**Analýza a implementace firewallu a systému NDR pro optimalizaci bezpečnosti počítačové sítě**

**Analysis and implementation of firewall and NDR system to optimize computer network security**

Projekt V

Studijní program: Informatika a kybernetika ve zdravotnictví

Autor práce: Šimon Kochánek

Vedoucí práce: RNDr. Dagmar Brechlerová, Ph.D

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra informačních a komunikačních technologií v lékařství Akademický rok: 2023/2024

**Z a d á n í P r o j e k t V**

Student: **Šimon Kochánek**

Obor: Informatika a kybernetika ve zdravotnictví

Téma: **Analýza a implementace firewallu a systému NDR pro optimalizaci bezpečnosti počítačové sítě**

Téma anglicky: **Analysis and implementation of firewall and NDR system to optimize computer network security**

Z á s a d y p r o v y p r a c o v á n í :

Student zkoumá současné metody a nástroje pro zabezpečení počítačových sítí s hlavním zaměřením na firewall a systémy Network Detection and Response (NDR). Cílem je analyzovat open source řešení a demo verze od vybraných komerčních dodavatelů, porovnat je z hlediska jejich efektivity, výkonu a kompatibility. Na základě zjištěných výsledků student navrhne řešení pro vybudování bezpečného firewallu a systému NDR. Výsledkem bude konkrétní doporučení pro implementaci těchto řešení v praxi.

Seznam odborné literatury:

MARTINÁSEK, Zdeněk. Bezpečnost ICT 2. Přednáška: Problematika logování, systémy IDS a IPS. Brno: Vysoké učení technické v Brně, 2022.

SPAM Titan. Network Segmentation Best Practices to Improve Security. [online] [cit. 23. 10. 2022]. Dostupné z: https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/.

ALDEN, Alexis. Network Segmentation Best Practices. [online] [cit. 23. 10. 2022]. Dostupné z: https://www.dodbuzz.com/network-segmentation-security-best-practices/.

ESET. Co je firewall? [online] [cit. 20. 10. 2022]. Dostupné z: https://www.eset.com/cz/firewall/.

BOUŠKA, Petr. VLAN – Virtual Local Area Network. [online] [cit. 18. 10. 2022]. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/.

Vedoucí: RNDr. Dagmar Brechlerová, Ph.D.

Konzultanti:

V Praze dne 6.11.2023

....................................................

studentka / student

....................................................

vedoucí práce

....................................................

vedoucí / zástupce ved. katedry

**PROHLÁŠENÍ**

Prohlašuji, že jsem práci s názvem „Analýza a implementace firewallu a systému NDR pro optimalizaci bezpečnosti počítačové sítě“ vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kladně 10.1.2024 …...….………...………………...

Šimon Kochánek

**PODĚKOVÁNÍ**

Rád bych vyjádřil upřímné poděkování doktorce Brechlerové za její vedení mého semestrálního projektu. Cením si jejího přístupu, který mi umožnil pracovat na projektu s větší svobodou a bez přísných pravidel. Děkuji jí za vedení a motivaci, které mi pomohly rozvíjet své schopnosti a mé pracovní příležitosti v oblasti kyberbezpečnosti. Její přístup k mému zpracování byl otevřený a konstruktivní, a jsem jí za to velmi vděčný.

**ABSTRAKT**

**Analýza a implementace firewallu a systému NDR pro optimalizaci bezpečnosti počítačové sítě**

V této studii se zaměřujeme na analýzu současných metod a nástrojů pro zabezpečení počítačových sítí, s hlavním důrazem na technologie firewallu a systémů Network Detection and Response (NDR). Hlavním cílem je prozkoumat a porovnat různé open source řešení a demo verze poskytované vybranými komerčními dodavateli. Porovnání bude založeno na kritériích efektivity, výkonu a kompatibility s existujícími systémy. Na základě získaných dat a analýzy student navrhne strategii pro implementaci efektivního a bezpečného firewallu a systému NDR.

**Klíčová slova**

Počítačové sítě, Firewall, Network Detection and Response (NDR), Bezpečnostní analýza

**ABSTRACT**

**Analysis and implementation of firewall and NDR system to optimize computer network security**

In this study, we focus on the analysis of current methods and tools for securing computer networks, with a focus on firewall technologies and Network Detection and Response (NDR) systems. The main objective is to explore and compare different open-source solutions and demos provided by selected commercial vendors. The comparison will be based on the criteria of efficiency, performance, and compatibility with existing systems. Based on the collected data and analysis, the student will propose an optimal strategy for implementing an efficient and secure firewall and NDR system.

**Keywords**

Computer Networks, Firewall, Network Detection and Response (NDR), Security Analysis

Obsah

[Seznam symbolů a zkratek 8](#_Toc158222966)

[1 Úvod 9](#_Toc158222967)

[1.1 Přehled současného stavu 10](#_Toc158222968)

[1.1.1 Od IDS a IPS k NDR: Evoluce detekce a reakce 10](#_Toc158222969)

[1.1.2 Role SOC, SIEM a SOAR 10](#_Toc158222970)

[1.1.3 Napojení systému NDR na SOC,SIEM,SOAR 11](#_Toc158222971)

[1.2 Cíle práce 12](#_Toc158222972)

[2 Metody 13](#_Toc158222973)

[2.1 Současné metody NDR 13](#_Toc158222974)

[2.2 Open-source řešení NDR 14](#_Toc158222975)

[2.3 Komerční řešení NDR 14](#_Toc158222976)

[2.4 Vytváření vlastního prototypu 15](#_Toc158222977)

[2.5 Návrh řešení 16](#_Toc158222978)

[3 Výsledky 17](#_Toc158222979)

[3.1 Srovnání vybraných open-source a komerčních řešení 17](#_Toc158222980)

[3.2 Testování prototypu pro ověření konceptu 17](#_Toc158222981)

[3.3 Navrhnuté řešení 17](#_Toc158222982)

[3.4 Doporučení pro implementaci 17](#_Toc158222983)

[4 Diskuse 19](#_Toc158222984)

[5 Závěr 20](#_Toc158222985)

[Seznam použité literatury 21](#_Toc158222986)

# Seznam symbolů a zkratek

#### Seznam zkratek

|  |  |
| --- | --- |
| Zkratka | Význam |
| NDR | Network Detection and Response (Síťová detekce a reakce) |
| IDS | Intrusion Detection System (Systém pro detekci prolomení) |
| IPS | Intrusion Prevention System(Systém pro prevenci prolomení) |
| SOC | Security Operations Center (Operační středisko) |
| SIEM | Security Information and Event Management (Správa bezpečnostních informací a událostí) |
| SOAR | Security Orchestration Automation and Response (Orchestrace bezpečnosti, automatizace a reakce) |
| ML | Machine Learning (Strojové učení) |
|  |  |

# Úvod

V současné éře digitální transformace je bezpečnost počítačových sítí zásadním pilířem pro udržitelný rozvoj a ochranu informačních aktiv jakékoliv organizace. S neustále se rozšiřujícím spektrem kybernetických hrozeb a rostoucí závislostí na digitální infrastruktuře se bezpečnostní řešení stávají nepostradatelnými pro zajištění integrity, dostupnosti a důvěrnosti citlivých dat. Tento projekt si klade za cíl prozkoumat současné metody a nástroje pro zabezpečení počítačových sítí, přičemž klade důraz na dvě klíčové oblasti: firewally a systémy Network Detection and Response (NDR).

Motivace k tomuto výzkumu vychází z potřeby porozumět a efektivně reagovat na dynamicky se vyvíjející kybernetické hrozby. V dnešní době, kdy organizace čelí stále složitějším a promyšlenějším útokům, je nezbytné mít nejen robustní, ale i adaptabilní bezpečnostní řešení. Projekt se zaměřuje na komparativní analýzu různých typů firewallů a NDR systémů, včetně open source řešení a demo verzí od vybraných komerčních dodavatelů.

Hloubkové porovnání a analýza těchto technologií umožní identifikovat klíčové faktory, které by měly být zohledněny při výběru bezpečnostního řešení pro organizace. Výsledkem této práce bude sada doporučení pro implementaci těchto technologií, která by měla pomoci organizacím zvýšit jejich schopnost odolávat proti kybernetickým hrozbám a zároveň udržet flexibilitu a škálovatelnost jejich bezpečnostních systémů.

Tento projekt by mohl přispět k lepšímu pochopení současných bezpečnostních výzev a nabídne praktické návrhy pro zlepšení bezpečnostních opatření v oblasti počítačových sítí, což je nesmírně důležité pro zachování důvěry a ochrany v digitálně propojeném světě.

## Přehled současného stavu

### Od IDS a IPS k NDR: Evoluce detekce a reakce

V počátcích zabezpečení počítačových sítí se spoléhalo převážně na Intrusion Detection Systems (IDS), které monitorovaly síťový provoz za účelem identifikace podezřelých aktivit. IDS byly neocenitelné pro jejich schopnost upozornit na potenciální hrozby, ale byla jasná jejich omezení – nedokázaly zabránit útoku. To vedlo k vývoji Intrusion Prevention Systems (IPS), které nejen detekovaly hrozby, ale také byly schopny aktivně zasáhnout a blokovat škodlivý provoz před tím, než by mohl způsobit škodu.

S nárůstem sofistikovanosti a objemu kybernetických hrozeb vznikla poptávka po dynamickém přístupu. Zde přichází na scénu Network Detection and Response (NDR). NDR umožňuje nejen detekovat a reagovat na hrozby v reálném čase, ale také poskytuje pokročilé analytické nástroje pro hloubkovou analýzu síťového provozu. NDR se stalo klíčovým prvkem v naší obraně, nabízející komplexní pohled na bezpečnostní situaci a umožňující adaptivní reakci na neustále se vyvíjející hrozby.

### Role SOC, SIEM a SOAR

V současném bezpečnostním ekosystému hrají klíčovou roli tři hlavní prvky: Security Operations Center (SOC), Security Information and Event Management (SIEM) a Security Orchestration, Automation and Response (SOAR).

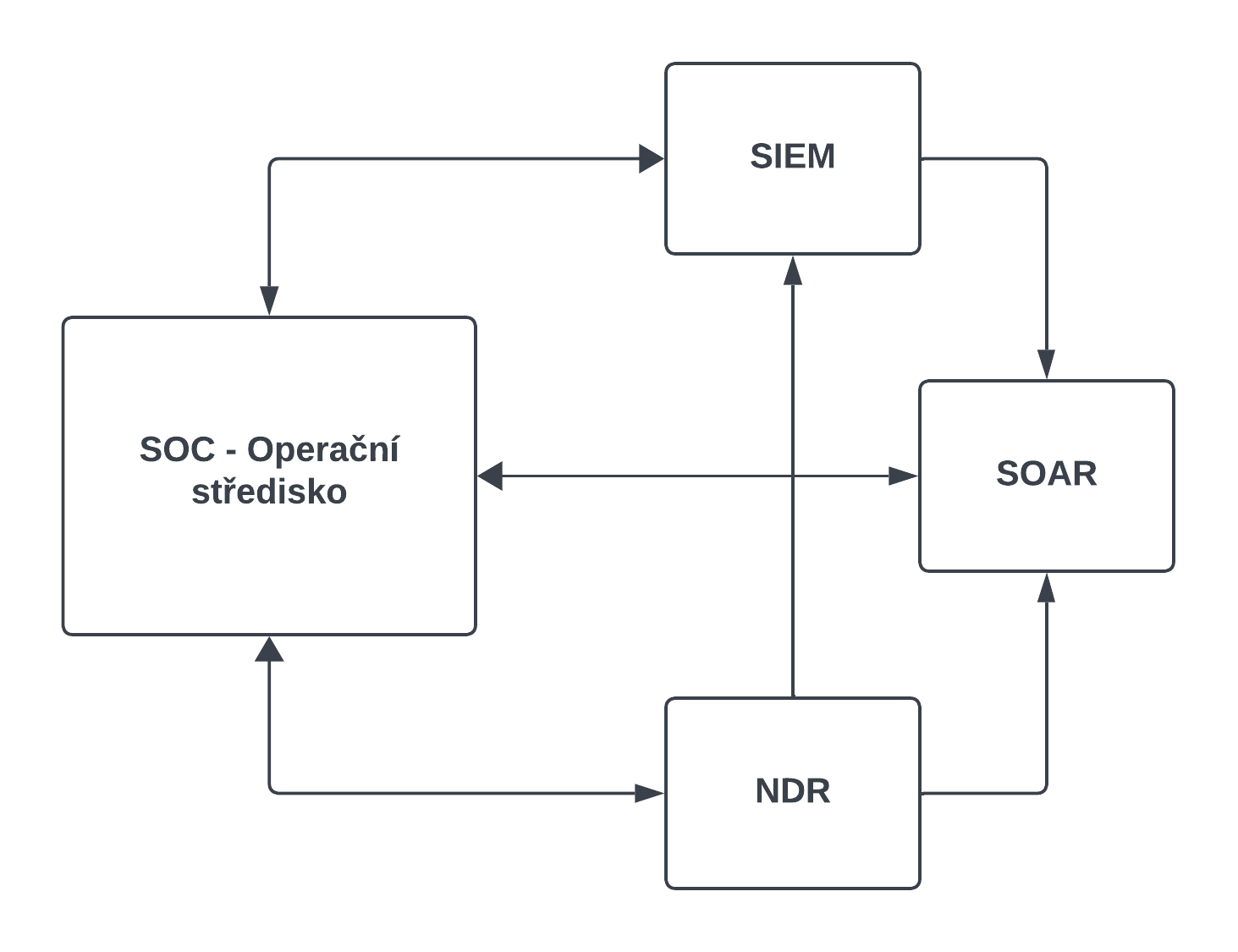
SOC představuje centrální místo pro monitorování a reakci na bezpečnostní incidenty, kde analytici využívají širokou škálu nástrojů a informací k detekci a řešení hrozeb v reálném čase.

SIEM systémy tvoří základ pro shromažďování, normalizaci a analýzu logů a událostí z celé sítě. Díky tomu je možné rychle identifikovat neobvyklé chování nebo potenciální bezpečnostní incidenty. SIEM také poskytuje cenné informace pro SOC, které pomáhají při rozhodovacím procesu a zvyšují celkovou efektivitu monitorování a reakce na incidenty.

SOAR přináší další dimenzi automatizace a koordinace do procesů řešení incidentů. Integrací s nástroji jako NDR a SIEM, SOAR umožňuje automatické provádění bezpečnostních operací, jako je blokování IP adres, izolace infikovaných systémů nebo aplikace bezpečnostních záplat. Tím se výrazně snižuje čas potřebný k reakci na incidenty a zvyšuje se celková obranyschopnost organizace proti kybernetickým hrozbám.

### Napojení systému NDR na SOC,SIEM,SOAR

Blokové schéma zapojení těchto čtyř prvků může vypadat takto:



A diagram of a company

Description automatically generated

**Obr. 1.1:** Blokové schéma zapojení NDR na systémy SOC,SIEM,SOAR. Model: autor.

NDR poskytuje detailní analýzu síťového provozu a detekci hrozeb, které jsou následně předány do SIEMu, který agreguje a analyzuje data z NDR a dalších zdrojů, identifikuje bezpečnostní incidenty a poskytuje komplexní pohled na bezpečnostní situaci.

SOAR je na SIEM napojen tak, že využívá jeho analýzy a upozornění k automatizaci reakcí na incidenty. Pomocí předdefinovaných procesů SOAR rychle reaguje na hrozby identifikované SIEM, což zahrnuje izolaci postižených systémů nebo blokování škodlivého provozu.

Obě tyto komponenty, SIEM a SOAR, jsou integrovány do SOC, který slouží jako operační centrum pro monitorování, analýzu a reakci na bezpečnostní incidenty. SOC využívá data a upozornění z SIEM a automatizované reakce z SOAR k efektivnímu řízení a mitigaci bezpečnostních hrozeb.

## Cíle práce

Hlavním cílem této práce je provést analýzu současných metod Network Detection and Response (NDR) a navrhnout řešení pro NDR a firewally, které bude vhodné pro implementaci v reálném prostředí. K tomuto řešení také přidám sadu doporučení pro tuto implementaci. Pro splnění hlavního cíle byly stanoveny následující konkrétní úkoly:

Prozkoumat současné metody NDR: Tento podcíl zahrnuje detailní průzkum a zhodnocení stávajících metod NDR. Zaměříme se na jejich funkčnost, efektivitu a schopnost reagovat na nejnovější kybernetické hrozby. Cílem je poskytnout komplexní přehled současného stavu technologií NDR.

Analyzovat Open Source řešení NDR: Zde se zaměříme na detailní prozkoumání dostupných open source NDR řešení. Analyzovat budeme jejich výhody, nevýhody, možnosti implementace a efektivitu v porovnání s komerčními produkty.

Analyzovat komerční řešení: Tento podcíl se věnuje detailní analýze komerčně dostupných NDR řešení. Budeme hodnotit jejich funkčnost, výkonnost, kompatibilitu s existujícími systémy a celkovou efektivitu.

Porovnat Open-source a komerční řešení: Udělat tabulku porovnání rozdílů a slovně zhodnotit každé odůvodnění.

Vytvořit prototyp: Pro lepší pochopení ohledně návrhu řešení je potřeba si vytvořit prototyp, který naimplementuji v počítačové síti abych udělal tzv. PoC – Proof of Concept – ověření konceptu.

Navrhnout řešení pro NDR a firewall: Na základě získaných poznatků z analýzy a testování prototypu navrhneme konfiguraci NDR a firewallu, která bude reflektovat aktuální bezpečnostní požadavky a trendů.

Konkrétní doporučení pro implementaci: Výstupem práce bude sada konkrétních doporučení pro implementaci navrženého řešení NDR a firewallu v reálném provozu. Tato doporučení budou sloužit jako průvodce pro organizace, které hledají efektivní a bezpečné řešení pro zabezpečení svých sítí.

# Metody

## Současné metody NDR

Network Detection and Response (NDR) je klíčový koncept v oblasti kybernetické bezpečnosti, zaměřující se na identifikaci a reakci na neoprávněné či podezřelé aktivity v síťovém provozu. NDR kombinuje různé technologie a postupy, aby poskytovalo komplexní pohled na síťovou bezpečnost a umožňovalo rychlou reakci na potenciální hrozby. V praxi NDR funguje jako pokročilý systém detekce, který analyzuje síťový provoz a používá algoritmy strojového učení a chování založené na analýze pro identifikaci anomálií, které mohou signalizovat útok. Například, pokud dojde k podezřelému nárůstu síťového provozu nebo pokud systém detekuje nesrovnalosti ve způsobu, jakým jsou data posílána nebo přijímána, NDR toto vyhodnotí jako potenciální hrozbu.

Jedním z reálných příkladů použití NDR je detekce a reakce na pokročilé trvalé hrozby (APT). APT útoky jsou sofistikované a cílené, často zaměřené na dlouhodobou infiltraci sítě. NDR systém může detekovat neobvyklé vzorce komunikace nebo neautorizovaný přístup k citlivým datům, což umožňuje organizacím rychle reagovat a minimalizovat škody.

Dalším příkladem je odhalení škodlivého softwaru, který se pokouší o komunikaci s řídícím serverem. Tradiční bezpečnostní řešení možná takový provoz nezachytí, zatímco NDR by identifikovalo neobvyklou komunikaci jako podezřelou a upozornilo by na ni. Současně s detekcí hrozeb NDR systémy poskytují i podrobné informace, které pomáhají bezpečnostním týmům lépe porozumět povaze útoku. Tato data mohou zahrnovat časové údaje, geografické umístění, typy a objemy přenesených dat a další relevantní informace. Díky tomu je možné nejen rychle reagovat na bezprostřední hrozby, ale také lépe pochopit a předvídat budoucí útoky a vyvíjet účinnější obranné strategie.

## Open-source řešení NDR

V rámci mého projektu jsem se věnoval důkladnému zkoumání open-source řešení NDR. Open-source nástroje poskytují flexibilní a často finančně výhodnější alternativu k tradičním komerčním systémům. Klíčovým aspektem mého zkoumání bylo hodnocení, jak efektivně tyto nástroje identifikují a reagují na bezpečnostní hrozby, a jak dobře se integrují do existujících síťových a bezpečnostních infrastruktur.

Jedním z hlavních kroků bylo testování několika open-source NDR systémů. Zaměřil jsem se na jejich schopnost detekovat neautorizované přístupy, anomální síťový provoz. Při testování jsem simuloval různé druhy síťových útoků, včetně DoS útoků, skenování sítě a šíření malware, abych zhodnotil, jak rychle a přesně systémy reagují.

Důležitým aspektem bylo také hodnocení uživatelského rozhraní a správy těchto systémů. U open-source řešení je často výzvou jejich konfigurace a správa, protože mohou postrádat uživatelsky přívětivé rozhraní nebo podrobnou dokumentaci. Součástí mého hodnocení byla proto analýza dostupnosti podpůrných materiálů a komunity, která stojí za jednotlivými nástroji.

Dalším důležitým faktorem byla schopnost těchto řešení integrovat se s dalšími bezpečnostními nástroji, jako jsou firewally. Tato integrace je klíčová pro vytváření komplexního bezpečnostního řešení. Finální výběr se skládal z dvou nástrojů a to:Suricata[6]a Zeek[7]

Tyto nástroje společně zajistí funkcionalitu NDR. Jejich hodnocení uvedu ve výsledcích.

## Komerční řešení NDR

Po prozkoumání open-source řešení jsem se obrátil k výběru komerčních NDR produktů. Tyto produkty obvykle poskytují širší podporu, uživatelsky přívětivější rozhraní a pokročilé funkce, což představuje významný přínos pro organizace. Soustředil jsem se na analýzu vedoucích komerčních NDR nástrojů s dostupnými demo verzemi, abych mohl co nejvíce otestovat jejich funkcionalitu.

V průběhu testování jsem hodnotil, jak dobře tyto systémy detekují a reagují na různé typy kybernetických hrozeb. Zvláštní pozornost jsem věnoval jejich schopnosti identifikovat sofistikované útoky, jako jsou APT (Advanced Persistent Threats) nebo nulové dny (zero-day exploits). Kromě technického hodnocení jsem také zvažoval snadnost implementace a integrace těchto systémů do stávajících IT infrastruktur.

Jednou z významných výhod komerčních řešení, kterou jsem identifikoval, je jejich schopnost poskytovat podrobné analýzy a reporty, které pomáhají bezpečnostním týmům lépe porozumět a reagovat na bezpečnostní incidenty.

Přestože komerční řešení mohou nabízet větší pohodlí a pokročilé funkce, je důležité zvážit také jejich náklady. Velkou proměnnou je také finanční stránka. Cena licencí a podpory může být výrazně vyšší a při plné funkcionalitě to mohou být pro malé společnosti astronomické částky. Proto vyžadují komerční řešení více času a zvážení nejlepší varianty. Nakonec mi kvůli funkcionalitě a přístupnosti dema vypadl jako finalista Fortinet se svým FortiNDR[8].

## Vytváření vlastního prototypu

Pro validaci funkčnosti mého řešení jsem vyvinul prototyp a zřídil testovací prostředí. Využil jsem Mikrotik router, model RB750Gr3, k zřízení monitorovacího portu, který mi umožnil sledovat veškerý provoz procházející routerem.

Nejprve jsem si pomocí Wiresharku otestoval, zda monitorovací port (SPAN port) na Mikrotik routeru správně předává veškeré pakety na síťový port mého Linuxového počítače. Po potvrzení, že přenos paketů funguje bez problémů, jsem na počítači nainstaloval Suricatu a Zeek dle jejich dokumentace. Následně jsem tyto nástroje připojil k monitorovacímu portu na Mikrotik routeru a začal pracovat na nastavení a logování dat z NDR systému.

