POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Incident detection on SIEM events**
Jméno autora:	**Petr Poliak**
Typ práce:	Bc
Fakulta/ústav:	Faculty of electrical engineering
Katedra/ústav:	Department of Cybernetics
Oponent práce:	Ing. Tomáš Pevný, Ph.D.
Pracoviště oponenta práce:	Department of Computer Science, CTU in Prague

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **Zvolte položku.**

Hodnocení náročnosti zadání závěrečné práce.

Zadaní a náročnost dobře odpovídá zavěrečné práci bakalářského studia.

Splnění zadání **Zvolte položku.**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Zadání bylo splněno.

Zvolený postup řešení **Zvolte položku.**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Zvolené metody jsou v pořádku

Odborná úroveň **Zvolte položku.**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Pro vypracování práce student použil existující metody dostupné v knihovně scikit-learn v jazyce python. Jejich konkretní použití budí dojem, že se student nesnažil hluboce porozumět, jak fungují a raději je používal jako “černou krabičku.” To má bohužel negativní dopad na zavěry a užitečnost výsledků. Konkretně není jasné, zdali student používal “Support Vector Machines” s Gaussovským či linearním jadrem a na zakladě čeho zvolil penalizaci chyby. Podobně není jasné, proč neexperimentoval s různým nastaveních chyb prvniho a druhého typu. Tato opminutí může snížít přesnost klasifikátorů a tím i užitečnost experimentálního porovnání.
Práce rovněž obsahuje negativní výsledek o nevhodnosti metod založených na porovnání sekvencí. V jejich představení student zmiňuje možnost nastavení vah, ale tuto možnost nevyužil v experimentální části. Důsledkem může být opět snížená přesnost klasifikátoru.

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Formální a jazyková úroveň, rozsah práce Zvolte položku.

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Práce působí velmi nevyváženým dojmem. Zatímco velký prostor je věnován konkrétní implementaci (volba jazyka, knihoven, apod.), algoritmus je sám o sobě popsán velmi stručně a reprodukování výsledků by bylo bez přiloženého kódu velmi složité. Podobně, metody tvořící jádro řešení, konkrétně algoritmus SMOTE je popsán bez korektního matematického či algoritmického popisu.

Konkretní použití algoritmů je velmi vagní. Autor například zmiňuje algoritmus AdaBoost jako příklad algoritmu, kde je velmi jednoduché změnit penalizaci za chyby různých typů. Vzhledem k tomu, že na tento problém existuje několik vědeckých prací není jasné, kterou ma autor na mysli. Podovnou výtku mam k použití rozhodovacích stromů a nahodných lesů.

Výběr zdrojů, korektnost citací Zvolte položku.

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. 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.

V práci je opominuto velké množství citací. Například metoda SMOTE, kterou autor opužívá ve svém nejlepším řešení není citována. Podobně chybí citace u filtrování s pomocí Tomkových spojnic.

Další komentáře a hodnocení
Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

Vložte komentář (nepovinné hodnocení).

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm C

Datum: 30. Května, 2018 Podpis: