CSCI262 – System Security

Assignment 3

Timothy Mah

8750634

txamah001@mymail.sim.edu.sg

Initial Input

```python
class Event:
    def __init__(self, event_type, min_val, max_val, weight, name, mean, sd):
        self.type = event_type
        self.min = min_val
        self.max = max_val
        self.weight = weight
        self.name = name
        self.mean = mean
        self.sd = sd

    def generate_data(self, size):
        data = np.random.normal(loc=self.mean, scale=self.sd, size=size)
        return np.clip(data, self.min, self.max).astype(int) if self.type == 'D' else data
```

Each event is stored in a class object that holds event type (C or D), event name, min, max, weight, mean, and SD.

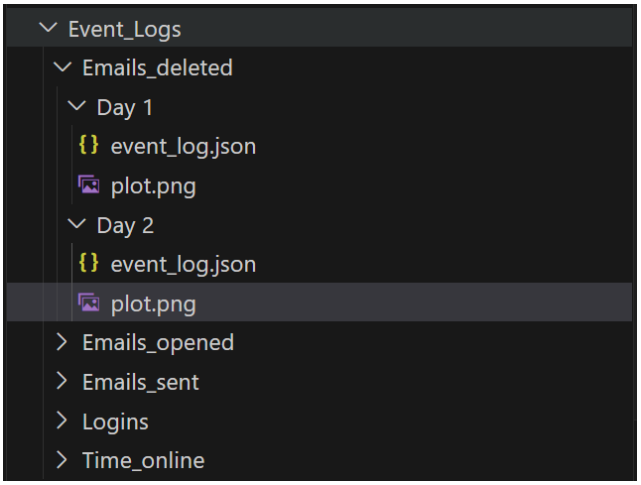
```
Data loaded:
No of days: 2
Logins          - Type: D, Range: 0.0-10.0, Mean: 6.0, SD: 4.0
Time online     - Type: C, Range: 0.0-40.5, Mean: 10.0, SD: 5.0
Emails sent     - Type: D, Range: 0.0-20.0, Mean: 3.0, SD: 2.0
Emails opened   - Type: D, Range: 0.0-25.0, Mean: 2.0, SD: 3.0
Emails deleted  - Type: D, Range: 0.0-53.0, Mean: 10.0, SD: 5.0


...Data generated liao!!
```

The app will echo the data read in from Events.txt and Stats.txt

```
Mean + SD
-----------
Logins          { day 1 mean: 5.96 day 2 mean: 5.71, expected mean: 6.0 }
Logins          { day 1 SD: 2.87 day 2 SD: 3.22, expected SD: 4.0 }
Time online     { day 1 mean: 10.74 day 2 mean: 9.97, expected mean: 10.0 }
Time online     { day 1 SD: 4.77 day 2 SD: 5.23, expected SD: 5.0 }
Emails sent     { day 1 mean: 2.38 day 2 mean: 2.54, expected mean: 3.0 }
Emails sent     { day 1 SD: 1.88 day 2 SD: 2.02, expected SD: 2.0 }
Emails opened   { day 1 mean: 2.08 day 2 mean: 1.67, expected mean: 2.0 }
Emails opened   { day 1 SD: 2.39 day 2 SD: 2.46, expected SD: 3.0 }
Emails deleted  { day 1 mean: 10.17 day 2 mean: 9.83, expected mean: 10.0 }
Emails deleted  { day 1 SD: 3.82 day 2 SD: 3.92, expected SD: 5.0 }
```

There will be inconsistency with generated mean and SD, and the expected mean and SD specified in Stats.txt. The app displays the inconsistencies towards the end of runtime.

