

A path, not a verdict

Today a finding gets a verdict on day one, with the least information it will ever have. **A path lets the call change when the facts do.** First pick the pattern, then walk the finding through it.

HYPOTHESIS

The pains are real. The paths are my hypotheses.

As far as I know, none of this is running end to end in the wild yet. Test it small and fast, and change it as you learn.

CACHED THE FIRST PULL: ALREADY LIVES SOMEWHERE, MINUTES

- How sensitive it is
- Exposed or not
- Who owns it
- What's installed
- Fixed already?

COSTLY REAL WORK, DAYS

- Does the code reach it?
- How big is the fix?

Quick exit **OURS**

DRIVEN BY
Can it come off the list fast?

- 1 Fixed already?
- 2 Blocked already?
- 3 Exposed?
- 4 Code reaches it? **COSTLY**
- 5 The call

Under attack

DRIVEN BY
Is it being used against someone now?

- 1 Exposed here?
- 2 Block it today
- 3 Name the owner
- 4 Targeted patch **COSTLY**
- 5 Proven fixed?

One fix, many places

DRIVEN BY
Is it in a shared piece?

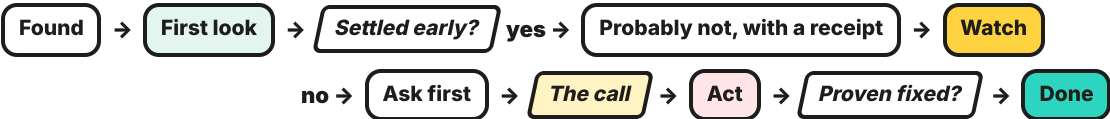
- 1 Fixed in the shared piece?
- 2 Who owns it?
- 3 Exposed where?
- 4 Roll out in waves **COSTLY**
- 5 Proven everywhere?

No name yet

DRIVEN BY
Nobody outside knows it exists.

- 1 Exposed, sensitive?
- 2 Where else? **COSTLY**
- 3 Block it?
- 4 Reproduce it **COSTLY**
- 5 The call

THE QUICK EXIT, STOP BY STOP



↻ **A claim expires:** a port opens, a feature ships, and the finding goes back to the first look on its own.

↻ **Not proven yet:** back to act. Done means evidence from a system, not a closed ticket.

"THEY WON'T OPEN UP." THREE LANES

- DOORS** If the system can change: doors in the walls. The most lift.
- MIRROR** If it can only bend: a one-way mirror lets security see in early.
- WALLS** If nothing moves: each team runs the path for what it owns.

How you run a lane is a separate dial: by hand, bootleg scripts, or agents (which need tools, a shared dictionary and access rules).

EVERYONE'S PART

Security	Runs the lookups, says how bad it could be, checks the evidence
App team	Is it called? Sizes the change. Changes the code
Platform	Fixed or blocked already? Keeps the record that proves it
The business	How sensitive. Owns the call, or names who does
A lookup service	Looks things up, drafts the receipt, watches for expiring claims