


What happens when you build a CTI team in sync with a Red team?

Evolving your adversary playbooks; Incorporating red team findings



Gert-Jan Bruggink

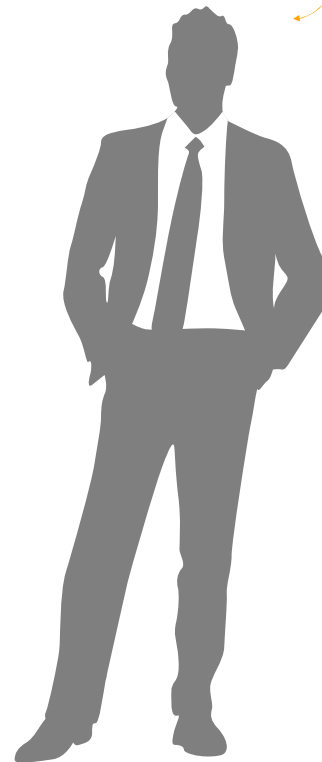
 @gertjanbruggink

SANS Purple Team Summit 2019

This is me

Gert-Jan Bruggink

(without the hair)



Roles

- Manager @ Deloitte Netherlands
- Capability lead cyber threat intelligence
 - Bluetivist



Recent projects

- Intelligence led red teaming exercises
 - Strategic threat assessments
 - CTI capability building



Focus

- Look at the bigger picture, help business understand what's going on and what's next
 - Assisting leaders in making informed decisions by utilizing cyber threat intelligence



Personal goal

- Pioneer new ways to enable business through effective and efficient risk management
- Find and enable synergy between teams



I like

- Do cool projects with cool people
- Stay on top of things. Did I tell you I was in CTI?
- Have loads of fun with the family



I don't like

- If we already get caught during the recce
- Magic tricks. Seriously, they annoy me



Our journey in adversary research

Gather around folks, let me tell you a **story**



Exploring synergy



Lessons learned



Forecast



Exploring synergy

Exploring synergy

Simplified approach to adversaries



5



Exploring synergy

The general CTI approach to adversary tracking



Objective

The eerie void of 'how did they do it'

Achievement

Intrusion & intelligence analysis

The past

The future



IOC research & feeds



Signatures



Adversary playbooks



Digital footprint



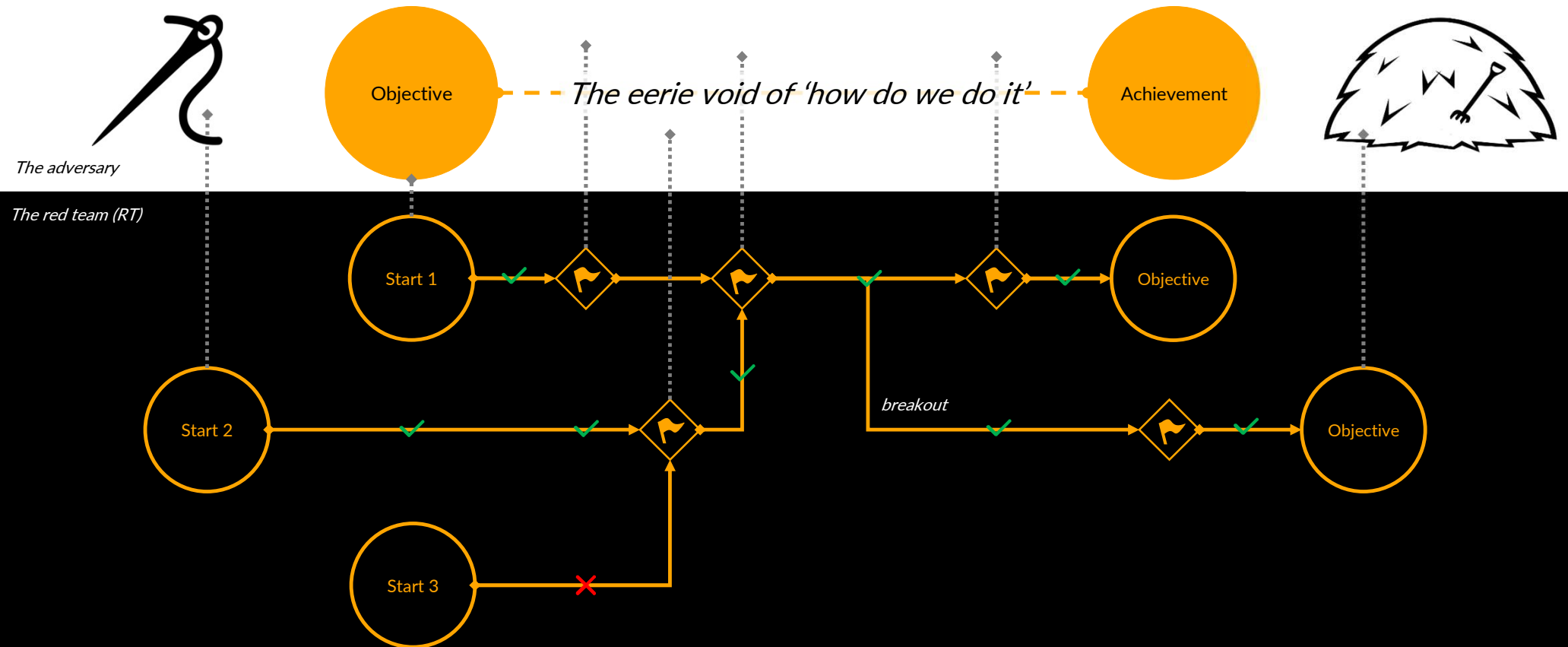
Intelligence products



Threat Libraries

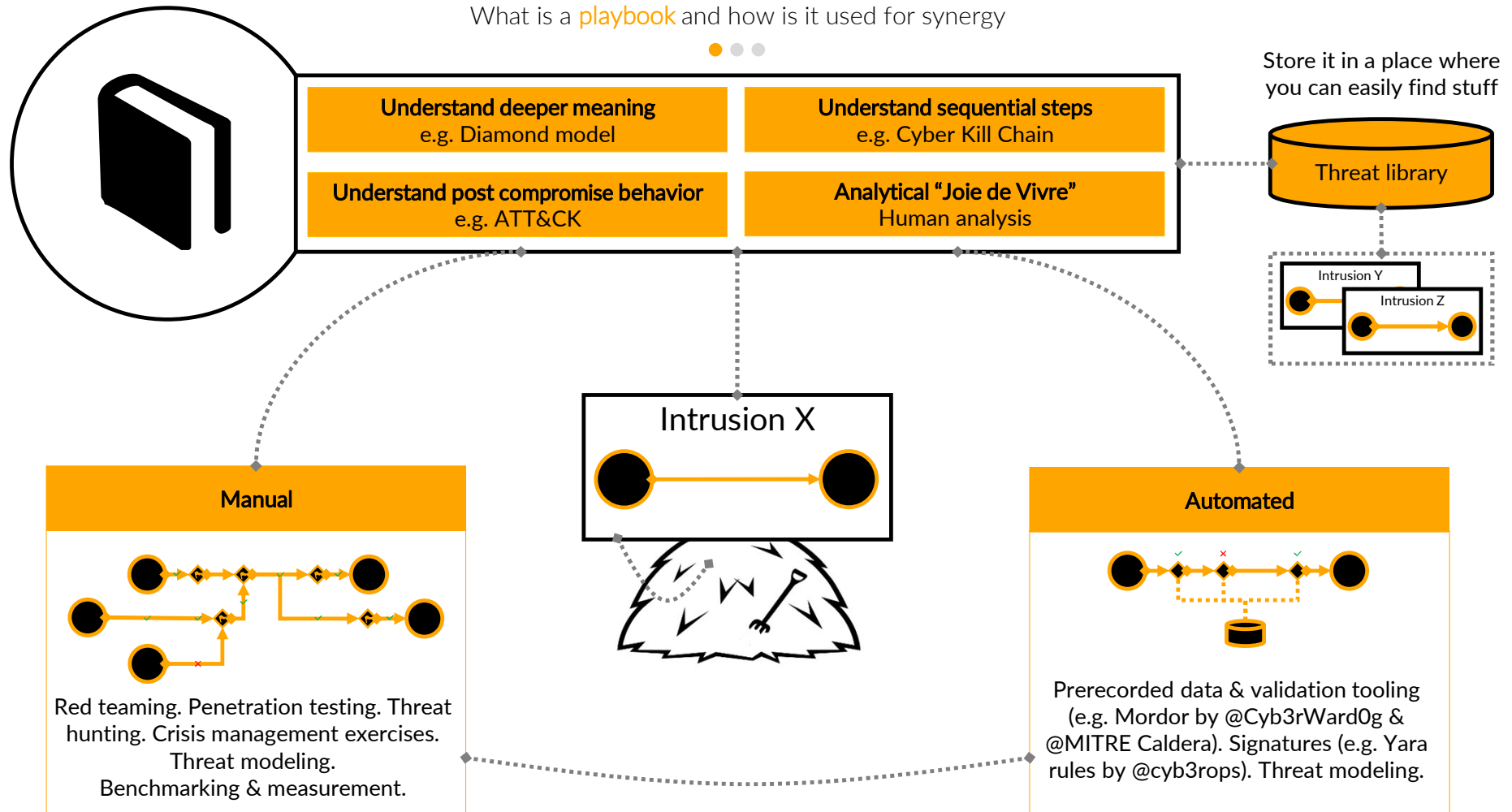
Exploring synergy

The general RT approach to adversary simulation



Establish the playbook

What is a **playbook** and how is it used for synergy

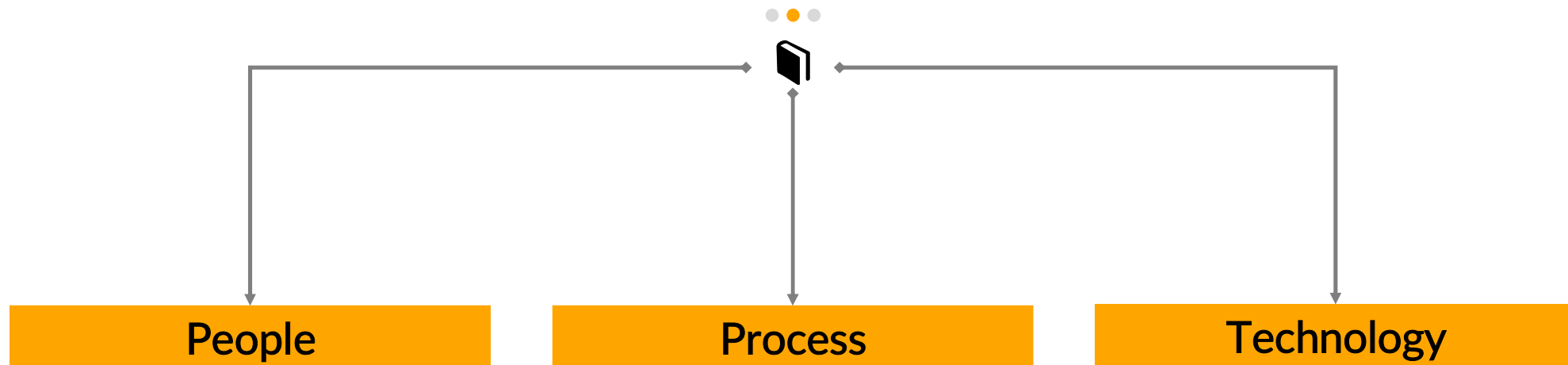




Lessons learned

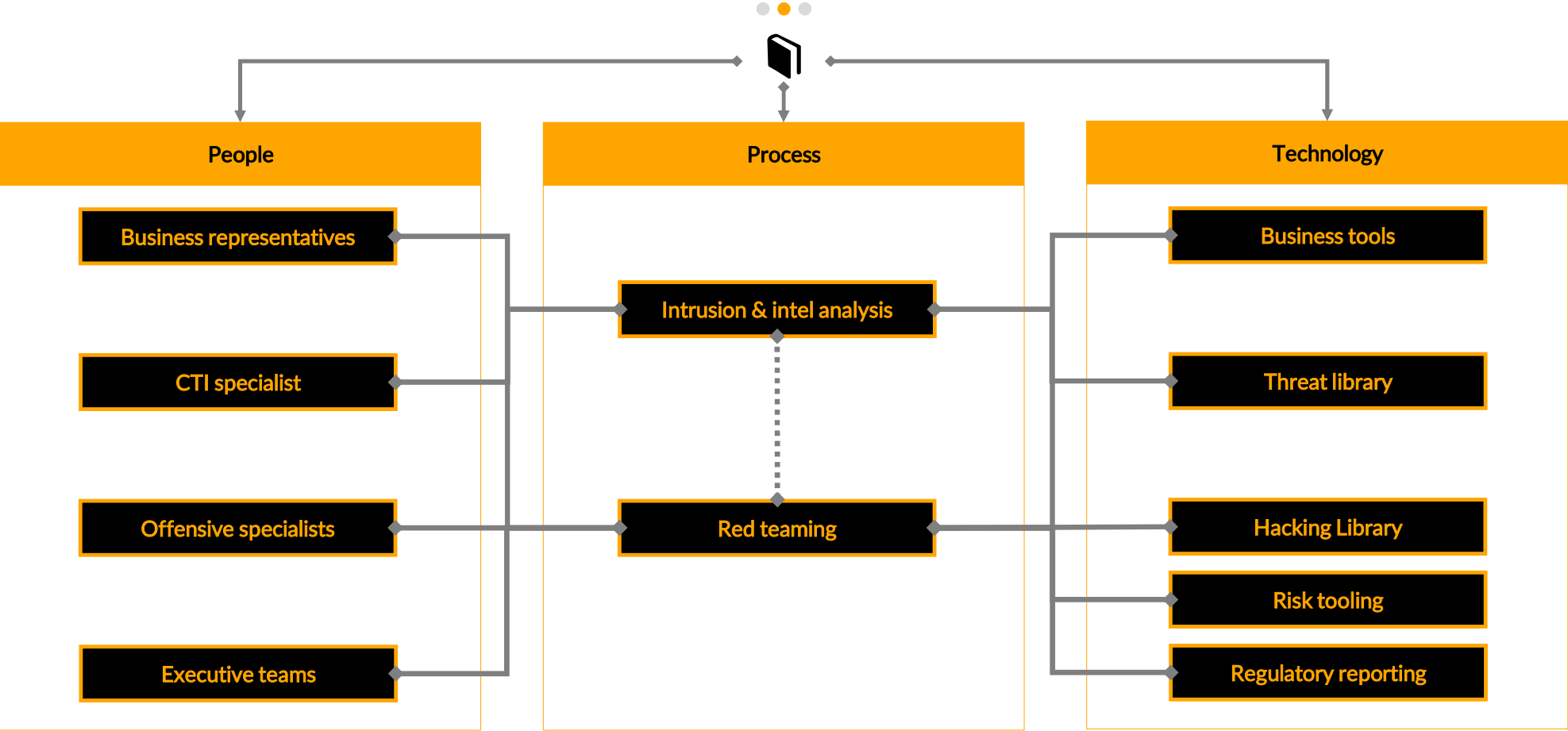
Integration in operations

Pragmatic integration of adversary playbook workflow



Integration in operations example

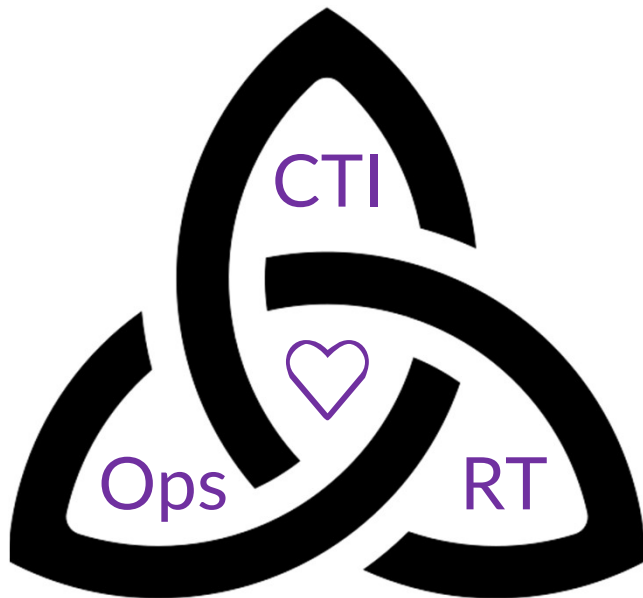
Playbook-based red team scenario's



Four important lessons learned

Evolving adversary playbooks

12



CTI jargon to manage uncertainty is not for everyone

The industries emphasizes IOC research, rather than emphasizing how the research affects specific situations

Setup explicit rules of engagement for purple team exercise, makes discussing RT results way more effective and less emotional

