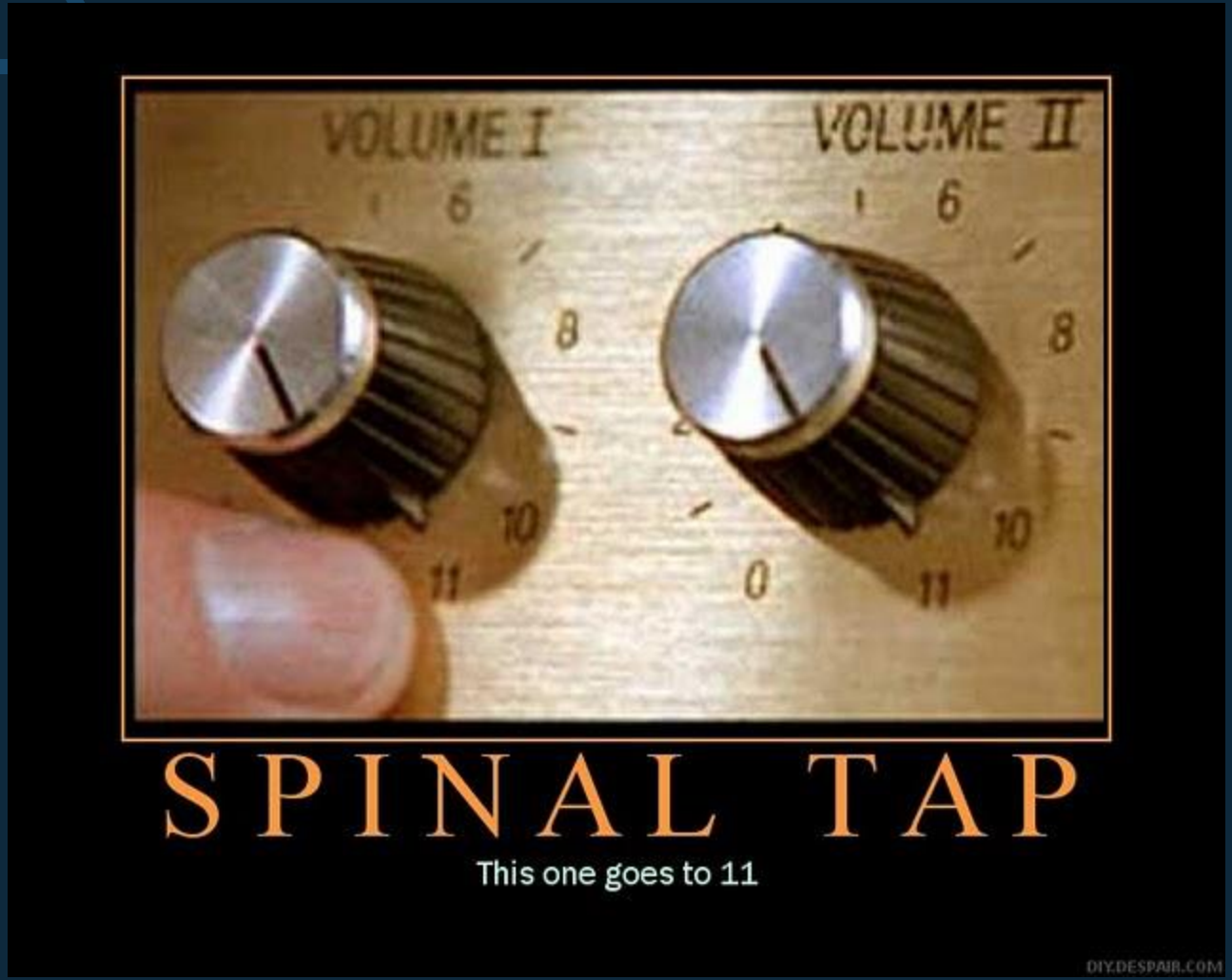
Taking AppSec to 11

