FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání bakalářské práce

Název:	Detekce bezpečnostních hrozeb v nastrojích pro správu bezpečnostních informací a událostí
Student:	Linda Šindelářová
Vedoucí:	Ing. Jiří Šlefr, MBA
Studijní program:	Informatika
Obor / specializace:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	do konce letního semestru 2023/2024

Pokyny pro vypracování

V ČR, stejně jako v jiných zemích EU, jsou stanovena pravidla pro zabezpečení dat a jejich ochranu pro různé typy firem (např. zdravotnictví, energetika, finanční sektor apod.)

1) Proveďte analýzu dostupných informačních zdrojů a SW nástrojů pro správu bezpečnostních informací a událostí (SIEM - Security Information and Event Management) a zanalyzujte souhrnně pravidla pro identifikaci bezpečnostních hrozeb v datech, které lze odhalit pomocí těchto nástrojů.

2) Navrhněte a implementujte pravidla zformulovaná v předchozí části pomocí nástrojů Elastic Stack (zejména pak části Elastic SIEM).

3) Připravte vzorek dat obsahující náhodně se vyskytující bezpečnostní hrozby a otestujte funkčnost implementovaných pravidel v nástroji Elastic SIEM.

Elektronicky schválil/a prof. Ing. Pavel Tvrdík, CSc. dne 3. ledna 2023 v Praze.

Bakalářská práce

DETEKCE BEZPEČNOSTNÍCH HROZEB V NÁSTROJÍCH PRO SPRÁVU BEZPEČNOSTNÍCH INFORMACÍ A UDÁLOSTÍ

Linda Šindelářová

Fakulta informačních technologií
Katedra počítačových systémů
Vedoucí: Ing. Jiří Šlefr, MBA
29. června 2023

Odkaz na tuto práci: Šindelářová Linda. *Detekce bezpečnostních hrozeb v nástrojích pro správu bezpečnostních informací a událostí.* Bakalářská práce. České vysoké učení technické v Praze, Fakulta informačních technologií, 2023.

Obsah

Seznam obrázků

Seznam výpisů kódu

Chtěla bych poděkovat především svému vedoucímu bakalářské práce, panu Jiřímu Šlefrovi, a jeho kolegovi Rudolfu Janouškovi za užitečné rady při tvorbě praktické části práce a za jejich ochotu a čas, který mi věnovali. Také bych chtěla poděkovat své rodině a přátelům za jejich podporu po celou dobu studia a psaní této práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne 29. června 2023 .....

Abstrakt

Tato bakalářská práce se věnuje bezpečnostním hrozbám v oblasti systémů a sítí a jejich detekci pomocí nástrojů pro správu bezpečnostních informací a událostí. Vychází zejména z legislativních požadavků na instituce, kterých se tyto hrozby týkají a analyzuje možná řešení. Zabývá se nástroji SIEM, analyzuje současný trh s těmito nástroji a navrhuje kritéria pro jejich výběr. Blíže rozebírá nástroje z rodiny Elastic Stack, jakožto nejpoužívanější opensource nástroje pro log management na trhu a popisuje konstrukci pravidel pro detekci hrozeb pomocí těchto nástrojů. V praktické části popisuje návrh vybraných pravidel v souladu s legislativními požadavky, jejich implementaci v nástroji Elastic SIEM a testuje jejich funkčnost.

Klíčová slova SIEM, bezpečnostní událost, bezpečnostní hrozba, log management, Elastic Stack

Abstract

This thesis focuses on security threats within IT systems and networks and detection of these threats using tools for security information and events management. It is based on legislative requirements for institutions that are affected by these threats and analyzes possible solutions. It focuses on SIEM tools, current market and criteria for their selection. It explores the tools from Elastic Stack family as today's most used open source tools for log management on the market and it describes the structure of rules for threat detection using these tools. In the practical section is described design of selected rules in accordance with mentioned legislative requirements, their implementation in Elastic SIEM and tests their functionality.

Keywords SIEM, security event, security threat, log management, Elastic Stack

Seznam zkratek

AWS	Amazon Web Services
CLF	Common Log Format
DDoS	Distributed Denial of Service
DNS	Domain Name System
ELF	Extended Log Format
EQL	Event Query Language
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Protection System
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KQL	Kibana Query Language
NF	Network Firewall
NIS	Network Information Security
NIST	National Institute of Standards and Technology
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operating System
OSI	Open Systems Interconnection
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
SQL	Structured Query Language
TCP	Transmission Control Protocol
UEBA	User and Entity Behavior Analytics
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAF	Web Application Firewall
XDR	Extended Detection and Response

Úvod

Bezpečnost v IT je velmi aktuální a důležité téma v ČR, EU i po celém světě. Využívání informačních technologií je v dnešním světě v podstatě každodenní záležitostí, stále se rozšiřuje do dalších oblastí a mnozí by se bez IT v zaměstnání i mimo něj neobešli. S neustále se rozšiřujícím využíváním ale také roste množství hrozeb, které na nás při používání jakékoliv formy informačních technologií čekají, proto roste i potřeba se zabývat IT bezpečností.

S takto rozšířeným využíváním informačních technologií a množstvím hrozeb se již v dnešní době nestačí bránit pouze z pozice jednotlivce. Jednotliví aktéři si pro používání informačních technologií, sítí a systémů nastavují pravidla pro jejich využívání, která si buď implementují sami nebo si je i nechávají zabezpečit specializovanými dodavateli bezpečnostních řešení.

V ČR, stejně jako v dalších státech EU, jsou stanovena základní pravidla a standardy pro zabezpečení dat a systémů, kterými by se určité typy firem měly při řešení své bezpečnosti řídit. Součástí těchto pravidel je také povinnost sbírat informace o bezpečnostních událostech a zavést systém, který bude detekovat hrozby a adekvátně na ně reagovat.

Ke sběru informací o dění v systémech a sítích slouží nástroje pro log management, ale pro detekci hrozeb, prevenci případných útoků nebo zabránění v jejich průběhu je vhodné využít SIEM nástroje. Ty poskytují určitý nadhled a umožňují hledání souvislostí mezi shromážděnými záznamy, které analyzují v reálném čase a díky této skutečnosti lze odhalit právě probíhající útoky nebo i komplexnější hrozby. Pro účinnou detekci a prevenci bezpečnostních hrozeb pomocí SIEM nástrojů je potřeba průběžně získávat záznamy o dění v sítích a systémech a správně nadefinovat pravidla, pomocí kterých se v záznamech identifikují podezřelé aktivity a chování, které mohou znamenat bezpečnostní hrozbu.

Předkládaná práce má teoretickou a praktickou část. V teoretické části nejdříve pojednává o aktuálních nařízeních platných v ČR, která souvisí s detekcí bezpečnostních hrozeb. Seznámí čtenáře se SIEM nástroji, jejich využitím při naplňování legislativních požadavků, zdroji záznamů, které jsou důležité k detekci hrozeb a jakým způsobem je možné hrozby a podezřelé chování detekovat. Poté rozebere současný stav trhu se SIEM nástroji, zmíní kritéria důležitá pro výběr vhodného nástroje a přiblíží nástroje rodiny Elastic Stack. V praktické části navrhuje a implementuje vybraná pravidla pro detekci hrozeb pomocí nástroje Elastic SIEM tak, aby byla v souladu s aktuálními nařízeními v ČR a následně otestuje jejich funkčnost.

Kapitola 1

Aktuální požadavky na kybernetickou bezpečnost

Stanovit obecné požadavky na kybernetickou bezpečnost, které budou aplikovatelné na všechny typy organizací je velmi obtížné, ba skoro nemožné, protože každá organizace má jiné nároky a záleží zde na mnoha faktorech. Za tímto účelem vznikla v ČR během posledních zhruba deseti let legislativní opatření, která se stále doplňují a přizpůsobují aktuálním požadavkům. Vybrané skupiny organizací se těmito pravidly musí řídit a pro ostatní mohou být vodítkem, jak svou kybernetickou bezpečnost zajistit. Legislativa se snaží stanovit základní úroveň opatření, kterou si následně organizace musí zpřísnit a přizpůsobit podle svých potřeb. K ideálnímu nastavení bezpečnostních opatření je možné využít služeb specializovaných firem, které pomáhají zanalyzovat potřeby dané organizace, navrhnout adekvátní řešení a zajistit jeho implementaci.

1.1 Kybernetická bezpečnost pohledem legislativy

1.1.1 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti [1] (dále jen Zákon), schválený v roce 2014 s nabytím účinnosti od roku 2015, sjednocuje a stanovuje základní úroveň bezpečnostních opatření, kterými se musí zákonem stanovené organizace řídit. Ukládá povinnost nahlašovat detekované incidenty a zavést systém, jak se bude na nalezené bezpečnostní incidenty reagovat.

Hlavním cílem Zákona je zvýšení kybernetické bezpečnosti, a to zejména v oblastech, které jsou nezbytné pro fungování státu. Určuje, které osoby a typy organizací se jím mají řídit, jaké mají povinnosti a jaká opatření mají zavést. Zákon se dotýká jen malého nejvýznamnějšího okruhu organizací, ale jeho posláním by se měly inspirovat i ostatní organizace při řešení své bezpečnosti.

Od roku 2014 prošel několika novelizacemi [1], kterými se mimo jiné rozšířil okruh organizací, kterých se týká. Aktuálně se jedná o tyto osoby a orgány:

- poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací,
- orgány a osoby zajišťující významnou síť,
- správci a provozovatelé
  - informačních a komunikačních systémů kritické informační infrastruktury,

  - významných informačních systémů,
  - informačních systémů základních služeb,
- poskytovatelé základních a digitálních služeb. [1]

Mezi základní služby podle Zákona řadíme ty, které jsou závislé na elektronické komunikaci nebo jejichž narušení by způsobilo škody a narušilo zabezpečení činností v odvětvích jako je energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura (online tržiště, internetové vyhledávače, cloud computing) a chemický průmysl. [1]

Zákon také stanovuje, jaká organizační a technická opatření se mají za účelem zvýšení bezpečnosti zavést. Příkladem technických opatření, která úzce souvisí s touto bakalářskou prací jsou:

- nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,
- nástroj pro detekci kybernetických bezpečnostních událostí,
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí. [1]

1.1.2 Vyhláška č. 82/2018 Sb.

Další důležitou legislativou týkající se této práce je vyhláška č. 82/2018 Sb. [2] (dále jen Vyhláška), která doplňuje Zákon o požadavky stanovené předpisy z Evropské unie, přesněji o směrnici NIS vydanou v roce 2016. Směrnice NIS (*Network Information Security*) byla zavedena za účelem stanovení jednotného standardu úrovně kybernetické bezpečnosti ve státech EU a zlepšení fungování vnitřního trhu (viz další kapitolu).

Tato vyhláška rozšiřuje okruh organizací, kterých se týká tento typ legislativy a určuje a upravuje:

- obsah a strukturu bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,
- 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,
- způsob likvidace dat, provozních údajů, informací a jejich kopií. [3]

Co se týče této bakalářské práce, Vyhláška přikazuje okruhu organizací vyplývajícího ze Zákona zavedení procesu pro detekci a vyhodnocení kybernetických bezpečnostních události a koordinaci a zvládání kybernetických bezpečnostních incidentů. Dále se mají definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu. Určuje také konkrétní pravidla a opatření týkající se správy bezpečnostních informací a událostí, která budou uvedena v dalších kapitolách.

Vyhláška také definuje některé významné hrozby, před kterými by se měly organizace chránit nebo alespoň detekovat jejich výskyt. Mezi takové hrozby patří například zneužití oprávnění uživatelů nebo administrátorů, provedení neoprávněných činností, zneužití identity, výskyt a spouštění škodlivého kódu; zneužití nebo neoprávněná modifikace dat, zneužití vnitřních prostředků, napadení elektronické komunikace odposlechem nebo modifikací (výčet všech hrozeb lze najít ve Vyhlášce [2]). Všechny tyto hrozby lze detekovat nástroji zmíněnými v následujících kapitolách.

1.1.3 Směrnice NIS2

Informační a komunikační technologie využíváme stále častěji a staly se součástí každodenního života. Tento vývoj vede také k rozšíření bezpečnostních hrozeb. Je skoro nemožné se jim bránit jako jednotlivec, tudíž je potřeba komplexnější řešení na úrovni státu, nebo ještě lépe koordinace reakcí a řešení na úrovni celé Evropské unie. Proto byl v roce 2016 první pokus o srovnání úrovně bezpečnosti v rámci EU v podobě směrnice NIS. [4]

Směrnice NIS dává členským státům EU široké možnosti v rámci vymezení oblasti působnosti této směrnice a způsobu řešení povinností v oblasti bezpečnosti a nahlašování incidentů, které stanovuje. Z přezkoumání vyplynuly velké rozdíly v zavedení těchto opatření v jednotlivých státech [5], a tudíž původní cíl této směrnice, kterým bylo srovnání úrovně bezpečnosti v členských státech EU, nebyl zcela naplněn.

Na konci roku 2022 vydal Evropský parlament a Rada Evropské unie směrnici NIS2 [5] týkající se opatření k zajištění vyšší společné úrovně kybernetické bezpečnosti v Evropské unii. Zavádí mnoho změn v zajišťování kybernetické bezpečnosti a rozšiřuje, rozděluje a pevněji stanovuje okruh organizací, kterých se bude týkat. Tyto změny jsou natolik zásadní, že se NÚKIB (*Národní úřad pro kybernetickou a informační bezpečnost*) rozhodl vytvořit zcela nový zákon o kybernetické bezpečnosti, který podle aktuálního plánu nabyde účinnosti v druhé polovině roku 2024.

Dle aktuálního návrhu (platného k 25. lednu 2023) [4] budou zasažené organizace rozděleny na několik typů podle toho, jak přísným režimem se budou řídit. Nově se budou tímto zákonem řídit všechny soukromé i veřejné organizace, které současně splňují tato pravidla:

- poskytují alespoň jednu službu uvedenou v přílohách směrnice,
- jsou středním nebo velkým podnikem, tedy zaměstnávají 50 a více zaměstnanců, nebo dosahují ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK). [4]

1.2 Nástroje pro řešení kybernetické bezpečnosti

Pro řešení kybernetické bezpečnosti ve firmách a splnění legislativních požadavků dnes existuje několik typů nástrojů. Následující typy nástrojů souvisí se zaznamenáváním událostí a činností v systému, detekcí bezpečnostních hrozeb z těchto záznamů a reakcí na ně.

Aby vůbec bylo možné hrozby detekovat, je potřeba z různých částí sítě a systému získat informace o dění a tyto informace vytřídit a centrálně uložit. O tyto funkce se starají nástroje pro log management. Sesbírané informace následně využijí SIEM (*Security Information and Event Management*) nástroje, které v nich dokáží identifikovat bezpečnostní incidenty a potenciální hrozby a tyto nálezy určitým způsobem reportovat. Dále přebírají roli SOAR (*Security Orchestration, Automation and Response*) nástroje, které na základě detekovaných hrozeb provedou automatickou akci k zastavení probíhajícího incidentu a minimalizaci následků tak, aby musel člověk zasahovat co nejméně.

1.2.1 Log management

Z legislativy vyplývá, že je potřeba zaznamenávat určité typy bezpečnostních událostí a tyto záznamy uchovávat pro analýzu v reálném čase, zjištění podrobností o incidentech a pro forenzní analýzu. Takový záznam se nazývá log.

Log je záznam událostí, které se odehrávají v systémech a sítích dané organizace. [6]

Log management je proces generování, přenosu, ukládání, analyzování a likvidace logů. [6]

Pro udržení bezpečnosti systémů a sítí roste potřeba shromažďovat záznamy z mnoha zdrojů, a je tedy zapotřebí hledat jiné řešení než ruční procházení logů. Proto jsou na trhu dostupné nástroje pro log management, díky kterým se správa logů zpřehlední a je potom jednodušší se v takovém množství záznamů zorientovat, analyzovat je a hledat v nich, co je potřeba. Log management bude podrobněji rozebrán v kapitole 2.2.1 jakožto součást SIEM.

1.2.2 SIEM

SIEM nástroje staví na log managementu. Základem je sběr, ukládání a prohledávání logů získaných z různých zařízení v síti a systému, SIEM navíc shromážděné logy doplňuje kontextovými informacemi a metadaty, díky kterým se dají odhalit komplexnější bezpečnostní hrozby a podezřelé aktivity. Další nadstavbou na rozdíl od log managementu je automatické upozorňování na nalezenou hrozbu a kategorizace podle její kritičnosti.

Ještě na úrovni log managementu se logy vyfiltrují a ponechají se jen ty, které jsou podle určitých kritérií vyhodnocené jako relevantní. Vyfiltrované logy následně prochází hlubší analýzou a korelací pomocí předem nadefinovaných pravidel. V případě, že nějaký log (nebo více logů) těmto pravidlům odpovídá, je možné, že se jedná o bezpečnostní hrozbu. Identifikovanou hrozbu je možné označit dle její závažnosti a následně o ní může být různými způsoby informován příslušný technik, který se jí bude dále zabývat. [7]

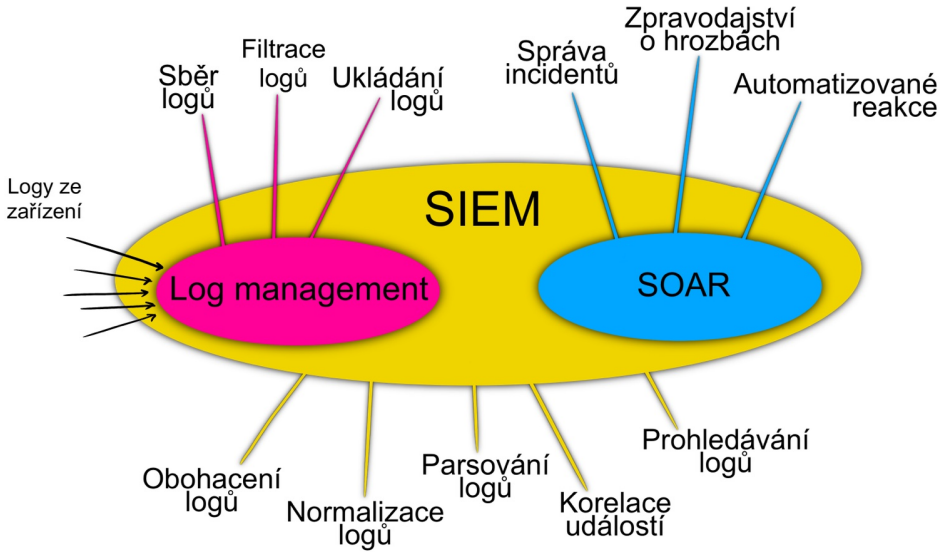
1.2.3 SOAR

Zatímco SIEM získává a koreluje logy ze zařízení ve vnitřní síti, SOAR získává informace o nejnovějších hrozbách z externích zdrojů jakými jsou zpravodajství o bezpečnostních hrozbách nebo informační zdroje třetích stran. Tím se vytváří nadhled nad vnitřní a vnější sítí a jejich bezpečností. Jedním z cílů tohoto řešení je automatická reakce na bezpečnostní události bez nutnosti zásahu nebo s minimálním zásahem IT technika, a tím zvýšení efektivity bezpečnostního systému.

Jak již vyplývá ze zkratky, SOAR zajišťuje tři funkce:

- **Orchestration** - SOAR umožňuje propojení bezpečnostních nástrojů a systémů tak, aby byla správa centralizovaná a SOC (*Security Operations Center*) získalo nadhled nad všemi komponentami a mohlo jednodušeji provádět jejich správu. [8]
- **Automation** - Možnost automatizace opakujících se činností.
- **Response** - SOAR nástroje ulehčují bezpečnostním technikům práci. Činí tak pomocí pravidel, po jejichž splnění se automaticky provede nastavená reakce na probíhající útok nebo jinou bezpečnostní hrozbu. [8]

Nástroje SIEM a SOAR spolu mohou velmi úzce spolupracovat. SOAR v podstatě staví na nálezech vyhodnocených ze SIEM nástrojů a provádí automatickou reakci, aby se co nejdříve zabránilo bezpečnostní hrozbě a eliminovaly se případné následky. SOAR je většinou již součástí SIEM nástrojů. Další kapitoly popisují zejména SIEM nástroje.



Obrázek 1.1 Log management, SIEM, SOAR a jejich hlavní funkce

Kapitola 2

Správa bezpečnostních informací a událostí

SIEM (správa bezpečnostních informací a událostí) je technologie, která umožňuje detekci hrozeb, dodržování pravidel a správu bezpečnostních incidentů prostřednictvím shromažďování a analýzy bezpečnostních a dalších typů událostí a utváření kontextu. Mezi základní funkcionality patří shromažďování a management logů z široké škály zdrojů, schopnost analyzovat tyto záznamy událostí a správa a reportování nalezených bezpečnostních incidentů. [9]

SIEM nástroj (nástroj pro správu bezpečnostních informací a událostí) je software umožňující shromažďování bezpečnostních dat z jednotlivých částí počítačových systémů a sítí, zobrazení těchto dat a možnost jejich dalšího využití prostřednictvím jediného rozhraní. [10]

2.1 Zdroje záznamů o událostech

V dnešní době využívá každá organizace nějaký počítačový systém a síť, do které je připojené velké množství zařízení. Mnoho organizací má i více geografických lokací, ať už v rámci jednoho města, státu nebo i po celém světě. Čím je daná organizace rozsáhlejší, má více různých typů zařízení ve firemní síti, využívá více systémů a má více zaměstnanců, kteří mají přístup k částem sítě a systémů, tím je náchylnější na kybernetické útoky, zejména při přeposílání dat a přístupu k citlivým informacím. Proto je potřeba sbírat záznamy o událostech z co nejvíce zdrojů, aby se co nejdříve detekovalo podezřelé chování a zabránilo se případným útokům. Také se musí brát v potaz užitečnost záznamů a zda nemohly být pozměněny (například záznamy ze zdrojů které nejsou dostatečně zabezpečené nebo které byly dokonce úspěšně napadené).

Zdroji záznamů o bezpečnostních událostech jsou nejčastěji:

- **Síťová zařízení**
  - **Routery** - Routery generují logy obsahující informace o zdrojích a cílech komunikace, objemu přenášených dat, použití protokolů atd. Mohou být nastaveny tak, aby byl určitý typ síťového provozu blokován. O síťové komunikaci procházející tímto routerem vytváří záznamy obsahující základní informace. [6]
  - **Load balancery** - Load balancer je softwarové nebo hardwarové zařízení, které slouží k rozdělení příchozích požadavků mezi další síťové prvky tak, aby byly rovnoměrně zatížené. Díky tomu nedojde k přetížení serverů, čímž by pak došlo ke zpomalení odpovědí nebo výpadkům.

Logy z těchto zařízení obsahují informace o provozu na síti a odpovědích serverů, jako například IP (*Internet Protocol*) adresa klienta, latence nebo kam byl požadavek přeposlán. Z logů se dají získat vzorce síťového provozu, které mohou sloužit k volbě efektivnějšího způsobu balancingu nebo například indikaci DDoS (*Distributed Denial of Service*) útoku.

- **Koncová zařízení** - Mezi koncová zařízení patří počítače, notebooky, mobilní telefony, tiskárny atd. Zaznamenávají historii používání, připojování na síť, odeslané a přijaté požadavky a odpovědi, instalovaný software, chybová hlášení apod.
- **IoT** (*Internet of Things*) - IoT je síť fyzických zařízení, která obsahují vestavěnou technologii pro komunikaci a snímání nebo interakci s jejich vnitřními stavy nebo vnějším prostředím. [9] Tato zařízení jsou vybavena senzory, procesory a softwarem, což umožňuje sběr logů a jejich odeslání. Mají většinou velmi omezenou velikost úložiště a paměti, tudíž nemohou ukládat velké množství logů a musí je hned odesílat nástroji pro centralizovanou správu logů, který je zpracuje a uloží do databáze. Logy z IoT zařízení obsahují informace o jednotlivých komponentách daných zařízení (například statusy mikrokontrolerů nebo průtok dat). [11]
- **Servery**
  - **Autentizační servery** - Vytváří záznamy o každém pokusu o autentizaci, kdy a odkud se uživatel přihlašuje, jeho uživatelské jméno a zda proběhlo přihlášení úspěšně nebo ne. [6]
  - **Proxy servery** - Proxy servery hrají důležitou roli v zajištění soukromí a regulaci přístupů. Veškerá komunikace s vnější sítí jde přes proxy server, tudíž proxy server může vytvářet záznamy a statistiky o využití a chování. Sleduje požadavky od uživatele společně s využívanou aplikací nebo službou. Pomocí analýzy tohoto chování se dá identifikovat například únik dat nebo díky monitorování délky procházejících paketů a jejich opakovanému odesílání/přijímání se dá například odhalit malware. Důležitými atributy záznamů z proxy serveru jsou datum a čas, klientova IP adresa a port, verze HTTP (*Hypertext Transfer Protocol*) protokolu, HTTP dotaz, typ obsahu, user agent, jméno uživatele, který je přihlášen ke klientu a jak s dotazem proxy server naložil. [11]
  - **DNS servery** - DNS (*Domain Name System*) je databáze, která slouží k překladu IP adresy cílového serveru na doménový název prostřednictvím DNS protokolu z DNS serveru. [12] Záznamy poskytují detailní informace o datech, která DNS server přijal a odeslal, a pomáhají tak získat informace o útočníkovi na DNS server. Díky záznamům z DNS serverů se například dají dohledat přístupy ke škodlivým webovým stránkám, a tím i kompromitovaná zařízení.
  - **Databázové servery** - Databázové servery jsou atraktivním cílem pro útočníky, protože často obsahují citlivé údaje o zaměstnancích, zákaznících organizace nebo o organizaci samotné. Ztráta, pozměnění nebo zveřejnění takových dat může způsobit velké škody a ohrozit chod organizace i její zákazníky.

    Záznamy obsahují zejména přístupy k citlivým datům společně s ID uživatele, jeho IP adresou a dotazem, který na server poslal. Kromě přístupů by se mělo zaznamenávat kopírování, změna a mazání databází, tabulek a aktivit privilegovaných uživatelů. Dále je dobré vytvářet záznamy o podezřelých aktivitách, například několik neúspěšných pokusů o přihlášení, neúspěšné dotazy na databázi nebo eskalace uživatelských práv.
- **Bezpečnostní systémy**
  - **Antivirový software** - Antivirový software je nejpoužívanější ochranou proti malware a počítačovým virům. Využívá databázi známých virů a pomocí prohledávání souborů na disku a porovnávání jejich obsahu se sekvencemi kódů známých virů z databáze identifikuje viry. Antivirus také detekuje podezřelý provoz na síti nebo chování programů pomocí zachytávání komunikace a sledování jejich aktivity. [6]

- **IDS a IPS** - (*Intrusion Detection System* a *Intrusion Prevention System*) systémy pro detekci (IDS) a prevenci (IPS) průniku. IDS pasivně sleduje provoz na síti, a pokud detekuje podezřelou aktivitu, vytvoří upozornění a vygeneruje záznam o tomto incidentu. IPS aktivně zabraňuje právě probíhajícím škodlivým aktivitám, které byly detekovány. [6]
- **Software pro vzdálený přístup** - Nejčastější možností pro vzdálený zabezpečený přístup k interním systémům organizace je VPN (*Virtual Private Network*). Po přihlášení k VPN serveru se data na klientu zašifrují a odešlou se vytvořeným tunelem na VPN server, který je dešifruje a přepošle na cílový server. Odpověď od cílového serveru se pošle firemnímu VPN serveru, ten ji zašifruje a přepošle zpět VPN klientovi, který si odpověď dešifruje.

  Cílem komunikace prostřednictvím VPN je, aby nikdo, ani ISP (*Internet Service Provider*, poskytovatel internetového připojení) neměl možnost zjistit, s kým klient komunikuje a cílový server neznal identitu klienta - ISP i cílový server znají jen adresu VPN serveru. Šifrováním komunikace mezi klientem a VPN serverem se zabrání čtení obsahu zpráv.

  VPN systémy vytváří záznamy o úspěšných i neúspěšných pokusech o přihlášení a o množství dat, která uživatel při daném přihlášení poslal a přijal. [6]
- **Software pro zjišťování zranitelností** - Tento typ softwaru vytváří záznamy o instalaci bezpečnostních záplat systému a zároveň pravidelně generuje záznamy o chybějících aktualizacích softwaru a možných zranitelnostech, které detekuje skenováním systému. [6]
- **Firewall** - Firewall je software nebo fyzické zařízení, které má kontrolu nad síťovým provozem a pomocí definovaných pravidel povoluje nebo zabraňuje komunikaci po síti. Zaznamenává se, jak firewall naložil s provozem na síti, zdrojovou a cílovou IP adresu, číslo portu a jaký protokol se využívá atd.

  Existuje několik typů firewallů, nejpoužívanějšími jsou WAF (*Web Application Firewall*) a NF (*Network Firewall*). WAF pracuje na 7., aplikační, vrstvě OSI (*Open Systems Interconnection*) modelu. Filtruje HTTP komunikaci mezi webovou aplikací a Internetem, a chrání tak před útoky jako SQL (*Structured Query Language*) injection nebo cross-site scripting. [13] NF pracuje na 3., síťové, vrstvě OSI modelu. Filtruje komunikaci na základě posouzení síťových protokolů, IP adres a portů odesílatele a příjemce procházejících paketů.

  Záznamy z firewallu jsou pro analýzu velmi důležité, protože obsahují záznamy o většině síťového provozu z a do vnitřních sítí. Pomocí těchto záznamů se dá detekovat například zero-day útok, na který v tu chvíli ještě není antivirový software připravený. Na záznamech z firewallu se může projevit jako velké množství zamítnutých nebo povolených pokusů o připojení s podezřelým hostem z vnější sítě.

  Windows firewall zaznamenává datum a čas připojení, IP adresy, port využívaný na zařízení ve vnitřní síti, protokol (TCP (*Transmission Control Protocol*)/UDP (*User Datagram Protocol*) a jestli byl paket zahozen nebo propuštěn. Dává tak možnost detekovat podezřelou aktivitu.

- **Aplikace** (software využívaný na jakémkoliv zařízení připojeném do firemní sítě) - Organizace využívají mnoho různých aplikací jako jsou webové aplikace, databáze, nástroje pro spolupráci apod., které jsou většinou nezbytné pro fungování celé firmy. Většina takových aplikací generuje záznamy o tom, co se v aplikaci děje. [6]
  - **Komunikace mezi serverem a klientem** - Zaznamenávání dotazů (například od klienta na databázový server) a odpovědí. Pomocí takových logů je možné detekovat neoprávněnou manipulaci a přístup k datům (souborům, složkám, …), ale také se tím dají zjistit a lépe vyřešit problémy s databází, webovým serverem apod. [6]

  - **Informace o uživatelích** - Záznamy o úspěšných i neúspěšných pokusech o přihlášení, využití oprávnění a změnách v nastavení účtu (například změna hesla, vytvoření/smazání účtu, změna přidělených oprávnění). Sběr těchto informací se dá využít například k identifikaci pokusu o prolomení přihlašovacích údajů pomocí brute force útoku, elevace oprávnění nebo také pro vedení záznamů, kdo ve kterou chvíli využíval danou aplikaci. [6]
  - **Informace o využití prostředků** - Počet transakcí za nějaký časový úsek (vteřina, hodina, ...) a jejich velikost (např. velikost emailů, přenášených souborů). Výrazná změna oproti průměrným hodnotám může indikovat malware nebo únik informací. [6]
  - **Významné události** - Mezi významné události patří spuštění/vypnutí aplikace, errory způsobující pád aplikace, významné změny v nastavení apod. [6]
- **Operační systémy** - Záznamy z operačních systémů (OS, *Operation System*) jsou velmi užitečné pro zkoumání podezřelých aktivit. Poté, co některý bezpečnostní systém detekuje podezřelou aktivitu, využijí se záznamy od OS ke zjištění podrobností - například který uživatel je v tu chvíli přihlášen, které služby jsou spuštěné apod.
  - **Systémové události** - Operační systém zaznamenává operace, které provádí. Většinou zaznamenává všechny nepovedené operace a z povedených jen některé nejvýznamnější, jako například vypnutí/zapnutí systému a služeb, zda se správně načetly drivery apod. Obsah těchto záznamů se liší podle typu OS, obvykle obsahují datum a čas, typ události, zda proběhla úspěšně, případně chybové kódy a hlášení. Některé operační systémy ani nedovolují administrátorům nastavit, které operace a jaké informace o nich se budou zaznamenávat. [6]
  - **Auditní záznamy** - Záznamy o úspěšných i neúspěšných pokusech o přihlášení uživatele, kdy uživatel přistupoval ke kterému souboru, záznamy o smazání souborů, změny v uživatelských účtech, v nastavení práv včetně jejich využívání. Administrátor systému může většinou nastavit, které události se budou zaznamenávat. [6]
- **Cloudové služby** - Cloudové služby generují velké množství různých typů záznamů. Takovými záznamy mohou být využití prostředků, přístupy jednotlivých uživatelů, podrobnější zaznamenávání činností administrátorských účtů apod. Větší poskytovatelé cloudových služeb jako například Microsoft Azure, AWS (*Amazon Web Services*) nebo Google Cloud proto nabízí možnost log managementu, většinou i s možností nastavení upozornění na závažná chybová hlášení.

