
Threat Modeling Wins for Agile AppSec



Rahul Raghavan

(Co Founder and Chief Evangelist, we45)



Yours Truly



Rahul Raghavan

(Co Founder and Chief Evangelist)

- Software Developer turned Security Engineer turned Techno Marketing Chappie!
- Head of Pre-sales and Solution Development
- Things that keep me up at night
 - AppSec Automation Models
 - DevSecOps Value Realisation
 - Threat Modeling / Test Case Automation
 - Penetration Testing 2.0

.....also an avid Cinephile!

Over the next 45 mins...

- ❖ Why Threat Model?
- ❖ Common Reasons for Failure
- ❖ Threat Modeling Schools of Thought
- ❖ Threat Playbook
- ❖ Threat Modeling and Security Testing

Application Security Today

- ❖ Increase in Tooling
- ❖ Increase in Test Iterations
- ❖ Feedback Loops (Shifting Right & Left)
- ❖ 'X'-as-Code execution models
- ❖ Integration with mainstream SDLC
- ❖ Metrics and Metadata (Vulnerabilities, Maturity etc)

The Castles of Threat Modeling

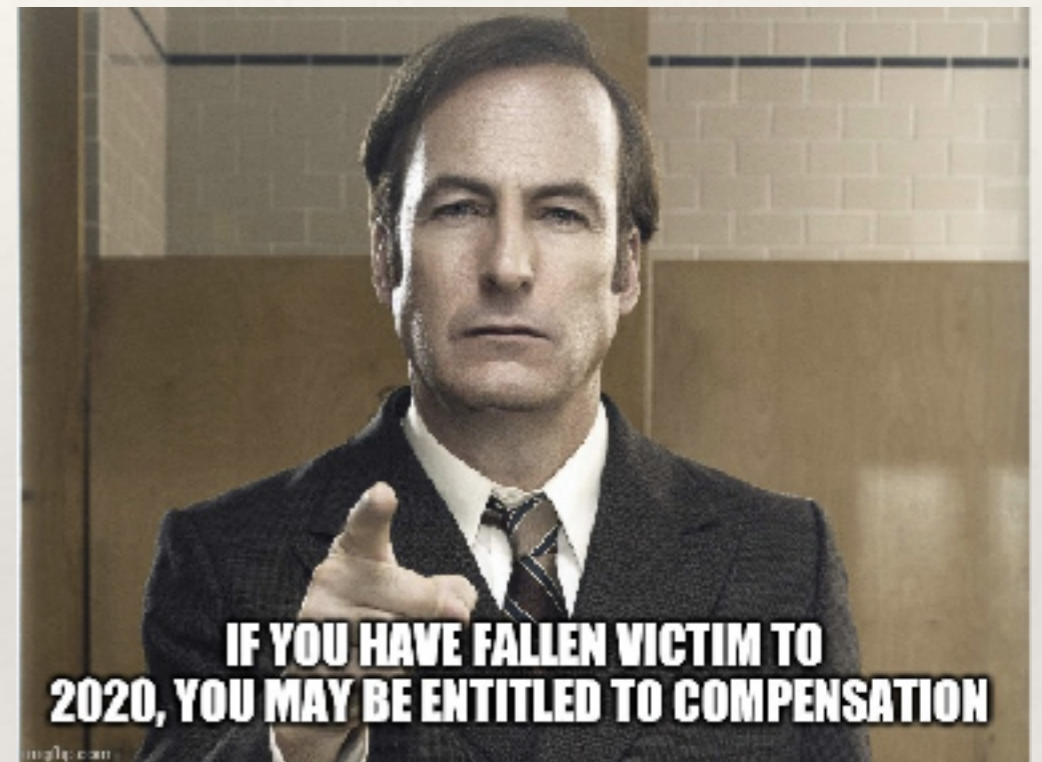
“Find 30% of issues even before they’re coded”

“Incident Response Teams are a thing of the past”

“AppSec is Dead without Threat Modeling”

**“In trust boundaries we trust” - everybody
else meet HR**

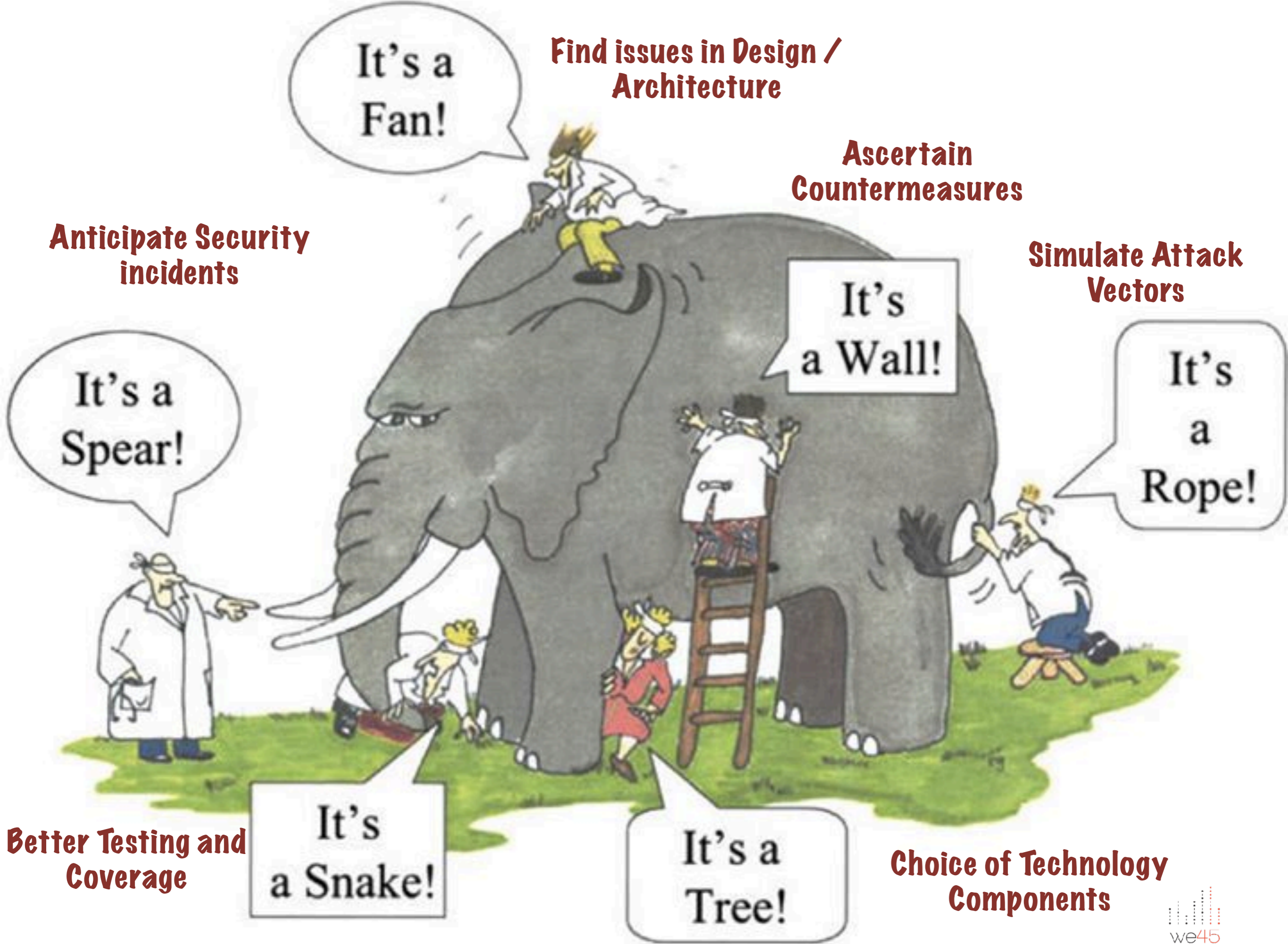
“Threat Modeling in 30 days!”



But at Ground Zero....



Why do These Things Keep Happening?



It's a Fan!

Find issues in Design / Architecture

Ascertain Countermeasures

Simulate Attack Vectors

Anticipate Security incidents

It's a Wall!

It's a Rope!

It's a Snake!

It's a Snake!

It's a Tree!

