KROLL

Breaking Down Threat Modeling Barriers in Agile AppSec

Rahul Raghavan

Senior Vice President (AppSec Advisory) Cyber Risk

Yours Truly

- Software Developer turned Security Engineer turned Techno Marketing Chappie!
- 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!

Kroll – Application Security Programs

Tooling

- SAST/SCA/DAST optimization
- Custom security automation and integration
- Security within /of the CI/CD

Metrics & Dashboards

- Vulnerability Correlation
- Feedback loops (Threat to Vulnerability mapping)
- Program effectiveness and future state readiness

Threat Modeling

- Story Driven and Component Driven modelling
- Mapped to engineering personas
- Program design and development

Skill Development

- Security Champions Program
- Brown-bag trainings
- Table-top walkthrough sessions

Program Development

- Maturity/Gap Assessments
- BSIMM/ OWASP SAMM framework implementations
- Strategy and Policy Development

Agile Penetration Testing

- Build-Operate-Transfer programs
- Smart automation to maximize efficiency
- Security Regression

Over the next 45 mins...

- Why Threat Model?
- Common Reasons for Failure
- Threat Modeling Schools of Thought
- 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

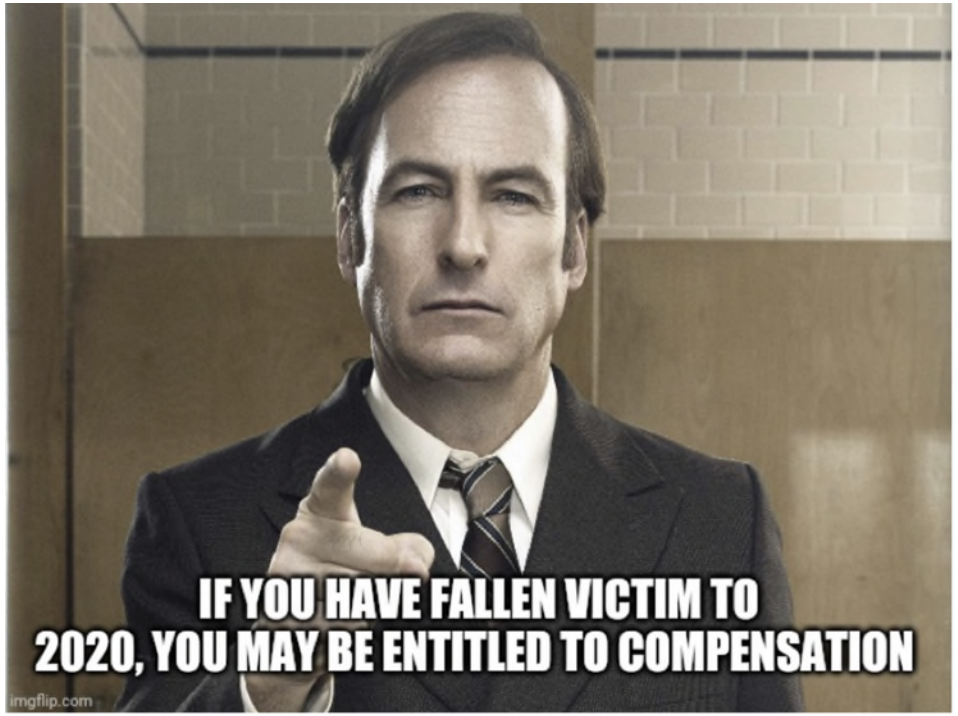
“Find 30% of issues even before they’re coded”

”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...

