

LEAN GAINS – SMALL TEAM EFFECTIVENESS



Ben May - Manager Cyber Security
ben.may@aemo.com.au

- Operating gas and electricity markets and power systems
- Delivers operational, development, and planning functions.
- Ownership 60% government; 40% market participants.
- Funded by market participants and operates on a cost recovery basis

AUSTRALIAN ENERGY MARKET

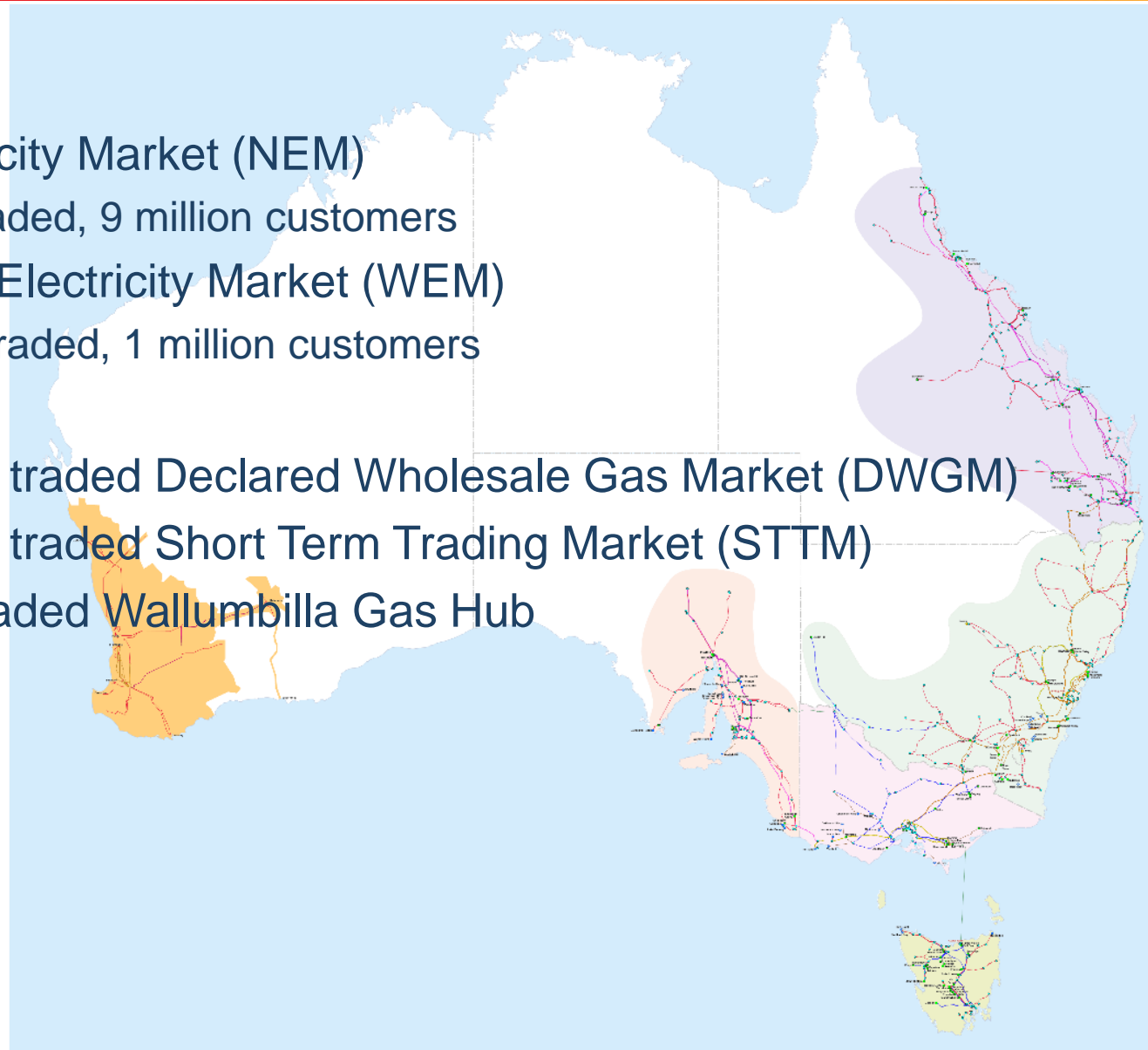


Electricity:

- National Electricity Market (NEM)
 - **\$7.7 billion** traded, 9 million customers
- WA Wholesale Electricity Market (WEM)
 - **\$500 million** traded, 1 million customers

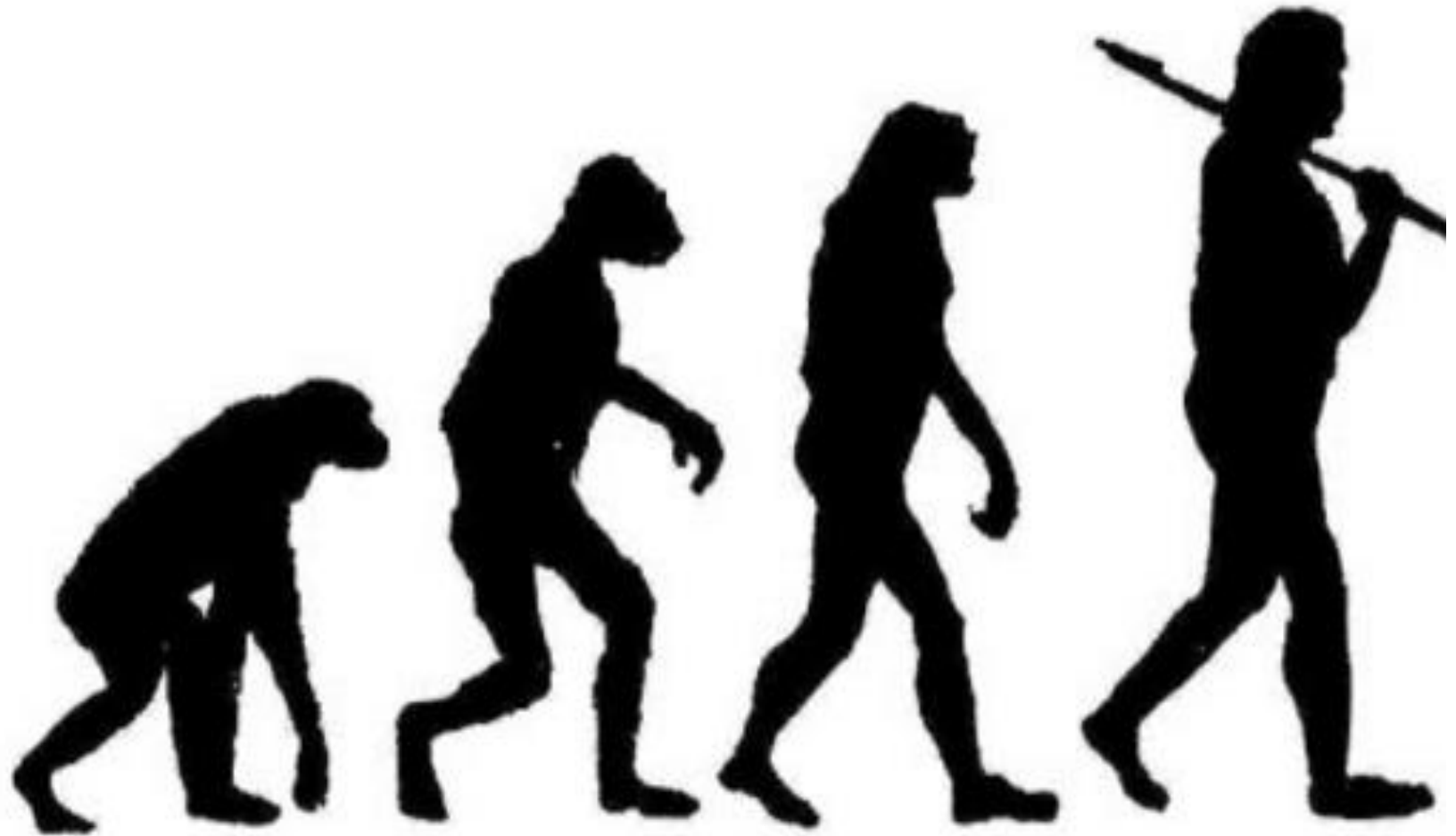
Gas:

- **\$899.5 million** traded Declared Wholesale Gas Market (DWGM)
- **\$557.8 million** traded Short Term Trading Market (STTM)
- **\$8.7 million** traded Wallumbilla Gas Hub



- Geographically dispersed team
- Complex environment
- Small organisation
- Significant Change
- Focus on Threat Detection and Response

EVOLUTION (MATURITY)



STAGE OF EVOLUTION



- Limited size team
- Defensive mindset
- Run our own infrastructure
- No known good state
- Security as an add-on

SMALL TEAM – NOT ALL BAD

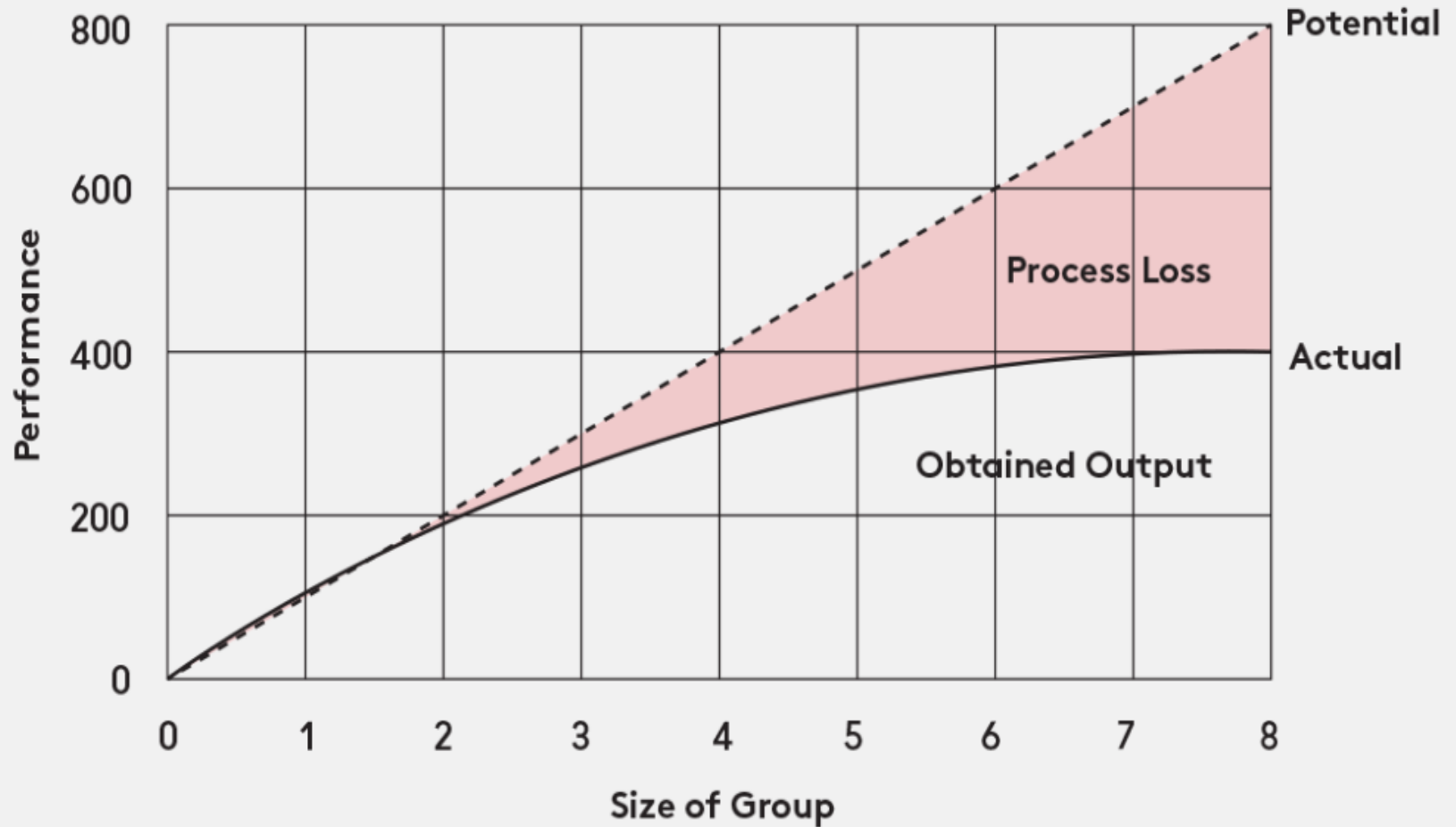
- Agile/Flexible
- Self Reliant as a team
- Ownership
- Communication



Amazon CEO Jeff Bezos's

"two pizza" rule: If a team can't be fed with two pizzas, it's too big.

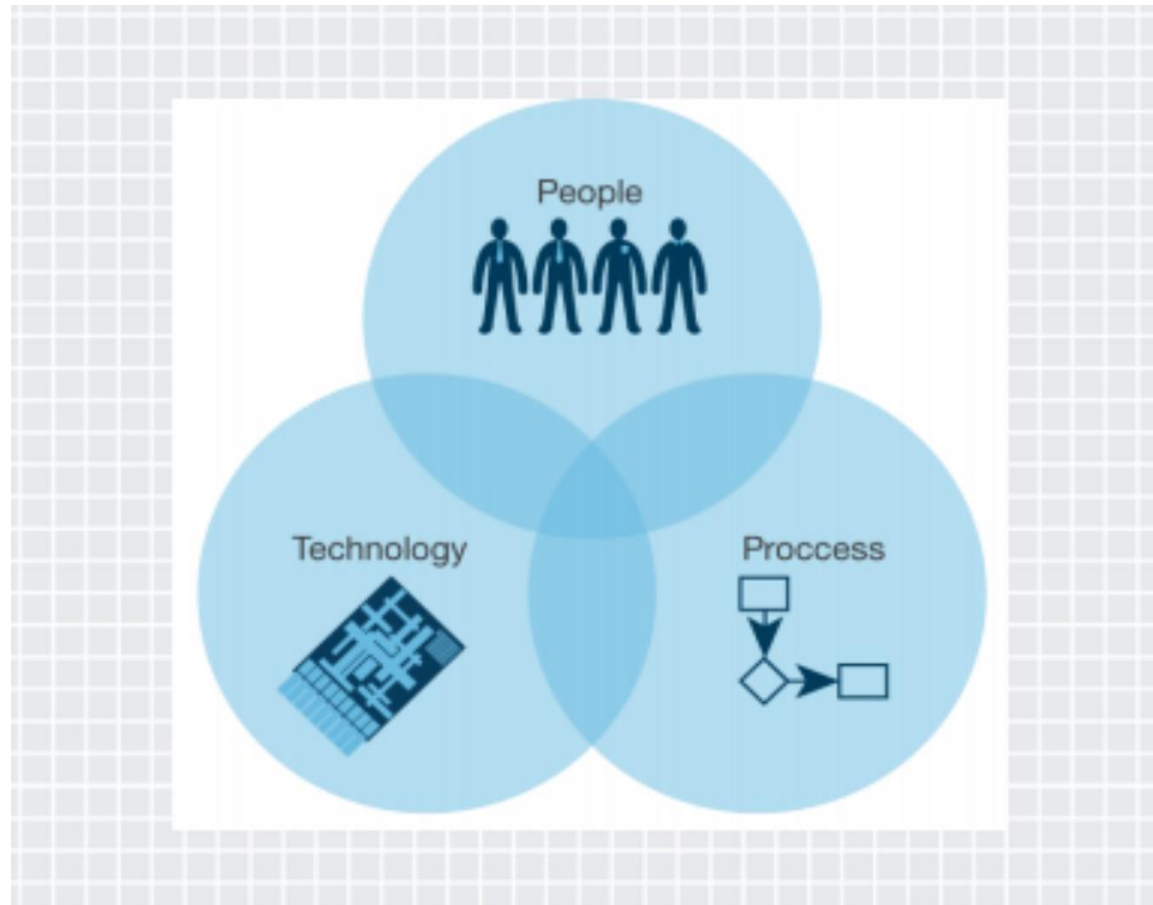
RINGLEMANN EFFECT



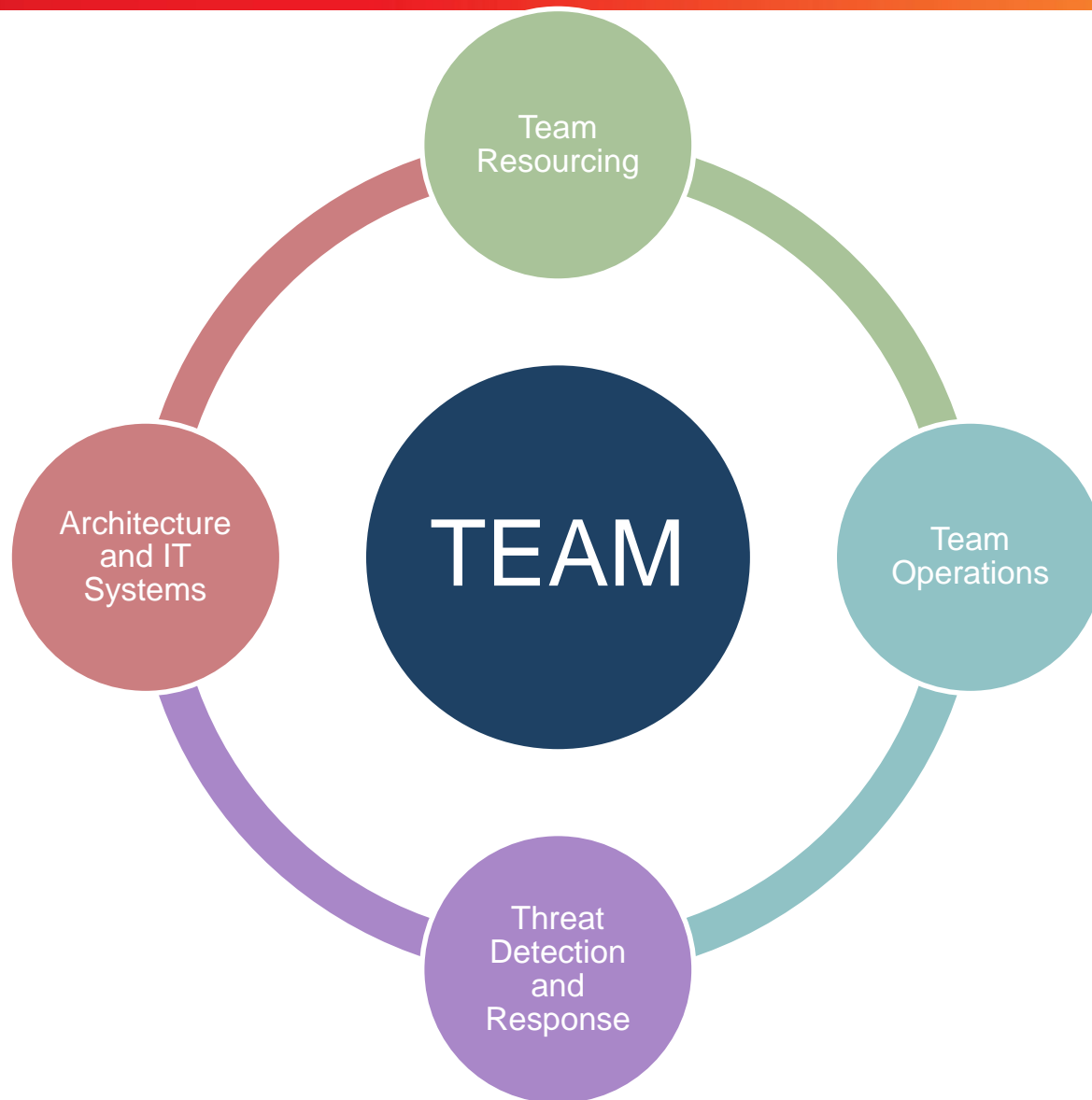
* "Is the ringlemann effect holding you back," <http://www.vanschneider.com/is-the-ringelmann-effect-holding-you-back>

