VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
DEPARTMENT OF INFORMATICS

NÁVRH METODIKY HODNOCENÍ EFEKTIVITY SYSTÉMU SIEM V ORGANIZACI

THE DESIGN OF THE MATURITY MODEL FOR MEASURING EFFECTIVITY OF THE SIEM SYSTEM IN THE ORGANISATION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **ZDEŇKA KOSKOVÁ**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. VIKTOR ONDRÁK, Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Studentka:	**Zdeňka Kosková**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Návrh metodiky hodnocení efektivity systému SIEM v organizaci

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je vytvoření metodiky pro hodnocení efektivity systému SIEM vycházející z matice MITRE ATT&CK for ICS.

Základní literární prameny:

COLBERT, E. J. Cyber-security of SCADA and Other Industrial Control Systems. Springer International Publishing Switzerland, 2016. ISBN 978-3-319-32125-7.

DOUCEK, P. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 9788074310508.

KOLOUCH, J. CyberSecurity. 1. vyd. CZ.NIC, 2019. ISBN 978-80-88168-31-7.

MILLER, D. R. Security Information and Event Management (SIEM) Implementation. McGraw-Hill, 2011. ISBN 978-0-07-170108-2.

ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

V bakalářské práci je řešena problematika hodnocení efektivity systému SIEM v průmyslovém prostředí. Jejím cílem je navržení metodiky, která pro hodnocení využívá matici MITRE ATT&CK for ICS. V práci jsou analyzována již existující řešení a jejich možná aplikace. Dále je popsáno hodnocení monitoringu v energetické společnosti, které společně s maticí tvoří základ návrhu vlastního řešení. Výsledkem práce je návrh kvantitativního hodnocení jednotlivých technik matice, jeho grafická interpretace a možnost bezpečného sdílení výsledků s ostatními CERT týmy.

Abstract

The bachelor‘s thesis addresses the issue of evaluating the effectiveness of the SIEM system in an industrial environment. The goal was to propose a methodology that uses a MITRE ATT&CK matrix for ICS for evaluation. The thesis first analyses existing solutions and their potential applications, followed by a description of monitoring evaluation in an energy company, which together with the matrix form the basis of the proposed solution. The main output of the thesis is a proposal for quantitative evaluation of individual techniques of the matrix, such as graphical interpretation and the possibility to share results securely with other CERT teams.

Klíčová slova

SIEM, monitoring, metodika, hodnocení, Mitre ATT&CK for ICS, průmyslové řídicí systémy, kybernetická bezpečnost

Keywords

SIEM, monitoring, methodology, maturity model, Mitre ATT&CK for ICS, industrial control systems, cyber security

Citace

KOSKOVÁ, Zdeňka. *Návrh metodiky hodnocení efektivity systému SIEM v organizaci.* Brno, 2021. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská. Vedoucí práce Ing. Viktor Ondrák, Ph.D.

Návrh metodiky hodnocení efektivity systému SIEM v organizaci

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně pod vedením pana Ing. Viktora Ondráka, Ph.D. Uvedla jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpala.

.....

Zdeňka Kosková

16. května 2021

Poděkování

Na tomto místě bych ráda poděkovala panu Ing. Viktoru Ondrákovi, Ph.D. za vedení bakalářské práce. Dále bych chtěla poděkovat energetické společnosti za poskytnutou příležitost, konzultace a odborné rady. V neposlední řadě bych ráda poděkovala rodině, partnerovi a přátelům za jejich podporu při tvorbě práce a pomoc při její závěrečné korektuře.

Obsah

Kapitola 1

Úvod

Průmyslové systémy byly dříve izolovány od IT prostředí a jejich prvky využívaly pro komunikaci především proprietární protokoly. S postupnou digitalizací a příchodem finančně dostupnějších řešení založených na protokolu TCP/IP dochází k jejich propojení s IT sítí a tím pádem ke zvýšenému riziku kybernetických útoků. Jasným důkazem jsou události na Ukrajině v letech 2015 a 2016, které vedly k výpadkům dodávek elektrické energie a zasáhly stovky tisíc zákazníků. Vzhledem k tomu, že průmyslové řídicí systémy ovládají fyzická zařízení, mohou na ně vedené útoky ohrozit zdraví či životy lidí nebo napáchat škody na životním prostředí. Zajistit bezpečný provoz těchto systémů je proto naprosto zásadní. Jedním z prvků, který napomáhá zvýšení kybernetické bezpečnosti, je bezpečnostní monitoring. Díky němu je možné identifikovat bezpečnostní události a případně tak zachytit útok v jeho rané fázi. Pro zajištění požadované bezpečnosti systémů je nutné opakovaně vyhodnocovat jeho efektivitu. Cílem této práce je tak navrhnout metodiku, která bude hodnotit efektivitu systému SIEM z pohledu matice MITRE ATT&CK for ICS.

Druhá kapitola bude věnována teoretickým východiskům práce, která poskytnou základní vhled do problematiky kybernetické bezpečnosti a s ní související české legislativy. Dále budou popsány průmyslové řídicí systémy a porovnány s prostředím informačních technologií. Následně bude představena matice ATT&CK for ICS, která tvoří znalostní bázi o chování útočníků, jejich taktikách, technikách a procedurách, jež

využívají v průmyslovém prostředí. V poslední části bude popsáno základní schéma systému SIEM, který slouží pro sběr a vyhodnocování bezpečnostních událostí. V kapitole 3 budou uvedeny základní informace o energetické společnosti a způsob jejího vyhodnocování monitoringu. V neposlední řadě budou představena a zhodnocena současná řešení, která využívají matici Mitre ATT&CK. Ve čtvrté kapitole bude popsán vlastní návrh hodnocení monitoringu za pomoci matice ATT&CK for ICS, interpretace výsledků a možnost jejich sdílení.

Kapitola 2

Teoretická východiska práce

2.1 Základní terminologie informační bezpečnosti

V následující podkapitole budou vysvětleny elementární pojmy týkající se informační bezpečnosti.

Data

Data jsou lidské poznání zaznamenané formalizovanou formou. [6]

Informace

Informace je interpretace dat, kterým člověk přisuzuje určitý význam. [6]

Informační systém

Informační systém můžeme definovat například jako soubor technických a lidských prostředků, které s využitím metod pro shromažďování, přenos, uchování a zpracování dat umožňují vytváření či prezentaci informací na základě uživatelských potřeb. [15]

Důvěrnost

Důvěrnost zajišťuje přístup k informacím, datům nebo informačnímu systému pouze oprávněným subjektům. [9]

Integrita

Integrita zajišťuje nemožnost narušení správnosti a úplnosti informace, dat nebo počítačového systému. [9]

Dostupnost

Dostupnost garantuje možnost přístupu oprávněného uživatele k informaci, datům nebo počítačovému systému v daný okamžik. [9]

Bezpečnost informací

Bezpečnost informací je zajištěna v případě, kdy dochází k zachování důvěrnosti, integrity a dostupnosti informací. [14]

Aktivum

Aktivum představuje jakýkoliv hmotný či nehmotný majetek, který má pro jednotlivce, organizaci nebo veřejnou správu hodnotu. [8]

Zranitelnost

Zranitelnost představuje nedostatek či slabé místo aktiva nebo zabezpečení, které může být jednou nebo více hrozbami využito k jeho poškození. [9][15]

Hrozba

Hrozba je potenciální událost, při které může dojít ke zneužití zranitelnosti aktiva a tím pádem i k jeho zničení, kompromitaci, úpravě dat nebo nedostupnosti služeb. [14][15]

Bezpečnostní událost

Bezpečnostní událost představuje identifikovatelný stav systému, služby nebo sítě, který značí, že mohlo dojít k narušení bezpečnostní politiky nebo selhání bezpečnostních opatření. Dále se může jednat o situaci, která doposud nikdy nenastala a mohla by být z hlediska bezpečnosti informací významná. [8][9]

Bezpečnostní incident

Bezpečnostní incident je jedna nebo více bezpečnostních událostí, které narušily bezpečnost informací nebo služeb informačního systému. [9]

Kybernetický útok

Kybernetický útok představuje úmyslné jednání jedince nebo skupiny, jehož účelem je narušení dostupnosti, důvěrnosti nebo integrity dat a to za pomoci informačních a komunikačních technologií. [9]

Opatření

Opatření jsou prostředky, s pomocí kterých je možné snížit riziko. [8]

Riziko

Riziko vyjadřuje pravděpodobnost využití zranitelnosti aktiva bezpečnostní hrozbou. [14]

Dopad

Dopad představuje následky působení hrozby na aktiva. [14]

2.2 Legislativa upravující kybernetickou bezpečnost v ČR

V následující kapitole bude stručně popsána legislativa ČR týkající se kybernetické bezpečnosti.

Legislativa

Kybernetická bezpečnost je v České republice v gesci Národního úřadu pro kybernetickou bezpečnost (NÚKIB), jakožto ústředního správního orgánu pro kybernetickou bezpečnost včetně ochrany informací v oblasti komunikačních systémů a kryptografické ochrany. [13] Dále je dle [13] upravována následujícími regulacemi:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti (ZoKB) vznikl za účelem úpravy práv a povinností osob a působnosti a pravomocí orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zároveň pokrývá požadavky Evropské unie na sjednocení právní úpravy členských států v podobě směrnice Evropského parlamentu a Rady (EU) 2016/1148 (směrnice NIS), která je do ZoKB transponována. [13]

Hlavními cíli ZoKB je ustanovení organizačních a technických bezpečnostních opatření, zavedení systému detekce, hlášení a reakce na kybernetické bezpečnostní incidenty a definování činností dohledových pracovišť. Mezi opatření organizačního charakteru jsou zařazeny například systém řízení bezpečnosti informací (ISMS), řízení rizik, řízení přístupu osob a další dle §5 odstavce 1. Dále jsou v paragrafu definována technická opatření, mezi nimiž můžeme nalézt ku příkladu požadavky na fyzickou bezpečnost, kryptografické prostředky, nástroje pro detekci, sběr a vyhodnocení kybernetických bezpečnostních událostí či bezpečnost průmyslových a řídicích systémů. Subjekty spadající pod ZoKB mají kromě zajištění bezpečnostních opatření povinnost hlásit kybernetické bezpečnostní incidenty. K tomuto účelu slouží vládní CERT, který je součástí NÚKIB a národní CSIRT jakožto právnická osoba definována §18 ZoKB. Roli národního CERT zastává v současné době správce domény CZ sdružení CZ.NIC. [9][13][1]

V zákoně jsou mimo jiné vymezeny pojmy jako významný informační systém, kritická informační infrastruktura či provozovatel základní služby, které jsou určovány na základě kritérií vymezených ve výše zmíněném výčtu regulací. Významnými informačními systémy se rozumí systémy, jež jsou spravovány orgány veřejné moci a jejich funkčnost má zásadní dopad na chod veřejné správy. Kritická informační infrastruktura (KII) je ovlivněna zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve kterém se předpokládá, že KII bude prvkem kritické infrastruktury (KI), která je tímto zákonem definována. Kritická informační infrastruktura je pak určena na základě možného narušení bezpečnosti informací informačního či komunikačního systému, jehož dopad spadá do průřezových a odvětvových kritérií podle nařízení vlády č. 432/2010 Sb., Základní služby představují služby, jichž provoz závisí na informačních systémech nebo sítích elektronických komunikací a v případě jejich narušení hrozí zásadní dopad na ekonomické či společenské činnosti následujících odvětví [9][1]:

- energetika
- doprava
- bankovnictví
- infrastruktura finančních trhů
- zdravotnictví
- vodní hospodářství
- digitální infrastruktura
- chemický průmysl [9]

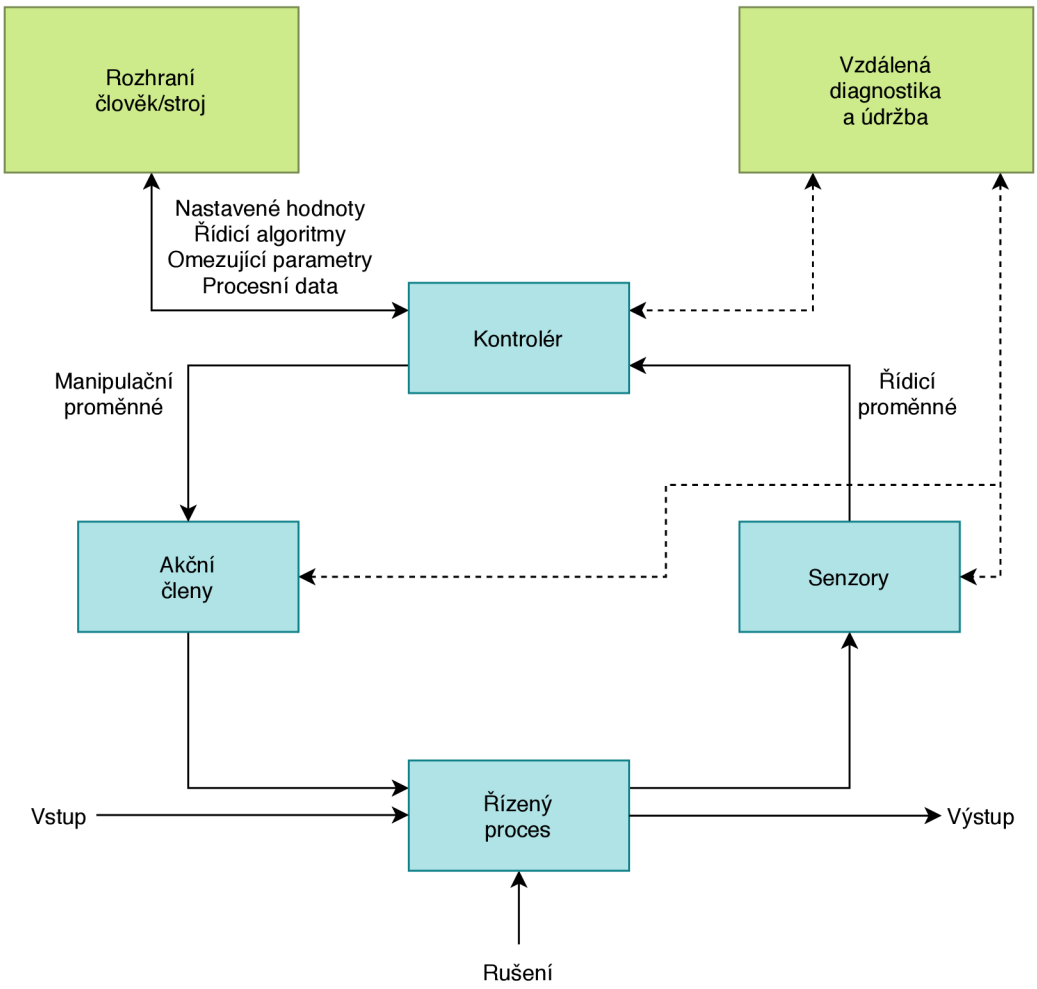
2.3 Průmyslové řídicí systémy

Následující kapitola bude věnována vybraným řídicím systémům a jejich součástem.

Průmyslové řídicí systémy (ICS) se sestávají z mnoha řídicích smyček, které jsou ovlivňovány skrze rozhraní člověk/stroj (HMI) a rozhraní vzdáleného přístupu diagnostiky a údržby. Systém řídí proces, jehož primárním úkolem je vytvoření požadovaného výstupu. K modifikaci řídicího procesu jsou využívány senzory, akční členy[1] a kontroléry (např. PLC). Senzory měří fyzikální vlastnosti, které jsou odesílány kontroléru v podobě řídicích proměnných. Ten je následně vyhodnotí a na základě cílových hodnot a řídicího algoritmu vytvoří odpovídající manipulační proměnné, které odešle akčním členům. Skrze ně je řízený proces přímo ovlivňován. [19]

K dohledu a nastavování výchozích hodnot a řídicích algoritmů je využíváno HMI. Skrze něj jsou také upravovány a zadávány parametry pro kontroléry. Další funkcí je zobrazení stavu procesu a to i v kontextu historických údajů. Pro předcházení a zaznamenání neobvyklého chování či poruchy jsou využívány nástroje pro diagnostiku a údržbu, které jsou schopné i obnovy. [19]

[1] Akčními členy mohou být například ventily, jističe, spínače, motory...

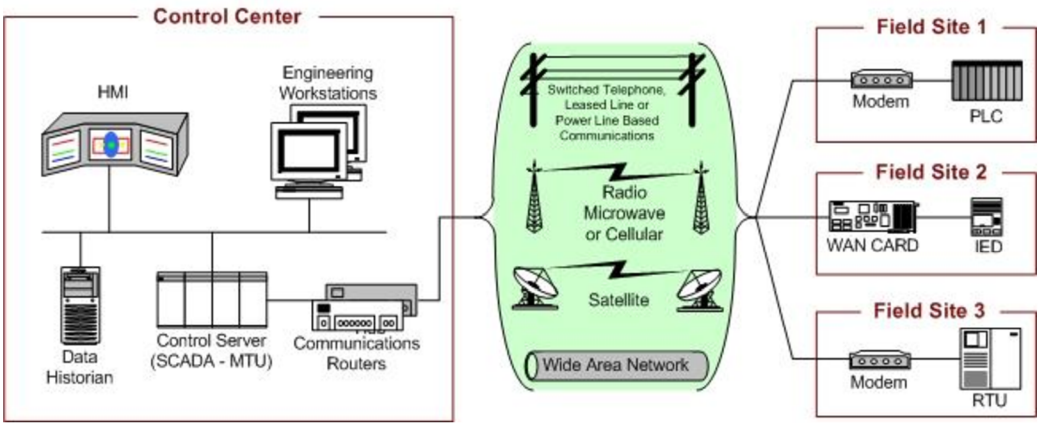


Obrázek 2.1: Obecné schéma řízení procesu v ICS. Převzato z [19], upraveno.

Systémy SCADA

Systémy pro dohled, řízení a sběr dat (SCADA) fungují na principu centrálního pracoviště, které získává informace od vzdálených aktiv. Ty jsou následně zobrazeny v textové či grafické podobě operátorovi. Kromě dohledu má operátor možnost řízení systému za pomoci HMI z centrálního pracoviště. Všechny tyto činnosti probíhají v reálném čase buď automatizovaně nebo na základě příkazů operátora v závislosti na nastavení a složitosti jednotlivých systémů. [19]

Komunikace mezi řídicím centrem a vzdálenými řídicími prvky jako jsou PLC, RTU či IED, probíhá například skrze počítačovou síť nebo radiokomunikace. Využívány jsou protokoly typické pro průmyslové prostředí (Modbus, DNP3, Ethernet/IP) [19].



Obrázek 2.2: Obecné schéma systémů SCADA. Převzato z [19].

PLC

PLC jsou zařízení ovládaná mikroprocesorem, která zajišťují lokální správu procesů. Jejich součástí je programovatelná paměť, do které jsou ukládány instrukce sloužící k zavedení funkcí, jako je řízení vstupů a výstupů, časování, komunikace, zpracování dat a souborů, aritmetika a další. Dalšími součástmi kontrolérů jsou napájecí zdroje, moduly pro vstup a výstup a rozhraní pro komunikaci. [19][5]

Hlavní funkcí PLC je načítání vstupních signálů ze senzorů, které na základě naprogramovaných instrukcí a řídicích příkazů promění na výstupní signály, s jichž pomocí mohou být následně ovládány aktuátory. Veškeré tyto činnosti probíhají v reálném čase v řádu milisekund, což klade požadavky na deterministické chování celého cyklu. Dalším specifikem jsou často náročné podmínky, ve kterých kontroléry pracují, ať už se jedná o teplotu, elektromagnetické rušení či vibrace. Komunikace PLC s nadřízenými procesy probíhá typicky v lokální síti skrze optické vlákno, ethernet či sériové spojení a odděluje tak reálný svět od kybernetického. [5]

Obrázek 2.3: PLC SIMATIC S7-300. Převzato z [16].

RTU

RTU jsou stejně jako PLC elektronická zařízení ovládaná mikroprocesorem. Dalším společným znakem je provoz v náročných podmínkách. Nejčastěji se můžeme setkat se dvěma typy RTU. První jsou využívány pro sběr dat v předdefinovaných intervalech ze senzorů provozovaných v terénu. Tato RTU jsou označována jako *field* RTU a představují rozhraní mezi senzory a druhým typem RTU – tzv. *station* RTU. Station RTU pak slouží nejen ke sběru dat z field RTU, ale zároveň přijímá příkazy řídicích kontrolérů. Následně vytváří výstupní hodnoty, za pomoci nichž řídí fyzická zařízení a procesy. Instalována jsou v odlehlých lokalitách a můžeme se setkat se zařízením, které kombinuje oba typy RTU. [5]

Hardware RTU je sestaven z mikroprocesoru, napájecího zdroje, CPU a digitálních či analogových modulů pro vstup a výstup. Navrhována jsou s podobnými vlastnostmi, jako mají PLC, stejně tak představují rozhraní mezi reálným a kybernetickým světem a postupně přebírají i identické programovací jazyky. S řídicím centrem, kterému na vyžádání odesílají nasbíraná data, mohou komunikovat skrze sítě WAN za pomoci GPRS, satelitního, mikrovlnného, IP a dalších druhů spojení. [5]

Obrázek 2.4: SIMATIC RTU3010C. Převzato z [17]

IED

V prostředí průmyslových řídicích systémů představují IED zařízení, která jsou schopna za pomoci jednoho či více procesorů přijímat a odesílat data nebo příkazy z externích zdrojů. Setkat se můžeme také s označením digitální ochranné relé. Každé IED se může lišit poskytovanými funkcemi v závislosti na výrobci. Mezi tyto funkce patří ochrana, řízení, monitorování, měření a komunikace. Konkrétně se pak může jednat o ochranu před nízkou či vysokou hladinou napětí, vzdálené či lokální řízení, hlášení stavu jističů, měření elektrického proudu a další. Ovládání ochranných relé probíhá za pomoci řídicích jednotek nebo automatizačního procesu z řídicího centra. K lokálnímu přístupu slouží zobrazovací displej na předním panelu. [5]

HMI

HMI je softwarová aplikace, která operátorovi ve vizuální podobě zprostředkovává informace o stavu procesů jako jsou hodnoty, data, trendy a další. Provozována může být na pracovních stanicích, tabletech, chytrých telefonech nebo zobrazovacích zařízeních. Dále může sloužit k ručnímu ovládání akčních členů. [5]

Pracovní stanice

Pracovní stanice je nejčastěji stolní počítač nebo server, který pracuje na běžných operačních systémech, jako je Microsoft Windows nebo Linux. Zde se nachází software pro programovaní kontrolérů (PLC, RTU, IED) a aplikací. Kromě změn logiky kontrolérů a aplikací je pracovní stanice využívána k nasazení změn firmwaru. [5]

Rozdíly mezi IT a ICS

Průmyslové řídicí systémy, na rozdíl od systémů IT, které spravují data, řídí fyzický svět. Z toho vyplývají rozdílné požadavky na chování, spolehlivost, rizika a priority pro oba typy systémů. Z pohledu ICS jsou nejzásadnějšími riziky taková, která jsou spojena se zdravím či bezpečností osob, vážnými enviromentálními dopady, snížením produkce nebo negativními dopady na ekonomiku státu. Hlavní rozdíly mezi IT a ICS systémy jsou shrnuty v následující tabulce. [19]

Kategorie	IT systémy	ICS systémy
Požadavky na výkon	Neprobíhá v reálném čase Odezva musí být konzistentní Je požadována vysoká propustnost Velké prodlevy a odchylky mohou být přípustné Nouzová interakce je méně kritická Může být zavedeno velmi striktní řízení přístupu	V reálném čase Odezva je časově kritická Malá propustnost je přijatelná Velké prodlevy a odchylky nejsou přípustné Odezva na lidskou a nouzovou interakci je kritická Přístup k ICS by měl být přísně kontrolován, ale neměl by zabraňovat v interakci člověk-stroj
Požadavky na dostupnost	Reakce jako rebooting jsou akceptovatelné Výpadky dostupnosti mohou být občasně tolerovány v závislosti na provozních požadavcích systému	Reakce jako rebooting mohou být neakceptovatelné vzhledem k požadavkům na dostupnost Možné vyžadování redundance systému Odstávky musí být plánovány dopředu Nutnost rozsáhlého testování před nasazením
Požadavky na řízení rizik	Správa dat Úplnost a integrita dat jsou prvořadé Občasné prostoje nejsou zásadním rizikem Zásadním dopadem rizik je zpoždění podnikových činností	Řízení fyzického světa Primární je bezpečnost lidí a ochrana procesu I chvilková prodleva nemusí být akceptovatelná Zásadními dopady rizik jsou neplnění regulací, dopady na životní prostředí, ztráty na životech, vybavení nebo produkci

Provoz systému	Systémy jsou navrženy pro běžné operační systémy. Vylepšení jsou přímočará s možností automatizovaného nasazení.	Rozdílné a proprietární operační systémy, často bez vestavěných bezpečnostních možností. Změny software musí být prováděny opatrně, nejčastěji jeho dodavateli.
Požadavky na zdroje	Systémy mají dostatek zdrojů pro podporu dodatečných aplikací třetích stran, jako jsou bezpečnostní řešení.	Systémy jsou navrženy pro podporu zamýšlených průmyslových procesů a nemusí mít dostatek paměti a výpočetních zdrojů pro podporu dodatečných bezpečnostních řešení
Komunikace	Standardní komunikační protokoly. Primárně drátová síť s možností lokálního bezdrátového připojení. Typické postupy pro IT síťování.	Mnoho proprietárních standardů a komunikačních protokolů. Použití mnoha typů komunikačních médií zahrnující dedikované drátové a bezdrátové spojení (radio, satelit). Sítě jsou komplexní a jejich správa může vyžadovat vysokou odbornost.

Řízení změn	Změny software jsou nasazovány pravidelně s ohledem na bezpečnostní politiky, procedury jsou často automatizované.	Změny software musí být důkladně testovány a nasazeny postupně, aby byla zabezpečena integrita řídicího systému. Výpadky ICS musí být často plánovány dopředu. ICS mohou využívat operační systémy, které již nejsou podporovány.
Podpora	Umožňuje různé druhy podpory.	Podpora je nejčastěji zprostředkována dodavateli.
Životnost komponent	Životnost je zhruba 3-5 let.	Životnost je zhruba 10-15 let.
Umístění komponent	Komponenty jsou jednoduše přístupné.	Komponenty mohou být oddělené, vzdálené a přístup k nim může vyžadovat rozsáhlé fyzické úsilí.

Tabulka 2.1: Porovnání IT a ICS prostředí. Převzato z [19], upraveno.

2.4 Matice ATT&CK for ICS

Matice ATT&CK for ICS vznikla pod záštitou americké neziskové organizace MITRE, která spolupracuje s vládou, průmyslem i akademickou obcí. Věnují se oblastem, jako je umělá inteligence, kvantová informatika, sdílení kybernetických hrozeb, kybernetická odolnost a další. ATT&CK for ICS vznikla v návaznosti na matici ATT&CK for Enterprise a to především jako reakce na kybernetické útoky na Ukrajině v letech 2015 a 2016, které jako první vedly k výpadkům dodávek elektrické energie. Vzhledem k rozdílům mezi podnikovou a průmyslovou oblastí nebyla ATT&CK for Enterprise schopna obsáhnout veškeré možnosti útočníkova chování, a proto došlo k její úpravě se zaměřením na průmyslové řídicí systémy. [12][3]

ATT&CK for ICS představuje souhrn znalostí o chování útočníků v průmyslových řídicích systémech. Kvůli rozdílům mezi jednotlivými typy systémů je obtížné definovat úroveň rozsahu a abstrakce této technologické oblasti. Autoři matice se pro překlenutí problému rozhodli využít úrovně 0-2 architektury Purdue a rozdělení aktiv do jednotlivých tříd. Tento postup byl zvolen především kvůli silné vazbě aktiv a jejich funkčního účelu. Zaměření na úrovně 0-2 architektury Purdue bylo zvoleno, protože ovládnutí právě systémů a funkcí této úrovně je pro útočníky ve většině případů stěžejní. Jedná se o: [3]

- Základní řídicí systémy
  - Řízení procesů
  - Operátorské řízení a monitoring
  - Aktuální a historická data
  - Poplašný systém
- Bezpečnostní přístrojové systémy a ochranné systémy
- Systémy správy a údržby

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Obrázek 2.5: Matice MITRE ATT&CK for ICS. Převzato z [3], upraveno.

Referenční architektura Purdue Enterprise

Referenční architektura Purdue slouží v případě matice ATT&CK for ICS k zařazení běžných funkcionalit různých typů řídicích systémů do pěti funkčních úrovní:

- Úroveň 4 - Podnikové systémy
  - Podnikové plánování a logistika
  - Tvorba systémů
- Úroveň 3 - Řízení provozu
  - Správa systému
  - Dohledové řízení
- Úroveň 2 - Dohledové a řídicí vybavení
  - Dohledové řídicí funkce
  - Monitoring sítě
  - Lokální zobrazení
- Úroveň 1 - Řídicí vybavení
  - Ochranná zařízení
  - Lokální řídicí zařízení
- Úroveň 0 - Řízené vybavení
  - Aktuátory
  - Senzory

Toto rozdělení je však orientační, protože v některých případech může dojít k překryvu jednotlivých úrovní. Technologie průmyslových řídicích systémů se běžně objevují v úrovních 0-2. Ale například v případě, kdy jsou nasazeny některé dohledové řídicí funkce, dochází k prolnutí s úrovní 3. V tomto případě tak model slouží především pro lepší pochopení a propojení chování útočníků v prostředí průmyslových systémů. [3]

Aktiva

V ATT&CK for ICS jsou vytvořeny třídy aktiv na základě funkcí jednotlivých komponent systémů, ke kterým je přistupováno jako k objektům. U každé třídy je vytvořen popis účelu, funkcionality, propojení s úrovní Purdue architektury, seznam technik, které může útočník použít, a důležité poznámky k samotné třídě aktiv. [3]

Taktiky

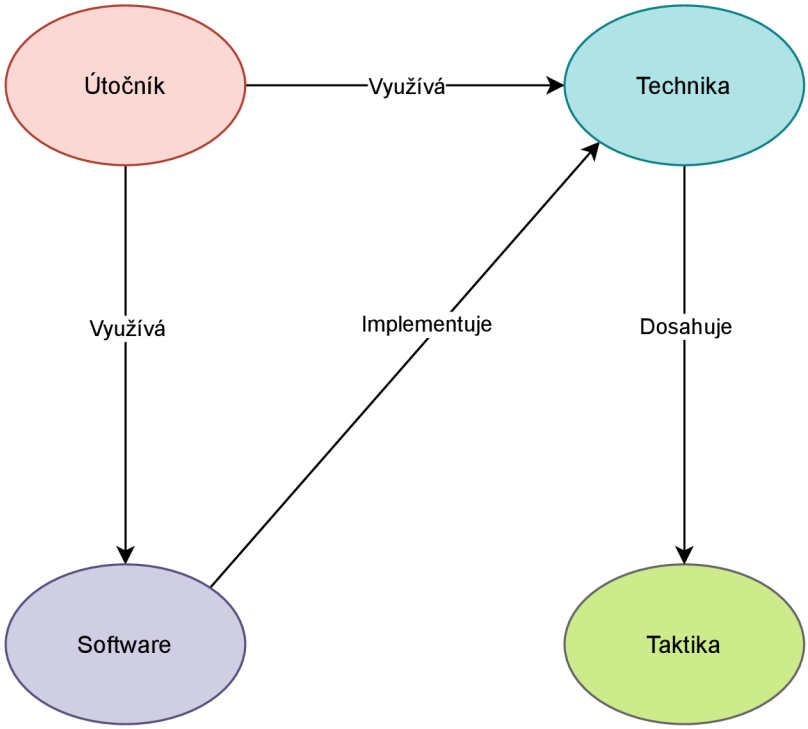
Taktiky v matici popisují cíl, kterého chce útočník v určité fázi svého postupu dosáhnout. Vysvětlují tak, proč jsou využívány dané techniky. Ty jsou propojeny s jednou nebo více taktikami v závislosti na dosaženém výsledku. Některé taktiky byly převzaty z matice pro podniky, ale velká část byla vytvořena specificky pro průmyslové prostředí. [3]

Techniky

Techniky vysvětlují, jakým způsobem útočníci dosahují svých cílů nebo co svým působením získají. V neposlední řadě popisují dopady na organizaci, kterými mohou být například finanční či produkční ztráty. [3]

Útočníci

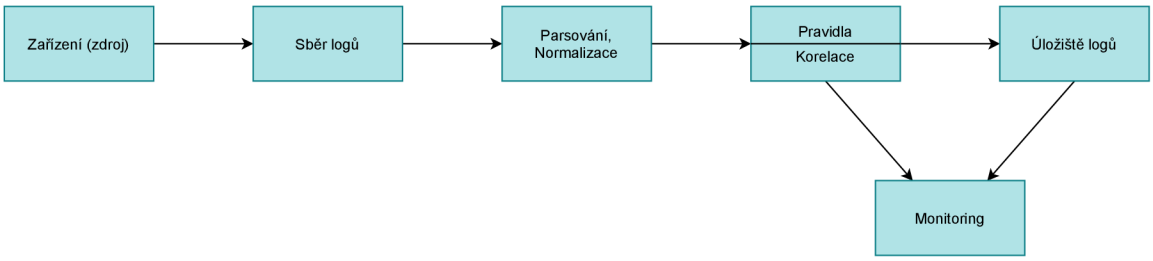
Součástí znalostní báze je seznam skupin útočníků, které byly identifikovány bezpečnostní komunitou na základě aktivit, které vedly k narušení bezpečnosti systémů. Účelem je nejen analyzování a pochopení chování útočníků, ale i identifikování nejvýznamnějších hrozeb. Zároveň dochází k propojení s technikami, které v rámci matice využívají. [3]



Obrázek 2.6: ATT&CK vztahy objektů. Převzato z [3], upraveno.

2.5 Řízení bezpečnosti informací a událostí

Základní schéma SIEM je rozděleno na šest oddělených částí nebo procesů. Těmi jsou zařízení, ze kterých sbíráme informace, získané informace v podobě logů, převedení logů do jednotného schématu, pravidla pro vyhodnocení, ukládání logů, vyhledání a monitoring záznamů. Jednotlivé části jsou schopny samostatného provozu, nicméně SIEM by bez nich jako celku nefungoval správně. [10]



Obrázek 2.7: Schéma SIEM. Převzato z [10], upraveno.

Zdroj

První částí SIEM jsou zařízení (počítače, routery, switche, firewally), aplikace (DNS, DHCP, webové servery, emailové služby) nebo jiný druh dat, ze kterých jsou získávány informace jako podklad pro vytvoření logů. Z pohledu SIEM jako samotné aplikace není toto zařízení jeho součástí, ale je zásadní pro funkčnost celého procesu. Před implementací je vhodné rozlišit, jaké informace a proč má smysl monitorovat, ať už z hlediska zvýšení bezpečnosti, nepřekročení kapacity zdrojů (lidských, výpočetního výkonu, kapacity úložiště), nebo legislativy. [10]

Sběr logů

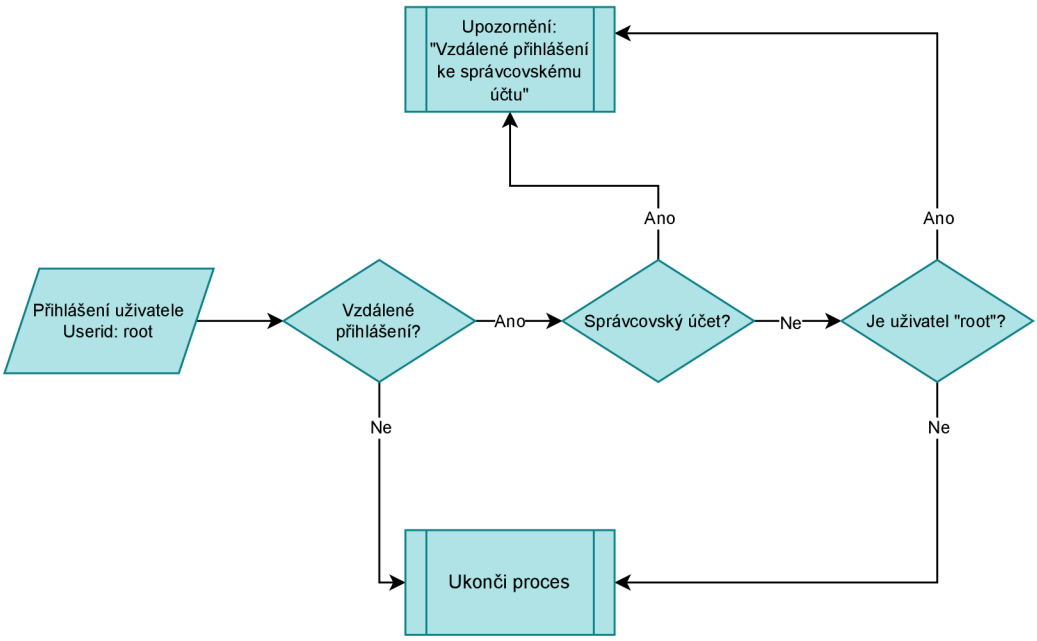
V tomto kroku je hlavním úkolem vygenerované logy importovat do SIEM. Způsoby načtení logů se liší podle jednotlivých aplikací, v principu však mohou být rozděleny na dvě základní metody. V prvním případě jsou logy odesílány samotným zařízením a jedná se o tzv. *push* metodu. *Pull* metodu iniciuje samotný SIEM, který se spojí se zařízením a od něj si logy vyžádá. Nevýhodou tohoto řešení může být fakt, že logy nebudou odesílány v reálném čase. [10]

Parsování a normalizace

Po naimportování logů z různých zdrojů do SIEM je nutné provést normalizaci. Výsledkem je jednotný formát logů bez ohledu na jejich původ. Díky tomu je snazší jejich čtení a tvorba pravidel. [10]

Vytváření pravidel

Pravidla obsahují podmínky, které jsou porovnávány s obsahem logů. V případě, kdy dojde ke shodě, SIEM vytvoří upozornění. Typicky jsou vytvářena pravidla postavená na Booleanově logice. [10]



Obrázek 2.8: Pravidla pro přihlášení administrátora. Převzato z [10], upraveno.

Uchování logů

Nejčastěji jsou využívány tři druhy uložení: v databázi, textovém souboru nebo binárním souboru. Ve většině případů jsou data ukládána v běžné databázi typu Oracle, MySQL nebo Microsoft SQL. [10]

Monitoring

Součástí SIEM je webové nebo aplikační rozhraní, s jehož pomocí můžeme zobrazit a analyzovat uložené logy v již normalizované podobě. [10]

Kapitola 3

Analýza současného stavu

Následující kapitola bude věnována analýze energetické společnosti a zasazení do legislativního kontextu. Kapitola vychází z poskytnutých materiálů a konzultací. Vzhledem k interním směrnicím společnosti a citlivosti informací budou data anonymizována. Dále budou analyzovány nástroje, které poskytují rámec pro hodnocení vycházející z matice ATT&CK.

3.1 Energetický trh

V České republice je hlavní legislativou upravující energetický trh zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon). Tímto zákonem byl zřízen Energetický regulační úřad, jehož hlavními činnostmi jsou [2]:

- Licencování a dozor energetických aktérů
- Regulace cen
- Ochrana spotřebitele

Energetický trh je rozdělen do tří odvětví: elektroenergetika, plynárenství a teplárenství. Licence jsou udělovány na základě písemné žádosti na dobu neurčitou, nejméně však 25 let, fyzickým nebo právnickým osobám. Podmínky pro udělení licence fyzické osobě jsou: věk alespoň 21 let, odborná a právní způsobilost a bezúhonnost.

V případě právnických osob musí tyto požadavky naplnit členové statutárního orgánu a dále je nutno určit odpovědného zástupce. Žadatel je také povinen prokázat, že disponuje finančními a technickými předpoklady a při výkonu činnosti neohrozí životy a zdraví osob, majetek nebo životní prostředí. [2]

Na trhu s elektřinou nalezneme mezi jeho účastníky výrobce, provozovatele přenosové soustavy, provozovatele distribučních soustav, operátora trhu, obchodníky s elektřinou a koncové zákazníky. Samotný trh je uskutečňován skrze zařízení elektrizační soustavy, jimiž jsou výrobny elektřiny, přenosové soustavy, distribuční soustavy, přímá vedení a elektrické přípojky. [2]

3.2 Základní informace o společnosti

Investorem je společnost, jež je zastoupena především na evropském trhu. V České republice působí jako několik samostatných subjektů, které spadají pod holdingovou společnost. Jednotlivé subjekty mají mezi sebou vymezené vztahy a na základě smluv si poskytují služby. Hlavními činnostmi jsou obchodování a výroba elektrické energie, výroba tepelné energie, provoz distribuční soustavy pro elektřinu, provoz datové infrastruktury a poskytování služeb.

Z hlediska legislativy kybernetické bezpečnosti vyplývají společnosti práva a povinnosti dle ZoKB a vyhlášky č. 82/2018 o kybernetické bezpečnosti. Na základě nařízení vlády č. 432/2010 Sb., a pozdějších znění se jedná o subjekt kritické infrastruktury.

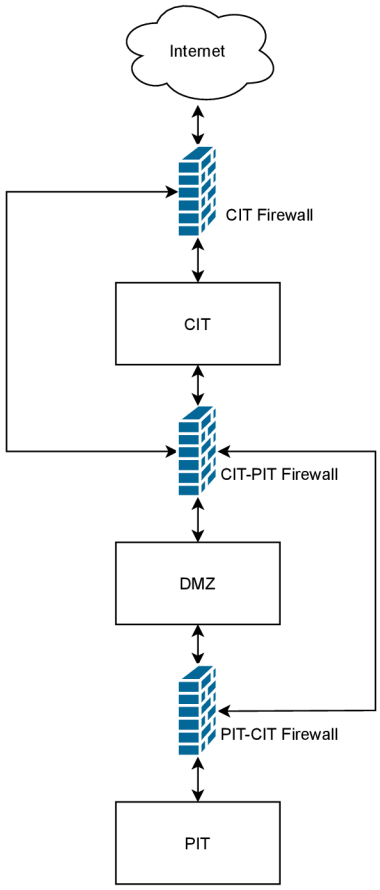
Společnost implementuje ISMS s ohledem na ZoKB a skupinovou směrnici řídící bezpečnost informací, která vychází z norem ISO/IEC 270xx. Cílem je zajištění důvěrnosti, dostupnosti a integrity informací, definování minimálních požadavků na ISMS, dále pak identifikace a hodnocení rizik.

Společnosti dále vyplývají práva a povinnosti z energetického zákona. Důležitým bodem je pak oddělení distribučních a přenosových soustav. [2]

3.3 Infrastruktura

Podle požadavků společnosti je infrastruktura rozdělena na dvě části: komerční a procesní, které jsou v rámci sítě odděleny. Zároveň jsou tak dodrženy požadavky na bezpečnost. Pro chod komerční infrastruktury jsou využívány komerční aplikace, pracovní počítače, mobilní výpočetní technika, tiskárny, faxy, datové servery a další informační systémy.

Procesní infrastruktura je vybavena technologiemi, které jsou nutné pro zajištění průmyslových procesů. V síti se vyskytují zařízení, jako jsou ochranná relé, programovatelné logické jednotky, řídicí terminály, průmyslové switche. Z legislativního i bezpečnostní hlediska je kladen důraz na dostupnost, proto je zajištěna redundance celého řešení. Jednotlivé komponenty průmyslového prostředí musí splňovat požadavky na náročnost provozních podmínek.



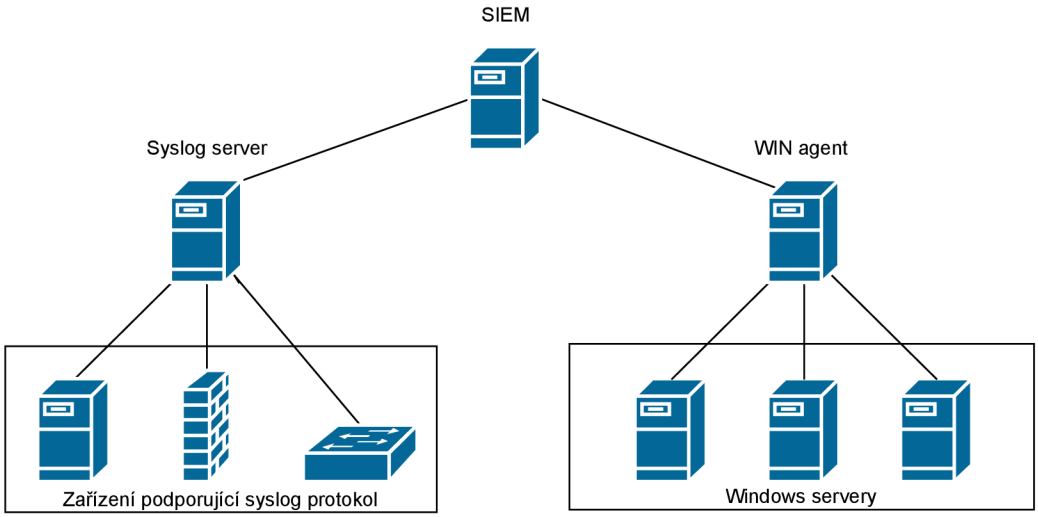
Obrázek 3.1: Schéma sítě

3.4 Sběr a vyhodnocování bezpečnostních událostí

Ze ZoKB vyplývá povinným osobám nutnost využívat nástroje sloužící pro sběr a vyhodnocování kybernetických bezpečnostních událostí (SIEM).

Architektura logování

SIEM přijímá nebo aktivně vyčítá logovací soubory z několika serverů (kolektorů). Záznamy jsou generovány na základě provozních událostí z koncových zařízení nebo bezpečnostních komponent, jako jsou IDS, firewally, či antiviry. Dále SIEM umožňuje monitorování síťového toku.



Obrázek 3.2: Architektura logování

Syslog

Syslog protokol je popsán ve specifikaci RFC 5424. Tento typ záznamů je generován síťovými a linuxovými zařízeními. Důležitými údaji z hlediska monitoringu jsou časová známka a priorita. Priorita je udávána na základě čísla zařízení (0-23) vynásobeného 8 a následným přičtením závažnosti.

Závažnost může být následující:

- Emergency(0): systém nelze použít
- Alert(1): je nutná okamžitá akce
- Critical(2): kritické podmínky
- Error(3): chyba
- Warning(4): varovné podmínky
- Notice(5): stojí za zmínku
- Informational(6): informační zpráva
- Debug(7): debugovací zpráva

Záznamy ze zařízení s operačním systémem Windows nemají formát syslogu. Závažnosti jsou definovány těmito stavy:

- Information: úspěšná akce
- Warning: událost, která by mohla způsobit problém
- Error: závažný problém
- Audit success
- Audit failure

Pravidla

Pravidla slouží pro analýzu záznamů v širším bezpečnostním kontextu. Umožňují vyhledávat konkrétní vzory a posloupnosti, které mohou indikovat bezpečnostní hrozby. Pravidla jsou rozdělena na dva typy: první sleduje události, druhý síťové toky. Skládají se z jednotlivých podmínek, které vytváří stavební bloky. Stavební bloky jsou využívány pro spojení podmínek, které jsou často užívané ve více pravidlech. V případě, kdy jsou definované podmínky splněny, dojde na základě pravidel k akci, například vygenerování upozornění.

3.5 Hodnocení monitoringu ve společnosti

Vzhledem k citlivosti informací popisuje následující kapitola problematiku na modelovém příkladu, který byl vytvořen na základě konzultace s CERT týmem.

Monitoring

Společnost rozděluje monitoring na přímý a nepřímý. Do přímého monitoringu jsou zahrnuty systémové logy:

- Logy systémové aktivity (např. administrátor) včetně úložišť
- Logy koncových zařízení (a agent-based)
- Logy ze standardních aplikací (např. SAP) a kustomizovaných aplikací
- Autentizační logy (např. Windows)
- Logy fyzické bezpečnosti
- SNMP logy

logy aplikací a služeb:

- HTTP, proxy logy
- DNS, DHCP a FTP logy
- Logy webových a SQL serverů

logy koncových bezpečnostních zařízení (monitorovacích a přihlašovacích nástrojů):

- Logy z ochran před malware (např. antivirus)
- Data loss protection (DLP)
- Nástroje, které zajišťují izolaci a zkoumání malware (např. sandbox, virtuální zařízení)
- Další relevantní bezpečnostní nástroje či zařízení

V nepřímém monitoringu jsou sledovány síťové IDS/IPS logy a logy síťových toků.

Každému typu monitoringu je při hodnocení přisuzována váha dle důležitosti. Jejich rozložení je následující:

- Systémové logy - 25 %
- Logy aplikací a služeb - 20 %
- Logy koncových bezpečnostních zařízení - 20 %
- Síťové IDS/IPS logy - 20 %
- Logy síťových toků - 15 %

Aktiva

Z hlediska bezpečnosti a dostupnosti dodávek elektrické energie je zásadní určit důležitost aktiv v daném prostředí. Ve společnosti jsou definovány 4 stupně důležitosti s různou váhou. V následující tabulce jsou popsána kritéria pro zařazení aktiv do jednotlivých stupňů:

Důležitost	Váha	Kritéria
Velmi vysoká	55 %	Aktiva, u kterých narušení důvěrnosti, dostupnosti a integrity může ohrozit existenci společnosti
Vysoká	35 %	Aktiva, u kterých narušení důvěrnosti, dostupnosti a integrity může vést k výrazným negativním důsledkům na procesy a aktivity společnosti
Střední	7 %	Aktiva, u kterých narušení důvěrnosti, dostupnosti a integrity může vést k postřehnutelným dopadům na procesy a aktivity společnosti, ale může být snadno zvládnuto
Nízká	3 %	Aktiva, u kterých narušení důvěrnosti, dostupnosti a integrity, může vést v nejhorších případech pouze k nevýznamnému (akceptovatelnému) negativnímu dopadu na procesy a aktivity společnosti

Tabulka 3.1: Kritéria pro zařazení aktiv dle důležitosti

Hodnocení

Před výpočtem celkového hodnocení monitoringu je nutné určit:

- Hodnocení kategorií aktiv
- Hodnocení pro každý stupeň důležitosti aktiv

Hodnocení kategorií aktiv

Pro výpočet pokrytí monitoringem jednotlivých kategorií je využíván následující postup:

1. Rozdělení aktiv do kategorií
2. Určení důležitosti kategorie (viz tabulka 3.1)
3. Určení celkového počtu aktiv pro každou kategorii
4. Určení počtu monitorovaných aktiv u jednotlivých typů monitoringu pro každou kategorii
5. Výpočet pokrytí monitoringem pro jednotlivé kategorie

V rámci kategorií jsou dále běžně ohodnocovány například servery, či firewally vyskytující se v DMZ. V tomto příkladu však nebudou uvažovány, protože nespadají do oblasti zaměření matice Mitre ATT&CK for ICS.

Výpočet skóre pro jednotlivé kategorie aktiv je prováděn níže uvedeným způsobem:

$$Skore = \left(\frac{MA_a}{CA} * a + \frac{MA_b}{CA} * b + \frac{MA_c}{CA} * c + \frac{MA_d}{CA} * d + \frac{MA_e}{CA} * e \right)$$

- CA - celkový počet aktiv
- MA - monitorovaná aktiva
- a - Systémové logy [25 %]
- b - Logy aplikací a služeb [20 %]
- c - Logy koncových bezpečnostních zařízení [20 %]
- d - Síťové IDS/IPS logy [20 %]
- e - Logy síťových toků [15 %]

V případě, kdy není možné některý z typů monitoringu provádět (například z důvodu dopadu na výkon strojů), je výpočet upraven a jeho váha je rovnoměrně rozdělena mezi ostatní. V následujícím příkladu nejsou využívány logy aplikací a služeb a logy koncových bezpečnostních zařízení:

$$Skore = \left[\frac{MA_a}{CA} * \left(a + \left(\frac{b+c}{3}\right)\right) + \frac{MA_d}{CA} * \left(d + \left(\frac{b+c}{3}\right)\right) + \frac{MA_e}{CA} * \left(e + \left(\frac{b+c}{3}\right)\right)\right]$$

Kategorie	Důležitost	CA	(a) 25 %	(b) 20 %	(c) 20 %	(d) 20 %	(e) 15 %	Skóre
Centrální SCADA	Velmi vysoká	152	152	152	N/A	152	152	100 %
Rozvodna typ 1	Velmi vysoká	1050	558	N/A	N/A	558	558	53,14 %
Rozvodna typ 2	Střední	2800	0	N/A	N/A	1400	1400	23,33 %

Tabulka 3.2: Hodnocení kategorií aktiv

Hodnocení stupňů důležitosti aktiv

Hodnocení pro každý stupeň důležitosti je vypočteno aritmetickým průměrem součtů skóre kategorií aktiv s danou důležitostí.

$$C_{vv} = \frac{\sum(Skore_{vv})}{n_{vv}}$$

- C_{vv} - Hodnocení stupně důležitosti velmi vysoká
- $Skore_{vv}$ - Skóre kategorie aktiv s důležitostí velmi vysoká
- n_{vv} - Počet kategorií aktiv s důležitostí velmi vysoká

Důležitost	CA	(a) 25 %	(b) 20 %	(c) 20 %	(d) 20 %	(e) 15 %	Skóre
Celkem velmi vysoká	1202	710	152	0	710	710	76,57
Celkem vysoká	0	0	0	0	0	0	0
Celkem střední	2800	0	0	0	1400	1400	23,33
Celkem nízká	0	0	0	0	0	0	0

Tabulka 3.3: Hodnocení stupňů důležitosti aktiv

Celkové hodnocení monitoringu

Celkové hodnocení monitoringu je určeno součtem násobků důležitosti kategorie aktiv a hodnocením stupně aktiv.

$$M = C_{vv} * D_{vv} + C_v * D_v + C_s * D_s + C_n * D_n$$

- M - Celkové hodnocení monitoringu
- C_{vv} - Celkem velmi vysoká
- D_{vv} - Důležitost velmi vysoká
- C_v - Celkem vysoká
- D_v - Důležitost vysoká
- C_s - Celkem střední
- D_s - Důležitost střední
- C_n - Celkem nízká
- D_n - Důležitost nízká

Modelový příklad neobsahuje aktiva s důležitostí vysoká a nízká. V tomto případě je celkové skóre monitoringu vypočítáno na základě váženého průměru.

$$M = \frac{C_{vv} * D_{vv} + C_s * D_s}{D_{vv} + D_s}$$

Důležitost	%	Skóre	Skóre*důležitost %
Celkem velmi vysoká	55 %	76,57 %	42,11 %
Celkem vysoká	35 %	0 %	0 %
Celkem střední	7 %	23,33 %	1,63 %
Celkem nízká	3 %	0 %	0 %
M =			71,00 %

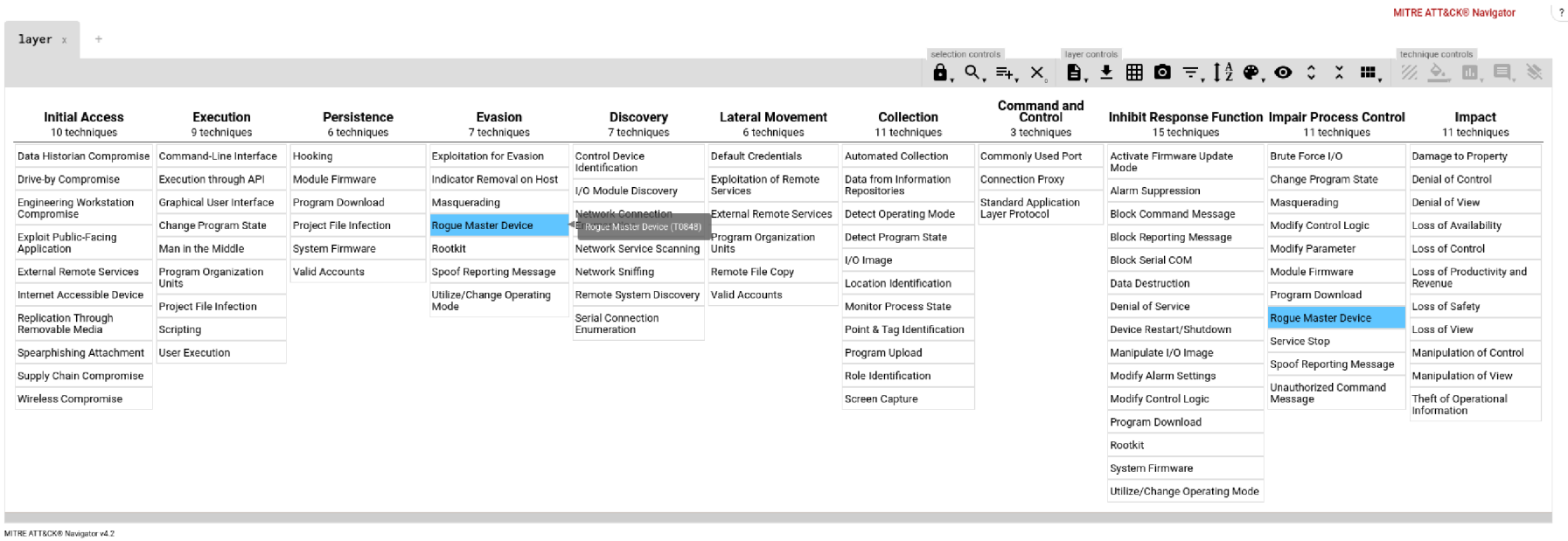
Tabulka 3.4: Celkové hodnocení monitoringu

3.6 Řešení vycházející z matice Mitre ATT&CK

ATT&CK Navigator

ATT&CK Navigator je nástroj, který umožňuje podrobnější vizualizaci matic ATT&CK (Enterprise, Mobile, ICS). Využit může být například k zobrazení pokrytí obrany, pro plánování cvičení red/blue teaming, sledování četnosti detekovaných technik aj. Umožňuje úpravu buněk matice, jako je například barevné kódování, přidání komentáře, či přiřazení číselných hodnot. Navigátor poskytuje možnost definování vrstev, pomocí kterých jsou vytvářeny vlastní pohledy. Zobrazeny tak mohou být pouze techniky relevantní pro danou platformu nebo konkrétního útočníka. Vrstvy je možné vytvořit přímo v Navigatoru nebo programově a následně je pomocí Navigatoru zobrazit. [11]

Navigator je opensource platforma hostovaná skrze github, zároveň však poskytuje možnost lokální instalace, která je doporučována v případě práce s citlivým obsahem. Podporovanými prohlížeči jsou Chrome, Firefox, Internet Explorer 11, Edge a Opera. [11]



Obrázek 3.3: ATT&CK Navigator. Převzato z [11].

DeTT&CT

Cílem projektu DeTT&CT (Detect Tactics, Techniques & Combat Threats) je poskytnout CERT týmům nástroj pro hodnocení kvality datových zdrojů, pokrytí viditelnosti, detekce a chování útočníků, za využití matice MITRE ATT&CK for Enterprise. Součástí řešení jsou: nástroj vytvořený v jazyce Python, soubory ve formátu YAML[1], DeTT&CT editor a skórovací tabulky. Funkcionalitami, které je možno využít, jsou: [4]

- Správa a ohodnocení kvality datový zdrojů
- Získání přehledu o viditelnosti
- Mapování pokrytí detekce
- Mapování chování útočníků
- Porovnání viditelnosti, detekce a chování útočníků, které umožní odhalit místa pro zlepšení a prioritizovat tak oblasti zaměření CERT týmu [4]

DeTT&CT nabízí tři módy pro ovládání: [4]

- Příkazový řádek
- Interaktivní menu
- DeTT&CT editor[4]

Příkazový řádek

V příkazovém řádku je možné zvolit pět módů a několik volitelných argumentů. Základní výpis příkazového řádku je uveden v následujícím textu: [4]

```
usage: dettect.py [-h] [--version] [-i]  ...

Detect Tactics, Techniques & Combat Threats

optional arguments:
  -h, --help         show this help message and exit
  --version          show program's version number and exit
  -i, --interactive  launch the interactive menu, which has support for all
```

[1]YAML je serializační jazyk, který je čitelný jak strojem, tak člověkem. V DeTT&CTu jsou YAML soubory využívány pro správu hodnocení a metadat.

```
                    modes

MODE:
  Select the mode to use. Every mode has its own arguments and help info
  displayed using: {editor, datasource, visibility, detection, group,
  generic} --help


    editor (e)       DeTT&CT Editor
    datasource (ds)  data source mapping and quality
    visibility (v)   visibility coverage mapping based on techniques and data
                     sources
    detection (d)    detection coverage mapping based on techniques
    group (g)        threat actor group mapping
    generic (ge)     includes: statistics on ATT&CK data source and updates on
                     techniques, groups and software
```

Interaktivní menu

Interaktivní menu obsahuje všechny módy jako příkazový řádek, ale nejsou zde dostupné veškeré argumenty.[4]

```
dettect.py [-i]

                  -= DeTT&CT =-
-- Detect Tactics, Techniques & Combat Threats --
                  version 1.4.2

Select a~mode:
1. Data source mapping
2. Visibility coverage mapping
3. Detection coverage mapping
4. Threat actor group mapping
5. Updates
6. Statistics
7. Quit
```