Activity Engine and Logs

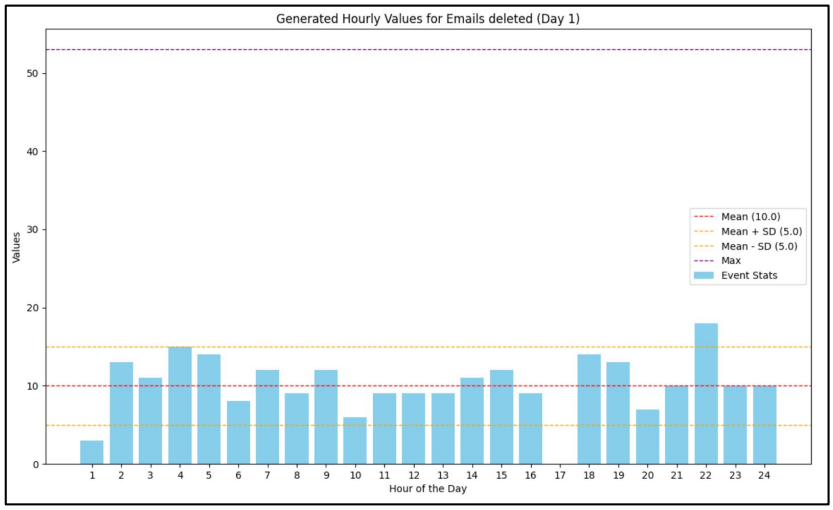


Events are stored in a folder named Event_logs. Within this parent folder, there are sub folders for the each day the user has input when running the app. In the image, there are two days.

ids.py {} event_log.json 1 ●

Event_Logs > Emails_deleted > Day 1 > {} event_log.json > ...


```
{"event": "Emails deleted", "message": "Event occurred 3 times", "hour": 1, "times": 3}
{"event": "Emails deleted", "message": "Event occurred 13 times", "hour": 2, "times": 13}
{"event": "Emails deleted", "message": "Event occurred 11 times", "hour": 3, "times": 11}
{"event": "Emails deleted", "message": "Event occurred 15 times", "hour": 4, "times": 15}
{"event": "Emails deleted", "message": "Event occurred 14 times", "hour": 5, "times": 14}
{"event": "Emails deleted", "message": "Event occurred 8 times", "hour": 6, "times": 8}
{"event": "Emails deleted", "message": "Event occurred 12 times", "hour": 7, "times": 12}
{"event": "Emails deleted", "message": "Event occurred 9 times", "hour": 8, "times": 9}
{"event": "Emails deleted", "message": "Event occurred 12 times", "hour": 9, "times": 12}
{"event": "Emails deleted", "message": "Event occurred 6 times", "hour": 10, "times": 6}
{"event": "Emails deleted", "message": "Event occurred 9 times", "hour": 11, "times": 9}
{"event": "Emails deleted", "message": "Event occurred 9 times", "hour": 12, "times": 9}
{"event": "Emails deleted", "message": "Event occurred 9 times", "hour": 13, "times": 9}
{"event": "Emails deleted", "message": "Event occurred 11 times", "hour": 14, "times": 11}
{"event": "Emails deleted", "message": "Event occurred 12 times", "hour": 15, "times": 12}
{"event": "Emails deleted", "message": "Event occurred 9 times", "hour": 16, "times": 9}
{"event": "Emails deleted", "message": "Event occurred 0 times", "hour": 17, "times": 0}
{"event": "Emails deleted", "message": "Event occurred 14 times", "hour": 18, "times": 14}
{"event": "Emails deleted", "message": "Event occurred 13 times", "hour": 19, "times": 13}
{"event": "Emails deleted", "message": "Event occurred 7 times", "hour": 20, "times": 7}
{"event": "Emails deleted", "message": "Event occurred 10 times", "hour": 21, "times": 10}
{"event": "Emails deleted", "message": "Event occurred 18 times", "hour": 22, "times": 18}
{"event": "Emails deleted", "message": "Event occurred 10 times", "hour": 23, "times": 10}
{"event": "Emails deleted", "message": "Event occurred 10 times", "hour": 24, "times": 10}
```

Within each day, there is a log file named event_log.json and a graph of the events named plot.png. Each event is plot across a 24-hour period. The log file is in JSON format to emulate real world logging with applications such as Loki. Discrete events are stored and processed as integers while continuous events are stored and processed as float values.

