UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA
PRÍRODOVEDECKÁ FAKULTA

MANAŽMENT BEZPEČNOSTNÝCH INFORMÁCIÍ A UDALOSTÍ PRE AKADEMICKÝ INFORMAČNÝ SYSTÉM

2021 **Bc. Eva MARKOVÁ**

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA
PRÍRODOVEDECKÁ FAKULTA

MANAŽMENT BEZPEČNOSTNÝCH INFORMÁCIÍ A UDALOSTÍ PRE AKADEMICKÝ INFORMAČNÝ SYSTÉM

DIPLOMOVÁ PRÁCA

Študijný program:	Informatika
Pracovisko (katedra/ústav):	Ústav informatiky
Vedúci diplomovej práce:	RNDr. JUDr. Pavol Sokol, PhD.

Košice 2021

Bc. Eva MARKOVÁ

Univerzita P. J. Šafárika v Košiciach
Prírodovedecká fakulta

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:	Bc. Eva Marková
Študijný program:	Informatika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor:	Informatika
Typ záverečnej práce:	Diplomová práca
Jazyk záverečnej práce:	slovenský
Sekundárny jazyk:	anglický

Názov: Manažment bezpečnostných informácií a udalostí pre akademický informačný systém

Názov EN: Security information and event management for academic information system

Cieľ: (1) Analýza aktuálnych prístupov k manažmentu bezpečnostných informácií a udalostí (SIEM) s ohľadom na akademické informačné systémy.
(2) Návrh pravidiel detekcie bezpečnostných hrozieb pre akademický informačný systém zohľadňujúc MITRE ATT&CK rámec.
(3) Návrh, implementácia a vyhodnotenie SIEM systému pre akademický informačný systém.

Literatúra:
(1) MURDOCH, D. W. SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter. Independent Publishing, 2019.
(2) COLLINS, Michael. Network Security Through Data Analysis: From Data to Action. O'Reilly Media, Inc., 2017.
(3) STROM, Blake E., et al. Finding cyber threats with ATT&CK-based analytics. Technical Report MTR170202, MITRE, 2017.

Vedúci:	RNDr. JUDr. Pavol Sokol, PhD.
Oponent:	prof. RNDr. Gabriel Semanišin, PhD.
Ústav :	ÚINF - Ústav informatiky
Riaditeľ ústavu:	doc. RNDr. Ondrej Krídlo, PhD.

Dátum schválenia: 28.04.2021

Poďakovanie

Týmto sa chcem poďakovať vedúcemu práce RNDr. JUDr. Pavlovi Sokolovi, PhD. za odborné vedenie, cenné rady a veľkú pomoc pri spracovaní problematiky tejto diplomovej práce.

Abstrakt v štátnom jazyku

V práci sa zaoberáme hľadaním vhodného riešenia manažmentu bezpečnostných informácií a udalostí pre akademický informačný systém (SIEM). SIEM systém je schopný detegovať bezpečnostné útoky, pričom vyhodnocuje bezpečnostné udalosti a informácie. Hlavným cieľom tejto práce je navrhnúť takýto systém, aby sme boli schopní včas riešiť samotné dopady na organizáciu, prípadne úplne zabrániť útokom. Vzhľadom k tomu, že akademický informačný systém generuje mnoho rôznych záznamov, bolo nutné tieto záznamy spracovať a prispôsobiť. Pre účely vytvorenia SIEM systému sme sa rozhodli využiť riešenie s otvoreným zdrojovým kódom ELK (Elasticsearch, Logstash, Kibana). Nad týmto riešením je postavený SIEM systém. Pri implementácii systému zohľadňujeme MITRE ATT&CK rámec. Vybrané hrozby, relevantné pre akademický informačný systém, sme odsimulovali na testovacom serveri, aby sme následne boli schopní vytvoriť pravidlá pre detekciu útokov na akademickom informačnom systéme, a aby sme tak predišli prípadným neželaným dopadom (únik a podobne) pre akademickú inštitúciu. Útoky, ktoré je možné očakávať v rámci akademického informačného systému môžeme rozdeliť do troch kategórií – útoky na úrovni operačného systému, na úrovni webovej aplikácie a na úrovni prihláseného používateľa. Poslednou časťou tejto diplomovej práce je vyhodnotenie systému, kde berieme do úvahy závažnosť výskytu bezpečnostných hrozieb v rámci akademického informačného systému.

Kľúčové slová: akademický informačný systém, manažment bezpečnostných informácií a udalostí, MITRE ATT&CK, udalosť

Abstrakt v cudzom jazyku

In this work we deal with the search for a suitable solution for security information and event management for the academic information system. The SIEM system is able to detect security attacks while evaluating security events and information. The main goal of this work is to design such a system, so we are able to address the impacts on the organization in time, or completely prevent attacks. Due to the fact, that the academic information system generates many different logs, it was necessary to process and adapt these logs. For the purpose of creating a SIEM system, we decided to use an open source solution ELK (Elasticsearch, Logstash, Kibana). The SIEM system is built on top of this solution. During the implementation, we take into account the MITRE ATT&CK framework. We simulated relevant threats for the academic information system on a test server in order to be able to create rules for detecting attacks on the academic information system, and to prevent possible unwanted impacts (leakage, etc.) for the academic institution. The attacks that can be expected within the academic information system can be divided into three categories - attacks at the level of the operating system, at the level of the web application and at the level of the logged in user. The last part of this thesis is the evaluation of the system, where we take into account the severity of security threats within the academic information system.

Keywords: academic information system, security information and event management, MITRE ATT&CK, event

Obsah

Zoznam ilustrácií

Zoznam tabuliek

Zoznam skratiek a značiek

APT Advanced Persistent Threat, pokročilé trvalé hrozby

CORR Correlation Optimization Retention and Retrieval, uchovávanie a načítanie optimalizácie korelácie

DBMS Database Management System, systém správy databázy

HIDS Host-based intrusion detection system, systém detekcie narušenia hostiteľa

HTTP Hypertext transfer protocol, hypertextový prenosový protokol

IaaS Infrastructure as a Service, infraštruktúra ako služba

IP Internet protocol, internetový protokol

LMS Log Management System, systém manažovania záznamov (logov)

NIDS Network intrusion detection system, systém detekcie narušenia siete

SaaS Software as a Service, softvér ako služba

SEC Security Event Correlation, korelácia bezpečnostných udalostí

SEM Security Event Management, manažment bezpečnostných udalostí

SIEM Security Information and Event Management, manažment bezpečnostných informácií a udalostí

SIM Security Information Management, manažment bezpečnostných informácií

SOC Security Operations Center, centrum bezpečnostných operácií

TCP Transmission Control Protocol, protokol riadenia prenosu

TTP Tactics, Techniques and Procedures, taktiky, techniky a postupy

WIDS Wireless Intrusion Detection System, systém detekcie narušenia bezpečnosti pre bezdrôtové siete

Úvod

Informačné systémy predstavujú vo väčšine prípadov súčasť kritickej infraštruktúry organizácie. Mnohokrát sa pri týchto systémoch zabúda na adekvátne zabezpečenie až do chvíle, kým nie je zaznamenaná udalosť, ktorá bezprostredne ohrozuje aktívum alebo procesy organizácie (bezpečnostný incident). V rámci informačných systémoch sú uložené dôležité aktíva organizácie, resp. prostredníctvom týchto systémov sa realizujú procesy nutné pre fungovanie organizácie. V akademickom prostredí môžeme medzi najdôležitejšie procesy zaradiť zabezpečenie výučby a výskumnej činnosti. Z tohto dôvodu môžeme medzi kritickú infraštruktúru akademických inštitúcií zaradiť akademický informačný systém. V rámci tohto systému sa kumuluje veľké množstvo osobných, resp. iných citlivých údajov, ktoré je potrebné chrániť a zabrániť ich narušeniu.

Z pohľadu minimalizácie dopadov bezpečnostných incidentov je elementárne dôležitá detekcia bezpečnostných útokov nevynímajúc vyhodnotenie bezpečnostných udalostí a súvisiacich informácií a kontextu. K tomuto účelu využívame systémy na manažment bezpečnostných informácií a udalostí (SIEM). Spustenie úspešného SIEM systému vyžaduje, aby boli identifikované aktíva, siete, nepoužívané siete, aplikácie a privilegované účty.

Hlavným cieľom tejto záverečnej práce je navrhnúť vhodný SIEM systém, ktorý by zohľadňoval akademické prostredie, bezpečnostné zraniteľnosti, bezpečnostné hrozby a typy útočníkov ohrozujúcich akademické informačné systémy. Zo záznamov (logov) systému by tento systém mal byť schopný detegovať. relevantnú množinu bezpečnostných hrozieb, ktorým by mohol v budúcnosti čeliť práve akademický informačný systém. Tento hlavný cieľ práce je bližšie konkretizovaný v troch čiastočných cieľoch.

V prvom cieli práce sa zameriavame na analýzu a porovnanie aktuálnych prístupov k manažmentu bezpečnostných informácií a udalostí (SIEM). Na základe výsledkov analýzy bude možné zvoliť najvhodnejšiu implementáciu SIEM systému pre akademické prostredie. Súčasťou druhého cieľa je navrhnúť pravidlá pre detekciu bezpečnostných hrozieb vzhľadom na akademický informačný systém s ohľadom na MITRE ATT&CK rámec. Tento rámec nám primárne poslúži na špecifikáciu relevantných bezpečnostných hrozieb a zraniteľností.

Vybrané hrozby sme simulovali na testovacom serveri, aby sme následne boli schopní vytvoriť pravidlá pre detekciu útokov na akademickom informačnom systéme. Posledným cieľom tejto záverečnej práce je návrh a implementácia samotného SIEM systému pre akademický informačný systém. V rámci práce sa tiež zameriavame na vyhodnotenie implementovaného SIEM systému.

Práca je rozdelená do piatich základných kapitol. V prvej kapitole sa venujeme základnému opisu SIEM systémov, ich vlastnostiam a komponentom. Tiež sme porovnali rôzne implementácie SIEM systémov či už s otvoreným, alebo uzavretým kódom. Druhá kapitola tejto práce predstavuje jej jadro, zaoberá sa taktikami, technikami a procedúrami útočníkov. Bližšie v nej popisujeme MITRE ATT&CK rámec a tiež APT skupiny, ktoré v dnešnej dobe predstavujú veľké riziko pre rôzne organizácie. Zároveň popisujeme základné taktiky a techniky MITRE ATT&CK rámca s ohľadom na APT skupiny, ktoré sa vo svojich kampaniach zameriavajú na akademické inštitúcie. V tretej kapitole sa venujeme návrhu a implementácii SIEM systému. Popisujeme v nej návrh technickej infraštruktúry a použité nástroje. Na písanie pravidiel využívame Sigma formát, pričom následne pravidlá konvertujeme do čitateľnej podoby pre ElastAlert. Štvrtá kapitola je venovaná detekcii hrozieb v rámci akademického informačného systému AiS2. Bezpečnostné hrozby, relevantné pre akademický informačný systém, delíme na tri hlavné kategórie – na úrovni operačného systému, na úrovni webovej aplikácie a na úrovni prihláseného používateľa. V rámci tejto kapitoly tiež prepájame MITRE ATT&CK rámec s hrozbami, ktoré sme identifikovali v rámci akademického informačného systému AiS2. Poslednou kapitolou našej práce je vyhodnotenie implementovaného SIEM systému, kde poukazujeme na implementované pravidlá a ich účinnosť v rámci systému.

1 Security Information and Event Management (SIEM)

SIEM systémy sú v dnešnej dobe veľmi žiadané vzhľadom k tomu, že s postupujúcimi a rastúcimi organizáciami sa zvyšuje aj úroveň útoku. Tým pádom sú bezpečnostné hrozby ťažšie detekovateľné, čo vedie k častému narúšaniu bezpečnosti. Samotné bezpečnostné incidenty sú vo viacerých prípadoch odhalené až po dlhšej dobe, pričom sa môže stať, že sú úplne nepovšimnuté. To môže viesť k ďalším podobným neodhaliteľným útokom. Práve preto je vhodným riešením SIEM systém. V organizácii si je potrebné tiež stanoviť aktíva, pričom samotné aktíva generujú mnoho bezpečnostných udalostí. V rámci našej práce staviame SIEM systém nad akademickým informačným systémom.

Informačný systém je možné definovať ako infraštruktúru (informačné a komunikačné prostriedky), ktorej znefunkčnenie, resp. ochromenie má za následok negatívny vplyv na organizáciu a jej procesy [1].

1.1 Úvod do SIEM systémov

SIEM systém v sebe predstavuje kombináciu štyroch prvkov, a to SIM (Manažment bezpečnostných informácií, Security Information Management), SEM (Manažment bezpečnostných udalostí, Security Event Management, LMS (Systém manažovania záznamov, Log Management System) a SEC (Korelácia bezpečnostných udalostí, Security Event Correlation) [2].

Manažment bezpečnostných informácií (Security Information Management, SIM) ukladá, analyzuje, manipuluje a podáva správy o bezpečnostných záznamoch. Manažment bezpečnostných udalostí (Security Event Management, SEM) monitoruje systémy v reálnom čase a je zameraný na záznamy udalostí, ktoré sú generované z rôznych zariadení. Systém manažovania záznamov (Log Management System, LMS) zhromažďuje a ukladá logy z rôznych systémov a hostiteľov. Korelácia bezpečnostných udalostí (Security Event Correlation, SEC) je prístup, ktorý pozoruje sled udalostí, ktoré naznačujú potenciálnu hrozbu a upozorňuje správcov.

SIEM systém umožňuje členom SOC vykonávať analýzy založené na upozorneniach a udalostiach s cieľom nájsť hlavnú príčinu bezpečnostných incidentov. Zhromažďuje viacero zdrojov údajov vrátane monitorovania siete, zariadení

a riešení na ochranu koncových staníc. SIEM systém je veľmi dôležitý, pokiaľ ide o riadenie bezpečnostných incidentov, ktoré sa vyskytnú v inštitúcii.

V závislosti od implementácie, SIEM systémy ponúkajú rôzne funkcionality. Umožňujú vytvárať nástenky s upozorneniami, pričom všetky výstrahy sú zlúčené do jedného nástroja. Korelácia udalostí zvyšuje vernosť zistení viacerých podozrivých udalostí na základe spoločných kritérií alebo podozrivého správania. SIEM systém je tiež schopný zameriavať sa na viacero súborov údajov, aby sa stanovila hlavná príčina bezpečnostného incidentu. Môžeme tiež definovať a spravovať detekcie na základe indikátorov a detekčných pravidiel. SIEM systém je ale na druhej strane povinný dodržiavať rôzne zásady a predpisy rôznych noriem pre rôzne časti odvetvia. SIEM systém vo všeobecnosti zahŕňa tieto funkcionality [3]:

- Monitorovanie zabezpečenia v reálnom čase,
- threat intelligence,
- profilovanie správania,
- monitorovanie údajov a používateľov,
- monitorovanie aplikácií a
- analýza.

Monitorovanie zabezpečenia v reálnom čase predstavuje centralizované ukladanie a korelácia logov umožňuje analýzu organizácie v reálnom čase. Poskytuje upozornenia o živej aktivite alebo útokoch na vykonanie defenzívnych meraní.

Threat Intelligence (TI) sa definuje ako zber a analýza informácií o hrozbách a útočníkoch a vzorov kreslenia, ktoré poskytujú schopnosť robiť rozhodnutia týkajúce sa prevencie a reakcie voči rôznym bezpečnostným udalostiam. Je to proces rozpoznávania alebo odhaľovania akýchkoľvek neznámych hrozieb, ktorým organizácie môžu čeliť. Hlavným cieľom TI je dostať do povedomia existujúce, resp. objavujúce sa hrozby, a vopred sa pripraviť na rozvoj v oblasti kybernetickej bezpečnosti. Tento proces, pri ktorom sa prevádzajú neznáme hrozby na známe, pomáha pri predvídaní útoku a vedie k lepšiemu a zabezpečenému systému v organizácii [4].

SOC riadený hrozbami je schopný spravovať SIEM, vykonávať Threat Intelligence a Threat Hunting. TI zlepšuje viditeľnosť a schopnosť nachádzať zložitejšie hrozby. Threat Hunting je proces zisťovania a vyhľadávania podozrivých aktivít na minulých

údajoch alebo logoch. Jedná sa o vytváranie hypotéz alebo indikátorov kompromitácie, pričom bezpečnostný analytik vytvára možné scenáre hrozieb s príslušnými aktérmi a vektormi hrozieb. Je to užitočné pri zisťovaní vzorov útokov, ktoré sa prostredníctvom SIEM systému nedetegujú [5].

Je nutné, aby centrum bezpečnostných operácií (Security Operations Center, SOC) pochopilo, ktoré aktíva ovplyvňujú ktoré procesy a aplikácie, implementovalo monitorovanie a pochopilo, ako útočník myslí a následne implementovať pravidlá, pomocou ktorých ich identifikuje [6].

TI poskytuje komplexné informácie o netradičných bezpečnostných hrozbách. Profilovanie a zdokonaľovanie vedomostí o potenciálnych útokoch, ktoré môžu ohroziť organizáciu. Pomáha porozumieť bezpečnostným rizikám najbežnejších vonkajších hrozieb, napr. zero-day zraniteľnosť, pokročilé pretrvávajúce hrozby a exploity [3].

Profilovanie správania predstavuje naučenie sa činnosti používateľa a spôsobu využívania zdrojov v organizácii. Profilovanie správania vytvára profily normálnej aktivity pre rôzne kategórie udalostí, ako sú sieťové toky, aktivita používateľov a prístup na server. Systém je schopný pomáhať pri upozorňovaní na akékoľvek odchýlky od normálneho správania [3].

Monitorovanie údajov a používateľov sa zameriava na autentifikáciu a autorizáciu používateľov. Spočiatku sa vykoná autentifikácia používateľa a potom sa skontrolujú oprávnenia používateľa k súborom, ku ktorým má prístup v databáze. Akýkoľvek prístup alebo zmena súboru, ktorá sa nemá vykonať, bude mať za následok neobvyklú aktivitu a vytvorí varovanie. Monitorovanie privilegovaných používateľov a prístup k citlivým údajom je požiadavkou na podávanie správ [3].

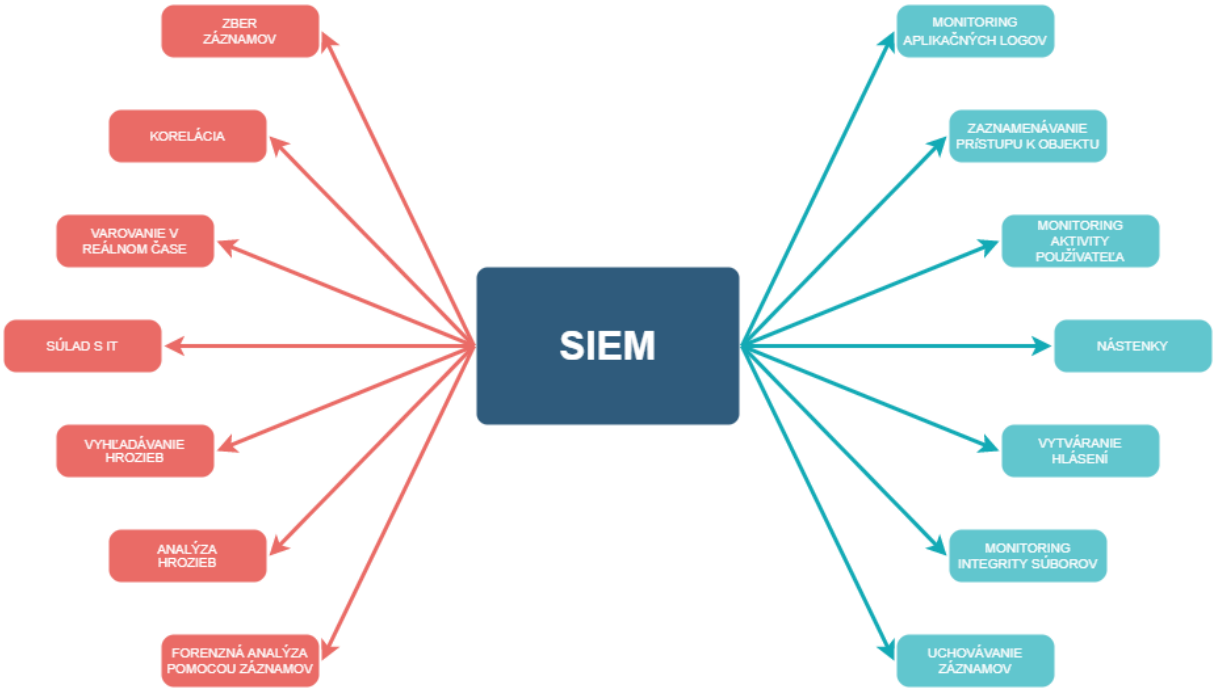
Monitorovanie aplikácií sleduje nedostatky v aplikácii, ako sú chyby alebo zraniteľnosť, ktoré sa využívajú cielenými útokmi. Schopnosť analyzovať toky aktivít z aplikácií umožňuje monitorovanie aplikačnej vrstvy [3].

Analýza umožňuje objavovanie, interpretáciu zmysluplných vzorov v analýze bezpečnosti údajov. Vyšetruje činnosť používateľa a prístup k zdrojom s cieľom identifikovať bezpečnostnú hrozbu, porušenie alebo zneužitie oprávnenia [3].

1.2 Základné vlastnosti SIEM systémov

Implementácia SIEM systému môže pomôcť v mnohých ohľadoch. Vďaka nemu vieme zvýšiť viditeľnosť v sieti. To umožňuje organizácii pozorne sledovať aktivitu používateľa, údaje, ku ktorým pristupuje, počet pokusov o prihlásenie a ďalšie informácie, ako je pridávanie nových používateľov, inštalácia nových aplikácií, výkon siete a podobne. Rovnako je možné sledovať všetky škodlivé aktivity a incidenty spôsobujúce výstrahy [7].

Ak je počet zariadení a aplikácií v sieti obrovský, potom aj súbory so záznamami (logmi) vytvorené zdrojmi bezpečnostných udalostí sú obrovské. Nájdenie škodlivého incidentu v týchto udalostiach nie je možné zhromaždením ich na jednom centralizovanom mieste. Na obrázku č. 1 môžeme vidieť typické schopnosti SIEM systémov [8] [9].



Obr. 1 Typické schopnosti SIEM systémov

- **Zber záznamov** – SIEM zbiera záznamy z rôznorodých zdrojov ako sú systémy Windows, systémy Unix / Linux, rôzne aplikácie, databázy a taktiež smerovače, prepínače a iné zariadenia.

- **Korelácia** – Prepája bezpečnostné udalosti, ako aj súvisiace údaje do zmysluplných balíkov, ktoré popisujú bezpečnostný incident, hrozbu alebo zraniteľnosť. Vykonáva sa na základe vyhľadávania logov, pravidiel a výstrah.
- **Varovanie v reálnom čase** – SIEM analyzuje udalosti a odosiela výstrahy analytikom SOC, aby ich informoval o okamžitých problémoch, a to buď prostredníctvom správ, emailov alebo nástenieк.
- **Súlad s IT**
- **Vyhľadávanie hrozieb (Threat hunting)** – Umožňuje bezpečnostnému tímu spúšťať dopyty na údajoch, analyzovať a filtrovať ich pre identifikáciu hrozieb alebo slabých miest.
- **Analýza hrozieb (Threat intelligence)** – SIEM je schopný analyzovať údaje a identifikovať hrozby v sieti. Nielenže identifikuje hrozby, ale tiež chápe ich možný vzťah k bezpečnostným udalostiam.
- **Forenzná analýza pomocou záznamov** – Analytik je schopný sledovať rôzne aktivity alebo útočníka v záznamoch.
- **Monitoring aplikačných záznamov** – Je schopný monitorovať záznamy z aplikácií, súbory so záznamami, záznamy bezpečnostných udalostí, záznamy služieb a systémové záznamy systému Windows, Unix a Linux.
- **Zaznamenávanie prístupu k objektu** – SIEM upozorňuje používateľov na ich súbory a priečinky - kto k nim pristupuje, kto ich odstránil, upravil, presunul a ďalšie činnosti. Vytvára správy o prístupe k objektom vo formátoch čitateľných pre človeka a odosiela upozornenia, ak k niektorému zo súborov / priečinkov majú prístup neoprávnené osoby.
- **Monitoring aktivity používateľa** – Táto vlastnosť systému SIEM umožňuje sledovanie podozrivého správania používateľov.
- **Nástenky** – Analytik SOC používa nástenky na vykonávanie správnych akcií v správnom čase a prijíma správne rozhodnutia pri nájdení anomálií v sieti.
- **Vytváranie hlásení** – SIEM poskytuje používateľom správy o bezpečnostných incidentoch a udalostiach súvisiacich so zabezpečením, ako sú aktivity škodlivého softvéru, úspešné a neúspešné prihlásenia a rôzne ďalšie škodlivé aktivity.
- **Monitoring integrity súborov** – SIEM uľahčuje monitorovanie integrity súborov v reálnom čase zabezpečením citlivých súborov a priečinkov.

- **Uchovávanie záznamov** – Táto funkcia umožňuje používateľom uchovávať historické záznamy a vykonávať forenzné vyšetrovanie a interné audity.

1.3 Komponenty SIEM systémov

Typický SIEM systém pozostáva zo 4 rôznych komponentov. Prvým komponentom sú samotné **údaje**. Organizácia častokrát využíva veľký počet zariadení, na ktorých je nainštalovaných niekoľko aplikácií. Väčšina aplikácií a softvérov v nich je predvolene schopná generovať záznamy (logy). Existujú rôzne druhy zariadení alebo systémov ako napríklad sieťové zariadenia, bezpečnostné nástroje (firewall,...), servery a aplikácie [9].

Ďalším komponentom sú **zberatelia / agenti / konektory**. Zberateľ je entita, ktorá prijíma informácie o bezpečnostnej udalosti generovanej v sieti. Základnou činnosťou, ktorú zberateľ robí, je to, že zhromažďuje a normalizuje informácie získané z rôznych zariadení pred ich odoslaním do centrálneho „nástroja“ (engine). Existuje niekoľko rôznych typov zberateľov. Každému z nich je pridelená iná úloha. Informácie, ktoré zhromažďujú zberatelia, sú v zásade záznamy zo serverov a zariadení pripojených k sieti prostredníctvom káblovej alebo bezdrôtovej siete.

Dôležitým komponentom je **centrálny „nástroj“ (engine)**. Je to miesto, kde prebieha korelácia údajov a analýza záznamov. Korelácia údajov je proces porovnávania sérií normalizovaných záznamov s cieľom určiť množinu súvisiacich udalostí na základe určitej množiny pravidiel. Používa koreláciu založenú na pravidlách, štatistickú alebo algoritmickú koreláciu a ďalšie metódy na vzájomné spájanie rôznych bezpečnostných udalostí. Analýza údajov je proces identifikácie vzorov a anomálií v korelovaných záznamoch, ktorý označuje aktivitu pokusu o narušenie alebo porušenie politiky. V tejto analýze sa analyzuje obrovské množstvo záznamov. Vytváranie hlásení a analýza záznamov sa taktiež vykonáva v centrálnom „nástroji“ (engine), rovnako ako aj analýza a monitorovanie úloh. V prípade podozrivej aktivity môže byť jej nahlásenie uskutočnené mnohými spôsobmi, napríklad upozornením správcu zaslaním emailu, zobrazením upozornenia v novom okne, na pracovnej ploche alebo spôsobom, ktorý uprednostňuje používateľ.

Posledným komponentom je **databáza**. Záznamy sa ukladajú na určité časové obdobie v závislosti od politiky uchovania. Uchovávanie záznamov je proces odstraňovania starších údajov, ktoré prekročili dobu uchovania na serveroch. Záznamy,

ktoré sa zhromažďujú z rôznych zariadení, sa ukladajú v centrálnom úložisku. Záznamy zhromaždené z týchto zariadení a aplikácií majú rôznu veľkosť, dôležitosť a dostupnosť. Databázy nie sú fyzickými zariadeniami, ktoré je možné nainštalovať na konkrétne miesto. Spravidla sú to cloudové úložiská, pretože sa používajú na ukladanie obrovského množstva údajov, avšak nevylučujú sa ani fyzické disky.

1.4 Implementácie SIEM systémov s uzavretým kódom

Jednou z úloh v rámci tejto diplomovej práce je analyzovať rôzne implementácie SIEM systémov dostupných pre zabezpečenie organizácií. Obdobne, ako aj u iných bezpečnostných produktov, aj tu nachádzame platené riešenia.

1.4.1 Splunk Enterprise

Splunk Enterprise [10] je softvérový produkt, ktorý umožňuje vyhľadávať, analyzovať, a vizualizovať údaje zhromaždené z komponentov akejkoľvek IT infraštruktúry. Prijíma údaje z webových stránok, aplikácií, senzorov, zariadení a podobne. Po definovaní zdroja údajov, Splunk Enterprise indexuje tok dát a analyzuje ich na sériu jednotlivých udalostí, ktoré je možné zobraziť a prehľadávať. Splunk Enterprise môže byť rozšírený pomocou aplikácií. Ponúka viac ako tisíc aplikácií, pričom je možné vytvoriť si vlastnú podľa konkrétnych potrieb.

Výstrahy upozorňujú, keď výsledky vyhľadávania pre historické aj reálne výsledky vyhovujú nakonfigurovaným podmienkam. Výstrahy je možné nakonfigurovať tak, aby spúšťali rôzne akcie, ako napríklad odosielanie výstražných informácií na určené emailové adresy a podobne.

Nástenky obsahujú panely modulov, ako sú vyhľadávacie polia, grafy a podobne. Zobrazujú výsledky dokončených vyhľadávaní a údaje z vyhľadávaní v reálnom čase, ktoré prebiehajú na pozadí.

Pivot predstavuje tabuľku, graf alebo vizualizáciu údajov, ktoré sa dajú vytvoriť pomocou programu „Pivot Editor“. Editor umožňuje mapovať atribúty definované objektmi údajového modelu na tabuľku, graf alebo vizualizáciu údajov bez toho, aby museli na ich generovanie písať vyhľadávania v jazyku SPL (Search Processing Language).

1.4.2 IBM QRadar

IBM QRadar SIEM [11] pomáha bezpečnostným tímom presne zisťovať a určovať priority bezpečnostných hrozieb v rámci podniku. Súčasne poskytuje inteligentné informácie, ktoré umožňujú tímom rýchlo reagovať a znižovať dopad bezpečnostných incidentov. Vďaka konsolidácii záznamov a údajov o sieťových tokoch z tisícok zariadení, koncových staníc a aplikácií distribuovaných v rámci siete QRadar koreluje všetky tieto rôzne informácie a agreguje súvisiace udalosti do jedného upozornenia. To je najmä z dôvodu, aby sa urýchlila analýza a riešenie bezpečnostných incidentov. QRadar SIEM je k dispozícii na lokálnom zariadení, ale aj v cloudovom prostredí. Je to komerčný nástroj, ktorý je podporovaný aj na platforme Linux.

Tento SIEM systém poskytuje centralizovaný prehľad o protokoloch, toku a udalostiach v prostrediach v prostredí Software as a Service (SaaS) a Infrastructure as a Service (IaaS). Umožňuje centrálne sledovanie všetkých udalostí súvisiacich s konkrétnou bezpečnostnou hrozbou na jednom mieste. Poskytuje "out-of-the-box" analýzu, ktorá automaticky analyzuje logy a sieťové toky na detekciu bezpečnostných hrozieb a generovanie prioritných upozornení. Na to, aby boli dodržané interné organizačné zásady, IBM QRadar poskytuje vopred zostavené správy a šablóny.

1.4.3 AlienVault USM Anywhere

USM Anywhere [12] je platforma, ktorá je schopná nájsť alebo identifikovať nesprávne nakonfigurované systémy, hostiteľov, ktorí vzišli z radaru správy aktív a systémy ohrozené škodlivým softvérom. Je tiež schopný nájsť nevhodný alebo neoprávnený prístup k citlivým údajom alebo zdrojom od interných aj externých strán.

Na zabezpečenie siete USM Anywhere využíva predovšetkým korelačné pravidlá. Pravidlá spájajú udalosti dohromady do zmysluplných skupín a premieňajú údaje na užitočné informácie. Je tiež možné vytvoriť pravidlá orchestrácie, ktoré zabezpečia operácie zabezpečenia siete.

Poskytuje výkonnú detekciu hrozieb, reakciu na incidenty a správu súladu s predpismi na jednotnej platforme. Kombinuje všetky základné bezpečnostné funkcie potrebné na efektívne sledovanie bezpečnosti v cloudových a lokálnych prostrediach – zisťovanie aktív, hodnotenie zraniteľností, detekcia narušenia, monitorovanie správania,

správa protokolov SIEM a neustále informácie o hrozbách. USM Anywhere je cloudové bezpečnostné riešenie, ktoré je možné si prispôsobiť podľa aktuálnych potrieb [13].

1.4.4 ArcSight

ArcSight [14] má moduly na monitorovanie udalostí, analýzu správania, systém pravidiel pre spracovávanie bezpečnostných udalostí. Vzhľadom na uzavretý zdrojový kód je ťažké pridať nové funkcie. ArcSight používa vlastný CORR (Correlation Optimized Retention and Retrieval) engine ako databázový spravovací systém (Database Management System – DBMS). V systéme nie je implicitne implementovaná možnosť ukladania udalostí prichádzajúcich bez konkrétneho vzoru alebo masky. To znamená, že na pridávanie nových informácií, je potrebný ďalší zásah do systému. Systém implementuje centralizované ukladanie údajov. Jadro systému ArcSight ESM je licencované podľa množstva logov za deň. Okrem jadra je potrebné mať licenciu aj na rôzne nastavenia a možnosti, napríklad počet používateľov, vývoj vlastných konektorov, počet zdrojov udalostí, moduly zhody, správa protokolov atď.

ArcSight SIEM [15] pozostáva z troch vrstiev. Prvá vrstva je pre zariadenia, ktoré generujú logy a druhá vrstva je pre konsolidáciu týchto logov. Posledná vrstva sa používa na účely monitorovania. Centrálny server SIEM sa správa ako rodič a komunikuje so strednými SIEM servermi, ktoré sú známe ako podriadené. Podriadené uzly zhromažďujú všetky údaje z rôznych zariadení a normalizujú zhromaždené udalosti predtým, ako prechádzajú do centrálneho servera na účely korelácie a nahlasovania.

1.5 Implementácie SIEM systémov s otvoreným kódom

Pre účely našej diplomovej práce sú dôležité riešenia s otvoreným kódom. Medzi tie patrí napríklad Elastic Stack, Splunk Free, AlienVault OSSIM a podobne. Tieto riešenia sú síce plne dostupné a škálovateľné podľa potrieb, avšak môžu mať nejaké obmedzenia. Napríklad Splunk Free je obmedzený v rámci maximálnej povolenej sieťovej prevádzky, pričom povoľuje len 500MB denne. Elastic Stack ponúka len rolu administrátora, zatiaľ čo iné komerčné riešenia majú k dispozícii rôzne role užívateľov. Dôležité pre nás je však to, že implementácie s otvoreným kódom si nastavujeme od začiatku až po koniec podľa potreby.

1.5.1 Splunk Free

Splunk Free [16] poskytuje obmedzený prístup k funkciám Splunk Enterprise. Táto licencia je určená na samostatnú inštaláciu na jednu inštanciu. Umožňuje indexovať 500MB za deň, pričom pri prekročení prichádza upozornenie na porušenie licencie. Hlavnými obmedzeniami sú objem indexovaných dát za deň a odstránené funkcie. Licencia Splunk Free umožňuje hromadne načítať väčšie súbory až dvakrát za 30 dní, čo môže byť užitočné pri forenznom posudzovaní veľkých súborov údajov. Táto bezplatná licencia zabráni prehľadávaniu, ak sa v 30-dňovom okne vyskytnú tri upozornenia. Splunk Free síce bude pokračovať v indexovaní údajov, ale deaktivuje funkciu vyhľadávania. Táto funkcia sa obnoví, keď v priebehu tridsiatich dní existuje menej ako tri varovania o porušovaní licencie. Splunk Free má obmedzených niekoľko funkcií. Upozorňovanie nie je k dispozícii. Neexistujú žiadni používatelia ani role, ktoré by bolo možné konfigurovať. Konfigurácie distribuovaného vyhľadávania a klastrovanie indexov nie je k dispozícii a ďalšie.

1.5.2 IBM QRadar Community Edition

Komunitná edícia [17] je plne funkčná bezplatná verzia programu QRadar. Vyžaduje nízku pamäť, spracováva menej udalostí za sekundu a obsahuje trvalú licenciu. Táto verzia je obmedzená na 50 udalostí za sekundu a 5000 sieťových tokov za minútu. Podporuje rôzne doplnkové aplikácie, ale nevyužíva sa pre podniky. QRadar Community Edition umožňuje používateľom, študentom, bezpečnostným profesionálom a vývojárom aplikácií učiť sa a využívať najnovšie funkcie QRadar bez vypršania platnosti alebo časového limitu.

1.5.3 AlienVault OSSIM

AlienVault OSSIM [18] je SIEM systém s otvoreným kódom, ktorý obsahuje kompletizáciu udalostí, normalizáciu a koreláciu. Bol spustený bezpečnostnými technikmi z dôvodu nedostatku produktov s otvoreným zdrojovým kódom. Bol vytvorený špeciálne na riešenie jediného problému. Poskytuje mnoho základných bezpečnostných funkcií ako napríklad zisťovanie aktív, posúdenie zraniteľností,

detekcia nepovoleného vstupu, monitorovanie správania a korelácia udalostí SIEM systémom.

Využíva AlienVault Open Threat Exchange (OTX) [19], čo umožňuje používateľom prispievať a prijímať informácie o škodlivých hostiteľoch v reálnom čase. Okrem toho je AlienVault OSSIM neustále vyvíjaný. OSSIM obsahuje nasledujúce softvérové komponenty [20]:

- PRADS [21], používané na identifikáciu hostiteľov a služieb pasívnym monitorovaním sieťovej prevádzky.
- Snort [22], ktorý sa používa ako systém detekcie narušenia (IDS) a tiež sa používa na krížovú koreláciu s OpenVAS.
- Suricata [23] tiež používaná ako IDS systém.
- TCPtrack [24] používaný na informácie o reláciách, ktoré môžu poskytnúť užitočné informácie na koreláciu útoku.
- Munin [25] na analýzu trafiky a „watchdogging“.
- NFSen [26] / NFDump [27], ktorý sa používa na zhromažďovanie a analýzu informácií NetFlow.
- FProbe [28], ktorý sa používa na generovanie údajov NetFlow zo zachytenej prevádzky.
- Nagios [29], ktorý sa používa na monitorovanie hostiteľov a špecifikovaných portov z hľadiska dostupnosti aktív a úplného monitorovania miestneho systému.
- OpenVas [30] sa používa na hodnotenie zraniteľnosti založeného na práci s aktívami.
- OSSIM obsahuje aj nástroje vyvinuté samostatne, z ktorých najdôležitejší je generický korelačný modul s podporou logickej smernice a integrácia protokolov s doplnkami.

Zahŕňa systém detekcie narušenia hostiteľa (HIDS), systém detekcie narušenia siete (NIDS), systém detekcie narušenia bezpečnosti pre bezdrôtové siete (WIDS), komponenty monitorovania sieťových uzlov, analýzu anomálií siete, skener zraniteľností, systém výmeny informácií o hrozbách medzi používateľmi, sadu

doplnkov na analýzu a koreláciu záznamov protokolu syslog s rôznymi externými zariadeniami a službami.

1.5.4 Elastic Stack

Elastic Stack [31] je sada nástrojov vyvinutá spoločnosťou Elastic. Medzi tieto nástroje patria Elasticsearch, Logstash, Kibana a rôzne Beats nástroje. Elastic Stack je zadarmo, open-source a vhodný na fulltextové vyhľadávanie. Elastic ponúka dve cesty na použitie ich nástrojov, a to možnosť umiestnenia v cloude alebo možnosť umiestnenia priamo na lokálnom počítači.

Elasticsearch je škálovateľná, distribuovaná databáza dokumentov so zabudovanou funkciou vyhľadávania, agregácie a regulácie. Typ databázy je NoSQL, bola vytvorená Shayom Banonom v roku 2010. Zálohuje služby ako Microsoft Azure Search, Wordpress a časti Stack Exchange.

Logstash je nástroj na agregáciu prichádzajúcich záznamov a správ, ich spracovanie úpravou alebo doplnením logovacích dát a ich následné posunutie do Elasticsearch. Posielanie záznamov priamo do Elasticsearch bez Logstash môže viesť k nekonzistentným dátam. Na druhej strane, Kibana predstavuje webové klientske rozhranie. S programom Elasticsearch ľahko pracuje s grafmi a vizualizačnými údajmi.

Beats nástroje sú malé nástroje na čítanie záznamov z rôznych zdrojov. Zvyčajne posielajú dáta priamo do Logstash alebo Elasticsearch. Metricbeat slúži na čítanie záznamov z operačného systému a aplikácií. Packetbeat monitoruje sieť. Winlogbeat číta záznamy z „Windows Event Log“. Filebeat zbiera údaje z textových logovacích súborov. Libbeat umožňuje vytvoriť si vlastný beat nástroj podľa uváženia.

Samotný Elastic Stack nám ponúka tiež modul na upozorňovanie správcov v prípade nepriaznivých situácií, pričom kontinuálne monitoruje logy pre predkonfigurované podmienky.

Tab. 1 Porovnanie SIEM systémov

	Splunk Free	**Splunk Enterprise**	**IBM QRadar Community Edition**	**IBM QRadar**	**AlienVault OSSIM**	**USM Anywhere**	**ArcSight**	**ELK**
Open-source	✓	X	✓	X	✓	X	X	✓

Denné množstvo dát	Do 500MB	bez limitu	bez limitu	bez limitu	bez limitu	bez limitu	bez limitu	bez limitu
Nástenky	✓	✓	✓	✓	X	✓	✓	✓
Alerting	X	✓	✓	✓	?	✓	✓	✓
Účty	len admin	bez limitu	bez limitu	bez limitu	bez limitu	3 role (read-only, analyst, manager)	bez limitu	len admin
Doplnky	✓	✓	X	✓	✓	✓	✓	✓
Škálovateľnosť	Single Server	bez limitu	?	bez limitu	Single Server	SaaS	bez limitu	bez limitu
Aplikácie	X	✓	X	✓	X	✓	✓	✓
Vyhľadávanie a reporty	obmedzené	✓	✓	✓	✓	✓	✓	✓
Cena	zadarmo	platené	zadarmo	platené	zadarmo	platené	platené	zadarmo
MITRE ATT&CK	X	✓	X	✓	X	✓	✓	✓

V tabuľke č. 1 môžeme vidieť porovnanie vyššie spomínaných implementácií SIEM systémov. Porovnávali sme ich z niekoľkých rôznych hľadísk. Jedným z najdôležitejších kritérií je to, či je daná implementácia založená na otvorenom kóde (open-source), keďže nasadenie a prevádzka SIEM systému je finančne náročná záležitosť. Keďže chceme implementovať SIEM systém nad akademickým informačným systémom, je potrebné, aby sme mohli SIEM systém konfigurovať a modifikovať podľa našich potrieb. Medzi implementácie založené na otvorenom kóde patria Splunk Free, IBM QRadar Community Edition, AlienVault OSSIM a Elastic Stack. Splunk Free je obmedzený tým, že povoľuje maximálnu dennú sieťovú prevádzku len do 500MB. Aj napriek tomu, že implementácia systémov s otvoreným kódom (open-source) je vo všeobecnosti náročná (keďže je potrebné si všetko nastaviť vlastnoručne), ukázalo sa, že je výhodou, že si správca SIEM systému môže všetko nastaviť sám podľa vlastných potrieb.

Dôležitým atribútom je tiež možnosť vytvárať si vlastné nástenky. Jedine AlienVault OSSIM túto funkcionalitu nepodporuje, a teda je pre nás nie najvhodnejšou implementáciou. Spoločnosť AT&T túto možnosť vytvárať nástenky pridala do komerčného nástroja USM Anywhere. V našom systéme potrebujeme tiež odosielať

upozornenia o podozrivej aktivite správcom. Všetky vyššie spomenuté implementácie okrem Splunk Free a AlienVault OSSIM podporujú zasielanie výstrah.

Ďalším atribútom, ktorý sledujeme je schopnosť vytvárať účty s rôznymi rolami. Zatiaľ čo Splunk Free a Elastic Stack podporujú vytvorenie len administrátorského účtu, ostatné implementácie neudávajú limit tomuto parametru. Pridávať doplnky do systémov umožňujú všetky implementácie, okrem IBM QRadar Community Edition. AlienVault OSSIM za doplnok považuje podporu komunity na fórach.

Zatiaľ čo väčšina z implementácií nemá obmedzenú škálovateľnosť, Splunk Free a AlienVault OSSIM je možné nainštalovať len na jeden server. USM Anywhere funguje ako SaaS infraštruktúra. Možnosť doinštalovať rôzne aplikácie umožňujú takmer všetky implementácie, obmedzené sú len implementácie s otvoreným kódom a to Splunk Free, IBM QRadar Community Edition a AlienVault OSSIM. Vyhľadávanie a vytváranie reportov umožňujú takmer všetky systémy. Obmedzenú funkcionalitu má len Splunk Free.

Implementácie s otvoreným kódom sú, samozrejme, zadarmo. Splunk Enterprise a ArcSight majú cenník nastavený podľa toho, koľko údajov pretečie za deň cez systém. IBM QRadar si účtuje poplatky v závislosti od počtu zaznamenaných udalostí za sekundu a USM Anywhere v závislosti od toho, koľko dní chceme uchovávať dáta v systéme. Splunk Enterprise si napríklad účtuje za údaje o veľkosti 10GB na deň počas roka približne 25 tisíc amerických dolárov pre nelimitované množstvo používateľov. Pri IBM QRadar hardvér začína na cene 10 400 amerických dolárov, cloudové riešenie na 800 dolároch za mesiac.

Na účely našej práce je najdôležitejším atribútom spolupráca s MITRE ATT&CK rámcom. Väčšina implementácií s otvoreným kódom nemá vytvorené žiadne pomocné metódy a aplikácie pre podporu MITRE ATT&CK. Pre Elastic Stack sú vytvorené návody, ako pracovať s týmto rámcom. USM Anywhere zverejnil webináre týkajúce sa práce s týmto rámcom. Splunk Enterprise, ArcSight a IBM QRadar podporujú aplikácie na prácu s MITRE ATT&CK, avšak jedná sa o implementácie s uzavretým kódom. V tabuľke č. 2 sa nachádza porovnanie minimálnych hardvérových požiadaviek.

Tab. 2 Porovnanie minimálnych hardvérových požiadaviek SIEM systémov

	Splunk Free	**Splunk Enterprise**	**IBM QRadar Community Edition**	**IBM QRadar**	**AlienVault OSSIM**	**USM Anywhere**	**ArcSight**	**ELK**
OS	Linux, MacOS, Windows	Linux, Windows	Linux	Linux	Linux	Linux	Linux	Linux, MacOS, Windows
RAM	2GB	12GB	8GB	8-10GB	4-8GB	12GB	48GB	8GB
CPU	Intel Nehalem	Intel Nehalem	2 jadrá	2 jadrá	2 jadrá	4 CPU	8 jadier	2 jadrá
HDD	-	-	250GB	250GB	250GB	150GB	1,5TB	-

Analýzou viacerých implementácií sme došli k záveru, že najlepšou voľbou pre naše účely je Elastic Stack. Jedná sa o implementáciu s otvoreným kódom, denné množstvo dát nie je obmedzené, ponúka možnosť tvorby nástenieк. Pomocou doplnku ElastAlert sme schopní vytvárať upozornenia a posúvať ich správcom akademického informačného systému. Systém vieme skonštruovať na viacerých serveroch, čim vieme minimalizovať dopad výpadku na takmer nulový. Jedinou nevýhodou je, že každý, kto má prístup k systému, má administrátorské oprávnenia, preto je potrebné zvážiť, kto môže prispievať k chodu a funkcionalite SIEM systému. Hardvérové požiadavky neovplyvnili náš výber.

2 Taktiky, techniky a postupy

Za útokmi sa obvykle skrývajú rôzne motívy (ciele) a účel. Motív vychádza z toho, že cieľový systém ukladá alebo spracováva niečo cenné. Účelom útoku môže byť narušenie rôznych operácií cieľovej organizácie, ukradnutie cenných informácií kvôli zvedavosti alebo dokonca pomsta. Tieto motívy alebo ciele závisia od duševného stavu útočníka, jeho dôvodu pre vykonanie takejto činnosti a jeho zdrojov a schopností. Keď útočník určí svoj cieľ, môže použiť rôzne nástroje, techniky a metódy na zneužitie slabých miest v počítačovom systéme alebo v bezpečnostných zásadách a ovládacích prvkoch [32].

Medzi motívy útočníkov, ktoré súvisia s akademickým informačným systémom radíme napríklad:

- krádež informácií,
- manipulácia s údajmi,
- finančná strata pre cieľ,
- poškodenie reputácie cieľa,
- túžba po pomste a
- túžba po finančnom zisku.

Útok vo všeobecnosti môžeme zapísať ako rovnicu „Útok = Motív (Cieľ) + Metóda (Taktiky, techniky a postupy) + Zraniteľnosť“.

Slovné spojenie „taktiky, techniky a postupy“ (TTP) sa vzťahuje na vzorce činností a metód spojených s konkrétnymi aktérmi hrozieb alebo so skupinami aktérov hrozieb. TTP sú užitočné pri analýze hrozieb a profilovaní aktérov hrozieb, a môžu sa ďalej použiť na posilnenie bezpečnostnej infraštruktúry organizácie. Taktika je definovaná ako „stratégia, pomocou ktorej útočník vykoná útok od začiatku do konca“. Technika je definovaná ako „technické metódy používané útočníkom na dosiahnutie medzivýsledkov útoku“. Postup je definovaný ako „organizačný prístup, ktorý útočníci použijú na zahájenie útoku“. Aby sme pochopili a bránili sa pred útočníkmi, je dôležité porozumieť ich použitým taktikám, technikám a postupom [33].

Zraniteľnosť je existencia slabiny, chyba v dizajne alebo implementácii, ktorá pri zneužití vedie k neočakávanej a nežiaducej udalosti ohrozujúcej bezpečnosť

systému. Ak by tieto chyby zabezpečenia zostali nepovšimnuté, otvorilo by to dvere rôznym typom vírusov a útokom [34].

Na prácu s taktikami, technikami a procedúrami využívame rámec MITRE ATT&CK, ktorý nám poskytuje pohľad na správanie sa útočníkov v reálnom svete. Zameriava sa na to, ako externí protivníci kompromitujú a pôsobia v rámci počítačových sietí. Tiež nám poskytuje spôsoby detekcie a mitigácie rôznych techník. V tomto rámci si vieme prezrieť podrobnosti o rôznych APT skupinách, o nástrojoch a podobne.

