Anti-Abuse
SIDN

FIAT! 2016

5 februari 2016

Maarten Wullink & Moritz Müller, SIDN

SIDN labs
Internet Research & Innovation

SIDN

SIDN

- SIDN = registry van .nl

- Diensten
  - Voor internetters: gebruiken van .nl domeinnamen (resolving)
  - Voor registrars: domeinnaamregistratie, met DNSSEC-support
  - Voor registries: back-end registry services (.amsterdam en .aw)
  - Voor abuse/CERT community: data en early warning services (in ontwikkeling)

- Besteding resultaat
  - SIDN Fonds: gebruik en maatschappelijke impact van de internetinfra
  - **SIDN Labs**: R&D voor meer veiligheid, stabiliteit en schaalbaarheid van internetinfra zelf (.nl, DNS en als geheel)
  - Registars en andere stakeholders: hulp bij technologie-adoptie (bijv. DNSSEC, AbuseHUB, Campus Challenge)
  - *In the end* impact op de internetgebruiker (individu of organisatie)

SIDN labs
Internet Research & Innovation

SIDN

SIDN Labs

- Doel: ontwikkelen en evalueren van
  - Nieuwe mechanismes en systemen die de security en stabiliteit van .nl, het DNS en de internet infra vergroten
  - Nieuwe diensten voor SIDN
  - Beide zo veel mogelijk samen met de Nederlandse R&D community

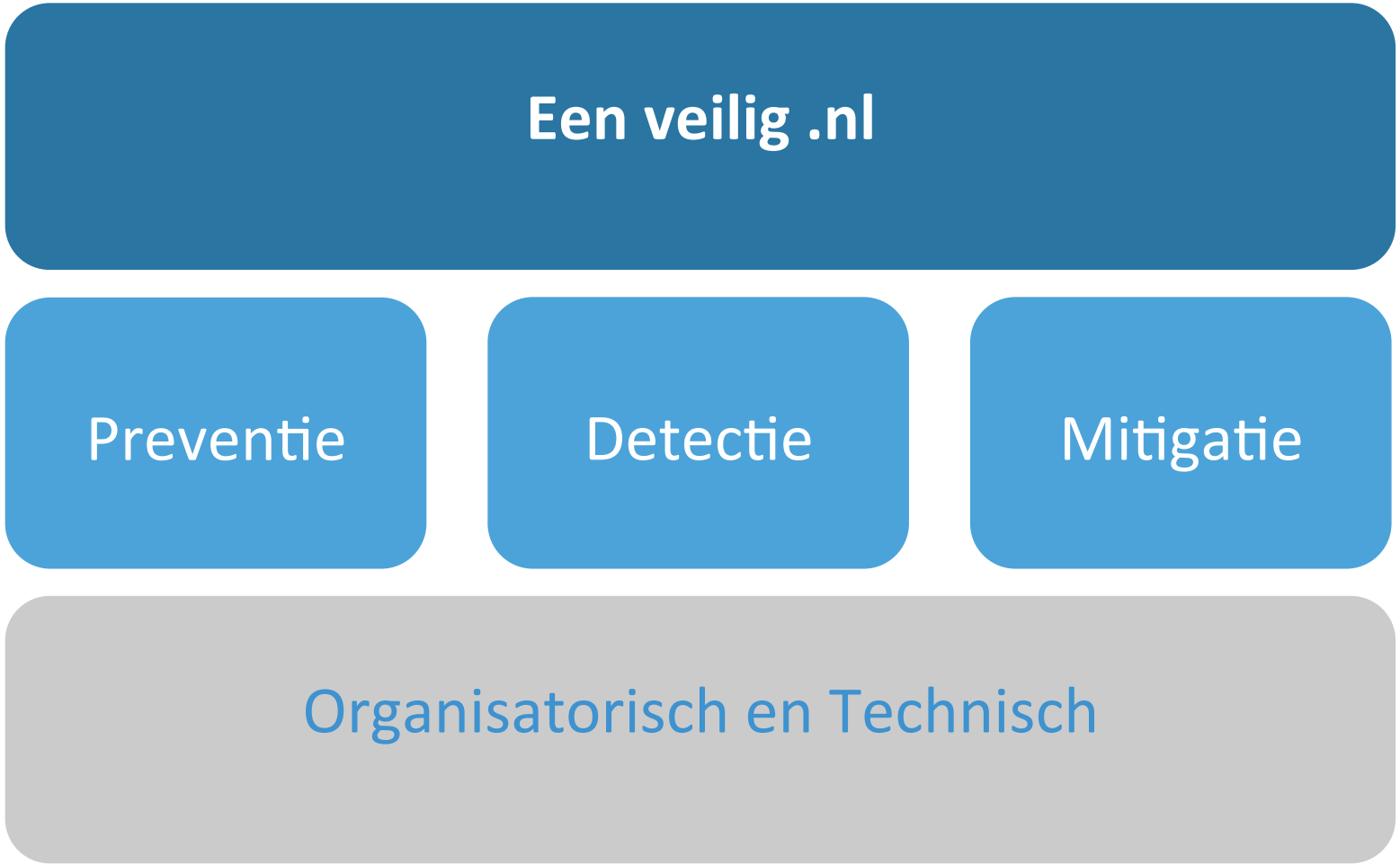
- Beoogde impact:
  - Verhoogde waarde van het internet (afgeleid: versterkte reputatie van SIDN als onafhankelijk expertisecentrum)
  - Verder geïnnoveerde dienstverlening SIDN
  - Versterkte positie van onderzoek uit Nederland met toegevoegde waarde voor .nl en het internet

- Labnetwerk voor prototyping/evaluatie

SIDN labs
Internet Research & Innovation

SIDN

Anti-Abuse

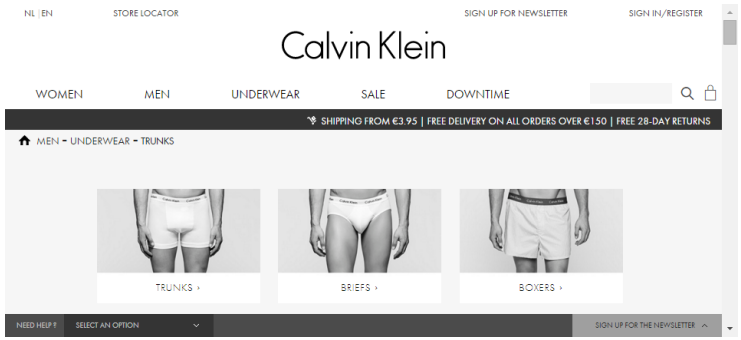


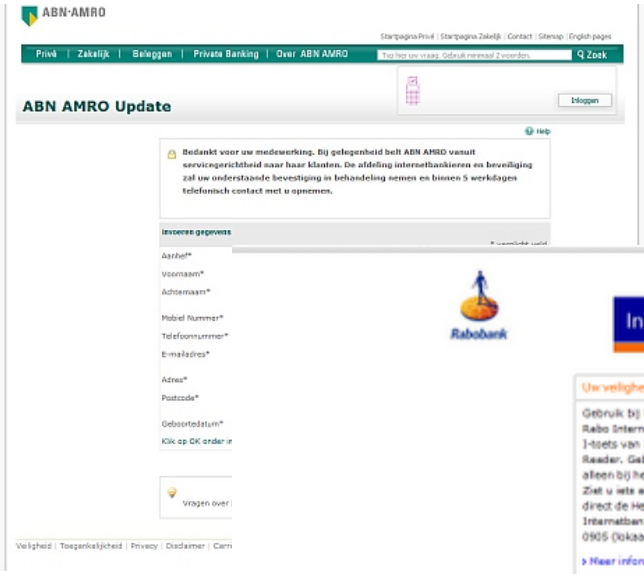
SIDN labs
Internet Research & Innovation

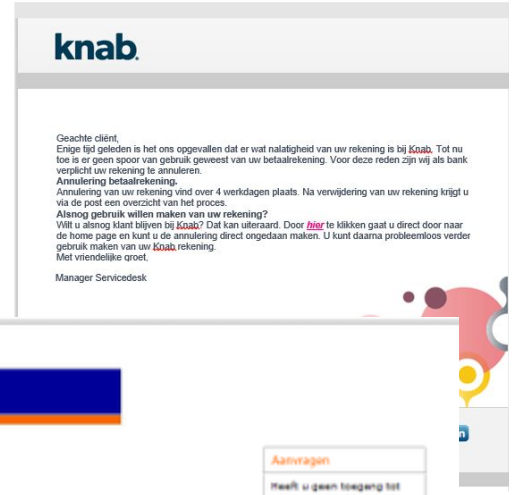
SIDN

Preventie

Phishing







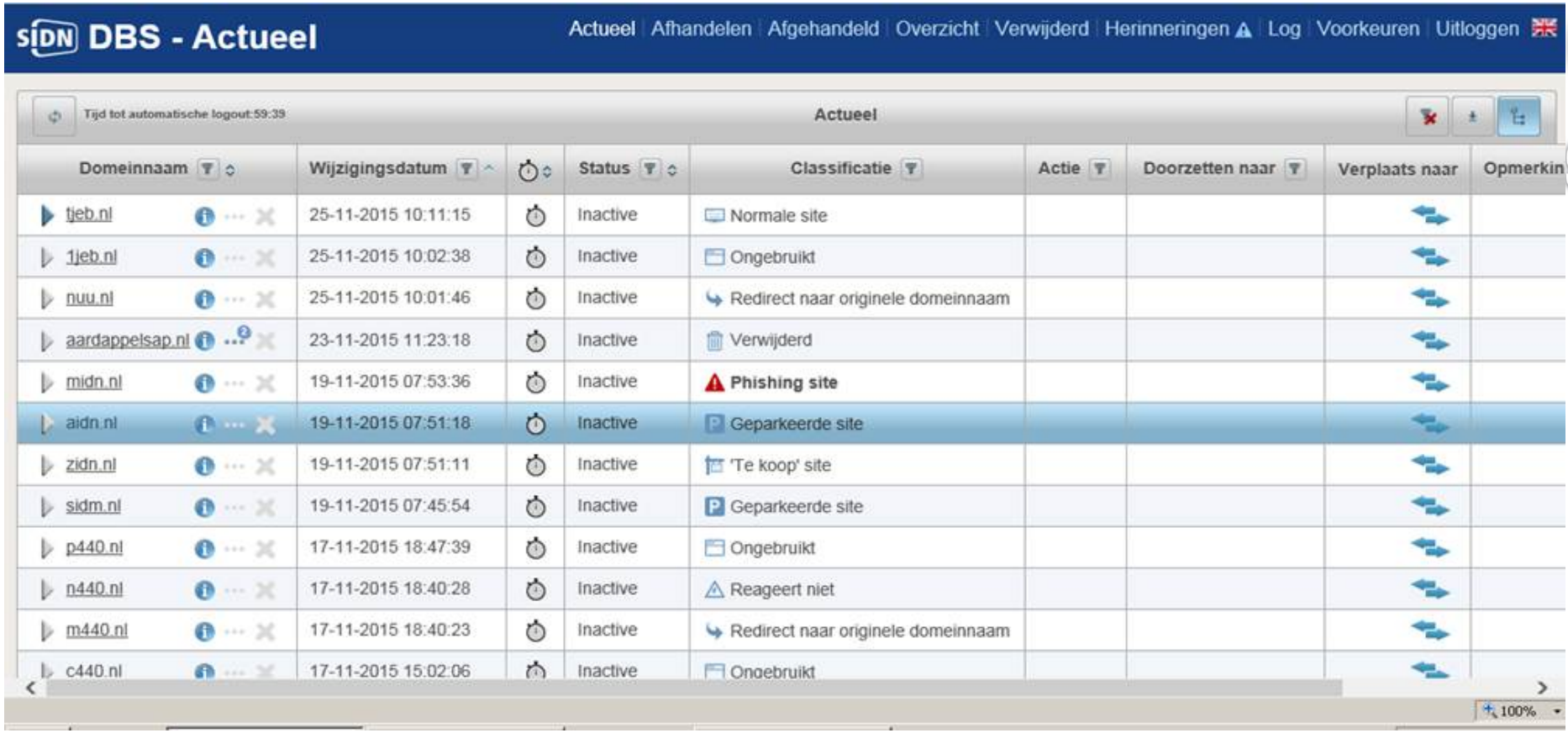
SIDN labs
Internet Research & Innovation

SIDN

Domeinnaambewakingsservice (DBS)

- Real-time monitoring
- Alle .nl-domeinnamen (binnenkort ook andere TLD’s)
- Classificatie websites (Phishing, malware etc.)

Domeinnaambewakingsservice (DBS)



Rijksoverheid

.nl control

Zelf 100% controle over uw domeinnaam. Er worden geen wijzigingen doorgevoerd zonder uw nadrukkelijke toestemming.

- wijzigen gegevens domeinnaam
- (houder, admin-c, tech-c, nameserver, DNSSEC-sleutelmateriaal)
- wijzigen gegevens contactpersoon
- domeinnaam verhuizen
- domeinnaam verwijderen
- wijzigen van de glue records van de in-zone nameserver

SIDN labs
Internet Research & Innovation

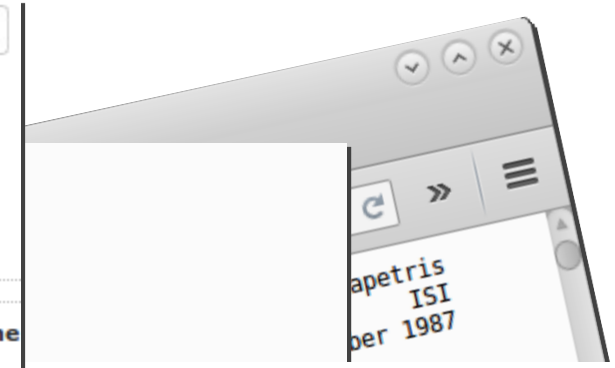
SIDN

Security / Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

By Larry Seltzer | Posted 2009-04-22 Email Print

OPINION: Attack shows the potential for serious spoofing attacks that could leave end users helpless. The only real solution is DNSSEC, which will take years to implement under the best of circumstances.



Follow via:

DNS cache poisoning attacks exploited in the wild

HOME « NEWS « TOP SECURITY STORIES « GOOGLE'S MALAYSIAN DOMAINS HIT WITH DNS CACHE POISONING...

GOOGLE'S MALAYSIAN DOMAINS HIT WITH DNS CACHE POISONING ATTACK

ave provided more details in their "30 Days of DNS
' HD Moore's statement on DNS cache poisoned AT&T
ces are starting to see evidence of DNS cache poisoning
appears to be an attempt to take advantage of the
y :" client 143.

DNS poisoning slams web traffic from millions in China into the wrong hole

ISP blames unspecified attack for morning outage

By John Leyden, 21 Jan 2014

GMT (04:24 BST)

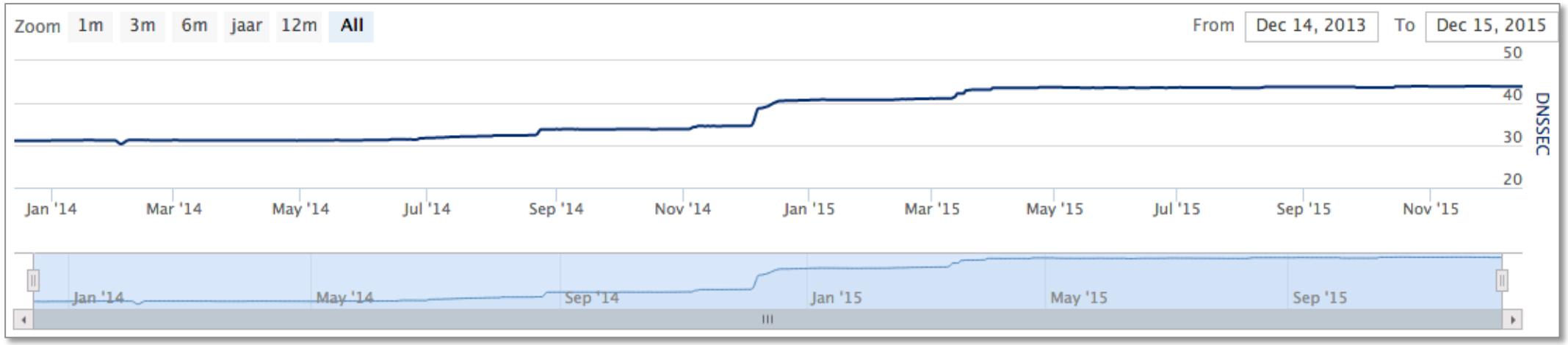
s of DNS Attack Activity"
ed AT&T DNS servers. Numerous
ng attempts on their local
"recent" DNS cache poisoning
lnerable if any of the results below are

Scatterplot

DNSSEC

- Incentive voor het signeren van domein namen

- 44% van alle .nl domeinnamen heeft DNSSEC support



SIDN labs
Internet Research & Innovation

SIDN

ValiBox

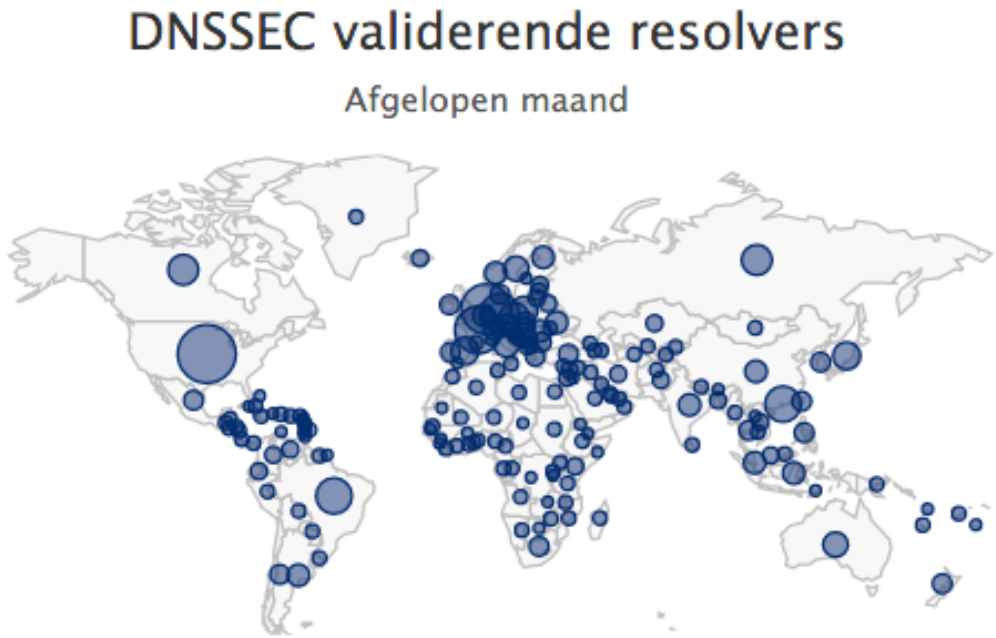
- Thuis validatie test
- GL-INET device
- Gebaseerd op OpenWRT
- Aangepaste Unbound resolver

SIDN labs
Internet Research & Innovation
SIDN

DNSSEC validatie

- SIDN validerende resolver
  - Pilot bij een educatieve instelling

- stats.sidnlabs.nl



SIDN labs
Internet Research & Innovation

SIDN

Wetenschappelijk onderzoek

- REMEDI3S for TLDs (REMEDI3S-TLD)
  - Ontwikkelen van security metrics for top-level domains (TLDs)
  - Universiteit Delft, NCSC en SIDN

- The Open INTernet Evolution Library (OpenINTEL)
  - Platform waarmee de evolutie van het internet geanalyseerd wordt, door continue DNS metingen uit te voeren.
  - Universiteit Twente, SURFnet en SIDN

- Self-managing Anycast Networks for the DNS (SAND)
  - Bepalen optimale plaatsing van gevirtualiseerde DNS anycast nodes, voor een zelfsturende DNS anycast dienst
  - Universiteit Twente, NLnet Labs en SIDN

TU Delft

UNIVERSITY OF TWENTE.

SURF NET

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

NLnet Labs

SIDN labs
Internet Research & Innovation

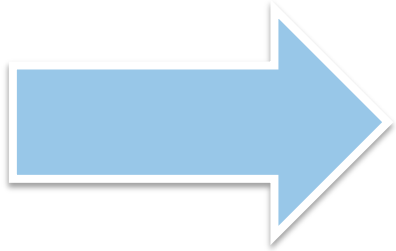
SIDN

Detectie

Waar zoeken we naar?

