# TOWARDS BUILDING NETWORK OUTLIER DETECTION SYSTEM FOR NETWORK TRAFFIC MONITORING


***Josef Koumar***, CESNET a.l.e. & CTU in Prague

*Jaroslav Pešek*, *CESNET a.l.e. & CTU in Prague*

*Kamil Jeřábek*, *CESNET a.l.e. & BUT*

*Tomáš Čejka*, *CESNET a.l.e. & CTU in Prague*

# MOTIVATION

There are several challenges which slow Machine Learning adoption to the practise of detection of security threats in network traffic:

- Present of data drifts in normal network traffic
- Novel threats or versions of the known one
- Lack of datasets from real-world environment
- Features are often based on specific parameters of the network, thus, limited transferability

These limitation cause high false positive rates in deployment of current classification and detection approaches

# OUR FOCUSE

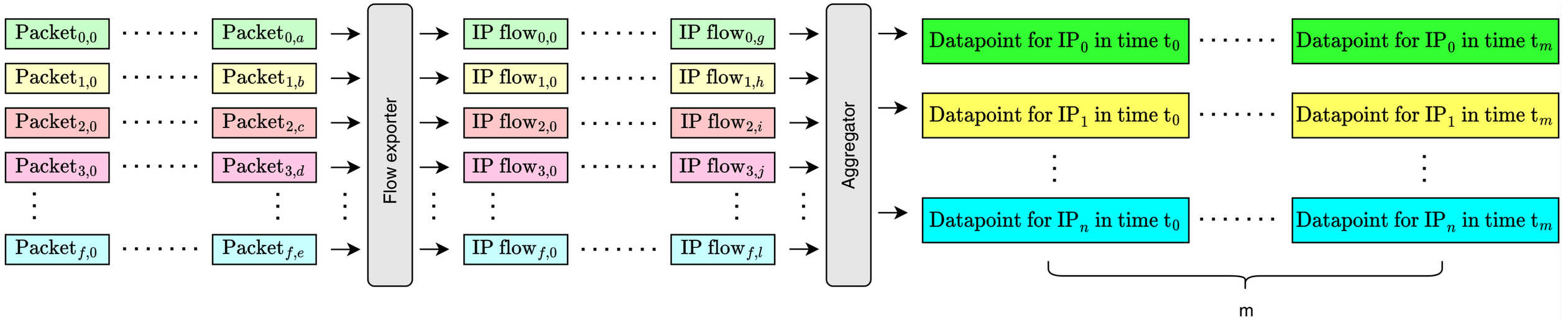
Therefore, we focuse on the detection of outliers (anomalies, abnormalities) which do not have these limitations.

The outlier is a data point that deviates significantly from other observed data points, enough to raise suspicion that it was generated by a different mechanism.

The deviation of outlier from observed data can be, for example, based on distribution, trend or seasonality.

cesnet

# NETWORK TRAFFIC PROCESSING



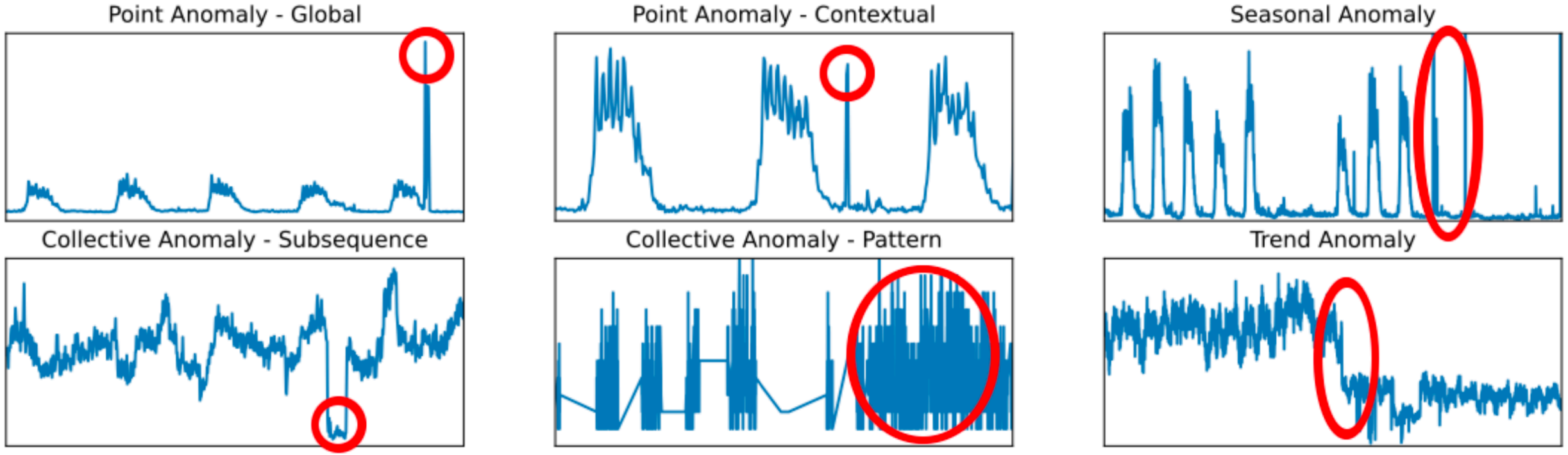
# DEFINITION OF DATAPOINT

The datapoint from the network traffic forms the time series. These time series are multivariate with following time series metrics:

- Number of IP flows, packets, bytes
- Number of unique destination IP addresses
- Number of unique destination ASNs
- Number of unique destination countries
- TCP/UDP ratio
- Packet direction ratio
- Average TTL and duration of IP flows

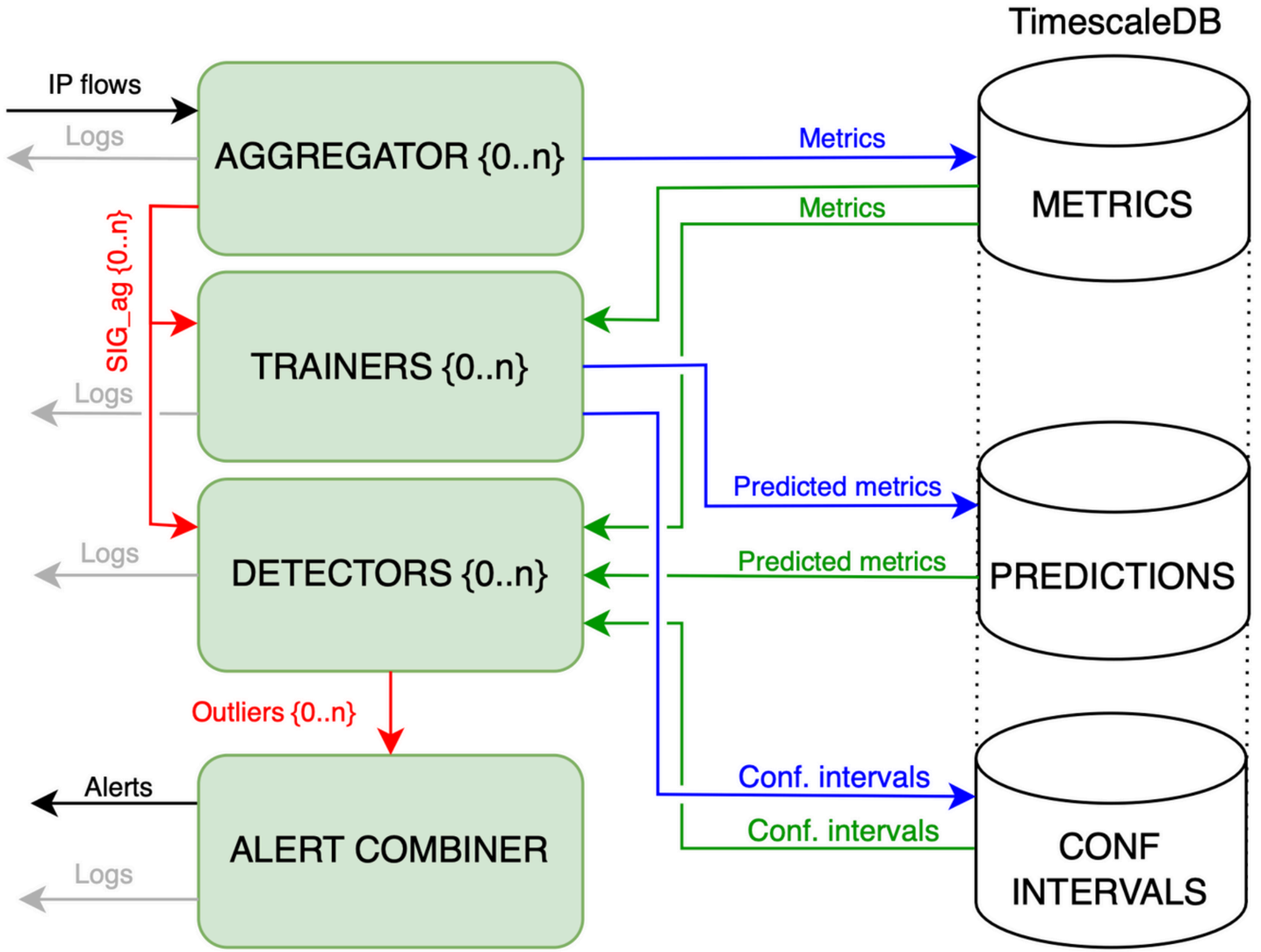
cesnet

# TYPE OF OUTLIERS IN NETWORK TRAFFIC



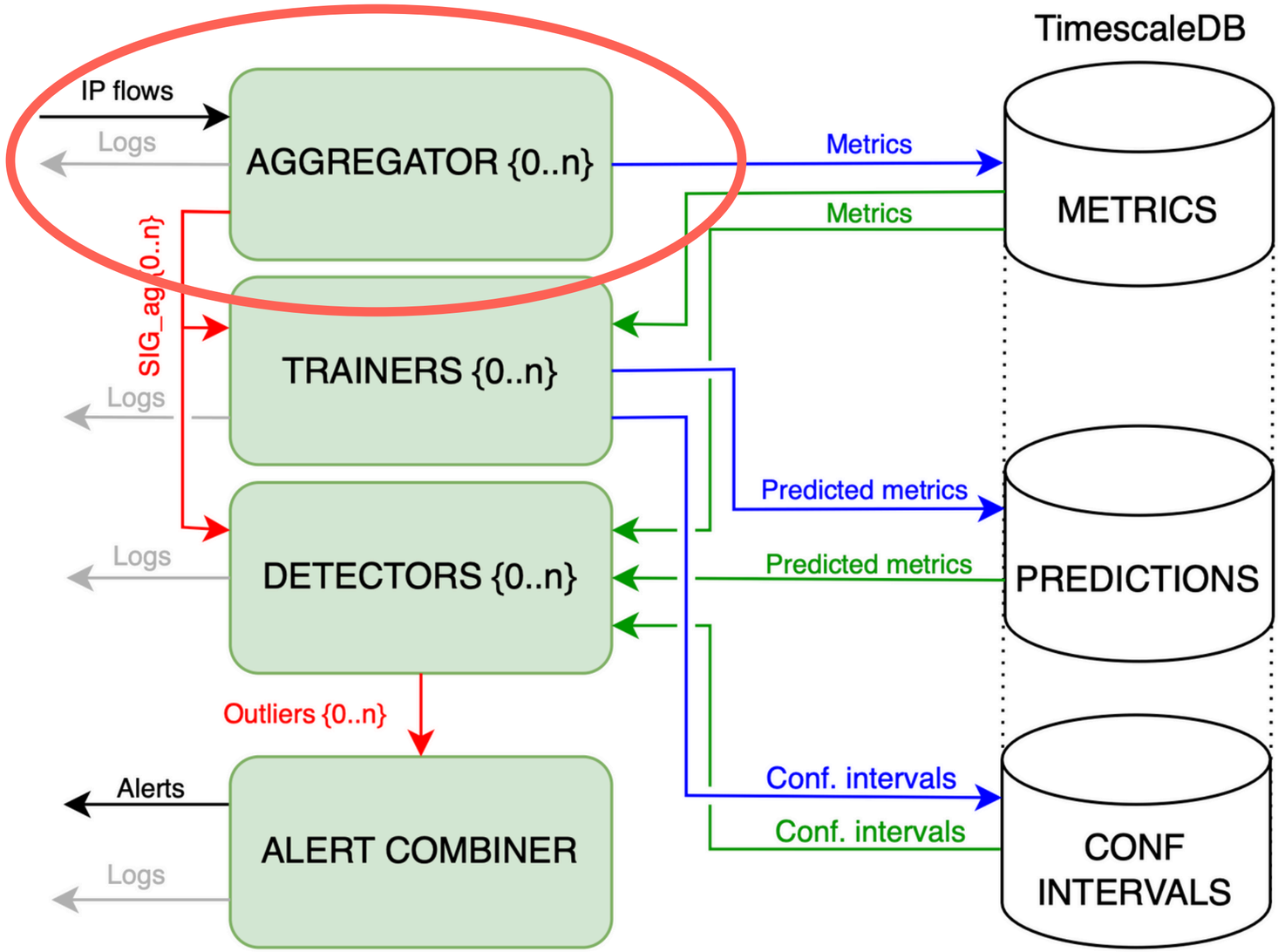
# NETWORK OUTLIER DETECTION SYSTEM (NODS)

- **Built from open-source software**
- Enable deployment of anomaly/outlier detection methods based on the **forecasting of network traffic** in real-world scenarios
- **Successfully deployed** on the **real-world ISP network CESNET3**



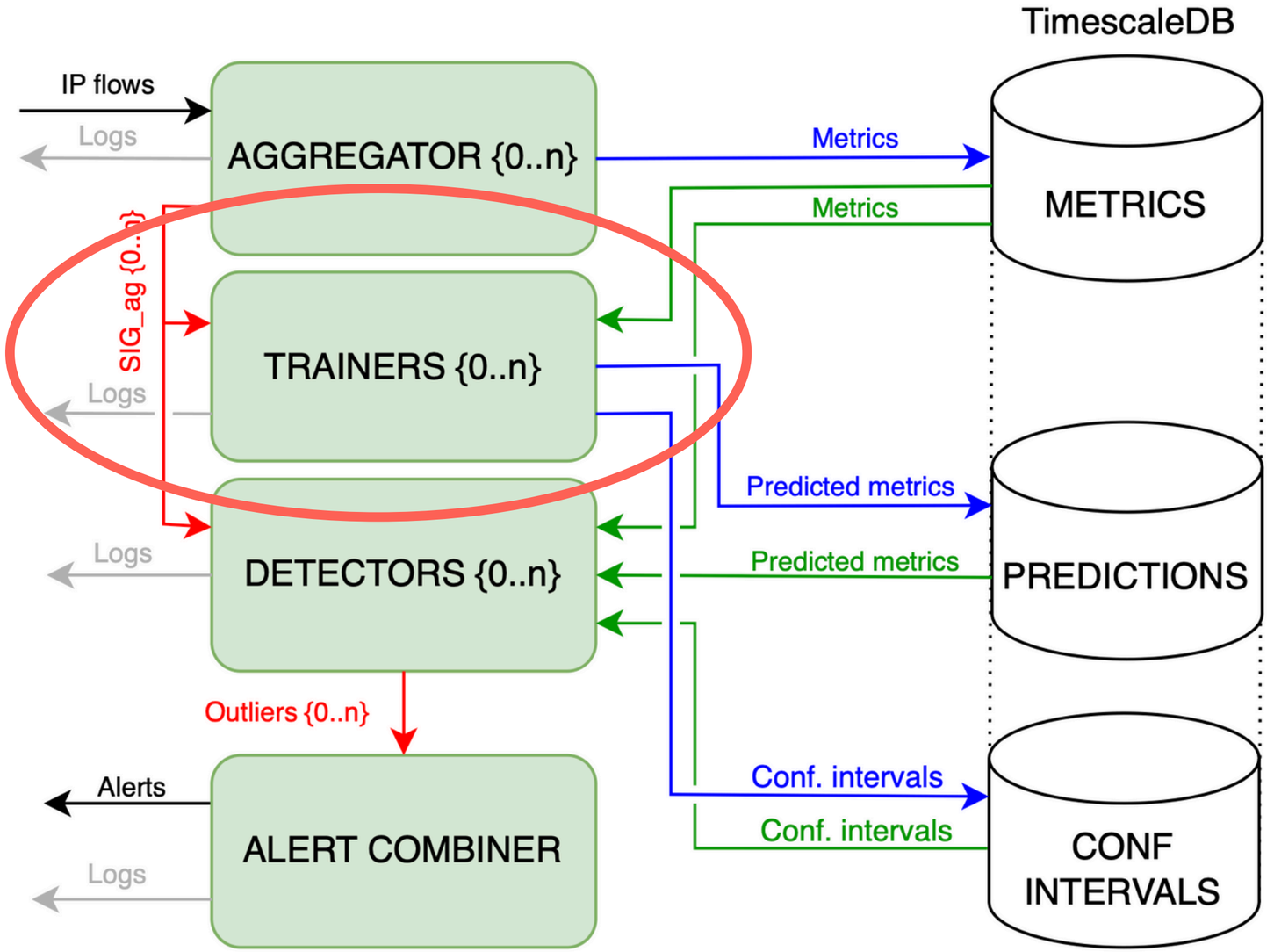
# AGGREGATOR

- Aggregates IP flows into datapoints
- Push datapoints into database
- Send control signal to Trainers and Detectors modules
- Multiple Aggregators run in the system



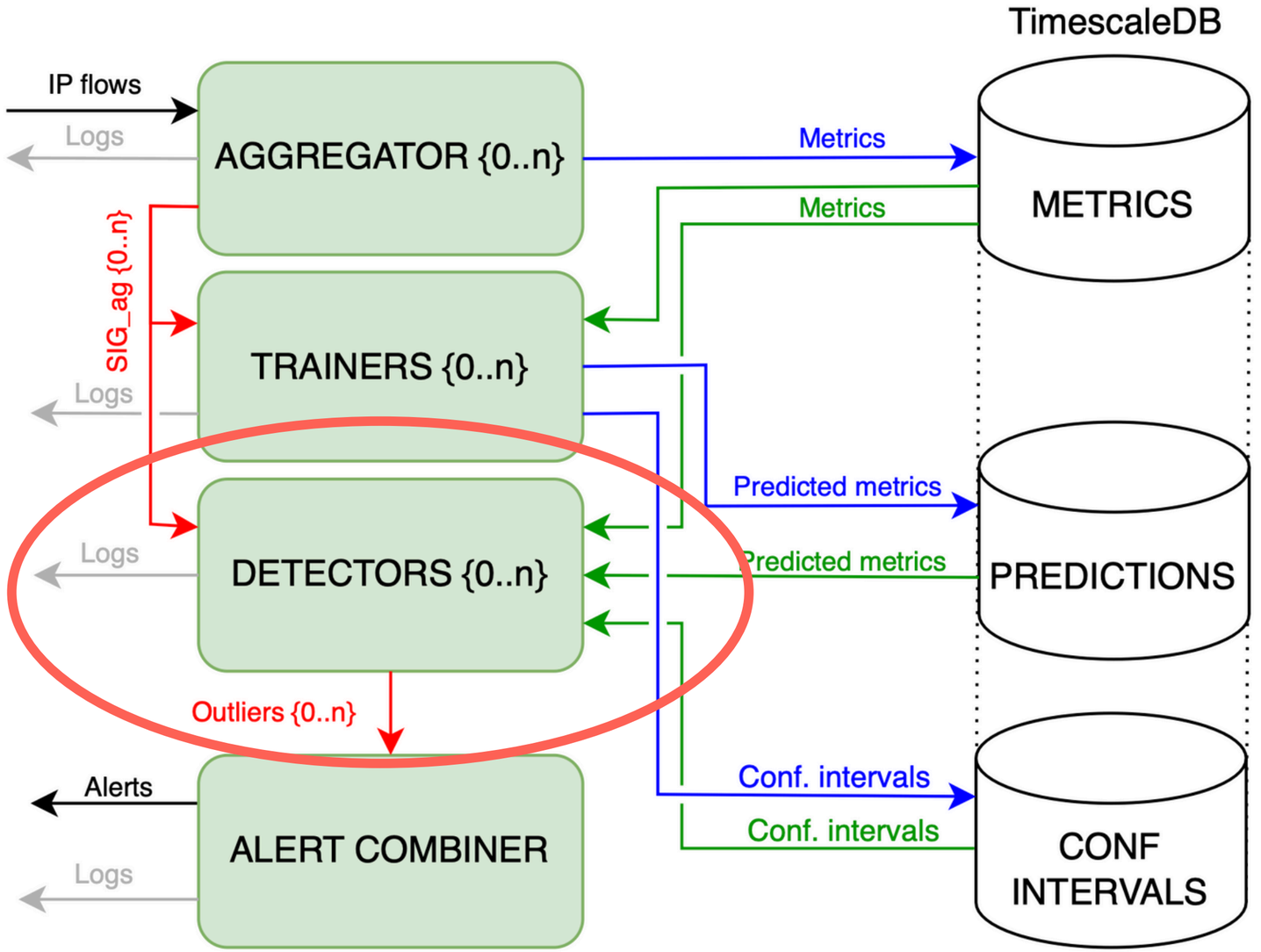
# TRAINERS

- Trainers module **manage training** of models
- Receives signal from the Aggregator module to run processes
- **Run trainer routine of model** if the training period of model pass
- After trainer rutine of model finish training process it push predictions into DB



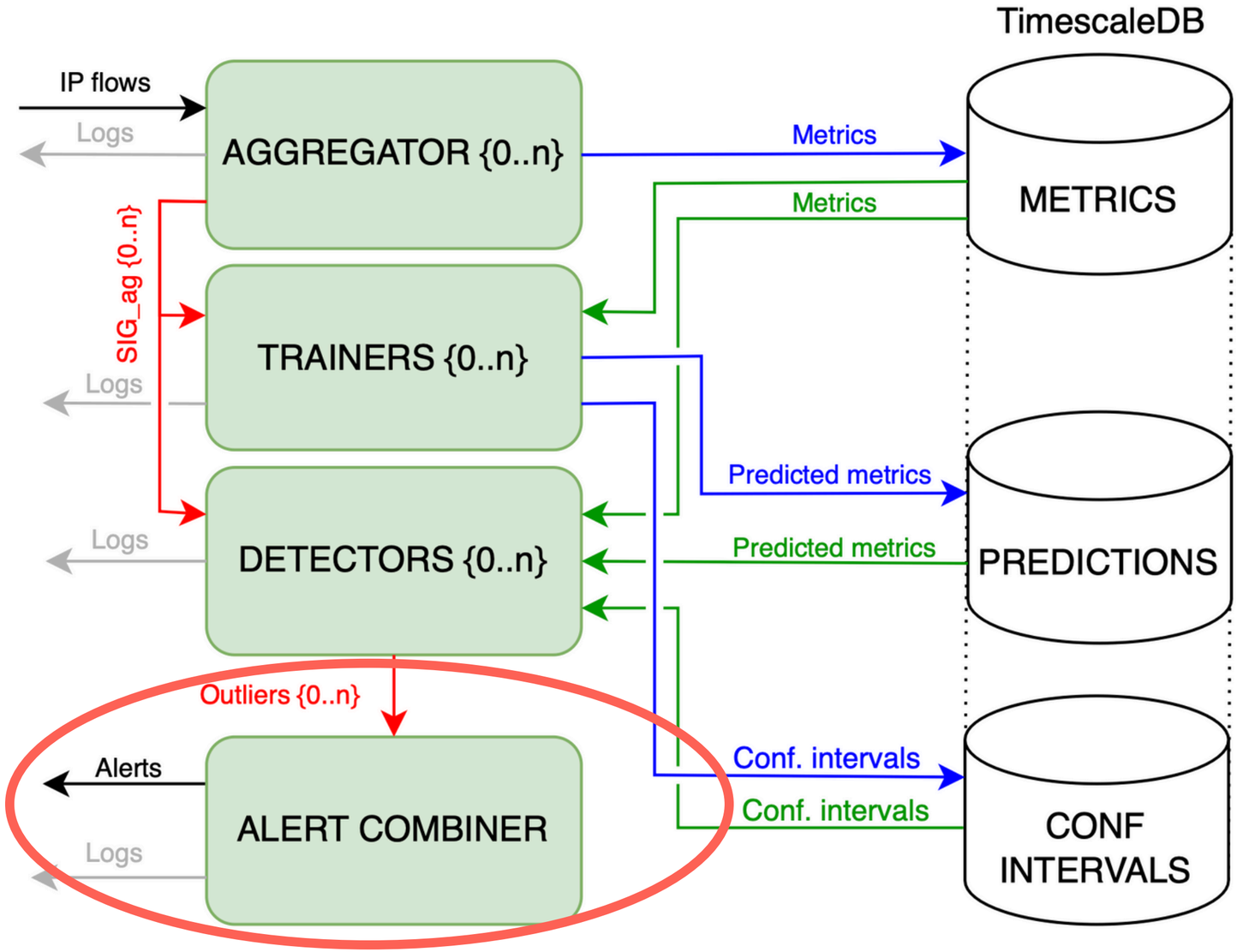
# DETECTORS

- Detectors module **manage detection process** of models
- Detection process for forecasting based outlier detectors is the **comparison of observed values with forecasted values**
- Outliers are sent to the Alert Combiner module



# ALERT COMBINER

- **Multiple detectors operate on various time series metrics**, which can lead to the same anomaly being detected multiple times across different detectors.
- To reduce redundant alerts and ease the load on the SoC team, the Alert Combiner module consolidates these detections by **grouping outliers** with the same timestamp, and applying **categorization**.



# SYSTEM PROCESSES

**Aggregator**

- Capturing datapoints
- Push datapoints into DB
- w — Aggregation window

**Trainers**

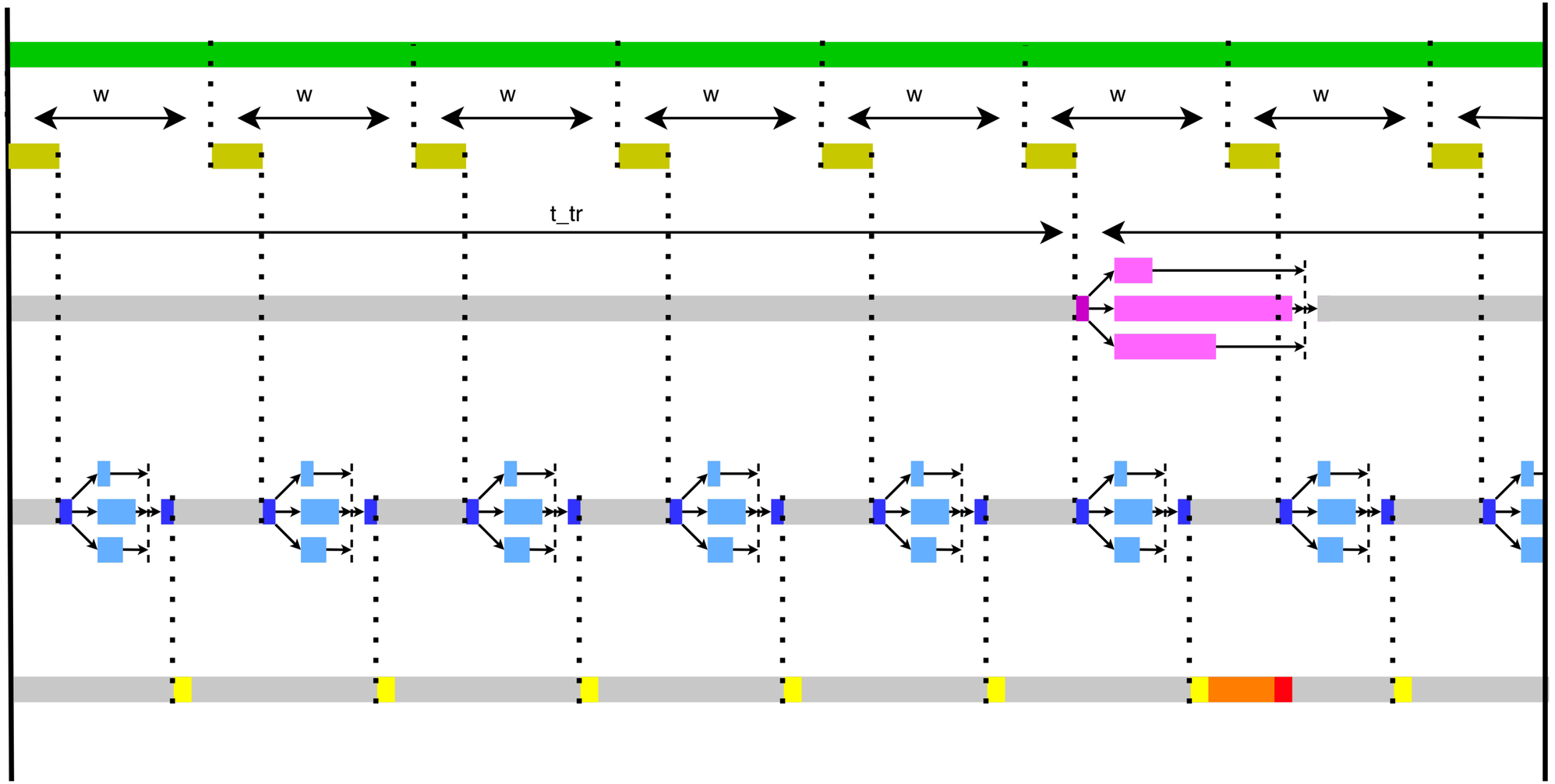
- Trainers maintener n-th trainer running Trainers maintener waiting Trainer
- t_tr — window

**Detectors**

- Detectors maintener
- n-th detector running
- Detectors maintener waiting

**Alert Combiner**

- Collecting anomalies
- Combination of anomalies
- Export incidents
- Alert Combiner waiting

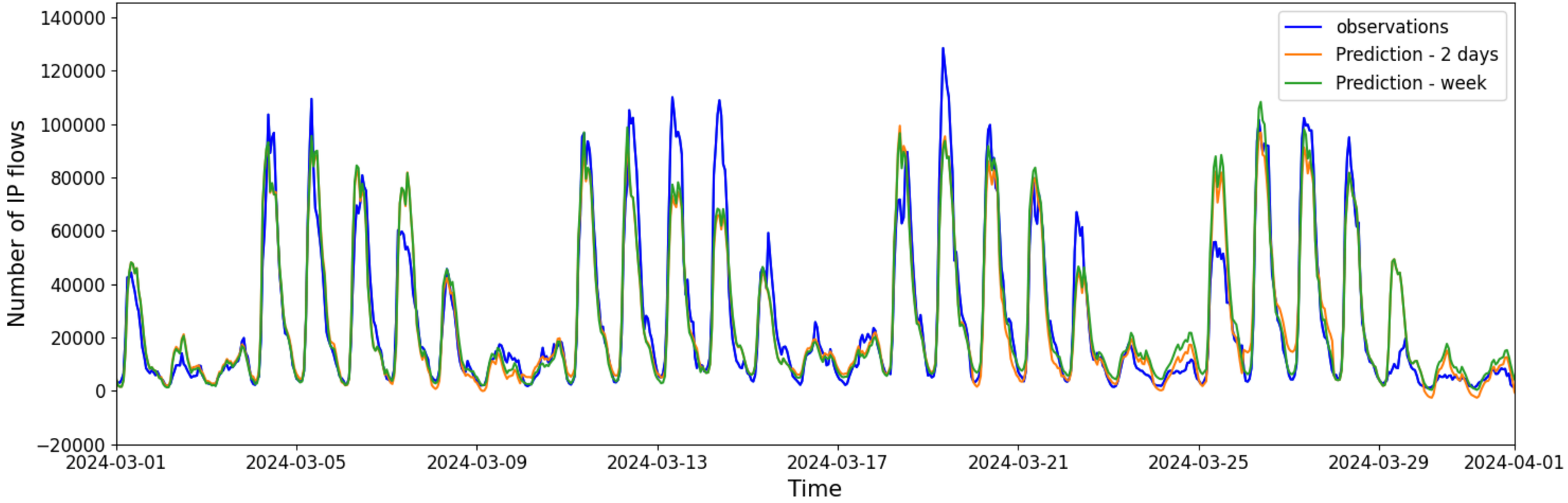


# DEPLOYMENT

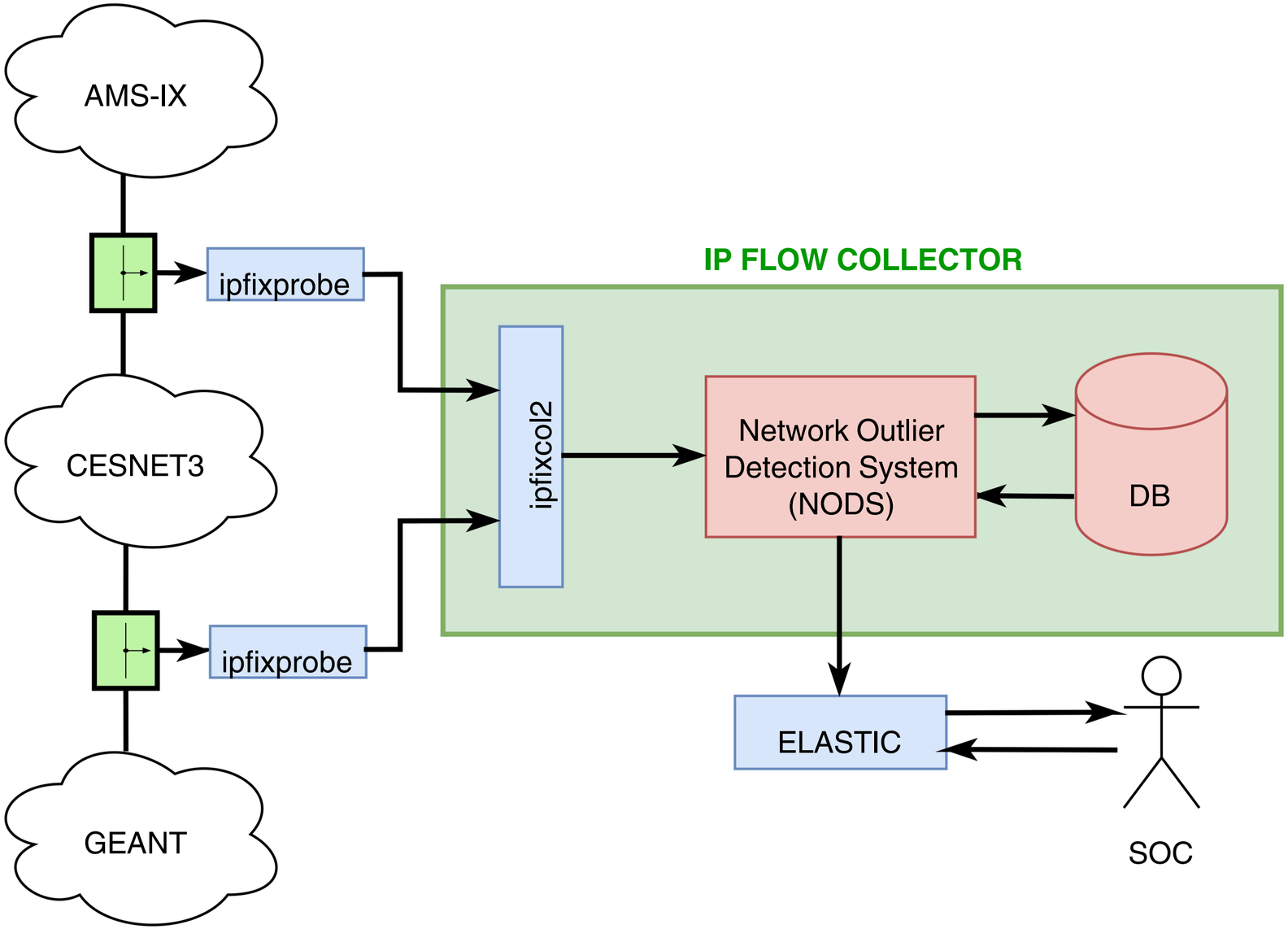
In the first deployment of NODS, we used following models:

- Mean Outlier Detection (MOD)
- Differential Outlier Detector (DOD)
- Seasonal Autoregressive Integrated Moving Average (SARIMA)

By now we are ready do deploy GRU-FCN forecasting model.



