

## Incident Command System (ICS101)

The Incident Command System (ICS) was developed after devastating wildfires in Southern California in 1970. Thousands of firefighters responded but found it difficult to work together. They knew how to fight fires individually but lacked a common framework to work as a larger group.

ICS is a framework that is meant to provide minimum recommendations for effective incident response in emergency situations. As a result, it has been modified for the needs of different localities, and it is now used globally in different ways.

### PagerDuty Definitions

**Incident** - An incident is any unplanned disruption or event that is actively affecting customer ability to use the product.

**Incident response** - approach to addressing and managing an incident.

**Major Incident** - A major incident requires a coordinated response between multiple teams.

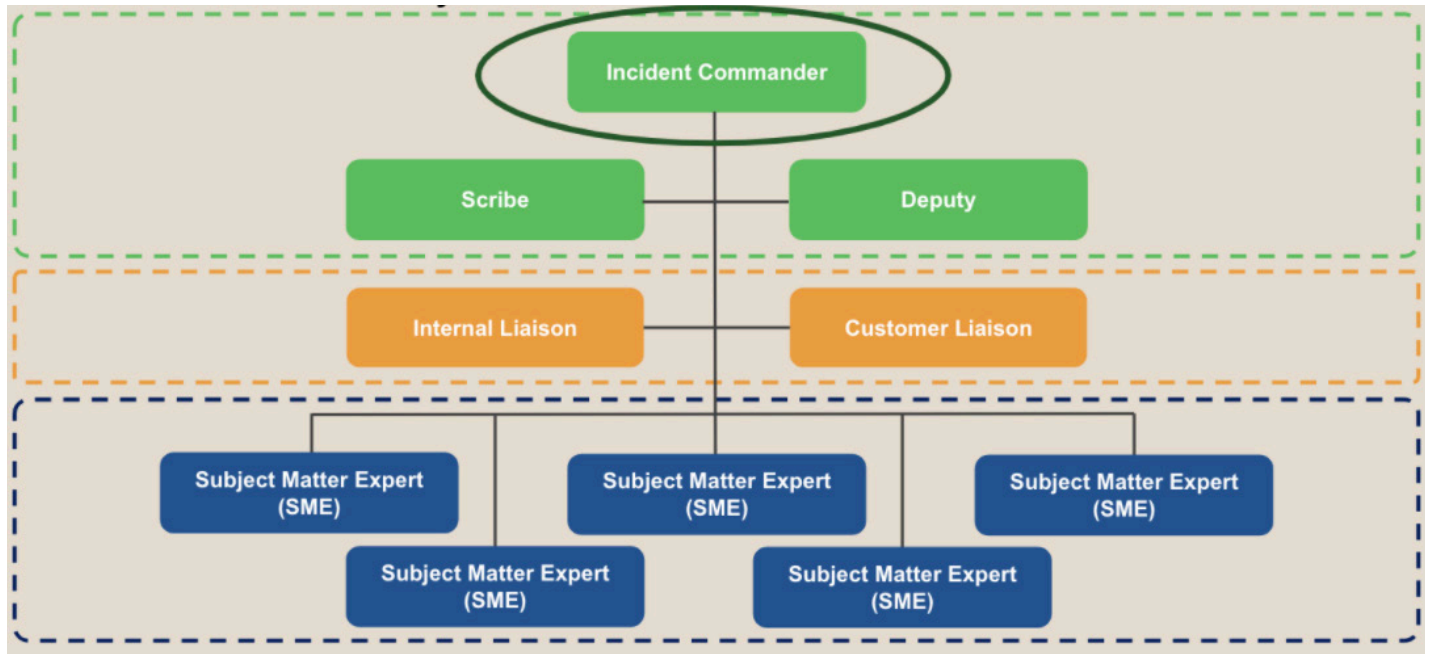
### What are *your* organization's definitions?

#### The Four 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
- Mobilization and coordination required, typically cross-functional

#### The Four Commonalities of Minor Incidents

- Timing is a surprise: typically little to no warning
- Not urgent; can be handled during normal business hours
- Situation is a known failure with a fix
- Within the responsibilities of a small team



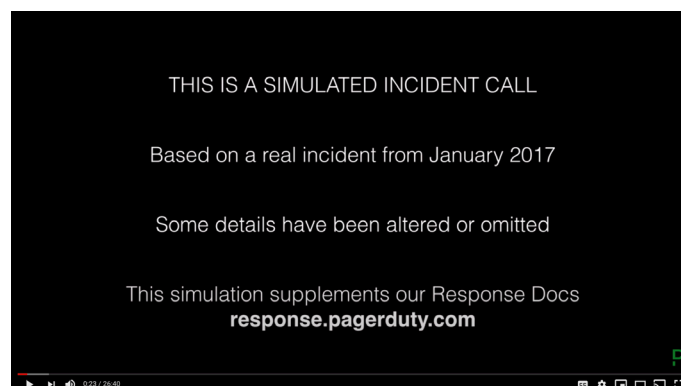
## Importance of Having an Incident Commander

- You must have one, and only one, person that is in command
- Single source of truth
- Responsible for coordinating and delegating, not resolving
- Keep things moving towards a decision

## Don't Neglect the Postmortem

- It is the last step of your Incident Response Process
- Blameless is key. If you name and shame people in a Postmortem, it demotivates everyone. Next time someone makes a mistake, they might not own up to it because they'll be afraid of getting shamed too. You want people to bring up problems because then you get to fix them quickly.

[Watch this: Simulated Incident Response Recording](#)



Open Source Guides & Framework  
[response.pagerduty.com](https://response.pagerduty.com) | [postmortems.pagerduty.com](https://postmortems.pagerduty.com)