EuroVeil

European GNSS interference monitoring across CORS networks

Architecture, scope, capabilities and development plan

Proposal for EUPOS · October 2026

One portal for interference across networks

EuroVeil takes receiver streams and RINEX files from many CORS networks, reduces them to a few quality numbers per station, and reports interference events.

For every event: when it happened, how severe it was, which bands and constellations were affected, and which stations saw it.

Run through EUPOS. Each member network is a tenant.

1000

stations on one server, first target

4

input families: RTCM MSM, Septentrio SBF, Leica OEM7, RINEX

5

detectors, from C/N0 drop to data outage

~12

weeks to pilot start (estimate)

Scope

What EuroVeil does, and what it leaves to the specialised tools

The wide tool, not the deep one

Does

- Ingests streams and files from many networks
- Detects jamming, spoofing indicators, interference, degradation and outages
- Times stream events to the second
- Reports severity, bands and constellations
- Correlates events across stations and networks
- Alerts operators and feeds a public map

Leaves out

- Storing RINEX or raw streams
- Position computation
- Per-satellite history
- Spectrum waterfalls
- Forecasting and emitter localisation
- Heuristic spoofing scores

GeoVeil and SeptoVeil stay the deep tools and feed EuroVeil through its API.

Built on six earlier projects

GV

GeoVeil

OEM7 parsers; per-station baselines frozen during events; receiver flag and position jump as trusted spoofing signals

SV

SeptoVeil

SBF blocks for RF status, OSNMA and C/N0; event tracker rules

RT

geoveil-rtknma

Network, caster, station hierarchy; watchdogs; proof that heuristic spoofing scores had no skill

CN

geoveil-cn0

RINEX handling; 2 to 6 dB of C/N0 change is normal variation

RF

RINEX_FUTURE

MSM-first ingestion; station identity from registration, not file headers

TS

TrimbleSPEC

Spectrum CSV parser, kept for a later input

Capabilities

Inputs, detection, events, correlation and the portal

Six ways for a network to deliver data

1 Pull from caster

NTRIP client reading RTCM 3 MSM4 to MSM7. The primary path.

2 Connect to receivers

TCP to Septentrio SBF or Leica OEM7 logs. Needs a VPN or firewall opening.

3 Operator pushes streams

NTRIP server to the EuroVeil caster, or receiver to a EuroVeil TCP port.

4 RINEX files

SFTP, HTTPS POST, or scheduled fetch from an archive. Processed, then deleted.

5 Edge agent

Runs inside the operator's network and sends reduced metrics. Raw data never leaves.

6 External detector API

GeoVeil and SeptoVeil push their own detections.

Five detectors, fed by any input

D1	**C/N0 drop**	Median C/N0 in a band falls 3 dB or more on at least 60% of satellites	Observations
D2	**Tracking loss**	Satellites in a band drop by 30% or more, or a whole band disappears	Observations
D3	**Receiver RF detection**	Receiver reports an interferer, a notch, or AGC change above the station baseline	RF status
D4	**Spoofing indicators**	Receiver spoofing flag, OSNMA failure, or position over 150 m from registered	RF status, position
D5	**Data outage**	Stream connected but no valid epochs, or stream down	Any stream

Thresholds are initial values; each detector is calibrated on recorded data before it ships.

