Systém pro rychlou detekci a ověření zranitelností infrastruktury

Bc. Lukáš DOLEŽEL

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Lukáš Doležel**
Osobní číslo:	**A22340**
Studijní program:	**N0613A140022 Informační technologie**
Specializace:	**Kybernetická bezpečnost**
Forma studia:	**Kombinovaná**
Téma práce:	**Systém pro rychlou detekci a ověření zranitelností infrastruktury**
Téma práce anglicky:	**System for Rapid Detection and Verification of Infrastructure Vulnerabilities**

Zásady pro vypracování

1. Popište aktuální řešení pro hledání zranitelností.
2. Vyberte zdroje dat podporující optimalizaci skenů zranitelností, zkrácení času mezi objevením zranitelnosti a informováním správce infrastruktury.
3. Navrhněte systém využívající podpůrná data.
4. Naimplementujte navržený systém.
5. Otestujte funkčnost implementovaného systému.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. BROTHERSTON, Lee a Amanda BERLIN. _Defensive security handbook: best practices for securing infrastructure_. Sebastopol, CA: O'Reilly Media, 2017, 1 online zdroj (xx, 261 stran). ISBN 9781491960356. Dostupné také z: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1498009&authtype=ip,shib&custid=s3936755.
2. FRIEDMAN, Jon a Bassam KHAN, SHUTTLEWORTH, Susan, ed. CYBEREDGE GROUP, LLC. Definitive GuideTM to Complete Network Visibility: How to Get High-Performing, Secure Networks While Staying Within Budget [online]. 1. Annapolis, USA: CyberEdge Group, 2020, 62 s. [cit. 2022-12-01]. ISBN 978-1-948939-10-2. Dostupné z: [https://cyber-edge.com/resources/definitive-guide-to-complete-network-visibility/](https://cyber-edge.com/resources/definitive-guide-to-complete-network-visibility/ "https://cyber-edge.com/resources/definitive-guide-to-complete-network-visibility/").
3. SHROBE, Howard E., David L. SHRIER a Alex PENTLAND. _New solutions for cybersecurity_. Cambridge, MA: MIT Press, [2018], 1 online zdroj. MIT Connection Science and Engineering Ser. ISBN 9780262346641. Dostupné také z: https://proxy.k.utb.cz/login?url=https://doi.org/10.7551/mitpress/11636.001.0001?locatt=mode:legacy.
4. SAIRUM, Jetty a Sagar RAHALKAR. Securing Network Infrastructure. Birmingham, England: Packt Publishing, 2019. ISBN 978-1838642303.
5. ORZACH, Yoram a Deepanshu KHANNA. Network Protocols for Security Professionals. Birmingham, England: Packt Publishing, 2022. ISBN 1789953480.
6. ENOKA, Seth. Cybersecurity for small networks: a no-nonsense guide for the reasonably paranoid. San Francisco, CA: No Starch Press, 2022. ISBN 978-171-8501-485.
7. DAVIS, Royce. The Art of Network Penetration Testing: Free practice environment. Shelter Island: Manning Publications, 2021. ISBN 9781617296826.

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **5. listopadu 2023**
Termín odevzdání diplomové práce: **13. května 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 5. ledna 2024

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomové práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky. Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne .....

podpis studenta

ABSTRAKT

Diplomová práce se zabývá návrhem systému pro rychlou detekci a ověření zranitelností v IT infrastruktuře. Cílem je vyvinout řešení, které bude schopné proaktivně identifikovat slabá místa systémů a poskytovat podklady pro jejich včasnou nápravu. V teoretické části jsou popsány základní oblasti kybernetické bezpečnosti, včetně správy zranitelností, analýzy síťového provozu a logování událostí. Dále je uveden přehled existujících dohledových systémů a nástrojů pro sběr bezpečnostních dat. Praktická část se věnuje návrhu architektury detekčního systému, který kombinuje různé datové zdroje, jako jsou výstupy ze skenerů zranitelností, záznamy síťových toků a systémové logy. Navržený systém využívá pokročilé metody korelace událostí a obohacování dat z externích zdrojů o hrozbách pro zvýšení přesnosti a relevance výstupů. Implementovaná detekční pravidla pokrývají známé i dosud neznámé zranitelnosti a jsou optimalizována pro výkon a kvalitu detekce. Práce demonstruje praktickou využitelnost navrženého řešení a jeho potenciál pro zlepšení úrovně kybernetické bezpečnosti v organizacích.

Klíčová slova: detekce zranitelností, kybernetická bezpečnost, analýza síťového provozu, korelace událostí, threat intelligence

ABSTRACT

This master's thesis focuses on designing a system for rapid detection and verification of vulnerabilities in IT infrastructures. The goal is to develop a solution capable of proactively identifying weak points in systems and providing data for their timely remediation. The theoretical part describes fundamental areas of cybersecurity, including vulnerability management, network traffic analysis, and event logging. An overview of existing monitoring systems and tools for collecting security data is also provided. The practical part is dedicated to designing the architecture of a detection system that combines various data sources, such as outputs from vulnerability scanners, network flow records, and system logs. The proposed system utilizes advanced methods of event correlation and enrichment of data from external threat intelligence sources to increase the accuracy and relevance of outputs. The implemented detection rules cover both known and previously unknown vulnerabilities and are optimized for performance and

detection quality. The thesis demonstrates the practical applicability of the proposed solution and its potential for improving the level of cybersecurity in organizations.

Keywords: vulnerability detection, cybersecurity, network traffic analysis, event correlation, threat intelligence

Rád bych na tomto místě poděkoval všem, kteří mě podporovali při psaní této diplomové práce a během celého studia.

Mé největší poděkování patří mé rodině, za jejich neutuchající podporu a trpělivost v průběhu mého studia.

Velký dík náleží také vedoucímu mé diplomové práce, Ing. Davidovi Malaníkovi, Ph.D., za odborné vedení, cenné rady, věcné připomínky a čas, který mi věnoval během konzultací. Jeho odborné znalosti a zkušenosti významně přispěly ke zkvalitnění této práce.

V neposlední řadě děkuji všem vyučujícím a kolegům z Fakulty aplikované informatiky za předané znalosti, inspirativní diskuze a vytvoření podnětného studijního prostředí.

OBSAH

ÚVOD

Zajištění kybernetické bezpečnosti je v dnešním propojeném a digitalizovaném světě naprosto klíčové. S rostoucí složitostí IT infrastruktury a sofistikovaností kybernetických hrozeb čelí organizace výzvě, jak efektivně identifikovat a řešit zranitelnosti ve svých systémech dříve, než je zneužijí útočníci.

Tato diplomová práce se zaměřuje na vývoj systému pro rychlou detekci a ověření zranitelností v IT infrastruktuře. Cílem je navrhnout řešení, které bude schopné proaktivně vyhledávat slabá místa. Práce zkoumá stávající přístupy a nástroje s otevřeným zdrojovým kódem pro detekci zranitelností a navrhuje architekturu, která kombinuje analýzu síťového provozu, skenování zařízení a obohacování dat z externích zdrojů.

Navržený systém má potenciál významně přispět k posílení bezpečnostní úrovně organizací tím, že umožní rychlejší odhalování a řešení zranitelností. To pomůže minimalizovat plochu útoku a snížit riziko úspěšných průniků a narušení. Práce tak přispívá k oboru kybernetické bezpečnosti návrhem prakticky využitelného detekčního řešení.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost se vyčleňuje z tradičního IT světa jako unikátní disciplína, která již není považována za podobor softwarového inženýrství či správy systémů. Existuje několik charakteristik, které kybernetickou bezpečnost odlišují od ostatních IT oblastí. Patrně nejvýraznějším rozdílem je vrozená přítomnost inteligentního protivníka, který se v této oblasti nevyhnutelně vyskytuje.

Přítomnost inteligentního protivníka vyžaduje odlišný přístup, disciplínu a způsob myšlení ve srovnání s tradičními úkoly vývojářů nebo systémových administrátorů, kteří si mohou být navzájem protivníky, často však neúmyslně. V oblasti bezpečnosti, ať již simulujeme útok, nebo se proti němu bráníme, musíme zvážit perspektivu a potenciální kroky našeho protivníka a snažit se je anticipovat. Naši protivníci jsou stále lidské bytosti s vlastní vůlí, které mohou uvažovat, předpovídat, soudit, analyzovat, přemýšlet a plánovat. Mohou rovněž projevovat emoce, jako je radost, smutek, chamtivost, strach, triumf či pocit viny. Jak útočníci, tak obránci mohou využívat emocí svých lidských oponentů. Například útočník může spoléhat na pocit trapnosti, když drží počítačový systém jako rukojmí a hrozí zveřejněním citlivých dat. Obránci naopak mohou využít strach z odvetných akcí a promyšleně zabezpečeného systému, který by mohl vést k odhalení útočníka, což by ho vystavilo riziku následků jeho činů. Tím pádem zůstává lidský faktor klíčovou součástí kybernetické bezpečnosti.

Dalším důležitým aspektem oboru je neustálá přítomnost nejistoty a nutnost pracovat s neúplnými daty. Informační systém, který je dnes považován za bezpečný díky nejmodernějším bezpečnostním technologiím a osvědčeným postupům, nemusí být bezpečný zítra. Kdy přejdeme od běžného monitorování k obraně a záchraně před kolapsem způsobeným inteligentním protivníkem?

Musíme přepokládat a odhadovat pravděpodobnosti – někdy implicitně, jindy explicitně. Jako útočníci nikdy nepoznáme všechny detaily cílového systému a nebudeme vědět, zda o nás obránci již vědí a hrají s námi hru na kočku a myš. Obránci zase nebudou mít informace o všech možných útocích nebo zranitelnostech, kterým mohou čelit.

Problémy spojené s inteligentním protivníkem a nejistotou naznačují, že porozumění kybernetické bezpečnosti vyžaduje hlubší pochopení lidského myšlení a řešení problémů. To znamená, že je nutné přijmout a rozvíjet specifické způsoby myšlení, které nám pomohou učit se a aplikovat naše dovednosti efektivněji.

1.1 Útok a Obrana

Kybernetická bezpečnost je obor, který byl dlouho podceňován, avšak v posledních letech získává na významu. Co činí tento obor tak zajímavým, je možná právě fakt, že obsahuje herní prvky boje mezi více entitami, které usilují o dosažení protichůdných cílů. Často je role obránce či útočníka zakořeněna v osobnosti jedince, a tak je snaha vytvořit neproniknutelnou pevnost stejně intenzivní jako touha ji zničit, nebo se do ní pouze nepozorovaně vloupat a získat strážený poklad.

Je fascinující, že role obránce a útočníka jsou na sobě vzájemně závislé; v tomto oboru nemůže jedna existovat bez druhé, a jejich každodenní soupeření připomíná strategickou hru. Každá z rolí se stává zkušenější, pečlivější a sofistikovanější díky výzvám, které před sebe staví ta druhá. Tato dynamika vztahu objasňuje, proč se oblast kybernetické bezpečnosti stává časem stále složitější.

Pro lepší pochopení této dynamiky si představme fiktivní postavy Boba a Evu, notoricky známé z kryptografie. Uvažujme, že Bob má cenný majetek, který chce chránit – například vzrostlou jabloň. Bob si přeje, aby si jablka mohl trhat pouze on. Útočnice Eva by naopak dala cokoli za to, aby mohla jablka Bobovi ukrást. Zpočátku Bob nevěnuje bezpečnosti svého stromu žádnou zvláštní pozornost, což Evě umožňuje snadno přijít a jablko ukrást. Avšak jak se Eva stává stále lepší v krádežích, Bob se rovněž stává lepším v ochraně svého stromu.

Když si Bob poprvé všimne Eviny krádeže, postaví strážní věž, ze které bude strom hlídat. Eva však usoudí, že Bob musí někdy spát a všímá si, kdy odchází do postele, aby se poté ke stromu tiše připlížila. Bob poté postaví vysokou kamennou zeď kolem stromu. Eva ji sice nedokáže prorazit nebo přelézt, ale zjistí, jak zeď podkopat. Bob nato vycvičí hlídacího psa, aby strom chránil. Eva však zjistí, že psa může o svých neviných úmyslech přesvědčit pomocí pamlsků. Bob se zdokonalí v hardwarové bezpečnosti a nainstaluje kamery a alarmy, aby ho varovaly, kdykoliv se Eva přiblíží. Eva se naučí, jak kamery a alarmy deaktivovat.

Tento souboj vůlí může teoreticky pokračovat ad infinitum.

2 ZÁKLADNÍ DĚLENÍ BEZPEČNOSTNÍCH DOMÉN

Analýza logů a událostí ze serverů, aktivních prvků a koncových stanic, společně s důkladným zkoumáním síťového provozu, představuje základní pilíře pro identifikaci a prevenci kybernetických hrozeb v moderních IT infrastrukturách. Zatímco logy poskytují podrobné záznamy o aktivitách na systémech a aplikacích, analýza síťového provozu umožňuje hlubší vhled do toho, jak data proudí mezi zařízeními a aplikacemi v rámci sítě. Tato kombinace nabízí komplexní přehled o chování systémů a uživatelů, umožňuje identifikovat anomálie a potenciální bezpečnostní hrozby, jako jsou malware, phishingové útoky a pokusy o neoprávněný přístup.

Analýza síťového provozu hraje hlavní roli při detekci zranitelností, které nemusí být zřejmé pouze z analýzy logů. Sledováním a vyhodnocováním vzorců komunikace v síti, včetně neobvyklého nárůstu provozu, komunikace na neobvyklých portech nebo nečekaných zeměpisných destinací, mohou bezpečnostní týmy odhalit pokusy o zneužití zranitelností v reálném čase. Techniky jako DPI a analýza toku dat umožňují rozpoznat i sofistikované útoky, které se snaží maskovat svou přítomnost v běžném síťovém provozu. Navíc, využití pokročilých analytických nástrojů a umělé inteligence pro analýzu síťového provozu může výrazně zvýšit schopnost organizace predikovat a předcházet bezpečnostním incidentům tím, že poskytuje upozornění na anomální chování, které by mohlo indikovat pokus o zneužití nebo již probíhající útok.

Kombinací analýzy systémových logů a síťového provozu se organizacím umožňuje nejen pasivně reagovat na bezpečnostní incidenty, ale také aktivně monitorovat a zlepšovat svou bezpečnost. Toto proaktivní sledování a analýza jsou nezbytné pro rychlou identifikaci a nápravu zranitelností, minimalizaci rizika a ochranu před APT, které cílí na různé zájmové sítě. Díky těmto metodám mohou bezpečnostní týmy lépe porozumět dynamice hrozeb ve svých sítích a přizpůsobit své obranné strategie tak, aby byly vždy o krok napřed před útočníky.

2.1 Správa zranitelností na síti

Správa zranitelností na síti je proces detekce zranitelností, který se zaměřuje na síťový provoz, zařízení účastnící se na jeho přenosu, nebo na aplikace a služby, jež jsou zdrojem či příjemcem tohoto provozu. Zranitelnosti mohou vzniknout kvůli špatné konfiguraci, nebo zastaralému softwaru komunikujícímu na síti a mohou být útočníky snadno zneužity.

Správa zranitelností by měla být klíčovou součástí jakékoli organizace, která se ve své činnosti spoléhá na IT technologie. Slouží k detekci bezpečnostních problémů na síti tím, že provádějí komplexní analýzu sítě za účelem identifikace slabých míst v její

bezpečnosti. Je nezbytnou součástí bezpečnostní infrastruktury každého IT oddělení. Ačkoliv jde o poměrně přímočarý proces s jasnými cíli a výstupy, který by měl být prováděn pravidelně a jehož technická podstata se nemění, stále existuje určité nepochopení ohledně toho, co správa zranitelností skutečně obnáší a co dělá. Proto je důležité vysvětlit, proč je správa zranitelností důležitá a proč by se měla pravidelně provádět.

Správa zranitelností je součástí procesu hodnocení bezpečnosti jakékoli sítě nebo systému. Přestože je to proces přímý, může být časově náročný v závislosti na počtu systémů, které je třeba kontrolovat a následném vyhodnocení výsledků. Nejlepším přístupem je systematické a organizované skenování. Zároveň zde existuje velký prostor pro automatizaci, jak ve fázi provedení testů, tak při jejich vyhodnocení.[1]

2.1.1 Analýza síťového provozu

Ačkoli bychom mohli polemizovat o užitku kontroly síťového provozu, v dnešní době, kdy podíl šifrovaného provozu, na internetu dosahuje téměř 100%, se může zdát, že tento přístup nemá smysl.[2] Hlavním zdrojem informací pro bezpečnostní systémy však již nejsou uživatelská data, ale takzvaná flow data, vytvořená ze skupin jednotlivých hlaviček paketů, které jsou sdružovány do toků dat. S rostoucím objemem šifrovaného provozu a rychlostí jeho přenosu se kompletní analýza provozu pomocí DPI stává problematickou i z hlediska vyžadovaného výkonu. Existují nicméně přístupy, jak zvládnout analýzu takového objemu dat.

Podle statistik z léta 2023 tvořily dvě třetiny síťového provozu video streamy, a do zbylé třetiny spadá vše ostatní, včetně přenosu velkých bloků dat, nazývaných „elephant flows“. Tyto velké přenosy dat typicky není třeba kontrolovat celé, ale z pohledu analýzy toku postačí sledovat počátek a zbytek lze po několika kilobajtech ignorovat. Ačkoli jsou tyto statistiky uváděné pro celý internet, jsou aplikovatelné i na menší (korporátní) sítě. Pokud bychom v dohledované síti omezili přístup na YouTube a další streamovací služby, množství provozu by kleslo o zmíněné dvě třetiny a možná i více, což by mohlo být dostatečné pro umožnění DPI za přijatelných nákladů. Tento přístup však představuje další komplexní řešení pro síťový dohled.[3]

Nepostradatelným prvkem, který umožňuje detekci zranitelností na síti bez nutnosti aktivního skenování, je takzvaná síťová viditelnost. Jedná se o důležitou vlastnost sítě, umožňující detekci nově připojených zařízení a odhad jejich účelu v síti na základě komunikace mezi jednotlivými zařízeními. Tato vlastnost také umožňuje detekci anomálního chování zařízení, což může upozornit na přítomnost zranitelnosti. Mnoho služeb v dnešních operačních systémech je „plug and play“ a automaticky oznamují svou dostupnost v síti, což vyvolává otázku, zda je vhodné, aby daná služba na daném hos-

titelském systému byla aktivní a komunikovala. Důležité je zvážit také zdroje dat pro nástroje síťového monitoringu. Mezi dva nejběžnější patří:

- Průtoková data, neboli flow data (získaná ze zařízení, jako jsou směrovače),
- Paketová data (z SPAN portů a síťových TAP).[7]

S klesající využitelností analýzy dat přenášených v payloadu paketu se pozornost přesunula k analýze IP hlaviček a díky umělé inteligenci i k analýze provozu pomocí postranních kanálů. IP hlavičky se v provozu vyskytují stále v nešifrované podobě, což umožňuje jejich analýzu. To lze využít například k rozdělení síťových zařízení do skupin, kdy například DNS servery komunikující na netradičních portech mohou signalizovat konfigurační či bezpečnostní problémy.

Zvýšila se také rychlost, s jakou jsou sdíleny informace o škodlivých hostech na Internetu. Například skenery či C2 servery jsou často detekovány a označeny během několika hodin či dnů a tato informace je skrze API online databází přístupná komukoliv.

Využití nástrojů, jako jsou DarkTrace nebo GreyCortex Mendel, které při své činnosti využívají umělou inteligenci, umožňuje snadné nastavení základních komunikačních vzorců (baseline) a v reálném čase detekuje odchylky od těchto standardů. Tento přístup se ukázal být extrémně účinný zejména u SCADA a IoT zařízení, ale je aplikovatelný i v běžných uživatelských sítích, kde například neobvyklá aktivita uživatele mimo standardní pracovní dobu, zahájení odesílání dat mimo časové okno určené pro zálohy, odesílání na nestandartní IP adresu, nebo komunikace serverů na nestandartních portech může indikovat bezpečnostní problém, jako je aktivita útočníka nebo šíření síťového červa.

2.1.2 Skenování zařízení v síti

Základní skenování sítě, například pomocí nástroje 4.1.1 Network Mapper, je poměrně jednoduchou záležitostí a s využitím několika základních NSE skriptů může být velice efektivní. Při takovém skenování je však potřeba zajistit viditelnost skenovacího nástroje do všech podsítí, což může vyžadovat detailní znalosti o fungování sítě a často i mnoho hodin konfigurace aktivních síťových prvků a bezpečnostních prvků před prvním skenováním.

Kromě přípravy síťových prvků na plánované skenování mohou být překážkou i existující ochranná opatření, jako například IPS systémy, DDoS filtry (pračky), nebo inteligentní firewally. Tyto nástroje mohou skenování kompletně zastavit, proto je potřeba je nastavit tak, aby umožnily provedení skenování. Je také nutné zvážit, zda tuto výjimku ponechat trvale aktivní, nebo ji vždy aktivovat před samotným skenováním.

Cílem skenování je objevení otevřených portů na zařízeních. Základním bezpečnostním pravidlem (Least privilege) je, že pokud není potřeba, aby port byl otevřený, měl by být uzavřený (filtrovaný)[8], čímž se sníží základna pro útok proti danému zařízení. Dalším důležitým zjištěním při skenování je odhalení továrních přihlašovacích údajů a přístupnost továrního přístupu obecně. Pokud je možné se přihlásit na doménový řadič, router, firewall nebo rozhraní pro vzdálenou správu (např. IPMI, iDrac, iLom) s využitím továrního hesla na účet root, jedná se o zranitelnost, kterou je třeba odstranit.

Skenování lze rozdělit na dvě části:

1. Skenování aktivních síťových prvků a serverů poskytujících služby typu DNS, DHCP, tiskové servery, VoIP aj., které se v čase příliš často nemění. Výsledky z tohoto skenování lze poměrně snadno automatizovat do podoby rozdílových reportů.

2. Skenování koncových zařízení s minimálně jedním rozhraním, jako jsou aplikační servery vývojářů, koncové stanice nebo terminály uživatelů, IP telefony aj. Pokud tato zařízení nejsou spravována centrálně pomocí domény a bezpečnostních politik a jsou pod plnou kontrolou uživatelů, může být skenování a vyhodnocení výsledků náročné a často zahrnuje intenzivní komunikaci s uživateli.

Pro maximální automatizaci aktivních testů na zařízeních lze využít nástroje jako 4.1.2 Nessus nebo 4.1.3 OpenVAS, které podstatnou část těchto testů automatizují a obsahují databázi zranitelností, jež použijí proti svým cílům, aby prověřily jejich zranitelnost. Zde je třeba zvážit rizika, která tento přístup přináší.[9]

2.2 Logy událostí ze zařízení

Analýza logů a událostí ze serverů, síťových prvků a koncových stanic představuje další složku v oblasti kybernetické bezpečnosti a správy IT infrastruktury. Tato činnost umožňuje organizacím monitorovat, vyhodnocovat a reagovat na různé aktivity, potenciální zranitelnosti a hrozby v reálném čase. Bezpečnostní logy jsou záznamy, které obsahují informace o událostech, které mají potenciální bezpečnostní význam. Tyto logy mohou pocházet z různých zdrojů, včetně operačních systémů serverů a koncových stanic, síťových zařízení a bezpečnostních aplikací, jako jsou firewally, antivirové programy a IDPS systémy. Obsahují záznamy o úspěšných a neúspěšných přihlášeních, změnách systémových konfigurací, přístupech k souborům a dalších důležitých událostech.

Vzhledem k obrovskému množství generovaných záznamů je zásadní využít efektivní nástroje a postupy pro jejich správu. Bez správné konfigurace logovacích politik a analytických nástrojů může být analýza logů jako hledání jehly v kupce sena. Moderní

systémy pro správu logů a událostí 3.3 pomáhají organizacím zpracovávat, analyzovat a korelovat velké objemy dat v reálném čase, což umožňuje rychlou identifikaci a reakci na potenciální bezpečnostní incidenty.

Detekce zranitelností je oblastí, ve které analýza logů hraje zásadní roli. Logy mohou obsahovat stopy, které naznačují přítomnost zranitelností v systémech nebo pokusy o jejich zneužití. Analyzováním těchto záznamů mohou bezpečnostní týmy identifikovat slabá místa v infrastruktuře a prioritizovat jejich opravy, čímž se snižuje riziko úspěšných kybernetických útoků.

Efektivní analýza logů a událostí vyžaduje kombinaci pokročilých technologií, odborných znalostí a pečlivě navržených procesů. To zahrnuje definování toho, které události a logy jsou pro organizaci nejdůležitější, nastavení upozornění na podezřelé aktivity a průběžné vzdělávání týmů o nejnovějších hrozbách a trendech v kybernetické bezpečnosti. Přestože je analýza logů náročná, její význam pro ochranu digitálních aktiv a zajištění kontinuity IT systémů je nezpochybnitelný.

3 PŘEHLED DOHLEDOVÝCH SYSTÉMŮ

3.1 Správa bezpečnostních informací

SIM se zaměřuje na sběr logových souborů a jejich ukládání v centrálním repozitáři pro pozdější analýzu. Proto se SIM často označuje také jako správa logů. Řešení SIM jsou většinou založena na agentech, kteří běží na sledovaných serverech a počítačích. Tito agenti předávají logy a další související bezpečnostní informace centrálnímu SIM serveru. Systémoví administrátoři se pak mohou přihlásit do konzole a kontrolovat bezpečnostní zprávy, grafy a diagramy v reálném čase.

Některé SIM systémy používají lokální filtry pro normalizaci, zkoumání a čištění logů před odesláním na centrální server. To pomáhá snížit množství dat posílaných přes síť (což by mohlo způsobit zahlcení síťové šířky pásma) a ukládaných na SIM serveru (což by mohlo rychle zaplnit diskový prostor). Filtrování musí být provedeno způsobem, který nebrání schopnosti rekonstruovat stav systému, který spustil bezpečnostní incident.

