Tímový projekt 1 - Dokumentácia

Systém pre manažment incidentov

Zadanie

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

Obsah

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 sieťach, 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 podrobný návod ako krok za krokom reagovať na špecifické typy incidentov [5, 6]. Poskytuje preddefinované postupy prípravy na špecifické typy incidentov, taktiež postupy reakcie, keď dôjde k incidentu a zotavenia sa z nich. Tieto preddefinované postupy treba jasne dodržiavať.

1.2.1 Kľúčové komponenty playbookov

- **Špecifické typy incidentov:** Každá príručka je vytvorená na mieru pre konkrétny scenár incidentu. Zameriava sa na konkrétne typy 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.

Kľúčové 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 kľúčové pre organizačný tok práce a sú kľúčom 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 zraniteľnosti v softvéri. Každá zraniteľnosť má jedinečný CVE identifikátor a obsahuje podrobné informácie o chybe,
- **NIST NVD** - spravované organizáciou NIST. Poskytuje podrobné 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 podrobné 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 zdieľanie 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 vďaka štandardizovaným a sémanticky obohateným údajom, čo umožňuje efektívne zdieľanie 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 štandarde, 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 zdieľanie 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 uľahčuje 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 interaguje 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 sťažiť 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 izolovane [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 zohľadňujú interné procesy a štruktúry. V dôsledku toho nie sú verejne dostupné alebo ľahko prenositeľné medzi rôznymi organizáciami.

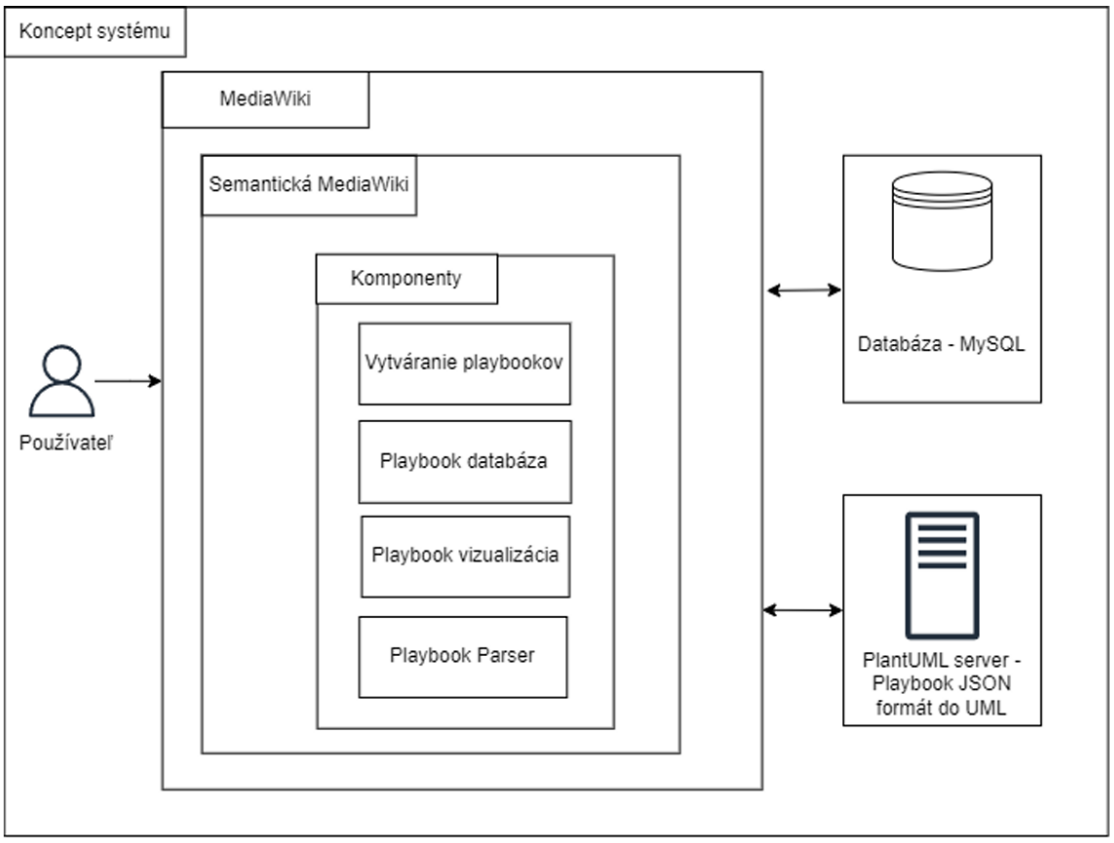
Navyše, vytvorenie efektívnych a univerzálnych playbookov vyžaduje značné zdroje, vrátane odborných znalostí a času [6]. Každá organizácia má svoje vlastné špecifiká, ktoré robia univerzálne riešenia menej efektívnymi. Z tohto dôvodu sú k dispozícii len obmedzené generické playbooky, ktoré často neposkytujú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

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 dáta. 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

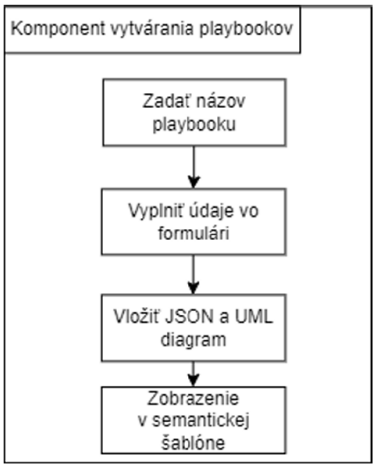
stránky vo formáte wiki.

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 pridávať viaceré tagy oddelené čiarkou, používajú sa na priraďovanie 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

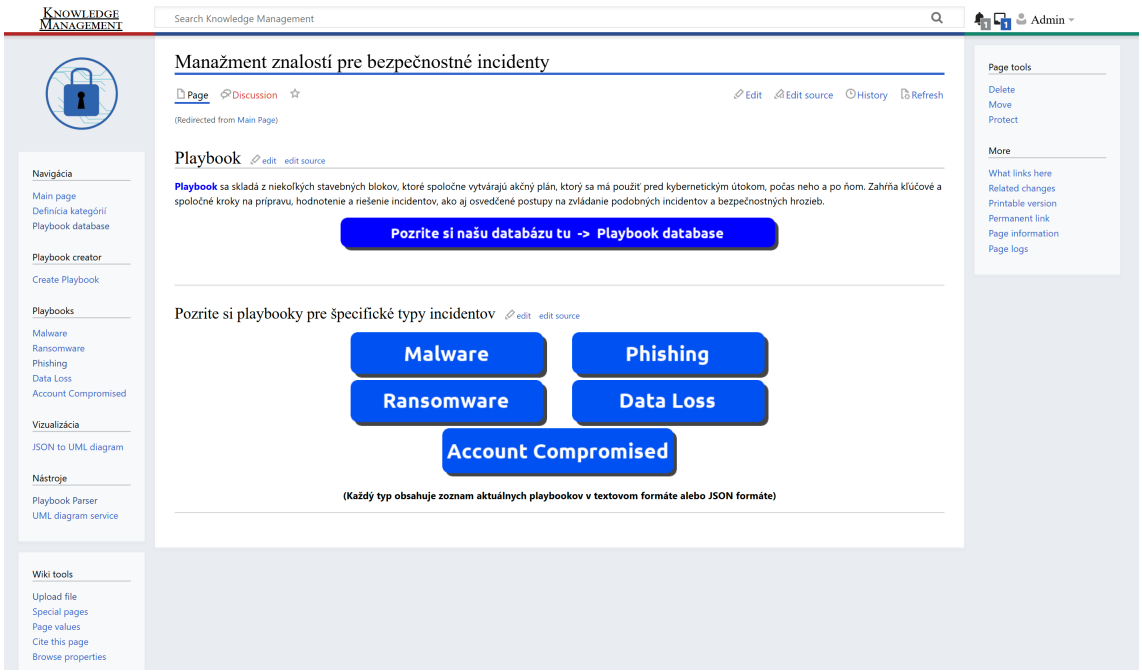
Na zlepšenie prehľadnosti a použiteľnosti je do riešenia integrovaný PlantUML server. PlantUML je nástroj na generovanie rôznych typov UML diagramov ako sú diagramy tried, sekvenčné diagramy, stavové diagramy a ďalšie, jednoduchým a intuitívnym spôsobom.

