

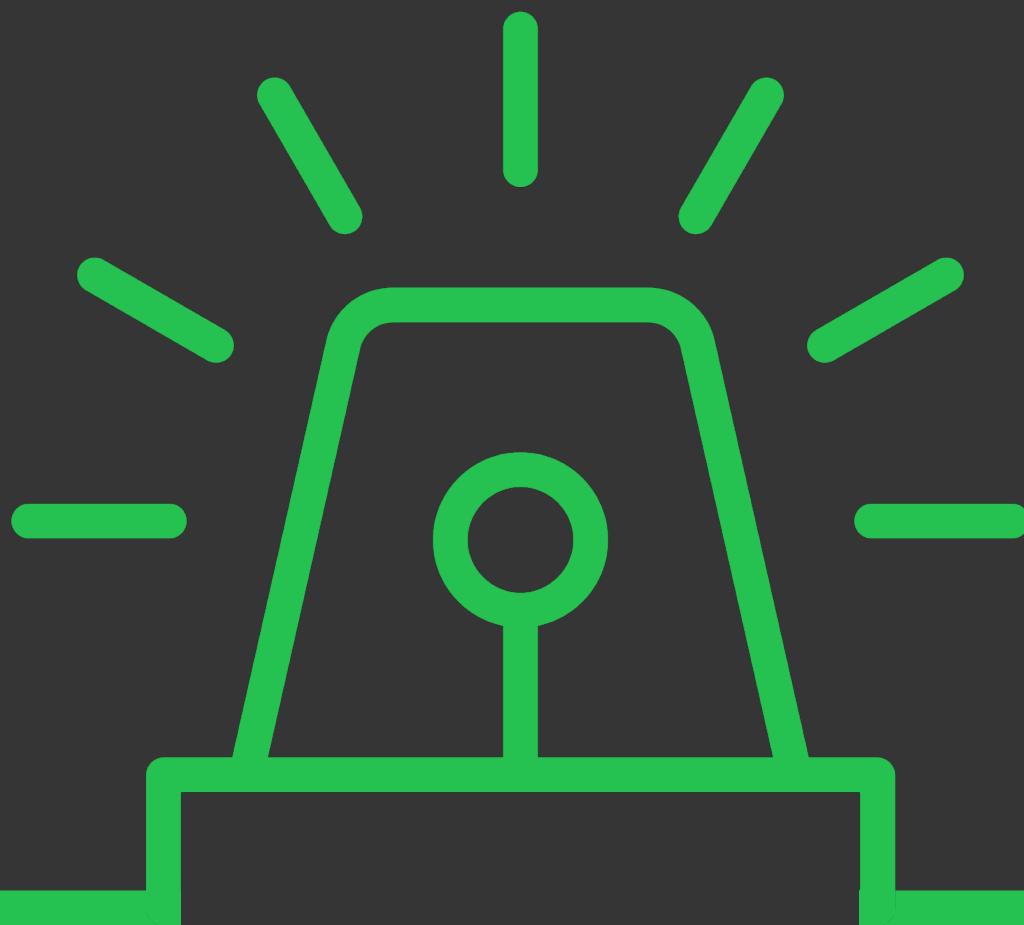
Incident Response Training

PAGERDUTY UNIVERSITY



Rich Adams

Security & Incident Response

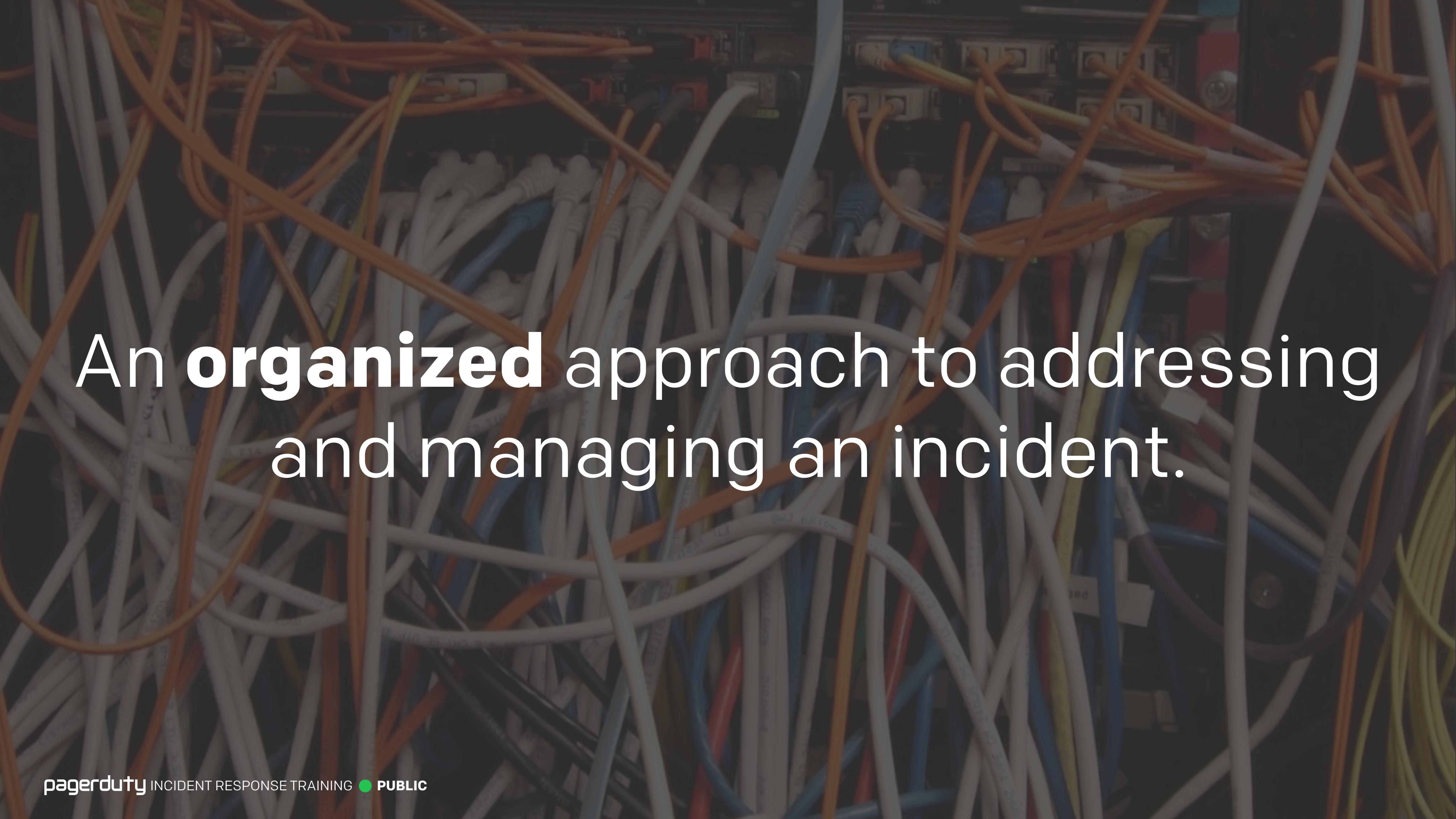




Learn how to effectively manage incidents within your organization.



Replace chaos with calm.



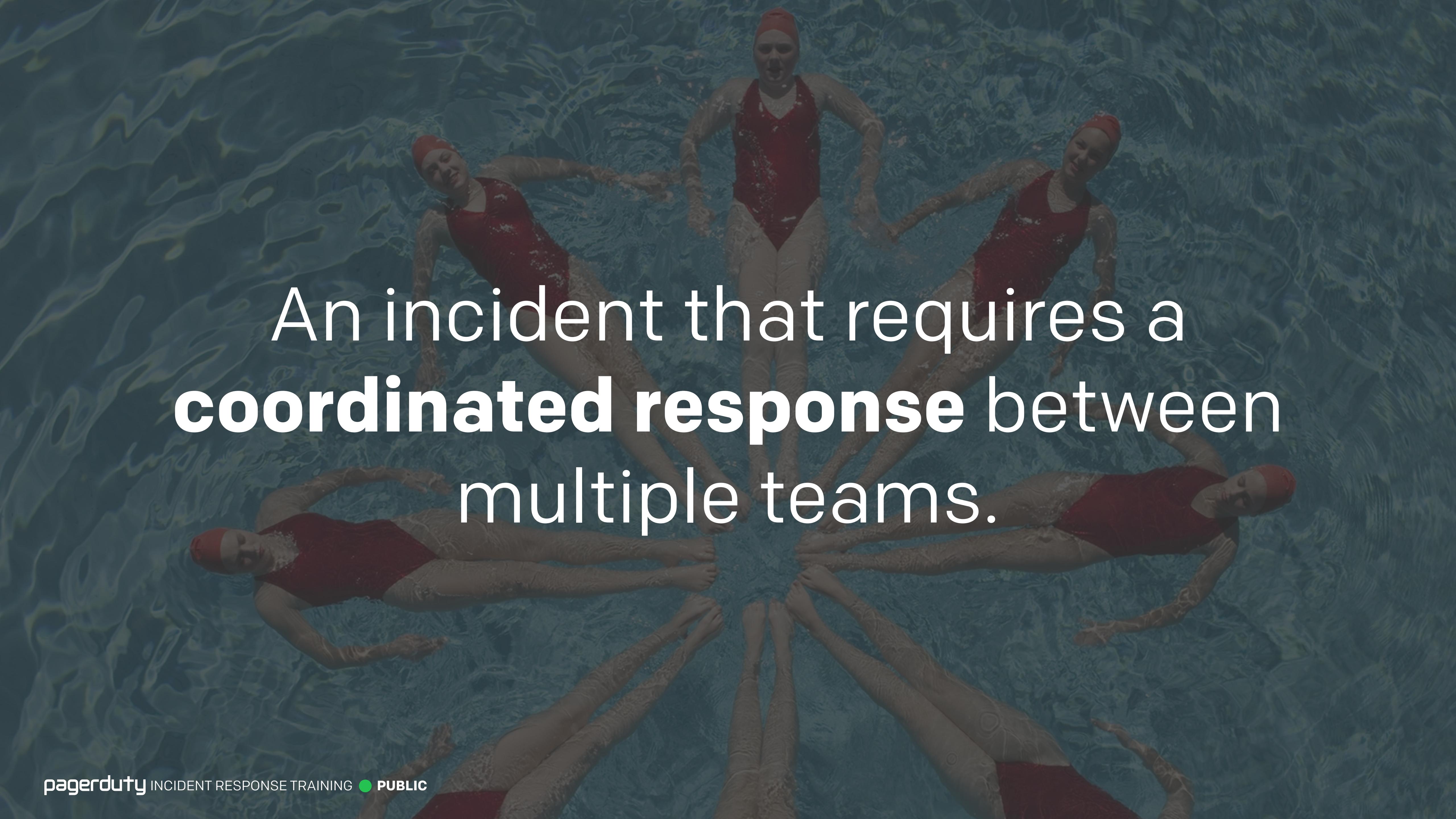
An organized approach to addressing
and managing an incident.

A firefighter wearing a helmet and turnout gear is spraying a powerful stream of water from a hose onto a large, intense fire. The fire is bright orange and yellow, with thick smoke billowing upwards. The firefighter's hose is held high, and the spray is directed at the base of the flames.

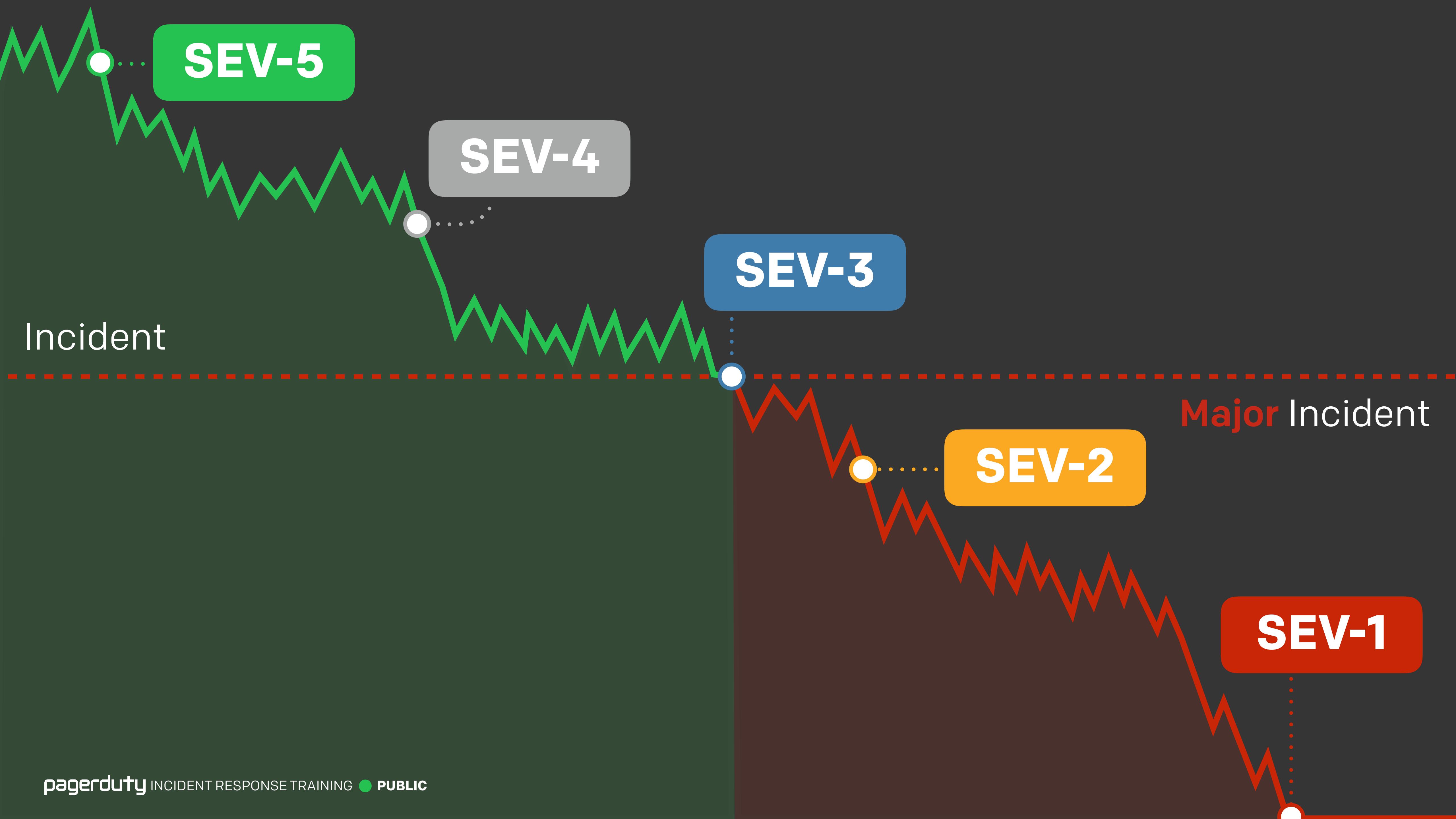
The goal is to handle the situation in
a way that **limits damage** and
reduces recovery time and costs.

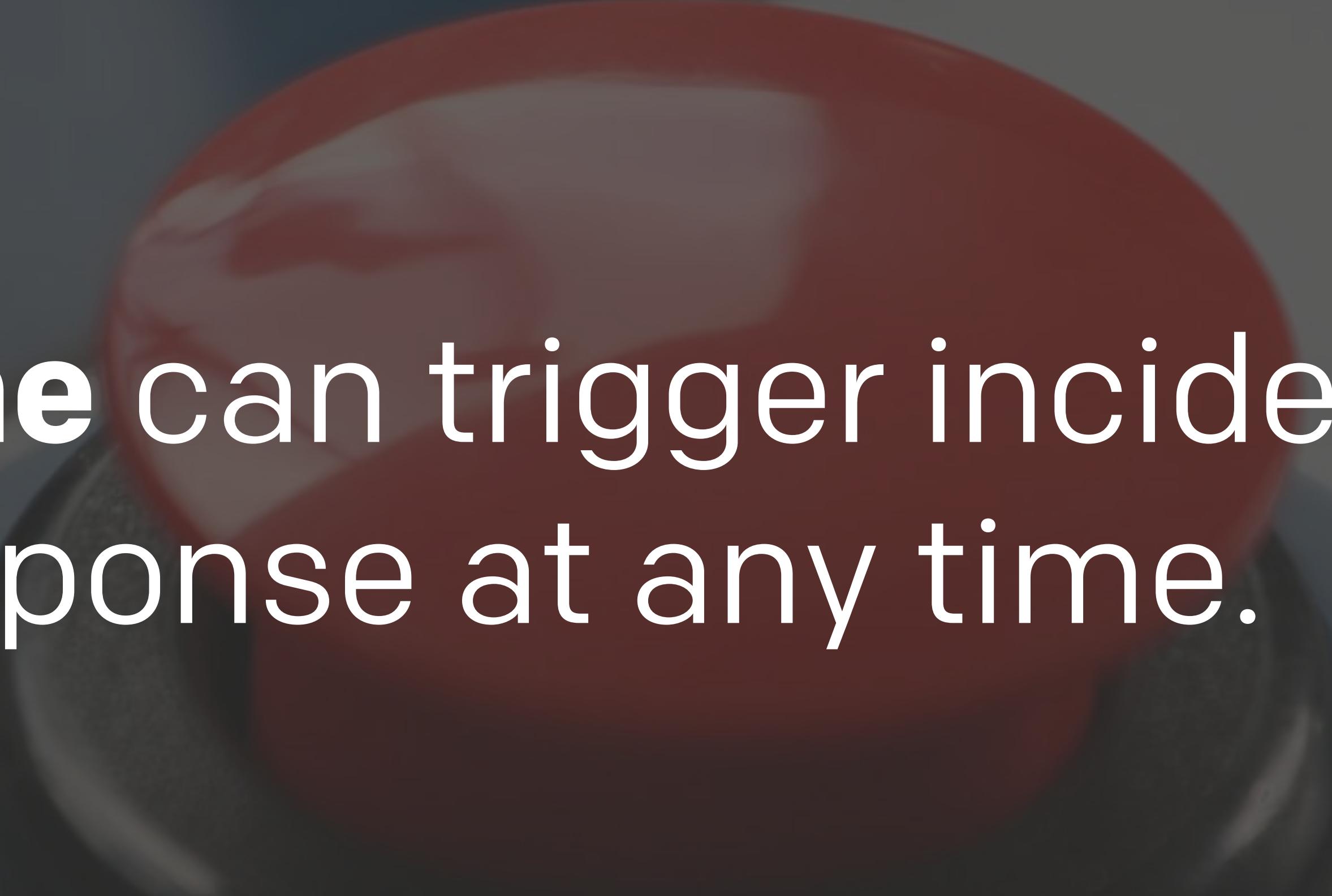
A dark, grainy photograph of a computer setup. In the background, a computer monitor displays a bright orange and yellow flame. In the foreground, a server rack unit is visible, with several cables and components attached. The overall atmosphere is one of a technical or industrial setting that has suffered a severe failure.

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

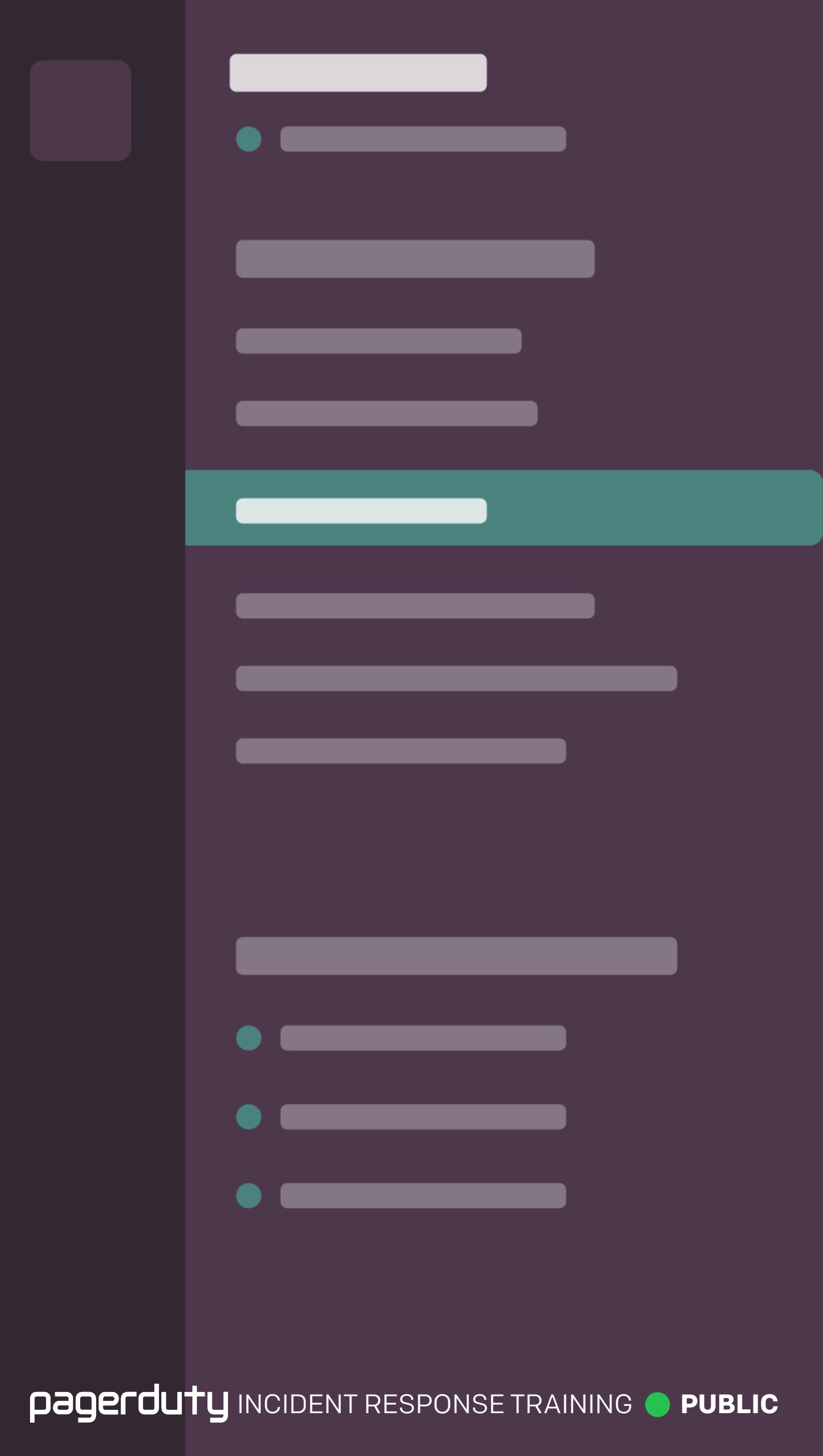


An incident that requires a
coordinated response between
multiple teams.





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.

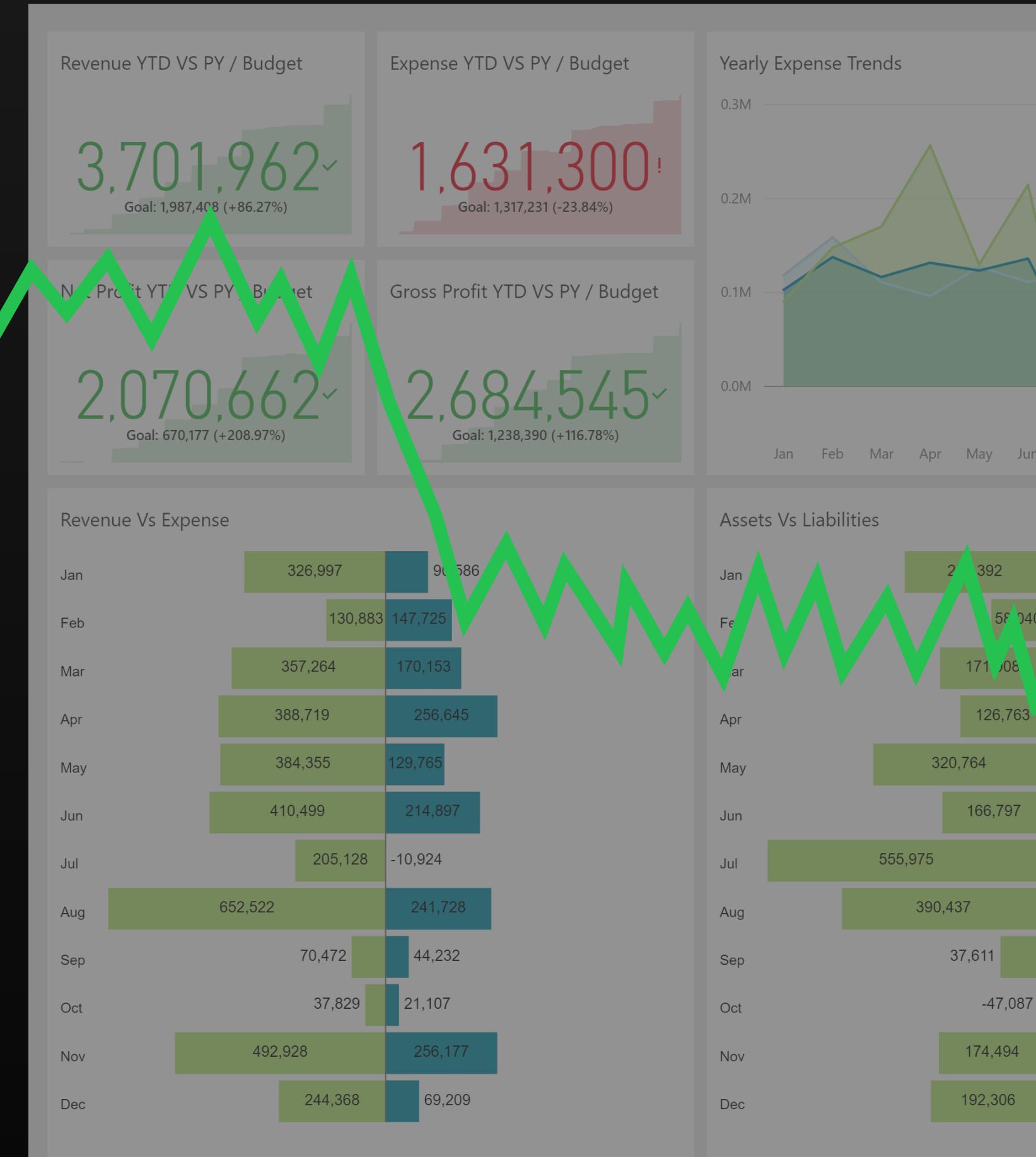
ℹ️ Use [!ic responders](#) to see who the team responders are.

pd Incident triggered: <https://example.pagerduty.com/incident/PD5I34R>



!ic page

PEACETIME



News has been shut down to prevent damage

this Stop error screen, appears again, follow

your software is properly installed. Your hardware or software manufacturer

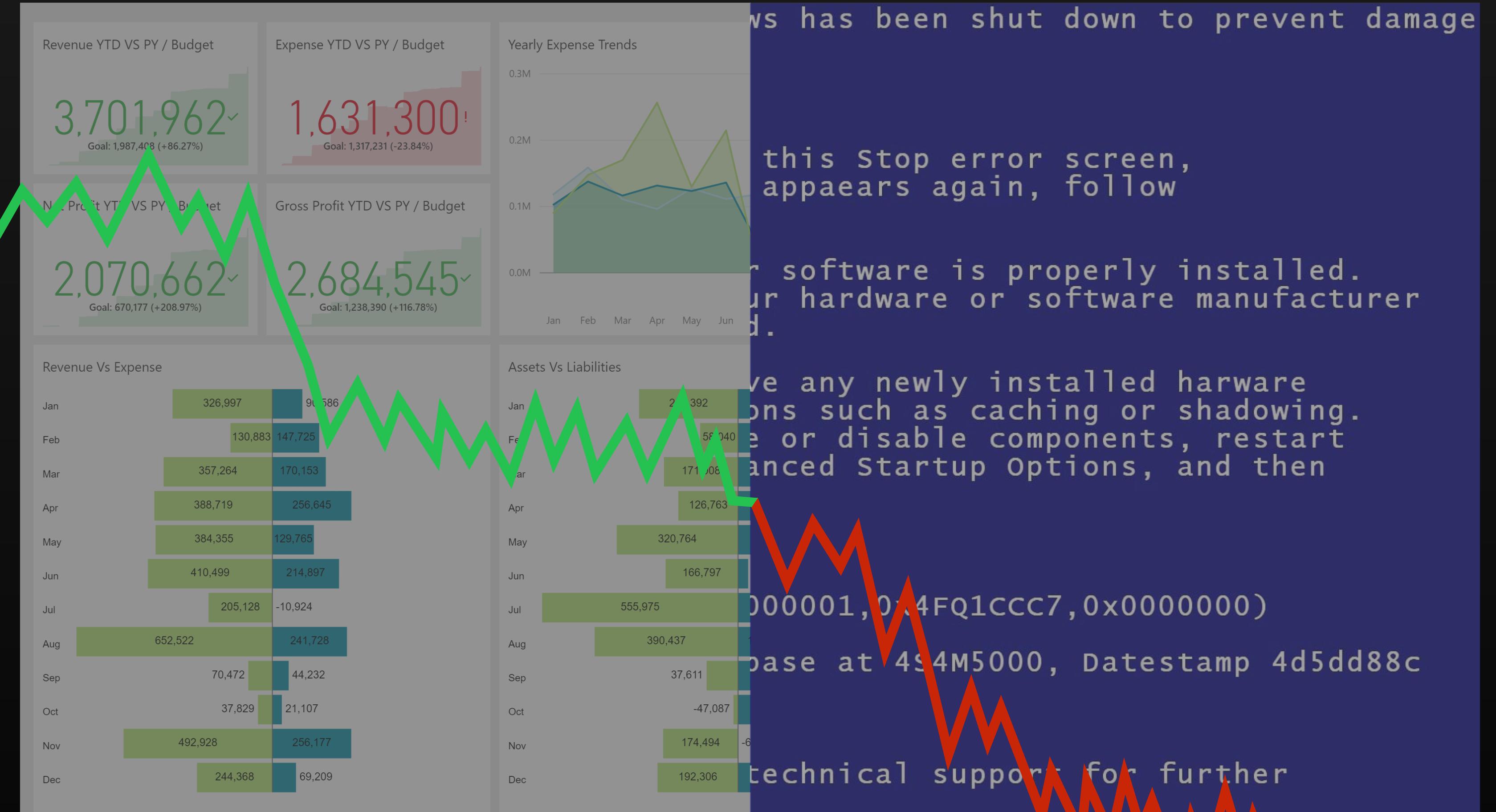
any newly installed hardware or software such as caching or shadowing. Disable or disable components, restart Enhanced Startup Options, and then