Klíčové vlastnosti SIM:

- Sběr a ukládání logů v centrálním úložišti.
- Často založeno na agentech běžících na sledovaných systémech.
- Předávání logů a bezpečnostních informací na centrální server.
- Filtrování a čištění logů před odesláním (v některých případech).

3.2 Správa bezpečnostních událostí

SEM se zabývá identifikací, sběrem, monitorováním, vyhodnocováním, korelací a sledováním systémových událostí a upozornění. V jistém smyslu je SEM vylepšením SIM, ačkoliv obě oblasti jsou považovány za samostatné oblasti správy bezpečnosti. Stejně jako v případě SIM jsou data obvykle přenášena z hostitelského počítače do centrálního repozitáře pomocí protokolů jako SNMP nebo syslog. Centralizovaný repozitář zajišťuje, že události a upozornění jsou uchovávány bezpečným a forenzně validním způsobem.

Informace jsou poté analyzovány pomocí bezpečnostních algoritmů a statistických výpočtů za účelem identifikace hrozeb, zranitelností a rizik. SEM dokáže analyzovat přicházející záznamy podle jejich významnosti a okamžitě upozornit odpovědné osoby, kdykoli záznam vyžaduje pozornost. Centralizace také usnadňuje identifikaci událostí, které ovlivňují více systémů. Primárním účelem nástrojů SEM je identifikovat upozornění nebo události, které stojí za vyšetření, jako jsou například přihlášení administrátorů mimo pracovní dobu.

Klíčové vlastnosti SEM:

- Identifikace, sběr, monitorování, vyhodnocování a korelace systémových událostí a upozornění.
- Analýza událostí pomocí bezpečnostních algoritmů a statistických výpočtů.
- Identifikace hrozeb, zranitelností a rizik.
- Real-time upozornění na významné události.
- Centralizovaný pohled umožňující detekci událostí ovlivňujících více systémů.

3.3 Správa bezpečnostních informací a událostí

Nástroje SIEM kombinují schopnosti SIM a SEM. SIEM shromažďuje, organizuje a analyzuje bezpečnostní aktivity z mnoha hardwarových a softwarových zdrojů v IT infrastruktuře organizace.

SIEM agreguje data jak v reálném čase, tak i historická data z routerů, switchů, serverů, počítačů, antivirů, firewallů, IPS/IDS, podnikových aplikací, databází a dalších. Na tato data aplikuje předem definovaná analytická pravidla pro identifikaci hrozeb, vzorců chování a podezřelých aktivit, které vyžadují akci nebo vyšetření administrátora.

Kromě primárního účelu, kterým je bezpečnost, mnoho podniků využívá SIEM také k prokázání souladu s regulacemi a standardy na ochranu dat, jako jsou GDPR, HIPAA, PCI-DSS nebo SOX. SIEM může být užitečný i pro správu kapacity zdrojů, kdy umožňuje sledovat růst dat a využití šířky pásma v čase a proaktivně plánovat budoucí potřeby.[4]

Klíčové vlastnosti SIEM:

- Kombinace schopností SIM a SEM.
- Sběr a analýza bezpečnostních dat z různých zdrojů v IT infrastruktuře.
- Aplikace analytických pravidel pro detekci hrozeb a podezřelých aktivit.
- Podpora vyšetřování bezpečnostních incidentů a reakce na ně.
- Využití pro prokazování souladu s regulacemi a pro správu kapacity.

Shrnutí hlavních rozdílů:

- SIM se zaměřuje na sběr a správu logů, SEM se zaměřuje na monitorování a analýzu událostí, SIEM kombinuje oba přístupy.

- SIM typicky využívá agenty, SEM a SIEM agregují data z různých zdrojů.
- SEM poskytuje real-time upozornění a korelaci událostí z více systémů, což SIM typicky neumožňuje.
- SIEM přidává pokročilou analýzu, podporu vyšetřování, prokazování souladu a správy kapacity.

3.4 EDR/XDR

Počet koncových zařízení se neustále zvyšuje, stejně jako jejich rozmanitost. Už se nejedná pouze o notebooky a pracovní stanice. S rostoucím počtem vzdálených pracovníků se také zvyšuje potřeba zabezpečit a monitorovat různá koncová zařízení a jejich vzájemná propojení v celém prostředí organizace.

Koncová zařízení zůstávají hlavním vstupním bodem pro kybernetické útoky, často pomocí phishingu. Proto se strategie zabezpečení koncových bodů staly pro podniky kritickou potřebou. Antivirová ochrana sama o sobě již nestačí na ochranu před sofistikovanými kybernetickými hrozbami.

EDR se zaměřuje na zabezpečení koncových bodů a poskytuje přehled a kontrolu nad zařízeními, jako jsou stolní počítače, notebooky a mobilní zařízení. Řešení EDR monitorují aktivity a chování koncových zařízení tak, aby mohly detekovat bezpečnostní incidenty a reagovat na ně. Poskytují detailní informace o každém koncovém bodu, jako jsou aktivity procesů, změny souborů, síťová spojení a systémové události, což bezpečnostním týmům umožňuje rychle identifikovat hrozby a reagovat na ně.

Na druhé straně XDR zaujímá širší přístup k zabezpečení celého podniku. Poskytuje bezpečnostním týmům ucelený pohled na stav zabezpečení organizace, aby mohly rychle a informovaně rozhodovat o detekci hrozeb a reakci na ně. XDR nativně integruje data z více bezpečnostních produktů, včetně EDR, síťové bezpečnosti, cloudové bezpečnosti a e-mailové bezpečnosti, a poskytuje tak jednotný pohled na bezpečnostní hrozby v celé organizaci.

Obvykle jsou tato různá bezpečnostní řešení sjednocena a nabízena dodavatelem XDR, ale XDR může podporovat i technologie třetích stran prostřednictvím partnerství nebo předkonfigurovaných bezproblémových integrací. Řešení XDR využívají pokročilé analýzy a algoritmy strojového učení k identifikaci a prioritizaci hrozeb, automatizaci pracovních postupů reakce na incidenty a poskytování praktických poznatků pro zlepšení bezpečnostních operací. XDR také aplikuje průběžně aktualizované informace o hrozbách, aby přidalo kontext a umožnilo lepší detekci.[5]

4 DATA A NÁSTROJE PRO JEJICH SBĚR

4.1 Data ze sítě

V dnešní době, kdy se většina komunikace odehrává prostřednictvím počítačových sítí, je analýza síťových dat důležitým nástrojem pro zajištění kybernetické bezpečnosti. Síť představuje bohatý zdroj informací, které lze využít k odhalení potenciálních zranitelností a hrozeb.

Jak je zmíněno v kapitole 2.1 Management zranitelností a jejich podkapitolách, ze sítě lze získat dva základní typy dat:

- Průtoková data (flow data) — poskytují informace o síťovém provozu mezi zařízeními, včetně zdrojů, cílů a typů přenášených dat. Umožňují analyzovat provoz na vysoké úrovni a identifikovat vzorce komunikace a anomálie.
- Paketová data — nabízejí podrobný pohled na konkrétní síťové pakety, včetně obsahu dat a informací z hlaviček. Jsou nezbytná pro hlubší analýzu a detekci pokročilých hrozeb, jako jsou specifické malwary či škodlivé komunikace.

Významnou vlastností síťových dat je jejich standardizace. Komunikace mezi hostiteli v síti využívá univerzálně uznávané protokoly a formáty hlaviček, což usnadňuje analýzu a detekci hrozeb. Standardizace v síťové komunikaci přináší několik výhod pro detekci zranitelností:

- Bez ohledu na typy zařízení nebo aplikací v síti můžeme očekávat, že data budou sledovat určité formáty a protokoly.
- Tato předvídatelnost umožňuje vývoj robustních nástrojů a metod pro monitorování a analýzu síťového provozu.
- Díky standardizaci lze efektivněji nasazovat bezpečnostní opatření a automatizovat detekci hrozeb.[10]

Analýza síťových dat hraje nezastupitelnou roli v zajištění kybernetické bezpečnosti. Standardizace síťové komunikace usnadňuje detekci zranitelností a hrozeb, což dokazují i úspěšné výzkumné projekty, jako je FETA.[6] Při hledání a řešení bezpečnostních problémů by proto měla být síť prvním místem, kam se obrátit, neboť poskytuje cenné informace potřebné pro účinnou ochranu IT infrastruktury.

4.1.1 Network Mapper

Nmap je bezplatný open-source nástroj pro průzkum sítě a audit zabezpečení, který slouží k aktivnímu průzkumu, jehož cílem je interakce s hosty a přímé ověření zranitelností. Je hojně využíván systémovými a síťovými administrátory pro úkoly jako

inventarizace sítě, správa aktualizačních plánů a monitorování dostupnosti hostitelů či služeb.

Výhody Nmapu:

- Okamžitá odezva na nově objevené zranitelnosti v síti.
- Proaktivní přístup umožňuje včasné odhalení zranitelností.

Nevýhody Nmapu:

- Ověření přítomnosti zranitelnosti může omezit dostupnost běžící aplikace nebo celého hosta.
- Provedení komplexního skenování vyžaduje detailní plánování, aby nedošlo k nečekanému přetížení síťových prvků.
- Periodické skenování stejných zranitelností nemusí být efektivní v porovnání s riziky, která přináší.
- Interpretace výsledků skenování často vyžaduje zkušeného analytika.

Nmap efektivně využívá IP pakety k zjištění dostupných hostitelů v síti, identifikaci nabízených služeb včetně jejich verzí, operačních systémů, použitých firewallů a dalších charakteristik. Je navržen pro efektivní skenování rozsáhlých sítí, ale je účinný i pro jednotlivé hostitele. Nmap je kompatibilní s hlavními operačními systémy a je dostupný v textovém i grafickém rozhraní.

Určení, zda je služba na dálku zranitelná nebo již opravená, může být komplikované. Získání verze aplikace pomocí hlaviček nebo bannerů často nestačí, protože výrobci operačních systémů mohou implementovat bezpečnostní opravy bez změny verze (tzv. backport). Nejspolehlivějším ověřením zranitelnosti je její aktivní využití, což však může způsobit pád služby a vyvolat dlouhé hodiny frustrace, pokud není služba opravená.[11]

4.1.2 Nessus

Nessus od společnosti Tenable je jedním z předních nástrojů pro detekci zranitelností. Je známý svou schopností rychle skenovat síť a identifikovat bezpečnostní slabiny v systémech a aplikacích. Tento software slouží k posouzení bezpečnosti tím, že prohledává sítě a hledá zranitelnosti, jako jsou zastaralé softwary, špatně nakonfigurované systémy nebo známé slabiny, které mohou útočníci zneužít. Nessus je tedy nástrojem pro aktivní průzkum sítě, podobně jako Nmap.

Nessus patří do portfolia produktů Tenable, které zahrnuje také Tenable.io pro cloudovou bezpečnost a Tenable.sc pro řízení zranitelností ve velkých organizacích. Tenable tak nabízí komplexní řešení pro audit a zabezpečení IT infrastruktury.

Nessus je využíván v různých průmyslových odvětvích pro detekci zranitelností a posouzení bezpečnosti. Umožňuje automatické skenování sítě, analýzu nalezených dat a generování přehledných reportů, které organizacím pomáhají pochopit a řešit bezpečnostní rizika. Díky své flexibilitě a rozsáhlé databázi známých zranitelností je Nessus efektivním nástrojem pro bezpečnostní týmy v rámci pravidelného bezpečnostního monitoringu a auditu.

Společnost Tenable nabízí tři verze svého nástroje Nessus: Essentials, Professional a Expert. Nessus Essentials je bezplatná verze určená pro vzdělávací účely, studenty a jednotlivce začínající v oblasti kybernetické bezpečnosti, umožňující skenovat až 16 IP adres. Nessus Professional je prvním krokem k pokročilejším nabídkám, zaměřeným na konzultanty, penetrační testery a malé a střední podniky, poskytující neomezené skenování IT prostředí pro odhalení zranitelností.

Nessus Expert je prémiová nabídka, která rozšiřuje možnosti verze Professional o dva další prvky. Prvním je skenování webových aplikací (DAST), které poskytuje komplexní přehled o bezpečnostních problémech webových aplikací, včetně zranitelností v vlastním aplikačním kódu i ve zranitelných verzích komponent třetích stran. Druhou funkcionalitou je skenování IaC, umožňující kontrolu kódových repozitářů před nasazením, což zabraňuje neúmyslnému zanesení zranitelností do cloudu. Nessus Expert také umožňuje skenovat až 5 domén pro odhalení a posouzení všech přidružených subdomén, s možností rozšíření v případě potřeby.[12]

Hlavní výhodou Nessus je jeho ucelený výstup. Kromě samotného skenu je možné získaná data přímo převést do připraveného přehledného reportu, který lze prezentovat dále nebo předat příslušnému organizačnímu celku k nápravě. Další výhodou jsou optimalizované skeny a aktualizované databáze zranitelností ve formě běžných chybných konfigurací a základních přihlašovacích údajů od různých výrobců. Tyto databáze umožňují odstranit většinu běžných zranitelností ještě před jejich objevením útočníkem.[13]

Nessus získává svou databázi zranitelností z vlastního výzkumu společnosti Tenable a také z veřejně dostupných zdrojů, jako jsou databáze CVE. Tenable průběžně aktualizuje svou databázi, aby zajistila, že Nessus dokáže detekovat nejnovější hrozby. Frekvence aktualizací závisí na zvoleném licenčním modelu, ale obecně jsou vydávány každý den nebo každý týden.

4.1.3 Open Vulnerability Assessment System

OpenVAS je open-source nástroj pro skenování zranitelností v síťové infrastruktuře a aplikacích. Jedná se o komplexní řešení, které umožňuje automatizované testování známých zranitelností a slabých míst v zabezpečení systémů. OpenVAS původně vznikl v roce 2006 jako fork tehdy proprietárního Nessusu a zpočátku na něm pracovaly firmy Intevation a DN-Systems. V roce 2008 došlo k významnému milníku, kdy byla založena společnost Greenbone, která začala projekt OpenVAS aktivně rozvíjet a podporovat.

I po zapojení společnosti Greenbone zůstává OpenVAS dostupný jako open-source nástroj. Greenbone však nabízí i komerční produkty a služby postavené na této technologii, jako je Greenbone Vulnerability Management. Společnost také významně přispívá do open-source komunity. V roce 2017 došlo k přejmenování frameworku z "OpenVAS"na "Greenbone Vulnerability Management"(GVM) počínaje verzí GVM-10, která následovala po OpenVAS-9. Kód zůstal open-source. Další milníky ve vývoji zahrnují přechod od protokolu OTP k OSP ve verzi GVM-11, změnu verzování na kalendářní model ve verzi GVM 20.08 nebo představení skeneru Notus ve verzi 22.4.

Architektura OpenVAS se skládá z několika komponentů. Skener provádí samotné testování pomocí databáze NVT, která obsahuje tisíce testů pro různé operační systémy, síťové služby a aplikace. Výsledky skenování jsou ukládány a spravovány v databázi, ke které lze přistupovat přes webové rozhraní nebo API. Tato centralizovaná architektura umožňuje efektivní správu a analýzu výsledků skenování z jediného místa. OpenVAS také podporuje distribuované skenování pomocí slave skenerů, což umožňuje škálování na rozsáhlé infrastruktury.

OpenVAS nabízí řadu funkcí pro efektivní správu zranitelností. Umožňuje plánování pravidelných skenů, konfiguraci politiky testování a generování podrobných reportů. Nástroj také poskytuje doporučení pro nápravu nalezených zranitelností a umožňuje jejich sledování v čase. Integruje se s dalšími bezpečnostními nástroji a podporuje automatizaci pomocí skriptů. OpenVAS také nabízí možnost vytváření vlastních testů a rozšíření databáze NVT pro specifické potřeby organizace. Díky pravidelnému skenování a včasnému odhalení zranitelností pomáhá OpenVAS snižovat riziko úspěšných útoků a minimalizovat potenciální dopady na organizaci.

Jednou z hlavních výhod OpenVAS je jeho otevřenost a rozšiřitelnost. Komunita kolem projektu, včetně společnosti Greenbone, aktivně přispívá k vývoji a aktualizaci databáze testů, což zajišťuje pokrytí nejnovějších hrozeb. OpenVAS je také multiplatformní a lze jej nasadit na různých operačních systémech, jako jsou Linux, Windows nebo macOS. Otevřený zdrojový kód umožňuje uživatelům kontrolovat a upravovat nástroj podle svých potřeb, což je výhodné pro organizace s přísnými bezpečnostními požadavky.[14]

Při používání OpenVAS je nezbytné analyzovat a prioritizovat výsledky na základě kritičnosti aktiv a potenciálního dopadu zranitelností. OpenVAS by měl být součástí širšího programu řízení zranitelností, který zahrnuje pravidelné aktualizace, penetrační testování a další bezpečnostní opatření. Je také důležité zajistit, aby byl OpenVAS sám o sobě zabezpečený a nakonfigurovaný podle best practices, aby se předešlo jeho zneužití útočníky. Pravidelné aktualizace a sledování bezpečnostních oznámení týkajících se samotného OpenVAS jsou klíčové pro udržení jeho integrity.

Při implementaci OpenVAS je vhodné zvážit začlenění dalších bezpečnostních nástrojů a technik, jako jsou pravidelné aktualizace a patchování systémů, používání silné autentizace a řízení přístupu, monitorování sítě a detekce anomálií a implementace bezpečnostních politik a postupů.

Díky kombinaci open-source základů a komerční podpory ze strany společnosti Greenbone zůstává OpenVAS důležitým nástrojem pro organizace, které chtějí posílit svůj bezpečnostní postoj a snížit riziko úspěšných kybernetických útoků.

4.1.4 Srovnání Nessus a OpenVAS

Nessus a OpenVAS jsou dva široce využívané nástroje pro skenování zranitelností v počítačových sítích a systémech. Oba dokáží detekovat širokou škálu bezpečnostních slabin, od chybějících bezpečnostních záplat přes slabá hesla až po nesprávně nakonfigurované služby. Používají se k pravidelnému bezpečnostnímu auditu IT infrastruktury a pomáhají organizacím udržovat jejich systémy zabezpečené a chráněné před potenciálními útoky.

Nessus je komerční nástroj vyvíjený společností Tenable, zatímco OpenVAS je open-source projekt s velkou komunitou uživatelů a vývojářů. Nessus nabízí pokročilejší funkce a širší pokrytí zranitelností díky své rozsáhlé databázi, která obsahuje přes 50 000 kontrol. Je také rychlejší při skenování a podporuje více operačních systémů včetně Windows a různých linuxových distribucí. Nessus nabízí i více možností exportu výsledných reportů.

OpenVAS, na druhou stranu, těží z výhod open-source modelu. Zájemci mohou zkoumat a upravovat jeho zdrojový kód a přizpůsobovat si ho podle svých potřeb. I když má menší databázi zranitelností (kolem 26 000 kontrol), OpenVAS umí lépe pracovat s falešně pozitivními nálezy a poskytuje nástroje pro jejich analýzu. Jako open-source řešení je také zcela zdarma, což z něj dělá atraktivní volbu zejména pro menší organizace a projekty s omezeným rozpočtem.

Oba nástroje každopádně představují důležitou součást komplexní strategie kybernetické bezpečnosti. Pravidelné skenování pomáhá identifikovat slabá místa v zabezpečení sítě a systémů a poskytuje cenné podklady pro jejich nápravu. Reporty generované

těmito nástroji obsahují detailní informace o nalezených zranitelnostech včetně jejich závažnosti a doporučených kroků k remediacím. Správci IT infrastruktury tak mohou efektivně prioritizovat bezpečnostní upgrady a záplatování a průběžně zvyšovat celkovou úroveň zabezpečení organizace.[15]

Srovnání Nessus vs OpenVAS:

- Nessus je placený, OpenVAS je open-source a zdarma
- Nessus má větší databázi zranitelností (50 000+ vs 26 000)
- Nessus je rychlejší a detekuje více slabin
- Nessus podporuje více OS (Windows, Linux), OpenVAS jen Linux
- Nessus má více možností exportu reportů
- OpenVAS umožňuje analýzu falešně pozitivních nálezů
- OpenVAS lze upravovat a přizpůsobovat díky open-source kódu

4.1.5 Suricata a Snort

Suricata a Snort jsou open-source nástroje pro pasivní monitoring sítě. Oba nástroje jsou si v základních funkcích velmi podobné, hlavní rozdíl spočívá ve využití procesoru hosta. Zatímco Snort ve verzi 2.x je jednovláknová aplikace, Suricata dokáže škálovat své worker procesy na teoreticky neomezené množství jader procesoru. S příchodem Snortu 3 se však situace mění, neboť i ten již podporuje vícevláknové zpracování. Přesto ale Suricata stále nabízí některé pokročilejší funkce a vyšší výkon.

Suricata je vysoce výkonný síťový IDS, IPS a NSM systém. Tento open-source projekt se široce používá pro analýzu síťového provozu s cílem identifikovat potenciální bezpečnostní hrozby, jako jsou útoky, komunikace malwaru v síti a zranitelnosti. Suricata je známá svou schopností zpracovávat velké objemy dat v reálném čase, což z ní dělá nejen ideální nástroj pro použití v rozsáhlých a náročných síťových prostředích, ale lze ji použít i pro monitoring malé domácí sítě nebo kanceláře. Běžně dostupnými metalickými síťovými kartami je schopná zvládnout provoz o nízkých desítkách gigabitů za sekundu. Je však nutné zmínit, že výkon závisí na mnoha faktorech, především na výkonu hardwaru, množství a optimalizaci detekčních pravidel a na optimalizaci konfigurace samotného nástroje a jeho přizpůsobení na hardware.

Snort ve verzi 3 přichází s řadou významných vylepšení, jako je nový parser a syntaxe pravidel, podpora vícevláknového zpracování, sdílená konfigurace, přístup k množství pluginů, vylepšené zpracování TCP a pravidel. V mnoha ohledech tak dohání nebo

předhání Suricatu. Nicméně Suricata stále drží náskok v některých pokročilých funkcích a celkovém výkonu.[16]

Jednou z hlavních předností Suricaty je její pokročilá detekční schopnost, která využívá signatury, anomálie v síťovém provozu a pokročilé analýzy protokolů k identifikaci potenciálně škodlivého chování. Suricata podporuje rozsáhlé sady pravidel, které lze přizpůsobit a aktualizovat podle specifických bezpečnostních potřeb organizace. To umožňuje efektivně reagovat na nejnovější hrozby a zranitelnosti. V tomto ohledu nabízí Suricata stále více možností než Snort.[17]

Díky modularitě a flexibilitě lze Suricatu i Snort integrovat s dalšími bezpečnostními nástroji a technologiemi, což umožňuje vytvořit komplexní bezpečnostní řešení. Například je lze propojit se systémy 3.3 SIEM, což poskytuje centralizovaný přehled o bezpečnostním stavu síťového prostředí a usnadňuje rychlou reakci na identifikované hrozby.

Při monitorování rozsáhlých sítí se však objevuje problém se sběrem a dopravou dat k monitorovacímu prostředku. V případě, že monitoring neprovádíme pouze na vstupní bráně, ale i na vnitřních segmentech sítě, je nutné zajistit dopravu dat z těchto segmentů k centrálnímu monitorovacímu prostředku. To může vést k významnému zatížení sítě přenosem duplicitního provozu. Řešením tohoto problému může být použití distribuovaného monitoringu a zpracovávat data lokálně v segmentu kde se vyskytují. V případě, že jsou instance Suricaty nasazeny na jednotlivých segmentech sítě a jejich výstupy jsou pak agregované na centrálním serveru, přenosem zpracovaných dat se objem přenášeného provozu zmenší na desetinu nebo méně podle detailnosti výstupu. Při nasazování Suricaty v rozsáhlých sítích je tedy důležité pečlivě zvážit architekturu monitoringu a zvolit vhodné metody pro sběr a přenos dat tak, aby se minimalizovalo zatížení sítě a zároveň se zachovala efektivita detekce hrozeb.

4.2 Systémové logy

Sběr a analýza systémových logů hraje nezastupitelnou roli v detekci zranitelností, protože poskytuje cenné informace o chování systému, které mohou indikovat potenciální slabiny. Sběr systémových logů je pro maximální účinost a výtěžnost lepší provádět ze serverů a uživatelských stanic provozujících systémy Windows a Linux. Jak tento proces může přispět k detekci zranitelností?

Linuxové systémy nabízejí mnoho nástrojů a služeb pro zaznamenávání systémových událostí. Jádro systému a většina služeb produkují logovací záznamy, které jsou typicky ukládány ve `/var/log`. Pro sběr a centralizaci logů lze využít nástroje jako je **rsyslog** nebo **syslog-ng**, které umožňují flexibilní konfiguraci a přesměrování logů na centrální logovací server. Analýza těchto logů může odhalit neobvyklé chování, jako jsou opako-

vané neúspěšné pokusy o přihlášení, neautorizované přístupy k souborům nebo spuštění neznámých procesů, což mohou být indikátory zranitelností nebo probíhajících útoků.

Windows systémy ukládají události do Logu událostí Windows, které jsou přístupné přes Prohlížeč událostí. Tyto logy jsou rozděleny do několika kategorií, včetně logů aplikací, bezpečnosti, setupu, systému a předávaných událostí. Pro detekci zranitelností jsou zvláště důležité bezpečnostní logy, které obsahují informace o úspěšných a neúspěšných pokusech o přihlášení, změnách politik bezpečnosti a dalších bezpečnostních událostech. Windows Server umožňuje konfiguraci zásad auditu, které mohou být nastaveny pro sledování specifických typů událostí. Pro centralizovaný sběr logů lze využít nástroje jako WEF společně s WEC serverem.

Ať už sběr logů probíhá na Linuxových nebo Windows systémech, klíčem k efektivní detekci zranitelností je systematická analýza shromážděných dat. Moderní nástroje pro správu logů a 3.3 SIEM systémy umožňují agregovat, normalizovat a analyzovat velké objemy logů z různých zdrojů. Použitím pravidel, algoritmů strojového učení a korelace událostí, tyto systémy pomáhají identifikovat podezřelé aktivity, které by mohly naznačovat přítomnost zranitelností v systému. Bohužel detekce zranitelní tímto způsobem je zároveň největší slabinou takového pasivního sytému. Jedná se totiž o detekci ex-post kdy dostáváme informaci o tom, že o zranitelnosti už někdo ví a pokouší se jí zneužít. V případě, že logové záznamy z nějakého důvodu přestanou docházet, je otázkou jestli sbíráme dostatečné množství logových záznamů, abychom dokázali detekovat zda se zranitelnost podařilo zneužít, nebo útočník vzdal své snahy.

Sběr a analýza systémových logů je zásadní pro odhalování a řešení zranitelností v IT infrastruktuře. Ačkoli se procesy sběru logů liší mezi Linuxovými a Windows systémy, cíl zůstává stejný: získat přehled o chování systému, který umožní včasné detekování a reakci na bezpečnostní hrozby.

4.2.1 Windows

Systémy Windows jsou používány hlavně ve firemních sítích, což z nich činí lákavý cíl pro kybernetické útočníky. K efektivní ochraně před útoky a zneužitím zranitelností je nezbytné provádět důkladný sběr a analýzu logů. WEF a WEC jsou hlavní komponenty, které umožňují efektivní sběr logů ve Windows prostředí, a umožňují tak detekci zranitelností.

WEF umožňuje automatické předávání událostí z různých Windows počítačů do centrálního umístění, což usnadňuje monitorování a analýzu. Tento proces funguje bez potřeby agentů na klientech, což zjednodušuje nasazení a údržbu. Administrátoři mohou konfigurovat skupinové politiky, aby určili, které události budou předávány, což umožňuje zaměřit se na konkrétní logy relevantní pro bezpečnostní monitorování. Vy-

užití WEF pro detekci zranitelností spočívá ve schopnosti shromažďovat logy zabezpečení, aplikací a systému z různých strojů na jednom místě. To zahrnuje záznamy o neúspěšných pokusech o přihlášení, změnách v konfiguraci zabezpečení, používání privilegovaných účtů a mnoho dalších. Shromažďováním těchto dat mohou bezpečnostní analytici lépe identifikovat vzorce chování, které naznačují pokusy o zneužití zranitelností.

WEC je služba na straně serveru, která přijímá logy odeslané pomocí WEF z klientů. WEC může být nakonfigurován pro přijímání logů od libovolného počtu klientů, což umožňuje centralizovanou analýzu a uchovávání logů. Kombinace WEC s pokročilými nástroji pro analýzu logů a SIEM řešeními vytváří silný systém pro odhalování podezřelých aktivit a potenciálních zranitelností v síti. Konfigurace WEC zahrnuje nastavení událostí, kde administrátoři specifikují, které typy logů mají být sbírány, a filtrování, které umožňuje výběr pouze těch záznamů, které jsou relevantní pro bezpečnostní potřeby organizace. Tím se zajistí, že analytici se nebudou muset prokousávat nepotřebnými daty a mohou se soustředit na skutečně důležité informace.[18]

Použitím WEF a WEC pro centralizovaný sběr a analýzu logů mohou organizace výrazně zlepšit svou schopnost rychle detekovat a reagovat na zranitelnosti. Například, zvýšený počet neúspěšných pokusů o přihlášení z neobvyklých geografických lokací může indikovat pokusy o útok hrubou silou na slabá hesla. Podobně, detekce neobvyklých změn v konfiguraci systému nebo aplikací může naznačovat přítomnost malware nebo zneužití zranitelnosti k získání zvýšených oprávnění.

Sběr a analýza logů jsou základními kameny pro efektivní detekci zranitelností ve Windows prostředí. Implementací WEF a WEC, společně s pokročilými analytickými nástroji, mohou organizace zlepšit své bezpečnostní operace, rychle identifikovat potenciální zranitelnosti a zamezit kybernetickým útokům dříve, než způsobí škody. Tento proaktivní přístup k bezpečnosti je nezbytný v současném neustále se měnícím kybernetickém prostředí.

4.2.2 Linux

Základem pro sběr bezpečnostních dat v systémech založených na Linuxu je Linux Audit Subsystem. Tento subsystém je typicky nainstalován na většině distribucí, avšak jeho konfigurace je v rukou administrátorů. Kromě Linux Audit Subsystemu existují i další nástroje a služby, které mohou být použity pro detekci zranitelností a monitorování bezpečnosti, jako například SELinux, AppArmor nebo různé antivirové a anti-malware programy. Ačkoliv je možné využít různé agentní systémy, detekce zranitelností přímo v systému je komplexní výzvou, zejména kvůli nutnosti periodického auditu. Tento proces je třeba přizpůsobit specifickému využití operačního systému a

zohlednit fakt, že periodický audit může zatěžovat systém, což může ovlivnit provoz produkčních systémů.

Pasivní detekce zranitelností na systému Linux spočívá v monitorování a analýze dat, která systém generuje během normálního provozu. Zde se uplatňují logovací systémy, zaznamenávající široké spektrum událostí, včetně systémových chyb a neautorizovaných přístupů. Logy neúspěšných pokusů o přihlášení mohou odhalit pokusy o útoky hrubou silou, zatímco záznamy systémových chyb naznačují možné slabiny v softwaru. Tato metoda však často vede k odhalení zranitelností až po jejich zneužití, případně pokusu o jejich zneužití. Navíc logy nemusí vždy zachytit všechny pokusy o útok nebo zneužití zranitelností, zejména pokud útočník použije sofistikované techniky pro skrytí své aktivity. Následuje příklad záznamu logu o neúspěšném přihlášení:

```
1 Jun 10 10:22:33 debian sshd[17345]: Failed password for invalid user admin from
    192.168.1.25 port ssh2
```

Listing 1 : Ukázka logu špatného přihlášení

Na druhou stranu, aktivní detekce zahrnuje přímé testování bezpečnosti systému, často prostřednictvím simulovaných útoků nebo skenování agentem uvnitř běžícího operačního systému. Tyto metody mohou efektivně identifikovat zranitelnosti dříve, než je útočník objeví nebo zneužije. Hlavní výhodou je možnost proaktivního objevení slabých míst, ale je třeba brát v úvahu potenciální zátěž pro systém, kterou je předem těžké definovat a v produkčním prostředí může představovat problém. Některé typy skenování mohou způsobit výpadky služeb nebo poškodit data, proto je důležité pečlivě naplánovat a otestovat tyto aktivity před jejich nasazením v produkčním prostředí.

Kombinace pasivních a aktivních metod detekce zranitelností, doplněná o efektivní využití logovacích systémů, zajistí robustní obranu proti kybernetickým hrozbám v Linuxových systémech. Pro dosažení nejvyšší možné bezpečnosti je nezbytné pravidelně auditovat systémy a přizpůsobit bezpečnostní opatření aktuálním hrozbám. Pravidelný audit a aktualizace bezpečnostních opatření by měly být doplněny také o pravidelné zálohování dat, testování obnovy ze záloh a školení uživatelů v oblasti bezpečnosti. Tento přístup umožňuje nejen identifikovat a řešit stávající zranitelnosti, ale také poskytuje proaktivní obranu proti nově vznikajícím bezpečnostním výzvám, čímž výrazně zvyšuje odolnost IT infrastruktury.

V souhrnu, detekce zranitelností v Linuxových systémech vyžaduje kombinaci pasivních a aktivních metod, společně s dalšími bezpečnostními opatřeními, jako jsou pravidelné zálohy, testování obnovy a školení uživatelů. Pasivní metody zahrnují monitorování systémových logů a analýzu dat generovaných během běžného provozu, ale nemusí vždy zachytit všechny pokusy o útok. Aktivní metody spočívají v přímém testování bezpečnosti systému pomocí simulovaných útoků nebo skenování, ale je třeba vzít v úvahu jejich potenciální dopad na výkon a stabilitu systému, zejména v produkč-

ním prostředí. Pravidelný audit, aktualizace bezpečnostních opatření a další zmíněné praktiky jsou důležité pro zajištění vysoké úrovně bezpečnosti Linuxových systémů.

4.3 Korelace dat

Korelace dat je klíčovým aspektem pro rychlou detekci a ověření zranitelností v infrastruktuře. Jedná se o proces kombinování a analýzy dat z různých zdrojů, jako jsou síťové logy, logy operačních systémů, data z bezpečnostních zařízení a další relevantní informace. Důležitou součástí tohoto procesu je také integrace dat z externích zdrojů, jako jsou TI zdroje a databáze jako AbuseIPDB, MISP a OTX. Cílem korelace dat je identifikovat souvislosti a vzorce, které mohou naznačovat přítomnost zranitelností nebo pokusů o jejich zneužití.

Začlenění dat z TI zdrojů a databází poskytuje další cenné informace pro rychlejší a přesnější detekci hrozeb. Tyto zdroje často obsahují informace o známých škodlivých IP adresách, doménách, IoC a dalších artefaktech souvisejících s kybernetickými hrozbami. Například korelace mezi podezřelou aktivitou zaznamenanou v interních logách a informacemi o škodlivých IP adresách z databáze AbuseIPDB může naznačovat probíhající pokus o útok z již známého zdroje hrozeb.

Platformy jako MISP umožňují sdílení a korelaci informací o hrozbách mezi organizacemi a bezpečnostními komunitami. Začlenění dat z MISP do procesu korelace může poskytnout včasné varování o nově se objevujících hrozbách a zranitelnostech, které byly identifikovány jinými organizacemi. Například korelace mezi podezřelým chováním zaznamenaným v interních systémech a IoC sdílenými prostřednictvím MISP může pomoci rychle identifikovat a potvrdit přítomnost specifické hrozby v infrastruktuře.[20]

Databáze TI, jako je například OTX, MISP nebo komerční služby typu FireEye iSIGHT Intelligence, jsou cenným zdrojem informací o hrozbách. Tyto platformy agregují data z různých veřejných i privátních zdrojů, včetně zpravodajských služeb, bezpečnostních týmů, honeypotů a dalších senzorů. Korelace dat z těchto TI zdrojů s interními logy a dalšími daty může pomoci identifikovat souvislosti mezi pozorovanou aktivitou a známými hrozbami. Například detekce komunikace s IP adresou nebo doménou, která je v těchto databázích označena jako součást botnetu, malwarové kampaně nebo je spojována s útočníky typu APT, může signalizovat, že došlo ke kompromitaci systému. TI tak poskytuje dodatečný kontext a umožňuje lépe pochopit povahu hrozeb a zacílit bezpečnostní opatření.

Začlenění dat z TI zdrojů a online databází do procesu korelace dat přináší několik výhod:

1. Poskytuje dodatečný kontext a informace, které mohou usnadnit identifikaci a potvrzení bezpečnostních incidentů.

2. Umožňuje rychlejší reakci na nově se objevující hrozby, protože organizace mohou využít znalosti a zkušenosti širší bezpečnostní komunity.

3. Pomáhá prioritizovat bezpečnostní incidenty na základě známé závažnosti a dopadu souvisejících hrozeb.

Je však důležité poznamenat, že efektivní integrace dat z TI zdrojů a databází vyžaduje pečlivé plánování a implementaci. Organizace musí zajistit, aby data byla spolehlivá, aktuální a relevantní pro jejich konkrétní prostředí. Je také nutné věnovat pozornost aspektům, jako je správa a ochrana citlivých informací, dodržování právních a regulačních požadavků a zajištění interoperability mezi různými systémy a platformami.

Korelace dat, včetně integrace informací z TI zdrojů a online databází je mocným nástrojem pro rychlou detekci a ověření zranitelností v infrastruktuře. Poskytuje dodatečný kontext, usnadňuje identifikaci hrozeb, umožňuje rychlejší reakci a pomáhá prioritizovat bezpečnostní incidenty. Při správné implementaci může výrazně přispět ke zvýšení celkové úrovně zabezpečení a odolnosti organizace vůči kybernetickým hrozbám.[19]

4.4 Detekce anomálií

Detekce anomálií je důležitou součástí procesu identifikace a ověřování zranitelností v infrastruktuře, protože detekce anomálií umožňuje odhalit neobvyklé vzorce a chování, které mohou naznačovat přítomnost bezpečnostních hrozeb. Nicméně, je třeba pečlivě volit parametry a pravidla pro detekci anomálií, aby nedocházelo k zahlcení falešnými poplachy.

Při detekci zranitelností je důležité si uvědomit, že přítomnost anomálie nemusí nutně znamenat existenci zranitelnosti. Anomálie však mohou sloužit jako indikátory potenciálních problémů nebo probíhajících útoků, které ještě nebyly odhaleny jinými bezpečnostními mechanismy. Proto je detekce anomálií cenným nástrojem pro včasnou identifikaci neznámých zranitelností a hrozeb. Je však třeba najít rovnováhu mezi citlivostí detekce a množstvím generovaných upozornění, aby bezpečnostní týmy nebyly zahlceny a mohly se efektivně zaměřit na nejvýznamnější incidenty. Příkladem takové nechtěné anomálie může být příjem špatných přihlašovacích údajů v pondělí ráno.

V kontextu operačních systémů můžeme sledovat různé typy anomálií, které mohou naznačovat přítomnost zranitelností nebo podezřelých aktivit. Například neobvyklý nárůst počtu přihlášení, zejména z neznámých zdrojů nebo v neobvyklých časech, může signalizovat pokusy o neoprávněný přístup. Objevení nových aplikací nebo procesů, které nebyly schváleny, může naznačovat instalaci malwaru nebo neautorizovaného soft-

waru. Otevření neobvyklých síťových portů nebo pokusy aplikací o přístup do nestandardních částí systému mohou také indikovat potenciální bezpečnostní problémy.

V síťovém prostředí lze detekovat anomálie na základě různých faktorů. Přítomnost neobvyklých protokolů, jako je například nešifrovaný HTTP provoz v prostředí, kde je standardem HTTPS, může naznačovat pokusy o obcházení bezpečnostních opatření. Využívání neobvyklých technik, jako je zneužití DNS TXT záznamů pro command-and-control komunikaci, může být známkou probíhajícího útoku. Neobvyklá síťová aktivita mimo běžné pracovní hodiny může také indikovat podezřelé chování, které vyžaduje další vyšetřování.

Velký pokrok v oblasti detekce anomálií a obecně v kybernetické bezpečnosti přináší zavádění umělé inteligence a strojového učení. Tyto technologie umožňují analyzovat obrovské objemy dat a odhalovat vzorce a anomálie, které by mohly být pro lidské analytiky obtížně odhalitelné, nebo umožňují filtrování anomálií a výběr opravdu závažných vzorců pro analýzu lidksými analitiky. Modely umělé inteligence a strojového učení se mohou učit z historických dat a adaptovat se na měnící se prostředí, což umožňuje efektivnější detekci nových a neznámých hrozeb. Nicméně, jejich implementace vyžaduje pečlivý přístup, aby se minimalizovalo riziko falešných poplachů a zajistila se transparentnost a interpretovatelnost výsledků.[21]

5 ZDROJE DAT PRO DETEKCI ZRANITELNOSTÍ

Při detekci zranitelností v infrastruktuře je důležité využívat různé zdroje informací, které mohou poskytnout cenné poznatky o potenciálních hrozbách. Threat Intel neboli zpravodajství o hrozbách je hlavním zdrojem informací pro detekci aktuálně zneužívaných zranitelností. Společnosti jako Eset, Mandiant, Future Recorded, CrowdStrike, FireEye aj. poskytují aktuální informace o nových hrozbách, trendech v oblasti kybernetické bezpečnosti a IoC. Tyto informace mohou pomoci bezpečnostním týmům identifikovat potenciální zranitelnosti v jejich infrastruktuře a přijmout proaktivní opatření k jejich zmírnění. Platformy, které tyto firmy nabízí pro získávání informací, také umožňují organizacím sdílet informace o hrozbách a spolupracovat při jejich řešení.

Databáze jsou dalším cenným zdrojem informací pro detekci zranitelností. Platformy jako Virus Total, Censys, AbuseIPDB, MISP, OTX aj. shromažďují a agregují data z různých zdrojů, včetně bezpečnostních výzkumníků, organizací a komunit. Tyto databáze obsahují informace o škodlivých IP adresách, doménách, certifikátech, haších malwaru a dalších IoC. Integrací těchto databází do procesů detekce zranitelností mohou organizace rychleji identifikovat potenciální hrozby a korelovat je s aktivitami pozorovanými v jejich vlastní infrastruktuře.

Posledním vyznamným zdrojem informací pro detekci zranitelností, jsou například projekt Sentinel od CZ.NIC, OpenCTI, TheHive nebo ZenArmor, které poskytují nástroje a služby, které mohou organizacím pomoci odhalit zranitelnosti v jejich infrastruktuře. Například projekt Sentinel od CZ.NIC monitoruje českou národní doménu a upozorňuje na potenciální bezpečnostní hrozby. ZenArmor nabízí platformu pro automatizovanou detekci hrozeb za pomoci umělé inteligence a správu zranitelností. Využitím těchto projektů mohou organizace získat dodatečné informace a nástroje pro zlepšení své schopnosti detekovat a řešit zranitelnosti.

5.1 Threat Intel

V současném kybernetickém světě, kde se neustále objevují nové hrozby a zranitelnosti, je TI od předních společností jako Eset, Mandiant, Recorded Future, CrowdStrike, Cisco a OTX neocenitelným zdrojem informací pro detekci a prevenci útoků. Tyto společnosti poskytují aktuální a relevantní informace o nejnovějších hrozbách, včetně využívaných TTP a jejich aktuálních cílů, což pomáhá bezpečnostním analytikům lépe porozumět a bránit se proti těmto hrozbám.

Společnost Eset, známá svými antivirovými a bezpečnostními řešeními, poskytuje svým zákazníkům přístup k rozsáhlé databázi informací o hrozbách. Jejich výzkumný tým neustále monitoruje a analyzuje nové hrozby a zranitelnosti, se zvláštním zamě-

řením na APT. Eset poskytuje podrobné reporty o těchto hrozbách, včetně IoC, které mohou být integrovány do bezpečnostních řešení prostřednictvím API. Tyto informace pomáhají organizacím rychle detekovat zranitelnosti skrze reakci na hrozby, které takto objeví ve své infrastruktuře.[22]

Mandiant, nyní součást společnosti Google, je dalším velkým hráčem v oblasti TI. Jejich zpravodajství se zaměřuje na poskytování včasných a relevantních informací o APT hrozbách a jejich TTP. Mandiant kombinuje poznatky z vlastního výzkumu, zpravodajských zdrojů a incidentů, které řeší pro své klienty, aby poskytl komplexní pohled na aktivity APT skupin. Jejich reporty obsahují podrobné informace o nástrojích, technikách a infrastruktuře používané útočníky, stejně jako o jejich cílech a motivacích.[23]

Recorded Future je přední společností v oblasti TI, která využívá pokročilé technologie a analytiku k poskytování včasných a relevantních informací o hrozbách. Jejich platforma shromažďuje a analyzuje data z široké škály otevřených i uzavřených zdrojů, včetně dark webu, fór a sociálních médií. Recorded Future poskytuje podrobné informace o aktivitách APT skupin, jejich cílech a TTP, a také prediktivní analýzu, která pomáhá organizacím předvídat a připravit se na potenciální hrozby.[24]

CrowdStrike je další významnou společností v oblasti TI, známou především svou platformou Falcon. Tato platforma poskytuje pokročilé možnosti detekce a reakce na hrozby napříč různými zařízeními a prostředími. CrowdStrike využívá své rozsáhlé znalosti o APT skupinách a jejich TTP k poskytování včasných a relevantních informací o hrozbách. Jejich služba Falcon X nabízí podrobné analýzy APT kampaní, včetně informací o používaných nástrojích, technikách a infrastruktuře.[25]

Cisco, světový lídr v oblasti síťových technologií, také nabízí cenné TI služby. Jejich tým Talos Intelligence Group se zaměřuje na výzkum a analýzu hrozeb, včetně APT. Talos poskytuje podrobné reporty o nových hrozbách a zranitelnostech, včetně informací o jejich dopadu a možných protiopatřeních. Cisco také nabízí nástroje jako Cisco Threat Response, který integruje data o hrozbách z různých zdrojů a poskytuje jednotný pohled na bezpečnostní události.[26]

Kromě výše zmíněných společností existuje řada dalších poskytovatelů TI, kteří přispívají k detekci a prevenci hrozeb. Společnost IBM X-Force Exchange zase nabízí platformu pro sdílení a analýzu informací o hrozbách mezi organizacemi. Využitím kombinace různých TI zdrojů mohou organizace získat komplexní pohled na hrozby a zranitelnosti a lépe se bránit proti stále sofistikovanějším útokům. TI informace poskytované těmito společnostmi jsou neocenitelným zdrojem pro bezpečnostní analytiky. Díky včasným a relevantním informacím o používaných TTP a aktuálních cílech útočníků mohou organizace přijmout proaktivní opatření k ochraně svých systémů a dat. Přístup k IoC prostřednictvím API navíc usnadňuje integraci těchto dat do bezpečnost-

ních řešení a procesů organizace, což umožňuje rychlejší detekci a reakci na hrozby.

5.1.1 X.com

Sociální sítě jako X.com hrají významnou roli v rychlém šíření informací o nově objevených zranitelnostech a bezpečnostních hrozbách. Díky otevřené a přístupné povaze těchto platforem mohou bezpečnostní experti, výzkumníci, ale i útočníci snadno sdílet své poznatky a zkušenosti s širokou veřejností. Tento proces sdílení informací je často mnohem rychlejší než tradiční metody, jako jsou pravidelné týdenní nebo měsíční reporty vydávané bezpečnostními firmami, které musí projít interním schvalovacím procesem.

Na sociálních sítích jako X.com se setkávají odborníci z různých oblastí kybernetické bezpečnosti, kteří diskutují o nejnovějších trendech, technikách a nástrojích používaných jak pro ochranu, tak i pro útok. Bezpečnostní experti zde často sdílejí své objevy a analýzy nových zranitelností, včetně technických detailů a možných dopadů. Zároveň však tyto platformy přitahují i pozornost útočníků, kteří zde mohou hledat inspiraci pro své aktivity nebo sdílet vlastní poznatky o zneužitelných zranitelnostech. Tato otevřená výměna informací může vést k rychlejšímu odhalení a opravě bezpečnostních chyb, ale zároveň také poskytuje útočníkům cenné informace, které mohou zneužít před vydáním oficiálních oprav.

Jednou z výhod sociálních sítí jako X.com je, že umožňují prakticky komukoli přispět k odhalování a hlášení bezpečnostních problémů. Není nutné pracovat pro velkou technologickou firmu nebo být profesionálním bezpečnostním výzkumníkem, aby člověk mohl narazit na zranitelnost a sdílet své poznatky s komunitou. Mnohdy stačí tweetnout několik screenshotů a stručný popis problému, aby se informace začala šířit a upoutala pozornost odborníků i médií. Tento přístup demokratizuje proces odhalování zranitelností a zvyšuje šanci, že budou bezpečnostní chyby rychle identifikovány a opraveny.

Na druhou stranu, otevřená forma sdílení informací o zranitelnostech na sociálních sítích může představovat výzvu pro dotčené firmy a organizace. Pokud je zranitelnost veřejně odhalena dříve, než má firma šanci na ni adekvátně zareagovat a vydat opravu, může to vést k zvýšenému riziku zneužití a potenciálním škodám. Firmy se tak mohou ocitnout pod tlakem, aby urychleně vydaly záplaty nebo přijaly jiná opatření pro zmírnění dopadu zveřejněné zranitelnosti. Zároveň však otevřenost sociálních sítí ztěžuje firmám utajování bezpečnostních problémů a nutí je k transparentnosti a odpovědnosti vůči uživatelům a veřejnosti.[27]

5.2 Online Databáze

5.2.1 VirusTotal

VirusTotal je oblíbená online platforma, která slouží jako komplexní nástroj pro analýzu a detekci malwaru, podezřelých souborů a URL adres. Hlavním účelem VirusTotalu je poskytovat uživatelům možnost prověřit soubory a URL adresy pomocí více než 70 antivirových skenerů a služeb pro detekci malwaru. Výsledkem je podrobná zpráva o tom, zda byl soubor nebo URL adresa označena některým z těchto skenerů jako škodlivá, což pomáhá uživatelům identifikovat potenciální hrozby.

Kromě detekce malwaru může VirusTotal přispět i k odhalování zranitelností v infrastruktuře organizace. Jedním ze způsobů je analýza souborů a URL adres, které jsou v rámci infrastruktury používány nebo sdíleny. Pokud VirusTotal odhalí, že některý z těchto souborů nebo URL adres je spojován s malwarem nebo jinými hrozbami, může to být indikátorem zranitelnosti nebo kompromitace systému. Díky tomu mohou bezpečnostní týmy proaktivně identifikovat a řešit potenciální slabiny v infrastruktuře.

