**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](#_Toc158184809)

[1 Úvod 9](#_Toc158184810)

[1.1 Přehled současného stavu 10](#_Toc158184811)

[1.1.1 Od IDS a IPS k NDR: Evoluce detekce a reakce 10](#_Toc158184812)

[1.1.2 Role SOC, SIEM a SOAR 10](#_Toc158184813)

[1.1.3 Napojení systému NDR na SOC,SIEM,SOAR 11](#_Toc158184814)

[1.2 Cíle práce 12](#_Toc158184815)

[2 Metody 13](#_Toc158184816)

[2.1 Současné metody NDR 13](#_Toc158184817)

[2.2 Open-source řešení NDR 14](#_Toc158184818)

[2.3 Komerční řešení NDR 15](#_Toc158184819)

[2.4 Vytváření vlastního prototypu 16](#_Toc158184820)

[2.5 Návrh řešení 16](#_Toc158184821)

[2.6 Doporučení pro implementaci 16](#_Toc158184822)

[3 Výsledky 18](#_Toc158184823)

[4 Diskuse 20](#_Toc158184824)

[5 Závěr 21](#_Toc158184825)

[Seznam použité literatury 22](#_Toc158184826)

# 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) |
|  |  |

# 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).

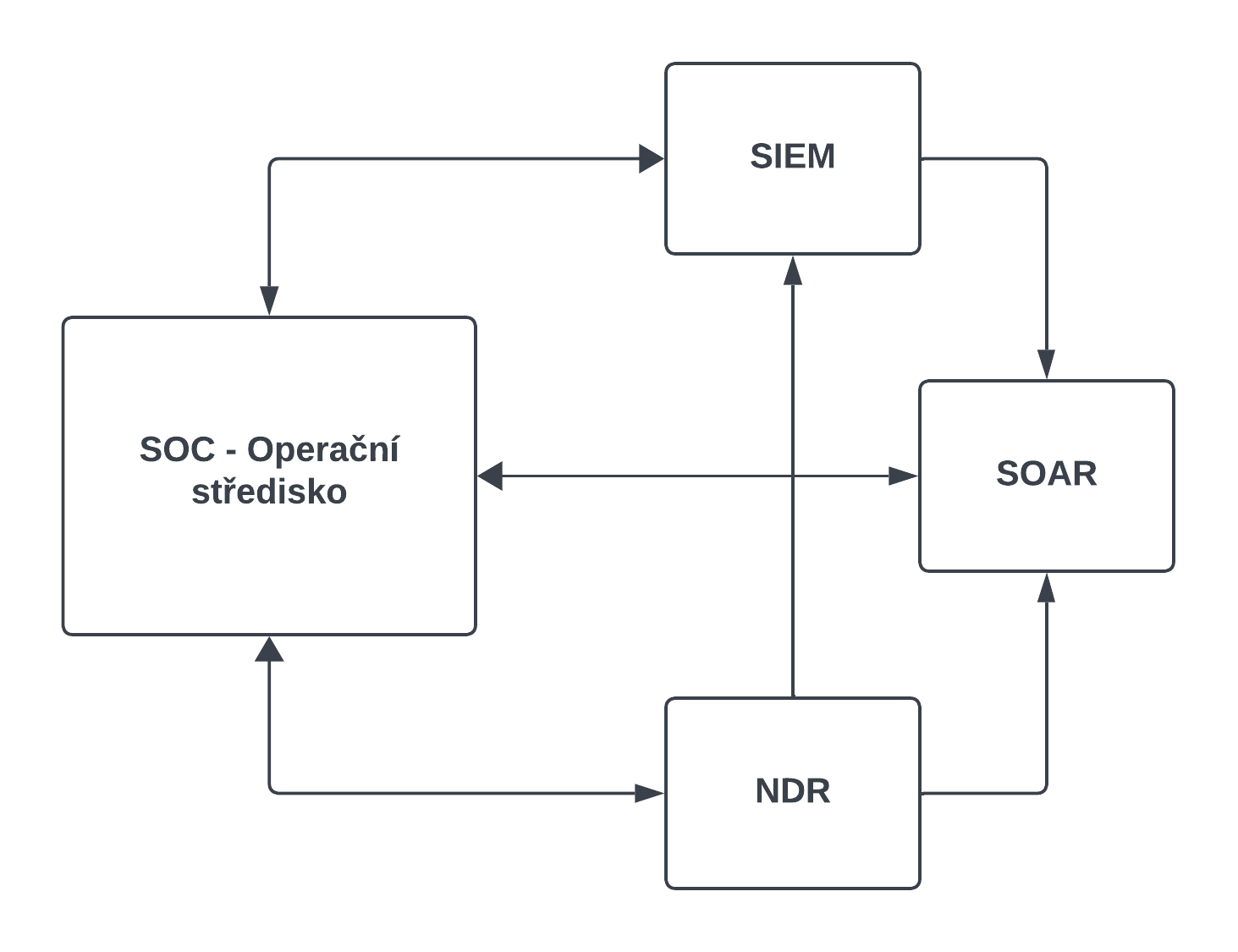
SOC představuje centrální místo pro monitorování a reakci na bezpečnostní incidenty, kde analytici využívají širokou škálu nástrojů a informací k detekci a řešení hrozeb v reálném čase.

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 naimplementuju 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 snaží komunikovat 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 ověření funkcionality mého řešení jsem si vytvořil prototyp a testovací prostředí. Pomocí routeru značky Mikrotik modelu RB750Gr3 jsem vytvořil monitorovací port abych na něj mohl připojit NDR řešení. Tento port mi dávál veškerou komunikaci která přes router prošla.

## Návrh řešení

Na základě získaných informací a poznatků z předchozích částí bude vypracován návrh řešení pro NDR a firewall. Tento proces zahrnuje integraci nejlepších prvků z open-source, komerčních řešení a vlastního prototypu. Zaměříme se na vytvoření modelu, který bude schopen efektivně detekovat a reagovat na kybernetické hrozby, zatímco zůstane flexibilní a škálovatelný pro různé organizační potřeby. Bude kladen důraz na praktickou aplikovatelnost, snadnou implementaci a údržbu tohoto řešení.

## Doporučení pro implementaci

Poslední část se věnuje formulaci konkrétních doporučení pro implementaci navrženého řešení v reálných podmínkách. Zde budou popsány postupy a kroky potřebné pro úspěšné nasazení, konfiguraci a správu NDR a firewall systémů. Dále se zaměříme na vytvoření plánu pro pravidelné aktualizace, monitorování a hodnocení výkonnosti systému. Tato část bude obsahovat také směrnice pro měření účinnosti a návratnosti investice po implementaci.

# Výsledky

## Srovnání vybraných open-source a komerčních řešení

## Testování prototypu pro ověření konceptu

## Navrhnuté řešení

## Doporučení pro implementaci

Věnujte kapitolu pouze přehlednému podání výsledků, nikoliv jejich diskusi. Data uvádějte zejména v grafech a tabulkách. Preferovány jsou grafy – tabulky se všemi naměřenými hodnotami, ze kterých grafy vycházejí, lze umístit do příloh práce.

Výsledky mají vždy obsahovat hlavní text, který zasadí prezentované obrázky a tabulky do souvislosti s předchozím textem a čtenáře prezentovanými daty provede. Prezentování výsledků ve formě nekomentovaného obrázkového alba je v drtivé většině případů nevhodné.

Na každý obrázek musí být uveden odkaz v textu, který má formát jako v následující větě. Obrázek se vždy čísluje a popisuje pod obrázkem, viz příklad na Obr. 3.1.



**Obr. 3.1:** Tulipány před ozářením kryptonitem. Fotografie: autor.

Obrázky číslujte podle hlavní kapitoly, ve které se vyskytují. Podkapitoly se již neuvažují. To znamená, že obrázky v úvodu (typicky kap. 1) budou: Obr. 1.1, Obr. 1.2 atd. V metodách (typicky druhá velká kapitola) budou číslovány Obr. 2.1, Obr. 2.2, Obr. 2.3 atd.

Popis tabulky, na rozdíl od obrázku, je zpravidla nad tabulkou, viz Tabulka 3.1. Není nutné v něm opisovat celý obsah záhlaví tabulky, které následuje hned vzápětí. Jednotlivé proměnné v tabulce jsou řazeny do sloupců. V tabulce jsou nezávislé proměnné, kategorie probandů apod. řazeny vlevo, závislé proměnné vpravo. Jednotky uvádějte v kulatých závorkách v záhlaví tabulky, ne u každého čísla zvlášť. Vysvětlující poznámky (např. dosažená hladina významnosti, zda jsou data udávána jako průměr + směrodatná chyba průměru, jaký statistický test byl použit apod.) jsou umisťovány pod tabulku a odkaz na ně se udává jako horní index (symboly, čísla, písmena) na příslušném místě tabulky. Na každý obrázek a tabulku je třeba odkazovat z hlavního textu.

**Tabulka 3.1:** Reakční čas *T*20 signálu periferní saturace kyslíkem, *Sp*O2, měřený třemi různými přístroji.

|  |  |  |  |
| --- | --- | --- | --- |
|  | *T*20 (s) | | |
| Fáze | Root Radical-7 | Nellcor N-600 | Carescape B650 |
| Hypoxická | 52±15\* | 65±19\* | 56±15 |
| Hyperoxická | 43±14 | 55±28 | 49±15 |
| Hyperkapnická | 75±23 | 119±47# | 73±41# |

Data byla měřena pro shodnou skupinu 14 probandů a jsou uvedena jako aritmetický průměr ± směrodatná odchylka. Symboly \* a # značí statisticky významný rozdíl (*p*<0,05) časů pro shodnou fázi.

# Diskuse

V této části shrňte získané výsledky (hlavní zjištění práce) a následně tyto výsledky interpretujte s ohledem na cíle práce. Lze též získané výsledky a výstupy konfrontovat s výsledky a výstupy jiných autorů, výrobky jiných společností apod. Nezbytné je správné uvádění zdrojů (citace prací, které jsou zde porovnávány a diskutovány). Diskutují se rovněž limitace práce. Nakonec lze nastínit další směřování práce do budoucna, opatrně spekulovat o klinickém významu práce apod.

# Závěr

Závěr stručně shrnuje splnění vytyčených cílů práce.

Shrnutí splněných (nebo snad v menší míře nesplněných) cílů práce navazuje na úvod práce. Z dalších částí práce (metody, výsledky a diskuse) je přebíráno jen to nejpodstatnější a v minimální nutné míře – závěr práce nemá být zopakováním abstraktu, výsledků nebo diskuse. Konec závěru může obsahovat podložené spekulace o významu práce do budoucna nebo výrazná doporučení pro další výzkum nebo praxi, pokud z výsledků předkládané práce přímo vyplývají.

# 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].