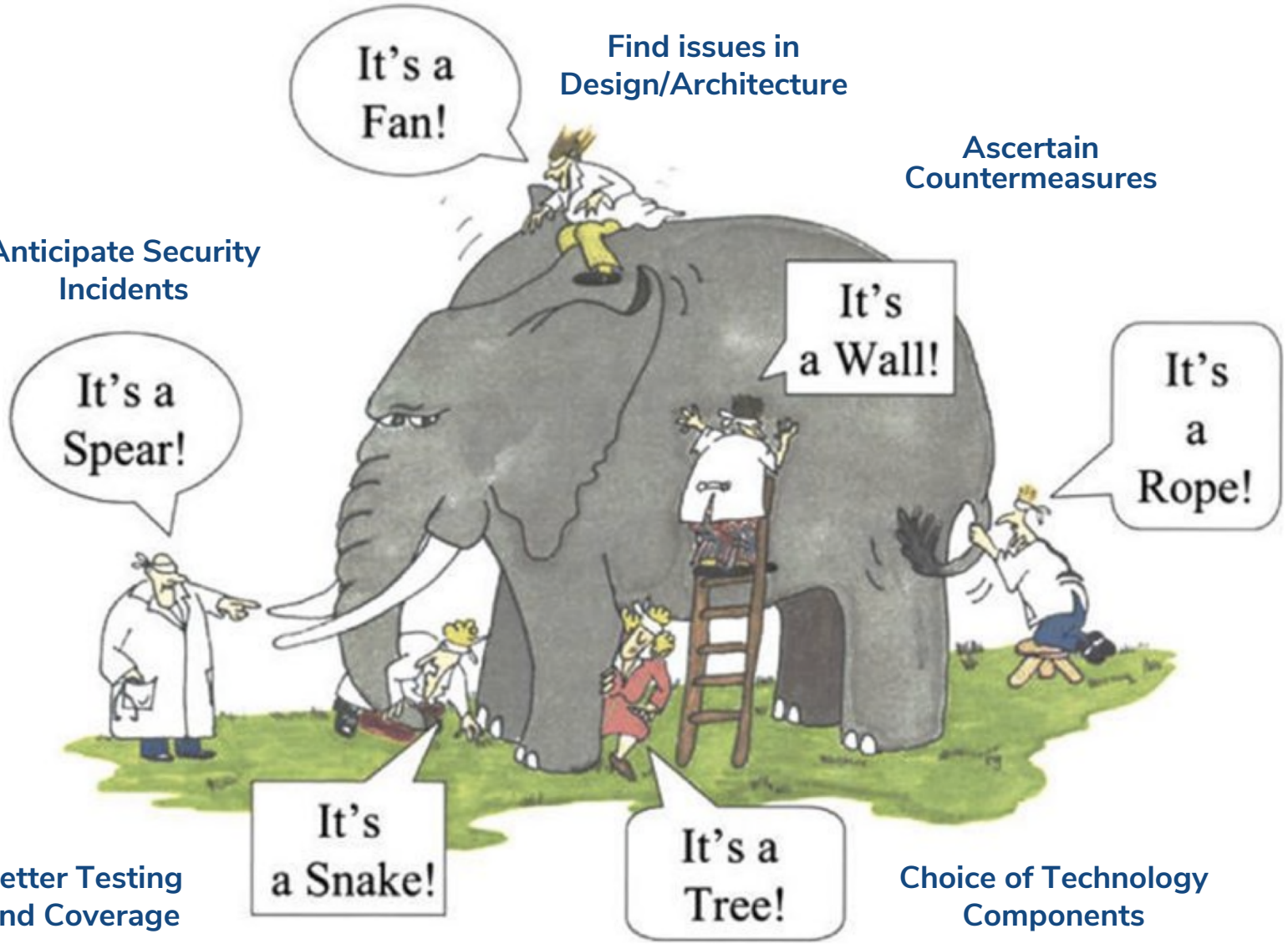
Why do Threat Models Fail?

Definition of Threat Modeling

Find issues in Design/Architecture

Ascertain Countermeasures

Anticipate Security Incidents



Simulate Attack Vectors

Better Testing and Coverage

Choice of Technology Components

~~Definition of Threat Modeling~~

Motivation to Threat Model

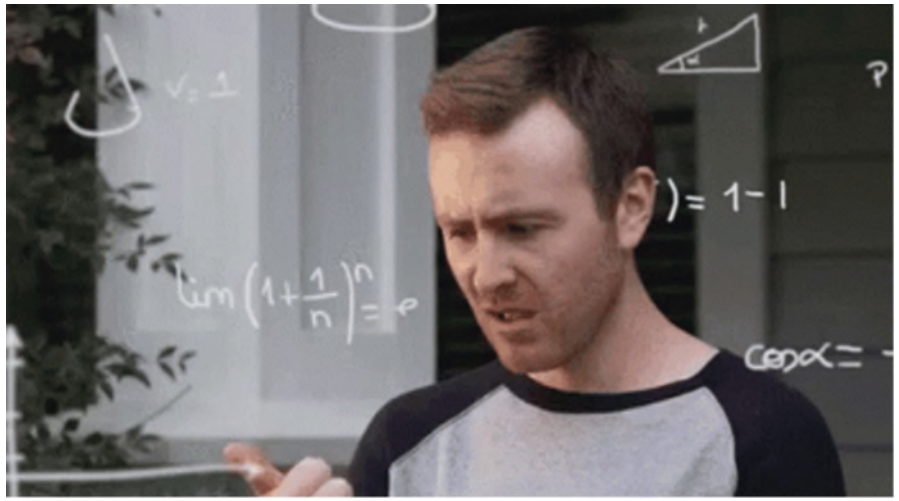
1. Not Understanding WHY

- Identify architecture / design flaws
- Understand inherent threats to system components
- Evaluate attach 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: “Progress over Perfection!”

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: Manual / Open Source

Component Driven Threat Modeling

System Driven

Known Issues

Pre-Design / Design

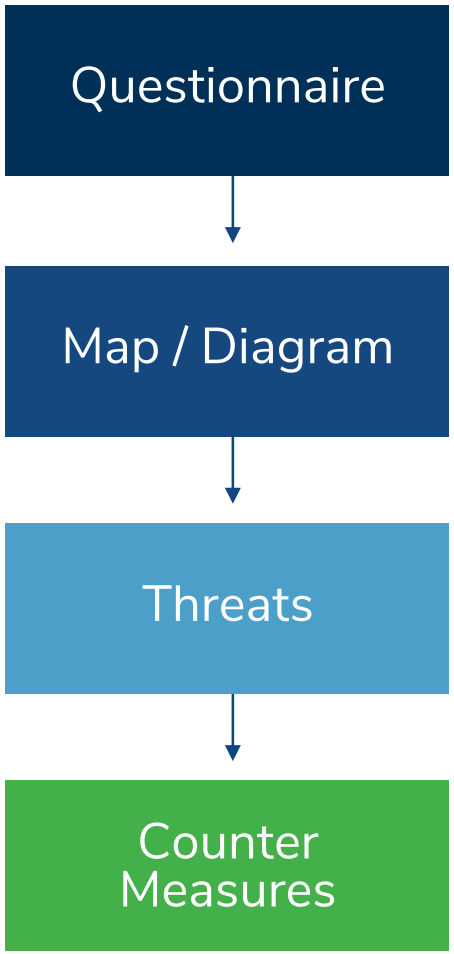
Security Professionals / Developers / Architects

Focus on Scale

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

Component Driven Threat Modeling

Generic Workflow



- Technology Stack (Language, Components, Cloud Provider)
- Domain (BFSI, Healthcare...)
- Compliance Checks

- Process Flow / Data Flow
- Actors / Users

- List of threats and associated tasks

- Remediation and validation strategies

Story Driven Threat Modeling

The Anatomy

Use Case

- What is the functionality?

Abuse (Misuse) Case

- What all can go wrong with it?

Attack Model

- How long can abuse case come to life?

An Example


User Story
Abuser Story
Attack Model / Threat Scenario
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 abuser, 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

Threat Modeling

A means to efficient Security Testing

The Anatomy

Use Case

- What is the functionality?

Abuse / Misuse Case

- What all can go wrong with it?