Dalším přínosem VirusTotalu je možnost obohacení dat zachycených v infrastruktuře organizace pomocí dotazování jeho API. VirusTotal nabízí rozhraní API, které umožňuje automatizovaně odesílat soubory a URL adresy k analýze a získávat podrobné informace o jejich reputaci a detekci hrozeb. Integrací tohoto API do bezpečnostních nástrojů a procesů organizace lze významně rozšířit schopnosti detekce a analýzy hrozeb.[28]

Je důležité zmínit, že VirusTotal nabízí různé úrovně přístupu k API v závislosti na zvoleném licenčním modelu. Bezplatná verze API má omezení v počtu dotazů za den a poskytuje základní informace o analyzovaných souborech a URL adresách. Placené licence, jako je například VirusTotal Enterprise, nabízejí vyšší limity dotazů, pokročilé funkce a přístup k dodatečným datům a statistikám.[29]

Představme si například situaci, kdy systém pro monitorování sítě zachytí podezřelý soubor stahovaný z neznámé URL adresy. Bezpečnostní tým může tento soubor a URL adresu odeslat přes API VirusTotalu k analýze. Výsledný datový výstup může vypadat následovně:

```
{
  "resource": "https://example.com/suspicious.exe",
  "scan_id": "1db0ad7dbcec06...",
  "scan_date": "2024-03-06 14:20:48",
  "permalink": "https://www.virustotal.com/...",S
  "positives": 10,
  "total": 76,
  "scans": {
    "ESET-NOD32": {
      "detected": true,
      "result": "Trojan.Downloader.Qakbot.AA"
    },
    "Kaspersky": {
      "detected": true,
      "result": "Trojan.Win32.Qakbot.gen"
```

```
    },
    ...
  }
}
```

Listing 2 : Výsledek dotazu na VirusTotal API

Tento výstup ukazuje, že podezřelý soubor „suspicious.exe“ byl detekován 10 z celkových 76 antivirových skenerů jako malware, konkrétně jako varianta malwaru Qakbot. Díky tomu může bezpečnostní tým okamžitě podniknout kroky k zamezení šíření a vyšetřování potenciální hrozby, jako je izolace zasažených systémů, blokování škodlivé URL adresy a hledání dalších indicií kompromitace v síti.

V případě placené licence VirusTotal Enterprise by výstup mohl obsahovat dodatečné informace, jako jsou historická data o souboru nebo URL adrese, podrobnosti o chování malwaru v sandboxovém prostředí, či vztahy k dalším známým hrozbám. Tyto rozšířené informace poskytují bezpečnostním týmům hlubší kontext a přehled o hrozbách, což usnadňuje jejich prioritizaci a řešení.

Výstup z VirusTotalu také poskytuje cenné informace pro threat hunting a zpravodajství o hrozbách. Analýzou dat z VirusTotalu mohou bezpečnostní týmy odhalovat nové trendy a vzorce útoků, identifikovat cílené kampaně a sledovat aktivity konkrétních hrozeb. Tyto poznatky pomáhají organizacím lépe porozumět aktuální hrozbám a přijímat proaktivní opatření k posílení své bezpečnostní postury.

5.2.2 Censys a Shodan

Censys a Shodan jsou dvě přední platformy pro mapování a analýzu internetové infrastruktury, které poskytují cenné informace o zařízeních, službách a zranitelnostech v globálním měřítku. Jejich hlavním účelem je neustále skenovat veřejný internetový prostor, identifikovat dostupné hostitele, otevřené porty a běžící služby. Tyto informace jsou následně zpřístupněny uživatelům prostřednictvím webového rozhraní a API, což umožňuje efektivní vyhledávání a analýzu dat.

Jedním z hlavních přínosů Censysu a Shodanu pro detekci zranitelností v infrastruktuře je jejich schopnost identifikovat zařízení a služby, které mohou být zranitelné vůči známým hrozbám. Díky pravidelnému skenování internetu dokážou odhalit instance zastaralého nebo nepatchovaného softwaru, chybně nakonfigurovaných služeb nebo zařízení vystavených do internetu bez adekvátního zabezpečení. Tyto informace pomáhají organizacím identifikovat slabá místa v jejich vlastní infrastruktuře a přijímat opatření k jejich nápravě.

Kromě toho mohou Censys a Shodan přispět k obohacení dat zachycených v infrastruktuře organizace prostřednictvím dotazování jejich API. Integrací API těchto platforem do bezpečnostních nástrojů a procesů lze automaticky získávat dodatečné

informace o IP adresách, doménách a zařízeních, se kterými organizace interaguje. Tyto informace mohou zahrnovat detaily o otevřených portech, běžících službách, používaných certifikátech nebo historických změnách v konfiguraci.

Představme si například situaci, kdy bezpečnostní monitoring zachytí komunikaci mezi interním systémem a neznámou externí IP adresou. Dotazem na API Censysu nebo Shodanu lze o této IP adrese získat následující informace:

```
{
  "ip": "192.0.2.42",
  "ports": [
    {
      "port": 22,
      "protocol": "ssh",
      "service": {
        "name": "OpenSSH",
        "version": "7.4"
      }
    },
    {
      "port": 80,
      "protocol": "http",
      "service": {
        "name": "Apache httpd",
        "version": "2.4.29"
      }
    }
  ],
  "location": {
    "country": "United States",
    "city": "New York"
  },
  "autonomous_system": {
    "asn": 12345,
    "description": "Example ISP"
  }
}
```

Listing 3 : Příkladný výsledek dotazu na Censys/Shodan API

Z této odpovědi lze vyčíst, že daná IP adresa má otevřené porty 22 (SSH) a 80 (HTTP), na kterých běží konkrétní verze služeb OpenSSH a Apache. Dále jsou k dispozici informace o geografické lokaci IP adresy a autonomním systému, ke kterému náleží. Tyto údaje mohou bezpečnostnímu týmu pomoci vyhodnotit rizikovost komunikace, identifikovat potenciálně zranitelné služby a určit další kroky v rámci vyšetřování incidentu.

Co se týče licencování, Censys i Shodan nabízejí bezplatnou i placenou verzi přístupu ke svým datům a funkcím. Bezplatné verze poskytují omezený počet dotazů na API za den a přístup k základním informacím o hostech a službách. Placené verze nabízejí výrazně vyšší limity dotazů, pokročilé vyhledávací možnosti a přístup k historickým datům a trendům. Placené verze také umožňují integraci s dalšími nástroji a automatizaci pracovních postupů.[30]

Z hlediska kvality a množství dat poskytují placené verze Censysu a Shodanu významně větší hodnotu pro organizace s rozsáhlou infrastrukturou a komplexními bezpečnostními potřebami. Vyšší limity dotazů a pokročilé funkce umožňují provádět roz-

sáhlé analýzy a korelovat data z různých zdrojů, což vede k lepšímu přehledu o hrozbách a efektivnější detekci a reakci na incidenty. Placené verze také nabízejí přístup ke specializovaným datovým sadám a analytickým nástrojům. Oba nástroje poskytují rozsáhlé pokrytí internetového prostoru, ale mohou se lišit v frekvenci a hloubce skenování určitých rozsahů IP adres nebo portů.

5.2.3 AbuseIPDB

AbuseIPDB je veřejná databáze sloužící k shromažďování a sdílení informací o IP adresách, které byly zapojeny do různých typů zneužití, jako je rozesílání spamu, malwarové infekce, DDoS útoky, skenování portů a další nelegální aktivity na internetu. Hlavním účelem AbuseIPDB je poskytnout komunitu a nástroje pro identifikaci a hlášení škodlivých IP adres, čímž přispívá k bezpečnějšímu online prostředí.

Ačkoli AbuseIPDB není primárně určen pro detekci zranitelností v infrastruktuře, může nepřímo přispět k jejich odhalení. Pokud jsou IP adresy patřící do infrastruktury organizace nahlášeny v AbuseIPDB v souvislosti s podezřelou aktivitou, může to být indikátorem kompromitace systémů nebo přítomnosti zranitelností, které jsou zneužívány útočníky. Pravidelná kontrola vlastních IP rozsahů v AbuseIPDB může pomoci odhalit potenciální bezpečnostní incidenty a přijmout nápravná opatření.

Integrace API AbuseIPDB do bezpečnostních nástrojů a procesů organizace umožňuje obohacení dat zachycených v infrastruktuře o reputační informace. Při detekci komunikace s neznámou IP adresou lze pomocí API dotazu zjistit, zda je daná adresa přítomna v databázi AbuseIPDB a jaké jsou dostupné informace o její aktivitě. Tyto údaje mohou pomoci při vyhodnocování rizikovosti komunikace a rozhodování o dalších krocích.

```
{
  "ip": "192.0.2.42",
  "abuse_confidence_score": 80,
  "country_code": "US",
  "usage_type": "Fixed Line ISP",
  "isp": "Example ISP",
  "domain": "example.com",
  "total_reports": 10,
  "last_reported_at": "2023-05-15T08:30:00Z",
  "reports": [
    {
      "categories": [
        "14",
        "18"
      ],
      "created_at": "2023-05-14T10:15:00Z"
    },
    ...
  ]
}
```

Listing 4 : Výsledek dotazu na AbuseIPDB API

Z této odpovědi lze vyčíst, že daná IP adresa má skóre spolehlivosti zneužití 80 ze 100, což naznačuje vysokou pravděpodobnost zapojení do škodlivých aktivit. Dále

jsou k dispozici informace o zemi, typu využití, poskytovateli internetových služeb a doméně spojené s IP adresou. Důležité jsou také údaje o celkovém počtu hlášení a jejich kategoriích (např. 14 pro SPAM a 18 pro Brute-Force). Tyto informace mohou být cenné při analýze bezpečnostních incidentů, určování priorit a komunikaci s externími stranami.[31]

Co se týče kvality a množství dat, AbuseIPDB spoléhá na hlášení od své komunity uživatelů. Bezplatná verze umožňuje omezený počet dotazů na API a přístup k základním informacím o IP adresách. Placená verze, AbuseIPDB Premium, nabízí vyšší limity dotazů, podrobnější informace o incidentech a možnost stahování kompletních datových sad. Placená verze také umožňuje integraci s dalšími nástroji a automatizaci pracovních postupů.[32]

Kvalita dat v AbuseIPDB závisí na aktivitě a spolehlivosti komunity přispěvatelů. I když mohou existovat falešně pozitivní hlášení, celkově poskytuje AbuseIPDB cenný zdroj informací o IP adresách zapojených do škodlivých aktivit. Je důležité mít na paměti, že AbuseIPDB by neměl být používán jako jediný zdroj informací pro bezpečnostní rozhodování, ale spíše jako doplněk k dalším nástrojům a technikám detekce hrozeb. Informace z AbuseIPDB by měly být vždy ověřeny a posouzeny v kontextu dalších bezpečnostních událostí a indikátorů.

5.2.4 Malware Information Sharing Platform

MISP je open-source platforma určená pro sdílení, ukládání a korelaci informací o kybernetických hrozbách a IoC. Hlavním účelem MISP je usnadnit spolupráci a výměnu informací mezi organizacemi, bezpečnostními týmy a výzkumníky, což vede k efektivnější detekci, prevenci a reakci na kybernetické hrozby.

MISP může významně přispět k detekci zranitelností v infrastruktuře tím, že poskytuje včasné a relevantní informace o nových hrozbách, zranitelnostech a útočných kampaních. Sdílení informací o odhalených zranitelnostech, včetně podrobností o jejich zneužití a dopadech, umožňuje organizacím rychle identifikovat a řešit potenciální slabá místa ve vlastních systémech. MISP také podporuje sdílení informací o opravách a ochranných opatřeních, což usnadňuje včasnou implementaci bezpečnostních záplat a konfigurací.[20]

Integrace API MISP do bezpečnostních nástrojů a procesů organizace umožňuje obohacení dat zachycených v infrastruktuře o kontextové informace z komunity MISP. Při detekci podezřelé aktivity, jako je komunikace s neznámou IP adresou nebo doménou, lze pomocí API dotazu zjistit, zda jsou tyto indikátory přítomny v MISP a jaké jsou dostupné informace o souvisejících hrozbách. Tyto údaje mohou pomoci při vyhodnocování závažnosti incidentu, určování priorit a volbě vhodných nápravných

opatření.

```
{
  "Event": {
    "id": "123",
    "info": "Malware Campaign - Emotet",
    "date": "2023-05-15",
    "published": true,
    "threat_level_id": "2",
    "Attribute": [
      {
        "id": "456",
        "type": "ip-dst",
        "category": "Network activity",
        "value": "192.0.2.42",
        "comment": "C2 server for Emotet malware",
        "Tag": [
          {
            "name": "malware-type:emotet"
          },
          {
            "name": "tlp:amber"
          }
        ]
      },
      ...
    ]
  }
}
```

Listing 5 : Výsledek dotazu na MISP API

Z této odpovědi lze vyčíst, že daná IP adresa (192.0.2.42) je spojená s malwarovou kampaní Emotet a slouží jako C2 server. Atribut má přiřazené značky (tagy) označující typ malwaru a úroveň sdílení informací TLP. Tyto informace mohou být cenné při analýze bezpečnostních incidentů, určování rozsahu a dopadu malwarové infekce a komunikaci s dalšími týmy a organizacemi.

Pokud jde o kvalitu a množství dat, MISP spoléhá na aktivní zapojení a příspěvky své komunity uživatelů. Základní verze MISP je open-source a zdarma, což umožňuje organizacím provozovat vlastní instance a přispívat do sdílené znalostní báze. Existují také placené služby a podpory poskytované třetími stranami, které nabízejí hostování, správu a rozšířené funkce MISP.

Kvalita dat v MISP závisí na odbornosti a spolehlivosti přispěvatelů. Vzhledem k otevřené povaze platformy mohou existovat neúplné nebo neověřené informace. Je důležité pečlivě posuzovat zdroje a spolehlivost sdílených dat a ověřovat jejich relevanci pro konkrétní prostředí. Celkově však MISP poskytuje cenný zdroj informací o hrozbách a umožňuje organizacím těžit ze společných znalostí a zkušeností bezpečnostní komunity.

Pro většinu organizací je základní open-source verze MISP dostačující pro účely sdílení a získávání informací o hrozbách. Placené služby mohou být přínosné pro organizace s omezenými interními zdroji nebo specifickými požadavky na integraci, automatizaci nebo podporu.

Při implementaci MISP je důležité stanovit jasné procesy a politiky pro sdílení a

využívání informací, zajistit kvalitu a relevanci přispívaných dat a pravidelně vyhodnocovat přínos platformy pro bezpečnostní operace organizace. MISP by měl být integrován do širšího ekosystému bezpečnostních nástrojů a procesů, aby se maximalizovala jeho hodnota při detekci, analýze a reakci na hrozby.

5.2.5 Open Threat Exchange

OTX je platforma pro sdílení a analýzu informací o kybernetických hrozbách provozovaná společností AlienVault (nyní součástí AT&T Cybersecurity). Hlavním účelem OTX je poskytovat globální komunitu a nástroje pro shromažďování, sdílení a využívání aktuálních dat o hrozbách, IoC a dalších relevantních informací. OTX umožňuje organizacím a bezpečnostním týmům přístup k rozsáhlé znalostní bázi hrozeb a podporuje spolupráci při jejich detekci a prevenci.

Využití OTX může významně přispět k detekci zranitelností v infrastruktuře organizace. Platforma shromažďuje a analyzuje informace o nových zranitelnostech, malwaru, phishingových kampaních a dalších hrozbách z různých zdrojů, včetně bezpečnostních výzkumníků, vendorů a uživatelů. Tyto informace zahrnují podrobnosti o zneužívaných zranitelnostech, IoC a doporučená nápravná opatření. Pravidelným monitoringem a využitím těchto dat mohou organizace rychleji identifikovat potenciální zranitelnosti ve svých systémech a přijmout cílená opatření k jejich odstranění.

Integrace API OTX do bezpečnostních nástrojů a procesů organizace umožňuje obohacení dat zachycených v infrastruktuře o aktuální informace o hrozbách. Při detekci podezřelé aktivity, jako je komunikace s neznámou IP adresou, doménou nebo výskyt specifického souboru, lze pomocí API dotazu zjistit, zda jsou tyto indikátory známé v komunitě OTX a jaké jsou dostupné informace o souvisejících hrozbách. Tyto údaje mohou pomoci při vyhodnocování závažnosti incidentu, určování rozsahu kompromitace a volbě vhodných kroků pro její řešení.

Příklad datového výstupu z OTX API pro konkrétní indikátor (hash souboru):

```
{
  "indicator": "1a79a4d60de6718e8e5b326e338ae533",
  "type": "FileHash-MD5",
  "description": "Emotet malware payload",
  "created": "2023-05-10T08:15:00Z",
  "tags": [
    "malware",
    "emotet",
    "trojan"
  ],
  "references": [
    "https://example.com/emotet-analysis",
    "https://example.org/emotet-ioc"
  ],
  "relationships": [
    {
      "type": "downloaded-from",
      "target": {
        "indicator": "http://example.com/malware.exe",
```

```
        "type": "URL"
      }
    },
    ...
  ]
}
```

Listing 6 : Výsledek dotazu na OTX API

Z této odpovědi lze vyčíst, že daný hash (1a79a4d60de6718e8e5b326e338ae533) je spojen s malwarem Emotet, který funguje jako trojský kůň. Indikátor je opatřen popisem, značkami (tagy) a referencemi na další informace. Důležité jsou také vztahy (relationships) k dalším indikátorům, v tomto případě URL adresa, ze které byl malware stažen. Tyto informace mohou být cenné při analýze malwarových infekcí, mapování infrastruktury útočníků a sdílení poznatků s dalšími týmy a organizacemi.

Co se týče kvality a množství dat, OTX těží z rozsáhlé globální komunity přispěvatelů a partnerů. Kvalita dat v OTX je obecně vysoká díky aktivnímu zapojení odborné komunity a procesům ověřování a obohacování dat ze strany AlienVault. Přesto je důležité kriticky vyhodnocovat relevanci a spolehlivost informací pro konkrétní prostředí a účely. Údaje z OTX by měly být používány jako jeden ze zdrojů pro informovaná rozhodnutí o bezpečnosti, v kombinaci s dalšími nástroji a interními poznatky.

5.3 Projekty

5.3.1 Sentinel

Projekt Sentinel, vyvíjený a provozovaný sdružením CZ.NIC, je bezplatná služba zaměřená na zvýšení bezpečnosti a stability české internetové infrastruktury. Sentinel navazuje na předchozí projekt Honeypot as a Service, který byl spuštěn v roce 2014 a poskytoval organizacím možnost provozovat vlastní honeypoty a sdílet data o útocích. S rostoucím zájmem o službu a potřebou komplexnějšího řešení se CZ.NIC rozhodl projekt HaaS dále rozvinout a vytvořit Sentinel.

Hlavním účelem Sentinelu je monitorovat síťový provoz a identifikovat potenciální hrozby a anomálie, které mohou signalizovat kompromitaci systémů nebo probíhající útoky. Služba využívá kombinaci honeypotů, aktivního skenování a pokročilé analýzy dat k odhalení škodlivých aktivit a poskytuje užitečné informace pro zvýšení bezpečnosti sítí. Oproti projektu Honeypot as a Service nabízí Sentinel propracovanější infrastrukturu, širší pokrytí a pokročilejší analytické nástroje.

Sentinel hraje důležitou roli při detekci zranitelností v síťové infrastruktuře. Služba nasazuje honeypoty v různých sítích k odhalení škodlivých aktivit a sběru informací o útočnících a jejich taktikách. Analýzou dat z honeypotů a sledováním síťového provozu může Sentinel identifikovat zranitelné systémy, infikovaná zařízení a další bezpečnostní rizika.[33]

5.4 Common Vulnerability Scoring System

Hodnocení zranitelností podle CVSS je široce používaný standard pro posuzování závažnosti bezpečnostních zranitelností v softwarových systémech. CVSS poskytuje konzistentní a standardizovaný způsob, jak kvantifikovat dopad a riziko spojené s každou zranitelností, což umožňuje organizacím prioritizovat své úsilí v oblasti řízení a nápravy zranitelností.

CVSS skóre se počítá na základě několika metrik, které zohledňují různé aspekty zranitelnosti, jako je způsob přístupu, složitost útoku, rozsah dopadu a další faktory. Základní metriky CVSS zahrnují vektor útoku (např. síťový, lokální, fyzický), složitost útoku (nízká, vysoká), požadované oprávnění (žádné, nízké, vysoké), interakci uživatele (žádná, požadovaná) a rozsah dopadu (nezměněný, změněný). Tyto metriky jsou kombinovány pomocí standardizovaného vzorce pro výpočet celkového skóre CVSS v rozsahu od 0 do 10, přičemž vyšší skóre označuje závažnější zranitelnosti.[34]

CVSS také poskytuje kvalitativní hodnocení závažnosti, které rozděluje zranitelnosti do kategorií jako „nízká“, „střední“, „vysoká“ a „kritická“ na základě vypočteného skóre. Například zranitelnosti se skóre 9,0 nebo vyšší jsou považovány za kritické, zatímco zranitelnosti se skóre 3,9 nebo nižší jsou považovány za nízké.[35]

Jednou z hlavních výhod používání CVSS je, že poskytuje společný jazyk a měřítko pro komunikaci o závažnosti zranitelností mezi různými stranami, jako jsou dodavatelé softwaru, bezpečnostní výzkumníci a koncové organizace. To usnadňuje spolupráci a umožňuje efektivnější sdílení informací o zranitelnostech a jejich řešení.

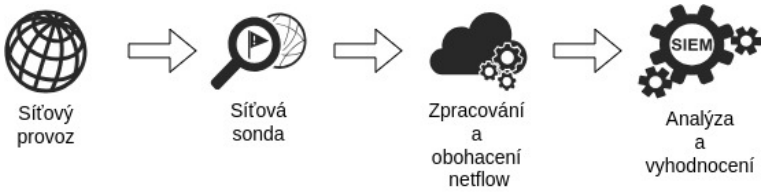
CVSS skóre jsou široce používána v databázích zranitelností a bezpečnostních bulletinech, jako jsou NVD a CVE. Mnoho nástrojů pro skenování zranitelností a systémů pro správu záplat také integruje CVSS skóre, aby pomohlo organizacím prioritizovat a řešit zranitelnosti na základě jejich závažnosti.

Je důležité poznamenat, že zatímco CVSS poskytuje užitečný způsob kvantifikace závažnosti zranitelností, nemělo by to být jediné kritérium používané při rozhodování o prioritách nápravy. Organizace by měly také zvážit další faktory, jako je hodnota zasažených aktiv, expozice vůči hrozbám a provozní dopady, aby získaly ucelenější pohled na riziko a informovaly své strategie zmírňování rizik.[36]

II. PRAKTICKÁ ČÁST

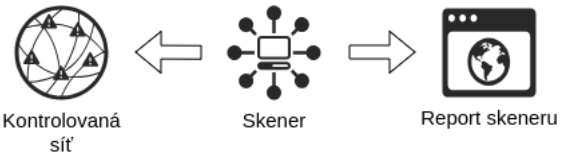
6 ARCHITEKTURA SYSTÉMU

Navrhovaný systém pro analýzu síťového provozu a detekci zranitelností se skládá ze tří hlavních částí: vstupní, předzpracování a obohacování dat a finální zpracování, analýza a vyhodnocení dat.



Obrázek 6.1 : Systém pro pasivní analýzu provozu

Vstupní část systému je zodpovědná za sběr a prvotní zpracování surového síťového provozu. Může fungovat ve dvou režimech - pasivní analýza procházejícího provozu nebo aktivní skenování systémů za účelem odhalení potenciálních zranitelností. V pasivním režimu vstupní část monitoruje síťový provoz, dekóduje pakety a extrahuje z nich relevantní informace. V aktivním režimu vstupní část cíleně skenuje systémy, hledá otevřené porty, identifikuje běžící služby a snaží se odhalit známé zranitelnosti.



Obrázek 6.2 : Systém pro aktivní skenování

Část zpracování a obohacování dat přebírá data ze vstupní části a provádí jejich další zpracování. Cílem je připravit data do podoby vhodné pro následnou analýzu a obohatit je o dodatečný kontext z externích zdrojů. Tato část parsuje a normalizuje data, extrahuje klíčové údaje jako IP adresy, porty, protokoly atd. Pro vybrané údaje pak provádí volání na externí API služby, které poskytují doplňující informace. Například pro IP adresy může zjišťovat geolokaci, informace o vlastníkovi, reputační skóre apod. Tím se původní data obohatí o cenný kontext usnadňující jejich interpretaci.

Poslední částí systému je část pro finální zpracování, analýzu a vyhodnocení dat. Tato část již není v rámci diplomové práce detailně řešena, neboť její konkrétní podoba se může lišit dle požadavků a případů užití každého zákazníka a jeho systémů. Pro účely práce byl jako úložiště dat zvolen Elasticsearch, který poskytuje výkonné možnosti indexace a vyhledávání dat a simuluje úložiště dat pro 3.3 SIEM. Klíčovou vlastností této části systému je ale schopnost integrovat data i z dalších zdrojů a systémů. To umožňuje korelovat údaje z analyzovaného síťového provozu například s logy, záznamy o incidentech a dalšími daty v SIEM. Propojení a společná analýza dat z více zdrojů

poskytuje ucelenější bezpečnostní přehled a usnadňuje odhalení komplexnějších hrozeb. Flexibilní integrace rozličných datových zdrojů je tedy zásadním požadavkem na tuto část systému.

Popsaný systém jako celek poskytuje funkcionalitu pro detailní analýzu síťového provozu, detekci bezpečnostních hrozeb a zranitelností a přípravu obohacených dat pro následné zpracování a vizualizaci. Jeho modulární architektura a schopnost integrace různých technologií v poslední části zajišťuje dobrou přizpůsobitelnost konkrétním potřebám organizací.

6.1 Faktory ovlivňující nasazení detekčních systémů

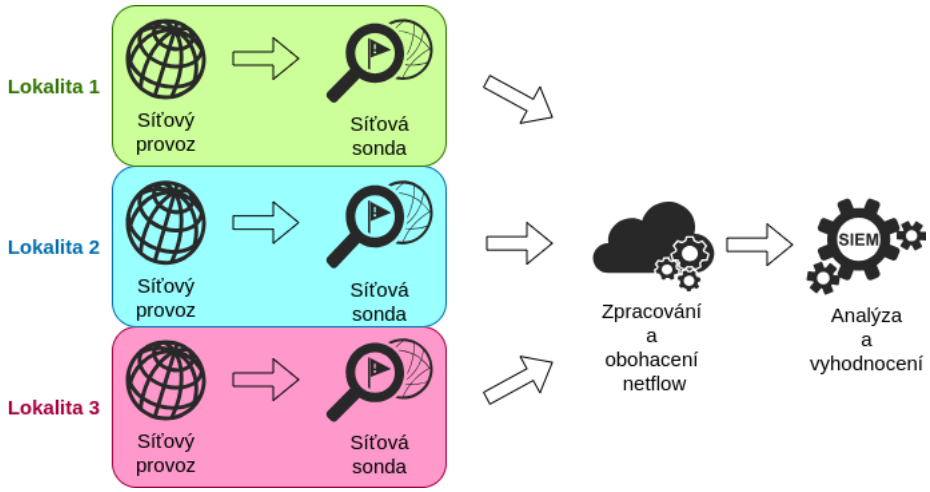
Při nasazování detekčních systémů v sítích různých velikostí je třeba zvážit několik faktorů pro optimalizaci sběru dat. Jedním z nejvýznamnějších parametrů je velikost sítě, která není dána pouze fyzickou délkou kabelů, ale také linkovou a síťovou architekturou. Linková architektura popisuje způsob, jakým jsou zařízení rozdělena na linkové vrstvě, například pomocí VLAN a MPLS. Síťová architektura se zabývá adresováním a směrováním na úrovni síťové vrstvy, typicky pomocí IP adres. Díky technologiím jako je VRF se může architektura sítě dynamicky měnit, aniž by bylo nutné fyzicky zasahovat do zapojení síťových prvků, což má významný dopad na způsob monitorování sítě.

