



SØREN EGEDE KNUDSEN

Danish Energy Agency
Denmark

- More than 20 years' experience in cybersecurity
- Worked as the CTO of Ezenta a security company in Denmark in addition to consulting
- Part of the a Managed Detection and Response group, driving the ICS services field
- Henley MBA, GIAC GRID, CCIE

@SorenEKnudsen

The building blocks of good detection and response services for the ICS environment

By:
Søren Egede Knudsen
Chief Advisor
Danish Energy Agency

sek@ens.dk



TM©

FIFA WORLD CUP
RUSSIA 2018

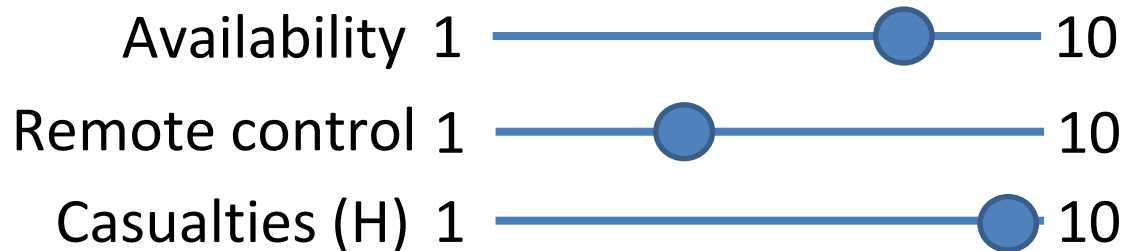
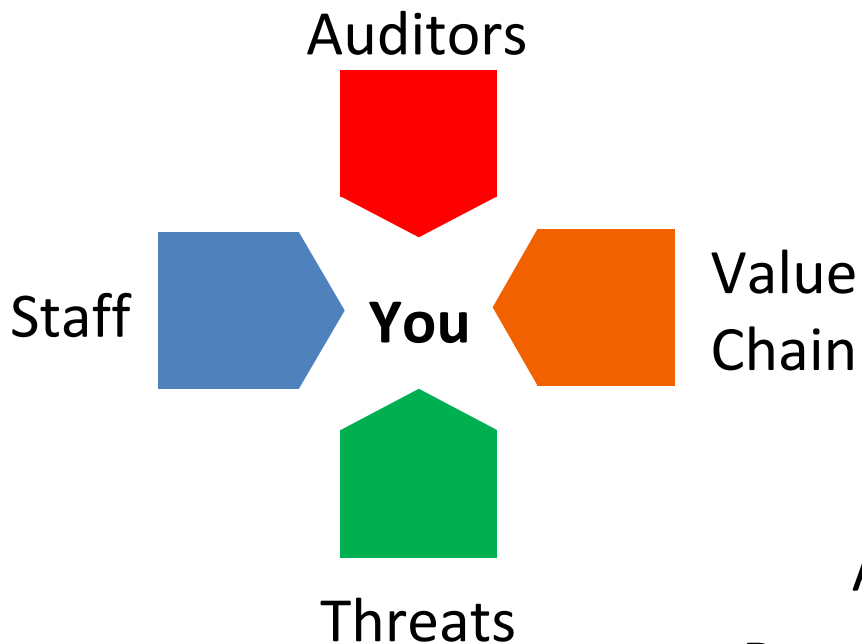
THE TEAM Leadership

Nobody want managers we want leaders!

Understanding the peoples value set are critical



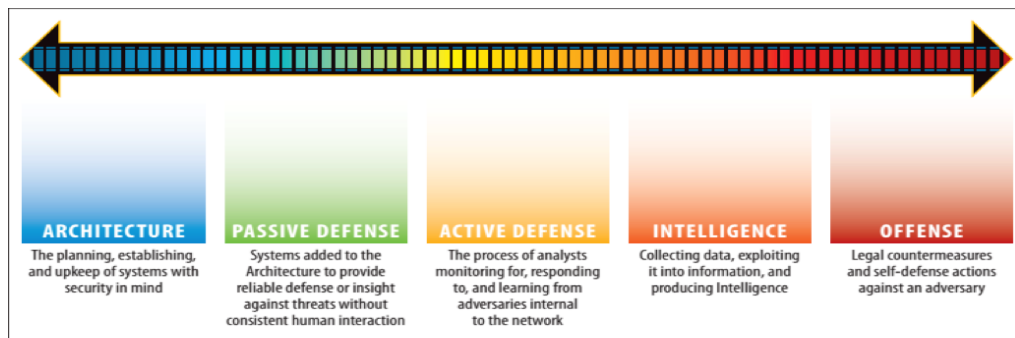
Organisational priorities



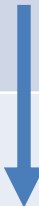
TEAM Setting

Define the needed technical level of the team

Recommended



TEAM Setting

Name	Skills	Personality	
Manager	People, Business and Technical skills and experience. IT and OT.	Transformational leader Common purpose / goal Value based Honest	
Security Network specialist/Analyst	FW, IDS, OT, IT, SIEM, Network	Team player Follow a list Communicative	
OS Security specialist/Analyst	Windows, Linux, application, SIEM, OT		
IR and forensics analyst	OS, Network, pen-test, forensics, OT		Plus: Analytic, Digger
SCADA specialist	IT, OT, SCADA processes and logic		Plus: Process Analytic

Empower the team!

