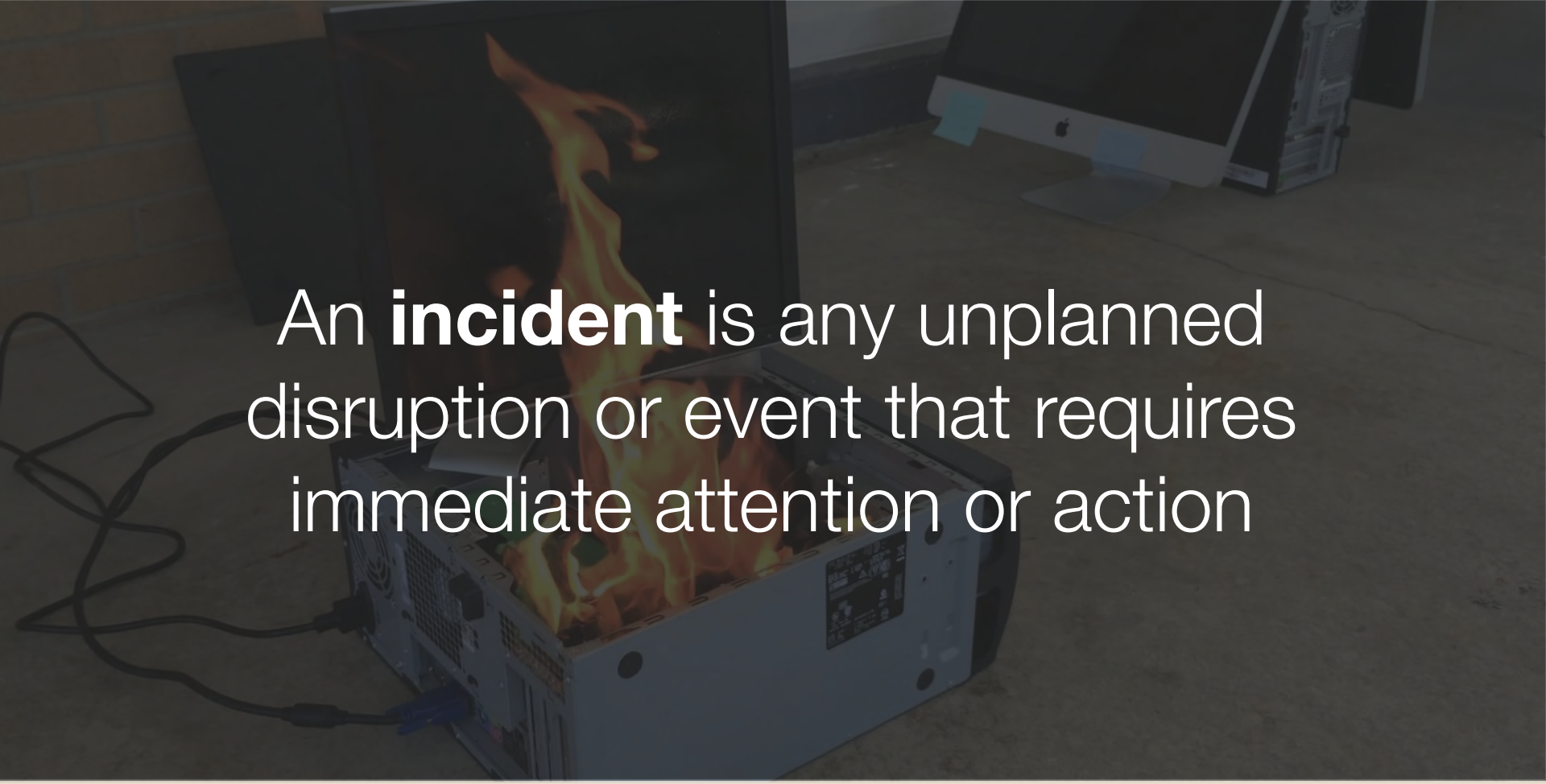
PagerDuty

Don’t Panic!

