

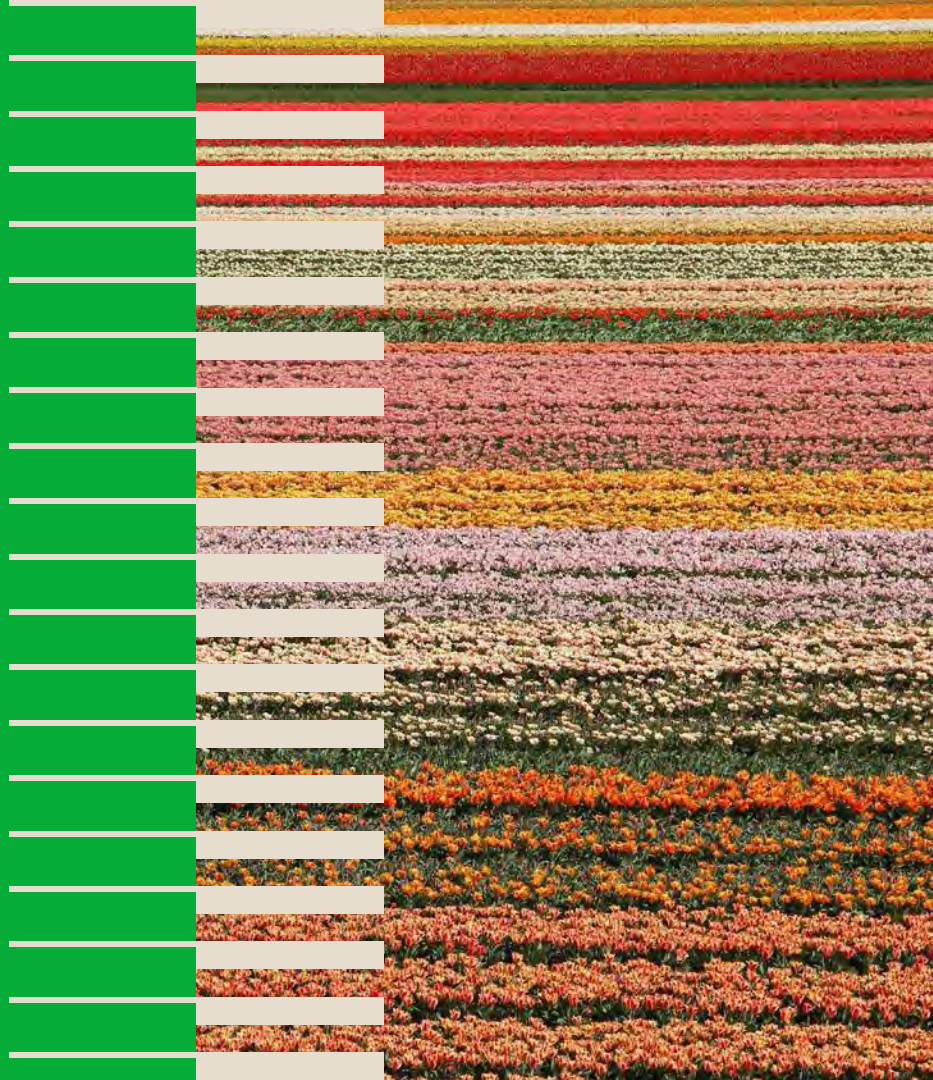
PagerDuty

# Don't Panic!

## Effective Incident Response

*Presented by*  
@QuintessenceAnx  
DevOps Advocate

2021

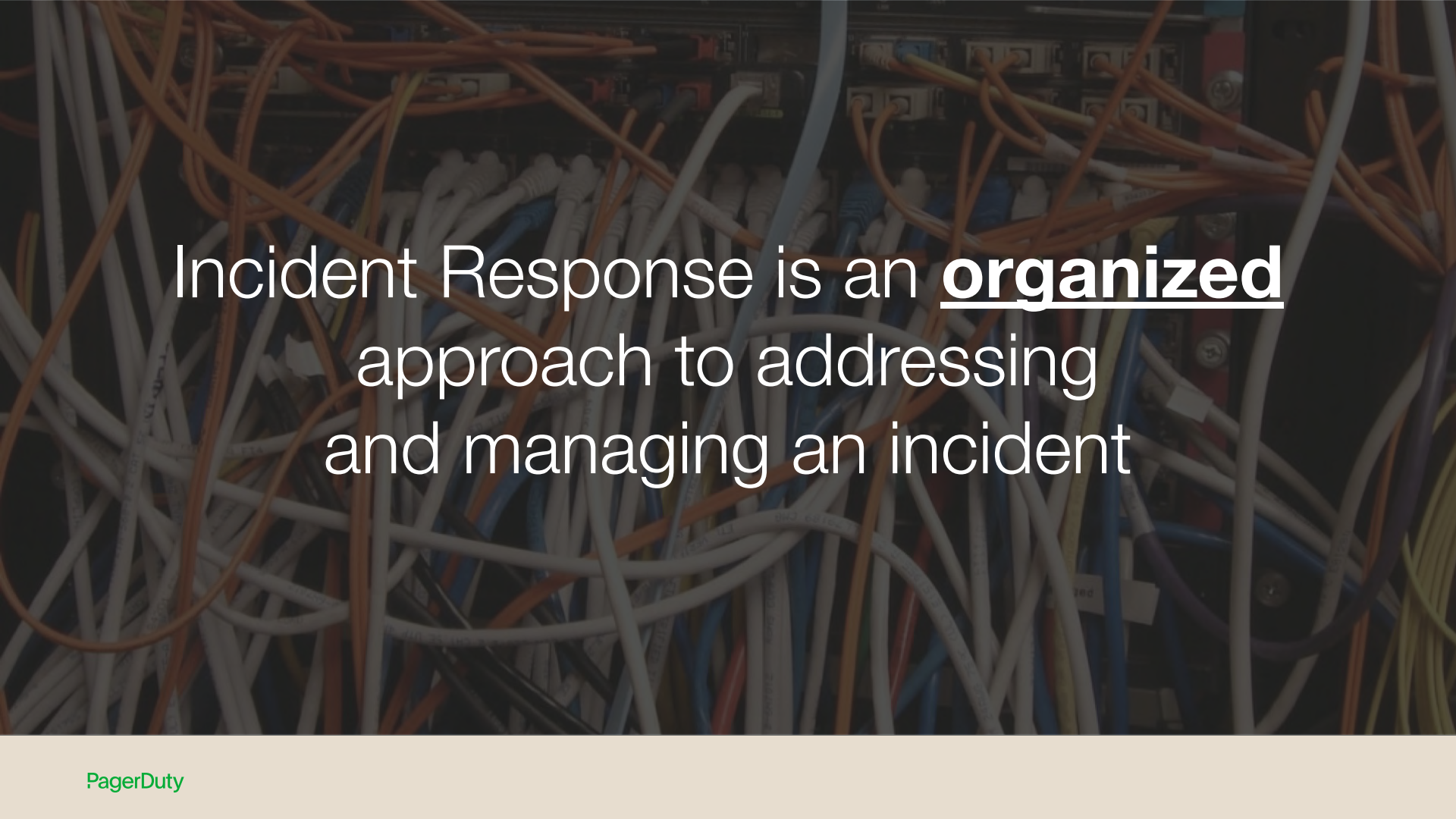


A photograph of a server rack in a data center. The front panel of the server is open, and bright orange and yellow flames are visible inside, indicating a fire. In the background, there are other server racks and a computer monitor. The overall scene is dimly lit, with the fire providing the primary light source.


