VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

NÁSTROJ PRO VIZUALIZACI A ANALÝZU KORELAČNÍCH PRAVIDEL SIEM NASAZENÝCH V KYBERPROSTORU

WEB APPLICATION FOR VISUALIZATION AND ANALYSIS OF CORRELATION RULES DEPLOYED IN CYBERSPACE

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Hana Závišková

AUTHOR

VEDOUCÍ PRÁCE — Ing. Yehor Safonov

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Hana Závišková ***ID:*** 241133

Ročník: 3 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Nástroj pro vizualizaci a analýzu korelačních pravidel SIEM nasazených v kyberprostoru

POKYNY PRO VYPRACOVÁNÍ:

Hlavním cílem bakalářské práce je návrh a implementace webové aplikace sloužící pro vizualizaci a efektivní správu SIGMA pravidel s cílem jejich efektivního vývoje a pokrytí co nejširšího spektra vektorů útoků. Grafické uživatelské rozhraní bude integrovat moderní způsoby vizualizace a mít formu interaktivní webové aplikace. Vizualizace bude rozšiřovat existující MITRE ATT&CK model a umožní bezpečnostnímu expertovi zkoumat nasazenou množinu SIEM anebo EDR pravidel z různých perspektiv. V teoretické části proveďte analýzu existujících technik vizualizace a bezpečnostních standardů, nastudujte problematiku SIGMA pravidel a kategorizace zdrojů logů, popište principy MITRE ATT&CK, Pyramid of Pain, Threat Intelligence platforem a Cyber Kill Chain. Zaměřte se na moderní bezpečnostní doporučení organizace ENISA. Identifikované poznatky integrujte do aplikace. V rámci praktické části realizujte experimentální pracoviště, proveďte srovnání moderních způsobů vizualizace použitých v moderních SIEM (Netwitness, QRadar, Splunk apod.). Navrhněte způsoby vizualizace nasazených Sigma pravidel. Implementujte architekturu webové aplikace a realizujte minimálně tří zobrazení.

DOPORUČENÁ LITERATURA:

[1] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. CZ.NIC, 2019. ISBN 978-80-88168-31-7.

[2] DIOGENES, Yuri a Dr. Erdal OZKAYA. Cybersecurity – Attack and Defense Strategies. 2nd Edition. Packt Publishing, 2019. ISBN 9781838822217.

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 28.5.2024

Vedoucí práce: Ing. Yehor Safonov

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Ve světě neustále se vyvíjejících moderních technologií roste potřeba vytváření kybernetických bezpečnostních strategií pro ochranu digitálních infrastruktur, neboť se rapidně zvyšují počty kybernetických útoků.

Hlavním cílem bakalářské práce je vytvořit nástroj pro vizualizaci korelačních pravidel systémů SIEM. Nástroj je realizován formou rozšíření existující webové aplikace a klade si za cíl umožnit bezpečnostnímu expertovi či uživateli aplikace zkoumat uživatelská Sigma pravidla podle různých kritérií a na základě různých pohledů.

Z teoretického hlediska se bakalářská práce zaměřuje na seznámení čtenáře se základy kybernetické bezpečnosti z hlediska motivace zajišťování bezpečnosti, vysvětlení základních pojmů nezbytných pro pochopení obsahu práce a rozbor perspektiv, jakými způsoby lze na kybernetické útoky nahlížet. Obsahuje také popis vybraných kybernetických útoků, jejichž výběr vychází z vypracovaných statistik provedených kybernetických útoků na Českou republiku za období prvních třech kvartálů roku 2023. Následuje vysvětlení principu detekce a prevence vzniku kybernetických incidentů, technologií pro zajištění ochrany v kyberprostoru včetně problematiky zdrojů logů a platforem pro zjišťování informací o hrozbách a principů vyšetřování kybernetických incidentů. Následuje úvod do problematiky právní úpravy kybernetické bezpečnosti včetně popisu doporučení organizace ENISA.

Praktická část bakalářské práce je dále rozdělena na čtyři kapitoly. V první části byla provedena analýza dostupných webových frameworků, které mohou být použity v rámci vývoje aplikace, a analýza způsobů vizualizace pravidel použitých ve dvou moderních SIEM řešeních. Druhá fáze se věnuje návrhu různých pohledů, pomocí nichž lze zajistit příjemné, intuitivní a interaktivní prostředí pro zobrazení uživatelských pravidel. Součást vizualizačních návrhů tvoří komponenty dostupné v knihovně D3.js a práce s maticí MITRE *ATT&CK*. Druhá fáze také zahrnuje vytvoření struktury pro rozložení prvků ve webové aplikaci. Třetí fáze je orientována na přiblížení samotné implementace vhodných zobrazení, které vyplývají z analýzy provedené ve druhé fázi. Zahrnuje také popis experimentálního prostředí, v němž byla aplikace vyvíjena, a způsob získání dat. Poslední fáze je zaměřena na testování vizuální části aplikace z pohledu uživatele.

Celou práci zakončuje závěr, v němž jsou shrnuty výsledky bakalářské práce, kterých bylo dosaženo, a návrhy na vylepšení aplikace do budoucna.

KLÍČOVÁ SLOVA

Aktér hrozby, D3.js, ENISA, MITRE ATT&CK, SIEM, Sigma pravidla, Vue, vizualizace, webová aplikace.

ABSTRACT

In a world of constantly evolving modern technologies, there is a growing need of developing cyber security strategies to protect digital infrastructures as the number of cyber attacks is rapidly increasing.

The main goal of the bachelor thesis is to create a tool for visualizing correlation rules of SIEM systems. The tool is implemented as an extension to an existing web application and aims to allow a security expert or application user to explore user Sigma rules according to different criteria and based on different views.

From a theoretical point of view, the bachelor's thesis focuses on introducing the reader to the basics of cyber security in terms of the motivation for providing security, explaining the basic concepts necessary to understand the content of the thesis and analyzing the perspectives in which cyber attacks can be viewed. It also contains a description of selected cyber attacks, the selection of which is based on the statistics of cyber attacks on the Czech Republic for the first three quarters of the year 2023. This is followed by an explanation of the principles of detection and prevention of cyber incidents, technologies for ensuring protection in cyberspace, including the issue of log sources and platforms for detecting information about threats and the principles of cyber incident investigation. This is followed by an introduction to the legal regulation of cyber security, including a description of ENISA recommendations.

The practical part of the bachelor thesis is further divided into four chapters. In the first part, an analysis of available web frameworks that can be used in application development and an analysis of the rule visualization methods used in two modern SIEM solutions were performed. The second phase focuses on the design of different views that can be used to provide a pleasant, intuitive and interactive environment for displaying user rules. The visualization designs include the components available in the D3.js library and working with the MITRE *ATT&CK* matrix. The second phase also includes the creation of a structure for the layout of the elements in the web application. The third phase is oriented towards approaching the actual implementation of the appropriate views that result from the analysis performed in the second phase. It also includes a description of the experimental environment in which the application was developed and how the data was obtained. The last phase focuses on testing the visual part of the application from the user's perspective.

The whole thesis finishes with a conclusion, which summarizes the results of the bachelor's thesis, which have been achieved, and suggestions for improving the application in the future.

KEYWORDS

D3.js, ENISA, MITRE ATT&CK, SIEM, Sigma rules, Threat actor, Vue, vizualization, web application.

ZÁVIŠKOVÁ, Hana. *Nástroj pro vizualizaci a analýzu korelačních pravidel SIEM nasazených v kyberprostoru*. Bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024. Vedoucí práce: Ing. Yehor Safonov

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Hana Závišková
VUT ID autora:	241133
Typ práce:	Bakalářská práce
Akademický rok:	2023/24
Téma závěrečné práce:	Nástroj pro vizualizaci a analýzu korelačních pravidel SIEM nasazených v kyberprostoru

Prohlašuji, že svou závěrečnou práci jsem vypracovala samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu bakalářské práce panu Ing. Yehoru Safonovi za odborné vedení, pravidelné konzultace, trpělivost, podporu a podnětné návrhy k práci. Dále bych ráda poděkovala své rodině a přátelům za podporu a svým kolegům z týmu *Cyber Defense Center* za odborné konzultace.

Obsah

Seznam obrázků

[0]Při kreslení obrázků v této bakalářské práce byly použité ikony dostupné z webové stránky <www.flaticon.com>, jsou zde zveřejněny a šířeny pod licencí CC 3.0 BY. Ikony byly vytvořeny autory: *Freepik, Soodabeh, Iconsea, Rukanicon, RaftelDesign, Tulpahn, Srip, Vector Stall, Ning Nong, Rosa Suave*

Seznam tabulek

Úvod

Ve světě neustále se vyvíjejících moderních technologií roste potřeba vytváření kybernetických bezpečnostních strategií pro ochranu digitálních infrastruktur, neboť se rapidně zvyšují počty kybernetických útoků. Pro posílení kybernetické bezpečnosti jsou využívány různé technologie, které dokáží monitorovat provoz v síti, aktivity na koncových zařízeních, vytvářet behaviorální modely aktivit na síti a při detekci škodlivé aktivity dokáží zasáhnout. Některé technologie jsou již založeny na umělé inteligenci, přesto je výhodné bezpečnostní technologii definovat zásady a pravidla, kterých by se měla organizace držet a při porušení těchto zásad odeslat upozornění bezpečnostnímu týmu. Jedná se o definování a implementaci detekčních a korelačních pravidel, jejichž aplikaci bezpečnostní systémy podporují.

Hlavním cílem bakalářské práce je implementace nástroje, který bude vhodně a přehledně zobrazovat uživatelská Sigma pravidla podle různých pohledů a na základě různých dat. Tato bakalářská práce rozvíjí již existující aplikaci *Sigma Tools*, která se zaměřuje na správu a překlad Sigma pravidel do jazyků různých platforem SIEM. Práce aplikaci rozvíjí v podobě vizuální klientské části.

Bakalářská práce se dělí na teoretickou a praktickou část, které dohromady tvoří pět kapitol. V teoretické části je čtenář seznámen se základy kybernetické bezpečnosti, které zahrnují motivaci zajišťování kybernetické bezpečnosti v digitálních infrastrukturách, vysvětlení základních pojmů nezbytných pro pochopení obsahu práce a rozbor perspektiv pohledů, kterými lze na kybernetické útoky nahlížet, konkrétně seznámení se s modely *Pyramid of Pain* a *Cyber Kill Chain*. Obsahuje také popis vybraných kybernetických útoků, jejichž výběr vychází z vypracovaných statistik provedených kybernetických útoků na Českou republiku za období prvních třech kvartálů roku 2023. Následuje vysvětlení principu detekce a prevence vzniku kybernetických incidentů, technologií pro zajištění ochrany v kyberprostoru a úvod do vyšetřování kybernetických incidentů, který zajišťuje bezpečnostní operační centrum (SOC). Následně je čtenář seznámen s problematikou zdrojů logů a platforem pro zjišťování informací o hrozbách. V poslední fázi teoretické části je shrnuta právní úprava kybernetické bezpečnosti vztahující primárně k území České republiky a Evropské unie včetně popisu doporučení organizace ENISA.

V rámci praktické části třetí kapitoly je provedena analýza vizualizačních šablon a technik, které lze použít při tvorbě webové aplikace. Jedná se o popis frameworku `Vue`, pomocí nějž je vyvíjena klientská část původní aplikace a také její rozšíření v podobě této práce pro zachování jednotnosti jazyků. Součást analýzy tvoří také zhodnocení kladů a záporů knihoven `D3.js`, `Bootstrap pro Vue` a `Vuetify`. Následně je provedeno srovnání vizualizačních technik bezpečnostní technologie SIEM a jeho produktů QRadar od společnosti IBM a NetWitness Platform od RSA.

Třetí kapitola se zaměřuje na popis návrhů a možných způsobů zobrazení Sigma pravidel ve webové aplikaci. Součástí návrhů jsou diagramy *Sankey*, *Sunburst* a interaktivní stromová struktura, které definuje knihovna `D3.js`. Mezi návrhy také patří tabulkové zobrazení, rozevírací nabídky a zobrazení pravidel v matici *ATT&CK*.

Čtvrtá kapitola se zaměřuje na samotnou implementaci vhodných vizualizačních technik, které vyplývají z třetí kapitoly, a na popis experimentálního prostředí pro vývoj webu a realizaci práce. Jedná se o popis realizace rozšíření klasické MITRE *ATT&CK* matice pomocí zvýraznění technik, které útoky využívají, dále o zobrazení uživatelských pravidel ve vertikální tabulkové struktuře seskupených dle zdrojů dat. Kapitola implementace obsahuje také popis statistické tabulky a skupinového sloupcového grafu, které obsahují hodnoty procentuálních počtů vykonaných útoků na jednotlivé ekonomické sektory za období červen 2022–2023. Graf je realizovaný pomocí knihovny `D3.js` a zobrazení uživatelských pravidel je provedeno obdobným způsobem jako v matici *ATT&CK*. Součástí je také popis realizace interaktivní tabulky pro získání informací o skupinách hrozeb APT a zobrazení používaných taktik a technik a registrovaných uživatelských pravidel v horizontální stromové struktuře.

Pátá a poslední kapitola popisuje testování aplikace z pohledu uživatele a tedy i klientské části aplikace. Byl vymyšlen scénář, který může sloužit také jako návod pro pohyb a získávání informací napříč různými pohledy realizované v rámci této práce.

1 Základy kybernetické bezpečnosti

Kybernetická bezpečnost není pouze pojem v počítačovém průmyslu. Dá se chápat jako sada procesů, postupů a technologických řešení, které zvyšují stupeň ochrany systémů a sítí před digitálními útoky. Počty kybernetických útoků se každým rokem rapidně zvyšují. Útočníci na dnešní dobu rychle se vyvíjejících moderních technologií reagují neustálým rozvojem a zdokonalováním nástrojů a metod, které mají za cíl např. odcizit data, poškodit pověst firmy, získat finanční prostředky nebo oběti jinak uškodit. [1]

Začátek kapitoly bude věnován vysvětlování základních pojmů z oblasti kybernetické bezpečnosti, které jsou nezbytné pro porozumění probíraného tématu. V další části bude vysvětlena problematika kybernetických útoků a budou popsány různé způsoby, jak na kybernetický útok nahlížet.

1.1 Základní pojmy

V úvodu kapitoly základy kybernetické bezpečnosti je klíčové se obeznámit s definicemi základních a často používaných termínů v oblasti kybernetické bezpečnosti. Výklad základních pojmů si klade za cíl zabránit problémům či nejasnostem při chápání obsahu textu a myšlenek v něm vyjádřených. Mezi základní termíny patří:

- Aktér hrozby (angl. *Threat Actor*) – jednotlivec nebo skupina lidí, kteří záměrně zneužívají slabá místa v systémech či sítích [2].
- Aktivum (angl. *Asset*) – cokoliv, co chce jednotlivec, organizace nebo veřejná správa chránit [3].
- Bezpečnostní událost (angl. *Security Event*) – aktivita, která může vést k ovlivnění informačních systémů, technologií a pravidel, které jsou definovány k jeho ochraně [3].
- Severita události (angl. *Event Severity*) – udává míru vlivu nežádoucí události na bezpečnost informačních systémů. Severitu dělíme do pěti úrovní, které stručně shrnuje následující tabulka 1.1. [4]

Tab. 1.1: Srovnání závažností bezpečnostních událostí [4].

Úroveň	**Popis severity**
1	Kritický incident ovlivňující významnou část infrastruktury.
2	Významný incident ovlivňující omezený počet systémů.
3	Incident způsobuje chyby nebo velké zatížení systému.
4	Incident způsobuje menší problémy s chodem služby.
5	Nedostatky vedoucí k málo závažným problémům.

- Bezpečnostní hrozba (angl. *Security Threat*) – možná příčina nechtěné události, která může způsobit znehodnocení systému a jeho předmětů ochrany [3].
- Bezpečnostní incident (angl. *Security Incident*) – porušení nebo stav ohrožení bezpečnostních politik, pravidel a standardů využívaných v oblasti informačních a komunikačních technologií [3].
- Zranitelnost (angl. *Vulnerability*) – chyba či slabé místo v systému nebo zařízení, které může být zneužito aktérem hrozby k vykonání škodlivých aktivit [3].
- Riziko (angl. *Risk*)– pravděpodobnost, že hrozba zneužije zranitelnosti aktiva [3].
- Zneužití (angl. *Exploit*) – zneužití známé zranitelnosti systému [3].
- Průnik (angl. *Impact*) – jedná se o důsledek útoku, o němž mluvíme v případě úspěšného poškození či ztráty aktiv [5].
- Škodlivý kód (angl. *Malware*) – je obecně veškerý kód nebo jeho část, který je nebezpečný pro systémy. Hlavními důvody tvorby škodlivých kódů jsou krádeže, zašifrování, změny, smazání dat nebo jiné poškození jakýchkoliv jiných aktiv [6].
- Plocha útoku (angl. *Attack Surface*) – popisuje celou škálu slabin a zranitelností systému, které může útočník zneužít [5].

1.2 Perspektivy pohledu na kybernetické útoky

Na začátek je důležité zmínit, co je to kybernetický útok. Kybernetický útok (angl. *Cyber Attack*) je jakákoliv nežádoucí aktivita cílená na IT (angl. *Information Technology*) infrastrukturu, která se zaměřuje obecně na poškození či odcizení aktiv [3]. Poškození dat může mít mnoho podob. Protože aktivem nemusí být pouze informace nebo data, můžeme k tomuto termínu zařadit i poškození reputace organizace, digitální vydírání, znemožnění fungování systémů, krádež identity a mnoho dalších kyberkriminálních činů.

Dělení kybernetických útoků může být nejednotné. Existuje však rozdíl mezi vnitřním a vnějším útokem, mezi fyzickým a programovým útokem a mezi aktivním a pasivním útokem. Vnitřní útok, jak již název napovídá, je útok proveden zevnitř infrastruktury, může se jednat o sabotáž, či porušení bezpečnostních politik organizace zaměstnancem. Vnější útok je prováděn aktérem hrozby z vnějšku organizace s cílem získat přístup dovnitř organizace, či provádět odposlech. Fyzickým útokem může být např. vloupání se k hmotným prvkům infrastruktury organizace. Naopak programovým útokem lze rozumět např. vzdálené připojení do systému a distribuci škodlivého kódu. Pod pojmem aktivní útok si lze představit např. modifikaci přenášených zpráv, odepření služby, či tzv. APT (angl. *Advanced Persistent Threat*) neboli trvalá významná hrozba. Obvykle se jedná o krádež dat, při čemž útočník

zůstává dlouhý čas v infrastruktuře organizace neodhalen. Naopak pasivním útokem lze chápat např. odposlouchávání dat, analýzu síťového provozu nebo dnes hojně využívané sociální inženýrství. Pro většinu informačních systémů a organizací jsou všechny typy útoků nepřijatelné, všechny totiž mohou vést k zisku důvěrných informací. [7, 8]

Na základě veřejně dostupných informací Národního úřadu pro kybernetickou a informační bezpečnost (zkr. *NÚKIB*) byla vypracována statistika počtu vykonaných kybernetických útoků nahlášených organizaci NÚKIB za první tři kvartály roku 2022 a 2023 a přehled procentuálního zastoupení jednotlivých typů těchto útoků za první tři kvartály roku 2023. Realizované kybernetické útoky se vztahují výhradně na území České republiky. Statistiky jsou ilustrovány pomocí grafů 1.1 a 1.2.

Na kybernetické útoky je možné nahlížet z různých perspektiv a to z pohledu hodnoty digitálních stop tzv. IOC (angl. *Indicator of Compromise*) pro útočníka, které ilustruje obrázek 1.3 a model *Pyramid of Pain*, a z pohledu, co předchází samotnému útoku a jak aktér hrozby postupuje, zobrazuje obrázek 1.4 a modely *Cyber kill chain* a MITRE *ATT&CK*. [12, 17]

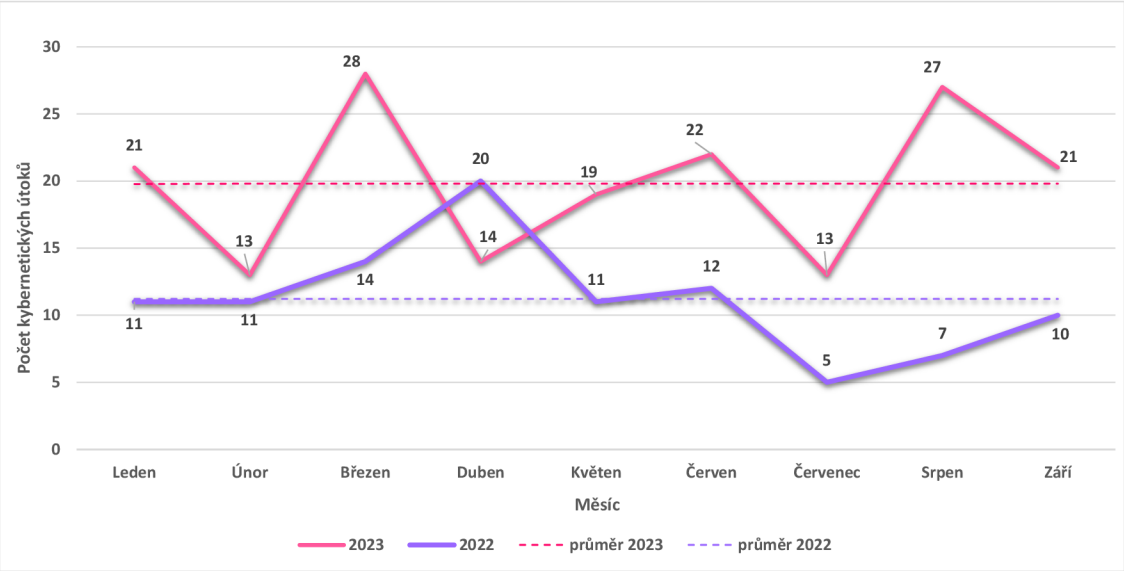
Nejčastější kybernetické útoky

Z grafu 1.1 je patrné porovnání počtu realizovaných kybernetických útoků na Českou republiku za první tři kvartály roků 2022 a 2023. Je patrné, že kvantita kybernetických útoků rapidně narůstá. V roce 2022 bylo v průměru vykonáno 11 útoků za měsíc, v roce 2023 se průměrná čísla zvětšila o celých 9 útoků za měsíc.

Nejčastější typy realizovaných útoků[1] ilustruje graf 1.2, z něj je patrná dominance útoků na dostupnost služby, které se pohybují okolo 64 % ze všech vykonaných útoků. Další významné zastoupení zde mají útoky na informační bezpečnost, využití škodlivého kódu a průnik do systému organizace, všechny mají zastoupení v průměru okolo 10 %. Méně významné zastoupení mají i škodlivé aktivity jako pokus o průnik do systému, podvod a sběr informací, tyto aktivity se vyskytují v průměru kolem 1 % případů. Následně jsou popsány nejpoužívanější techniky útoků:

- Dostupnost služby – tento útok cílí primárně na významné snížení či úplné odepření dostupnosti služby. Lze jej realizovat vyčerpáním šířky pásma sítě nevyžádaným provozem z jednoho systému tzv. *Denial of Service* (zkr. DoS) nebo z mnoha systémů tzv. *Distributed Denial of Service* (zkr. DDoS). Aktéři hrozeb mohou cílit na webové stránky (včetně internetového bankovnictví), e-mailové služby či na DNS (angl. *Domain Name System*) servery. Hlavní technikou k obraně před těmito útoky je filtrování síťového provozu. [9]

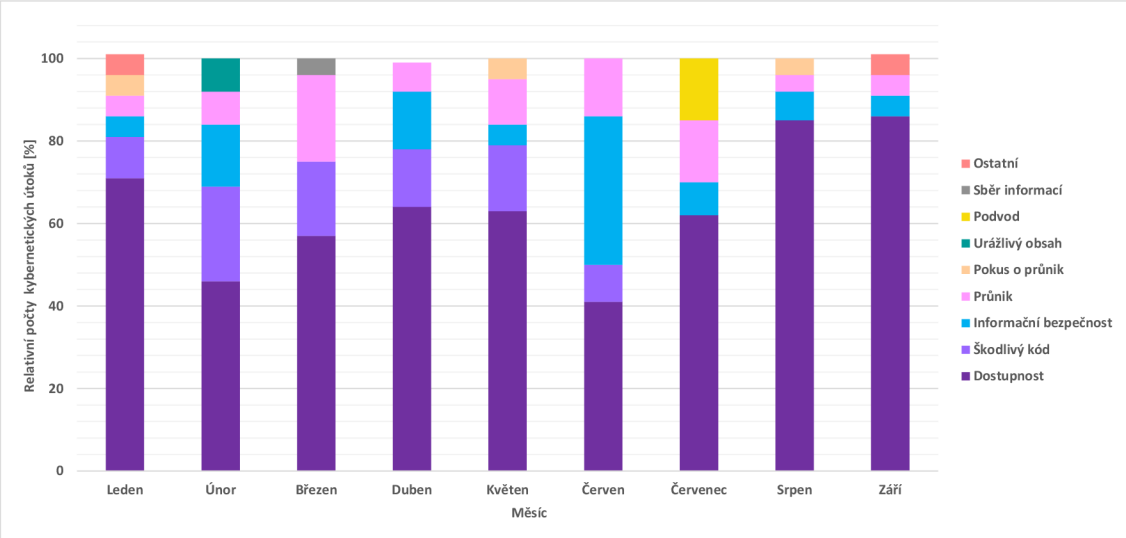
[1] Na výše zmíněné typy útoků nelze pohlížet separátně. Např. podvod, či škodlivý kód mohou způsobit průnik do systému.



Obr. 1.1: Srovnání počtu kybernetických útoků nahlášených NÚKIB za první tři kvartály roku 2022 a 2023 [16].

- Informační bezpečnost – útoky na informační bezpečnost lze rozumět neautorizovaný přístup k datům nebo neautorizované změny informací. Tento typ útoku se nazývá útok mužem uprostřed (angl. *Man-in-the-Middle*). V rámci tohoto útoku dochází k narušení bezpečnosti komunikace a útočník se dostane do prostoru mezi odesílatele a adresáta bez jejich vědomí. Útočník je pak schopen komunikaci odposlouchávat či data pozměnit. Nejčastějšími typy útoku mužem uprostřed jsou zachycení a sledování provozu v síti, otrava ARP (angl. *Address Resolution Protocol*) protokolu nebo otrava DNS záznamů. [10]
- Škodlivý kód – obecně škodlivé kódy zastřešuje termín *malware*, jejichž cílem je poškodit nebo zneužít zařízení, službu, síť či identitu uživatele. Jedním z mnoha možných způsobů distribuce škodlivých kódů je dnes velmi rozšířený *phishing*. *Phishing* je typ sociálního inženýrství, který k distribuci škodlivých kódů používá e-mail, textové zprávy či přímo hlasové hovory. [1]

  Existuje mnoho druhů škodlivých kódů, některé z nich jsou popsány níže [11]:
  - viry – ke svému šíření potřebují lidskou součinnost,
  - červi – mají schopnost sami se rozmnožovat v infikovaném systému,
  - *ransomware* – škodlivý kód spuštěný v oběti systému zašifruje data a požaduje za dešifrování výkupné,
  - trojské koně – vydávají se za legitimní aplikace, ale ve skutečnosti mohou provádět na pozadí škodlivé aktivity,
  - *adware* – nabízí uživatelům nevyžádané reklamy.



Obr. 1.2: Procentuální vývoj počtu kybernetických útoků hlášených NÚKIB za první tři kvartály roku 2023 [16].

Pyramid of pain

Model tzv. pyramidy bolesti zobrazuje vztah mezi typy IOC, které bezpečnostní týmy mohou použít k identifikaci hrozby, a mírou bolesti, která je útočníkovi způsoba odhalením jednotlivých typů indikátorů [12]. Model je strukturován do tvaru pyramidy, v jejíž spodní části se nachází indikátory snadné k provádění jejich změn jako jsou hodnoty hash funkcí, IP adresy nebo doménová jména. Vyšší části pyramidy už zobrazují indikátory nejsložitější a nejkomplexnější na jejich změnu jako jsou nástroje a TTP (angl. *Tactics, Techniques, and Procedures*) [13]. V následujícím obrázku 1.3 jsou vyobrazeny jednotlivé úrovně pyramidy bolesti. Úrovně pyramidy lze rozdělit na dvě kategorie – tradiční a behaviorální IOC. Vysvětlení jednotlivých indikátorů pyramidy bolesti [12, 13]:

- **Tradiční indikátory** jsou takové údaje, které se zjišťují z incidentu [14].
  - **Hashovací funkce** poskytují jedinečné hodnoty jednotlivým souborům tzv. otisky. Pro bezpečnostní týmy je získat tyto identifikátory stejně snadné jako pro aktéra hrozby. Protože jsou kryptografické hashovací funkce deterministické a velmi citlivé na změnu, může útočník otisk snadno změnit, a proto samotné odhalení hodnoty hashovací funkce souboru spjatého s incidentem není jediný indikátor, který musí analytik zvážit při odhalování a zastavení útoku. Příkladem hashovací funkce je rodina SHA (angl. *Secure Hash Algoritm*) nebo MD5 (angl. *Message-Digest Algoritm*).
  - **IP adresy** (angl. *Internet Protocol address*) jsou jedním z nejběžnějších

IOC. Obrana systému založená pouze na odmítnutí určitých IP adres není dostatečná. Adresy lze jednoduše měnit či skrýt např. pomocí VPN (angl. *Virtual Private Network*) tunelu nebo pomocí anonymního proxy serveru.

  - **Doménová jména** je ve srovnání s IP adresami obtížnější měnit, ale není to nemožné. Existují služby jako DDNS (angl. *Dynamic Domain Name System*) a DGA (angl. *Domain-Generated Algorithms*), které umožňují upravovat doménová jména pomocí rozhraní API[2] (angl. *Application Programming Interface*).

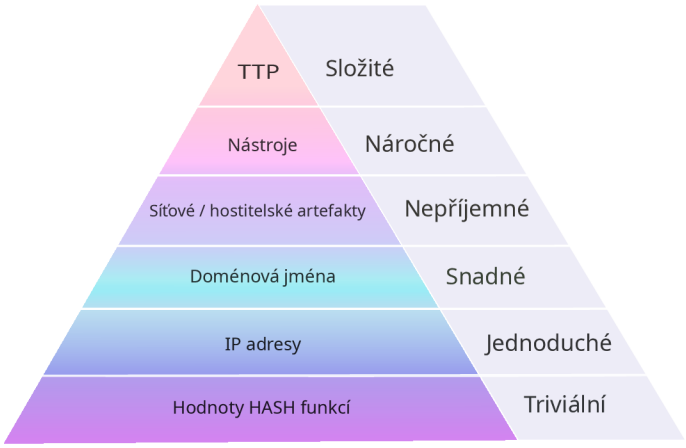
- **Behaviorální indikátory** kombinují další pokročilejší ukazatele, aby byl bezpečnostní analytik schopný vytvořit celkový obrazec škodlivého chování [14].
  - **Síťové/hostitelské artefakty** (angl. *Network/Host Artifacts*) aktivit pomáhají bezpečnostním týmům určit rozdíl mezi běžným a škodlivým provozem v síti či v hostitelském systému. Může se jednat o vzory URL (angl. *Uniform Resource Locator*) adres, příkazové a řídící informace, objekty registru, adresáře a taky soubory. Odmítnutí síťových/hostitelských artefaktů může útok podstatně zpomalit.
  - **Nástroje** (angl. *Tools*) pro realizaci útoku aktérem hrozby se stávají stále více sofistikovanějšími. Pomocí různých nástrojů zvyšují útočníci pravděpodobnost úspěchu svého útoku. Takové nástroje mají za cíl např. skenovat zranitelnosti v systémech, tvořit a nasazovat škodlivé kódy nebo provádět útoky hrubou silou na slabou autentizaci za účelem odcizení přihlašovacích údajů. Vypořádání se s odhalením a odepřením použití nástrojů je pro útočníka velmi náročné.
  - **TTP** (angl. *Tactics, Techniques and Procedures*) neboli taktiky, techniky a procedury popisují ucelený komplex metod útočníka počínaje jeho chováním a konče způsoby aplikování chování na útok. Organizace, které se dokáží bránit na tomto stupni, jsou schopny přímo čelit praktikám útočníka jako celku. Zároveň schopnost obrany na stupni TTP představuje pro aktéra hrozby velkou překážku a podstatně se snižuje pravděpodobnost úspěchu útoku.

Cyber kill chain

Model *Cyber Kill Chain*[3], nazývaný též jako životní cyklus kybernetických útoků, popisuje jednotlivé fáze kybernetického útoku, ve kterých mohou bezpečnostní týmy odhalit útočníka a hrozbu zvrátit. Tento model ilustruje obrázek 1.4. Nejčastěji se

[2] API je propojení různých aplikací, aby spolu mohly komunikovat. [15]

[3] Původní podobu sedmivrstvého modelu vyvinula společnost *Lockheed Martin* v roce 2011. [18]



Obr. 1.3: Pyramid of pain [12].

tento model používá k obraně proti hrozbám APT jako je např. *ransomware*, trojské koně, *spoofing* a techniky sociálního inženýrství. Původní model životního cyklu útoku měl sedm fází. Protože jsou kybernetické útoky neustále vyvíjeny a rozšiřovány, vznikl tak model obohacený o osmou fázi – monetizaci. Každá fáze modelu souvisí s konkrétním typem aktivity v rámci kybernetického útoku nezávisle na tom, zda se jedná o vnitřní nebo vnější typ útoku. Vysvětlení jednotlivých fází modelu *Cyber Kill Chain* [17, 18]:

1. **Průzkum** (angl. *Reconnaissance*) – je první fáze, kdy aktéři hrozeb začínají identifikovat cíle útoku, určovat zranitelnosti v systémech oběti, zkoumat potenciální vstupy do systému a plánovat útok. Čím více informací dokáže útočník nasbírat, tím se může zvyšovat pravděpodobnost úspěchu útoku.
2. **Příprava** (angl. *Weaponization*) – ve druhé fázi vytváří aktér hrozby vektor útoku[4]. Útočník zde také vyvíjí maximální úsilí, aby snížil pravděpodobnost odhalení bezpečnostním řešením.
3. **Doručení** (angl. *Delivery*) – v této fázi aktér hrozby zahajuje útok proti vybranému cíli. Může se jednat o zprostředkování vektoru útoku např. odesláním škodlivé přílohy e-mailu. Pro zvýšení pravděpodobnosti úspěchu se doručování kombinuje s technikami sociálního inženýrství.
4. **Zneužití** (angl. *Exploitation*) – ve čtvrtém kroku aktér hrozby spustí škodlivý kód v systému oběti. Mezi běžné příklady zneužití patří např. skriptování, ovládání lokálního plánování úloh nebo dynamická výměna dat.
5. **Instalace** (angl. *Installation*) – je fáze přicházející bezprostředně po fázi zneužití. Tehdy útočník přímo instaluje vektor útoku do systémů oběti. V této fázi končí aktivity příprav a útočník vstupuje do systému oběti a začíná nad

[4]Vektor útoku je způsob, kterým útočník zneužívá zranitelnost [3].

ním přebírat kontrolu. Může si také vytvořit tzv. zadní vrátka, aby mohl stále se systému oběti přistupovat.

6. **Ovládání** (angl. *Command and Control*) – během šesté fáze útočník používá svůj vektor útoku nainstalovaný v systému oběti ke vzdálenému ovládání zařízení. Aktér hrozby se také může v zařízení či síti pohybovat laterálně, aby nebyl bezpečnostními prvky odhalen a vytvořil si další místa pro vstup do oběti.
7. **Akce** (angl. *Actions on Objective*) – aktér hrozby podniká závěrečné kroky, které souvisí se záměrem útoku. Běžně se jedná o odcizení, zničení, zašifrování nebo o nezákonné rozmnožování a rozšiřování dat.
8. **Monetizace** (angl. *Monetization*) – v poslední fázi se útočníci zaměřují na získávání finančních příjmů z úspěšně provedeného útoku. Může se jednat o různé formy vydírání, výkupného či prodej citlivých informací na temném webu[5]. Fáze monetizace však nemusí být přítomná u všech typů kybernetických útoků.

Obr. 1.4: *Cyber kill chain* [20].

MITRE *ATT&CK*

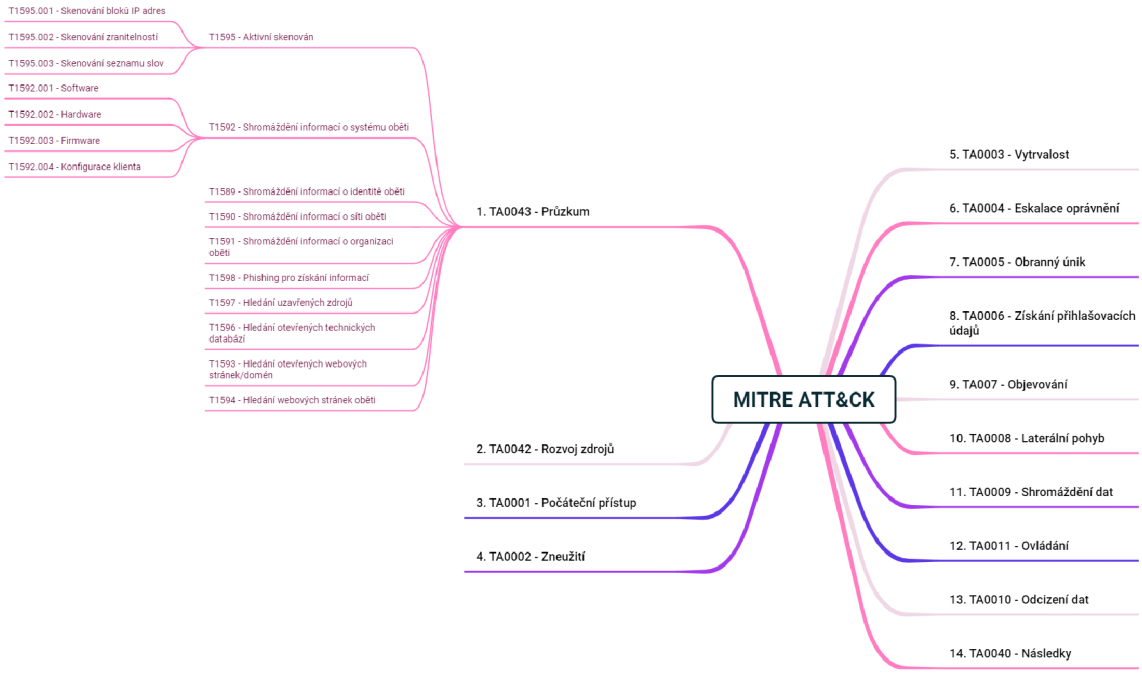
Rámec MITRE *ATT&CK*[6] (angl. *Adversarial Tactics, Techniques and Common Knowledge*) je veřejně dostupná znalostní databáze obsahující popis taktik a technik, které útočníci využívají v reálném světě k realizaci svých kybernetických útoků. Jedná se o behaviorální model, který obsahuje [23]:

[5]Temné weby jsou překryvné sítě, které využívají internet, ale dostat se na ně lze pouze pomocí speciálních programů [19].

[6]Rámec MITRE *ATT&CK* vyvinula společnost MITRE v roce 2013 za účelem pomoci organizacím porozumět problematice zabezpečení systémů a odhalit jejich zranitelnosti [21].

- **taktiky**, které popisují krátkodobé cíle útočníka,
- **techniky**, které označují způsoby, jak lze dosáhnout taktických cílů,
- **dílčí techniky**, které popisují konkrétní způsoby, jak útočníci dosahují taktických cílů.

Taktiky, techniky a dílčí techniky jsou zobrazeny jako sady datových matic. Ukázka struktury *ATT&CK* matice je vyobrazena na obrázku 1.5. Každá taktika, technika i dílčí technika má svůj jedinečný identifikátor. Identifikátory taktik se skládají z písmen „TA“ a čtyřmístného celočíselného kódu (např. taktika průzkum TA0043). Identifikátory technik mají podobnou strukturu jako identifikátory taktik, liší se pouze úvodním písmenem „T“ namísto „TA“ (např. technika aktivní skenování T1595). Dílčí techniky nesou stejný základ identifikátoru jako nadřazené techniky, pouze se k němu z pravé strany připojuje další třímístný kód. Tento kód dílčí techniky začíná hodnotou 001 a u dalších dílčích technik se vždy inkrementuje o hodnotu 1 (např. dílčí technika skenování bloků IP adres T1595.001). [21]



Obr. 1.5: Ukázka struktury matice MITRE *ATT&CK* [25].

Součástí znalostní báze *ATT&CK* je technická dokumentace, ve které lze najít podrobné informace o jednotlivých taktikách, technikách i dílčích technikách. Dokumentace poskytuje bezpečnostním týmům a organizacím ucelený pohled na různé formy kybernetických hrozeb. Celistvost pohledu na kybernetické hrozby podporují doporučení, jakými způsoby lze hrozby detekovat a případně zmírnit jejich následky. Také principy detekce a mitigace mají své unikátní identifikátory. Ty se liší počá-

tečními písmeny – detekce začíná písmeny „DS“ a mitigace písmenem „M“. U obou identifikátorů následuje celočíselný čtyřmístný kód. Např. technika aktivní skenování má doporučení pro detekci „DS0029“ a pro mitigaci „M1056“. [25]

Model *ATT&CK* definuje matice pro různé technologické domény, ty specifikují prostředí, ve kterých útoky probíhají. V rámci každé domény pak rámec definuje jednotlivé platformy, což jsou systémy, které útočník reálně používá. Platformou může být operační systém či aplikace. Souhrn technologických domén a jejich platforem lze nalézt v tabulce 1.2. V současné době je model zdokumentován pro tři typy domén. [26]

Tab. 1.2: Technologické domény *ATT&CK* modelu a jejich platformy [23].

Technologická doména	**Platforma**
Podnikové sítě a internetové úložiště	PRE[7], Windows, MacOS, Linux, internetové úložiště, síť a kontejnery
Mobilní telefony	Android, iOS
Průmyslové řídící systémy	–

Počet taktik v rámci *ATT&CK* modelu se liší v závislosti na konkrétní technologické doméně. Doména pro podnikové a internetové úložiště popisuje celkem 14 taktik, doména pro mobilní telefony a doména pro průmyslové řídící systémy popisují celkem 12 taktik, které ale nejsou zcela totožné [25]. V rámci této práce budou popsány taktiky domény podnikové a internetového úložiště[8]. [21, 24]:

1. **Průzkum** (angl. *Reconnaissance*) – útočník si mapuje prostředí oběti a shromažďuje informace pro budoucí útok. Mezi poptávaná data mohou patřit informace o zaměstnancích (jejich pracovní pozice, kontaktní údaje či přihlašovací údaje), informace o infrastruktuře organizace a další podrobnosti.
2. **Rozvoj zdrojů** (angl. *Resource Development*) – protivník vytváří, nakupuje nebo krade zdroje, které může použít v dalších fázích jako jsou např. zakoupení doménových názvů, vytvoření e-mailových účtů nebo krádež certifikátů.
3. **Počáteční přístup** (angl. *Initial Access*) – aktér hrozby se snaží proniknout do sítě oběti zneužitím systémových zranitelností či cíleným *phishing* útokem.
4. **Zneužití** (angl. *Execution*) – útočník spouští škodlivý kód v systému oběti pomocí lokálního nebo vzdáleného přístupu.
5. **Vytrvalost** (angl. *Persistence*) – je taktika, při níž se útočník snaží přetrvat v systému oběti i po provedení akcí jako je restartování systému, změna přihlašovacích údajů a dalších zásahů, které by mohly přerušit útočníkovi přístup do

[7]PREATT&CK dokumentuje chování protivníka ve fázích průzkumu a rozvoji zdrojů. Je nezávislý na konkrétní technologii [23].

[8]Zobrazení všech *ATT&CK* matic lze nalézt na stránce: `https://attack.mitre.org/`.

systému. Mezi takové techniky patří např. přidání části kódu do spouštěcího kódu.

6. **Eskalace oprávnění** (angl. *Privilege Escalation*) – protivník se snaží navýšit svá práva v rámci systému oběti, aby mohl podnikat širší spektrum aktivit. Toho může dosáhnout využitím systémových zranitelností, či zneužitím chybné konfigurace systému.
7. **Obranný únik** (angl. *Defense Evasion*) – útočník se nadále snaží vyhnout svému odhalení. Tato taktika zahrnuje techniky jako je deaktivace bezpečnostních programů, šifrování dat a probíhajících skriptů nebo využívání legitimních procesů k zamaskování svého škodlivého kódu.
8. **Získávání přihlašovacích údajů** (angl. *Credential Access*) – aktér hrozby podniká kroky nezbytné k odcizení názvů účtů a jejich hesel, to mu poskytuje legitimně vyhlížející přístup do systémů. Přihlašovací údaje lze zjistit pomocí technik zaznamenávání úderů do klávesnice nebo získáním hesel, které jsou uložené v operačním systému nebo jiné aplikaci.
9. **Objevování** (angl. *Discovery*) – útočník mapuje systém oběti zevnitř. To umožňuje útočníkovi nabýt vědomosti o nejatraktivnějších cílech, které lze ovládat.
10. **Laterální pohyb** (angl. *Lateral Movement*) – protivník se pohybuje systémem oběti s cílem pozorovat jeho primárního cíl, k tomu často bývá zapotřebí pohyb přes několik systémů či účtů. K pozorování svého cíle mohou využívat vlastní nástroje nebo výchozí dostupné nástroje sítě a operačního systému, které mohou být hůře odhalitelné.
11. **Shromáždění dat** (angl. *Collection*) – útočník shromažďuje relevantní informace o svém cíli, které následně odcizí. Pro shromažďování dat se využívají různé typy disků, internetové prohlížeče, použití mikrofonu a kamer a e-mailová komunikace.
12. **Ovládání** (angl. *Command and Control*) – Aktér hrozby komunikuje s napadenými systémy za účelem jejich ovládnutí. Následně se snaží zamaskovat svůj škodlivý provoz za legitimní provoz, aby se vyhnul odhalení.
13. **Odcizení dat** (angl. *Exfiltration*) – útočník pracuje na krádeži dat, které získal ze systému své oběti, takový přenos často zahrnuje kompresi dat a šifrování, aby se vyhnul svému odhalení.
14. **Následky** (angl. *Impact*) – v závěru se protivník snaží snížit dostupnost systému či služeb, narušit integritu dat či úplně zničit systémy oběti. Poškodit data může např. pomocí útoku *ransomware* viz kapitola 1.2.

Porovnání modelů *ATT&CK* a *Cyber Kill Chain*

Oba modely se používají k detekci a obraně proti kybernetickým útokům, mají však mezi sebou významné rozdíly. Model *Cyber Kill Chain* primárně umožňuje organizacím porozumět jednotlivým fázím průběhu kybernetických útoků. *Cyber Kill Chain* nebere také v úvahu útoky na internetová úložiště (cloud), předpokládá klasické doručení z vnějšku systému. Další nevýhodou *Cyber Kill Chain* modelu je, že jeho fáze se zaměřují na chování síťových útoků, ale nepopisují útoky na cílové stanice. [21, 22]

Zatímco rámec *ATT&CK* poskytuje komplexní pohled na taktické cíle útočníků a jak těchto cílů dosahují. Model *ATT&CK* je pravidelně aktualizován a zahrnuje informace o používaných nástrojích a hrozbách spojených s každou taktikou a technikou. Také poskytuje informace o jednotlivých aplikacích a operačních systémech, které obsahují slabinu zneužitelnou konkrétním vektorem útoku. Překonává tedy omezení modelu *Cyber Kill Chain*.[21]

1.3 Detekce a prevence kybernetických incidentů

Kromě prevence vzniku kybernetických incidentů je také důležité zajistit jejich detekci. Detekce kybernetických incidentů je proces monitorování událostí v počítačovém systému. [27]

V této kapitole jsou popsány způsoby detekce a prevence vzniku kybernetických incidentů a často používané nástroje a technologie pro zajištění komplexní kybernetické bezpečnosti systému.

1.3.1 Systém detekce průniku

IDS (angl. *Intrusion Detection System*) je specifický typ zařízení nebo softvér, který má za úkol monitorovat síťový provoz za účelem detekce škodlivých aktivit. Obecně nalezené škodlivé aktivity bývají shromažďovány pomocí centrálního systému správy informací. Existuje mnoho typů IDS systémů. Může se jednat o antivirový program či komplexní vrstvené monitorovací systémy. Typy IDS se liší podle toho, které části infrastruktury monitorují. Systém NIDS (angl. *Network Intrusion Detection Systems*) detekuje narušení a monitoruje provoz v síti. IDS lze implementovat i přímo na koncovém zařízení, jedná se o tzv. HIDS (angl. *Host Intrusion Detection Systems*). Systém IDS lze také umístit před server a monitorovat provoz proudící ze zařízení a zpět, jedná se o systém detekce průniku založený na protokolu, tzv. PIDS (angl. *Protocol-based Intrusion Detection Systems*). Systémy IDS jsou založeny na dvou typech detekcí [28, 30]:

- **Detekce na základě signatur** odhaluje hrozby pomocí hledání konkrétních vzorů (podobností). Takovými vzory mohou být např. známé sekvence škodlivých instrukcí, které využívají známé útoky. Nevýhodou detekce na základě signatur je, že není schopná odhalit nové neznámé typy útoků.
- **Detekce na základě sledování anomálií** je novější způsob detekce, který dokáže odhalit i neznámé typy škodlivých kódů. Tato metoda využívá strojové učení k vytvoření tzv. modelu důvěryhodné aktivity. Není však stoprocentně spolehlivá, může generovat velké množství falešných poplachů, protože neznámá ač legitimní aktivita může být označena za škodlivou.

1.3.2 Systém prevence průniku

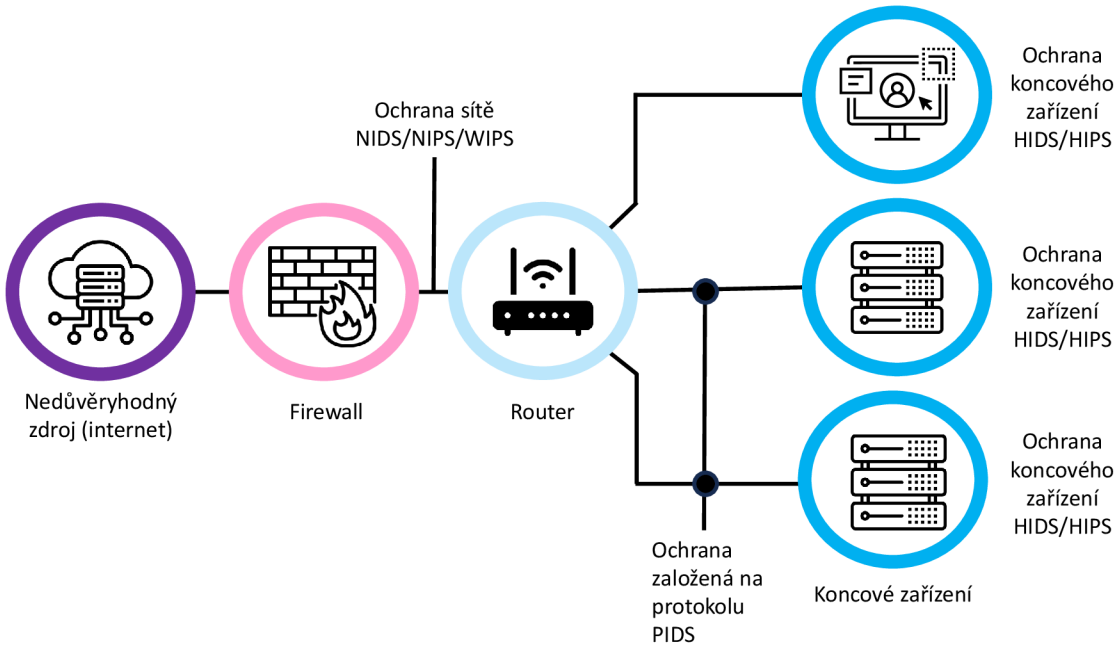
IPS (angl. *Intrusion Prevention System*) je systém umožňující zabezpečení sítě, který zahrnuje její nepřetržitý monitoring. IPS má za úkol hledat škodlivé aktivity a podnikat konkrétní kroky potřebné k jejímu zabránění, např. blokování komunikace stanice se známou nebezpečnou webovou stránkou. IPS je tedy vyspělejší systém než IDS. Systém IPS podobně jako IDS používá techniky prevence útoku založené na signaturách, anomáliích a navíc monitorování na základě pravidel. Funkce IPS závisí na typu řešení. Může se jednat o síťový prevenční systém NIPS (angl. *Network-based Intrusion Prevention System*), který chrání síť před podezřelými aktivitami nebo jeho variantu chránící bezdrátovou síť WIPS (angl. *Wireless Intrusion Prevention System*). Samozřejmě ochrana je důležitá i pro koncová zařízení a tu zajišťuje systém HIPS (angl. *Host-based Intrusion Prevention System*). [29, 30]

1.3.3 Srovnání použití systémů IDS a IPS

IDS a IPS jsou nedílnou součástí zabezpečení systémů, sítí, aplikací a informací malých i velkých korporací. V procesu detekce jsou si podobné. Oba systémy totiž umožňují monitorování sítě a provozu, odeslání upozornění na detekovanou aktivitu, oba systémy se také dokáží učit, rozpoznat a následně minimalizovat falešné poplachy a také uchovávat záznamy o rozsahu a výsledcích monitorování, a tak usnadňují správci systému kontrolu nad provedenými činnostmi. [30]

Jak již bylo zmíněno v podkapitolách 1.3.1 a 1.3.2, systémy IDS a IPS se mohou nacházet různých částech infrastruktury. Jejich umístění ilustruje obrázek 1.6.

Ačkoliv mají mnoho vlastností společných, existují mezi IDS a IPS zásadní rozdíly, které shrnuje tabulka 1.3.



Obr. 1.6: Umístění typů systému detekce a prevence průniku v infrastruktuře [34].

Tab. 1.3: Srovnání systémů IDS a IPS [27, 30].

IDS	**IPS**
Systém pro detekování a monitorování	Systém pro detekování, kontrolu a prevenci
Posílá upozornění	Posílá upozornění a podniká kroky k zastavení hrozby
Nepodporuje kontrolu šifrovaných aktivit	Je vhodnější pro ochranu aplikací

1.3.4 Ostatní technologie pro zajištění ochrany kyberprostoru

Jak bylo znázorněno výše v podkapitole 1.3.3, detekční a prevenční systémy se mohou nacházet v různých částech infrastruktury. Na základě pozice systému v infrastruktuře lze rozlišit specifické technologie, které umožňují detekci a monitorování aktivit a ve většině případů i prevenci vzniku škodlivých aktivit. Tyto systémy dohromady tvoří komplexní bezpečnostní strategii organizací či jiných infrastruktur. Populární technologie jsou charakterizované v dalších částech kapitoly tak, jak bývají v praxi implementovány za sebou [42]:

1. EDR (angl. *Endpoint Detection and Response*)
2. XDR (angl. *Extended Detection and Response*)
3. ASM (angl. *Attack Surface Management*)
4. Log manažer (angl. *Log Manager*)

5. SIEM (angl. *Security Information and Event Management*)
6. NDR (angl. *Network Detection and Response*)
7. SOAR (angl. *Security Orchestration, Automation, and Response*)

EDR

EDR je nástroj, který umožňuje detekovat, vyšetřovat a reagovat na škodlivé aktivity prováděné na koncových zařízeních. Dokáže reagovat i na pokročilé kybernetické hrozby. EDR sbírá data o všech činnostech koncového zařízení, které souvisí se zabezpečením a které mohou být nezbytné k forenzní analýze[9]. Jedná se o sběr dat síťových připojení, spouštění procesů, načítání ovladačů, změn registrů, přístupů k disku a k paměti. EDR technologie také disponuje strojovým učením pro minimalizaci falešně pozitivních nálezů. [33]

XDR

XDR je komplexní bezpečnostní řešení, které umožňuje identifikovat, vyšetřovat a reagovat na pokročilé kybernetické hrozby. Hrozby mohou pocházet i z více zdrojů včetně cloudu, sítí a e-mailových služeb. XDR není jediný nástroj, který si zákazník koupí a implementuje. XDR totiž kombinuje stávající bezpečnostní řešení zákazníka a požadované rozšíření do jednoho celistvého bezpečnostního systému. Výhodou XDR je, že z jediného rozhraní poskytuje vyhledávání hrozeb napříč doménami a různých zdrojů hrozeb a je vhodný pro sběr dat k provedení forenzních analýz. [33]

ASM

Správa plochy vektorů útoků sestává z nepřetržitého monitorování, analýz a oprav softvérových zranitelností, které mohou tvořit útočnou plochu potenciálních vektorů útoků. ASM se provádí z pohledu aktéra hrozby, nikoli obránce. Má za úkol identifikovat potenciální cíle útočníka a vyhodnocovat rizika na základě šancí útočníka, jak snadno lze vybraný cíl kompromitovat. Řešení ASM z pohledu útočníka umožňuje bezpečnostním týmům (více viz kapitola 1.5.1) vytvářet proaktivní zabezpečení, které dokáže čelit rostoucímu a měnícímu se povrchu útoku. [41]

Log manažer

Organizace generují velké množství protokolových dat prostřednictvím sítí, systémů a uživatelů. To je také důvod k zavedení systematického procesu správy a monitorování

[9]Forenzní analýza je proces vyhledávání a interpretace digitálních dat pro trestní, obchodní, či soudní účely [32].

dat z různých souborů logů. Správce logů se tedy stará o shromažďování dat, jejich analýzu a ukládání. Data protokolů poskytují informace potřebné k odstraňování problémů, zlepšování výkonu systémů a monitorování zabezpečení. [46]

Podrobnější vysvětlení souboru logu, sběru logů a kategorizace zdrojů logů bude vysvětleno v kapitole 1.4.

SIEM

Technologie SIEM zajišťují detekci, vyhodnocení a reakci na kybernetické hrozby. Umožňují také sběr dat pro provedení forenzní analýzy, navrhovat pravidla bezpečnostní politiky a korelační pravidla. [39]

SIEM je komplexní systém, který se stará o řízení bezpečnosti [40]:

- **informací** – tzv. systém SIM (angl. *Security Information Management*) sbírá, analyzuje, ukládá systémové informace a nahlašuje problémy, které v nich nalezne;
- **událostí** – tzv. systém SEM (angl. *Security Event Manager*) monitoruje a koreluje události v reálném čase a okamžitě upozorňuje na aktuální bezpečností incidenty.

Podrobnější vysvětlení fungování řešení SIEM a pravidel bude následovat v kapitole 1.4.

NDR

Technologie NDR má za úkol identifikovat a zastavit síťové hrozby, které není možné detekovat pomocí známých vzorců útoků nebo signatur. NDR využívá prostředky strojového učení a behaviorální analýzu k monitorování síťových aktivit, které jsou potřebné k vytvoření obrazu standardního chování v síti. Následně umožňuje detekovat škodlivou aktivitu pomocí odchylek chování od naučeného normálu, tedy hledá anomální aktivity, které mohou být spojeny s aktivitou škodlivého kódu, laterálním pohybem či s odcizováním dat. [31]

SOAR

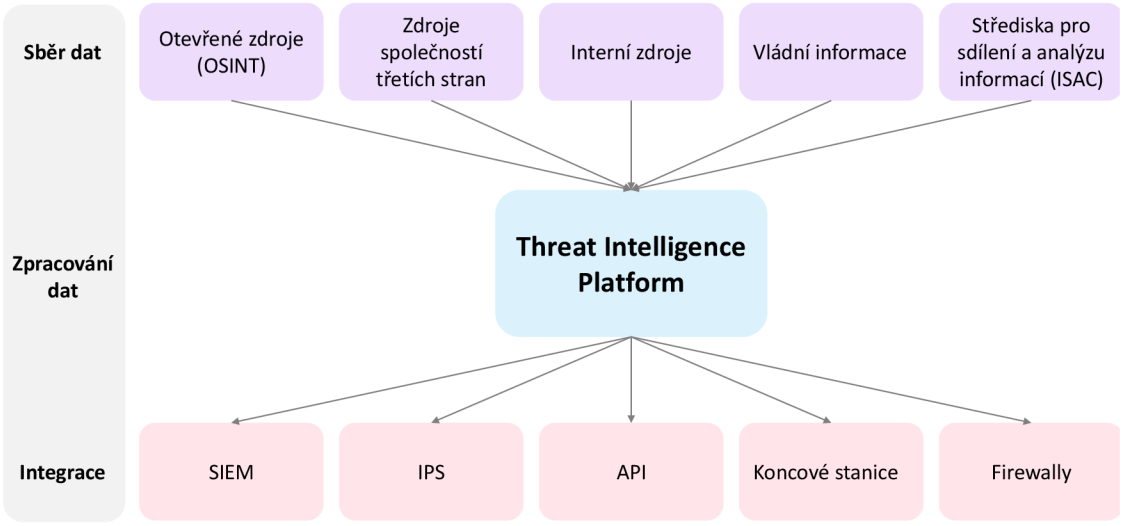
SOAR je pokročilý systém, který umožňuje shromažďovat informace o bezpečnostních hrozbách a reagovat na ně automaticky, tedy bez lidského zásahu. To snižuje potřebu ručních zásahů při řešení incidentů. Platformy SOAR výrazně zlepšují efektivitu bezpečnostních operací. Umožňují koordinaci, provádění a automatizaci úkolů v rámci bezpečnostních týmů a to všechno je k dispozici v jednom systému. [33]

1.3.5 Platformy pro zjišťování informací o hrozbách (TIP)

TIP (angl. *Threat Intelligence Platform*) pomáhají bezpečnostním týmům odhalovat nejnovější informace o hrozbách. TIP poskytují analytikům takové druhy informací, jejichž používání lze zautomatizovat, a tak usnadnit analytikům práci se shromažďováním a správou dat o hrozbách, jedná se např. o technické informace o hrozbách včetně jejich IOC, výsledky z analýz hrozeb provedené člověkem a další informace shromažďovanými lidmi za účelem kontroly podezřelých aktivit. TIP představuje technologické řešení, jehož princip je vyobrazen na obrázku 1.7 a má za úkol provádět [35]:

- **agregaci dat** neboli shromažďování informací o hrozbách z různých zdrojů v odlišných formátech. Informace mohou pocházet z otevřených zdrojů OSINT (angl. *Open Source Intelligence*), od společností třetích stran, z interních či vládních zdrojů a ze zdrojů středisek pro sdílení a analýzu informací (angl. *Information Sharing and Analysis Centers*). Mezi podporované formáty zdrojových dat patří např. STIX (angl. *Structured Threat Information eXpression*), TAXII (angl. *Trusted Automated eXchange of Intelligence Information*), JSON (angl. *JavaScript Object Notation*), XML (angl. *Extensible Markup Language*), email, CSV (angl. *Comma-separated Values*), textový formát, PDF (angl. *Portable Document Format*) a formát dokumentu *Microsoft Word*.
- **zpracování dat**, tento proces zahrnuje normalizaci dat neboli převádění dat z různých formátů do jednotné podoby, odstraňování duplicitních informací a obohacení dat, tedy zamezení hlášení falešně pozitivních nálezů.
- **integraci TIP do existujících bezpečnostních systémů** za účelem sběru informací o hrozbách a následného správného vyhodnocení událostí. TIP je možné integrovat do mnoha technologických řešení, např. SIEM, IPS a do zařízení jako jsou koncové stanice či *firewally*.
- **sdílení informací** o hrozbách, které napomáhají analytikům při analýze hrozby, pochopení kontextu a důsledků hrozby a při předvídání hrozeb.

Platformy TIP mohou být nasazovány jako SaaS (angl. *Software-as-a-Service*), tedy správa softvéru je zajišťována třetí stranou, nebo jako *on-premise* řešení, tedy správa platformy je řešena interně v rámci společnosti [36]. Kromě komerčních řešení existuje mnoho volně dostupných platforem pro získání informací o hrozbách, např. *AlienVault Open Threat Exchange, Open Cyber Threat Intelligence Platform* nebo *VirusTotal* [38].



Obr. 1.7: Princip fungování platforem *Threat Intelligence* [37].

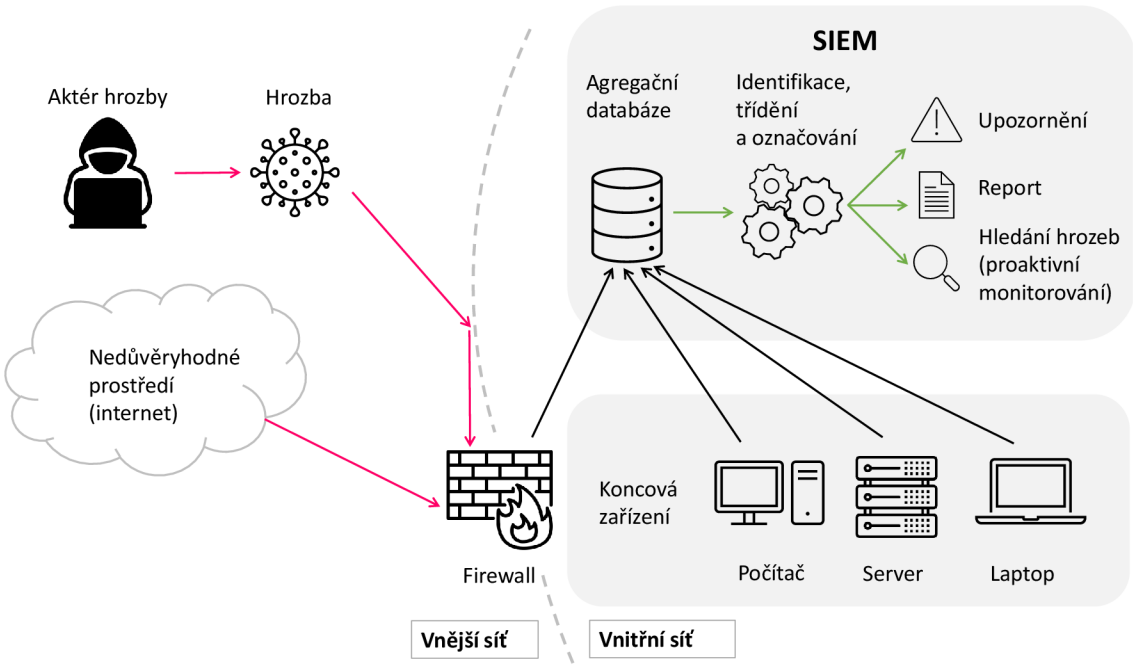
1.4 Řešení systémů SIEM

SIEM platformy zahrnují funkce shromažďování dat událostí a logů, která jsou vytvářena mnoha různými zdroji, např. aplikacemi, hostitelskými systémy či bezpečnostními zařízeními. Nasbíraná data často bývají v různých formátech, proto SIEM musí nejprve data normalizovat a následně je ukládá do centralizované databáze. Dále má za cíl nasbíraná data třídit a označovat, o jaká data se skutečně jedná, např. úspěšné přihlášení, aktivita škodlivého kódu, jiná bezpečnostní hrozba a mnoho dalších typů dat. SIEM řešení umožňují definovat korelační pravidla, která umožňují provádět nad databází událostí dotazy, a tak odhalovat související aktivity a také bezpečnostní hrozby. Pokud SIEM odhalí porušení bezpečnostních politik, vygeneruje oznámení pro bezpečnostní tým s informacemi o události a následně je na bezpečnostním týmu, aby událost prošetřil. Proces řešení systémů SIEM ilustruje obr. 1.8. [43, 44]

Sigma pravidla

V systémech SIEM se používají pravidla Sigma[10], která umožňují detekovat a odhalit anomálie ve sledovaném prostředí. Anomálie mohou vést ke vzniku bezpečnostního incidentu. Generalizovaná Sigma pravidla standardizují postupy detekce hrozeb a jsou multiplatformní, tzn. že nejsou závislé na konkrétní SIEM platformě.

[10]Sigma pravidla lze nalézt v knihovně na stránce: `https://github.com/SigmaHQ/sigma/tree/master/rules`.



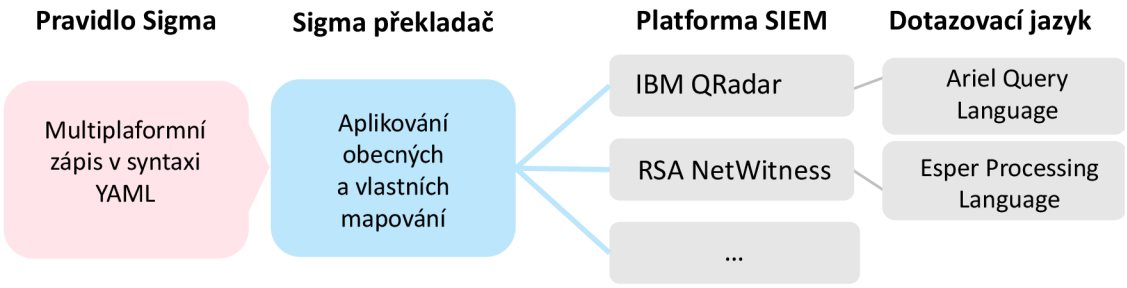
Obr. 1.8: Proces SIEM řešení [44].

Mezi platformy, které podporují pravidla Sigma lze zařadit např. IBM QRadar, RSA NetWitness, Splunk a mnoho dalších. [45]

Pravidla Sigma jsou psána ve formátu pro člověka čitelném a snadném na zápis. Jedná se o syntaxi YAML (angl. *YAML Ain't Markup Language*). Sigma může obsahovat různé prvky, nejčastějšími prvky jsou [45]:

- **Název** (angl. *Title*) je stručným a přesným popisem detekce.
- **Stav** (angl. *Status*) označuje fázi vývoje pravidla, např. experimentální, testování, apod.
- **Popis** (angl. *Description*) pravidla obsahuje vysvětlení, co má pravidlo dělat a detekovat.
- **Jméno autora** (angl. *Author*) pravidla.
- **Datum** (angl. *Date*) vytvoření pravidla.
- Jedinečný **identifikátor** (angl. *Id*) přiřazený konkrétnímu pravidlu.
- **Licenční podmínky** (angl. *License*), za kterých lze vytvořené pravidlo použít.
- **Úroveň závažnosti** (angl. *Level*) či priorita pravidla Sigma.
- **Zdroj dat** (angl. *Log Source*) označuje typy dat, na které se pravidlo vztahuje.
- **Podmínky** (angl. *Condition*), při jejichž splnění dojde k aktivaci pravidla.
- **Značky** (angl. *Tags*) lze využít např. k namapování pravidel na specifické techniky či dílčí techniky frameworku MITRE *ATT&CK*.

Pravidla Sigma lze implementovat do systému SIEM pomocí překladu[11] do dotazovacího jazyka, který používá konkrétní platforma SIEM (více viz podkapitola 2.2). Proces překladu zobrazuje obr. 1.9



Obr. 1.9: Proces překladu Sigma pravidel do jazyků SIEM platforem [50].

Na obrázku 1.10 je znázorněno vzorové pravidlo, které je přeložené do formátu jazyka EPL (angl. *Esper Processing Language*), který podporuje SIEM platforma NetWitness vendora RSA. Toto pravidlo se zaměřuje na detekci události, kdy dochází k odstranění politiky podmíněného přístupu neoprávněným subjektem. Bezprostředně po vzniku této události je vygenerováno upozornění.

```
@Name('os_win_mcsft_sact-audit_log_cleared')
    @Description('Alert is fired when Windows Audit log is cleared. We are
looking for the event id 517')
    @RSAAlert(oneInSeconds=0)
    SELECT * FROM Event(
            /* Statement: reference id which is generated during audit log
cleaning */
            (device_type IN ( 'winevent_nic' ) AND device_class IN (
'Windows Hosts' ) AND reference_id IN ( '517' ))
        );
```

Obr. 1.10: Vzorové pravidlo překonvertované do jazyka *Esper Processing Language*.

Kategorizace zdrojů logů

Před samotným popisem kategorizace zdrojů logů je nutné uvést, co je to soubor logu a jakým způsobem lze logy získávat. Soubor logu je automaticky generovaný datový soubor, který slouží jako zdroj podrobných informací o provedených aktivitách

[11] Převod Sigma pravidel do dotazovacích jazyků různých platforem SIEM lze provést v online prostředí: `https://uncoder.io/`.

v aplikacích, na serverech, v operačních systémech a jiných zařízeních či softvérech a to vše včetně časových razítek. Soubory logů mohou být tedy generovány jako informace o událostech různých zdrojů dat, které vypovídají o veškerých aktivitách prováděných různými systémy či uživateli systémů. [46]

Mezi monitorovaná zařízení se nejčastěji řadí přepínače, směrovače, přístupové body, *firewally*, servery (Windows, Linux), webové servery (Apache, Tomcat...), autentizační servery, hypervizory, kontejnery, aplikace, uživatelské stanice a mnoho dalších [47]. Řešení správy logů a řešení SIEM se mohou vzájemně doplňovat a v některých případech si mohou i konkurovat. SIEM systémy disponují integrovanou funkcí shromažďování logů z různých zdrojů do centrálního úložiště podobně jako log manažery. Hlavním rozdílem mezi systémy SIEM a log manažery je ten, že SIEM systémy se zabývají zpracováním, analýzou a filtrováním logovacích dat dříve, než se dostanou k uživateli. Zatímco log manažery poskytují přístup ke všem vygenerovaným datům v reálném čase, tedy log manažery nepotřebují tak velkou režii jako SIEM řešení. [48]

Určení zdroje logů v Sigma pravidlech je důležité pro správnost a účinnost SIEM detekcí.[12] Každá definice zdroje logů je v rámci Sigma pravidla popsána třemi poli [49]:

- kategorie (angl. *category*) – definuje výběr zdrojů logů zapsaných určitou skupinou produktů, např. *firewally*, webové servery, aplikace a další.
- produkt (angl. *product*) – používá se k výběru zdroje logů určitého produktu či systému, např. Windows, Linux, Azure, Cisco a mnoho dalších.
- služba (angl. *service*) – pomocí služby se blíže specifikují podmnožiny produktu. Může se jednat např. o specifické zdroje zabezpečení v produktu Windows.

1.5 Vyšetřování kybernetických útoků

V předchozích kapitolách byly popsány metody detekce (IDS), prevence (IPS) a komplexní systém řešení zajišťující i reakci na kybernetické incidenty (SIEM). Tato kapitola bude věnována vyšetřování událostí, na které upozorní systémy SIEM.

1.5.1 Bezpečnostní operační centrum (SOC)

O vyšetření a analýzu vygenerovaných upozornění čili ochranu aktiv se stará bezpečnostní operační centrum, tzv. SOC tým (angl. *Security Operation Center*). Investigace kybernetických incidentů si klade za cíl stanovit vektor útoku, dopad incidentu

[12]Kompletní přehled kategorizace zdrojů logů lze nalézt na stránce: `https://github.com/SigmaHQ/sigma-specification/blob/main/Taxonomy_specification.md#log-sources`.

na zasažený systém a zjistit další nezbytné informace ke stanovení odpovídající reakce. [51]

SOC týmy spadají do tzv. *blue* týmů, jejichž cílem je chránit sledované systémy proti škodlivým aktivitám. Dále existují tzv. *red* týmy, neboli týmy provádějící penetrační testování za účelem testování zabezpečení organizace nebo jiného sledovaného prostředí. Posledním týmem je tzv. *purple* tým, který je zodpovědný za koordinaci úsilí a komunikace mezi oběma předchozími týmy. [52]

1.5.2 Model vyspělosti úrovně bezpečnosti kyberprostoru

Aktuální bezpečnostní schopnosti organizace popisuje tzv. model vyspělosti (angl. *Maturity Model*). Tento model popisuje, jak rychle je organizace schopna zareagovat na kybernetický incident. *Maturity* model zahrnuje pět fází, které definují kompletní životnost útoku od detekce po reakci na incidenty. Následující výčet definuje každou úroveň zabezpečení [53]:

0. úroveň – **minimální** úroveň zajišťuje preventivně orientovaný přístup jako např. nasazení firewallů, antivirových programů a další. Nezajišťuje obranu proti neznámým a sofistikovaným hrozbám a definuje pouze základní nebo žádné bezpečnostní zásady.
1. úroveň – **reaktivní** úroveň obsahuje již v malé míře implementaci postupů pro zmenšení plochy útoků, např. bezpečnostní monitorování kontrolních stavů, hodnocení zranitelností, správa a detekce nechráněných aktiv. Nedefinuje postupy detekce na incidenty. Trpí nedostatkem technologií, které by detekovaly škodlivou aktivitu.
2. úroveň – **proaktivní** úroveň implementuje řešení EDR a NDR. Silné bezpečnostní zásady, které ale kvůli nedostatku pracovníků a procesů nevyhodnocují závažnost událostí a jejich priority. Není odolná vůči neznámým hrozbám.
3. úroveň – **řízená** úroveň tvoří základní formální proces pro nepřetržité monitorování, detekci anomálních aktivit a omezení hrozeb, které detekují systémy EDR či NDR. Rozpoznávání hrozeb je také založeno na jednotlivých IOC a analýza aktivit slouží k odhalení známých TTP indikátorů. Obvykle je zajištěna střední doba detekce a odezvy.
4. úroveň – **optimální** úroveň zajišťuje komplexní uspořádání dat a událostí, které uchovává po dostatečně dlouhou dobu, aby bylo možné prozkoumat i pokročilé hrozby (APT). Vyšetřování na základě IOC i TTP je zabudované v pracovních postupech, které provádí SOC tým. Události mohou být SOC týmem hlídány a řešeny nepřetržitě. Obvykle SOC zajišťuje střední dobu detekce a reakce na událost.

1.5.3 Plán reakce na bezpečnostní incidenty (IRP)

IRP (angl. *Incident Response Plan*) napomáhá bezpečnostním analytikům odhalovat a řešit kybernetické bezpečnostní incidenty. Jedná se o dokument, který zahrnuje reakci organizace na incidenty, popisy postupů vyšetřování, role a odpovědnosti za činnosti popsané v IRP, specifikaci komunikace mezi analytickým týmem a organizací a další metriky. [54]

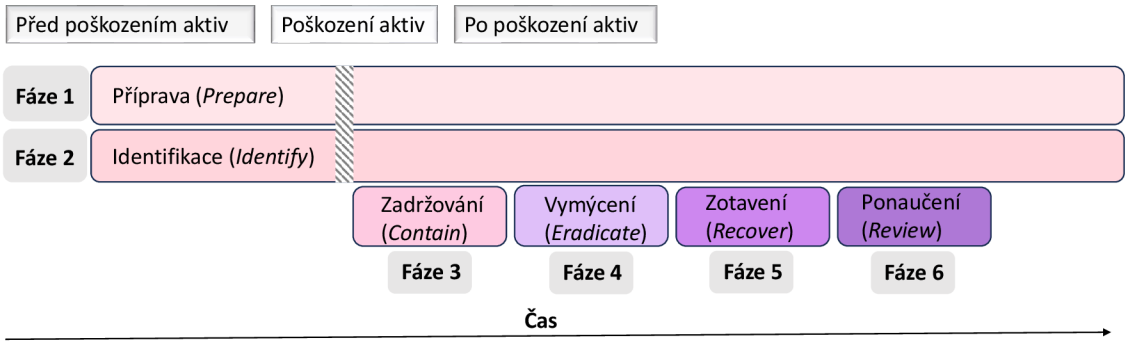
Plán reakce na incidenty zahrnuje šest fází, které zobrazuje obrázek 1.11 a popisují je následující odrážky [55]:

1. **Přípravná fáze** zahrnuje proškolení zaměstnanců ohledně jejich rolí a odpovědností v IRP. Následně by měla být účinnost plánu IRP a školení otestována cvičným narušením dat.
2. Ve **fázi identifikace** organizace určuje, zda se stal skutečný kybernetický incident. Pokud byl zjištěn incident, odpovídá na otázky typu: kdy se incident stal, kdo a jak jej objevil, jaké oblasti byly ovlivněny, má incident vliv na provoz či zda je známý zdroj kybernetického incidentu.
3. **Fáze zadržování** má za úkol zajistit, aby se následky kybernetického incidentu nešířily hlouběji do organizace a nezpůsobily tak další škody na aktivech. Doporučeným počátečním krokem při kompromitaci systému je odpojení zařízení ze sítě a prošetření události. V této fázi také pomohou aktualizace systému, kontrola událostí vzdáleného přístupu a změny hesel k účtům.
4. Ve **fázi vymýcení** je nutné najít a odstranit příčiny vzniku kybernetického incidentu, tedy bezpečně odstranit veškeré stopy *malwaru*.
5. **Zotavovací fáze** zajišťuje procesy obnovy dat a postižených systémů ze zálohy a uvádí systémy zpět do původního provozu.
6. **Fáze ponaučení** zahrnuje analýzu stávajícího IRP ve smyslu, které fáze organizace zvládla dobře a ve kterých si dobře nevedla. Zahrnuje také analýzu, jak lze vylepšit proces zabezpečení, jak lépe zaměstnance proškolit či jak zajistit, aby se narušení bezpečnosti již neopakovalo.

1.6 Právní úprava kybernetické bezpečnosti

Kromě znalosti technologických řešení pro zajištění ochrany kyberprostoru je nezbytné porozumět alespoň základní právní úpravě a definování druhů organizací, jichž se právní rámce pro budování bezpečnostních strategií týkají.

Prvním krokem k zajištění kybernetické bezpečnosti na území státu České republiky bylo uvedení v platnost strategického dokumentu jménem *Koncepce boje proti trestné činnosti v oblasti informačních technologií* již v roce 2001. Tento dokument



Obr. 1.11: Fáze plánu reakce na incidenty [55].

představoval první komplexní řešení pro zabezpečení českého kybernetického prostoru primárně z hlediska kyberkriminality. Jedním z mnoha cílů tohoto dokumentu byla též inicializace vzniku a podpora aktivit CERT (angl. *Central Emergency Response Team*) týmů. CERT týmy disponují odborníky v oblasti bezpečnosti, kteří reagují na incidenty a informují o nich další profesionály v oboru. První CERT tým vznikl již v roce 1998 ve Spojených státech amerických. V České republice (dále jen ČR) však vznikl první CERT tým až v roce 2004 pod záštitou organizace CESNET (angl. *Czech Education and Scientific NETwork*). V průběhu let 2001–2007 bylo vydáno mnoho strategických dokumentů za účelem vytváření bezpečného kybernetického prostoru v ČR. Další důležité kroky k zajištění kybernetické bezpečnosti z právního hlediska byly realizovány v roce [56, 57]:

- **2010**, kdy došlo k přijetí ustavení vlády č. 205 o řešení problematiky kybernetické bezpečnosti ČR, jehož součástí bylo ustanovení Ministerstva vnitra ČR národní autoritou pro oblast kybernetické bezpečnosti a zároveň v rámci ustanovení č. 380 uložilo ustanovení Ministerstvu vnitra povinnost zřídit Meziresortní koordinační radu pro oblast kybernetické bezpečnosti. Dalším důležitým krokem provedeným roku 2010 se stalo přijetí memoranda o zřízení CSIRT (angl. *Computer Security Incident Response Team*) týmů v dohodě s organizací CZ.NIC[13]. Hlavním cílem CSIRT týmů je převážně podílení se na řešení kybernetických incidentů, podpora koncových uživatelů a správců sítí a spolupráce s týmy CERT.
- **2011**, kdy byla zrušena Meziresortní koordinační rada pro oblast kybernetické bezpečnosti a novou národní autoritou pro kybernetickou bezpečnost se stal dle ustanovení č. 781 Národní bezpečnostní úřad. Pro roli koordinátora vznikla speciální Rada pro kybernetickou bezpečnost. Dále byla v tomto roce přijata

[13]Hlavním cílem CZ.NIC je správa a zajištění bezpečnosti nejvyšší úrovně domény *.cz*.

strategie pro oblast kybernetické bezpečnosti ČR na období 2011–2015.[14] Současně se strategií byl přijat akční plán, který definoval správné splňování strategických cílů.

- **2012**, kdy byl v souladu se strategií přijat věcný záměr zákona o kybernetické bezpečnosti a hned vzápětí byl připraven samotný návrh zákona.
- **2014**, kdy byl přijat a vstoupil v platnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti s účinností od 1. ledna 2015. Zároveň s ním vzešla v platnost vyhláška o kybernetické bezpečnosti a vyhláška o stanovení významných informačních systémů a jejich určujících kritériích. Podrobněji budou zákon o kybernetické bezpečnosti a vyhláška o kybernetické bezpečnosti rozepsány v následující podkapitole.
- **2016**, kdy Evropská unie přijala Směrnici Evropského parlamentu a Rady Evropské unie 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii [59]. Zkráceně se jedná o směrnici NIS (angl. *Network Information Security*), díky ní musel být existující Zákon o kybernetické bezpečnosti ČR novelizován. Směrnice NIS bude podrobněji popsána v následující podkapitole.
- **2017**, kdy byl novelou zákona 205/2017 Sb. zákona o kybernetické bezpečnosti založen nový orgán státní správy Národní úřad pro kybernetickou a informační bezpečnost, který přebral povinnosti Národního bezpečnostního úřadu a stal se tak novou národní autoritou pro oblast kybernetické bezpečnosti. Mezi primární úlohy NÚKIB patří např. provozování vládního CERT týmu, zajištění spolupráce mezi českými i mezinárodními CERT a CSIRT týmy, tvorba bezpečnostních standardů, podpora vzdělávání, výzkum a vývoj v oblasti kybernetické bezpečnosti [60].
- **2022–2024**, kdy koncem roku 2022 byla zveřejněna oficiální publikace Směrnice Evropského parlamentu a Rady Evropské unie 2022/2555, o opatřeních k zajištění vysoké společenské úrovně kybernetické bezpečnosti v Evropské unii, zkráceně NIS2, tedy novelizované verze směrnice NIS, která se touto směrnicí ruší. Datum nabytí platnosti směrnice připadalo na 16. ledna 2023 a účinnost směrnice připadá na 16. říjen 2024, tedy přesně 21 měsíců od data uvedení směrnice v platnost. Podrobněji bude směrnice NIS2 vysvětlena v následující podkapitole.

Zákon o kybernetické bezpečnosti (ZoKB)

Zákon o kybernetické bezpečnosti (dále ZoKB) reguluje práva a povinnosti osob i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti.

[14] Další strategie a jejich akční plány byly přijaty na období 2015–2020 a následně 2021–2025 [58].

ZoKB zapracovává předpis Evropské unie NIS. Hlavními cíli aplikace ZoKB jsou např. stanovení základní úrovně bezpečnostních opatření, vylepšení detekce a zavedení hlášení kybernetických incidentů, zavedení systému opatření pro reakci na kybernetické incidenty a upravení činnosti dohledových pracovišť. ZoKB směruje primárně k ochraně tzv. CIA triády (angl. *Confidentiality, Integrity, Availability*) neboli zajištění důvěrnosti dat (přístup k datům mají pouze oprávněné osoby), integrity (ochrana dat před neoprávněnou modifikací) a dostupnosti dat (data jsou oprávněnému uživateli dostupná vždy v případě potřeby). [56, 61]

ZoKB staví na dvou zásadách. První zásadou je minimalizování zásahů do práv soukromoprávních subjektů a druhou zásadu tvoří individuální odpovědnost za bezpečnost vlastních informačních systémů [56]. Aplikace ZoKB se vztahuje na povinné subjekty kybernetické bezpečnosti, jimiž jsou [62]:

- poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě,
- orgány nebo osoby zajišťující významné sítě,
- správci a provozovatelé informačních systémů kritické informační infrastruktury,
- správci a provozovatelé významných informačních systémů,
- správci a provozovatelé informačních systémů základních služeb,
- provozovatelé základních služeb,
- poskytovatelé digitálních služeb.

Nejsou-li povinnosti plynoucí ze ZoKB povinnými subjekty splněny, může NÚKIB uložit subjektu pokutu ve výši až 5 000 000 Kč dle závažnosti přestupku[15].

Vyhláška o kybernetické bezpečnosti

Vyhláška č. 82/2018 Sb., celým jménem o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), představuje náhradu starší vyhlášky č. 316/2014 Sb. Současná vyhláška o kybernetické bezpečnosti (dále jen VoKB) zapracovává evropskou směrnici NIS a také vysvětluje důležité termíny, které ZoKB nedefinuje. VoKB pro povinné subjekty ve smyslu aplikace ZoKB upravuje náležitosti týkající se [61]:

- obsahu a struktury bezpečnostní dokumentace a bezpečnostních opatření,
- typů, kategorií a hodnocení významnosti kybernetických bezpečnostních incidentů,
- způsobu hlášení kybernetických bezpečnostních incidentů,
- oznamování provedení reaktivních opatření a jejich výsledků,

[15] Druhy přestupků a výše pokut při nedodržení povinností subjektů jsou uvedeny v § 25 zákona č. 181/2014 Sb. o kybernetické bezpečnosti.

- vzorů oznámení kontaktních údajů a jejich formy,
- způsobů likvidace dat, provozních údajů, informací a jejich kopií.

Evropská směrnice NIS

NIS je první směrnicí vytvořenou Evropskou unií jako komplexní dokument, který si klade za cíl zajistit jednotnou a vysokou úroveň zabezpečení v rámci sítí a informačních systémů v členských státech Evropské unie. Do doby vzniku směrnice NIS se úrovně legislativních rámců v oblasti kybernetické bezpečnosti členských států výrazně lišily a některé státy neregulovaly kybernetickou bezpečnost vůbec. Povinnosti plynoucí ze směrnice NIS nabývají organizační a legislativní povahy a některé se vztahují přímo definované kategorie regulovaných subjektů. Mezi organizační a legislativní povinnosti subjektů lze zahrnout [63]:

- **přijetí strategie** – každý členský stát by měl mít zajištěnou národní strategii pro bezpečnost sítí a informačních systémů s ohledem na strategické cíle státu a definování konkrétních bezpečnostních opatření.
- **založení centrálního orgánu** – každému členskému státu je uložena povinnost zřídit národní autoritu, která mimo jiné bude sloužit pro výměnu informací na úrovni Evropské unie.
- **založení CSIRT týmů** – týmy CSIRT zajišťují podporu při řešení kybernetických bezpečnostních incidentů.
- **zřízení skupiny pro spolupráci a skupin CSIRT** – obě skupiny mají dle směrnice za úkol spolupracovat v rámci členských států jak po strategické stránce, to zajišťují skupiny pro spolupráci (angl. *Cooperation Group*), tak po technické stránce, technickou část mají na starost skupiny CSIRT. Obě skupiny se skládají ze zástupců jednotlivých členských států.

Směrnice NIS se vztahuje k provozovatelům základních služeb a poskytovatelům digitálních služeb. Skupina provozovatelů základních služeb je tvořena subjekty spadajících do odvětví energetiky, dopravy, bankovnictví, zdravotnictví, distribuce pitné vody a digitální infrastruktury. Skupina provozovatelů elektronických služeb je tvořena subjekty v odvětví internetového obchodu, webových vyhledávačů a poskytovatelů webového úložiště (angl. *Cloud Computing*). [63]

Evropská směrnice NIS2

Směrnice NIS2 přináší zásadní změny v regulaci oblasti kybernetické bezpečnosti členských států Evropské unie. Změny zasahují jak strategickou, tedy povinnosti dopadající na NÚKIB a Evropskou agenturu pro bezpečnost sítí a informací (ENISA), tak i operativní úroveň, tedy regulace práv a povinností subjektů, společností a státních organizací ČR. Nejvýznamnější povinnosti dopadající na strategickou úroveň

ČR zahrnují přijetí národní strategie kybernetické bezpečnosti pro konkrétní oblasti, určení jednoho CSIRT nebo CERT týmu pro koordinaci zveřejňování informací o zranitelnostech a jejich předávání do Evropské databáze zranitelností spravovanou agenturou ENISA, hlubší spolupráci při řešení kybernetických incidentů a sdílení strategických informací a zkušeností na vnitrostátní úrovni i mezi členskými státy a mnoho dalších. Za nedodržení či porušení uložených povinností hrozí dle čl. 34 směrnice NIS2 základním[16] subjektům pokuta až ve výši 10 milionů EUR nebo 2 % celkového celosvětového ročního obratu, nebo důležitým[17] subjektům ve výši až 7 milionů EUR nebo 1,4 % celkového celosvětového ročního obratu podniku. [59]

Výčet základních neboli vysoce kritických odvětví, která jsou regulována Evropskou směrnicí NIS2, definuje příloha I směrnice 2022/2555 [65, 66]:

- **energetika** – regulace v této oblasti dopadá zejména na elektroenergetické podniky a výrobce elektrické energie, na provozovatelé distribučních a přenosových soustav elektrické energie a zemního plynu, na provozovatelé dobíjecích bodů, dálkového vytápění a chlazení, ropovodů, těžby, zpracování a skladování ropy, zemního plynu a vodíku.
- **doprava** – regulace letecké dopravy se vztahuje výhradně na dopravce ve smyslu využívání ke komerčním účelům, řídící orgány letiště včetně letišť samotných a jejich pomocných zařízení a na provozovatelé kontroly řízení provozu. V rámci železniční dopravy jsou povinnými subjekty provozovatelé železničních infrastruktur a služeb železničních podniků. Regulace v rámci vodní dopravy se vztahuje k řídícím orgánům přístavů a ke společnostem vnitrozemské, námořní, pobřežní osobní a nákladní dopravy a služeb lodní dopravy s výjimkou jejich jednotlivých plavidel. Právní povinnosti plynou i pro provozovatelé inteligentních dopravních systémů v rámci silniční dopravy a orgány zajišťující kontrolu řízení provozu.
- **bankovnictví a finanční trhy** – regulovanými subjekty jsou tedy úvěrové instituce, provozovatelé obchodních systémů a ústřední protistrany.
- **zdravotnictví** – mezi povinné subjekty tohoto odvětví patří provozovatelé zdravotní péče, referenční laboratoře Evropské unie, subjekty provádějící výzkum a vývoj léčivých výrobků a výrobci základních farmaceutických přípravků a přípravků kriticky důležitých v případě mimořádné situace.
- **pitná a odpadní voda** – regulace v rámci odvětví pitné vody spadá na dodavatelé a distributory vody určené k lidské spotřebě, jejichž distribuční aktivity tvoří podstatnou část jejich odborné činnosti. Povinné subjekty též

[16]Mezi základní subjekty patří společnosti s více než 250 zaměstnanci, s obratem 50 mil. EUR nebo rozvahou (hodnota aktiv a pasiv společnosti) 43 mil. EUR. [64]

[17]Mezi důležité subjekty patří společnosti s více než 50 zaměstnanci a ročním obratem nebo rozvahou 10 mil. EUR. [64]

tvoří podniky, jejichž činnost odvádění, vypouštění nebo čištění odpadních vod, splašek nebo průmyslových odpadních vod tvoří podstatnou část jejich obecné činnosti.

- **digitální infrastruktura a řízení služeb informačních a komunikačních technologií** – povinnosti vyplývající z NIS2 pro tato odvětví se týkají provozovatelů výměnných uzlů internetu, DNS (s výjimkou operátorů kořenových serverů), poskytovatelů služeb *cloud computing*, datových center, sítí pro doručování obsahu, služeb vytvářejících důvěru, veřejných sítí elektronických komunikací, veřejně dostupných služeb elektronických komunikací, řízených služeb a řízených bezpečnostních služeb.
- **veřejná správa** – v rámci tohoto odvětví se regulace řídí vnitrostátním právem a regulovány jsou ústřední a regionální subjekty veřejné správy, tedy institucí významných pro chod státu.
- **vesmír** – regulovanými subjekty zde jsou provozovatelé pozemních infrastruktur, které vlastní, spravují a provozují členské státy Evropské unie nebo soukromé subjekty a které podporují poskytování služeb v rámci kosmického prostoru vyjma poskytovatelů veřejných elektronických komunikací.

Výčet důležitých odvětví, která jsou regulována Evropskou směrnicí NIS2, definuje příloha II směrnice 2022/2555 [65, 66]:

- **poštovní a kurýrní služby** – povinnosti spadají na subjekty zajišťující výběr, třídění, přepravu a dodání poštovních zásilek a na poskytovatelé kurýrních služeb.
- **nakládání s odpady** – povinnými subjekty v rámci odpadního hospodářství jsou zařízení určená pro nakládání s odpady, samotní obchodníci, zprostředkovatelé a dopravci, pokud tyto aktivity tvoří jejich hlavní ekonomickou činnost.
- **chemický průmysl** – regulovanými subjekty jsou podniky pro výrobu, distribuci a skladování chemických látek nebo směsí.
- **potravinářství** – povinnosti vyplývají pro velkoobchodní distribuci potravin a pro jejich průmyslovou výrobu nebo zpracování.
- **výroba** – regulace se vztahuje na společnosti zabývající se výrobou zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických, elektrických a optických přístrojů, strojů a zařízení, dopravních prostředků, přívěsů, návěsů a zařízení kromě motocyklů.
- **digitální poskytovatelé** – povinnými subjekty jsou poskytovatelé internetových tržišť, vyhledávačů a služeb platforem sociálních sítí.
- **výzkum** – povinnosti se vztahují na výzkumné organizace, které využívají výsledky výzkumu komerčně, s výjimkou vzdělávacích institucí.

Evropská agentura pro síťovou a informační bezpečnost

Agentura ENISA (angl. *European Union Agency for Cybersecurity*) byla zřízena v rámci plnění nařízení Evropského parlamentu a Rady Evropské unie č. 460/2004. V uplynulých letech byl mandát evropské agentury několikrát prodloužen nařízeními[18] Evropského parlamentu a Rady Evropské unie, z nichž každé nařízení rušilo platnost nařízení předchozího. Poslední prodloužení mandátu se konalo dne 17. dubna 2019 nařízením Evropského parlamentu a Rady č. 2019/881 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti"). [67]

V rámci agentury ENISA existuje několik skupin expertů zaměřených na různé oblasti. Jedná se o skupiny řešící otázky kybernetické bezpečnosti v odvětví zdravotnictví, umělé inteligence, dopravní infrastruktury a inteligentních dopravních systémů, finančního sektoru, důvěryhodných služeb[19] a otázky v rámci dosahování strategických cílů. ENISA vydává mnoho doporučení, standardů a vzdělávacích manuálů s cílem zlepšit kybernetickou odolnost členských států Evropské unie zejména v tématech cloud prostředí, kritické infrastruktury, kryptografie, krizového řízení v kybernetickém prostoru, kybernetické hrozby, právní úprava kybernetické bezpečnosti, hlášení a reakce na kybernetické incidenty, analýza trhu kybernetické bezpečnosti, řízení rizik a mnoho dalších. Jedná se například o dokumenty [67]:

- **hlášení kybernetických incidentů** národním regulačním orgánům a výměnou informací o incidentech podle Evropského kodexu elektronických komunikací zkráceně EECC (angl. *European Electronic Communications Code*), a to ve formě ročních reportů a také hlášení konkrétních významných kybernetických incidentů. Tento standard také uvádí strukturu a prahové hodnoty pro hlášení incidentů včetně pokynů k posouzení míry dopadu incidentu na poskytované služby.
- **průvodce řízením incidentů** poskytuje komplexní přehled osvědčených postupů a metodik pro efektivní zvládnutí kybernetických bezpečnostních incidentů. Zahrnuje pracovní postupy a procesy pro řešení, analýzu, reakci a hlášení incidentu.
- **výroční zpráva přehledu hrozeb** informuje o stavu kybernetické bezpečnosti v rámci EU formou každoročních reportů. Popisuje hrozby a statistiky pozorovaných trendů útoků se zaměřením na aktéry hrozeb a techniky používaných jednotlivými útoky[20] včetně analýzy dopadů a motivace incidentů.

[18] Mandát ENISA byl prodloužen nařízeními č. 1007/2008, č. 580/2011, č. 526/2013.

[19] Činnost skupiny je zaměřena na validaci elektronických podpisů, razítek, pečetí a certifikátů.

[20] Dokument *Threat Landscape* tvoří jeden z primárních zdrojů dat pro zobrazení pohledu dle druhů sektorů a pohledu na útoky v matici *ATT&CK*, jejichž implementace je popsána v podkapitolách 4.2.3 a 4.2.1.

2 Analýza vizualizačních šablon a technik

V internetovém prostředí existuje mnoho dostupných knihoven, rámců a šablon pro vytvoření příjemné a interaktivní webové aplikace. Tato bakalářské práce rozšiřuje již existující webovou aplikaci jménem *Sigma Tools* pro správu a překlad Sigma pravidel. Pro vytvoření klientské části aplikace byl již vybrán webový framework `Vue` verze 3, dále byla implementována zobrazení pomocí knihoven `D3.js` (angl. *Data-Driven Documents*) a `Vuetify`.

Na technologickém trhu existuje mnoho vendorů poskytujících služby SIEM systémů. SIEM se stal základní nepostradatelnou složkou řešení kybernetické bezpečnosti. Jednotlivá řešení se však mohou vzájemně lišit a to zejména ve způsobech grafického zobrazení. Druhá část této kapitoly bude tedy zaměřena na porovnání designu pravidel v SIEM řešeních.

2.1 Analýza webových frameworků a knihoven

Tato kapitola popisuje vybrané dostupné knihovny a šablony, které jsou vhodné pro použití v rámci praktické části bakalářské práce.

2.1.1 Webový framework Vue

`Vue` se řadí mezi nejpopulárnější webové frameworky. Jedná se o rámec založený na jazycích HTML (angl. *Hypertext Markup Language*), CSS (angl. *Cascading Style Sheets*) a Javaskript (angl. *JavaScript*) nebo Typeskript (angl. *TypeScript*). Obecná struktura šablony `Vue` souboru se skládá ze tří částí: *template, script, style*. Struktura je znázorněna na obrázku 2.1

```
<template>
  <!--HTML kod -->
</template>

<script>
    // funkcni cast kodu Javaskript/Typeskript
</script>

<style>
    /*CSS vizualni styly*/
</style>
```

Obr. 2.1: Struktura souboru rámce `Vue`.

`Vue` umožňuje webovou aplikaci rozdělit na několik částí a ty pak vyvíjet nezávisle na sobě. Jedná se o tedy model založený na komponentách, v těchto komponentách

lze snadno definovat kód, který se v rámci aplikace často opakuje, např. navigační lišta či patička.

K základním funkcím `Vue` patří [73]:

- Deklarativní vykreslování (angl. *Declarative Rendering*) – `Vue` rámec rozšiřuje základní syntaxi značkovacího jazyka HTML o možnost vypsat HTML výstup pomocí Javaskriptu.
- Reaktvita (angl. *Reactivity*) – `Vue` automaticky sleduje změny provedené v kódu Javaskriptu a efektivně aktualizuje objektově orientovanou reprezentaci HTML dokumentu tzv. DOM (angl. *Document Object Model*), když zaznamená změnu.

2.1.2 D3.js knihovna

`D3.js` je bezplatná knihovna[1] vizualizačních technik dat založená na jazyce Javaskript. Poskytuje mnoho šablon pro tvorbu různých typů grafů a map v rámci webové aplikace. Většina knihoven poskytující šablony grafů, poskytuje kód již hotového grafu. Zatímco `D3.js` poskytuje dílčí stavební bloky, které se dají kombinovat a z nich vytvářet pokročilá grafická zobrazení vytvořená na míru. `D3.js` umožňuje jednoduché vyžádání dat na základě HTTP (angl. *Hypertext Transfer Protocol*) požadavku a dokáže zpracovávat data v běžných datových formátech jako jsou CSV, TSV (angl. *Tab-separated Values*) a JSON. [68]

Výhody:

- Podporuje propojení s frameworkem `Vue`.
- Umožňuje dynamickou správu dat a transformaci dat do užitečných formátů.
- Je vhodný pro vytváření grafických struktur na míru pomocí základních stavebních bloků.
- Široká komunita přispívajících vývojářů a výukových materiálů.

Nevýhody:

- Je složitější na implementaci, protože vyžaduje znalosti jazyků HTML, CSS, Javaskript a SVG (angl. *Scalable Vector Graphics*).
- Vývojář se musí naučit novou syntaxi pro bloky `D3.js`.
- Při vývoji poměrně jednoduchého zobrazení musí vývojář napsat velké množství kódu.

`D3.js` samozřejmě není jedinou dostupnou knihovnou poskytující vizualizaci založenou na jazyce Javaskript. Existuje velké množství alternativních řešení, která lze použít pro vytvoření moderní a interaktivní webové aplikace, např. *Chart.js, Highcharts, Plotly.js, Google Charts...* a mnoho dalších.

[1] Kódy knihovny `D3.js` lze nalézt na adrese: `https://github.com/d3/d3`.

2.1.3 Knihovna Bootstrap pro Vue

`Bootstrap` je jedním z nejpopulárnějších rámců[2] s otevřeným kódem pro tvorbu uživatelsky přívětivé grafické části webové aplikace. Poskytuje mnoho komponent a šablon pro vývoj interaktivní webové aplikace, jako jsou např. tlačítka, ikony, formuláře a mnoho dalších. Pomocí speciálně vytvořené knihovny `Bootstrap-vue` lze využívat komponenty `Bootstrap` ve `Vue` projektu. [69]

Výhody:

- Interaktivní web ve spojení `Vue` a `Bootstrap`.
- Dostupný kód zdarma.
- Mnoho dostupné dokumentace.
- Snadné použití i pro začátečníky v designu webových aplikací.

Nevýhody:

- Je náročné vytvářet pokročilejší způsoby zobrazení nad rámec knihovny.
- Není vhodné pro složitější projekty, které vyžadují unikátní design.

2.1.4 Framework komponentů Vuetify

`Vuetify` je zdarma dostupná kolekce[3] předem připravených `Vue` komponent, které obsahují užitečné funkce jako např. dynamická témata aplikací, rozložení prvků v aplikaci, různá tlačítka, seznamy a mnoho dalších prvků. [70]

Výhody:

- Umožňuje vytvořit příjemný design i pro náročné vývojáře.
- Obsahuje velké množství komponentů a dokumentace.
- Rozšířená aktivní komunita vývojářů.

Nevýhody:

- Změna některých funkcí v šabloně může být obtížná.
- Podporuje tzv. materiálový design vytvořený společností Google, tento styl může někomu přidat příliš výrazný a nevhodný.

[2]Kódy knihovny `Bootstrap-vue` lze nalézt na adrese: `https://github.com/bootstrap-vue/bootstrap-vue`.

[3]Kódy kolekce `Vuetify` lze nalézt na adrese: `https://github.com/vuetifyjs/vuetify`.

2.2 Vizualizace pravidel v platformách SIEM

Tahle kapitola je věnována popisu a srovnání vizualizace pravidel dvou SIEM řešení. Srovnání bude zaměřeno na část vizualizace Sigma pravidel. Pro tyto účely byli vybráni vendoři IBM s řešením QRadar a RSA s řešením NetWitness Platform.

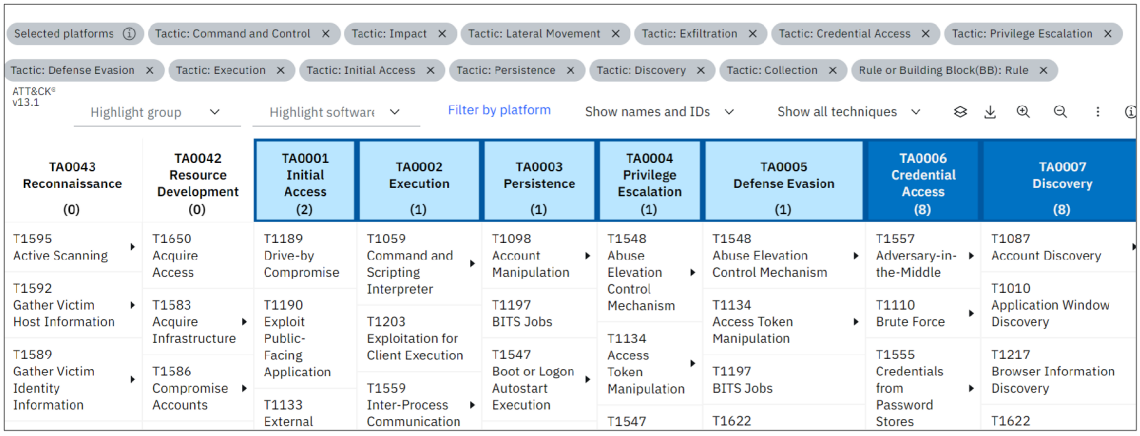
2.2.1 SIEM řešení QRadar

QRadar je platforma vyvinutá společností IBM celým názvem *International Business Machines Corporation*, která se stará o správu zabezpečení sítě. QRadar využívá kombinaci toků síťových událostí, korelaci událostí a hodnocení zranitelností na základě aktiv. QRadar umožňuje zaznamenávat aktivity (logy) v reálném čase a provádět pokročilá vyhledávání na základě různých kritérií a to za pomocí uživatelského rozhraní či přímo dotazem. Dotazy pro vyhledávání aktivit, událostí a jiných informací jsou založené na strukturovaném dotazovacím jazyku AQL (angl. *Ariel Query Language*), který umožňuje komunikaci s databázemi Ariel. QRadar umožňuje také zobrazit bezpečnostní události do přehledných grafů založených na čase. [71]

Vizualizace Sigma pravidel v QRadaru

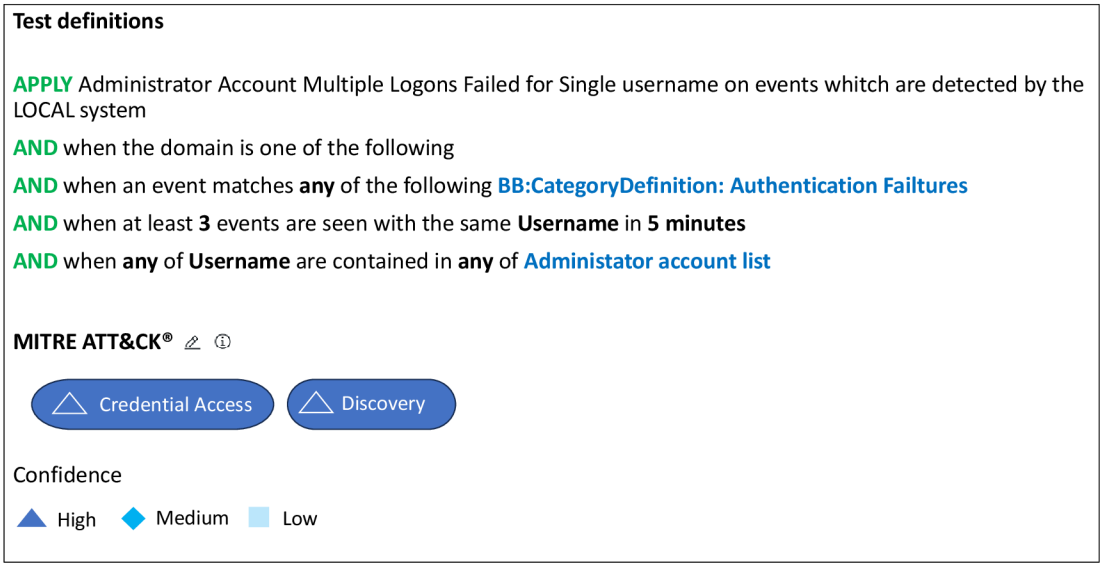
Jak již bylo zmíněno v úvodu kapitoly 2, každý vendor, který poskytuje řešení SIEM, řeší design (nejen Sigma pravidel) jinak. K zobrazení pravidel v QRadaru jsou zapotřebí vyšší přístupová práva, která uděluje administrátor. Veškerá pravidla zobrazuje a spravuje karta „*Use Case Manager*“, což je rozšíření pro platformu QRadar stejného vendora. V této záložce se dají pravidla vyhledat dle různých filtrů, např. dle názvu, dostupnosti, přiřazené skupiny, zdroje aktivit, domén, taktik a technik rámce *ATT&CK* a podle mnoha dalších různých kritérií.

Protože jsou jednotlivá pravidla namapována na *ATT&CK* taktiky a techniky, umožňuje QRadar zobrazit pravidla (kromě klasické tabulky) v matici *ATT&CK* rámce (viz obr. 2.2) a to včetně zobrazení názvů taktik, technik a jejich identifikátorů. Toto zobrazení umožňuje analytikovi filtrovat pravidla, která jsou zaměřená na činnosti různých skupin hrozeb, např. APT30. Také umožňuje filtrovat pravidla na základě používaného škodlivého softvéru, např. 4H RAT a na základě typu platformy, např. Google Workspace. Dle počtu používaných technik z jednotlivých taktik jsou políčka taktik zabarvena (světlejší barva představuje malé množství používaných technik konkrétní taktiky). Matice *ATT&CK* však není jediných možným zobrazením souvisejícím s mapováním na MITRE *ATT&CK*. QRadar zobrazuje statistiky počtu implementovaných pravidel dle MITRE taktik a automaticky generuje několik druhů grafů.



Obr. 2.2: Zobrazení vzorových pravidel v matici rámce *ATT&CK*.

Po rozbalení vybraného pravidla[4] se v levé polovině okna zobrazí informace o pravidle (viz obr. 2.3) a v pravé polovině okna se zobrazí grafický strom, který ukazuje propojení pravidla a jeho bloků (viz obr. 2.4).

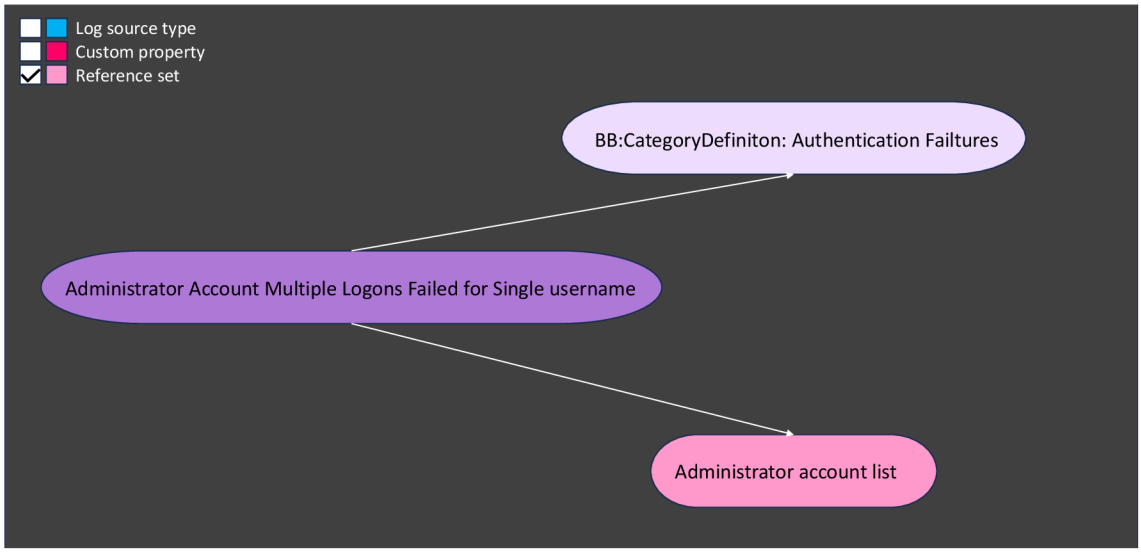


Obr. 2.3: Některé parametry nasazeného pravidla.

Informací o pravidle se zobrazuje mnoho včetně: názvu pravidla; zda je pravidlo povoleno; jaké jsou výsledky testování pravidla; poznámky; definice pravidla; mapování na taktiky *ATT&CK* včetně určení úrovně důvěrnosti (vysoká, střední, nízká); přiřazení pravidla ke skupině; data vytvoření a aktualizace pravidla včetně jeho vývojáře a typů zdrojů aktivit. Zobrazené informace specifikují i akce, které se mají provést po splnění kritérií pravidel.

[4]Obrázky 2.2, 2.3 a 2.4 jsou vystřiženy z prostředí QRadar reálného zákazníka, proto jsou údaje identifikující organizaci odstraněny, aby nedošlo k poškození zákazníka.

Vizuální zobrazení pravidla a jeho částí si klade za cíl usnadnit analytikovi orientaci ve vztazích pravidel a jejich částí. Konkrétně obrázek 2.4 zobrazuje pravidlo „Administrator Account Multiple Logons Failed for Sigle Username“, které hlídá počet neúspěšných pokusů o přihlášení k privilegovanému administrátorskému účtu, ve vztahu k tzv. „Building block“ a „Admnistrator Account List“. Stavebními bloky se v QRadaru rozumí soubory testů, které samy o sobě nevedou k okamžité akci, ale používají se při tvorbě a aplikaci korelačních pravidel [71]. Může se jednat např. o skupiny IP adres, jména privilegovaných uživatelů nebo názvy událostí. Druhá součást pravidla tzv. seznam administrátorských účtů definuje, u kterých účtů má pravidlo hlídat počty neúspěšných přihlášení.



Obr. 2.4: Grafické zobrazení nasazeného pravidla a jeho částí.

2.2.2 SIEM řešení NetWitness Platform

NetWitness Platform je řešení vyvinuté společností RSA. Jedná se o řešení, které bezpečnostním týmům umožňuje rychle detekovat identifikovat, pochopit a vyřešit rozsah bezpečnostní hrozby. NetWitness poskytuje komplexní přehled logů, síťových dat, dat koncových bodů včetně analýzy chování uživatelů a entit v reálném čase a umožňuje aplikaci analýzy hrozeb v cloudovém prostředí, v místní síti i ve virtuálním prostředí. Také zajišťuje možnosti automatizace a orchestrace pro vyšetřování a reakci na události. [72]

Podobně jako QRadar dává zákazníkovi platforma NetWitness možnost tvorby korelačních pravidel, kterým se v terminologii NetWitness přezdívá *Incident Rules* neboli pravidla pro incidenty. Samotná pravidla umožňující zachycení a odhalení potenciální škodlivé aktivity se nazývají ESA (angl. *Event Stream Analysis*) pravidla.

ESA pravidla používají deklarativní jazyk EPL (angl. *Event Processing Language*) pro práci s daty událostí, např. filtrování, agregaci a mnoho dalších činností. Jedno pravidlo pro incident může obsahovat více ESA pravidel. O zasílání upozornění bezpečnostnímu týmu se pak starají právě pravidla pro incident. [72]

Vizualizace Sigma pravidel v NetWitness Platform

Zobrazení překonvertovaných Sigma pravidel[5] do syntaxe RSA v platformě NetWitness lze dohledat v horní části stránky v záložce „*ESA Rules*“. V tomto prostoru se dají jednotlivá pravidla vyhledat v tabulce manuálně či filtrovat dle klíčových slov. Po otevření ESA pravidla (viz obr. 2.5) se otevře nová karta s definicí pravidla, kterou lze upravovat. Lze zde nastavit název pravidla, přidat jednoduchý popis, dále určit, zda se jedná o zkušební pravidlo (angl. *Trial Rule*) a určit prahovou hodnotu paměti (angl. *Memory Threshold*), aby se ESA pravidlům znemožnilo používat nadměrné množství paměti [72]. Dále umožňuje nastavit možnost zasílání upozornění (angl. *Alert*) a určit závažnost aktivity (angl. *Severity*), která může nabývat hodnot: *Low, Medium, High, Critical*. Následuje samotná definice pravidla v jazyce EPL, která provádí dotazy nad databází shromážděných dat událostí. Tohle konkrétní pravidlo se zaměřuje na detekci úspěšných přihlášení do tunelu VPN ze dvou různých IP adres mimo Českou a Slovenskou republiku.

Jak již bylo vysvětleno výše, ESA pravidla tvoří součást pravidla incidentu, který odesílají upozornění bezpečnostnímu týmu na potenciálně škodlivou aktivitu. Úkolem bezpečnostního týmu je pak upozornění a s ním spojené události prošetřit a vyřešit. Tento přístup je velmi efektivní a to primárně z důvodu zajištění korelace událostí a následně odeslání jednoho upozornění na škodlivou aktivitu namísto n upozornění z každého dílčího ESA pravidla. Způsob, kterým se ESA pravidla přidávají do pravidla incidentu ilustruje obr. 2.6. Konkrétně se jedná o dvě ESA pravidla, která při objevení definované události vytvoří jedno upozornění pro bezpečnostní tým.

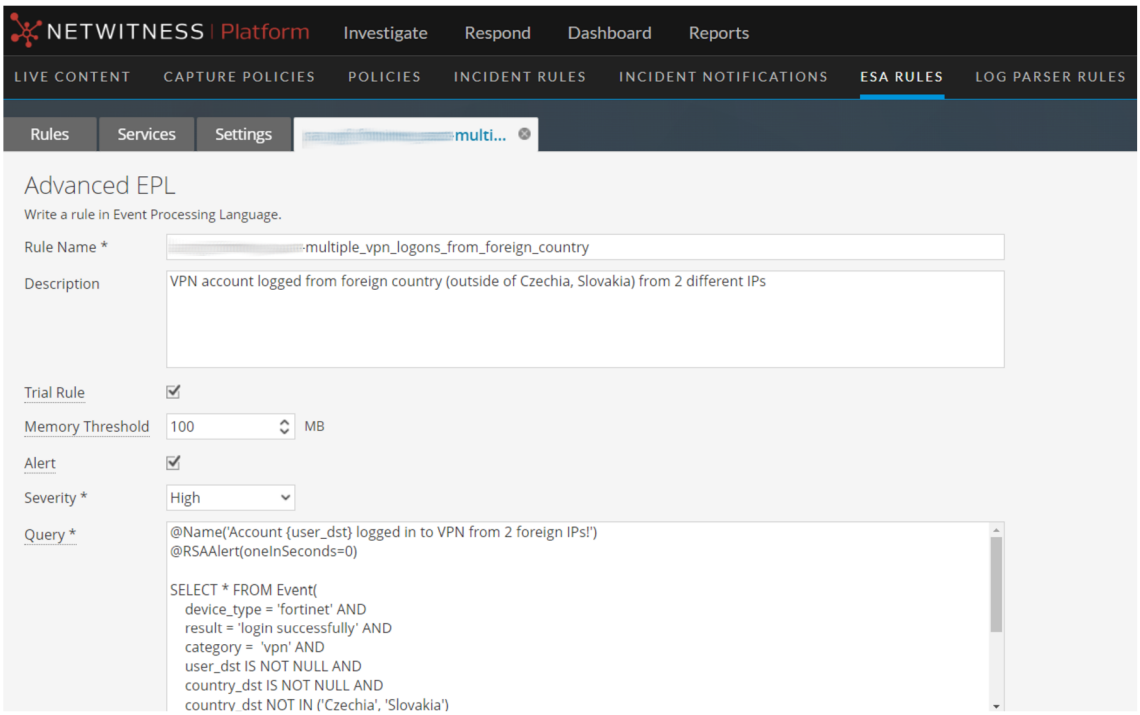
2.2.3 Srovnání způsobů vizualizace pravidel použitých v SIEM

V kapitolách 2.2.1 a 2.2.2 byly popsány možnosti zobrazení pravidel v SIEM řešeních QRadar a NetWitness Platform. Je zřejmé, že grafické pojetí (nejen) pravidel obou vendorů se velmi liší. NetWitness Plaform řešení má oproti QRadaru výrazně méně propracované zobrazení. NetWitness zobrazuje použitá pravidla přehledně v tabulce, nad kterou lze vyhledávat pomocí klíčových slov, zatímco QRadar umožňuje vyhledávat pravidla na základě různých kritérií, např. dle dostupnosti pravidla, dle skupin,

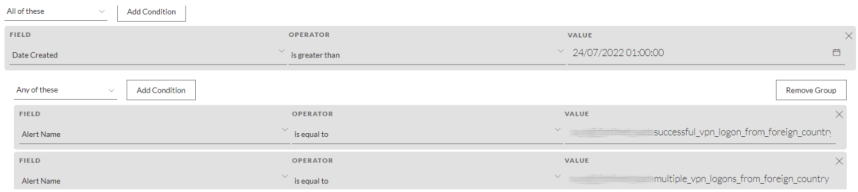
[5]Obrázky 2.5 a 2.6 jsou vystřiženy z prostředí NetWitness Platform reálného zákazníka, proto jsou některé udaje identifikující organizaci rozostřeny, aby nedošlo k poškození zákazníka.

do kterých je pravidlo přiřazeno, dle dat, kdy byla pravidla vytvořena i modifikována a dle mnoha dalších kritérií. NetWitness i QRadar podporují tvoru korelačních pravidel. NetWitness však korelaci zobrazuje pouze v rámci tabulky (viz obr. 2.6), zatímco QRadar zobrazuje vzájemný vztah pravidel a stavebních bloků navíc v interaktivním diagramu (viz obr. 2.4).

QRadar disponuje pro bezpečnostního analytika velkou výhodou, a sice mapováním pravidel na dostupný rámec *ATT&CK*, který je zobrazen v přehledné matici, nad kterou lze také provádět filtrování informací. Obě platformy mají však i společnou vlastnost, a to zobrazení statistik v různých typech grafů. V NetWitness se jedná se o trendy, např. nejpoužívanější zdrojové IP adresy, či nejpoužívanější cílové porty a to vše zobrazené v závislosti na čase. A v QRadaru lze např. zobrazit události vygenerované různými zdroji logů v čase. Závěrem lze říci, že QRadar má oproti NetWitness zobrazení propracovanější.



Obr. 2.5: Některé parametry ESA pravidla v platformě NetWitness.



Obr. 2.6: Implementování ESA pravidel do pravidla incidentu.

3 Návrhy na vizualizaci Sigma pravidel

Před samotným popisem grafické vizualizace webové aplikace je důležité provést analýzu možných způsobů zobrazení, které se dají uskutečnit modifikací dostupných rámců popsaných v kapitole 2.1. Použitý návrh by měl splňovat určitá kritéria. Webová aplikace by měla být jednoduchá a intuitivní. Také by měla obsahovat interaktivní prvky a být vhodně moderně designovaná. Následující části kapitoly popisují různé návrhy zobrazení. Je důležité také zmínit, že návrhy nemusí být vždy použity separátně, v některých případech se dají kombinovat.

3.1 Zobrazení pomocí *Sankey* diagramu

Sankey diagram je způsob zobrazení propojení hodnot z jedné datové sady do druhé. Elementy datových sad se nazývají uzly a propoje mezi uzly se nazývají odkazy. *Sankey* diagram je ideální volbou zobrazení pro propojení dat typu *many-to-many*[1]. Diagram zobrazuje v prohlížeči grafické vektorové struktury SVG nebo VML (angl. *Vector Markup Language*) podle toho, co je pro daný prohlížeč vhodnější. *Sankey* diagram je součástí dostupné otevřené knihovny `D3.js` popsané v kapitole 2.1. [74]

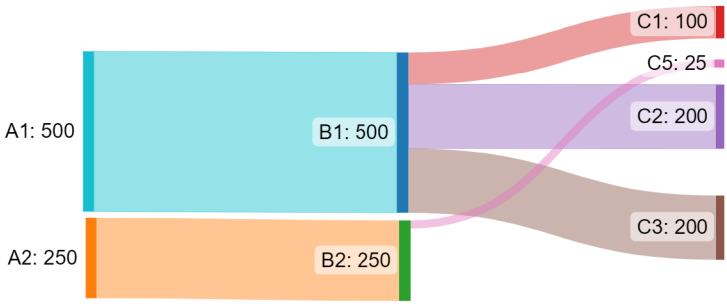
Výhodou diagramu je, že se dá naprogramovat v interaktivní formě, např. při najetí myší na odkaz se zobrazí popisek s názvem zdrojového a cílového uzlu a hodnotou šířky odkazu či lze jednoduše vykreslit celou cestu ze zdrojového uzlu do uzlu cílového pomocí změny barvy odkazů na cestě. *Sankey* diagram lze zobrazit v mnoha úrovních (sloupcích, viz obr. 3.1)[2]. Knihovna diagramu si řeší rozložení uzlů automaticky, alternativně lze přidat funkce pro zobrazení uzlů ve specifickém pořadí a v konkrétních sloupcích. Jakmile diagram obsahuje velké množství dat, nese s sebou významnou vizualizační slabinu a tou je nepřehlednost. Tomu se však alespoň částečně dá zabránit zvýrazněním požadované cesty od zdrojového uzlu k cílovému, jak bylo popsáno výše, nebo zajistit interaktivitu v podobě rozbalení a sbalení uzlů diagramu při kliknutí na prvek.

Prvním návrhem zobrazení je tedy mapování Sigma pravidel na různé parametry v několika úrovních za pomocí *Sankey* diagramu z knihovny `D3.js`. Jednotlivé úrovně (sloupce) obsahují data:

1. úroveň – fáze modelu *Cyber Kill Chain*;
2. úroveň – různé vektory kybernetických útoků;
3. úroveň – techniky útoků obsažené v modelu MITRE *ATT&CK*;
4. úroveň – zdroj vygenerovaných dat;

[1] Jedná se o typ mapování mnoho dat ku mnoha datům.

[2] Obrázek byl pro demonstrační účely vytvořen na stránce: `https://sankeymatic.com/build/`.



Obr. 3.1: Příklad grafického zobrazení *Sankey* diagramu.

5. úroveň – samotná Sigma pravidla, která odpovídají vlastnostem v předchozích úrovních.

Výhodou tohoto typu zobrazení je, že zákazník dokáže přesně určit, která pravidla nasadit k zajištění své bezpečnostní strategie. Získá povědomí o tom, která pravidla jsou doporučena k implementaci na základě kritérií uvedených v jednotlivých úrovních.

3.2 Zobrazení pomocí *Sunburst* diagramu

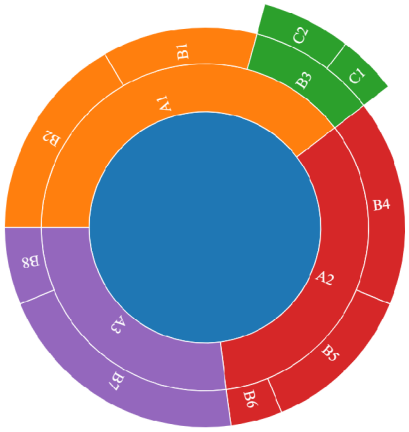
Diagram *Sunburst* je další populární způsob zobrazení dat, která vyžadují hierarchické uspořádání. Diagram[3] vykresluje data vektorovou grafikou v kruhové podobě viz obr. 3.2. Každý hierarchicky nadřízený uzel představuje rodiče a podřízený uzel potomka. Velikost každého segmentu grafu představuje část kruhu, kterou element zabírá. Graf *Sunburst* je součástí otevřené knihovny `D3.js`. [75]

Výhodou tohoto kruhového diagramu je schopnost přizpůsobení se a je vhodný pro větší množství dat, která si vyžadují zobrazení v příjemné srozumitelné formě. Graf *Sunburst* lze také naprogramovat do interaktivní podoby, která umožňuje uživatelům přibližovat a oddalovat požadovanou část diagramu, a tak zajistit detailnější pohled na data. Obdobně jako u *Sankey* diagramu umožňuje *Sunburst* zobrazit popisky uzlů včetně jejich velikosti.

Druhý návrh zobrazení tedy spočívá ve vytvoření kruhového diagramu *Sunburst* dostupného v knihovně `D3.js`. Získání informací o doporučených Sigma pravidlech by mohlo vycházet z podobného způsobu obsahu úrovní jako v zobrazení pomocí *Sankey* diagramu viz kapitola 3.1. Zde není však výhodné použít stejné uspořádání, konkrétně není vhodné ponechat zdroj dat až na čtvrté úrovni. A to z toho důvodu, že různé názvy zdrojů dat by se v rámci celého obvodu čtvrté úrovně velmi často

[3]Obrázek byl pro demonstrační účely vytvořen na stránce: `https://codepen.io/thecraftycoderpdx/pen/rJYNRv`.

opakovaly a to by mohlo působit nepřehledně. Částečným řešením tohoto problému by mohlo být umístění zdrojů dat na druhou úroveň, kde by se názvy opakovaly v podstatně menší míře, nebo zdroje dat ze zobrazení vynechat. Na základě těchto poznatků lze vyvodit závěr, že kruhové zobrazení dat pro výběr konkrétního Sigma pravidla není vhodnou volbou.

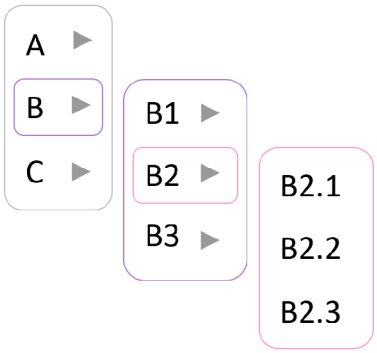


Obr. 3.2: Příklad grafického zobrazení *Sunburst* diagramu.

3.3 Tabulkové zobrazení

Zobrazení dat pomocí tabulky je jedním z nejjednodušších řešení grafické reprezentace dat. Zejména interaktivní forma rozevíracích nabídek s sebou nese mnoho výhod. Šetří místo na stránce, zajišťuje ustálený a esteticky příjemný vzhled uživatelského rozhraní a zajišťuje přehlednost dat. Je vhodný i pro velké množství dat a jejich uspořádání bude stále stejné a přehledné. Příklad rozevírací nabídky ilustruje obr. 3.3.

Třetí možností zobrazení Sigma pravidel, které jsou vhodné k implementaci v závislosti na kritériích je právě rozevírací nabídka. Toto zobrazení lze použít také pro hierarchické mapování dat, které bylo popsáno v kapitole 3.1. Ačkoliv rozevírací nabídky na první pohled neposkytují tak jednoznačné mapování jako *Sankey* diagram, mohou být při prozkoumávání dat mnohem přehlednější. Uživatel se může proklikávat různými kritérii, která mu pomohou vybudovat bezpečnostní strategii. S tabulkovým zobrazením souvisí další návrhy vizualizace pravidel, které jsou popsány v následujících podkapitolách.



Obr. 3.3: Příklad rozevírací nabídky.

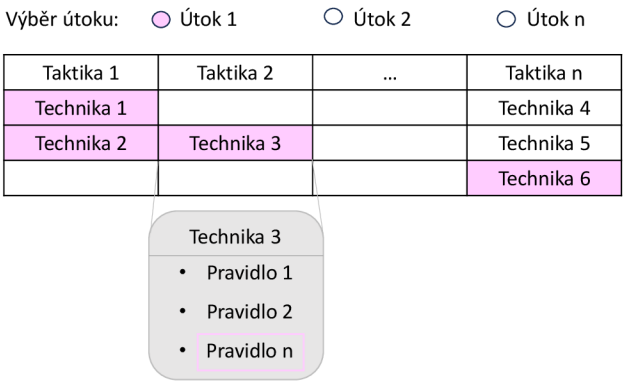
3.3.1 Zobrazení v matici *ATT&CK*

Pomocí rozevírací nabídky lze také naprogramovat logiku filtrování v databázi dat. Čtvrtý návrh zobrazení pracuje právě s filtrací dat v databázi, kde každé Sigma pravidlo disponuje hodnotou unikátního identifikátoru. Pomocí tohoto identifikátoru lze v databázi snadno nalézt konkrétní pravidlo. Návrh předpokládá existenci vizuální podoby matice *ATT&CK* ve webové aplikaci. Uživatel by v tomto případě mohl být schopen vybrat si konkrétní pravidlo, které by získal doporučením na základě požadovaných kritérií např. ze zobrazení v *Sankey* diagramu, a po vybrání pravidla by se podbarvila konkrétní MITRE technika v matici *ATT&CK*. Protože jednou z funkčních částí aplikace je právě vytváření, správa a autentizace uživatelů, je možné udržovat seznam implementovaných pravidel určitého uživatele a to právě pomocí přehledného zabarvení konkrétní buňky matice.

Jak již bylo zmíněno v kapitole 1.6, organizace ENISA každoročně vydává report o aktuálních kybernetických hrozbách. Reporty mimo jiné obsahují mapování kybernetických útoků na jednotlivé MITRE *ATT&CK* techniky. Součástí čtvrtého návrhu je tedy funkcionalita aplikace, ve které uživatel snadno z nabídky vybere jeden či více druhů kybernetických útoků, proti kterým se chce bránit. Při výběru konkrétních útoků se v MITRE matici podbarví techniky s nimi spojeny a na základě jedinečného identifikátoru či názvu *ATT&CK* technik, které jsou také obsaženy v každém Sigma pravidle, se mohou uživateli zobrazit konkrétní Sigma pravidla, která jsou s technikou spojena. Čtvrtý návrh ilustruje obr. 3.4

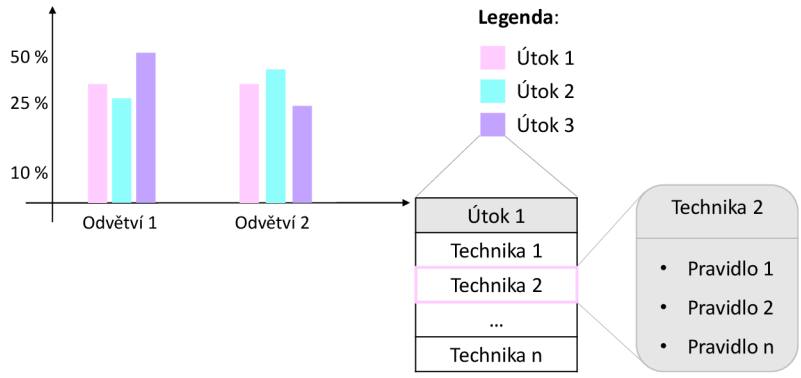
3.3.2 Zobrazení pravidel na základě ekonomické činnosti

Předchozí filtrování pravidel v databázi na základě identifikátoru nebo názvu techniky je vhodné pro uživatele či zákazníka, který má vytvořenou představu, kterou část plochy vektorů útoků potřebuje pokrýt. V praxi se však lze velmi často setkat se zákazníky, kteří vytvořenou představu nemají. A právě tento případ pokrývá pátý



Obr. 3.4: Příklad zobrazení Sigma pravidel v matici *ATT&CK*.

návrh. Tento návrh uvažuje výběr pravidel, která pokryjí potřebnou plochu vektorů útoků, na základě druhu ekonomické činnosti. Druhy ekonomických činností je myšleno např. energetika, doprava, bankovnictví, zdravotnictví a další. Součástí již dříve zmíněných každoročních reportů, které vydává organizace ENISA, jsou mj. statistiky počtu kybernetických útoků cílených na jednotlivá ekonomická odvětví. Tyhle informace se dají zpracovat do dvou pohledů. Prvním z nich je samotná tabulka, v níž uživatel získá obecný přehled počtů spáchaných útoků. Druhý pohled se zaměřuje na přehledné vykreslení statistických dat do sloupcového grafu. Jak již bylo zmíněno, z reportu organizace ENISA je možné získat nejčastější MITRE *ATT&CK* techniky používané při útocích. Také zobrazení pomocí grafu uvažuje existenci těchto dat. Uživatel by byl schopen rozšířit svoji bezpečnostní strategii na základě výběru technik používaných při útocích. Zobrazení ilustruje obr. 3.5.



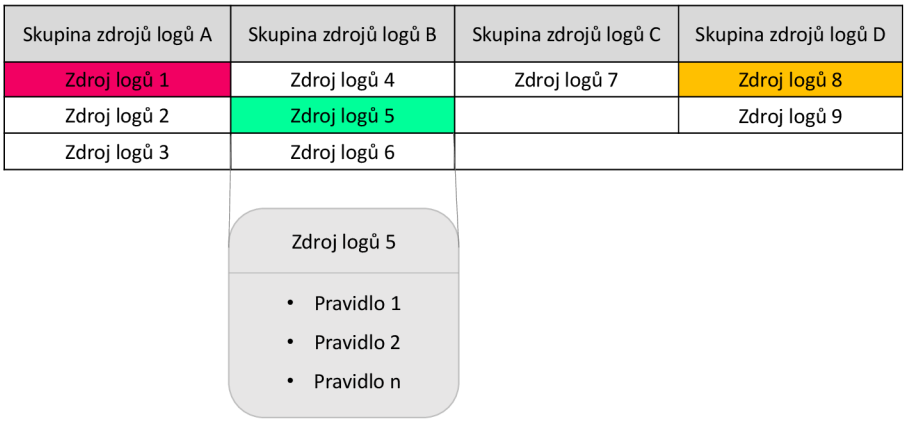
Obr. 3.5: Příklad zobrazení Sigma pravidel na základě výběru sektoru a útoku.

3.3.3 Zobrazení pravidel na základě zdrojů logů

Dalším pohledem patřícím mezi tabulkové vizualizace je zobrazení pravidel na základě zdrojů logů. Což může tvořit další kritérium pro vytvoření komplexní bezpečnostní strategie. Každé Sigma pravidlo obsahuje informaci určující typ dat, na které se pravidlo vztahuje. Zobrazení rozlišuje čtyři skupiny zdrojů logů:

- Bezpečnostní aplikace (např. antivirus),
- operační systémy (např. Windows),
- síťová zařízení (např. GitHub),
- ostatní aplikace (např. proxy server).

Pohled je navržen do vertikální struktury, kde jednotlivé skupiny logů tvoří záhlaví a konkrétní zdroje logů řádky tabulky. Logika zobrazování pravidel je obdobná jako u zobrazení v MITRE *ATT&CK* matici. Jestliže zdroj logů obsahuje alespoň jedno Sigma pravidlo, je po kliknutí na buňku tabulky zobrazeno dialogové okno se seznamem pravidel. Buňky tabulky jsou podbarveny na základě procentuální počtu výskytu pravidel. Pohled pomocí zdrojů logů znázorňuje obr. 5.5.

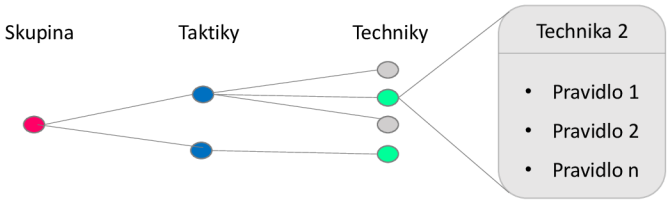


Obr. 3.6: Příklad zobrazení Sigma pravidel na základě zdrojů logů.

3.4 Zobrazení pravidel na základě skupin hrozeb

Jak již bylo vysvětleno v kapitole 1.2 kybernetické útoky se stávají stále více sofistikovanější. Kybernetické útoky nemusí být prováděny izolovaně, např. pouze *phishing* techniky či pouze spuštění škodlivého kódu. Ve většině případů je třeba na vektory útoků pohlížet uceleně. Za trvalými významnými hrozbami mohou stát skupiny aktérů hrozeb. Skupiny hrozeb používají k dosažení vytyčeného cíle určité vektory útoku a běžně se skupiny zaměřují na organizace, které působí ve specifickém ekonomickém odvětví, např. bankovnictví.

Sedmý návrh pohledu na Sigma pravidla tedy spočívá v zobrazení konkrétních pravidel na základě výběru známých skupin hrozeb. Návrh předpokládá, že zákazník má povědomí o existenci skupin hrozeb a chce vytvořit obranný štít proti technikám konkrétní skupiny hrozeb. Informace o nositelích hrozby lze získat z oficiálních databází MITRE *CREF Navigator* a MITRE *ATT&CK groups*.[4] Poslední forma vizualizace uvažuje existenci interaktivní tabulky, která obsahuje informace o jednotlivých APT skupinách. V této tabulce lze vyhledávat podle klíčových slov a řadit položky podle abecedy. Každý záznam tabulky obsahuje referenci na otevření dialogového okna. V něm je vykreslena interaktivní horizontální stromová struktura, která mapuje specifickou skupinu hrozeb na MITRE taktiky a techniky, které jsou APT skupinou využívány. Listy stromu neboli uzly, které nemají potomky, jsou barevně odlišeny v závislosti na tom, zda má uživatel již implementované alespoň jedno pravidlo pokrývající techniku. V tomto pohledu si také uživatel dokáže zobrazit pravidla na základě výběru techniky ve stromové struktuře. Interaktivní stromová struktura mapování zmíněných dat je vyobrazena na obr. 3.7.



Obr. 3.7: Příklad zobrazení Sigma pravidel na základě výběru APT skupiny a korespondující MITRE techniky.

3.5 Návrh pro zobrazení webové stránky

Při tvorbě návrhu designu webové stránky je nejprve vhodné rozmyslet si její základní strukturu (viz obr. 3.8). Důležité je také brát v úvahu účel webové stránky. Webová stránka si klade za cíl intuitivní zobrazení Sigma pravidel dle různých kritérií a v souvislosti v různými druhy dat. Obecná struktura aplikace se skládá ze tří částí:

- **horizontální navigační lišty**, která umožňuje přesměrovávat uživatele mezi jednotlivými funkčními částmi aplikace;
- **vertikální navigační lišty**, která umožňuje uživateli přepínat mezi vizualizačními komponentami;

[4]Informace o skupinách hrozeb lze nalézt na adresách MITRE *CREF*: `https://crefnavigator.mitre.org/tree2` a MITRE *ATT&CK*: `https://attack.mitre.org/groups/`.

- **obsahu stránky**, který tvoří pohledy na vizualizaci uživatelských Sigma pravidel dle různých kritérií.

Obr. 3.8: Rozložení elementů webové stránky.

Kromě struktury stránky je také důležité navrhnout, jakým způsobem by měla být data zobrazena. Návrh plyne z analýzy provedené v kapitole 3. Klientská část webová aplikace disponuje čtyřmi hlavními pohledy a k navigování mezi nimi slouží vertikální přepínače. Taktéž je v každém pohledu přítomná základní horizontální navigační lišta pro přepínání mezi dalšími funkčními částmi aplikace, které nejsou součástí této práce. První pohled se skládá ze dvou komponent, mezi nimiž lze navigovat pomocí dalších horizontálních přepínačů. Obě komponenty vychází ze základní MITRE *ATT&CK* matice. V první komponentě jsou zvýrazněny jednotlivé techniky na základě procentuálního počtu uživatelských pravidel obsahující označení konkrétní techniky. Druhá komponenta prvního pohledu se zaměřuje na podbarvení MITRE *ATT&CK* technik, které jsou získány po vybrání určitého kybernetického útoku uživatelem. Druhý pohled tvoří vertikálně strukturovaná tabulka, jejíž buňky obsahují různé druhy zdrojů dat. Buňky jsou též podbarveny na základě procentuálního počtu uživatelských pravidel obsahující označení konkrétního zdroje logů. Třetí pohled se opět skládá ze dvou komponent a pro zachování konzistentního vzhledu aplikace, je také využita další vodorovná lišta pro směrování mezi komponentami. První komponenta třetího pohledu obsahuje tabulku statistik vykonaných kybernetických útoků na různá ekonomická odvětví. Druhá komponenta zobrazuje stejná statistická data ve sloupcovém grafu a v rámci legendy je možné zobrazit MITRE *ATT&CK* techniky používaných v kybernetických útocích prováděných na ekonomické sektory. Poslední pohled se věnuje zobrazení informací o skupinách hrozeb a vizualizaci mapovaných dat v interaktivní horizontální stromové struktuře. Detailní popis implementace všech zobrazení bude více popsán v kapitole 4.2

4 Implementace vhodné formy vizualizace

Tato kapitola bude věnována popisu experimentálního prostředí, ve kterém byla vyvíjena webová aplikace, a popisu samotného řešení grafického uživatelského rozhraní klientské části webu.

4.1 Popis experimentálního prostředí

Grafické uživatelské rozhraní neboli frontend webové aplikace bylo vyvíjeno v rámci domácí sítě za použití vývojového prostředí *Visual Studio Code*. Pro úplné fungování klientské části aplikace je nutná komunikace s backend (funkční) částí aplikace. Backend aplikace je součástí experimentální sítě pana Ing. Yehora Safonova. Pro vzdálený přístup k experimentální síti je nutné použití VPN zabezpečeného tunelu. Ve vzdálené síti se nachází webový server určený pro běh kódu aplikace. Webový server je opatřen IP adresou 10.50.0.2 a běží na operačním systému Linux. Aplikace, kterou tato práce rozšiřuje, je založená na architektuře mikroservis[1]. Nejdůležitějšími mikroservisami pro tvorbu této práce je mikroservisa pravidel a mikroservisa *matrix*. Mikroservisa pravidel pravidelně získává data z mikroservisy *Sigma*, která pracuje s nástrojem *Git* a z něj pravidelně dynamicky získává pravidla, která následně mikroservisa pravidel ukládá do databáze. K položkám v databázi pak lze snadno přistupovat pomocí HTTP požadavků na tzv. *endpointy*. Mikroservisy následně provádějí API požadavky na získání dat z databáze. Mikroservisa *matrix* získává data pro zobrazení pomocí zdrojů logů a MITRE *ATT&CK* matice. Taktéž řeší funkcionalitu zvýrazňování buněk v maticích na základě procentuálního počtu uživatelských pravidel z celkového počtu pravidel. Veškeré součásti webové aplikace jsou nasazené na vývojovém serveru ve formě *Docker* kontejnerů[2].

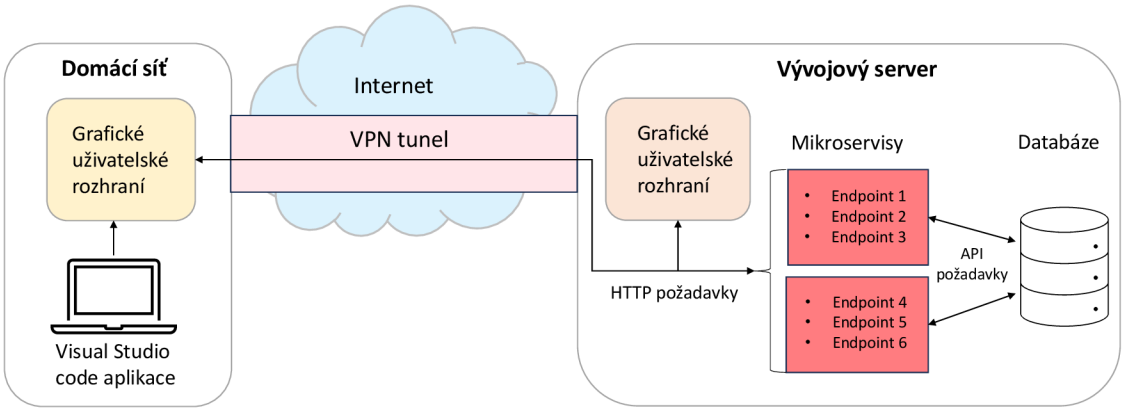
Princip vývoje a připojení do experimentální sítě znázorňuje obr. 4.1. Celková zmíněná síť je mnohem rozsáhlejší, ale pro účely této práce je dostačující zjednodušená topologie. Je důležité zmínit, že původní aplikace, kterou tato práce rozšiřuje, disponuje vlastním grafickým uživatelským rozhraním. Klientská část vyvíjená v rámci této bakalářské práce tedy následně stávající frontend rozšíří.

4.2 Realizace řešení

Jak již bylo zmíněno v kapitole 3.5, struktura webové stránky je rozdělena do třech částí – horizontální navigační lišty, vertikální navigační lišty a obsahu stránky.

[1] Jedná se o logické části aplikace, z nichž každá se zaměřuje na plnění konkrétní funkcionality.

[2] Kontejnery *Docker* umožňují rychlé spouštění aplikací v prostředí odděleném od základního systému [50].



Obr. 4.1: Zobrazení části experimentálního prostředí.

Horizontální navigační lišta obsahuje logo aplikace, název webové stránky a tři tlačítka pro přepínání mezi funkčními částmi aplikace. První tlačítko tvoří odkaz na seznam veškerých Sigma pravidel a pod druhým tlačítkem se skrývá seznam uživatelských pravidel. První dvě tlačítka slouží k přesměrování na funkcionality aplikace, které byly vytvořeny v rámci jiné práce. V rámci této práce byl vytvořen pohled *Vizualization*, který si klade za cíl zobrazit uživateli jeho uložená pravidla dle různých kritérií a v několika odlišných grafických komponentách.

Při navigování mezi pohledy se ve skutečnosti se nejedná o načtení nové stránky ze serveru. Klientská část webu je vyvíjena za účelem zachování tzv. *Single-page Application* přístupu. Aplikace *Single-page* jsou takové, které načtou HTML stránku a následně dynamicky aktualizují obsah této stránky pomocí jazyka Javaskript, bez načítání celé nové stránky ze serveru [73]. Navigování pomocí vertikální lišty v rámci záložky *Vizualization* je implementováno pomocí přepínání mezi komponentami `Vue`. V url adrese je tedy vždy vidět cesta */matrix* nezávisle na komponentě, která je právě načtena. Pro všechny vizualizační komponenty totiž cesta */matrix* tvoří nadřazený `Vue` pohled (angl. *view*), v níž jsou všechny komponenty registrovány a je mezi nimi přepínáno pomocí podmínek *v-if*. Jestliže není uživatelem vybrána žádná komponenta k zobrazení, automaticky se načítá komponenta matice *ATT&CK*. Obdobně je tomu při prvním načtení aplikace a úspěšné autentizace uživatele.

4.2.1 Pohled na matici *ATT&CK*

Jak již bylo zmíněno první pohled se zaměřuje na zobrazení pravidel v matici MITRE *ATT&CK*. Klasická matice tedy tvoří výchozí bod pro následující dva pohledy. Následující pohledy zastřešuje nadřazená komponenta, která slouží jako šablona pro obě komponenty. Jsou v ní obě komponenty registrované a obsahuje dílčí horizontální

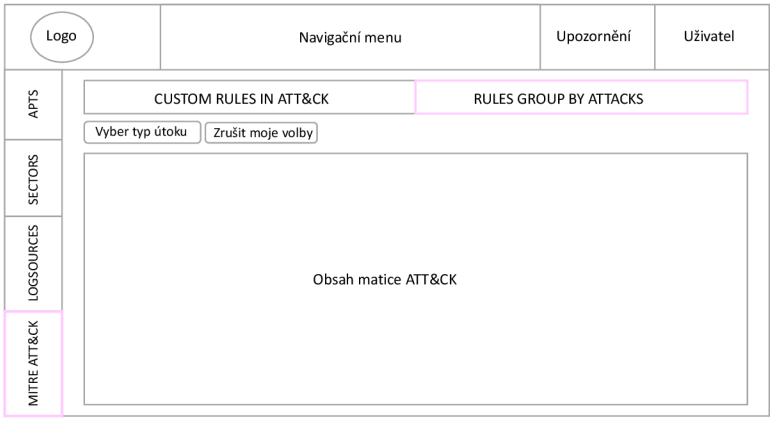
navigační lištu pro přepínání mezi komponentami. Mezi komponentami je přepínáno pomocí podmínek *v-if* a *v-else*. Při načtení se automaticky zobrazí první komponenta matice *ATT&CK*.

Při načtení výchozí komponenty je zobrazena matice *ATT&CK*. Záhlaví matice tvoří názvy MITRE taktik a buňky matice jsou vyplněny názvy MITRE technik (popis matice viz kapitola 1.2). Data jsou získávána ze serveru pomocí HTTP požadavku na koncový bod */getMitreMatrix*, který je definován v rámci backendové části aplikace. Při načítání dat je zobrazen indikátor načítání, aby uživatel neměl pocit, že je stránka prázdná. V rámci backendu je také definován endpoint pro získávání identifikátoru a názvu uživatelských pravidel spojených s konkrétní MITRE technikou. Dále je definovaná funkce pro získávání barvy pro buňky matice na základě procentuálního počtu uživatelských pravidel v poměru ku všem pravidlům. Barvy na pozadí buněk signalizují uživateli, kolik pravidel pokrývá konkrétní MITRE techniku (červená – nejméně, zelená – nejvíce pravidel). Jestliže má uživatel uloženo alespoň jedno pravidlo pokrývající specifickou techniku, zobrazí se po rozkliknutí dialogové menu se seznamem uložených pravidel. Pro zachování konzistentnosti vzhledu aplikace je zmíněné dialogové menu součástí všech pohledů. Obsahuje vždy název MITRE techniky a seznam pravidel s ním spojených. Po kliknutí na pravidlo ze seznamu je uživatel přesměrován na stránku všech klientských pravidel, jejíž zobrazení nebylo předmětem této práce.

Druhá komponenta je schématicky vykreslena na obr. 4.2. První komponenta disponuje obdobnou strukturou rozložení elementů, pouze neobsahuje tlačítka „vyber typ útoku“ a „zrušit moje volby“. Druhá komponenta je skrytá pod druhou záložkou dílčí horizontální navigace *Rules group by attacks*, na kterou nasměruje uživatele po kliknutí podmínka *v-if*. Tato komponenta využívá existující MITRE *ATT&CK* matici. Primárně se však zaměřuje na zvýraznění MITRE technik konkrétních vybraných útoků.

Jak již bylo zmíněno v kapitole 1.6 z každoročních reportů lze získat informace o technikách, které jsou útoky nejčastěji používány. Mapování názvu útoků na identifikátory a názvy MITRE technik je uloženo v souboru ve formátu json. V kódu je vytvořena funkce, která načítá zmíněný json soubor a data z endpointu */getMitreMatrix* ihned po načtení komponenty. Obě odpovědi jsou následně kombinovány tak, aby výsledný formát dat byl obdobný jako na obr. 4.3 a tím se zajistilo mapování názvů útoků a technik dostupných v souboru na nadřazené taktiky.

V rámci kódu je také definovaná reaktivní reference, která udržuje vztah názvů útoků, cesty k obrázkům korespondujících s útoky a položku pro udržování stavu, které z útoků byly uživatelem vybrány (hodnota nastavena na *true*) a které zůstávají neoznačeny (hodnota *false*). Po kliknutí na tlačítko „vyber typ útoku“ (viz obr. 4.2) se uživateli otevře dialogové okno s mřížkou, jehož strukturu ilustruje obr. 4.4.

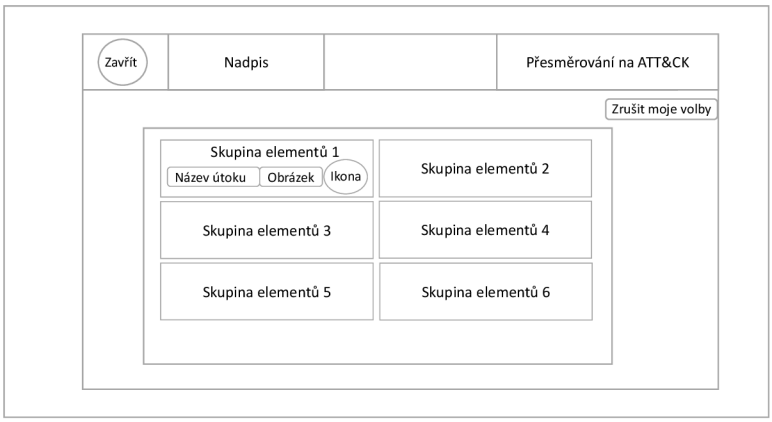


Obr. 4.2: Struktura prvního pohledu pomocí *ATT&CK* matice.

```
tableName: "DDOS"
data:
    category: ['Resource Development']
    id: "T1583"
    tactic: "Acquire Infrastructure"
```

Obr. 4.3: Příklad kombinovaných dat pro zobrazení dle útoků.

Skupiny elementů vždy obsahují tlačítko s názvem útoku, obrázek, který vystihuje typ útoku, a ikonu fajfky. Po kliknutí na kterýkoliv z elementů se změní barva tlačítka a ikony a stav vybraných útoků se aktualizuje. Opětovným kliknutím je možné útok odebrat ze sledovaných. Je možné vybrat jeden nebo více útoků. Vybráním typu útoků se zapíší názvy používaných technik do pole, které je následně procházeno a techniky jsou vyhledávány v kombinovaných datech (viz obr. 4.3). Prohledávání v kombinovaných datech je důležité pro získání mapování MITRE technik na taktiky a na základě dvojic techniky a taktiky jsou v matici podbarvovány specifické buňky. Zrušit uživatelský výběr pravidel lze pomocí tlačítka, které se nachází v komponentě i v dialogovém okně pro výběr útoku. Jestliže má uživatel zaregistrováno alespoň jedno pravidlo související s technikou, je po kliknutí na techniku zobrazeno opět dialogové okno se seznamem pravidel obdobně jako u první komponenty. Zda technika obsahuje alespoň jedno uživatelské pravidlo pomáhá v obou komponentách zjistit titulek obsahující počet pravidel po najetí myší na techniku a také změna druhu kurzoru. Jestliže technika neobsahuje žádné pravidlo, zůstává kurzor výchozí v podobě šipky. Pakliže ale obsahuje alespoň jedno pravidlo, změní se kurzor při najetí myší na techniku na ukazatel.



Obr. 4.4: Struktura dialogového okna pro výběr útoku.

4.2.2 Pohled na matici zdrojů logů

Druhý pohled v rámci druhé záložky vertikální navigační lišty se zaměřuje na zobrazení pravidel podle druhu zdrojů dat, tedy podle aplikací, platforem, zařízení a systémů, ze kterých jsou generované logovací zprávy. Tento pohled vychází z analýzy návrhů provedené v podkapitole 3.3.3. Data pro vertikální tabulkové zobrazení jsou načítána ze serveru pomocí HTTP požadavků na koncový bod podobně, jako tomu bylo u dat pro MITRE *ATT&CK* matici. Endpoint, který získává data pro tabulku z databáze, je definován v backendové části aplikace a nese název */getLogsourceMatrix*. Pohled na pravidla seskupených dle zdrojů dat je koncipován obdobně jako pohled na MITRE matici. Při stahování dat ze serveru se objevuje indikátor načítání dat. Rovněž jsou jednotlivé buňky zabarveny dle procentuálního počtu uživatelských pravidel náležící určitému zdroji logů ku celkovému počtu všech klientských pravidel. Stejně tak pro otevření dialogového okna se seznamem všech pravidel je nutné, aby specifický zdroj logů pokrýval alespoň jedno pravidlo. Zda zdroj logů pokrývá minimálně pravidlo, je uživatel schopen zjistit okamžitě bez dalších klikání a to podobně jako bylo popsáno v podkapitole 4.2.1 – tedy pomocí titulku s počtem pravidel při najetí myší na buňku a pomocí změny druhu kurzoru myši.

4.2.3 Pohled na pravidla dle druhů sektorů

Třetí pohled se znovu skládá ze dvou komponent, které jsou spojeny nadřazenou komponentou. Rodičovská komponenta obsahuje registraci komponent a dílčí horizontální navigační lištu. Mezi komponentami je přepínání ztvárněno stejným způsobem jako bylo popsáno v podkapitole 4.2.1, tedy pomocí podmínek *v-if* a *v-else*. První komponenta disponuje tabulkou, ve které jsou zaznamenány statistiky

procentuálních počtů kybernetických útoků prováděné na sektory jako jsou např. veřejná správa, cílená osoba či široká veřejnost, zdravotnictví, digitální infrastruktura a další. Tabulka je vykreslena pomocí `Vuetify` komponenty *v-table*. Číselné záznamy v tabulce jsou barevně zvýrazněny podle jejich hodnoty:

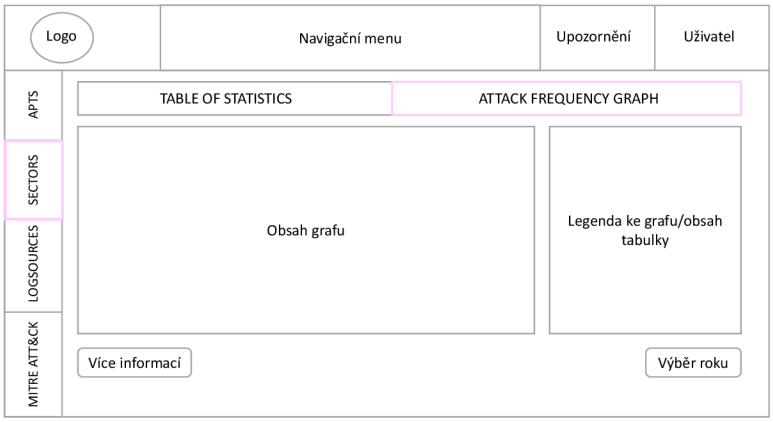
- 0–13 % – zelená barva značí nízké procento vykonaných útoků;
- 14–17 % – žlutá barva signalizuje středně vysoký počet útoků;
- 18–29 % – oranžová barva označuje vysoký počet kybernetických útoků;
- 30 a více % – červená barva značí velmi vysoký počet vykonaných útoků na ekonomické odvětví.

Data v tabulce jsou načítána ze souboru formátu json a značky pro stylování buněk jsou součástí souboru. Následně je stylování prováděno v kódu pomocí kaskádových stylů. Tlačítko pod tabulkou „více informací“ informuje uživatele o původu statistických dat. Tlačítko je spojeno s reaktivní referencí a lze pomocí něj otevřít dialogové okno a opětovným kliknutím nebo kliknutím na ikonu křížku jej znovu uzavřít, tedy nastavit hodnotu reference na nepravdu (angl. *false*). Komponenta rozevírací nabídky „výběr roku“ umožňuje uživateli vybrat časové období, pro které požaduje načíst statistická data. Pro tuto práci byla zpracována data za období červen 2022–2023. V době dokončení této práce ještě nebudou k dispozici statistiky od organizace ENISA na další období (2023–2024), proto tvoří období 2022–2023 výchozí a jediný výběr v nabídce.

Dominantou druhé komponenty třetího pohledu je seskupený sloupcový graf, který vykresluje stejná statistická data pro období 2022–2023 jako tabulka v první komponentě. Strukturu druhé komponenty je možné nalézt na obr. 4.5. Graf i jeho legenda jsou kódovány pomocí knihovny `D3.js` (viz analýza v podkapitole 2.1.2). Šířka kontejneru obsahující graf i legendu je dynamicky přizpůsobena šířce uživatelské zobrazovací jednotce. V kódu je definován tzv. posluchač událostí, který při změně šířky okna prohlížeče změní i šířku kontejneru, která je nastavena na 75 % celkové šířky zobrazovací jednotky. Osa x zahrnuje popisky názvů jednotlivých ekonomických odvětví, které jsou pro lepší čitelnost rotovány o 15 stupňů doprava. Délka horizontální osy koresponduje s nastavenou šířkou grafu. Hodnoty na vertikální ose y přidává knihovna `D3.js` automaticky. V kódu je definován pouze rozsah hodnot svislé osy, tedy od nuly do maximální hodnoty procentuálního počtu kybernetických útoků. Pro lepší orientaci v grafu jsou vykresleny tenké vodorovné vodící čáry, které začínají vždy v popiskách hodnot svislé osy a končí podobně jako osa x při dosažení přednastavené šířky grafu. Sloupce v grafu představují procentuální počet jednotlivých kybernetických útoků provedených na specifické ekonomické odvětví. V kódu je vytvořený objekt, který mapuje názvy útoků na barvy v hexadecimálním tvaru. Těmito barvami jsou následně vyplněny jak sloupce útoků v grafu, tak položky legendy související s názvy útoků. Při vykreslování sloupců grafu je viditelná

také animace pro růst sloupců odspodu nahoru, která trvá dvě sekundy.

Součástí kontejneru pro vykreslení je i zmíněná legenda. Legenda vykresluje názvy kybernetických útoků a před nimi čtverečky o velikosti 18×18 pixelů vyplněné barvami z mapovacího objektu popsaného dříve. Po najetí myší na čtvereček legendy se element zvýrazní bílým stínem a kurzor se změní na ukazatel. Tyhle změny již uživateli naznačují, že se jedná o aktivní tlačítko. Po kliknutí na čtvereček se uživateli místo legendy zobrazí tabulka. Tabulka je jedinečná pro všechny čtverečky legendy, protože se vztahuje k názvu útoku a v řádcích vrací seznam použitých MITRE technik konkrétního útoku. Data pro tabulky jsou získávána podobných způsobem jako u zobrazení v matici *ATT&CK* (viz podkapitola 4.2.1), tedy pomocí kombinace dat z lokálního json souboru a dat vrácených z koncového bodu */getMitreMatrix*. Po najetí myší na určitou MITRE techniku ze seznamu se zobrazí titulek s počtem uživatelských pravidel, které techniku pokrývají. Jestliže je počet pravidel nenulový, kurzor myši se změní na ukazatel a lze na řádek kliknout a tak zobrazit dialogové okno se seznamem uživatelských uložených pravidel, které je stejné jako v předchozích zobrazeních pro zachování jednotnosti vzhledu aplikace.



Obr. 4.5: Struktura třetího pohledu dle druhů sektorů.

4.2.4 Pohled na pravidla dle skupin hrozeb

Čtvrtý pohled skrytý v poslední záložce vertikální navigační lišty se zaměřuje na získání informací o skupinách hrozeb a zobrazení uživatelských pravidel za pomocí vykreslení horizontální stromové struktury knihovny `D3.js`. Při načtení zobrazení se vykreslí interaktivní tabulka kódovaná pomocí `Vuetify` komponenty *v-data-table*. Záhlaví tabulky obsahuje položky:

- ID skupiny hrozeb – jedinečný identifikátor skupiny hrozeb dle společnosti MITRE ve formátu „Gxxxx“, kde „xxxx“ je číselná hodnota, např. G0005.

- Jméno nositele hrozby – nese označení ve tvaru „APT“ a připojenou číselnou hodnotou, např. APT12.
- Asociované skupiny – jsou to skupiny přímo nebo nepřímo spojené se skupinami APT. Může je spojovat používání stejných technik nebo zastřešení stejnou sponzorskou zemí.
- Popis skupiny – poskytuje více informací o konkrétní skupině hrozby.
- Vizualizace – zobrazí grafickou strukturu stromu pro nositele hrozby.

V kódu je definován objekt s položkou, která rozhoduje, zda mají být řádky tabulky podle sloupce řaditelné či nikoliv. Řazení řádků je povoleno pouze pro sloupce „ID skupiny hrozeb“ a „Název nositele hrozby“. Řadit lze najednou pouze dle jednoho sloupce vzestupně či sestupně. Je možné provádět vyhledávání nad daty v tabulce, které je nezávislé na velikosti písmen. Vyhledávání je prováděno v textovém poli `Vuetify` *v-text-field* a je nastaveno s možností vyčistění pole. Tedy uživatel nemusí ručně mazat to, co si přál vyhledat, ale stačí stisknou křížek. Více informací o dané APT skupině je možné zobrazit kliknutím na šipku v konkrétním řádku a stejně tak ji zpět zabalit. Poslední sloupec tabulky obsahuje v každém řádku ikonu stromové struktury. V kódu jsou nastaveny pro zobrazení tři řádky tabulky. Ale komponenta *v-data-table* obsahuje rozevírací nabídku s možnostmi počtu zobrazených řádků: 3, 5, 10 a všechny. Stejně tak je možné přepínat mezi skupinami zobrazených řádků vpřed i vzad. Popsaná data jsou do tabulky načítána pomocí HTTP požadavku na koncový bod */getAptTable*, který vrací data z databáze umístěné na serveru. Pod tabulkou je opět umístěno tlačítko reaktivní reference na otevírání dialogu pro získání více informací o datech, se kterými tento pohled pracuje. Ikony v posledním sloupci při kliknutí vrací název APT skupiny a otevírají dialogové okno s kompletním vykresleným `D3.js` interaktivním stromem.

V rámci této práce a zobrazení dle skupin hrozeb byla data pro tabulku a stromy nejprve posbírána a simulována v podobě json souborů a následně byly v rámci jiné závěrečné práce vytvořeny koncové body pro dynamické načítání dat z databáze a snazší správu těchto dat. Stromy knihovny `D3.js` vyžadují pro správné zobrazení hierarchických dat specifický formát dat, který naznačuje obr. 4.6. Data pro `D3.js` stromy jsou tedy získávána pomocí HTTP požadavků na koncový bod */getAptTree*. Protože endpoint vrací více informací, než je pro účely tohoto zobrazení nutné, bylo třeba vyfiltrovat pouze názvy skupin hrozeb a jejich používané techniky. Dále bylo nutné vyfiltrovaná data kombinovat s daty vrácenými z koncového bodu */getMitreMatrix* pro získání nadřazených taktik ke všem používaným technikám. Kombinování dat pro všechny stromy probíhá ihned při načtení komponenty. `D3.js` stromy jsou vykreslovány právě pomocí kombinovaných dat. Filtrování dat pro zobrazení stromu konkrétní skupiny hrozeb probíhá až po kliknutí na ikonu ve sloupci „vizualizace“.

```
name: "APT skupina",
children: [{
    name: "Taktika",
    children: [{
        name: "Technika",
        children: [{
                name: "Pravidlo"
        }]
    }]
}]
```

Obr. 4.6: Formát dat pro `D3.js` stromy.

Po zobrazení dialogu se vykreslí kompletní strom, který má rozbalené všechny větve a všichni potomci jsou viditelní. Nad samotnou horizontální stromovou strukturou je zobrazen nadpis, který informuje, pro kterou APT skupinu hrozeb byl strom vykreslen. Dialog lze uzavřít kliknutím na ikonu křížku nebo mimo obsah dialogového okna. Některé APT skupiny používají velké množství technik a strom působí nepřehledně. Proto dialog obsahuje tlačítko pro sbalení všech uzlů stromu, které způsobí vykreslení pouze kořenového uzlu – názvu APT skupiny. Když je celý strom sbalený, změní se název v tlačítku z původního „sbalit celý strom“ na „rozbalit celý strom“ a intuitivně se po kliknutí znovu vykreslí kompletní struktura stromu. Podobně lze sbalit nebo rozbalit celý strom nebo jen určitou větev kliknutím na libovolný uzel, který není list. List stromu je takový uzel, který neobsahuje žádné potomky.

Jednotlivé uzly stromu jsou podbarveny na základě jejich hloubky. Kořenový uzel je vybarven červenou barvou, protože představuje nositele kybernetické hrozby. Taktiky, neboli uzly v první úrovni hloubky stromu, jsou vybarveny modrou barvou. A uzly druhé úrovně, které zde představují listy stromu, disponují výchozí šedou barvou. Obdobně jako v předchozích zobrazeních jsou uživatelská Sigma pravidla zobrazována v závislosti na MITRE taktikách a technikách. Funkce pro získání pravidel tedy přijímá jako první argument jméno rodiče listu (tedy jméno taktiky) a jako druhý argument jméno listu (tedy jméno techniky). Jestliže technika obsahuje alespoň jedno pravidlo, je uzel zbarven zelenou barvou a kurzor je při najetí myší na takový uzel změněn na ukazatel. Po najetí myší na listový uzel jsou také zobrazeny titulky, které uživatele informují o počtu obsažených pravidel. V rámci jednotnosti aplikace je pro zobrazení seznamu pravidel použito stejné dialogové okno po kliknutí na zeleně zbarvený list stromu jako v předchozích zobrazeních.

5 Testování klientské části aplikace

Organizace, která spadá do sektoru zdravotnictví, dostala varování od Národního úřadu pro kybernetickou a informační bezpečnost týkající se šíření kybernetického útoku *ransomware*, za kterým stojí čínský aktér hrozby – skupina APT3. A protože organizace jednoznačně spadá pod povinné subjekty dle nařízení NIS Evropské unie, je povinná aktualizovat bezpečnostní strategii, je-li to nutné. Správce informační bezpečnosti v organizaci nechce riskovat vysoké pokuty a potřebuje se dozvědět, která slabá místa je schopen zabezpečit pomocí Sigma pravidel, aby zabránil provedení útoku *ransomware* na organizaci. Interní SOC tým správci poradil, že informace, které potřebuje, mu pomůže získat webová aplikace *Sigma Tools*. Správce již má nějaký čas založený účet v aplikaci a některá pravidla už organizace má implementována.

Po úspěšném přihlášení do aplikace je správce přesměrován na první základní pohled matice *ATT&CK*, který zobrazuje obr. 5.1. V matici lze vyčíst, že již má několik pravidel implementovaných, nejvíce jich pokrývá technika *Exploit Public-Facing Application* – šest pravidel, po kliknutí na techniku se mu zobrazí dialogové okno se seznamem pravidel. Tento pohled mu však nedodá potřebné informace, jak organizaci ochránit proti *ransomware*. Klikne tedy na druhou záložku v rámci horizontální navigace „Rules group by attacks“, zde se dozví, co potřebuje. Všimne se tlačítka „vyber typ útoku“, klikne na něj a otevře se dialogové okno (viz obr. 5.2), ve kterém zaklikne možnost *ransomware*. Označení útoku může provést kliknutím na tlačítko s názvem útoku, na obrázek i na ikonu fajfky. Při najetí myší na neoznačený útok se zobrazí titulek „vybrat“ a při najetí na označený útok se zobrazí „odebrat“. Označené útoky snadno správce pozná tak, že tlačítka změní svoji barvu z modré na fialovou a ikona fajky změní barvu z bílé barvy na zelenou a vykreslí se v kruhu. Všechny navolené útoky lze odebrat jak v dialogovém okně, tak v hlavní komponentě po kliknutí na tlačítko „zrušit moje volby“. Následně si zobrazí MITRE techniky, které jsou nejčastěji používány pro útoky *ransomware*, v matici *ATT&CK* (viz obr. 5.3). Správce si prohlédl zvýrazněné techniky a zjistil, že mnoho z nich nemá pokryté žádným pravidlem, protože se mu nezobrazilo dialogové okno. Zatímco např. technika *Create Account* obsahuje čtyři pravidla. Tuhle informaci zjistil z titulku při najetí myší na buňku, díky změně kurzoru myši z výchozí šipky na ukazatel když se po kliknutí na buňku otevřelo dialogové okno se seznamem pravidel (viz obr. 5.4). Správce ze zvědavosti zkusil označit další typ útoku a zjistil, že se v matici podbarvují buňky stále stejnou barvou, z čehož tedy není schopen odlišit, které techniky se vztahují ke kterému útoku. Na druhou stranu rozumí této implementaci, protože dva různé útoky mohou používat stejné MITRE techniky. Z toho důvodu je výhodné vybrat si jeden typ útoku a jeho techniky prozkoumat.

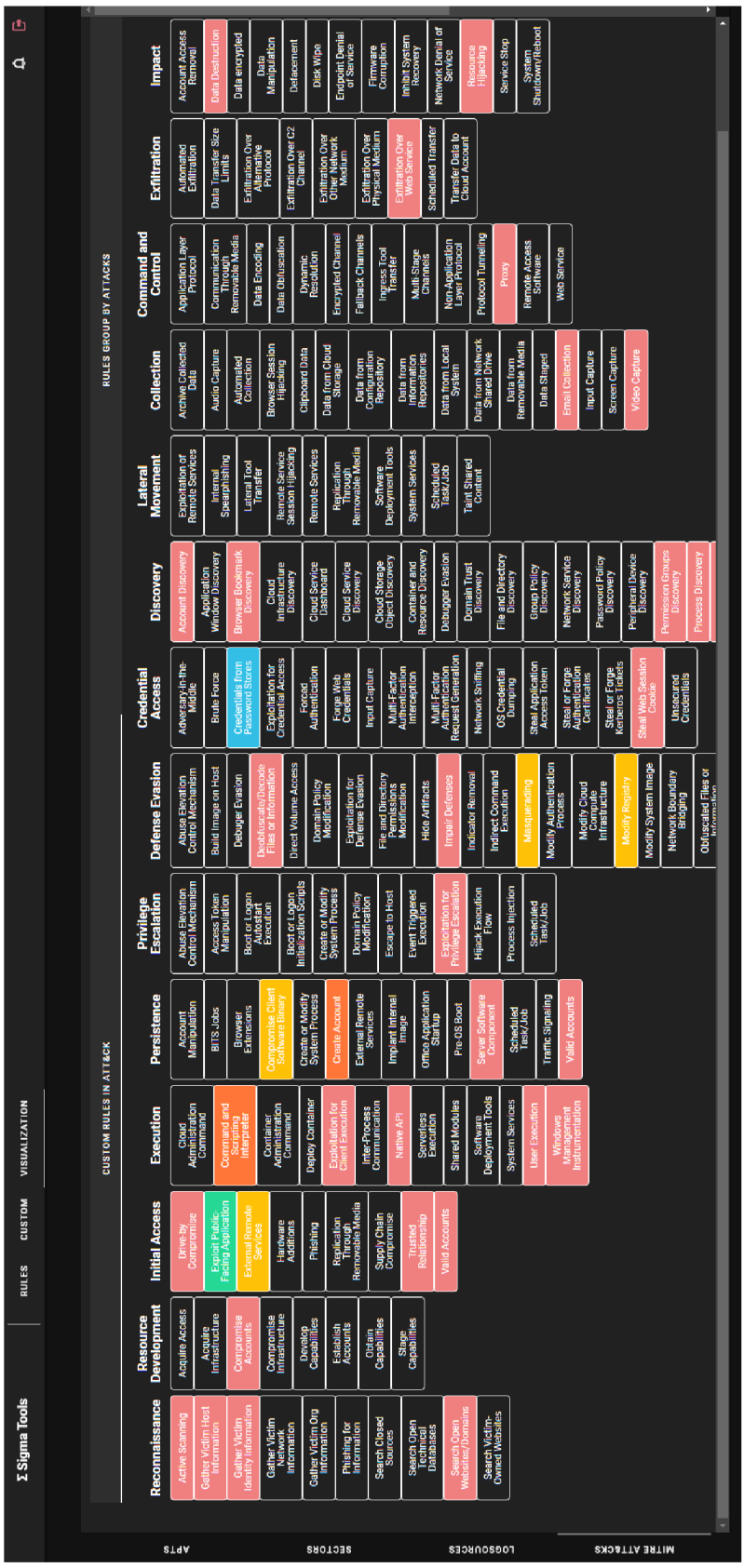
V organizaci se nachází velké množství zařízení s operačním systémem Windows. Na sdílený disk je ukládáno obrovské množství informací a citlivých údajů o pacientech. Poškození těchto dat by mohlo mít nepředstavitelné následky. Správce se rozhodl přejít na záložku „logsources“. Byl spokojený, když uviděl buňku „Windows“ ve sloupci „Operating System“, v zelené barvě (viz obr. 5.5) – ta totiž značí největší procentuální počet pravidel ku všem uživatelským pravidlům. Seznam všech pravidel si zobrazil ve stejném dialogovém okně po kliknutí na buňku jako ukazuje obr. 5.4, kde si potvrdil, že má implementovanou ochranu mj. pro techniku *Create account* také pro zařízení Windows např. pomocí pravidla pro vytvoření nového lokálního účtu „local_user_creation“. Tedy kdyby si chtěla skupina aktérů hrozeb přímo vytvořit nový účet pro znehodnocení dat na disku, bude o aktivitě organizace vědět.

Správce zajímá, jestli už někdy byly prováděny *ransomware* útoky na zdravotnický sektor. Přešel na záložku „sectors“ a v tabulce statistik (viz obr. 5.6) provedených útoků zjistil, že za období 2022–2023 bylo provedeno 13 % kybernetických útoků typu *ransomware* na půdě Evropské unie na zdravotnický sektor, které vychází z vyjádření organizace ENISA. Nejedná se sice o kriticky vysoké číslo, ale pravděpodobnost útoku není nulová. Tabulka sice je dostatečně přehledná, ale pro porovnání s hodnotami např. pro jiné sektory či jiné útoky lépe poslouží vykreslený sloupcový graf v druhé horizontální záložce „attack frequency graph“, zobrazen na obr. 5.7. Při pohledu na legendu grafu zjistí, že sloupec útoku *ransomware* vyplňuje fialová barva, také si všimne změny stínu v ohraničení čtverečku legendy, jakmile přes něj přejede myší. To signalizuje, že čtvereček je tlačítko. Po kliknutí na něj se místo legendy objeví tabulka s názvem vybraného útoku v záhlaví – tedy *ransomware*. Tabulku vykreslenou místo legendy znázorňuje obr. 5.8. Správce vidí v tabulce MITRE seznam technik, které souvisejí s vybraným útokem a pozná, že se jedná o pohled zpracovaný nad stejnými daty jako v případě zobrazení technik útoků v matici *ATT&CK* (viz obr. 5.3). Podobným způsobem jako ukazuje obr. 5.4 si zobrazí seznam pravidel v modálním okně pokrývající konkrétní techniku za předpokladu, že technika obsahuje alespoň jedno uložené pravidlo. Správce si v tomhle pohledu všimne, že graf zůstává kromě počáteční animace růstu sloupců neměnný. Usoudí, že by mohl být také interaktivní a např. po kliknutí na sloupec v grafu určitého útoku nebo na čtvereček legendy by mohly zůstat zobrazeny jen sloupce pro stejný útok, který uživatel vybral.

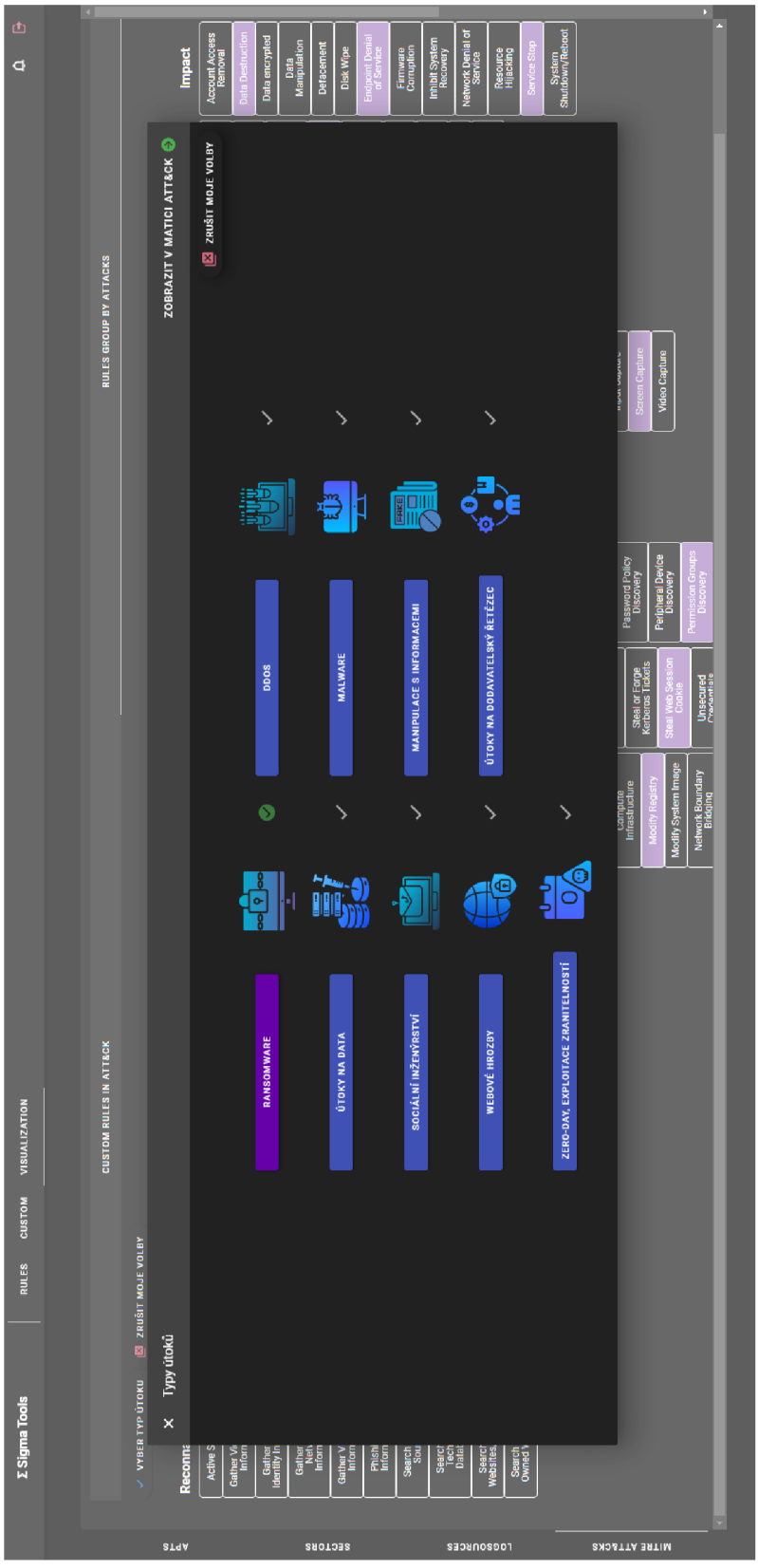
Teď už správce zajímá pouze jediné, dozvědět se nějaké informace o skupině hrozeb APT3, před kterou NÚKIB organizaci varoval. Potřebné informace nalezne v poslední záložce „apts“. V tabulce záznam pro skupinu APT3 jednoduše vyhledá pomocí hledacího okna (viz obr. 5.9) nebo manuálním procházením záznamů v tabulce. Z popisu skupiny se dozvídá, že primárním cílem jsou momentálně politické

organizace v Hongkongu, to však neznamená výhradním a jediným cílem. Správce se rozhodl porovnat techniky používané skupinou APT3 a techniky používané v rámci *ransomware* útoku, aby zjistil, zda se alespoň některé z nich shodují. Všiml si ikony stromové struktury ve sloupci „vizualizace“ a zobrazil si celý horizontální strom taktik a technik, které používá útočící skupina (viz obr. 5.10). Uznal, že takové zobrazení mapování většího počtu dat není příliš čitelné, a proto ocenil tlačítko pro sbalení celého stromu a následně rozbaloval jednotlivé uzly taktik, aby mohl porovnat techniky skupiny s technikami útoku. Zjistil, že se skutečně některé techniky shodují a že varování od NÚKIB nesmí brát na lehkou váhu. Rozhodl se pokrýt techniky pravidly, které se shodují. Ve stromě jednoduše zjistil, které techniky jsou pravidly pokryté, resp. které obsahují alespoň jedno pravidlo, protože takové uzly byly zabarveny zelenou barvou, kdežto ostatní techniky šedou. Při najetí myší na zelené listy se kurzor změnil na ukazatel a po kliknutí se podobně jako v předchozích případech objevilo dialogové okno se seznamem pravidel.

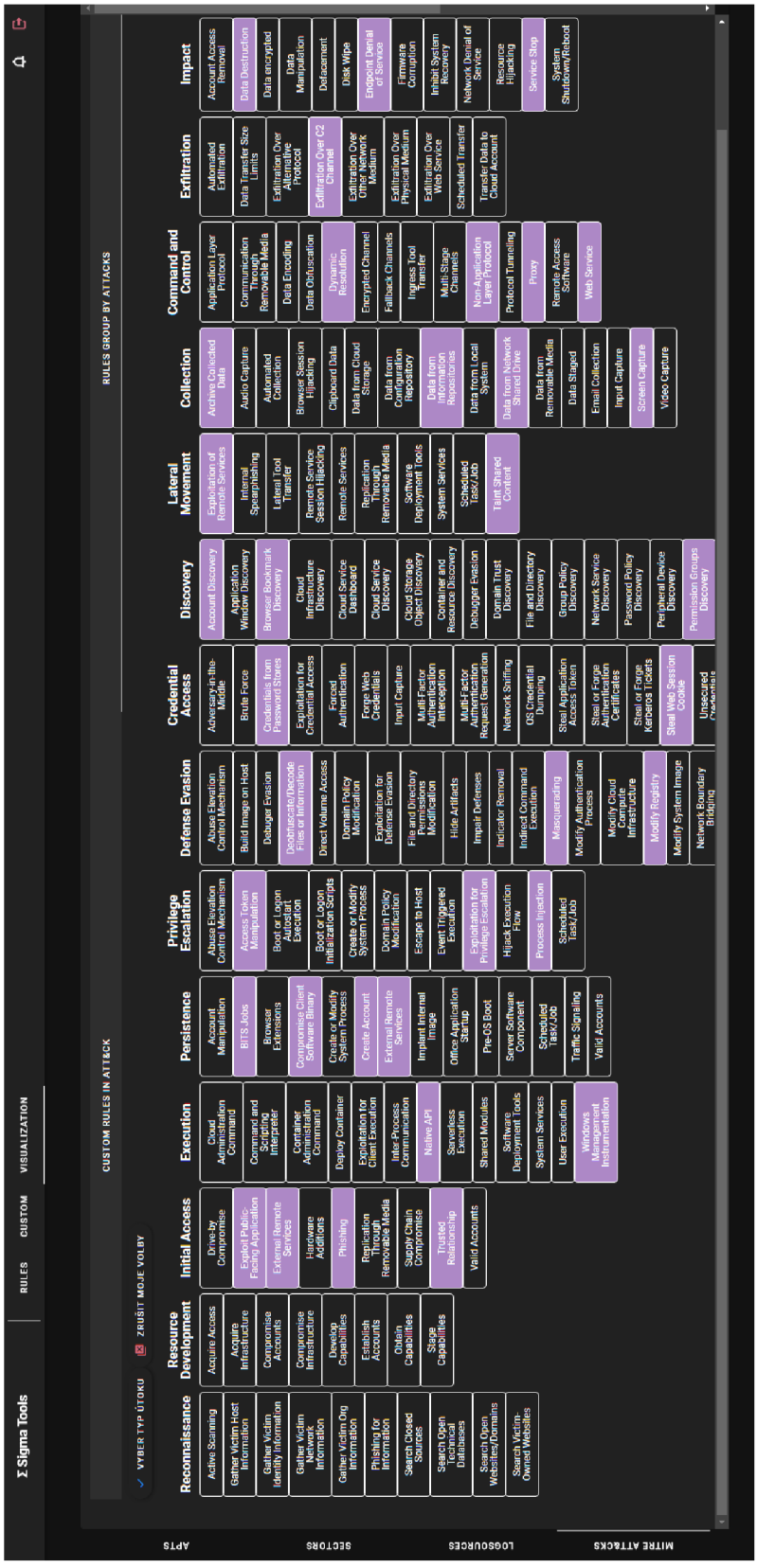
Která pravidla má organizace implementována, správce viděl v několika různých pohledech. Ale aby byl schopen pokrýt pravidly techniky MITRE, které si z předchozích zobrazení vybral, potřeboval by umožnit vyhledávání v seznamu všech dostupných Sigma pravidel. Seznam veškerých pravidel sice v aplikaci přítomný je, ale chybí nad ním implementace vyhledávání nejen podle názvu pravidla, ale také podle klíčových slov v samotné definici pravidla.



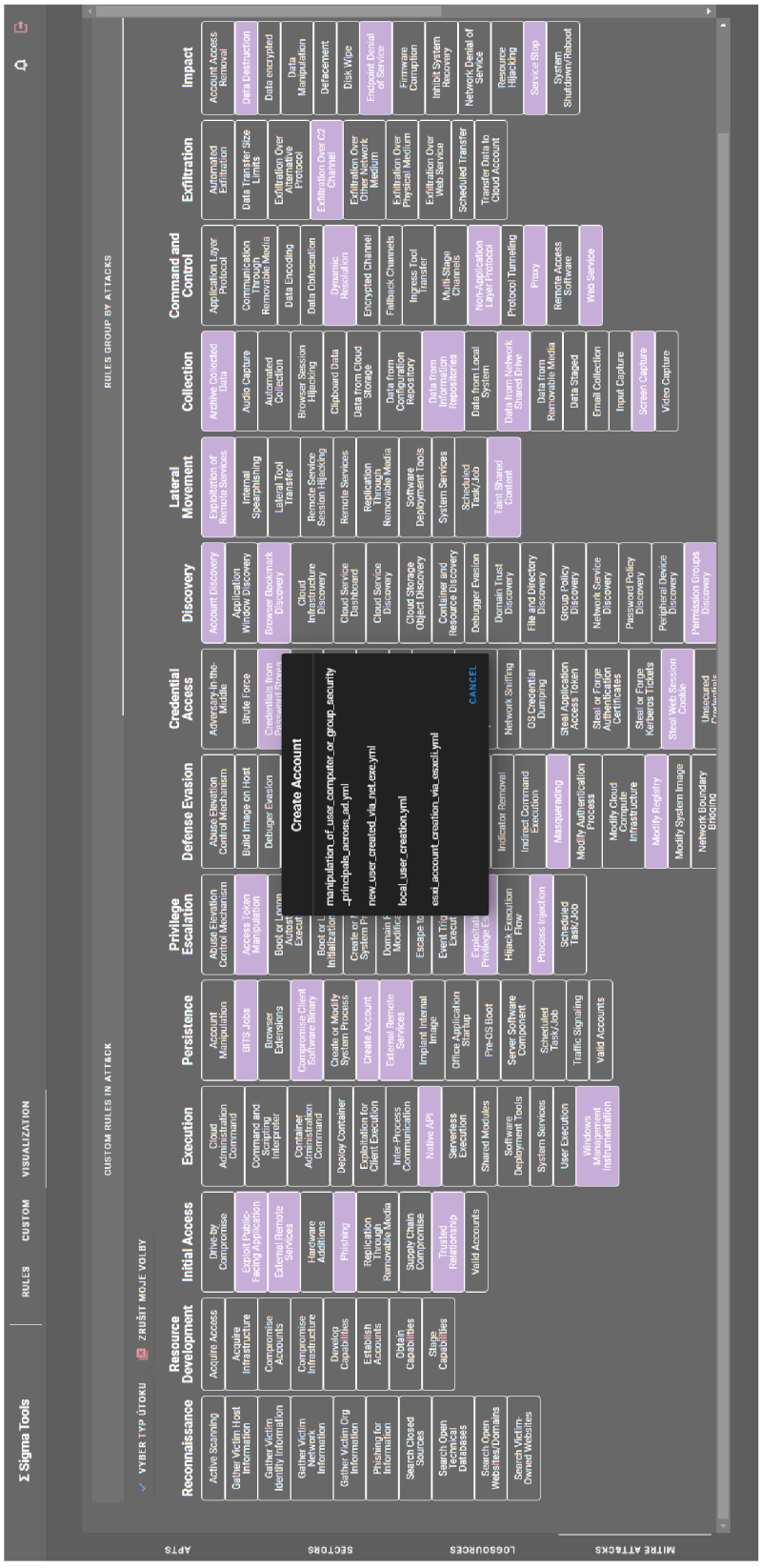
Obr. 5.1: Základní zobrazení pravidel v matici *ATT&CK*.



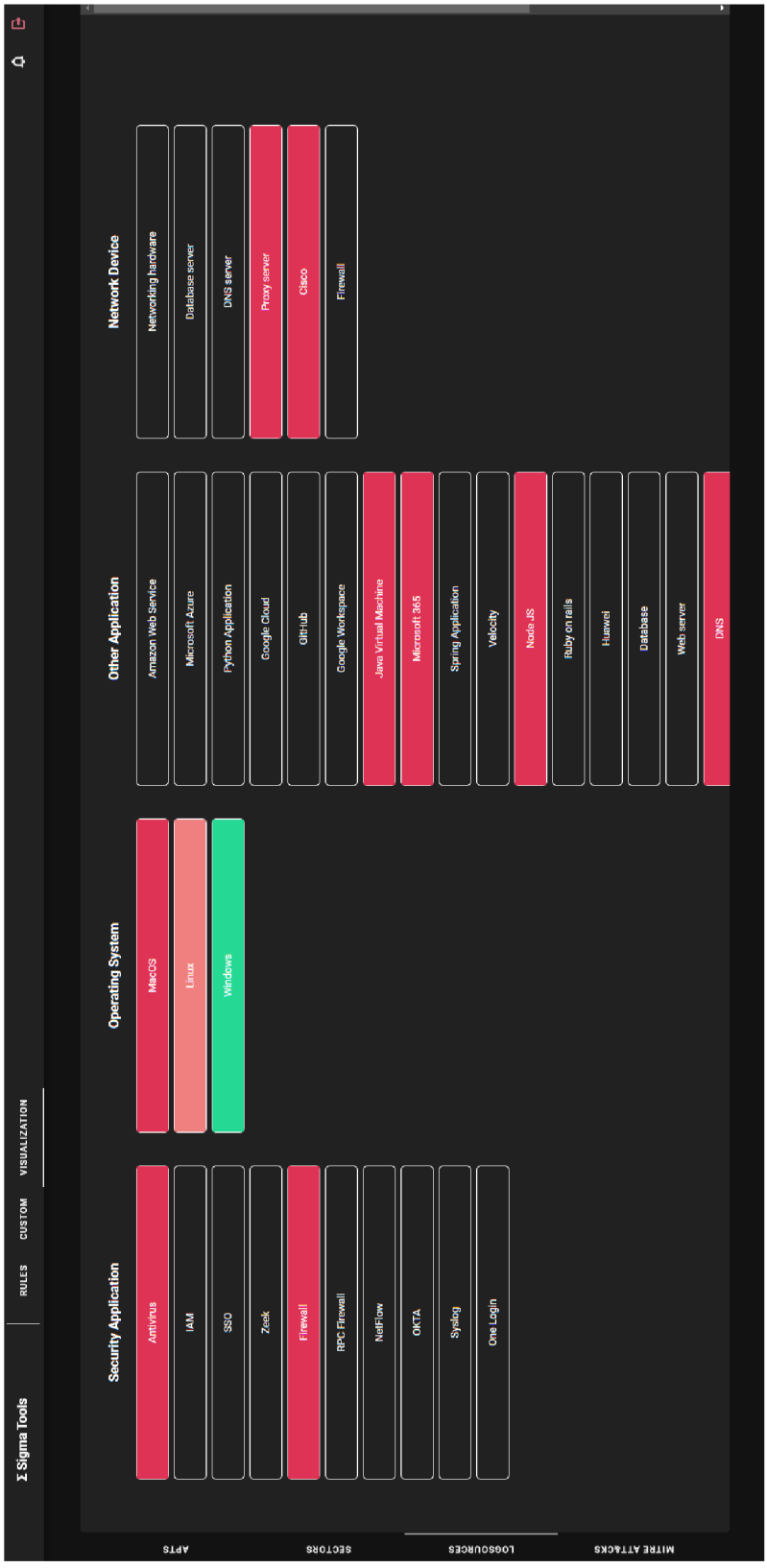
Obr. 5.2: Dialogové okno pro výběr útoku.



Obr. 5.3: Zvýrazněné techniky využívané v útoku *ransomware*.



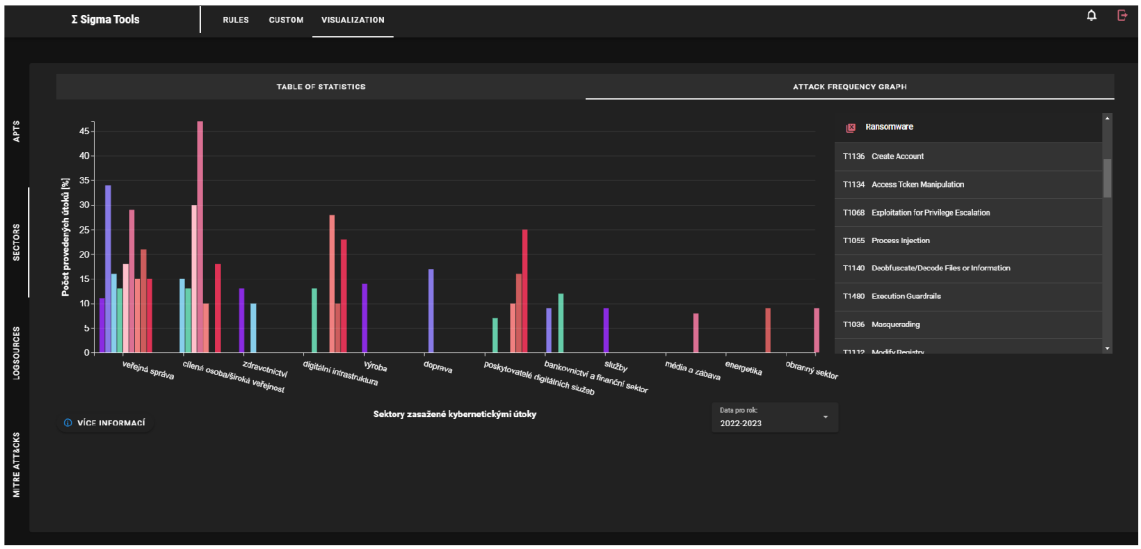
Obr. 5.4: Seznam pravidel pro techniku *Create account*.



Obr. 5.5: Zobrazení pravidel v matici zdrojů logů.

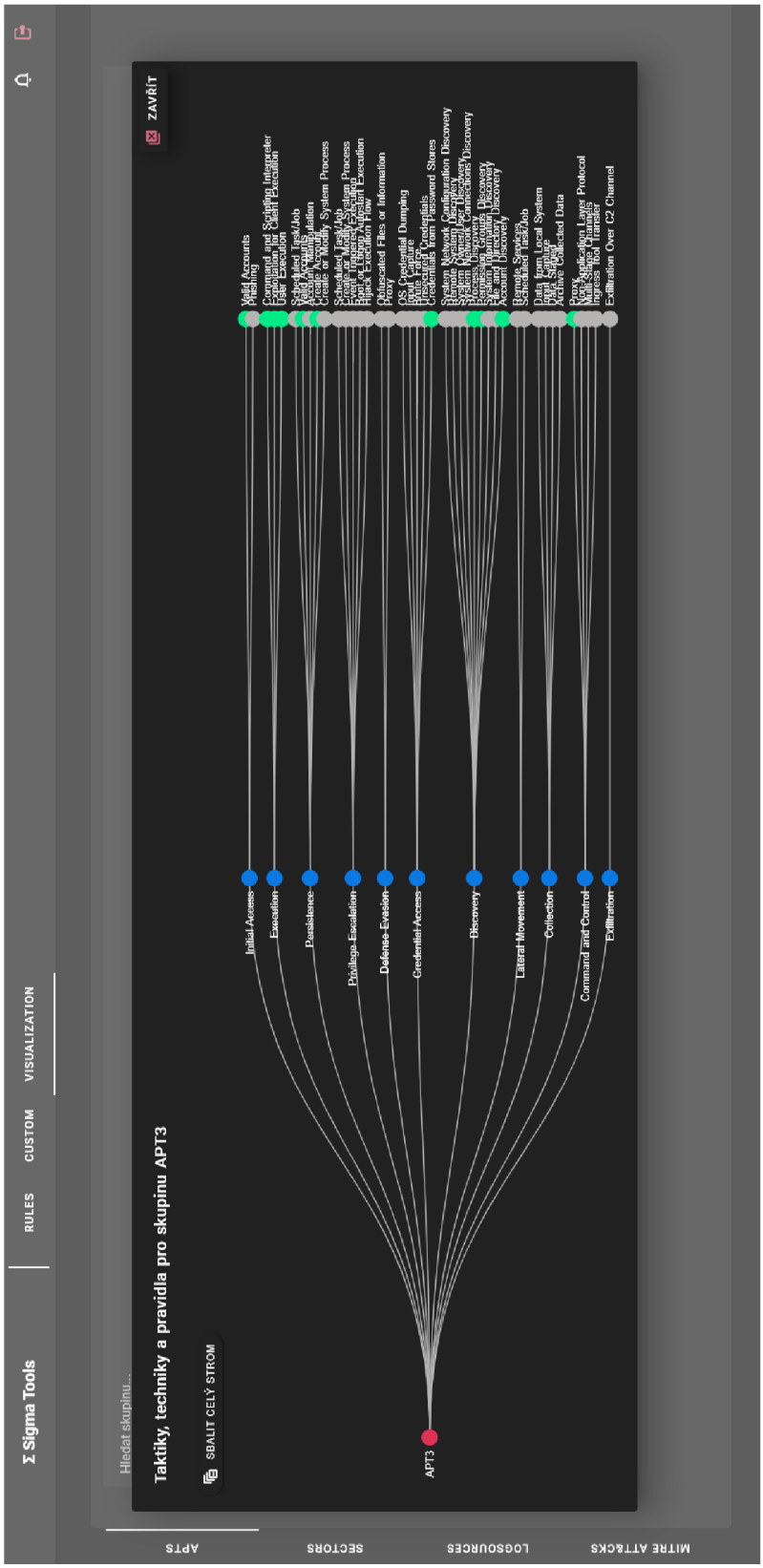
Obr. 5.6: Zobrazení statistik kybernetických útoků za období 2022–2023 v tabulce.

Obr. 5.7: Zobrazení statistik kybernetických útoků za období 2022–2023 v grafu.



Obr. 5.8: Tabulka MITRE technik pro vybraný útok z legendy grafu.

Obr. 5.9: Tabulka informací o nositelích hrozeb.



Obr. 5.10: Stromová struktura mapování taktik, technik a pravidel skupiny APT3.

Závěr

V rámci bakalářské práce byl vytvořený vizualizační nástroj ve formě rozšíření webové aplikace pro vizualizaci Sigma pravidel pomocí nových pohledů.

V teoretické části byla nastudovaná problematika základů kybernetické bezpečnosti (viz kapitola 1.1), byly popsány perspektivy pohledů na kybernetické incidenty *Pyramid of Pain*, *Cyber Kill Chain* a MITRE *ATT&CK* (viz kapitola 1.2). Dále byly charakterizovány způsoby detekce a prevence vzniku kybernetických incidentů, technologie používány pro zajištění kybernetické bezpečnosti a platformy pro zjišťování informací o hrozbách (viz kapitola 1.3). Dále byla nastudována problematika systémů SIEM, Sigma pravidel a zdrojů logů (viz kapitola 1.4). Následně byl čtenář uveden do základních principů vyšetřování kybernetických incidentů SOC týmu včetně vysvětlení modelu vyspělosti úrovně bezpečnosti v kyberprostoru a popisu plánu reakce na incidenty (viz kapitola 1.5). V poslední řadě v rámci teoretické části byl čtenář seznámen s právní úpravou kybernetické bezpečnosti vztažené primárně k území České republiky, ale i k celému území Evropské unie se zaměřením na bezpečnostní doporučení organizace ENISA (viz kapitola 1.6).

V rámci praktické části se pak druhá kapitola zaměřovala na provedení analýzy vizualizačních technik a dostupných šablon. Ta zahrnovala seznámení se s frameworkem `Vue`, knihovnou `D3.js`, `Bootstrap pro Vue` a `Vuetify` (viz kapitola 2.1). Součástí analýzy byl také popis a srovnání vizualizačních technik SIEM platforem IBM QRadar a RSA NetWitness, který nese závěr, že QRadar má zobrazení pravidel mnohem více propracované z hlediska možnosti vyhledávání pravidel, zobrazování korelací mezi pravidly graficky a zobrazení pravidel v matici *ATT&CK* (viz kapitola 2.2). V době odevzdání práce byla vydána aktualizovaná verze technologie NetWitness, která nahrnovala významné změny ve vizuální části. Tato verze však nebyla do analýzy a srovnání zahrnuta.

Následující třetí kapitola se zaměřovala na provedení analýzy způsobů zobrazení pravidel (viz kapitola 3). Ze srovnání diagramů knihovny `D3.js` *Sankey* (viz kapitola 3.1) a *Sunburst* (viz kapitola 3.2) plyne závěr, že diagram *Sunburst* není pro zobrazení dat navrženého typu vhodný z důvodu velkého množství opakování názvů kritérií. Na druhou stranu *Sankey* diagram může být pro velké množství dat nepřehledný, tomu se však dá částečně předejít zvýrazněním odkazů mezi uzly při najetí myši. Součástí analýzy byly i další návrhy jako zobrazení zvýraznění MITRE technik na základě uživatelských pravidel nebo zvýraznění technik používaných vybranými útoky ve stejné matici *ATT&CK* (viz kapitola 3.3.1). Dále zobrazení statistik provedených kybernetických útoků na různé sektory v podobě tabulky a grafu za období červen 2022–2023, které vycházejí z reportu organizace ENISA (viz kapitola 3.3.2). Součástí návrhu bylo také zobrazení pravidel na základě zdrojů logů (viz

kapitola 3.3.3), které jsou obsaženy v tagu pravidla. Poslední návrh tvořil zobrazení pravidel na základě výběru skupiny hrozby a zobrazení MITRE taktik, technik a pravidel ve stromové struktuře knihovny `D3.js` (viz kapitola 3.4). Kapitola také obsahuje popis struktury obecného rozložení komponentů v rámci hlavního pohledu (viz kapitola 3.5).

Čtvrtá kapitola praktické části se zaměřovala na samotný způsob implementace grafického zobrazení pohledů v rámci webové aplikace a obsahovala také strukturu rozložení komponentů v rámci pohledů. Bylo zde vysvětleno experimentální pracoviště a přístup ke vzdálené testovací síti, koncovým bodům a databázi (viz kapitola 4.1). Dále zde byly vysvětleny způsoby sběru, zdroje a formáty dat potřebných pro daná zobrazení. Následně byly detailně popsány všechny realizované pohledy včetně druhu použitých komponent a knihoven (viz kapitola 4.2).

Poslední pátá kapitola byla věnována testování aplikace a její vizuální části z pohledu uživatele (viz kapitola 5). Byly popsány veškeré pohledy implementované v aplikaci na základě vymyšleného scénáře, jehož závěr měl být, že správce organizace získá veškeré potřebné informace o tom, která pravidla implementovat z uživatelsky příjemné a interaktivní webové aplikace. Veškerý realizovaný grafický design byl zdokumentovaný v podobě přiložených snímků obrazovky. Z testování vyplynulo několik námětů na zlepšení aplikace do budoucna. V prvním pohledu na zvýraznění MITRE technik v matici *ATT&CK* by bylo vhodné podbarvení technik pro jednotlivé útoky barevně odlišit. Na druhou stranu techniky se mohou mezi útoky opakovat a potom by bylo podbarvování buněk v matici nedostatečné a bylo by zapotřebí realizovat jiné odlišení pro techniky stejných útoků. V pohledu na graf statistik vykonaných kybernetických útoků by mohla být vylepšena interaktivita grafu. Například po vybrání určitého sloupce útoku v grafu nebo konkrétního útoku v legendě grafu by mohly zůstat viditelné pouze sloupce stejného útoku. V rámci vizuální části je tedy uživatel schopen efektivně zhodnotit, která pravidla implementovat a rozšířit tak bezpečnostní strategii organizace. Na druhou stranu v aplikaci není přítomna žádná funkcionalita pro vyhledávání mezi veškerými pravidly například podle názvu MITRE techniky, podle zdroje logů či podle jiných klíčových slov v definicích pravidel. Dalším krokem zlepšení do budoucna je překlad vizuální části do anglického jazyka pro zajištění jednotnosti jazyků v rámci celé aplikace a migrace vizuální části této práce, která byla vyvíjena lokálně, do produkčního prostředí na server v experimentální síti.

Literatura

[1] BRABENCOVÁ, Petra, 2022. Kybernetická bezpečnost. Online. Dostupné z: https://itjede.cz/blog/kyberneticka-bezpecnost. [cit. 2023-10-12].

[2] IBM. What is a threat actor? Online. IBM. Dostupné z: https://www.ibm.com/topics/threat-actor. [cit. 2023-10-12].

[3] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef, 2022. Výkladový slovník Kybernetické bezpečnosti. Online. 5. dopl. vyd. Praha. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2023-10-13].

[4] KIDD, Chrissy, 2022. Incident Severity Levels 1-5 Explained. Online. Dostupné z: https://www.splunk.com/en_us/blog/learn/incident-severity-levels.html. [cit. 2023-10-13].

[5] SAFONOV, Yehor, 2018. APLIKACE PRO GRAFICKOU REPREZENTACI PRŮBĚHU ÚTOKU. Online, Bakalářská práce, vedoucí Ing. Zdeněk Martinásek, Ph.D. Brno: Vysoké učení technické v Brně. Dostupné z: https://dspace.vutbr.cz/bitstream/handle/11012/82141/final-thesis.pdf?sequence=-1&isAllowed=y. [cit. 2023-10-13].

[6] MALWAREBYTES. What is malware? Online. Dostupné z: https://www.malwarebytes.com/malware. [cit. 2023-10-15].

[7] BURDA, Karel, 2013. Bezpečnost informačních systémů. Online. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. ISBN 978-80-214-4890-2. Dostupné z: https://www.vut.cz/studenti/predmety/detail/98543?armsgt=in6OqD9Kjv. [cit. 2023-10-28].

[8] BEZPALEC, Pavel. Utoky na site. Online. CESKE VYSOKE UCENI TECHNICKE V PRAZE. Dostupné z: https://publi.cz/books/223/02.html. [cit. 2023-11-27].

[9] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2023. Kybernetické incidenty pohledem NÚKIB - leden 2023. Online. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1934-kyberneticke-incidenty-pohledem-nukib-leden-2023/. [cit. 2023-11-12].

[10] MICROSOFT, 2023. MITM – Hrozba veřejných sítí: Kyberbezpečnost #2. Online. Dostupné z: https://studuj.digital/2023/09/28/mitm-hrozba-verejnych-siti-kyberbezpecnost-2/. [cit. 2023-11-12].

[11] MCAFEE, 2023. Co je malware? Online. Dostupné z: https://www.mcafee.com/cs-cz/antivirus/malware.html. [cit. 2023-11-12].

[12] DRAKE, Veronica, 2022. The Pyramid of Pain and Cyber Threat Intelligence. Online. Dostupné z: https://flashpoint.io/blog/the-pyramid-of-pain-and-cyber-threat-intelligence/. [cit. 2023-10-25].

[13] LABS, Picus, 2023. What Is Pyramid of Pain? Online. PICUS SECURITY. Dostupné z: https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain. [cit. 2023-10-28].

[14] ČERMÁK, Martin, 2018. Ukazatelé kompromisu. Online, Bakalářská práce, vedoucí doc. Ing. Jaroslav Dočkal, CSc. Vysoká škola Karla Engliše, a.s. Dostupné z: https://is.vske.cz/th/quxub/bakaprace6_Cermak.pdf.[cit. 2023-10-29].

[15] JAVOREK, Honza, 2020. Co je API? Online. Dostupné z: https://cojeapi.cz/. [cit. 2023-10-29].

[16] NUKIB, 2023. Kybernetické incidenty pohledem NÚKIB. Online. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/. [cit. 2023-11-09].

[17] CROWDSTRIKE, 2022. WHAT IS THE CYBER KILL CHAIN? PROCESS & MODEL. Online. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/. [cit. 2023-10-29].

[18] SENTINELONE, 2023. What Is The Cyber Kill Chain? Steps, Examples, & How To Use It. Online. Dostupné z: https://www.sentinelone.com/cybersecurity-101/cyber-kill-chain/. [cit. 2023-10-29].

[19] FRANCESCO, 2022. Co je to Dark Web, jak se na něj dostat a kam se na něm vydat? Online. CDR. Dostupné z: https://cdr.cz/clanek/co-je-dark-web-jak-se-na-nej-dostat-kam-se-na-nem-vydat. [cit. 2023-10-30].

[20] LOCKHEED MARTIN, 2023. Cyber Kill Chain. Online.[cit. 2023-10-27]. Dostupné z: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[21] SOLDIERS, Winter, 2023. Understanding Cyber Kill Chain, MITRE ATT&CK Framework and Unified Kill Chain. Online. Dostupné z: https://medium.com/@wintersoldiers/understanding-cyber-kill-chain-mitre-att-ck-framework-and-unified-kill-chain-f306ceca19be. [cit. 2023-11-12].

[22] LIU, Timothy. Taking Security Strategy to the Next Level: The Cyber Kill Chain vs. MITRE ATT&CK. Online. ISACA. Dostupné z: https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-security-strategy-to-the-next-level. [cit. 2023-11-24].

[23] STROM, Blake E., Andy APPLEBAUM, Doug P. MILLER, Kathryn C. NICKELS, Adam G. PENNINGTON a Cody B. THOMAS, 2018. MITRE. MITRE ATT&CK®: Design and Philosophy. Online. Dostupné z: https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf. [cit. 2023-11-13].

[24] TRELLIX, 2023. What Is the MITRE ATT&CK Framework? Online. Dostupné z: https://www.trellix.com/security-awareness/cybersecurity/what-is-mitre-attack-framework/. [cit. 2023-11-12].

[25] MITRE, 2023. ATT&CK®. Online. Dostupné z: https://attack.mitre.org/. [cit. 2023-11-13].

[26] Detekce pokročilých útoků v událostech Flowmon ADS, 2021. Online, Bakalářská práce, vedoucí doc. Ing. Pavel Čeleda, Ph.D. Brno: Masarykova univerzita. Dostupné z: https://is.muni.cz/th/y5jww/BP_Adamec.pdf. [cit. 2023-11-13].

[27] MATUŠICOVÁ, Viktória, 2021. Webová aplikace pro zobrazení kybernetických útoků v lokálních sítích. Online, Bakalářská práce, vedoucí Ing. Yehor Safonov. Brno: Vysoké učení technické v Brně. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=227579. [cit. 2023-11-24].

[28] BARRACUDA. Intrusion Detection System. Online. BARRACUDA. Dostupné z: https://www.barracuda.com/support/glossary/intrusion-detection-system. [cit. 2023-11-24].

[29] VMWARE. What is an intrusion prevention system? Online. VMWARE. Dostupné z: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html. [cit. 2023-11-24].

[30] LEDESMA, Josue, 2022. IDS vs. IPS: What Organizations Need to Know. Online. VARONIS. Dostupné z: https://www.varonis.com/blog/ids-vs-ips#similarities-and-differences. [cit. 2023-12-05].

[31] PALO ALTO NETWORKS. What Is Network Detection and Response (NDR)? Online. PALO ALTO NETWORKS. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-network-detection-and-response. [cit. 2023-12-05].

[32] RISK ANALYSIS CONSULTANTS. Digitální forenzní analýza. Online. RISK ANALYSIS CONSULTANTS. Dostupné z: https://www.rac.cz/cs/digitalni-forenzni-institut/digitalni-forenzni-analyza/. [cit. 2023-12-05].

[33] SYSDIG. EDR vs. XDR vs. SIEM vs. MDR vs. SOAR. Online. SYSDIG. Dostupné z: https://sysdig.com/learn-cloud-native/detection-and-response/edr-vs-xdr-siem-vs-mdr-vs-sor/. [cit. 2023-12-05].

[34] ASHTARI, Hossein, 2022. Intrusion Detection System vs. Intrusion Prevention System: Key Differences and Similarities. Online. SPICE WORKS. Dostupné z: https://www.spiceworks.com/it-security/network-security/articles/ids-vs-ips/. [cit. 2023-12-04].

[35] ANOMALI. What is a Threat Intelligence Platform (TIP)? Online. Dostupné z: https://www.anomali.com/resources/what-is-a-tip. [cit. 2024-01-17].

[36] LEANIX. THE DIFFERENCE BETWEEN SaaS vs. On-Premise. Online. Dostupné z: https://www.leanix.net/en/wiki/saas/saas-vs-on-premise#SaaS-vs-on-premise-comparison. [cit. 2024-01-18].

[37] CYBER THREAT INTELLIGENCE PLATFORMS (TIPs) [@DR. DEEPAK (D3) FORENSICS], 2018. Online. 2018. Dostupné z: Linkedin, https://www.linkedin.com/pulse/cyber-threat-intelligence-platforms-tips-forensics-. [cit. 2024-01-18].

[38] SOCRADAR, 2023. Top 10 Best Free Cyber Threat Intelligence Sources and Tools in 2023. Online. Dostupné z: https://socradar.io/top-10-best-free-cyber-threat-intelligence-sources-and-tools-in-2023/. [cit. 2024-01-18].

[39] GONZÁLEZ-GRANADILLO, Gustavo; GONZÁLEZ-ZARZOSA, Susana a DIAZ, Rodrigo, 2021. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Online. Dostupné z: https://doi.org/10.3390/s21144759. [cit. 2023-11-26].

[40] DIGITÁLNÍ PEVNOST. SIEM. Online. Dostupné z: https://www.digitalnipevnost.cz/viki/siem. [cit. 2023-11-26].

[41] IBM. What is attack surface management? Online. IBM. Dostupné z: https://www.ibm.com/topics/attack-surface-management. [cit. 2023-12-07].

[42] DE LA LOZ, Gonzalo, 2023. Opportunity identification & security tools avaible to our partners. Online. Dostupné z: https://konferencesecurity.cz/. [cit. 2023-12-07].

[43] ČERMÁK, Miroslav. SIEM: Auditing a monitoring. Online. Dostupné z: https://www.cleverandsmart.cz/siem-auditing-a-monitoring/. [cit. 2023-12-07].

[44] VC3. What Is Security Information and Event Management (SIEM), and Why Is It Important to Your Business? Online. VC3. Dostupné z: https://www.vc3.com/blog/what-is-siem. [cit. 2023-12-07].

[45] LABS, Picus, 2023. What Are Sigma Rules? Online. Dostupné z: https://www.picussecurity.com/resource/glossary/what-is-sigma-rule. [cit. 2023-11-26].

[46] SOLARWINDS. What Is Log Management? Online. SOLARWINDS. Dostupné z: https://www.solarwinds.com/resources/it-glossary/log-management. [cit. 2023-12-05].

[47] Top 10 Log Sources You Should Monitor [@ksparenberg], 2018. Online. 2018. Dostupné z: DNSstuff, https://www.dnsstuff.com/top-10-log-sources-you-should-monitor. [cit. 2024-01-22].

[48] SHARIF, Arfan, 2023. SIEM VS LOG MANAGEMENT. Online. 2023. Dostupné z: Crowdstrike, https://www.crowdstrike.com/cybersecurity-101/observability/siem-vs-log-management/. [cit. 2024-01-23].

[49] SIGMAHQ. Logsources. Online. 13.1.2024. Dostupné z: https://sigmahq.io/docs/basics/log-sources.html#logsource-basics. [cit. 2024-01-23].

[50] MATUŠICOVÁ, Viktória, 2023. Webová aplikace pro generalizaci SIEM korelačních pravidel. Online, Diplomová práce, vedoucí Ing. Yehor Safonov. Brno: Vysoké učení technické v Brně. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=254275. [cit. 2023-12-07].

[51] ARICOMA. Komplexní bezpečnostní dohled (SOC). Online. Dostupné z: https://www.aricoma.com/cs/co-delame/kyberneticka-bezpecnost/bezpecnostni-dohled-formou-sluzby/soc. [cit. 2023-11-26].

[52] TIMONERA, Kaye. Red Team vs Blue Team vs Purple Team: Differences Explained. Online. Dostupné z: https://www.esecurityplanet.com/networks/red-team-vs-blue-team-vs-purple-team/. [cit. 2023-11-26].

[53] VAZQUEZ, Iratxe. Security Operations Maturity Model II : What is it? Online. Dostupné z: https://www.watchguard.com/wgrd-news/blog/security-operations-maturity-model-ii-what-it. [cit. 2023-11-26].

[54] CRANFORD, JJ. INCIDENT RESPONSE (IR): PLAN & PROCESS. Online. CROWDSTRIKE. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/incident-response/. [cit. 2023-11-26].

[55] ELLIS, DAVID. 6 Phases in the Incident Response Plan. Online. SECURITY METRICS. Dostupné z: https://www.securitymetrics.com/blog/6-phases-incident-response-plan. [cit. 2023-11-26].

[56] STUPKA, Václav, 2018. Kybernetická bezpečnost v České republice. Online, Disertační práce. Brno: Masarykova univerzita, Právnická fakulta, Ústav práva a technologií. Dostupné také z: https://is.muni.cz/th/d5zot/DP_final.pdf.

[57] ERBEN, Lukáš, 2014. Příchod hackerů: zrod CERT a CSIRT. Online. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-zrod-cert-a-csirt/. [cit. 2024-01-27].

[58] NÚKIB. Strategie / Akční plán. Online. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/. [cit. 2024-01-27].

[59] NÚKIB. NÁVRH NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A DALŠÍCH PŘEDPISŮ. Online. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145. [cit. 2024-01-27].

[60] CYBERSECURITY, 2017. Kybernetická bezpečnost (Cyber Security). Online. Dostupné z: https://www.cybersecurity.cz/basic.html. [cit. 2024-01-27].

[61] NÚKIB. Legislativa KB. Online. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/. [cit. 2024-01-27].

[62] BEZPEČNOST PRÁCE, 2021. KYBERNETICKÁ A INFORMAČNÍ BEZPEČNOST. LEGISLATIVA, POVINNOSTI A TYPY KYBERNETICKÝCH ÚTOKŮ. Online. Dostupné z: https://www.bezpecnostprace.info/kybernetika-informace/kyberneticka-bezpecnost-legislativa-povinnost/#tab3. [cit. 2024-01-27].

[63] UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ. Směrnice NIS. Online. Dostupné z: https://www.utb.cz/cybersecurity/nis/. [cit. 2024-02-02].

[64] Co je NIS2? (a další často kladené otázky), 2023. Online. 2023. Dostupné z: Bidefender, https://www.bitdefender.cz/post/co-je-nis2-a-dalsi-casto-kladene-otazky. [cit. 2024-02-07].

[65] SMĚRNICE: SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 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), 2022. Online. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=CS.

[66] SLUŽBY UVEDENÉ V PŘÍLOZE I. Online. In: NÚKIB. Dostupné z: https://osveta.nukib.cz/pluginfile.php/58365/mod_page/content/316/Priloha-1_Graficke-znazorneni-bez-nazvu_logo_v1.0.pdf. [cit. 2024-02-07].

[67] ENISA, c2005-2024. Online. Dostupné z: https://www.enisa.europa.eu/. [cit. 2024-05-21].

[68] D3 IN DEPTH. Introduction to D3.js. Online. D3 IN DEPTH. Dostupné z: https://www.d3indepth.com/introduction/. [cit. 2023-12-08].

[69] AZAM, Shehroz, 2020. How to Use Bootstrap with Vue.js. Online. LINUXHINT. Dostupné z: https://linuxhint.com/install-use-bootstrap-with-vue-js/. [cit. 2023-12-08].

[70] VUETIFY. Introduction. Online. VUETIFY. Dostupné z: https://vuetifyjs.com/en/introduction/why-vuetify/. [cit. 2023-12-08].

[71] IBM, c2012–2022. IBM Documentation. Online. Dostupné z: https://www.ibm.com/docs/en/qsip/7.5. [cit. 2023-11-27].

[72] NETWITNESS. SIEM – Security Information and Event Management. Online. NETWITNESS. Dostupné z: https://www.netwitness.com/solutions/evolved-siem/. [cit. 2023-12-05].

[73] HERODEVS. Introduction. Online. HERODEVS. Dostupné z: https://vuejs.org/guide/introduction.html. [cit. 2023-12-07].

[74] GOOGLE CHARTS. Sankey Diagram. Online. GOOGLE CHARTS. Dostupné z: https://developers.google.com/chart/interactive/docs/gallery/sankey. [cit. 2023-12-09].

[75] ZEBRA BI, 2023. How to Customize Sunburst Chart in D3.js. Online. ZEBRA BI. Dostupné z: https://zebrabi.com/guide/how-to-customize-sunburst-chart-in-d3-js/#Introduction_to_D3js_Sunburst_Chart. [cit. 2023-12-09].

Seznam symbolů a zkratek

API *Application Programming Interface* – Knihovna funkcí, protokolů a nástrojů pro programování aplikací

AQL *Ariel Query Language* – Dotazovací jazyk Ariel

ARP *Address Resolution Protocol* – Protokol pro rozlišení adres

ASM *Attack Surface Management* – Správa plochy vektorů útoku

ATT&CK *Adversarial Tactics, Techniques and Common Knowledge* – Protivníkovy taktiky, techniky a obecné znalosti

CERT *Central Emergency Response Team* – Týmy reagující na bezpečnostní incidenty

CESNET *Czech Education and Scientific NETwork* – Výzkumná a vzdělávací síť České republiky

CIA *Confidentiality, Integrity, Availability* – triáda pro zajištění důvěrnosti, integrity a dostupnosti

CSIRT *Computer Security Incident Response Team* – Týmy specializované na řešení bezpečnostních incidentů

CSS *Cascading Style Sheets* – Kaskádové styly

CSV *Comma-separated values* – Hodnoty oddělené čárkou

ČR Česká republika

D3 *Data-Driven Documents* – Dokumenty řízené daty

DDNS *Dynamic Domain Name System* – Dynamický systém doménových jmen

DDOS *Distributed Denial of Service* – Distribuovaný útok na odepření služby

DGA *Domain-Generated Algorithms* – Algoritmy pro generování domén

DNS *Domain Name System* – Systém doménových jmen

DOM *Document Object Model* – Objektový model dokumentu

DOS *Denial of Service* – Útok na odepření služby

EDR *Endpoint Detection Response* – Reakce na detekce v koncových zařízeních

EECC *European Electronic Communications Code* – Evropský kodex elektronických komunikací

ENISA *European Union Agency for Cybersecurity* – Agentura Evropské unie pro kybernetickou bezpečnost

EPL *Esper Processing Language* – Jazyk pro zpracování Esper

ESA *Event Stream Analysis* – Analýza toku událostí

HIDS *Host intrusion detection systems* – Systém detekce průniku na koncovém zařízení

HIPS *Host-based intrusion prevention system* – Systém prevence průniku na koncovém zařízení

HTML *Hypertext Markup Language* – Značkovací jazyk

HTTP *Hypertext Transfer Protocol* – Hypertextový přenosový protokol

IBM *International Business Machines Corporation* – Mezinárodní obchodní společnost

IDS *Intrusion Detection System* – Systém detekce průniku

IOC *Indicator of Compromise* – Indikátor kompromisu

IP *Internet Protocol* – Internetový protokol

IPS *Intrusion Prevention System* – Systém prevence narušení

IRP *Incident Response Plan* – Plán reakce na incidenty

ISAC *Information Sharing and Analysis Centers* – Střediska pro sdílení a analýzu informací

IT *Intormation Technology* – Informační technologie

JSON *JavaScript Object Notation* – Zápis objektů v jazyce JavaScript

MD5 *Message-Digest Algoritm* – Algoritmus digitalizace zpráv

NDR *Network Detection Response* – Reakce na detekce v síti

NIDS *Network intrusion detection systems* – Síťový systém detekce průniku

NIPS *Network-based intrusion prevention system* – Síťový systém prevence průniku

NIS *Network Information Security* – Evropská směrnice pro kybernetickou bezpečnost

OSINT *Open Source Intelligence* – Zpravodajství z otevřených zdrojů

PDF *Portable Document Format* – Formát přenosného dokumentu

PIDS *Protocol-based intrusion detection systems* – Systém detekce průniku na základě protokolu

SEM *Security Event Management* – Systém pro správu bezpečnostních událostí

SHA *Secure Hash Algoritm* – Bezpečný algoritmus heš

SIEM *Security Information and Event Management* – Systém pro správu bezpečnostních informací a událostí

SIM *Security Information Management* – Systém pro správu bezpečnostních informací

SOAR *Security Orchestration, Automation, and Response* – Bezpečnostní orchestrace, automatizace a reakce

SOC *Security Operation Center* – Bezpečnostní operační cetrum

SSH *Secure Shell* – Zabezpečené prostředí Shell

STIX *Structured Threat Information eXpression* – Strukturované vyjádření informací o hrozbách

SVG *Scalable Vector Graphics* – Škálovatelná vektorová grafika

SaaS *Software as a Service* – Softvér poskytovaný jako služba

TAXII *Trusted Automated exchange of Intelligence Information* – Důvěryhodná automatizovaná výměna zpravodajských informací

TIP *Threat Intelligence Platform* – Platforma pro získávání informací o hrozbách

TSV *Tab-separated values* – Hodnoty oddělené tabulátorem

TTP *Tactics Techniques and Procedures* – Taktiky, techniky a procedury

UEBA *User and entity behavior analytics* – Analýza chování uživatelů a subjektů

URL *Uniform Resource Locator* – Unifikovaný lokátor zdrojů

VML *Vector Markup Language* – Vektorový značkovací jazyk

VoKB Vyhláška o kybernetické bezpečnosti České republiky

VPN *Virtual Private Network* – Virtuální soukromá síť

WIPS *Wireless intrusion prevention system* – Systém prevence průniku v bezdrátové síti

XDR *Extended Detection and Response* – Rozšířená detekce a reakce

XML *Extensible Markup Language* – Rozšiřitelný značkovací jazyk

YAML *YAML Ain't Markup Language* – YAML není značkovací jazyk

ZoKB Zákon o kybernetické bezpečnosti České republiky

A Návod na spuštění webové stránky

Vzhledem k tomu, že byla vyvíjena pouze vizuální nikoliv funkční část aplikace, je pro správné fungovaní webu nutný přístup k backendové části. Ta se ve formě Docker kontejneru nachází na serveru v experimentální síti. Pro přístup do sítě je nutné použití VPN tunelu. V případě potřeby získání přístupových údajů do tunelu VPN je možné se obrátit na pana Ing. Yehora Safonova. Dále je možné extrahovat a zobrazit obsah komprimované elektronické přílohy a otevřít jej ve vývojovém prostředí např. *Visual Studio Code*.

Po získání přístupu do VPN a přihlašovacích údajů k aplikaci je nutné doinstalovat potřebné balíčky a knihovny. Pro nainstalování knihovny `D3.js` je nezbytné použití příkazu v terminálu:

```
npm install d3
```

Dále je nutné doinstalovat `Vue CLI` a přidat knihovnu `Vuetify` pomocí příkazu:

```
npm install -g @vue/cli
vue add vuetify
```

A doinstalovat všechny zbylé závislosti, zda je to nutné pomocí příkazu:

```
npm install
```

Jakmile jsou nainstalované potřebné balíčky a je zajištěn přístup do sítě VPN, lze aplikaci spustit příkazem:

```
npm run dev
```

A v libovolném webovém prohlížeči zadat adresu lokálního projektu, která se zobrazí v terminálu, může mít následující tvar:

```
http://localhost:3000/
```

Po správném načtení stránky se uživateli zobrazí přihlašovací formulář do aplikace.

B Obsah elektronické přílohy

Součástí bakalářské práce je elektronická příloha obsahující zdrojový kód vizuální části aplikace. Struktura přílohy je následující:

- `/` ... kořenový adresář přílohy
  - `assets` ... obrázky v aplikaci
  - `components` ... komponenty uživatelské části aplikace
    - `apt`
      - `AptViz.vue` ... zobrazení dle APT skupin
    - `matrix` ... komponenty pro dle zobrazení MITRE a zdrojů logů
      - `LogsourceComponent.vue` ... matice zdrojů logů
      - `CombinationMitreComponent.vue` ... navigace v pohledu MITRE
      - `Attacks.vue` ... techniky útoků v matici
      - `MitreComponent.vue` ... matice ATT&CK
      - `DialogMenu.vue` ... dialogové okno
    - `sectors` ... komponenty pro zobrazení dle sektorů
      - `data2022` ... data pro pohled dle sektorů
        - `dle_sektoru2022.json` ... data pro kombinaci do tabulek
        - `graf2022.json` ... data pro graf
        - `utoky2022.json` ... data pro tabulku statistik
      - `data2023` ... pro toto období nejsou data zatím k dispozici
      - `data2024` ... pro toto období nejsou data zatím k dispozici
      - `Graph.vue` ... graf statistik
      - `Table.vue` ... tabulky statistik
      - `GrafViz.vue` ... navigace v pohledu dle sektorů
  - `router` ... router soubory
    - `index.ts` ... směrování na pohledy
  - `services` ... pomocné funkce kontrolerů
    - `MatrixService.ts` ... funkce pro http požadavky
  - `views` ... pohledy
    - `MatrixView.vue` ... pohled na záložku vizualizace