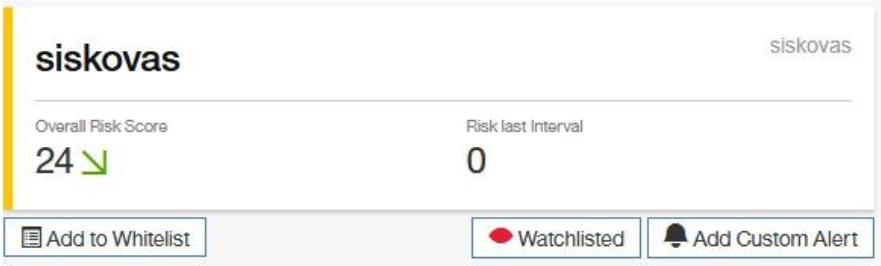
Pro tyto účely byl zvolen případ užití týkající se zachycení podezřelých IP adres komunikujících v síti pod účtem monitorovaného uživatele. Vyhodnocení IP adres jakožto potencionálně nebezpečných probíhá na nadstavbové externí databázi IBM X-Force, kde jsou shromažďovány zranitelnosti a exploity z celého světa.

Jsou použita data z reálné fungující implementace, z toho důvodu jsou některá uživatelská jména nebo citlivé údaje úmyslně skryty.

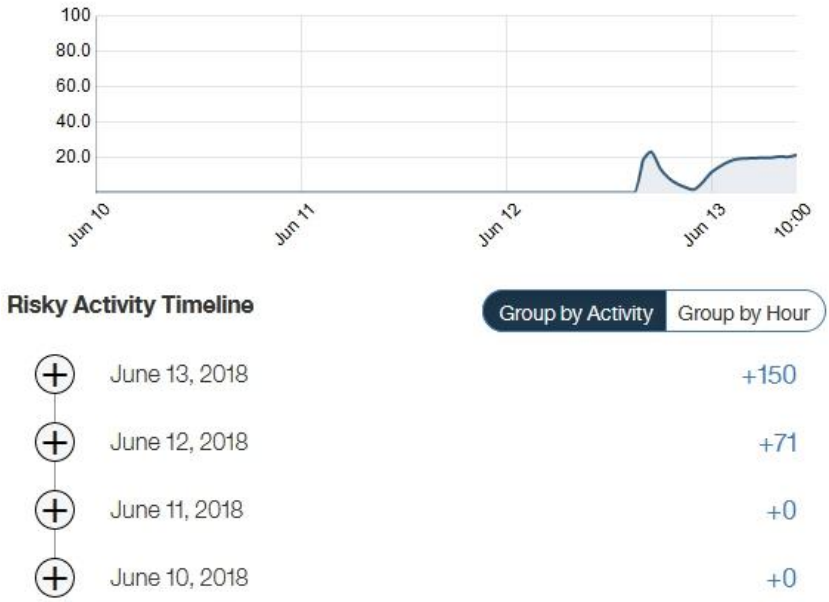
Prvotním krokem je demonstrovat, jak vypadá modul v případě, že tento uživatel přistupuje většinu času na správné IP adrese. V dalším kroku budou IP adresy (konkrétně 10 IP adres) nahrazeno potencionálně nebezpečnými. Tento krok by měl významně zvednout generování Sense událostí, a tudíž i změnit skóre a grafickou distribuci UBA modulu. Konečným výstupem by v tomto kroku mělo být překročení stanovené hranice, po které bude uživatel vyhodnocen jako velmi nebezpečný a bude generován bezpečnostní incident poukazující na tuto skutečnost.

Počáteční stav uživatele a jeho sense flow

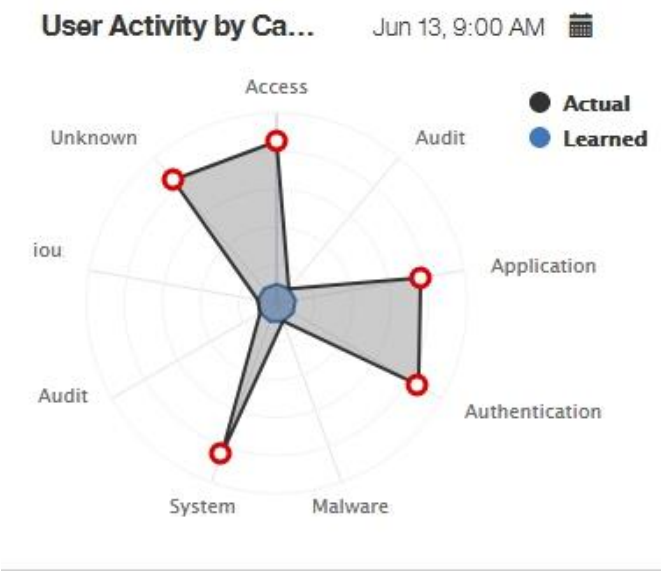
Jak lze vidět z přiložených screenů, již na začátku provedl uživatel některé úkony, které byly v rozporu s nastavenými politikami. Byla přidána na watchlist a rovněž byl sledován stav přidaného sense skóre. Na spider grafu jsou vyobrazeny nejčastější aktivity, ty se týkají autentizace, přístup do sítě a rovněž komunikace s aplikacemi.



Obrázek 29 - Use case – prvotní skóre, vlastní zpracování



Obrázek 30- Use case – časová osa rizikových aktivit, vlastní zpracování



Obrázek 31 - Use case – prvotní spider graf, vlastní zpracování

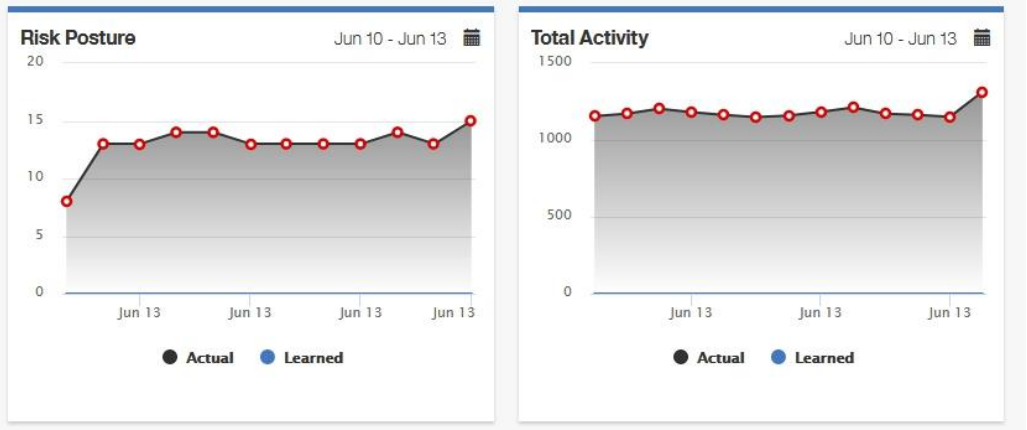
Stav uživatele po přidání potenciálně nebezpečných IP adres

Náhlý nárůst v komunikaci pod uživatelovými credentials a s potenciálně nebezpečnou IP adresou je zapříčiněn zasíláním zdrojů logů do QRadaru. Pro tyto účely je užito skriptu **logrun.pl**, který je přítomen v QRadaru. Díky tomuto skriptu lze simulovat reálný provoz a testovat chování SIEM aplikace. Bližší informace o těchto záznamech jsou obsaženy na začátku kapitoly věnující se instalaci SIEM aplikací.

Nutno ještě zmínit, že v případě užití tohoto skriptu je nutné respektovat limity licencování, protože lze velmi rychle přetížit procesování logů. V případě překročení pak QRadar události nejdříve staví do fronty a později je zahazuje.

```
[root@qradar ~]# ps aux| grep logrun
root       407  4.9  0.0 140496  4648 ?        S    09:12   5:12 /usr/bin/perl -
w /opt/qradar/bin/logrun.pl -f /opt/qradar/bin/Eventlog_SRV01.txt -u 192.168.15.
26 -l -t 300
root      2198  5.1  0.0 140628  5080 ?        S    09:13   5:19 /usr/bin/perl -
w /opt/qradar/bin/logrun.pl -f /opt/qradar/bin/Fortigate1_2.txt -u 192.168.15.25
 -l -t 300
root      9653  5.5  0.0 140496  5084 pts/0    R    10:56   0:00 /usr/bin/perl -
w /opt/qradar/bin/logrun.pl -f /opt/qradar/bin/siskovas.csv -u 192.168.15.25 -l
-t 300
root     10501  0.0  0.0 112660   964 pts/0    S+   10:56   0:00 grep --color=au
to logrun
```

Obrázek 32 -Zasílání událostí pomocí logrun skriptu, vlastní zpracování



Obrázek 33 - Use case – změna v aktivitách, vlastní zpracování

Na přiloženém grafu je vidět rapidní nárůst v objemu přijímaných událostí, který byl mnohdy na samé hranici licencování. Vzrostl počet sledovaných uživatelů v infrastruktuře, tudíž je zde i nárůst v množství prohřešků proti definovaným politikám.

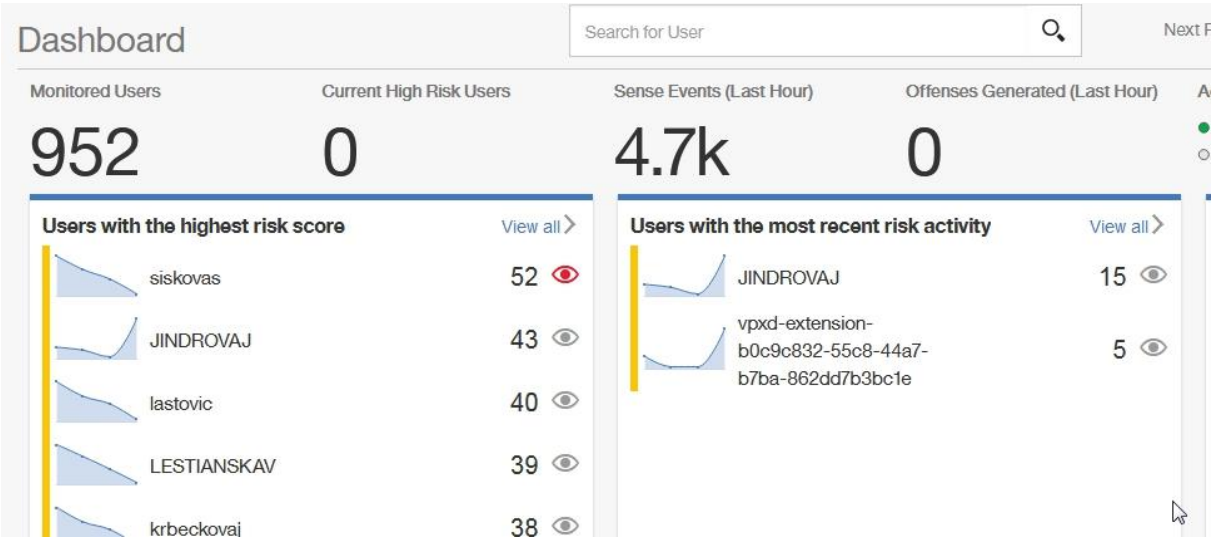
Po zavedení tří nových zdrojů logovacích událostí je v rámci infrastruktury monitorováno 952 uživatelů, kteří jsou schopni generovat 4,7k událostí typu IBM Sense za hodinu. Nyní byly použity níže uvedené IP adresy z databáze IBM X-Force, které jsou klasifikovány jako nebezpečné. Tyto IP adresy jsou asociovány na jediné uživatelské jméno, což by mělo demonstrovat chování UBA modulu v případě nálezu podezřelých IP adres a aplikace předdefinovaných use case pro tento případ.

Nutno zmínit, že ani jedna z adres není vedena jako mallware, jedná se o kombinaci spam nebo exploit IP adres.

190.236.81.254
181.64.192.178
202.83.42.93
203.115.80.174
186.81.117.162
190.131.220.29
190.223.40.174
190.237.183.143
202.134.9.157

Obrázek 34 - Nebezpečné IP adresy – IBM X-force, vlastní zpracování

Po předefinování IP adres na potenciálně nebezpečné pozvolna začíná stoupat sense skóre smyšleného uživatele ***siskovas***, přičemž skóre kolísá v závislosti na objemu přijímaných událostí a nastavení tzv. *decay*, tedy o kolik bude skóre poníženo za určitou časovou periodu.

