

OWASP Changing the Game

A study of heroic behavior

Jason Kent
Director, Web Application Security
KzEuNjE0LjQ0Ni4wODcw

Qualys

whoami



Dean's inventions



Dean's inventions



Solutions

- When we are faced with problems, we try to find solutions
- The problems facing today's Application Security professionals are many, but the solutions to them need to be simple

Why Web App Security Matters

Visible Targets

“The inherent need for many web applications to be Internet visible makes them a logical target”

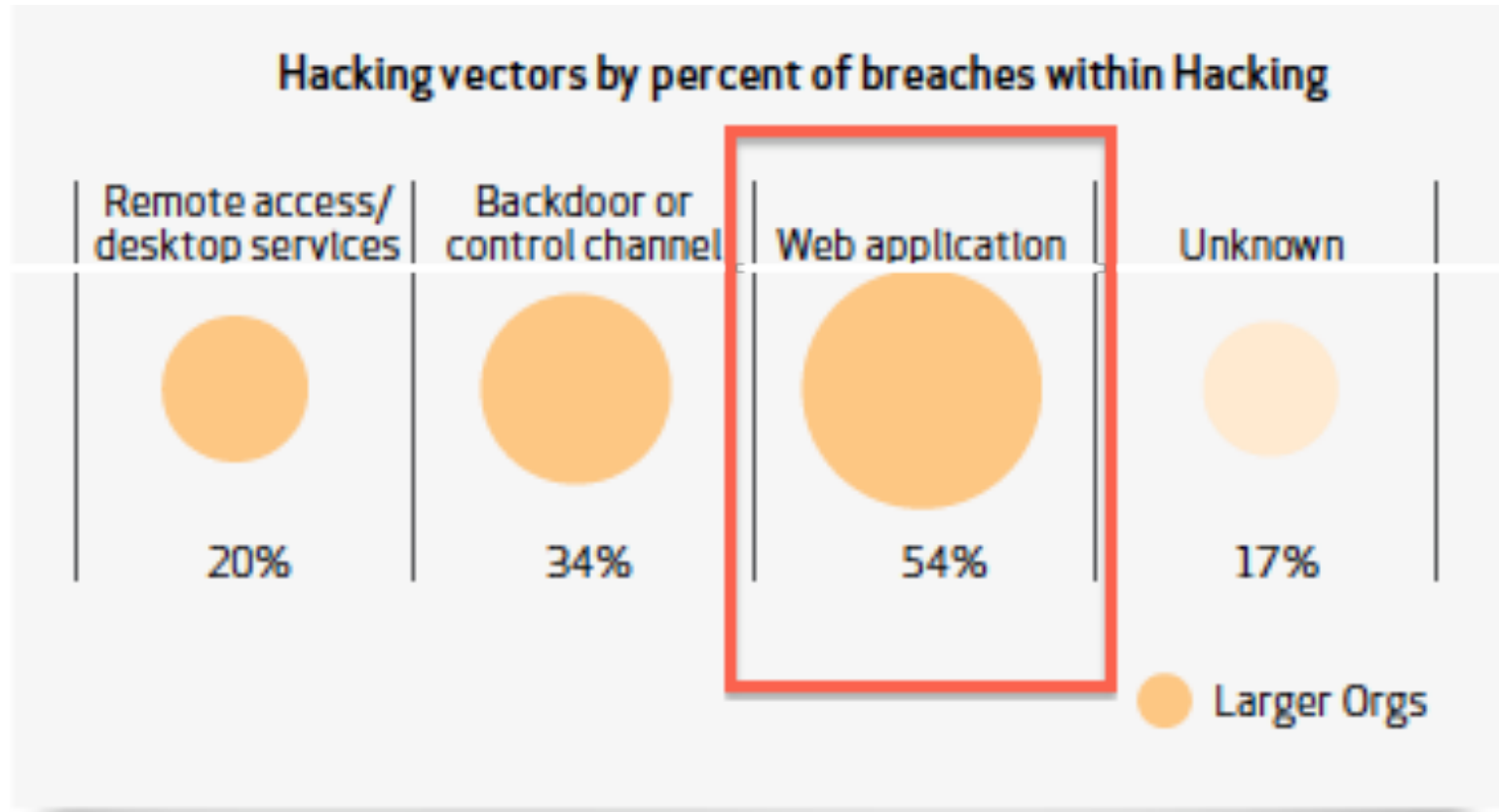
Associated with Data Loss

“Web Applications....were associated with over a third of total data loss”

Popular and Successful Attack Vector

“Web applications abound in many larger companies, and remain a popular (54% of breaches) and successful (39% of records) attack vector. “

Why Web App Security Matters



Why Web App Security Matters

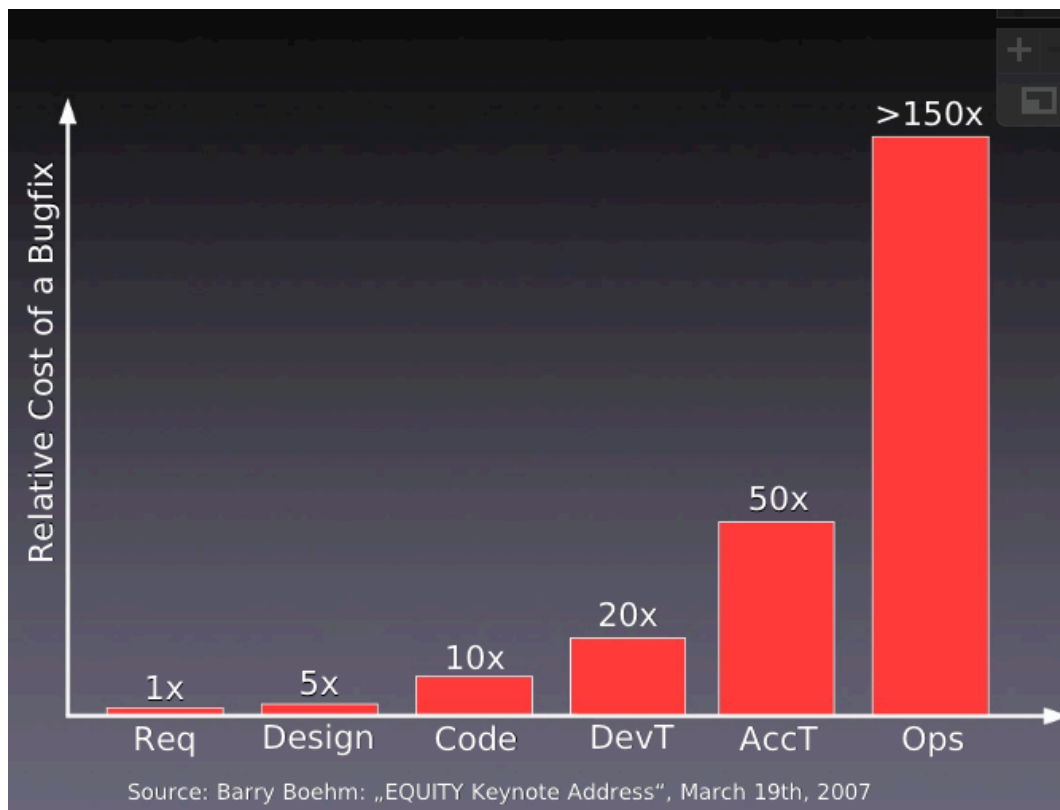
Compromised assets by percent of breaches and percent of records*

Type	Category	All Orgs		Larger Orgs	
POS server (store controller)	Servers	50%	1%	2%	<1%
POS terminal	User devices	35%	<1%	2%	<1%
Desktop/Workstation	User devices	18%	34%	12%	36%
Automated Teller Machine (ATM)	User devices	8%	<1%	13%	<1%
Web/application server	Servers	6%	80%	33%	82%
Database server	Servers	6%	96%	33%	98%
Regular employee/end-user	People	3%	1%	5%	<1%
Mail server	Servers	3%	2%	10%	2%
Payment card (credit, debit, etc.)	Offline data	3%	<1%	0%	<1%
Cashier/Teller/Waiter	People	2%	<1%	2%	<1%
Pay at the Pump terminal	User devices	2%	<1%	0%	<1%
File server	Servers	1%	<1%	5%	<1%
Laptop/Netbook	User devices	1%	<1%	5%	<1%
Remote access server	Servers	1%	<1%	7%	<1%
Call Center Staff	People	1%	<1%	7%	<1%

*Assets involved in less than 1% of breaches are not shown

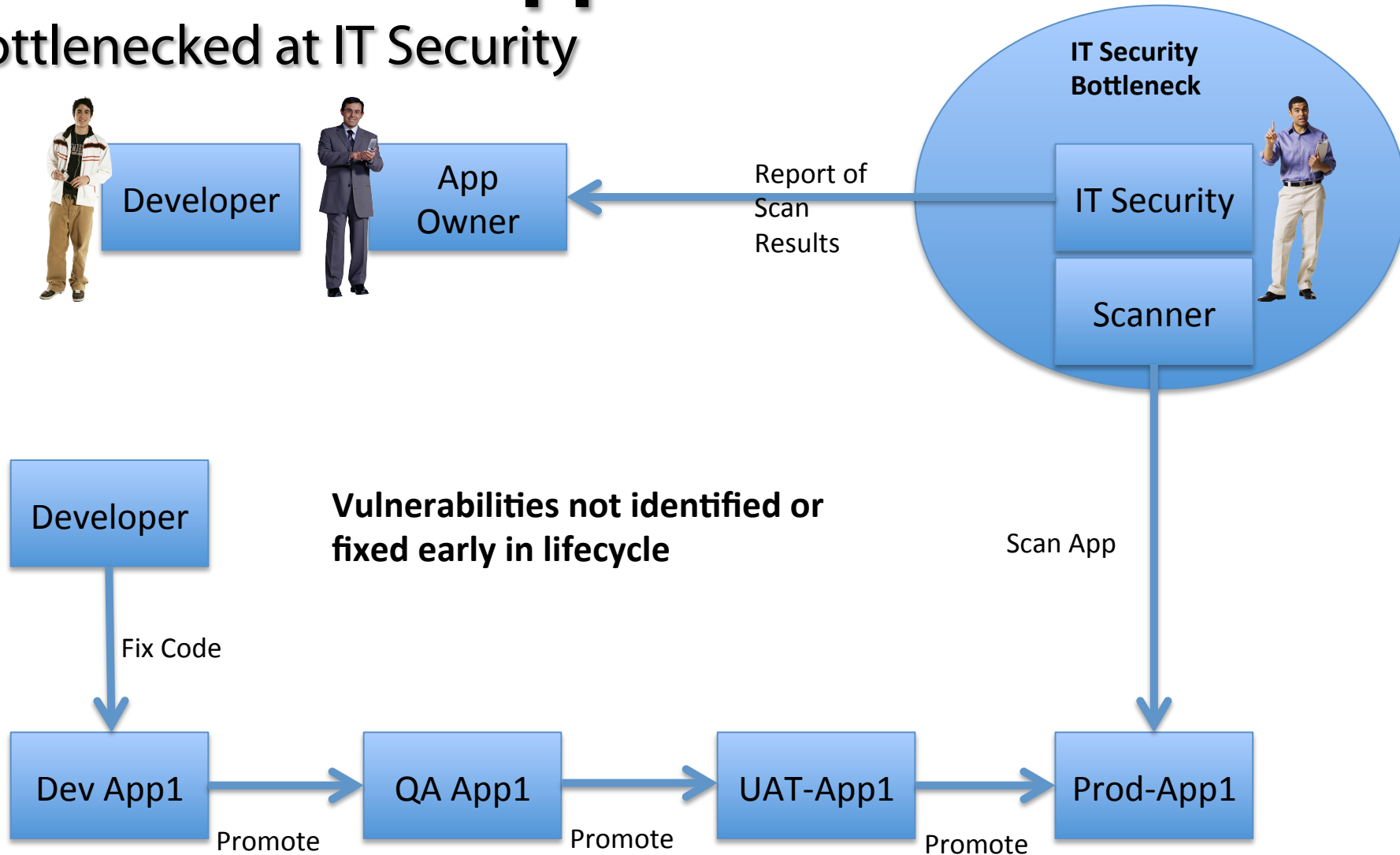
Best Practice - Security Early in Lifecycle

The costs for fixing security flaws are dramatically lower the earlier in the development lifecycle they are fixed



Conventional Approach

Bottlenecked at IT Security



Today

- Web Applications are often not secure
- We spend time chasing the application owners to fix code
- They don't have a project for it and one has to be created
- We spend more time creating paperwork than doing work

