VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

VYUŽITÍ FUZZY LOGIKY PRO VÝBĚR VHODNÉHO SYSTÉMU SIEM V PODNIKU

USING FUZZY LOGIC TO SELECT A SUITABLE SIEM SYSTEM IN A COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Tomáš Kilián**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. et Ing. Zuzana Janková, Ph.D.**
SUPERVISOR

BRNO 2025

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Tomáš Kilián**
Vedoucí práce:	**Ing. et Ing. Zuzana Janková, Ph.D.**
Akademický rok:	2024/25
Studijní program:	Informační management

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

Využití fuzzy logiky pro výběr vhodného systému SIEM v podniku

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Diplomová práce se zabývá využitím fuzzy logiky pro vyhodnocování systémů pro správu bezpečnostních informací a událostí. Řešení bude využívat programové prostředí MATLAB.

Základní literární prameny:

DOSTÁL, Petr, 2011. Advanced decision making in business and public services. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-747-5.

JURA, Pavel. Základy fuzzy logiky pro řízení a modelování. Brno: Vutium, 2003. ISBN 80-214-2261-0.

HANSELMAN, Duane a LITTLEFIELD, Bruce. Mastering MATLAB. Velká Británie: Pearson Education Limited, 2012. ISBN 978-0-273-75213-4.

KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2024/25

V Brně dne 9.2.2025

L. S.

doc. Ing. Miloš Koch, CSc. garant	prof. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Obsahem diplomové práce je využití fuzzy logiky pro podporu rozhodování managementu při výběru vhodného systému SIEM do současného informačního prostředí společnosti XYZ a.s. Teoretická část je zaměřena na popis fuzzy logiky, seznámení se s programovým prostředím MATLAB s důrazem na jeho aplikaci při tvorbě fuzzy modelu. V praktické části jsou pak aplikovány principy fuzzy logiky a modelování k výběru nejvhodnějšího systému SIEM z možných řešení pro informační prostředí společnosti XYZ a.s. s využitím programového prostředí MATLAB.

Klíčová slova

fuzzy logika, fuzzy model, kritéria, kybernetická bezpečnost, manažerské rozhodování, MATLAB, podpora rozhodování, SIEM

Abstract

The content of the thesis is the use of fuzzy logic to support management decision-making in the selection of a suitable SIEM system for the current information environment of XYZ a.s. The theoretical part is focused on the description of fuzzy logic and an introduction to the MATLAB software environment with an emphasis on its application in the creation of a fuzzy model. In the practical part, principles of fuzzy logic and modelling are applied to select the most suitable SIEM system from possible solutions for the information environment of XYZ a.s. using the MATLAB software environment.

Keywords

fuzzy logic, fuzzy model, criteria, cybersecurity, managerial decision-making, MATLAB, decision-making support, SIEM

Bibliografická citace

KILIÁN, Tomáš. *Využití fuzzy logiky pro výběr vhodného systému SIEM v podniku*. Online, diplomová práce. Zuzana JANKOVÁ (vedoucí práce). Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2025. Dostupné z: https://www.vut.cz/studenti/zav-prace/detail/165204. [cit. 2025-05-14].

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 14. 5. 2025

Bc. Tomáš Kilián

autor

Poděkování

Velice rád bych poděkoval paní Ing. et Ing. Zuzaně Jankové, Ph.D. za cenné odborné rady, ochotu a lidský přístup během vedení této diplomové práce. Dále bych rád poděkoval Ing. Patrikovi Valentovi za věcné připomínky vedoucí k dokončení této diplomové práce. V neposlední řadě mé poděkování patří rodině a přátelům za veškerou jejich podporu v průběhu celého mého studia.

OBSAH

ÚVOD

V současném digitálním světě, kde se kybernetické bezpečnostní hrozby vyvíjejí s alarmující rychlostí, je efektivní zabezpečení dat, informací a veškerých dalších aktiv z pohledu dostupnosti, důvěrnosti a integrity pro společnosti naprosto nezbytnou součástí jejich podnikání. Systémy pro správu bezpečnostních informací a událostí (Security Information and Event Management, dále jen SIEM) se ve společnostech mohou stát klíčovým nástrojem pro komplexní monitorování, korelování a analýzu kybernetických bezpečnostních událostí. Avšak jejich výběr a implementace může představovat složitý proces, který vyžaduje zohlednění široké škály faktorů, jako jsou např. technické požadavky, rozpočet na kybernetickou bezpečnost, specifické potřeby společnosti, očekávané kybernetické bezpečnostní hrozby apod.

V této souvislosti se fuzzy logika ukazuje jako vhodný nástroj, který dokáže poskytnout flexibilní a intuitivní přístup k hodnocení a výběru vhodného systému SIEM. Fuzzy logika, vycházející z teorie fuzzy množin, totiž umožňuje zohlednit nejistoty a nejednoznačnosti, které často provázejí rozhodovací procesy nejen v oblasti informační, resp. kybernetické bezpečnosti. Namísto striktního binárního myšlení, které je v tradičních rozhodovacích modelech běžné, umožňuje fuzzy logika zohlednit různé úrovně pravděpodobnosti a váhy jednotlivých zvolených hodnotících kritérií. Pomocí fuzzy pravidel a systémů lze modelovat složité vztahy mezi různými parametry, které ovlivňují efektivitu a vhodnost jednotlivých vybraných řešení.

Tato diplomová práce má podpořit management společnosti, zejména v oblasti kybernetické bezpečnosti, který jednak hodlá implementovat vhodný systém SIEM do svého informačního prostředí a jednak zvažuje trvalou koupi licence programového prostředí MATLAB, které je v čase, sofistikovaně a poměrně snadno schopno zpracovávat a vyhodnocovat fuzzy systémy a je vhodně implementovatelné do současného informačního prostředí společnosti.

Každá společnost pro svá inovační rozhodnutí a aktivity musí nejprve zmapovat své možnosti, tj. jak teoreticky vhodný „terén“ pro cílené užití, tak možnosti implementace ve své praxi.

Tím se práce zabývá v úvodní části. Tedy vymezuje teoretická východiska, definuje použité principy fuzzy logiky a popisuje programové prostředí MATLAB se zacílením na jeho aplikaci zejména pro podporu rozhodování. Dále představuje informační a kybernetickou bezpečnost spolu se systémy SIEM.

Pro další účely je třeba představit danou společnost a stanovit samotná hodnotící kritéria s nadefinovanými atributy, na jejichž základě budou hodnoceny dostupné varianty systémů SIEM. Tato kritéria je dále z důvodu vyhodnocení, a též přehlednosti, potřeba rozdělit do tří kategorií. Výstupy fuzzy modelu je patřičné prezentovat ve vhodných grafických vizualizací. Samotný fuzzy model je zhotoven v programovém prostředí MATLAB a je využit k porovnání vybraných systémů SIEM.

Teprve poté, tj. na základě získaných výstupů, resp. grafických vizualizací, je možné formulovat doporučení pro podporu rozhodování managementu společnosti ve volbě vhodného systému SIEM, mj. vzhledem k jejímu současnému informačnímu prostředí.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Primárním cílem diplomové práce je využití fuzzy logiky pro vyhodnocování systémů pro správu bezpečnostních informací a událostí s využitím programového prostředí MATLAB.

Vytvořený fuzzy model v programovém prostředí MATLAB bude managementu společnosti XYZ a.s. sloužit pro vyhodnocení jednotlivých systémů pro správu bezpečnostních informací a událostí a bude poskytovat podporu při procesu rozhodování o jeho výběru, jenž bude implementován do informačního prostředí společnosti XYZ a.s. za účelem zvýšení úrovně kybernetické bezpečnosti. Diplomová práce je rovněž chápána jako podpora implementace programového prostředí MATLAB do současného informačního prostředí společnosti XYZ a.s., a to především pro možnost vyhodnocování s využitím fuzzy logiky coby podpory pro rozhodování ve společnosti XYZ a.s.

K tomu, aby bylo primárního cíle diplomové práce dosaženo, je potřeba provést postupné kroky (splnit dílčí cíle).

Prvním dílčím cílem je *vymezit teoretická východiska* v první kapitole této diplomové práce. Teoretická východiska poslouží k porozumění principům fuzzy logiky, díky jejichž aplikaci dále vznikne vhodný fuzzy model. Též v této části budou popsány obecné kroky tvorby fuzzy modelu v programovém prostředí MATLAB. Závěr této části diplomové práce bude věnován úvodu do informační a kybernetické bezpečnosti, včetně představení systémů pro správu bezpečnostních informací a událostí.

V druhé kapitole této diplomové práce bude zpracován druhý dílčí díl, a to *představení současného stavu společnosti* XYZ a.s. Tedy bude představena její organizační struktura, zmapováno její současné informační prostředí a budou nadefinována její hodnotící kritéria a atributy systémů pro správu bezpečnostních informací a událostí. V závěru této části diplomové práce budou zpracovány další dílčí cíle, a to *představení souhrnné nabídky* systémů pro správu bezpečnostních informací a událostí a následné *vyhodnocení pěti nejvhodnějších* s využitím Saatyho metody. Právě těchto pět nejvhodnějších systémů pro správu bezpečnostních informací a událostí bude detailněji představeno.

Základní platformou této diplomové práce bude pro formulování potřebných výstupů kapitola třetí, kde dojde ke splnění dalšího dílčího cíle, čímž je *zhotovení fuzzy modelu*

v programovém prostředí MATLAB. Tento model bude schopen vyhodnotit systémy pro správu bezpečnostních informací a událostí. Výstupy z modelu budou poté prezentovány formou příslušných grafických vizualizací.

Posledním dílčím cíle je na základě získaných výstupů fuzzy modelu *poskytnout podporu pro formulování a navržení doporučení*, resp. výběr nejvhodnějšího systému pro správu bezpečnostních informací a událostí, zejména s ohledem k současným možnostem implementace do informačního prostředí společnosti XYZ a.s. Tedy v závěru třetí kapitoly této diplomové práce bude prezentováno nezávazné doporučení výběru jednoho z vyhodnocených systémů pro správu bezpečnostních informací a událostí a tím bude podpořeno rozhodování managementu společnosti XYZ a.s.

1 TEORETICKÁ VÝCHODISKA PRÁCE

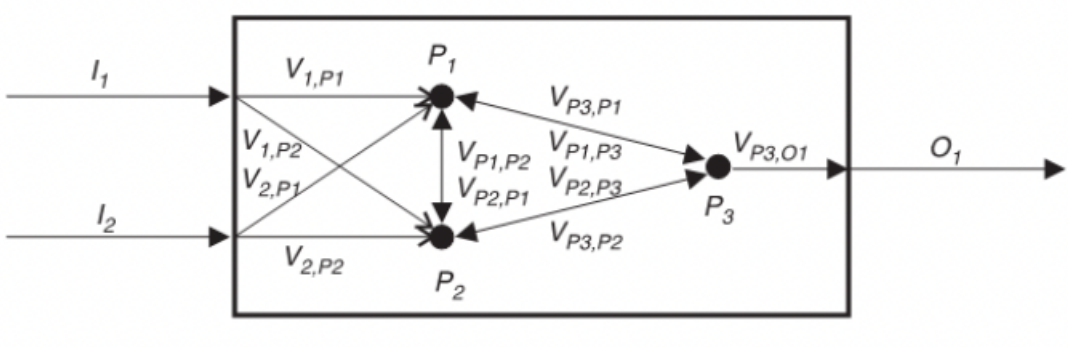
Následující kapitola se zabývá nejprve představením pojmů z teorie fuzzy logiky a s ní souvisejících odborných termínů. Dále jsou popsány obecné principy tvorby fuzzy modelu v programovém prostředí MATLAB. Závěr této kapitoly je věnován informační a kybernetické bezpečnosti spolu se systémem SIEM.

1.1 Pokročilé metody manažerského rozhodování

Management je disciplína, která se zabývá plánováním, organizováním, výběrem a rozmístěním spolupracovníků, vedením lidí a kontrolou s cílem dosáhnout stanovených cílů organizace. Tyto funkce se označují jako tzv. *sekvenční manažerské funkce*, jelikož se realizují postupně (ale mohou se částečně překrývat). Těmito funkcemi prostupují *manažerské funkce paralelní* (průběžné), mezi které se řadí analyzování řešených problémů, rozhodování a realizace (tj. implementace). Konkrétně *rozhodování* prezentuje výběr jednoho nebo více přípustných řešení na základě dostupných informací a analýz, jejich sdělení, prosazování a kontrolu plnění tohoto nebo těchto řešení [1, s. 5-6].

Důležitým pojmem z oblasti rozhodování je tzv. *systémový přístup*. Jedná se o způsob myšlení nebo řešení problémů, komplexně zkoumající jevy nebo procesy, který bere v potaz vnitřní i vnější souvislosti. Jeho cílem je nejen pomáhat vyřešit analyzovaný problém, ale též daný problém pochopit a vhodně formulovat. K tomuto systémový přístup používá modelování a simulaci. Na vytvořeném modelu lze změnami vstupních parametrů simulovat různé stavy a způsoby chování systémů, zkoumat trendy nebo zjišťovat citlivost systémů na změny vstupních parametrů. Samotný systém představuje ohraničenou množinu prvků se vzájemnými vazbami [2, s. 2-3].

Systém S je tedy možno zapsat jako množinu $S = \{P, V, I, O\}$, kde P je neprázdná množina prvků, V představuje neprázdnou množinu všech vazeb, I je neprázdná množina všech vstupů a O zase neprázdná množina všech výstupů [3, s. 17].



Obrázek č. 1: Ukázka schématu systému S

(Zdroj: [3])

Systémy pak možno dělit na tvrdé a měkké. Zatímco *tvrdé systémy* jsou využívány při modelování dobře strukturovaných problémů (např. technického charakteru), jejichž řešení lze snadno algoritmizovat, *měkké systémy* shrnují takové systémy, jejichž struktura není přesně definována a údaje jsou neurčité nebo neúplné (např. ve společenských vědách, včetně ekonomie a managementu). Tedy pro měkké systémy platí, že jejich vlastnosti, chování a problémy jsou popsány spíše mlhavě. *Model*, jakožto zjednodušená reprezentace reality, slouží k lepšímu porozumění vlastnostem a chování právě těchto systémů [2, s. 12].

Tradiční metody manažerského rozhodování (např. intuitivní rozhodování, analytické metody, porovnávání alternativ, empirické rozhodování aj.), často spoléhají na intuici a zkušenosti manažerů (kteří vždy nesou za rozhodnutí zodpovědnost), avšak s rostoucí složitostí a dynamikou podnikatelského prostředí neustále roste potřeba využívat pokročilejších metod manažerského rozhodování jako např. umělé neuronové sítě, generické algoritmy, simulační modely, teorii her a fuzzy logiku. Tyto metody umožňují získat kvantitativní podklady jak pro rozhodování, tak pro navrhování optimálních měkkých systémů. Výstupy pokročilých metod manažerského rozhodování vedou ke kvalitnějšímu rozhodovacímu procesu, zvláště pokud se jedná o multikriteriální a těžce algoritmizované úlohy. Nevýhodou těchto metod jsou vyšší nároky na prostředky, jakými jsou např. finance, čas, technické požadavky, odborné znalosti a podobně [3, s. 19].

1.2 Fuzzy logika

Běžná reprezentace znalostí je tradičně postavena na tzv. bivalentní logice, kde každý výrok může být pouze pravdivý nebo nepravdivý, bez dalších možností. Tento přístup, vycházející z Booleovy algebry a používaný také v binární logice pro digitální systémy, pracuje výhradně se dvěma hodnotami pravdivosti a základními logickými operacemi, jako jsou konjunkce (AND), disjunkce (OR) a negace (NOT). Lidské myšlení a rozhodování je však často spojeno s nepřesností a neurčitostí, což bivalentní logika nedokáže dostatečně zohlednit [4, s. 150-151].

Fuzzy logika, kterou představil a rozvinul americký matematik Lotfi A. Zadeh, přináší do tradičních logických systémů koncept mezihodnot a přibližných hodnocení [5, s. 7].

Na rozdíl od bivalentní logiky umožňuje fuzzy logika přiřadit výrokům stupně pravdivosti na škále mezi 0 (zcela nepravdivý) a 1 (zcela pravdivý). Tento přístup tak zavádí částečnou pravdivost, kterou lze díky specifických funkcí členství řídit pomocí lingvistických proměnných, tedy proměnných vyjadřujících hodnoty slovně [6, s. 4].

Výraz *fuzzy* v angličtině znamená mlhavý, nejasný, neostrý či neurčitý, a proto bývá fuzzy logika označována jako logika pracující s neostrými či nejasnými pojmy. Jejím klíčovým přínosem je schopnost efektivně pracovat s těmito pojmy, které jsou pro lidské rozhodování přirozené. Člověk při řešení složitých úloh obvykle nepoužívá přesně naměřené hodnoty, ale spíše obecné pojmy, jako jsou „daleko, blízko“, „rychle, pomalu“ nebo „nízko, vysoko“, tedy jazykové výrazy nevyjádřené čísly. Právě pro technické řešení těchto komplexních úloh nachází fuzzy logika spolu s teorií fuzzy množin široké uplatnění [7, s. 9].

1.2.1 Běžná množina

Základními stavebními kameny teorie množin jsou pojmy „množina“ a „prvek“. Jestliže U je množina, potom zápis $x \in U$ znamená, že x je prvkem množiny U. V opačném případě, tedy zápis $x \notin U$, indikuje, že x není prvkem množiny U. Způsob specifikace prvků je irelevantní [7, s. 14].

Množina tedy představuje soubor, který obsahuje přesně definované prvky. Lze ji považovat za skupinu prvků, které mají společnou určitou vlastnost důležitou pro jedince,

jenž ji používají. Množiny se vždy značí velkým písmenem a její prvky písmenem malým. Existují dva způsoby možného zápisu množin. Prvním způsobem je zapsání množiny jako výčet prvků, např.

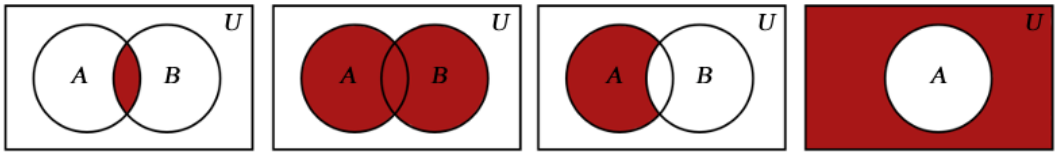
$$U = \{1;\ 3;\ 5;\ 7\}. \tag{1}$$

Druhý přípustný způsob zápisu množiny je pomocí jejích vlastností, tedy

$$U = \{x \in X; P(x)\}, \tag{2}$$

kde *X* je univerzum, ze kterého jsou vybírány prvky *x* do množiny *U* a formule *P(x)* popisuje, jaké mají prvky množiny vlastnosti [4, s. 129-131].

S množinami lze dále provádět různé operace. Mezi ty základní patří průnik, sjednocení, rozdíl a doplněk [4, s. 134].

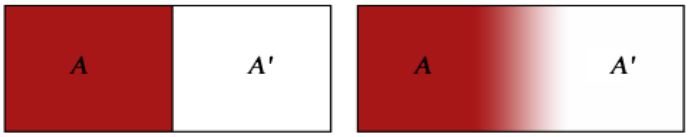


Obrázek č. 2: Průnik, sjednocení, rozdíl a doplněk

(Zdroj: Vlastní zpracování dle: [7], s. 15)

1.2.2 Fuzzy množina

V teorii fuzzy množin je pro běžné množiny, aby nedošlo k záměně, používán výraz *ostrá množina* (crisp set). Pro *fuzzy množinu* (fuzzy set) *F* nemusí platit pouze $x \in F$ nebo $x \notin F$, jako tomu je u ostrých (běžných) množin. Totiž prvek *x* může patřit do fuzzy množiny *F* jen částečně [7, s. 22].



Obrázek č. 3: Ostrá a neostrá (fuzzy) hranice mezi množinami

(Zdroj: Vlastní zpracování dle: [7], s. 21)

U fuzzy množin nejsou vyžadovány ostré hranice. Každá fuzzy množina je totiž přesně definována *funkcí členství* (membership function). Tato funkce přiřazuje každému prvku v uvažované fuzzy množině *F* jeho stupeň členství v této množině [8, s. 5-7].

Jedná se tedy o funkci, která mapuje univerzum *X* na celý interval $\langle 0; 1\rangle$. Funkci členství μ_F fuzzy množiny *F* lze tedy popsat jako funkci

$$\mu_F: X \to \langle 0; 1\rangle, \tag{3}$$

přičemž již nelze konstatovat, zda nějaký prvek je nebo není prvkem fuzzy množiny *F*. Každý prvek x ∈ X má totiž míru členství

$$\mu_F(x) \in \langle 0; 1\rangle, \tag{4}$$

tedy může nabývat libovolných hodnot od 0 (včetně) do 1 (včetně) [7, s. 22].

1.2.3 Standardní funkce členství

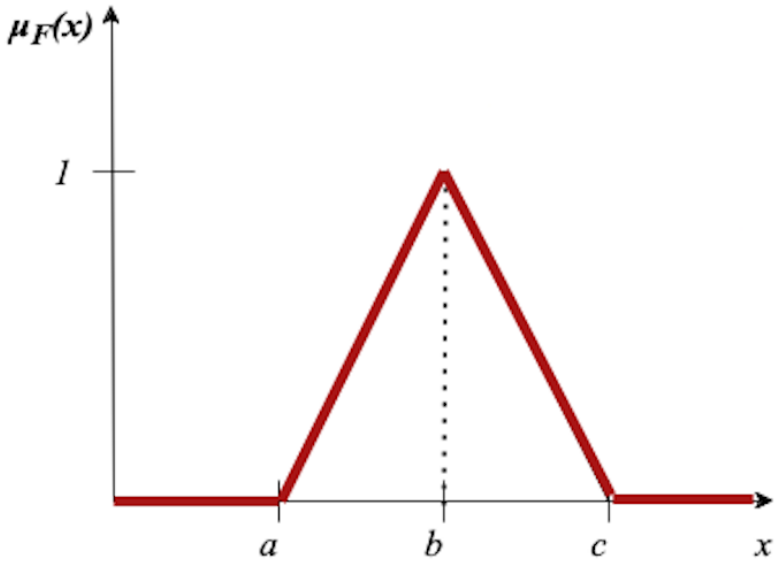
Tvar funkce členství může nabývat různých tvarů. Mezi ty nejčastější patří tvary členských funkcí typu Λ, Π, Z a S [9, s. 11].

Funkce členství typu Λ

Též někdy nazývána jako trojúhelníková funkce členství, je plně popsána třemi parametry $\{a, b, c\}$, přičemž musí platit vztah $a < b < c$. Matematicky lze tento typ funkce členství definovat jako

$$\mu_F(x) = \begin{cases} 0, & x < a \\ \dfrac{x-a}{b-a}, & a \le x \le b \\ \dfrac{c-x}{c-b}, & b \le x \le c \\ 0, & x > c \end{cases}, \tag{5}$$

tedy na intervalu od *a* do *b* je funkce rostoucí, v bodě *b* funkce dosahuje svého maxima a dále od bodu *b* do bodu *c* je funkce klesající. Mimo interval $\langle a; c\rangle$ má funkce nulovou hodnotu [5, s. 9].



Obrázek č. 4: Tvar funkce členství typu Λ

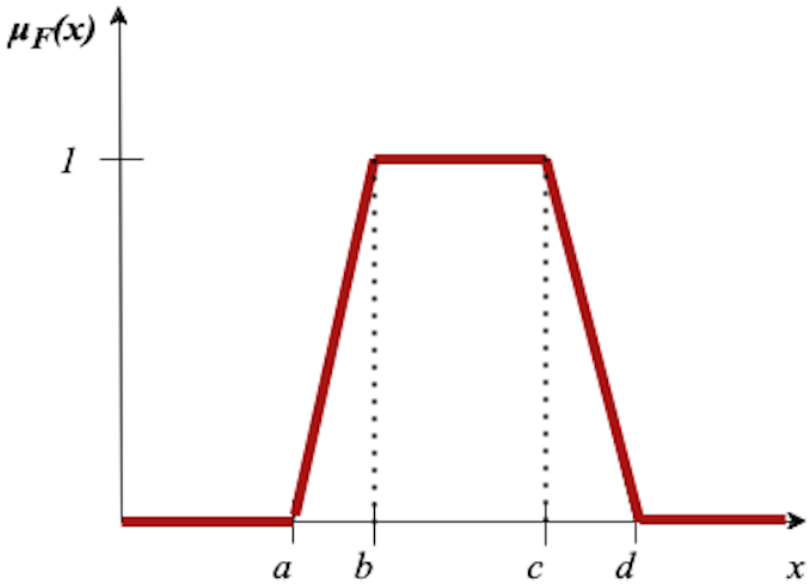
(Zdroj: Vlastní zpracování dle: [7], s. 23)

Funkce členství typu Π

Tento typ funkce členství je popsán čtyřmi parametry $\{a, b, c, d\}$, kde musí platit vztah $a < b < c < d$. Matematicky tento typ funkce členství vyjádřit jako

$$\mu_F(x) = \begin{cases} 0, & x < a \\ \dfrac{x-a}{b-a}, & a \leq x \leq b \\ 1, & b \leq x \leq c \\ \dfrac{d-x}{c-d}, & c \leq x \leq d \\ 0, & x > d \end{cases} \quad (6)$$

kdy z bodu a do bodu b je funkce rostoucí, v bodě b funkce dosahuje svého maxima a je konstantní do bodu c, z bodu c do bodu d je funkce klesající. Mimo interval $\langle a; d \rangle$ funkce dosahuje hodnoty nula [5, s. 10].



Obrázek č. 5: Tvar funkce členství typu Π

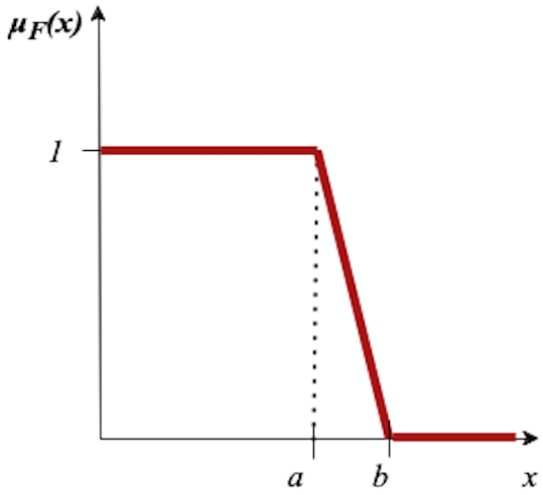
(Zdroj: Vlastní zpracování dle: [7], s. 24)

Funkce členství typu Z

Funkce členství typu Z odpovídá v intervalu $\langle a; b\rangle$ intervalu $\langle c; d\rangle$ u funkce členství typu Π. Matematicky lze funkci členství typu Z zapsat jako

$$\mu_F(x) = \begin{cases} 1, & x < a \\ \dfrac{b-x}{b-a}, & a \leq x \leq b \\ 0, & x > b \end{cases}, \tag{7}$$

kdy na rozdíl od funkce členství typu Π nemá funkce členství typu Z rostoucí část. Začíná na konstantní úrovni 1 a od bodu a do bodu b je funkce klesající. Hodnoty funkce od bodu b a dále jsou nulové [7, s. 23].



Obrázek č. 6: Tvar funkce členství typu Z

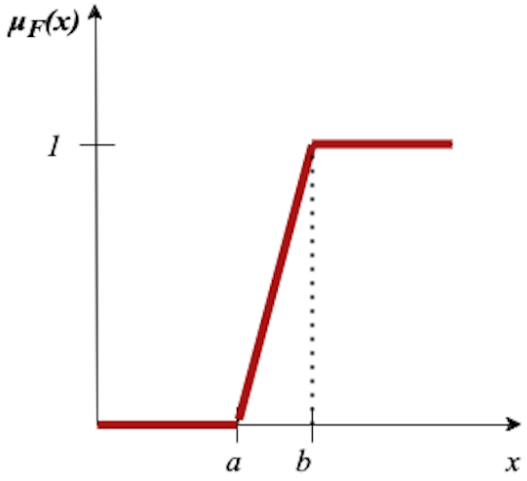
(Zdroj: Vlastní zpracování dle: [7], s. 23)

Funkce členství typu S

Funkce členství typu S odpovídá v intervalu $\langle a; b\rangle$ funkci členství typu Π. Matematicky tuto funkci členství lze zapsat jako

$$\mu_F(x) = \begin{cases} 0, & x < a \\ \dfrac{x-a}{b-a}, & a \leq x \leq b, \\ 1, & x > b \end{cases} \tag{8}$$

přičemž se ale od funkce členství typu Π liší tím, že od bodu b je funkce konstantní a již neklesá [7, s. 23].



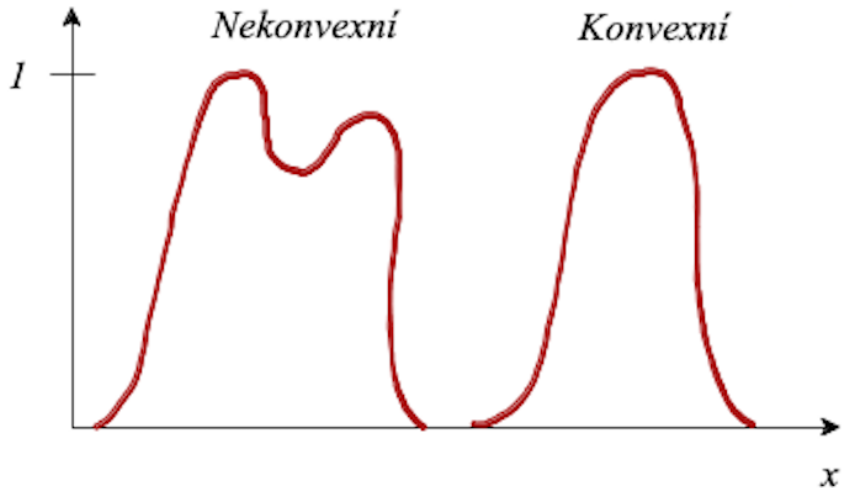
Obrázek č. 7: Tvar funkce členství typu S

(Zdroj: Vlastní zpracování dle: [7], s. 23)

1.2.4 Vlastnosti fuzzy množin

Pro pochopení vlastností fuzzy množin jsou dány fuzzy množiny *A* a *B* definované na univerzu *X* a *Y*.