2.2 Funkce SIEM

Jak již bylo řečeno v kapitole 1.2.2, základním stavebním kamenem SIEM nástrojů je správa logů neboli log management. Shromážděné logy prochází filtrací a normalizací, aby se daly následně analyzovat a korelovat. To probíhá většinou pomocí pravidel, kterými se v lozích detekují bezpečnostní hrozby. Nálezy se následně reportují na dashboard nebo nastavenou notifikací. Z nálezů získanými SIEM nástroji následně čerpají SOAR nástroje, kterými je možné učinit jednodušší automatickou reakci k eliminaci hrozby a jejích následků. Funkce SIEM se tedy dají rozdělit na následující 3 složky:

- log management,
- analýza a korelace událostí,
- reportování nálezů a reakce.

2.2.1 Log management

Množství a rozdílnost logů se stále zvyšuje a díky zavedení log managementu se jejich správa zpřehlední a je snazší se v takovém množství orientovat. Log management je proces vytváření a shromažďování záznamů o událostech z různých relevantních zdrojů (2.1) ve firemní síti, jejich ukládání do databáze a normalizace, díky které se dají analyzovat a korelovat. Pomáhá zajistit, aby byly záznamy relevantně detailní a byly uložené a dostupné po přiměřenou dobu. Tu mají některé organizace stanovenou ve Vyhlášce [2]. Provozovatelé informačních a komunikačních systémů kritické informační infrastruktury a poskytovatelé základních služeb musí záznamy uchovávat alespoň 18 měsíců od jejich vytvoření. Pro provozovatele významných systémů platí pouze 12měsíční lhůta. [2]

Logy mohou obsahovat mnoho různých informací o událostech v systému a síti. Přesný obsah a formát záleží na zdroji, kterým je log vytvořen. Dle Vyhlášky (1.1.2) mají logy obsahovat tyto atributy:

- datum a čas, kdy se činnost stala (včetně časového pásma),
- typ události činnosti,
- identifikátor zařízení nebo služby, která událost činnost zaznamenala,
- uživatelský účet, pod kterým se událost činnost stala,
- síťový identifikátor (IP adresa, MAC adresa) zařízení, které událost vyvolalo,
- zda proběhla činnost úspěšně nebo neúspěšně. [2]

Tyto atributy poskytují základní informace o dané události, které je pro přesnější identifikaci typu hrozby, jejího původce a případných škod potřeba doplnit logy z dalších zdrojů a podrobnějšími záznamy.

Vyhláška (1.1.2) také určuje typy událostí, které je nezbytné zaznamenávat:

- přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
- činnosti provedené pod administrátorským účtem,
- úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
- neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
- činnosti uživatelů, které mohou mít vliv na bezpečnosti informačního a komunikačního systému,
- zapnutí a vypnutí zařízení, systému, služby,
- kritická a chybová hlášení,
- přístupy a pokusy o manipulaci se záznamy o událostech, změny v nastavené nástrojů pro zaznamenávání událostí. [2]

Pro správnou funkci log managementu a detekci bezpečnostních incidentů je potřeba neustále získávat záznamy o událostech ze všech dostupných a relevantních zdrojů, které musí mít synchronizovaný čas. Synchronizace času musí proběhnout minimálně jednou za 24 hodin. [2] Většina zdrojů záznamů o událostech běží nepřetržitě, tím pádem jsou logy generovány po celou dobu běhu. Některé zdroje běží ale jen jednou za čas nebo periodicky, a tudíž generují logy v dávkách a intervalech. Tento fakt je potřeba zohlednit při analýze a tvorbě detekčních pravidel. [10]

2.2.1.1 Shromažďování logů

SIEM nástroje většinou zahrnují jeden nebo více serverů provádějících analýzu logů, jeden nebo více databázových serverů a jak již bylo zmíněno, mnoho zařízení, která generují logy. Shromažďování logů zahrnuje samotný sběr logů ze zdrojových zařízení, jejich doručení na server, zpracování a uložení do databáze.

V rámci tohoto procesu je tedy potřeba určit, jak se budou data přenášet na centrální server (jaké protokoly se využijí), zajistit důvěrnost, integritu a dostupnost (zda budou data při přenosu šifrovaná, využije se pro jejich přenos speciální kanál apod.) a nastavit, jak často se budou přenášet, aby nedošlo k zahlcení nebo aby naopak kvůli zastaralým logům nedošlo k nedostatečně včasnému zásahu proti bezpečnostní hrozbě.

Pro získávání logů ze zařízení existují podle publikace organizace NIST (*National Institute of Standards and Technology*) [6] dvě metody:

1. **Agentless metoda** - Sběr logů bez nutnosti instalace a konfigurace dalšího software na každém zdrojovém zařízení. NIST [6] dále rozděluje tuto metodu na dva možné způsoby průběhu:

   a. **Push metoda** - Koncová zařízení proaktivně posílají logy SIEM serveru, tudíž se server nemusí u každého zařízení autentizovat a přenos je jednodušší. Z toho ale plyne i nevýhoda, protože tím, že se server nepřipojuje ke koncovému zařízení, nemůže ověřit správnost dat.

   b. **Pull metoda** - SIEM server iniciuje přenos dat. K tomu je potřeba, aby měl přístupové údaje ke každému zařízení a při každém přenosu se autentizoval. Tento přístup je časově náročnější, tudíž se hodí pro přenos logů po větších dávkách jednou za časový úsek.

   Agentless metoda je vhodná pro zařízení s proprietárním operačním systémem, který nedovoluje instalaci agenta. V případě této metody provádí veškerou filtraci, shromažďování a normalizaci logů SIEM server.

2. **Agent-based metoda** - Tato metoda vyžaduje instalaci softwaru na zařízení generující logy. Tento program provádí i základní filtraci a normalizaci určitých typů logů a pravidelně je odesílá SIEM serveru, kde se provádí jejich analýza a uložení do databáze. Díky tomu, že filtrace logů probíhá již na zdrojových zařízeních, přenáší se méně dat na SIEM server, což vede k menšímu zatížení sítě při přenosu a serveru při zpracovávání logů. Zároveň se mohou logy dočasně uložit v agentu, pokud nastane výpadek spojení se SIEM serverem.

2.2.1.2 Ukládání logů

Nejjednodušším řešením pro ukládání logů je ukládání na jeden server, který obsahuje všechny logy a zároveň provádí jejich analýzu. Toto řešení je ale vhodné pouze pro menší organizace. Pro větší organizace, které se musí vypořádat s větším množstvím dat, je vhodné využít kombinaci více serverů. Dle publikace NIST [6] se zde nabízí několik možností:

1. Každý ze serverů má jednu nebo více specializovaných funkcí, jako například analýzu, krátkodobé nebo dlouhodobé úložiště apod.

2. Zapojení serverů pro ukládání dat tak, aby byla data uložena redundantně. To umožní přepnutí na záložní server při výpadku primárního serveru bez ztráty (nebo s minimální ztrátou) dat.

3. Zapojení serverů do více vrstev. To znamená, že servery z první vrstvy přijímají logy z generátorů logů a přeposílají je serveru z další vrstvy buďto tak, jak je získaly z generátorů nebo již vyfiltrované nebo i normalizované. Díky tomuto typu zapojení jsou servery v druhé a vyšší

vrstvě chráněné před přímými útoky. Toto řešení je vhodné pro organizace, kde je méně spolehlivá síť mezi první a druhou vrstvou. Generátory předají logy serveru první vrstvy a ten je přepošle do druhé vrstvy, až to bude síť umožňovat.

Mezi těmito možnostmi ukládání se organizace musí rozhodnout podle vlastních možností a potřeb - zda je potřeba vytvářet zálohy a zda se logy přenáší pouze po zabezpečené a spolehlivé lokální síti. Dalším důležitým kritériem při výběru řešení je doba, po kterou musí být logy uložené a dostupné. Pro některé organizace vyplývá tato doba z Vyhlášky (uvedeno výše), ostatní organizace by se měly touto dobou inspirovat, ale mohou si ji nastavit dle vlastního uvážení.

2.2.1.3 Filtrace logů

Tím, že se logy sbírají z co nejvíce zařízení, může jich být opravdu mnoho. Proto je potřeba je filtrovat, aby se následně analyzovaly a ukládaly jen ty, které obsahují nějaké přínosné a „zajímavé“ informace. Jak již bylo uvedeno v rámci kapitoly o shromažďování logů (2.2.1.1), tato filtrace může probíhat na agentu, tzn. před odesláním záznamů serveru, nebo až na SIEM serveru.

2.2.1.4 Normalizace logů

Kromě shromažďování, ukládání a filtrace logů plní log management další důležitou funkci - normalizaci logů. Protože ze zařízení přichází logy ve své původní formě, je normalizace logů nezbytná pro jejich následnou analýzu a korelaci. Logy přichází často v různých typech souborů a formátech obsahu a v rámci normalizace se záznamy o událostech převedou do jednoho formátu a slovníku, který je srozumitelný danému SIEM nástroji, a ten je pak může analyzovat a vizualizovat. Častými problémy při normalizaci logů jsou:

- **Nekonzistentní čas** - I přes synchronizaci času, která má podle legislativy probíhat alespoň jednou za 24 hodin [2] se může stát, že budou v záznamech ze dvou různých zařízení uvedené určité časové údaje, i když byla souslednost událostí ve skutečnosti jiná (o několik vteřin i minut). [6]
- **Různé atributy obsahu** - Zdroje záznamů zaznamenávají nejdůležitější informace o dané události. Každý zdroj ale může za důležité považovat jiné atributy a některé zdroje ani nedovolují nastavit, které informace se budou zaznamenávat. To může ústit v situaci, kdy jeden zdroj generuje záznamy například s ID uživatelského účtu a jiný pouze s IP adresou jakožto identifikátorem zdroje události. V některých případech je nemožné nebo velmi obtížné propojit takové dva záznamy do jedné události.

  Rozdílnosti mohou být i v rámci jednoho atributu. Například když jeden firewall po zahození packetu vygeneruje log s informací „drop“ a jiný firewall nazve tuto událost jako „deny“. Toto se dá řešit nastavením samotného zařízení, pokud to umožňuje, nebo vhodnou normalizací logů.
- **Různé formáty obsahu** - Obsah logů se může lišit nejen ve sledovaných atributech, ale také ve formě jejich zápisu. Existuje mnoho typů souborů pro záznam událostí. Jedním z nejčastějších je formát JSON (*JavaScript Object Notation*), který obsahuje páry klíč-hodnota a je dobře čitelný pro člověka. To samé platí pro formát Windows Event Logs, který bývá oproti formátu JSON podrobnější a týká se pouze záznamů, které vzniknou v operačním systému Windows. Dalším využívaným typem je CLF (*Common Log Format*), který je jedním z nejstarších typů. Na rozdíl od dříve zmíněných formátů neobsahuje záznamy typu klíč-hodnota a celý záznam je v jednom řádku a bez názvů atributů. Formát ELF (*Extended Log format*) je odvozený z CLF a liší se v tom, že je detailnější a ke každé hodnotě je uveden i název atributu.

  Kromě odlišností v podobě formátu celého souboru a zvolených oddělovačích atributů se mohou lišit i samotné zápisy atributů. Častým příkladem je formát data, kdy jeden zdroj může

uvádět datum ve formátu MM-DD-YYYY a druhý například DD/MM/YY. [6]

Tento typ problému se dá řešit vhodně nastaveným parsováním záznamů.

Kvůli rozdílům v záznamech z různých zdrojů je potřeba zavést automatizovaný proces, kterým se záznamy převedou do jednotného formátu s jednotnými datovými typy atributů. Díky tomu se dají události lépe analyzovat a zároveň je pro člověka jednodušší záznamům porozumět a hledat v nich souvislosti.

Parsery jsou softwarové komponenty, které dokáží rozpoznat typ logu na základě struktury dat a pomocí předdefinovaných pravidel z nich extrahují důležité atributy a jejich hodnoty. U nestandardních typů logů je potřeba, aby uživatel nadefinoval pravidla pro parsování pomocí regulárních výrazů nebo v rámci grafického rozhraní, pokud to nástroj nabízí. [14]

Normalizovaným logům je potřeba přiřadit kategorie, aby bylo jasné, čeho se týkají. Takovými kategoriemi může být autentizace, vzdálené operace, systémové události apod. Další možností, jak zpřehlednit logy a dát jim větší význam je jejich obohacení. Obohacením logů je myšleno přiřazení nějaké extra informace nebo významu nějakému atributu, jako například určení, že jde o administrátorský účet, že se jedná o interní IP adresu, do jaké skupiny tato adresa patří atd.

2.2.2 Analýza a korelace událostí

Tato část je jádrem celého procesu hledání hrozeb. K identifikaci hrozeb a vytvoření upozornění na podezřelé chování využívá SIEM detekční pravidla. Může se jednat o vyhledávání konkrétního záznamu nebo hodnoty, korelaci dat získaných ze zdrojů detekci atypického chování pomocí strojového učení.

2.2.2.1 Jednoduchá pravidla

Jednoduché SIEM detekční pravidlo vyhledává konkrétní typ záznamu (například pomocí Windows Event ID) nebo hodnotu určitých atributů. Může detekovat například překročení nastavené prahové hodnoty určitého atributu záznamu, vypnutí nebo zapnutí určité služby, komunikaci s určitou IP adresou. Také bývá užitečné pro upozornění na kritické chybové hlášení, které může být ihned zasláno elektronickou poštou nebo jiným zvoleným způsobem.

2.2.2.2 Korelace událostí

Hledání vztahů mezi dvěma a více záznamy se nazývá korelace událostí. Korelace probíhá pomocí předem nadefinovaných korelačních pravidel, což jsou logické výrazy, jejichž splnění vyvolá varování nebo spustí automatickou reakci. Tato pravidla specifikují sled událostí, který je považován za podezřelé chování a může znamenat bezpečnostní hrozbu v podobě zranitelnosti nebo právě probíhajícího bezpečnostního incidentu. Jsou postavena na známých vzorcích útoků a zranitelností. Když je korelace úspěšná, tzn. spojení několika záznamů odpovídá nějakému pravidlu, vytvoří se většinou nový log spojující důležité informace do jednoho záznamu.

2.2.2.3 UEBA

Technologii UEBA (*User and Entity Behavior Analytics*) využívají pokročilejší SIEM nástroje. Jedná se o výsledek strojového učení, které podle vzorců chování uživatelů pomáhá určit vhodné nastavení prahových hodnot v korelačních pravidlech a zdrojích logů a zároveň identifikuje podezřelé chování, které neodpovídá naučeným vzorcům. Tato technologie pomáhá detekovat hrozby, které nejsou známé nebo je pro ně obtížné nadefinovat korelační pravidla. Mezi takové hrozby patří například útoky z vnitřní sítě vyvolané některým ze zaměstnaneckých účtů nebo útoky, které probíhají delší časový úsek a tím pádem jsou těžko detekovatelné. [15]

2.2.3 Reportování nálezů a reakce

Kromě detekce je potřeba na nálezy reagovat. SIEM reportuje nalezené hrozby a podezřelé chování pomocí upozornění, které následně zpracuje zaměstnanec SOC a předá je k řešení příslušným IT specialistům.

