

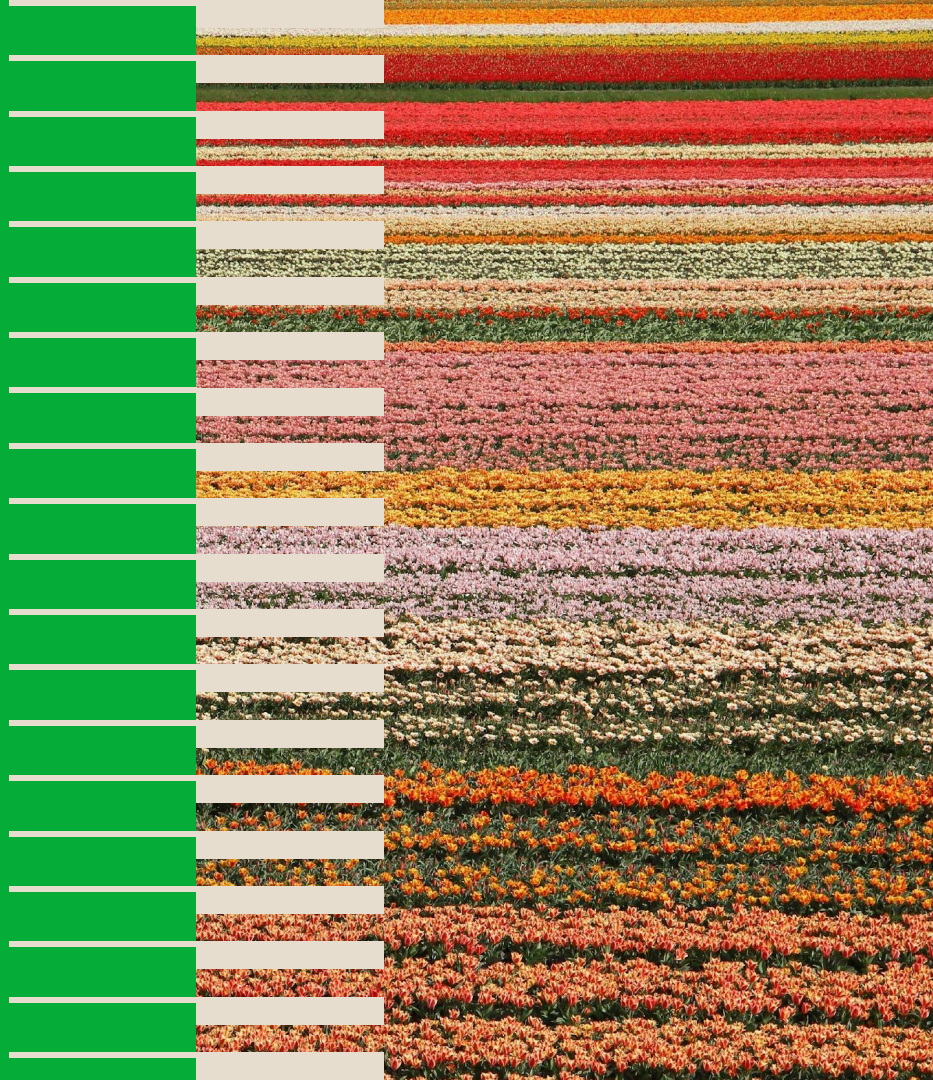
PagerDuty

Don't Panic!

Effective Incident Response

Presented by
@QuintessenceAnx
DevOps Advocate

2021



What We'll Be Learning Today:

After completing this training, you will be able to:

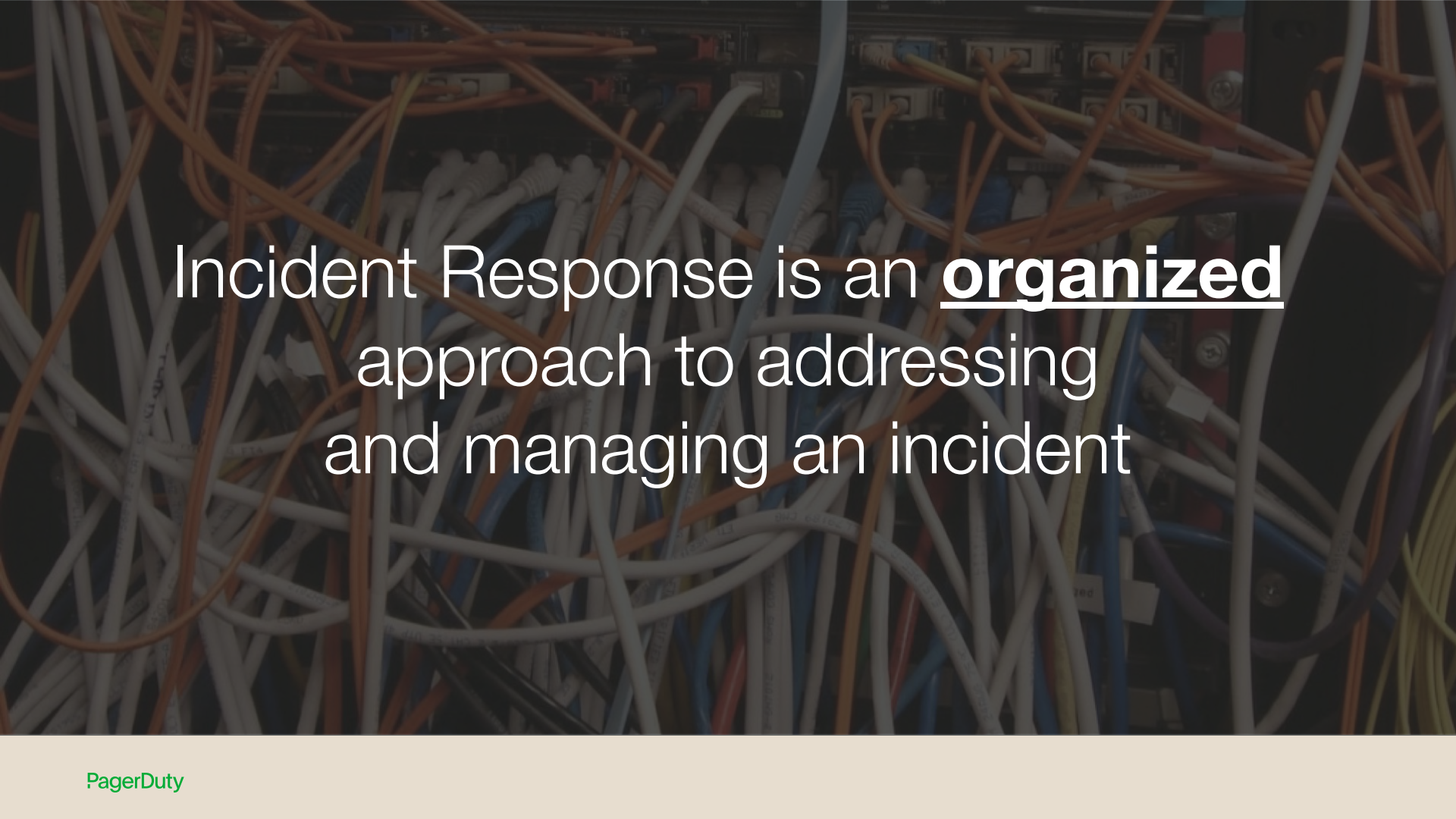
- Build a foundation for an effective incident response process in your organization
- Understand suggested practices needed for successful incident response
- Identify practices that limit damage and reduce recovery time and costs

A photograph of a server rack in a data center. The server rack is open, and a bright fire is burning inside, with flames reaching up. In the background, there are other server racks and a computer monitor. The overall scene is dimly lit, with the fire providing the main 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 holding tools like a hammer and a saw. The text 'Replace chaos with calm' is overlaid in the center of the image.