App Sec Today



Dean's philosophy

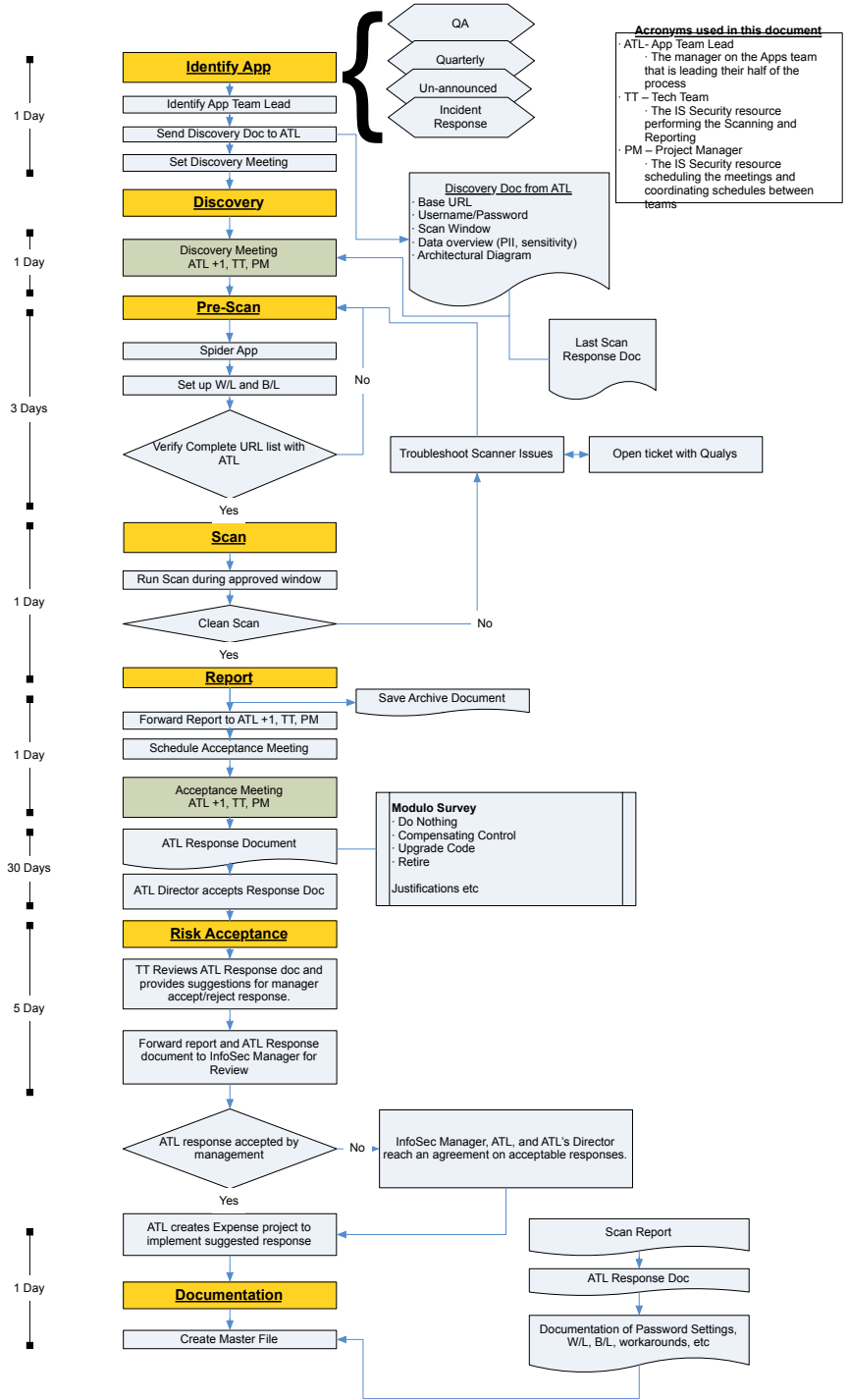
- Never build a south pointing chariot
- Attack the problem in a manner that suits everyone
- Try to find a solution that uses normal behaviors as a guide

Trends

- Some organizations are mandating scanning in the SDLC
 - Most are failing at it
- DEV Teams are begging for a way to get the App Sec Team off of their back

Why failing?



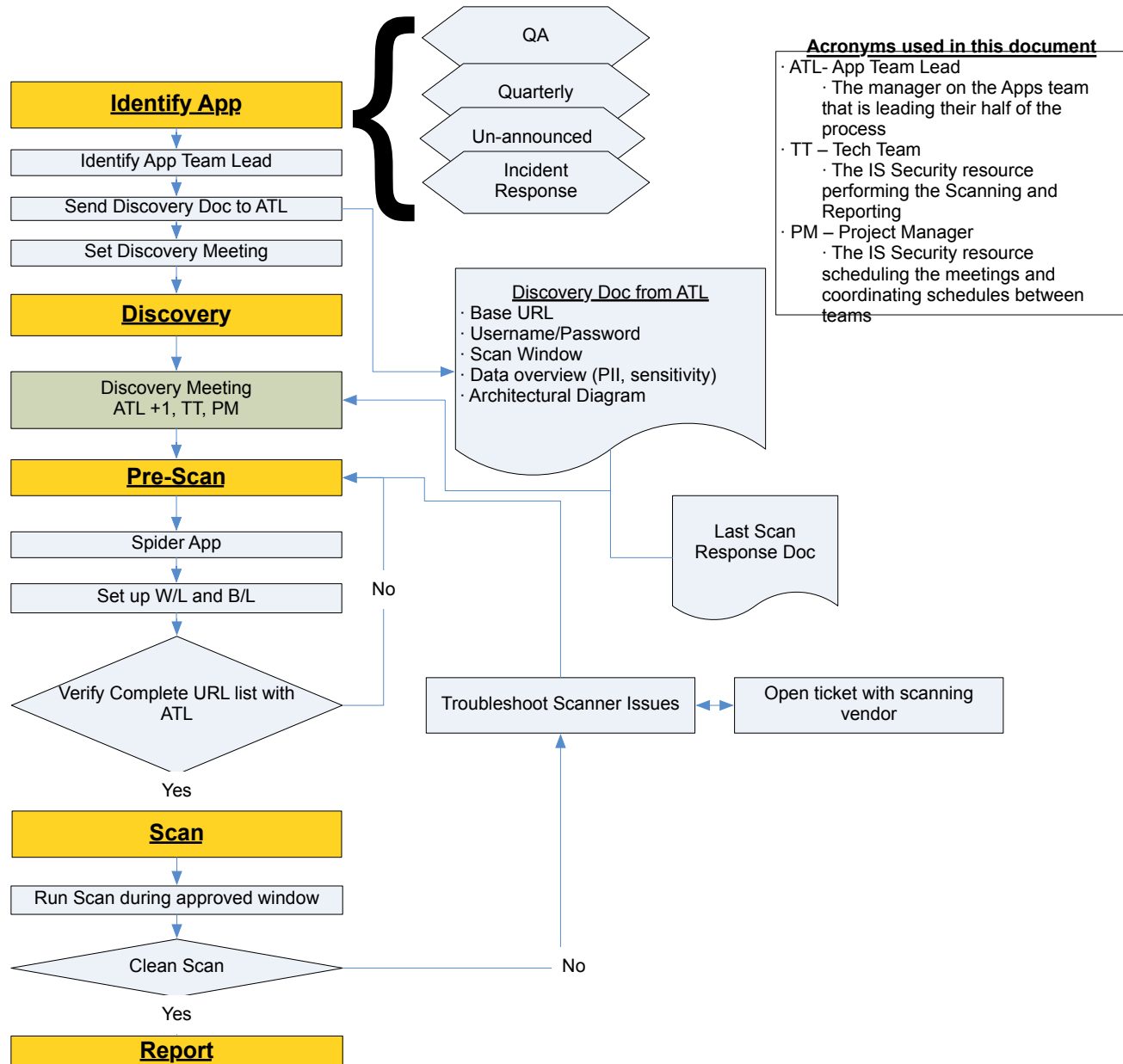


1 Day

1 Day

3 Days

1 Day



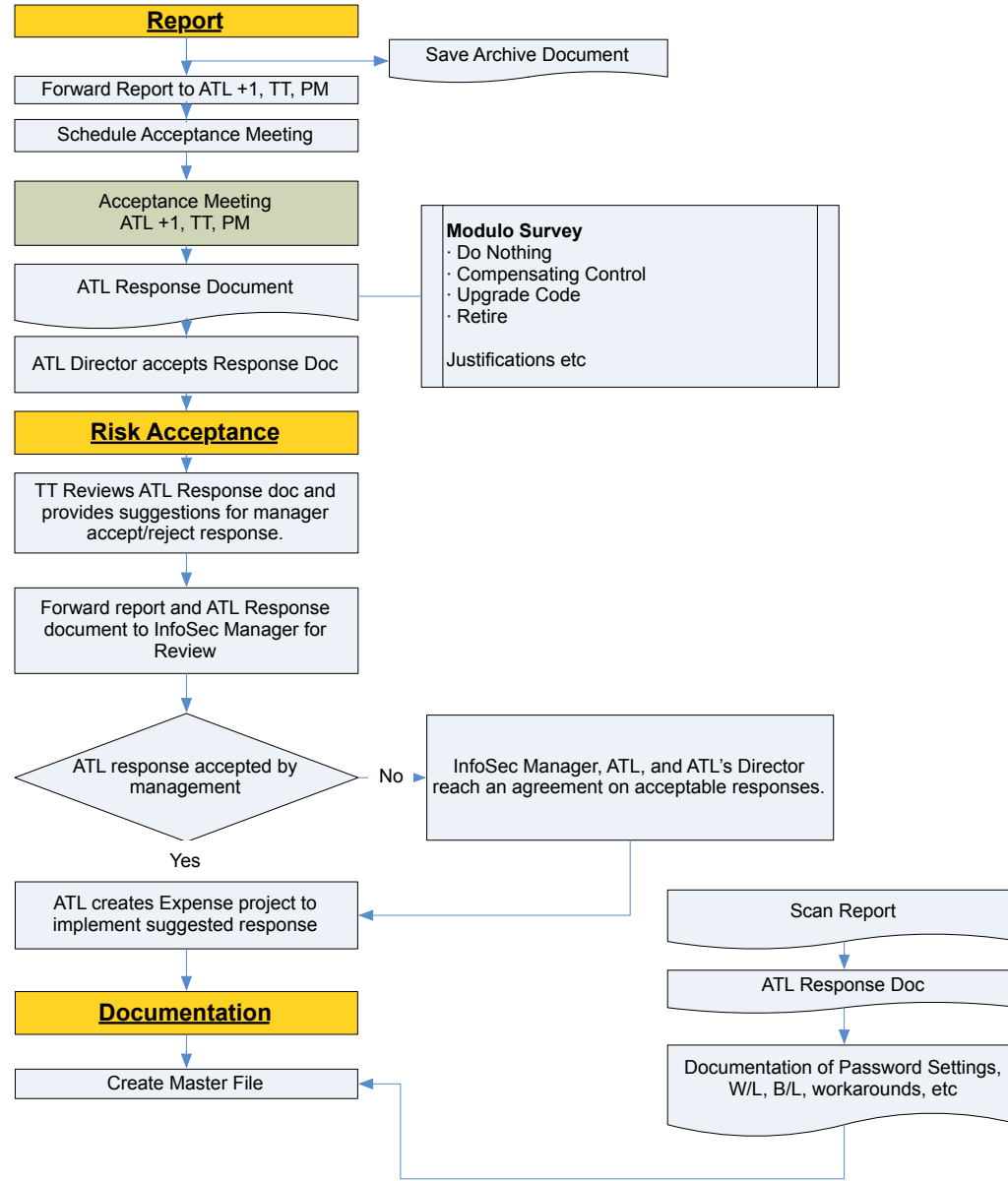
1 Day

1 Day

30 Days

5 Day

1 Day



App Sec Tomorrow

- Security bugs are function bugs
- The same QA processes apply
- The QA team and DEV are familiar with App Sec Tools - Scanners, Proxies (ZAP anyone?) are used as a QA step
- Tools all feed standard DEV reporting tools (Bugzilla)

