

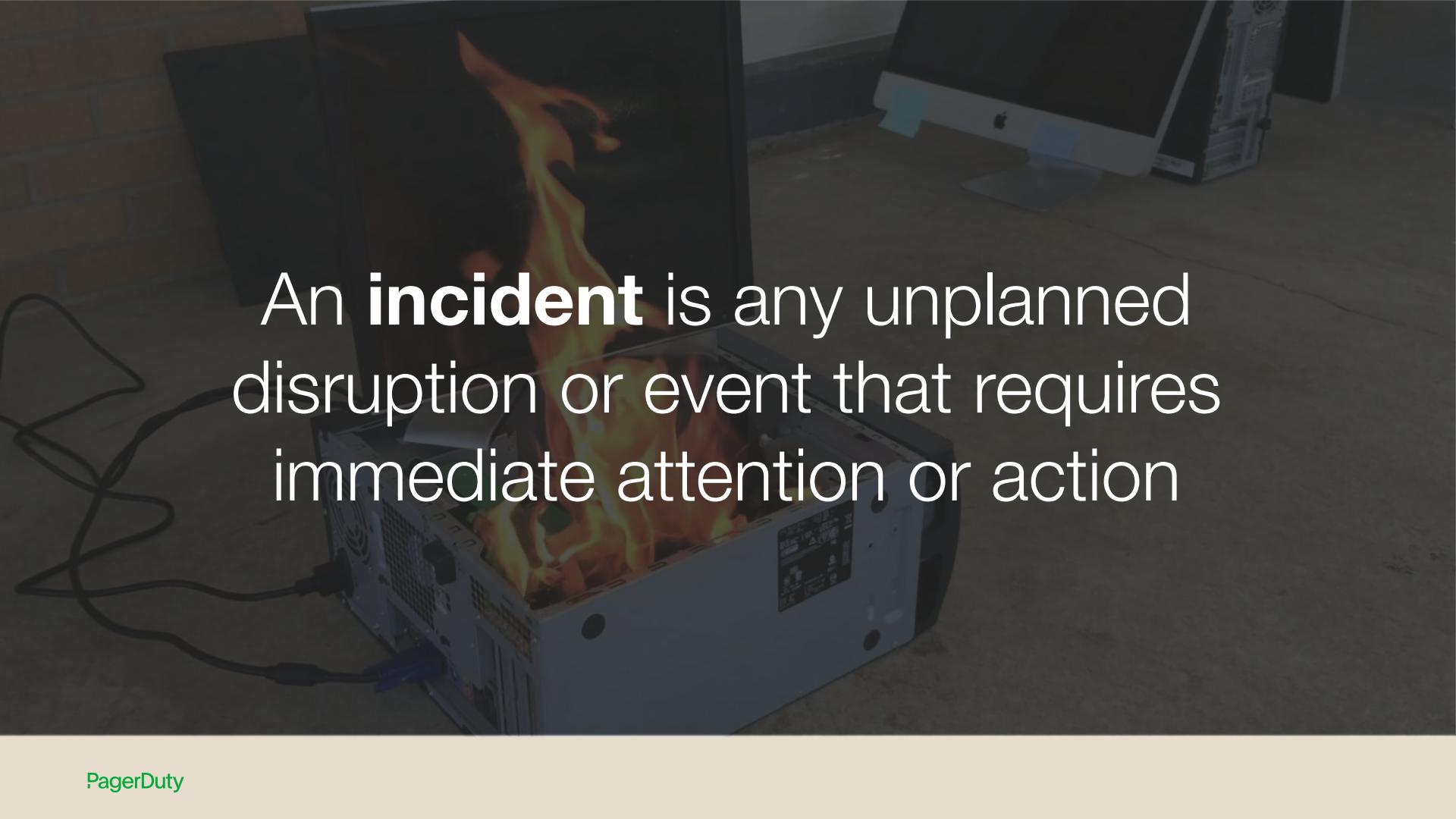
# Don't Panic!

## Effective Incident Response

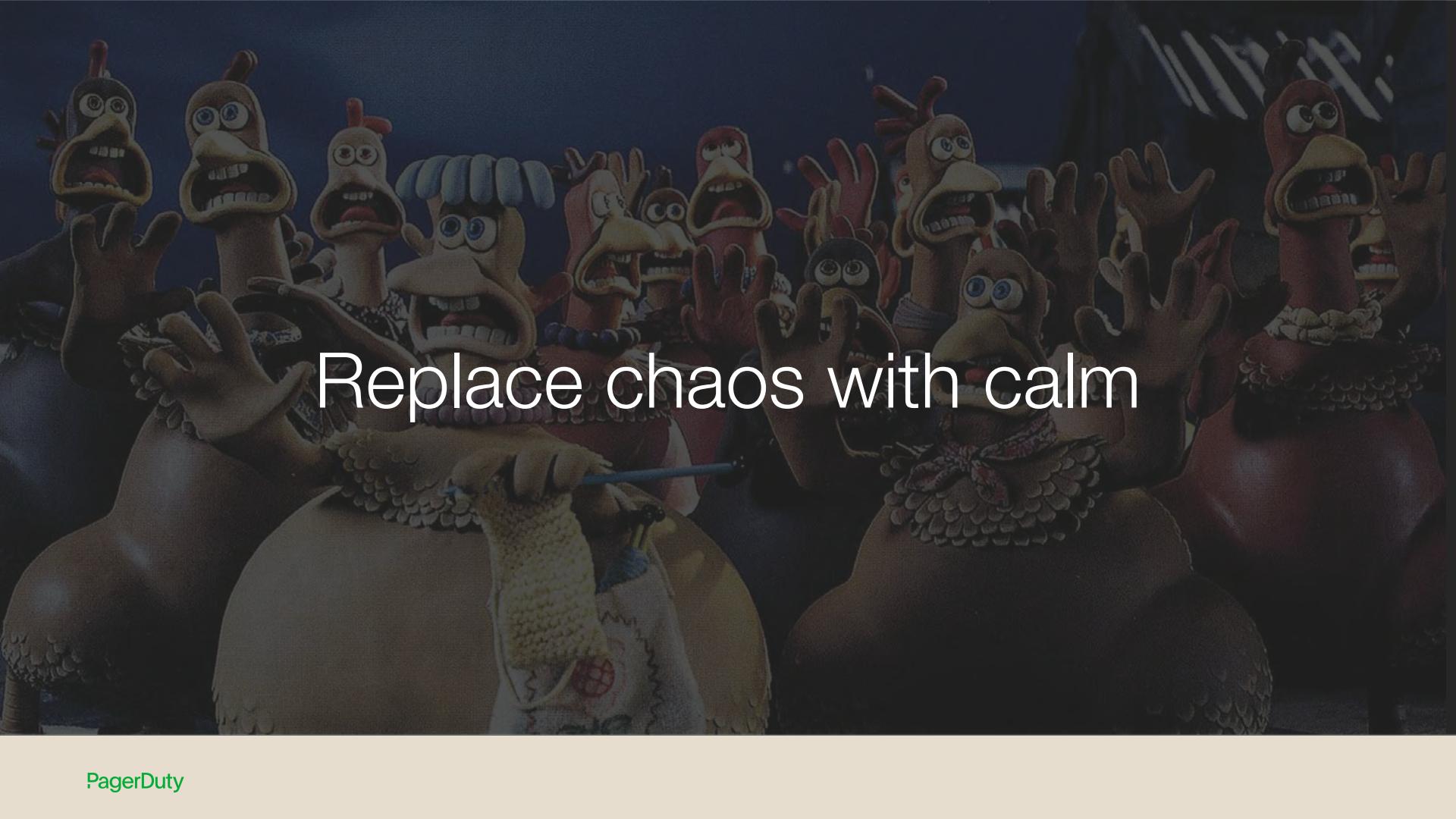
*Presented by*  
@QuintessenceAnx  
DevOps Advocate

2021

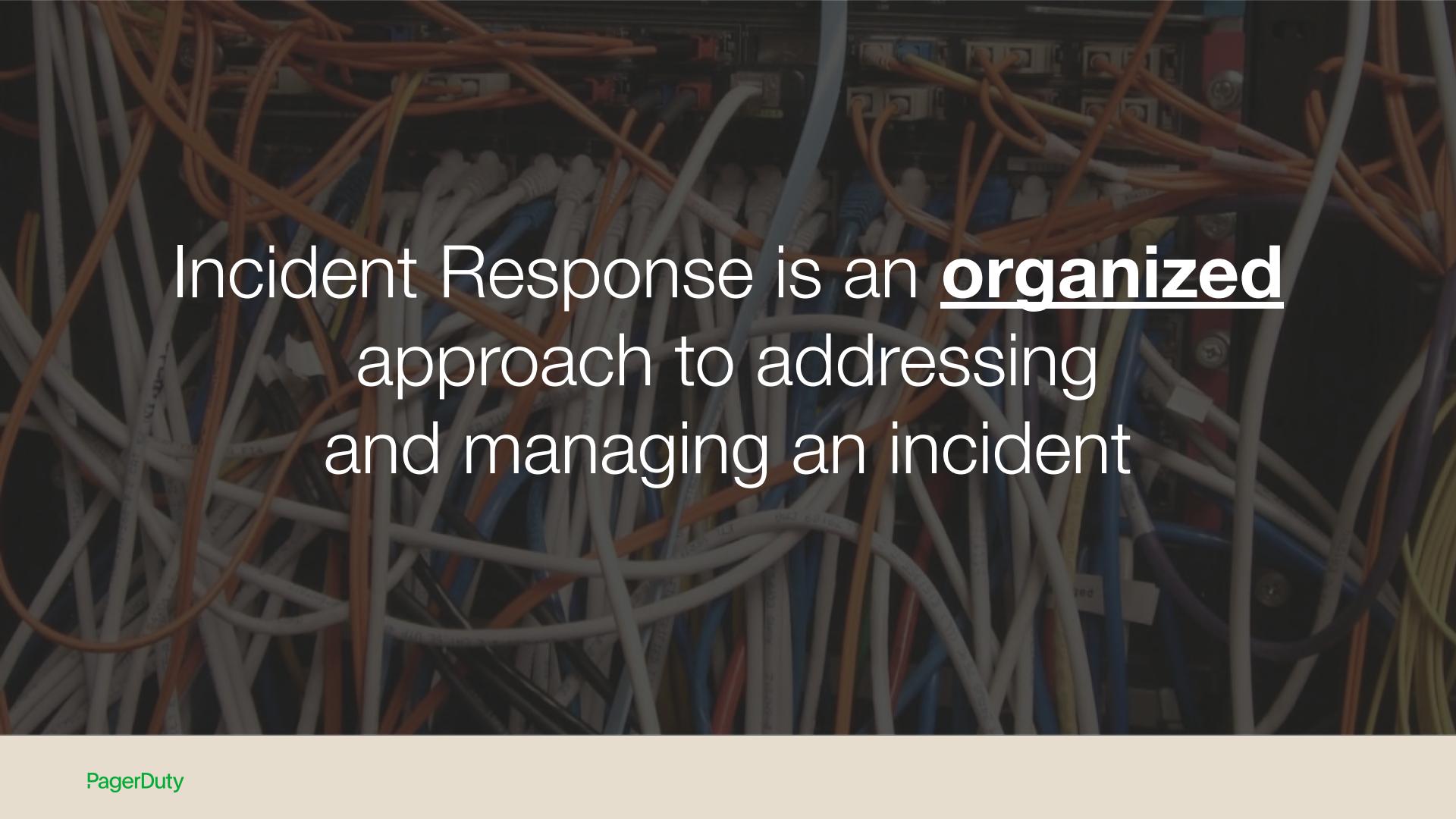


A photograph of a computer setup. In the foreground, a server tower with a blue and orange flame pattern on its side is connected to a black power strip. Behind it, a computer monitor shows a close-up of a fire. To the right, a white iMac sits on a desk. A black keyboard is partially visible in the bottom left corner.

An **incident** is any unplanned disruption or event that requires immediate attention or action

A chaotic scene from the movie 'Madagascar'. In the center, King Julien, the lemur king, is frantically knitting a garment with a blue needle and yellow yarn. He has a look of intense concentration and slight panic on his face. Behind him, a large crowd of various animal characters, including a zebra, a lion, and several other lemurs, are shouting and gesturing wildly, creating a sense of pandemonium. The background is dark and filled with the silhouettes of more characters.

