SITO:
Security Intelligence for TLD Operators

Moritz Müller | 5th CENTR Jamboree - 17 May 2016, Brussels, Belgium

Assets of TLD Operator

- Domain names
- Registrant information
- Registrar information
- …

Challenges and Goal

Generic defense mechanisms (e.g. Firewalls) don't have insight into operational data, e.g.:

- Transactions in the Domain name Registration System (DRS)
- DNS traffic to our name servers

GOAL: protect the *integrity* and *security* of .nl through *anomaly detection* modules that continuously analyze *DRS* transactions and *DNS* traffic

DRS Transactions

Registrars can:

- Transfer domain names
- Change registrant information
- Change name server information
- Delete name servers and domain names
- …

→ Domain names get stolen or redirected to malicious content

DRS Transactions - Modules

Detection of suspicious name server changes

- Based on IP reputation and country

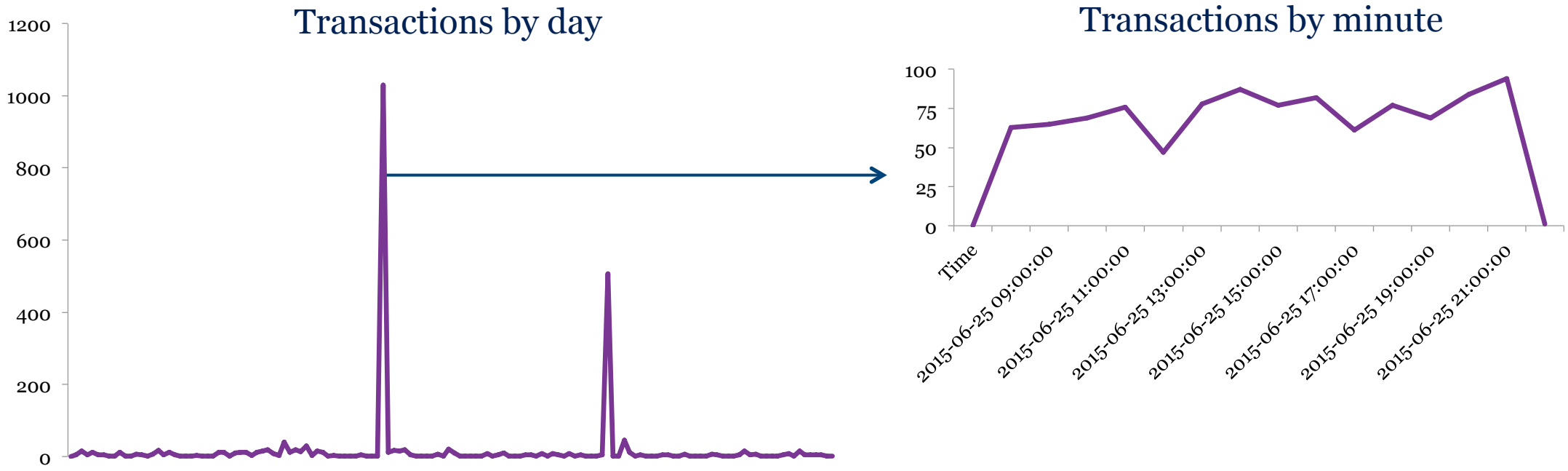
Detection of illegal transactions

- E.g. attempted transfer without token

Detection of unusual transfers

- Based on transfer spikes

DRS Transactions – Illegal transactions



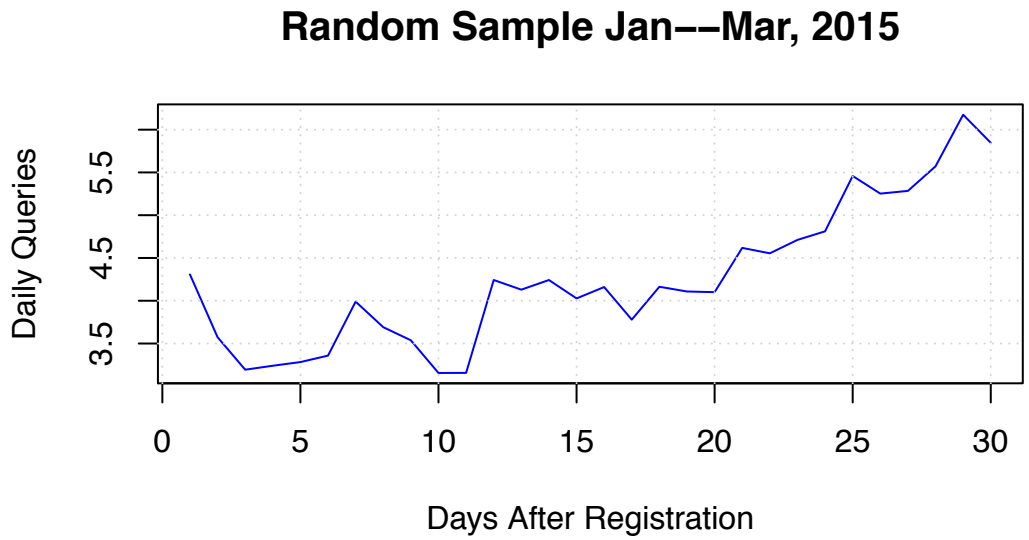
- Failed transfers per day of one registrar
- Over 1000 unique domain names affected

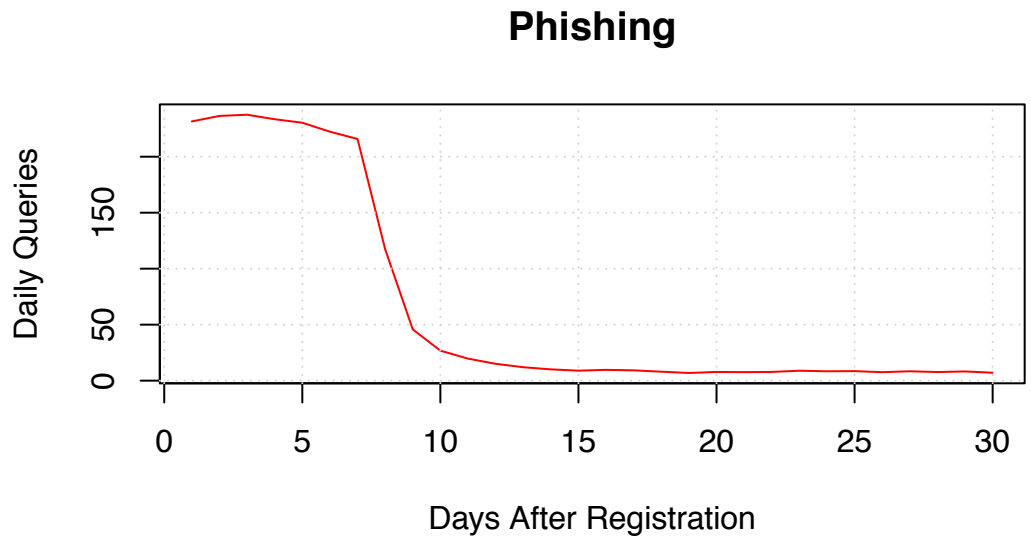
DRS Transactions – Preliminary Results

- So far, few malicious activities detected
- Outliers often misconfiguration at the registrar
- Continuous evaluation necessary
- Feedback from registrars

DNS Traffic

- Domains are misused for malicious content or botnet command and control
- DNS Traffic for malicious domains differs from “good” domains





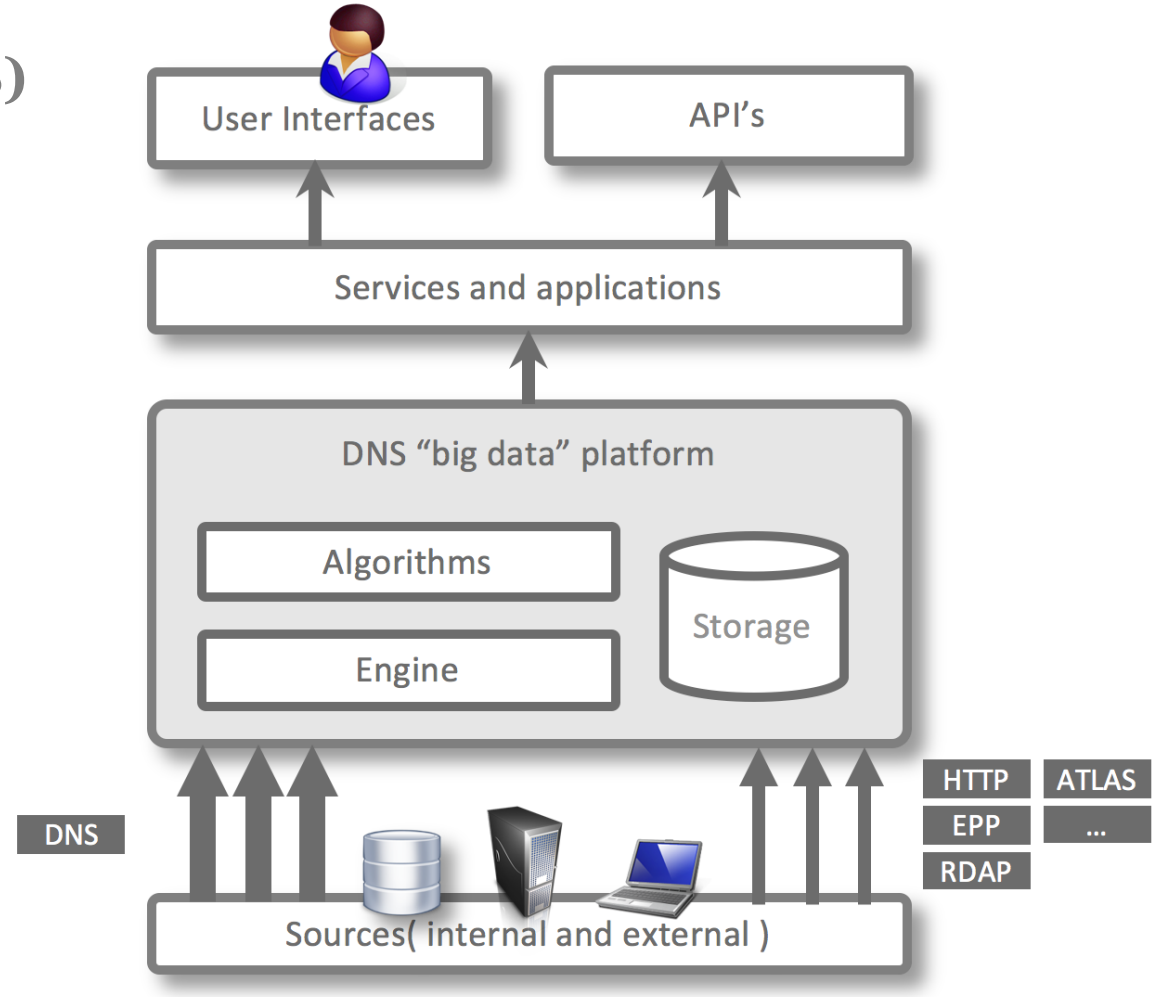
ENTRADA Architecture

SQL on Hadoop (Impala + Parquet +HDFS)

Main components

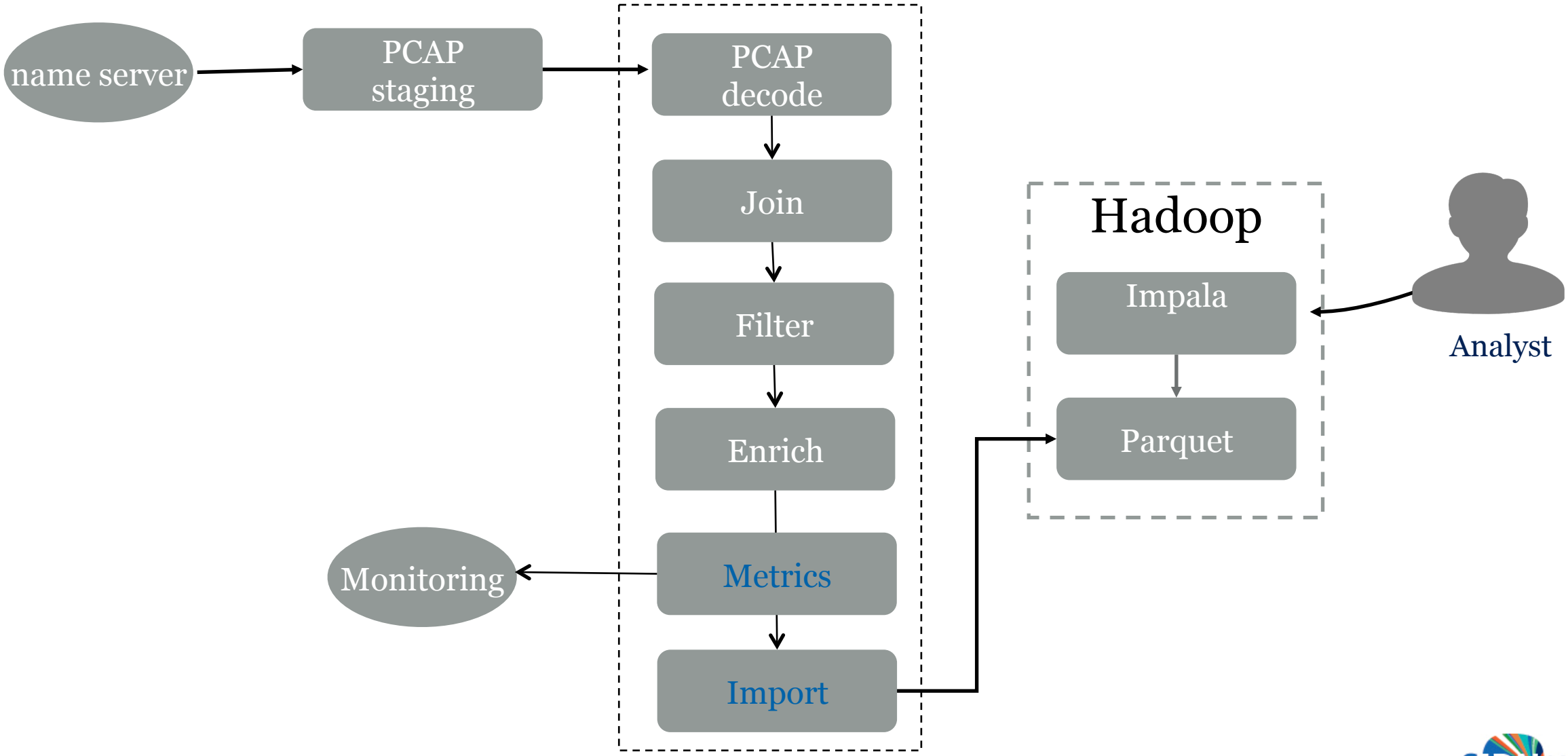
- Data sources
- Platform
- Applications and services
- Privacy framework

- Stores > 400 Million queries daily



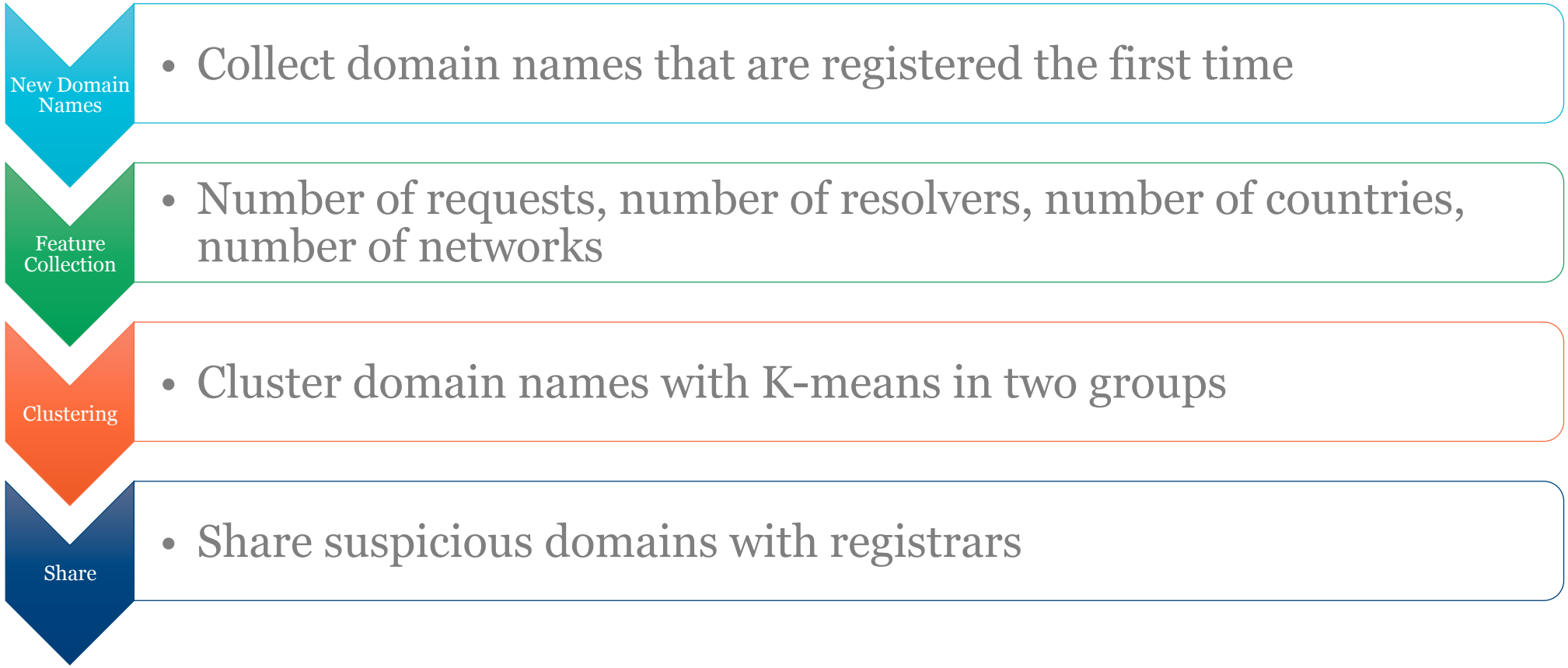
Open source: entrada.sidnlabs.nl

ENTRADA Workflow



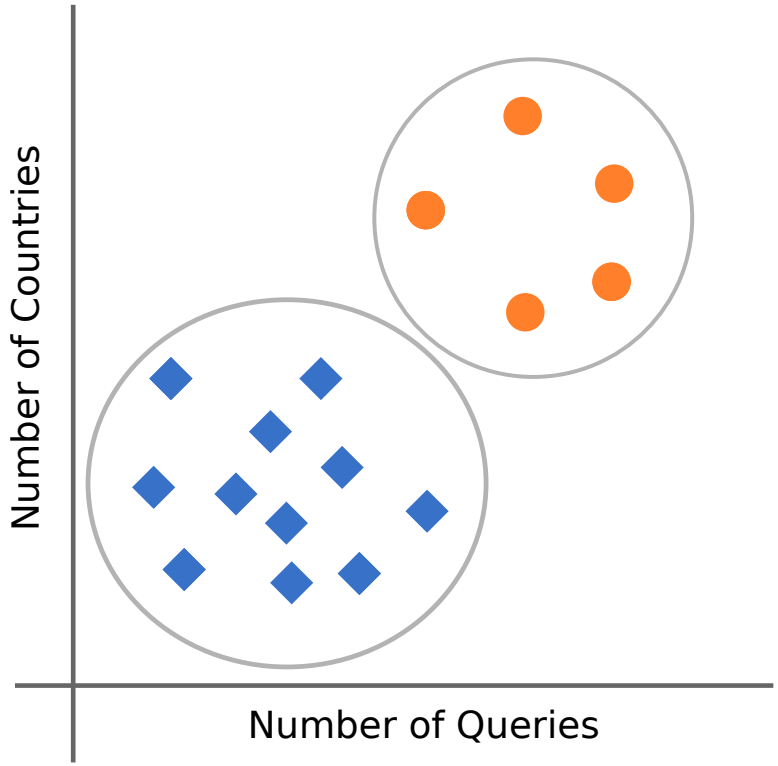
Query data available for analysis within 10 minutes

nDEWS


New Domain Names
• Collect domain names that are registered the first time
Feature Collection
• Number of requests, number of resolvers, number of countries, number of networks
Clustering
• Cluster domain names with K-means in two groups
Share
• Share suspicious domains with registrars

