

Mastering Outages with Incident Command for DevOps: Learning from the Fire Department

Brent Chapman

DevOps Enterprise Summit

24 October 2018

Brent@GreatCircle.com

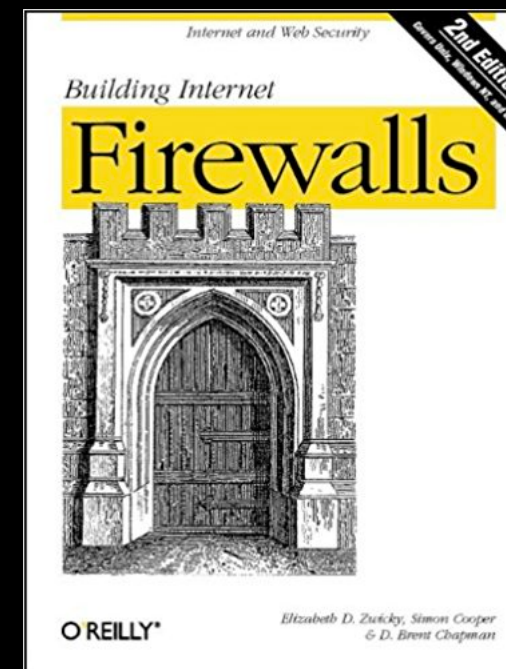
@brent_chapman

These Slides
j.mp/grtcrc1-181024



Great Circle

Majordomo

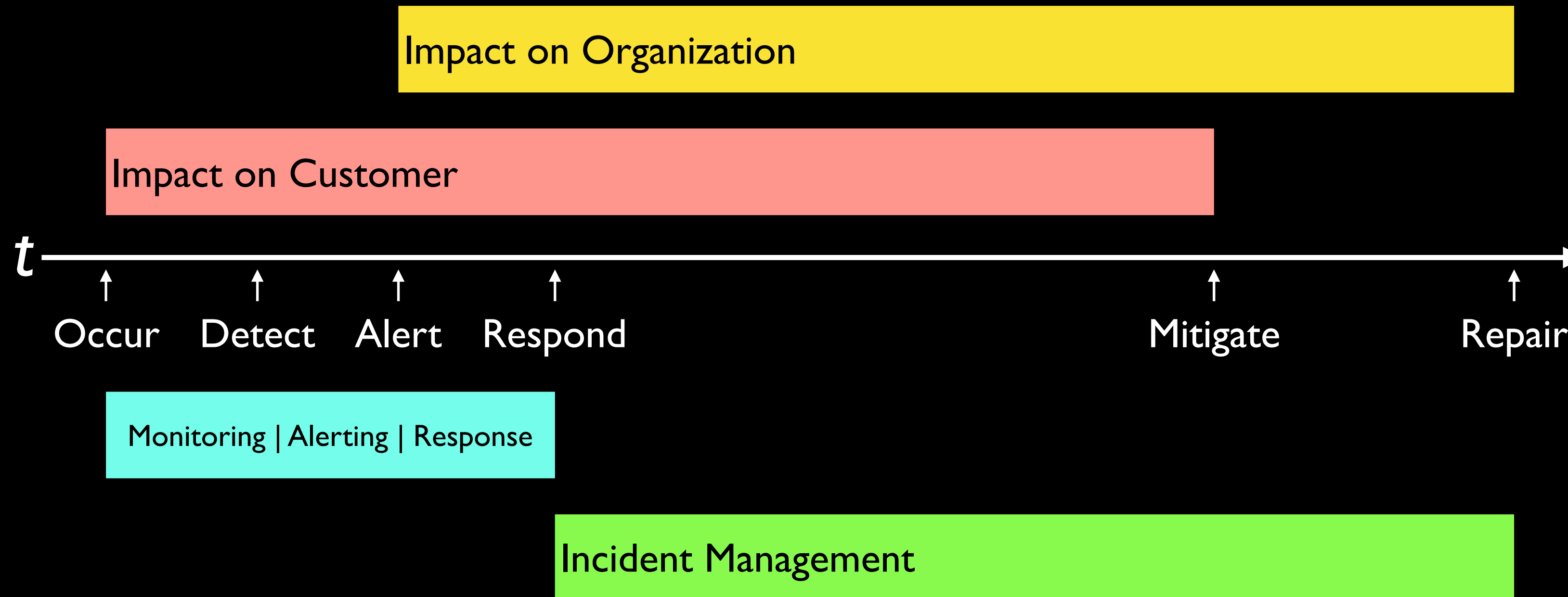


Great Circle

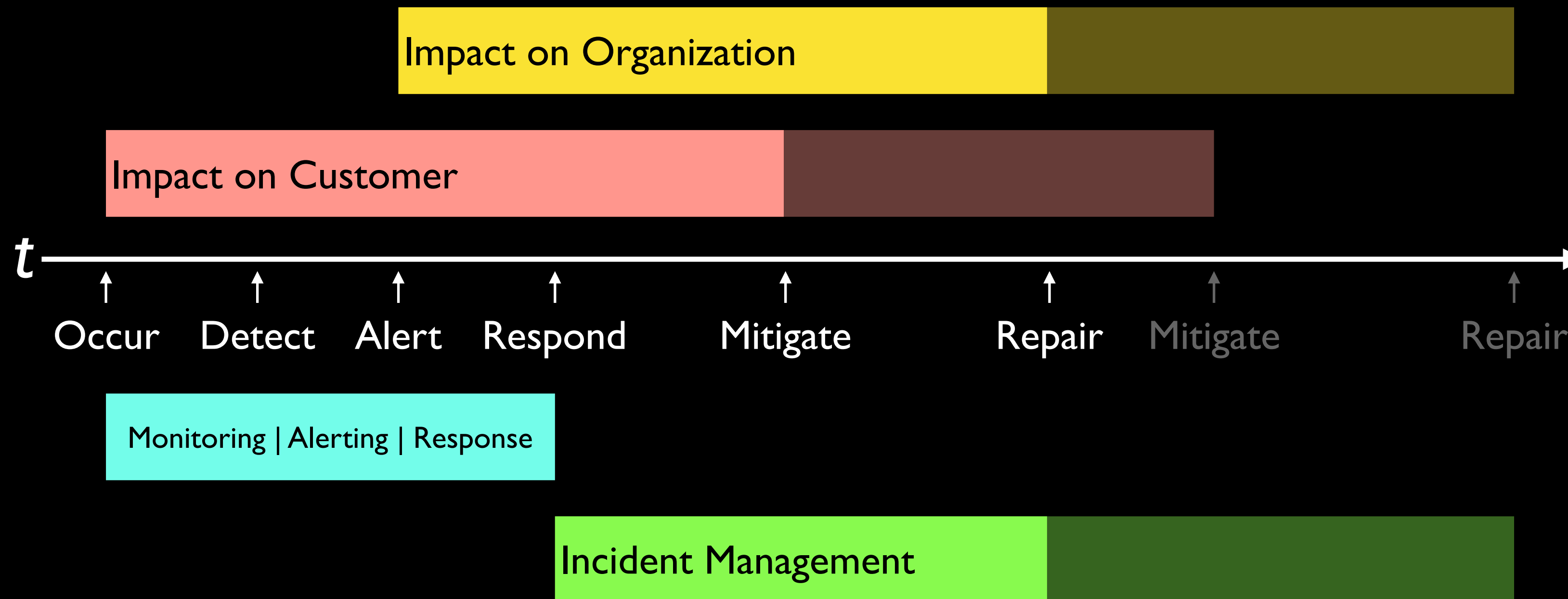


Incident response is a
critical capability

Incident Management Timeline



Incident Management Timeline





Normal Operations vs. Emergency Operations





Incident Command System works well for IT incidents



Key ICS Principles

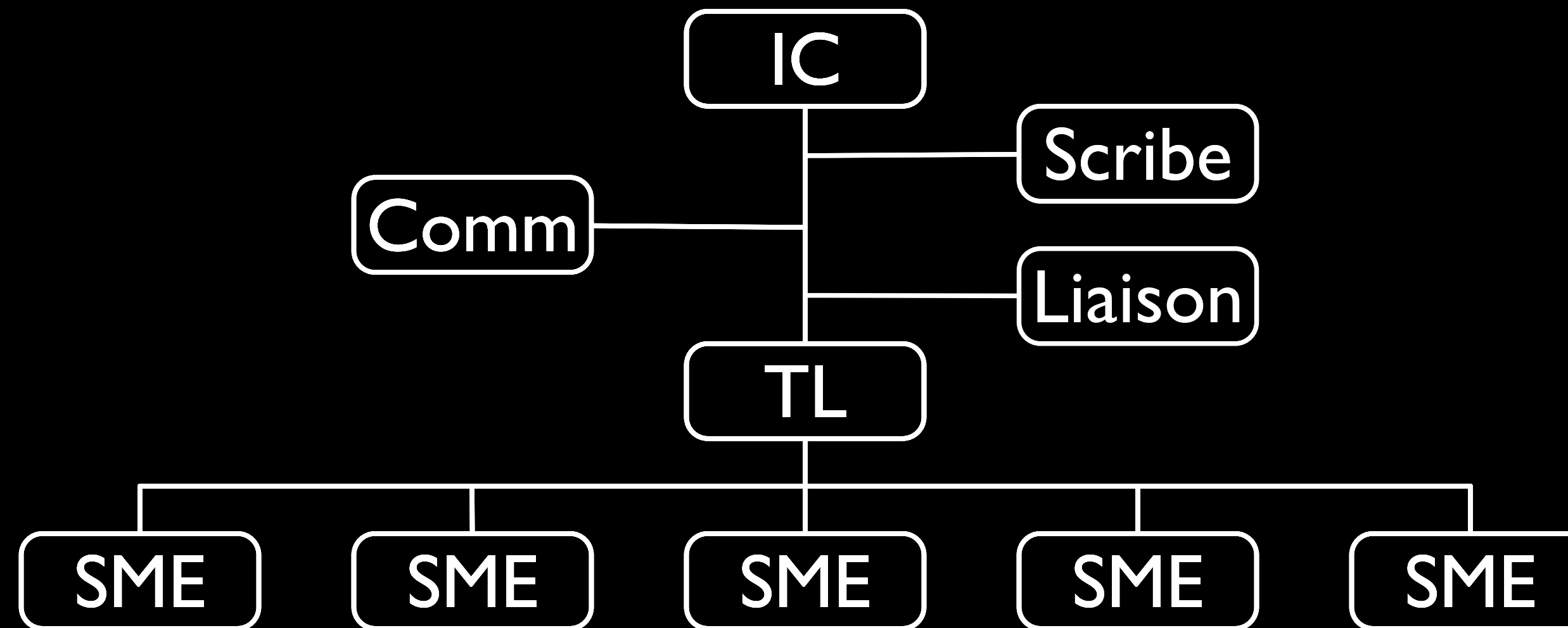
- Modular & scalable organization structure
- Manageable span of control
- Unity of command
- Explicit transfers of responsibility
- Clear communications
- Shared action plans
- Management by objective
- Time management
- Comprehensive resource management
- Designated incident facilities



A few tweaks make
ICS work even better
for IT incidents



ICS-ish org chart for IT incidents



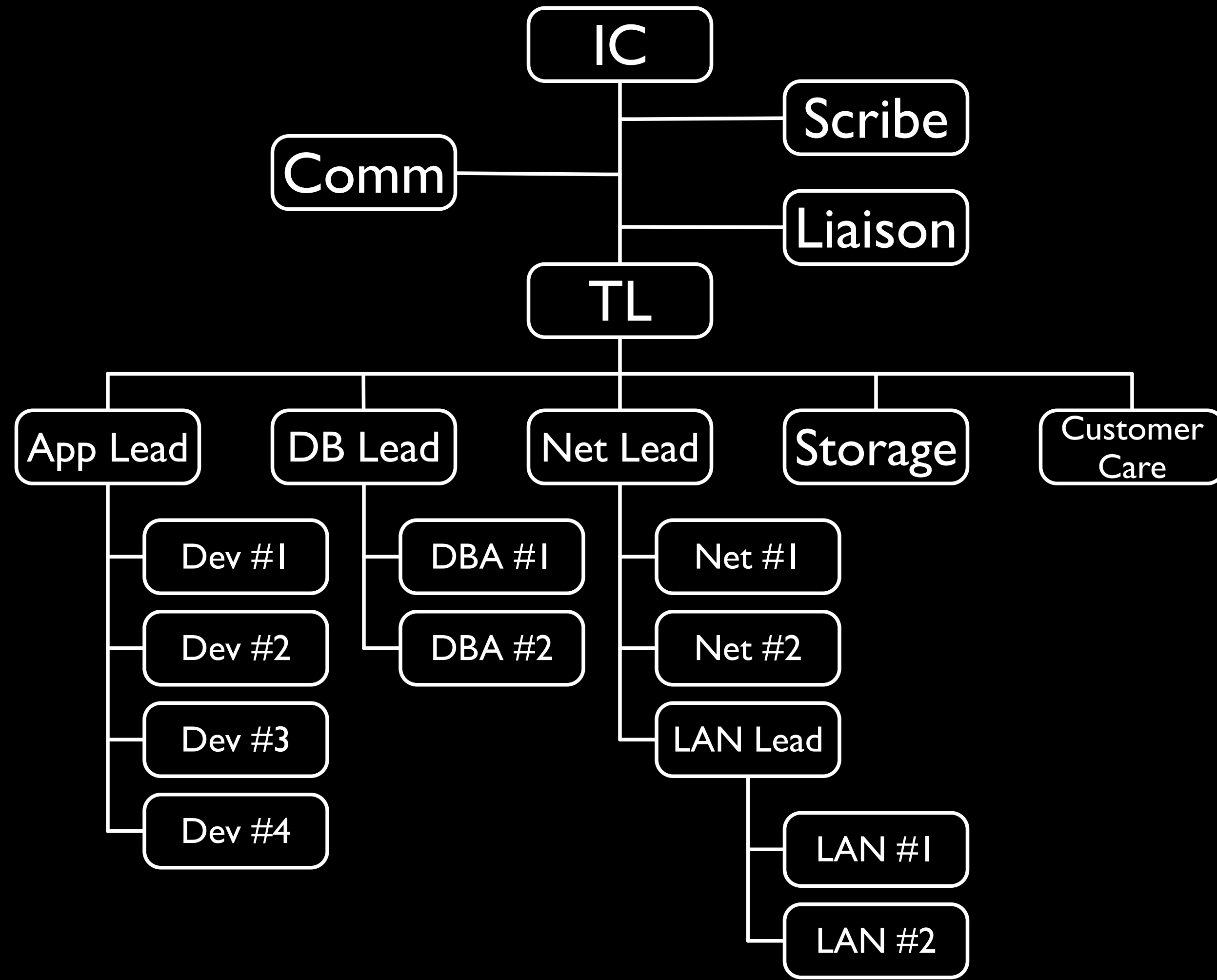
IC = Incident Commander

TL = Tech Lead

SME = Subject Matter Expert



Org chart grows as incident unfolds





Focus on roles,
not individuals



Practice, practice,
practice, then
practice some more



Senior managers can
inadvertently disrupt
incident response

Brent Chapman

Please contact me
with questions!

Brent@GreatCircle.com
@brent_chapman

Available for consulting, training,
and in-house presentations

*Site Reliability Engineering:
How Google Runs Production Systems
&*

PagerDuty Incident Response
docs & checklists
response.pagerduty.com

*The Site Reliability Workbook:
Practical Ways to Implement SRE*
landing.google.com/sre/book

These Slides
j.mp/grtcrc1-181024