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 firefighter helicopter is shown in the upper left, dropping a large volume of water onto a wildfire. The fire is intense, with bright orange and yellow flames rising from a line of trees. In the foreground, three firefighters in full protective gear, including helmets and oxygen tanks, are standing and observing the operation. The scene is set in a wooded area with some brush in the immediate foreground.

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

A photograph of a server room with a server rack on fire. The server rack is in the foreground, and the fire is bright orange and yellow. In the background, there are several computer monitors and a tower PC. The text is overlaid on the image.

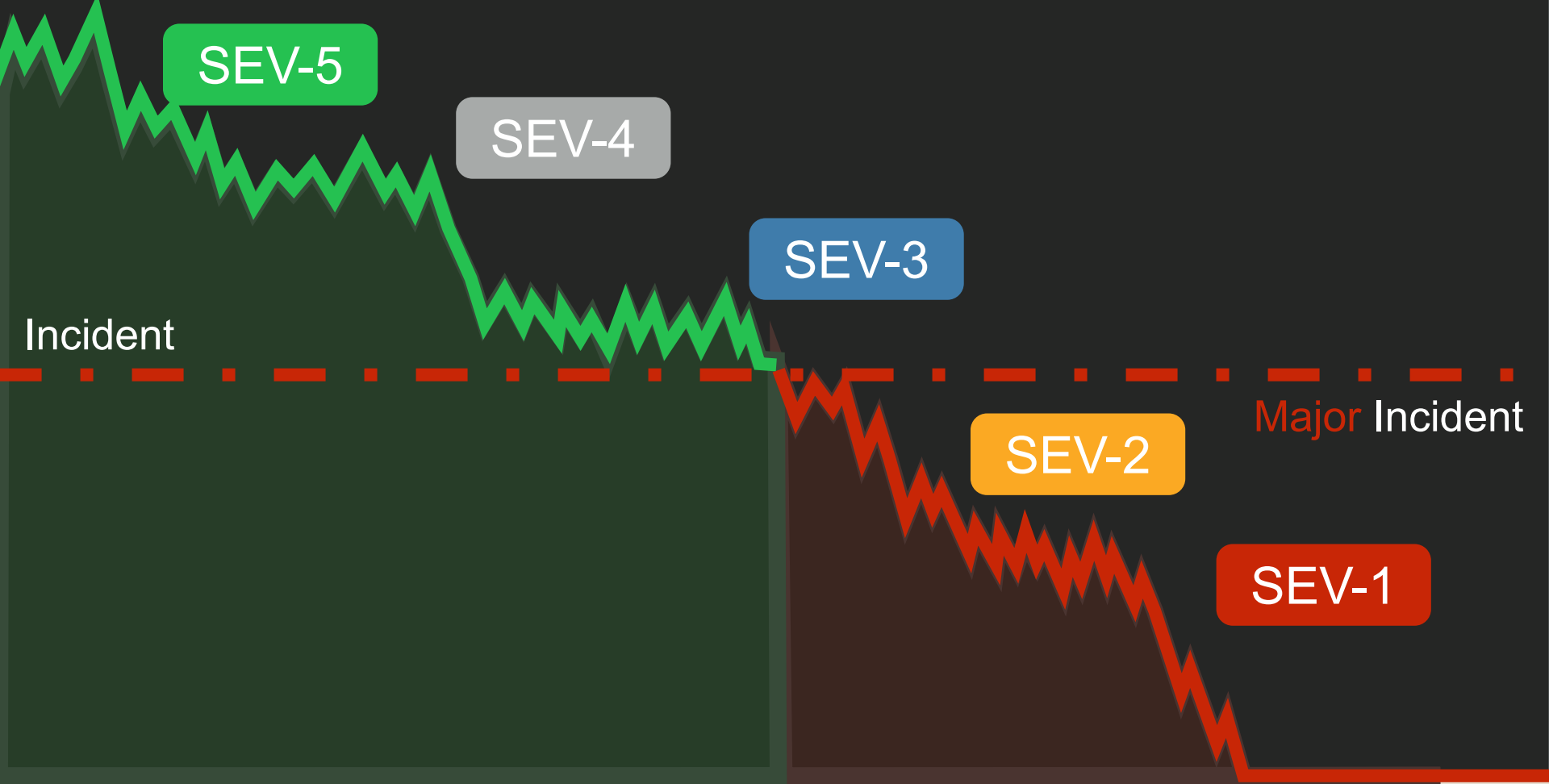
An incident is an unplanned
disruption or event that requires
immediate attention or action



