

Tímový projekt 2 - Dokumentácia

Systém pre manažment incidentov

Vedúci projektu: Ing. Štefan Balogh, PhD.

Členovia tímu: Bc. Adam Budziňák

Bc. Tomáš Petráni

Bc. Daniel Ondrejka

Bc. Radovan Borsig

Bc. Filip Kolenčík

Zadanie

Zadanie obsahuje návrh a implementáciu frameworku pre znalostný manažment vhodny pre CSIRT team. Ďalšou časťou zadania je vytvorenie učinných postupov pre jednotlivé typy útokov formou playbookov. Playbooky ma umožňovať framework vytvárať manualne, alebo importovať existujuce z iných zdrojov. Framework by mal tiež podporovať automatizované spúšťanie vybraných častí playbookov.

Obsah

1 Teoretická časť	1
1.1 CSIRT	1
1.2 Playbook	1
1.2.1 Klúčové komponenty playbookov	2
1.2.2 Význam playbookov	2
1.3 Manažment znalostí	2
1.3.1 Znalosti pre bezpečnostné incidenty	3
2 Dostupné zdroje znalostí a incidentov	4
2.1 Databázy	4
2.2 Bezpečnostné komunity a fóra	4
3 Existujúce riešenia pre manažment znalostí	5
3.1 SASP	5
3.1.1 Výhody	5
3.1.2 Nevýhody	5
3.2 MISP	5
3.2.1 Výhody	6
3.2.2 Nevýhody	6
3.3 Ad2Play	6
3.4 Nevýhody existujúcich riešení	7
4 Použité riešenie	8
4.1 Popis použitého riešenia	8
4.1.1 Komponent vytváranie playbookov	9
4.1.2 Komponent vizualizácie playbookov	10
4.1.3 Komponent playbook parser	10
4.2 Ukážka použitého riešenia	10
5 Zimný semester - vylepšenia	12
5.1 Implementácia štandardu CACAO 2.0	12
5.2 Implementácia CACAO roaster	15
5.3 Handling nahrávania playbookov	16
5.4 YAML formát	16

6 Letný semester - vylepšenia	17
6.1 Výber playbookov	17
6.2 Dodefinovanie playbookov	17
6.3 Vylepšenie GUI	19
6.4 Automatické nahrávanie playbookov	19
6.5 Vizualizácia playbookov	22
7 Testovanie playbookov	23
7.1 Scenár 1 - Otvorenie škodlivého súboru	23
7.2 Scenár 2 - Podozrivé pripojenie na univerzitný systém	26
7.3 Scenár 3 - Šírenie malvéru cez podvodnú doménu v e-mailoch	29
8 Zápisnice	31
Zoznam použitej literatúry	45

1 Teoretická časť

1.1 CSIRT

Computer Security Incident Response Team (CSIRT), sú tímy s príslušne kvalifikovanými a dôveryhodnými členmi organizácie, ktorí riešia incidenty počas ich životného cyklu [1].

CSIRT sa vyvinuli, aby slúžili ako hlavná opora kybernetickej bezpečnosti, sietí a informačných systémov [2]. Často sú prirovnávané k hasičskému zboru, zasahujúcemu v núdzových situáciách na podporu a poskytovanie pomoci, ale tiež zabezpečujú, aby boli získané a zdieľané ponaučenia a taktiež skúsenosti po incidentoch. CSIRT sa venuje bezpečnostným incidentom vzniknutým v počítačových sietach, ktorých riešenie tímy koordinujú a snažia sa im v budúcnosti predchádzať.

Okrem spracovania incidentov môže CSIRT poskytovať ďalšie reaktívne služby [3], ako sú výstrahy a varovania, riešenie zraniteľností, manipulácia s artefaktmi, proaktívne služby, ako je sledovanie technológie, vývoj nástrojov, služby detekcie narušenia a skenovania. Nakoniec aj služby riadenia kvality bezpečnosti napríklad ako zvyšovanie informovanosti, certifikácia produktov alebo školenia.

1.2 Playbook

Playbook inak nazývaný aj príručka [4], je kolekcia stratégií, plánov a pokynov určených na systematické dosahovanie konkrétnych cieľov. Slúži ako sprievodca či manuál, ktorý obsahuje osvedčené postupy a kľúčové akcie, ktoré majú jednotlivci alebo tímy dodržiavať v rôznych scenároch. Príručky sa bežne používajú v podnikaní, športe, informačných technológiách a v mnoho ďalších oblastiach pri vykonávaní úloh a reagovaní na rôzne výzvy. Pomáhajú štandardizovať operácie, zefektívňujú rozhodovacie procesy a majú celkový dopad na zlepšovanie výkonnosti [4, 5].

Playbook kybernetickej bezpečnosti obsahuje podrobny návod ako krok za krokom reagovať na špecifické typy incidentov [5, 6]. Poskytuje preddefinované postupy prípravy na špecifické typy incidentov, taktiež postupy reakcie, keď dojde k incidentu a zotavenia sa z nich. Tieto preddefinované postupy treba jasne dodržiavať.

1.2.1 Klúčové komponenty playbookov

- **Špecifické typy incidentov:** Každá príručka je vytvorená na mieru pre konkrétny scenár incidentu. Zameriava sa na konkrétny typ incidentov (napr. trójske kone, ransomware, vírusy či ukradnutie údajov),
- **Nástroje a techniky:** Špecifikuje nástroje a techniky, ktoré sa majú použiť pre konkrétny typ incidentu,
- **Úlohy a zodpovednosti:** Členom tímu priraďuje špecifické úlohy relevantné pre daný typ incidentu,
- **Overenie a validácia:** Opatrenia, ktoré zabezpečia úplné vyriešenie incidentu. Môže obsahovať aj kontrolné zoznamy na potvrdenie odstránenia a obnovy.

Klúčové komponenty [6] pomáhajú zabezpečiť koordinovanú a rýchlu odozvu s cieľom minimalizovať škody, obnoviť normálnu prevádzku a predísť budúcim incidentom.

1.2.2 Význam playbookov

Playbooky sú nevyhnutné pre zabezpečenie konzistentného a koordinovaného prístupu k riešeniu incidentov [6]. Pomáhajú:

- **Minimalizovať dopad incidentov:** Rýchla a efektívna reakcia môže výrazne znížiť spôsobené škody,
- **Zlepšiť komunikáciu:** Playbooky zaručujú, že všetci členovia tímu vedia čo majú robiť, a tak to zlepšuje internú aj externú komunikáciu počas trvania incidentu,
- **Zvýšiť dôveru:** Mať playbooky pripravené a otestované zvyšuje dôveru tímov v ich schopnosti zvládnuť incidenty.

1.3 Manažment znalostí

Efektívny manažment znalostí pomáha organizáciám rýchlo reagovať na zmeny na trhu, zlepšovať výkonnosť a inovácie, a udržiavať konkurenčnú výhodu [7].

Manažment znalostí (KM) je multidisciplinárny prístup na identifikáciu, získavanie, organizovanie, ukladanie, zdieľanie a využívanie znalostí a informácií na zlepšenie výkonnosti organizácie [8]. Zahŕňa vytváranie prostredia, ktoré povzbudzuje a podporuje vytváranie, zdieľanie a aplikáciu vedomostí na dosiahnutie cieľov organizácie.

Znalosti sú nevyhnutným zdrojom organizácie a môžeme povedať, že úspech firmy od nich závisí [9]. Každá organizácia by mala vedieť, aké znalosti má, aké potrebuje, ako sú tieto znalosti uložené a ako sa zdieľajú medzi zamestnancami. Odpovede na tieto otázky sú klúčové pre organizačný tok práce a sú klúčom k dosiahnutiu cieľov a stratégií organizácie.

Existuje viacero definícií manažmentu znalostí, no pre našu prácu si ju zadefinujeme ako získavanie správnych znalostí dostupných správnym ľuďom v správnom čase. Inými slovami, účinný manažment znalostí zabezpečuje, že potrebné znalosti sú ľahko dostupné na použitie, keď sú potrebné.

1.3.1 Znalosti pre bezpečnostné incidenty

Znalostami v kontexte kybernetickej bezpečnosti môžeme považovať informácie, zručnosti a odbornosti [10] potrebnej na identifikáciu, analýzu a aj reakciu na bezpečnostné incidenty. Znalosti sú kritickou súčasťou efektívnej reakcie na incidenty, pretože organizáciám umožňujú včasne a efektívne odhaliť hrozby a reagovať na ne.

2 Dostupné zdroje znalostí a incidentov

2.1 Databázy

Databázy slúžia na systematické zhromažďovanie, uchovávanie a zdieľanie informácií o bezpečnostných hrozbách, zraniteľnostiach a incidentoch. Medzi najdôležitejšie databázy patrí:

- **MITRE ATT&CK** - dokumentuje taktiky, techniky a postupy útočníkov. Pomáha porozumieť hrozbám a vytvárať obranné stratégie tým, že poskytuje prehľad o fázach útokov a umožňuje mapovanie útokov a identifikáciu zraniteľných miest,
- **Common Vulnerabilities and Exposures (CVE)** - zaznamenávanie známych zraniteľností v softvéri. Každá zraniteľnosť má jedinečný CVE identifikátor a obsahuje podrobne informácie o chybe,
- **NIST NVD** - spravované organizáciou NIST. Poskytuje podrobne informácie o zraniteľnostiach podľa ich závažnosti a typu. Ponúka analytické informácie a metriky rizika, ktoré pomáhajú pri hodnotení a riadení zraniteľností.

Tieto databázy ponúkajú komplexné a podrobne údaje o taktikách útočníkov, zraniteľnostiach a metrikách rizika.

2.2 Bezpečnostné komunity a fóra

Komunity a fóra poskytujú rýchly prístup k praktickým radám a skúsenostiam z prvej ruky, čo môže byť veľmi užitočné pri riešení konkrétnych problémov alebo hľadania najnovších trendov a techník v oblasti kybernetickej bezpečnosti. Medzi najvýznamnejšie dva patria:

- **FIRST (Forum of Incident Response and Security Teams)** - FIRST je globálna komunita, ktorá združuje tímy pre reakciu na bezpečnostné incidenty (CSIRT). Členstvo v FIRST umožňuje prístup k rôznym zdrojom, ako sú správy o hrozbách, technické analýzy a kontakty na iné CSIRT tímy,
- **SANS Internet Storm Center (ISC)** - Centrum poskytuje denné správy, analýzy útokov a praktické rady na zvýšenie bezpečnosti. SANS ISC je cenným zdrojom aktuálnych informácií o kybernetických hrozbách.