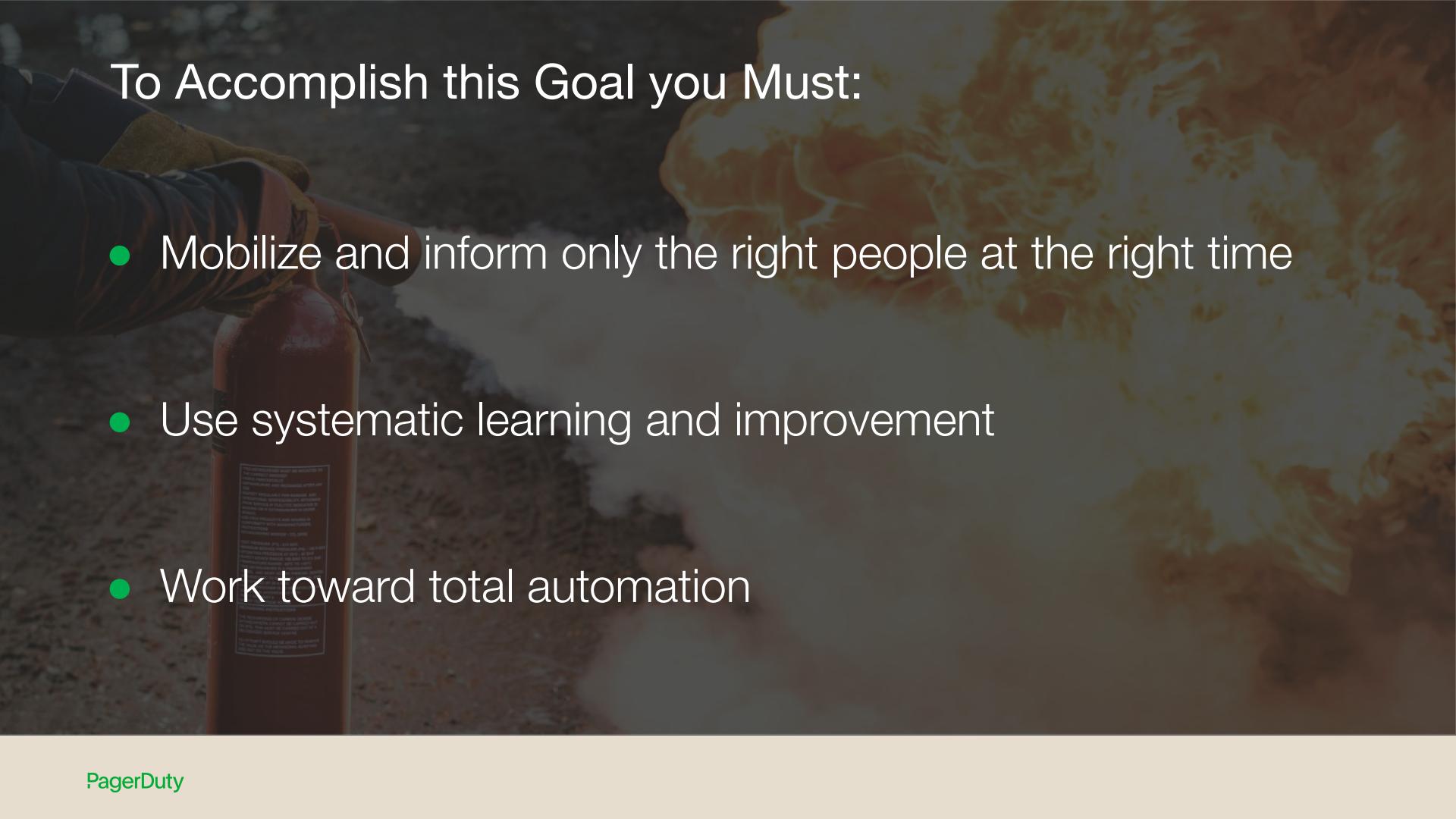
Replace chaos with calm



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

A firefighter wearing a helmet and turnout gear is spraying a powerful stream of water onto a large, billowing fire. The fire is bright orange and yellow, with thick smoke rising into the air. The firefighter's arm and the hose are visible on the left side of the frame.

The goal of Incident Response is to handle the situation in a way that limits damage and reduces recovery time and costs

A dramatic photograph of a firefighter in full gear, including a helmet and oxygen tank, spraying a powerful stream of water onto a large, billowing fire. The fire is intense, with bright orange and yellow flames and thick smoke billowing upwards. The firefighter's position is on the left, facing right towards the fire.

## To Accomplish this Goal you Must:

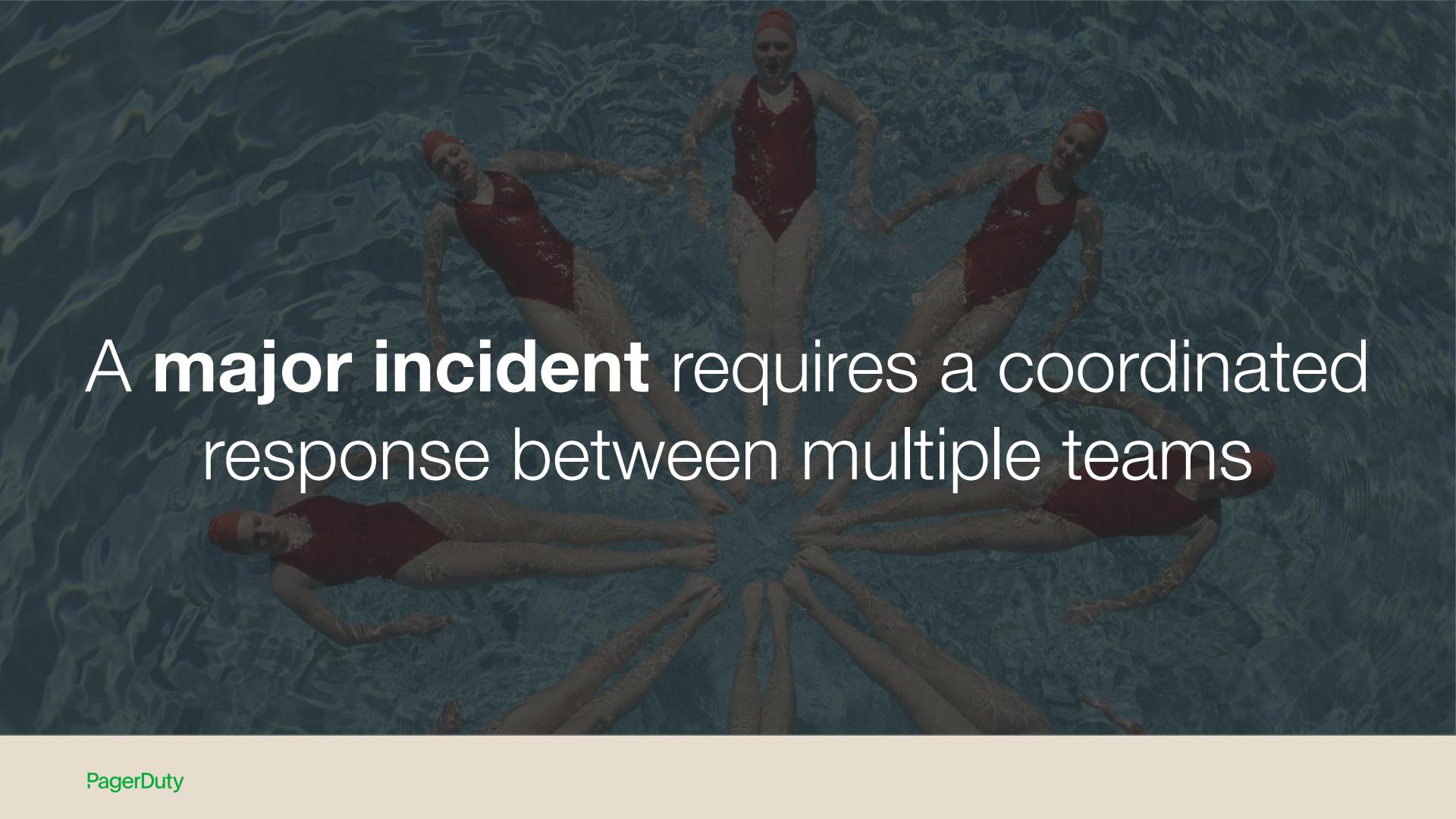
- Mobilize and inform only the right people at the right time
- Use systematic learning and improvement
- Work toward total automation



Based on the Incident Command System,  
originally developed for California wildfire  
response.

A photograph of a computer setup. In the foreground, a silver server tower sits on the floor, with several black power cables trailing off from its back. Behind it, a black computer monitor displays a bright orange and yellow flame. To the right, a white iMac computer is visible, also displaying a flame on its screen. The background shows a brick wall and a wooden floor.

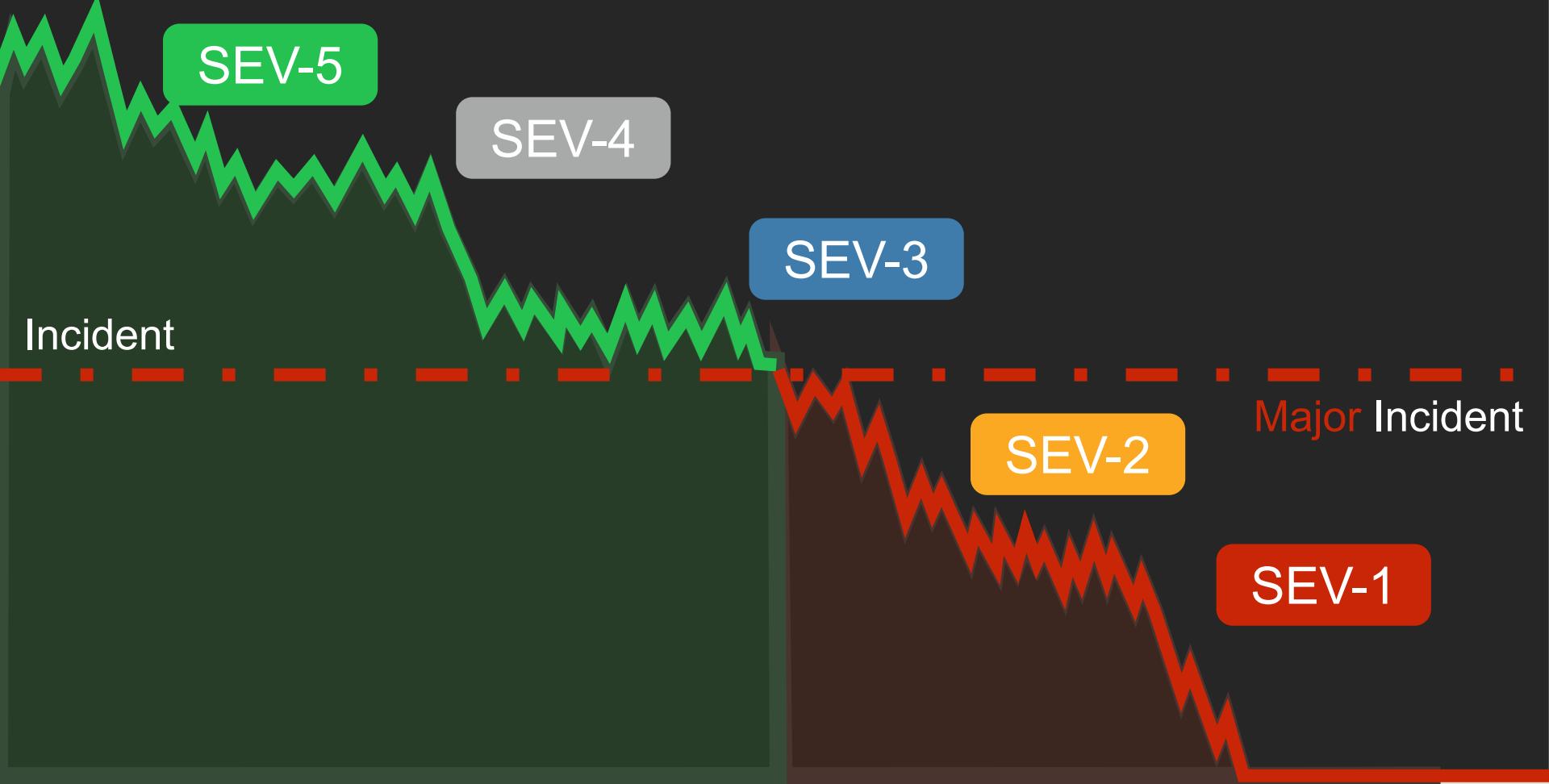
An incident is an unplanned disruption or event that requires immediate attention or action

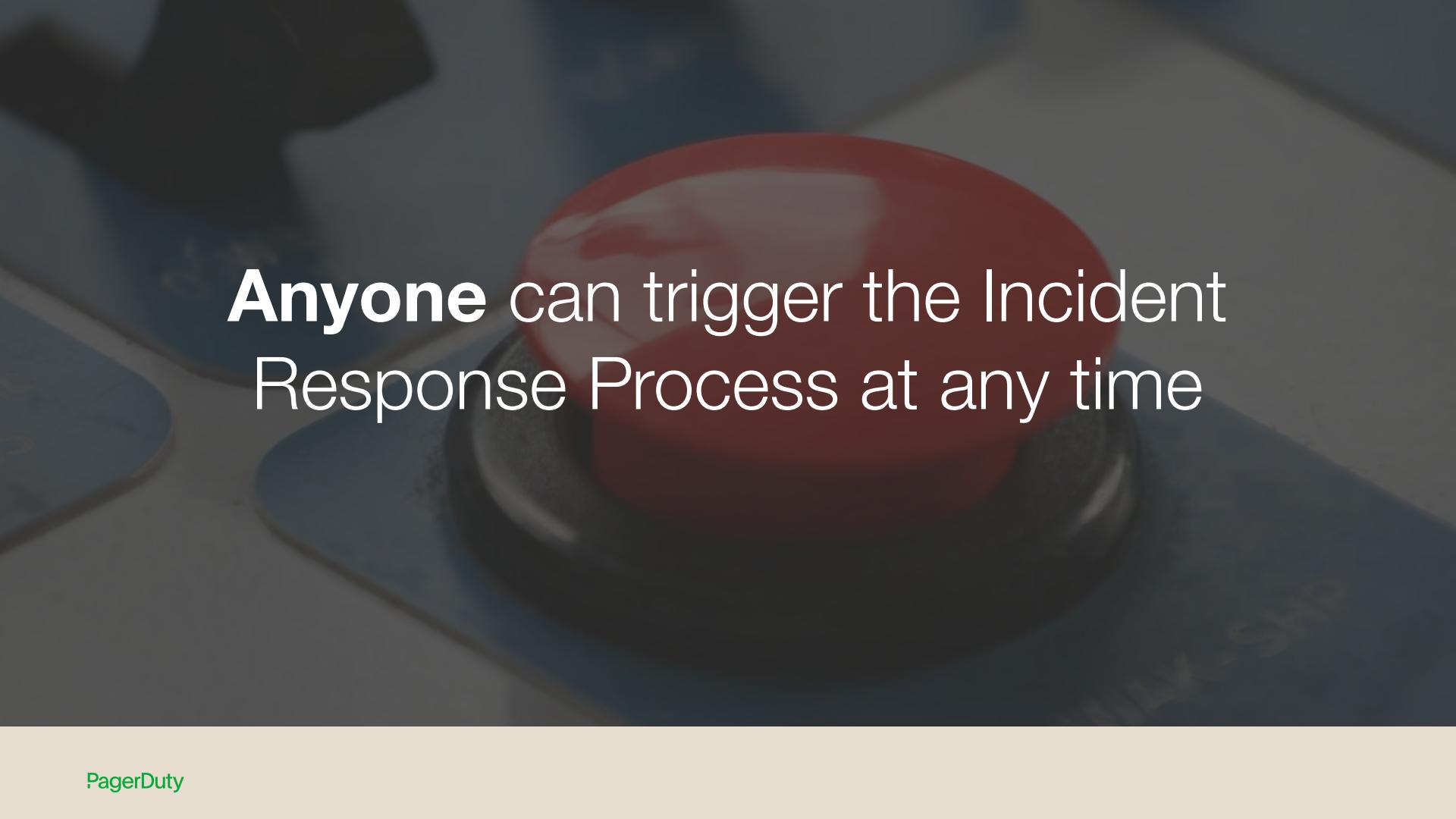
A photograph of several swimmers in a pool. They are wearing red swim caps and dark red swimsuits. Some are floating on their backs, while others are in various swimming strokes. The water is clear and blue, with visible ripples and reflections. The swimmers are arranged in a loose cluster, suggesting a team or group effort.

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

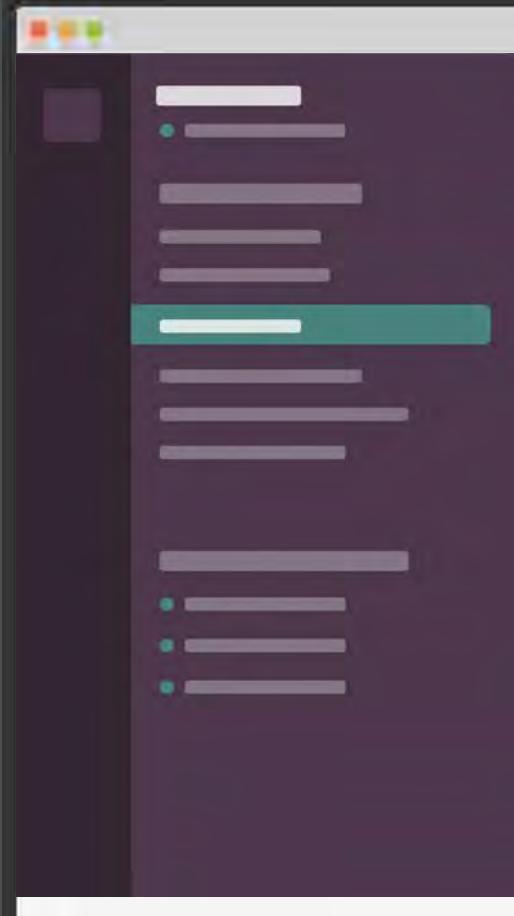
# The 4 Commonalities of Major Incidents

- Timing is a surprise; little or no warning
- Time matters; need to respond quickly
- Situation rarely perfectly understood at the start
- Require mobilization and coordination, typically cross-functional



A close-up photograph of a red circular button with a metallic edge, mounted on a dark, textured panel. In the background, a person's hand is visible, blurred, reaching towards the right side of the frame.

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



**Rich Adams** 11:12  
!ic page



**Officer URL** APP 11:12

Police Paging Incident Commanders(s)

- ✓ Arup Chakrabarti has been paged.
- ✓ Paul Rechsteiner has been paged.
- ✓ Renee Lung has been paged.

ⓘ Use [!ic responders](#) to see who the team responders are.

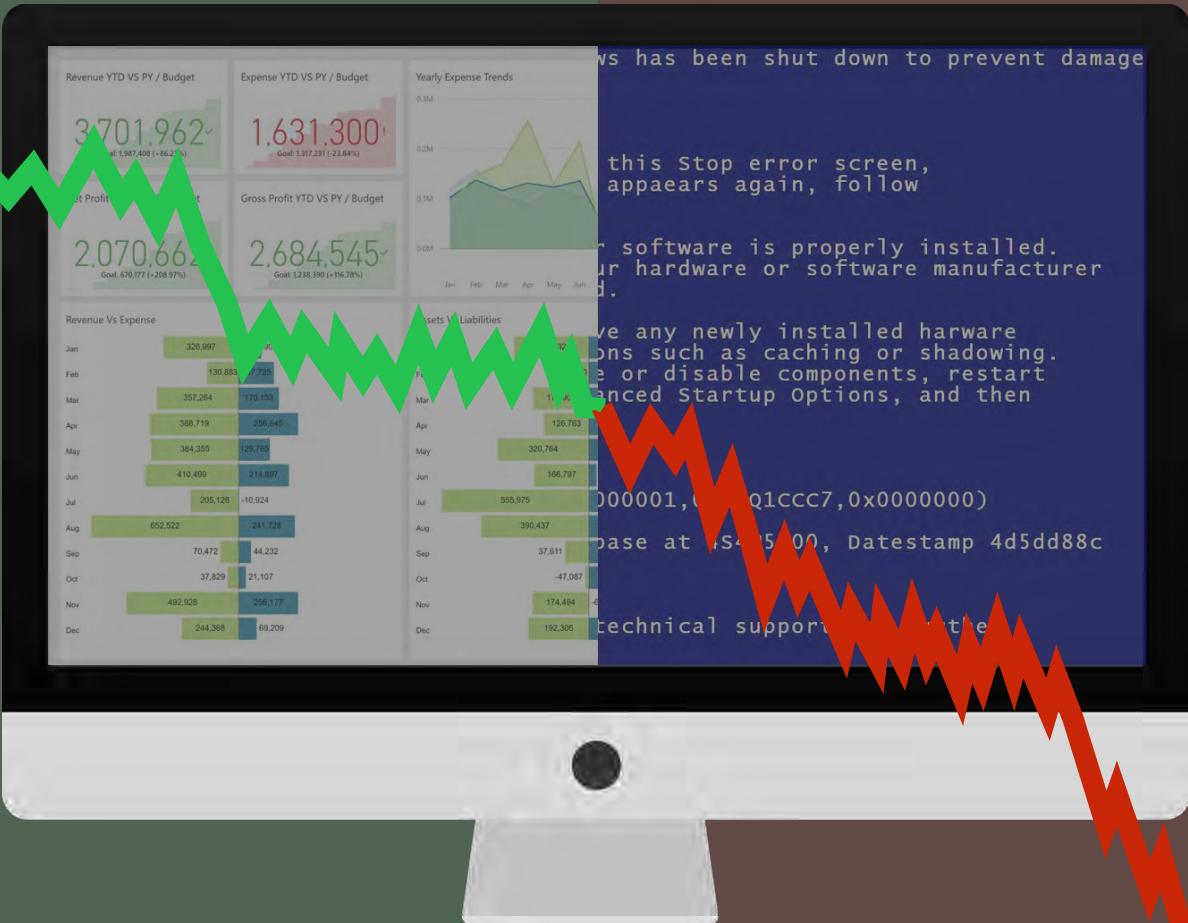
pd Incident triggered:

<https://example.pagerduty.com/incident/PD5I34R>



!ic page

# PEACETIME



# WARTIME

# NORMAL



# EMERGENCY

OK



NOT OK

A woman with long, dark hair is shown from the side, looking down at her smartphone. The screen of the phone is brightly lit, casting a glow on her face and hand. The background is dark and out of focus.

