INSyT

Innovative **N**etwork **S**ecurit**y** **T**echnologies

Overview

We present a python package INSyT that utilizes cutting edge large language models in order to monitor and classify raw log line text with the purpose of detecting network intrusions.

INSyT

Outline

1. The Problem
2. The Data
3. The Model
4. The Results
5. The Backend
6. The Front End
7. Future Work

The Problem

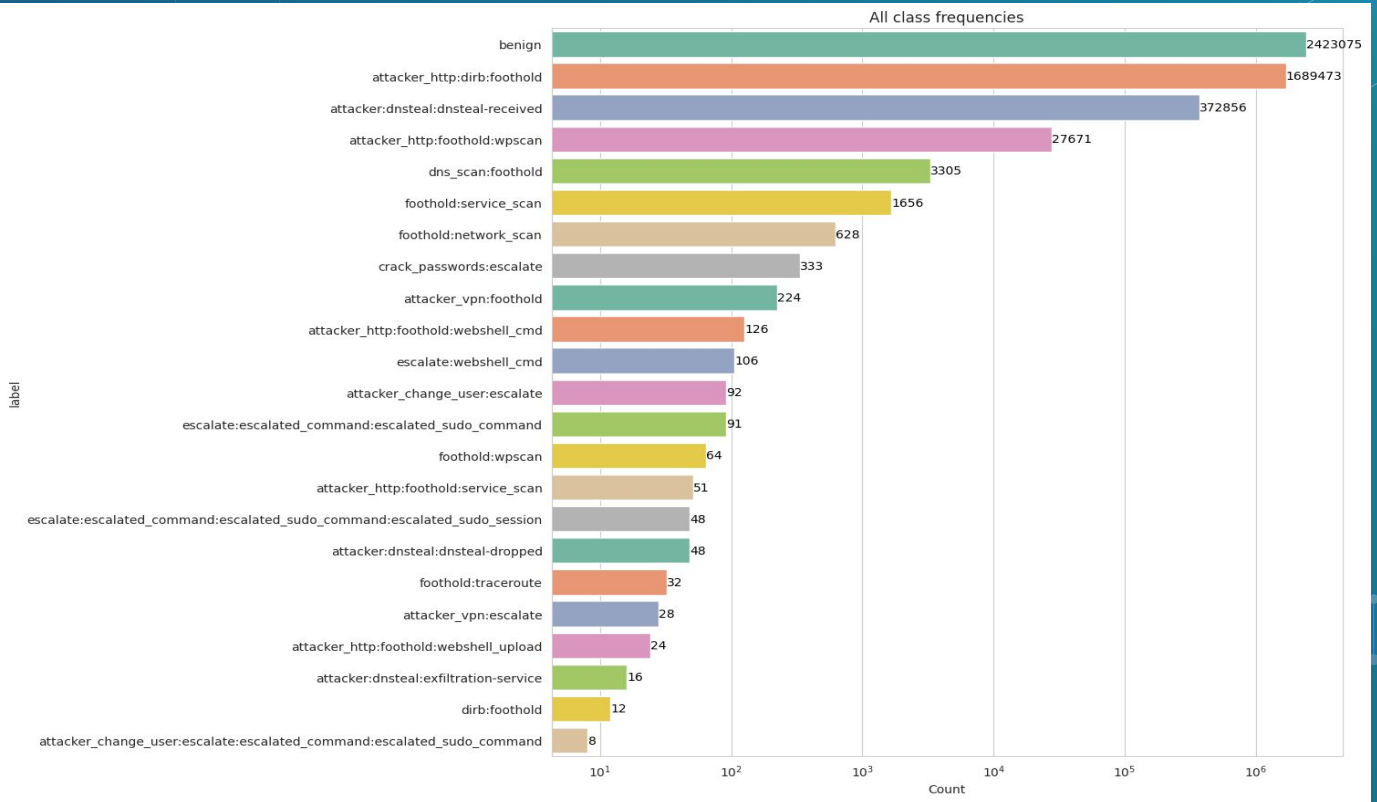
Network intrusion refers to unauthorized access or activity on a computer network, often with malicious intent, such as stealing data or disrupting services. Our goal is to help detect and classify these attacks.

The Data

We found a research group in Australia that simulated 22 different types of attacks on 7 different servers over 7 days and hosted their data publicly[1].

1. Landauer, M., Skopik, F., Frank, M., Hotwagner, W., Wurzenberger, M., & Rauber, A. (2022). AIT Log Data Set V2.0 (v2_0) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.5789064

The Data

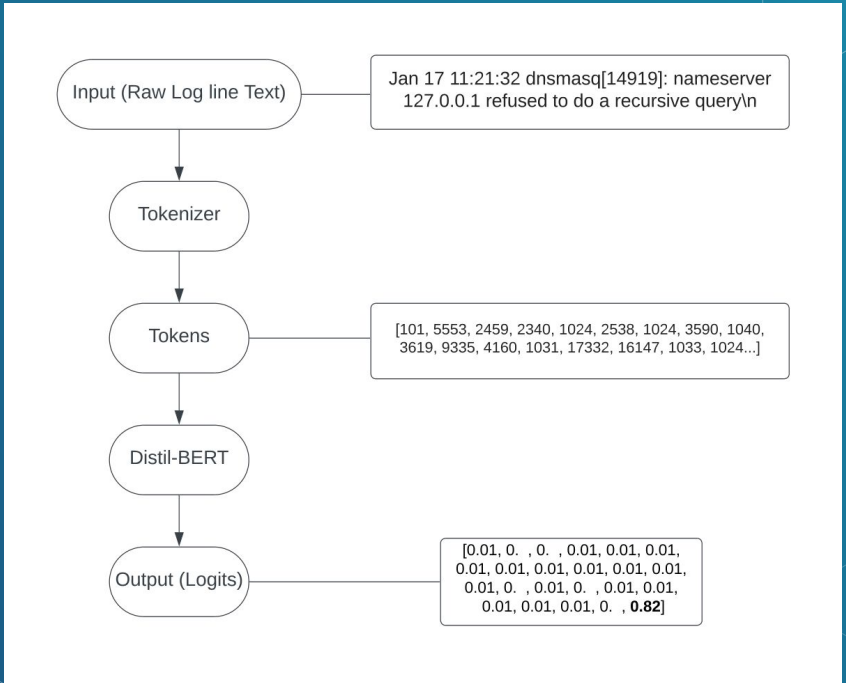


One crucial problem was the class imbalance.

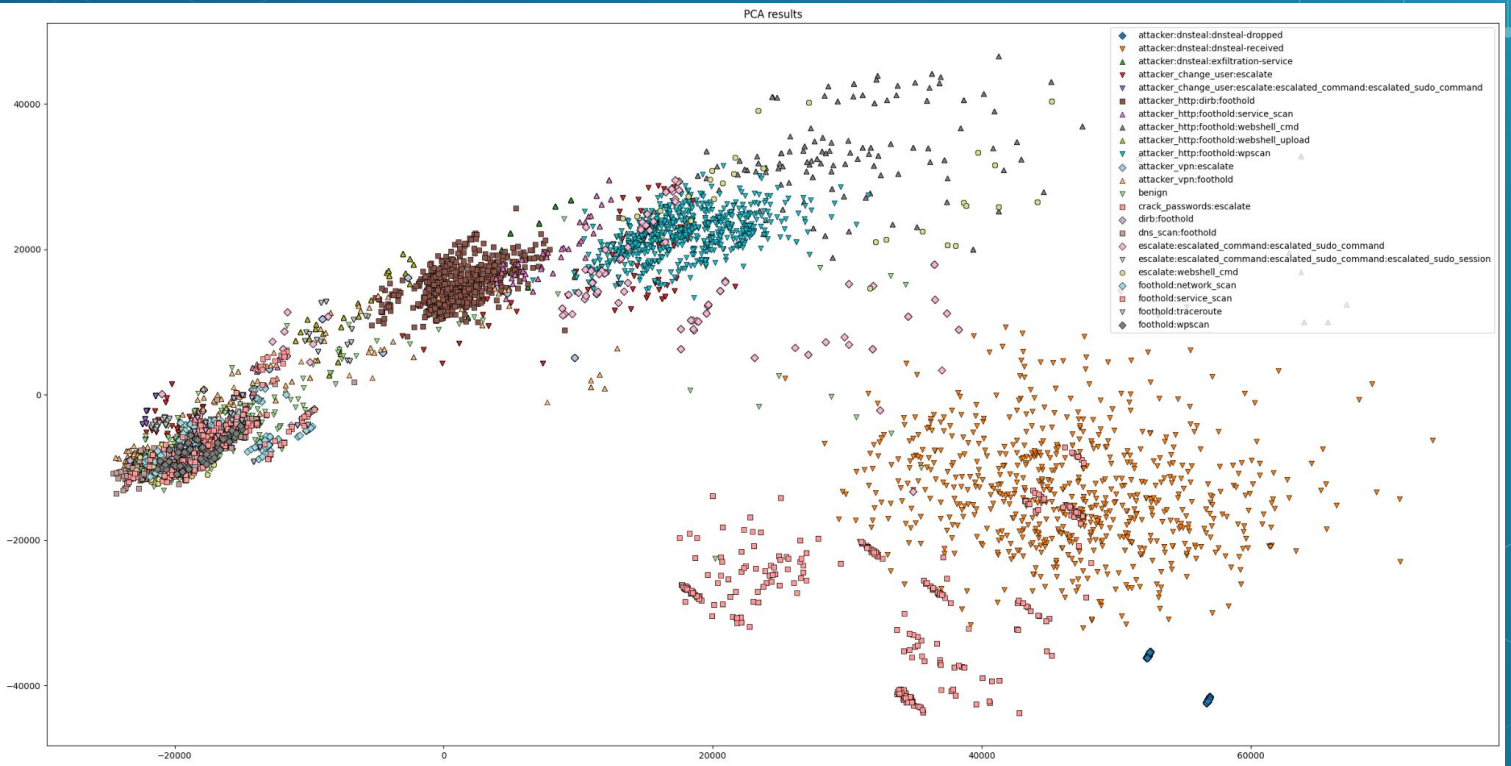
The Model

We used the Distil-BERT classifier for our training model, the BERT model can handle natural language, and being Distil-BERT it can perform quick inference even on a CPU.

The Model

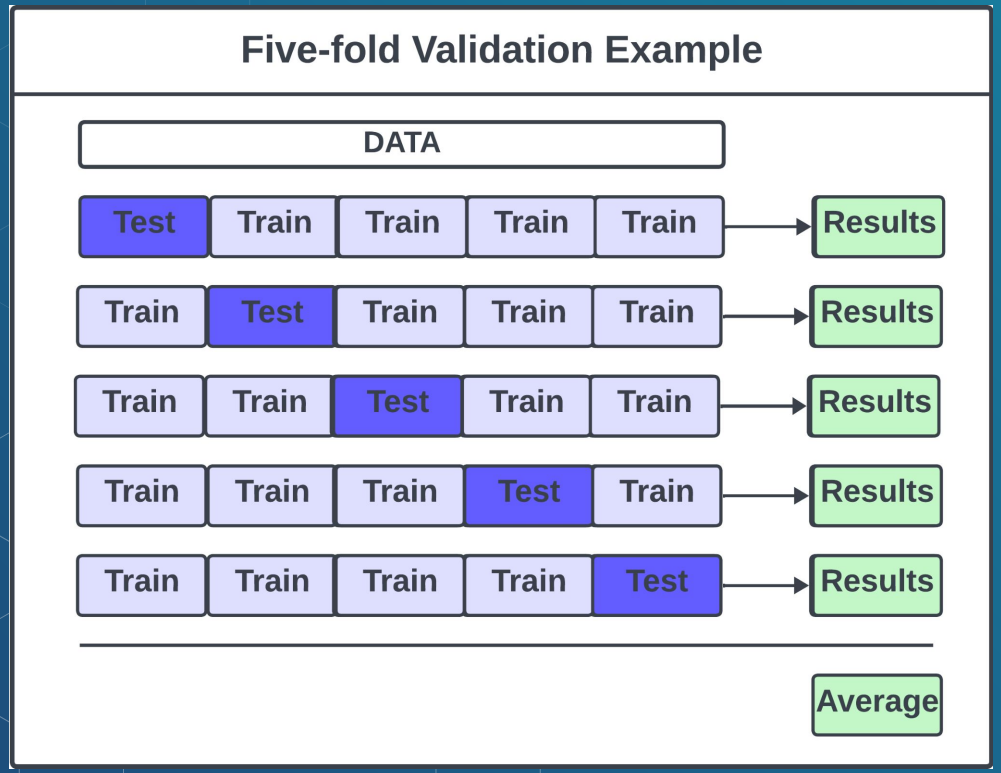

Input (Raw Log line Text)
Jan 17 11:21:32 dnsmasq[14919]: nameserver 127.0.0.1 refused to do a recursive query\n
Tokenizer
Tokens
[101, 5553, 2459, 2340, 1024, 2538, 1024, 3590, 1040, 3619, 9335, 4160, 1031, 17332, 16147, 1033, 1024...]
Distil-BERT
Output (Logits)
[0.01, 0. , 0. , 0.01, 0.01, 0.01, 0.01, 0.01, 0.01, 0.01, 0.01, 0.01, 0.01, 0. , 0.01, 0. , 0.01, 0.01, 0.01, 0.01, 0. , **0.82**]