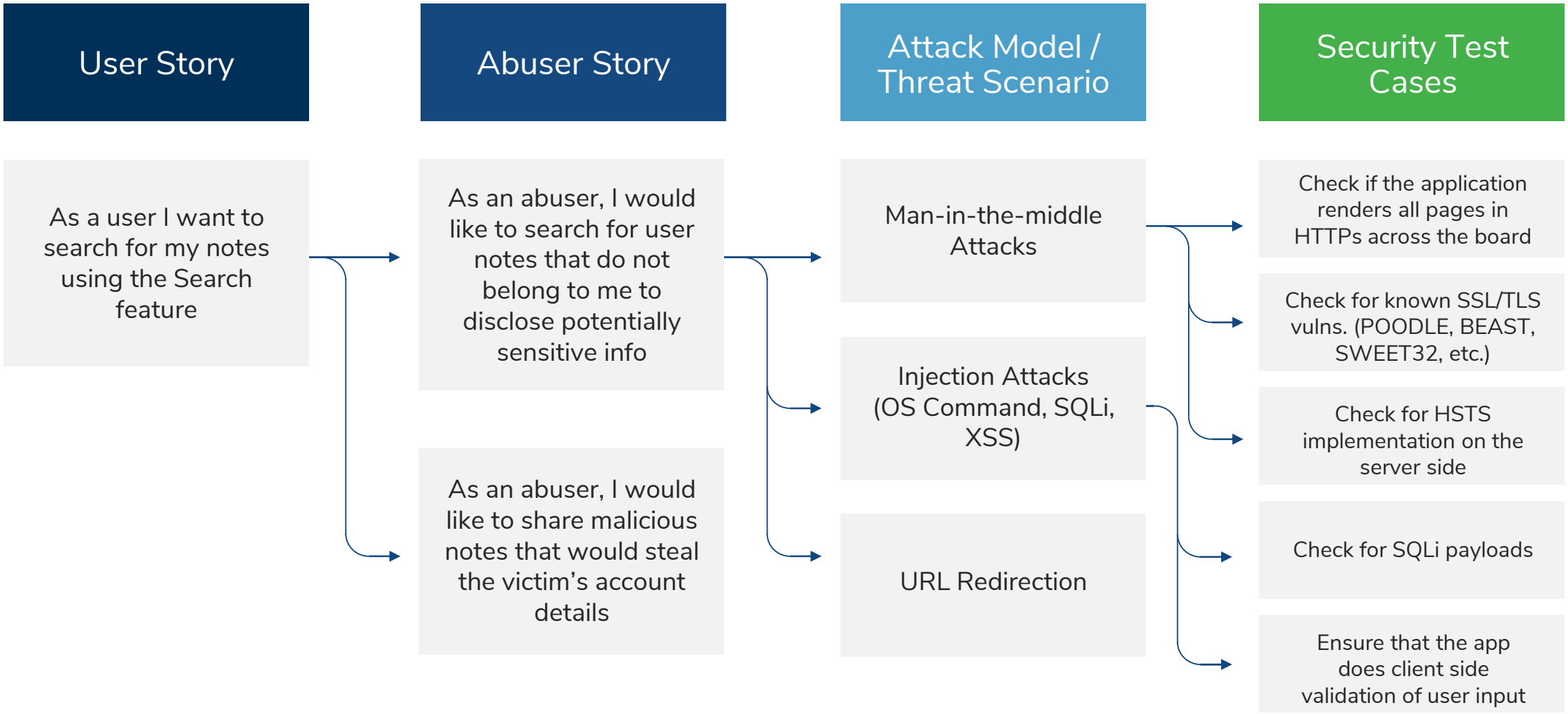
Attack Scenario

- How can an abuse case come to life?

Test Scenario

- How plausible are they?

An Example


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 abuser, 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