Reportované incidenty mohou mít různou závažnost, podle které se například vytvoří záznam v incident managementu, zobrazí se výstraha na dashboard SOC nebo se například pošle upozornění pomocí elektronické komunikace.

Závažnost se vyjadřuje pomocí funkce pro hodnocení rizik, do kterého je zapojena úroveň hrozby, dopadu a zranitelnosti. Ve Vyhlášce (1.1.2) jsou navržené stupnice pro hodnocení závažnosti hrozeb, zranitelností a rizik, ale je na každé organizaci, aby si jednotlivé stupnice a funkci pro hodnocení celkového rizika upravila dle svých potřeb.

Identifikované bezpečnostní incidenty je potřeba ohodnotit dle jejich závažnosti a významnosti a podle toho se zavede strategie pro jejich řešení. Pro vyhodnocení kritičnosti je dobré zohlednit počet dotčených osob, způsobené škody, důležitost dotčených aktiv informačního a komunikačního systému, dopady na služby poskytované jinými systémy, délku trvání incidentu, zeměpisný rozsah incidentu a další dopady. [2]

Vyhláška [2] definuje tři kategorie bezpečnostních incidentů:

1. **Méně významný kybernetický bezpečnostní incident**, při kterém dochází k méně závažnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

2. **Významný kybernetický bezpečnostní incident**, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

3. **Velmi významný kybernetický bezpečnostní incident**, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.

Důležitou součástí současných SIEM nástrojů je také automatická reakce na závažné incidenty. V takových případech provede nástroj předem určená opatření k zabránění právě probíhajícímu kybernetickému útoku a minimalizaci jeho dopadů na počítačový systém a celou organizaci.

Takovým opatřením může být zablokování IP adresy útočníka nebo jinak nebezpečné IP adresy nebo zamezení přístupu uživateli s podezřelým chováním (například poté, co se pokusil několikrát neúspěšně přihlásit a po mnoha pokusech se přihlásil úspěšně).

K automatickým reakcím a managementu řešení reportovaných incidentů se využívají SOAR nástroje, které jsou už většinou integrované v současných SIEM nástrojích. Vyžívají detekcí ze SIEM nástrojů a udělají další krok v řešení incidentů, a to právě onu automatickou reakci.

Kapitola 3
SIEM nástroje

3.1 Analýza trhu SIEM nástrojů

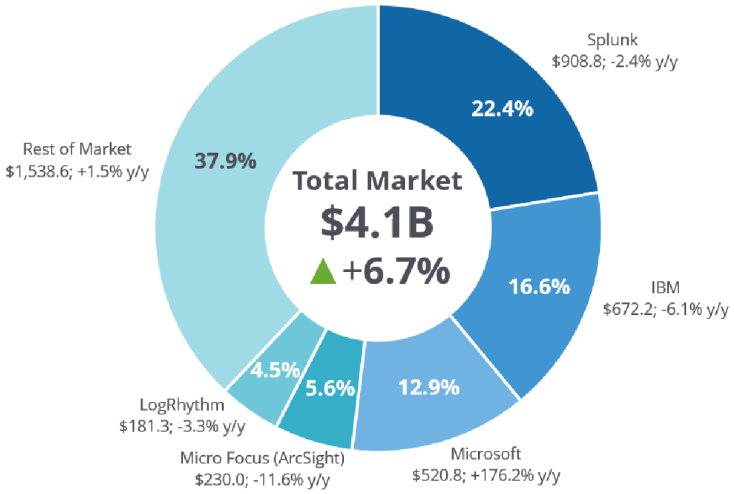
V dnešní době je výběr SIEM nástrojů opravdu velký a nové nástroje stále přibývají. Je tu ale několik velkých hráčů, kteří už mnoho let nabízí stabilní a spolehlivé bezpečnostní řešení. Každý zdroj uvádí trochu jiné poměry jejich zastoupení na trhu a jiný celkový objem trhu se SIEM nástroji, ale v největších reprezentantech na trhu se shodují.

Firma Splunk se svým řešením Splunk Enterprise Security má největší podíl na trhu se SIEM nástroji, a stále rozšiřuje své působení. Dále velmi známý QRadar SIEM od firmy IBM a v posledních letech přibližně stejným podílem zastoupený Microsoft, který v rámci Microsoft Azure nabízí nástroj Sentiel. Mezi lety 2020 a 2021 získala značný, stále rostoucí tržní podíl i firma Elastic s opensource nástroji v rámci Elastic Stack a relativně novým produktem Elastic SIEM (z roku 2019 [16]). [17, 18]

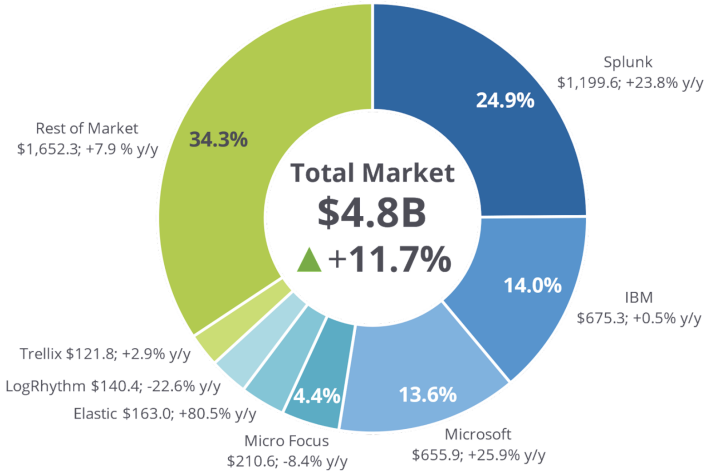
Jak je vidět na grafech od firmy Gartner (3.1, 3.2), objem trhu SIEM nástrojů mezi roky 2020 a 2021 značně vzrostl a přibylo několik firem, jejichž podíl tvoří značnou část na trhu. I v roce 2022 se objevili další významní hráči na trhu. Často zmiňovanými jsou například Fortinet, SolarWinds nebo McAfee, který se začátkem roku 2022 spojil s firmou FireEye a nově je známe pod jménem Trellix. [19]

Objem trhu SIEM nástrojů se v roce 2022 pohyboval kolem 5,1 miliard USD a předpokládá se, že i nadále poroste velmi rychle. Podle odhadů firmy IMARC Group by měl do roku 2028 vzrůst až na 8,5 miliard USD. [20]

I podle údajů z výzkumů od společnosti Forrester (srovnání Forrester Wave: Security Analytics Platforms z let 2020 a 2022) přibylo mnoho dalších hráčů na trhu nástrojů analyzujících bezpečnost a některé se naopak stáhly do ústraní. Tento výzkum neanalyzuje čistě SIEM nástroje, jako například výše uvedené srovnání od firmy Gartner, nýbrž i nástroje úzce související se SIEM (jako SOAR nebo XDR (*Extended detection and response*)). Firmy IBM, Splunk, Securonix, Exabeam a Microsoft byly již v roce 2020 mezi lídry co se týče působnosti na trhu a zajímavosti jejich produktů. Nově se k nim v roce 2022 přidává Elastic, který ještě v roce 2020 neměl rozpoznatelný podíl a ve výzkumu ani nebyl uveden. [21, 22]



Obrázek 3.1 Podíl SIEM nástrojů na celosvětovém trhu v USD za rok 2020, Gartner [17]



Obrázek 3.2 Podíl SIEM nástrojů na celosvětovém trhu v USD za rok 2021, Gartner [18]

3.2 Kritéria pro výběr nástroje

Při výběru vhodného nástroje je dobré zvážit několik kritérií, která napomáhají k nalezení nástroje, který nejlépe odpovídá aktuálním i budoucím požadavkům dané organizace. Mezi taková kritéria patří:

- **Škálovatelnost** - Pro výběr nástroje je potřeba zvážit nejen aktuální požadavky, ale myslet i na budoucí růst firmy. Ideální SIEM nástroj by měl být připravený na zvyšující se požadavky na škálovatelnost nebo i změnu strategie firmy.
- **Korelační mechanismus** - Mnoho SIEM nástrojů nabízí předdefinovaná korelační pravidla, která se dají přímo nebo s nějakou úpravou využít a ušetří to mnoho času. Důležitá je rozmanitost korelačních funkcí, aby pokryly co nejvíce vektorů útoků. Všechny nástroje podporují korelační pravidla (bez toho by to nebyl SIEM nástroj), ale pouze některé umožňují korelaci ve více dimenzích a detekci hrozeb, které ještě nejsou známé. [23]
- **Dashboardy** - Dashboardy poskytují přehled nad všemi sledovanými prostředky a metrikami. Dashboardy by měly být přehledné a jednoduše přizpůsobitelné (pomocí widgetů, nastavení filtrů zobrazovaných informací apod.), měly by nabízet shrnutí pomocí grafů, tabulek a zároveň i možnost poskytnutí detailních informací.
- **Zpravodajství o hrozbách** - Zpravodajství poskytuje informace o nejnovějších hrozbách jako jsou nebezpečné IP adresy, škodlivé soubory, neošetřené zranitelnosti apod. Tyto aktuality jsou důležité, protože lze díky nim rychle přidat detekční pravidla, nainstalovat bezpečnostní záplaty nebo jinak zakročit a minimalizovat tím možnost případného útoku.
- **Reakce na incidenty** - Reakcemi jsou nadefinované akce, které provede nástroj jako reakci na detekovanou hrozbu nebo podezřelou aktivitu. Jedná se většinou o základní akce jako zablokování nebezpečné IP adresy, odepření přístupu uživateli apod. Probíhají ihned v reakci na analýzu v reálném čase, čímž se zabrání dopadům dříve, než by se k reakci dostal odpovědný technik. [23]

  Jedná se o funkci, kterou zajišťuje SOAR. V současných SIEM nástrojích je už většinou zakomponovaná a některé nástroje umožňují za tímto účelem propojení s nástroji třetích stran.
- **Strojové učení** - Pomocí strojového učení nástroj přizpůsobuje svá vyhodnocení a rozhodnutí na základě historických dat. Napomáhá efektivnějším rozhodnutím, nastavením správných hodnot v pravidlech a eliminováním tzv. false-positives. Existuje řada modelů strojového učení, proto je potřeba vybrat nástroj, který bude mít ten nejvhodnější pro potřeby dané firmy. [24]
- **Úložiště** - Jak již bylo zmíněno v předchozí kapitole (2.2.1.2), je nutné zvážit, zda bude mít každý ze serverů svou specifickou funkci (např. krátkodobé nebo dlouhodobé úložiště), zda budou zapojeny redundantně nebo ve vícero vrstvách. Dalším pohledem na způsoby ukládání dat je, zda se budou ukládat na lokální servery nebo do nějakého cloudového úložiště. SIEM nástroj by měl být vybrán podle podpory zvoleného způsobu ukládání a případně by měl umožňovat přechod do cloudu nebo naopak. Zároveň by měl umožňovat nastavit, jaká data se budou ukládat, jakým způsobem a také likvidaci dat, která nemusí být ukládána nebo archivována nebo kterým již vypršela lhůta, po kterou mají být, například podle Vyhlášky (1.1.2), uložena.
- **Cloud nebo on-premise** - Velmi důležitým kritériem při výběru SIEM nástroje je, zda bude celé řešení nasazeno v cloudu (známé také jako *SIEM as a Service*) nebo on-premise - přímo na fyzických zařízeních dané firmy. Obě možnosti mají svá pro i proti. Výhodou cloudového

řešení je rychlost nasazení, kdy může poskytovatel pomoci s počáteční konfigurací a nemusí se procházet celou zdlouhavou instalací na zařízení ve firmě. Další výhodou je menší omezení úložiště, celková přizpůsobitelnost a nižší náklady na nasazení.

Zatímco náklady na nasazení cloudového řešení jsou nízké, průběžné provozní náklady se časem nasčítají a celkově mohou rychle přesáhnout jednorázové výdaje za nasazení on-premise.

Přenos citlivých dat do/z cloudového úložiště ovšem může být rizikový. Riziko se dá sice snížit šifrováním nebo větší mírou autentizace, ale například pro firmy z kritické infrastruktury je vhodné on-premise řešení, protože riziko spojené s přenosem a ukládáním citlivých dat je příliš vysoké. Mezi nevýhody cloudového řešení také může patřit omezený přístup k surovým logům tak, jak přišly ze zdrojových zařízení. Některé SIEM nástroje toto neumožňují a místo toho poskytnou pouze reporty založené na těchto datech. Surové logy je ale potřeba ukládat pro forenzní analýzu a audity. [25, 26]

- **Opensource nebo komerční řešení** - Při vybírání nástroje je důležité zohlednit i ekonomický pohled. Opensource nástroje se dají stáhnout zdarma, není potřeba platit drahé licenční poplatky. Nemusí nabízet tolik funkcí jako komerční nástroje, ale dají se přizpůsobit specifickým požadavkům a potřebám firmy. Kolem známějších opensource nástrojů existují velké komunity uživatelů, kteří poskytnou podporu a pomoc při instalaci nebo řešení problémů.

  Využívání zpoplatněných nástrojů vyžaduje jednorázový nebo pravidelný, často nemalý, poplatek za licenci, který se ještě odvíjí od množství instalací nebo využívaných prostředků. Zato nabízí pokročilejší funkce, které většina opensource nástrojů nemá, například více způsobů reportování, pokročilejší analytické funkce nebo využití machine learningu apod. a navíc poskytují i zákaznickou podporu. Mohou ale vyžadovat zakoupení speciálního hardwaru nebo najmutí proškolených techniků pro správu a údržbu, což ještě více navyšuje náklady.

- **Nástroje třetích stran** - Možnost propojení SIEM nástroje s dalšími nástroji (například SOAR) i od jiných poskytovatelů je užitečná vlastnost, která umožní komplexnější bezpečnostní řešení a zjednoduší práci s vícero typy bezpečnostních nástrojů.

- **Kompatibilita logů** - Pro analýzu je potřeba shromažďovat logy z mnoha zařízení, tím pádem je nutné převést mnoho různých typů logů na jeden, který se dá poté analyzovat. K tomu slouží normalizace logů. Je dobré ověřit, zda je SIEM nástroj kompatibilní se všemi typy logů, které daná firma potřebuje a případně podporuje vytvoření vlastního parseru nebo přizpůsobení existujících. [27]

3.3 Nástroje rodiny Elastic Stack

Elastic Stack je opensource nástroj skládající se ze čtyř komponent, jejichž hlavním cílem je shromažďování dat jakéhokoliv typu a z jakéhokoliv zdroje a jejich analýza a vizualizace v reálném čase. Původně se skládal pouze ze tří komponent, od čehož bylo i odvozeno jméno ELK Stack - Elasticsearch, Logstash, Kibana. V roce 2015 byla vydaná nová komponenta Beats a nástroj se přejmenoval na Elastic Stack. Všechny komponenty se navzájem doplňují, ale i každá sama za sebe je efektivní a plní svou funkci, proto se nemusí nutně využívat všechny čtyři. [28]

3.3.1 Výhody nástrojů Elastic Stack

Elastic od začátku sází na transparentnost a možnost spolupráce v rámci Elastic komunity. Díky tomu, že Elastic poskytuje nástroje zdarma v opensource podobě, není nutné platit licenční poplatky, a navíc je možné si kód upravit tak, aby co nejlépe odpovídal potřebám každého a přispět vývoji nástrojů. [29]

Elastic řešení je známé také pro svou škálovatelnost. Nástroje je možné nasadit přímo na určená zařízení, v podobě kontejneru nebo do privátního či veřejného cloudu.