Poté, co jsem ověřil funkčnost monitorovacího portu (SPAN portu) na Mikrotik routeru pomocí Wiresharku a nainstaloval Suricatu a Zeek, jsem provedl sérii testovacích útoků přes router. Začal jsem s DoS útoky, při kterých můj NDR systém okamžitě identifikoval podezřelé SYN FLOOD alerty pocházející z IP adresy útočníka. Následně jsem testoval opakované neoprávněné přístupy, které systém rovněž úspěšně detekoval.

Pokračoval jsem pokusy o proniknutí pomocí různých exploitů a skenovacích technik, abych ověřil, jak dobře dokáže NDR systém identifikovat a reagovat na rozmanité hrozby. Výsledky byly povzbudivé – Suricata a Zeek spolehlivě rozpoznávaly pokusy o využití zranitelností a neobvyklé skenovací aktivity, což mi poskytlo cenné informace pro další ladění bezpečnostních pravidel.

## Návrh řešení

Po důkladném testování prototypu jsem dospěl k závěru, že finální verze našeho NDR řešení by měla být založena na kombinaci softwarů Suricata a Zeek. Tento výběr je motivován především snadností implementace, která mi umožní rychle a efektivně nasadit systém v naší síti. Suricata a Zeek se ukázaly jako mimořádně flexibilní a konfigurovatelné nástroje, což mi dává možnost přizpůsobit bezpečnostní opatření specifickým potřebám naší organizace.

Kromě toho hraje významnou roli také finanční aspekt. Oba tyto nástroje jsou dostupné jako open-source, což znamená, že nejsou spojeny s licenčními poplatky typickými pro komerční bezpečnostní řešení. Tato skutečnost představuje významnou úsporu nákladů, aniž bychom museli dělat kompromisy v kvalitě nebo efektivitě detekce a reakce na hrozby. Efektivní využití těchto nástrojů také umožňuje alokovat finanční prostředky na další důležité bezpečnostní iniciativy a technologie.

Dalším klíčovým faktorem pro výběr Suricata a Zeek je jejich schopnost integrace s existujícími systémy a technologiemi. Díky otevřené architektuře těchto nástrojů můžu snadno zajistit jejich propojení s ostatními komponenty naší bezpečnostní infrastruktury, jako jsou SIEM a SOAR platformy, což zvyšuje celkovou sílu a soudržnost našeho bezpečnostního ekosystému.

# Výsledky

## Srovnání vybraných open-source a komerčních řešení

Tabulka 3.1 představuje srovnání mezi komerčním řešením NDR, zastoupeným produktem FortiNDR, a open-source řešením, kombinací Suricata a Zeek.

Komerční produkt FortiNDR vyniká pokročilými algoritmy pro detekci hrozeb, což mu umožňuje identifikovat minimálně 95% potenciálních hrozeb. To je výsledek vývoje a investic do výzkumu, které komerční produkty často podstupují. Kapacitní možnosti FortiNDR jsou rovněž významné, s možností zpracovat až 100 Gbps, což umožňuje jeho nasazení ve velkých a náročných síťových prostředích. Tento produkt je optimalizován pro integraci s dalšími produkty Fortinet, což zjednodušuje jeho začlenění do stávajících infrastruktur. Jeho intuitivní rozhraní a jednoduché nasazení do stávající infrastruktury jsou reflektovány ve vysokých nákladech na pořízení a provoz.

Na druhé straně, open-source řešení zastoupené kombinací Suricata a Zeek nabízí vysokou přizpůsobitelnost s efektivitou detekce hrozeb až 90%. Ačkoliv má nižší kapacitní možnosti ve srovnání s FortiNDR, jeho schopnost zpracovat až 10 Gbps stále pokrývá potřeby mnoha organizací. Velkou výhodou je široká kompatibilita s různými nástroji a systémy, což umožňuje jeho efektivní integraci do různorodých prostředí. Složitější ovládání je vynahrazeno vysokou mírou rozšířitelnosti díky otevřené architektuře, což dává uživatelům možnost upravit systém podle svých specifických potřeb. Přestože náklady na pořízení jsou nulové, je třeba zvážit potenciální výdaje na hardware nebo technickou podporu. Ještě je důležité říci že Suricata zvládá hlavně známé hrozby a rychleji je schopná na ně reagovat. Má také větší podporu pro formáty reputačních databází. Oproti tomu Zeek má sofitstikované algoritmy na rozpoznávání anomálií a neznámých hrozeb a je schopen dávat kvalitní data o bezpečnostních hrozbách a jejich mitigacích.

Díky tomuto porovnání jsem si pro závěrečné řešení vybral open-source možnost.

