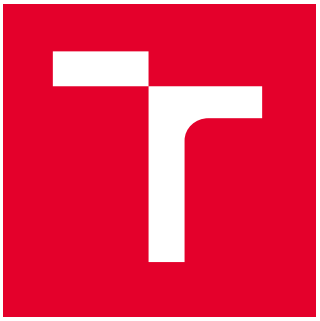


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

NÁSTROJ PRO GENERALIZACI AUTOMATIZOVANÝCH SOAR SCÉNÁŘŮ PRO SDÍLENÍ ZNALOSTÍ V ODVĚTVÍ POČÍTAČOVÉ BEZPEČNOSTI

TOOL FOR GENERALIZING AUTOMATED SOAR SCENARIOS FOR CYBERSECURITY KNOWLEDGE SHARING

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — **Miriam Ištoňová**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Yehor Safonov**

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Miriam Ištoňová ***ID:*** 241038

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

NÁZEV TÉMATU:

Nástroj pro generalizaci automatizovaných SOAR scénářů pro sdílení znalostí v odvětví počítačové bezpečnosti

POKYNY PRO VYPRACOVÁNÍ:

Hlavním cílem bakalářské práce je návrh a implementace nástroje sloužící pro generalizaci automatizovaných SOAR scénářů (playbooků) s cílem efektivního sdělování znalostí reakce na kyberbezpečností incidenty. V rámci bakalářské práce bude provedena analýza volně dostupných playbooků a vhodných datových struktur pro jejich správu (např. COPS, CACAO). Obecný SOAR formát bude reprezentován vhodnými datovými strukturami, umožňujícími efektivně popsat kroky reakce na KBI. Navržená aplikace bude provádět automatickou konverzi jednoho vybraného SOAR formátu na jeho generalizovanou podobu. V teoretické části argumentujte specifika moderních formátů pro ukládání SOAR playbooků, nastudujte problematiku bezpečnostního monitoringu, popište hlavní rozdíly mezi SIEM a SOAR systémy, vysvětlete principy automatické reakce na incidenty a hierarchii SOC. Zaměřte se na existující techniky tvorby playbooků a možností exportu (např. Splunk SOAR, QRadar SOAR, Chronicle SOAR a další). Identifikované poznatky integrujte do nástroje.

DOPORUČENÁ LITERATURA:

[1] BOLLINGER, Jeff, Brandon ENRIGHT a Matthew VALITES. Crafting the InfoSec playbook: security monitoring and incident response master plan. Beijing: O'Reilly, [2015]. ISBN 1491949406.

[2] MARTINEZ, Roberto Incident Response with Threat Intelligence. Packt Publishing, 2022. ISBN 1801070997.

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

Vedoucí práce: Ing. Yehor Safonov

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

ABSTRAKT

Dnešnú dobu by bolo možné definovať ako množstvo, rýchlosť a možnosti. Dohľadové centrá bezpečnosti zareagovali na výzvu množstva neutíchajúcich informácií nástrojom monitorovania a kategorizácie ako je SIEM. Avšak v prípade samotných incidentov, ponúka svoju rýchlosť a automatizáciu reakcie vyspelé riešenie SOAR. Ako každá technológia aj SOAR ponúkaný rôznymi spoločnosťami, prispieva ku možnostiam jednotlivých štruktúr a formátov scenáru reakcie, čo prináša jasnú výzvu zjednodušenia, spolupráce a generalizácie.

Bakalárska práca sa preto zameriava na realizáciu nástroja konverzie, s cieľom zjednotenia a zovšeobecnenia formátu automatizovaných SOAR scenárov za pomoci využitia vyvíjajúceho sa playbook štandardu CACAO. Hlavným prínosom nástroja je možnosť zjednotenia použitia SOAR scenárov, zabezpečenie úspešnej konverzie a tým zjednodušenie zdieľania znalostí v oblasti počítačovej bezpečnosti.

Teoretická časť práce teda popisuje aktuálnu problematiku bezpečnostného monitoringu, vysvetľuje dôležitosť automatizácie v rámci reakcie na incidenty a ponúka podrobnú analýzu a zrovnanie dostupných technológií a formátov scenárov automatickej reakcie na incidenty. Praktická časť je úzko spojená a závisí na výsledkoch analýzy. Zameriava sa na voľbu a návrh vhodného formátu popisu jednotlivých scenárov automatickej reakcie ako hlavne následnej implementácii samotného nástroja konverzie.

KĽÚČOVÉ SLOVÁ

SOAR, playbook, scenár, konverzia, formát, CACAO, SIEM, SOC, generalizácia

ABSTRACT

Today's era could be defined as quantity, speed and possibilities. Security monitoring centers have responded to the challenge of an unrelenting amount of information with monitoring and categorization tools such as SIEM. However, in case of incidents themselves, the speed and automation of response is offered by an advanced SOAR solution. Like any technology, SOAR offered by different companies also contributes to the variety of individual response scenario structures and formats, bringing the clear challenge of simplification, collaboration and generalization.

Therefore, the bachelor thesis focuses on the implementation of a conversion tool, with the goal of unifying and generalizing the format of automated SOAR scenarios using the evolving CACAO playbook standard. The main benefit of the tool is the ability to unify the use of SOAR scenarios, ensure successful conversion and thus facilitate knowledge sharing in the field of cybersecurity.

The theoretical part of this thesis focuses on the current issue of security monitoring, explains the importance of automation within incident response and offers a detailed analysis and comparison of available technologies and formats of automated incident response playbooks. The practical part is closely related and depends on the results of the analysis. It focuses on the selection and design of a suitable format for the description of the individual automatic response scenarios as well as the following final implementation of the conversion tool itself.

KEYWORDS

SOAR, playbook, scenario, conversion, format, CACAO, SIEM, SOC, generalization

IŠTOŇOVÁ, Miriam. *Nástroj pro generalizaci automatizovaných SOAR scénářů pro sdílení znalostí v odvětví počítačové bezpečnosti*. Bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024. Vedúci práce: Ing. Yehor Safonov

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Miriam Ištoňová
VUT ID autora:	241038
Typ práce:	Bakalárska práca
Akademický rok:	2023/24
Téma závěrečnej práce:	Nástroj pro generalizaci automatizovaných SOAR scénářů pro sdílení znalostí v odvětví počítačové bezpečnosti

Vyhlasujem, že svoju záverečnú prácu som vypracovala samostatne pod vedením vedúcej/cého záverečnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autorka uvedenej záverečnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto záverečnej práce som neporušila autorské práva tretích osôb, najmä som nezasiahla nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomá následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autorky*

*Autor podpisuje iba v tlačenej verzii.

POĎAKOVANIE

Rada by som sa poďakovala vedúcemu mojej bakalárskej práce, pánovi Ing. Yehorovi Safonovi, za odborné vedenie počas konzultácií, podnetné návrhy, pripomienky k práci, trpezlivosť a neustálu podporu a pomoc. Veľká vďaka patrí tiež Tomášovi Veverkovi za nenahraditeľné rady vždy v ten správny čas. V neposlednom rade ďakujem mojej rodine a priateľom, za neutíchajúcu podporu počas celého štúdia.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Detekčné operačné centrá (SOC) reagujú na rýchlosť dnešnej doby a záplavy dát ohľadom kyberbezpečnostných incidentov (KBI) využívaním rôznych technológií a nasadzovaním automatizácie. Medzi základný nástroj monitorovania patrí SIEM a vrchol automatizácie reakcie na incidenty sa dosahuje riešením SOAR. SOAR ponúka nespočetné množstvo scenárov, inak povedané rozhodovacích postupov či playbookov, ktoré umožňujú definíciu a automatické vykonanie konkrétnych predefinovaných krokov. [2]

Existuje však mnoho spoločností, ktoré toto riešenie ponúka a ich jednotlivé scenáre nie sú vôbec identické, čo prináša výhodu proprietárnosti, no výzvu zovšeobecnenia, zjednotenia a zdieľania verejnosti. Cieľom tejto bakalárskej práce je preto návrh a následne samotná realizácia nástroja konverzie, s dôrazom na zjednotenie a generalizáciu formátu automatizovaných SOAR scenárov za pomoci využitia vyvíjajúceho sa playbook štandardu CACAO. Finálny, prakticky použitý generalizovaný CACAO formát týchto prekonvertovaných scenárov vychádza z podrobnej analýzy dostupných formátov a SOAR riešení od dvanástich spoločností. Hlavným prínosom samotného nástroja konverzie je teda vízia zovšeobecnenia formátu použitia SOAR scenárov, zabezpečenie úspešnej konverzie scenárov od spoločnosti Splunk a tým zjednodušenie zdieľania znalostí v oblasti počítačovej bezpečnosti.

Bakalárska práca sa celkovo delí na 6 kapitol, z ktorých je prvá polovica venovaná teoretickej a druhá praktickej časti. Úvodná kapitola sa venuje základným pojmom problematiky bezpečnostného monitoringu, stratégii a fungovaniu SOC centra. Obsahuje tiež vysvetlenie a porovnanie technológií SIEM a SOAR (viď časť 1.5). Druhá kapitola sa venuje ako princípom automatizácie, definícií scenáru automatickej reakcie, tak jej hlavnému posolstvu a vyobrazeniu analýzy dostupných SOAR riešení (viď časť 2.3.) V tretej kapitole, ktorá tvorí základ pre voľbu finálneho generalizovaného formátu, sa zameriava na podrobnú analýzu dostupných formátov a štandardov ako je Sigma (v súvislosti so SIEM), COPS a CACAO, z ktorého následne vychádza samotný návrh štruktúry finálneho konvertovaného scenára.

Štvrtou kapitolou sa cez návrh finálnej štruktúry scenára, jej následne aplikovanie v prvotnej manuálnej transformácií a popisu požiadaviek nástroja konverzie, dostáva k samotnej praktickej časti implementácii nástroja. V piatej kapitole realizácie konvertora sú popísané použité technológie a jazyky, vysvetlená logika spôsobu konverzie, podrobne zosumarizované tabuľky všetkých použitých parametrov v rámci scenára, ukážka finálneho výstupu generalizovaného scenára a vysvetlený integrovaný záznam logov. Posledná kapitola sa venuje testovaniu konverzie a využitiu výstupného scenára ako vstupu pre jeho grafické znázornenie v aplikácii SOAR PLAYBOOK DESIGNER.

V neposlednom rade je na konci práce možné nájsť jednotlivé prílohy, ktorých súčasťou je rozsiahlejšia ukážka dostupných štandardov, podoba originálu a manuálne transformovanej verzie ukážkových scenárov z podkapitoly 4.2 a taktiež samotný návod na spustenie vytvoreného nástroja a popis obsahu elektronickej prílohy tejto bakalárskej práce.

1 Úvod do rozvíjajúcej sa problematiky bezpečnostného monitoringu

Pre pochopenie kontextu a základných súvislostí, ktoré sú spojené s riešením SOAR technológie, je nevyhnutné vysvetlenie základných pojmov, princípov a nástrojov bezpečnostného monitoringu. SOAR je neoddeliteľnou súčasťou tejto problematiky a preto budú potrebné informácie zdelené v tejto kapitole.

1.1 Význam a princíp fungovania bezpečnostného dohľadového centra

SOC je organizovaná skupina kyberšpecialistov, ktorá sa zaoberá kybernetickou obranou a riešením kyberbezpečnostných incidentov. Úlohou organizovaného SOC tímu je hlavne prevencia, detekcia, analýza a reakcia s prípadným reportom vzhľadom na zaznamenané bezpečnostné incidenty.[1]

Za bezpečnostný incident sa považuje akcia podniknutá prostredníctvom použitia informačného systému alebo siete, ktorej výsledkom je skutočný alebo potencionálne nepriaznivý vplyv na tento systém alebo sieť, ktorého je súčasťou, či na dáta v ňom uložené. Incidentu predchádza udalosť, za ktorú je považovaný akýkoľvek pozorovaný výskyt v systéme a/alebo v sieti. SOC dennodenne typicky pracuje s niekoľkými miliónmi až desiatkami miliárd bezpečnostných udalostí. Môže to byť napríklad pripojenie užívateľa k zdieľanému súboru, čo samozrejme za bežných okolností nie je identifikované ako škodlivá či nepriaznivá aktivita. V prípade ak by, ale mohlo ísť o potencionálny útok, prichádzame k pojmu *alert*. Alert je technické upozornenie, že k udalosti došlo. Typickým generátorom alertov je napríklad SIEM, za ktorý zodpovedá SOC a je dôležitým pojmom v tejto problematike a bude mu neskôr venovaná bližšia pozornosť.[1]

Existujú tri najbežnejšie typy dohľadových centier: interné, externé a virtuálne. Interný SOC je reprezentovaný zamestnancami pracujúcimi na plný úväzok v konkrétnom spoločnom priestore s prístupom k infraštuktúre. Externý SOC sa líši tým, že niektoré až všetky funkcie sú spravované externým poskytovateľom spravovaných bezpečnostných služieb (MSSP[1]), ktorý sa špecializuje na anlýzu a reakciu na incidenty. Ďalšou možnosťou je ešte virtuálny SOC, kde sa zamestnanci väčšinou nenachádzajú na konkrétnom pracovisku a sú to obvykle ľudia na čiastočný úväzok alebo na dohodu, ktorí spolupracujú podľa vopred stanovených noriem a predpisov danej organizácie.[2]

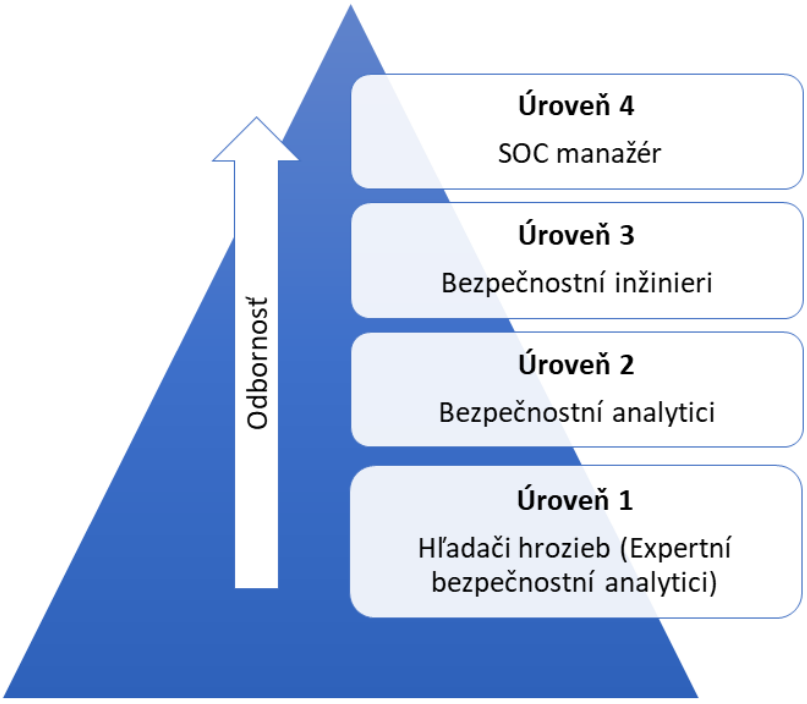
[1]MSSP (*Managed Security Service Provider*) – externý poskytovateľ bezpečnostných služieb.

Aktivity, úlohy a zodpovednosti dohľadových centier bezpečnosti sa teda delia do troch základných kategórií [3]:

- **Príprava, plánovanie a prevencia** – zahŕňa udržiavanie inventáru všetkého, čo treba chrániť, vykonávanie údržby systémov, plánovanie reakcie na incidenty a pravidelné testovanie a hodnotenie zraniteľností (slabých miest systému),
- **Monitorovanie, detekcia a reakcia** – zahŕňa neustále monitorovanie jednotlivých zariadení či celej infraštruktúry, správu logov (alertov), detekciu potencionálnych útokov či hrozieb a konkrétne postupy ako reakciu na incidenty,
- **Zotavenie sa, obnova a plnenie predpisov** – zahŕňa zotavenie a obnovenie po konkrétnych spôsobených škodách, využitie získaných informácií z daného incidentu a poučenie sa do budúcna či dodržiavanie a správa všeobecne platných predpisov.

Hierarchia SOC

SOC sa primárne delí na 4 základné úrovne (obrázok 1.1). S výškou úrovne stúpa aj level odbornosti.



Obr. 1.1: Základná hierarchia SOC [4].

Na úrovni 1 sa nachádzajú hľadači hrozieb (expertní bezpečnostní analytici), ktorí sa špecializujú na zisťovanie a obmedzovanie všetkého čo by mohlo byť potencionálne ohrozujúce. Úroveň 2 schováva bezpečnostných analytikov, ktorí ako prví reagujú na bezpečnostné incidenty. Zisťujú, vyšetrujú, prioritizujú hrozby a následne identifikujú postihnuté miesta či užívateľov, ktorým navrhujú vhodné opatrenia. Bezpečnostní inžinieri sú zodpovední za správu samotnej architektúry organizácie. Testujú, implementujú a udržiavajú jej samotný bezpečný chod. Na najvyššej úrovni samotný SOC manažér je ten, ktorý na všetko dohliada a zodpovedá sa priamo hlavnému bezpečnostnému manažérovi organizácie (CISO[2]). [3]

1.2 Stratégia monitoringu a reakcie na kybernetické incidenty

Výsledkom spoľahlivého monitorovania je reakcia na jeho zachytené události a incidenty. Za reakciu na incident sa považuje teda organizovaný, strategický prístup k detekcii a riadeniu kyberbezpečnostných útokov. To navyše takým spôsobom, aby sa minimalizovali škody, doba zotavenia či celkové náklady organizácie. Plán reakcie na incidenty by mal teda odpovedať na 4 základné otázky – Čo? Kto? Kedy? Ako? Medzi základné monitorovacie nástroje patrí SIEM a jeho najnovší nasledovník SOAR, ktorý sa zameriava na samotnú reakciu a spracovanie incidentov. Oba tieto nástroje budú podrobnejšie porovnané v nasledujúcej podkapitole 1.3. [5]

Zameranie tejto podkapitoly sa však venuje používaným stratégiam vrámci SOC. Za tradičnú stratégiu je považované podrobné monitorovanie, kategorizácia a riešenie logov – teda alertov, ktoré vygeneruje SIEM. Alternatíva a nový prístup s integráciou SIEM riešení prináša tzv. OODA[3] kruh, vykreslený na obrázku 1.2 [6]:

Obr. 1.2: OODA kruh popisujúci chod a reakciu na incidenty SOCu.

[2]CISO (*Chief Information Security Officer*) – riaditeľ a manažér informačnej bezpečnosti.
[3]OODA (*Observe, Orient, Decide and Act*) – moderná stratégia SOC tímu.

Spôsobom akým teda fungujú detekčné operačné centrá dnes, je hlavne OODA. Pozorovať, analyzovať, rozhodnúť sa a následne konať. Pozorovanie spočíva hlavne v zbieraní dát zo záznamov z koncových zariadení. Následne je potrebné zoskupené dáta analyzovať, teda korelovať, pretriediť a reportovať. Podľa získaných informácii je potrebné rozhodnúť sa a nasadiť ďalšie kroky, k čomu slúžia tzv. scenáre, ktoré definujú manuálne, polo-automatizované či úplne automatické kroky jeden za druhým, usporiadané v štruktúre podobnej rozhodovacieho stromu. Finálnym krokom je teda čin a ideálne čo najjednoduchšie a aspoň čiastočne automatizované riešenie. Týmto sa znova dostáva na začiatok kruhu a k opakovanému postupu. [6]

1.3 Technológie typu *Security Information and Event Management*

SIEM je dlhodobo považovaný za základnú technológiu dohľadového centra bezpečnosti. Systémy SIEM existujú desaťročia, ale s vývinom technológií a dôrazom na automatizáciu, sa objavujú nástroje novej generácie. Napríklad SOAR, ktorý tvorí nadstavbu a pridáva prvky ako hlavne automatizáciu reakcie na bezpečnostné incidenty. [7]

SIEM monitorovanie a Sigma pravidlá

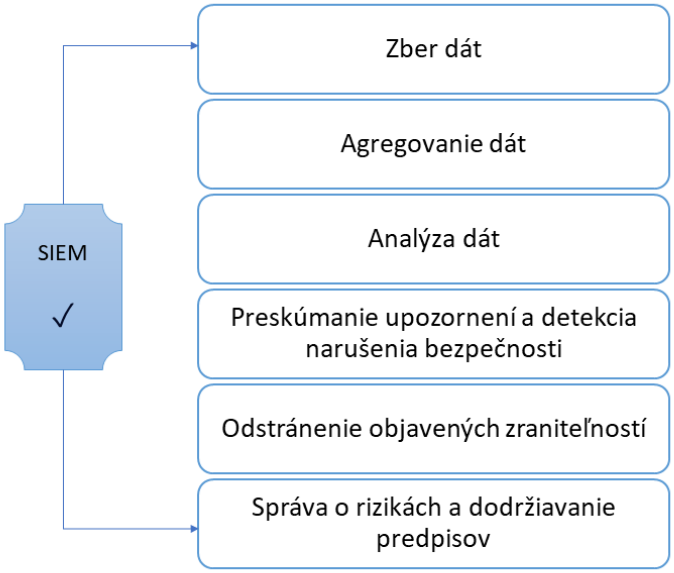
Riešenia na správu bezpečnostných informácií a udalostí (SIEM) využívajú pravidlá a štatistické korelácie na premenu zachytených logov a udalostí z bezpečnostných systémov na informácie, s ktorými sa dá ďalej pracovať a reagovať na ne. Na základe týchto infomácií, sú následne SOC tímy schopné odhaliť hrozby v reálnom čase a zahájiť reakciu na incidenty či ďalšie postupy. [7]

Pravidlá Sigma[4] boli vyvinuté ako *open-source* projekt s cieľom poskytnúť jednotný, štandardizovaný formát, ktorý bude fungovať naprieč rôznymi proprietárnymi riešeniami SIEM. Na popis pravidiel sú používané súbory typu YAML[5]. Sigma umožňuje zisťovať a odhaliť anomálie naprieč zachytenými logmi a identifikovať tak podozrivú aktivitu. Hlavnou výhodou tohto formátu je „spoločný jazyk“ na vzájomné zdieľanie pravidiel detekcie. SOC analytici sú denne zaplavovaní tisíckami logov a takto existujú pravidlá, ktoré majú jasne zadefinovaný formát a sú prevádzané na vlastné mapovanie jednotlivých SIEM poskytovateľov. [9]

[4]Verejne dostupné úložisko preddefinovaných pravidiel dostupné na: `https://github.com/SigmaHQ/sigma`.

[5]YAML (*Yet Another Markup Language*) – ľudsky čitateľný jazyk na serializáciu údajov, často používaný na zápis konfiguračných súborov.

Kombinovaním dát z rôznych systémov, počítačových sietí a aplikácií môžeme SIEM funkcie a postup fungovania vystihnúť nasledujúcimi dôležitými krokmi opísanými na obrázku 1.3 [8]:



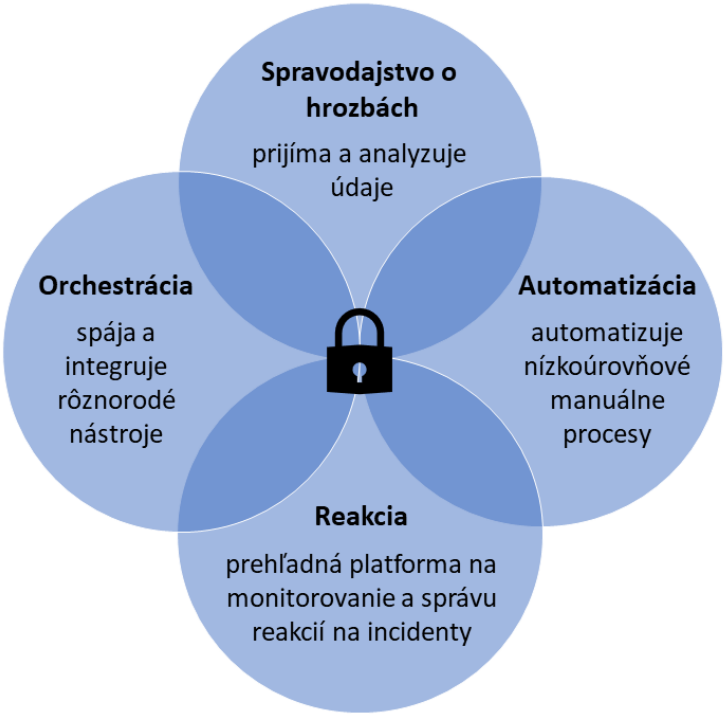
Obr. 1.3: Správa bezpečnostných informácií a udalostí (SIEM).

1.4 Technológie *Security Orchestration, Automation and Response*

Za SOAR sa považuje riešenie kombinácie 3 rôznych technológií: bezpečnostnej orchestrácie, automatizácie a platforiem pre reakciu na bezpečnostné incidenty spolu s analýzou hrozieb. SOAR riešenia umožňujú organizáciám zhromažďovanie a agregovanie obrovského množstva bezpečnostných údajov a upozornení z mnohých zdrojov (napr. aj v spolupráci so SIEM technológiami) čo im následne umožňuje vytvárať automatizované procesy a postupy (scenáre[6]) odhaľovania a reakcie na incidenty. Ich cieľom je reagovať na bezpečnostné incidenty s malou až takmer žiadnou nutnosťou ľudskej interakcie analytika, čím sa znižuje tlak na SOC a zvyšuje sa celková efektivita. [10]

[6]Scenár automatickej reakcie (*angl. playbook*) – preddefinované postupy akcií vo formáte rozhodujúcich procesov.

SOAR je teda komplexné riešenie spojenia technológií, uplatňujúce najvyšší možný stupeň automatizácie a zahŕňa tieto základné spomínané technológie definované na obrázku 1.4 [11]:



Obr. 1.4: SOAR ponúkajúci mix technológii pre efektivitu reakcie na incidenty.

Orchestrácia spočíva v integrácií rôznorodých nástrojov pod jednu strechu. Zabezpečuje tak zber a analýzu rôznych potrebných údajov. Medzi prepojené technológie môžeme zaradiť napr. skenery zraniteľností, produkty na ochranu koncových zariadení, *firewally*, systémy na detekciu a prevenciu narušenia či samotné platformy SIEM. Následne prichádza na rad **automatizácia**. Tá vytvára štandardizované, automatické a preddefinované procesy a akcie, nazývané scenáre, ktoré nahrádzajú manuálne riešenia analytikov. Ak sa napríklad v e-maile zamestnanca nájde škodlivá adresa identifikovaná počas skenovania, nasadí sa scenár automatickej reakcie, ktorý upozorní zamestnanca na potencionálny problém a zablokuje IP adresu[7] odosielateľa. Technológia **bezpečnostnej reakcie** ponúka analytikom jednotný pohľad na správu, monitorovanie, plánovanie a vykazovanie činností po nalezení problému, a to všetko v rámci jednej platformy. Takýto všeobecný, jednotný pohľad umožňuje spoluprácu a zdieľanie **spravodajských informácií o hrozbách** v kruhoch bezpečnostných, sieťových a systémových tímov. Zahŕňa taktiež navyše činnosti po ukončení reakcie na incident, ako je manažment prípadov a podávanie správ. [11]

[7]IP adresa (*angl. Internet Protocol address*) – unikátna adresa zariadenia v prostredí internetu.

1.5 Technické porovnanie systémov SIEM a SOAR

Zatiaľ čo SIEM a SOAR sú nástroje určené na riešenie v podstate rovnakého problému, sú to riešenia nezameniteľné, dokonca komplementárne. Majú však svoje jasné rozdiely, ktoré sú pozorovateľné hneď v spôsobe zbere dát. SIEM sa zameriava na vyhodnocovanie logov (LES[8]), kde SOAR agreguje dáta z viacerých zdrojov technológií a SIEM je často jednou z nich. SIEM zisťuje potencionálne bezpečnostné incidenty a tieto výstrahy je možné na základe vyššie spomínaných pravidiel organizovať a kategorizovať, no finálne vyšetrovanie musí byť vykonané a sfinalizované manuálne SOC tímom. Keď sa jedná o SOAR, vyšetrovanie, spracovanie upozornení a hlavne nasadené reakcie je automatizované. SOAR teda významne posúva SIEM na vyšší level a ponúka výsledky v podobe konkrétnych automatizovaných akcií. Porovnanie súvislostí týchto technológií je možné vidieť tiež na obrázku 1.5 [10]:

Obr. 1.5: Porovnanie súvislostí SIEM, SOC a SOAR [12].

Veľa SIEM poskytovateľov integruje aj SOAR možnosti, hlavne s dôrazom na automatizáciu, čím prezentujú tieto systémy ako „SIEM novej generácie“ [11]. SIEM a SOAR však tvoria najvýkonnejšiu kombináciu v spolupráci. Integráciou SIEM s platformou SOAR sú organizácie schopné využívať výhody monitorovania a korelácie udalostí v reálnom čase systému SIEM a zároveň orchestrovať a automatizovať reakciu na incidenty prostredníctvom SOAR. Táto synchronizácia umožňuje bezpečnostným tímom rýchlu reakciu na vyvíjajúce sa incidenty a SOAR je efektívnejšou možnosťou pre organizácie hľadajúce robustné a sofistikované riešenie. [8]

[8]LES (*Log Event Sources*) – zaznamenané zdroje udalostí, logy.

2 Kľúčové kritéria reakcie na KBI a analýza SOAR riešení

Táto práca sa zamieriava na scenáre automatickej reakcie (spomínané playbooky), ktoré sú súčasťou riešenia SOAR (viď kapitola 1.4) pri reakcii na KBI (kyberbezpečnostný incident). Preto bude táto kapitola venovaná podrobnej definícii čo playbook je, objasneniu automatizácie a sprostredkovaniu analýzy dostupných SOAR riešení. Pre jednoduchosť, presnosť významu a zachovanie medzinárodnosti pojmu, bude v rámci práce naďalej používaný výraz „playbook“.

2.1 Automatizácia z pohľadu reakcie na incident

Čo vlastne automatizácia reakcie na incidenty znamená? Všeobecne to už bolo naznačené v kapitole 1.4, no presnejšie povedané, znamená to použitie logiky riadenej určitými pravidlami, strojového učenia či umelej inteligencie pre rôzne účely. [13]

Hlavným účelom a benefitom SOAR automatizácie je SOC. Umožňuje bezpečnostným analytikom dosiahnuť viac za kratší čas, pričom sa z procesu reakcie na incidenty nevylučuje ľudská interakcia a kontrola. Automatizácia je ako ibalgin na bezpečnostnú horúčku upozornení a incidentov. Spoločnosť DarkReading ponúka číslo 40%, ktoré hovorí o tom koľko % organizácií nedokáže reagovať aspoň na štvrtinu svojich bezpečnostných upozornení. Kým útoky sa odohrávajú v priebehu niekoľkých minút, typické zistenie a reakcia tímu zaberie aj týždne či dokonca mesiace. S automatizáciou a modernými technológiami ako SOAR, vieme však skrátiť čas odozvy na incident či náklady v priemere o viac ako 80%. [14]

Každý automatizovaný krok môže ušetriť minúty a SOAR playbooky teda umožňujú organizácii zvládnuť viac reakcií na problémy za rovnaký čas. Kyberbezpečnostný tím sa tak môže sústrediť na vážne hrozby namiesto riešenia všedných úloh. Medzi zadania, ktoré možno automatizovať a vykonať pomocou technológie SOAR patria napríklad [15]:

- Skúmanie a analýza spravodajských zdrojov o hrozbách,
- Vyšetrovanie incidentov, ktoré zahŕňa analýzu a zber logov,
- Aktualizáciu lístkov úloh,
- Zhromažďovanie metrík a vytváranie správ,
- Posielanie upozornení e-mailom,
- Riešenie upozornení a alertov.

SOAR je teda mocným nástrojom a jeho najväčším prínosom okrem orchestrácie a zdieľania spravodajských informácii o potencionálnych útokov sú práve playbooky, vďaka ktorým je automatizácia jednoduchšia a užívateľsky prívetivá.

2.2 Problematika scenáru automatickej reakcie

Playbook môžeme definovať ako postup určitých krokov/akcií, ktoré sa majú vykonať na základe nejakej logiky a môžu sa vykonávať pravidelne, náhodne alebo sú spúšťané na základe predošlej automatizovanej či manuálnej udalosti alebo upozornenia. Playbook pozostáva teda z postupu za sebou idúcich nadväzujúcich blokov, kde každý je reprezentáciou určitej akcie, ktorá sa má vykonať. Akciu predstavuje každá činnosť či bezpečnostná operácia, ktorú treba vykonať na zistenie, vyšetrenie, prevenciu, zmiernenie, nápravu či ako reakciu na určitý bezpečnostný stav, ktorý už nastal alebo je ešte potencionálnou budúcnosťou. [16]

Scenár automatickej reakcie alebo playbook, je teda digitalizovaný, dohodnutý postup na riešenie bezpečnostného incidentu. Spája v sebe znalosti a skúseností najuznávanejších bezpečnostných odborníkov a štandardizovaných postupov čím vzniká pevne definovaný a opakovateľný postup logických, nadväzujúcich akcií a postupov, ktoré môžu byť do bodky vykonané a dodržiavané i nováčikmi. Poradie akcií a krokov, ktoré majú byť vykonané je teda pevne stanovené, čím sa zabezpečuje nevyhnutnosť následnosti a logiky. [17]

Každú akciu playbooku môžeme teda nazvať stavebným blokom, kde dokopy pospájané a naseba logicky napojené vytvárajú určitú štruktúru. Tak ako všetko, aj playbooky maju svoje rôzne používané formáty v akých sa ukladajú a prezentujú. Vlastnosť či názov, ktorý všetky playbooky spája je rozhodovací proces. Mohol by sa považovať za niečo ako rozhodovací strom či graf, no je to predovšetkým vývojový diagram. Postup procesu začína v počiatočnom bode a akonáhle je podmienka splnená či akcia vykonaná, nastáva posun k ďalšej nižšie definovanej akcii až kým sa nedosiahne koniec. [18]

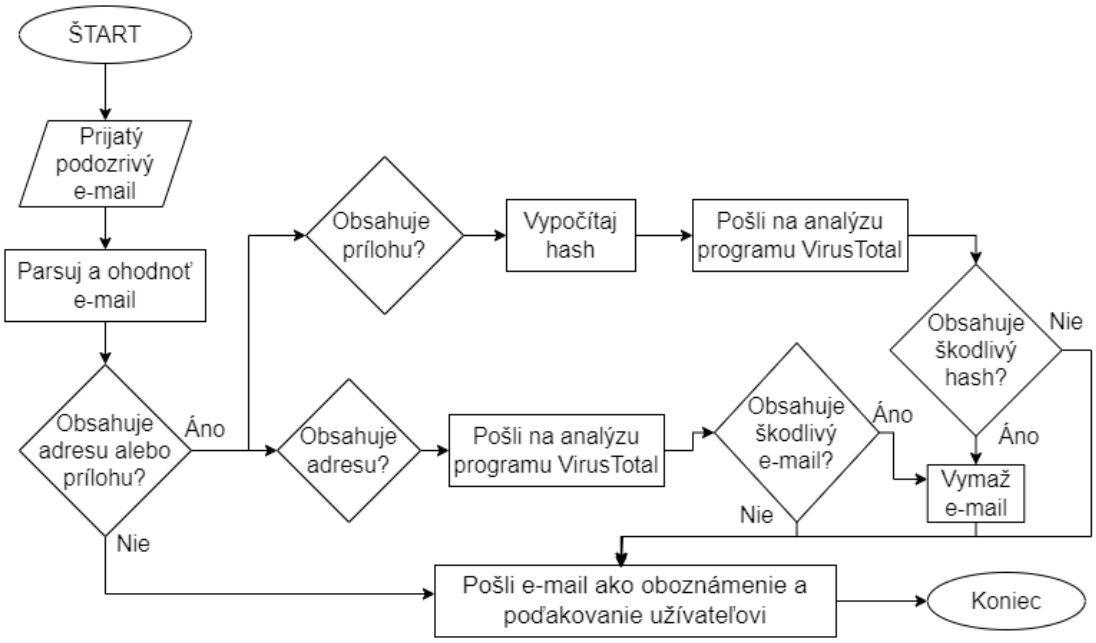
Takáto zložitá štruktúra rozhodovacieho procesu je ukladaná a prístupná pre SOAR systémy v rôznych formátoch často závislých na konkrétnom výrobcovi, no zväčša to býva známy súbor JSON[1], ktorý je známy práve pre stromové štruktúry a ukladanie objektívne orientovaných dát. V prípade akcií, ktoré sú reprezentované jednotlivými blokmi je JSON logickou voľbou, no vrámci práce budú spomenuté aj ďalšie dostupné formáty playbookov na základe analýzy nasledujúcej kapitoly.

Na ďalšej strane je možné vidieť porovnanie rôznej podoby playbooku vo formáte vývojového diagramu (viď obrázok 2.1) – kde je logický proces ľahko viditeľný či pochopiteľný, a pod ním na obrázku 2.2 je priložená ukážka vo formáte JSON. Ukážka JSON playbooku bola použitá priamo od spoločnosti Splunk, ktorá má voľne prístupné[2] určité množstvo scenárov automatickej reakcie na platforme GitHub[3].

[1] JSON (*JavaScript Object Notation*) – štandardný formát ukladania objektových dát.

[2] Dostupné na adrese: `https://github.com/phantomcyber/playbooks`.

[3] GitHub – poskytovateľ internetového hostingu pre vývoj softvéru s použitím verzovacieho nástroja Git.



Obr. 2.1: Príklad automatickej reakcie na phishingový e-mail v podobe vývojového diagramu [15].

```
"nodes": {
                "0": {
                    "data": {
                        "advanced": {
                            "join": []
                        },
                        "functionName": "on_start",
                        "id": "0",
                        "type": "start"
                    },
                    "errors": {},
                    "id": "0",
                    "type": "start",
                    "warnings": {},
                    "x": 19.999999999999986,
                    "y": -6.394884621840902e-14
                },
                "1": {
                    "data": {
                        "advanced": {
                            "join": []
                        },
                        "functionName": "on_finish",
                        "id": "1",
                        "type": "end"
                    },
```

Obr. 2.2: Ukážka zápisu blokov (angl. *nodes*) vo voľne dostupnom Splunk scenári.

2.3 Porovnanie a analýza dostupných SOAR riešení

Na odhalenie aktuálnej situácie dostupných playbookov a zorientovanie sa na trhu ponúkaných SOAR riešení od rôznych spoločností, bola vykonaná podrobná analýza. Vybraných bolo 12 základných a najviac používaných či dostupných SOAR riešení, ktorých formy boli preštudované a porovnané. Medzi mená analyzovaných SOAR technológií v tejto práci patria:

1. QRadar SOAR,
2. Cortex SOAR,
3. Splunk SOAR,
4. FortiSOAR,
5. Microsoft Sentinel,
6. InsightConnect SOAR,
7. Chronicle SOAR (historicky Siemplify),
8. Smart SOAR,
9. Swimlane SOAR,
10. Elastic SOAR,
11. The HIVE project (voľne dostupný)[4],
12. Shuffle SOAR (voľne dostupný)[5].

V rámci porovnania boli zostrojené dve tabuľky 2.1 a 2.2. Tabuľka 2.1 sa zameriava na zhodnotenie situácie ohľadom voľne dostupných SOAR scenárov, či daná spoločnosť scenáre sprostredkúva alebo ich pre ňu niekto zdieľa predovšetkým na platforme Github. Ak boli pre danú spoločnosť playbooky nájdené, tabuľka zahŕňa ich presné počty a formáty zápisu. Toto porovnanie je nenahraditeľným zistením pre ďalší postup práce a zameraním sa na návrh a zvolenie vhodného formátu ukladania scenárov. Tabuľka 2.2 ponúka porovnanie SOAR z pohľadu jednotlivých vybraných vlastností tejto technológie. Zvolené porovnávané ponúkané možnosti jednotlivých riešení sú spojené s opätovným zameraním sa na scenáre, a navyše ponúkajú reálnu komparáciu, prehľad a zhodnotenie aktuálnej situácie na trhu.

V rámci tabuliek bolo použitých niekoľko rôznych značiek. Fajka „✓“ intuitívne zastupuje hodnotu „áno“. Značka „↑“ znamená, že danú informáciu si užívateľ, v prípade kúpy produktu, musí na stránke vyžiadať sám. Tiež opakujúcim sa znakom je „−“, ktorý vyjadruje momentálne nedohľadateľnú, verejnosti neponúkanú či nerelevantná informáciu (ak nasleduje v bunke za položkou „Nie“). Niektoré SOAR riešenia od vybraných vendorov neboli do tabuľky 2.2 zaradené, nakoľko nebolo pre nich možné dohľadať skúmané vlastnosti, ani po priamom kontaktovaní spoločnosti vedúcim tejto bakalárskej práce, na ktorú napr. D3 Security vôbec nereagoval.

[4]Voľne dostupné úložisko na adrese: `https://github.com/TheHive-Project/TheHive`.
[5]Voľne dostupné úložisko na adrese: `https://github.com/Shuffle/Shuffle`.

Tab. 2.1: Tabuľka porovnania SOAR riešení a ich verejnej dostupnosti playbook repozitárov s výpisom jednotlivých počtov.

Spoločnosť	**Názov riešenia**	**Voľne dostupný repozitár**	**Počet scenárov**	**Formát scenárov**	**Voľne dostupné konektory**	**Počet konektorov**
IBM	Qradar SOAR	✓	81 [19, 20]	`.resz /.xml / .json / python`	✓	168 [21]
PaloAlto	Cortex XSOAR	✓	900+ [22]	.yml - COPS	Nie	–
Splunk	Splunk SOAR	✓	131 [23]	.json / python	✓	452 [24]
Fortinet	FortiSOAR	✓	160 [25]	.json	✓	377 [26]
Microsoft	Microsoft Sentinel	✓	100+ [27]	.json	✓	45 [28]
Rapid7	InsightConnect SOAR	Nie	–	–	✓	290 [29]
Google	Chronicle SOAR	Nie	–	–	✓	12 [30]
D3 Security	Smart SOAR	Nie	–	–	Nie	–
Swimlane	Swimlane SOAR	Nie	–	–	Nie	–
Elastic	Elastic SOAR	Nie	–	–	Nie	–
StrangeBee	The HIVE project	–	–	–	–	–
Shuffle	Shuffle SOAR	–	–	–	–	–

Tab. 2.2: Tabuľka porovnania SOAR riešení so zameraním na oficiálne a zaujímavé ponúkané možnosti produktu.

Názov riešenia	**Spoločnosť**	**Model nasadenia**	**Množstvo užívateľov**	**Skúška zadarmo (DEMO)**	**Počet predpripravených scenárov**	**Počet integrácii s ďalšími nástrojmi**	**Podpora mobilnej verzie**	**Skrátenie času odozvy na incident o/až do [%]**
QRadar SOAR	IBM	SaaS/on-premise	2-100 alebo ↑	✓	–	270+	Nie	85
Cortex XSOAR	PaloAlto	SaaS – predplatné balíčkov	↑	✓	–	700+	✓	90
Splunk SOAR	Splunk	SaaS/on-premise pre určité verzie	↑	✓	100+	300+	✓	98
FortiSOAR	Fortinet	SaaS/on-premise	Záleží na licenčnom modeli	✓	800+	500+	✓	98
Microsoft Sentinel	Microsoft	SaaS/on-premise	Záleží na licenčnom modeli	✓	330+	–	Nie	–
InsightConnect SOAR	Rapid7	SaaS/on-premise	Neobmedzené	✓	–	300+	Nie	–

V nasledujúcom texte budú uvedené informácie v tabuľkách 2.1 a 2.2 stručne popísané. Dôraz bude kladený na popis vlastností samotného riešenia, zdôvodnenie a zhrnutie informácií či finálne zhodnotenie a porovnanie technológií.

QRadar SOAR od spoločnosti IBM [31]:
Riešenie QRadar SOAR, ktoré získalo ocenenie *Red Dot* za dizajn grafického užívateľského rozhrania, ponúka možnosť nasadenia technológie spôsobom *SaaS*[6] alebo *on-premise*[7] pre min. 2 až 100 užívateľov, DEMO[8] skúšku produktu zadarmo a sľubuje až viac ako 270 prepojení (integrácií) s inými nástrojmi. Medzi jednu z jeho výhod je zaraďovaná doba skrátenia času odozvy na incident, ktorá dosahuje až 85%, čím je potvrdený prínos automatizácie centrám SOC. Čo sa týka voľne dostupných scenárov a konektorov, ktorými by bolo možné sa inšpirovať, bolo dohľadané patrné množstvo v rôznych formátoch no určite by QRadar nebol zaradený medzi vodcu voľného zdieľania informácií ohľadne tejto problematiky.

Cortex XSOAR od spoločnosti PaloAlto [33, 34]:
Technológia Cortex XSOAR je založená na ponúkaných predplatných *SaaS* balíčkoch tzv. „*Packs*“ a zaberá poprednú priečku v počte integrácií s ďalšími nástrojmi. Cortex kladie veľký dôraz na integráciu umelej inteligencie do svojho riešenia a prináša taktiež podporu mobilnej verzie nástroja, ktorá ponúka užitočné možnosti na zefektívnenie práce SOC. Opäť znižuje čas reakcie na incident o niečo viac s porovnaním QRadar a ponúka najvačšie množstvo voľne dostupných scenárov. V prípade formátu scenárov je dôležité spomenúť vlastný prínos spoločnosti PaloAlto a pokus o návrh otvoreného formátu s názvom COPS (viď kapitola 3.2).

Splunk SOAR od spoločnosti Splunk [35, 36]:
Splunk ponúka lokálne nasadenie SOAR iba pre určité verzie a zároveň sa s verejnosťou delí iba o vybrané informácie, no určite s integráciami a voľne dostupnými scenármi, vo formáte JSON alebo python, nešetrí. Jeho dosah skrátenia času odozvy na incident naberá spád až 98%, čím sa spolu s Fortinet riešením dostáva na vrchol. Historicky bola táto technológia nazývaná Phantom, no dnes pod názvom Splunk ponúka aj podporu mobilnej verzie, čím podobne ako Cortex, prinášajú reakciu na incident na dosah vrecka. Z praktického pohľadu tejto práce, boli Splunk scenáre zhodnotené ako najvhodnejšie na nastávajúcu prácu, nakoľko spôsob spracovania a ukladania dát patrí medzi najprehľadnejší a najjednoduchší. Splunk navyše ku každému scenáru ponúka vizuálne spracovanie rozhodovacieho procesu, kde môže byť patrné hlavne dôležité krokovanie a rozdelenie scenára do jednotlivých akcií.

[6] SaaS (*Software as a Service*) – licenčný model na základe predplatného, prístup k softvéru cez internet [32].

[7] *On-premise* – softvér nainštalovaný na lokálnom hardvéri.

[8] DEMO (skrátene z angl. *demonstration*) – ukážkový náhľad technológie s obmedzenými možnosťami, ponúkaný užívateľovi zadarmo.

FortiSOAR od spoločnosti Fortinet [37, 38, 39]:
Spomínaný FortiSOAR predpripravuje líderské tabuľkové množstvo scenárov spolu s minimálne 500 prepojeniami na ďalšie nástroje, k čomu navyše pripája rovnaké rekordné skrátenie času odozvy na incident ako Splunk. Nezaostáva taktiež ani v podpore mobilnej verzie a na verejnom úložisku predostiera značné množstvo verejne dostupných scenárov a konektorov. Formát uloženia sa opakuje a nadobúda podobu JSON.

Microsoft Sentinel od spoločnosti Microsoft [40, 41]:
Microsoft Sentinel je považovaný za komplexnejšie riešenie z dôvodu netajeného spojenia technológií SIEM a SOAR. Väčšina SOAR funkcií je do neho integrovaných. To ako je možné jeho sprovoznenie sa vyvíja od licenčného modelu a samozrejme ponúka určité množstvo predpripravených scenárov. Pár z nich spolu s konektormi je voľne dostupných vo formáte JSON a pridáva ďalšie nenehraditeľné dáta. Podpora mobilnej verzie ešte nebola zavedená no predovšetkým je toto riešenie určite neoddeliteľne významnou technológoiu poprednej spoločnosti ako je Microsoft.

InsightConnect SOAR od spoločnosti Rapid7 [42]:
InsightConnect určite nepatrí medzi technológie obmedzujúce počet užívateľov a ponúka značné množstvo vopred predpripravených integrácií s inými nástrojmi podobne ako Splunk. Síce neboli zatiaľ dohľadané voľne dostupné scenáre, Rapid7 ale ponúka úložisko s voľne dostupnými konektormi. Napriek určitým zatiaľ neistým informáciam patrí InsightConnect medzi popredné technológie so zameraním na zvýšenie automatizácie idúc ruka v ruke znižovaniu potreby skriptovania samotnými SOC členmi.

Chronicle SOAR od spoločnosti Google [43, 44]:
Môžeme usúdiť, že Google sa pustil do SOAR riešenia len nedávno, a preto je možné sa stretnúť s jeho historickým názvom Siemplify. Siemplify je spoločnosť založená v meste Tel Aviv, ktorá bola len pred rokom odkúpená Googlom. Tento nástroj ponúka plne automatizované riešenie, čím si Google zabezpečuje krok s dobou a rozširuje svoje populárne služby o ďalšie vlastnosti. Bolo taktiež nájdených pár voľne dostupných konektorov pre ďalšie nástroje, no ostatné informácie už boli ťažšie dohľadateľné.

Smart SOAR od spoločnosti D3 Security [45]:
Spoločnosť D3 Security považuje svoje SOAR riešenie za jedno z popredných. Prezentuje svoje riešenie jednoduchým grafickým rozhraním, modernými vlastnosťami a až 10-krát rýchlejšou odozvou na incident. Napriek tomu však na stránke nebolo možné dohľadať nami signifikantné informácie a po priamom kontaktovaní nereagoval. D3 totižto ponúka veľa kvalitných informácií vrátane porovnaní vlastného riešenia so SOAR od iných spoločností, bohužiaľ je však všetko dostupné len na dúfajúce vyžiadanie.

Swimlane SOAR od spoločnosti Swimlane [46]:
Swimlane prichádza s myšlienkou posunutia automatizácie na vyšší level pre samotného užívateľa. Ponúka užívateľsky prívetivú platformu, prezentovanú tiež pod názvom Turbine, v ktorej sa trošku líši od tradičných SOAR tým, že integruje nízkokódové riešenia scenárov automatickej reakcie. Navyše, spolu so samotným dôrazom na umelú inteligenciu, zastáva popredné miesta popularity na trhu.

Elastic SOAR od spoločnosti Elastic [47]:
Nasledujúce tri technológie spolu veľmi úzko súvisia a pracujú medzi sebou ako vzájomné konektory. Elastic obohacuje trh o ďalšie automatizačné riešenie a sľubuje zákazníkom optimalizáciu, jednoduchosť, flexibilitu a otvorenosť. Pre bližšie informácie, je však znova nutné pátranie pomocou vyžiadania o dokumentáciu a taktiež neponúka voľne dostupné úložisko s ukážkou scenárov.

The HIVE projekt od spoločnosti StrangeBee [44, 48, 49]:
TheHive je prezentovaný ako 4v1 bezpečnostná platforma reakcie na incidenty, ktorá sa vyslovene nedefinuje ako SOAR, ale spĺňa všetky kritéria na naplnenie tejto technológie. TheHive je voľne dostupné riešenie spojené s MISP[9] platformou, skladajúce sa z dvoch hlavných častí. Samotný TheHive, ktorý slúži ako orchestrátor, plus Cortex[10], ktorý je zodpovedný za analýzu a automatizáciu. Nástrojom Cortex sa nemyslí Cortex XSOAR skúmaný v priložených tabuľkách, ale samostaný voľne dostupný nástroj, na ktorom automatizácia nie je úplne priamočiara a vyžaduje znalosť jednoduchých skriptov v jazyku Python. TheHive sa preto napriek svojej ľahkej dostupnosti zaradzuje k náročnejším SOAR systémom pri pohľade na užívateľa. Všetky automatizačné kroky je nutné vykonávať pomocou rozhrania API[11], kde je žiadúce kódovanie namiesto použitia jednoduchých vizuálnych platforiem so stavebnými blokmi. Napriek tomu je však TheHive populárnym riešením.

Shuffle SOAR od spoločnosti Shuffle [50]:
Ďalším voľne dostupným SOAR riešením na trhu je spomínaný Shuffle. Tento softvér je zameraním na prepojenie viac ako 2000 existujúcich aplikácií a nevyžaduje, tak ako väčšina spomínaných SOAR riešení, programátorské znalosti, ale ponúka vyspelé grafické užívateľské rozhranie. Za zaujímavosť Shuffle je možné považovať fakt, že jednotlivé bloky scenárov sú v podstate predom zadefinované a využívané akcie určitých už známych aplikácií, ktoré je možné medzi sebou prepojiť a dosiahnuť tým žiadaný výsledok. Shuffle spolu s TheHive a Elastic veľmi úzko súvisia a z dôvodu voľne dostupných riešení sú medzi sebou pravidelne integrované a zdieľajú funkcie.

[9] MISP (*Malware Information Sharing Platform*) – softvér a komunita na zhromažďovanie, analýzu a zdieľanie indikátorov o KBI a škodlivom softvéri.

[10] Voľne dostupné úložisko na adrese: `https://github.com/TheHive-Project/Cortex`.

[11] API (*Application programming interface*) – súbor funkcií a postupov, umožňujúcich vytvárať aplikácie, ktoré pristupujú k údajom operačného systému, inej aplikácie alebo služby.

Medzi základné vlastnosti každého porovnávaného SOAR systému je teda možné zaradiť – automatizáciu, integrácie s inými nástrojmi, interaktívne grafické užívateľské rozhranie, vstavanú správu incidentov, podporu lokálnych/internetových či hybridných nasadení, zabudované spravodajstvo o hrozbách, určitý počet predpripravených scenárov automatickej reakcie a v neposlednom rade využívanie umelej inteligencie pre zjednodušenie a maximalizáciu procesov. Aj keď dnešná doba nepísaným pravidlom stanovuje trend DEMO skúšky či komentovaných prehliadok produktov, pri každom SOAR riešení je táto verzia s limitovanými funkciami na vyžiadanie od konkrétnej technológie.

Zvolenie jednoznačného lídra, je takmer nemožné a ako to chodí pri každom produkte, aj v tomto prípade je nevyhnutné zváženie jednotlivých kľúčových vlastností či cenové možnosti, ktoré každý SOAR ponúka, na základe čoho sa očakáva určité vykryštalizovanie správnej voľby. Medzi signifikantné parametre sa určite môžu zaradiť – podpora grafického rozhrania či naopak vyššia užívateľská náročnosť v prípade nutnosti programátorských znalostí, financie, rôzne licenčné a nasadzovacie modely či ďalšie zaujímavé vlastnosti ako napríklad podpora mobilnej verzie a rýchlosť reakcie.

Pre účely tejto práce boli ako najvhodnejší kandidáti zvolené tie riešenia, ktoré ponúkajú určité voľne dostupné množstvo scenárov či poprípade integrácií. Je vhodné teda vypichnúť QRadar, Cortex, Splunk, Fortinet a Microsoft Sentinel. Fakt, že niektoré riešenia sú poskytované ako *open-source*, ešte neznamená, že zverejňujú aj proprietárne riešenia scenárov a práve pri TheHive a Shuffle sa ukážky týchto rozhodovacích postupov nepodarilo dohľadať. V nasledujúcich kapitolách budú teda voľne dostupné scenáre SOAR riešení z tabuľky 2.1 použité pre nadväzujúcu analýzu, voľbu vhodného typu formátu a generalizáciu samotným nástrojom.

3 Analýza voľne dostupných signifikantných formátov a štandardov

Ako je patrné už z výsledkov analýzy dostupných SOAR riešení v kapitole 2.3, scenáre automatickej reakcie sú navrhované a definované v rôznych formátoch. Najčastejšie prevláda ukladanie dát do formátu JSON (viď tabľka 2.1), no zaznamenané boli aj Python, XML[1] či napríklad YAML, ktorý je súčasťou voľne dostupného návrhu COPS[2]. Je teda zrejmé, že zvolený formát sa odvíja od rozhodnutia konkrétnej spoločnosti, čo nevedie k ideálnej situácií v prípade zmeny zvolenej značky produktu a nemožnosti použitia už raz vytvorených scenárov „na mieru“. Pre dosah cieľa zjednotenia, jednoduchosti zdieľania a vizualizácie by poslúžil generalizovaný formát, pred ktorým samotným návrhom bude v tejto kapitole priblížená analýza dôležitých štandardov.

Pred samotnou voľbou vhodného všeobecného formátu scenárov automatickej reakcie, bolo teda vykonané porovnanie aktuálneho stavu trhu a na nasledujúcich riadkov budú priblížené nájdené signifikantné formáty či štandardy.

3.1 Charakteristika formátu Sigma

V náväznosti na kapitolu 1.3 kde bola Sigma už načrtnutá a je dostupný link na GitHub repozitár, bude bližšie priblížený samotný formát Sigma pravidiel. Sigma je teda generický formát signatúry pravidiel navrhnutý pre SIEM systémy. Funguje ako všeobecný štandard, z ktorého je možná konverzia pravidla do formátu konkrétneho riešenia danej spoločnosti. Na ukladanie jednotlivých pravidiel bol zvolený formát súboru YAML, ktorý je ľahko čitateľný ako človekom, tak i počítačom. [51]

Tento formát je dôležitým pokrokom a môže slúžiť ako inšpirácia pre voľbu všeobecného formátu pre SOAR scenáre. Každé pravidlo, vo formáte Sigma, obsahuje nasledujúce povinné (zvýraznené tučne, angl. *required*) a voliteľné (angl. *optional*) parametre [52]:

- **Názov** (angl. *Title*) – názov pravidla.
- Identifikačné číslo (angl. *ID*) – jednoznačný identifikátor pravidla.
- Status (angl. *Status*) – popisuje typ pravidla (experimentálny/normálny).
- Popis (angl. *Description*) – vysvetlenie obsahu pravidla.
- Autor (angl. *Author*) – dáta o autorovi pravidla.

[1] XML (*eXtensible Markup Language*) – rozšíriteľný značkovací jazyk.

[2] COPS (*Collaborative Open Playbook Standard*) – voľne dostupný štandard, definujúci postup scenárov reakcie na digitálnu kriminalistiku.

- Referencia (angl. *Reference*) – odkaz obsahujúci vysvetlenie riešeného problému.
- Upravené (angl. *Modified*) – dátum úpravy pravidla.
- **Zdroj logov** (angl. *Logsource*) – rozsah prehľadávaných dát v rámci pravidla.
- Kategória (angl. *Category*) – výber logov generovaných určitou skupinou systémov ako napríklad server či antivírusový program.
- Produkt (angl. *Product*) – výber logov generovaných špecifickým produktom alebo aplikáciou.
- Služba (angl. *Service*) – výber podmožiny logov produktu, napríklad operačný systém Windows či Linux.
- **Detekcia** (angl. *Detection*) – vyhľadávanie špecifických hodnôt, kľúčových slov a časových rámcov.
- **Podmienka** (angl. *Condition*) – vyhľadávanie hodnôt v rámci detekcie na základe určitých parametrov.
- Falošne pozitívne (angl. *False positives*) – vysvetlenie situácií, kedy pravidlo môže viesť k falošne pozitívnym výsledkom.
- Stupeň (angl. *Level*) – stupeň závažnosti (nízka, stredná, vysoká, kritická).

3.2 Charakteristika štandardu COPS

COPS je voľne dostupný štandard vyvinutý primárne na popis scenárov reakcie využívajúcich digitálnu forenznú analýzu. Formát popisu a ukladania je YAML, ktorý bol zvolený vzhľadom na jeho jednoduchú čitateľnosť človekom a simultánnu schopnosť popisu zložitej vnorenej štruktúry údajov. Tento štandard užívateľovi sľubuje tri základné vlastnosti: otvorenosť, automatizáciu a viditeľnosť. COPS je teda voľne dostupný, *open-source* formát, čo zahŕňa možnosť podieľania sa na jeho vylepšení či zmeny. Ponúka čiastočne až plne automatizované riešenia, čím poskytuje členom organizácie (SOC tím, manažment) jasný prehľad o procese reakcie na incident.

Playbook typu COPS obsahuje 2 skupiny základných parametrov a to všeobecné parametre scenáru a jednotlivé parametre každej akcie (bloku), ktorá sa má v rámci postupu vykonať. Medzi všeobecné parametre pre playbook boli definované [53]:

- Identifikačné číslo (angl. *ID*) – jednoznačný playbook identifikátor.
- Meno (angl. *Name*) – playbook názov.
- Popis (angl. *Description*) – vysvetlenie čo scenár robí.
- Akcie/Úlohy (angl. *Tasks*) – zoznam jednotlivých akcií/úloh/krokov scenáru.
- Identifikátor prvého kroku (angl. *Starttaskid*) – id prvej úlohy scenáru.
- Vstupy (angl. *Inputs*) – zoznam vstupov, ktoré do scenára vchádzajú.
- Výstupy (angl. *Outputs*) – zoznam výstupov po ukončení playbook úloh.

Medzi parametre popisujúce jednotlivé úlohy sú ďalej definované [53]:

- Identifikačné číslo (angl. *ID*) – unikátny identifikátor každej akcie na úrovni scenáru.
- Identifikačné číslo úlohy (angl. *Taskid*) – globálny identifikátor každej akcie, potrebný pri zdieľaní rovnakých úloh pre viacero rôznych scenárov.
- Typ (angl. *Type*) – jeden z týchto typov: *title* (predstavuje novú časť/záhlavie scenáru), *regular* (skript alebo manuálna úloha) alebo *condition* (na rozhodnutie, aká bude nasledujúca vykonaná úloha).
- Meno (angl. *Name*) – názov úlohy.
- Popis (angl. *Description*) – vysvetlenie princípu úlohy.
- Názov skriptu (angl. *ScriptName*) – ak daný krok je plne automatizovaný, definuje sa skript, ktorý sa má pre naplnenie úlohy spustiť.
- Značky (angl. *Tags*) – akákoľvek dodatočne potrebná informácia pre daný krok.
- Podmienka (angl. *Condition*) – v tomto poli sa bude nachádzať vnorená mapa zoznamu vetiev (úloh), ktorou má scenár pokračovať podľa výsledku skriptu.
- Argumenty skriptu (angl. *ScriptArguments*) – vstupy jednotlivej úlohy.
- Nasledujúca úloha (angl. *Nexttasks*) – navigácia na úlohu, ktorá sa ma vykonať ako ďalšia.
- Podmienky navigácie (angl. *Conditions*) – na základe výsledku sa vyberie nasledujúci krok.

Ukážka uloženia dát scenáru automatickej reakcie vo formáte YAML štandardu COPS je súčasťou prílohy A tejto práce.

3.3 Charakteristika štandardu CACAO

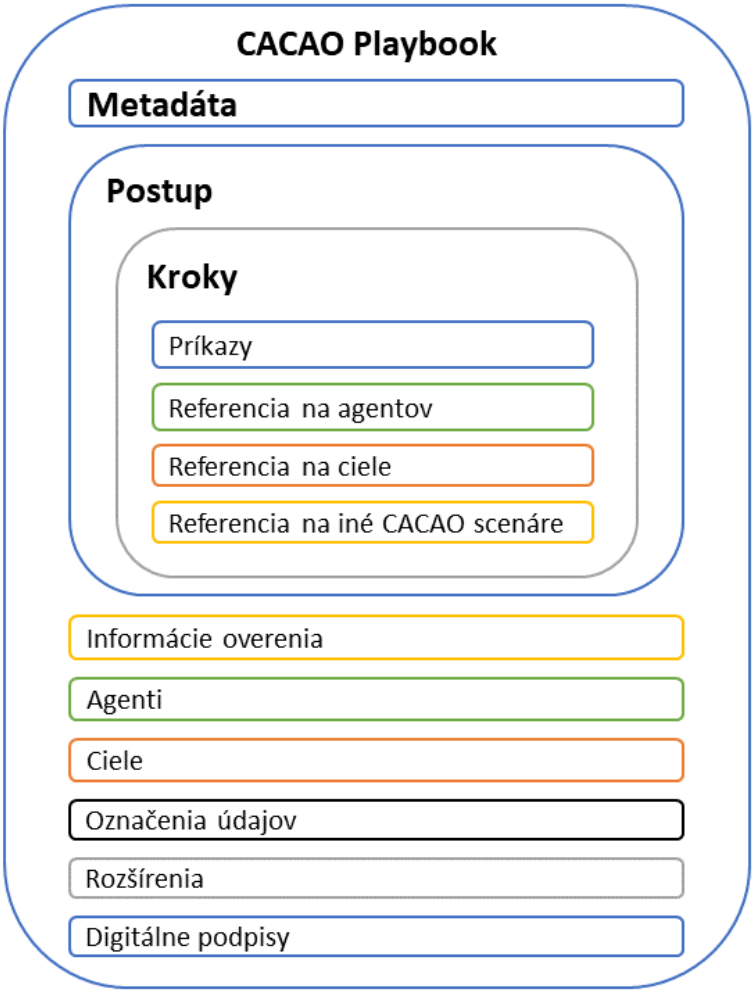
CACAO[3] je špecifikovaná navrhovaná schéma pre scenáre automatickej reakcie, ktorej hlavným cieľom je popis formátu, ktorý je možné vytvárať a zdieľať štruktúrovaným a štandardizovaným spôsobom naprieč hranicami organizácií a limitáciami jednotlivých proprietárnych technologických riešení.

Táto výzva moderného trhu, ktorá bola v podobe Sigma pravidiel naplnená pre SIEM systémy, sa snaží byť aplikovaná aj na SOAR riešenia. Situácia, kde by došlo k okamžitej použiteľnosti zdieľaného scenáru v bezpečnostnej infraštruktúre bez toho, aby vyžadoval určitú úpravu alebo aktualizáciu, je považovaná za veľmi zriedkavú. Tieto úpravy sú nutné z dôvodov ako napríklad rozdiely prostredí či rôznej úrovne abstrakcie samotných scenárov.

[3]CACAO (*Collaborative Automated Course of Action Operations*) – definícia štandardu pre implementáciu scenáru reakcie na incident v oblasti kyberbezpečnosti.

Kvôli zjednodušeniu situácie a zjednoteniu štandardov, sa technická komisia organizácie OASIS Open[4] podieľa na vytvorení všeobecnejšieho formátu CACAO, ktorý je však stále len návrhom v procese vývinu a po vykonanej analýze sa nepotvrdilo ešte jeho aktívne používanie žiadnym zo spoločností porovnávaných SOAR riešení z predošlej kapitoly 2.3.

CACAO teda podľa najnovšej verzie 2.0 definuje nasledujúce triedy objektov: playbook (metadáta), kroky postupu, príkazy, informácie overenia, agentov, ciele, označenia údajov, rozšírenia a digitálne podpisy (viď obrázok 3.1). [16]



Obr. 3.1: CACAO playbook štruktúra.

Pre nasledujúci návrh tejto práce budú nevyhnutné najmä prvé dve základné časti/typy objektov a to informácie o scenári, teda metadáta, spolu s postupom. Medzi povinné parametre playbook metadát patria [16]:

[4]OASIS (*Organization for the Advancement of Structured Information Standards)* – neziskové konzorcium, ktoré pracuje na vývoji, zbližovaní a prijímaní voľne dostupných štandardov pre kyberbezpečnosť a ďalšie odvetvia v oblasti informatiky a technológií.

