

10 questions to find where your time goes during an incident

Answer them thinking about the last real incident you had, not about how the process is supposed to work. The ones you struggle to answer usually point to where the time goes.

DETECT

- 1 Did you find out from an alert, or because someone complained?**
If a user or a teammate told you, the clock had been running for a while before you knew.
- 2 Did the alert say what was broken, or only that something was wrong?**
A symptom alert, like "high latency", forces you to start investigating from scratch.

DIAGNOSE

- 3 How long did it take from the alert to knowing what failed?**
Not until it was fixed, until you knew the cause. It is the stretch almost nobody measures, and the one that drags on the most.
- 4 How many tools did you have to open to piece the context together?**
Every jump from one tab to another costs time, and context gets lost along the way.
- 5 Could you link the failure to the last change within a few minutes?**
Many incidents arrive right after a deployment or a configuration change. Knowing what changed cuts the search short.
- 6 Did it take one specific person to understand what was going on?**
If the diagnosis depends on who is on call, it depends on luck.

ACT

- 7 Was the fix written down anywhere?**
A runbook nobody can find at 3 a.m. might as well not exist.
- 8 Is it clear what can be done without asking for permission, and what cannot?**
If every action is debated on the spot, time slips away exactly when you need it most.
- 9 How did you check that it was really fixed?**
Without a clear check, the incident can come back and you start all over again.

LEARN

- 10 Was it the first time it happened?**
If it had happened before, the costliest time is not this incident, it is all the ones still to come.

Now what? Start with the questions you struggled to answer. If you want to go through them with your real case, send me a DM on Instagram or LinkedIn.