THE PEOPLE YOU WANT

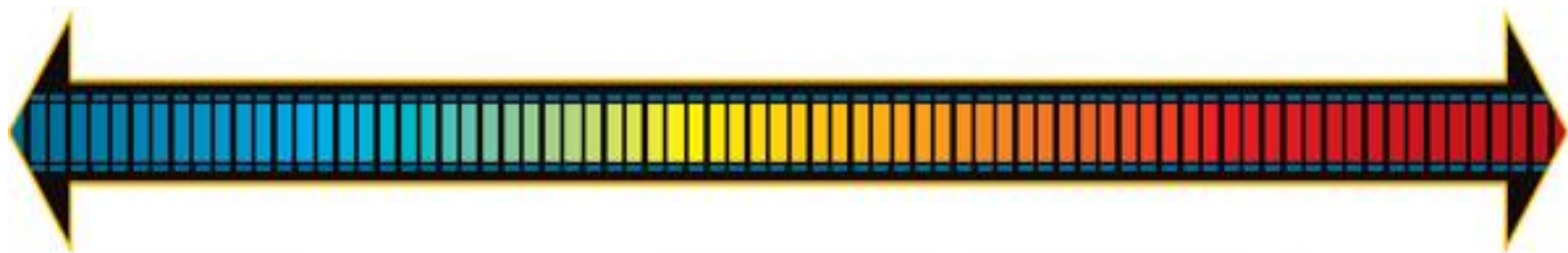
- Passionate
- Offensive mindset
- Ownership
- Focus



RESEARCH AND CONTINUOUS EVOLUTION



TEAM RESOURCING SLIDING SCALE OF CYBER – ROB LEE *

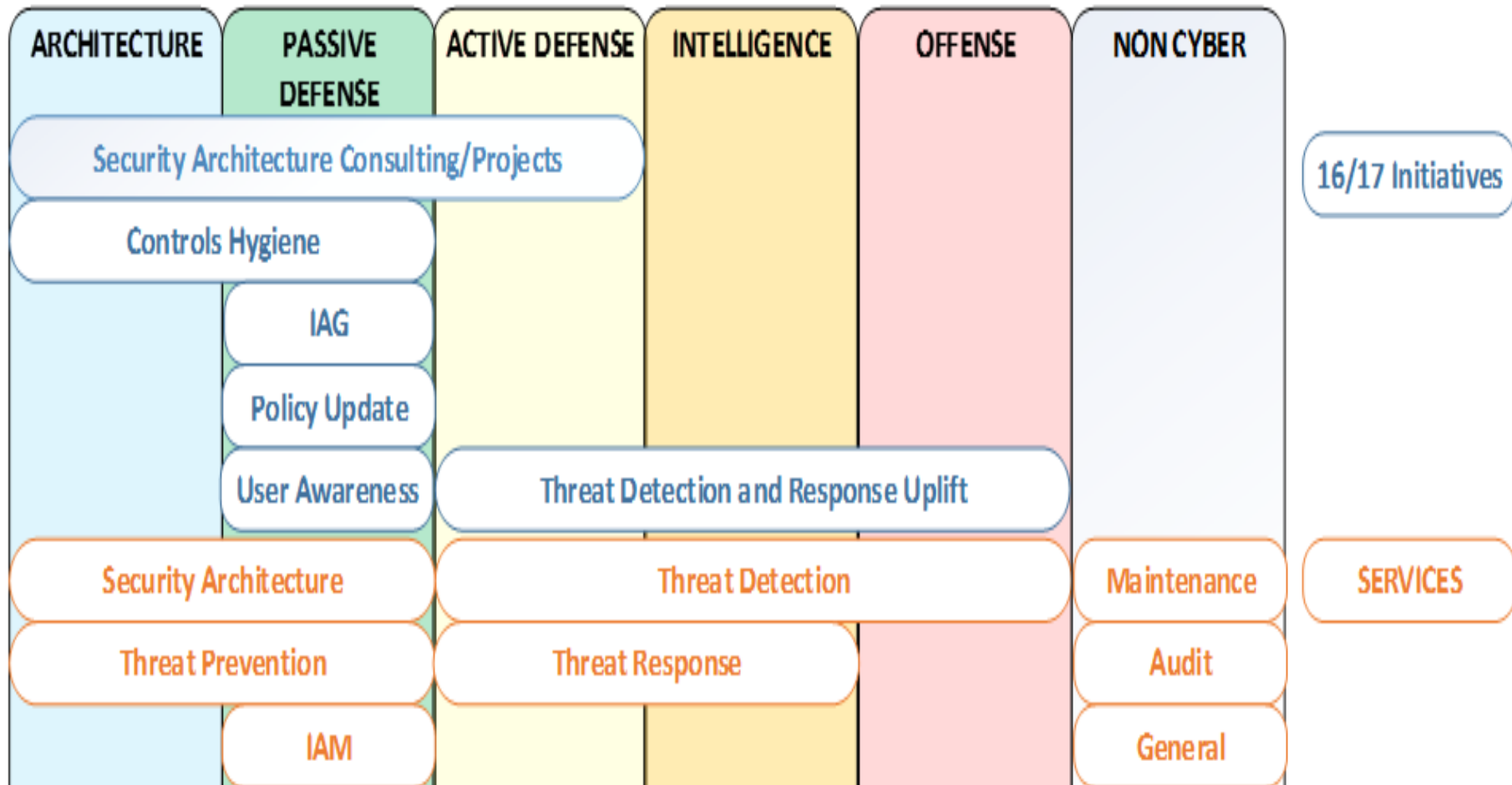


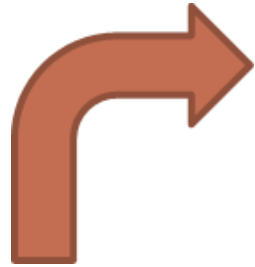
Value Towards Security

Costs

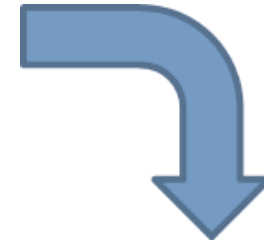
* 'The Sliding Scale of Cyber security', <https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240>

TEAM RESOURCING ALIGN TEAM DELIVERABLES





Incident Response

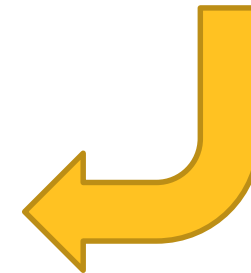


**Asset and Network
Security
Monitoring**

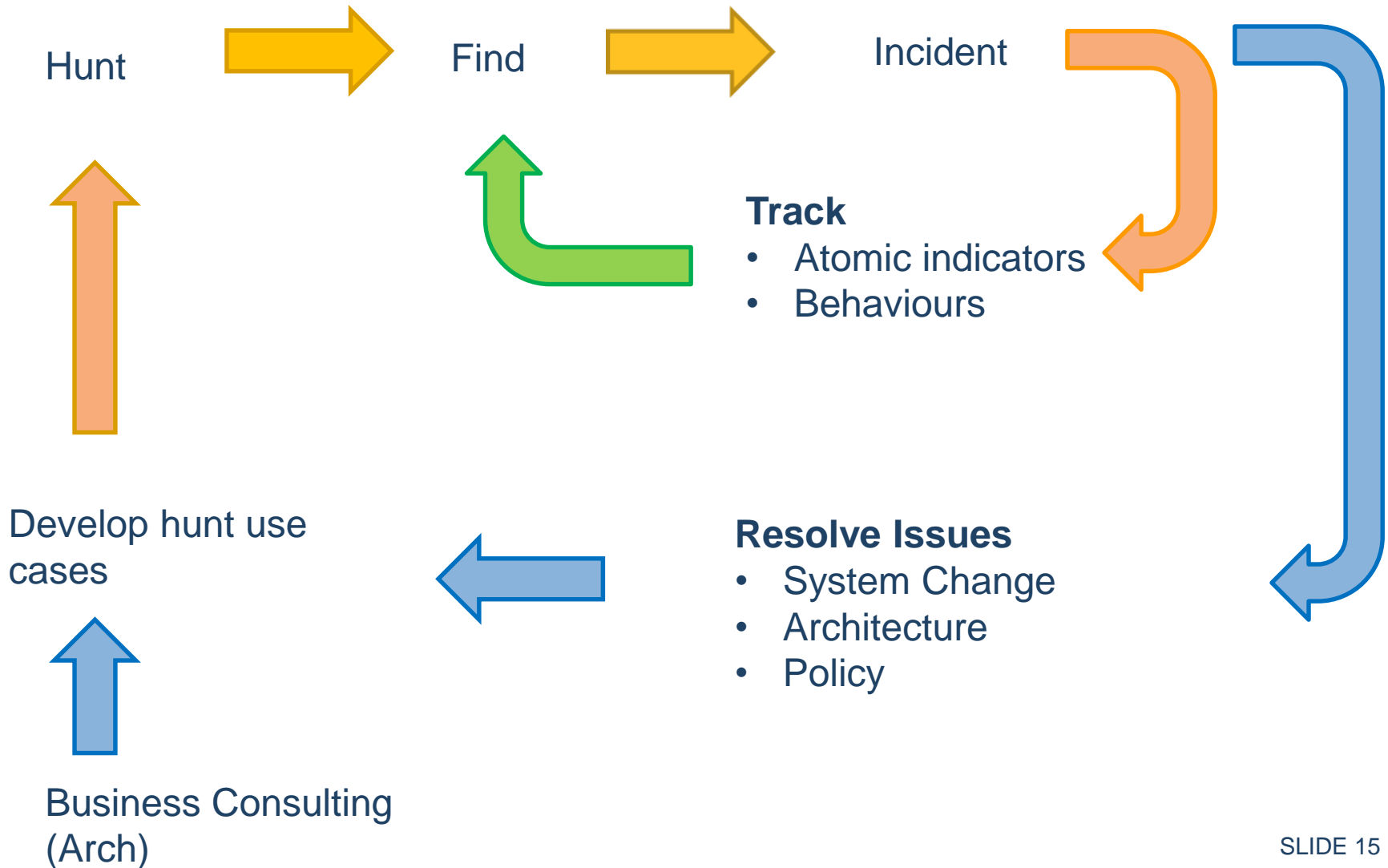
**Threat and Environment
Manipulation**



**Threat Intelligence
Consumption**



TEAM OPERATIONS PROCESS - EXAMPLE













THREAT DETECTION AND RESPONSE INTELLIGENCE DRIVEN COMPUTER NETWORK DEFENSE *



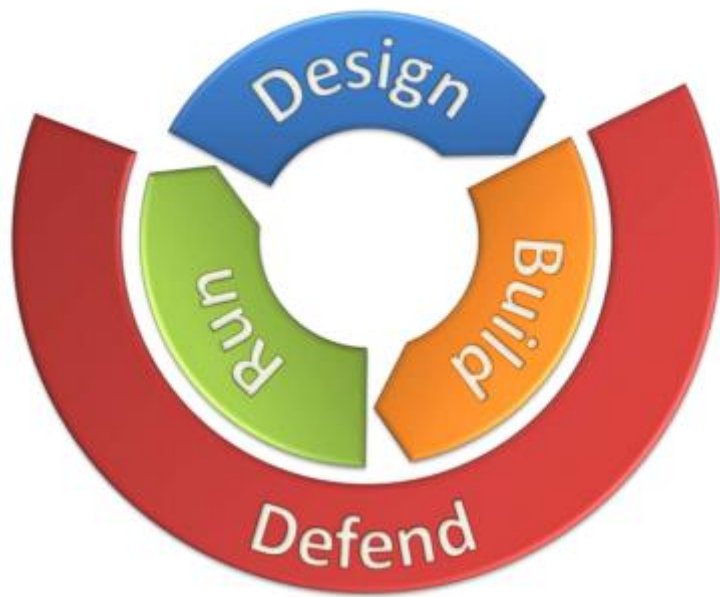
* *"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"*
www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

THREAT DETECTION AND RESPONSE EXAMPLE

-   **AEMO Intel Tier** (3 items)
tier 4 (15) - tier 3 (8) - tier 1 (3)
-   **AEMO Intel Action** (1 item)
alert all (6)
-   **AEMO Intel Type** [open]
-   **AEMO Email Cloud** [open]
-   **AEMO Kill Chain** (3 items)
kc1 - recon (12) - kc7 - action on objectives (11) - kc3 - delivery (3)

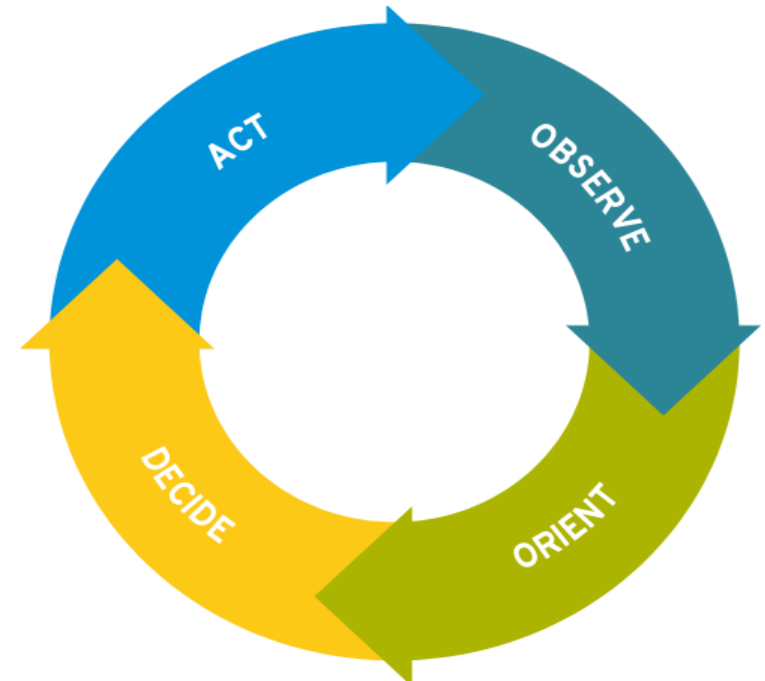
ARCHITECTURE AND IT SYSTEMS

DEFENDABLE ARCHITECTURES *



- **Visibility**
- **Manageability**
- **Survivability**

- **Observe** – Collect
- **Orient** – Analyse
- **Decide** – Judge
- **Act** - Execute



*“the capability to evolve, to adapt, to learn, and deny such capability to the enemy” **

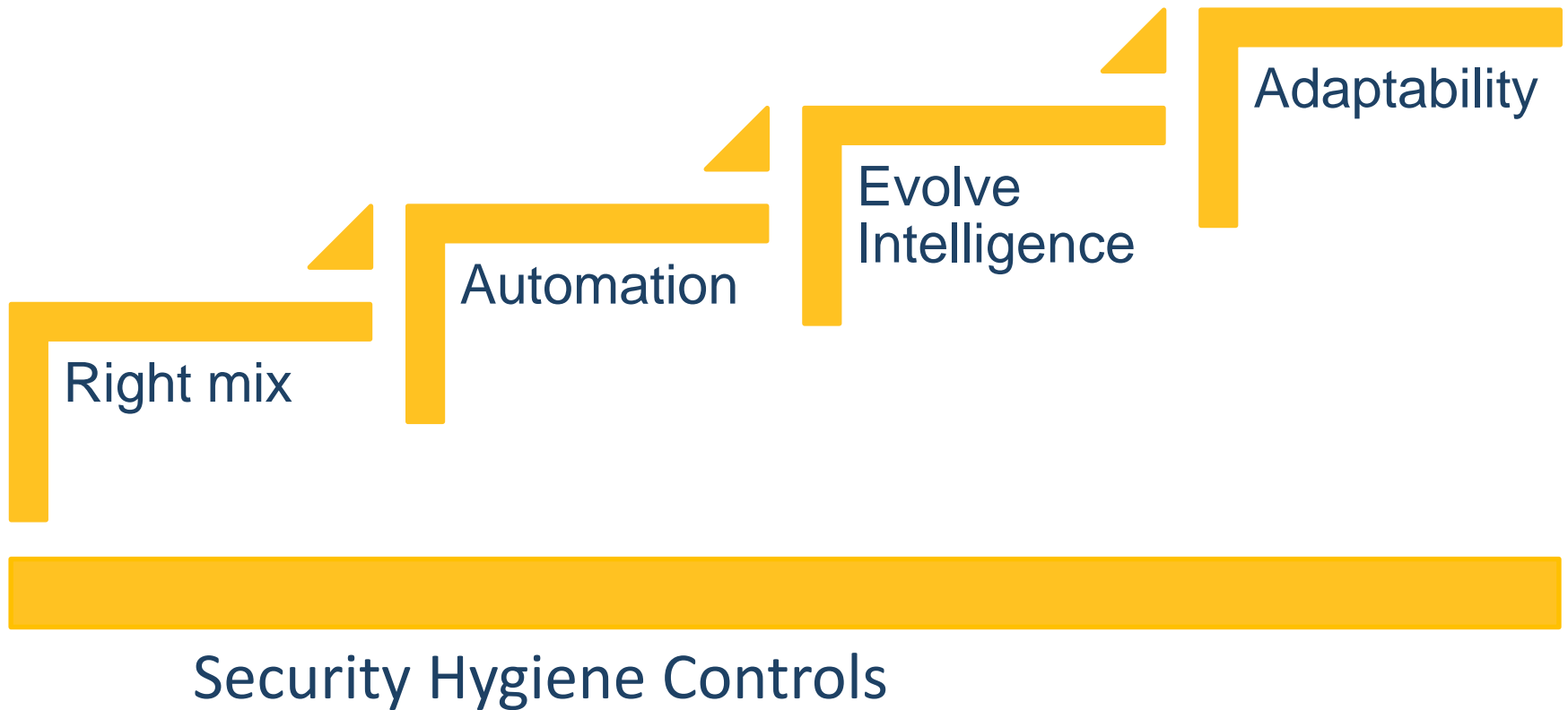
* “Science, Strategy and War: The Strategic Theory of John Boyd”, Frans P.B. Osinga, PP237

FORCE MULTIPLIERS

- Training
- Automation
- Leverage other teams
- Build gates (Architecture)
- Feedback cycle (Architecture)
- Passive defence



NEXT STEPS



SUMMARY - OBSERVATIONS - KEY POINTS



- **People are key**
- **Focus on important things**
- **Leverage others**
- **Feedback loop & adaptation**
- **Utilise force multipliers**

QUESTIONS