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.

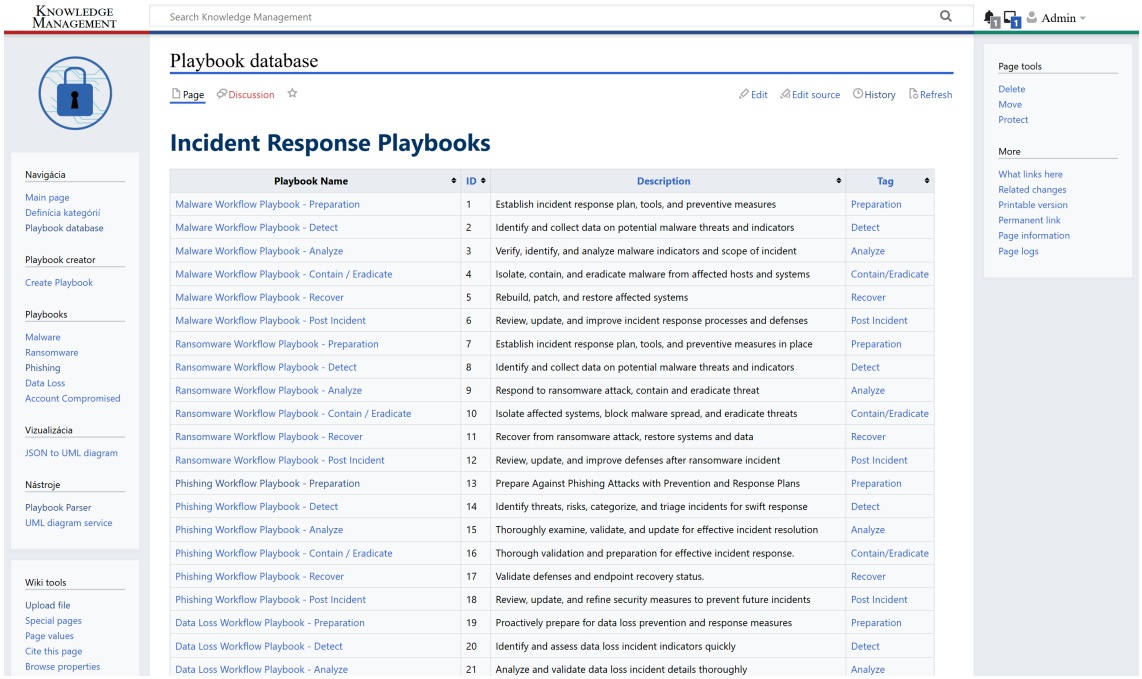
4.1.3 Komponent playbook parser

Tento komponent je kľúčovým 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.