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

A group of chickens from the movie 'Chicken Run' are shown in a chaotic scene. They have their hands raised, and some are looking towards the camera with wide-eyed, frantic expressions. The background is dark and blurry, suggesting an indoor setting. The overall tone is one of panic and disorder.

Replace chaos with calm



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




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

## 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

A photograph of a wildfire scene. In the upper left, a helicopter is dropping a large amount of water from a bucket. In the foreground, three firefighters in full gear are looking towards the fire. The background is filled with thick smoke and bright orange flames. The overall scene is dark and smoky.

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

A photograph of a server rack on fire. The server rack is the central focus, with bright orange and yellow flames rising from its front. In the foreground, a laptop is open, and its screen is also on fire. The background shows a desk with a computer monitor and other equipment. The overall scene is dark, with the fire providing the primary light source.

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

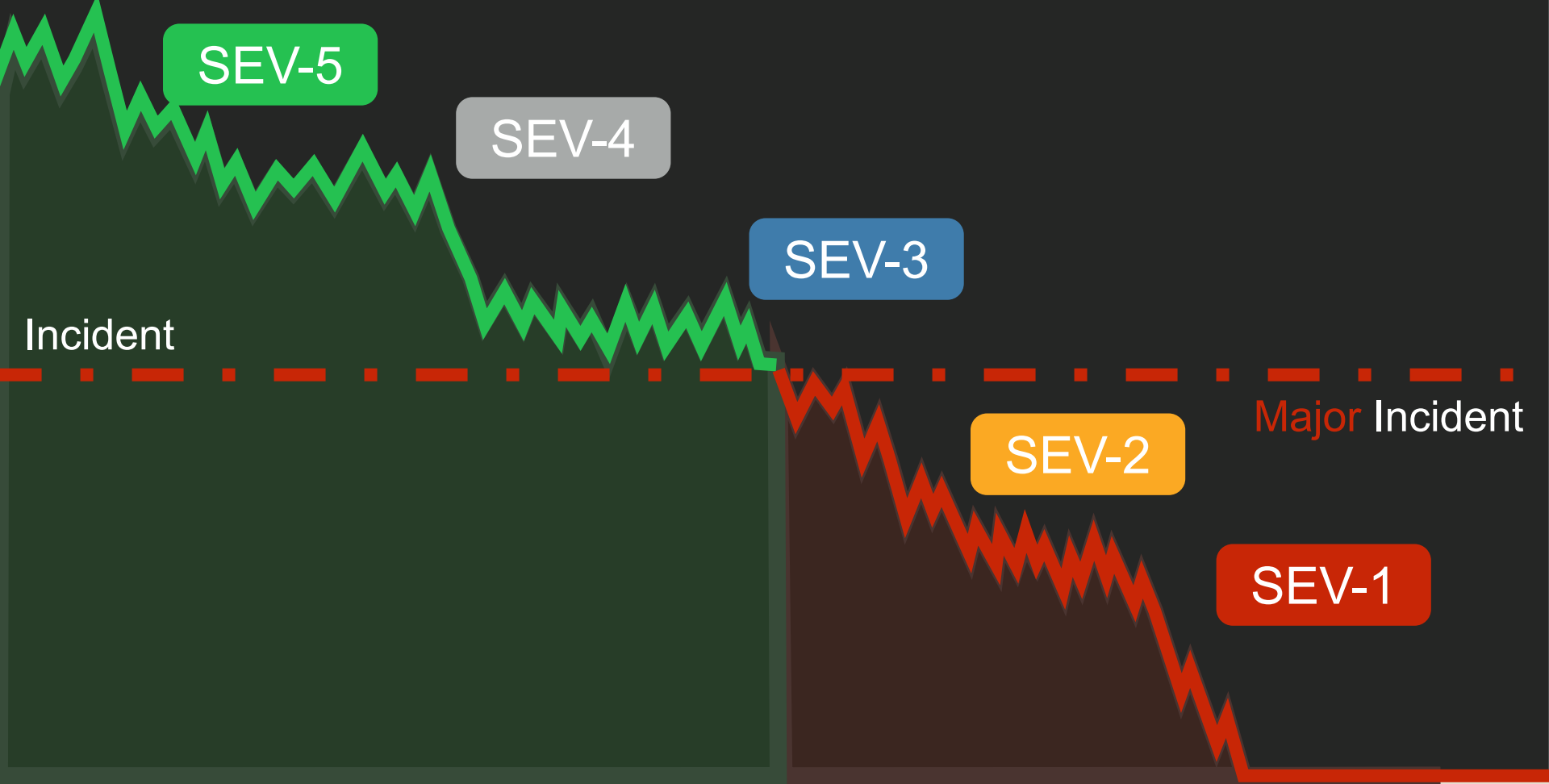


A group of swimmers in red swimsuits and caps are floating in a circle in blue water, holding hands. The scene is viewed from above, creating a circular pattern of hands and bodies in the water. The water has a textured, wavy appearance.

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

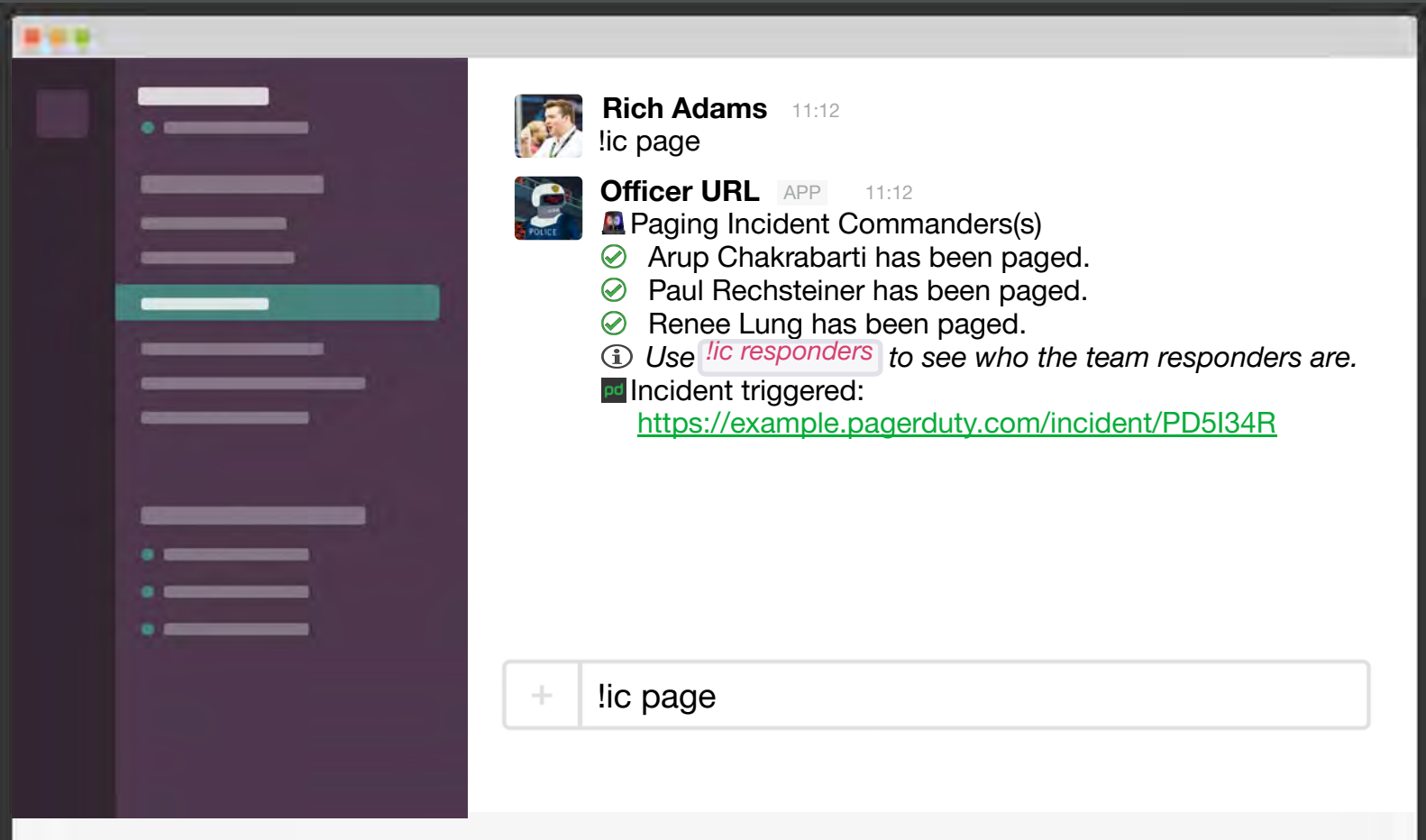
# The 4 Commonalities of Major Incidents

- 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 emergency stop button on a control panel. The button is circular and has a textured surface. It is mounted on a dark blue or grey panel. The background is slightly blurred, showing other parts of the control panel.

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



**Rich Adams** 11:12


!lic page




**Officer URL** APP 11:12

 Paging Incident Commanders(s)

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

 Use **!lic responders** to see who the team responders are.

 Incident triggered:

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

+ !lic page

PEACETIME



WARTIME

NORMAL



EMERGENCY

OK



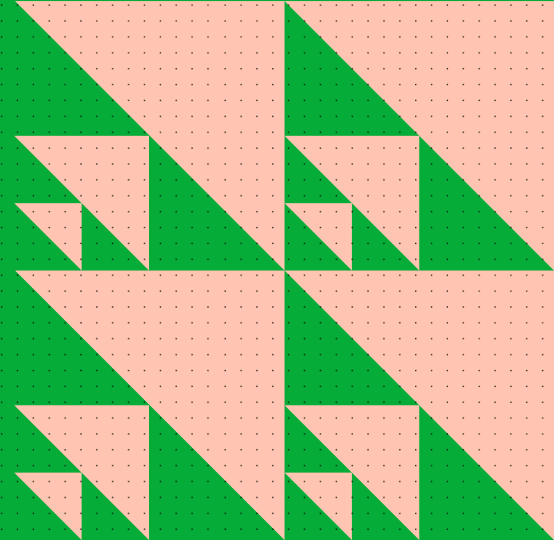
NOT OK



A person with long, dark hair is seen from behind, looking out at a bright, glowing sunset or fire. The scene is dimly lit, with the primary light source being the orange and yellow glow of the sun or fire in the background. The person's hair is dark and appears to be blowing slightly. The overall mood is contemplative and serene.

# Decision Paralysis

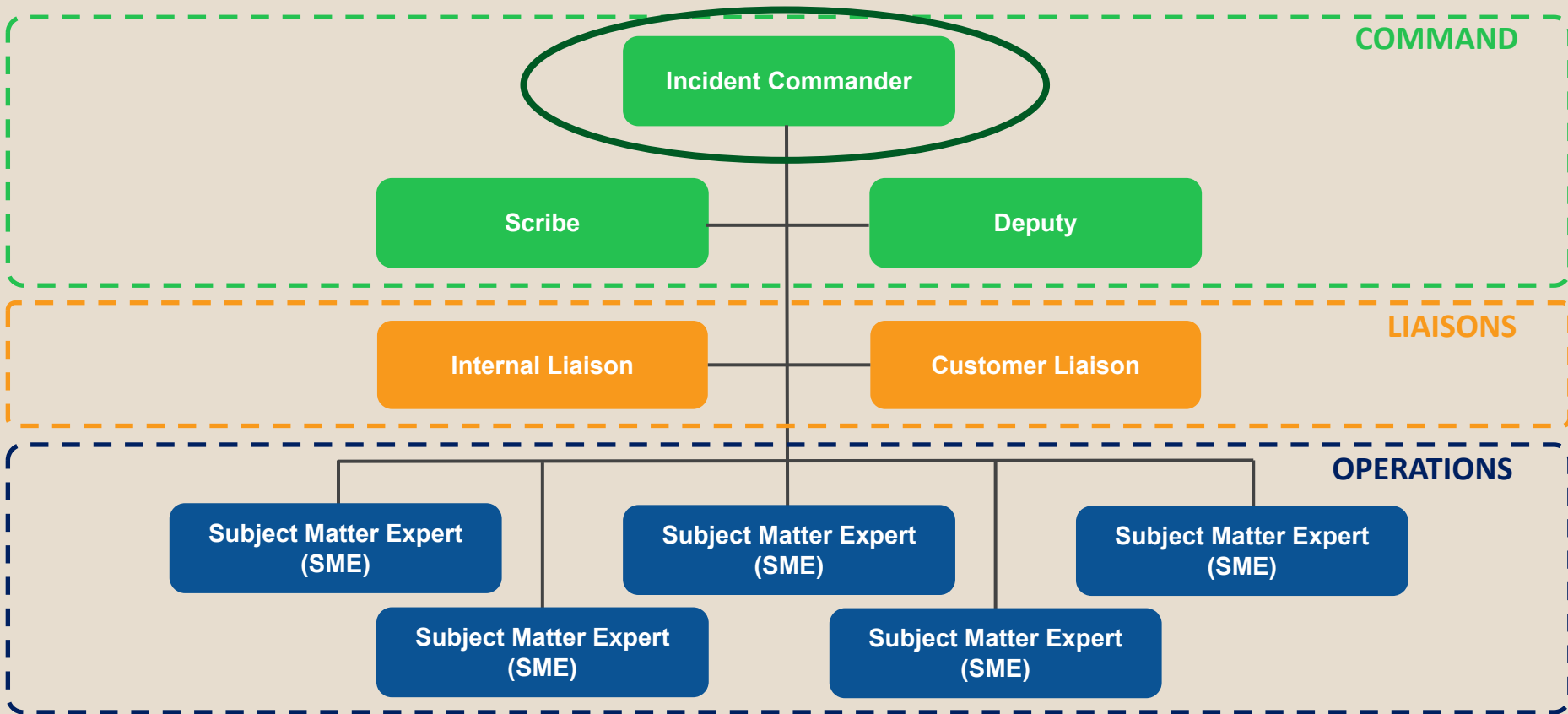
# People Roles & Incident Categorization