Dalším klíčovým parametrem je vytížení sítě. Pro účely detekce je totiž nezbytné dopravit k detekčnímu prvku kompletní zkopírovaný síťový provoz. Tento provoz lze získat například pomocí SPAN portů na přepínačích nebo pomocí specializovaných TAP zařízení. V praxi to znamená, že pokud je nutné provoz dopravit do jiné části sítě k monitorovacímu prvku, tak i ve špičce musí být k dispozici minimálně dvojnásobná přenosová kapacita, aby bylo možné zajistit spolehlivou funkci síťové infrastruktury a sběr dat pro detekční systém, nebo je třeba řešit filtraci síťového provozu v místě jeho kopírování.

Po zajištění dostatečné kapacity pro dopravu provozu k detekčnímu systému je třeba zvážit, jaké typy zranitelností chceme detekovat. Základem je detekce zneužití známých zranitelností u serverů a aplikací dostupných z Internetu, jako jsou například nezabezpečené webové aplikace, neaktualizované servery se známými chybami zabezpečení nebo služby vystavené útokům hrubou silou. Zde je důležité rozhodnout, zda analyzovat veškerý provoz směřující na hraniční bránu sítě, nebo se zaměřit pouze na provoz cílený na servery a aplikace v DMZ. DMZ je speciální síťový segment, který obsahuje servery a služby přístupné z Internetu, ale je oddělen od vnitřní sítě organizace. Pokud se však omezíme jen na analýzu provozu z/do Internetu, vědomě se tím vzdáváme možnosti odhalit útoky pocházející zevnitř sítě, například od vlastních zaměstnanců.

Vnitřní hrozby však patří mezi nejnebezpečnější a mohou zahrnovat zneužití oprávnění, krádeže dat nebo šíření malwaru.

V malých sítích s řádově desítkami zařízení, typicky s jedním hraničním routerem a několika málo VLAN, je nasazení monitorovacích prostředků poměrně přímočaré. Centralizovaný monitorovací systém může pokrýt celou síť a poskytovat ucelený přehled o bezpečnostní situaci. U rozsáhlejších sítí, zejména takových, které se skládají z několika samostatných lokalit s vlastním přístupem do Internetu, je však vhodnější použít distribuovaný monitoring, jak je naznačeno v kapitole 4.1.5 Suricata a Snort. Každá monitorovaná lokalita má v takovém případě vlastní nezávislý monitorovací systém, který pokrývá místní síťový provoz a detekuje hrozby specifické pro danou lokalitu. Výhodou tohoto přístupu je lepší škálovatelnost, redundance a přizpůsobení místním podmínkám. Nevýhodou může být vyšší komplexita a náklady na správu více samostatných systémů.



Obrázek 6.3 : Distribuovaný systém pro pasivní analýzu

Nezávisle na zvoleném přístupu k monitoringu je důležité zmínit, že objem zpracovaného provozu síťovou sondou odesílaného do centrálního systému pro další analýzu tvoří typicky jen setiny až desetiny původního objemu, v závislosti na nastavené úrovni detailnosti výstupu. Detekční systémy jako Suricata provádějí prvotní filtraci a agregaci síťových toků, čímž významně redukují objem dat nutný pro další zpracování a dlouhodobé ukládání.

Správná implementace detekčních systémů v síti vyžaduje pečlivé zvážení výše uvedených faktorů a přizpůsobení architektury monitoringu konkrétním potřebám a omezením dané organizace. Vhodně navržený a nasazený systém detekce hrozeb může významně přispět k zajištění bezpečnosti sítě a ochraně důležitých aktiv.

6.2 Aktivní průzkum sítě

Aktivní skenování zranitelností je dalším klíčovým prvkem v zajištění bezpečnosti a odolnosti počítačových sítí a systémů. Proto byl tento nástroj zvolen jako součást navrhovaného bezpečnostního řešení. OpenVAS je open-source skener, který dokáže identifikovat a vyhodnotit širokou škálu bezpečnostních slabin v různých systémech a aplikacích.

Jednou z hlavních předností OpenVAS je jeho rozsáhlá databáze zranitelností, která je pravidelně aktualizována a rozšiřována díky aktivní komunitě vývojářů a bezpečnostních expertů. Tato databáze pokrývá zranitelnosti v operačních systémech, síťových zařízeních, databázích, webových aplikacích a mnoha dalších komponentech. Díky tomu je OpenVAS schopen odhalit i nejnovější a méně známé slabiny.

Velkou výhodou OpenVAS je jeho flexibilita a přizpůsobitelnost. Skener lze konfigurovat podle specifických potřeb organizace, definovat vlastní politiky skenování a integrovat ho s dalšími bezpečnostními nástroji. OpenVAS podporuje automatizaci skenování pomocí rozhraní příkazové řádky a API, což umožňuje jeho snadné začlenění do CI/CD procesů a skriptů pro pravidelné testování.[45]

Důležitou součástí práce s OpenVAS je pravidelnost skenování a aktualizace databáze zranitelností. Nové slabiny se objevují každý den a je nutné udržovat přehled o aktuálním stavu zabezpečení. Proto je vhodné nastavit automatické skenování v pravidelných intervalech a průběžně aplikovat záplaty a aktualizace na základě výsledků testů.

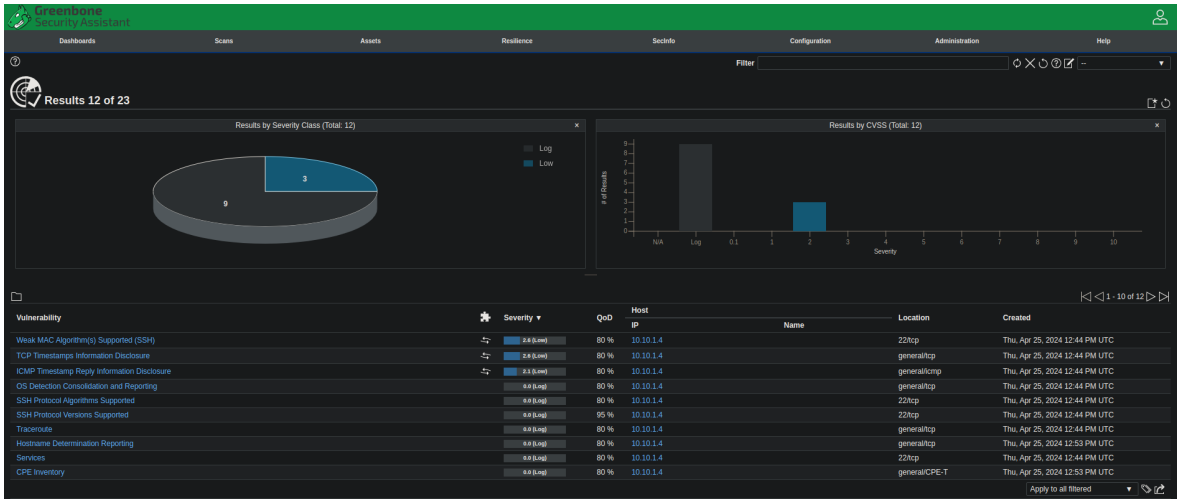
6.2.1 Nasazení systému

Greenbone Community Edition (obsahující OpenVAS skener) je v systému nasazen pomocí Docker kontejnerů. Toto řešení bylo zvoleno kvůli komplexitě systému, který se skládá z mnoha různých služeb (gvmd, ospd-openvas, gsa, redis, postgresql atd.) a také kvůli jednoduchosti správy a aktualizacím. Tyto služby jsou spouštěny každá ve vlastním kontejneru a jsou orchestrovány pomocí docker-compose.

OpenVAS je v systému nasazen jako samostatný element ze 2 důvodu:

1. Kvůli jeho samostatnému grafickému rozhraní Greenbone Security Assistant, které umožňuje pohodlnou práci se skenerem přes webové rozhraní - zadávání skenů, prohlížení výsledků apod.(Obrázek 6.4)

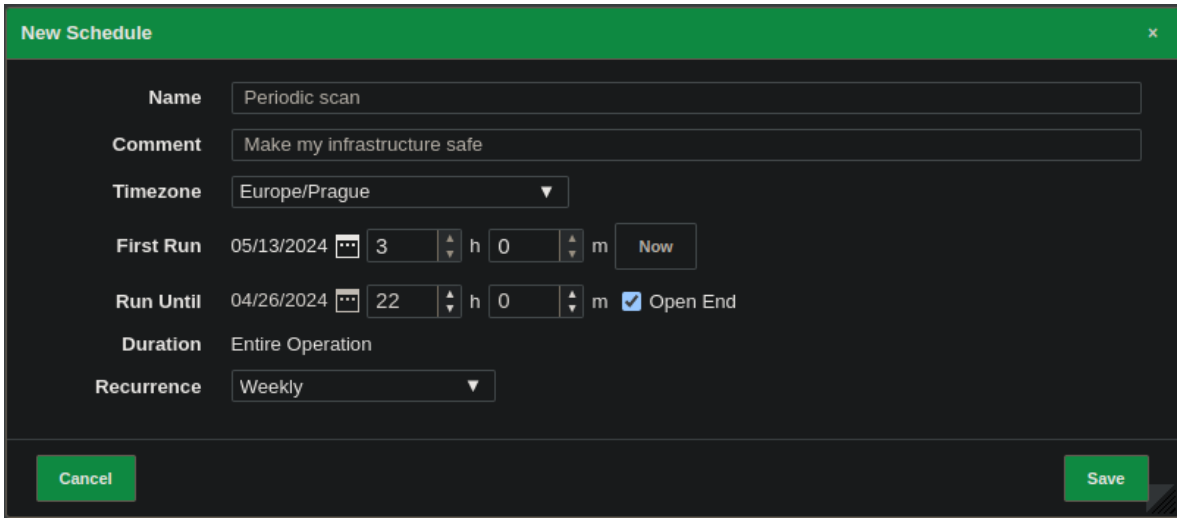
2. Jak je zmíněno výše, práce neřeší samotné SIEM řešení proto se nasazení omezilo na grafický výstup samotného Greenbone Security Assistant.



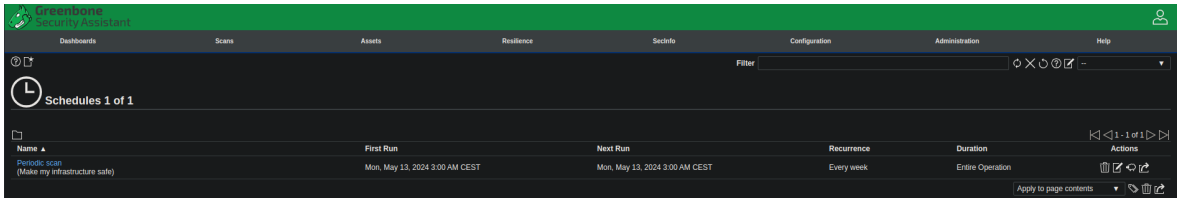
Obrázek 6.4 : Výstup skenování

Greenbone/OpenVAS ale také poskytuje možnosti integrace se SIEM systémy. Data o nalezených zranitelnostech mohou být exportována v různých formátech (XML, CSV...) a pravidelně zasílána do SIEMu pro další zpracování a korelaci s ostatními bezpečnostními událostmi na úrovni SIEM, ale protože se jedná o informace vnitřních systémů a informace o nalezených zranitelnostech jsou poskytované již samotným OpenVAS, není nutné data exportovat přes Logstash a nalezené infrormace dále obohacovat.[46]

Co se týče periodického skenování, to lze v OpenVAS nastavit pomocí takzvaných Schedules (Obrázek 6.5 a 6.6). V GSA může být vytvořen Schedule, který definuje kdy a jak často se má určitý sken spouštět. Jsou k dispozici flexibilní možnosti nastavení - jednou denně, v určitý den v týdnu, každých X hodin apod.



Obrázek 6.5 : Nastavení plánovaného skenování



Obrázek 6.6 : Obrazovka naplánových skenování

6.2.2 Aktualizace databáze zranitelností

Výhodou nasazení OpenVAS v Dockeru jako souboru konteinerů je především jejich udržitelnost a nenáročnost na správu. Aktualizace je v tomto případě stejně jednoduchá jako nasazení samotného nástroje a probíhá ve 2 krocích opět pomocí bash skriptu:

```
#!/bin/bash
COMPOSE_FILE="$DOWNLOAD_DIR/docker-compose.yml"
PROJECT_NAME="greenbone-community-edition"

echo "Pulling latest data container images..."
docker compose -f $COMPOSE_FILE -p $PROJECT_NAME pull notus-data vulnerability-
  tests scap-data dfn-cert-data cert-bund-data report-formats data-objects

echo "Restarting containers..."
docker compose -f $COMPOSE_FILE -p $PROJECT_NAME up -d

echo "Feed update process started. This may take several minutes to complete."
echo "Check the logs of ospd-openvas and gvmd containers to monitor the progress."
```

Listing 7 : Aktualizace Feedů pro OpenVAS

1. Nejprve dojde ke stažení nejnovějších obrazů datových kontejnerů (pull). Ty obsahují aktuální verze feedů (VT, SCAP, CERT data atd.).

2. Následně se kontejnery spustí (up -d) a při startu se automaticky provede kopírování dat z obrazů do příslušných docker volumes.

3. Nakonec běžící služby (ospd-openvas, gvmd) detekují nová data ve volumes a začnou je načítat do paměti a databáze. Tento proces může trvat i desítky minut v závislosti na množství aktualizovaných dat.

Po úspěšném dokončení celého procesu budou v systému k dispozici nejaktuálnější feedy a je možné provádět skeny s nejnovějšími informacemi o zranitelnostech.[47]

6.3 Síťový monitoring

Síťový monitoring pomocí IDS/IPS je klíčovým nástrojem pro zajištění bezpečnosti a spolehlivosti počítačových sítí. Proto byl tento systém implementován do navrhovaného systému. Tyto systémy jsou schopny analyzovat síťový provoz na různých vrstvách, od základní IP komunikace až po aplikační protokoly.

Moderní IDS/IPS systémy podporují parsování a inspekci širokého spektra protokolů. Kromě tradičních protokolů jako HTTP, DNS, FTP či SMTP zvládají i novější

a komplexnější protokoly jako QUIC, který kombinuje transportní a kryptografické funkce. Podpora pro QUIC umožňuje IDS/IPS systémům monitorovat a chránit i nejmodernější webové a mobilní aplikace.

Na aplikační vrstvě jsou IDS/IPS systémy schopny rozpoznat a analyzovat komunikaci mnoha běžných aplikací a služeb. Kromě webových aplikací to mohou být systémy pro vzdálenou správu, chatovací a streamovací platformy a mnohé další. Pomocí specifických modulů a pravidel dokáží tyto systémy kontrolovat aplikační provoz, vyhledávat známky útoku či neautorizované aktivity a identifikovat anomálie.

Analýza šifrovaného provozu představuje pro IDS/IPS systémy výzvu, nicméně i zde mají k dispozici různé metody detekce. Mohou například extrahovat certifikáty ze šifrovaných spojení a kontrolovat jejich platnost, důvěryhodnost vydavatele či shodu se jménem serveru. Také mohou detekovat pokusy o downgrade na slabší verze šifrovacích protokolů či použití nezabezpečených šifer. Některé IDS/IPS dokonce umožňují dešifrování provozu za použití poskytnutých privátních klíčů pro hlubší inspekci.

Důležitou funkcí pokročilých IDS/IPS systémů je schopnost zachytávat a ukládat přenášená data pro forenzní analýzu a zpětné vyšetřování incidentů. To může zahrnovat automatické ukládání podezřelých souborů, e-mailových příloh či celých PCAP záznamů komunikace na základě definovaných pravidel.

Díky kombinaci detailní inspekce protokolů, pokročilých detekčních metod a možností zachytávání dat poskytují moderní IDS/IPS systémy silné nástroje pro ochranu před síťovými hrozbami. Jejich nasazení, správná konfigurace a průběžné vylepšování jsou nezbytné pro udržení kyberbezpečnosti v dnešním rychle se měnícím prostředí.

6.3.1 Nasazení systému

Jak je zmíněno v teoretické části této práce, neexistuje mnoho systémů, které by k těmto účelům šlo využít. Proto byl pro nasazení zvolen systém 4.1.5 Suricata. Jeho nasazení i provoz jsou poměrně nenáročné a systém funguje spolehlivě i s konfigurací doručenou při instalaci. Mimo jiné na tento IDS/IPS systém spoléhají i některá komerční řešení.

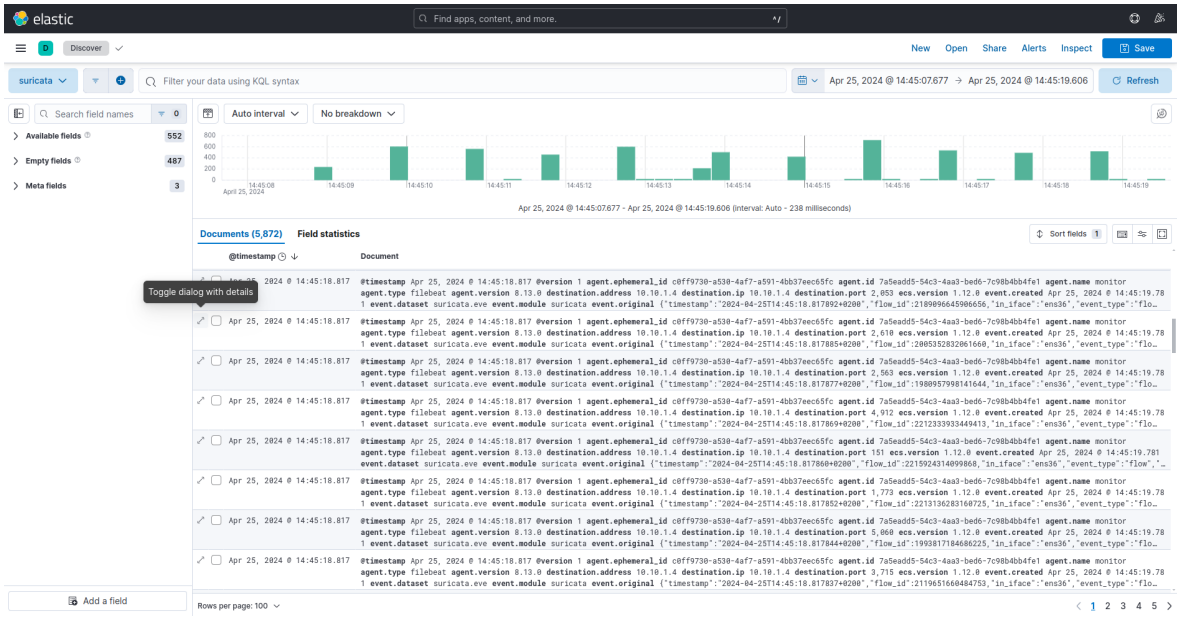
```
1 add-apt-repository ppa:oisf/suricata-stable
2 apt install suricata
```

Listing 8 : Instalace IDS/IPS Suricata

Výhodou je instalovat Suricatu z APT repozitářů, ale Suricata samozřejmě umožňuje instalaci i ze zdrojových kódů, která umožňuje zakompilovat do instalace pouze potřebnou funkcionalitu a tím pádem i závislosti.

Samotná konfigurace poskytuje mnoho možností, jak přizpůsobit funkcionalitu s ohledem na požadavky organizace na sběr dat, zatížení HW a optimalizaci zpracování síťového provozu pro dosažení maximálního množství zpracovaného provozu. Protože

Suricata využívá data z HW zařízení (především síťových karet), mnoho možností optimalizace se nachází i mimo konfiguraci samotné Suricaty.[37]



Obrázek 6.7 : Výstup Suricaty uložený v Elasticsearch

6.3.2 Aktualizace pravidel

Pro stažení a aktualizaci pravidel byl použit nástroj **suricata-update**, který umožňuje automatizovaně stahovat a ukládat pravidla ze zvolených zdrojů. Zdroje je samozřejmě možné přidávat a v případě placených zdrojů je potřeba zadat v konfiguraci zdrojů licenční klíč. Tento nástroj se instaluje souběžně se Suricatou pokud je instalována z repozitářů, ale možné ho nainstalovat i samostatně.[39]

```
# Update sources
suricata-update update-sources

# List sources
suricata-update list-sources

# Enable source
suricata-update enable-source ptresearch/attackdetection

# Update rules set
suricata-update
```

Listing 9 : Příklad práce se suricata-update

Samotná automatizace stahování a aktualizace Suricaty je řešena bash skriptem pomocí plánovače **cron**, který zajistí aktualizaci pravidel bez přerušení provozu. Tento skript se stará o stažení nejnovějších pravidel pomocí nástroje **suricata-update** a následně provede restart Suricaty, aby se nová pravidla načetla a aplikovala na síťový provoz.

```
#!/bin/bash

suricata-update
sleep 10
suricatasc -c ruleset-reload-nonblocking
```

Listing 10 : Aktualizace pravidel pro detekci

Zde je třeba zmínit, že pro úspěšné provedení tohoto skriptu je třeba zajistit 2 podmínky:

- příkaz `suricatasc` přepokládá, že je funkční ovládání Suricaty přes socket,
- je k dispozici alespoň jednou tolik paměti RAM co Suricata nyní využívá (případně více pokud je nová sada pravidel výrazně větší).

Ruleset-reload-nonblocking totiž načte novou sadu pravidel do paměti a připraví ji k použití zatím co stará sada nadále existuje v paměti a je využívána enginem Suricaty. Až je nová sada pravidel připravena, tak dojde k jejich záměně a stará sada je smazána.[40]

6.4 Obohacování dat z online databází

Získávání dodatečného kontextu z externích zdrojů pomocí API je důležitou součástí moderních systémů pro detekci a prevenci hrozeb. Tyto systémy mohou dotazovat různé databáze, služby pro reputaci IP adres, DNS, IoC a další zdroje, aby obohatily data získaná analýzou síťového provozu a zvýšily přesnost a relevanci detekce.

V středně velké síti s provozem v řádu stovek megabytů za sekundu může být počet dotazů na externí API poměrně vysoký. Pokud by systém dotazoval API pro každý analyzovaný paket či tok, mohlo by to rychle překročit limity a budget pro využívání těchto služeb. Je proto důležité pečlivě zvážit, která data opravdu vyžadují dodatečný kontext, a implementovat efektivní cachování a filtrování dotazů.

Ceny za využívání API pro obohacování bezpečnostních dat se mohou značně lišit v závislosti na poskytovateli a zvoleném plánu. Některé služby účtují poplatky za každý dotaz, jiné nabízejí měsíční paušál s omezeným počtem dotazů. Pro středně velkou síť s vysokým počtem dotazů mohou náklady na API snadno dosáhnout stovek až desítek tisíců dolarů měsíčně. Je proto nutné pečlivě vybrat poskytovatele a nastavit limity využití tak, aby náklady zůstaly v rozumných mezích.

Neustálé dotazování API také klade vysoké nároky na výpočetní výkon a síťovou infrastrukturu. Systém musí být schopen rychle generovat a odesílat dotazy, přijímat a zpracovávat odpovědi a integrovat získaná data do svých detekčních a analytických procesů. To může vyžadovat robustní a škálovatelnou architekturu s load balancingem, cachováním a vysokou dostupností.

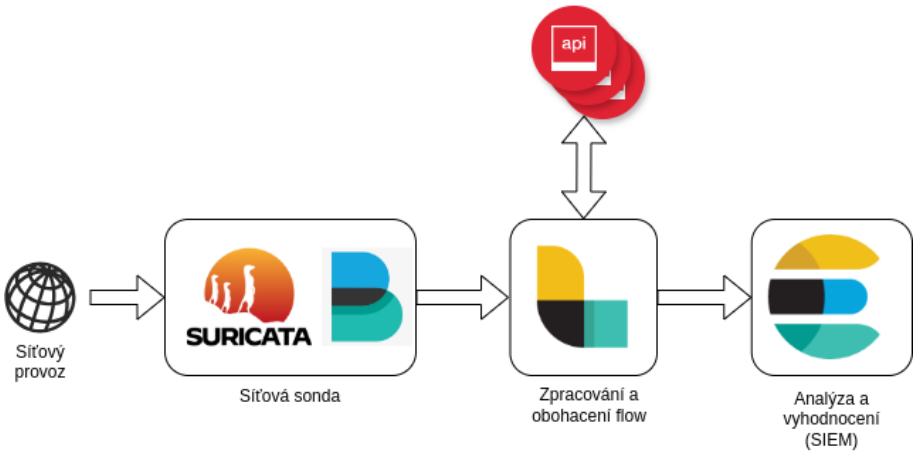
Jedním z přístupů, jak optimalizovat využití API a snížit náklady a zátěž, je cílené dotazování na základě pravidel odvozených z threat intelligence. Místo plošného obohacování všech dat systém dotazuje API pouze pro určité podezřelé události, indikátory nebo anomálie identifikované pomocí interních heuristik a modelů hrozeb. Tím se významně sníží počet dotazů při zachování vysoké relevance získaných informací.

