{mthree}

Postmortems

Site Reliability Engineering

Overview

In this module we will learn what a postmortem is and how blameless postmortems better serve to goal of continuous improvement.

Learning Objectives

- Define postmortem
- Reasons for postmortems
- Explain the blameless culture

What is a Postmortem?

- Part of the incident response process
  - Detect
  - Respond
  - Resolve
  - LEARN
- According to SRE

  A postmortem is a written report of an incident, its impact, the actions taken to mitigate or resolve it, the root cause(s), and the follow-up actions to prevent the incident from recurring.

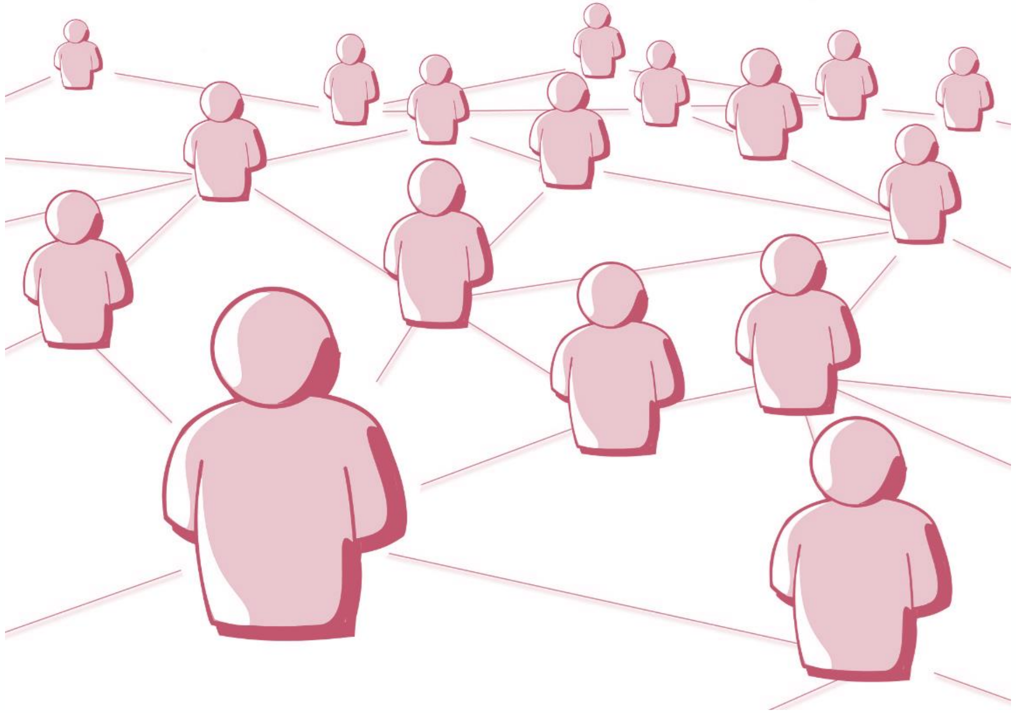
Postmortem Objectives

- ↘ Failure is an opportunity for improvement
- ↘ Learn
  - >>> What went right?
  - >>> What went wrong?
  - >>> Where did we get lucky?
- ↘ Follow-up actions

{mthree}

To Blame or Not to Blame

- Human tendency is to look for who to blame.
  - >>> Blameless postmortems don't work. Be blame-aware but don't go negative (techbeacon.com)
- It is not the person that failed. It is the system that failed.
  - >>> If the system is not correct, the incident WILL happen again.
  - >>> Focus on the system to make a repeat failure less likely.
- Person is now the expert in how to correct the system.



{mthree}

Blameless Postmortem Process

- Embrace risk
  - >>> Incidents are a learning opportunity
  - >>> Learn from mistakes more than successes
- Capture information during incident response efforts
- Focus on proactively preventing the incident
  - >>> Watch for the tendency to point fingers
- Use a standard format for postmortem reports

{mthree}

Problem Statement

- What was the problem?
- First statement of the problem may not be accurate
  - What lead up to the incident?
  - What unexpected result occurred as a result of changes to the system?
  - Why did the incident occur?

Impact Statement

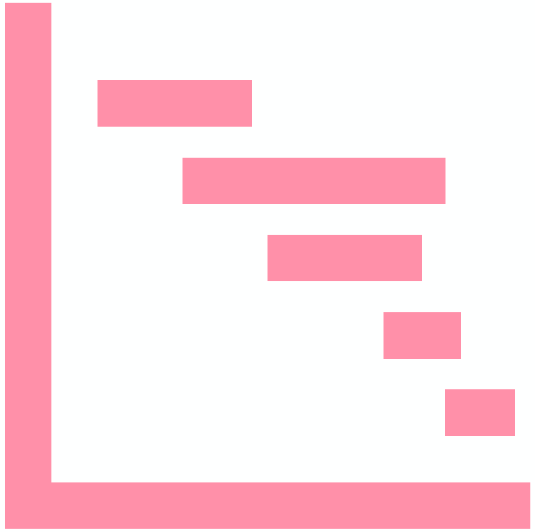
- What was the impact?
- Who was impacted?
  - Internal
  - External
  - Drawn into the response
- What percentage of the customers were impacted?
- How much income was lost?
- What regulatory or legal consequences were incurred?

Detection

- Who detected the incident?
- When did the incident start?
- When did the incident become known?
  - Measure mean time to detection (MTTD)
- What would improve MTTD?

Timeline

- Tasks completed during recovery
- Mean time to recovery (MTTR)



{mthree}

Root Cause(s)

- How to prevent reoccurrence?
- Focus on root cause: do not settle for proximate cause.
  - Use Five Whys
    - Why did the ship sink?
      - Proximate Cause: Because it filled with water and no longer had any buoyancy.
    - Why did it fill with water?
      - Proximate Cause: Because it hit an iceberg that ripped the hull and flooded numerous water-tight compartments.
    - Why did it hit an iceberg?
      - Ultimate Cause?

Corrective Actions

- Tasks and actions to be done
  - Deadlines
  - Assignment of responsibility
  - Follow-up
- Automate fix?
  - May need to be manual
  - May need to be referred to development team

Share the Postmortem

↘ The purpose of the postmortem is to learn.

- >>> Must be shared
- >>> Must be easily located in the next emergency
- >>> May need supporting documents which are also shared

{mthree}

Summary
Q&A

{mthree}

References

- ↘ Blameless PostMortems and a Just Culture – Code as Craft
- ↘ Google SRE – Postmortem Culture
- ↘ Google SRE Workbook – Postmortem Culture: Learning from Failure