POSUDEK VEDOUCÍHO ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Anomaly Detection in Threat Intellience Data**
Jméno autora:	**Bc. Petr Marek**
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Vedoucí práce:	Štěpán Kopřiva, MSc.
Pracoviště vedoucího práce:	Katedra počítačů

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Zadání práce hodnotím jako náročnější. Student musel nastudovat netriviální množství informací jednak o způsobech detekce anomálií v časových řadách, dále nastudovat frameworky pro vhodnou paralelizaci a v neposlední řadě se seznámit s doménou síťové bezpečnosti.

Splnění zadání **splněno**

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.

Student splnil zadání v celém rozsahu – nastudoval techniky detekce anomálií, seznámil se s doménou a navrhl algoritmus pro detekci anomálií nad logy z threat intelligence detektorů. Vzhledem k nevhodnosti paralelizace výpočtu detektorů anomálií, kde stačí spustit jeden detektor pro každou časovou řadu student paralelizoval předzpracování logů do jednotlivých časových řad.

Aktivita a samostatnost při zpracování práce **A - výborně**

Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven. Posuďte schopnost studenta samostatné tvůrčí práce.

Student pracoval na zadání samostatně a pravidelně konzultoval svůj postup s vedoucím. Na konzultace byl připraven a sám aktivně navrhoval další postup řešení avyhledával relevantní publikace.

Odborná úroveň **B - velmi dobře**

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

Odborná úroveň technické práce je velmi dobrá. Student byl schopen zkombinovat několik existujících přístupů do jednoho modelu a tento model implementovat. Velmi kladně hodnotím využití frameworku pro paralelizaci dat, který celou práci posunuje blízko reálnému nasazení. Dále kladně hodnotím, jakým způsobem se student vypořádal s anomáliemi různého druhu, čímž opět roste praktická hodnota prezentovaného řešení.

Odborná úroveň zprávy je také velmi dobrá. Je škoda, že student v práci nevěnoval větší prostor popisu různých metod detekce anomálií v časových řadách. Dále postrádám lepší popis implementace, konkrétně kroky transformace logů do časových řad.

Formální a jazyková úroveň, rozsah práce **C - dobře**

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

Formální a jazykové zápisy jsou na výborné úrovni. Odvedené penzum technické práce je velmi dobré a je jen škoda, že není dostatečně popsáno v práci jako takové co se rozsahu týče..

Výběr zdrojů, korektnost citací **A - výborně**

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.

Výběr zdrojů i způsob citací jsou na výborné úrovni..

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 A NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení.

Student se rozhodl pracovat na tématu, které je aplikované a jehož řešení vyžaduje skloubit jak teoretické znalosti, tak i znalost domény síťové bezpečnosti a praktické schopnosti implementovat myšlenky v podobě kódu v podstatě produkční kvality.

Student zadání splnil velmi dobře a navrhl a naimplementoval model, který je bez pochyby použitelný jako detektor anomálií v časových řadách. Tento model otestoval kal na syntetických, tak i na reálných datech. V práci student tento model velice dobře a jasně popsal.

Jako jediný nedostatek práce vidím nedostatečný popis některých sekcí implementačního charakteru, který čtenáři nedovoluje dobře porozumět vykonané technické práci.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **C - dobře.**

Datum: 23.1.2018 Podpis: