Google

Incident Management

SREDay - Warsaw - 2026-10-22

Joshua Borkowski-Clark
Senior Site Reliability Engineer



Site Reliability Engineering

sre.google

Basics

- The premise of incident management is to **respond to an incident in a structured way.**

- Large-scale incidents can be **confusing**; a structure that teams agree on beforehand can reduce chaos.

- Formulating rules about how to communicate and coordinate your efforts **before disaster strikes** allows your team to concentrate on resolving an incident when it occurs.

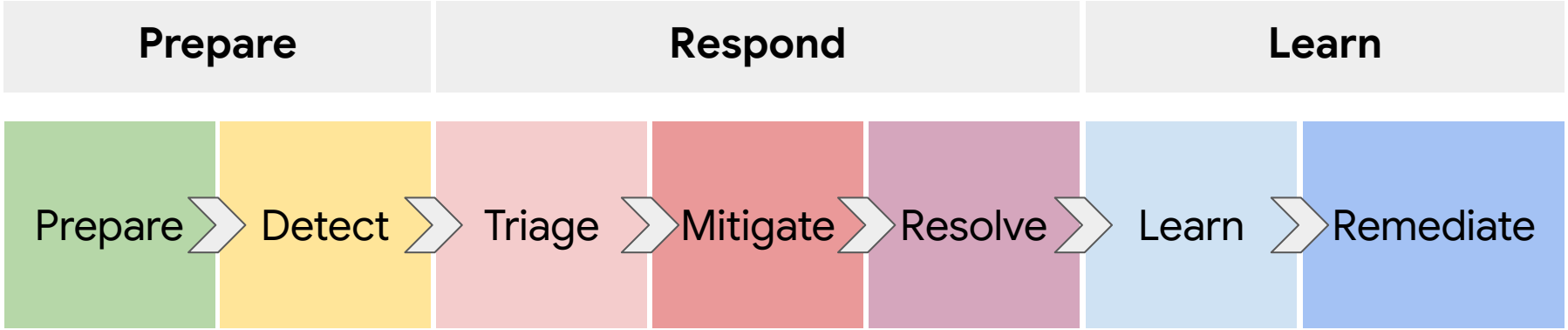
Agenda

1. Incident Lifecycle
2. Incident Command System (ICS)
3. How to Manage an Incident



Incident Lifecycle

Incident Lifecycle





Incident Command System

How to respond

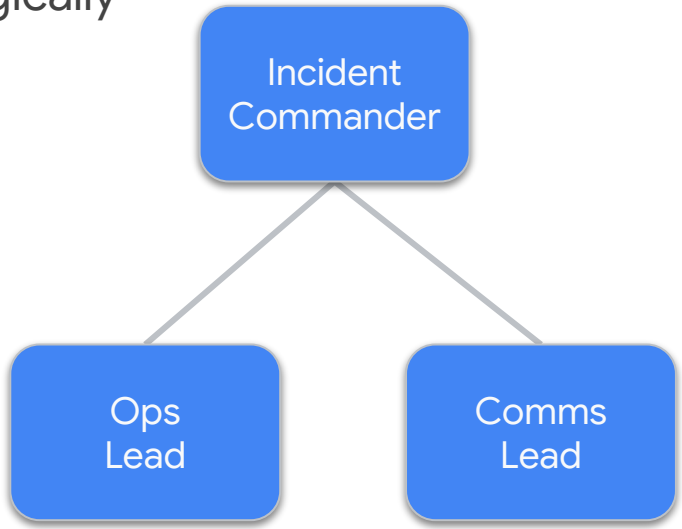
*To handle an issue that has been **escalated** and requires an **immediate**, **continuous**, and organized **response** to address it.*

Why

- **Familiarity**: We all use the same "language"
- **Structure**: We all know what to expect and who is who in an incident
- **Scalability**: Can address smaller and huge, planetary events
- **Transferability**: Facilitates transfer of responsibility between people and teams (handoffs)

Core Roles

- The **Incident Commander (IC)** thinks strategically
  - A professional question-asker
  - Assigns objectives
- The **Operations (Ops) Lead** is tactical
  - The do-er; How to get the objectives done
- The **Communications (Comms) Lead**
  - Keeps stakeholders informed.
  - Answers questions
  - The IC sometimes does this too.



“Three Cs” of Incident Management

- **Coordinate** response effort
- **Communicate** between incident responders, within the organization, and to the outside world
- Maintain **command** over the incident response

Key skills: Command, Control, Communications

Make decisions and keep the teams focused on the same goals

- Each role needs to take charge and drive their part of response
  - The Incident Commander has overall responsibility
  - Each person leading a subteam owns and drives their specific part
  - Clear line of authority
- **Incident Commander** specifics:
  - Build a response team, keep track of who is doing what
  - Focus on the strategic needs
    - “Get the service running again by mitigating X first, then Y”
    - “Minimize customer impact by fixing the easy 90% first, then the tough 10%”
    - “We have to drain cluster X first”
  - Make timely decisions

Key skills: Command, Control, Communications

Know what is going on. Coordinate people. Be continuously aware.

- Somebody needs to coordinate the response so that the responders are working in concert
  - The Incident Commander does this for the entire team
  - Each person leading a subteam does this for their subteam
  - Manageable Span of Control

- **Incident Commander** specifics:
  - Make sure responders work towards the appropriate goals
  - Make sure executives & others don't begin parallel responses
  - Coordinate flows of information between responders

Key skills: Command, Control, Communications

Take notes, be clear, and ensure everybody has the same context.

- Define a consistent communication/coordination process, manage it, and keep it from going off track

- Good communications:
  - Ensures responders and external stakeholders have the same set of facts
  - Prevents rumors from becoming the official state
  - Ensures smooth interactions with affected customers & others

Communications is critical to success in an incident, and often affects even Command and Control!



How to Manage a Incident

How To: Declaration

- Establish primary communications channels
  - IRC, Chat, Video Conference, Phone Bridge, etc
- Establish tracking mechanism
  - Create shared "working" document, Tooling
- Explain what we know
  - "We have no idea" is a valid incident state!
- Assign roles as needed
  - Use "team names" to document participation and who's who, if time permits
- Think about the incident title
  - That's the first thing people will read to decide if the incident affects them

How to: Coordination

- IC sets up the response
  - Identifies Leads and gives them objectives
- Leads stay tightly in sync - talk often
  - Structure your communications
  - Use shared "working" document to keep detailed state
  - Good notes can help ramping up extra people
- (if necessary) Assign a Scribe to take notes
  - You think you can IC and take notes but you usually can’t
- Over-communicate

How to: Communicate

- Keep Communication Central
  - Plan in advance!
  - Sync side conversations back to the main channel (Scribe)
- Track
  - Keep a work log, and exec summary
  - Clear, concise, no jargon. Include enough detail.
  - Limit confidential information & avoid PII
- Delegate **Comms Lead** before you're overloaded,
  - Avoid doing Incident Commander AND Communications

How to: Handovers

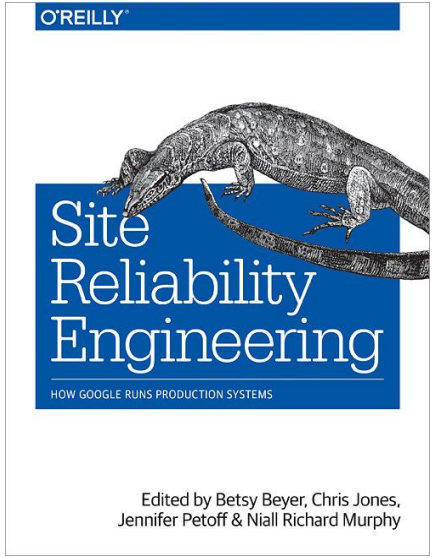
- **Why**
  - Bigger incidents can take a while
  - Responder fatigue & point of diminishing returns
  - Responders feel out of their depth and are unable to be effective
  - Scope changed, different expertise required

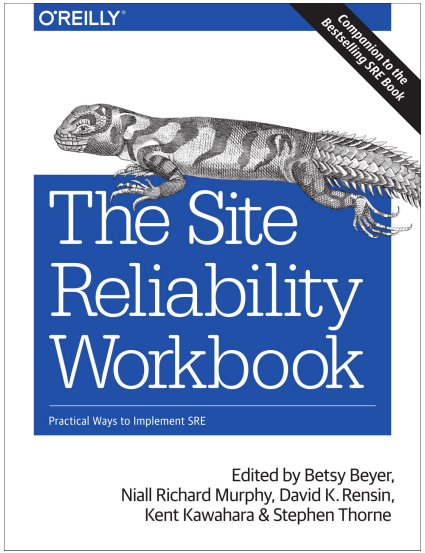
- **How**
  - Be explicit - Handovers are never implicit
  - Consider using two phased handover
  - Plan the handover ahead of time

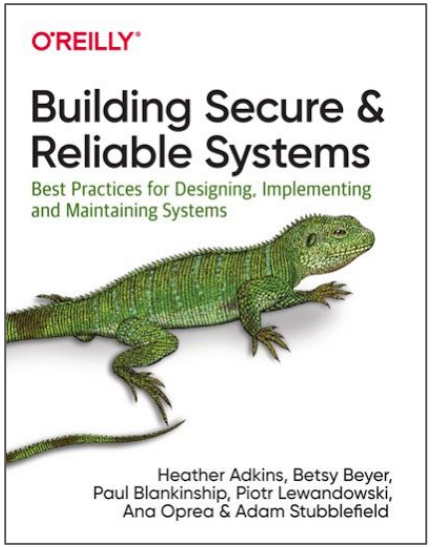
How do you get good at this?

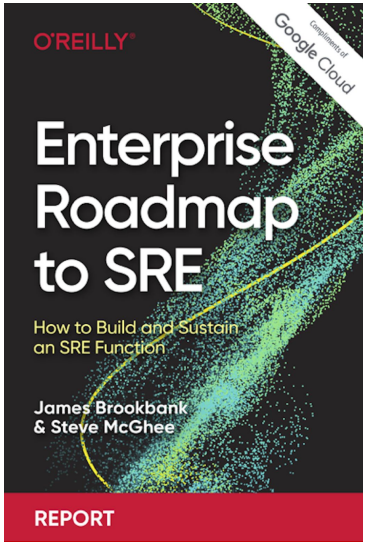
- Prepare an Incident Management Plan
- Run trainings (for all stakeholders)
- Practice
  - Wheel of Misfortune
- Further Reading

Follow us on Twitter: @googlesre. Find Google SRE publications—including the SRE Books, articles, trainings, and more—for free at sre.google/resources.



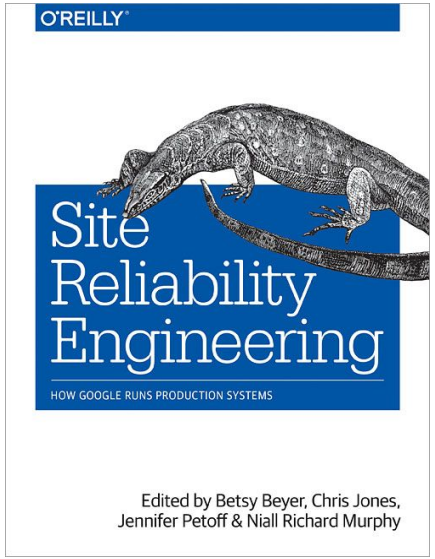


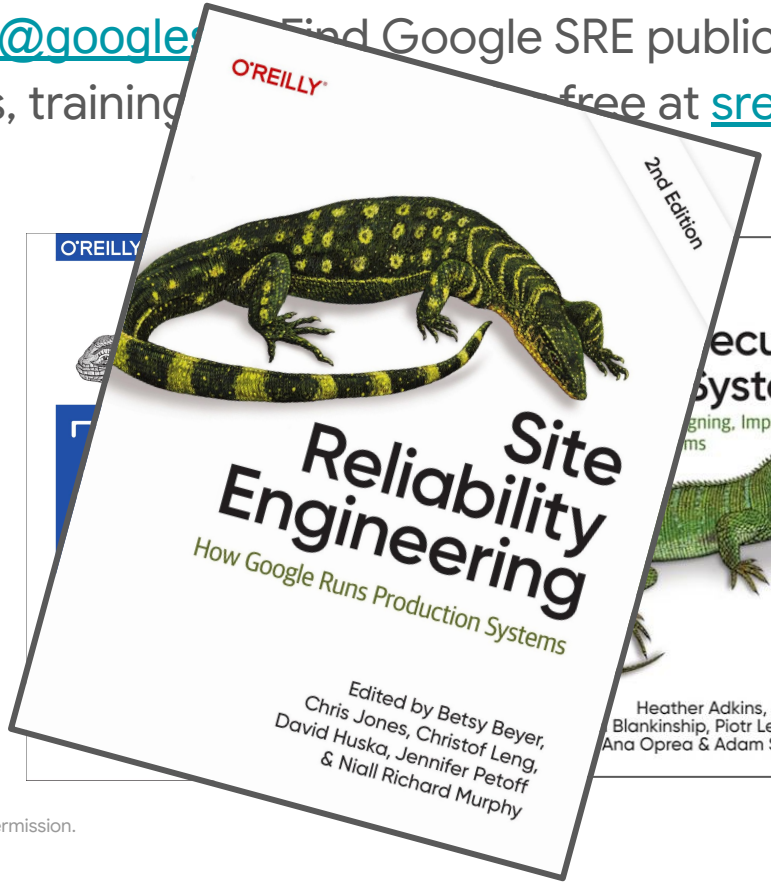


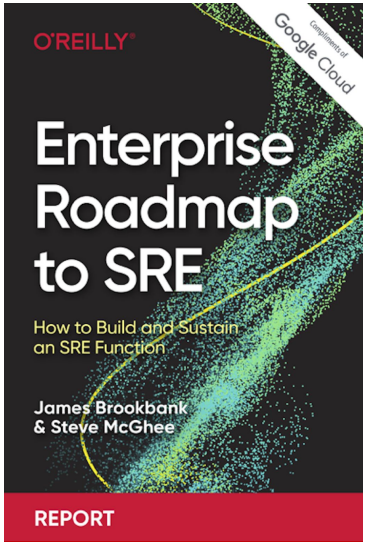


Book covers copyright O'Reilly Media. Used with permission.

Follow us on Twitter: @google… Find Google SRE publications—including the SRE Books, articles, training… free at sre.google/resources.







Book covers copyright O'Reilly Media. Used with permission.

Thank you

