User Aided
Malicious Domain Detection

10th CENTR R&D Workshop | 2017-05-29
Frankfurt am Main

Moritz Müller

FRAUDE HELPDESK.nl SIDN LABS

About FHD and SIDN

FRAUDEHELPDESK.nl

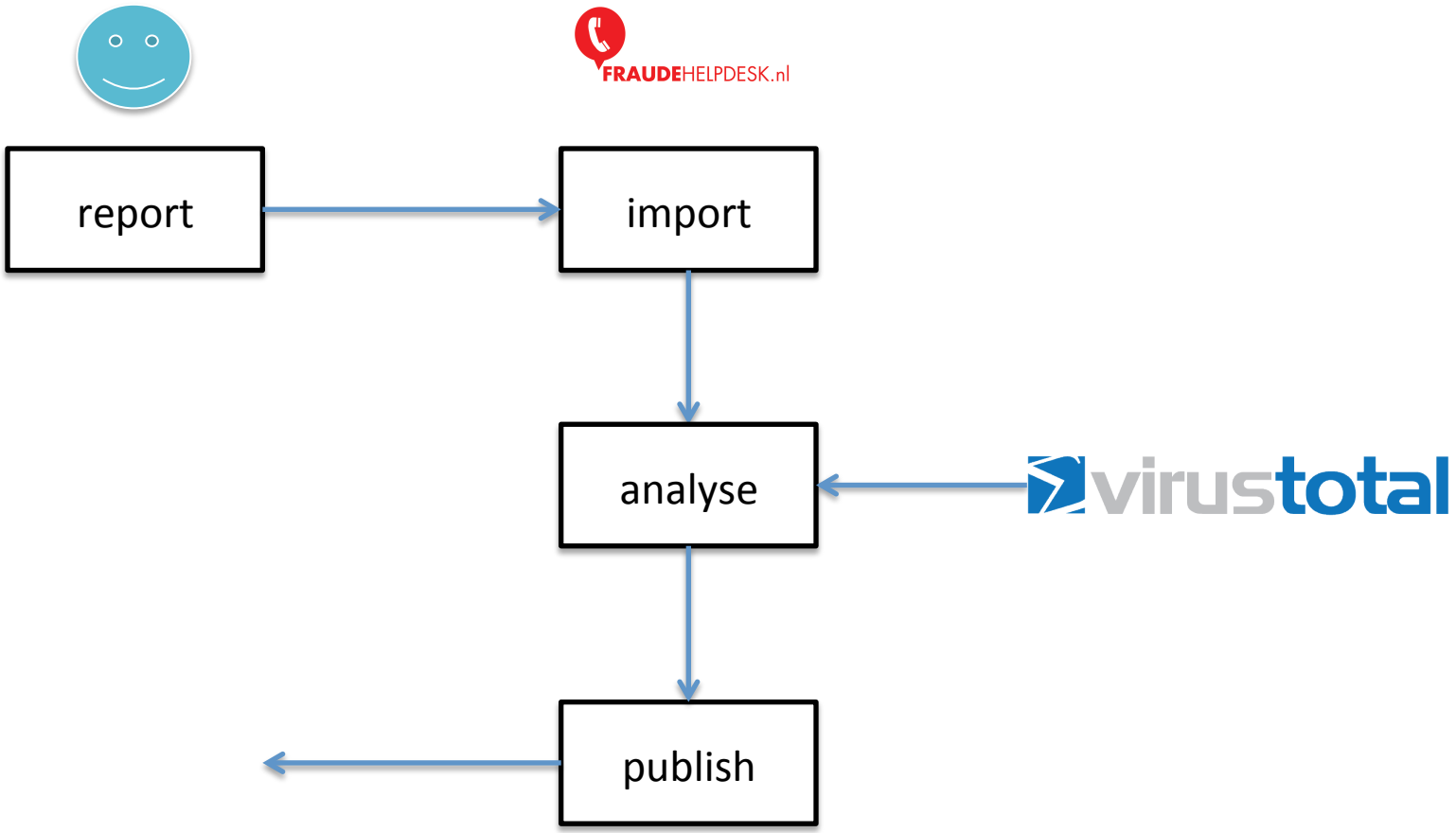
SIDN LABS

Goal of JTIE

- Joint Threat Intelligence Enrichment

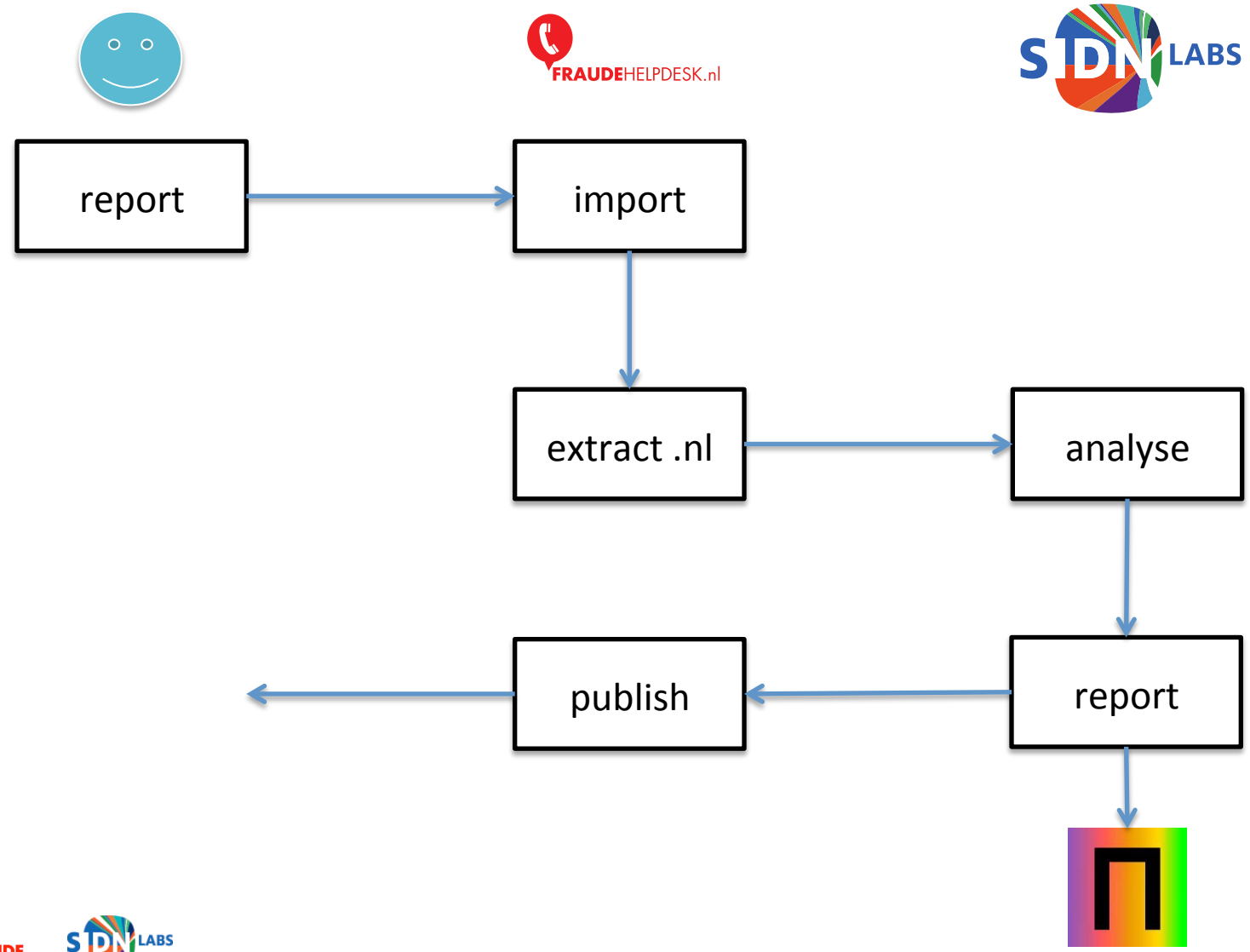
- We want to classify mails faster in order to warn and protect more users from phishing and fraud

Fraudehelpdesk Workflow

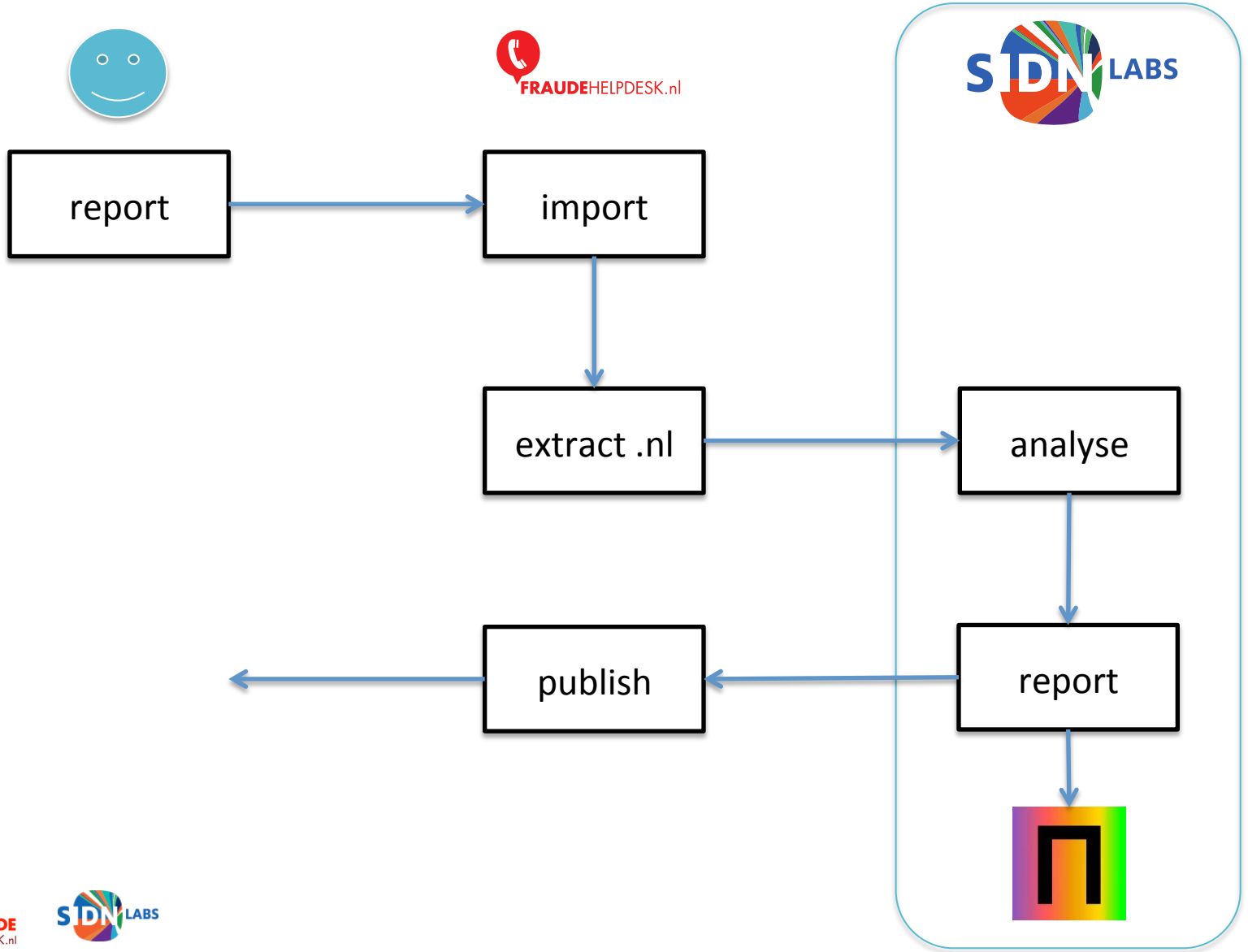


FRAUDE HELPDESK.nl SIDN LABS

JTIE Workflow for .nl



JTIE Workflow for .nl



FRAUDE HELPDESK.nl SIDN LABS

What does FHD share?

- The .nl domain name
- The full URLs (cleaned from privacy sensitive data)
- Unique mail ID

What does SIDN share?

- DNS queries from the last 7 days
- Query Peak (yes/no)
- Age
- Registrar (pseudonym)
- Classification Score

What does SIDN share?

- DNS queries from the last 7 days
- Query Peak (yes/no)
- Age
- Registrar (pseudonym)
- **Classification Score (0-3)**
  - is it a young domain? (+1)
  - is it registered at a suspicious registrar? (+1)
  - does it have query peak? (+1)

Results after 6 months

- **2.200** unique .nl domain names

  extracted from 90.000 mails

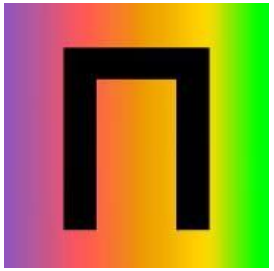
- **88** domains for sure phishing
- majority not known by Virustotal

Results after 6 months

- Why so many duplicates?
  - Many legitimate domain names from phishing targets (e.g. banks, PayPal, ...)
  - Different users report the same mail
- Why so few phishing?

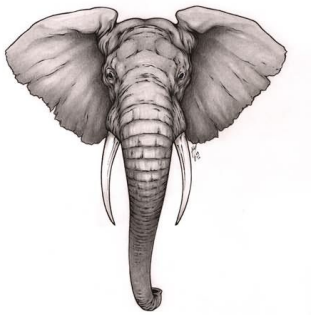
Takedown with Netcraft

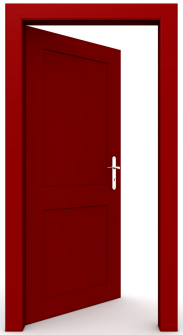
- Netcraft contacts registrars, hosters and registrants of phishing domains
- With our homemade crawler we can analyze the content
- Automatically submit domain to Netcraft
  - if *SCORE >= 2*
  - and website is still online
- 1 false positive (1,1%)
- Takedown after 90 min (on average)



