Better routing security through concerted action

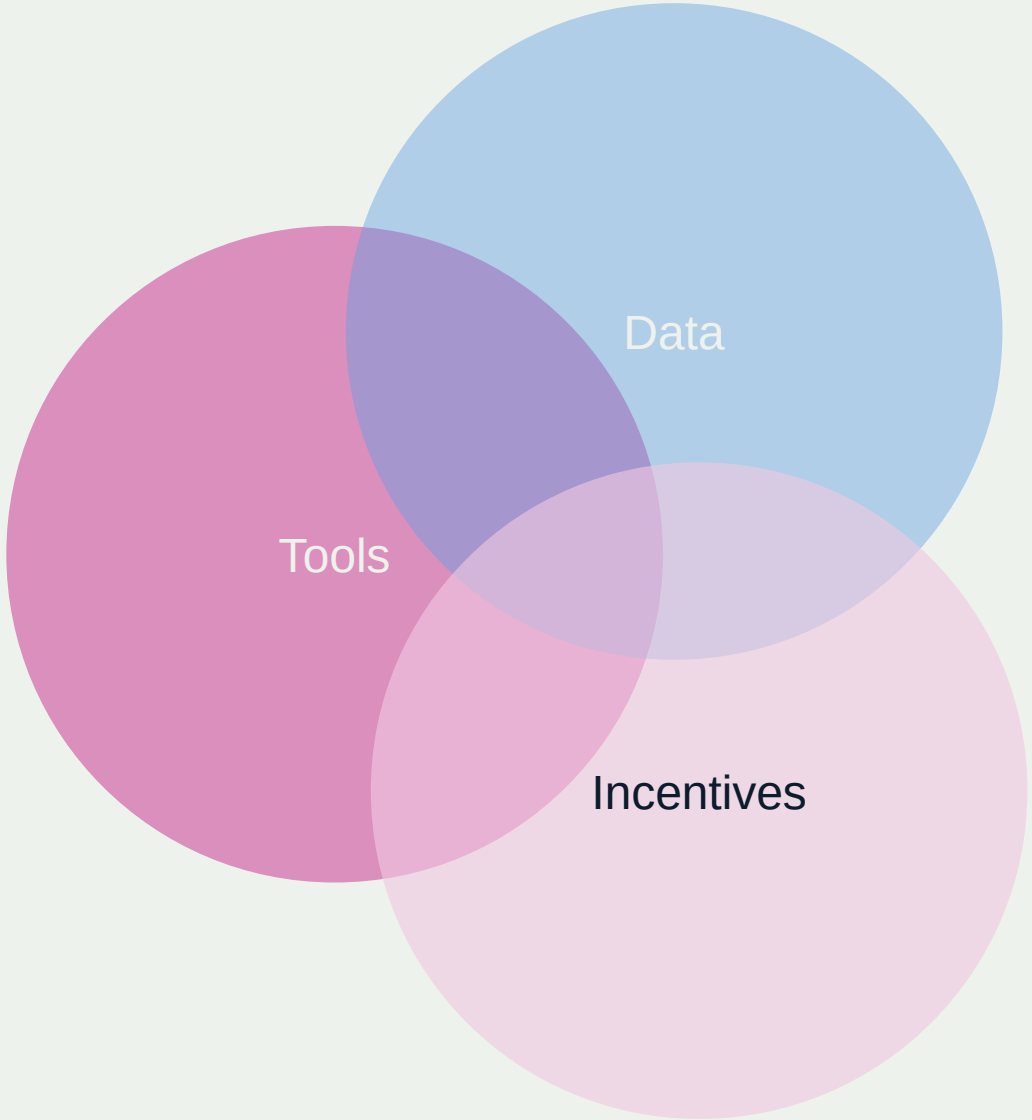
KISMET

Andrei Robachevsky

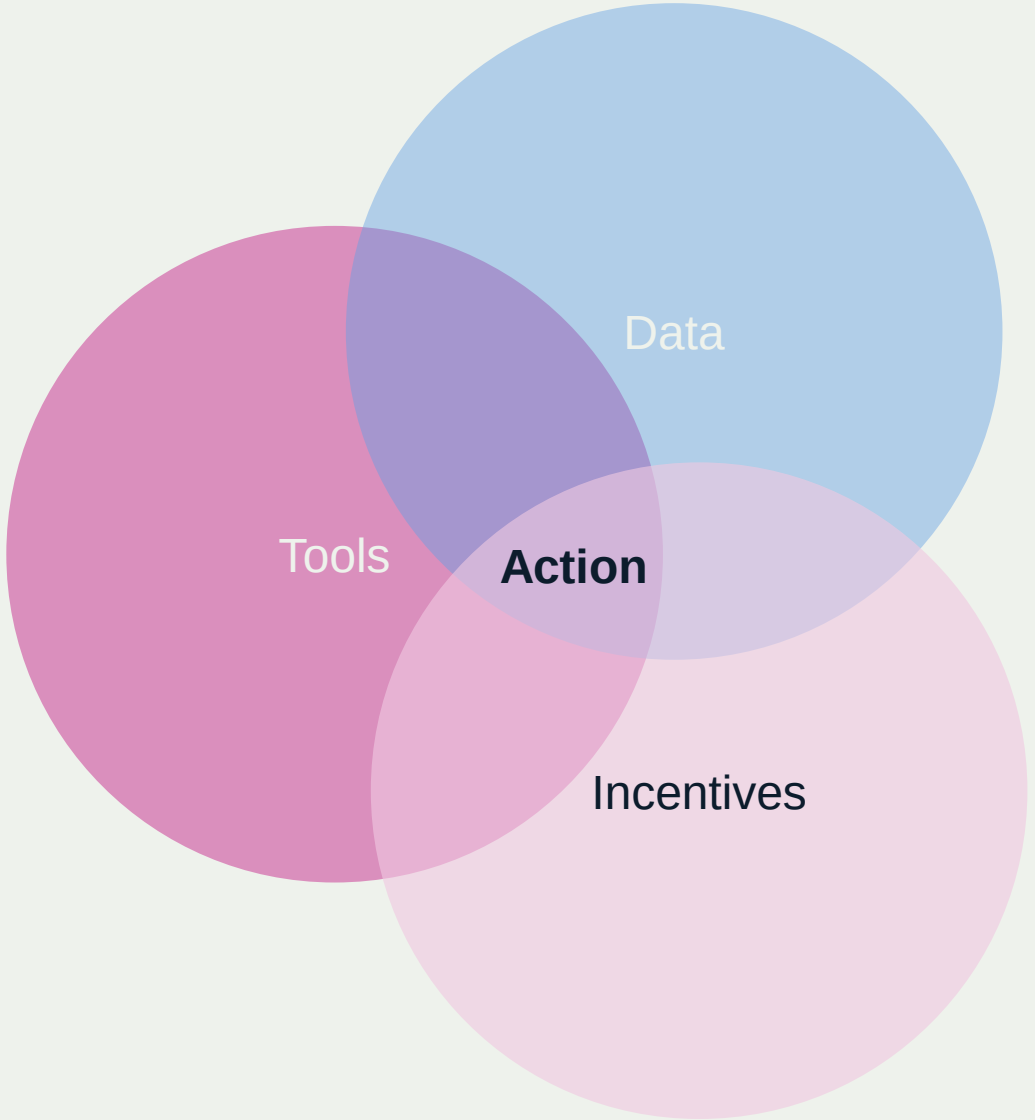
robachevsky@isoc.org

- Why MANRS
- Measuring MANRS
- Routing transparency

Routing security - Why is it so hard?



Routing security - Why is it so hard?



The playing field

- Each player can contribute to routing security
  - And be the cause of an incident
- Most of them would like to have a more secure routing system
  - Routing incidents are hard to debug and fix
- Most of them have little incentive
  - One’s network security is in the hands of others

We have a typical collective action problem

Two neighbours may agree to drain a meadow, which they possess in common; because it is easy for them to know each others mind; and each must perceive, that the immediate consequence of his failing in his part, is, the abandoning the whole project. But it is very difficult, and indeed impossible, that a thousand persons should agree in any such action; it being difficult for them to concert so complicated a design, and still more difficult for them to execute it; while each seeks a pretext to free himself of the trouble and expense, and would lay the whole burden on others.

[David Hume. A Treatise of Human Nature]

“[T]he commons […] is justifiable only under conditions of low-population density. As the human population has increased, the commons has had to be abandoned in one aspect after another”

[Garrett Hardin. The tragedy of the Commons]

Can this problem be solved without regulation?

Norms may provide a solution in such cases

- Need to agree on **values**. And **behaviors** that support these values

Common Value

- Resilient and secure global routing system

Behaviors

- Do not accept and propagate other’s mistakes (Validate what you accept from the neighbors)
- Protect your neighbors from your own mistakes (avoid policy violations)
  - Do not hijack
  - Do not leak
- Enable others to validate

From Behaviors to Norms

Widely accepted as a good practice

Not exactly a least common denominator, but not too high either

Visible and Measurable

Action – who can make an impact?

- Edge and access networks
- Transit providers
- IXPs
- CDNs and Cloud providers

Network operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

MANRS IXP Actions

Action 1

Prevent propagation of incorrect routing information

This mandatory action requires IXPs to implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).

Action 2

Promote MANRS to the IXP membership

IXPs joining MANRS are expected to provide encouragement or assistance for their members to implement MANRS actions.

Action 3

Protect the peering platform

This action requires that the IXP has a published policy of traffic not allowed on the peering fabric and performs filtering of such traffic.

Action 4

Facilitate global operational communication and coordination

The IXP facilitates communication among members by providing necessary mailing lists and member directories.

Action 5

Provide monitoring and debugging tools to the members.

The IXP provides a looking glass for its members.

MANRS for CDN&Cloud - a draft action set

Action 1
Prevent propagation of incorrect routing information

Egress filtering

Ingress filtering – non-transit peers, explicit whitelists

Action 2
Prevent traffic with illegitimate source IP addresses

Anti-spoofing controls to prevent packets with illegitimate source IP address

Action 3
Facilitate global operational communication and coordination

Contact information in PeeringDB

and relevant RIR databases

Action 4
Facilitate validation of routing information on a global scale

Publicly document ASNs and prefixes that are intended to be advertised to external parties.

Action 5
Encourage MANRS adoption

Actively encourage MANRS adoption among the peers

Action 6
Provide monitoring and debugging tools to peering partners

Provide monitoring tools to indicate incorrect announcements from peers that were filtered by the CDN&Cloud operator.

Users of the commons:

- those who always behave in a narrow, self-interested way and never cooperate (free-riders)
- those who are unwilling to cooperate with others unless assured that they will not be exploited by free- riders
- those who are willing to initiate reciprocal cooperation in the hopes that others will return their trust
- and perhaps a few genuine altruists who always try to achieve higher returns for a group

[Elinor Ostrom. Revisiting the Commons: Local Lessons, Global Challenges]

Mutually Agreed Norms for Routing Security

MANRS provides baseline recommendations in the form of Actions

- Distilled from common behaviors – BCPs, optimized for low cost and low risk of deployment
- With high potential of becoming norms

MANRS builds a visible community of security minded operators

- Social acceptance and peer pressure

MANRS

Why join MANRS?

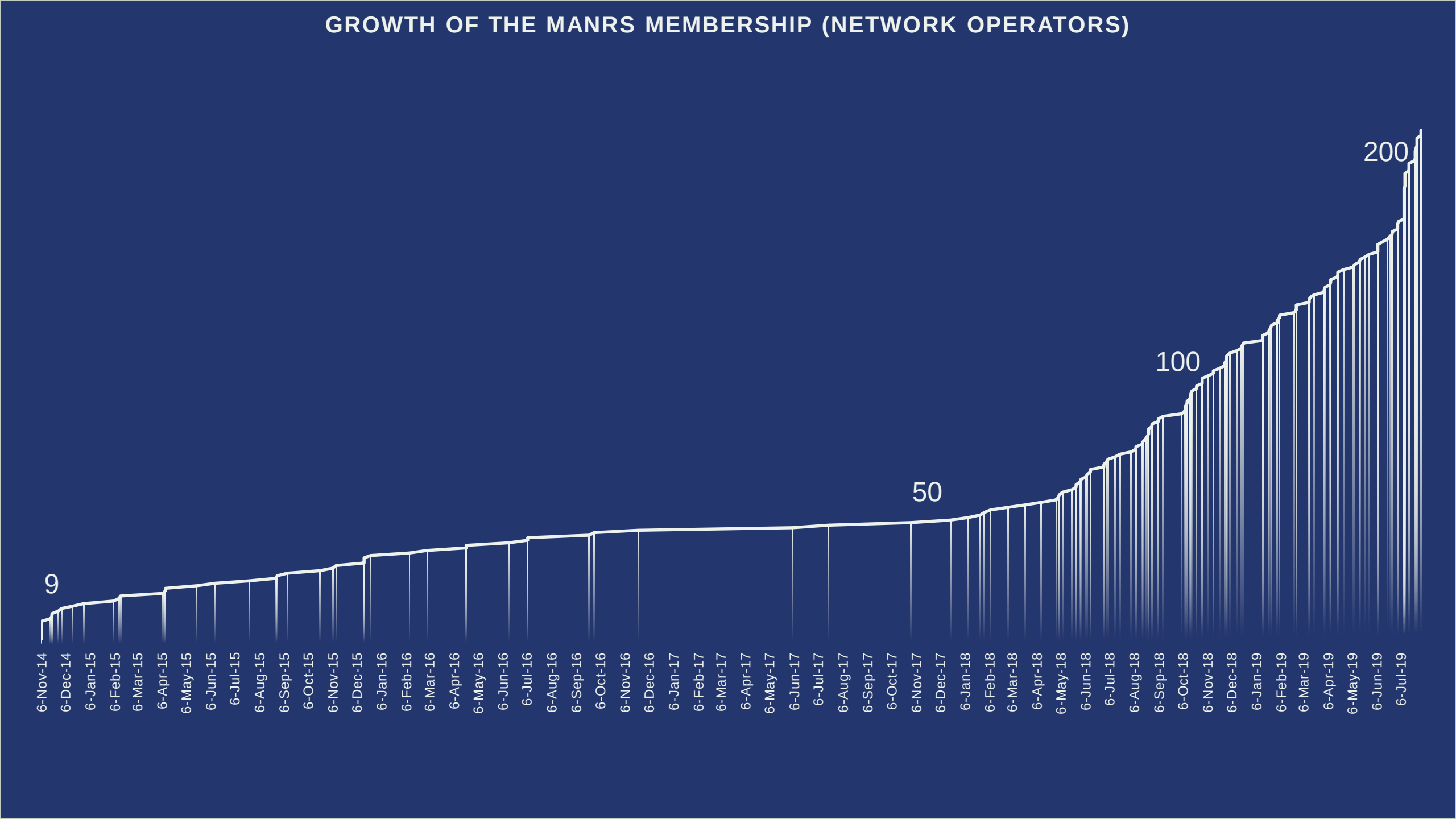
- **Improve your security posture and reduce the number and impact of routing incidents**
- Demonstrate that these practices are reality
- **Meet the expectations of the operators community**
- Join a community of security-minded operators working together to make the Internet better
- **Use MANRS as a competitive differentiator**

MANRS – is it getting traction?

240 ISPs

45 IXPs

GROWTH OF THE MANRS MEMBERSHIP (NETWORK OPERATORS)



Measuring MANRS

MANRS Observatory, https://observatory.manrs.org

Motivation

Inform MANRS members about their degree of commitment

- Improve reputation and transparency of the effort
- Facilitate continuous improvement and correction

Provide a factual state of routing security as it relates to MANRS

- Support the problem statement with data
- Demonstrate the impact and progress
- Network, country, region, over time

Improve robustness of the evaluation process

- Make it more comprehensive and consistent
- Reduce the load
- Allow preparation (self-assessment)

Data sources and caveats

Action	Measurement	Data source	Caveats
Filtering *M1, M1C, M2, M2C*	Route hijacks and leaks	BGPStream.com	False positives, obscure algorithms, vantage points
Filtering *M3, M3C, M4, M4C*	“Bogon” announcements	CIDR report	Limited vantage points
Anti-spoofing *M5*	Negative tests	CAIDA Spoofer	Sparse, active
Coordination *M8*	Registered contacts	RIRs Whois DBs	Stale/non-responsive contacts not detected
Global validation *M7IRR, M7RPKI, M7RPKIN*	Coverage of routing announcements	IRRs, RPKI	

How to calculate? E.g. M2 - route hijack by an AS?

Impact

- M2 = f(#pre… …dress span, duration, propagation)
- Not all prefixe…
- Type of the…

Conformity

- M2 = f(#distinct incidents, resolution time)
- # incidents and resolution time show the degree of negligence
- Incident is a sign of non-conformance

Events and incidents. E.g. M2C

Weight

- Events are weighted depending on the distance from the culprit
- M1C (ASPATH-1), 0.5*M1C(ASPATH-2), 0.25*M1C(ASPATH-3)… min 0.01
- **NB!:** Due to the challenge of correctly defining the customer cone (and area of responsibility) currently we only measure incidents in adjacent networks (next hop)

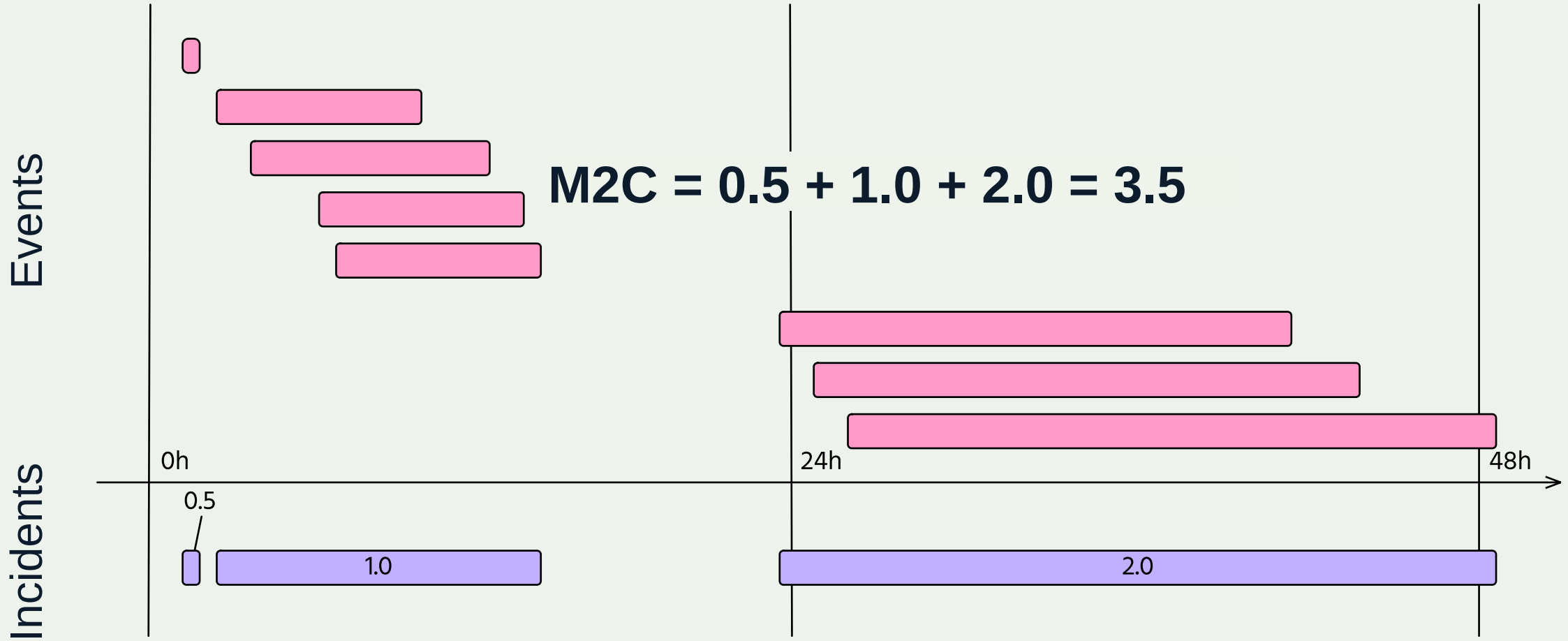
Incident

- Events with the **same weight** that share the **same time span** are merged into an **incident**.

Duration

- Non-action is penalized
  - < 30min = 0.5
  - < 24hour = 1
  - > 24hour =+1 for each subsequent 24-hour period

Filtering: Events and incidents



Metrics and normalization

Using normalization function – $f(x) = e^{-\alpha x^n}$

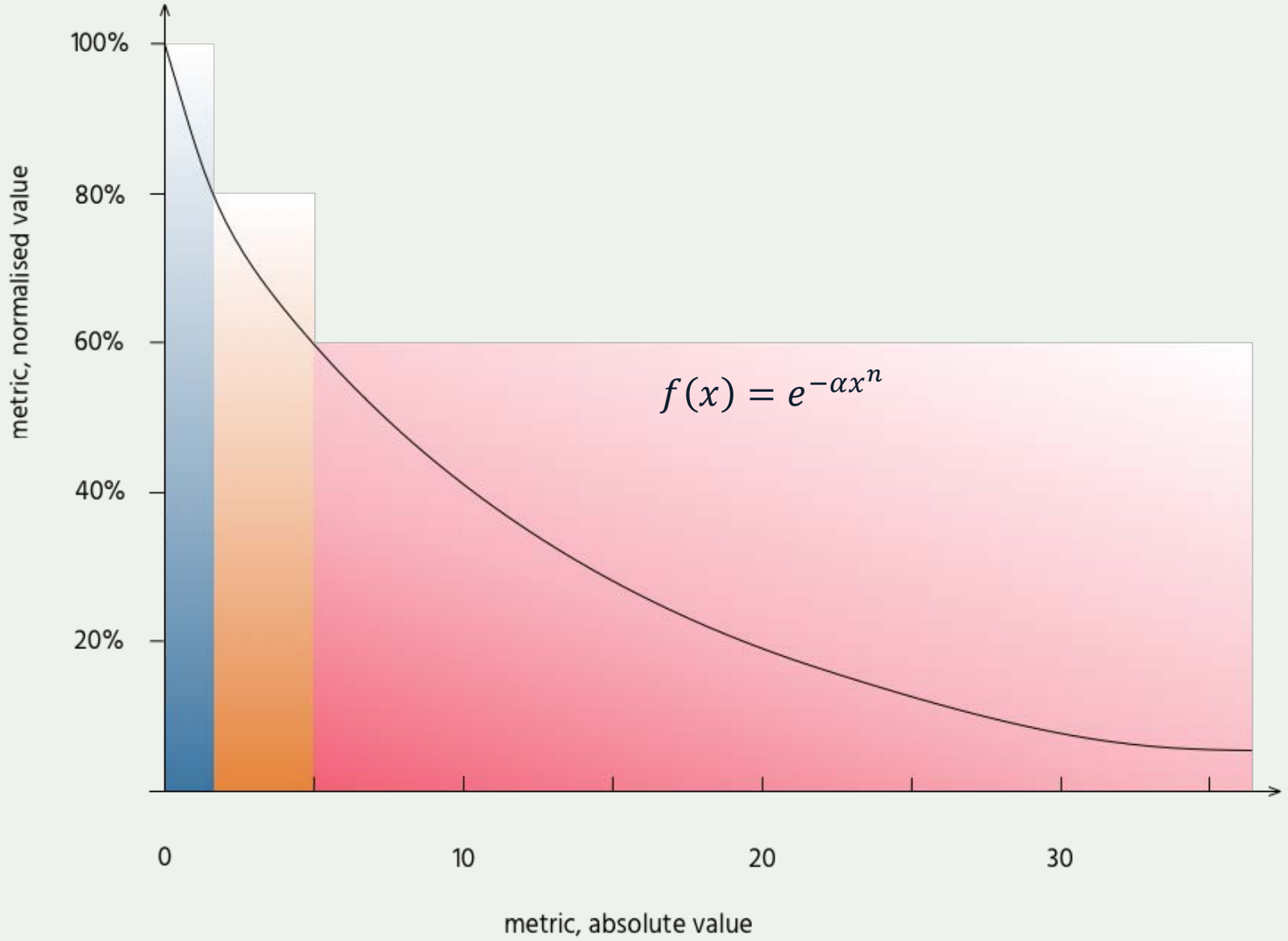
Using 2 interpolation points corresponding to 2 thresholds

(Lagging-Aspiring-Ready).

- E.g. Filtering

Ready	Aspiring	Lagging
≤1.5	1.5 ÷ 5	>5
≥90%	60 – 90%	<0.60%

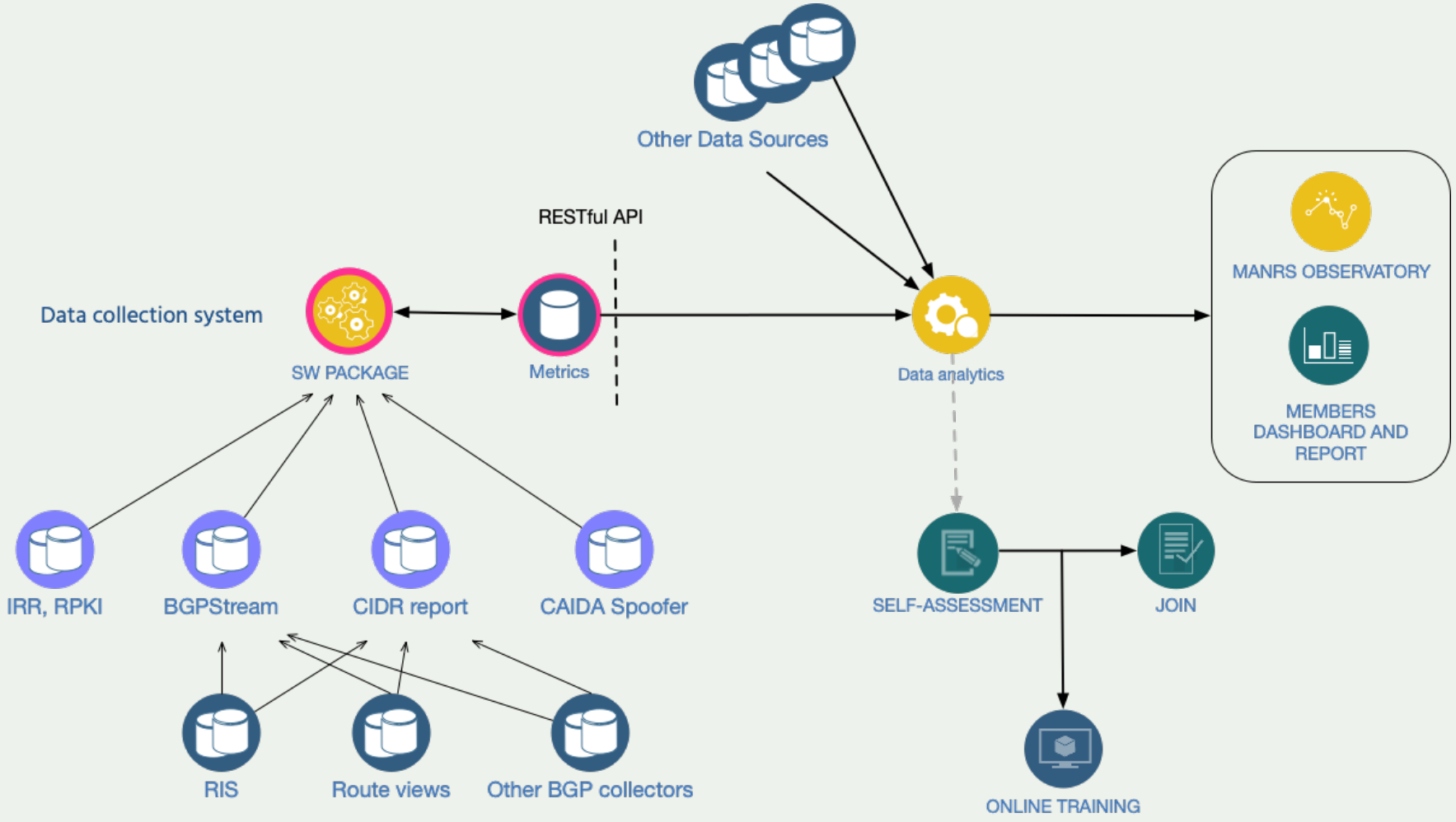
Metrics and normalization



Thresholds

Metric	Absolute			Normalized		
	Ready	Aspiring	Lagging	Ready	Aspiring	Lagging
Filtering	≤1.5	1.5 ÷ 5	>5	≥80%	60 – 80%	<60%
Anti-spoofing	0	0.5	≥1	>60%	60%	<60%
Coordination	0	-	1	100%	-	0%
Global Validation IRR	≤0.1	0.1 ÷ 0.5	>0.5	≥90%	50 – 90%	<50%
Global Validation RPKI	≤0.1	0.1 ÷ 0.5	>0.5	≥90%	50 – 90%	<50%

MANRS Observatory: How does it all fit together?

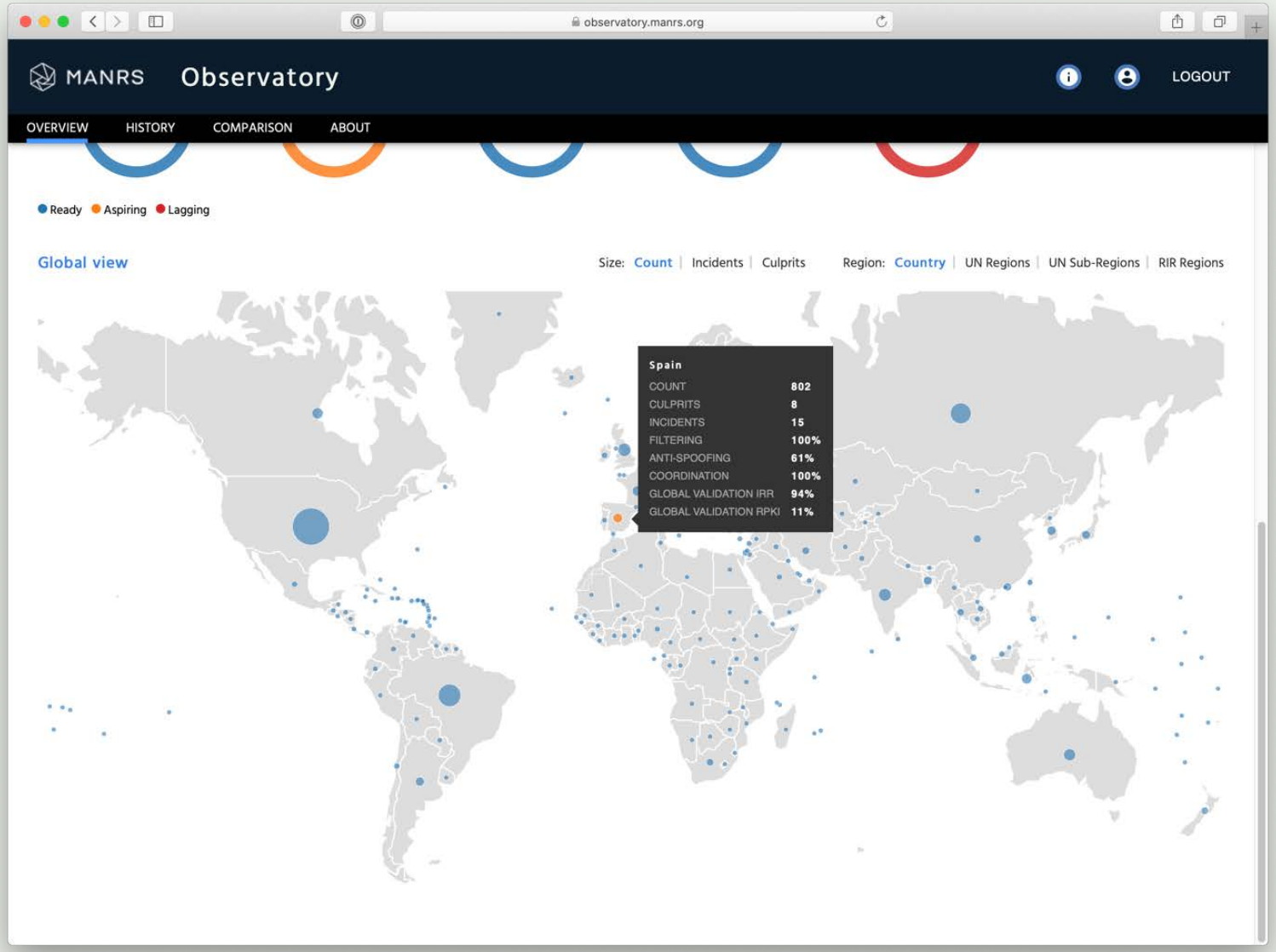


MANRS Observatory

Provides a factual state of routing security as it relates to MANRS

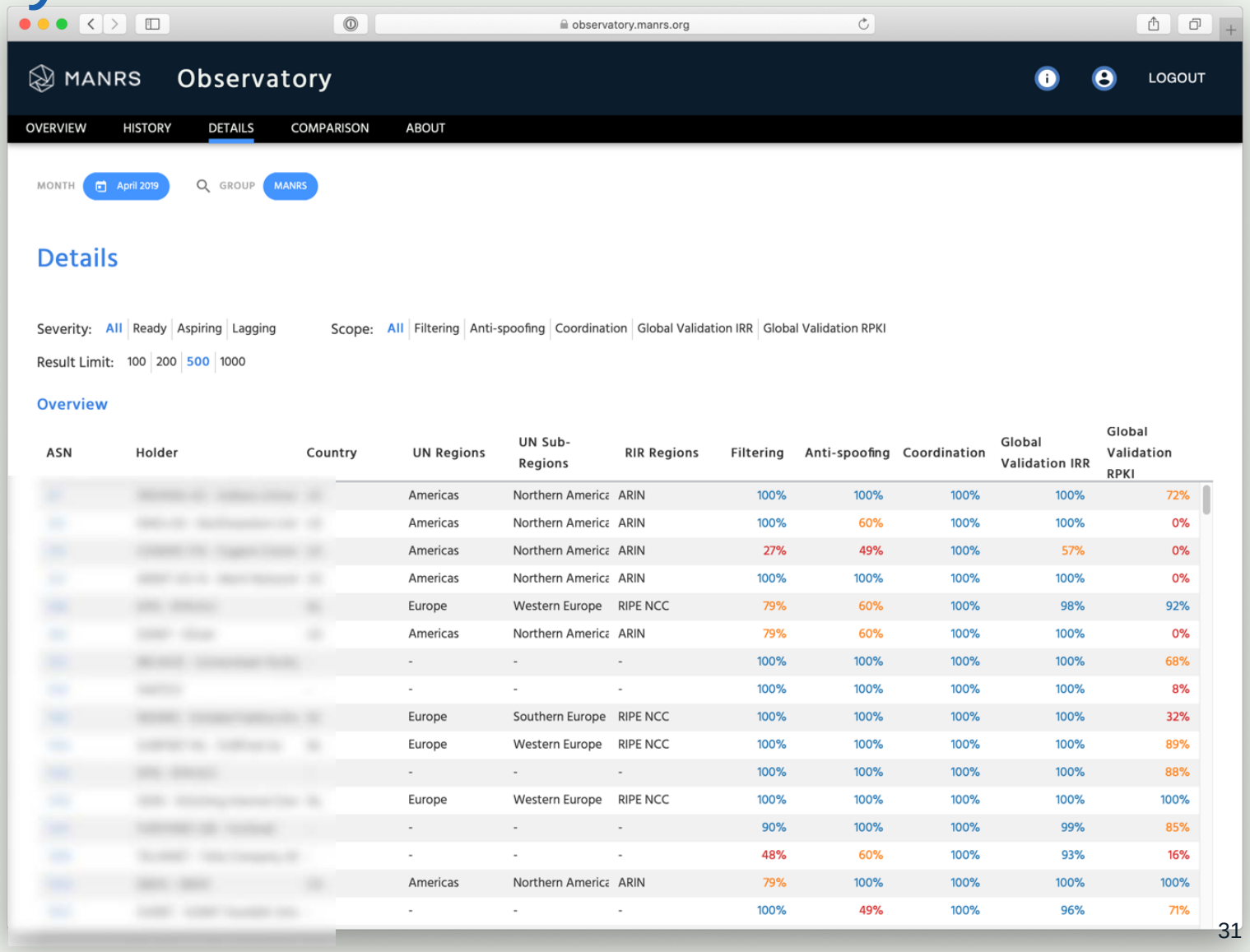
MANRS Observatory

Provides a factual state of routing security as it relates to MANRS



MANRS Observatory

Informs MANRS members about their degree of commitment



ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	100%	100%	100%	72%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	60%	100%	100%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	27%	49%	100%	57%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	100%	100%	100%	100%	0%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	79%	60%	100%	98%	92%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	79%	60%	100%	100%	0%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	68%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	8%
[redacted]	[redacted]	[redacted]	Europe	Southern Europe	RIPE NCC	100%	100%	100%	100%	32%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	89%
[redacted]	[redacted]	[redacted]	-	-	-	100%	100%	100%	100%	88%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	90%	100%	100%	99%	85%
[redacted]	[redacted]	[redacted]	-	-	-	48%	60%	100%	93%	16%
[redacted]	[redacted]	[redacted]	Americas	Northern America	ARIN	79%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	100%	49%	100%	96%	71%

Challenges

- Quality of data
- Sustainability of data
- Normalization

Routing transparency – a more general case

Is the Internet routing system transparent?

Yes, to a certain extent. Public route collectors (RIS, RouteViews, PCH) make a lot of data available

- Some portions of the Internet and some of the relationships are not visible as they are not being exposed to these route collectors

But making sense from these data is a heavy lift, available only to few

- BGP data is very noisy
- Analysis requires assumptions about relationships between operators and other heuristics

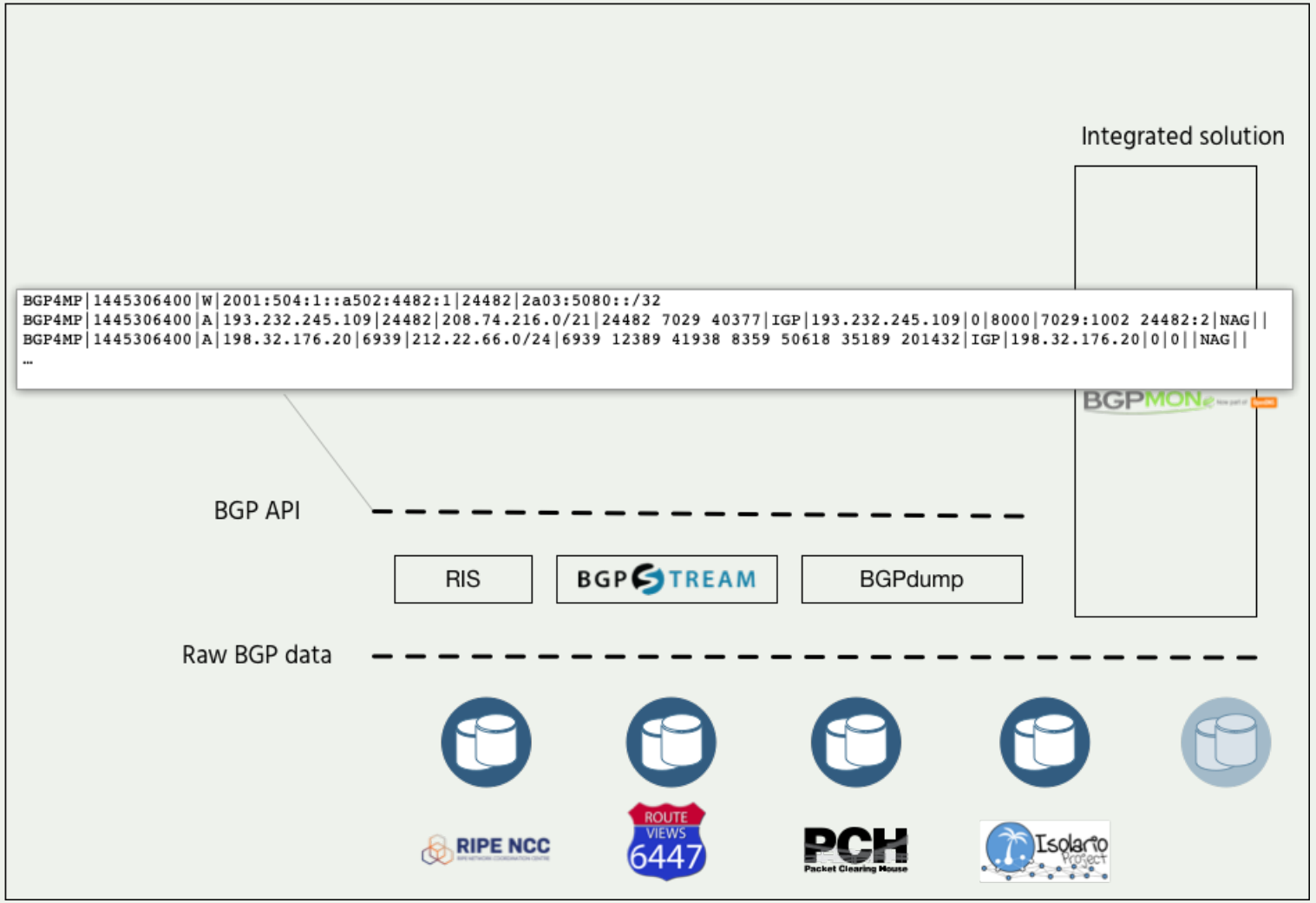
Why do we need more transparency?

The Bitcanal case:

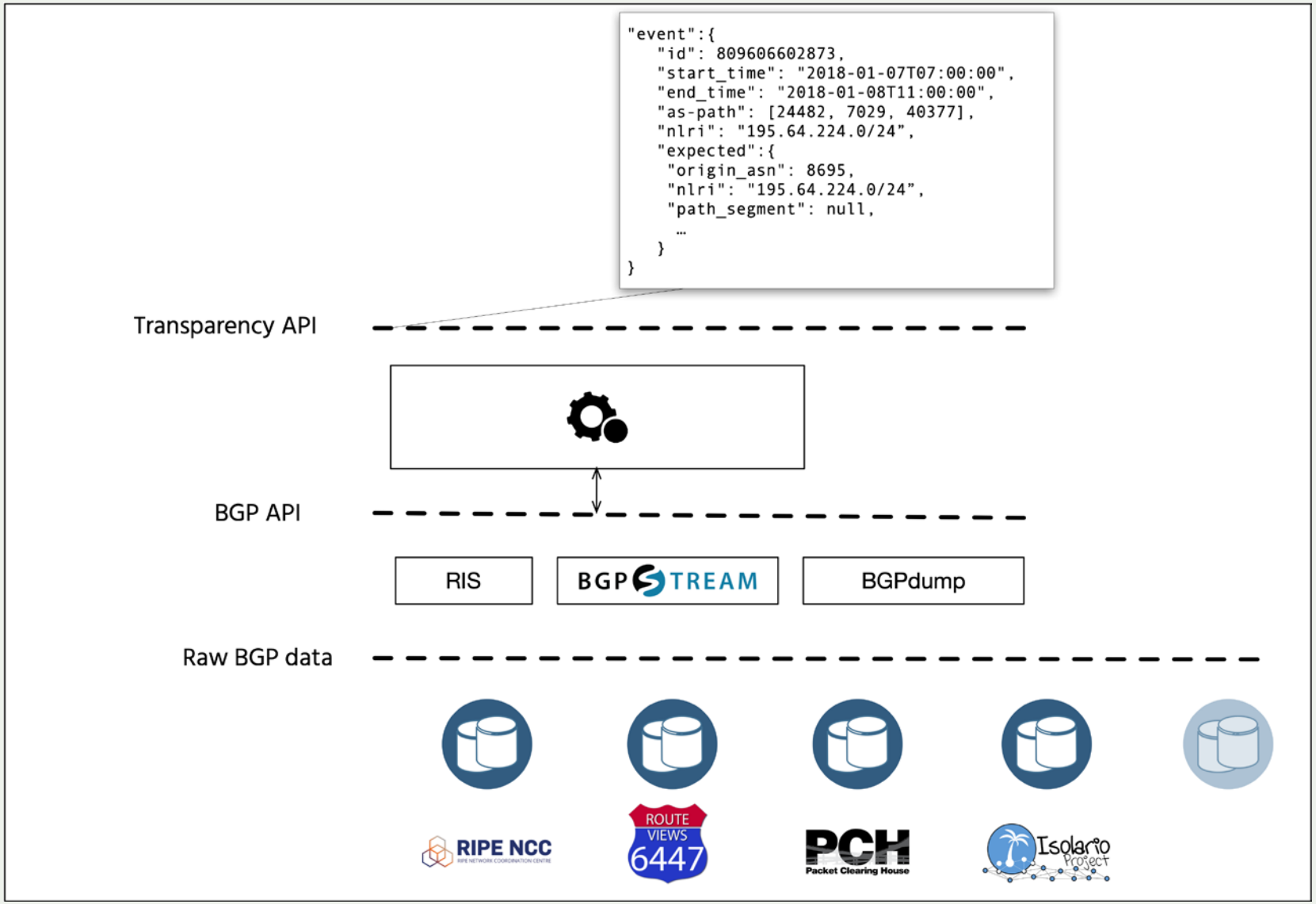
- "*As should be blatantly self-evident to pretty much everyone who has ever looked at any of the Internet's innumeriable prior incidents of very deliberately engineered IP space hijackings, all of the routes currently being announced by AS3266 (Bitcanal, Portugal) except for the ones in 213/8 are bloody obvious hijacks*." Ronald F. Guilmette, NANOG ML, June 2017.

Ability to see (and analyse) unusual/suspicious events that are happening in the Internet routing with many eyes will **more clearly** expose systematic abuse or gross negligence, allow to remedy anomalies **quicker**, and **better** inform research and discussions related to routing security with stable references.

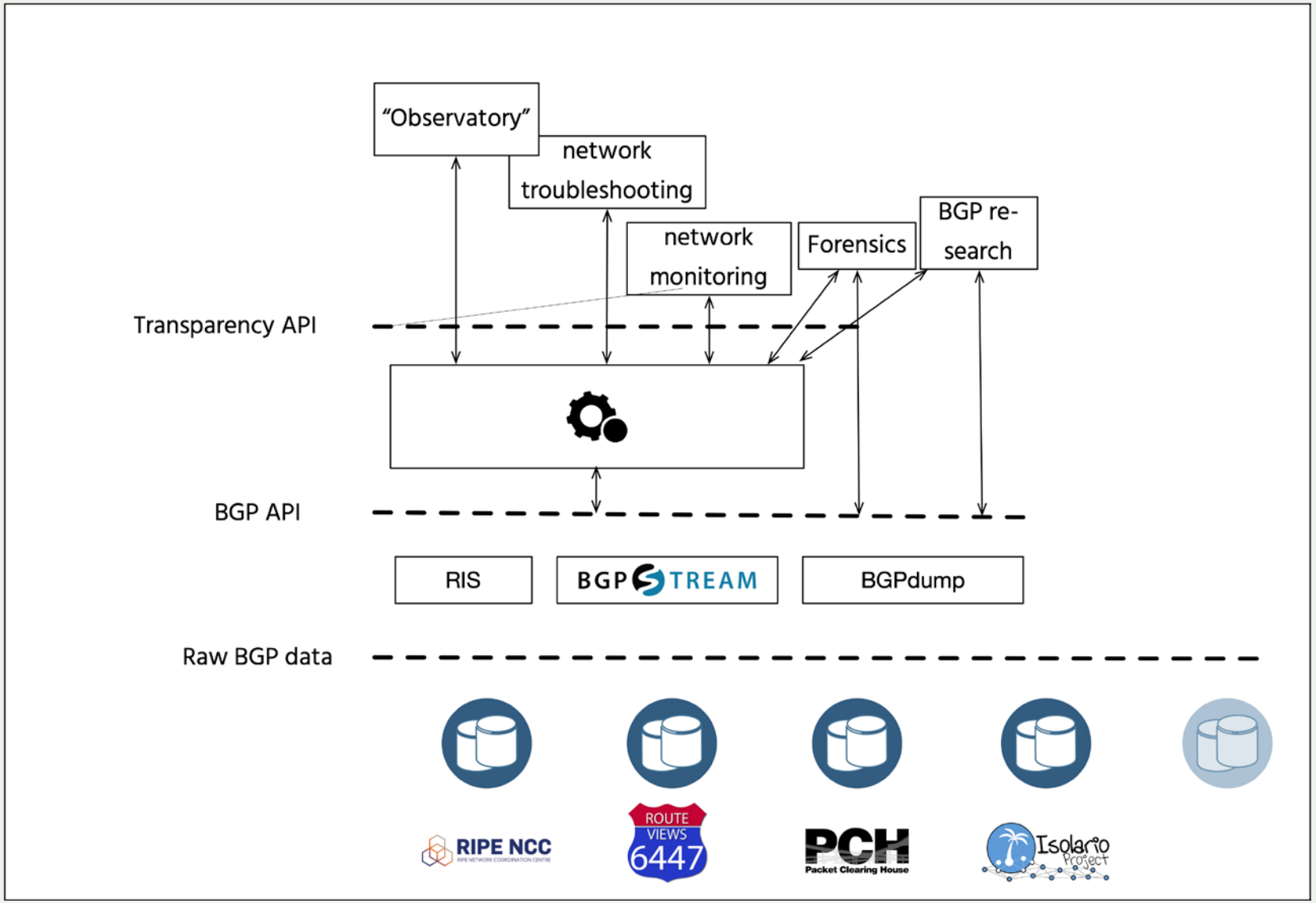
Conceptual view – current situation



Conceptual view – another common layer



Conceptual view – another common layer



What answers the service like this could offer?

Were there any unusual events related to a specific prefix over last year/month/week?

Were there any unusual events potentially affecting a specific network?

What were the unusual events (if any) related to a specific networks?

With what certainty can we assume that the unusual event is a routing attack, rather than a legitimate change?

The unusual event related to my network is a false positive, how can I report and fix this?

…. ?

What are the requirements?

Open. Should be provided as a free service to the community

Transparent. Heuristics and methodology should be open and subject to modifications

Community driven. Impartial and responsive to community needs. Also regarding methodology improvements

Questions?

https://www.manrs.org

Feedback: manrs@isoc.org