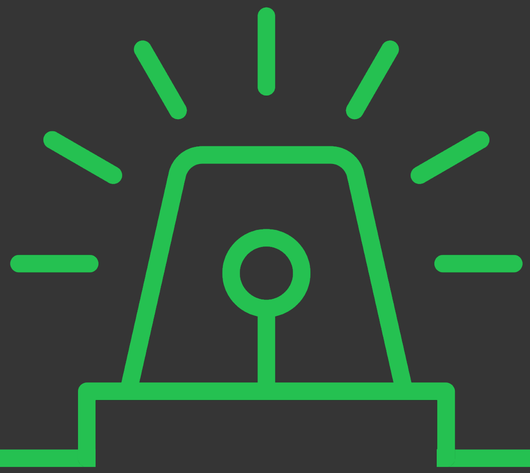
# Incident Response Training

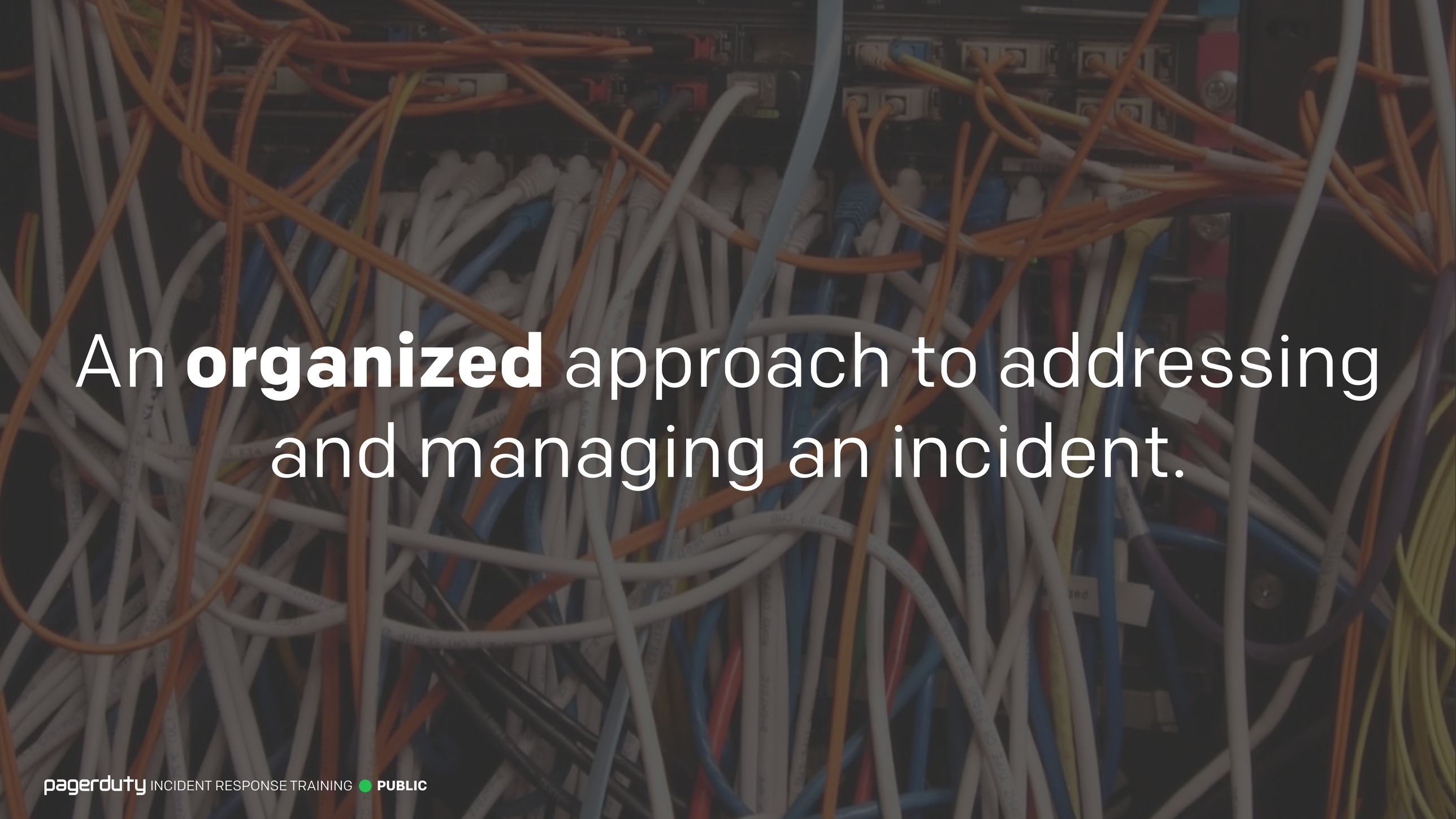
PAGERDUTY UNIVERSITY

**Rich Adams**
Security & Incident Response



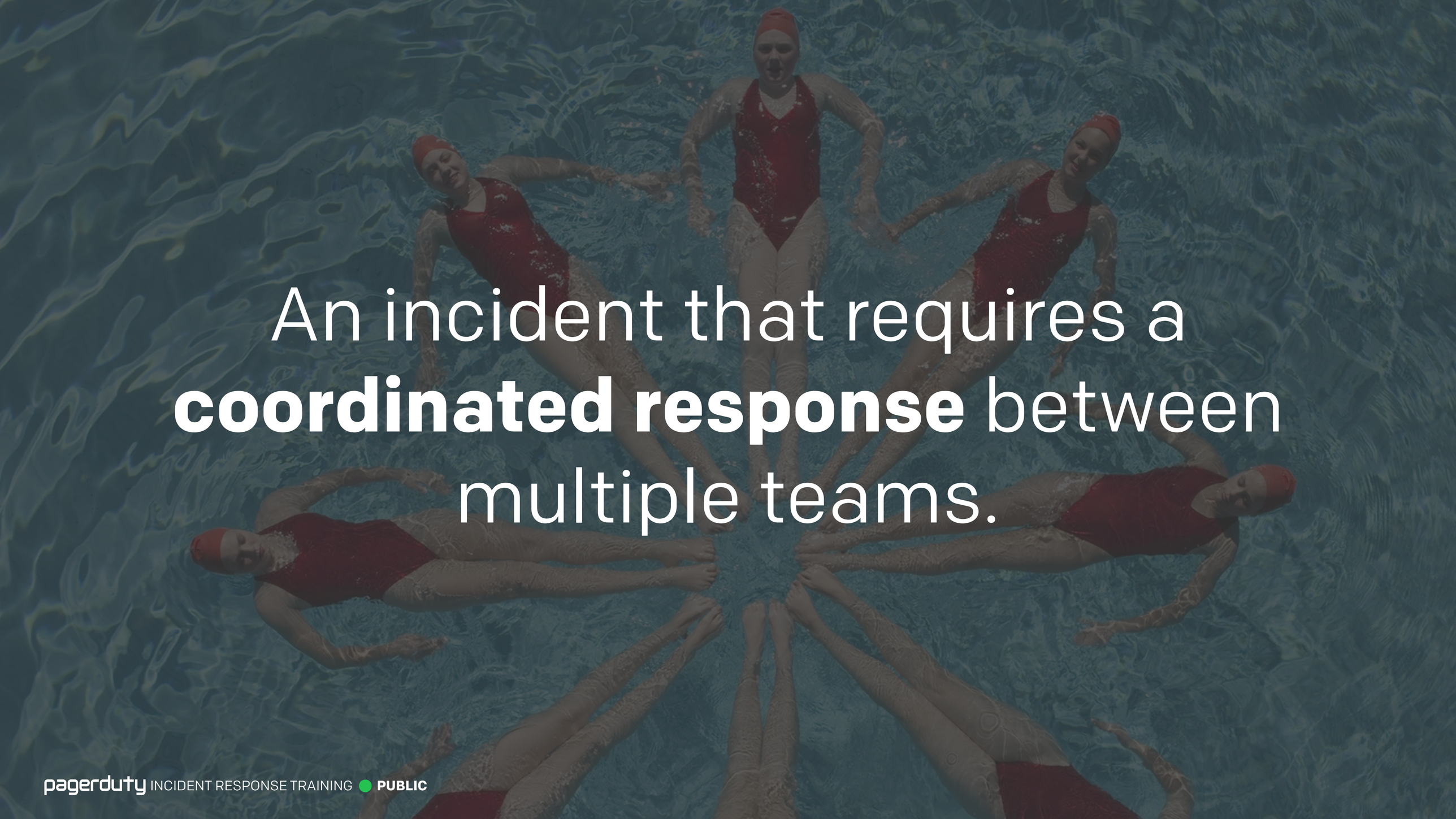

Learn how to **effectively manage incidents** within your organization.


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

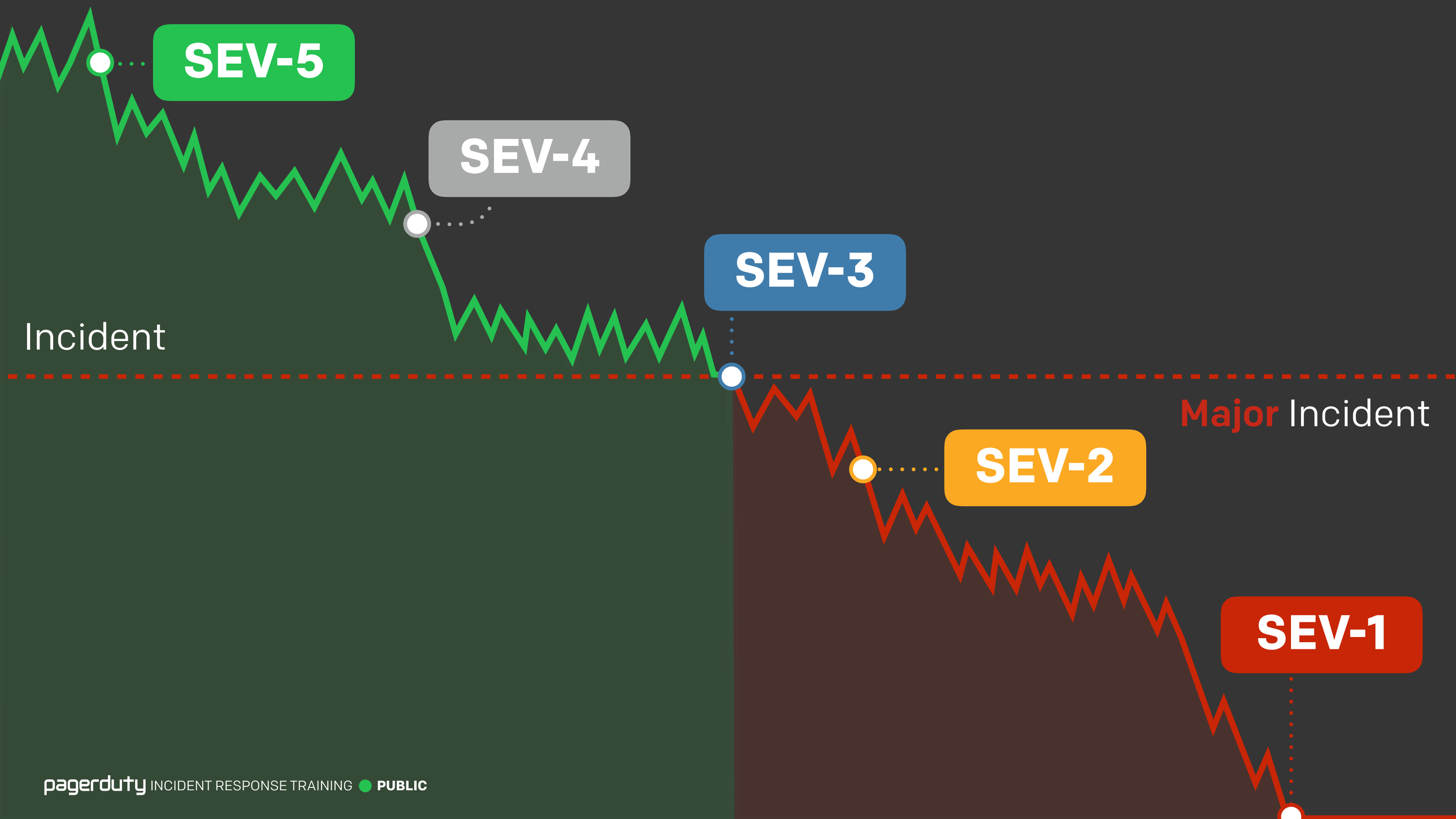

An **organized** approach to addressing
and managing an incident.

The goal is to handle the situation in a way that **limits damage** and **reduces** recovery time and costs.

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



An incident that requires a **coordinated response** between multiple teams.


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

KEY TAKEAWAY

**Anyone** can trigger incident response 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.

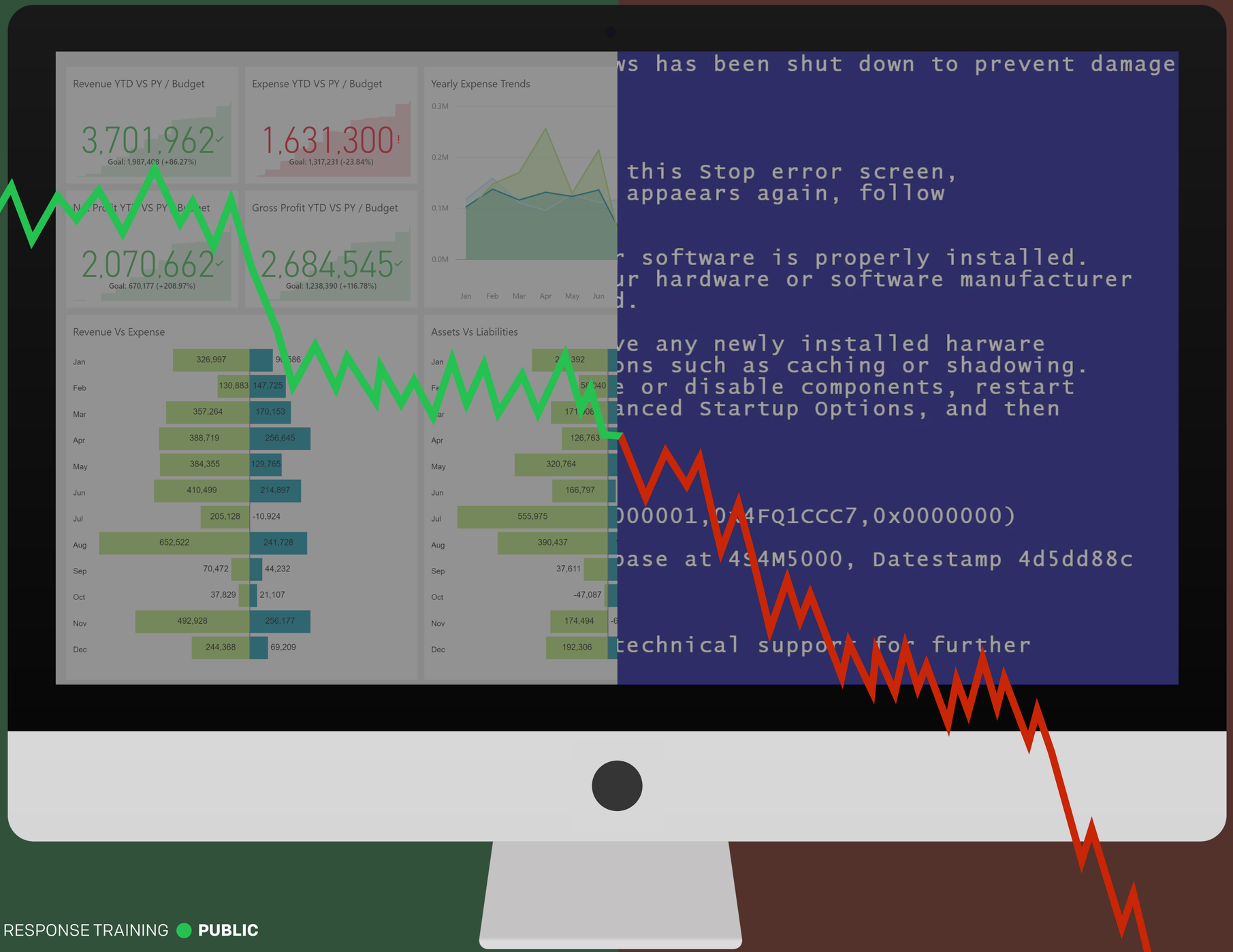
Renee Lung has been paged.

*Use* `!ic responders` *to see who the team responders are.*

Incident triggered: https://example.pagerduty.com/incident/PD5I34R

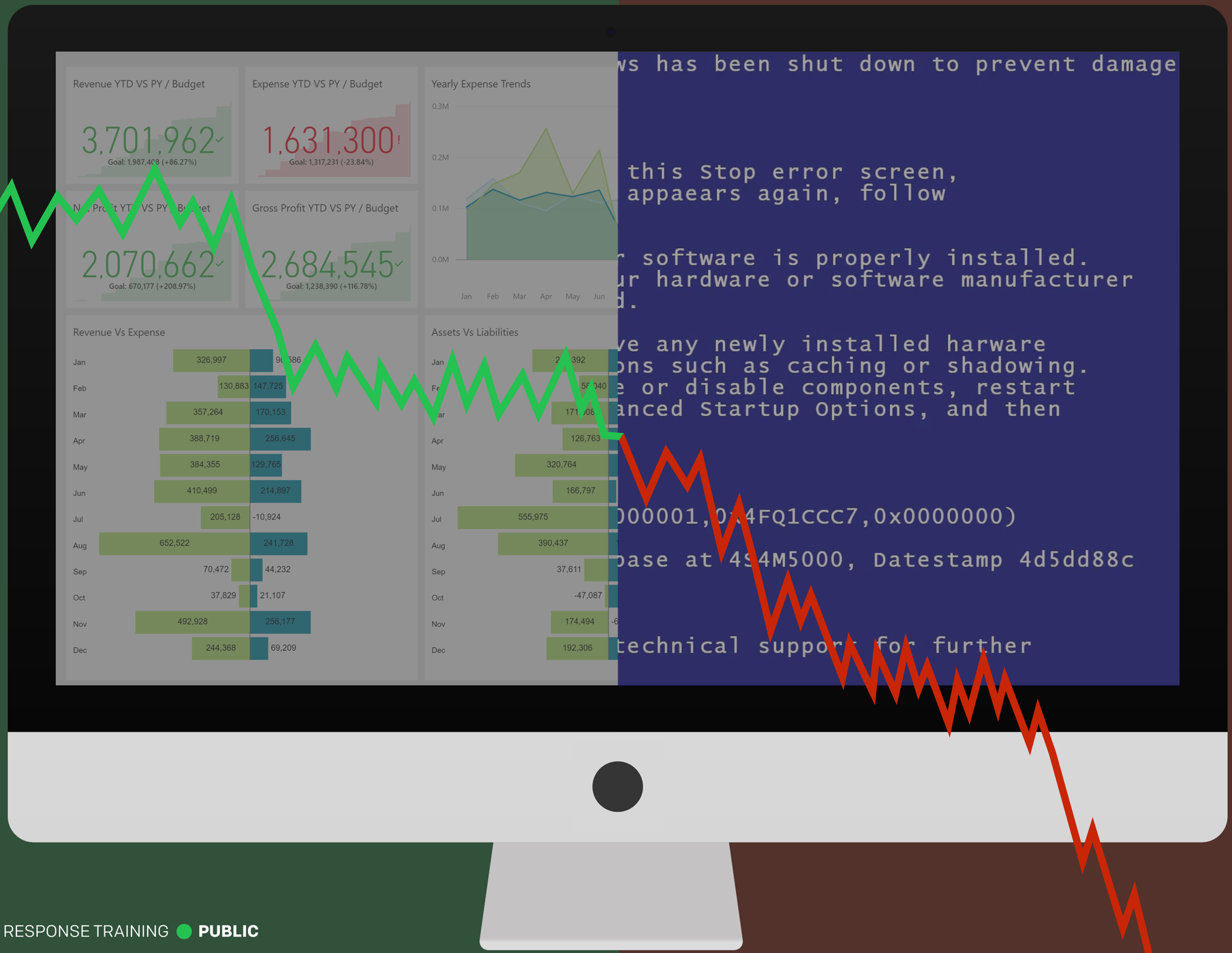
+ !ic page

PEACETIME

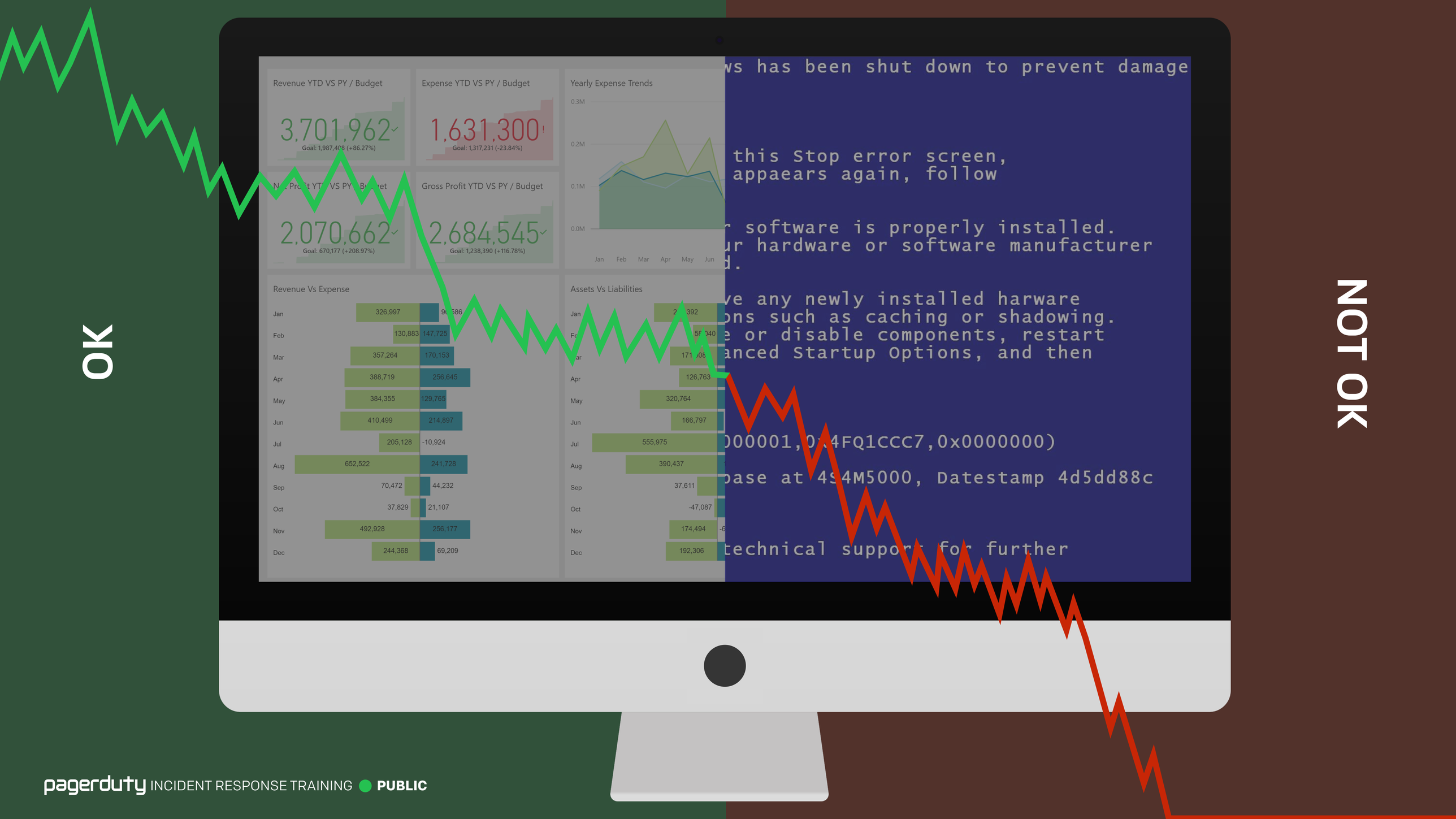



WARTIME

NORMAL




EMERGENCY


OK
NOT OK
Revenue YTD VS PY / Budget
3,701,962
Goal: 1,987,408 (+86.27%)
Expense YTD VS PY / Budget
1,631,300
Goal: 1,317,231 (-23.84%)
Yearly Expense Trends
0.3M
0.2M
0.1M
0.0M
Jan Feb Mar Apr May Jun
Gross Profit YTD VS PY / Budget
2,070,662
Goal: 670,177 (+208.97%)
2,684,545
Goal: 1,238,390 (+116.78%)
Revenue Vs Expense
Jan 326,997
Feb 130,883 147,725
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
Assets Vs Liabilities
Apr 126,763
May 320,764
Jun 166,797
Jul 555,975
Aug 390,437
Sep 37,611
Oct -47,087
Nov 174,494
Dec 192,306
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
000001,0x4FQ1CCC7,0x0000000)
base at 4s4M5000, Datestamp 4d5dd88c
technical support for further

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

National Incident Management System **(NIMS)**

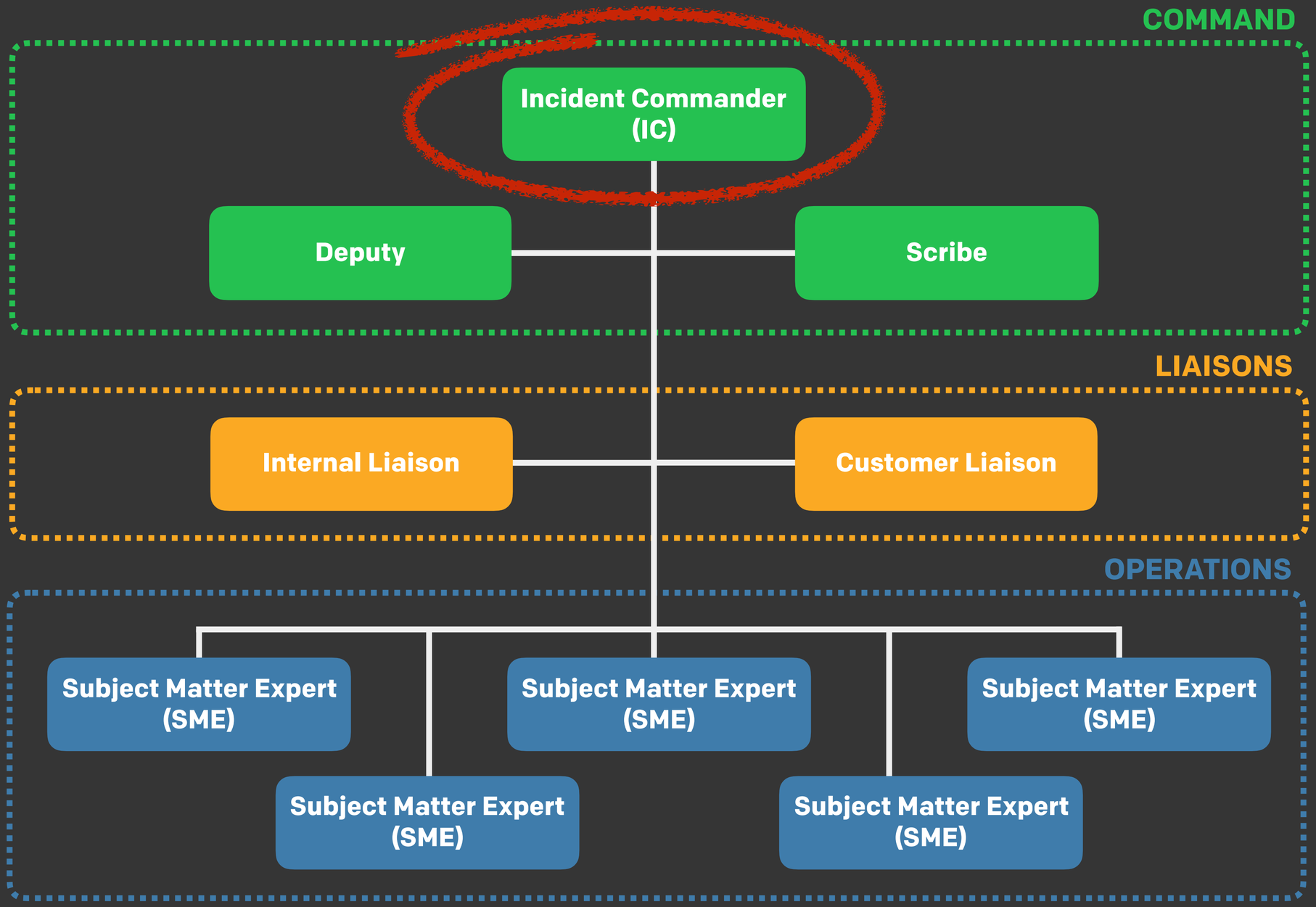
Coordinated Incident Management System **(CIMS)**