Rámec MITRE ATT&CK [35] je celosvetovo dostupná vedomostná základňa protichodných taktík a techník založená na pozorovaniach v reálnom svete. Tento rámec sa používa ako základ na vývoj špecifických modelov a metodológií bezpečnostných hrozieb. MITRE prístup je založený na piatich princípoch [36]:

- zahŕňa postkompromitačnú detekciu,
- zameriava sa na správanie,
- používa model založený na hrozbách,
- iteruje podľa návrhu a
- vyvíja a testuje sa v realistickom prostredí.

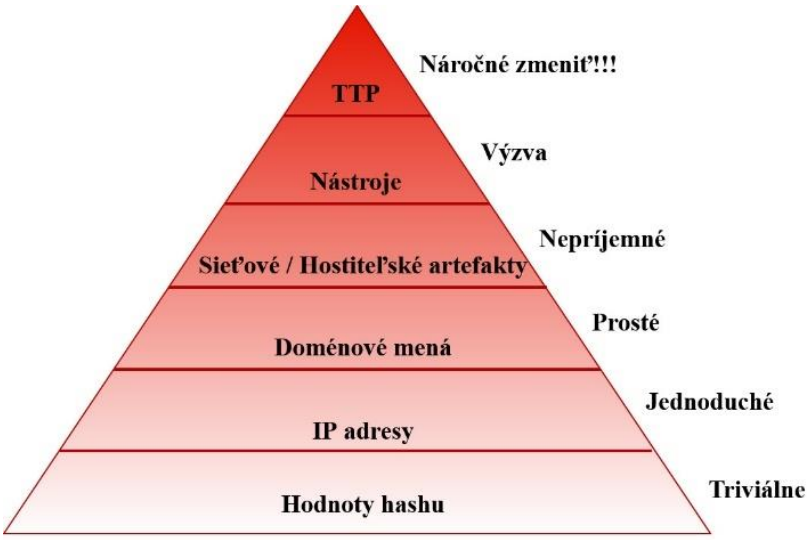
Ide o rámec založený na pozorovaní správania sa útočníkov v reálnom svete, ktorý je voľne prístupný. Na obrázku č. 2 môžeme vidieť Cyber Kill Chain [37] mapovaný do MITRE ATT&CK rámca. Cyber Kill Chain pozostáva zo siedmich krokov, ktoré opisujú činnosti, ktoré musí útočník vykonať na dosiahnutie cieľa.

Obr. 2 Cyber Kill Chain mapovaný do rámca MITRE ATT&CK

MITRE ATT&CK vznikol z projektu, ktorý dokumentoval a kategorizoval postkompromitačné protivnícke taktiky, techniky a postupy (TTP) proti operačným systémom Microsoft Windows s cieľom zlepšiť detekciu škodlivého správania. Časom

sa rozšíril o operačné systémy Linux aj MacOS. ATT&CK je model správania, ktorý pozostáva z nasledujúcich hlavných komponentov:

- taktiky označujúce krátkodobé, taktické protivnícke ciele počas útoku,
- techniky opisujúce prostriedky, pomocou ktorých protivníci dosahujú taktické ciele,
- čiastočné techniky (subtechniques), ktoré opisujú konkrétnejšie prostriedky, pomocou ktorých protivníci dosahujú taktické ciele na nižšej úrovni ako techniky a
- zdokumentované protichodné používanie techník, ich postupov a iných metaúdajov.



Obr. 3 Pyramída bolesti [38]

Na obrázku č. 3 môžeme vidieť model „pyramídy bolesti“, ktorý bol vytvorený bezpečnostným expertom Davidom J Biancom v roku 2013. Každá úroveň pyramídy predstavuje rôzne typy indikátorov útoku, ktoré môžu byť použité na odhaľovanie aktivít protivníka. Pyramída je rozdelená podľa toho, koľko „bolesti” (práce) spôsobí útočníkovi, keď indikátory identifikujeme a bude musieť meniť svoje taktiky. Rámec MITRE ATT&CK sa podľa modelu „pyramídy bolesti“ (obrázok č. 3) zaoberá práve taktikami, technikami a postupmi, pretože tie útočníci menia len veľmi zriedkavo. Zmeniť tieto spôsoby a návyky pre útočníka nie je triviálne, zatiaľ čo zmeniť IP adresy, doménové mená alebo digitálne odtlačky (hashe) je v súčasnosti veľmi jednoduché.

2.1 Podrobnejšia štruktúra rámca MITRE ATT&CK

Vzťah medzi taktikami, technikami a čiastočnými technikami je vizualizovaný v MITRE ATT&CK matici. Taktika je v podstate skupina techník, ktorú môžu využiť protivníci na dosiahnutie cieľa. Niektoré techniky sú rozdelené ešte na čiastočné techniky, ktoré detailnejšie opisujú ako môže byť dané správanie dosiahnuté [39]. MITRE ATT&CK rámec je organizovaný do „technologických domén“ [40]:

- Enterprise (predstavujúca tradičné siete alebo cloudové technológie),
- Mobile (pre mobilné komunikačné zariadenia) a
- ICS (pre priemyselné riadiace systémy).

V rámci každej technologickej oblasti definuje viac „platforiem“ – operačný systém, aplikácia, pričom techniky a čiastočné techniky sa môžu týkať viacerých platforiem. Pre Enterprise to sú Linux, MacOS, Windows, AWS, Azure, GCP, SaaS, Office 365 a Azure AD, a pre Mobile sú to Android a iOS.

Taktiky reprezentujú dôvod techniky alebo čiastočnej techniky. Opisujú teda dôvod vykonania akcie útočníkom. S taktikou sa zaobchádza ako so „značkami“, pri ktorých technika alebo čiastočná technika spadá do jednej alebo viacerých taktických kategórií v závislosti od rôznych výsledkov, ktoré sa dajú pomocou tejto techniky dosiahnuť. Každá taktika obsahuje definíciu opisujúcu kategóriu, a slúži ako návod na to, aké techniky by mali byť použité v taktike. MITRE ATT&CK rámec popisuje napríklad taktiku „prieskum“ (Reconnaissance).

Techniky reprezentujú spôsob, ako útočník dosiahol taktický cieľ vykonaním akcie. Tiež môžu reprezentovať, čo útočník získa vykonaním akcie. **Čiastočné techniky** sú špecifickejším opisom toho, aké správanie bolo použité na dosiahnutie cieľa. Do taktiky „prieskum“ padne napríklad technika „aktívne skenovanie“ (T1595). Postupy sú tiež dôležitým komponentom TTP konceptu. Sú to špecifické implementácie techník a čiastočných techník, ktoré boli použité útočníkmi.

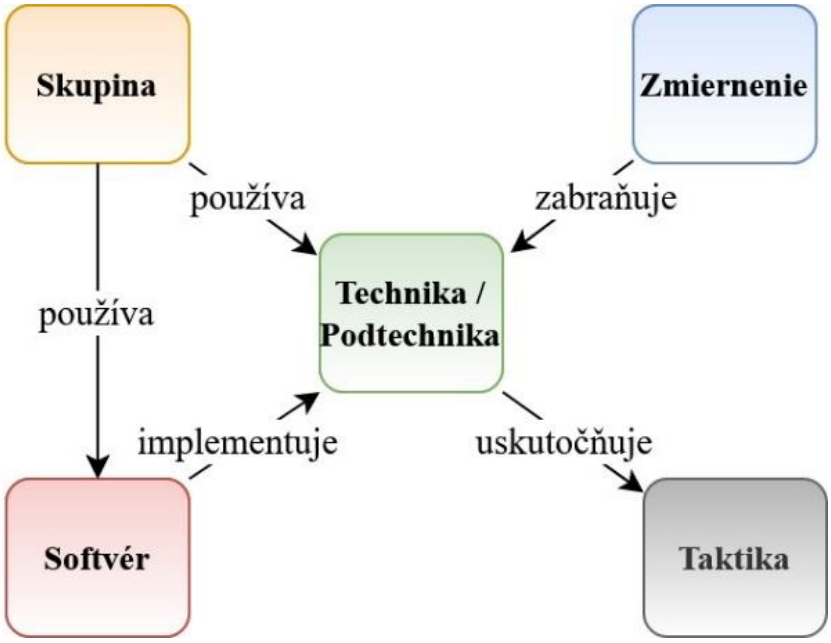
Známi útočníci, ktorí sú sledovaní a nahlasovaní verejnými a súkromnými organizáciami, sú označovaní v rámci MITRE ATT&CK v **skupinách**. Tento rámec sa primárne zameriava na APT skupiny, no zahŕňa aj iné pokročilé skupiny, ako napríklad

finančne motivovaných aktérov. Skupiny môžu používať techniky priamo alebo využívať rôzne typy softvérov, ktoré implementujú techniky.

Softvér je rozdelený do dvoch hlavných kategórií, a to na nástroje a malvér. Nástroj môže byť komerčný, s otvoreným kódom, vstavaný alebo verejne prístupný softvér, ktorý by mohol použiť obranca, člen „red team-u“, penetračný tester, ale aj útočník vo svoj prospech. Táto kategória zahŕňa softvér, ktorý sa všeobecne nenachádza v organizácii, ako aj softvér, ktorý je všeobecne dostupný ako súčasť operačného systému. Medzi príklady týchto nástrojov radíme napríklad PsExec, Metasploit, Mimikatz, ale aj súčasti operačného systému Windows ako Net, netstat, Tasklist a podobne. Malvér je škodlivý softvér. Medzi malvér radíme napríklad Emotet, Agent Tesla a podobne.

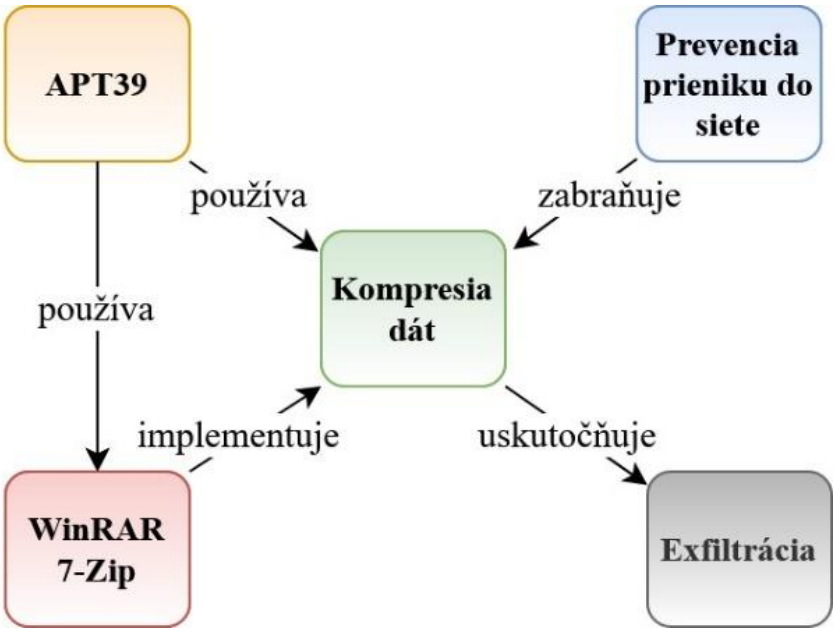
Zmiernenia v ATT&CK predstavujú bezpečnostné koncepcie a triedy technológií, ktoré možno použiť na zabránenie úspešnému vykonaniu techniky alebo čiastočnej techniky.

Každá zložka ATT&CK nejakým spôsobom súvisí s inými komponentmi. Vzťahy opísané vyššie je možné znázorniť na obrázku č. 4.



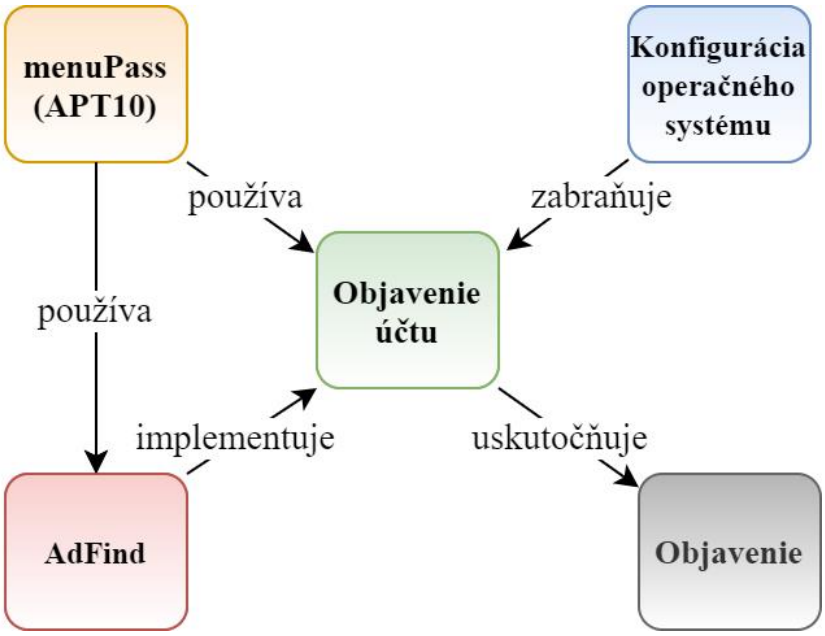
Obr. 4 Vzťahy komponentov rámca MITRE ATT&CK

Na obrázku č. 5 môžeme vidieť znázornené vzťahy pre prípad, keď APT39 používa WinRAR alebo 7-Zip na kompresiu archivovaných ukradnutých dát:



Obr. 5 Vzťahy komponentov rámca MITRE ATT&CK – príklad APT39 skupiny

Na obrázku č. 6 môžeme vidieť príklad pre skupinu menuPass (APT10). Táto skupina na objavenie účtov využíva nástroj AdFind.

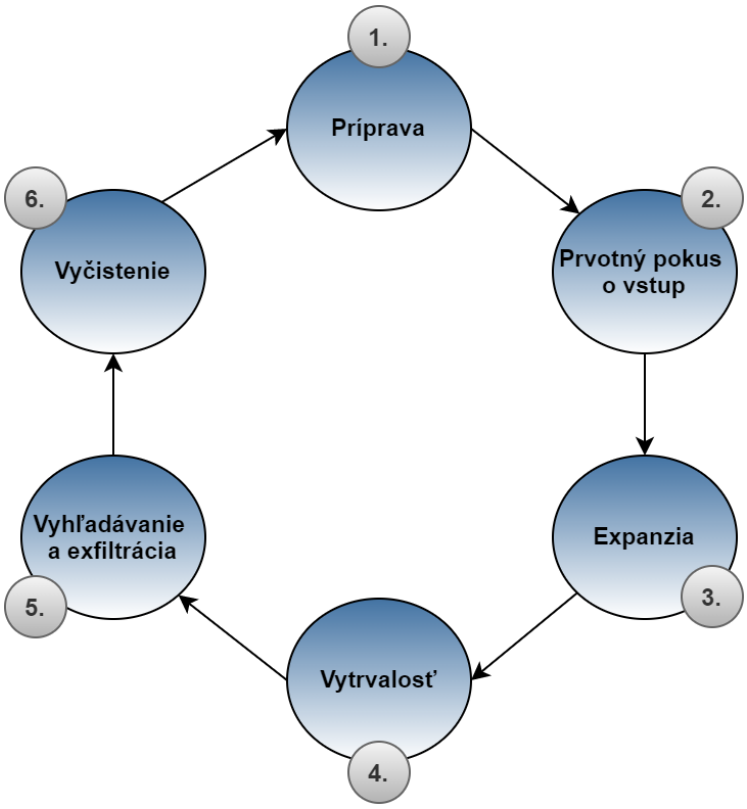


Obr. 6 Vzťahy komponentov rámca MITRE ATT&CK – príklad APT10 skupiny

2.1.1 Advanced Persistent Threat (APT)

APT skupiny sú známe tým, že útočník získa neautorizovaný prístup do cieľovej siete a ostáva neodhalený dlhší čas. V APT slovo „pokročilá“ označuje použitie techník na zneužitie základných chýb systému. Slovo „trvalá“ označuje externý systém velenia a riadenia (C&C system), ktorý neustále extrahuje údaje a monitoruje počítačovú sieť obete. Slovo „hrozba“ znamená zapojenie človeka do koordinácie. Útoky APT sú veľmi sofistikované útoky, pri ktorých útočník používa dobre prepracovaný škodlivý kód v kombinácii s koordinovanými technikami, pri ktorých útočníci po splnení určitého cieľa vyčistia dôkazy o škodlivých činnostiach. Útoky APT sa zvyčajne vykonávajú proti organizáciám, ktoré majú cenné informácie, ako sú finančné, zdravotnícke, obranné a letecké, výrobné a obchodné odvetvia. Hlavným cieľom týchto útokov je skôr získať citlivé informácie ako sabotovať organizácie a ich sieť. Medzi metódy používané na uskutočnenie útoku patria rôzne techniky sociálneho inžinierstva na zhromažďovanie informácií o cieli, techniky zabraňujúce detekcii bezpečnostnými mechanizmami a techniky na udržanie prístupu na dlhú dobu. Aby útočník uspel v získaní počiatočného prístupu, musí vykonať prieskum zraniteľností v cieľovej sieti. APT útoky zvyčajne vykonáva zločinecká skupina alebo zločinecká organizácia [41].

Jednou z dôležitých charakteristík APT je, že pri uskutočňovaní útoku vykonávajú viac fáz. Fázy takýchto útokov sú prieskum, získanie prístupu, objavenie, zachytenie a exfiltrácia údajov. Škodlivé kódy, ktoré sa používajú na vykonávanie takýchto útokov, sú navrhnuté a napísané takým spôsobom, že sa zameriavajú na konkrétne chyby zabezpečenia v počítačovej sieti obete. Len čo protivník vstúpi do cieľovej siete, nadviaže spojenie so serverom a stiahne škodlivé kódy pre ďalšie útoky. V počiatočnej fáze procesu útoku APT vytvorí útočník cez server viac vstupných bodov, aby udržal prístup k cieľovej sieti. APT skupiny často využívajú tzv. zero-day zraniteľnosti. Útoky vykonávané APT skupinami teda môžu ľahko obísť bezpečnostné mechanizmy, ako je brána firewall, antivírusový softvér, IDS / IPS a emailový spamový filter [42]. Na obrázku č. 7 môžeme vidieť **životný cyklus** APT [43].



Obr. 7 Životný cyklus APT

Prvou fázou životného cyklu APT je **príprava**, kedy útočník definuje cieľ, vykonáva rozsiahly výskum zameraný na cieľ, organizuje tím, zostavuje alebo získava nástroje a vykonáva testy na detekciu. Útoky APT zvyčajne vyžadujú vysokú úroveň prípravy, pretože útočník nemôže riskovať, že ho detegujú. Pred vykonaním útoku môžu byť potrebné ďalšie zdroje a údaje .

Ďalšia fáza zahŕňa **prvotný pokus o vstup** do cieľovej počítačovej siete. Bežnou technikou použitou pri počiatočnom vniknutí je neoprávnené získavanie údajov emailom typu phishing alebo zneužívanie zraniteľností na verejne dostupných serveroch. Po získaní informácií od cieľa útočníci tieto informácie použijú na uskutočnenie ďalších útokov na cieľovú sieť. V tejto fáze sa škodlivý kód alebo škodlivý softvér nasadí do cieľového systému s cieľom nadviazať pripojenie.

Primárnym cieľom fázy **expanzie** je rozšírenie prístupu do cieľovej siete a získanie poverení. Hlavným cieľom útočníka v tejto fáze je získanie prihlasovacích údajov správcu na eskaláciu privilégií a získanie ďalšieho prístupu k systémom v sieti. Útočníci na zisk prihlasovacích údajov väčšinou používajú techniky ako sociálne inžinierstvo, zneužitie zraniteľností a distribúcia infikovaných zariadení USB. Po získaní

prihlasovacích údajov k cieľu je pohyb útočníka v počítačovej sieti ťažko vysledovateľný, pretože útočník používa legitímne používateľské meno a heslo.

Fáza **vytrvalosti (perzistencie)** zahŕňa udržanie prístupu k cieľovému systému. Aby si útočníci udržali prístup k cieľovému systému, dodržiavajú určité techniky alebo postupy, medzi ktoré patrí napríklad použitie prispôsobeného škodlivého softvéru alebo nástrojov. Tieto nástroje sú navrhnuté tak, aby ich nedokázal odhaliť antivírus. Ďalším spôsobom, ako zachovať vytrvalosť, je vyhľadanie miest na inštaláciu škodlivého softvéru, ktoré sa neskúmajú často. Medzi tieto umiestnenia patria smerovače, servery, brány firewall, tlačiarne a podobne.

Vo fáze **vyhľadávania a exfiltrácie** útočník dosahuje cieľ, ktorým je spravidla získanie prístupu k prostriedku, ktorý sa dá použiť na vykonanie ďalších útokov, alebo použitie tohto prostriedku na získanie finančného zisku. Útočníci sa spravidla zameriavajú na konkrétne údaje alebo dokumenty pred zahájením útoku. Bežnou metódou vyhľadávania a exfiltrácie je odcudzenie všetkých údajov vrátane dôležitých dokumentov, emailov, zdieľaných diskov a iných typov údajov nachádzajúcich sa v cieľovej sieti.

Vyčistenie je posledná fáza, keď útočník vykoná určité kroky, aby zabránil odhaleniu a odstránil dôkazy o kompromitácii. To zahŕňa vyhýbanie sa detekcii a elimináciu dôkazov o vniknutí. Útočníci musia zaistiť, aby systém vyzeral tak, ako vyzeral pred získaním prístupu a narušením siete.

Medzi skupiny, ktoré sa zameriavali na akademické inštitúcie, radíme Charming Kitten, Stolen Pencil, APT19, DarkHydrus, SilverTerrier, Turla, Leviathan a menuPass. Týmito skupinami boli využívané techniky existujúce v rámci MITRE ATT&CK rámca. My sme sa zamerali na tie, ktoré sú uskutočniteľné v akademickom informačnom systéme. Zo štrnástich taktík, ktoré nám ponúka MITRE ATT&CK rámec tieto skupiny využili jedenásť vo svojich útokoch (v zameraní na operačný systém Linux).

2.1.2 Taktika: Počiatočný prístup (Initial Access) a Perzistencia (Persistence)

Útočník sa snaží získať prístup do počítačovej siete a udržať si ho. Počiatočný prístup pozostáva z techník, ktoré používajú rôzne vstupné vektory na získanie

počiatočnej „opory“ v sieti [44]. Opory získané počiatočným prístupom môžu umožniť nepretržitý prístup, napríklad platné účty a použitie externých vzdialených služieb.

Perzistencia spočíva v technikách, ktoré útočníci používajú na udržanie prístupu k systémom po reštartoch a iných prerušeniach [45]. Medzi techniky, ktoré sa používajú v rámci perzistencie, patria všetky zmeny prístupu, akcie alebo konfigurácie, ktoré im umožňujú udržať si oporu v systémoch. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, bola využívaná z týchto taktík táto jedna technika a jej čiastočná technika, ktorá je uvedená v tabuľke č. 3.

Tab. 3 Techniky pre taktiky Počiatočný prístup a Perzistencia

Označenie	Názov	Popis
T1078	Valid Accounts	získanie a zneužitie prihlasovacích údajov účtov
T1078.003	Valid Accounts: Local Accounts	získanie a zneužitie prihlasovacích údajov lokálnych účtov

2.1.3 Taktika: Vykonávanie (Execution)

V rámci tejto taktiky sa útočník pokúša vykonávať škodlivý kód. Vykonanie spočíva v technikách, ktorých výsledkom je kód riadený útočníkom v lokálnom alebo vzdialenom systéme [46]. Techniky, pri ktorých sa vykonáva škodlivý kód, sa často spájajú s technikami všetkých ostatných taktík na dosiahnutie cieľov, ako je prieskum siete alebo odcudzenie údajov. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, boli využívané z tejto taktiky dve techniky, ktoré sú uvedené v tabuľke č. 4.

Tab. 4 Techniky pre taktiku Vykonávanie

Označenie	Názov	Popis
T1059	Command and Scripting Interpreter	zneužitie príkazových riadkov na spúšťanie príkazov, skriptov alebo binárnych súborov
T1204.002	User Execution: Malicious File	spustenie škodlivého súboru

2.1.4 Taktika: Eskalácia privilégií (Privilege Escalation)

V rámci tejto taktiky sa útočník snaží získať oprávnenia vyššej úrovne. Eskalácia privilégií pozostáva z techník, ktoré útočníci používajú na získanie oprávnení vyššej úrovne v systéme alebo počítačovej sieti organizácie [47]. Útočníci môžu často vstúpiť a preskúmať sieť s neprivilegovaným prístupom, ale na splnenie cieľov potrebujú vyššie oprávnenia. Bežným prístupom je využívať bezpečnostné zraniteľnosti alebo nesprávne konfigurácie. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, boli využívané z tejto taktiky dve techniky, ktoré sú uvedené v tabuľke č. 5.

Tab. 5 Techniky pre taktiku Eskalácia privilégií

Označenie	Názov	Popis
T1055	Process Injection	injekcia kódu do procesov
T1078.003	Valid Accounts: Local Accounts	získanie a zneužitie prihlasovacích údajov lokálnych účtov

2.1.5 Taktika: Únik pred ochranou (Defense Evasion)

V rámci tejto taktiky sa útočník snaží vyhnúť odhaleniu. Táto taktika pozostáva z techník, ktoré útočníci používajú, aby zabránili odhaleniu počas celej kompromitácie [48]. Medzi techniky používané na únik pred ochranou patrí odinštalovanie alebo zakázanie bezpečnostného softvéru alebo šifrovanie údajov a skriptov. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, boli využívané z tejto taktiky štyri techniky, ktoré sú uvedené v tabuľke č. 6.

