Antagonist
(anomaly tagging on historical data)

https://github.com/vriccobene/antagonist

IETF 120 - Hackathon
July 20-21st, 2024
Vancouver

Why do we need Antagonist?

- Antagonist is a **Label Store** for Network Anomaly Detectors
- Network Anomaly Detection is the art of understanding when something is not working as expected in the network
  - It is an **iterative process** that requires **continuous improvement**
  - To improve the process it is necessary to enable cooperation between multiple teams, operators, providers and vendors need to interoperate.
  
  → **A standardized format for information exchange is key**

- Antagonist supports the following use cases:
  - **Exchange of anomaly detection labels** between different operators or teams
  - **Persistency** of anomaly detection labels generated by ML models
  - **Enable network engineers to easily validate** the result of the detection and provide feedback to the model (active learning)
  - **Provisioning of labels to ML** for dynamic retraining
Hackathon Plan

✓ Validation with real operational data (Cloud domain)
✓ Validation with a ML-based Network Anomaly Detector (Autoencoder)
✓ Validate support for Re-training of ML-based models
✓ Add partial support for Metadata Filtering and search
✓ Fix some deployment and integration bugs
The YANG model contains all the information that we need to automatically generate dashboards.
Next Steps

- Improve deployment and stability of the PoC
- Evaluate and Improve Scalability (kubernetes, etc.)
- Integrate and Validate with network operational data
Team

- Vincenzo Riccobene - vincenzo.riccobene@huawei-partners.com
- Reshad Rahman - rrahman@equinix.com
- Antonio Roberto - antonio.roberto@huawei.com
- Thomas Graf - thomas.graf@swisscom.com
- Benoit Claise - benoit.claise@huawei.com