- Typ (angl. *Type*) – priradená hodnota musí byť „playbook“.
- Špecifikácia verzie (angl. *Spec_version*) – priradená hodnota verzie musí byť „cacao-2.0“.
- Identifikačné číslo (angl. *ID*) – jednoznačný playbook identifikátor.
- Meno (angl. *Name*) – playbook meno.
- Vytvorené kým (angl. *Created_by*) – ID zostaviteľa daného scenáru.
- Vytvorené (angl. *Created*) – čas vytvorenia scenáru.
- Posledná zmena (angl. *Modified*) – čas poslednej zmeny v scenári.
- Štart postupu (angl. *Workflow_start*) – prvý definovaný krok postupu.

Ďalšou povinnou časťou je postup (angl. *Workflow*), ktorý je entitou definícií všetkých jednotlivých krokov, ktoré sa v rámci playbooku majú vykonať. Kroky alebo inak povedané bloky sú delené na rôzne typy na základe funkcie, ktorú vykonávajú. Medzi povinné parametre, ktoré sa však pre rôzny typ kroku môžu odlišovať, sú zaraďované [16]:

- Typ (angl. *Type*) – výber z možností ako štart (angl. *Start*), koniec (angl. *End*), krok (angl. *Action*), playbook nasledujúci krok (*Playbook-action*), paralelné (angl. *Parallel*) a rôzne podmienky (angl. *If-condition, While-condition, Switch-condition*).
- Príkazy (angl. *Commands*) – list príkazov, ktoré majú byť vykonané v rámci daného kroku ak je definovaný typ *action*.
- Agent (angl. *Agent*) – entity vykonávajúce príkazy definované v objekte nazývanom „*agent-target*“.
- Identifikačné číslo scenáru (angl. *playbook_id*) – ak je predom definovaný typ *Playbook-action*.
- Nasledujúce kroky (angl. *Next_steps*) – ak je definovaný typ *parallel*.
- Podmienka (angl. *Condition*) – ak je definovaná podmienka typu *if-condition* alebo *while-condition* používa sa tento parameter na definíciu kontrolovanej veci.
- Ak pravda (angl. *On_true*) – ak je kontrolovaná podmienka vyhodnotená ako splnená/pravdivá, vykoná sa nasledujúci krok definovaný pre tento *on_true* parameter.

Medzi voliteľné parametre sa zaraďujú napríklad popis (angl. *description*), dôležitosť (angl. *severity*), značky (angl. *labels*), podpisy (angl. *signatures*), externé referencie (angl. *external_references*) atď.

Ukážka scenáru vo formáte vyvíjajúceho sa štandardu CACAO je pridaná v prílohe B tejto práce.

4 Návrh nástroja generalizácie automatizovaných SOAR scenárov

Pred samotným vytvorením a implementáciou nástroja bolo potrebné zvoliť vhodný všeobecný formát na zobrazenie finálnych generalizovaných SOAR scenárov, manuálne overiť prevod zvoleného vstupného formátu na výstupný a pripraviť návrh funkcionalít samotného nástroja ako aj popis jeho podoby.

4.1 Návrh štruktúry a parametrov na uloženie SOAR scenáru

Zvolenie a návrh korektnej dátovej štruktúry na popis a ukladanie SOAR scenáru nie je jednoduchý a úplne krátkodobý proces, no na základe podrobnej analýzy aktuálnych SOAR riešení (viď kapitola 2.3) a dostupných formátov či štandardov samotných scenárov (viď kapitola 3), bolo rozhodnuté nasledovne.

Ako finálny formát pre popis, uloženie a zobrazenie scenárov automatickej reakcie bol zvolený štandard CACAO a samotná dátová štruktúra bude popísaná v JSON. CACAO najlepšie podporuje víziu zjednotenia no zároveň minimalizáciu zmeny. COPS vyniká svojou jednoduchosťou a čitateľnosťou, no vyžaduje komplexnú transformáciu parametrov. V CACAO štruktúre sú taktiež navyše zachované paralelné vetvy postupov, ktoré sú pri reakcii na incident v určitých prípadoch výhodou. Formát JSON je oproti YAML síce zložitejší, no ponúka lepšiu možnosť zanorenia objektov a podporovateľnejšiu prácu pri prípadnej nadstavbe programom. Navyše, samotná štruktúra a usporiadanie parametrov v CACAO formáte sú veľmi užívateľsky prívetivé, zrozumiteľné a ľahko čitateľné. Pre čitateľa je takmer intuitívne rozpoznanie jednotlivých krokov a funkcionalít scenáru, nakoľko sú rozdelené do samostatných menších „slovníkov“.

Ako základné povinné a niektoré voliteľné parametre budú vo finálnom všeobecnom formáte použité hlavne tieto parametre:

- *Type* – fixný parameter, ktorý musí byť priradený.
- *Spec_version* – fixný parameter, ktorý musí byť priradený.
- *ID* – slúžiaci ako originálny identifikátor.
- *Name* – pre pomenovanie scenáru.
- *Description* – nutný popis pre bližsie pochopenie playbook funkcie.
- *Playbook_types* – zaradenie scenára do určitej skupiny pre ľahšiu identifikáciu.
- *Created_by* – na určenie autora.
- *Modified* – dátum a čas poslednej zmeny scenáru.

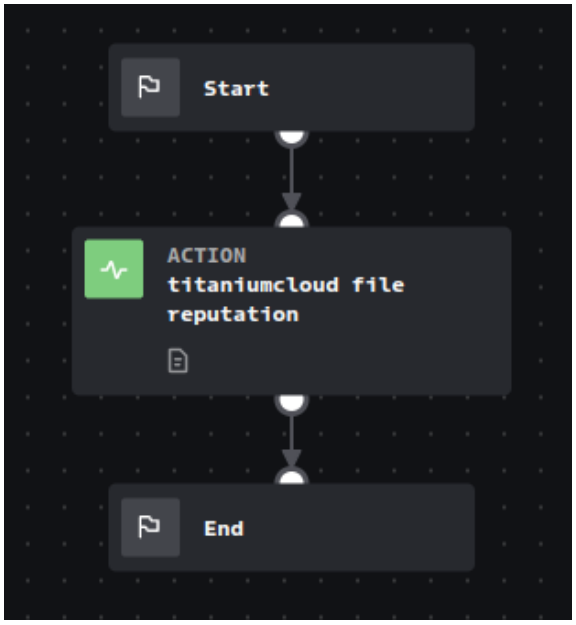
- *Labels* – dôležité doplňujúce informácie, odkazy.
- *External_references* – nepovinné, ale užitočné v prípade externých linkov.
- *Playbook_variables* – definícia playbook premenných, s ktorými sú vykonávané určité operácie.
- *Workflow_start* – prvý playbook blok.
- *Workflow* – nevyhnutné pre definíciu a popis jednotlivých krokov scenáru.
- *Playbook_extentions* – vymenovanie použitých konektorov.
- *Extensions_definitions* – definícia a popis jednotlivých konektorov.
- *Signatures* – voliteľné v prípade podpisov.

Tieto parametre boli následne použité ako základ pri samotnom manuálnom prevedení známych scenárov spoločnosti na tento zvolený a navrhovaný formát. Podrobne priblížené sú v nasledujúcej kapitole samotnej implementácie a prílohách tejto práce.

4.2 Manuálna transformácia vybraných scenárov

Z dôvodu jednoduchosti a najlepšej dostupnosti, boli na prvotnú manuálnu transformáciu zvolené scenáre od spoločnosti Splunk, ktoré sú voľne dostupné na ich GitHub úložisku[1]. Na testovacie účely transformácie boli vybrané dva jednoduché scenáre.

4.2.1 Playbook 1 – Zisťovanie reputácie požadovaného súboru



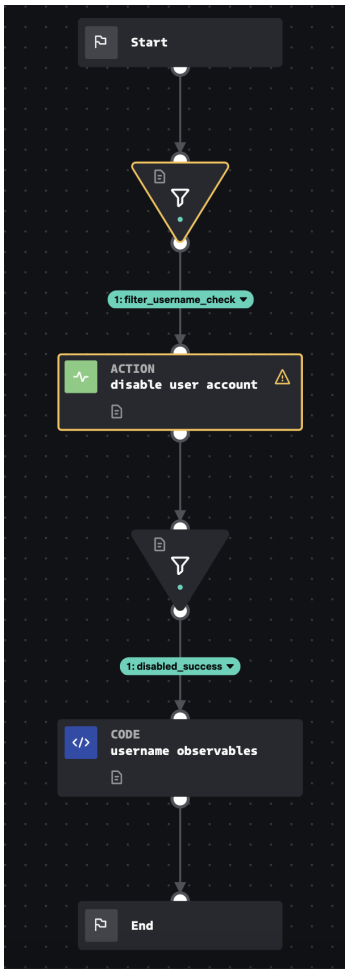
Obr. 4.1: Playbook hodnotenia povesti súboru.

[1]Splunk GitHub úložisko: `https://github.com/phantomcyber/playbooks`.

Tento playbook bol zvolený z hlavného dôvodu – jednoduchosti. Má oficiálny názov *ReversingLabs_TitaniumCloud_File_Reputation*[2]. Úlohou tohto scenára je zistenie tzv. reputácie teda informácií ohľadom konkrétneho súboru, ktoré vykonáva na základe požiadavkov a komunikácie s *Reversinglabs TitaniumCloud* riešením. Táto platforma poskytuje užitočné informácie o známych škodlivých súboroch a jeho vlastnostiach či hrozbách.

Playbook na obrázku 4.1 sa skladá z troch častí/blokov a to začiatočného *start*, stredného vykonávajúceho konkrétny dopyt na konektor/platformu *Reversinglabs TitaniumCloud* a konečného *end*, ktorý definuje koniec postupu scenáru. Ukážka pôvodného a transformovaného scenáru sa nachádza v prílohe C.

4.2.2 Playbook 2 – Blokácia užívateľa v službe *Active Directory*



Obr. 4.2: Playbook blokácie užívateľa v rámci *Active Directory*.

[2]Dostupný na úložisku Github: `https://github.com/phantomcyber/playbooks/blob/6.2/ReversingLabs_TitaniumCloud_File_Reputation.json`.

Tento playbook je špecifický pre Microsoft službu *Active Diretory*, tzv. adresárovú službu, ktorá je založená na protokole LDAP[3] a bol vybraný z dôvodu transformácie a ukážky využitia blokov rozhodovacej podmienky (na obrázku 4.2 znázornené ako trojuholníky/filtre).

Úlohou scenára[4], ktorý sa pôvodne skladá zo šiestich blokov je prípadné zablokovanie konkrétneho užívateľa v rámci služby *Active Directory* (AD). Ukážka pôvodného a transformovaného scenáru sa nachádza v prílohe C.

AD je databáza a súbor služieb, ktoré pomáhajú spravovať a definovať čo, a ktorí užívatelia môžu v sieti vykonávať. Databáza uchováva informácie vo forme objektov, ktoré majú priradené jednotlivé parametre. Môže sa jednať napr. o užívateľa s jednotlivými jedinečnými atribútmi ako meno, heslo, priradené zariadenie, skupina, práva atď. Hlavnou službou AD je *Active Directory Domain Services* (AD DS) v rámci ktorej servery, tzv. radiče domény (DC) vykonávajú kontrolu prístupu k doméne na základe overenia a autorizácie používateľa. [54]

4.3 Funkcionalita a požiadavky nástroja konverzie

Špecifikáciu funkčnosti alebo jednoducho povedané špecifikáciu požiadaviek je možné rozdeliť na dve hlavné oblasti. Jedná sa o funkčné a nefunkčné požiadavky, ktorých definícia je nutnosťou pred samotnou stavbou programu. Funkčnými požiadavkami sa rozumie to, čo má byť samotný softvér schopný vykonať a bez ich naplnenia sa považuje program za nefunkčný. Nefunkčné požiadavky naopak popisujú skôr jednotlivé vlastnosti softvéru a nesúvisia už priamo s popisom jeho funkčnosti. [55]

Funkčné požiadavky

1. Nástroj bude umožnovať automatickú konverziu Splunk SOAR scenárov.
2. Konverzia bude možná pre zadaný súbor predpripravených Splunk scenárov.
3. Konverzia bude možná pre určitý formát scenáru – bude prebiehať kontrola.
4. Výstupom konverzie bude generalizovaný scenár, spĺňajúci zvolený formát.
5. Program bude vykonávať REST[5] API požiadavku (angl. *request*) na konverziu daného scenára.
6. Samotný konvertor načíta a namapuje potrebné informácie o jednotlivých krokoch scenáru na základe slovníka s definovanými spojeniami blokov.
7. Nástroj by mal mať podobu mikroslužby (angl. *microservice*).

[3]LDAP (*Lightweight Directory Access Protocol*) – protokol umožňujúci ľahký prístup k adresáru.

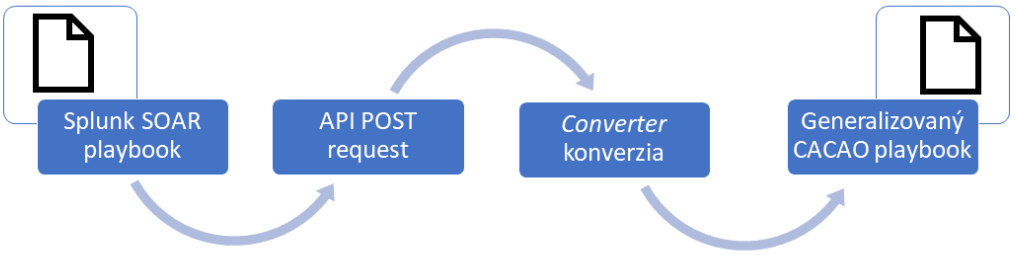
[4]Dostupný na úložisku GitHub: `https://github.com/phantomcyber/playbooks/blob/6.2/AD_LDAP_Account_Locking.json`.

[5]REST (*Representational State Transfer*) – softvérova architektúra, aplikačné rozhranie komunikácie dát pomocou HTTP (Hypertext Transfer Protocol) [56].

Nefunkčné požiadavky

1. Nástroj bude naprogramovaný pomocou frameworku Flask[6] v jazyku Python.
2. Vstupný scenár musí byť vo formáte JSON typu najnovšej verzie Splunk SOAR systému (nesmie obsahovať v dátach kľúč „joint“).
3. Výstupný generalizovaný scenár bude spĺňať zvolený CACAO formát.

Na obrázku 4.3 je znázornená funkcionalita a všeobecný postup nástroja konverzie. Po načítaní určitého Splunk SOAR playbooku prebehne REST API požiadavka typu POST[7] na konverziu. Následne bude vykonaná extrakcia informácií a ich mapovanie na zvolený formát, kde výstupom bude playbook v generalizovanom CACAO formáte.



Obr. 4.3: Návrh funkčnosti nástroja konverzie.

Motivácia funkčnosti konvertora siaha do vízie všeobecného nástroja použiteľného na konverziu scenárov všetkých spoločností, s cieľom generalizácie formátu a zdieľania, no pre účely tejto práce sa zameriava na funkčnú požiadavku konverzie scenárov od spoločnosti Splunk pre ich dostupnosť a najprijateľnejší formát či štruktúru parametrov.

[6]Flask – mikro webový *framework* naprogramovaný v jazyku Python.
[7]POST – jedna z dotazovacích metód protokolu HTTP.

5 Implementácia nástroja automatizovanej konverzie

5.1 Voľba technológií a logika konvertora

Na zostrojenie nástroja konverzie bol použitý mikro webový *framework* Flask, ktorý svojou jednoduchosťou a možnosťou využitia na stavbu softvéru naplnil požiadavky. Flask je považovaný za mikro *framework* pretože nevyžaduje žiadne ďalšie nástroje či nejaké dodatočné interné knižnice a ponúka sa ako základový kameň pre zhotovenie softvéru. Je založený na jazyku Python, a preto bol Python zvolený aj ako programovací jazyk cieľového konvertora – čo je finálna podoba nástroja. Flask vyniká hlavne svojou jednoduchosťou a keďže u nástroja konverzie sa navyše priamo nevyžaduje zostrojenie databázy ako ani prístup k administrácii, je výherným kandidátom pre zostrojenie konvertora. [57]

Flask ako mikro *framework* podporuje aj náplň požiadavky podoby mikroslužby alebo inak povedané mikroservisi (angl. *microservice*). Mikroservisa je typ architektúry, ktorý sa zameriava na oddelenie jednotlivých funkcionalít aplikácie na menšie nezávislé celky, ktoré spoločnou spoluprácou vytvárajú komplexný celok. Základnou vlastnosťou či výhodou je ich nezávislosť a teda možnosť separátneho nasadenia a funkčnosti. To zjednodušuje napríklad proces zmien a aktualizácií, bez nutnosti zásahu do iných mikroslužieb. [58]

Spomínané vlastnosti mikroslužieb sú hlavnými prvkami, ktoré podporili voľbu tohto spôsobu implementácie pre nástroj konverzie. Konvertor je teda implementovaný ako nezávislý program, funkcionalita, ktorá môže byť následne využitá či implementovaná do robustnejšej aplikácie. Výstupné generalizované scenáre môžu byť teda použité ako vstup pre pokročilejší program.

Na ukážku využitia bude v kapitole testovania priblížené použitie výstupných CACAO scenárov ako vstup pre ich grafické vyobrazenie v aplikácií SOAR PLAYBOOK DESIGNER, ktorý bol zhotovený ako bakalársky výstup študenta fakulty informačných technológií Vysokého Učení Technického v Brne, Martina Hemzu. [59]

Pre samotnú implementáciu a prácu s kódom bolo zvolené vývojové prostredie Pycharm od spoločnosti JetBrains, pre jeho jednoduchosť, užívateľskú prívetivosť a predošlé skúsenosti. V rámci jazyka Python, pre implementáciu všetkých potrebných funkcií a behu programu boli využité a integrované nasledovné knižnice: *sys, io* pre prácu s vstupnými a výstupnými parametrami, *json*, *os* pre prácu s funkciami operačného systému, *logging* na správu a záznam logov, *uuid* pre generovanie unikátnych identifikátorov, *OrderedDict* na prácu a usporiadanie slovníkov, *datetime* pre prácu s časom a *request* na posielanie požiadaviek konverzie.

Implementovaná logika samotnej konverzie

Finálny spôsob konverzie si prešiel viacerými fázami premeny, kde musela byť zohľadnená predovšetkým rozmanitosť jednotlivých parametrov (ktorým je venovaná nasledujúca časť 5.2) a zložitosť usporiadania hodnôt v originálnej Splunk podobe scenára. JSON štruktúra je špecifická ukladaním dát v podobe páru „kľúč“:„hodnota“, čo bolo zohľadnené pri každom prístupe ku konkrétnym hodnotám.

Základnou funkciou využitia Flask *framework* je možnosť posielania požiadaviek ako POST, ktorá bude slúžiť ako inicializácia konverzie. Žiadosť je posielaná na konkrétnu adresu koncového bodu (angl. *endpoint*), ktorý je v hlavnej aplikácii *app.py* definovaný pomocou `@app.route()` a slúži na vykonanie definovanej funkcie konverzie. *Endpoint* si jednoducho môžeme predstaviť ako lajcky povedané server, na ktorý budú posielané požiadavky na konverziu scenára za scenárom a on nám bude vracať prekonvertované CACAO scenáre.

Po zaslanej požiadavke, nasleduje teda spustenie `process_json_conversion()` funkcie zodpovednej za inicializáciu samotného objektu konvertora, ktorý pre každý scenár vytvorí inštanciu potrebných parametrov, postupu blokov a nakoniec finálnu štruktúru *cacao_json*, ktorá je už len sformátovaná a uložená do výstupného súboru generalizovaného CACAO scenára. Hlavnou logickou vývrtkou konvertovania je tvorba tzv. pomocnej slovníkovej štruktúry väzieb jednotlivých blokov na základe ich identifikátorov (IDs). Následne sú pre každé ID, ktoré reprezentuje vlastne jednotlivý blok z postupu, zistené jeho parametre, určený typ a vytvorený blok je pridaný do finálnej celkovej *cacao_json* štruktúry. Viď obrázok 5.3 spôsob aplikovanej logiky konverzie.

Tento postup vytvorenia pomocného slovníka je nevyhnutný z dôvodu nutnosti uvedenia ID nasledujúceho kroku v každom CACAO bloku. Postupnosť blokov za sebou je v Splunk scenári definovaná v kľúči „edges“, kde začiatočný alebo aktuálny blok predstavuje hodnotu „sourceNode“ a nasledujúci „targetNode“. Pomocnú štruktúru je si teda možné predstaviť ako slovník ID bloku a zoznamu ID pre nasledujúce bloky – `{„ID sourceNode": [„ID targetNode", „ID targetNode"]}`.

Obr. 5.1: Spôsob aplikovaného postupu konverzie.

5.2 Mapovanie a popis použitých parametrov

Nakoľko má Splunk scenár svoj špecifický formát, jeho prevedenie na finálny všeobecný CACAO sa nezaobišlo bez prvotného namapovania a usporiadania všetkých použitých parametrov. Pri implementácií jednotlivých parametrov sa vychádzalo z kapitoly charakteristiky 3.3 ako aj samotného návrhu predchádzajúcej časti 4.1.

Základom každého scenára, ako už bolo spomínané, sú jeho metadáta, postup jednotlivých krokov/blokov a prípadné informácie o rozšíreniach. Na nasledujúcich stranách bude používaný najmä termín *blok*, ktorý predstavuje rôzne typy krokov, ktoré môžu byť v rámci scenáru definované.

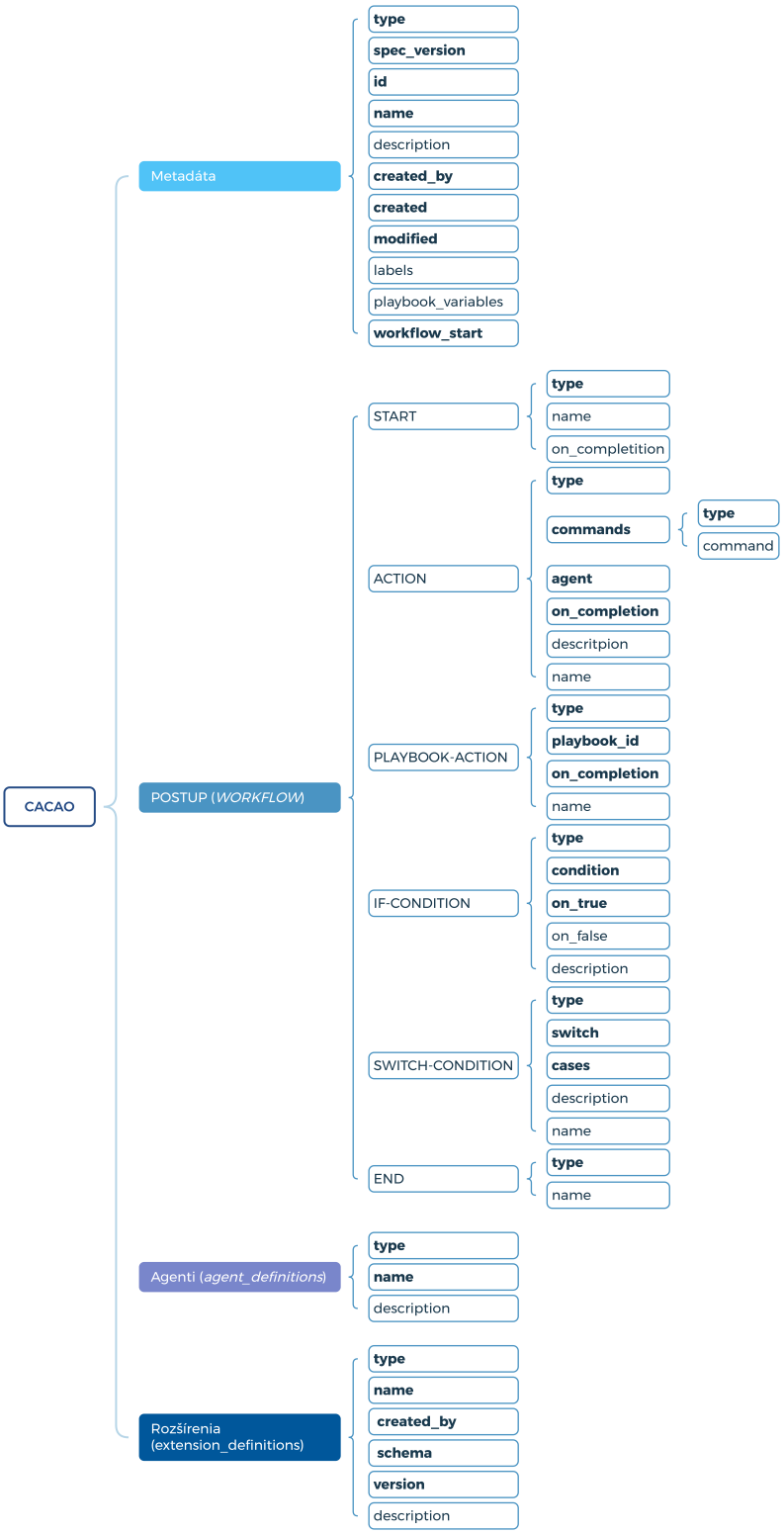
Medzi jednotlivé typy blokov, ktoré boli implementované v rámci nástroja patria: *start, action, playbook-action, if-condition, switch* a *end*. Z dôvodu časovej náročnosti a malej využiteľnosti v originálnom Splunk formáte bola implementácia blokov typu *parallel* a *while-condition* vynechaná.

Základné statické mapovanie pre správnu konverziu a určenie typu bloku na základe originálneho Splunk na CACAO je možné vidieť na nasledujúcom výpise 5.1. V prípade CACAO *action* bloku sa jedná o viacero Splunk typov, ktoré vykonávajú podobné funkcie a ďalej sa ich rozlíšenie prejaví v jednotlivých parametroch *action* bloku.

Výpis 5.1: Mapovanie Splunk typu bloku na CACAO *action* typ.

```
BLOCK_TYPE_MAPPING = {
    "start": "start",
    "action": "action",
    "code": "action",
    "playbook": "playbook-action",
    "filter": "if-condition",
    "format": "action",
    "prompt": "action",
    "utility": "action",
    "decision": "if-condition",
    "end": "end"
}
```

Parametre blokov nie sú však pre všetky rovnaké a líšia sa na základe typu jednotlivého bloku. Na obrázku 5.2 je prehľadné rozdelenie a priblíženie jednotlivých použitých parametrov, ktoré boli zvolené na základe ich povinnosti podľa charakteristiky CACAO formátu či následného významového uváženia v prípade voliteľných. Pri použití parametrov bolo zacielené na zachovanie čo najväčšieho množstva pôvodných Splunk údajov s cieľom ich efektívneho zobrazenia v generalizovanom formáte.



Obr. 5.2: Mapa použitých CACAO parametrov (povinné označené tučne).

Ďalej budú pomocou podrobných tabuliek špecifikované všetky typy blokov, agenti, prípadné rozšírenia a metadáta ako aj ich použité parametre v rámci konvertora. Implementácia bola vykonaná tak aby boli dodržané predovšetkým povinné parametre (podfarbené a označené hviezdičkou) a v prípade konkrétneho mapovania je informácia uvedená v popise parametra. Tabuľka tak vždy obsahuje tri stĺpce popisujúce názov parametra, jeho dátový typ a následne podrobný popis čo je jeho úlohou s doplňujúcimi informáciami mapovania na originál Splunk hodnoty scenára.

Tab. 5.1: Parametre bloku typu ***start***.

Parameter	**Dátový typ**	**Popis**
type*	string	Pre block typu *start* musí byť ***start***.
on_completion*	identifier	ID nasledujúceho bloku scenáru. Generované vo formáte UUID.
name	string	Názov bloku. Rovná sa originál Splunk „functionName“ hodnote.

Tab. 5.2: Parametre bloku typu ***action***.

Parameter	**Dátový typ**	**Popis**
type*	string	Pre block typu *action* musí byť ***action***.
commands*	list	Zoznam príkazov, ktoré majú byť vykonané v rámci tohto bloku. Závisí na pôvodnom Splunk type bloku. V prípade *action* sa rovná parametrom priblíženým v tabuľke 5.3.
agent*	identifier	ID agenta, ktorý vykonáva príkazy bloku a je bližšie definovaný v *agent_definitions*.
on_completion*	identifier	ID nasledujúceho bloku scenáru. Generované vo formáte UUID.
name	string	Názov bloku. Rovná sa originál Splunk „functionName“ hodnote.
description	string	Popis a priblíženie funkcie bloku. Ak existuje, rovná sa originál Splunk „description“ hodnote.

Tab. 5.3: Použité parametre v rámci príkazov – ***commands***.

Parameter	Dátový typ	Popis
type*	string	Musí byť zvolený z vybraných vopred stanovených možností typov ako *manual, bash, powershell* atď. **V prípade tejto práce dodefinované a používané *splunk* a *python*.**
command	string	Text definujúci príkaz, ktorý sa má vykonať. Ak v originál Splunk scenári existuje v rámci bloku „filter“ alebo „query“ hodnota, je priradená parametru *command*.

Tab. 5.4: Použité parametre v rámci agenta – ***agent_definitions***.

Parameter	Dátový typ	Popis
type*	string	**Prednastavené pre účely nástroja na hodnotu „organization“**, nakoľko Splunk konektory sú definované na úrovni názvu organizácie.
name*	string	Rovná sa originál Splunk „connector“ hodnote.
description	string	Rovná sa originál Splunk „connectorConfigs“ hodnote.

Tab. 5.5: Parametre bloku typu ***playbook-action***.

Parameter	Dátový typ	Popis
type*	string	Pre block typu *playbook-action* musí byť ***playbook-action***.
playbook_id*	identifier	ID nadväzujúceho scenára, ktorý sa má vykonať. Zistí sa na základe definovaného mena nasledujúceho scenára „playbookName“, ktoré je vyhľadávané medzi vstupnými scenármi, ak scenár existuje zistí sa z jeho dát ID, ktoré sa rovná hodnote „hash“.
on_completion*	identifier	ID nasledujúceho bloku scenáru. Generované vo formáte UUID.
name	string	Názov bloku. Rovná sa originál Splunk „functionName“ hodnote.

Tab. 5.6: Parametre bloku typu ***if-condition***.

Parameter	Dátový typ	Popis
type*	string	Pre block typu *if-condition* musí byť ***if-condition***.
condition*	string	Jedná sa o *boolean* výraz, ktorý ak je splnený nasleduje blok uložený v parametri *on_true*. Rovná sa kombinácií originálnych Splunk hodnôt „param“+„op“+„value“. Táto trojkombinácia je uložená pod originálnou Splunk hodnotou „conditions“ a podmienku určuje iba tá s hodnotou 0 pre „conditionIndex“.
on_true*	identifier	ID nasledujúceho bloku scenáru v prípade platnej podmienky.
on_false	identifier	ID nasledujúceho bloku scenáru v prípade nesplnenej podmienky. Vyskytuje sa iba v prípade, že v originál Splunk scenári nájdeme aj hodnotu 1 pre „conditionIndex“.
description	string	Popis a priblíženie funkcie bloku. Ak existuje, rovná sa originál Splunk „description“ hodnote.

Každý blok je okrem iného identifikovaný unikátnym ID, ktoré je generované vo formáte UUID verzie 4 využitím Python knižnice *uuid*. V CACAO formáte je navyše pre lepšiu užívateľskú prehľadnosť pridaný aj názov samotného bloku, a preto finálny oficiálny unikátny identifikátor bloku má formát „typ bloku– –ID“.

Ukážka viď výpis 5.2, kde je možné vidieť priradenie identifikátora preddefinovaného typu *end* premennej *on_completion*, teda pre nasledujúci blok scenára, ktorý bude i jeho posledným (typu *end*).

Výpis 5.2: Priradenie ID pre nasledujúci konečný blok.

```
1 import uuid
2 ...
3 self.on_completion = "end--" + str(uuid.uuid4())
```

Na zistenie typu aktuálneho a nasledujúceho bloku sa využíva predovšetkým preddefinované statické mapovanie viď výpis 5.1. Unikátny identifikátor môže byť priradený v rámci parametrov *created_by, on_completion, on_true, on_false, agent, id, workflow_start a playbook_id*.

Tab. 5.7: Použité parametre v rámci rošírení – ***extension_definitions***.

Parameter	Dátový typ	Popis
type*	string	Pre jednotlivé rozšírenie (konektor) musí byť ***extension-definition***.
name*	string	Rovná sa originál Splunk „connector“ hodnote.
created_by*	identifier	Rovná sa ID agenta, podľa ktorého je rozšírenie definované.
schema*	string	Normatívna definícia rošírenia. Môže mať podobu názvu webovej adresy URL (angl. *Uniform Resource Locator*) alebo vysvetľujúceho textu. Rovná sa originál Splunk „connector“ hodnote, nakoľko Splunk v scenároch URL nedefinuje.
version*	string	Verzia konektora, rovná sa originál Splunk „connectorVersion“ hodnote.
description	string	Rovná sa originál Splunk „connectorConfigs“ hodnote.

Tab. 5.8: Parametre bloku typu ***switch***.

Parameter	Dátový typ	Popis
type*	string	Pre block typu *switch* musí byť ***switch***.
switch*	string	Hodnota, ktorá určuje aký blok z parametru *cases* bude nasledovať. Rovná sa originál Splunk hodnote „param“ druhej časti za dvojbodkou, ktorá je tiež uložená v zozname premenných *playbook_variables*. Určujúci parameter pre „param“ je opäť prítomnosť hodnoty 0 pre „conditionIndex“ v „conditions“.
cases*	dictionary	Zoznam všetkých možností, ktoré môže parameter *switch* nadobudnúť, spolu s ich idetifikátormi pre nasledujúci blok.
name	string	Názov bloku. Rovná sa originál Splunk „functionName“ hodnote.
description	string	Popis a priblíženie funkcie bloku. Ak existuje, rovná sa originál Splunk „description“ hodnote.

Tab. 5.9: Použité parametre v rámci metadát – ***metadata***.

Parameter	Dátový typ	Popis
type*	string	Pre časť metadát musí byť ***playbook***.
spec_version*	string	Pre časť metadát musí byť ***cacao-2.0***.
id*	identifier	Unikátne ID scenára. Rovná sa originál Splunk „hash“ hodnote. V prípade chýbajúceho parametra *hash*, nastavené ma hodnotu „Unknown_id“.
name*	string	Názov scenára (playbooku). Rovná sa originál Splunk „category“ hodnote.
created_by*	identifier	Nastavené predpripravenou hodnotou mena autorky tejto práce – „miriam-istonova“.
created*	timestamp	Pôvodný čas vzniku originálneho Splunk scenára. Rovná sa originál „create_time“ hodnote.
modified*	timestamp	Čas vzniku aktuálnej prekonvertovanej verzie scenára. Generovaný automaticky pomocou Python knižnice *datetime* vo formáte „%Y-%m-%dT%H:%M:%S.%f%z“.
workflow_start*	identifier	ID začiatočného *start* bloku, ktoré zahajuje celý scenár. Generované pomocou *uuid*.
description	string	Popis a priblíženie funkcie scenára. Ak existuje, rovná sa originál Splunk „description“ hodnote.
labels	list of string	Potrebné doplňujúce detaily scenára. Môžu zahŕňať hodnoty ako „terms, labels, tags“. Rovná sa originál Splunk „tags“ hodnote.
playbook_vars	dictionary	Správny celý názov parametru je ***playbook_variables*** (z praktických dôvodov v tabuľke skrátené). Jedná sa o zoznam používaných rôznych premenných v rámci scenára naprieč rôznymi blokmi. Definované na konci scenára pred agentami na základe rozhodujúcej podmienky pri bloku typu *switch* viď tabuľka 5.8. Potrebná definícia parametru o aký ide typ, čiže ***type***.

Tab. 5.10: Parametre bloku typu ***end***.

Parameter	Dátový typ	Popis
type*	string	Pre block typu *end* musí byť ***end***.
name	string	Názov bloku. Rovná sa originál Splunk „functionName“ hodnote.

```
"workflow_start": "start--813c77c2-c28e-479e-b536-4f1fa92649c7",
    "workflow": {
        "start--813c77c2-c28e-479e-b536-4f1fa92649c7": {
            "type": "start",
            "name": "on_start",
            "on_completion": "if-condition--77f74b1d-a748-453d-a27c-07c8713cf514"
        },
        "if-condition--77f74b1d-a748-453d-a27c-07c8713cf514": {
            "type": "if-condition",
            "description": "Checks if a artifact exists",
            "condition": "artifact:*.id != 'None' ",
            "on_true": "if-condition--7791e49a-4212-47cc-b116-f3300965f63c",
            "on_false": "action--ee8be181-f112-4fed-81a1-58e4fa4fd42e"
        },
        "if-condition--7791e49a-4212-47cc-b116-f3300965f63c": {
            "type": "if-condition",
            "description": "Only dispatch playbooks against new artifacts.",
            "condition": "artifact:*.id != 'None' ",
            "on_true": "playbook-action--0273a37e-d6e5-4510-8498-e932a876f8ea"
        },
        "playbook-action--0273a37e-d6e5-4510-8498-e932a876f8ea": {
            "type": "playbook-action",
            "name": "dispatch_dns_denylisting_playbooks",
            "playbook_id": "b9a29bbb0e6a16e670d94e2b556576f41a673bf4",
            "on_completion": "if-condition--a559cce0-4ed3-4b03-bfd3-ee9e17ea84f0"
        },
        "action--678f7928-0c49-4db7-a2ac-339f40a4b5ee": {
            "type": "action",
            "name": "format_note",
            "description": "Format a note that merges together normalized data. ",
            "commands": [
                {
                    "type": "splunk",
                    "command": "Splunk SOAR blocked the following domains:\n\n|
                                domain | status | source |\n| --- | --- | ---
                                |\n%%\n| {0} | {1} | {2} |\n%%\n"
                }
            ],
            "agent": "c4799127-4ca8-4658-b07e-4db816858454",
            "on_completion": "action--a2bbea69-2267-482a-9320-397f27f8651e"
        },
```

Obr. 5.3: Ukážka blokov *start, if-condition, playbook-action* a *action*.

5.3 Ukážka finálneho výstupu konvertora

Po úspešnej implementácii sa táto časť bude venovať ukážke finálneho výstupu konvertora, teda samotnému transformovanému generalizovanému CACAO scenáru. Ako ukážkový playbook bude použitý opäť *AD_LDAP_Account_Locking.json*, ktorý bol v časti 4.2.2 bližšie opísaný a taktiež pred samotnou implementáciou manuálne transformovaný, viď príloha C.4 (pre originál viď C.3).

Na obrázkoch 5.4, 5.5 a 5.6 sa nachádza finálna ukážka automaticky prekonvertovaného Splunk scenára na zvolený generalizovaný CACAO pomocou programu konvertora. Každý blok alebo časť scenára je označená samostatnou farbou pre lepšiu čitateľnosť a orientáciu.


```
{
    "type": "playbook",
    "spec_version": "cacao-2.0",
    "id": "732595dc155a58ef5d12b3104904aa7b3237d745",
    "name": "Account Locking",
    "description": "Accepts user name that needs to be disabled in Microsoft LDAP
                    Active Directory. Generates an observable output based on the
                    status of account locking or disabling.",
    "created_by": "miriam-istonova",
    "created": "2023-08-17T18:46:35.895213+00:00",
    "modified": "2024-05-20T19:17:58.298299+0000",
    "labels": [
        "user",
        "microsoft_ad_ldap",
        "disable_account",
        "D3-AL",
        "active_directory"
    ],
    "workflow_start": "start--5ed38841-114e-4e90-8bc1-08e1fbb4c68d",
    "workflow": {
        "start--5ed38841-114e-4e90-8bc1-08e1fbb4c68d": {
            "type": "start",
            "name": "on_start",
            "on_completion": "if-condition--132b7261-e615-4c59-859f-44b4472979ee"
        },
        "if-condition--132b7261-e615-4c59-859f-44b4472979ee": {
            "type": "if-condition",
            "description": "Filter user name inputs to route inputs to appropriate
                            actions.",
            "condition": "playbook_input:user != '' ",
            "on_true": "action--a75bda9e-2193-4a02-a3d8-714c86b05369"
        },
```


Obr. 5.4: Finálna ukážka konverzie – metadáta a blok *start*.

```
"action--1e3f9d40-8d66-4b7b-b95b-ba65c555f886": {
            "type": "action",
            "name": "username_observables",
            "description": "Format a normalized output for each user.",
            "commands": [
                {
                    "type": "python",
                    "command": "\n    # Write your custom code here...\n
username_observables__observable_array = []\n    \n    for user, sam_account,
user_dn, status, msg, prev_status in zip(filtered_result_0_parameter_user,
filtered_result_0_parameter_use_samaccountname, filtered_result_0_data___user_dn,
filtered_result_0_status, filtered_result_0_message,
filtered_result_0_data___starting_status):\n        user_acc_status = {\n
\"type\": \"Microsoft AD LDAP user name\",\n            \"value\": user,\n
\"message\": msg,\n            \"status\": status\n        }\n        \n
username_observables__observable_array.append(user_acc_status)\n
#phantom.debug(username_observables__observable_array)\n"
                }
            ],
            "agent": "c4799127-4ca8-4658-b07e-4db816858454",
            "on_completion": "end--cb6c3e6f-8c51-450f-810f-8615d14e1798"
        },
        "end--cb6c3e6f-8c51-450f-810f-8615d14e1798": {
            "type": "end",
            "name": "on_end"
        },
        "action--a75bda9e-2193-4a02-a3d8-714c86b05369": {
            "type": "action",
            "name": "disable_user_account",
            "description": "Disable user account from filtered playbook inputs.",
            "commands": [
                {
                    "type": "splunk"
                }
            ],
            "agent": "a5730e5d-a396-4695-92c2-35ff391aaf45",
            "on_completion": "if-condition--2eaecdd5-86e9-4642-a33a-5b1dd24efc23"
        },
        "if-condition--2eaecdd5-86e9-4642-a33a-5b1dd24efc23": {
            "type": "if-condition",
            "description": "filter check if the user is disabled successfully.",
            "condition": "disable_user_account:action_result.status == 'success' ",
            "on_true": "action--1e3f9d40-8d66-4b7b-b95b-ba65c555f886"
        }
    },
```


Obr. 5.5: Finálna ukážka konverzie – bloky *action, end* a *if-condition.*

```
"agent_definitions": {
        "c4799127-4ca8-4658-b07e-4db816858454": {
            "type": "organization",
            "name": "Splunk-default",
            "description": "Agent for blocks that are originally from splunk by type
                            format, code and utility."
        },
        "a5730e5d-a396-4695-92c2-35ff391aaf45": {
            "type": "organization",
            "name": "AD LDAP",
            "description": ["microsoft ad ldap"]
        }
    },
    "extension_definitions": {
        "6a794e31-5d5a-4765-99ff-bb9455ef3cb1": {
            "type": "extension-definition",
            "name": "AD LDAP",
            "description": ["microsoft ad ldap"],
            "created_by": "a5730e5d-a396-4695-92c2-35ff391aaf45",
            "schema": "AD LDAP",
            "version": "v1"
        }
    }
}
```


Obr. 5.6: Finálna ukážka konverzie – definícia agentov a rozšírení.

Oproti manuálnej konverzii návrhu boli pre automatizovanú konverziu prevedené a implementované tieto zmeny:

- V prvotnej časti metadát boli vynechané nepovinné parametre *playbook_types*, *playbook_activities* a *playbook_processing_summary*.
- Pre blok typu *if-condition* bol aktualizovaný spôsob určovania parametrov podmienky.
- Pre blok typu *action* bol pridaný povinný parameter *agent* a zároveň odobraté nepovinné parametre vstupu/výstupu, ktoré môžu byť implementované v rámci rošírenia programu do budúcna.
- Preskočená bola tiež implementácia nepovinných slovníkov *playbook_extensions*, *target_definitions* a *signatures*, ktoré patria medzi podnety budúcnosti.
- Pridaná časť detailnej definície agentov scenára.

Jednotlivé bloky nemusia byť nutne vo výslednom scenári zoradené postupne za sebou presne ako logicky nadväzujú. Poradie blokov určuje ich poradie zadefinovania v originálnom Splunk scenári v slovníku *edges*, ktorý je pri ich tvorbe prechádzaný. Pre podrobnejšie vysvetlenie a súvislosti logiky viď časť 5.1.

5.4 Záznam logov priebehu konverzie

Na sledovanie správnosti behu programu, záznamu jednotlivých udalostí a prípadné ladenie a odstraňovanie chýb bol ako súčasť programu zakomponovaný zber udalostí/logov. Samotný Flask má v sebe zaintegrované základné logovanie, no v rámci programu bol tento preddefinovaný *logger* s názvom *werkzeug* „deaktivovaný“ a na záznam udalostí sa v rámci programu používa Python knižnica *logging*.

