

To DevSecOps or not to DevSecOps

Using an Archetype-based model of
Security in DevOps

Mario Platt @madplatt
Consultant - Interim CISO - vCISO -
CISO Advisor

The 2 schools of thought

DevSecOps

 **Abhay Bhargav** @abhaybhargav · Feb 24, 2019

Replying to @dinodaizovi

For one, **devsecops** fosters (or at least aims to) more collaboration with cross functional teams than traditional enterprise security constructs. Working with cross functional teams leads to a codified knowledge base (automation) and the cycle continues. 1/

1 1 1 1 1

 **Dino A. Dai Zovi** @dinodaizovi · Jul 21, 2019

Replying to @bascule and @thephreck

Yeah, I feel like a lot of "**DevSecOps**" still doesn't quite get the most important aspect of having security *be* engineering teams to increase empathy. Working to secure the org using the same tools and same environment prevents "do as I say, not as I do."

1 1 1 6 1

 **Avi Douglen** @sec_tigger · Dec 5, 2019

Replying to @secfigo @EndlessMason and 2 others

Absolutely agree with this! For now, we still need to treat it like something on its own - because that's what it is, right now. But it shouldn't be, and that is what we need to be working towards, when **DevSecOps** is not a thing.

1 1 1 2 1

 **Kelly Shortridge @ RSAC** @swagitda_ · Jun 5, 2019

Replying to @swagitda_ @anton_chuvakin and @nicolefv

My definition of **DevSecOps** is "a marketing term invented for security professionals who don't understand how to work with DevOps but who want to preserve their relevancy without real effort, ideally by buying a solution they understand with a new shiny label"

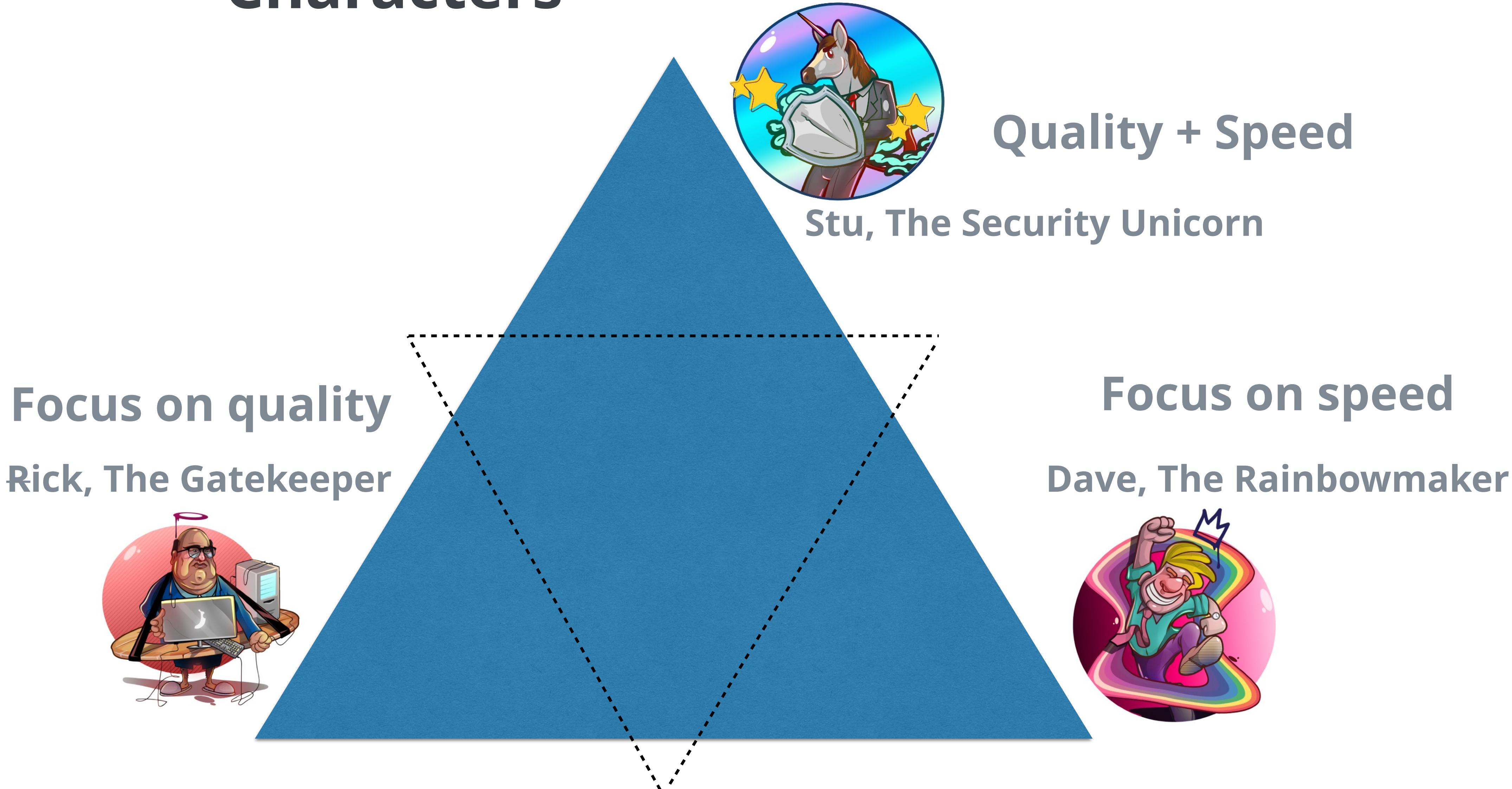
7 7 16 1

**Can ‘DevSecOps’ be useful to
anyone else ?**

Control & Governance functions

Engineering organisation

DevOps Security Archetype model - Characters



DevOps Security Archetype model - Organisations / Teams



The Security Unicorns

The Gatekeepers



The Rainbowmakers



Meet Dave and his team of Rainbowmakers



Dave and the teams aren't negligent or stupid.

They lack **contextual awareness** to do better.

Process, social practice and cognitive load
considerations are failing THEM

Meet Dave and his team of Rainbowmakers



Essential characteristics:

- **No integrated security telemetry**
- **Avoids engagement with Compliance**
- **No secure baselines or modelling of threats**
- **Limited automated testing overall**
- **No product level security reporting**
- **Security is someone else's job, or output of pentests/audits**

Meet Rick and his team of Gatekeepers



Dick and the teams aren't thick or business averse

They **lack understanding of control reliance** in a DevOps world and have **inertia due to past success** of their current model

Team Topologies and poor traceability from technical checks to Compliance objectives are failing THEM

Meet Rick and his team of Gatekeepers



Essential characteristics:

- **Gated processes supported by committees and Review Boards**
- **Limited understanding and trust of modern development practices & engineers**
- **Policies and standards developed outside of Engineering context**
- **Lack of technical knowledge, or worse, outdated threat models**

Meet Stu and his team of Security Unicorns



Stu and the teams are.... OK :)

They have a great Engineering culture and are a learning organisation.

Compliance colleagues **don't work in silos**, but **collaborate to establish process and then trust** that the teams are focused in developing quality software

Meet Stu and his team of Security Unicorns



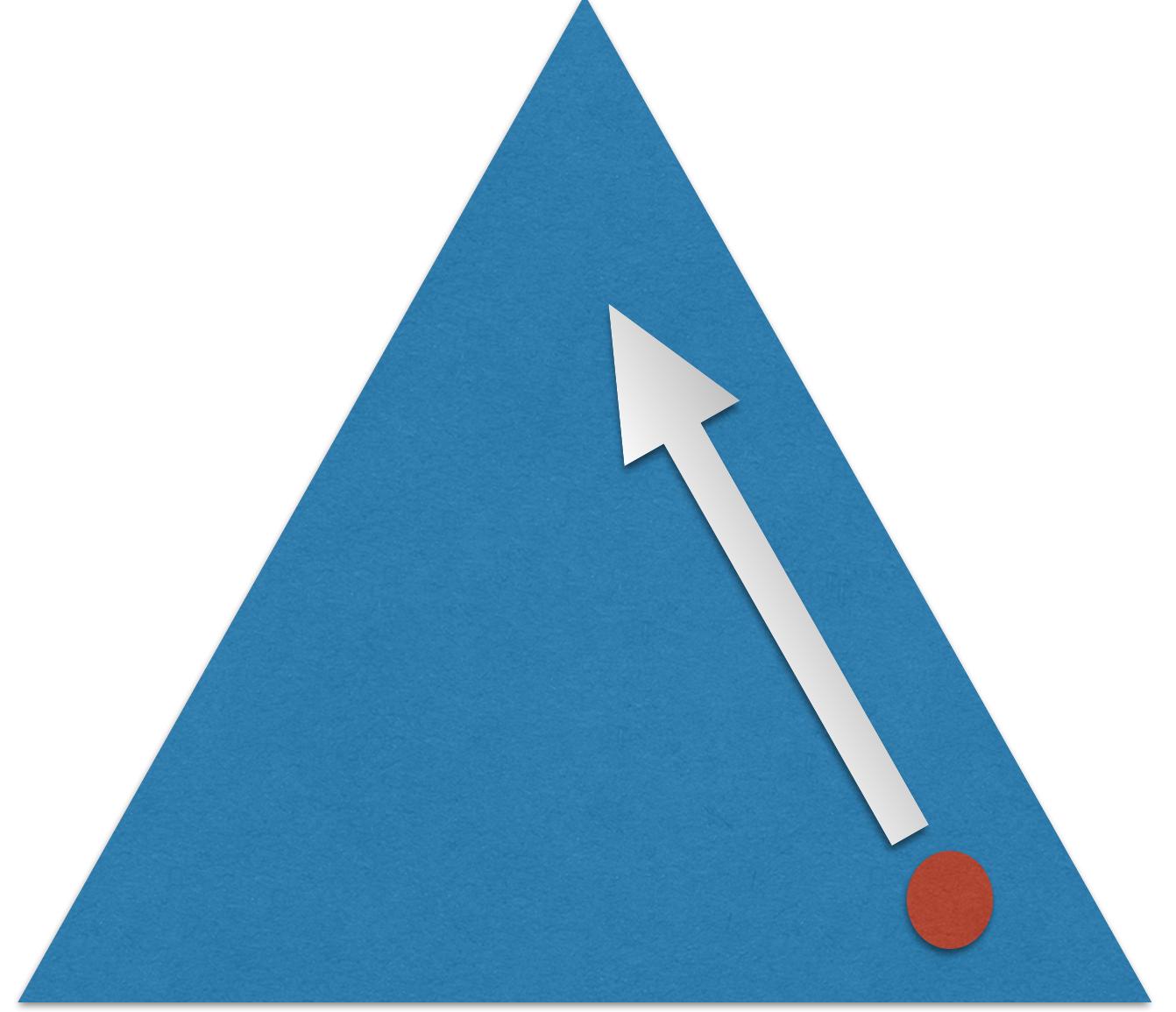
Essential characteristics:

- **Security is embedded into DevOps practices**
- **Security is an element of product/service quality**
- **Teams keep up to date threat models of what they build**
- **Their process has the right security at the right time.**
- **Compliance IS Code**
- **Less Command and Control from Compliance, more collaboration**

Patterns of Constraints

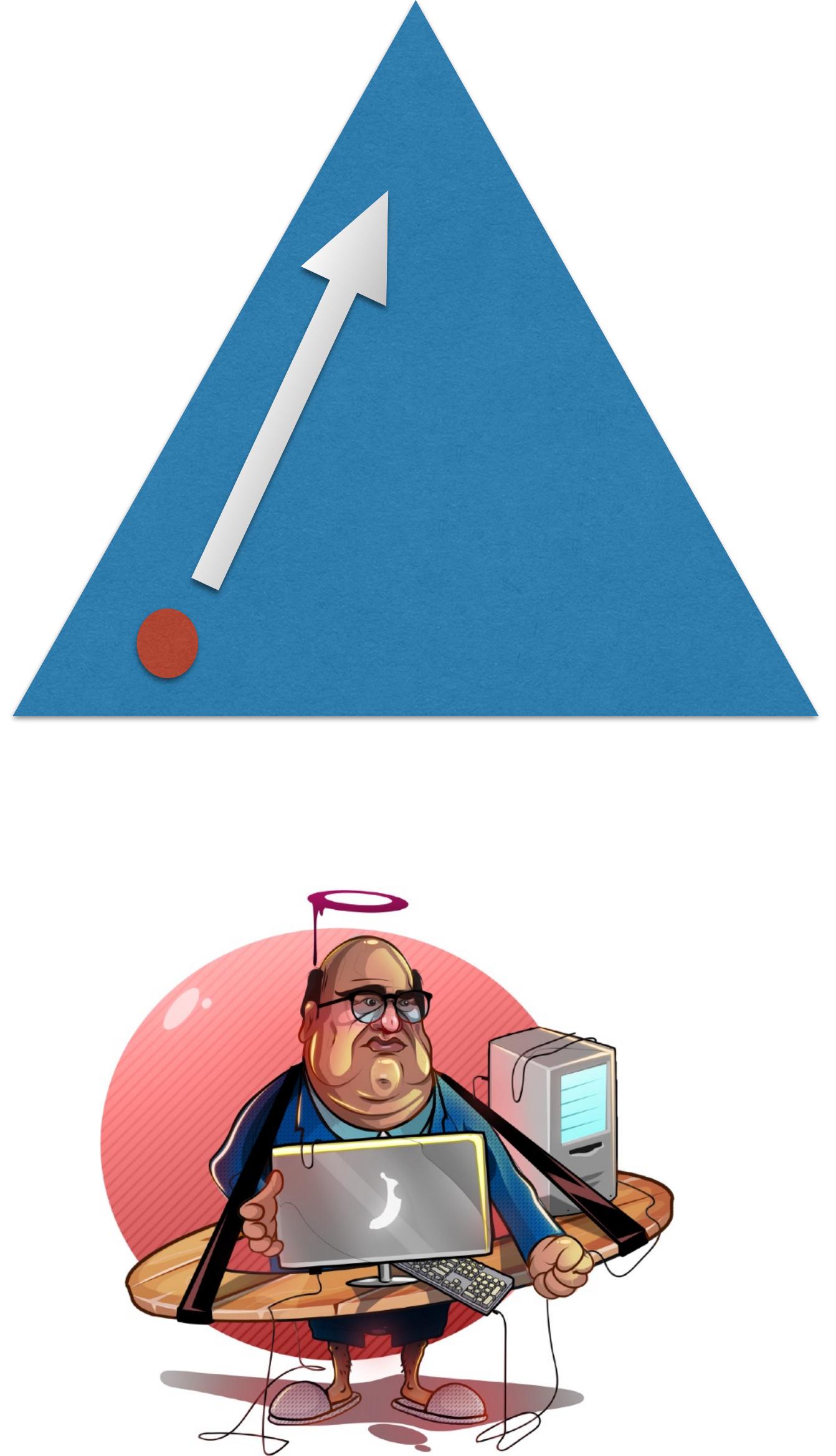
Rainbowmaker constraints

- **Lack of Security Telemetry**
- **Product Management security visibility**
- **Security Expertise by DevOps and Software Engineers**
- **Poor Process assurance and practices**
- **Low sense of agency and ownership for security**



Gatekeeper constraints

- Assignment of security responsibilities
- Spending money on the wrong things
- Gated processes and out-of-band approvals
- Control reliance mismatches
- Policy ISN'T Code
- Command and control culture
- Inertia due to past success



The Communication Challenge



**Management systems
Practices and stories
Language used**



Management systems

“However you define [security] will influence your choice of things you measure - and vice versa!

What you measure, may very well become your definition of [security], whether you want this or not”

Adapted from Busch



ISMS - Policies, Standards, Procedures
Risk register and risk treatment plans
Compliance standards

JIRA (or other case management)
Observability tooling and alerting
CI/CD and Version Control systems

And the language is different too



Control testing
Testing procedures
Evidence review
Checklists and spreadsheets
Compliance to
Risk analysis and uncertainty

Control... blah blah
control.... Blah....
Governance... blah... Risks....
Blah... Compliance....blah blah
Boogey man at the door

Wall of Confusion and Despair

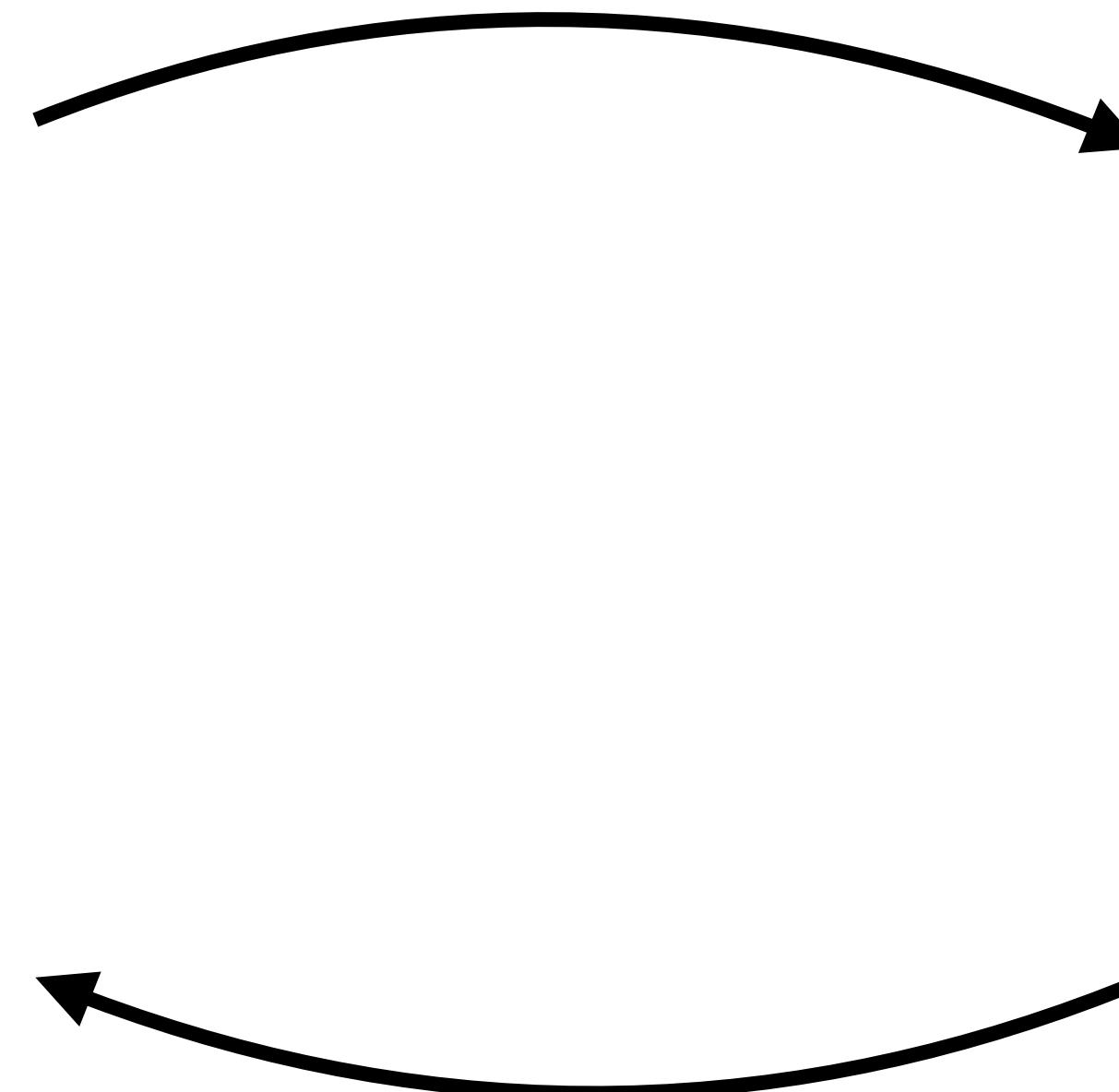


Code Tools
Processes and procedures
Delivery artefacts
Specifications
Sprints and Stories

Features... bah blah... that
looks cool.... Blah blah...
Speed.... Argh can't get that
function to work blah blah
They won't get out of the
way...

Uncontextualised Policies Syndrome

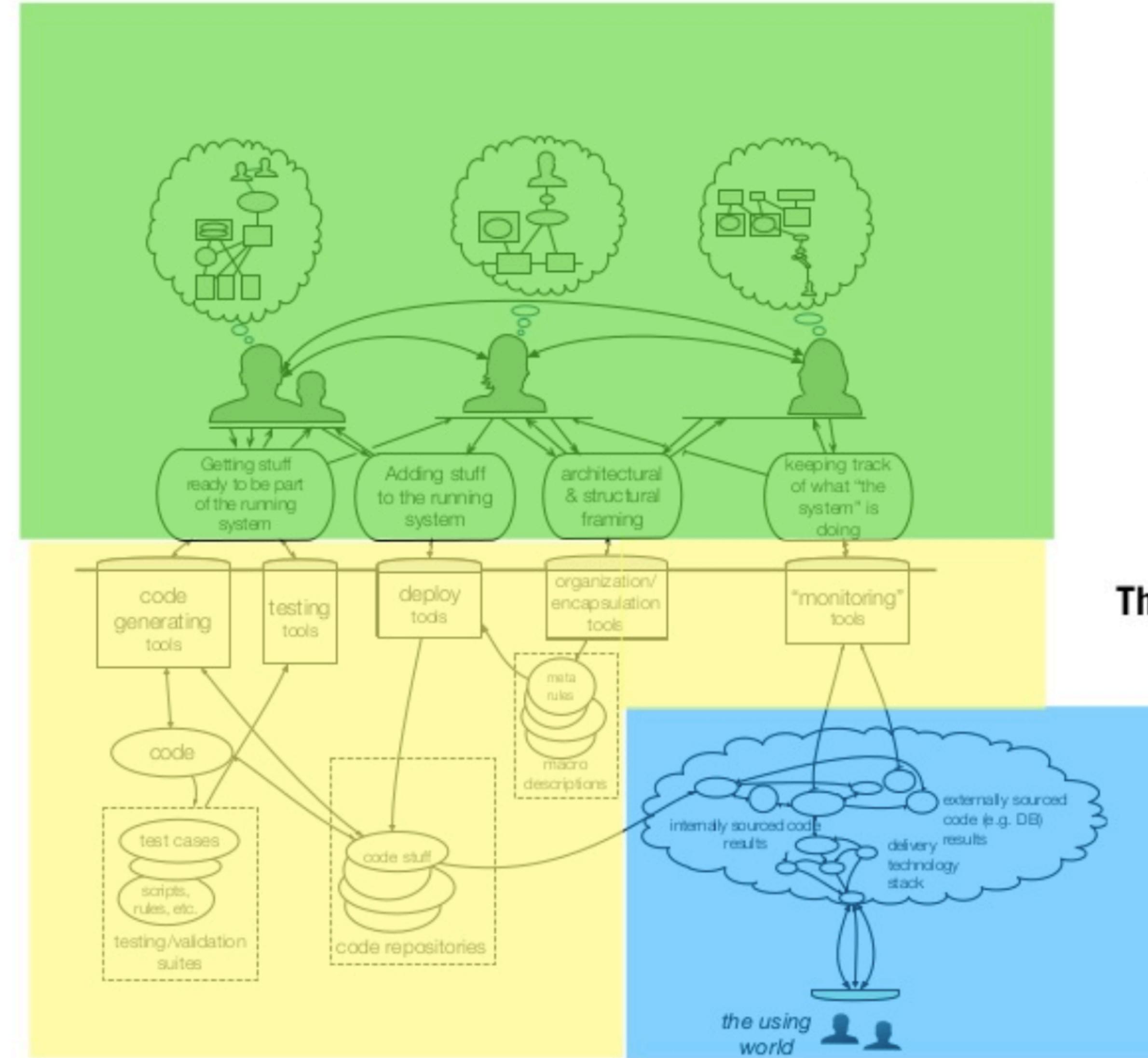
I've written policies
They're really good because I was technical a decade ago



Which policies and where ?
Those patterns don't make sense anymore. What are you on about ?

They see the system differently.

They say the same names, but they mean different things



***The Work Is Done
Here***

**The Stuff You Build and
Maintain With**

**Your Product Or
Service**

In service of stakeholder needs



Spectrum between Efficiency and Thoroughness
Hollnagel ETTO Principle



Executive Due-diligence
Meeting audit and compliance requirements
Meet contractual obligations

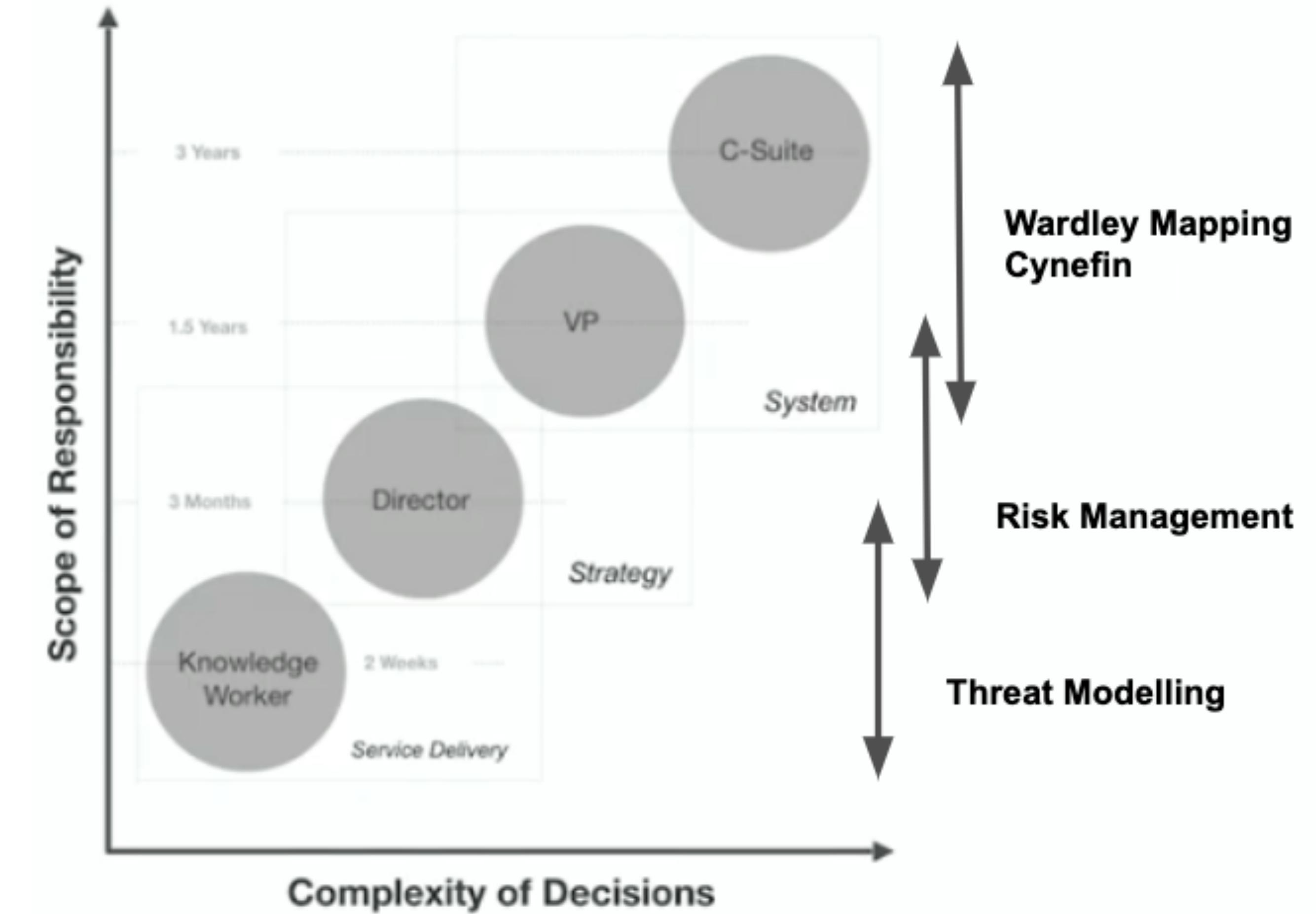


Deliver product features
Meet roadmap and client obligations
Maintain stable systems
Drive efficiency in development and operations

Complexity of decisions vs Scope of responsibility

The timespan of their narratives are different.

Sprints vs managing risks

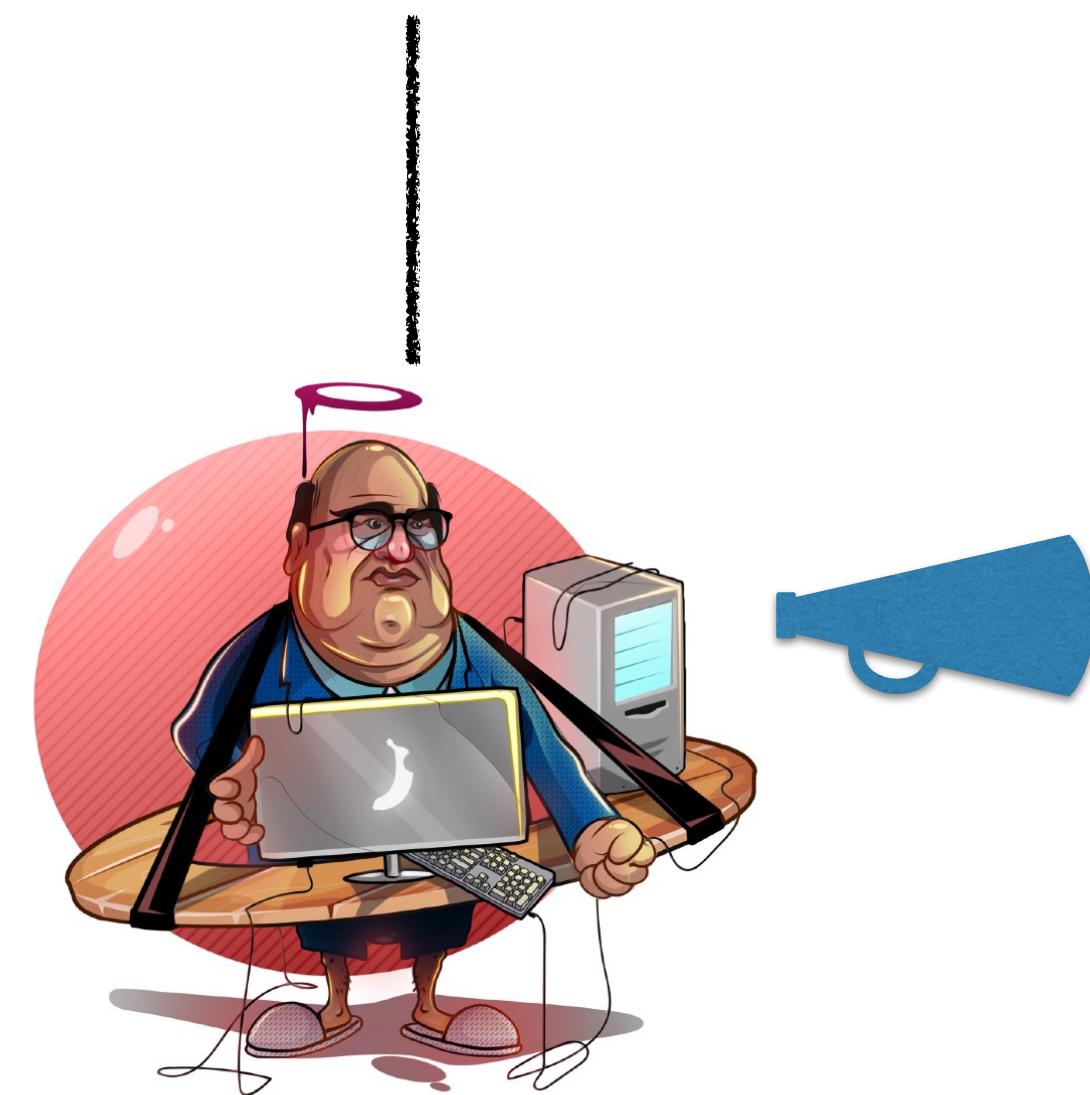


Requirements



OWASP

Application Security Verification Standard 4.0



Helping communicate
between different mental
models

Mapping and traceability

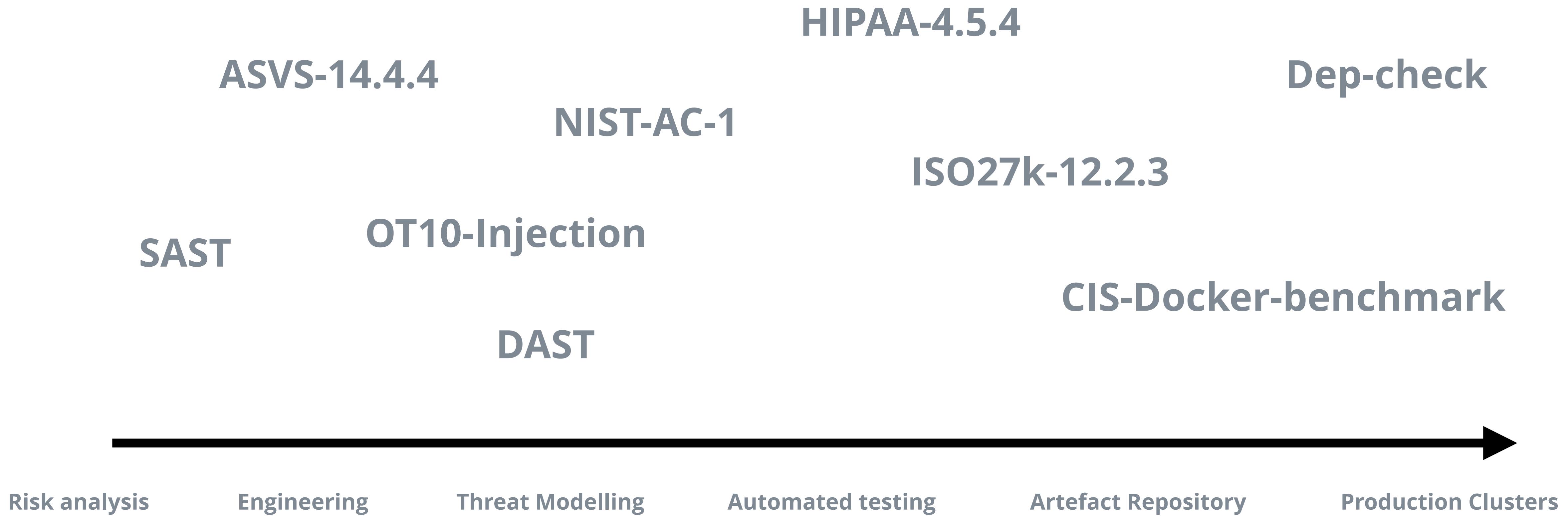
Implementation



Life is too short · AppSec is tough · Cheat!

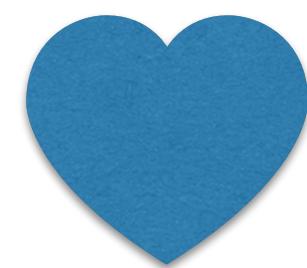


Use metadata for traceability glue



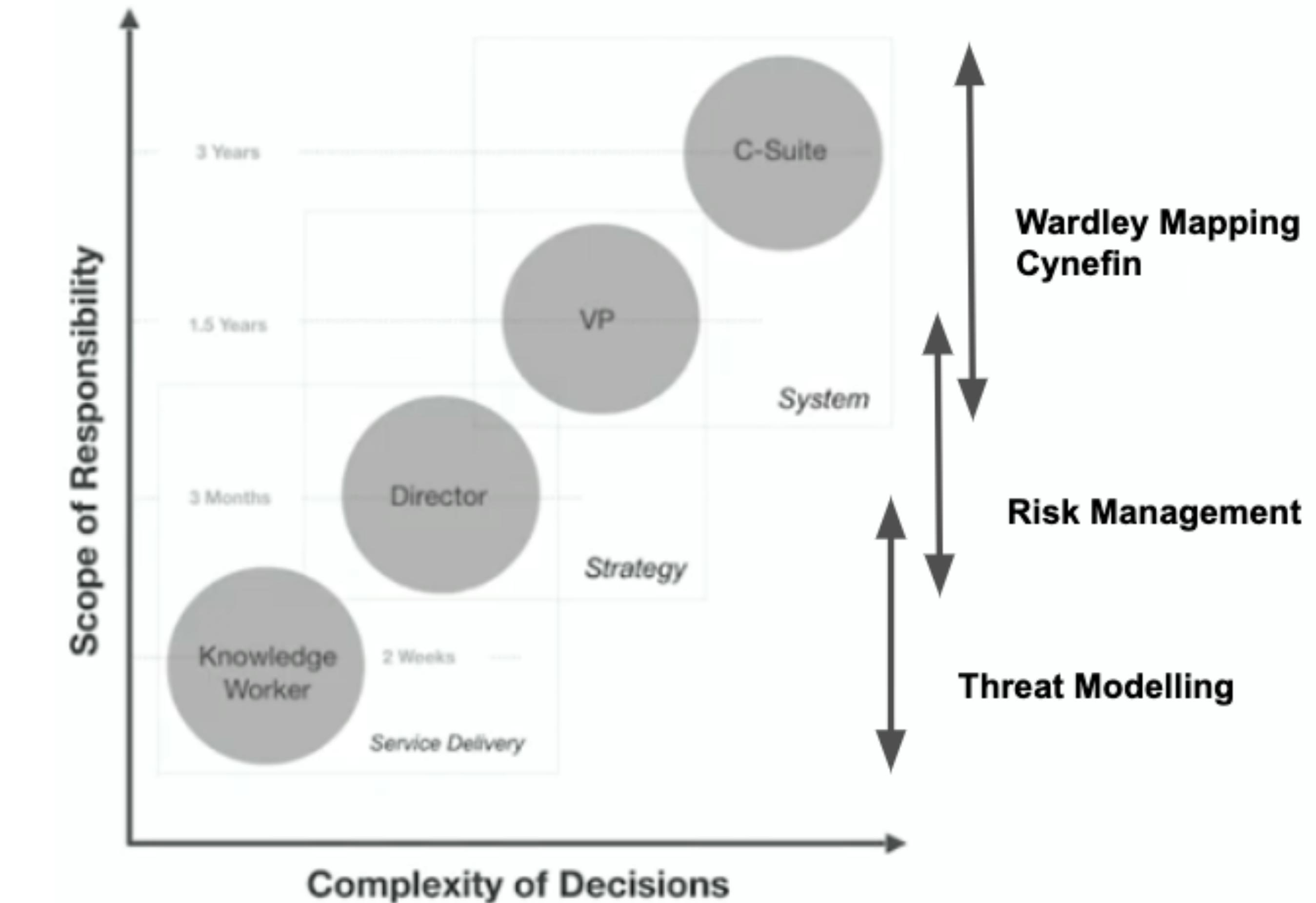
But how do we connect them ?

Threat Modelling



Risk Management

???



Jabe Bloom - 'Whole Work: Sociotechnicity & DevOps' - <https://www.youtube.com/watch?v=WtfncGAeXWU>

<https://medium.com/@marioplatt/social-practices-and-timespan-of-discretion-in-cyber-security-cef4fdc16663>

Strategies & Systemic Risk

C-Suite and VP

Risk Management

VP and Directors

Threat Modelling

Directors and Knowledge Workers

Strategic Risk

Trusted

Reputable

Product / Service Risk

Hardened

Recoverable

Key Risk Indicators

Confidential system components > 65% baseline met

Confidential systems without tested recovery plan > 2

Threat

Security misconfiguration

Service recovery

Mitigation

Develop and apply baseline

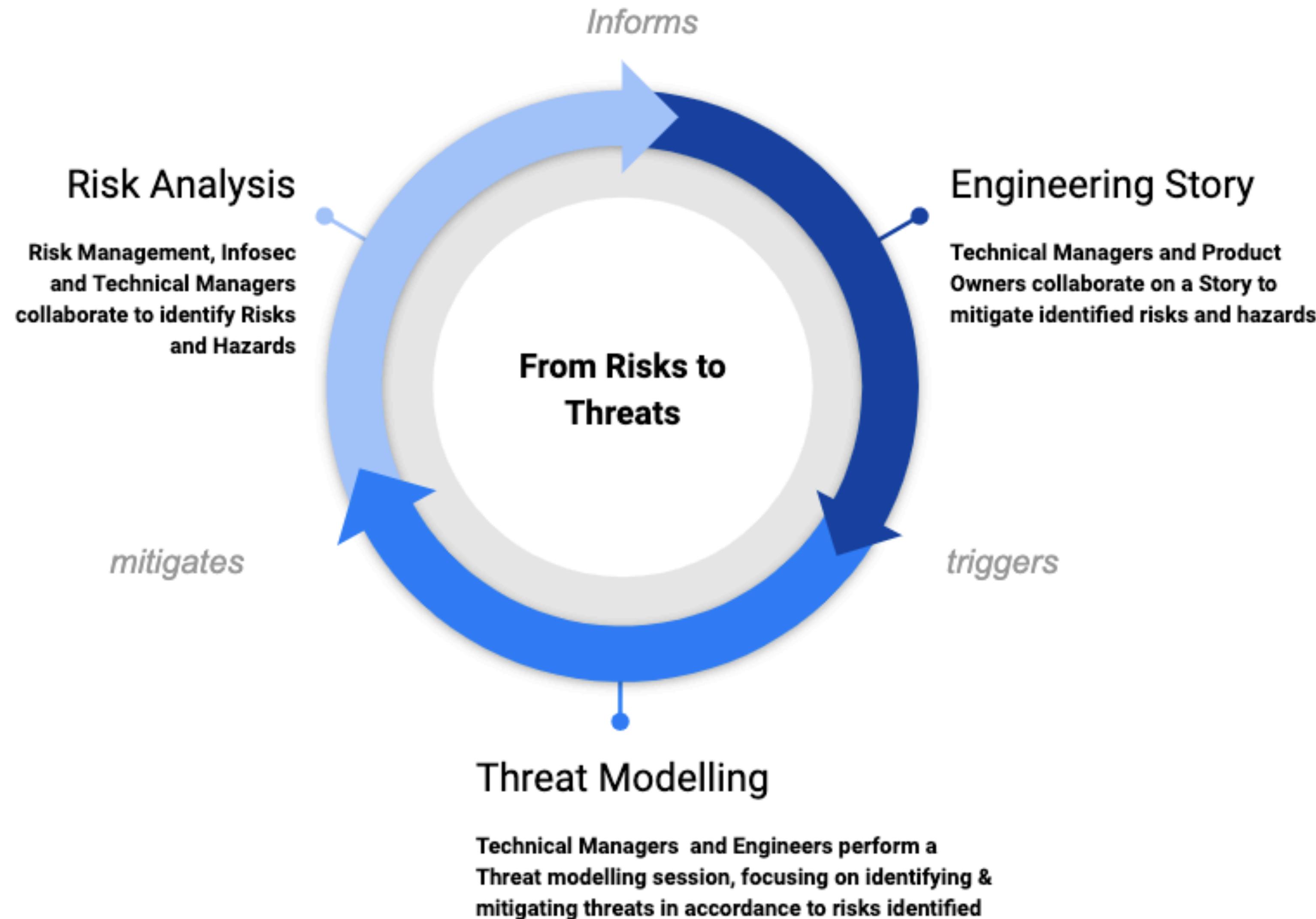
Define and test recovery plan

Validation

Compliance as Code

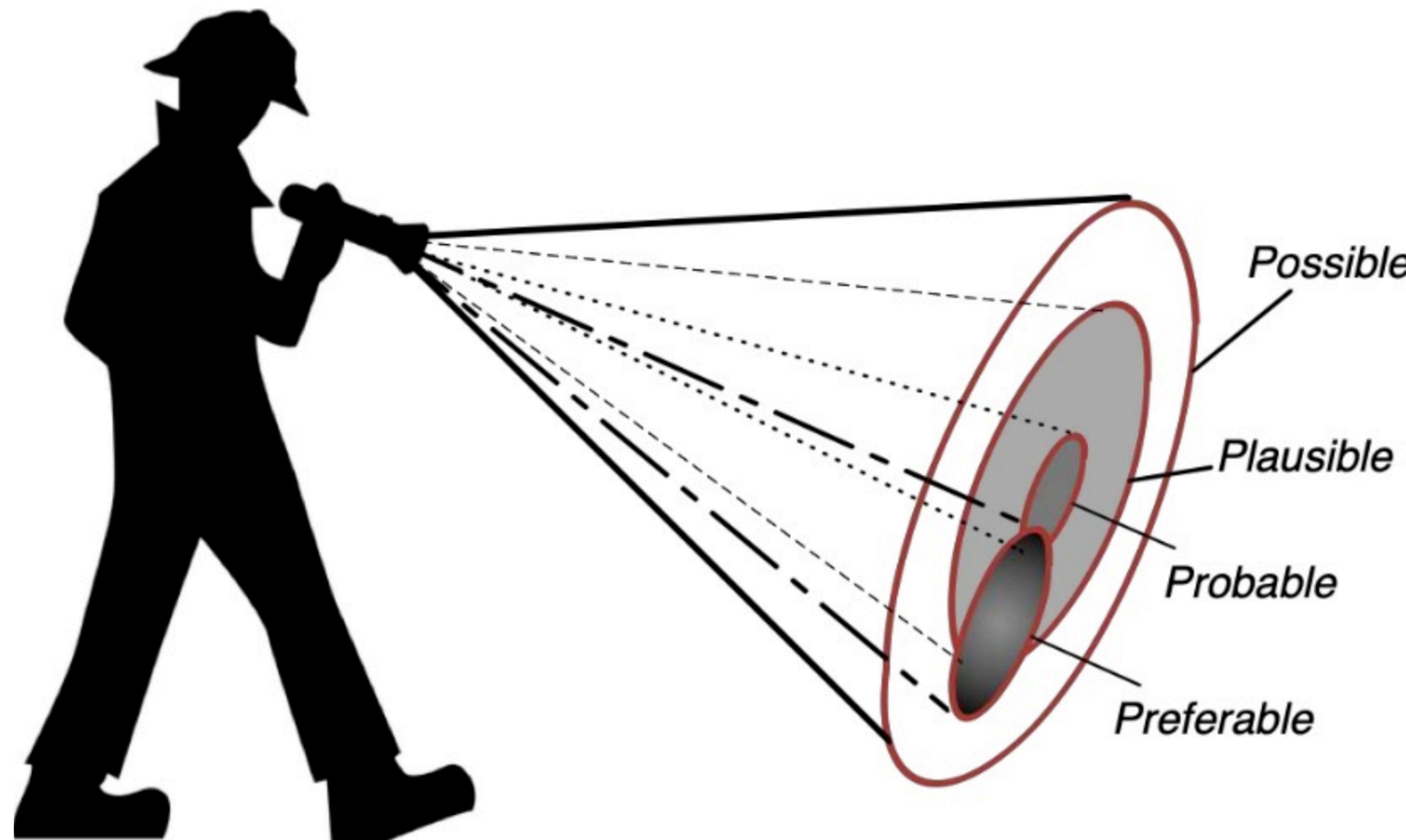
Scheduled testing with post-mortem

And process to connect them

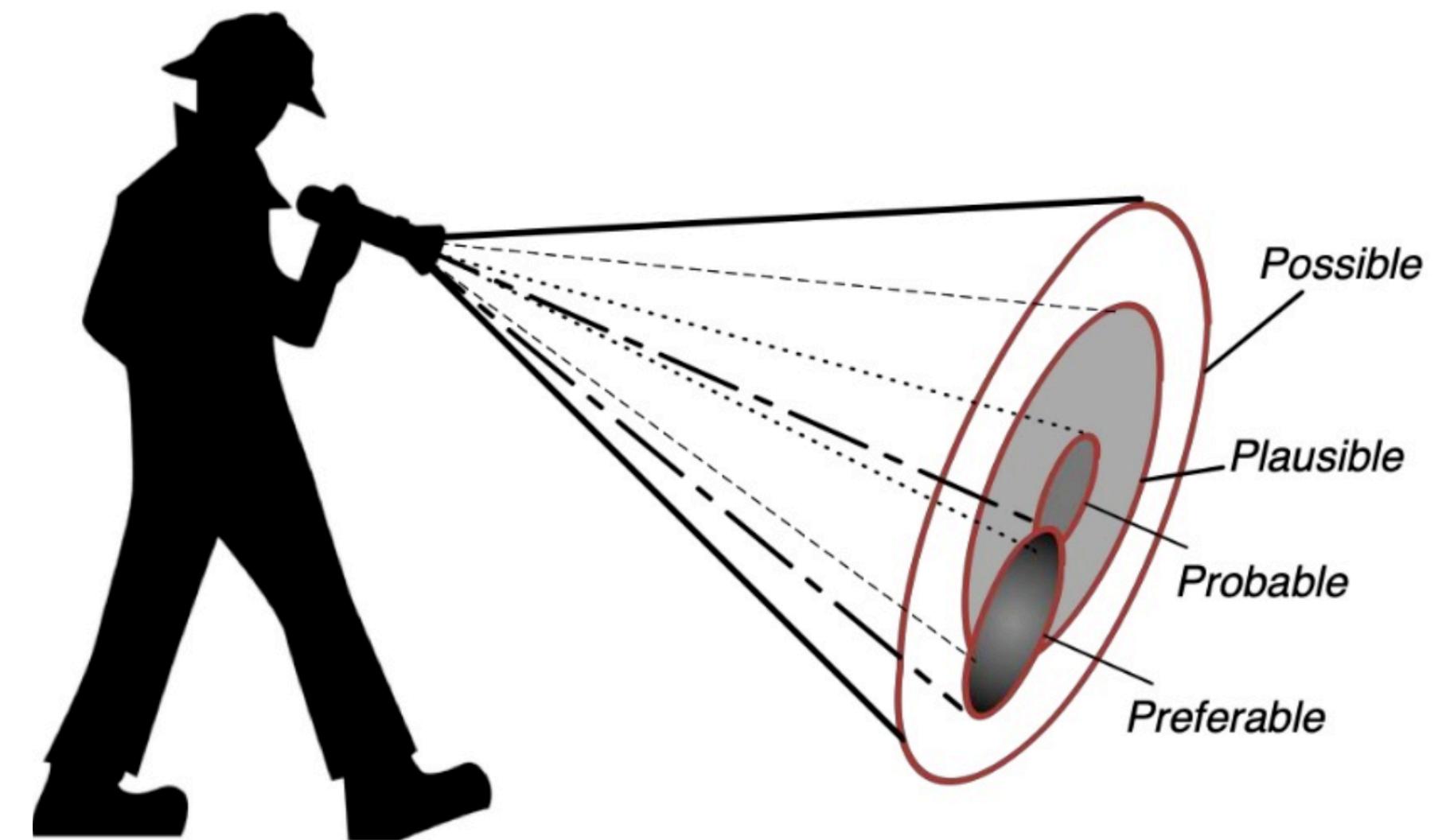
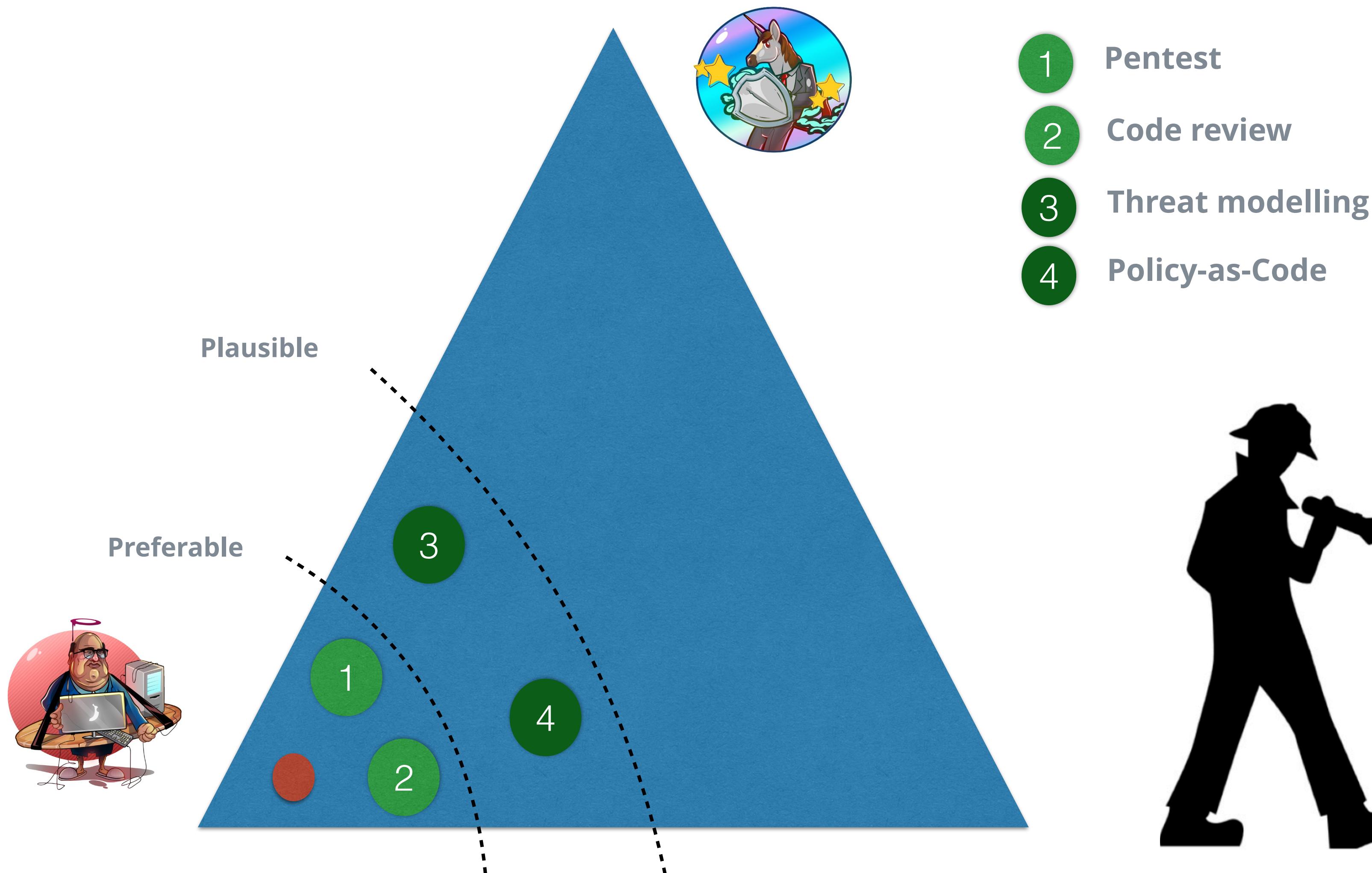