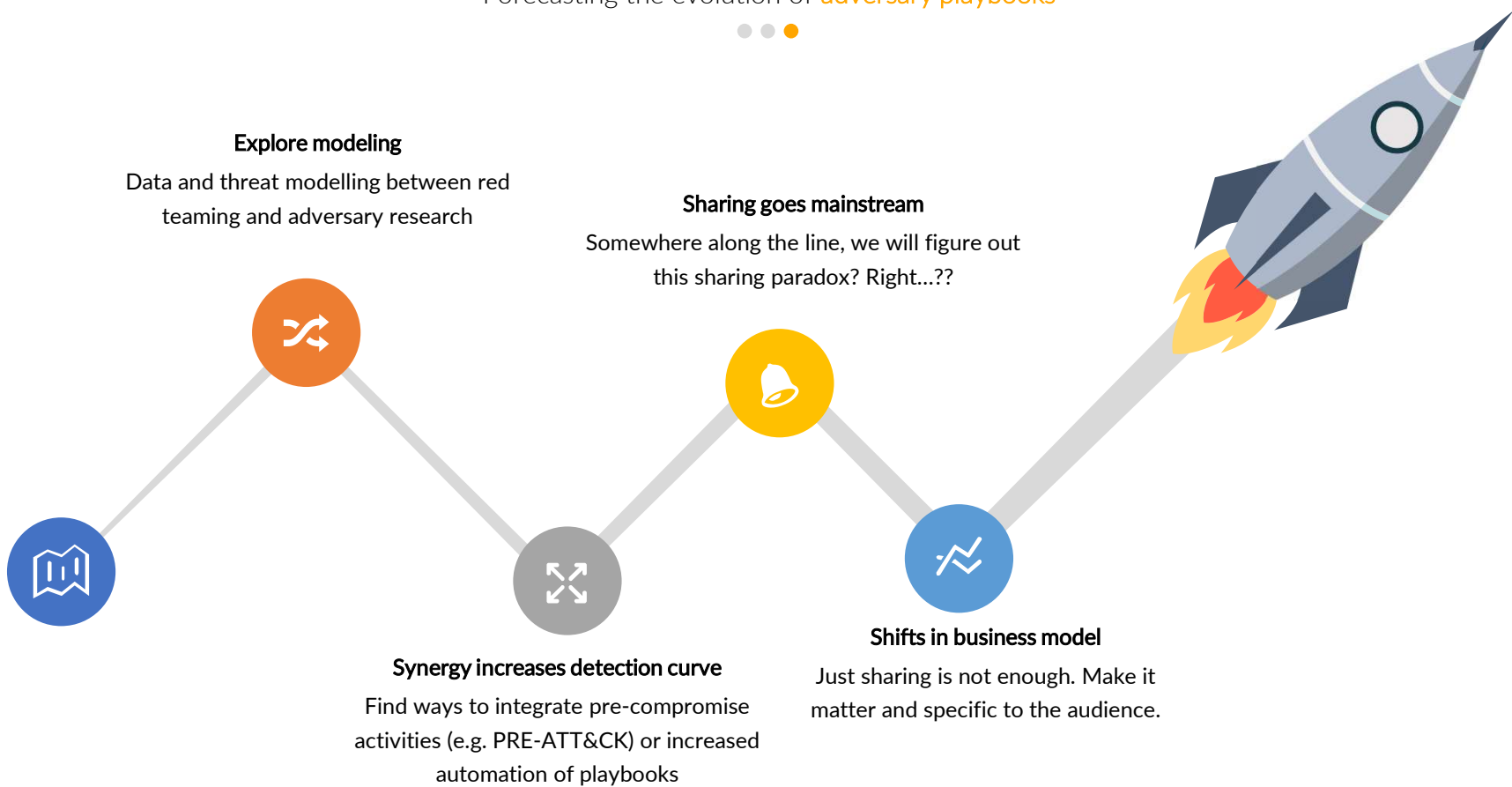
RT findings and indicators are amazing to use for forecasting, we should model it!



Forecast

Future of the field

Forecasting the evolution of **adversary playbooks**



THANK YOU

See you next time!

Gert-Jan Bruggink

Twitter & LinkedIn /gertjanbruggink

Shout out to Givan Kolster & @OlafHartong;
Thx for the support gents!