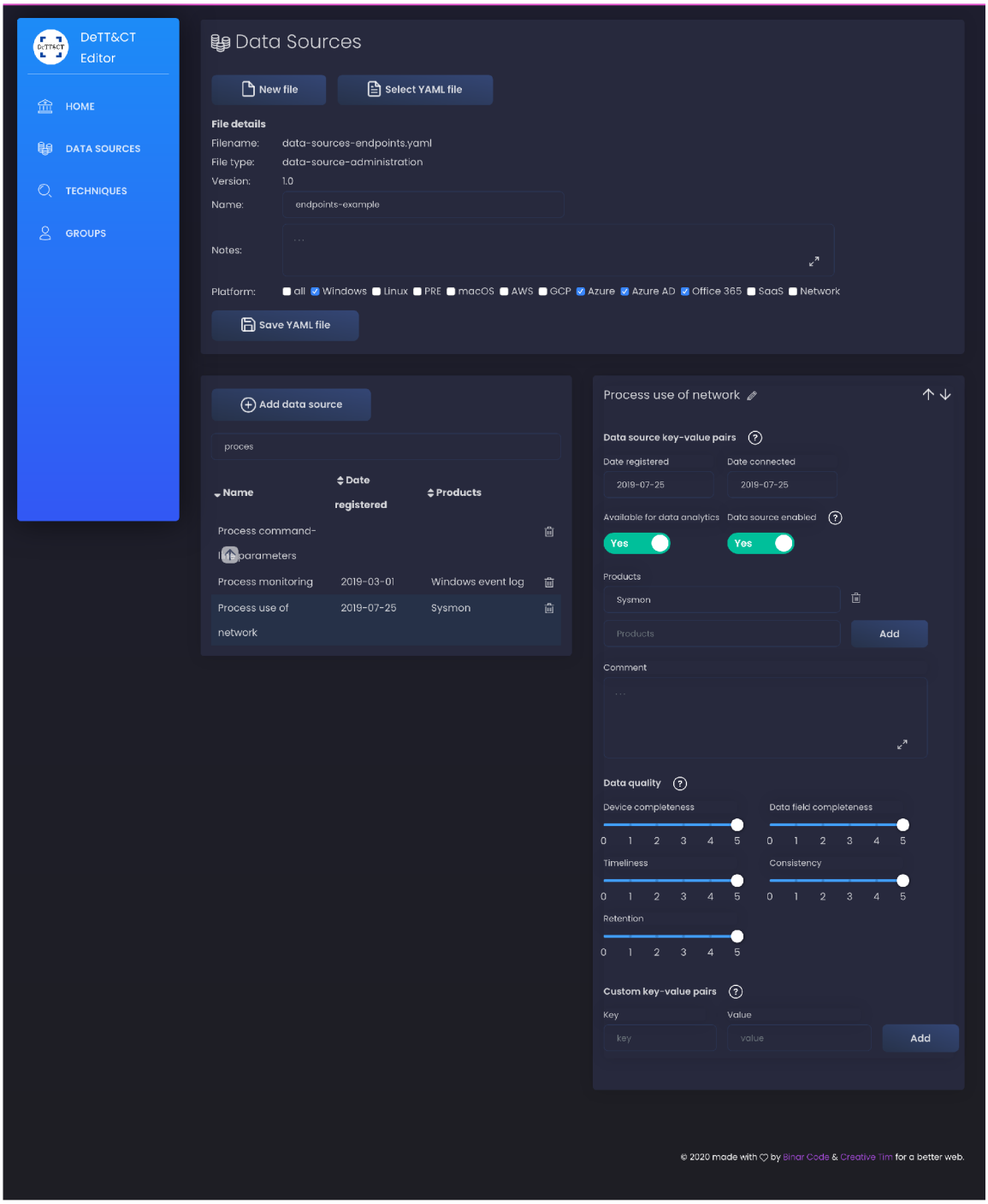
```
                  -= DeTT&CT =-
-- Detect Tactics, Techniques & Combat Threats --
                  version 1.4.2

Menu: Data source mapping

Select the YAML file with data sources:
```

```
Path: sample-data/
1. sample-data/data-sources-endpoints.yaml
2. sample-data/techniques-administration-endpoints.yaml
3. sample-data/data-sources-empty.yaml
4. sample-data/groups.yaml
8. Change path
9. Back to main menu.
```

DeTT&CT editor

V editoru jsou upravovány soubory YAML, obsahující zdrojová data, techniky a skupiny. Hostován je na platformě GitHub nebo může být spuštěn lokálně po zadání příkazu: [4]

```
python dettect.py editor
```



Obrázek 3.4: DeTT&CT editor. Převzato z [4].

Zdrojová data

Zdrojovými daty jsou logy nebo události generované systémy, bezpečnostními či síťovými zařízeními apod. V matici ATT&CK for Enterprise je jich definováno přibližně 60 (například zachycování paketů, monitorování souborů) a rámec DeTT&CT je přebírá. Tato zdrojová data jsou spravována v YAML souboru. Rámec nabízí hodnocení kvality pro každý datový zdroj. V rámci kvality je sledováno pět parametrů: [4]

- Device completeness - hodnotí, zda jsou požadovaná data dostupná ze všech zařízení
- Data field completeness - hodnotí, zda jsou dostupná požadovaná pole a zda obsahují potřebná data
- Timeliness - hodnotí, kdy jsou data dostupná a jaký je rozdíl mezi časovou známkou a reálným časem nastalé události
- Consistency - hodnotí standardizaci názvů datových polí a datových typů
- Retention - porovnává, po jakou dobu jsou data uchovávána vzhledem k požadovanému časovému období [4]

Následující tabulka definuje podmínky pro přiřazení daného skóre jednotlivým parametrům: [4]

Skóre	Device completeness	Data field completeness	Timeliness	Consistensy	Retention
0 - žádná	Nevím/ neaplikovatelné.	Nevím/ neaplikovatelné.	Nevím/ neaplikovatelné.	Nevím/ neaplikovatelné.	Nevím/ neaplikovatelné.
1 - slabá	Zdroje dat jsou dostupné z 1-25 % zařízení.	Požadované hodnoty jsou dostupné z 1-25 %.	Trvá dlouho, než jsou data dostupná. Mezi časovou známkou dat a událostí je velká prodleva.	1-50 % polí má standardizovaný název a typ.	Doba uchování dat pokrývá 1-25 % požadovaného časového období.
2 - dostatečná	Zdroje dat jsou dostupné z 26-50 % zařízení.	Požadované hodnoty jsou dostupné z 26-50 %.			Doba uchování dat pokrývá 26-50 % požadovaného časového období.
3 - dobrá	Zdroje dat jsou dostupné z 51-75 % zařízení.	Požadované hodnoty jsou dostupné z 51-75 %.	Data nejsou dostupná hned, ale prodleva je akceprovatelná. Mezi časovou známkou dat a událostí je malá prodleva.	51-99 % polí má standardizovaný název a typ.	Doba uchování dat pokrývá 51-75 % požadovaného časového období.
4 - velmi dobrá	Zdroje dat jsou dostupné ze 76-99 % zařízení.	Požadované hodnoty jsou dostupné z 76-99 %.			Doba uchování dat pokrývá 76-99 % požadovaného časového období.
5 - výborná	Zdroje dat jsou dostupné ze 100 % zařízení.	Požadované hodnoty jsou dostupné z 100 %.	Data jsou dostupná hned. Časová známka dat je 100 % přesná.	100 % polí má standardizovaný název a typ.	Data jsou uchovávána po celou dobu požadovaného časového období.

Tabulka 3.5: Parametry pro hodnocení zdrojových dat, převzato z [4], upraveno

V souboru YAML je hodnocení datových zdrojů ukládáno následujícím způsobem:[4]

```
- data_source_name: Process monitoring
  date_registered: 2019-03-01
  date_connected: 2017-01-01
  products: [Windows event log]
  available_for_data_analytics: True
  comment: ''
  data_quality:
  device_completeness: 5
  data_field_completeness: 5
  timeliness: 5
  consistency: 5
```

Pokrytí viditelnosti

V návaznosti na hodnocení zdrojů dat je možné určit hrubý odhad viditelnosti pro každou techniku. Druhým přístupem je využití hodnocení zdrojů dat a následného hodnocení viditelnosti expertním odhadem na základě následujících parametrů: [4]

Skóre	Popis
0 - žádná	Žádná viditelnost
1 - nízká	Dostačující zdroje dat s dostatečnou kvalitou pokrývají jeden aspekt procedury v rámci techniky
2 - střední	Dostačující zdroje dat s dostatečnou kvalitou pokrývají více než jeden aspekt procedury v rámci techniky
3 - dobrá	Dostačující zdroje dat s dostatečnou kvalitou umožňují pokrytí téměř všech známých procedur v rámci techniky
4 - výborná	Zdroje dat a požadovaná kvalita poskytují pokrytí všech známých procedur v rámci techniky

Tabulka 3.6: Parametry pro hodnocení pokrytí viditelnosti. Převzato z [4], upraveno.

Pokrytí detekce

Hodnocení detekce závisí na expertním odhadu posuzovatele, který dle parametrů v následující tabulce hodnotí úroveň detekce, pokrytí techniky z hlediska jejich zná-

mých aspektů, výskytu případů false negative či false positive, možnosti vyhnutí se detekci a zda probíhá detekce v reálném čase. [4]

Skóre	Úroveň detekce	Čas	Pokrytí techniky	Možnost vyhnutí se detekci	False negatives	False positives
-1 - žádná	Žádná detekce	N/A	Žádná	N/A	N/A	N/A
0 - forenzní/ kontext	Žádná	Pravděpodobně ne v reálném čase	Žádná	N/A	N/A	N/A
1 - základní	Založena na signaturách	Pravděpodobně ne v reálném čase	Malé množství aspektů techniky	Vyhnutí se je možné	Velmi mnoho	Pravděpodobně mnoho
2 - uspokojivá	Pravidla (Korelace)	Pravděpodobně ne v reálném čase	Více aspektů techniky oproti úrovni 1/Základní	Vyhnutí se je možné	Mnoho	Mohou být přítomé
3 - dobrá	Více komplexní analýza	V reálném čase	Mnoho známých aspektů techniky	Vyhnutí se je možné	Jsou přítomné	Mohou být přítomné, ale jsou snadno rozpoznatelné a lze je vytřídit.
4 - velmi dobrá	Více komplexní analýza	V reálném čase	Téměř všechny známé aspekty techniky	Vyhnutí se je náročné	Málo	Mohou být přítomné, ale jsou snadno rozpoznatelné a lze je vytřídit.
5 - výborná	Více komplexní analýza	V reálném čase	Všechny známé aspekty techniky	Vyhnutí se je náročné	Velmi málo	Mohou být přítomné, ale jsou snadno rozpoznatelné a lze je vytřídit.

Tabulka 3.7: Parametry pro hodnocení pokrytí detekce. Převzato z [4], upraveno.

Mapování útočníků

Při mapování útočníků jsou vybírány jednotlivé techniky, které jsou využívány během útoků. Mapování může být prováděno několika způsoby v závislosti na požadovaném výsledku, kterým může být: [4]

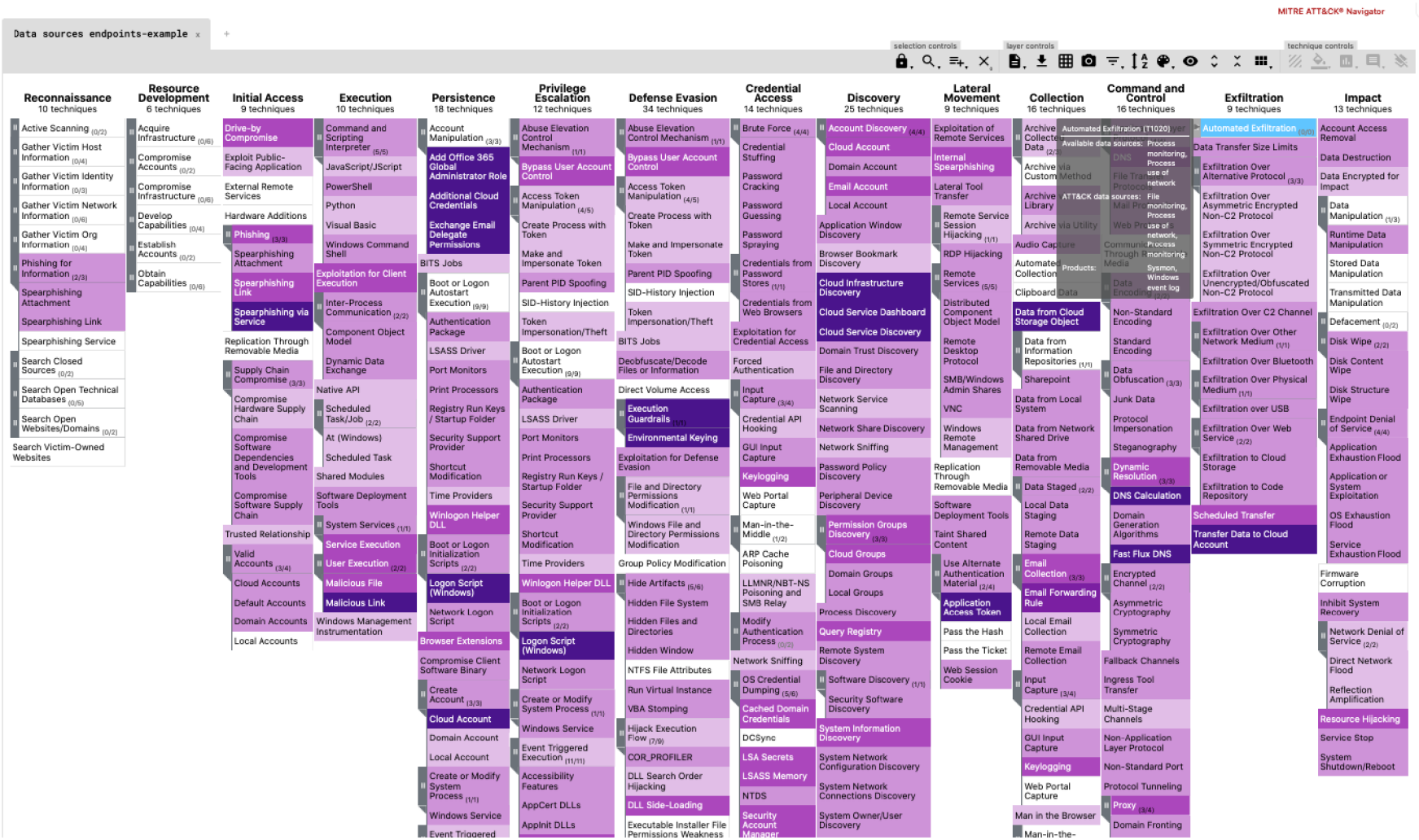
- Celkový přehled všech útočníků, kteří jsou evidováni v matici ATT&CK for Enterprise ve formě heat mapy
- Vytváření přehledu z vybrané části útočníků evidovaných ATT&CK for Enterprise ve formě heat mapy
- Vytváření vlastního přehledu na základě znalostí z týmu threat intelligence, nebo na základě technik použitých red týmem při cvičeních
- Porovnání útočníky používaných technik s naměřenou úrovní pokrytí viditelnosti nebo detekce
- Porovnání různých skupin útočníků
- Vizualizace možných postupů útočníka na základě jím užívaného software[4]

V YAML souboru mohou být zaznamenávány následující informace: [4]

- Jméno útočníka
- Kampaň
- Techniky užité útočníkem v rámci kampaně
- Použitý software v rámci kampaně
- Značka, zda je útočník povolen při načítání YAML souboru (ovlivní, zda bude zahrnut ve vizualizaci pomocí Navigatoru) [4]

Vizualizace

DeTT&CT umožňuje konverzi souborů s hodnocením do formátu JSON, který lze následně importovat do ATT&CK Navigatoru. Tímto způsobem mohou být vizualizovány výsledky pokrytí datových zdrojů, viditelnosti, detekce i chování útočníků ve formě heat mapy. [4]



Obrázek 3.5: Vizualizace pokrytí zdrojů dat. Převzato z [4].

Sigma

Sigma je obecný otevřený formát, jehož hlavním cílem je poskytnout CERT týmům jednotný strukturovaný nástroj, kterým budou schopni popsat své detekční metody a sdílet je s ostatními týmy. Formát pravidel je flexibilní, jednoduchý na vytvoření a aplikovatelný na jakýkoliv druh logů. Součástí řešení je úložiště již vytvořených pravidel přiřazených k technikám MITRE ATT&CK for Enterprise a konvertor, který převádí Sigma pravidla do formátu jiných nástrojů. [18]

Pravidla

Sigma pravidla jsou vytvořena v jazyce YAML a obsahují následující data: [18]

1. Metadata
    - Název, status, popis, reference, tagy (propojení s Mitre ATT&CK) atd.
2. Zdroje dat
    - Z jakého typu zařízení a služby log pochází
3. Detekce
    - Seznam polí
4. Podmínky
    - Jaké podmínky musí být splněny (alespoň 1/všechny...) [18]

Následující příklad uvádí Sigma pravidlo pro detekci Mimikatz:

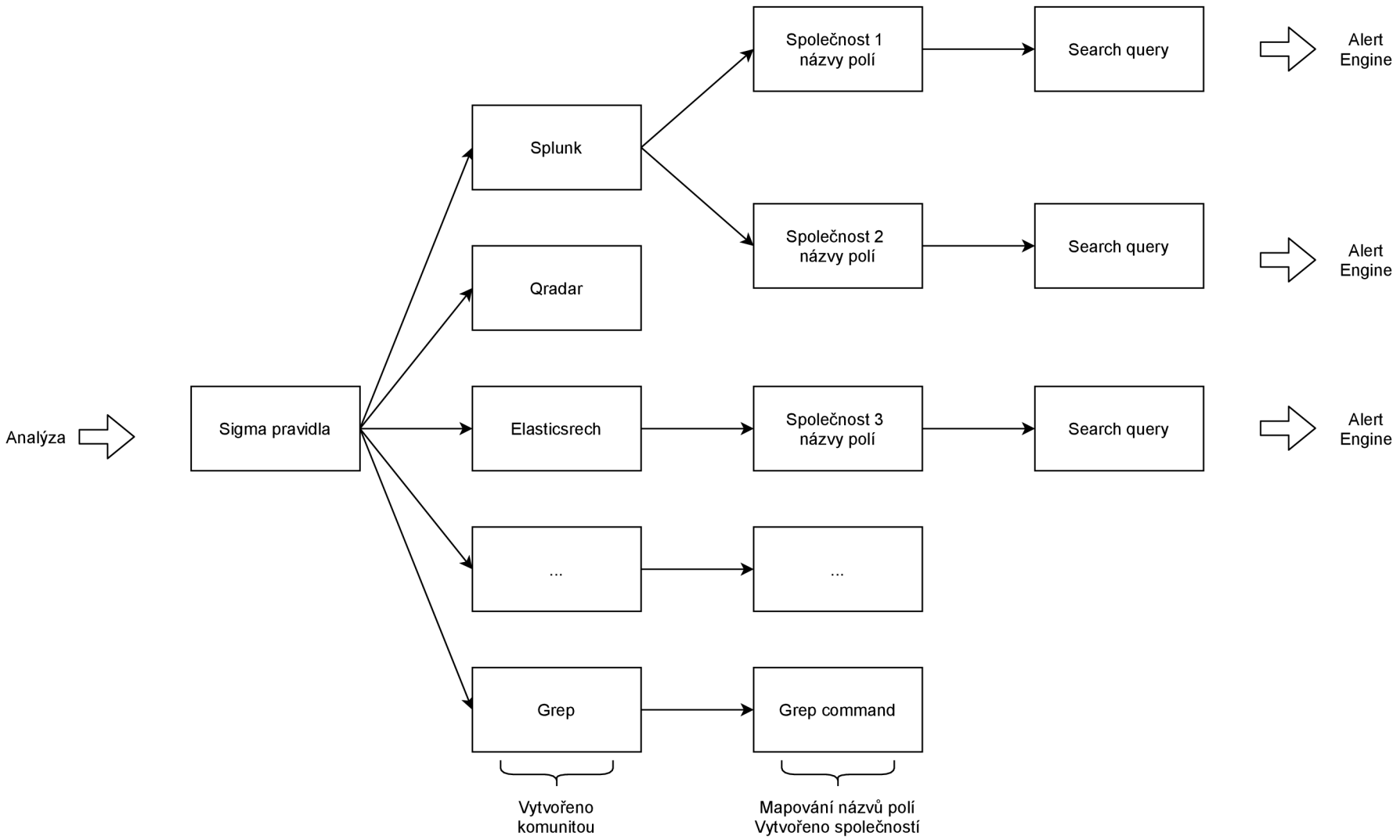
```
title: Mimikatz Detection LSASS Access
id: 0d894093-71bc-43c3-8c4d-ecfc28dcf5d9
status: experimental
description: Detects process access to LSASS which is typical for Mimikatz
  (0x1000 PROCESS_QUERY_ LIMITED_INFORMATION,
   0x0400 PROCESS_QUERY_INFORMATION "only old versions",
   0x0010 PROCESS_VM_READ)
tags:
- attack.t1003
- attack.s0002
- attack.credential_access
- car.2019-04-004
```

```
author: Sherif Eldeeb
date: 2017/10/18
logsource:
product: windows
service: sysmon
detection:
selection:
EventID: 10
TargetImage: 'C:\windows\system32\lsass.exe'
GrantedAccess:
- '0x1410'
- '0x1010'
condition: selection
fields:
- ComputerName
- User
- SourceImage
falsepositives:
- Some security products access LSASS in this way.
level: high
```

Sigmac

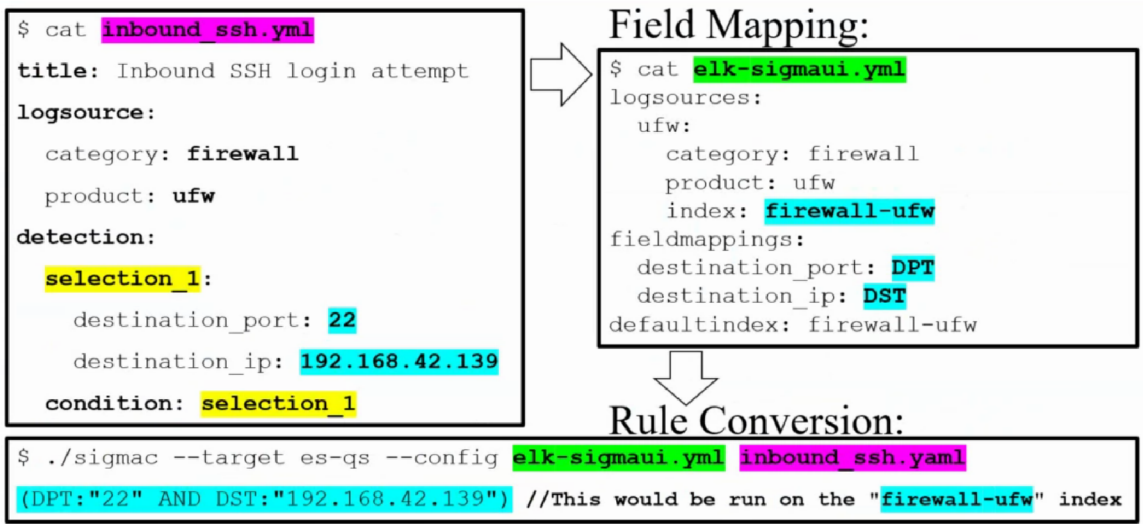
Nástroj Sigmac slouží k převádění pravidel na dotazy nebo vstupy do formátu podporovaných platforem. Těmi jsou například:[18]

- Splunk (plainqueries and dashboards)
- ElasticSearch Query Strings
- ElasticSearch Query DSL
- Kibana
- Elastic X-Pack Watcher
- Logpoint
- Microsoft Defender Advanced Threat Protection (MDATP)
- Azure Sentinel / Azure Log Analytics
- Sumologic
- ArcSight
- QRadar
- Qualys [18]



Obrázek 3.6: Konverze signatur na alert queries. Převzato z [7], upraveno.

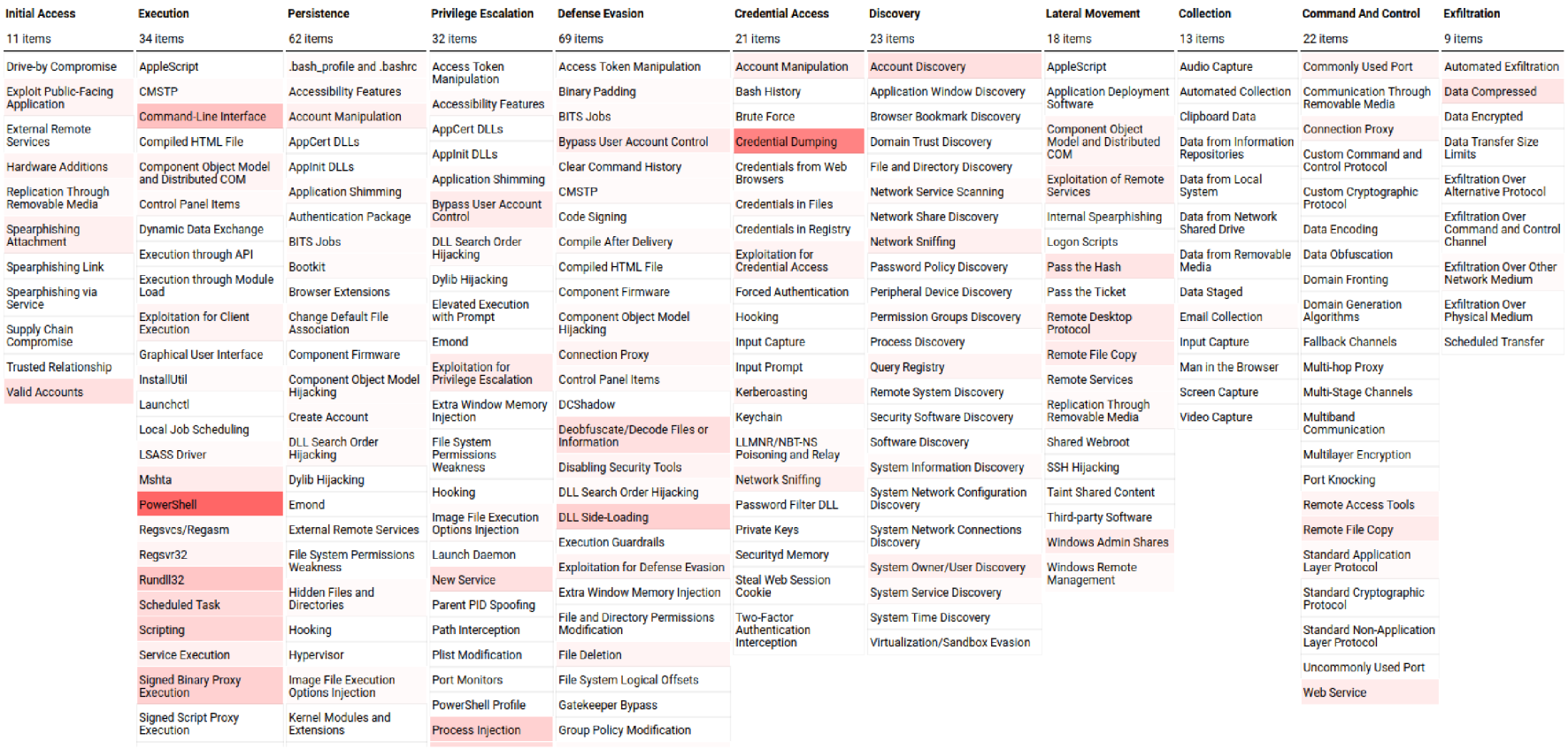
Konverze pravidel prochází dvěma stupni. První stupeň probíhá za pomoci Sigmac, který převede Sigma pravidla do předdefinovaného formátu dle požadované platformy. V druhé úrovni je nutné provést mapování názvů polí, které jsou v daném systému používány. [18]



Obrázek 3.7: Mapování názvů polí. Převzato z [7].

Sigma2attack

Nástroj Sigma2attack generuje ze složky obsahující sigma pravidla soubor, který lze importovat do ATT&CK Navigatoru. Tímto způsobem lze vizualizovat pokrytí pravidel v rámci matice. Pravidla musí obsahovat tag ve formátu attack.tXXXX (například attack.t1086). [18]



Obrázek 3.8: Vizualizace Sigma2attack. Převzato z [18].

3.7 Zhodnocení

Výše zmíněná řešení vycházející z matice Mitre ATT&CK jsou nástroje, jež mohou CERT týmům posloužit jako doplněk hodnocení monitoringu a zároveň mohou za pomoci vizualizace nástrojem ATT&CK Navigator usnadnit komunikaci s managementem, či sdílení výsledků s jinými týmy.

Nevýhodou řešení DeTT&CT je závislost na expertním odhadu, tedy úrovni znalostí hodnotitele. Další překážkou tohoto řešení je zaměření pouze na matici Enterprise. Jeho využití je tak omezeno pouze na IT prostředí. Pokud by podniky monitorující průmyslové prostředí chtěly tento způsob hodnocení využít (zaměření na matici ICS), musely by upravit zdrojový kód nástroje, nebo vytvořit svůj vlastní.

S primárním zaměřením na matici Enterprise se setkáme i u nástroje Sigma. Zde to však díky obecnému formátu pravidel nepředstavuje zásadní problém. Při mapování technik je jedinou nutností zadat tagy definované maticí ICS a při vizualizaci upravit JSON soubor tak, aby Navigator pracoval se správnou maticí.

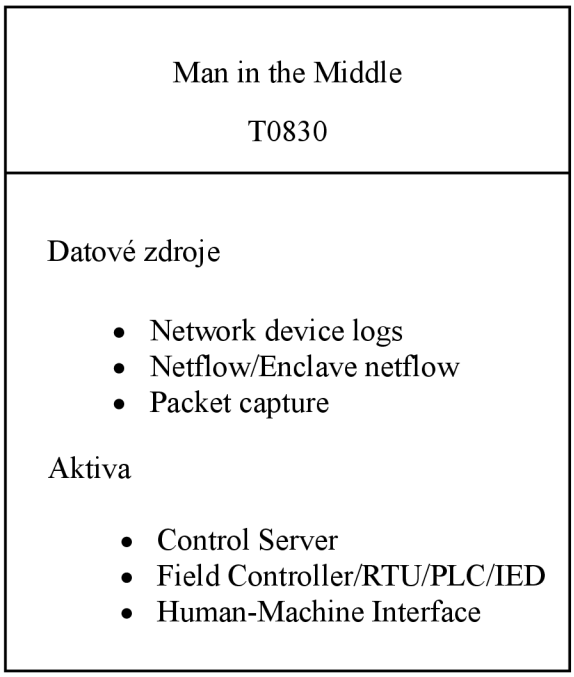
Velkým kladem je, že všechna tato řešení jsou doporučována v rámci bezpečnostní komunity a jsou jí využívána. Zmiňována jsou také organizací SANS Institute, která poskytuje školení a certifikace profesionálů v oblasti kybernetické bezpečnosti (jedná se například o penetrační testování, etické hackování, bezpečnostní management, audit, bezpečnost průmyslových řídicích systémů).

Po konzultaci s CERT týmem byl vznesen požadavek pro kvantitativní hodnocení monitoringu v rámci matice. Kapitola 3.5 bude proto použita jako vstup pro výpočty při návrhu vlastního řešení.

Kapitola 4

Vlastní návrh řešení

Vlastní návrh řešení bude vycházet z modelového příkladu v kapitole 3.5 a bude popsán na technikách Man in the Middle a Program Download.



Obrázek 4.1: Man in the Middle - ATT&CK for ICS. Převzato z [3], upraveno.

Pro hodnocení efektivity systému SIEM vycházející z matice Mitre ATT&CK for ICS je navržen následující postup:

1. Výběr relativních technik
2. Dekompozice aktiv
3. Mapování datových zdrojů
4. Ohodnocení vybraných technik
5. Mapování na detekční pravidla
6. Vizualizace výsledků

4.1 Výběr relevantních technik

Vzhledem k rozsáhlosti matice a časové náročnosti na její celkové ohodnocení bude CERT týmu doporučeno vybrat relevantní techniky pro dané prostředí. Techniky je možné ohodnotit z pohledu důležitosti, a tím dále prioritizovat oblast zaměření.

4.2 Dekompozice aktiv

Z pohledu matice jsou aktiva rozdělena na skupiny aktiv, jimiž jsou:

- Control Server
- Data Historian
- Engineering Workstation
- Field Controller/RTU/PLC/IED
- Human-Machine Interface
- Input/Output Server
- Safety Instrumented System/Protection Relay

Společnost v rámci hodnocení monitoringu určuje kategorie aktiv, které neposkytují dostatečně detailní pohled. Proto bude nutné jednotlivé kategorie dekomponovat.

Kategorie aktiv Rozvodna typ 1 bude po dekompozici obsahovat tato aktiva:

- HMI
- RTU
- PLC
- Ochranná relé
- Převodníky

Následně budou dekomponovaná aktiva namapována na skupiny aktiv v matici:

- HMI -> Human-Machine Interface
- RTU -> Field Controller/RTU/PLC/IED
- PLC -> Field Controller/RTU/PLC/IED
- Ochranná relé -> Safety Instrumented System/Protection Relay
- Převodníky -> Input/Output Server

Kategorie aktiv	Důležitost	CA	(a)	(b)	(c)	(d)	(e)	Skupina aktiv v ATT&CK
Centrální SCADA		152			x			
Řídicí server - Control Server	velmi vysoká	28	28	28	x	28	28	Control Server
Řídicí server - Data Historian	velmi vysoká	4	4	4	x	4	4	Data Historian
Řidicí server - HMI	velmi vysoká	60	60	60	x	60	60	Human-Machine Interface
Engineering workstation	velmi vysoká	60	60	60	x	60	60	Engineering Workstation
Rozvodna typ 1		1050		x	x			
HMI	velmi vysoká	60	32	x	x	32	32	Human-Machine Interface
RTU	velmi vysoká	90	48	x	x	48	48	Field Controller/RTU/PLC/IED
PLC	velmi vysoká	60	32	x	x	32	32	Field Controller/RTU/PLC/IED
Ochranná relé	velmi vysoká	750	398	x	x	398	398	Safety Instrumented System/Protection Relay
Převodníky	velmi vysoká	90	48	x	x	48	48	Input/Output Server
Rozvodna typ 2		2800		x	x			
HMI	střední	160	0	x	x	80	80	Human-Machine Interface
RTU	střední	240	0	x	x	120	120	Field Controller/RTU/PLC/IED
PLC	střední	160	0	x	x	80	80	Field Controller/RTU/PLC/IED
Ochranná relé	střední	2000	0	x	x	1000	1000	Safety Instrumented System/Protection Relay
Převodníky	střední	240	0	x	x	120	120	Input/Output Server

Tabulka 4.1: Dekompozice kategorií aktiv na skupiny aktiv matice

Human-Machine Interface		
	Počet monitorovaných aktiv	
Systémové logy	32	
Logy aplikací a služeb	x	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	32	
Logy síťových toků	32	
Celkový počet aktiv		60
Field Controller/RTU/PLC/IED		
Systémové logy	80	
Logy aplikací a služeb	x	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	80	
Logy síťových toků	80	
Celkový počet aktiv		150
Safety Instrumented System/Protection Relay		
Systémové logy	398	
Logy aplikací a služeb	x	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	398	
Logy síťových toků	398	
Celkový počet aktiv		750
Input/Output Server		
Systémové logy	48	
Logy aplikací a služeb	x	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	48	
Logy síťových toků	48	
Celkový počet aktiv		90

Tabulka 4.2: Dekompozice aktiv Rozvodna typ 1

Control Server		
	Počet monitorovaných aktiv	
Systémové logy	28	
Logy aplikací a služeb	28	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	28	
Logy síťových toků	28	
Celkový počet aktiv		28
Data Historian		
Systémové logy	4	
Logy aplikací a služeb	4	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	4	
Logy síťových toků	4	
Celkový počet aktiv		4
Human-Machine Interface		
Systémové logy	60	
Logy aplikací a služeb	60	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	60	
Logy síťových toků	60	
Celkový počet aktiv		60
Engineering Workstation		
Systémové logy	60	
Logy aplikací a služeb	60	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	60	
Logy síťových toků	60	
Celkový počet aktiv		60

Tabulka 4.3: Dekompozice aktiv Centrální SCADA

Human-Machine Interface		
Počet monitorovaných aktiv		
Systémové logy	0	
Logy aplikací a služeb	x	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	80	
Logy síťových toků	80	
Celkový počet aktiv		160
Field Controller/RTU/PLC/IED		
Systémové logy	0	
Logy aplikací a služeb	x	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	200	
Logy síťových toků	200	
Celkový počet aktiv		400
Safety Instrumented System/Protection Relay		
Systémové logy	0	
Logy aplikací a služeb	x	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	1000	
Logy síťových toků	1000	
Celkový počet aktiv		2000
Input/Output Server		
Systémové logy	0	
Logy aplikací a služeb	x	
Logy koncových bezpečnostních zařízení	x	
Síťové IDS/IPS logy	0	
Logy síťových toků	120	
Celkový počet aktiv		240

Tabulka 4.4: Dekompozice aktiv Rozvodna typ 2

4.3 Mapování datových zdrojů

Datové zdroje matice budou CERT týmem namapovány dle typů monitoringu v kapitole 3.5. Pro celkové hodnocení techniky pak poslouží především jako vodítko, které typy monitoringu je vhodné v rámci techniky sledovat. Detailnější pohled na monitoring nedává smysl ve společnosti provádět. Proto je zvolen tento postup, který alespoň částečně zpřesní výpočet oproti pouhému porovnání množství celkových a monitorovaných aktiv. Zároveň nemusí být některé datové zdroje matice v daném prostředí monitoringem sledovány. V tomto případě se jedná například o Alarm history či Alarm tresholds, které jsou řešeny provozem a nebudou tak při hodnocení monitoringu brány v potaz.

Datové zdroje ATT&CK for ICS	Datové zdroje prostředí
Alarm history	Není v daném prostředí řešeno
Alarm thresholds	Není v daném prostředí řešeno
Anti-virus	Logy koncových bezpečnostních zařízení
API monitoring	Logy aplikací a služeb
Application logs	Logy aplikací a služeb
Asset management	Síťové IDS/IPS logy
Authentication logs	Systémové logy
Binary file metadata	Logy koncových bezpečnostních zařízení
Controller parameters	Systémové logy
Controller program	Logy aplikací a služeb
Data historian	Systémové logy
Data loss prevention	Logy koncových bezpečnostních zařízení
Detonation chamber	Není v daném prostředí řešeno
Digital signatures	Síťové IDS/IPS logy
Email gateway	Logy aplikací a služeb
File monitoring	Logy koncových bezpečnostních zařízení
Host network interfaces	Síťové IDS/IPS logy
Mail server	Systémové logy

Malware reverse engineering	Logy koncových bezpečnostních zařízení
Netflow/Enclave netflow	Logy síťových toků
Network device logs	Síťové IDS/IPS logy
Network intrusion detection system	Síťové IDS/IPS logy
Network protocol analysis	Logy síťových toků
Packet capture	Logy síťových toků
Process command-line parameters	Systémové logy
Process monitoring	Systémové logy
Process use of network	Logy síťových toků
Sequential event recorder	Systémové logy
SSl/TLS inspection	Logy síťových toků
Third-party application logs	Logy aplikací a služeb
Web application firewall logs	Systémové logy
Web logs	Logy aplikací a služeb
Web proxy	Logy aplikací a služeb
Windows error reporting	Systémové logy
Windows event logs	Systémové logy
Windows registry	Systémové logy

Tabulka 4.5: Mapování datových zdrojů matice na typy monitoringu

4.4 Hodnocení vybraných technik

Při ohodnocení vybraných technik bude postupováno tímto způsobem:

1. Výběr skupiny aktiv v rámci techniky a určení důležitosti
2. Přiřazení typu monitoringu
3. Výpočet pro kategorie aktiv
4. Výpočet pro důležitost
5. Výpočet celkového skóre techniky

Výběr skupiny aktiv v rámci techniky a určení důležitosti

Při hodnocení techniky Program Download nahlédneme do specifikace matice, která přiřazuje skupiny aktiv:

- Field Controller/RTU/PLC/IED
- Safety Instrumented System/Protection Relay

Tyto skupiny aktiv se nacházejí v kategoriích aktiv Rozvodna typ 1 a 2, které mají přiřazenou důležitost velmi vysoká a střední. Skupina aktiv Field Controller/RTU-/PLC/IED bude mít pro výpočet přiřazenou kategorii aktiv Rozvodna typ 1 s důležitostí velmi vysoká a Rozvodna typ 2 s důležitostí střední. To stejné bude platit i pro Safety Instrumented System/Protection Relay.

Přiřazení typu monitoringu

Dále určíme, jaké typy monitoringu jsou pro kategorie aktiv dostupné. U rozvodnen typu 1 a 2 se jedná o:

- Systémové logy
- Síťové IDS/IPS logy
- Logy síťových toků

V následujícím kroku vyhledáme v matici datové zdroje, které jsou přiřazeny k dané technice a na základě mapování zjistíme, k jakému typu monitoringu patří. V tomto případě se jedná o:

- Sequential event recorder -> Systémové logy
- Controller program -> Logy aplikací a služeb
- Network protocol analysis -> Logy síťových toků
- Packet capture -> Logy síťových toků

Abychom určili, které typy monitoringu budou do výpočtu vstupovat, porovnáme dostupné typy monitoringu a datové zdroje matice. Jak již bylo zmíněno dříve, dopad na výkon strojů ovlivňuje, zda je některý typ monitoringu pro danou kategorii aktiv

prováděn. Jako příklad můžeme uvést porovnání u techniky Program Download, kde zjistíme, že datový zdroj Controller program je zařazen do skupiny logy aplikací a služeb, které na Rozvodně typ 1 a 2 nejsou sledovány. Logy aplikací a služeb tedy nebudou do výpočtu vstupovat. Tímto způsobem dojde ke zkreslení pokrytí techniky z pohledu definovaných datových zdrojů matice, protože Controller program nebude do výpočtu zahrnut. Stále se však bude jednat o přesnější výpočet, než je pouhý poměr počtu monitorovaných a celkových aktiv. V tomto případě bude doporučena alespoň evidence této skutečnosti.

Pro techniku Program Download budou výše zmíněným postupem určeny tyto typy monitoringu vstupující do výpočtu:

- Systémové logy
- Logy síťových toků

Výpočet pro kategorie aktiv

Pro techniku Program download můžeme přejít k výpočtu pokrytí monitoringem pro jednotlivé kategorie aktiv s danou důležitostí (vyznačeno barevně v tabulce).

$$Skore = \left[\frac{MA_a}{CA} * \left(a + \left(\frac{b+c+d}{2} \right) \right) + \frac{MA_e}{CA} * \left(e + \left(\frac{b+c+d}{2} \right) \right) \right]$$

- CA - celkový počet aktiv
- MA - monitorovaná aktiva
- a - Systémové logy [25 %]
- b - Logy aplikací a služeb [20 %]
- c - Logy koncových bezpečnostních zařízení [20 %]
- d - Síťové IDS/IPS logy [20 %]
- e - Logy síťových toků [15 %]

Skupina aktiv		Field Controller/RTU/PLC/IED	
Kategorie aktiv		Rozvodna typ 1	Rozvodna typ 2
Důležitost		velmi vysoká	střední
Celková počet aktiv (CA)		150	400
Systémové logy	25 %	80	0
Logy aplikací a služeb	20 %	x	x
Logy koncových bezpečnostních zařízení	20 %	x	x
Síťové IDS/IPS logy	20 %	x	x
Logy síťových toků	15 %	200	200
Skore =		89,0 %	22,5 %

Tabulka 4.6: Hodnocení pro kategorie aktiv

Výpočet pro důležitost

Ve chvíli, kdy máme vytvořené výpočty pro všechny kategorie v rámci skupin aktiv, můžeme přejít na výpočet pro jednotlivé důležitosti.

$$C_{vv} = \frac{\sum(Skore_{vv})}{n_{vv}}$$

- C_{vv} - Hodnocení stupně důležitosti velmi vysoká
- $Skore_{vv}$ - Skóre kategorie aktiv s důležitostí velmi vysoká
- n_{vv} - Počet kategorií aktiv s důležitostí velmi vysoká

		Velmi vysoká	Vysoká	Střední	Nízká
Celkový počet aktiv (CA)		900	0	2400	0
Systémové logy	25 %				
Logy aplikací a služeb	20 %				
Logy koncových bezpečnostních zařízení	20 %				
Síťové IDS/IPS logy	20 %				
Logy síťových toků	15 %	598		1200	
C =		71,2 %	x	62 %	x

Tabulka 4.7: Výpočet pro důležitosti

Výpočet celkového skóre techniky

Posledním krokem pro ohodnocení celkového pokrytí techniky Program download monitoringem je přepočet důležitostí s ohledem na jejich přisuzovanou váhu.

$$M = C_{vv} * D_{vv} + C_s * D_s$$

- M - celkové skóre monitoringu pro danou techniku
- C_{vv} - Celkem velmi vysoká
- D_{vv} - Důležitost velmi vysoká
- C_s - Celkem střední
- D_s - Důležitost střední

Důležitost	%	C*D
Velmi vysoká	55 %	39,16
Vysoká	35 %	x
Střední	7 %	4,34
Nízká	3 %	x
Celkové skóre monitoringu pro danou techniku (M) =		70 %

Tabulka 4.8: Celkové hodnocení pokrytí techniky

Technika Program Download je v modelovém příkladu pokryta monitoringem ze 70 %, technika Man in the Middle je pokryta z 85 %.

Program Download									
Skupina aktiv		Field Controller/RTU/PLC/IED		**Safety Instrumented System/Protection Relay**					
Kategorie aktiv		Rozvodna typ 1	Rozvodna typ 2	Rozvodna typ 1	Rozvodna typ 2				
Důležitost		velmi vysoká	střední	velmi vysoká	střední	velmi vysoká	vysoká	střední	nízká
Celkový počet aktiv (CA)		150	400	750	2000	900	0	2400	0
Systémové logy	25 %	80	0	398	0				
Logy aplikací a služeb	20 %	x	x	x	x				
Logy koncových bezpečnostních zařízen	20 %	x	x	x	x				
Síťové IDS/IPS logy	20 %	x	x	x	x				
Logy síťových toků	15 %	200	200	398	1000	598		1200	
		89,00 %	22,50 %	53,00 %	22,50 %	71,00 %	x	62,00 %	x
Velmi vysoká	55 %	39,05 %							
Vysoká	35 %	x							
Střední	7 %	4,34 %							
Nízká	3 %	x							
Celkové skóre monitoringu		70,00 %							

Tabulka 4.9: Kompletní výpočet pro techniku Program Download

Man in the Middle											
Skupina aktiv		Control server	Field Controller/RTU/PLC/IED		Human-machine interface						
Kategorie aktiv		Centralní SCADA	Rozvodna typ 1	Rozvodna typ 2	Centrální SCADA	Rozvodna typ 1	Rozvodna typ 2				
Důležitost		velmi vysoká	velmi vysoká	střední	velmi vysoká	velmi vysoká	střední	velmi vysoká	vysoká	střední	nízká
Celková počet aktiv (CA)		28	150	400	60	60	160	298	0	560	0
Systémové logy	25 %	x	x	x	x	x	x				
Logy aplikací a služeb	20 %	x	x	x	x	x	x				
Logy koncových bezpečnostních zařízení	20 %	x	x	x	x	x	x				
Síťové IDS/IPS logy	20 %	28	80	200	60	32	80	200		200	
Logy síťových toků	15 %	28	200	200	60	32	80	320		200	
		100,00 %	91,00 %	50,00 %	100,00 %	53,00 %	50,00 %	86,00 %	x	80,00 %	x
Velmi vysoká	55 %	47,00 %									
Vysoká	35 %	x									
Střední	7 %	6,00 %									
Nízká	3 %	x									
Celkové skóre monitoringu		85,00 %									

Tabulka 4.10: Kompletní výpočet pro techniku Man in the Middle

4.5 Mapování na detekční pravidla

Hodnocení pokrytí datových zdrojů není jediným ukazatelem, který je vhodné sledovat. Vzhledem k tomu, že nevypovídá o skutečnosti, zda je nad monitorovanými datovými zdroji prováděno vyhodnocení/akce, bude CERT týmu doporučeno provést mapování technik matice na detekční pravidla.

Vzhledem ke složitosti exportu jednotlivých pravidel ze systému SIEM (problémovými jsou především návaznosti stavebních bloků) je nejjednodušším postupem vytvoření externí evidence pravidel s přiřazením daných technik. K tomuto účelu mohou posloužit pravidla ve formátu Sigma.

Samotné přiřazení pravidel k technice však nemusí poskytovat dostatečnou úroveň hodnocení. CERT týmu bude doporučeno, aby zvážil vytvoření hodnocení na základě expertního odhadu, které bude definovat potřebná kritéria. Pro vytvoření takového typu hodnocení může být vhodným zdrojem nástroj DeTT&CT.

4.6 Vizualizace výsledků

Pro vizualizaci pokrytí datových zdrojů a detekčních pravidel bude doporučen nástroj ATT&CK Navigator. Vzhledem k rozsáhlosti a složitosti matice je tento nástroj nejvhodnější. Poskytuje funkce jakými jsou přiřazení skóre, barevné škálování či vkládání komentářů a nemá smysl v tomto ohledu vymýšlet vlastní řešení. Nástroj je vyvíjen samotnou organizací Mitre a je pravidelně aktualizován. Dalším pozitivem je interpretovatelnost nejen pro zaměstnance na technických pozicích, ale i pro management.

Vizualizace pokrytí monitoringu

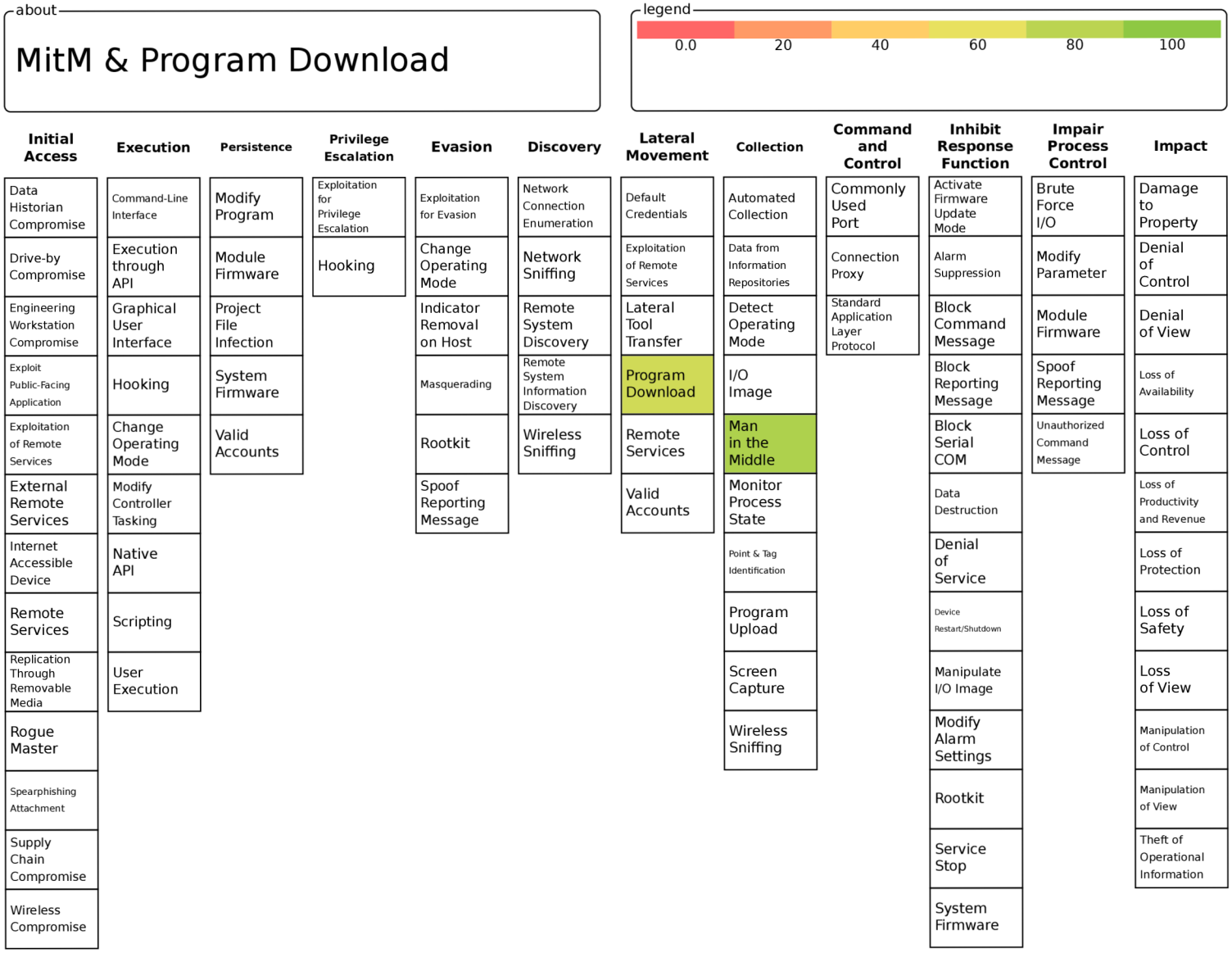
ATT&CK Navigator umožňuje dva přístupy k vizualizaci výsledků. První možností je manuální ohodnocení jednotlivých technik přímo z uživatelského rozhraní. Další možností je vytvoření kódu ve formátu JSON, který je vstupem pro ATT&CK Navigator. Následující příklad zobrazuje techniky Man in the Middle a Program Download

z pohledu pokrytí monitoringem na základě číselných výsledků uvedených v kapitole Výpočet celkového skóre techniky. V levé horní části je prostor pro pojmenování vizualizace či komentář. V pravé horní části je umístěna zvolená barevná škála, která se v tomto případě pohybuje v rozmezí od 0 do 100 %. Jednotlivé techniky jsou zabarveny na základě vypočtených hodnot.

Příklad zdrojového kódu, ze kterého byla vygenerována vizualizace na obrázku 4.2:


```
{
  "name":"MitM & Program Download",
  "versions":{
    "attack":"9",
    "navigator":"4.3",
    "layer":"4.2"
  },
  "domain":"ics-attack",
  "description":"",
  "filters":{
    "platforms":[
      "Field Controller/RTU/PLC/IED",
      "Safety Instrumented System/Protection Relay",
      "Control Server",
      "Input/Output Server",
      "Windows",
      "Human-Machine Interface",
      "Engineering Workstation",
      "Data Historian"
    ]
  },
  "sorting":0,
  "layout":{
    "layout":"side",
    "aggregateFunction":"average",
    "showID":false,
    "showName":true,
    "showAggregateScores":false,
    "countUnscored":false
  },
  "hideDisabled":false,
  "techniques":[
    {
      "techniqueID":"T0830",
      "tactic":"collection-ics",
      "score":85.45,
```

```
      "color":"",
      "comment":"",
      "enabled":true,
      "metadata":[
      ],
      "showSubtechniques":false
    },
    {
      "techniqueID":"T0843",
      "tactic":"lateral-movement-ics",
      "score":70.16,
      "color":"",
      "comment":"",
      "enabled":true,
      "metadata":[
      ],
      "showSubtechniques":false
    }
  ],
  "gradient":{
    "colors":[
      "#ff6666",
      "#ffe766",
      "#8ec843"
    ],
    "minValue":0,
    "maxValue":100
  },
  "legendItems":[
  ],
  "metadata":[
  ],
  "showTacticRowBackground":false,
  "tacticRowBackground":"#000000",
  "selectTechniquesAcrossTactics":true,
  "selectSubtechniquesWithParent":false
}
```



Obrázek 4.2: Vizualizace výsledků hodnocení technik

4.7 Shrnutí

Tvorba metodiky založená na kvantitativním hodnocení s sebou nese několik problémů, které ovlivňují přesnost výsledku. Tyto problémy se váží především na mapování datových zdrojů. Monitoring ve společnosti nemá smysl provádět na takové úrovni podrobnosti, která je využívána v matici. Datové zdroje matice je tak nutné přiřadit k typům monitoringu. Některé z nich dokonce nejsou monitoringem pokryty vůbec. Jedná se o datové zdroje, které jsou řešeny provozem. Posledním problémem je absence monitoringu u některých kategorií aktiv, například z důvodu vysokých požadavků na výkon. Tímto způsobem dochází při hodnocení techniky k vyřazení některých datových zdrojů matice. Všechna tato omezení je při vyhodnocování nutné brát na zřetel.

Na druhé straně v případě kvalitativního hodnocení, jako je například DETT&CT zmíněný v analytické části, narážíme na problematiku přesnosti expertního odhadu. Určitá omezení tak přináší obě metody. Zde je ke zvážení CERT týmu, který z přístupů pro něj poskytuje relevantnější informace, nebo zda by nebylo vhodné přístupy kombinovat.

Celkové vyhodnocení matice je náročné jak časově, tak z hlediska lidských zdrojů nezávisle na použitém typu hodnocení. V návrhu je proto CERT týmu doporučeno identifikovat relevantní techniky na základě jím stanovených kriterií.

Pro sdílení výsledků s ostatními CERT týmy bude doporučeno použít pro vizualizaci nástroj ATT&CK Navigator a pro sdílení detekčních pravidel formát Sigma.

I přes všechna výše zmíněná omezení poskytuje navržená metodika relevantní data, na jejichž základě lze identifikovat slabá místa monitoringu z pohledu matice ATT&CK for ICS. Jedná se o hodnocení z perspektivy útočníků a jimi užívaných technik, taktik a procedur. Metodika dále poskytuje možnost bezpečného sdílení výsledků s ostatními CERT týmy a umožňuje komunikovat výsledky hodnocení srozumitelným způsobem i pro netechnické pracovníky.

Navržený způsob hodnocení monitoringu je dále možné rozšířit o hodnocení důležitosti jednotlivých technik a tím dále zúžit zaměření CERT týmu.

Kapitola 5

Závěr

V první části práce byla představena teoretická východiska práce. Popsána byla problematika kybernetické bezpečnosti, průmyslových řídicích systémů a v neposlední řadě byla představena matice MITRE ATT&CK for ICS. Druhá část byla věnována analýze hodnocení monitoringu v energetické společnosti. Dále byla analyzována již existující řešení vycházející primárně z matice MITRE ATT&CK for Enterprise. Byly zhodnoceny jejich přínosy a možnosti využití. Na tomto základě a požadavcích společnosti byla v poslední části práce navržena metodika založená na kvantitativním hodnocení vycházející z matice MITRE ATT&CK for ICS. V rámci shrnutí byly diskutovány její přínosy a omezení. Dále byly navrženy možnosti sdílení výsledků mezi CERT týmy.

Literatura

[1] *Zákon č. 181/2014 Sb., ze dne 23. července 2014, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [Sbírka zákonů]. Česká republika. Dostupné z: https://www.nukib.cz/download/publikace/legislativa/2020-02-01_novelizace_zneni_zakona_181_2014_final.pdf.

[2] *Zákon č. 458/2000 Sb., ze dne 28. listopadu 2000, o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon).* Česká republika. Dostupné z: https://www.eru.cz/documents/10540/463082/Energetick%C3%BD%20z%C3%A1kon+-+zn%C4%9Bn%C3%AD%20do+31.+7.+2017/3c905076-0399-4839-a807-85d77ab2ce8c.

[3] Alexander, O. *MITRE ATT&CK®for Industrial Control Systems: Design and Philosophy* [online]. The MITRE Corporation. Dostupné z: https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT%26CK_for_ICS_-_Philosophy_Paper.pdf.

[4] cdc rabobank. *GitHub - rabobank-cdc/DeTTECT: Detect Tactics, Techniques & Combat Threats* [online]. [cit. 2021-04-12]. Dostupné z: https://github.com/rabobank-cdc/DeTTECT.

[5] Colbert, E. J. *Cyber-security of SCADA and Other Industrial Control Systems.* Springer International Publishing Switzerland, 2016. ISBN 978-3-319-32125-7.

[6] Doucek, P. *Řízení bezpečnosti informací: 2.rozšířené vydání o BCM 2. přeprac. vyd.* Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[7] Institute, S. *Cyber Security Training / SANS Courses, Certifications & Research* [online]. [cit. 2021-04-12]. Dostupné z: https://www.sans.org/.

[8] Jirásek, P., Novák, L. a Požár, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Policejní akademie ČR v Praze, Česká pobočka AFCEA. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/vykladovy_slovnik_KB_3_vydani.pdf.

[9] Kolouch, J. *CyberSecurity*. 1. vyd. CZ.NIC, 2019. ISBN 978-80-88168-31-7.

[10] Miller, D. R. *Security Information and Event Management (SIEM)Implementation*. McGraw-Hill, 2011. ISBN 978-0-07-170108-2.

[11] Mitre. *ATT&CK Navigator* [online]. [cit. 2021-04-12]. Dostupné z: https://mitre-attack.github.io/attack-navigator/.

[12] MITRE. *The MITRE Corporation* [online]. [cit. 2020-12-12]. Dostupné z: https://www.mitre.org/.

[13] NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2020-11-14]. Dostupné z: https://www.nukib.cz/cs/.

[14] Ondrák, V. *Problematika ISMS v manažerské informatice*. 1. vyd. CERM, 2013. ISBN 978-80-7204-872-4.

[15] Požár, J. *Základy teorie informační bezpečnosti*. Vydavatelství PA ČR, 2007. ISBN 78-80-7251-250-8.

[16] Siemens. *Product Details - Industry Mall - Siemens USA* [online]. [cit. 2020-12-12]. Dostupné z: https://mall.industry.siemens.com/mall/en/us/Catalog/Product/6AG13146CH047AB0.

[17] Siemens. *Product Details - Industry Mall - Siemens USA* [online]. [cit. 2020-12-12]. Dostupné z: https://mall.industry.siemens.com/mall/en/us/Catalog/Product/6NH31120BA000XX0.

[18] SigmaHQ. *GitHub - SigmaHQ/sigma: Generic Signature Format for SIEM Systems* [online]. [cit. 2021-04-12]. Dostupné z: https://github.com/SigmaHQ/sigma.

[19] Stouffer, K. *Guide to Industrial Control Systems (ICS) Security* [online]. National Institute of Standards and Technology. Dostupné z: http://dx.doi.org/10.6028/NIST.SP.800-82r2.

Seznam použitých zkratek

CERT	**C**omputer **E**mergency **R**esponse **T**eam
CSIRT	**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DLP	**D**ata **L**oss **P**revention
DMZ	**D**emilitarizovaná **z**óna
DNS	**D**omain **N**ame **S**ystem
FTP	**F**ile **T**ransfer **P**rotocol
GPRS	**G**eneral **P**acket **R**adio **S**ervice
HMI	**H**uman-**M**achine **I**nterface
HTTP	**H**ypertext **T**ransfer **P**rotocol
ICS	**I**ndustrial **C**ontrol **S**ystems
IDS	**I**ntrusion **D**etection **S**ystem
IED	**I**ntelligent **E**lectronic **D**řevice
IPS	**I**ntrusion **P**revention **S**ystems
ISMS	**I**nformation **S**ecurity **M**anagement **S**ystem
IT	**I**nformační **t**echnologie
JSON	**J**avaScript **O**bject **N**otation
KII	**K**ritická **i**nformační **i**nfrastruktura
KI	**K**ritická **i**nfrastruktura
NIS	**N**etwork and **I**nformation **S**ystems
NÚKIB	**N**árodní **ú**řad pro **k**ybernetickou a **i**nformační **b**ezpečnost
PLC	**P**rogrammable **L**ogic **C**ontroller
RTU	**R**emote **T**erminal **U**nit
SCADA	**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
SIEM	**S**ecurity **I**nformation and **E**vent **M**anagement
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol
SQL	**S**tructured **Q**uery **L**anguage
WAN	**W**ide **A**rea **N**etwork
YAML	**Y**AML **A**in't **M**arkup **L**anguage
ZoKB	**Z**ákon **o** **k**ybernetické **b**ezpečnosti