Například pokud systém zaznamená pokus o připojení na známý C2 server nebo detekuje škodlivý soubor, může automaticky dotázat API pro reputaci přidružených IP adres, domén a souborových hashí. Naopak běžná legitimní komunikace nevyžaduje dodatečné kontextové informace. Kombinace místní analýzy a cíleného dotazování tak poskytuje efektivní rovnováhu mezi hloubkou inspekce a náklady na externí služby.

Důležitým aspektem využívání API je také rychlost aktualizace informací ve srovnání s lokálními databázemi. V oblasti kybernetických hrozeb se situace mění velmi dynamicky - nové hrozby se objevují prakticky neustále a indikátory kompromitace rychle zastarávají. Lokálně stažené a neaktualizované databáze IoC proto mohou vést k falešně negativním detekcím. Naproti tomu API obvykle poskytují nejaktuálnější informace v reálném čase, což umožňuje detekovat i zcela nové a neznámé hrozby. Průběžné dotazování API tak zajišťuje, že systém pracuje s nejčerstvějšími poznatky o aktuálních hrozbách.

6.4.1 Dotazování API pomocí nástroje Logstash

Logstash je open-source nástroj pro sběr, parsování a obohacování logů z různých zdrojů. Jednou z jeho silných stránek je schopnost dotazovat se na externí API služby a obohacovat zpracovávané logy o dodatečné informace. Tuto funkcionalitu lze využít například pro získání reputace souborů pomocí různých API s využitím `http` modulu.



Obrázek 6.8 : Dotazování API

Dotazování na API v Logstashi funguje následovně:

1. Logstash přijme vstupní událost (log) a zpracuje ji podle konfigurace v sekci "input".

2. V sekci „filter“ se pomocí podmínek vybírají události, které chceme obohatit daty z API. Můžeme zde parsovat a extrahovovat relevantní informace z logu.

3. Pokud událost splňuje podmínky, vytvoří se HTTP požadavek na specifikovanou API URL. Parametry požadavku (např. cesta, hlavičky, autentizace) se definují v konfiguraci.

4. API vrátí odpověď ve formátu JSON, XML apod. Tuto odpověď můžeme pomocí Logstashe zparsovat a vybrat z ní potřebné informace.

5. Vybrané informace z API odpovědi se vloží do původní události jako nová pole.

6. Obohacená událost putuje dál ke zpracování a výstupu podle konfigurace v sekci "output".


```
{
  "_index": "filebeat-8.13.0-2024.03.30",
  "_id": "nt5rkY4BomRhU5JvvsAM",
  "_version": 1,
  "_score": 0,
  "_ignored": [
    "event.original.keyword"
  ],
  "_source": {
    "virustotal_response": {
      "data": {
        "links": {
          "self": "https://www.virustotal.com/api/v3/files/131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267"
        },
        "id": "131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbdfd8267",
        "attributes": {
          "first_submission_date": 1148405181,
          "last_analysis_date": 1711765921,
          "magic": "EICAR virus test files",
          "names": [
            "eicar[1].com",
            "eicar.txt",
            "eicar_test_file.com-kopia.exe",
            "eicar_test_file.com-kopia 2.zip",
            "eicar_test_file.com",
            "eicar.com",
            "X5O P  AP 4 PZX54 P  7CC 7  EICAR-STANDARD-ANTIVIR.txt",
            "eicar.command",
            "php4hyXuD",
            "eicar.com.txt",
            "php6axSml",
            "phpeTMIbD",
            "test.txt",
            "eicar2.pdf",
            "maltox.txt",
            "eicar_test.txt",
            "Passfoto.jpg",
```


Obrázek 6.9 : Výstup z VT v Elasticsearch

Konkrétní příklady dotazování na API v Logstashi můžou vypadat takto:

```
if [suricata][eve][event_type] == "fileinfo" and [suricata][eve][fileinfo][state] ==
    "CLOSED" {
  http {
    url => "https://www.virustotal.com/api/v3/files/%{[suricata][eve][fileinfo][md5
    ]}"
    headers => {
      "x-apikey" => "X-API-KEY"
    }
    target_body => "virustotal_response"
  }
}
```

Listing 11 : Logstash požadavek na API VirusTotalu

Vysvětlení konfigurace z výpisu 11:

1. Podmínka `if` vybírá pouze události, kde pole **[suricata][eve][event_type]** má hodnotu „fileinfo“ a zároveň pole **[suricata][eve][fileinfo][state]** má hodnotu „CLOSED“. Tyto události reprezentují soubory detekované IDS Suricata.

2. Pro vybrané události se vytvoří HTTP GET požadavek na API URL **https://www.virustotal.com/api/v3/files/**, kde se za lomítko doplní hash souboru (MD5) extrahovaný z pole **[suricata][eve][fileinfo][md5]**.

3. V hlavičce požadavku se předá API klíč pro autentizaci.

4. Odpověď od VirusTotal API se uloží do nového pole **virustotal_response** v původní události.

5. Obohacená událost (Obrázek 6.9) se pošle dál ke zpracování.

```
if [suricata][eve][event_type] == "http" {
  http {
    url => "https://api.abuseipdb.com/api/v2/check"
    method => "GET"
    query => {
      "ipAddress" => "%{[source][ip]}"
      "maxAgeInDays" => "30"
      "verbose" => true
    }
    headers => {
      "Key" => "OWN-API-KEY"
      "Accept" => "application/json"
    }
    target_body => "abuseipdb_response"
  }
}
```

Listing 12 : Logstash požadavek na API AbuseIPDB

Tato podmínka obohacuje data všech hostů, kteří se pokouší připojit na hlídaný webový server. V reálném světe tento dohled nedává příliš smysl, ale jako příklad je tento dotaz validní. Za předpokladu, že by server byl dostupný z Internetu, bychom rychle dostali informace o adresách skenerů, ale také bychom rychle přišli i limit dotazů. V reálném nasazení by bylo možná vhodné, do podmínky přidat adresu URL našeho API, kde se předkládá mnohem nižší provoz.

Vysvětlení konfigurace z výpisu 12:

1. V sekci filter je blok `if` **[suricata][eve][event_type]**, který spustí dotaz na AbuseIPDB API pouze pokud je proveden „http“ požadavek.
2. `url` specifikuje základní URL pro AbuseIPDB API.
3. `method` je nastaveno pro **GET** požadavek.
4. `ipAddress` se nastaví na hodnotu pole **[source][ip]** z aktuální události.
5. `maxAgeInDays` určuje množství hlášení za definovaný počet dní.
6. `Key` obsahuje osobní AbuseIPDB API klíč.
7. `Accept` je nastaveno na **application/json** pro přijetí JSON odpovědi.
8. `target_body` určuje název pole, do kterého se uloží tělo API odpovědi.

Ukázka konfigurace 11 a 12 patří do sekce `filter` v konfiguraci Logstashe. Tímto způsobem lze využít Logstash pro dotazování různých API k obohacování událostí o cenné informace z externích zdrojů. Podobným způsobem by se dalo dotazovat na reputaci IP adres, domén, hash hodnot atd. Z bezpečnostního hlediska je ovšem nutné dobře zabezpečit API klíče a používat šifrovanou komunikaci (HTTPS), aby citlivá data nemohla uniknout. Nevýhodou takové podmínky ovšem je, že k dotazu na API dojde při každém úspěšném zachycení souboru což ve větších sítí, nebo sítích s intenzivním provozem může působit problémy s přetěžováním API, nebo rychlým vyčerpáním možství dotazů. Proto je vhodnější dotaz upravit tak, aby k volání docházelo pouze v případech, že přenos souboru se uskuteční v rámci flow, které je označené jako **alerted**.

6.4.2 Korelace datových zdrojů

Korelace v kontextu bezpečnostního monitoringu a detekce hrozeb je proces kombinování a analyzování dat z různých zdrojů s cílem identifikovat souvislosti, vzorce a anomálie, které mohou indikovat bezpečnostní incident nebo kompromitaci systému. Korelační techniky umožňují dát zdánlivě nesouvisející události do kontextu a odhalit komplexní útoky, které by při izolovaném zkoumání jednotlivých datových bodů zůstaly nepovšimnuty.

Efektivita a spolehlivost korelace do značné míry závisí na kvalitě a důvěryhodnosti vstupních dat. Bezpečnostní systémy obvykle čerpají data z široké škály zdrojů, včetně interních logů, síťových senzorů, endpoint agentů a externích zpravodajských kanálů. Každý z těchto zdrojů má své silné a slabé stránky z hlediska úplnosti, přesnosti a spolehlivosti poskytovaných informací. Pro úspěšnou korelaci je nutné pečlivě

vyhodnotit kvalitu a relevanci každého zdroje a odpovídajícím způsobem upravit váhu a důvěryhodnost přiřazenou jeho datům.

Zvláště u online zdrojů, jako jsou veřejné a komerční databáze IoC, reputační služby a kanály pro sdílení threat intelligence, je důvěryhodnost klíčovým faktorem. Volně dostupné zdroje mohou poskytovat cenné informace, ale často postrádají důkladnou kontrolu kvality, ověřování a aktuálnost. Hrozí tedy vyšší riziko falešně pozitivních nálezů, zastarání údajů a neúplného pokrytí hrozeb. Placené služby obvykle nabízejí vyšší kvalitu a spolehlivost díky přísnějším procesům ověřování, častější aktualizaci a širšímu rozsahu zdrojů. Jejich využití však znamená dodatečné náklady, které je třeba zvážit v kontextu celkového bezpečnostního rozpočtu a přínosů.

Bez ohledu na kvalitu a původ dat je pro efektivní korelaci nezbytná přítomnost kvalifikovaných bezpečnostních analytiků. Žádný automatizovaný systém nedokáže zcela nahradit lidskou expertízu a úsudek při vyhodnocování a interpretaci korelovaných dat. Analytici s hlubokou znalostí hrozeb, zkušenostmi s forensní analýzou a porozuměním specifickému prostředí organizace dokáží oddělit relevantní signály od šumu, odhalit falešně pozitivní nálezy a identifikovat skutečné incidenty vyžadující zásah. Jejich role je klíčová pro přeměnu surových dat na akční zpravodajské informace a pro řízení odpovídajících reakcí na incidenty.

7 PRAVIDLA

Suricata je open source systém, který nabízí rozsáhlé možnosti pro tvorbu pravidel pro detekci hrozeb na základě analýzy síťového provozu. Pravidla Suricaty umožňují detekovat podezřelé aktivity a škodlivý provoz na různých vrstvách ISO/OSI modelu.

Na síťové vrstvě Suricata podporuje klíčová slova pro detekci založenou na IP adresách, TTL, IP volbách a fragmentaci. Na transportní vrstvě lze detekovat na základě portů, TCP flagů, sekvencí a oken. Suricata také umožňuje detekovat specifické protokoly aplikační vrstvy jako HTTP, DNS, TLS/SSL, SSH, FTP, SMB, SMTP a mnoho dalších.[41]

```
1 alert tcp any any -> any any (msg:"Detekce SYN flood utoku"/; flow:stateless/; flags
    :S,12; threshold: type both, track by_src, count 1000, seconds 1; sid:1000001;
    rev:1;)
2 alert tcp any any -> any 22 (msg:"Detekce pokusu o bruteforce utok na SSH"; flow:
    to_server,established; ssh.proto; content:"SSH-"; depth:4; ssh.protoversion
    :1.99,<; ssh.softwareversion:"PuTTY"; sid:1000002; rev:1;)
3 alert tcp any any -> any 25 (msg:"Detekce pokusu o odeslani spamu pres SMTP"; flow:
    established,to_server; smtp.command:MAIL; smtp.address.from:/spammer.com$/; smtp
    .header:.+Subject\s*:\s*(?:(?:Free|Cheap).*?\b(?:meds|pills|watches)\b|Work from
     home|Earn $\d+)/; sid:1000003; rev:1;)
```

Listing 13 : Příklady pravidel pro TCP, SSH a SMTP

Pro každý z těchto protokolů aplikační vrstvy Suricata poskytuje specializovaná klíčová slova, která umožňují detailní inspekci jednotlivých polí protokolu. Například pro HTTP lze detekovat na základě URI, hlaviček, cookies, verzí protokolu atd. Pro DNS jsou k dispozici klíčová slova pro detekci query, odpovědí, typů záznamů apod.

Kromě využití předdefinovaných klíčových slov pravidla Suricaty podporují také regulární výrazy (PCRE), které dávají velkou flexibilitu pro hledání vzorů v payloadu paketů. Regulární výrazy umožňují vytvářet komplexní signatury pro detekci na základě obsahu. Je však třeba mít na paměti, že použití PCRE může být výpočetně náročné, obzvlášť při aplikaci na obsah paketů. Neoptimalizované nebo příliš obecné regulární výrazy mohou vést ke značnému vytížení CPU a zpomalení detekce. Je proto důležité používat PCRE uvážlivě a snažit se o co nejpřesnější a nejkratší možné výrazy. Suricata naštěstí nabízí některé optimalizace jako `pcre_prefilter` pro částečnou kompenzaci režie PCRE.

```
1 alert http any any -> any any (msg:"Detekce podezreleho obsahu v HTTP pozadavku";
    flow:to_server,established; http.method; content:"POST"; http.uri; pcre:"//(?:
    admin|manage|setup|config)/i"; sid:1000004; rev:1;)
```

Listing 14 : Příklad pravidla s PCRE

Pro ještě větší rozšíření detekčních schopností Suricata umožňuje využít skriptovací jazyk Lua. Skripty v Lua dávají možnost implementovat vlastní logiku pro inspekci provozu a generování alertů nad rámec možností samotných pravidel. Lua skripty se registrují v pravidlech a spouští se během zpracování každého paketu. Podobně jako u PCRE, i použití Lua skriptů může být výpočetně náročné, pokud se volají nad každým

paketem. Při implementaci Lua skriptů je třeba dbát na to, aby byly co nejrychlejší a volaly se jen v odůvodněných případech.

```
alert http any any -> any any (msg:"Detekce podezrele kratkeho User-Agent pomoci Lua
    "; flow:to_server,established; http.method; content:"GET"; http.user_agent; lua:
    check_user_agent.lua; sid:1000005; rev:1;)
```

Listing 15 : Příklad pravidla s LUA

```
function init (args)
local min_length = tonumber(args["min_length"]) or 10
return 0, {min_length = min_length}
end

function match(args)
local ua = tostring(HttpGetRequestHeader("User-Agent"))
if ua:len() < args["min_length"] then
return 1
end
return 0
end
```

Listing 16 : Lua skript *„check_ user_ agent.lua“*

Zajímavým prvkem pravidel Suricaty jsou také Datové sady (Datasets). Jde o mechanismus pro načítání externích dat (IP adresy, domény, řetězce…) do pojmenovaných množin, které lze následně využít v pravidlech přes klíčové slovo dataset. Datové sady umožňují udržovat rozsáhlé blacklisty nebo whitelisty odděleně od pravidel a zefektivňují jejich správu a sdílení. Použití datových sad může výrazně zrychlit detekci, protože odpadá nutnost opakovaně prohledávat velké množiny dat přímo v pravidlech. Tímto způsobem lze udržovat až miliony domén, nebo url, bez výrazného výkonového zatížení detekce.[42]

```
alert dns any any -> any any (msg:"Detekce DNS dotazu na domenu z blacklistu"; dns.
    query; dataset:isset,domains_blacklist,dns_query; sid:1000006; rev:1;)
```

Listing 17 : Příklad pravidla s Datovou sadou

```
malware.com
phishing.net
spam.org
...
```

Listing 18 : Příklad obsahu souboru *„domains_ blacklist“*

7.1 Detekce zranitelností

Detekce zranitelností a hrozeb pomocí pravidel pro Suricatu je důležitou součástí zabezpečení počítačových sítí. Suricata je open-source nástroj pro detekci a prevenci průniků (IDS/IPS), který umožňuje monitorovat síťový provoz a identifikovat potenciální bezpečnostní hrozby na základě definovaných pravidel. Tato pravidla popisují charakteristické vzorce útoků, škodlivých aktivit nebo zneužití zranitelností a umožňují Suricatě tyto hrozby detekovat a případně na ně reagovat.

Pravidla pro Suricatu se typicky skládají z několika klíčových částí, jako jsou hlavičky pro identifikaci protockolů a portů, obsahové vzory pro hledání specifických řetězců nebo binárních sekvencí v paketech, a metadata pro klasifikaci a kategorizaci

alertů. Pravidla mohou být velmi jednoduchá, detekující např. přítomnost určitého klíčového slova v HTTP požadavku, nebo naopak velmi komplexní, využívající pokročilé techniky jako PCRE regulární výrazy, Lua skripty nebo externí datové sady pro detekci sofistikovaných hrozeb.

Při vytváření pravidel pro Suricatu je důležité najít rovnováhu mezi přesností detekce a výkonem systému. Příliš obecná pravidla mohou generovat velké množství falešně pozitivních alertů a zatěžovat analytiky bezpečnostního týmu, zatímco příliš specifická pravidla zase mohou propásnout nové nebo mutované hrozby. Je proto nutné pravidla průběžně testovat, ladit a aktualizovat na základě měnící se bezpečnostní situace a zpětné vazby z reálného provozu.

7.1.1 Známé zranitelnosti

Detekce známých zranitelností pomocí pravidel od komunity a vlastnoručně napsaných pravidel je důležitou součástí proaktivní bezpečnostní strategie. Veřejně dostupné zdroje, jako jsou otevřené databáze zranitelností (např. NVD, CVE), bezpečnostní bulletiny dodavatelů software nebo diskuzní fóra bezpečnostní komunity, poskytují cenné informace o nově objevených zranitelnostech a souvisejících indikátorech útoků. Tyto informace lze využít k vytvoření detekčních pravidel pro Suricatu, která umožní včas odhalit pokusy o zneužití těchto zranitelností v síťovém provozu.

Komunitní pravidla, vytvářená a sdílená bezpečnostními experty a organizacemi z celého světa, představují rychlý a efektivní způsob, jak rozšířit detekční schopnosti Suricaty o signatury pro nejnovější hrozby. Zdroje jako Emerging Threats, Snort nebo komunitní repozitáře na GitHubu nabízejí rozsáhlé sady pravidel, které pokrývají široké spektrum zranitelností a útoků. Tato pravidla jsou většinou založena na analýze reálných útoků a jsou průběžně aktualizována tak, aby reflektovala nejnovější trendy a techniky používané útočníky. Začlenění těchto komunitních pravidel do konfigurace Suricaty může významně zvýšit schopnost systému detekovat známé hrozby.

Kromě komunitních pravidel je však důležité vytvářet i vlastní detekční pravidla na základě informací z interních zdrojů a vlastních znalostí prostředí. Každá organizace má svá specifika, ať už jde o používané technologie, architekturu sítě, kritické systémy a data, nebo bezpečnostní politiky. Tato specifika by měla být zohledněna při tvorbě vlastních pravidel, která doplňují obecná komunitní pravidla a přizpůsobují detekci konkrétnímu prostředí. Vlastní pravidla mohou cílit na zranitelnosti v interních aplikacích, detekovat neobvyklé vzorce chování uživatelů nebo reagovat na informace z bezpečnostních testů a auditů.

Při tvorbě vlastních pravidel je nutné vycházet z důkladné znalosti síťové infrastruktury, používaných protokolů a služeb. Cenným zdrojem informací jsou také logy a

záznamy z různých bezpečnostních nástrojů (firewally, antiviry, systémy pro správu identit a přístupů...), které mohou odhalit anomálie a podezřelé aktivity. Tyto informace lze využít k definici charakteristických vzorců útoků a jejich přenesení do podoby detekčních pravidel. Vlastní pravidla by měla být přesně cílená, aby minimalizovala falešně pozitivní detekce, ale zároveň dostatečně obecná, aby pokryla různé varianty a mutace útoků.

Příklad vlastního pravidla pro detekci pokusu o SSH připojení na DNS servery z IP adresy, která nepatří skupině administrátorů:

```
alert tcp !$ADMIN_NET any -> $DNS_SERVERS 22 (msg:"Pokus o pripojeni na SSH port DNS
    serveru z neopravneneho rozsahu"; flow:to_server,established; threshold:type
    limit, track by_src, count 1, seconds 30; classtype:attempted-admin; sid
    :1000007; rev:1;)
```

Listing 19 : SSH pravidlo

Kombinace komunitních a vlastních pravidel umožňuje dosáhnout komplexního pokrytí známých zranitelností a hrozeb. Je však důležité pravidla průběžně revidovat, testovat a aktualizovat v souladu s vývojem bezpečnostní situace a změnami v prostředí. Pravidelná analýza alertů generovaných Suricatou, zpětná vazba od bezpečnostních týmů a korelace s dalšími zdroji informací pomáhá identifikovat oblasti pro zlepšení a optimalizaci pravidel. Správně nastavená a udržovaná sada detekčních pravidel je klíčovým předpokladem pro efektivní fungování Suricaty a včasnou detekci a reakci na bezpečnostní incidenty.

7.1.2 Neznámé zranitelnosti

Detekce neznámých zranitelností představuje značnou výzvu, protože se jedná o hrozby, pro které zatím neexistují známé signatury nebo detekční pravidla. Tyto zranitelnosti, často označované jako „zero-day“ nebo „0-day“, jsou zvláště nebezpečné, protože je útočníci mohou zneužít dříve, než jsou vydány bezpečnostní záplaty nebo aktualizována detekční pravidla. Vzhledem k tomu, že tradiční přístupy založené na signaturách zde selhávají, je nutné se zaměřit na alternativní metody detekce.

Jedním z klíčových přístupů k detekci neznámých zranitelností je hledání anomálií a odchylek od normálního chování sítě a systémů. Jak bylo zmíněno v předchozí kapitole, monitorování připojení na servery z nestandardních sítí je dobrým příkladem. Pokud zaznamenáme pokusy o přístup k citlivým systémům ze zdrojových IP adres, které nepatří do očekávaného rozsahu (např. interní sítě nebo sítě důvěryhodných partnerů), může to být indikátor probíhajícího útoku nebo pokusu o průzkum sítě. Tyto anomálie je třeba důkladně vyšetřit a analyzovat, zda se nejedná o známky zneužití dosud neznámé zranitelnosti.

Dalším přístupem je analýza vzorců chování na aplikační vrstvě. Moderní útoky často zneužívají zranitelnosti ve webových aplikacích, databázích nebo API rozhra-

ních. I když nemusíme znát přesnou podstatu zranitelnosti, můžeme hledat odchylky od očekávaných vzorců komunikace a datových toků. Například neobvykle dlouhé nebo složité HTTP požadavky, pokusy o injektáž SQL kódu, nebo volání neexistujících API endpointů mohou naznačovat probíhající útok. Pomocí technik strojového učení a behaviorální analýzy lze trénovat modely normálního chování aplikací a detekovat odchylky v reálném čase.

```
alert http any any -> any any (msg:"Neobvykle dlouhy nebo slozity HTTP pozadavek";
    flow:to_server,established; content:"GET"; http_method; content:"POST";
    http_method; content:"HTTP/1.1"; http_protocol; pcre:"/(?:GET|POST)\s+\S{2000,}/
    i"; threshold:type limit, track by_src, count 1, seconds 30; classtype:attempted
    -recon; sid:1000008; rev:1;)
```

Listing 20 : Neobvykle dlouhý nebo složitý HTTP požadavek

```
alert http any any -> any any (msg:"Pokus o SQL injection"; flow:to_server,
    established; content:"SELECT"; nocase; pcre:"/(\w+)(?:'|\s+)(?:FROM|INTO|UPDATE)
    /i"; threshold:type limit, track by_src, count 1, seconds 30; classtype:web-
    application-attack; sid:1000009; rev:1;)
```

Listing 21 : Pokus o SQL injection

```
alert http any any -> any any (msg:"Volani neexistujiciho API endpointu"; flow:
    to_server,established; content:"GET"; http_method; content:"POST"; http_method;
    pcre:"/\/api\/\S+\s+HTTP\/\d\.\d/i"; http_uri; content:"404"; http_stat_code;
    threshold:type limit, track by_src, count 1, seconds 30; classtype:attempted-
    recon; sid:1000010; rev:1;)
```

Listing 22 : Volání neexistujícího API endpointu

Kromě toho je důležité sledovat i neobvyklé vzorce chování uživatelů a koncových zařízení. Náhlé změny v přihlašovacích zvyklostech, přístupy k citlivým datům mimo běžnou pracovní dobu, nebo pokusy o eskalaci oprávnění mohou být příznaky kompromitace uživatelských účtů nebo zařízení.

Při detekci neznámých zranitelností hraje klíčovou roli také sdílení informací a spolupráce s bezpečnostní komunitou. Účast v diskuzních fórech, odebírání bezpečnostních bulletinů a sledování zpráv o nově objevených zranitelnostech pomáhá udržovat přehled o aktuálních hrozbách. Sdílení vlastních poznatků a IoC s ostatními organizacemi zase přispívá k rychlejšímu odhalení a reakci na nové hrozby. Platformy jako MISP nebo OTX usnadňují výměnu informací o hrozbách a pomáhají komunitě společně čelit i neznámým zranitelnostem.

Detekce neznámých zranitelností vyžaduje proaktivní přístup, neustálou ostražitost a schopnost rychle reagovat na neobvyklé vzorce chování a anomálie. I když nemůžeme spoléhat na existující signatury, kombinace různých detekčních technik, sdílení informací a neustálé zlepšování našich bezpečnostních opatření nám pomáhá držet krok i s těmi nejnovějšími a neznámými hrozbami.

7.2 Optimalizace pravidel

Optimalizace pravidel z hlediska výkonu je klíčovým aspektem při nasazení systémů jako je Suricata. Neefektivní nebo špatně napsaná pravidla mohou významně zatěžovat

systémové prostředky, způsobovat vysokou míru falešně pozitivních detekcí a v konečném důsledku snižovat schopnost systému odhalovat skutečné hrozby. Proto je důležité věnovat pozornost výkonnostním aspektům při tvorbě a ladění detekčních pravidel.

