Antagonist

(Anomaly Tagging on historical data)

IETF 119 - Hackathon

March 16-17th, 2024

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

Problem Statement

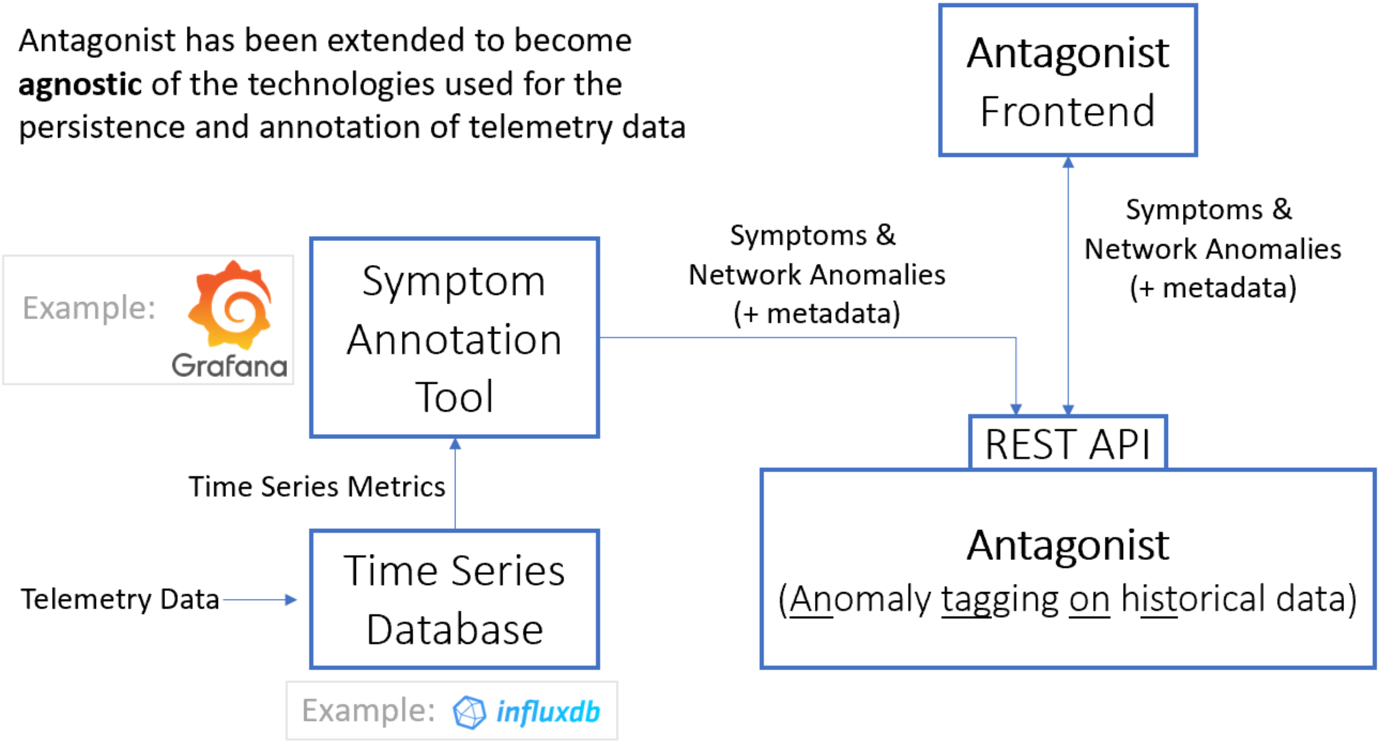
- Want to solve Automated **Network Anomaly Detection**?
  - How do you know if you are doing a good job?
  - How do you know how to iteratively improve?
  - How can you learn from this iterative process?
- One step towards the solution:
  - A YANG model to standardize the way anomalies are described
  - A YANG model to standardize knowledge of what went well and what not
- This enables a **structured and consistent exchange of anomaly related metadata**:
  - Between Network Operators, Academia, Vendors, etc.
  - Between Network Experts and AI Algorithms (Ground Truth, Validation)

Hackathon - Plan

- ✓ **Validate the new version of the YANG models** defined in the drafts, providing an implementation:
- ✓ Extend the **Proof-of-concept** to:
  - ✓ Expose an API based on the above YANG models
  - ✓ Make the project agnostic of the timeseries database used
- ✓ Enable Antagonist to supports **two use cases**:
  - ✓ A Network Operator tags symptoms and network issues (**ground truth**)
  - ✓ A Network Operator **validates** anomaly detection generated by AI algorithms

Hackathon – Software

Antagonist has been extended to become **agnostic** of the technologies used for the persistence and annotation of telemetry data

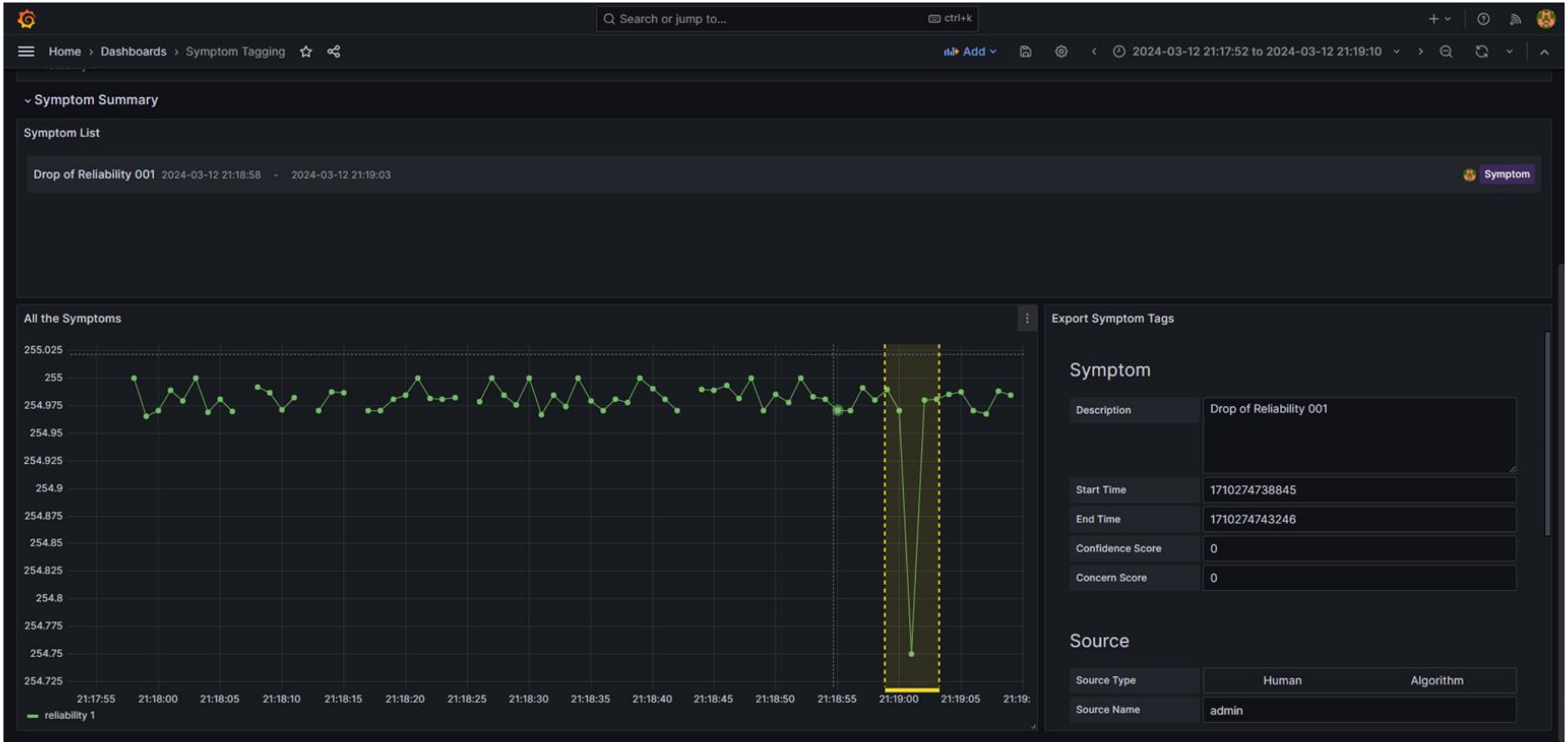


Antagonist exposes a REST API to support **ingestion** and **exposure** of symptoms and network anomaly data and semantic metadata.

The exposed data can be used as ground-truth.

Source Code: https://github.com/vriccobene/antagonist

Antagonist – Labelling a Symptom



Drop of Reliability 001 2024-03-12 21:18:58 - 2024-03-12 21:19:03

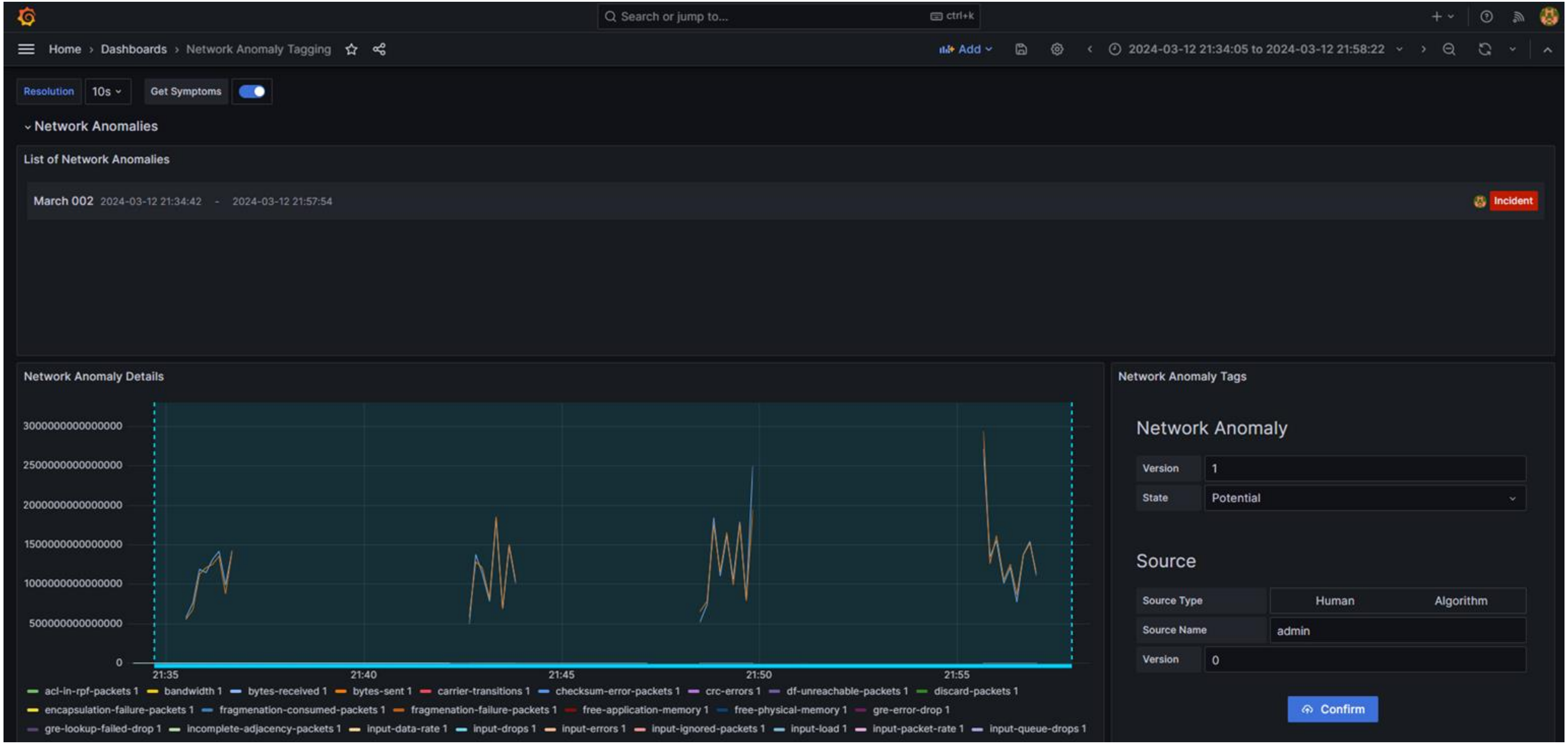
Symptom

Description	Drop of Reliability 001
Start Time	1710274738845
End Time	1710274743246
Confidence Score	0
Concern Score	0

Source

Source Type	Human	Algorithm
Source Name	admin	

Antagonist – Labelling incidents



March 002 2024-03-12 21:34:42 - 2024-03-12 21:57:54 Incident

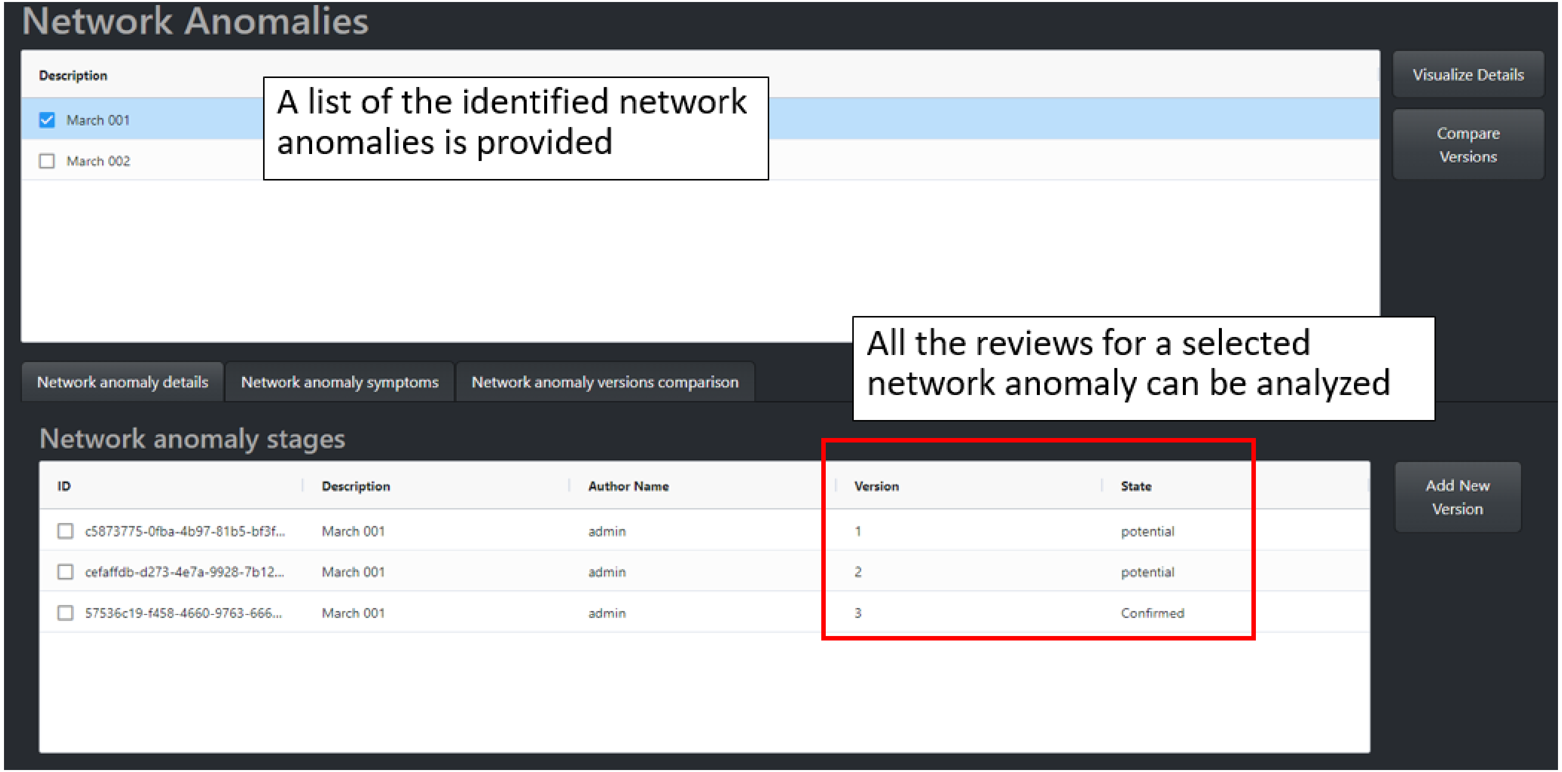
Network Anomaly

Version	1
State	Potential

Source

Source Type	Human	Algorithm
Source Name	admin	
Version	0	

Antagonist – Exposure of the Network Anomalies



Network Anomalies

Description
☑ March 001
□ March 002

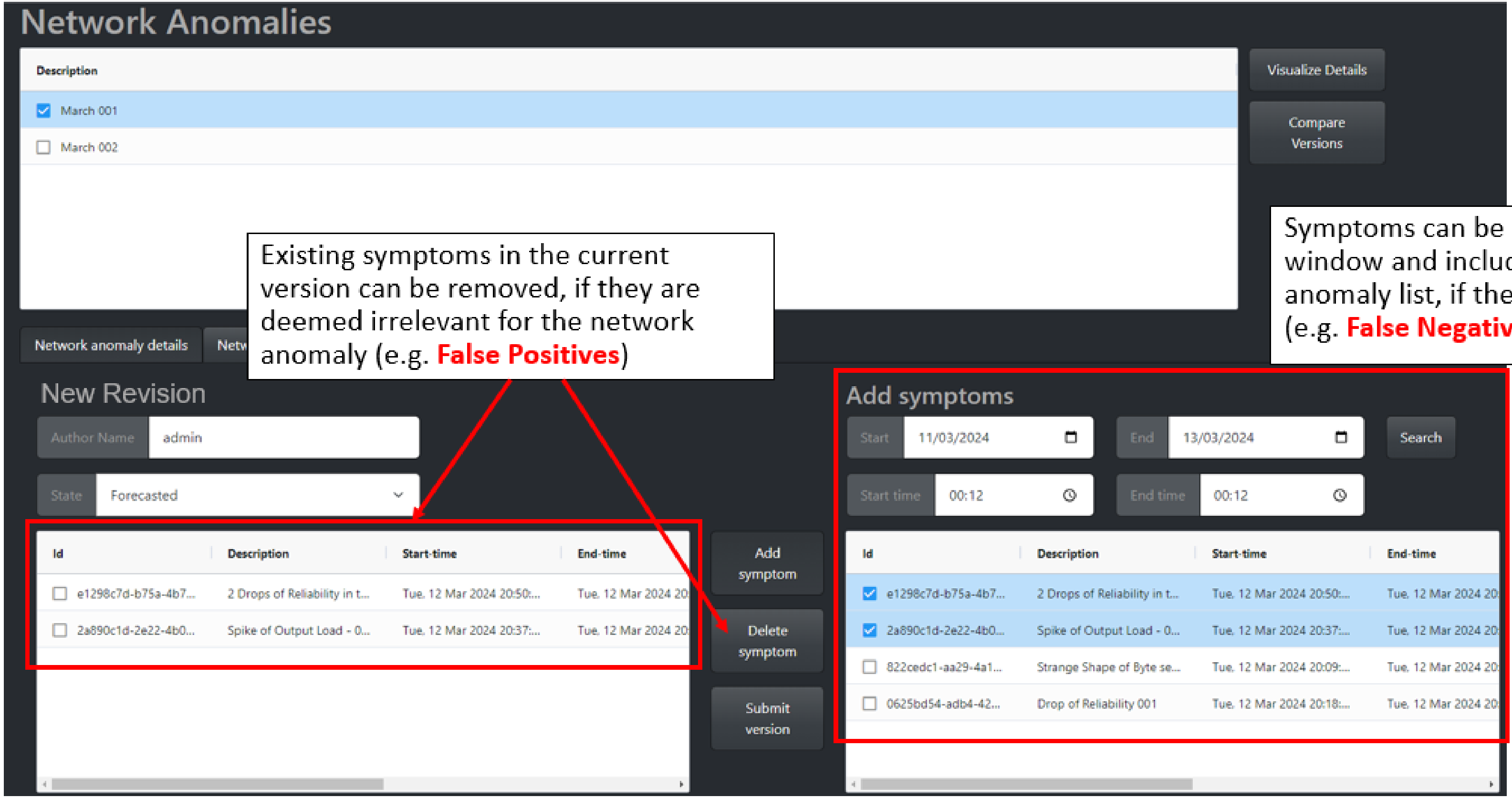
A list of the identified network anomalies is provided

All the reviews for a selected network anomaly can be analyzed

Network anomaly stages

ID	Description	Author Name	Version	State
□ c5873775-0fba-4b97-81b5-bf3f...	March 001	admin	1	potential
□ cefaffdb-d273-4e7a-9928-7b12...	March 001	admin	2	potential
□ 57536c19-f458-4660-9763-666...	March 001	admin	3	Confirmed

Antagonist – Exposure of the Network Anomalies



Network Anomalies

Description
☑ March 001
☐ March 002

New Revision

Author Name: admin

State: Forecasted

Id	Description	Start-time	End-time
☐ e1298c7d-b75a-4b7...	2 Drops of Reliability in t...	Tue, 12 Mar 2024 20:50:...	Tue, 12 Mar 2024 20
☐ 2a890c1d-2e22-4b0...	Spike of Output Load - 0...	Tue, 12 Mar 2024 20:37:...	Tue, 12 Mar 2024 20

Add symptoms

Start: 11/03/2024 End: 13/03/2024

Start time: 00:12 End time: 00:12

Id	Description	Start-time	End-time
☑ e1298c7d-b75a-4b7...	2 Drops of Reliability in t...	Tue, 12 Mar 2024 20:50:...	Tue, 12 Mar 2024 20
☑ 2a890c1d-2e22-4b0...	Spike of Output Load - 0...	Tue, 12 Mar 2024 20:37:...	Tue, 12 Mar 2024 20
☐ 822cedc1-aa29-4a1...	Strange Shape of Byte se...	Tue, 12 Mar 2024 20:09:...	Tue, 12 Mar 2024 20
☐ 0625bd54-adb4-42...	Drop of Reliability 001	Tue, 12 Mar 2024 20:18:...	Tue, 12 Mar 2024 20

Existing symptoms in the current version can be removed, if they are deemed irrelevant for the network anomaly (e.g. **False Positives**)

Symptoms can be retrieved by time window and included in the network anomaly list, if they were missed before (e.g. **False Negatives**)

The information collected by Antagonist can be used by network engineers to review the network anomaly history, or can be provided to AI algorithms as additional knowledge for training.

What’s next?

1. **Validate** the project with **network operational data from operators**
2. Finalize **validation of that the data models** are satisfactory and sufficient to reflect the necessary information

Thanks to…

- Vincenzo Riccobene – Huawei
- Antonio Roberto - Huawei
- Benoit Claise - Huawei
- Thomas Graf – Swisscom
- Wanting Du - Swisscom
- Alex Huang Feng – INSA Lyon