**Tabulka. 3.1:** Porovnání komerčního a open-source NDR řešení

|  |  |  |
| --- | --- | --- |
| **Kritérium** | **FortiNDR** | **Suricata + Zeek** |
| **Detekce hrozeb (%)** | Pokročilejší algoritmy než u open-source zajišťují minimálně 95% | Přizpůsobitelnost umožňuje efektivitu až 90% |
| **Kapacitní možnosti** | Zpracuje až 100 Gbps | Zpracuje až 10 Gbps |
| **Kompatibilita** | Optimální s produkty Fortinet | Široká kompatibilita s různými nástroji |
| **Uživatelská přívětivost** | Intuitivní rozhraní | Složitější ovládácí prvky |
| **Rozšířitelnost** | Možná jen v rámci Fortinet ekosystému | Open-source architektura poskytuje vysokou flexibilitu |
| **Náklady** | Vysoké v řádech stovek tisíc českých korun | Nulové, pokud nepotřebujeme hardware nebo technickou podporu |

## Navrhnuté řešení

Zde je rozplánováno na fáze jak velmi abstraktně udělat řešení NDR pro menší organizaci. Je nutno brát zřetel na požadavky každé organizace a podle těch se řídit, např jestli je to organizaci s vysokou pravděpodobností vnitřní kompromitace tak aplikovat více NDR serverů na segmenty sítě atd.

**Fáze 1: Příprava a Plánování**

Analýza sítě: Nejprve provedeme důkladnou analýzu stávající síťové infrastruktury organizace, abychom pochopili její specifika, včetně mapování všech připojených zařízení a služeb.

Výběr hardwaru: Pro Suricata a Zeek vybereme dedikovaný hardwarový server s dostatečným výpočetním výkonem a síťovou propustností. Doporučujeme server s minimálně 4 CPU jádry, 16 GB RAM a gigabitovou síťovou kartou.

Definice bezpečnostní politiky: Stanovíme bezpečnostní politiku, která bude reflektovat potřeby organizace a zajistí správnou konfiguraci detekčních pravidel Suricata a Zeek.

**Fáze 2: Implementace**

Instalace a konfigurace: Suricata a Zeek budou nainstalovány na předem vybraném serveru. Nakonfigurujeme je tak, aby přijímali všechny informace z předem zmíněné síťové karty.

Nastavení monitorovacího portu: Na hlavním síťovém zařízení (např. switchi) nastavíme port mirroring (SPAN), aby kopíroval veškerý provoz na port, kde bude připojen server s Suricata a Zeek.

Ladění a pravidla: Optimalizujeme výkon Suricata a Zeek pro prostředí organizace a definujeme specifická detekční pravidla zaměřená na nejčastější hrozby relevantní pro organizaci.

**Fáze 3: Testování a Ladění**

Validační testy: Provedeme sérii testů pro ověření, že Suricata a Zeek správně detekují testovací hrozby a útoky, a že jsou schopny generovat upozornění a logy.

Ladění konfigurace: Na základě výsledků testů upravíme a zmírníme konfiguraci a pravidla pro maximalizaci efektivity a minimalizaci falešných pozitivů.

**Fáze 4: Nasazení a Monitorování**

Uvedení do provozu: Po úspěšném testování a ladění bude systém uveden do plného provozu.

Připojení NDR řešení na firewally a routery: Naše NDR musí mít přístup posílat své bezpečnostní politiky na perimetr firewally a další routery a firewally v síti. Tuto možnost je důležité ověřit a případně zprovoznit.

Průběžné monitorování: Zavedeme procesy pro průběžné monitorování výstrah a logů generovaných Suricata a Zeek, abychom zajistili, že jakékoli bezpečnostní incidenty budou rychle identifikovány a řešeny.

Případné další napojení na další systémy: Pokud bude mít naše organizace takovou možnost tak můžeme

Tímto způsobem může malá organizace efektivně implementovat Suricata a Zeek jako robustní NDR řešení, které posílí její obranu proti kybernetickým hrozbám a zvýší celkovou bezpečnost její počítačové sítě.

## Doporučení pro implementaci

Na základě navrhnutého řešení pro implementaci NDR systému pomocí Suricata a Zeek v malé organizaci, je zde několik doporučení, která mohou pomoci zefektivnit proces implementace a zvýšit celkovou bezpečnostní odolnost organizace:

**Komplexní analýza rizik:** Nezbytný krok před zahájením jakékoliv implementace. Je důležité detailně posoudit potenciální hrozby a zranitelnosti specifické pro danou organizaci. Z této analýzy pak vyplývají klíčové oblasti, které vyžadují zvýšenou pozornost v rámci monitorování a ochrany. Součástí tohoto procesu je také neustálé zajištění základních principů kybernetické bezpečnosti: důvěrnosti (Confidentiality), integrity (Integrity) a dostupnosti (Availability)

**Segmentace sítě**: V případě, že analýza odhalí vysokou pravděpodobnost vnitřní kompromitace, doporučuje se aplikovat segmentaci sítě. Pro každý segment sítě může být nainstalován samostatný NDR server, což umožňuje detailnější monitorování a rychlejší identifikaci hrozeb v rámci specifických částí sítě.