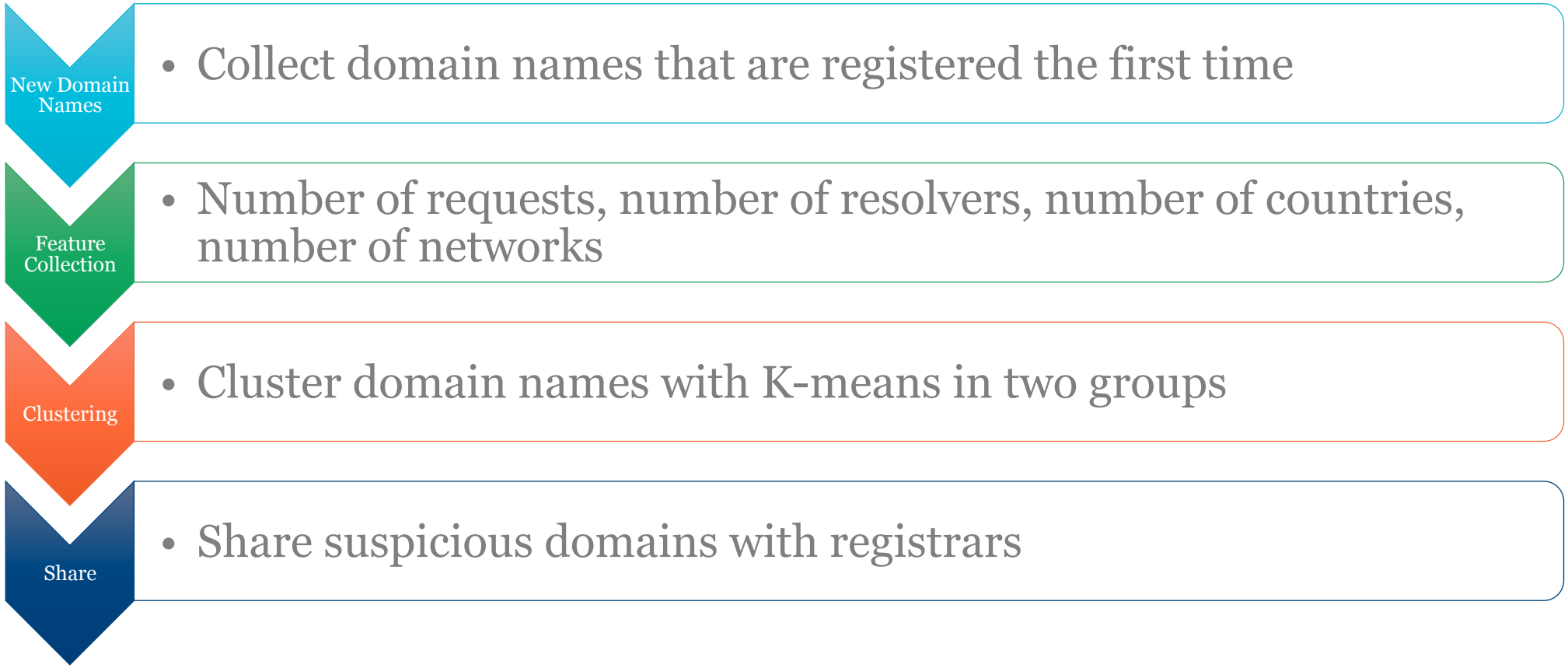
nDEWS

- Cluster domain names with K-means in two groups



K-means with K = 2 and two features

nDEWS


New Domain Names
• Collect domain names that are registered the first time
Feature Collection
• Number of requests, number of resolvers, number of countries, number of networks
Clustering
• Cluster domain names with K-means in two groups
Share
• Share suspicious domains with registrars

