The Clutter That's Choking AppSec

Rahul Raghavan, Co Founder & Chief Evangelist, we45

Yours Truly

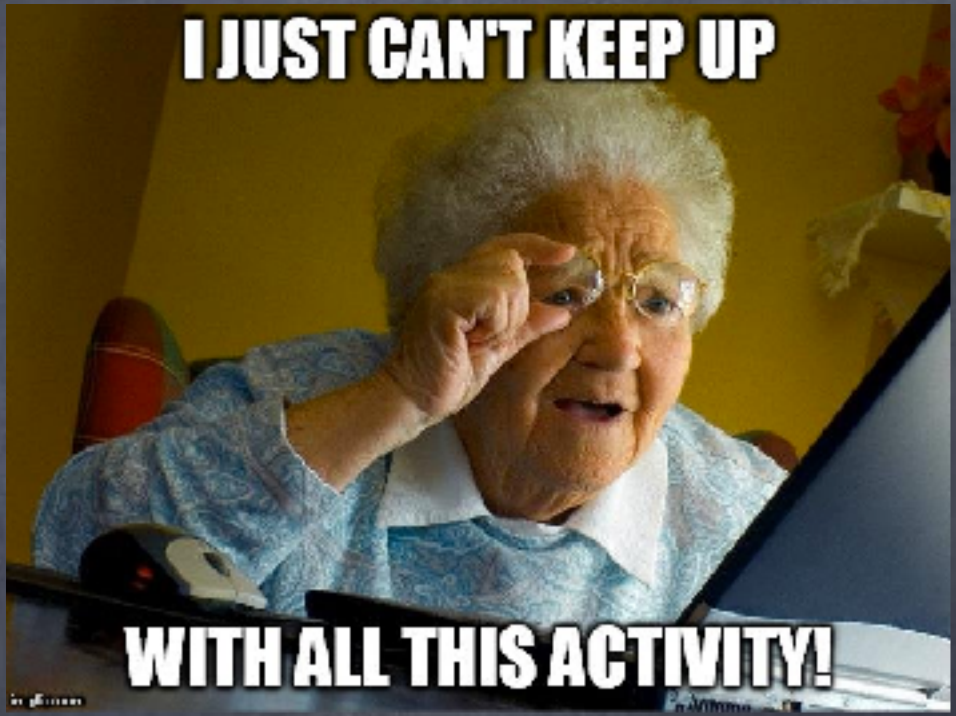
- Software Developer turned Security Engineer turned Techno Marketing Chappie!
- Co Founder, Head of Pre-Sales and Client Solutioning at we45
- Things that prevent me from kicking myself to work
  - DevSecOps and AppSec Automation
  - Automation RoI Realisation Models
  - Risk Based Vulnerability Management
  - Appsec 2.0

Product Engineering Today

- Waterfall…Agile…AgileFall??
- Accelerated Deployments - Advent of DevOps
- Microservices and Serverless Architecture
- Dependence on Third Party Libraries
- Automation Testing - Functional and Performance

we45

Application Delivery



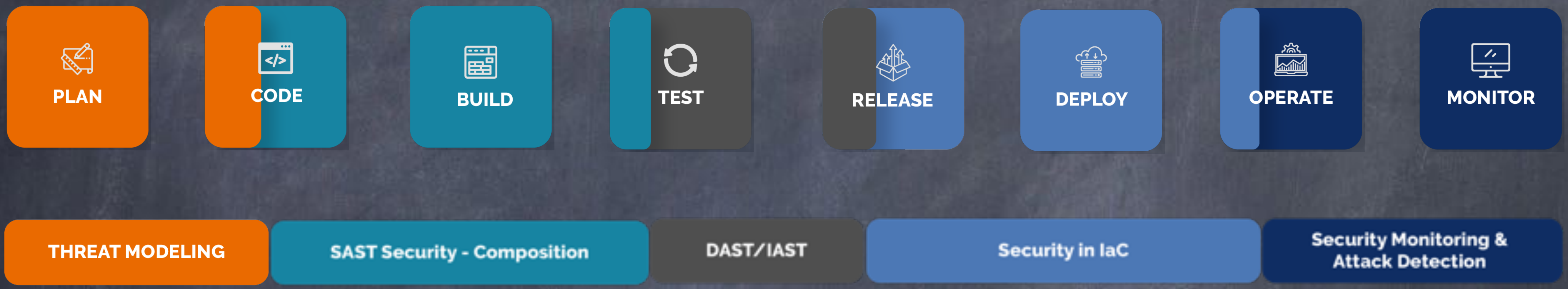
Or...

GREAT SCOTT!
THAT'S A BIG NUMBER!
I JUST CAN'T KEEP UP
WITH ALL THIS ACTIVITY!