Pitfalls in selecting people

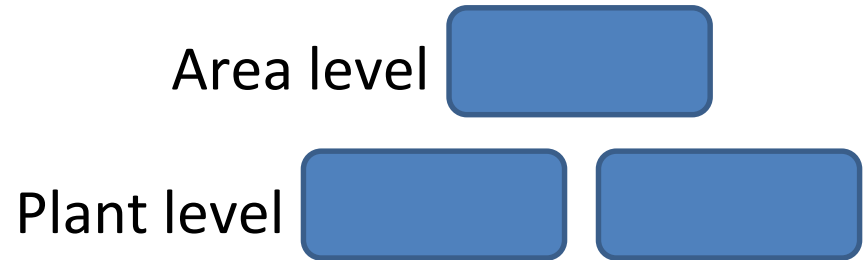
- Selecting “do’ers”
- IT not OT focused
- Only technical knowledge
- Not team player

TEAM Structure

Integrated team (in-house & consultants)

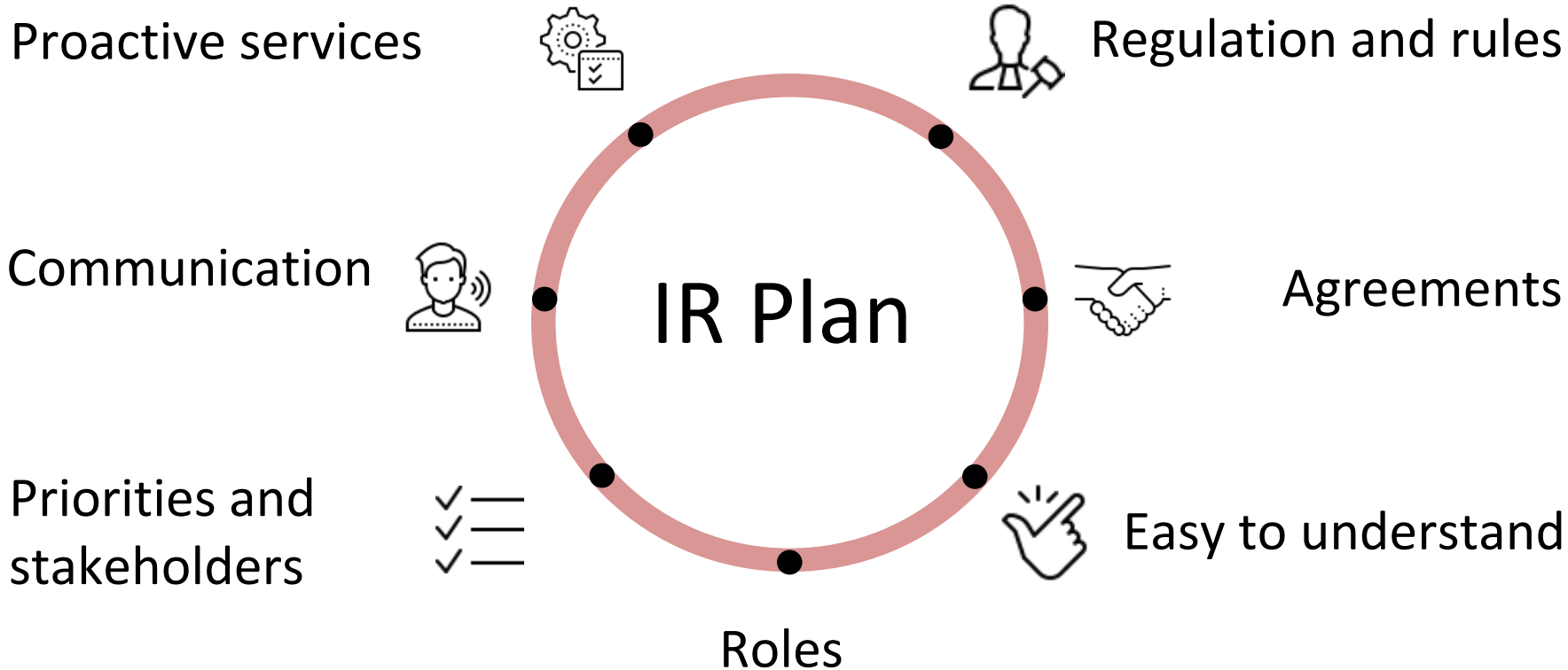


Horizontal vs hieratical team



R=Responsible, A=Accountable, C=Consulted, I=Informed

Incident response plan



Building blocks

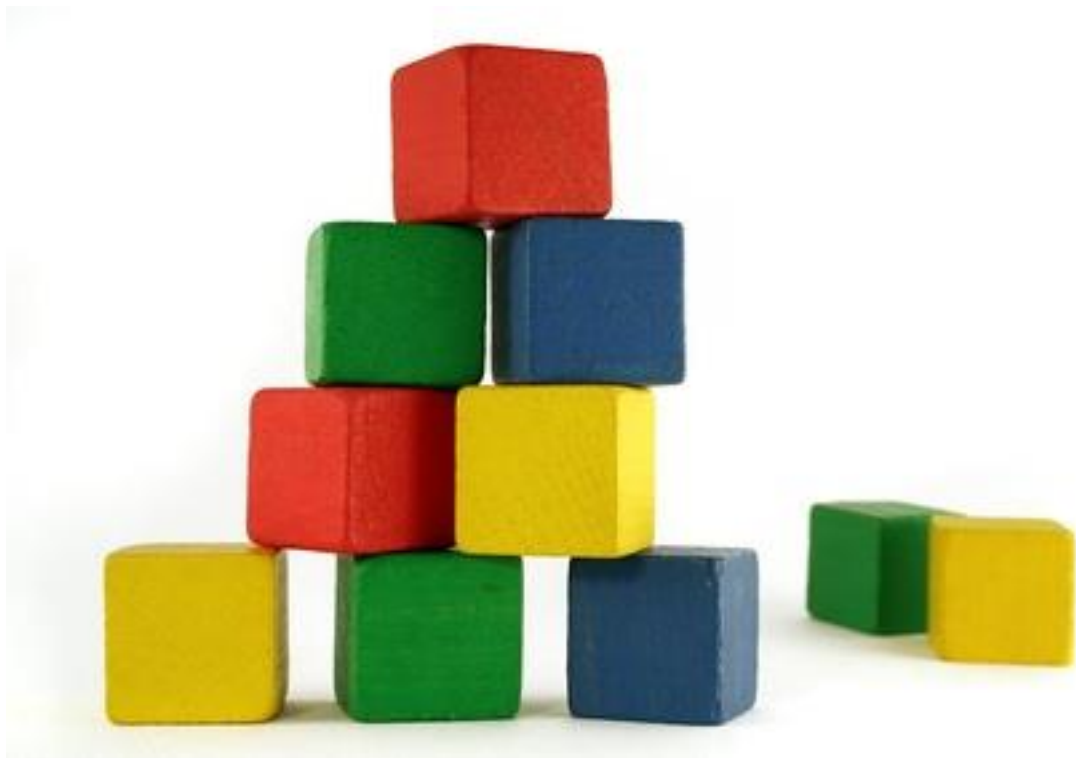
Organisational priorities

leadership

Team members

Skills and experience

Visibility



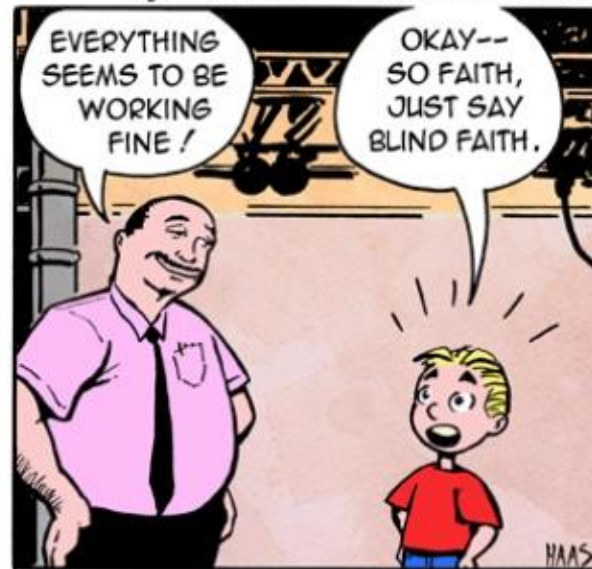
THANK YOU!

ICS visibility

LITTLE BOBBY



by Robert M. Lee and Jeff Haas



APRIL 1, 2018

Incident readiness

Are you ready for an incident?

