14 Questions Are All You Need

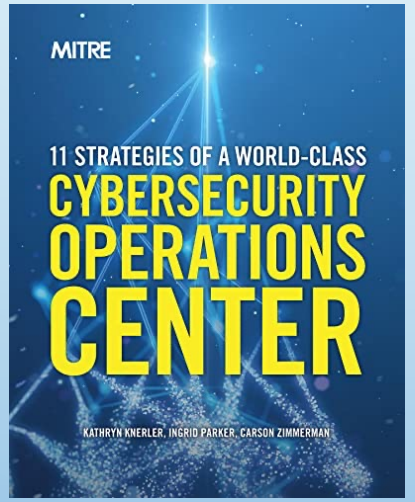
Carson Zimmerman

FIRST 2024

About Carson

- Worked in Security Operations for >20 years
- Formerly Chief Architect @ Ardalyst
- Formerly SOC investigations team lead @ Microsoft
- Check out my book if you haven't already

  $0/Free: https://mitre.org/11Strategies

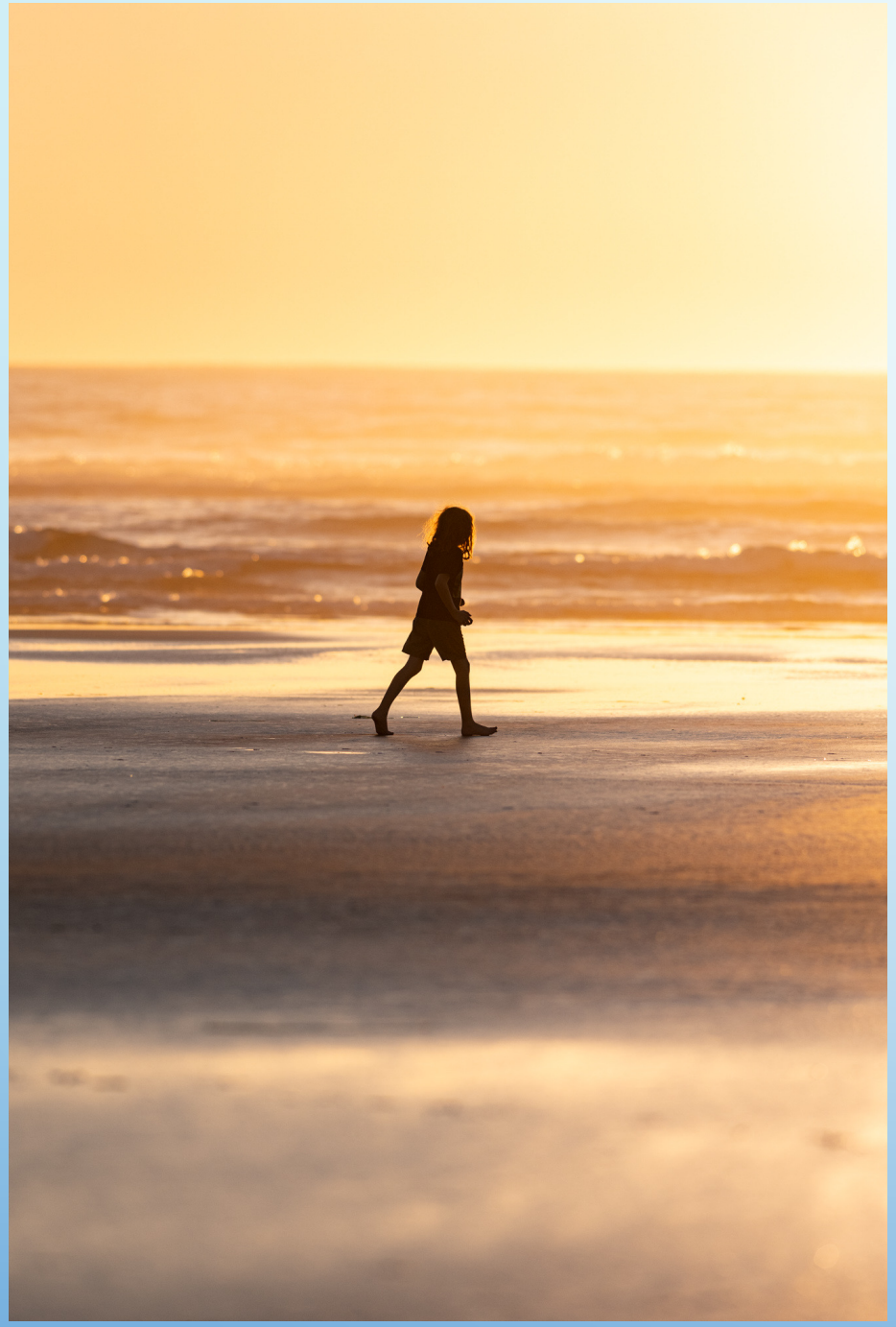


Not speaking on behalf of my employer, past or present;
any opinions expressed are my own.

First, I will tell you a story about FIRST… 2023

How is Your SOC doing, really?

- Plenty of ways to measure SOC capability and maturity
  - ENISA CSIRT Maturity + Open CSIRT SIM3 Frameworks: 45 questions
  - SOC CMM: 100s of questions
  - ATT&CK for detection & telemetry coverage: 100s of tiles, but don't treat it as a strict checklist
  - You're probably doing metrics already (ex: mean time to *)
- What if you don't have time for that?
- What if you want something lightweight?
- What are the areas you need to measure that are most likely hindering success?



In the next ~20 minutes…

14 measures of SOC growth and performance

Intent

Considerations for “good” and bad

Causal factors

Don’t get wrapped up in instrumentation- “anecdata” is often just as powerful

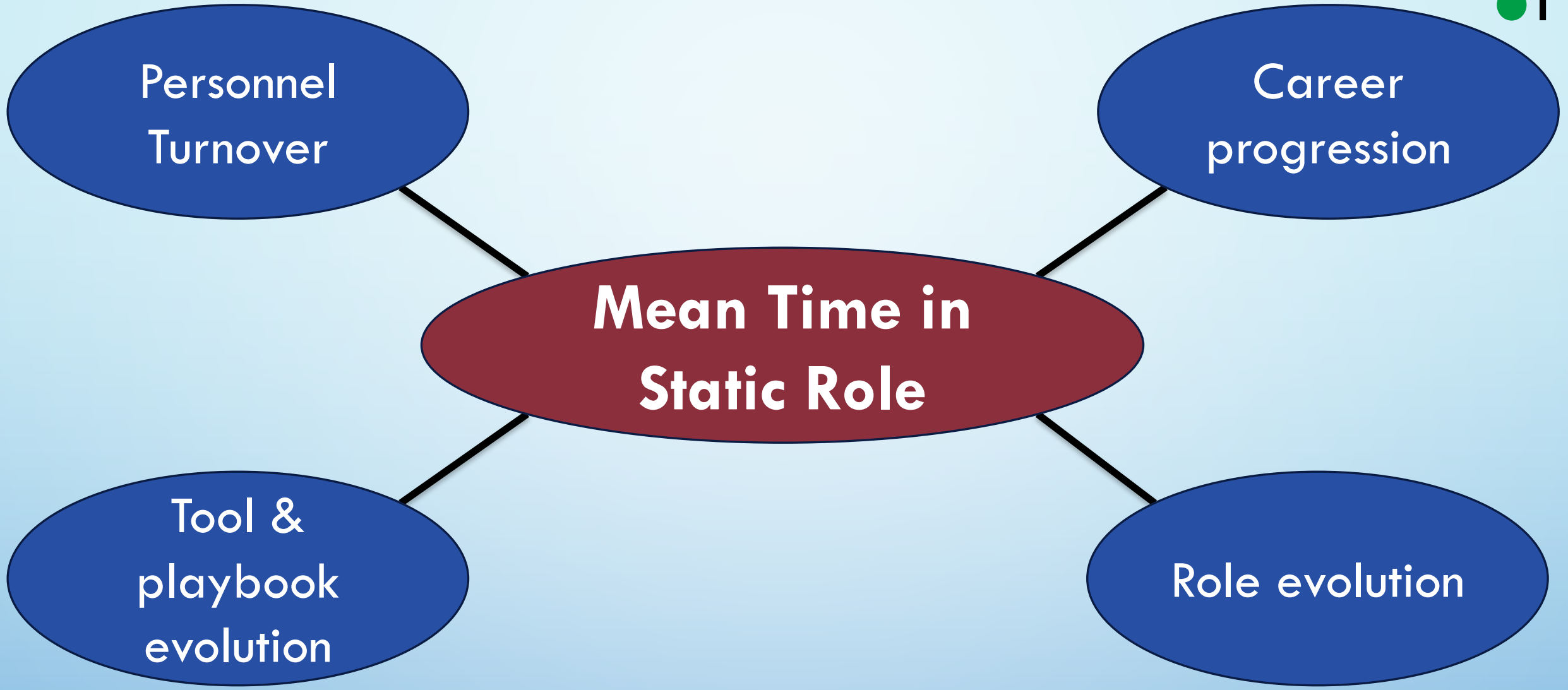
Not going to define a static target

What is right for you may not be right for another SOC

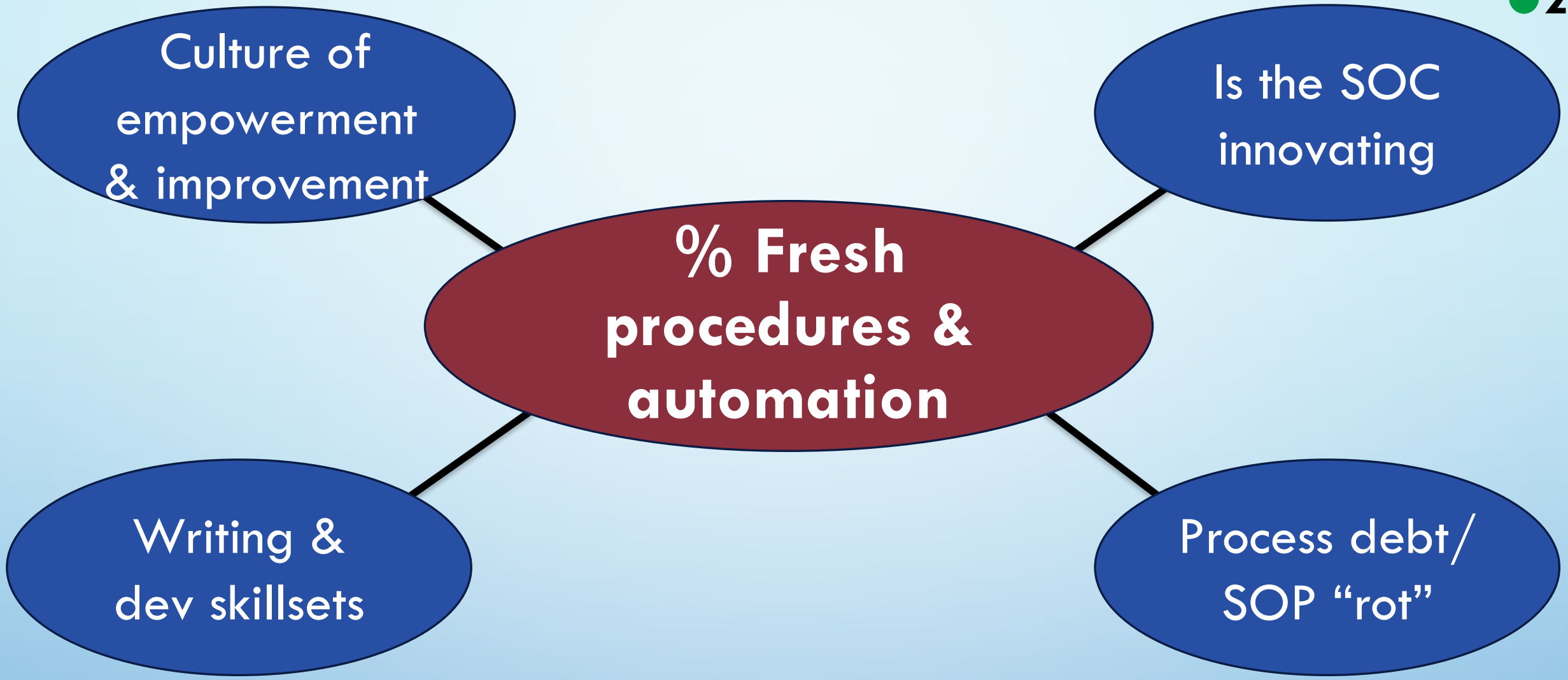
Growth Measures

Is the SOC driving continual improvement?

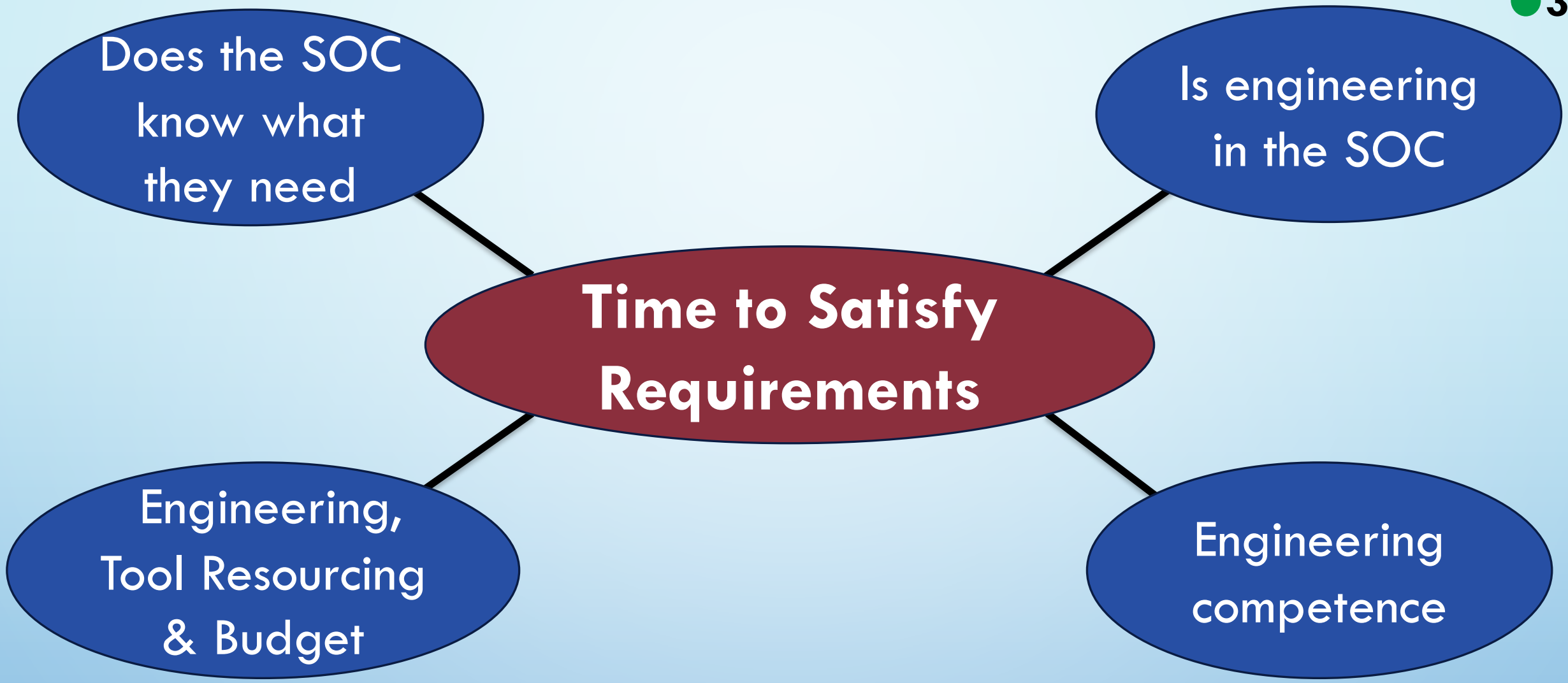
(see my talk “Save Your SOC From Stagnation” @ FIRST last year)



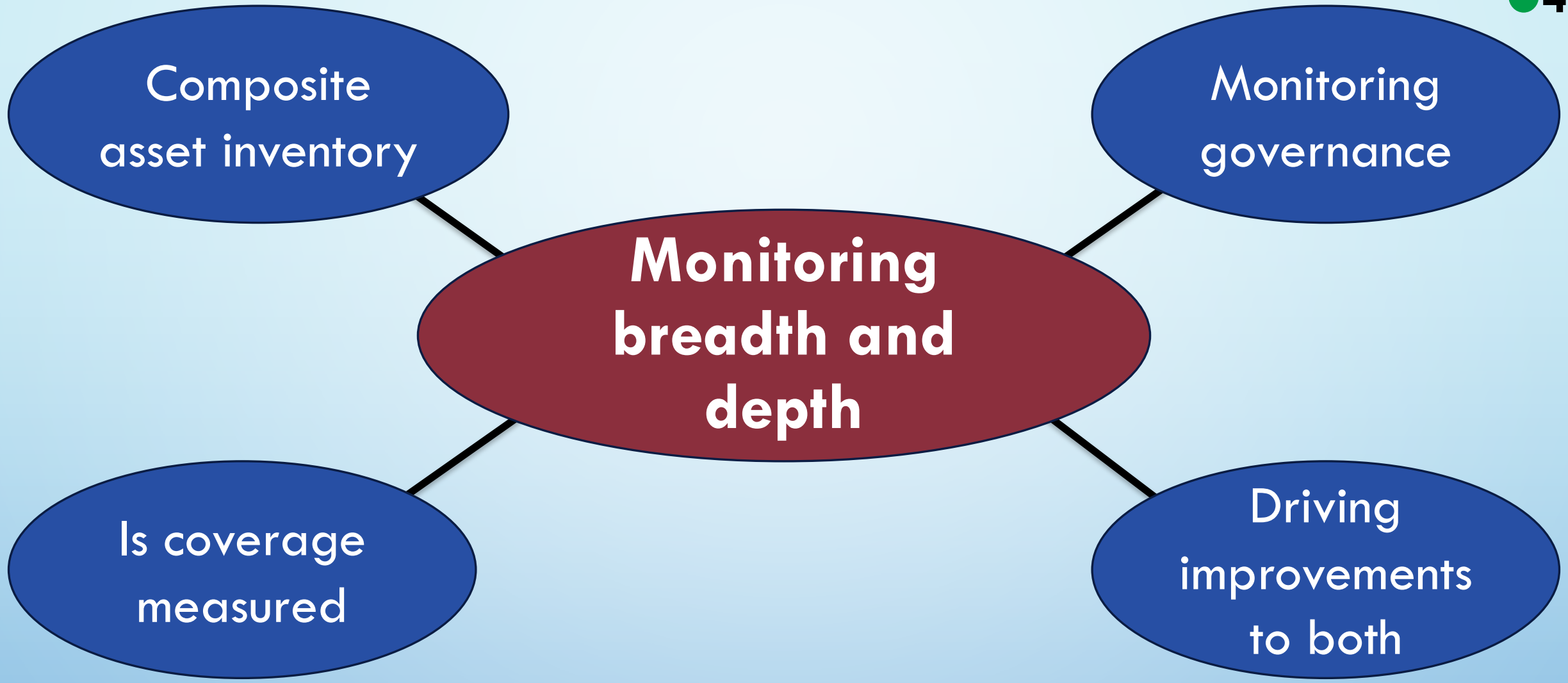
Time duration that a team member has performed the same tasks, with the same responsibilities, in the same way



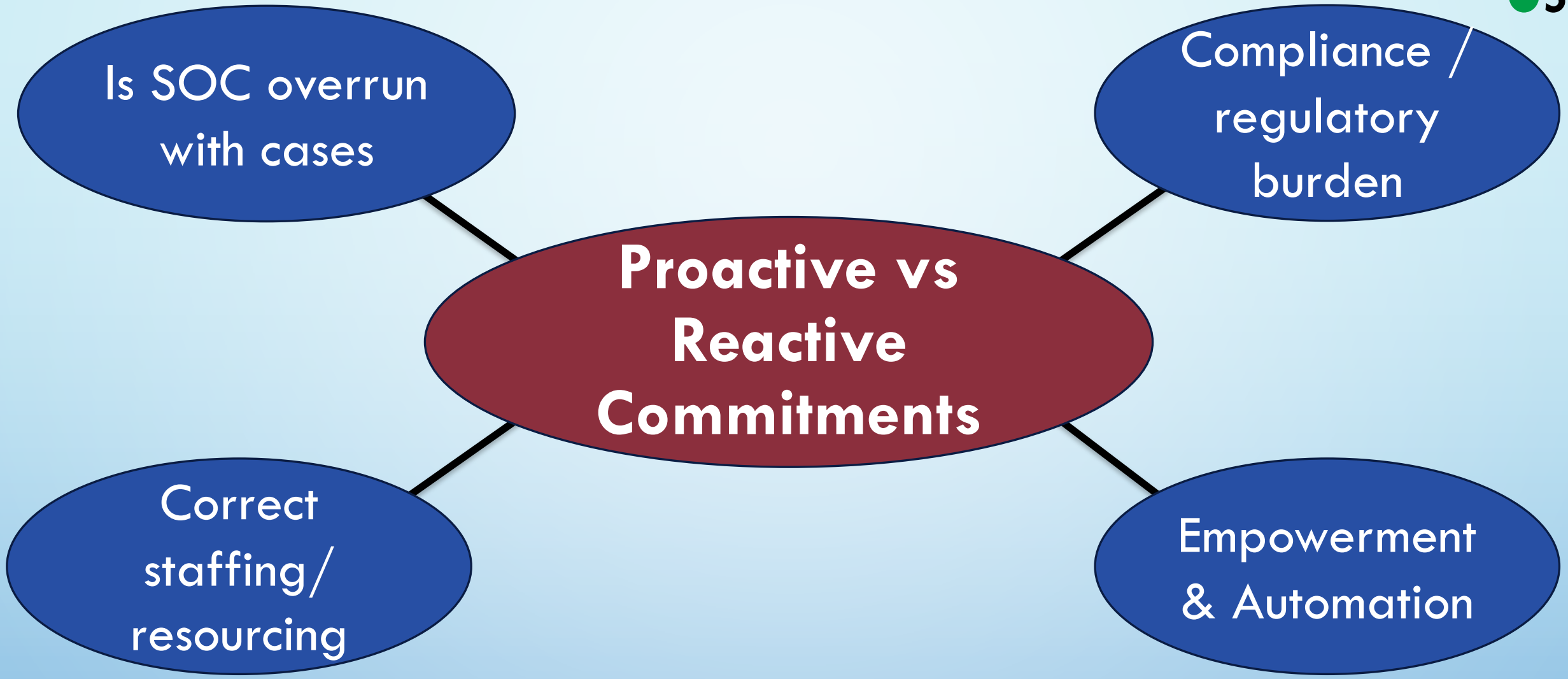
What % of SOPs, playbooks, analytic notebooks, and automation (SOAR) have been updated in the last year



Average time duration from when an operational/engineering requirement is identified, to when it is satisfied



What is the rate of change and accuracy of monitoring coverage, and its underlying composite asset inventory



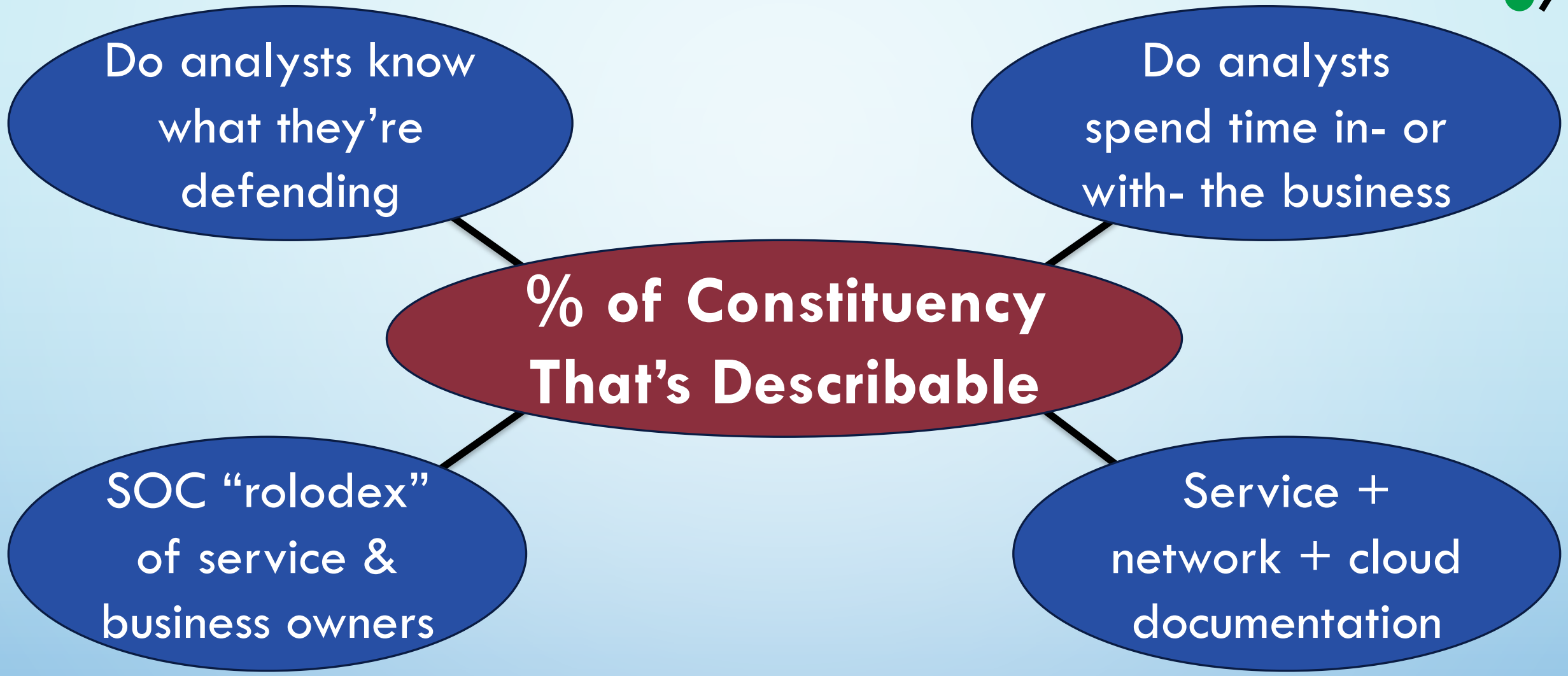
For each person or team, what % of their time is on reactive (unplanned, incident) **work vs proactive work** (dev, SOPs, learning)

Of bugs/problems identified during incidents (prevent, detect, respond, etc.), **what % are fixed after 1 year**

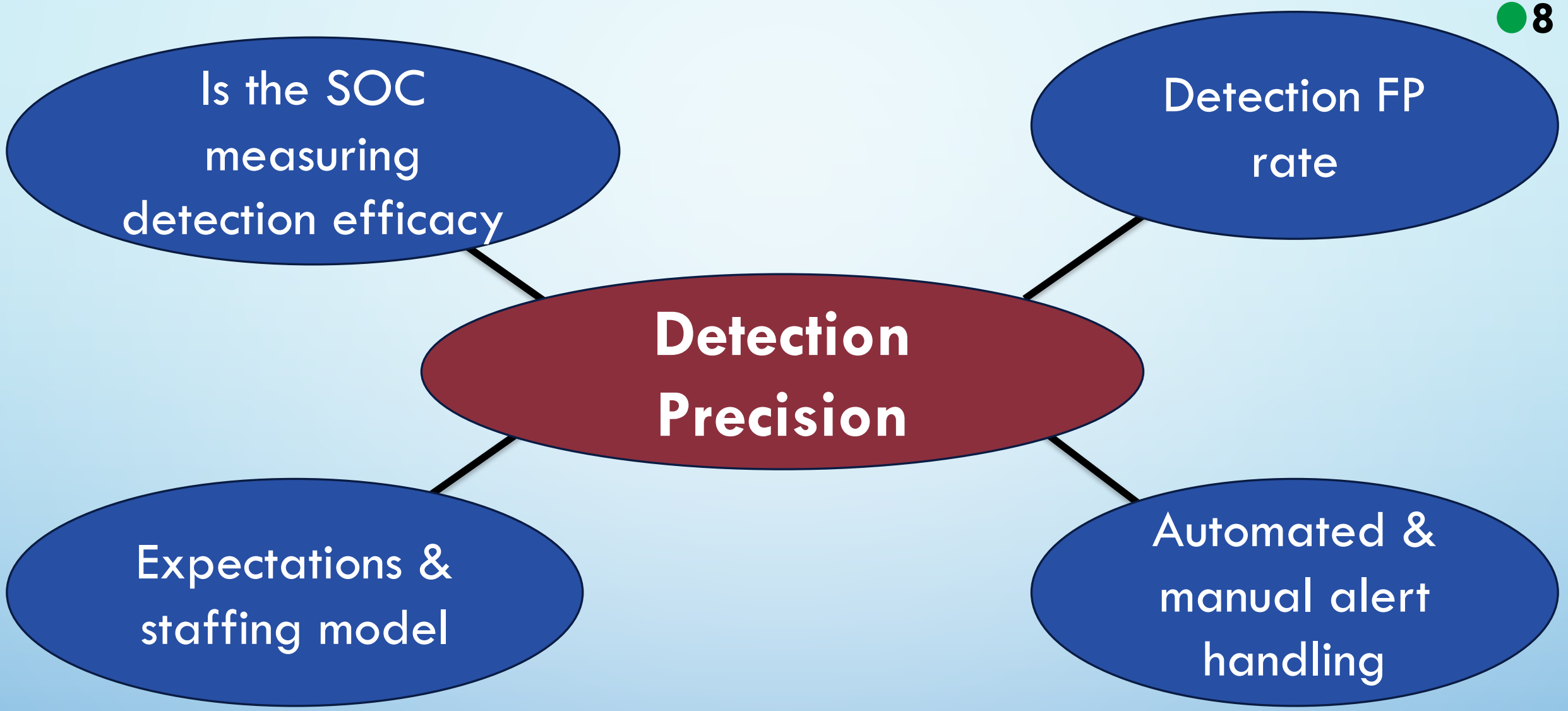
Performance Measures

Is the incident funnel healthy?

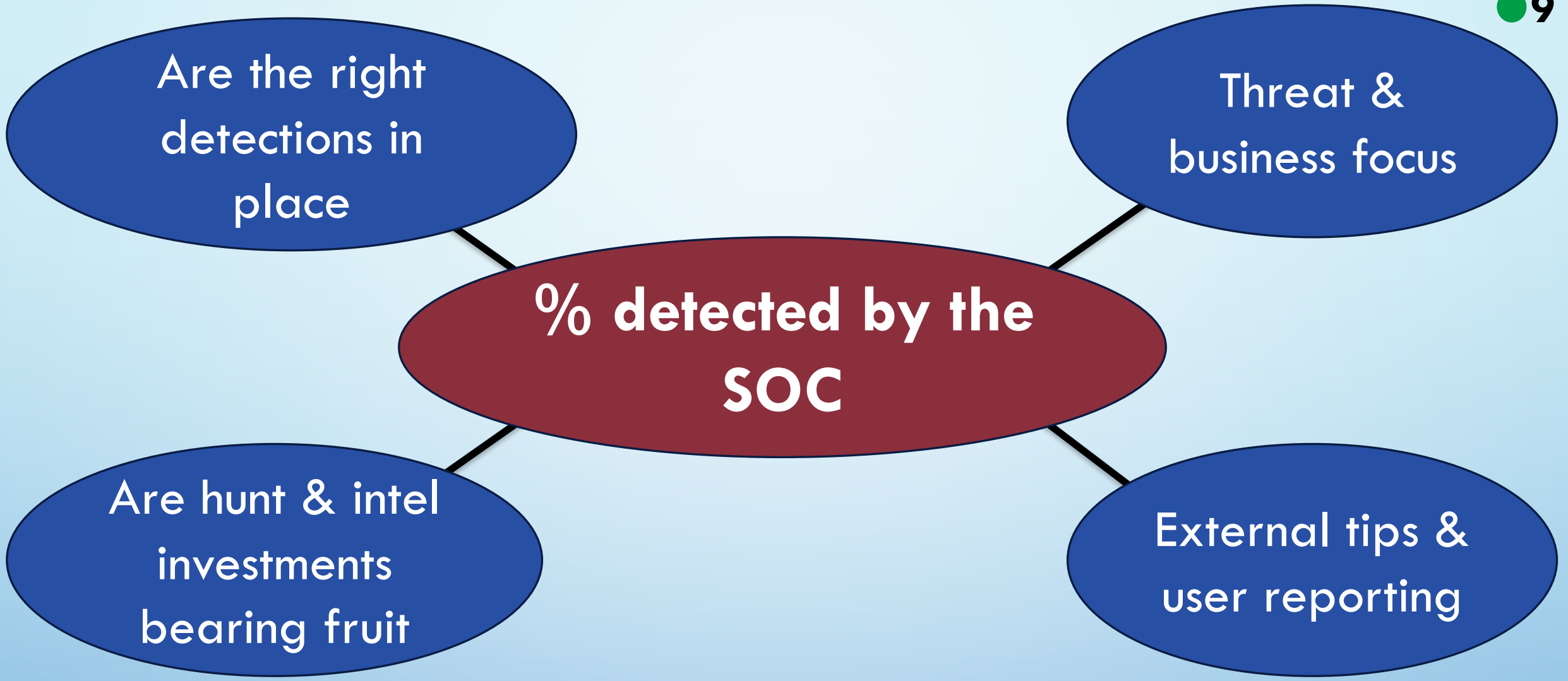
Detect -> Investigate -> Respond -> Recover



Given 15 minutes' notice, what percentage of the enterprise can the SOC (collectively) **describe: mission/business, IT/OT/cloud infra**



Of all the alerts that go to triage or automation, what % are true positives



What % of true positive cases started with SOC detection & hunt vs outside reports (intel, tips, users, etc.) (related to recall)

Of all alerts and cases that SOC humans handled, what % of them should have been handled by humans (vice automation, filtering/tuning, or rerouting to another team)

Of all investigative questions posed, what % were correctly answered in 2 hours or less

Correct & complete identification of threat

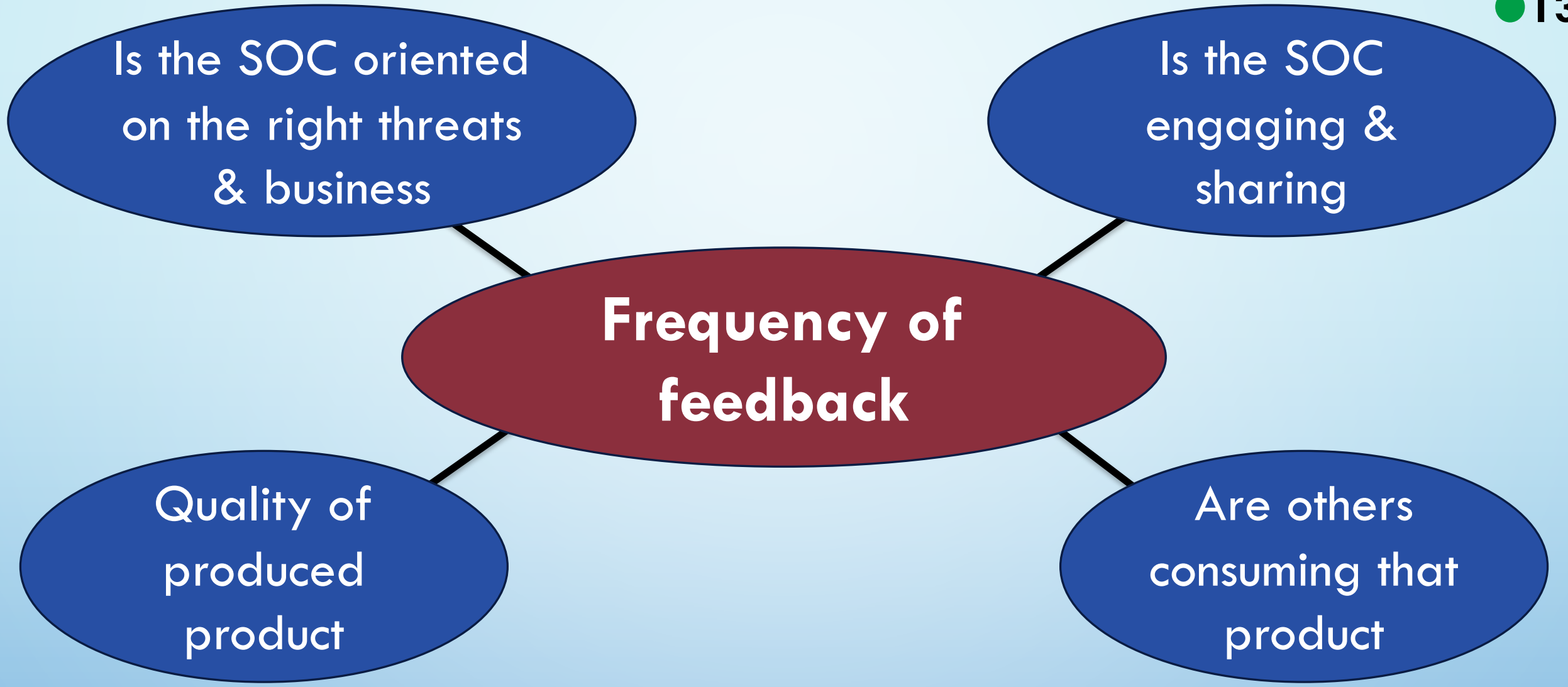
Can the SOC "push the button?"