# The Four Steps of an Incident



# Roles of Incident Response

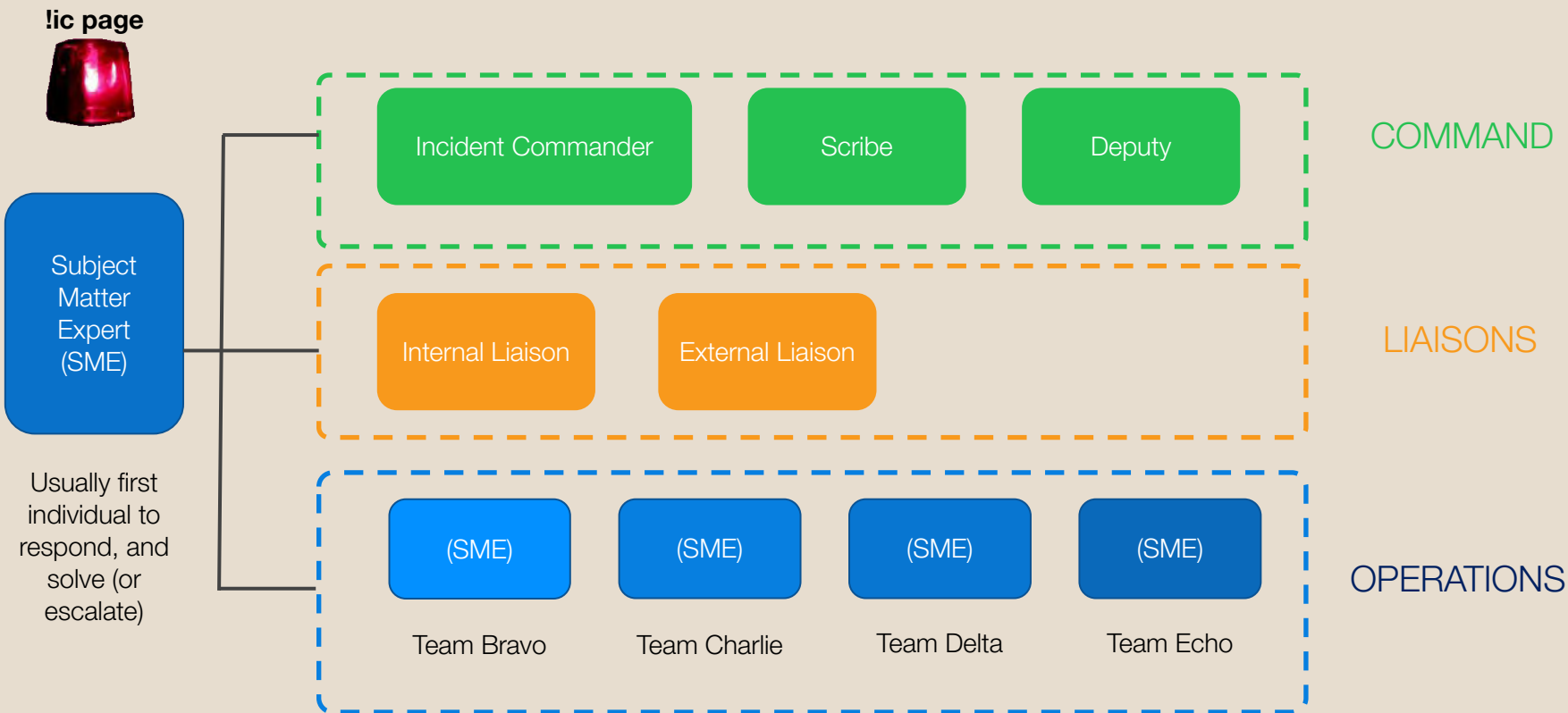


# Setting this up at scale

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)

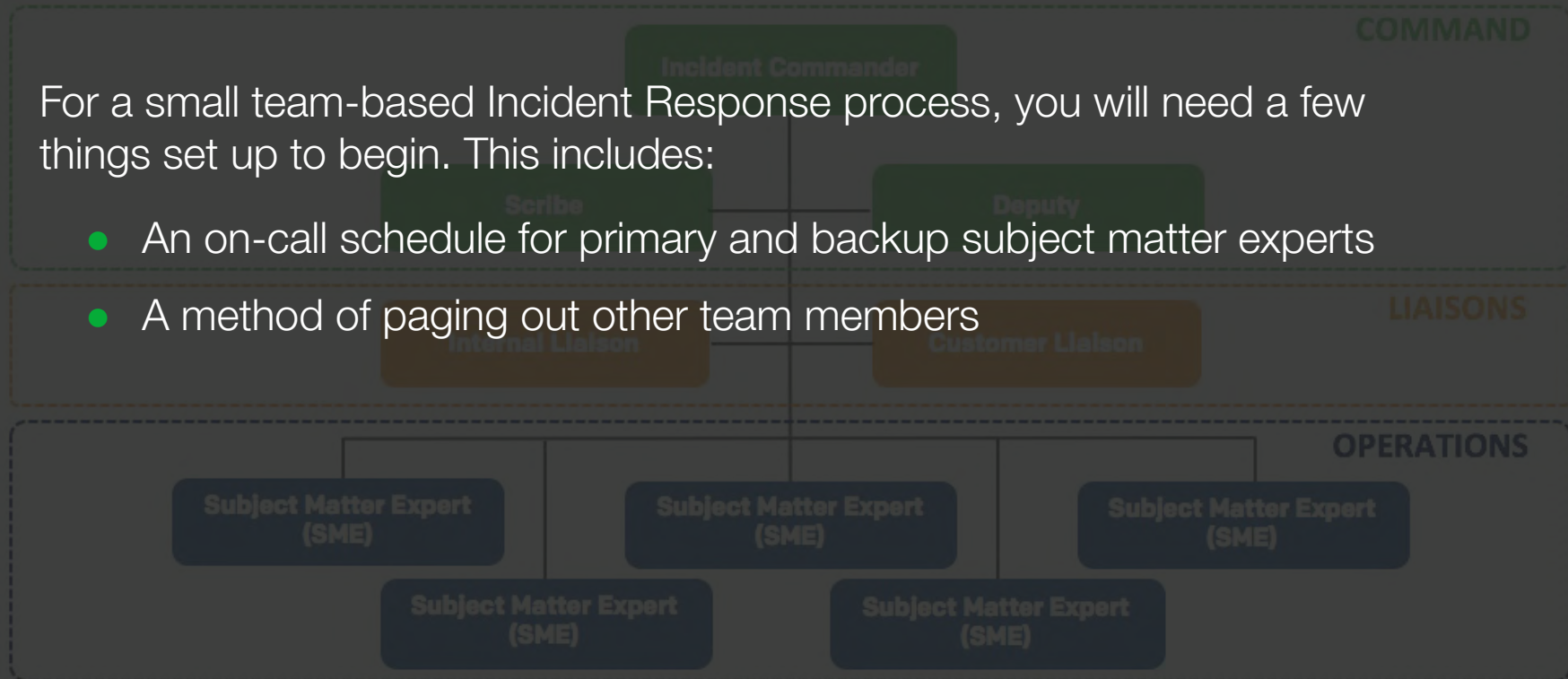
# Incident Response - typical sequence of events