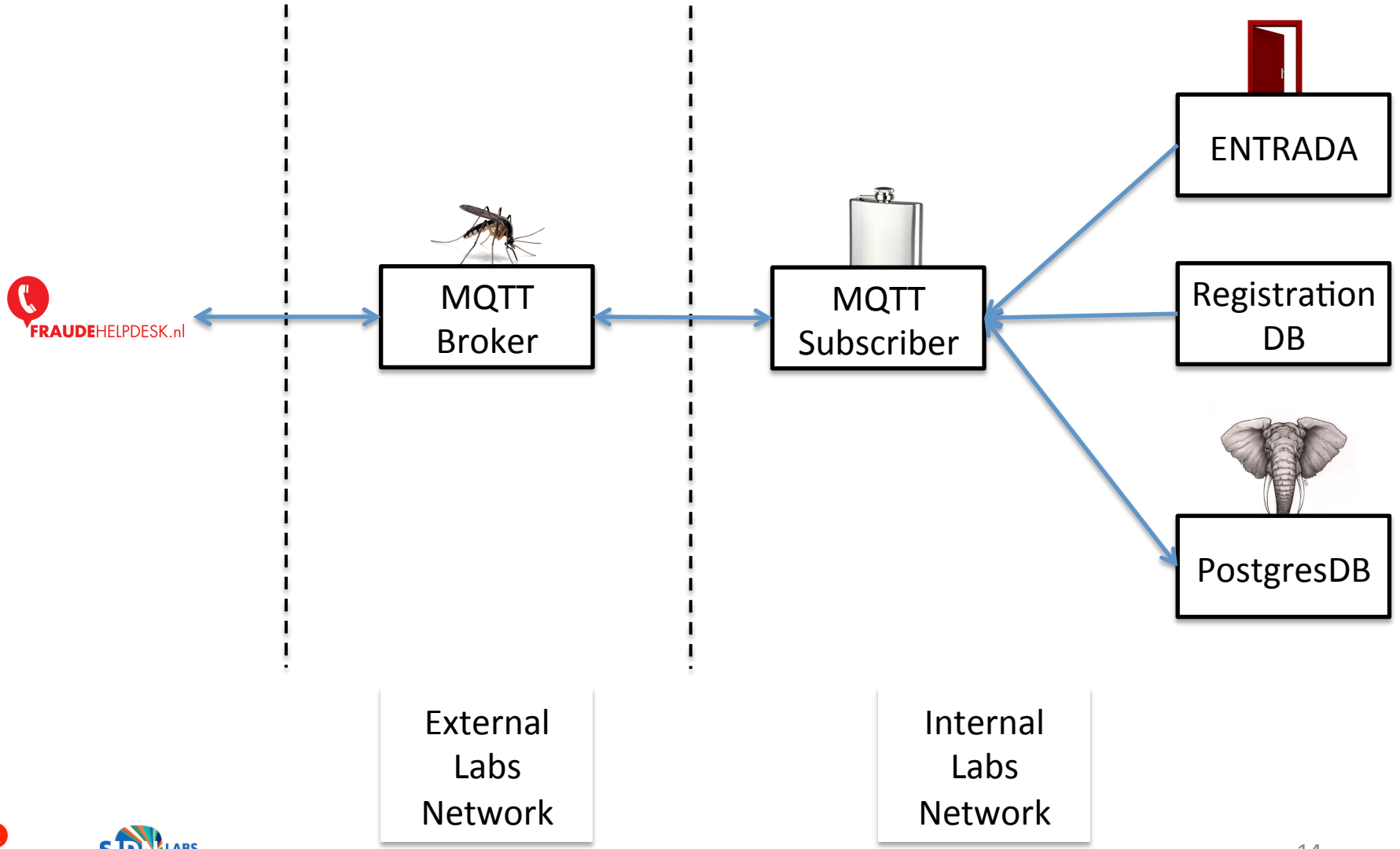
How do we share it?

- Mosquitto MQTT Broker
- Flask Python Web Framework
- ENTRADA
- Postgres DB





Setup


FRAUDEHELPDESK.nl
MQTT Broker
MQTT Subscriber
ENTRADA
Registration DB
PostgresDB
External Labs Network
Internal Labs Network

Next steps

- Rebuild backend
- Extract more features:
  - Website content
  - Registration data
  - URL
- Follow URL shorteners
- Whitelisting
- Improve peak detection

Summary

- Pre-filtering by users is powerful
- Straight forward phishing detection
- Easy ENTRADA use case

Is there room for collaboration?

Questions?

Moritz Müller

Research Engineer

moritz.muller@sidn.nl

@dhr_moe

www.sidnlabs.nl

Elmer Lastdrager

Cybercrime Researcher

ELastdrager@fraudehelpdesk.nl

@elmerlastdrager

www.fraudehelpdesk.nl