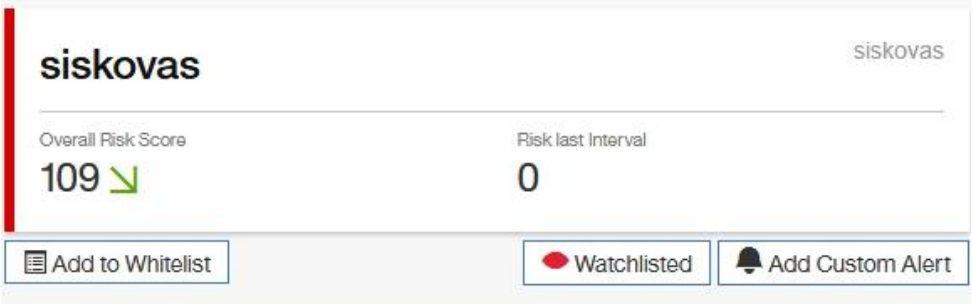


Obrázek 35 - Use case, nárůst skóre a dashboard, vlastní zpracování

Obrázek 36 - Use case – seznam spuštěných pravidel, vlastní zpracování

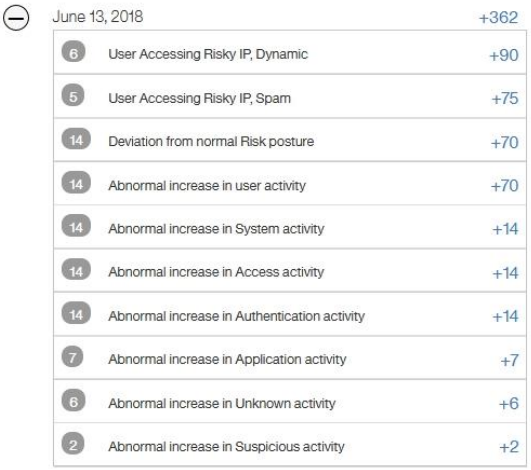
V rámci UBA modulu je kromě vytváření vlastních pravidel pro uživatelskou analýzu rovněž zaznamenáno, jaká další pravidla byla spuštěna, resp. překročena u daného uživatele. Na seznamu výše lze vidět, že kromě několika pravidel specifických pro UBA modulu jsou spouštěna pravidla pro zdrojovou a cílovou adresu, které také poukazují na určité nebezpečí plynoucí z povahy IP adres. Mimo to je zde evidován i zdroj logů X-Force, který vyhodnocuje IP adresy jako rizikové. Z čehož je vidět, jak komplexní je obraz, který QRadar poskytuje už při své základní funkcionalitě. O to více je tento pohled umocněn v případě užití nadstavbových modulů typu UBA.

Po určitém čase je skóre uživatele natolik vysoké, že se změní jeho klasifikace na velmi rizikového, a protože překročil stanovenou hranici, bude generován bezpečnostní incident poukazující na tuto skutečnost. Níže je vidět grafické znázornění pro uživatele, rozpis rizikových aktivit, za které skóre získal a také vygenerovaná offense, která je kromě přiřazení v UBA modulu vedena a notifikována také v klasickém prostředí QRadaru.



Obrázek 37 - Use case – překročení limitu pro generování offense, vlastní zpracování

V rámci uživatelského přehledu v UBA modulu je přístupný i seznam aktivit proti politikám a jejich ohodnocení dle potenciální rizikovosti. Z povahy případu užití je zřejmé, že nejvíce bodů je za spouštění offensí asociovaných se zjištěním rizikové IP adresy. Kromě toho jsou vyhodnoceny aktivity související s uživatelskou aktivitou, která se vymyká již naučeným patternům uživatele.

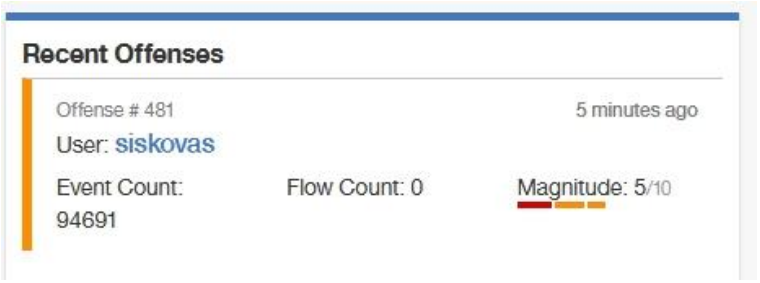


Obrázek 38 - Use case – rozpis rizikových aktivit uživatele, vlastní zpracování

Zvýšená aktivita a rizikové aktivity jsou promítnuty do spider grafu uživatele, který nyní zobrazuje rozpoložení aktivit v mnohem větším množství a rovněž jsou zde uplatněny i některé naučené algoritmy strojového učení. Nutno zmínit, že míra naučených postupů se zvyšuje s počtem přijatých událostí a rovněž časem, který se může aplikace „učit.“

Obrázek 39 -Use case, modifikace spider grafu – zvýšení aktivity, vlastní zpracování

Jak již bylo zmíněno, konečným výstupem tohoto případu užití by měl být vznik bezpečnostního incidentu, který je propojen do UBA modulu, ale zároveň se ukazuje v klasickém prostředí QRadaru.



Obrázek 40 - Use Case – generování offense, UBA modul, vlastní zpracování

Obrázek 41 - Use case – generování offense, prostředí QRadaru, vlastní zpracování

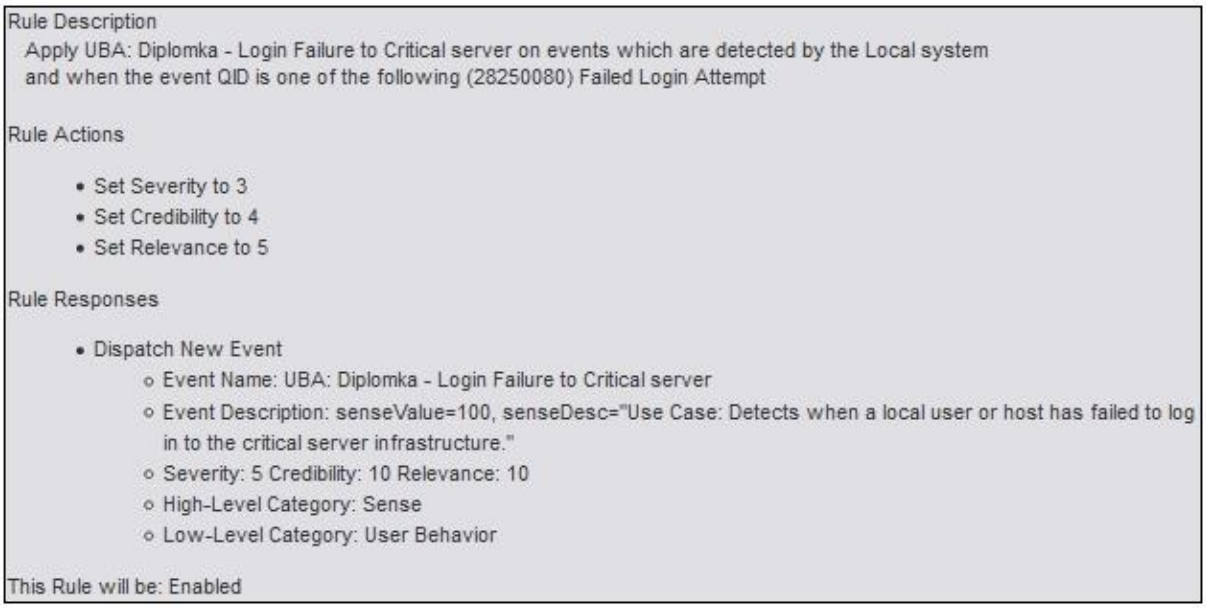
8.2.1 Vlastní Use case – login failure

V této části bude demonstrováno užití vlastního případu užití UBA modulu. Tento případ bude zacílen na možnost přidání UBA aspektu k jakémukoliv pravidlu, konkrétně se bude jednat o pravidlo zkoumající špatné zadání credentials. Proces špatného zadání autorizačních údajů může čas od času znamenat překlep pravého uživatele, faktem ale je, že pokud bude tato skutečnost nastávat často, může se jednat o snahu násilného přístupu do síťové infrastruktury.

Pro tento případ budou užity shodná data jako v předchozím případě.

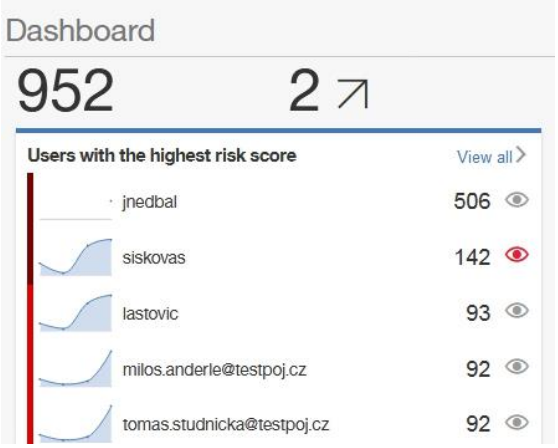
Prvním krokem bude vytvoření pravidla monitorující špatná přihlášení uživatelů do sítě. Pravidla lze implementovat plošně na všechny monitorované uživatele, nicméně z důvodu nutného zatajení citlivých uživatelských údajů, je spuštěné pravidlo ukázáno pouze na uživateli **jnedbal**.

Po spuštění wizarda pro vytvoření event rule je vygenerováno následující pravidlo.



Obrázek 42 - Use case – vytvořené pravidlo pro monitoring login failure, vlastní zpracování

Pravidlo je aplikováno v případě, že je detekována událost specifikovaná jako QID 28250080 (Failed Login Attempt). Pravidlo nastaví hodnoty atributů u události pro credibilitu, relevanci a severitu. Kromě toho bude vytvořena nová událost s názvem „UBA: Diplomka – Login Failure to Critical server.“ Tato událost upraví skóre v UBA modulu u uživatele, který se dopustil špatného přihlášení. Kromě toho je zobrazen text vysvětlující, o jaký případ užití se jedná. Událost spadá do log source IBM sense a je ohodnocena jinými hodnotami atributů pro severitu, credibilitu a relevanci. Poslední řádek znamená, že pravidlo je zapnuto okamžitě po ukončení wizardu.



Obrázek 43 -Use case, nárůst skóre uživatele, vlastní zpracování

Výše je možné vidět, že uživatelé **jnedbal** a **siskovas** jsou barevně odlišeni od ostatních uživatelů. Jedná se o velmi rizikové uživatele a povahou svých aktivit překročili nastavenou hranici politik, což zapříčinilo vznik offense.

Obrázek 44 - Use case – rozpis rizikových aktivit uživatele, vlastní zpracování

V rozpisu aktivit je vidět veliká penalizace za login failure, tato hodnota sense skóre byla nastavena především z časových důvodů, aby bylo možné dobře demonstrovat funkcionalitu vytvořeného pravidla.

Obrázek 45 - Use Case – generování offense, UBA modul, vlastní zpracování

Konečným výstupem celého use case je jako v předchozím případu generování bezpečnostního incidentu poukazujícího na velmi rizikové chování uživatele.

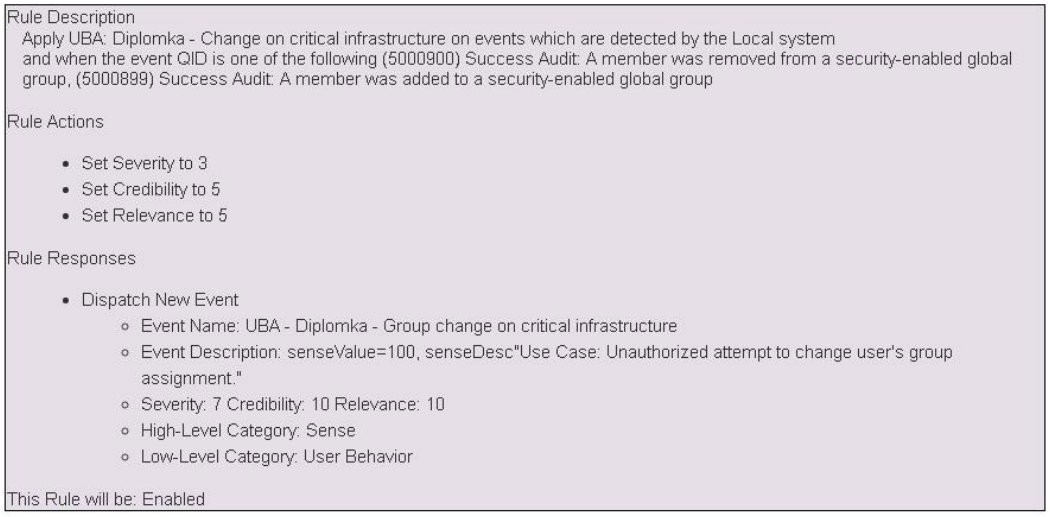
8.2.2 Vlastní Use Case – uživatelská změna na serveru

