

Varieties of Incident Response

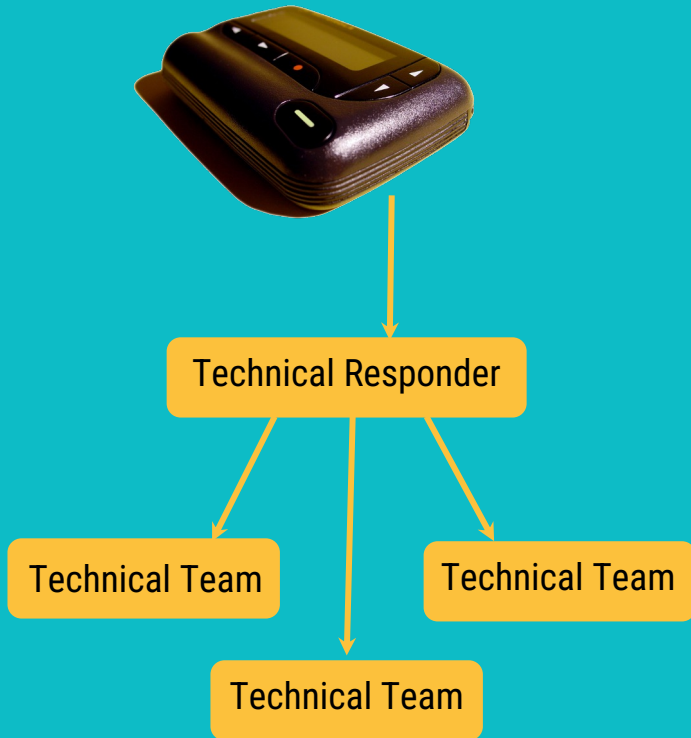
There's more to it than you might think!



Kurt Andersen
SRE Architect
Blameless.com
@drkurta



When the pager goes off...



The OODA Loop

Observe

Orient

Decide

Act

(repeat...)

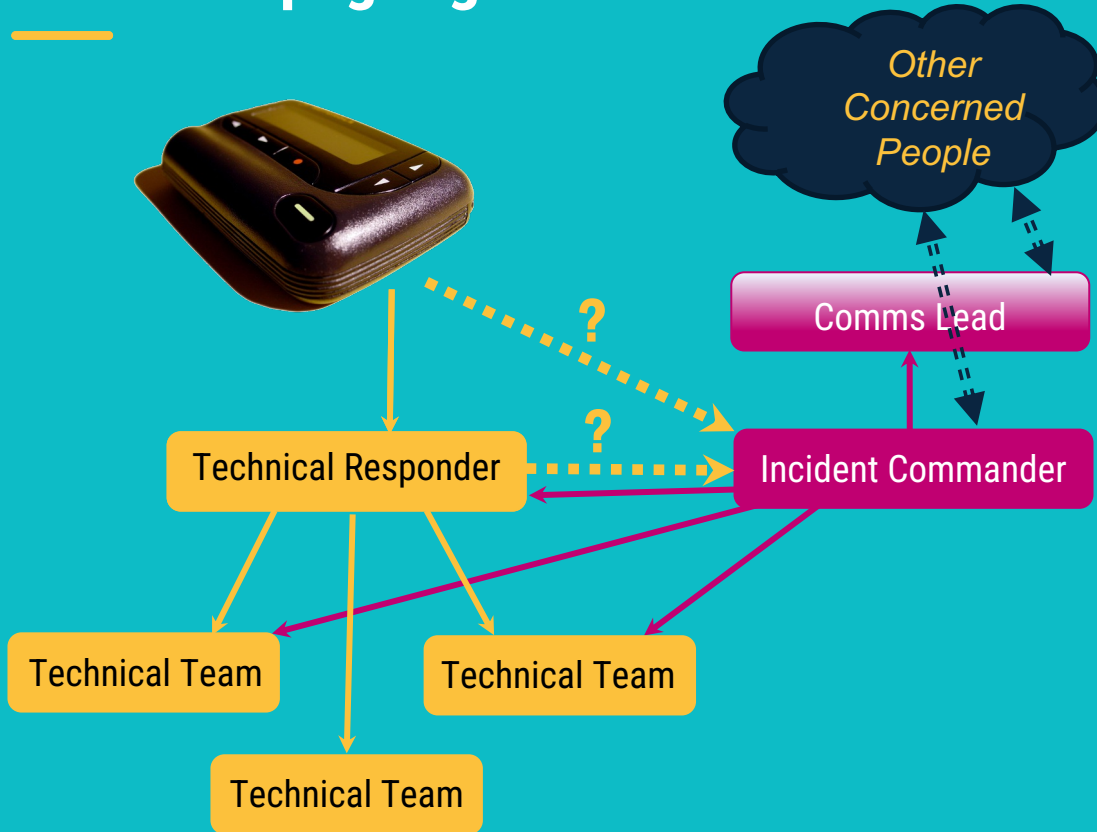
Diagnosis:

- Figure out what is happening
- Figure out what to do
- Figure out what *can* be done about it

Therapy:

- Take action to mitigate the issue
- Ensure that the action was effective

When the pager goes off...



Recruitment:

- Get the right people involved

Response Coordination:

- Who does what, when?

Communication:

- Outside of the response team

Response Task Categories

Technical

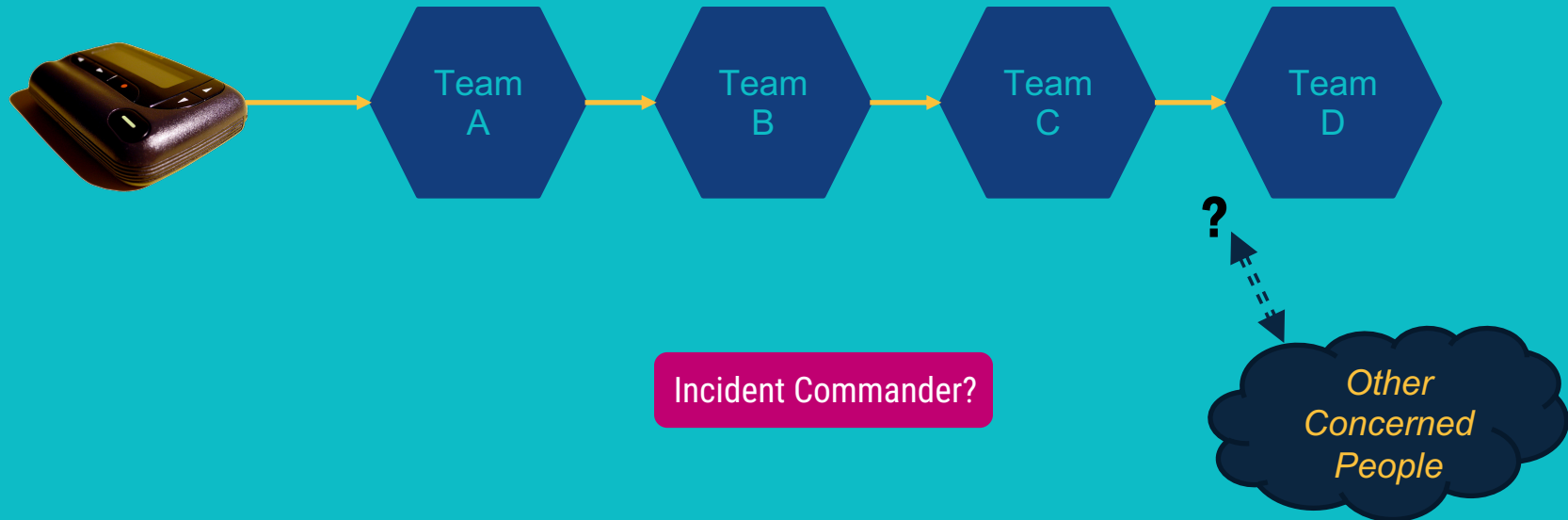
Diagnostic
Therapeutic

Logistical / Administrative

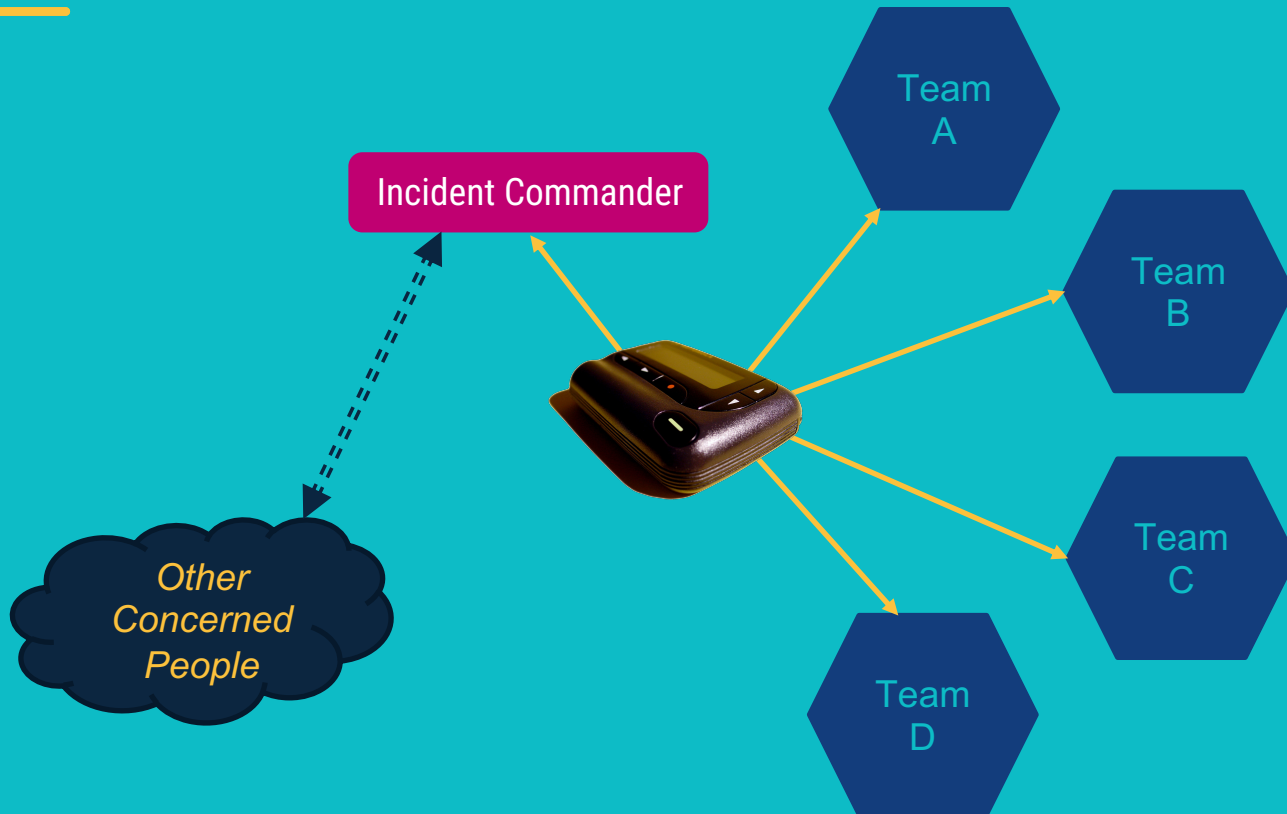
Recruiting
Communication

Shared Coordination

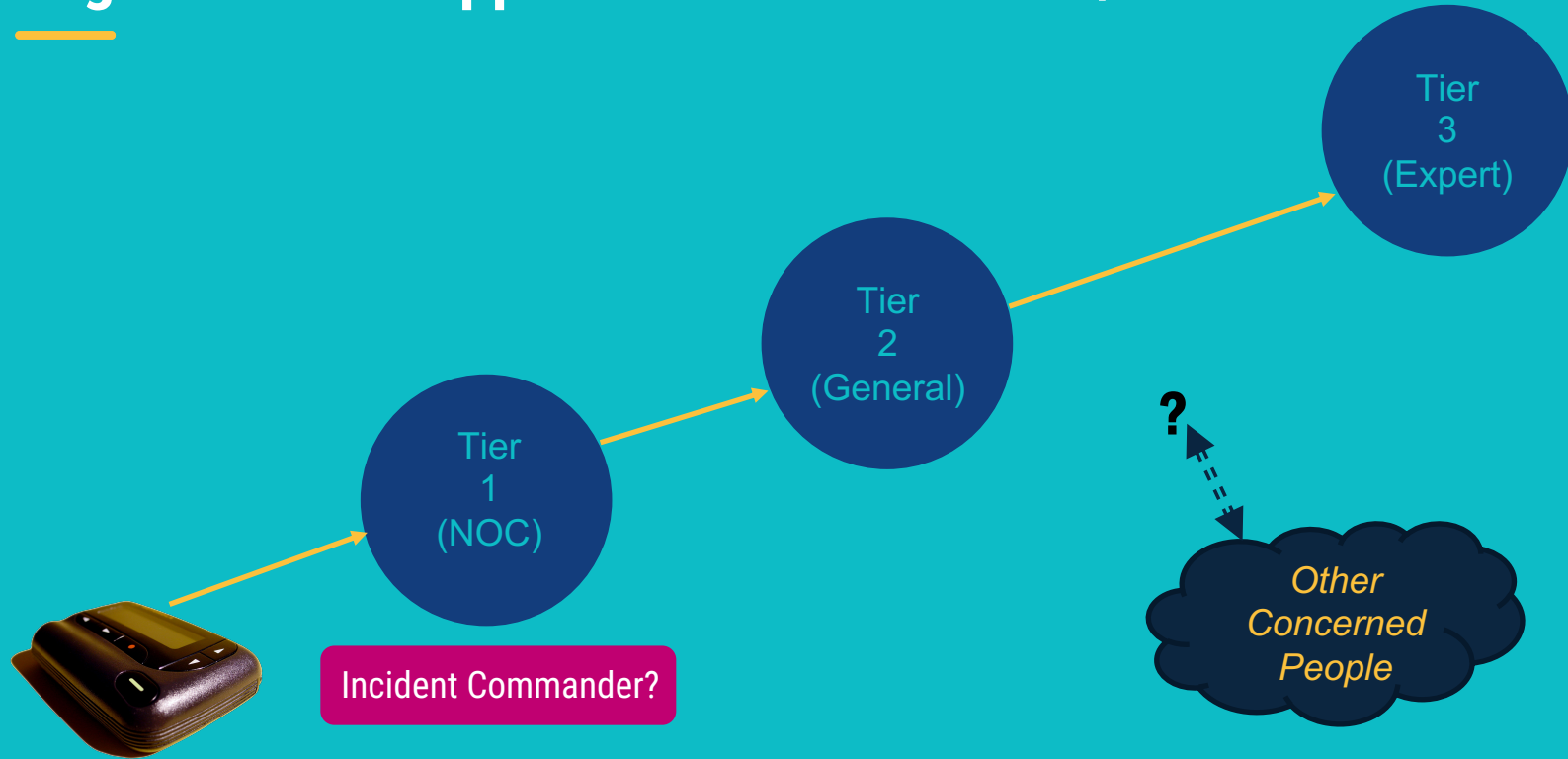
Organizational Approaches – “One at a Time”



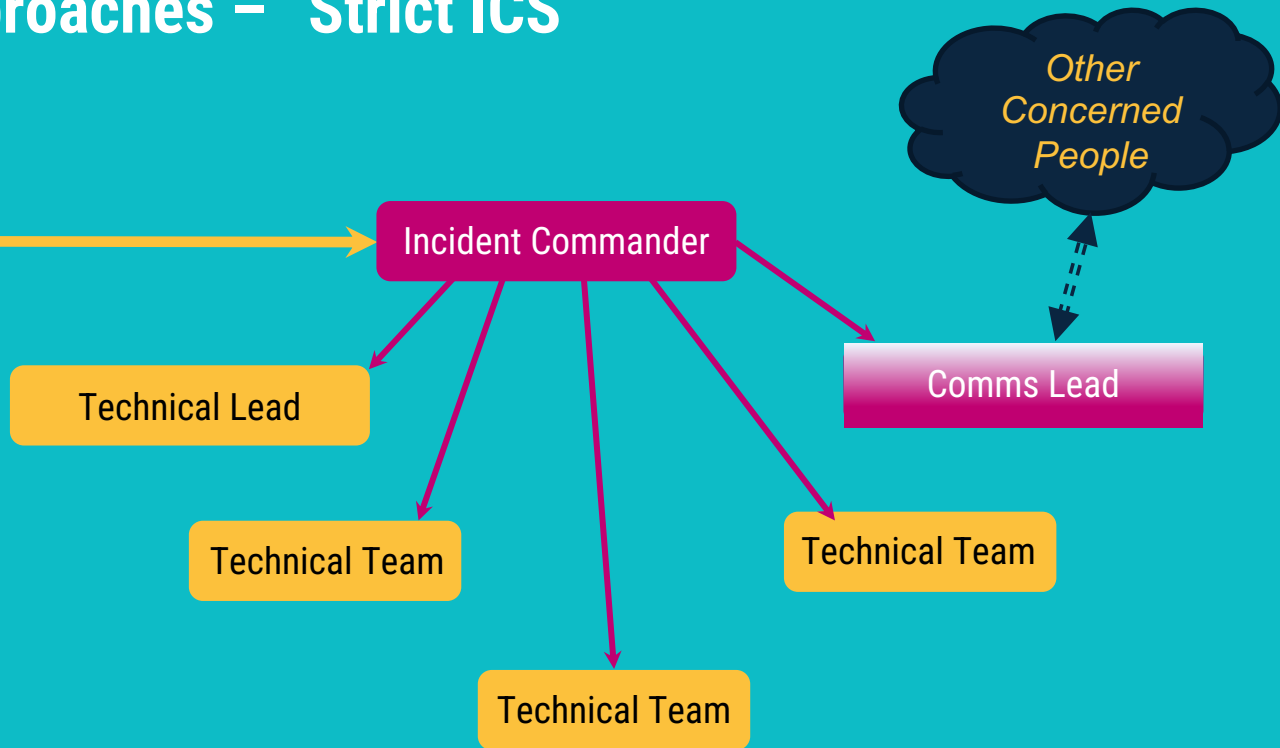
Organizational Approaches – “All Hands On Deck”