# DEPLOYMENT

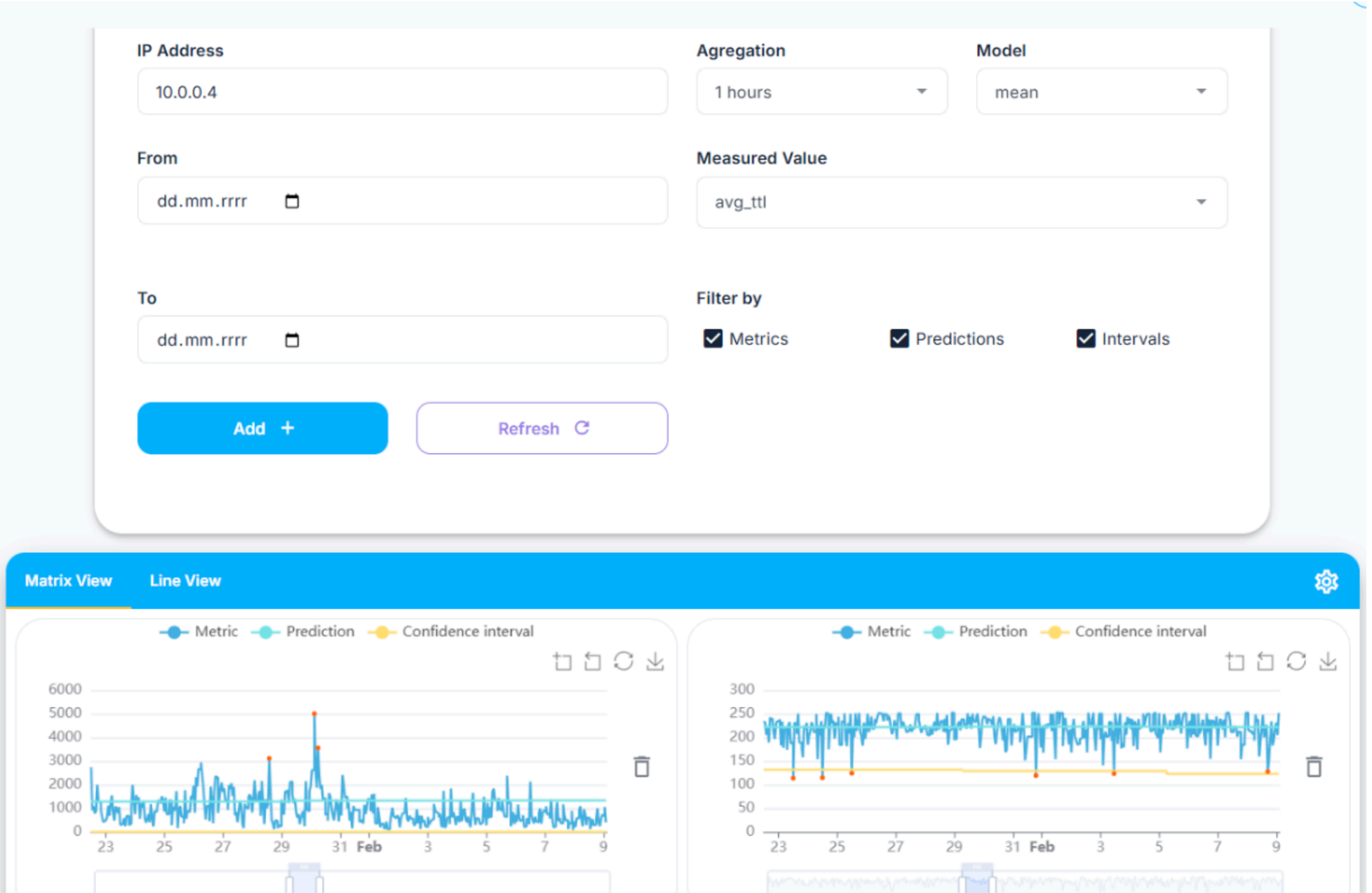



- We deploy the system into CESNET3 network (Czech Education and Science Network)
- Monitored 100k active IP addresses
- Detected ~ 500k outliers for 10 minutes aggregation interval in one month (0.11%)
- Detected ~ 390k outliers for one hour aggregation interval in one month (0.52%)
- Marked ~ 3k incidents as crucial

# LESSONS LEARNED

- High false positives after cold start
  → use learning phase
- Alerting everything to SoC team
  → risk of all detection being ignored due too False Positives
- Only ~0.17% of datapoints marked as outliers, but the absolute number of outelirs is too many to handle by SoC
  → group into incidents for SoC
- Diverse anomalies detected which are hard to evaluate for non-experts
  → consider LLM-based interpretation
- ISP-level scans add noise
  → filter early to improve detection
- IP address with sparse traffic
  → weakens forecasting and obtaining high number of False Positive

# FUTURE WORK


IP Address
10.0.0.4
Agregation
1 hours
Model
mean
From
dd.mm.rrrr
Measured Value
avg_ttl
To
dd.mm.rrrr
Filter by
Metrics
Predictions
Intervals
Add +
Refresh
Matrix View
Line View
Metric
Prediction
Confidence interval
6000
5000
4000
3000
2000
1000
0
23
25
27
29
31
Feb
3
5
7
9
Metric
Prediction
Confidence interval
300
250
200
150
100
50
0
23
25
27
29
31
Feb
3
5
7
9

# SIDE EFFECTS OF WORK

We created **CESNET TimeSeries24 dataset** which contains time series created from **66 billion IP flows** that contain **4 trillion packets** that carry approximately **3.7 petabytes of data**

Time Series Metrics:

- Number of IP flows, packets, bytes
- Number of unique destination IP addresses
- Number of unique destination ASNs
- Number of unique destination countries
- TCP/UDP ratio
- Packet direction ratio
- Average TTL and duration of IP flows

Aggegation:

- 10 minutes
- 1 hour
- 1 day

Identifiers:

- IP addresses
- Institutions
- Institution subnets

cesnet

# THANK YOU FOR YOUR ATTENTION

CESNET TimeSeries24

dataset

CESNET TS-Zoo library