ATT&CK ‘Metaverse’

Exploring the limitations of applying ATT&CK

Gert-Jan Bruggink

ATT&CKCON 3.0
29 & 30 March 2022

Why am I here?

- A cyber security ‘metaverse’
- Lessons from the limitations
- Practitioner feedback

Who am I?

Gert-Jan Bruggink

cyber threat cartographer

&

founder Venation

10+ InfoSec.
High tech, manufacturing, financial services, governmental.
Cyber threat intelligence (CTI) based risk management.
Intelligence-led Red Teaming.
Capability building & leadership.
Strategic change through (CTI, SOC & Cyber) transformation programs.
Father x 2, Entrepreneurship, Gaming, Painting, Lego, Meme's.

@gertjanbruggink
github.com/gertjanbruggink
/gertjanbruggink

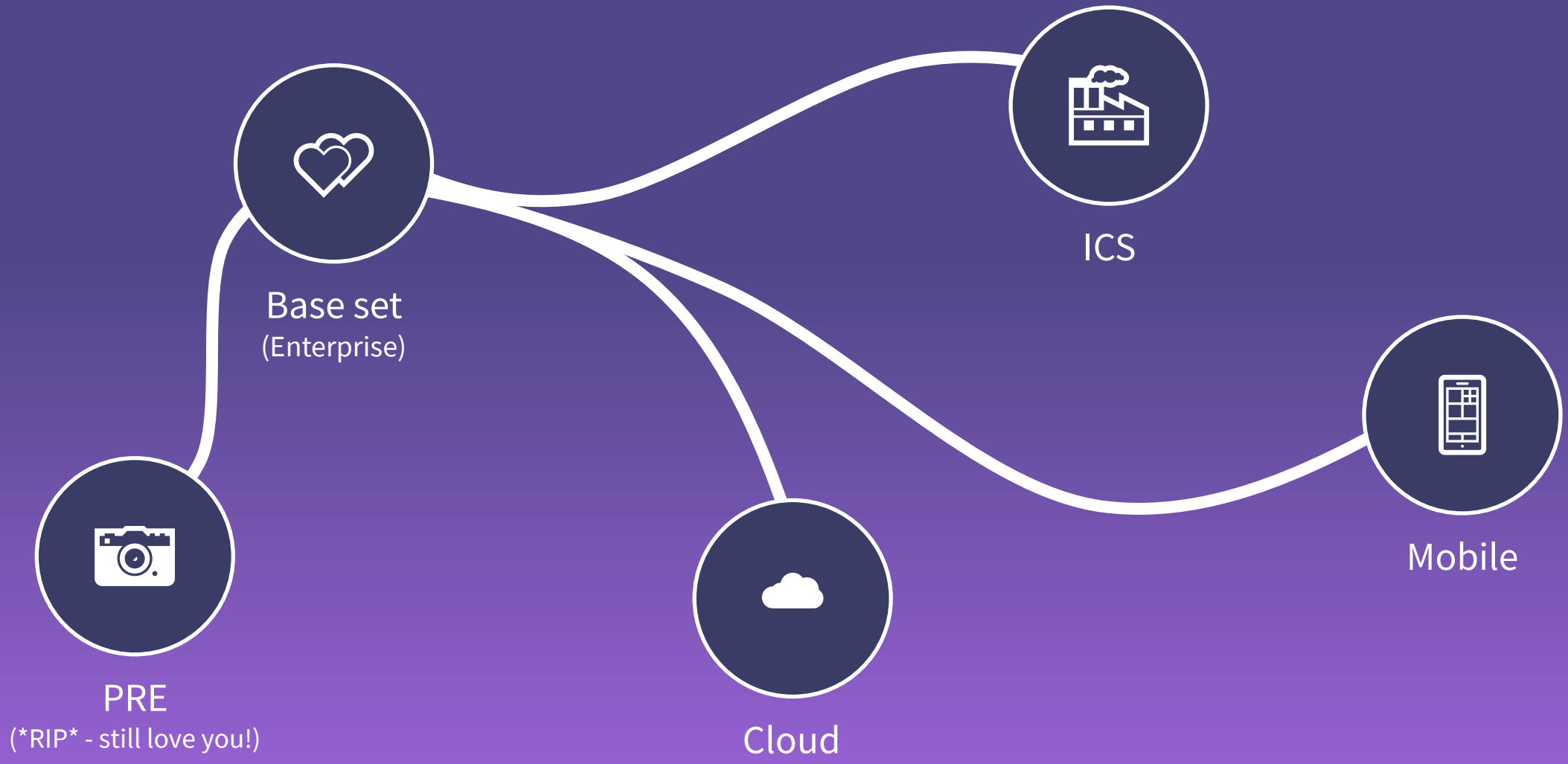
What am I going to talk about?

- ✓ Evolution & lessons learned
- ✓ Adoption & lessons learned
- ✓ Usage & lessons learned

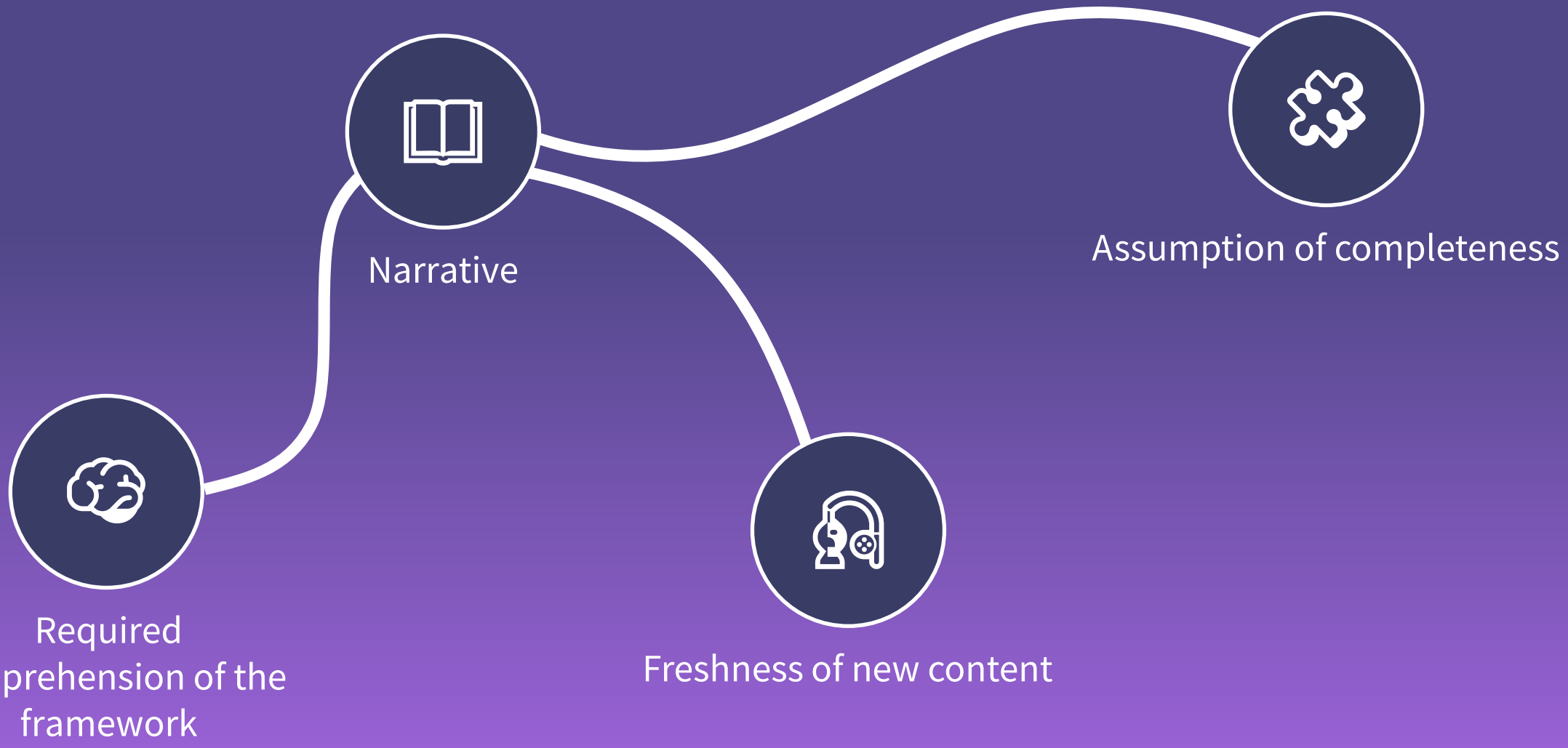
Evolution

The terrifying ‘first look’ at ATT&CK

Constant expansion and structuring



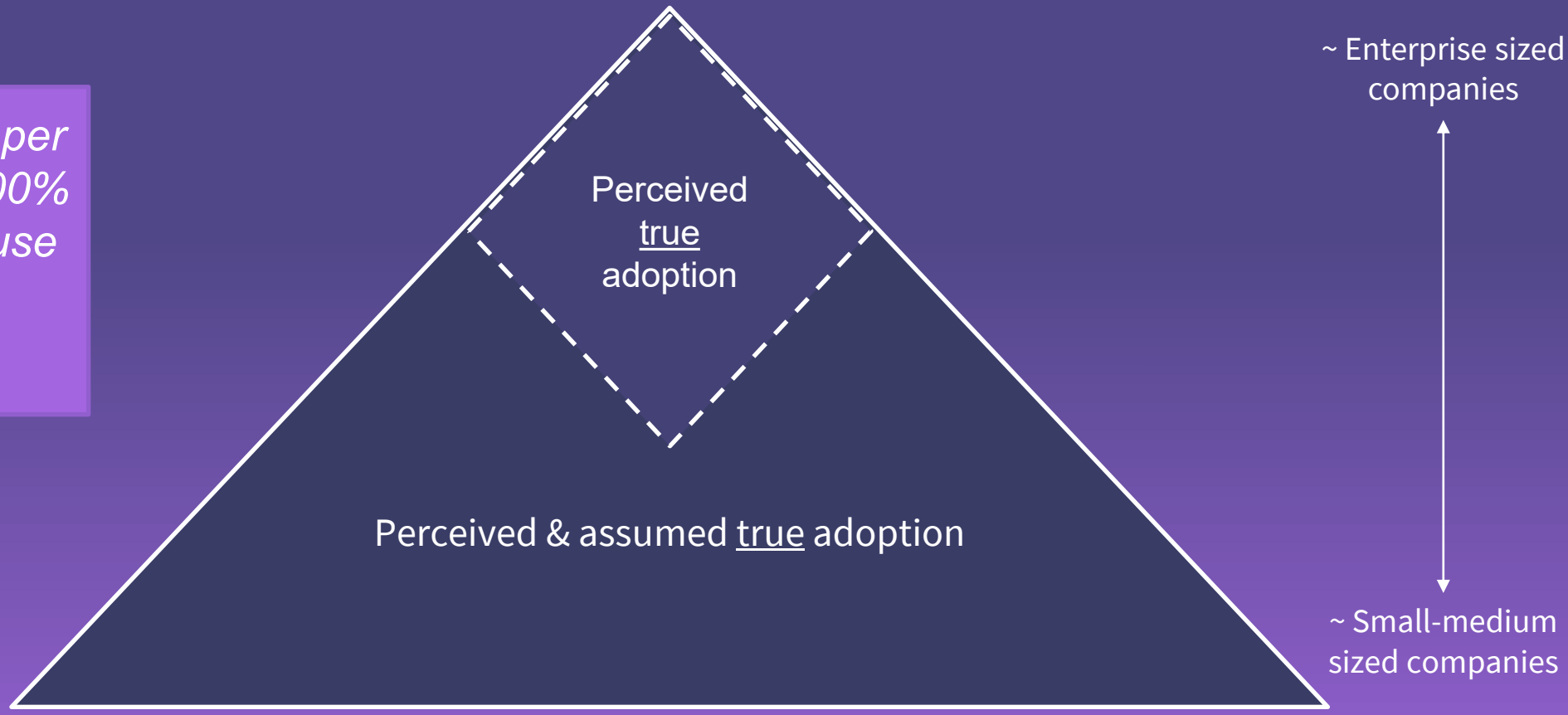
Storytelling using ATT&CK



adoption

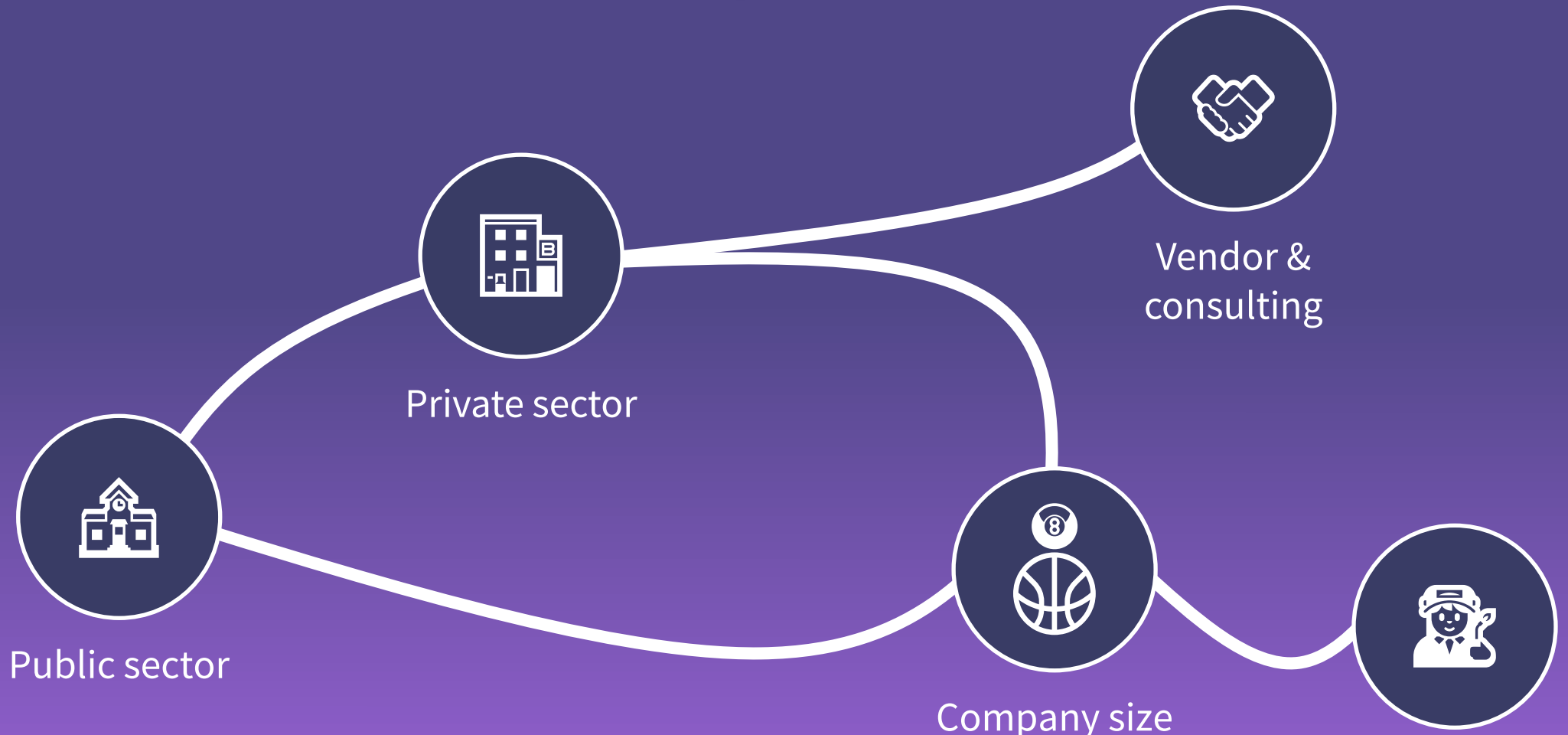
‘how-many-teams-actually-use-ATT&CK’ bias

Research paper “ABC”: 80-100% companies use ATT&CK



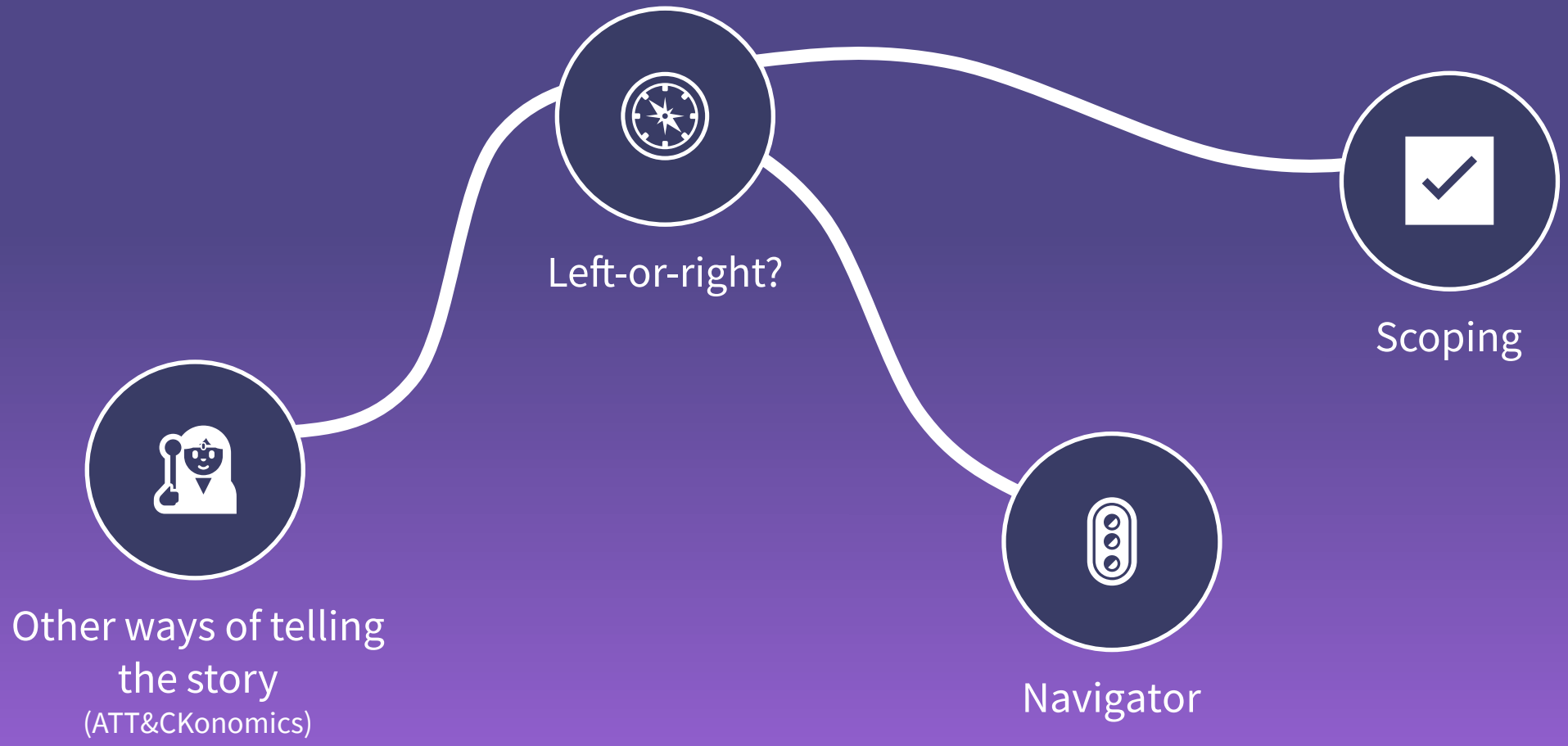
Do not assume everyone is using the framework - or uses it in the intended way

Where is the adoption (more-or-less)



Applications outside of operations

Main motivation usecase: prioritization



Usage

Setting the scene: example starting points

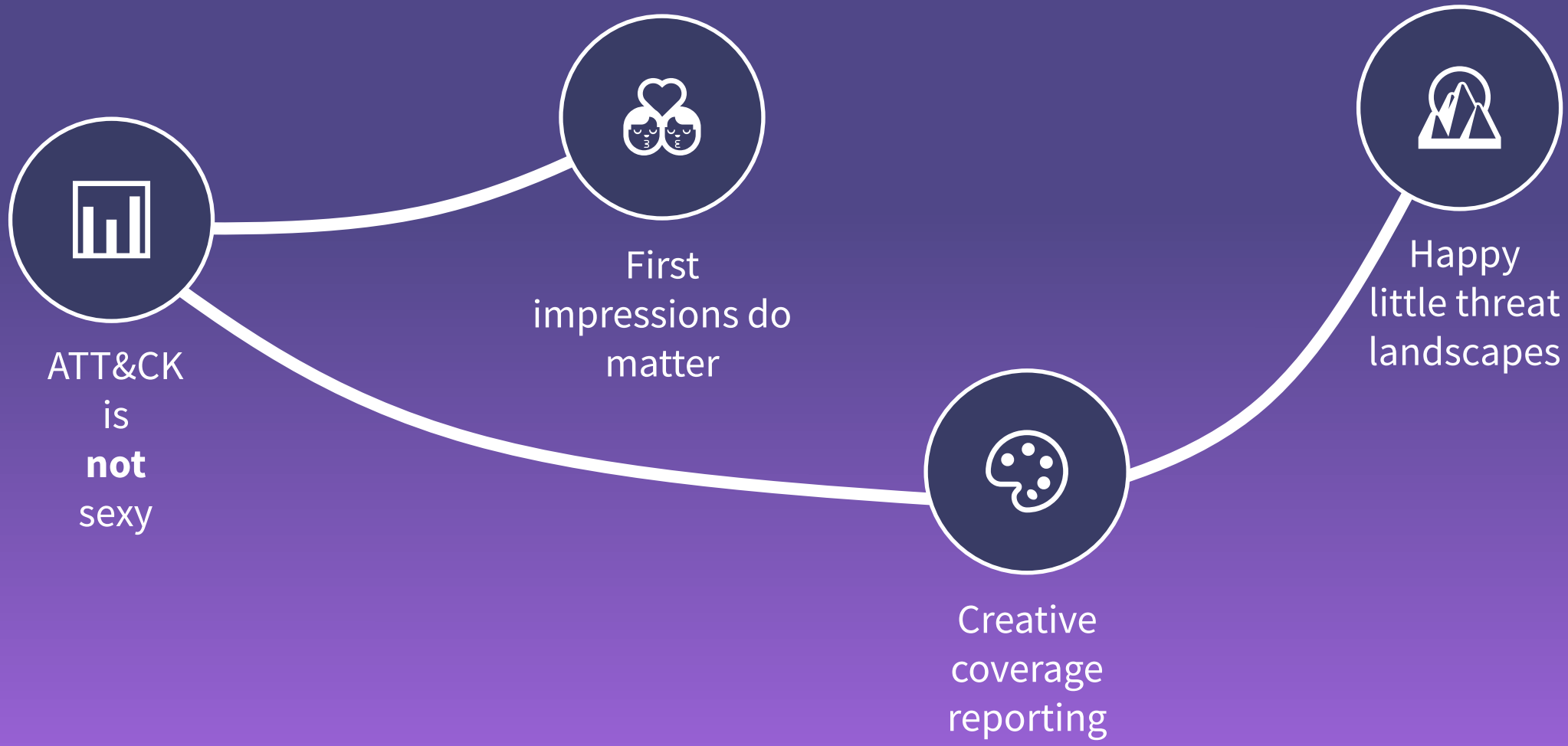
Teams new to ATT&CK

- How does the framework help me tell a better story to my leadership?
- Can we use the framework to help us do basics better?
- Will using it save us costs along the way?

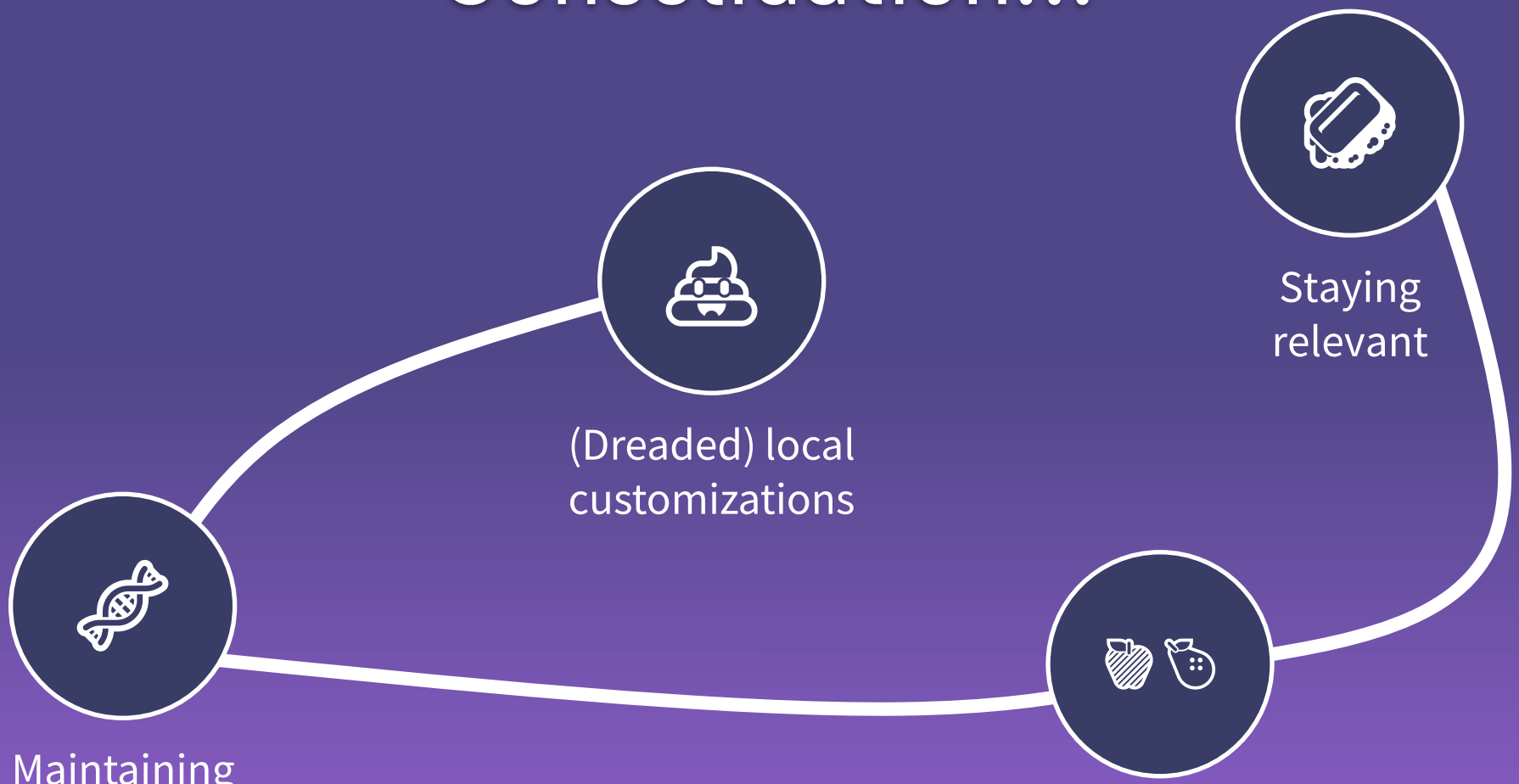
Teams seasoned in using ATT&CK

- Where will the framework give better context/nuance in attacks against similar companies?
- What test scenarios should be prioritized when validation controls with our capabilities (e.g. hunting, red teaming)?
- Can you prepare a cost-effectiveness assessment of our controls, compared to adversaries (and techniques) targeting our vertical?

The dreaded ‘bingo card’ visuals



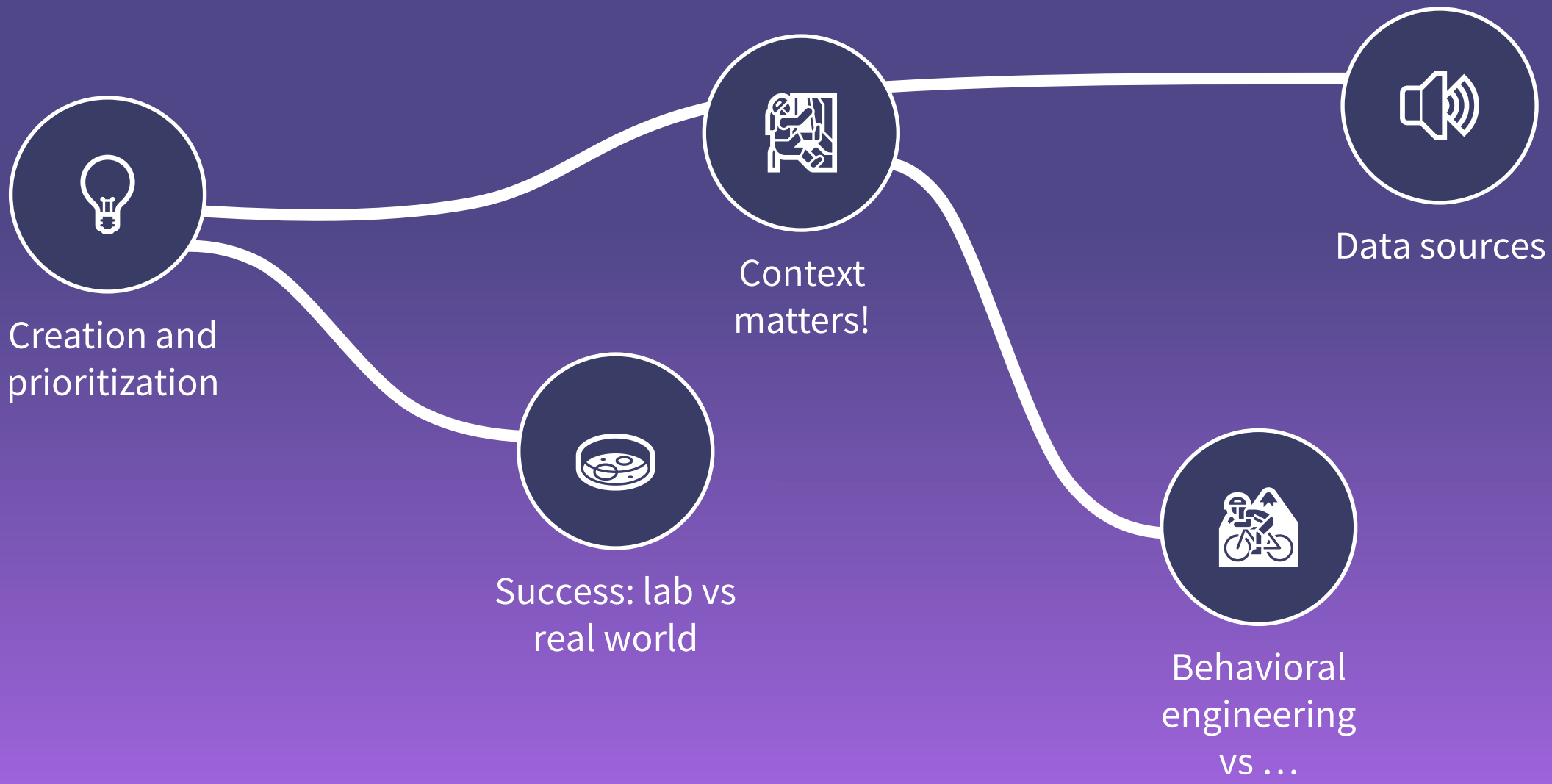
Consolidation...



