



Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Jiří Šlefr, MBA
Student:	Linda Šindelářová
Název práce:	Detekce bezpečnostních hrozeb v nástrojích pro správu bezpečnostních informací a událostí
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	30. června 2023

Hodnotící kritéria

1. Splnění zadání

- ▶ [1] zadání splněno
- [2] zadání splněno s menšími výhradami
- [3] zadání splněno s většími výhradami
- [4] zadání nesplněno

Studentka z pohledu zadavatele splnila všechny body zadání.

2. Písemná část práce

95 /100 (A)

Celá práce je informačně vyvážená. Struktura je volena tak, aby i neznalý čtenář měl možnost se dobře v tématu zorientovat a logicky postupovat po celé práci. Studentka při popisu nepřeskakuje z tématu na téma a celá práce je velmi pěkně čitelná. Po přečtení práce si čtenář vytvoří jednoznačný přehled o problematice hrozeb, legislativě s nimi spojenými a o možnostech, jak přistupovat k jejich odhalování. Externí zdroje a citace jsou přehledně a jasně vyznačeny, typografie i jazyková stránka bez výhrad.

3. Nepísemná část, přílohy

89 /100 (B)

Studentka měla dopředu danou technologii, kterou má pro řešení použít, jejíž zvládnutí je netriviální, stejně jako překlopení teoretických, slovně definovaných pravidel do kódu, který daná pravidla aplikuje a v datech vyhledává. V rámci práce jsou využity "základní" mechanismy pro práci s daty v dané technologii a implementaci pravidel, která jsou naprosto funkční a aplikovatelná samostatně nebo v kombinaci mezi sebou. V práci mi chybí realizace příkladu "komplexního" pravidla, které ale nebylo podmínkou pro úplnost práce.

4. Hodnocení výsledků, jejich využitelnost

100 /100 (A)

Implementovaná pravidla jsou plně použitelná v reálném nasazení a byla testovaná na reálných výstupech.

5. Aktivita studenta

- ▶ [1] **výborná aktivita**
- [2] velmi dobrá aktivita
- [3] průměrná aktivita
- [4] slabší, ale ještě dostatečná aktivita
- [5] nedostatečná aktivita

Studentka si v rámci práce samostatně domlouvala a docházela na konzultace, zejména při praktické části a zasílala včas nové verze práce, jako podklad pro diskusi. Návrhy a doporučení na změny v práci vždy zohlednila.

6. Samostatnost studenta

- [1] výborná samostatnost
- ▶ [2] **velmi dobrá samostatnost**
- [3] průměrná samostatnost
- [4] slabší, ale ještě dostatečná samostatnost
- [5] nedostatečná samostatnost

Studentka fungovala velmi samostatně, pouze v případě seznamování se s technologií v praktické části byla poskytnuta vyšší míra podpory, která je ale, vzhledem ke komplexitě technologie, pochopitelná.

Celkové hodnocení

95 /100 (A)

Celkově na mě velmi dobře působí čitelnost a přehlednost celé práce. Zejména v teoretické oblasti dostává čtenář ucelené shrnutí legislativy, hrozeb a způsobů, jak se s nimi vypořádat. Téma logmanagementu a bezpečnosti je velmi aktuální a práce jako taková je skvělým vstupem pro ty, kteří s tématem začínají nebo se mu profesionálně nevěnují. Praktická část je hezkým potvrzením, že pro vypořádání se s běžnými hrozbami není třeba vynakládat příliš prostředků a stačí využít technologie dostupné i zdarma. Skvělá práce!

Instrukce

Splnění zadání

Posudte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posudte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posudte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posudte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posudte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posudte schopnost studenta samostatně tvůrčí práce.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.