Nespornou výhodou nástrojů Elastic Stack a zejména Elasticsearch oproti jiným prohledávacím nástrojům je rychlost vyhledávání i ve velkém objemu dat. Toho je dosaženo zejména knihovnou, kterou Elasticsearch využívá. Jedná se o vyhledávací knihovnu Apache Lucene, která využívá invertovanou indexaci, což znamená, že se ke klíčovému slovu přiřadí ID souborů, ve kterých se slovo vyskytuje namísto přiřazování množiny klíčových slov k jednotlivým souborům jako je tomu v dopředné indexaci. Díky tomu se vyhledávaný výraz ihned asociuje se soubory, ve kterých se vyskytuje a není tedy potřeba procházet množinu výrazů přiřazenou ke každému ID souboru, zdali se tam náhodou nevyskytuje hledaný výraz. [30]

3.3.2 Elastic Stack komponenty

3.3.2.1 Logstash

Logstash je nástroj určený pro generování, sběr a zpracování logů ze všech možných zdrojových zařízení. Jedná se o různé typy dat i různé typy formátu jejich zápisu. Logstash tedy zároveň nabízí možnost parsování a normalizace dat do jednotného formátu, díky kterému lze data zpracovávat a analyzovat v dalších nástrojích. Pomocí knihovny, která nabízí různé filtry, může uživatel upravit, který typ atributů a části logů stojí za zmínku a mají se objevit v normalizovaných záznamech. Logstash navíc obohacuje logy o metadata ze zdrojových zařízení. [28]

3.3.2.2 Beats

Nástroj Beats slouží jako jednoduchý agent k doručení dat od zdrojů záznamů nástrojům Logstash nebo Elasticsearch. Obsahuje množství komponent specializovaných na určitý typ záznamů nebo zařízení:

- **Auditbeat** - sleduje systémové procesy a aktivitu uživatelů, komunikuje s linuxovým auditním frameworkem,
- **Filebeat** - přeposílá a centralizuje logy a soubory,
- **Functionbeat** - shromažďuje a přenáší záznamy z cloudových služeb,
- **Heartbeat** - monitoruje dostupnost aplikací a dobu jejich odezvy,
- **Metricbeat** - shromažďuje metriky a další údaje ze serverů a systémů,
- **Packetbeat** - umožňuje sledování provozu na síti a poskytuje přehled o výkonu aplikací, době odezvy a errorech,
- **Winlogbeat** - shromažďuje Windows event logy o spuštění nové služby, připojení nového úložiště a dalších bezpečnostních událostech. [30]

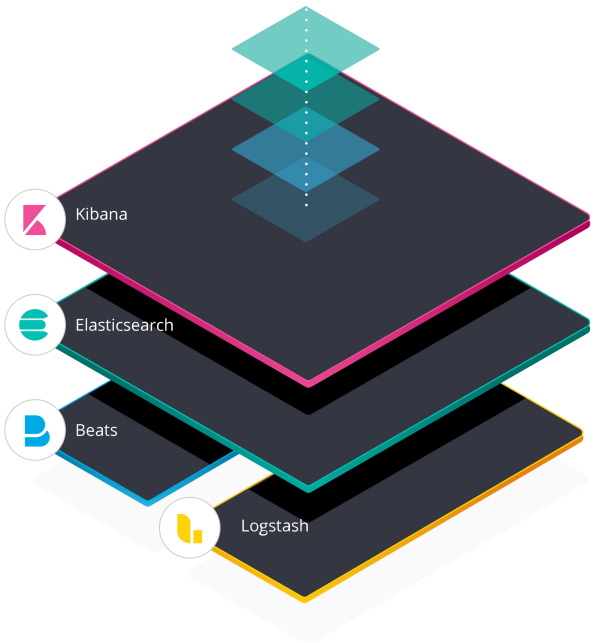
3.3.2.3 Elasticsearch

Elasticsearch je využívaný k prohledávání, indexaci a analýze dat. Komunikace s Elastic Search serverem probíhá prostřednictvím HTTP REST API a odpovědi jsou generovány ve formátu JSON. SQL databáze nejsou připravené na analýzu jakéhokoliv typu dat, tudíž Elasticsearch využívá NoSQL datové úložiště a díky tomu je schopen analyzovat strukturovaná i nestrukturovaná data. Je založen na knihovně Apache Lucene, což je velmi výkonný vyhledávač a poskytuje širokou škálu vyhledávacích možností. Kromě fulltextového vyhledávání se používá k analýze logů a zkoumání různých metrik dat. [28]

3.3.2.4 Kibana

Kibana je nástroj zodpovědný za vizualizaci, zkoumání a vyhledávání v datech. Velmi dobře pracuje s daty shromážděnými nástrojem Elasticsearch tím, že je zobrazí v různých typech grafů a z různých pohledů. Obsahuje širokou škálu předpřipravených šablon, které ušetří čas, ale poskytuje i možnost vytvořit si vlastní šablonu nebo uzpůsobit stávající dle představ a potřeb pro lepší a detailnější práci s daty a statistikami.

Kromě vizualizace dat jsou součástí tohoto nástroje také dashboardy. Všechny grafy nebo jinak vizualizovaná data i dashboardy lze převést do formátu CSV pro další práci s výstupy nebo jejich sdílení. [28]



Obrázek 3.3 Elastic Stack komponenty

[31]

3.3.3 Benefity placené verze

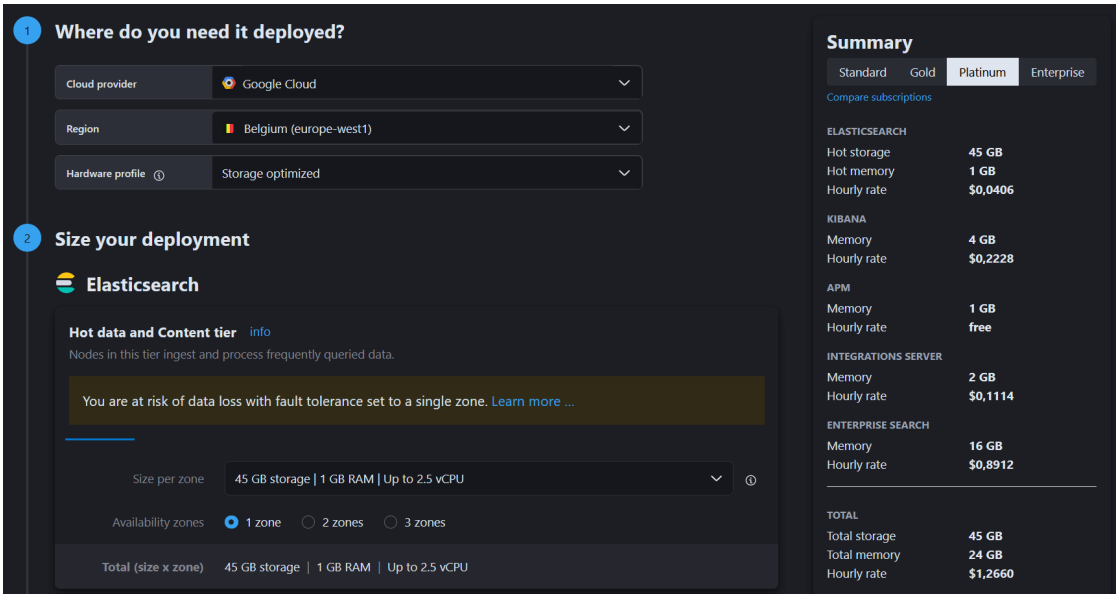
Elastic Stack a jeho jednotlivé komponenty je možné stáhnout on-premise nebo s nimi pracovat v rámci Elastic Cloud.

On-premise verze dnes existuje ve třech edicích (*Basic, Platinum, Enterprise*), z čehož edice *Basic* je zdarma a poskytuje základní funkce Elastic řešení. Oproti placeným edicím (*Platinum*, *Enterprise* a dnes už zaniklé *Gold*) postrádá některé funkce, zejména v oblasti upozornění a reakcí na nálezy, detekce anomálií pomocí machine learningu, úpravy a export dashboardů a hlavně zcela postrádá zákaznickou podporu. [32]

Instalace nástrojů na vlastní zařízení zabere nějaký čas, je potřeba provádět pravidelné aktualizace a výkon je omezen dostupným hardware. Za nasazení do Elastic Cloud je nutné platit (neexistuje bezplatná edice), ale ve výsledku to ušetří čas a úsilí. Cloudové řešení obecně ušetří čas minimálně v počáteční fázi a není závislé na hardware - je k němu možné přistoupit v podstatě odkudkoliv bez nutnosti mít u sebe konkrétní zařízení s nainstalovaným software.

Jednou z výhod Elastic Cloud na rozdíl od řešení mnoha jiných firem je, že se platí pouze za reálně využité hardwarové prostředky. Za Elastic Cloud je možné platit paušálně nebo každý měsíc zaplatit podle využitých prostředků. Existují čtyři edice Elastic Cloudu (*Standard, Gold, Platinum, Enterprise*), které se, podobně jako on-premise edice, liší množstvím nabízených funkcí a úrovní zákaznické podpory. [33]

Elastic nabízí různé hardwarové profily, kde si zákazník může nakonfigurovat, kolik potřebuje úložiště, paměti nebo jaký typ procesoru mu bude stačit. Tyto profily jsou buďto optimalizované podle velikosti úložiště (vhodné pro velké množství dat, která se budou spravovat a ukládat), podle výkonu procesoru (pokud je prioritou rychlé zpracování a analýza dat) nebo vyvážený profil. Výslednou cenu za využívání Elastic Cloud je možné spočítat pomocí kalkulačky, kterou Elastic nabízí. Umožňuje navolit poskytovatele cloudu, kolik prostředků bude potřeba pro každý nástroj a jaký cenový profil bude zvolen. Kalkulačka může sloužit i jako vodítko při rozhodování při nasazování on-premise. [33]



Obrázek 3.4 Kalkulačka ceny za Elastic Cloud v USD (2023) [34]

Kapitola 4

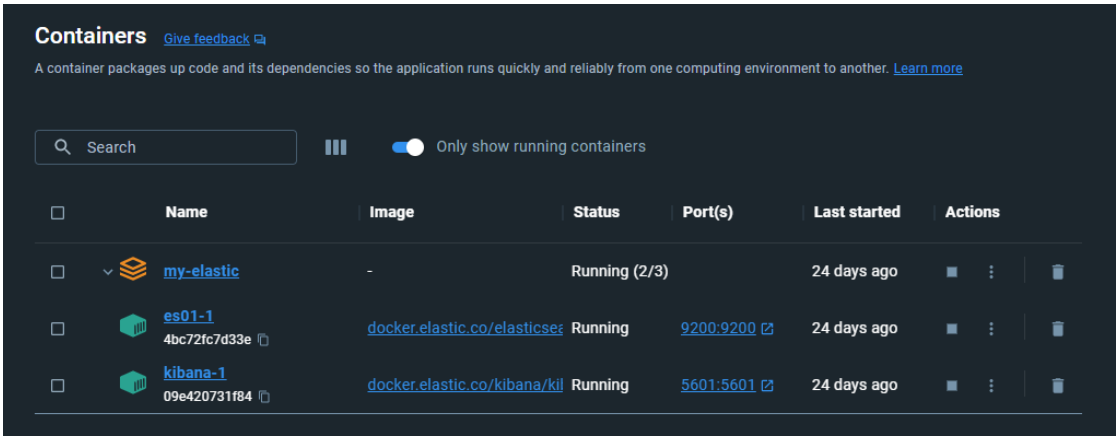
Implementace detekčních pravidel v nástrojích Elastic Stack

4.1 Instalace nástrojů Elastic Stack

Ke zpracování praktické části bylo potřeba nainstalovat vybrané nástroje Elastic Stack, a to nástroj Kibana, Elasticsearch, Winlogbeat a Packetbeat. Jak již bylo řečeno v předchozí kapitole (3.3), Elasticsearch je základním nástrojem pro prohledávání logů a pomocí nástroje Kibana se dají výsledky prohledávání vizualizovat (viz obrázky v kapitole 4.2). Oba tyto nástroje je možné nainstalovat buďto nativně nebo jako Docker image, z čehož byla pro vypracování této bakalářské práce zvolena druhá varianta.

Docker je virtualizační nástroj, který slouží k izolaci aplikací do tzv. kontejnerů.

Pro instalaci do Dockeru je potřeba soubor *docker-compose.yml*, pomocí kterého se dá nasadit více kontejnerů najednou (v případě této práce se jednalo o jeden kontejner pro nástroj Kibana a jeden pro Elasticsearch). Tento soubor obsahuje konfiguraci jednotlivých komponent a instrukce pro stažení image a jejich spuštění. Řešení Elastic Security, jehož součástí je i Elastic SIEM vyžaduje nastavení autentizace a šifrování komunikace, aby mohl nástroj Kibana bezpečně komunikovat s nástrojem Elasticsearch.



Obrázek 4.1 Docker kontejner - Elasticsearch a Kibana

K získání logů, které bude možné analyzovat a korelovat, byly z balíčku nástrojů Beats nainstalovány nástroje Winlogbeat a Packetbeat. Nástroj Winlogbeat shromažďuje záznamy o událostech v operačním systému Windows, Packetbeat zaznamenává provoz na síti, ke které je zařízení připojeno. U obou těchto nástrojů bylo také zapotřebí nastavit autentizaci vůči nástroji Elasticsearch. Toto nastavení se provádí v konfiguračním souboru *winlogbeat.yml*, resp. *packetbeat.yml*.

4.2 Návrh pravidel pro vybrané bezpečnostní hrozby

Zdrojem záznamů, kterými budou detekční pravidla otestovaná, je notebook s operačním systémem Windows, ze kterého sbírá záznamy nástroj Winlogbeat a prostředí domácí sítě, jejíž provoz zaznamenává nástroj Packetbeat.

V této kapitole bude popsán proces tvorby detekčních pravidel a názorně ukázané možné využití jednotlivých typů detekčních pravidel, která Elastic SIEM nabízí. Elastic taktéž nabízí možnost integrace předdefinovaných pravidel, která ovšem nejsou v této práci využita, aby byl vidět proces tvorby detekčních pravidel.

Základem pro sestavení ukázek detekčních pravidel byly typy událostí, které se mají podle Vyhlášky (1.1.2) zaznamenávat (uvedeno v kapitole 2.2.1). Hrozby, které jsou následujícími pravidly detekovány byly vybrány tak, aby byly využity uvedené typy záznamů a aby byly co nejlépe uplatněny možnosti pravidel Elastic SIEM.

4.2.1 Prohledávání logů

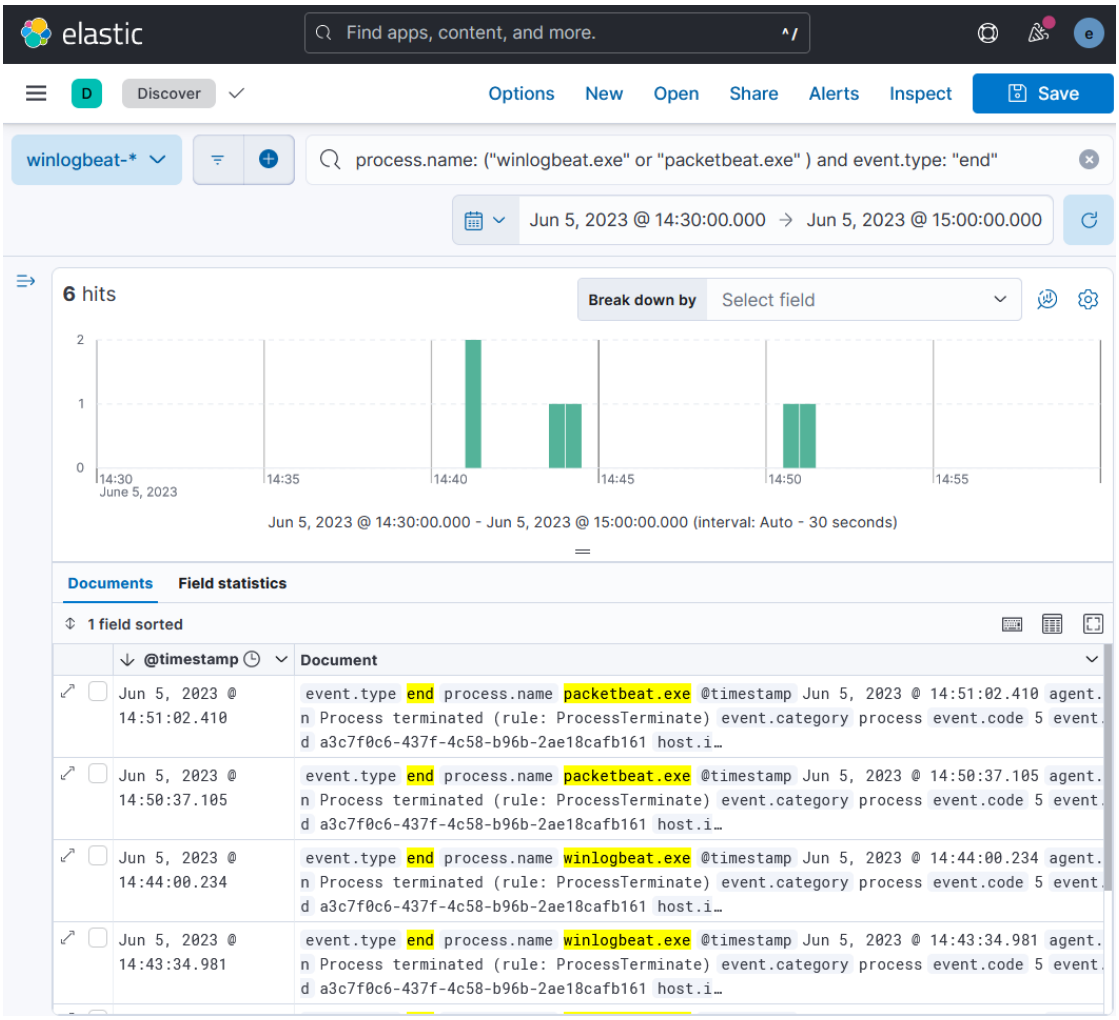
Jednou z možností, jak detekovat podezřelé chování nebo bezpečnostní hrozbu je vyhledávání záznamů pomocí dotazů v jazyce KQL.

