BGP Security

Hijack and Route Leak Detection

Lefteris Manassakis | COO, Code BGP

✉ lefteris@codebgp.com

dknog13

March 9-10, 2023
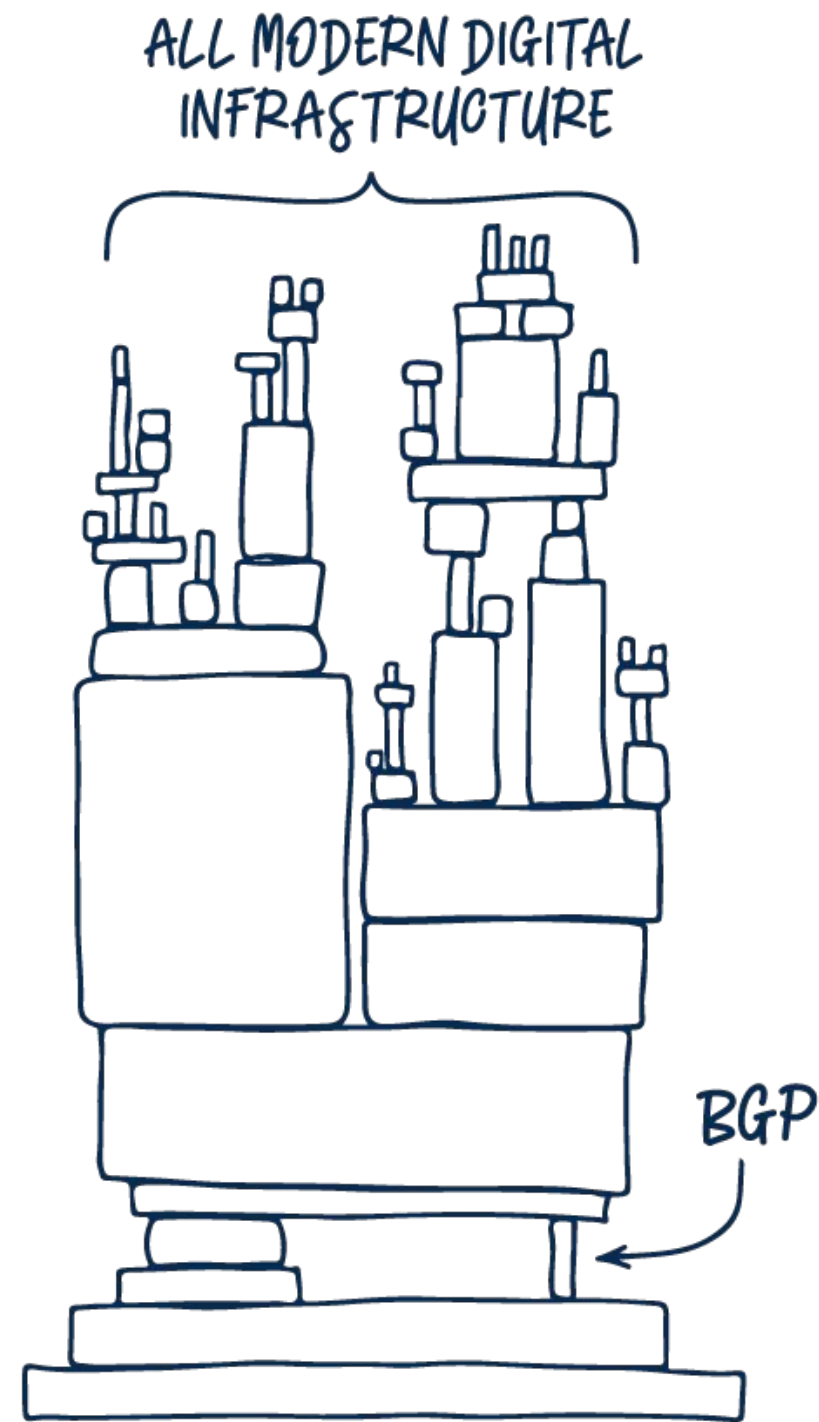
About me

Lefteris Manassakis

COO & co-founder | Code BGP

✉ lefteris@codebgp.com

🌐 https://manassakis.net/

⚠️ **BGP** hijacks, leaks & misconfigurations **affect your network**

ALL MODERN DIGITAL
INFRASTRUCTURE

BGP

- BGP events critically affect **reliability, security, and performance**

- Only the **tip of the iceberg** gets known

Code BGP

3

Types of BGP prefix hijacks

- **Classification by Announced AS–Path**

  - **Origin–AS (or Type–0):** The hijacker AS announces – as its own – a prefix that it is not authorized to originate. This is the most commonly observed hijack type.
  - **Type–N (N ≥ 1):** The hijacker AS announces an illegitimate path for a prefix it does not own. The announced path contains the ASN of the victim (first AS in the path) and hijacker, e.g., {AS50414, ASx, ASy, AS1 – 212.46.55.0/24}, while the sequence of ASes in the path is not a valid route, e.g., AS50414 is not an actual neighbor of ASx.

Types of BGP prefix hijacks

- **Classification by Affected Prefix**

  - **Exact Prefix Hijacking:** The hijacker announces a path for exactly the same prefix announced by the legitimate AS. Since shortest AS-paths are typically preferred, only a part of the Internet that is close to the hijacker (e.g., in terms of AS hops) switches to route towards the hijacker.
  - **Sub-Prefix Hijacking:** The hijacker AS announces a more specific prefix of the prefix of the legitimate AS. Since the more specific prefixes are preferred, the entire Internet routes traffic towards the hijacker to reach the announced sub-prefix.
  - **Squatting:** The hijacker AS announces a prefix owned but not (currently) announced by the owner AS.
  - For a comprehensive prefix hijack taxonomy please check the ARTEMIS paper.

Route Leaks

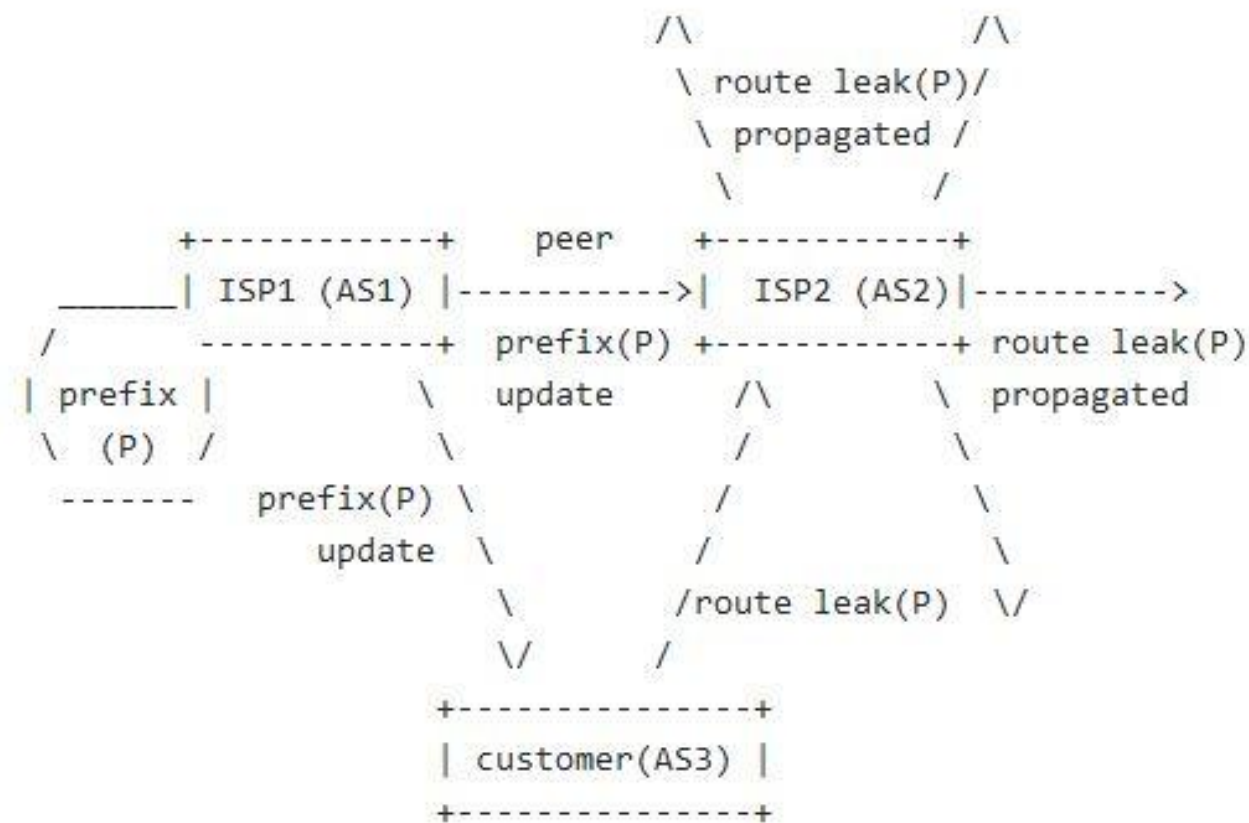- **Definition:** A route leak is the propagation of routing announcement(s) beyond their intended scope.

```
                               /\               /\
                               \ route leak(P)/
                                \ propagated /
                                 \         /
          +------------+   peer   +------------+
     _____| ISP1 (AS1) |--------->|  ISP2 (AS2)|---------->
    /      ------------+ prefix(P) +------------+ route leak(P)
   | prefix |          \   update      /\        \ propagated
   \  (P)  /            \             /            \
    -------       prefix(P) \        /              \
              update  \        /                \
                       \      /route leak(P)  \/
                        \/    /
                     +---------------+
                     | customer(AS3) |
                     +---------------+

          Figure 1: Basic Notion of a Route Leak
```

  - For different types of route leaks please check RFC 7908.

Challenges of hijack and route leak detection

- **Speed**
- **Accuracy**
- **Evasion**
- **Privacy and flexibility**

ARTEMIS

https://bgpartemis.org
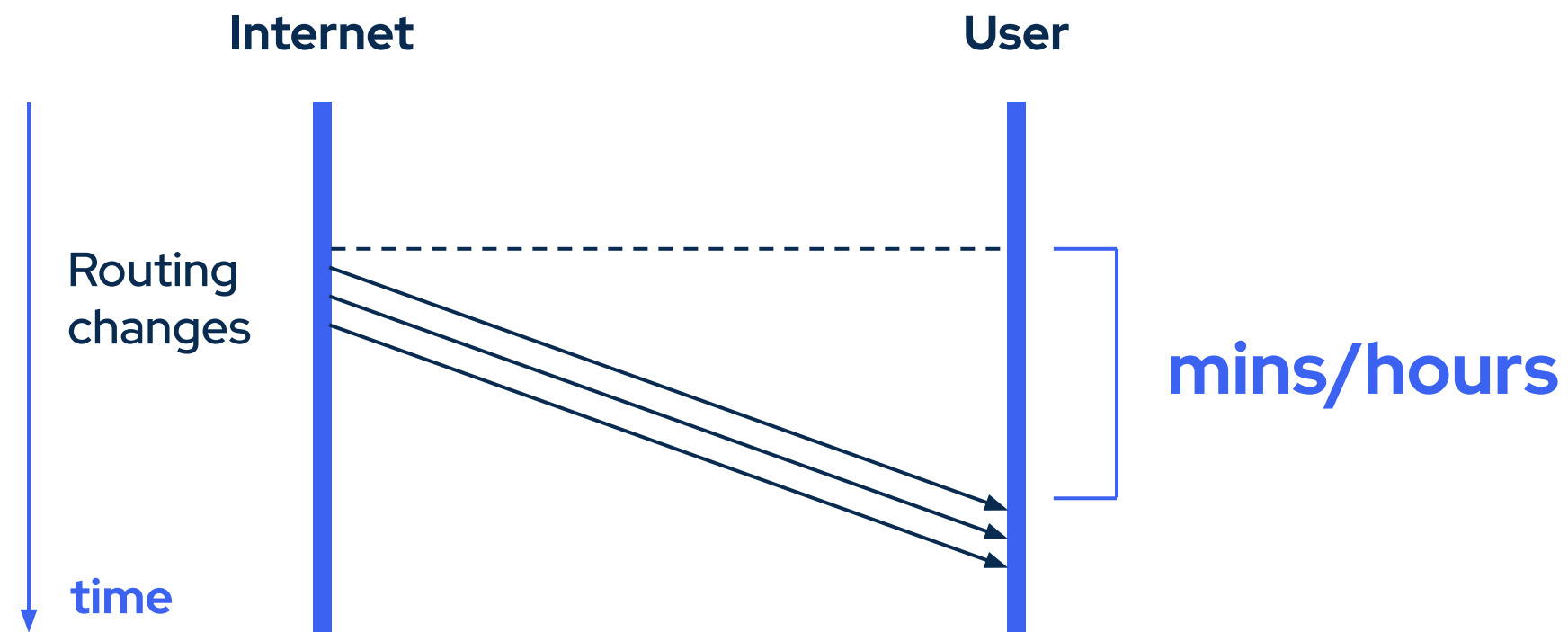
- On-prem **open-source** tool we developed
- We support a community of users

- Precursor of the Code BGP Platform
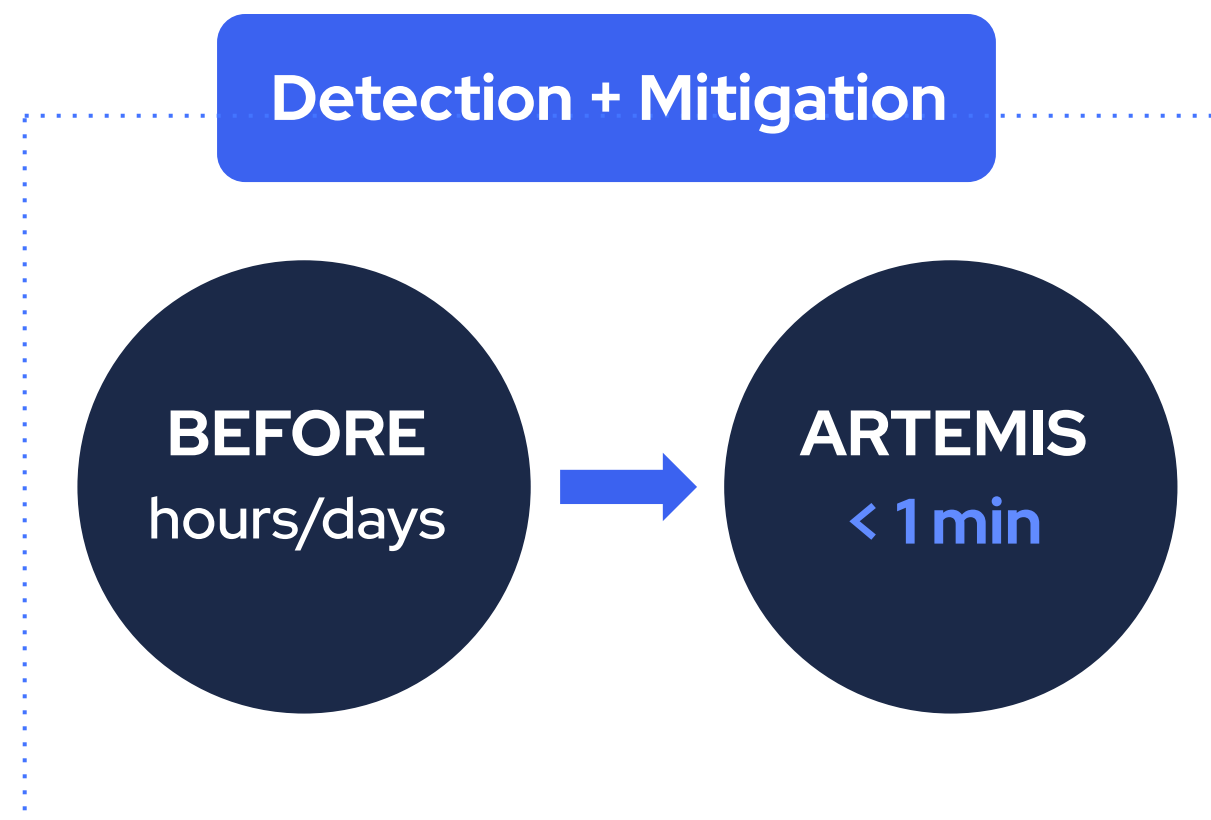
- The Code BGP Platform is offered as a SaaS subscription
- Both are self-operated, leveraging the contextual knowledge of the Network Operator

Detection + Mitigation

BEFORE
hours/days

➡

ARTEMIS
< 1 min

"ARTEMIS is a **fantastic** replacement for BGPmon. All around it seems like **an incredibly well-built tool** and **I use it in prod all the time**"

Chris Cummings
Network Engineer & modem.show podcast host

ARTEMIS Overview

Data Sources

ARTEMIS
(on-prem)

User

RIS live

BGPstream

Public BGP feeds

BGP/BMP

Your BGP routers

**Monitoring
& detection**

Exact-prefix type-0/1,
path + policy violations,
sub-prefix, squatting
attacks

UI

Notifications
(slack/email/syslog)

Configuration
(Yaml)

Code BGP Platform

Monitor · Detect · Protect

USER

| Alerting | Automation | Dashboards |

CODE BGP PLATFORM

State of prefixes & routes

REAL-TIME TELEMETRY

1,600+ BGP monitors

Your BGP routers

RPKI
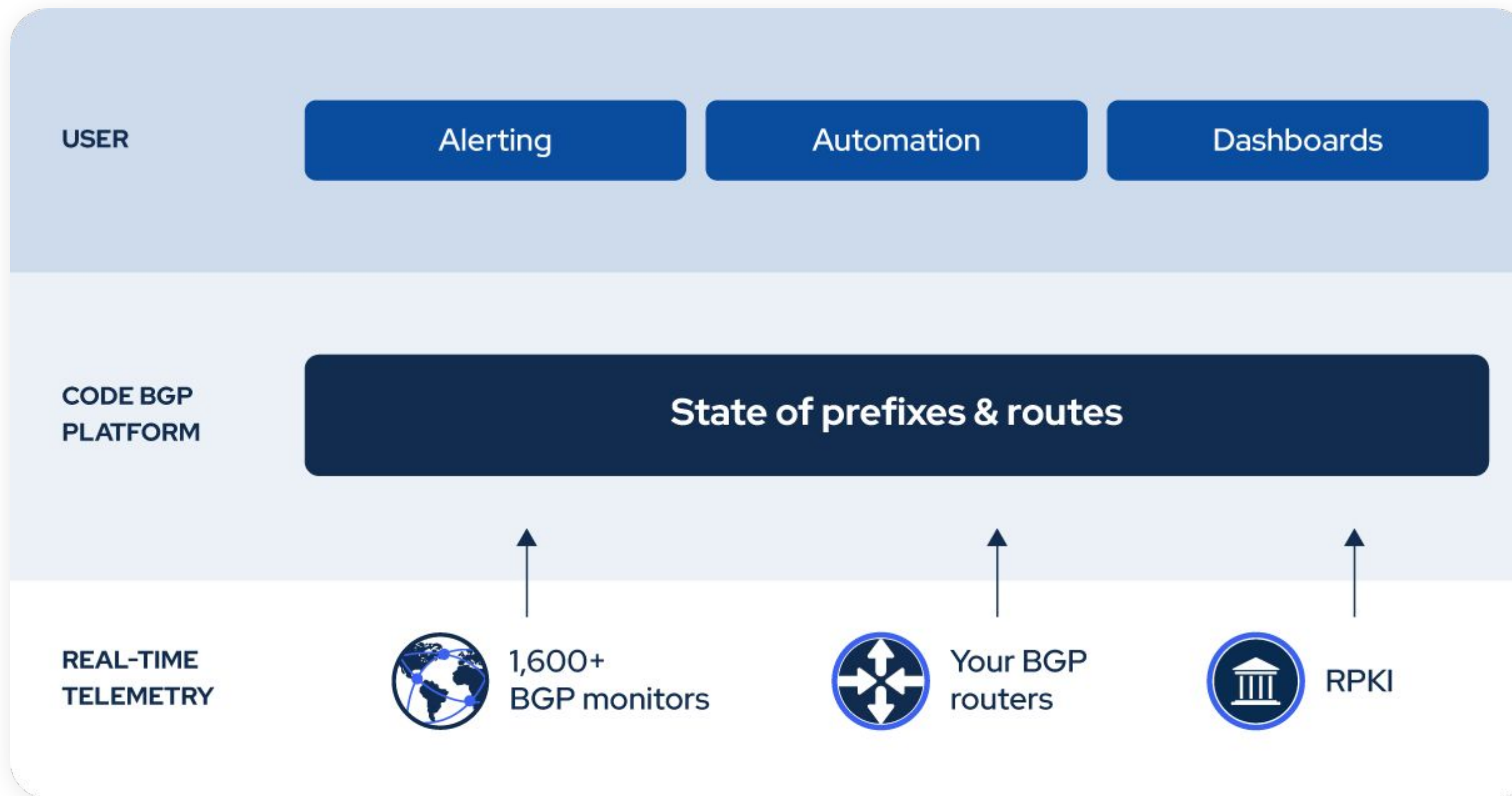
Code BGP

Data service: Code BGP Monitor

BGP Monitoring Service developed by
Code BGP

- Route Reflection (RFC 4456)

- BGP Add-Path (RFC 7911)

- **186** full feed peerings (v4 & v6)

Code BGP monitors

Data Service: RIS Live

Provides real-time JSON BGP messages via a fully filterable interactive WebSocket JSON API, and a full stream ("firehose") containing all of the messages generated by RIS. → https://ris-live.ripe.net/

Total peerings (IPv4 & IPv6):
1448
BGP full feeds:
- IPv4: **366**
- IPv6: **401**

List of Route Collectors: https://ris.ripe.net/docs/10_routecollectors.html

List of Peers: https://www.ris.ripe.net/peerlist/all.shtml

Data service: Your routers

- **Multi-hop** BGP sessions

Data center

Cloud

Internet

Offices

My router
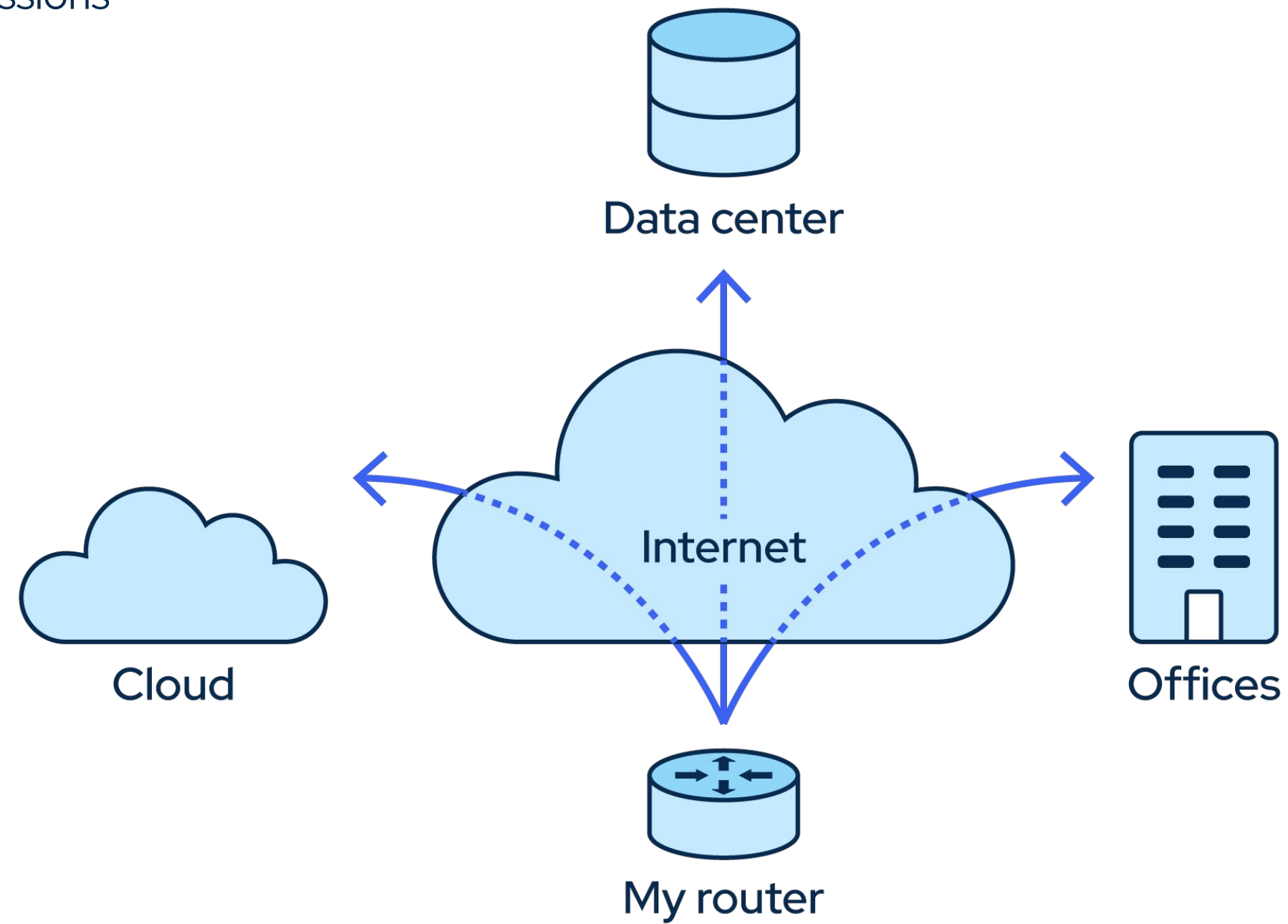
Data Service: RPKI

- Tracking the state of **ROA certificates**

- **Validating** BGP updates and detecting **invalids**

Certificate Authorities

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

ARIN
American Registry for Internet Numbers

lacnic

APNIC

AFRINIC
The Internet Numbers Registry for Africa

ROAs

| Track certificates' state | Validate BGP updates |
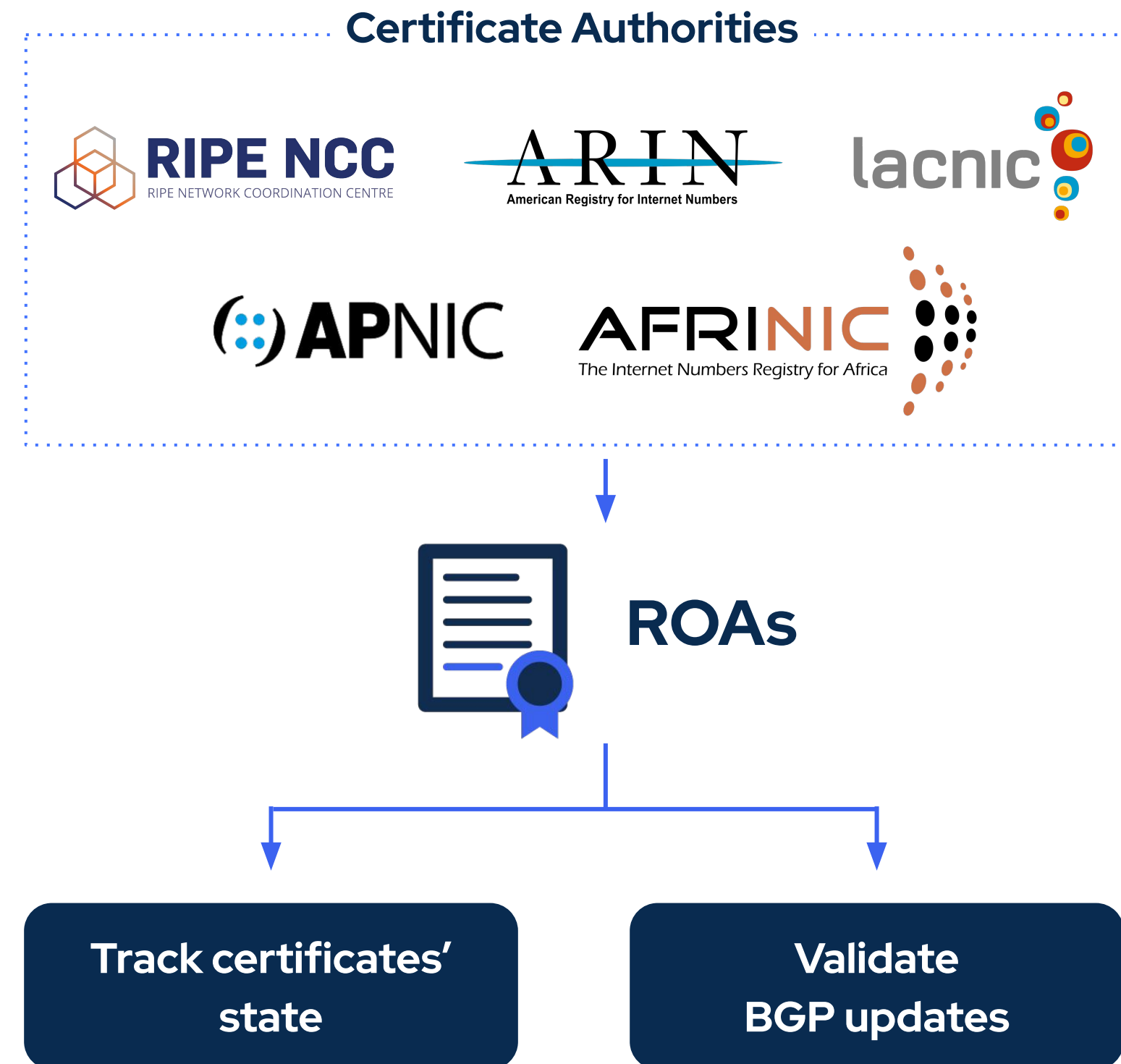
Alert Types

Supported Alert Types	Description
Exact Prefix Hijack	Illegal origin ASes that announce configured prefixes.
Sub-Prefix Hijack	Illegal origin ASes that announce subprefixes of configured prefixes.
Route Leak	Unexpected prefixes in the list of prefixes that are announced by configured ASes.
New Neighbor	New neighbors that appear to peer with configured ASes. Possible AS path manipulation.
Neighbor Leak/Hijack	New neighbors that not only appear to peer with configured ASes, but also propagate their prefixes.
Squatting	Illegal origin ASes announcing prefixes that are not currently announced by configured ASes.
RPKI-Invalid Detection	RPKI-Invalid announcements of configured prefixes by other ASes.
RPKI-Invalid Announcement	RPKI-Invalid announcements by configured ASes.
RPKI-Invalid Propagation	RPKI-Invalid routes propagated by configured ASes.
RPKI-NotFound Propagation	RPKI-NotFound routes propagated by configured ASes.
Bogon Prefix	Announcements of bogon prefixes by configured ASes.
Bogon AS	In-path presence of bogon ASes, in routes towards configured prefixes.
AS Path Comparison	Discrepancies in AS paths towards the same prefix, comparing between different Data Services, up to a terminating (end) AS.
Prefix Comparison	Discrepancies in prefixes announced by configured ASes, comparing between different Data Services.
Custom	User-defined

GraphQL basics

- **What it is**
  - Query language for APIs
  - Runtime for fulfilling queries with existing data
- **Features**
  - Ask exactly the data you need
  - Get many resources in single request
  - Single endpoint + type system: organized in terms of types and fields, not endpoints
  - No-version API evolution
  - Integration with own data + code
  - Supports subscriptions

GraphQL subscriptions

- Subscriptions are a **GraphQL feature** that allows a server to send data to its clients when a specific event happens. They are implemented with WebSockets, and the server maintains a steady connection to its subscribed client. This also breaks the "Request–Response–Cycle" that were used for all previous interactions with the API.

- Instead, the client initially opens up a **long–lived connection** to the server by sending a subscription query that specifies which event it is interested in. Every time this particular event happens, the server uses the connection to push the event data to the subscribed client(s).

GraphQL API | Editor ▶ Prettify History Explorer Docs

```
1  Subscription AutonomousSystemNumbers {
2    autonomousSystems(order_by: {number: asc}) {
3      number
4    }
5  }
6
```

Insert Alert Rules using the UI

1 Add Alert Rule

2 Add Parameters

3 Preview Parameters & Add GQL Subscription

How we use GraphQL Subscriptions for Alert Rules

- **Example** of a subscription query (which is entered to the system as a mutation) to detect exact prefix hijacks for prefixes belonging to Code BGP (AS 50414).

```
mutation MutationExactPrefixHijack {
    insertAlertSubscription(object: {name: "Exact Prefix Hijack", query: "subscription IllegalOriginsFromWhichExactPrefixesAreAnnounced($asns:
[bigint!] = [], $prefixes: [cidr!] = []) { routes(where: {originAutonomousSystem: {number: {_nin: $asns}}, prefix: {network: {_in: $prefixes}}}
order_by:
{as_path: asc, prefix: {network: asc}, originAutonomousSystem: {number: asc}}) { originAutonomousSystem { number } prefix { network } as_path
}}", vars: {asns:[50414],
prefixes:["212.46.55.0/24","2a12:bc0::/48","2a12:bc0:1::/48","2a12:bc0:2::/48","2a12:bc0:3::/48","2a12:bc0:4::/48","2a12:bc0:5::/48"]},
fire_alert_regex: "^.*routes.*as_path.*$", type: "as_origin_violation_exact", severity: "critical", description: "Illegal origin ASes that
announce configured prefixes."}) {
        id
        name
        query
        vars
        fire_alert_regex
        type
        severity
        description
    }
}
```

Exact Prefix Hijack detected for root DNS prefix – Jan 27

- AS 24028 announced prefix 2001:500:2f::/48 which belongs to ISC, and serves as the IPv6 prefix of the "F–Root" domain server (AS 3557)
- Seen only by one source, which happens to be a neighbor of the offending network. The limited propagation is possibly due to RPKI ROV

Exact Prefix Hijacks detected for root DNS prefixes – Feb. 25

- AS 7639 announced prefix 2001:500:a8::/48 which belongs to NASA and is the IPv6 prefix of the "E-Root" domain server (AS 21556)
- At the exact same time, the same AS 7639 announced prefix 2001:500:2f::/48 which belongs to F-Root (ISC AS 3557)

Exact Prefix Hijacks detected for root DNS prefixes – Feb. 25

- The "E-Root" 2001:500:a8::/48 prefix is not covered by a RPKI ROA. The event lasted 2 days

Exact Prefix Hijacks detected for root DNS prefixes – Feb. 25

- The "F-Root" 2001:500:2f::/48 prefix is covered by a RPKI ROA. The event lasted 18 hours

Type-1 Hijack detected – Mar. 7 (false positive!)

- AS 48287 appeared twice as a first hop neighbor of ICANN (AS 20144) and propagated prefix 2001:500:3::/48. These events lasted 14 seconds (the 1st) and 16 minutes (the 2nd).

Prefix Hijacking Demo

Questions

✉ lefteris@codebgp.com

🌐 codebgp.com