

# Hello Conf42 DevOps 2025 🙌





PagerDuty

# Don't Panic! Effective Incident Response

---

Daniel Afonso @danieljcafonso

January 23, 2025





# Daniel Afonso

**Senior Developer Advocate at PagerDuty**

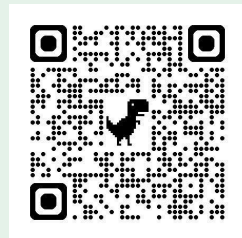
**Instructor at Egghead.io**


**Author of “State Management with React Query”**

dafonso@pagerduty.com

<https://community.pagerduty.com>

**@danieljcafonso**





Incident Response is an **organized**  
approach to addressing  
and managing an incident





1

Use systematic learning and improvement

2

Mobilize and inform **only** the right people at the right time

3


Automate everything you can

A narrow, cluttered alleyway in Japan, likely a traditional market or residential street. The scene is filled with various signs, including a large blue sign with white Japanese characters '酒場' (Bar) and 'ナベサン' (Nabe-san), a white sign with red text 'スナック ガルシア' (Snack Garcia), and a red sign with white text '一歩' (Ichibu). There are also smaller signs for '花園一番街' (Kawana Ichiban-gai), 'スナック ガルシア', 'GNETTO', and '深夜' (Shinya). The alleyway is lined with buildings, and the ground is paved. A utility pole with many wires is visible on the left. The overall atmosphere is one of a busy, traditional Japanese street.

Replace **chaos** with **calm**

Photo by sugar jet



A photograph of a forest fire. The scene is dark and smoky, with bright orange and yellow flames rising from the trees. The smoke is thick and grey, filling the air. The trees are mostly birches, with their white bark visible. The ground is covered in dark, charred wood and some green moss. The overall atmosphere is one of destruction and danger.

An **incident** is any unplanned disruption or degradation of service that is actively affecting customers' ability to use the product



A large, intense fire with bright orange and yellow flames. In the foreground, the silhouettes of several people are visible, appearing to be on a structure or platform, possibly engaged in firefighting or rescue work. The background is dominated by the fire, which is very bright and fills most of the frame.

A **major incident** requires a coordinated response between multiple teams



Agree and **standardize on base concepts** to avoid confusion



NORMAL

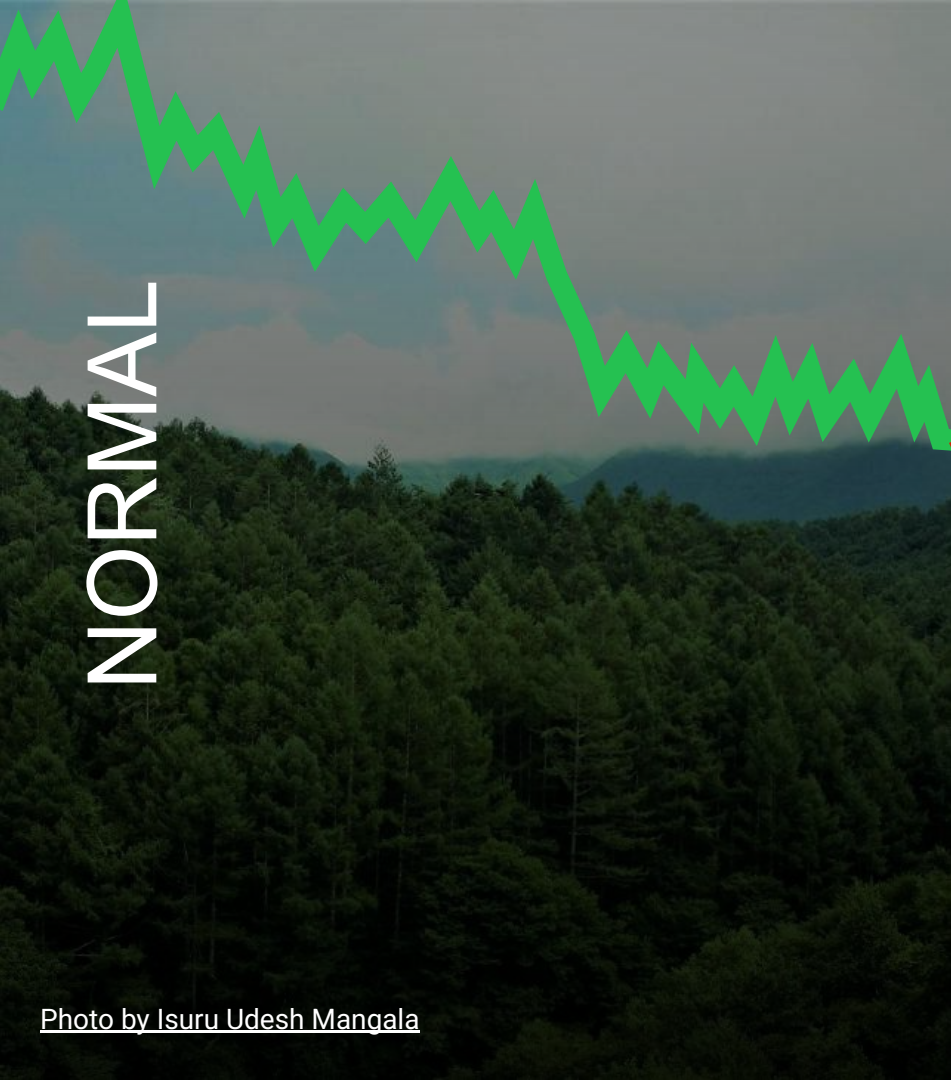


Photo by Isuru Udesch Mangala

EMERGENCY

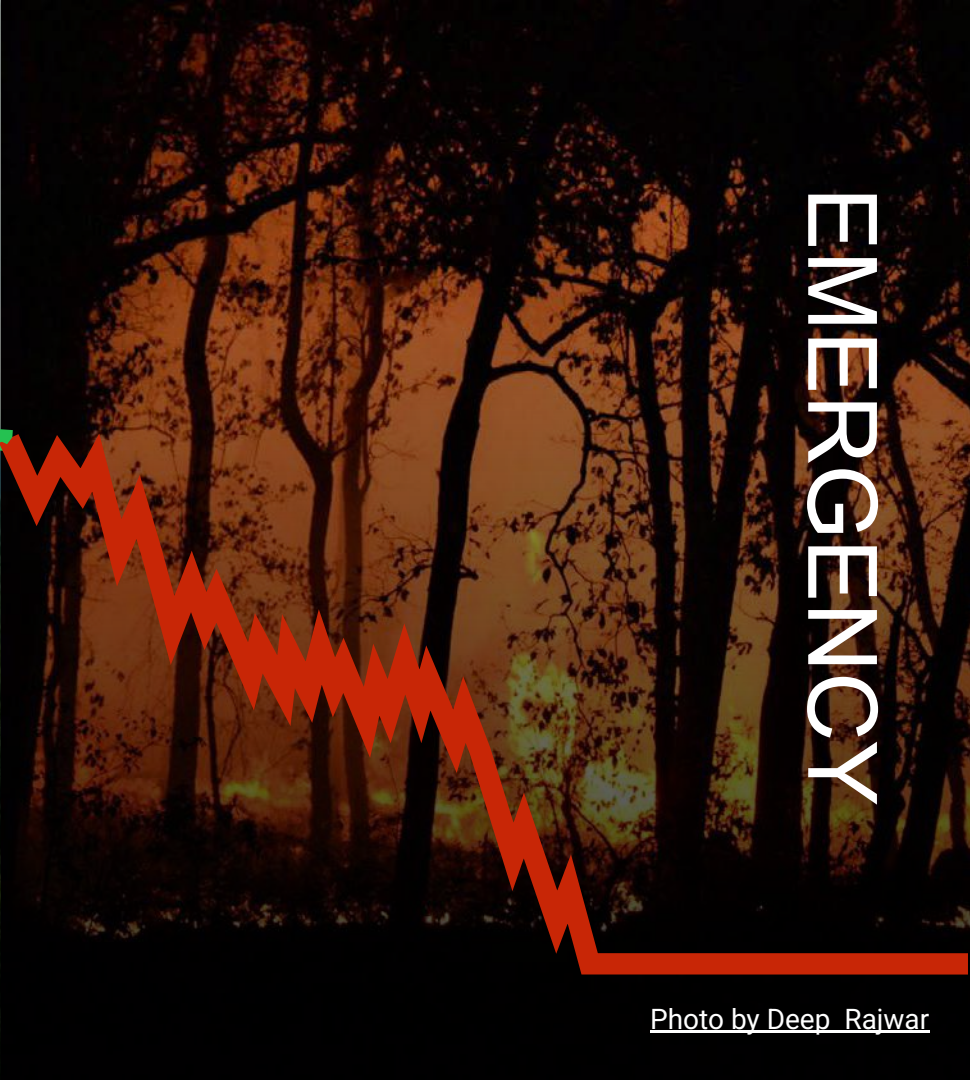


Photo by Deep Rajwar



**Metrics must be business  
related and actionable**



A red fire alarm pull station is mounted on a light-colored wall. The device is rectangular with a white pull handle in the center. The background is a plain, slightly textured wall.

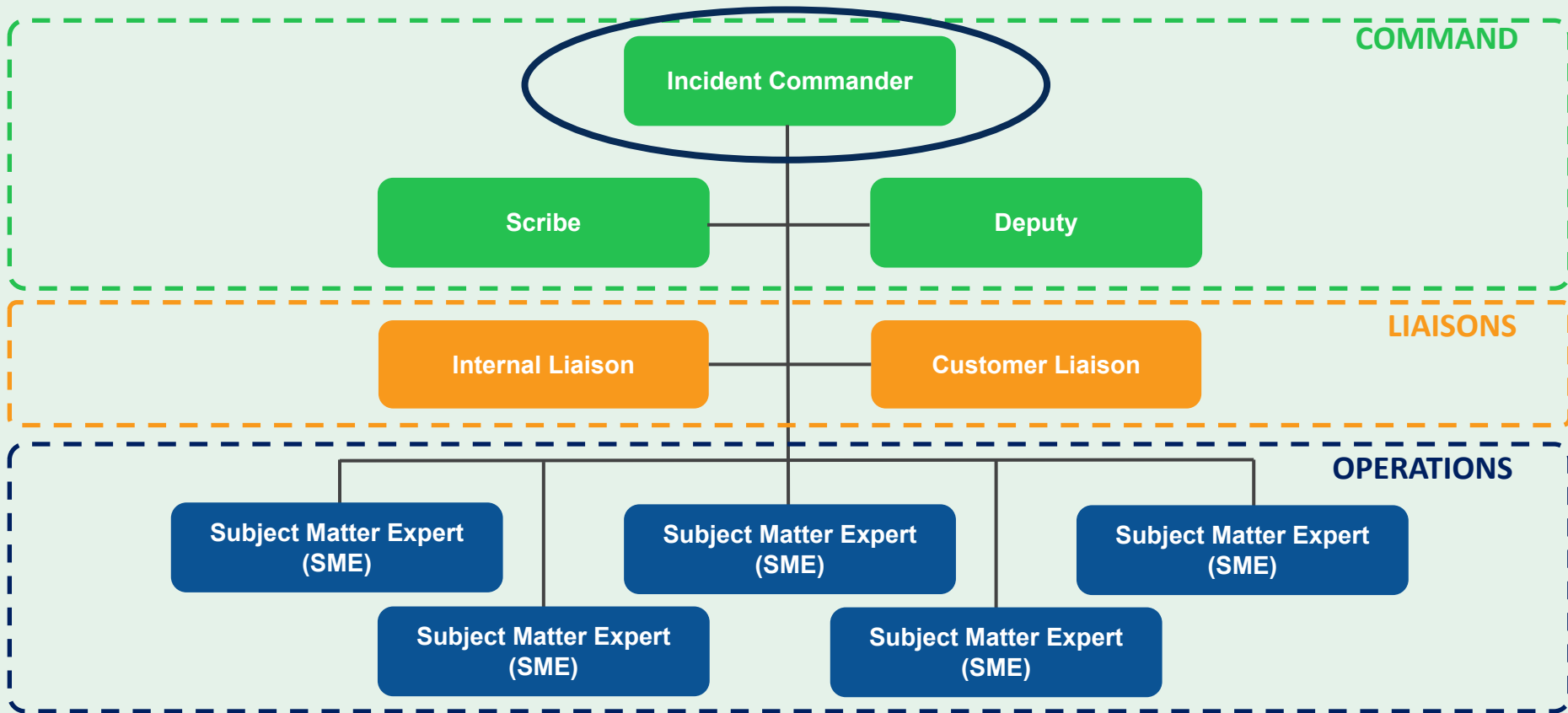
**Anyone** can trigger the Incident Response Process at any time

# The Four Steps of an Incident





# Roles of Incident Response





**How do I prepare** to manage  
incident response teams?



## Step 1

Ensure **explicit** processes and expectations exist and people are **trained**



## Step 2

**Practice** running major incidents as a team

A dark, moody photograph of a desk. In the foreground, an open notebook with lined pages is visible. A fountain pen lies on the left page, and a marker lies on the right page. The background is a dark, textured surface, possibly a desk or a wall. The overall lighting is low, creating a professional and focused atmosphere.

## Step 3

Find ways to **tune your processes**  
for your teams to work



# DAILY REPORT SCHEDULE

## Step 4

## Make Checklists



# Example Checklists



## Start of Incident: Mobilize Response

---

- Join the #incident-war-room and Zoom call
- Announce self as Incident Commander
- Acknowledge the incident
- Assign deputy
- Assign scribe
- Confirm liaison present
- Confirm SMEs present
- Run lic responders to get list of oncalls on Slack



## Incident Response Loop

---

- Size-up the situation
  - What's wrong?
  - Which systems are affected?
  - Is this affecting multiple systems?
  - What's the customer impact?
- Stabilize the incident
  - What actions can we take?
  - Was there a related change or deploy?



## Reminders during an Ongoing Incident

---

- Suggest people leave call if they are not required
- SME, Scribe, Comms handoff to avoid fatigue
- Incident Commander Swap
  - Ask deputy to take over
  - Summarize status
  - Announce change in command



## Incident Resolved

---

- Notify customers of resolution
- Scale down the response
  - Direct all follow up to #incident-followup
  - Announce end of incident call
- Resolve the PD incident
- Create the post-incident review
  - Assign review owner
- Send email to incident-reports@pd.com



## Step 5

Don't neglect the  
**post-incident review**



A close-up photograph of a person's feet wearing blue denim jeans and brown leather boots. The person is stepping on a yellow-painted curb. A large, thick, white, stringy substance is being pulled out from the sole of the boot, suggesting a slip-and-fall accident involving a spill. The background is a blurred outdoor setting with a road and trees.


# Incident Response **pitfalls** and **how to avoid them**

[Photo by Gratisography](#)

A man in a dark suit, checkered shirt, and striped tie pointing his right index finger towards the camera. The text "Executive Swoop" is overlaid in the center.

# Executive Swoop

Photo by Lukas



## **Executive Swoop one**

*“Let’s try and resolve this in 10 minutes please!”*





## Executive Swoop two

*“Can I get a spreadsheet of all affected customers?”*

A photograph of wooden Scrabble tiles arranged in a grid. The top row contains 'D' (2 points) and 'O' (1 point). The middle row contains 'I' (1 point) and 'T' (4 points). The bottom row contains 'N' (1 point), 'O' (1 point), and 'W' (4 points). The tiles are slightly offset and set against a plain white background. Overlaid on the tiles is the text 'Executive Swoop three' in a bold white font, and below it, the phrase '“Do what I say”' in a white script font.

**Executive Swoop three**

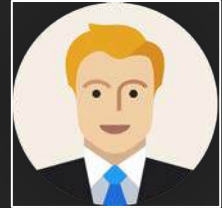
*“Do what I say”*





Do you wish to take command?

...





# Failure to Notify **Stakeholders**

[Photo by chepté cormani](#)

A person with short blonde hair, wearing a red turtleneck and a grey jacket, is shouting into a large white megaphone. The megaphone is held up to their mouth, and its large circular opening is on the right side of the frame. The background is a dark, solid color. The text "Too frequent status updates" is overlaid in white, with "Too frequent" in a bold font.

**Too frequent** status updates

Photo by Edmond Dantès





# Red Herrings

| City              | Number |
|-------------------|--------|
| DOVER             | 297    |
| NORWICH           | 189    |
| LIVERPOOL         | 112    |
| FIELD             | 78     |
| HULL              | 38     |
| NEWCASTLE         | 98     |
| FILEY             | 23     |
| SCARBOROUGH       | 23     |
| HARROGATE         | 37½    |
| MANCHESTER        | 91     |
| YORK              | 17     |
| DURHAM            | 15     |
| GLASGOW           | 223    |
| MCCLESFIELD       | 100½   |
| CONCASTER         | 55     |
| ROCHDALE          | 64     |
| LONDON            | 229    |
| BRADFORD          | 50½    |
| SHEFFIELD         | 69     |
| BARROW IN FURNESS | 134    |
| BEDFORD           | 165    |
| BIRMINGHAM        | 152    |

# Other common pitfalls

**Debating the severity of an incident during the call**

**Discussing process and policy decisions**

**Not disseminating policy changes**

**Hesitating to escalate to other responders**

**Neglecting the post-incident review and follow up activities**

**Trying to take on multiple roles**

**Getting everyone on the call**

**Forcing everyone to stay on the call**

**Assuming silence means no progress**



# Summary

- Use the Incident Command System for managing incidents
- An Incident Commander takes charge during emergency scenarios
- Set expectations upward
- Work with your team to set explicit processes and expectations
- Practice, practice, practice!
- Don't forget to review and improve



More details on

[response.pagerduty.com](https://response.pagerduty.com)

Connect with us at

[community.pagerduty.com](https://community.pagerduty.com)

PagerDuty  
commons/





Thank you!

# Don't Panic! Effective Incident Response

Daniel Afonso

@danieljcafonso

