

SHMIT

Chasing network events

MANRS RPKI Week, 5th July 2022

Massimiliano Stucchi
stucchi@isoc.org



Looking for hints

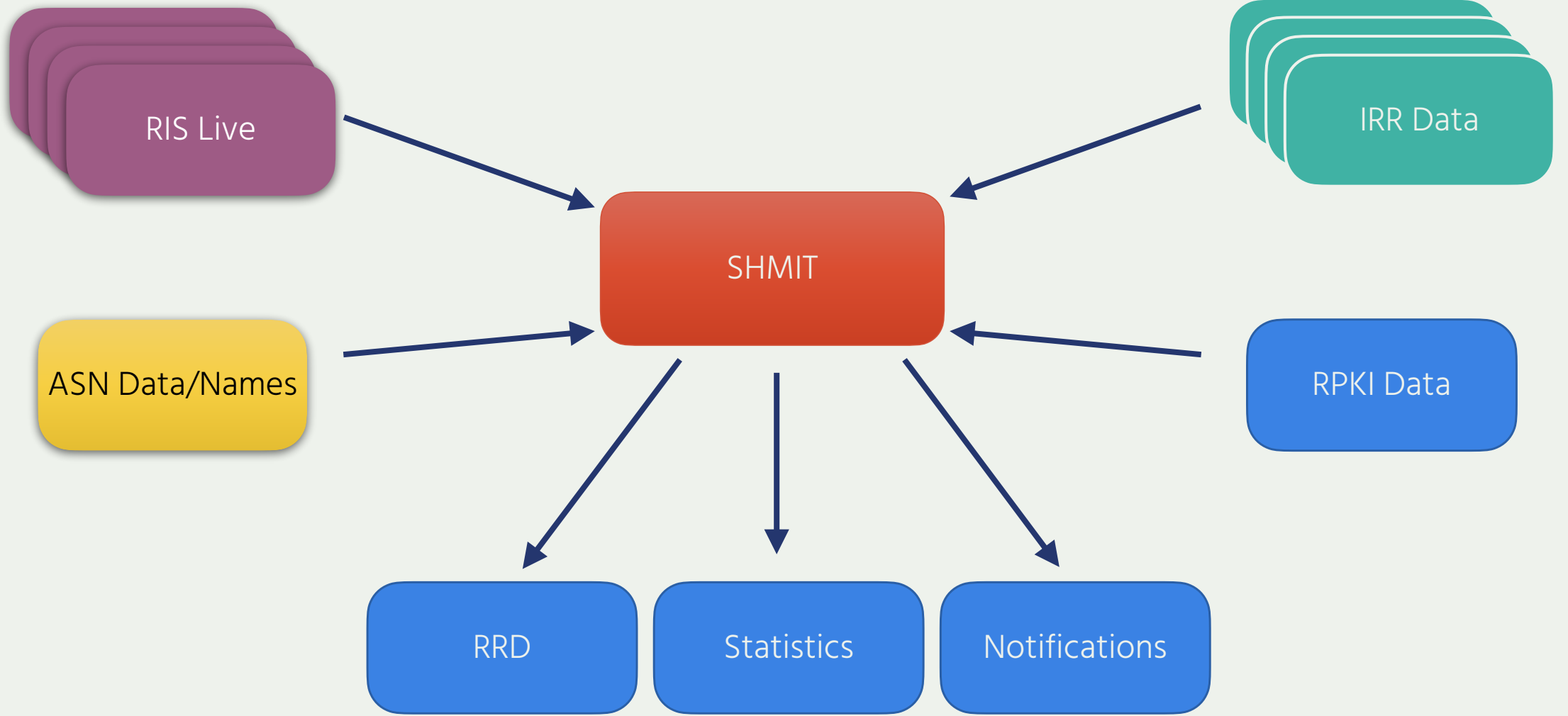
- At ISOC, we need a tool to “chase” shutdowns
- And one to have better insights into hijacks
- After checking for available products, we decided to try coming up with something on our own



Shutdown and Hijacks Monitoring and Identification Tool (SHMIT)

- Based on the same concept as BGPAlerter
 - It looks into ASN in the path, rather than only origin
- Built using python instead of javascript
 - Leveraging asyncio





Data produced

- Number of updates per ASN and per country
 - With Valid/Invalid/Unknown RPKI Status
 - With Valid/Invalid IRR Status
- Number of updates where ASN is in the path
 - With Valid/Invalid/Unknown RPKI Status
 - With Valid/Invalid IRR Status
- And more



“Plugin system”

- We can easily add data sources and data analysis
- For shutdowns we are planning on using some platform for anomaly detection
 - Feeding data from SHMIT
- Fine tuning is required for detection, an ongoing work



Requirements

- 2 cores
- 16 gigabytes of RAM
 - IRR Data raises the bar
- Decent network connectivity



The future

- Fine tuning our data collection
- Additional sources
- Opening access to the code repo on GitHub



Questions ?

stucchi@isoc.org

[@stucchimax](#)

<https://t.me/stucchimax>

