Semantic Metadata Annotation for Network Anomaly Detection

OPSAWG/NMRG WG

IETF 118

November 4-5th, 2023

Hackathon

draft-netana-opsawg-nmrg-network-anomaly-semantics

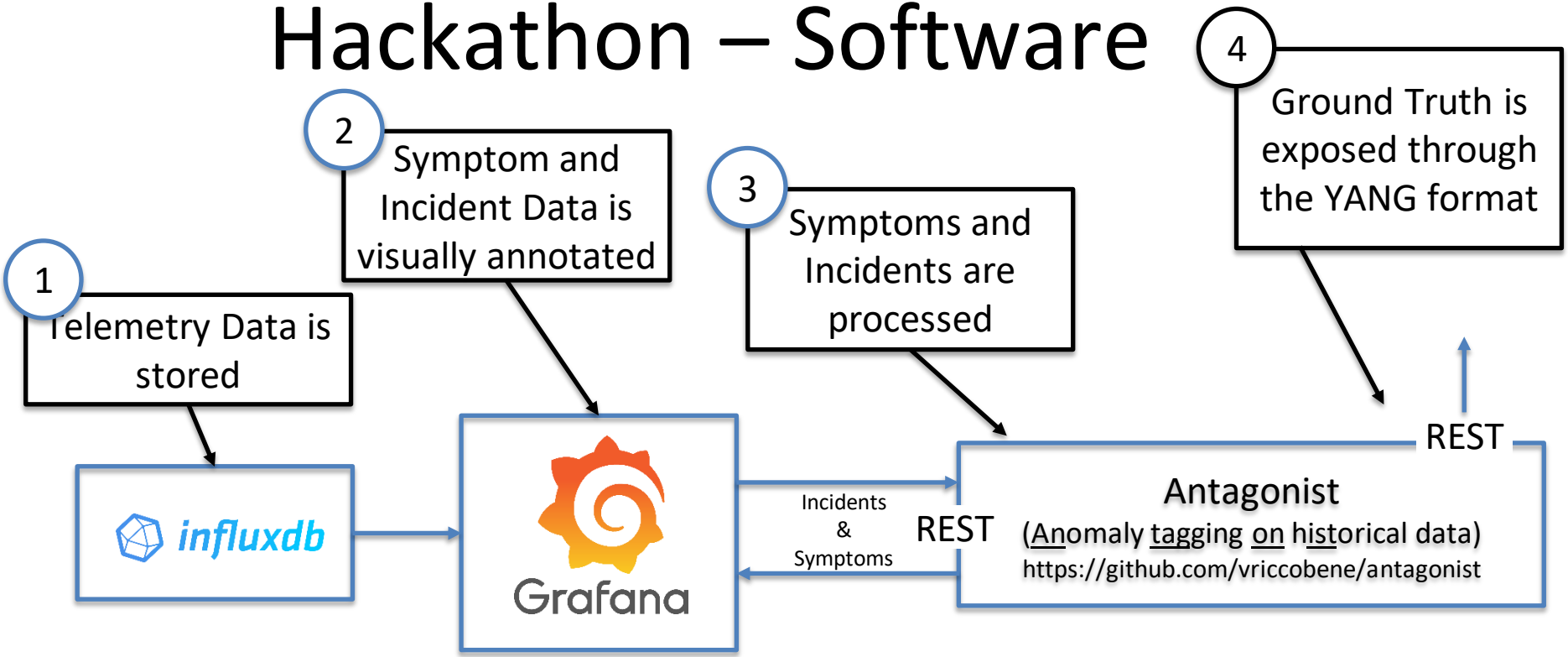
Problem Statement

- Want to solve the Automated Network Anomaly Detection?
  - How do you know if you are doing a good job?
  - How do you know how to improve?
- One step towards the solution:
  - A YANG model to standardize the way anomalies are described
- This can enables a structured and consistent exchange of data between:
  - Network engineers investigating anomalies
  - Human and Machines, for
    - Ground Truth
    - Validation

