Posudek oponenta diplomové práce

Jméno: Bc. Jiří Bauer

Název práce: Detekce anomálií pomocí doménových reputací na základě klasifikace stažených souborů

Jméno oponenta: Ing. Jan Zíka

Diplomová práce se zabývá vývojem systému Marlowe, který je využíván v Avast Software, s. r. o., pro detekci anomalit. Za anomalitu v našem kontextu považujeme dva základní případy:

1. z domény s dobrou reputací byl uživatelem stažen soubor, který byl Avastem označen jako škodlivý;
2. z domény uživatelé stahují větší množství škodlivých souborů, přestože doména jako taková zablokovaná není.

První případ poukazuje na možnost nesprávné detekce souboru (tzv. false positive), druhý naopak na chybějící detekci na URL (tzv. false negative). Oběma těmto scénářům je potřeba ze zřejmých důvodů předcházet.

Vytvořený systém využívá jednak anonymizovaná data od uživatelů a jednak data z ostatních vnitřních systémů, hledá v nich anomality a snaží se je vyřešit, případně nevyřešené incidenty zobrazuje v dashboardu, který byl pro tento účel vytvořen.

Student prokázal schopnost samostatně dokončit projekt většího rozsahu, od návrhu použití jednotlivých technologií, přes implementaci jeho součástí, až po testování a monitorování jeho chodu. Systém funguje v ostrém provozu 5 měsíců bez chyb nebo nutnosti údržby. Zdrojový kód je logicky členěn a je psaný čistým stylem.

Vzhledem k rozmanitosti použitých technologií a rozsahu projektu práci hodnotím jako nadprůměrně náročnou; vzhledem k pečlivému a preciznímu přístupu studenta během jednotlivých fází projektu navrhuji klasifikaci A (výborně).

Ing. Jan Zíka

Praha 25. 5. 2018