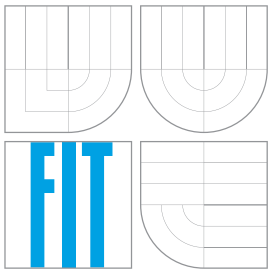
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

PLATFORMA PRO ZPRACOVÁNÍ HROZEB

CYBER THREAT INTELLIGENCE PLATFORM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — JERGUŠ JACKO
AUTHOR

VEDOUCÍ PRÁCE — Ing. MATEJ KAČIC
SUPERVISOR

BRNO 2016

Zadání bakalářské práce/18006/2015/xjacko03

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav inteligentních systémů Akademický rok 2015/2016

Zadání bakalářské práce

Řešitel: **Jacko Jerguš**
Obor: Informační technologie
Téma: **Platforma pro zpracování hrozeb**
Cyber Threat Intelligence Platform
Kategorie: Bezpečnost

Pokyny:

1. Seznamte se se standardy STIX, TAXII, CybOX a analyzujte způsob, jak zabezpečit výměnu informací o hrozbách, útocích a incidentech mezi organizacemi.
2. Na základě analýzy navrhněte platformu pro zpracování hrozeb a incidentů v oblasti bezpečnosti IT.
3. Implementujte systém složený z webové služby, databáze a webového administračního rozhraní.
4. Nástroj otestujte na poskytnutém testovacím vzorku dat od vedoucího.
5. Diskutujte možnosti dalšího rozšíření.

Literatura:

- Barnum, Sean. Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX). MITRE Corporation (2012): 11.
- Davidson, Mark, and Charles Schmidt. The TAXII Services Specification. The MITRE Corporation (2012).
- Dle doporučení vedoucího.

Pro udělení zápočtu za první semestr je požadováno:

- První dva body zadání.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Kačic Matej, Ing.**, UITS FIT VUT
Datum zadání: 1. listopadu 2015
Datum odevzdání: 18. května 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav inteligentních systémů
612 66 Brno, Božetěchova 2

L.S.

doc. Dr. Ing. Petr Hanáček
vedoucí ústavu

Abstrakt

Cieľom práce je vytvoriť webovú platformu, ktorá poskytne zjednodušený popis, spracovanie a výmenu bezpečnostných incidentov za pomoci dostupných štandardov STIX, TAXII, CybOX, IDEA. Platforma poskytuje restové API pre zhromažďovanie externých udalostí vo fomráte IDEA, nástroj pre vytvárenie STIX formátovaných modelov udalostí a mechanizmus pre výmenu spracovaných udalostí s využitím služieb popísaných štandardom TAXII.

Abstract

Main goal of this thesis is to create an web application platform, which provides simplified characterization, adaptation and exchange of cyber threat incidents using the STIX, TAXII, CybOX and IDEA standards. Platform has implemented rest API to collect external events in IDEA format, tool for creating STIX formatted models of events and model exchange mechanism based on TAXII described services.

Kľúčové slová

STIX, TAXII, CybOX, IDEA, spracovanie bezpečnostných hrozieb, výmena bezpečnostných hrozieb

Keywords

STIX, TAXII, CybOX, IDEA, cyber thrat analysis, cyber threat exchange

Citácia

JACKO, Jerguš. *Platforma pro zpracování hrozeb*. Brno, 2016. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Kačic Matej.

Platforma pro zpracování hrozeb

Prehlásenie

Čestne prehlasujem, že som vypracoval túto bakalársku prácu samostatne pod vedením pána Ing. Mateja Kačica. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

.....
Jerguš Jacko
18. mája 2016

Poďakovanie

Veľmi rád by som poďakoval vedúcemu mojej bakalárskej práce Ing. Matejovi Kačicovi za jeho odborné rady a pripomienky. Poďakovanie si taktiež zaslúži moja rodina, za ich trpezlivosť a pomoc.

Obsah

Kapitola 1

Úvod

V súčasnej dobe sa bezpečnostné hrozby a ich komplexnosť rozvíja rýchlejšie ako kedykoľvek predtým vďaka viac a viac pokročilejšími, schopnejšími a motivovanými útočníkmi. Pri analýze bezpečnostných incidentov sa často stretávame so znovu-používaním tých istých útokov, pretože sú osvedčené, fungujú a organizácie nedržia krok s potrebou ich prevencie. Pre udržanie kroku s týmito rozvíjajúcimi a stálymi hrozbami sa musíme zamerať na akcie, ktoré sú skoršou fázou životného cyklu počítačového útoku a musíme vytvoriť všeobecné zázemie pre štandardizovanie informácií o bezpečnostných hrozbách.

Rýchlejšia detekcia a prevencia vyžaduje viac inteligentné, automatické a plynulé zdieľanie týchto hrozieb. Ideálne by sme sa mali usilovať o zdieľanie ihneď v momente výskytu bezpečnostnej hrozby. Zdieľanie, zbieranie a zdokonalovanie spracovania hrozieb na základe spolupráce nie je nič nové, ale zvyčajne založené na manuálnej činnosti (copy-paste metóda z rôznych dokumentov), nedostatočne spracovanou konceptuálnou informáciou, keďže rozličné zdroje poskytujú odlišné úrovne a spracovanie kontextu, detailov a termínov. Spôsob a obsah zdieľania poznatkov o bezpečnostných hrozbách môže zvýšiť naše poznanie útočníka a jeho metódy. Toto poznanie môže nastať, keď máme dostatok informácií zo širokej škály spolupracujúcich účastníkov. Žiadny jednotlivec nemôže nazhromaždiť všetky relevantné informácie. Preto je dôležité pristúpiť na štandardizáciu informácií o bezpečnostných hrozbách a incidentoch.

V rámci tejto bakalárskej práce sa pokúsim navrhnúť a naimplementovať platformu pre spracovanie hrozieb a incidentov v oblasti bezpečnosti IT a ukázať problémy, s ktorými som sa pri mojom výskume stretol, pričom sa zameriam na efektívne využitie štandardov STIX, TAXII, CybOX a IDEA.

Práca je členená do štyroch kapitol. Základným princípom a architektúrou štandardov sa zaoberá pomerne obšírnejšia úvodná druhá kapitola. Tretia kapitola analyzuje využitie štandardov pri požiadavkách platformy, analyzuje základný koncept riešenia a spôsoby k jeho prístupu. Návrh výslednej platformy, pozostávajúcej z webovej služby, databázy a webového administračného rozhrania je popísaný v štvrtej kapitole. V záverečnej piatej kapitole sa nachádza návrh rozšírení do budúcnosti a testovanie platformy pri vytváraní modelov na základe analýzy poskytnutých scenárov.

Kapitola 2

Štandardy pre spracovanie hrozieb

Štandardy pre spracovanie bezpečnostných hrozieb, útokov a incidentov poskytujú účinný prostriedok pri analýze a zdieľaní bezpečnostných informácií. Zabezpečujú lepšiu automatizáciu a proces ich spracovania.

Structured Threat Information Expression (STIX), *Trusted Automated Exchange of Indicator Information* (TAXII) a *Cyber Observable Expression* (CybOX) sú voľne dostupné, otvorenou komunitou riadené špecifikácie, ktoré pomáhajú s automatickou výmenou informácií o bezpečnostných hrozbách a incidentoch. Tieto špecifikácie sú výsledkom snahy o ich štandardizovanú reprezentáciu, ktoré softvér môže využívať pre jednoduchšie zdieľanie hrozieb a incidentov medzi spoločnosťami a organizáciami.

Intrusion Detection Extensible Alert (IDEA), riadená organizáciou CESNET [7] predstavuje pokus o definovanie modelu štandardu, ktorý by pokrýval dnešné požiadavky pre rozličné riešenia z oblasti bezpečnostných incidentov, s braním ohľadu na doposiaľ existujúce formáty, ich výhody a slabiny.

V nasledujúcich podkapitolách sú vyššie zmienené špecifikácie podrobnejšie popísané a vysvetlené.

2.1 STIX

Structured Threat Information Expression (STIX) je jazyk pre zabezpečenie štandardizovanej reprezentácie, zachytávania, charakterizácie a komunikácie informácií o bezpečnostných hrozbách a incidentoch. Nie je to program ani nástroj, ale komponenta, ktorá podporuje štrukturalizovaný spôsob využitia pre lepšiu efektívnosť, konzistenciu a automatizáciu spracovania informácií o bezpečnostných hrozbách v programoch a nástrojoch. Táto štandardizovaná reprezentácia je lepšie využiteľná mnohých v prípadoch použitia (2.1.1), súvisiacich s procesom analýzy, spracovania a zdieľania bezpečnostnej hrozby. STIX poskytuje zjednocujúcu architektúru (2.1.2), ktorá sumarizuje rôznorodú škálu informácií o bezpečnostných hrozbách (2.1.3).

Nasledujúce podkapitoly boli spracované z [5].

2.1.1 Model použitia STIXu

Stix je zameraný na podporu celej oblasti prípadov použitia pri analýze, zbieraní, spracovaní a zdielaní informácií o bezpečnostných hrozbách. Model prípadov použitia (obrázok 2.1) sa skladá z nasledujúcich celkov:

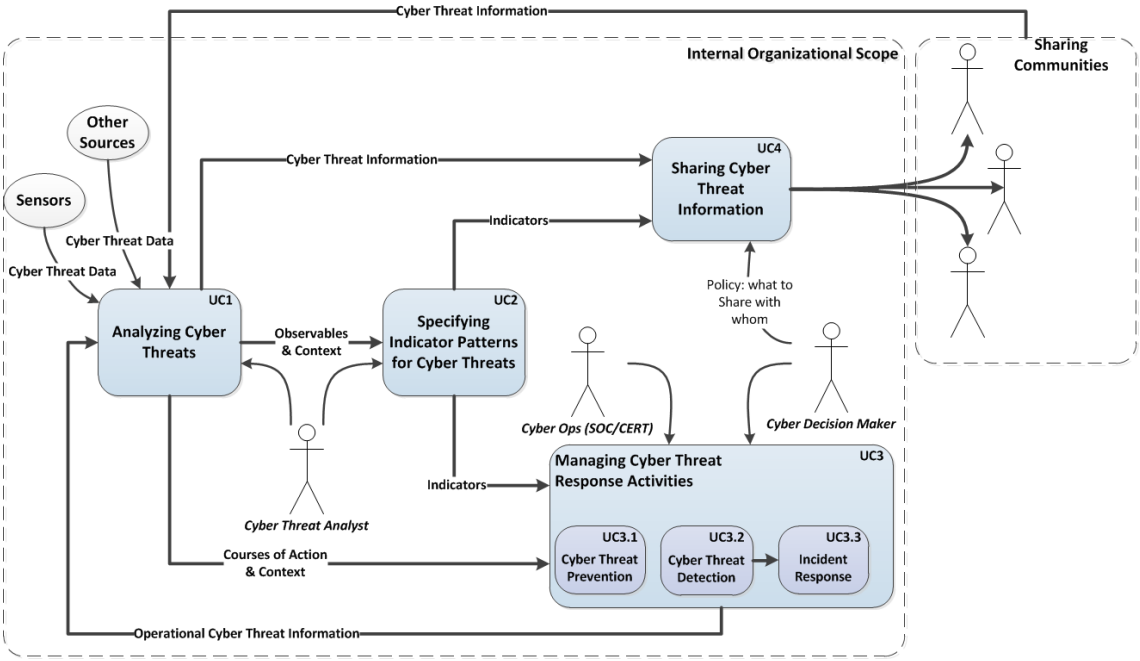
- *Analýza bezpečnostných hrozieb (UC1)*
  Bezpečnostný analytik *Cyber Threat Analyst* analyzuje informácie o bezpečnostnej hrozbe, nazbierané z rôznych zdrojov (komunity *Sharing communities*, senzory *Senzors*, podobné bezpečnostné hrozby a ostatné dostupné zdroje), založených na manuálnej aj automatickej činnosti zhromažďovania informácií. Analytik sa snaží pochopiť a identifikovať princíp bezpečnostnej hrozby, ktorý následne chrakterizuje všetkými dostupnými poznatkami (správanie, možnosti, zámery, akcie, konatelia). Následne, po tejto charakterizácií a pochopení hrozby, analytik môže špecifikovať relevantné vzory indikátorov (*Indicator* 2.1.3) hrozieb, navrhnúť odpovedajúce postupy a zdieľať poznatky s ďalšími zakomponovanými účastníkmi.

- *Špecifikovanie vzorov indikátorov bezpečnostných hrozieb (UC2)*
  Bezpečnostný analytik *Cyber Threat Analyst* špecifikuje merateľné vzory, reprezentujúce viditeľnú charakteristiku (*Observable* 2.1.3)) danej bezpečnostnej hrozby a charakterizuje relevantné dáta pre interpretovanie, narábanie a aplikovanie týchto vzorov a ich výsledkov. Tieto vzory sú ďalej využiteľné v spracovaní a zdieľaní poznatkov o bezpečnostných hrozbách.

- *Spracovanie odpovedajúcich aktivít (UC3)*
  Bezpečnostný zamestnanci *Cyber Ops* a zakomponovaný účastníci *Cyber Decision Maker* spoločne pracujú na prevencií, detekcií, vyšetrovaní a akciách voči aktivitám bezpečnostných hrozieb. Preventívne opatrenia môžu zmierniť zraniteľnosť, slabé stránky a chyby, ktoré môžu byť aktivitou bezpečnostnej hrozby využité. Po odhalení a vyšetrení konkrétnych incidentov, môžu byť vykonané akcie spojené s reakciou na tieto incidenty.

  - *Prevencia (UC3.1)*
    Bezpečnostný zamestnanec, rozvinie potenciálnu prevenciu pre identifikovanú hrozbu a vyberie vhodné spôsoby pre jej implementáciu, ktorú zrealizuje iný operatívny personál.
  - *Detekcia (UC3.2)*
    Bezpečnostní zamestnanci aplikujú mechanizmy na monitorovanie a sledovanie bezpečnostných hrozieb, za účelom zistenia výskytu špecifických hrozieb. Tieto mechanizmy sú zvyčajne aplikované vzory indikátorov (UC2).
  - *Reakcia (UC3.3)*
    Bezpečnostný personál reaguje na detekcie potenciálnych bezpečnostných hrozieb, vyšetruje čo sa stalo, alebo čo sa deje, pokúšajú sa identifikovať aktuálnu hrozbu a realizujú nápravné opatrenia ((*COA* 2.1.3)).

- *Zdieľanie informácií o bezpečnostných hrozbách (UC4)*
  Bezpečnostný zamestnanec *Cyber Decision Maker* vyhodnotí, ktoré zhromaždené bezpečnostné informácie (UC1) a vzory (UC2) si môže dovoliť zdieľať a s kým (komunity, organizácie) si ich môže dovoliť zdieľať.



Obr. 2.1: Model prípadou využitia STIXu, prevzaté z [5]

2.1.2 Architektúra STIXu

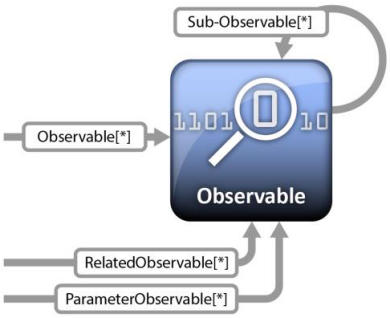
Diagram architektúry STIXu (príloha A.1) znázorňuje základný koncept spracovania bezpečnostnej hrozby ako nezávislú a znova-použiteľnú konštrukciu a charakterizuje všetky vzťahy jej komponent (2.1.3).

Orientované hrany medzi jednotlivými komponentami naznačujú ich vzájomný vzťah pre nadväzujúcu implementáciu súvislostí bezpečnostnej hrozby. Cieľový prvok orientovanej hrany je konceptuálny typ (komponenta), ktorá je navrhovaná, ale nie vyžadovaná pre zužitkovanie špecifickej STIX implementácie konštrukcie východzej hrany. Čiže cieľová komponenta orientovanej hrany je rozvinutím aktuálnej informácie o bezpečnostnej hrozbe. Popis orientovanej hrany vyjadruje jej slovný vzťah medzi komponentami, pokiaľ hranatá zátvorka s hviezdičkou v popise hrany vyjadruje, že vzťah medzi komponentami môže existovať nula až nekonečno krát.

2.1.3 Štruktúra STIXu

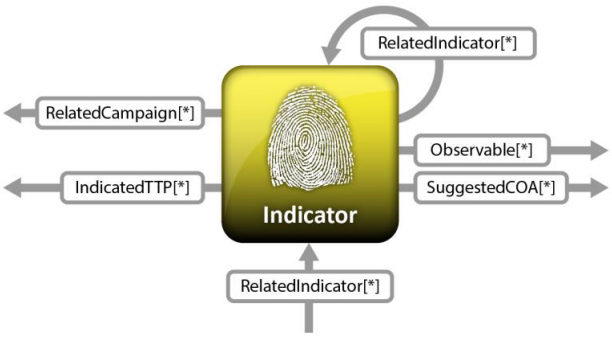
STIX jazyk zahŕňa osem podstatných komponent—*Observable*, *Indicator*, *Incident*, *TTP*, *ExploitTarget*, *CourseOfAction*, *Campaign* a *ThreatActor*— ktoré sa podieľajú na výslednej architektúre a konštrukcií jazyka STIX. Význam týchto komponent je popísaný v nasledujúcich bodoch:

- **Observable** je tá časť bezpečnostnej hrozby, ktorú vidíme. Sú to stavové vlastnosti alebo merateľné udalosti, týkajúce sa operácií s počítačmi a sieťami. Observable môže byť informácia o kľúči registru, o súbore (jeho meno, hash, veľkosť..), emailová správa obdržaná zo špecifickej adresy, bežiaca služba, odoslaná HTTP požiadavka.. Je to základná komponenta STIX architektúry 2.1.2. Jej vyjadrenie a popis predstavuje formát v štandarde CybOX (2.2).



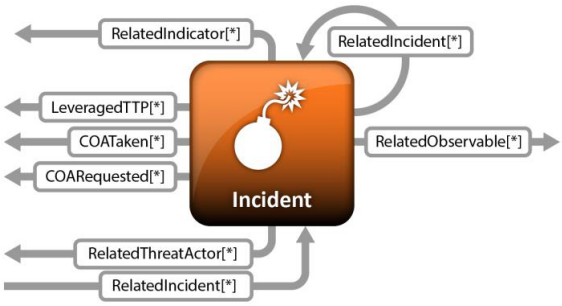
Obr. 2.2: Observable, komponenta architektúry STIX, prevzaté z [5]

- **Indicator** určuje, aké hrozby by sme mali hľadať v systéme a prečo práve tie. Prináša konkrétne pozorovateľné vzory *Observable* a v kombinácií s kontextovými informáciami má predstavovať artefakty alebo správanie záujmov v rámci kontextu počítačovej bezpečnosti. Skladajú sa z jedného alebo viacerých pozorovateľných vzorov *Observable*, ktoré sú potenciálne namapované do *TTP* kontextu a obohatené s ďalšími príslušnými metadátami, ako napríklad časový rámec, zdroj informácií, IDS (Intrusion Detection System) pravidlá..



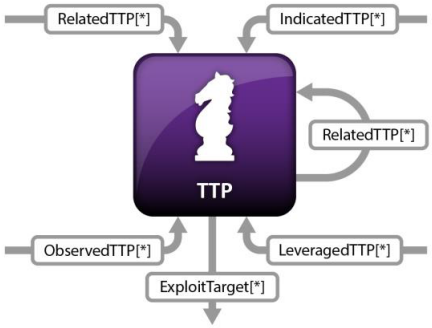
Obr. 2.3: Indicator, komponenta architektúry STIX, prevzaté z [5]

- **Incident** je diskrétna inštancia indikátora *Indicator*, ktorá ovplyvňuje organizáciu. Je to set aktivít, spojených s tým istým útočníkom z kontextu. Zahŕňa údaje, ako časovo založené informácie, zúčastnené strany, ovplyvnené aktivity, dopad vplyvu incidentu, odozva vykonaných opatrení *COA*, zdroj informácií o incidente a podobne.



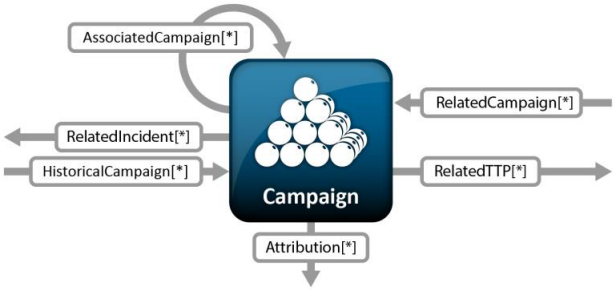
Obr. 2.4: Incident, komponenta architektúry STIX, prevzaté z [5]

- **Tactics, Techniques, and Procedures (TTP)** reprezentuje správanie alebo metódy (zvyklosti) útočníka, teda, čo robí a ako to robí. Pozostáva zo špecifického chovania útočníka (vzory útokov, exploity, malware), zdrojov útočníka (nástroje, infraštruktúra, fiktívne charaktery), zamýšľané efekty útoku atď. TTP hrá centrálnu rolu v informáciach a inteligencií týkajúcej sa bezpečnostných hrozieb.



Obr. 2.5: TTP, komponenta architektúry STIX, prevzaté z [5]

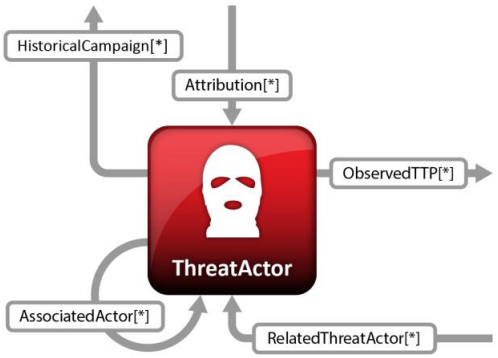
- **Campaign** sleduje zámer útočníka (prečo robí danú činnosť) prostredníctvom setu Incidentov a TTP, ideálne naprieč organizáciami. Môže pozostávať z podozrivého zamýšľaného efektu útočníka, súvisiacich TTP, zdroja informácií kampane, atď.



Obr. 2.6: Campaign, komponenta architektúry STIX, prevzaté z [5]

- **Threat Actor** je ten, kto je zodpovedný za danú hrozbu/incident. Je to charakteri-

zácia škodlivých protivníkov, predstavujúcich hrozbu kybernetického útoku, vrátane predpokladaného zámeru a historicky pozorovaného správania. Skladá sa z charakterizácie identity, podozrenia na motiváciu, podozrenia zamýšľaného útoku, histórie TTP a pod.

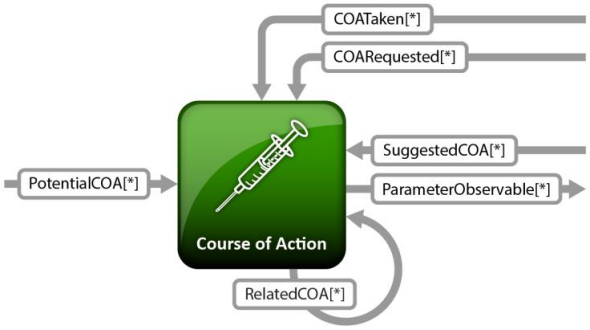


Obr. 2.7: Threat Actor, komponenta architektúry STIX, prevzaté z [5]

- **Exploit Target** je zraniteľnosť alebo slabosť v softvéri, systémoch, počítačových sieťach alebo konfigurácií, ktoré sú cieľom exploitu daného útočníka (TTP daného Threat Actora). Pozostáva z identifikácie alebo charakterizácie zraniteľnosti, zo slabosti danej identifikácie/charakterizácie, konfigurácie identifikácie/charakterizácie, potenciálnych COA, zdroj jeho informácií a pod.

Obr. 2.8: Exploit Target, komponenta architektúry STIX, prevzaté z [5]

- **Courses of Action (COA)** sú defenzívne akcie proti hrozbe (prevencia, sanácia, zmierňovanie). Sú to osobité opatrenia, ktoré je potrebné prijať na riešenie hrozby, či sú to nápravné alebo preventívne riešenia, alebo zodpovednosť na zvrátenie alebo zmiernenie potenciálnych dopadov incidentu. Skladajú sa z ich príslušnej fázy usmerňovania kybernetickej hrozby (napr. reakcia na incident..), typu, popisu, ciela, štrukturované znázornenie (napr. IPS pravidlo, automatizovaný patch..), pravdepodobného dosahu, pravdepodobných nákladov, odhadovanej účinnosti COA, atď.



Obr. 2.9: COA, komponenta architektúry STIX, prevzaté z [5]

2.2 CybOX

CybOX je popis štandardizovanej štruktúry pre reprezentáciu časti bezpečnostnej hrozby *Observable*. Je to popis dynamickej udalosti alebo stavovej vlastnosti, napríklad popis objektov sieťového pripojenia, ktoré je sprostredkované voči špecifickej adrese, MD5 hash súboru, proces, URI modifikácie a mnoho ďalších popisov [20]. CybOX podobne ako STIX (2.1), sa zameriava na dostatočne flexibilné a komplexné riešenie pre pokrytie všetkých požiadaviek prípadov využitia 2.1.1 pri manipulácií s časťou *Observable*. CybOX môže byť využitý pri posudkoch hrozieb, manažmentu záznamov, charakterizácií malvéru, zdieľaní indikátora, reakcie na incidenty.

2.3 TAXII

Trusted Automated Exchange of Indicator Information (TAXII) je preferovaná metóda výmeny informácií, ktoré sú reprezentované vo formáte jazyka STIX (2.1). Táto metóda umožňuje bezpečnú, rýchlu a automatickú výmenu informácií o bezpečnostných hrozbách medzi rôznymi organizáciami a ich partnermi.

TAXII nie je nástroj alebo program, ale snaha o štandardizovanú definíciu kolekcie služieb, správ a protokolov na výmenu informácií o hrozbách a incidentoch. Na základe tejto špecifikácie výmeny informácií podporuje organizácie pre dosiahnutie dobre fungujúcej detekcie, prevencie a zmiernenie dopadu bezpečnostných hrozieb.

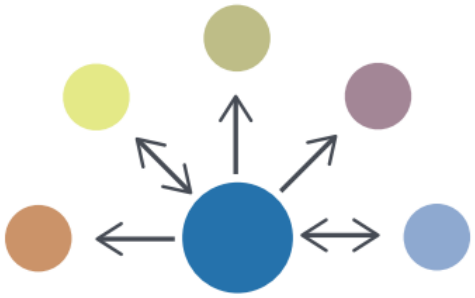
V nasledujúcich podkapitolách boli informácie čerpané z [6].

2.3.1 Modely výmeny informácií

TAXII je zameraný na použitie pre všetkých tvorcov, vývojárov a spotrebiteľov zaoberajúcich sa spracovaním bezpečnostných hrozieb, vrátane vlády, premyslu a akademickej pôdy. Preto podporuje nasledujúce tri široko využívané modely výmeny informácií:

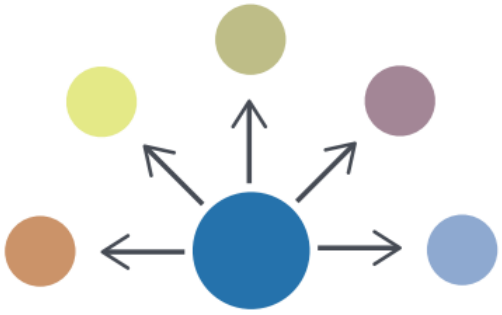
- **Hub and Spoke** model funguje na princípe, že jedna organizácia koná ako sklad (hub) pre všetkých zdieľajúcich účastníkov (spokes). Spoke zdieľa informácie s hubom, ktorý následne zdieľa ďalej túto informáciu s ostatnými spokes. Hub môže vykonávať analýzu alebo filtrovanie pred zdieľaním novej informácie. V tomto modeli sa informácie môžu zdieľať v smere spoke - hub, ale aj v smere hub - spoke.

Výhody tejto architektúry sú v možnosti spoka informácie len prijímať a nezdieľať, čo môže byť požadovanou funkciou niektorých organizácií vzhľadom k zachovaniu svojej privátnej databázy bezpečnostných hrozieb.



Obr. 2.10: Hub and spoke diagram, prevzaté z [6]

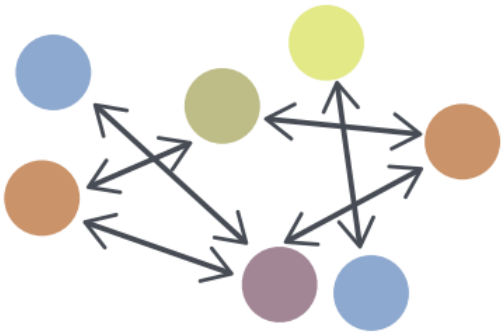
- **Source/Subscriber** (Zdroj/Odberateľ) je architektúra, kde jedna organizácia koná ako samostatný zdroj informácií pre všetkých odberateľov. Informácie tu tečú v smere zdroj - odberateľ.



Obr. 2.11: Source/Subscriber diagram, prevzaté z [6]

- **Peer to Peer** model zdieľania informácií využíva logiku, kde všetky organizácie konajú ako konzument aj producent. V tejto architektúre sa informácie zdieľajú medzi všetkými peermi, od jedného k ďalšiemu.

  Výhodou tejto architektúry je jej transparentnosť informácií voči ostatným organizáciám.



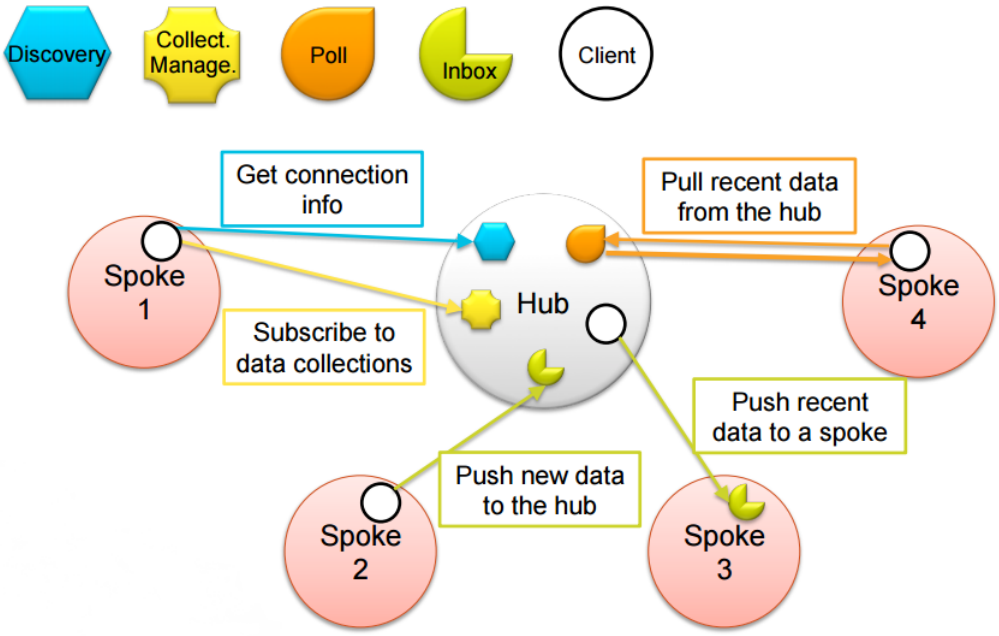
Obr. 2.12: Peer to Peer diagram, prevzaté z [6]

2.3.2 Služby zabezpečujúce výmenu informácií

TAXII definuje nasledujúce štyri služby, kde každá služba je voliteľná a služba môže byť kombinovaná v rôznych spôsoboch pre rôzne modely výmeny informácií.

- **Inbox** - služba pre obdržanie nových informácií.
- **Poll** - služba pre vyžiadanie nových informácií.
- **Collection Management** - služba pre učenie o odberateľoch a vyžiadanie odberateľov o zber dát.
- **Discovery** - učenie, ktoré služby sú podporované a ako s nimi spolupracovať.

Príklad využitia služieb je znázornený na obrázku 2.13. Tento príklad kombinuje všetky štyri služby výmeny informácií s modelom výmeny informácií *Hub and Spoke*.



Obr. 2.13: Príklad využitia služieb pre model "Hub and Spoke", prevzaté z [21, p. 21]

2.4 IDEA

Intrusion Detection Extensible Alert (IDEA), predstavuje model pre výmenu množstva dát, generovaných rôznymi typmi IDS *Intrusion detection systems* systémov, honeypotov, systémových analyzátorov a analyzátorov dátových tokov. Tento model poskytuje značnú rozšíriteľnosť vďaka možnosti pridávania vlastných kľúčov a dát, schopnosť označovať anonymizované, nepresné, neúplné či podvrhnuté dáta, schopnosť rozlišovať vlastné, agregované/korelované udalosti a udalosti tretích strán ako aj možnosť využívania rôznych slovníkov a značiek pre popis zdroja/cieľa/detektora. Model IDEA je možné popísať v troch bodoch:

- **Dizajn** modelu kladie požiadavky pre jednoduchú reprezentáciu dátových typov rôznych programovacích jazykov. Preto je IDEA vo formáte JSON [8] s dvojlevelovou hĺbkou stromu kľúčov a atribútov.
- **Klasifikácia** dát modelu pre udalosti podľa typu incidentu (malvér, narušenie, krádež, zraniteľnosť..), typu sieťového protokolu (ssh, dns, http..), zdroja/cieľa (proxy, pishing, spam, botnet), detekčného uzla (tok dát, datagram, korelácia..) či popis príloh a objektov (exploit, syslog, malvér..).
- **Definícia** modelu zahŕňa niekoľko povinných a voliteľných kľúčov, ktoré zabezpečia jednoznačnosť, validitu a rozšíriteľnosť modelu. Medzi povinné kľúče sa radia formát, identifikátor, čas detekcie a kategória detekovanej udalosti. Príklad definície modelu znázorňuje nasledujúca JSON štruktúra:

```
{
    "Format": "IDEA0",
    "ID": "85d6f78w-9987-497a-r9s7-bcbde759sd3q",
    "DetectTime": "2016-04-19T18:03:32Z",
    "Category": ["Abusive.Spam"],
    "Description": "URL spam reference",
    "Source": [
        {
            "Type": ["OriginSpam"],
            "URL": ["http://www.example.com/"],
            "Proto": ["tcp", "http", "www"]
        }
    ]
}
```

Kapitola 3

Analýza

Výmena informácií o hrozbách, útokoch a incidentoch medzi organizáciami sa dá docieliť využitím štandardizovaných formátov pre popis bezpečnostných hrozieb a využívaním štandardizovanej výmeny informácií medzi organizáciami. Dôležitou vlastnosťou výmeny informácií je ich kvalitné spracovanie na základe prvotnej analýzy a následné efektívne zdieľanie. V tejto kapitole sa budem venovať práve tomuto spracovaniu a zdieľaniu za pomoci dostupných štandardov.

Z analýzy štandardov pre spracovanie bezpečnostných hrozieb (kapitola 2) vyplýva zjednodušený poznatok, že STIX (2.1) je jazyk, ktorý môže využívať CybOX (2.2) tvary a komunikácia je možná s využitím TAXII (2.3). Čiže STIX chrakterizuje to, čo má byť povedané, pokým TAXII definuje, ako je jazyk STIX zdieľaný.

Analýza potrieb platformy spracovania hrozieb sa skladá z dvoch častí. Prvá časť zahŕňa *front-end* pre analýzu nových aj existujúcich bezpečnostných incidentov. Druhá časť má zabezpečiť spoľahlivý a bezpečný *back-end* pre automatizáciu ukladania a zdieľania incidentov. Funkcia front-endu by mala poskytovať *API1* pre spracovanie a analýzu kolekcie incidentov a *API2* pre zber nových incidentov. *API1* využije štandardy STIX a CybOX pre popis incidentov z databázy, ktoré budú analyzované analytikom. *API2* bude restové API, na ktoré sa budu zasielať nové detekované incidenty. Back-end zabezpečí vhodné ukladanie nových a stávajúcich incidentov a za pomoci štandardu TAXII zdieľanie spracovaných incidentov s partnerskými organizáciami.

3.1 Existujúce riešenia

V súčastnosti existuje Python knižnica "libtaxii"[11] a Java knižnica "java-stix"[2] pre implementáciu TAXII klienta a invokáciu služieb TAXII servera a bezpečný koncept TAXII serveru "Yeti"[18]. Aktuálne, TAXII definuje zasielanie XML správ cez protokol HTTP(S), ale jeho dizajn dovoľuje aj implementáciu iných riešení. Pre implementáciu/popis bezpečnostných incidentov vo formáte STIX je možné využiť Python knižnicu "python-stix"[12] alebo Java knižnicu "java-stix"[3], ktorá poskytuje API pre zjednodušené vytváranie a spracovanie hrozieb vo formáte definovanom jazykom STIX.

3.2 Koncept

S využitím poznatku o štandardoch a výsledku analýzy potrieb platformy je zostavený koncept riešenia fungovania platformy (obrázok 3.1).

Koncept sa skladá z niekoľkých účastníkov, logického rozloženia a zabezpečenia jednotlivých služieb platformy.

Účastníci sú nasledujúci:

- **Zákazníci** poskytujú novo detekované incidenty, ktoré vystavujú na *restové API* platformy.
- **Organizácia poskytujúca systém** pre analýzu a spracovanie incidentov. Zabezpečuje zbieranie a popis incidentov vo formáte STIX s využitím CybOX a poskytuje zdieľanie incidentov s partnerskými organizáciami za pomoci štandardu TAXII.
- **Iné organizácie**, s ktorými prebieha zdieľanie analyzovaných dát si vymieňajú informácie pomocou štandardu TAXII. Model zdieľania závisí na požadovanej špecifikácií partnerských organizácií vzhľadom na transparentnosť výmeny informácií.

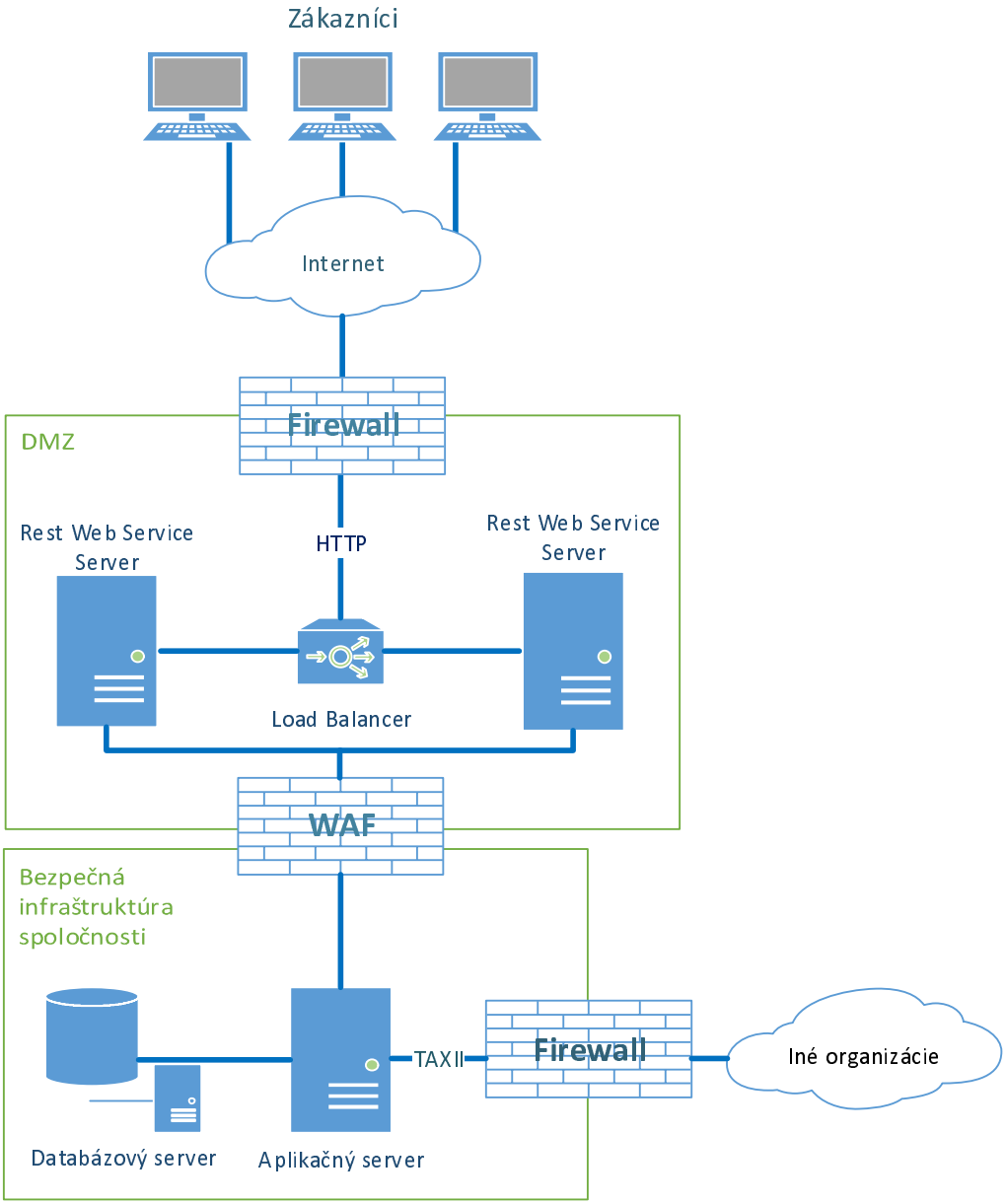
Služby, ktoré poskytuje platforma sa delia na nasledujúce logické celky:

- **Rest Web Service Server** (RWSS) vystavuje *rest API* voči zákazníkom pre izolovaný zber bezpečnostných incidentov (umožnuje pristupovať k dátam na určitom mieste pomocou HTTP dotazov). Definuje vzdialené procedúry a protokol pre ich volanie.
- **Databázový server** zabezpečuje uloženie a agregáciu bezpečnostných incidentov. Uchováva spracované aj nespracované bezpečnostné incidenty vo formáte STIX s využitím CybOX.
- **Aplikačný server** postavený na *Apache Tomcat*, ktorý poskytuje aplikačné GUI pre prácu s bezpečnostnými incidentami (ich transformáciu do STIX podoby, grafická analýza incidentov) a službu pre zdieľanie bezpečnostných incidentov, založenú na popise služieb štandardom TAXII. Služba pre zdieľanie incidentov môže byť implementovaná viacerými spôsobmi podľa požadovaného modelu zdieľania 2.3.1.

O zabezpečenie platformy a jej logických celkov sa stará niekoľko *firewall*ov:

- *Firewall medzi zákazníkmi a RWSS* sa stará o blokovanie nežiaducej komunikácie. Vystavuje *RWSS* do *DMZ (DeMilitarized Zone)* zóny. DMZ zóna je časť logickej podsiete, ktorá obsahuje a vystavuje služby pre externú komunikáciu na väčšie a nedôveryhodné siete, zvyčajne na internet.
- *WAF (Web Apllication Firewall)* aplikuje kolekciu pravidiel na HTTP prenos dát, konkrétne pokrýva bežné útoky ako XSS (cross-site scripting) a SQL injekcie. Vďaka tomuto firewallu je zabezpečená bezpečná infraštruktúra spoločnosti, v ktorej sa nachádza databázový a aplikačný server platformy.
- *Firewall medzi aplikačným serverom a vonkajšími organizáciami*, s ktorými zdieľa platforma incidenty, zabezpečuje filtrovanie komunikácie, obmedzené len na pravidlá bezpečných TAXII definovaných prenosov.

Pre vyváženie záťaže požiadavkov na RWSS sa stará *Load Balancer*, ktorý zvyšuje kapacitu a spoľahlivosť služby. Load balancer koná ako reverzný proxy server a distribuuje záťaž medzi ostatné RWSS servery.



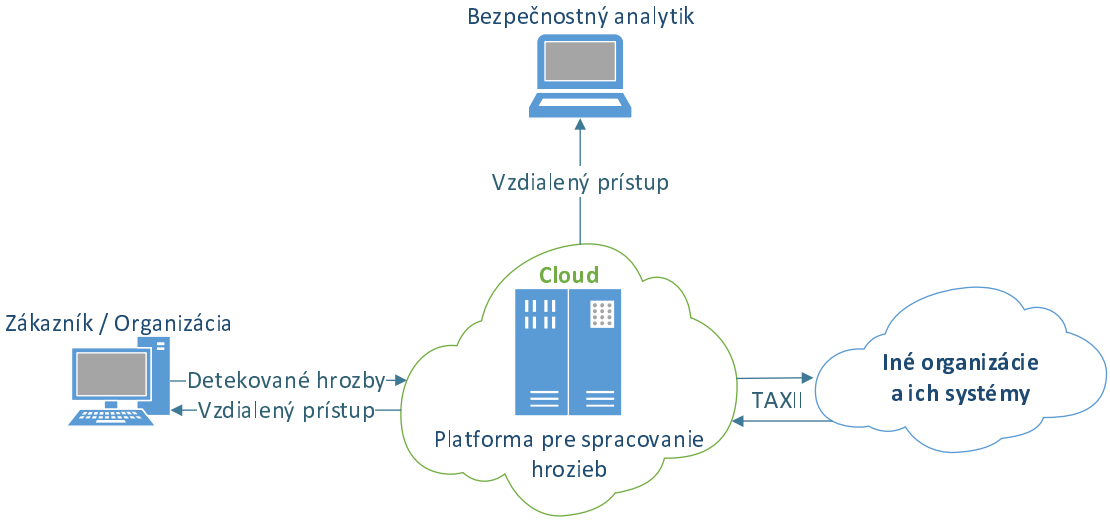
Obr. 3.1: Koncept riešenia platformy pre spracovanie hrozieb

3.3 Spôsoby prístupu ku konceptu

Na koncept riešenia platformy sa môžeme pozerať z viacerých hľadísk vzhľadom pre nasadenie a implementáciu výsledného systému.

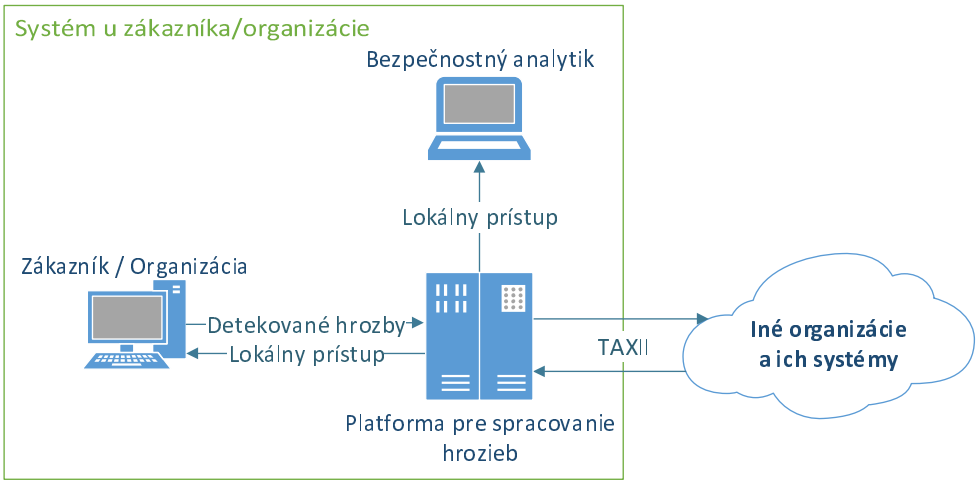
Prístup 1 (obrázok 3.2) definuje platformu pre spracovanie hrozieb ako službu, ktorá je nasadená na vzdialenom mieste (Cloud). Organizácia/zákazník odosiela detekované bezpečnostné incidenty na toto vzdialené miesto, na ktoré má webový prístup a nazhromaždené bezpečnostné incidenty môže spravovať (bezpečnostný analytik spracovávať a vyhodnocovať). Iné organizácie s podobným alebo rovnakým systémom môžu pomocou štandardu TAXII zdieľať informácie s týmto vzdialeným miestom. Výhodou tohoto prístupu je jed-

noduchšie nasadenie platformy pre organizácie/ zákazníkov, pretože systém môže bežať na serveroch spravovaných poskytovateľom platformy a zákazník dostane len vzdialený prístup.



Obr. 3.2: Prístup 1

Prístup 2 (obrázok 3.3) definuje platformu pre spracovanie hrozieb ako službu, ktorá je nasadená na serveroch zákazníka / organizácie. Zdieľanie bezpečnostných incidentov prebieha pomocou štandardu TAXII s partnerskými organizáciami a ich systémami. Výhodou tohoto modelu je, že organizácia a bezpečnostný analytik majú priamy prístup k platforme pre spracovanie hrozieb.



Obr. 3.3: Prístup 2

Kapitola 4

Návrh riešenia

Po analýze problémov, potrieb, funkcií konceptu platformy a existujúcich riešení implementácie štandardov sa táto kapitola venuje konkrétnemu riešeniu jednotlivých častí platformy.

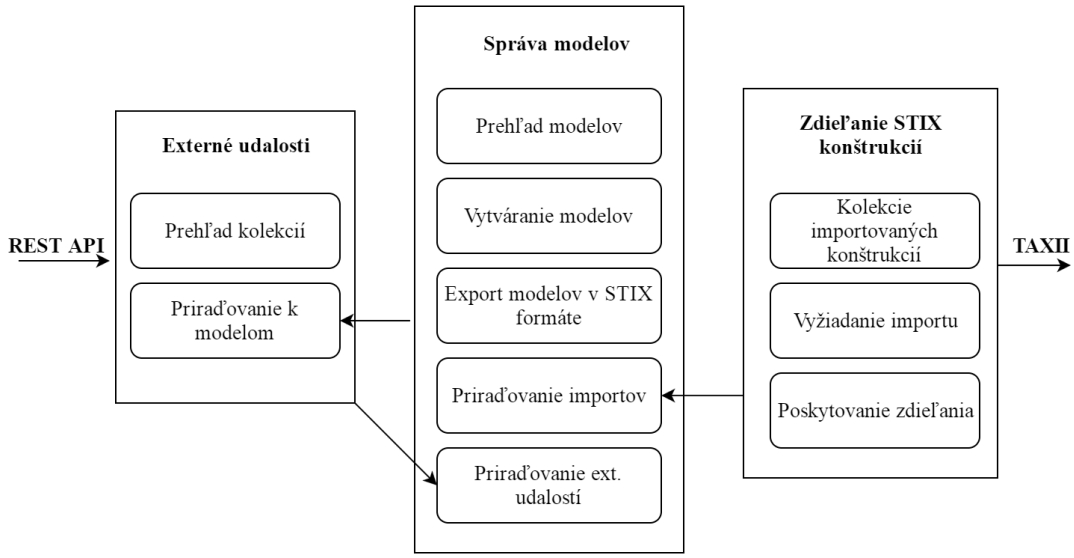
Platforma je naimplementovaná ako *JavaEE (verzia 8)* [15] webová aplikácia bežiaca s na serveri *Apache Tomcat (verzia 7.0.52)* [19] s využitím technológie *Java Server Faces JSF (verzia 2.2)* [13], ktorá separuje logiku webovej aplikácie od jej statických elementov a s využitím komponenty *PrimeFaces (verzia 6.0.RC2)* [23], ktorá slúži ako knižnica JSF grafických elementov kompatibilných s HTML5. Databázový server je postavený na technológií *MySql (verzia 14.14, distrib 5.5.49)* [14], ktorý poskytuje uchovávanie dátových modelov bezpečnostných incidentov a udalostí. Databázové tabuľky sú namapované (objektovo-relačné mapovanie) na Java objekty za pomoci frameworku *Hibernate (verzia 5.1.0 Final)* [16], čo zjednodušilo implementáciu o nutnosť vykonávať databázové dotazy pri každej zmene dát. Funkcionalitu RESTful web API služby pre zber externých udalostí poskytuje framework *Jersey (verzia 2.22.2)* [17].

Výber technológií pre implementáciu platformy vychádzal z potreby implementácie štandardov STIX a TAXII, pre ktoré existujú knižnice pre programovací jazyk Python a knižnice pre jazyk Java. Zvolená cesta Java implementácie je odôvodnená väčším rozšírením vývoja dynamických webových aplikácií práve v tomto jazyku.

Medzi ponúkané funkcie platformy patrí:

- Prehľad externých udalostí, ktoré boli zaslané na RESTful API platformy a ich priraďovanie STIX formátovaným modelom.
- Konštrukcia a editácia modelov STIX architektúry a exportovanie ich konštrukcie do formátu STIX XML.
- Import STIX formátovaných konštrukcií z iných platforiem podporujúcich TAXII výmenu informácií o bezpečnostných incidentoch.
- Zdieľanie vytvorených modelov pomocou služieb definovaných TAXII štandardom.
- Správa prístupu užívateľov platformy.

Ich znázornenie a vzájomné previazanie je možné vidieť na obrázku 4.1.



Obr. 4.1: Schéma poskytovanej funkcionality platformy.

Každý spomínaný prvok platformy je vysvetlený a popísaný v nasledujúcich podkapitolách, ktoré sú koncipované ako funkčné časti celku platformy.

4.1 Logický model nadväzovania STIX komponent

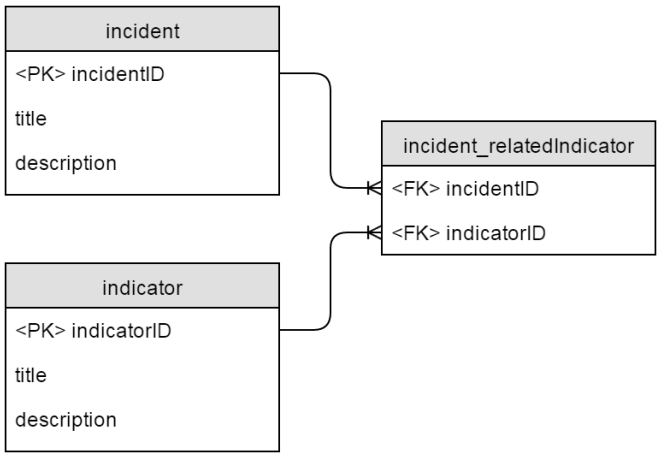
Platforma poskytuje pridávanie všetkých komponent STIX architektúry so základnými atribútmi, konkrétne titulom a popisom. Komponenty na seba voliteľne odkazujú podľa vzťahov architektúry. Nakoľko vzťahy medzi komponentami tvoria komplexný a vo výsledku robustný model analyzovanej udalosti, platforma túto skutočnosť využíva v nadväzovaní doposiaľ vytvorených komponent pre ich budúce zúžitkovanie pri analýze modelov. To znamená, že novo pridávané komponenty môžu využívať históriu komponentov pri tvorbe aktuálne modelovanej udalosti, ale aj reverzne, kde staré komponenty budú na seba naväzovať novo pridávané komponenty. Tento fakt vo výsledku vytvára rozsiahlejšie modely, ak analytik použil z histórie komponentu, ktorá mala rovnaký význam ako komponenta, ktorú chcel namodelovať.

4.2 Databázový model

Databázový model platformy zobrazený na obrázku 4.3 popisuje vzťahy jednotlivých tabuliek relačnej databázy (zobák predstavuje kardinalitu "N", inak kardinalita "1"). Model znázorňuje logiku previazania funkčných celkov a spôsob ich ukladania.

Chýbajúcu časť modelu tvoria tabuľky komponent STIXu, ktoré neboli pre ich komplexnosť v tejto práci vyobrazené. Tabuľky komponent obsahujú atribúty *identifikátor*, *titul* a *popis*. Vzťahy medzi týmito tabuľkami sú rovnako previazané ako vzťahy komponent v prílohe A.1 a ich kardinalita vzťahov je "N"ku "N", čo dopĺňa reálny model databázy o tabuľky

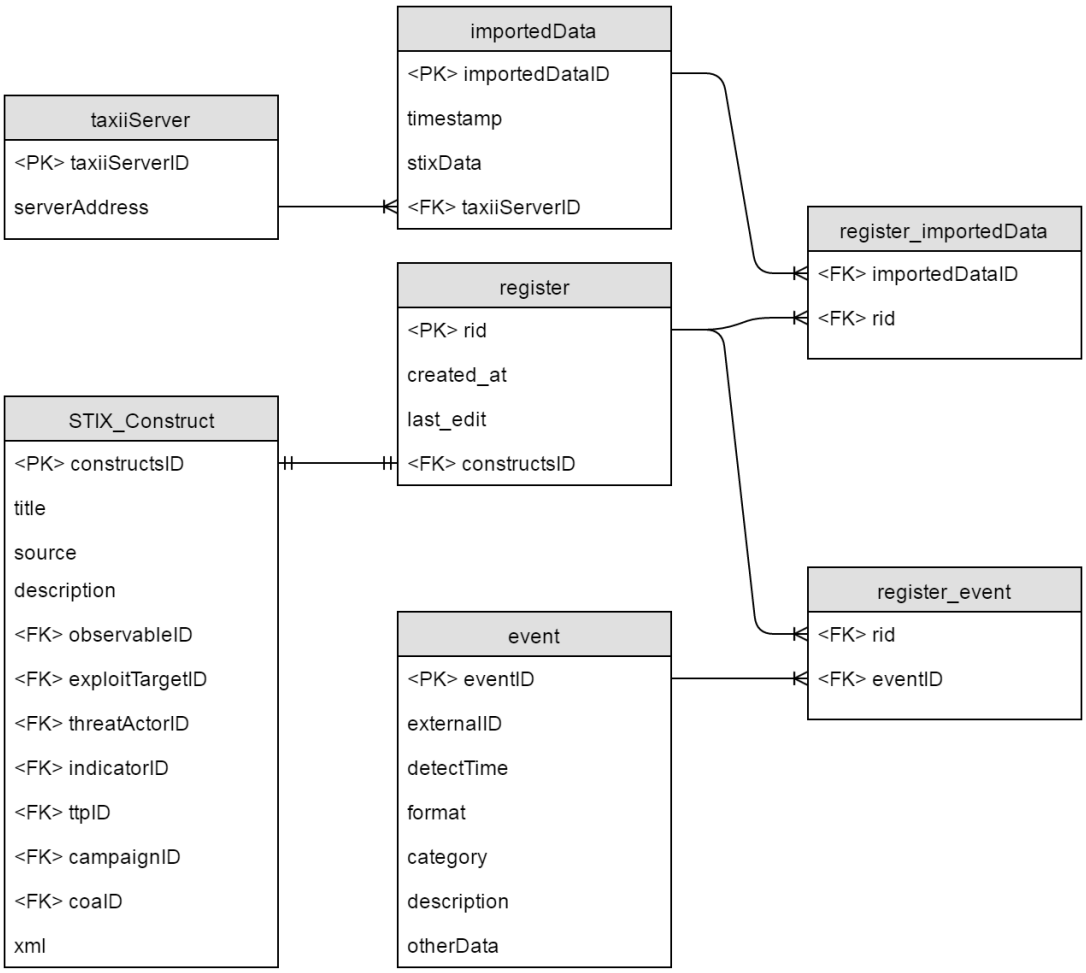
vzťahov s cudzími kľúčmi (príklad na obrázku 4.2).



Obr. 4.2: Príklad vzťahu dvoch STIX komponent databázového modelu.

Popis jednotlivých tabuliek databázového modelu:

- Tabuľka *event* uchováva dáta externých udalostí, ktoré boli poslané na restové API platformy. Medzi jej atribúty patria povinné prvky IDEA formátu a jeden atribút, ktorý uchováva kompletný IDEA formát externej udalosti.
- Tabuľka *taxiiServer* predstavuje adresy TAXII serverov, z ktorých boli doposiaľ importované STIX formátované udalosti.
- Tabuľka *importedData* uchováva všetky importované udalosti, ktoré sa ukladajú ako textové pole STIX formátovanej udalosti, časové razítko prevedeného importu a cudzí kľúč odkazujúci na tabuľku taxiiServer.
- Tabuľka *STIX_Construct* slúži pre uchovávanie dát STIX formátovanej konštrukcie, kde atribúty *title*, *source*, *description* predstavujú prvky hlavičky konštrukcie, *xml* uchováva XML formát konštrukcie a zvyšné atribúty predstavujú cudzie kľúče tabuliek jednotlivých komponent STIX architektúry.
- Tabuľka *register* predstavuje hlavnú tabuľku pre modelovanie STIX formátovaného incidentu. Uchováva informácie o priradených STIX konštrukciách. Dôvodom oddelenia od tabuľky STIX_Construct je ľahší prístup ku konštrukciám, pre prípad výmeny STIX udalostí za pomoci TAXII servera.
- Tabuľky *register_importedData* a *register_event* sú pomocné tabuľky pre uchovávanie informácií o priradených externých udalostiach k určitému STIX modelu a uchovávanie informácií o priradených importovaných dátach.



Obr. 4.3: Základ databázovového modelu platformy spracovania hrozieb.

4.3 Externé udalosti

Platforma vystavuje RESTful API, na ktoré môžu byť zasielané bezpečnostné udalosti vo formáte IDEA. Pre zaslanie udalosti, je nutné spolu s payloadom obsahujúcim IDEA formát zaslať v hlavičke autentikáciu užívateľa. Autentifikovanie prebieha v móde basic, ktorý funguje ako overenie zaslanej autentikácie reťazcom *meno:heslo* enkódovanom do formátu BASE64 [9]. Udalosti sú z IDEA formátu rozparsované a priamo uložené ako záznam v tabuľke databázy. V prípade zlej autentifikácie alebo konfliktu v databáze vráti API zdroju príslušný stavový kód.

Využitie prehľadu externých udalostí môže nahradiť analýzu udalostí v detekčných systémoch za analýzu udalostí priamo na platforme, čo umožní priame spracovanie výsledkov analýzy do štandardizovaného STIX formátu a v prípade potreby, jeho následné zdieľanie. Prehľad externých udalostí umožňuje priame priradenie udalosti k STIX modelom platformy.

4.4 Spracovanie a popis udalostí

Spracovanie udalostí na STIX model prebieha naviazaním vytvorených komponent v sekcií *STIX Construct Register* na nový záznam registru. O popis naviazaných komponent a vytvorenie STIX XML formátovaného balíku sa starajú obslužné funkcie, ktoré cyklicky prechádzajú vzájomne naviazané komponenty v dátovom modeli, popisujú ich dáta do štruktúr poskytujúcich knižnicou *java-stix* a tieto štruktúry vracajú funkcii, z ktorej boli volané. Takto vrátené štruktúry obsahujú stromovité usporiadanie dát naviazaných komponent a môžu byť v prípade validity vyexportované do textového reťazca, ktorý platforma uloží do databázy. Z databázy je možné za pomoci platformy tento reťazec získať ako súbor vo formáte XML, s ktorým môže užívateľ vykonávať ďalšie operácie (napr. vizualizácia/ editácia externými nástrojmi).

4.5 Výmena spracovaných udalostí

Pre výmenu spracovaných udalostí sú v platforeme implementované služby *discovery* a *poll* za pomoci popisu služieb poskytovaných knižnicou *java-taxii*. Tieto služby sú využité pri TAXII modeli zdieľania *peer-to-peer* s vyžiadaním exportu nových dát od určitého dátového razítka.

Pre vyžiadanie importu dát poskytuje platforma možnosť *TAXII import*. Ten je zabezpečený implementáciou TAXII klienta platformy za pomoci popisu služieb pre vyžiadanie dát, taktiež poskytujúcich knižnicou *java-taxii*. Klient vyžiada dáta zo zadaného serveru, ktoré ešte nemá uložené vo svojej lokálnej databáze importovaných udalostí. Zabráneniu duplicity uložených/vyžiadaných dát sa overuje na základe časového razítka záznamu každej spracovanej STIX udalosti.

Importované dáta môžu v budúcnosti napomôcť k riešeniu nových udalostí, k spätnej analýze dát a vyhodnotením doplňujúcich informácií STIX modelov platformy (napríklad vyhodnotenie rozsiahlej kampane útočníka), nakoľko importované dáta môžu byť k týmto modelom spätne pridružené.

Kapitola 5

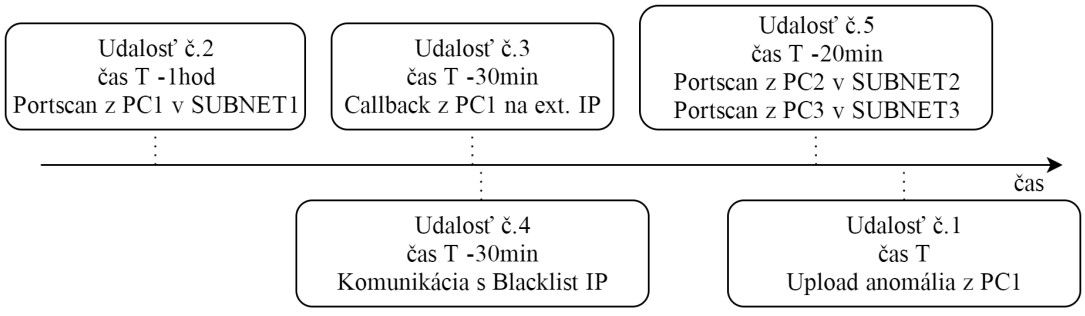
Výsledky a zhodnotenie práce

5.1 Testovanie

Platforma bola testovaná pri analyzovaní a popisovaní niekoľkých modeloch prípadov bezpečnostných incidentov. Východzie externé udalosti pre analýzu boli namodelované aby pokryli väčšinu komponent a vzťahov architektúry STIXu. Výsledné STIX formátované XML súbory platformy, popisujúce zostavené situácie boli externe overené nástrojom *stix-validator* [4] pre účel zistenia validity ich zostavenia.

5.1.1 Model 1 - cielený útok

Scenár modelu cieleného útoku je nasledovný: v detekčnom systéme, ktorý vykonáva analýzu sieťového toku v lokálnej banke, bola detekovaná *udalosť č.1* anomália - upload veľkého množstva dát z PC1 na neznámu zahraničnú IP adresu v čase T, na ktorú upozornil systém bezpečnostného analytika. Analytik po prezretí histórie udalostí v systéme uvidel niekoľko záznamov, ktoré by mohli byť s uploadom dát pridružené: *udalosť č.2* portscaning[1] z PC_1 na SUBNET_1 v čase T mínus 1hod, *udalosť č.3* callback z PC_1 na externú IP adresu v čase T mínus 30min, *udalosť č.4* komunikácia s blacklistovou IP adresou v čase T mínus 30min a *udalosť č.5* niekoľko rovnakých portscanov z rôznych počítačov v rôznych podsieťach v časovom rámci T až T mínus 20min. Pre lepšie znázornenie je možné na obrázku 5.1 vidieť zaznamenané udalosti usporiadané v čase. Všetky udalosti boli následne exportované do navrhnutej platformy spracovania bezpečnostných incidentov.



Obr. 5.1: Časová os zachytenia externých udalostí pre model - cielený útok.

[1] Hlavným cieľom port scanningu je zistiť, ktoré porty ciela sú dostupné, nedostupné a filtrované. [1]

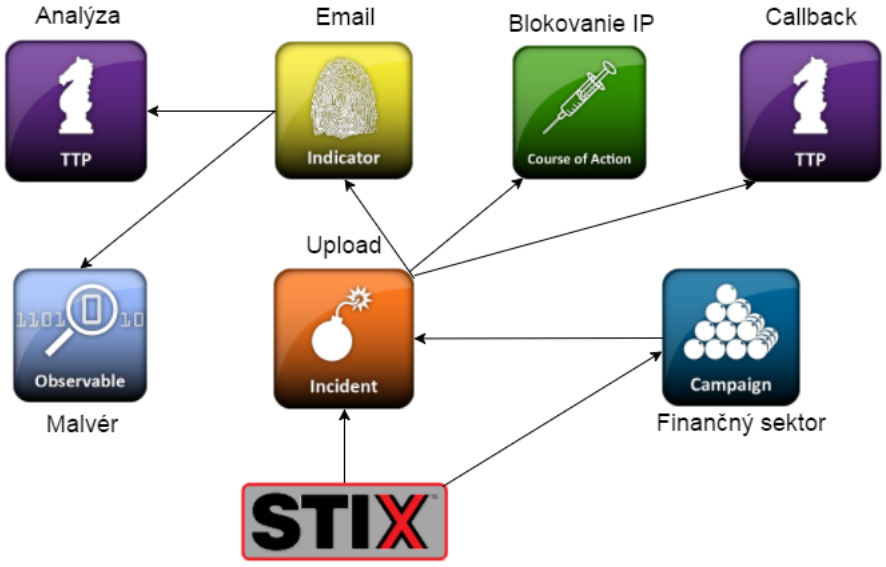
Vytvorenie modelu (5.2) v platforme začína pridaním nového *STIX Construct Register*, ku ktorému analytik priradí udalosti č.1-5, ktoré nájde v sekcie *External events*. Ako východziu komponentu STIX balíku je možné jednoznačne určiť *Incident* s popisom detekovanej udalosti č.1 (anomália - upload dát z PC_1 na externú IP adresu v čase T).

Vyhodnotením udalostí č.2, č.3 a č.4 bola zistená *TTP*, ktorá vykonáva portscan siete s následným odoslaním získaných dát na zahraničnú IP adresu (callback) a ďalšou prebiehajúcou komunikáciou. Táto TTP je priradená ako *LaveragedTTP*, predchádzajúca detekovanému incidentu.

Pri ďalšom skúmaní sa analytik snaží prísť na príčinu tohoto incidentu. Po komunikácií s používateľom PC_1, ohľadom jeho práce počas časového rámca T až T mínus jeden deň, analytik zistil, že používateľ obdržal reklamný email (ponuka motoriek) s infikovanou prílohou, ktorá bola otvorená, čo bolo príčinou inštalácie malvéru do PC_1. Nakoľko používateľ pred T mínus 30 dní vyhľadával na internete z PC_1 ponuky motoriek na predaj, analytik vyhlási tento fakt ako analýzu neznámeho útočníka s cieľom potencionálneho útoku. Získanými informáciami možno rozšíriť model o komponentu *Indicator* (emailová správa), ktorú priradíme ako *RelatedIndicator* existujúceho incidentu, o komponentu *Observable* (malvérová príloha), ktorú priradíme k vytvorenému indikátoru a o komponentu *TTP* (analýza), ktorú priradíme ako *IndicatedTTP* indikátora.

Ako posledná nám zostala udalosť č.5, ktorá naznačuje šírenie malvéru po lokálnej sieti banky. Tento fakt analytik pridá do popisu existujúcej TTP (callback). Keďže malvéru nevie analytik v prípustnej dobe zabrániť, ako *Course od Action* navrhne dočasné blokovanie komunikácie so zahraničnými IP adresami, aby významne neobmedzil činnosť a poskytované služby lokálnej banky a zároveň eliminoval činnosť malvéru pri kradnutí dát s potenciálne citlivými údajmi. Navrhnutú COA analytik priradí do modelu ako *RequestedCOA* incidentu.

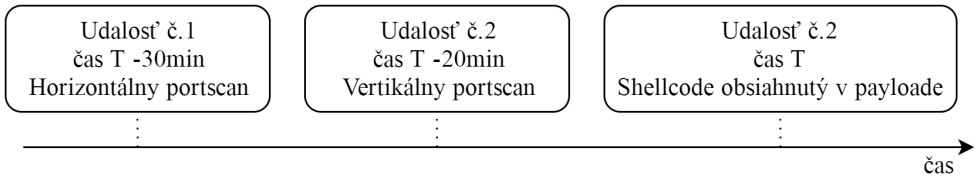
Pri importe nových STIX incidentov z iných platforiem za pomoci funkcie platformy *TAXII import*, analytik narazil na podobný model incidentu s rovnakým zameraním a použitými TTP. Tento poznatok pridal do zostavovaného modelu ako komponentu *Campaign* so zameraním na finančný sektor a odkazom na importovaný STIX incident.



Obr. 5.2: Schéma STIX modelu - cielený útok.

5.1.2 Model 2 - využitia zraniteľnosti serveru

Scenár pre zostavenie modelu využitia zraniteľnosti serveru je následovný: v organizácií pre poskytovanie webových služieb neznámy útočník vymazal diskové polia niekoľkých serverov v čase T. Pri skúmaní zaznamenaných udalostí detekčného systému, ktorý vykonáva analýzu sieťového toku, analytik sústredil svoju pozornosť na sled záznamov ktoré predchádzali tomuto bezpečnostnému incidentu. Konkrétne *udalosť č.1* horizontálny scan[2] z externej IP na webovú službu v čase T mínus 120 min., *udalosť č.2* vertikálny scan[3] z externej IP na IP webového serveru v čase T mínus 110 min., *udalosť č.3* detekované zaslanie payloadu[4] so shellcodom[5] z externej IP na IP serveru v čase T mínus 90min. Pre lepšie znázornenie je možné na obrázku 5.1 vidieť zaznamenané udalosti usporiadané v čase. Všetky udalosti boli následne exportované do navrhnutej platformy spracovania bezpečnostných incidentov.



Obr. 5.3: Časová os zachytenia externých udalostí pre model - cielený útok.

Vytvorenie modelu (5.4) v platforme začína pridaním nového *STIX Construct Register*, ku ktorému analytik priradí udalosti č.1-3, ktoré nájde v sekcie *External events*. Ako východziu komponentu STIX balíku je možné jednoznačne určiť *Incident* s popisom vykonaného shellcodu (vymazanie diskových polí) a *ThreatActor* útočníka na základe zdrojovej IP adresy incidentu č.3.

Vyhodnotením udalostí č.1-2, bola zistená *TTP*, ktorá vykonáva portscan služieb za účelom nájdenia zraniteľností. Na základe analýzy payloadu (nový *Indicator*) z udalosti č.3, bola odhalená zraniteľnosť [22] *buffer overflow*[6] na bežiacej službe Apache verzie 2.4.0, ktorá umožnila útočníkovi vykonať škodlivý shellcode. Informácie získané analýzou sú namodelované ako priradenie indikátora (payload) vo vzťahu *RelatedIndicator* k existujúcemu incidentu (shellcode). Indikátoru je následne priradený TTP (portscan) ako vzťah *IndicatedTTP* a útočníkovi je priradený vo vzťahu *ObservedTTP*. Zraniteľnosť (buffer overflow) je namodelovaná ako komponenta *ExploitTarget* vo vzťahu k existujúcemu TTP.

Analytik aplikoval ako ošetrenie zraniteľnosti upgrade služby Apache na najnovšiu verziu, ktorá má túto zraniteľnosť opravenú a následne túto akciu namodeloval ako komponentu *Course of Action* so vzťahom *PotentialCOA* k existujúcemu ExploitTargetu.

[2]Horizontálny scan sa zameriava na rovnaký port naprieč viacerými cieľmi. [1]
[3]Vertikálny scan sa zameriava na skenovanie viacero portov na jednom cieli.[1]
[4]Payload je časť prenášaných dát, kvôli ktorým sa prenos dát uskutočňuje.
[5]Shellcode je malý kúsok kódu, ktorý je obsiahnutý v payloade pri exploitácií softvérovej zraniteľnosti.[10]
[6]Buffer overflow je anomália, kde program počas zapisovaní dát do vyrovnávacej pamäti (tzv. bufferu) prekročí vymedzené hranice a prepíše susediaci úsek operačnej pamäti.