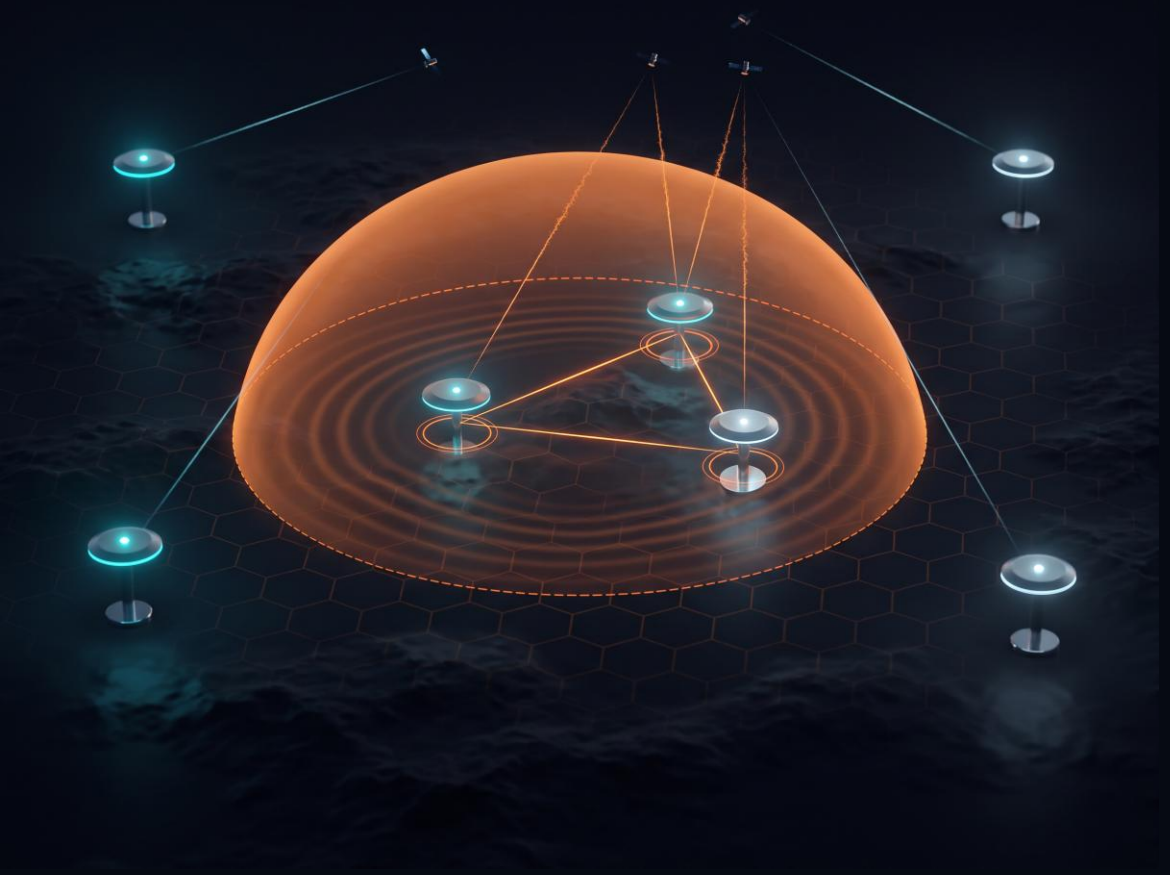
Each event: when, how bad, and what

4	**Critical**	Over 15 dB, band lost, several bands, or confirmed spoofing
3	**Major**	10 to 15 dB, or 30% of satellites lost in a band
2	**Minor**	6 to 10 dB
1	**Info**	3 to 6 dB, or RF detection without signal impact

Type	jamming, spoofing, interference, degradation, outage
Time	start, end and last seen, in UTC
Affected	bands and constellations
Metrics	largest C/N0 drop, share of satellites, centre frequency, bandwidth
Confidence	suspected or confirmed
Evidence	per-satellite C/N0 from 5 minutes before to 5 minutes after

Severity is stored once and can only rise while an event is open.

Incidents link events across networks



1. **Grouping**
   Same band, within 2 minutes, stations within 150 km
2. **One site, one vote**
   A site registered in two networks counts once
3. **Escalation**
   Three or more agreeing stations raise severity one step
4. **Network artefact**
   Over half of one network at once, with no neighbour confirming
5. **Space weather**
   Wide sunlit-side drops or high Kp are tagged, not escalated

Private detail, coarse public map

Network operators

- See their own stations in full detail
- Roles: owner, admin, viewer
- Thresholds per network and per station
- Maintenance windows silence alerts
- Joining is by invitation through EUPOS