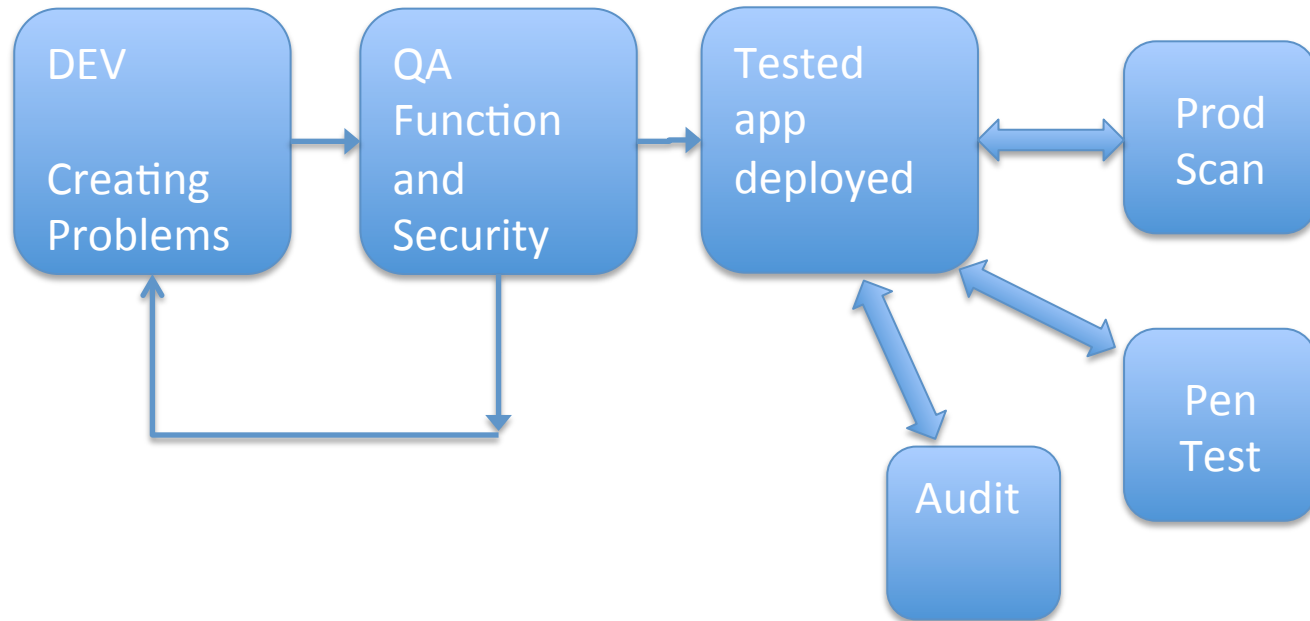
How close are we?

- ZAP is gaining popularity with QA
- Some tools on the market can be setup for QA to use
- Open Source is ruling processes, we need to harness that
 - Selenium
 - Thread Fix

The ultimate workflow

- DEV checks code into their DEV/QA system
 - QA performs function tests and app scans at the same time
 - They return bugs to DEV
 - DEV realizes they are using a bad validation routine or regularly forgetting tokens etc...
 - DEV fixes their libraries to match best security practice