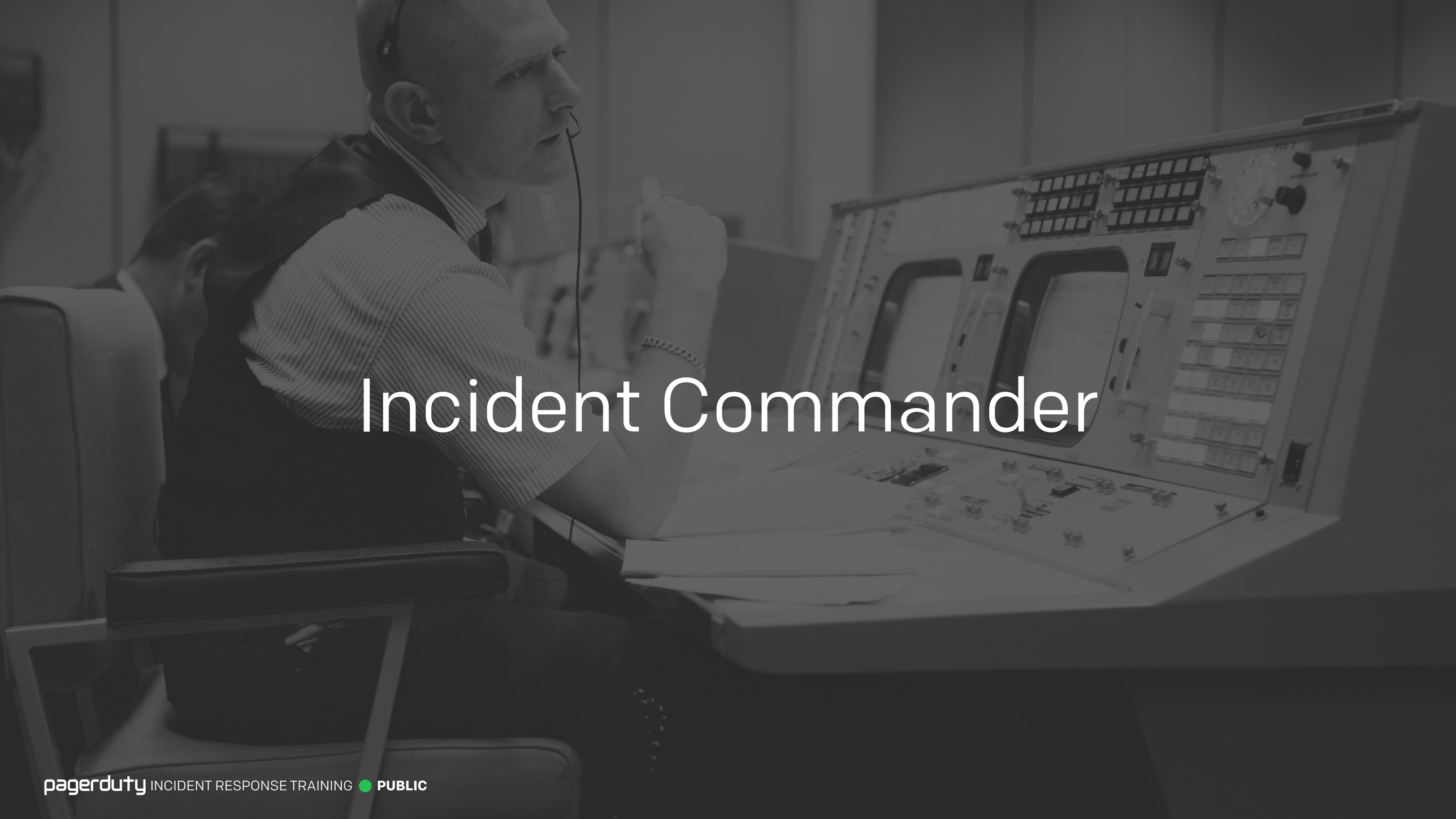
Australasian Inter-Service Incident Management System **(AIIMS)**

Gold-Silver-Bronze Command Structure **(GSB)**

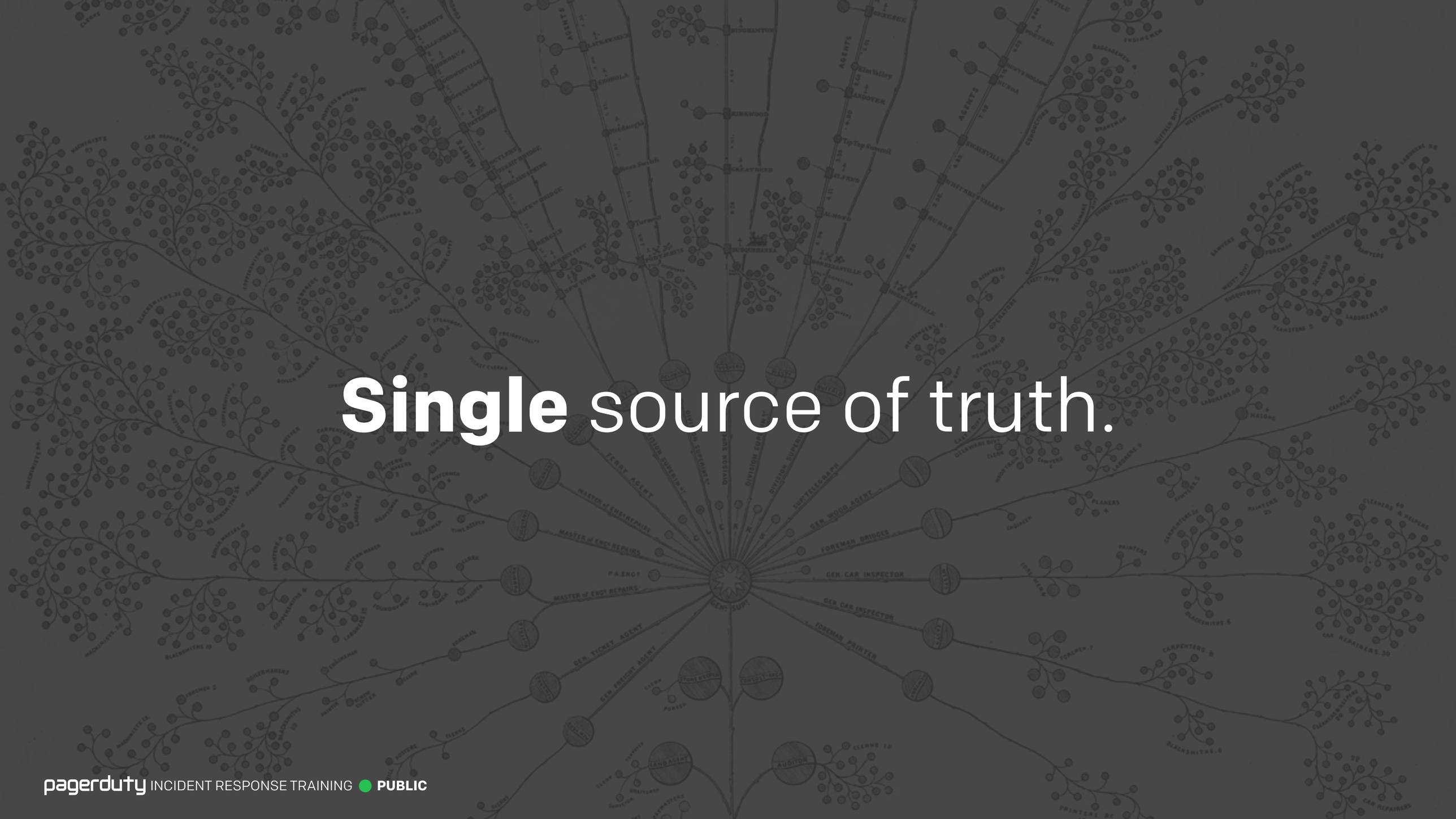
Incident Command System **(ICS)**

... and many other similar systems used in around the world.


COMMAND
Incident Commander (IC)
Deputy
Scribe
LIAISONS
Internal Liaison
Customer Liaison
OPERATIONS
Subject Matter Expert (SME)
Subject Matter Expert (SME)
Subject Matter Expert (SME)
Subject Matter Expert (SME)
Subject Matter Expert (SME)



# Incident Commander



# **Single** source of truth.


Becomes the **highest authority**.

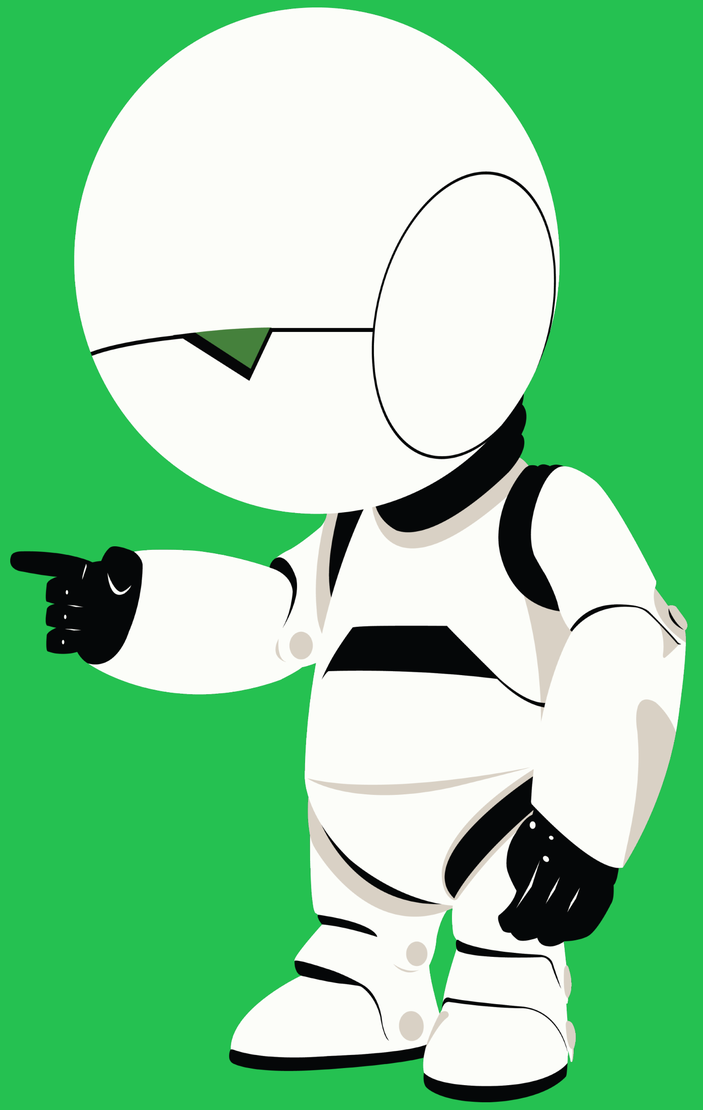

# Yes, they even **outrank the CEO**.

*Make sure your CEO knows this in advance!*

KEY TAKEAWAY

Not a resolver.
**Coordinates** and delegates.