3 Existujúce riešenia pre manažment znalostí

3.1 SASP

Jedným z kľúčových výskumov v tejto oblasti je výskumná práca "SASP: a Semantic web-based Approach for management of Sharable cybersecurity Playbooks" [11]. SASP predstavuje návrh založený na sémantickom webe, ktorý umožňuje efektívne zdielanie a správu playbookov pre kybernetickú bezpečnosť. Tento systém využíva ontológie na reprezentáciu znalostí a umožňuje ich automatické spracovanie a vyhľadávanie. Významnou výhodou SASP je jeho schopnosť zlepšiť interoperabilitu medzi rôznymi systémami a nástrojmi tým, že poskytuje štandardizované a sémanticky obohatené údaje.

3.1.1 Výhody

- schopnosť zlepšiť interoperabilitu vdaka štandardizovaným a sémanticky obohateným údajom, čo umožňuje efektívne zdielanie a využívanie znalostí medzi rôznymi systémami,
- automatizované spracovanie, umožnené ontológiami a CACAO štandardom, zvyšuje efektivitu reakcie na incidenty,
- štandardizácia playbookov poskytuje jednotné postupy a scenáre, čo zjednodušuje riešenie incidentov.

3.1.2 Nevýhody

- náročnosť implementácie, ktorá vyžaduje pokročilé znalosti o semantickom webe, ontológiách a CACAO štardarde, čo môže byť pre niektoré organizácie náročné,
- potreba pravidelnej údržby a aktualizácie ontológií a playbookov, aby boli relevantné a aktuálne,
- SASP nie je aktuálne dostupný a je stále vo fáze vývoja.

3.2 MISP

Malware Information Sharing Platform (MISP) [12] je ďalším významným riešením pre manažment znalostí v oblasti kybernetickej bezpečnosti. Táto platforma je navrhnutá na zdielanie informácií o malvéroch, indikátoroch kompromitácie (IOC) a ďalších relevantných

bezpečnostných informáciách medzi rôznymi organizáciami.

MISP sa skladá z nasledujúcich hlavných komponentov: databáza IOC, zdielateľné rozhranie a analytické nástroje. Komponent databázy IOC slúži ako centralizované úložisko pre indikátory kompromitácie a ďalšie bezpečnostné údaje. Zdielateľné rozhranie poskytuje nástroje a API na bezpečné zdieľanie informácií medzi organizáciami a posledný komponent analytických nástrojov umožňuje analýzu a vzťahy medzi údajmi, čím pomáhajú identifikovať vzorce a súvislosti medzi incidentmi [12].

3.2.1 Výhody

- schopnosť umožniť rýchle zdieľanie a prijímanie informácií o hrozbách, čo zvyšuje schopnosť reagovať na nové kybernetické útoky,
- relatívne jednoduchá implementácia a podpora širokej škály formátov dát ulahčuje jeho nasadenie a integráciu s existujúcimi bezpečnostnými systémami.

3.2.2 Nevýhody

- bezpečnostné obavy spojené so zdieľaním citlivých informácií, ktoré môžu byť rizikové, ak nie sú dodržiavané správne bezpečnostné opatrenia.

3.3 Ad2Play

Medzi príbuzné aplikácie patrí prototyp Ad2Play [13], ktorý poskytuje riešenie pre efektívnejšiu reakciu na incidenty, ako aj ponúka používateľsky priateľské rozhranie na správu playbookov a bezpečnostných incidentov. Prototyp je SOAR riešenie navrhnuté na automatizáciu reakcie na incidenty pre priemyselné IoT zariadenia. Skladá sa z frontendovej časti vyvinutej pomocou Vue.js a backendovej časti postavenej na Node.js, tvoriacich centrálnu SOAR-Platformu. Táto platforma interahuje s databázou MongoDB.

Hoci Ad2Play poskytuje robustné riešenie pre správu playbookov, má svoje nedostatky. Jedným z hlavných obmedzení je absencia sémantického vyhľadávania, čo znamená, že používateľom môže chýbať možnosť efektívneho a presného vyhľadávania informácií. Okrem toho, Ad2Play neponúka vizualizáciu playbookov pomocou diagramov, čo môže stažiť pochopenie a úpravu komplexných playbookov pre menej skúsených používateľov.

3.4 Nevýhody existujúcich riešení

Jedným z hlavných problémov je nedostatok integrácie medzi rôznymi nástrojmi a systémami. Mnohé frameworky pre manažment znalostí a nástroje pre reakcie na incidenty fungujú izolované [10], čo môže viesť k problémom so zdieľaním informácií a koordináciou reakcií na incidenty. Táto fragmentácia spôsobuje, že informácie sú často dostupné len v obmedzenom rozsahu a neumožňujú komplexný pohľad na bezpečnostné incidenty, čo môže spomaliť a skomplikovať reakcie na tieto incidenty.

Ďalším problémom je nedostatok robustných open-source riešení pre manažment znalostí špecifický pre bezpečnostné incidenty [14]. Väčšina dostupných systémov a nástrojov je komerčná, čo môže byť pre menšie organizácie finančne náročné. Open-source riešenia by mohli poskytnúť flexibilitu a prístupnosť, ktoré by umožnili širšiu adopciu manažmentu znalostí v rôznych typoch organizácií.

Následne za slabú stránku považujeme nedostatok playbookov pre reakciu na incidenty [15]. Táto situácia je spôsobená hlavne tým, že väčšina existujúcich playbookov je interná a šitá na mieru konkrétnym potrebám organizácií. Mnohé organizácie vytvárajú svoje vlastné playbooky na základe unikátnych IT infraštruktúr, bezpečnostných politík a špecifických rizík, ktorým čelia. Tieto playbooky sú často výsledkom dlhodobých skúseností a prispôsobení, ktoré zohladňujú interné procesy a štruktúry. V dôsledku toho nie sú verejne dostupné alebo ľahko prenositeľné medzi rôznymi organizáciami.

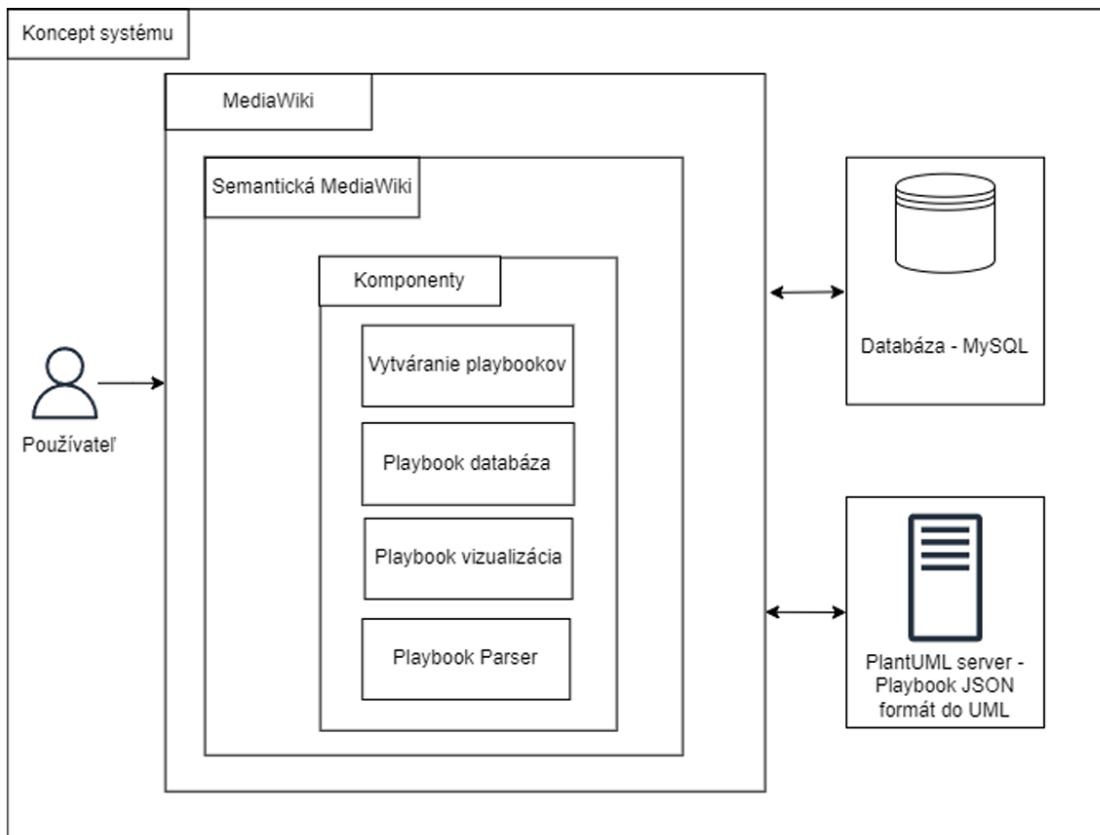
Navýše, vytvorenie efektívnych a univerzálnych playbookov vyžaduje značné zdroje, vrátane odborných znalostí a času [6]. Každá organizácia má svoje vlastné špecifiká, ktoré robia univerzálne riešenia menej efektívnymi. Z tohto dôvodu sú k dispozícii len obmedzené generické playbooky, ktoré často neposkytujú dostatočnú úroveň detailov a prispôsobenia na konkrétné scenáre.

4 Použité riešenie

V rámci tohto tímového projektu budeme používať riešenie, ktoré navrhol Adam Budziňák vo svojej bakalárskej práci, ktorá mala názov: Manažment znalostí pre bezpečnostné incidenty. V tejto práci bol vytvorený framework pre manažment incidentov, ktorý sme použili ako základ pre našu prácu. Toto riešenie budeme postupne vylepšovať a pridávať novú funkcia.

4.1 Popis použitého riešenia

Diagram použitého riešenia je zobrazený na obrázku č. 1. Architektúra riešenia je postavená



Obr. 1: Diagram použitého riešenia.

na sémantickej MediaWiki [16]. Sémantická MediaWiki je rozšírenie pre MediaWiki, ktoré pridáva možnosť ukladať a dotazovať sa na štruktúrované dátá. Sémantická MediaWiki využíva RDF (framework popisu zdrojov) a SPARQL (dotazovací jazyk) na manipuláciu a dopytovanie dát. MediaWiki je open-source softvérový nástroj [17] na správu obsahu, ktorý vyvinula Wikipedia. Umožňuje používateľom vytvárať, upravovať a spravovať webové

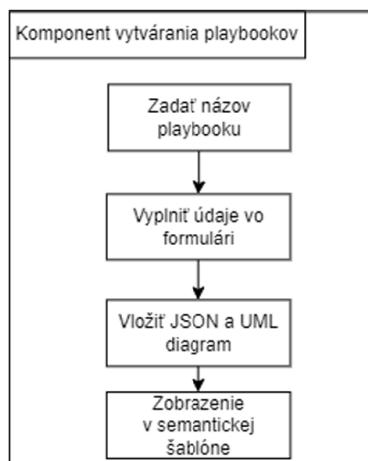
stránky vo formáte wiki.

Backend systému MediaWiki je napísaný v programovacom jazyku PHP a všetok textový obsah ukladá do databázy. Frontend je postavený na HTML, CSS a JavaScripte, čo umožňuje vytvoriť interaktívne a používateľsky prívetivé rozhranie.

Databáza použitá v tomto riešení je MySQL kvôli jej spoľahlivosti, výkonu a širokej podpore pre MediaWiki. Databáza je vytvorená automaticky pomocou pripojenia softvérového nástroja MediaWiki, čo umožňuje štruktúrované ukladanie informácií a ich jednoduché vyhľadávanie. Semantická MediaWiki využíva túto existujúcu databázu a pridáva možnosť používať sémantické dotazy, čím rozširuje schopnosti MediaWiki o pokročilé vyhľadávanie a správu štruktúrovaných dát.

4.1.1 Komponent vytváranie playbookov

Diagram komponentu vytvárania playbookov je zobrazený na obrázku č. 2. Vytváranie



Obr. 2: Diagram vytvárania playbookov.

playbookov je realizované pomocou Page Forms od sémantickej MediaWiki. Tento komponent využíva formuláre a vlastnosti na vytváranie a úpravu playbookov. Používatelia môžu prostredníctvom jednoduchého a intuitívneho formulára zadávať potrebné údaje a priložiť prílohy ako je JSON súbor alebo UML diagram. Každý playbook, ktorý sa vytvorí pomocou tohto formulára obsahuje v tomto riešení nasledujúce údaje:

- Id: jedinečný identifikátor, playbooku,
- Tags: umožňuje pridať viaceré tagy oddelené čiarkou, používajú sa na priradovanie viacerých hodnotových dát k playbooku, čo umožňuje lepšiu kategorizáciu a

vyhľadávanie,

- Description: obsahuje popis playbooku,
- Use: informácie o tom, ako sa playbook používa,
- JSON: odkaz na playbook v súbore JSON, ak je k dispozícii, inak sa zobrazuje text No JSON file.
- Image: UML diagram priradený k playbooku, ak je k dispozícii, inak sa zobrazuje text No Image.

4.1.2 Komponent vizualizácie playbookov

Na zlepšenie prehľadnosti a použiteľnosti je do riešenia integrovaný PlantUML server. PlantUML je nástroj na generovanie rôznych typov UML diagramov ako sú diagramy tried, sekvenčné diagramy, stavové diagramy a ďalsie, jednoduchým a intuitívny spôsobom.

Tento komponent umožňuje používateľom jednoduchšie pochopiť a upravovať playbooky prostredníctvom vizuálnych reprezentácií UML. Diagramy generované pomocou PlantUML servera zobrazujú jednotlivé kroky a procesy v playbookoch, čo uľahčuje ich pochopenie a implementáciu.

4.1.3 Komponent playbook parser

Tento komponent je klúčovým prvkom celého riešenia. Je implementovaný pomocou PHP a JavaScriptu, aby zabezpečil efektívnu a presnú analýzu a spracovanie playbookov pre bezpečnostné incidenty. Komponent slúži na spracovanie JSON vstupu a jeho konverziu do MediaWiki textového formátu. Používateľ zadá JSON do formulára, následne je tento JSON spracovaný a prevedený do MediaWiki textu, ktorý je zobrazený na stránke. Zároveň má používateľ možnosť stiahnuť tento prevedený text ako súbor.

4.2 Ukážka použitého riešenia

KNOWLEDGE MANAGEMENT

Search Knowledge Management Search

Admin ▾

Manážment znalostí pre bezpečnostné incidenty

[Page](#) [Discussion](#) [☆](#)

(Redirected from Main Page)

Playbook [edit](#) [edit source](#)

Playbook sa skladá z niekoľkých stavebních blokov, ktorí spoločne vytvárajú akčný plán, ktorý sa má použiť pred kybernetickým útokom, počas neho a po ňom. Zahŕňa klúčové a spoločné kroky na prípravu, hodnotenie a rešenie incidentov, ako aj osvedčené postupy na zvládanie podobných incidentov a bezpečnostných hrozieb.

Pozrite si našu databázu tu -> Playbook database

Pozrite si playbooky pre špecifické typy incidentov [edit](#) [edit source](#)

Malware

Ransomware

Phishing

Data Loss

Account Compromised

Phishing

Data Loss

Account Compromised

(Každý typ obsahuje zoznam aktuálnych playboookov v textovom formáte alebo JSON formáte)

Page tools

- [Delete](#)
- [Move](#)
- [Protect](#)

More

- [What links here](#)
- [Related changes](#)
- [Printable version](#)
- [Permanent link](#)
- [Page information](#)
- [Page logs](#)

Obr. 3: Hlavná stránka.

KNOWLEDGE MANAGEMENT

Search Knowledge Management Search

Admin ▾

Playbook database

[Page](#) [Discussion](#) [☆](#)

Incident Response Playbooks

Playbook Name	ID	Description	Tag
Malware Workflow Playbook - Preparation	1	Establish incident response plan, tools, and preventive measures	Preparation
Malware Workflow Playbook - Detect	2	Identify and collect data on potential malware threats and indicators	Detect
Malware Workflow Playbook - Analyze	3	Verify, identify, and analyze malware indicators and scope of incident	Analyze
Malware Workflow Playbook - Contain / Eradicate	4	Isolate, contain, and eradicate malware from affected hosts and systems	Contain/Eradicate
Malware Workflow Playbook - Recover	5	Rebuild, patch, and restore affected systems	Recover
Malware Workflow Playbook - Post Incident	6	Review, update, and improve incident response processes and defenses	Post Incident
Ransomware Workflow Playbook - Preparation	7	Establish incident response plan, tools, and preventive measures in place	Preparation
Ransomware Workflow Playbook - Detect	8	Identify and collect data on potential ransomware threats and indicators	Detect
Ransomware Workflow Playbook - Analyze	9	Respond to ransomware attack, contain and eradicate threat	Analyze
Ransomware Workflow Playbook - Contain / Eradicate	10	Isolate affected systems, block malware spread, and eradicate threats	Contain/Eradicate
Ransomware Workflow Playbook - Recover	11	Recover from ransomware attack, restore systems and data	Recover
Ransomware Workflow Playbook - Post Incident	12	Review, update, and improve defenses after ransomware incident	Post Incident
Phishing Workflow Playbook - Preparation	13	Prepare Against Phishing Attacks with Prevention and Response Plans	Preparation
Phishing Workflow Playbook - Detect	14	Identify threats, risks, categorize, and triage incidents for swift response	Detect
Phishing Workflow Playbook - Analyze	15	Thoroughly examine, validate, and update for effective incident resolution	Analyze
Phishing Workflow Playbook - Contain / Eradicate	16	Thorough validation and preparation for effective incident response.	Contain/Eradicate
Phishing Workflow Playbook - Recover	17	Validate defenses and endpoint recovery status.	Recover
Phishing Workflow Playbook - Post Incident	18	Review, update, and refine security measures to prevent future incidents	Post Incident
Data Loss Workflow Playbook - Preparation	19	Proactively prepare for data loss prevention and response measures	Preparation
Data Loss Workflow Playbook - Detect	20	Identify and assess data loss incident indicators quickly	Detect
Data Loss Workflow Playbook - Analyze	21	Analyze and validate data loss incident details thoroughly	Analyze

Page tools

- [Delete](#)
- [Move](#)
- [Protect](#)

More

- [What links here](#)
- [Related changes](#)
- [Printable version](#)
- [Permanent link](#)
- [Page information](#)
- [Page logs](#)

Obr. 4: Databáza playbookov.

The screenshot shows a 'Malware Infection Response' playbook entry in a knowledge management system. The 'Page' tab is selected. Key details include:

- ID:** 100
- Tags:** Analyze, Contain/Eradicate, Recover, Post Incident, Detect
- Description:** Steps to respond to a malware infection
- Parsed Playbook:** Malware Infection Response
- Use:** Steps:
 - Isolate the infected system from the network
 - Identify the type and source of the malware
 - Quarantine affected files and systems
 - Remove the malware using antivirus or anti-malware tools
 - Conduct a thorough system scan to ensure complete removal
- Contact:** Incident Manager (incident.manager@example.com)
- JSON file:** A diagram showing the structure of the playbook. It includes a main object 'incident' with properties: id (IR-001), title (Malware Infection Response), description (Steps to respond to a malware infection), steps (a list of 5 steps), and contact (Incident Manager). Each step has a 'step_number' and a 'description'.

Obr. 5: Ukážka vzhľadu playbooku.

5 Zimný semester - vylepšenia

V tejto časti sú popísané vylepšenia, ktoré sme vykonali na zlepšenie pôvodného riešenia počas zimného semestra.

5.1 Implementácia štandardu CACAO 2.0

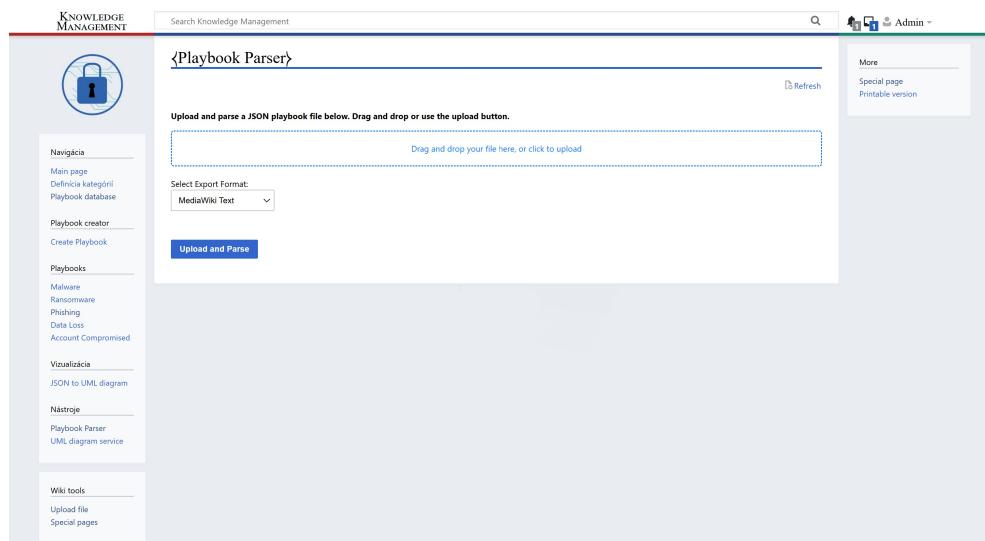
Pôvodné riešenie obsahuje len obmedzený jednoduchý štandard pre vytváranie playbookov. My sme implementovali štandard CACAO 2.0 do tohto riešenia. CACAO (Collaborative Automated Course of Action Operations) [18] je štandard vyvinutý organizáciou OASIS (Organization for the Advancement of Structured Information Standards), ktorý slúži na automatizáciu reakcií na kybernetické hrozby. Je navrhnutý tak, aby umožnil organizáciám zdieľať, koordinovať a implementovať bezpečnostné opatrenia efektívnejsie a automatizované.

