BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2019
http://excel.fit.vutbr.cz

Konverze záznamů kybernetických incidentů

Pavel Eis*

Abstrakt
Existuje celá řada platforem a systémů určených ke sdílení kybernetických bezpečnostních incidentů a událostí, které často používají rozdílné bezpečnostní formáty. Tímto způsobem dochází ke ztížení nebo přímo nemožnosti sdílení bezpečnostních incidentů a událostí mezi organizacemi, které využívají rozdílné platformy. Řešením tohoto problému může být vznik konvertorů, které jsou schopné převádět používané bezpečnostní formáty mezi sebou. Tato práce se zabývá převodem mezi bezpečnostními formáty IDEA, MISP a STIX. Při konverzi je důležité dbát na postup, aby nedošlo ke ztrátě informací, nebo aby při chybném převodu nevznikl jiný druh události, než byl reprezentován původní událostí. Pokud je převod dostatečně přesný, může být jednodušeji dosaženo přesnější a širší analýzy kybernetických bezpečnostních incidentů.

Klíčová slova: bezpečnostní incident — reprezentace bezpečnostních incidentů — konverze bezpečnostních formátů — platformní konektory

Přiložené materiály: Ukázka kybernetických incidentů v podporovaných formátech

*xeispa00@stud.fit.vutbr.cz, *Fakulta informačních technologií, Vysoké učení technické v Brně*

1. Úvod

Bezpečnostní události jsou na počítačové síti administrátora detekovány několikrát denně (např. skenování portů a pokusy o zneužití zranitelností systému). Pokud se ale na síti administrátora objeví komplexní bezpečnostní událost, může být těžké ji správně zpracovat kvůli nedostatku informací a detailů, které by pomohly správci vyřešit daný problém. Tuto problematiku pomáhají řešit pokročilé sdílecí platformy a systémy. Navíc mnoho těchto sdílecích platforem zavádí i automatizovanou analýzu událostí, která ulehčí manuální analýzu prováděnou správci. Ovšem pokud chtějí dvě organizace sdílet události mezi sebou, není to vždy tak jednoduché, obzvláště pokud každá používá jiný bezpečnostní formát pro reprezentaci událostí. Jedním z možných řešení je vytvořit konvertor, který umožní konvertovat používané bezpečnostní formáty mezi sebou a pomůže sdílená data efektivněji využívat. Některým sdílecím platformám se v posledních letech dostává velké pozornosti od velkých i menších organizací a možnost propojení těchto platforem pomocí konvertoru může mít mnohdy i mezinárodní dopad.

Některé platformy se pokoušejí implementovat vlastní konvertory, např sdílecí platforma MISP [1] umožňuje konverzi kybernetických událostí do vlast-

ního MISP core formátu [2] (dále odkazován pouze jako MISP formát), ale také do formátu STIX [3] verze 1 i 2. Výsledek této konverze je užitečný a pro účely konverze byly navrhnuty vlastní STIX objekty. Formát STIX takové rozšíření umožňuje a díky této úpravě mohou být převedeny skoro všechny informace ze vstupní MISP události. Převod maximálního množství hodnot ze vstupní události je ve finále jednou z klíčových vlastností správně navrženého konvertoru (pokud jsou hodnoty převedeny korektně). Zatím ale neexistuje konvertor, který by umožňoval konverzi mezi formátem IDEA [4] a MISP a ani konverzi mezi formátem IDEA a formátem STIX. Formát IDEA je vyvíjen a používán sdružením Cesnet. Na vývoji platformy MISP se značně podílela organizace NATO a formát STIX je pod správou konsorcia OASIS[1].

Přínosem této práce je analýza a návrh konverze mezi formáty IDEA, MISP a proprietární verzí formátu STIX platformy C3ISP[2]. Výstupem práce jsou dva konvertory (konverzní knihovny). První konvertor umí konvertovat bezpečnostní formát IDEA do formátu MISP a naopak. Druhý bude umět konvertovat bezpečnostní formát STIX 2.0 do formátu IDEA, oboustranná konverze bude rovněž umožněna. Následně vzniknou konektory, které realizují propojení s platformami a automatickou konverzi nově vzniklých událostí z jednoho bezpečnostního formátu do druhého s využitím konverzních knihoven. Je důležité, aby bylo při převodu zachováno co největší množství původních informací (některé informace mohou být nekompatibilní mezi formáty) včetně jejich původního významu. Dalším kritériem konverze je dodržet sémantiku polí (atributů) formátu.

2. Analýza konvertovaných formátů

Formát STIX byl vytvořen pro přenos strukturovaných informací o kybernetických incidentech. Při vývoji tohoto formátu byl kladen důraz na komplexitu formátu, která umožňuje důkladně popsat kybernetický incident se všemi detaily, které přidají automatizované nástroje, ale i správci samotní (převzato z [3]). Platforma C3ISP využívá komplexity formátu STIX a obaluje tímto formátem vlastní detekované události exportované v bezpečnostním formátu CEF [5]. Formát CEF je minimalistický formát a hodí se pro popis např. síťových informací, které definují průběh incidentu. Události formátu CEF jsou poté obaleny formátem STIX, který nabízí objekty pro důkladnější popis a analýzu incidentu.

Výpis 1. Ukázka bezpečnostní události formátu CEF uvnitř proprietární verze formátu STIX platformy C3ISP

```
CEF:0|Security|Log_Analyzer|1.0|100|
ssh-2018-12-03T10:30:54.000+0100|5|
src=192.168.0.1 app=ssh2 user=root
type=0 reason=bad_password
outcome=failure date=1543828854000
dtz=Europe/Rome
```

Některé události platformy C3ISP ve formátu CEF obsahují kategorii události uvnitř atributu *cat* (např. *cat=Trojan*) v tzv. rozšíření události (část události za posledním oddělovačem 'l'). V ukázce CEF události (Výpis 1) si lze ale všimnout, že některé druhy událostí mohou být odlišeny různými způsoby. V tomto případě napoví proprietární dokumentace platformy C3ISP. Jedná se o neúspěšný útok hrubou silou hádáním hesla uživatele.

Formát MISP byl vytvořen jako nosný formát pro platformu MISP. Jejím hlavním cílem je umožnit sdílet data IT komunitám veřejných nebo privátních sektorů. Sdílená data jsou z různých domén, mezi které patří kybernetická bezpečnost (incidenty), finanční sektory a mnohé další (převzato z [1]). Hlavním nosičem informací jsou tzv. MISP atributy a MISP objekty. Samotné MISP atributy mezi sebou neudržují žádný vztah. Někdy je ale vhodné seskupit více atributů k sobě (např. skupina IP adres naznačuje, že patří do jedné organizace). Pro tento účel byly zavedeny tzv. MISP objekty[3] (např. MISP objekt *Netflow*) seskupující více MISP atributů k sobě (např. několik IP adres). Kategorie MISP událostí je určena pomocí tzv. taxonomií[4] neboli tagů. Každý tag je složen z posloupnosti dvou až tří klíčů (jmenný prostor, predikát, hodnota), které pomáhají k bližšímu určení druhu události. Příkladem může být tag *europol-incident:malware="distribution"*.

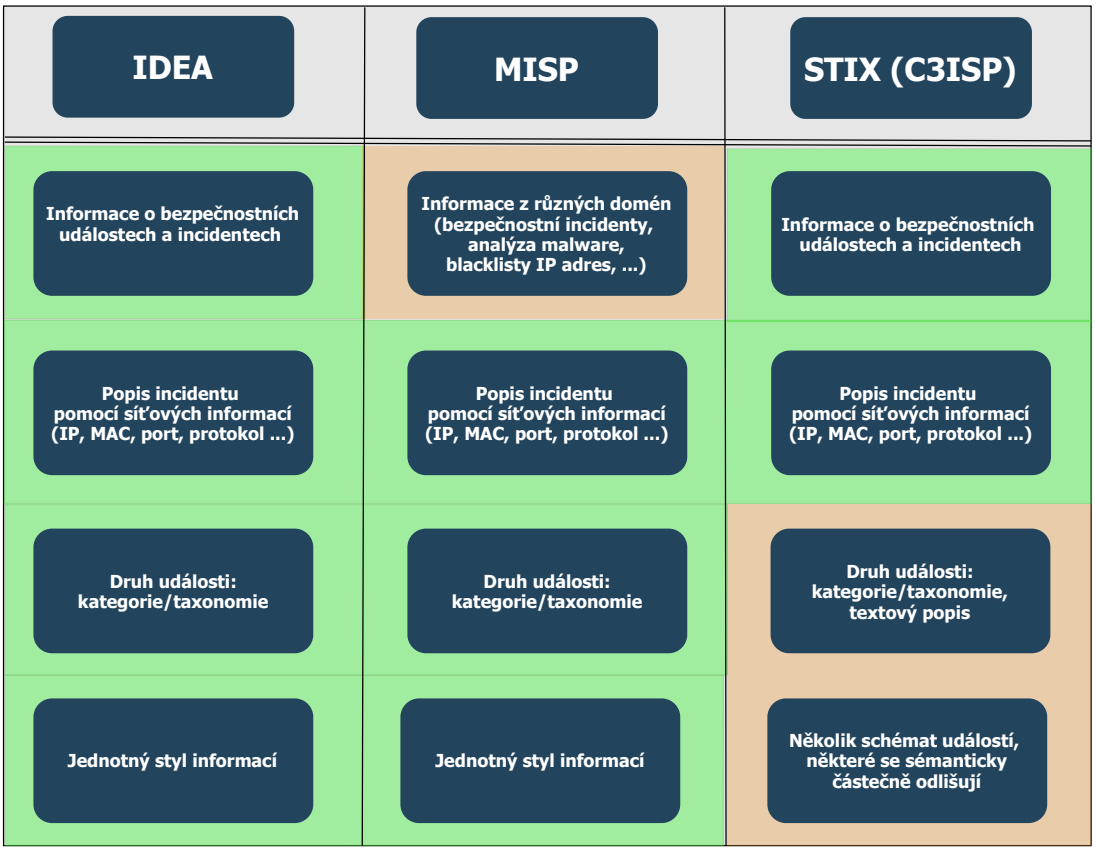
Formát IDEA byl vytvořen pro přenos informací automatických detekčních systémů, často nazývaných IDS (Intrusion Detection System). Vzhledem k tomuto hlavnímu účelu formátu byly navrhnuty požadavky na strukturu formátu IDEA. Důležitým požadavkem formátu byla jeho jednoduchost, protože komplexnost formátů často přináší dvojznačnost, která není žádoucí při automatickém zpracování velkého množství událostí, které je generováno systémy IDS. Bezpečnostní zprávy formátu IDEA jsou také generovány velmi blízko samotným detekčním zařízením, které mohou být umístěny na platformách s omezeným

[1] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

[2] https://c3isp.eu/

[3] https://www.misp-project.org/objects.html

[4] https://www.misp-project.org/taxonomies.html



Obrázek 1. Základní vlastnosti konvertovaných formátů (zelené podbarvení daného řádku značí stejné vlastnosti, oranžové podbarvení řádku značí pouze podobné vlastnosti)

výkonem a proto je důležitá nezavislost na pokročilých knihovnách a nástrojích, které mouhou vyžadovat vysoký výkon (převzato z [4]). Právě kvůli těmto požadavkům byl vytvořen vlastní formát a nebyl použit již existující, např. komplexnější formát. Sdílení dat s formátem STIX nebo MISP je pouze malá část infrastruktury, kterou jednodušuje upraví konvertor formátů. Ostatní části infrastruktury pracují efektivněji s využitím formátu IDEA.

