

# The seven questions

Most critical findings aren't. The scan can't tell you which, and almost none of the answers live with security. **Qualify with prejudice:** start from "probably not," and make every finding earn its place.

THE SCAN

9.8

→

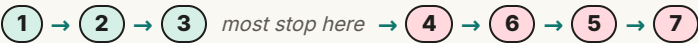
AFTER 7 Qs

3.7

Same finding, now under the bar for acting today. **The questions tell you if the worst case is your case.**

| 1-3 Is it real?                                                                                                                                         |                                                                                        | Mostly cheap lookups. Most findings stop here.                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| 1                                                                                                                                                       | <b>Has it already been fixed?</b> <span>CHEAP LOOKUP</span>                            | WHO KNOWS<br><u>Platform teams and vendors</u>                  |
| Vendors often fix a flaw without changing the version number. On paper it still looks vulnerable.                                                       |                                                                                        |                                                                 |
| 2                                                                                                                                                       | <b>Is something already blocking the way in?</b> <span>CHEAP LOOKUP</span>             | WHO KNOWS<br><u>Platform and network teams</u>                  |
| A setting, a firewall rule, a feature that's turned off.                                                                                                |                                                                                        |                                                                 |
| 3                                                                                                                                                       | <b>Can anyone reach it, and is anyone trying to?</b> <span>CHEAP LOOKUP</span>         | WHO KNOWS<br><u>App and platform teams; threat intelligence</u> |
| Code that never runs. A door nobody can get to. A flaw nobody uses yet, or one being used right now.                                                    |                                                                                        |                                                                 |
| 4 Does it matter?                                                                                                                                       |                                                                                        | The business decides.                                           |
| 4                                                                                                                                                       | <b>How sensitive is it, if it's exposed or if it's down?</b> <span>NEEDS PEOPLE</span> | WHO KNOWS<br><u>The business, data owners and operations</u>    |
| Exposed: the money, customers and data it can reach, and the regulator. Down: who depends on it, whether their work can wait, and when it matters most. |                                                                                        |                                                                 |
| 5-7 Can we act?                                                                                                                                         |                                                                                        | How, when, and who.                                             |
| 5                                                                                                                                                       | <b>Can we change it safely, and how fast?</b> <span>NEEDS PEOPLE · ASK LAST</span>     | WHO KNOWS<br><u>App teams and operations</u>                    |
| The most expensive question. It pulls a team off their work to size a fix. Save it for findings that have earned it.                                    |                                                                                        |                                                                 |
| 6                                                                                                                                                       | <b>Should we retire it instead?</b> <span>NEEDS PEOPLE</span>                          | WHO KNOWS<br><u>The business and the app owner</u>              |
| Sometimes the best fix is turning it off.                                                                                                               |                                                                                        |                                                                 |
| 7                                                                                                                                                       | <b>Who would actually do the work?</b> <span>NEEDS PEOPLE</span>                       | WHO KNOWS<br><u>The org chart, sort of</u>                      |
| If nobody owns it, it doesn't get fixed, no matter how critical it is.                                                                                  |                                                                                        |                                                                 |

ONE WAY TO ORDER THEM



- Being attacked now:** 3 first. Block it today, name an owner, patch, then check.
- Same flaw in 300 apps:** find the shared piece. One rebuild beats 300 tickets.
- Old app, no team:** 7 first. Retire it, wrap it, or get a fix from the vendor.
- Crown jewels:** 4 first. A higher bar to take it off the list.
- A model, not *the* model. Write yours down so the same facts get the same answer, and change it when it's wrong.

KEEP THE RECEIPTS

RECEIPT

FINDING

QUESTION

ANSWER

SOURCE

WHO · WHEN

DECISION

CALL BY

**Evidence, not someone's word.** Other teams supply it. Whoever makes the call still owns it. The trail also shows where the time really goes.