

Anomaly Alerting for RIPE Atlas



Presentation Agenda

- Project Context
- The Solution
- Anomaly Detection
- Prototype

Project Context

About us

- Second year students
- Software engineers



Project Context

Main question from RIPE:

How to provide more value to Anchor hosts?

Our choice:

Monitoring software.

Problem Statement

- Hard to monitor neighboring AS networks
- The current solutions are complicated (status-check api)

The Solution

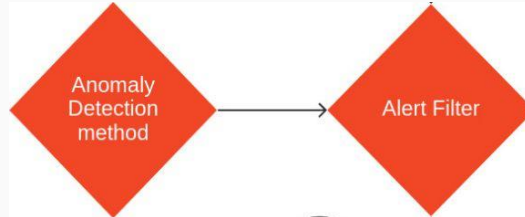
Solution

Our answer:

- *A monitoring system*
- *RIPE Atlas data*
- *Easy to set up*
- *Customizable*

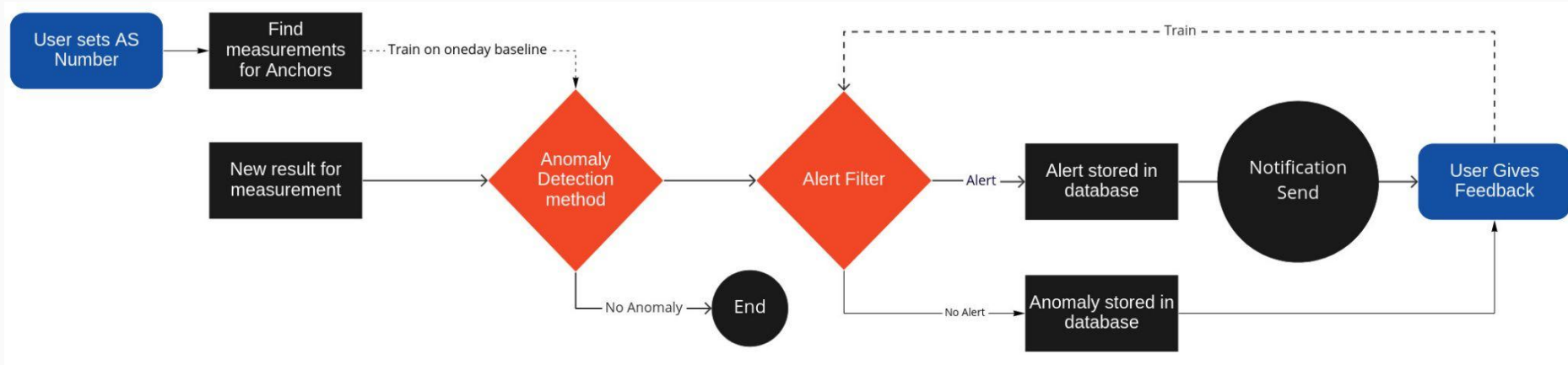
The Solution

Plugable Detection Methods



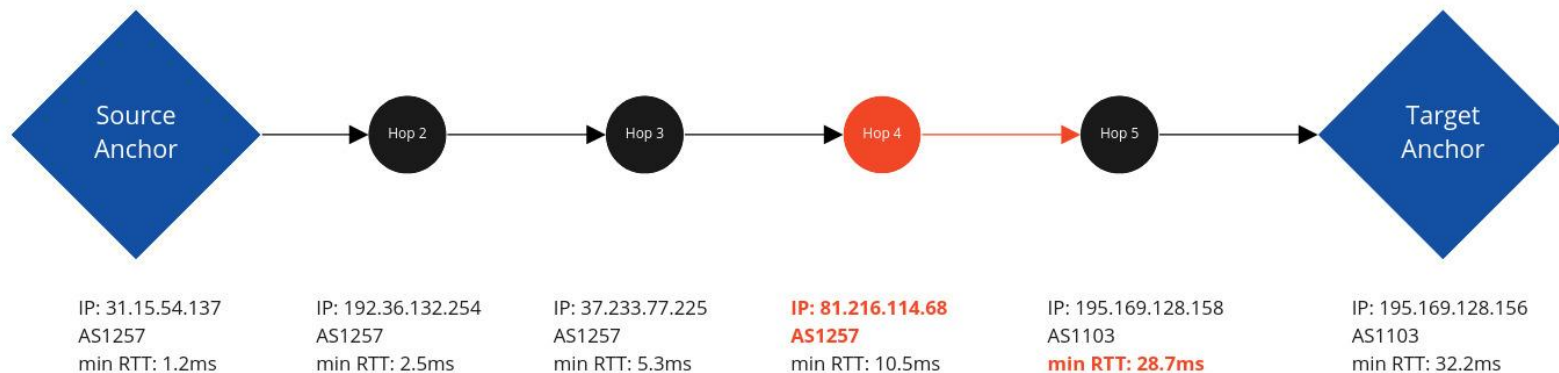
Filter Alerts based on Feedback

Project Diagram

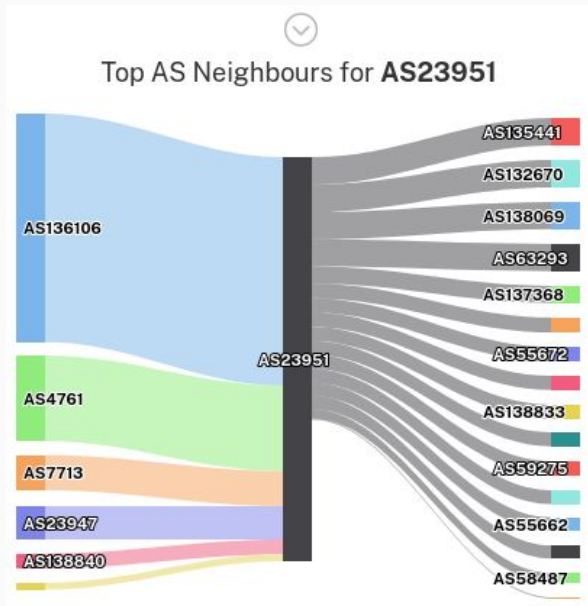


Anomaly Detection

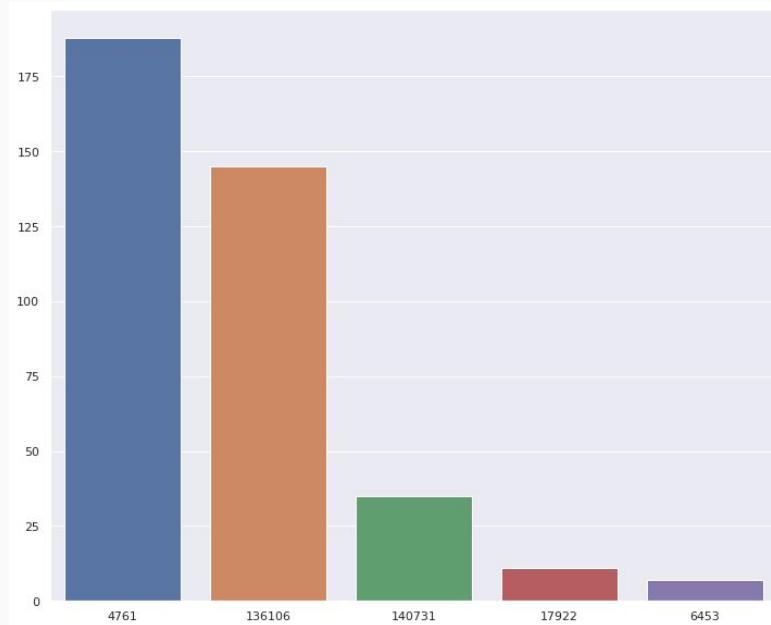
Current Method: Entry Point Delay



Example on AS23951 Neighbors check

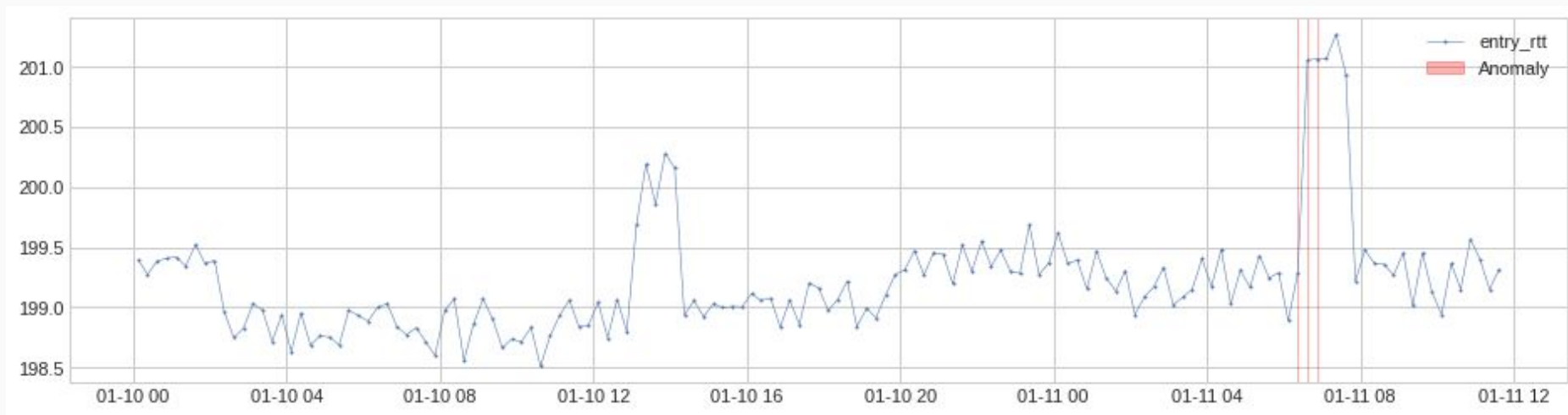


Ripe Stat result for neighbours

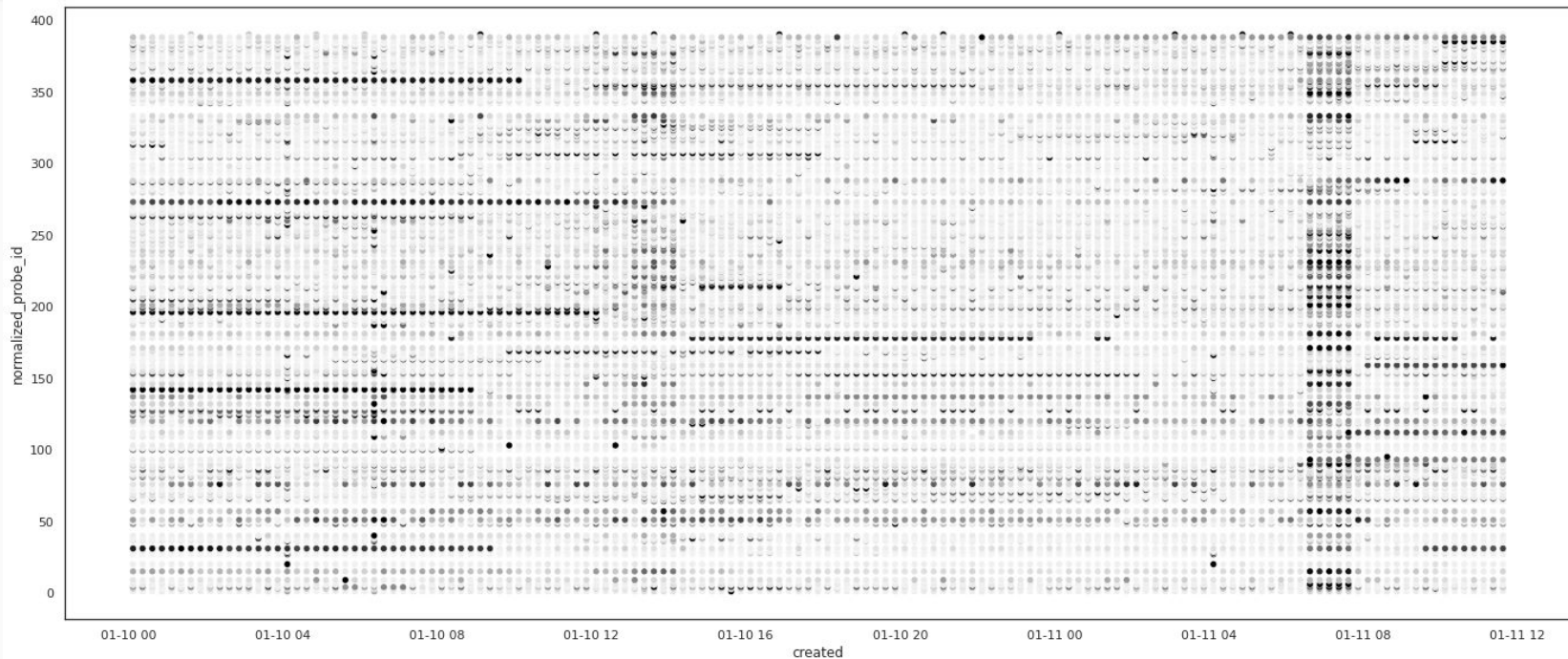


Amount of probes that found certain neighbor with current detector

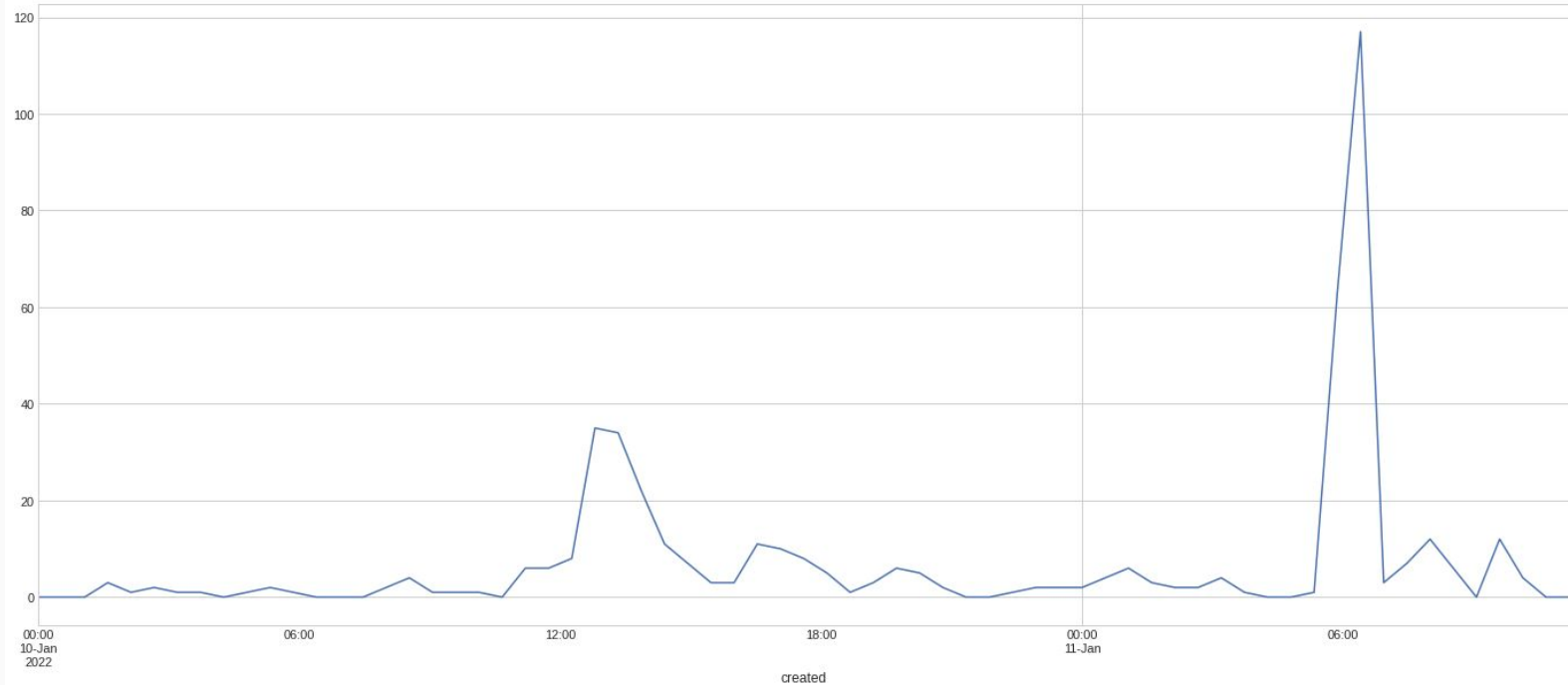
Anomaly detection in RTT per probe on entry hop



Multivariate plot of minimum RTT



Aggregated anomalies in single AS



Other Detector Ideas






Traceroute based:

- Route Change in neighboring connection
- Delay in entire neighboring network (maybe averaging?)

Ping based

- Anchor delay per country (or as)
- Anchor Down

Prototype

-  Dashboard
-  Alerts Feedback
-  [Settings](#)
-  Feedback
-  Documentation

Adjust Monitoring settings

AS Numbers



Set the AS number that you want to monitor.

AS 1103

The monitoring process is running. AS belongs to: SURFNET-NL - SURF B.V..

SAVE

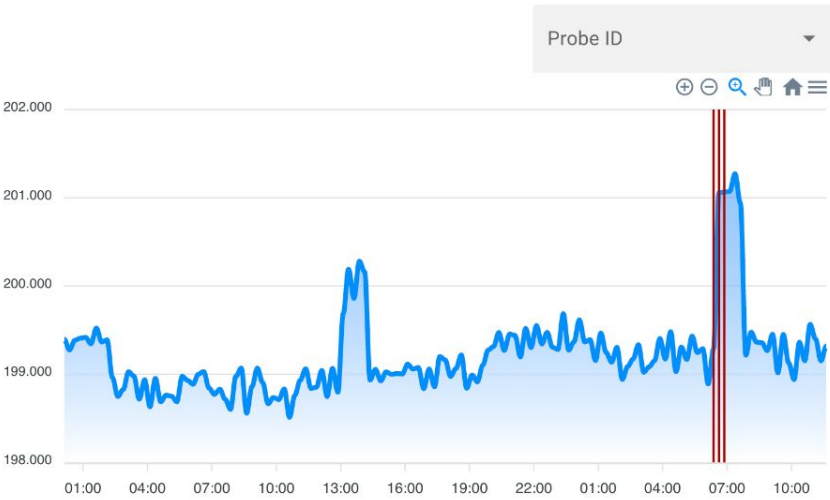
- Dashboard
- Alerts Feedback
- Settings
- Feedback
- Documentation

Recent Alerts

Timestamp	Alert Description
2022-05-10 10:37	Ping above 100ms for 5 minutes now.
2022-05-17 12:19	RTT increased to 420ms
2022-05-17 12:19	119 probes had a route change around ASN1103
2022-05-10 10:42	Connection to anchor has been lost.


1-4 of 4

Probes Anomaly Graph



Anomaly Overview and Feedback



Timestamp	Detection Method	IP Addresses	AS Number	Anomaly Score	Value Increase	Alert Description	Prediction	Feedback
2022-05-10 10:37	Traceroute	195.169.128.156	1103	75	10	Ping above 100ms for 5 minutes now.	Alert	 
2022-05-17 12:19	Entrypoint RTT	195.169.122.151	1103	50	3.2	RTT increased to 420ms	No Alert	 
2022-05-17 12:19	Route Change	195.169.122.151	1103	80	10.1	119 probes had a route change around ASN1103	No Alert	 
2022-05-10 10:42	Ping	195.169.128.156	1103	33	0	Connection to anchor has been lost.	No Alert	 

- Dashboard
- Anomaly Overview
- Network Topology

- Documentation
- Settings

Alerts Anomalies All

Timestamp	AS	Change Value
2 hours ago	AS13079	160 ms RTT increase
Fri 2 feb 01:12	AS13079	119 probes changed

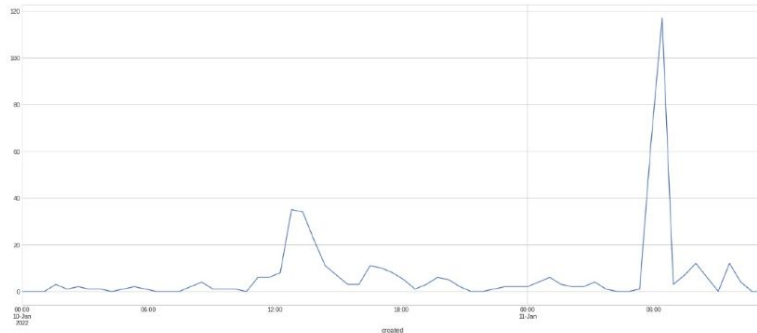


Entry Point RTT

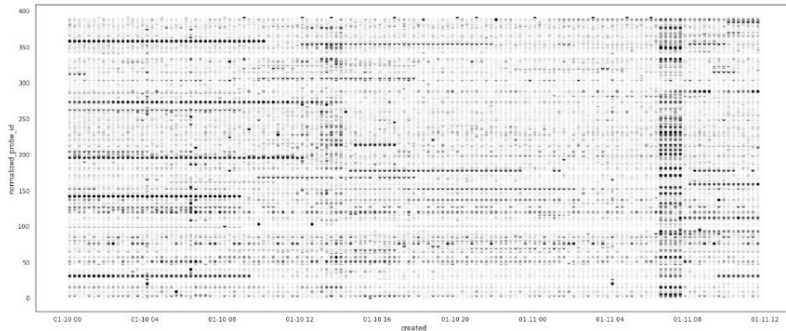
Feedback:

Wed 9 feb 06:12 2022
Round trip time increased to

AS Total Score

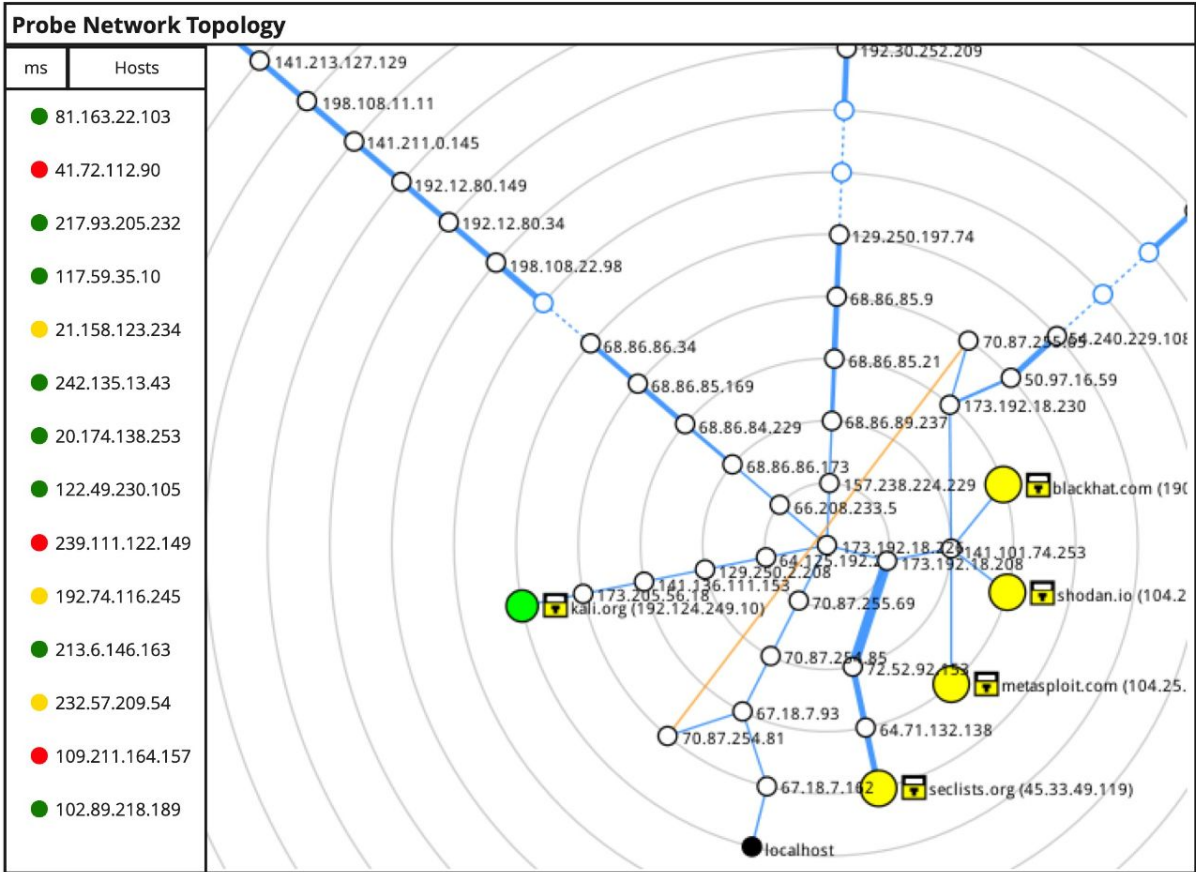


Overview AS



- Dashboard
- Anomaly Overview
- Network Topology

Network Topology



- Documentation
- Settings

Come meet us for a demo!

Github pre-release!

Work in progress of the monitoring tool.

<https://github.com/Wolframfriele/ripe-alerts>

Thank You!

Questions?