KQL (*Kibana Query Language*) je jednoduchý dotazovací jazyk pro filtrování dat. [30]

Dle Vyhlášky (1.1.2) je potřeba zaznamenávat úspěšné i neúspěšné přístupy k záznamům o událostech, pokusy o manipulaci se záznamy a změny v konfiguraci zdrojů záznamů. Změnou v konfiguraci zdrojů záznamů může být i zastavení zaznamenávání, toho se v našem prostředí docílí vypnutím služby Winlogbeat nebo Packetbeat. Vypnutí služeb je zároveň další činností, která se má podle Vyhlášky (1.1.2) zaznamenávat. Vypnutí služeb Winlogbeat a Packetbeat bylo proto zvoleno pro ukázku prohledávání logů pomocí KQL dotazu a následně pro implementaci pravidla založeného na tomto dotazu.

Na ukázce 4.2 je vidět prostředí Kibana a příklad dotazu v jazyce KQL společně s jeho výsledkem. Tento dotaz vrací pouze logy týkající se vypnutí služby Winlogbeat nebo Packetbeat a je možné nastavit, z jakého časového úseku mají být prohledávané logy, zde se jedná o úsek 30 minut. Na grafu je pak na časové ose vizualizován počet logů odpovídajících KQL dotazu. V dolní části obrázku jsou v tabulce konkrétní logy odpovídající danému dotazu. Jednotlivá pole, například *process.name*, je možné přidat jako samostatné sloupce tabulky, podle kterých se dají logy řadit. O každém logu je možné zobrazit podrobnosti v podobě tabulky nebo formátu JSON. Každý KQL dotaz se dá uložit i s časovým filtrem pro pozdější použití.

Tímto způsobem se dá jednorázově vyhledat konkrétní log nebo množina logů odpovídající hodnotami svých parametrů zadanému KQL dotazu.



Obrázek 4.2 Ukázka dotazu v jazyce KQL

4.2.2 Tvorba detekčních pravidel

Elastic SIEM, stejně jako ostatní SIEM nástroje, umožňuje nadefinování pravidel, která se pravidelně spouští v nastavených časových periodách. Pravidla prohledávají logy z časového úseku od předchozího spuštění pravidla a je možné nastavit prohledávání i starších logů (pravidlo běží například každých pět minut a prohledává logy z posledních sedmi minut). Nálezům získaným detekčními pravidly se dá nastavit závažnost (*severity*) v podobě čtyř úrovní (*low, medium, high, critical*) a rizikovost (*risk score*) na stupnici od 0 do 100. Dále je možné uvést podrobnosti o pravidle nebo o události, kterou zachytává, příklady false-positive nálezů nebo postup při vyšetřování nálezu a jak se v takovém případě chovat.

Důležitou součástí je také nastavení upozornění na nálezy emailem, prostřednictvím MS Teams, platformy Jira apod. Tato možnost není součástí základní Elastic edice, tudíž nebude v práci ukázána. I bez zakoupeného balíčku se ale nálezy zobrazí na Elastic Security dashboard, kde se dají přehledně spravovat.

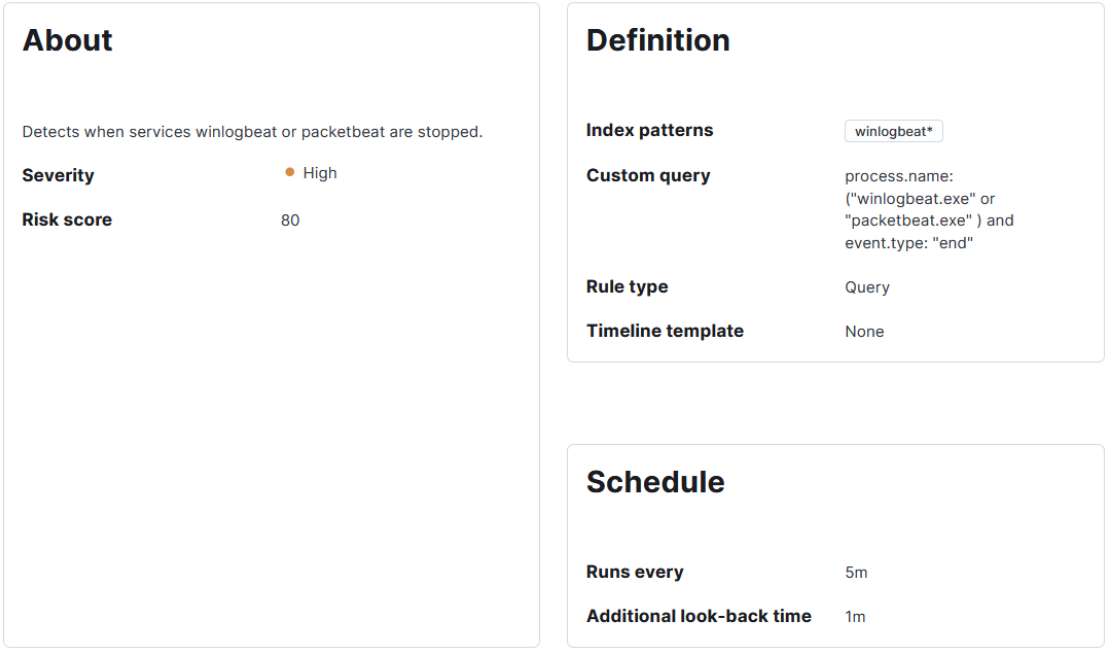
Elastic SIEM nabízí celkem šest typů detekčních pravidel [35], každý je vhodný k uplatnění v jiné situaci:

- Custom Query,
- Machine Learning (součástí pouze platinum a enterprise edice),
- Threshold,
- New Terms,
- Indicator Match,
- Event Correlation.

4.2.2.1 Detekční pravidla typu Custom Query

Z KQL dotazu použitého při jednorázovém prohledávání logů je možné vytvořit detekční pravidlo. Pro vytvoření pravidla byl využit KQL dotaz z ukázky 4.2.

Jak je vidět na obrázku 4.3 z prostředí Kibana, pravidlo detekuje vypnutí služby Winlogbeat nebo Packetbeat, spouští se každých pět minut a prohledává záznamy z posledních šesti minut. Pravidlu je nastavena vysoká závažnost a rizikovost 80/100, protože se jedná o služby zaznamenávající činnosti v systému a síti, a tím pádem jsou nezbytné pro detekci hrozeb. Změnou názvů služeb v poli *process.name* je možné detekovat vypnutí dalších důležitých nebo i jiných služeb.



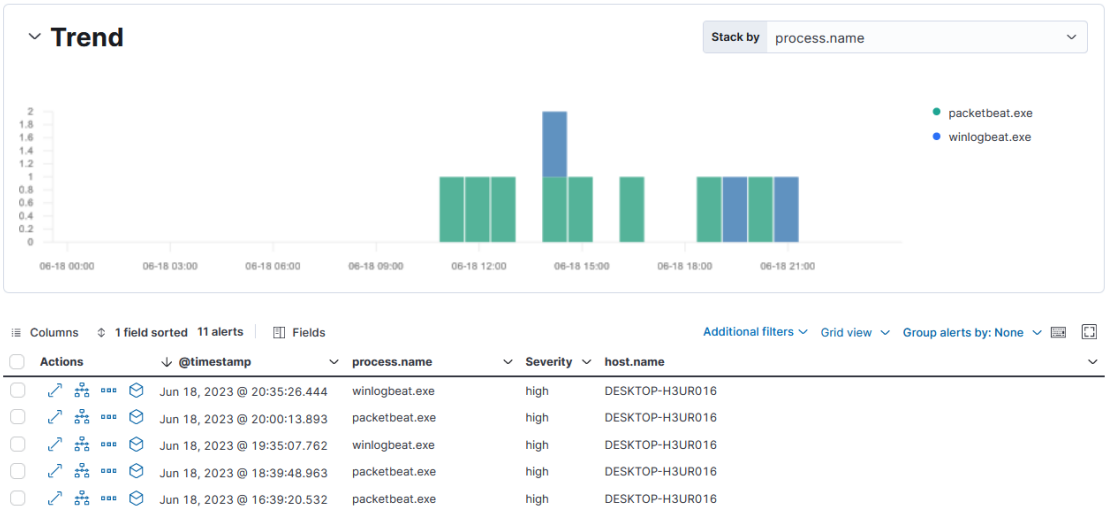
Obrázek 4.3 Ukázka Custom Query

Pro otestování pravidla byl vytvořen vzorek dat pomocí skriptu 1. Tento skript restartuje službu Winlogbeat nebo Packetbeat, mezi kterými se náhodně rozhoduje a poté čeká jednu vteřinu až dvě hodiny (7200 vteřin) před dalším restartováním jedné ze služeb. Restartování služeb proběhne celkem 11krát. V rámci restartování se služby vypínají a zapínají, tudíž vzniká záznam o vypnutí služby, který zachycuje výše uvedené pravidlo.

```
$runs = 0
while ( $runs -le 10 ) {
    $service = "winlogbeat", "packetbeat" | Get-Random
    Write-Host Stopping service $service

    Restart-Service $service

    $pause = Get-Random -Minimum 1 -Maximum 7200
    $time = Get-Date -format "HH:mm:ss"

    Write-Host Waiting for $pause seconds...
    Start-Sleep -Seconds $pause

    $runs++
}
```

Výpis kódu 1 Skript pro restartování služeb Winlogbeat a Packetbeat

Obrázek 4.4 ukazuje detekce tímto pravidlem po simulaci vypnutí a zapnutí služeb Winlogbeat a Packetbeat pomocí výše uvedeného skriptu. Na grafu jsou nálezy barevně rozlišeny, vypnutí služby Packetbeat je znázorněno zeleně, Winlogbeat modře. Níže jsou záznamy jednotlivých nálezů s podrobnostmi.

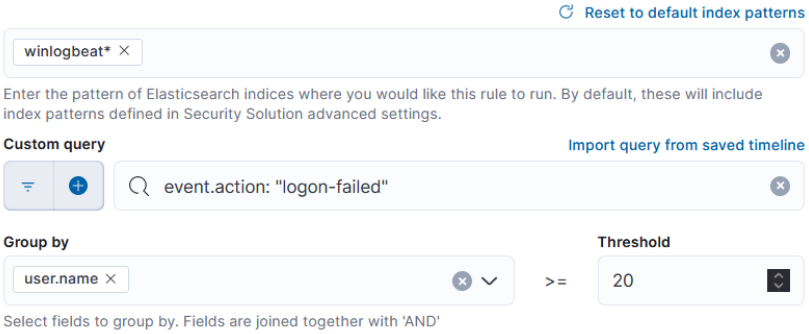


Obrázek 4.4 Nálezy pravidlem pro detekci vypnutí služby Winlogbeat nebo Packetbeat

4.2.2.2 Detekční pravidla typu Threshold

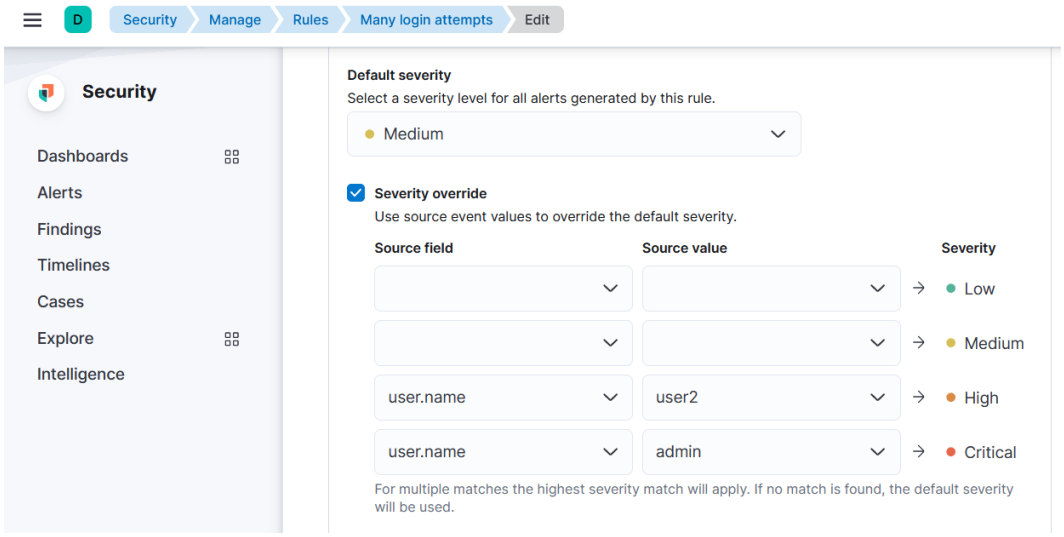
Pravidly typu Threshold je možné detekovat nadměrný výskyt určitých událostí pomocí nastavení prahové hodnoty (*threshold*). Při překročení této prahové hodnoty se vyvolá alert.

Vyhláška (1.1.2) nařizuje určitým organizacím zaznamenávat úspěšné i neúspěšné pokusy o přihlašování a odhlašování. K detekci podezřelé aktivity pomocí takových záznamů může sloužit následující pravidlo. Obrázek 4.5 uvádí příklad threshold pravidla, které vyvolá upozornění (*alert*) při více než dvaceti neúspěšných pokusech o přihlášení k jednomu uživatelskému účtu za určitou dobu. Pravidlo vyhledává v záznamech z nástroje Winlogbeat záznamy, jejichž pole *event.action* má hodnotu *logon-failed*. Vyfiltrované záznamy agreguje podle hodnoty pole *user.name*, a pokud je záznamů se stejným *user.name* více než dvacet, vyvolá alert. Tomuto pravidlu bylo nastaveno, aby běželo každé tři minuty a prohledávalo záznamy z posledních pěti minut.