Tab. 6 Techniky pre taktiku Únik pred ochranu

Označenie	Názov	Popis
T1027.005	Obfuscated Files or Information: Indicator Removal from Tools	odstránenie indikátorov z nástrojov
T1055	Process Injection	injekcia kódu do procesov

T1078.003	Valid Accounts: Local Accounts	získanie a zneužitie prihlasovacích údajov lokálnych účtov
T1562.001	Impair Defenses: Disable or Modify Tools	deaktivácia bezpečnostných nástrojov kvôli vyhnutiu sa detekcii nástrojov a aktivít

2.1.6 Taktika: Prístup k údajom (Credential Access)

V rámci tejto taktiky sa útočník pokúša ukradnúť účty a heslá. Prístup k údajom pozostáva z techník odcudzenia prihlasovacích údajov, ako sú názvy účtov a heslá [49]. Používanie účtov legitímnych používateľov môže útočníkom poskytnúť prístup do systémov, sťažiť ich detekciu a poskytnúť príležitosť vytvoriť viac účtov, ktoré im pomôžu dosiahnuť ich ciele. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, boli využívané z tejto taktiky štyri techniky, ktoré sú uvedené v tabuľke č. 7.

Tab. 7 Techniky pre taktiku Prístup k údajom

Označenie	Názov	Popis
T1003	OS Credential Dumping	pokus o vytiahnutie údajov pre získanie prihlasovacích údajov
T1110	Brute Force	použitie techniky hrubej sily na získanie prístupu k účtom
T1552.001	Unsecured Credentials: Credentials In Files	vyhľadávanie súborov v lokálnych súborových systémoch a vzdialených zdieľaniach súborov, ktoré obsahujú nezabezpečené údaje
T1555	Credentials from Password Stores	hľadanie bežných miest na ukladanie hesiel pre získanie údajov používateľov

2.1.7 Taktika: Objavenie (Discovery)

V rámci tejto taktiky sa útočník snaží spoznať prostredie. Táto taktika spočíva v technikách, ktoré môže protivník použiť na získanie znalostí o systéme

a lokálnej počítačovej sieti organizácie [50]. Tieto techniky pomáhajú nepriateľom pozorovať prostredie a orientovať sa v ňom. Na dosiahnutie cieľa zhromažďovania informácií sa často používajú natívne nástroje operačného systému. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, bolo využívaných z tejto taktiky 14 techník, ktoré sú uvedené v tabuľke č. 8.

Tab. 8 Techniky pre taktiku Objavenie

Označenie	Názov	Popis
T1007	System Service Discovery	získanie informácií o registrovaných službách
T1016	System Network Configuration Discovery	získanie informácií o konfigurácii siete
T1018	Remote System Discovery	získanie zoznamu ďalších systémov podľa IP adresy, názvu hostiteľa alebo iného logického identifikátora v sieti
T1033	System Owner/User Discovery	identifikácia primárneho používateľa, aktuálne prihláseného používateľa a podobne
T1049	System Network Connections Discovery	získanie zoznamu sieťových spojení
T1057	Process Discovery	získanie zoznamu procesov
T1069.001	Permission Groups Discovery: Local Groups	získanie zoznamu lokálnych systémových skupín a oprávnení
T1069.002	Permission Groups Discovery: Domain Groups	získanie zoznamu doménových systémových skupín a oprávnení
T1082	System Information	získanie detailných informácií o operačnom systéme a hardvéri

	Discovery	
T1083	File and Directory Discovery	objavenie súborov a adresárov
T1087.001	Account Discovery: Local Account	získanie zoznamu účtov v lokálnom systéme
T1087.002	Account Discovery: Domain Account	získanie zoznamu doménových účtov
T1124	System Time Discovery	získanie informácií o systémovom čase
T1201	Password Policy Discovery	získanie informácií o politike hesiel

2.1.8 Taktika: Bočný pohyb (Lateral Movement)

V rámci tejto taktiky sa útočník snaží pohybovať sa prostredím (prechádza z jedného zariadenia na iné v rámci počítačovej siete organizácie). Táto taktika pozostáva z techník, ktoré protivníci používajú na vstup a riadenie vzdialených systémov v rámci počítačovej siete [51]. Dosiahnutie ich primárneho cieľa často vyžaduje preskúmanie siete s cieľom nájsť svoj cieľ a následné získanie prístupu k nemu. Dosiahnutie ich cieľa často znamená dosiahnutie zisku prostredníctvom viacerých systémov a účtov. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, boli využívané z tejto taktiky dve techniky, ktoré sú uvedené v tabuľke č. 9.

Tab. 9 Techniky pre taktiku Bočný pohyb

Označenie	Názov	Popis
T1021.004	Remote Services: SSH	použitie platných účtov na prihlásenie pomocou SSH
T1570	Lateral Tool Transfer	prenos nástrojov alebo súborov medzi systémami

2.1.9 Taktika: Zber (Collection)

V rámci tejto taktiky sa útočník snaží zhromaždiť údaje. Zber pozostáva z techník, ktoré môžu útočníci použiť na zhromažďovanie informácií a zdrojov, z ktorých sa zhromažďujú informácie, ktoré sú relevantné pri dosahovaní cieľov útočníkov [52]. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, boli využívané z tejto taktiky tri techniky, ktoré sú uvedené v tabuľke č. 10.

Tab. 10 Techniky pre taktiku Zber

Označenie	Názov	Popis
T1005	Data from Local System	prehľadávanie súborových systémov alebo lokálnych databáz
T1213	Data from Information Repositories	využitie úložísk informácií na ťažbu cenných údajov
T1560.001	Archive Collected Data: Archive via Utility	komprimácia alebo šifrovanie údajov použitím nástrojov tretej strany

2.1.10 Taktika: Velenie a riadenie (Command And Control)

V rámci tejto taktiky sa útočník snaží komunikovať s narušenými systémami, aby ich mohol ovládať. Velenie a riadenie [53] pozostáva z techník, ktoré môžu protivníci použiť na komunikáciu so systémami, ktoré ovládajú, v rámci počítačovej siete obete. Protivníci sa bežne pokúšajú napodobniť normálny očakávaný prenos, aby sa vyhli odhaleniu. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, bolo využívaných z tejto taktiky päť techník, ktoré sú uvedené v tabuľke č. 11.

Tab. 11 Techniky pre taktiku Velenie a riadenie

Označenie	Názov	Popis
T1071.001	Application Layer Protocol: Web Protocols	komunikácia pomocou protokolov aplikačnej vrstvy spojených s webovým prenosom

T1071.002	Application Layer Protocol: File Transfer Protocols	komunikácia pomocou protokolov aplikačnej vrstvy spojených s prenosom súborov
T1071.003	Application Layer Protocol: Mail Protocols	komunikácia pomocou protokolov aplikačnej vrstvy spojených s doručovaním elektronickej pošty
T1105	Ingress Tool Transfer	prenos nástrojov alebo súborov z externého systému do kompromitovaného prostredia
T1132.001	Data Encoding: Standard Encoding	šifrovanie údajov pomocou štandardného systému šifrovania údajov

2.1.11 Taktika: Exfiltrácia (Exfiltration)

V rámci tejto taktiky sa útočník sa snaží získať údaje. Exfiltrácia [54] spočíva v technikách, ktoré môžu protivníci použiť na odcudzenie údajov z počítačovej siete. Keď zhromaždia údaje, útočníci ich často zbalia, aby sa pri ich odstraňovaní vyhli odhaleniu. To môže zahŕňať rôzne spôsoby prevencie detekcie, ako sú kompresia a šifrovanie. Pri skupinách, ktoré sa zameriavajú na akademické inštitúcie, bola využívaná z tejto taktiky jedna technika, ktorá je uvedená v tabuľke č. 12.

Tab. 12 Techniky pre taktiku Exfiltrácia

Označenie	Názov	Popis
T1567.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	exfiltrácia dát do cloudového úložiska

2.2 Prepojenie pozorovaných dát a MITRE ATT&CK rámca

Na to, aby sme mohli s týmto rámcom pracovať, je potrebné vedieť ako mapovať dáta do matice, ktorú nám sprostredkúva tento rámec. Mapovať dáta do MITRE ATT&CK rámca môžeme z dvoch rôznych zdrojov dát – buď priamo z reportu, alebo z pôvodných (raw) dát. Mapovanie z reportu zahŕňa 6 krokov [55]:

1. pochopenie útoku,
2. nájdenie vykonanej činnosti,
3. preskúmanie činnosti,
4. "preloženie" činnosti na taktiku,
5. zistenie, aká technika bola použitá a
6. porovnanie výsledkov s inými analytikmi.

Pochopenie útoku je veľmi dôležitým krokom pri mapovaní, keďže nie každý útok je možné bez bližších a doplňujúcich informácií adekvátne vyhodnotiť. Z tohto dôvodu je potrebné podrobné preštudovanie správy (reportu), prípadne nájdenie relevantných informácií v rámci threat intelligence.

Pri hľadaní vykonanej činnosti je potrebné zamerať sa na to, čo robil aktér hrozby prípadne škodlivý program na danom zariadení V reportoch si vieme vyznačiť konkrétne činnosti (môže sa priamo jednať o slovesá), a tiež je potrebné zamerať sa na detaily, aby nám nič neuniklo. Ďalším krokom je dodatočne preskúmať činnosť, ktorá bola vykonaná, ak sme niečomu úplne neporozumeli. Keďže hovoríme o MITRE ATT&CK rámci, je potrebné danú činnosť „preložiť“ do jazyka tohto rámca. Inými slovami mapovať danú činnosť do kategórie podľa toho, čo chcel útočník dosiahnuť. Tento rámec nám ponúka dvanásť rôznych možností, a to:

- počiatočný prístup (Initial Access),
- vykonanie (Execution),
- vytrvalosť (Persistence),
- eskalácia privilégií (Privilege Escalation),
- obranné úniky (Defense Evasion),
- prístup k osobným údajom (Credential Access),
- objavenie (Discovery),
- „bočný“ pohyb (Lateral Movement),
- kolekcia (Collection),
- velenie a riadenie (Command and Control),
- exfiltrácia (Exfiltration) a

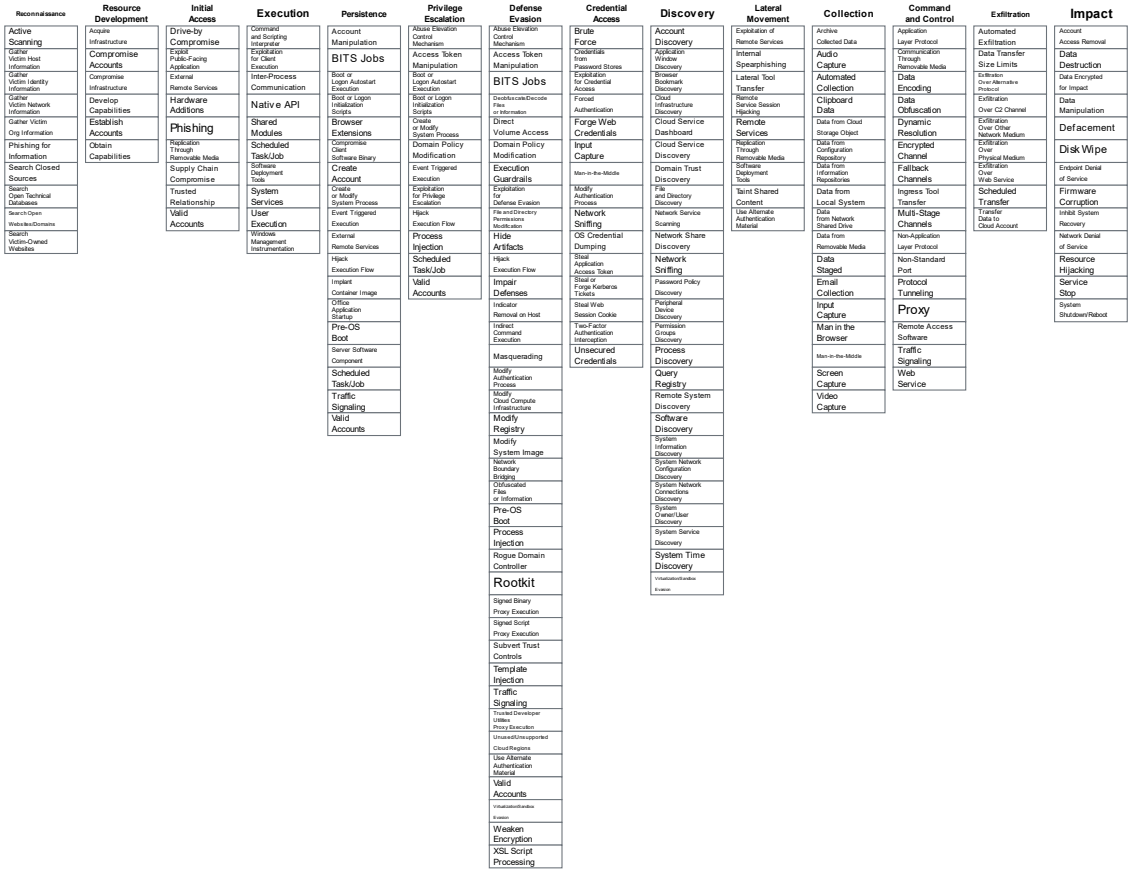
- dopad (Impact).

Nakoniec je potrebné zistiť, aká konkrétna technika bola použitá. Stratégiou by mohlo byť najprv sa pozrieť na zoznam techník pre danú taktiku, vyhľadávať v dialógovom okne na webovej stránke rámca, prípadne si vyznačiť kľúčové slová a špecifické príkazy a podľa nich hľadať vhodnú techniku. Posledným a bonusovým krokom je porovnať výsledky s inými analytikmi, ale to v našom prípade nebude relevantné, keďže chceme vytvoriť automatizovaný systém.

Pri mapovaní do MITRE ATT&CK z pôvodných (raw) dát je postup veľmi podobný. Pri tomto je dôležité si uvedomiť, že musíme sledovať príkazy príkazového riadka (shellu), nezvyčajné správanie zariadenia, pracovať s forenznými diskovými obrazmi, sledovať sieťovú komunikáciu daného zariadenia .

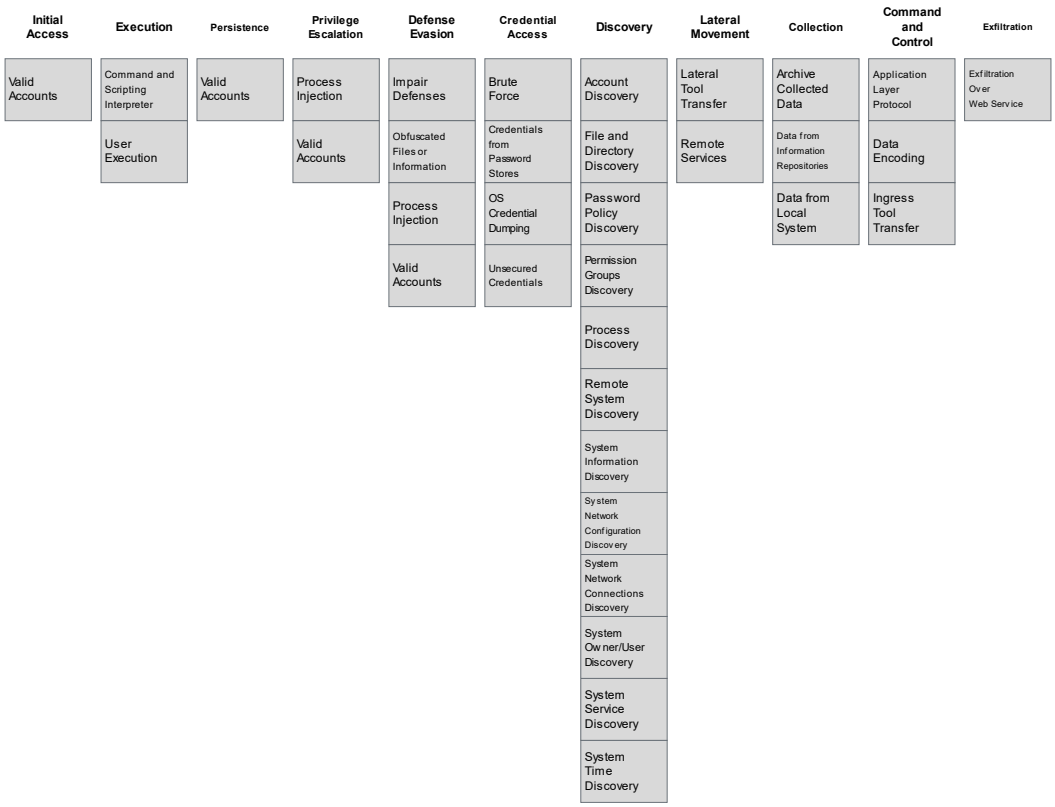
Pri ukladaní a analýze mapovaných dát je dôležité si zodpovedať na niekoľko otázok, ako napríklad to, komu majú byť určené dáta, ako ich budeme prepájať s inými informáciami, aké detailné má byť mapovanie alebo akým spôsobom sa budú importovať a exportovať dáta.

MITRE ATT&CK rámec nám ponúka tzv. navigátor [56], ktorý nám dovoľuje si zvýrazňovať techniky, ktoré sú pre nás dôležité a podobne. Teda pri samotnej analýze bezpečnostných rizík a analýze hrozieb, ktoré sú relevantné pre akademický informačný systém máme k dispozícii takúto platformu, s ktorou môžeme pracovať podľa vlastných potrieb. Na obrázku č. 8 môžeme vidieť techniky z rámca MITRE ATT&CK:



Obr. 8 ATTACK navigátor

Na obrázku č. 9 môžeme vidieť vyznačené techniky, ktoré sa vykonávali v rámci známych útokov na akademické inštitúcie. Pre akademické a výskumné inštitúcie sú špecifické útoky, vďaka ktorým útočníci získavajú osobné, prípadne iné citlivé údaje, a následne vydierajú inštitúcie zverejnením týchto údajov za účelom získania finančného zisku.



Obr. 9 Techniky využívajúce sa v rámci útokov na akademické inštitúcie

2.3 Vytváranie odporúčaní z techník

Po úspešnom mapovaní dát do rámca MITRE ATT&CK je ďalším krokom vytváranie odporúčaní z techník. Nie je nutné vykonať tento krok, ale častokrát je to výhodné a celkovo to môže organizácii veľmi pomôcť v zabezpečení. Samotné vytváranie odporúčaní sa skladá z niekoľkých činností:

1. určenie prioritných techník,
2. prieskum, ako sa tieto techniky používajú,
3. prieskum ochrany voči týmto technikám,
4. prieskum schopností / obmedzení organizácie,
5. určenie kompromisov organizácie a
6. vytvorenie odporúčaní.

V prvom kroku je dôležité určiť si prioritné techniky, keďže samotný rámec poskytuje cez 260 techník. Otázkou môže byť, s akými dátami pracujeme, čo pokryjú nástroje, ktoré používame alebo prípadne čo robia protivníci. V prípade, že sa

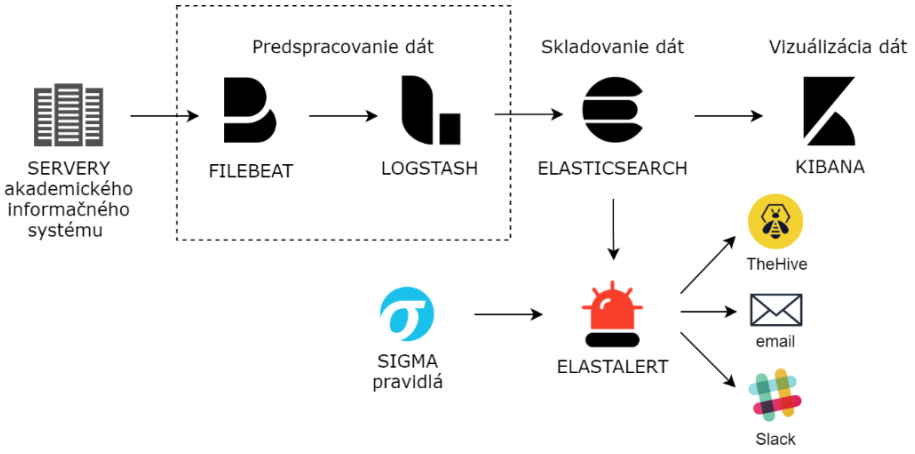
zameriame na otázku „Čo robia protivníci?“, hovoríme o modelovaní bezpečnostných hrozieb. Ďalej je potrebné preskúmať, ako sa tieto techniky používajú. Inými slovami, aké konkrétne postupy sa používajú pre danú techniku. Je veľmi dôležité, aby sa obranná reakcia prekrývala s aktivitou. Dôležité je preskúmať rôzne ochrany voči týmto technikám. V súčasnosti viacero zdrojov poskytuje defenzívne informácie indexované podľa rámca MITRE ATT&CK. Každá technika je v tomto rámci podrobne popísaná. Tiež nechýba spôsob, ako ju detegovať, prípadne ako jej zabrániť, alebo ju zmierniť. Netreba zabudnúť preskúmať, aké sú schopnosti, prípadne obmedzenia organizácie. Je potrebné zamerať sa na to, aké zdroje údajov, obrana, prípadne zmiernenie sú už zavedené, ktoré produkty sú už nasadené a podobne. Dôležité je určiť si postup organizácie k informačnej bezpečnosti, teda zvážiť výhody a nevýhody všetkých ochranných opatrení. Nakoniec je potrebné vytvoriť potrebné odporúčania, ktoré môžu byť technické, pre manažment, SOC a podobne.

3 Návrh a implementácia SIEM systému

V predchádzajúcich kapitolách sme sa venovali existujúcim implementáciám SIEM systémov a tiež si vysvetlili, čo predstavuje práca s MITRE ATT&CK rámcom. Po hlbšej analýze sme sa rozhodli, že pre naše účely využijeme práve riešenie s otvoreným kódom Elastic Stack, ktorý poskytuje mnoho rôznych nástrojov zadarmo. Poskytuje nám neobmedzenú sieťovú prevádzku, umožňuje nám spracovávať a vizualizovať dáta. Elastic Stack ponúka nástroje, ktoré sú plne škálovateľné podľa potrieb. Pomocou Beats nástrojov môžeme sledovať správanie serverov, na ktorých je nasadený akademický informačný systém.

3.1 Návrh riešenia

Na obrázku č. 10 sa nachádza schéma nášho systému. Z testovacieho a vývojového serveru akademického informačného systému zbierame záznamy pomocou nástroja Filebeat. Následne dáta spracúvame pomocou nástroja Logstash. Všetky dáta sú uchovávané v NoSQL databáze Elasticsearch. Pomocou vizualizačného nástroja Kibana vytvárame rôzne grafy. Dáta však nestačí len uchovávať, sledovaním je potrebné vytvárať pravidlá, na základe ktorých sme schopní detegovať rôzne hrozby. Z MITRE ATT&CK rámca sme vybrali niekoľko relevantných techník, ktoré sme následne odsimulovali a zaznamenali sme správanie súborov so záznamami. Odsledovali sme kľúčové správanie a na základe toho sme vytvorili pravidlá vo formáte Sigma. Následne pomocou nástroja ElastAlert zasielame upozornenia o podozrivej aktivite do platformy TheHive. Systém si bližšie popíšeme v ďalších podkapitolách.



Obr. 10 Schéma navrhnutého systému

Tiež bude potrebné zvážiť, nakoľko je ktorý atribút v daných záznamoch potrebný a dôležitý. Chceme, aby náš SIEM systém bol efektívny a škálovateľný pre rôzne akademické informačné systémy, nie len pre systém AiS2.

3.1.1 Akademický informačný systém AiS2

Akademický informačný systém AiS2 beží na troch rôznych serveroch – testovací, vývojový a produkčný. Všetky tri servery majú rovnakú architektúru. To znamená, že SIEM systém, ktorý bude implementovaný na testovacom serveri, je bez problémov možné nasadiť pre ďalšie dva servery. Architektúru akademického informačného systému AiS2 možno popísať ako klient-server architektúru. V rámci tejto architektúry klient odosiela požiadavku na webový server Apache2 prostredníctvom protokolov HTTP alebo HTTPS. Tento webový server požiadavku spracuje a pošle ju na server Tomcat, ktorý ju tiež spracuje a ďalej pošle Java servletom. Tie predstavujú jadro celého akademického informačného systému AiS2. Tieto servery generujú niekoľko druhov rôznych záznamov (logov), a to v súboroch access.log, error.log a ais.log.

V rámci akademického informačného systému evidujeme subsystémy, v rámci ktorých sa pracuje s osobnými informáciami. Konkrétne sa jedná o prijímacie konanie, evidenciu štúdia, ubytovanie v študentských domovoch, prepojenia na externé systémy a všeobecnejší pohľad na aplikačnú vrstvu a riadenie prístupu. Vo všeobecnosti aktíva delíme na primárne a sekundárne, pričom v akademickom informačnom systéme v rámci primárnych evidujeme obchodné procesy a informácie a medzi sekundárne radíme softvér, hardvér, siete, fyzické miesta a pracovníkov.

3.1.2 Analýza rizík

Analýzu rizík [57] je možné vykonávať v rôznych rozsahoch v závislosti od aktív, rozsahu známych bezpečnostných zraniteľností a predchádzajúcich incidentov zasahujúcich organizáciu. Môže byť kvalitatívna alebo kvantitatívna, prípadne kombinácia oboch, záleží na okolnostiach. Forma analýzy musí byť v súlade s vytvorenými kritériami hodnotenia rizík ako súčasť stanovenia kontextu.

Kvalitatívna analýza rizík využíva k popisu veľkosti potenciálnych dopadov (nízke, stredné, vysoké), pravdepodobnosť, že tieto dopady nastanú a škálu

kvalifikačných atribútov. Kvalitatívna analýza je ľahko pochopiteľná, ale na druhej strane je závislá na subjektívnom výbere škály. Kvalitatívne úrovne dopadu sú nízky (obmedzený negatívny vplyv na činnosť organizácie a jej aktíva), stredný (závažný vplyv na činnosť organizácie a jej aktíva) a vysoký (veľmi závažný až katastrofický vplyv na činnosť organizácie a jej aktíva). Kvalitatívne vyjadrenie pravdepodobnosti, že udalosť nastane je nulová, nízka, stredná a vysoká [57].

Kvantitatívna analýza rizík využíva číselné hodnoty pre dopady a pravdepodobnosť a využíva pri tom dáta z rôznych zdrojov. Závisí na presnosti a úplnosti číselných hodnôt a platnosti použitých modelov. Každé bezpečnostné riziko je potrebné ohodnotiť a následne určiť typ ošetrenia rizika. Riziko môžeme akceptovať, vyhnúť sa mu, limitovať ho alebo ho preniesť.

Na vytvorenie efektívneho SIEM systému bolo potrebné spraviť analýzu rizík akademického informačného systému. Samotná analýza rizík pozostáva z niekoľkých hlavných krokov:

1. Určenie všetkých aktív organizácie.
2. Určenie relevantných bezpečnostných hrozieb voči nájdeným aktívam.
3. Určenie bezpečnostných požiadaviek vyplývajúcich z právnych predpisov a technických noriem.
4. Určenie zraniteľností nájdených aktív.
5. Určenie existujúcich bezpečnostných opatrení.

Pri tvorbe zoznamu aktív je potrebné zohľadňovať aj osobu, ktorá je za dané aktívum zodpovedná (vlastník aktíva). Zodpovednosť je vo všeobecnosti nutné zohľadňovať aj pri stanovení aktív, pri analýze procesov s aktívami, ako aj pri riešení incidentov.

V rámci akademického informačného systému AiS2 bola vykonaná kvantitatívna analýza rizík. Boli identifikované aktíva, hrozby, zraniteľnosti a bezpečnostné riziká tohto informačného systému. Taktiež bola navrhnutá stratégia a plán ošetrenia rizík. Úlohou bolo zlepšiť informačnú bezpečnosť s cieľom priniesť výsledky v súlade s celkovou politikou organizácie.

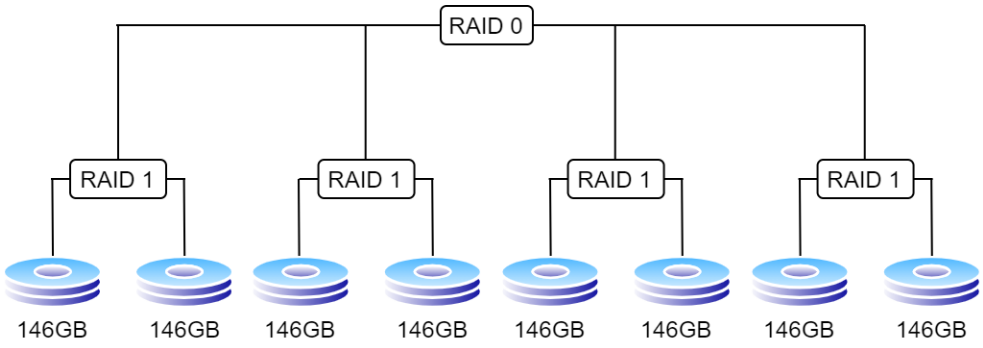
3.2 Implementácia

V tejto kapitole popisujeme implementačnú časť nášho systému. Zahŕňa návrh technickej infraštruktúry, inštaláciu nástrojov Elasticsearch, Logstash a Kibana, agenta Filebeat na servery akademického informačného systému a následne spracovanie záznamov, ktoré sú vo všeobecnosti v neštruktúrovanej forme. Zo záznamov sme vyextrahovali relevantné údaje, ktoré sme použili pri písaní detekčných pravidiel vo formáte Sigma. Pravidlá sme neskôr prekonvertovali do podoby čitateľnej pre ElastAlert, ktorý v prípade nájdenia zhody v záznamoch posiela upozornenia do platformy TheHive.

3.2.1 Návrh technickej infraštruktúry

Predtým ako sme mohli nainštalovať ELK a pridružené nástroje na server, bolo potrebné pripraviť hardvérové vybavenie. Na zostavenie infraštruktúry sme využili zariadenie HP ProLiant DL380p Gen8 Server. K dispozícii máme 64GB operačnej pamäte, pričom minimálne požiadavky pre ELK je 8GB operačnej pamäte. Ukázalo sa, že ELK s pridruženými nástrojmi na serveri na našej infraštruktúre priemerne využíva 8-9GB operačnej pamäte.

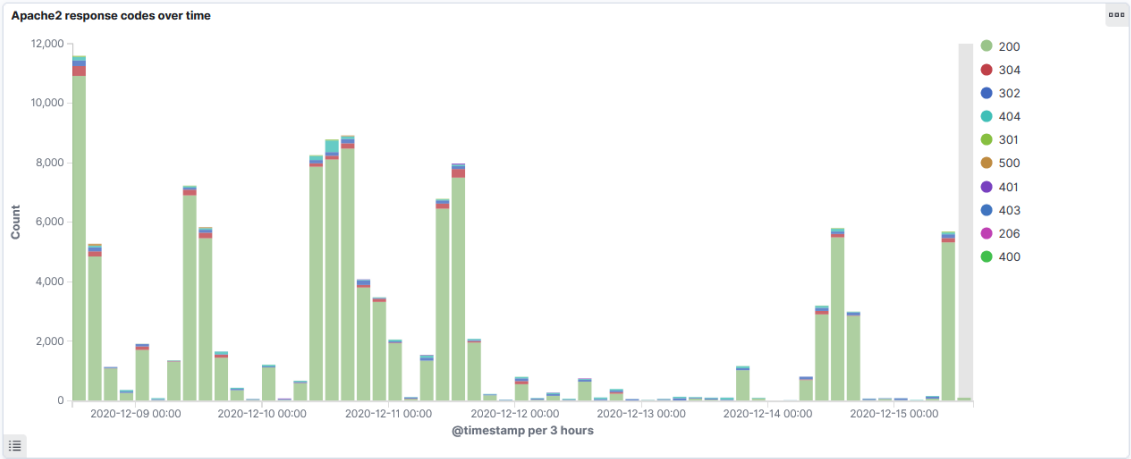
V rámci našej infraštruktúry máme 8 diskov o veľkosti 146GB, čo dokopy predstavuje 1184GB. Vzhľadom k tomu, že využívame RAID10, na zápis máme k dispozícii 546GB. Na server sme nainštalovali operačný systém Ubuntu 20.04.1 LTS. Denne do databázy Elasticserach zapíšeme v priemere štyri milióny záznamov. Na obrázku č. 11 môžeme vidieť zapojenie pevných diskov.



Obr. 11 Rozloženie pevných diskov

3.2.2 ELK

Na uvedenie SIEM systému do prevádzky bolo potrebné nainštalovať komponenty na server, ktorý nám sprístupnila univerzita. Nainštalovali sme nástroje Elasticsearch, Logstash a Kibana verzie 7.8.1. Ako sme už spomínali, Elasticsearch slúži na uchovávanie dát. Logstash využívame na ich predspracovanie, pričom bolo potrebné upraviť záznamy (logy) z rôznych zdrojov do čitateľného tvaru. Kibana slúži na vizualizáciu. Na obrázku č. 12 je možné vidieť príklad vizualizácie (typy odpovedí webového servera Apache2).



Obr. 12 Typy odpovedí webového servera Apache2 v závislosti od času

3.2.3 Filebeat

Filebeat [58] je nástroj slúžiaci na prepravu a centralizáciu logov. Filebeat, ktorý je nainštalovaný ako agent na serveroch, sleduje nami určené konkrétne súbory záznamov (logov) alebo adresáre s týmto záznamami. Následne zhromažďuje záznamy (logy), udržiava si informáciu o spracovaných záznamoch a preposiela ich na indexovanie do Logstashu.

Filebeat je nainštalovaný na testovacom a vývojovom serveri. Preposiela nám záznamy (logy) z webového servera Apache2, záznamy zo súboru audit.log, históriu príkazového riadka a tiež aplikačné záznamy (logy) akademického informačného systému AiS2. Tieto záznamy bolo potrebné spracovať tak, aby boli čitateľné. Na ich spracovanie sme využili nástroje grok [59] a kv [60], ktoré nám ponúka priamo Logstash. Nástroj grok slúži na spracovávanie neštruktúrovaných záznamov

do štruktúrovanej formy. Na druhej strane, nástroj kv pomáha automaticky spracovávať správy, ktoré sú v tvare kľúč=hodnota.

3.2.4 Záznamy (logy) z webového servera Apache2

Z prístupových záznamov (logov) uložených v súbore access.log webového servera vieme vyčítať viacero zaujímavých informácií (ukážka záznamu je zobrazená na obrázku č. 13). Nie len, že vieme tieto logy upraviť na čitateľné dáta, vieme na základe IP adresy obohatiť tieto údaje aj o geolokalizáciu zariadenia.

```
ais2-test.science.upjs.sk/... x.x.x.x - - [15/Dec/2020:12:41:37 +0100] "POST
url;sessionid=00000000000000000000000000000000 HTTP/1.1" 302 -
"https://ais2-test.science.upjs.sk/url" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:83.0) Gecko/20100101 Firefox/83.0"
```

Obr. 13 Ukážka záznamu zo súboru access.log

Zo záznamu, ktorého príklad je uvedený na obrázku č. 13, vieme vyextrahovať nasledujúce atribúty [61]:

- apache2.access.body_sent.bytes – počet odoslaných bytov,
- apache2.access.geoip.city_name – názov mesta,
- apache2.access.geoip.continent_code – kód kontinentu,
- apache2.access.geoip.country_code2 – kód krajiny,
- apache2.access.geoip.country_code3 – kód krajiny,
- apache2.access.geoip.country_name – názov krajiny,
- apache2.access.geoip.ip – IP adresa,
- apache2.access.geoip.latitude – zemepisná šírka,
- apache2.access.geoip.longitude – zemepisná dĺžka,
- apache2.access.geoip.postal_code – poštové smerovacie číslo,
- apache2.access.geoip.region_code – kód regiónu,
- apache2.access.geoip.region_name – názov regiónu,
- apache2.access.geoip.timezone – časová zóna,
- apache2.access.http_version – verzia http,

- apache2.access.method – metóda (GET, POST, ...)
- apache2.access.referrer – sprostredkovateľ http,
- apache2.access.remote_ip – IP adresa klienta,
- apache2.access.response_code – kód odpovede http,
- apache2.access.url – URL žiadosti http,
- apache2.access.user_agent.device – názov fyzického zariadenia,
- apache2.access.user_agent.name – názov agenta (Chrome, Firefox,...),
- apache2.access.user_agent.os – názov operačného systému,
- apache2.access.user_agent.os_name – názov operačného systému,
- apache2.access.user_agent.patch – oprava verzie agenta používateľa a
- apache2.access.user_name – používateľské meno použité pri základnej autentifikácii.

3.2.5 Záznamy (logy) zo súboru audit.log

Súbor audit.log obsahuje informácie o tom, kto vstúpil do systému a aké operácie vykonal za dané časové obdobie. Tieto záznamy (logy) sú užitočné na udržanie bezpečnosti a tiež na obnovenie stratených transakcií. Na obrázku č. 14 je ukážka záznamu (logu).

```
type=USER_LOGIN msg=audit(1618341187.792:30433629): pid=29591 uid=0
auid=4294967295 ses=4294967295 msg='op=login acct= "xxx"
exe="/usr/sbin/sshd" hostname=xxx addr=x.x.x.x terminal=ssh res=failed'
```

Obr. 14 Ukážka záznamu zo súboru audit.log

Zo záznamov uložených v súbore audit.log vieme extrahovať nasledujúce atribúty [62]:

- audit_acct – užívateľ, ktorý spustil proces,
- audit_addr – IP adresa klienta,
- audit_auid – audit ID,
- audit_counter - jedinečné ID záznamu,

- audit_epoch – časová pečiatka,
- audit_exe – cesta k súboru, ktorý bol použitý na vyvolanie analyzovaného procesu,
- audit_hostname – hosťovské meno klienta,
- audit_op – vykonávaná operácia,
- audit_pid – ID procesu,
- audit_res – výsledok operácie,
- audit_ses – ID relácie,
- audit_terminal – terminál, z ktorého bol analyzovaný proces,
- audit_type – typ záznamu a
- audit_uid – ID používateľa.

3.2.6 Záznamy (logy) zo súboru cmd.log

Záznamy zo súboru cmd.log boli vytvorené zo súboru .bash_history. Súbor .bash_history obsahuje históriu vykonávaných príkazov v systéme. Pre detekciu techník v zameraní na operačný systém je nutné, aby sme zaznamenávali príkazy spúšťané v systéme. Príklad záznamu zo súboru cmd.log je zobrazený na obrázku č. 15.

```
Apr 16 09:08:27 hostname user: SESSION = 00000, from_remote_host =
x.x.x.x, USER = user, PWD = /xxx, CMD = xxxxxxxxxxxxxxxxxxxx
```

Obr. 15 Ukážka záznamu zo súboru cmd.log

Z vyššie uvedeného záznamu vieme extrahovať nasledujúce atribúty:

- bash_hostname – hosťovské meno servera,
- bash_user – užívateľ, v ktorého kontexte sa vykonal príkaz,
- bash_session – ID relácie,
- bash_from_remote_host – IP adresa,
- bash_pwd – aktuálny adresár a
- bash_cmd – samotný príkaz.

Záznamy tohto typu je potrebné zbierať a analyzovať z dôvodu, že jeden zo spôsobov zahladenia stôp útočníka je vymazanie naposledy vykonávaných príkazov. My však tieto príkazy zasielame do databázy tesne po vykonaní, teda vieme zachytiť všetky vykonané príkazy, vrátane prípadného pokusu o vymazanie histórie.

3.2.7 Aplikačné záznamy (logy) AiS2

Aplikačné záznamy (logy) akademického informačného systému sú heterogénne. To reflektuje rôznorodosť jednotlivých modulov tohto systému. Všetky záznamy však majú tri rovnaké atribúty:

- ais_level – úroveň logu (INFO, DEBUG, WARN, ERROR),
- ais_logger – logger a
- ais_threadname – názov vlákna, ktorý v systéme AiS2 vykonával kód a urobil zápis do logu.

Prvým typom aplikačných záznamov, ktorými sa zaoberáme sú tie, ktoré vypovedajú o úspešnom alebo neúspešnom prihlásení do systému. Na obrázku č. 16 môžeme vidieť ako vyzerá jeden z viacerých druhov aplikačných záznamov (logov) akademického informačného systému.

```
2021-04-14 12:48:27,624 INFO [threadname xxx] Auth -
LoginAction:IP=x.x.x.x;session.id=00000000000000000000000000000000;user=xx
x;remoteUser=xxx;locale=SK;loginResult=fail
```

Obr. 16 Ukážka aplikačného záznamu AiS2 (autentifikácia)

Vyššie uvedené záznamy (logy) okrem ais_level, ais_logger a ais_threadname navyše obsahujú informácie ako:

- ais_action – vykonávaná akcia,
- ais_action_result – výsledok akcie,
- ais_clientip – IP adresa klienta,
- ais_locale – jazyk,

- ais_session_id – ID relácie
- ais_submsg – zvyšné údaje v rámci logu,
- ais_username – meno používateľa, pre ktorého sa vykonáva aplikačný kód a
- ais_username2 – meno prihláseného používateľa.

Ďalším druhom aplikačných logov AiS2 sú také, ktoré evidujú prístupy k jednotlivým modulom akademického informačného systému. Príklad týchto záznamov (logov) je uvedený na obrázku č. 17.

2021-04-14 18:05:37,789 INFO [wuieXxxxxxxxxx xxx] a.g.v.s.VSxxxxxApp - {"userLogin":"xxx","userRoles":"1,2,3,4,5","appCode":"VSxxxxx","appRoles":"3,4,5"}

Obr. 17 Ukážka aplikačného záznamu AiS2 (prístup k aplikáciám)

Záznamy, ktoré evidujú prístupy k jednotlivým modulom AiS2, okrem základných polí obsahujú ďalšie, ktoré nám poskytujú doplňujúce informácie:

- ais_appCode – kód spustenej aplikácie,
- ais_appRoles – role, ktoré môžu pristúpiť k aplikácii,
- ais_userLogin – meno prihláseného používateľa,
- ais_userRoles – role prihláseného používateľa a
- ais_userName – meno používateľa, pre ktorého sa vykonáva aplikačný kód.

3.2.8 Pravidlá detekcie písané vo formáte Sigma

Pravidlá, ktoré sme implementovali do nástroja ElastAlert, sú najprv písané vo formáte Sigma a následne prekonvertované, aby bol ElastAlert schopný ich spracovávať. Sigma [63] je všeobecný a otvorený formát podpisu, ktorý umožňuje jednoduchý opis relevantných logov udalostí. Formát pravidla je flexibilný, ľahko sa píše a je použiteľný pre akýkoľvek súbor s logmi. Hlavným účelom je poskytnúť štruktúrovanú formu, v ktorej môžu vedci alebo analytici opísať nimi navrhnuté

detekčné metódy a umožniť ich zdieľanie s ostatnými. Štruktúru pravidiel písaných vo formáte Sigma je možné vidieť na obrázku č. 18.

```
title: Test title
status: experimental
description: Test description
author: Eva Markova
date: 2021/04/20
modified: 2021/04/21
logsource:
    category: web
detection:
    selection:
        test_field:
            - "value1"
            - "value2"
    timeframe: 600s
    condition: selection
fields:
    - test_field
level: high
```

Obr. 18 Štruktúra pravidiel písaných vo formáte Sigma

3.2.9 ElastAlert

ElastAlert [64] je jednoduchý rámec na upozorňovanie na anomálie alebo rôzne zaujímavé činnosti získané z údajov v databáze Elasticsearch. Databáza je pravidelne dopytovaná a údaje sú odovzdávané pravidlám, ktoré určujú, kedy sa nájde zhoda. Ak dôjde k zhode, vygeneruje sa jedno alebo viac varovaní, ktoré na základe zhody vykonajú príslušné kroky.

ElastAlert obsahuje niekoľko typov pravidiel so spoločnými paradigmami monitorovania, napríklad frekvenčné pravidlá, pravidlá typu čierna alebo biela listina a podobne. V súčasnosti je ElastAlert schopný odosielať varovania cez rôzne rozhrania ako JIRA [65], email, OpsGenie [66], SNS [67], Slack [68], TheHive [69] a podobne. Ďalšie typy pravidiel sa dajú importovať alebo si môžeme napísať vlastné.

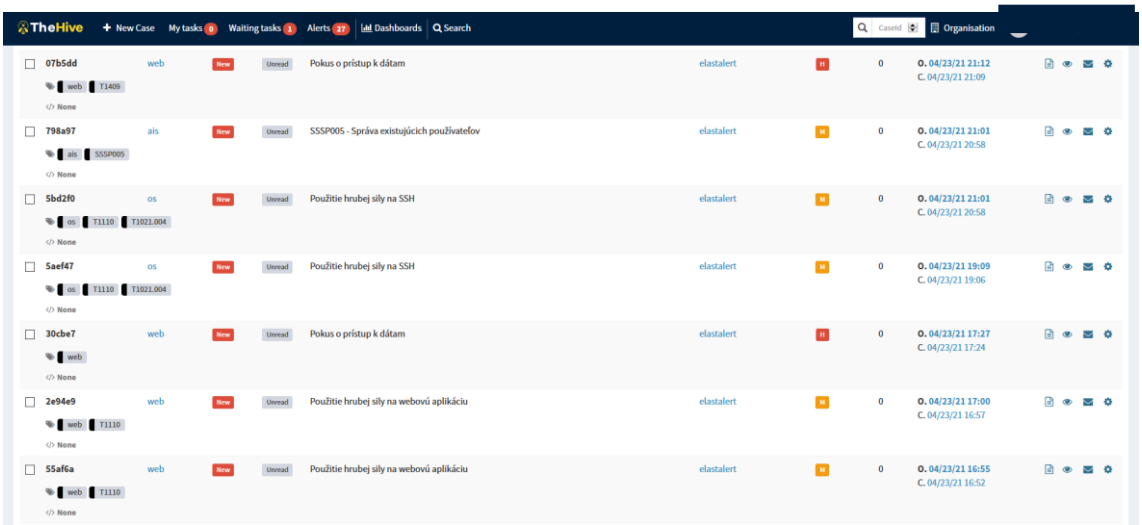
Má tri hlavné komponenty a to typy pravidiel, varovania a vylepšenia. Typ pravidla je zodpovedný za spracovanie údajov vrátených z databázy Elasticsearch. Inicializuje sa konfiguráciou pravidla, odovzdanými údajmi, ktoré sa vracajú z dopytu na Elasticsearch s filtrami pravidla, a na základe týchto údajov sa vytvoria zhody. Varovania sú zodpovedné za prijatie opatrení na základe zhody. Zhoda môže obsahovať ľubovoľné údaje pridané typom pravidla. Vylepšenia sú spôsoby, ako zachytiť výstrahu a nejakým

spôsobom ju upraviť alebo vylepšiť. Štruktúru pravidiel písaných pre ElastAlert je možné vidieť na obrázku č. 19.

```
name: test_title_0
description: Test description
index: winlogbeat-*
priority: 2
realert:
  minutes: 0
filter:
- query_string:
    query: test_field:("value1" OR "value2")
type: any
alert:
- debug
```

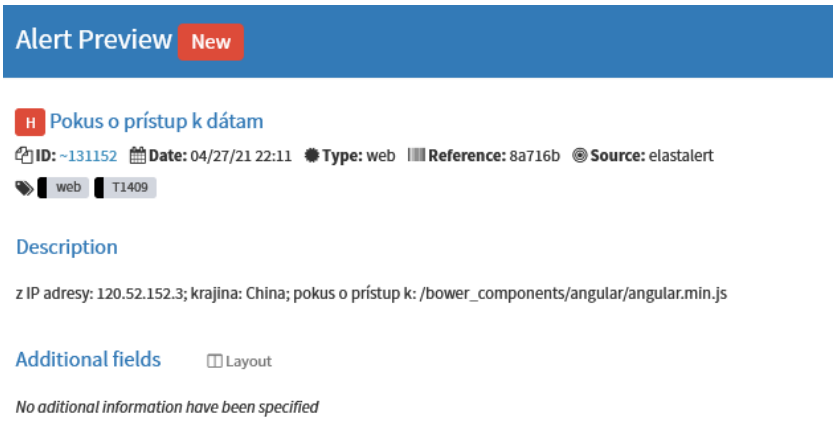
Obr. 19 Štruktúra pravidiel pre ElastAlert

V našom SIEM systéme ElastAlert slúži práve na upozorňovanie správcov o podozrivej aktivite na serveroch akademického informačného systému. ElastAlert po vyhodnotení pravidla na detekciu posiela upozornenie tímu CSIRT-UPJS do platformy TheHive [69], ktorá slúži na riešenie bezpečnostných incidentov. Prepojenie medzi platformou TheHive a SIEM systémom bolo vytvorené vytvorením používateľa elastalert v platforme, následným vytvorením API kľúča a použitím na prepojenie v pravidlách. Na obrázku č. 20 môžeme vidieť zoznam upozornení v tejto platforme.



Obr. 20 Upozornenia zo SIEM systému v platforme TheHive

Na obrázku č. 21 môžeme vidieť príklad upozornenia ohľadom pokusu prístupu k dátam. Môžeme vidieť, že potenciálny útočník sa snažil pristúpiť k údajom z IP adresy 120.52.152.3, pričom prislúchajúca krajina pre túto IP adresu je Čína. Upozornenie má značky web, čo označuje, že sa jedná o hrozbu na úrovni webovej aplikácie a T1409, čo prislúcha prepojenej technike z MITRE ATT&CK rámca. Potenciálny útočník sa snažil pristúpiť k „/bower_components/angular/angular.min.js“.



Obr. 21 Príklad upozornenia v platforme TheHive

4 Detekcia hrozieb pre AiS2

Na to, aby sme vytvorili relevantné pravidlá, bolo nutné, aby sme vybrali techniky z MITRE ATT&CK rámca, ktoré je nutné sledovať. Vzhľadom k analýze bezpečnostných rizík spätých s akademickým informačným systémom sme došli k záveru, že je dôležité sledovať APT skupiny, ktoré sa svojimi útokmi zamerali na akademické a vzdelávacie inštitúcie. Takouto skupinou je napríklad menuPass (APT10). Vzhľadom k tomu, že akademický informačný systém beží na operačnom systéme Linux, taktiky, techniky a postupy, ktoré je nutné detegovať, sa opäť zúžili na menšiu množinu. Delíme ich na tri skupiny:

- TTP v rámci bezpečnostných hrozieb na úrovni operačného systému,
- na úrovni webovej aplikácie a
- na úrovni prihláseného používateľa.

Techniky samé o sebe nemusia byť podozrivé, avšak v nadväznosti na seba môžu byť vnímané ako narušenie niektorých z hlavných bodov bezpečnosti. Napríklad spustenie príkazu *whoami* v nás môže evokovať podozrivé správanie, pretože na serveri akademického informačného systému nie je potrebné tento príkaz vykonávať. Používateľ, ktorý je legitímny, nepotrebuje zisťovať pod akým účtom je prihlásený.

Kybernetické hrozby sa neustále vyvíjajú s novšími taktikami, technikami a postupmi prispôsobenými na základe zraniteľností cieľovej organizácie. Analytici v rámci bezpečnostného operačného centra (SOC) musia vykonávať nepretržité monitorovanie indikátorov kompromitácie, aby mohli efektívne detegovať a reagovať na vyvíjajúce sa kybernetické hrozby. Indikátormi kompromitácie sú stopy, resp. artefakty získaných údajov, ktoré sa nachádzajú v počítačovej sieti alebo operačnom systéme organizácie, a ktoré naznačujú potenciálnu škodlivú činnosť. Sú to informácie o podozrivých alebo škodlivých činnostiach, ktoré sa zhromažďujú z rôznych bezpečnostných zariadení v sieťovej infraštruktúre [70].

4.1 Bezpečnostné hrozby na úrovni operačného systému

Bezpečnostné hrozby na úrovni operačného systému sú väčšinou zamerané na vykonávané techniky v rámci operačného systému. Súvisia s vytváraním účtov

v systéme, objavovaním informácií o systéme, alebo s použitím hrubej sily na pripojenie sa cez protokol SSH. Keďže akademický informačný systém AiS2 je prevádzkovaný na distribúcii operačného systému Linux, zameriavame sa v rámci analýzy len na tento operačný systém. Ak v nasledujúcom texte uvedieme operačný systém, myslíme tým operačný systém Linux.

4.1.1 Vytvorenie účtu v lokálnom systéme

Medzi dôležitú činnosť, ktorú je potrebné detegovať patrí technika **T1136** – Create Account. Ide o vytvorenie účtu v rámci lokálneho operačného systému. Útočníci môžu vytvárať účty na udržanie prístupu v cieľovom systéme. S dostatočnými oprávneniami môžu útočníci vytvorenie takéhoto účtu využiť na získanie prístupu k systému, čo nevyžaduje udržiavanie vzdialeného prístupu k systému.

4.1.2 Objavenie rôznych informácií o systéme

K technikám, ktoré využívajú útočníci v rámci hrozieb na úrovni operačného systému, zaraďujeme:

- **T1016** – System Network Configuration Discovery – získavanie podrobností o konfigurácii siete a nastaveniach systémov, ku ktorým pristupujú. V AiS2 sa môže jednať napríklad o vykonanie príkazu *ifconfig*.
- **T1018** – Remote System Discovery – získavanie zoznamu ďalších systémov podľa IP adresy, názvu hostiteľa alebo iného logického identifikátora v sieti. Môže sa jednať o vykonanie príkazu *cat /etc/hosts*.
- **T1033** – System Owner/User Discovery – identifikácia primárneho používateľa, alebo skupiny používateľov, ktorí bežne používajú systém. V AiS2 je možné napríklad vykonať príkaz *whoami*.
- **T1049** – System Network Connections Discovery – získanie zoznamu sieťových pripojení k alebo z ohrozeného systému. Túto informáciu vieme získať vykonaním príkazu *lsof*.
- **T1057** – Process Discovery – získavanie informácií o spustených procesoch v systéme. V AiS2 môže ísť o vykonanie príkazu *ps -aux*.

- **T1069.001** – Permission Groups Discovery: Local Groups – objavenie lokálnych skupín v systéme a ich oprávnení. Vykonaním príkazu *groups* vieme získať tieto informácie.
- **T1069.002** – Permission Groups Discovery: Domain Groups – objavenie doménových skupín v systéme a ich oprávnení. V AiS2 môže dôjsť k odhaleniu týchto informácií pomocou príkazu *ldapsearch*.
- **T1082** – System Information Discovery – získanie podrobných informácií o operačnom systéme, hardvéri a podobne. Vykonaním príkazu *uname* vieme získať napríklad názov operačného systému.
- **T1083** – File and Directory Discovery – vyhľadávanie a prehľadávanie súborov a adresárov v systéme. Pomocou príkazu *tree* alebo *dir* vieme zistiť obsah adresárov.
- **T1087.001** – Account Discovery: Local Account – objavenie lokálnych účtov v systéme. Vykonaním príkazu *cat /etc/passwd* vieme odhaliť lokálne účty v systéme.
- **T1087.002** – Account Discovery: Domain Account – objavenie doménových účtov v systéme. V AiS2 môže dôjsť k odhaleniu týchto informácií pomocou príkazu *ldapsearch*.
- **T1201** – Password Policy Discovery – získanie prístupu k podrobným informáciám o politike hesiel používanej v sieti. Na serveroch AiS2 vieme túto informáciu získať pomocou príkazu *pwpolicy*.

V princípe ide o získanie základných informácií o operačnom systéme ako napríklad objavenie účtov, zistenie vlastníka systému, zistenie oprávnení skupín a podobne. Tieto aktivity však môže vykonávať aj administrátor systému, preto sme vygenerovaným varovaniam, ktoré poukazujú na vykonanie takejto činnosti, určili strednú závažnosť. Ak však tieto príkazy nevykonáva administrátor, môže sa jednať o prvotný kontakt útočníka so systémom. Ukážka pravidla na zistenie procesov v systéme je na obrázku č. 22.

```yaml
title: Process Discovery
status: experimental
description: T1057
author: Eva Markova
date: 2021/04/10
logsource:
    category: os
detection:
    selection:
        bash_cmd:
            - "*/proc*"
            - "*ps*"
    condition: selection
fields:
   - bash_from_remote_host
   - bash_username
level: medium
```

Obr. 22 Ukážka pravidla na detekciu hrozieb na úrovni OS

Na obrázku č. 23 môžeme vidieť ukážku prekonvertovaného pravidla do čitateľnej podoby pre ElastAlert.

```yaml
filter:
- query:
    query_string:
      query: bash_cmd.keyword:(*\/proc* OR *ps*)
index: filebeat-*
name: Process-Discovery_0
priority: 2
realert:
  minutes: 1
type: any

alert: hivealerter
```

Obr. 23 Ukážka prekonvertovaného pravidla na detekciu hrozieb na úrovni OS

4.1.3 Detekcia útoku na prihlasovacie údaje služby SSH založené na použití tzv. hrubej sily

Útočník môže použiť rôzne typy útokov na prelomenie hesla v akademickom informačnom systéme. Medzi nich patria napríklad slovníkový útok alebo použitie tzv. hrubej sily na prihlasovacie údaje.

Slovníkový útok je pokus o prelomenie hesla pomocou hádania. Útočníci môžu hádať heslá pomocou manuálneho alebo automatizovaného prístupu. Tento útok sa

pokúša spojiť najbežnejšie sa vyskytujúce slová alebo bežne používané slová v každodennom živote.

Pri prelomení hesla hrubou silou sa vykonáva veľké množstvo odhadov s cieľom úspešne získať heslo cieľového systému. Zahŕňa to kontrolu všetkých kombinácií znakov, kým sa nenájde správne heslo. Útoky hrubou silou sú najvhodnejšie na získavanie hesiel, ktoré sú krátke alebo nie príliš zložité. Útoky hrubou silou sú náročné na čas a zdroje.

Dôležitou činnosťou, ktorú je potrebné detegovať, je pokus o prienik do systému pomocou protokolu SSH. Túto hrozbu sme prepojili s MITRE ATT&CK rámcom pomocou techník **T1110** – Brute Force a **T1021.004** – Remote Services: SSH.

Na obrázku č. 24 môžeme vidieť príklad pravidla na detekciu útoku na prihlasovacie údaje v službe SSH založené na použití tzv. hrubej sily. Ide o typ útoku, pri ktorom sa skúšajú rôzne kombinácie prihlasovacích údajov.

```
title: Brute Force ssh
status: experimental
description: T1110 and T1021-004
author: Eva Markova
date: 2019/10/25
modified: 2020/12/15
logsource:
    category: authentication
detection:
    selection:
        audit_res: failed
        audit_exe: sshd
    timeframe: 600s
    condition: selection | count(audit_res) by audit_addr > 30
fields:
    - audit_addr
level: medium
```

Obr. 24 Pravidlo na detekciu útoku na prihlasovacie údaje služby SSH

Na detekciu útoku na prihlasovacie údaje v službe SSH založené na použití tzv. hrubej sily je potrebné sledovať dva atribúty – audit_addr, čo je IP adresa klienta, ktorý sa prihlasuje a audit_res, čo je výsledok akcie (úspešné alebo neúspešné prihlásenie). V prípade, že za 600 sekúnd je z jednej IP adresy viac ako 30 neúspešných pokusov o prihlásenie, môžeme povedať, že ide o útok na prihlasovacie údaje založené na použití tzv. hrubej sily. Toto pravidlo je následne nutné prekonvertovať, aby bolo

čitateľné pre ElastAlert. To sa deje príkazom *python3 tools/sigmac rules/my_rules/bruteforce.yml -t elastalert --config backend_config*. Na obrázku č. 23 môžeme vidieť ako tento príkaz prekonvertoval pravidlo. V prípade, že je podmienka na detekciu hrubej sily splnená, ElastAlert odosiela varovanie do platformy TheHive.

```
name: brute_force_ssh_0
description: T1110 and T1021-004
index: filebeat-*
priority: 3
realert:
  minutes: 0
filter:
- query_string:
    query: (audit_exe:"sshd" AND audit_res:"failed")
query_key: audit_addr
type: metric_aggregation
buffer_time:
  seconds: 600
doc_type: doc
metric_agg_type: cardinality
metric_agg_key: audit_res
max_threshold: 30
alert:
- debug
```

Obr. 25 Prekonvertované pravidlo na detekciu útoku na prihlasovacie údaje služby SSH

V rámci tejto práce sme využili aj Sigma pravidlá z verejného repozitára [63] zamerané na službu auditd. Sme schopní detegovať nasledujúce techniky:

- **T1036.003** – Masquerading: Rename System Utilities – premenovanie legitímnych systémových nástrojov pre vyhnutie sa bezpečnostným mechanizmom.
- **T1040** – Network Sniffing – odpočúvanie sieťového prenosu, vrátane zachytenia informácií o prostredí.
- **T1059.004** – Command and Scripting Interpreter: Unix Shell – zneužitie unixového príkazového riadka na vykonávanie príkazov.
- **T1071** – Application Layer Protocol – komunikácia pomocou protokolov aplikačnej vrstvy.
- **T1095** – Non-Application Layer Protocol – použitie protokolov inej ako aplikačnej vrstvy na komunikáciu.
- **T1132** – Data Encoding – šifrovanie údajov kvôli sťaženiu detekcie.

- **T1505.003** – Server Software Component: Web Shell – vytváranie zadných vrátok pomocou webového príkazového riadka (shellu) na získanie stabilného prístupu k systému.
- **T1546.004** – Event Triggered Execution: .bash_profile and .bashrc – zabezpečenie perzistencie pomocou vykonávania škodlivých príkazov.
- **T1560.001** – Archive Collected Data: Archive via Utility – komprimácia alebo šifrovanie údajov pred samotnou exfiltráciou.
- **T1562.006** – Impair Defenses: Indicator Blocking – blokovanie zhromažďovania a analyzovania indikátorov alebo udalostí.
- **T1574.006** – Hijack Execution Flow: LD_PRELOAD – vykonávanie vlastných škodlivých aktivít pomocou únosu dynamického prepájača na načítanie knižníc.

Keďže APT skupiny vo všeobecnosti tieto techniky využívajú vo svojich kampaniach (nie len na akademické inštitúcie), určite je vhodné bezpečnostné hrozby využívajúce tieto techniky detegovať. Nebolo nutné vytvárať nové pravidlá, keďže tieto sa už nachádzali vo verejnom repozitári [63]. Avšak bolo potrebné upraviť názvy atribútov, keďže v našom SIEM systéme evidujeme atribúty zo súboru audit.log pod názvami „audit_názov“ a tieto z verejného repozitára obsahovali názvy bez prefixu „audit_“.

4.2 Bezpečnostné hrozby na úrovni webovej aplikácie

Hrozby na úrovni webovej aplikácie sme vybrali podľa OWASP Top Ten [71], čo predstavuje zoznam najdôležitejších bezpečnostných rizík pre webové aplikácie. Útočník pri útokoch tohto typu zneužíva zraniteľnosti vo webových aplikáciách. Útoky sú útočníkmi vykonávané automatizovane napríklad pomocou nástroja burpsuite alebo curl.

4.2.1 Cross-site Scripting (XSS)

Útok typu Cross-site Scripting (XSS) sme s MITRE ATT&CK rámcom prepojili pomocou techniky **T1189** – Drive-by Compromise, ktorá hovorí o tom, že útočníci

môžu získať prístup do systému prostredníctvom používateľa, ktorý navštívi webovú stránku počas bežného prehliadania.

Cross-site Scripting útoky (XSS alebo CSS) využívajú zraniteľné miesta v dynamicky generovaných webových stránkach, ktoré umožňujú útočníkom vkladať skript na strane klienta do webových stránok zobrazených inými používateľmi. Nastáva, keď sú neplatné vstupné údaje zahrnuté v dynamickom obsahu, ktorý sa odošle do webového prehliadača používateľa na vykreslenie. Útočníci vložia (injektujú) škodlivý JavaScript, VBScript, ActiveX, HTML alebo Flash na spustenie v systéme tak, že ho skryjú pred legitímnymi požiadavkami. Tieto škodlivé skripty môžu dokonca prepísať obsah webových stránok HTML. Bežné XSS útoky využívajú HTML tagy <script>, </script>, <img>, <input> a <body>. Na hľadanie XSS útokov využívame takéto regulárne výrazy [72]:

- /((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>)/ix – na detekciu jednoduchého XSS útoku,
- /((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+((\%3E)|>)/I – na detekciu útoku použitím HTML tagu <img>.

Pravidlo na detekciu XSS útokov je vidieť na obrázku č. 26.

```
title: XSS scan
status: experimental
description: Detects XSS
author: Eva Markova
date: 2019/10/25
modified:
logsource:
    category: web
detection:
    selection:
        apache2.access.url|contains:
            - "%3C%2F*%3E"
            - "%3C%2F*>"
            - "%3C/*%3E"
            - "%3C/*>"
            - "<%2F*%3E"
            - "<%2F*>"
            - "</*%3E"
            - "</*>"
    timeframe: 600s
    condition: selection
fields:
    - apache2.access.remote_ip
level: high
```

Obr. 26 Pravidlo na detekciu XSS útokov

V rámci pravidla sa zaoberáme hexadecimálnymi zápismi znakov „<“, „/“, „>“, keďže útočníci častokrát využívajú obfuskáciu na obídenie rôznych bezpečnostných politík. Na obrázku č. 27 je vidieť prekonvertované pravidlo.

```
filter:
- query:
    query_string:
      query: apache2.access.url.keyword:(*%3C%2F*%3E*
      OR *%3C%2F*>* OR *%3C\/*%3E* OR *%3C\/*>* OR
      *<%2F*%3E* OR *<%2F*>* OR *<\>
index: filebeat-*
name: XSS-scan_0
priority: 2
realert:
  minutes: 1
type: any

alert: hivealerter
```

Obr. 27 Prekonvertované pravidlo na detekciu XSS útokov

4.2.2 Path Traversal

Útok typu Path Traversal sme prepojili s rámcom MITRE ATT&CK pomocou techniky **T1083** – File and Directory Discovery. Technika hovorí o tom, že útočník sa snaží prehľadávať súborový systém.

Keďže ide o operačný systém Linux, často sa útočník snaží získať prístup k súboru „/etc/passwd“, v ktorom sa nachádza zoznam používateľov. Tento typ útoku využíva nedostatočné overovanie bezpečnosti alebo neprimeranú sanitáciu používateľom zadaných mien súborov, aby sa znaky popisujúce prechod do nadradeného adresára presunuli do API súborov. Útok tohto typu je schopný odhaliť adresárovú štruktúru webovej aplikácie. Pri útokoch týkajúcich sa prechodu adresárom je nutné pozrieť súbory so záznamami (logmi) pre webový server a hľadať v nich špeciálne znaky ako napríklad ../../../../etc/ alebo ..\..\..\etc\passwd. Na detekciu útokov typu path traversal využívame regulárny výraz [72]:

- /(\.|(%|%25)2E)(\.|(%|%25)2E)(\/|(%|%25)2F|\\|(%|%25)5C)/ix

Na obrázku č. 28 vidieť časť pravidla pre detekciu útokov takéhoto typu. Útočníci kvôli obchádzaniu bezpečnostných politík častokrát využívajú klasické alebo dvojité šifrovanie znakov. Po prvom šifrovaní znak „/“ predstavuje „%2F“. Po druhom šifrovaní znak „/“ predstavuje „%252F“, preto sme sa snažili zachytiť všetky prípady, ktoré môžu nastať.

```
title: Path traversal
status: experimental
author: Eva Markova
date: 2019/10/25
modified:
logsource:
    category: web
detection:
    selection:
        apache2.access.url|contains:
                - "..\/"
                - ".%2E\/"
                - "%2E.\/"
                - "%2E%2E\/"
                - ".%2E%2F"
                - "%2E.%2F"
                - "%2E%2E%2F"
                - ".%2E%252F"
                - "%2E.%252F"
                - "%2E%2E%252F"
                - "..\\"
                - ".%2E\\"
```

Obr. 28 Pravidlo na detekciu útoku typu path traversal

Na obrázku č. 29 je vidieť pravidlo prekonvertované pre ElastAlert.

```
filter:
- query:
    query_string:
      query: apache2.access.url.keyword:(*..\/*
      OR *.%2E\/* OR *%2E.\/* OR *%2E%2E\/* OR
      *.%2E%2F* OR *%2E.%2F* OR *%2E%2E%2F* OR
      *.%2E%252F* OR *%2E.%252F* OR *%2E%2E%252F*
      OR *..\\* OR *.%2E\\* OR *%2E%2E\\* OR *..%25*
      OR *.%2E%25* OR *%2E%2E%25* OR *..%255C* OR
      *.%2E%255C* OR *%2E%2E%255C*)
index: filebeat-*
name: Path-traversal_0
priority: 2
realert:
  minutes: 0
type: any

alert: hivealerter
```

Obr. 29 Prekonvertované pravidlo na detekciu útoku typu path traversal

4.2.3 Útoky na prihlasovacie údaje

Útoky na prihlasovacie údaje sme vo všeobecnosti prepojili s technikou **T1110** – Brute Force. Táto technika v princípe pokrýva rôzne typy útokov na prihlasovacie údaje.

Útoky na prihlasovacie údaje, najmä heslá, sa vykonávajú s cieľom získať neoprávnený prístup alebo získať kontrolu nad cieľovým počítačovým systémom. Útočníci ich uskutočňujú napríklad za účelom získania prístupu k cieľovému systému, získania oprávnení v systéme, alebo za účelom odcudzenia rôznych citlivých údajov. Spravidla sa heslá používajú na identifikáciu používateľa (preukázanie svojej totožnosti) a následne overenie (autentifikáciu) v systéme. Útočníci sa snažia získať tieto prístupové údaje rôznymi technikami a autentifikovať sa v systéme, aby mohli využívať oprávnenia, ktoré má bežný používateľ. Vykonávajú rôzne techniky na získanie hesiel a získanie prístupu k cieľovému systému. Útočník môže použiť rôzne typy útokov na prelomenie hesla v akademickom informačnom systéme. Bližší popis k týmto typom útokov sa nachádza v kapitole 4.1.3. Na obrázku č. 30 je vidieť pravidlo na detekciu útoku na prelomenie prihlasovacích údajov v rámci webovej aplikácie.

```
title: Brute Force web
status: experimental
author: Eva Markova
date: 2020/12/10
logsource:
    category: web
detection:
    selection:
        ais_action_result: fail
        ais_action: LoginAction
    timeframe: 600s
    condition: selection | count(ais_action_result) by ais_clientip > 30
fields:
    - ais_clientip
    - ais_username2
    - ais_subject_id
level: medium
```

Obr. 30 Pravidlo na detekciu útoku na prihlasovacie údaje v rámci webovej aplikácie

V rámci tohto pravidla sledujeme či počet neúspešných prihlásení je pre jednu konkrétnu IP adresu väčší ako 30. Ak áno, evidujeme túto aktivitu ako pokus o útok

na prihlasovacie údaje použitím tzv. hrubej sily. Na obrázku č. 31 je vidieť prekonvertované pravidlo pre ElastAlert.

```
filter:
- query:
    query_string:
      query: (ais_action_result:"fail" AND ais_action:"LoginAction")
query_key: ais_clientip
index: filebeat-*
name: Brute-Force-web0
priority: 3
realert:
  minutes: 1
type: frequency
num_events: 20
timeframe:
  minutes: 2

alert: hivealerter
```

Obr. 31 Prekonvertované pravidlo na detekciu útoku na prihlasovacie údaje v rámci webovej aplikácie

4.2.4 Pokus o neoprávnený prístup k údajom

Z pohľadu informačných systémov, v ktorých sa uchovávajú osobné údaje, resp. iné citlivé údaje, je dôležité sledovať aktivity používateľov, ktoré by mohli viesť k neoprávnenému prístupu k údajom, a teda narušenie dôvernosti. V rámci prístupových záznamov webového servera Apache2 sledujeme, či za krátky časový okamih neevidujeme viacero prístupov k URL odkazom, ktoré vracajú odpoveď servera s označením 404 (stránka nenájdená, resp. súbor nenájdený). Takáto aktivita môže vzbudzovať dojem, že sa potenciálny útočník snaží pristúpiť k údajom, ktoré by mimo informačný systém nemali byť dostupné. Na obrázku č. 32 je možné vidieť pravidlo na detekciu pokusu o neoprávnený prístup k údajom.

```
title: Access to Data
status: experimental
description: Detects response codes 404
author: Eva Markova
date: 2019/10/25
modified: 2020/12/15
logsource:
    category: web
detection:
    selection:
        apache2.access.response_code: 404
    timeframe: 600s
    condition: selection | count(apache2.access.response_code)
                           by apache2.access.remote_ip > 30
fields:
    - apache2.access.remote_ip
level: medium
```

Obr. 32 Pravidlo na detekciu pokusu o neoprávnený prístup k údajom

Pri tejto činnosti sledujeme či je kód odpovede 404 a agregujeme tieto kódy vzhľadom na IP adresu. Pravidlo prekonvertované do podoby čitateľnej pre ElastAlert je vidieť na obrázku č. 33.

```
name: access_to_data_0
description: Detects response codes 404
type: frequency
index: filebeat-*
num_events: 20
timeframe:
  minutes: 2
priority: 3
realert:
  minutes: 1
filter:
- query_string:
    query: apache2.access.response_code:"404"
query_key: apache2.access.remote_ip
```

Obr. 33 Prekonvertované pravidlo na detekciu pokusu o neoprávnený prístup k údajom

4.2.5 Neuskutočniteľná cesta

V rámci akademického informačného systému sme sa rozhodli sledovať tiež aktivitu, ktorá môže byť vyhodnotená ako neuskutočniteľná cesta. To znamená, že sme sa zamerali na pokusy o prihlásenie sa do akademického informačného systému z rôznych krajín za krátke časové obdobie. Takúto aktivitu môže spôsobiť použitie

VPN, avšak v tých horších prípadoch sa môže jednať o kompromitáciu účtu. Na obrázku č. 34 je pravidlo pre detekciu takejto aktivity na účte.

```
title: Impossible Travel Activity
status: experimental
author: Eva Markova
date: 2021/04/20
logsource:
    category: ais
detection:
    selection:
        ais_action: "LoginAction"
    condition: selection | count(ais_clientip_geoip_country_name)
                           by ais_username > 2
fields:
    - ais_
level: medium
```

Obr. 34 Pravidlo na detekciu neuskutočniteľnej cesty

V rámci tohto pravidla sledujeme, či sa používateľ za krátke časové obdobie nepokúšal prihlásiť aspoň z troch rôznych krajín. Na obrázku č. 35 vidieť prekonvertované pravidlo.

```
filter:
- query:
    query_string:
      query: ais_action:"LoginAction"
index: filebeat-*
max_threshold: 2
metric_agg_key: ais_clientip_geoip.country_name.keyword
metric_agg_type: cardinality
name: Impossible-Travel-Activity_0
priority: 3
query_key: ais_username.keyword
realert:
  minutes: 1
type: metric_aggregation

alert: hivealerter
```

Obr. 35 Prekonvertované pravidlo na detekciu neuskutočniteľnej cesty

4.2.6 Vloženie (injection)

Útok vložením (injection) sme prepojili s MITRE ATT&CK rámcom pomocou techník **T1068** – Exploitation for Privelege Escalation, ktorá súvisí so zneužitím zraniteľností za účelom zisku oprávnení, **T1190** – Exploit Public-Facing

Application, ktorá hovorí o zneužití zraniteľností systému pomocou softvérov, údajov alebo príkazov a s **T1491** – Defacement, čo súvisí s úpravou obsahu dostupného interne alebo externe v sieti.

Útoky vložením (injection**)** sa používajú na priamu manipuláciu s databázou pomocou škodlivých dopytov alebo príkazov. Aplikácie často používajú SQL príkazy na autentifikáciu používateľov do aplikácie a podobne. Dôvod, prečo útoky takéhoto typu fungujú je ten, že aplikácia pred odovzdaním SQL príkazu správne neoverí vstup. Napríklad ***SELECT * FROM tablename WHERE UserID = 2302*** sa zmení na ***SELECT * FROM tablename WHERE UserID = 2302 OR 1=1*** pridaním výrazu „OR 1=1“, ktorý nadobúda vždy pravdivú hodnotu. Na detekciu útoku typu SQL injection je potrebné monitorovať a analyzovať súbory záznamov z webových serverov a databázy. Na hľadanie útokov takéhoto typu využívame regulárne výrazy [73]:

- /((\%27)|(\'))(%20)union/ix
- /\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix

Tieto regulárne výrazy slúžia na detekciu základných útokov typu SQL injection. Prvý regulárny výraz hovorí o rôznych formách výrazu „‘%20union“ a druhý regulárny výraz zachytáva všetky výrazy obsahujúce reťazec „‘or“.

Na pozadí akademického informačného systému beží databáza Oracle. Vzhľadom k tomu, že sa používa SQL syntax, aj databáza Oracle je náchylná na SQL vloženie (injection). Na obrázku č. 36 môžeme vidieť časť pravidla písaného vo formáte Sigma pre detekciu útoku SQL injection.

```
title: SQL Injection
status: experimental
description: Detects SQL injection
author: Eva Markova
date: 2019/10/25
modified:
logsource:
    category: web
detection:
    selection:
        apache2.access.url|contains:
            - "%27%20union"
            - "%27%20UNION"
            - "'%20union"
            - "'%20UNION"
```

Obr. 36 Pravidlo na detekciu SQL injection

Na detekciu SQL injection sme použili vyhľadávanie regulárnych výrazov v poli apache2.access.url. Regulárne výrazy sledujú, či sa v URL odkaze vyskytujú znaky indikujúce, že na webovú aplikáciu bol vykonávaný útok typu SQL injection. Na obrázku č. 37 vidieť pravidlo prekonvertované pre ElastAlert.

```
filter:
- query:
    query_string:
      query: apache2.access.url.keyword:(*%27%20union* OR
      *%27%20UNION* OR *'%20union* OR *'%20UNION* OR
      *%27%6F%72* OR *%27%6Fr* OR *%27%6FR* OR *%27%6F%52*
      OR *%27o%72* OR *%27O%72* OR *%27or* OR *%27OR* OR
      *%27o%52* OR *%27O%52* OR *%27%4F%72* OR *%27%4Fr* OR
      *%27%4FR* OR *%27%4F%52* OR *'%6F%72* OR *'%6Fr* OR
      *'%6FR* OR *'%6F%52* OR *'o%72* OR *'O%72* OR *'or* OR
      *'OR* OR *'o%52* OR *'O%52* OR *'%4F%72* OR *'%4Fr* OR
      *'%4FR* OR *'%4F%52*)
index: filebeat-*
name: SQL-Injection_0
priority: 2
realert:
  minutes: 1
type: any

alert: hivealerter
```

Obr. 37 Prekonvertované pravidlo na detekciu SQL injection

4.3 Bezpečnostné hrozby na úrovni prihláseného používateľa

Poslednou skupinou bezpečnostných hrozieb relevantných pre akademický informačný systém sú hrozby na úrovni prihláseného používateľa. Pre hrozby tohto typu nevieme úplne určiť techniky z MITRE ATT&CK rámca, avšak vieme ich prepojiť s taktikami z tohto rámca:

- TA0006 – Credential Access,
- TA0007 – Discovery a
- TA0009 – Collection.

4.3.1 Neoprávnený prístup k modulu AiS2

V rámci tejto kategórie teda sledujeme pokusy o neoprávnený prístup k modulom akademického informačného systému AiS2. Keď vezmeme do úvahy napríklad aplikáciu SSSP005 (Správa existujúcich používateľov), ku ktorej môže pristúpiť len

užívateľ s rolami operátor univerzity/fakulty, pomocný operátor univerzity/fakulty alebo správca používateľov univerzity/fakulty, tak vieme odchytiť pokusy o prístup k tejto aplikácii. Na to, aby bolo odoslané varovanie do platformy TheHive stačí, aby potenciálny útočník pristúpil k URL odkazu tejto aplikácie. Príklad takéhoto pravidla vo formáte Sigma vidieť na obrázku č. 38.

```
title: Management of existing users
status: experimental
author: Eva Markova
date: 2019/10/25
modified: 2020/12/15
logsource:
    category: ais
detection:
    selection:
        ais_appCode: SSSP005
    filter:
        ais_userRoles:
          - "*,x,*"
          - "x,*"
          - "*,x"
          - "*,y,*"
          - "y,*"
          - "*,y"
          - "*,z,*"
          - "z,*"
          - "*,z"
    condition: selection and not filter
fields:
    - ais_userLogin
level: medium
```

Obr. 38 Pravidlo na kontrolu prístupu k aplikácii SSSP005

Na obrázku č. 39 je pravidlo prekonvertované pre ElastAlert.

```
filter:
- query:
    query_string:
      query: (ais_appCode:"SSSP005" AND
      (NOT (ais_userRoles.keyword:(*,x,* OR
       x,* OR *,x OR *,y,* OR y,* OR *,y OR
       *,z,* OR z,* OR *,z))))
index: filebeat-*
name: management_of_existing_users_0
priority: 3
realert:
  minutes: 1
type: any

alert: hivealerter
```

Obr. 39 Prekonvertované pravidlo na kontrolu prístupu k aplikácii SSSP005

4.3.2 Prístup k viacerým aplikáciám súvisiacich s osobnými údajmi používateľov

Činnosťou, ktorú je vhodné v rámci akademického informačného systému AiS2 sledovať je pristupovanie k viacerým aplikáciám súvisiacich s osobnými údajmi používateľov. Pri tejto činnosti vychádzame z hypotézy, že pri kompromitácii účtu útočník môže získavať informácie o účte, do ktorého získal prístup. K detekcii tejto činnosti sledujeme otvorenie aplikácií obsahujúcich osobné údaje používateľa, napríklad SSSP005 – Správa existujúcich používateľov alebo SSSP003 – Správa používateľa za krátke časové obdobie. Na obrázku č. 40 je vidieť ukážku pravidla vo formáte Sigma.

```
title: View user management applications
status: experimental
author: Eva Markova
date: 2021/04/20
logsource:
    category: ais
detection:
    selection:
        ais_appCode: SSSP*
    condition: selection | count(ais_appCode) by ais_username > 1
fields:
    - ais_
level: medium
```

Obr. 40 Pravidlo na sledovanie prístupu k modulom súvisiacim s používateľmi

Ak potenciálny útočník pristúpi k aspoň dvom aplikáciám, ktoré súvisia s osobnými údajmi používateľov, zasielame upozornenie do platformy TheHive. Na obrázku č. 41 vidieť pravidlo pre tento typ bezpečnostnej hrozby prekonvertované pre ElastAlert.

```
filter:
- query:
    query_string:
      query: ais_appCode.keyword:SSSP*
buffer_time:
  minutes: 5
index: filebeat-*
max_threshold: 1
metric_agg_key: ais_appCode.keyword
metric_agg_type: cardinality
name: View-user-management-applications_0
priority: 3
query_key: ais_username.keyword
realert:
  minutes: 1
type: metric_aggregation

alert: hivealerter
```

Obr. 41 Prekonvertované pravidlo na sledovanie prístupu k modulom súvisiacim s používateľmi

4.3.3 Zaslanie žiadosti o zmenu hesla v službách Office365

Akademický informačný systém AiS2 umožňuje v aktuálnej verzii možnosť zmeny hesla príslušného používateľského účtu v službe Office365. Z pohľadu bezpečnosti ide o významnú funkcionalitu. Kompromitácia používateľského účtu v rámci AiS2 umožní útočníkovi tzv. lateral movement a posun do služby Office365. Z tohto dôvodu sme sa rozhodli monitorovať zasielanie takýchto žiadostí. Na obrázku č. 42 vidieť pravidlo na detekciu zaslania žiadosti.

```
title: Reset Password For Office365
status: experimental
author: Eva Markova
date: 2021/04/20
logsource:
    category: ais
detection:
    selection:
        logMessage: "reset office365"
    condition: selection
level: low
```

Obr. 42 Pravidlo na detekciu zaslania žiadosti o zmenu hesla v službách Office365

V prípade, že atribút logMessage obsahuje reťazec „reset office365“, zasielame upozornenie do platformy TheHive s menom používateľa a časovou pečiatkou žiadosti

o zmenu. Na obrázku č. 43 je vidieť pravidlo prekonvertované do čitateľnej podoby pre ElastAlert.

```
filter:
- query:
    query_string:
      query: logMessage:"reset\ office365"
index: filebeat-*
name: Reset-Password-For-Office365_0
priority: 3
realert:
  minutes: 1
type: any
```

Obr. 43 Prekonvertované pravidlo na detekciu zaslania žiadosti o zmenu hesla v službách Office365

4.3.4 Prístup k neexistujúcemu modulu AiS2

V rámci tejto diplomovej práce sme sa zamerali aj na detekciu pokusov o prístup k neexistujúcemu modulu AiS2. Ak sa používateľ dopytuje na neexistujúci modul, vnímame to ako potenciálnu hrozbu pre akademický informačný systém. Na obrázku č. 44 je možné vidieť pravidlo pre detekciu tejto aktivity.

```
title: Non-existing module
status: experimental
author: Eva Markova
date: 2021/04/20
logsource:
    category: ais
detection:
    selection:
        apache2.access.url: "kodAplikacie"
        apache2.access.response_code: 500
    condition: selection
level: medium
```

Obr. 44 Pravidlo na detekciu prístupu k neexistujúcemu modulu AiS2

Ak modul neexistuje, nemáme k nemu aplikačné záznamy (logy), a preto musíme sledovať atribúty z prístupových záznamov webového servera Apache2. Ak kód odpovede je 500, nastáva „Internal Server Error“ a my vieme povedať, že daný modul v AiS2 neexistuje. Na obrázku č. 45 vidieť prekonvertované pravidlo na detekciu.

```
filter:
- query:
    query_string:
      query: (apache2.access.url:"kodAplikacie" AND
              apache2.access.response_code:"500")
index: filebeat-*
name: Non-existing-module_0
priority: 3
realert:
  minutes: 1
type: any

alert: hivealerter
```

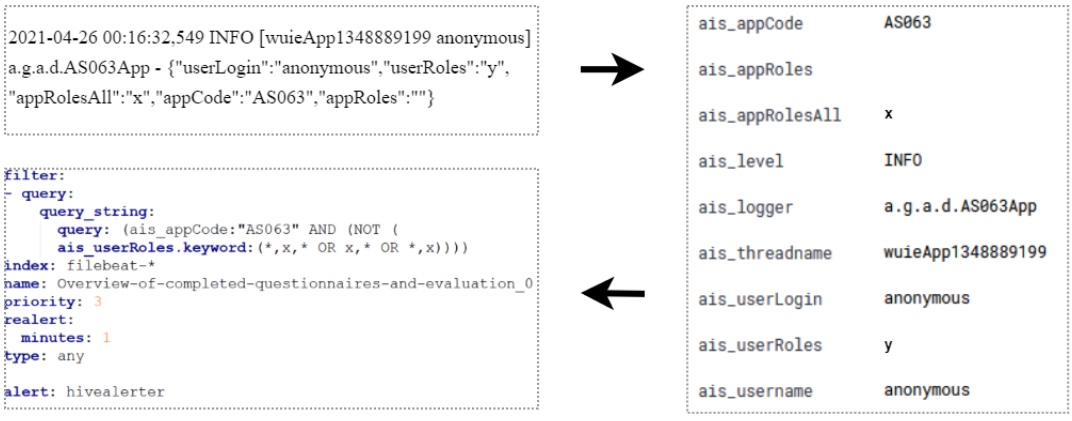
Obr. 45 Prekonvertované pravidlo na detekciu prístupu k neexistujúcemu modulu AiS2

5 Vyhodnotenie

V rámci tejto diplomovej práce sme vytvorili 19 pravidiel na detekciu hrozieb na úrovni prihláseného používateľa, 14 pravidiel s ohľadom na operačný systém a 6 pravidiel s ohľadom na webovú aplikáciu. Taktiež sme využili 12 pravidiel z verejného repozitára na detekciu hrozieb zo záznamov služby auditd. Najdôležitejšie pre akademický informačný systém AiS2 sú tie pravidlá, ktoré detegujú aktivitu na úrovni prihláseného používateľa. Pre každú bezpečnostnú hrozbu je dôležité vyhodnotiť závažnosť jej vyskytnutia sa v systéme. Určili sme tri úrovne – nízka, stredná a vysoká. Hrozby a k ním prislúchajúce pravidlá vyhodnocujeme na základe možnosti výskytu falošných upozornení a prípadného neželaného dopadu na organizáciu.

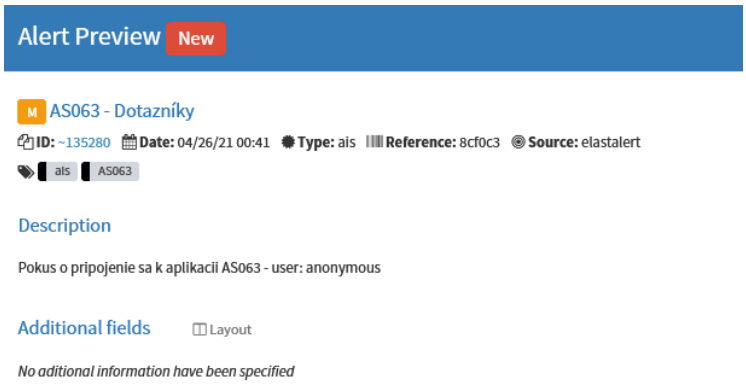
5.1 Vyhodnotenie pravidiel k bezpečnostným hrozbám na úrovni prihláseného používateľa

Až 16 z pravidiel na úrovni prihláseného používateľa súvisí s neoprávneným prístupom k rôznym modulom AiS2. Ako príklad uvedieme situáciu, keď sa neautorizovaný používateľ snaží pristúpiť k modulu AS063 (Prehľad uskutočnených dotazníkov, vyhodnotenie) a nemá priradenú rolu zamestnanec. V tomto prípade získavame záznam v pôvodnej, nespracovanej forme, z ktorého následne extrahujeme atribúty. Nad týmito atribútmi sa vykoná pravidlo, ktoré deteguje podozrivú činnosť. Následne ElastAlert odosiela hlásenie do platformy TheHive. Na obrázku č. 46 môžeme vidieť postup na vyhodnotenie prístupu k aplikácii AS063.



Obr. 46 Postup vyhodnocovania prístupu k aplikácii AS063

Ukážka upozornenia v platforme TheHive je na obrázku č. 47. Môžeme vidieť, že upozornenie má strednú závažnosť a tiež vidíme meno používateľa, ktorý sa k danému modulu snažil pristúpiť. V tomto prípade sa jedná o používateľa „anonymous“, teda neprihláseného používateľa.



Obr. 47 Ukážka upozornenia pre pokus o neoprávnený prístup k modulu AS063

V tabuľke č. 13 je možné vidieť, aké role používateľov môžu pristúpiť ku konkrétnemu modulu.

Tab. 13 Moduly a role k nim prislúchajúce

Označenie modulu	Názov modulu	Role, ktoré môžu pristúpiť k modulu
AS063	Prehľad uskutočnených dotazníkov, vyhodnotenie	• zamestnanec
EP007	Evidencia požiadaviek na verejné obstarávanie	• zamestnanec • operátor VO • správca VO
LZ020	Prehľad zamestnancov a pracovných pomerov na strediskách	• zamestnanec • správca zamestnaneckých pomerov na univerzite/fakulte
SSSA001	Správa aplikácií	• správca AIS a centrálnych číselníkov
SSSM001	Monitor pripojení AiS2	• správca AIS a centrálnych číselníkov • lokálny správca systému AIS
SSSP005	Správa existujúcich používateľov	• operátor univerzity/fakulty • pomocný operátor univerzity/fakulty • správca používateľov univerzity/fakulty
VSES040	Evidencia hodnotenia študentov	• vyučujúci • zapisovateľ pedagogickej činnosti na stredisku

		• študijný poradca predmetov strediska • kontrolór pedagogickej činnosti na stredisku
VSES070	Administrácia školného a poplatkov	• referent školného a poplatkov • prezerač školného a poplatkov
VSES105	Administrácia štipendií	• štipendijný referent • prezerač štipendií
VSES118	Prehľad študentov, individuálny prístup na osobné údaje,...	• administrátor štúdia študentov • študijný poradca štúdia študentov • študijný poradca (koordinátor) študijného programu
VSES229	Hodnotenie štátnych skúšok	• administrátor štátnych skúšok • člen štátnicovej komisie • administrátor predmetov štátnych skúšok na stredisku
VSES310	Doktorandi školiteľa, garanta študijného programu	• školiteľ doktoranda • garant štúdia III. stupňa • vedúci strediska doktoranda
VSPK014	Evidencia uchádzačov, prihlášok	• administrátor prihlášok prijímacieho konania • prezerač prihlášok PK • prezerač osobných údajov prihlášok PK
VSPK055	Elektronické návratky	• administrátor prihlášok prijímacieho konania
VSPK066	Zoznam evidovaných elektronických prihlášok AiS2	• administrátor prihlášok prijímacieho konania
VSUB001	Evidencia, spracovanie žiadostí o ubytovanie	• administrátor žiadostí o ubytovanie • administrátor žiadostí o ubytovanie študentov

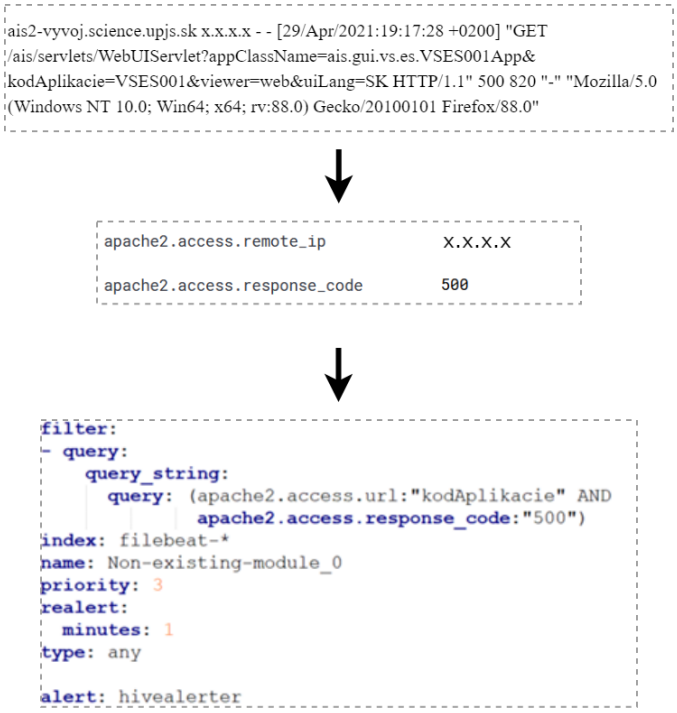
Ďalšie pravidlo súvisí s prístupom k viacerým aplikáciám súvisiacich s osobnými údajmi používateľov. Ako príklad uvedieme situáciu, kedy používateľ pristupoval k modulom SSSP005 – Správa existujúcich používateľov a SSSP003 – Správa používateľa. Na obrázku č. 48 vidieť záznamy v pôvodnej nespracovanej forme, pričom sme z nich vyextrahovali atribúty ais_appCode a ais_username a časovú pečiatku. Aplikovaním pravidla na detekciu takejto činnosti získavame upozornenie v platforme TheHive.

Obr. 48 Postup vyhodnocovania prístupu k aplikáciám súvisiacich s osobnými údajmi používateľov

Ďalšou sledovanou aktivitou v rámci akademického informačného systému AiS2 je žiadosť o zmenu hesla v službách Office365. V prípade, že používateľ akademického informačného systému AiS2 požiada o zmenu hesla v službách Office365, zasielame upozornenie do platformy TheHive. Na obrázku č. 50 vidieť postup vyhodnocovania, pričom dôležitým atribútom je ais_username.

Obr. 49 Postup vyhodnocovania žiadosti o zmenu hesla v službách Office365

Posledným pravidlom je pravidlo na detekciu pokusu o prístup k neexistujúcemu modulu AiS2. Ak sa používateľ snaží pristúpiť k neexistujúcemu modulu, odosielame upozornenie do platformy TheHive. Postup vyhodnotenia je na obrázku č. 52. Dôležitými atribútmi sú IP adresa, odkiaľ prišla požiadavka na webový server a kód odpovede.



Obr. 50 Postup vyhodnocovania pokusu o prístup k neexistujúcemu modulu AiS2

Vo všeobecnosti teda máme pre AiS2 19 implementovaných pravidiel, pričom ich môžeme zaradiť do štyroch kategórií. V tabuľke č. 14 je možné vidieť tieto pravidlá. Závažnosť sme určili podľa toho, aký dopad by to malo na organizáciu v prípade, že by sa ukázalo, že naozaj ide o škodlivú aktivitu vykonanú v AiS2. Tiež sme brali do úvahy prípady, kedy by sa mohlo jednať o falošné upozornenia. Detekcia vypovedá o tom, či sa nám v rámci SIEM systému podarilo aktivitu takéhoto typu detegovať.

Tab. 14 Vyhodnotenie pravidiel na detekciu hrozieb na úrovni prihláseného používateľa

Kategória	Vykonaná činnosť	Názov pravidla	Závažnosť hrozby	Detekcia
ais	curl ...názovModulu...	Module	stredná	✓
ais	prístup k SSSP003 a SSSP005	View modules with information about users	vysoká	✓
ais	reset hesla v službách Office365	Reset password for Office365	nízka	✓
ais	dopyt na neexistujúci modul	Non-existing module	stredná	✓

5.2 Vyhodnotenie pravidiel k bezpečnostným hrozbám na úrovni operačného systému

Okrem bezpečnostných hrozieb na úrovni prihláseného používateľa, ktoré sme schopní detegovať, je potrebné tiež otestovať funkčnosť nami vytvorených pravidiel pre detekciu hrozieb na úrovni operačného systému. Týchto pravidiel je spolu 14.

V tabuľke č. 15 je vidieť, ktoré pravidlá po otestovaní detegovali činnosť prípadného útočníka na úrovni operačného systému. V stĺpci „vykonaná činnosť“ sa nachádza činnosť, ktorá bola vykonaná na simuláciu hrozby pre akademický informačný systém. Väčšine bezpečnostných hrozieb na tejto úrovni sme určili závažnosť s hodnotou „stredná“ z dôvodu, že tieto príkazy môže vykonávať tiež

administrátor systému. Ak však identifikujeme pokus o použitie tzv. hrubej sily na prelomenie hesla, závažnosť je vysoká.

Tab. 15 Vyhodnotenie pravidiel na detekciu hrozieb na úrovni operačného systému

Kategória	Vykonaná činnosť	Názov pravidla	Závažnosť hrozby	Detekcia
OS	príkaz *ifconfig*	System Network Configuration Discovery	stredná	✓
OS	príkaz *cat /etc/hosts*	Remote System Discovery	stredná	✓
OS	príkaz *whoami*	System Owner User Discovery	stredná	✓
OS	príkaz *lsof*	System Network Connections Discovery	stredná	✓
OS	príkaz *ps -aux*	Process Discovery	stredná	✓
OS	príkaz *groups*	Permission Groups Discovery: Local Groups	stredná	✓
OS	príkaz *ldapsearch*	Permission Groups Discovery: Domain Groups	stredná	✓
OS	príkaz *uname*	System Information Discovery	stredná	✓
OS	príkaz *tree*	File and Directory Discovery	stredná	✓
OS	príkaz *cat /etc/passwd*	Account Discovery: Local Account	stredná	✓
OS	príkaz *ldapsearch*	Account Discovery: Domain Account	stredná	✓
OS	použitie hrubej sily na prelomenie hesla	Brute Force ssh	vysoká	✓

	v službe SSH			
OS	príkaz *useradd test*	Create Account	stredná	✓
OS	príkaz *pwpolicy*	Password Policy Discovery	stredná	✓

5.3 Vyhodnotenie pravidiel k bezpečnostným hrozbám na úrovni webovej aplikácie

Poslednou kategóriou bezpečnostných hrozieb pre akademický informačný systém sú bezpečnostné hrozby na úrovni webovej aplikácie. Pravidiel na detekciu hrozieb na tejto úrovni je dokopy 6. V tabuľke č. 16 je vidieť tieto pravidlá. Ich závažnosť je určená ako „vysoká“, pretože ak by sa jednalo o úspešné dokončenie útoku, mohlo by dôjsť k úniku citlivých údajov, čo by pre organizáciu znamenalo, že čelí kybernetickému útoku, ktorý sa týka používateľov či už serverov akademického informačného systému alebo samotného akademického informačného systému AiS2.

Tab. 16 Vyhodnotenie pravidiel na detekciu hrozieb na úrovni webovej aplikácie

Kategória	Vykonaná činnosť	Názov pravidla	Závažnosť hrozby	Detekcia
web	pokus o injekciu	SQL Injection	vysoká	✓
web	opakovaný pokus o prístup k URL .../fotky/1.jpg	Access to Data	vysoká	✓
web	použitie hrubej sily na heslo vo webovej aplikácii	Brute Force web	vysoká	✓
web	pokus o cross-site scripting	XSS scan	vysoká	X
web	pokus o prístup k ../../etc/passwd	Path Traversal	vysoká	✓

web	použitie VPN pri prihlasovaní sa	Impossible Travel	vysoká	✓

Keďže máme dokopy vo všetkých troch kategóriách 39 nami vytvorených pravidiel, úspešnosť detekcie je rovná pomeru počtu detegovaných pokusov o škodlivú činnosť k počtu všetkých pokusov o škodlivú činnosť (38/39). Úspešnosť je teda 97,43%. Chybovosť pri pravidle XSS Scan nastala z dôvodu nesprávneho využitia regulárnych výrazov v pravidlách.