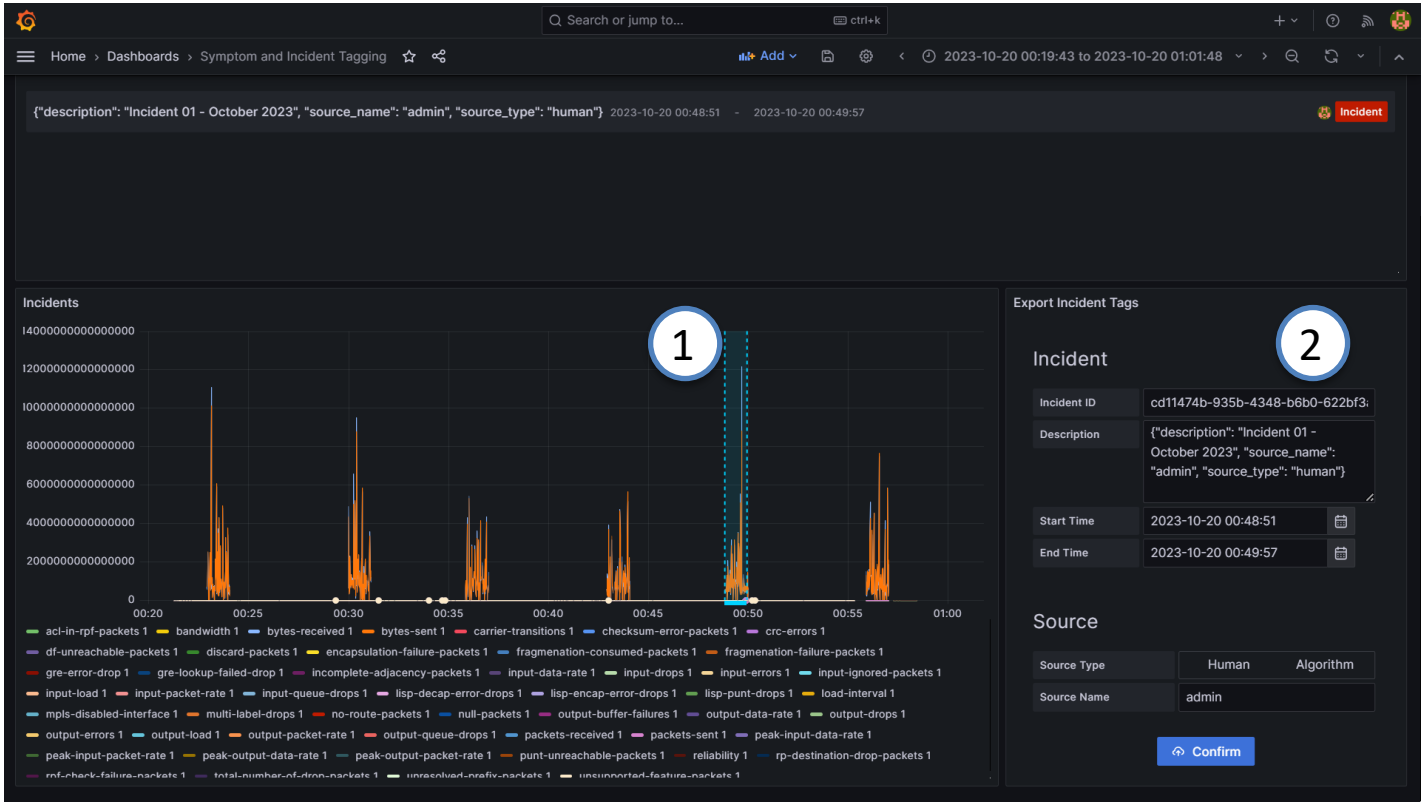
Hackathon - Plan

- ✓ Finalize metadata **semantics and ontology** (draft-netana-opsawg-nmrg-network-anomaly-semantics)
- ✓ Create **YANG models**
  - ✓ ietf-symptom-semantic-metadata.yang
  - ✓ ietf-incident-semantic-metadata.yang
- ✓ Implement a **Proof-of-concept** to support annotation of operational Network Telemetry (RFC 9232) data.
- ✓ Support the following **two use cases**:
  - ✓ Network operator annotates a network incident to generate **ground truth**
  - ✓ Network operator **validates (and corrects)** network incidents annotated by anomaly detection algorithms.

Hackathon – Software



Antagonist – Labelling incidents

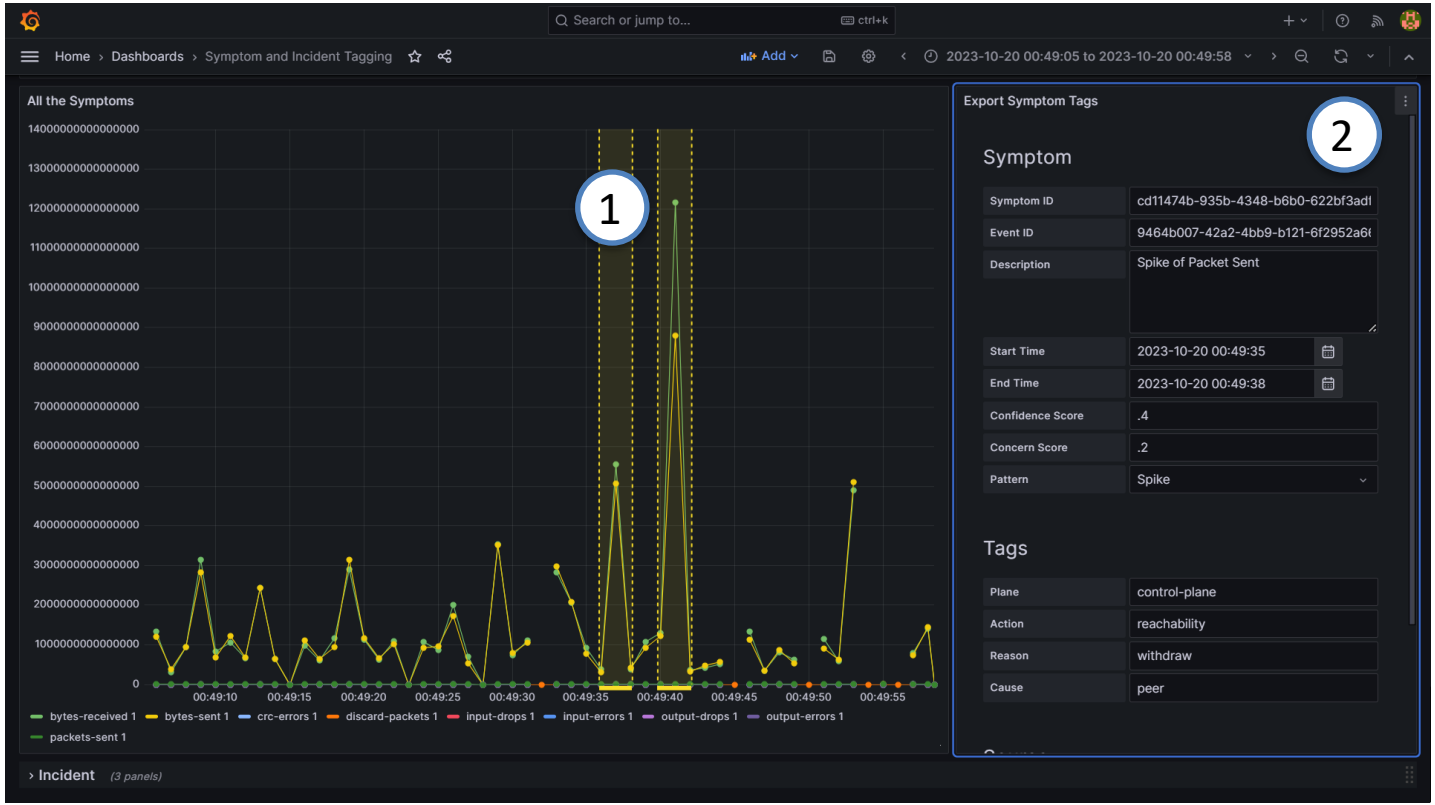


(1) Vertical dotted lines are the tagged incidents.

(2) Once the incident is selected, the user can add all the details.

Once the incident is defined it gets submitted to Antagonist.

Antagonist – Labelling a Symptom



(1) Vertical dotted lines are the tagged symptoms.

(2) Once the symptom is selected, the user can add all the details.

Once the symptom is defined it gets submitted to Antagonist.

What’s next?

1. Improve the project and the code
2. Integrate this framework with some real anomaly detection system to do:
   - Use the ground truth as label data
   - Upload detected anomalies on the system

Thanks to…

- Vincenzo Riccobene – Huawei
- Alex Huang-Feng – INSA Lyon
- Wanting Du – Swisscom
- Thomas Graf - Swisscom