Public map

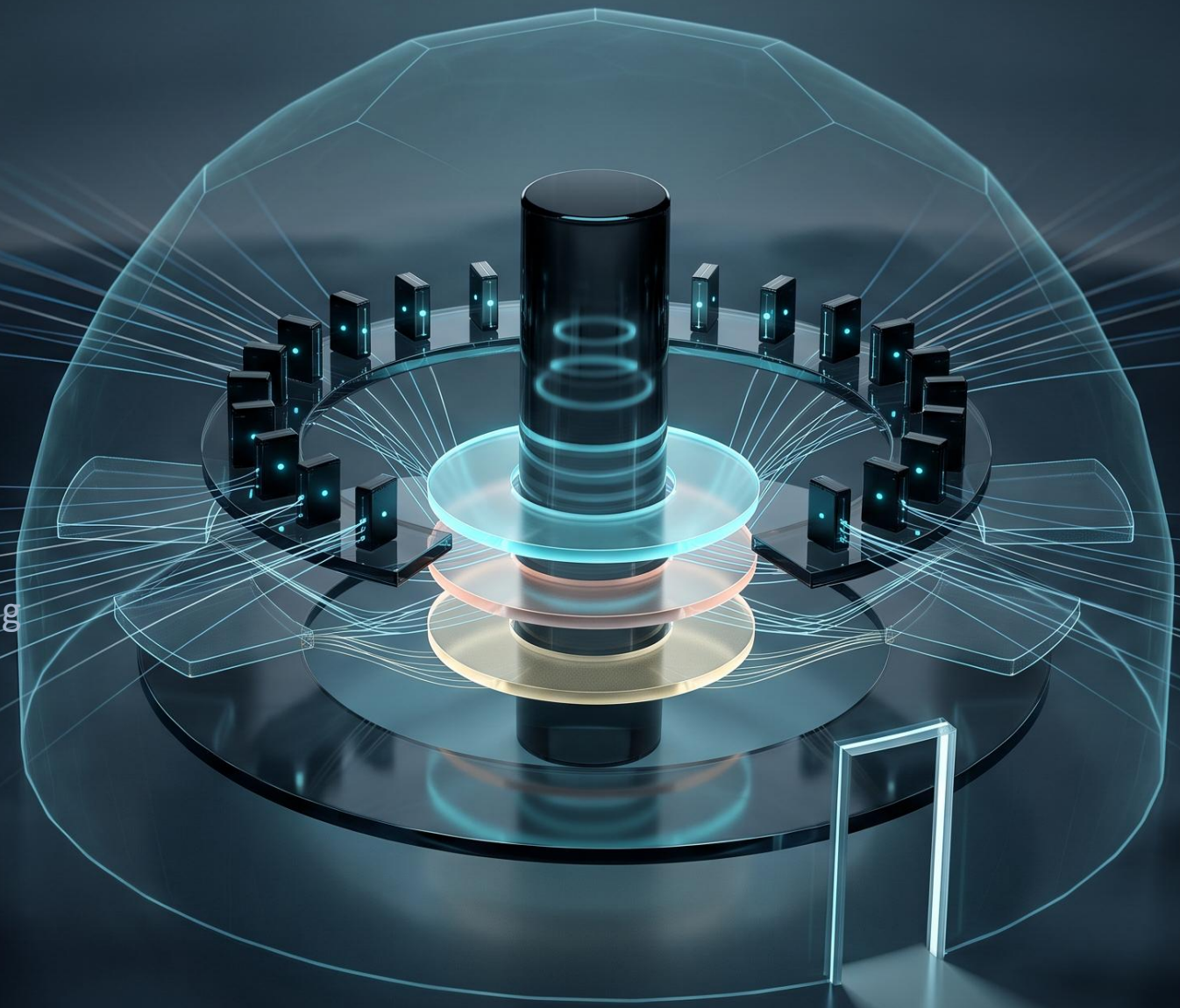
- Cells of about 20 km
- 15-minute delay
- No station identity
- Each network chooses private, coarse or full sharing
- Private is the default

Alerts

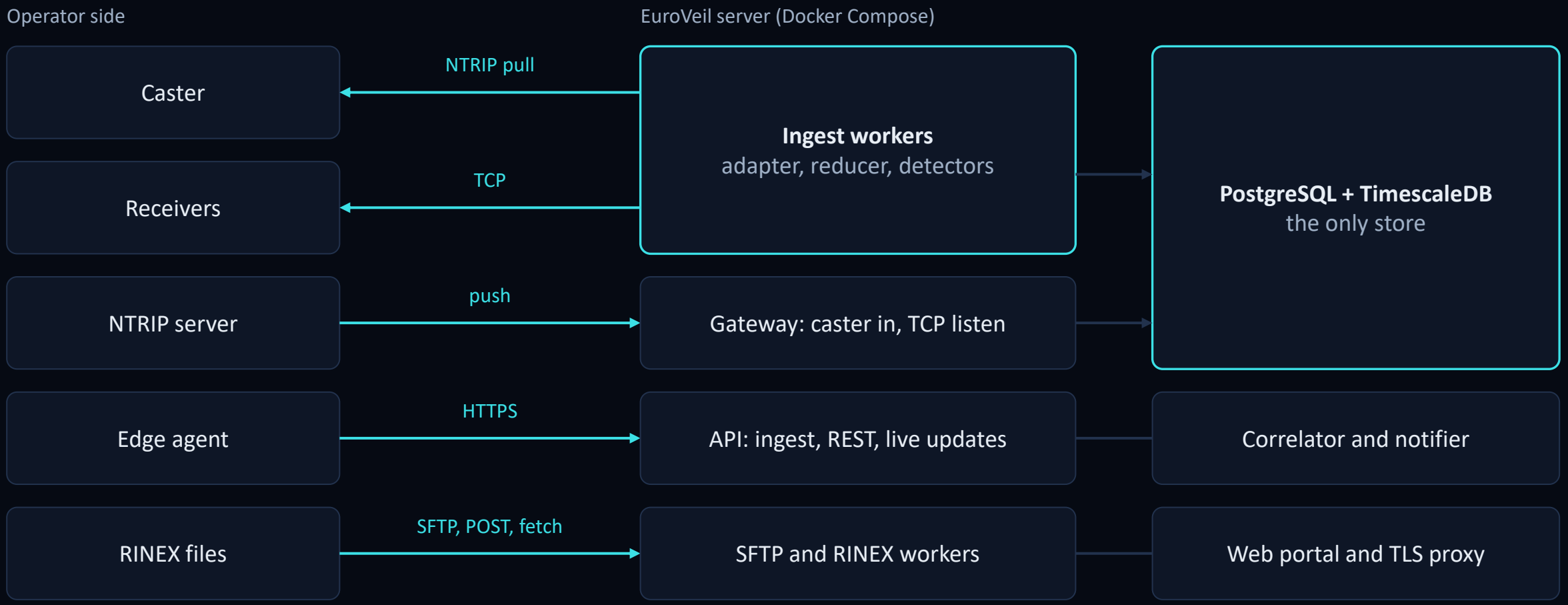
- Email, webhook, Telegram
- Sent on open, escalation and close
- Filter by network, severity and type
- At most one per station and type in 10 minutes
- Daily reminder for long events

Architecture

Components, data flow, storage, security and scaling

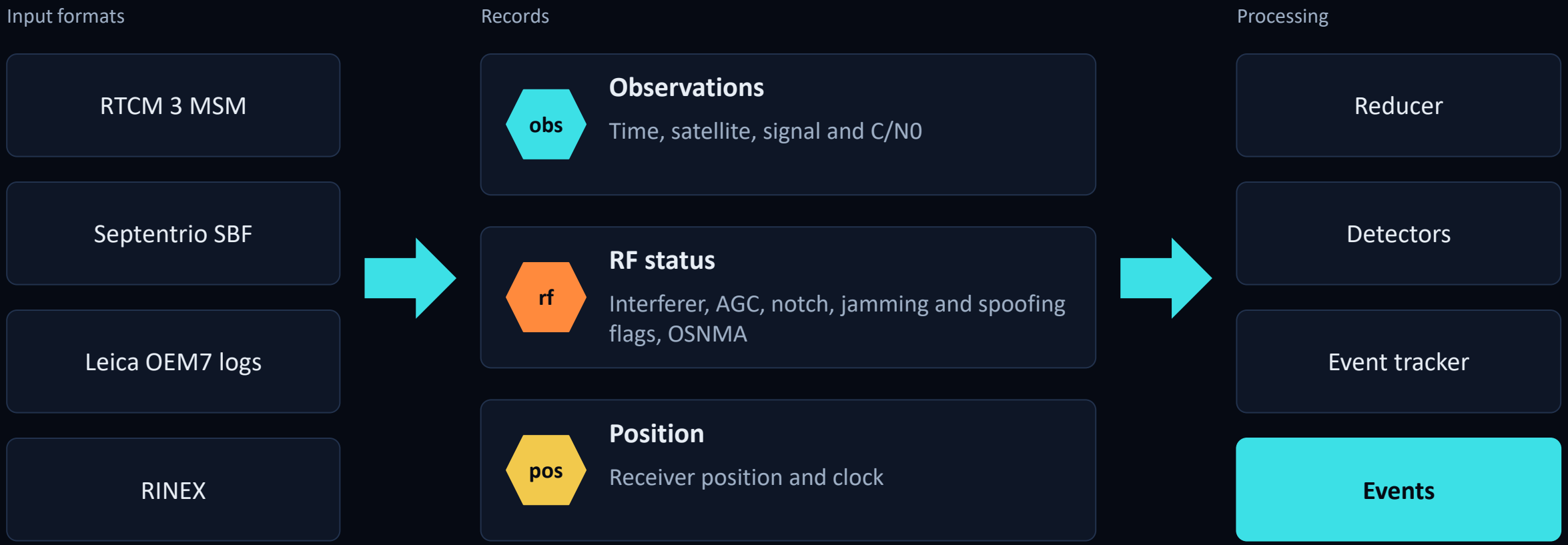


One server, one database, scalable workers



No message bus in version 1. Adding capacity means starting another worker, on this host or another.

Three record types keep detectors neutral



Detectors never see a vendor format, so a new receiver type needs only a new adapter.

What is stored, and for how long

Data	Kept	Note
5-minute metrics per station, constellation and band	Multi-year	About 1.3 billion rows a year at 1000 stations; estimated 25 to 40 GB compressed
Events and incidents	Forever	Start, end, severity, bands, constellations, tags
Event evidence	1 year (open)	Per-satellite C/N0 around each event
RINEX files	Deleted after processing	A ledger row is kept; failed files are held 7 days for debugging
Raw streams	Not stored	Reduced in memory at the native rate
Audit log	2 years	Configuration changes and logins

Safety is in the first milestone

1 Authentication

Passwords hashed with argon2, TOTP for admins, API keys with scopes

2 Tenant isolation

Every row carries its network; row-level security in the database

3 Protected credentials

Stream logins encrypted in the database; no secrets in git

4 No destructive API

No flush or bulk delete; deletions are soft and admin-only

5 Tested backups

Nightly dump and WAL archive, with a restore test in CI

6 Self-monitoring

Per-stream state, and a watchdog for streams that connect but send nothing

Scaling is a deployment change

1

Now

One host, 2 to 8 ingest workers, one database. Up to about 1000 stations.

2

More load

Workers on additional hosts. Edge agents take over parsing. A read replica serves the public map.

3

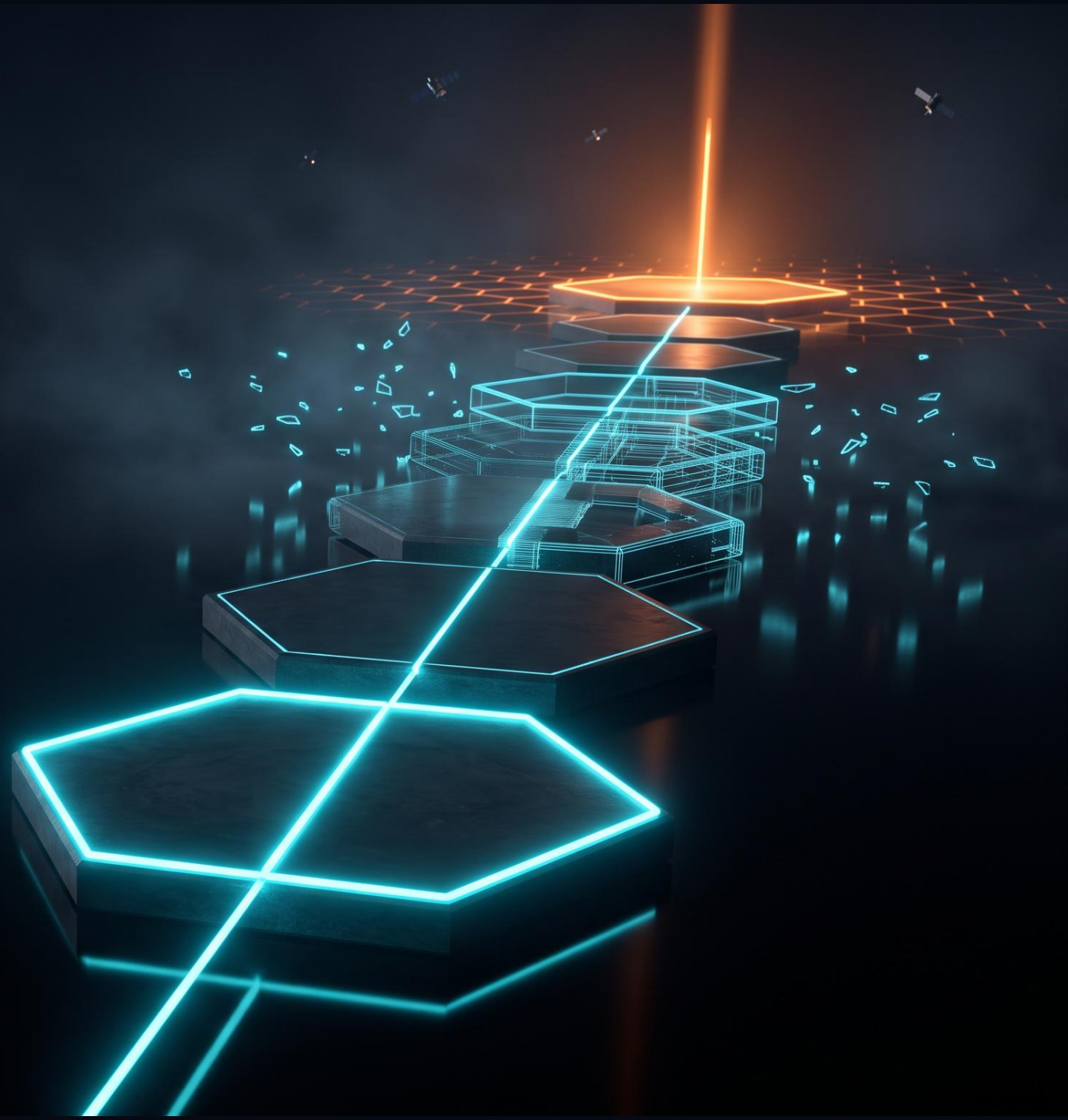
Beyond about 5000 stations

A message bus between adapters and detectors, evidence in object storage, database partitioned by region.

The three-record contract is what keeps stage 3 from being a rewrite.

Development plan

Milestones, validation and risks



Eight milestones, 12 weeks to pilot start

M0 Foundations

Login, network and station registry, CI, tested backups

1 week

M1 First stream to first event

ROMPOS over NTRIP; C/N0 and outage events on a map

2 weeks

M2 Receiver-native inputs

OEM7 and SBF streams; RF and spoofing detectors

2 weeks

M3 RINEX and push ingestion

SFTP, POST and archive fetch; files deleted after use

1.5 weeks

M4 Correlation and alerting

Cross-network incidents; email, webhook, Telegram

1.5 weeks

M5 Portal and public map

Invited EUPOS members onboard; coarse public map

2 weeks

M6 Edge agent and scale

Agent behind firewalls; 1000 simulated stations for 72 h

2 weeks

M7 Pilot

ROMPOS and two other EUPOS networks for a month

4+ weeks

Durations are estimates for one developer with AI assistance.

No detector ships unmeasured

1. **One thin slice first**

   A real ROMPOS stream producing a real event on a map before any second input format

2. **Replay before release**

   Each detector runs against recorded data with known outcomes; hit and false-alarm rates are written down

3. **Versioned configuration**

   Thresholds live in the database; events record the version that produced them

4. **Honest documentation**

   Docs describe only what exists

Validation data

- GeoVeil OEM7 history with receiver spoofing flags
- SeptoVeil SBF captures from ten receivers
- Kraken field campaigns near Constanța, June to September 2026
- EUREF station COST, 8 April 2026, as RINEX
- Quiet ROMPOS weeks, for the false-alarm rate

Main risks and the plan's answers

Risk	Answer
C/N0-only detection is too noisy on some receivers	Per-station baselines, a majority-of-satellites rule, and calibration per receiver family during the pilot
Operators will not open firewalls or share caster logins	Edge agent and push paths
Python decoding is too slow at 1000 stations and 1 Hz	Decode only C/N0 fields; sampling interval per network; load test in M6; Rust decoder as fallback
Receivers are not configured to send the needed data	Stream state names what is missing; a checklist per receiver family
A single server is a single point of failure	Edge agents buffer; backups are tested; a second host is a deployment change

Decisions needed to start

1. **Evidence retention**
   One year, or multi-year like the metrics

2. **EUPOS agreements**
   Do they cover sharing interference data, or is an annex needed

3. **Hosting and administration**
   Which body hosts the server and acts as platform admin

4. **Trimble spectrum input**
   In the first year, or when a Trimble network joins

Next step: start M0, foundations.