Vytvorili sme preklady do CACAO štandardu pre playbooky nasledovných spoločností a formáty:

- Fortinet FortiSOAR,
- LogicHub SOAR,

- Chronicle Security,
- Microsoft Sentinel.

Databáza playbookov, ktorá poskytuje playbooky, ktoré využívajú rôzne spoločnosti je dostupná na GitHube [19]. Spoločnosti, pre ktoré boli vytvorené preklady sme vybrali na základe vysokého počtu dát v databáze a takisto preto, lebo majú vhodný formát na ďalšie spracovanie a dajú sa aj vizuálne čítať. Tieto playbooky neobsahujú CACAO štandard, ale sú napísané pre konkrétnu spoločnosť, ktorá ich používa. Po nahratí playbooku na stránke, je možné zvoliť, ktorý typ playbooku sa má preložiť do CACAO štandardu. Následne je možné preložený playbook exportovať do textového súboru, zobraziť ho ako mediaWiki text na stránke alebo je možné exportovať iba príkazy do textového súboru.



Obr. 6: Nahrávanie playbooku na stránke.

Playbook v CACAO štandarde po preklade obsahuje nasledujúce údaje:

- type: typ playbooku,
- spec_version: verzia playbooku,
- id: id playbooku,
- name: názov playbooku,
- created_by: autor playbooku,
- created: čas vytvorenia playbooku,

The screenshot shows a web interface for managing knowledge. On the left, there's a sidebar with various navigation links such as 'Main page', 'Definícia kategórií', 'Playbook database', 'Create Playbook', 'Malware', 'Ransomware', 'Phishing', 'Data Loss', 'Account Compromised', 'Vizualizácia', 'JSON to UML diagram', 'Nástroje', 'Playbook Parser', 'UML diagram service', and 'Wiki tools'. The main content area has a title '{Playbook Parser}' and a section 'Playbook: OOB Content - Hash Lookup'. It contains a JSON configuration block with several sections: 'Workflow', 'Commands', and 'Actions'. The 'Workflow' section includes 'start' and 'action' types. The 'Commands' section contains multiple command definitions, each with a 'description' and 'action' type. The 'Actions' section lists actions like 'Drop columns', 'Add one or more fields', 'Convert LQL table to HTML table', and 'Analyze suspicious files and URLs'. A 'Description' field at the top states 'No description available.'

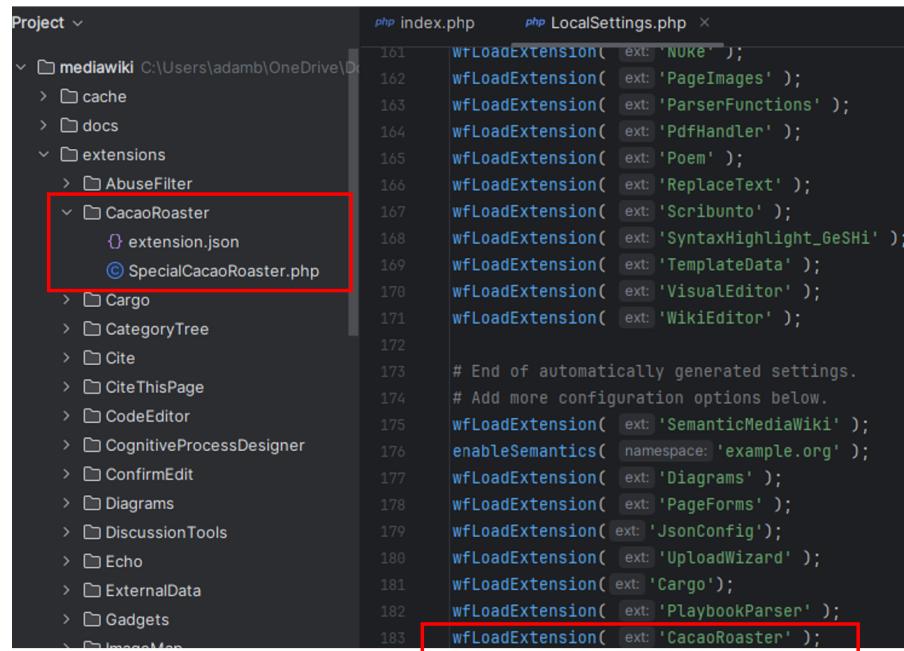
Obr. 7: Playbook zobrazený ako MediaWiki text.

- modified: čas modifikácie playbooku,
- workflow_start: prvý krok, ktorý sa má začať vykonávať,
- workflow: kroky, ktoré sa majú vykonávať, každý krok obsahuje ešte ďalšie údaje, ako je type, name, on_completion alebo commands.

Tieto polia sa musia nachádzať v CACAO 2.0 štandarde. Okrem týchto polí sa v playbooku v CACAO štandarde môžu nachádzať aj iné polia. Ak sa v pôvodnom playbooku nenachádzali povinné polia pre CACAO štandard, hľadali sme aliasy, ktorými by sa mohli nahradiť jednotlivé polia. Ak sme alias nenašli vygenerovali sme timestamp (pre údaje o čase vytvorenia alebo čase modifikácie) alebo náhodný reťazec pre údaj o identifikátore).

5.2 Implementácia CACAO roaster

Bola pridaná funkcia CACAO Roaster [20], ktorá slúži pre vytváranie, úpravu a vizualizáciu playbookov, ktoré sú už v CACAO štandarde. Bola vytvorená extension v Mediawiki a následne načítaná v LocalSettings.php pre spustenie.

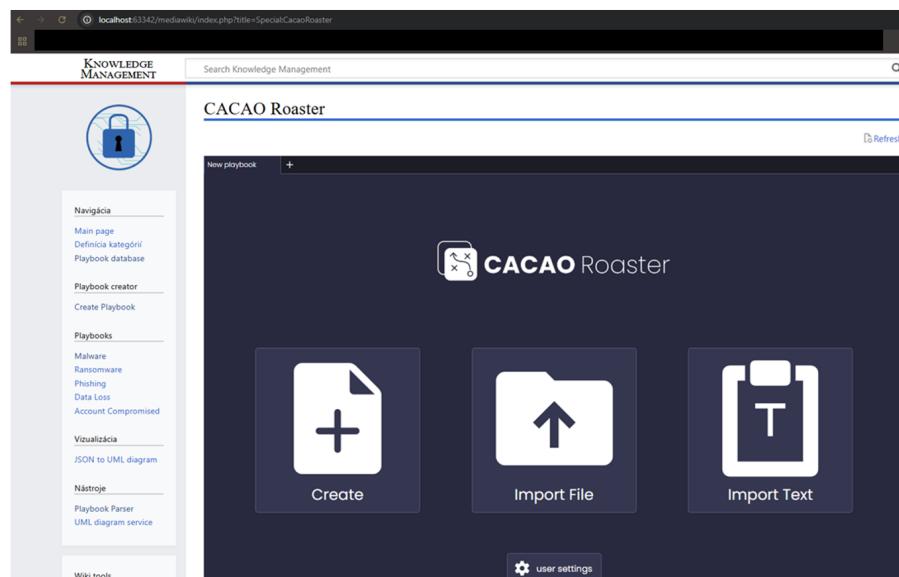


The screenshot shows a code editor with two tabs: index.php and LocalSettings.php. The LocalSettings.php tab is active, displaying PHP code. A red box highlights the line 'wfLoadExtension(ext: 'CacaoRoaster');' at the bottom of the file. On the left, a file tree shows the Mediawiki project structure, with a red box highlighting the 'CacaoRoaster' folder under the 'extensions' directory.

```
Project ▾
  mediawiki C:\Users\adamb\OneDrive\Documents\mediawiki>
    > cache
    > docs
    > extensions
      > AbuseFilter
        > CacaoRoaster
          > extension.json
          < SpecialCacaoRoaster.php
      > Cargo
      > CategoryTree
      > Cite
      > CiteThisPage
      > CodeEditor
      > CognitiveProcessDesigner
      > ConfirmEdit
      > Diagrams
      > DiscussionTools
      > Echo
      > ExternalData
      > Gadgets
      > ImageMagick
```

```
php index.php      php LocalSettings.php ×
161 wfLoadExtension( ext: 'NUKE' );
162 wfLoadExtension( ext: 'PageImages' );
163 wfLoadExtension( ext: 'ParserFunctions' );
164 wfLoadExtension( ext: 'PdfHandler' );
165 wfLoadExtension( ext: 'Poem' );
166 wfLoadExtension( ext: 'ReplaceText' );
167 wfLoadExtension( ext: 'Scribunto' );
168 wfLoadExtension( ext: 'SyntaxHighlight_GeSHi' );
169 wfLoadExtension( ext: 'TemplateData' );
170 wfLoadExtension( ext: 'VisualEditor' );
171 wfLoadExtension( ext: 'WikiEditor' );
172
173 # End of automatically generated settings.
174 # Add more configuration options below.
175 wfLoadExtension( ext: 'SemanticMediaWiki' );
176 enableSemantics( namespace: 'example.org' );
177 wfLoadExtension( ext: 'Diagrams' );
178 wfLoadExtension( ext: 'PageForms' );
179 wfLoadExtension( ext: 'JsonConfig' );
180 wfLoadExtension( ext: 'UploadWizard' );
181 wfLoadExtension( ext: 'Cargo' );
182 wfLoadExtension( ext: 'PlaybookParser' );
183 wfLoadExtension( ext: 'CacaoRoaster' );
```

Obr. 8: Pridanie extension do MediaWiki.



Obr. 9: Vzhľad CACAO roaster na stránke.

5.3 Handling nahrávania playbookov

Táto funkcia zahŕňa nahratie pôvodného playbooku, konverzia playbooku do CACAO štandardu a náslené nahratie playbooku do databázy v našom riešení. Táto funkcia bolo dokončená až počas letného semestra a je podrobne popísaná v podkapitole Automatické nahrávanie playbookov.