Druhy vlastní případ užití UBA modulu bude zaměřen především na problém, který je čas od času možné v síťové infrastruktuře pozorovat. Jedná se o snahu zařadit různé uživatele do skupin, které mají vyšší spektrum pravomocí a zároveň nepodléhají tak rozsáhlému monitoringu podnikaných aktivit, protože se u nich očekává jistá míra znalostí bezpečnostních rizik. Monitoring je prováděn i u pokusu o přidání, a především u uživatelů, kteří nemají přístup k administrátorskému účtu nebo operují z účtu, který administrátorské pravomoce nemá.

Pro tento případ jsou užita shodná data jako v případě předdefinovaných use case.

Vytvořené pravidlo bude sledovat aktivitu na doménovém kontroleru, v případě, že bude evidována aktivita v rozporu se stanovenou politikou následuje generování bezpečnostního incidentu poukazujícím na tuto skutečnost. Pravidlo je možné užít plošně na jakéhokoliv „provinilého“ uživatele, demonstrováno však bude pouze na uživateli **jnedbal**.

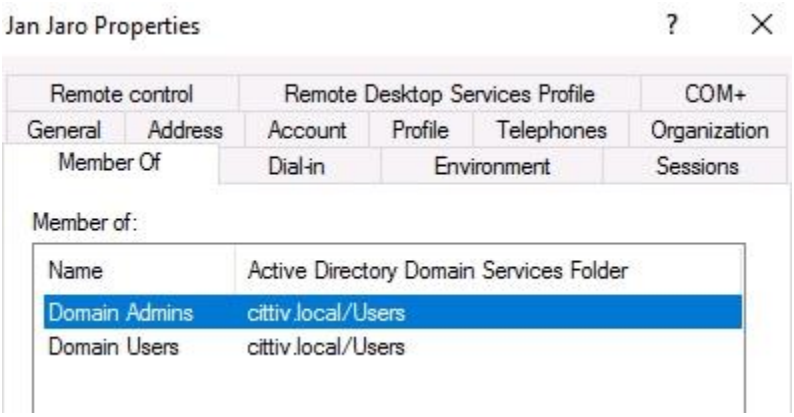
Pravidlo je vytvořeno přes instalační wizard QRadaru, kde jsou blíže specifikovány jeho parametry.



Obrázek 46 - Use case – vytvořené pravidlo pro sledování změny na serveru, vlastní zpracování

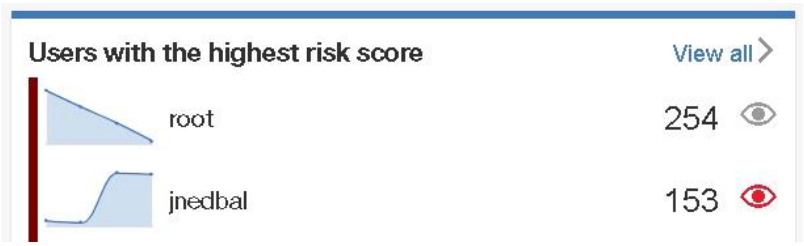
Pravidlo je aplikováno v případě, že je detekována přijatá událost související se změnou uživatelovy skupiny a zároveň tato činnost není provedena někým s administrátorskou pravomocí. Pravidlo nastaví hodnoty závažnosti, kredibility a relevantnosti a jako odezvu generuje novou událost s názvem „*UBA – Diplomka – Group change on critical infrastrucute.“* Tato událost v první řadě zvýší skóre v UBA modulu u uživatele, který se pokusil o změnu. Událost vysvětluje, že se jedná o neautorizovaný pokus o změnu uživatelova skupinového zařazení. Opět

jsou upraveny hodnoty pro závažnost, kredibilitu a relevantnost dané události. Událost svou povahou spadá pod IBM sense log source a pravidlo je zapnuto ihned po ukončení instalačního wizardu.

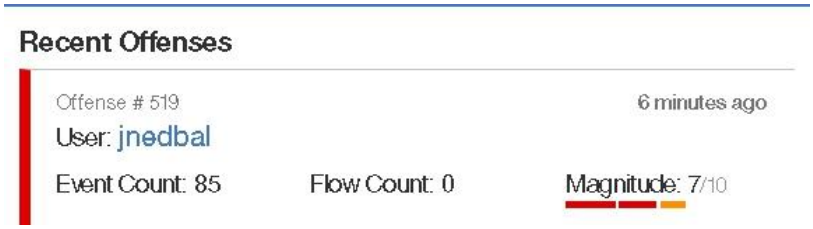


Obrázek 47 - Use Case – přidání uživatele do skupiny doménových administrátorů, vlastní zpracování

Po vytvoření platného pravidla byla provedena akce nekorespondující s aktivním rulesetem – konkrétně přidání normálního doménového uživatele do skupiny doménových administrátorů. Přidání uživatele **jjaro** bylo provedeno z účtu s rozšířenou pravomocí **jnedbal**. Jelikož má uživatel pravomoce na tuto operaci, lze přidání do skupiny na jeho účtu provést. Tato akce je ihned rozpoznána prostředím QRadaru, který z příchozí události vyčte jak účet, který byl přeřazen tak účet, ze kterého byla změna provedena. Tento uživatel má sice rozšířené pravomoce, avšak neměl by být schopen přeřazovat tímto způsobem uživatele v infrastruktuře (nejedná se o administratora). Z toho důvodu je vytvořena další událost poukazující na neautorizovaný pokus a je generována offense, která se ukáže v UBA modulu i v QRadaru pod záložkou „Offenses."

