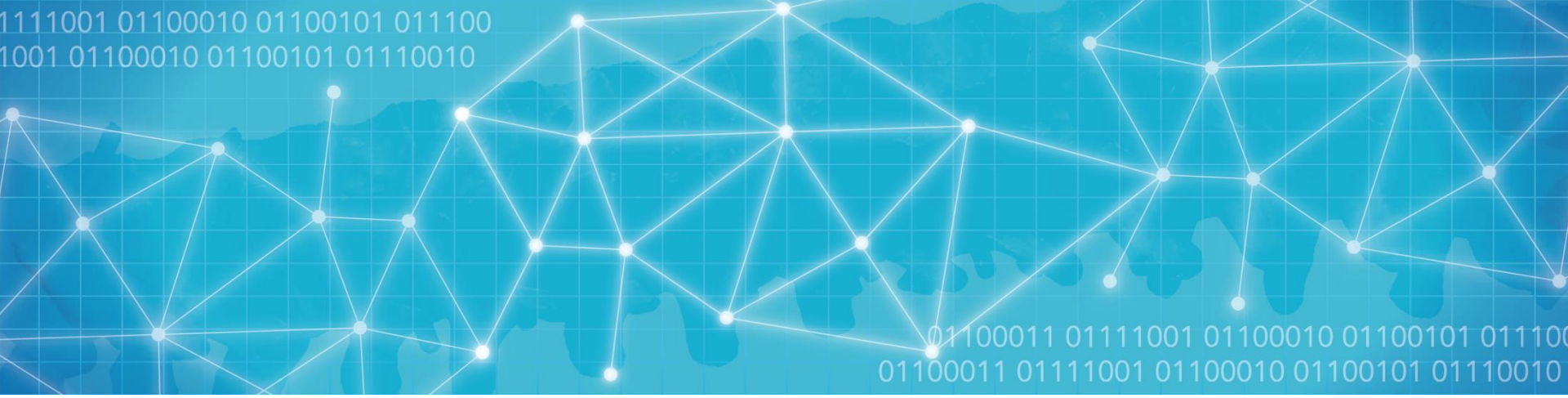


Gaining and Maintaining Support for a SOC

Jim Goddard

Executive Director, Kaiser Permanente

Objectives

Agenda

1. Lessons learned
2. How to build interest
3. Producing tangible benefits
4. Building momentum
5. Communicating success
6. Expanding the ecosystem
7. Quantitative metrics

Lessons learned while building a SOC

- Investment is multi-year
- Agile development, not waterfall
- Mission must be focused
- Remember the triad of people, process and technology
- Seasoned leadership is essential
- Be visible
- Avoid silo’s
- Manage 24/7 expectations

Why support is so important

- Investment is for the long haul
- SOC is not self-reliant
- Expectations can be too easily misplaced

Common objections must be overcome

Aren't we already compliant?

Can we just purchase a tool?

INVESTMENT DECISION PROCESS

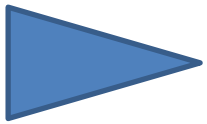
Will this guarantee against a breach?

What is the ROI?

Can't we just outsource this?

Crisis events whether internal or external often stimulate interest, but you have to take it home from there

UNCERTAINTY



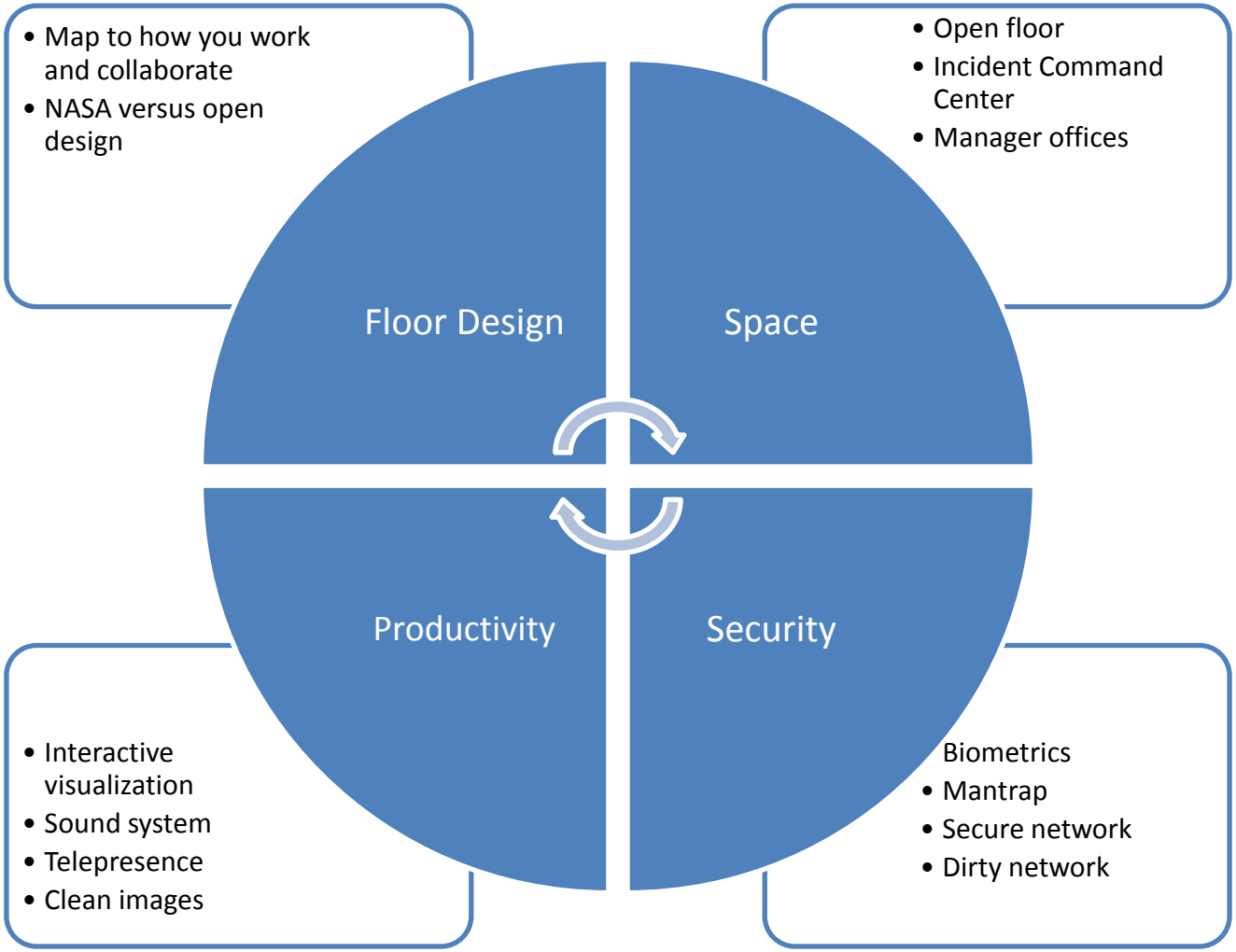
Explaining events in a way people understand → Illustrating a solution → Overcoming objections

BUILD INTEREST

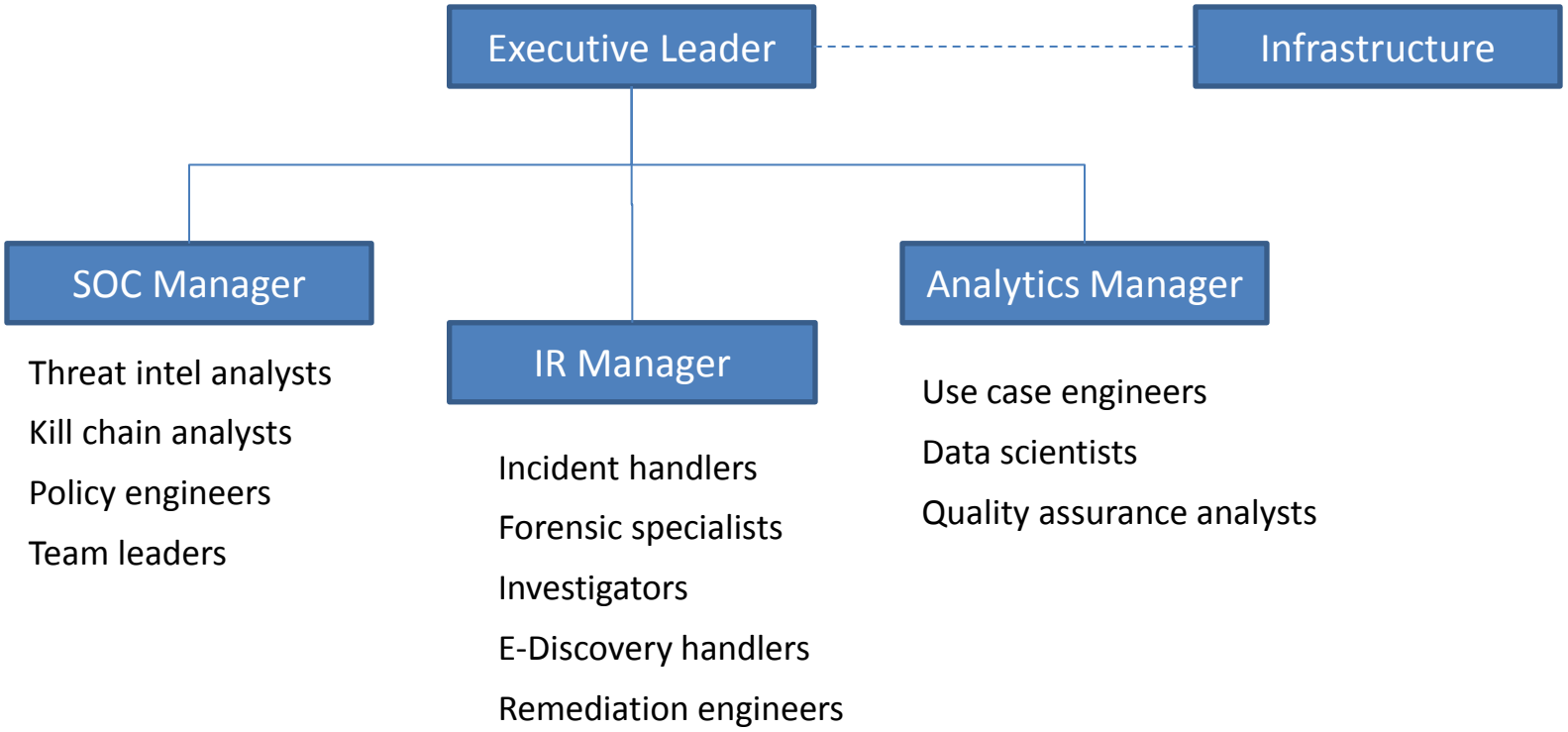
Produce tangible benefits people “get”

- Physical presence with visualization
- Diverse skillsets
- Actionable events, not data analysis
- Rapid, high touch response

Physical design



Make sure your organization has enough reach



Build momentum with quick wins

Year 1

Security & Event Management (SIEM)
Flow data
Security control data (e.g., malware)
Threat intel & IOC detection
Reference lists

Year 2

Log data analytics
Raw data capture
IOC sweeps & quarantine
Lateral movement
Data visualization

Year 3

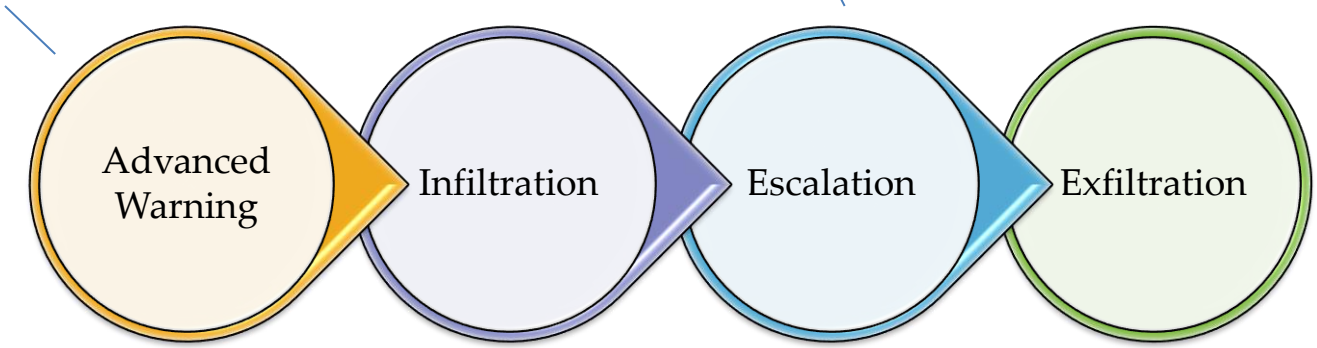
Application level analysis
Countermeasure automation
Big data analytics

MOMENTUM

Startup use cases can get you more actionable events

Day 1 domains
Imposter domains
Threat & reputation feeds

Internal scanning
Connection anomalies
User baselining



Callbacks
IDS exploits
Domain name entropy

Volumetric analysis
Entropy analysis
Frequency analysis

Communicate wins that people will read

- Give up the techie talk and explain
- Make the communication accessible (no Powerpoint; simple text that looks good on a phone).
- Be brief **(2-3 swipes on a phone**). Executives don't have time to figure out what you are trying to say.
- Give them what they want to know, not what you want to say.
- Never be late.

What you should try to communicate (with responsibility)

- Incident alerts and updates
- Countermeasure application
- Threat intelligence (formal and informal)
- Operational metrics
- Customer inquiries

Continue to expand your ecosystem

INITIAL GROUPS TO CO-OPT:

- ✓ Incident Response
- ✓ Legal
- ✓ Compliance
- ✓ Senior executives

LONGER TERM VALUE:

- ✓ Infrastructure
- ✓ Service Desk
- ✓ Architecture & Strategy
- ✓ Sales

Operational metrics will also help drive perception

Area	Metrics
Detection	• Detected versus reported • Correct designations for response • Time to analyze and resolve • False positives
Response	• Time to contain, by severity • Indicators of compromise with actionable events
Remediation	• Time to remediate, by severity • Repeat incidents

Questions?