

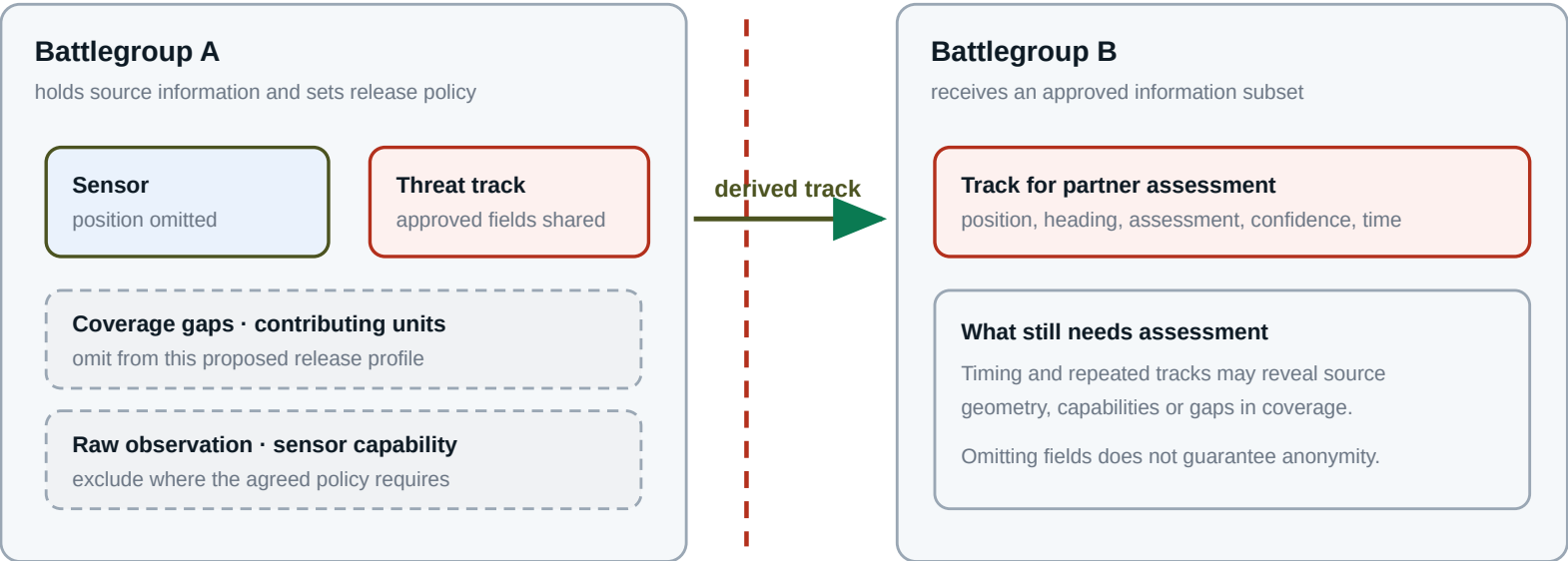
Sharing useful information with controlled disclosure

Limit unnecessary source detail while providing a partner with useful warning. Assess both released fields and what can be inferred.



THE SITUATION

Example release profile: share the track



RELEASE BOUNDARY

ILLUSTRATIVE FIELD SELECTION — NOT A GENERAL REDACTION IMPLEMENTATION

Include if approved

- ✓ Reported threat position
- ✓ Heading, speed, track history
- ✓ What it is assessed to be
- ✓ Confidence in that assessment
- ✓ When it was observed
- ✓ Its releasability label
- ✓ A global event ID for dedupe

Omit by policy

- ✗ Where your sensor is
- ✗ What sensor, and its range
- ✗ The raw observation itself
- ✗ Which units contributed
- ✗ Where you have no coverage
- ✗ Your confidence workings
- ✗ Any credential or key detail

Release the information needed for the agreed purpose. Review combinations of observations as well as individual fields before claiming source protection.

SEVEN DESIGN CHECKS — NOT A CLAIM OF IMPLEMENTATION ORDER OR END-TO-END DEPLOYMENT

1

Is the peer workload acceptable?

Check evidence against the agreed workload policy and bind it to the intended peer.

2

Is this peer authorised?

Bind the peer region to an authenticated identity and the agreed sharing policy.

3

Is the message well formed?

Envelope and typed payload are validated against the published schema.

4

Is this releasable to them?

Classification and releasability must permit transfer to this specific peer. This is the disclosure decision.

5

Have we seen it before?

Suppress repeats within the retained event history; define restart and side-effect rules.

6

Is anything missing?

Per-origin sequence numbers detect a gap and say so, instead of quietly claiming a complete picture.

7

Does it make sense?

Type-specific merge policy accepts or rejects the state transition.

Assurance and release policy are separate checks

Workload appraisal establishes software assurance under a policy; authorisation determines which partner may receive which information. Neither decision automatically supplies the other.

The implemented replication session filters whole events, then forwards accepted envelopes.

It does not provide a general field-redaction or inference-prevention service.

Keeping content secret from relays requires an endpoint-encrypted path and appropriate keys.

Evidence and residual disclosure

Filtering, duplicate handling and replay have supporting tests within one process.

That does not establish a full protected exchange between deployed formations.

Encryption does not hide all traffic metadata. Repeated observations may reveal information even when each individual message is releasable. Retained replay state is memory-only.

This diagram is a proposed release profile, not evidence that all source data is always withheld.