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

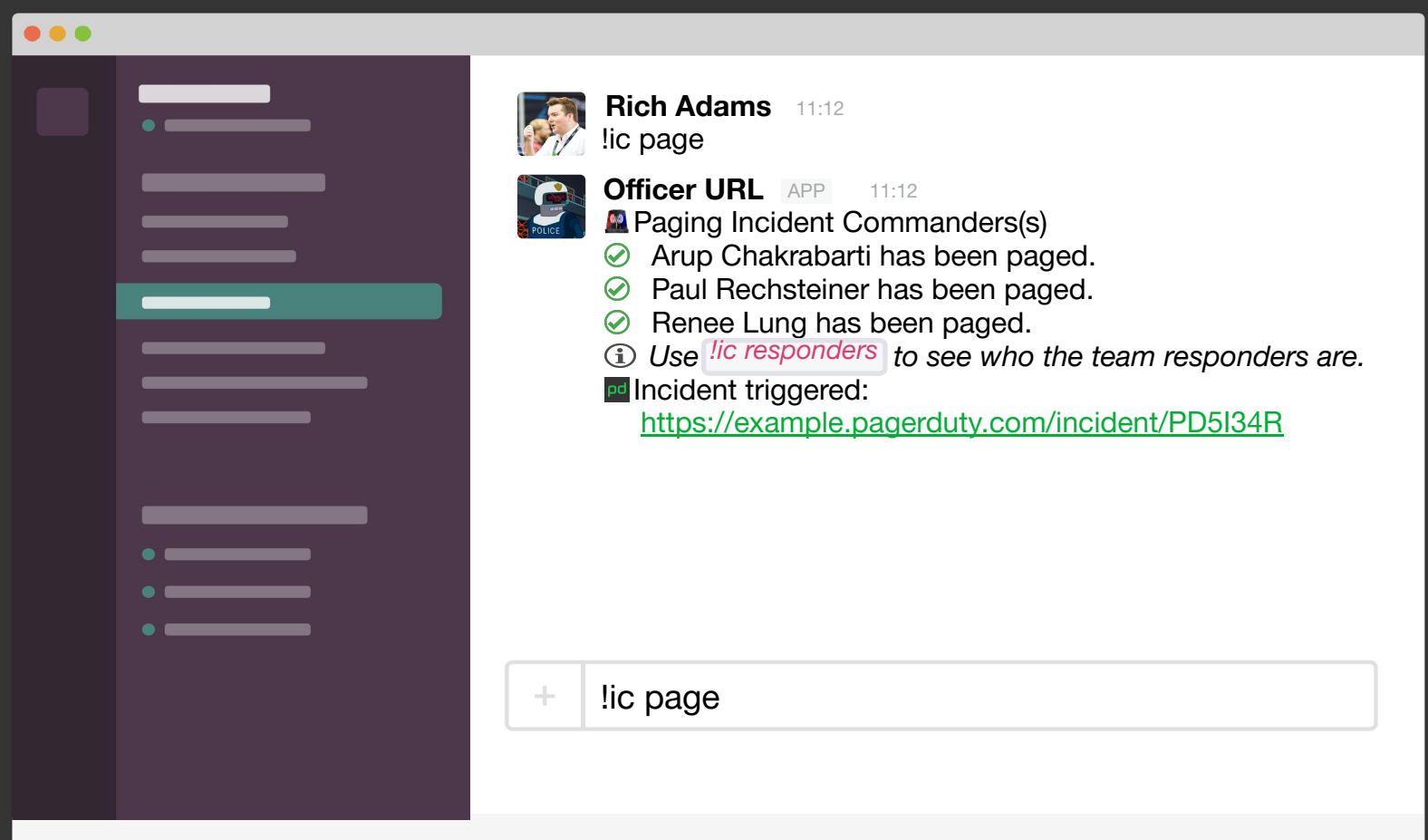
The 4 Commonalities of Major Incidents

- 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

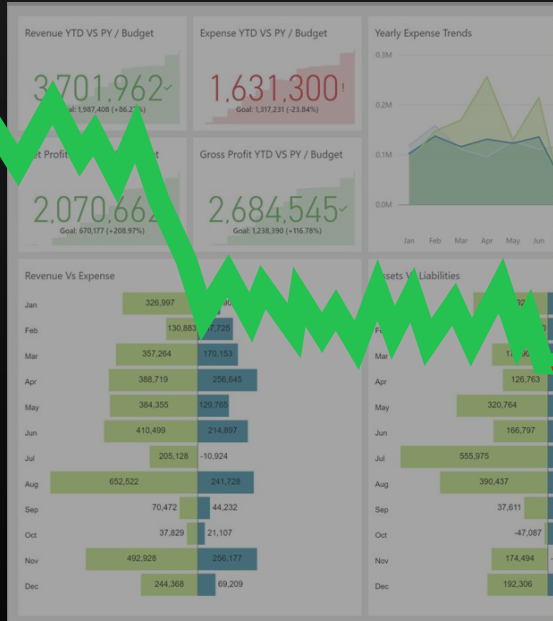


A close-up photograph of a red emergency button on a control panel. The button is oval-shaped and has a glossy finish. It is mounted on a dark blue or grey panel. The background is slightly blurred, showing other parts of the panel. The text is overlaid on the image in white.

Anyone can trigger the Incident Response Process at any time



PEACETIME



...s has been shut down to prevent damage

this Stop error screen, appears again, follow

... software is properly installed. ... your hardware or software manufacturer

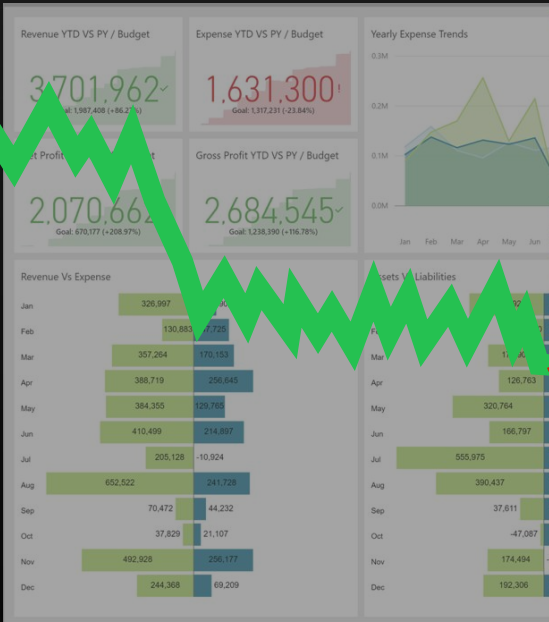
...ve any newly installed hardware ... ons such as caching or shadowing. ... or disable components, restart ... anced Startup Options, and then

```
000001, (0x01ccc7,0x00000000)
base at 454500, Datestamp 4d5dd88c
```

... technical support

WARTIME

NORMAL



...s has been shut down to prevent damage

this Stop error screen, appears again, follow

... software is properly installed. Your hardware or software manufacturer

...ve any newly installed hardware or software components, such as caching or shadowing. Disable or disable components, restart the computer with Advanced Startup Options, and then

```
000001, (0x00000000, 0x00000000)
base at 0x54500, Datestamp 4d5dd88c
```