The Model

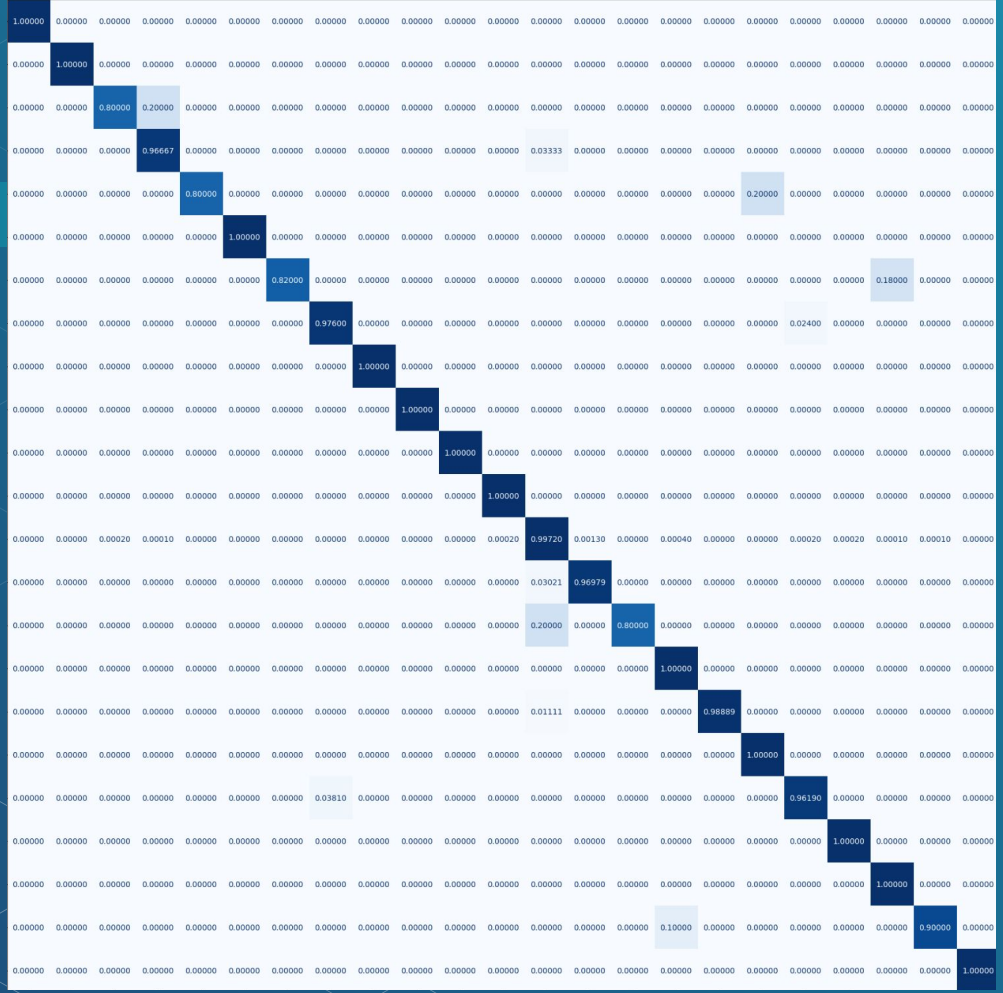


We used PCA to plot the tokenized vectors in 2D space.