000001,0x4FQ1CCC7,0x00000000)
base at 4S4M5000, Datestamp 4d5dd88c

technical support for further

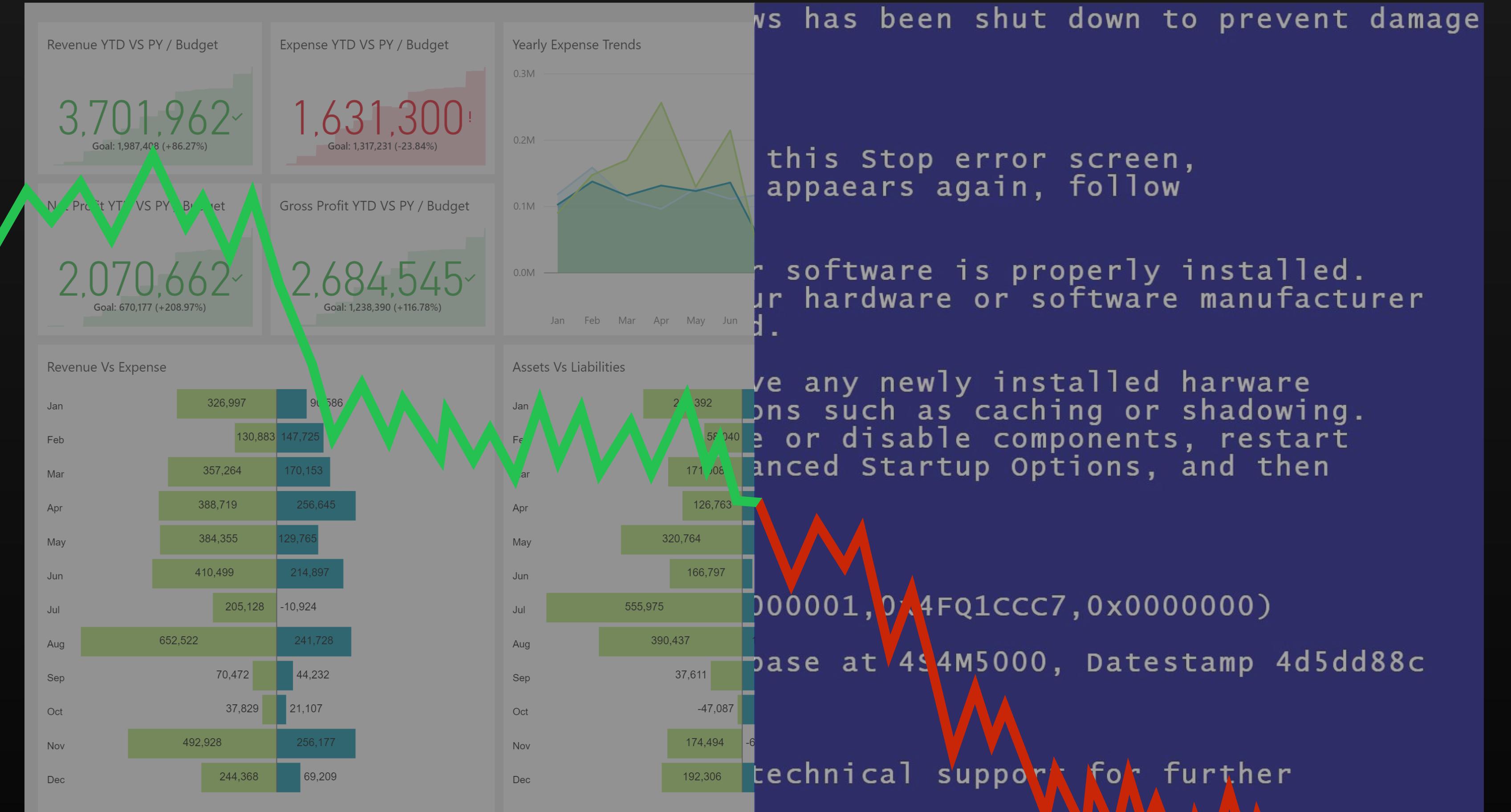
WARTIME

NORMAL



EMERGENCY

OK



News has been shut down to prevent damage

this Stop error screen, appears again, follow

your software is properly installed. Your hardware or software manufacturer

any newly installed hardware or software such as caching or shadowing. Disable or disable components, restart Enhanced Startup Options, and then

000001,0x4FQ1CCC7,0x0000000)
base at 4S4M5000, Datestamp 4d5dd88c

technical support for further

NOT OK

A dramatic scene of a wildfire. In the upper left, a helicopter drops a massive column of water onto the flames. In the lower right, several firefighters in full protective gear stand ready. The fire is intense, with bright orange and yellow flames and thick smoke filling the background.

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 (**AIIIMS**)



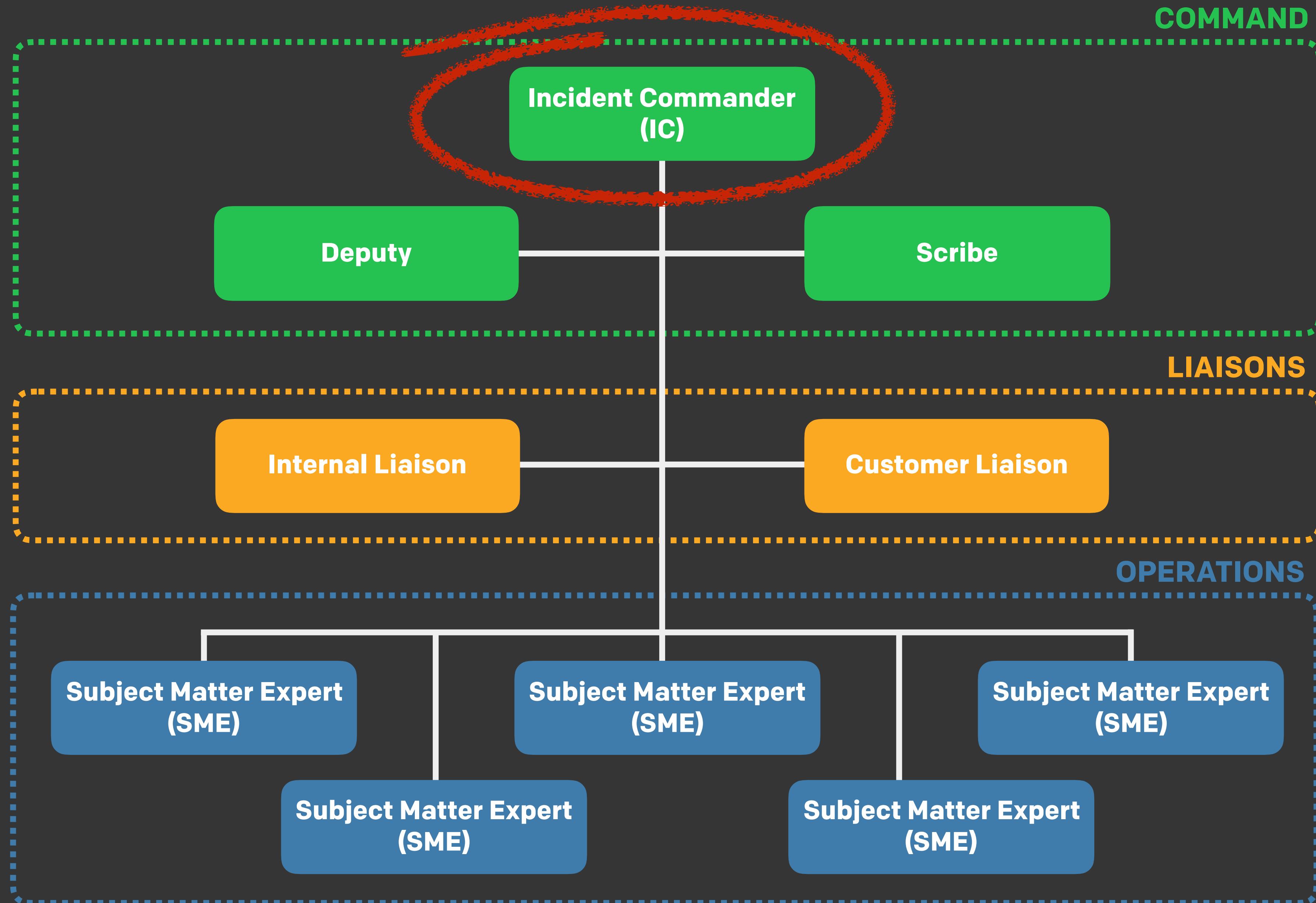
Gold-Silver-Bronze Command Structure (**GSB**)



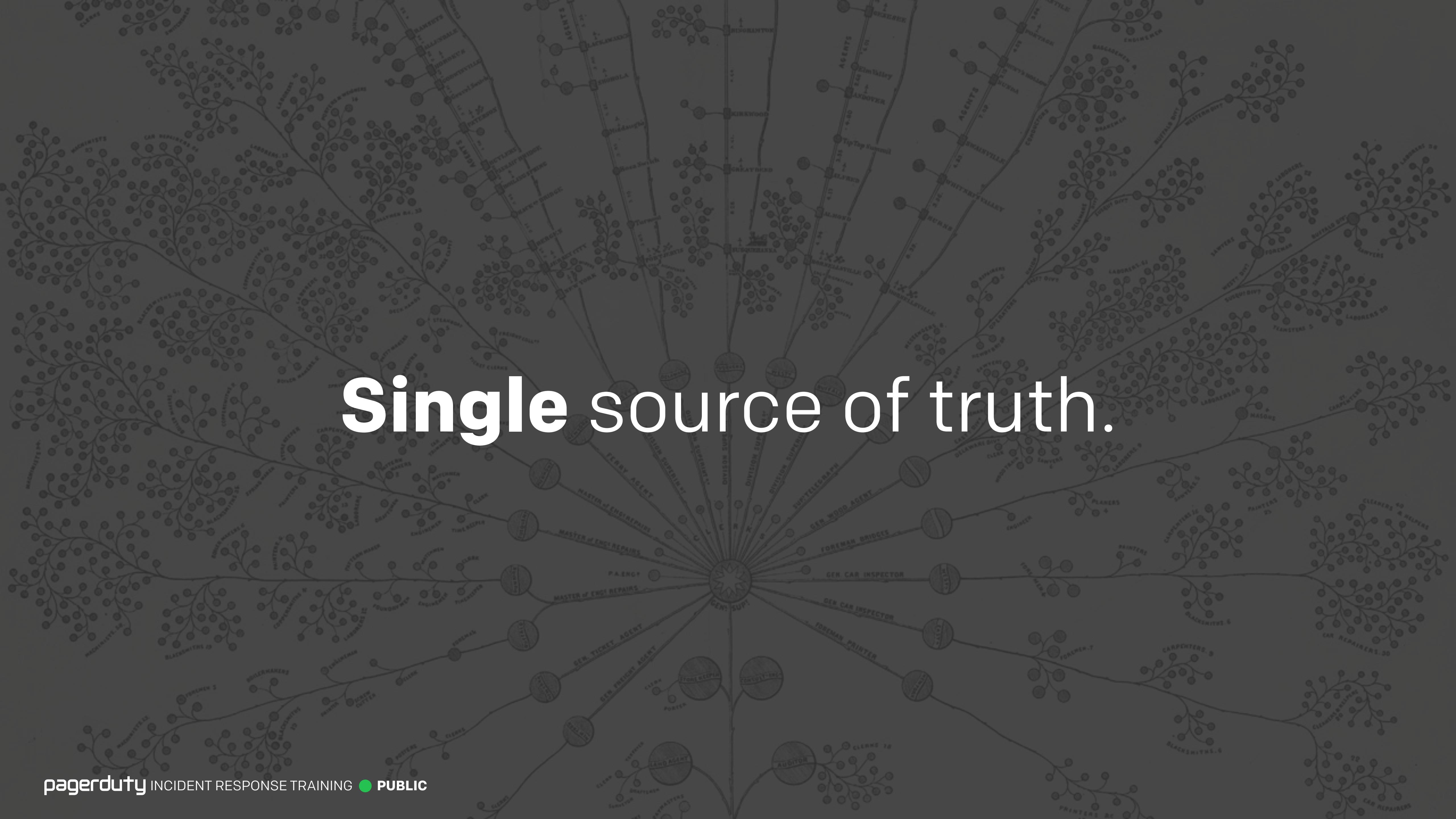
Incident Command System (**ICS**)



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



Incident Commander



Single source of truth.