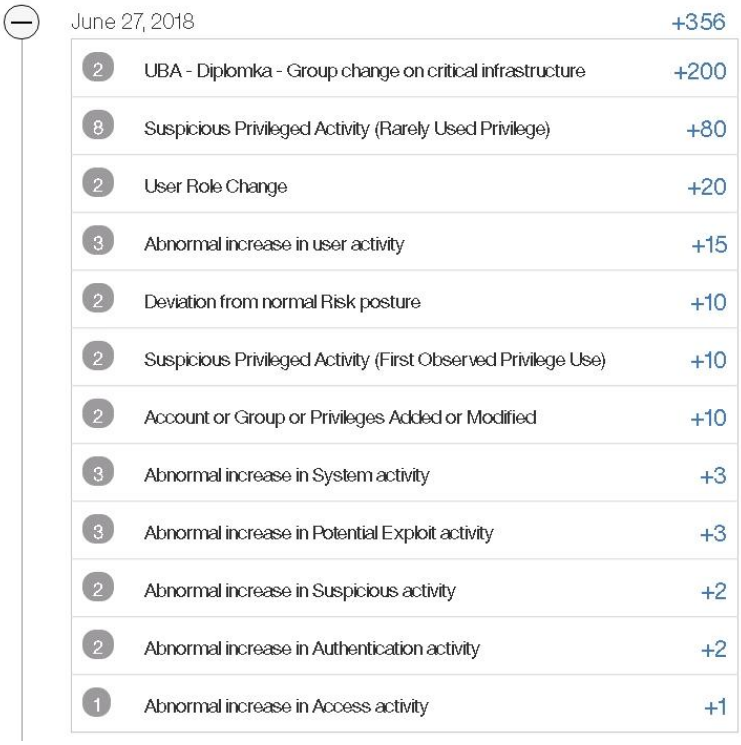


Obrázek 48 - Use case – změna uživatelského skóre po spuštění pravidla, vlastní zpracování



Obrázek 49 - Use case – generování bezpečnostního incidentu po spuštění pravidla, vlastní zpracování

Níže lze vidět, jakým způsobem byl tento počin ohodnocen v rámci UBA modulu – kromě samotného vlastnoručně definovaného pravidla UBA přičítá i za aktivitu, která je u tohoto uživatele neobvyklá (vzácně použitá). Dále zde nechybí ohodnocení za změnu uživatelské role, abnormální zvýšení aktivity nebo modifikaci privilegií.



Obrázek 50 - Use case – seznam podezřelých aktivit, vlastní zpracování

Obrázek 51 - Use case – spider graf po spuštění group pravidla, vlastní zpracování

Ze spider grafu lze nyní jasně vyčíst, že uživatel povahou svého chování operuje v mezích potencionálního exploitu a časté systémové autentizace. Algoritmy strojového učení predikují budoucí aktivitu v SIM auditu, který se změnou uživatelských rolí a skupin souvisí.

Obrázek 52 - Use case – historie bezpečnostních incidentů, vlastní zpracování

Výše je možné vidět, že UBA modul si v rámci audit. politiky uchovává záznamy z předchozí prohřešků a přehledně je zobrazuje v rámci svého GUI. Na základě těchto bezpečnostních incidentů je možné zahájit investigaci uživatele za účelem určení povahy podezřelého chování. Vytvořený bezpečnostní incident je zároveň výstupem potvrzující funkcionalitu vlastního vytvořeného pravidla pro účely UBA modulu a sledování uživ. aktivity.

9 Zhodnocení praktické části (shrnutí výsledků)

V rámci praktické části byla demonstrována funkcionalita uživatelské behaviorální analýzy dvou konkrétních SIEM aplikací. V případě AlienVaultu OSSIM/USM nebyl nalezen žádný samostatný UBA modul sbírající informace a data o monitorovaných uživatelích v síti. Tato funkcionalita je i přesto rozebírána na oficiálním fóru – vypisují se workshopy, které mají napomáhat k analýze uživatelských dat a byla přislíbena před samotnou implementací jedním ze specialistů společnosti. Dá se předpokládat, že pod pojmem uživatelské analýzy je v tomto případě myšlen sběr v rámci logovacích aktivit a jejich pokročilé funkcionality, které jsou ještě navíc součástí pouze komerční verze USM, ke které se není možné, bez zdlouhavé komunikace s prodejními manažery, dostat. Z důvodu absence UBA modulu nebylo možné demonstrovat ani předdefinované nebo vlastní vytvořené use case.

V případě UBA modulu přítomném v QRadaru bylo možné sledovat podrobné informace o uživatelích, na které byly ještě navíc aplikovány modely strojového učení. UBA modul QRadaru využívá pro řešení problematického chování set vestavěných případů užití, který lze rozšířit o libovolný vlastní use case. Byla představena funkcionalita modulu včetně užitých principů strojového učení. V případě předdefinovaného případu užití byl demonstrován proces rozpoznání nebezpečných IP adres a adekvátních reakcí na ně – generování událostí a bezpečnostních incidentů, navýšení rizikové skóre apod. Posléze byly vytvořeny dva vlastní případy užití, které demonstrují nasazení principů UBA na jakékoliv pravidlo. Případy byly zaměřeny na špatnou autentizaci a na neoprávněnou změnu či pokus o změnu uživatelské skupiny, asociované se zvýšením pravomocí, bez administrátorských práv. Všechny výše zmíněné případy byly úspěšně deployovány a jejich koncovým výstupem byl vždy vznik bezpečnostního incidentu upozorňující na potenciální hrozbu v síťové infrastruktuře.

Lze konstatovat, že v rámci zvolených SIEM aplikací si v kontextu uživatelské behaviorální analýzy vedl jednoznačně lépe IBM Security QRadar SIEM. K tomuto faktu přispívá nejen absence fungujícího UBA modulu u AlienVaultu, ale také velký problém se škálovatelností a schopností auditovat logy u větších firem (jak bylo rozebráno v komparativní části práce). Tyto nedostatky jsou natolik závažné, že se užití, ať už open source nebo komerční verze této SIEM aplikace, nedoporučuje. Smysl užití AlienVaultu lze vidět při deploymentu na velmi malé infrastruktury, které generují malý počet událostí za den, a tudíž budou splněny legislativní požadavky na auditing logů. Avšak i v tomto případě by bylo nutné užití komerční verze, neboť funkcionalita open source je natolik osekaná, že nelze dělat takřka nic kromě základního monitoringu datového toku a vytváření rulesetu. Ostatní funkcionalita (monitoring událostí, pokročilé vyhledávání, reporting nebo síťová behaviorální analýza) je zpřístupněna až pro verzi AlienVault USM.

10 Závěry a doporučení

Cílem této práce bylo hlubší prozkoumání možností, které plynou z užití principů behaviorální analýzy uživatelů, a to konkrétně pro SIEM systémy. Samotná myšlenka práce vychází z premisy, že nestačí svou síťovou infrastrukturu chránit zvenčí, ale stejně adekvátně by měla být chráněna zevnitř.

Aby bylo možné provést reálnou implementaci a prošetření problematiky, bylo nutné důkladné nastudování nejen týkající se funkcionality SIEM a UBA, nýbrž také zjistit proveditelnost řešení v rámci legislativního rámce ČR. Následujícím logickým krokem posléze bylo definování SIEM principů a bližší seznámení s konkrétními SIEM aplikacemi v rovině praktické i teoretické. Dalším cílovým požadavkem bylo již zmíněné demonstrování implementace dvou konkrétních SIEM aplikací, u kterých byla předem zjištěna presence užití UBA modulu. Tyto zjištění byla kritická pro pozdější část práce, neboť se během procesu implementace UBA modulu pro jednu ze SIEM aplikací ukázalo, že není schopná integrovat funkcionalitu UBA, ačkoliv byla dopředu přislíbena. Z toho důvodu byla funkcionalita behaviorální analýza demonstrována pouze pro SIEM aplikaci od firmy IBM s názvem IBM Security QRadar SIEM.

V rámci demonstrování funkcionality SIEM aplikací lze říci, že se do určité míry jedná o doporučený postup, jak v případě implementace SIEM aplikace, tak v nastavení a vysvětlení funkcionality UBA modulu. Práce rovněž nastiňuje jakési srovnání dvou užitých SIEM aplikací a jejich doporučené užití v kontextu velikosti organizace a robustnosti specifického deploymentu. Díky korektně nastavenému SIEM systému s aktivním UBA modulem bylo demonstrováno, jak snadné a efektivní je vyhledávání potencionálních hrozeb zvenčí, ale i zevnitř. Tento fakt do jisté míry potvrzuje premisu o nutnosti vlastnictví stejného či podobného software, aby byla firma před těmito hrozbami chráněna a mohla bezpečně operovat v kybernetické rovině. Nutno zmínit, že ačkoliv je SIEM předepsán Zákonem o kybernetické bezpečnosti pro všechny organizace z tzv. kritické infrastruktury, implementace těchto principů a softwaru je doporučena pro všechny druhy organizací nehledě na jejich velikost nebo míru působnosti na trhu.

Naproti tomu je vhodné podotknout, že implementace SIEM a pokročilých modulů pro správu a monitoring síťové infrastruktury je vhodné si nechat nasadit od odborníka. V opačném případě by mohly být následky špatného nasazení pro firmu a její citlivé informace fatální. Ať už se jedná o špatně nastavená pravidla, nesledování všech důležitých zdrojových zařízení nebo sledování až příliš zařízení, což vede k přehlcení systému a včasná detekce hrozby se pak mnohdy rovná hledání jehly v kupce sena.

Pokud se bude tato práce držet své hlavní myšlenky, že nejcennější entitou je informace, ať už v kontextu snížení entropie či jako uchovatel hodnoty organizace, lze pak pokračování této tématiky vidět v kontinuálním zlepšování kognitivních procesů software, resp. jeho integrace se strojovým učením. Je sice pravda, že kooperace se strojovým učením, konkrétně s IBM Watsonem, už je přítomna pro UBA modul během psaní této práce, nicméně jeho funkcionalita je spíše omezena na detekci a shromažďování informací o podezřelých datových tocích nebo komunikaci v síti. Dalším mezníkem by mohla být vyšší míra učení, vizualizace datového toku a tudíž hrozeb, a rovněž také automatizace některých procesů spojených s investigací podezřelého uživatele.

Pokud bych měl zhodnotit, co mi přinesla tato práce, pak to bylo bezesporu nutné prohloubení znalostí v oblastech týkajících se SIEM aplikací, neboť jsem kromě IBM Security QRadar SIEM jinou nepoužíval a rovněž pak jejich pokročilou funkcionalitu v podobě jejich kooperace se strojovým učením a uživatelskou behaviorální analýzou. Z praktického hlediska mi tato práce přinesla možnost implementace výše zmíněného software a také blízké seznámení s funkcionalitou uživatelské behaviorální analýzy a strojového učení.

11 Seznam použité literatury

AlienVault OSSIM: Documentation [online]. 2018 [cit. 2018-06-04]. Dostupné z: https://www.alienvault.com/documentation/

AlienVault: System requirements [online]. 2018 [cit. 2018-06-11]. Dostupné z: https://www.alienvault.com/docs/data-sheets/AV-USM.pdf

CHERRY, Kendra. *Behavior analysis: Definition* [online]. 2018 [cit. 2018-06-04]. Dostupné z: https://www.verywellmind.com/what-is-behavior-analysis-2794865

Cybersecurity: Definition. *Merriam-Webster* [online]. 2018 [cit. 2018-06-08]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity

ČERMÁK, Miroslav. *APT: Definice APT* [online]. 2012 [cit. 2018-06-04]. Dostupné z: https://www.cleverandsmart.cz/APT-je-jen-dalsi-buzzword/

ČERMÁK, Miroslav. *Behaviorální analýza: Ochrana před APT díky UBA* [online]. 2012 [cit. 2018-06-04]. Dostupné z: https://www.cleverandsmart.cz/ochrani-nas-behavioralni-analyza-site-pred-apt/

ČERMÁK, Miroslav. *Zero day attack* [online]. 2012 [cit. 2018-06-04]. Dostupné z: https://www.cleverandsmart.cz/zero-day-attack/

DARDICK, Glenn S. *Cyber Forensics Assurance* [online]. 2010 [cit. 2018-06-03]. DOI: 10.4225/75/57b2926c40cda. Dostupné z: http://ro.ecu.edu.au/adf/77/