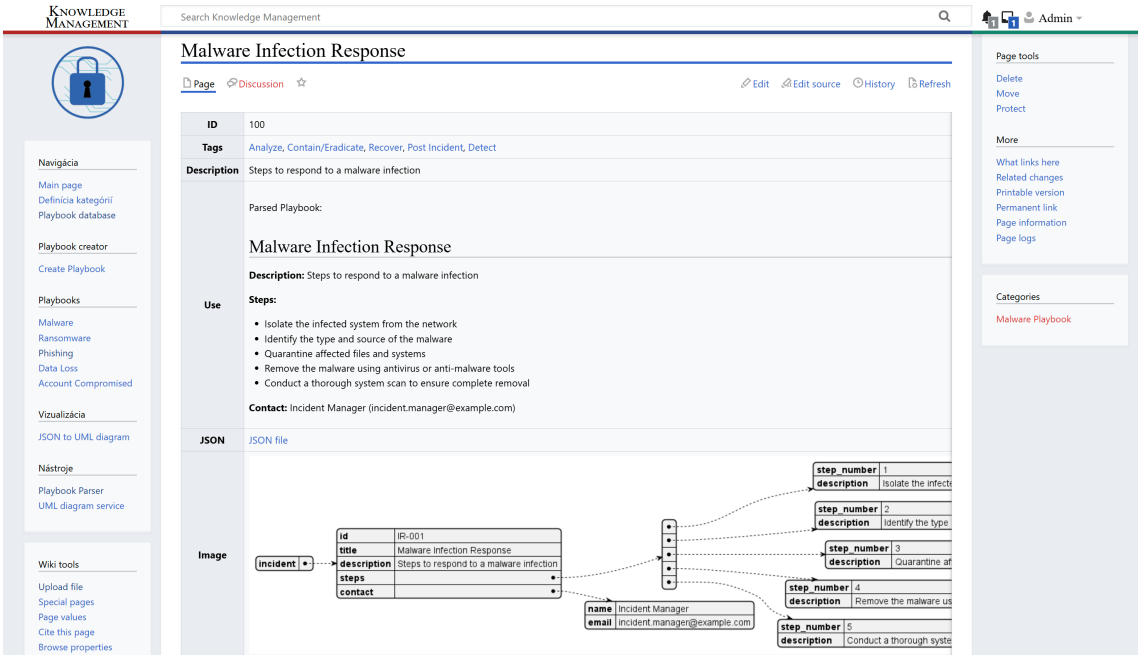
4.2 Ukážka použitého riešenia



Obr. 3: Hlavná stránka.



Obr. 4: Databáza playbookov.



Obr. 5: Ukážka vzhľadu playbooku.

5 Naše vylepšenia

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

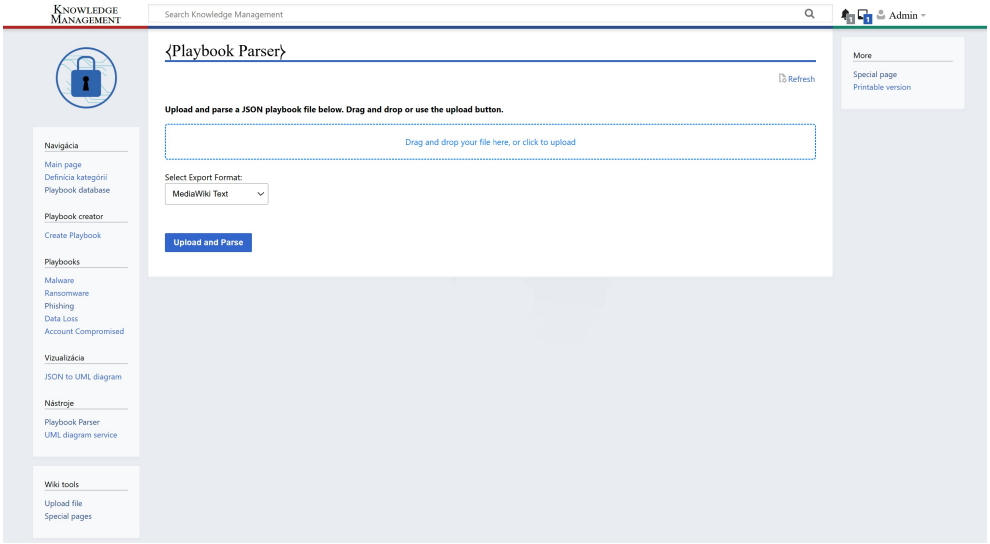
5.1 Implementácia štandardu CACAO 2.0

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 efektívnejšie a automatizovane.