Becomes the **highest authority**.

A young boy with glasses and a cap sits in a director's chair, shouting into a megaphone labeled "DIRECTOR".

Yes, they even outrank the CEO.

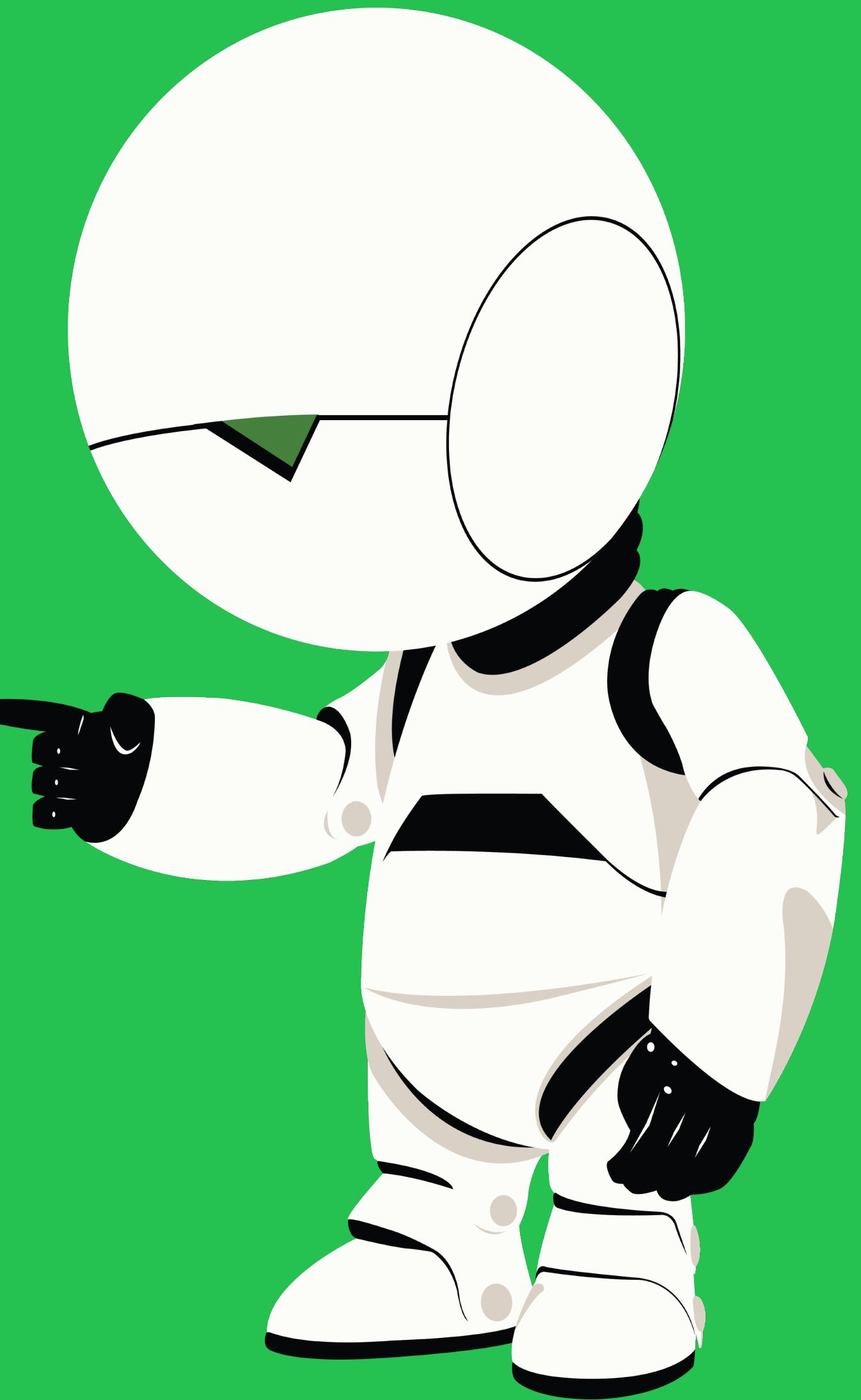
Make sure your CEO knows this in advance!



Not a resolver.
Coordinates and delegates.



DON'T
PANIC





I'm Rich.

I'm the Incident Commander.



Introduce yourself.



INCIDENT
COMMANDER

Say “**Incident Commander**”.



Good communication is essential.



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

KEY TAKEAWAY

Clear is better than concise.



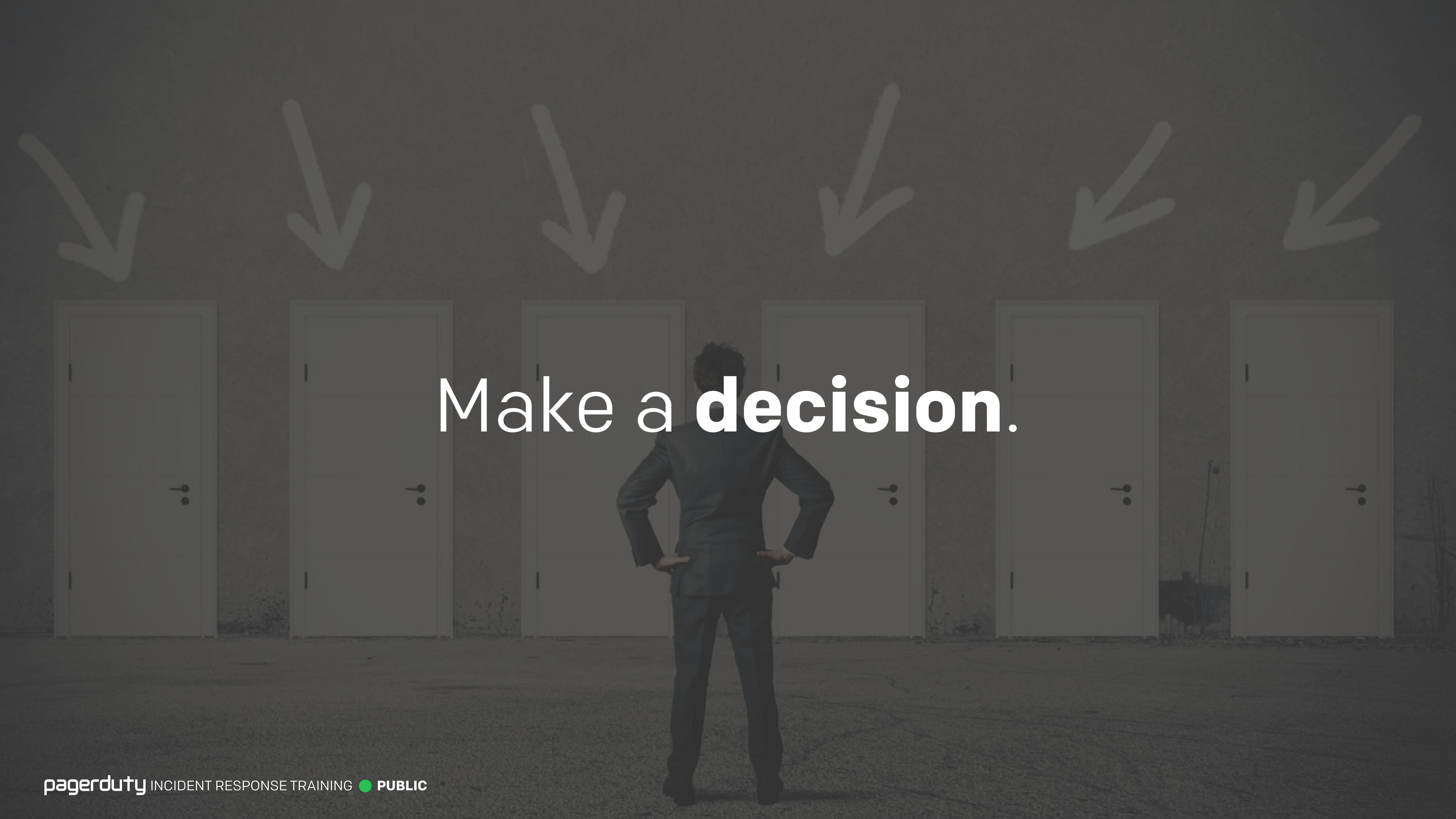
What's wrong?



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.

“Are there any **strong** objections?”



DON'T DO THIS

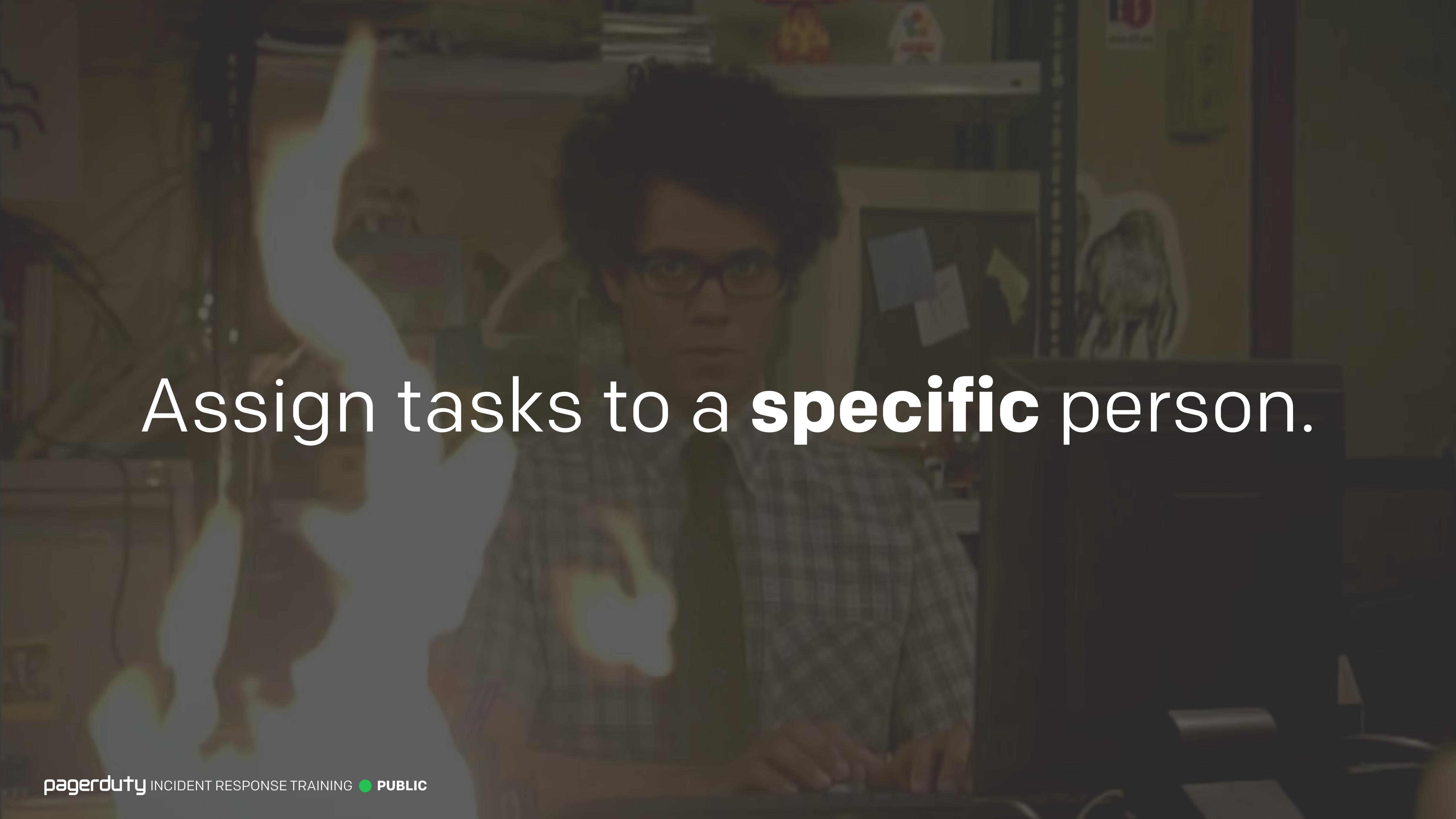
“Can someone...”



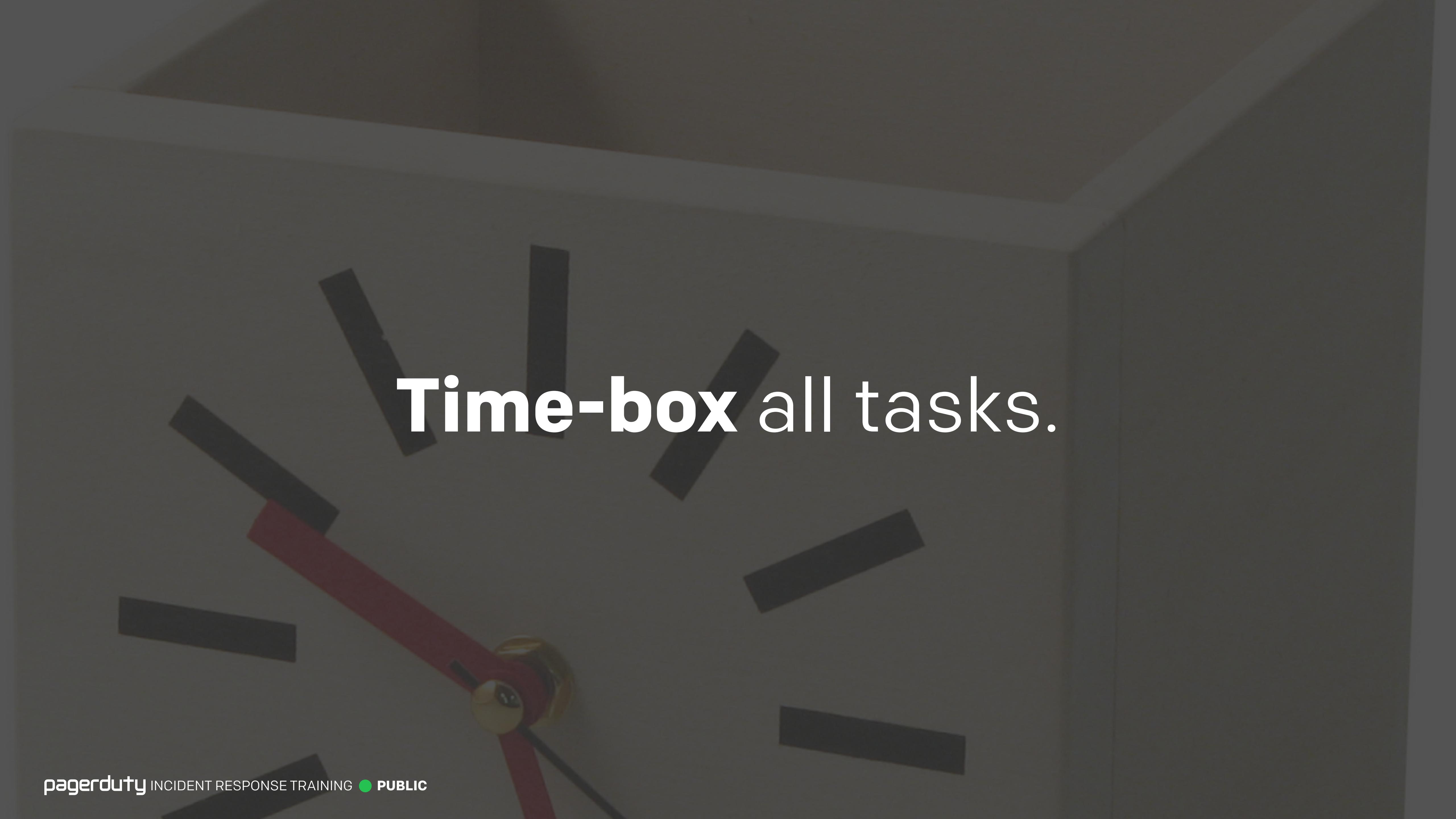
Eric, I'd like you to investigate the increased latency, try to find the cause. I'll come back to you in 5 minutes. Understood?

Understood.



A man with dark hair and glasses, wearing a light-colored button-down shirt, is seated at a desk in an office environment. He is looking directly at a computer monitor which displays a dark, indistinct interface. The background shows shelves with books and various office supplies.

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?



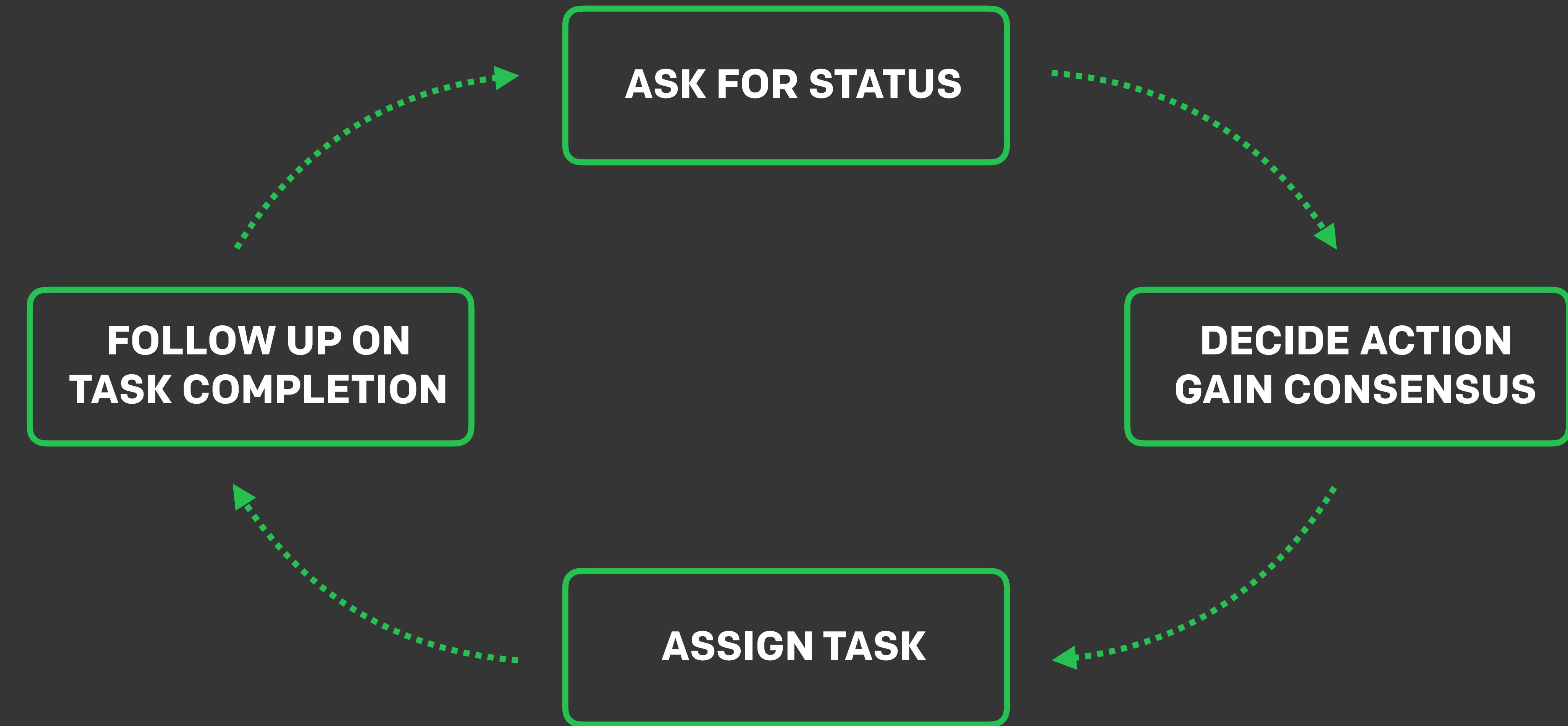
How much time do you need?

