# An Architecture for a Network Anomaly Detection Framework draft-netana-nmop-network-anomaly-architecture-00

Motivation and architecture of a Network Anomaly Detection Framework and the relationships to other documents describing network symptom semantics and network incident lifecycle

wanting.du@swisscom.com pierre.francois@insa-lyon.fr thomas.graf@swisscom.com vincenzo.riccobene@huawei-partners.com alex.huang-feng@insa-lyon.fr

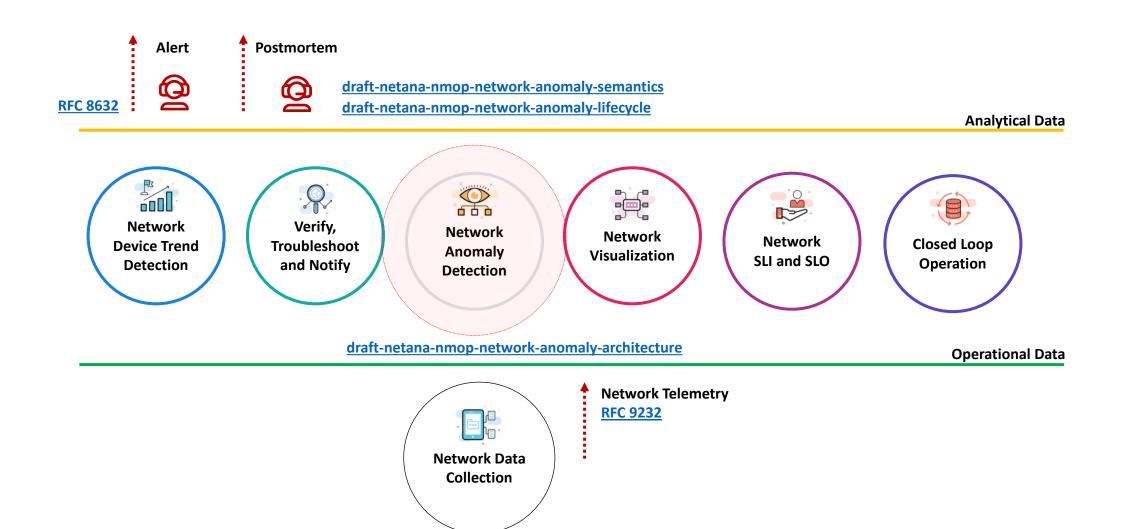
# Why This I-D?

## A Reminder

- ➤ This document describes motivation and a generic and extensible architecture of a Network Anomaly Detection Framework.
- Anchors draft-netana-nmop-networkanomaly-semantics and draft-netana-nmopnetwork-anomaly-lifecycle documents.
- Different applications will be described and exampled with open-source running code.

## Structuring Anomaly Detection NMOP Effort

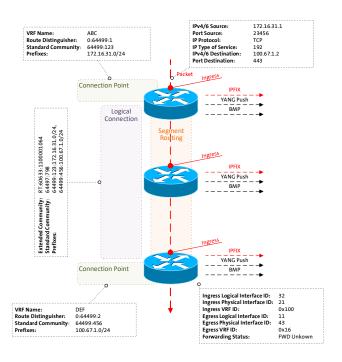
Integrates into Data Mesh



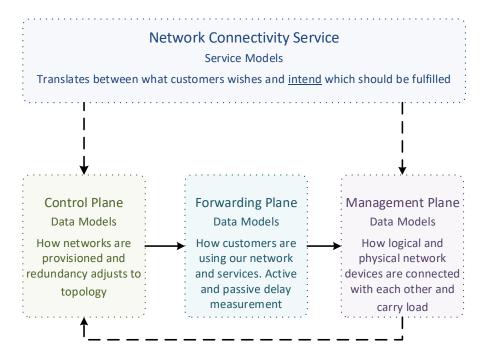
## What to monitor

Which metrics are collected

« Network operators connect customers in routing tables called Connectivity Services »



« Network Telemetry(RFC 9232) describes how to collect data from all 3 network planes efficiently »



## What does Network Anomaly Detection mean

Monitor changes, called outliers, in networks



# Network Anomaly Detection

For Connectivity Services, Network Anomaly Detection constantly monitors and detects any network or device topology change, along with their associated forwarding consequences for customers as outliers. Notifications are sent to the Network Operation Center before the customer is aware of service disruptions. It offers operational metrics for in-depth analysis, allowing to understand in which platform the problem originates and facilitates problem resolution.



#### **Answers**

What changed and when, on which connectivity service, and how does it impact the customers?



#### **Focuses**

Provides meaningful connectivity service impact information before customer is aware of and support in root-cause analysis.



#### **Data Mesh**

Consumes operational real-time Forwarding Plane, Control Plane and Management Plane metrics and produces analytical alerts.



#### **Direction**

From connectivity service to network platform.

## What our motivation is

Automate learn and improve

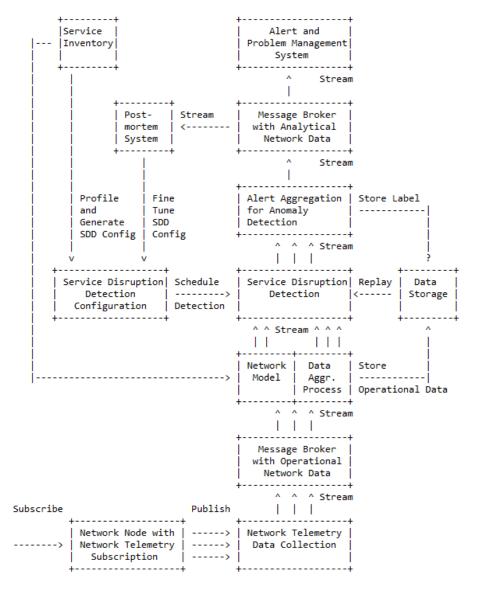
From network incidents postmortems we network operators learn and improve so does network anomaly detection and supervised and semi-supervised machine learning.

The more network incidents are observed, the more we can improve. With more incidents the **postmortem process needs be automated, let's get organized** first by defining human and machine-readable metadata semantics and annotate operational and analytical data.

Let's get further organized by exchanging standardized labeled network incident data among network operators, vendors and academia to collaborate on academic research.

« The community working on Network Anomaly Detection is probably the only group wishing for more network incidents »

## Elements of the Architecture

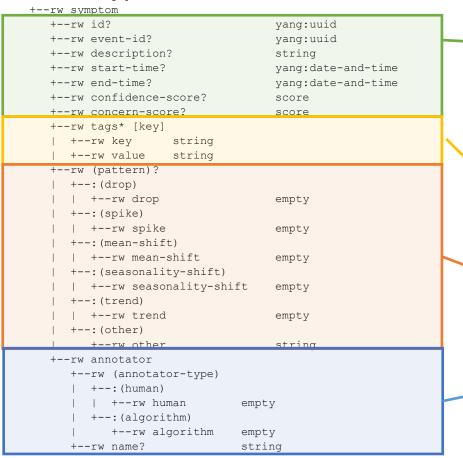


- Service Inventory contains list of the connectivity services.
- Service Disruption Detection processes aggregated network data to decide whether a service is degraded or not.
- Service Disruption Detection Configuration defines the set of approaches that need to be applied to perform SDD.
- Operational Data Collection manages network telemetry subscriptions and transforms data into message broker.
- Operational Data Aggregation produces data upon which detection of a service disruption can be performed.
- Network Modeling establishes knowledge of network relationships.
- Data Profiling categorizes nondeterministic customer related data.
- Detection Strategies for a profile a detection strategy is defined.
- Machine Learning is commonly used to detect outliers or anomalies.
- Storage some algorithms may relay on historical (aggregated) operational data to detect anomalies.
- Alerting consolidates analytical insights and notifies.
- Postmortem refines and stores the network anomaly and symptom labels into the Label Store.
- Replaying to validate refined anomaly and symptom labels, historical operational data is replayed.

## Semantic Metadata Annotation for Network Anomaly Detection

# draft-netana-nmop-network-anomaly-semantics

module: ietf-symptom-semantic-metadata



- Symptom ID and description uniquely identifies the detected anomaly. Event ID, start/end-time and confidence/concern-score uniquely identifies the network event with its start and end time, how confident the system identified the anomaly and how concerned an operator should be.
- Tags allows to add customer information.
- Pattern describes the identified pattern of the anomaly.
- Annotator Name, Type, describes wherever the anomaly was detected by a human or algorithm and uniquely identifies the system who/which detected.

## **Experiment:** Network Anomaly Lifecycle

draft-netana-nmop-network-anomaly-lifecycle

« Network Anomaly Detection is an iterative process that requires continuous improvement »

#### 4. Lifecycle of a Network Anomaly

The lifecycle of a network anomaly can be articulated in three phases, structured as a loop: Detection, Validation, Refinement.

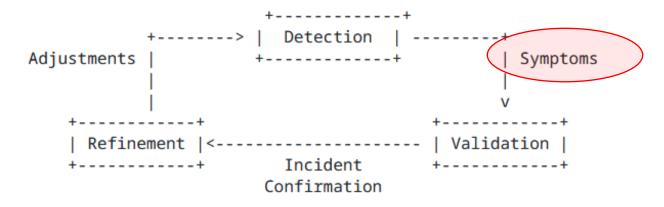


Figure 1: Anomaly Detection Refinement Lifecycle

Each of these phases can either be performed by a network expert or an algorithm or complementing each other. Detection: The Network Anomaly

Detection stage is about the continuous
monitoring of the network through
Network Telemetry [RFC9232] and the
identification of symptoms.

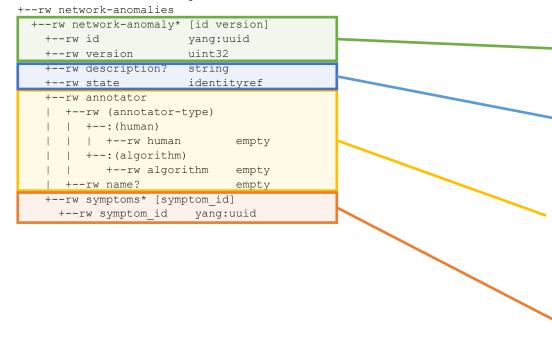
Validation: Decides if the detected symptoms are signaling a real incident or if they are to be treated as false positives.

Refinement: Network operator performs detailed postmortem analysis of the network incident, collected Network Telemetry data and detected anomaly with the objective to identify useful adjustments in the Network Telemetry data collection and Anomaly Detection system.

## **Experiment:** Network Anomaly Lifecycle

# draft-netana-nmop-network-anomaly-lifecycle

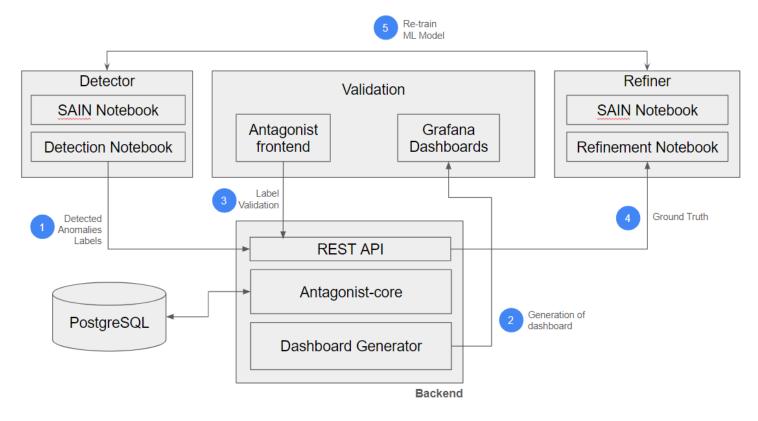
module: ietf-network-anomaly-metadata



- ID and Description uniquely identifies the detected network anomaly (as a container of symptoms).
- Description and State provide general information regarding the anomaly and .
- Annotator describes the entity that observed the network anomaly: this can be a human or an algorithm (anomaly detection system).
- Symptoms provides a list of symptoms (based on ietf-symptom-metadata) that are part of this network anomaly.

## **Experiment:** Antagonist

anomaly tagging on historical data



### **Next Steps:**

- > Improve scalability
- Validate with Swisscom Data

#### **Goals:**

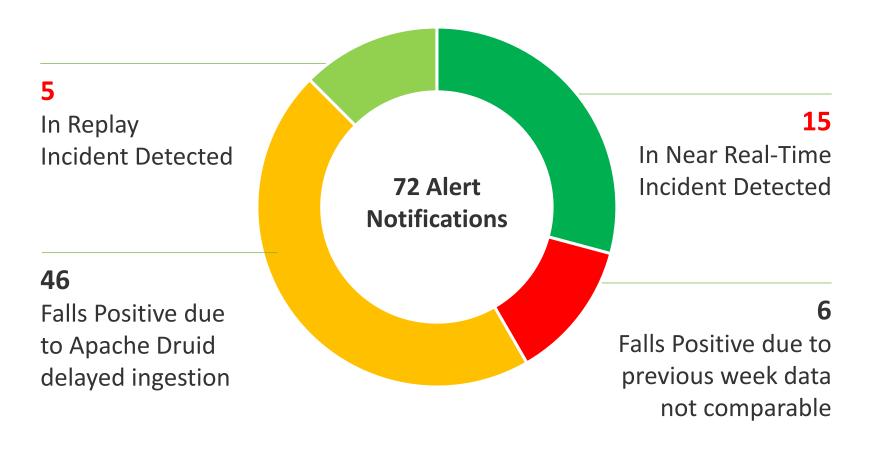
- Prove that YANG models contain all the necessary information
- Validate models across a wide range of use-cases
- Show interoperability between

#### Done so far:

- ✓ Validation with real operational data (Cloud monitoring)
- ✓ Validation with rule-based Network Anomaly Detector (SAIN RFC9417/RFC9418)
- ✓ Validation with a ML-based Network Anomaly Detector (Autoencoder)
- ✓ Add support for Re-training of MLbased models
- ✓ Add partial support for Metadata Filtering and search
- ✓ YANG model refinements to reflect the results of the coding
- ✓ Automatic dashboard generation

## **Swisscom** - Cosmos Bright Lights PoC Summary

After 20 Incidents and 18 Months Time

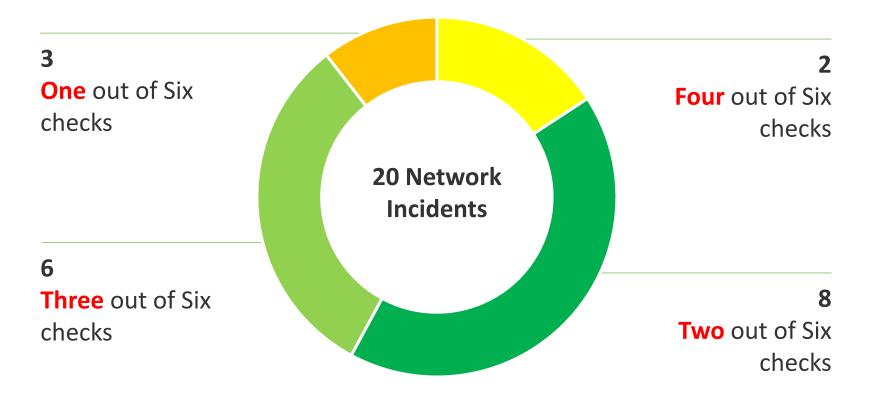


## Key Facts in V0 (2023-2024)

- ➤ 16 L3 VPNs proactively monitored.
- ➤ Individual Service Disruption Detection rule accuracy is beyond 90%. Summed accuracy is beyond 95%.
- Max Concern score ranged between 0.06 and 0.85. In average 0.46.
- In 4 cases additional YANG, in 13 cases additional BMP, in 2 cases Netconf Transaction-ID and 1 case additional L2 IPFIX metrics would have helped to gain more visibility.
- Key observability feature missing: BMP Local RIB with Path Marking.

## Swisscom – PoC Detail and Outlook

Multiple Perspectives increases Accuracy



## **Key Improvements in V1 (2024)**

- > >12000 L3 VPNs proactively monitored since June 2024.
- Realtime Streaming eliminates delayed ingestion falls positives and scaling.
- Improved profiling. Compares to multiple previous weeks and discard largest deviation eliminates falls positives.
  - -> Work In progress

## **Key Improvements in V2 (2025)**

- Annotate operational and analytical Network Incident data for reproduction.
- Enabling automated workflow. From PowerPoint slide decks to data driven actionable insights.

## An Architecture for a Network Anomaly Detection Framework

Status, Summary and Next steps

#### Status of draft-netana-nmop-network-anomaly-architecture

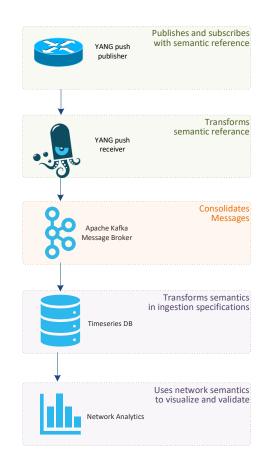
Reference document to anchor anomaly detection work items.

# Status of draft-netana-nmop-network-anomaly-semantics and draft-netana-nmop-network-anomaly-lifecycle

- Referenced draft-netana-nmop-network-anomaly-architecture as the architecture document.
- Change the term source to annotator and updated the YANG modules accordingly.
- Added/updated terminology section with references to <u>draft-ietf-nmop-terminology</u> and <u>draft-netana-nmop-network-anomaly-architecture</u>.
- Moved data mesh and outlier detection section to <u>draft-netana-nmop-network-anomaly-architecture</u>.

#### **Next Steps**

- ➤ Request adoption for all 3 anomaly detection documents starting with draft-netana-nmop-network-anomaly-architecture.
- ➤ NMOP interim meeting on September 11<sup>th</sup> proposal
  - ➤ Network incident postmortem examples from Swisscom and Bell Canada
  - > Detailing documents, updates and hackathon experiment results
  - > Invite other operators to contribute on experiments



## Relevant Papers for more Details

#### Practical Anomaly Detection in Internet Services: An ISP centric approach

Alex Huang Feng\*, Pierre Francois\*, Kensuke Fukuda<sup>‡</sup>, Wanting Du<sup>‡</sup>, Thomas Graf<sup>†</sup>, Paolo Lucente<sup>§</sup>, Stéphane Frénot\*

\*INSA Lvon, Inria, CITI, UR3720, Villeurbanne, France alex.huang-feng@insa-lyon.fr, pierre.francois@insa-lyon.fr, stephane.frenot@insa-lyon.fr <sup>‡</sup>National Institute of Informatics, Tokyo, Japan kensuke@nii.ac.jp †Swisscom, Zurich, Switzerlar wanting.du@swisscom.com, thomas.graf@swisscom.com §pmacct.net, Barcelona, Spain paolo@pmacct.net

SPs. Therefore, monitoring and anomaly detection has become essential for SPs. In this paper, we present an one-gion greater an one-gion greater and project aimed at identifying anomalies in Internet services provided by an ISS. We aim at detecting anomalies within the domain managed by the ISP that impact the customers and the domain managed by the ISP that impact the customers and elected issues.

Anomaly detection (AD) has been and topic in the instance of the control of the con

#### I. INTRODUCTION

ity for customer Autonomous Systems (ASes) connected to an Simulated environments mimicking the deployed network depend on the ISP peerings to reach the Internet and an production data [7]-[9]. incident between them and the Internet can have detrimental In this paper, we focus on detecting anomalies within a implications for their business.

Adviser—I-leastlying assemilie in a network is a crutial colorer for latenties Service Proteiner (SPN). Assemilier (SPN), a broad that impact the traffic of the ISP contoners can lead integrated that interpretation of the company. Moreover, ident anomalised in the reputation of the company. Moreover, ident anomalised in the reputation of the company. Moreover, ident anomalised in the reputation of the company. Moreover, ident anomalised in the control of the company of the company

inear reat time, giving innormation that allows the operator to regularities in the cash. Most research projects saming at describe the collected network telemetry metrics and illustrate how they are processed using open-source solutions. We introve solutions, but introve as set of use cases showing that an ISP can monitor Internet services using IEF standard metrics. researchers have been able to develop methods to detect anomalies in data from the public domain, with a focus on Internet services include providing global Internet reachabildetecting anomalies in the global Internet topology [4, 5].

Internet Service Provider (ISP) and serving private customers and manually generated anomalies have also been used to within the ISP (e.g. FTTH). Disruptions in the network that test anomaly detection [6]. Very few projects use production affect the connectivity of an ISP not only significantly degrade data coming from an ISP to detect anomalies and root cause the organization's reputation but also have implications on the analysis within a single domain. AD within an AS have only company's revenue. Customers subscribed to Internet services been investigated by very few researchers having access to

mplications for their business.