The Results

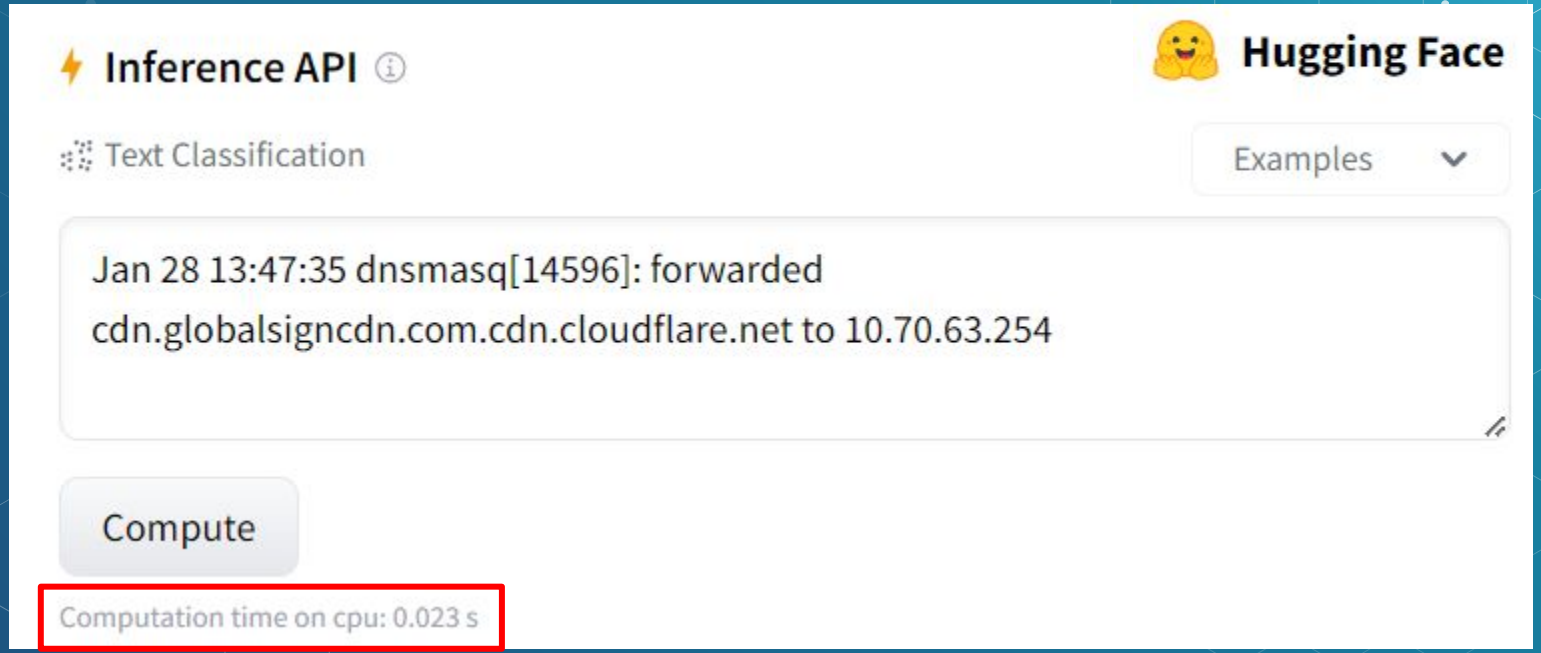


- Stratified sampling
- Five fold cross validation
- Limited to 10,000 samples
- Averaged results of test confusion matrix