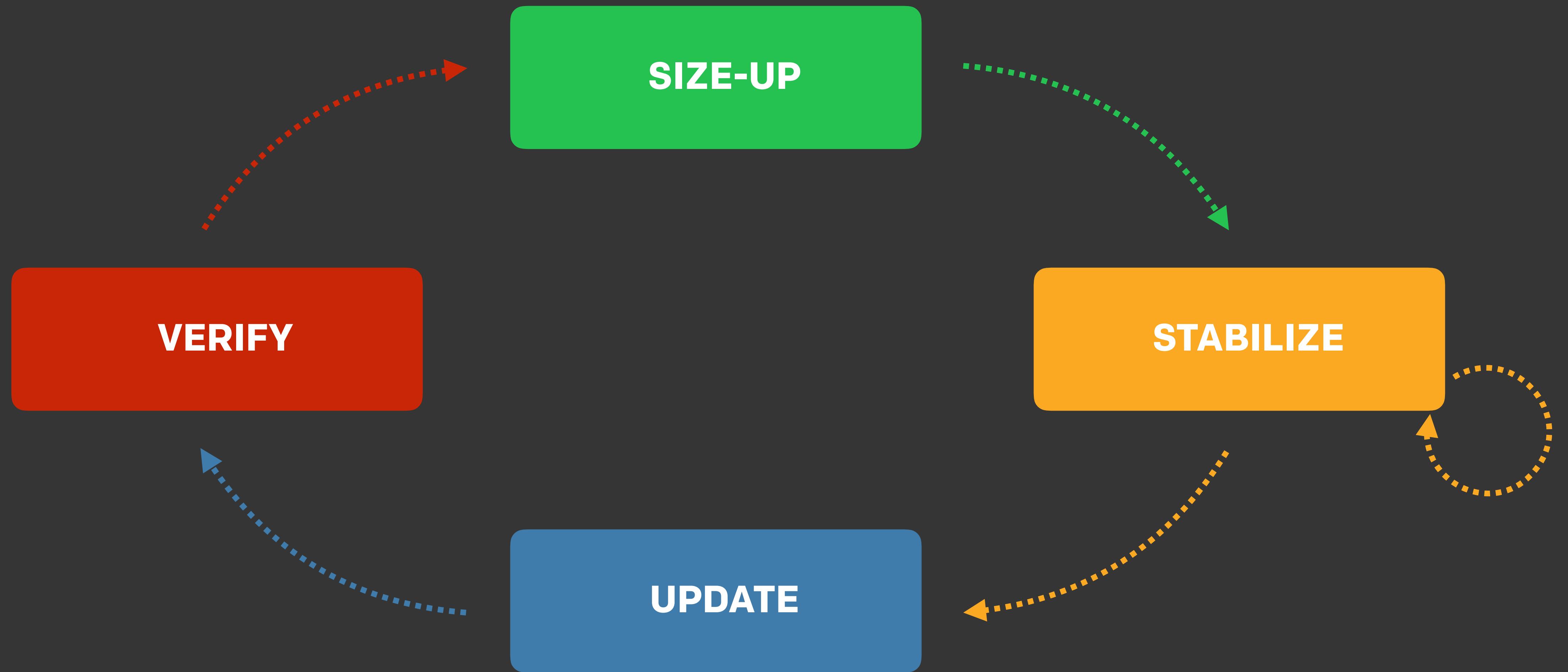


20 minutes should be enough.



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







“Ignore the IC, do what I say!”



Do you wish to take command?

...



A man with short brown hair and glasses, wearing a light blue shirt and a patterned tie, is looking down at a laptop screen. He is holding a white mug with a blue logo in his left hand. The background is dark and out of focus.

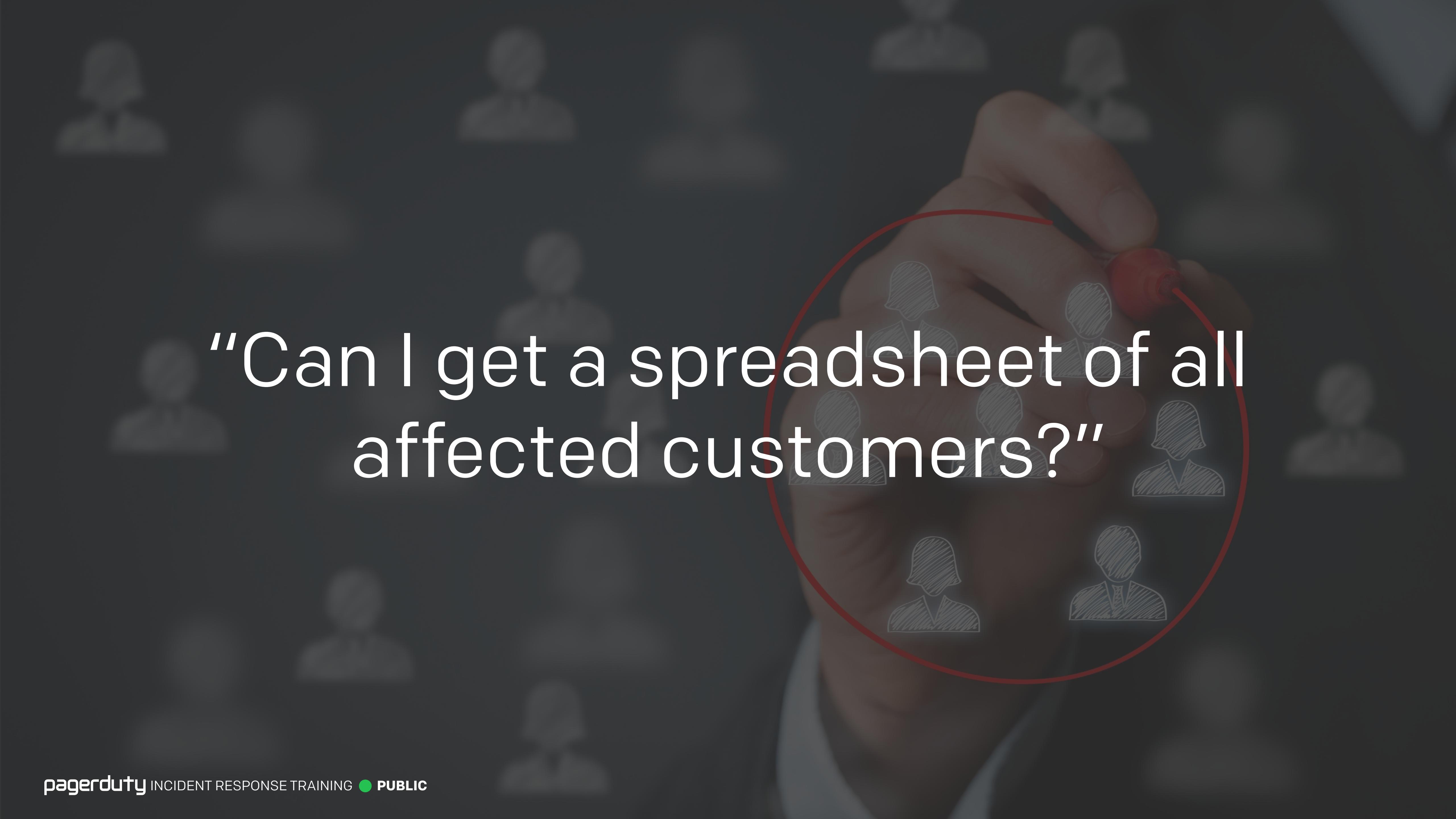
Executive Swoop

A dark, out-of-focus background image of a person wearing a dark suit jacket, a white shirt, and a blue tie with white polka dots. Their hands are clasped in front of them. The lighting is dramatic, with strong highlights on the tie and hands.

“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.



Notify stakeholders.

A close-up photograph of a person's face, showing them laughing exuberantly. Their hands are clasped together over their eyes and nose, with fingers spread. The person has short brown hair and is wearing a red and white striped shirt.

The belligerent responder.



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



Do responders get tired?

A photograph showing two people's hands in the foreground. A person with a yellow sleeve is handing a thick, green book to another person whose arm is extended from the right side of the frame. The background is a blurred outdoor setting with trees and a building.

Handovers are encouraged.

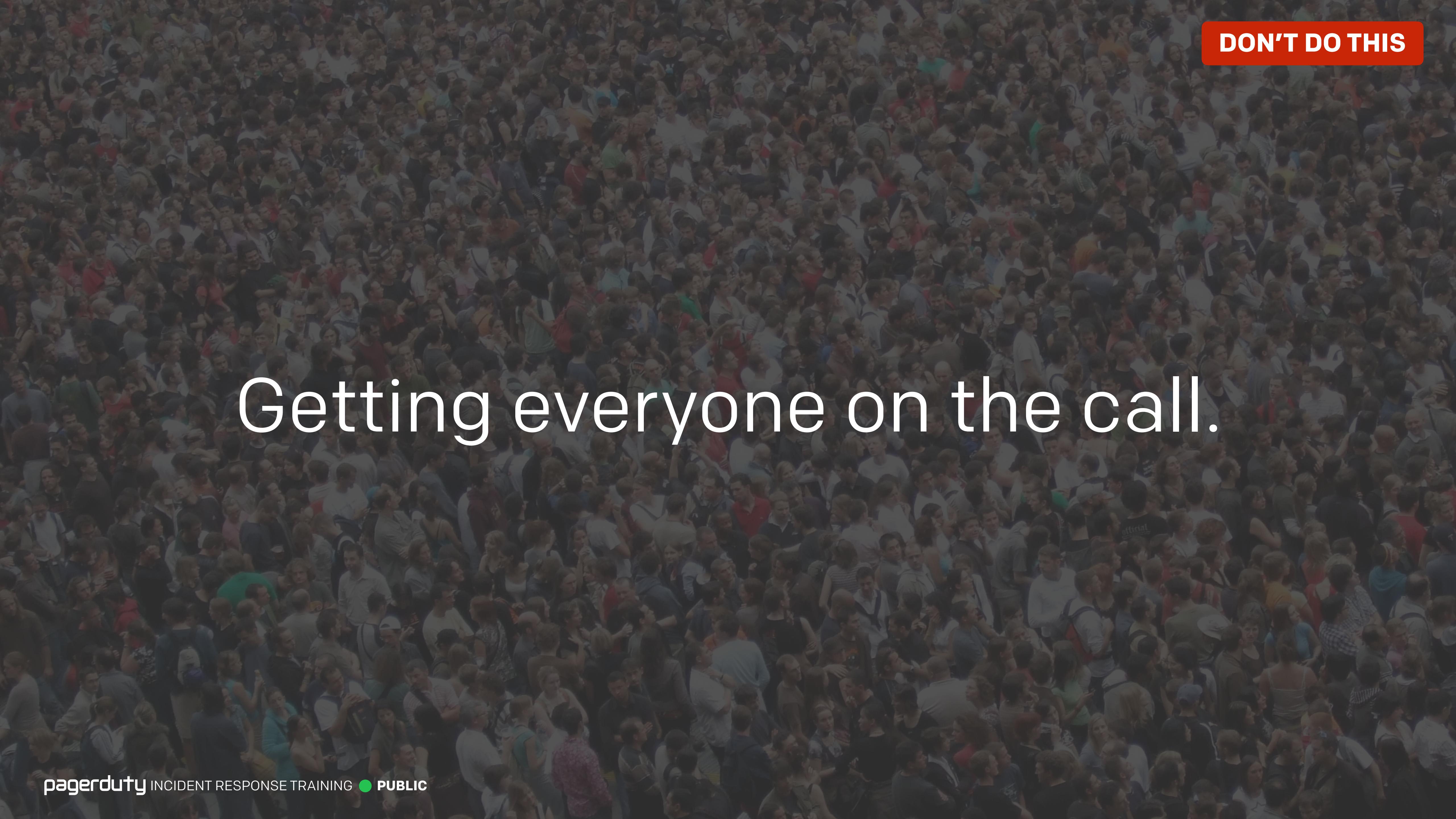


Everyone on the call, be advised
I'm handing over command to
Eric.



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

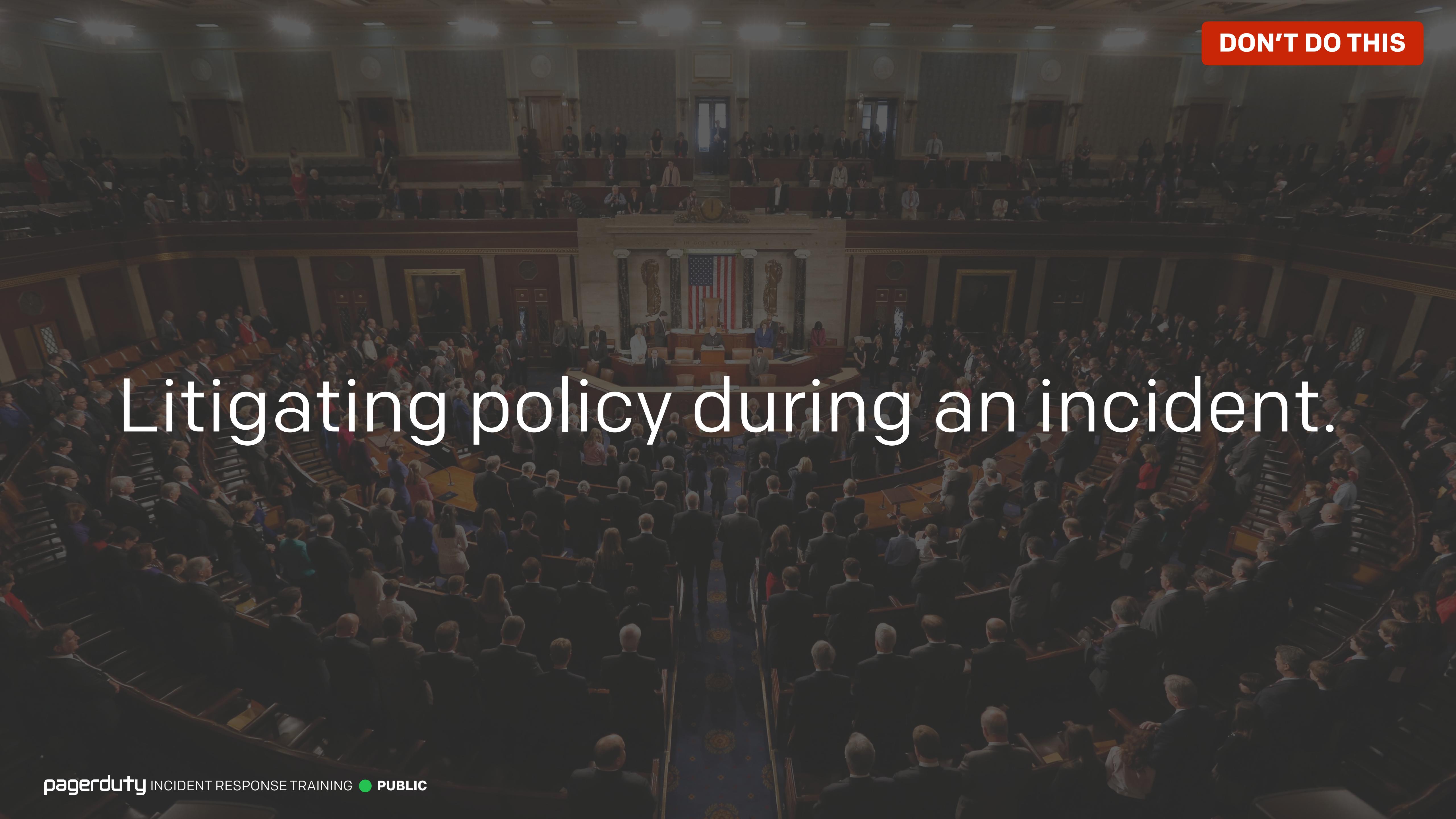
Requiring deeply technical ICs.

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



Don't neglect the post-mortem.



Create the post-mortem.

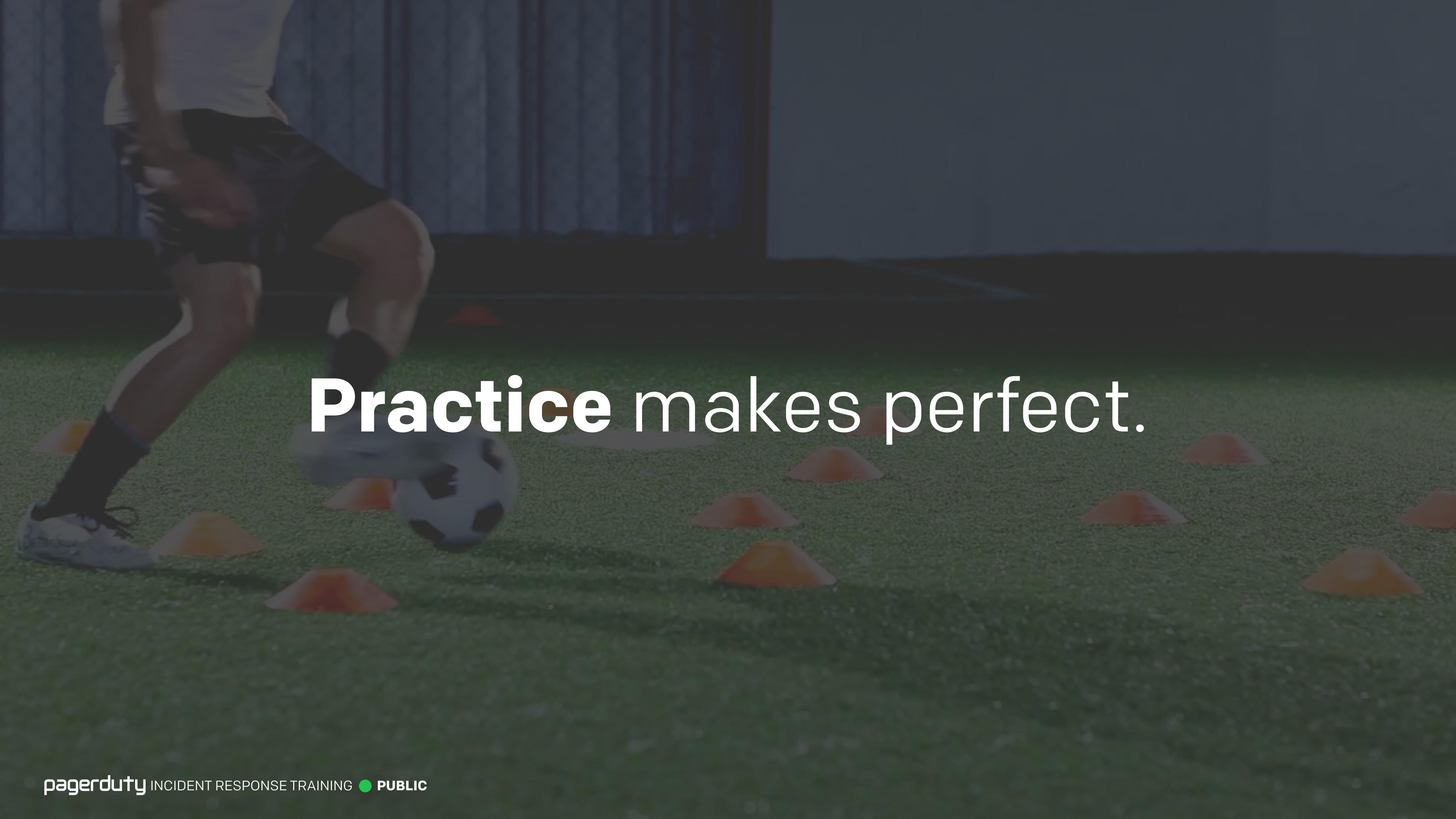


Pick an owner.



Blameless.

Review the process too!

A person is practicing soccer drills on a grassy field. They are wearing a light blue shirt, dark shorts, and socks with a red and white stripe. They are kicking a black and white soccer ball between a series of orange traffic cones arranged in a zigzag pattern. The background shows a building with vertical siding and a clear sky.

Practice makes perfect.



<https://responsepagerduty.com>



REPO 105 517

[Home](#)[Getting Started](#)[On-Call](#)[Being On-Call](#)[Who's On-Call?](#)[Alerting Principles](#)[Before an Incident](#)[What is an Incident?](#)[Severity Levels](#)[Different Roles](#)[Call Etiquette](#)[Complex Incidents](#)[During an Incident](#)

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 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 tasks should be delegated.

- 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-aufstaucht-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*fBPpHzol5M-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/2016/03/635944677511654874-1232941586_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/AAAAAAAABww/6PJpke00EFs/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/AAAAAAAABzw/6hH-latP7rU/s1600/african%2Bamerican%2Bbaton%2Bpass%2Brelay%2Bracers%2Bgenerations%2Bcourtesy%2Bof%2BTTheo%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_%282819599074868%29.jpg

Technical: <https://elkjjerkyforthesoul.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 UNIVERSITY