Pre jednoduchšie ladenie a rozlišovanie prípadných chýb programu bolo logovanie implementované ako do samotného konvertora (skripty `app.py` a `converter.py`) tak i do tzv. klientskej časti (`client_file_folder_posts.py`), ktorá vykonáva samotné POST požiadavky pre každý playbook. Finálne záznamy logov sú automaticky vygenerované po spustení programu a uložené do priečinku „log“ pod názvami `clients_posts.log` a `converter_app.log`.

Na obrázku 5.7 je ukážka hlavného logovania klienského súboru, kde sú informácie pre každý POST playbooku zapisované a ohodnotené postupne ako:

- Výpis názvu aktuálneho playbooku, ktorý bude konvertovaný.
- Status konverzie (200 = úspešne, 400 = neúspešne).
- V prípade neúspechu (angl.*error*) je automaticky vypísaný aj popis chyby. Ak prebehne konverzia úspešne, vypíše sa úspešná hláška štýlu: „Playbook konvertovaný bez problémov“.
- Na koniec je vypísaný názov priečinku a samotného súboru pod akým je nový playbook uložený. V prípade chyby ide o nepodporovaný formát vstupného playbooku, starej verzie Splunk SOAR nazývaný Phantom, ktorého konverziu konvertor nepodporuje.

Logy sú ukladané vo formáte: `dátum, čas - level logu - popis udalosti`. Úrovne (level) logov sa rozdeľujú na základe závažnosti informácie, ktorú ponúkajú. Medzi základných 5 od najmenej závažného po najviac seriózne patria:

1. *DEBUG* – diagnostika pri ladení programu.
2. *INFO* – informatívny výpis o behu programu.
3. *WARNING* – udalostí, ktoré môžu byť problematické.
4. *ERROR* – popisujú chyby, ktoré spôsobujú nesprávny beh programu.
5. *FATAL* – udalostí spôsobujúce celkový pád programu.

Pre účely konvertora sú v logovaciom výpise použité úrovne *INFO, WARNING* a *ERROR*, kde *WARNING* a *ERROR* popisujú v tomto prípade rovnakú „chybu“ len v rôznych log súboroch. Jedná sa o situáciu nepodporovaného vstupného formátu, kedy sa konverzia nevykoná a pokračuje sa na ďalší playbook v priečinku. V prípade priamo logov konvertora (viď 5.8), ak by nastala závažná chyba logiky programu či nepriradenej premennej, zobrazí sa so statusom 500 úrovne *ERROR* s popisom chyby.

```
2024-05-20 21:17:58,239 - INFO - ------------------------ Starting converting ------------------
2024-05-20 21:17:58,239 - INFO - Output folder CACAO_converted_playbooks created.
2024-05-20 21:17:58,240 - INFO - Converting --> activedirectory_reset_password.json
2024-05-20 21:17:58,254 - INFO - 400
2024-05-20 21:17:58,255 - ERROR - Error processing file activedirectory_reset_password.json:
Expecting value: line 1 column 1 (char 0)
2024-05-20 21:17:58,255 - INFO - Unsupported playbook format. Skipping...
2024-05-20 21:17:58,255 - INFO - Converting --> Active_Directory_Disable_Account_Dispatch.json
2024-05-20 21:17:58,265 - INFO - 200
2024-05-20 21:17:58,267 - INFO - Playbook converted without problems.
2024-05-20 21:17:58,268 - INFO - Saved as -->
CACAO_converted_playbooks/Active_Directory_Disable_Account_Dispatch.json_converted
2024-05-20 21:17:58,268 - INFO - Converting --> Active_Directory_Enable_Account_Dispatch.json
2024-05-20 21:17:58,279 - INFO - 200
2024-05-20 21:17:58,280 - INFO - Playbook converted without problems.
2024-05-20 21:17:58,280 - INFO - Saved as -->
CACAO_converted_playbooks/Active_Directory_Enable_Account_Dispatch.json_converted
2024-05-20 21:17:58,280 - INFO - Converting --> advanced_playbook_tutorial.json
2024-05-20 21:17:58,293 - INFO - 400
2024-05-20 21:17:58,293 - ERROR - Error processing file advanced_playbook_tutorial.json:
Expecting value: line 1 column 1 (char 0)
2024-05-20 21:17:58,293 - INFO - Unsupported playbook format. Skipping...
2024-05-20 21:17:58,293 - INFO - Converting --> AD_LDAP_Account_Locking.json
2024-05-20 21:17:58,301 - INFO - 200
2024-05-20 21:17:58,302 - INFO - Playbook converted without problems.
2024-05-20 21:17:58,302 - INFO - Saved as -->
CACAO_converted_playbooks/AD_LDAP_Account_Locking.json_converted
...
2024-05-20 21:17:59,873 - INFO - ------------------------ Conversion finished ------------------
```

Obr. 5.7: Záznamy udalostí priebehu jednotlivých požiadaviek – *clients_posts.log*.

```
[2024-05-20 21:17:58,299] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,307] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,318] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,331] WARNING | app >>> Input playbook format
unsupported. Cannot be converted sorry. Skipping... -- 400
[2024-05-20 21:17:58,340] WARNING | app >>> Input playbook format
unsupported. Cannot be converted sorry. Skipping... -- 400
[2024-05-20 21:17:58,350] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,364] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,374] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,384] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,395] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,406] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,414] INFO | app >>> Conversion successful -- 200
[2024-05-20 21:17:58,422] INFO | app >>> Conversion successful -- 200
```

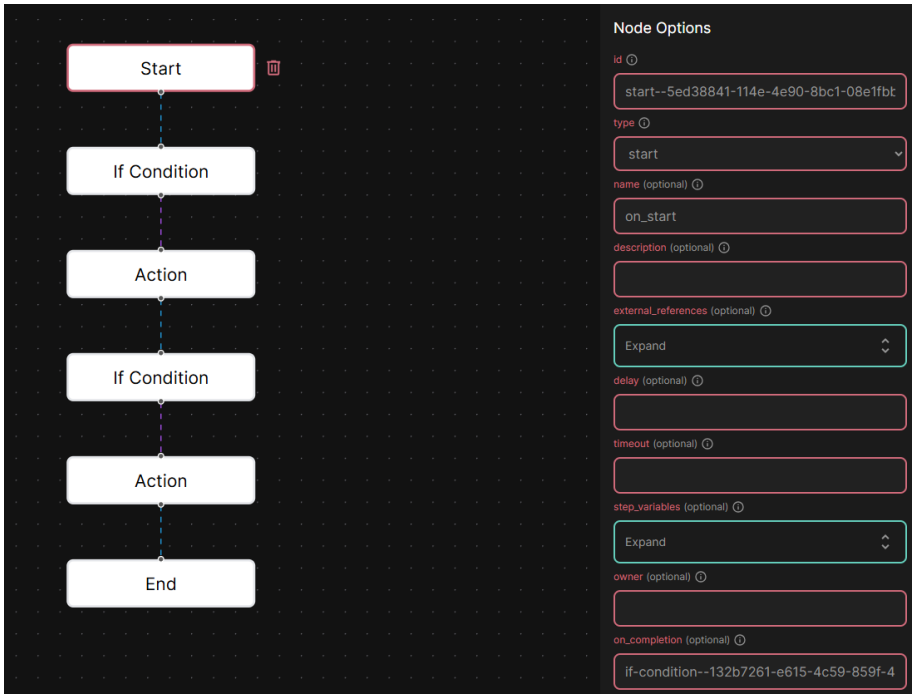
Obr. 5.8: Záznamy udalostí priebehu konverzie – *converter_app.log*.

6 Testovanie funkčnosti konverzie a využitia scenáru

Okrem zabezpečenia požadovaného formátu vstupného scenára, ktorý je kontrolovaný pri behu programu pred samotnou konverziou, bolo otestované taktiež využitie samotnej finálnej podoby transformovaných scenárov. Z celkového počtu 131 originál vstupných Splunk scenárov (voľne dostupných na GitHub Splunk úložisku[1]) bolo za splnenia všetkých podmienok na vstupný formát, pomocou implementovaného nástroja úspešne prekonvertovaných 74 playbookov.

Ako bolo už načrtnuté v časti 5.1, testovanie bolo prevedené ako vyzobrazenie CACAO konvertovaných scenárov vo webovom nástroji SOAR PLAYBOOK DESIGNER [59], ktorý umožňuje grafické zobrazenie jednotlivých SOAR scenárov. Na ukážku možnosti grafického zobrazenia jednotlivých finálnych CACAO scenárov budú použité nasledovné playbooky:

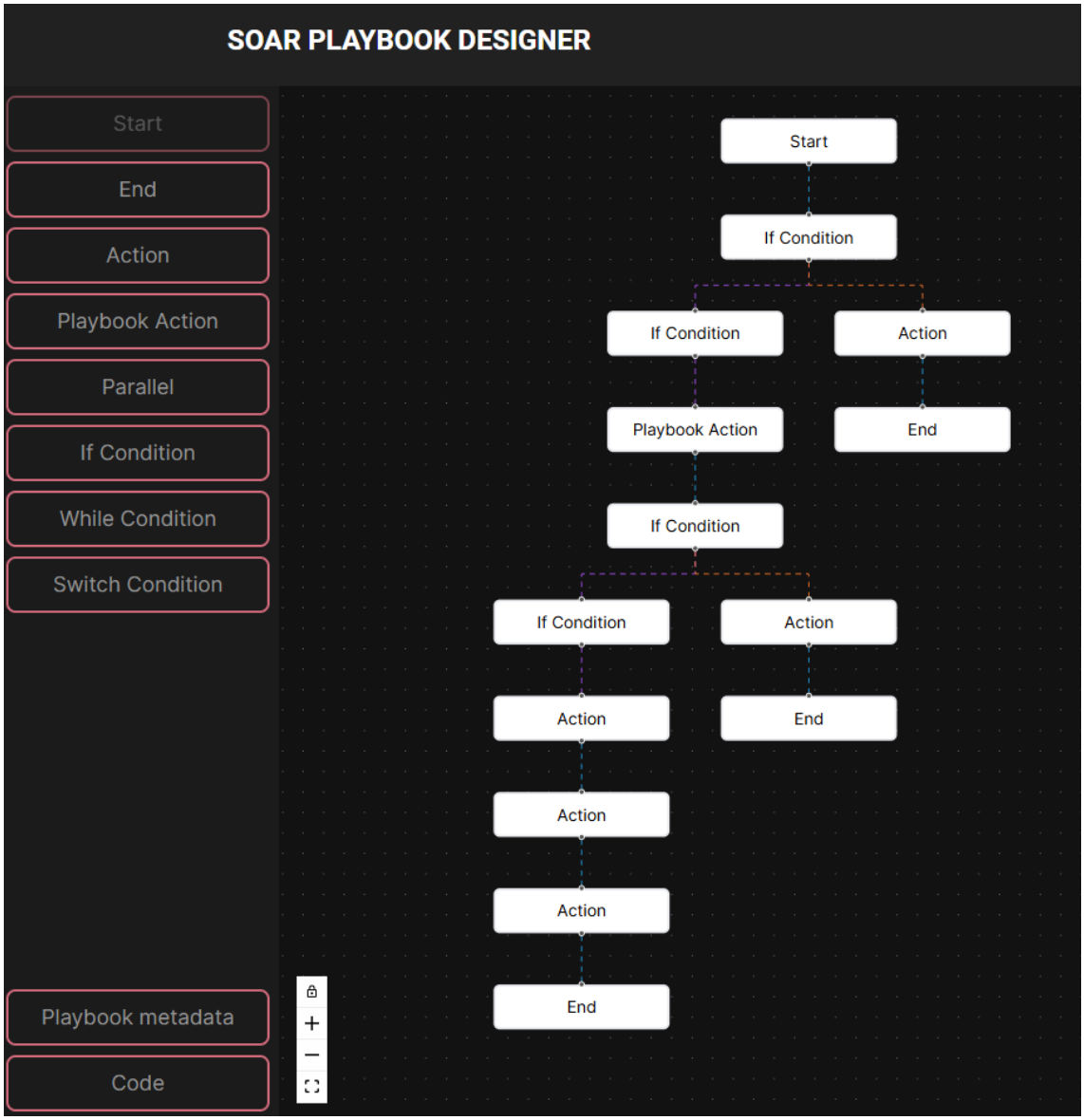
- *converted_AD_LDAP_Account_Locking.json* – viď CACAO ukážka 5.3.
- *converted_DNS_Denylisting_Dispatch.json* – ukážka zložitejšieho vetvenia za použitia *playbook-action* typu bloku.
- *converted_VirusTotal_v3_Identifier_Reputation_Analysis.json* – ukážka najrozvetvenejšieho scenára za použitia *switch* bloku.



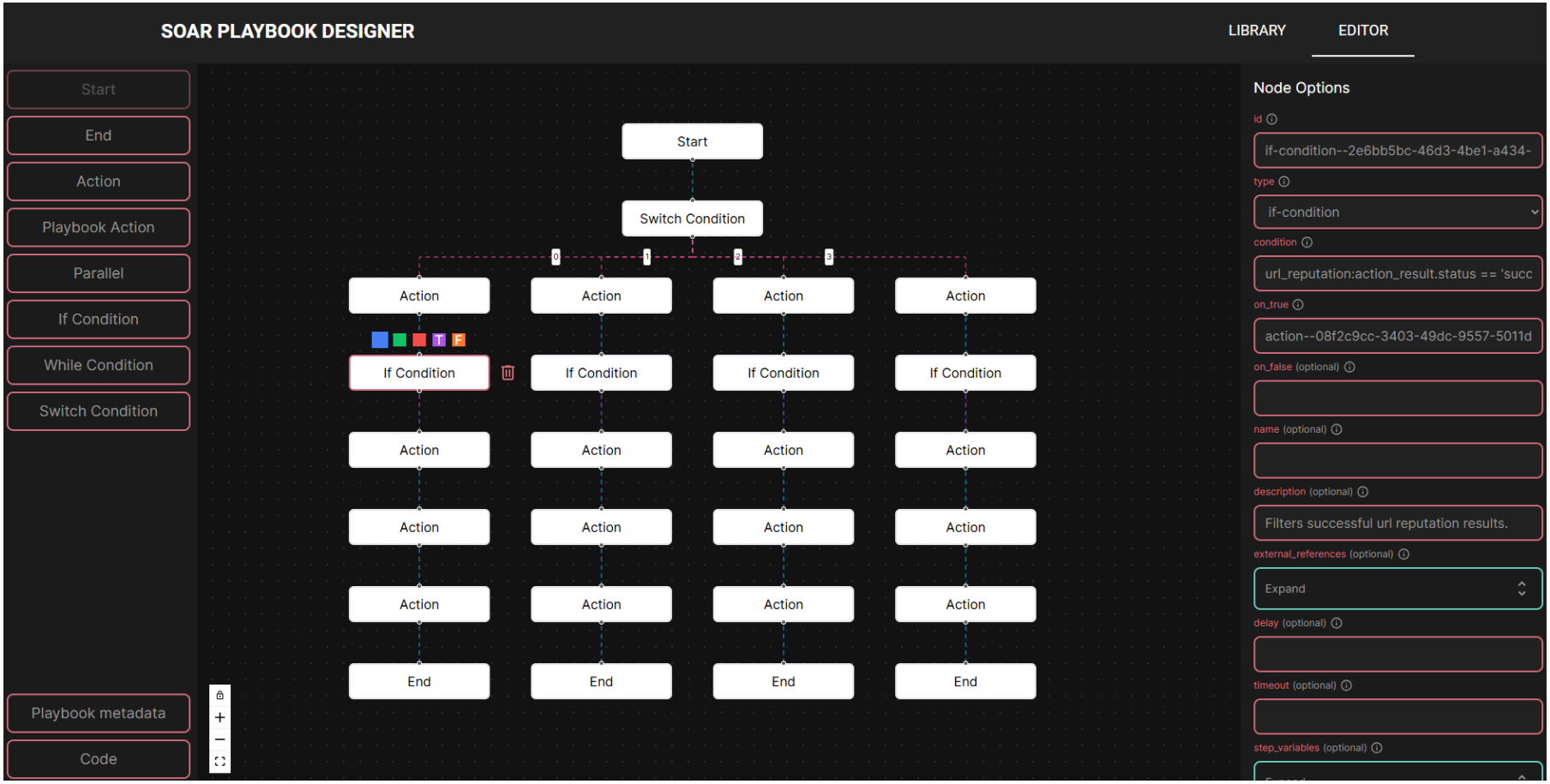
Obr. 6.1: *converted_AD_LDAP_Account_Locking.json* – grafické zobrazenie.

[1]Splunk GitHub: `https://github.com/phantomcyber/playbooks`.

Na obrázku 6.1 je možné vidieť vyobrazenie scenára ako aj pravú bočnú lištu, ktorá sa zobrazí po kliknutí na jednotlivý blok scenára. V tomto prípade je to pre prvý blok typu *start*. Na obrázku 6.2 je možné okrem samotného vetvenia scenára vidieť taktiež ľavú lištu, ktorá ponúka možnosť tvorby/pridania bloku zvoleného typu do scenára ako aj dve tlačítka na zobrazenie uložených parametrov metadát a samotného JSON kódu štruktúry CACAO konvertovaného scenára. Po nahraní JSON finálneho playbooku sa zobrazí práve táto jeho grafická podoba. Tretí obrázok 6.3 ponúka okrem grafickej podoby scenára i celkový pohľad na podobu webového nástroja.



Obr. 6.2: *converted_DNS_Denylisting_Dispatch.json* – grafické zobrazenie.



Obr. 6.3: *converted_VirusTotal_v3_Identifier_Reputation_Analysis.json* – grafické zobrazenie.

Záver

Cieľom tejto bakalárskej práce bol návrh a implementácia nástroja na generalizáciu formátu automatizovaných SOAR scenárov (playbookov), s víziou efektívneho zdieľania znalostí v oblasti reakcie na kyberbezpečnostné incidenty.

Dôraz bol zamierený ako na vhodnú voľbu generalizovaného formátu, ktorého finálna podoba bola realizovaná pomocou využitia vyvíjajúceho sa CACAO štandardu, tak predovšetkým na dosiahnutie samotnej konverzie playbookov za pomoci implementovaného nástroja. Hlavným prínosom samotného nástroja konverzie je teda generalizovaný CACAO formát použitia SOAR scenárov, zabezpečenie úspešnej konverzie 74 playbookov od spoločnosti Splunk a tým podpora zdieľania znalostí v oblasti počítačovej bezpečnosti.

Bakalárska práca bola rozdelená do šiestich kapitol, ktoré zahŕňajú teoretickú a praktickú časť. V teoretickej časti sa venovalo problematike bezpečnostného monitoringu, stratégii a fungovaniu SOC centra, boli vysvetlené a porovnané technológie SIEM a SOAR (viď časť 1.5), priblížili sa princípy automatizácie, zadefinoval scenár automatickej reakcie, uskutočnila analýza dostupných SOAR riešení (viď kapitola 2.3 ako aj analýza dostupných formátov a štandardov, z ktorej bola nakoniec odvodená a zvolená finálna všeobecná CACAO štruktúra pre scenáre konverzie.

Praktická časť sa cez návrh finálnej štruktúry scenára, jej následne aplikovanie v prvotnej manuálnej transformácií a popisu požiadaviek nástroja konverzie, zaoberala hlavne samotnou realizáciou nástroja konverzie. V práci boli priblížené použité technológie a jazyky, vysvetlená logika spôsobu konverzie, podrobne zosumarizované tabuľky všetkých použitých parametrov v rámci scenára, ukážka finálneho výstupu generalizovaného scenára, vysvetlený integrovaný záznam logov a taktiež otestovaná použiteľnosť výsledných scenárov ako vstup pre ich grafické znázornenie v aplikácii SOAR PLAYBOOK DESIGNER.

Samotnú víziu do budúcna a podnety na vylepšenie zahŕňa myšlienka realizácie konverzie SOAR scenárov od ďalších spoločností. Pre náročnosť a komplexnosť formátov, spolu s časovým obmedzením bol pre účel tejto práce na realizáciu konvertora zvolený vstup najprijateľnejšieho formátu scenáru od spoločnosti Splunk. Vízia generalizácie a poskytnutia všeobecného CACAO formátu však siaha do budúcna i za hranice ďalších spoločností ponúkajúcich SOAR riešenia. V rámci efektivity konverzie a cieľa zachovania pôvodných obsahových informácií playbooku čo v najväčšej miere, boli tiež s cieľom vylepšenia pridané určité hodnoty pre niektoré parametre v rámci finálneho formátu.

Na koniec práce boli tiež pridané prílohy, ktorých súčasťou je rozsiahlejšia ukážka dostupných štandardov, podoba originálu a manuálnej konverzie prvotných scenárov, návod na spustenie vytvoreného nástroja a tiež popis obsahu elektronickej prílohy.

Literatúra

[1] KNERLER, Kathryn; PARKER, Ingrid a ZIMMERMAN, Carson. *11 Strategies of a World-Class Cybersecurity Operations Center.* 2. vydanie. The MITRE Corporation, 2022. ISBN 979-8-9856450-4-0. [cit. 2023-11-25].

[2] CHRISSY, Kidd. *SOCs: Security Operation Centers Explained.* Online. SPLUNK. Dostupné z: `https://www.splunk.com/en_us/blog/learn/soc-security-operation-center.html?301=/en_us/data-insider/what-is-a-security-operations-center.html`. [cit. 2023-11-25].

[3] IBM. *What an Security Operations Center (SOC) does.* Online. Dostupné z: `https://www.ibm.com/topics/security-operations-center`. [cit. 2023-11-25].

[4] VIELBERTH, Manfred; FICHTINGER, Ines; BÖHM, Fabian a PERNUL, Günther. *Security Operations Center: A Systematic Study and Open Challenges.* Online. IEEE. 2020, roč. 8, s. 227756 - 227779. ISSN 2169-3536. Dostupné z: IEEE Access, `https://doi.org/10.1109/ACCESS.2020.3045514`. [cit. 2023-11-25].

[5] IREI, Alissa a SHEA, Sharon. *What is incident response? Plans, teams and tools.* Online. TechTarget. Aktualizované Marec 2023. Dostupné z: `https://www.techtarget.com/searchsecurity/definition/incident-response`. [cit. 2023-11-25].

[6] JURGEN. *An OODA-driven SOC Strategy using: SIEM, SOAR and EDR.* Online. Correlated Security. Dostupné z: *http://correlatedsecurity.com/an-ooda-driven-soc-strategy-using-siem-soar-edr/.* [cit. 2023-11-25].

[7] EXABEAM. *The ESSENTIAL GUIDE TO SIEM.* Online. EXCLUSIVE-NETWORKS. Dostupné z: `https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/The-Essential-Guide-to-SIEM.pdf`. [cit. 2023-11-26].

[8] SIDDIQUI, Laiba. *SIEM vs SOAR: What's The Difference?* Online. SPLUNK. Dostupné z: `https://www.splunk.com/en_us/blog/learn/siem-vs-soar.html`. [cit. 2023-11-26].

[9] SHARMA, Ax. *Sigma rules explained: When and how to use them to log events.* Online. CSO. Dostupné z: `https://www.csoonline.com/article/572973/sigma-rules-explained-when-and-how-to-use-them-to-log-events.html`. [cit. 2023-11-26].

[10] NICHOLLS, Mark. *What is SOAR and how does it improve threat detection and remediation?* Online. REDSCAN. Aktualizované 5.9.2023. Dostupné z: https://www.redscan.com/news/what-is-security-orchestration-automation-and-response-soar-and-how-does-it-improve-threat-detection-and-remediation/. [cit. 2023-11-26].

[11] SHEA, Sharon. *SOAR (security orchestration, automation and response).* Online. TECHTARGET. Aktualizované Marec 2023. Dostupné z: https://www.techtarget.com/searchsecurity/definition/SOAR. [cit. 2023-11-26].

[12] SAFONOV, Yehor. *Konference Security 2023.* Online. ARICOMA. Dostupné z:https://konferencesecurity.cz/. [cit. 2023-11-27].

[13] IREI, Alissa a FROEHLICH, Andrew. *Incident response automation: What it is and how it works.* Online. TECHTARGET. Dostupné z: https://www.techtarget.com/searchsecurity/tip/Incident-response-automation-What-it-is-and-how-it-works. [cit. 2023-12-03].

[14] RAPID7. *SOC Automation Playbook.* Online. Dostupné z: https://www.rapid7.com/info/soc-automation-playbook/. [cit. 2023-12-03].

[15] BYKOWSKI, Katie. *How to Build an Incident Response Playbook.* Online. SWIMLANE. Dostupné z: https://swimlane.com/blog/incident-response-playbook/. [cit. 2023-12-03].

[16] JORDAN, Bret a THOMSON, Allan. *CACAO Security Playbooks Version 2.0.* Online. OASIS-OPEN. Dostupné z:https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html. [cit. 2023-12-03].

[17] SIRP. *8 Ways Playbooks Enhance Incident Response.* Online. Dostupné z: https://www.sirp.io/blog/8-ways-playbooks-enhance-incident-response/. [cit. 2023-12-03].

[18] NELSON, Daniel. *Co je to rozhodovací strom?* Online. UNITE. Dostupné z: https://www.unite.ai/cs/co-je-rozhodovac%C3%AD-strom/. [cit. 2023-12-04].

[19] THE IR GURUS. *Playbooks.* Online. GitHub. Dostupné z: https://github.com/TheIRGurus/Playbooks/tree/main. [cit. 2023-12-07].

[20] DEMISTO. *What does this pack do?* Online. GitHub. Dostupné z: https://github.com/demisto/content/tree/master/Packs/QRadar. [cit. 2023-12-07].

[21] IBMRESILIENT. *IBM SOAR Community Applications.* Online. GitHub. Dostupné z: https://github.com/ibmresilient/resilient-community-apps. [cit. 2023-12-07].

[22] DEMISTO. *Cortex XSOAR Platform - Content Repository.* Online. GitHub. Dostupné z: https://github.com/demisto/content. [cit. 2023-12-08].

[23] PHANTOMCYBER. *Community Playbooks.* Online. GitHub. Dostupné z: https://github.com/phantomcyber/playbooks. [cit. 2023-12-08].

[24] SPLUNK. *Splunk SOAR Connectors.* Online. GitHub. Dostupné z: *https://github.com/orgs/splunk-soar-connectors/repositories.* [cit. 2023-12-08].

[25] FORTINET. *Solution-pack-soar-framework.* Online. GitHub. Dostupné z: https://github.com/fortinet-fortisoar/solution-pack-soar-framework/tree/develop/playbooks. [cit. 2023-12-08].

[26] FORTINET. *Fortinet - FortiSOAR Integrations.* Online. GitHub. Dostupné z: https://github.com/orgs/fortinet-fortisoar/repositories. [cit. 2023-12-08].

[27] AZURE. *Azure-Sentinel.* Online. GitHub. Dostupné z: https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks. [cit. 2023-12-08].

[28] AZURE. *DataConnectors.* Online. GitHub. Dostupné z: https://github.com/Azure/Azure-Sentinel/tree/master/DataConnectors. [cit. 2023-12-08].

[29] RAPID7. *Insightconnect-plugins.* Online. GitHub. Dostupné z: https://github.com/rapid7/insightconnect-plugins. [cit. 2023-12-08].

[30] VMRAY. *VMRay Connector for Chronicle SOAR.* Online. GitHub. Dostupné z: https://github.com/vmray/chronicle-soar/tree/main. [cit. 2023-12-08].

[31] IBM. *IBM Security QRadar SOAR.* Online. Dostupné z: https://www.ibm.com/products/qradar-soar. [cit. 2023-12-08].

[32] AZURE. *What is SaaS?* Online. Dostupné z: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas/. [cit. 2023-12-08].

[33] PALOALTO NETWORKS. *Cortex-XSOAR.* Online. Dostupné z: https://www.paloaltonetworks.com/cortex/cortex-xsoar. [cit. 2023-12-08].

[34] CORTEX XSOAR. *Welcome.* Online. Dostupné z: https://xsoar.pan.dev/docs/welcome. [cit. 2023-12-08].

[35] SPLUNK. *Splunk Security Orchestration, Automation and Response (SOAR).* Online. Dostupné z: https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation.html. [cit. 2023-12-08].

[36] SPLUNK. *Splunk SOAR Features.* Online. Dostupné z: https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation-features.html. [cit. 2023-12-08].

[37] FORTINET. *Security Orchestration, Automation, and Response (SOAR).* Online. DostupnÃľz:https://www.fortinet.com/products/fortisoar. [cit. 2023-12-08].

[38] FORTINET. *ORDERING GUIDE FortiSOAR.* Online. Dostupné z: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortisoar.pdf. [cit. 2023-12-08].

[39] FORTINET. *FortiSOAR Empowers Security Operations to Accelerate Incident Response.* Online. Dostupné z: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortisoar-empowers-security-operations-incident-response.pdf. [cit. 2023-12-08].

[40] MICROSOFT. *Microsoft Sentinel.* Online. Dostupné z: https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel. [cit. 2023-12-08].

[41] BAKSHI, Kavish. *What's New: More NEW Microsoft Sentinel SOAR solutions.* Online. TECHCOMMUNITY.MICROSOFT. Aktualizované 13.12.2023. Dostupné z: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/what-s-new-more-new-microsoft-sentinel-soar-solutions/ba-p/3696467. [cit. 2023-12-08].

[42] RAPID7. *Go Easier on Your Analysts with Automation.* Online. Dostupné z: https://www.rapid7.com/products/insightconnect/. [cit. 2023-12-08].

[43] GOOGLE. *Chronicle SOAR Overview.* Online. Dostupné z: https://cloud.google.com/chronicle/docs/soar/overview-and-introduction/soar-overview. [cit. 2023-12-09].

[44] I ZAMORA, Marc Amills. *Deployment of a SOAR open-source tool called the Hive.* Bakalárska práca. Barcelona: Polytechnic University of Catalonia, 2022.

[45] D3 SECURITY. *Smart SOAR For every stack.* Online. Dostupné z: https://d3security.com/. [cit. 2023-12-09].

[46] SWIMLANE. *A Modern Approach to Security Automation.* Online. Dostupné z: https://swimlane.com/swimlane-turbine/. [cit. 2023-12-09].

[47] ELASTIC. *Elastic Security for SOAR. Online.* Dostupné z: https://www.elastic.co/security/soar. [cit. 2023-12-09].

[48] STRANGEBEE. *SECURITY INCIDENT RESPONSE FOR THE MASSES.* Online. Dostupné z: https://thehive-project.org/. [cit. 2023-12-09].

[49] MISP. *MISP Threat Sharing.* Online. Dostupné z: https://www.misp-project.org/. [cit. 2023-12-10].

[50] SHUFFLE. *Shuffle.* Online. Dostupné z: https://shuffler.io/. [cit. 2023-12-10].

[51] SIGMAHQ. *Sigma - Generic Signature Format for SIEM Systems.* Online. GitHub. Dostupné z: https://github.com/SigmaHQ/sigma. [cit. 2023-12-10].

[52] SIGMAHQ. *Sigma specification.* Online. GitHub. Dostupné z: https://github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md. [cit. 2023-12-10].

[53] DEMISTO. *COPS - Collaborative Open Playbook Standard.* Online. GitHub. Dostupné z: https://github.com/demisto/COPS/tree/master. [cit. 2023-12-11].

[54] DETECT. *Active Directory (AD), centralizovaná správa, bezpečnosť.* Online. Dostupné z: https://detect.sk/active-directory-ad-centralizovana-sprava-bezpecnost/. [cit. 2024-05-26].

[55] MSG LIFE. *Funkčné testovanie – functional testing.* Online. Dostupné z: https://msgtester.sk/funkcne-testovanie/. [cit. 2024-05-20].

[56] RED HAT. *What is a REST API? Online.* Dostupné z: https://www.redhat.com/en/topics/api/what-is-a-rest-api#rest. [cit. 2024-05-26].

[57] IT NETWORK. *Lekce 1 - Úvod do frameworku Flask a webových aplikací v Pythonu.* Online. Dostupné z: https://www.itnetwork.cz/python/flask/uvod-do-frameworku-flask-a-webovych-aplikaci-v-pythonu. [cit. 2024-05-22].

[58] NEWMAN, Sam. *Building Microservices.* 2. vydanie. O'Reilly Media, 2021. ISBN 9781492034025. [cit. 2024-05-23].

[59] HEMZA, Martin. *Pokročilý webový nástroj pro správu bezpečnostních korelačních pravidel a kyberbezpečnostních reakcí.* Brno, 2024. Dostupné také z: `https://www.vut.cz/studenti/zav-prace/detail/155315`. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií, Ústav inteligentních systémů. Vedoucí práce Kamil Malinka. [cit. 2024-05-25].

Zoznam symbolov a skratiek

AD *Active Directory* – databáza a súbor služieb, ktoré pomáhajú spravovať a definovať čo, a ktorí užívatelia môžu v sieti vykonávať

AD DS *Active Directory Domain Services* – hlavná služba AD

API *Application Programming Interface* – súbor funkcií a postupov, umožňujúce vytvárať aplikácie, ktoré pristupujú k údajom operačného systému, inej aplikácie alebo služby

CACAO *Collaborative Automated Course of Action Operations* – efinícia štandardu pre implementáciu scenáru reakcie na incident v oblasti kybernetickej bezpečnosti

CISO *Chief Information Security Officer* – riaditeľ a manažér informačnej bezpečnosti

COPS *Collaborative Open Playbook Standard* – voľne dostupný štandard, definujúci primárne postup scenárov reakcie využívajúcich digitálnu forenznú analýzu

DC *Domain Controller* – server v rámci AD, ktorý vykonáva kontrolu prístupu k doméne na základe overenia a autorizácie používateľa

DEMO *Demonstration* – ukážkový náhľad technológie s obmedzenými možnosťami, ponúkaný užívateľovi zadarmo

HTTP *Hypertext Transfer Protocol* – internetový protokol ktorý umožňuje komunikáciu, teda prenos súborov medzi serverom a webovým prehliadačom

ID *Identification* – identifikačné číslo

IDE *Integrated Development Environment* – vývojové prostredie, softvér s integrovanými nevyhnutnými funkciami editora, kompilátora a interpreta pre vývoj programu

IP *Internet Protocol* – používané v spojení IP adresa

JSON *JavaScript Object Notation* – štandardný formát uladania objektových dát

KBI skratka pre kyberbezpečnostný incident

LDAP *Lightweight Directory Access Protocol* – protokol umožňujúci ľahký prístup k adresáru

LES *Log Event Sources* – zaznamenané zdroje udalostí, logy

MISP *Malware Information Sharing Platform* – softvér a komunita na zhromažďovanie, analýzu a zdieľanie indikátorov o KBI a škodlivom softvéri

OASIS *Organization for the Advancement of Structured Information Standards* – neziskové konzorcium, ktoré pracuje na vývoji, zbližovaní a prijímaní voľne dostupných štandardov pre kyberbezpečnosť a ďalšie odvetvia v oblasti informatiky a technológií

MSSP *Managed Security Service Provider* – externý poskytovateľ bezpečnostných služieb

OODA *Observe, Orient, Decide and Act* – moderná stratégia SOC tímu

POST Jedná sa o dotazovaciu metódu protokolu HTTP.

REST *Representational State Transfer* – softvérova architektúra, aplikačné rozhranie komunikácie dát pomocou HTTP

Saas *Software as a Service* – licenčný model na základe predplatného, prístup k softvéru cez internet

SIEM *Security Information and Event Management* – monitorovací nástroj

SOAR *Security Orchestration Automation and Response* – vyspelá technológia spájajúca tri významné riešenia: orchestráciu, automatizáciu a reakciu na bezpečnostné incidenty

SOC *Security Operations Centre* – organizovaná skupina kyberšpecialistov, ktorá sa zaoberá kybernetickou obranou a riešením kyberbezpečnostných incidentov

XML *eXtensible Markup Language* – rozšíriteľný značkovací jazyk

URL *Uniform Resource Locator* – jednotné skrátené ozunačenie pre názov webovej adresy

YAML *Yet Another Markup Language* – ľudsky čitateľný jazyk na serializáciu údajov, často používaný na zápis konfiguračných súborov

Zoznam príloh

A Ukážka scenáru vo formáte COPS

Tento playbook je ukážkou testovacej verzie kontroly autenticity (pravosti) e-mailu. Spočíva v načítaní testovacieho e-mailu zo serveru a jeho následným parsovaním. Potrebné údaje sú extrahované, uložené, porovnávané a vyhodnotené. [22]

Ukážka však slúži predovšetkým na priblíženie formátu a štruktúry scenáru, nie jeho samotnej funkcionality. Preto boli základné definované parametre COPS formátu z kapitoly 3.2 zvýraznené červenou a tučne v prvej priblíženej časti scenára.

```yaml
id: playbook-checkEmailAuthenticity-test
version: -1
name: playbook-checkEmailAuthenticity-test
starttaskid: "0"
tasks:
  "0":
    id: "0"
    taskid: 8f3af618-18e3-454d-836f-2179ca55aed0
    type: start
    task:
      id: 8f3af618-18e3-454d-836f-2179ca55aed0
      version: -1
      name: ""
      iscommand: false
      brand: ""
    nexttasks:
      '#none#':
      - "1"
    separatecontext: false
    view: |-
      {
        "position": {
          "x": 50,
          "y": 50
        }
      }
    note: false
    timertriggers: []
    ignoreworker: false
  "1":
    id: "1"
    taskid: b58b4b73-e328-4e88-8f1e-58201c9f6aec
    type: regular
    task:
      id: b58b4b73-e328-4e88-8f1e-58201c9f6aec
      version: -1
      name: Bring email from server
      description: Sends http request. Returns the response as json.
      scriptName: http
      type: regular
```

```
iscommand: false
      brand: ""
    nexttasks:
      '#none#':
      - "2"
    scriptarguments:
      body: {}
      filename: {}
      headers: {}
      insecure: {}
      method:
        simple: GET
      password: {}
      proxy: {}
      saveAsFile:
        simple: "yes"
      unsecure: {}
      url:
        simple:
https://raw.githubusercontent.com/demisto/content/master/TestData/CheckEmailAuthenticity_test_mail.eml
      username: {}
    separatecontext: false
    view: |-
      {
        "position": {
          "x": 50,
          "y": 195
        }
      }
    note: false
    timertriggers: []
    ignoreworker: false
  "2":
    id: "2"
    taskid: 010d86e9-a3e6-45ae-8762-e7847d7f29d8
    type: regular
    task:
      id: 010d86e9-a3e6-45ae-8762-e7847d7f29d8
      version: -1
      name: Parse Email
      description: Parse an email from an eml or msg file and populate all relevant context
data to investigate the email. Also extracts inner attachments and returns them to the war
room. The incident labels themselves are preserved and not modified - only the "Label/x"
context items that originated from the labels, and the best practice is to rely on these for
the remainder of the playbook.
      scriptName: ParseEmailFiles
      type: regular
      iscommand: false
      brand: ""
    nexttasks:
      '#none#':
      - "3"
    scriptarguments:
      entryid:
        simple: ${File.EntryID}
      max_depth: {}
      parse_only_headers: {}
    results:
    - AttachmentName
    separatecontext: false
```

```
view: |-
      {
        "position": {
          "x": 50,
          "y": 370
        }
      }
    note: false
    timertriggers: []
    ignoreworker: false
  "3":
    id: "3"
    taskid: 651f04dc-657a-45c9-8580-5bb531564f58
    type: regular
    task:
      id: 651f04dc-657a-45c9-8580-5bb531564f58
      version: -1
      name: Check Authenticity
      description: Checks Email authenticity based on its SPF, DMARC and DKIM
      scriptName: CheckEmailAuthenticity
      type: regular
      iscommand: false
      brand: ""
    scriptarguments:
      DKIM_override_fail: {}
      DKIM_override_neutral: {}
      DKIM_override_none: {}
      DKIM_override_pass: {}
      DKIM_override_permerror: {}
      DKIM_override_policy: {}
      DKIM_override_temperror: {}
      DMARC_override_fail: {}
      DMARC_override_none: {}
      DMARC_override_pass: {}
      DMARC_override_permerror: {}
      DMARC_override_temperror: {}
      SPF_override_fail: {}
      SPF_override_neutral: {}
      SPF_override_none: {}
      SPF_override_pass: {}
      SPF_override_permerror: {}
      SPF_override_softfail: {}
      SPF_override_temperror: {}
      headers:
        simple: ${Email.Headers}
    separatecontext: false
    view: |-
      {
        "position": {
          "x": 50,
          "y": 545
        }
      }
    note: false
    timertriggers: []
    ignoreworker: false
```

```
view: |-
  {
    "linkLabelsPosition": {},
    "paper": {
      "dimensions": {
        "height": 590,
        "width": 380,
        "x": 50,
        "y": 50
      }
    }
  }
inputs: []
outputs: []
fromversion: 5.0.0
```

B Ukážka scenáru vo formáte CACAO

Táto príloha obsahuje ukážku príkladu scenáru vo formáte vyvíjajúceho sa štandardu CACAO. Daný playbook slúži ako demonštrácia samotnej štruktúry formátu, nereprezentuje reálne objekty. [16]

Povinné parametre boli označené červenou a tučne.


```
{
  "type": "playbook",
  "spec_version": "cacao-2.0",
  "id": "playbook--61a6c41e-6efc-4516-a242-dfbc5c89d562",
  "name": "Find Malware FuzzyPanda",
  "description": "This playbook will look for FuzzyPanda on the network and in a
SIEM",
  "playbook_types": [ "investigation" ],
  "playbook_activities": [ "analyze-collected-data", "identify-indicators" ],
  "playbook_processing_summary": {
    "data_markings": true
  },
  "created_by": "identity--5abe695c-7bd5-4c31-8824-2528696cdbf1",
  "created": "2023-02-19T08:00:24.918Z",
  "modified": "2023-02-19T08:00:24.918Z",
  "valid_from": "2023-02-19T08:00:24.918Z",
  "valid_until": "2023-12-31T23:59:59.999Z",
  "derived_from": [ "playbook--00ee41a2-c2ca-41da-8ea9-681344eb3926" ],
  "priority": 3,
  "severity": 70,
  "impact": 5,
  "industry_sectors": [ "aerospace", "defense" ],
  "labels": [ "malware", "fuzzypanda", "apt" ],
  "external_references": [
    {
      "name": "ACME Security FuzzyPanda Report",
      "description": "ACME security review of FuzzyPanda 2021",
      "source": "ACME Security Company, Solutions for FuzzyPanda 2021, January
2021. Available online: http://www.example.com/info/fuzzypanda2021.html",
      "url": "http://www.example.com/info/fuzzypanda2021.html",
      "external_id": "fuzzypanda 2023.01",
      "reference_id": "malware--2008c526-508f-4ad4-a565-b84a4949b2af"
    }
  ],
  "markings": [
    "marking-statement--6424867b-0440-4885-bd0b-604d51786d06",
    "marking-tlp--bab4a63c-aed9-4cf5-a766-dfca5abac2bb"
  ],
  "playbook_variables": {
    "__data_exfil_site__": {
      "type": "ipv4-addr",
      "description": "The IP address for the data exfiltration site",
      "value": "1.2.3.4"
    }
  },
```

```
"workflow_start": "start--07bea005-4a36-4a77-bd1f-79a6e4682a13",
  "workflow_exception": " ... ",
  "workflow": {
    "start--07bea005-4a36-4a77-bd1f-79a6e4682a13": {
      "type": "start",
      "name": "Start Playbook Example 1",
      "on_completion": "action--7f40f9d7-de39-4027-ab97-15035beff2ff"
    },
    "action--7f40f9d7-de39-4027-ab97-15035beff2ff": {
      "type": "action",
      "name": "IP Lookup",
      "description": "Lookup the IP address in the SIEM",
      "on_completion": "end--6b23c237-ade8-4d00-9aa1-75999738d557",
      "commands": [
        {
          "type": "manual",
          "command": "Look up IP __data_exfil_site__:value in SIEM",
          "playbook_activity": "identify-indicators"
        }
      ]
    },
    "end--6b23c237-ade8-4d00-9aa1-75999738d557": {
      "type": "end",
      "name": "End Playbook Example 1"
    }
  },
  "playbook_extensions": { ... },
  "authentication_info_definitions": { ... },
  "agent_definitions": { ... },
  "target_definitions": { ... },
  "extension_definitions": { ... },
  "data_marking_definitions": {
    "marking-statement--6424867b-0440-4885-bd0b-604d51786d06": {
      "type": "marking-statement",
      "id": "marking-statement--6424867b-0440-4885-bd0b-604d51786d06",
      "created_by": "identity--5abe695c-7bd5-4c31-8824-2528696cdbf1",
      "created": "2023-02-19T08:00:24.918Z",
      "statement": "Copyright 2023 ACME Security Company"
    },
    "marking-tlp--bab4a63c-aed9-4cf5-a766-dfca5abac2bb": {
      "type": "marking-tlp",
      "id": "marking-tlp--bab4a63c-aed9-4cf5-a766-dfca5abac2bb",
      "created_by": "identity--5abe695c-7bd5-4c31-8824-2528696cdbf1",
      "created": "2022-10-01T00:00:00.000Z",
      "tlpv2_level": "TLP:GREEN"
    }
  },
  "signatures": [ ... ]
}
```

C Ukážka manuálnej transformácie scenárov

Táto príloha je hlavným výstupom kapitoly 4.2 a poskytuje ukážky pôvodných scenárov a ich následných manuálnych mapovaní a pretransformovaní do zvoleného CACAO formátu. Vybrané scenáre sú od spoločnosti Splunk a sú voľne dostupné na GitHub verejnom úložisku.

C.1 Playbook 1 – *ReversingLabs TitaniumCloud File Reputation* – originál


```
{
    "blockly": false,
    "blockly_xml": "<xml></xml>",
    "category": "File Reputation",
    "coa": {
        "data": {
            "description": "Queries ReversingLabs TitaniumCloud for file reputation.",
            "edges": [
                {
                    "id": "port_0_to_port_2",
                    "sourceNode": "0",
                    "sourcePort": "0_out",
                    "targetNode": "2",
                    "targetPort": "2_in"
                },
                {
                    "id": "port_2_to_port_1",
                    "sourceNode": "2",
                    "sourcePort": "2_out",
                    "targetNode": "1",
                    "targetPort": "1_in"
                }
            ],
            "hash": "9fa2c2696f530c43b9d0c8ff0a57f1d94ed75b98",
            "nodes": {
                "0": {
                    "data": {
                        "advanced": {
                            "join": []
                        },
                        "functionName": "on_start",
                        "id": "0",
                        "type": "start"
                    },
                    "errors": {},
                    "id": "0",
                    "type": "start",
                    "warnings": {},
                    "x": 1000,
                    "y": 419.9999999999993
```

```
                "1": {
                    "data": {
                        "advanced": {
                            "join": []
                        },
                        "functionName": "on_finish",
                        "id": "1",
                        "type": "end"
                    },
                    "errors": {},
                    "id": "1",
                    "type": "end",
                    "warnings": {},
                    "x": 1000,
                    "y": 660
                },
                "2": {
                    "data": {
                        "action": "file reputation",
                        "actionType": "investigate",
                        "advanced": {
                            "customName": "titaniumcloud file reputation",
                            "customNameId": 0,
                            "join": [],
                            "note": "Queries Reversinglabs TitaniumCloud for a file hash
                                     reputation"
                        },
                        "connector": "Reversinglabs TitaniumCloud v2",
                        "connectorConfigs": [
                            "reversinglabs_titaniumcloud_v2"
                        ],
                        "connectorId": "0fd5a550-35a4-4641-9d28-9237ec71cf3c",
                        "connectorVersion": "v1",
                        "functionId": 1,
                        "functionName": "titaniumcloud_file_reputation",
                        "id": "2",
                        "parameters": {
                            "hash": "artifact:*.cef.fileHash"
                        },
                        "requiredParameters": [
                            {
                                "data_type": "string",
                                "field": "hash"
                            }
                        ],
                        "type": "action"
                    },
                    "errors": {},
                    "id": "2",
                    "type": "action",
                    "warnings": {},
                    "x": 980,
                    "y": 520
                }
            },
            "notes": ""
        },
        "input_spec": null,
        "output_spec": [
            {
                "contains": [],
                "datapaths": [
                    "file_reputation_1:action_result.data.*.rl.malware_presence.status"
                ],
                "deduplicate": false,
                "description": "Classification",
                "metadata": {},
                "name": "Classification"
            }
        ],
        "playbook_type": "automation",
        "python_version": "3",
        "schema": "5.0.8",
        "version": "5.5.0.108488"
    },
    "create_time": "2023-06-01T13:20:14.880779+00:00",
    "draft_mode": false,
    "labels": [
        "*"
    ],
    "tags": [
        "Externally Authored Content"

}
```

C.2 Playbook 1 – *ReversingLabs TitaniumCloud File Reputation* – návrh

Komentár nie je oficíalne JSON formátom podporovaný, no v nasledujúcej ukážke ich pár bolo pridaných za dvojlomítkom a slúžia na informačné účely pre samotnú implementáciu.

```
{
   "type": "playbook",   // fixný parameter
   "spec_version": "cacao-2.0",   // fixný parameter
   "id": "playbook--71a6c41e-6efc-4516-a242-dfbc5c89d562",  // originálny identifikátor
   "name": "TitaniumCloud_File_Reputation",
   "description": "Queries ReversingLabs TitaniumCloud for file reputation.",
   "playbook_types": [ "investigation" ], // pridať možnosť definície "Automation"
   "playbook_activities": [ "analyze-collected-data" ],
   "playbook_processing_summary": {
     "data_markings": true

   },

   "created_by": "miriam-istonova", // create-time
   "created": "2023-06-01T13:20:14.880Z",
   "modified": "2023-12-03T16:19:24.918Z",
   "labels": [ "Externally Authored Content" ], //tags originálneho Splunk scenáru
   "external_references": [

     {
       "name": "Reversinglabs TitaniumCloud",
       "description": "Queries Reversinglabs TitaniumCloud for a file hash reputation",
       "url": "https://splunkbase.splunk.com/app/6879"
     }
   ],
   "playbook_variables": {
     "__data_exfil_site__": {
       "type": "hash",
       "description": "Hash value from the inspected file",
       "value": "ef9e7175fe883e3dc0d77dfad982846b"
     }
   },

   "workflow_start": "start--999ea005-4a36-4a77-bd1f-79a6e4682a13",
   "workflow": {

     "start--999ea005-4a36-4a77-bd1f-79a6e4682a13": {
       "type": "start",
       "name": "Start",
       "on_completion": "action--8880f9d7-de39-4027-ab97-15035beff2ff"
     },

     "action--8880f9d7-de39-4027-ab97-15035beff2ff": {
       "type": "action",
       "name": "titaniumcloud file reputation",
       "description": "Titaniumcloud File reputation",
       "on_completion": "end--6b23c237-ade8-4d00-9aa1-75999738d557",
       "in_args": null,
       "out_args": ["Classification"],
       "commands": [
         {
           "type": "investigate",
           "command": "artifact:*.cef.__data_exfil_site__", // viď hash parameter
           "playbook_activity": "titaniumcloud_file_reputation"
         }
       ]
     },

     "end--6b23c237-ade8-4d00-9aa1-75999738d557": {
       "type": "end",
       "name": "End"
     },

   },
```

```
  "agent_definitions": { ... },
  "target_definitions": { ... },

  "extension_definitions": {
    "connector1": {

             "name": "Reversinglabs TitaniumCloud v2",
             "connectorId": "0fd5a550-35a4-4641-9d28-9237ec71cf3c"
             "connectorConfigs": ["reversinglabs_titaniumcloud_v2"],
            "connectorVersion": "v1",
            "reference_id": "titanium-0fd5a550-35a4-4641-9d28-9237ec71cf3c"
           },
   },
  "signatures": [ ... ]
}
```

C.3 Playbook 2 – Blokácia užívateľa v službe *Active Directory* – originál


```
{
    "blockly": false,
    "blockly_xml": "<xml></xml>",
    "category": "Account Locking",
    "coa": {
        "data": {
            "description": "Accepts user name that needs to be disabled in Microsoft LDAP
Active Directory. Generates an observable output based on the status of account locking or
disabling.",
            "edges": [
                {
                    "id": "port_0_to_port_2",
                    "sourceNode": "0",
                    "sourcePort": "0_out",
                    "targetNode": "2",
                    "targetPort": "2_in"
                },
                {
                    "conditions": [
                        {
                            "index": 0
                        }
                    ],
                    "id": "port_2_to_port_3",
                    "sourceNode": "2",
                    "sourcePort": "2_out",
                    "targetNode": "3",
                    "targetPort": "3_in"
                },
                {
                    "id": "port_4_to_port_1",
                    "sourceNode": "4",
                    "sourcePort": "4_out",
                    "targetNode": "1",
                    "targetPort": "1_in"
                },
                {
                    "id": "port_3_to_port_5",
                    "sourceNode": "3",
                    "sourcePort": "3_out",
                    "targetNode": "5",
                    "targetPort": "5_in"
                },
                {
                    "conditions": [
                        {
                            "index": 0
                        }
                    ],
                    "id": "port_5_to_port_4",
                    "sourceNode": "5",
                    "sourcePort": "5_out",
                    "targetNode": "4",
                    "targetPort": "4_in"
                }
            ],
```

```
            "hash": "732595dc155a58ef5d12b3104904aa7b3237d745",
            "nodes": {
                "0": {
                    "data": {
                        "advanced": {
                            "join": []
                        },
                        "functionName": "on_start",
                        "id": "0",
                        "type": "start"
                    },
                    "errors": {},
                    "id": "0",
                    "type": "start",
                    "warnings": {},
                    "x": 19.999999999999986,
                    "y": -6.394884621840902e-14
                },
                "1": {
                    "data": {
                        "advanced": {
                            "join": []
                        },
                        "functionName": "on_finish",
                        "id": "1",
                        "type": "end"
                    },
                    "errors": {},
                    "id": "1",
                    "type": "end",
                    "warnings": {},
                    "x": 19.999999999999986,
                    "y": 864
                },
                "2": {
                    "data": {
                        "advanced": {
                            "customName": "username filter",
                            "customNameId": 0,
                            "delimiter": ",",
                            "delimiter_enabled": true,
                            "description": "Filter user name inputs to route inputs to
appropriate actions.",
                            "join": [],
                            "note": "Filter user name inputs to route inputs to appropriate
actions."
                        },
                        "conditions": [
                            {
                                "comparisons": [
                                    {
                                        "conditionIndex": 0,
                                        "op": "!=",
                                        "param": "playbook_input:user",
                                        "value": ""
                                    }
                                ],
                                "conditionIndex": 0,
                                "customName": "filter_username_check",
                                "logic": "and"
                            }
                        ],
```

```
"functionId": 1,
                        "functionName": "username_filter",
                        "id": "2",
                        "type": "filter"
                    },
                    "errors": {},
                    "id": "2",
                    "type": "filter",
                    "warnings": {},
                    "x": 60,
                    "y": 140
                },
                "3": {
                    "data": {
                        "action": "disable account",
                        "actionType": "generic",
                        "advanced": {
                            "customName": "disable user account",
                            "customNameId": 0,
                            "delayTime": 0,
                            "description": "Disable user account from filtered playbook
inputs.",
                            "join": [],
                            "note": "Disable user account from filtered playbook inputs."
                        },
                        "connector": "AD LDAP",
                        "connectorConfigs": [
                            "microsoft ad ldap"
                        ],
                        "connectorId": "a5730e5d-a396-4695-92c2-35ff391aaf45",
                        "connectorVersion": "v1",
                        "functionId": 1,
                        "functionName": "disable_user_account",
                        "id": "3",
                        "parameters": {
                            "use_samaccountname": true,
                            "user": "filtered-
data:username_filter:condition_1:playbook_input:user"
                        },
                        "requiredParameters": [
                            {
                                "data_type": "string",
                                "default": false,
                                "field": "user"
                            }
                        ],
                        "type": "action"
                    },

                    "errors": {},
                    "id": "3",
                    "type": "action",
                    "warnings": {},
                    "x": 0,
                    "y": 328
                },
```

```
"4": {
                    "data": {
                        "advanced": {
                            "customName": "username observables",
                            "customNameId": 0,
                            "description": "Format a normalized output for each user.",
                            "join": [],
                            "note": "Format a normalized output for each user."
                        },
                        "functionId": 1,
                        "functionName": "username_observables",
                        "id": "4",
                        "inputParameters": [
                            "filtered-
data:filter_disable_account:condition_1:disable_user_account:action_result.parameter.user",
                            "filtered-
data:filter_disable_account:condition_1:disable_user_account:action_result.parameter.use_sama
ccountname",
                            "filtered-
data:filter_disable_account:condition_1:disable_user_account:action_result.data.*.user_dn",
                            "filtered-
data:filter_disable_account:condition_1:disable_user_account:action_result.status",
                            "filtered-
data:filter_disable_account:condition_1:disable_user_account:action_result.message",
                            "filtered-
data:filter_disable_account:condition_1:disable_user_account:action_result.data.*.starting_st
atus"
                        ],
                        "outputVariables": [
                            "observable_array"
                        ],
                        "type": "code"
                    },
                    "errors": {},
                    "id": "4",
                    "type": "code",
                    "userCode": "\n    # Write your custom code here...\n
username_observables__observable_array = []\n    \n    for user, sam_account, user_dn,
status, msg, prev_status in zip(filtered_result_0_parameter_user,
filtered_result_0_parameter_use_samaccountname, filtered_result_0_data___user_dn,
filtered_result_0_status, filtered_result_0_message,
filtered_result_0_data___starting_status):\n        user_acc_status = {\n
\"type\": \"Microsoft AD LDAP user name\",\n            \"value\": user,\n
\"message\": msg,\n            \"status\": status\n        }\n        \n
username_observables__observable_array.append(user_acc_status)\n
#phantom.debug(username_observables__observable_array)\n",
                    "warnings": {},
                    "x": 0,
                    "y": 680
                },
                "5": {
                    "data": {
                        "advanced": {
                            "customName": "filter disable account",
                            "customNameId": 0,
                            "delimiter": ",",
                            "delimiter_enabled": true,
                            "description": "filter check if the user is disabled
successfully.",
                            "join": [],
                            "note": "filter check if the user is disabled successfully."
                        },
```

```
"conditions": [
                            {
                                "comparisons": [
                                    {
                                        "conditionIndex": 0,
                                        "op": "==",
                                        "param": "disable_user_account:action_result.status",
                                        "value": "success"
                                    }
                                ],
                                "conditionIndex": 0,
                                "customName": "disabled_success",
                                "logic": "and"
                            }
                        ],
                        "functionId": 2,
                        "functionName": "filter_disable_account",
                        "id": "5",
                        "type": "filter"
                    },
                    "errors": {},
                    "id": "5",
                    "type": "filter",
                    "warnings": {},
                    "x": 60,
                    "y": 500
                }
            },
            "notes": "Inputs: users\nInteractions: Microsoft AD LDAP\nActions: Account
Locking/Disabling\nOutputs: observables"
        },
        "input_spec": [
            {
                "contains": [
                    "user name"
                ],
                "description": "A user name provided to be disable - AD LDAP",
                "name": "user"
            }
        ],
        "output_spec": [
            {
                "contains": [],
                "datapaths": [
                    "username_observables:custom_function:observable_array"
                ],
                "deduplicate": false,
                "description": "An array of observable dictionaries ",
                "metadata": {},
                "name": "observable"
            }
        ],
        "playbook_type": "data",
        "python_version": "3",
        "schema": "5.0.10",
        "version": "6.0.1.123902"
    },
    "create_time": "2023-08-17T18:46:35.895213+00:00",
    "draft_mode": false,
    "labels": [
        "*"
    ],
    "tags": [
        "user",
        "microsoft_ad_ldap",
        "disable_account",
        "D3-AL",
        "active_directory"
    ]
}
```

C.4 Playbook 2 – Blokácia užívateľa v službe *Active Directory* – návrh

Návrh pokrýva transformáciu hlavnej štruktúry ako metadáta (popisujúce všeobecné vlastnosti playbooku), prevažne povinné parametre, objekty jednotlivých krokov (bloky), konektory či prípadné rozšírenia a občasné komentáre slúžia ako podnety pre samotnú implemetáciu.

```
{
  "type": "playbook", // fixný parameter
  "spec_version": "cacao-2.0", // fixný parameter
  "id": "playbook--856ac71-6efc-4516-a1c42-dfbc6eb24d562",
  "name": "LDAP_Account_Locking",
  "description": "Accepts user name that needs to be disabled in Microsoft LDAP Active Directory.
Generates an observable output based on the status of account locking or disabling.",
  "playbook_types": ["remediation"], // pretože vykonáva finálnu funkciu blokovania účtu
  "playbook_activities": ["analyze-collected-data"],
  "playbook_processing_summary": {
    "data_markings": true
  },
  "created_by": "miriam-istonova",
  "created": "2023-08-17T18:46.880Z", // create - time
  "modified": "2023-12-10T16:19:24.918Z",
  // tags originálneho Splunk scenáru:
  "labels": ["user", "microsoft_ad_ldap", "disable_account", "D3-AL", "active_directory"],

  "playbook_variables": {
    // bude doplnené
  },

  "workflow_start": "start--879ea025-4a36-74a7-bd1f-6e479a682a13",
  "workflow": {

                "start--879ea025-4a36-74a7-bd1f-6e479a682a13": {
                    "type": "start",
                    "name": "Start",
                    "on_completion": "if-condition--9780f9d7-de39-4a27-ab97-035b15eff2ff"
                },

                "if-condition--9780f9d7-de39-4a27-ab97-035b15eff2ff": {
                  "type": "if-condition", // filter
                  "name": "username filter", // návrh možného pridania parametru
                  "description": "Filter user name inputs to route inputs to appropriate actions.",
                  //nutná úprava a prepojenie s playbook_variables:
                  "condition": "__playbook_input_user__:user",

                  "on_true": "action--7780f9d7-de39-3627-ab97-ff2ff15035be"
                },

                "action--7780f9d7-de39-3627-ab97-ff2ff15035be": {
                  "type": "action",
                  "name": "disable user account",
                  "description": "Disable user account from filtered playbook inputs.",
                  "on_completion": "if-condition--d79780f9-1d39-4a27-cb96-eff2035b15ff",
                  "in_args": //doplniť,
                  "out_args": ["observable_array"], //zmeniť
```

```
"commands": [{
                    "type": "investigate", // nový krok
                    "command": "artifact:*.cef.__data_exfil_site__", // viď hash parameter
                    "playbook_activity": "titaniumcloud_file_reputation"}]
                },

                "if-condition--d79780f9-1d39-4a27-cb96-eff2035b15ff": {
                  "type": "if-condition", // filter
                  "name": "filter disable account", // návrh možného pridania parametru
                  "description": "Filter check if the user is disabled successfully.",
                  "condition": "__disable_user_account__:staus", //nutnosť doplnenia
                  "on_true": "action--6680f9d7-de39-3627-db97-ff2ff15035bf",
                },

                "action--6680f9d7-de39-3627-db97-ff2ff15035bf": {
                  "type": "action",
                  "name": "username observables",
                  "description": "Format a normalized output for each user.",
                  "on_completion": "end--6b23c237-ade8-4d00-9aa1-75999738d557",
                  "in_args": //doplniť,
                  "out_args": ["observable_array"], //skontrolovať

                  "commands": [{
                    "type": "code", // nový krok
                    "command": "", //nutné dodefinovať
                  }]
                },

                "end--6b23c237-ade8-4d00-9aa1-75999738d557": {
                  "type": "end",
                  "name": "End"
                }

},

  "playbook_extensions": {
    "connector1": "ldap-a5730e5d-a396-4695-92c2-35ff391aaf45",
  },

  "agent_definitions": {...},
  "target_definitions": {...},
  "extension_definitions": {
    "connector1": {

        "name": "AD LDAP",
        "connectorId": "a5730e5d-a396-4695-92c2-35ff391aaf45"
        "connectorConfigs": ["microsoft ad ldap"],
        "connectorVersion": "v1",
        "reference_id": "ldap-a5730e5d-a396-4695-92c2-35ff391aaf45"
    },
  },
  "signatures": [...],
}
```

D Návod na spustenie nástroja

Na spustenie nástroja konverzie je potrebné naplniť iba 3 základné požiadavky:

- Programovací jazyk *Python* – odporúčaná verzia 3.10 a vyššie.
- Potrebné balíčky z `requirements.txt` – možné doinštalovať pomocou: `pip install -r requirements.txt`.
- Spúšťať v prostredí IDE – napríklad *PyCharm* alebo *Visual Studio Code*.

Samotný nástroj bol vyvíjaný na operačnom systéme Windows v IDE[1] prostredí **PyCharm** od spoločnosti JetBrains a preto je tento postup zaručený. Po otvorení priečinku elektronickej prílohy v tomto prostredí, jediné čo je potrebné je nastavenie interpreta na nainštalovaný Python a v pravo hore **je po zvolení daného súboru možné tento súbor pomocou zelenej šípky spustiť**.

Pre správny chod programu je nutné spustiť súbory v tomto poradí:

1. `app.py` – spustenie Flask API.
2. `client_file_folder_posts.py` – skript požiadaviek automatickej konverzie.

Po úspešnej konverzii sa nad umiestneným „client“ skriptom v súbore *client* objaví nový priečinok ***CACAO_converted_playbooks*** v ktorom je možné nájsť všetky prekonvertované generalizované CACAO scenáre.

[1] IDE (*Integrated Development Environment*) – vývojové prostredie, softvér s integrovanými nevyhnutnými funkciami editora, kompilátora a interpreta pre vývoj programu.

E Obsah elektronickej prílohy

Priečinok elektronickej prílohy pozostáva z dvoch hlavných častí. Jednou je samotný priečinok so všetkými finálnymi prekonvertovanými CACAO scenármi pomocou vytvoreného nástroja. Druhý priečinok je vlastne samotný nástroj konverzie, po ktorom spustení sa v priečinku *client* automaticky vytvorí nový priečinok výstupu transformovaných scenárov *CACAO_converted_playbooks*. Po spustení programu je taktiež automaticky vytvorený ďalší priečinok *log*, ktorý ukladá súbory záznamov priebehu udalostí.

- `SOAR_konvertor+transformovane_scenare` ... priečinok súborov elektr. prílohy
  - `CACAO_final_converted_playbooks` ..... priečinok s finálnymi scenármi
  - `flask_soar_converter` ..... priečinok kompletného nástroja konverzie
    - `src` ..... priečinok obsahujúci zdrojové kódy
      - `client` ..... priečinok skriptu požiadaviek a vstupných scenárov
        - `SPLUNK_input_playbooks` ..... priečinok vstupných scenárov
        - `client_file_folder_posts.py` ..... skript požiadaviek konverzie
      - `data_blocks` ..... priečinok obsahujúci triedy objektov blokov
        - `action.py` ..... súbor triedy typu bloku *action*
        - `agent.py` ..... súbor triedy agentov
        - `end.py` ..... súbor triedy typu bloku *end*
        - `extension.py` ..... súbor triedy rozšírení
        - `ifko.py` ..... súbor triedy typu bloku *if-condition*
        - `metadata.py` ..... súbor triedy metadát
        - `playbook.py` ..... súbor triedy typu bloku *playbook-action*
        - `start.py` ..... súbor triedy typu bloku *start*
        - `switch.py` ..... súbor triedy typu bloku *switch*
      - `app.py` ..... súbor hlavného *flask* programu
      - `config.py` ..... súbor prednastavených premenných
      - `converter.py` ..... súbor nástroja konverzie
    - `requirements.txt` ..... súbor závislostí pre beh programu