Analysis Engine

ids.py 2 | analysis_results.txt

analysis_results.txt

```
ANALYSIS ENGINE:
Mean + SD
-----------
Logins          { day 1 mean: 5.96, day 2 mean: 5.58, expected mean: 6.0 }
Logins          { day 1 SD: 3.33, day 2 SD: 3.37, expected SD: 4.0 }
Time online     { day 1 mean: 11.58, day 2 mean: 11.36, expected mean: 10.0 }
Time online     { day 1 SD: 5.70, day 2 SD: 5.50, expected SD: 5.0 }
Emails sent     { day 1 mean: 3.08, day 2 mean: 3.12, expected mean: 3.0 }
Emails sent     { day 1 SD: 1.50, day 2 SD: 1.96, expected SD: 2.0 }
Emails opened   { day 1 mean: 1.46, day 2 mean: 1.79, expected mean: 2.0 }
Emails opened   { day 1 SD: 1.44, day 2 SD: 1.93, expected SD: 3.0 }
Emails deleted  { day 1 mean: 9.58, day 2 mean: 8.17, expected mean: 10.0 }
Emails deleted  { day 1 SD: 4.95, day 2 SD: 3.71, expected SD: 5.0 }

Totals
-----------
Logins          { 277 }
Time online     { 550.3907037572159 }
Emails sent     { 149 }
Emails opened   { 78 }
Emails deleted  { 426 }
```

The totals along with generated mean and SD, are printed into a file named analysis_results.txt

Alert Engine

```
/ids.py Events.txt Stats.txt 2
Data loaded:
No. of days: 2
Logins          - Type: D, Range: 0.0-10.0, Mean: 6.0, SD: 4.0
Time online     - Type: C, Range: 0.0-40.5, Mean: 10.0, SD: 5.0
Emails sent     - Type: D, Range: 0.0-20.0, Mean: 3.0, SD: 2.0
Emails opened   - Type: D, Range: 0.0-25.0, Mean: 2.0, SD: 3.0
Emails deleted  - Type: D, Range: 0.0-53.0, Mean: 10.0, SD: 5.0

...Data generated liao!!

Enter the path to a new Stats.txt or press 'q' to quit: Stats2.txt
Data loaded:
No. of days: 2
Logins          - Type: D, Range: 0.0-10.0, Mean: 6.0, SD: 3.0
Time online     - Type: C, Range: 0.0-40.5, Mean: 10.0, SD: 4.0
Emails sent     - Type: D, Range: 0.0-20.0, Mean: 3.0, SD: 1.0
Emails opened   - Type: D, Range: 0.0-25.0, Mean: 2.0, SD: 4.0
Emails deleted  - Type: D, Range: 0.0-53.0, Mean: 10.0, SD: 6.0

...Data generated liao!!

Enter the path to a new Stats.txt or press 'q' to quit: q
Exiting program.
```

The program will run an initial data generation and analysis as baseline. Then it takes user input for another stats file. Then it performs data generation and analysis against the baseline. This process repeats until user enters ‘q’. All subsequent stats file loaded will be analysed against the baseline.