5.4 YAML formát

Pridali sme rozšírenie, ktoré nám umožňuje pracovať aj s YAML (Yet Another Markup Language) formátom playbooku. Doteraz sme vedeli spracovávať iba JSON (JavaScript Object Notation) formát playbookov. V tomto rozšírení sme využili komponent Symfony YAML [21], ktorý umožňuje jednoduché čítanie, zapisovanie a manipuláciu s YAML súbormi v PHP. Symfony YAML poskytuje API na parsovanie YAML súborov do PHP štruktúr (polia, objekty) a naopak.

Po pridaní tejto funkcionality je možné nahrať YAML formát playbooku na stránke a následne sa tento playbook preloží do CACAO štandardu. Z preloženého playbooku je možné potom exportovať príkazy do textového súboru.

6 Letný semester - vylepšenia

V tejto časti je popísaná naša práca počas letného semestra, kde sme sa snažili vylepšiť nás systém pre manažment incidentov. Pridali sme funkcionality a tiež vylepšili už existujúce. V podkapitolách nižšie sú podrobne rozpisane tieto vylepšenia.

6.1 Výber playbookov

Počas zimného semestra sme vytvorili preklady do CACAO štandardu pre spoločnosti FortiNet, LogicHub, Chronicle, Microsoft Sentinel a XSOAR (YAML formát). Pre tieto spoločnosti sa v databáze nachádzalo veľké množstvo playbookov, niektoré z nich ale neboli veľmi vhodné pre fakultný CSIRT, preto bolo potrebné vybrať najvhodnejšie playbooky, ktoré sú použiteľné pre univerzitný CSIRT. Z každej spoločnosti sme vybrali nižšie uvedený počet playbookov:

- **Fortinet FortiSOAR** - 54,
- **LogicHub SOAR** - 20,
- **Chronicle Security** - 1,
- **Microsoft Sentinel** - 22 ,
- **XSOAR (YAML)** - 47.

To znamená, že dokopy sme vybrali okolo 140 playbookov, ktoré sú vhodné pre fakultný CSIRT. Vyberali sme podľa typu týchto playbookov (či sú to playbooky pre Malware, Phishing, ...), vybrali sme také typy, aké by mohli byť vhodné pre CSIRT.

6.2 Dodefinovanie playbookov

Po vybraní vhodných playbookov sme tieto playbooky potrebovali dodefinovať. Po preklade playbookov do CACAO štandardu sme si však všimli, že by bolo vhodné doplniť niektoré parametre pre úplné porozumenie jednotlivých krokov. Na doplnenie týchto chýbajúcich parametrov sme využili umelú inteligenciu, ktorej sme poskytli daný playbook a prompt aby doplnila časti playbooku aby bol tento playbook pochopiteľný L1 SOC analytikom. Nižšie sú uvedené parametre, ktoré bolo potrebné doplniť alebo upraviť.

agent_definitions - kto vykonáva určitú akciu v určitom kroku, definuje aktérov (ľudských alebo automatizovaných), ktorí vykonávajú akcie v jednotlivých krokoch playbooku. Každý agent má: id, name, description (čo robí) a agent_type (napr. človek alebo systém). Príklad, ako je tento parameter znázornený v playbooku je zobrazený na obrázku č. 10.

```
"agent_definitions": {  
    "agent--f3ed9f5b-1451-4c4b-b68e-beb2f71faef0": {  
        "type": "agent",  
        "id": "agent--f3ed9f5b-1451-4c4b-b68e-beb2f71faef0",  
        "name": "SOC Analyst",  
        "description": "Security Operations Center analyst responsible for monitoring and taking action ...  
        "agent_type": "human"  
    },  
},
```

Obr. 10: Vzhľad parametra agent_definitions v playbooku.

target_definitions - na čo sa určitá akcia aplikuje v jednotlivých krokoch. Definuje objekty alebo systémy, na ktoré sa akcie zameriavajú. Každý target obsahuje: id, name a target_type: (indikátor, systém, súbor, ...). Príklad, ako je tento parameter znázornený v playbooku je zobrazený na obrázku č. 11.

```
"target_definitions": {  
    "target--d3e8acba-9299-421b-a574-16f499a087e1": {  
        "type": "target",  
        "id": "target--d3e8acba-9299-421b-a574-16f499a087e1",  
        "name": "Email Address Indicator",  
        "description": "The email address indicator being investigated for blocking.",  
        "target_type": "indicator"  
    },  
    "target--dbac78f2-ea71-4374-b41a-c9f570ce0d26": {  
        "type": "target",  
        "id": "target--dbac78f2-ea71-4374-b41a-c9f570ce0d26",  
        "name": "Firewall System",  
        "description": "The firewall system used to block email address indicators.",  
        "target_type": "system"  
    },  
},
```

Obr. 11: Vzhľad parametra target_definitions v playbooku.

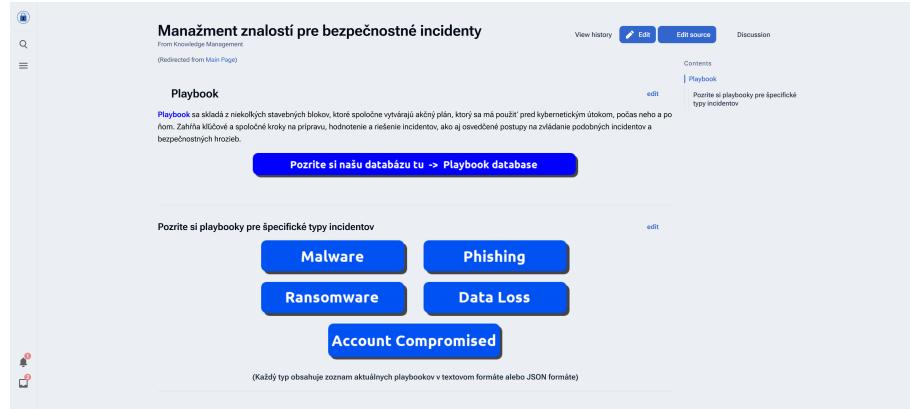
Agenti a ciele na ktoré sa určitá akcia zameriava sú potrebné v každom kroku, aby bolo jasné, kto má vykonávať daný krok a na aký objekt alebo systém je daný krok zameraný. Tieto definície v pôvodných playbookoch chýbali, preto sme ich doplnili.

Taktiež boli doplnené niektoré kroky a príkazy na lepšie pochopenie ako postupovať v každom kroku. Bolo potrebné doplniť aj priority, severity a impact playbooku aby sa

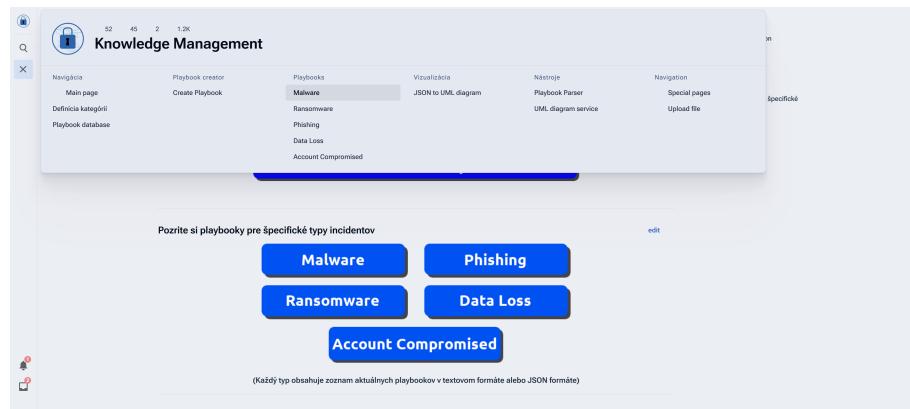
vedelo ako je daný playbook dôležitý alebo ako je problém, ktorý rieši daný playbook závažný. Tiež bol doplnený aj lepší popis, čo daný playbook robí a na čo slúži.

6.3 Vylepšenie GUI

Počas tohto semestra prebehlo aj grafické vylepšenie stránky. Na obrázkoch nižšie je možné vidieť zmenu oproti predchádzajúcej verzii.



Obr. 12: Hlavná stránka po vylepšení.



Obr. 13: Bočný panel po vylepšení.

6.4 Automatické nahrávanie playbookov

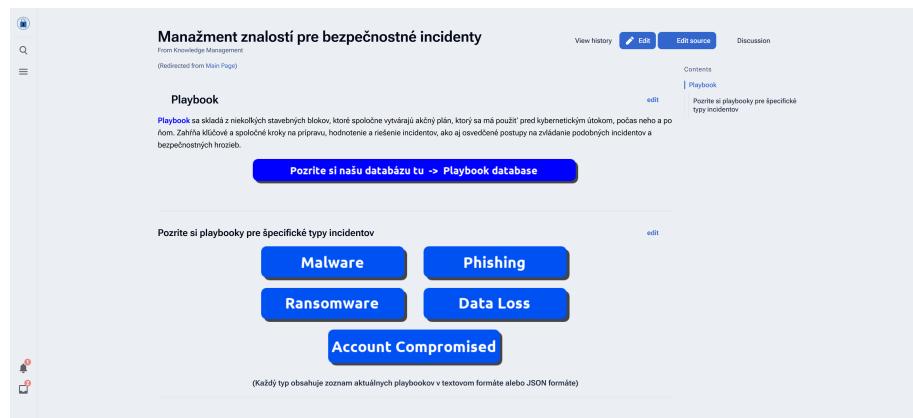
Už počas zimného semestra sme začali s implementáciou funkcie na automatické nahrávanie playbookov do databázy. Cieľom bolo aby sa vybraný playbook automaticky nahral do databázy po kliknutí na tlačidlo upload. Toto sa nám nepodarilo dokončiť počas zimného semestra ale až počas letného.

Teraz už tátó funkcia funguje tak ako má, po kliknutí na Playbook Parser sa dostaneme na stránku, kde je možné nahrať playbook. Je tam niekoľko možností ako je:

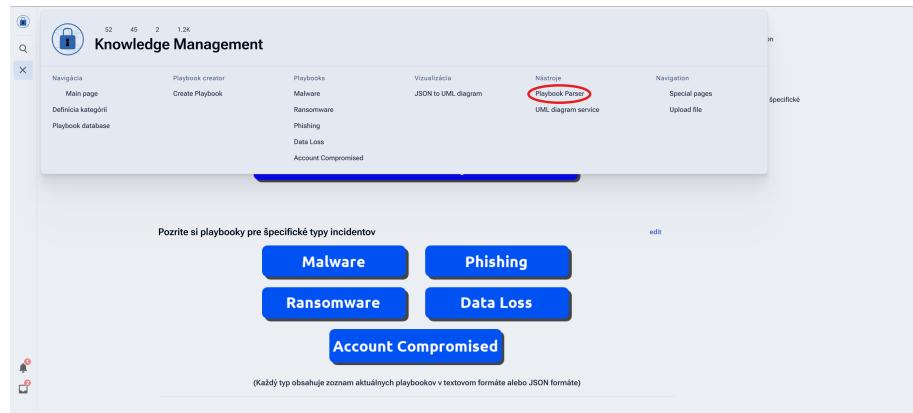
- nahratie playbooku už v CACAO štandarde,
- preklad LogicHub playbooku do CACAO štandardu,
- preklad FortiNet playbooku do CACAO štandardu,
- preklad Chronicle playbooku do CACAO štandardu,
- preklad Sentinel playbooku do CACAO štandardu,
- preklad YAML playbooku do CACAO štandardu,
- export príkazov do textového súboru,
- export celého playbooku do textového súboru,
- zobrazenie playbooku ako MediaWiki text.

Po zvolení prvých 6 možností sa zobrazí nové okno, kde je možné pred vložením do databázy ešte vybrať kategóriu playbooku (z niekoľkých možností) a pridať nieké tagy do playbooku. Tiež je možné upraviť popis alebo použitie playbooku, ale nie je to povinné pole. Ak nechceme nič meniť ani pridať, stačí kliknúť na Save page a playbook bude nahratý do databázy playbookov.

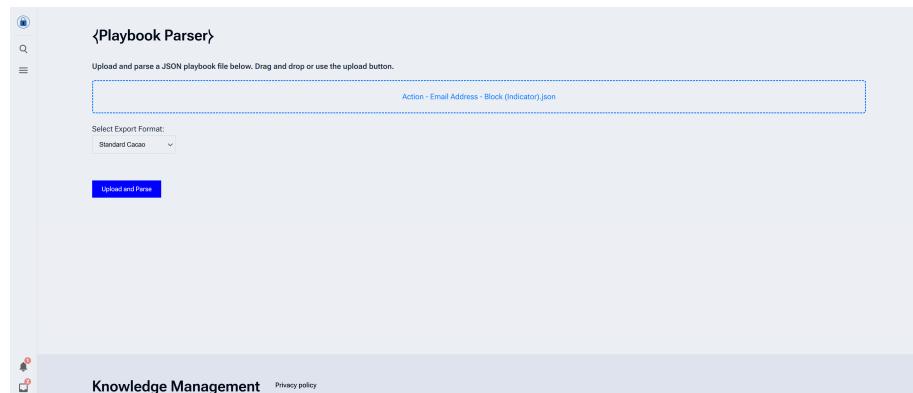
Ak klikneme na možnosť nahrať CACAO playbook, to znamená že playbook už je v CACAO štandarde a nie je potrebné ho prekladať. Ak klikneme na možnosti 2 - 6, tak sa playbook najprv preloží do CACAO štandardu a až potom sa nahrá do databázy. Ak kliknememe na možnosti exportu príkazov alebo exportu celého playbooku do textového súboru, tak je potrebné aby playbook už bol preložený do CACAO štandardu, inak táto možnosť nebude fungovať. Vizuálny popis ako postupovať pri nahrávaní playbooku do databázy je zobrazený na nižšie uvedených obrázkoch.



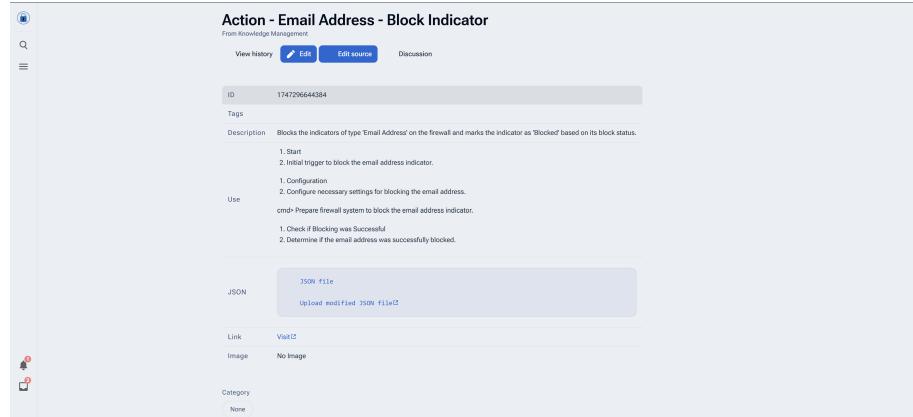
Obr. 14: Krok 1: Hlavná stránka.



Obr. 15: Krok 2: Bočný panel a výber Playbook Parser.



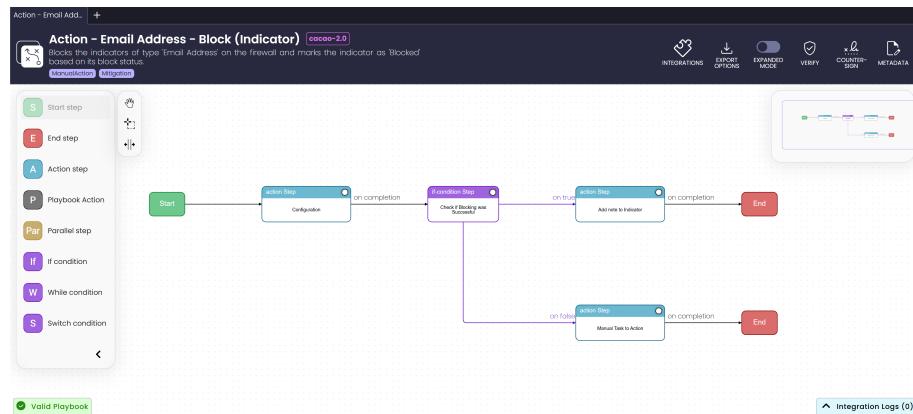
Obr. 16: Krok 3: Ak chceme nahrať playbook, ktorý už je v CACAO štandarde, tak nahráme playbook a klikneme na možnosť upload and parse, zobrazí sa nové okno, ak chceme niečo doplniť (tagy, kategóriu), môžme, potom klikneme na možnosť Save page.



Obr. 17: Krok 4: Playbook je nahraný v databáze na stránke a môžme ho používať.

6.5 Vizualizácia playbookov

Už počas zimného semestra bol pridaný extension CACAO Roaster [20], pomocou ktorého je možné vizualizovať playbooky, ktoré sú už v CACAO štandarde. Vizualizáciou playbooku môžeme lepšie pochopiť význam playbooku a na čo je určený daný playbook, pretože sú tam graficky zobrazené jednotlivé kroky vykonávania a postup pri riešení incidentov. Na obrázku č. 18 je zobrazený playbook, ktorý slúži na zablokovanie podozrivnej emailovej adresy, vizualizácia je cez tento CACAO Roaster.



Obr. 18: Vizualizácia playbooku pomocou CACAO Roaster.

7 Testovanie playbookov

V tejto časti sú znázornené rôzne scenáre, aký útok alebo situácia môže nastaviť a následne budeme testovať či sa podľa určeného playbooku dá daná situácia vyriešiť a playbook je užitočný alebo nie.

7.1 Scenár 1 - Otvorenie škodlivého súboru

Zamestnanec dostane e-mail, ktorý vyzerá ako faktúra od známeho dodávateľa. Otvorí priložený Excel súbor – ten však obsahuje škodlivý skript, ktorý sa spustí automaticky po otvorení súboru. Tento skript stiahne škodlivý program z internetu, ktorý sa snaží ukradnúť heslá a prístupové údaje. Zároveň sa tento škodlivý program šíri do ďalších počítačov v sieti. O pár minút neskôr si zamestnanec všimne, že sa jeho počítač spomaľuje a niektoré okná sa zasekávajú. EDR (Endpoint Detection and Response) systém (napr. CrowdStrike alebo SentinelOne) pošle alert do SIEMu (Security Information and Event Management) o podezrivej aktivite PowerShelli. SIEM je centrálny systém, ktorý zbiera logy a udalosti z rôznych zariadení (firewally, servery, EDR, sieťové zariadenia, cloud, ...), analyzuje ich v reálnom čase, detektuje incidenty, vzory správania alebo hrozby a upozorňuje bezpečnostný tím (SOC) na podezrivé aktivity. Následne SOC analytik dostane hlásenie a otvára tento incident a postupuje podľa playbooku, konkrétnie playbook Malware Incident response.

Playbook obsahuje nasledovné kroky:

- **Identifikácia** — zistuje sa, čo sa stalo. Analytik si pozrie alert, overí ho, následne porovná hash súboru na VirusTotal — nájde, že ide o známy malware. Potom tiež zistí, že rovnaký e-mail dostali ešte 3 ďalší kolegovia.
- **Analýza** — ako sa tento malware dostal do PC ? Analytik preverí e-mail — ukáže sa, že odosielateľ bol podvrhnutý (phishing), potom analytik skontroluje logy, zistí že Excel sa pokúsil pripojiť na neznámu IP a tiež že sa skript pokúsil vytvoriť naplánovanú úlohu (task).
- **Izolácia** - analytik použije EDR na vzdialené odpojenie infikovaných zariadení od siete. Ostatné podezrivé stroje sa tiež izolujú ako preventívne opatrenie.
- **Foreznná analýza** - získa sa pamäť RAM (memory dump), pomocou nástroja (napr. Volatility) sa pozrú bežiace procesy a potvrdí sa prítomnosť malvéru v pamäti aj jeho pokusy o pripojenie von.

- **Čistenie** - vymažú sa podozrivé súbory, zrušia plánované úlohy, odstránia sa registre. EDR aj AV kontrola potvrdia, že systémy sú čisté.
- **Obnova** - obnovia sa súbory zo záloh, pracovné stanice sa opravia alebo preinštalujú a overí sa, že systémy sú aktualizované.
- **Report** - vytvorí sa incident report, aktualizujú sa bezpečnostné postupy. Vedenie dostane správu o tomto incidente a naplánuje školenie pre zamestnancov (ako rozpoznať podvodné emaily).
- **Uzatvorenie incidentu** - po kontrole sa incident oficiálne uzatvára. Dôkazy sa archivujú, systém sa vráti do normálnej prevádzky.

V tomto scenári bolo ukázané, že SOC (Security Operations Center) analytik dokázal vyriešiť tento typ incidentu pomocou tohto playbooku. To znamená, že playbook je vhodný na používanie pri incidentoch typu Malware. V scenárii sú veľmi podrobne popísané jednotlivé kroky v playbooku. Keď chceme len export príkazov z tohto playbooku a stručný popis, stačí nahrať playbook na stránke Playbook Parser a zvoliť možnosť export All Comands, následne sa stiahne textový súbor s príkazmi, ktorý je možné vidieť na obrázku nižšie.

```

# Initial Detection
# Trigger malware response workflow

# Initial Triage
# Confirm malware presence and scope
cmd> 1. Review AV/EDR alerts
2. Check file hashes against VirusTotal
3. Identify initial IOC spread

# Delivery Vector Analysis
# Determine infection pathway
cmd> 1. Check email logs for phishing
2. Review web proxy entries
3. Analyze removable media access

# Containment Measures
# Isolate affected systems
cmd> Invoke-EDRIsolation -Hostname [target_host] -Reason &#039;Malware
containment&#039;

# Forensic Evidence Gathering
# Collect malware artifacts
bash> volatility -f [memory_dump] malprocsan

# Malware Eradication
# Remove malicious components
cmd> 1. Delete registry entries
2. Remove scheduled tasks
3. Clean file system artifacts

# System Restoration
# Return systems to operational state
cmd> 1. Restore from clean backups
2. Rebuild compromised systems
3. Verify patch levels

# Lessons Learned
# Document incident findings
cmd> 1. Create after-action report
2. Update runbooks
3. Schedule staff training

# Incident Closure
# Malware incident officially resolved

```

Obr. 19: Export príkazov z playbooku.

7.2 Scenár 2 - Podozrivé pripojenie na univerzitný systém

Univerzitný systém je nečakane kontaktovaný z externých IP adres, ktoré pochádzajú zo zahraničia. Tieto IP adresy sa objavujú v logoch firewallu a nepatria medzi známe alebo legítimne služby. Systém zistí tieto pripojenia v čase mimo prevádzky (napr. o 03:00 ráno). Na tento scenár bol použitý playbook Suspicious IP Analysis.

Playbook obsahuje nasledovné kroky:

- **Spustenie playbooku** — alert zo SIEM alebo IDS (Intrusion Detection System) spustí automatické kroky, ked firewall zaznamená externý prístup na citlivý systém. Následne playbook pokračuje do IP zberu.
- **Zber údajov** — analytik spustí skript, ktorý prehľadá logy firewallu, vyfiltruje záznamy s tagom EXTERNAL_ACCESS, extrahuje jedinečné IP adresy a výsledok uloží do súboru /tmp/suspicious_ips.txt.
- **Geolokácia a reputácia** - IP adresy sa jednotlivo posielajú do služby Abuse-IPDB (kontrola reputácie) a zistuje sa krajina pôvodu pomocou MaxMind GeoLite2 databázy. Tieto dátia sa uložia do /tmp/geo_results.txt.
- **Hodnotenie rizika** - automaticky sa hľadajú podozrivé krajinu, ak sa nájdu, odošle sa e-mail SOC tímu. SOC tím dostane správu s napríklad dvoma vysoko-rizikovými IP adresami.
- **Rozhodnutie o blokovanie** - rizikové IP adresy sa následne blokujú pomocou programu iptables. Potom rizikové IP adresy nemajú ďalej prístup do univerzitnej siete.
- **Dokumentácia** - do zdieľaného Google Sheet súboru s názvom „University IP Logs“ sa pridá: IP adresa, krajina, reputácia.
- **Ukončenie** - incident je zaznamenaný, podozrivé IP adresy sú blokované a SOC tím je informovaný. Prípad sa uzavrie.
- **Uzatvorenie incidentu** - po kontrole sa incident oficiálne uzatvára. Dôkazy sa archivujú, systém sa vráti do normálnej prevádzky.

V tomto scenári bolo ukázané, že SOC analytik (SOC tím) dokázal vyriešiť tento typ incidentu pomocou tohto playbooku. To znamená, že playbook je vhodný na používanie pri

incidentoch typu blokovanie podozrivých IP adries. V scenári sú veľmi podrobne popísané jednotlivé kroky v playbooku. Keď chceme len export príkazov z tohto playbooku a stručný popis, stačí nahrať playbook na stránke Playbook Parser a zvoliť možnosť export All Comands, následne sa stiahne textový súbor s príkazmi, ktorý je možné vidieť na obrázku nižšie.

```

# New External Connection
# Detection of external IP accessing sensitive systems

# Extract Connection Data
# Collect IP and session details from logs
bash> zgrep &#039;EXTERNAL_ACCESS&#039; /var/log/uni-firewall/*.log | awk
&#039;{print $5}&#039; | sort -u &gt; /tmp/suspicious_ips.txt

# Geolocation Analysis
# Identify country and risk level for IPs
bash> xargs -a /tmp/suspicious_ips.txt -I{} curl -ss
&#039;https://api.abuseipdb.com/api/v2/check?ipAddress={}&#039; -H &#039;Key:
$ABUSEIPDB_KEY&#039; | jq .data
bash> mmdblookup --file /usr/share/GeoIP/GeoLite2-Country.mmdb --ip {} country
names en

# Threat Evaluation
# Determine required response based on geolocation
bash> grep -E &#039;Russia|China|North Korea&#039; /tmp/geo_results.txt | mailx -s
&#039;High Risk IP Alert&#039; $SOC_EMAIL

# Blocking Decision
# Implement firewall blocks for confirmed threats
bash> xargs -a /tmp/highrisk_ips.txt -I{} sudo iptables -A INPUT -s {} -j DROP

# Update Records
# Log findings in university security spreadsheet
cmd> import gspread; gc = gspread.service_account(); sh = gc.open(&#039;University
IP Logs&#039;).sheet1; sh.append_row([ip, country, risk_score])

# Process Completed
# IP analysis workflow finished

```

Obr. 20: Export príkazov z playbooku.

7.3 Scenár 3 - Šírenie malvéru cez podvodnú doménu v e-mailoch

L1 SOC analytik dostáva alert zo SIEMu, že viacerým používateľom v rámci univerzity prišiel e-mail s prílohou a odkazom na určitú doménu. Doména je novo registrovaná, zneužíva názov univerzity a odkazuje na škodlivý ZIP archív s malvériom. Pre tento scenár bol využitý playbook s názvom: Block Domain.

Playbook obsahuje nasledovné kroky:

- **Overenie podozrivnej domény** — L1 SOC Analytik skontroluje doménu v Threat Intel systéme (VirusTotal, IBM X-Force, AbuseIPDB...), v SIEMe zistí, ktorí používatelia navštívili alebo klikli na doménu a vyhodnotí, či je hrozba skutočná (v tomto prípade áno). Nakoniec potvrdí doménu ako škodlivú.
- **Blokovanie domény na e-mailovej bráne** — analytik sa prihlási do Symantec Messaging Gateway (SMG), v sekcií Malware Policies - Block List pridá škodlivú doménu. E-maily z/do tejto domény budú zablokované.
- **Blokovanie domény cez iné nástroje** - analytik blokuje škodlivú doménu aj cez iné nástroje ako FireEye Email Security, Zscaler, Trend Micro Apex One, Proofpoint Threat Response.
- **Ukončenie incidentu** - doména bola označená ako škodlivá a bola zablokovaná naprieč všetkými hlavnými platformami.

V tomto scenári bolo ukázané, že SOC analytik dokázal vyriešiť tento typ incidentu pomocou tohto playbooku. To znamená, že playbook je vhodný na používanie pri incidentoch typu blokovanie podozrivých alebo škodlivých domén. V scenári sú veľmi podrobne popísané jednotlivé kroky v playbooku. Keď chceme len exportovať príkazov z tohto playbooku a stručný popis, stačí nahrať playbook na stránke Playbook Parser a zvoliť možnosť export All Commands, následne sa stiahne textový súbor s príkazmi, ktorý je možné vidieť na obrázku nižšie.

```

# Start - Validate Domain
# Initial step: confirm the domain is malicious before applying blocks.

# Validate Suspicious Domain
# L1 SOC Analyst enriches and confirms domain reputation.
cmd> 1. Check domain reputation in Threat Intel platform
2. Search SIEM for past connections to the domain
3. Confirm it isn't a false positive

# Block Domain - Symantec Messaging Gateway
# Prevent emails from or to the malicious domain at the gateway.
cmd> 1. Log into SMG Admin Console
2. Go to Policies &gt; Malware Policies
3. Add domain to Block List and save

# Block Domain - FireEye Email Security
# Add malicious domain to the blocklist in FireEye Email Security.
cmd> 1. Access FireEye Email Security Manager
2. Navigate to Policies &gt; Sender Domain Protection
3. Add domain to block list and deploy

# Block Domain - Zscaler
# Block web access to the domain via Zscaler.
cmd> 1. Log into Zscaler Admin Portal
2. Go to Policy &gt; URL & Cloud App Control
3. Create URL Filtering rule to block domain and save

# Block Domain - Trend Micro Apex One
# Enforce blocklist update in Apex One for the malicious domain.
cmd> 1. Open Apex One console
2. Go to Web Reputation &gt; Blocklisted Domains
3. Add domain and save policy

# Block Domain - Proofpoint Threat Response
# Use Proofpoint TR to enforce domain block across email and web protections.
cmd> 1. Log into Proofpoint Threat Response
2. Go to Domain Blocking &gt; Add Domain
3. Enter domain, choose &quot;Block&quot;, and confirm

# Done
# Confirmed malicious domain is blocked on all platforms.

```

Obr. 21: Export príkazov z playbooku.

8 Zápisnice

Zápisnica

Dátum konania: 8.10.2024

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Administrácia: Diskutovalo sa o administratívnych otázkach týkajúcich sa projektov a úloh.
- Web stránka: Bolo dohodnuté, že sa zriadi nová webová stránka na účely projektu, pričom bude nasadená na server poskytnutý vedúcim.
- Implementácia nových riešení: o Úlohou tímu bude pripraviť návrh skriptov a implementovať ich do systému.
 - Úlohou tímu bude pripraviť návrh skriptov a implementovať ich do systému.
- Discord + GIT: Diskusia o potrebe vytvorenia platformy na komunikáciu a správu zdrojových kódov. Dohodlo sa na použití Discorda pre komunikáciu a GITu pre správu kódu.

Úlohy do ďalšieho stretnutia:

- Dokončiť platformu Discord a GIT na lepšiu tímovú spoluprácu.
- Aktualizovať webovú stránku a nasadiť ju na server.

