Incident Management Roles

Last updated by | Justin Bryant | Aug 25, 2023 at 9:24 AM PDT

Incident Management Roles

An incident is no time to have multiple people doing duplicate work. It's also a terrible time to have important tasks ignored, all because everyone thought somebody else was working on it. Incidents are made worse when incident response team members can't communicate, can't cooperate, and don't know what each other is working on. Work gets repeated, work gets ignored, customers and the business suffer.

That's why effective incident response teams designate clear roles and responsibilities. Team members know what the different roles are, what they're responsible for, and who is in which role during an incident.

Contents

First Responder

- The person/team that receives the alert, assesses the impact and if it is a P1/P2 starts the incident management process This person/team may be the one that can resolve the issue or supports a team that is escalated to.

Incident Manager

- Each incident is driven by the incident manager (IM) *(A.K.A "Incident Commander" in DataDog)*, who has overall responsibility and authority for the incident. This person is indicated by the assignee of the incident issue. During a major incident, the incident manager is empowered to take any action necessary to resolve the incident, which includes paging additional responders in the organization and keeping those involved in an incident focused on restoring service as quickly as possible.
- The IM can also devise, and delegate roles as required by the incident, for example, multiple tech leads if more than one stream of work is underway, or separate internal and external communications managers.
- In complicated or large incidents, it's advisable to bring on another qualified incident manager as a backup "sanity check" for the IM. They can focus on specific tasks that free up the IM, such as keeping the timeline. We use the chat room's topic to show who is currently in which role, and this is kept up to date if roles change during an incident.

Communications Manager

- A person familiar with public communications, possibly from the customer support team or public relations. Responsible for writing and sending internal and external communications about the incident.
- Collect customer responses, interface with executives and other high-level stakeholders.
- May only be needed when there are potential PR related concerns

---

Tech Lead

- The tech lead is typically a senior technical responder. They are responsible for developing theories about what's broken and why, deciding on changes, and running the technical team during the incident. This role works closely with the incident manager.
- Communicate updates to incident manager and other team members, document key theories and actions taken during the incident for later analysis, participate in incident postmortem, page additional responders and subject matter experts.

Customer Support Lead

- The person in charge of making sure incoming tickets, phone calls, and tweets about the incident get a timely, appropriate response.
- Pass customer-sourced details to the incident-response team.

Scribe

- A scribe is responsible for recording key information about the incident and its response effort.
- Maintain an incident timeline, keep a record of key people and activities throughout the incident.