Choice of Technology Components

Better Testing and Coverage

~~Definition of Threat Modeling~~

Motivation to Threat Model

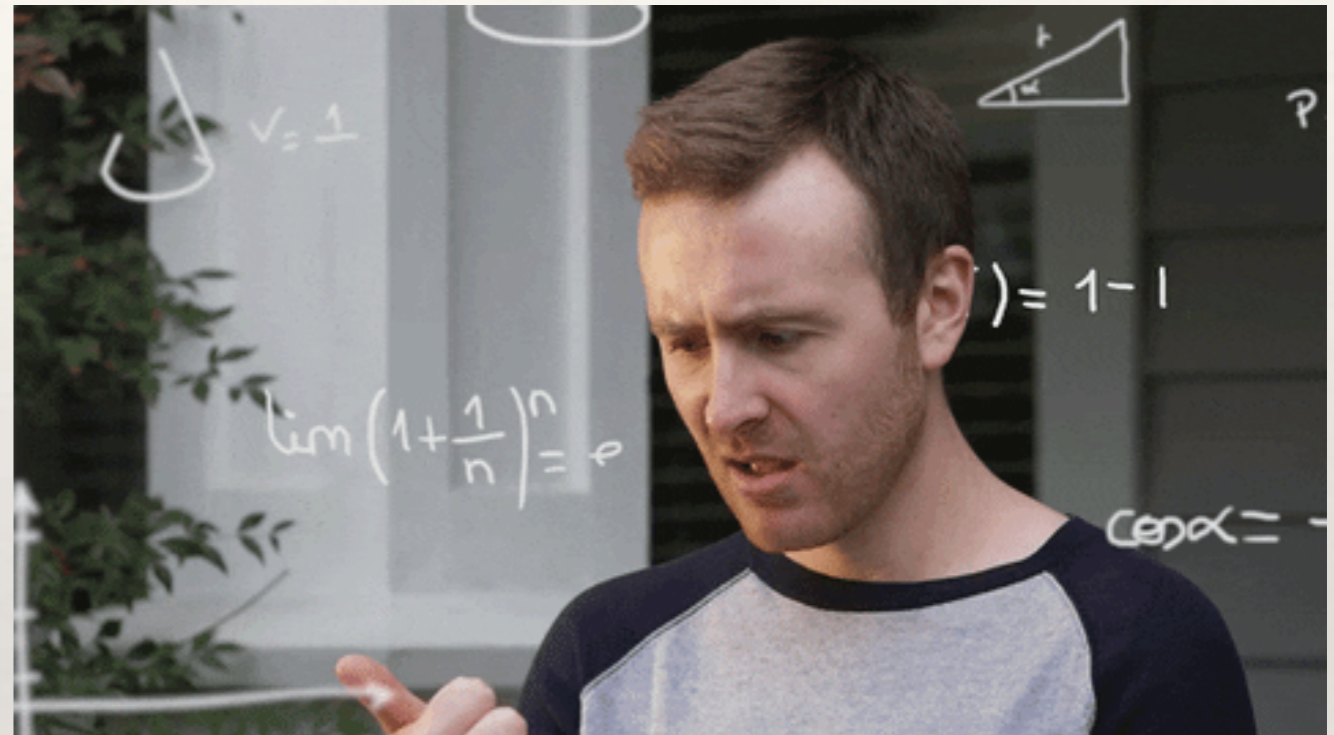
1. Not understanding WHY

- ❖ Identify architecture / design flaws
- ❖ Understand inherent threats to system components
- ❖ Evaluate attack surfaces : abuse cases
- ❖ Ascertain depth of security test cases
- ❖ Change - Impact Analysis

PS : “There is no one size fits all”

2. An over-emphasis on HOW

- ❖ What methodology should I use?
- ❖ What tool should I use?
- ❖ How should it be documented?
- ❖ Who should be doing it?
- ❖ Is it complex enough?



PS : “Document what you do, not the other way around”

The Threat Modeling Schools of Thought

Story Driven Threat Modeling

Attack Driven - What If?