Termín ďalšieho stretnutia:

15.10.2024

Zápisnica

Dátum konania: 15.10.2024

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Dohodlo sa na nasledujúcim zadelení rolí:
 - Bc. Adam Budziňák – Šéf tímu
 - Bc. Daniel Ondrejka – Zapisovateľ
- Existujúce riešenia: Odporučilo sa prezrieť a analyzovať už existujúce riešenia na tému, v prácach alebo na internete
- Funkcionalita: Diskutovalo sa o možnej implementácii automatizácie playbookov
- Web stránka: Vedúcemu práce bola odprezentovaná tímová web stránka projektu
- Zadanie úloh na nasledujúce stretnutie

Úlohy do ďalšieho stretnutia:

- Pozrieť a naštudovať si už existujúce riešenia
- Pridať stručný text o čom je téma na tímovú web stránku projektu
- Šéf tímu si pripraviť prezentáciu o možnom riešení

Termín ďalšieho stretnutia:

22.10.2024

Zápisnica

Dátum konania: 22.10.2024

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Šéf tímu mal svoju prezentáciu k existujúcim riešeniam
- Existujúce riešenia: Preberala sa možná implementácia určitých funkcionálít z existujúcich riešení
- Štandard playbookov:
 - Prezerali sa rôzne štandardy pre tvorbu playbookov a diskutovalo sa o možnosti výberu štandardu CACAO 2.0
 - Diskutovalo sa aj o vytváraní aliasov respektíve mapovaní do našeho štandardu
- Automatizácia: Preberalo sa prípadné čítanie commandov z playbookov a vytváranie skriptov z nich
- Zadanie úloh na nasledujúce stretnutie

Úlohy do ďalšieho stretnutia:

- Prejsť CACAO 2.0 štandard pre playbooky
- Prejsť ostatné štandardy
- Pripraviť dokument s popisom ako sa ostatné štandardy mapujú na CACAO 2.0 štandard

Termín ďalšieho stretnutia:

5.11.2024

Zápisnica

Dátum konania: 5.11.2024

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Prezentovali sa mapovania na štandard CACAO 2.0
- Jednotlivé mapovania na následne porovnávali
- Konzultovali sme vytvorenie databázy z mapovaní, spôsob namapovania
- Blížšie sme sa pozerali na časti CACAO 2.0
- Povedali sme si ako by mohlo naše riešenie fungovať

Úlohy do ďalšieho stretnutia:

- Rozdeliť úlohy pre členov tímu šéfom tímu na začiatok práce na realizácii
- Práca na zadanej úlohe od šéfa tímu

Termín ďalšieho stretnutia:

19.11.2024

Zápisnica

Dátum konania: 19.11.2024

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Rozdelilo sa spracovanie štandardov na CACAO 2.0

Úlohy do ďalšieho stretnutia:

- Práca na spracovaní prideleného štandardu

Termín ďalšieho stretnutia:

26.11.2024

Zápisnica

Dátum konania: 26.11.2024

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Prezentovali sa vytvorené možnosti konverzie
- Ukážka prepisu na text
- Spôsob vytiahnutia príkazov z playbooku
- Konzultoval sa možný grafický nástroj na vizualizáciu CACAO 2.0

Úlohy do ďalšieho stretnutia:

- Pridať vytvorené konverzie do web aplikácie
- Začiatok práce na príprave konkrétnych playbookov, ktoré sa budú používať

Termín ďalšieho stretnutia:

Po dohode

Zápisnica

Dátum konania: 10.1.2025

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Rozdelenie úloh

Úlohy do ďalšieho stretnutia:

- Vytvorenie dokumentácie
- Vylepšenie GUI
- Vytvoriť handling nahrávania playbookov
- Vytvoriť konverziu z Yaml formátu
- CACAO Roster

Termín ďalšieho stretnutia:

Po dohode

Zápisnica

Dátum konania: 26.2.2025

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Prezentovalo sa čo sa urobilo, aktuálny stav

Úlohy do ďalšieho stretnutia:

- Zmanažovať upload na playbooky
- Pozrieť sa na typy kyber útokov na školu

Termín ďalšieho stretnutia:

Po dohode

Zápisnica

Dátum konania: 12.3.2025

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Prezentovanie doterajšej práce
- Konzultácia ohľadom tvarov príkazov pre shell v playbookoch

Úlohy do ďalšieho stretnutia:

- Pokračovať v príprave playbookov

Termín ďalšieho stretnutia:

26.3.2025

Zápisnica

Dátum konania: 26.3.2025

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Prezentovanie doterajšej práce

Úlohy do ďalšieho stretnutia:

- Dopracovať grafovú reprezentáciu playbookov
- Upraviť sadu playbookov na použitie pre fakultný CSIRT

Termín ďalšieho stretnutia:

9.4.2025

Zápisnica

Dátum konania: 9.4.2025

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Prezentovanie doterajšej práce
- Ukážka a konzultácia vybraných a upravených playbookov

Úlohy do ďalšieho stretnutia:

- Pokračovať v príprave ďalších playbookov

Termín ďalšieho stretnutia:

23.4.2025

Zápisnica

Dátum konania: 23.4.2025

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Prezentovanie doterajšej práce

Úlohy do ďalšieho stretnutia:

- Vyhľadávanie podľa typu incidentu
- Rozdelenie klasifikácie incidentov

Termín ďalšieho stretnutia:

7.5.2025

Zápisnica

Dátum konania: 7.5.2025

Vypracoval: Daniel Ondrejka

Zúčastnili sa:

Ing. Štefan Balogh, PhD.
Bc. Adam Budziňák
Bc. Tomáš Petráni
Bc. Daniel Ondrejka
Bc. Filip Kolenčík
Bc. Radovan Borsig

Obsah stretnutia:

- Prezentovanie doterajšej práce

Úlohy do ďalšieho stretnutia:

- Úprava nahrávania playbookov
- Vypracovanie dokumentácie

Termín ďalšieho stretnutia:

Posledné stretnutie

Zoznam použitej literatúry

1. ISO/IEC. *Information technology — Information security incident management — Part 1: Principles and process*. ISO, 2023. Č. ISO/IEC 27035-1:2023(en). Dostupné tiež z: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-2:v1:en>.
2. KAMARA, Irene a BOOM, Jasper. *Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices*. 2022. Dostupné z DOI: 10.13140/RG.2.2.10565.52967.
3. KILLCRECE, Georgia et al. *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon Software Engineering Institute, 2003. Dostupné tiež z: https://insights.sei.cmu.edu/documents/1605/2003_002_001_14099.pdf.
4. BIGELOW, Stephen J. *Compare runbooks vs. playbooks for IT process documentation*. 2024. Dostupné tiež z: <https://www.techtarget.com/searchitoperations/tip/Compare-runbooks-vs-playbooks-for-IT-process-documentation>.
5. HOLLENBERGER, John. *Incident Response Plans, Playbooks, and Policy*. 2023-05. Dostupné tiež z: <https://www.fortinet.com/blog/ciso-collective/incident-response-plans-playbooks-policy>.
6. CYBERSECURITY a (CISA), Infrastructure Security Agency. *Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems*. 2021. Dostupné tiež z: https://soc.cyber.wa.gov.au/pdfs/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.
7. DALKIR, Kimiz. *Knowledge Management in Theory and Practice*. Second. Cambridge, Massachusetts, London, England: The MIT Press, 2011. Dostupné tiež z: <https://ibmehub.com/opac-service/pdf/read/Knowledge%20Management%20in%20Theory%20and%20Practice%20by%20Kimiz%20Dalkir-%20Jay%20Liebowitz.pdf>.
8. ALAVI, Maryam a LEIDNER, Dorothy. Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. *MIS Quarterly*. 2001, roč. 1, s. 107–. Dostupné z DOI: 10.2307/3250961.

9. NONAKA, Ikujiro a TAKEUCHI, Hirotaka. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. Oxford University Press, 1995.
10. GONASHVILI, Mariami. *Knowledge Management for Incident Response Teams*. 2019. Dipl. pr. Masaryk University, Faculty of Informatics. Available at: https://is.muni.cz/th/pupg1/Knowledge_Management_For_Incident_Response_Teams.pdf.
11. AKBARI GURABI, Mehdi, MANDAL, Avikarsha, POPANDA, Jan, RAPP, Robert a DECKER, Stefan. SASP: a Semantic web-based Approach for management of Sharable cybersecurity Playbooks. In: *Proceedings of the 17th International Conference on Availability, Reliability and Security*. Vienna, Austria: Association for Computing Machinery, 2022. ARES '22. ISBN 9781450396707. Dostupné z DOI: 10.1145/3538969.3544478.
12. PROJECT, MISP. *MISP (Malware Information Sharing Platform)*. [B.r.]. Available at: <https://www.misp-project.org>.
13. EMPL, Philip. *Ad2Play Prototype* [<https://github.com/ad2play/ad2play>]. [B.r.]. GitHub repository.
14. ENISA. *Exploring the Opportunities and Limitations of Current Threat Intelligence Platforms* [<https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms>]. 2017. Public Version 1.0, December 2017.
15. STRATEGIC, Center for a (CSIS), International Studies. *A Shared Responsibility: Public-Private Cooperation for Cybersecurity* [https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220322_Lostri_Public_Private_Cooperation.pdf?VersionId=aoeH8e0s0uhaBPp8HPVgi.qkEXFmj2yX]. 2023.
16. KRÖTZSCH, Markus, VRANDECIC, Denny, VÖLKEL, Max, HALLER, Heiko a STUDER, Rudi. *Semantic MediaWiki* [https://www.semantic-mediawiki.org/wiki/Semantic_MediaWiki]. 2024. Dostupné tiež z: <https://www.semantic-mediawiki.org/wiki/SemanticMediaWiki..>
17. FOUNDATION, WIKIMEDIA. *MediaWiki* [<https://www.mediawiki.org/wiki/MediaWiki>]. 2024. Dostupné tiež z: <https://www.mediawiki.org/wiki/MediaWiki>.

18. JORDAN, Bret a THOMSON, Allan. *CACAO Security Playbooks Version 2.0* [OASIS Committee Specification 01]. 2023. Dostupné tiež z: <https://docs.oasis-open.org/cacao/security-playbooks/v2.0/cs01/security-playbooks-v2.0-cs01.html>. Latest version: <https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html>.
19. SCHLETTE, Daniel, EMPL, Philip, CASELLI, Marco, SCHRECK, Thomas a PER-NUL, Günther. Do You Play It by the Books? A Study on Incident Response Playbooks and Influencing Factors. In: *Proceedings of the 45th IEEE Symposium on Security and Privacy, SP 2024, San Francisco, CA, USA, May 20-23, 2024*. IEEE, 2024, s. 1–19.
20. OPEN CYBERSECURITY ALLIANCE. *CACAO Roaster*. 2024. Dostupné tiež z: <https://github.com/opencybersecurityalliance/cacao-roaster>. GitHub repository.
21. CONTRIBUTORS, Symfony. *Symfony YAML Component*. 2024. Dostupné tiež z: <https://github.com/symfony/yaml>. GitHub repository.