- Domeinnamen die gebruikt worden voor:
  - Phishing
  - Webshops met namaakproducten
  - Distributie van malware

- Botnet clients



“BIG DATA” analytics

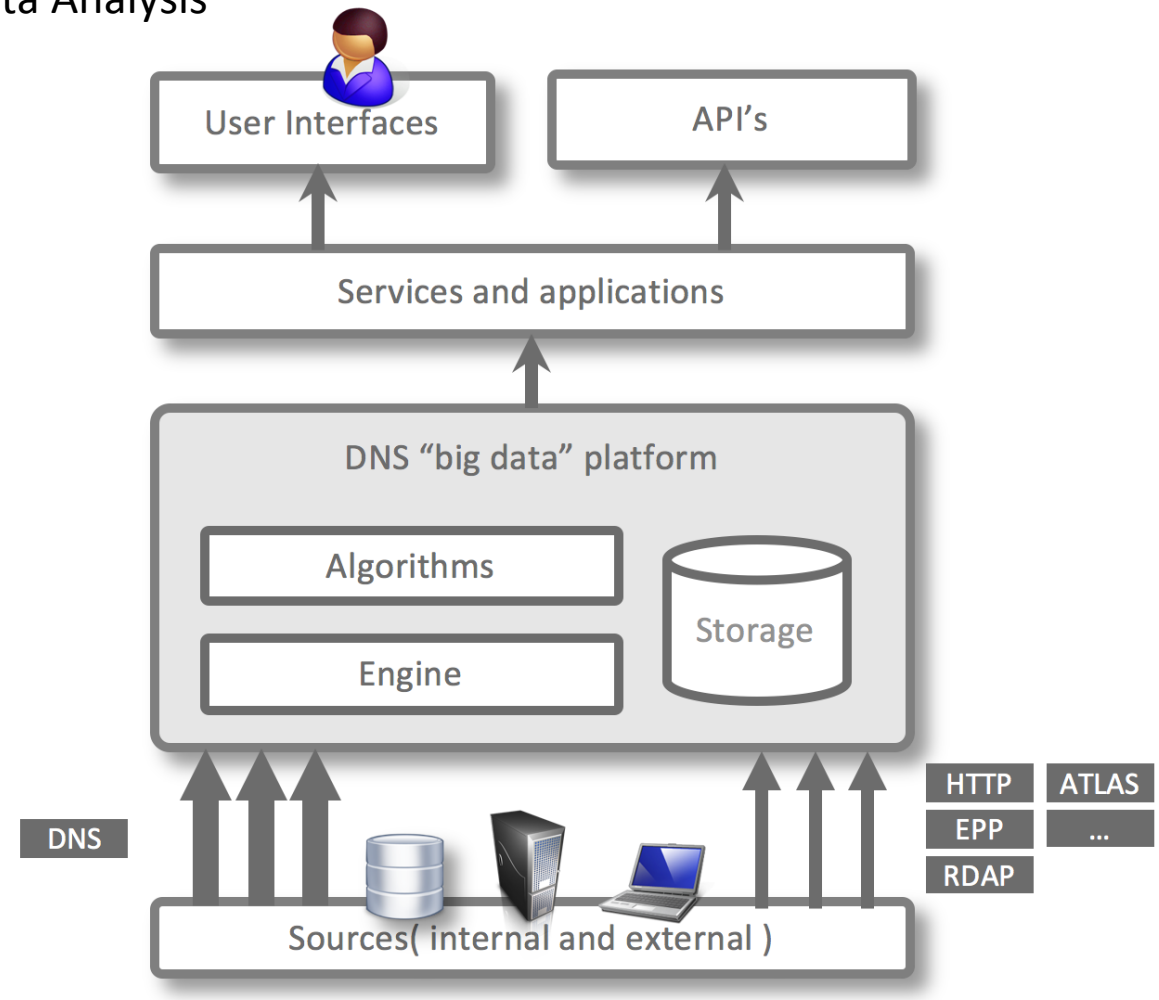
SIDN labs
Internet Research & Innovation

SIDN

ENTRADA

ENhanced Top-level Domain Resilience through Advanced Data Analysis

- ‘**DNS big data**’ systeem
- **Doel**: ontwikkelen van toepassingen welke de veiligheid en stabiliteit van .nl, DNS en het Internet verhogen
- **ENTRADA** hoofd componenten
  - Applicaties en services
  - Platform en data bronnen
  - Privacy framework
  - Platform + privacy framework = ENTRADA

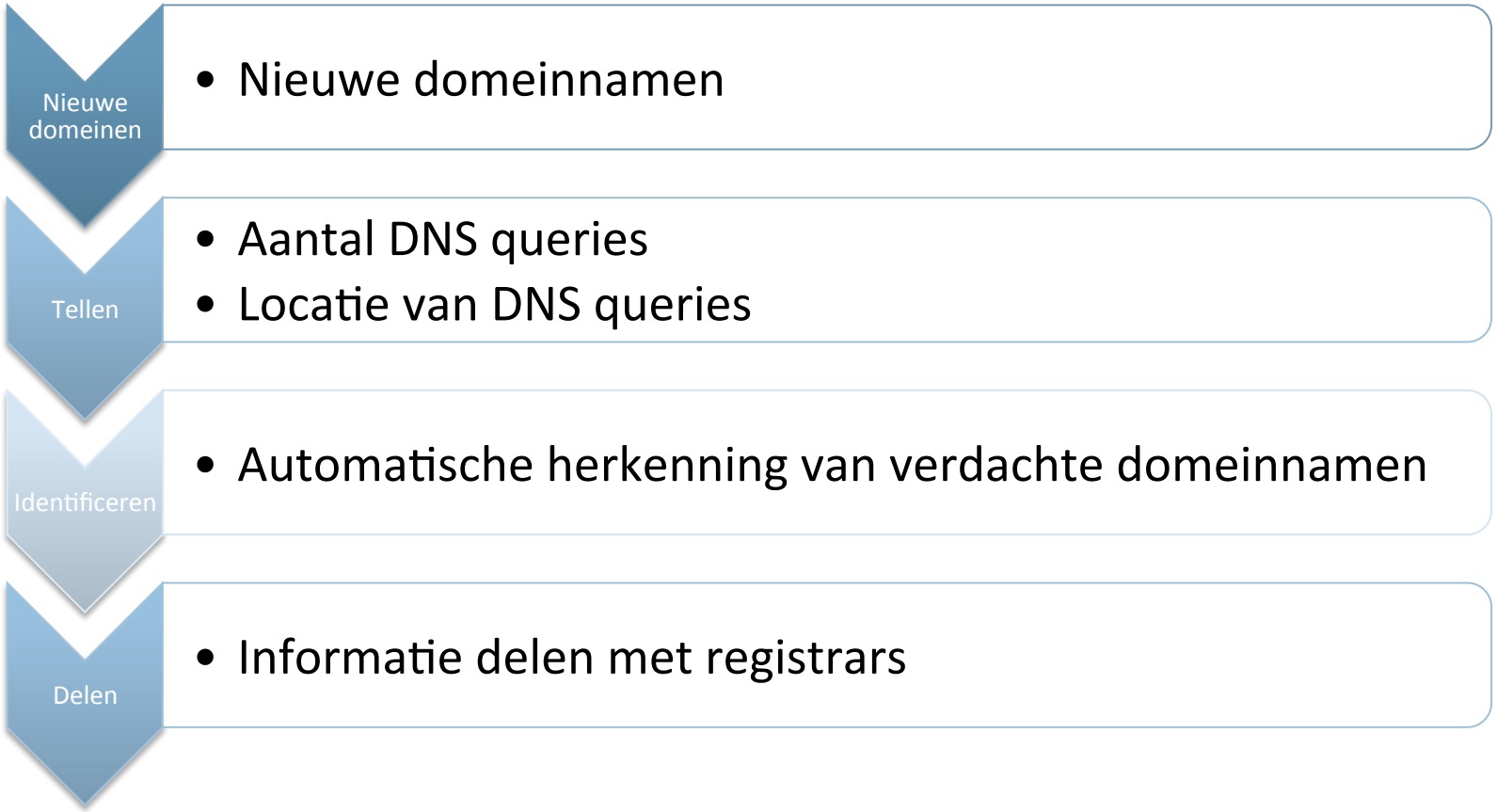


SIDN labs
Internet Research & Innovation

SIDN

Security Intelligence for Top-level Domain Operators (SITO)

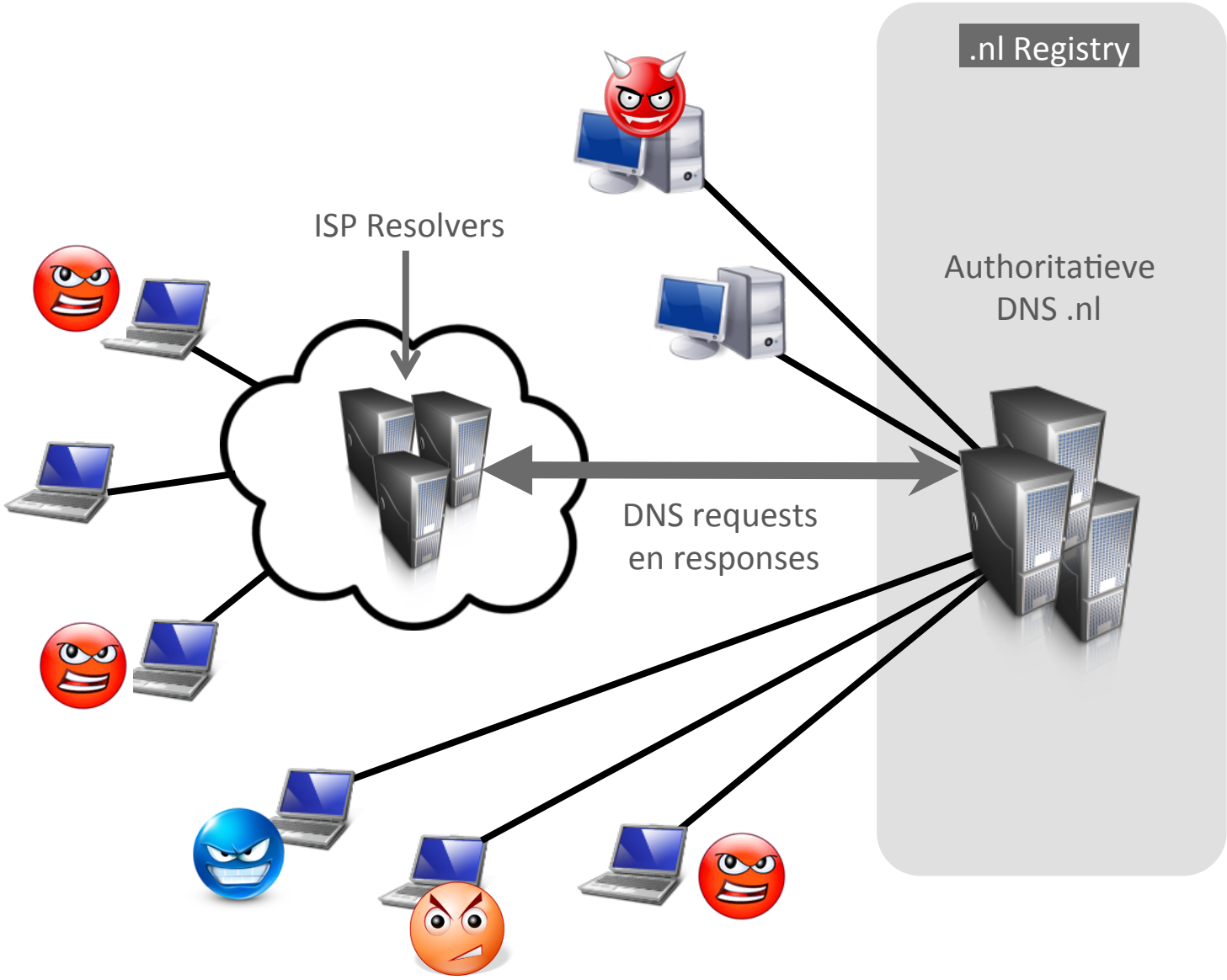
Herkenning van verdachte nieuwe domeinnamen



SIDN labs
Internet Research & Innovation

SIDN

Botnet client detectie



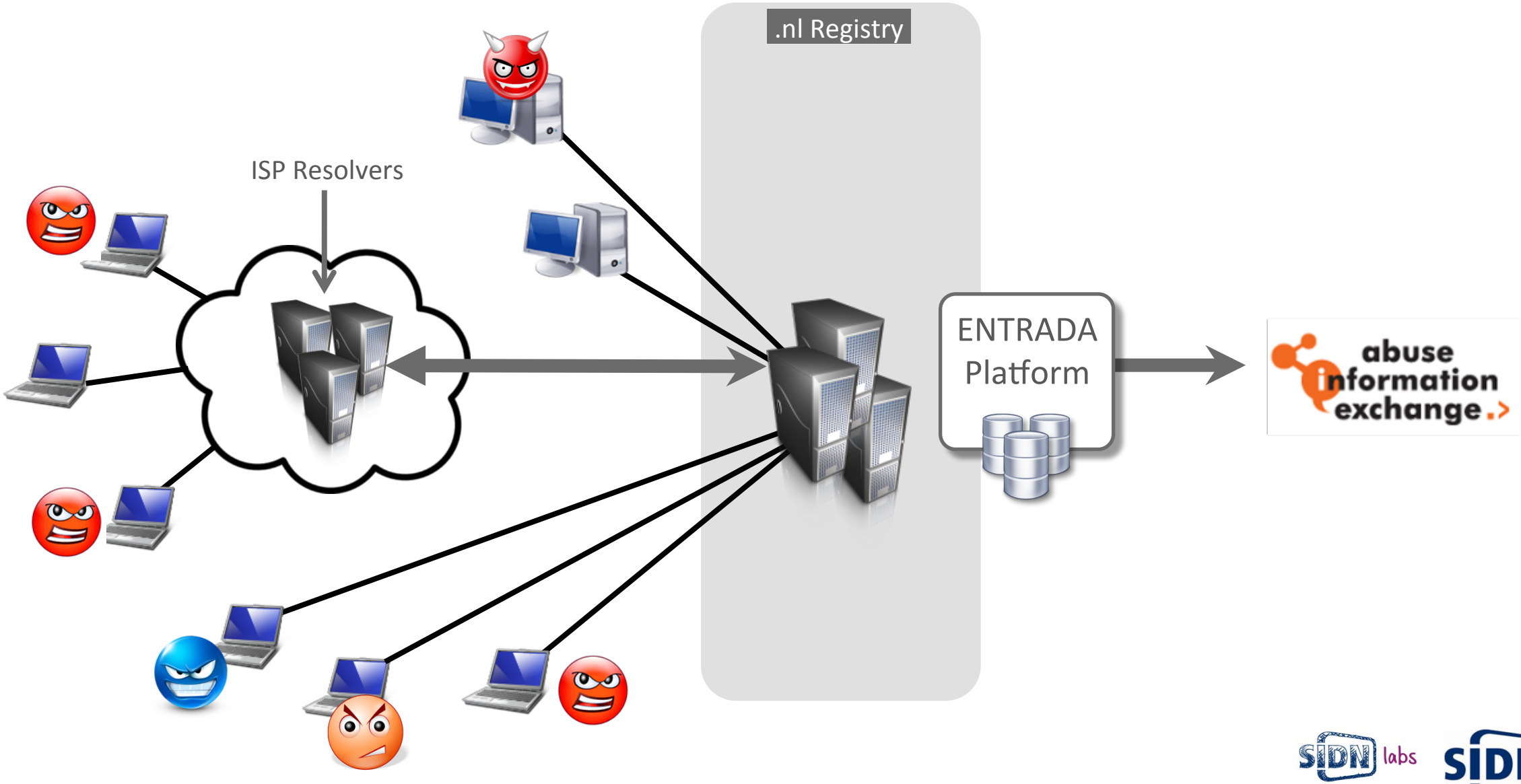
Malafide activiteiten:

- Spam-runs
- Botnets
- DNS-amplificatie aanval

SIDN labs
Internet Research & Innovation

SIDN

Botnet client detectie – koppeling met AbuseHUB



SIDN labs
Internet Research & Innovation

SIDN

Mitigatie

Actionable intelligence

- AbuseHub
  - Nederlandse ISPs tegen internet-abuse
  - Informatie van “Reliable notifiers”

- SIDN
  - Reliable notifier van NL infecties
  - 5-10 per dag

SIDN labs
Internet Research & Innovation

SIDN

Abuse204.nl

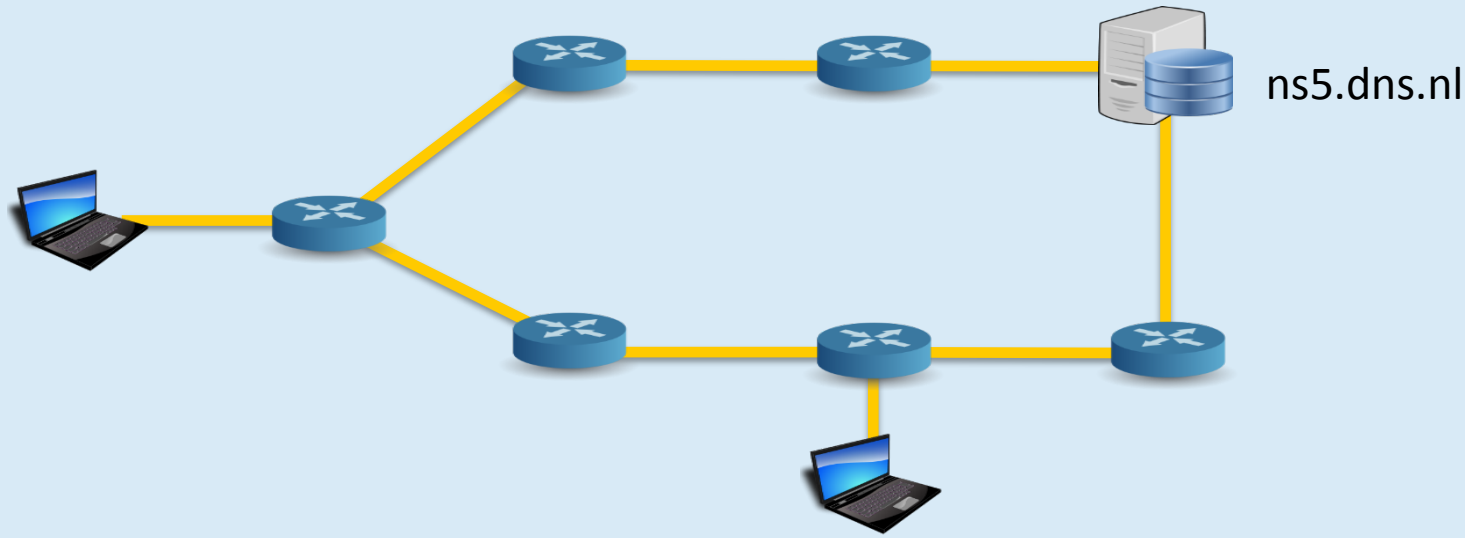
- Verminderen van phishing en malware in de .nl zone
- Gebaseerd op **Netcraft**
- In samenwerking met registrars en hosting provider

SIDN labs
Internet Research & Innovation

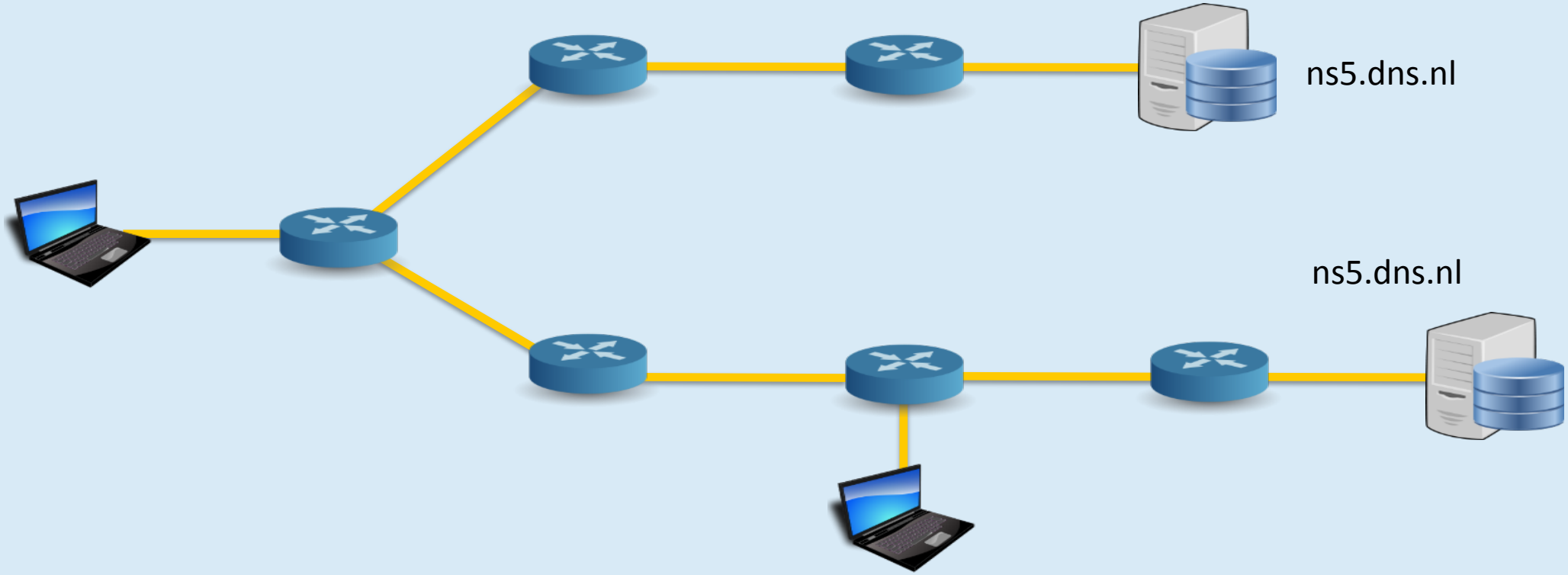
SIDN

DNS Anycast – Wat routers denken

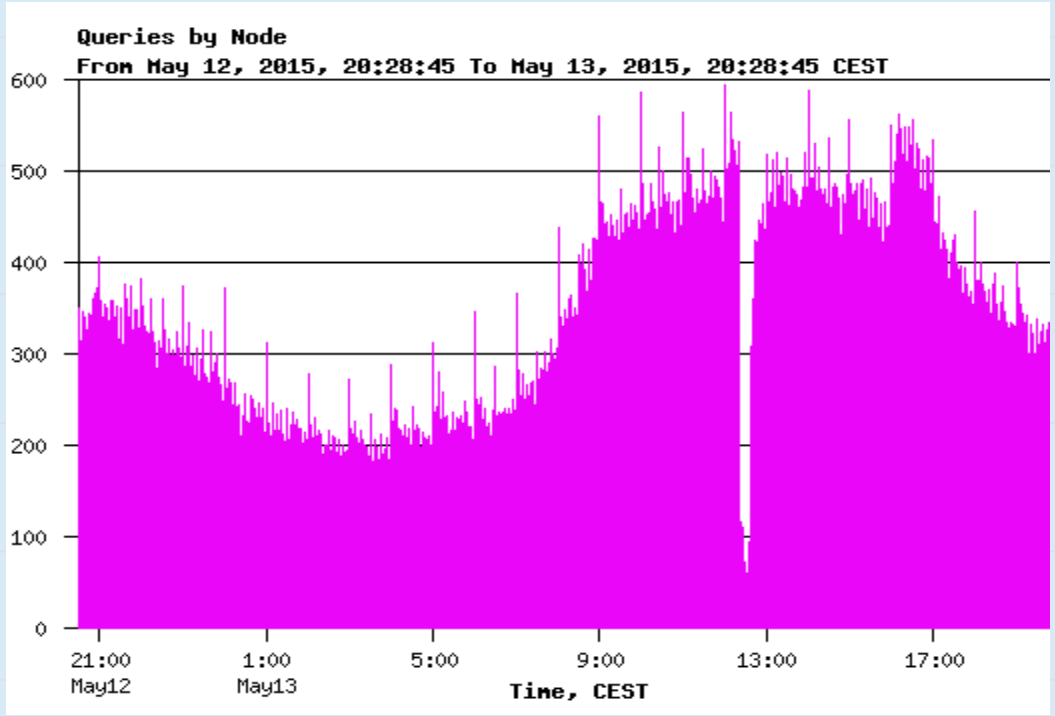
- Hogere beschikbaarheid van DNS
  - Tegen DDOS
  - Tegen netwerk storing
- Wat denken de routers?

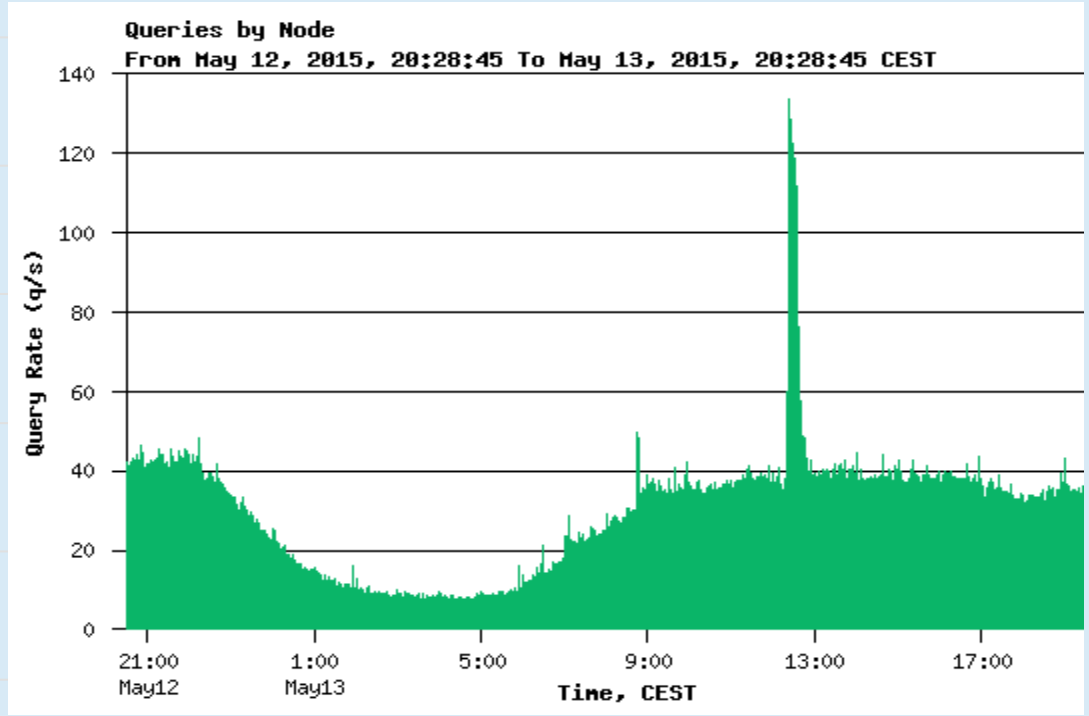


DNS Anycast – Hoe het werkelijk is



Het werkt!