Jedním z hlavních faktorů ovlivňujících výkon pravidel je použití datových sad. Datové sady umožňují seskupit podobná pravidla a aplikovat na ně společné podmínky, což může významně snížit počet pravidel, která musí být vyhodnocena pro každý paket nebo tok. Typickým příkladem budiž domény, které jsou komunitou označeny za škodlivé, nebo místo definice stovek samostatných pravidel pro detekci různých typů SQL injektáže můžeme vytvořit jednu datovou sadu obsahující klíčová slova a vzory související s SQL injektáží a tuto sadu pak použít v menším počtu obecnějších pravidel. Použití datových sad také usnadňuje správu a aktualizaci pravidel, protože změny provedené v datové sadě se automaticky projeví ve všech pravidlech, která tuto sadu používají.

Další optimalizačním technikou je použití klíčového slova `fast_pattern`. Toto klíčové slovo určuje, která část obsahu pravidla má být použita jako rychlý vyhledávací vzor. Suricata používá několik algoritmů pro rychlé vyhledávání vzorů v paketech a tocích, včetně Aho-Corasick (AC), Hyperscan (HS), Aho-Corasick Ken Steele varianty (AC-KS) a Aho-Corasick Boyer-Moore (AC-BS). Pokud pravidlo obsahuje klíčové slovo `fast_pattern`, Suricata nejprve vyhledá tento vzor pomocí zvoleného algoritmu (ve výchozím nastavení se používá Aho-Corasick) a pouze pokud je vzor nalezen, provede vyhodnocení zbytku pravidla. Tím se výrazně snižuje počet pravidel, která musí být plně vyhodnocena pro každý paket. Při výběru obsahu pro `fast_pattern` je důležité zvolit dostatečně specifický vzor, který se bude vyskytovat v cílených hrozbách, ale zároveň nebude příliš častý v běžném provozu, aby nedocházelo k nadměrnému počtu falešně pozitivních detekcí. Suricata umožňuje konfigurovat, který algoritmus má být použit pro vyhledávání vzorů, a to jak globálně, tak pro jednotlivá pravidla. Na podporovaných platformách je doporučeno použít algoritmus Hyperscan, který obecně poskytuje nejlepší výkon. Na běžném hardwaru, kde Hyperscan není k dispozici, je doporučeno použít algoritmus AC-KS, který má lepší výkon než výchozí algoritmus AC.[43]

```
1 alert http any any -> any any (msg:"SQL Injection Attempt"; flow:to_server,
    established; content:"POST"; http_method; content:"SELECT"; fast_pattern; nocase
    ; http_uri; content:"FROM"; nocase; http_uri; content:"WHERE"; nocase; http_uri;
     sid:1000011; rev:1;)
```

Listing 23 : Příklad pravidla využívající `fast_pattern`

Další klíčová slova a techniky, které mohou přispět k optimalizaci výkonu pravidel. Například klíčové slovo "depth"omezuje, jak daleko v paketu nebo toku bude Suricata hledat zadaný obsah. Podobně klíčové slovo "offset"určuje, od jaké pozice v paketu nebo toku má vyhledávání začít. Vhodné použití těchto klíčových slov může snížit

množství dat, které musí být prohledáno a tím zrychlit zpracování pravidel. Dalším užitečným klíčovým slovem je "flowbits", které umožňuje nastavovat a testovat příznaky pro jednotlivé toky. Pomocí "flowbits"můžeme vytvářet komplexnější pravidla, která detekují sekvence událostí nebo stavové informace v rámci relací, aniž bychom museli opakovaně vyhodnocovat stejné podmínky.

```
alert tcp any any -> any 80 (msg:"Suspicious User-Agent String"; flow:to_server,
    established; content:"User-Agent: "; http_header; content:"|28|Mozilla/5.0|29|";
     nocase; http_header; depth:18; offset:12; sid:1000012; rev:1;)
```

Listing 24 : Příklad pravidla využívající „depth“ a „offset“

Při optimalizaci pravidel je také důležité pečlivě zvážit celkový počet a složitost pravidel. Každé dodatečné pravidlo a podmínka zvyšuje nároky na systémové prostředky a může zpomalovat zpracování provozu. Proto je vhodné pravidelně revidovat a odstraňovat zastaralá nebo redundantní pravidla, slučovat podobná pravidla do obecnějších pomocí datových sad a používat co nejspecifičtější podmínky pro omezení falešně pozitivních detekcí. Rovněž je užitečné sledovat statistiky výkonu a využití zdrojů při běhu Suricaty a na základě těchto informací identifikovat problematická pravidla a oblasti pro optimalizaci.

Optimalizace výkonu pravidel je kontinuální proces, který vyžaduje pravidelnou údržbu, testování a ladění. Použití technik jako datové sady, `fast_pattern`, omezení hloubky a ofsetu vyhledávání, společně s pečlivou správou celkové sady pravidel, může významně zlepšit výkon a efektivitu Suricaty při detekci hrozeb. Zároveň je důležité najít rovnováhu mezi výkonem a pokrytím hrozeb, aby optimalizace nevedla ke snížení schopnosti systému odhalovat skutečné útoky. Pravidelná zpětná vazba od analytiků a korelace s dalšími zdroji informací o hrozbách pomáhá této rovnováhy dosáhnout a udržovat pravidla aktuální a efektivní.

7.2.1 Aho-Corasick

Aho-Corasick je algoritmus pro vyhledávání více řetězců současně, který byl publikován v roce 1975 Alfredem V. Ahem a Margaret J. Corasickovou. Algoritmus nejprve vytvoří konečný automat (trie) ze sady hledaných řetězců a poté prochází vstupní text znak po znaku. Při každém kroku aktualizuje stav automatu a pokud se dostane do koncového stavu, znamená to, že byl nalezen jeden nebo více hledaných řetězců. Aho-Corasick má lineární časovou složitost vzhledem k délce vstupního textu a počtu hledaných řetězců, což z něj činí efektivní algoritmus pro vyhledávání vzorů. Je široce používán v aplikacích, jako jsou antivirové programy, systémy pro detekci narušení a zpracování přirozeného jazyka.

7.2.2 Boyer-Moore

Algoritmus Boyer-Moore je efektivní algoritmus pro vyhledávání podřetězce v řetězci, který se často používá v aplikacích pro zpracování textu a detekci vzorů, jako jsou antivirové programy nebo systémy pro detekci narušení. Hlavní myšlenkou algoritmu je začít porovnávání hledaného podřetězce s textem od konce podřetězce a postupovat směrem doleva. Pokud dojde k neshodě, algoritmus využívá dva předpočítané posuny (tzv. „bad character shift“ a „good suffix shift“) k přeskočení pozic v textu, kde se hledaný podřetězec určitě nemůže nacházet. Tím se eliminuje zbytečné porovnávání a významně se zrychluje vyhledávání, zejména pro delší podřetězce a texty. V nejlepším případě, kdy se hledaný podřetězec v textu nenachází, má algoritmus Boyer-Moore lineární časovou složitost *O(n)*, kde n je délka prohledávaného textu. V nejhorším případě, kdy se hledaný podřetězec v textu opakuje, je časová složitost *O(mn)*, kde m je délka hledaného podřetězce. I přes tento nejhorší případ je algoritmus Boyer-Moore v průměru výrazně rychlejší než jiné algoritmy pro vyhledávání podřetězců, jako je například naivní algoritmus s časovou složitostí *O(mn)* pro všechny případy.

7.2.3 Hyperscan

Hyperscan je open-source knihovna pro vysokorychlostní vyhledávání regulárních výrazů, vyvinutá společností Intel. Je optimalizována pro vícejádrové procesory a využívá pokročilé techniky, jako je vektorové zpracování a paralelizace, aby dosáhla vysoké propustnosti a nízké latence. Hyperscan podporuje širokou škálu regulárních výrazů, včetně rozšířených funkcí jako jsou lookbehind assertions, podmíněné výrazy a backreferences. Jednou z klíčových vlastností Hyperscanu je schopnost kompilovat a prohledávat stovky nebo tisíce regulárních výrazů současně, což je užitečné pro aplikace, jako jsou systémy pro detekci narušení, kde je potřeba kontrolovat síťový provoz oproti rozsáhlým sadám signatur. Hyperscan je integrován do Suricaty jako jeden z algoritmů pro vyhledávání vzorů a na podporovaných platformách je doporučen pro nejlepší výkon.

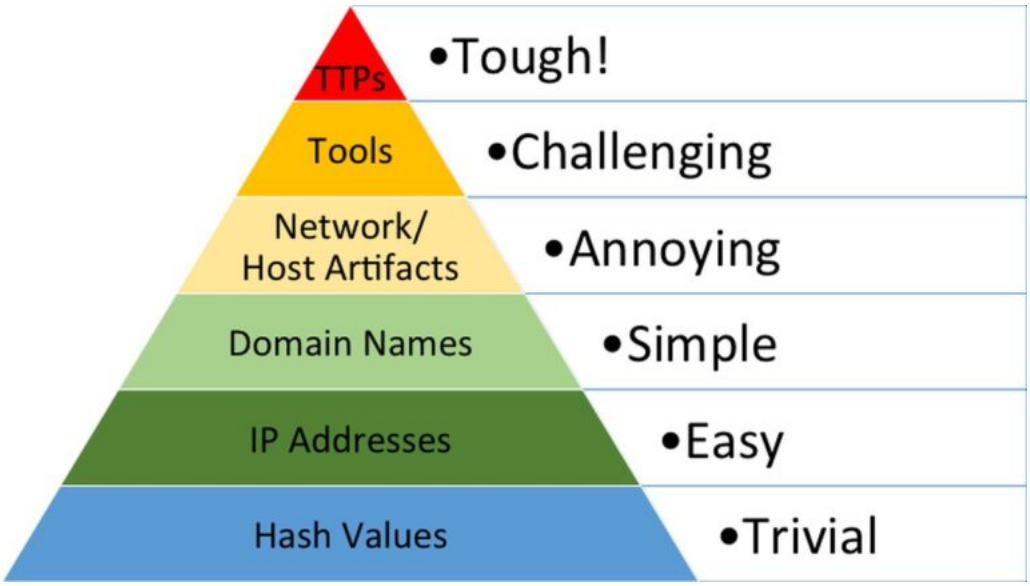
7.2.4 Aho-Corasick Ken Steele

Aho-Corasick Ken Steele varianta je modifikací původního algoritmu Aho-Corasick, kterou navrhl Ken Steele. Tato varianta se zaměřuje na zlepšení výkonu algoritmu při vyhledávání vzorů v situacích, kdy je počet hledaných řetězců relativně malý a vstupní text je dlouhý. AC-KS dosahuje zrychlení pomocí techniky zvané „failure transition caching“. Tato technika ukládá do mezipaměti informace o přechodech mezi stavy konečného automatu při selhání shody, což snižuje počet přístupů do paměti a zlepšuje lokalitu referencí. Díky tomu je AC-KS efektivnější než původní algoritmus Aho-Corasick v určitých scénářích. V Suricatě je AC-KS jedním z dostupných algoritmů pro vyhle-

dávání vzorů a je doporučen na běžném hardwaru, kde není k dispozici algoritmus Hyperscan, protože poskytuje lepší výkon než standardní Aho-Corasick algoritmus.

7.3 Pyramida bolesti

Pyramida bolesti je koncept v oblasti kybernetické bezpečnosti, který ilustruje různé typy IoC a jejich relativní hodnotu pro obránce a útočníky. Autorem konceptu je David J. Bianco, který jej představil v roce 2013 na svém blogu. Pyramida se skládá ze sedmi vrstev, které jsou seřazeny od nejméně hodnotných a nejsnáze nahraditelných indikátorů (na spodní části pyramidy) po nejhodnotnější a nejobtížněji nahraditelné indikátory (na vrcholu pyramidy).



Obrázek 7.1 : Pyramida bolesti
[49]

Čím výše v pyramidě se indikátor nachází, tím větší bolest způsobí útočníkovi, pokud je tento indikátor odhalen a zneužit obráncem. Zároveň platí, že indikátory na vyšších vrstvách pyramidy mají delší životnost a jsou pro útočníky obtížněji nahraditelné, zatímco indikátory na nižších vrstvách mají kratší životnost a útočníci je mohou snadno změnit nebo nahradit. Z druhé strany platí analogie pro obránce, čím výše v pyramidě se indikátor nachází tím těžší je pro obránce indikátor odhalit a k odhalení je třeba větší usilí a více bolesti.[48]

Textový popis jednotlivých vrstev:

1. Hašovací hodnoty jsou unikátní otisky souborů nebo dat, které lze použít k identifikaci malwaru nebo škodlivých souborů. Mají velmi krátkou životnost, protože útočníci mohou snadno upravit malware, čímž se změní i jeho hašovací hodnota.

Životnost se pohybuje v řádu dnů až týdnů a během aktivní fáze vývoje můžeme identifikovat zároveň až několik desítek aktivních hašovacích hodnot.

2. IP adresy identifikují zdroj nebo cíl síťové komunikace a mohou být použity k blokování škodlivého provozu. Mají o něco delší životnost než hašovací hodnoty, ale stále poměrně krátkou. Útočníci mohou snadno změnit IP adresy pomocí proxy serverů nebo botnetu. Životnost se pohybuje v řádu dnů až měsíců, v závislosti na tom, kdy je provoz na danou IP adresu aktivně blokován a tato činnost je spozorována útočníky.

3. Názvy domén jsou lidsky čitelné adresy, které se překládají na IP adresy. Útočníci je často používají pro hostování škodlivých serverů nebo C2 infrastruktury. Mají střední životnost, protože útočníci mohou rychle změnit DNS záznamy nebo zaregistrovat nové domény. Životnost se pohybuje v řádu týdnů až měsíců a platí to stejné co u IP adresy s tím rozdílem, že sehnat doménu se správnou reputací, aby útočníci nebudili zbytečnou pozornost je finančně i časově náročnější.

4. Artefakty v síťovém provozu jsou specifické vzory nebo anomálie v síťovém provozu, které mohou indikovat škodlivou aktivitu, například neobvyklé vzory v User-Agent nebo specifické URI parametry. Mají relativně dlouhou životnost, protože vyžadují změny v kódu malwaru nebo infrastruktuře útočníka. Životnost se pohybuje v řádu měsíců až let. Až do této vrstvy je možné plně využívat schopnosti navrhovaného pasivního systému a některé síťové artefakty zasahují i do vrstvy s nástroji.

5. Artefakty v hostitelském systému jsou specifické indikátory na kompromitovaných zařízeních, jako jsou registry keys, názvy souborů, mutex objekty nebo specifické řetězce v paměti. Mají dlouhou životnost, protože vyžadují podstatné změny v kódu malwaru. Životnost se pohybuje v řádu let.

6. Nástroje jsou software nebo skripty používané útočníky k provedení útoku nebo kompromitaci systému, například konkrétní malware, exploity nebo nástroje pro skenování portů. Mají velmi dlouhou životnost, protože vývoj nových nástrojů vyžaduje značné úsilí a zdroje. Životnost se pohybuje v řádu let až desetiletí, případně do kompromitace nástrojů. V případě kompromitace nástrojů dochází k utlumení činnosti útočníků a ti provádí tzv. „retooling“. Zde je třeba zmínit, že ke kompromitaci nástrojů často dochází neopatrností útočníků, kteří nedostatečně uklízí svou infrastrukturu.

7. TTPs popisují chování, postupy a techniky používané útočníky, například specifické kroky při průniku do systému, laterálním pohybu nebo exfiltraci dat. Mají

nejdelší životnost ze všech vrstev pyramidy, protože představují základní chování a postupy útočníků, které se v čase mění jen velmi pomalu a k jejich úplně obměně dochází až s výměnou samotného útočníka. Zvyk je železná košile. Životnost se pohybuje v řádu let až desetiletí.

7.4 Kvalita detekce

Kvalita detekce a detekčních pravidel v oblasti kybernetické bezpečnosti je úzce spjata s úrovní obecnosti pravidel a přesností detekce. Při tvorbě detekčních pravidel je důležité najít rovnováhu mezi obecností a specifičností. Příliš obecná pravidla mohou vést k vysokému počtu falešně pozitivních detekcí, kdy jsou neškodné aktivity označeny jako škodlivé. To může vést k zahlcení bezpečnostních týmů a ztížení identifikace skutečných hrozeb. Na druhou stranu, příliš specifická pravidla mohou vést k opačnému problému - falešně negativním detekcím, kdy škodlivé aktivity uniknou detekci, protože nesplňují úzce definovaná kritéria pravidla.

Přesnost detekce je klíčovým faktorem při hodnocení kvality detekčních pravidel. Vysoká přesnost znamená, že pravidla správně identifikují škodlivé aktivity a generují minimum falešně pozitivních detekcí. Toho lze dosáhnout pečlivým laděním pravidel, využitím více indikátorů kompromitace a kontextových informací, a průběžnou aktualizací pravidel na základě nových poznatků o hrozbách. Zároveň je důležité pravidelně vyhodnocovat efektivitu detekčních pravidel a upravovat je tak, aby reflektovaly měnící se taktiky, techniky a postupy útočníků. Kvalitní detekční pravidla by měla být schopna odhalit nejen známé hrozby, ale také nové a vznikající hrozby, což vyžaduje kombinaci signaturových a behaviorálních přístupů k detekci.

7.4.1 Detekování IoC vs eskalace pravidel

Detekování jednotlivých IoC a eskalace pravidel jsou dva různé přístupy k identifikaci potenciálních hrozeb v kybernetické bezpečnosti. Oba přístupy mají své výhody a nevýhody a jejich použití závisí na konkrétních potřebách a prostředí organizace.

Detekování jednotlivých IoC spočívá v identifikaci specifických artefaktů, jako jsou IP adresy, názvy domén, hašovací hodnoty souborů nebo síťové artefakty, které jsou známé jako indikátory škodlivé aktivity. Tento přístup může generovat upozornění i v případě, že detekovaný IoC pochází z obecné nebo dobře známé domény, která sama o sobě nemusí být škodlivá. To může vést k velkému počtu upozornění, která vyžadují další analýzu a vyhodnocení, často pomocí SIEM systému. Výhodou tohoto přístupu je, že umožňuje odhalit potenciální hrozby na základě známých indikátorů, ale může také generovat značné množství falešně pozitivních upozornění, která mohou zatěžovat bezpečnostní týmy.

Eskalace pravidel pomocí kombinace klíčových slov jako `noalert`, `flowint`, `flowbits` a `xbits` představuje sofistikovanější přístup k detekci hrozeb. Tento přístup se zaměřuje na vytváření komplexních pravidel, která berou v úvahu více faktorů a kontextové informace před generováním upozornění. Klíčové slovo `noalert` se používá k potlačení upozornění pro určitá pravidla, pokud nejsou splněny další podmínky. `Flowint` umožňuje sledovat a ukládat informace o síťových tocích, které mohou být použity pro korelaci událostí a identifikaci anomálií. `Flowbits` a `xbits` jsou stavové proměnné, které umožňují předávat informace mezi různými pravidly a rozhodovat o generování upozornění na základě kombinace více faktorů. Tento přístup může významně snížit počet falešně pozitivních upozornění a zaměřit se na skutečné hrozby, ale vyžaduje větší úsilí při tvorbě a ladění pravidel.

```
alert dns $HOME_NET any -> any any (msg:"Seznam.cz DNS query"; dns.query; content:"
    seznam.cz"; noalert; flowbits:set,seznam.cz.dns; sid:1000000; rev:2;)
```

Listing 25 : Pravidlo č.1 využívající `noalert` a `flowbits`

```
alert dns $HOME_NET any -> any any (msg:"Suspicious Large DNS TXT Query"; dns.query;
     dns.rrtype == 16; content:"|00 10|"; offset:2; depth:2; byte_test:2,>,500,0,
    relative; flowbits:isset,seznam.cz.dns; threshold: type both, track by_src,
    count 1, seconds 60; sid:1000001; rev:1;)
```

Listing 26 Pravidlo č.2 využívající `flowbits`

Vysvětelní funkce pravidel z výpisu 25 a 26:

První pravidlo:

- `alert` toto pravidlo by generovalo výstrahu, viz. předposlední bod
- `dns` sleduje DNS provoz
- `$HOME_NET any -> any any` sleduje odchozí provoz z vnitřní sítě kamkoliv
- `flow:established,to_server` sleduje ustavený TCP tok směrem k serveru
- `dns.query` sleduje DNS dotazy
- `content:"seznam.cz"` DNS dotaz musí obsahovat řetězec „seznam.cz“
- `noalert` zablokuje generování výstrahy
- `flowbits:set,seznam.cz.dns` nastaví příznak flowbit „seznam.cz.dns“, který se dá využít dalšími pravidly

Druhé (navazující) pravidlo:

- `dns.rrtype == 16` sleduje pouze TXT záznamy (typ 16)
- `content:"|00 10|"; offset:2; depth:2` hledá hodnoty 00 10 na offsetu 2, pouze v prvních 2 bajtech

- `dsize:>500` testuje zda je obsah payloadu větší než 500 bajtů
- `flowbits:isset,seznam.cz.dns` aplikuje se jen když je nastaven flowbit z prvního pravidla
- `threshold: type both, track by_src, count 1, seconds 60` generuje výstrahu jen pokud se pravidlo triggered víckrát než 1x za 60 sekund ze stejné zdrojové IP

Dohromady ta pravidla detekují podezřele velké DNS TXT dotazy na veřejně známou a uživateli často navštěvovanou doménu „seznam.cz“. Detekování IoC domény „seznam.cz“ by způsobovalo zahlcení SIEMu. Z historických zkušeností víme, že DNS TXT záznamy byly zneužity pro extrakci dat. První pravidlo nastaví `flowbits` když vidí jakýkoliv dotaz na „seznam.cz“. Druhé pravidlo vygeneruje `alert` pokud je `flowbits` nastaven a zároveň velikost TXT záznamu přesahuje 500 bajtů, ale pouze pokud se to stane víckrát za minutu ze stejné zdrojové IP adresy. Je důležité zmínit, že `flowbits` platí pouze v rámci daného toku (flow). Každý tok má svou vlastní sadu flowbitů. Navazující pakety ve stejném toku mohou testovat a nastavovat flowbity nastavené předchozími pravidly aplikovanými na pakety z téhož toku.[44]

Výběr mezi detekováním jednotlivých IoC a eskalací pravidel závisí na několika faktorech, včetně velikosti a složitosti prostředí, dostupných zdrojů a požadované úrovně detekce. V ideálním případě by měla organizace využívat kombinaci obou přístupů - detekování známých IoC pro odhalení základních hrozeb a eskalaci pravidel pro identifikaci pokročilých a cílených útoků. Pravidelná aktualizace a ladění pravidel na základě nových poznatků o hrozbách a zpětné vazby z vyšetřování incidentů je klíčová pro udržení efektivity a přesnosti detekce bez ohledu na zvolený přístup.

7.4.2 Nové hrozby a tvorba pravidel

Psaní pravidel na míru je klíčovou součástí efektivní detekce nových hrozeb, zejména v době, kdy se objeví nová malwarová kampaň. V počátečních fázích šíření nového malwaru jsou informace často kusé a rozptýlené napříč bezpečnostní komunitou. V této fázi je důležité aktivně sledovat relevantní zdroje, jako jsou fóra, blogy, sociální média a kanály threat intelu, a shromažďovat dostupné informace o nové hrozbě.

Jakmile jsou k dispozici první technické detaily, jako jsou IoC, vzorky malwaru nebo popis chování, je možné začít s tvorbou detekčních pravidel. V této fázi je často nutné pracovat s fragmenty informací a postupně je zapojovat do detekce. To může zahrnovat tvorbu pravidel pro detekci známých IoC, jako jsou IP adresy, domény nebo hašovací hodnoty souborů, ale také pravidel pro detekci behaviorálních vzorců, jako jsou specifické síťové toky nebo sekvence systémových volání. Důležité je také provázat

nová pravidla s již existujícími pravidly, která detekují podobné nebo související hrozby, aby se vytvořil ucelený detekční systém.

S postupem času a dalším šířením malwaru se v komunitě objevují podrobnější analýzy a ucelenější informace o hrozbě. Threat intel týmy a bezpečnostní výzkumníci vydávají detailní reporty, které popisují technické detaily, jako jsou použité exploity, infrastruktura útočníků, cíle kampaně a doporučení pro detekci a mitigaci. Tyto informace jsou cenným zdrojem pro vytváření a vylepšování detekčních pravidel. Je důležité průběžně aktualizovat existující pravidla na základě nových poznatků a přidávat nová pravidla pro detekci dalších aspektů hrozby.

V některých případech se v komunitě objeví tzv. „threat hunter playbook“, který poskytuje ucelený pohled na danou hrozbu a popisuje konkrétní kroky, jak ji detekovat a vyšetřovat ve vlastních sítích. Tyto playbooky jsou velmi cenné, protože kombinují technické detaily s praktickými postupy a často vycházejí ze zkušeností bezpečnostních týmů, které již s danou hrozbou pracovaly. Threat hunter playbooky však nejsou k dispozici pro každou novou hrozbu a jejich tvorba vyžaduje značné úsilí a odbornost. Proto je důležité být schopen pracovat i s méně ucelenými zdroji informací a průběžně je zapojovat do detekce.

Psaní pravidel na míru vyžaduje kontinuální úsilí a flexibilitu. Je nutné neustále sledovat nové informace, vyhodnocovat jejich relevanci a rychle je promítat do detekčních pravidel. Spolupráce s ostatními členy bezpečnostní komunity, sdílení poznatků a zkušeností a aktivní přispívání k tvorbě znalostní báze jsou klíčové pro efektivní detekci nových hrozeb. Pouze kombinací různých zdrojů informací, průběžnou aktualizací pravidel a proaktivním přístupem lze udržet krok s neustále se vyvíjejícím prostředím hrozeb a zajistit včasnou detekci a reakci na nové malwarové kampaně.

