Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Marek Bertovič
Vedoucí práce: Ing. Filip Štěpánek
Název práce: Utilization of Threat Intelligence in Information Security
Obor: Počítačová bezpečnost

Datum vytvoření: 2. 6. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* ***2=náročnější zadání,*** *3=průměrně náročné zadání,* *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Výsledná platforma nutná pro integraci korelačních algoritmů se skládá ze dvou částí -- konkrétně části zpracovávající SIEM (Security Information and Event Management) a části obsluhující tzv. "Threat Intelligence Management". Studentovo řešení vyžadovalo propojení obou částí, tedy důkladné nastudování veškeré dokumentace a aplikačních poznámek obou částí a jejich následné propojení. Toto není explicitně zmíněno v zadání nicméně propojení bylo nutné pro úspěšnou realizaci ZP.

Z tohoto důvodu hodnotím zadání jako náročné.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání bylo splněno. Výstupem je funkční prototyp platformy zpracovávající TI. Součástí platformy jsou i algoritmy detekující realizované hrozby v síťovém provozu -- konkrétně se jedná o detekci TOR komunikace, ransomware a phishingu. Tyto algoritmy byly zakomponovány do výsledného řešení a jejich funkčnost otestována na předem vygenerovaných datech.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami,* *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
ZP splňuje požadavky na rozsah diplomové práce. Jedinou výtku mám k tomu, že uživatelský manuál není součástí textu ZP -- avšak je přiložen na CD.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*95 (A)*

Popis kritéria:
Posuďte, 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.

Komentář:
Student při řešení problému postupoval logicky -- zmapoval používanou terminologii a existující řešení. Jelikož se jednalo převážně o komerční produkty, zvolil si cestu navržení vlastní platformy skládající se z volně dostupných součástí (viz bod 1). Následně pro výslednou platformu navrhl sadu korelačních algoritmů, které detekují předem popsané hrozby. Tyto kroky jsou řádně zaznamenány a výsledek otestován. Text je srozumitelný a jednotlivé kroky na sebe navazují.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*95 (A)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
Práce je psaná v anglickém jazyce a splňuje typografické a jazykové požadavky. Překlepy a podobné nedostatky se vyskytují v práci v minimální míře.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*95 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Text je řádně ocitován a obsahuje dostatečný seznam jak vědecké tak odborné literatury.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*100 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Výsledkem ZP je funkční prototyp platformy zpracovávající TI (viz bod 2) -- ten byl navržen a otestován v laboratorních podmínkách. V době psaní posudku probíhalo nasazení výsledných korelačních algoritmů v rámci SOC týmu zabývajícím se automatizovanou detekcí realizovaných hrozeb v IT infrastruktuře v reálném čase. Konflikt s licenčními podmínkami či autorským právem zjištěn nebyl.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Platforma prezentovaná v rámci práce je složena z dostupných součástí a pokrývá celý životní cyklus TI. Je možné ji použít v rámci výzkumu anebo k získání základních znalostí k práci s podobnou platformou, kterou je možné používat pouze s placenou licencí. Množinu detekovaných hrozeb lze rozšířit přidáním dalších korelačních algoritmů.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Student pracoval aktivně a samostatně. Pravidelně se účastnil konzultací, kde prezentoval dílčí výsledky své práce.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*100 (A)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Výsledek práce splňuje zadání a byl vyzkoušen mnou i lidmi z mého okolí v laboratorních podmínkách. Během spolupráce student pravidelně konzultoval svůj postup a reagoval na mé dotazy a poznámky. Text je srozumitelný a náležitě členěný. Výstupem je platforma, která dokáže detekovat realizované hrozby v síťové komunikaci na základě zachycených dat. Tyto hrozby se detekují pomocí studentem navržených a integrovaných algoritmů a zahrnují:
- TOR komunikaci
- Phishing
- Ransomware

Řešení mimo jiné pokrývá celý životní cyklus TI (Threat Intelligence). Podobná řešení jsou k dispozici pouze v rámci placené licence. Výstup práce je tedy možné využít v akademické oblasti nebo pro didaktivní účely.

Podpis vedoucího práce: