ITHI:
Identifier Technology Health Indicators

Defining Metrics

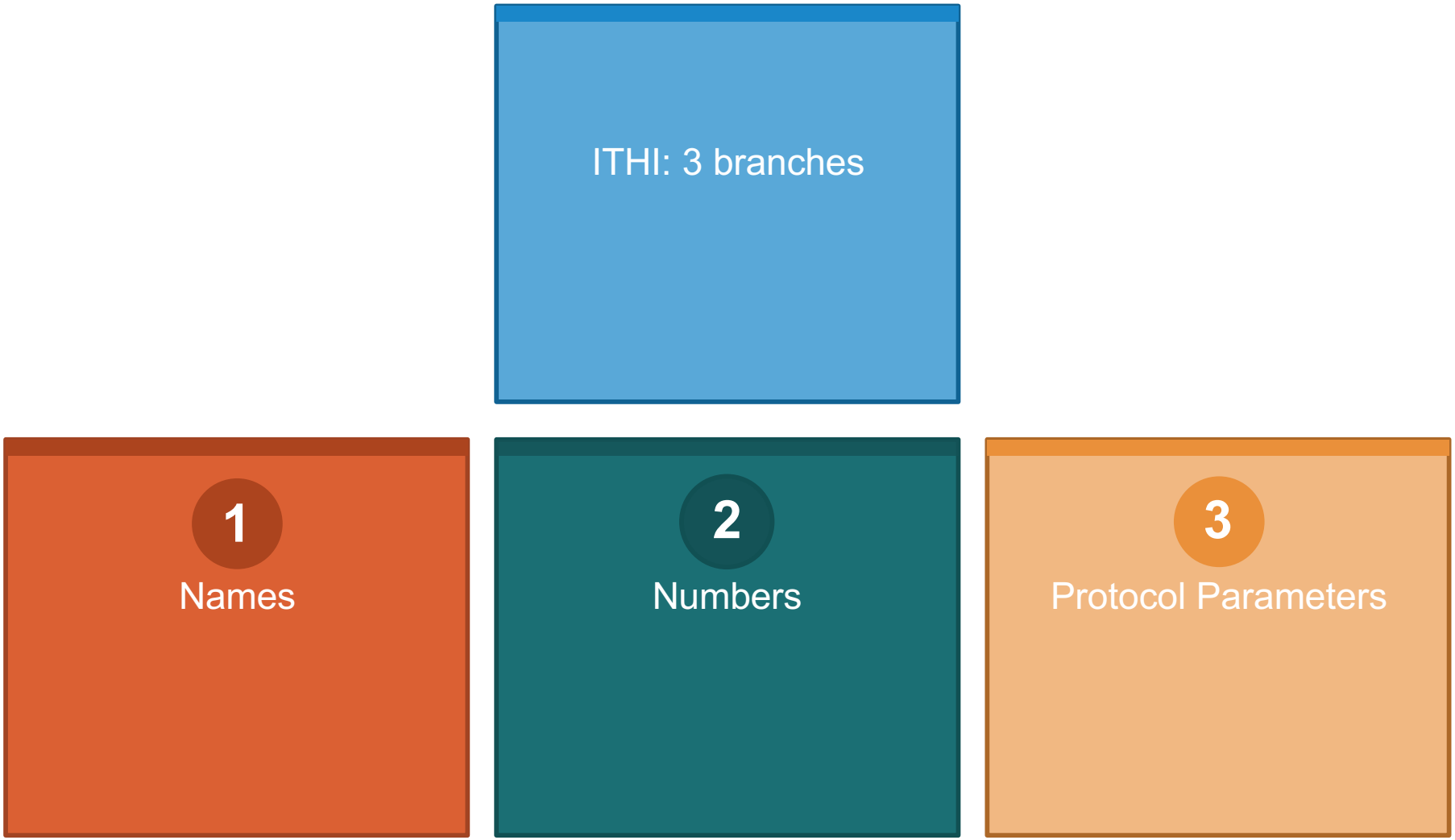
Alain Durand

Lacnic 28 / Lacnog 2017
September 2017

ITHI GOAL

- ITHI: Identifier Technology Health Indicators
- Track over time a set of indicators that reflect the “health” of the system of identifiers ICANN
- The “actual” value of any of those indicators may not as important to us as the trend they are on.
- ITHI work will stop at presenting the data and leave it to the community to take any action deemed necessary (e.g. new policy).

ITHI Branches



ITHI Numbers

NRO-Driven Process

Number Community Participation

- The NRO is driving the evaluation of ITHI metrics for the Numbers community.
- The RIR registry services have proposed a set of metrics focused on data accuracy. Those metrics are now being reviewed by the RIR community*.
- It is expected that this branch of the project will be merged with the overall ITHI initiative at a later point in time.

(*) https://www.nro.net/global-consultation-on-identifier-technical-health-indicators-ithi-project/

ITHI Names

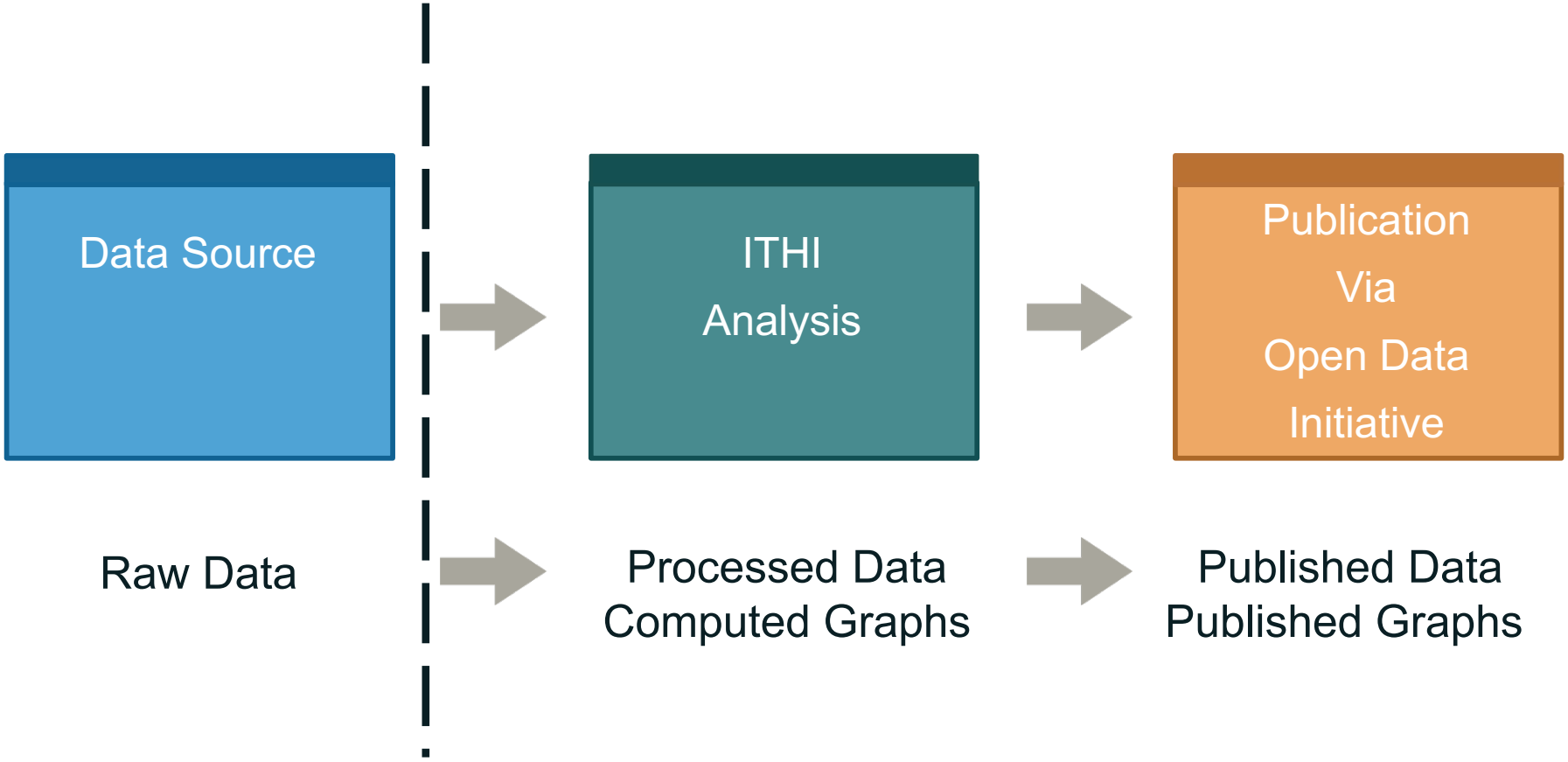
ITHI: Names

- We have identified 5 “Problem Areas”:
  - DNS Data (In-)Accuracy
  - DNS Abuse
  - Overhead in DNS Root Traffic
  - DNS Leakage
  - DNS Resolver Misbehavior

- Over time, new problem areas could be defined, and/or some could removed.

ITHI Names: Process

- For each “Problem Area”, we will put in place a 3-stage pipeline



Candidate Metric Related to Data (in-)Accuracy

M1	Data (In-)Accuracy
M1 encompass 2 sub-metrics	
M1.1	Number of “validated complaints” per million registrations
	A “validated complaint” is a complaint received by the ICANN compliance department that has been acted on. In other words, this is not an obviously frivolous complaint.
M1.2	whois.icann.org/en/whoisars

Candidate Metrics Related to Abuse

M2	Number of abuses in the ICANN DAAR* feeds for each TLD
M2 encompass 4 sub-metrics	
M2.1	Spam
M2.2	Phishing
M2.3	Malware
M2.4	Botnet

(*)DAAR: Domain Abuse Activity Reporting: https://www.icann.org/octo-ssr/daar

Candidate Metric Related to Overhead in Root Traffic

M3	The overhead to the minimum traffic that would be required in a “best case” scenario where all DNS resolvers were only asking for TLDs that exists and would respect the associated TTLs.
M3 encompass 2 sub-metrics	
M3.1	% of NX domain
M3.2	% of queries that should never have been sent (TTL)

Candidate Metric Related to Leakage

M4	Leakage

M4 encompass a list of
“Top-N” strings seen at the root
that have not been delegated by ICANN
or put on the RFC6761 ”Special Use Names”

Candidate Metric Related to Resolver Misbehavior

M5	% of top 10k DNS resolvers interfering with end-user DNS traffic
M5 encompass 2 sub-metrics	
M5.1	% of top 10k resolvers giving falsified answers
M5.2	% of top 10k resolvers intercepting port 53

ITHI Protocol Parameters

Scoped to DNS Related Registries

Candidate Metric Related to DNS Usage

M6	DNS Usage
M6 encompass 3 sub-metrics	
M6.1	DNS Protocol Parameter Usage
	M6.1 encompass the list of parameters and their frequencies plus a list of unregistered parameters (and their frequencies).
M6.2	DNSsec signed zones
M6.3	TLS usage

Candidate Metric Related to DNS Usage

M6	DNS Usage
M6 encompass 3 sub-metrics	
M6.1	DNS Protocol Parameter Usage
	M6.1 encompass the list of parameters and their frequencies plus a list of unregistered parameters (and their frequencies).
M6.2	DNSsec signed zones
M6.3	TLS usage

We need help from DNS recursive server operators to collect data