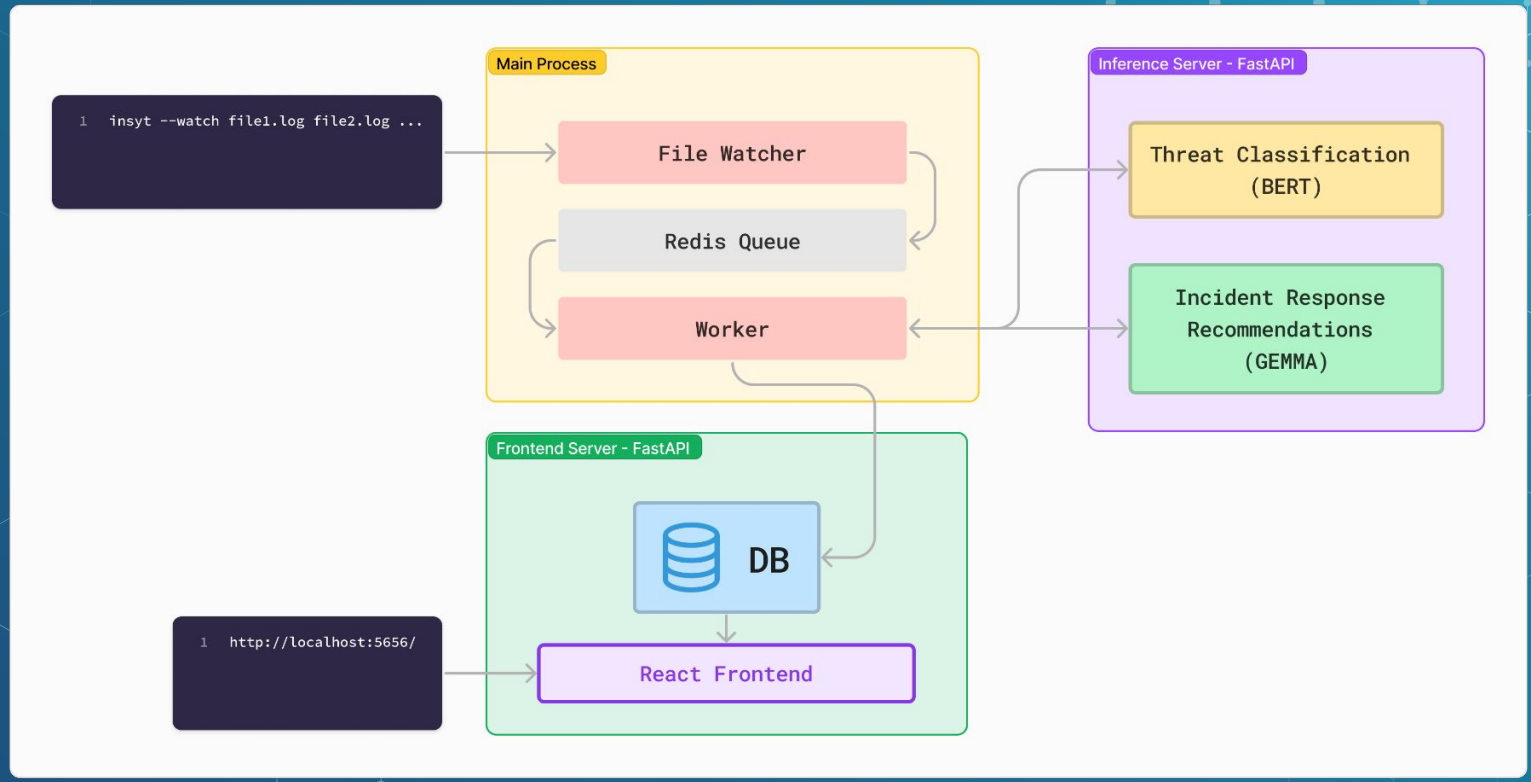


- Even with class imbalance, good results
- A better performance metric would be testing on data outside the dataset