The ‘TTP’* discussion

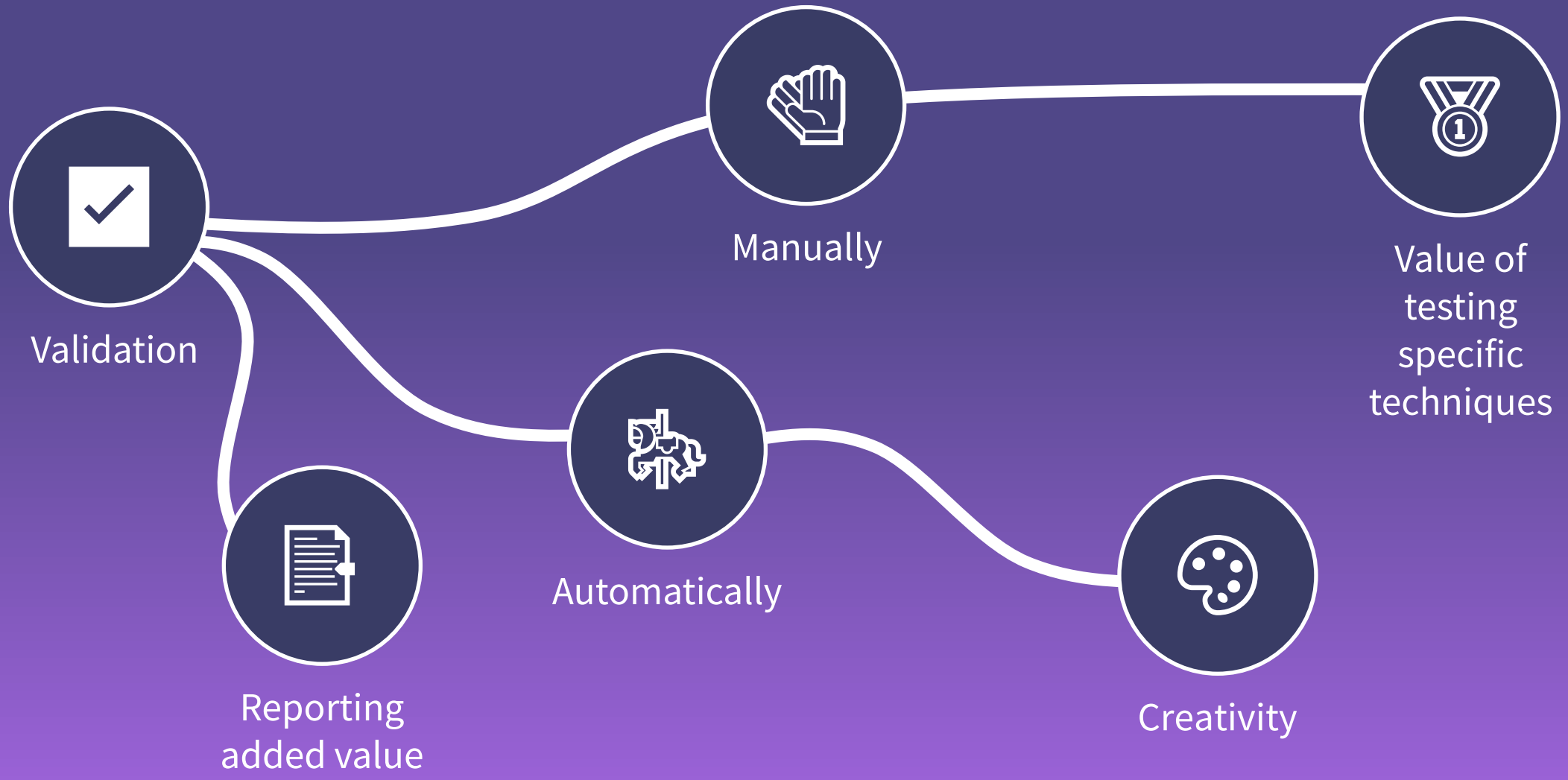
*Tactics, Techniques and Procedures

Engineering your hypotheses



Building scenarios to provide context

Validating scenarios



The future of ATT&CK remains the community

People

(e.g. continue expanding the education the ‘adopting’ community)

Process

(e.g. sharing feedback)

Technology

(e.g. vendor ecosystem)

Recap & course of action

- Don’t complain, just provide feedback.
- Contribute == getting creds
- The community decides ATT&CK direction: this is widely underestimated.

Consider today

If you would revisit our ATT&CK usage today:

- ✓ What is our level of (true) adoption of the framework?
- ✓ How are we telling the right, nuanced, story - from procedure- to board room?

Let’s continue expanding the ATT&CK ‘metaverse’!

Gert-Jan Bruggink
gertjanbruggink@venation.digital

@gertjanbruggink
/gertjanbruggink