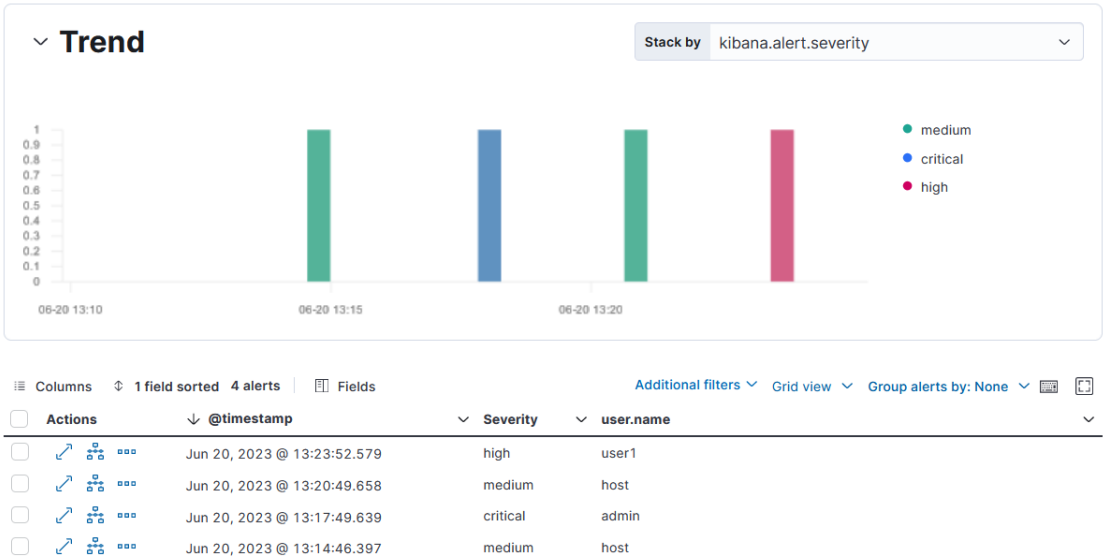


Obrázek 4.5 Ukázka threshold detekčního pravidla

Vyhláška (1.1.2) výslovně nařizuje zaznamenávat činnosti prováděné pod administrátorským účtem z důvodu vyšších oprávnění. Proto se hodí odlišit nálezy týkající se administrátorského (nebo jiného účtu s vyššími oprávněními) od běžných účtů. U všech pravidel, nejen typu Threshold, je možné upřesnit nastavení závažnosti. Výchozí závažnost (*Default severity*) se aplikuje na všechny nálezy kromě těch, které obsahují určitou hodnotu v poli upřesněnou dále. Na ukázce 4.6 je výchozí závažnost nastavena na střední úroveň, a pokud by se neúspěšná přihlášení týkala lokálního admin účtu, jednalo by se o kritickou závažnost. Uživatel *user2* má na tomto zařízení vyšší oprávnění než běžní uživatelé, proto mu byla nastavena vysoká závažnost. Obrázek 4.7 ukazuje detekce tímto pravidlem s rozdíly v závažnosti (*severity*) u jednotlivých uživatelských účtů.



Obrázek 4.6 Upřesnění nastavení závažnosti

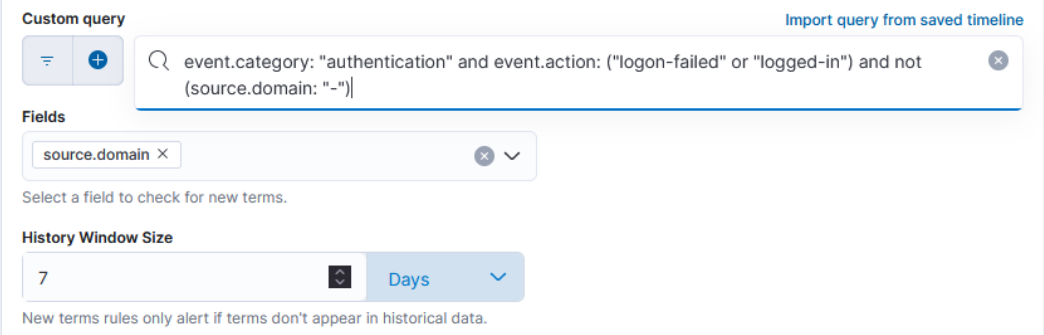


Obrázek 4.7 Nálezy pravidlem pro detekci 20 a více neúspěšných pokusů o přihlášení

4.2.2.3 Detekční pravidla typu New Terms

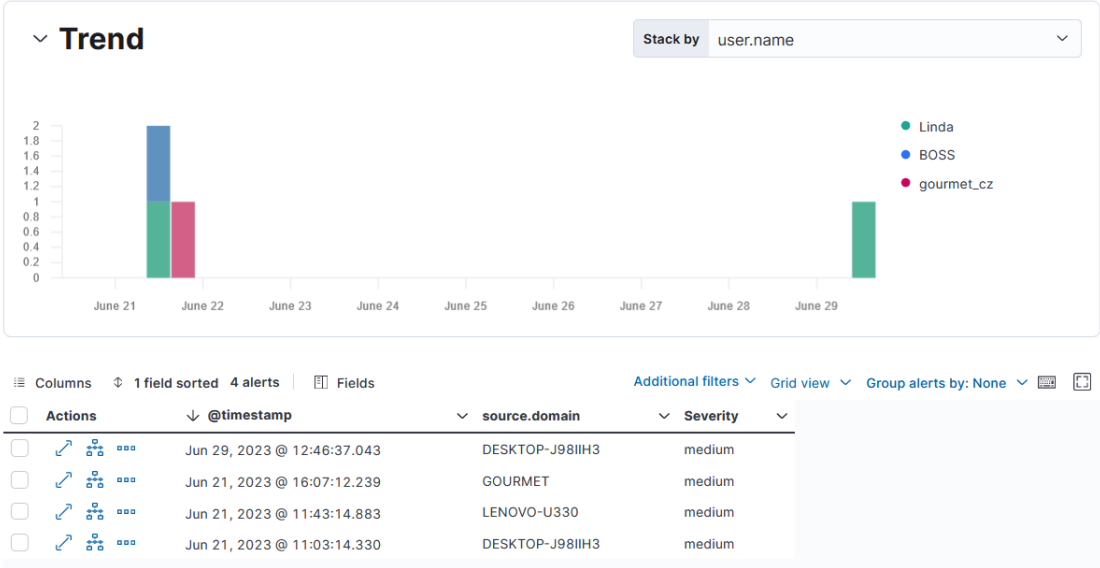
Podle Vyhlášky (1.1.2) je potřeba zaznamenávat činnosti uživatelů, které mohou mít vliv na bezpečnost systému. Takovou činností může být přihlášení do systému z nového zařízení, které nemusí být adekvátně nastaveno, aby odpovídalo bezpečnostním požadavkům organizace nebo ze zařízení, ze kterého se uživatel nepřihlašuje běžně.

Pravidla typu New Terms detekují výskyty nových hodnot v určitých polích logů. Na ukázce 4.8 je vidět tvorba pravidla, které detekuje pokusy o připojení ke sdílené složce z nového zařízení v lokální síti, ať už úspěšné nebo neúspěšné. Pravidlo vybírá z logů zaznamenaných nástrojem Winlogbeat pouze ty, které zaznamenávají události týkající se autentizace (*event.category: "Authentication"*), která proběhla úspěšně nebo neúspěšně (*event.action: ("logon-failed" or "logged-in")*) a nemají v poli *source.domain* hodnotu *"-"*. Autentizace se *source.domain* hodnoty *"-"* jsou typu 5. Tento typ se nazývá *service logon* a probíhá, když OS Windows spouští službu, a ta se má přihlásit jako uživatel. [36] Pravidlo běží každých deset minut a upozorňuje na hodnoty pole *source.domain*, které se během posledních sedmi dní (hodnota *History Window Size*) vyskytly poprvé.



Obrázek 4.8 Ukázka pravidla typu New Terms

Na obrázku 4.9 je vidět prostředí Kibana a nálezy tímto pravidlem po několika pokusech o připojení k notebooku s OS Windows a běžící službou Winlogbeat, který sdílí složku v lokální síti a přístup ke složce je chráněn heslem. Pokusy o připojení ke sdílené složce proběhly z několika zařízení s OS Windows v lokální síti. Pohled na obrázku zobrazuje detekce v rámci osmi dnů (od 21. 6. 2023 do 29. 6. 2023). Dne 21. 6. se pokusila připojit tři nová zařízení, mezi nimi i zařízení *DESKTOP-J98IIH3*, které se opět pokusilo připojit dne 29. 6. Pravidlo analyzuje historii pokusů o připojení jen z předchozích sedmi dní, proto je na obrázku vidět zachycený nový pokus o přihlášení z tohoto zařízení.



Obrázek 4.9 Nálezy pravidlem pro detekci pokusů o připojení z neznámé domény

4.2.2.4 Detekční pravidla typu Event Correlation

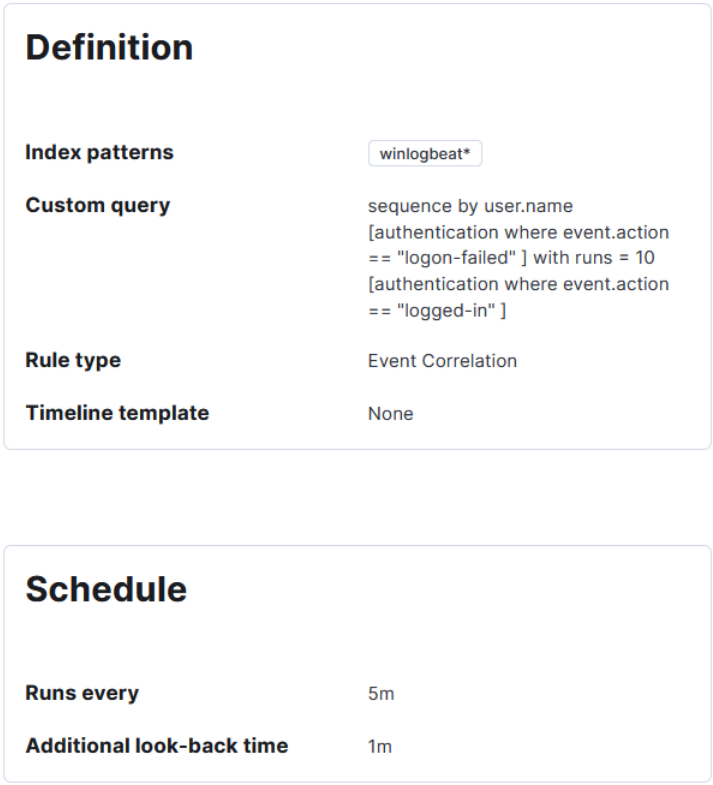
Korelační pravidlo se v Elastic SIEM definuje pomocí jazyka EQL.

EQL (*Event Query Language*) je dotazovací jazyk pro hledání sekvencí v datech jako jsou logy nebo metriky. [30]

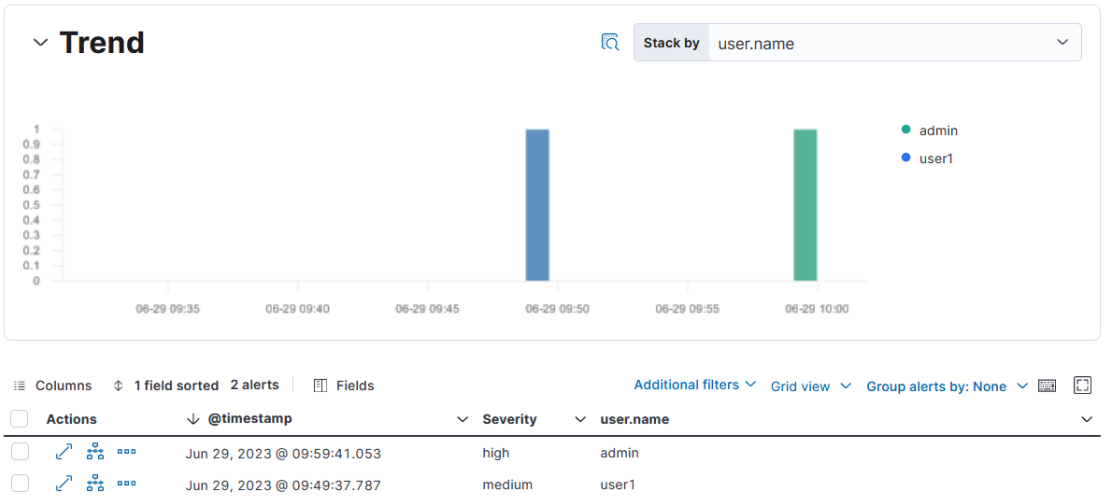
Ukázkou využití jazyka EQL je vyhledání sekvence pokusů o přihlášení uživatele. Následující pravidlo 4.10 ukazuje další využití záznamů úspěšných a neúspěšných pokusů o přihlášení, které se mají dle Vyhlášky (1.1.2) zaznamenávat. Pravidlo detekuje sekvenci deseti neúspěšných pokusů o přihlášení k jednomu uživatelskému účtu následovaných úspěšným přihlášením. V sekci *Schedule* je vidět, že se spouští každé tři minuty a koreluje logy z posledních čtyř minut.

Pravidlo vybírá logy kategorie *authentication*, a pokud po deseti záznamech s *event.action* hodnoty *"logon-failed* týkajících se jednoho uživatele následuje úspěšný pokus (*event.action* s hodnotou *"logged-in"* týkající se stejného uživatele, jedná se o nález.

Pravidlu byla nastavena střední (*medium*) závažnost a podobně jako v jednom z předchozích pravidel byla administrátorskému účtu nastavena vyšší závažnost, zde *high*. Na obrázku 4.11 je vidět, že po simulaci deseti a více neúspěšných pokusů o přihlášení následovaných úspěšným přihlášením k účtu *user1* pravidlo vyvolalo alert se střední (*medium*) závažností a při simulaci pokusů o přihlášení k účtu *admin* byla závažnost alertu vysoká (*high*).



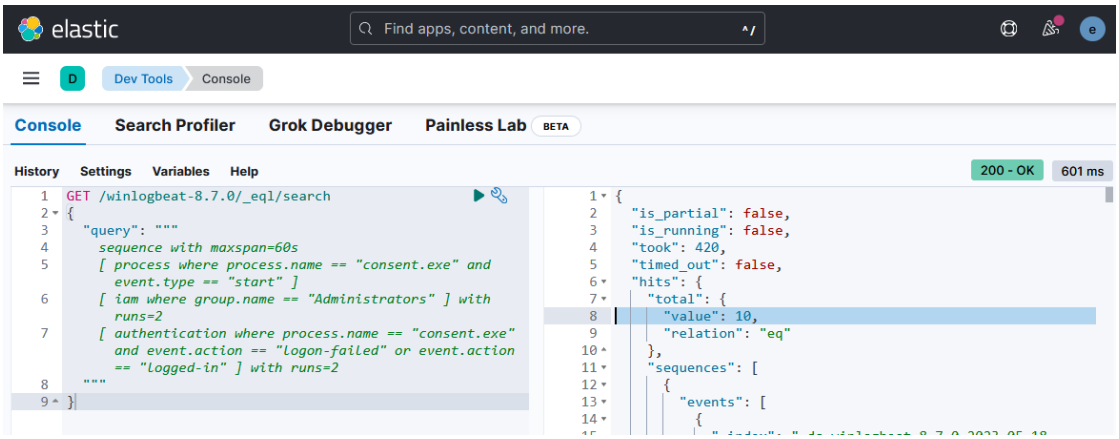
Obrázek 4.10 Ukázka korelačního detekčního pravidla



Obrázek 4.11 Nálezy pravidlem pro detekci sekvence neúspěšných pokusů o přihlášení následovaných úspěšným přihlášením

Dle Vyhlášky (1.1.2) je nutné zaznamenávat neúspěšné pokusy o provedení činnosti kvůli nedostatku oprávnění. Jako další příklad byla proto zvolena detekce pokusu o manipulaci se soubory ve sdílené složce uživatelem, který k dané operaci nemá dostatečná oprávnění. Za účelem zjištění sekvence událostí, kterými se bude definovat EQL pravidlo byla daná hrozba nasimulována. K tomu byla vytvořena sdílená složka a v ní několik souborů. Ke složce byla uživateli *user1* nastavena pouze práva na čtení jejích souborů a ve speciálních oprávněních mu bylo zakázáno mazání této složky, jejích podsložek a souborů. Následně byl pod uživatelským účtem *user1* proveden pokus o smazání souboru z této složky, což vyžadovalo administrátorské oprávnění. Heslo k administrátorskému účtu bylo několikrát zadáno nesprávně a jednou správně, aby byly v záznamech obě varianty.

Poté byly v nástroji Kibana pomocí KQL dotazu s časovým omezením nalezeny záznamy týkající se nasimulované hrozby. Podle nalezených záznamů byl navržen EQL dotaz a jeho správnost byla ověřena ve vývojářské konzoli. Prostředí vývojářské konzole je vidět na obrázku 4.12.