The Advent of DevSecOps

- Security = Continuous Feedback + Improved Automation
- End of chain activities broken down to piece meal engagements
- Assessments have become more decentralised
- Transformation of engineering tools and platforms - interfacing capabilities

Agile + DevSecOps



PLAN

CODE

BUILD

TEST

RELEASE

DEPLOY

OPERATE

MONITOR

THREAT MODELING

SAST Security - Composition

DAST/IAST

Security in IaC

Security Monitoring & Attack Detection

Ahem!

100:10:1

Dev:Ops:Security

Jason the Tester

AppSec Engg - R & R

Manage Vulnerabilities

Automate tools in CI/CD

Security Assessments

Compliance Audits

Draft Security Reports

Remediation Assistance

Security Research

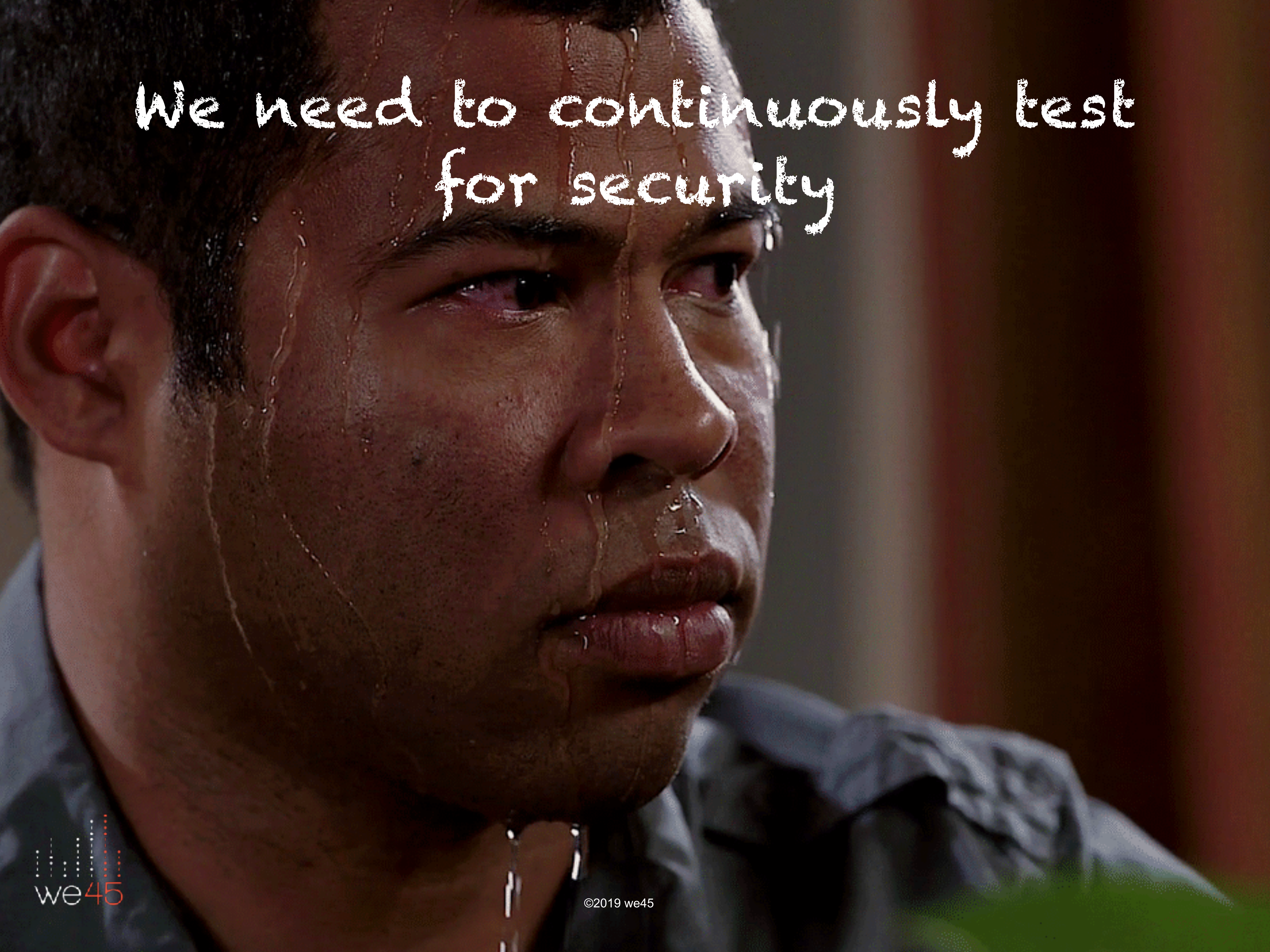
Threat Modelling

Onboard Tools

Validation of Fixes

Respond to customer questionnaires

Security Training



We need to continuously test for security

Jason the Tester

AppSec Engg - R & R

Manage Vulnerabilities

Automate tools in CI/CD

Compliance Audits

Security Assessments

Draft Security Reports

Remediation Assistance

Threat Modelling

Onboard Tools

Validation of Fixes

Respond to customer questionnaires

Security Training

The Anatomy of a Vulnerability

Attributes (DAST)

- Vulnerability Name
- Affected Instance - URL, Method, Parameter
- CWE ID
- CVSS Score
- Vulnerability Description, Remediation, Reference
- Scanner Confidence Score

Attributes (SAST)

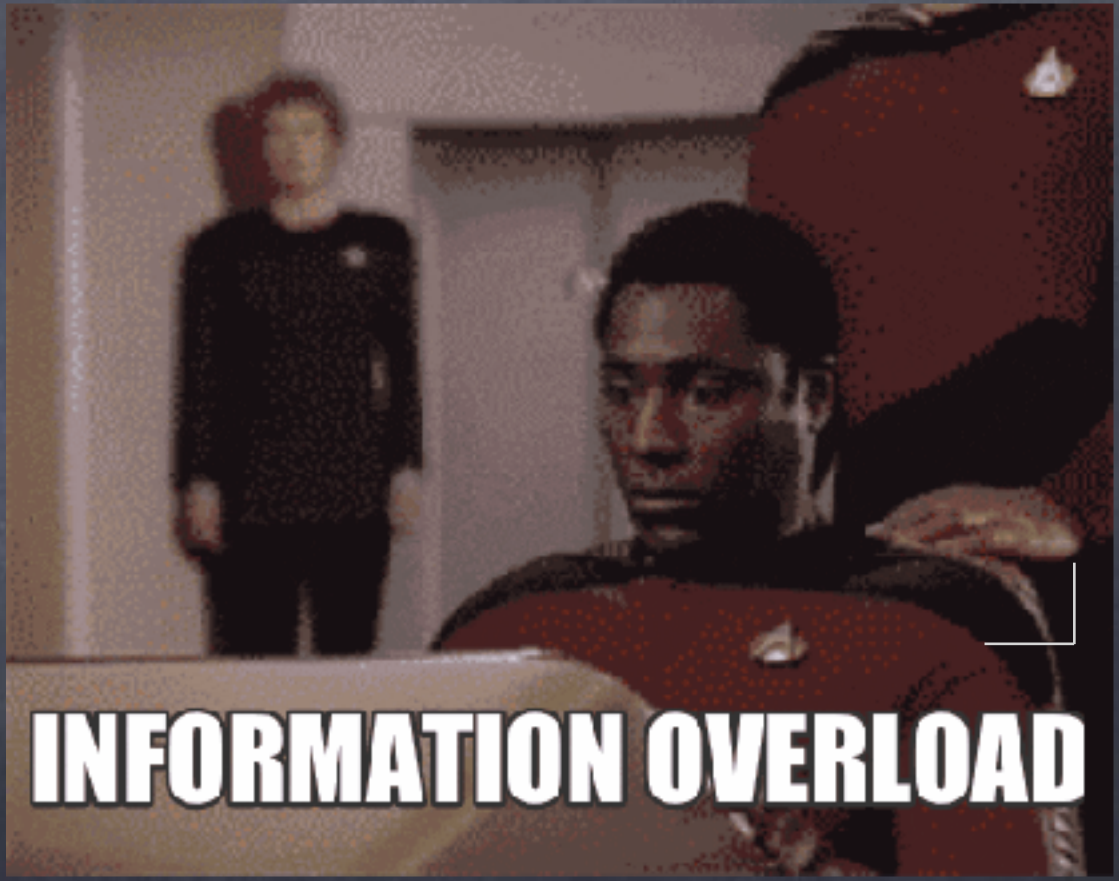
- Vulnerability Name
- Affected Instance - File Path, Starting Line Number, Ending Line Number
- Request / Response Headers
- CWE ID
- CVSS Score
- Vulnerability Description, Remediation, Reference

Attributes (SCA)

- Vulnerability Name
- Affected Instance - Package Name, Package version that's vulnerable
- Request / Response Headers
- CWE ID
- CVSS Score
- Vulnerability Description, Remediation, Reference

Diversity and Scale of Scope

- Servers
- Containers
- Applications
- API Services
- Databases
- Orchestration Services
- Cloud Services
- Third Party Dependencies



THE CLUTTER!