Abuse Cases

Post Design / Development

Security Professionals / Developers

Focus on Depth

E.g : ThreatPlayBook, Manual

Component Driven Threat Modeling

System Driven

Known Issues

Pre Design / Design

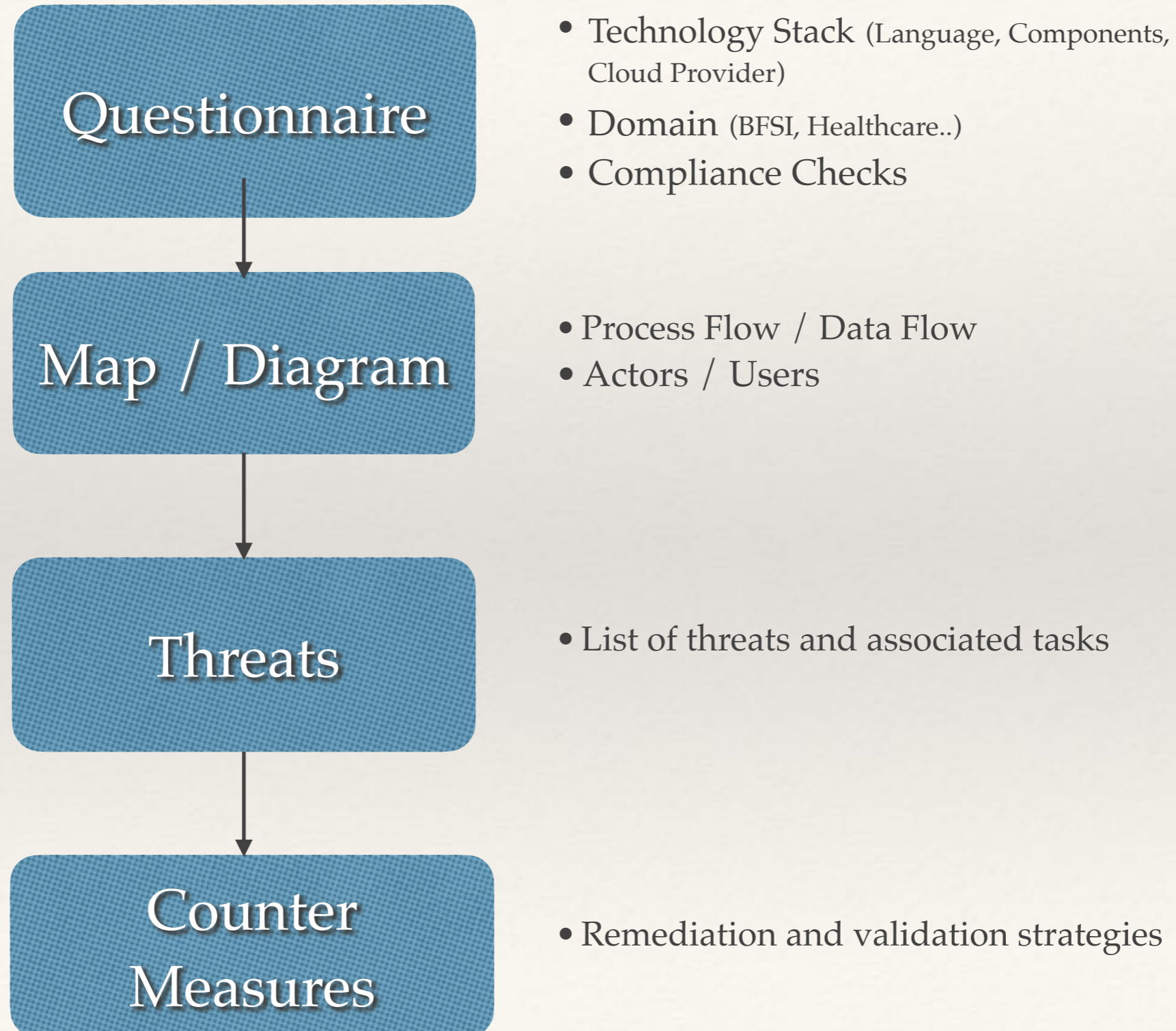
Security Professionals / Developers / Architects

Focus on Scale

E.g : Ir*** *i**, *D *l*m**t*

Component Driven Threat Modeling

Generic Workflow



Story Driven Threat Modeling

The Anatomy

Use Case

What is the functionality?