With metadata - Compliance, Policy, ASVS, Cheatsheets

Our world view



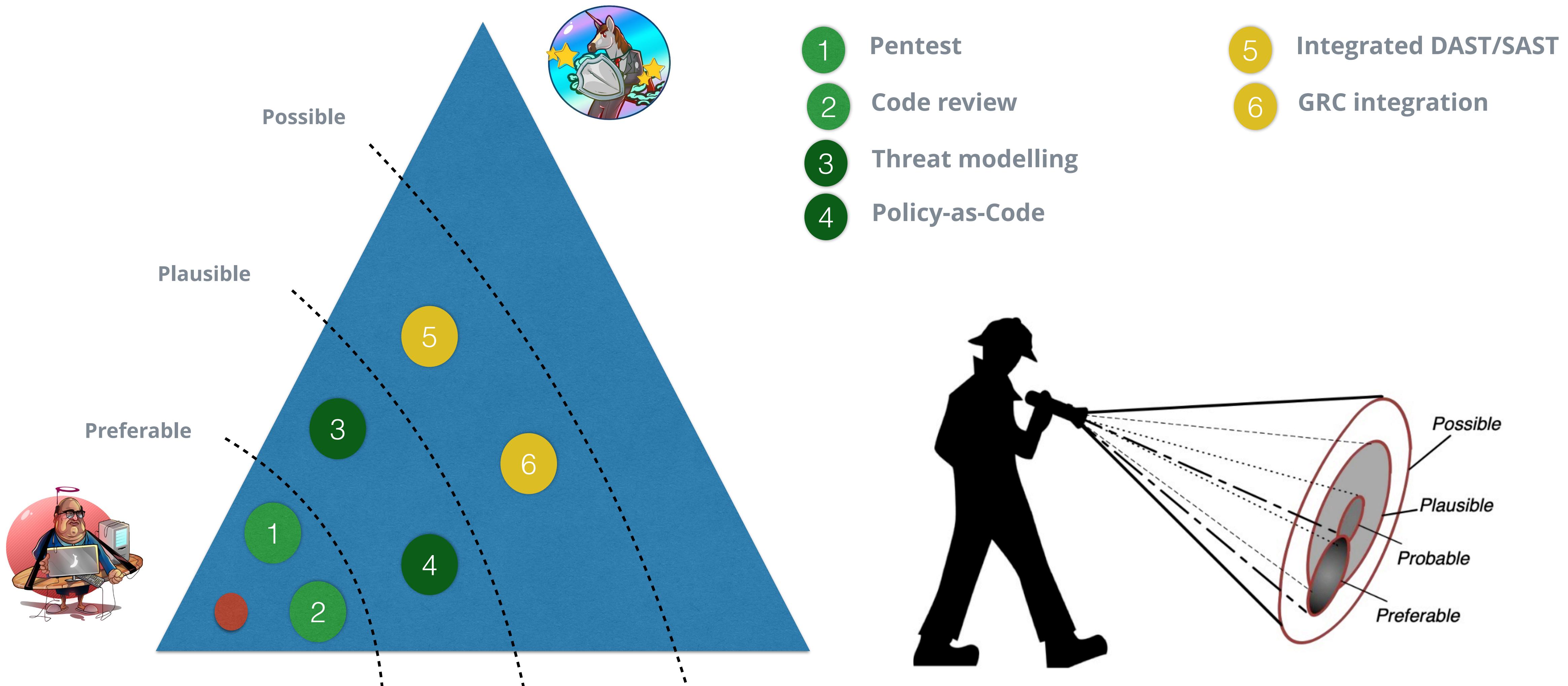
Meet them where they are



Constraint is TRUST in both teams and process/automation

Jabe Bloom @cyetain <https://www.slideshare.net/cyetain/three-frames-devopsdays-atl>

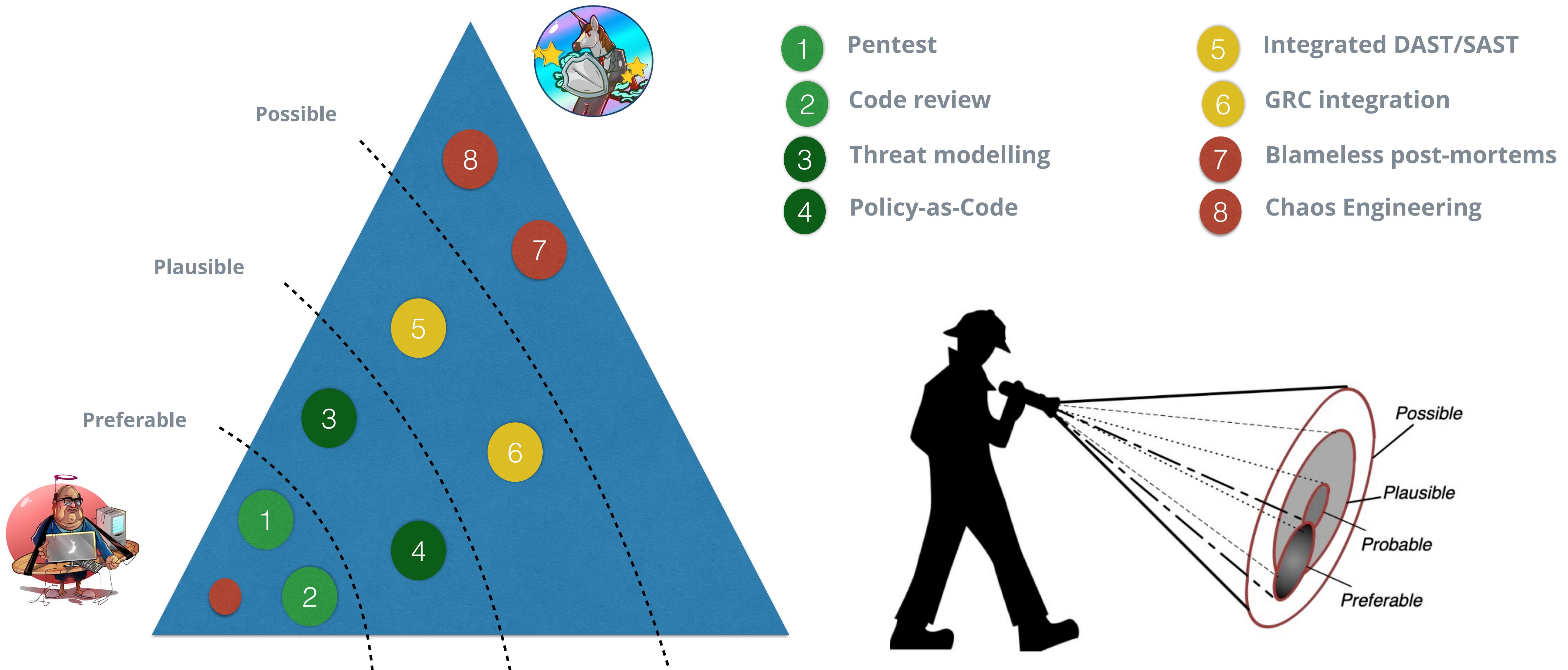
Meet them where they are



Constraint is TRUST in both teams and process

Jabe Bloom @cyetain <https://www.slideshare.net/cyetain/three-frames-devopsdays-atl>

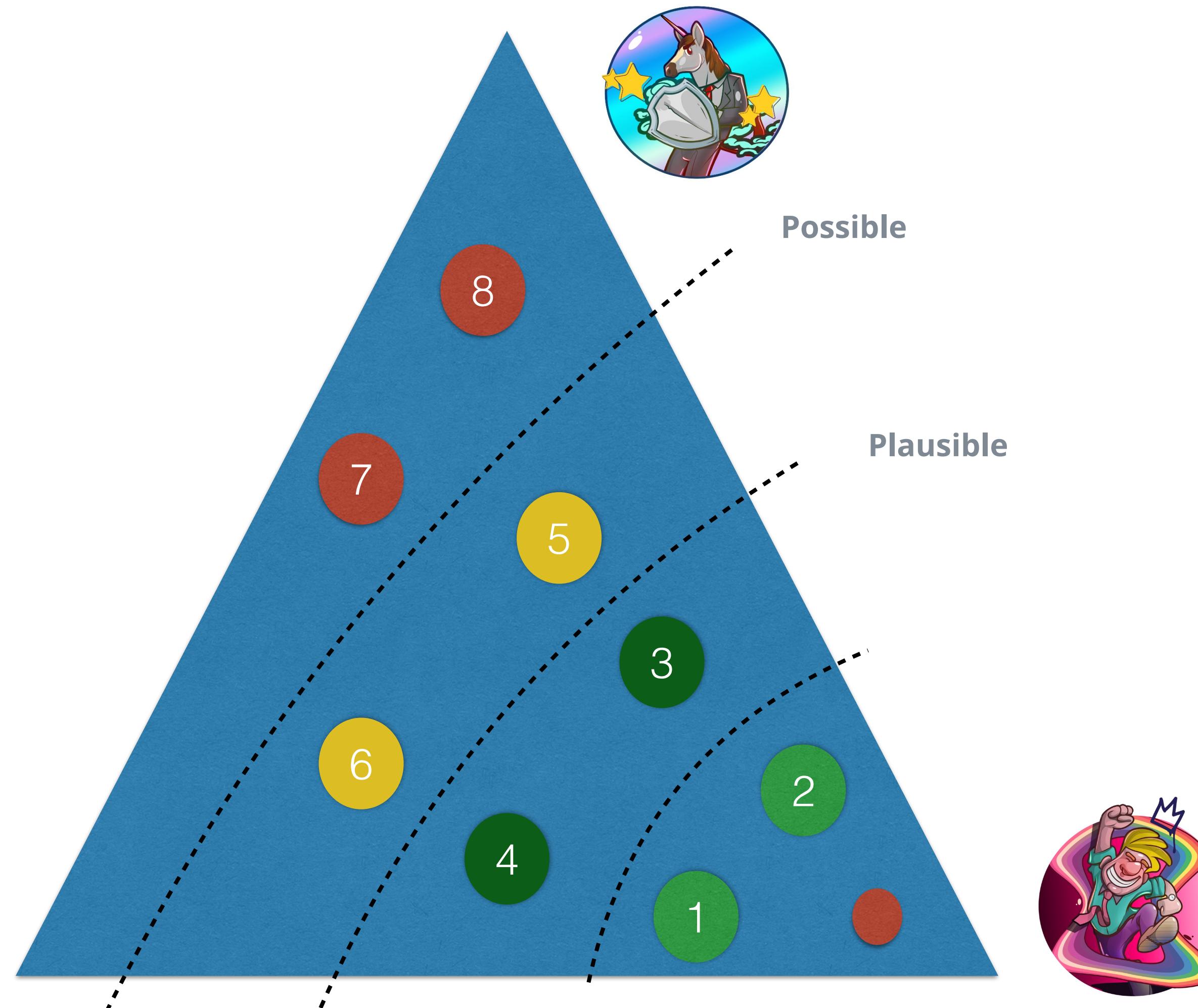
Meet them where they are



Constraint is TRUST in both teams and process

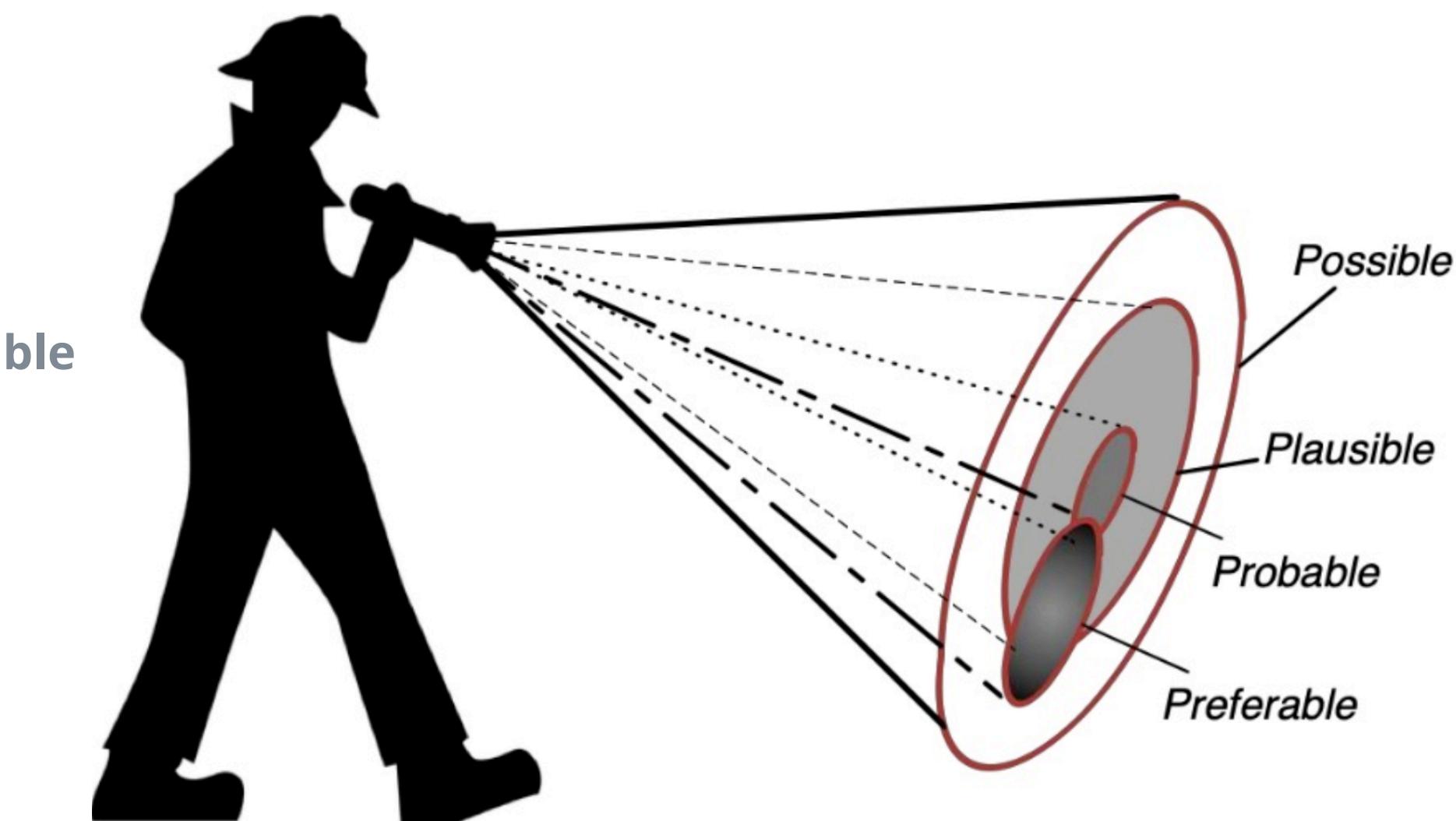
Jabe Bloom @cyetain <https://www.slideshare.net/cyetain/three-frames-devopsdays-atl>

Meet them where they are



- 1 TM with STRIDE
- 2 Process assurance
- 3 Baseline tooling
- 4 Policy-as-Code

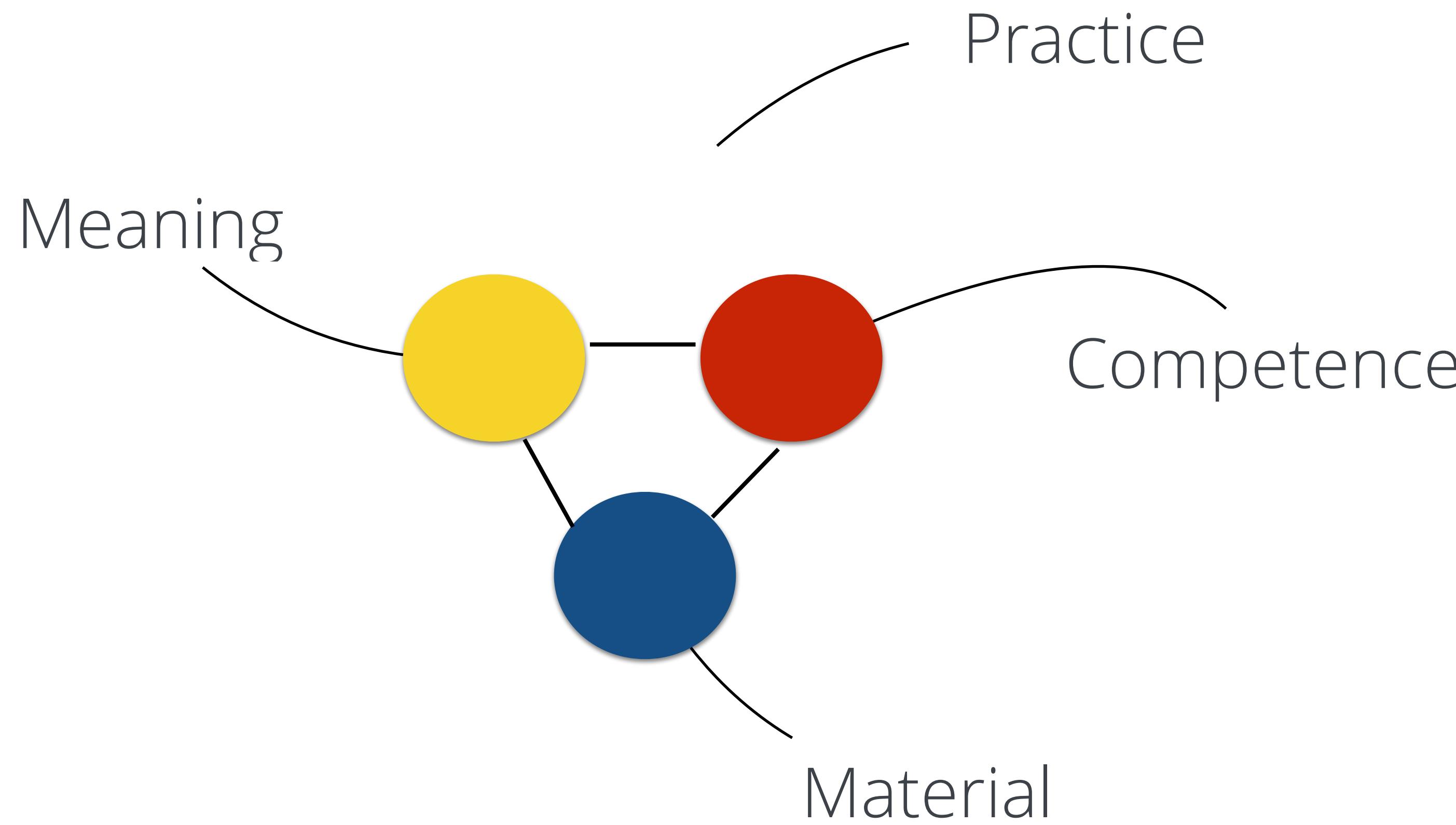
- 5 TM w/ methodology
- 6 Scenario Testing
- 7 Risk analysis
- 8 Security backlog ownership



Constraints are Agency and Ownership

Jabe Bloom @cyetain <https://www.slideshare.net/cyetain/three-frames-devopsdays-atl>

You also need to
manage the
meaning of practices



“material, meaning and competence are **not just interdependent, they are also mutually shaping**” Elizabeth Shove

Evolve the Meaning of Practices

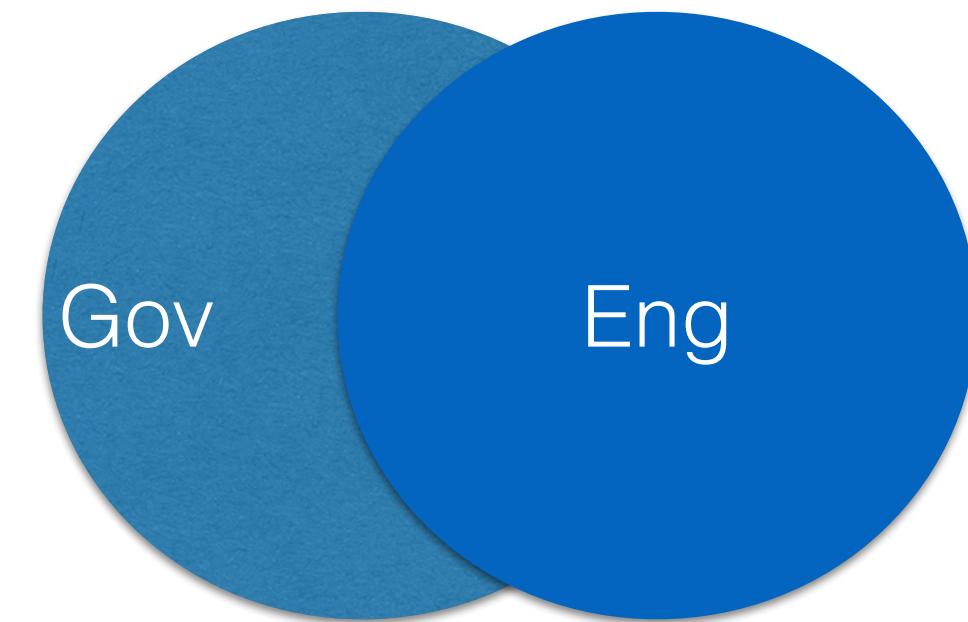
**“In a DevOps world, a Pentest is
not for finding security issues.
It’s to improve process”**

Mohammed A. Imran

Team interactions also evolve

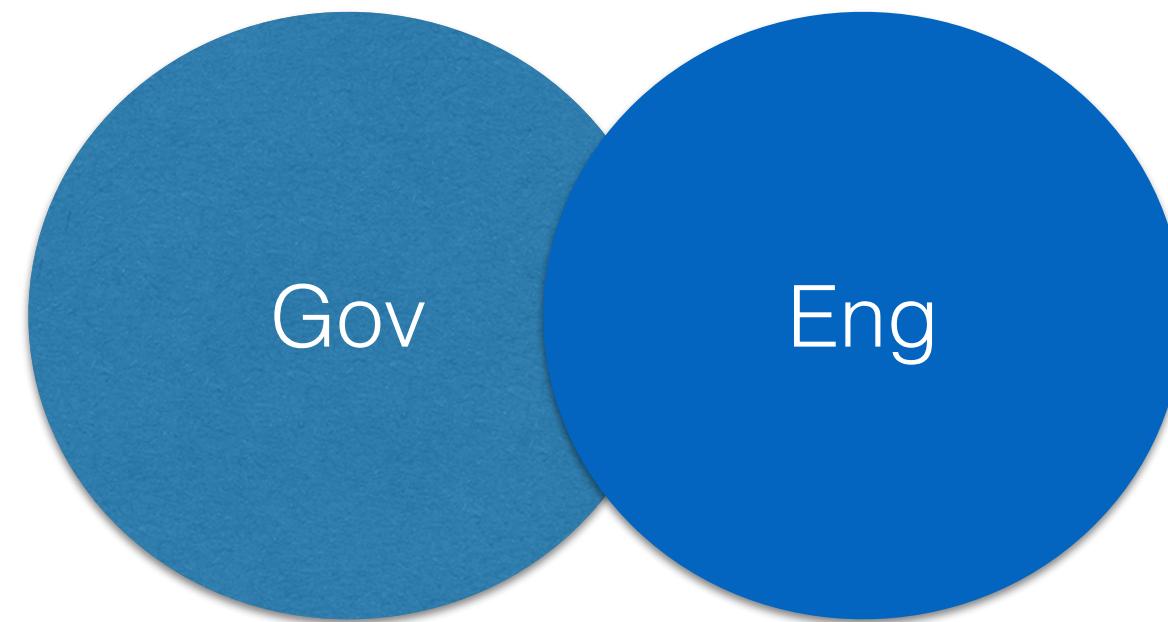
We need to change our “Team Topologies”
based on effectiveness and maturity of our
practices and capabilities

'Team Topologies' applied to Cyber Security



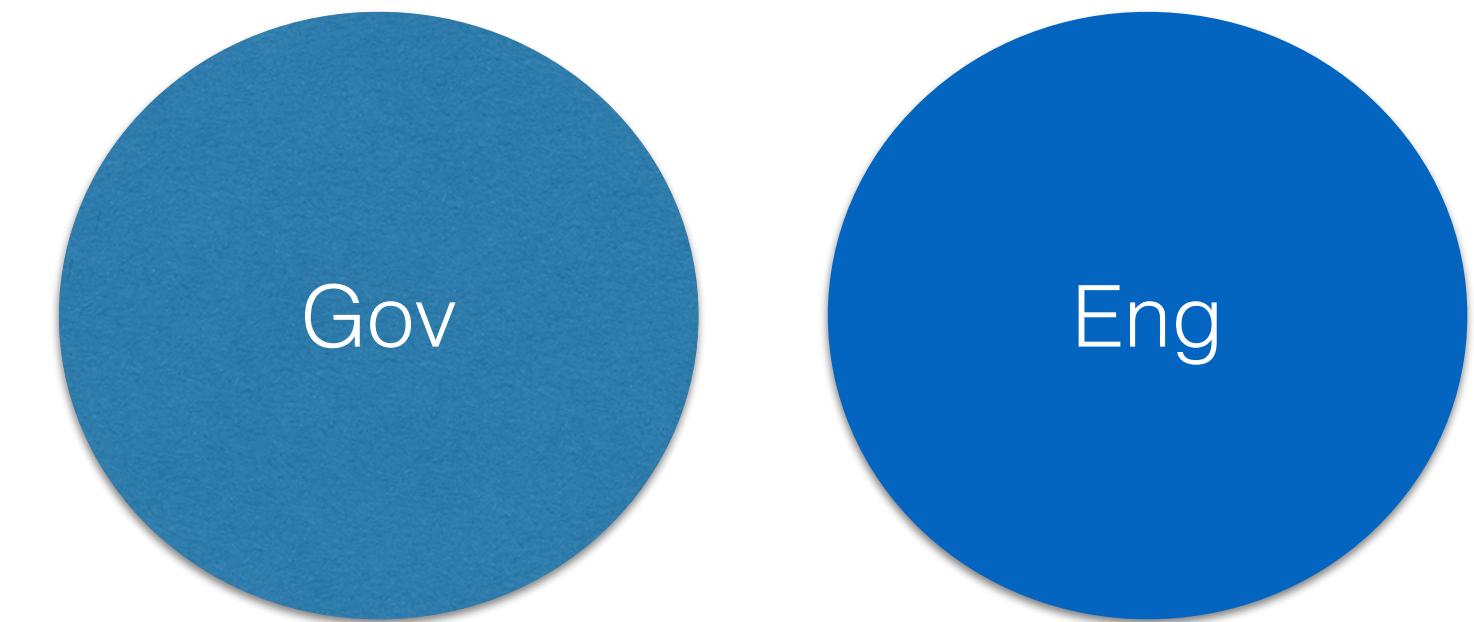
Collaboration

- Governance mapping (metadata management)
- Joint Threat modelling and Risk assessments
- Visibility and Reporting
- Management system updates



Facilitation

- Focus on cross-team training and contextual guidance
- Separate Threat modelling and Risk assessment sessions
- Boundary spanning more active between domains



X-as-a-Service

- Fully defined interfaces (Team or actual APIs)
- Informed/Supportive roadmaps
- Exception Management

Team Evolutionary Path



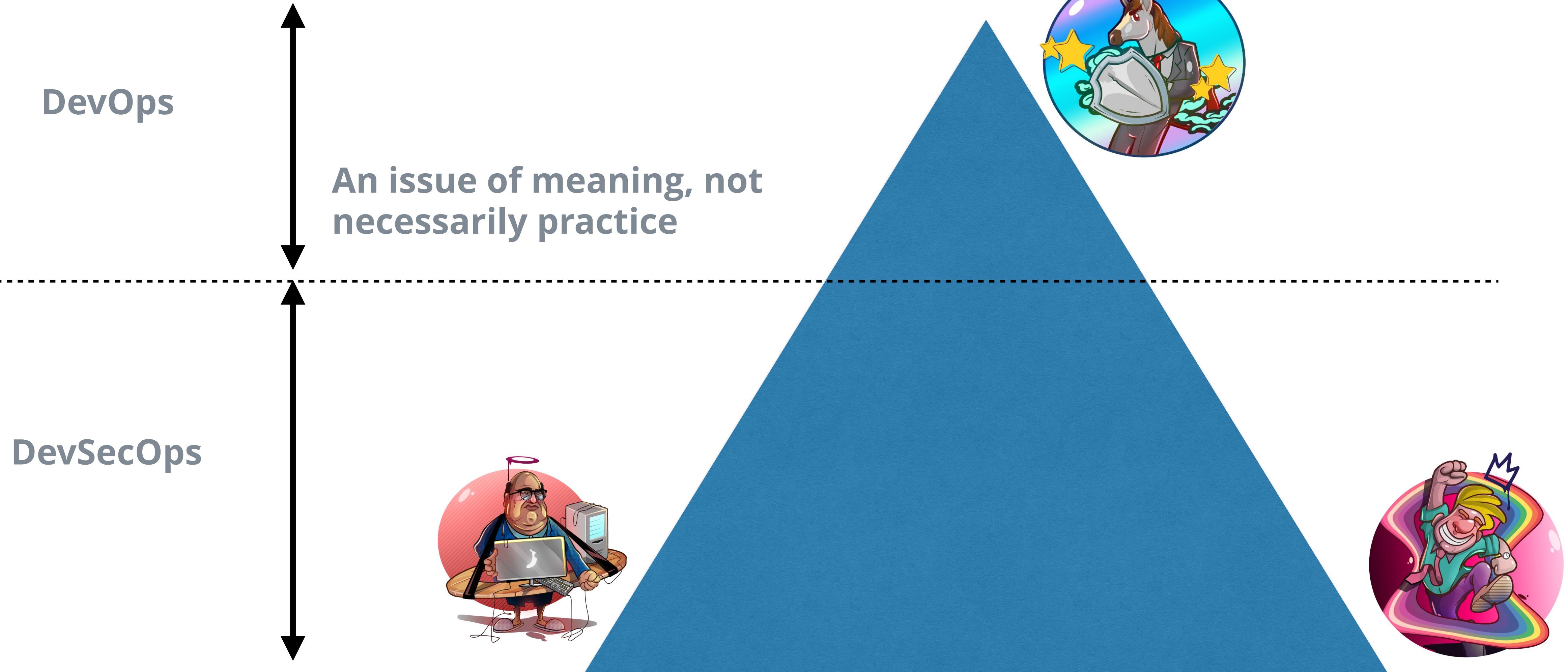
So, should YOU DevSecOps or not ?

TRUST + AGENCY = (SECURE) DEVOPS



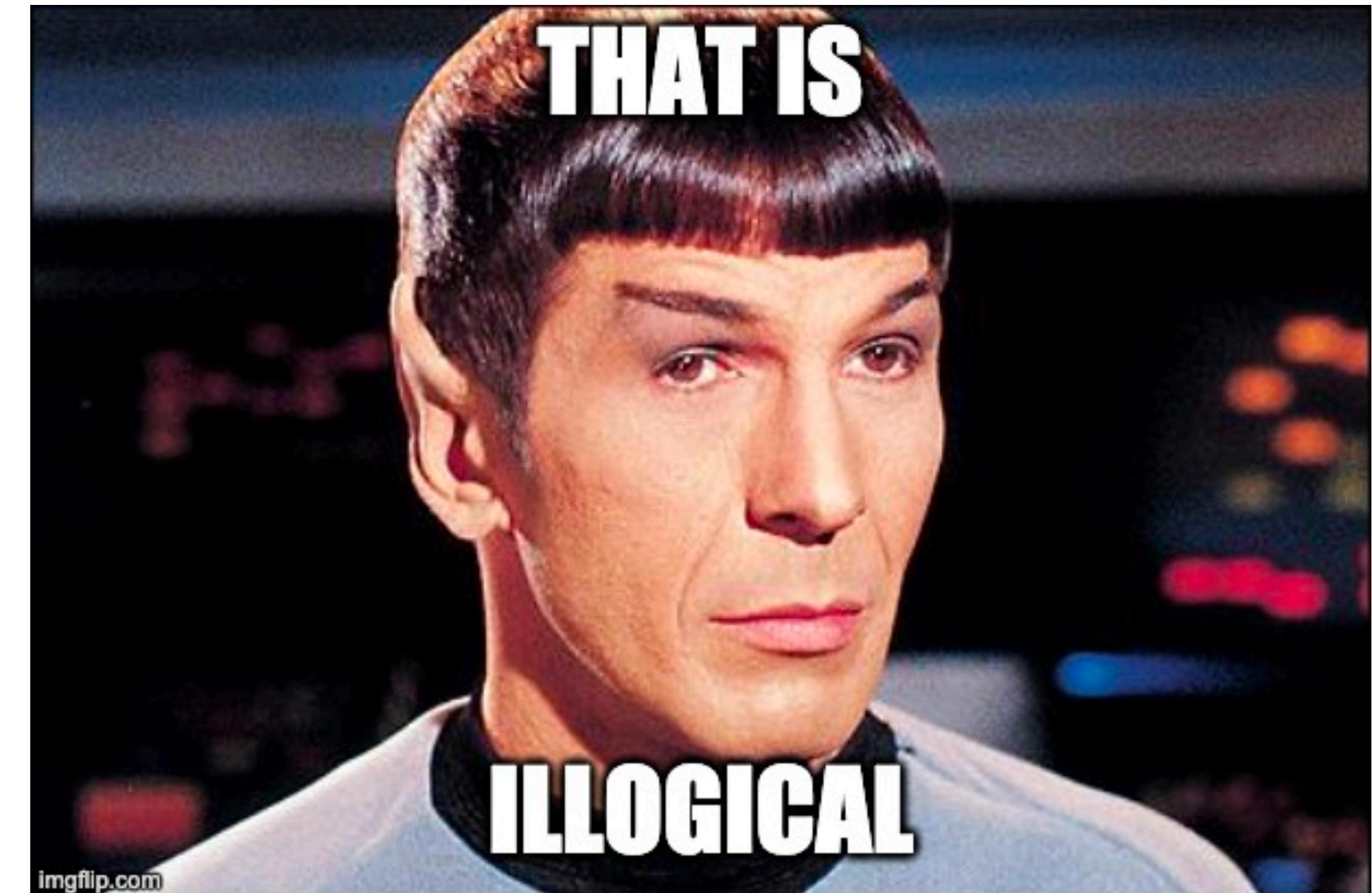
How will language used affect your transformation efforts ?

To DevSecOps or not ?



If your strategy mentions 'DevSecOps' and you're not

- Benefit Governance teams from shorter feedback loops
- Train Governance teams to understand systems of record
- Not increasing agency and ownership of security across Product teams in their language
- Not enabling the best possible Developer experience you can afford
- Not actively trying to breakdown siloed barriers and connect governance systems



Q&A



Mario Platt

mario.platt@privacybeacon.io

Twitter: @madplatt

LinkedIn: [marioplatt](#)

Medium: @marioplatt