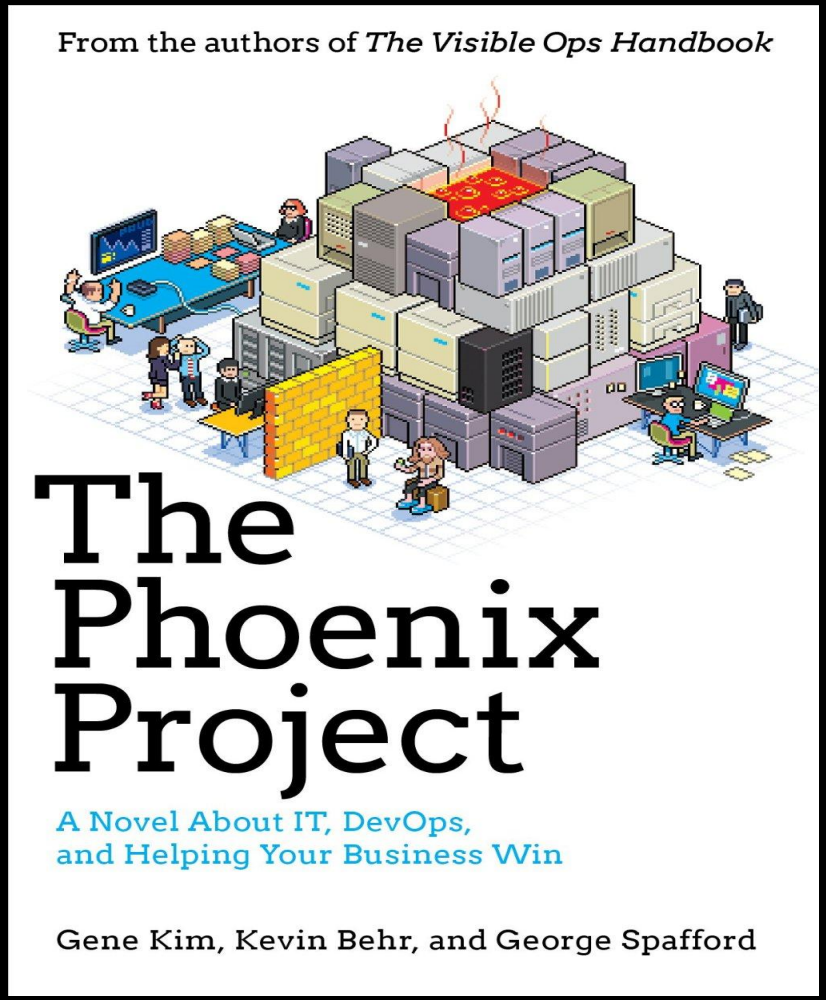
AppSec Pipelines, DevOps, and Making Things Better.

SnowFROC 2016

Matt Tesauro, Infinitiv

Assembly Lines


VOLUME I
VOLUME II
SPINAL TAP
This one goes to 11
DIY.DESPAIR.COM



The Phoenix Project

3 Ways of DevOps

Strategies for Improving Operations

#1 – Workflow

Look at your purpose and those processes which aid it

Timeline

Flow [rate] – the speed work goes through the process

#1 Workflow

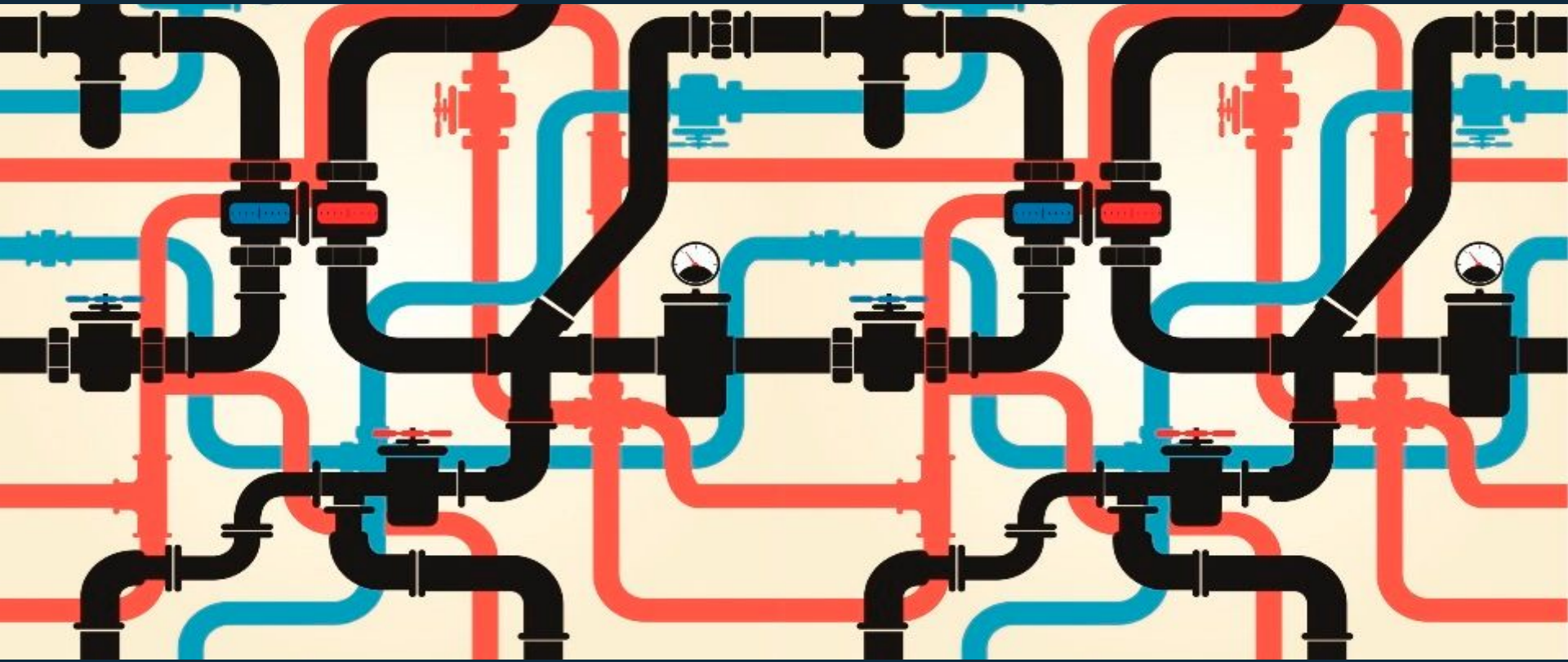
First of the three ways

- Each Step Repeatable
- Never Pass on Defects
- Local optimizations with a global view