... technical support

EMERGENCY

OK

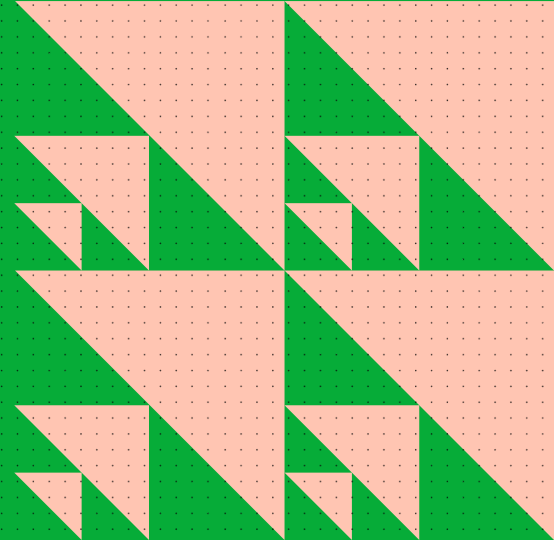


NOT OK

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

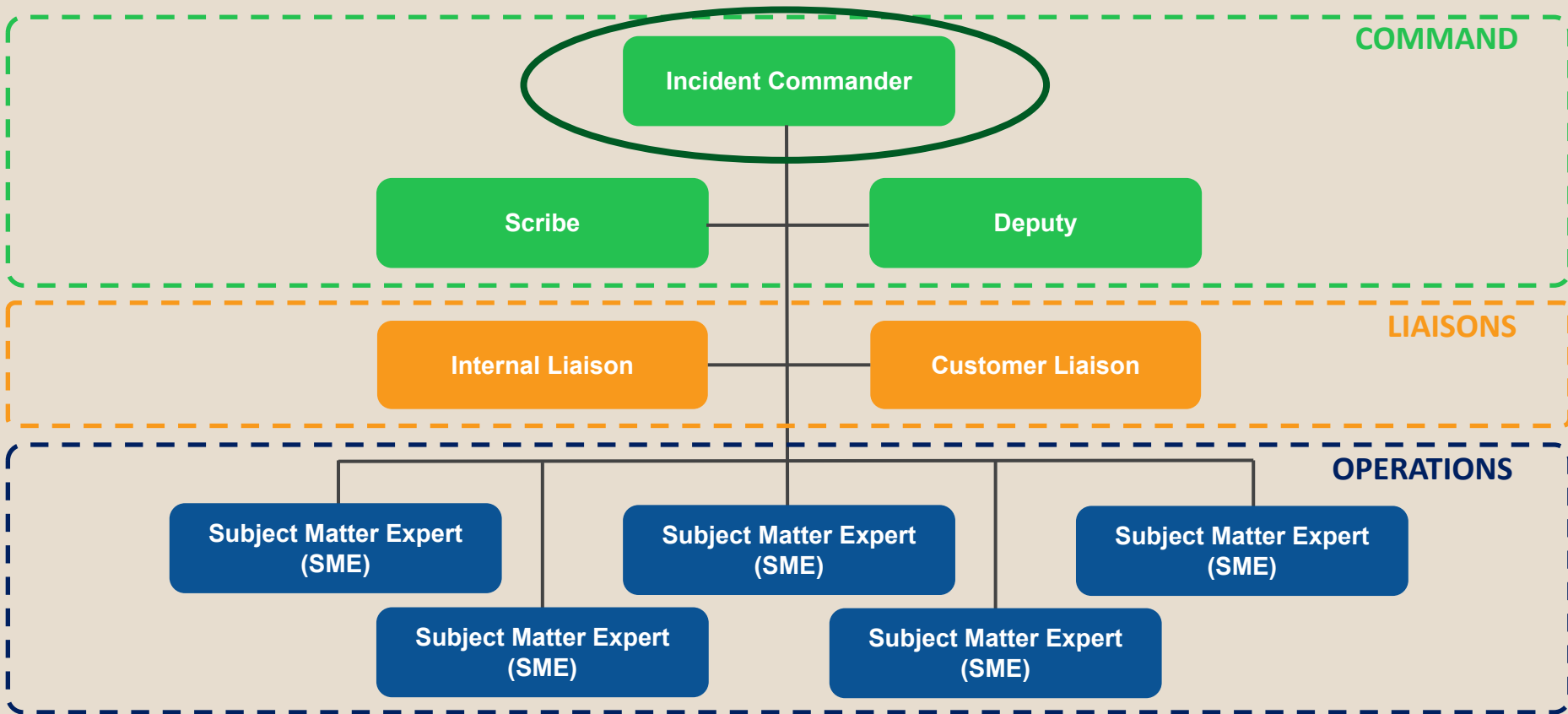
People Roles & Incident Categorization



The Four Steps of an Incident



Roles of Incident Response

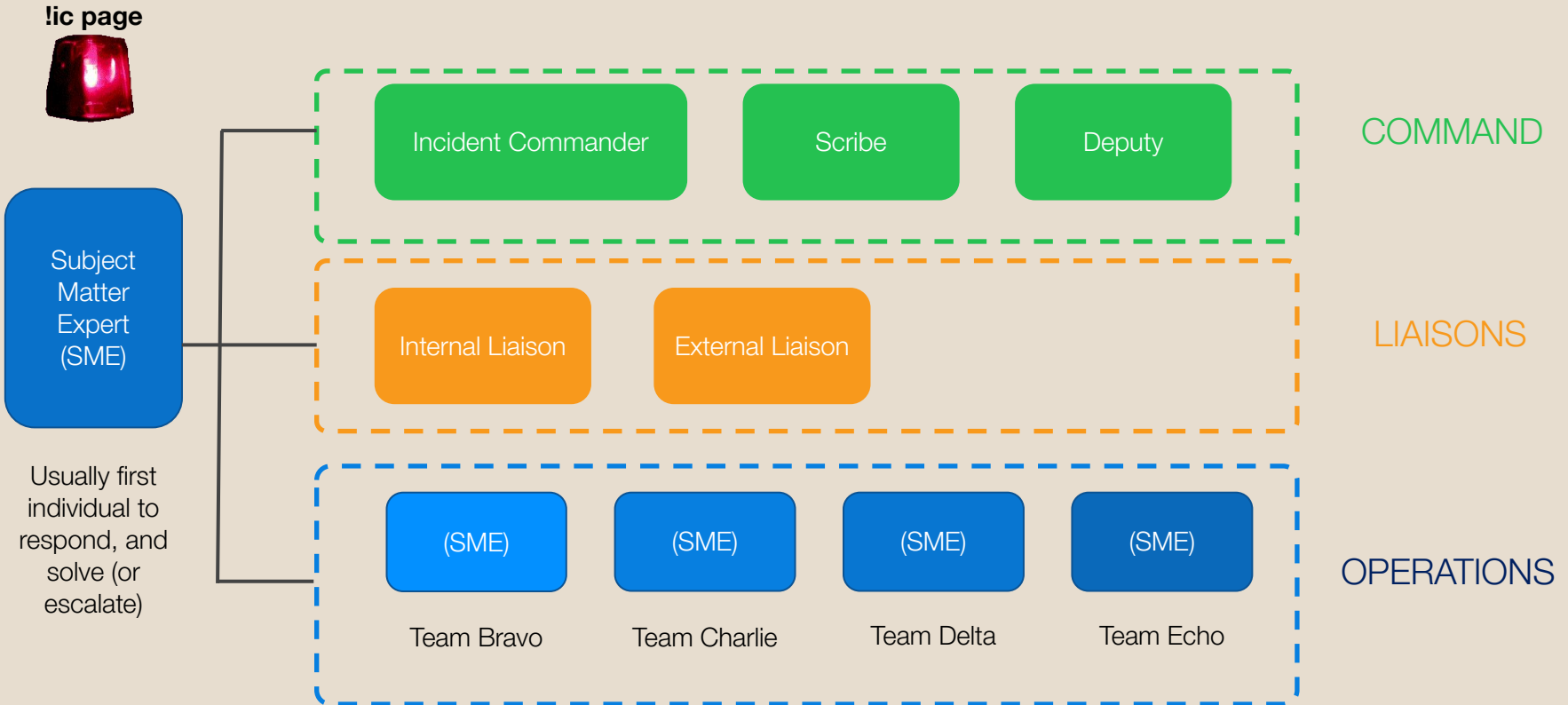


Setting this up at scale

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)

