

BUSINESS

FILLED IN BY

DATE

REVIEW AGAIN ON

1 What we don't sort byLesson 1

2 The gateLesson 2

The label or score on an alert (Critical, High, 9.8) does not decide what we fix first.

OUR RULE:

Q1 Is someone actually using this attack right now? (CISA KEV list, vendor says so, IT provider says so, or EPSS 0.9+)

Q2 Can a stranger on the internet reach the thing with the flaw?

Yes to both: **P1** fix within 24 hours.

DECIDED BY:

WHO'S CALLED, HOW:

☐ EMERGENCY FIXES PRE-APPROVED WITH IT PROVIDER · AGREED ON:

3 Our top systemsLesson 3 · money, email, customer data, the thing we can't open without

SYSTEM	WHAT BREAKS IF IT'S DOWN OR STOLEN	OWNER	FIXES IT

The order: Box 1 is always P1. Otherwise Box 2 is P2, Box 3 is P3, Box 4 is P4, and a top system moves a problem up one level. Work P1 first. Inside a level, a top system first, then the score.

4 Fix deadlinesLesson 4 · the clock starts when a problem is confirmed and assigned

P1	Box 1	24 hours
P1	Box 2 on a top system	72 hours
P2	Other Box 2; Box 3 on a top system	30 days
P3	Other Box 3; Box 4 on a top system	90 days
P4	Other Box 4	180 days

MISSED DEADLINES GO TO:

24-HOUR COVERAGE (HOW):

AGREED (SIGNATURE):

Fixed means updated, setting changed, taken off the internet, or removed. A barrier in front can lower a problem one level, never out of Box 1.

5 ExceptionsLesson 4 · P1/P2 signed by the owner · expired means overdue again

WHAT ISN'T BEING FIXED	WHY	WHAT WE'RE DOING INSTEAD	SIGNED	EXPIRES