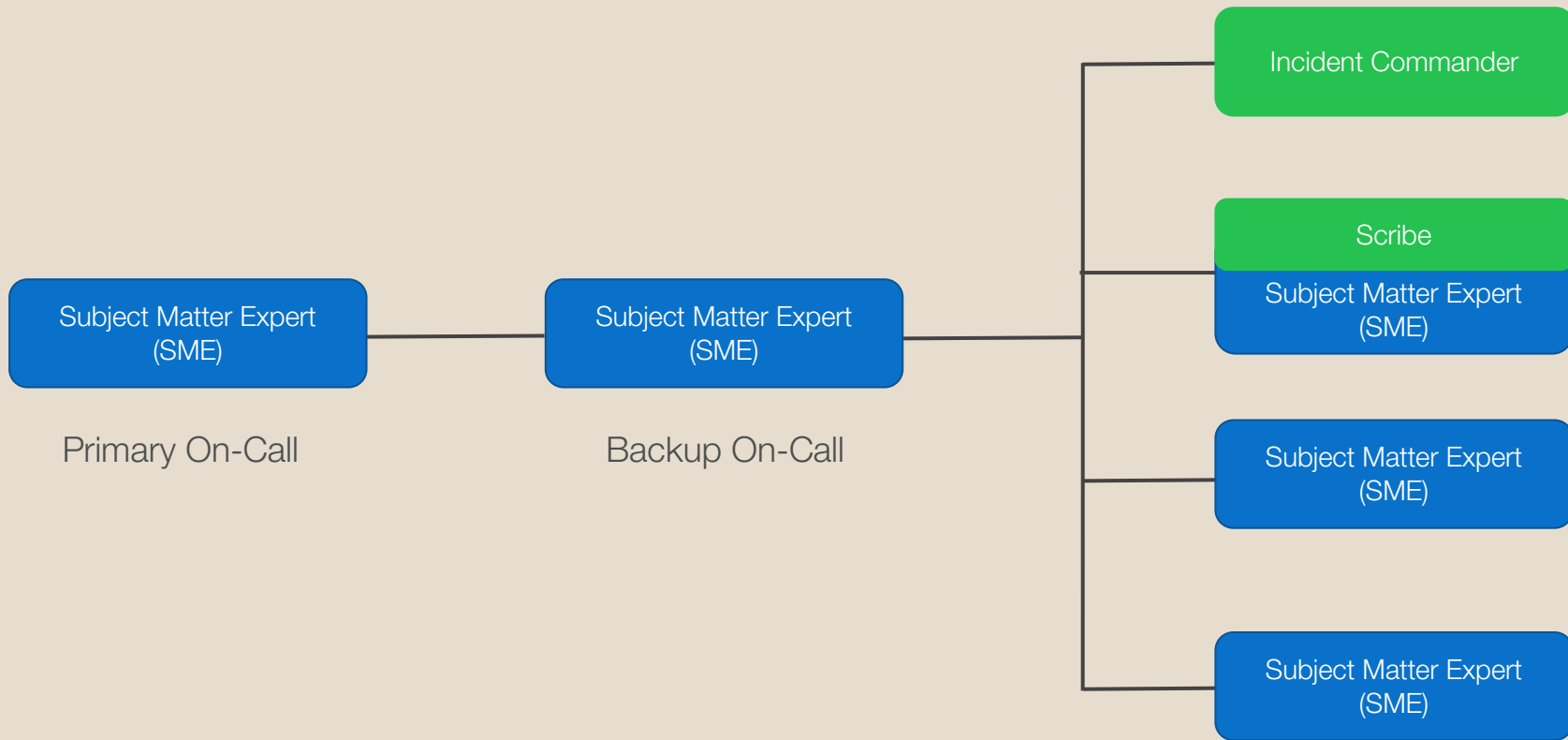
# How Do The Roles Scale Down?

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

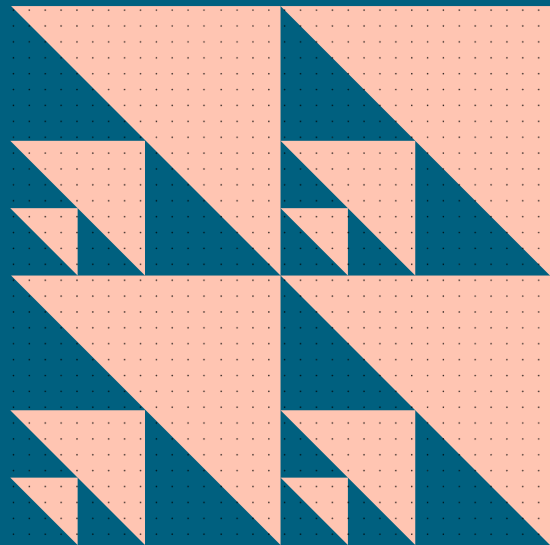


# Small Team Incident Response





# Incident Commander: Role and Responsibilities



A group of chickens from the movie 'Chicken Run' are shown in a chaotic scene. They have their hands raised in the air, and their expressions are one of panic and confusion. The background is dark and blurry, suggesting a night scene or a dimly lit interior. The text 'Replace chaos with calm' is overlaid in the center of the image in a white, sans-serif font.

Replace chaos with calm



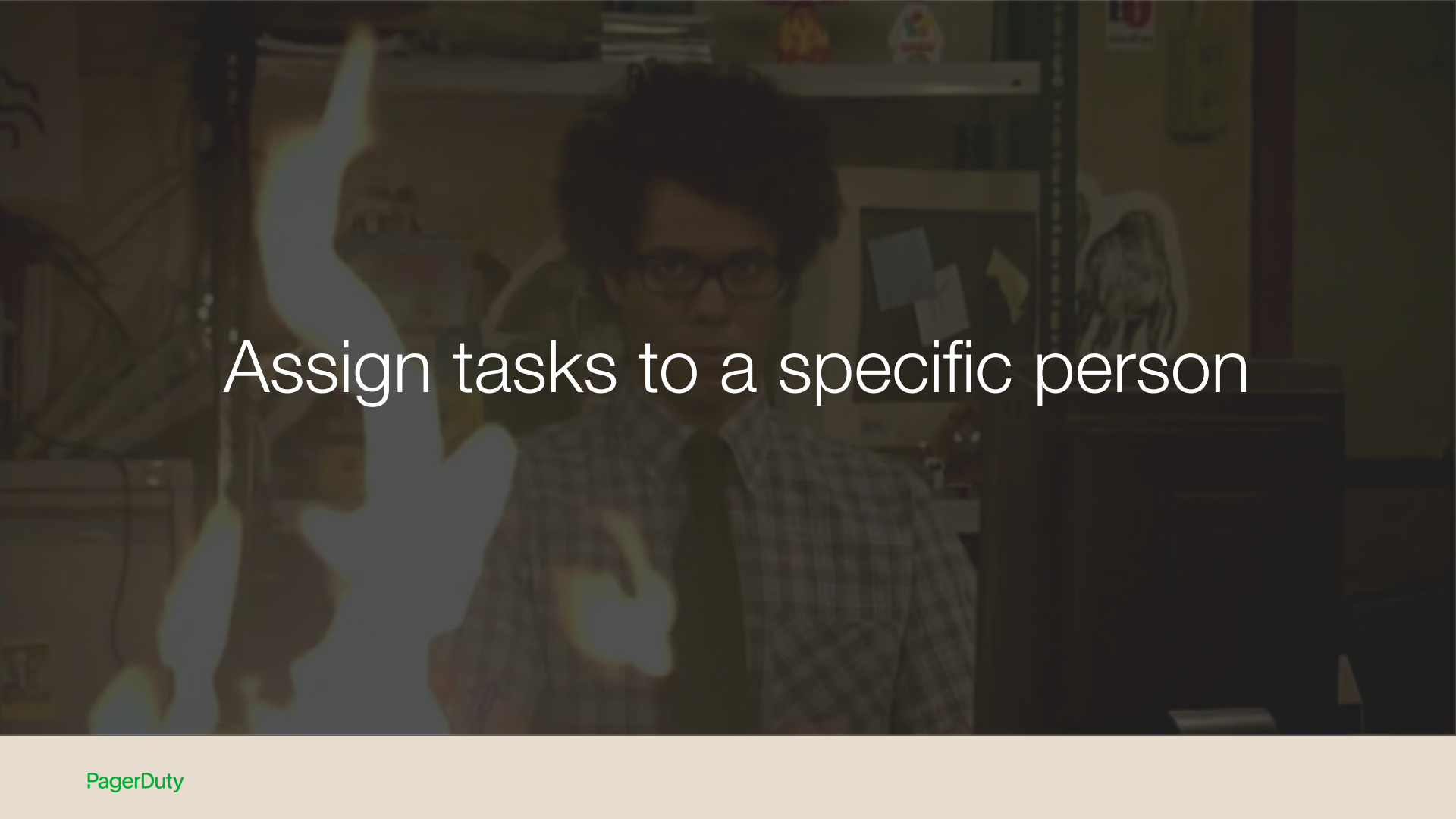
# Single source of reference

The background of the slide features a dark, low-key photograph of a crowd of people. Their arms and hands are raised in various gestures, some pointing upwards, others with palms facing forward. The lighting is dramatic, highlighting the silhouettes against a slightly lighter, hazy background, creating a sense of collective action or agreement.

Gain **consensus**  
“Are there any **strong** objections”



Make a **decision**


A man with glasses and a checkered shirt is pointing at a whiteboard in an office. The whiteboard has a diagram with a central circle and several arrows pointing outwards. The background is slightly blurred, showing office shelves and papers.

Assign tasks to a specific person

A row of five chess pieces is shown against a dark background. From left to right, they are a Bishop, a King, a Queen, a Rook, and a Knight. The pieces are light-colored and have a glossy finish. The text is overlaid on the center of the image.

Becomes the highest authority

(Yes, even higher than the CEO)