% of containment within SLO

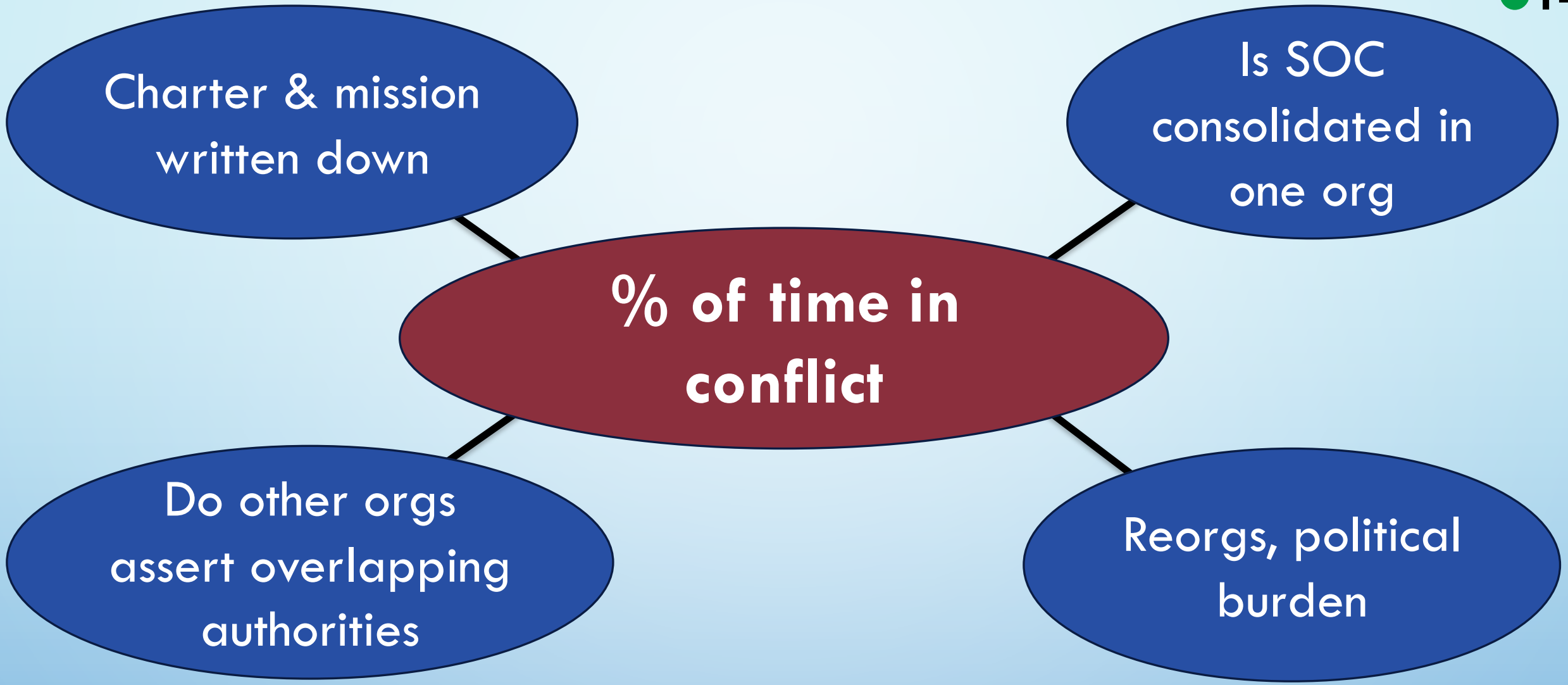
Tooling capability, coverage, training

Partners' willingness & ability to support

What % of incidents achieved full containment or eviction of an adversary within stated objectives (SLAs, SLOs)



How often (daily, weekly) **is the SOC's community** (other SOCs, constituents) **responding to SOC intel** (reports, dashboards, etc.)



What proportion of time (daily, weekly) **is SOC leadership in conflict with itself or others over mission scope, authorities**

What's Next?

- Use these 14 questions to:
  - Focus your energy
  - Tell your story
  - Make things better
- Have an opinion? Let's talk after.

www.linkedin.com/in/carson-zimmerman