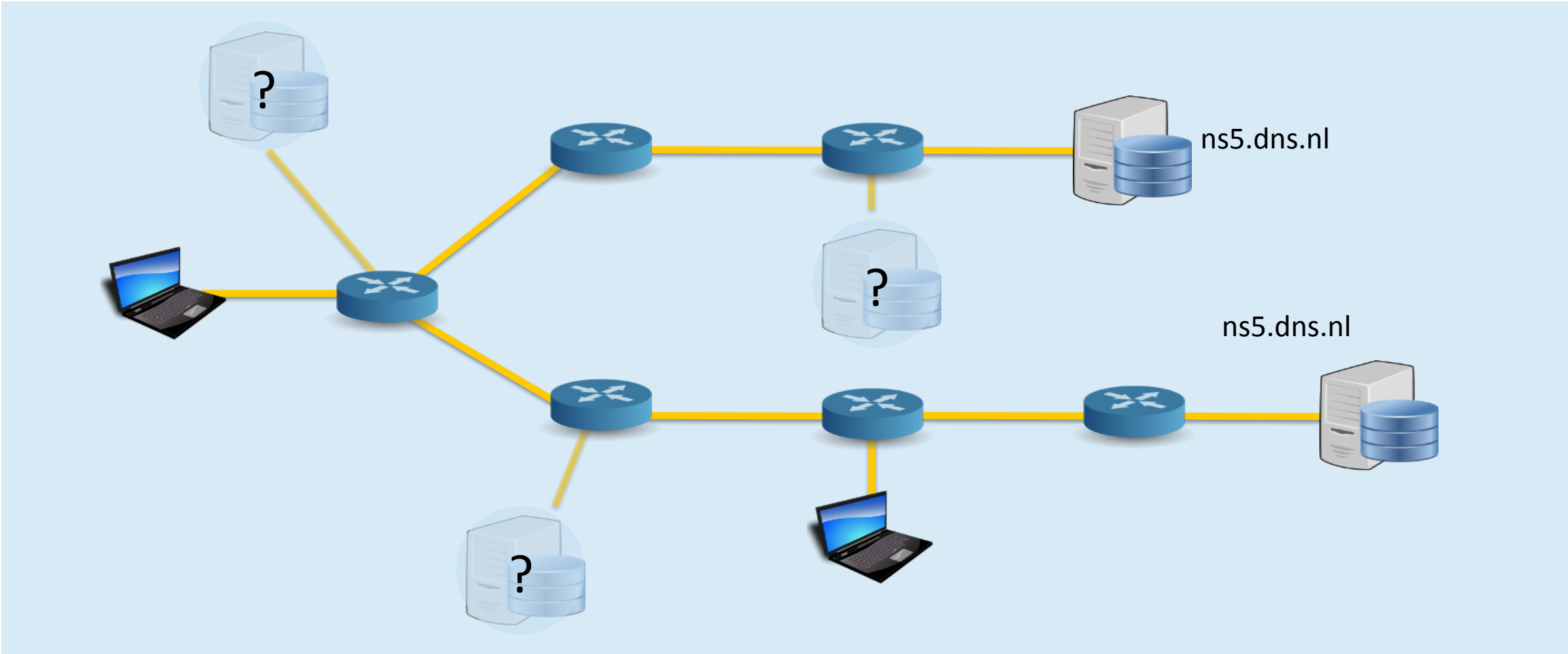


AMS-IX storing Woensdag 13-05-2015

SIDN labs
Internet Research & Innovation

SIDN

SAND – Onderzoek: Waar plaatsen wij onze servers?



Vragen?

Maarten Wullink

Research Engineer

maarten.wullink@sidn.nl

@wulliak

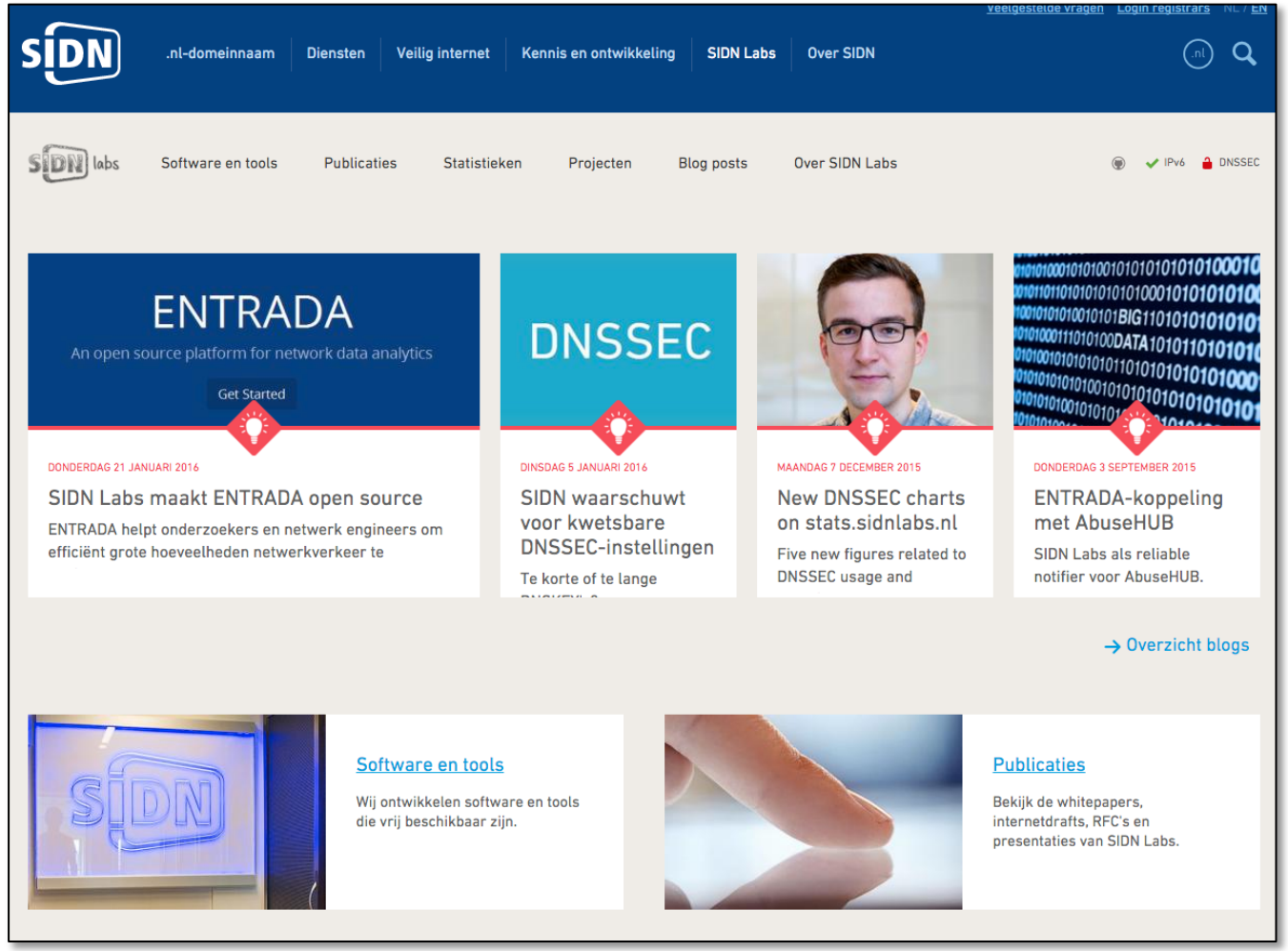
Moritz Müller

Research Engineer

moritz.muller@sidn.nl

@moritz_cmu

www.sidnlabs.nl



SIDN labs
Internet Research & Innovation

SIDN