Posudek oponenta bakalářské práce

Student: Kučma Tomáš
Téma: Systém pro automatický sběr, vyhodnocení a aktualizaci YARA pravidel (id 25023)
Oponent: Křivka Zbyněk, Ing., Ph.D., UIFS FIT VUT

1. **Náročnost zadání** — **obtížnější zadání**
   Student se musel seznámit s celou řadou technologií a ty být schopen integrovat do nového automatizovaného řešení pro přidávání a synchronizaci Yara pravidel z různých externích zdrojů. Obtížnější bylo seznámení s nástroji a procesy, které jsou interní ve firmě Avast.
2. **Splnění požadavků zadání** — **zadání splněno**
   Všechny body zadání byly perfektně splněny. Navíc došlo k vytvoření pomocného nástroje na porovnání dvou Yara pravidel, který lze využít i v jiných projektech.
3. **Rozsah technické zprávy** — **je v obvyklém rozmezí**
4. **Prezentační úroveň předložené práce** — **92 b. (A)**
   Text je sepsán čtivě, členěn logicky a kapitoly dobře navazují. V sekci 5.1 by bylo vhodné hutný text o práci s pravidly doplnit například stavovým diagramem.
5. **Formální úprava technické zprávy** — **90 b. (A)**
   Po typografické i jazykové stránce je text na velmi vysoké úrovni a prohřešky se omezují na překlepy nebo drobné pravopisné chyby, kterých je však jen málo, takže neruší výborný dojem.
6. **Práce s literaturou** — **85 b. (B)**
   Student pracuje především s interními zdroji společnosti a zdroji spíše praktického charakteru. Všechny jsou na vhodných místech citovány. Drobnou vadou na kráse jsou mírně nekonzistentní formáty datům u různých záznamů (číselný vs. textový zápis měsíce).
7. **Realizační výstup** — **95 b. (A)**
   Implementace je pěkně navržena a kód je přehledný a dobře čitelný, čemuž pomáhá i vhodně zvolený jazyk Python. Velký důraz byl kladen na testy jak při vývoji, tak potom při otestování výsledného systému.
8. **Využitelnost výsledků**
   Jelikož je implementace řádně otestována a ověřena na praktických externích zdrojích, tak může být systém nasazen ve firmě Avast. Nástroj na porovnání Yara pravidel by mohl být využit i v jiných projektech pracujících s Yara pravidly.
9. **Otázky k obhajobě**
   - Na obr. 5.3 je uveden dvakrát atribut scan_id. Je nějaká souvislost takto pojmenovaného atributu v ScanStartedNotification a ze ScanResult?
10. **Souhrnné hodnocení** — **91 b. výborně (A)**
    Perfektní text, pěkná a využitelná implementace s drobným rozšířením. Dávám výborné hodnocení.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 30. května 2022

Křivka Zbyněk, Ing., Ph.D.
oponent