The Results : Inference Speed

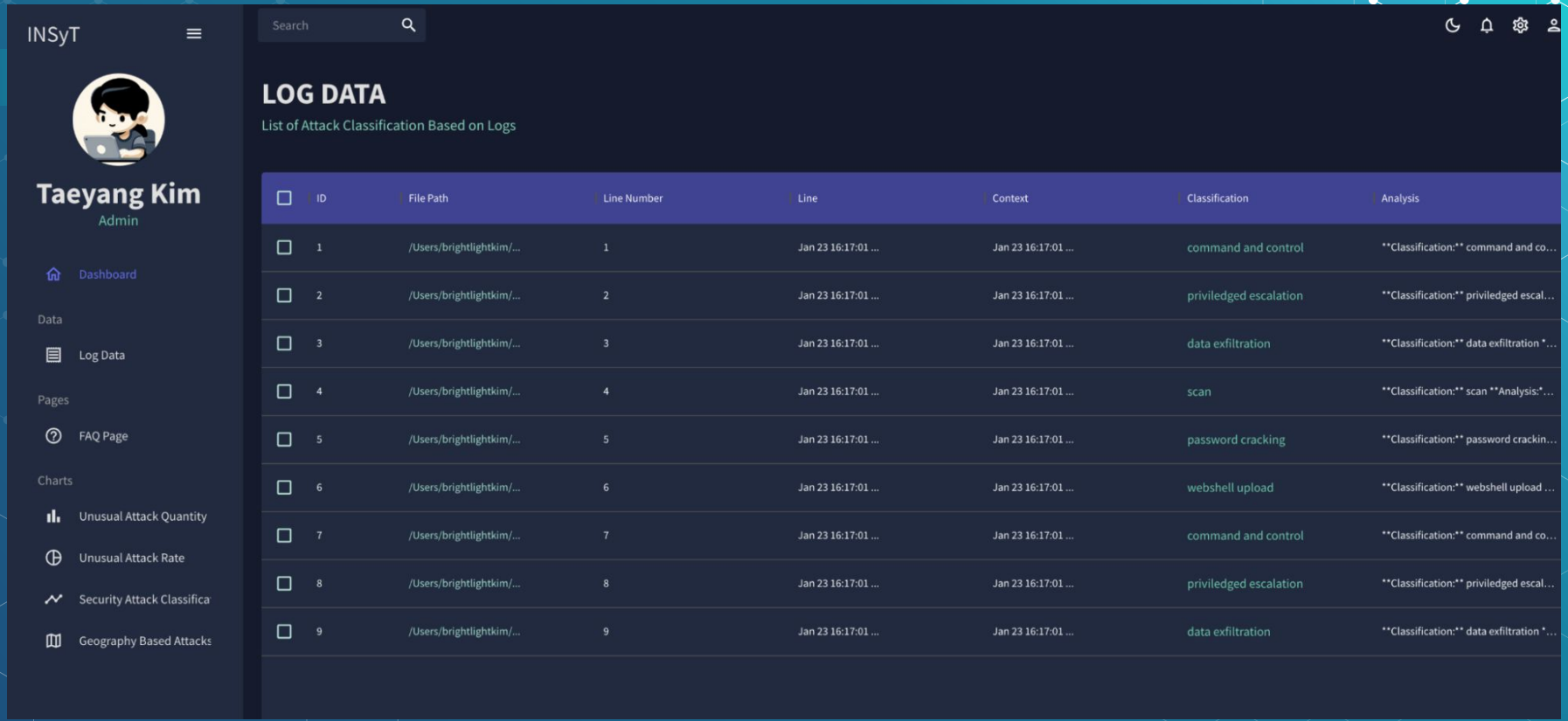


The Backend


INSyT Package
1 insyt --watch file1.log file2.log ...
Main Process
File Watcher
Redis Queue
Worker
Inference Server - FastAPI
Threat Classification (BERT)
Incident Response Recommendations (GEMMA)
Frontend Server - FastAPI
DB
1 http://localhost:5656/
React Frontend

The Package: Demo


INSyT
Search
Taeyang Kim
Admin
Dashboard
Data
Log Data
Pages
FAQ Page
Charts
Unusual Attack Quantity
Unusual Attack Rate
Security Attack Classifica
Geography Based Attacks
DASHBOARD
Welcome to your dashboard
DOWNLOAD REPORTS
12,361
Bugs Reported
+14%
431,225
Attaks Reported
+21%
32,441
Log Data
+5%
1,500
Unusual Attacks
+43%
Security Attack Classification
Total: 53,243
4000
3000
2000
1000
benign
command and control
priviledged escalation
data exfiltration
scan
password cracking
webshell upload
us
france
japan
Recent Attack Classification
01e4dsa
johndoe
2024-03-28
command and control
0315dsaa
jackdower
2024-03-27
priviledge escalation
01e4dsa
aberdohnny
2024-03-25
benign
Unusual Attack Rate
Unusual Attack Quantity
400
350
300
250
200
150
100
50
webshell upload
password crackir
scan
data exfiltration
priviledged escal
Geography Based Attacks


INSyT
Search
Taeyang Kim
Admin
Dashboard
Data
Log Data
Pages
FAQ Page
Charts
Unusual Attack Quantity
Unusual Attack Rate
Security Attack Classifica
Geography Based Attacks
LOG DATA
List of Attack Classification Based on Logs
ID
File Path
Line Number
Line
Context
Classification
Analysis
1 /Users/brightlightkim/... 1 Jan 23 16:17:01 ... Jan 23 16:17:01 ... command and control **Classification:** command and co...
2 /Users/brightlightkim/... 2 Jan 23 16:17:01 ... Jan 23 16:17:01 ... priviledged escalation **Classification:** priviledged escal...
3 /Users/brightlightkim/... 3 Jan 23 16:17:01 ... Jan 23 16:17:01 ... data exfiltration **Classification:** data exfiltration *...
4 /Users/brightlightkim/... 4 Jan 23 16:17:01 ... Jan 23 16:17:01 ... scan **Classification:** scan **Analysis:*...
5 /Users/brightlightkim/... 5 Jan 23 16:17:01 ... Jan 23 16:17:01 ... password cracking **Classification:** password crackin...
6 /Users/brightlightkim/... 6 Jan 23 16:17:01 ... Jan 23 16:17:01 ... webshell upload **Classification:** webshell upload ...
7 /Users/brightlightkim/... 7 Jan 23 16:17:01 ... Jan 23 16:17:01 ... command and control **Classification:** command and co...
8 /Users/brightlightkim/... 8 Jan 23 16:17:01 ... Jan 23 16:17:01 ... priviledged escalation **Classification:** priviledged escal...
9 /Users/brightlightkim/... 9 Jan 23 16:17:01 ... Jan 23 16:17:01 ... data exfiltration **Classification:** data exfiltration *...