Pro kategorizaci událostí slouží atribut *Category*, který obsahuje pole kategorií události [6] (např. [*Malware.Trojan*]). Většina informací formátu IDEA je k nalezení uvnitř objektů *Source* a *Target*. Tyto objekty přenáší síťové informace o zdrojích a obětích incidentu. Mezi tyto informace patří výčet IP adres, portů, použitých protokolů atd. Dodatečné informace a přílohy jsou k nalezení uvnitř objektů *Attach*.

Všechny tyto formáty používají pro popis incidentu především síťové informace. Některé formáty nabízejí i jiné, dodatečné informace, které ale nemusí být vždy kompatibilní s ostatními formáty. Některými vlastnostmi se ale formáty také liší (základní shrnutí viz Obrázek 1) a tyto problémy je nutné detekovat v první fázi vývoje a navrhnout jejich správné řešení. Tato část zabere nejvíce času, ale zároveň je nejdůležitější částí analýzy konverze.

3. Návrh konverze formátů

Formát IDEA přenáší 3 důležité druhy informací. Druh incidentu (kategorie), čas detekce a informace o průběhu kybernetického incidentu popsané síťovými informacemi. Následující část textu je zaměřena především na návrh konverze těchto částí incidentů.

Při vývoji konvertoru mezi formáty IDEA a MISP byl umožněn přístup k reálně využívané instanci MISP platformy, kterou provozuje centrum CIRCL (The Computer Incident Response Center Luxembourg). Až po detailním průzkumu instance byly nalezeny i události, které svým obsahem a myšlenkou korespondovaly k běžnému obsahu událostí formátu IDEA. Při konverzi událostí formátu MISP do formátu IDEA je tedy konvertována pouze předem definováná část událostí. Základem filtrace užitečných událostí je volba vhodných tagů, kterými když jsou události označeny, budou konvertovány. Po analýze dostupných taxonomií jsou vybrány ty, kterými jsou označované požadované události, nebo které podle svého popisu slouží tomuto účelu.

Díky vzniklému filtračnímu listu tagů se podařilo odstranit značnou část událostí, které nejsou relevantní. Nicméně některé zbývající události jsou nejednoznačné. Např. událost označena tagem *circl:incident-classification="malware"* může označovat udá-

lost generovanou systémem IDS, kdy došlo k přenosu škodlivého malware, nebo může jít pouze o analýzu daného malware, který byl detekován při nějakém incidentu. Pod jedním tagem se tak mohou skrývat dva odlišné koncepty událostí, kdy jeden z nich by neměl být konvertován. Proto bylo provedeno i několik dalších heuristik, které zlepšovali poměr správně vyfiltrovaných událostí. Nicméně stále nepřinášely uspokojivé výsledky.

Na základě konzultací s vývojáři MISP platformy bylo doporučeno, vzhledem k danému problému filtrace, vytvořit si vlastní list taxonomií (jmenný prostor), který by byl kopií 1:1 kategorií využívaných formátem IDEA a byl následně využíván pro označování takových událostí. Velmi podobné taxonomie jsou už ale definovány a formát IDEA z nich dokonce vychází. Těmito taxonomiemi jsou jmenné prostory ECSIRT a RSIT. Po bližší analýze těchto dvou jmenných prostorů vyplývá, že pokud je MISP událost označena takovýmto tagem, jedná se téměř vždy o událost generovanou systémem IDS. Pokud je tedy MISP událost označena alespoň jedním tagem pocházejícím z těchto jmenných prostorů, dojde ke konverzi. Kategorie převáděných událostí formátu IDEA jsou konvertovány také do těchto jmenných prostorů, jelikož jejich predikáty (druhé klíčové slovo taxonomie) jsou skoro totožné s kategoriemi formátu IDEA. Při konverzi formátu IDEA do formátu MISP jsou kategorie konvertovány do taxonomií stejných dvou jmenných prostorů (RSIT a ECSIRT), jelikož jsou jejich hodnoty dobře mapovatelné na kategorie formátu IDEA.

Čas detekce události IDEA je uvnitř atributu *DetectTime*. Atribut MISP události, který značí časovou informaci o detekci události, je atribut *date*, ten ale obsahuje pouze datum bez časové informace. Při konverzi do formátu MISP je tedy časová informace useknuta a při konverzi z formátu MISP do formátu IDEA se nabízejí dvě východiska:

- nastavit čas na 00:00:00
- iterovat přes všechny časové značky MISP události (každý atribut i objekt mají svojí vlastní časovou značku, která značí vznik nebo poslední změnu) a pokud je časová značka ze stejného dne jako *date*, poté nejstarší časová značka bude použita. Je pravděpodobné, že nejstarší časová značka bude svou hodnotou blíž k detekci, než prostý čas 00:00:00, protože událost je do MISP instance často vložena co nejdříve po detekci a její atributy ihned poté.

Pro konverzi síťových informací formátu IDEA byly vytvořeny vlastní MISP objekty, které jsou svojí definicí v podstatě totožné s IDEA objekty *Source* a *Target*. S využitím vlastních objektů jsou informace udrženy pohromadě jako v původní IDEA zprávě. Konverze z formátu MISP do formátu IDEA hledá samostatné MISP atributy síťových informací a konvertuje i seskupené MISP atributy uvnitř MISP objektů, které slouží pro přenos síťových informací. Při popisu této části konverze může pro lepší vizualizaci problému pomoci vytvoření konverzní tabulky. V podstatě se jedná o mapování atributů k sobě, ale ne vždy se jedná o pouhou kopii atributu. V ukázkové konverzní tabulce (Tabulka 1) je vidět, že hodnota jednoho atributu může být někdy rozdělena i do dvou (*ip-src|port* je složený atribut). Navíc IP adresa verze 4 i 6 je v MISP formátu vkládána do jednoho atributu, ale ve formátu IDEA se verze IP adres rozdělují.

Konverze kategeorie z C3ISP verze formátu STIX do formátu IDEA je méně přímočará. Kategorie události je u značné části událostí uvedena v rozšiřující části formátu CEF (atribut *cat*), v některých případech je ale roztroušena do více atributů nebo vyjádřena pouze slovním popisem. V takových případech je nutné nadefinovat vlastní sadu regulárních výrazů, které pomocí vyhledávání klíčových slov dokážou odhalit správnou kategorii události. Pokud nemůže být kategorie přesně určena pomocí regulárních výrazů (stále je důležité dbát na přesnost převodu), nezbývá nic jiného než použít IDEA kategorii *Other*. Taková kategorie by měla být použita v krajních případech, protože kategorizace událostí je velice důležitá a při použití kategorie *Other* se tato informace zamlžuje.

Časové atributy jsou uvedeny uvnitř hlavičky CEF formátu, v některých případech jsou evedeny uvnitř rozšíření CEF formátu. Pokud není určen časový údaj z těchto dvou pozic, je použita časová značka STIX objektu, který definuje několik časových atributů. Síťové informace jsou převážně uvedeny v rozšíření formátu CEF. Na základě využívaných atributů rozšíření byla proto vytvořena opět konverzní tabulka, jejíž úryvek se nachází v Tabulce 2.

Při konverzi z formátu IDEA do formátu STIX platformy C3ISP stačí vybrat správné schéma STIX objektu, do kterého budou konvertovány události. Časové značky jsou konvertovány do atributů STIX objektu (*created* a *last_observed*). Pro kategorii události obsahuje STIX objekt samostatný atribut.