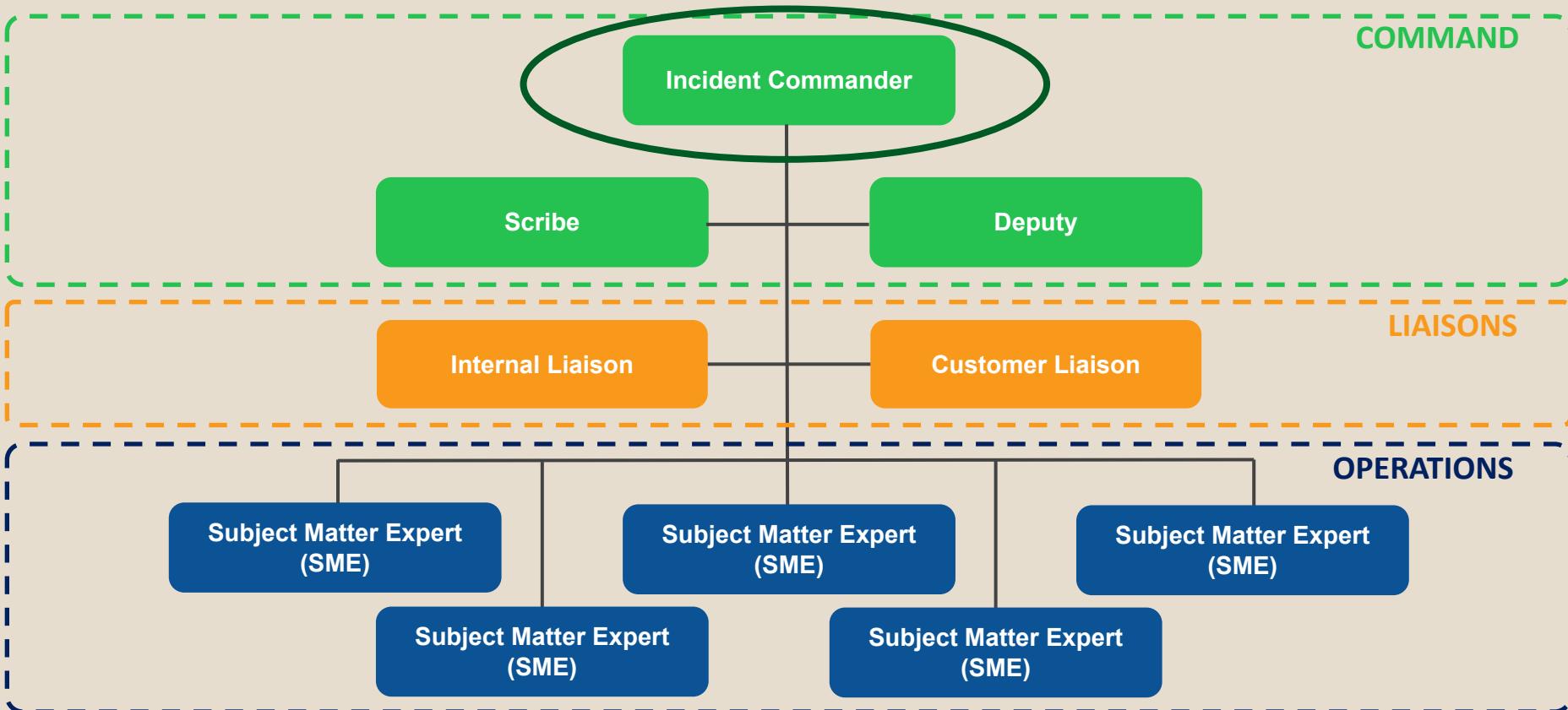
# Decision Paralysis

# People Roles & Incident Categorization

# The Four Steps of an Incident



# Roles of Incident Response

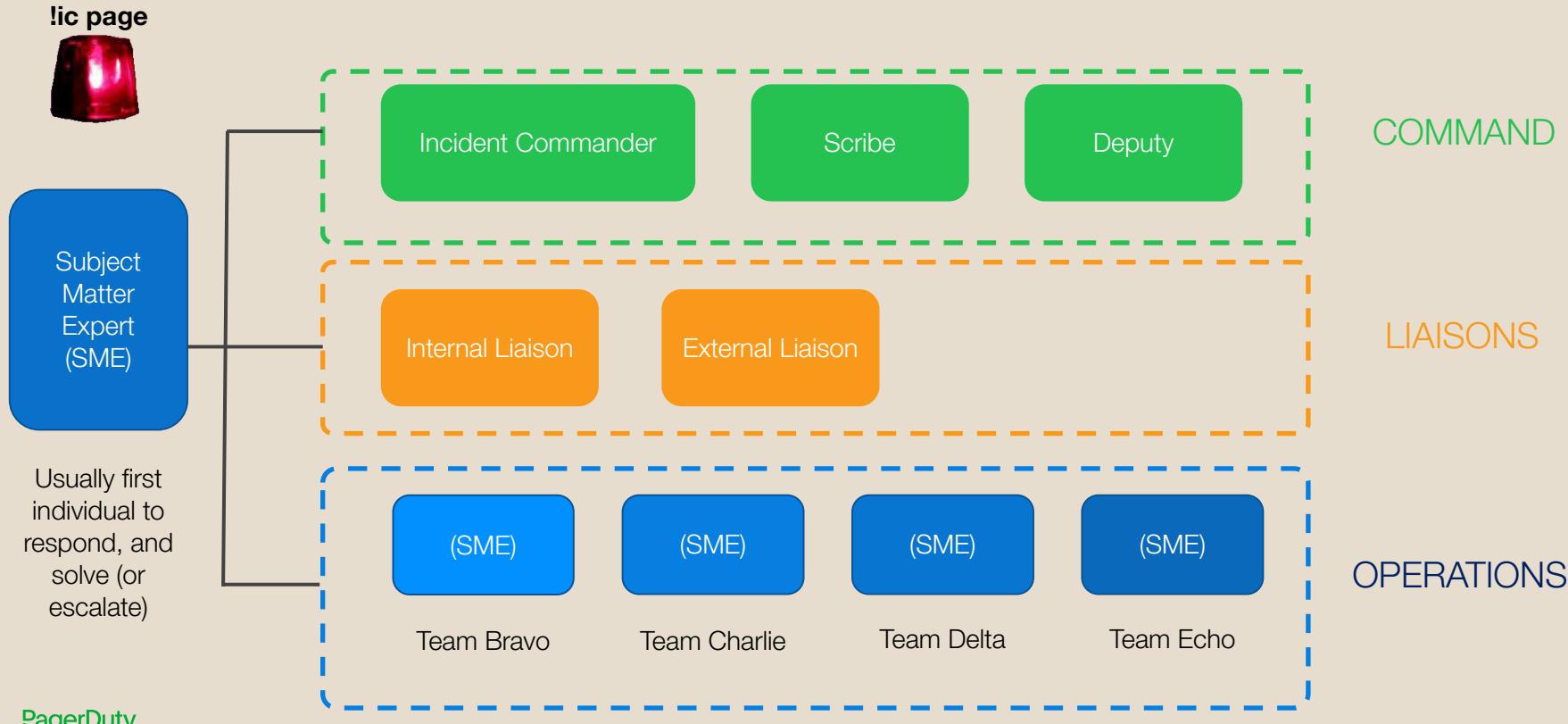


# Setting this up at scale

For a department-wide Incident Response process, you will need a few things set up to begin. This includes:

- An on-call schedule for a primary and backup Incident Commander (this role is team agnostic)
- On-call schedules for primary and backup subject matter experts (one primary and one backup for each team)
- Additional on-call rotations for other roles
- A method of paging team members (response mobilization)

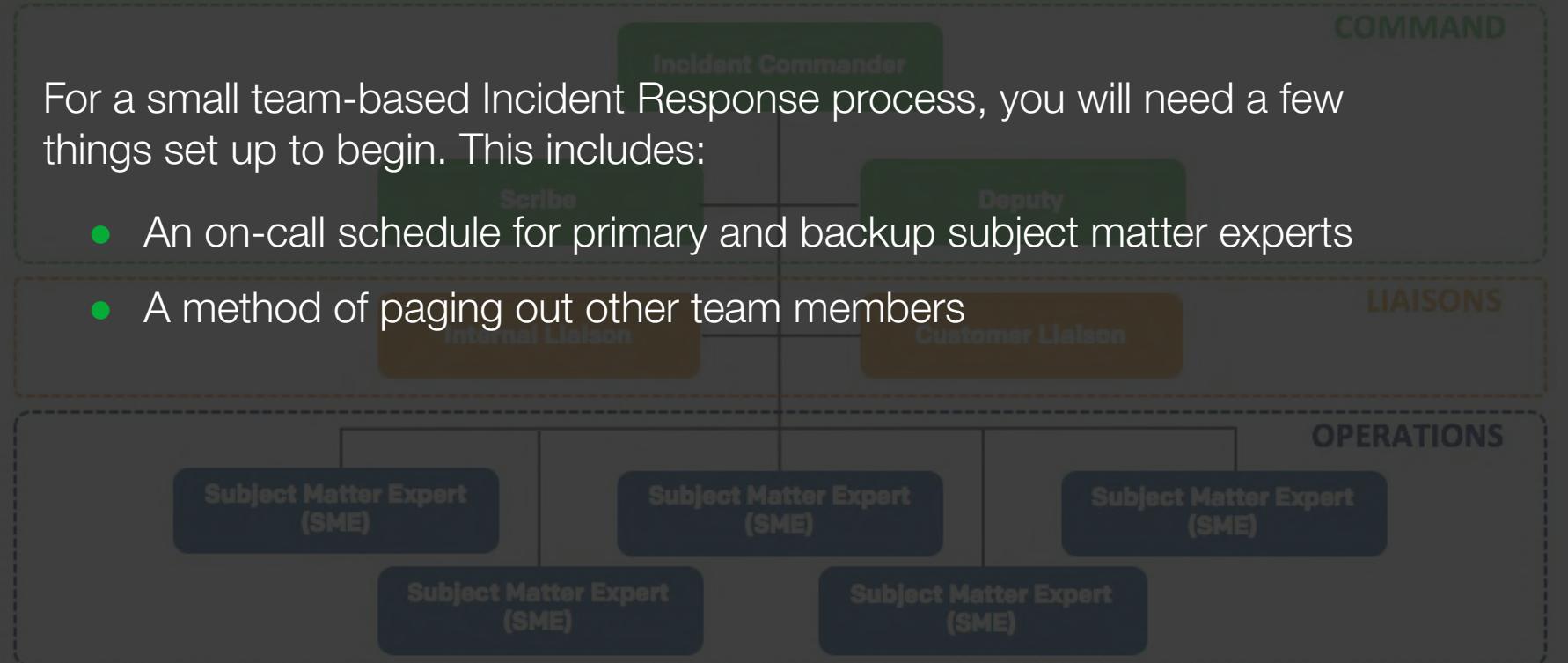
# Incident Response - typical sequence of events



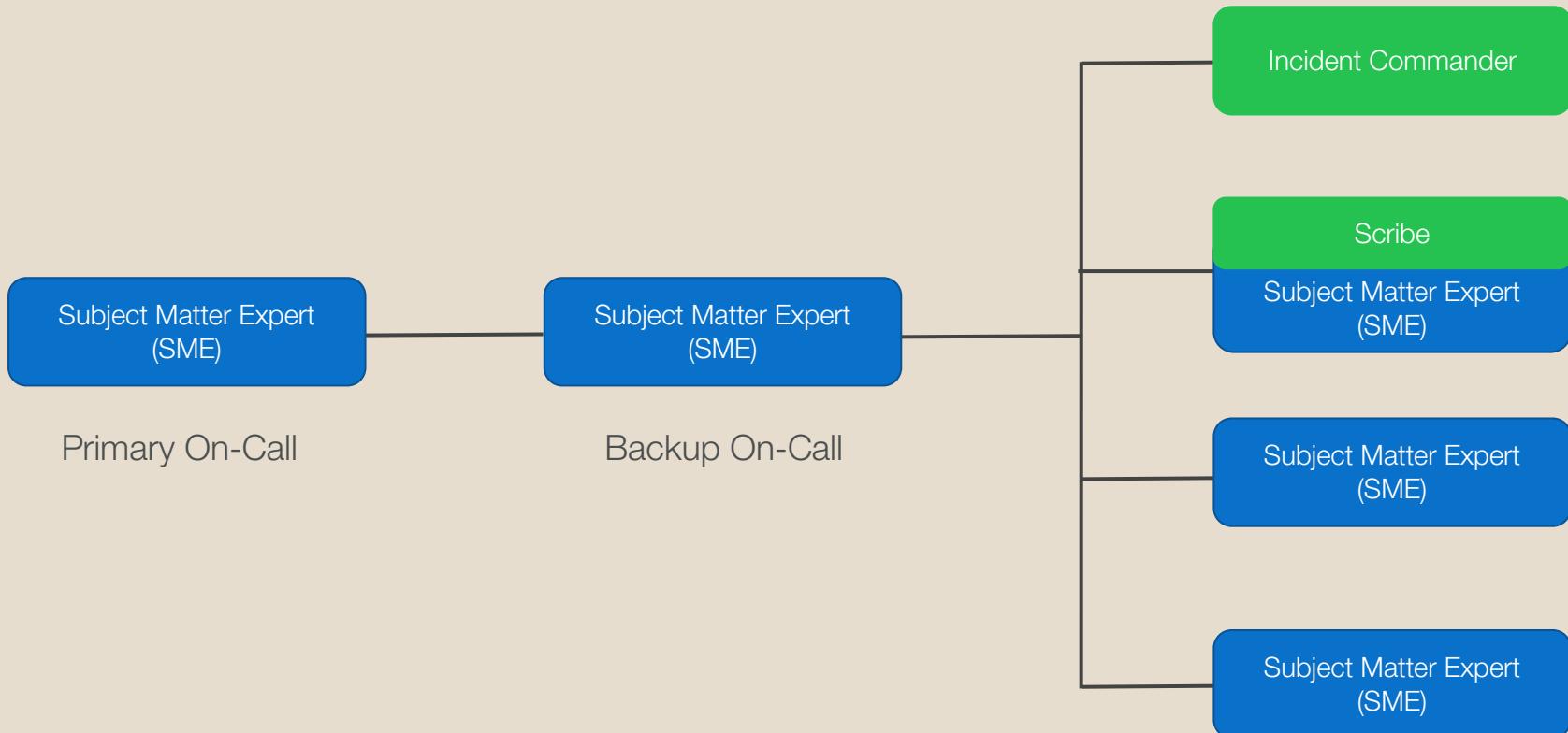
# How Do The Roles Scale Down?

For a small team-based Incident Response process, you will need a few things set up to begin. This includes:

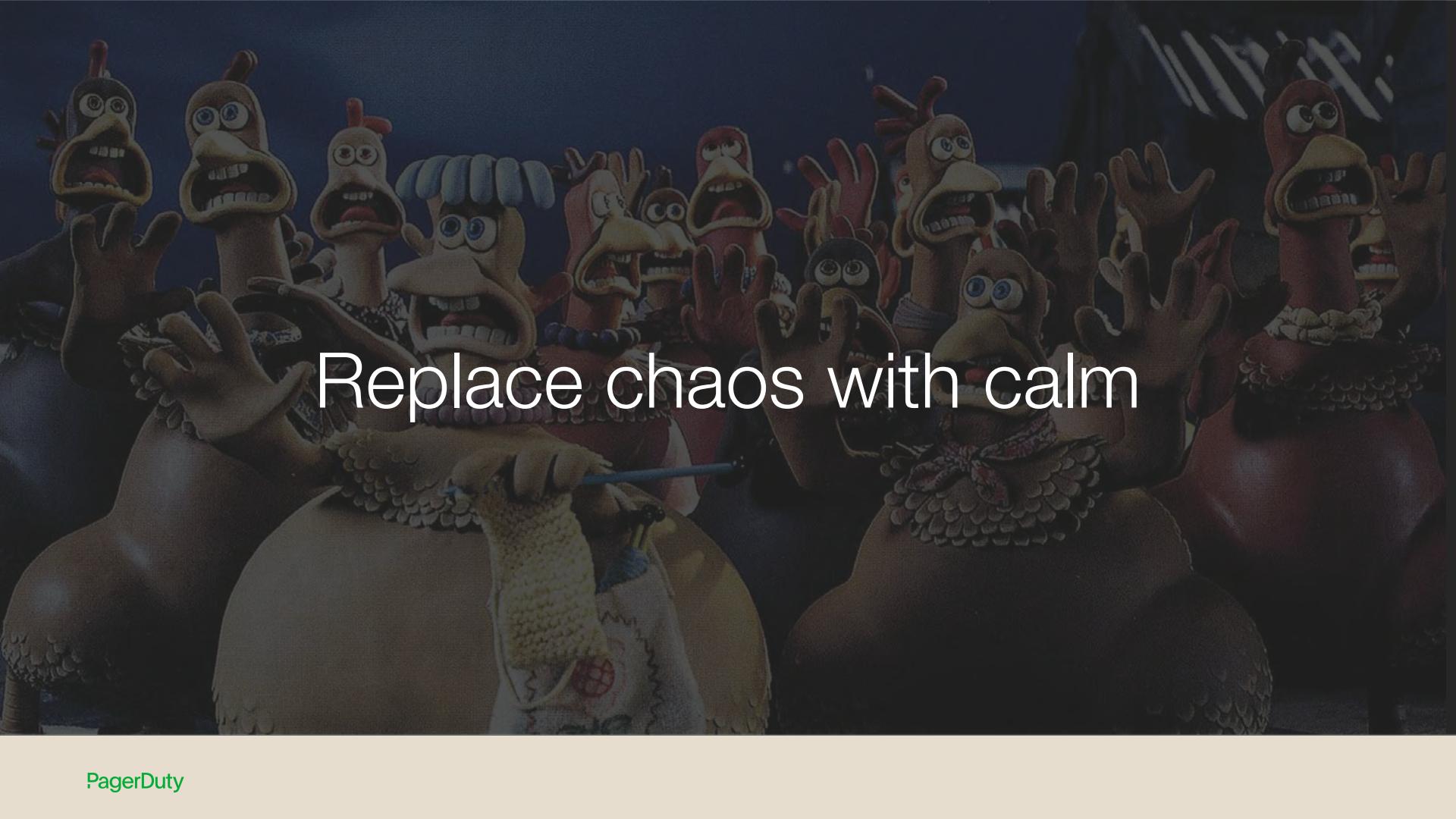
- An on-call schedule for primary and backup subject matter experts
- A method of paging out other team members



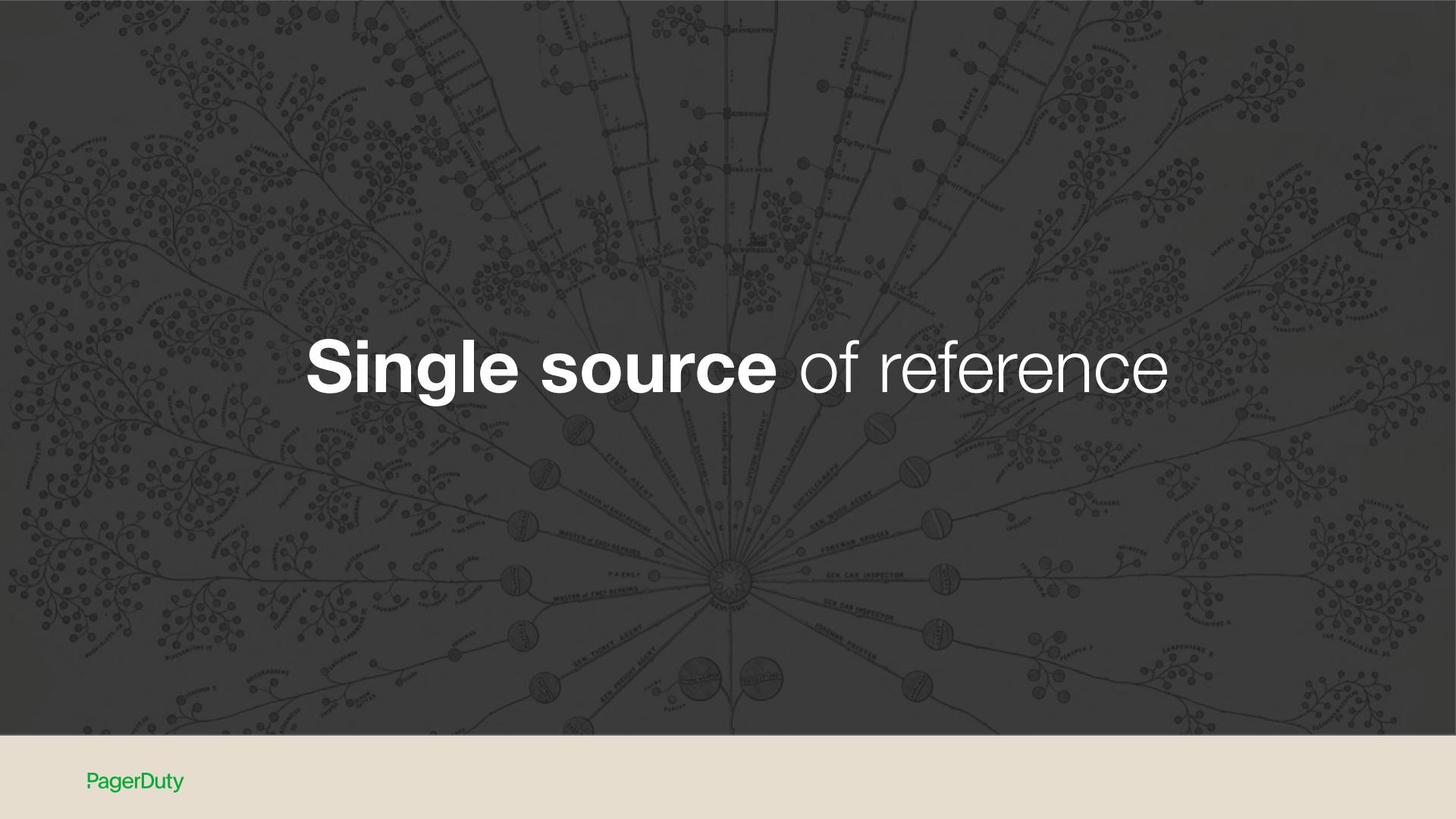
# Small Team Incident Response



# Incident Commander: Role and Responsibilities

A chaotic scene from the movie 'Madagascar'. In the center, King Julien, the lemur king, is frantically knitting a garment with a blue needle and yellow yarn. He has a look of intense concentration and slight panic on his face. Behind him, a large crowd of various animal characters, including a zebra, a lion, and several other lemurs, are shouting and gesturing wildly, creating a sense of pandemonium. The background is dark and filled with the silhouettes of more characters.

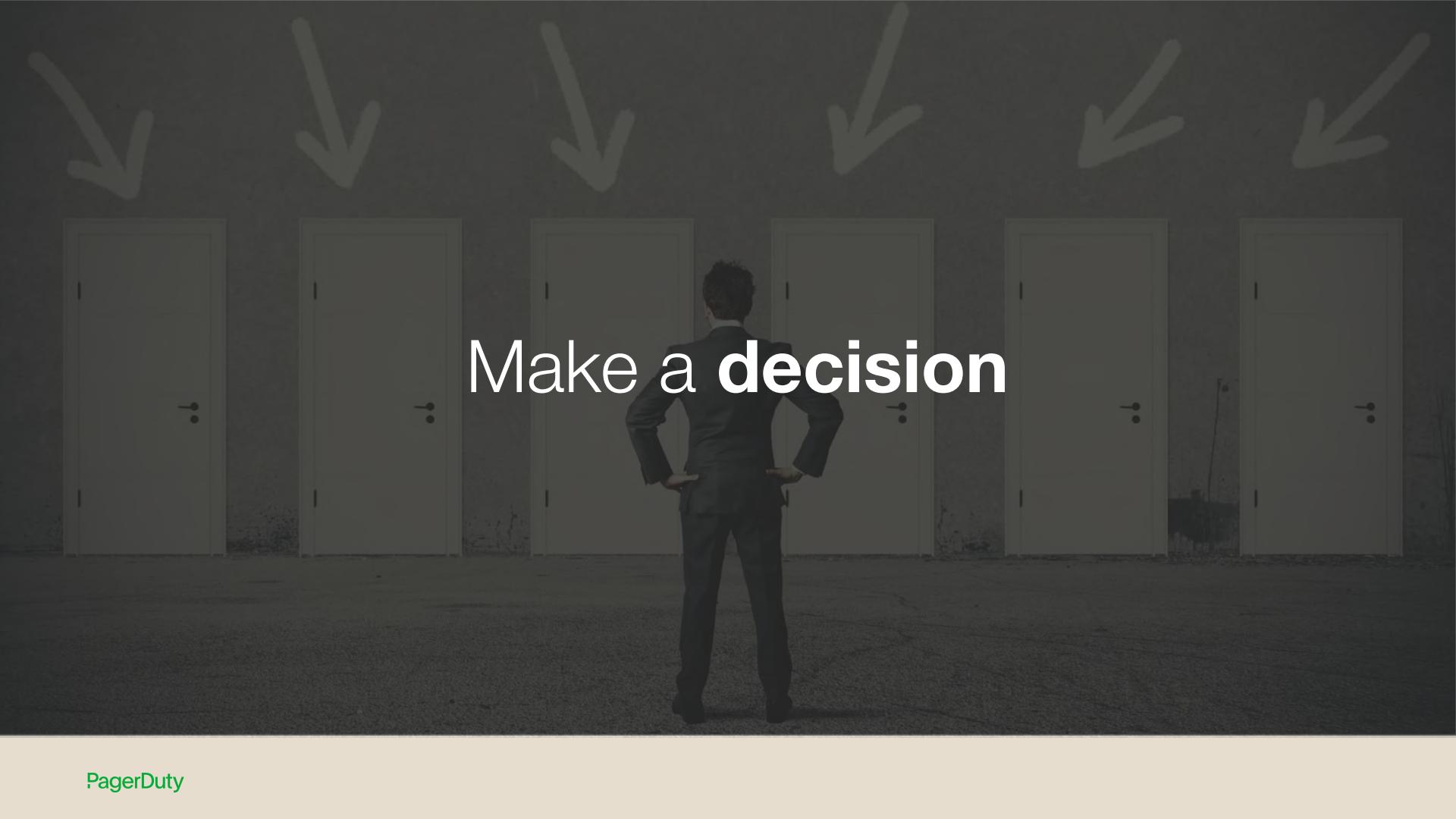
Replace chaos with calm



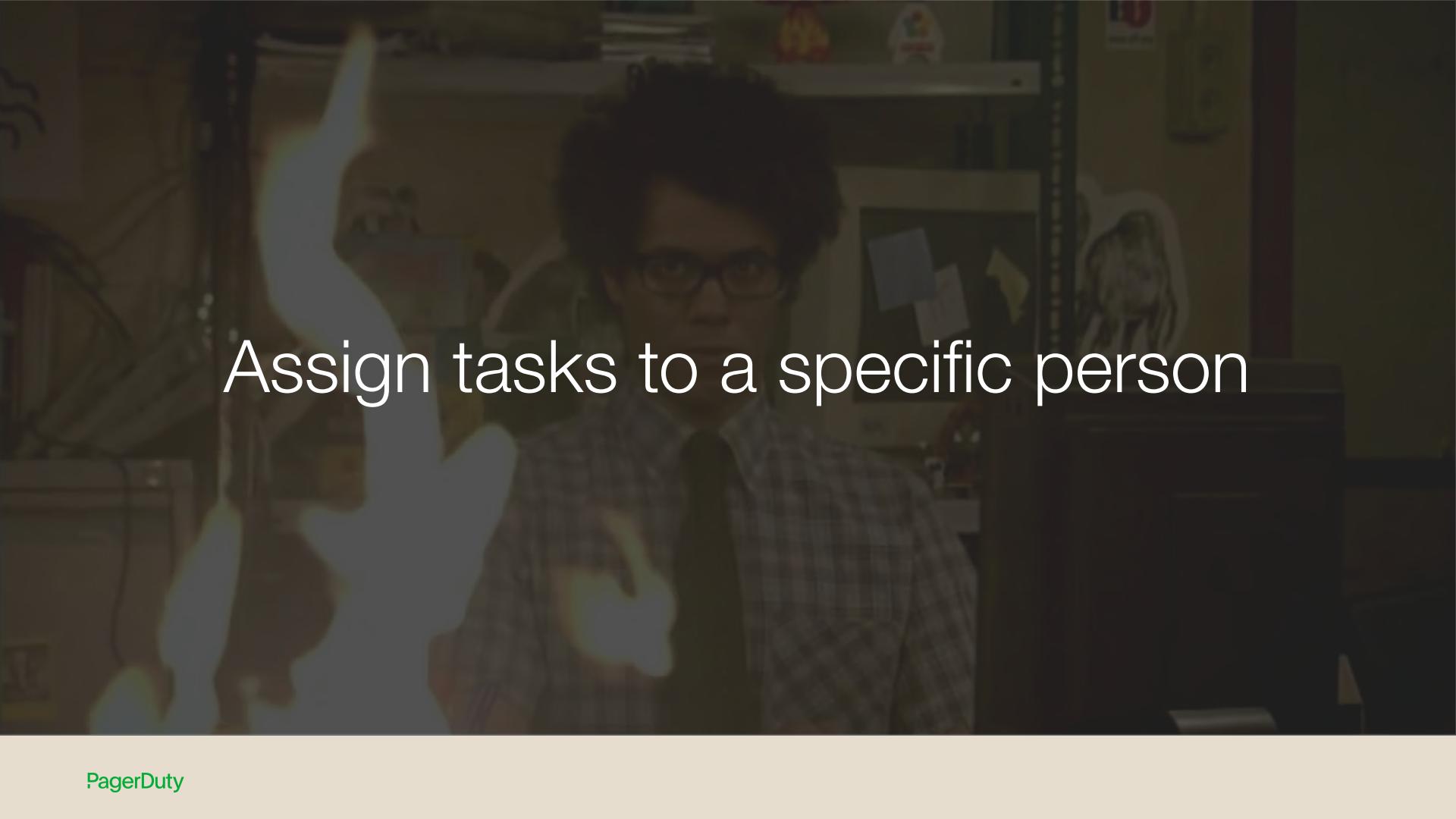
# Single source of reference

# Gain **consensus**

“Are there any **strong** objections”



Make a **decision**

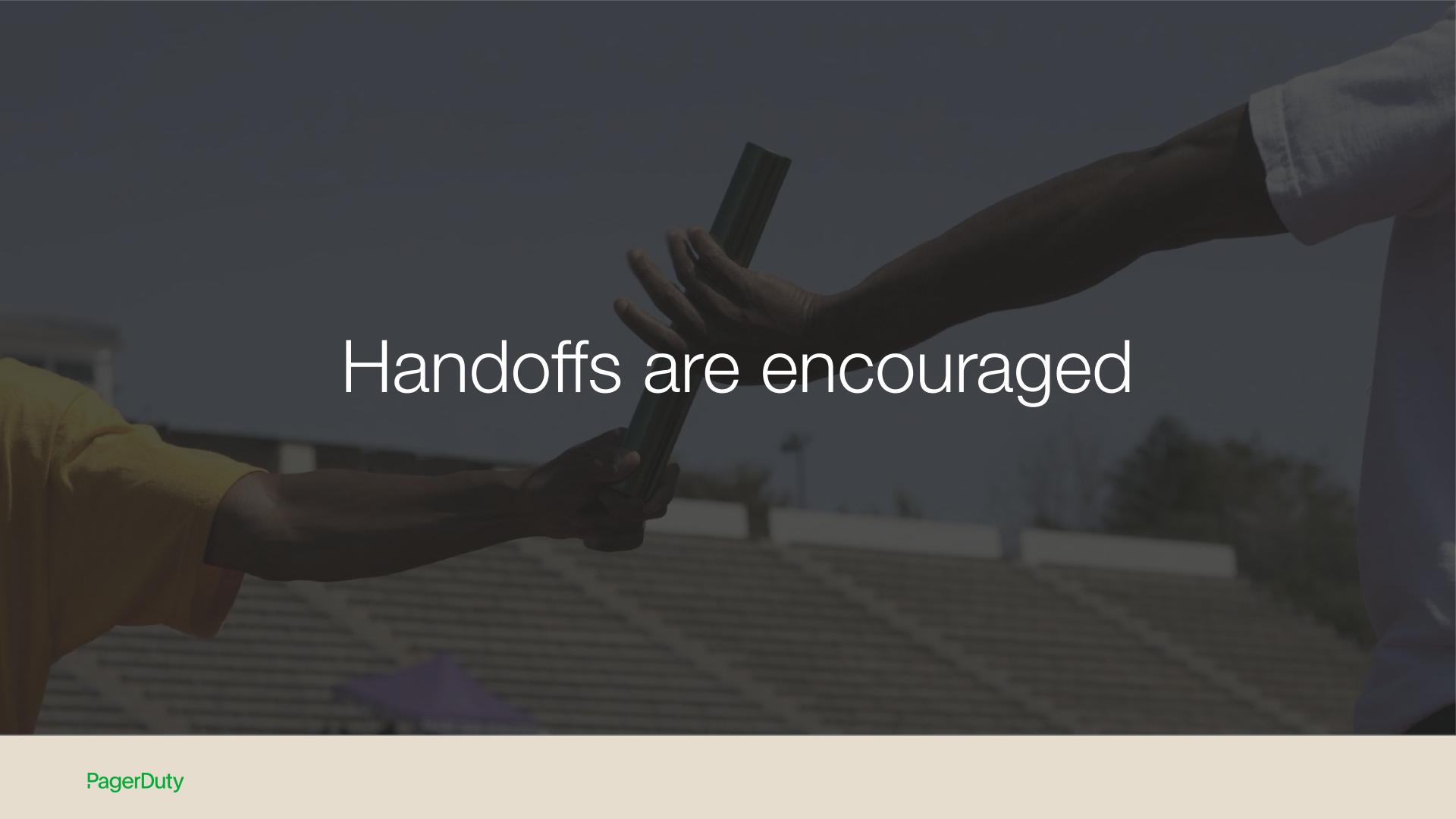
A medium shot of a man with dark hair and glasses, wearing a plaid shirt. He is looking down and slightly to the left, focused on something in his hands which are partially visible. The background is a blurred indoor setting with shelves and various items.

# Assign tasks to a specific person

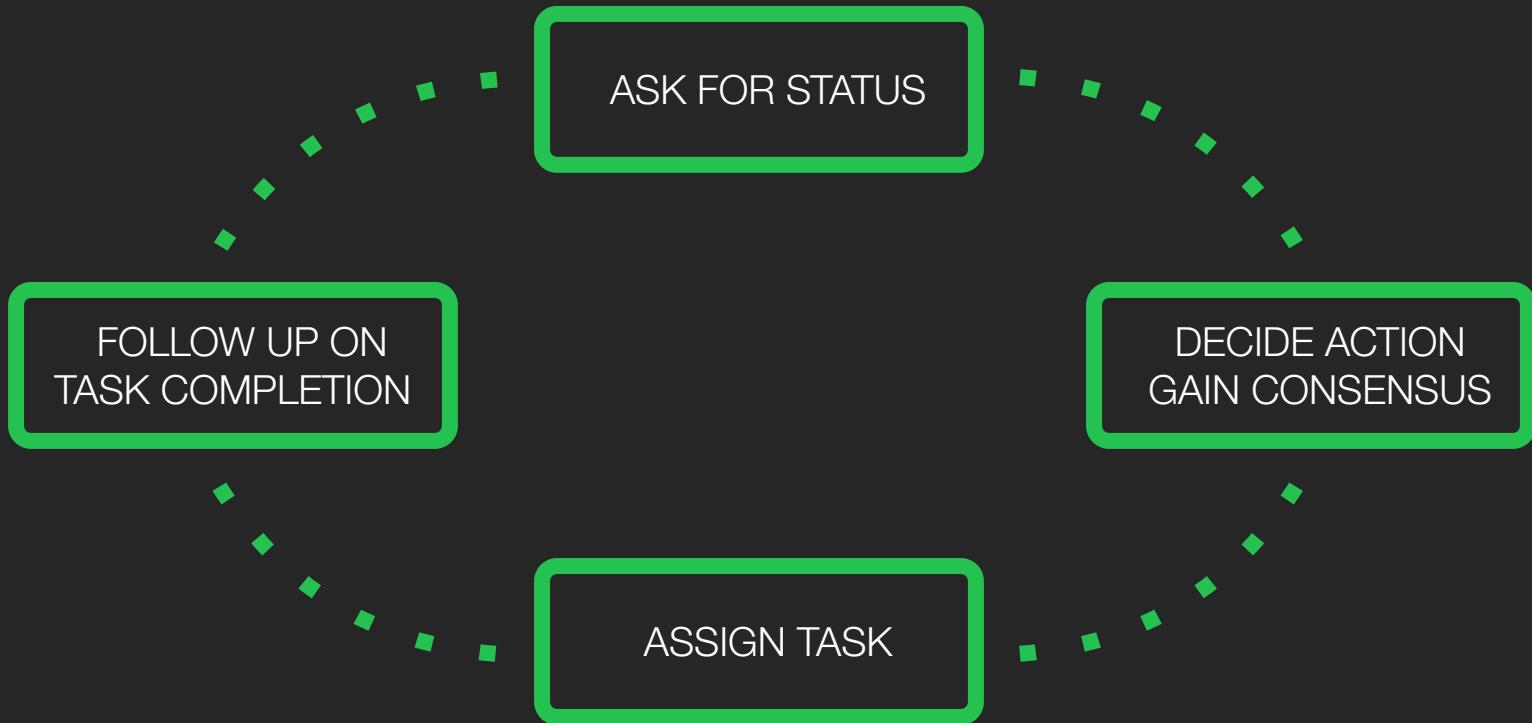


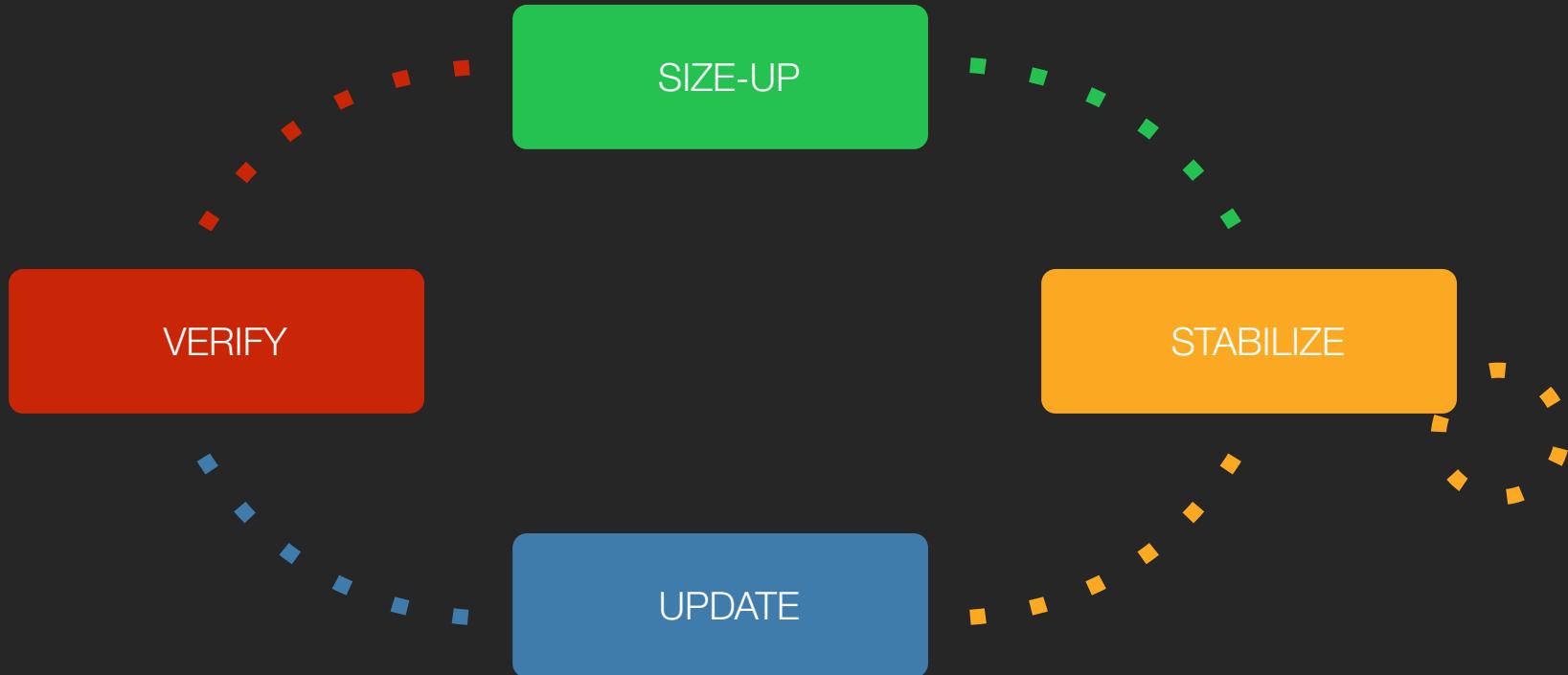
Becomes the highest authority  
(Yes, even higher than the CEO)

# Deep technical knowledge is not required

A photograph of a relay race handoff. Two runners are shown from the side, wearing athletic gear. The runner on the left is handing a green baton to the runner on the right. They are on a track field with bleachers visible in the background.

Handoffs are encouraged





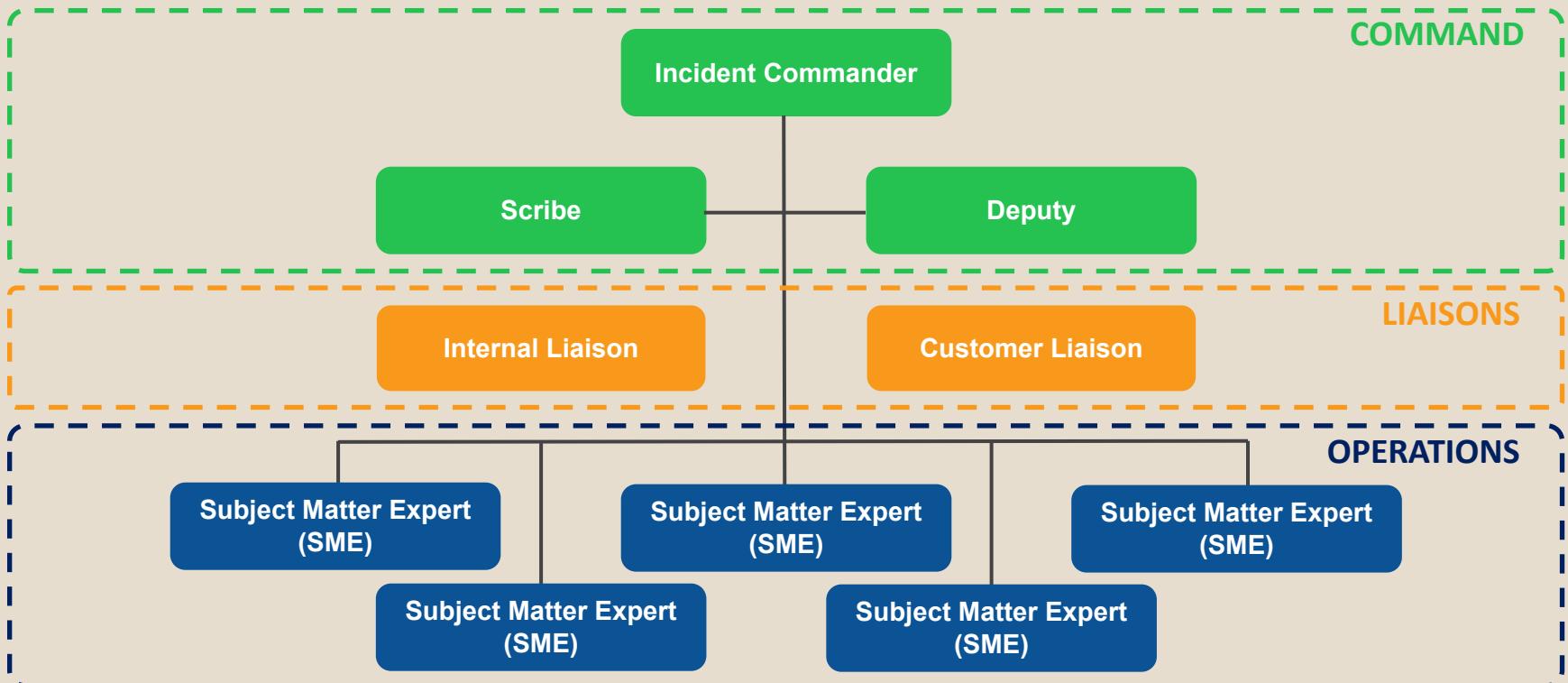
# Quick Tips for New Incident Commanders

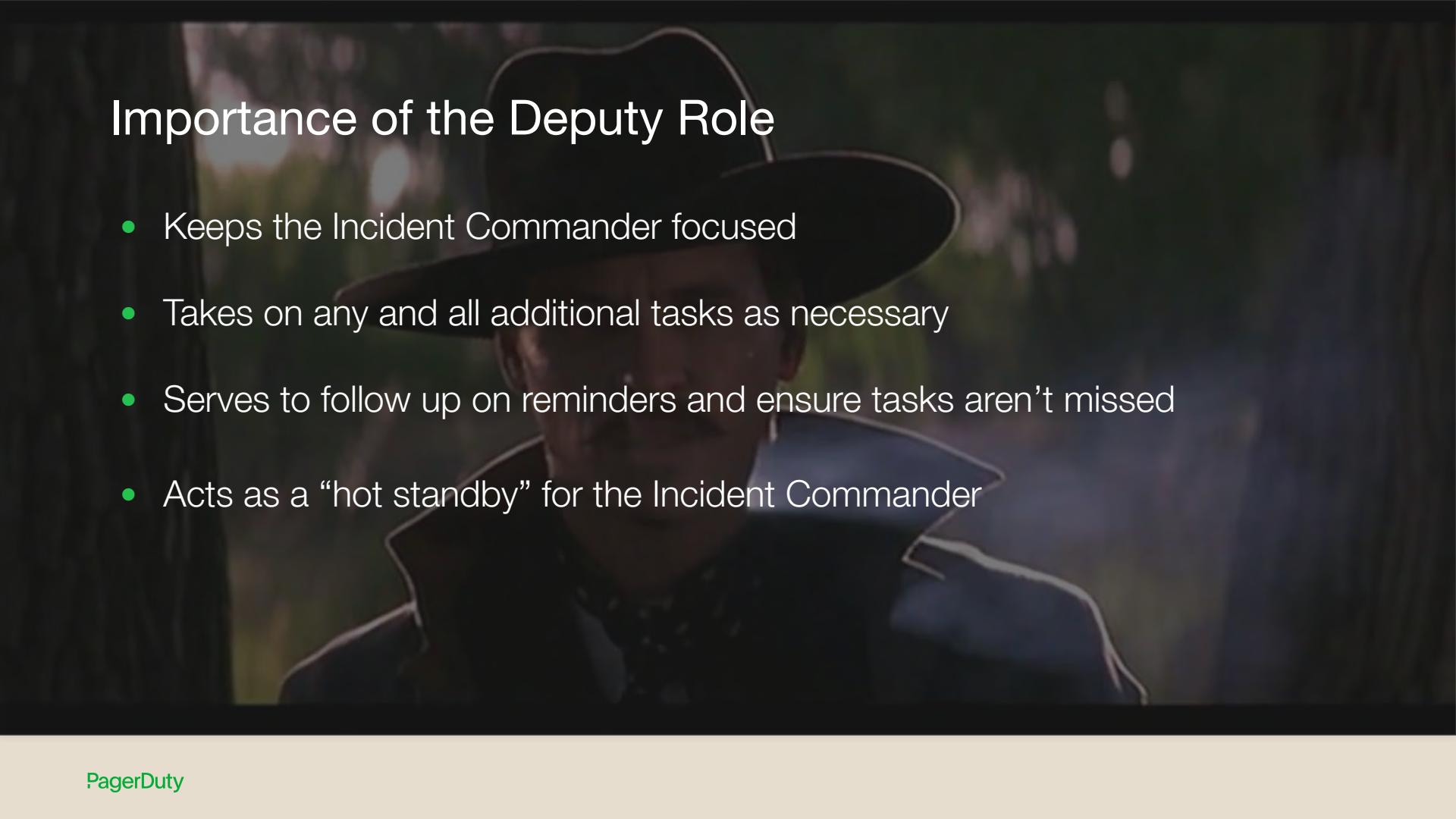
- Introduce yourself on the call with your name and that you are the Incident Commander
- Avoid acronyms
- Speak slowly and with purpose
- On the call, kick people off if they are being disruptive
- Time-box tasks and check in for status updates
- Explicitly declare when the response has ended

# Summary: Importance of the Incident Commander

- Keeps everyone focused
- Keeps decision-making moving
- Helps to avoid the bystander effect
- Keep things moving towards a resolution during a major incident

# Roles of Incident Response





# Importance of the Deputy Role

- Keeps the Incident Commander focused
- Takes on any and all additional tasks as necessary
- Serves to follow up on reminders and ensure tasks aren't missed
- Acts as a “hot standby” for the Incident Commander

# Importance of the Scribe

- Documents the incident timeline and important events as they occur
- The incident log will be used during the post-mortem process
- Note when important actions are taken, follow-up items, and status updates
- Anyone can be a Scribe

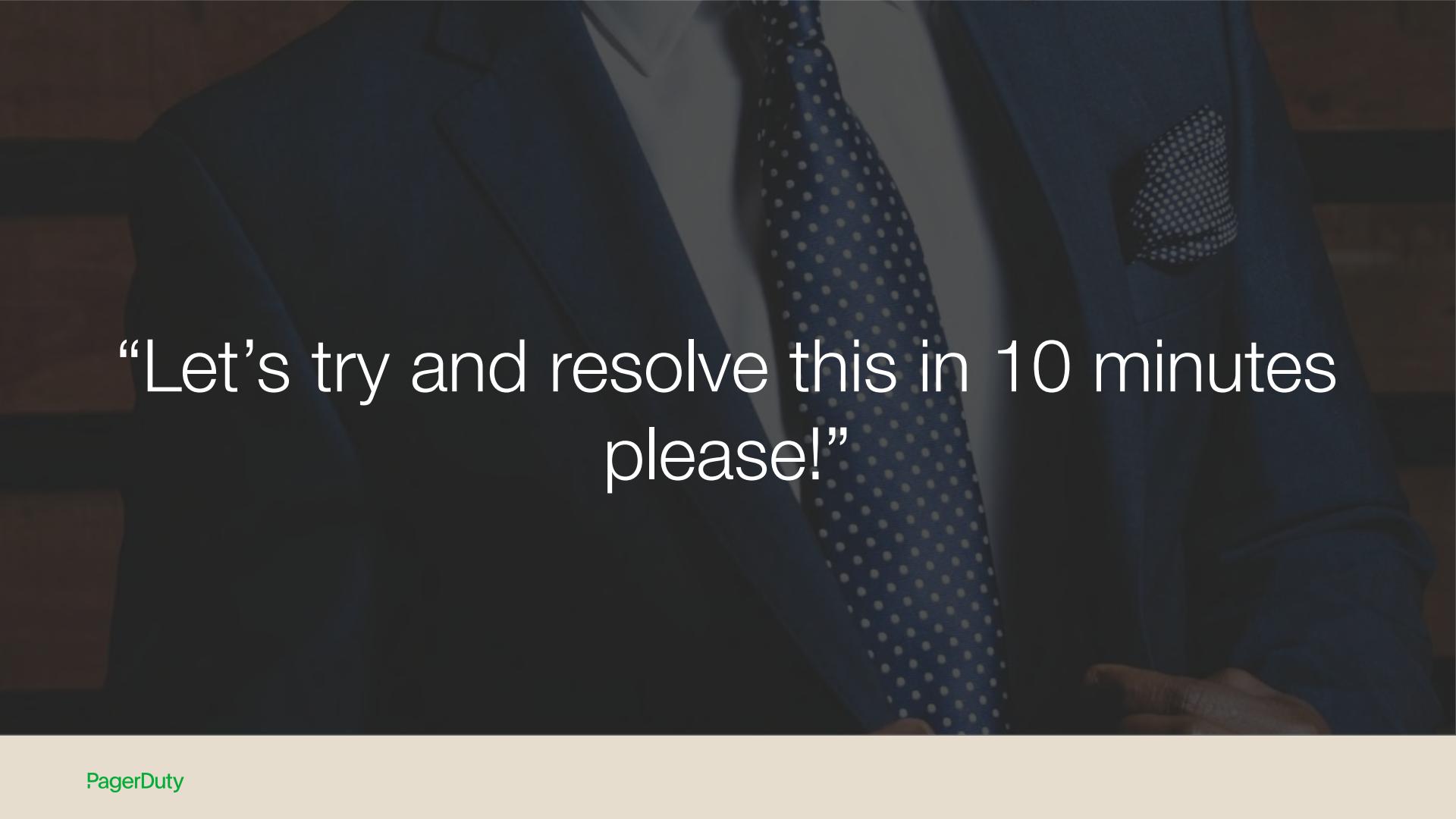
# Importance of the Communications Liaison Roles

- Can be external, internal, or both
- Notifies customers of current conditions, and informs the Incident Commander of relevant feedback
- Crafts language appropriate status updates and notification messages
- Typically a member of the Support team

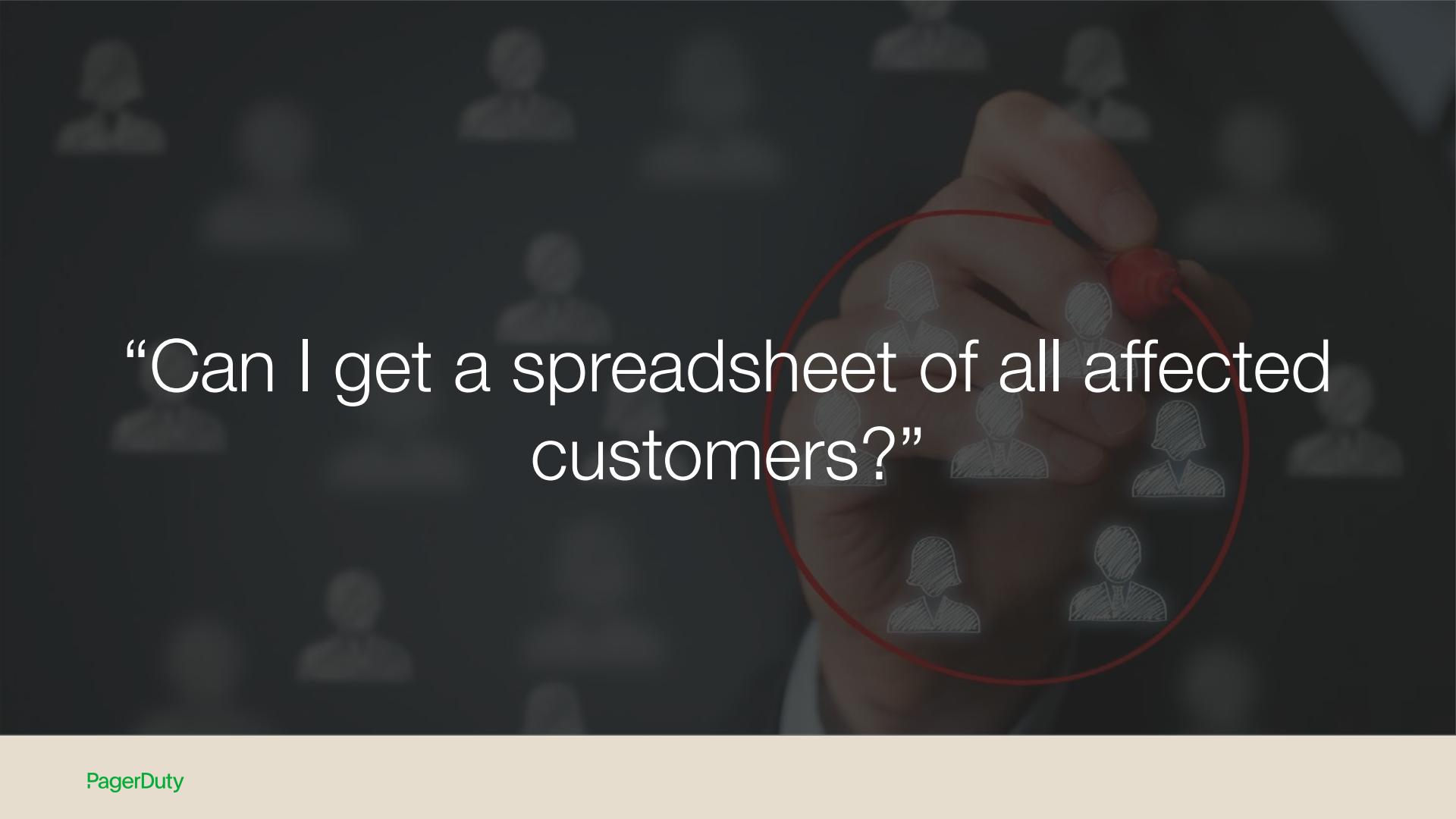
# Incident Response Pitfalls

A dark, grainy photograph of a man with glasses and a mustache, wearing a suit and tie, looking surprised or shocked. He is holding a briefcase.

# Executive Swoop

A close-up photograph of a man from the chest up. He is wearing a dark blue suit jacket over a white shirt and a blue tie with white polka dots. His hands are clasped in front of him. He has short brown hair and is looking slightly downwards and to his right with a neutral to slightly serious expression.

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

A dark background featuring a chalkboard texture. A hand is visible on the right side, holding a red marker and drawing a circle around several small, light-colored user profile icons. The icons represent various people, both male and female. The overall theme suggests a process of identifying specific individuals from a larger group.

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



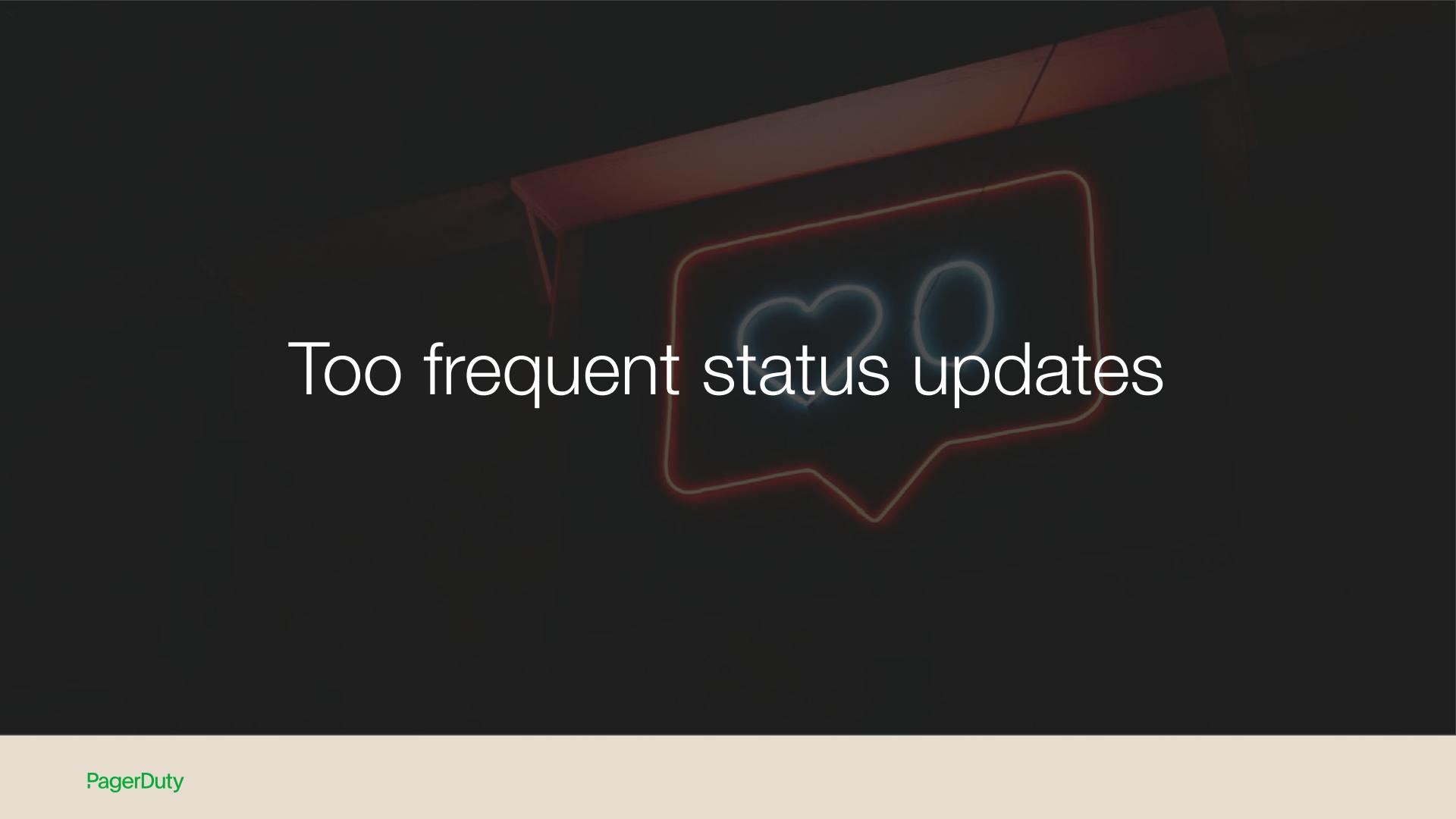
“Do what I say”



Do you wish to take command?



# Failure to Notify Stakeholders



Too frequent status updates

A close-up photograph of a person's face, appearing to be screaming or shouting with their mouth wide open and hands covering their ears. The background is a plain, light color.

# Red Herrings

# Anti-Patterns

- 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 postmortem and follow up activities
- Trying to take on multiple roles
- Not disseminating policy changes
- Getting everyone on the call
- Forcing everyone to stay on the call
- Assuming silence means no progress



How do I prepare to manage  
incident response teams?

# Step 1

Ensure **explicit** processes and expectations exist

## Step 2

Practice running major  
incidents as a team

## Step 3

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

A dark, slightly blurred background image of a clipboard. The clipboard has a white paper titled 'DAILY REPORT SCHEDULE'. On the paper is a grid with columns labeled '7AM', '11AM', and '3PM'. Several checkmarks are visible in the grid, such as a large 'X' in the top row under '7AM' and a large 'V' in the second row under '11AM'. A hand holding a pen is pointing towards the grid.

## 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 !ic 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 postmortem
  - Assign postmortem owner
- Send email to incident-reports@pd.com



STOP

Don't neglect the postmortem

# Postmortems for Beginners

- A Brief Overview: high level of the impact (1-2 sentences)
- What happened: Detailed description, usually 1-2 paragraphs or more depending on length of response efforts
- What went well?
- What didn't go so well?
- Action items - if you don't have any, what was the point of having a response?

# Detailed Postmortems

- Brief Overview: high level of the impact (1-2 sentences)
- What Happened: Detailed description (usually 1-2 paragraphs, or more)
- What went well
- What didn't go so well
- Action Items (if you don't have any, what was the point of having a response?)
- Contributing factors
- Resolution actions
- Impact: who did this affect, by how much, for how long?
- Internal Messaging
- External Messaging (direct either to affected customers or all customers)
- Detailed Timeline of Events

# Summary

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

# Links and Resources:

<https://noti.st/quintessence>



# response.pagerduty.com

PagerDuty Incident Response 

Incident Response > Training > **Incident Commander**



**Home** So you want to be an Incident Commander (IC)? You've come to the right place! You don't need to be a senior team member to become an IC, anyone can do it providing you have the requisite knowledge (yes, even an intern!)

**Getting Started**

**On-Call**

**Being On-Call**

**Who's On-Call?**

**Alerting Principles**

**Before an Incident**

**What is an incident?**

**Severity Levels**

**Purpose**

If you could boil down the purpose of an Incident Commander to one sentence, it would be:

*Keep the incident moving towards resolution.*

The Incident Commander is the decision maker during a major incident; Delegating tasks and listening to input from subject matter experts in order to bring the incident to resolution. They become the highest ranking individual on any major incident call, regardless of their day-to-day rank. Their decisions made as commander are final.

Your job as an Incident Commander is to listen to the call and to watch the incident Slack room in order to provide clear coordination, recruiting others to gather context/details. **You should not be performing any actions or remediations, checking graphs, or investigating logs.** Those

# Q&A

@QuintessenceAnx  
<https://noti.st/quintessence>