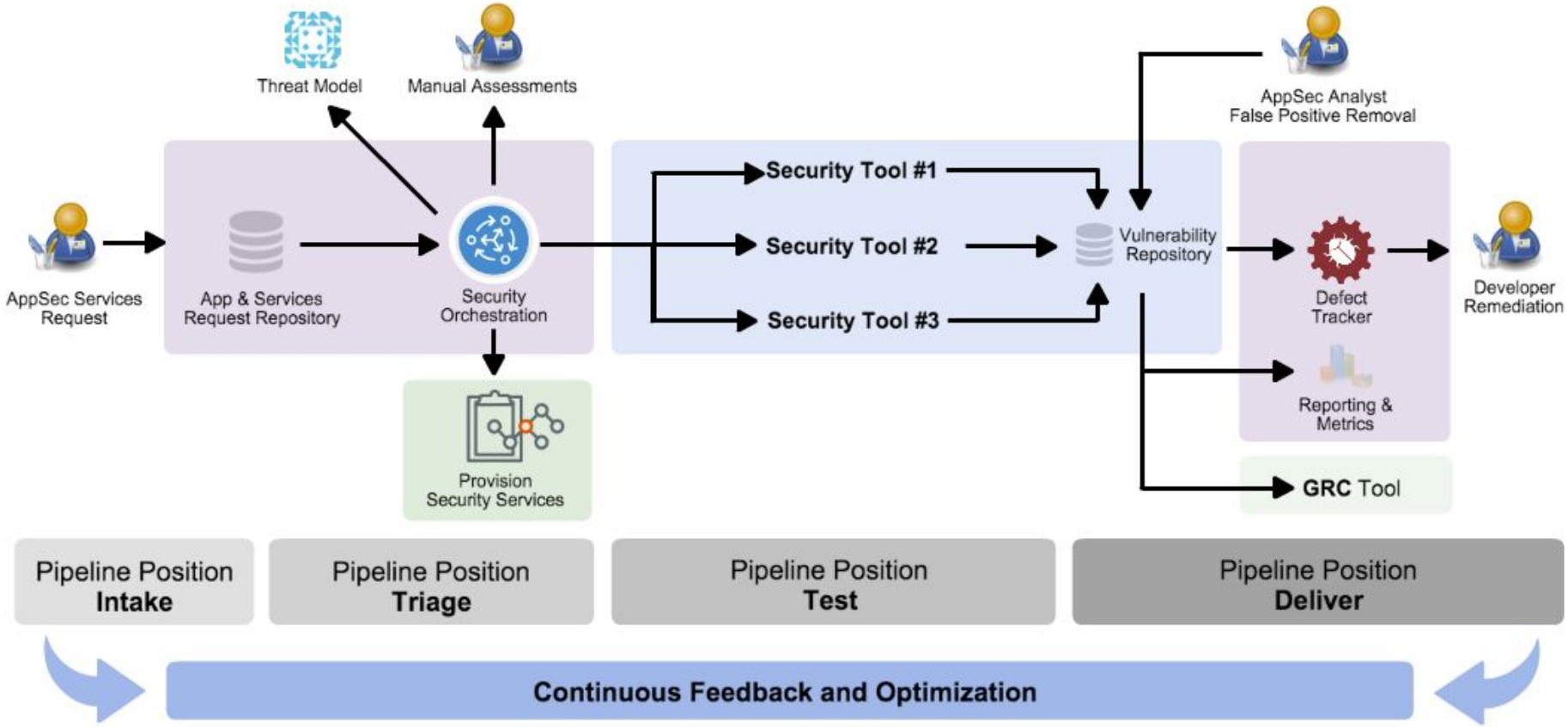
AppSec Pipelines

Figuring out your workflow

AppSec Pipelines



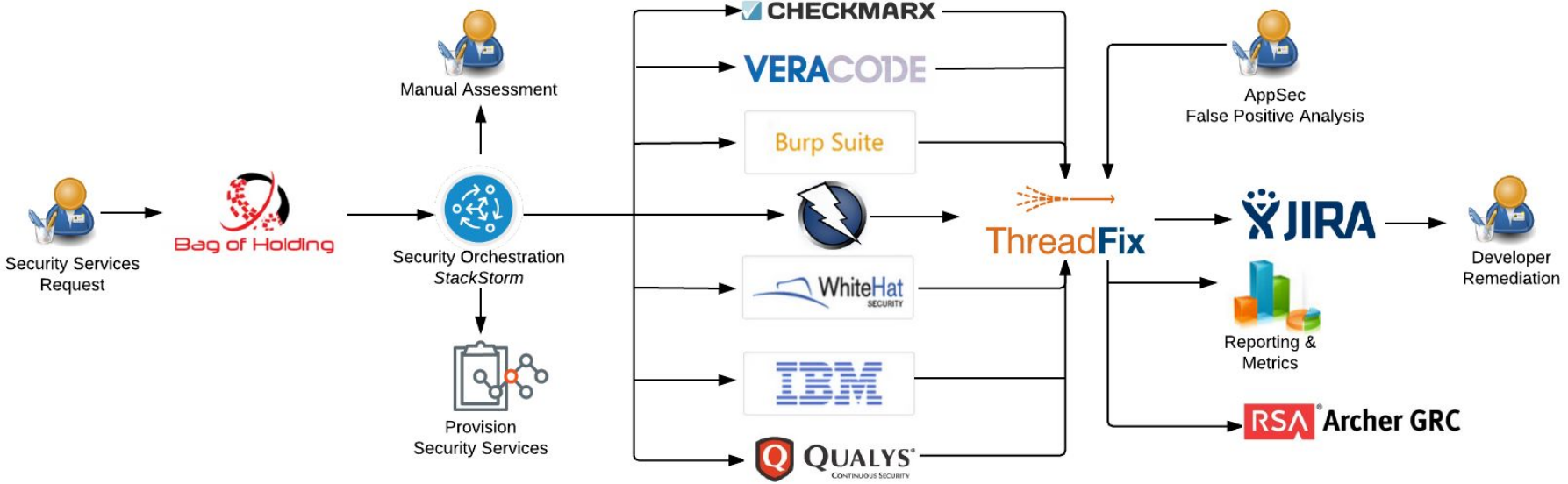
Rugged Devops - AppSec Pipeline Template