Today, routing between different ASes is established using and find unwanted traffic flows impacting their business. We BGP [1]. ISPs managing an AS configure policies in their describe the target use cases in Section II. Instead of solely routers based on the business relationship they have with using BGP activity as a source of data, as done in [7], we their neighboring ASes. Generally, ISPs classify their BGP use a larger set of monitoring information, allowing us to neighbors into Customers, Settlement-free Peers and Tran-sit Providers. Customer ASes compensate the ISP to reach authors in [8] focus on detecting performance issues from the Internet, Settlement-free peers are mutual arrangements end-to-end users, while the work presented in this paper also between two ISPs to exchange Internet traffic without any covers anomalies impacting the traffic from peerings. In [9] financial compensation and Transit Providers provide access anomaly detection is based on traffic information with a focu on network intrusion detection, while the project presented

#### **Daisy: Practical Anomaly Detection in large** BGP/MPLS and BGP/SRv6 VPN Networks

Alex Huang Feng alex.huang-feng@insa-lyon.fr Univ Lyon, INSA Lyon, Inria, CITI, EA3720 Villeurbanne, France

Thomas Graf thomas.graf@swisscom.com Swisscom Zurich, Switzerland

Pierre Francois pierre.francois@insa-lvon.fr Univ Lyon, INSA Lyon, Inria, CITI, EA3720

Wanting Du wanting.du@swisscom.com Zurich, Switzerland

Stéphane Frenot stephane.frenot@insa-lyon.fr Univ Lyon, INSA Lyon, Inria, CITI, EA3720

> Paolo Lucente paolo@pmacct.net Barcelona, Spain

We present an architecture aimed at performing Anomaly Detection for BGP/MPLS VPN services, at scale. We describe in modern, large BGP/MPLS VPN and BGP/IPv6 Segment Routing VPN deployments. We describe an architecture required to collect the necessary routing information at scale. We discuss the various dimensions which can be used to detect anomalies, and the caveats of the real world impacting the level of difficulty of such anomaly detection and network modeling. We argue that a rule-based anomaly detection approach, defined for each customer type, is best suited given the current state of the art. Finally, we review the current IETF contributions which are required to benefit from a fully open, standard, architecture.

#### ACM Reference Format:

Alex Huang Feng, Pierre Francois, Stéphane Frenot, Thomas Graf, Wanting Du. and Paolo Lucente. 2023. Daisy: Practical Anomaly tion in large BGP/MPLS and BGP/SRv6 VPN Networks. Ir Applied Networking Research Workshop (ANRW '23), July 24, 2023. San Francisco, CA, USA. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3606464.3606470

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers of and counts permissions. To Copy or makings, or appointing, to post on servers to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions⊕acm.org.

ANRW '23, July 24, 2023, San Francisco, CA, USA

© 2023 Copyright held by the owner/author(s). Publication rights licensed to

ACM ISBN 979-8-4007-0274-7/23/07...\$15.00 https://doi.org/10.1145/3606464.3606470

Customers subscribing to BGP/MPLS VPN services usually come along with stringent Service Level Agreements. Conanomalies in their services in a timely fashion, while accommodating for scale. Around 10 thousand L3 VPNs in our Swisscom use case. Long-lasting outages, detected by the customer before the service provider, are detrimental to the perception of service quality, and may dramatically impact

The goal of the presented architecture is to provide an anomaly detection solution that scales while being flexible on the following aspects: (i) the dimensions that must be used to detect anomalies are multiple; (ii) VPN customers wear different profiles in terms of normal and abnormal values for such dimensions; (iii) the amount of information collected to produce values for such dimensions is extremely large in such deployments: around 175 thousand messages/second in our use case; (iv) the operating costs for managing an anomaly detection solution must be kept low; and (v) the networking platforms providing the service may come from different vendors and have different monitoring canabilities

The remainder paper is structured as follows. In section 2, we define what is considered a network anomaly and preser the associated challenges behind its detection. In Section 3. we describe the Daisy architecture. In Section 4, we review the ongoing IETF efforts aimed at filling the gaps for a fully open, standard, Anomaly Detection (AD) implementation And finally, in section 5, we present the first results of Daisy

We describe some of the challenges associated with customer diversity, and a non-exhaustive list of anomalies targeted by the base recipes from our limited proof of concept deployment

### Paper "Practical Anomaly Detection in Internet Services: An ISP centric approach"

Published at AnNet Workshop (In conjunction with IEEE NOMS) Seoul, South Korea (6–10 May 2024) DOI: 10.1109/NOMS59830.2024.10575071

Paper "Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks" published

at ACM/IRTF ANRW'23

San Francisco, USA (24 July 2023)

Open access: http://hal.science/hal-04307611