O *konvexní* fuzzy množině lze hovořit tehdy, jestliže pro každé dva prvky $x, y \in X$ a pro každé $\lambda \in \langle 0; 1 \rangle$ platí, že hodnota funkce členství v jakémkoliv bodě, který leží mezi body *x* a *y* (jeho poloha je dána velikostí parametru λ), je větší než nejmenší z obou krajních hodnot $\mu_A(x), \mu_A(y)$ [7, s. 26-27].



Obrázek č. 8: Nekonvexní a konvexní fuzzy množina

(Zdroj: Vlastní zpracování dle: [7], s. 23)

Nosič (support) fuzzy množiny *A* lze matematicky zapsat jako

$$S(A) = \left\{ \frac{x}{\mu_A(x)} > 0 \right\}, \tag{9}$$

přičemž ostrá množina *S* je definovaná jako množina všech prvků univerza *X*, které mají kladnou funkci členství [7, s. 27].

Šířka (width) konvexní fuzzy množiny *A* s nosičem *S(A)* je rozdíl suprema a infima nosiče *S(A)*, tedy

$$width(A) = \sup\big(S(A)\big) - \inf\big(S(A)\big), \tag{10}$$

Pokud je nosič fuzzy fuzzy množiny ohraničený, lze supremum a infimum nahradit maximem a minimem. Šířka fuzzy množiny poté vyjadřuje jejich rozdíl [7, s. 27].

Výška (height) fuzzy množiny *A* je definována jako

$$hgt(A) = \sup\big(\mu_A(x)\big), x \in X. \tag{11}$$

Jestliže výška fuzzy množiny *A* je rovna 1, tak lze tuto množinu považovat za *normální*, v opačném případě jde o množinu *subnormální* [7, s. 27].

Jádro (nucleus) fuzzy množiny *A* je definováno jako ostrá množina všech prvků, jejichž funkce členství je rovna 1, tedy

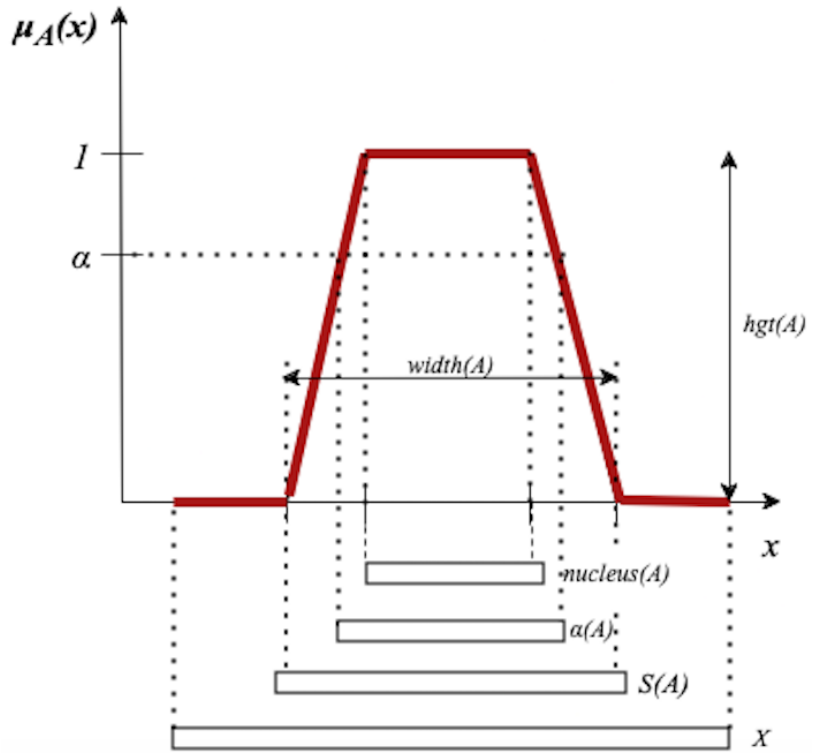
$$nucleus(A) = \left\{x \in \frac{X}{\mu_A(x)} = 1\right\}. \tag{12}$$

Jestliže je hodnota funkce členství rovna 1 pouze v jediném bodě, lze tento bod označit za *špičkovou hodnotu* (peak value), např. u funkce členství typu Λ [7, s. 27].

α-řez (α-cut) fuzzy množiny *A* je definován jako

$$\alpha(A) = \left\{x \in \frac{X}{\mu_A(x)} \geq \alpha\right\}, \tag{13}$$

kde $\alpha \in \langle 0; 1\rangle$ a *α(A)* je ostrá množina [7, s. 27].



Obrázek č. 9: Základní vlastnosti fuzzy množin

(Zdroj: Vlastní zpracování dle: [7], s. 27)

1.2.5 Operace s fuzzy množinami

Fuzzy logika používá pro sčítání, odčítání, násobení a dělení pravidla

$$[a;b] + [c;d] = [a + c; b + d], \tag{14}$$

$$[a;b] - [c;d] = [a - d; b - c], \tag{15}$$

$$[a;b] \cdot [c;d] = [min(a \cdot c, a \cdot d, b \cdot c, b \cdot d)\,; \max\,(a \cdot c, a \cdot d, b \cdot c, b \cdot d], \tag{16}$$

$$\frac{[a;b]}{[c;d]} = \left[min\left(\frac{a}{c}, \frac{a}{d}, \frac{b}{c}, \frac{b}{d}\right); \max\,(\frac{a}{c}, \frac{a}{d}, \frac{b}{c}, \frac{b}{d}\right]. \tag{17}$$

Z těchto pravidel následně vychází operace s fuzzy množinami [9, s. 9-10].

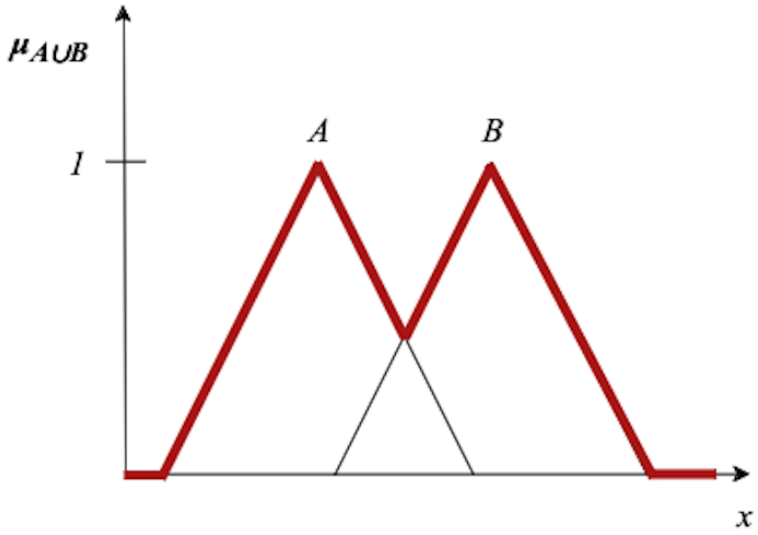
Stejně jako s ostrými množinami, tak i s fuzzy množinami lze vykonávat příslušné operace. Předpokladem jsou dvě ekvivalentní fuzzy množiny *A* a *B*. Pokud pro všechna $x \in X$ platí rovnost funkcí členství, tedy $\mu_A(x) = \mu_B(x)$, je možné zapsat $A = B$. Jestliže fuzzy množina *A* je podmnožinou fuzzy množiny *B*, tedy pokud pro všechna $x \in X$ platí $\mu_A(x) \leq \mu_B(x)$, lze zapsat $A \subseteq B$. Na rozdíl od ostrých (běžných) množin, v teorii fuzzy množin není interpretace operací s fuzzy množinami vůbec snadná, jelikož z intervalu $\langle 0; 1\rangle$ může funkce členství nabývat všech hodnot [7, s. 28].

Fuzzy sjednocení

Fuzzy sjednocení lze matematicky vyjádřit jako

$$\mu_{A \cup B}(x) = ma\,x\big(\mu_A(x); \mu_B(x)\big)\,, \tag{18}$$

kdy se jedná o fuzzy množinu maxim funkcí členství všech prvků univerza *X* [9, s. 10].



Obrázek č. 10: Fuzzy sjednocení

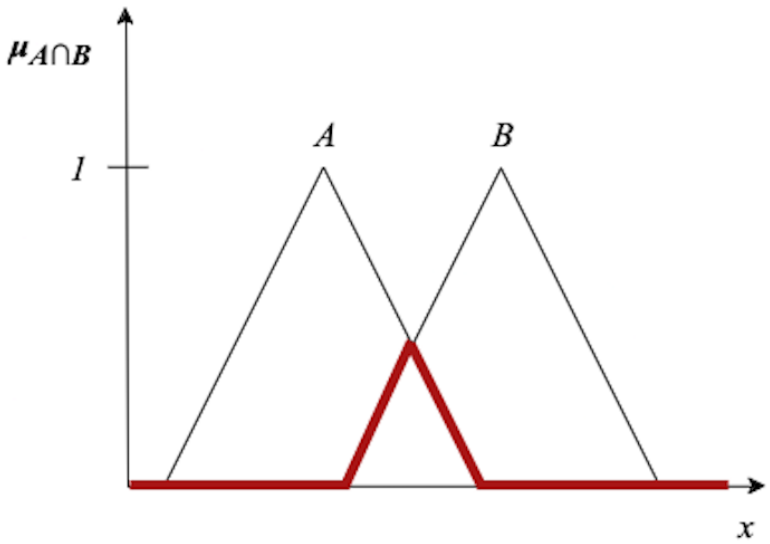
(Zdroj: Vlastní zpracování dle: [5], s. 19)

Fuzzy průnik

Fuzzy průnik lze matematicky zapsat jako

$$\mu_{A\cap B}(x) = min\left(\mu_A(x); \mu_B(x)\right), \tag{19}$$

kdy se jedná o fuzzy množinu minim funkcí členství všech prvků univerza X [9, s. 10].



Obrázek č. 11: Fuzzy průnik

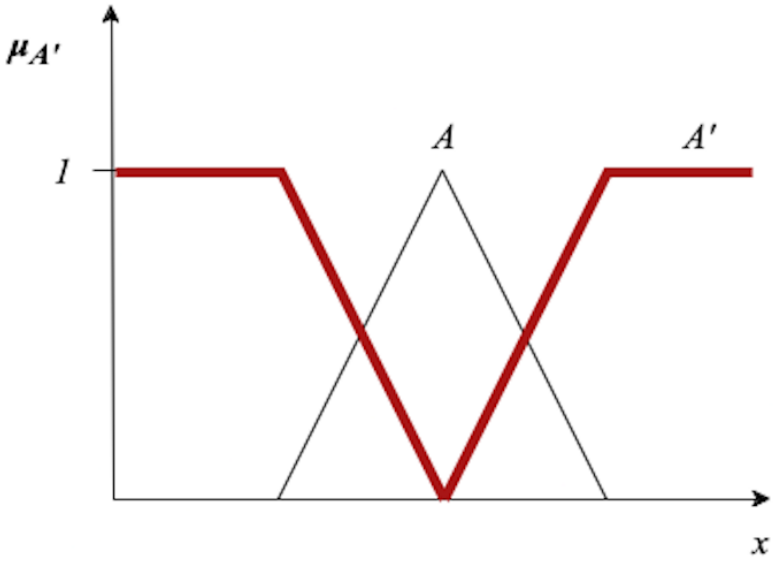
(Zdroj: Vlastní zpracování dle: [5], s. 19)

Fuzzy doplněk

Fuzzy doplněk, též někdy nazýván jako fuzzy komplement, je možné matematicky zapsat jako

$$\mu_{A'}(x) = 1 - \mu_A(x), \tag{20}$$

kdy doplňkem fuzzy množiny A je fuzzy množina A' všech prvků univerza X, jejichž hodnota funkce členství vyjadřuje, kolik v původní fuzzy množině A chybí prvku do plného členství [9, s. 10].



Obrázek č. 12: Fuzzy doplněk

(Zdroj: Vlastní zpracování dle: [5], s. 20)

1.2.6 Proces fuzzy zpracování

Tvorba systému s fuzzy logikou zahrnuje tři základní kroky. Prvním krokem je fuzzifikace, následně proběhne krok fuzzy inference a jako poslední krok se vykoná defuzzifikace [9, s. 11].

Obrázek č. 13: Rozhodování s využitím fuzzy zpracování

(Zdroj: Vlastní zpracování dle: [9], s. 11)

Fuzzifikace

Prvním krokem v procesu fuzzy zpracování je *fuzzifikace*. Ta představuje převedení reálných proměnných na jazykové proměnné, které reprezentují jednotlivá vstupní kritéria modelované problematiky. Obvyklý počet atributů jedné takové proměnné se v praxi pohybuje od tří do sedmi. Při modelování dané problematiky jsou pro každou proměnnou vybrány atributy, jejichž slovní popisy by měly být stručné, výstižné a dostatečně obecné, např. u proměnné riziko lze zvolit atributy jako žádné, malé, střední, vysoké a velmi vysoké. Stupeň členství atributů proměnné v množině je vyjádřen matematickou funkcí. Existuje mnoho tvarů funkcí členství. V praxi jsou nejvíce využívané funkce členství typu Λ, Π, Z a S v lineární podobě, případně vyhlazené S křivky. Stupeň členství v množině se týká vstupních i výstupních funkcí [3, s. 23].

Fuzzy inference

Po fuzzifikaci následuje krok *fuzzy inference*, která definuje chování systému pomocí nadefinovaných pravidel typu $\langle Když \rangle$, $\langle Potom \rangle$, $\langle S\ váhou \rangle$ na jazykové úrovni. Tato pravidla jsou definována pomocí podmínkových vět, ve kterých je možné využívat logické operátory jako AND (průnik), OR (sjednocení) a NOT (doplněk). Podmínkové věty mají známou formu programovacích jazyků

$$\langle Když \rangle Vstup_a \langle AND \rangle Vstup_b \ldots \\ \ldots Vstup_x \langle OR \rangle Vstup_y \ldots \langle Potom \rangle Výstup_1 \langle S\ váhou \rangle z, \quad (21)$$

tj. když (nastane stav) $Vstup_a$ a $Vstup_b$, …, $Vstup_x$ nebo $Vstup_y$ … potom (je situace) $Výstup_1$ s váhou pravidla z, kde z odpovídá hodnotám v intervalu 0 (včetně) až 1 (včetně) [3, s. 23].

Každá kombinace atributů proměnných, vstupujících do systému a vyskytujících se v podmínce $\langle Když \rangle$, $\langle Potom \rangle$ představuje jedno pravidlo. Každé pravidlo je nutné ohodnotit příslušným stupněm podpory, tedy stanovit váhu daného pravidla v systému z. Sada těchto fuzzy pravidel je jádrem expertních systémů. V rámci průběhu optimalizace expertních systémů lze váhu pravidel měnit, jelikož výsledek expertního systému s fuzzy logikou je poměrně závislý na správném určení významu definovaných pravidel. Tato pravidla si tvoří uživatel sám [3, s. 24].

Výstupem fuzzy inference je jazyková proměnná, která může vyjadřovat např. zda dané rozhodnutí zamítnout, zvážit či přímo doporučit [3, s. 24].

Defuzzifikace

Posledním krokem v procesu fuzzy zpracování je *defuzzifikace*. V rámci tohoto kroku je výstup fuzzy inference, tedy jazyková proměnná, převeden na reálné proměnné. Cílem defuzzifikace je převedení fuzzy hodnoty výstupní proměnné tak, aby co nejlépe slovně vystihovala výsledek fuzzy výpočtu [3, s. 24].

1.3 Tvorba fuzzy modelu s využitím programového prostředí MATLAB

Tato podkapitola se zabývá tvorbou fuzzy modelu v programovém prostředí MATLAB.

1.3.1 Programové prostředí MATLAB

MATLAB od společnosti The MathWorks představuje výkonné programové programovací prostředí zejména pro vědecké a inženýrské výpočty. Název MATLAB je odvozen ze slov *MATrix LABoratory*, jelikož jeho základním datovým elementem je matice, někdy též označována jako pole [10, s. 1].

Přestože programové prostředí MATLAB bylo původně primárně navrženo jako uživatelsky přívětivé rozhraní pro profesionálně vyvinuté numerické podprogramy lineární algebry, s postupným vývojem do něj byly integrovány další funkce, jako např. uživatelské grafické rozhraní a vizualizace, což snížilo význam numerických rutin lineární algebry. I přes tuto změnu programového prostředí MATLAB poskytuje širokou škálu užitečných funkcí maticové algebry [11, s. 310].

Programové prostředí MATLAB se využívá především k matematickým výpočtům, modelování a simulování, datovým analýzám a zpracování, vizualizaci, grafice a vývoji algoritmů. Proto je oblíbené zejména v akademické sféře, kde s ním akademičtí pracovníci a studenti pracují v začátečnických i pokročilých kurzech matematiky, přírodních vědách a zejména v inženýrství. V průmyslu je programové prostředí MATLAB využíváno pro výzkum, k vývoji a designu [10, s. 1].

V základu programové prostředí MATLAB obsahuje nástroje a funkce, které slouží k řešení těch nejběžnějších typů úloh. Pro řešení pokročilých a složitějších úloh je možné doinstalovat doplňky, tzv. *toolboxy*, což jsou sady specializovaných nástrojů navržených k řešení specifických typů úloh. Mezi nejznámější toolboxy patří ty pro signálové zpracovávání, řídící systémy, symbolické výpočty nebo pro návrh a implementaci fuzzy systémů [10, s. 1].

Právě programové prostředí MATLAB ve verzi R2024b spolu s doplňkem Fuzzy Logic Toolbox je využito pro účely teoretické i praktické části této diplomové práce.

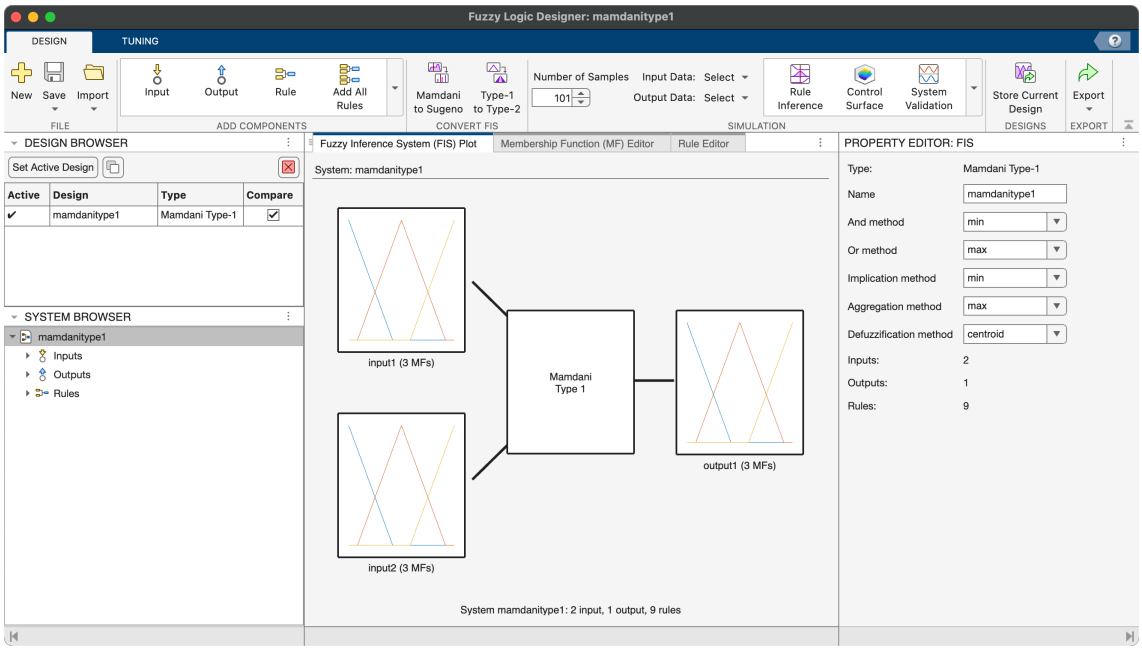
1.3.2 Fuzzy Logic Toolbox

Fuzzy Logic Toolbox poskytuje funkce a nástroje pro analýzu, návrh a simulaci fuzzy systémů, včetně možnosti specifikovat a nastavit vlastní vstupy, výstupy, funkce členství a bázi pravidel. Dovoluje také automatické nastavování funkcí členství a pravidel fuzzy systému na základě zvolených dat [12].

V režimu příkazového řádku pro psaní skriptů nebo pomocí propracovaného uživatelského grafického rozhraní umožňuje naplnit znalostní bázi fuzzy systémů. Fuzzy Logic Toolbox obsahuje základní nástroje pro vytvoření, editaci a optimalizaci *fuzzy inferenčních systémů* (dále jen FIS), které lze propojovat do stromových struktur. Mezi tyto nástroje patří Fuzzy Logic Designer, který obsahuje zejména editor funkcí členství (Membership Function Editor), editor pravidel (Rule Editor), prohlížeč pravidel (Rule Inference) a prohlížeč řídící plochy (Control Surface) [7, s. 120].

1.3.3 Fuzzy Logic Designer

Tento nástroj je možné spustit příkazem *fuzzyLogicDesigner*. Díky přívětivému uživatelskému grafickému rozhraní umožňuje provést všechny kroky tvorby FIS. Skládá se z několika návrhových a ladících nástrojů, např. FIS Plot umožňuje definovat pro daný FIS vstupy a výstupy, název a ostatní parametry, včetně vizualizace jeho struktury [13].



Obrázek č. 14: Fuzzy Logic Designer

(Zdroj: Vlastní zpracování)

Jedním z důležitých parametrů je volba vhodného typu FIS. Fuzzy Logic Toolbox podporuje FIS druhu Mamdani a Sugeno v provedeních typu 1 a typu 2. Zároveň umožňuje převádění z jednoho druhu FIS na ten druhý [13] [14].

Mamdani FIS je považován za více intuitivní a lépe přizpůsobivý lidským vstupům. Báze pravidel je uživateli lépe interpretovatelná, protože pravidla mohou být formulována v přirozeném jazyce a přímo odrážet lidské rozhodovací procesy. Díky těmto vlastnostem je Mamdani FIS často preferován v úlohách, při kterých je třeba zachovat vysokou míru srozumitelnosti a interpretovatelnosti výstupu. Mezi takové úlohy patří například ty z manažerského rozhodování. Nevýhodou je vyšší výpočetní náročnost při složitějších FIS a nutnost důkladného návrhu funkcí členství i pravidel. Defuzzifikace Mamdani FIS výstupu, tedy fuzzy množiny, je prováděna některou z metod (např. *metoda těžiště* (centroid) nebo *metoda bisector*), která při výpočtu konečného ostrého výstupu využívá všechen obsah plochy pod funkcí členství výstupní fuzzy množiny [14] [15].

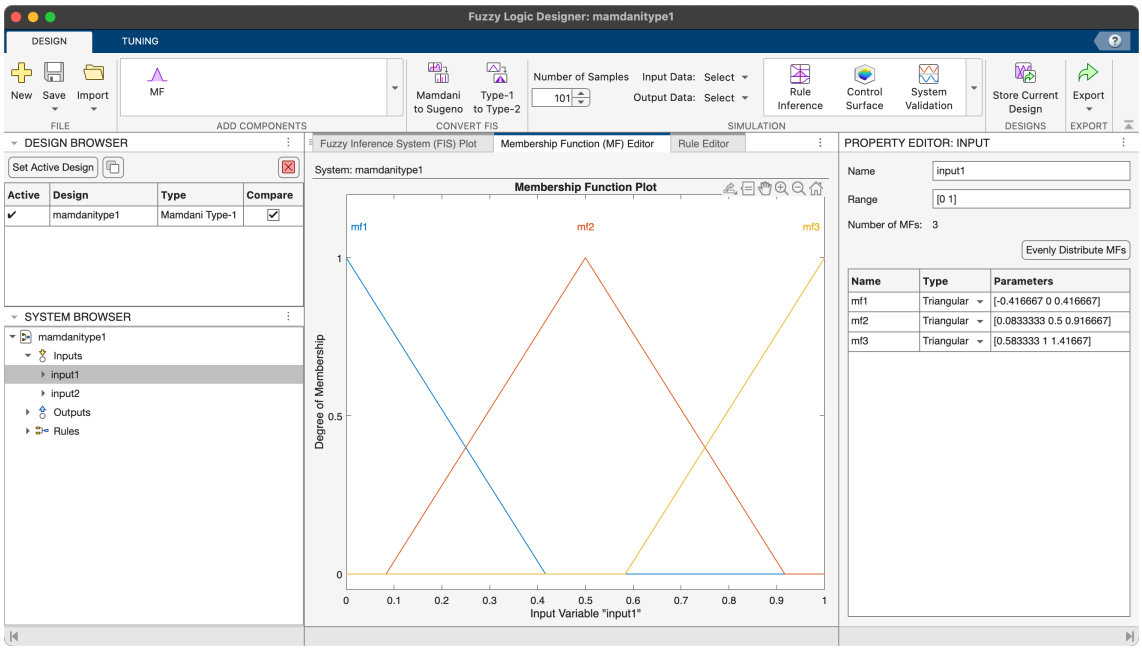
Sugeno FIS je navržen tak, aby kombinoval flexibilitu fuzzy logiky s precizností matematických modelů. Mezi jeho silné stránky patří efektivita výpočtů a přesnost výstupů. Proto se příliš nehodí pro manažerské účely, ale spíše pro matematické analýzy, kde jsou právě tyto vlastnosti výstupů vyžadovány. Výstupem Sugeno FIS je totiž funkce

členství, která je buď konstantní, nebo lineární funkcí vstupních hodnot. Krok defuzzifikace pro Sugeno FIS probíhá výpočtem váženého průměru nebo váženého součtu několika datových bodů kombinující výstupní funkci členství s váhami použitých pravidel [14].

Pro FIS typu 1 platí, že jeho funkce členství má pro jakoukoli hodnotu v univerzu pouze jedinou hodnotu stupně členství. Funkce členství u FIS typu 1 sice modeluje stupeň členství v dané jazykové množině, ale nemodeluje neurčitost stupně členství. Pro modelování vyšší úrovně neurčitosti ve stupni členství je určen FIS typu 2. Funkce členství pro FIS typu 2 může stupeň členství nabývat z určitého rozsahu hodnot. To znamená, že namísto jediné hodnoty stupně členství (jako u FIS typu 1), může funkce členství u FIS typu 2 vyjadřovat neurčitost pomocí intervalu, čímž lépe pokrývá situace, kde vstupy nebo pravidla nejsou přesně definovány a obsahují více možností pro přiřazení hodnoty stupně členství [16].

1.3.4 Editor funkcí členství

Editor funkcí členství umožňuje, jak již z jeho názvu vyplývá, přidávat, odebírat, nastavovat a upravovat funkce členství. Pro každý vstup i výstup zde lze nastavit požadovaný počet funkcí členství, jejich název, typ tvaru funkce členství (např. trojúhelníkový, S a Z, zvonový, sigmoidní nebo Gaussovy křivky aj.), včetně parametrů jako krajní body a maximum funkce členství. Počet funkcí členství musí odpovídat počtu atributů [13].

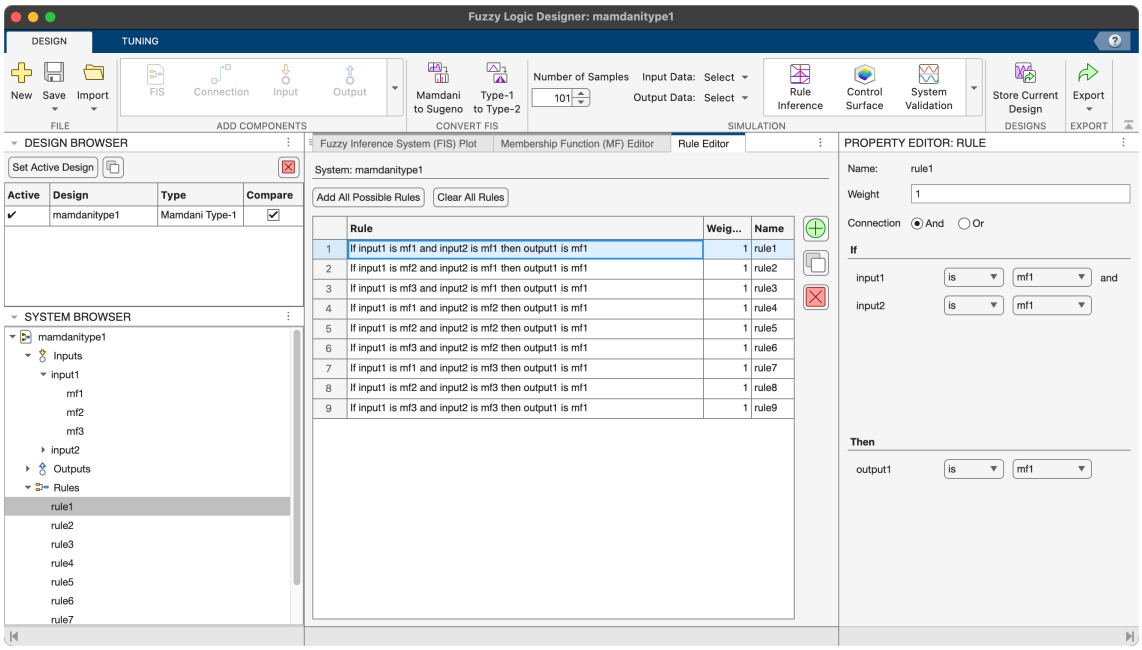


Obrázek č. 15: Editor funkcí členství

(Zdroj: Vlastní zpracování)

1.3.5 Editor pravidel

Editor pravidel slouží ke tvorbě a správě ⟨$Když$⟩, ⟨$Potom$⟩, ⟨$S\ váhou$⟩ pravidel, která definují závislosti mezi vstupními a výstupními proměnnými. Proto tyto pravidla lze vytvářet až po nastavení vstupů a výstupů FIS a k nim nadefinovaných příslušných funkcí členství. Vztahy mezi jednotlivými kritérii s atributy jsou definovány pomocí logických operátorů AND a OR. Kromě ručního zadávání pravidel nabízí tento editor volbu nechat všechna možná pravidla automaticky vygenerovat. Poté je ovšem nutné každému takto vygenerovanému pravidlu zvolit expertně určenou hodnotu na jeho výstupu [13].

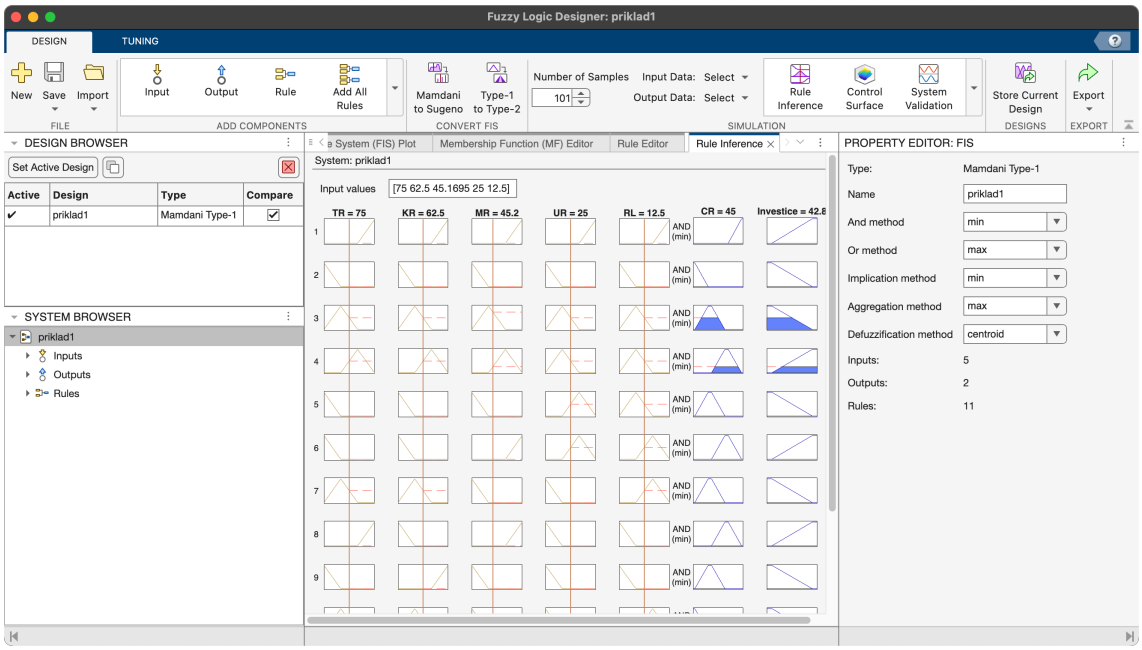


Obrázek č. 16: Editor pravidel

(Zdroj: Vlastní zpracování)

1.3.6 Prohlížeč pravidel

Prohlížeč pravidel nabízí grafický pohled na to, jak byla všechna pravidla nadefinována. Tento nástroj je užitečný obzvláště při analýze FIS s větším počtem kritérií a atributů, protože uživateli umožňuje testovat různé kombinace vstupních hodnot. A to buď číselným zadáním vstupních hodnot do textového pole ve vrchní části editoru, nebo posunem úrovně vstupu, která je reprezentována svislou barevnou linií u jednotlivých kritérií. Během posouvání svislé linie nebo číselného zadávání vstupních hodnot je možné sledovat změny ve výstupech a zároveň identifikovat pravidla, která k těmto výstupům vedla [13].

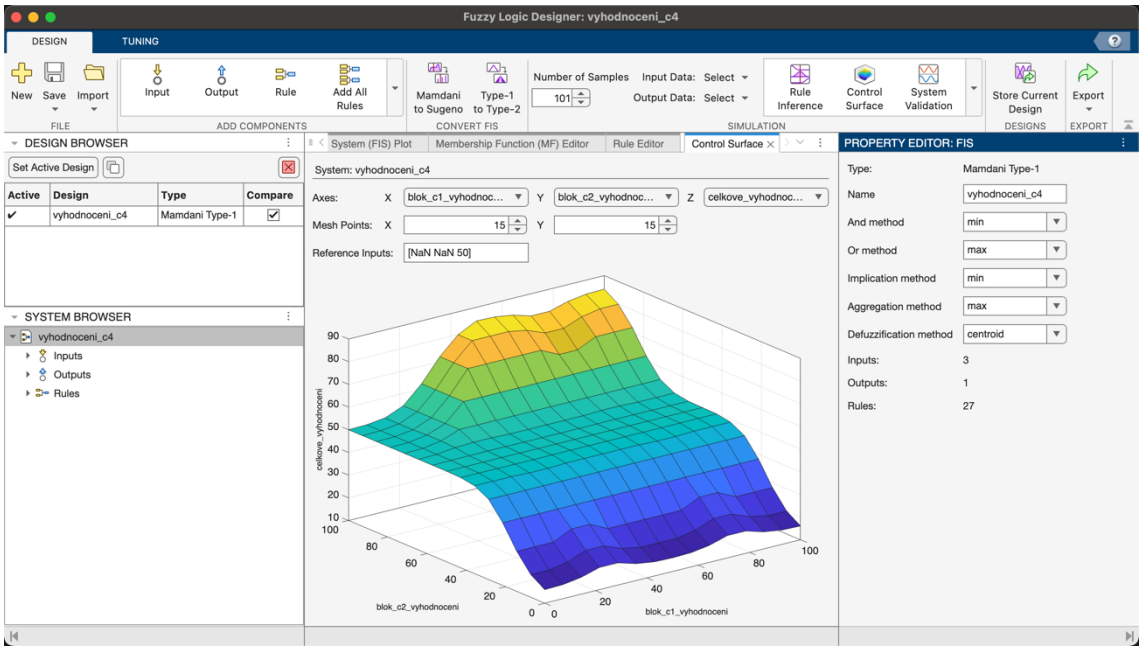


Obrázek č. 17: Prohlížeč pravidel

(Zdroj: Vlastní zpracování)

1.3.7 Prohlížeč řídící plochy

Prohlížeč řídící plochy poskytuje trojrozměrný pohled na výstupní hodnotu FIS pro všechny možné kombinace dvou vstupních proměnných. Osa *X* a osa *Y* představuje vstupní proměnné a osa *Z* reprezentuje výstupní hodnotu FIS. Míra naplnění maximální hodnoty výstupu je barevně znázorněna, kdy platí, že čím je barva tmavší, tím horší je výsledná hodnota výstupu a naopak, čím světlejší barva je, tím se výsledná hodnota výstupu přibližuje té možné maximální. Je doporučeno, aby barevné a svislé přechody byly plynulé a vyhlazené. Výsledná řídící plocha je ovlivněna vytvořenými pravidly a jejich nadefinováním [13].

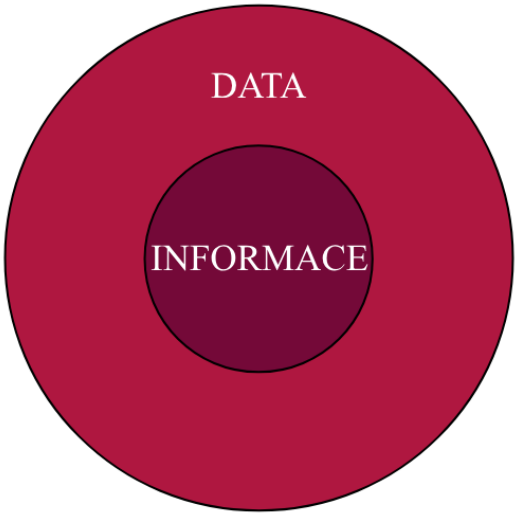


Obrázek č. 18: Prohlížeč řídící plochy

(Zdroj: Vlastní zpracování)

1.4 Informační bezpečnost

Data představují nezpracovaná fakta nebo stavy, které samotné nemají konkrétní význam. Jde tedy o surové hodnoty, které lze sbírat, ukládat a zpracovávat. Mohou to být čísla, znaky nebo jiné hodnoty, které postrádají kontext. *Informace* jsou data, která byla zpracována, organizována nebo analyzována tak, že dostanou kontext, smysl nebo význam. Tedy data, která mají strukturu a mohou být využita k rozhodování, či ke komunikaci se stávají informacemi, které odpovídají na základní otázky co, proč nebo jak. Informace jsou cennější, protože mohou obsahovat citlivé údaje, rozhodnutí nebo osobní data, která je nutné chránit [17, s. 46-47].



Obrázek č. 19: Data a informace

(Zdroj: Vlastní zpracování dle: [17], s. 47)

Informační bezpečnost, někdy označována jako InfoSec, se věnuje ochraně dat a informací v jakékoliv formě (fyzické, elektronické či jiné formě) před nežádoucími bezpečnostními hrozbami, jako neoprávněný přístup, užití, zveřejnění, narušení, modifikace a destrukce. Jejím cílem je zajistit důvěrnost, integritu a dostupnost informací v celém jejich životním cyklu, což zahrnuje jejich shromažďování, uchovávání, přenos, zpracování i vymazání. Informační bezpečnost obsahuje širokou škálu bezpečnostních opatření k ochraně všech typů dat a informací, nejen těch v elektronické podobě. Bezpečnostní opatření mohou být *technická*, *organizační* a *procesní*. Informační bezpečnost též zahrnuje komplexní procesy, které pomáhají organizacím vytvářet a udržovat bezpečné prostředí pro správu dat a informací. Mezi takové procesy patří identifikace, hodnocení a analýza rizik, na jejichž základě se provádí implementace bezpečnostních opatření za účelem zmírnění identifikovaných rizik. Dále se provádí procesy jako monitorování a audit, vzdělávání a školení [18, s. 3-5].

Informační bezpečnost je definována řadou norem ISO 27000, kam patří např. *ISO/IEC 27001*, což je mezinárodně platný standard, který specifikuje požadavky na zavedení, implementaci, provoz, monitorování, přezkoumávání, údržbu a neustálé zlepšování *systému řízení bezpečnosti informací* (Information Security Management System, dále jen ISMS) [19].

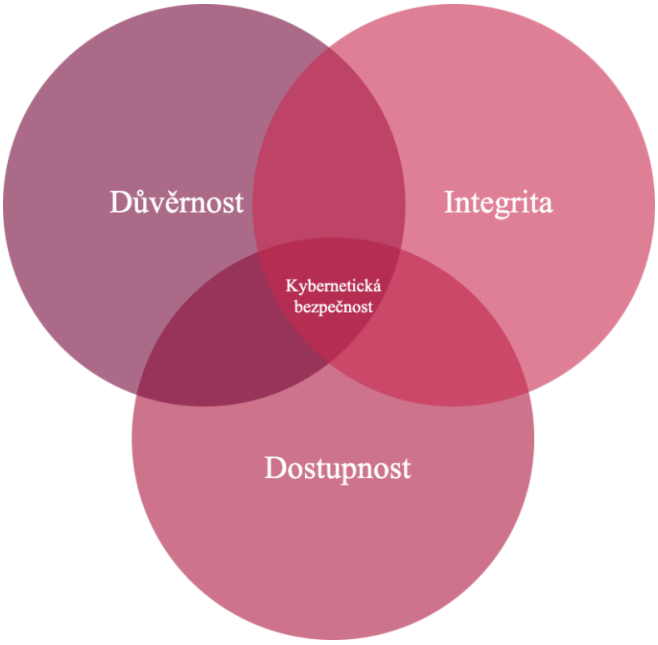
1.4.1 Kybernetická bezpečnost

Kybernetický prostor je pomyslné hrací pole, kde se odehrávají veškeré útočné a obranné akce spojené s kybernetickou bezpečností, kybernetickými bezpečnostními událostmi a kybernetickými bezpečnostními incidenty, ochranou digitálních dat apod. Lze si jej představit jako virtuální realitu, která nemá konec ani začátek, ovšem je zcela závislá na technologiích nacházejících se ve světě reálném. Odborně je kybernetický prostor definován jako digitální prostředí, které umožňuje vznik, zpracování a výměnu informací, je tvořeno informačními systémy a službami a sítěmi elektronických komunikací. Mezi jeho znaky patří decentralizovanost, globálnost, otevřenost, interaktivnost a bohatost na informace [17, s. 35-37].

Kybernetická bezpečnost představuje souhrn nástrojů, politik, bezpečnostních konceptů, bezpečnostních opatření, pokynů, přístupů k řízení rizik, školení, osvědčených postupů, zajištění a technologií, které lze použít k ochraně kybernetického prostoru a aktiv příslušné společnosti a její uživatelů. Mezi tyto aktiva se řadí výpočetní technika, lidé, infrastruktura, aplikace a služby, telekomunikační systémy, včetně přenášených i uložených dat a informací v kybernetickém prostoru. Obecně se za *aktivum* považuje cokoliv, co má určitou hodnotu pro osobu, organizaci nebo stát. Dále je možné aktiva dělit na dvě skupiny, a to na aktiva *primární* a *podpůrná*. Kybernetická bezpečnost tedy usiluje o to, aby byla zajištěna a dlouhodobě udržována požadovaná úroveň bezpečnostních vlastností jednotlivých aktiv proti relevantním bezpečnostním rizikům v kybernetickém prostoru. Je proto podmnožinou informační bezpečnosti s tím, že se oproti ní zabývá především ochranou digitálních technologií, komunikačních sítí, informačních systémů, digitálních informací a dat proti kybernetickým bezpečnostním hrozbám. Cílem kybernetické bezpečnosti je tak zajistit, aby aktiva byla odolná vůči útokům a byla chráněna před zneužitím [20, s. 97-98].

Při uplatňování kybernetické bezpečnosti, která je realizována v kybernetickém prostoru i mimo něj, dochází k implementaci několika základních principů, mezi které patří *CIA*, *prvky kybernetické bezpečnosti* (lidé, technologie, procesy) a *životní cyklus kybernetické bezpečnosti* (prevence, detekce, reakce). Tyto principy jsou nazývány *triády kybernetické bezpečnosti* [17, s. 45].

Konkrétně triáda CIA reprezentuje důvěrnost (confidentiality), integritu/celistvost (integrity) a dostupnost (availability). *Důvěrnost* znamená skutečnost, že k informacím, datům, či informačním a komunikačním technologiím (Information and Communication Technologies, dále jen ICT) mají přístup pouze subjekty, které jsou k tomu autorizované (oprávněné). *Integrita* představuje nemožnost zásahu do informací, dat, ICT a jejich nastavení apod. jiným subjektem než takovým, který je k tomuto úkonu oprávněn. A *dostupnost* lze definovat jako garanci možnosti přístupu k informacím, datům nebo ICT v okamžiku potřeby [17, s. 45-54].



Obrázek č. 20: Triáda CIA a kybernetická bezpečnost

(Zdroj: Vlastní zpracování dle: [17], s. 56)

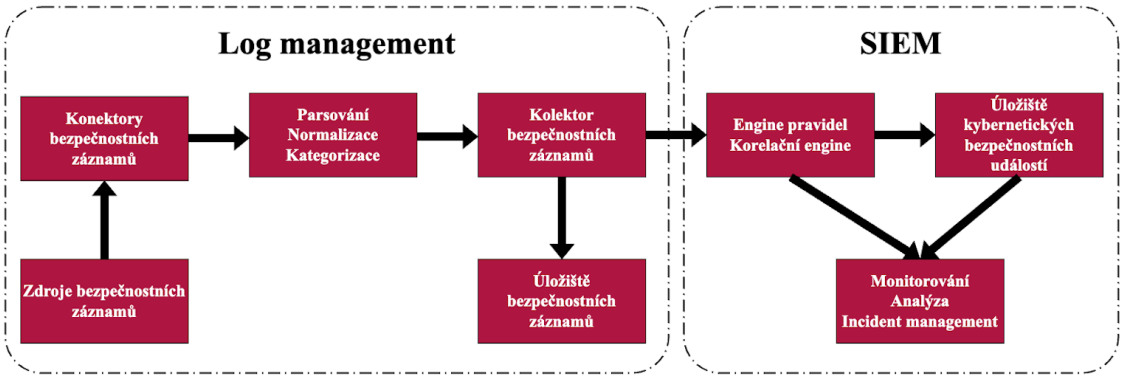
Mezi další důležité pojmy z oblasti kybernetické bezpečnosti patří kybernetická bezpečnostní hrozba, riziko, kybernetická bezpečností událost a kybernetický bezpečnostní incident. *Kybernetická bezpečnostní hrozba* představuje něco, co je schopno narušit běžný stav aktiva a zasáhnout do práv jiných subjektů. *Riziko* vyjadřuje potenciál, že se hrozba stane reálnou a využije *zranitelnost* (tj. slabé místo) aktiva. *Kybernetická bezpečnostní událost* je událost, která může způsobit narušení bezpečnosti aktiva. *Kybernetický bezpečnostní incident* představuje narušení bezpečnosti aktiva. V kontextu kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů jsou klíčovým nástrojem systémy *SIEM*, které zajišťují jejich detekci, analýzu a následnou reakci [17, s. 68-81].

Systém SIEM

Obecně systém SIEM umožňuje monitorovat, agregovat, ukládat a korelovat kybernetické bezpečnostní události nad spravovanou infrastrukturou. Jedná se tedy o další vrstvu nad správou bezpečnostních záznamů, tzv. *log managementem*. Ten primárně umožňuje sběr a ukládání bezpečnostních záznamů ze spravované infrastruktury v tzv. surovém (raw) formátu. Následně jsou tyto bezpečnostní záznamy parsovány, normalizovány, kategorizovány a případně ukládány do požadovaného strukturovaného formátu. Tento proces umožňuje identifikaci kybernetických bezpečnostních událostí, se kterými poté operuje systém SIEM. Ten proto představuje ústřední platformu moderních *bezpečnostních operačních center* (Security Operations Center, dále jen SOC), neboť shromažďuje kybernetické bezpečnostní události z mnoha typů zdrojů (např. antivirových systémů, firewallů, webových serverů, databázových serverů, routerů, produkčních i testovacích serverů apod.), které koreluje a následně vygeneruje bezpečnostní upozornění, která mohou vést k bezpečnostním hlášením. Kromě těchto klíčových schopností existuje mezi dostupnými systémy SIEM několik rozdílů, které obvykle odrážejí rozdílné postavení systémů SIEM na trhu [21, s. 1-2].

Kybernetické bezpečnostní události systém SIEM vyhodnocuje optimálně v reálném čase. Může také doplňovat informace dávající datům v kybernetických bezpečnostních událostech kontext, jako např. informace o uživatelích, výsledcích bezpečnostních skenů, informace z externích zdrojů apod. Tyto obohacené kybernetické bezpečnostní události jsou také následně agregovány, korelovány a je nad nimi prováděna analýza, která má identifikovat potenciální kybernetické bezpečnostní hrozby v monitorované infrastruktuře [17, s. 461].

Pro systémy SIEM jsou důležité parametry jako výkon, báze korelačních pravidel, rychlost zpracovávání v reálném čase, komplexnost, odolnost, škálovatelnost, možnosti reakce a hlášení, cena, licenční model, doba uchovávání kybernetických bezpečnostních událostí a další [21, s. 6].



Obrázek č. 21: Základní schéma log managementu a systému SIEM

(Zdroj: Vlastní zpracování dle: [21], s. 2)

Systém SIEM není vhodný pro všechna prostředí. Zatímco firewall nebo antispam má smysl implementovat do infrastruktury v podstatě každé společnosti, systém SIEM představuje robustní řešení, které vyžaduje poměrně dost zdrojů, ať už lidských (k jeho údržbě a zpracovávání bezpečnostních upozornění), finančních (na jeho zavedení) nebo technických (pro jeho správné fungování). Údržba by měla být prováděna denně, přičemž její náročnost se zvyšuje s velikostí monitorované infrastruktury. Systémy SIEM jsou také velice náchylné na sebemenší změny uvnitř monitorované infrastruktury, kdy i malá změna může způsobit generování mnoha falešně pozitivních (false positive) bezpečnostních upozornění. Rozhodnutí, zda systém SIEM využít, záleží na velikosti společnosti, včetně velikosti její infrastruktury, hodnotě chráněných aktiv a náročnosti implementace a údržby [17, s. 461].

Mimo jiné, během vypracovávání této diplomové práce probíhalo v České republice schvalování *nového zákona o kybernetické bezpečnosti* (dále jen nZoKB) a s ním spojených nových vyhlášek. Ten zpracoval Národní úřad pro kybernetickou a informační bezpečnost (dále jen NÚKIB) za účelem adaptace požadavků evropské směrnice *Network and Information Security 2* (dále jen NIS2) do českého právního řádu. Subjekty regulované dle tohoto nového zákona budou plnit stanovené povinnosti až se vstupem nového zákona v platnost, což bude pravděpodobně v polovině roku 2025. Nicméně jedním z požadavků pro regulované subjekty v rámci technických opatření bude povinnost využívat nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, což by měly pokrýt funkcionality, které nabízí právě systémy SIEM. Tím se dá

očekávat, že pravděpodobně vzroste poptávka po tomto nástroji, aby regulované subjekty splňovaly požadavky nZoKB [22] [23].

2 ANALÝZA SOUČASNÉHO STAVU

Následující část diplomové práce v úvodu obsahuje základní informace o analyzované společnosti, která je z důvodu zachování její anonymity pojmenována jako XYZ a.s. Tato kapitola poté pokračuje zmapováním informačního prostředí společnosti XYZ, návrhem hodnotících kritérií a atributů pro fuzzy model a analýzou dostupných systémů SIEM.

2.1 Základní informace o společnosti

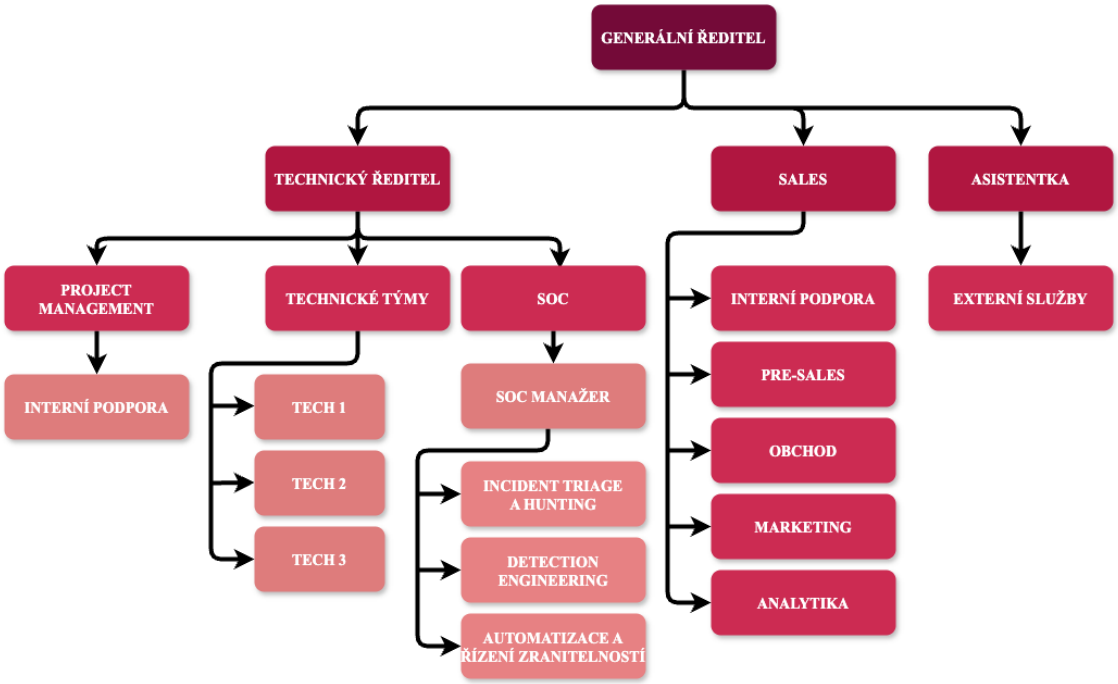
Název společnosti:	XYZ a.s.
Právní forma:	akciová společnost
Základní kapitál:	2 000 000 Kč
Hlavní ekonomická činnost (CZ-NACE):	62090 – Ostatní činnosti v oblasti informačních technologií
Ostatní ekonomické činnosti (CZ-NACE):	J – Informační a komunikační činnosti; 00 – Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona; 855 – Ostatní vzdělávání; 7219 – Ostatní výzkum a vývoj v oblasti přírodních a technických věd
Počet zaměstnanců:	48

2.2 Představení společnosti

Společnost XYZ byla založena roku 2009 a z pohledu účetnictví splňuje parametry malé účetní jednotky, ale i přes tento fakt bude pravděpodobně zasažena nZoKB jakožto poskytovatel řízené bezpečnostní služby. Společnost působí zejména na českém trhu, kde se prezentuje jako systémový integrátor v oblasti komplexní bezpečnosti, což zahrnuje bezpečnost informačních technologií, včetně jejich fyzické bezpečnosti a ochrany informací. Do portfolia nabízených služeb patří poskytování odborných návrhů pro vybudování, provoz a zdokonalení systému řízení bezpečnosti ICT, analytické služby, návrhy, realizace a provoz optimálních řešení sloužící k ochraně informačních aktiv a kritických procesů zákazníka. Společnost nově provozuje své bezpečnostní operační centrum (Security Operations Center, dále jen SOC), které nabízí zákazníkům eliminaci

rizik spojených s kybernetickými bezpečnostními hrozbami s využitím bezpečnostního monitoringu. Mezi ostatní služby poskytované společností XYZ patří např. provádění školení z oblasti kybernetické bezpečnosti, audity kybernetické společnosti aj.

2.3 Organizační struktura společnosti



Obrázek č. 22: Organizační struktura společnosti XYZ

(Zdroj: Vlastní zpracování dle: interní dokumentace společnosti XYZ)

Na obrázku č. 22 je znázorněna organizační struktura společnosti XYZ, kterou řídí generální ředitel. Ten se částečně angažuje v Sales týmu a úzce spolupracuje s technickým ředitelem. Má svou asistentku, jež je odpovědná za externí služby, jako jsou např. účetnictví, školení bezpečnosti a právní služby.

Na Sales tým spadají činnosti spojené s marketingem, obchodem a analytikou. Věnuje se tedy průzkumu trhu, hledání nových potenciálních zákazníků a partnerů, zákaznické podpoře, připravování a uzavírání obchodních smluv, pořádání konferencí, ale také správou sociálních sítí a webových stránek společnosti XYZ nebo audity kybernetické bezpečnosti. Právě pro tyto potřeby je Sales tým rozdělen na menší týmy (Interní podpora, Pre-sales, Obchod, Marketing a Analytika).

Technický ředitel je odpovědný za celý technický úsek společnosti XYZ. Navrhuje a rozhoduje o způsobu implementace technických řešeních, schvaluje nové interní procesy nebo úpravy těch současných. Spolu s generálním ředitelem nejčastěji vedou různá obchodní jednání. Technický ředitel má pod sebou několik technických týmů, jenž mají určeného svého týmového vedoucího, který za daný tým zodpovídá. Tým TECH 1 se zabývá činnostmi a nástroji spojenými se správou bezpečnostních záznamů, tedy log managementem. Tým TECH 2 má na starosti technologie zabývající se ochranou koncových bodů v síti a tým TECH 3 spravuje servery, privátní sítě a vybrané technologie, kterými jsou např. interní XWiki nebo ticketing systém. Tým Project Management spolu s Interní podporou se pak stará o poskytování potřebných podkladů technickým týmům a dohlíží na řádném plnění zadaných úkolů a stanovených cílů.

Tým SOC je veden SOC manažerem a dělí se dále na tři menší týmy. Tým Incident Triage a Hunting řeší kybernetické bezpečnostní události, kybernetické bezpečnostní incidenty a provádí tzv. hunting, což je proaktivní přístup, který spočívá v aktivním a iterativním vyhledávání pokročilých kybernetických bezpečnostních hrozeb. Členové týmu Detection Engineering navrhují a optimalizují pravidla pro detekci kybernetických bezpečnostních událostí a vytváří postupy pro vyhodnocování vzniklých kybernetických bezpečnostních událostí. Tým Automatizace a řízení zranitelností poté řeší automatizaci interních procesů, tvoří reporty pro zákazníky SOC a také sleduje aktuální zranitelnosti, o kterých následně informuje zainteresované strany.

2.4 Informační a komunikační technologie společnosti

Společnost XYZ vlastní několik serverů. Ty, které se týkají vývoje a testování, provozuje společnost XYZ ve vlastní serverovně. Ostatní servery, zejména provozní, jsou umístěny v datacentru externí společnosti z důvodu poskytnuté vyšší míry zabezpečení. Na většině serverech je využívána virtualizace. Největší podíl na těchto serverech má serverový operační systém Linux, především jeho distribuce CentOS.

Podvojné účetnictví, správu mezd, fakturaci a daňovou evidenci spravuje společnost XYZ v účetním programu Money S3. Důležitou roli v chodu společnosti XYZ zastává soubor cloudových služeb Microsoft 365 Copilot. V rámci předplatného Microsoft 365 Copilot společnost XYZ využívá Microsoft SharePoint ke sdílení firemních dokumentů,

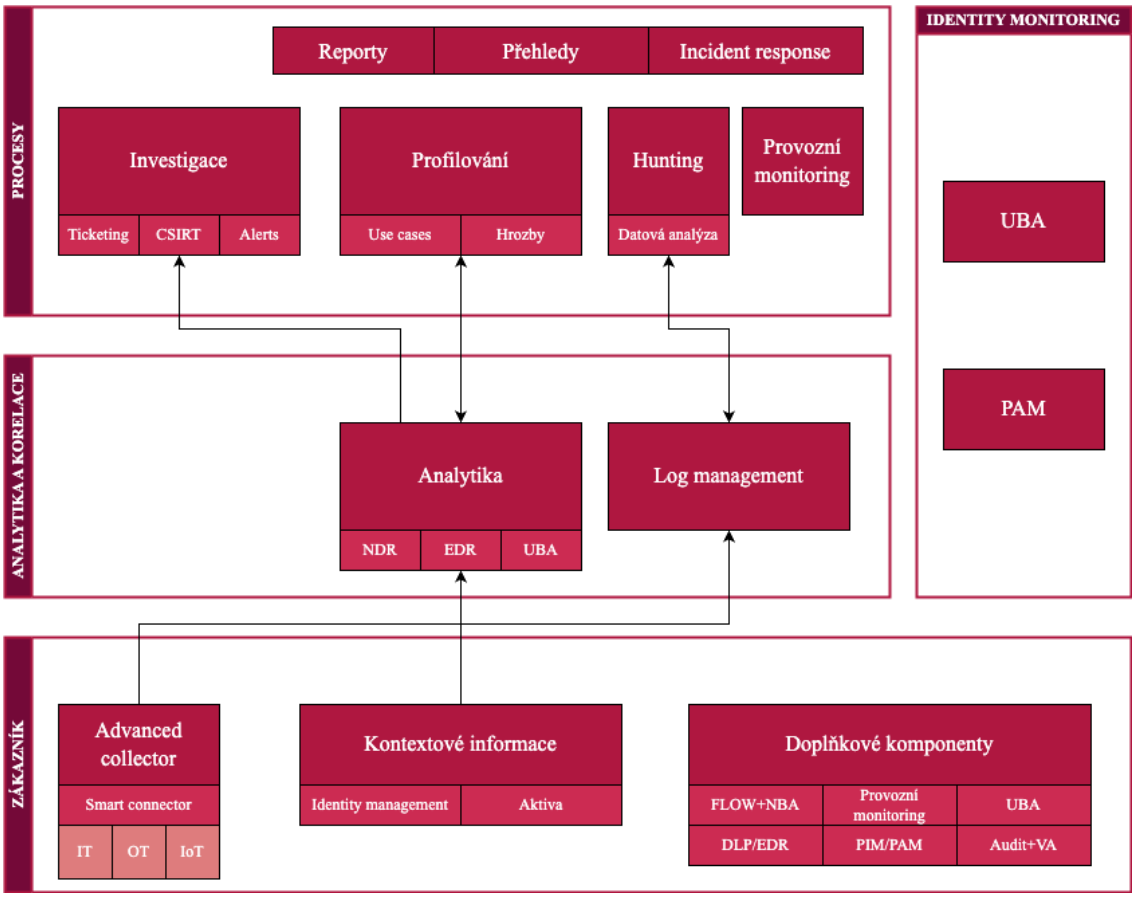
programová aplikace Microsoft Teams slouží jako hlavní komunikační kanál spolu s e-mailovým klientem Microsoft Outlook a pro tvorbu potřebné dokumentace jsou užívány programová aplikace Microsoft Word, Microsoft Excel, Microsoft PowerPoint, případně Microsoft Visio.

Komunikace se zákazníky probíhá především skrze ticketing systém Easy Redmine. Interní procesy, návody, postupy a další dokumentaci společnost XYZ eviduje ve své interní XWiki. Technické týmy pracují se systémem Git, který podporuje lepší správu verzí souborů, zejména zdrojových kódů.

Provozní monitoring serverů, síťových zařízení a dalších technologií zajišťuje open-source monitorovací systém Centreon. Pro monitorování síťového provozu na bázi analýzy datových toků (tzv. NetFlow) a chování sítě je implementován nástroj Flowmon od společnosti Progress. Koncová zařízení jsou zabezpečena nástrojem na detekci a reakci na kybernetické bezpečnostní hrozby od společnosti ESET.

Pro sběr, zpracování, distribuci a ukládání bezpečnostních záznamů využívá společnost XYZ pokročilý nástroj syslog-ng a službu Windows Event Forwarding v kombinaci s Windows Event Collector. Díky těmto řešením je společnost XYZ schopna sbírat bezpečnostní záznamy ze serverů, aplikací, síťových prvků, adresářových služeb, databází, webových serverů, firewallů, provozního monitoringu apod. Společnost XYZ také sbírá auditní a Exchange mailové bezpečnostní záznamy z cloudové služby Microsoft 365 Copilot.

Veškeré sesbírané bezpečnostní záznamy jsou napojeny do robustního nástroje ArcSight Logger od společnosti Open Text, který usnadňuje společnosti XYZ správu bezpečnostních záznamů. Umožňuje totiž jejich vysoký průtok a efektivní dlouhodobé ukládání. Tento nástroj také poskytuje rychlou analýzu bezpečnostních záznamů, generování reportů a též je vhodným nástrojem pro provádění huntingu [24].



Obrázek č. 23: Současná infrastruktura SOC společnosti XYZ

(Zdroj: Vlastní zpracování dle: interní dokumentace společnosti XYZ)

Log management je ve společnosti XYZ zaveden na dostatečně vysoké úrovni, viz obrázek č. 23. Je pokryta kompletní infrastruktura ICT (včetně cloudové služby), což společnosti přináší zajištění souladu s předpisy, lepší efektivitu a detailní přehled o současném stavu infrastruktury.

Společnost XYZ se snaží využívat zejména programové aplikace a systémy s open-source licencí, jelikož toto řešení pro ni nepředstavuje finanční zatížení.

Konkrétnější informace a informace o využívání ostatních ICT ve společnosti XYZ podléhají dohodě o mlčenlivosti.

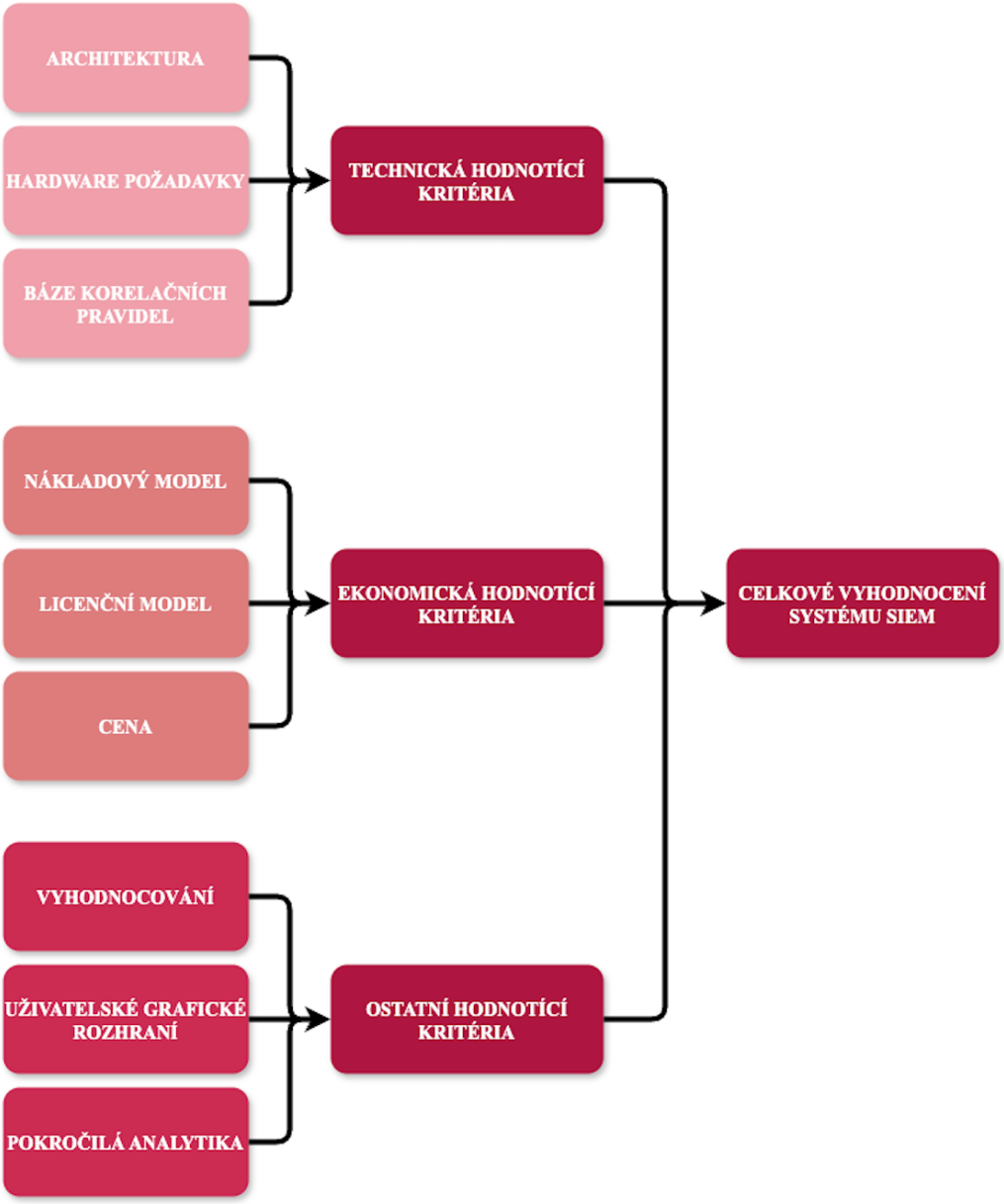
2.5 Hodnotící kritéria systémů SIEM

Technický ředitel má hlavní slovo při volbě hodnotících kritérií systémů SIEM, jelikož disponuje strategickým přehledem o celkové bezpečnostní architektuře společnosti XYZ.

Tento přehled mu umožňuje definovat kritéria, jež jsou klíčová pro dosažení dlouhodobých bezpečnostních cílů společnosti. Díky svým hlubokým znalostem a zkušenostem v oblasti kybernetické bezpečnosti, které má podložené získaným certifikátem Architekt kybernetické bezpečnosti, může identifikovat taková hodnotící kritéria, která zajistí kompatibilitu a integraci systému SIEM s ostatními bezpečnostními nástroji a systémy, případně s patřičnou legislativou. Technický ředitel také hraje klíčovou roli v optimalizaci nákladů, protože může definovat kritéria, která zajistí nejlepší poměr mezi cenou a výkonem, a zároveň splní bezpečnostní požadavky společnosti. Též jeho strategický přístup a schopnost řízení rizik jsou nezbytné pro výběr kritérií, která budou podporovat dlouhodobou bezpečnostní strategii společnosti XYZ.

Na výběru hodnotících kritérií by se měl podílet také expertní tým TECH 1, jelikož disponuje hlubokými znalostmi a zkušenostmi v oblasti log managementu. Tento tým má strategický přehled o stávajících logovacích systémech a nástrojích používaných ve společnosti XYZ, což jim umožňuje definovat kritéria, která zajistí, že systém SIEM bude kompatibilní s existujícími nástroji a snadno se integruje do současné infrastruktury.

Tedy na základě interních konzultací s technickým ředitelem společnosti XYZ a vedoucím expertního týmu TECH 1 bylo zvoleno devět hodnotících kritérií, která lze strukturovat do tří kategorií, a to *technická*, *ekonomická* a *ostatní* hodnotící kritéria systémů SIEM, viz obrázek č. 24.



Obrázek č. 24: Struktura hodnotících kritérií systémů SIEM

(Zdroj: Vlastní zpracování)

Jednotlivé atributy pro vybraná hodnotící kritéria spolu s váhami atributů byly též nadefinovány na základě interních konzultací s technickým ředitelem společnosti XYZ a vedoucím expertního týmu TECH 1.

2.5.1 Technická hodnotící kritéria

Architektura

Toto hodnotící kritérium představuje základní schopnost systému SIEM se přizpůsobovat aktuálním a budoucím potřebám společnosti XYZ. V rámci architektury lze posuzovat různé varianty, které se liší podle složitosti, schopnosti rozšiřování a škálovatelnosti. Každá z těchto variant ovlivňuje, jak efektivně a dlouhodobě bude systém SIEM reagovat na rostoucí objemy dat, kybernetické bezpečnostní hrozby a měnící se technologické požadavky.

Jednoduchá architektura je variantou, která se zaměřuje na snadnou implementaci a správu. Systém SIEM s touto architekturou není příliš komplexní, což usnadňuje jeho nasazení a údržbu. Tento typ architektury může být vhodnější pro menší společnosti, kde nejsou kladeny vysoké požadavky na rozsah a složitost bezpečnostního monitoringu.

Rozšiřitelná architektura nabízí větší flexibilitu a schopnost přidávat nové funkce či moduly. Tato architektura umožňuje snadnější integraci nových technologií, což zajišťuje dlouhodobou kompatibilitu s měnícími se požadavky společnosti.

Vysoce škálovatelná architektura je nejvíce vážená varianta, protože systém SIEM musí být schopný efektivně zvládat stále rostoucí objemy dat a kybernetických bezpečnostních událostí. Systém SIEM s touto architekturou je schopen se flexibilně přizpůsobovat růstu společnosti a rostoucím požadavkům na výkonnost bez ztráty efektivity. Vysoká škálovatelnost je klíčová pro větší společnosti nebo prostředí, kde objem dat roste exponenciálně (tedy např. v SOC).

Atributy pro toto hodnotící kritérium jsou tedy: *jednoduchá*, *rozšiřitelná* a *vysoce škálovatelná*.

Hardware požadavky

Hardware požadavky ovlivňují výkon, škálovatelnost a celkovou efektivitu systému SIEM, což je důležité pro efektivní detekci, analýzu a reakci na kybernetické bezpečnostní události.

Nízké hardware požadavky má systém SIEM, který dokáže fungovat na standardních serverech s nižšími specifikacemi, např. do 32 gigabytů (dále jen GB) počítačové paměti (Random Access Memory, dále jen RAM) a standardními pevné disky. Tento typ konfigurace může být vhodný pro menší společnosti nebo prostředí s omezeným rozpočtem, kde není potřeba zpracovávat velké objemy dat. U takového systému SIEM je ale třeba brát v úvahu, že jeho výkon může být omezený při složitějších operacích i rychlému růstu objemu dat.

Střední hardware požadavky představují vyvážený kompromis mezi výkonem a náklady na hardware. Jsou vhodnější pro střední společnosti, které mají větší objem dat, ale stále nevyžadují extrémně výkonný hardware. Takový server může obsahovat např. 32-64 GB RAM, standardní pevné i rychlejší polovodičové disky (Solid-State Drive, dále jen SSD). Systém SIEM s těmito požadavky je schopen efektivně zvládat průměrné objemy bezpečnostních záznamů.

Vysoké hardware požadavky se vztahují na systém SIEM, který vyžaduje výkonné servery s vyššími nároky na procesory, paměť a úložný prostor, tedy např. více než 64 GB RAM a výkonné SSD disky, případně s rozhraním pro nevolatilní paměť (Non-Volatile Memory Express, dále jen NVMe). Tento typ konfigurace je vhodný pro větší společnosti, které zpracovávají velké objemy dat a potřebují zajistit vysoký výkon pro detekci a analýzu v reálném čase.

Speciální hardware požadavky představují vysoce specifické nároky na hardware, které zahrnují např. specializované servery, operační systémy, procesory a úložiště, hardwarové akcelerátory pro urychlení analýzy dat, vysokou RAM apod. Tento typ konfigurace je vyžadován v extrémně náročných prostředích, kde je potřeba zpracovávat obrovské objemy dat v reálném čase nebo provádět složité analýzy.

Atributy daného hodnotícího kritéria jsou: *nízké*, *střední*, *vysoké* a *speciální*.

Báze korelačních pravidel

Báze korelačních pravidel definuje, jak efektivně systém SIEM dokáže analyzovat a korelovat kybernetické bezpečnostní události. Korelační pravidla slouží k identifikaci vzorců chování, které mohou indikovat potenciální kybernetické bezpečnostní hrozby nebo anomálie v běžném provozu. Kvalita a flexibilita těchto pravidel má zásadní vliv

na schopnost systému SIEM detekovat a případně reagovat na kybernetické bezpečnostní incidenty.

Omezená báze korelačních pravidel označuje základní soubor pravidel (přibližně 1000 korelačních pravidel), která pokrývají pouze ty nejobecnější scénáře a vzory, které jsou běžné v menších společnostech.

Standardní báze korelačních pravidel poskytuje širší soubor pravidel (obvykle 1000 až 2000 korelačních pravidel), která pokrývají běžné kybernetické bezpečnostní incidenty a umožňují efektivní detekci standardních kybernetických bezpečnostních událostí. Systém SIEM s takovouto bází korelačních pravidel je vhodný zejména pro malé a střední společnosti, které potřebují detekovat a reagovat na nejznámější kybernetické bezpečnostní události (např. pokusy o neoprávněný přístup nebo neobvyklé síťové aktivity), aniž by byly příliš náročné na implementaci a údržbu. Soubor pravidel lze rozšiřovat či jinak upravovat.

Pokročilá báze korelačních pravidel zahrnuje sofistikovanější pravidla (základní počet korelačních pravidel se obvykle pohybuje od 2000 a více), která dokážou detekovat komplexnější vzory a scénáře. Systém SIEM spolu s touto bází korelačních pravidel je nejvhodnější zejména pro společnosti s vyššími požadavky na informační a kybernetickou bezpečnost, které potřebují detekovat pokročilé kybernetické bezpečnostní události nebo anomálie, jako jsou např. cílené útoky nebo útoky využívající specifické techniky. Jsou také vyžadovány hlubší znalosti pro její správu.

Dynamická báze korelačních pravidel představuje nejflexibilnější a nejkomplexnější variantu, která umožňuje dynamickou tvorbu a úpravu korelačních pravidel na základě současných podmínek a nově identifikovaných kybernetických bezpečnostních hrozeb. Systém SIEM, který disponuje dynamickou bází korelačních pravidel je vhodný pro společnosti, které čelí neustále se vyvíjejícím kybernetickým bezpečnostním hrozbám a jež potřebují rychle reagovat na nové bezpečnostní výzvy. Dynamická báze korelačních pravidel je schopná automaticky upravit pravidla a vzory dle aktuálního provozu v infrastruktuře ICT, což poskytuje flexibilitu a efektivitu v reálném čase.

Atributy tohoto hodnotícího kritéria proto jsou: *omezená*, *standardní*, *pokročilá* a *dynamická*.

Tabulka č. 1: Technická hodnotící kritéria – slovně

(Zdroj: Vlastní zpracování)

TECHNICKÁ HODNOTÍCÍ KRITÉRIA - slovně			
N	**ARCHITEKTURA**	**HARDWARE POŽADAVKY**	**BÁZE KORELAČNÍCH PRAVIDEL**
1	VYSOCE ŠKÁLOVATELNÁ	SPECIÁLNÍ	DYNAMICKÁ
2	ROZŠIŘITELNÁ	VYSOKÉ	POKROČILÁ
3	JEDNODUCHÁ	STŘEDNÍ	STANDARDNÍ
4		NÍZKÉ	OMEZENÁ

Tabulka č. 2: Technická hodnotící kritéria – číselně

(Zdroj: Vlastní zpracování)

TECHNICKÁ HODNOTÍCÍ KRITÉRIA - číselně			
N	**ARCHITEKTURA**	**HARDWARE POŽADAVKY**	**BÁZE KORELAČNÍCH PRAVIDEL**
1	60	10	50
2	30	20	40
3	10	30	10
4		40	0

V tabulce č. 1 jsou znázorněna technická hodnotící kritéria systémů SIEM spolu s nadefinovanými atributy. V tabulce č. 2 jsou jednotlivým atributům přiřazeny váhy, které byly stanoveny na základě interních konzultací s technickým ředitelem společnosti XYZ a vedoucím expertního týmu TECH 1.

2.5.2 Ekonomická hodnotící kritéria

Nákladový model

Nákladový model systému SIEM definuje, jakým způsobem budou náklady na jeho implementaci a provozování rozloženy v průběhu času. Ovlivňuje také finanční plánování společnosti, její schopnost přizpůsobit se měnícím se požadavkům a efektivní řízení rozpočtu.

Model kapitálových výdajů (Capital Expenditures, dále jen CapEx) představuje takový nákladový model, kde většina nákladů na pořízení a implementaci systému SIEM je vynaložena jednorázově na začátku, což znamená vysoké počáteční investice. Tento model je proto vhodný pro společnosti, které mají dostatek finančních prostředků na pokrytí jednorázových nákladů, ale preferují mít kontrolu nad hardware a software

v dlouhodobém horizontu. Může být také výhodný pro společnosti, které plánují dlouhodobé používání systému SIEM a mají stabilní finanční prostředky pro jednorázovou investici. Avšak, není příliš vhodný pro společnosti s omezeným počátečním rozpočtem, protože velké počáteční výdaje mohou představovat výraznou finanční zátěž.

Model provozních výdajů (Operational Expenditures, dále jen OpEx) se zaměřuje na pravidelné provozní náklady, které jsou rozloženy v průběhu času (místo jednorázových investic). Tento model je vhodný zejména pro společnosti, které preferují rozložení nákladů na menší a pravidelně se vyskytující platby, což zajišťuje větší finanční flexibilitu. Tento model je často spojen s cloudovými řešeními nebo službami založenými na předplatném, kde společnosti platí pouze za skutečné využívání systému SIEM. Tento přístup může být výhodný pro společnosti s nižšími počátečními finančními prostředky, ale dlouhodobě mohou být celkové náklady vyšší než při modelu CapEx, zejména pokud si společnost udržuje dlouhodobý kontrakt.

Hybridní model kombinuje výhody modelů CapEx a OpEx, což společnostem umožňuje využívat jak jednorázové investice, tak i pravidelné provozní náklady. Tento model může zahrnovat např. pořízení hardware a software (model CapEx) spolu s platbami za provozní náklady (model OpEx) na služby, jako jsou cloudové úložiště nebo pravidelná údržba. Hybridní model je vhodný zejména pro společnosti, které chtějí mít určitou kontrolu nad hardwarem, ale zároveň potřebují flexibilitu a nižší počáteční náklady spojené s cloudovými službami nebo předplatnými. Tento model tedy poskytuje větší rovnováhu mezi počátečními náklady a dlouhodobými provozními náklady.

Atributy pro toto hodnotící kritérium jsou: *CapEx*, *OpEx* a *hybridní*.

Licenční model

Licenční model stanovuje, jak bude systém SIEM licencován a jaké náklady budou spojeny s jeho používáním. Může ovlivňovat flexibilitu systému SIEM a jeho schopnost růst v souladu s potřebami společnosti.

Gigabyty za den (dále jen GB/den) je licenční model, kde jsou náklady stanoveny na základě objemu dat, který je systém SIEM schopen zpracovat během jednoho dne. Tento model je vhodný pro společnosti, které generují větší množství dat, ale objem dat

lze snadno odhadnout. Tedy pro společnosti, které mají stabilní objem generovaných dat a které chtějí mít přehled o nákladech na základě skutečného využití. Tento model může být flexibilní, ale při rostoucím objemu dat může být nákladově náročnější, protože cena závisí na množství dat, která systém SIEM musí zpracovat.

Licenční model založený na počtu uživatelů představuje takový model, kde jsou náklady stanoveny dle počtu uživatelů, kteří mají přístup k systému SIEM. Je vhodný pro společnosti, kde je jasně stanoven počet osob, které potřebují mít přístup k systému SIEM (např. větší společnosti s vyšším počtem analytiků a bezpečnostních specialistů).

Licenční model na základě počtu zařízení, která jsou napojena do systému SIEM, je vhodný pro společnosti, které mají mnoho různých zařízení (např. servery, pracovní stanice, síťové prvky a jiná zařízení), která generují bezpečnostní záznamy. Tedy tento model může být efektivní pro společnosti s rozsáhlou infrastrukturou ICT, avšak je důležité sledovat, jak se tato infrastruktura mění a přizpůsobovat licencování podle aktuálního počtu zařízení.

Licencování dle počtu událostí za sekundu (Events Per Second, dále jen EPS) se zaměřuje na počet bezpečnostních záznamů, které je schopen systém SIEM zpracovat během jedné sekundy. Tento model je vhodný pro společnosti, které generují velké množství bezpečnostních záznamů a potřebují flexibilitu v tom, jaký objem dat budou schopny analyzovat a monitorovat. Model EPS je vhodný pro vyhodnocování v reálném čase.

Atributy tohoto hodnotícího kritéria jsou: *GB/den*, *počet uživatelů*, *počet zařízení* a *EPS*.

Cena

Toto ekonomické hodnotící kritérium představuje průměrné náklady na pořízení, implementaci a provozování a další parametry spojené se systémy SIEM. Může se může lišit v závislosti na různých faktorech, jako jsou např. licenční modely, požadavky na hardware, náklady na školení a údržbu apod.

Nízká cena označuje cenovou variantu, kdy se průměrné (roční) náklady spojené se systém SIEM pohybují obvykle do 250 000 Kč ročně. Zahrnuje také open-source systémy SIEM.

Střední cena představuje vyváženou variantu, která nabízí solidní množství funkcí a možností, a to za přiměřené náklady. Průměrné (roční) náklady takového systému SIEM se nejčastěji pohybují od 250 000 do 1 000 000 Kč. Systém SIEM s touto cenovou úrovní obvykle poskytuje široké spektrum funkcí v oblasti analýzy, reportování a integrace s jinými bezpečnostními nástroji.

Vysoká cena se vztahuje na systém SIEM, který poskytuje např. vysoce pokročilé funkce, robustní integrace, rozsáhlou škálovatelnost, výkonné analytické nástroje, možnost přizpůsobovat korelační pravidla apod. Vysoké průměrné (roční) náklady, které se pohybují od částky 1 000 000 Kč až do 1 500 000 Kč, odráží také vyšší náklady na instalaci, školení, pravidelnou údržbu a podporu.

Velmi vysoká cena odpovídá nejdražší variantě systému SIEM. Obvyklé průměrné (roční) náklady se pohybují nad částkou 1 500 000 Kč. Takovýto systém SIEM již obvykle poskytuje vysokou škálovatelnost, pokročilou a dynamickou korelaci kybernetických bezpečnostních událostí a je schopen zpracovávat obrovské objemy dat.

Atributy daného hodnotícího kritéria jsou: *nízká*, *střední*, *vysoká* a *velmi vysoká*.

Tabulka č. 3: Ekonomická hodnotící kritéria – slovně
(Zdroj: Vlastní zpracování)

EKONOMICKÁ HODNOTÍCÍ KRITÉRIA - slovně			
N	**NÁKLADOVÝ MODEL**	**LICENČNÍ MODEL**	**CENA**
1	HYBRIDNÍ	EPS	VELMI VYSOKÁ
2	OPEX	POČET ZAŘÍZENÍ	VYSOKÁ
3	CAPEX	POČET UŽIVATELŮ	STŘEDNÍ
4		GB/DEN	NÍZKÁ

Tabulka č. 4: Ekonomická hodnotící kritéria – číselně
(Zdroj: Vlastní zpracování)

EKONOMICKÁ HODNOTÍCÍ KRITÉRIA - číselně			
N	**NÁKLADOVÝ MODEL**	**LICENČNÍ MODEL**	**CENA**
1	60	50	10
2	15	5	20
3	25	15	30
4		30	40

V tabulce č. 3 jsou znázorněna ekonomická hodnotící kritéria systémů SIEM spolu s nadefinovanými atributy. V tabulce č. 4 jsou jednotlivým atributům přiřazeny váhy,

které byly stanoveny na základě interních konzultací s technickým ředitelem společnosti XYZ a vedoucím expertního týmu TECH 1.

2.5.3 Ostatní hodnotící kritéria

Vyhodnocování

Jedná se o rychlost, se kterou systém SIEM dokáže zpracovat, analyzovat a vyhodnocovat bezpečnostní záznamy, kybernetické bezpečnostní události apod.

Vyhodnocování s vysokou latencí označuje variantu, kde doba mezi přijetím bezpečnostního záznamu a jeho vyhodnocením může být relativně delší (v řádu vyšších jednotek až desítek minut). Systém SIEM s vyhodnocováním s vysokou latencí je vhodný pro společnosti, které mají nižší nároky na okamžitou detekci kybernetických bezpečnostních událostí a které jsou schopny tolerovat zpoždění při analýze kybernetických bezpečnostních incidentů.

Mírná latence představuje vyhodnocování bezpečnostních záznamů s určitou prodlevou (v řádu nižších jednotek minut), ale stále dostatečně rychle na to, aby bylo možné reagovat na případnou kybernetickou bezpečnostní událost nebo kybernetický bezpečnostní incident.

Vyhodnocování v reálném čase znamená, že systém SIEM vyhodnocuje bezpečnostní záznamy téměř okamžitě, což umožňuje včasnou detekci kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, včetně bezprostřední reakce na ně. Takový systém SIEM je vhodný pro společnosti, které čelí pokročilým kybernetickým bezpečnostním hrozbám a které potřebují okamžitě detekovat a reagovat na kybernetické bezpečnostní incidenty. Reálný čas vyhodnocování je vhodný zejména pro kritické infrastruktury.

Automatizované vyhodnocování s využitím umělé inteligence (Artificial Intelligence, dále jen AI) představuje využívání AI a strojového učení k automatizovanému vyhodnocování bezpečnostních záznamů v reálném čase. Systém SIEM s tímto modelem je schopen analyzovat a korelovat kybernetické bezpečnostní události na základě vzorců chování, detekovat anomálie a kybernetické bezpečnostní hrozby bez lidského zásahu a automaticky reagovat na kybernetické bezpečnostní události.

Atributy daného hodnotícího kritéria jsou: *vysoká latence*, *mírná latence*, *reálný čas* a *automatizované AI*.

Uživatelské grafické rozhraní

Přístupnost a použitelnost uživatelského grafického rozhraní (Graphical User Interface, dále jen GUI) ovlivňuje efektivitu práce bezpečnostních analytiků a administrátorů systému SIEM. Kvalitní a intuitivní GUI umožňuje rychlé a efektivní monitorování, analýzu a reakci na kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty. Naopak špatně navržené nebo složité GUI může snížit produktivitu bezpečnostních analytiků.

Neintuitivní GUI má takový systém SIEM, který je složitý na ovládání, s obtížnou navigací a který často vyžaduje vyšší úroveň školení nebo zkušeností pro efektivní používání. Bezpečnostní analytici se mohou často setkat s problémy při hledání potřebných funkcí, při analýze kybernetických bezpečnostních událostí nebo s nedostatečnou dokumentací.

Standardním GUI se vyznačuje systém SIEM, který je relativně snadno použitelný a intuitivní pro většinu uživatelů, ale stále může vyžadovat určité školení nebo zvyknutí si na specifické funkce a nastavení. Tento typ GUI obvykle nabízí přehlednou strukturu, rozumné uspořádání a dostatečnou podporu pro základní analýzu a správu.

Systém SIEM může poskytovat i pokročilé GUI, které je navrženo pro odborníky a pokročilé uživatele, kteří vyžadují větší úroveň přizpůsobení a komplexnosti. Takové rozhraní obvykle nabízí rozsáhlé možnosti konfigurace, pokročilé analytické nástroje a nástroje pro detailní analýzu dat, což umožňuje vysoce efektivní správu. Systém SIEM s pokročilým GUI je vhodný pro společnosti, které mají zkušené bezpečnostní analytiky a administrátory, kteří potřebují rychlý přístup k podrobným informacím, vizualizacím a nastavením.

Atributy pro dané hodnotící kritérium: *neintuitivní*, *standardní* a *pokročilé*.

Pokročilá analytika

Pokročilá analytika umožňuje identifikaci komplexních vzorců chování, anomálií a neznámých kybernetických bezpečnostních hrozeb, což je nezbytné pro proaktivní

zabezpečení společnosti. Systém SIEM s vysoce vyvinutými analytickými schopnostmi může výrazně zlepšit kvalitu detekce a snížit riziko neodhalení potenciální kybernetické bezpečnostní hrozby.

Systém SIEM bez pokročilé analytiky se spoléhá zejména na základní korelace a vytvořené datové zdroje. Proto je vhodný především pro drobné a menší společnosti.

Základní pokročilá analytika v systému SIEM nabízí vyspělejší analytické nástroje, jako např. korelace mezi různými datovými zdroji, funkce pro zautomatizované vyhodnocování kybernetických bezpečnostních událostí na základě přednastavených pravidel apod.

Systém SIEM s dynamickou pokročilou analytikou představuje vysoce pokročilý systém využívající AI a strojové učení k dynamické analýze bezpečnostních záznamů a jiných dat. Nabízí tedy např. automatickou aktualizaci analytických modelů, provádění prediktivní analýzy atd.

Atributy tohoto hodnotícího kritéria jsou: *žádná*, *základní* a *dynamická*.

Tabulka č. 5: Ostatní hodnotící kritéria – slovně

(Zdroj: Vlastní zpracování)

OSTATNÍ HODNOTÍCÍ KRITÉRIA - slovně			
N	**VYHODNOCOVÁNÍ**	**UŽIVATELSKÉ GRAFICKÉ ROZHRANÍ**	**POKROČILÁ ANALYTIKA**
1	AUTOMATIZOVANÉ AI	POKROČILÉ	DYNAMICKÁ
2	REÁLNÝ ČAS	STANDARDNÍ	ZÁKLADNÍ
3	MÍRNÁ LATENCE	NEINTUITIVNÍ	ŽÁDNÁ
4	VYSOKÁ LATENCE		

Tabulka č. 6: Ostatní hodnotící kritéria – číselně

(Zdroj: Vlastní zpracování)

OSTATNÍ HODNOTÍCÍ KRITÉRIA - číselně			
N	**VYHODNOCOVÁNÍ**	**UŽIVATELSKÉ GRAFICKÉ ROZHRANÍ**	**POKROČILÁ ANALYTIKA**
1	50	60	50
2	40	40	40
3	10	0	10
4	0		

V tabulce č. 5 jsou znázorněna ostatní hodnotící kritéria systémů SIEM spolu s nadefinovanými atributy. V tabulce č. 6 jsou jednotlivým atributům přiřazeny váhy,

které byly stanoveny na základě interních konzultací s technickým ředitelem společnosti XYZ a vedoucím expertního týmu TECH 1.

2.6 Současná nabídka systémů SIEM

Sales tým společnosti XYZ provedl průzkum trhu se systémy SIEM a ve spolupráci s technickým ředitelem vymezili s pomocí metody *nejlepší praxe* (tzv. best practice) několik dostupných systémů. Přehled vymezených systémů SIEM s jejich ohodnocením dle nadefinovaných hodnotících kritérií je zobrazen v tabulkách č. 7 a 8.

Tabulka č. 7: Přehled ohodnocených systémů SIEM – slovně

(Zdroj: Vlastní zpracování dle: interní dokumentace společnosti XYZ)

SYSTÉM SIEM	TECHNICKÁ HODNOTÍCÍ KRITÉRIA			EKONOMICKÁ HODNOTÍCÍ KRITÉRIA			OSTATNÍ HODNOTÍCÍ KRITÉRIA		
	ARCHITEKTURA	HARDWARE POŽADAVKY	BÁZE KORELAČNÍCH PRAVIDEL	NÁKLADOVÝ MODEL	LICENČNÍ MODEL	CENA	VYHODNOCOVÁNÍ	UŽIVATELSKÉ GRAFICKÉ ROZHRANÍ	POKROČILÁ ANALYTIKA
LevelBlue Unified Security Management	Jednoduchá	Střední	Omezená	OpEx	Počet zařízení	Střední	Reálný čas	Standardní	Základní
BlackStratus SIEMStorm	Rozšiřitelná	Nízké	Omezená	OpEx	Počet zařízení	Nízká	Mírná latence	Neintuitivní	Základní
Exabeam Security Management Platform	Vysoce škálovatelná	Vysoké	Dynamická	CapEx	Počet uživatelů	Vysoká	Automatizované AI	Neintuitivní	Dynamická
IBM QRadar SIEM	Vysoce škálovatelná	Vysoké	Pokročilá	Hybridní	EPS	Velmi vysoká	Reálný čas	Standardní	Dynamická
LogRhythm SIEM	Rozšiřitelná	Vysoké	Standardní	Hybridní	Počet uživatelů	Vysoká	Reálný čas	Pokročilé	Základní
Trellix Enterprise Security Manager	Rozšiřitelná	Střední	Standardní	OpEx	Počet zařízení	Vysoká	Mírná latence	Neintuitivní	Základní
OpenText Enterprise Security Manager	Vysoce škálovatelná	Střední	Standardní	CapEx	EPS	Střední	Reálný čas	Standardní	Základní
OpenText Sentinel Enterprise	Rozšiřitelná	Vysoké	Standardní	OpEx	EPS	Vysoká	Mírná latence	Neintuitivní	Základní
Rapid7 InsightIDR	Vysoce škálovatelná	Nízké	Standardní	OpEx	Počet uživatelů	Střední	Automatizované AI	Standardní	Dynamická
NetWitness Logs	Vysoce škálovatelná	Vysoké	Pokročilá	Hybridní	EPS	Vysoká	Reálný čas	Neintuitivní	Základní
Securonix Unified Defense SIEM	Vysoce škálovatelná	Vysoké	Dynamická	OpEx	GB/den	Střední	Automatizované AI	Pokročilé	Dynamická
SolarWinds Security Event Manager	Jednoduchá	Střední	Omezená	CapEx	Počet zařízení	Nízká	Reálný čas	Standardní	Základní
Splunk Enterprise Security	Vysoce škálovatelná	Vysoké	Dynamická	Hybridní	GB/den	Velmi vysoká	Reálný čas	Pokročilé	Dynamická
Trustwave SIEM Operations Edition	Rozšiřitelná	Střední	Standardní	OpEx	Počet zařízení	Střední	Mírná latence	Standardní	Základní
TeskaLabs SIEM	Jednoduchá	Nízké	Standardní	Hybridní	EPS	Nízká	Reálný čas	Standardní	Základní

Tabulka č. 8: Přehled ohodnocených systémů SIEM – číselně

(Zdroj: Vlastní zpracování dle: interní dokumentace společnosti XYZ)

SYSTÉM SIEM	TECHNICKÁ HODNOTÍCÍ KRITÉRIA			EKONOMICKÁ HODNOTÍCÍ KRITÉRIA			OSTATNÍ HODNOTÍCÍ KRITÉRIA		
	ARCHITEKTURA	HARDWARE POŽADAVKY	BÁZE KORELAČNÍCH PRAVIDEL	NÁKLADOVÝ MODEL	LICENČNÍ MODEL	CENA	VYHODNOCOVÁNÍ	UŽIVATELSKÉ GRAFICKÉ ROZHRANÍ	POKROČILÁ ANALYTIKA
LevelBlue Unified Security Management	10	30	0	15	5	30	40	40	40
BlackStratus SIEMStorm	30	40	0	15	5	40	10	0	40
Exabeam Security Management Platform	60	20	50	25	15	20	50	0	50
IBM QRadar SIEM	60	20	40	60	50	10	40	40	50
LogRhythm SIEM	30	20	10	60	15	20	40	60	40
Trellix Enterprise Security Manager	30	30	10	15	5	20	10	0	40
OpenText Enterprise Security Manager	60	30	10	25	50	30	40	40	40
OpenText Sentinel Enterprise	30	20	10	15	50	20	10	0	40
Rapid7 InsightIDR	60	40	10	15	15	30	50	40	50
NetWitness Logs	60	20	40	60	50	20	40	0	40
Securonix Unified Defense SIEM	60	20	50	15	30	30	50	60	50
SolarWinds Security Event Manager	10	30	0	25	5	40	40	40	40
Splunk Enterprise Security	60	20	50	60	30	10	40	60	50
Trustwave SIEM Operations Edition	30	30	10	15	5	30	10	40	40
TeskaLabs SIEM	10	40	10	60	50	40	40	40	40

S využitím *Saatyho metody*, která je též známá jako *Analytický hierarchický proces*, lze stanovit váhy jednotlivých hodnotících kritérií a následně vymezit nejpřijatelnější systémy SIEM.

Tabulka č. 9: Hodnotící stupnice Saatyho metody

(Zdroj: Vlastní zpracování dle: [25])

DŮLEŽITOST	DEFINICE
1	**Rovnocenné** hodnotící kritérium *i* s hodnotícím kritériem *j*
2	**Velmi slabě preferované** hodnotící kritérium *i* před hodnotícím kritériem *j*
3	**Slabě preferované** hodnotící kritérium *i* před hodnotícím kritériem *j*
4	**Středně preferované** hodnotící kritérium *i* před hodnotícím kritériem *j*
5	**Silně preferované** hodnotící kritérium *i* před hodnotícím kritériem *j*
6	**Silněji preferované** hodnotící kritérium *i* před hodnotícím kritériem *j*
7	**Velmi silně preferované** hodnotící kritérium *i* před hodnotícím kritériem *j*
8	**Opravu velmi silně preferované** hodnotící kritérium *i* před hodnotícím kritériem *j*
9	**Absolutně preferované** hodnotící kritérium *i* před hodnotícím kritériem *j*

V tabulce č. 9 je zobrazena hodnotící stupnice Saatyho metody, dle které je možné v Saatyho matici stanovit důležitost jednotlivých hodnotících kritérií. Hodnotící stupnice Saatyho metody byla konzultována s technických ředitelem společnosti XYZ.

Po vyplnění Saatyho matice lze následně pomocí podílu geometrického průměru jednotlivých řádků Saatyho matice s celkovým součtem daných geometrických průměrů získat váhy zvolených hodnotících kritérií.

Tabulka č. 10: Saatyho matice

(Zdroj: Vlastní zpracování)

i/j	Architektura	Hardware požadavky	Báze korelačních pravidel	Nákladový model	Licenční model	Cena	Vyhodnocování	Uživatelské grafické rozhraní	Pokročilá analytika	GEOMETRICKÝ PRŮMĚR	VÁHA
Architektura	1	3	0,5000	0,3333	0,2000	0,2500	0,1667	4	2	0,6853	0,0509
Hardware požadavky	0,3333	1	0,2500	0,2000	0,1429	0,1667	0,1250	2	0,5000	0,3324	0,0247
Báze korelačních pravidel	2	4	1	0,5000	0,2500	0,3333	0,2000	5	3	1,0000	0,0743
Nákladový model	3	5	2	1	0,3333	0,5000	0,2500	6	4	1,4592	0,1084
Licenční model	5	7	4	3	1	2	0,5000	8	6	3,0080	0,2235
Cena	4	6	3	2	0,5000	1	0,3333	7	5	2,1131	0,1570
Vyhodnocování	6	8	5	4	2	3	1	9	7	4,1472	0,3081
Uživatelské grafické rozhraní	0,2500	0,5000	0,2000	0,1667	0,1250	0,1429	0,1111	1	0,3333	0,2411	0,0179
Pokročilá analytika	0,5000	2	0,3333	0,2500	0,1667	0,2000	0,1429	3	1	0,4732	0,0352
									SUMA	**13,4596**	**1,0000**

Pomocí Saatyho matice, která je zobrazena v tabulce č. 10, bylo zjištěno, že největší váhu s hodnotou 0,3081 má hodnotící kritérium Vyhodnocování. Naopak hodnotící kritérium Uživatelské grafické rozhraní má nejmenší váhu s hodnotou 0,0179.

Se stanovenými váhami jednotlivých hodnotících kritérií, které byly vypočteny pomocí Saatyho metody, lze spočítat celkové skóre daných systémů SIEM, kdy pět systémů SIEM s nejvyšším skóre lze vyhodnotit pomocí fuzzy modelu v MATLAB. Stanovené váhy hodnotících kritérií jsou dále využity i v samotném fuzzy modelu při stanovení důležitosti znalostní báze.

Tabulka č. 11: Přehled systémů SIEM a jejich skóre

(Zdroj: Vlastní zpracování dle: interní dokumentace společnosti XYZ)

SYSTÉM SIEM	TECHNICKÁ HODNOTÍCÍ KRITÉRIA			EKONOMICKÁ HODNOTÍCÍ KRITÉRIA			OSTATNÍ HODNOTÍCÍ KRITÉRIA			SKÓRE	POŘADÍ
	ARCHITEKTURA	HARDWARE POŽADAVKY	BÁZE KORELAČNÍCH PRAVIDEL	NÁKLADOVÝ MODEL	LICENČNÍ MODEL	CENA	VYHODNOCOVÁNÍ	UŽIVATELSKÉ GRAFICKÉ ROZHRANÍ	POKROČILÁ ANALYTIKA		
VÁHA	0,0509	0,0247	0,0743	0,1084	0,2235	0,1570	0,3081	0,0179	0,0352		
LevelBlue Unified Security Management	10	30	0	15	5	30	40	40	40	23,1514	12.
BlackStratus SIEMStorm	30	40	0	15	5	40	10	0	40	16,0265	13.
Exabeam Security Management Platform	60	20	50	25	15	20	50	0	50	33,6302	7.
IBM QRadar SIEM	60	20	40	60	50	10	40	40	50	**40,5692**	**3.**
LogRhythm SIEM	30	20	10	60	15	20	40	60	40	30,5676	9.
Trellix Enterprise Security Manager	30	30	10	15	5	20	10	0	40	13,3826	15.
OpenText Enterprise Security Manager	60	30	10	25	50	30	40	40	40	**37,5810**	**5.**
OpenText Sentinel Enterprise	30	20	10	15	50	20	10	0	40	23,1923	11.
Rapid7 InsightIDR	60	40	10	15	15	30	50	40	50	32,3548	8.
NetWitness Logs	60	20	40	60	50	20	40	0	40	**41,0709**	**1.**
Securonix Unified Defense SIEM	60	20	50	15	30	30	50	60	50	**38,5432**	**4.**
SolarWinds Security Event Manager	10	30	0	25	5	40	40	40	40	25,8056	10.
Splunk Enterprise Security	60	20	50	60	30	10	40	60	50	37,2008	6.
Trustwave SIEM Operations Edition	30	30	10	15	5	30	10	40	40	15,6691	14.
TeskaLabs SIEM	10	40	10	60	50	40	40	40	40	**40,6468**	**2.**

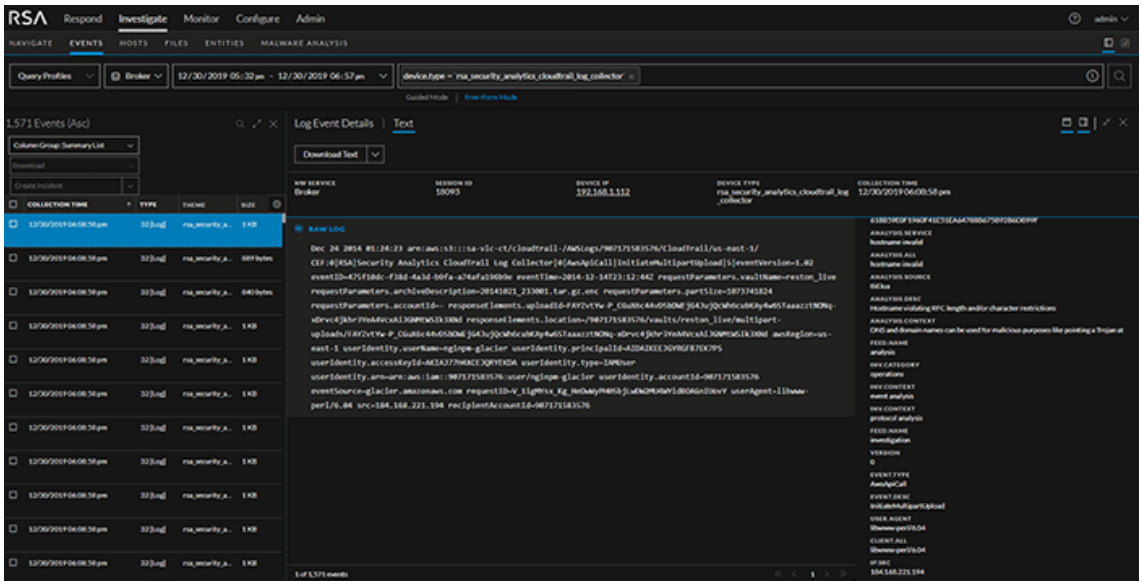
V tabulce č. 11 je na základě číselných hodnot atributů a vah hodnotících kritérií vypočítáno celkové skóre jednotlivých systémů SIEM. Pět nejvyšších hodnot konečného skóre dosáhly systémy SIEM *NetWitness Logs*, *TeskaLabs SIEM*, *IBM QRadar SIEM*, *Securonix Unified Defense SIEM* a *OpenText Enterprise Security Manager*.

2.6.1 NetWitness Logs

NetWitness Logs, vyvíjený společností RSA (dnes součástí platformy NetWitness), představuje moderní a výkonný systém SIEM určený k pokročilé analýze a korelaci bezpečnostních záznamů. Je navržen pro korelaci a analýzu dat z více než 350 zdrojů (včetně cloudových služeb, aplikací a síťových zařízení), s cílem identifikovat a prioritizovat kybernetické bezpečnostní hrozby v reálném čase. Z hlediska analytických schopností nabízí NetWitness Logs pokročilou analytiku, která využívá automatizace za účelem zefektivnění identifikace anomálií a potenciálních kybernetických bezpečnostních incidentů. Systém disponuje pokročilou sadou korelačních pravidel, která lze dále přizpůsobovat dle potřeb společnosti, čímž umožňuje efektivní reakci na známé i neznámé kybernetické bezpečnostní hrozby. Potenciální zájemci mohou požádat o demoverzi [26].

Architekturou se jedná o vysoce škálovatelný systém SIEM, jenž je vhodný pro komplexní prostředí s rozsáhlým provozem ICT. Pro zajištění vysokého výkonu jsou doporučeny vysoké hardwarové požadavky, tedy servery s více než 64 GB RAM, SSD NVMe a výkonné vícejádrové procesory. NetWitness Logs GUI nabízí řadu možností, avšak není dostatečně přívětivé, je složitější k navigaci a jeho dokumentace není příliš rozsáhlá.

Licencování je obvykle založeno na modelu EPS. Náklady lze kombinovat ve formě OpEx i CapEx, přičemž průměrné roční náklady se pohybují běžně kolem 800 000 až 1 500 000 Kč (v závislosti na rozsahu nasazení, počtu EPS a úrovni integrací).



Obrázek č. 25: Ukázka prostředí NetWitness Logs

(Zdroj: [26])

2.6.2 TeskaLabs SIEM

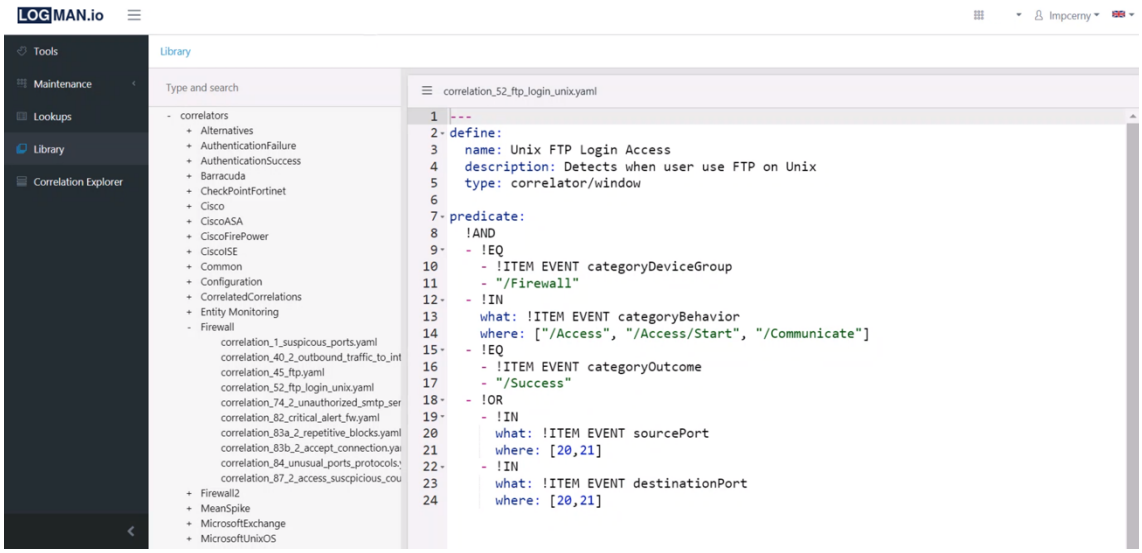
TeskaLabs SIEM je moderní systém SIEM vyvíjený českou technologickou společností TeskaLabs. Zaměřuje se na poskytování centralizovaného přehledu nad kybernetickou bezpečností jednotlivých společností v reálném čase a podporuje zejména prostředí vyžadující vysoký stupeň zabezpečení, jako jsou mobilní sítě, průmyslové systémy a prostředí s kritickou infrastrukturou. TeskaLabs SIEM je otevřená platforma, tedy nehrozí proprietární uzamčení (tzv. vendor lock-in). Nabízí také rozsáhlé možnosti využití pro Business Inteligence, Big Data aj. Disponuje přívětivě navrženým GUI pro snadné používání i bez pokročilé technické expertízy, které je navíc dostupné nejen v anglickém, ale i v českém jazyce [27].

Jeho jednoduchá architektura umožňuje flexibilní nasazení v různých prostředích. Z hlediska hardware požadavků je TeskaLabs SIEM poměrně nenáročný a k provozu si běžně vystačí i s méně něž 32 GB RAM a pevnými disky. Nabízí standardní bázi korelačních pravidel, která umožňuje bezpečnostním analytikům definovat a spravovat korelační pravidla pro detekci běžných i mírně pokročilých kybernetických bezpečnostních událostí.

Licenční model TeskaLabs SIEM je založen na modelu EPS. Vzhledem ke své jednoduchosti a přizpůsobitelnosti spadá cenově do nižší nákladové kategorie,

kdy se průměrné roční náklady mohou pohybovat kolem 250 000 Kč (v závislosti na rozsahu a způsobu nasazení). Nákladový model je založen na kombinaci CapEx i OpEx.

TeskaLabs SIEM disponuje pokročilou analytikou, která usnadňuje korelaci kybernetických bezpečnostních událostí z různých zdrojů, vizualizaci kybernetických bezpečnostních hrozeb a tvorbu detekčních scénářů. Dále umožňuje konfigurovatelné přehledy, sledování provozních metrik, vyhodnocování i vizualizaci kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů v reálném čase.



Obrázek č. 26: Ukázka prostředí TeskaLabs SIEM

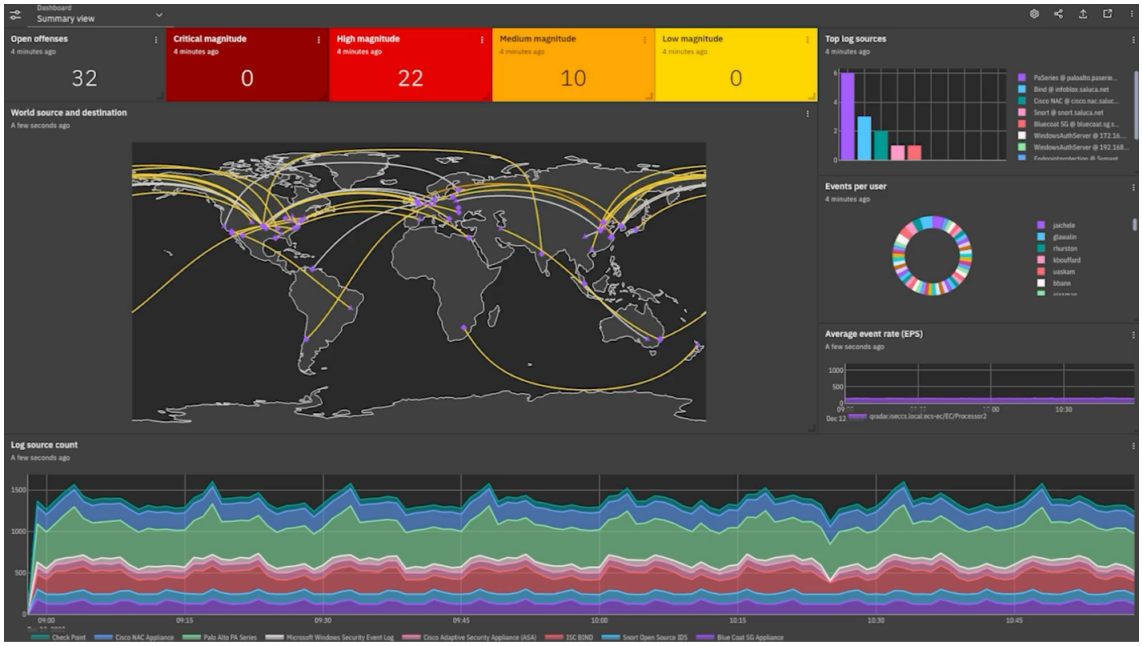
(Zdroj: [27])

2.6.3 IBM QRadar SIEM

QRadar SIEM, který je vyvíjen a udržován společností IBM, představuje komplexní řešení, které společnostem poskytuje aktivní monitorování, odhalování a eliminaci kybernetických bezpečnostních hrozeb v reálném čase. Tento systém SIEM je navržen pro korelaci a analýzu rozsáhlých objemů dat pocházejících z různorodých zdrojů v rámci monitorované infrastruktury ICT s cílem identifikovat potenciální kybernetické bezpečnostní incidenty. Disponuje přívětivým GUI, dynamickou pokročilou analytikou s přístupem k nejnovějším detekčním obsahům. IBM nabízí zájemcům o QRadar SIEM možnost živé demoverze [28].

Z technického hlediska IBM QRadar SIEM vyniká vysoce škálovatelnou a modulární architekturou, která je schopna zpracovávat velké objemy dat v reálném čase. Podporuje distribuovaná nasazení a horizontální škálování, což je ideální pro velké společnosti s náročnými požadavky na výkon. Pro efektivní zpracování dat v reálném čase vyžaduje výkonný hardware, tedy servery s dostatečnou pamětí (až s více než 64 GB RAM), SSD NVMe a výkonné vícejádrové procesory. Báze korelačních pravidel je pokročilá a umožňuje bezpečnostním analytikům vytvářet složitější pravidla.

Nákladový model IBM QRadar SIEM kombinuje CapEx a OpEx. Licencování je založeno především na modelu EPS. Celkové náklady tohoto systému SIEM se mohou výrazně lišit v závislosti na velikosti nasazení, zvoleném modelu licencování a případných doplňkových funkcích, ale v průměru se pohybují kolem 1 800 000 Kč ročně.



Obrázek č. 27: Ukázka přehledu z IBM QRadar SIEM

(Zdroj: [28])

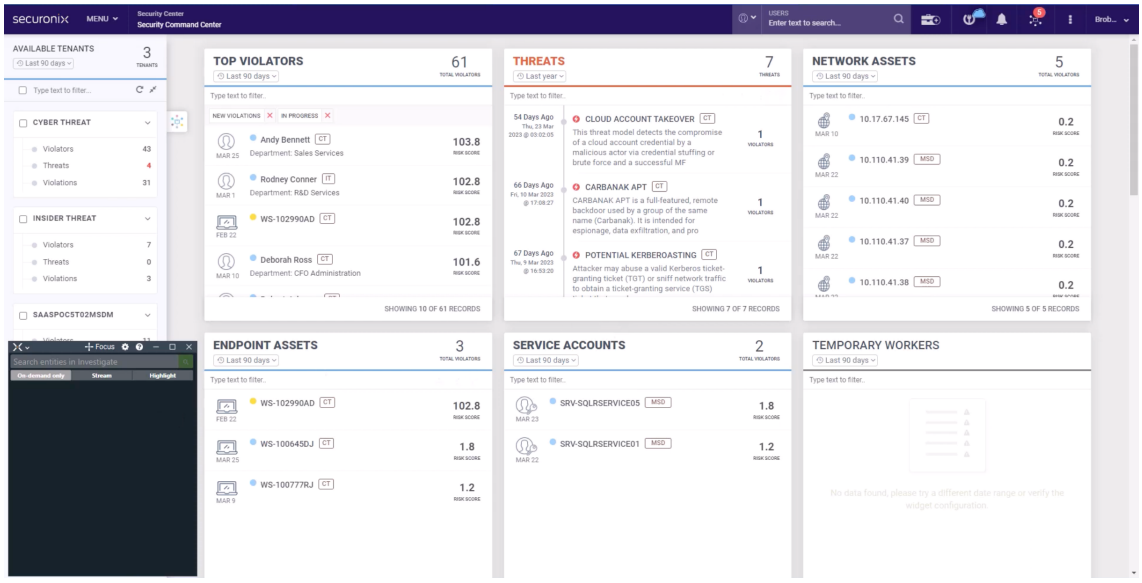
2.6.4 Securonix Unified Defense SIEM

Unified Defense SIEM, vyvíjený a udržovaný společností Securonix, představuje moderní cloudově orientované bezpečnostní řešení, které se zaměřuje na detekci kybernetických bezpečnostních hrozeb v reálném čase pomocí umělé inteligence a jejich zkoumání pomocí dynamické pokročilé analytiky. Nabízí pokročilé a moderní GUI, které

je velmi dobře hodnoceno odbornou komunitou pro svou přehlednost, jednoduchost použití a přizpůsobitelnost. Společnost Securonix nabízí zájemcům možnost zdarma si vyžádat demoverzi tohoto systému SIEM, aby mohli sami otestovat jeho funkce a výhody [29].

Securonix Unified Defense SIEM disponuje dynamickou bází korelačních pravidel, která se dokáže automaticky aktualizovat a přizpůsobovat nově vznikajícím kybernetickým bezpečnostním hrozbám, čímž výrazně zvyšuje detekční schopnosti celého systému SIEM. Architektura je vysoce škálovatelná, především díky cloudové infrastruktuře (např. podpora MS Azure), což z něj činí ideální nástroj i pro velké společnosti nebo prostředí s vysokými nároky na objem zpracovávaných dat. Vyhodnocování bezpečnostních záznamů a kybernetických bezpečnostních událostí probíhá v reálném čase, přičemž AI pomáhá odhalovat sofistikovanější kybernetické bezpečnostní hrozby. Lokální komponenty odpovídají středním hardware požadavkům.

Licencování Securonix Unified Defense SIEM probíhá nejčastěji na základě objemu zpracovaných dat (tedy GB/den), což odpovídá trendu mezi cloudovými systémy SIEM. Nákladový model Securonix SIEM je zpravidla OpEx, přičemž roční náklady se obvykle pohybují kolem 500 000 až 1 000 000 Kč (v závislosti na objemu dat a dalších faktorech, jako jsou přídavné analytické moduly či rozšířené možnosti automatizace).



