Improving routing security through concerted action

Workshop with the EC, September 27, 2021

Andrei Robachevsky

robachevsky@isoc.org

Why is routing security so hard?

- 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

Can this problem be solved without regulation?

Norms may provide a solution

- Need an agreement on **values**. And on **behaviors** that support these values

Common Value

- Resilient and secure global routing system

Behaviors

- Do not accept and propagate mistakes of others (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

The Solution: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to reduce the most common routing threats

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

- Demonstrated commitment to routing security
- Social acceptance and peer pressure

MANRS Programmes

Network Operators

Internet Exchange Points

Content Delivery Networks (CDNs) and Cloud Providers

Network Equipment Vendors

MANRS Network Operators Programme

Launched in 2014 by a handful of network operators with the following goals:

- Raise awareness of routing security problems and encourage the implementation of actions that can address them.
- Promote a culture of collective responsibility toward the security and resilience of the Internet's global routing system.
- Mobilize the Internet industry to address routing security problems.
- Provide a framework for network operators to better understand and address issues relating to the security and resilience of the Internet's global routing system.

Network operators – MANRS launch, November 2014

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 databases (RIR whois, IRR, PeeringDB)

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

MANRS IXP Programme

Internet Exchange Points (IXPs) are a collaborative focal point to discuss and promote the importance of routing security.

Launched in 2018, the IXP Programme addresses the unique needs and concerns of IXPs with a separate set of MANRS actions.

IXPs can implement actions that demonstrate their commitment to routing security and bring significant improvement to the resilience and security of the peering relationships.

MANRS IXP Program - launched in April 2018

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 CDN and Cloud Programme

Launched in 2020, the CDN and Cloud Provider Programme helps by requiring egress routing controls so networks can prevent incidents from happening.

Leveraging CDNs’ and cloud providers’ peering power can have significant positive spillover effect on the routing hygiene of networks they peer with.

Goals include:

- Create a secure network peering environment
- Encourage better routing hygiene from peering partners
- Demonstrate responsible behavior
- Improve operational efficiency for peering interconnections, minimizing incidents and providing more granular insight for troubleshooting

MANRS for CDN&Cloud – March 31, 2020

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.

MANRS for equipment vendors

Benefits for vendors

- MANRS can help articulate a common core security features
- MANRS can help to signal the level of security awareness
- MANRS can improve collaboration between vendors and network operators

Benefits for MANRS

- Make adoption of MANRS easier for network operators
- Leverage vendors’ outreach and training programs to promote MANRS

Areas of impact

Technical

- A core feature set necessary for implementing MANRS

Training

- Inclusion of MANRS in training programs

Promotion

- Provide “space” for MANRS at e.g. customer events

Advisory

- Implementation advise and improved documentation

Development

- Collaborate in developing solutions to routing (security) problems

MANRS for Equipment Vendors – September 16, 2021

Action 1

Provide Solutions

4 Scenarios corresponding to technical actions in other programs

Action 2

Promote

Promote MANRS through training and technical content

Ongoing Activities

Advisory

Development

Contribution

Promotion

Increasing adoption

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 operator community**
- Join a community of security-minded operators working together to make the Internet better
- **Use MANRS as a competitive differentiator**

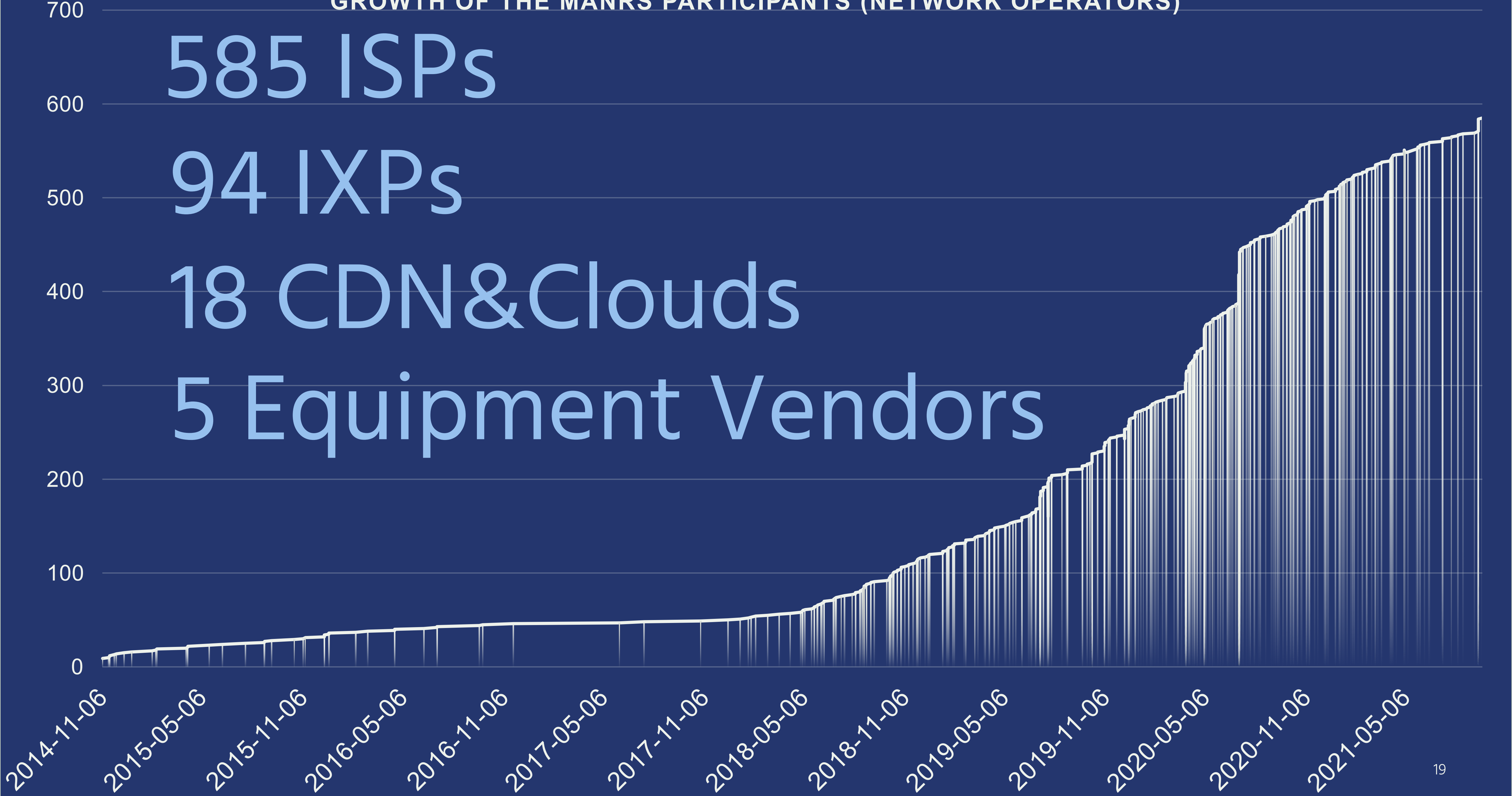
GROWTH OF THE MANRS PARTICIPANTS (NETWORK OPERATORS)

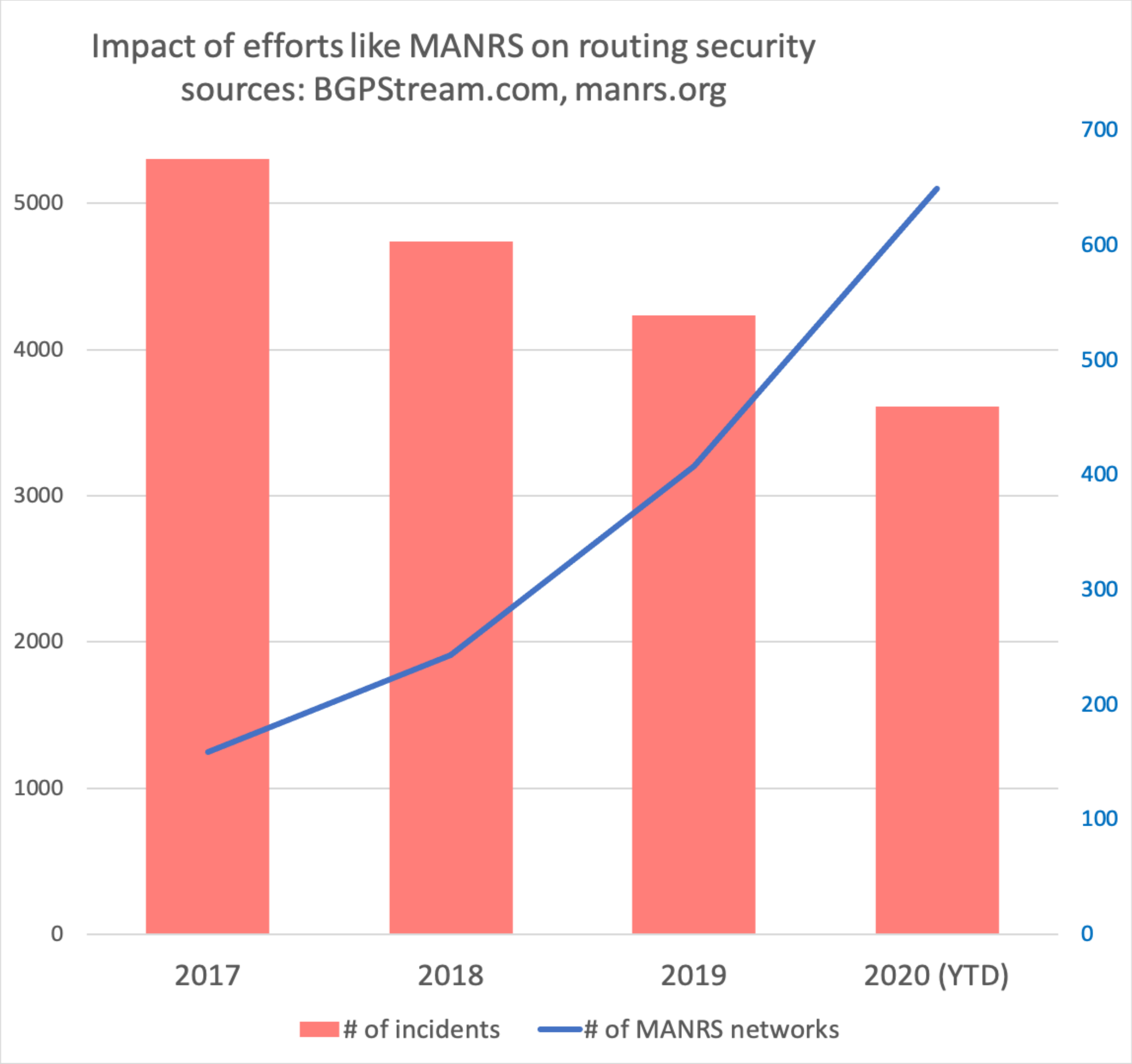
585 ISPs

94 IXPs

18 CDN&Clouds

5 Equipment Vendors




Impact of efforts like MANRS on routing security
sources: BGPStream.com, manrs.org
5000
4000
3000
2000
1000
0
700
600
500
400
300
200
100
0
2017
2018
2019
2020 (YTD)
🟥 # of incidents
# of MANRS networks

MANRS Observatory

https://observatory.manrs.org/

MANRS Observatory

Provide a factual state of MANRS readiness and track it over time

Measurements are:

- Transparent – using publicly accessible data
- Passive – no cooperation from networks required
- Evolving – MANRS community decide what gets measured and how

MANRS Observatory Access

Publicly launched in August 2019

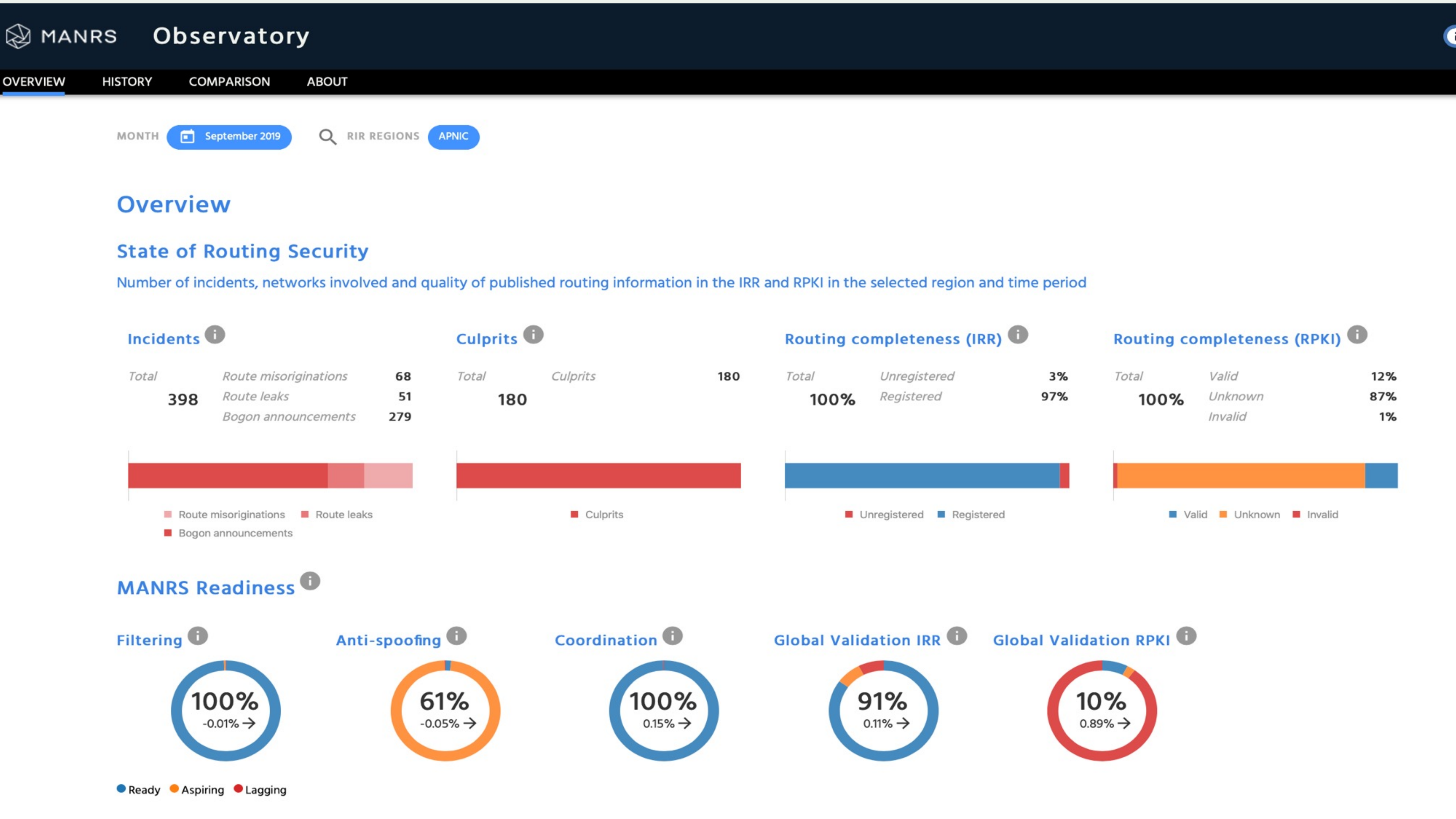
Uses trusted, publicly available third-party data

Anyone may view aggregated data

Only MANRS Participants have access to detailed data about their own network

Caveats:

- There are still some false positives
- Lack of security controls is not always visible



MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH September 2019 RIR REGIONS APNIC

Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
398	*Route misoriginations*	68
	Route leaks	51
	Bogon announcements	279

■ Route misoriginations ■ Route leaks ■ Bogon announcements

Culprits

Total		
180	*Culprits*	180

■ Culprits

Routing completeness (IRR)

Total		
100%	*Unregistered*	3%
	Registered	97%

■ Unregistered ■ Registered

Routing completeness (RPKI)

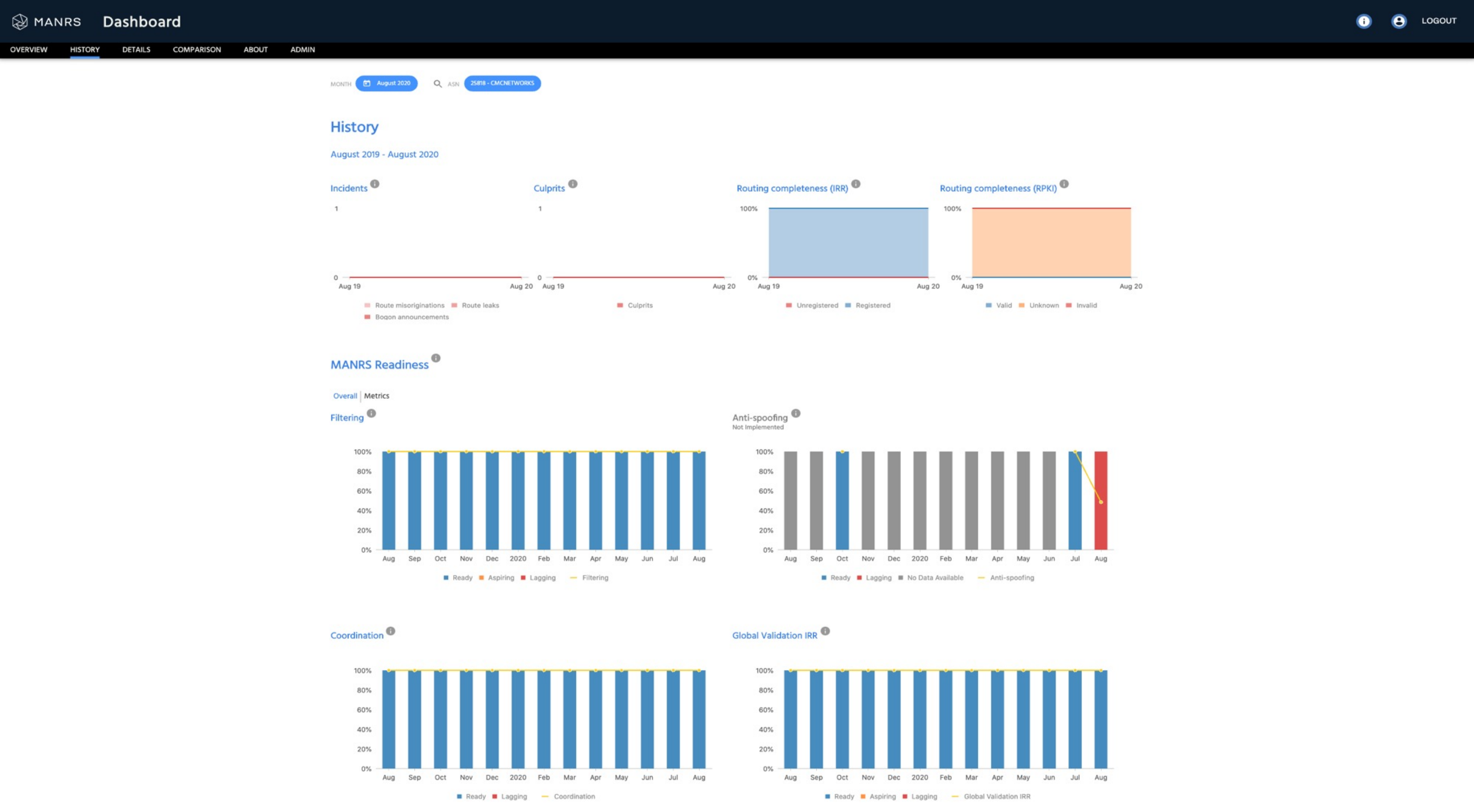
Total		
100%	*Valid*	12%
	Unknown	87%
	Invalid	1%

■ Valid ■ Unknown ■ Invalid

MANRS Readiness

Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
100% -0.01% →	61% -0.05% →	100% 0.15% →	91% 0.11% →	10% 0.89% →

● Ready ● Aspiring ● Lagging



MONTH August 2020 ASN 25818 - CMCNETWORKS

History

August 2019 - August 2020

Incidents

Culprits

Routing completeness (IRR)

Routing completeness (RPKI)

MANRS Readiness

Overall | Metrics

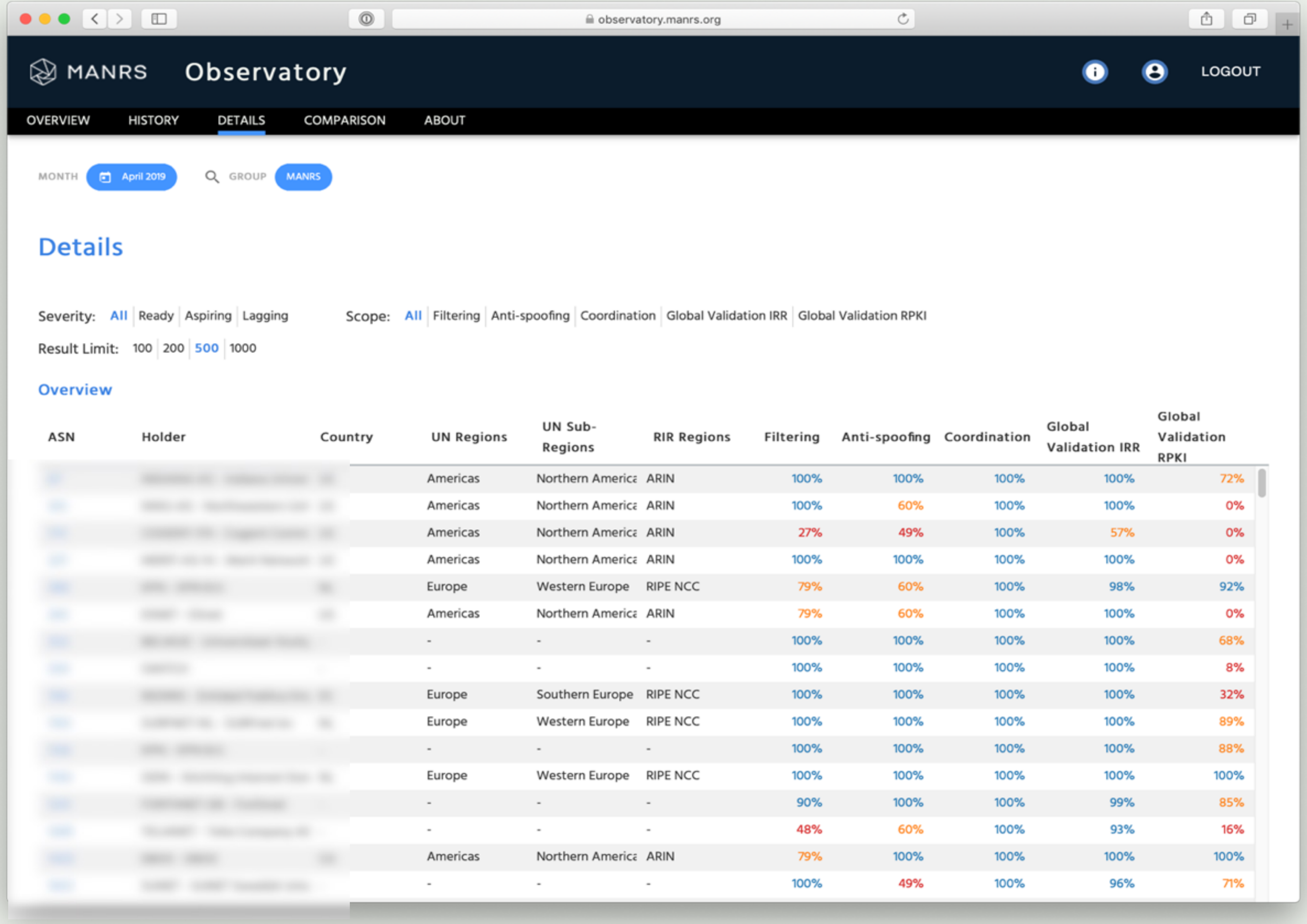
Filtering

Anti-spoofing

Not Implemented

Coordination

Global Validation IRR



MONTH April 2019 GROUP MANRS

Details

Severity: All | Ready | Aspiring | Lagging

Scope: All | Filtering | Anti-spoofing | Coordination | Global Validation IRR | Global Validation RPKI

Result Limit: 100 | 200 | 500 | 1000

Overview

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 Americ	ARIN	100%	100%	100%	100%	72%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	100%	60%	100%	100%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	27%	49%	100%	57%	0%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	ARIN	100%	100%	100%	100%	0%
[redacted]	[redacted]	[redacted]	Europe	Western Europe	RIPE NCC	79%	60%	100%	98%	92%
[redacted]	[redacted]	[redacted]	Americas	Northern Americ	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 Americ	ARIN	79%	100%	100%	100%	100%
[redacted]	[redacted]	[redacted]	-	-	-	100%	49%	100%	96%	71%

LEARN MORE:

https://www.manrs.org

FOLLOW US:

/RoutingMANRS

Thank you.

manrs@isoc.org

manrs.org