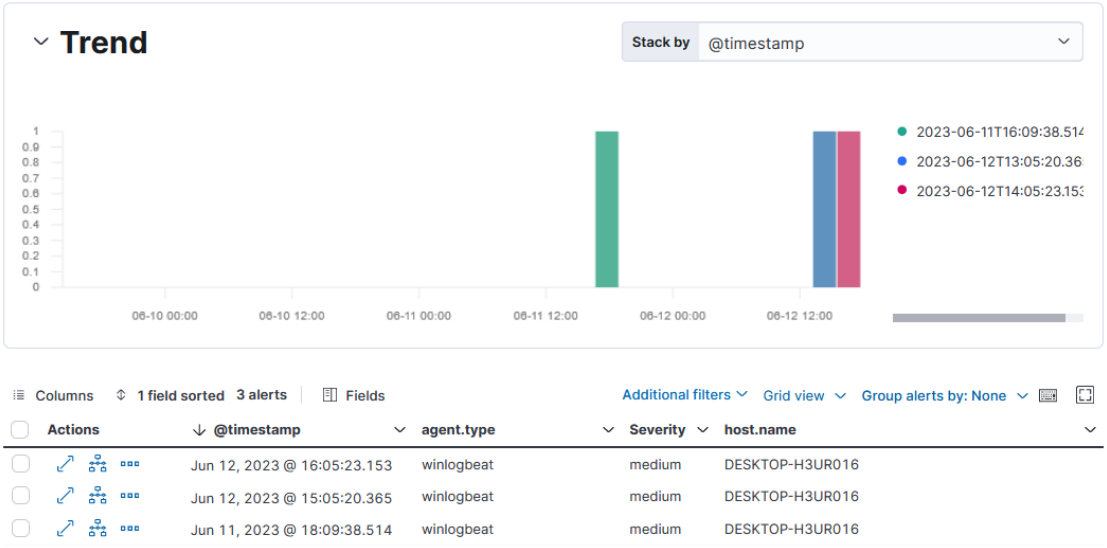


Obrázek 4.12 Vyhledávání sekvence logů ve vývojářské konzoli

V levé části obrázku je GET požadavek ve formátu JSON zaslaný nástroji Elasticsearch. V části *query* je samotný EQL dotaz, který hledá sekvenci událostí v rozmezí 60 vteřin (*maxspan=60s*). V hranatých závorkách jsou jednotlivé události skládající se z hodnoty pole *event.category* (zde *process*, *iam* a *authentication*) a podmínky za klíčovým slovem *where*. Prvním hledaným záznamem je vytvoření procesu *consent.exe*, což je proces *Consent UI for administrative applications* a spouští se ve chvíli, kdy se danou akcí ovlivní celý systém nebo soubory ve složce jiného uživatele a k jejíž provedení jsou potřeba administrátorská oprávnění. Dalším záznamem v sekvenci je vyhodnocení členství ve skupině *Administrators* a sekvence je zakončena záznamem o výsledku přihlášení k administrátorskému účtu. Dotaz hledá obě varianty - kdy se přihlášení povedlo (*event.action == "logged-in"*) i kdy se nezdařilo (*event.action == "logon-failed"*).

V pravé části obrázku je odpověď nástroje Elasticsearch, také ve formátu JSON, která říká, že takovýchto sekvencí existuje v rámci všech záznamů z nástroje Winlogbeat deset (zvýrazněno na řádku č. 8) a dále jsou vypsané všechny odpovídající logy.

Ve vývojářské konzoli bylo tedy ověřeno, že navržený EQL dotaz funguje podle předpokladů a nachází hledanou sekvenci logů. Následně bylo pomocí této sekvence vytvořeno korelační detekční pravidlo se střední závažností. Na obrázku 4.13 jsou vidět nálezy tímto pravidlem v rozmezí šesti dní. V tomto období byly provedeny tři pokusy o smazání souboru ve sdílené složce uživatelem *user1*.



Obrázek 4.13 Nálezy pravidlem pro detekci pokusů o manipulaci se soubory ve sdílené složce

Po rozkliknutí každého z alertů je možné zjistit více podrobností a mimo jiné také změnit status daného alertu na jednu z hodnot *open, acknowledged, closed*. Kromě toho je možné daný alert přidat k nějakému řešenému případu (*case*), což umožňuje zobrazení souvisejících nálezů na jednom místě a zpřehlednění jejich vyšetřování. Pokud je daný nález tzv. *false-positive* (případ, kdy pravidlo nesprávně vyhodnotí, že se jedná o hrozbu), je z něj možné vytvořit výjimku nastavením, že při určitých hodnotách nějakého pole se nebude jednat o pozitivní nález. Jinak je samozřejmě možné podchytit false-positive nálezy úpravou definice pravidla.

Závěr

Studie kybernetických bezpečnostních hrozeb ukazují, že se jejich počet a komplexita neustále zvyšuje. S raketovým nástupem AI se bude situace pravděpodobně zhoršovat, a proto je nutné včas reagovat. Je potřeba zajistit chod organizací kritické infrastruktury, které mají povinnost se chránit. Tato povinnost je definována českými i evropskými legislativními normami. Mezi tyto normy patří zákon o kybernetické bezpečnosti, vyhláška č. 82/2018 Sb. vycházející z evropské směrnice NIS a nově i směrnice NIS 2, kterou v ČR uvidíme v podobě nového kybernetického zákona v průběhu roku 2024.

Teoretická část práce rozebírá tyto legislativní požadavky a zaměřuje se na pravidla spojená s detekcí bezpečnostních hrozeb. Seznamuje čtenáře s technologií SIEM, kterou je možné některé legislativní požadavky naplnit, jejími funkcionalitami, souvisejícími nástroji a možnými zdroji záznamů pro analýzu a detekci hrozeb.

Jedním z cílů práce bylo zanalyzovat současný stav a nedávný vývoj trhu SIEM nástrojů. V této části čerpá práce z mnoha veřejných zdrojů informací o SIEM a trhu SIEM nástrojů, zejména z reportů analýz trhu prováděnými pravidelně společnostmi Gartner a Forrester. Průzkumy prováděné těmito společnostmi ukazují, že je dnes mnoho možností, jak legislativní požadavky splnit a není vždy nutné volit drahé řešení. Analýza těchto zdrojů také ukázala, že trh se SIEM nástroji v posledních letech rostl, předpokládá se růst i nadále a přibývá mnoho nových firem nabízejících svá bezpečnostní řešení. Zdroje analýz se také shodují v nejsilnějších hráčích na trhu a zaznamenání rychlého nástupu popularity nástrojů Elastic Stack.

Nástroje Elastic Stack se před několika lety nově objevily v analýzách trhu a usilovně se derou mezi první pozice co se týče zastoupení na trhu. Přiblížení skladby a možností těchto nástrojů bylo dalším dílčím cílem teoretické části práce. Firma Elastic nabízí nástroje zdarma i v několika placených variantách a umožňuje nasazení on-premise i do cloudu.

V návrhu nového zákona o kybernetické bezpečnosti je i značné rozšíření okruhu organizací, které budou povinny se řídit legislativními opatřeními. Mnoho takových organizací si nebude moci dovolit zpoplatněné bezpečnostní řešení vzhledem k vyšším pořizovacím i provozním nákladům. Dá se předpokládat nárůst poptávky po zdarma nabízených nástrojích, jako je například Elastic Stack.

V praktické části bylo předvedeno, že je možné pomocí Elastic SIEM vyhovět legislativním požadavkům. V navržených detekčních pravidlech je předvedeno možné využití záznamů událostí, které je podle Vyhlášky potřeba shromažďovat. Současně byla implementovanými pravidly pokryta většina typů detekčních pravidel, která nabízí Elastic SIEM, a tím byla názorně ukázána všestrannost těchto nástrojů. Lze předpokládat, že Elastic SIEM bude jedním z využívaných řešení pro organizace, které se budou nově budou muset tímto typem legislativy řídit.

Bibliografie

1. ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi.cz* [online]. Znění od 6. 8. 2022 [cit. 2023-03-16]. Dostupné z: `https://www.zakonyprolidi.cz/cs/2014-181`.
2. ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky* [online]. 2018, částka 43 [cit. 2023-03-18]. ISSN 1211-1244. Dostupné z: `https://www.nukib.cz/download/publikace/legislativa/vkb_82-2018sb.pdf`.
3. NÚKIB. *Legislativa KB* [online]. [cit. 2023-04-13]. Dostupné z: `https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/`.
4. NÚKIB. *Nová směrnice EU o kybernetické bezpečnosti „NIS 2“ a návrh nového zákona o kybernetické bezpečnosti* [online]. [cit. 2023-04-13]. Dostupné z: `https://osveta.nukib.cz/course/view.php?id=145`.
5. EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. Směrnice Evropského parlamentu a Rady (EU) 2022/2555, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2). In: *Úřední věstník Evropské unie* [online]. Prosinec 2022 [cit. 2023-03-19]. Dostupné z: `https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=EN`.
6. KENT, Karen; SOUPPAYA, Murugiah. *Guide to Computer Security Log Management* [online]. NIST SP 800-92. NIST, National Institute of Standards a Technology, Září 2006. Dostupné z DOI: `10.6028/NIST.SP.800-92`.
7. MELNICK, Jeff. *SIEM vs Log management* [online]. Newtrix, 2023-03-17. [cit. 2023-04-05]. Dostupné z: `https://blog.netwrix.com/2021/04/28/siem-vs-log-management/`.
8. *Frequently asked questions* [online]. Elastic. [cit. 2023-05-29]. Dostupné z: `https://www.elastic.co/what-is/`.
9. *Information Technology Glossary - Essential Information Technology Terms Definitions* [online]. Gartner. [cit. 2023-04-13]. Dostupné z: `https://www.gartner.com/en/information-technology/glossary/`.
10. JOHNSON, L. Arnold; DEMPSEY, Kelley; ROSS, Ron; GUPTA, Sarbari; BAILEY, Denis. *Guide for Security - Focused Configuration Management of Information Systems* [online]. NIST SP 800-128. NIST, National Institute of Standards a Technology, Říjen 2019. Dostupné z DOI: `10.6028/NIST.SP.800-128`.

11. *Different types of logs in SIEM and their log formats* [online]. ManageEngine Log360. [cit. 2023-04-24]. Dostupné z: https://www.manageengine.com/log-management/siem/collecting-and-analysing-different-log-types.html.
12. *IP Addressing: DNS Configuration Guide, Cisco IOS XE Release 3S* [online]. Cisco Systems, Inc., 2015. [cit. 2023-04-24]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/xe-3s/dns-xe-3s-book.pdf.
13. *What is Azure Web Application Firewall on Azure Application Gateway?* [online]. Microsoft, 2023-03-10. [cit. 2023-06-12]. Dostupné z: https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview.
14. KRISHNAN, Hiranmayi. *SIEM simplified: A guide for beginners* [online]. ManageEngine Log360, 2022-02-16. [cit. 2023-05-01]. Dostupné z: https://www.manageengine.com/log-management/cyber-security/siem-simplified-a-guide-for-beginners.html.
15. MONTIE, Samuel. *What is SIEM UEBA and how it can help me?* [Online]. BitLyft, Květen 2022. [cit. 2023-06-10]. Dostupné z: https://www.bitlyft.com/resources/siem-ueba-modern-cybersecurity-attack.
16. *SIEM & Security Analytics* [online]. Elastic. [cit. 2023-04-13]. Dostupné z: https://www.elastic.co/security/siem.
17. ABRAHAM, Michelle; KISSE, Christopher. *Worldwide Security and Information Event Management Market Shares, 2020: SaaS-Focused Rise* [online]. Říjen 2021. [cit. 2023-05-02]. Dostupné z: https://www.splunk.com/en_us/pdfs/resources/analyst-report/idc-market-share-2020-siem.pdf.
18. NICHOLS, Mike; PAQUETTE, Mike. *Elastic continues to gain momentum in SIEM market* [online]. Elastic, 2022-10-14. [cit. 2023-05-02]. Dostupné z: https://www.elastic.co/blog/elastic-continues-to-gain-momentum-in-siem-market.
19. NOVINSON, Michael. FireEye McAfee Enterprise XDR Business Renamed Trellix. *CRN, The Channel Company* [online]. 2022 [cit. 2023-04-13]. Dostupné z: https://www.crn.com/news/security/fireeye-mcafee-enterprise-xdr-business-renamed-trellix.
20. IMARC GROUP. *Security Information and Event Management (SIEM) Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2023-2028* [online]. Únor 2023. [cit. 2023-04-15]. SR112023A6059. Dostupné z: https://www.imarcgroup.com/security-information-event-management-market.
21. CANNER, Ben. *Findings: The Forrester Wave – Security Analytics Platforms, Q4 2020* [online]. 2020-12-02. [cit. 2023-05-21]. Dostupné z: https://solutionsreview.com/security-information-event-management/findings-the-forrester-wave-security-analytics-platforms-q4-2020/.
22. *Elastic Recognized as a Leader in Security Analytics by Independent Research Firm* [online]. Business Wire, 2022-12-14 [cit. 2023-05-16]. Dostupné z: https://www.businesswire.com/news/home/20221213006099/en/Elastic-Recognized-as-a-Leader-in-Security-Analytics-by-Independent-Research-Firm.
23. AKBAS, Ertugrul. *How to Select the Right SIEM Solution?* [Online]. 2021-07-18. Dostupné také z: https://www.peerspot.com/articles/how-to-select-the-right-siem-solution.
24. WILLIAMS, Andrew. *What to Consider Before Choosing the Right SIEM Tool* [online]. mimecast, 2022-11-29. [cit. 2023-04-05]. Dostupné z: https://www.mimecast.com/blog/what-to-consider-before-choosing-the-right-siem-tool/.
25. *Cloud SIEM: Features, Capabilities, and Advantages* [online]. Exabeam, 2022-04-20. [cit. 2023-04-16]. Dostupné z: https://www.exabeam.com/explainers/next-gen-siem/cloud-siem-features-capabilities-and-advantages/.

26. MILLER, Jason. *Managed SIEM vs. SIEM on-prem: pros cons* [online]. 2018-09-21. [cit. 2023-04-30]. Dostupné z: https://www.bitlyft.com/resources/managed-siem-vs-siem-on-prem-pros-cons.
27. CANNER, Ben. *The Minimum Requirements For Enterprise SIEM Solutions* [online]. Solutions Review, 2021-05-19. Dostupné také z: https://solutionsreview.com/security-information-event-management/the-minimum-requirements-for-enterprise-siem-solutions/.
28. *The Elastic Stack and its components: Elasticsearch, Kibana, Logstash, Beats* [online]. Quintagroup. [cit. 2023-04-14]. Dostupné z: https://quintagroup.com/services/the-elastic-stack-and-its-components-elasticsearch-kibana-logstash-and-beats.
29. *Why free and open?* [Online]. Elastic. [cit. 2023-06-14]. Dostupné z: https://www.elastic.co/about/free-and-open.
30. *Elastic Docs* [online]. Elastic. [cit. 2023-04-20]. Dostupné z: https://www.elastic.co/guide/index.html.
31. *The ELK Stack: From the Creators of Elasticsearch* [online]. Elastic. [cit. 2023-06-15]. Dostupné z: https://www.elastic.co/what-is/elk-stack.
32. *Elastic Stack Subscriptions* [online]. Elastic. [cit. 2023-06-20]. Dostupné z: https://www.elastic.co/subscriptions.
33. *Elastic pricing* [online]. Elastic. [cit. 2023-06-20]. Dostupné z: https://www.elastic.co/pricing/.
34. *Elastic Cloud (Elasticsearch Service) Pricing Calculator* [online]. Elastic. [cit. 2023-06-14]. Dostupné z: https://cloud.elastic.co/pricing?elektra=pricing-page.
35. *Create a Detection Rule* [online]. Elastic. [cit. 2023-06-03]. Dostupné z: https://www.elastic.co/guide/en/security/current/rules-ui-create.html.
36. FLORES, John; HANSON, Diana. Administrative tools and logon types [online]. 2022 [cit. 2023-05-10]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-tools-logon-types.