Systém pro označování artefaktů

David Čermák

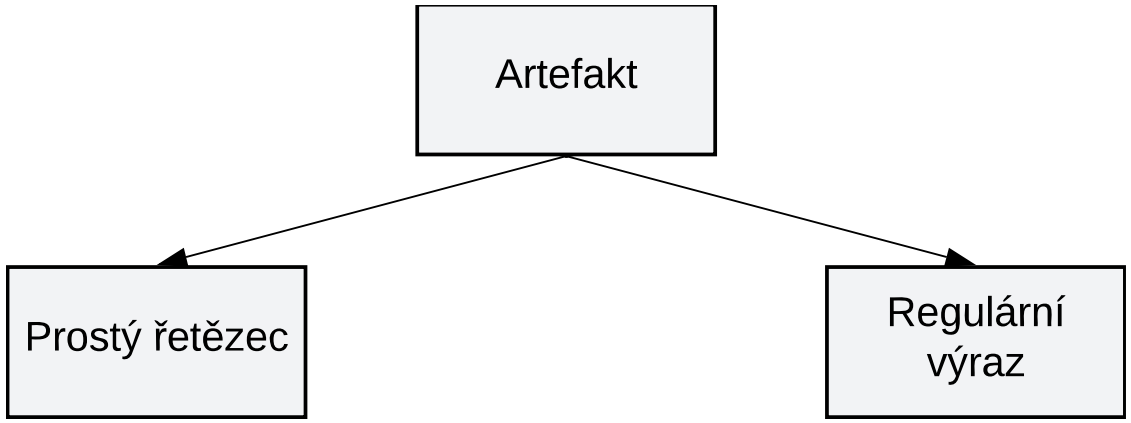
vedoucí: Ing. Dominika Regéciová

- Poskytování informací o artefaktech interním systémům
- Klasifikace artefaktů

Příklady artefaktů:

Přístup k souboru:	C:\Windows\wusa.lock
IP adresa:	191.233.81.105
URL adresa:	www.ebay.com
Vytvoření třídy:	TForm1

- Ukládání artefaktů a regulárních výrazů
- Dynamické označování artefaktů štítky
- Automatická aktualizace databáze na základě událostí
- Webové aplikační rozhraní



Artefakt1:

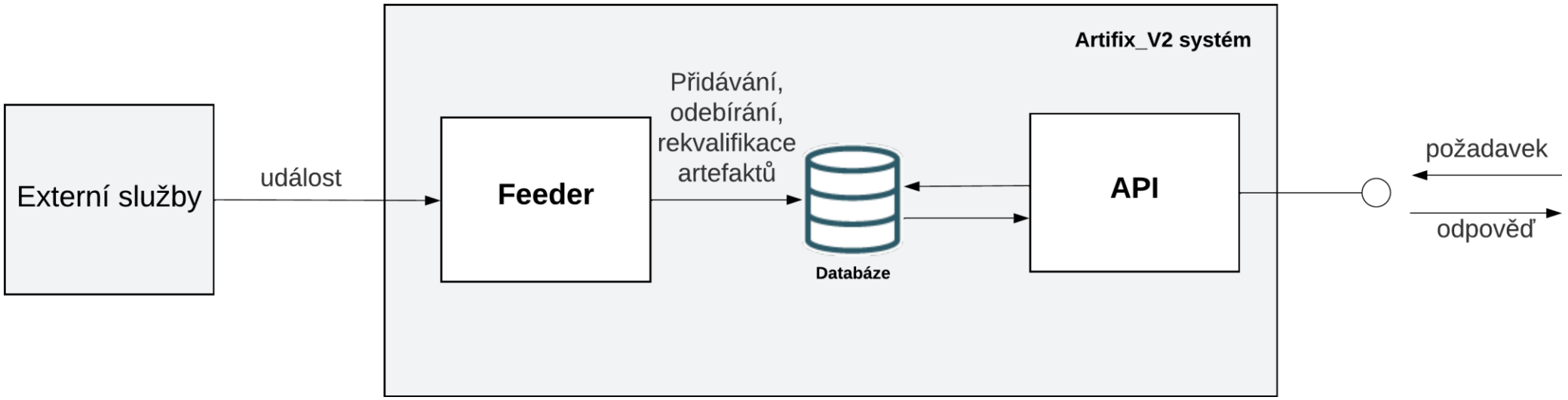
Typ:	Přístup k souboru
Hodnota:	C:\Windows\wusa.lock
Štítky:	Závažnost: Bezpečné
	Typ souborů: Různé

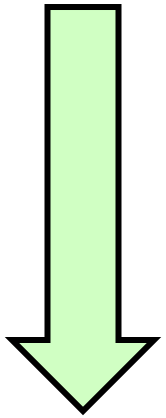
Artefakt2:

Typ:	IP adresa
Hodnota:	191.233.81.105
Štítky:	Závažnost: Trojský kůň
	Platforma: Windows

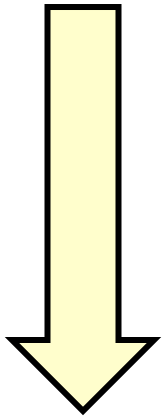
- Nastudování problematiky analýzy škodlivého kódu
- Současný systém a jeho nedostatky
  - statická databáze
  - nepodporuje označování
  - vztahy mezi vzorky a artefakty
- Návrh

- Systém složen ze tří částí:
  1. **Databáze** – prosté artefakty a regulární výrazy
  2. **Webové aplikační rozhraní** – operace s artefakty a štítky, vyhledávání a filtrace
  3. **Feeder** – aktualizace databáze na základě událostí





- **Zimní semestr**
  - Nedostatky současného systému
  - Návrh
  - Implementace databáze



- **Letní semestr**
  - Webové aplikační rozhraní
  - Podpora regulárních výrazů
  - Feeder
  - Testování

Děkuji za pozornost!