AppSec Loves Agile

Agile On The Beach 2024

Gerald Benischke - @giskard23 - @beny23@infosec.exchange - beny23.github.io

About me

- I remember Java 1.0
- Maker of software
  - HMRC
  - Equal Experts
  - Money Super Market
  - Barclays
  - Bank of America
- Breaker of software
  - AppSec lead
- Juggler of plates
  - Ooredoo FinTech

@giskard23


MR. MEN

Journey 3

Train Service

Departs	Arrives
11:12 On time	13:44
Birmingham New Street (BHM)	**Exeter St Davids** (EXD)

2h 32m • 6 stop(s) • CrossCountry • Towards Plymouth

View calling points +

Journey 4

Train Service

Departs	Arrives
14:02	16:15
Exeter St Davids (EXD)	**Truro** (TRU)

2h 13m • 6 stop(s) • Great Western Railway • Towards Penzance

View calling points +

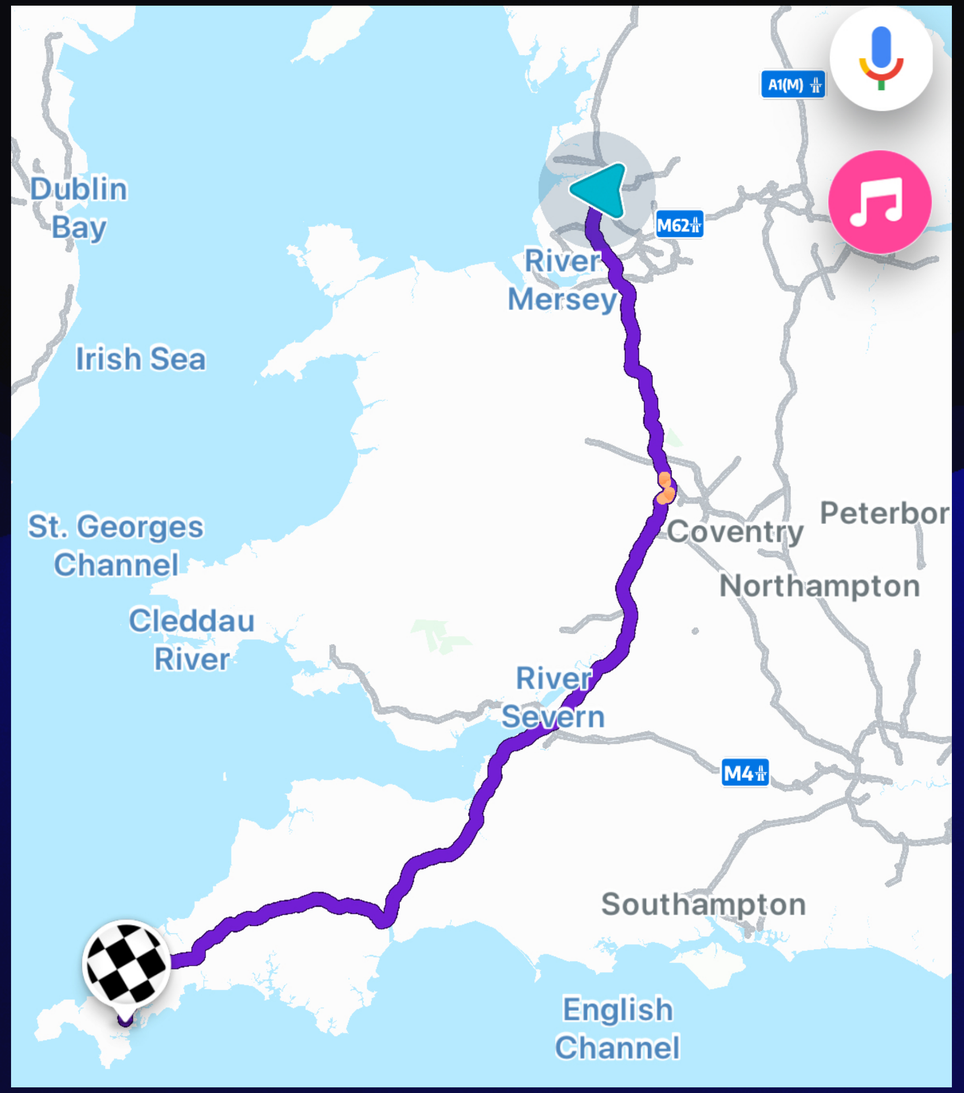
Journey 5

Train Service

Departs	Arrives
16:20 On time	16:33
Truro (TRU)	**Penryn (Cornwall)** (PYN)

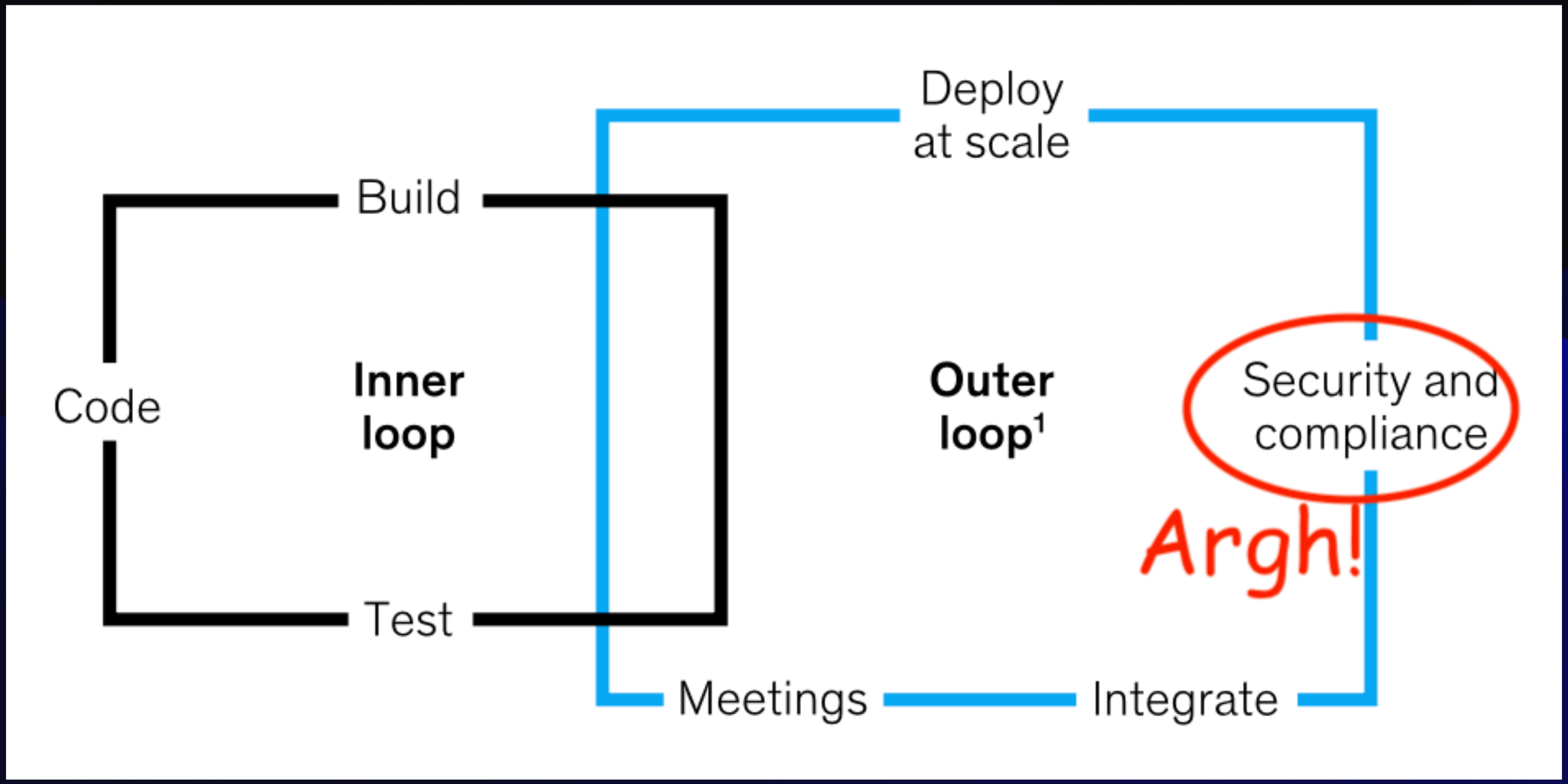
13m • 2 stop(s) • Great Western Railway • Towards Falmouth Docks

View calling points +



You promised AppSec? Agile?

That McKinsey article

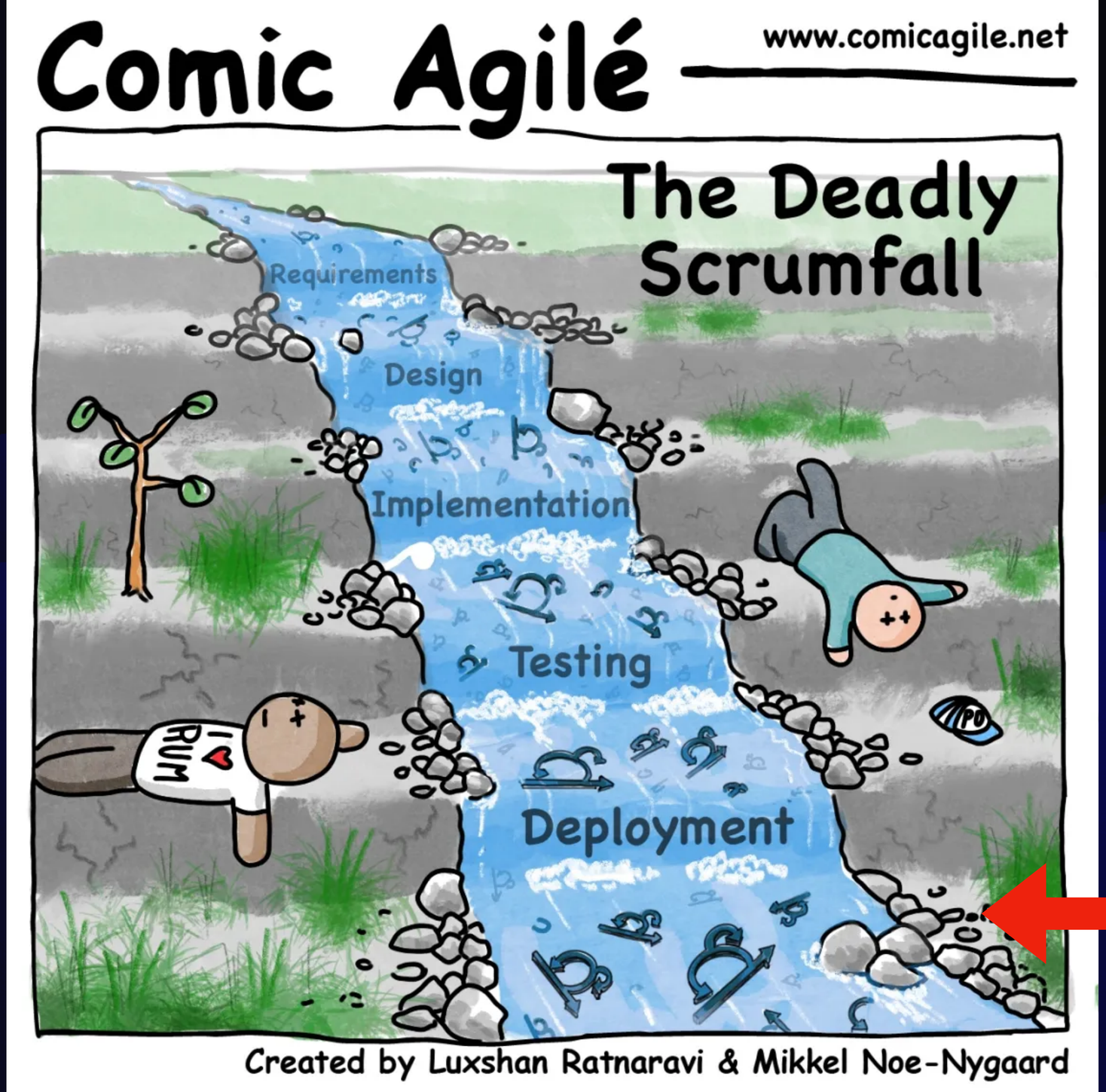

Deploy
at scale
Build
Code
Inner
loop
Outer
loop[1]
Security and
compliance
Argh!
Test
Meetings
Integrate

Security specialists. Arghhh! They’re all sitting in their ‘ivory tower’ without anything better to do than to take a baseball bat to your hard work and tell you how you’ve not considered some obscure vulnerability CVE-1423/4234 in a library that you didn’t even know existed. Not only that, there is definitely no way that you can deploy now, even when the product owner is breathing down your neck saying that nobody is going home until we’ve fixed this!

(c) Alison Kirkpatrick

Why did nobody tell me about this?

screams the Head of Security three days before the project concludes



Security gets involved sometime here

Alignment between Developers and Security

Manifesto for Agile Software Development

We are uncovering better ways of developing
software by doing it and helping others do it.
Through this work we have come to value:

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

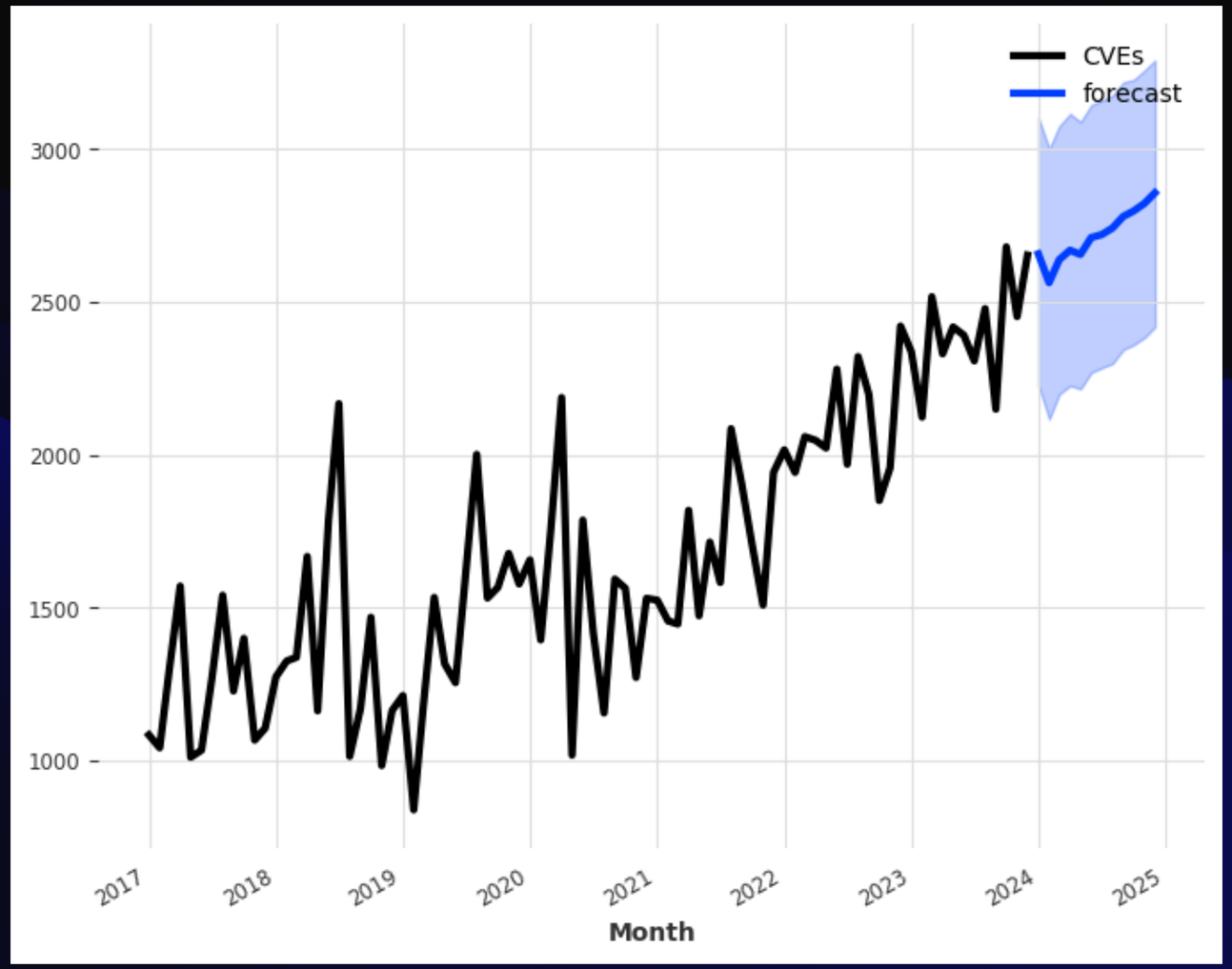
That is, while there is value in the items on
the right, we value the items on the left more.

Individuals and Interactions

over processes and tools

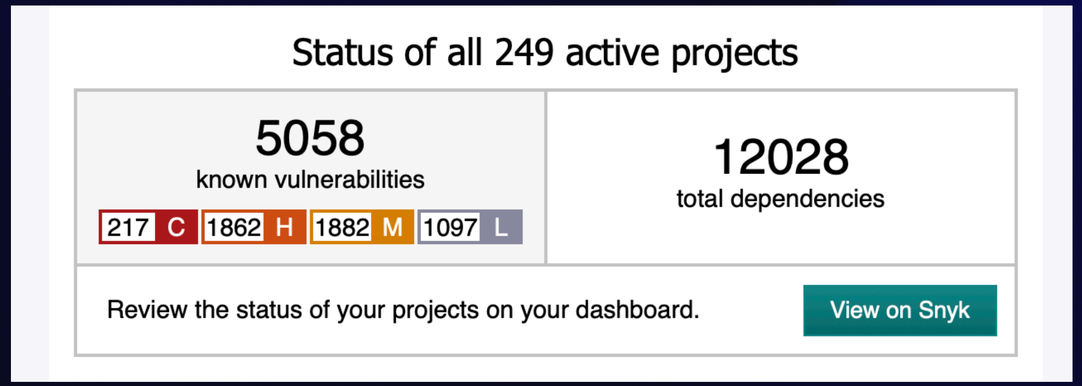
The Supply Chain

Supply Chain Vulnerabilities



https://jerrygamblin.com/

We’ll just disable the vulnerability check while we push out this critical update

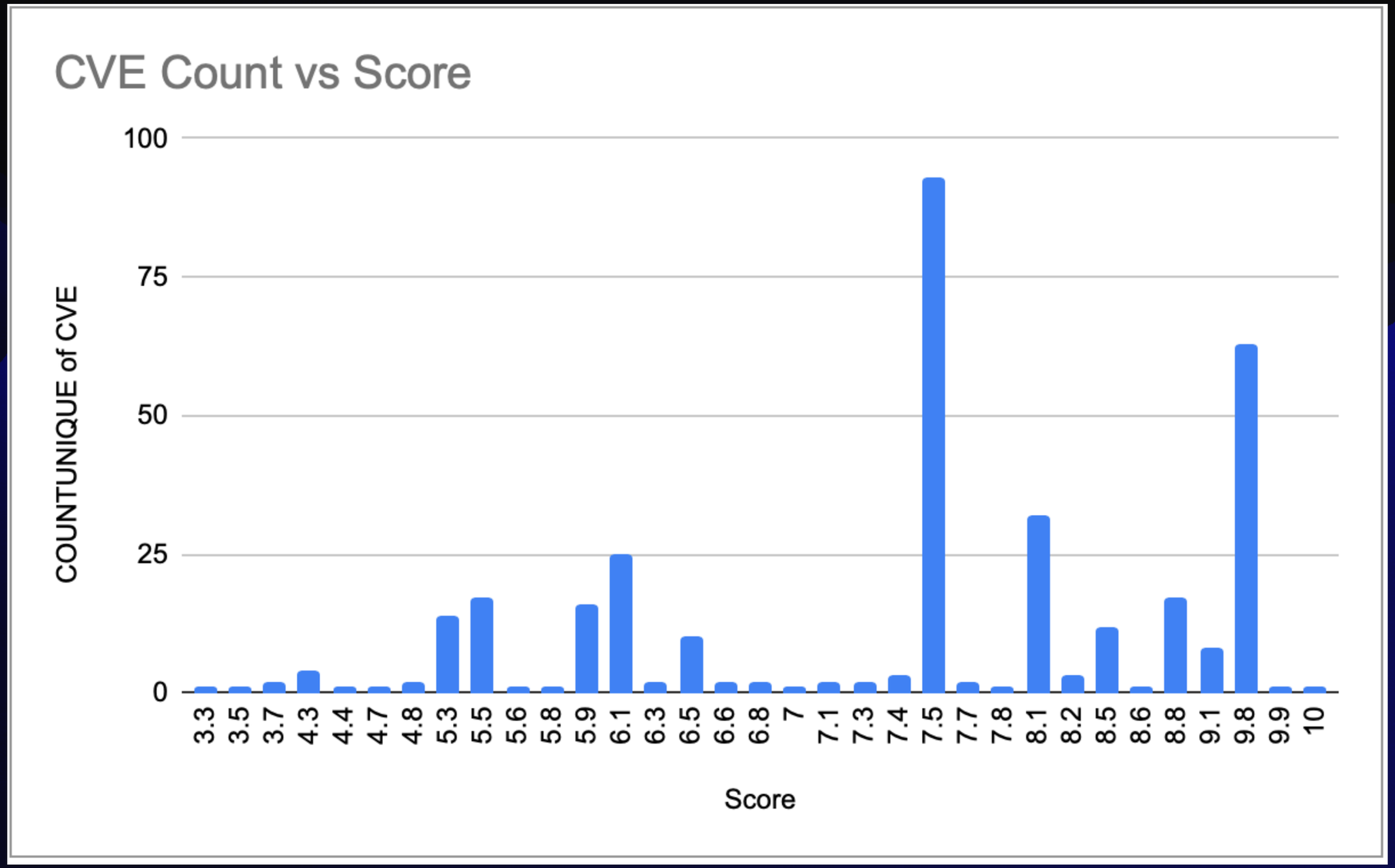


Security Simplified: Our AI-Based Approach Stops Attacks Before They Start.

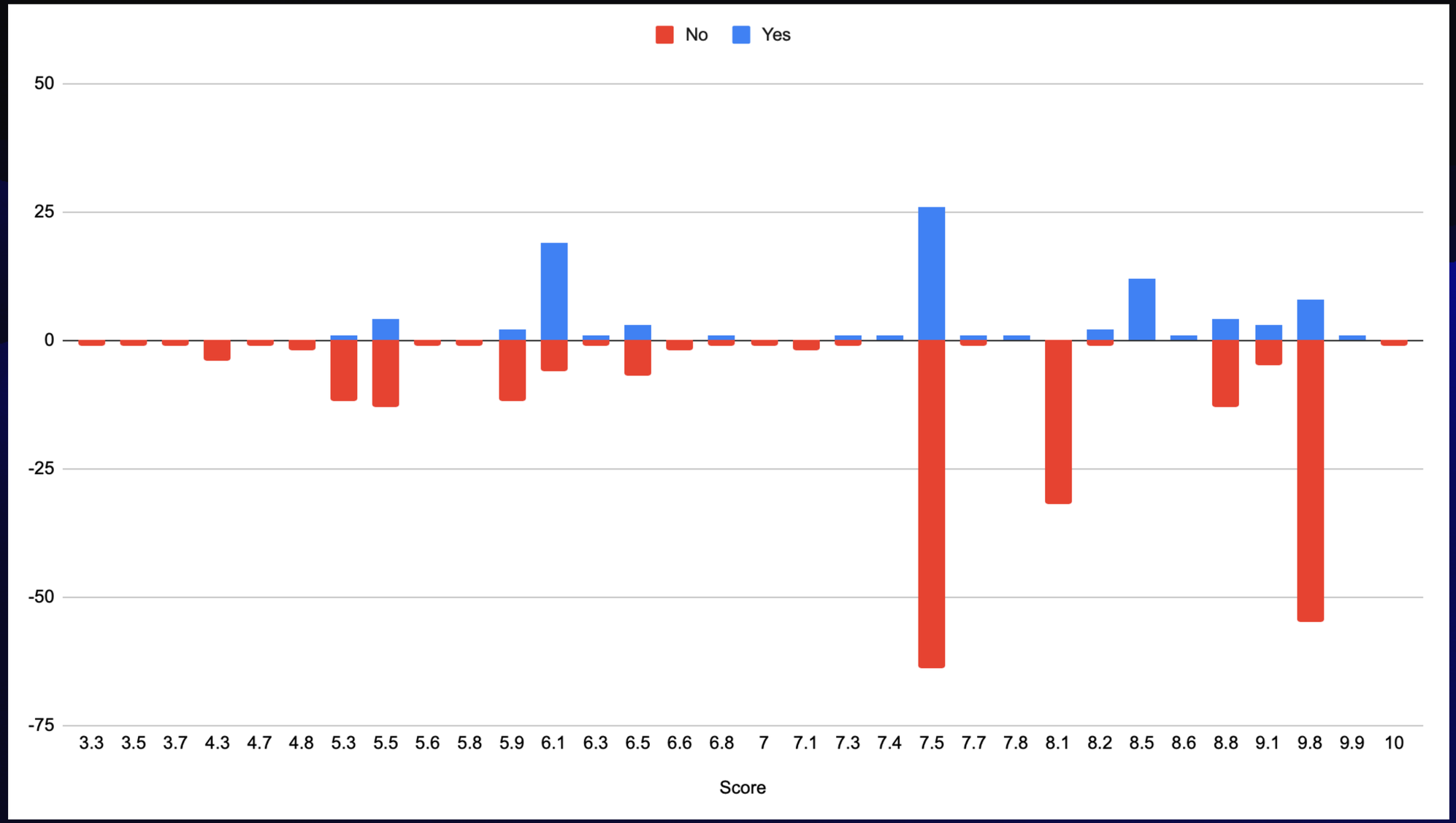
Unleash the Power of AI: Proactive, Intelligent, and Comprehensive Cybersecurity Solutions.

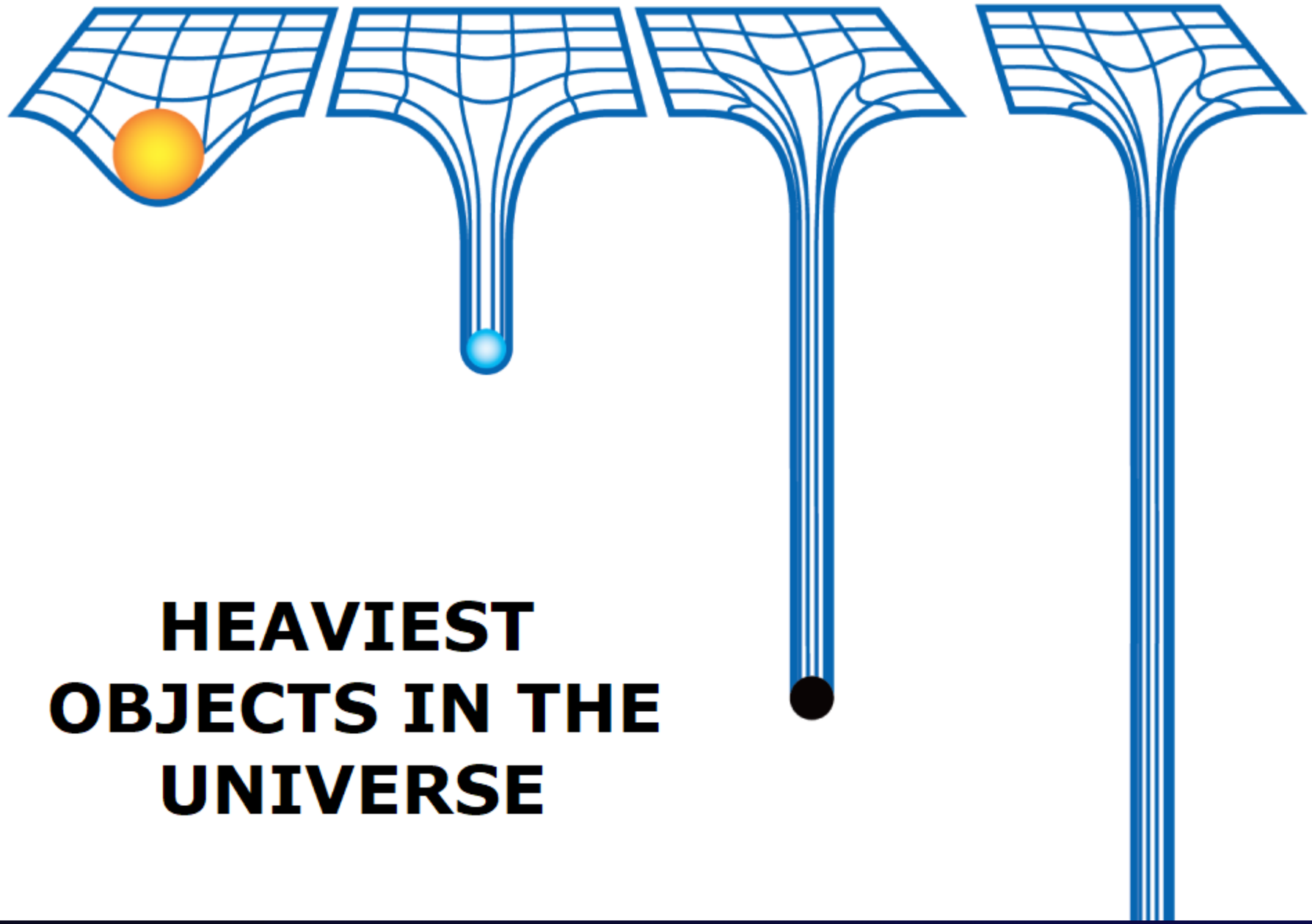
CVSS Score =
Common Vulnerability Scoring System
Score

Needs Action?



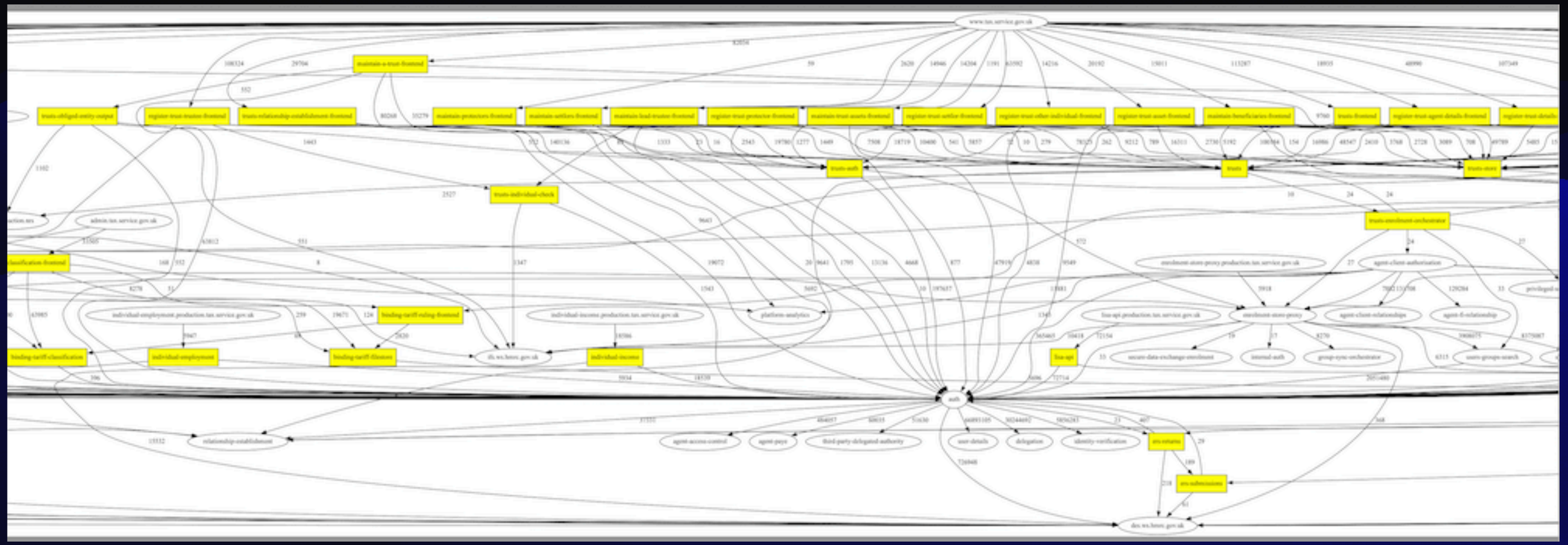
Needs Action?



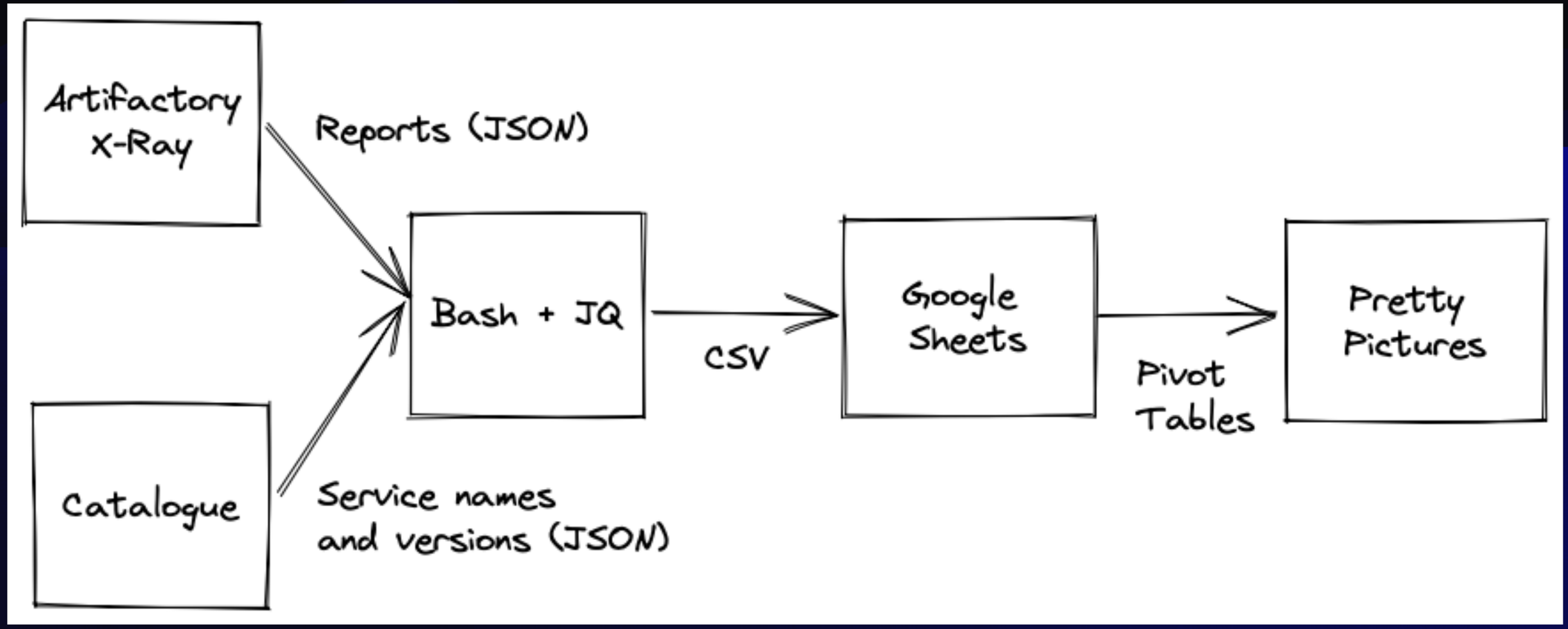

Sun
Neutron star
Black hole
node_modules
HEAVIEST OBJECTS IN THE UNIVERSE


THAT SOUNDS LIKE A LOT OF WORK!
makeameme.org

Scale Makes Us Fail

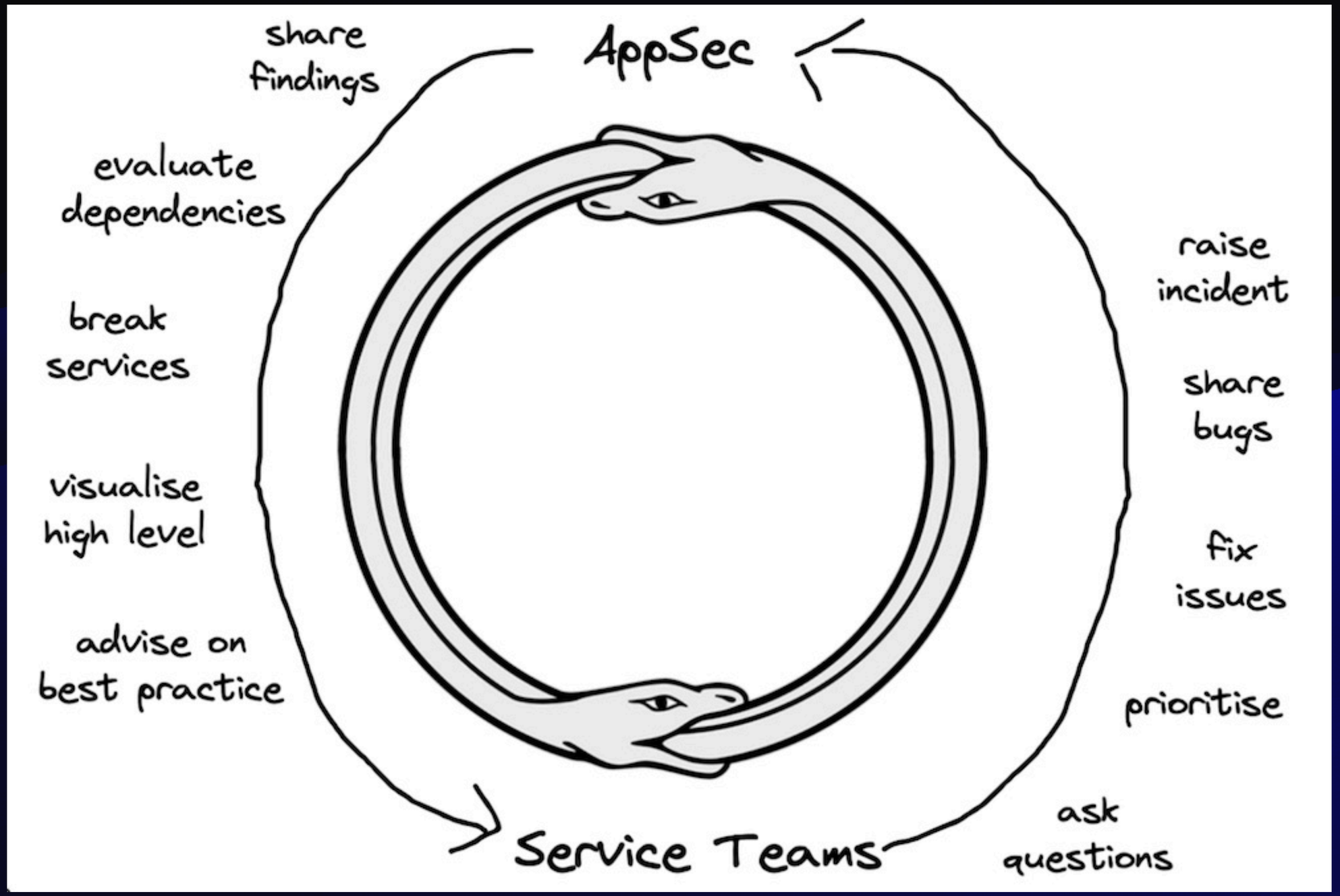


Vulnerability Curation Pipeline



Start Small
Spreadsheets are your Friend
Iterate!

Secure Software
over security checklists


share findings
AppSec
evaluate dependencies
break services
visualise high level
advise on best practice
raise incident
share bugs
fix issues
prioritise
ask questions
Service Teams

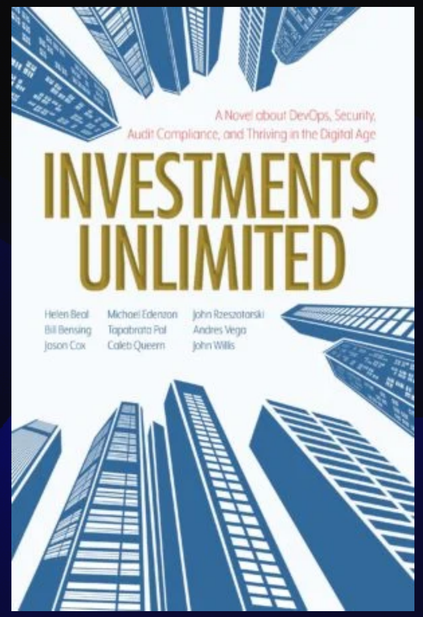
But I need to prove to the regulator!!!

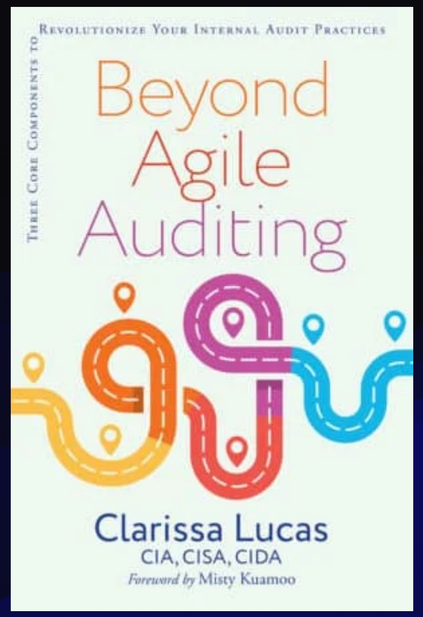
screams the Head of Security three days before the project concludes

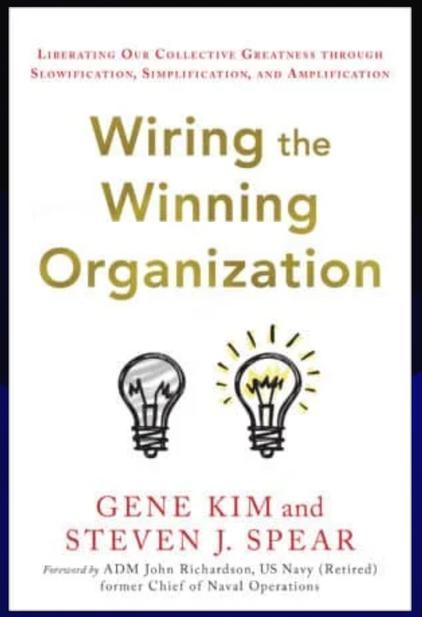
Regulators like DevOps

Regulators like Agile

Spirit of Regulation

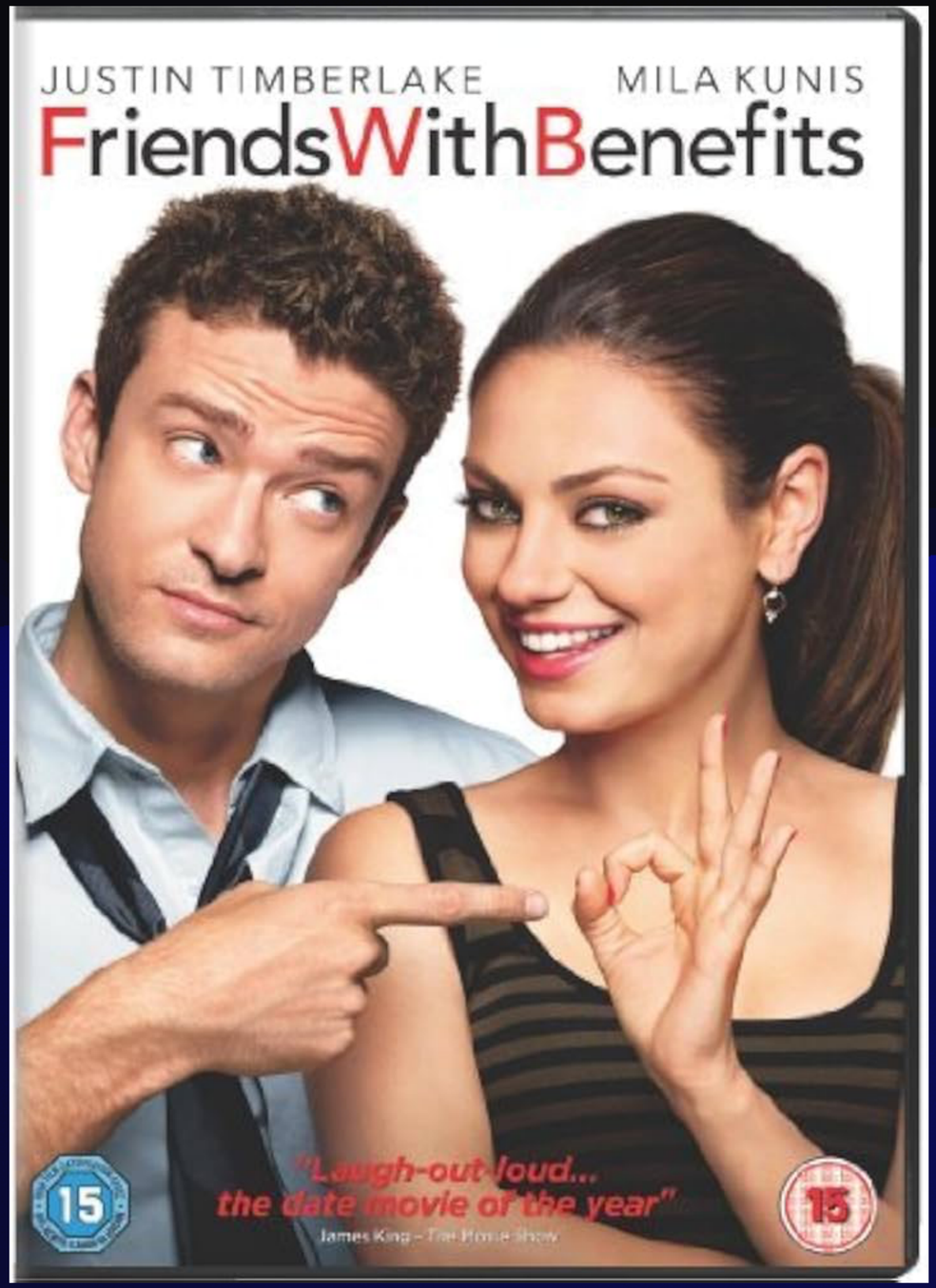

A Novel about DevOps, Security, Audit Compliance, and Thriving in the Digital Age
INVESTMENTS UNLIMITED
Helen Beal
Bill Bensing
Jason Cox
Michael Edenzon
Topobrata Pal
Caleb Queern
John Rzeszotarski
Andres Vega
John Willis


Three Core Components to Revolutionize Your Internal Audit Practices
Beyond Agile Auditing
Clarissa Lucas
CIA, CISA, CIDA
Foreword by Misty Kuamoo


Liberating Our Collective Greatness through Slowification, Simplification, and Amplification
Wiring the Winning Organization
GENE KIM and
STEVEN J. SPEAR
Foreword by ADM John Richardson, US Navy (Retired)
former Chief of Naval Operations

Book Club

Auditors are our friends



Collaboration
over policies

What is the biggest fire?

I don’t have time to work on these policies, there are too many fires!

screams the Head of Security after five weeks of being chased for input

Collaboration

~~over~~ on policies

What Does Good Look Like? (WDGLL)

Security is a Team Sport

No, I don’t mean scrum

Responding to Change

over perfect security


THIS IS
FINE

AppSec Loves Agile

Use the Agile Manifesto

Individuals and Interactions over processes and tools

Secure Software over security checklists

Collaboration on policies

Responding to Change over perfect security


People over Process

Questions?

AppSec Loves Agile

Gerald Benischke - @giskard23 - @beny23@infosec.exchange - beny23.github.io