

Report for email system event modeler and intrusion detection System

Name: Tan Jing Sen, Edwin and Gonzales Riel Vance

Student Number: 8083150 and 7559136

Initial Input

The program processes two input files, Events.txt and Stats.txt, to model events and detect anomalies effectively.

Storing Input Data:

- **Events Data:** Defines event properties e.g. name/type/range/weight
- **Stats Data:** Provide statistical parameters for each of the event

Validating Input Data:

- Verify event value ranges, weight and type integrity
- Ensure that Events.txt and Stat.txt are consistent.

Directories Setup: Creates directories needed for base logs, monitoring logs and analysis results

Activity Engine

The Activity Engine uses event parameters and statistical data to simulate daily activity.

Log Generation:

- Simulation of event data based on mean and standard deviation.
- Event values respect defined ranges and are rounded appropriately

Log saved in JSON format:

- logs/baseline for baseline phase data.
- logs/monitoring for real-time monitoring data.

Progress Feedback: Updates every 5 days or at the process end for simulations spanning multiple days.

Analysis Engine

The Analysis Engine calculates baseline statistics for each event over the simulated days.

Statistics Calculation:

- Compute mean and standard deviation for every event over simulated baseline data
- Output stored in baseline_stats.json

Dynamic Monitoring:

- Accept new statistics dynamically during runtime for iterative monitoring
- Ensure that updated statistics and event definitions are consistent

Alert Engine

Detects anomalies by comparing current data with baseline statistics.

Anomaly Detection: Anomalies are flagged if the daily anomaly counter exceeds twice the total event weights.

Deviation Calculation:

- Addition of weighted deviations from the anomaly counter
- Event importance determine absolute deviations

Reporting:

- Generates daily reports which include anomaly counters, deviations and status
- Save all the alert details as JSON files in the analysis directory

Summary

This program is a flexible and efficient solution for event modelling and anomaly detection. With the combination of flexible input handling, dynamic monitoring, detailed reporting and robust validation, it is reliable as a solution for intrusion detection. Its modular architecture supports extensibility and scalability which ensures the ability to adapt to changing requirements