Event_Logs > analysis_results.txt

```
ANALYSIS ENGINE: Mean + SD
-----------
Logins          { day 1 mean: 4.71 day 2 mean: 5.38, expected mean: 6.0 }
Logins          { day 1 SD: 2.39 day 2 SD: 2.60, expected SD: 4.0 }
Time online     { day 1 mean: 10.03 day 2 mean: 9.89, expected mean: 10.0 }
Time online     { day 1 SD: 4.66 day 2 SD: 5.28, expected SD: 5.0 }
Emails sent     { day 1 mean: 3.00 day 2 mean: 2.08, expected mean: 3.0 }
Emails sent     { day 1 SD: 1.35 day 2 SD: 1.38, expected SD: 2.0 }
Emails opened   { day 1 mean: 2.96 day 2 mean: 2.54, expected mean: 2.0 }
Emails opened   { day 1 SD: 2.77 day 2 SD: 2.21, expected SD: 3.0 }
Emails deleted  { day 1 mean: 10.79 day 2 mean: 11.08, expected mean: 10.0 }
Emails deleted  { day 1 SD: 4.45 day 2 SD: 4.11, expected SD: 5.0 }

Totals
-----------
Logins          { 242 }
Time online     { 477.9189255753997 }
Emails sent     { 122 }
Emails opened   { 132 }
Emails deleted  { 525 }

Anomaly Detection
-----------
Day 1 Logins         : Anomaly Score: 107.00, Threshold: 452, Status: Passed
Day 2 Logins         : Anomaly Score: 123.00, Threshold: 516, Status: Passed
Day 1 Time online    : Anomaly Score: 276.73, Threshold: 1443.6318999386308, Status: Passed
Day 2 Time online    : Anomaly Score: 272.78, Threshold: 1423.8816535137676, Status: Passed
Day 1 Emails sent    : Anomaly Score: 345.00, Threshold: 720, Status: Passed
Day 2 Emails sent    : Anomaly Score: 235.00, Threshold: 500, Status: Passed
Day 1 Emails opened  : Anomaly Score: 46.00, Threshold: 142, Status: Passed
Day 2 Emails opened  : Anomaly Score: 39.33, Threshold: 122, Status: Passed
Day 1 Emails deleted : Anomaly Score: 199.20, Threshold: 1036, Status: Passed
Day 2 Emails deleted : Anomaly Score: 204.80, Threshold: 1064, Status: Passed
```

This is the analysis results and anomaly detection of the baseline. Since it is the baseline, all days' anomaly score would be under threshold hence all days pass.

Event_Logs2 > analysis_results.txt

```
ANALYSIS ENGINE: Mean + SD
-----------
Logins          { day 1 mean: 5.25 day 2 mean: 5.75, expected mean: 6.0 }
Logins          { day 1 SD: 3.03 day 2 SD: 2.88, expected SD: 3.0 }
Time online     { day 1 mean: 9.80 day 2 mean: 10.11, expected mean: 10.0 }
Time online     { day 1 SD: 3.78 day 2 SD: 4.17, expected SD: 4.0 }
Emails sent     { day 1 mean: 2.67 day 2 mean: 2.50, expected mean: 3.0 }
Emails sent     { day 1 SD: 1.37 day 2 SD: 1.06, expected SD: 1.0 }
Emails opened   { day 1 mean: 1.75 day 2 mean: 2.67, expected mean: 2.0 }
Emails opened   { day 1 SD: 2.45 day 2 SD: 3.51, expected SD: 4.0 }
Emails deleted  { day 1 mean: 8.71 day 2 mean: 10.38, expected mean: 10.0 }
Emails deleted  { day 1 SD: 5.53 day 2 SD: 6.30, expected SD: 6.0 }

Totals
-----------
Logins          { 264 }
Time online     { 477.7124747910643 }
Emails sent     { 124 }
Emails opened   { 106 }
Emails deleted  { 458 }

Anomaly Detection
-----------
Day 1 Logins         : Anomaly Score: 160.00, Threshold: 452, Status: Passed
Day 2 Logins         : Anomaly Score: 176.00, Threshold: 516, Status: Passed
Day 1 Time online    : Anomaly Score: 337.67, Threshold: 1443.6318999386308, Status: Passed
Day 2 Time online    : Anomaly Score: 348.90, Threshold: 1423.8816535137676, Status: Passed
Day 1 Emails sent    : Anomaly Score: 610.00, Threshold: 720, Status: Passed
Day 2 Emails sent    : Anomaly Score: 570.00, Threshold: 500, Status: Failed
Day 1 Emails opened  : Anomaly Score: 20.00, Threshold: 142, Status: Passed
Day 2 Emails opened  : Anomaly Score: 31.00, Threshold: 122, Status: Passed
Day 1 Emails deleted : Anomaly Score: 132.67, Threshold: 1036, Status: Passed
Day 2 Emails deleted : Anomaly Score: 159.33, Threshold: 1064, Status: Passed
```

This is the second analysis and anomaly detection of the second run. The stats file used has different parameters from the stats file used to generate baseline hence there are events that are beyond baseline threshold, marked as failed.