# DON'T PANIC



I’m Rich.

I’m the Incident Commander.


**Introduce** yourself.


Say “Incident **Commander**”.


Good **communication** is essential.

DON’T DO THIS

Let’s get the IC on the RC, then get a BLT for all the SME’s.

KEY TAKEAWAY

# **Clear** is better than concise.

What’s wrong?

What actions can we take?

What are the risks involved?


Make a **decision**.


Gain **consensus**.

This background is blue.

Are there any strong objections?

. . .

Hearing none. Let’s proceed.

KEY TAKEAWAY

"Are there any **strong** objections?"

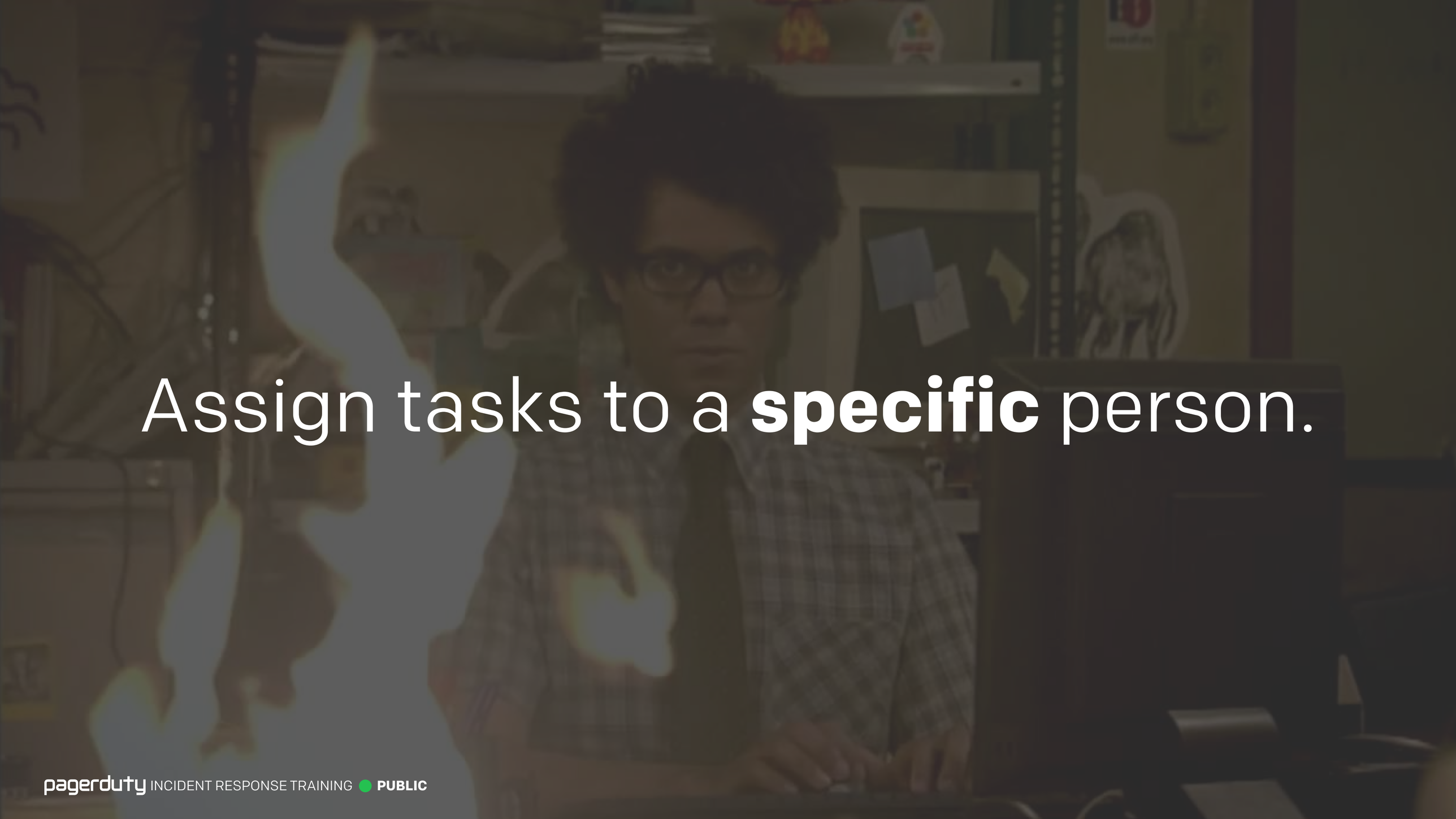

12
1
2
3
4
5
6
7
8
9
10
11

DON’T DO THIS

“Can **someone**...”

Eric, I'd like you to investigate the increased latency, try to find the cause. I'll come back to you in 5 minutes. Understood?

Understood.



Assign tasks to a **specific** person.


**Time-box** all tasks.


Get **acknowledgement**.

Eric, it's been 5 minutes. Do you have any information on the latency issue?

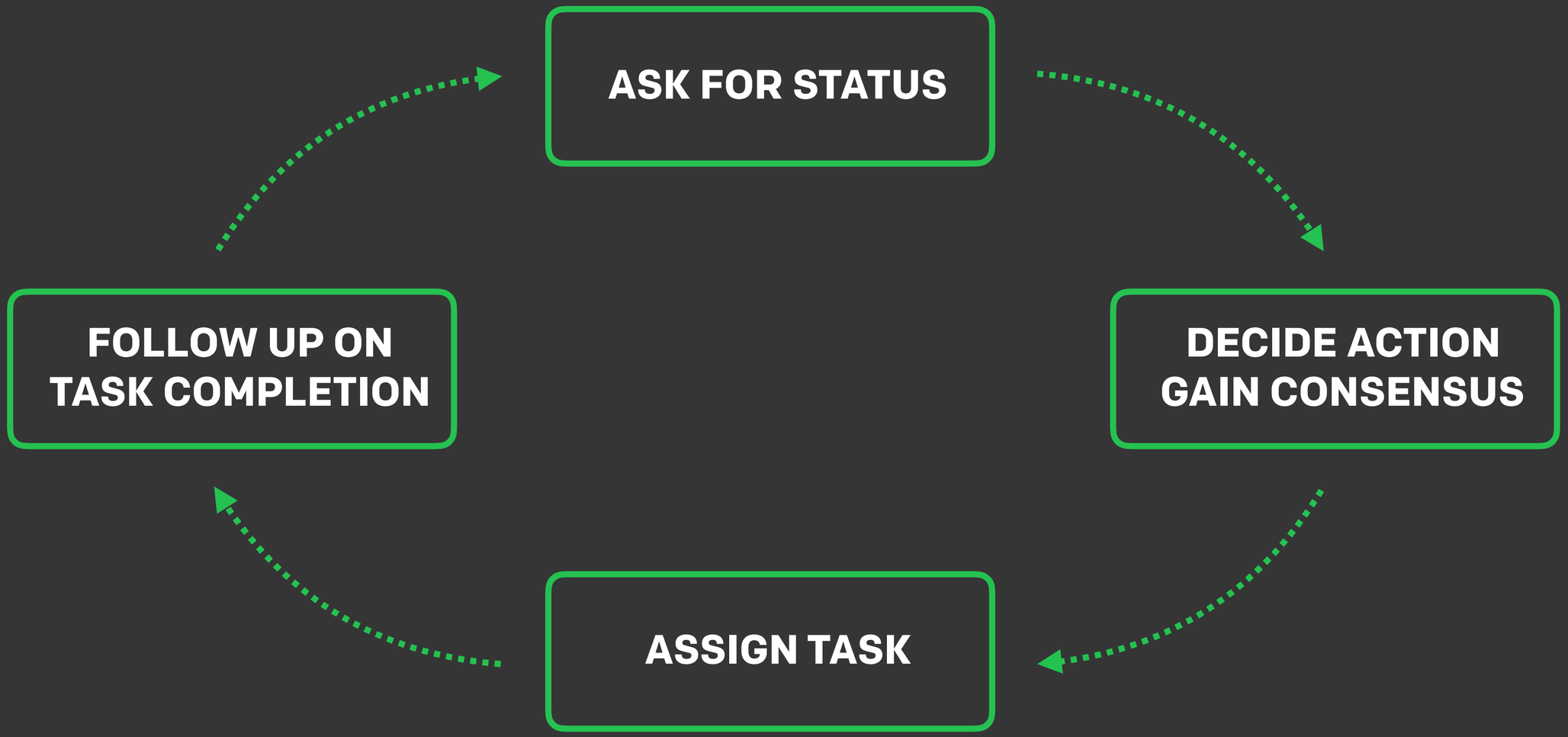
Yes, it looks like it was a bad firewall rule.

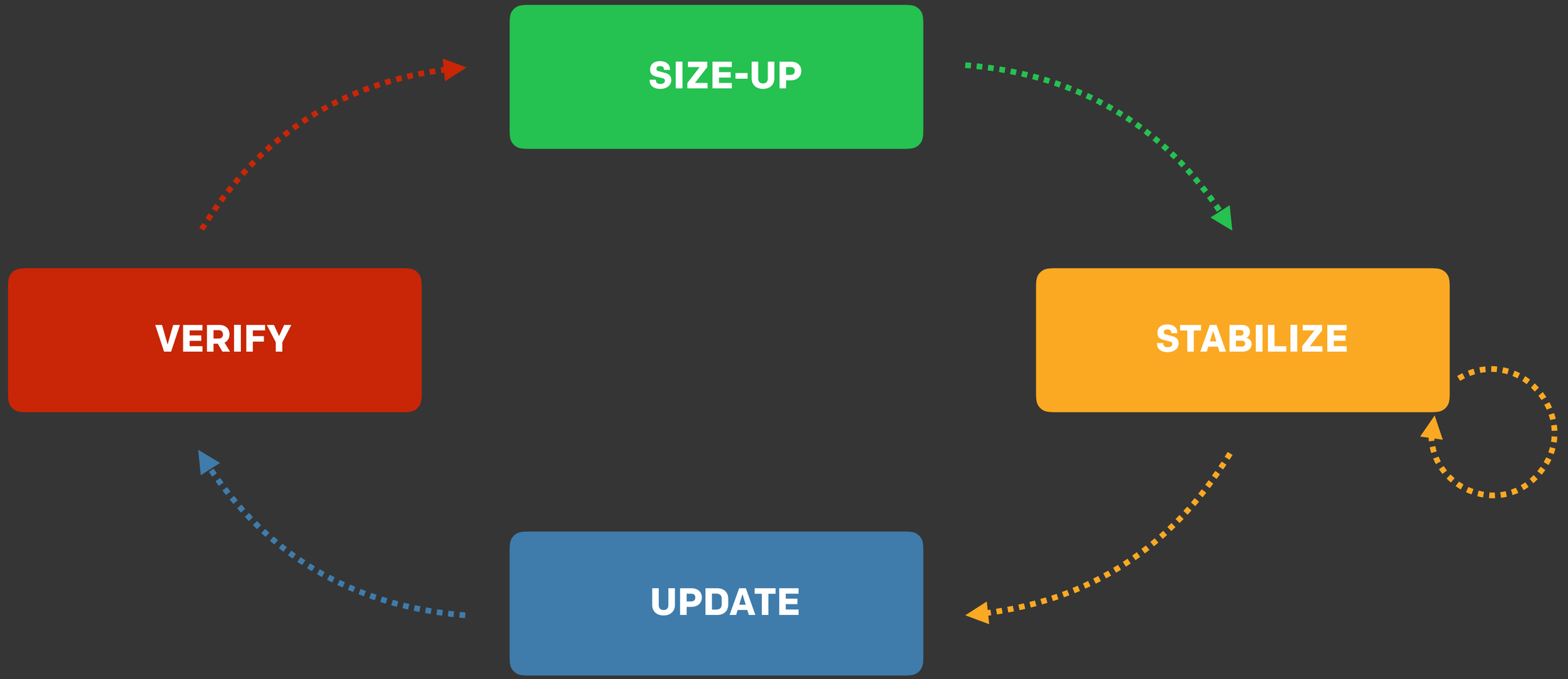

# What if they need more time?

How much time do you need?

20 minutes should be enough.

OK, I'll come back to you in 20.


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


SIZE-UP
STABILIZE
UPDATE
VERIFY


“Ignore the IC, do what I say!”

KEY TAKEAWAY

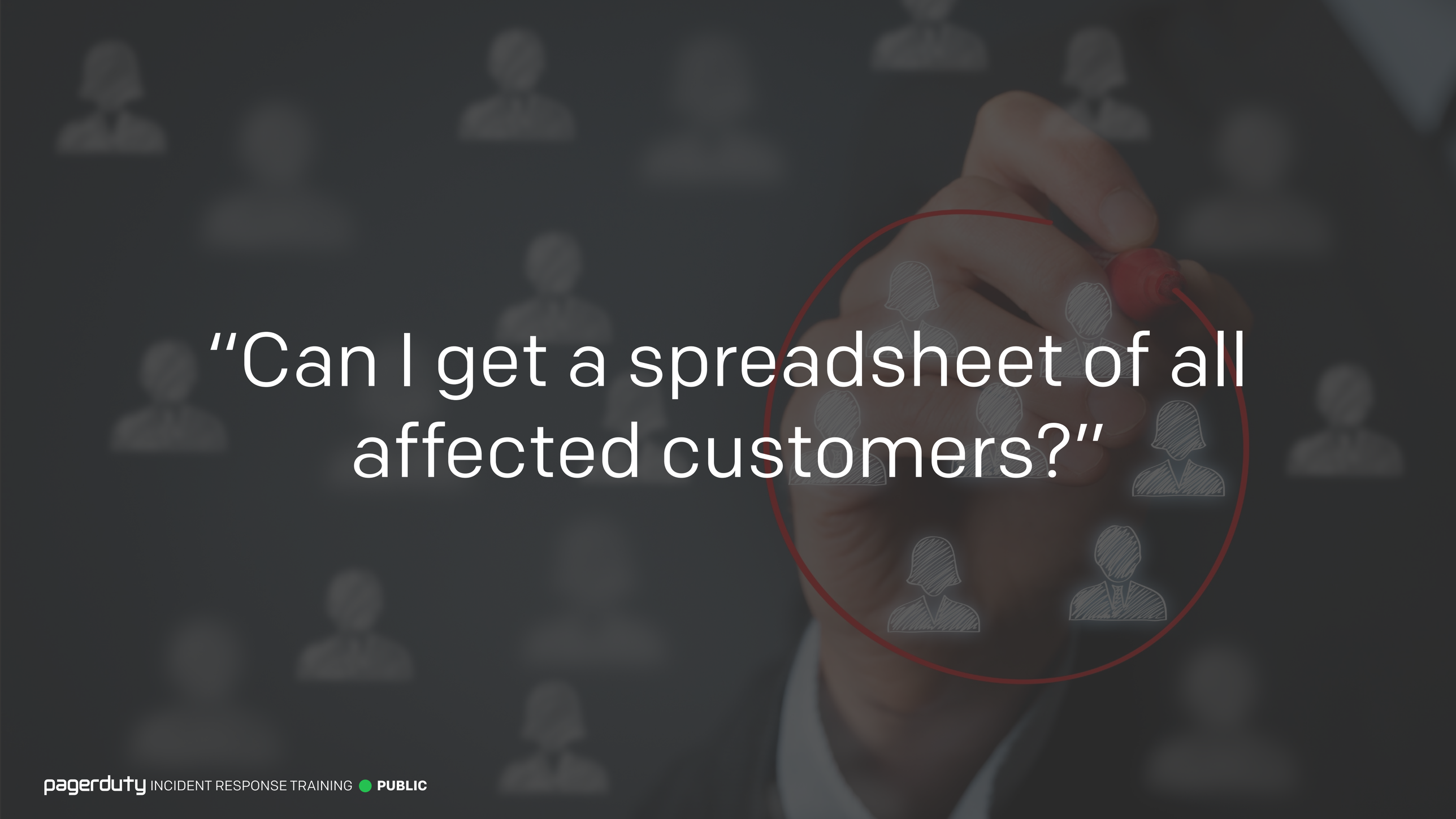
Do you wish to take command?

. . .

# Executive Swoop


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

We’re in the middle of an incident, please keep your comments until the end.


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

We can either get you that list, or fix the incident. Not both. The incident takes priority.


# “Is this really a SEV-1?”

We do not discuss incident severity during the call. We're treating this as a SEV-1.

KEY TAKEAWAY

# **Notify** stakeholders.


The belligerent responder.

You’re being disruptive. Please stop, or I will have to remove you from the call.

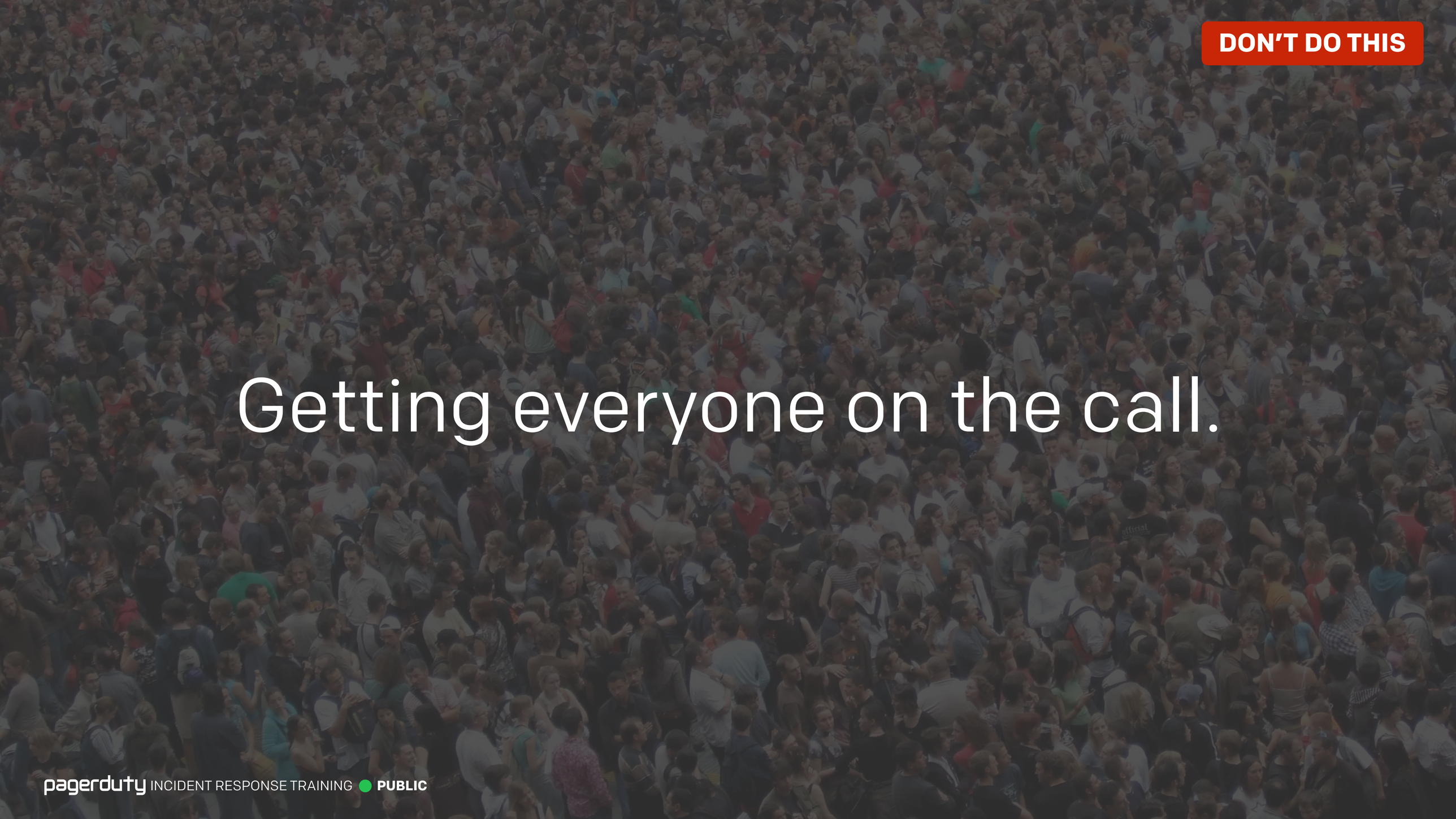
# Do responders get tired?


