Postmortem Template

Title

[Write three-to-five-word description of the incident.]

Incident description

[Write two or three sentences describing the incident. Make it understandable to management and business stakeholders.]

How was the incident detected?

[Describe how the incident was detected. Include who, what, where, why, and how.]

How was the incident stabilized?

[Describe how the incident was stabilized. Include who, what, where, why, and how.]

How were customers affected?

[Describe which customers were impacted and the exact impact. Include who, what, where, why, and how. If customers reported issues, link those in here as well.]

How were employees affected?

[Describe how employees were affected. Include who, what, where, why, and how.]

Timeline

[Everything should be in the same time zone.]

Pre-incident

- 01/01/2019 00:00:00 UTC [Add relevant information in chronological order.]

Incident

- 01/01/2019 00:00:00 UTC [Add relevant information in chronological order.]

Post-incident

- 01/01/2019 00:00:00 UTC [Add relevant information in chronological order.]

Sources

- [Links to monitoring, dashboards, logs]

What went well

1. [Identify things that worked well to fend off for help resolve the incident. Each should be brief.]

Contributing causes

1. [Identify factors that caused the incident, delayed its detection, or delayed its resolution. Each should be brief.]

Corrective actions

1. [Describe what changes have or will be taken to prevent or mitigate this or similar incidents in the future. Changes listed here include but are not limited to testing, alerting, monitoring, logging, backups, and anything else related. Doing postmortems is an evolving practice inside the organization, so changes to the postmortem process itself should be included as well. Add relevant links to these items tracked in ticketing systems.]

Metrics

When did the incident begin?

[first errors recorded]

When did the incident end?

[service restored]

When did we detect the incident?

[alert fired/customer notified]

Time to detect

[start_time – detect_time]

Time to resolve

[start_time – end_time]