Obrázek č. 28: Ukázka prostřední Securonix Unified Defense SIEM

(Zdroj: [29])

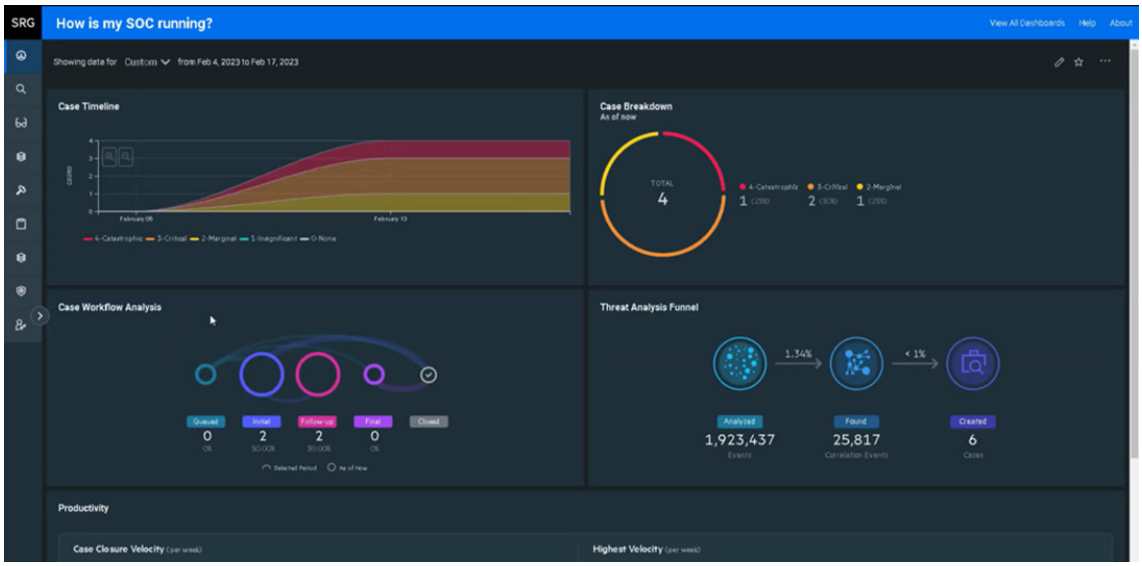
2.6.5 OpenText Enterprise Security Manager

OpenText Enterprise Security Manager je systémem SIEM, který umožňuje monitorovat, detekovat a reagovat na kybernetické bezpečnostní hrozby v reálném čase. Tedy shromažďuje, koreluje a analyzuje velké objemy dat z různých zdrojů v rámci monitorované infrastruktury ICT společnosti, aby identifikoval kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty. K tomuto účelu využívá výkonný korelační engine. OpenText Enterprise Security Manager je vysoce škálovatelný a přizpůsobitelný pro různé potřeby společností a dokáže shromažďovat a analyzovat data z více než 450 různých typů zdrojů bezpečnostních záznamů. Pro analýzu dat a reporting poskytuje přizpůsobitelné grafy a přehledy [30][31].

Z technického hlediska OpenText Enterprise Security Manager vyniká vysoce škálovatelnou architekturou, která je schopna zpracovávat až více než 100 000 EPS a ukládat terabyty dat. Tato architektura je ideální pro větší společnosti s náročnými požadavky na výkon a škálovatelnost. Pro efektivní zpracování dat v reálném čase tento systém SIEM běžně vyžaduje 32-64 GB RAM, SSD i pevné disky a 8 nebo více přidělených virtuálních procesorů. Báze korelačních pravidel je standardní s počtem přesahujících 1000 korelačních pravidel, což umožňuje detekci známějších kybernetických útoků a anomálií. Tento systém SIEM je vyvíjen společností Open Text, stejně jako ArcSight Logger, který společnost XYZ využívá pro log management. Proto lze očekávat jejich snadnou integraci.

Nákladový model OpenText Enterprise Security Manager je především CapEx. Licencování je založeno na modelu EPS. Celkové náklady tohoto systému SIEM se běžně pohybují v rozmezí od 600 000 do 1 000 000 Kč ročně.

V oblasti ostatních hodnotících kritérií OpenText Enterprise Security Manager nabízí vyhodnocování v reálném čase, standardní intuitivní GUI a základní pokročilou analytiku.



Obrázek č. 29: Ukázka přehledu z OpenText Enterprise Security Management

(Zdroj: [30])

3 VLASTNÍ NÁVRH ŘEŠENÍ

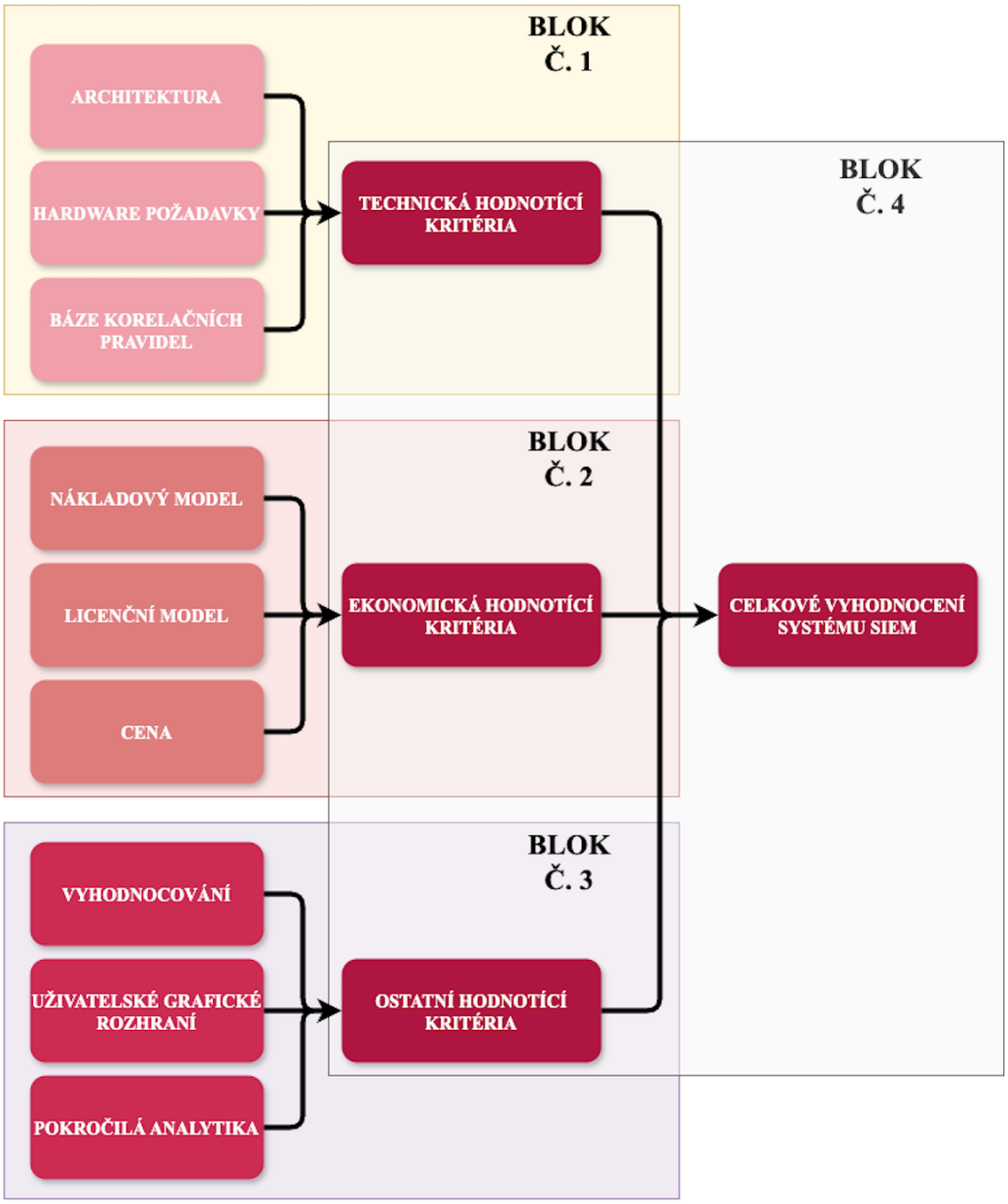
Tato část diplomové práce se zaměřuje na zhotovení fuzzy modelu pro vyhodnocování systémů SIEM v programovém prostředí MATLAB s využitím doplňku Fuzzy Logic Toolbox, včetně popisu uživatelského hodnotícího skriptu a aplikace s GUI pro přívětivější interakci s fuzzy modelem. Výstupy tohoto fuzzy modelu jsou prezentovány formou grafických vizualizací. V závěru této části diplomové práce je prezentováno nezávazné doporučení výběru jednoho z analyzovaných systémů SIEM (včetně jeho odhadovaných nákladů na implementaci do současného informačního prostředí) a tím bude podpořeno rozhodování managementu společnosti XYZ.

3.1 Fuzzy model v programovém prostředí MATLAB

Fuzzy model pro vyhodnocování systémů SIEM vychází z návrhu hodnotících kritérií (včetně jejich vah) a atributů, které byly nadefinovány ve druhé kapitole této diplomové práce. Ke zhotovení tohoto fuzzy modelu bylo využito programové prostředí MATLAB ve verzi *R2024b*.

3.1.1 Blokové rozdělení fuzzy modelu

Z důvodu optimalizace znalostní báze je užitečné fuzzy model (tedy FIS) pro vyhodnocování systémů SIEM rozdělit do tří, resp. čtyř bloků. Jednotlivé bloky (*fuzzy inferenční subsystémy*, dále jen FIsS) fuzzy modelu představují jednu kategorii nadefinovaných hodnotících kritérií, tedy blok č. 1 představuje technická hodnotící kritéria, blok č. 2 ekonomická hodnotící kritéria a blok č. 3 ostatní hodnotící kritéria. Každý z těchto bloků obsahuje tři vstupy a jeden výstup. Za čtvrtý blok lze považovat FIsS pro vyhodnocení celého fuzzy modelu napříč všemi bloky. Celkové vyhodnocení míry vhodnosti analyzovaných systémů SIEM a návrh doporučení pro management společnosti XYZ jsou realizovány na základě výsledků ze všech tří, resp. čtyř bloků fuzzy modelu (tedy na základě výstupů jednotlivých FIsS).



Obrázek č. 30: Blokové rozdělení fuzzy modelu

(Zdroj: Vlastní zpracování)

Rozdělením fuzzy modelu, které je znázorněno na obrázku č. 30, dojde k výraznému snížení počtu pravidel, která by musela být vytvořena k pokrytí všech možných kombinací vstupů fuzzy modelu. Konkrétně k pokrytí všech možných kombinací devíti vstupů bez rozdělení do bloků (a pouze při využití logického operátoru AND) by bylo nutné vytvořit 82 944 pravidel, zatímco samostatně pro blok č. 1 jen 48 pravidel, pro blok č. 2 též 48 pravidel a pro blok č. 3 pouze 36 pravidel. Tedy celkově po rozdělení fuzzy

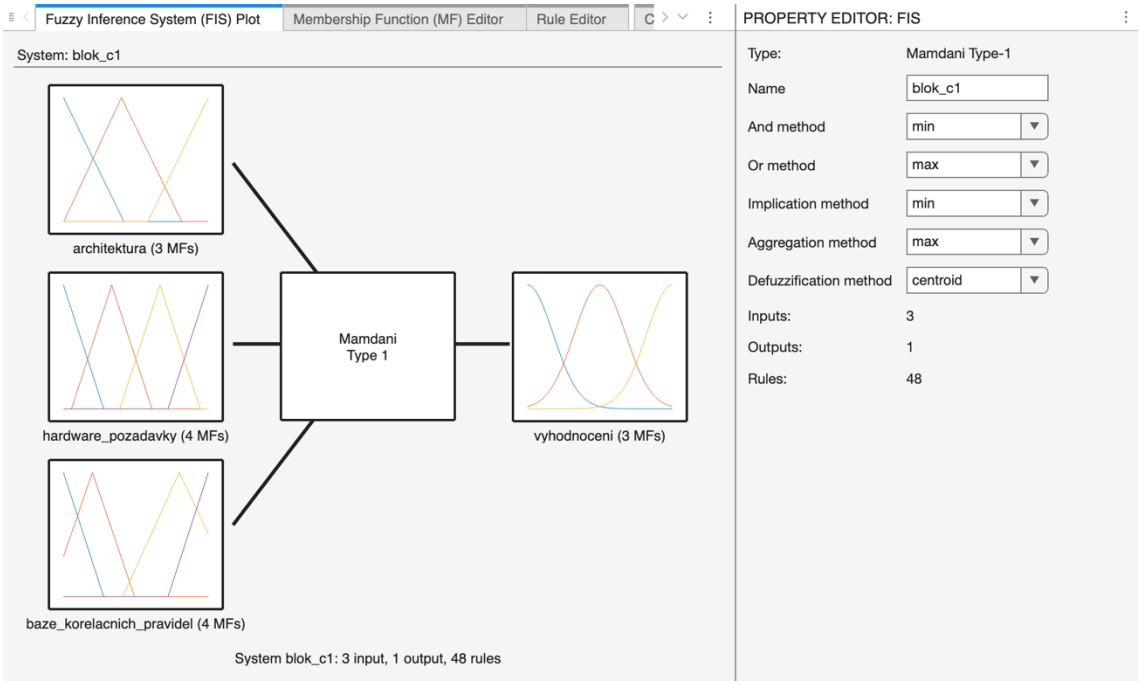
modelu do tří bloků je nutné vytvořit 132 pravidel k pokrytí všech možných kombinací vstupů, resp. 159 pravidel s připočtením dalších 27 pravidel z čtvrtého (vyhodnocovacího) bloku. Rozdíl mezi fuzzy modelem bez rozdělení do bloků a fuzzy modelem s rozdělením do bloků činí 82 812 pravidel, resp. 82 785 pravidel.

3.1.2 Bloky fuzzy modelu

Jednotlivé bloky fuzzy modelu byly vytvořeny pomocí nástroje Fuzzy Logic Designer, který byl představen v první kapitole této diplomové práce. Jeden blok fuzzy modelu odpovídá jednomu souboru ve formátu *.fis*. Řešení fuzzy modelu, tedy celého FIS (tj. tří, resp. čtyř FIsS), je založeno na druhu Mamdani v provedení typu 1.

Vstupy a výstupy

Nejdříve je nutné nadefinovat počet vstupů, který se odvíjí od počtu hodnotících kritérií vyčleněných pro daný blok fuzzy modelu. Tedy každý blok fuzzy modelu obsahuje tři vstupy a jeden výstup.



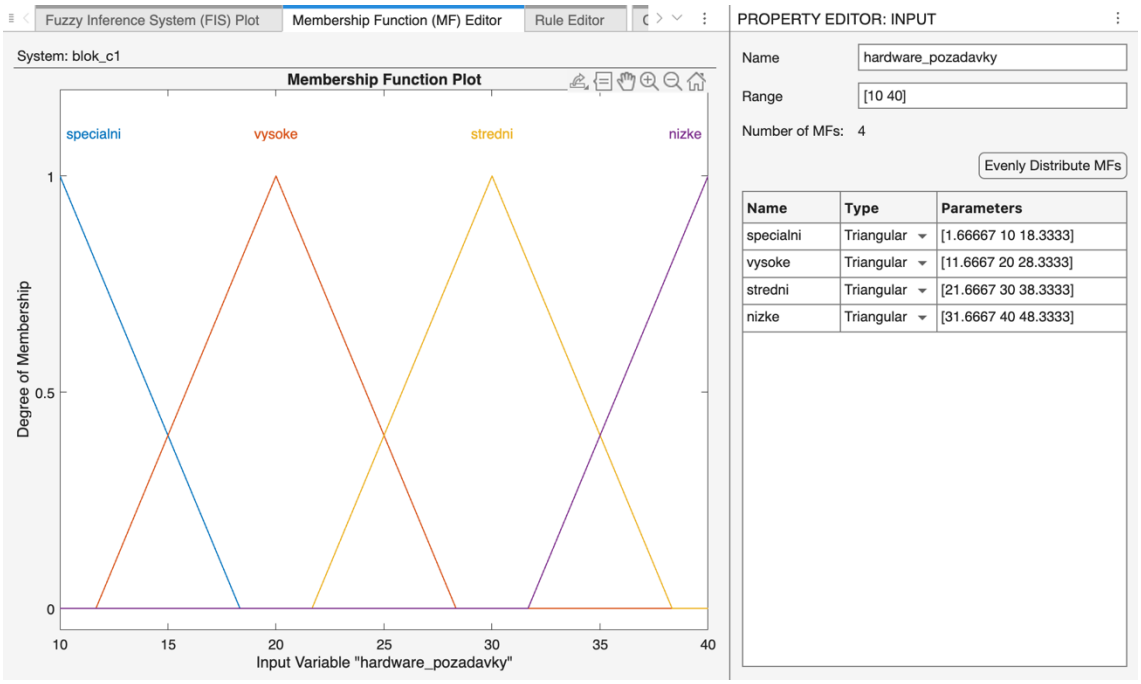
Obrázek č. 31: Ukázka Mamdani FIsS pro blok č. 1

(Zdroj: Vlastní zpracování)

Na obrázku č. 31 je znázorněn FIsS pro vyhodnocení bloku č. 1 fuzzy modelu, který na vstupu přijímá nadefinovaná hodnotící kritéria, tj. Architektura, Hardware požadavky a Báze korelačních pravidel. Obdobně jsou složeny i ostatní bloky fuzzy modelu (tedy jedno hodnotící kritérium odpovídá jednomu vstupu daného bloku fuzzy modelu).

Funkce členství

Druhý krok tvorby bloku fuzzy modelu zahrnuje pojmenování každého jeho vstupu a výstupu, definování rozsahu hodnot vstupů a výstupu, včetně pojmenování a nastavení jejich funkcí členství. To vše probíhá v editoru funkcí členství.

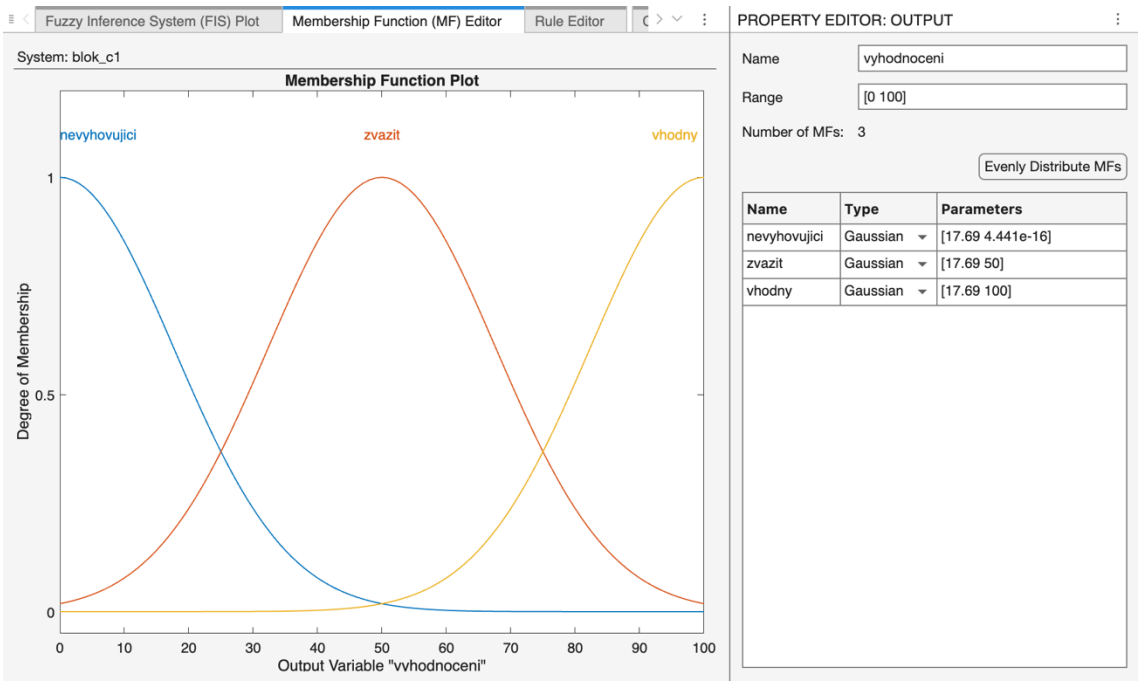


Obrázek č. 32: Ukázka funkcí členství vstupu bloku č. 1

(Zdroj: Vlastní zpracování)

Na obrázku č. 32 se nachází graf funkcí členství vstupu (tj. hodnotícího kritéria) Hardware požadavky, přičemž dané funkce členství reprezentují čtyři atributy hodnotícího kritéria o rozsahu hodnot 10 až 40. Všechny čtyři funkce členství mají tvar typu Λ a jsou pojmenovány dle příslušného atributu, kdy jejich špičková hodnota odpovídá přidělené hodnotě daného atributu (tedy atribut Speciální dosahuje maxima funkce členství v hodnotě 10, atribut Vysoké dosahuje maxima funkce členství v hodnotě 20 atd.). Sousedící funkce členství se vždy protínají (k čemuž může posloužit funkce *Evently Distribute MFs*, která automaticky rozdělí existující funkce členství v celém nastaveném

rozsahu). Funkce členství pro ostatní vstupy jednotlivých FIsS jsou tvořeny obdobně, pouze se liší názvem, počtem atributů a rozsahem hodnot.



Obrázek č. 33: Ukázka funkcí členství výstupu bloku č. 1

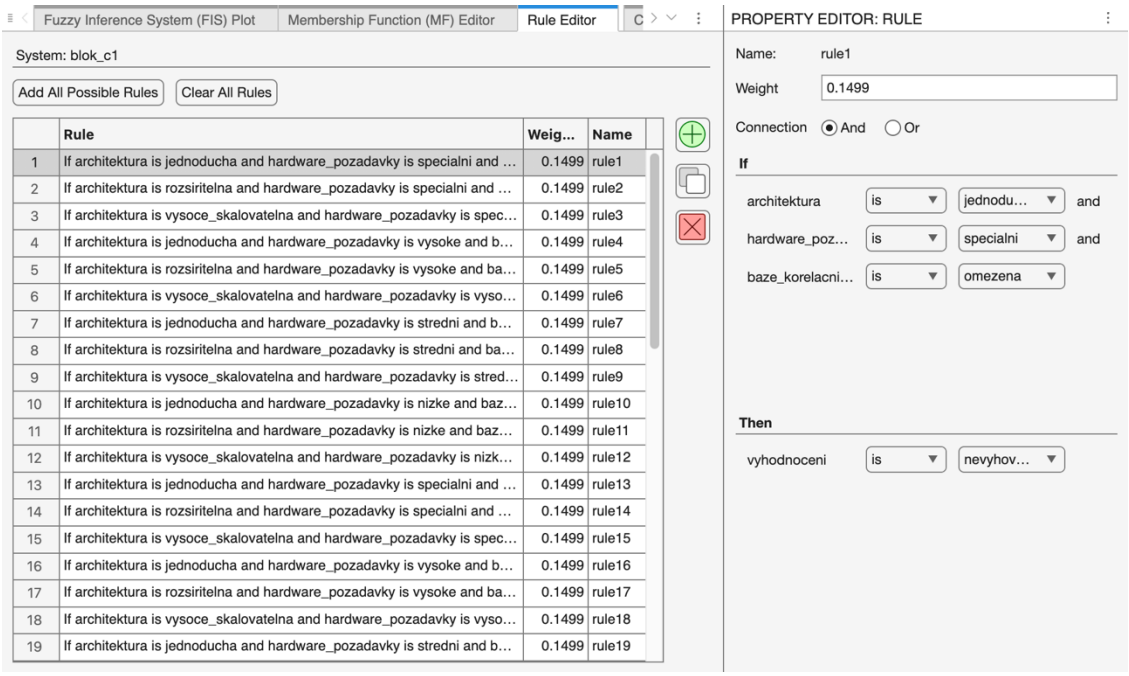
(Zdroj: Vlastní zpracování)

Na obrázku č. 33 je znázorněn graf funkcí členství výstupu každého FIsS. Výstup každého bloku fuzzy modelu má nastaven rozsah hodnot na 0 až 100 a jeho funkce členství je tvořena tvarem typu Gaussovy křivky. Rozsahy jednotlivých funkcí členství každého výstupu byly stanoveny funkcí *Evently Distribute MFs* a následně byly schváleny technický ředitelem společnosti XYZ.

Pravidla

Třetím a posledním krokem tvorby bloku fuzzy modelu je nadefinování pravidel v editoru pravidel. Pravidla definují výstup pro libovolnou kombinaci vstupů. Proto, aby byl výstup co nejpřesnější, vzniká potřeba pokrýt všechny možné kombinace vstupů. Programové prostředí MATLAB právě pro tuto potřebu nabízí funkci *Add All Possible Rules*. Takto vytvořeným pravidlům je poté nutné přidělit logický operátor pro spojení vstupů, hodnotu výstupu a také váhu samotného pravidla.

Všechna vytvořená pravidla jednotlivých FIsS mají pro spojení vstupů nastaven pouze logický operátor AND. Váhy samotných pravidel vychází ze Saaty metody. Tedy všechna pravidla v bloku č. 1 fuzzy modelu mají nastavenou váhu na hodnotu 0,1499 (což odpovídá součtu vah technických hodnotících kritérií), všechna pravidla v bloku č. 2 fuzzy modelu mají váhu o hodnotě 0,4889 (tj. součet vah ekonomických hodnotících kritérií) a všechna pravidla v bloku č. 3 fuzzy modelu mají nastavenou váhu na hodnotu 0,3612 (tj. součet vah ostatních hodnotících kritérií). Čtvrtý (vyhodnocovací) blok má váhu všech pravidel nastavenou na hodnotu 1, jelikož hodnotící skript, jenž propojuje jednotlivé bloky fuzzy modelu, pracuje s již váhami ovlivněnými výstupy předchozích tří bloků.

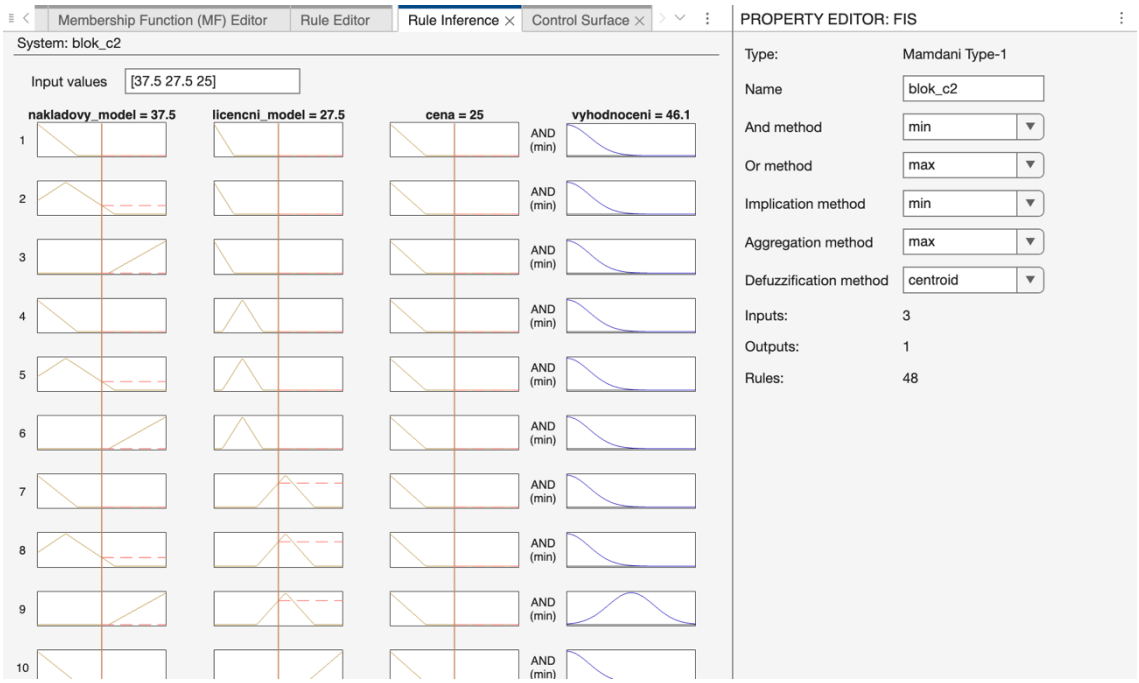


Obrázek č. 34: Ukázka pravidel bloku č. 1

(Zdroj: Vlastní zpracování)

Na obrázku č. 34 je znázorněno nastavení pravidla bloku č. 1 fuzzy modelu, kdy atributy vstupů (tj. hodnotících kritérií) odpovídají nejnižším hodnotám, a proto je nastavena hodnota výstupu jako nevyhovující.

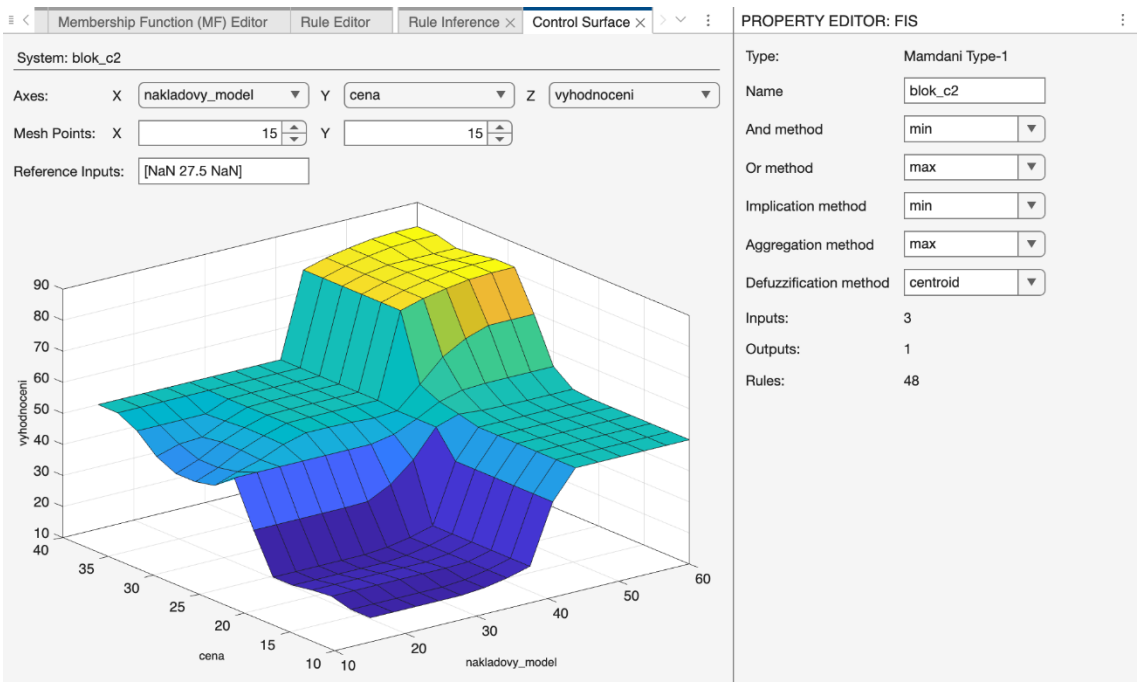
V prohlížeči pravidel, který je zachycen na obrázku č. 35, je pak možné sledovat změny ve výstupu při různých kombinací vstupů jednotlivých bloků fuzzy modelu.



Obrázek č. 35: Ukázka prohlížeče pravidel bloku č. 2

(Zdroj: Vlastní zpracování)

Prohlížeč řídící plochy poté umožňuje náhled na hodnoty výstupu pro různé kombinace dvou vstupů.

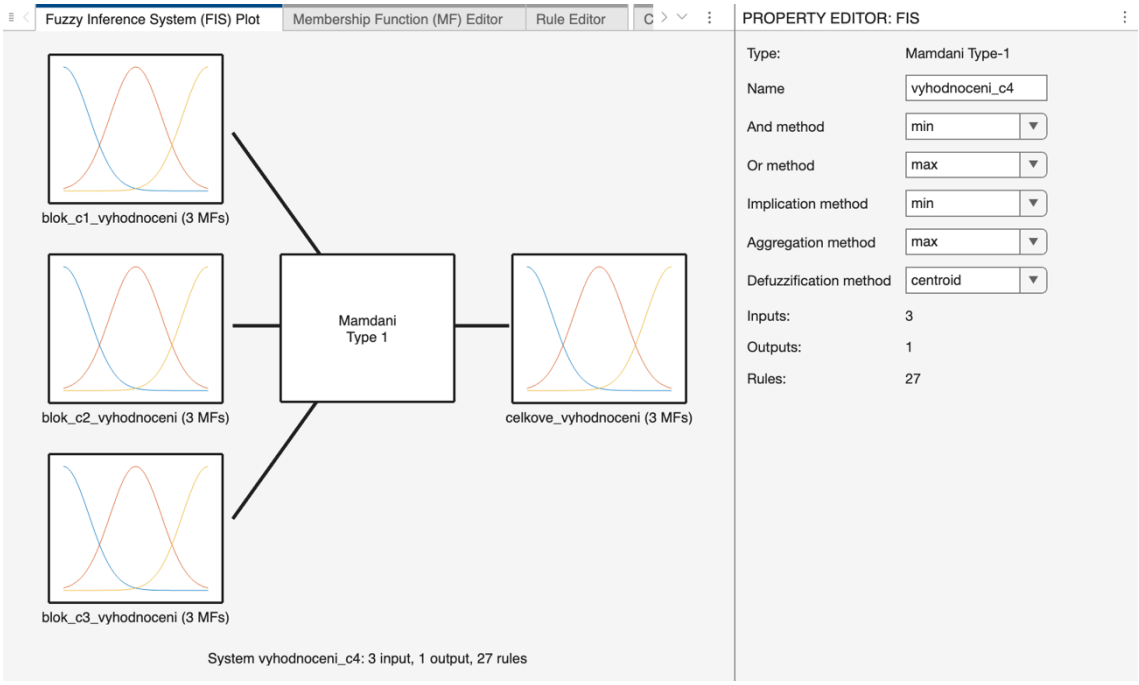


Obrázek č. 36: Ukázka prohlížeče řídící plochy bloku č. 2

(Zdroj: Vlastní zpracování)

Na obrázku č. 36 je zachycen prohlížeč řídící plochy, kdy osy *X* a *Y* představují vstupy bloku č. 2 fuzzy modelu, které jsou nastavené na hodnotící kritéria Nákladový model a Cena. Osa *Z* reprezentuje výstup bloku č. 2 fuzzy modelu, tedy vyhodnocení nastavených hodnotících kritérií. Je patrné, že s rostoucími hodnotami na osách *X* a *Y* dochází k nárůstu hodnoty na ose *Z*.

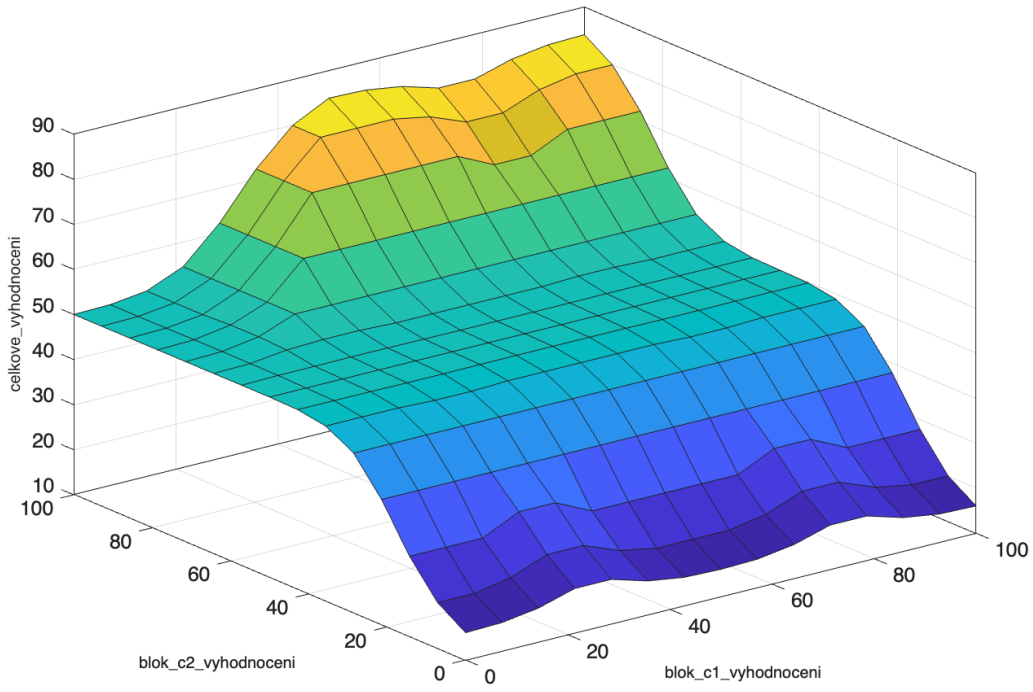
Po vytvoření bloků č. 1-3 fuzzy modelu byl vytvořen čtvrtý FIsS, tedy čtvrtý blok fuzzy modelu, který je schopen vyhodnotit míru vhodnosti systému SIEM na základě výstupů z bloků č. 1-3 fuzzy modelu.



Obrázek č. 37: Ukázka Mamdani FIsS pro blok č. 4

(Zdroj: Vlastní zpracování)

Čtvrtý (tedy vyhodnocovací) blok fuzzy modelu je opět FIsS druhu Mamdani v provedení typu 1. Jeho tři vstupy odpovídají výstupům bloků č. 1-3 fuzzy modelu, tedy jednotlivý vstup má rozsah hodnot 0 až 100 a je složen ze tří funkcí členství. Pokrytí všech možných kombinací vstupů je tvořeno 27 pravidly s váhou o hodnotě 1. Výstup představuje celkovou míru vhodnosti analyzovaného systému SIEM, tedy podklad pro nezávazné doporučení výběru jednoho z analyzovaných systémů SIEM k podpoře rozhodování managementu společnosti XYZ.



Obrázek č. 38: Řídící plocha bloku č. 4

(Zdroj: Vlastní zpracování)

Na obrázku č. 38 je zachycena řídící plocha bloku č. 4 fuzzy modelu, kdy osy *X* a *Y* představují vstupy bloku č. 4 fuzzy modelu, tj. v tomto případě výstup bloku č. 1 a výstup bloku č. 2. Osa *Z* reprezentuje výstup bloku č. 4 fuzzy modelu, tedy míru vhodnosti systému SIEM.

Implementace

Na základě výše popsaných kroků a informací byly v rámci fuzzy modelu pro vyhodnocování systémů SIEM vytvořeny celkem čtyři soubory ve formátu *.fis*, a to *blok_c1.fis* (tj. vyhodnocení technických hodnotících kritérií), *blok_c2.fis* (tj. vyhodnocení ekonomických hodnotících kritérií), *blok_c3.fis* (tj. vyhodnocení ostatních hodnotících kritérií) a *vyhodnoceni_c4.fis* (který vyhodnocuje míru vhodnosti systému SIEM na základě výstupů z bloků č. 1-3 fuzzy modelu).

Dále byly vytvořeny soubory *vyhodnoceni_skript.m* a *vyhodnoceni_app.mlapp*. Soubor ve formátu *.m* představuje textový soubor obsahující uživatelský hodnotící skript pro vyhodnocení systémů SIEM. Soubor ve formátu *.mlapp*, který se používá k vývoji a ukládání aplikací, obsahuje informace o rozložení vizuálních komponent, MATLAB

kód (který konfiguruje funkce aplikace) a metadata aplikace s GUI pro vyhodnocení systémů SIEM.

Celé řešení tohoto fuzzy modelu se tedy skládá ze šesti souborů, a to ze čtyř souborů ve formátu *.fis*, jednoho souboru ve formátu *.m* a jednoho souboru ve formátu *.mlapp*. Všechny uvedené soubory jsou umístěny do jednoho adresáře, kdy pro korektní fungování implementace řešení tohoto fuzzy modelu je nutné zachovat tuto adresářovou strukturu, jelikož skripty obsažené v souboru ve formátu *.m* a *.mlapp* přistupují k daným souborům ve formátu *.fis* pomocí relativní cesty.

3.1.3 Vyhodnocování prostřednictvím uživatelského hodnotícího skriptu

Uživatelský hodnotící skript je sestrojen v souboru *vyhodnoceni_skript.m*. Lze jej spustit prostřednictvím MATLAB konzole (tzv. *Command Window*). Poté je nutné zadat všech devět vstupních hodnot, tedy zadat číselnou hodnotu atributu odpovídajícího hodnotícího kritéria systému SIEM přímo do MATLAB konzole. Na základě takto zadaných hodnot je provedeno vyhodnocení systému SIEM, přičemž na výstupu uživatelského hodnotícího skriptu je slovní i číselné vyhodnocení analyzovaného systému SIEM.

Prvním krokem uživatelského hodnotícího skriptu je načtení souborů ve formátu *.fis*, které odpovídají jednotlivým blokům fuzzy modelu, do příslušných proměnných pomocí funkce *readfis()*.

```
blok_c1 = readfis("blok_c1.fis");
blok_c2 = readfis("blok_c2.fis");
blok_c3 = readfis("blok_c3.fis");
blok_c4 = readfis("vyhodnoceni_c4.fis");
```

Obrázek č. 39: Kód pro načtení FIsS

(Zdroj: Vlastní zpracování)

Na obrázku č. 39 je zobrazeno načtení příslušných souborů ve formátu *.fis* do proměnných *blok_c1*, *blok_c2*, *blok_c3* a *blok_c4* pomocí funkce *readfis()*.

Dalším krokem je načtení vstupů od uživatele do proměnných pomocí funkce *input()*. Načítání všech devíti vstupních hodnot je založeno na stejném způsobů.

```
cena = input("Bodove ohodnoceni ceny daneho systemu SIEM (10 - velmi vysoka, 20 - vysoka, 30 - stredni a 40 - nizka): ");
while cena<10 || cena>40
    disp("Zadana hodnota je mimo bodovy interval tohoto hodnoticiho kriteria.")
    cena = input("Bodove ohodnoceni ceny daneho systemu SIEM (10 - velmi vysoka, 20 - vysoka, 30 - stredni a 40 - nizka): ");
end
```

Obrázek č. 40: Ukázka kódu pro načtení vstupní hodnoty

(Zdroj: Vlastní zpracování)

Kód, který je uveden na obrázku č. 40, je ukázkou načtení vstupní hodnoty od uživatele. Konkrétně se jedná o načtení vstupní hodnoty hodnotícího kritéria Cena. Proto je zadaná hodnota uložena do proměnné *cena*. Pomocí konstrukce *while … end* (což je cyklus, který se opakuje, dokud zadaná podmínka není splněna) je ošetřeno, aby uživatel mohl zadat pouze hodnoty z nastaveného rozsahu hodnot vstupu. Uvnitř této konstrukce je proto složená podmínka s logickým operátorem OR, která definuje povolený rozsah hodnot, jenž odpovídá rozsahu hodnot vstupu v daným FIsS. Pokud tedy uživatelem zadaná hodnota pro vstup *cena* bude mimo rozsah hodnot 10 až 40, bude uživatel vyzván k opětovnému zadání hodnoty z povoleného rozsahu. Pokud uživatel zadá vstupní hodnotu z nastaveného rozsahu, dojde ke splnění podmínky a uživatel následně může zadat hodnotu pro další vstup, případně je proveden další nadefinovaný krok.

Po zadaní hodnot pro všechny vstupy do konkrétních proměnných, následuje vyhodnocení jednotlivých bloků fuzzy modelu, které probíhá pomocí funkce *evalfis()*.

```
% vyhodnoceni bloku c. 1
blok_c1_vyhodnoceni = evalfis(blok_c1, [architektura, hardware_pozadavky, baze_korelacnich_pravidel]);
% vyhodnoceni bloku c. 2
blok_c2_vyhodnoceni = evalfis(blok_c2, [nakladovy_model, licencni_model, cena]);
% vyhodnoceni bloku c. 3
blok_c3_vyhodnoceni = evalfis(blok_c3, [vyhodnocovani, uzivatelske_graficke_rozhrani, pokrocila_analytika]);
% vyhodnoceni bloku c. 4
celkove_vyhodnoceni = evalfis(blok_c4, [blok_c1_vyhodnoceni, blok_c2_vyhodnoceni, blok_c3_vyhodnoceni]);
```

Obrázek č. 41: Kód pro vyhodnocení jednotlivých bloků fuzzy modelu

(Zdroj: Vlastní zpracování)

Na obrázku č. 41 je znázorněno vyhodnocení jednotlivých bloků fuzzy modelu poté, co jednotlivým blokům fuzzy modelu byly přiřazeny uživatelem zadané hodnoty vstupů. Výstupy těchto vyhodnocení jsou uloženy do proměnných *blok_c1_vyhodnoceni*, *blok_c2_vyhodnoceni*, *blok_c3_vyhodnoceni* a *celkove_vyhodnoceni*.

Po vyhodnocení všech bloků fuzzy modelu již následuje pouze číselné a slovní vypsání výsledku vyhodnocení.

```
disp("Celkove vyhodnoceni systemu SIEM: ");
disp(celkove_vyhodnoceni(1)+ " %");

if celkove_vyhodnoceni(1)<50
    disp("Dany system SIEM je nevyhovujici.");
elseif celkove_vyhodnoceni(1)<65
    disp("Dany system SIEM je treba dukladne zvazit.");
else
    disp("Dany system SIEM je vhodny.");
end
```

Obrázek č. 42: Kód pro vypsání výsledku vyhodnocení

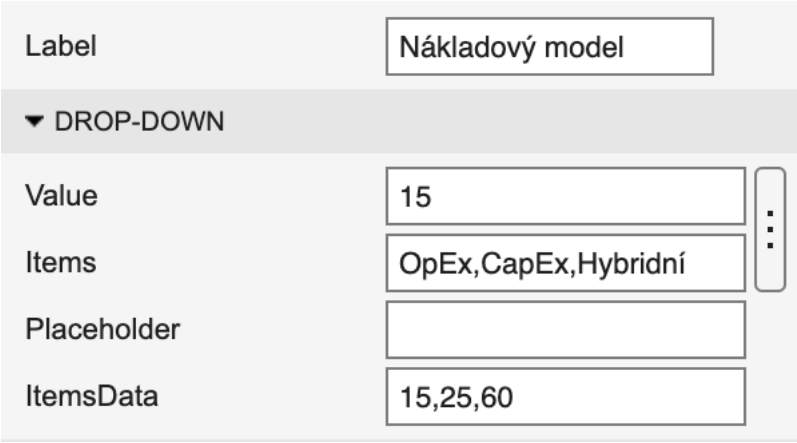
(Zdroj: Vlastní zpracování)

Kód pro číselné i slovní vyhodnocení analyzovaného systému SIEM (viz obrázek č. 42) obsahuje podmínku, že když je hodnota proměnné *celkove_vyhodnoceni* menší jak 50, tak je analyzovaný systém SIEM nevyhovující, pokud je hodnota proměnné menší jak 65, tak je analyzovaný systém SIEM třeba důkladně zvážit a pokud je hodnota proměnné větší jak 65, tak je analyzovaný systém SIEM vhodný k implementaci do informačního prostředí společnosti XYZ. Daná hodnotící škála byla konzultována a schválena technickým ředitelem společnosti XYZ.

3.1.4 Vyhodnocování prostřednictvím aplikace s GUI

Jelikož vyhodnocování systémů SIEM prostřednictvím uživatelského hodnotícího skriptu, který je spouštěn přímo v MATLAB konzoli, nemusí být dostatečně přívětivou formou, byla vytvořena aplikace s GUI. Ta se otevírá skrze spustitelný soubor s názvem *vyhodnoceni_app.mlapp* a nabízí GUI pro přívětivější interakci mezi uživatelem a daným fuzzy modelem.

V případě aplikace s GUI uživatel zadává vstupní hodnoty do fuzzy modelu skrze komponenty *Drop Down* a *Edit Field*. Komponenta Drop Down slouží k výběru právě jednoho atributu daného hodnotícího kritéria z předem nadefinovaného seznamu, viz obrázek č. 43.



Obrázek č. 43: Ukázka nastavení komponenty Drop Down

(Zdroj: Vlastní zpracování)

Komponenta Edit Field umožňuje uživateli zadat textový řetězec, kdy konkrétně v tomto případě uživatel zadává název analyzovaného systému SIEM.

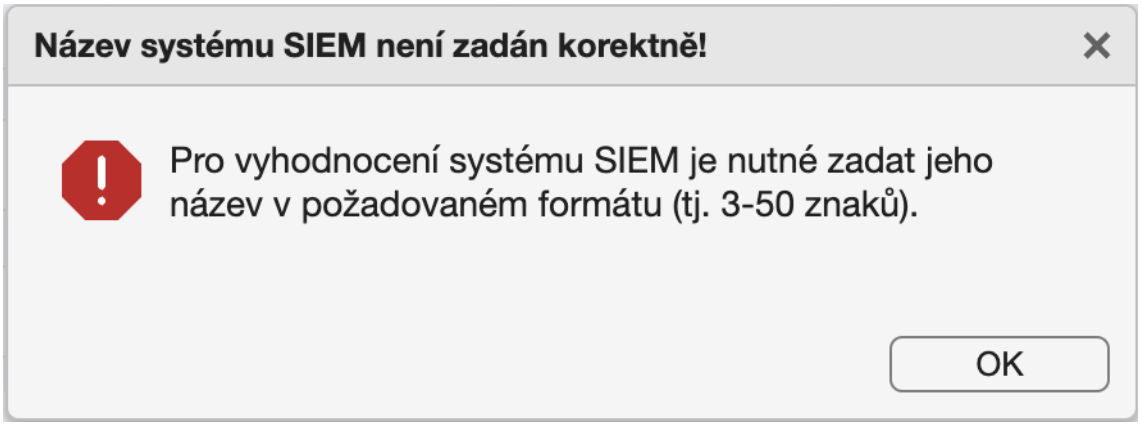
Obrázek č. 44: MATLAB aplikace s GUI

(Zdroj: Vlastní zpracování)

Jak je znázorněno na obrázku č. 44, aplikace s GUI pro vyhodnocování systémů SIEM je dále tvořena komponentami *Button*, *Label* a *Panel*. Komponenta Button představuje tlačítko, které reaguje na stisknutí uživatelem. Konkrétně tlačítko *VYHODNOTIT* spouští

skript pro vyhodnocení analyzovaného systému SIEM a tlačítko *RESET* vrací stavy a hodnoty komponent, se kterými uživatel pracoval, do výchozího stavu. Komponenta Label slouží k zobrazení statického textu (jako např. nadpisy a popisky) a zároveň jako prostor, kam se vypisuje výsledek skriptu pro vyhodnocení analyzovaného systému SIEM. Komponenta Panel sdružuje ostatní komponenty (v tomto případě devět komponent Drop Down, které představují hodnotící kritéria) do jednoho kontejneru pro usnadnění správy a zlepšení přehlednosti GUI.

Skript pro vyhodnocení analyzovaného systému SIEM, který se provede po spuštění tlačítka *VYHODNOTIT*, vychází primárně z uživatelského hodnotící skriptu. První změnou hned na počátku skriptu je přidání ověření, zda uživatel zadal název analyzovaného systému do komponenty Edit Field. Pokud uživatel název analyzovaného systému SIEM nezadal nebo ho zadal v nesprávném formátu (tj. mimo rozsah 3-50 znaků), tak skript dále nepokračuje a uživatel je vyzván k nápravě, viz obrázek č. 45.



Obrázek č. 45: Upozornění na nesprávně zadaný formát názvu systému SIEM

(Zdroj: Vlastní zpracování)

Pokud uživatel zadal název analyzovaného systému SIEM ve správném formátu, skript pokračuje načtením vstupních hodnot z komponent Edit Field a Drop Down.

```
architektura = app.arch.Value;
hardware_pozadavky = app.hwp.Value;
baze_korelacnich_pravidel = app.bkp.Value;
```

Obrázek č. 46: Ukázka načtení vstupních hodnot fuzzy modelu

(Zdroj: Vlastní zpracování)

Na ukázce zachycené na obrázku č. 46 je znázorněno načtení vstupních hodnot fuzzy modelu. Zde se konkrétně jedná o načtení vstupů bloku č. 1 fuzzy modelu, kdy např. do proměnné *architektura* je uložena hodnota komponenty Drop Down, která má název *arch* a odpovídá hodnotícímu kritériu Architektura. Obdobným způsobem jsou načítány ostatní vstupní hodnoty, liší se pouze názvy proměnných a názvy komponent Drop Down.

Následně proběhne načtení patřičných souborů ve formátu *.fis* a dále dojde k samotnému vyhodnocení jednotlivých bloků fuzzy modelu. To je prováděno stejným způsobem jako v uživatelském hodnotícím skriptu.

Jako poslední krok skriptu proběhne výpis výsledku celkového vyhodnocení analyzovaného systému SIEM.

```
app.label1_eval.Visible = "on";
app.label2_eval.Visible = "on";
app.label3_eval.Visible = "on";
app.label4_eval.Visible = "on";

app.label2_eval.Text = num2str(celkove_vyhodnoceni(1)) + " %";

if celkove_vyhodnoceni(1)<50
    app.label4_eval.Text = strcat('Systém SIEM "',nazev,'" je nevyhovující.');
    app.label2_eval.BackgroundColor = [0.8431, 0.2667, 0.3216];
    app.label4_eval.BackgroundColor = [0.8431, 0.2667, 0.3216];
elseif celkove_vyhodnoceni(1)<65
    app.label4_eval.Text = strcat('Systém SIEM "',nazev,'" je třeba důkladně zvážit.');
    app.label2_eval.BackgroundColor = [0.9647, 0.7255, 0.1922];
    app.label4_eval.BackgroundColor = [0.9647, 0.7255, 0.1922];
else
    app.label4_eval.Text = strcat('Systém SIEM "',nazev,'"je vhodný.');
    app.label2_eval.BackgroundColor = [0.3529, 0.7804, 0.2196];
    app.label4_eval.BackgroundColor = [0.3529, 0.7804, 0.2196];
end
```

Obrázek č. 47: Ukázka kódu pro vypsání výsledku vyhodnocení systému SIEM

(Zdroj: Vlastní zpracování)

V rámci posledního kroku skriptu, který je znázorněn na obrázku č. 47, proběhne nejprve zobrazení komponent *label1_eval*, *label2_eval*, *label3_eval* a *label4_eval*, kdy *label2_eval* a *label4_eval* jsou komponenty určené přímo k výpisu výsledku vyhodnocování analyzovaného systému SIEM. Aby bylo možné výsledek vyhodnocení do těchto komponent vypsat, je nutné pomocí funkce *num2str* převést číselný výsledek na textový řetězec. Poté následuje samotné vypsání výsledku hodnocení (do patřičných komponent Label), který odpovídá zvolené hodnotící škále. V proměnné *nazev* je uložena hodnota z komponenty Edit Field, tedy název analyzovaného systému SIEM, který je vkládán k výsledku vyhodnocování. A na závěr, pokud je daný systém SIEM

nevyhovující, jsou dotčené komponenty Label zbarveny do červené barvy, pokud je daný systém SIEM třeba důkladně zvážit, tak jsou dotčené komponenty Label zbarveny do žluté barvy a pokud je daný systém SIEM vhodný k implementaci, tak jsou dotčené komponenty Label zbarveny do zelené barvy.

Po vyhodnocení jednoho analyzovaného systému SIEM je patřičné skrze zmáčknutí tlačítka *RESET* vrátit aplikaci s GUI do původního stavu pro snadnější vyhodnocení dalšího systému SIEM.

```
app.arch.Value = 10;
app.hwp.Value = 20;
app.bkp.Value = 0;
app.nmo.Value = 15;
app.lmo.Value = 5;
app.cen.Value = 10;
app.vyh.Value = 0;
app.ugr.Value = 0;
app.pan.Value = 10;

app.label1_eval.Visible = "off";
app.label2_eval.Visible = "off";
app.label3_eval.Visible = "off";
app.label4_eval.Visible = "off";

app.label2_eval.Text = ("");
app.label4_eval.Text = ("");
app.ef1_name.Value = ("");
app.label2_eval.BackgroundColor = "none";
app.label4_eval.BackgroundColor = "none";
```

Obrázek č. 48: Ukázka kódu pro reset aplikace s GUI

(Zdroj: Vlastní zpracování)

Skript (jenž je znázorněn na obrázku č. 48) na pozadí tohoto tlačítka vrací hodnoty komponent Drop Down a Edit Field do původního stavu, schovává komponenty Label určené pro výpis výsledku vyhodnocování analyzovaného systému SIEM a maže z nich výstupy vyhodnocování i barevné formátování.

3.2 Vyhodnocení systémů SIEM

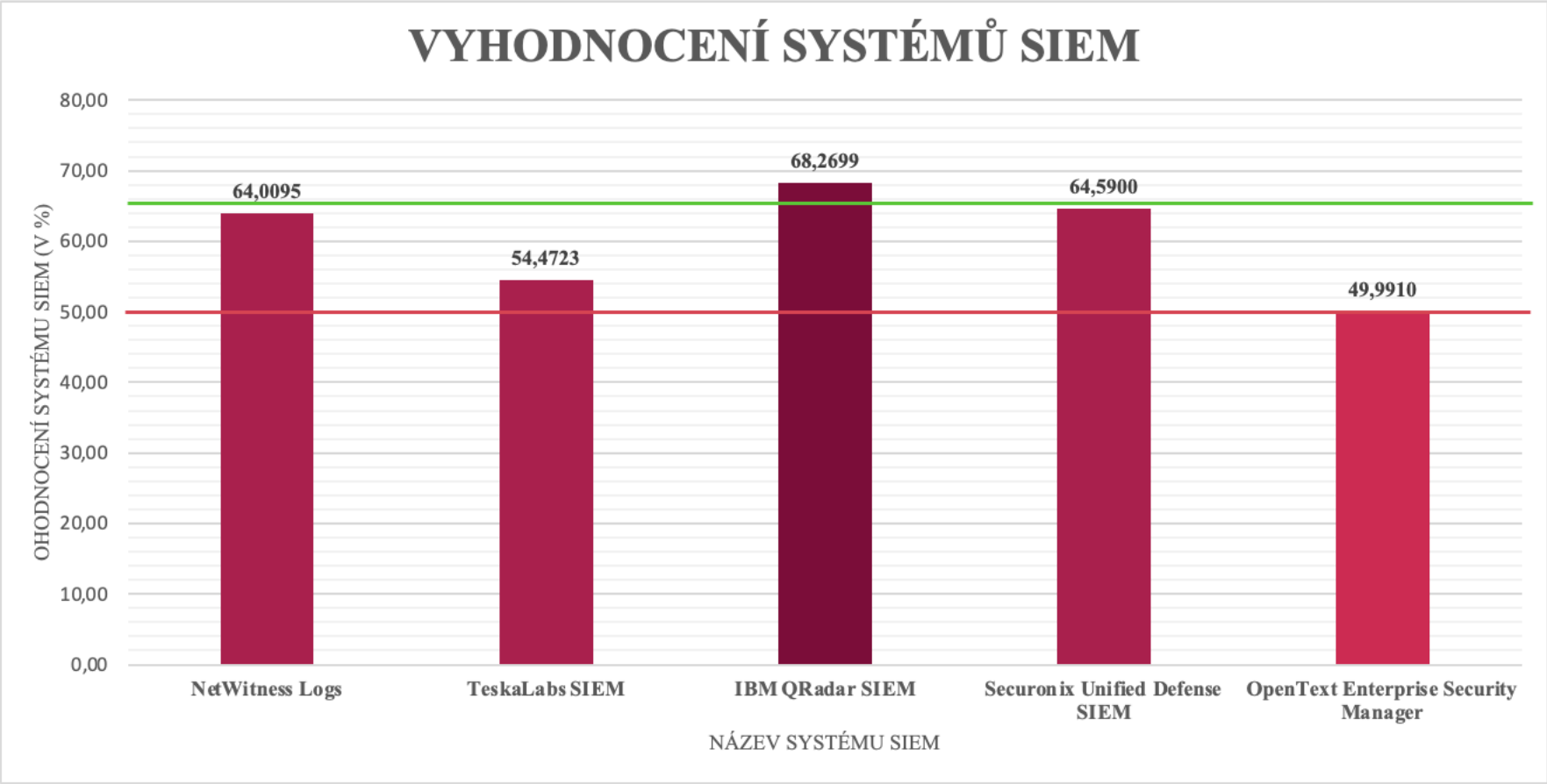
Výsledky vyhodnocování analyzovaných systémů SIEM představují výstupy fuzzy modelu, které byly získány prostřednictvím uživatelského hodnotícího skriptu, resp. aplikace s GUI.

Tabulka č. 12: Vyhodnocení systémů SIEM

(Zdroj: Vlastní zpracování)

SYSTÉM SIEM	VYHODNOCENÍ (V %)	DOPORUČENÍ
NetWitness Logs	64,0095	Daný systém SIEM je třeba důkladně zvážit.
TeskaLabs SIEM	54,4723	Daný systém SIEM je třeba důkladně zvážit.
IBM QRadar SIEM	68,2699	Daný systém SIEM je vhodný.
Securonix Unified Defense SIEM	64,5900	Daný systém SIEM je třeba důkladně zvážit.
OpenText Enterprise Security Manager	49,9910	Daný systém SIEM je nevyhovující.

Z tabulky č. 12 je patrné, že nejvyšší míry vhodnosti k implementaci do současného informačního prostředí společnosti XYZ dosahuje systém SIEM od společnosti IBM, tj. *IBM QRadar SIEM*. A proto tedy fuzzy model tento systém SIEM nezávazně doporučil managementu společnosti XYZ (a to jako jediného z pěti analyzovaných systémů SIEM) jako *vhodné řešení* k implementaci do jejího současného informačního prostředí, a to s výslednou hodnotou *68,2699 %* (viz obrázek č. 49, obrázek č. 50 a obrázek č. 51).



Obrázek č. 49: Vyhodnocení systémů SIEM

(Zdroj: Vlastní zpracování)

```
>> vyhodnoceni_skript
Bodove ohodnoceni architektury daneho systemu SIEM (10 - jednoducha, 30 - rozsiritelna a 60 - vysoce skalovatelna): 60
Bodove ohodnoceni hardware pozadavku daneho systemu SIEM (10 - specialni, 20 - vysoke, 30 - stredni a 40 - nizke): 20
Bodove ohodnoceni baze korelacnich pravidel daneho systemu SIEM (0 - omezena, 10 standardni, 40 pokrocila a 50 dynamicka): 40
Bodove ohodnoceni nakladoveho modelu daneho systemu SIEM (15 - OpEx, 25 - CapEx a 60 - hybridni): 60
Bodove ohodnoceni licencniho modelu daneho systemu SIEM (5 - pocet zarizeni, 15 - pocet uzivatelu, 30 - GB/den a 50 - EPS): 50
Bodove ohodnoceni ceny daneho systemu SIEM (10 - velmi vysoka, 20 - vysoka, 30 - stredni a 40 - nizka): 10
Bodove ohodnoceni vyhodnocovani daneho systemu SIEM (0 - vysoka latence, 10 - mirna latence, 40 - realny cas a 50 - automatizovane AI): 40
Bodove ohodnoceni uzivatelskeho grafickeho rozhrani daneho systemu SIEM (0 - neintuitivni, 40 - standardni a 60 - pokrocile): 40
Bodove ohodnoceni pokrocile analytiky daneho systemu SIEM (10 - zadna, 40 - zakladni a 50 - dynamicka): 50
Celkove vyhodnoceni systemu SIEM:
68.2699 %
Dany system SIEM je vhodny.
```

Obrázek č. 50: Vyhodnocení IBM QRadar SIEM – uživatelský hodnotící skript

(Zdroj: Vlastní zpracování)

Obrázek č. 51: Vyhodnocení IBM QRadar SIEM – aplikace s GUI

(Zdroj: Vlastní zpracování)

Systémy SIEM Securonix Unified Defense SIEM a NetWitness Logs skončily těsně pod hranicí vhodného systému SIEM (s výslednou hodnotou 64,5900 % a 64,0095 %) a doporučení managementu společnosti XYZ pro tyto systémy SIEM tedy zní tak, že by je bylo nutné ještě dále analyzovat a jejich implementaci do současného informačního prostředí společnosti XYZ důkladně zvážit. To samé doporučení platí i pro systém SIEM od společnosti TeskaLabs (tj. TeskaLabs SIEM), avšak jeho výsledná hodnota již odpovídá pouze 54,4723 %. Systém SIEM OpenText Enterprise Security Manager dosahuje (jako jediný z pěti analyzovaných systémů SIEM) výsledné hodnoty těsně pod 50 % (konkrétně 49,9910 %), a proto doporučení managementu společnosti

XYZ pro tento systém SIEM zní tak, že se jedná o nevhodný systém SIEM k implementaci do současného informačního prostředí společnosti XYZ.

3.2.1 Odhadované náklady na implementaci IBM QRadar SIEM

Uvedené ceny jednotlivých položek jsou pouze orientační odhady a mohou se lišit v závislosti na konkrétních podmínkách a dodavatelích. Odhadované ceny jednotlivých položek jsou uváděny v Kč bez započtení daně z přidané hodnoty (dále jen DPH).

Společnost XYZ by případnou implementaci IBM QRadar SIEM provedla bez využití externího dodavatele. Využila by však externích konzultantů pro co nejhladší průběh implementace tohoto systému SIEM do jejího současného informačního prostředí.

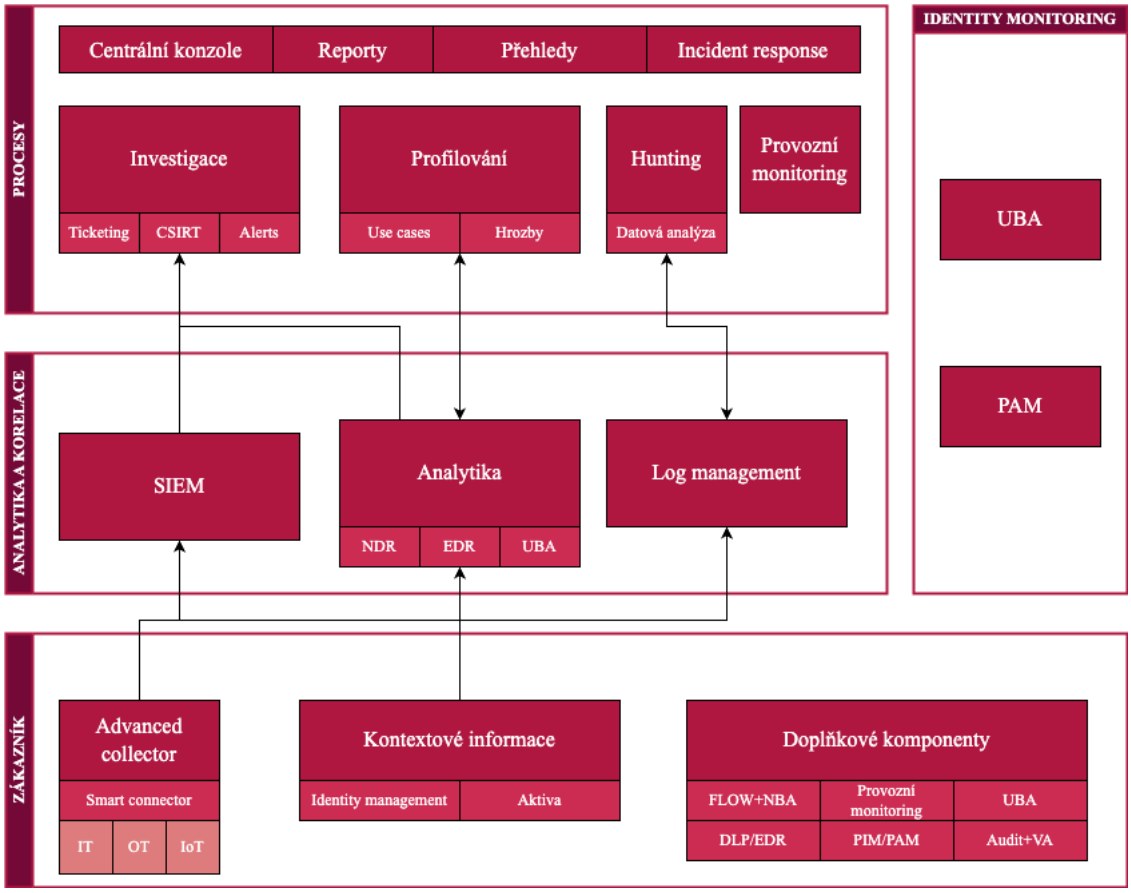
Fyzický server, na kterém by IBM QRadar SIEM běžel, by společnost XYZ vyšel přibližně na 350 000 Kč. Součástí tohoto serveru je 24jádrový procesor, 256 GB RAM a 2 TB SSD NVM. Dané kapacity je možné v budoucnu ještě navyšovat. Tento server by měl podporovat virtualizaci (prostřednictvím aktuálně využívaného hypervizora společnosti XYZ), kde bude využíván operační systém Red Hat Enterprise Linux, jehož roční licence stojí téměř 19 000 Kč [32].

Odborné konzultace, které by zahrnovaly pomoc s návrhem architektury, instalací, konfigurací a úvodním nastavením IBM QRadar SIEM, by společnost XYZ vyšly na vyšší desítky tisíc Kč (tj. kolem 100 000 Kč). Společnost XYZ by musela vynaložit přibližně 400 000 Kč za tzv. software install licenci IBM QRadar SIEM, která umožňuje instalaci tohoto systému SIEM na daný virtuální server a dále poskytuje přístup k nejnovějším aktualizacím, bezpečnostním záplatám a zaručuje podporu po dobu 12 měsíců. Společnost XYZ také předpokládá, že z počátku provozu IBM QRadar SIEM bude dostačující licence, která rozšiřuje kapacitu zpracovávání na 2 500 EPS a umožňuje správu kybernetických bezpečnostních událostí. Tato licence vyjde na přibližně 1 500 000 Kč. Obě licence je nutné každoročně obnovovat [33].

Školení pěti bezpečnostních analytiků SOC společnosti XYZ v rozsahu tří pracovních dnů by vyšlo na 60 000 Kč.

Implementace IBM QRadar (bez započtení ročních licencí na provoz) do současného informačního prostředí společnosti XYZ by tedy vyšla přibližně na 510 000 Kč, přičemž každým rokem provozu by společnost XYZ zaplatila přes 1 900 000 Kč za obnovu

potřebných licencí. Na obrázku č. 52 je poté znázorněna infrastruktura SOC společnosti XYZ po implementaci daného systému SIEM.



Obrázek č. 52: Infrastruktura SOC společnosti XYZ se systémem SIEM

(Zdroj: Vlastní zpracování dle: interní dokumentace společnosti XYZ)

3.3 Náklady na implementaci programového prostředí MATLAB

Aby společnost XYZ mohla sestavit a používat daný fuzzy model pro vyhodnocování systémů SIEM a případně využívat fuzzy logiku i v dalších případech pro podporu rozhodování, je nutné, aby zakoupila příslušné licence programové prostředí MATLAB spolu s doplňkem Fuzzy Logic Toolbox.

Tabulka č. 13: Porovnání cen licencí k produktům společnosti The MathWorks
(Zdroj: Vlastní zpracování dle: [34])

LICENCE	CENA MATLAB	CENA FUZZY LOGIC TOOLBOX
Trvalá	58 566,00 Kč	33 467,00 Kč
Roční	23 427,00 Kč	13 387,00 Kč

Jak je znázorněno v tabulce č. 13 (kde jsou ceny uváděny bez DPH), tak trvalá standardní (tj. komerční) licence programového prostředí MATLAB by společnost XYZ vyšla na přibližně 58 566 Kč a trvalá standardní licence doplňku Fuzzy Logic Toolbox by ji vyšla na dalších přibližně 33 467 Kč, což dohromady činní 92 033 Kč. Kdyby se společnost XYZ rozhodla jít cestou předplatného, tak by ji roční standardní licence programového prostředí MATLAB vyšla na přibližně 23 427 Kč a roční standardní licence doplňku Fuzzy Logic Toolbox by ji vyšla na dalších přibližně 13 387 Kč, tedy dohromady na 36 814 Kč ročně [34].

Jelikož společnost XYZ zvažuje pravidelné využívání programového prostředí MATLAB spolu s doplňkem Fuzzy Logic Toolbox, vyplatí se jí z dlouhodobého hlediska zakoupení trvalé standardní licence. S ohledem na tuto licenci je však nezbytné konstatovat, že pro zajištění přístupu k nejaktuálnější verzi programového prostředí MATLAB a doplňků bude společnost XYZ povinna pravidelně obnovovat službu tzv. *MathWorks Software Maintenance Service*. Obvykle je první rok této služby zahrnut v ceně trvalé licence. Po uplynutí této doby je možné službu dobrovolně opakovaně prodlužovat. Jestliže nedojde k prodloužení, lze i nadále používat verzi programového prostředí MATLAB, která byla zakoupena s trvalou licencí, avšak je zrušen přístup k novým verzím, aktualizacím i technické podpoře. Pozdější obnovení služby MathWorks Software Maintenance Service je obvykle možné, ale může být dražší než průběžné prodlužování, protože cena obnovení může záviset na tom, po jakou dobu byla tato služba neaktivní [35].

Programové prostředí MATLAB spolu s Fuzzy Logic Toolbox disponuje poměrně složitějším GUI a mnoha pokročilými funkcemi, což k jeho obsluze vyžaduje osobu s patřičnými zkušenostmi. Proto by bylo vhodné osoby, které budou s programovým prostředím MATLAB pracovat, i dostatečně zaškolit. K tomuto účelu nabízí společnost The MathWorks zdarma na svých stránkách edukativní videa týkající se práce s programovým prostředním MATLAB a doplňkem Fuzzy Logic Toolbox.

3.4 Přínos návrhu řešení

Hlavním přínosem zhotoveného fuzzy modelu je podpoření a zefektivnění manažerského rozhodování ve společnosti XYZ, a to nejen v rámci výběru vhodného systému SIEM do jejího současného informačního prostředí. Doposud totiž byly nové ICT a bezpečnostní nástroje vybírány na základě nabytých zkušeností techniků a manažerů (tzn. metody nejlepší praxe), různých doporučení nebo dle jejich osvědčení se během zkušebního provozu. Toto řešení je ne vždy efektivní a často časově náročné i nedostatečně kvantitativně podloženo. Využitím zhotoveného fuzzy modelu je získáno číselné vyhodnocení a slovní doporučení, které by mělo podpořit konkrétně implementaci vhodného systému SIEM do současného informačního prostředí společnosti XYZ. Zhotovený fuzzy model lze ovšem dále rozšiřovat, různě modifikovat, či vytvořit zcela nový fuzzy model, aby byl schopen vyhodnocovat konkrétní problematiky, a to vše díky propracovanému programovému prostředí MATLAB spolu s doplňkem Fuzzy Logic Toolbox. A proto aplikace patřičného fuzzy modelu může zefektivnit manažerské rozhodování a dále může zlepšit týmovou spolupráci a komunikaci v rámci např. návrhu hodnotících kritérií, jejich vah apod.

ZÁVĚR

Cílem této diplomové práce bylo využití fuzzy logiky pro vyhodnocování systémů pro správu bezpečnostních událostí a informací s využitím programového prostředí MATLAB za účelem podpory rozhodování managementu společnosti XYZ.

Aby došlo ke splnění tohoto cíle, byl s využitím programového prostředí MATLAB a doplňku Fuzzy Logic Toolbox zhotoven fuzzy model o třech, resp. čtyřech blocích, jehož výstupem bylo číselné vyhodnocení analyzovaného systému pro správu bezpečnostních událostí a informací a také slovní doporučení udávající míru vhodnosti daného systému pro správu bezpečnostních událostí a informací do současného informačního prostředí společnosti XYZ. Právě toto doporučení má nezávazně sloužit k podpoře rozhodování managementu společnosti XYZ ve výběru vhodného systému pro správu bezpečnostních událostí a informací do současného informačního prostředí. Ovšem ještě před tím, než došlo k samotnému zhotovení fuzzy modelu, bylo nutné ve spolupráci s technických ředitelem společnosti XYZ a expertním týmem TECH 1 stanovit hodnotící kritéria, dle kterých budou jednotlivé systémy pro správu bezpečnostních událostí a informací hodnoceny. Po stanovení hodnotících kritérií, jejich atributů a následném rozdělení hodnotících kritérií do tří kategorií (a to technických, ekonomických a ostatních) byly těmto hodnotícím kritériím stanoveny váhy s využitím Saatyho metody, na jejichž základě bylo následně možné vymezit pět nejpřijatelnějších systémů pro správu bezpečnostních událostí a informací ze seznamu dodaného Sales týmem společnosti XYZ. Těchto pět nejvhodnějších systémů pro správu bezpečnostních událostí a informací bylo prostřednictvím uživatelského hodnotícího skriptu, resp. aplikace s uživatelským grafických rozhraním vyhodnoceno zhotoveným fuzzy modelem. V rámci toho nejvhodnějšího z pěti analyzovaných systémů pro správu bezpečnostních událostí byly popsány náklady spojené s jeho implementací do současného informačního prostředí společnosti XYZ.

V úvodu diplomové práce byla vymezena problematika a byl stanoven primární cíl spolu s dílčími cíli, kterých má být dosaženo k vyřešení dané problematiky.

V první kapitole byla stanovena teoretická východiska spojená s fuzzy logikou, informační a kybernetickou bezpečností, systémem pro správu bezpečnostních událostí a informací a také s programovým prostředím MATLAB a doplňkem Fuzzy Logic

Toolbox, které společnost XYZ také zvažuje implementovat do současného informačního prostředí, zejména ke tvorbě podkladů pro podporu rozhodování. Jednalo se o pojmy popisující principy fuzzy logiky, základy informační a kybernetické bezpečnosti a představení systému pro správu bezpečnostních událostí a informací, včetně programového prostředí MATLAB spolu s nástroji doplňku Fuzzy Logic Toolbox, které byly využity při tvorbě fuzzy modelu.

Druhá kapitola se zabývá analýzou problému a současné situace společnosti XYZ. Byly zde popsány základní informace o společnosti XYZ, jako jsou její hlavní a ostatní ekonomické činnosti, organizační struktura nebo užívané ICT a bezpečnostní nástroje. Po seznámení se se společností XYZ následovalo ve spolupráci s technickým ředitelem a expertním týmem TECH 1 stanovení hodnotících kritérií a jejich atributů pro systémy pro správu bezpečnostních událostí a informací. Poté byly představeny dostupné systémy pro správu bezpečnostních událostí a informací. Ty byly vybrány Sales týmem společnosti XYZ na základě provedeného průzkumu trhu s těmito systémy a na základě spolupráce s technickým ředitelem. Pomocí Saatyho metody byly jednotlivým hodnotícím kritériím stanoveny váhy, které umožnily ze seznamu systémů pro správu bezpečnostních událostí a informací od Sales týmu vybrat těch pět nejvhodnějších řešení do současného informačního prostředí společnosti XYZ. Těchto pět nejvhodnějších systémů pro správu bezpečnostních událostí a informací bylo v závěru druhé kapitoly detailněji popsáno.

Závěrečná kapitola diplomové práce se zabývá samotným návrhem a zhotovením fuzzy modelu, který je schopen vyhodnocovat systémy pro správu bezpečnostních událostí a informací. Návrh a zhotovení fuzzy modelu vychází z předchozích dvou kapitol. Fuzzy model byl rozdělen do tří, resp. čtyř bloků. Těmto blokům byly nadefinovány vstupy a výstupy, funkce členství a pravidla. Každý jeden blok fuzzy modelu z bloků č. 1-3 odpovídá jedné kategorii hodnotících kritérií. Blok č. 4 fuzzy modelu na základě výstupů z předchozích tří bloků fuzzy modelu udává číselné vyhodnocení analyzovaného systému pro správu bezpečnostních událostí a informací a slovní doporučení o jeho vhodnosti do současného informačního prostředí společnosti XYZ. Vyhodnocení analyzovaných systémů pro správu bezpečnostních událostí a informací bylo realizováno pomocí uživatelského hodnotícího skriptu a přívětivější aplikace s uživatelským grafickým rozhraním, kdy realizace těchto dvou řešení byla v této kapitole taktéž popsána. Z pěti

analyzovaných systémů pro správu bezpečnostních událostí a informací, které byly vymezeny a detailněji popsány v závěru druhé kapitoly této diplomové práce, zhotovený fuzzy model vyhodnotil IBM QRadar SIEM jako to nejvhodnější řešení k implementaci do současného informačního prostředí společnosti XYZ. A proto byly dále popsány náklady, které by společnost XYZ musela vynaložit na jeho implementaci do jejího současného informačního prostředí. Tyto informace spolu s nezávazným doporučením na výstupu zhotoveného fuzzy modelu mohou sloužit jako cenné poklady pro podporu rozhodování managementu společnosti XYZ ve výběru systému pro správu bezpečnostních událostí a informací do jejího současného informačního prostředí.

Na základě této diplomové práce by také měla společnost XYZ zvážit koupi trvalé licence programového prostředí MATLAB a doplňku Fuzzy Logic Toolbox, jelikož bylo dokázáno, že s jejich pomocí lze vhodně tvořit poklady pro členy managementu společnosti XYZ. Náklady na jejich pořízení spolu s přínosem navrhovaného řešení byly představeny v samotném závěru této diplomové práce.

SEZNAM POUŽITÉ LITERATURY

[1] DOSTÁL, Petr a JANKOVÁ, Zuzana. *Operační a systémová analýza: Pokročilé metody*. 2. aktualiz. vyd. Brno: Akademické nakladatelství CERM, 2023. ISBN 978-80-7623-108-5.

[2] VACEK, Jiří a PEŠÍK, Jiří. *Systémové přístupy v managementu*. Plzeň: Západočeská univerzita v Plzni, 2022. ISBN 978-80-261-1125-2.

[3] DOSTÁL, Petr; RAIS, Karel a SOJKA, Zdeněk. *Pokročilé metody manažerského rozhodování*. Praha: Grada Publishing, 2005. ISBN 978-80-247-6320-0.

[4] HENDL, Jan a kol. *Základy matematiky, logiky a statistiky pro sociologii a ostatní společenské vědy*. 3. dopl. vyd. Praha: Karolinum, 2022. ISBN 978-80-246-5400-3.

[5] RUTKOWSKI, Leszek. *FLEXIBLE NEURO-FUZZY SYSTEMS: Structures, Learning and Performance Evaluation*. Boston: Kluwer Academic Publishers, 2004. ISBN 1-4020-8042-5.

[6] GUO, Jia; CHEN, Ing-Ray a TSAI, Jeffrey J.P. A survey of trust computation models for service management in internet of things systems. Online. *Computer Communications*. 2017, vol. 97, s. 1-14. ISSN 0140-3664. Dostupné z: https://doi.org/10.1016/j.comcom.2016.10.012. [cit. 2024-10-28].

[7] JURA, Pavel. *Základy fuzzy logiky pro řízení a modelování*. Brno: Vutium, 2003. ISBN 80-214-2261-0.

[8] CHEN, Guanrong a PHAM, Trung Tat. *Introduction to Fuzzy Sets, Fuzzy Logic, and Fuzzy Control Systems*. USA: CRC Press, 2019. ISBN 978-0367397883.

[9] DOSTÁL, Petr. *Advanced decision making in business and public services*. Brno: Akademické nakladatelství CERM, 2011. ISBN 978-80-7204-747-5.

[10] GILAT, Amos. *MATLAB: An Introduction with Applications*. 6th ed. USA: Wiley, 2017. ISBN 978-1-119-25683-0.

[11] HANSELMAN, Duane a LITTLEFIELD, Bruce. *Mastering MATLAB*. Velká Británie: Pearson Education Limited, 2012. ISBN 978-0-273-75213-4.

[12] THE MATHWORKS. *Fuzzy Logic Toolbox*. Online. THE MATHWORKS. MathWorks. © 1994-2024. Dostupné z: https://www.mathworks.com/help/fuzzy/index.html. [cit. 2024-12-28].

[13] THE MATHWORKS. *Build Fuzzy Systems Using Fuzzy Logic Designer*. Online. THE MATHWORKS. MathWorks. © 1994-2024. Dostupné z: https://www.mathworks.com/help/fuzzy/building-systems-with-fuzzy-logic-toolbox-software.html. [cit. 2024-12-29].

[14] THE MATHWORKS. *Mamdani and Sugeno Fuzzy Inference Systems*. Online. THE MATHWORKS. MathWorks. © 1994-2024. Dostupné z: https://www.mathworks.com/help/fuzzy/types-of-fuzzy-inference-systems.html. [cit. 2024-12-29].

[15] THE MATHWORKS. *Defuzzification Methods*. Online. THE MATHWORKS. MathWorks. © 1994-2024. Dostupné z: https://www.mathworks.com/help/fuzzy/defuzzification-methods.html. [cit. 2024-12-29].

[16] THE MATHWORKS. *Type-2 Fuzzy Inference Systems*. Online. THE MATHWORKS. MathWorks. © 1994-2024. Dostupné z: https://www.mathworks.com/help/fuzzy/type-2-fuzzy-inference-systems.html. [cit. 2024-12-29].

[17] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

[18] ANDRESS, Jason. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd ed. Oxford: Elsevier, 2014. ISBN 978-0-12-800744-0.

[19] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [ISO]. *ISO/IEC 27001:2022 - Information security management systems*. Online.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [ISO]. ISO - International Organization for Standardization. 2025. Dostupné z: https://www.iso.org/standard/27001. [cit. 2025-01-02].

[20] VON SOLMS, Rossouw a VAN NIEKERK, Johan. From information security to cyber security. Online. *Computers & Security*. 2013, vol. 38, s. 97-102. ISSN 0167-4048. Dostupné z: https://doi.org/10.1016/j.cose.2013.04.004. [cit. 2024-12-30].

[21] GONZÁLEZ-GRANADILLO, Gustavo; GONZÁLEZ-ZARZOSA, Susana a DIAZ, Rodrigo. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Online. *Sensors*. 2021, vol. 21, no. 14, article 4759. Dostupné z: https://doi.org/10.3390/s21144759. [cit. 2024-12-30].

[22] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NÚKIB]. *Nový zákon o kybernetické bezpečnosti*. Online. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NÚKIB]. Portál NÚKIB. © 2024, 21. 11. 2024. Dostupné z: https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti. [cit. 2024-12-30].

[23] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NÚKIB]. *1. Obecné informace o směrnici NIS2*. Online. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NÚKIB]. Portál NÚKIB. © 2024, 1. 10. 2024. Dostupné z: https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti/okruh-obecne-informace-o-smernici-nis2. [cit. 2024-12-30].

[24] OPEN TEXT CORPORATION. *ArcSight Logger 7.3 Documentation*. Online. OPEN TEXT CORPORATION. OpenText | Information Management Solutions. © 2025. Dostupné z: https://www.microfocus.com/documentation/arcsight/logger-7.3. [cit. 2025-02-05].

[25] SAATY, T. L. Relative Measurement and Its Generalization in Decision Making Why Pairwise Comparisons Are Central in Mathematics for the Measurement of Intangible Factors The Analytic Hierarchy/Network Process. Online. *Rev. R. Acad.*

Cien. Serie A. Mat. 2008, vol. 102, no. 2, s. 251-318. Dostupné z: https://doi.org/10.1007/BF03191825. [cit. 2025-03-27].

[26] NETWITNESS. *Log Monitoring and Management – NetWitness Logs*. Online. NETWITNESS. Network Threat Detection & Cyber Security NetWitness. © 2025. Dostupné z: https://www.netwitness.com/products/log-management-monitoring. [cit. 2025-04-02].

[27] TESKALABS. *TeskaLabs SIEM*. Online. TESKALABS. TeskaLabs - Cyber security. © 2014-2025. Dostupné z: https://teskalabs.com/cz/products/siem. [cit. 2025-04-01].

[28] IBM. *IBM QRadar SIEM*. Online. IBM. IBM - United States. Dostupné z: https://www.ibm.com/products/qradar-siem. [cit. 2025-04-01].

[29] SECURONIX. *Enterprise SIEM Solutions*. Online. SECURONIX. Securonix - Unified Defense SIEM, TDIR, UEBA & SOAR Solutions. 2025. Dostupné z: https://www.securonix.com/products/siem-solutions. [cit. 2025-04-02].

[30] OPEN TEXT CORPORATION. *Enterprise SIEM Security Tool*. Online. OPEN TEXT CORPORATION. OpenText | Information Management Solutions. © 2025. Dostupné z: https://www.opentext.com/products/enterprise-security-manager. [cit. 2025-03-31].

[31] OPEN TEXT CORPORATION. *OpenText Enterprise Security Manager Product Overview*. Online, PDF. Open Text Corporation, © 2024. Dostupné z: https://www.opentext.com/media/product-overview/opentext-enterprise-security-manager-po-en.pdf. [cit. 2025-03-31].

[32] RED HAT. *Buy Red Hat Enterprise Linux Server*. Online. RED HAT. Red Hat. © 2025. Dostupné z: https://www.redhat.com/en/store/red-hat-enterprise-linux-server. [cit. 2025-04-25].

[33] CONVERGE SRL. *Licenze Software Multibrand edizione 3: Listino 1 - Prodotti IBM*. Online, PDF. Converge Srl, © 2025. Dostupné z:

https://convenzioni.converge.it/docs/ID_2230_SW_ED.3-Lotto_3_IBM-Listino_Licenze.pdf. [cit. 2025-04-25].

[34] THE MATHWORKS. *Pricing and Licensing*. Online. THE MATHWORKS. MathWorks. © 1994-2025. Dostupné z: https://www.mathworks.com/pricing-licensing.html. [cit. 2025-04-27].

[35] THE MATHWORKS. *MathWorks Software Maintenance Service*. Online. THE MATHWORKS. MathWorks. © 1994-2025. Dostupné z: https://www.mathworks.com/services/maintenance.html. [cit. 2025-04-27].

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH ZKRATEK

a.s.	akciová společnost
AI	umělá inteligence (Artificial Intelligence)
aj.	a jiné
apod.	a podobně
atd.	a tak dále
CapEx	kapitálové výdaje (Capital Expenditures)
DPH	daň z přidané hodnoty
EPS	události za sekundu (Events Per Second)
FIS	fuzzy inferenční systém
FIsS	fuzzy inferenční subsystém
GB	gigabyt
GB/den	gigabyty za den
GUI	uživatelské grafické rozhraní (Graphical User Interface)
ICT	informační a komunikační technologie (Information and Communication Technologies)
ISMS	systém řízení bezpečnosti informací (Information Security Management System)
Kč	koruna česká
mj.	mimo jiné
např.	například
NIS2	Network and Information Security 2
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
NVMe	rozhraní pro nevolatilní paměť (Non-Volatile Memory Express)
nZoKB	nový zákon o kybernetické bezpečnosti

OpEx	provozní výdaje (Operational Expenditures)
RAM	počítačová paměť (Random Access Memory)
resp.	respektive
SIEM	správa bezpečnostních informací a událostí (Security Information and Event Management)
SOC	bezpečnostní operační centrum (Security Operations Center)
SSD	polovodičový disk (Solid-State Drive)
tj.	to jest
tzn.	to znamená
tzv.	takzvaně

SEZNAM PŘÍLOH