**Handovers** are encouraged.

Everyone on the call, be advised I'm handing over command to Eric.

This is Eric, I'm now the Incident Commander.

# Anti-Patterns


DON’T DO THIS
Getting everyone on the call.

DON’T DO THIS


# Not letting responders leave.

DON’T DO THIS

# Too frequent status updates.

DON’T DO THIS

# Being overly focussed on an issue.

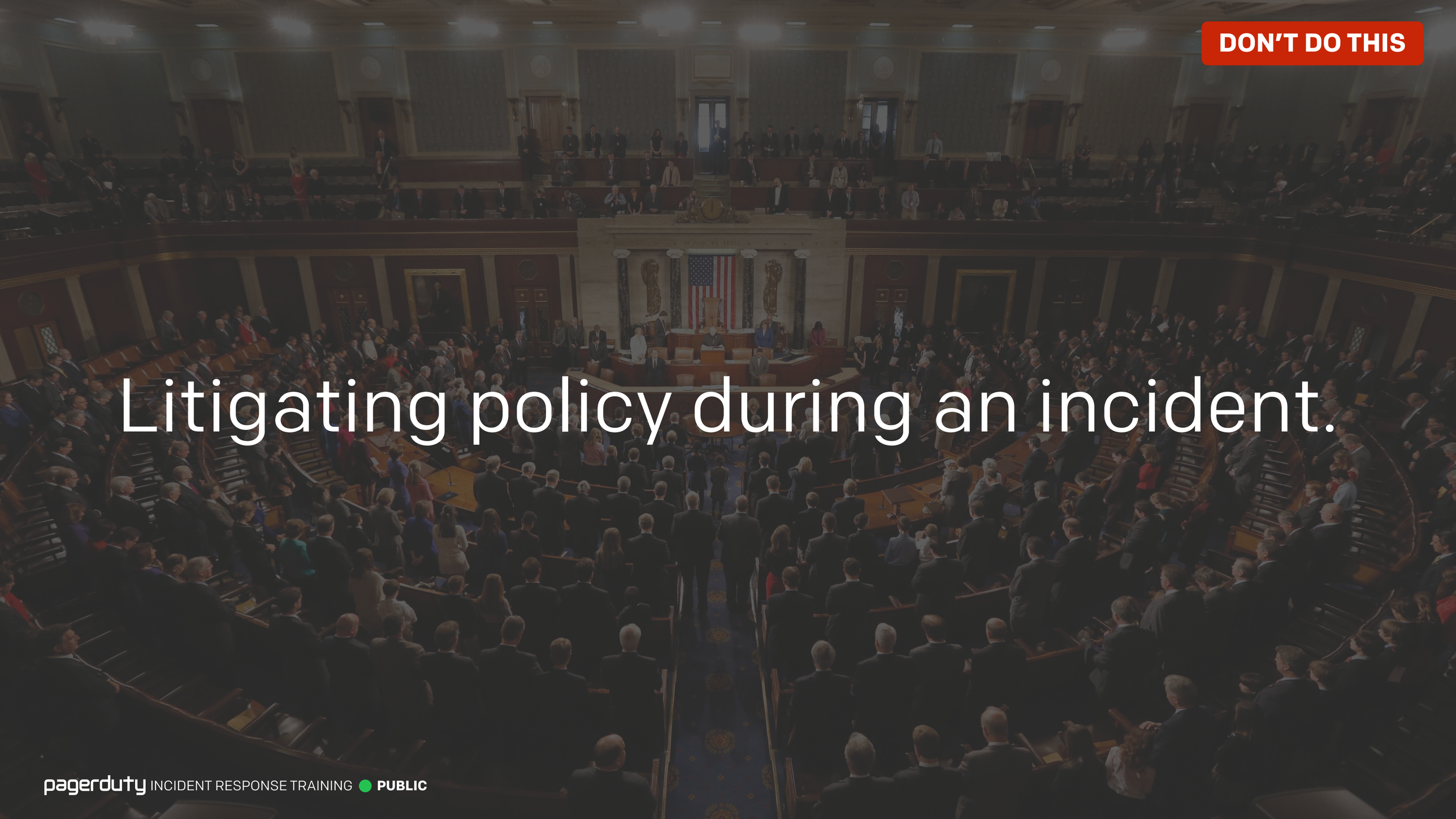
DON’T DO THIS

# Requiring deeply technical ICs.

DON’T DO THIS

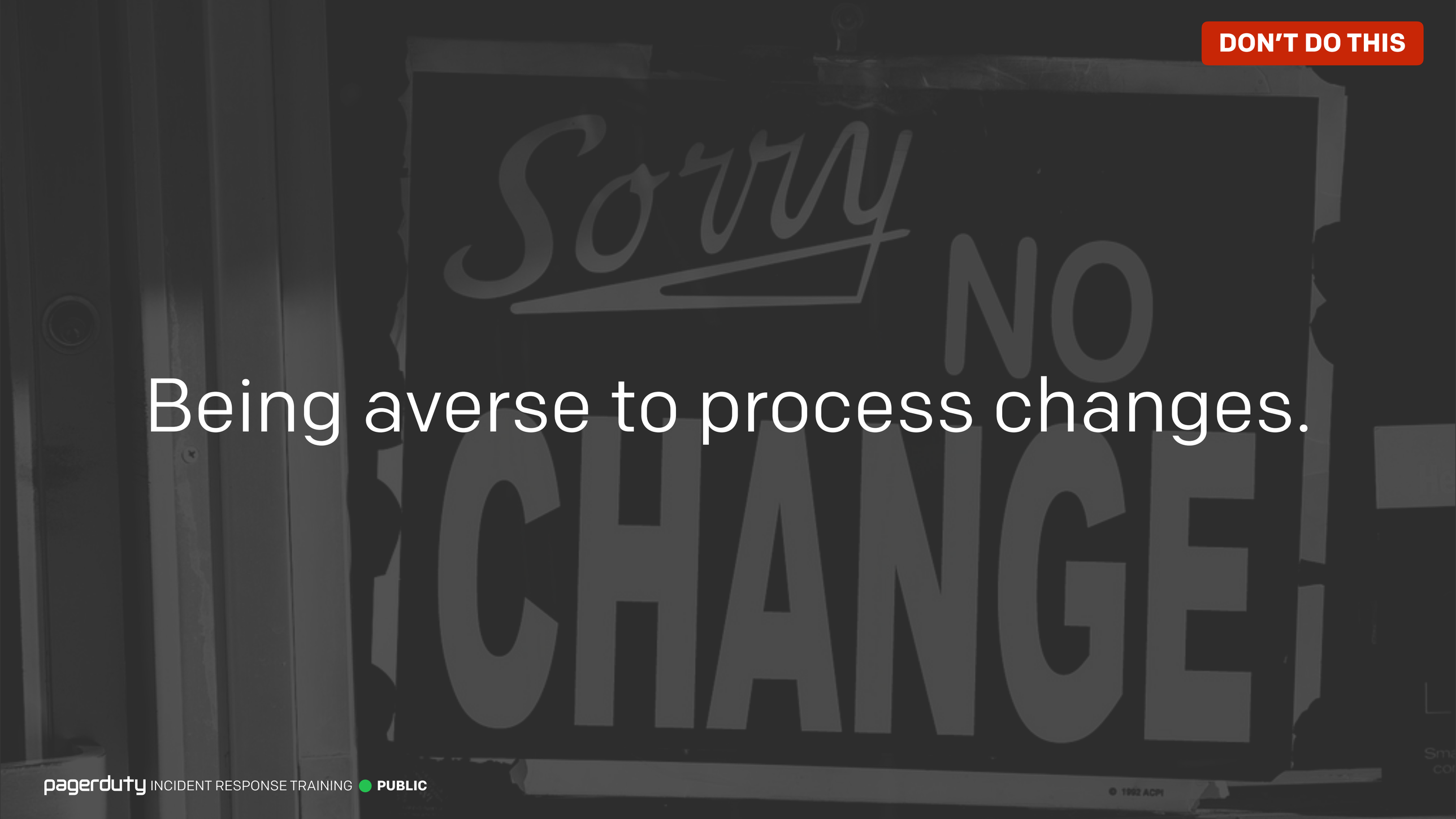

# Taking on multiple roles.

DON’T DO THIS



# Litigating policy during an incident.

DON’T DO THIS




# Being averse to process changes.

# ✔ Resolved

KEY TAKEAWAY

# Don’t neglect the **post-mortem**.

# **Create** the post-mortem.


Pick an **owner**.

