13 October 2021
ENISA Telecom Security Forum

The MANRS Project

Routing Security for the Internet

Internet Society

Kevin Meynell
Senior Manager, Technical & Operational Engagement
meynell@isoc.org

What is Routing and why is it needed?

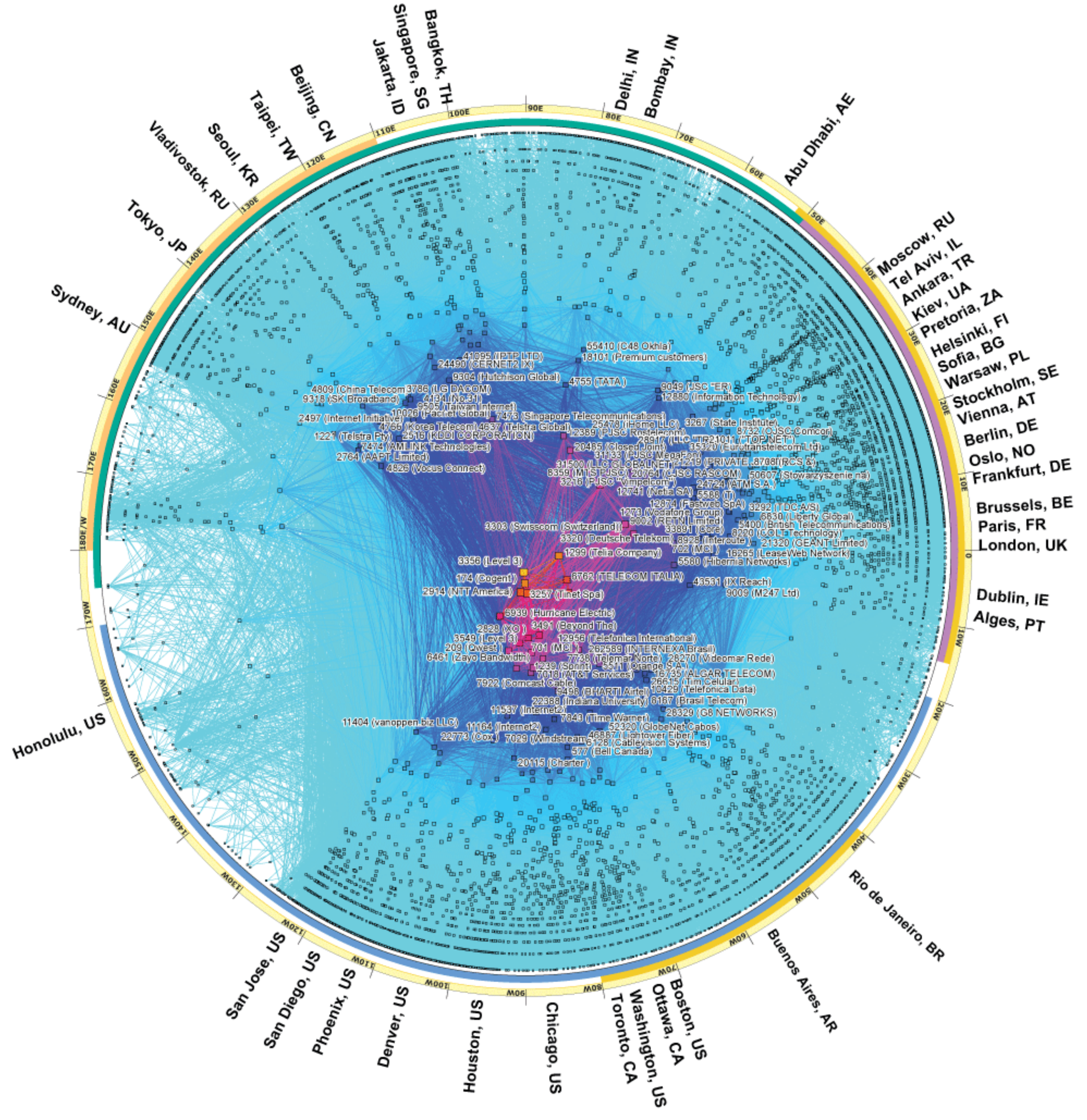
- The Internet is actually a global system of interconnected computer networks using the **TCP/IP protocols**
- **Routing** is needed to get packets from one destination to another (unless on the same subnet)
- **Routers** (aka gateways) are specialised computing devices that discover other connected networks and forward packets to them
- Each network is connected to the rest of Internet with a router
- Packets are forwarded by routers to other routers or final destination, based on IP addresses (usually blocks of IP addresses known as **prefixes**)
- Routers use **Border Gateway Protocol (BGP)** to exchange "reachability information" - networks they know how to reach
- Routers build a routing table (i.e. "road map") to pick the best route when sending a packet

Global Routing System Overview

(as of 12 October 2021)

72,315 networks known as Autonomous Systems connected to Internet, each using a unique Autonomous System Number (ASN) for identification

897,845 advertised IP prefixes (routes)



MANRS

https://www.caida.org/

The Routing Problem

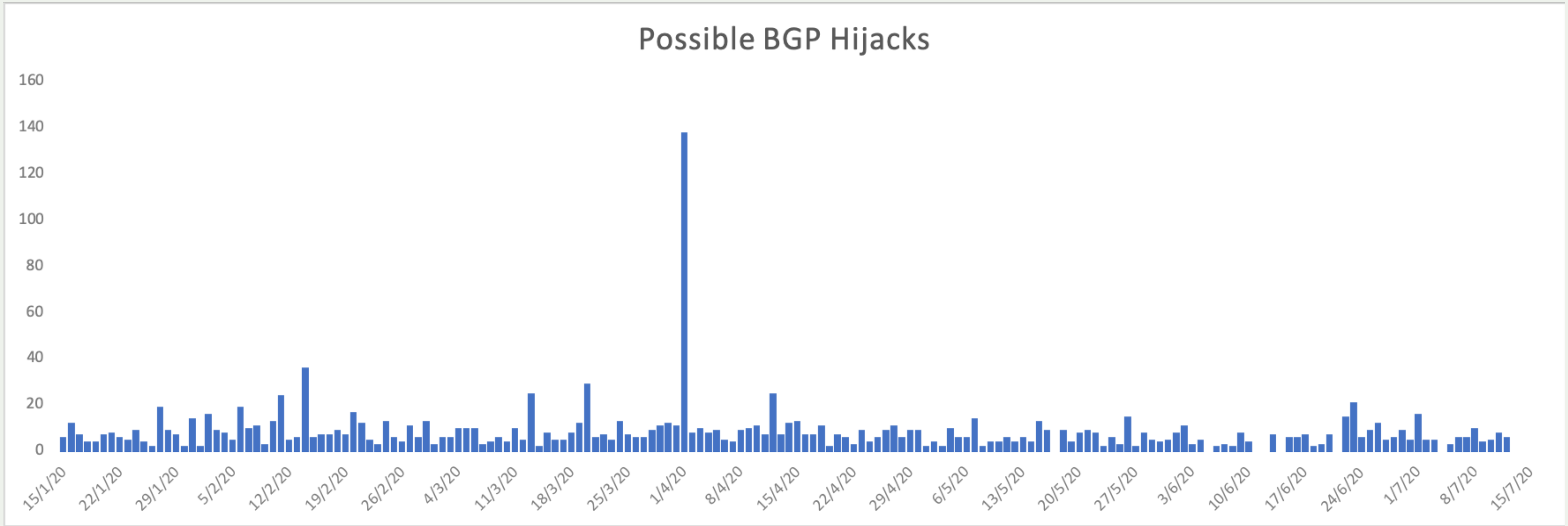
The Border Gateway Protocol (BGP) used by the Internet routing system is based entirely on *unverified trust* between networks

- No built-in validation that updates are legitimate
- Any network can announce any ASN or IP prefix
- Any network can claim to be another network

Routing Incidents Cause Real World Problems

Event	Explanation	Repercussions	Example
Route Leak	A network operator with multiple upstream providers announces to one upstream provider that is has a route to a destination through the other upstream provider. Often due to accidental misconfiguration.	Can be used for a MITM, including traffic inspection, modification and reconnaissance.	*June 2019. Verizon accepted incorrect routes from DQE Communications that diverted traffic destined for Cloudflare, Facebook & Amazon.*
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place and can cause Denial of Service (DoS) attacks or traffic interception.	*The 2008 YouTube hijack* *April 2018 Amazon Route 53 hijack*
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	*March 1, 2018. Memcached 1.3Tb/s reflection-amplification attack reported by Akamai*

The routing system is constantly under attack – incidents every day



http://bgpstream.com/

Introduction to MANRS

Provides well-defined actions to eliminate the most common threats in the global routing system

Brings together established industry best practices

Based on collaboration among participants and shared responsibility for the Internet infrastructure

4 no-cost programmes for Network Operators, IXPs, CDN/Cloud Providers & Vendors

MANRS Actions – Network Operators Programme

Launched November 2014. Actions 1, 3 and 4 are mandatory. Action 2 is optional.

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 relevant RIR database and/or PeeringDB

Global Validation

Facilitate validation of routing information on a global scale

Publish your routing data, so others can validate

Registering number resources in an IRR and/or creating ROAs for them

MANRS Actions – IXP Programme

Launched April 2018. Actions 1 and 2 are mandatory, plus at least one additional action is required.

Action 1

Prevent propagation of incorrect routing information

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 should provide encouragement or assistance for their members to implement the MANRS actions

Action 3

Protect the peering platform

IXPs should have 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

IXPs should facilitate communication amongst 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 Actions - CDN & Cloud Programme

- Was launched on 1 April 2020 to complement existing Network Operators and IXP programme.
- Principles developed by large industry players including Akamai, Azion, Cloudflare, Comcast, Facebook, Google, Microsoft, Nexica Oracle, Redder, Telefonica, TORIX, Verisign.
- Conformance with Actions 1-5 is mandatory. Action 6 is optional.

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 communicatio n and coordination

Contact information in relevant RIR database and/or PeeringDB

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 tools to indicate incorrect announcements from peers filtered by CDN

The MANRS Observatory

Checking Conformance

MANRS

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

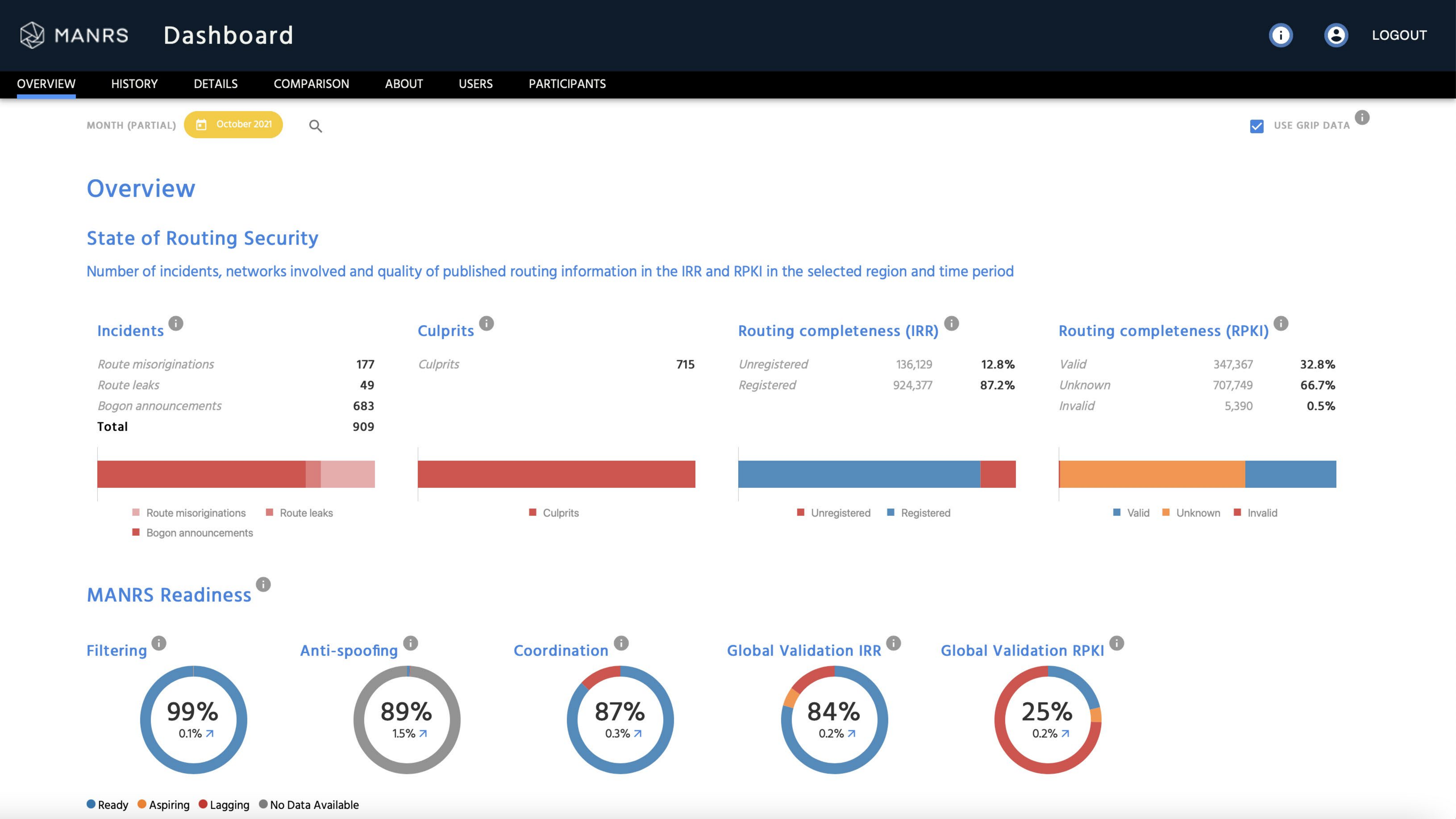
Tool to impartially benchmark ASes to improve reputation and transparency

Provide factual state of security and resilience of Internet routing system over time

Allow MANRS participants to easily check for conformancy

Collates publicly available data sources

- BGPStream / CAIDA GRIP
- CIDR Report
- CAIDA Spoofer Database
- RIPE Database / RIPE Stats
- PeeringDB
- IRRs
- RPKI Validator



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

Route misoriginations	177
Route leaks	49
Bogon announcements	683
Total	909

Culprits

Culprits	715

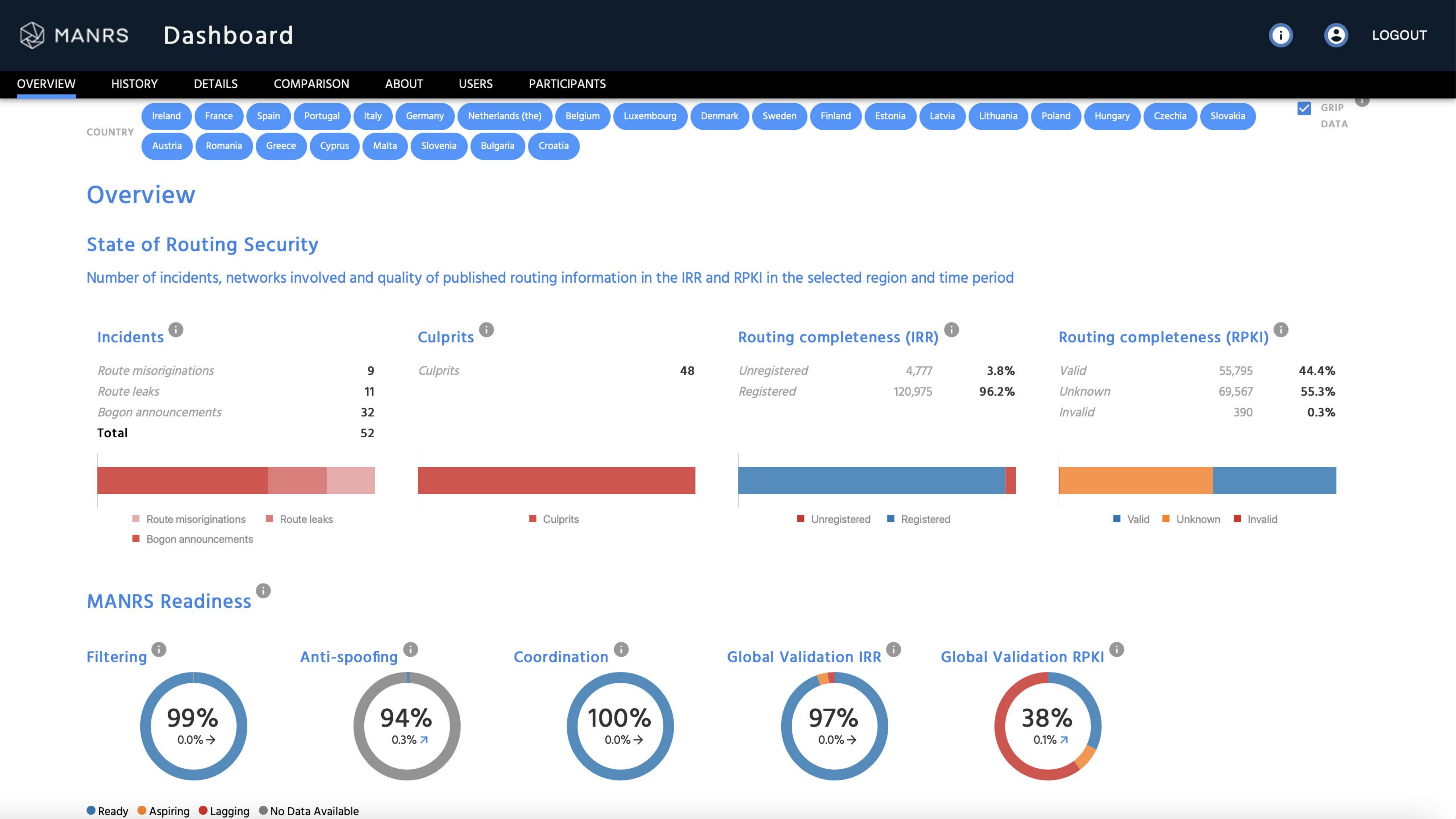
Routing completeness (IRR)

Unregistered	136,129	**12.8%**
Registered	924,377	**87.2%**

Routing completeness (RPKI)

Valid	347,367	**32.8%**
Unknown	707,749	**66.7%**
Invalid	5,390	**0.5%**

MANRS Readiness



MANRS Dashboard

LOGOUT

OVERVIEW HISTORY DETAILS COMPARISON ABOUT USERS PARTICIPANTS

COUNTRY: Ireland, France, Spain, Portugal, Italy, Germany, Netherlands (the), Belgium, Luxembourg, Denmark, Sweden, Finland, Estonia, Latvia, Lithuania, Poland, Hungary, Czechia, Slovakia, Austria, Romania, Greece, Cyprus, Malta, Slovenia, Bulgaria, Croatia

☑ GRIP DATA

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

Route misoriginations	9
Route leaks	11
Bogon announcements	32
Total	52

Culprits

Culprits	48

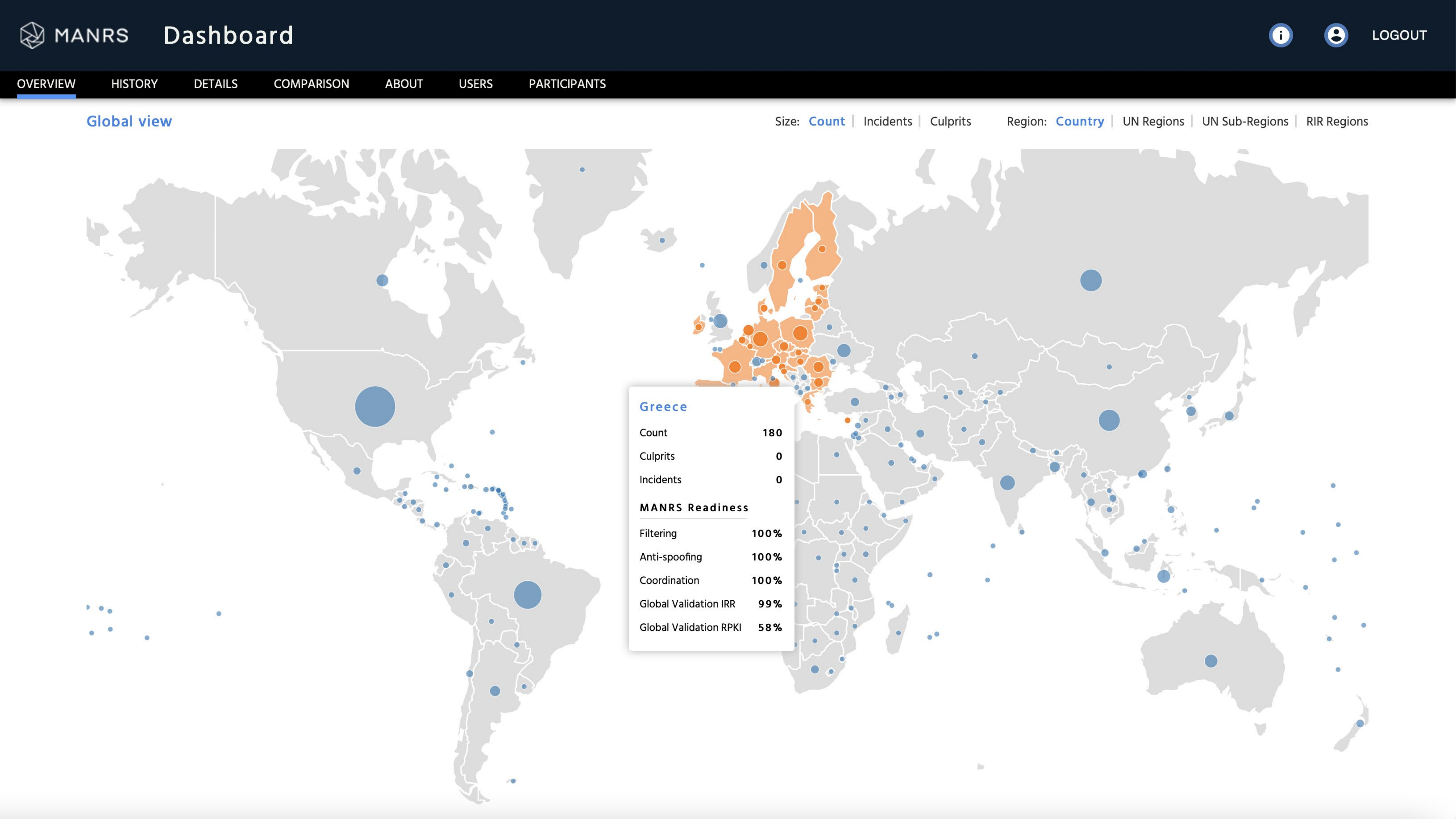
Routing completeness (IRR)

Unregistered	4,777	**3.8%**
Registered	120,975	**96.2%**

Routing completeness (RPKI)

Valid	55,795	**44.4%**
Unknown	69,567	**55.3%**
Invalid	390	**0.3%**

MANRS Readiness


MANRS
Dashboard
LOGOUT
OVERVIEW
HISTORY
DETAILS
COMPARISON
ABOUT
USERS
PARTICIPANTS
Size: Count | Incidents | Culprits
Region: Country | UN Regions | UN Sub-Regions | RIR Regions

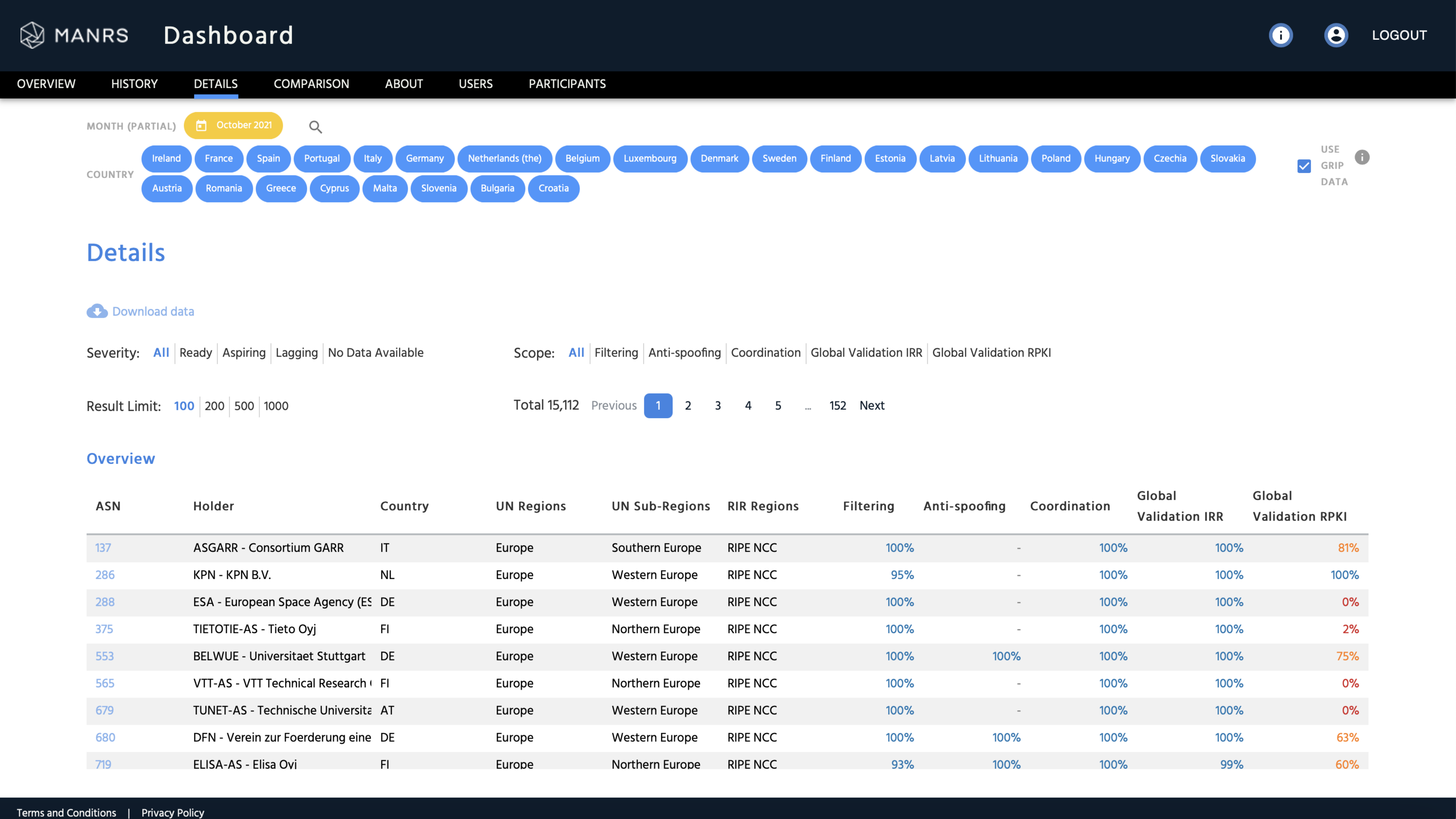
Global view

Greece

Count	180
Culprits	0
Incidents	0

MANRS Readiness

Filtering	100%
Anti-spoofing	100%
Coordination	100%
Global Validation IRR	99%
Global Validation RPKI	58%



MANRS Dashboard

MONTH (PARTIAL) October 2021

COUNTRY Ireland France Spain Portugal Italy Germany Netherlands (the) Belgium Luxembourg Denmark Sweden Finland Estonia Latvia Lithuania Poland Hungary Czechia Slovakia Austria Romania Greece Cyprus Malta Slovenia Bulgaria Croatia

☑ USE GRIP DATA

Details

Download data

Severity: All | Ready | Aspiring | Lagging | No Data Available

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

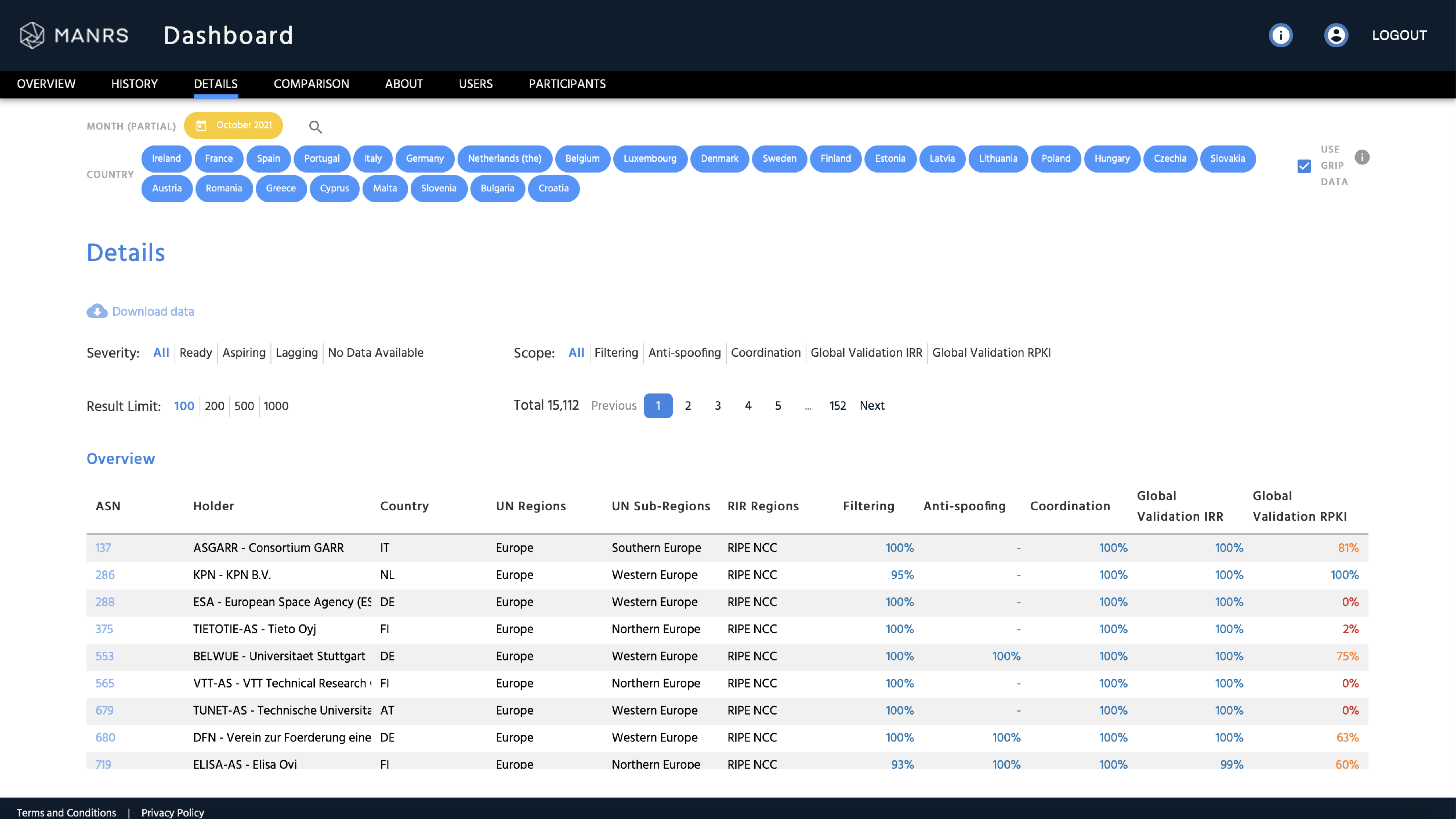
Result Limit: 100 | 200 | 500 | 1000

Total 15,112 Previous 1 2 3 4 5 ... 152 Next

Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
137	ASGARR - Consortium GARR	IT	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	81%
286	KPN - KPN B.V.	NL	Europe	Western Europe	RIPE NCC	95%	-	100%	100%	100%
288	ESA - European Space Agency (ES	DE	Europe	Western Europe	RIPE NCC	100%	-	100%	100%	0%
375	TIETOTIE-AS - Tieto Oyj	FI	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	2%
553	BELWUE - Universitaet Stuttgart	DE	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	75%
565	VTT-AS - VTT Technical Research (	FI	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	0%
679	TUNET-AS - Technische Universita	AT	Europe	Western Europe	RIPE NCC	100%	-	100%	100%	0%
680	DFN - Verein zur Foerderung eine	DE	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	63%
719	ELISA-AS - Elisa Oyj	FI	Europe	Northern Europe	RIPE NCC	93%	100%	100%	99%	60%

Terms and Conditions | Privacy Policy



MONTH (PARTIAL) October 2021

COUNTRY Ireland France Spain Portugal Italy Germany Netherlands (the) Belgium Luxembourg Denmark Sweden Finland Estonia Latvia Lithuania Poland Hungary Czechia Slovakia Austria Romania Greece Cyprus Malta Slovenia Bulgaria Croatia

☑ USE GRIP DATA

Details

Download data

Severity: All | Ready | Aspiring | Lagging | No Data Available

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

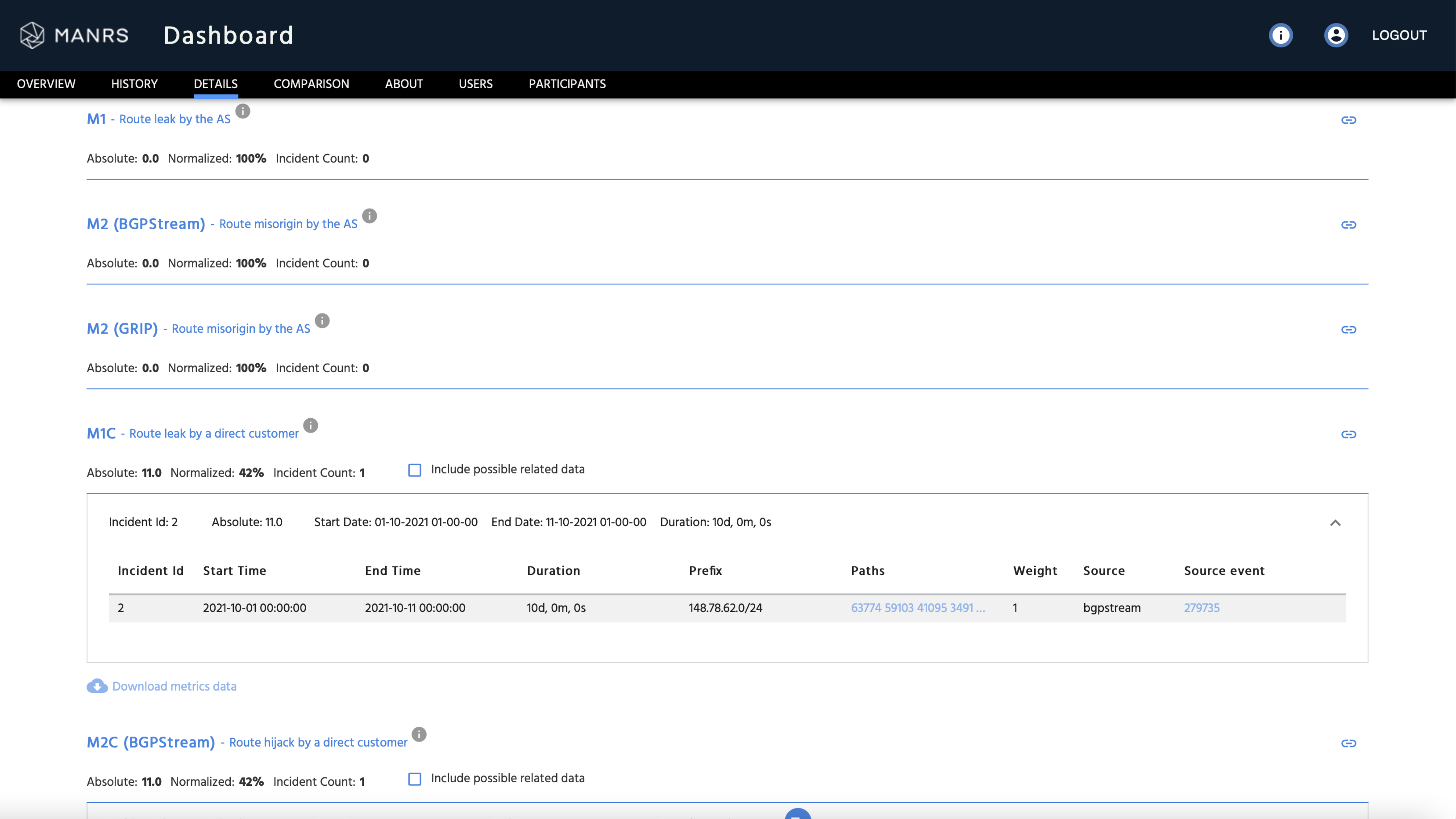
Result Limit: 100 | 200 | 500 | 1000

Total 15,112 Previous 1 2 3 4 5 ... 152 Next

Overview

ASN	Holder	Country	UN Regions	UN Sub-Regions	RIR Regions	Filtering	Anti-spoofing	Coordination	Global Validation IRR	Global Validation RPKI
137	ASGARR - Consortium GARR	IT	Europe	Southern Europe	RIPE NCC	100%	-	100%	100%	81%
286	KPN - KPN B.V.	NL	Europe	Western Europe	RIPE NCC	95%	-	100%	100%	100%
288	ESA - European Space Agency (ES	DE	Europe	Western Europe	RIPE NCC	100%	-	100%	100%	0%
375	TIETOTIE-AS - Tieto Oyj	FI	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	2%
553	BELWUE - Universitaet Stuttgart	DE	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	75%
565	VTT-AS - VTT Technical Research (	FI	Europe	Northern Europe	RIPE NCC	100%	-	100%	100%	0%
679	TUNET-AS - Technische Universita	AT	Europe	Western Europe	RIPE NCC	100%	-	100%	100%	0%
680	DFN - Verein zur Foerderung eine	DE	Europe	Western Europe	RIPE NCC	100%	100%	100%	100%	63%
719	ELISA-AS - Elisa Oyj	FI	Europe	Northern Europe	RIPE NCC	93%	100%	100%	99%	60%

Terms and Conditions | Privacy Policy



M1 - Route leak by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M2 (BGPStream) - Route misorigin by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M2 (GRIP) - Route misorigin by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M1C - Route leak by a direct customer

Absolute: **11.0** Normalized: **42%** Incident Count: **1** □ Include possible related data

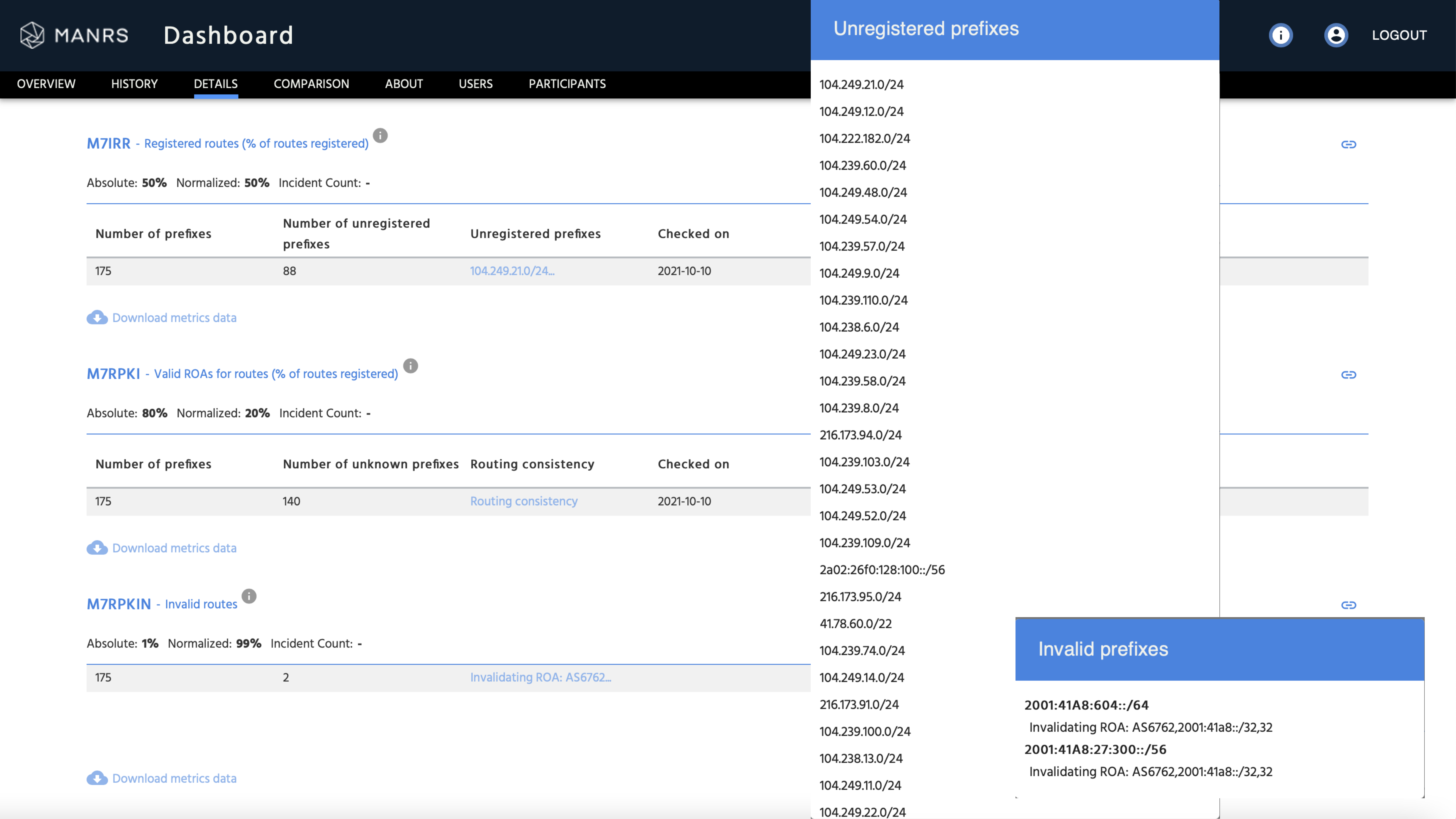
Incident Id: 2 Absolute: 11.0 Start Date: 01-10-2021 01-00-00 End Date: 11-10-2021 01-00-00 Duration: 10d, 0m, 0s

Incident Id	Start Time	End Time	Duration	Prefix	Paths	Weight	Source	Source event
2	2021-10-01 00:00:00	2021-10-11 00:00:00	10d, 0m, 0s	148.78.62.0/24	63774 59103 41095 3491 ...	1	bgpstream	279735

Download metrics data

M2C (BGPStream) - Route hijack by a direct customer

Absolute: **11.0** Normalized: **42%** Incident Count: **1** □ Include possible related data



M7IRR - Registered routes (% of routes registered)

Absolute: **50%** Normalized: **50%** Incident Count: **-**

Number of prefixes	Number of unregistered prefixes	Unregistered prefixes	Checked on
175	88	104.249.21.0/24...	2021-10-10

Download metrics data

M7RPKI - Valid ROAs for routes (% of routes registered)

Absolute: **80%** Normalized: **20%** Incident Count: **-**

Number of prefixes	Number of unknown prefixes	Routing consistency	Checked on
175	140	Routing consistency	2021-10-10

Download metrics data

M7RPKIN - Invalid routes

Absolute: **1%** Normalized: **99%** Incident Count: **-**

175	2	Invalidating ROA: AS6762...	

Download metrics data

Unregistered prefixes

104.249.21.0/24
104.249.12.0/24
104.222.182.0/24
104.239.60.0/24
104.249.48.0/24
104.249.54.0/24
104.239.57.0/24
104.249.9.0/24
104.239.110.0/24
104.238.6.0/24
104.249.23.0/24
104.239.58.0/24
104.239.8.0/24
216.173.94.0/24
104.239.103.0/24
104.249.53.0/24
104.249.52.0/24
104.239.109.0/24
2a02:26f0:128:100::/56
216.173.95.0/24
41.78.60.0/22
104.239.74.0/24
104.249.14.0/24
216.173.91.0/24
104.239.100.0/24
104.238.13.0/24
104.249.11.0/24
104.249.22.0/24

Invalid prefixes

2001:41A8:604::/64
Invalidating ROA: AS6762,2001:41a8::/32,32
2001:41A8:27:300::/56
Invalidating ROA: AS6762,2001:41a8::/32,32

MANRS Participation

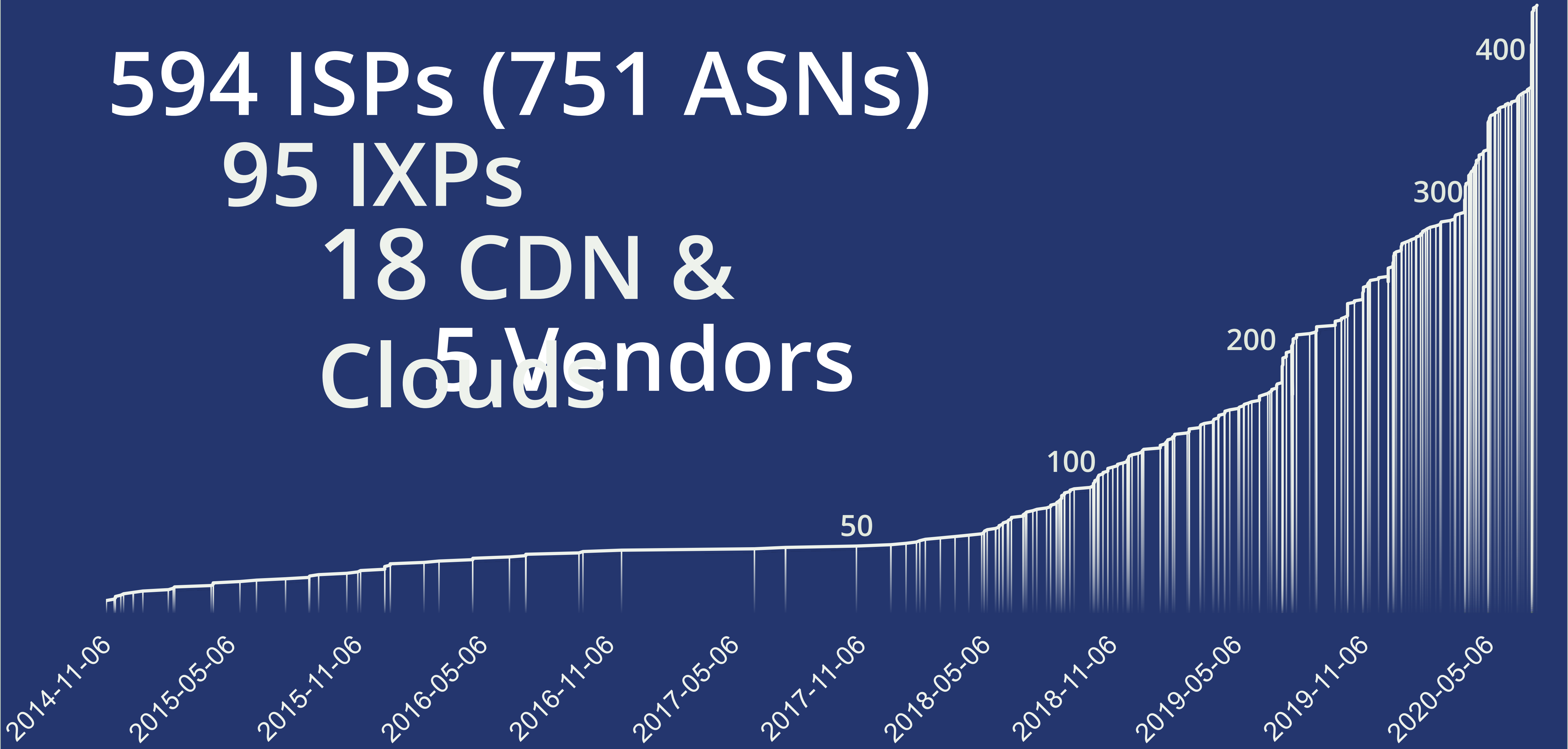
GROWTH OF THE MANRS MEMBERSHIP (NETWORK OPERATORS)

594 ISPs (751 ASNs)

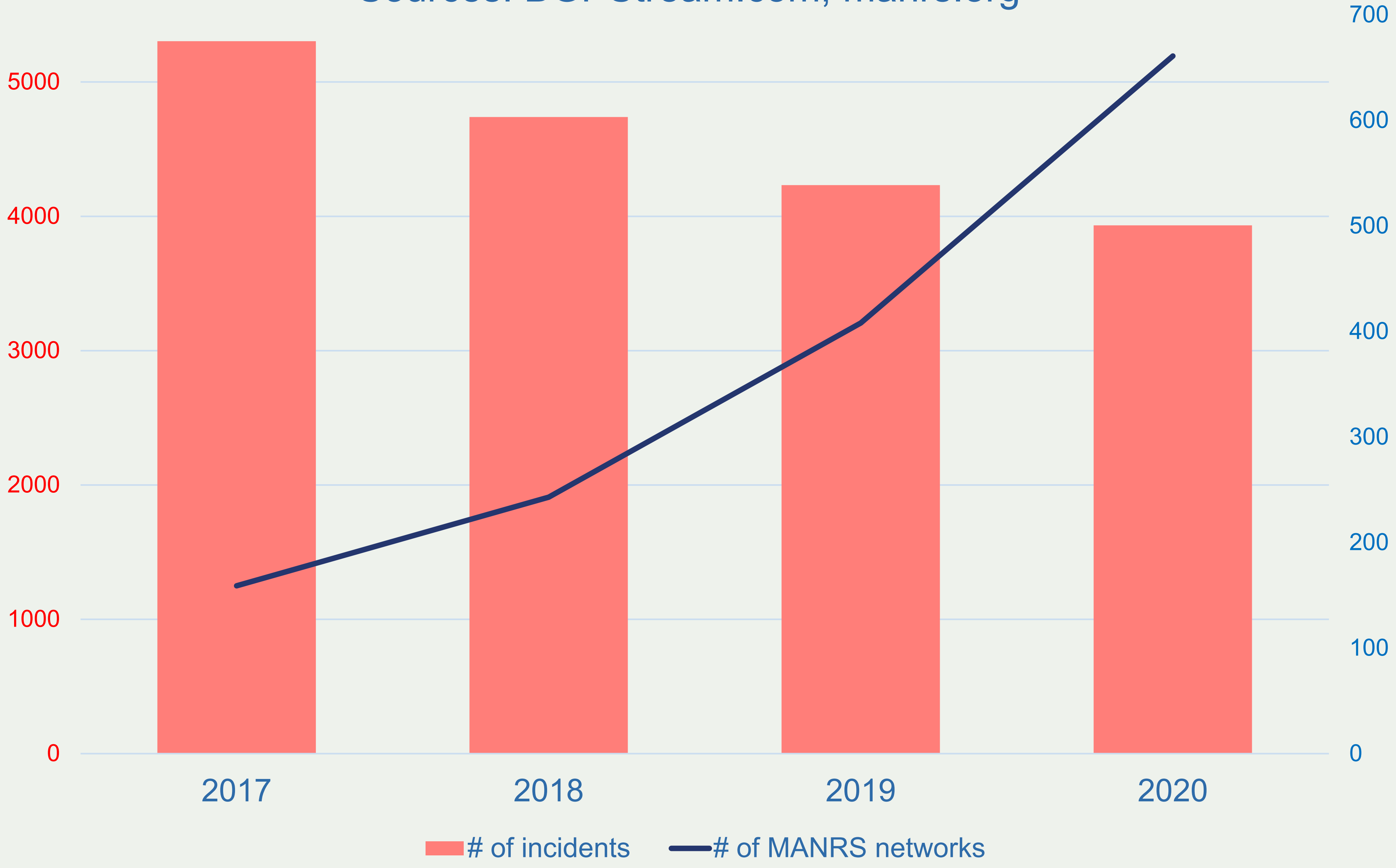
95 IXPs

18 CDN & Clouds

5 Vendors



Impact of implementing routing security measures
Sources: BGPStream.com, manrs.org



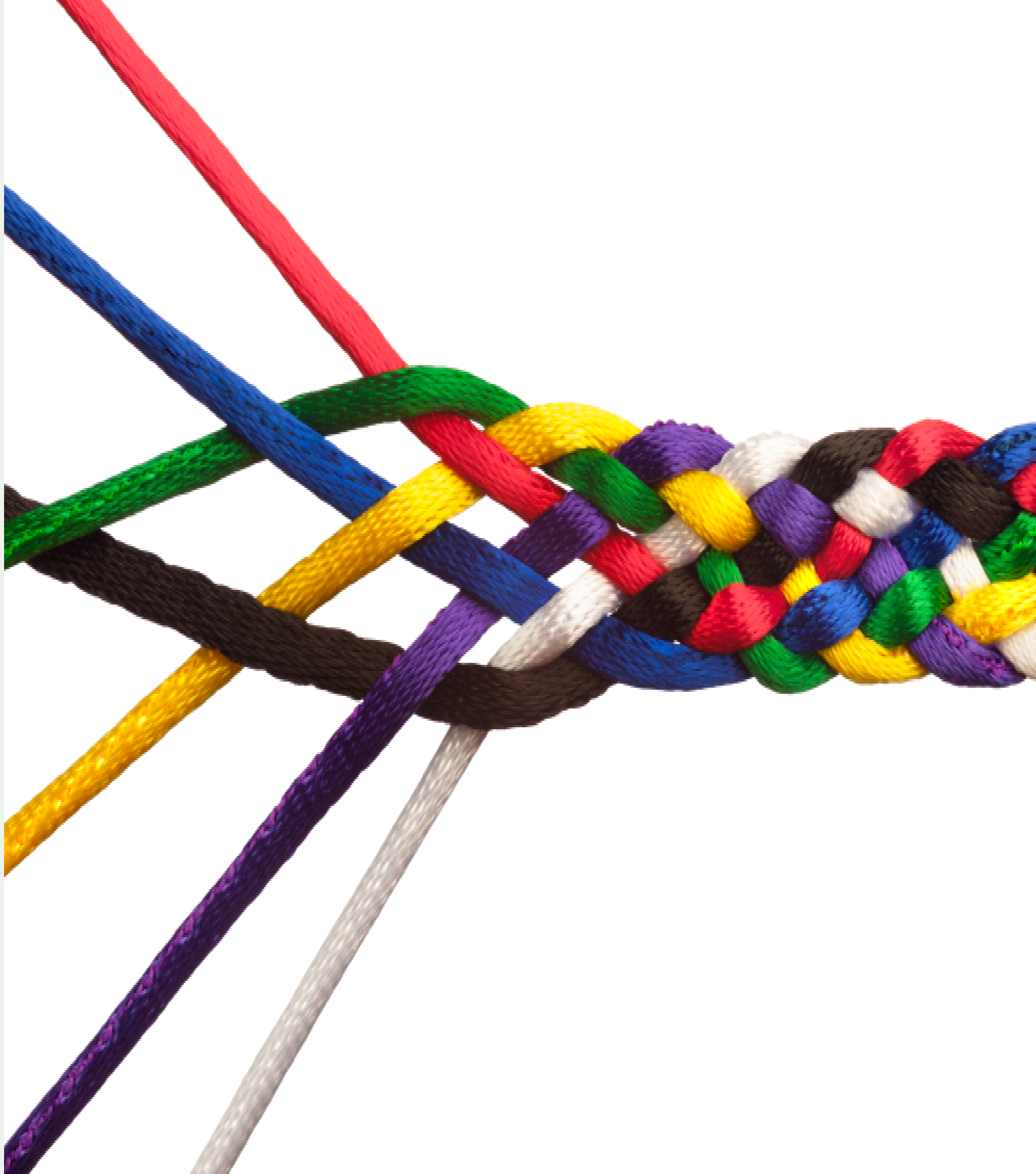
Join the MANRS Community

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the manifesto and promote MANRS objectives



MANRS

How can ENISA get involved?

- Identification of global routing system as critical Internet infrastructure
- Raise awareness of routing security in CSIRT and national critical infrastructure activities
- Encourage addition routing security incident monitoring and handling to service portfolios
- Help organise practical routing security workshops and/or develop routing security curriculums in the context of training-the-trainers and/or network forensics capacity building programmes
- Encourage addition of routing security to network security auditing programmes
- Inclusion of routing security activities in cyberdrills

Promote utilisation of the MANRS Observatory routing security monitoring tool