Detect Security Breaches with UBA [online]. 2015 [cit. 2018-08-22]. Dostupné z: https://www.gartner.com/smarterwithgartner/detect-security-breaches-early-by-analyzing-behavior/

Evolution of machine learning: SAS Insights [online]. 2017 [cit. 2018-09-27]. Dostupné z: https://www.sas.com/en_us/insights/analytics/machine-learning.html

IBM Security QRadar SIEM: Documentation v. 7.3.1 [online]. 2018 [cit. 2018-06-04]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_pdf_launch.html

IBM Security QRadar SIEM: System requirements [online]. 2018 [cit. 2018-06-11]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_ha_vrt_ap_reqs.html

IBM Security QRadar SIEM: User Behavior Analytics app [online]. 2018 [cit. 2018-06-16]. Dostupné z: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.UBAapp.doc/b_Qapps_UBA.pdf?view=kc

ISO 27000 DIRECTORY, 2013. *ISO/IEC 27002: Code of practise. ISO 27k standards* [online]. [cit. 2018-3-05]. Dostupné z: http://www.iso27001security.com/html/27002.html#Section11

ISO 27000 DIRECTORY, 2016. *IEC: About the IEC* [online]. [cit. 2018-02-04]. Dostupné z: http://www.iec.ch/about/?ref=menu

ISO 27000 DIRECTORY, 2016. *ISO: About ISO* [online]. [cit. 2018-02-04]. Dostupné z: http://www.iso.org/iso/home/about.htm

ISO 27000 DIRECTORY, 2016. *ISO: ISO Standard* [online]. [cit. 2018-02-04]. Dostupné z: http://www.iso.org/iso/home/standards.htm
ISO 27000 DIRECTORY: Information security management systems [online]. 2013 [cit. 2018-06-03]. Dostupné z: https://www.iso.org/standard/54534.html

ISO 27000 DIRECTORY: ISO 27003 [online]. 2017 [cit. 2018-06-03]. Dostupné z: https://www.iso.org/obp/ui/#!iso:std:63417:en

ISO 27000 DIRECTORY: ISO 27004 [online]. 2017 [cit. 2018-06-03]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27004:ed-2:v1:en

ISO 27000 DIRECTORY: Overview and vocabulary [online]. 2018 [cit. 2018-06-03]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Is your SIEM on the endangered list? [online]. 2015 [cit. 2018-08-22]. Dostupné z: https://searchsecurity.techtarget.com/feature/The-hunt-for-data-analytics-Is-your-SIEM-on-the-endangered-list

KAVANAGH, Kelly M. a Oliver ROCHFOLD. Gartner: Critical capabilities SIEM. *Gartner* [online]. 2015, [cit. 2018-06-08]. Dostupné z: https://solutionsreview.com/dl/Gartner_Critical_Capabilities_SIEM_2015_LRDL2.pdf

MAREŠ, Miroslav. *Definice bezpečnosti* [online]. [cit. 2018-06-03]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

MILLER, David. Security information and event management (SIEM) implementation. New York: McGraw-Hill, 2011. ISBN 0071701095.

NEDBAL, Jan. *Analýza a návrh nasazení SIEM řešení v prostředí středního podniku*. Hradec Králové, 2016. Bakalářská práce. Univerzita Hradec Králové. Vedoucí práce Mgr. Josef Horálek Ph.D.

NÚKIB: Aktuální legislativa [online]. 2018 [cit. 2018-06-04]. Dostupné z: https://www.govcert.cz/cs/kyberneticky-zakon/legislativa/

NÚKIB: Vyhláška č.82/2018 [online]. 2018 [cit. 2018-06-04]. Dostupné z: https://www.govcert.cz/cs/nova-vkb/

ROWE, Dale C., Barry M. LUNT a Joseph J. EKSTROM. The role of cyber-security in information technology education. In: *Proceedings of the 2011 conference on Information technology education – SIGITE '11* [online]. New York, New York, USA: ACM Press, 2011, 2011, s. 113- [cit. 2018-06-04]. DOI: 10.1145/2047594.2047628. ISBN 9781450310178. Dostupné z: http://dl.acm.org/citation.cfm?doid=2047594.2047628

SALADO, Alejandro a Roshanak NILCHIANI. Using Maslow's hierarchy of needs to define elegance in system architecture. *Procedia Computer Science* [online]. 2013, **16**, 927-936 [cit. 2018-06-08]. DOI: 10.1016/j.procs.2013.01.097. ISSN 18770509. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1877050913000987

SIEGEL, Eric. Predictive analytics: the power to predict who will click, buy, lie, or die. Hoboken, N.J.: John Wiley, c2013. ISBN 978-1-118-59647-0

Stanford glossary: Machine learning definition [online]. 1998 [cit. 2018-09-27]. Dostupné z: http://ai.stanford.edu/~ronnyk/glossary.html

TURCOTTE, Melissa, and Moore, Juston Shane. *User Behavior Analytics*. United States: N. p., 2017. Web. doi:10.2172/1345176.

UBA tools can thwart security attacks [online]. 2015 [cit. 2018-08-22]. Dostupné z: https://searchsecurity.techtarget.com/feature/User-behavioral-analytics-tools-can-thwart-security-attacks

User behavior analysis: What is UBA used for? [online]. 2018 [cit. 2018-06-04]. Dostupné z: https://www.quora.com/What-is-user-behavior-analysis-used-for?

VÍZNER, Lukáš, 2014. *Security information and event management v rámci cloudové infrastruktury* [online]. Hradec Králové, [cit. 2016-06-04]. Univerzita Hradec Králové. Vedoucí práce Mgr. Josef Horálek, Ph.D.

VON SOLMS, Rossouw a Johan VAN NIEKERK. *From information security to cyber security* [online]. 2013, **38** [cit. 2018-06-03]. DOI: 10.1016/j.cose.2013.04.004. ISSN 01674048. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167404813000801?via%3Dihub

WOLTERS KLUVER ČR, 2014. *Zákon č.181/2014 ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů.* In: ASPI [právní informační systém]. Praha: Wolters Kluwer ČR [vid. 2015-11-12]

ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. [cit. 2018-06-03]. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2.

Oskenované zadání práce

i