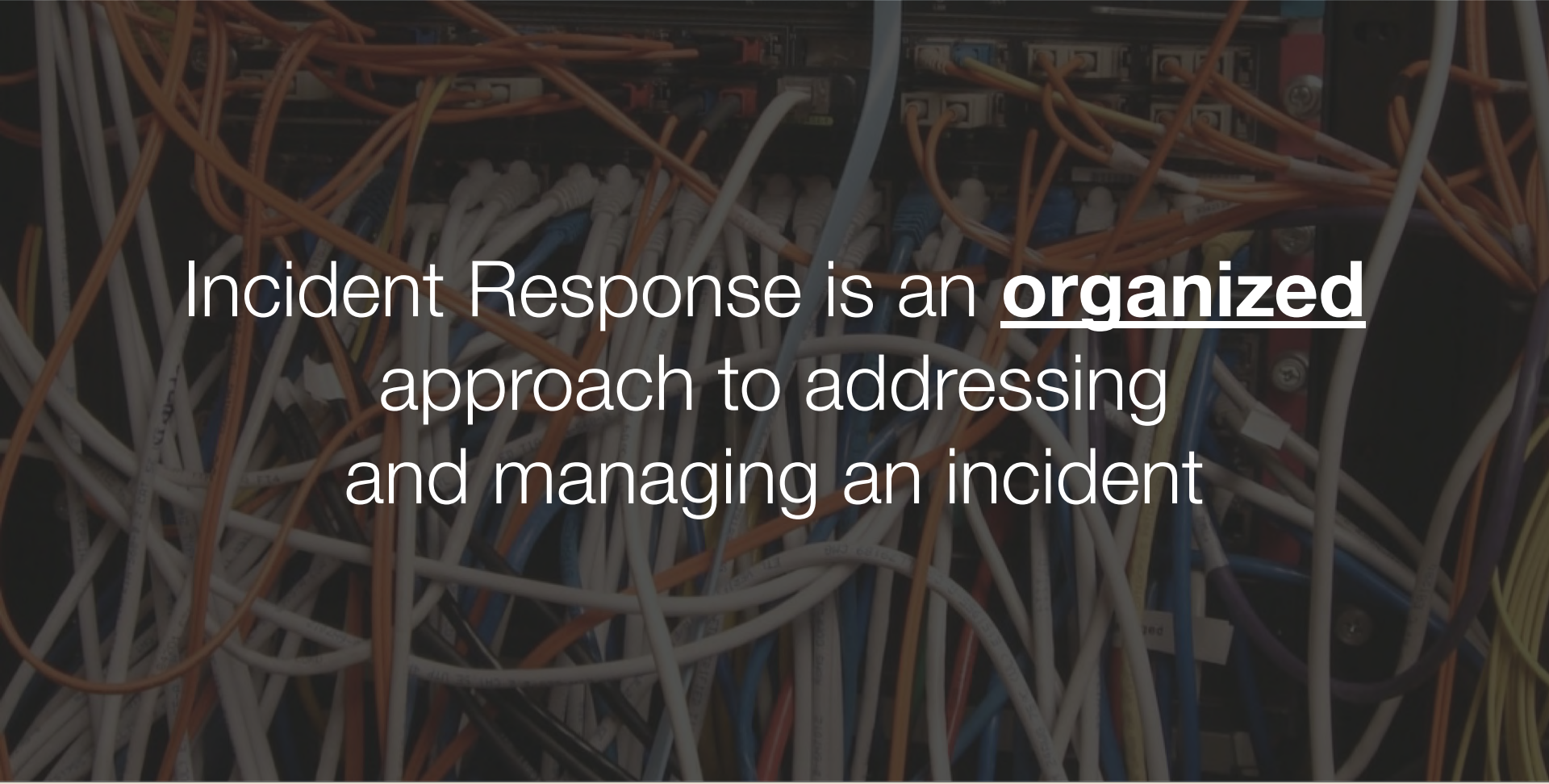
Effective Incident Response

Presented by
@QuintessenceAnx
DevOps Advocate

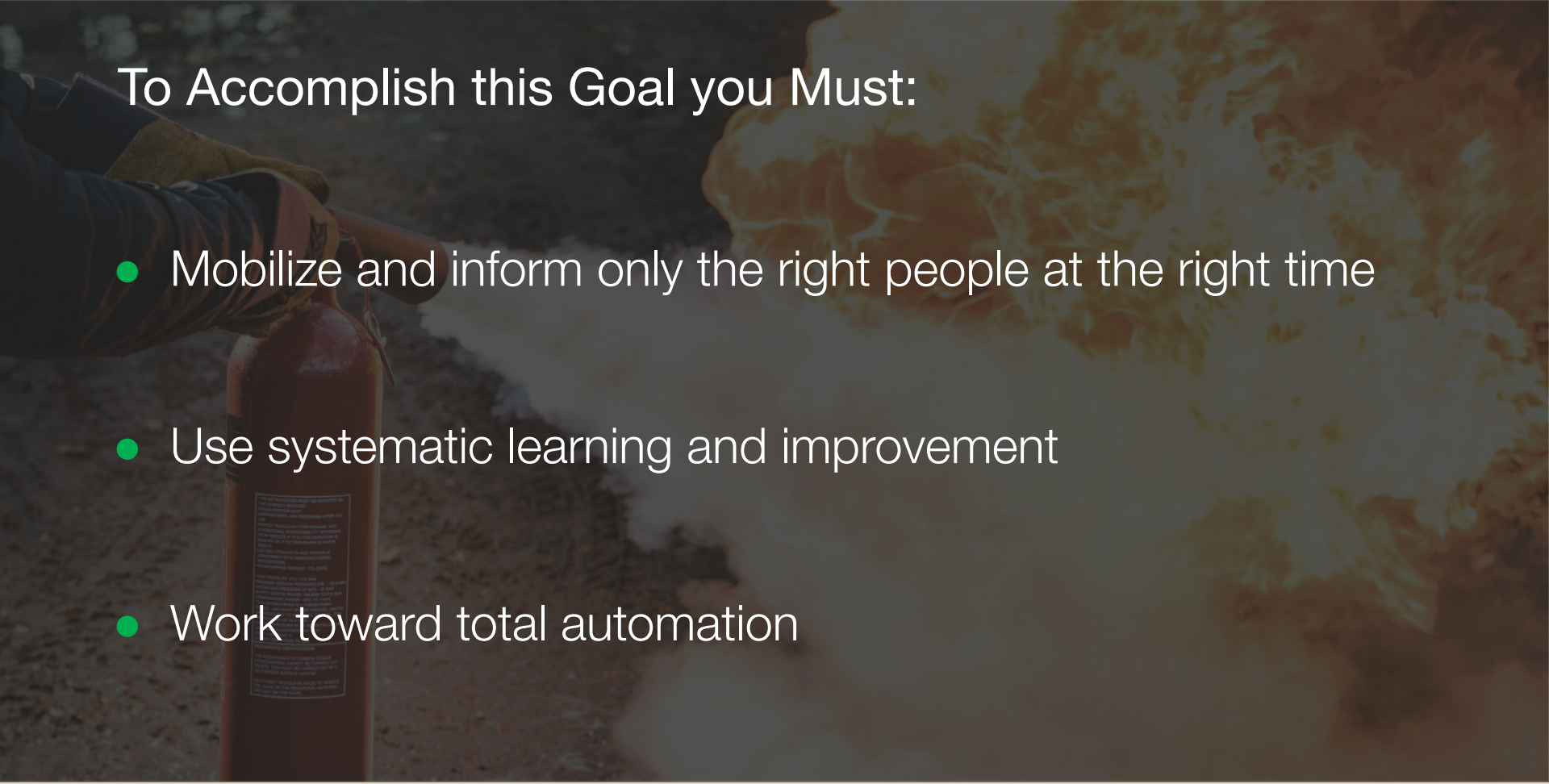
2021


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


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

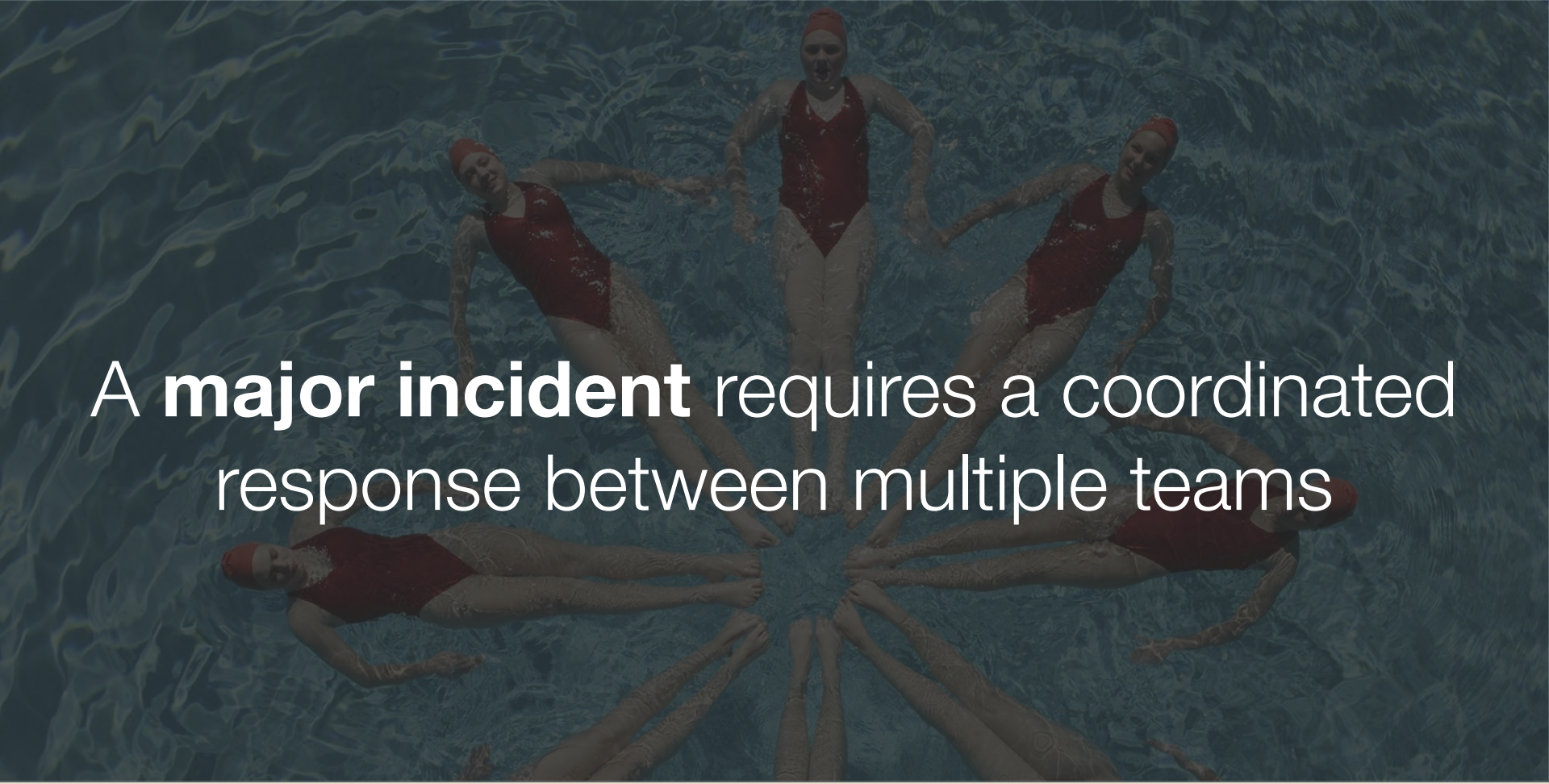


To Accomplish this Goal you Must:

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

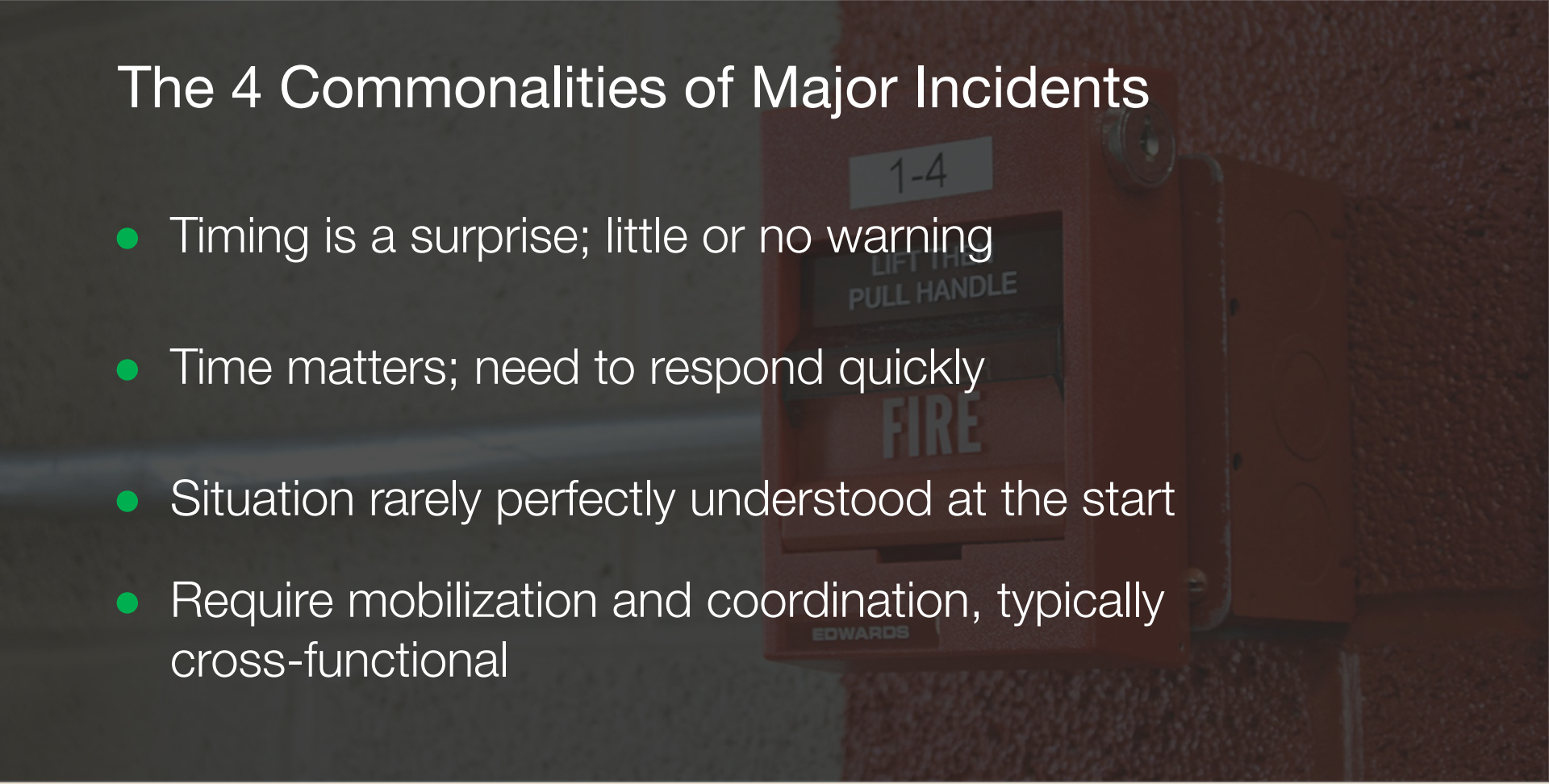
Based on the Incident Command System, originally developed for California wildfire response.


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

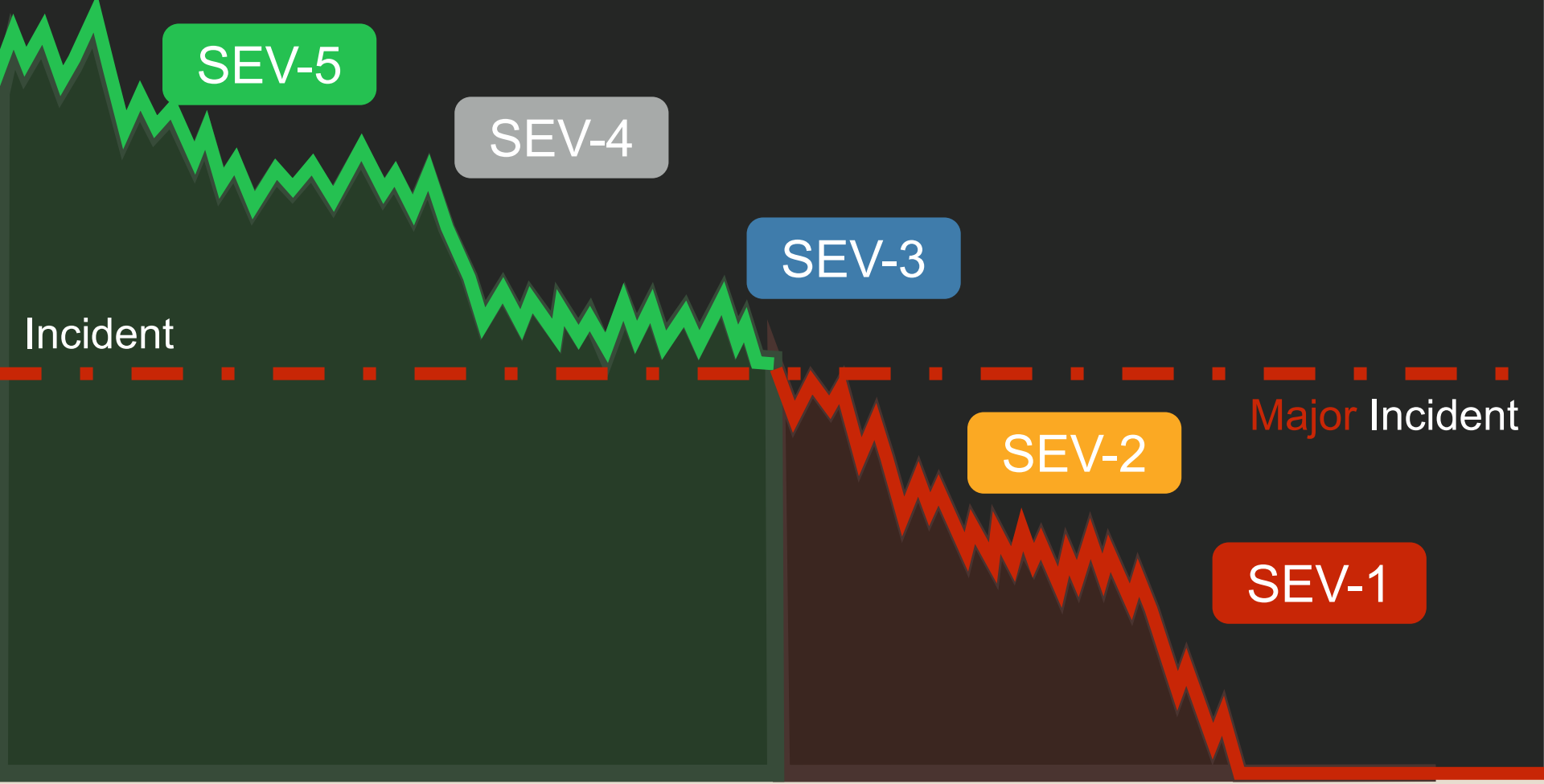


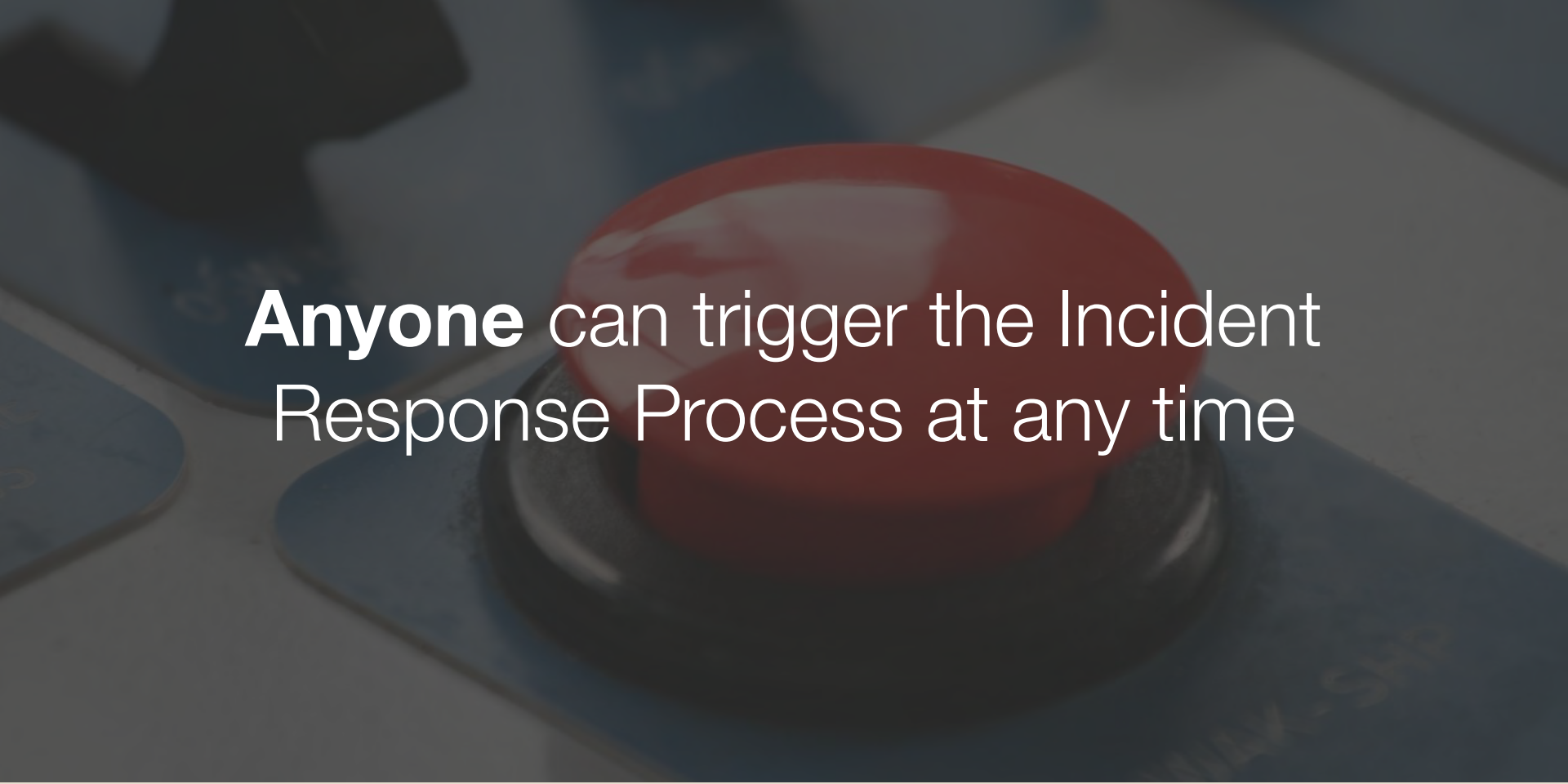
A **major incident** requires a coordinated response between multiple teams

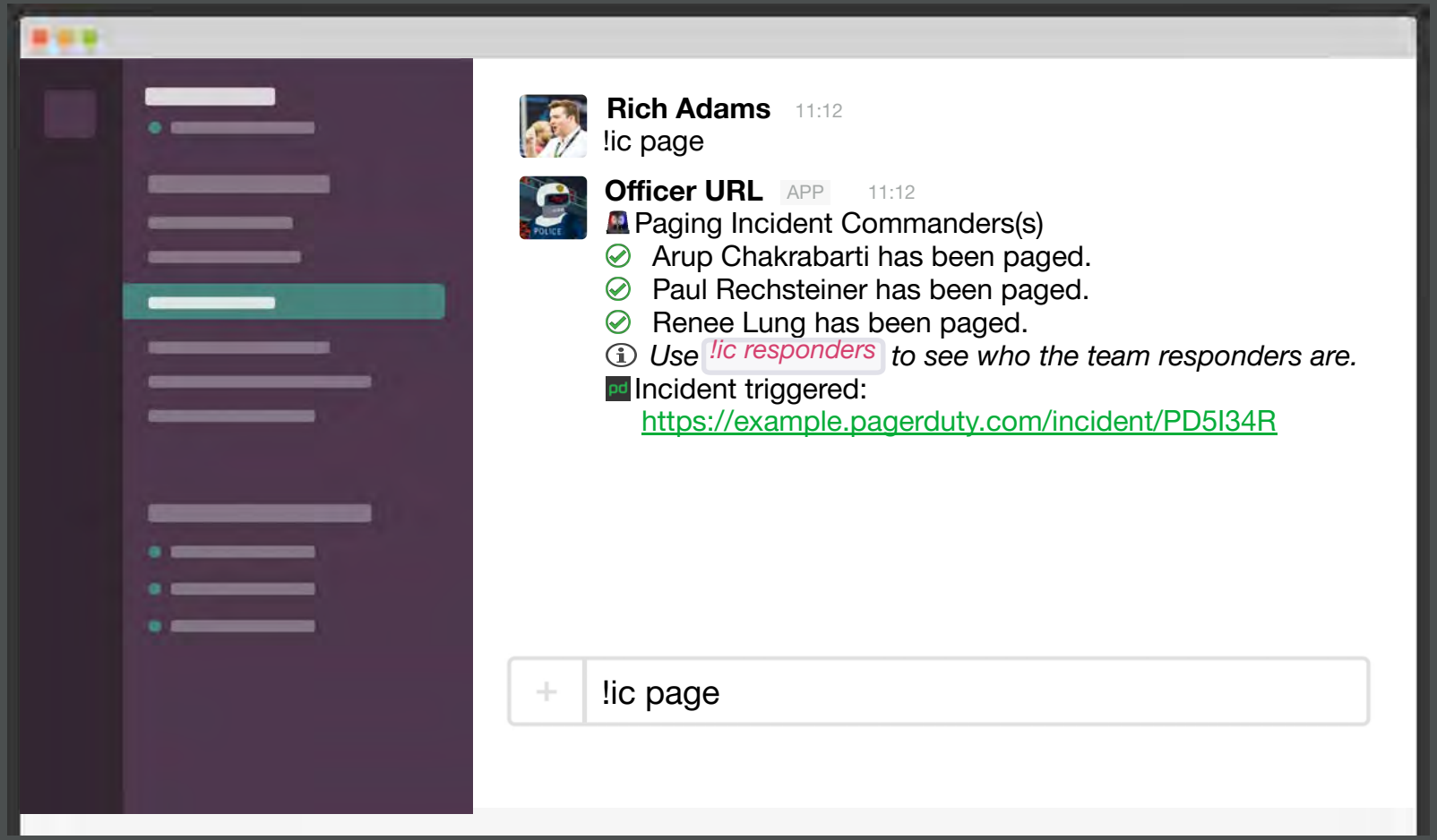
The 4 Commonalities of Major Incidents



- 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


SEV-5
SEV-4
SEV-3
Incident
Major Incident
SEV-2
SEV-1


Anyone can trigger the Incident Response Process at any time


Rich Adams 11:12
!ic 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 !ic responders to see who the team responders are.
Incident triggered:
https://example.pagerduty.com/incident/PD5I34R
!ic page

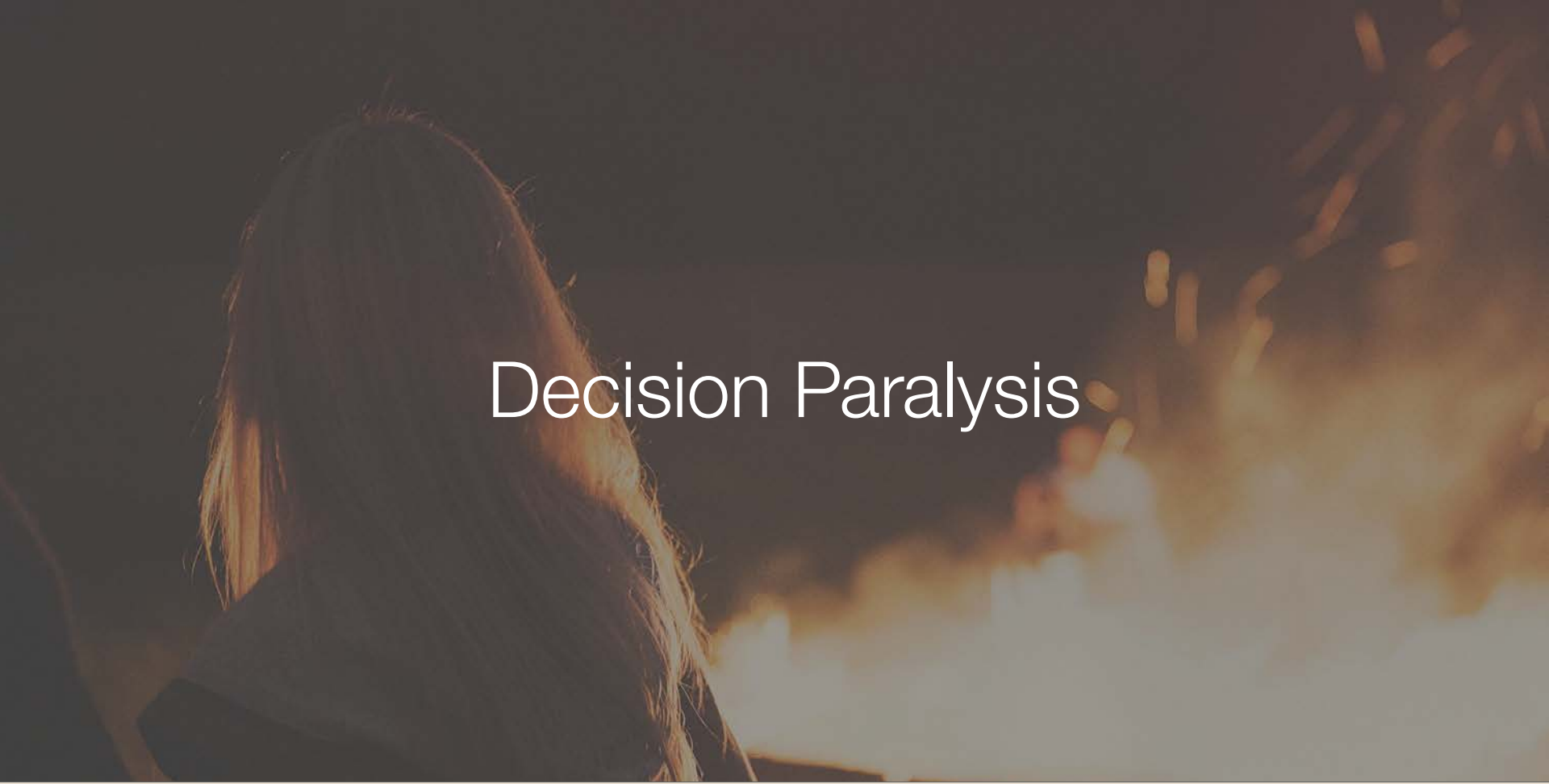

PEACETIME
WARTIME
Revenue YTD VS PY / Budget
3,701,962
Expense YTD VS PY / Budget
1,631,300
Yearly Expense Trends
Gross Profit YTD VS PY / Budget
2,684,545
Revenue Vs Expense
ws has been shut down to prevent damage
this Stop error screen,
appaears again, follow
software is properly installed.
hardware or software manufacturer
ve any newly installed harware
ons such as caching or shadowing.
or disable components, restart
anced Startup Options, and then
000001,
Q1CCC7,0x0000000)
base at
00, Datestamp 4d5dd88c
technical suppor

PagerDuty

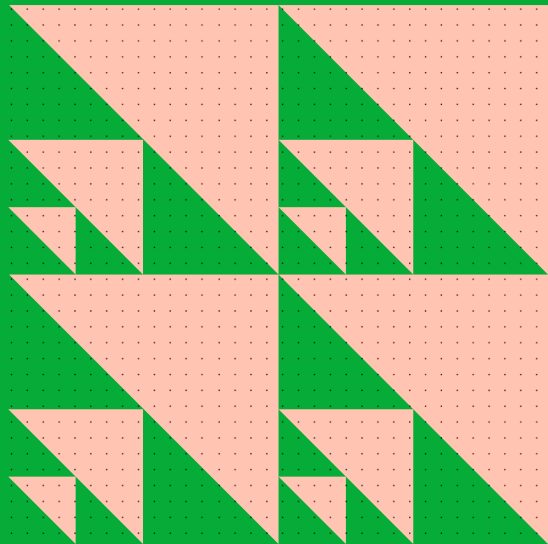

NORMAL
EMERGENCY
Revenue YTD VS PY / Budget
3,701,962
Expense YTD VS PY / Budget
1,631,300
Yearly Expense Trends
Gross Profit YTD VS PY / Budget
2,684,545
Revenue Vs Expense
ws has been shut down to prevent damage
this Stop error screen,
appaears again, follow
software is properly installed.
ur hardware or software manufacturer
d.
ve any newly installed harware
ons such as caching or shadowing.
e or disable components, restart
anced Startup Options, and then
000001,
Q1CCC7,0x0000000)
base at
00, Datestamp 4d5dd88c
technical suppor
PagerDuty


OK
NOT OK
Revenue YTD VS PY / Budget
3,701,962
Expense YTD VS PY / Budget
1,631,300
Yearly Expense Trends
Gross Profit YTD VS PY / Budget
2,684,545
Revenue Vs Expense
Jan 326,997
Feb 130,883 7725
Mar 357,264 170,153
Apr 388,719 256,645
May 384,355 129,765
Jun 410,499 214,897
Jul 205,128 -10,924
Aug 652,522 241,728
Sep 70,472 44,232
Oct 37,829 21,107
Nov 492,928 256,177
Dec 244,368 69,209
ws has been shut down to prevent damage
this Stop error screen,
appaears again, follow
r software is properly installed.
ur hardware or software manufacturer
d.
ve any newly installed harware
ons such as caching or shadowing.
e or disable components, restart
anced Startup Options, and then
000001,(Q1CCC7,0x0000000)
base at 5 00, Datestamp 4d5dd88c
technical suppor the