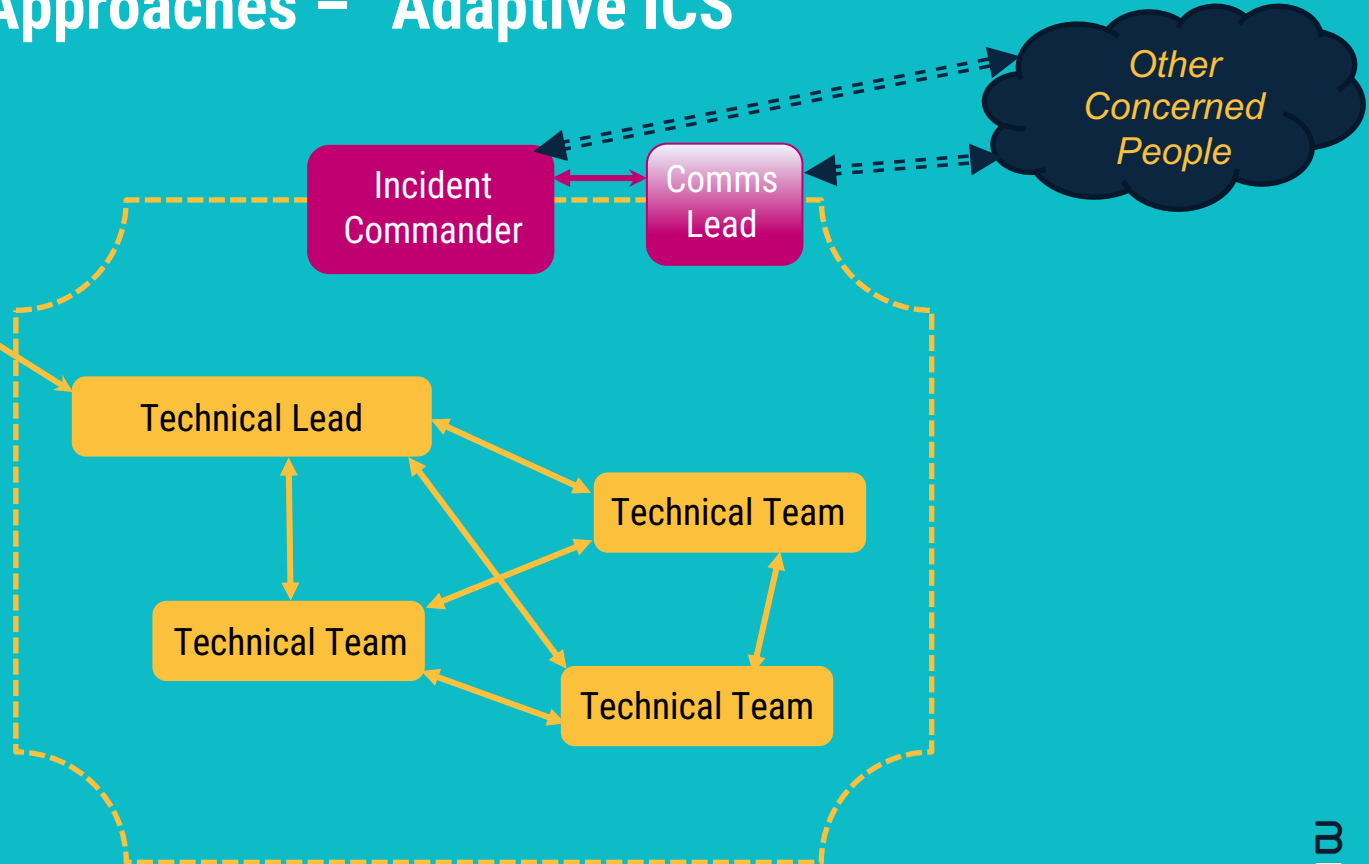
Organizational Approaches – “Escalation/Tiered”



Organizational Approaches – “Strict ICS”



Organizational Approaches – “Adaptive ICS”



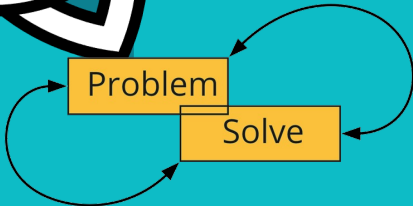
“The Response Trio”



Incident
Commander



Comms
Lead



Recap

The OODA Loop

Observe

Orient

Decide

Act

(repeat...)

Diagnosis:

- Figure out what is happening
- Figure out what to do
- Figure out what *can* be done about it

Therapy:

- Take action to mitigate the issue
- Ensure that the action was effective

Recruitment:

- Get the right people involved

Response Coordination:


- Who does what, when?

Communication:

- Outside of the response team

Organizational Models:

1. One at a time – pass the baton
2. All hands on deck
3. Escalation or tiered
4. Strict ICS
5. Adaptive ICS



Why is this
thing making
noise?

Suggestions for Further Reading

- Maguire, Laura. *Managing the Hidden Costs of Coordination*. <https://queue.acm.org/detail.cfm?id=3380779>
- Klein, Gary; et al. *Common Ground and Coordination in Joint Activity*. <http://dx.doi.org/10.1002/0471739448.ch6>
- Dekker, Sidney. *Why Do Things Go Right*. <https://safetydifferently.com/why-do-things-go-right/>

Questions? kurt@blameless.com or @drkurta on Twitter