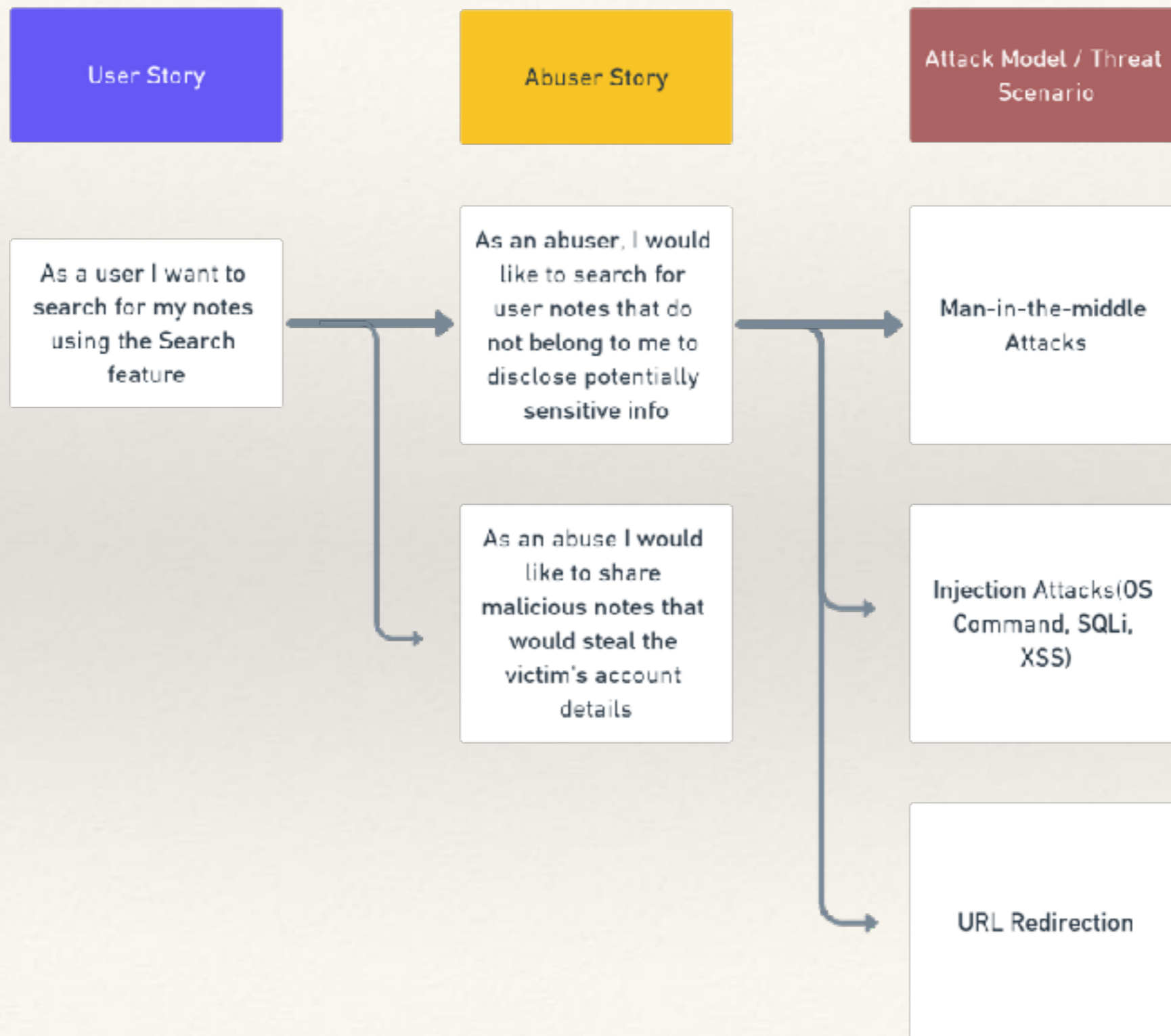
Abuse
Case

What all can go wrong with it?

Attack
Model

How can an abuse case
come to life?

An example



THREAT PLAYBOOK

<https://github.com/we45/ThreatPlaybook>

Threat Playbook

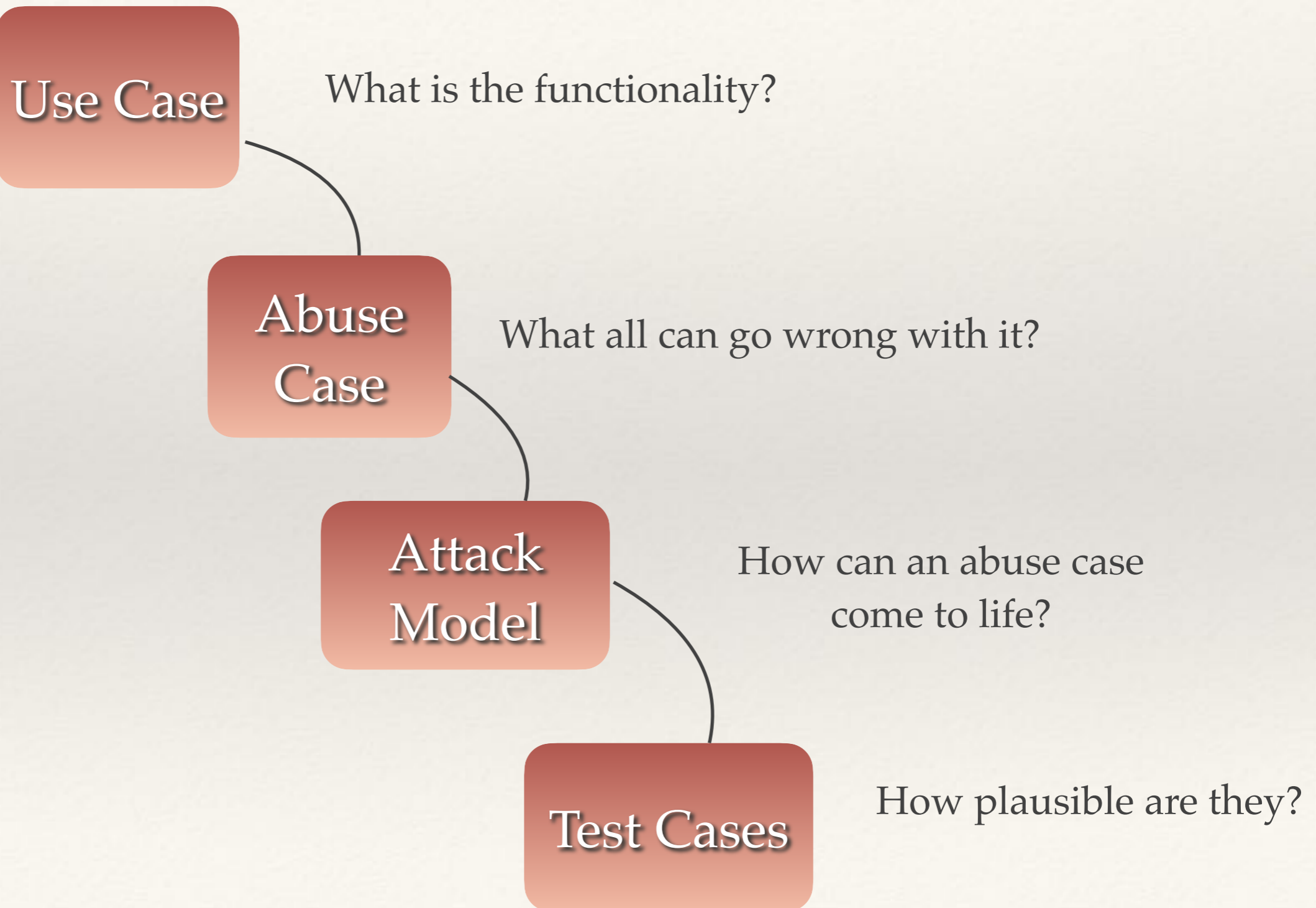
- ❖ “Threat-Modeling-As-Code” framework built on Python, MongoDB, GraphQL
- ❖ Best suited for Story driven threat modeling
- ❖ Threat-to-vulnerability correlation using CWE IDs
- ❖ Automation friendly, developer centric and open source

Threat Playbook - A Demo

Threat Modeling

A means to efficient Security Testing

The Anatomy



User Story

Abuser Story

Attack Model / Threat Scenario

Security Test Cases

As a user I want to search for my notes using the Search feature

As an abuser, I would like to search for user notes that do not belong to me to disclose potentially sensitive info

As an abuse I would like to share malicious notes that would steal the victim's account details

Man-in-the-middle Attacks

Injection Attacks(OS Command, SQLi, XSS)

URL Redirection

Check if the application renders all pages in HTTPs across the board

Check for known SSL/TLS vulns.(POODLE, BEAST, SWEET32, etc.)

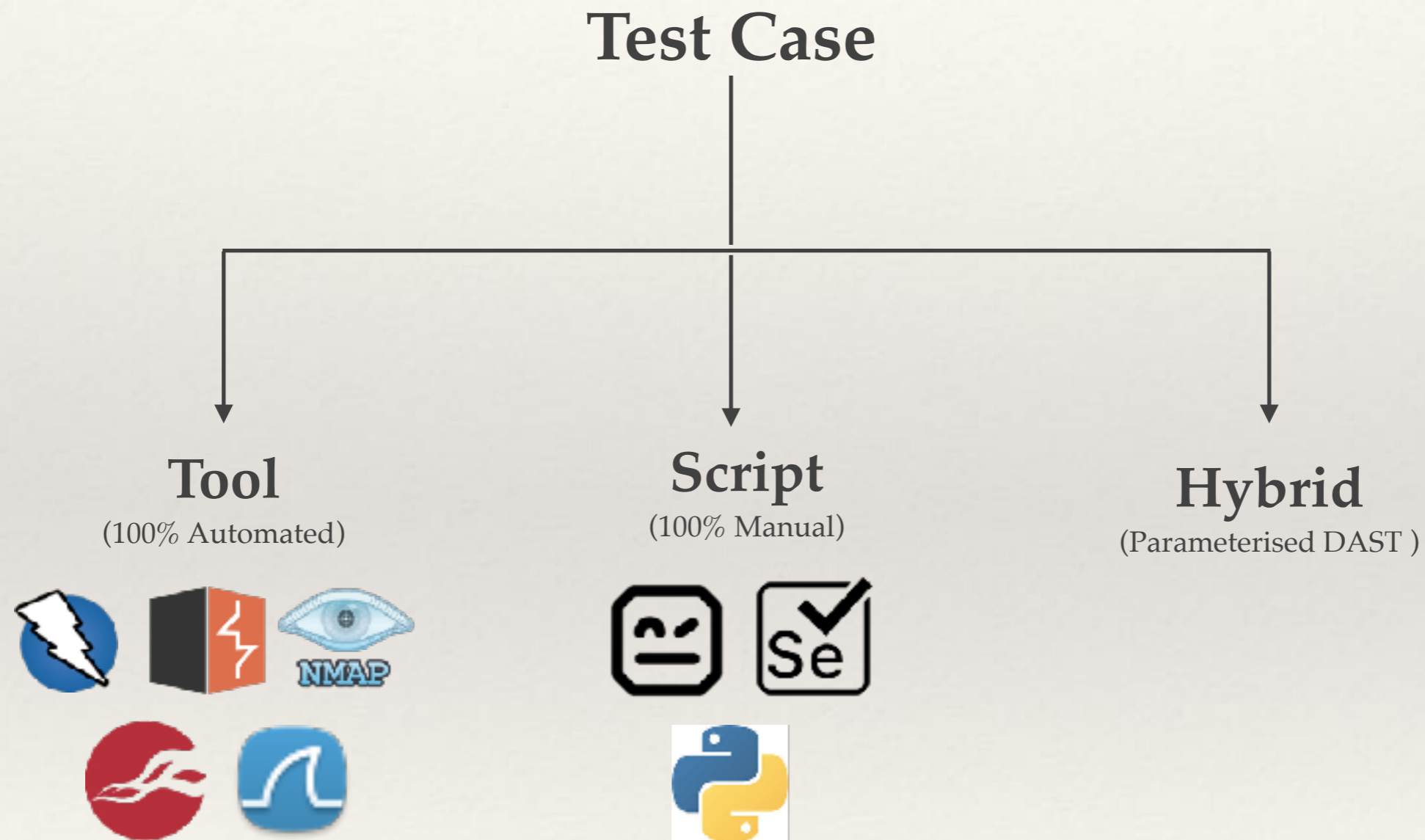
Check for HSTS implementation on the server side

Check for SQLi payloads

Ensure that the app does client side validation of user input



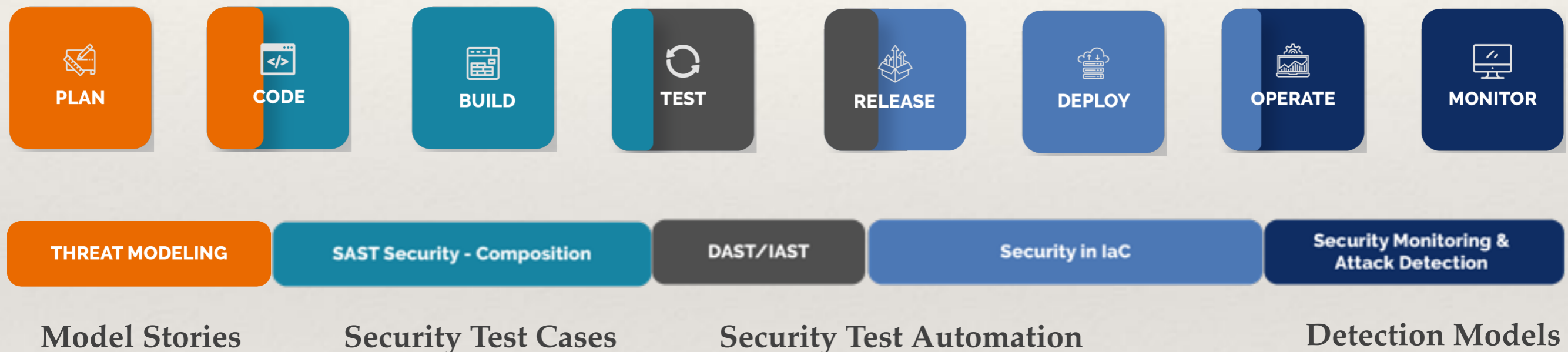
The Link to Automation



The Whole Nine Yards!



Agile Threat Modeling

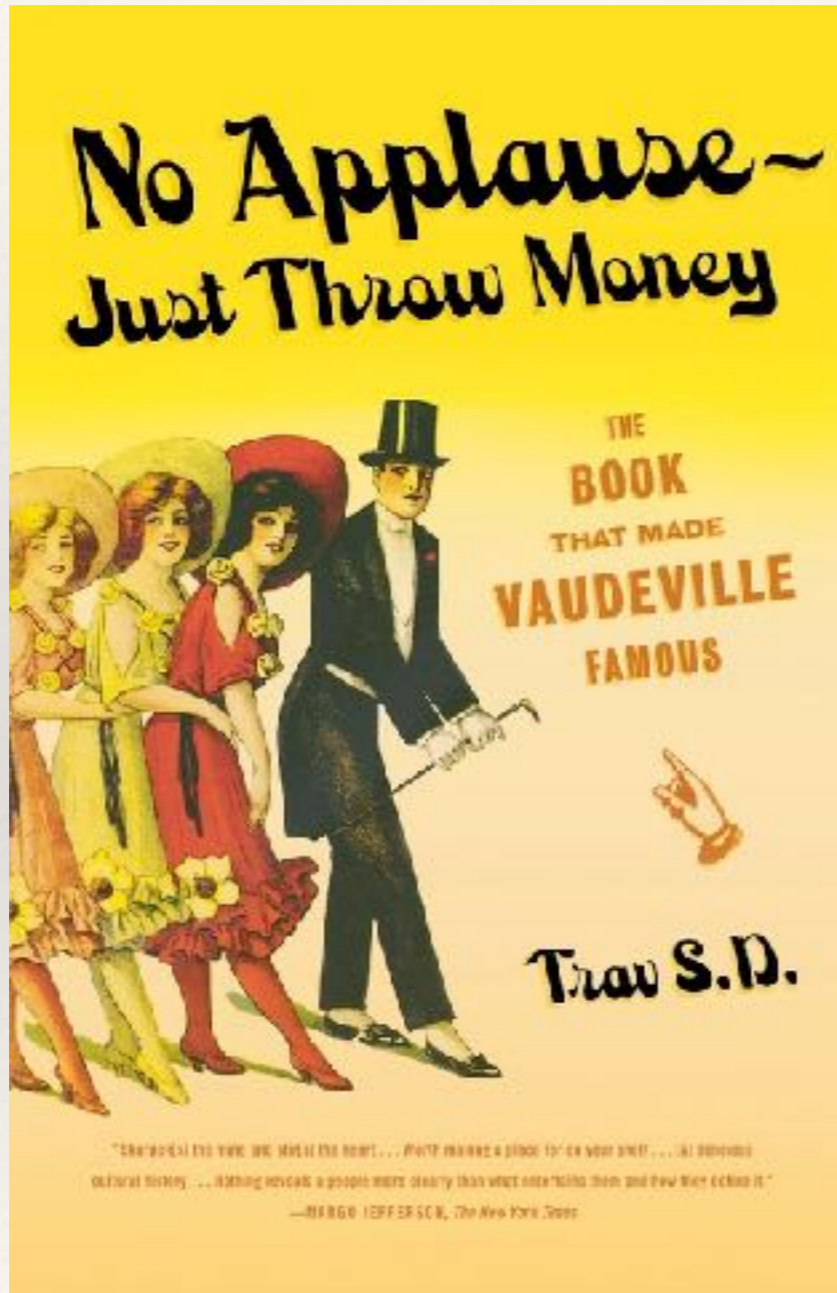


In Summary

- ❖ Know what works best for you!
- ❖ Balance between Depth and Scale
- ❖ Make Threat Modeling more accessible
- ❖especially to QA!
- ❖ Frequent Threat Modeling = Per Sprint
- ❖ Incremental + Consistent + Collaborative =



Thank You!



rahul@we45.com



@we45



we45