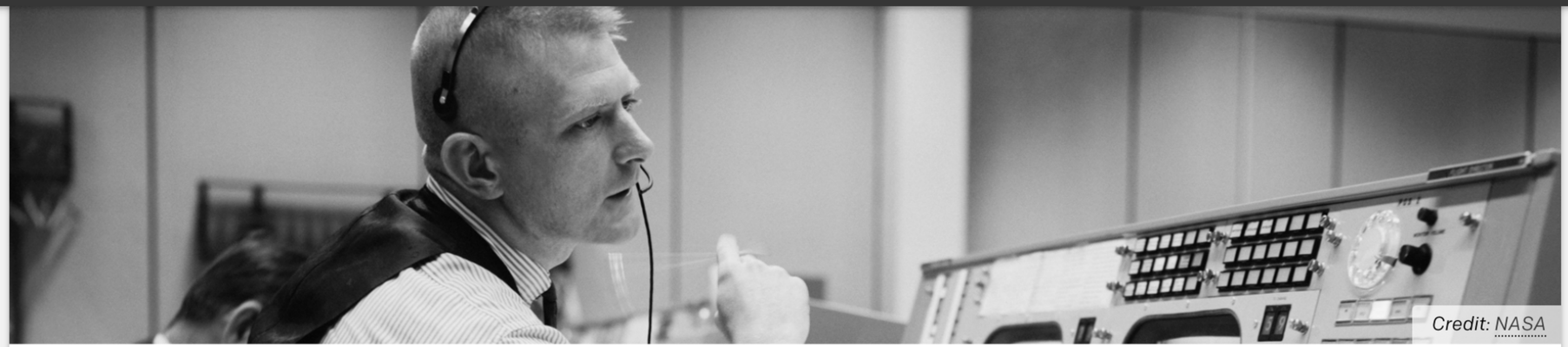

Blameless.

KEY TAKEAWAY

# Review the **process** too!


**Practice** makes perfect.

https://response.pagerduty.com



Credit: NASA

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 an 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 tasks should be delegated.

KEY TAKEAWAY

- Have an **Incident Commander**.
- **Clear** is better than concise.
- Are there any **strong** objections?
- Assign tasks to **individuals**.
- Keep **stakeholders** notified.
- **Handover** regularly.
- Don’t neglect the **post-mortem**.

**Learning:** https://www.nmbu.no/sites/default/files/styles/bildebanner_med_tekst/public/bannerbilde_cropped.png
**Chaos:** http://www.blogcdn.com/slideshows/images/slides/254/973/3/S2549733/slug/l/chicken-run-hennen-rennen-chicken-run-als-eines-tages-der-fliegende-zirkushahn-rocky-auftaucht-scheint-endlich-gingers-2.jpg
**Messy Cables:** https://blog.dotcom-monitor.com/wp-content/uploads/2013/06/horrible-cable-management-systems.jpg
**Fire Extinguish:** https://blog.servicemasterrestore.com/wp-content/uploads/2016/03/1115.6-How-to-Use-a-Fire-Extinguisher.jpg
**Computer Fire:** https://img-comment-fun.9cache.com/media/aMrdZ5P/aYXLN6nm_700w_0.jpg
**Synchronized Swimming:** http://quarterly.insigniam.com/wp-content/uploads/cache/2014/10/shutterstock_1481018421/1996472669.jpg
**Big Red Button:** http://s.newsweek.com/sites/www.newsweek.com/files/2016/06/06/ai-google-red-button-artificial-intelligence.jpg
**Normal:** https://i2.wp.com/databear.com/wp-content/uploads/2017/06/FA-Dashboard.png?fit=3840%2C2160
**Emergency:** https://i.ytimg.com/vi/_aT9r3ZFErY/maxresdefault.jpg
**ICS:** http://www.trbimg.com/img-58952e59/turbine/sd-me-wildfire-case-20170127
**Around the World:** https://upload.wikimedia.org/wikipedia/commons/0/0d/Iss007e10807.jpg
**Incident Commander:** https://upload.wikimedia.org/wikipedia/commons/6/60/Eugene_F._Kranz_at_his_console_at_the_NASA_Mission_Control_Center.jpg
**Source of Truth:** https://s-media-cache-ak0.pinimg.com/originals/f3/91/31/f391314c1752e9b7ea7cdad11f4039d7.jpg
**Chess:** http://www.thechesspiece.com/prodimages/Jazzy_chess_set_w_1500.jpg
**Outrank CEO:** https://edsurge.imgix.net/uploads/post/image/4410/10-1520986021.jpg
**Orchestra:** https://cdn-images-1.medium.com/max/2000/1*fBPpHzoI5M-K6TGpKrqDDA.jpeg
**Introduce:** https://douglasvermeeren.files.wordpress.com/2017/03/handshake.jpg
**"Incident Commander":** http://i0.wp.com/www.preparedex.com/wp-content/uploads/2017/02/Incident-Commander.jpg?fit=1698%2C1131
**Communication:** https://assets.entrepreneur.com/content/3x2/1300/20141106201954-good-communication-skills-help-you-find-long-term-success.jpeg
**Clear:** https://i.imgur.com/NnQhVMh.png
**Decision:** https://static1.squarespace.com/static/5244bc31e4b0d312c8099ac4/t/558ad556e4b0a7d87c0e7b65/1435161943391/DECISION+EFFECTIVENESS+%28DE%29.jpg?format=1500w
**Consensus:** https://3c1703fe8d.site.internapcdn.net/newman/gfx/news/hires/2016/thethingspeo.jpg
**Clock:** http://www.wikihow.com/images/5/54/Read-a-Clock-Step-6Bullet3-Version-2.jpg
**Assign Task:** https://i.ytimg.com/vi/y_pwBQuINSA/maxresdefault.jpg
**Time Box:** https://agilesetchu.files.wordpress.com/2015/09/timebox.jpg?w=1200

**Agree/Disagree:** http://blog.iproperty.com.sg/wp-content/uploads/2011/08/93506577.jpg
**Need Time:** https://static.pexels.com/photos/1778/numbers-time-watch-white.jpg
**Business Suit:** https://static.pexels.com/photos/29642/pexels-photo-29642.jpg
**Executive Swoop:** http://esq.h-cdn.co/assets/15/12/1600x800/landscape-1426858802-office-space-lumbergh1.png
**Suit:** http://az616578.vo.msecnd.net/files/2016/03/25/635944677511654874-1232941586_20150406171632-suit-man-jacket-corporate-business-shirt-tie-man.jpg
**Spreadsheet:** http://tubularinsights.com/wp-content/uploads/2016/01/video-marketing-target-audience.jpg
**Fire Alarm:** http://base-3.com/files/2013/03/fire_alarm_USPS.jpg
**Notification:** http://www.digitaltrix.com.br/wp-content/uploads/2016/04/layout_DTrix2-1.jpg
**Shouting:** https://lh3.googleusercontent.com/--pZnB_k0k1o/VuwmMWhcQgI/AAAAAAAAAww/6PJpke0OEFs/w1924-h1427/shout.jpg
**Tired:** https://cdn.idntimes.com/content-images/post/20170504/d1-b3fce02c6f36eecf663cd6aafea70ea4.jpg
**Handover:** http://1.bp.blogspot.com/-QnTDOI6-Xc0/Vi2yOMJwRNI/AAAAAAAAZw0/6hH-IatP7rU/s1600/african%2Bamerican%2Bbaton%2Bpass%2Brelay%2Bracers%2Bgenerations%2Bcourtesy%2Bof%2BTheo%2BFitzhugh%2Bshutterstock%2Bcom_50094679.jpg
**Anti-Patterns:** http://blogs.gartner.com/hank-barnes/files/2015/11/squarepeg.jpg
**Everyone:** https://a.spirited.media/wp-content/uploads/sites/2/2015/08/crowd-parkway.jpg
**Updates:** http://whitelabeled.nl/wp-content/uploads/2014/06/update-key-software.jpg
**Stop:** https://dukeofdollars.com/wp-content/uploads/2017/05/stop-sign.jpeg
**Tunnel Vision:** https://upload.wikimedia.org/wikipedia/commons/b/bc/Tunnel_Vision_%2819599074868%29.jpg
**Technical**: https://elkjerkyforthesoul.files.wordpress.com/2011/11/mathematics6.jpg
**Multiple Hats:** https://i.ytimg.com/vi/TZNNnTTwQrs/maxresdefault.jpg
**Congress:** https://www.brookings.edu/wp-content/uploads/2016/06/congress006-1.jpg
**No Change:** http://farm6.staticflickr.com/5114/6929697914_0fd3bd4457_b.jpg
**Neglect Post-Mortem:** http://www.newyorker.com/wp-content/uploads/2017/01/170102_r29228-1200x945-1481756110.jpg
**Post-Mortem:** http://www.marinerinvestments.com/wp-content/uploads/2016/03/10-Points-to-read-on-a-Mutual-Fund-Document.jpg
**Pick Owner:** http://www.basementlight.com/wp-content/uploads/2014/07/6-interview-questions.jpg
**Blameless:** http://images.huffingtonpost.com/2016-09-27-1474997998-3387706-Blame.jpg
**Work on Laptop:** http://www.freepik.com/free-photo/miniature-workmen-repairing-a-laptop-keyboard_991609.htm
**Practice:** https://i.ytimg.com/vi/2FwJLLGeTdU/maxresdefault.jpg

pagerduty pd u UNIVERSITY