Antagonist

https://datatracker.ietf.org/doc/draft-netana-nmop-network-anomaly-semantics/
https://datatracker.ietf.org/doc/draft-netana-nmop-network-anomaly-lifecycle/

IETF 121 - Dublin

3rd November 2024

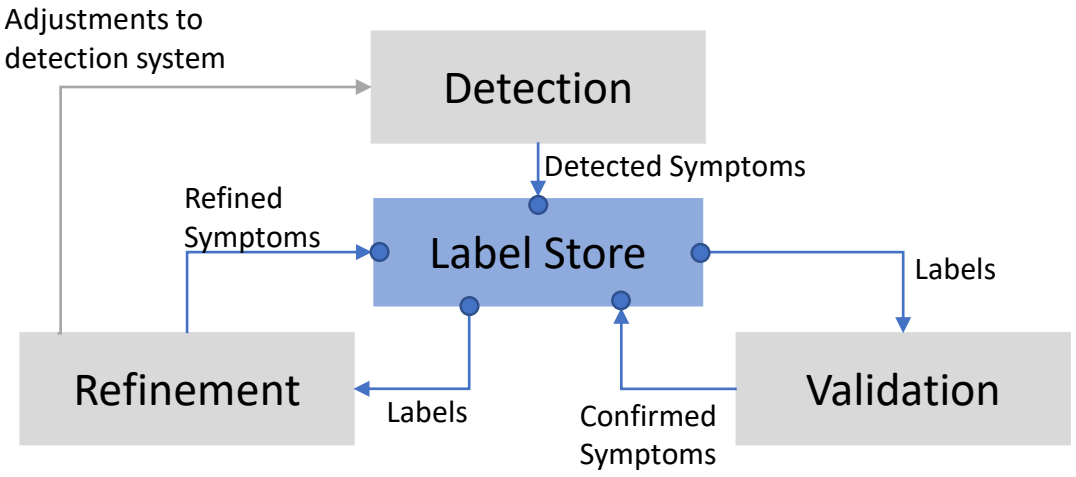
NMOP WG

Presenter: Vincenzo Riccobene

Team: Vincenzo Riccobene, Antonio Roberto, Thomas Graf, Wanting Du, Alex Huang Feng

Antagonist – ANomaly TAGging ON hISTorical data

- Antagonist is a **Label Store for network anomaly detection**
- It addresses two main challenges in the network anomaly detection domain:
  - The **creation of labelled datasets** to train and evaluate anomaly detection algorithms and technologies
  - The **support for the human-in-the-loop paradigm** for what concerns the automated anomaly detection process.



Detection: Continuous monitoring of the network through Network Telemetry [RFC9232] and runtime identification of symptoms.
[Validated with Human-based, Rule-based, ML-based]

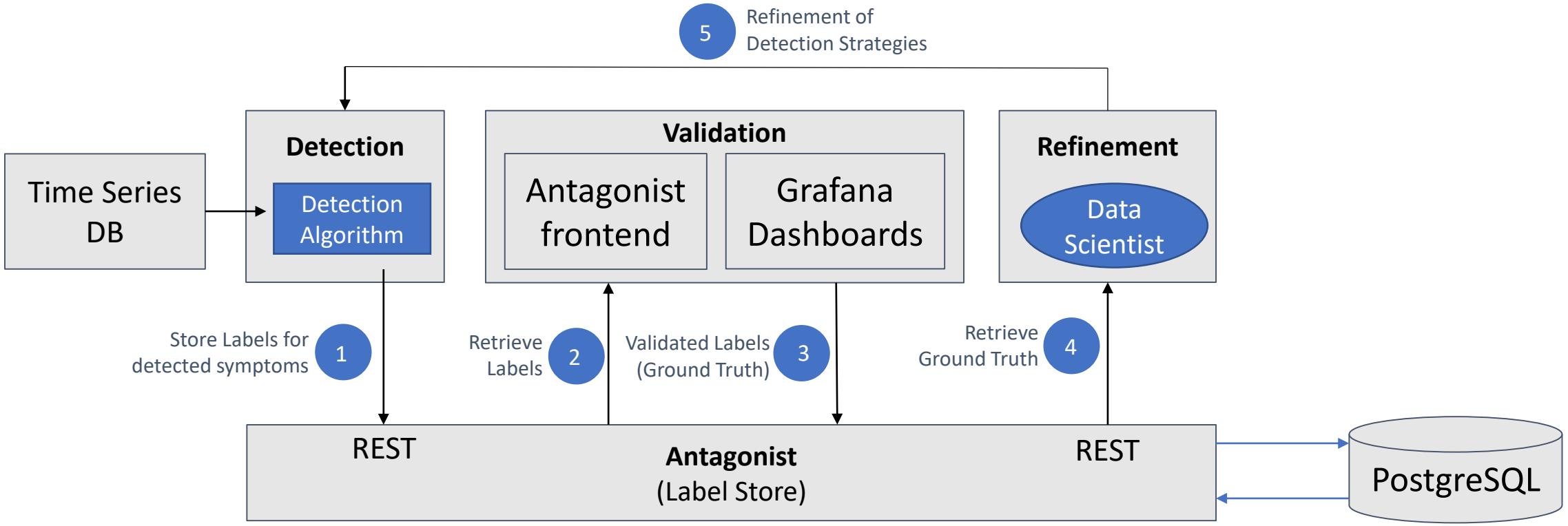
Validation: Verify if the detected symptoms are actually associated to a network incident or issue.

Refinement: Adjustment of the detection mechanism, to improve accuracy. This can include: update of the symptom expressions for SAIN, and retraining AI-based Network Anomaly Detection models

Work previously done on Antagonist

Antagonist – Development of Backend and Frontend to enable network experts to provide labels

- ✓ Implement Anomaly Label persistency and retrieval on PostgreSQL
- ✓ Implement REST API
- ✓ Integrate with timeseries data (via plugin mechanism)
- ✓ Implement Frontend GUI for data exploration, validation and refinement
- ✓ Implement automatic dashboard generation



What was done for the hackathon

- ✓Continued working on the integration of Antagonist with our implementation of RFC 9418 (rule-based anomaly detector).
- ✓Identified gaps in the YANG data models for the Label Store API and updated them for the notification of relevant states
- ✓Extended YANG main data model enabling an augmentation-based extension mechanism to support the different analysed use cases

Next Steps:

- ❑Update the REST API to reflect the new YANG data model
- ❑Integrate with Swisscom Lab

Anomaly Label Data Model

```
module: ietf-relevant-state
  +--rw relevant-state
     +--rw id              yang:uuid
     +--rw description?    string
     +--rw start-time      yang:date-and-time
     +--rw end-time?       yang:date-and-time
     +--rw anomalies* [id version]
        +--rw id                          yang:uuid
        +--rw version                     yang:counter32
        +--rw state                       identityref
        +--rw description?                string
        +--rw start-time                  yang:date-and-time
        +--rw end-time?                   yang:date-and-time
        +--rw confidence-score            score
        +--rw (pattern)?
        |  +--:(drop)
        |  |  +--rw drop?                 empty
        |  +--:(spike)
        |  |  +--rw spike?                empty
        |  +--:(mean-shift)
        |  |  +--rw mean-shift?           empty
        |  +--:(seasonality-shift)
        |  |  +--rw seasonality-shift?    empty
        |  +--:(trend)
        |  |  +--rw trend?                empty
        |  +--:(other)
        |     +--rw other?                string
        +--rw annotator!
        |  +--rw name                 string
        |  +--rw (annotator-type)?
        |     +--:(human)
        |     |  +--rw human?         empty
        |     +--:(algorithm)
        |        +--rw algorithm?     empty
        +--rw symptom!
        |  +--rw id                 yang:uuid
        |  +--rw concern-score      score
        +--rw service!
           +--rw id    yang:uuid
```

Generated YANG models

Symptom Semantic Data Model

```
augment /rsn:relevant-state/rsn:anomalies/rsn:symptom:
  +--rw action?              string
  +--rw reason?              string
  +--rw cause?               string
  +--rw (plane)?
     +--:(forwarding)
     |  +--rw forwarding?    empty
     +--:(control)
     |  +--rw control?       empty
     +--:(management)
        +--rw management?    empty
```

Service Data Model

```
augment /rsn:relevant-state/rsn:anomalies/rsn:service:
  +--rw vpn-service-container
     +--rw vpn-service* [vpn-id]
        +--rw vpn-id       string
        +--rw vpn-name?    string
        +--rw site-ids*    string
```

```
augment /rsn:relevant-state/rsn:anomalies/rsn:service:
  +--rw vpn-node-termination-container
     +--rw vpn-node-termination* [hostname route-distinguisher]
        +--rw hostname                inet:host
        +--rw route-distinguisher     string
        +--rw peer-ip*                inet:ip-address
        +--rw next-hop*               inet:ip-address
        +--rw interface-id*           int32
```

https://datatracker.ietf.org/doc/draft-netana-nmop-network-anomaly-lifecycle/

https://datatracker.ietf.org/doc/draft-netana-nmop-network-anomaly-semantics/

Thanks to the Team

Vincenzo Riccobene (Huawei) – vincenzo.riccobene@huawei-partners.com
Thomas Graf (Swisscom) - thomas.graf@swisscom.com
Alex Huang Feng (INSA Lyon) - alex.huang-feng@insa-lyon.fr
Wanting Du (Swisscom) - wanting.du@swisscom.com
Benoit Claise (Huawei) – benoit.claise@huawei.com

Fancy more info about it?
→ NMOP WG on Tuesday @9.30am (drafts)
→ NMOP WG on Tuesday @6pm (hackathon)