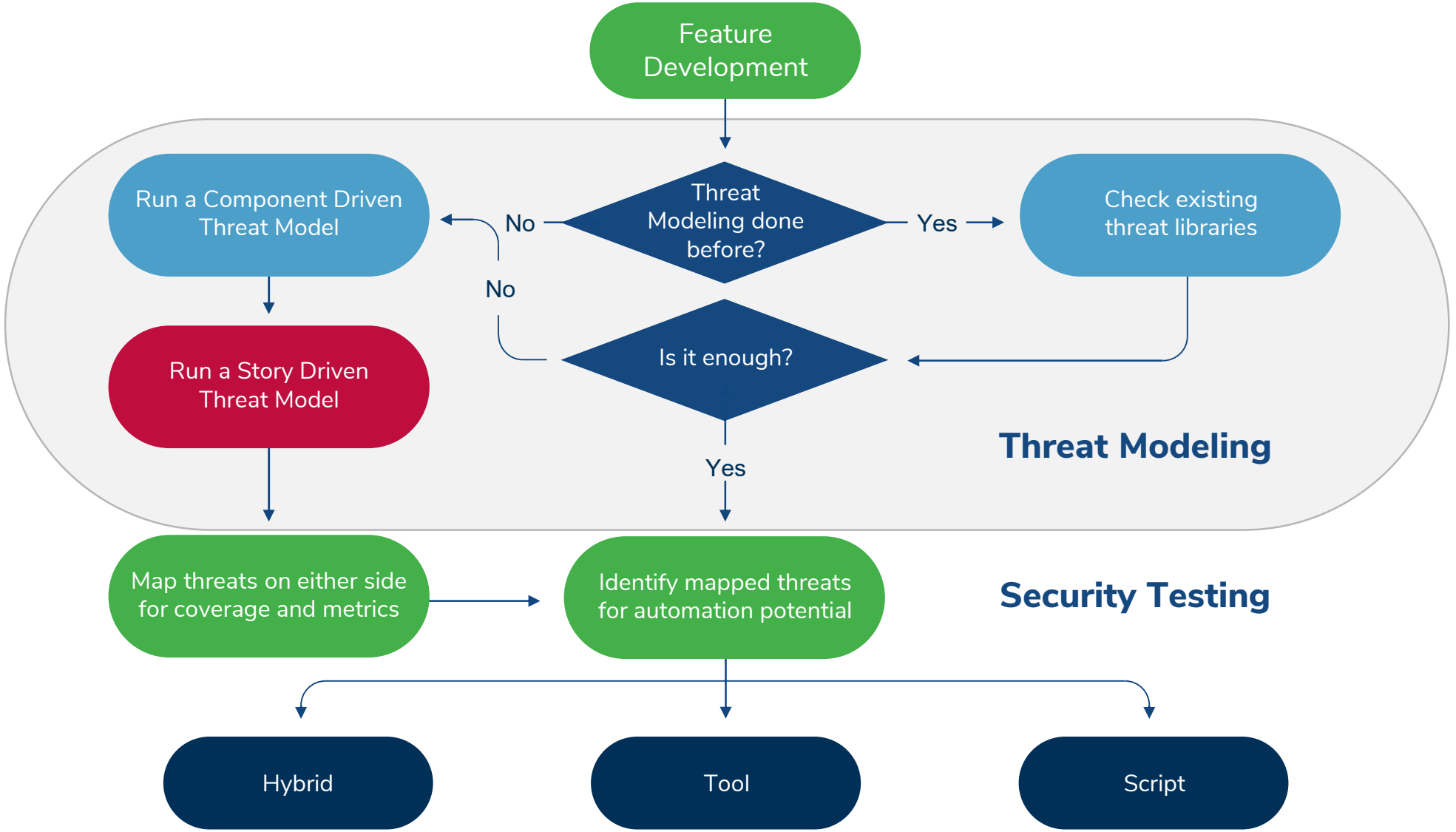
Test Case

Tool
(100% Automated)

Script
(100% Manual)

Hybrid
(Parameterised DAST)

The Whole Nine Yards!



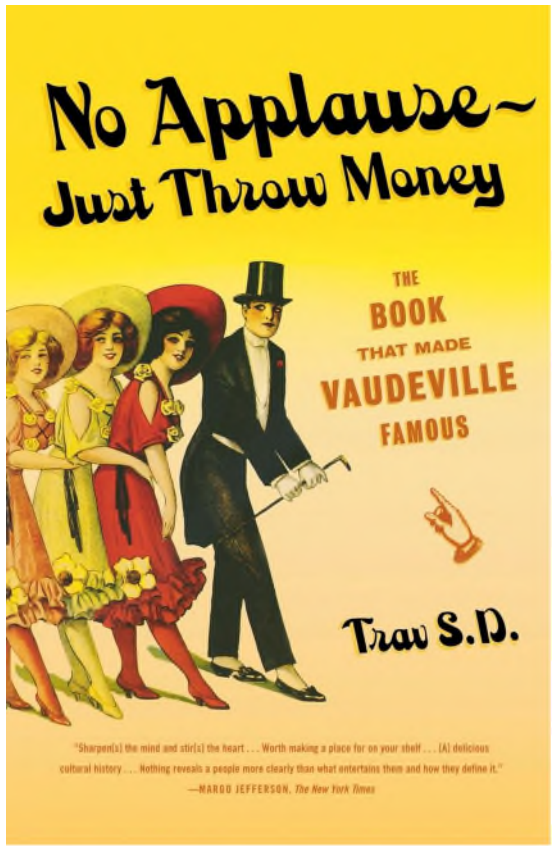
Agile Threat Modeling

Model Stories **Security Test Cases** **Security Test Automation** **Detection Models**

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.Raghavan@kroll.com

@rahul_raghav

torahulraghavan

[Kroll Threat Modeling Service Page]

[Kroll AppSec Service Page]