Living in a vacuum



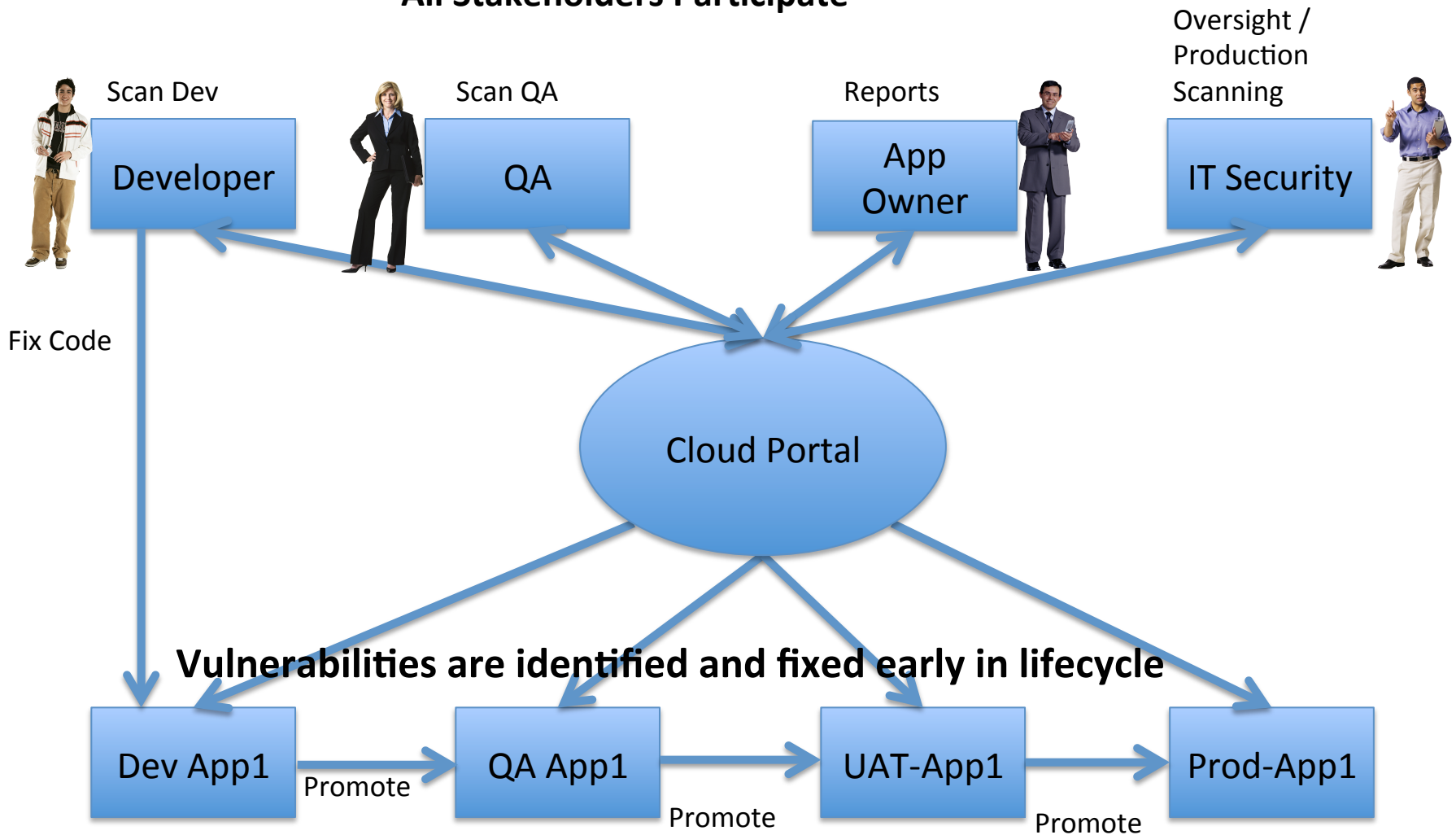
A reality

Automation is an efficiency force multiplier

– Jason Kent

Eliminating IT Security Bottleneck

All Stakeholders Participate



Live Demo



WAS v2

Help

Will Bechtel

Log Out

DashboardWeb ApplicationsScansReportsConfigurationKnowledgeBaseUsers

Dashboard

Thu 19 Apr 2012

26 total scanned web apps

All Vulnerabilities

231

HIGH Severity

10

MED Severity

118

LOW Severity

103

New Scan

Add Web Application

Most Vulnerable Web Applications

Web Application Name	Last Scan Date	Total Vulnerabilities	High	Med	Low	Severity
My First Web Application http://demo6.sea.qualys.com:80/	20 Apr 2012	21	7	6	8	HIGH
Gruyere - Sri Puthucode http://google-gruyere.appspot.com/239244276459/login	09 Apr 2012	16	3	2	11	HIGH
Portnov http://www.portnov.com	11 Nov 2011	134	—	94	40	MED

Your Last Scans

Scan Name	Scan Date	Status	Severity
Web Applicat... My First Web Application	20 Apr 2012	Running	—
Web Applicat... My First Web Application	09 Apr 2012	Finished	HIGH
Relaunch Sch... Gruyere - Sri Puthucode	09 Apr 2012	Finished	HIGH

Your Upcoming Scans

Task Name	Occurs	Next Date
Schedule - Demo - 3am demo.sea.qualys.com - webapp	Daily	20 Apr 2012
Schedule scan Web Appl... Gruyere - Sri Puthucode	Monthly	01 May 2012

Catalog

Total
517
373 New
50 Rogue
92 Approved
0 Ignored
2 In Subscription

Latest Reports

Web Application Report...
20 Apr 2012

Scan report - Online B...
20 Apr 2012



Thank You

jkent@qualys.com

@jkentakula