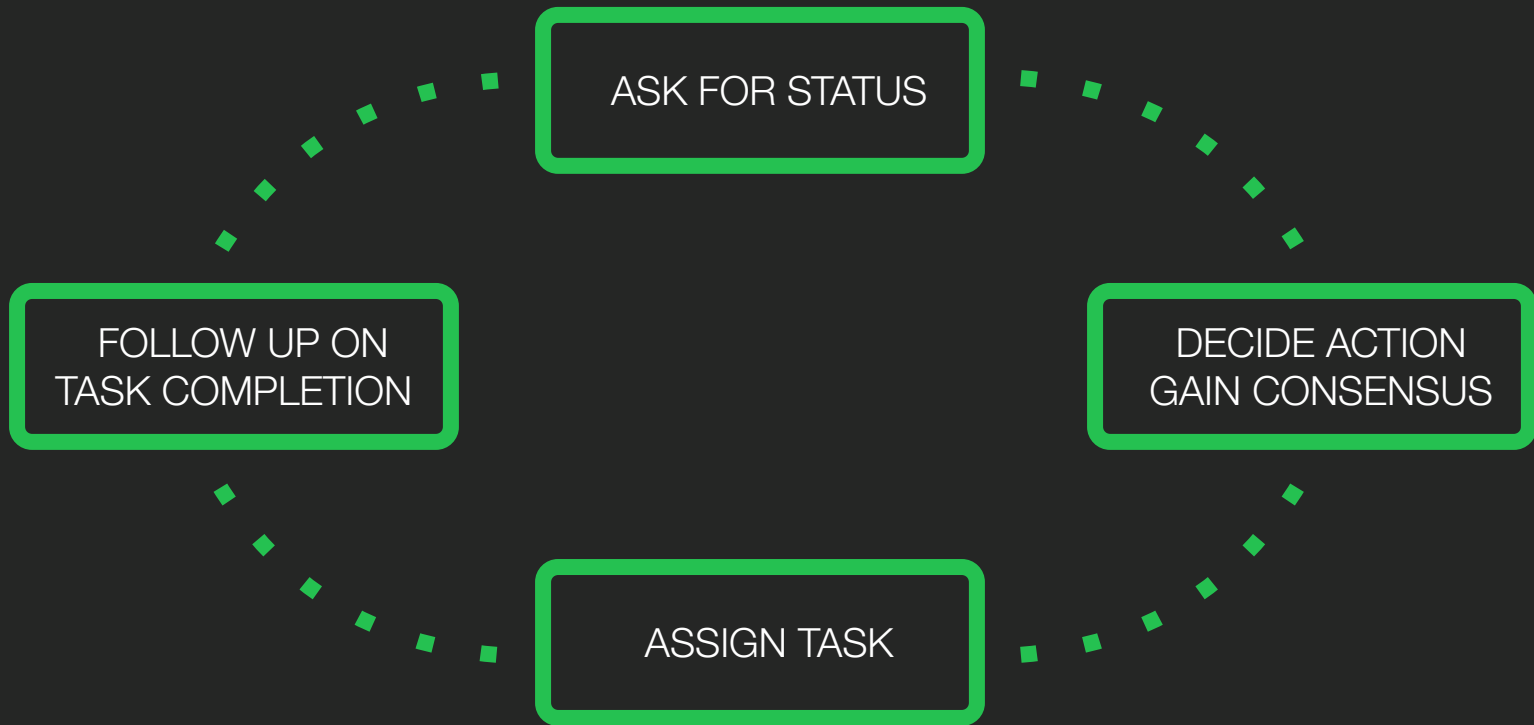


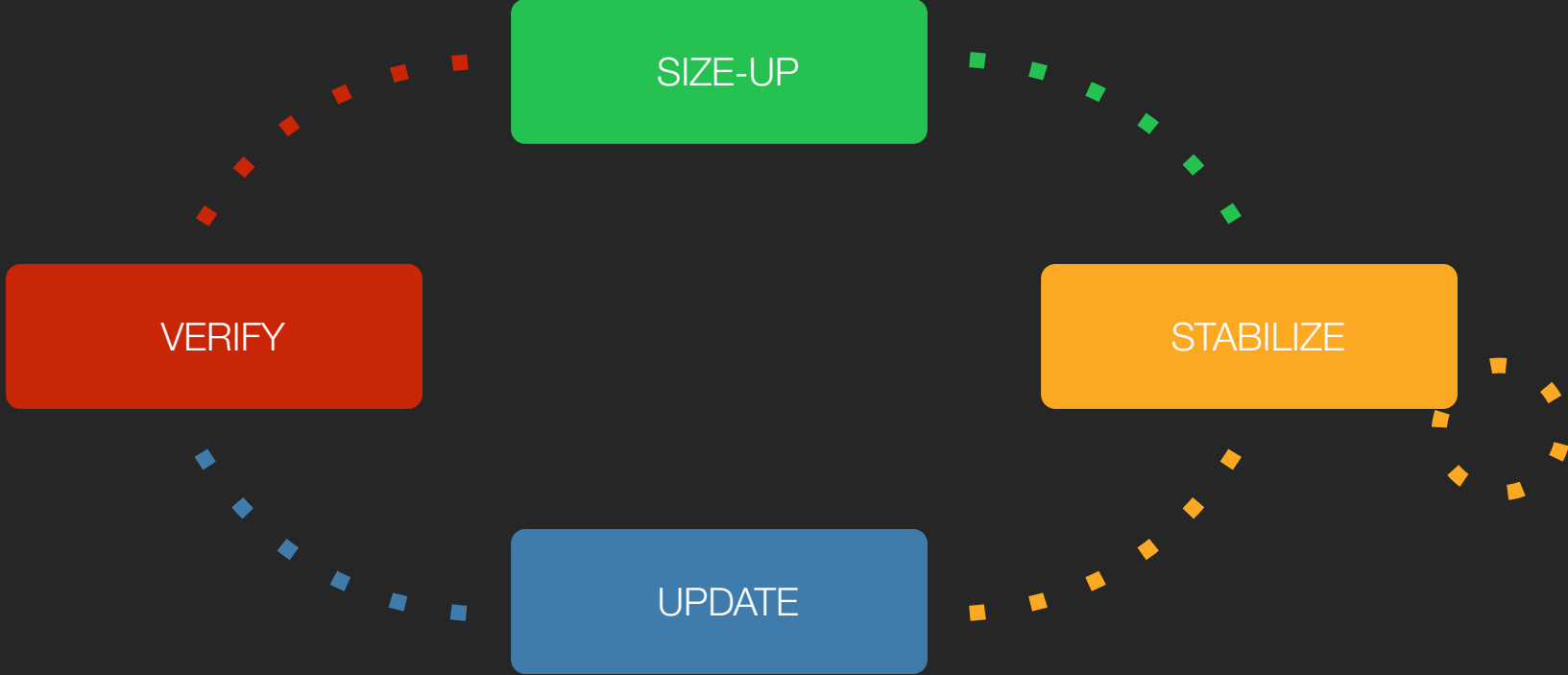
Deep technical knowledge is not required



A photograph showing two people's arms and hands in the process of passing a dark, cylindrical baton. The person on the left is wearing a yellow short-sleeved shirt, and the person on the right is wearing a white short-sleeved shirt. The background is a blurred outdoor setting with a tiled roof and some greenery under a clear sky. The image is dimly lit, with the text overlaid in white.

Handoffs are encouraged





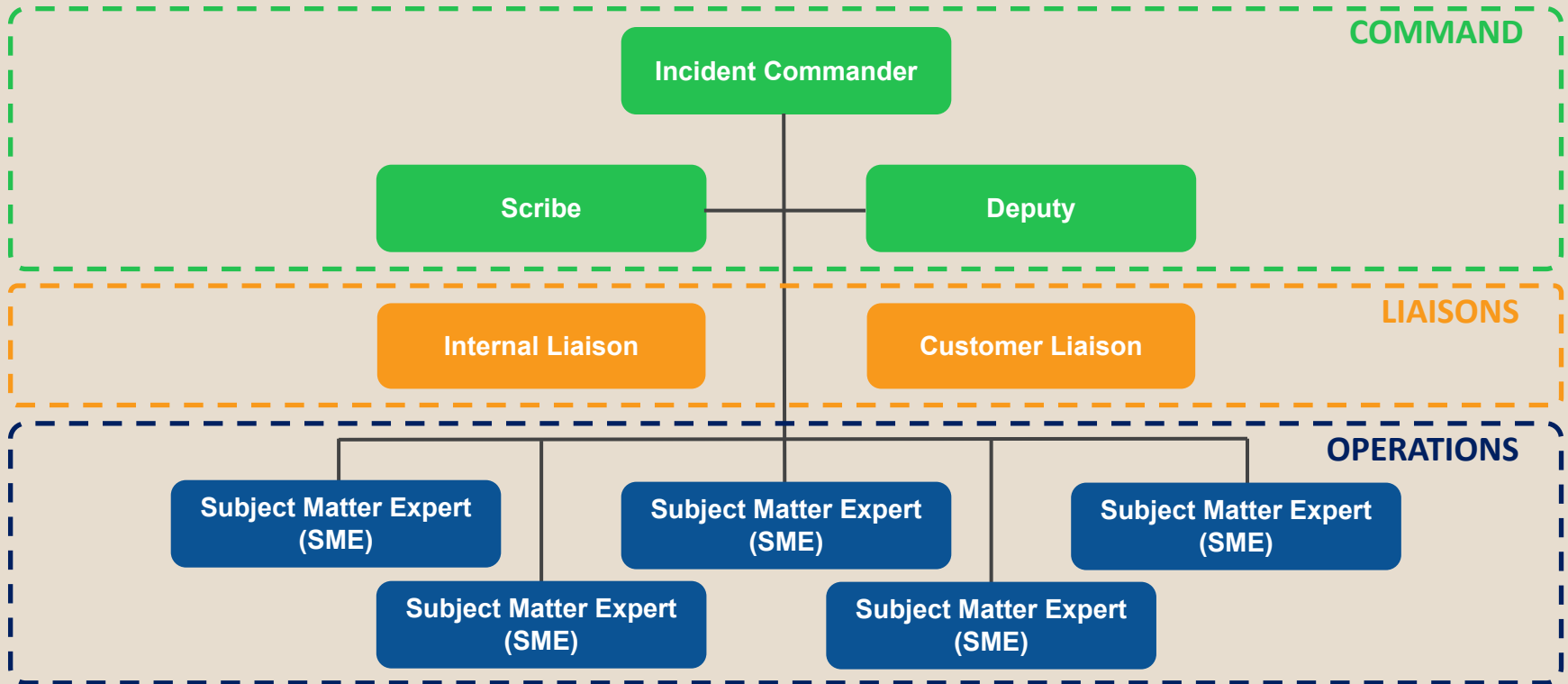
# Quick Tips for New Incident Commanders

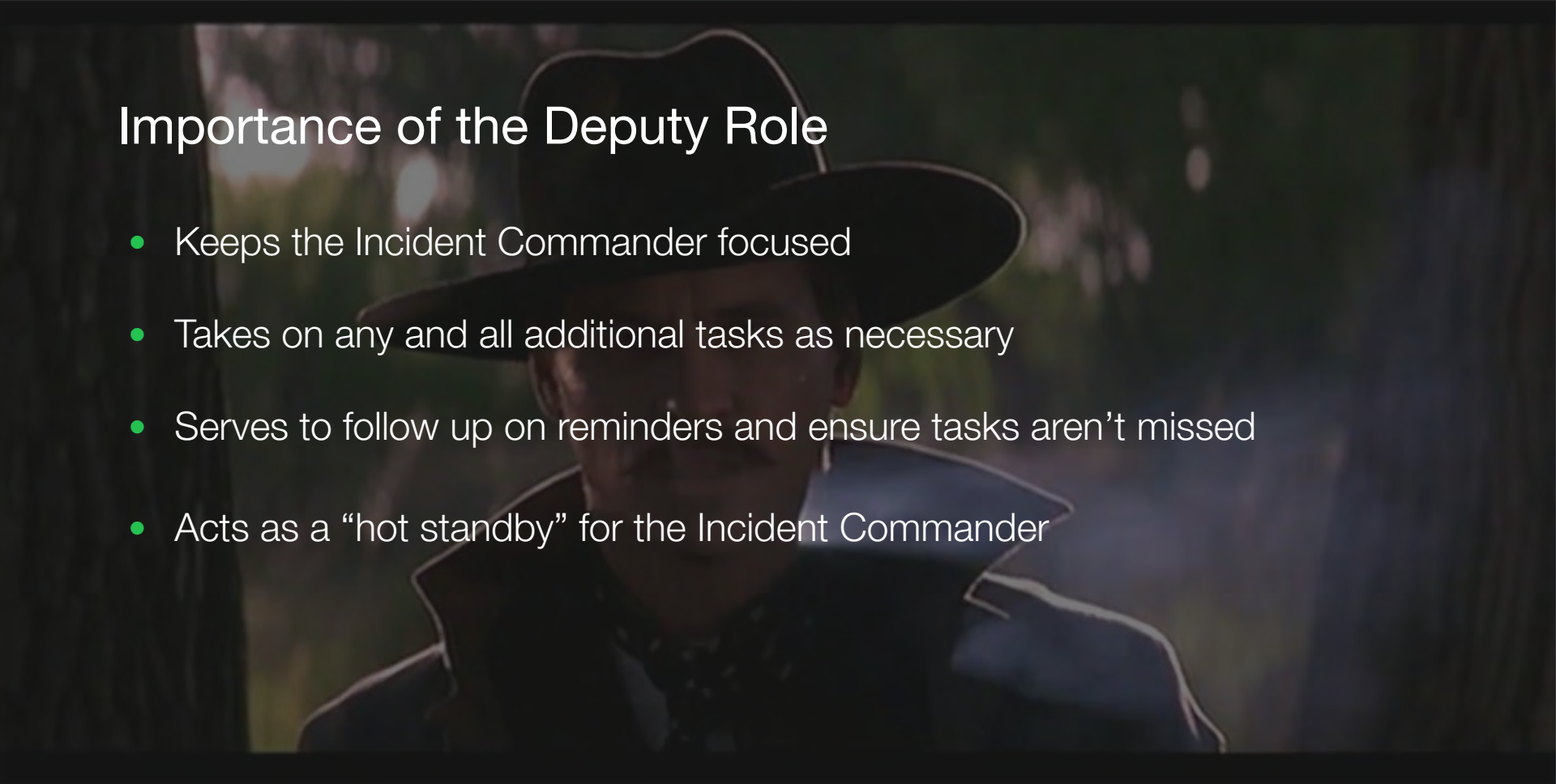
- Introduce yourself on the call with your name and that you are the Incident Commander
- Avoid acronyms
- Speak slowly and with purpose
- On the call, kick people off if they are being disruptive
- Time-box tasks and check in for status updates
- Explicitly declare when the response has ended

# 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

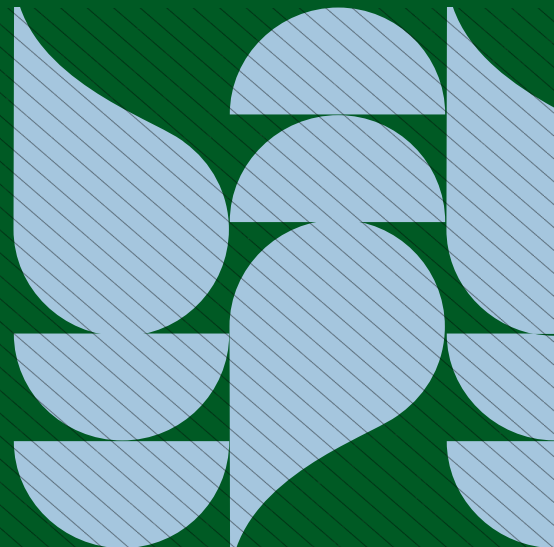
- Documents the incident timeline and important events as they occur
- The incident log will be used during the post-mortem process
- Note when important actions are taken, follow-up items, and status updates
- Anyone can be a Scribe



# 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 man in a light-colored suit, white shirt, and patterned tie, wearing glasses, is looking directly at the camera with a wide-eyed, surprised expression. His right hand is resting on a wire mesh basket. The background is a dimly lit office or hallway.

# Executive Swoop

A person wearing a blue suit jacket, a light blue shirt, and a blue tie with white polka dots. A patterned pocket square is visible in the jacket's breast pocket. The background is a brick wall. The image is dimmed to serve as a background for the text.

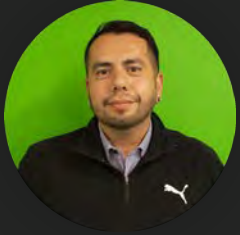
“Let’s try and resolve this in 10 minutes please!”



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



“Do what I say”



Do you wish to take command?

...



A miniature construction site is set up on a computer keyboard. Two tiny workers in blue jumpsuits and white hard hats are working. One worker in the foreground is carrying a pickaxe over his shoulder and walking across the keys. Another worker is behind him, also carrying a pickaxe. Several orange and white traffic cones are placed on various keys, including 'E', 'D', 'C', 'B', 'N', and 'M'. A green wheelbarrow is visible on the right side of the keyboard. The entire scene is dimly lit, with the text 'Failure to Notify Stakeholders' overlaid in the center.

# Failure to Notify Stakeholders





Too frequent status updates

A close-up photograph of a young child crying intensely. The child's eyes are closed, and their hands are pressed against their cheeks, partially covering their eyes. Their mouth is wide open in a cry. The image is dimmed with a dark grey overlay. The text "Red Herrings" is centered over the child's face.

# Red Herrings

# Anti-Patterns

A wooden gavel and a wooden mallet are positioned on a wooden surface. The gavel is on the left, and the mallet is on the right. The background is a dark, textured wood grain.

- 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

An open notebook with a fountain pen and a pen cap on a dark surface. The notebook is open to a blank page, and the pen is lying on the left page. The pen cap is lying on the right page. The background is dark and textured.

## Step 3

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

A hand is shown writing on a checklist titled "DAILY REPORT SCHEDULE". The checklist has columns for "PATIENT NAME", "TIME", and "STATUS". The "TIME" column has sub-columns for "7AM", "11AM", and "5PM". The "STATUS" column has checkboxes. A pen is writing a checkmark in the "7AM" column under the "PATIENT NAME" column. The text "Step 4" is written in green, and "Make Checklists" is written in white below it.

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



Don't neglect the postmortem

# Postmortems for Beginners

A miniature construction worker in orange overalls and a hard hat is standing on a keyboard. The worker is holding a hammer and appears to be working on the keys. The background is a dark, blurred image of a keyboard.

- 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

Getting Started

On-Call

Being On-Call

Who's On-Call?

Alerting Principles

Before an Incident

What is an Incident?

Severity Levels

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!)

### 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>