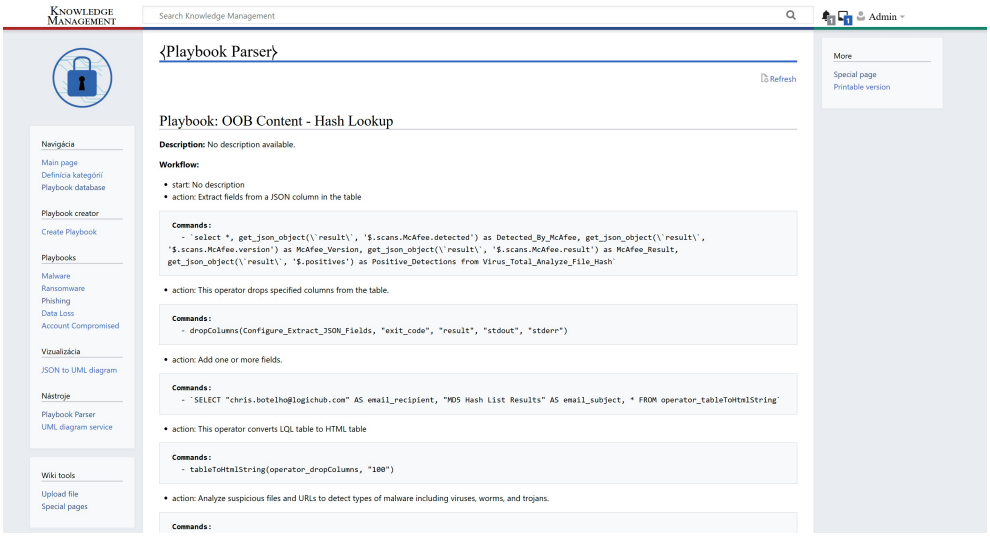
Vytvorili sme preklady do CACAO štandardu pre playbooky nasledovných spoločností:

- **Fortinet FortiSOAR**,
- **LogicHub SOAR**,
- **Chronicle Security**.

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.



Obr. 7: Playbook zobrazený ako MediaWiki text.

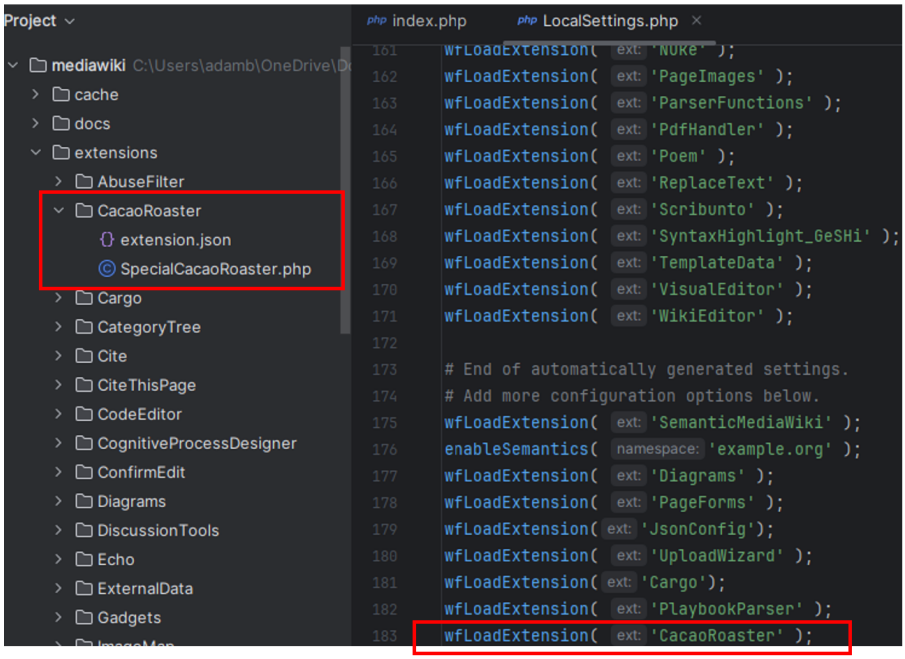
Playbook v CACAO štandarde po preklade obsahuje nasledujúce údaje:

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

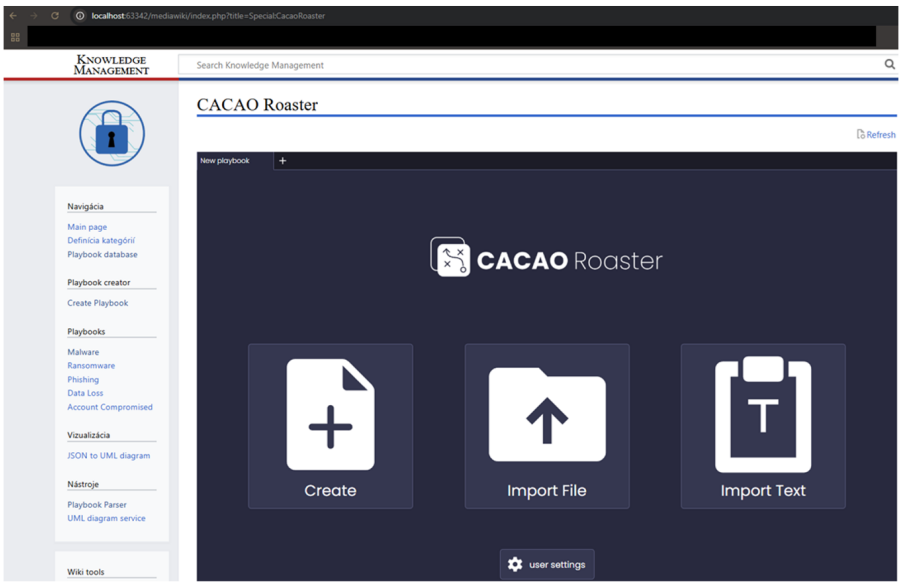
Tieto polia sa musia nachádzať v CACAO 2.0 štandarde. Okrem týchto polí sa v playbooku v CACAO štandarde môžu nachádzať aj iné polia. Ak sa v pôvodnom playbooku nenachádzali povinné polia pre CACAO štandard, hľadali sme aliasy, ktorými by sa mohli nahradiť jednotlivé polia. Ak sme alias nenašli vygenerovali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

5.2 Implementácia CACAO roaster

Pridanie funcionality pre vytváranie, úpravu a vizualizáciu CACAO playbookov pre projekt. Bola vytvorená extension v Mediawiki a následne načítaná v LocalSettings.php pre spustenie.



Obr. 8: Pridanie extension do MediaWiki.



Obr. 9: Vzhľad CACAO roaster na stránke.

5.3 Handling nahrávania playbookov

Táto funkcionalita zahŕňa nahratie pôvodného playbooku, konverzia playbooku do CACAO štandardu a náslené nahratie playbooku do databázy v našom riešení.

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 [20], 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 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 Kolenčik
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 Discordu 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 Kolenčik
Bc. Radovan Borsig

Obsah stretnutia:

- Dohodlo sa na nasledujúcom 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 pripraví 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 Kolenčik
Bc. Radovan Borsig

Obsah stretnutia:

- Šéf tímu mal svoju prezentáciu k existujúcim riešeniam
- Existujúce riešenia: Preberala sa možná implementácia určitých funkcionalít 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 nášeho 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 Kolenčik
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
- Bližšie 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 Kolenčik
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 Kolenčik
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 Kolenčik
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

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://nibmehub.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_Priatev_Cooperation.pdf?VersionId=aoeH8eOs0uhaBPp8HPVgi.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/Semantic$_{M}ediaWiki$..

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 PERNUL, 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. CONTRIBUTORS, Symfony. *Symfony YAML Component*. 2024. Dostupné tiež z: `https://github.com/symfony/yaml`. GitHub repository.