**Důkladné testování**: Než bude systém plně nasazen, je nezbytné provést důkladné testování všech aspektů řešení, včetně detekčních schopností, výkonu při zpracování velkého množství dat a integrace s existujícími bezpečnostními zařízeními, jako jsou firewally a routery. Testování by mělo zahrnovat simulované útoky a reálné provozní scénáře.

**Průběžné školení**: Zabezpečení je dynamický proces, a proto je důležité pravidelně školit personál na nejnovější hrozby a nejlepší postupy pro reakci na incidenty. To zahrnuje nejen technický personál, ale i koncové uživatele, kteří mohou hrát klíčovou roli v detekci a prevenci útoků.

**Integrace s dalšími bezpečnostními systémy**: Pokud to infrastruktura a rozpočet dovolí, zvažte další integraci NDR řešení s pokročilými bezpečnostními technologiemi, jako jsou SIEM a SOAR systémy. Tato integrace může zvýšit automatizaci, zjednodušit reakce na incidenty a poskytnout komplexnější pohled na bezpečnostní stav sítě.

Implementace NDR řešení pomocí Suricata a Zeek může významně přispět k posílení kybernetické obrany malé organizace. Klíčem k úspěchu je pečlivé plánování, důkladné testování a průběžné zdokonalování procesů a technologií.

# Diskuse

V diskuzi našich výsledků je důležité zdůraznit, že výběr mezi open-source a komerčními NDR řešeními není jen otázkou finančních nákladů, ale také specifických potřeb a kapacit organizace. Z našeho srovnání vyplývá, že komerční řešení jako FortiNDR nabízí robustní a uživatelsky přívětivé řešení s vysokou efektivitou detekce hrozeb a schopností zpracování velkého objemu dat. Toto je výhodné pro organizace, které hledají "out-of-the-box" řešení s minimální potřebou konfigurace a údržby. Na druhou stranu, Suricata a Zeek jako open-source nástroje poskytují větší flexibilitu a možnost přizpůsobení, což je zásadní pro organizace s omezenými rozpočty nebo speciálními požadavky na bezpečnost.

Jedním z omezení této práce je nedostatek empirických dat o dlouhodobé efektivitě navrhovaných řešení v různorodých provozních prostředích. Dalším krokem by tedy mělo být provádění rozsáhlých testů v reálných podmínkách, aby se ověřila adaptabilita a udržitelnost navrhovaných konfigurací v praxi.

# Závěr

V této práci jsme úspěšně analyzovali současné metody Network Detection and Response (NDR), porovnali open-source a komerční řešení a navrhli přizpůsobené NDR a firewall řešení pro malou organizaci, doprovázené sadou doporučení pro implementaci. Naše zjištění ukázala, že i přes určité výzvy v detekci neznámých hrozeb, open-source nástroje jako Suricata a Zeek nabízejí významnou flexibilitu a přizpůsobitelnost, které jsou zásadní pro efektivní ochranu v dynamickém kybernetickém prostředí. Navzdory splnění klíčových cílů práce jsme narazili na omezení, která naznačují potřebu dalšího výzkumu a vývoje pro zlepšení NDR systémů. Tato práce tak představuje pevný základ pro budoucí inovace v kybernetické bezpečnosti, s důrazem na rozvoj strategií pro boj proti pokročilým a neznámým kybernetickým hrozbám.

# Seznam použité literatury

[1] MARTINÁSEK, Zdeněk. Bezpečnost ICT 2. Přednáška: Problematika logování, systémy IDS a IPS. Brno: Vysoké učení technické v Brně, 2022.

[2] SPAM Titan. Network Segmentation Best Practices to Improve Security. [online] [cit. 23. 10. 2022]. Dostupné z: https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/.

[3] ALDEN, Alexis. Network Segmentation Best Practices. [online] [cit. 23. 10. 2022]. Dostupné z: https://www.dodbuzz.com/network-segmentation-security-best-practices/.

[4] ESET. Co je firewall? [online] [cit. 20. 10. 2022]. Dostupné z: https://www.eset.com/cz/firewall/.

[5] BOUŠKA, Petr. VLAN – Virtual Local Area Network. [online] [cit. 18. 10. 2022]. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/.

[6] Suricata. Online. © 2024 OISF. Dostupné z: <https://suricata.io/>. [cit. 2024-02-07].

[7] *Zeek*. Online. © 2020 The Zeek Project. Dostupné z: <https://zeek.org/>. [cit. 2024-02-07].

[8] *Fortinet - FortiNDR*. Online. © 2024 Fortinet, Inc. Dostupné z: [https://www.fortinet.com/products/netw ork-detection-and-response](https://www.fortinet.com/products/netw%20ork-detection-and-response). [cit. 2024-02-07].