8 THREAT INTELLIGENCE

Hraje důležitou roli v kyberbezpečnosti organizací tím, že poskytuje kontext, informace a přehled o aktuálních hrozbách a probíhajících kampaních v kyberprostoru. TI umožňuje organizacím lépe pochopit povahu, motivaci a TTP potenciálních útočníků, což jim pomáhá přizpůsobit jejich obranné strategie a zlepšit celkovou odolnost vůči kybernetickým útokům.

Jedním z hlavních přínosů TI je poskytování kontextu hrozeb. Díky analýze a korelaci informací z různých zdrojů, jako jsou zpravodajské služby, bezpečnostní komunity, dark web, otevřené zdroje a interní data, může TI vytvořit ucelený obraz o typech hrozeb, které organizace čelí. Tento kontext umožňuje bezpečnostním týmům prioritizovat své úsilí, alokovat zdroje efektivněji a zaměřit se na nejkritičtější hrozby.

TI také pomáhá organizacím hodnotit aktuální kampaně probíhající v kyberprostoru. Sledováním trendů, analýzou nových útočných vektorů a identifikací cílených odvětví či regionů mohou organizace získat cenné poznatky o potenciálních hrozbách, kterým mohou čelit. Tyto informace umožňují proaktivně upravovat bezpečnostní opatření, zvyšovat povědomí zaměstnanců a zlepšovat detekční schopnosti.

Díky porozumění TTP původce hrozby a identifikaci potenciálních budoucích kroků útočníka může TI pomoci organizacím předvídat, co mohou očekávat dál. Tyto informace jsou cenné pro přizpůsobení detekčních pravidel, aktualizaci datových sad a nastavení proaktivních obranných mechanismů. Schopnost předvídat budoucí kroky útočníka umožňuje organizacím být o krok napřed a minimalizovat dopad potenciálních útoků.

8.1 Zdroje

Ve své práci jsem využil především bezplatné zdroje dat, nebo zdroje dat s bezplatnou licencí pro otestování služby, ale je třeba zmínit, že bezplatné TI zdroje, jako jsou online databáze, platformy pro sdílení IoC jako MISP nebo komunitní fóra a sociální sítě, poskytují cenné informace sdílené bezpečnostní komunitou. Výhodou těchto zdrojů je jejich dostupnost a rychlost sdílení informací v případě rozsáhlých útoků nebo odhalení nových zranitelností. Komunita často reaguje velmi rychle a sdílí poznatky o probíhajících hrozbách, což může být užitečné pro včasnou detekci a reakci.

Na druhou stranu spolehlivost informací z bezplatných zdrojů může být diskutabilní. Jelikož přispěvatelé jsou často dobrovolníci z řad bezpečnostní komunity, může docházet k neúplným nebo neověřeným informacím. Je tedy nezbytné věnovat dodatečný čas a úsilí ověřování a validaci získaných dat před jejich použitím v produkčním prostředí. Dalším omezením bezplatných zdrojů je, že se komunita často zaměřuje na aktuálně

probíhající útoky a méně na dlouhodobé sledování hrozeb.

Placené TI zdroje, poskytované zejména antivirovými společnostmi a specializovanými bezpečnostními firmami, nabízejí vysokou kvalitu a spolehlivost informací. Tyto společnosti mají k dispozici rozsáhlé zdroje dat, včetně vzorků malwaru a telemetrických dat z celého světa, což jim umožňuje odhalovat nové hrozby a sledovat i dlouhodobě neaktivní hrozby. Placené služby často poskytují podrobné analýzy a doporučení pro konkrétní hrozby, včetně informací o nových zranitelnostech a jejich zneužívání v reálném čase.

Výhodou placených zdrojů je jejich spolehlivost a kvalita informací, která je zajištěna týmem profesionálních analytiků a robustní infrastrukturou pro sběr a zpracování dat. Zákazníci těchto služeb mají jistotu, že získávají ověřené a aktuální informace o hrozbách. Nevýhodou může být vyšší cena těchto služeb a potenciálně omezený přístup k některým datům, která mohou být považována za citlivá nebo proprietární.

V praxi je vhodné kombinovat bezplatné i placené zdroje TI pro získání komplexního přehledu o hrozbách. Bezplatné zdroje mohou poskytnout rychlé informace o nových hrozbách a umožnit sdílení poznatků v rámci bezpečnostní komunity, zatímco placené zdroje nabízejí spolehlivé a podrobné analýzy pro dlouhodobé sledování a pochopení hrozeb. Důležité je věnovat dostatečný čas výběru, ověřování a integraci TI zdrojů do bezpečnostních procesů organizace tak, aby poskytovaly maximální hodnotu pro detekci a prevenci hrozeb.

8.1.1 Dělení zdrojů

První skupinu, využitou pro systém vytvořený v této práci, tvoří online databáze, jako jsou AbuseIPDB, VirusTotal nebo informace o IoC poskytnuté komunitou. Tyto zdroje poskytují informace v „reálném“ čase a umožňují okamžitě reagovat na aktuální hrozby. Jejich hlavní výhodou je rychlost získání dat, která jsou relevantní v daném okamžiku. Nicméně platnost těchto informací rychle zastarává, často v řádu dnů až týdnů. Pokud data nejsou zpracována a využita bezprostředně po jejich získání, jejich hodnota se snižuje. Například IP adresa, která byla identifikována jako zdroj útoku, může být po několika dnech již neaktivní, nebo zranitelnost uvedená v CVE může být mezitím opravena vydáním bezpečnostní aktualizace. Proto je při využívání těchto zdrojů klíčové mít procesy pro rychlé zpracování a aplikaci získaných informací.

Druhou skupinu zdrojů pro Threat Intelligence tvoří reporty o hrozbách, analýzy útoků a webové stránky zaměřené na zneužívané zranitelnosti. Informace z těchto zdrojů mají delší dobu platnosti a poskytují podrobnější kontext o hrozbách, ale jejich zpracování vyžaduje více času a úsilí ze strany analytika.

Reporty a analýzy útoků často popisují pozadí útoku, motivaci útočníků a používané

TTP. Výstupem takového reportu nebo analýzy může být pro naši organizaci cenná informace, zda se také nemůžeme stát dalším cílem podobného útoku, nebo podnět ke kontrole vlastních systémů, abychom ověřili, zda jsme již nebyli cílem útoku, který naše systémy nezaznamenaly. Tyto informace jsou důležité pro pochopení celkového kontextu hrozeb a pro vytváření dlouhodobých strategií obrany.

Webové stránky věnující se zneužívaným zranitelnostem poskytují podrobné technické detaily o konkrétních zranitelnostech a možnostech jejich zneužití. Zpracování informací z těchto zdrojů vyžaduje manuální analýzu a interpretaci zkušeným analytikem, který dokáže zasadit získané poznatky do kontextu dané organizace a identifikovat ty, které jsou pro ni relevantní.

Reporty, analýzy útoků a informace o zranitelnostech jsou cenné pro pochopení celkového kontextu hrozeb a pro vytváření dlouhodobých strategií obrany. Jejich analýza a zpracování sice vyžaduje více času a úsilí, ale výsledkem je ucelený přehled o aktuálních hrozbách a jejich potenciálním dopadu na organizaci.

Při využívání různých zdrojů TI je důležité zvolit vhodnou kombinaci zdrojů s ohledem na potřeby a možnosti organizace. Online databáze poskytují rychlé a aktuální informace, které jsou vhodné pro okamžitou reakci na hrozby, zatímco reporty a analýzy nabízejí hlubší kontext a dlouhodobější přehled o trendech a aktérech hrozeb. Ideální je kombinovat oba typy zdrojů a využívat automatizované nástroje pro zpracování dat z online databází společně s manuální analýzou reportů a informací z webových stránek.

Při implementaci TI je také důležité zajistit pravidelnou aktualizaci a ověřování zdrojů, aby byla zajištěna relevance a spolehlivost získaných informací. Zastaralé nebo neověřené informace mohou vést k falešným poplachům nebo zanedbání důležitých hrozeb. Proto je nezbytné mít procesy pro hodnocení kvality zdrojů a jejich průběžnou aktualizaci.

Efektivní využívání různých typů zdrojů TI vyžaduje kombinaci automatizovaných nástrojů pro rychlé zpracování dat a lidských analytiků, kteří dokáží informace interpretovat a aplikovat v kontextu dané organizace. Tímto způsobem lze získat komplexní přehled o hrozbách a zvolit adekvátní opatření pro prevenci a detekci útoků.

8.2 Kolektivní inteligence

V práci je tento přístup zajištěn pouze na úrovni sdílení dat pomocí online databází, nicméně je třeba zmínit také větší obrázek takového sdílení, který je sice nad rámec systému, který se tato práce snaží představit, ale tato poslední kapitola by mohla nastínit další postup při širší realizaci takového systému. Sdílení informací o kybernetických hrozbách a spolupráce v rámci například komunity vysokých škol v České republice a Evropě je zásadní pro zajištění efektivní kybernetické bezpečnosti. Vytvoření jednotné

znalostní báze, do které by mohly přispívat různé výzkumné týmy v rámci univerzit a vysokých škol, by umožnilo sdílet cenné poznatky a zlepšit schopnost detekce a reakce na hrozby napříč celou akademickou sférou.

V rámci vysokoškolské komunity existují instituce s různými kapacitami a zdroji. Některé univerzity disponují špičkovými týmy a infrastrukturou pro analýzu malware a monitorování síťového provozu. Tyto školy mohou poskytovat cenné informace a analýzy ostatním členům komunity, kteří nemají vlastní pokročilé kapacity. Naopak menší školy, které potřebují informace pro zajištění vlastní bezpečnosti a kontroly systémů, mohou těžit ze sdílených dat a poznatků.

Klíčovým aspektem je vzájemná důvěra mezi vysokými školami. Všechny zapojené instituce by měly sdílet pouze ověřené a spolehlivé informace o hrozbách a zranitelnostech. Díky tomu mohou mít ostatní členové komunity jistotu, že získaná data jsou kvalitní a relevantní. Efektivní distribuce těchto informací mezi školami zajistí jejich maximální využití a umožní všem zlepšit vlastní bezpečnostní postoj.

Zpracovaná a ověřená data o hrozbách by měla být dále sdílena s národními subjekty v oblasti kybernetické bezpečnosti, jako je například Národní úřad pro kybernetickou a informační bezpečnost v České republice. Tím se cenné poznatky získané v akademické sféře dostanou i k dalším důležitým hráčům v oblasti národní kyberbezpečnosti. Na evropské úrovni pak lze informace sdílet s partnerskými organizacemi a agenturami EU, což umožní koordinovanou reakci na hrozby přesahující hranice jednotlivých států.

Tento model spolupráce a sdílení informací lze aplikovat i v dalších veřejných komunitách, nejen v akademické sféře. Zásadní je však vždy důvěra mezi členy komunity a dodržování principů zodpovědného zpracování a sdílení dat o hrozbách. Jen tak lze zajistit, že budou informace skutečně přínosné a efektivně využité pro posílení kybernetické bezpečnosti na všech úrovních.[50]

ZÁVĚR

Tato diplomová práce se zaměřila na klíčový aspekt detekce zranitelností v IT infrastruktuře - efektivní sběr a obohacování relevantních bezpečnostních dat. Navržená architektura integruje různé datové zdroje, včetně skenerů zranitelností, síťových sond a externích databází informací o hrozbách. Tím vytváří robustní základ pro budoucí systémy detekce zranitelností.

Je důležité zdůraznit, že tato práce se primárně nezabývá návrhem kompletního SIEM řešení. Místo toho se soustředí na prvotní, ale kritické kroky - zajištění kvalitních vstupních dat a jejich obohacení o kontext z threat intelligence zdrojů. Tento přístup umožňuje následný vývoj pokročilých detekčních mechanismů postavených na solidním datovém základu.

Navržený systém sběru a obohacování dat byl implementován s využitím open-source nástrojů a otestován v laboratorním prostředí se simulovanými daty. Ačkoliv nebyl nasazen v reálném produkčním prostředí, testy prokázaly jeho schopnost integrovat různorodé datové zdroje a poskytovat bezpečnostním analytikům cenné informace o potenciálních zranitelnostech.

Přirozené pokračování této práce by se mělo zaměřit na využití získaných obohacených dat k vývoji pokročilých metod detekce zranitelností. Zejména aplikace technik umělé inteligence a strojového učení na takto připravená data skýtá značný potenciál. AI modely mohou pomoci odhalovat skryté vzory, predikovat nové hrozby a významně zvýšit přesnost a včasnost detekce zranitelností.

Kromě rozvoje detekčních schopností by budoucí práce mohly zkoumat i možnosti integrace navržené architektury s dalšími bezpečnostními systémy a procesy, jako je automatizovaná prioritizace a náprava zranitelností či proaktivní údržba systémů.

Celkově tato diplomová práce položila důležitý základ pro budování efektivních systémů detekce zranitelností. Navržený přístup sběru a obohacování bezpečnostních dat představuje robustní a škálovatelné řešení, které organizacím umožní lépe čelit neustále se vyvíjejícím kybernetickým hrozbám. S dalším vývojem v oblasti detekce pomocí AI se otevírá cesta k ještě silnější ochraně IT infrastruktury.

SEZNAM POUŽITÉ LITERATURY

[1] VARGHESE, Jinson. *A Comprehensive Guide to Network Vulnerability Scanning.* Astra. Online. 2023, 30. říjen 2023. Dostupné z: https://www.getastra.com/blog/security-audit/network-vulnerability-scanning/ [cit. 2024-04-21]

[2] GOOGLE. Transparency report. *HTTPS encryption on the web* Online. 2024. Dostupné z: https://transparencyreport.google.com/https/overview?hl=en [cit. 2024-04-21]

[3] SUPPLYGEM. *99 Key Internet Statistics* Online. 2024. Dostupné z: https://supplygem.com/internet-usage-statistics [cit. 2024-04-21]

[4] OPENTEXT. *SIM, SEM, and SIEM: Definitions and Choosing the Right Enterprise Solution* Online. 2019, 12. června 2019. Dostupné z: https://supplygem.com/internet-usage-statistics [cit. 2024-04-21]

[5] PALO ALTO. *What is EDR vs. XDR?* Online. 2020. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-edr-vs-xdr [cit. 2024-04-21]

[6] CESNET. *Vynikající výsledky v rámci úvodní etapy projektu Analýza šifrovaného provozu pomocí síťových toků* [online]. 2023, 11. dubna 2023. Dostupné z: https://www.cesnet.cz/o-nas/tiskove-zpravy-1/vynikajici-vysledky-v-ramci-uvodni-etapy-projektu-analyza-sifrovaneho-provozu-pomoci-sitovych-toku-57 [cit. 2024-04-21]

[7] RAPID7. *Network Traffic Analysis.* Online. Dostupné z: https://www.rapid7.com/fundamentals/network-traffic-analysis/ [cit. 2024-04-25]

[8] WIKIPEDIE. *Principle of least privilege.* In: Wikipedia: the free encyclopedia. Online. San Francisco (CA): Wikimedia Foundation, 2001-, 12 March 2024, 21:27 UTC. Dostupné z: https://en.wikipedia.org/wiki/Principle_of_least_privilege [cit. 2024-04-25]

[9] GREENBONE AG. Scripting. GVM-Tools. Online. Greenbone AG, 2018-2024. Dostupné z: https://greenbone.github.io/gvm-tools/scripting.html [cit. 2024-04-25]

[10] GERVASI, Phil. *Flows vs. packet captures for network visibility.* Kentik Blog. Online. Kentik, 2022. Dostupné z: https://www.kentik.com/blog/flows-vs-packet-captures-for-network-visibility/ [cit. 2024-05-25]

[11] Remote OS Detection. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning.* Online. Sunnyvale: Insecure, 2008. Dostupné z: https://nmap.org/book/osdetect.html [cit. 2024-05-25]

[12] Tenable. *Nessus FAQs.* Online. Tenable, 2023. Dostupné z: https://www.tenable.com/products/nessus/nessus-faq [cit. 2024-04-25]

[13] Tenable. *Nessus Docs.* Online. Tenable, 2023. Dostupné z: https://docs.tenable.com/nessus [cit. 2024-04-25]

[14] Greenbone AG. *Background - Greenbone Community Documentation.* Online. 2023. Dostupné z: https://greenbone.github.io/docs/latest/background.html [cit. 2024-04-25]

[15] SOWMYASHREE, A. a H. S. GURUPRASAD. *Evaluation and Analysis of Vulnerability Scanners: Nessus and OpenVAS.* International Research Journal of Engineering and Technology (IRJET). 2020, 7(5), 2068-2073. ISSN 2395-0056. [cit. 2024-04-25]

[16] Cisco. *Snort 3 — Now available!* Online. San Francisco: Cisco, 2021. Dostupné z: https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/004/341/original/snort3_information.pdf?161247 [cit. 2024-04-25]

[17] MORIARTY, Alex. *Suricata vs. Snort: Similarities and Differences.* Netgate. Online. Austin, TX, 2022. Dostupné z: https://www.netgate.com/blog/suricata-vs-snort [cit. 2024-04-25]

[18] MICROSOFT CORPORATION. *Use Windows Event Forwarding to help with intrusion detection.* Windows Security | Microsoft Learn. Online. 2023. Dostupné z: https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/use-windows-event-forwarding-to-assist-in-intrusion-detection [cit. 2024-04-25]

[19] MINASSIAN, Carlo. *Critical Capabilities of a Modern SOC - Data collection and correlation.* LinkedIn. Online. 2023. Dostupné z: https://www.linkedin.com/pulse/critical-capabilities-modern-soc-data-collection-carlo-minassian/ [cit. 2024-04-25]

[20] MISP Project. *MISP Documentation and Support.* Online. 2023. Dostupné z: https://www.misp-project.org/documentation/ [cit. 2024-04-25]

[21] NAKAR, Ori. *Threat Hunting Through Anomaly Detection on Your Data Lake.* Imperva. Online. Imperva, 2024. Dostupné z: https://www.imperva.com/blog/threat-hunting-through-anomaly-detection-on-your-data-lake/ [cit. 2024-04-25]

[22] ESET. *Threat intelligence for targeted cyberattack prediction.* Online. ESET, 2023. Dostupné z: https://www.eset.com/int/business/services/threat-intelligence/ [cit. 2024-04-25]

[23] Mandiant. *Threat Intelligence | Cyber Threat Intelligence Platform.* Online. Milpitas (California): Mandiant, 2023. Dostupné z: https://www.mandiant.com/advantage/threat-intelligence [cit. 2024-04-25]

[24] RECORDED FUTURE. *Threat Intelligence: Identify, Investigate, and Prioritize Cyber Threats* Online. Somerville (Massachusetts): Recorded Future, 2023. Dostupné z: https://www.recordedfuture.com/products/threat-intelligence [cit. 2024-04-25]

[25] CROWDSTRIKE. *Threat Intelligence Products* Online. Austin (Texas): CrowdStrike, 2023. Dostupné z: https://www.crowdstrike.com/platform/threat-intelligence/ [cit. 2024-04-25]

[26] CISCO TALOS INTELLIGENCE GROUP. *Cisco Talos Intelligence Group - Comprehensive Threat Intelligence.* Online. Milpitas (California): Cisco Systems, 2023. Dostupné z: https://talosintelligence.com [cit. 2024-04-25]

[27] KROPOTOV, Vladimir a Fyodor YAROCHKIN. *Hunting Threats on Twitter: How Social Media can be Used to Gather Actionable Threat Intelligence.* Trend Micro. Online. 2019. Dostupné z: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter [cit. 2024-04-25]

[28] VIRUSTOTAL. *How it works.* VirusTotal Documentation. Online. 2022. Dostupné z: https://docs.virustotal.com/docs/how-it-works [cit. 2024-04-25]

[29] VIRUSTOTAL. *Public vs Premium API Online.* Madrid: VirusTotal, 2023. Dostupné z: https://docs.virustotal.com/reference/public-vs-premium-api [cit. 2024-04-25]

[30] SHODAN. *Shodan Account.* Online. San Francisco: Shodan, 2023. Dostupné z: https://account.shodan.io/billing [cit. 2024-04-25]

[31] AbuseIPDB. *AbuseIPDB APIv2 Documentation Online.* 2023. Dostupné z: https://docs.abuseipdb.com/#check-endpoint [cit. 2024-04-25]

[32] AbuseIPDB. *API Plans & Pricing.* Online. 2023. Dostupné z: https://www.abuseipdb.com/pricing [cit. 2024-04-25]

[33] Turris Documentation. *Turris Sentinel.* Online. Dostupné z: https://docs.turris.cz/basics/sentinel/intro/ [cit. 2024-04-25]

[34] FIRST. *Common Vulnerability Scoring System v3.1: Specification Document.* Online. 2019. Dostupné z: https://www.first.org/cvss/v3.1/specification-document [cit. 2024-04-25]

[35] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *CVSS Qualitative Severity Rating Scale.* Online. 2022. Dostupné z: https://nvd.nist.gov/vuln-metrics/cvss#qualitative-severity-rating-scale [cit. 2024-04-25]

[36] DANEN, Vincent. *Patch management needs a revolution, part 3: Vulnerability scores and the concept of trust.* In: Red Hat Blog. Online. January 23, 2024. Dostupné z: https://www.redhat.com/en/blog/patch-management-needs-a-revolution-part-3 [cit. 2024-04-25]

[37] OISF. *Suricata User Guide.* In: Suricata 8.0.0-dev documentation. Online. 2016-2024. Dostupné z: https://docs.suricata.io/en/latest/index.html [cit. 2024-04-26]

[38] OISF. *Performance.* In: Suricata 8.0.0-dev documentation. Online. 2016-2024. Dostupné z: https://docs.suricata.io/en/latest/performance/index.html [cit. 2024-04-26]

[39] OISF. *suricata-update - A Suricata Rule Update Tool.* In: suricata-update 1.3.3 documentation. Online. Dostupné z: https://suricata-update.readthedocs.io/en/latest/index.html [cit. 2024-04-26]

[40] OISF. *Rule Reloads.* In: Suricata 8.0.0-dev documentation. Online. 2016-2024. Dostupné z: https://docs.suricata.io/en/latest/rule-management/rule-reload.html#rule-reloads [cit. 2024-04-26]

[41] OISF. *Suricata Rules.* In: Suricata 8.0.0-dev documentation. Online. 2016-2024. Dostupné z: https://docs.suricata.io/en/latest/rules/index.html [cit. 2024-04-27]

[42] OISF. *Datasets.* In: Suricata 8.0.0-dev documentation. online. 2016-2024. Dostupné z: https://docs.suricata.io/en/latest/rules/datasets.html [cit. 2024-04-27]

[43] OISF. *Suricata Fast Pattern Determination Explained.* In: Suricata 7.0.5 documentation. Online. 2016-2024. Dostupné z: https://docs.suricata.io/en/suricata-7.0.5/rules/fast-pattern-explained.html [cit. 2024-04-27]

[44] OISF. *Flow Keywords.* In: Suricata Documentation. Online. 2023. Dostupné z: https://docs.suricata.io/en/latest/rules/flow-keywords.html [cit. 2024-04-27]

[45] Greenbone AG. *Using the Greenbone Management Protocol.* In: Greenbone Enterprise Appliance – GOS 22.04.19 Online. 2023. Dostupné z: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/gmp.html [cit. 2024-04-26]

[46] Greenbone AG. *Reports and Vulnerability Management.* In: Greenbone Enterprise Appliance – GOS 22.04.19. Online. 2023. Dostupné z: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/reports.html#reports-and-vulnerability-management [cit. 2024-04-26]

[47] GREENBONE AG. *Greenbone Community Documentation: Workflows.* Online. Greenbone AG, 2021-2024. Dostupné z: https://greenbone.github.io/docs/latest/22.4/container/workflows.html [cit. 2024-04-27]

[48] AttackIQ. *Pyramid of Pain.* Online. San Diego: AttackIQ. 2023. Dostupné z: https://www.attackiq.com/glossary/pyramid-of-pain/ [cit. 2024-04-27]

[49] AttackIQ. *Pyramid of Pain.* Obrázek. In: AttackIQ [online]. San Diego: AttackIQ. 2023. Dostupné z: https://www.attackiq.com/wp-content/uploads/2019/06/blog-pyramid-pain-01-768x432.jpg [cit. 2024-04-27]

[50] PAWAR, Shekhar. *The Power of Collective Intelligence: Leveraging Threat Intelligence to Protect Against Cyber Threats.* EC-Council. Online. 2023. Dostupné z: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/leveraging-threat-intelligence-to-protect-against-cyber-threats/ [cit. 2024-04-26]

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

API	Aplication Programagle Interface
APT	Advanced Persistent Threat
APT	Advanced Package Tool
C2	Command and Control
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DPI	Deep Packet Inspection
EDR	Endpoint Detection and Response
GSM	Greenbone Security Manager
HTTP	Hypertext Transfer Protocol
IaC	Infrastructure as Code
IDS	Intrusion Detection System
IDPS	Intrusion Detection Prevension System
IoC	Indicator of compromise
IP	Internet Protocol
IPS	Intrusion Prevension System
Nmap	Network Mapper
NSE	Nmap Scripting Engine
MISP	Malware Information Sharing Platform
MPLS	Multiprotocol Label Switching
NVD	National Vulnerability Database
NVT	Network Vulnerability Tests
NSM	Network Security Monitoring
OpenVAS	Open Vulnerability Assessment System
OTX	Open Threat Exchange
SIM	Security Information Management
SEM	Security Event Management
SIEM	Security Information and Event Management
SSH	Secure Shell
SPAN	Switch Port Analyzer
TAP	Test Access Point
TI	Threat Intelligence
TLP	Traffic Light Protocol

TTP	Tactics, Technics, Procedures
UEBA	User and Entity Behavior Analytics
VLAN	Virtual Local Area Network
VRF	Virtual routing and forwarding
WEC	Windows Event Collector
WEF	Windows Event Forwarding
XDR	eXtended Detection and Response

SEZNAM OBRÁZKŮ