PagerDuty

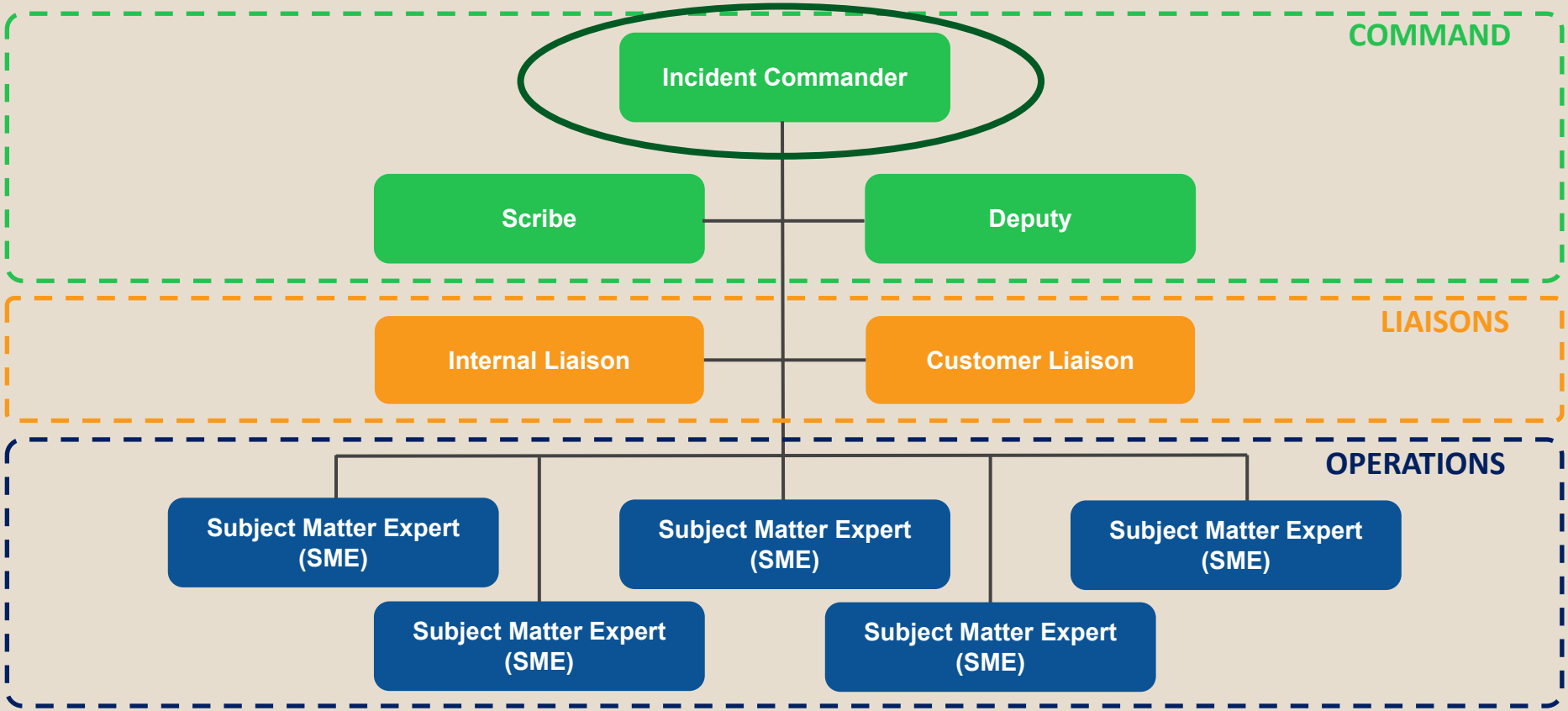

Decision Paralysis

People Roles & Incident Categorization



The Four Steps of an Incident

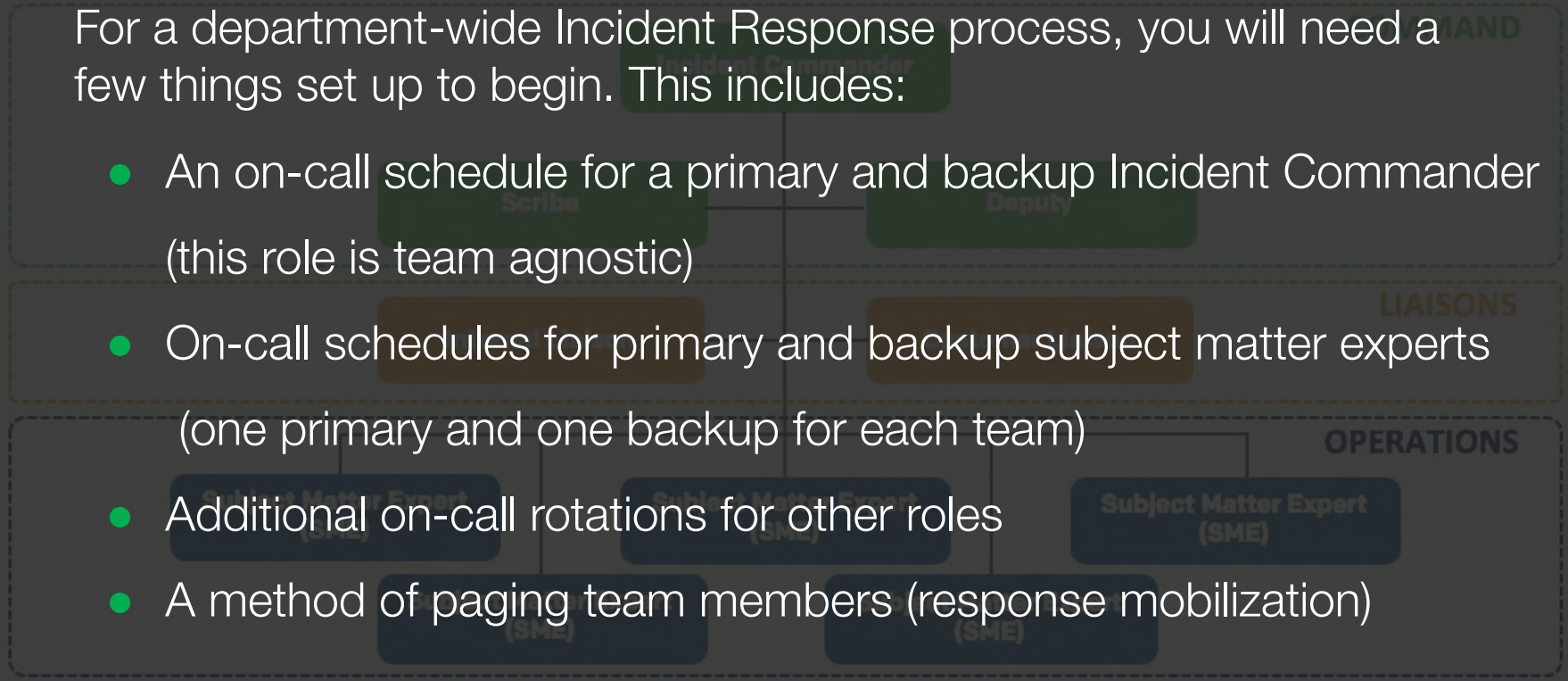
Roles of Incident Response



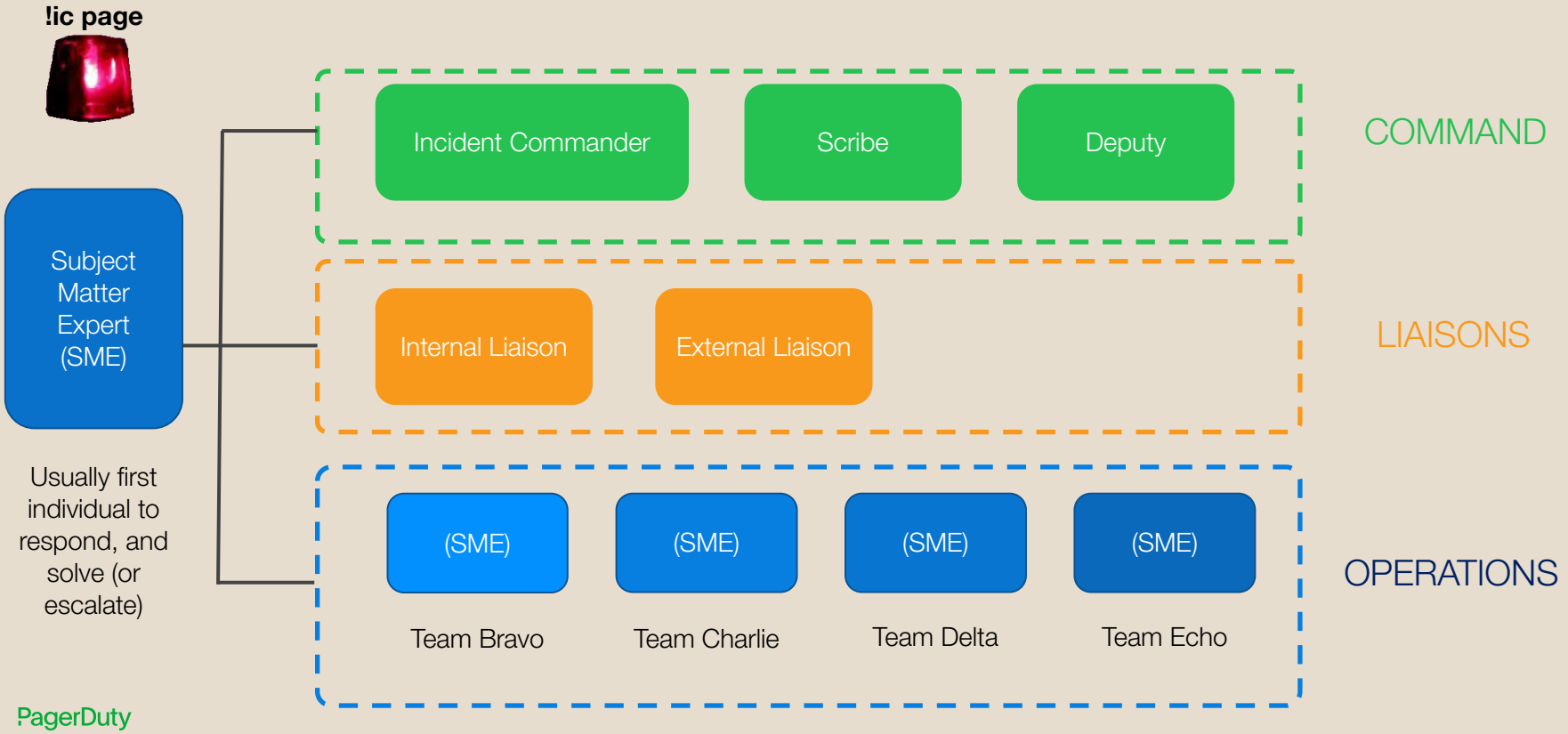
Setting this up at scale

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)



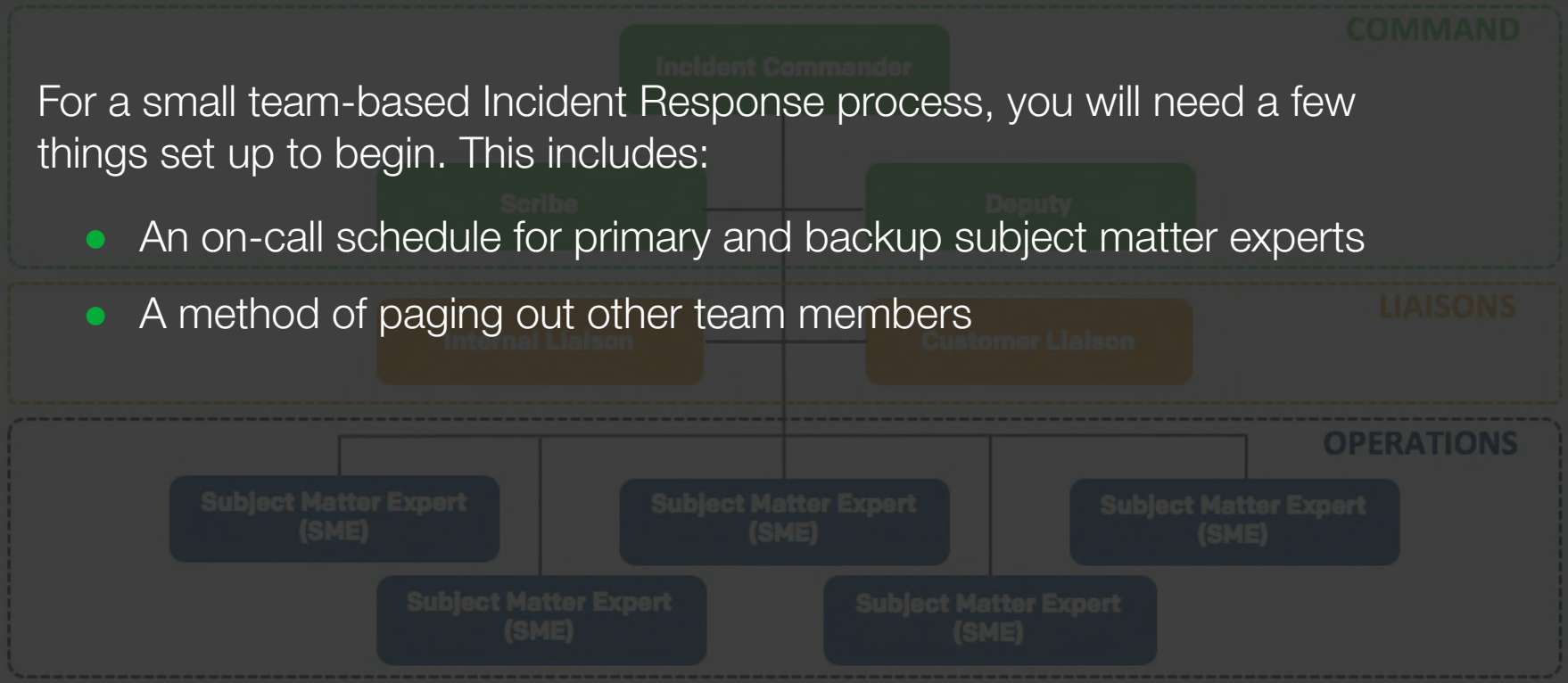
Incident Response - **typical sequence of events**



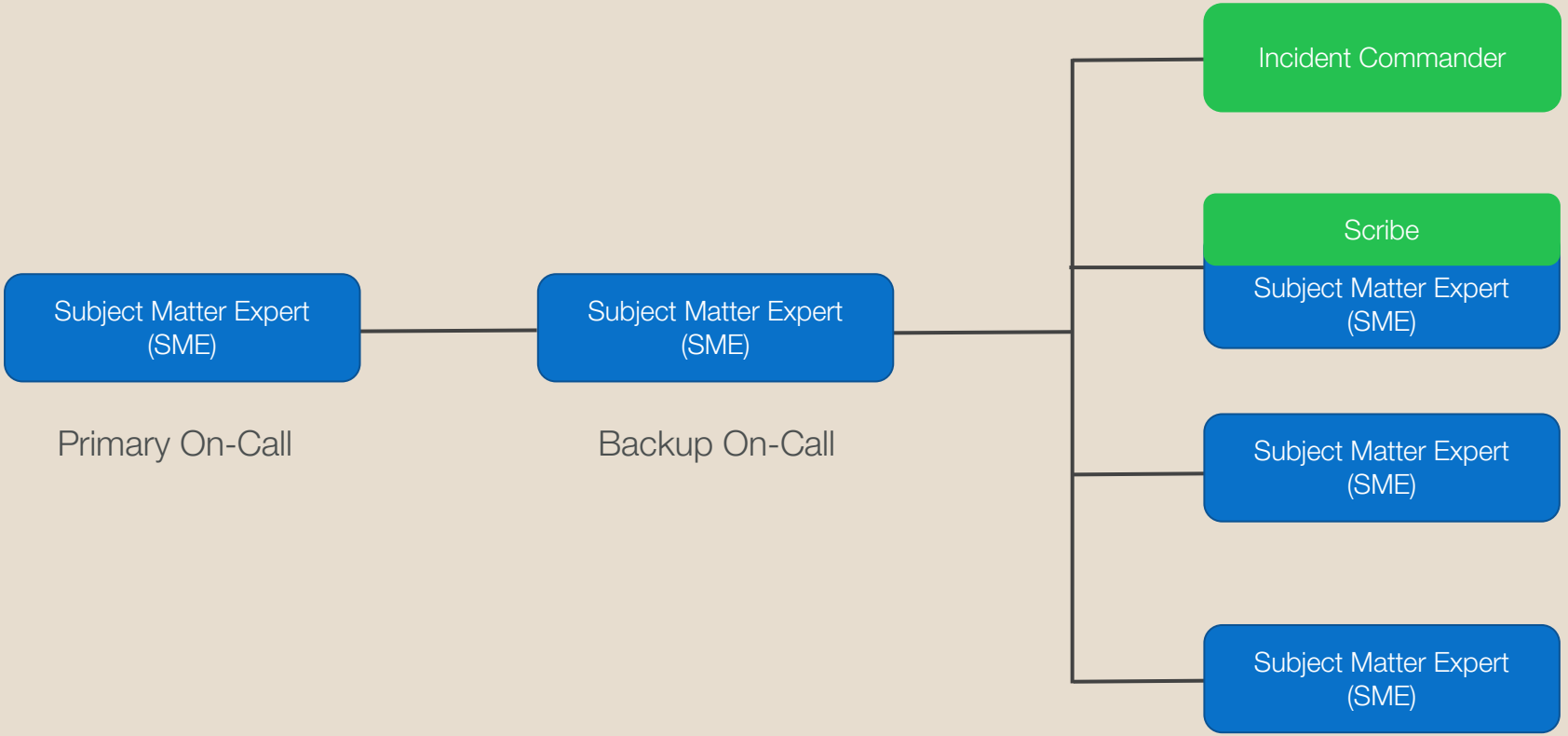
How Do The Roles Scale Down?

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

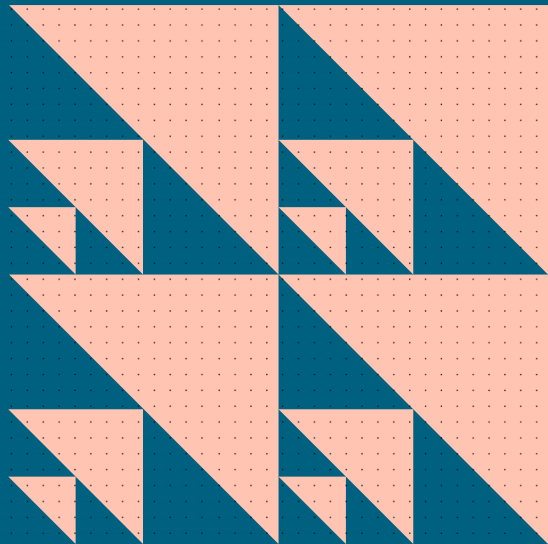
- An on-call schedule for primary and backup subject matter experts
- A method of paging out other team members



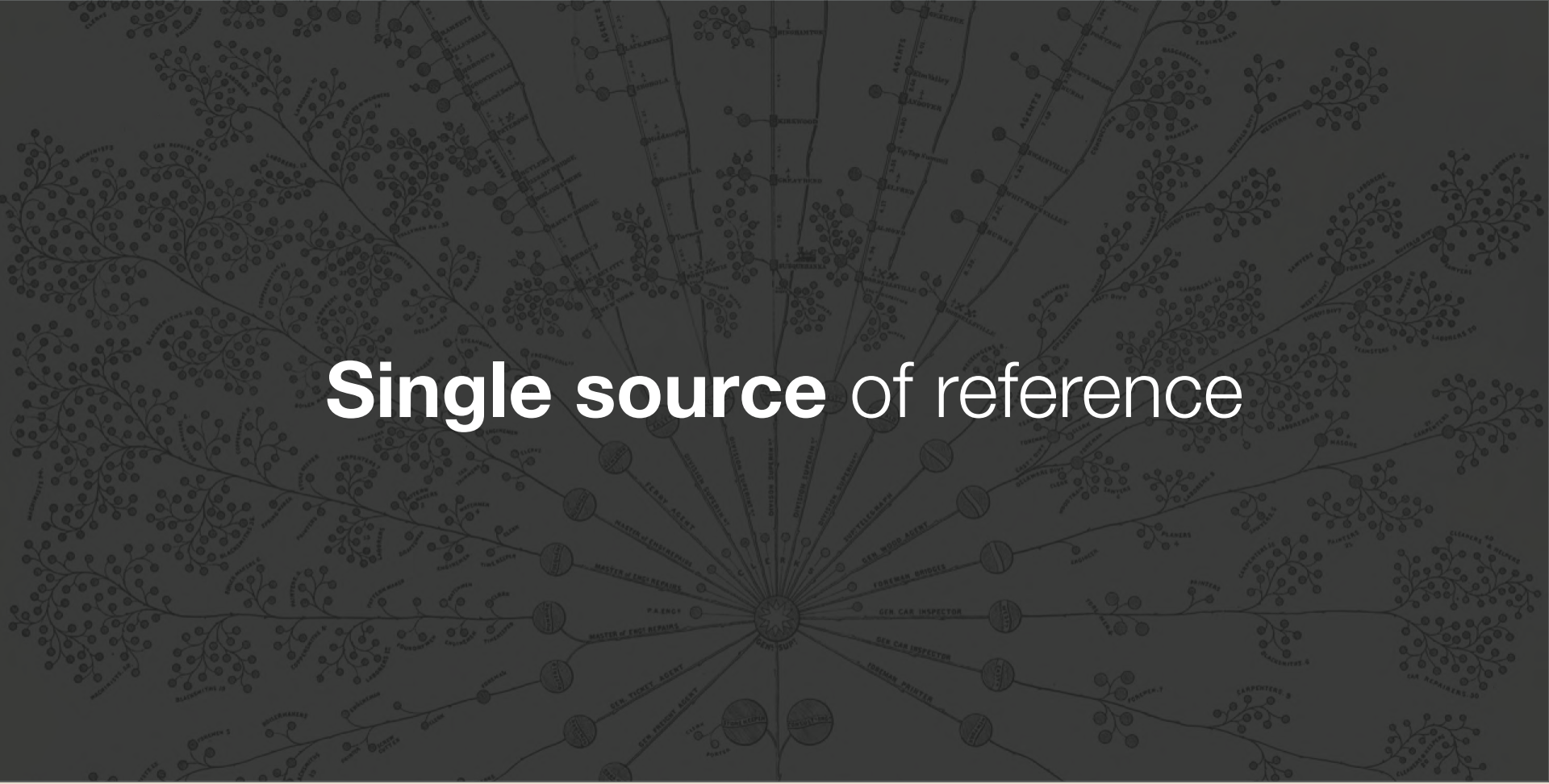
Small Team Incident Response



Incident Commander: Role and Responsibilities

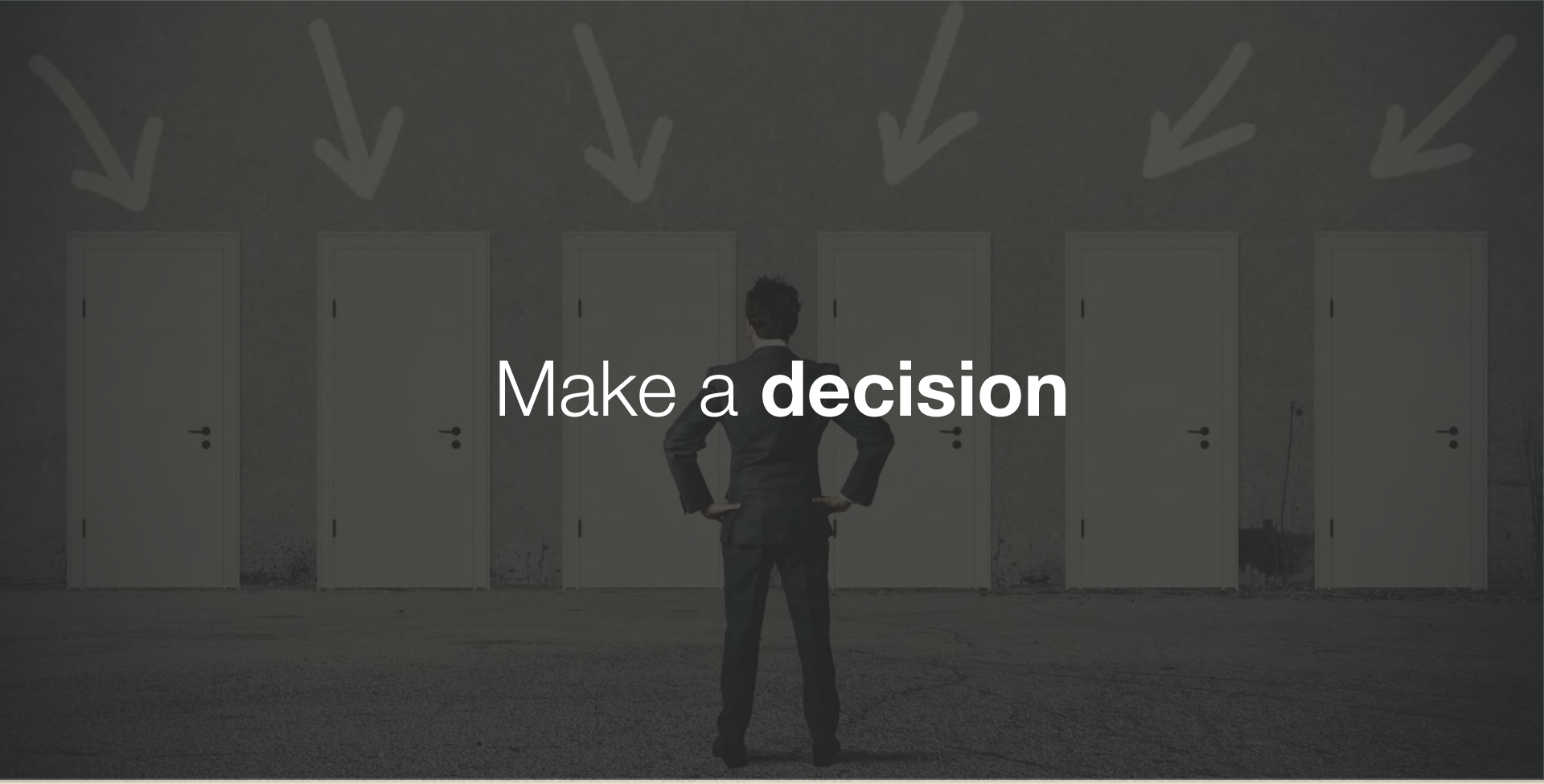


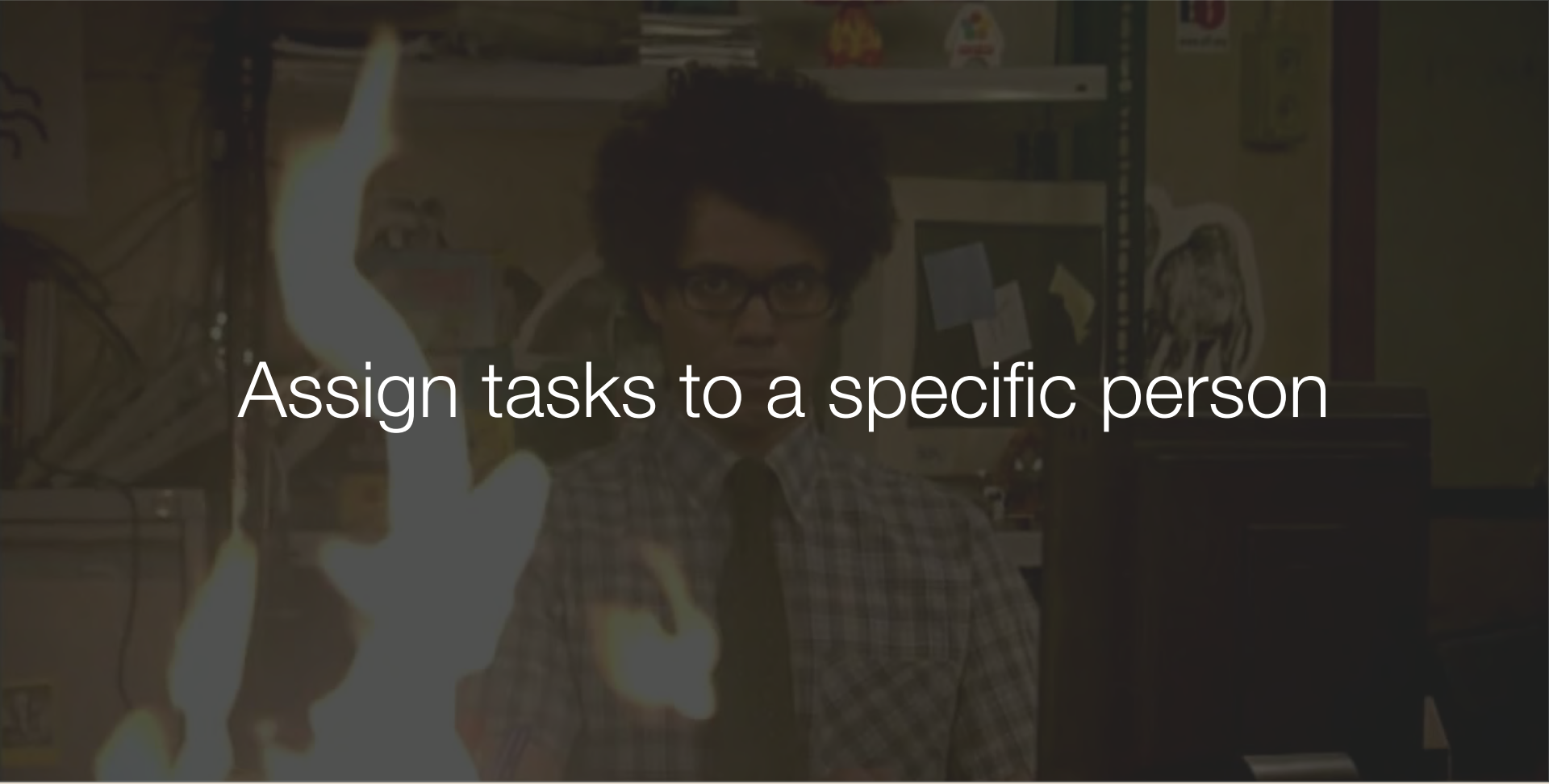

Replace chaos with calm



Single source of reference

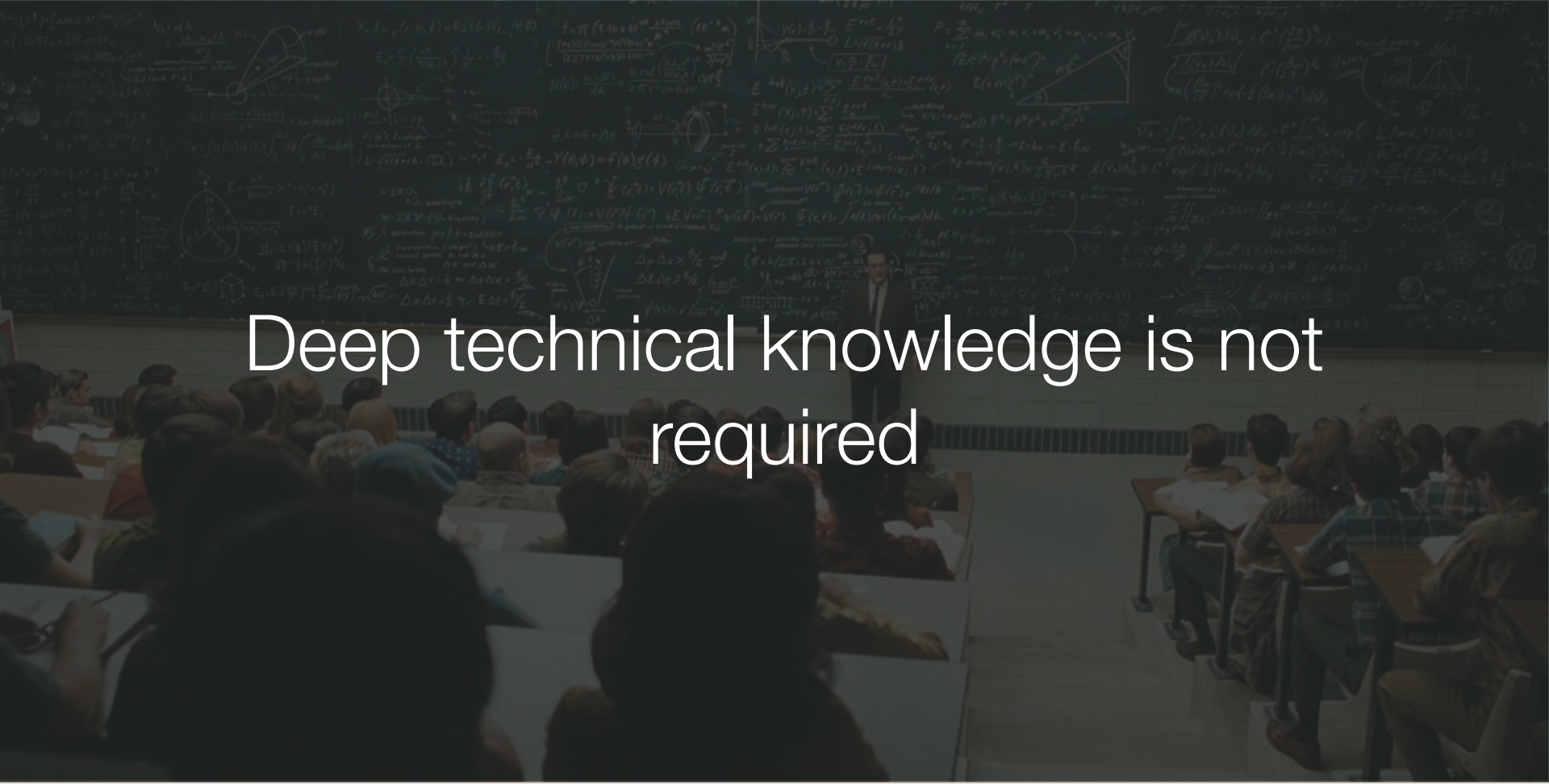

Gain **consensus**
“Are there any **strong** objections”


Make a **decision**

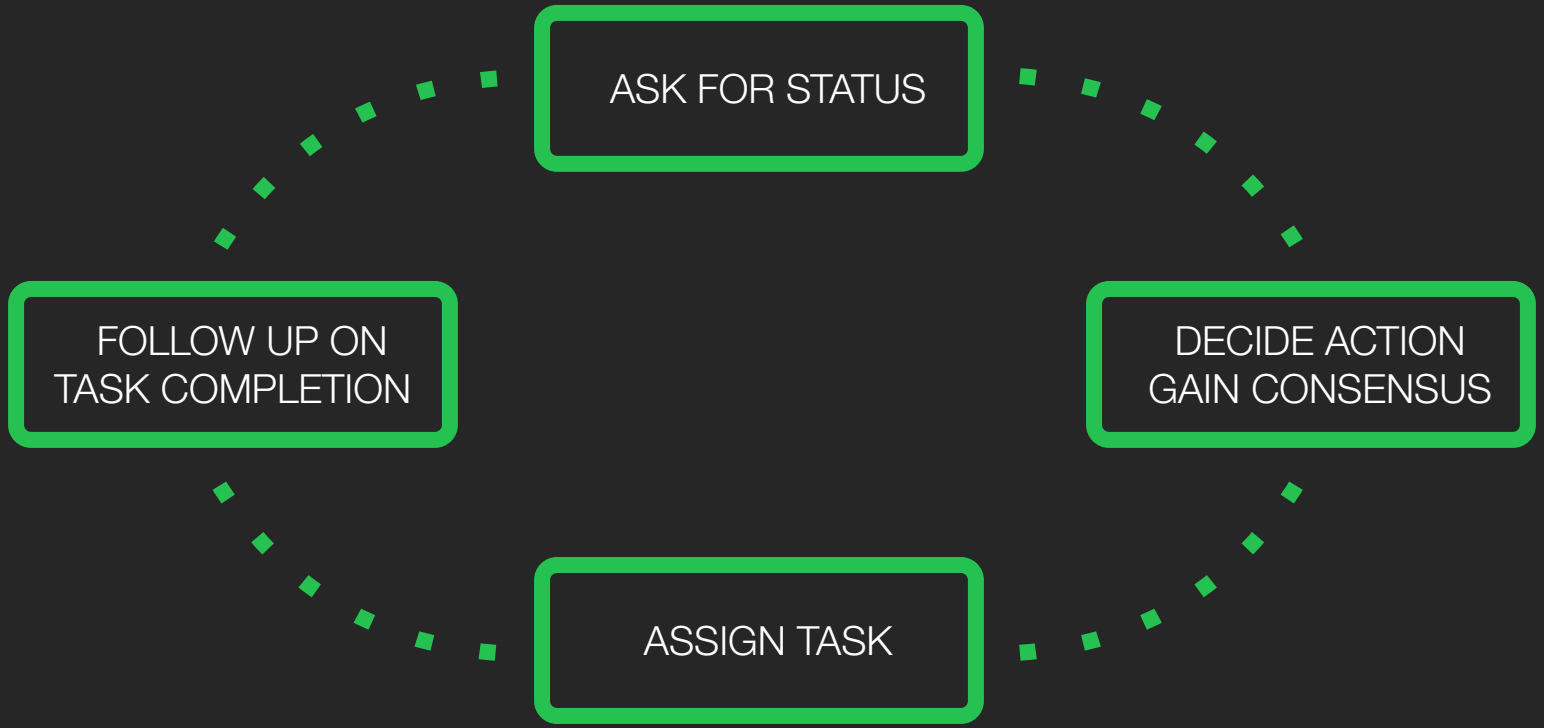

Assign tasks to a specific person

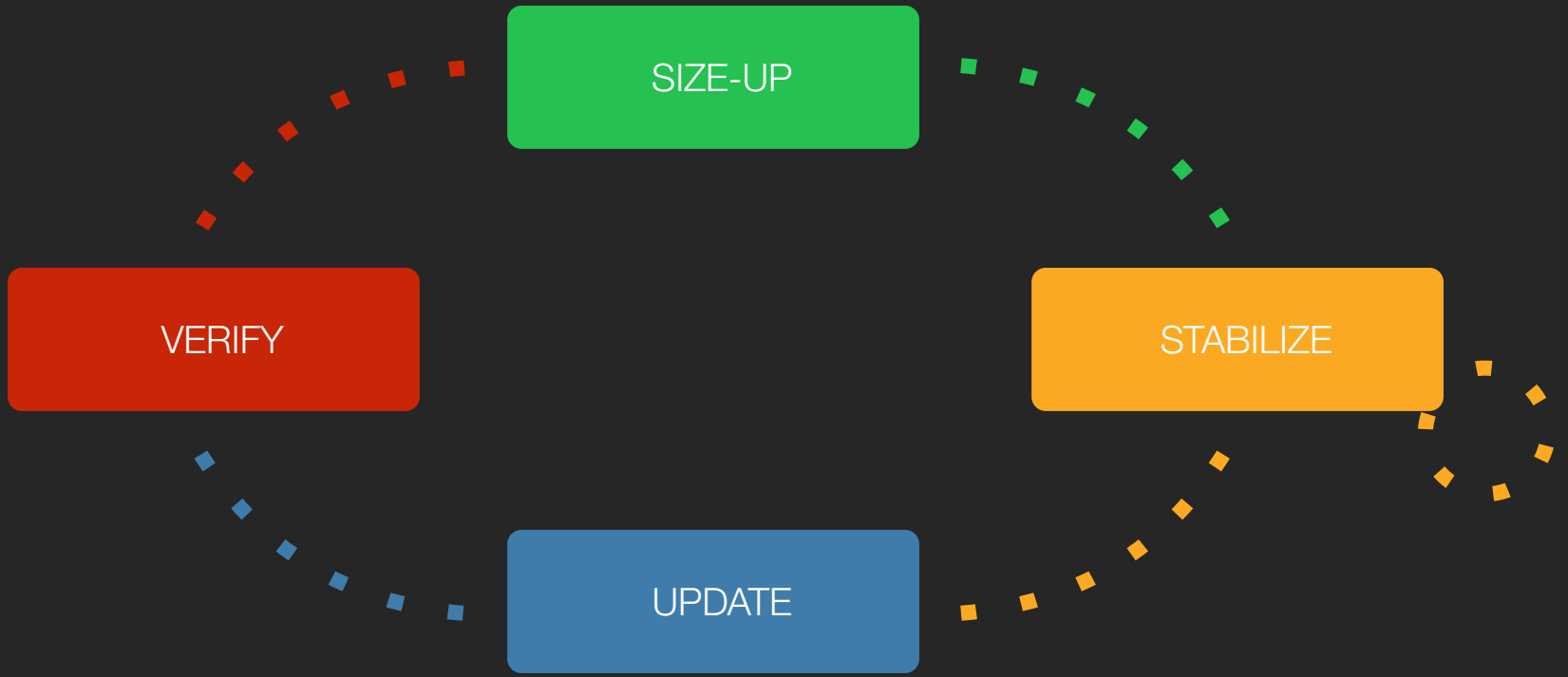
Becomes the highest authority

(Yes, even higher than the CEO)