- Vulnerability Overload
  - Triaging Issues
  - Documenting Issues
- Limited Application Security Bandwidth
- Interfacing with Engineering
- Regressing Vulnerabilities
- Effective Remediation

Vulnerability Overload

©2019 we45

Tools - No Consistency

- Different Names for the same vulnerabilities
- Severities dont map out
- Several False Positives
- No CWE Data
- No Risk/Impact/Prioritisation Approach
- Limited Remediation Information
- Limited/No Taxonomy Information

we45

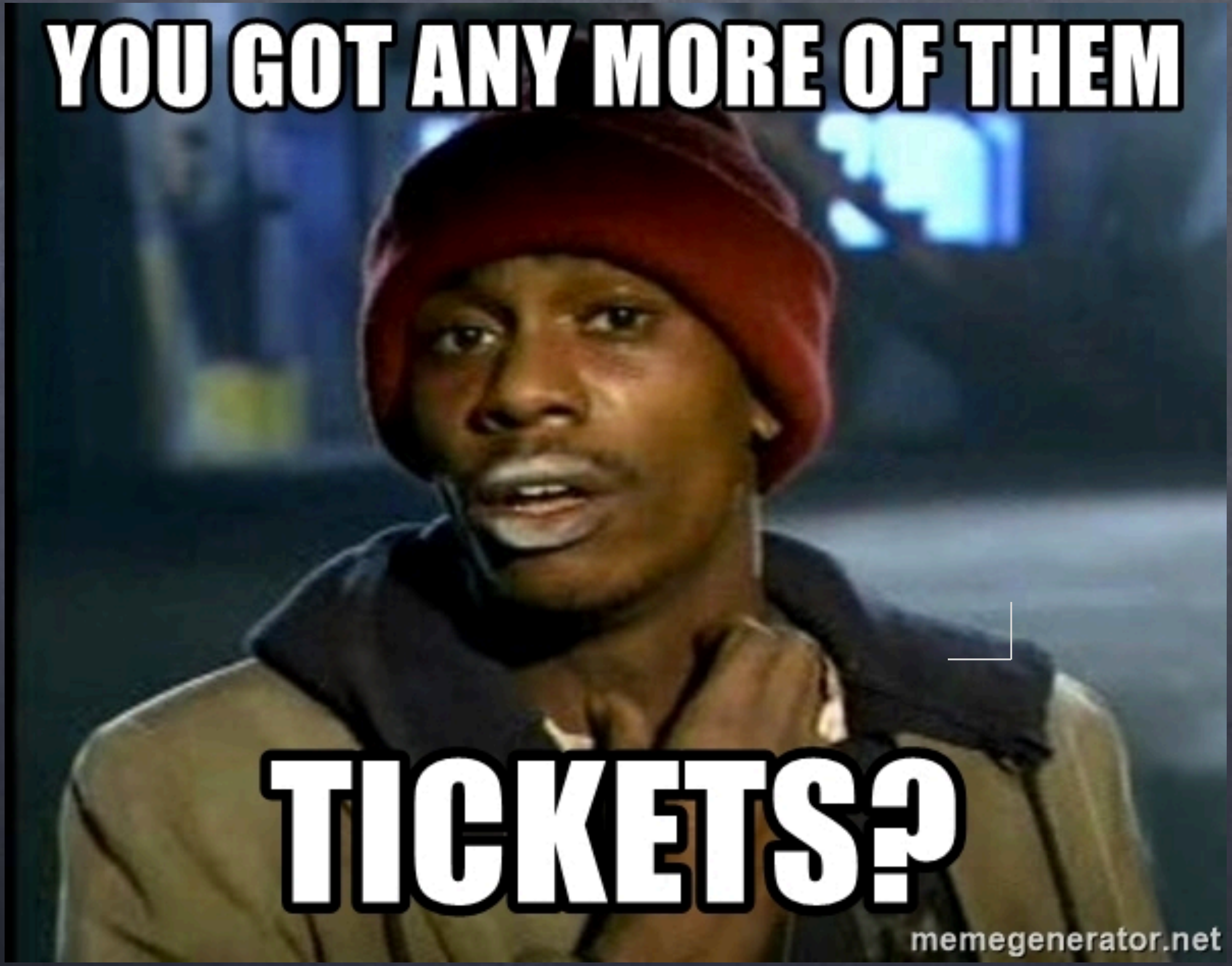
Results inconsistencies

Interfacing with Engineering

Integration Today

Security Teams be Like...

But Engineering Teams be Like…



Integration Points

- CI / CD -
- Bug Trackers - Bugs as Defects
- Communicators (Slack/Chat) - Faster Turnaround
- Metric Dashboards

Automated Correlation

Why Automate Correlation?

- Vulnerabilities at scale => Manual Merge doesn't scale
- Results need to be correlated across tools => SAST, DAST, SCA, IAST
- Eliminates the possibility of ignoring critical vulnerabilities
- Reduces the noise of low severity/inconsequential vulnerabilities
- Standardises Vulnerability Data Model and Nomenclature

Summary

- Application Security Scalability with DevSecOps is the new norm
- Lots o' tools == Lots o' data == Lots o' problems
- Integrate with Engineering Workflows
- Prioritise Remediations and More effective Security Fixes