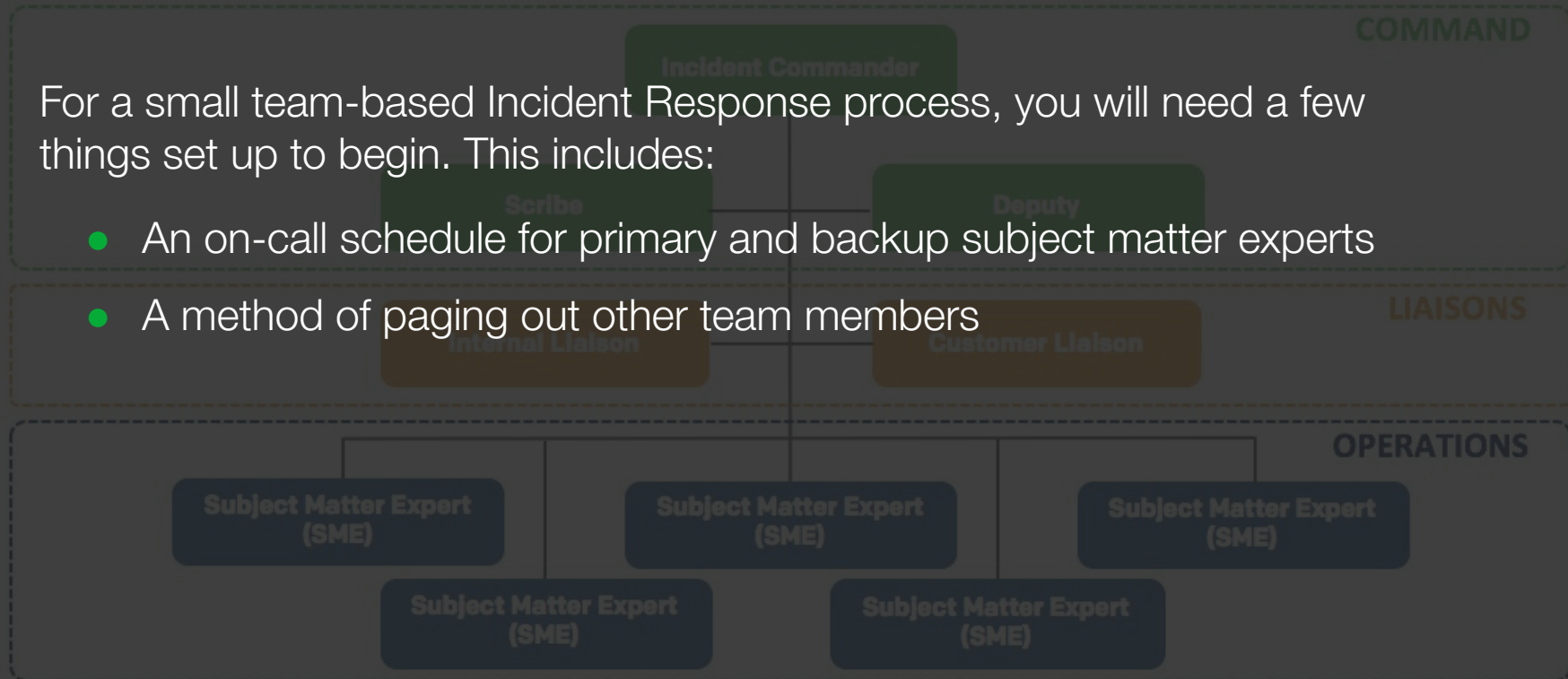
Incident Response - typical sequence of events



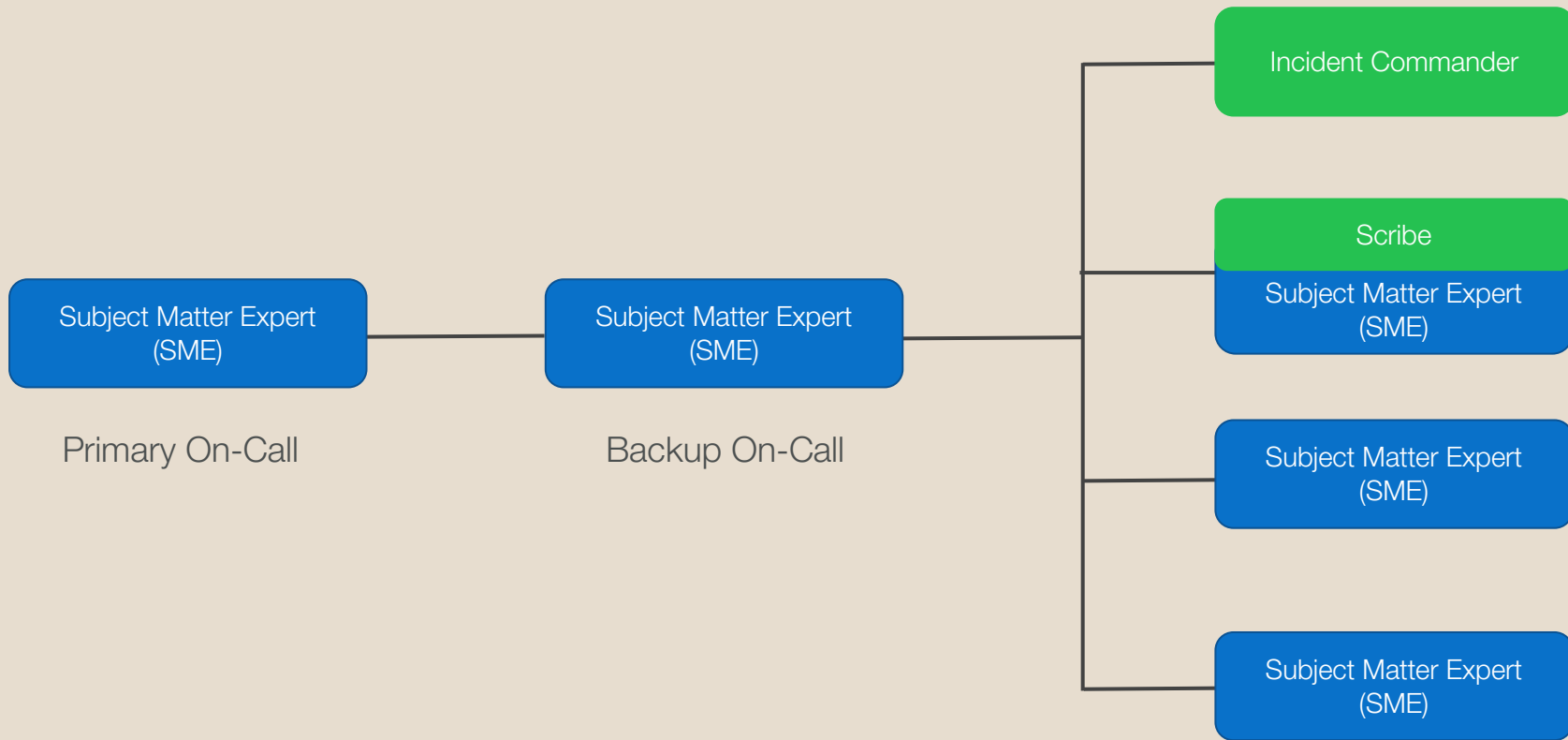
How Do The Roles Scale Down?

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

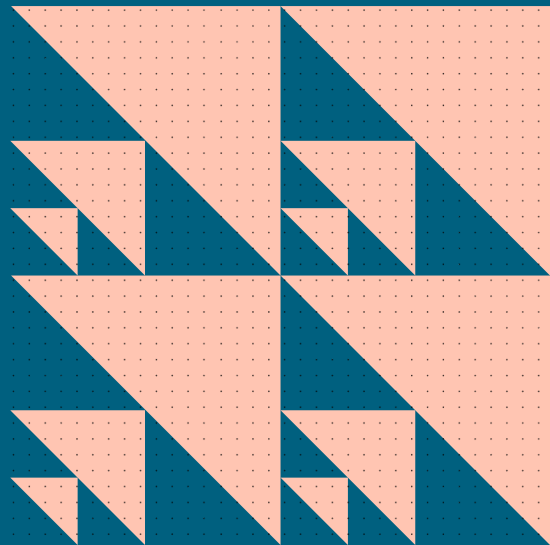
- An on-call schedule for primary and backup subject matter experts
- A method of paging out other team members



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 of panic and fear. The background is dark and blurry, suggesting a confined space. The text 'Replace chaos with calm' is overlaid in the center of the image.

