Manažment bezpečnostných informácií a udalosti pre akademický informačný systém

Analýza a návrh riešenia

Eva Marková

Abstrakt. 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. Pri implementácii zohľadníme MITRE ATT&CK rámec a tiež ISO/IEC 27000 a následne tento systém budeme optimalizovať.

Kľúčové slová: akademický informačný systém, ISO/IEC 27000, MITRE ATT&CK, SIEM

1 Úvod

Informačné systémy sú v organizáciách častokrát kritickými infraštruktúrami, ktoré je potrebné zabezpečiť a zabúda sa na nich, až do chvíle, kým nie je zaznamenaný bezpečnostný incident. Bezpečnostný incident je udalosť, ktorá bezprostredne ohrozila aktívum alebo činnosť organizácie. Informačný systém je infraštruktúra (informačné a komunikačné prostriedky), ktorej znefunkčnenie, resp. ochromenie má za následok negatívny vplyv na organizáciu a jej procesy. V akademickom prostredí sú najdôležitejšími procesmi zabezpečenie výučby a výskumnej činnosti. Z tohto dôvodu môžeme okrem iných zaradiť medzi kritickú infraštruktúru akademických inštitúcií aj 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 informácií. 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. Potom musí centrum bezpečnostných operácií (Security Operations Center, SOC) pochopiť, ktoré aktíva ovplyvňujú ktoré procesy a aplikácie, implementovať monitorovanie a pochopiť, ako útočník myslí a následne implementovať pravidlá, pomocou ktorých ich identifikuje [1].

Hlavným cieľom práce je navrhnúť vhodný SIEM systém, ktorý by zohľadňoval akademické prostredie a aktíva, zraniteľnosti, hrozby a typy útočníkov akademických informačných systémov. Z 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 podcieľoch. V prvom cieli práce sa zameriavame na analýzu a porovnanie aktuálnych prístupov k manažmentu bezpečnostných informácií a udalosti (SIEM). Jednou z možností je porovnanie implementácií rôznych SIEM systémov ako napríklad Elastic Stack [2], AlienVault OSSIM [3], IBM QRadar [4], Splunk [5] atď. SIEM systémy tiež porovnáme podľa toho, aký princíp modelovania bezpečnostných hrozieb využívajú. Na základe vykonanej analýzy sa rozhodneme, aký SIEM systém je pre riešenie nášho problému najvhodnejší.

Súčasťou druhého cieľa je pripraviť podrobnú analýzu bezpečnostných rizík pre akademický informačný systém na našej univerzite podľa noriem ISO/IEC 27000 vrátane zohľadnenia MITRE ATT&CK rámca. Tento rámec nám primárne poslúži na špecifikáciu relevantných bezpečnostných hrozieb a zraniteľností.

Vybrané hrozby odsimulujeme na testovacom serveri, aby sme následne boli schopní vytvoriť pravidlá pre detekciu útokov na akademickom informačnom systéme. Tiež bude potrebné navrhnúť dátový model, s ktorým budeme pracovať.

Posledným cieľom je návrh a implementácia samotného SIEM systému pre akademický informačný systém. Aby bol systém efektívny, je potrebné zamerať sa aj na optimalizáciu nami zadefinovaných pravidiel na detekciu.

2 Security Information and Event Management (SIEM)

SIEM systém v sebe predstavuje kombináciu štyroch prvkov [6]:

- SIM – Manažment bezpečnostných informácií (Security Information Management),
- SEM – Manažment bezpečnostných udalostí (Security Event Management),
- LMS – Systém manažovania logov (Log Management System) a
- SEC – Korelácia bezpečnostných udalostí (Security Event Correlation).

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 logov (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 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 narušaniu 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 a samotné aktíva generujú mnoho bezpečnostných udalostí.

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. Napríklad umožňujú pracovať s nástenkou 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 [7]:

- 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 umožňujú analýzu organizácie v reálnom čase. Poskytovanie upozornení o živej aktivite alebo útokoch na vykonanie defenzívnych meraní.

Threat intelligence 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.

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 bude pomáhať pri upozorňovaní na akékoľvek odchýlky od normálneho správania.

Monitorovanie údajov a používateľov sa zameriava na autentifikáciu a autorizáciu používateľov. Spočiatku sa vykoná autentifikácia užívateľa a potom skontroluje autorizované súbory, 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.

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.

Analýza umožňuje objavovanie, interpretáciu zmysluplných vzorov v analýze bezpečnosti údajov, ktorá sa skladá zo zobrazení násteniek, zostáv a funkcií dotazov. Vykonáva vyšetrovanie činnosti používateľa a prístupu k zdrojom s cieľom identifikovať bezpečnostnú hrozbu, porušenie alebo zneužitie oprávnenia.

2.1 Rôzne implementácie SIEM systémov

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 riešenia založené na otvorenom kóde (open-soruce), ako aj platené riešenia.

2.1.1 Elastic Stack

Elastic Stack [2] 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 2 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 logov a správ, ich spracovanie úpravou alebo doplnením logovacích dát a ich následné posunutie do Elasticsearch. Posielanie logov 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 logov z rôznych zdrojov. Zvyčajne posielajú dáta priamo do Logstash alebo Elasticsearch. Metricbeat slúži na čítanie logov z operačného systému a aplikácií. Packetbeat monitoruje sieť. Winlogbeat číta logy 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. Je schopný zasielať notifikácie na email, kolaboračné nástroje a podobne. Tiež je možné si doinštalovať akékoľvek nástroje a doplnky, ktoré sú potrebné na správne zhromažďovanie a spracovávanie informácií.

2.1.2 AlienVault OSSIM

AlienVault OSSIM [3] 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) [8], čo umožňuje užívateľom prispievať a prijímať informácie o škodlivých hostiteľoch v reálnom čase. Okrem toho je AlienVault OSSIM neustále vyvíjaný. OSSIM obsahuje nasledujúce softvérové komponenty [9]:

- PRADS [10], používané na identifikáciu hostiteľov a služieb pasívnym monitorovaním sieťovej prevádzky.
- Snort [11], ktorý sa používa ako systém detekcie narušenia (IDS) a tiež sa používa na krížovú koreláciu s OpenVAS.
- Suricata [12] tiež používaná ako IDS systém.
- TCPtrack [13] používaný na informácie o reláciách, ktoré môžu poskytnúť užitočné informácie na koreláciu útoku.
- Munin [14] na analýzu trafiky a „watchdogging“.
- NFSen [15] / NFDump [16], ktorý sa používa na zhromažďovanie a analýzu informácií NetFlow.
- FProbe [17], ktorý sa používa na generovanie údajov NetFlow zo zachytenej prevádzky.
- Nagios [18], ktorý sa používa na monitorovanie hostiteľov a špecifikovaných portov z hľadiska dostupnosti aktív a úplného monitorovania miestneho systému.
- OpenVas [19] 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. Hlavnou nevýhodou týchto riešení je obmedzená funkčnosť agregácie prijatých správ.

2.1.3 IBM QRadar

IBM QRadar SIEM [4] 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 udalosti súvisiace s konkrétnou bezpečnostnou hrozbou na jednom mieste. Tým sa eliminujú procesy manuálneho sledovania a bolo umožnené analytikom zamerať sa na vyšetrovanie a reakciu. 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.

2.1.4 ArcSight

Arcsight [20] 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. V prípade geograficky distribuovaných organizácií je potrebné preniesť všetky udalosti do centrálnej databázy, kde sa vykonáva celé spracovanie. 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. To znamená, že ArcSight je zameraný na veľké korporácie.

ArcSight SIEM [21] 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. Hlavnou výhodou tohto modelov je schopnosť dosiahnuť distribúciu záťaže a tiež sa vyhýba preťaženiu siete tým, že zasiela iba zachytené údaje podmnožiny rodičovi na analýzu.

2.1.5 Splunk

Splunk [5] produkty pre podniky a cloud pomáhajú pri vyhľadávaní, upozorňovaní, korelácii v reálnom čase a vizualizácii. Môže byť nainštalovaný ako softvér vo verejnom alebo súkromnom cloude alebo ako softvér ako služba (SaaS). Splunk poskytuje flexibilné analytické nástenky, ktoré vylepšujú vizualizačné schopnosti. Jeho silná vizualizácia a behaviorálna prediktívna a štatistická analýza pomáhajú odhaliť množstvo informácií o hrozbách z komerčných a zdrojov s otvoreným kódom.

Splunk možno použiť na budovanie a prevádzkovanie bezpečnostných operačných centier akejkoľvek veľkosti. Podporuje celú škálu operácií informačnej bezpečnosti vrátane hodnotenia polohy, monitorovania, spracovania výstrah a incidentov, analýzy a reakcie na porušenie a korelácie udalostí. Je schopný odhaľovať známe aj neznáme hrozby, skúmať ich, určovať dodržiavanie predpisov a používa pokročilú bezpečnostnú analýzu.

Tabuľka 1. Porovnanie rôznych implementácií SIEM systémov

SIEM	Open-source	Neobmedzená trafika	Vizualizácia dát	Inštalácia	Platformy
Elastic Stack	✓	✓	✓	Náročná	Windows, Linux, MacOS
AlienVault OSSIM	✓	✓	✓	Náročná	Windows, Linux, MacOS
IBM QRadar	X	✓	✓	Jednoduchá	Linux
ArcSight	X	✓	✓	Jednoduchá	Windows
Splunk	X	✓	✓	Jednoduchá	Windows, Linux, MacOS
Splunk Free	✓	X	✓	Jednoduchá	Windows, Linux, MacOS

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. 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. Vzhľadom

k tomu, že Elastic Stack poskytuje možnosť voľby nástrojov a tiež možnosť voľby Beats nástrojov, rozhodli sme sa pre túto možnosť.

2.2 Analýza rizík

Analýzu rizík [22] 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 [22].

Kvantitatívna analýza rizík využíva číselné hodnoty pre dopady, 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.

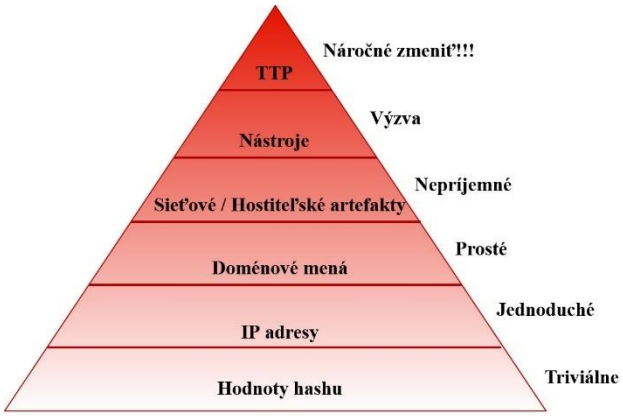
3 MITRE ATT&CK

MITRE ATT&CK [23] 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 [24]:

• 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. Zameriava sa na to, ako externí protivníci kompromitujú a pôsobia v rámci počítačových informačných sietí. 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. 1 Pyramída bolesti

Na obrázku č. 1 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” spôsobí útočníkovi, keď im tieto indikátory odoprieme. Rámec MITRE ATT&CK sa podľa modelu „pyramídy bolesti“ (obr. 1) zaoberá práve taktikami, technikami

a procedúrami, 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.

3.1 Podrobnejšia štruktúra ATT&CK

Vzťah medzi taktikami, technikami a čiastočnými technikami je vizualizovaný v 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 [25].

ATT&CK je organizovaná do „**technologických domén [25]**:

- 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.

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. Procedúry sú tiež dôležitým komponentom TTP konceptu. Sú to špecifické implementácie techník a čiastočných techník, ktoré boli použité útočníkmi.

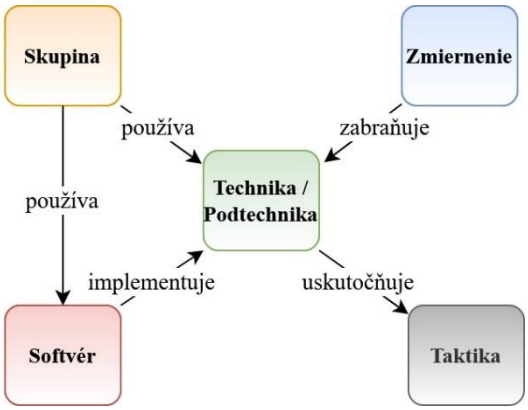
Známi protivníci, ktorí sú sledovaní a nahlasovaní verejnými a súkromnými organizáciami, sú označovaní v ATT&CK v **skupinách**. Skupiny sú definované ako pomenované skupiny narušenia, skupiny hrozieb, skupiny „hercov“ alebo kampaní, ktoré zvyčajne predstavujú cielenú a pretrvávajúcu aktivitu hrozieb. ATT&CK sa primárne zameriava na APT skupiny, no zahŕňa aj iné pokročilé skupiny, ako napríklad finančne motivovaní aktéri. Skupiny môžu používať techniky priamo alebo využívať softvér, ktorý implementuje techniky.

Útočníci bežne používajú pri prienikoch rôzne typy **softvéru**. Softvér je rozdelený do dvoch hlavných kategórií – nástroje a malvér. Nástroj je komerčný, s otvoreným kódom, vstavaný alebo verejne prístupný softvér, ktorý by mohol použiť obranca, člen „red team-u“, penetračný tester alebo útočník. Táto kategória zahŕňa softvér, ktorý sa všeobecne nenachádza v organizácii, ako aj softvér, ktorý je všeobecne dostupný ako súčasť operačného systému. Medzi nástroje patria napríklad PsExec, Metasploit, Mimikatz, ale aj nástroje vo Windows-e ako Net, netstat, Tasklist a podobne. Malvér

je komerčný softvér, ktorý môže, ale nemusí byť open-source a je určený na škodlivé účely. Medzi malvér radíme napríklad PlugX alebo CHOPSTICK a podobne.

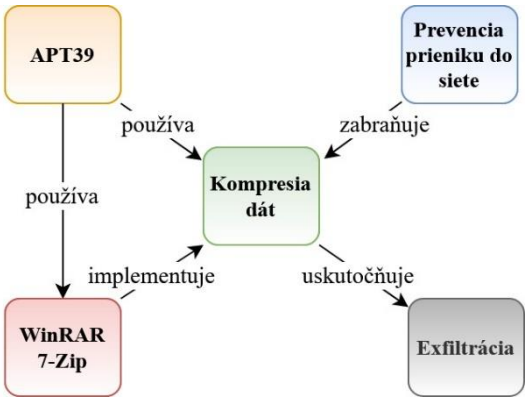
Zmiernenia v ATT&CK predstavujú bezpečnostné koncepcie a triedy technológií, ktoré možno použiť na zabránenie úspešnému vykonaniu techniky alebo čiastočnej techniky.

Každá zložka ATT&CK nejakým spôsobom súvisí s inými komponentmi. Vzťahy opísané vyššie je možné znázorniť na obrázku č. 2.



Obr. 2 Vzťahy komponentov rámca MITRE ATT&CK

Na obrázku č. 3 môžeme vidieť znázornené vzťahy pre prípad, keď APT39 používa WinRAR alebo 7-Zip na kompresiu archivovaných ukradnutých dát:



Obr. 3 Vzťahy komponentov rámca MITRE ATT&CK – príklad

3.2 Mapovanie dát do ATT&CK

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 ATT&CK môžeme z 2 rôznych zdrojov dát – buď priamo z reportu, alebo z pôvodných (raw) dát. Mapovanie z reportu zahŕňa 6 krokov [26]:

1. Pochopenie útoku
2. Nájdenie vykonanej činnosti
3. Preskúmanie činnosti
4. "Preloženie" činnosti na taktiku
5. Zistenie, aká technika bola použitá
6. Porovnanie výsledkov s inými analytikmi

Pochopenie útoku je veľmi dôležitým krokom pri mapovaní, keďže nie každý útok sa dá hneď na prvý pohľad analyzovať. Preto je potrebné podrobné preštudovanie reportu, prípadne nájdenie relevantných informácií na internete.

Pri hľadaní vykonanej činnosti je potrebné zamerať sa na to, čo robil útočník prípadne softvér na danom počítači. 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 12 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 list 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 zodpovedať si na niekoľko otázok. Pre koho majú byť tieto dáta? Na koľko chceme byť detailní pri vykonávaní tohto mapovania? Ako to bude prepojené s inými informáciami? Akým spôsobom sa budú importovať a exportovať dáta?

Jednou z možností je ukladať si tieto veci napríklad do Excelu, ale MITRE ATT&CK rámec nám ponúka tzv. navigátor [27], 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.

3.3 Vytváranie odporúčaní z techník

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

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
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 hrozieb. Ďalej je potrebné preskúmať, ako sa tieto techniky používajú, presnejšie, 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 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.

4 Návrh riešenia

V predošlých kapitolách sme sa pozreli na existujúce implementácie rôznych 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. Pomocou Beats nástrojov môžeme sledovať správanie serverov, na ktorých je nasadený akademický informačný systém. Použijeme Metricbeat, Packetbeat a tiež si pomocou Libbeat vytvoríme vlastný nástroj, aby sme monitorovali logy, ktoré sú relevantné.

AiS2 v podstate 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 bez problémov nasadíme na zvyšné dva. Architektúru AiS2 možno popísať ako klient-server architektúru. V rámci tejto architektúry klient odosiela http, resp. https požiadavku na webový server Apache2. 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 logov, a to v súboroch acces.log, error.log, catalina.log a ais.log.

Po nasadení SIEM systému na testovací server chceme simulovať rôzne útoky a zaznamenávať logy, ktoré sú generované, aby sme následne vedeli tieto bezpečnostné hrozby identifikovať v prípade, že nastanú. Pred samotnou simuláciou útokov na testovacom serveri je potrebné si určiť z MITRE ATT&CK rámca skupinu techník, ktoré budeme pozorovať.