Obr. 5.4: Schéma STIX modelu - využitie zraniteľnosti servera

5.2 Rozšírenia do budúcnosti

Nakoľko platforma poskytuje iba základné a nie kompletné využitie potenciálu štandardov STIX, TAXII, CybOX a IDEA, navrhoval by som do budúcna implementovať následujúce rozšírenia:

- Podpora kompletného dátového modelu každého elementu STIX architektúry.
- Implementácia zvyšných služieb TAXII štandardu. Konkrétne *Collection management* a *Inbox*.
- Možnosť výberu TAXII modelu výmeny informácií.
- Poskytnutie možnosti vizualizácia výsledného STIX dokumentu pomocou nástroja *StixViz* a *stix-to-html*.
- Rozparsovanie importovaných STIX formátovaných udalostí na dátové prvky poskytované databázovým modelom platformy a ich následné začlenenie.
- Pokročilejšia autentifikácia užívateľov pri zasielaní externých udalostí na RESTful API.
- Úprava užívateľského rozhrania platformy s využitím viac preemptívnych a intuitívnych prvkov, ako napríklad užívateľská navigácia v slede krokov spracovania externých udalostí za účelom vytvorenia a spracovania nového modelu bezpečnostného incidentu.

Platforma bola navrhované ako ľahko rozšíriteľný celok a implementácia rozšírení po ich hlbšej analýze by nemala byť zásadnou prekážkou.

Kapitola 6

Záver

Cieľom bakalárskej práce bolo navrhnúť a vytvoriť platformu pre spracovanie bezpečnostných hrozieb, incidentov a útokov s využitím štandardov STIX, TAXII, CybOX a IDEA, ktoré predstavujú efektívny prostriedok pri spracovaní, analýze a automatizácií zdieľania bezpečnostných informácií.

Výsledná platforma sa ukázala pri modelovaní niekoľkých prípadov bezpečnostných incidentov ako schopný nástroj, uľahčujúci popis udalostí do štandardizovaného formátu a ich následnú automatizovanú výmenu. Výsledok práce by pravdepodobne nebolo možné nasadiť do praktickej prevádzky, nakoľko popis udalostí je vykonaný s málo doplňujúcimi informáciami, čo by mohol byť nedostatočný faktor pre využitie v oblasti počítačovej bezpečnosti. Po implementácií navrhovaných rozšírení by však mohla byt platforma prakticky využiteľná.

Literatúra

[1] Ahanger, T. A.: Port Scan - A Security Concern. *International Journal of Engineering and Innovative Technology (IJEIT)*, ročník 3, č. 10, Apríl 2014, ISSN: 2277-3754.

[2] Back, G.; Bake, J.: java-taxii. GitHub repository. [online], 2016 [cit. 19.4.2016].
URL https://github.com/TAXIIProject/java-taxii

[3] Back, G.; Wunder, J.: java-stix. GitHub repository .[online], 2016 [cit. 20.4.2016].
URL https://github.com/STIXProject/java-stix

[4] Back, G.; Wunder, J.: STIX Document Validator. stix-validator, GitHub repository .[online], 2016, [cit. 22.4.2016].
URL https://github.com/STIXProject/stix-validator

[5] Barnum, S.: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™). [online], 2014-02-20, version 1.1, Revision 1, [cit. 10.4.2016].
URL
http://stixproject.github.io/getting-started/whitepaper/#architecture

[6] Connolly, J.; Davidson, M.; Schmidt, C.: The Trusted Automated eXchange of Indicator Information (TAXII™). [online], 2014-05-02, the MITRE Corporation, [cit. 18.4.2016].
URL http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_May_2014.pdf

[7] Intrusion Detection Extensible Alert (IDEA). [online], 2016, corporation CESNET, z. s. p. o, [cit. 1.5.2016].
URL https://idea.cesnet.cz/en/index

[8] Ecma International: *The JSON Data Interchange Format*. Október 2013, standard ECMA-404.
URL http:
//www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf

[9] IETF: The Base16,Base32,and Base64 Data Encodings. [online], Október 2006. RFC 4648, [cit. 10.5.2016].
URL https://tools.ietf.org/html/rfc4648

[10] Mason, J.; Small, S.; Monrose, F.; aj.: English Shellcode. [online], November 2009, [cit. 10.5.2016].
URL http://web.cs.jhu.edu/~sam/ccs243-mason.pdf

[11] The MITRE Corporation: *libtaxii 1.1.110.dev0 Documentation*. První vydání, [online], 2014 [cit. 16.3.2016].
URL http://libtaxii.readthedocs.org/en/latest/

[12] The MITRE Corporation: *python-stix 1.2.0.1.dev2 Documentation*. První vydání, [online], 2014 [cit. 19.4.2016].
URL http://libtaxii.readthedocs.org/en/latest/

[13] Oracle: JavaServer Faces Technology. [online], 2016, [cit. 8.5.2016].
URL http://www.oracle.com/technetwork/java/javaee/javaserverfaces-139869.html

[14] Oracle: MySQL 5.5 Reference Manual. [online], 2016, [cit. 29.4.2016].
URL http://dev.mysql.com/doc/refman/5.5/en/

[15] Oracle: Introduction to Java Platform Enterprise Edition 7. [online], Jún 2013, [cit. 11.5.2016].
URL http://www.oracle.com/technetwork/java/javaee/javaee7-whitepaper-1956203.pdf

[16] Red Hat, Inc.: Hibernate JavaDoc (5.1.0.Final). [online], 2016, [cit. 10.5.2016].
URL http://docs.jboss.org/hibernate/orm/5.1/javadocs/

[17] Red Hat, Inc.: Jersey 2.22.2 API Documentation. [online], 2016, [cit. 1.5.2016].
URL https://jersey.java.net/apidocs/latest/jersey/index.html

[18] The TAXII Team: *yeti Documentation*. Revision 1d948cda, [online], 2014 [cit. 19.4.2016].
URL http://yeti.readthedocs.org/en/latest/

[19] Apache Tomcat 7 Documentation. [online], April 2016, Version 7.0.69, The Apache Software Foundation, [cit. 11.5.2016].
URL http://tomcat.apache.org/tomcat-7.0-doc/index.html

[20] The MITRE Corporation: CybOX Object Listing. [online], máj 2016 [cit. 15.4.2016].
URL http://cyboxproject.github.io/documentation/objects/

[21] Threat-Intelligence-Sharing-using-STIX-and-TAXII. [online], máj 2014, organization HS SEDI, Homeland Security Systems Engineering and Development Institute, [cit. 12.3.2016].
URL http://secure360.org/wp-content/uploads/2014/05/Threat-Intelligence-Sharing-using-STIX-and-TAXII.pdf

[22] US-CERT/NIST: Vulnerability Summary for CVE-2014-0226, National Cyber Awareness System. [online], 2015-14-04, [cit. 5.5.2016].
URL https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0226

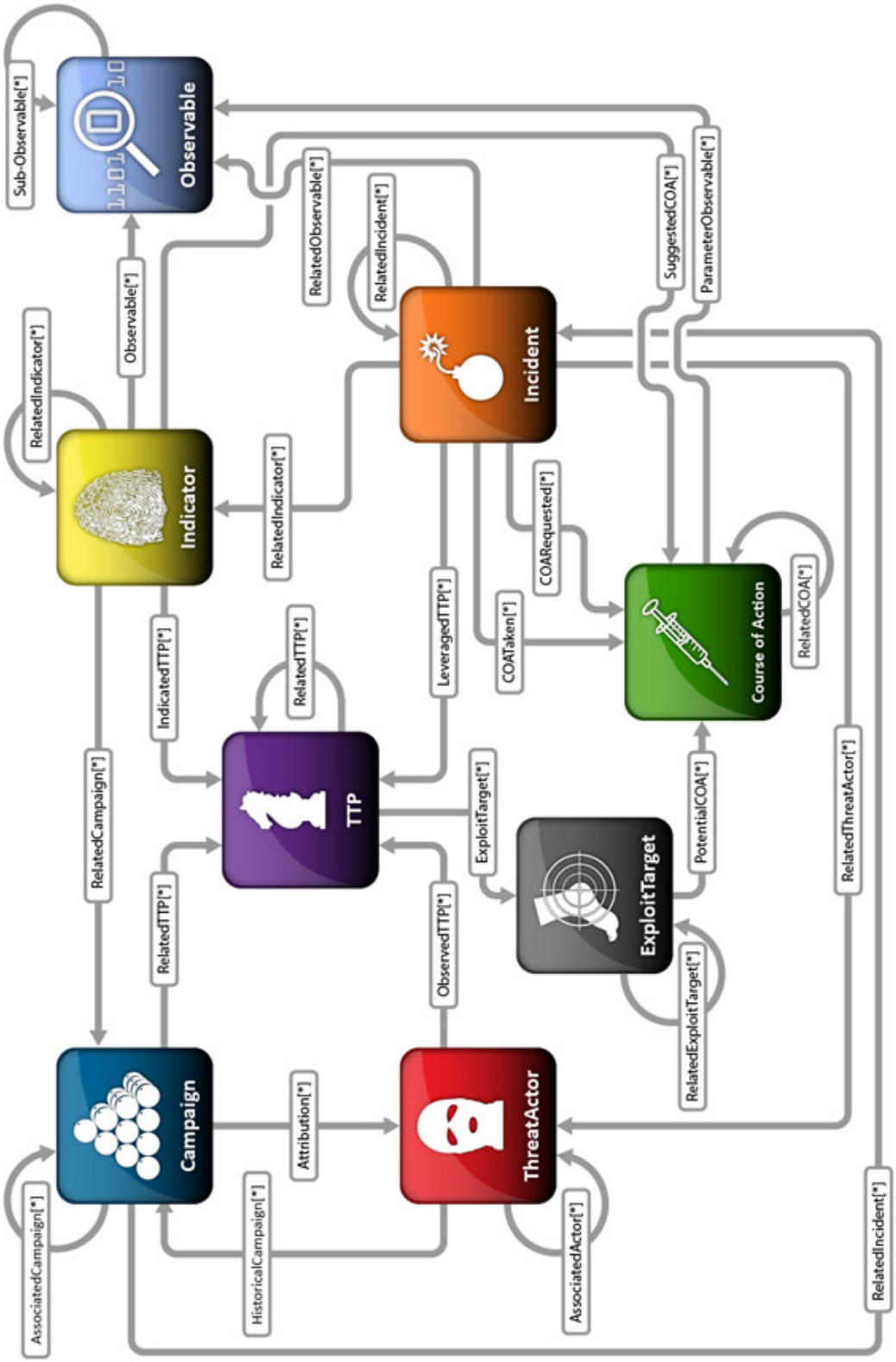
[23] Çağatay Çivici: PrimeFaces User guide v5.3. [online], October 2006, [cit. 22.4.2016].
URL http://www.primefaces.org/docs/guide/primefaces_user_guide_5_3.pdf

Prílohy

Zoznam príloh

Príloha A

Obrazové prílohy



Obr. A.1: Architektúra STIXu, prevzaté z [5]