Detegovanie anomálií v IP sieťach

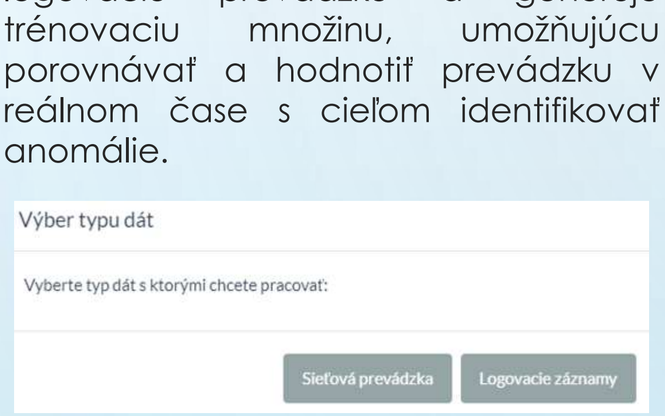
ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta riadenia a informatiky

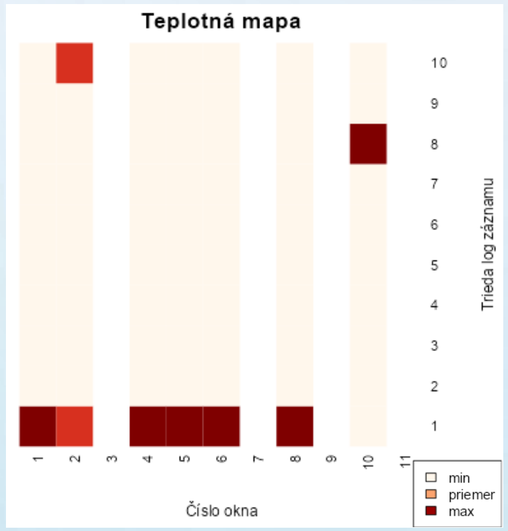
Riešiteľ: Bc. Roman Helis
Vedúci práce: Ing. Ondrej Škvarek, PhD.
Konzultant: prof. Ing. Martin Klimo, PhD.

	time	device	service	severity	process	processNumber	ip	portNumber	packetSize	frame.time_relative
1	2023-06-06 22:08:24	asterisk	voip	ERROR	chan_pjsip.c	2643				0
2	2023-06-06 22:32:30	asterisk	voip	ERROR	chan_pjsip.c	2643				1446
3	2023-06-06 22:56:14	asterisk	voip	ERROR	chan_pjsip.c	2643				2870
4	2023-06-06 23:19:56	asterisk	voip	ERROR	chan_pjsip.c	2643				4292
5	2023-06-06 23:31:56	asterisk	voip	ERROR	chan_pjsip.c	2643				5012

Cieľ

Vytvorenie pokročilého systému, ktorý analyzuje zaznamenanú sieťovú a logovaciu prevádzku a generuje trénovaciu množinu, umožňujúcu porovnávať a hodnotiť prevádzku v reálnom čase s cieľom identifikovať anomálie.



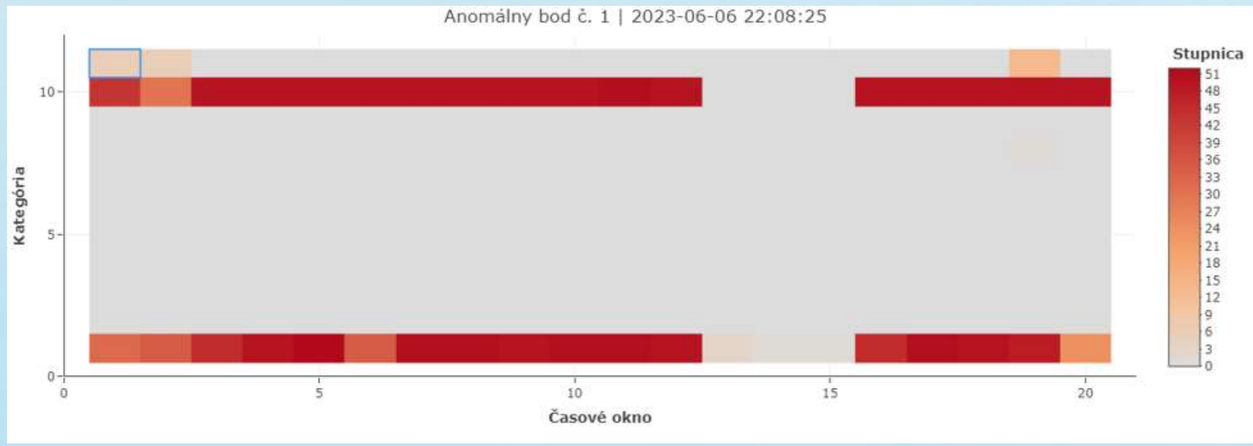


Trénovanie

1. Výber atribútov, podľa ktorých sa budú ďalej dáta spracovať (napr. service, severity, processNumber, ...)
2. Spracovanie logovacích záznamov
3. Kategorizácia dát podľa Shannon-Fanovho kódovania
4. Vytvorenie teplotnej mapy
5. Použitie hierarchického prístupu zhlukovania s výpočtom vzdialeností podľa Euklida, kde body patriace mimo polomeru sú vyhlásené za anomálne

Motivácia

Pomocou zaznamenaných logovacích záznamov sa snažíme detegovať anomálie, ktoré nám pomáhajú pri odhaľovaní a predchádzaniu sieťových útokov.



Detekcia anomálií

Načítajú sa parametre z trénovacej množiny, nastavíme časový interval detekcie nových logovacích záznamov.

Akonáhle je zistený nový logovací súbor, prebehne jeho spracovanie, počas ktorého sú dáta rozdelené do kategórií, porovnané s trénovacou množinou a následne vyhodnotené.