Záver

Hlavnou myšlienkou tejto diplomovej práce bolo implementovať SIEM systém, ktorý by bol schopný detegovať potenciálne bezpečnostné hrozby v rámci akademického informačného systému. Hlavným cieľom práce bolo vytvoriť škálovateľný SIEM systém. K tomuto účelu využívame akademický informačný systém AiS2, ktorý je v čase spracovania tejto práce využívaný na väčšine vysokých škôl v Slovenskej republike.

Prvým cieľom tejto diplomovej práce bolo preskúmať a analyzovať aktuálne prístupy k manažmentu bezpečnostných informácií a udalostí (SIEM) s ohľadom na akademické informačné systémy. Tomuto cieľu sme sa venovali v prvej kapitole, kde sme popísali základné informácie a vlastnosti o SIEM systémoch a komponenty SIEM systémov. Porovnali sme rôzne implementácie SIEM systémov či už s uzavretým, alebo otvoreným kódom. Popísali sme výhody a nevýhody použitia rôznych riešení, pričom pre účely tejto diplomovej práce sme sa rozhodli použiť voľne dostupné nástroje ELK (Elasticsearch, Logstash, Kibana).

Druhým cieľom našej práce bolo navrhnúť pravidlá detekcie bezpečnostných hrozieb pre akademický informačný systém s ohľadom na rámec MITRE ATT&CK. V rámci druhej kapitoly sa venujeme popisu taktík, techník a postupov, pričom plynulo prechádzame k MITRE ATT&CK rámcu. Taktiež popisujeme na čo tento rámec slúži, akú ma štruktúru a akým spôsobom sme schopní prepájať pozorované dáta s týmto rámcom. Tiež sme sa venovali tomu, akým spôsobom sa vytvárajú odporúčania pre organizáciu z techník. Priblížili sme pojem APT (Advanced Persistent Threat) skupina, opísali jej životný cyklus a zamerali sa na techniky, ktoré APT skupiny využívajú vo svojich kampaniach voči akademickým, vzdelávacím a výskumným inštitúciám. Samotné pravidlá sme navrhli vo štvrtej kapitole, kde sme sa venovali popisu bezpečnostných hrozieb relevantných pre akademický informačný systém. Bezpečnostné hrozby sme rozdelili na tri kategórie – bezpečnostné hrozby na úrovni operačného systému, na úrovni webovej aplikácie a na úrovni prihláseného používateľa. Dokopy sme implementovali 19 pravidiel vo formáte Sigma na detekciu bezpečnostných hrozieb na úrovni prihláseného používateľa, 14 pravidiel na detekciu bezpečnostných hrozieb na úrovni operačného systému a 6 pravidiel na detekciu bezpečnostných hrozieb na úrovni prihláseného používateľa. Taktiež sme v našom

SIEM systéme využili 12 pravidiel na detekciu bezpečnostných hrozieb z verejného repozitára súvisiacich so službou auditd.

Hlavným a posledným cieľom bolo navrhnúť, implementovať a vyhodnotiť SIEM systém pre akademický informačný systém. Návrhu a implementácii sa venujeme v tretej kapitole. Popisujeme akú architektúru má akademický informačný systém AiS2 a tiež, že bola pripravená analýza rizík pre AiS2. V ďalšej časti tejto kapitoly popisujeme návrh technickej infraštruktúry a tiež nástroje ako Elasticsearch, Logstash, Kibana a Filebeat. Venujeme sa popisu zdrojov záznamov, ktoré spracovávame v rámci SIEM systému. Spracovali sme záznamy z webového servera Apache2, záznamy zo súboru audit.log, históriu príkazového riadka a aplikačné záznamy AiS2. Tiež popisujeme nástroj ElastAlert, ktorý slúži na upozorňovanie správcov, pričom my preposielame upozornenia do platformy TheHive, ktorá slúži na riešenie bezpečnostných incidentov. Vyhodnoteniu SIEM systému sa venujeme v piatej kapitole, kde sme zvlášť vyhodnotili všetky tri kategórie bezpečnostných hrozieb pre akademický informačný systém. Určili sme závažnosť týchto hrozieb s ohľadom na dopad pre organizáciu a prípadne falošne pozitívnych upozornení. Celková úspešnosť nami navrhnutého SIEM systému je 97,43%, pričom až 38 nami implementovaných pravidiel bolo schopných detegovať škodlivú činnosť vykonávanú nad akademickým informačným systémom.

Do budúcna by sme na túto diplomovú prácu mohli nadviazať s problematikou vytvárania profilov útočníkov. Na tieto účely je potrebné prejsť techniky, ktoré sme už zachytili a korelovať ich s technikami používanými známymi APT skupinami. Tiež by bolo vhodné zbierať záznamy aj s databázy Oracle, pre detekciu manipulácie s databázou. Taktiež by bolo vhodné vytvoriť klaster a distribuovať Elasticsearch na viacero uzlov, aby sme v prípade výpadku vedeli používať SIEM systém aj naďalej. Vylepšenie systému by sme tiež mohli dosiahnuť zbieraním záznamov z „iptables“ a sledovať tak prípadné pokusy o uskutočňovanie techník z taktiky „bočný pohyb (lateral movement – TA0008)“ z MITRE ATT&CK rámca.

Zoznam použitej literatúry

1. O'brien, James A., and George M. Marakas. *Introduction to information systems*. Vol. 13. New York City, USA: McGraw-Hill/Irwin, 2005.
2. SIEM [online]. [cit. 2019-12-02]. Dostupné z: https://logdna.com/what-is-siem
3. SEKHARAN, S. Sandeep; KANDASAMY, Kamalanathan. Profiling SIEM tools and correlation engines for security analytics. In: 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). IEEE, 2017. p. 717-721.
4. MAVROEIDIS, VASILEIOS and BROMANDER, SIRI, 2017, Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. *2017 European Intelligence and Security Informatics Conference (EISIC)*. 2017. DOI 10.1109/eisic.2017.20. IEEE
5. Threat hunting [online]. [cit. 2021-04-16]. Dostupné z: http://staging-resources.malwarebytes.com/files/2018/09/Survey_ThreatHunting-2018_Malwarebytes.pdf
6. MURDOCH, D. W. SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter. Independent Publishing, 2019.
7. CINQUE, MARCELLO, COTRONEO, DOMENICO and PECCHIA, ANTONIO, 2018, Challenges and Directions in Security Information and Event Management (SIEM). *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. 2018. DOI 10.1109/issrew.2018.00-24. IEEE
8. DETKEN, KAI-OLIVER, RIX, THOMAS, KLEINER, CARSTEN, HELLMANN, BASTIAN and RENNERS, LEONARD, 2015, SIEM approach for a higher level of IT security in enterprise networks. *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. 2015. DOI 10.1109/idaacs.2015.7340752. IEEE
9. SAFARZADEH, MAHDIEH, GHARAEE, HOSSEIN and PANAHI, AMIR HOSSEIN, 2019, A Novel and Comprehensive Evaluation Methodology for

SIEM. *Information Security Practice and Experience*. 2019. P. 476-488. DOI 10.1007/978-3-030-34339-2_28. Springer International Publishing

10. Splunk Enterprise [online]. [cit. 2021-01-22]. Dostupné z: https://docs.splunk.com/Documentation/Splunk/8.1.1/Overview/AboutSplunkEnterprise
11. IBM QRadar [online]. [cit. 2019-12-02]. Dostupné z: https://www.ibm.com/us-en/marketplace/ibm-qradar-siem
12. USM Anywhere [online]. [cit. 2021-01-22]. Dostupné z: https://cybersecurity.att.com/documentation/usm-anywhere/user-guide/getting-started/getting-started.htm
13. USM Anywhere [online]. [cit. 2021-01-22]. Dostupné z: https://www.unifiedthreatworks.com/datasheets/DS-USM-Anywhere.pdf
14. ArcSight SIEM [online]. [cit. 2020-06-07]. Dostupné z: https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview
15. RAJA, M. Siva Niranjan; VASUDEVAN, A. R. Rule Generation for TCP SYN Flood attack in SIEM Environment. Procedia computer science, 2017, 115: 580-587.
16. Splunk Free [online]. [cit. 2021-01-22]. Dostupné z: https://docs.splunk.com/Documentation/Splunk/8.1.1/Admin/MoreaboutSplunkFree
17. IBM QRadar Community Edition [online]. [cit. 2021-01-22]. Dostupné z: https://www.ibm.com/community/qradar/ce/#about
18. AlienVault [online]. [cit. 2019-12-02]. Dostupné z: https://cybersecurity.att.com/products/ossim
19. AlienVault Open Threat Exchange (OTX) [online]. [cit. 2020-06-15]. Dostupné z: https://otx.alienvault.com/
20. AlienVault Patch Release v. 5.0.3. [online]. [cit. 2019-12-02]. Dostupné z: https://success.alienvault.com/s/question/0D50Z00008oGqV1SAK/alienvault-v503-patch-release
21. PRADS [online]. [cit. 2020-06-15]. Dostupné z: https://github.com/gamelinux/prads

22. Snort [online]. [cit. 2020-06-15]. Dostupné z: https://www.snort.org/
23. Suricata IDS [online]. [cit. 2020-06-15]. Dostupné z: https://suricata-ids.org/
24. TCPtrack [online]. [cit. 2020-06-15]. Dostupné z: https://linux.die.net/man/1/tcptrack
25. Munin [online]. [cit. 2020-06-15]. Dostupné z: http://munin-monitoring.org/
26. NFsen [online]. [cit. 2020-06-15]. Dostupné z: http://nfsen.sourceforge.net/
27. NFdump [online]. [cit. 2020-06-15]. Dostupné z: http://nfdump.sourceforge.net/
28. FProbe [online]. [cit. 2020-06-15]. Dostupné z: http://manpages.ubuntu.com/manpages/bionic/man8/fprobe.8.html
29. Nagios [online]. [cit. 2020-06-15]. Dostupné z: https://www.nagios.org/
30. OpenVAS [online]. [cit. 2020-06-15]. Dostupné z: https://openvas.org/
31. Elastic [online]. [cit. 2019-12-02]. Dostupné z: https://www.elastic.co/products/siem
32. AL-MOHANNADI, HAMAD, MIRZA, QUBLAI, NAMANYA, ANITTA, AWAN, IRFAN, CULLEN, ANDREA and DISSO, JULES, 2016, Cyber-Attack Modeling Analysis Techniques: An Overview. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. 2016. DOI 10.1109/w-ficloud.2016.29. IEEE
33. F. Maymí, R. Bixler, R. Jones and S. Lathrop, "Towards a definition of cyberspace tactics, techniques and procedures," *2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, USA, 2017, pp. 4674-4679, doi: 10.1109/BigData.2017.8258514.
34. EZELL, BARRY CHARLES, 2007, Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis*. 2007. Vol. 27, no. 3, p. 571-583. DOI 10.1111/j.1539-6924.2007.00907.x. Wiley
35. Rámec MITRE ATT&CK [online]. [cit. 2019-12-02]. Dostupné z: https://attack.mitre.org/
36. STROM, Blake E., et al. Finding cyber threats with ATT&CK-based analytics. Technical Report MTR170202, MITRE, 2017.
37. Cyber Kill Chain [online]. [cit. 2021-04-12]. Dostupné z: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
38. Pyramída bolesti [online]. [cit. 2021-04-12]. Dostupné z: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

39. STROM, Blake E., et al. Mitre att&ck: Design and philosophy. Technical report, 2018.
40. TATAM, Matt, et al. A review of threat modelling approaches for APT-style attacks. Helyion 7.1, 2021.
41. AHMAD, ATIF, WEBB, JEB, DESOUZA, KEVIN C. and BOORMAN, JAMES, 2019, Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*. 2019. Vol. 86, p. 402-418. DOI 10.1016/j.cose.2019.07.001. Elsevier BV
42. CHEN, PING, DESMET, LIEVEN and HUYGENS, CHRISTOPHE, 2014, A Study on Advanced Persistent Threats. *Advanced Information Systems Engineering*. 2014. P. 63-72. DOI 10.1007/978-3-662-44885-4_5. Springer Berlin Heidelberg
43. BREWER, ROSS, 2014, Advanced persistent threats: minimising the damage. *Network Security*. 2014. Vol. 2014, no. 4, p. 5-9. DOI 10.1016/s1353-4858(14)70040-6. Elsevier BV
44. Taktika Initial Access [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0001/
45. Taktika Persistence [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0003
46. Taktika Execution [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0002
47. Taktika Privilege Escalation [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0004
48. Taktika Defense Evasion [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0005
49. Taktika Credential Access [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0006
50. Taktika Discovery [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0007
51. Taktika Lateral Movement [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0008
52. Taktika Collection [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0009

53. Taktika Command and Control [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0011
54. Taktika Exfiltration [online]. [cit. 2021-04-16]. Dostupné z: https://attack.mitre.org/tactics/TA0010
55. MITRE ATT&CK tréning [online]. [cit. 2020-06-07]. Dostupné z: https://attack.mitre.org/resources/training/cti/
56. MITRE ATT&CK navigátor [online]. [cit. 2020-06-07]. Dostupné z: https://mitre-attack.github.io/attack-navigator/enterprise/
57. ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management.
58. Filebeat [online]. [cit. 2021-01-22]. Dostupné z: https://www.elastic.co/beats/filebeat
59. Plugin grok [online]. [cit. 2021-01-22]. Dostupné z: https://www.elastic.co/guide/en/logstash/current/plugins-filters-grok.html
60. Plugin kv [online]. [cit. 2021-01-22]. Dostupné z: https://www.elastic.co/guide/en/logstash/current/plugins-filters-kv.html
61. Polia logov webového servera [online]. [cit. 2021-01-22]. Dostupné z: https://www.elastic.co/guide/en/beats/filebeat/6.8/exported-fields-apache2.html
62. Polia logov služby auditd [online]. [cit. 2021-04-23]. Dostupné z: https://www.elastic.co/guide/en/beats/filebeat/current/exported-fields-auditd.html
63. Sigma [online]. [cit. 2021-01-22]. Dostupné z: https://github.com/Neo23x0/sigma
64. ElastAlert [online]. [cit. 2021-01-22]. Dostupné z: https://elastalert.readthedocs.io/en/latest/elastalert.html
65. JIRA [online]. [cit. 2021-01-22]. Dostupné z: https://www.atlassian.com/software/jira
66. OpsGenie [online]. [cit. 2021-01-22]. Dostupné z: https://www.atlassian.com/software/opsgenie
67. SNS [online]. [cit. 2021-01-22]. Dostupné z: https://aws.amazon.com/sns/
68. Slack [online]. [cit. 2021-01-22]. Dostupné z: https://slack.com/
69. TheHive [online]. [cit. 2021-01-22]. Dostupné z: https://thehive-project.org/

70. CATAKOGLU, ONUR, BALDUZZI, MARCO and BALZAROTTI, DAVIDE, 2016, Automatic Extraction of Indicators of Compromise for Web Applications. *Proceedings of the 25th International Conference on World Wide Web*. 2016. DOI 10.1145/2872427.2883056. International World Wide Web Conferences Steering Committee

71. OWASP Top Ten [online]. [cit. 2021-04-16]. Dostupné z: https://owasp.org/www-project-top-ten/

72. HAN, EI EI, 2015, Detection of Web Application Attacks with Request Length Module and Regex Pattern Analysis. *Advances in Intelligent Systems and Computing*. 2015. P. 157-165. DOI 10.1007/978-3-319-23207-2_16. Springer International Publishing

73. WAN, MIN and LIU, KUN, 2012, An Improved Eliminating SQL Injection Attacks Based Regular Expressions Matching. *2012 International Conference on Control Engineering and Communication Technology*. 2012. DOI 10.1109/iccect.2012.235. IEEE

Prílohy

Príloha A: Diplomová práca v elektronickej podobe, prílohy v elektronickej podobe

Príloha B: Pravidlá písané vo formáte Sigma

Príloha C: Pravidlá prekonvertované pre ElastAlert

Príloha D: Konfiguračné súbory pre Logstash

Príloha E: Konfiguračné súbory pre Filebeat

Príloha D:Konfiguračné súbory pre Logstash

/etc/logstash/conf.d/apache2.conf

```
input {
        beats {
                port => "5046"
        }
}

filter {
 if [fileset][name] == "access" {
    grok {
      match => { "message" =>
["%{IPORHOST:[apache2][access][remote_ip]} -
%{DATA:[apache2][access][user_name]}
\[%{HTTPDATE:[apache2][access][time]}\]
\"%{WORD:[apache2][access][method]}
%{GREEDYDATA:[apache2][access][url]}
HTTP/%{NUMBER:[apache2][access][http_version]}\"
%{NUMBER:[apache2][access][response_code]}
%{NOTSPACE:[apache2][access][body_sent][bytes]}(
\"%{DATA:[apache2][access][referrer]}\")?(
\"%{DATA:[apache2][access][agent]}\")?",
        "%{IPORHOST:[apache2][access][remote_ip]} -
%{DATA:[apache2][access][user_name]}
\\[%{HTTPDATE:[apache2][access][time]}\\] \"-\"
%{NUMBER:[apache2][access][response_code]} -" ] }
    }

    mutate {
      add_field => { "read_timestamp" => "%{@timestamp}" }
    }

    date {
      match => [ "[apache2][access][time]", "dd/MMM/YYYY:H:m:s Z" ]
      remove_field => "[apache2][access][time]"
    }

    useragent {
      source => "[apache2][access][agent]"
      target => "[apache2][access][user_agent]"
      remove_field => "[apache2][access][agent]"
    }

    geoip {
      source => "[apache2][access][remote_ip]"
      target => "[apache2][access][geoip]"
    }

  }
```

```
}


output {
        elasticsearch {
                hosts => ["localhost:9200"]
                index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
                document_type => "%{[@metadata][type]}"
        }
}
```

/etc/logstash/conf.d/audit-kv.conf

```
input {
        beats {
                port => "5049"
        }
}


filter {
        if [log][file][path] == "../audit.log" {

                grok {
                        match => { "message" =>
"type=%{WORD:audit_type}
msg=audit\(%{NUMBER:audit_epoch}:%{NUMBER:audit_counter}\):
%{GREEDYDATA:logMessage}" }
                }

                kv {
                        source => "logMessage"
                        field_split => " "
                        prefix => "audit_"
                }

                kv {
                        source => "audit_msg"
                        field_split => " "
                        prefix => "audit_"
                }
        }
}

output {
        elasticsearch {
                hosts => ["localhost:9200"]
                index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
                document_type => "%{[@metadata][type]}"
        }
}
```

/etc/logstash/conf.d/bash.conf

```
input {
        beats {
                port => "5047"
        }
}


filter {
        if [log][file][path] == ../cmd.log" {
                grok {
                        match => { "message" => "%{MONTH} %{MONTHDAY}
%{HOUR}:%{MINUTE}:%{SECOND} %{NOTSPACE:bash_hostname} (?:.*): SESSION
= %{NOTSPACE:bash_session}, from_remote_host =
%{NOTSPACE:bash_from_remote_host}, USER = %{NOTSPACE:bash_user}, PWD =
%{NOTSPACE:bash_pwd}, CMD = %{GREEDYDATA:bash_cmd}" }
                }
        }
}

output {

        elasticsearch {
                hosts => ["localhost:9200"]
                index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
                document_type => "%{[@metadata][type]}"
        }
}
```

/etc/logstash/conf.d/beats.conf

```
input {
        beats {
                port => "5044"
        }
}

output {
        elasticsearch {
                hosts => ["localhost:9200"]
                index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
                document_type => "%{[@metadata][type]}"
        }
}
```

/etc/logstash/conf.d/custom_logs.conf

```
input {
        beats {
                port => "5045"
        }
}

filter {
    grok {
       match => { "message" =>
"%{TIMESTAMP_ISO8601:[@metadata][timestamp]}
%{LOGLEVEL:ais_level}%{SPACE}\[%{DATA:ais_threadname}
(?<ais_username>(\w)*)\] %{NOTSPACE:ais_logger}%{SPACE}-
(?<logMessage>(.|\r|\n)*)" }
    }

  if [ais_logger] == "Auth" and [ais_level] == "INFO" {
     grok {
        match => {
          "logMessage" =>
["%{NOTSPACE:ais_action}:IP=%{DATA:ais_clientip};session.id=%{DATA:ais
_session_id};user=%{DATA:ais_username2};remoteUser=%{DATA:ais_remote_u
ser};locale=%{NOTSPACE:ais_locale}(?:((;)?login)
(?<ais_action_result>(succes|fail)))",

"%{NOTSPACE:ais_action}:IP=%{DATA:ais_clientip};session.id=%{DATA:ais_
session_id};user=%{DATA:ais_username2};remoteUser=%{DATA:ais_remote_us
er};locale=%{NOTSPACE:ais_locale}(?:((;)?login)
(?<ais_action_result>(succes|fail)))(?:;%{GREEDYDATA:ais_submsg})",

"%{NOTSPACE:ais_action}:IP=%{DATA:ais_clientip};session.id=%{DATA:ais_
session_id};user=%{DATA:ais_username2};locale=%{NOTSPACE:ais_locale} -
(?:((;)?logout) (?<ais_action_result>(succes)))",

"%{NOTSPACE:ais_action}:IP=%{DATA:ais_clientip};session.id=%{DATA:ais_
session_id};user=%{DATA:ais_username2};remoteUser=%{DATA:ais_remote_us
er};locale=%{NOTSPACE:ais_locale};saml.subjectid=%{DATA:ais_subject_id
};loginResult=%{DATA:ais_action_result}(?:;%{GREEDYDATA:ais_submsg})",

"%{NOTSPACE:ais_action}:IP=%{DATA:ais_clientip};session.id=%{DATA:ais_
session_id};user=%{DATA:ais_username2};remoteUser=%{DATA:ais_remote_us
er};locale=%{NOTSPACE:ais_locale};loginResult=%{DATA:ais_action_result
}(?:;%{GREEDYDATA:ais_submsg})",
```

```
"%{NOTSPACE:ais_action}:IP=%{DATA:ais_clientip};session.id=%{DATA:ais_
session_id};user=%{DATA:ais_username2};remoteUser=%{DATA:ais_remote_us
er};locale=%{NOTSPACE:ais_locale}loginResult=%{NOTSPACE:ais_action_res
ult}"
                        ]
      }
    }
    geoip {
      source => "ais_clientip"
      target => "ais_clientip_geoip"
    }

  }

  if [ais_logger] == "a.p.MDCFilter" {
    grok {
       match => {
         "logMessage" =>
"%{DATA:logMessage2},\"req.userAgent\":\"%{DATA:ais_req_userAgent}\""
       }
    }

    kv {
       source => "logMessage2"
       field_split => ","
       value_split => ":"
       remove_char_key => "\"\{\}"
       trim_value => "\"\{\}"
       prefix => "ais_"
    }

    kv {
       source => "ais_req.queryString"
       field_split => "&"
       value_split => "="
       prefix => "ais_"
    }
  }

  if [ais_threadname] =~ "wuieApp" and [logMessage] =~ "\{"  {

    kv {
       source => "logMessage"
       field_split => ","
```

```
        value_split => ":"
        remove_char_key => "\"\{\}"
        trim_value => "\"\{\}"
        prefix => "ais_"
    }

    kv {
        source => "ais_req.queryString"
        field_split => "&"
        value_split => "="
        prefix => "ais_"
    }
  }
}

output {
        elasticsearch {
                hosts => ["localhost:9200"]
                index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
                document_type => "%{[@metadata][type]}"
        }
}
```

Príloha E: Časť konfiguračných súborov pre Filebeat

filebeat.yml

```
filebeat.inputs:

- type: log
  enabled: true
  paths:
    - ..vyvoj/ais.log.????-??-??_??
  fields:
   env: vyvoj
   log_type: webapp
   log_name: ais
  multiline.pattern: ^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-
9]{2}
  multiline.negate: true
  multiline.match: after

- type: log
  enabled: true
  paths:
    - ..test/ais.log.????-??-??_??
  fields:
   env: test
   log_type: webapp
   log_name: ais
  multiline.pattern: ^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-
9]{2}
  multiline.negate: true
  multiline.match: after

- type: log
  enabled: true
  paths:
    - ..beta/ais.log.????-??-??_??
  fields:
   env: beta
   log_type: webapp
   log_name: ais
  multiline.pattern: ^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-
9]{2}
  multiline.negate: true
  multiline.match: after

- type: log
  enabled: true

  paths:
    - ..vyvoj-el/ais.log.????-??-??_??
  fields:
```

```
   env: vyvoj-el
   log_type: webapp
   log_name: ais
  multiline.pattern: ^[0-9]{4}-[0-9]{2}-[0-9]{2} [0-9]{2}:[0-9]{2}:[0-
9]{2}
  multiline.negate: true
  multiline.match: after

- type: log
  enabled: true
  paths:
    - ../cmd.log
  fields:
   log_name: ais
```

apache2.yml

```
- module: apache
  # Access logs
  access:
    enabled: true
    var.paths: ..vyvoj/accessFilebeat.log.*", ..vyvoj-
el/accessFilebeat.log.*", "..test/accessFilebeat.log.*", "..test-
el/accessFilebeat.log.*", "..beta/accessFilebeat.log.*", "beta-
el/accessFilebeat.log.*"]
```

auditd.yml

```
- module: auditd
  log:
    enabled: true
    var.paths: ["../audit.log"]
```