Deep technical knowledge is not required

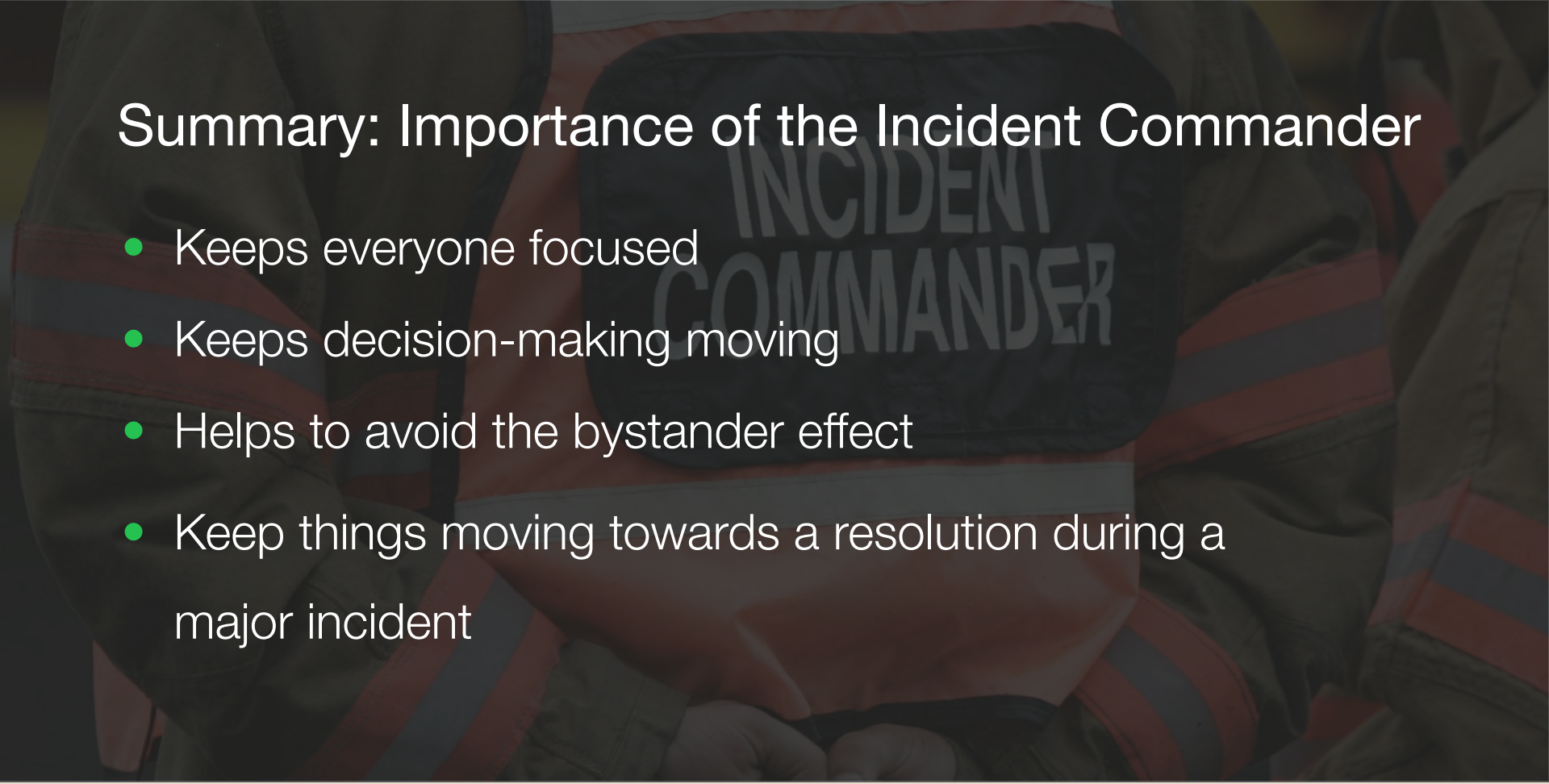

Handoffs are encouraged


ASK FOR STATUS
DECIDE ACTION
GAIN CONSENSUS
ASSIGN TASK
FOLLOW UP ON
TASK COMPLETION


SIZE-UP
STABILIZE
UPDATE
VERIFY

Quick Tips for New Incident Commanders

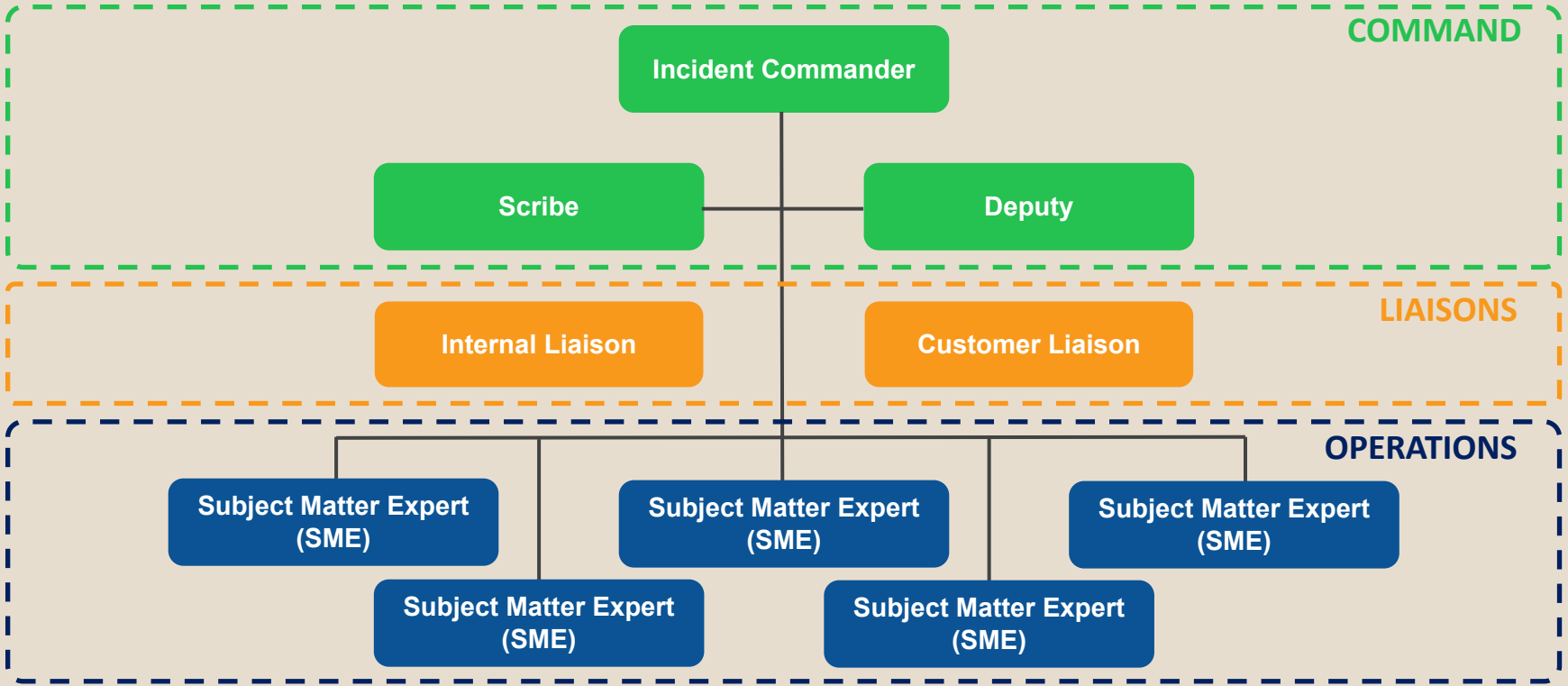
- Introduce yourself on the call with your name and that you are the Incident Commander
- Avoid acronyms
- Speak slowly and with purpose
- On the call, kick people off if they are being disruptive
- Time-box tasks and check in for status updates
- Explicitly declare when the response has ended