4. Implementace konverzních konektorů

Návrh a implementace konverzní knihovny je pouze jedna část celého procesu konverze událostí. Konverzní knihovna umí načtenou událost pouze překonvertovat a na výstupu vrátit výsledek konverze. Ještě je ale potřeba implementovat obslužné konektory, které

MISP atribut	IDEA událost
"**ip-dst**": "<hodnota>"	"**Target**": [{"IP4/6": ["<hodnota>"]}]
"**ip-src|port**": "<IP>|<port>"	"**Source**": [{ "IP4/6": "<IP>", "Port": [<port>] }]
"**src-port**": "<hodnota>"	"**Source**": [{"Port": [<hodnota>]}]
"**protocol**": "<hodnota>"	"**Source**": [{"Proto": ["<hodnota>"]}], "**Target**": [{"Proto": ["<hodnota>"]}]
"**src-as**": "<hodnota>"	"**Source**" [{"ASN": [<hodnota>]}]

Tabulka 1. Konverze MISP atributů obsahujících síťové informace

Atribut rozšíření formátu CEF	IDEA událost
src=<hodnota>	"**Source**": [{"IP4/6": ["<hodnota>"]}]
dst=<hodnota>	"**Target**": [{"IP4/6": ["<hodnota>"]}]
spt=<hodnota>	"**Source**": [{"Port": [<hodnota>]}]
dpt=<hodnota>	"**Target**": [{"Port": [<hodnota>]}]

Tabulka 2. Konverze CEF atributů obsahujících síťové informace

umí události správně načítat ze zdroje a rozebrat nosný formát (např. JSON). Někdy je navíc potřeba určité předzpracování, např. anonymizace dat, pokud organizace nechce zveřejňovat celý obsah události (některá data mohou být pro organizaci citlivá, ale byla by škoda kvůli tomu zahodit celý obsah události). Až po tomto bodě proběhne proces konverze. Poté je možné na události udělat finální drobné úpravy, například agregace a deduplikace událostí. Tento celý proces zpracování událostí znázorňuje Obrázek 2.

Konektory obsluhující konverzi mezi formáty MISP a IDEA převezmou autentizační udaje MISP platformy a následné propojení je realizováno pomocí knihovny *PyMISP* jazyka Python. Po připojení k instanci MISP platformy stahuje konektor nové události ve formátu JSON. Po načtení proběhne konverze a výsledné IDEA události jsou uloženy do souboru, kde už je převezme tzv. *Warden filer*, který nové události odesílá do Wardenu [8], sběrného místa sdílených bezpečnostních událostí v rámci organizace Cesnet. Přesně opačný postup probíhá u konverze formátu IDEA do formátu MISP. U konverze formátu STIX probíhá na STIXové straně přenos nových událostí pomocí protokolu HTTP(S). Vzniklé obslužné konektory mohou být spuštěny jako proces na pozadí a jsou konfigurovatelné dalšími parametry. Např. při konverzi z formátu MISP do formátu IDEA může být zvolena úroveň distribuce událostí pomocí protokolu TLP[5]. Pokud je zvolena úroveň *tlp:green*, z konverze jsou vyjmuty vyšší úrovně (tedy *tlp:amber* a *tlp:red*).

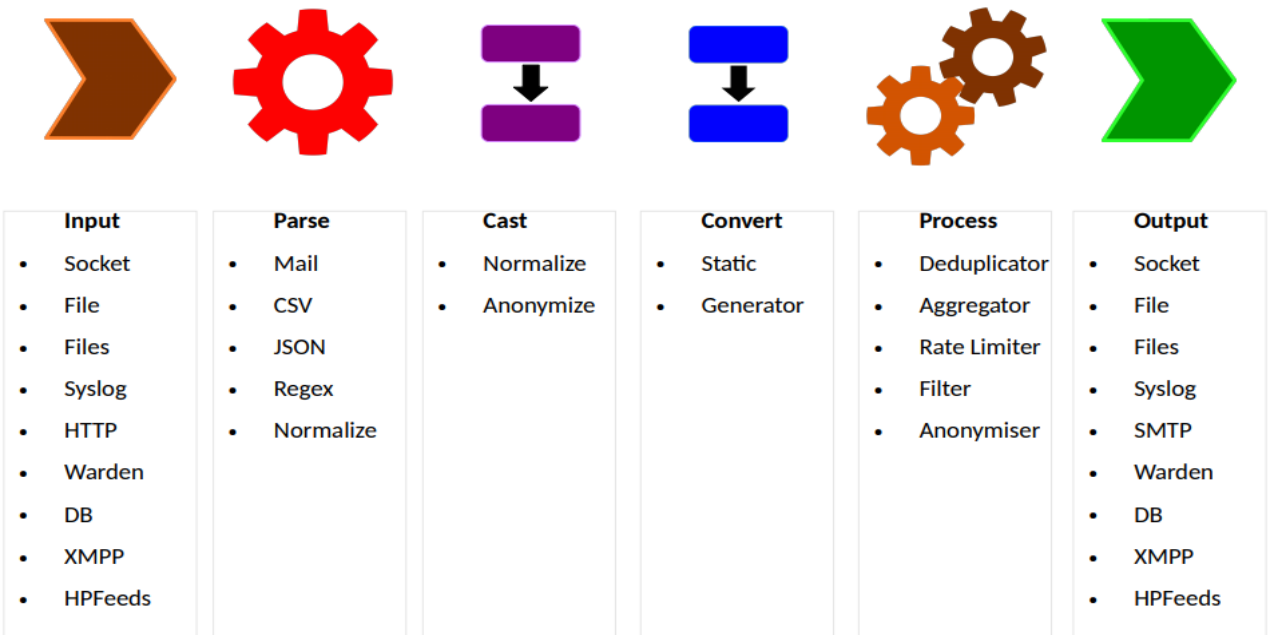
Komponenty takovýchto konektorů jsou velmi často podobné, až na výjimku samotné konverze. Při vývoji konvertorů byl použit framework zvaný *Deadbeat*[6], který má za úkol oprostit vývojáře od těchto rutinních komponent, aby se vývojář mohl plně věnovat samotné konverzi.

5. Výsledky implementace

Nově vzniklé konvertory jsou testovány na datech ze systému Warden. V průběhu konverze z formátu IDEA do formátu MISP byly použity stovky IDEA událostí, které byly pomocí konektorů automaticky překonvertovány a vloženy do MISP instance. Konverze z formátu MISP do formátu IDEA byla kontrolována jednoduchým testem. V MISP instanci se vytvořila nová událost, která obsahovala většinu všech hodnot, které byly navrženy v teoretickém návrhu k převodu. Tato událost se převedla pomocí konektoru do formátu IDEA a automatizovaně se porovnala

[5] https://www.us-cert.gov/tlp

[6] https://alchemist.cesnet.cz/deadbeat/doc/development/html/manual.html



Obrázek 2. Architektura konektorů (převzato z [7])

vůči manuálně vzorově překonvertované události. Proces testování lze i částečně automatizovat. Pomocí konektorů došlo k převodu událostí formátu IDEA do MISP, které se převedly zpět do formátu IDEA a automaticky se porovnal vzniklý rozdíl. Kontrola správné konverze byla ale z větší části manuální, aby došlo k otestování případů, které není možné tímto automatickým testováním podchytit. Výsledky testování neodhalily žádný problém při konverzi. Podobným způsobem proběhlo testování konverze formátu IDEA do formátu STIX. Výsledky testování opět neodhalily problémy v konverzi. Výsledkem implementace jsou 2 konverzní knihovny a 4 obslužné konektory. Všechny komponenty jsou implementovány v programovacím jazyce python.