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 open, suggesting a moment of collective action or agreement. The lighting is dramatic, highlighting the silhouettes against a slightly lighter, hazy background.


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



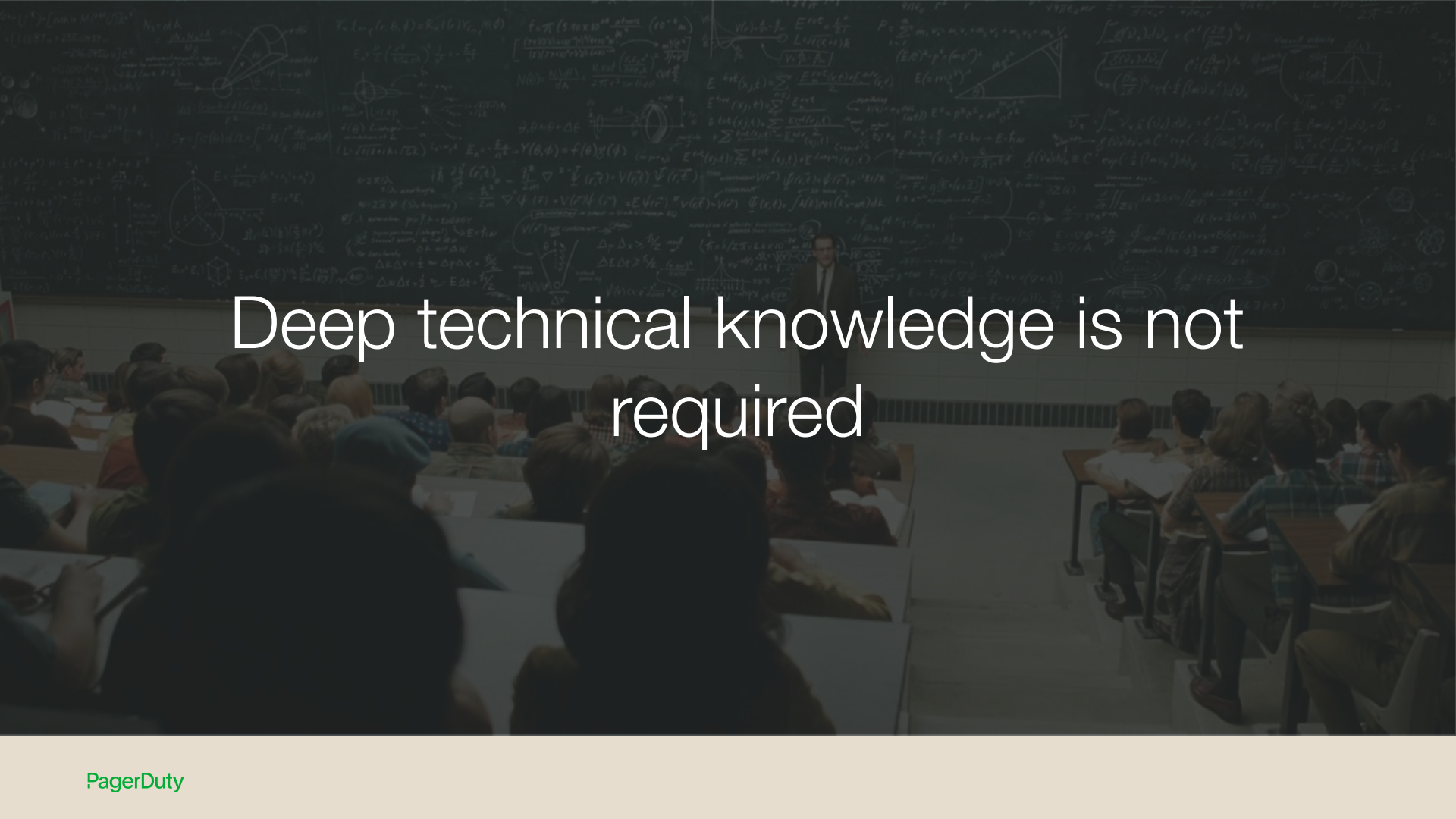
Make a **decision**

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 chess pieces, including a king, queen, rook, and knight, arranged on a chessboard. The pieces are light-colored and have a classic design. The king is the tallest piece, followed by the queen, rook, and knight. The knight is on the far right.

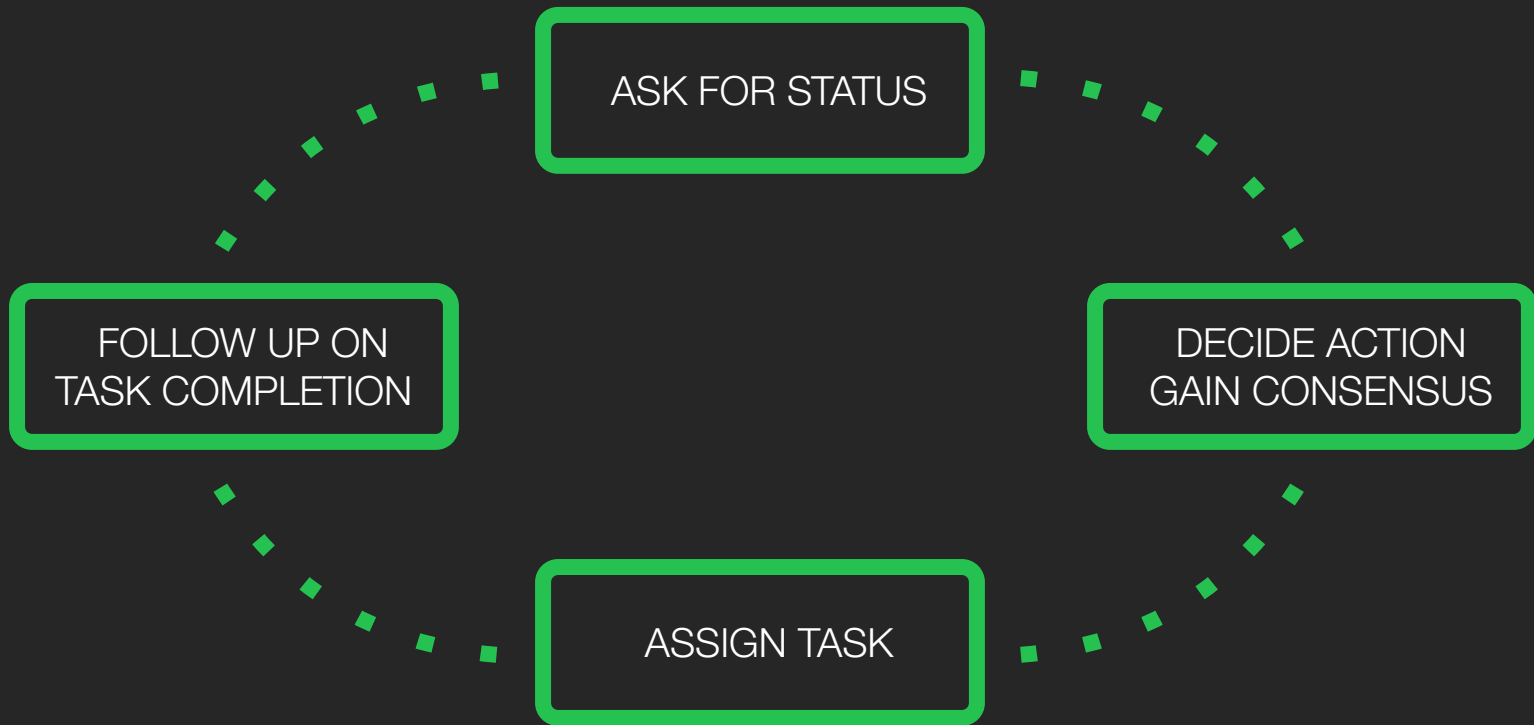
Becomes the highest authority
(Yes, even higher than the CEO)

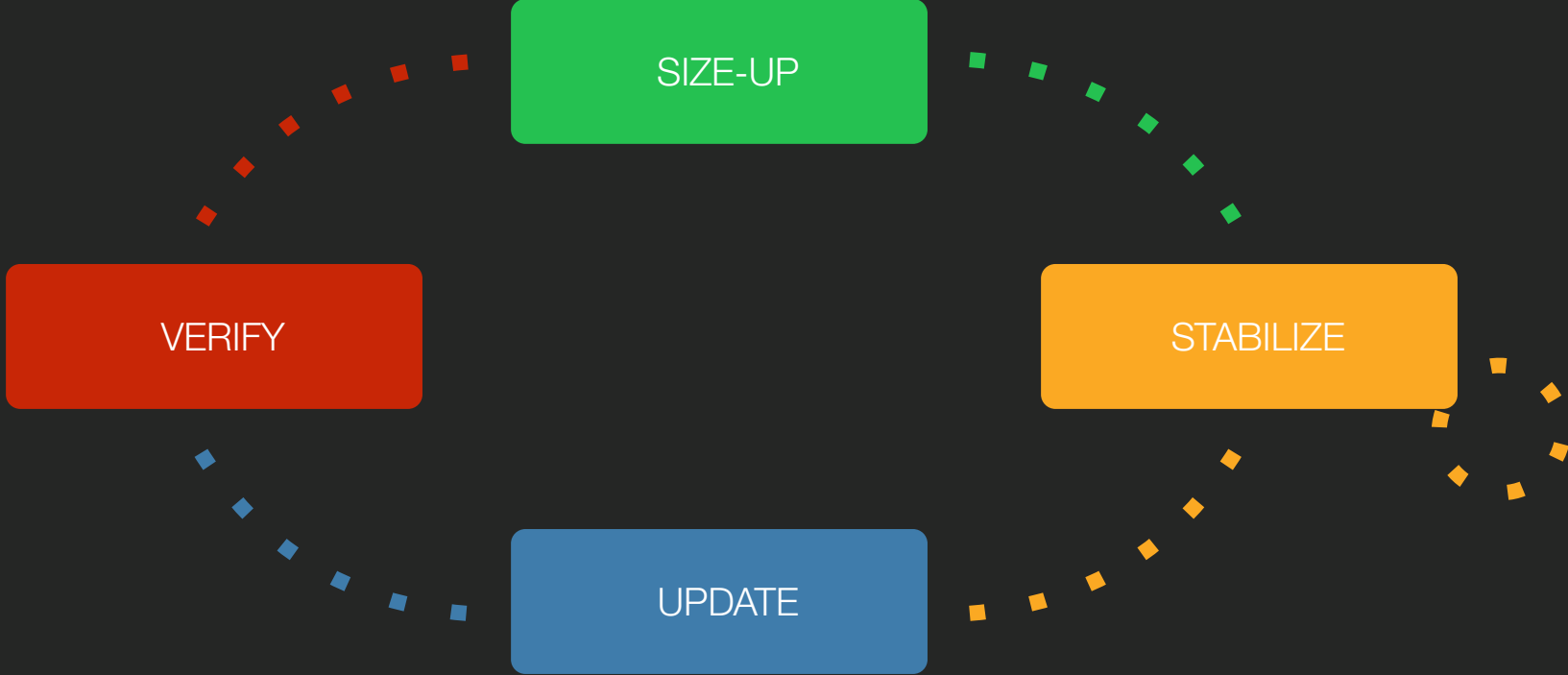


Deep technical knowledge is not
required

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 overall image has a dark, semi-transparent overlay.

Handoffs are encouraged





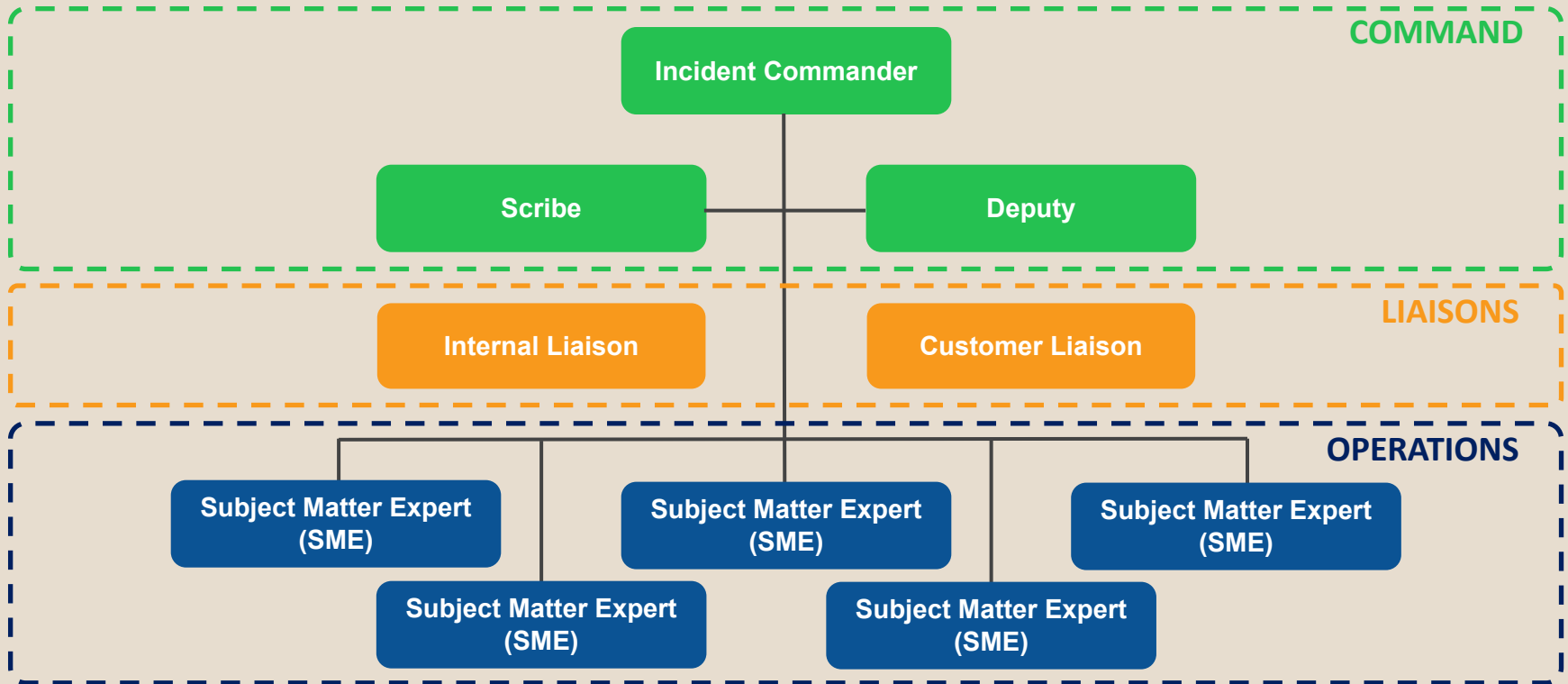
Quick Tips for New Incident Commanders

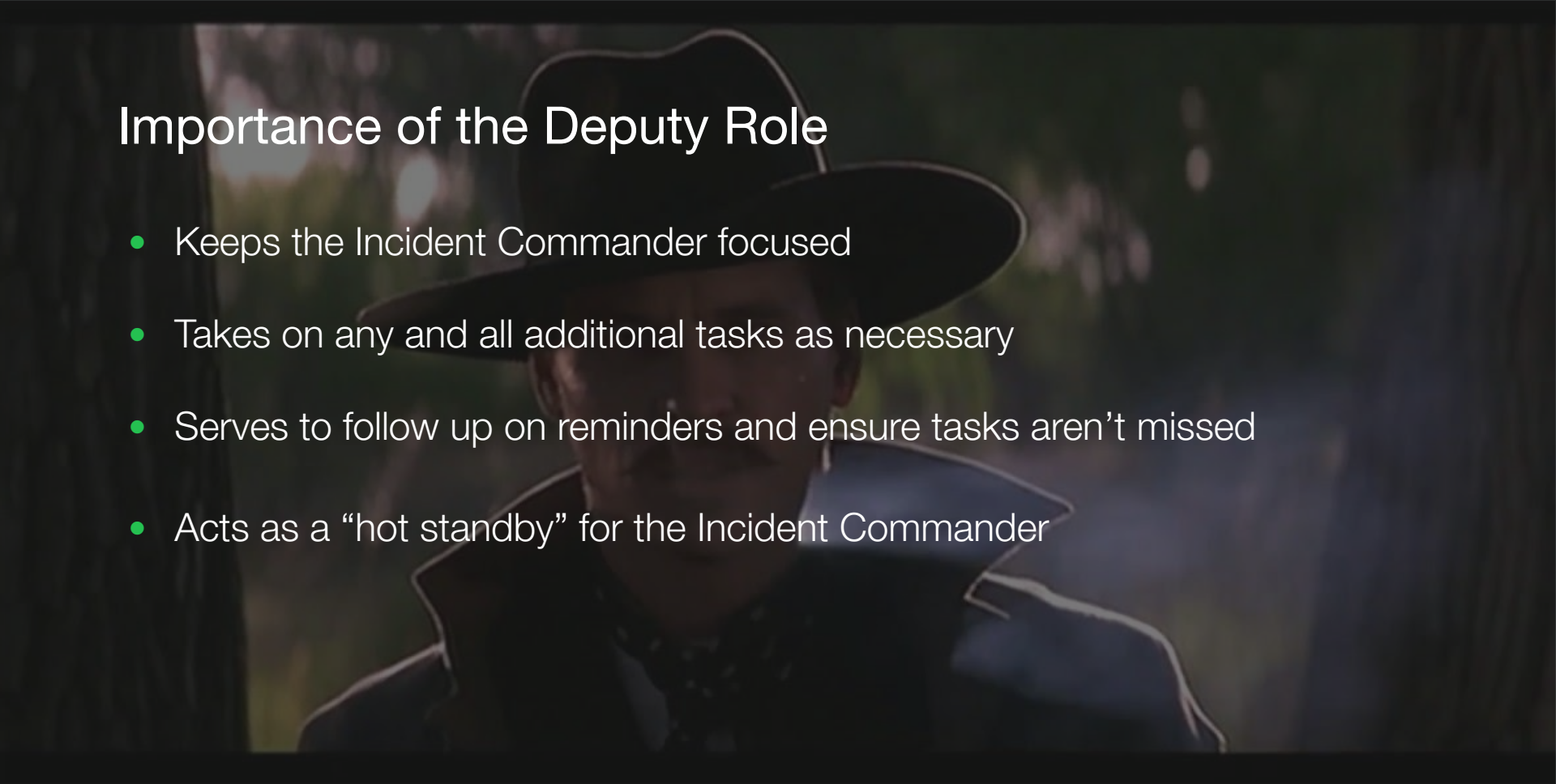
- Introduce yourself on the call with your name and that you are the Incident Commander
- Avoid acronyms
- Speak slowly and with purpose
- On the call, kick people off if they are being disruptive
- Time-box tasks and check in for status updates
- Explicitly declare when the response has ended

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

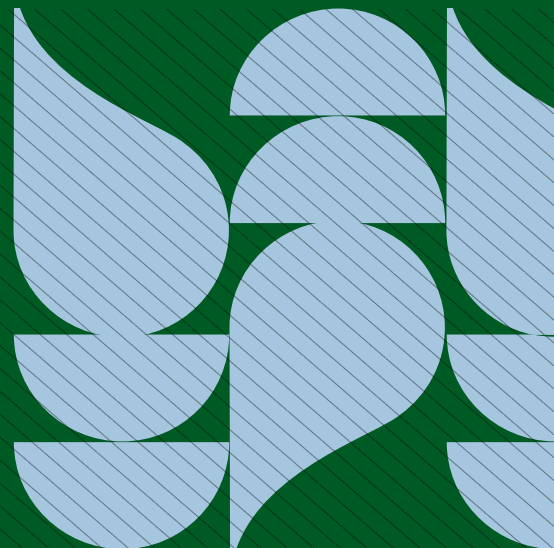
Importance of the Scribe

- 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 pointing his right index finger towards the camera. He has a wide-eyed, surprised, or perhaps indignant expression. He is standing in an office environment, with a wire mesh basket visible in the foreground on the left. The background is slightly blurred, showing office shelves and a door.

Executive Swoop



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



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

A close-up, low-angle shot of a person in a dark suit jacket, white shirt, and patterned tie. The person's hands are visible, adjusting the tie. The lighting is dramatic, with strong highlights and deep shadows, creating a professional and serious atmosphere. The background is dark and out of focus.

“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 visible. 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', 'Z', 'N', and 'M'. A small green wheelbarrow is on the right side of the keyboard. The entire scene is dimly lit, with the keyboard keys clearly visible.

Failure to Notify Stakeholders



Too frequent status updates

A close-up photograph of a baby crying intensely. The baby's eyes are closed, and their mouth is wide open in a scream. Their hands are pressed against their cheeks, a common gesture of distress. The image is dimmed with a dark grey overlay. The text "Red Herrings" is centered over the baby's face in a white, sans-serif font.

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

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 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

A hand is shown writing on a checklist titled "DAILY REPORT SCHEDULE" with a black pen. The checklist has a grid with columns for "TAM", "11AM", and "5P". 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

A red octagonal stop sign with the word "STOP" in white capital letters is mounted on a grey post. The background is a blurred landscape with a road and some greenery under a grey sky.

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

response.pagerduty.com



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

Purpose

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



Keep the incident moving towards resolution.

Being On-Call

Who's On-Call?

Alerting Principles

Before an Incident

What is an Incident?

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.

Severity Levels

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>