nDEWS Results

- Results after 9 months of evaluation

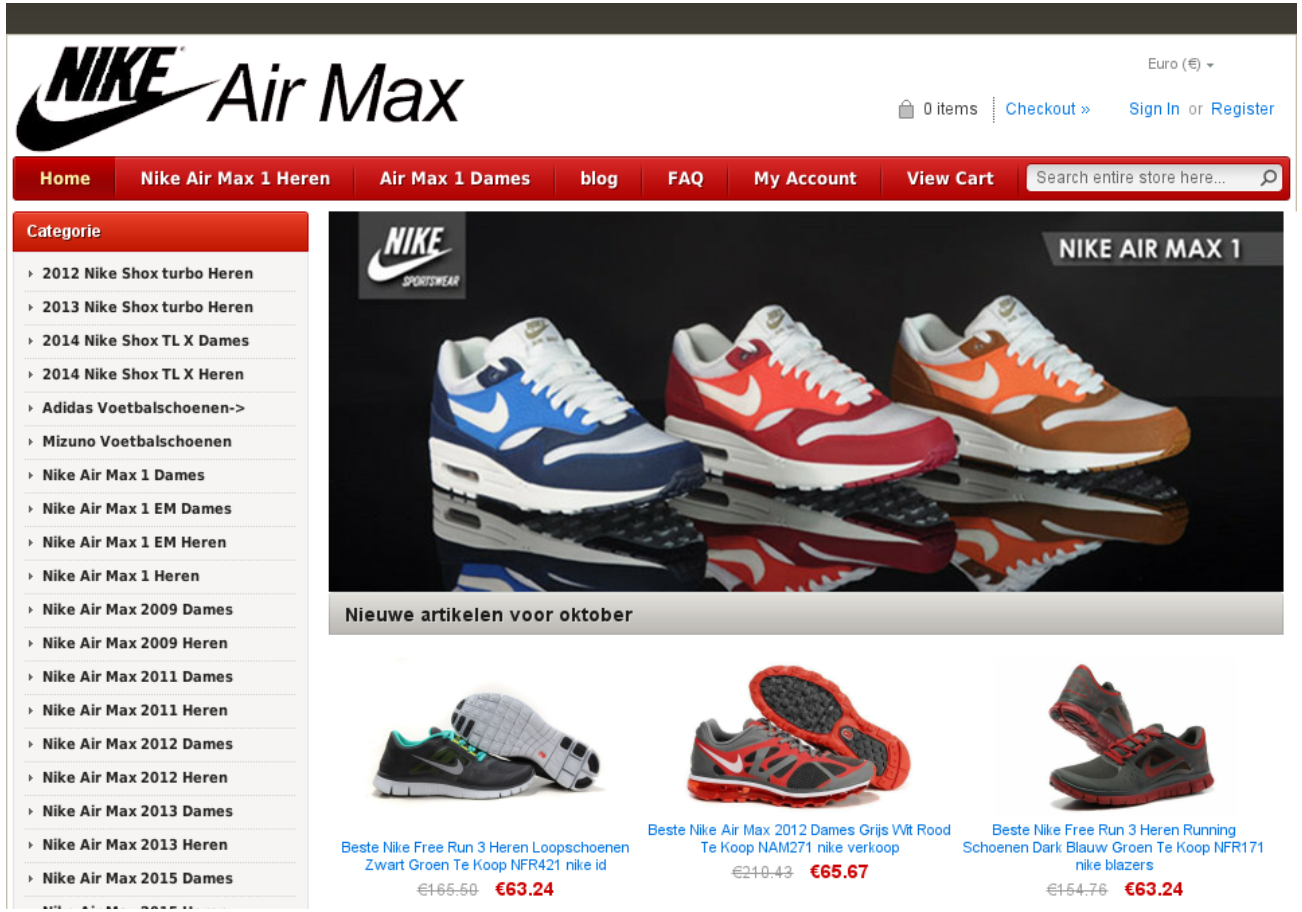
Cluster	Size	Requests	IPs	Countries	ASs
Normal	132,425	4.31	3.06	1.64	1.43
Suspicious	2,956	55.03	27.87	4.99	7.43

- Including:
  - Fake pharmacy web shops
  - Phishing websites
  - Malware
- High false positive rate on some days

nDEWS Results

- Many (fake) shoe stores
- Distributed with SPAM mails
- Big market – low penalties

- Future Work: detection of compromised domain names



Conclusions

- SITO keeps track of abnormal behavior in DNS and DRS traffic
- SITO is able to detect abnormal behavior; but it does not explain it

- Future Work:
  - connect with more registrars and hosting provider
  - improve false positive rate
  - extend towards hacked domain names

Moritz Müller

Research Engineer

moritz.muller@sidn.nl

 @dhr_moe

www.sidnlabs.nl

Thank you for your attention!