Pomocí vzniklého konvertoru a konektorů je možné se připojit k jakékoliv MISP instanci. Instance která posloužila k testování při vývoji je podle mnoha analýz událostí určena spíše pro sdílení analýz malware a různých blacklistů IP adres. Mnohem lepšího poměru převedených událostí může být dosaženo v případě připojení k jiné MISP instanci, která je používána pro sdílení událostí ze systémů IDS. Jelikož MISP platforma je aktuálně používána více než 1000 organizací, je velice pravděpodobné, že některé z nich budou MISP platformu používat pro sdílení takových událostí. S konverzí z formátu IDEA do formátu MISP problémy s filtrací událostí nejsou a je možné konvertovat všechny události formátu IDEA. Události proprietární verze formátu STIX lze převážně konvertovat všechny. Malé množství událostí je při konverzi ignorováno, jelikož svým obsahem nekorespondují přímo k formátu IDEA.

6. Závěr

Výsledkem této práce je úspěšná konverze mezi síťovými bezpečnostními formáty IDEA a MISP, a také konverze mezi formátem IDEA a modifikovanou verzí formátu STIX 2.0.

Konverze mezi bezpečnostními formáty nemusí být vždy přímočará, ale je velmi důležitá. Pomocí konvertorů je možné sdílet bezpečnostní události mezi organizacemi, které díky více událostem mohou lépe reagovat na aktuální hrozby. Navíc většina bezpečnostních událostí bývá zpracována automaticky a do hry mnohdy přichází i strojové učení a umělá inteligence. Síla těchto pokročilých metod se ale silně odvíjí od množství informací, na kterých se mohou tyto metody učit. Sdílení bezpečnostních událostí tedy může rozšířit obzory nejen samotným správcům, ale i strojům.

Tato práce se zabývala konverzí modifikované verze bezpečnostního formátu STIX 2.0. Možným rozšířením této práce je podpora konverze nemodifikovaného bezpečnostního formátu STIX verze 2.1. Tato verze má být dokončena tento rok (2019) a s novou verzí přichází nové objekty formátu, které jsou přizpůsobeny pro přenos událostí generovaných systémy IDS a mohlo by být dosaženo efektivnější a přesnější konverze. Specifikace nové verze ještě ale není dokončena a přesné závěry proto zatím nemohou být vyvozeny.

Poděkování

Rád bych poděkoval Ing. Martinu Žádníkovi, Ph.D. za velmi cenné rady v průběhu vývoje a odborné konzultace, jeho ochotu a čas, který mi věnoval. Dále bych

rád poděkoval Pavlu Káchovi ze sdužení Cesnet za příležitostné konzultace.

Literatura

[1] Cynthia Wagner, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. Misp: The design and implementation of a collaborative threat intelligence sharing platform. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pages 49–56. ACM, 2016.

[2] Alexandre Dulaunoy and Andras Iklody. MISP core format. Internet-Draft draft-dulaunoy-misp-core-format-07, Internet Engineering Task Force, February 2019. Work in Progress.

[3] Sean Barnum. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation*, 11:1–22, 2012.

[4] Pavel Kácha. Idea: Designing the data model for security event exchange. In *Proceedings of the 17th International Conference on Computers: Recent Advances in Computer Science*, 2013.

[5] ArcSight. Common event format, 2010. https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/78000/KB78712/en_US/CEF_White_Paper_20100722.pdf.

[6] Pavel Kácha. Idea: Security event taxonomy mapping. In *Proceedings of the 18th International Conference on Circuits, Systems, Communications and Computers*, 2014.

[7] Pavel Kácha. Framework pro konektory, 2017. https://sabu.cesnet.cz/_media/cs/2017-08-07_pavel_kacha_warden_a_konektory.pdf.

[8] Andrea Kropáčová Pavel Kácha, Michal Kostěnec. Warden 3: Security event exchange redesign. In *Proceedings of the 19th International Conference on Computers: Recent Advances in Computer Science*, 2015.