Súčasťou posledného cieľa je tiež optimalizácia tohto SIEM systému. Teda bude potrebné zvážiť nakoľko, je ktorý atribút v daných logoch potrebný a dôležitý. Chceme, aby náš SIEM systém bol efektívny a škálovateľný pre rôzne akademické informačné systémy, nie len pre systém AiS2.

5 Záver

V tomto článku sme vysvetlili, čo predstavuje pojem SIEM systém. Načrtli sme, ako funguje MITRE ATT&CK rámec a ako ho plánujeme využiť v našej práci. Tiež sme popísali niekoľko rôznych implementácií SIEM systémov, pričom sme ich porovnali a vybrali ten najlepší pre účel monitorovania akademického informačného systému.

V rámci práce tiež plánujeme navrhnúť vhodný dátový model, s ktorým budeme pracovať. Následne vytvoríme pravidlá detekcie s ohľadom na normy rodiny ISO/IEC 27000 a MITRE ATT&CK rámec.

Cieľom práce je vytvoriť škálovateľný SIEM systém, ktorý bude možné použiť pre akýkoľvek akademický informačný systém. Systém bude schopný identifikovať bezpečnostné hrozby z relevantnej množiny hrozieb a následne to nahlásiť správcovi systému. Výsledky práce bude možné aplikovať všeobecne na akademické informačné systémy. Akademický informačný systém AiS2 používame v rámci práce ako prípadovú štúdiu.

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. Elastic [online]. [cit. 2019-12-02]. Dostupné z: https://www.elastic.co/products/siem
3. AlienVault [online]. [cit. 2019-12-02]. Dostupné z: https://cybersecurity.att.com/products/ossim
4. IBM QRadar [online]. [cit. 2019-12-02]. Dostupné z: https://www.ibm.com/us-en/marketplace/ibm-qradar-siem
5. Splunk [online]. [cit. 2019-12-02]. Dostupné z: https://www.splunk.com/en_us/siem-security-information-and-event-management.html
6. SIEM [online]. [cit. 2019-12-02]. Dostupné z: https://logdna.com/what-is-siem
7. 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.
8. AlienVault Open Threat Exchange (OTX) [online]. [cit. 2020-06-15]. Dostupné z: https://otx.alienvault.com/
9. 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
10. PRADS [online]. [cit. 2020-06-15]. Dostupné z: https://github.com/gamelinux/prads
11. Snort [online]. [cit. 2020-06-15]. Dostupné z: https://www.snort.org/
12. Suricata IDS [online]. [cit. 2020-06-15]. Dostupné z: https://suricata-ids.org/]
13. TCPtrack [online]. [cit. 2020-06-15]. Dostupné z: https://linux.die.net/man/1/tcptrack
14. Munin [online]. [cit. 2020-06-15]. Dostupné z: http://munin-monitoring.org/
15. NFsen [online]. [cit. 2020-06-15]. Dostupné z: http://nfsen.sourceforge.net/
16. NFdump [online]. [cit. 2020-06-15]. Dostupné z: http://nfdump.sourceforge.net/
17. FProbe [online]. [cit. 2020-06-15]. Dostupné z: http://manpages.ubuntu.com/manpages/bionic/man8/fprobe.8.html
18. Nagios [online]. [cit. 2020-06-15]. Dostupné z: https://www.nagios.org/
19. OpenVAS [online]. [cit. 2020-06-15]. Dostupné z: https://openvas.org/
20. ArcSight SIEM [online]. [cit. 2020-06-07]. Dostupné z: https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview
21. RAJA, M. Siva Niranjan; VASUDEVAN, A. R. Rule Generation for TCP SYN Flood attack in SIEM Environment. Procedia computer science, 2017, 115: 580-587.
22. ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management.
23. Rámec Mitre Attack [online]. [cit. 2019-12-02]. Dostupné z: https://attack.mitre.org/
24. STROM, Blake E., et al. Finding cyber threats with ATT&CK-based analytics. Technical Report MTR170202, MITRE, 2017.
25. STROM, Blake E., et al. Mitre att&ck: Design and philosophy. Technical report, 2018.
26. Mitre Attack tréning [online]. [cit. 2020-06-07]. Dostupné z:]https://attack.mitre.org/resources/training/cti/
27. Mitre Attack navigator [online]. [cit. 2020-06-07]. Dostupné z: https://mitre-attack.github.io/attack-navigator/enterprise/