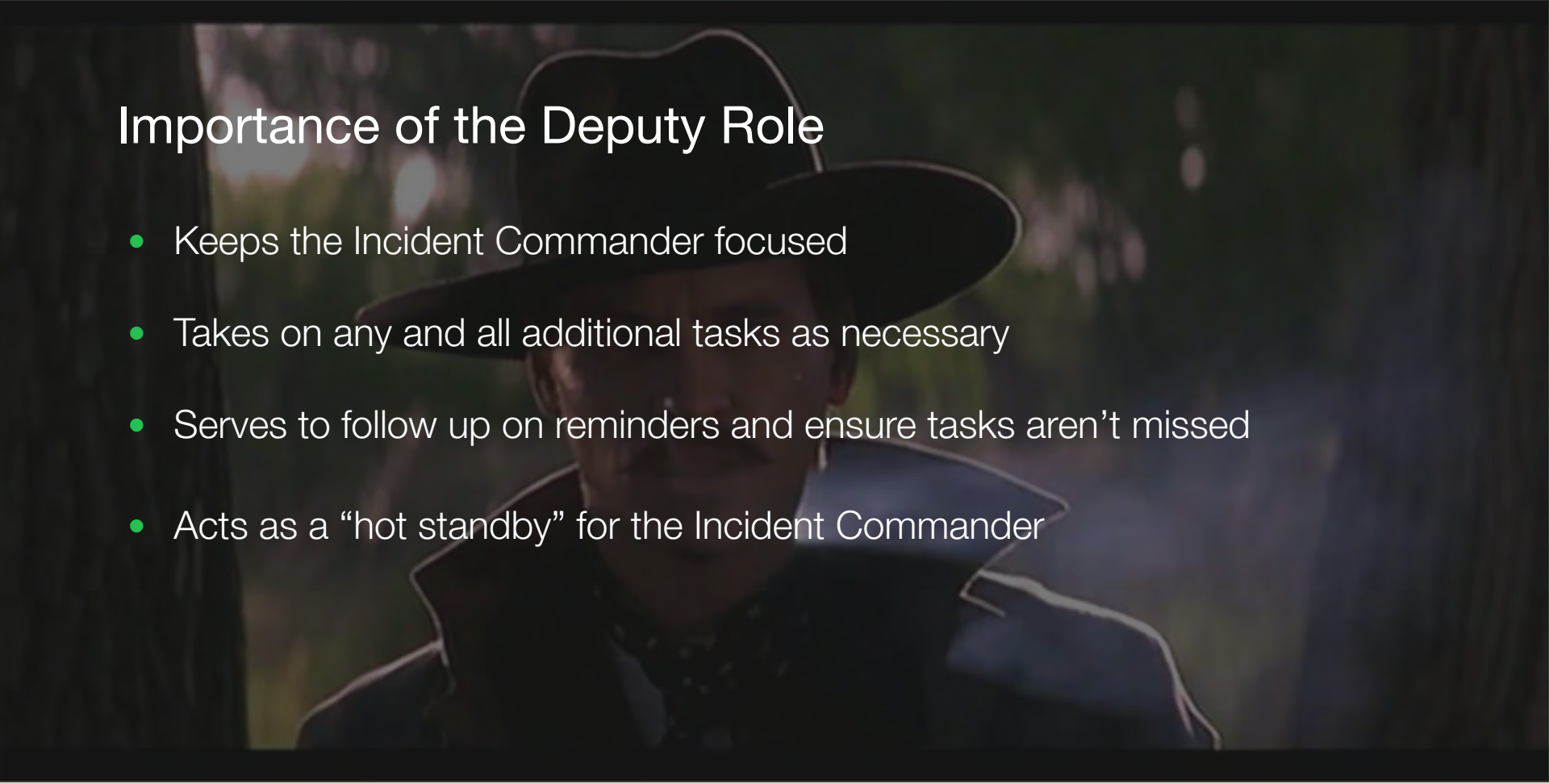


Summary: Importance of the Incident Commander

- 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

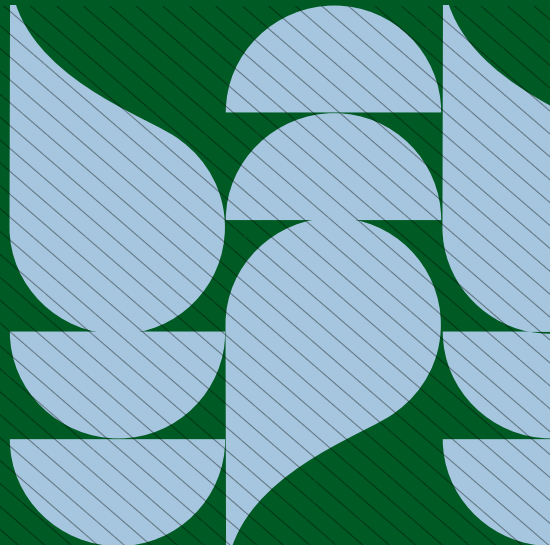
Importance of the Scribe

- 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

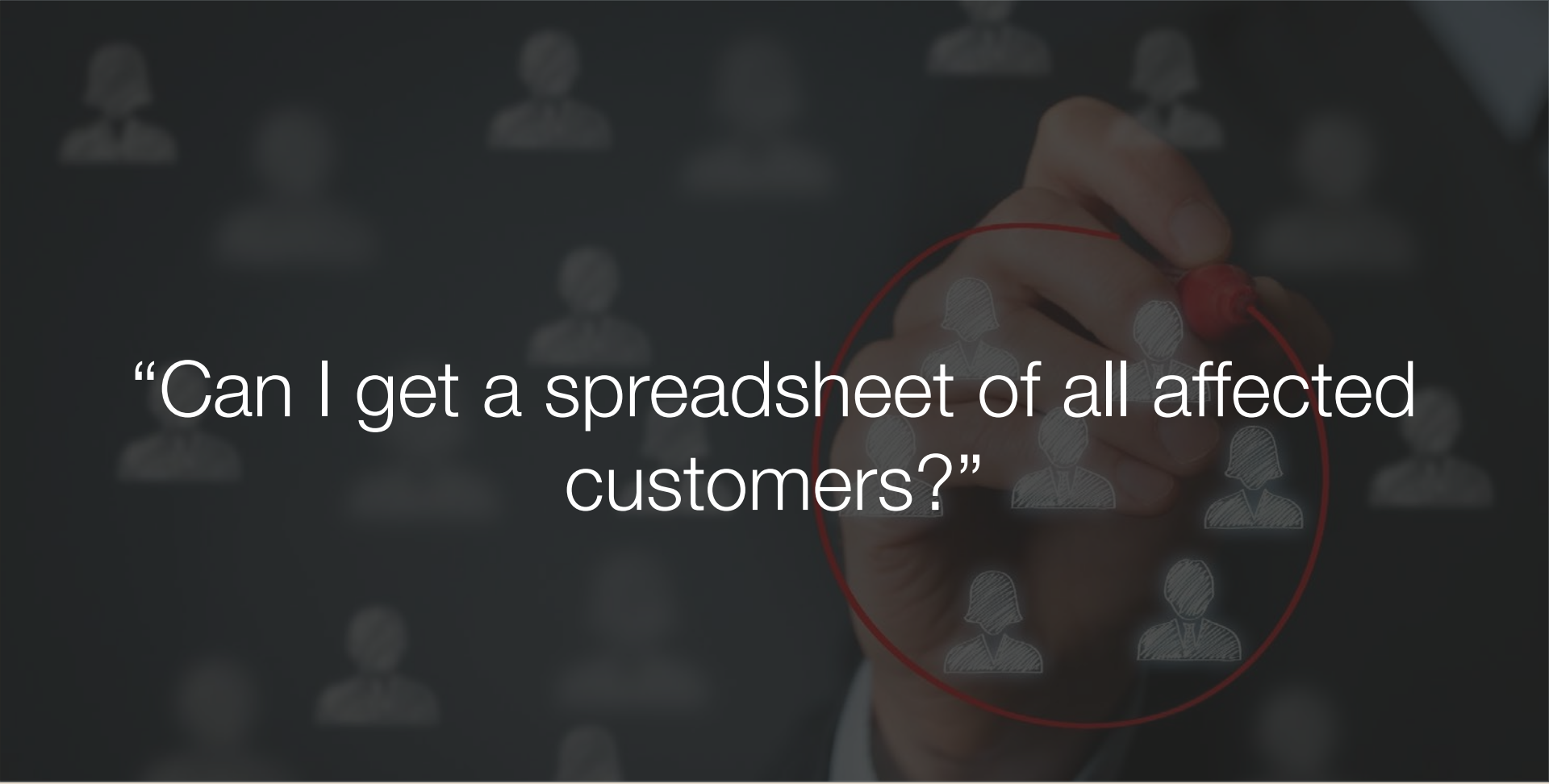
- Can be external, internal, or both
- Notifies customers of current conditions, and informs the Incident Commander of relevant feedback
- Crafts language appropriate status updates and notification messages
- Typically a member of the Support team

Incident Response Pitfalls



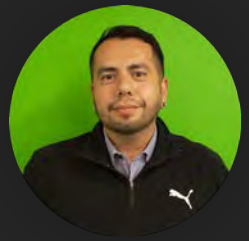

Executive Swoop


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


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


“Do what I say”

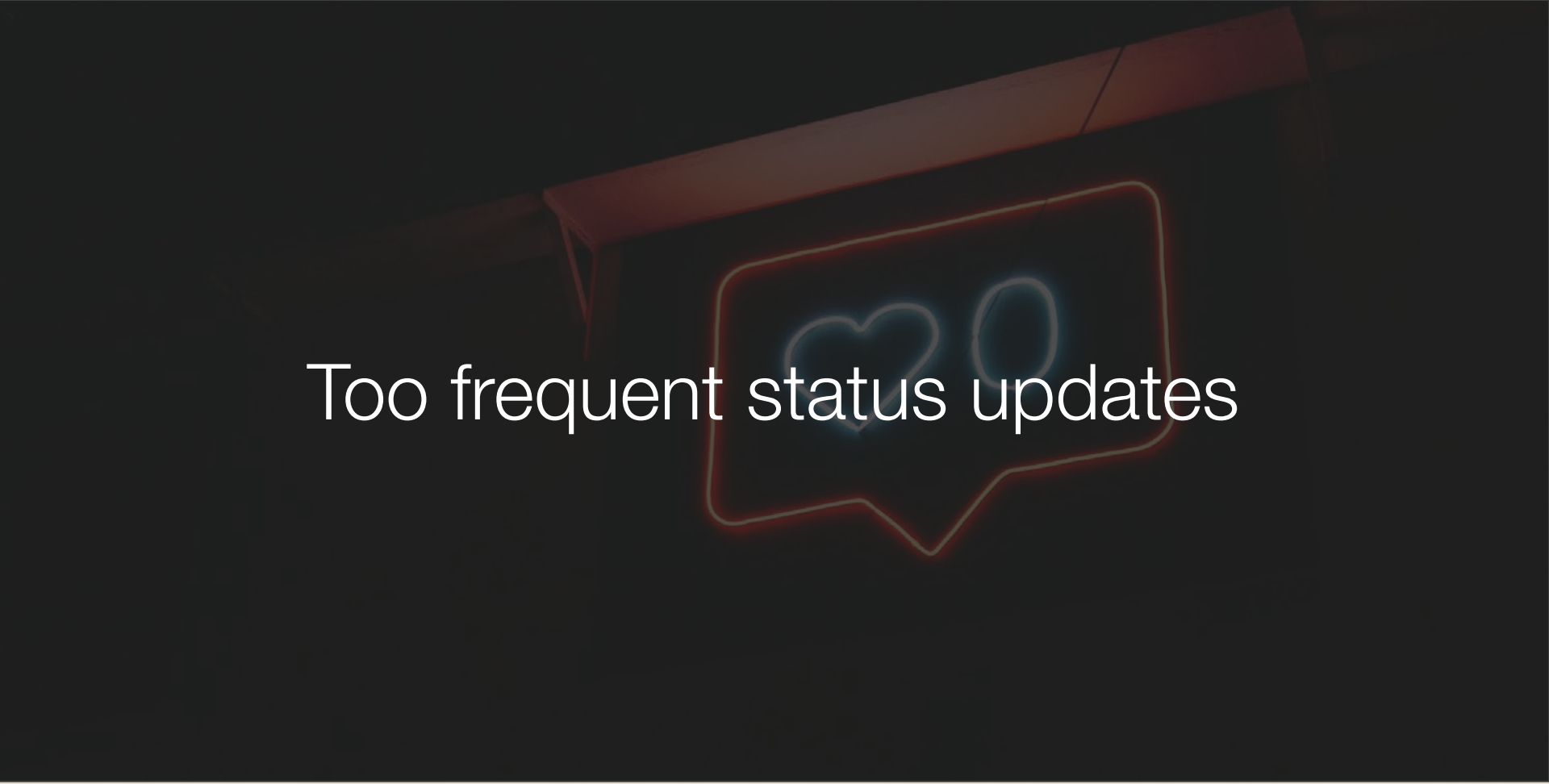
KEY TAKEAWAY



Do you wish to take command?

. . .


Failure to Notify Stakeholders



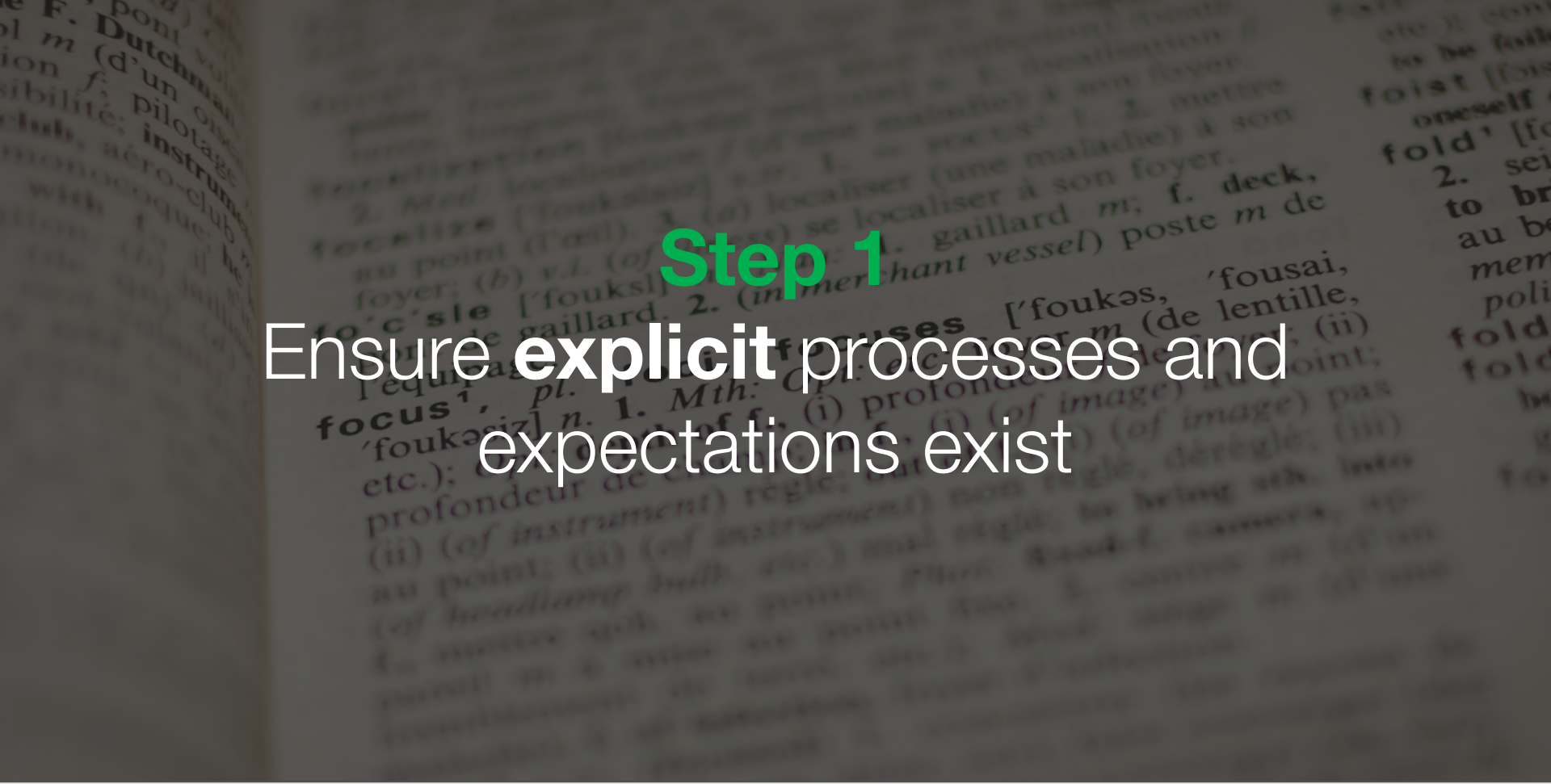
Too frequent status updates

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

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

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

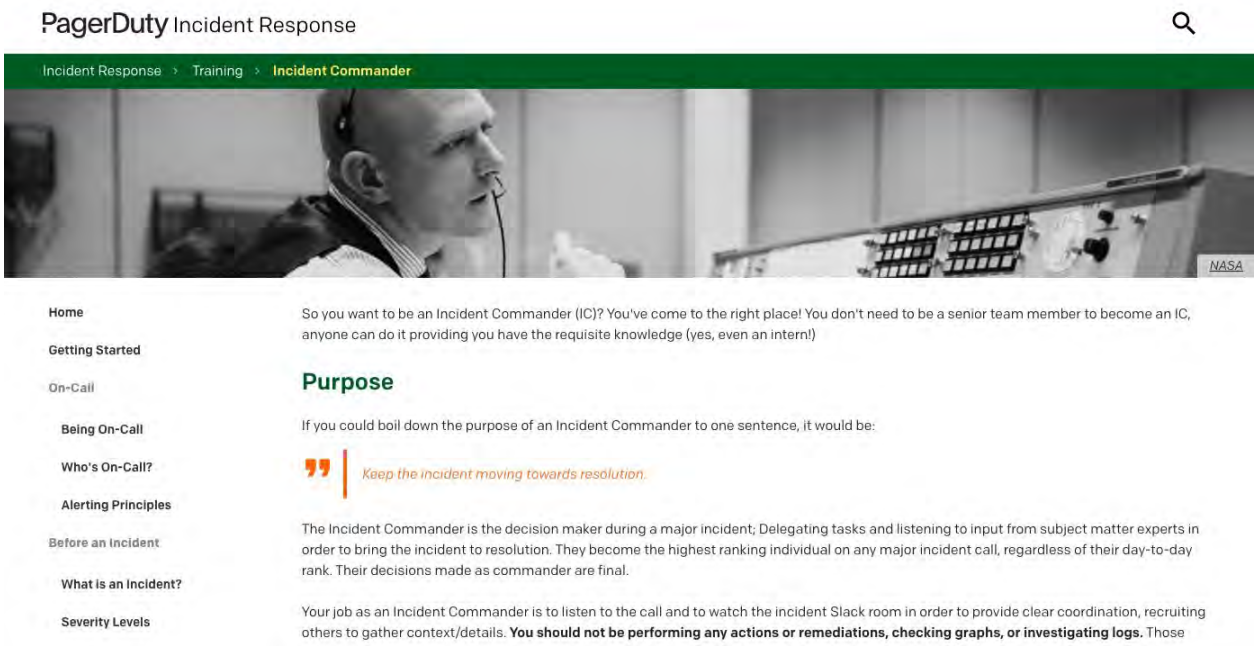
- Brief Overview: high level of the impact (1-2 sentences)
- What Happened: Detailed description (usually 1-2 paragraphs, or more)
- What went well
- What didn't go so well
- Action Items (if you don't have any, what was the point of having a response?)
- Contributing factors
- Resolution actions
- Impact: 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



Q&A

@QuintessenceAnx

https://noti.st/quintessence