Posudek oponenta závěrečné práce

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

Student: Bc. Marek Bertovič
Oponent práce: Ing. Jiří Buček
Název práce: Utilization of Threat Intelligence in Information Security
Obor: Počítačová bezpečnost

Datum vytvoření: 8. 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:
Zadání vyžaduje porozumět aktuální problematice Threat Intelligence (možno přeložit jako zpravodajství hrozeb), nastudovat nástroje pro příjem a obohacení externích proudů dat (feeds), prostudovat komplexní systém pro management bezpečnostních informací a událostí (SIEM) a vytvořit ucelený systém pro uplatnění Threat intelligence v systému informační bezpečnosti s důrazem na rychlost a možnost nasazení v produkčním prostředí.

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:
Student splnil zadání v plném rozsahu.

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:
Rozsah písemné zprávy je celkově přiměřený, ale části popisující realizaci jsou místy nepřehledné pro čtenáře, který nemá zkušenost se systémem Splunk. Chybí názorné diagramy a vysvětlení aspoň základů použitých příkazů.

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:
Po věcné stránce nemám žádné výtky.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*78 (C)*

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 psána angličtinou s občasnými gramatickými chybami a překlepy. Použitá notace diagramů v kapitole 2.1 je nepřehledná a její grafická podoba odpoutává pozornost od významu.

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:
Se zdroji student pracuje korektně

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*90 (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 je funkční aplikace jako modul do systému Splunk. Aplikace je nainstalována jednak v ukázkové (laboratorní) podobě na cloudu AWS, a jednak zřejmě v produkčním prostředí na ostrých datech.

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:
V aktuální podobě je práce využitelná jednak jako přehled problematiky Threat Intelligence v informační bezpečnosti, a jednak jako součást systému v konkrétní firmě, kde student práci vyvinul a testoval. Ukázková a testovací podoba práce (laboratorní prostředí) je v současnosti v provozu na cloudu Amazon Web Services, ale tato brzy zanikne a v příloze práce není kompletní a ucelený návod pro instalaci výsledků práce jinde (jsou tam pouze instalační skripty pro Splunk a Splunk forwarder, nikoli pro ostatní části systému). Na přiloženém CD chybí konfigurační soubory pro Collective Intelligence Framework, přestože jsou v práci slíbeny (str. 40).

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
Čím se liší Váš přístup k detekci ransomware nebo TOR pomocí Threat Intelligence od prostého použití SIEM s komerčním feedem?
Při konstrukci příkazů pro vyhledávání a korelaci dat používáte znalosti z vnitřního fungování platformy Splunk. Jsou Vámi používané funkce a datové struktury stabilní součástí systému, nebo je riziko, že by se mohly v příštích verzích Splunk změnit, což by porušilo funkčnost Vašich příkazů?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*90 (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:
Vzhledem ke značné náročnosti tématu i složitosti použitých technologií ve svém hodnocení zohledňuji zejména skutečnost, že student dotáhl práci do funkčního stavu včetně optimalizace výkonnosti tak, že výsledek je skutečně použitelný v praxi.

Podpis oponenta práce: