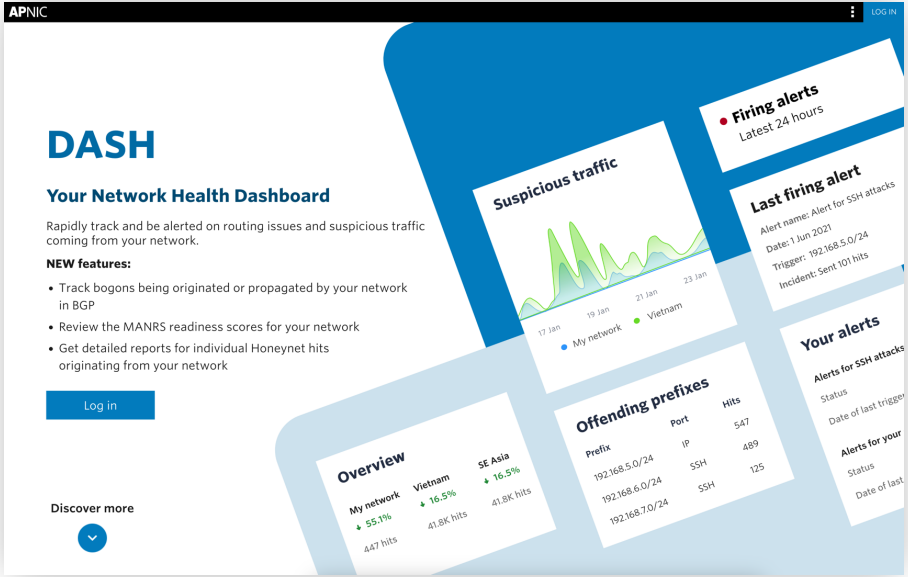
Real-time routing security at scale in DASH

Beau Gieskens

APNIC DASH

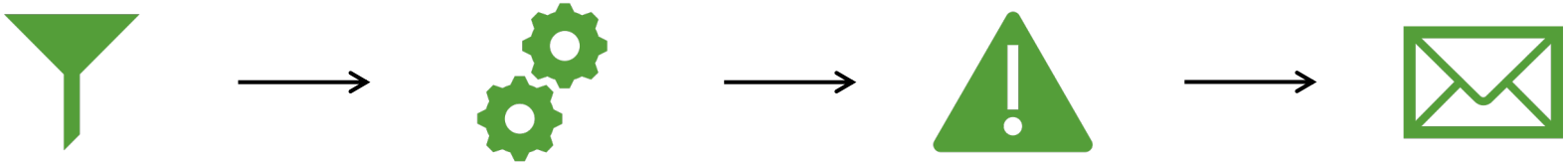
- Network health dashboard
- Available for all APNIC members at dash.apnic.net
- Helps with identification and resolution of Internet security issues.



Alerts in DASH

- Suspicious traffic within my network crosses a threshold
  - SSH brute force attacks
- One of my prefixes is being originated by an unexpected ASN (BGP leak or hijack)
- My routes are invalid according to RPKI
- No IRR route objects have been published for my routes

What is a routing status alert?



1.1.1.0/24
AS4608
Any of my prefixes

Wrong ASN
ROA not published
IRR mismatch

Triggered
Resolved

Original implementation

1.1.1.0/24

Wrong ASN

Original implementation

- Every 30 seconds (cron schedule)
- For each alert:
  - Query RPKI status from Routinator
  - Query IRR status from IRRd
  - Query BGP status from internal service (RIPE RIS mirror)
  - Put it all together

Growing pains

- Every 30 seconds became every 2 minutes
- … then 5 minutes
- … except the ones which take too long to process, which were done every hour instead

The Dream

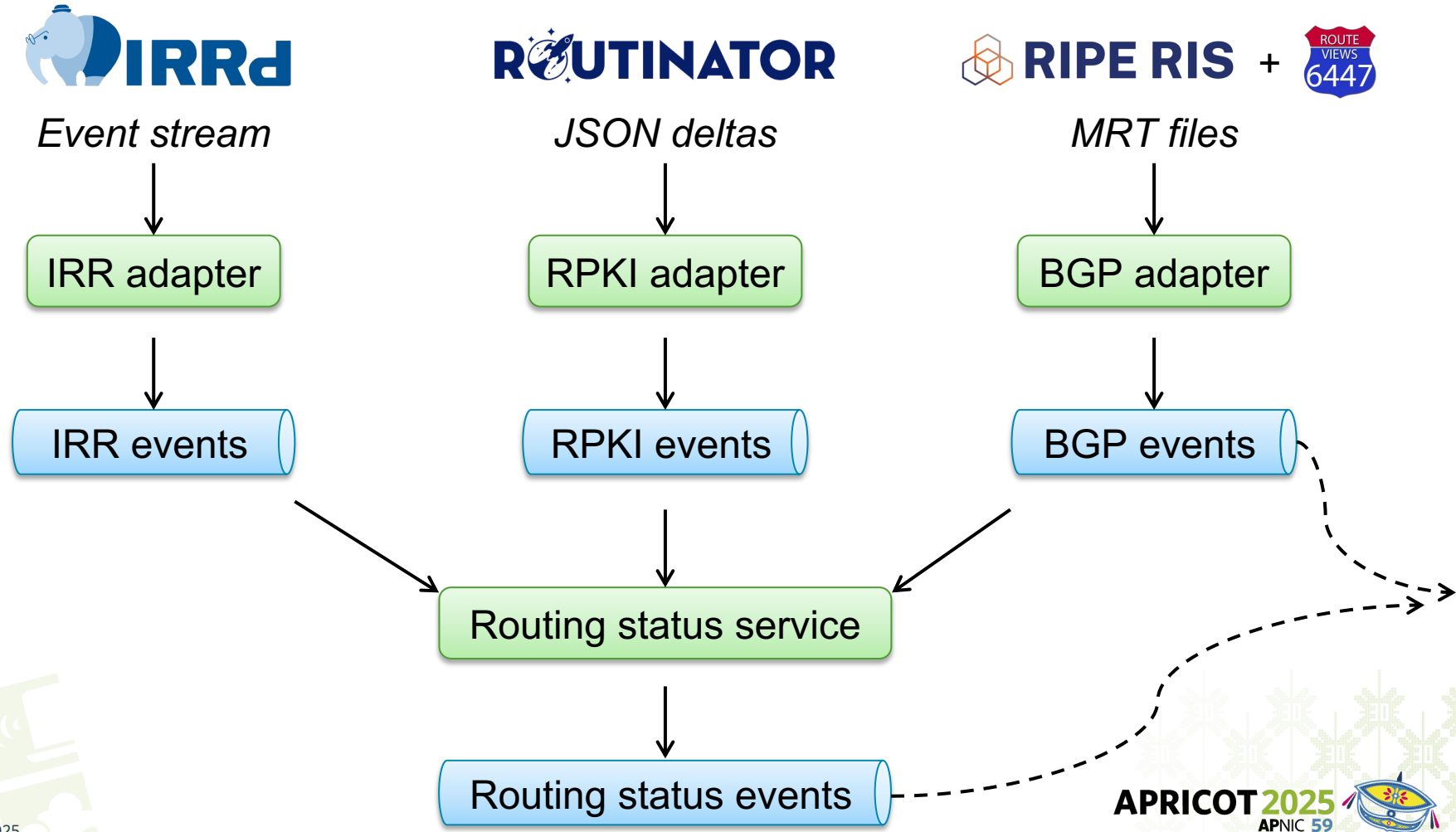
1.1.1.0/24

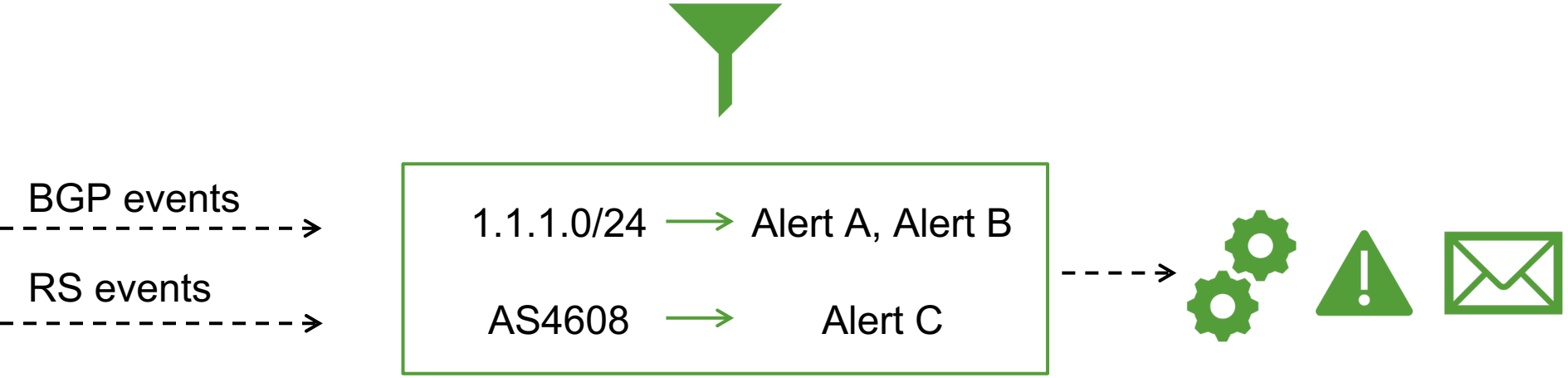
IRRd

ROUTINATOR

RIPE RIS

Wrong ASN


IRRd
ROUTINATOR
RIPE RIS + ROUTE VIEWS 6447
Event stream
JSON deltas
MRT files
IRR adapter
RPKI adapter
BGP adapter
IRR events
RPKI events
BGP events
Routing status service
Routing status events


BGP events
RS events
1.1.1.0/24
Alert A, Alert B
AS4608
Alert C

New architecture

- No more cron schedule
- Alerts trigger as soon as a relevant event comes through
- Upper limit is no longer on how many alerts we track, instead depends on how fast things change on the Internet!

Challenges – big changes

- BGP is likely the fastest-moving part of routing status
- If something crazy happens (and it does), it can easily overwhelm a system without mechanisms to handle it

Challenges – maintenance

- Event queues can be difficult to debug
- Still maintain the on-demand alert processing logic

Wins

- We were able to triple alert subscriber count in 2024!
- It became feasible to add 6 additional BGP collectors
  - Was only RIS RRC23 (Singapore)
  - Now includes RouteViews Sydney

2025 APRICOT APNIC 59

PETALING JAYA, MALAYSIA

19 – 27 February 2025

#apricot2025