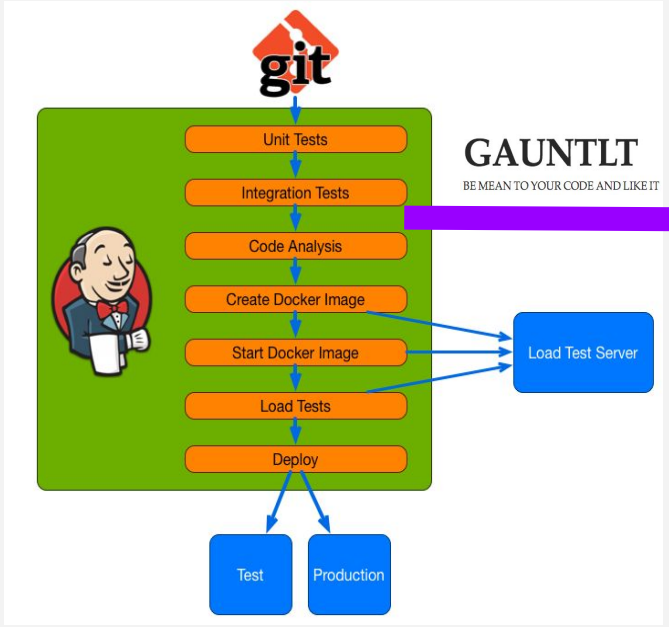
Key Features of AppSec Pipelines

- Designed for iterative improvement
- Provides a reusable path for AppSec activities to follow
- Provides a consistent process for both the team and our constituency
- One way flow with well-defined states
- Relies heavily on automation
- Grow in functionality organically over time
- Gracefully interconnects with the development process

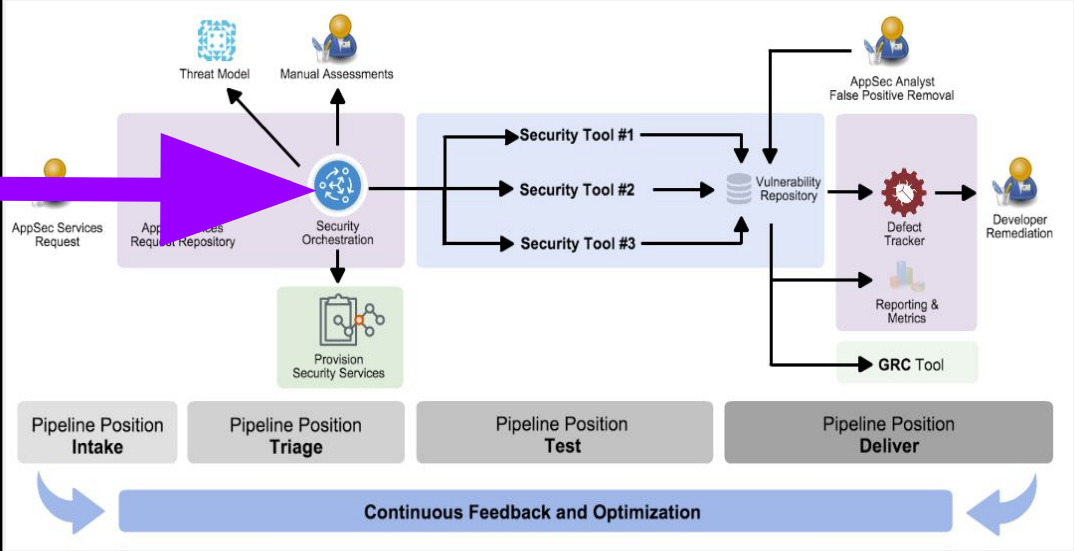
Pearson AppSec Pipeline



Integrating into the DevOps Pipeline



DevOps Pipeline



AppSec Pipeline

Spending time **optimizing** anything **other** than the critical resource is an **illusion**.

W. Edwards Deming

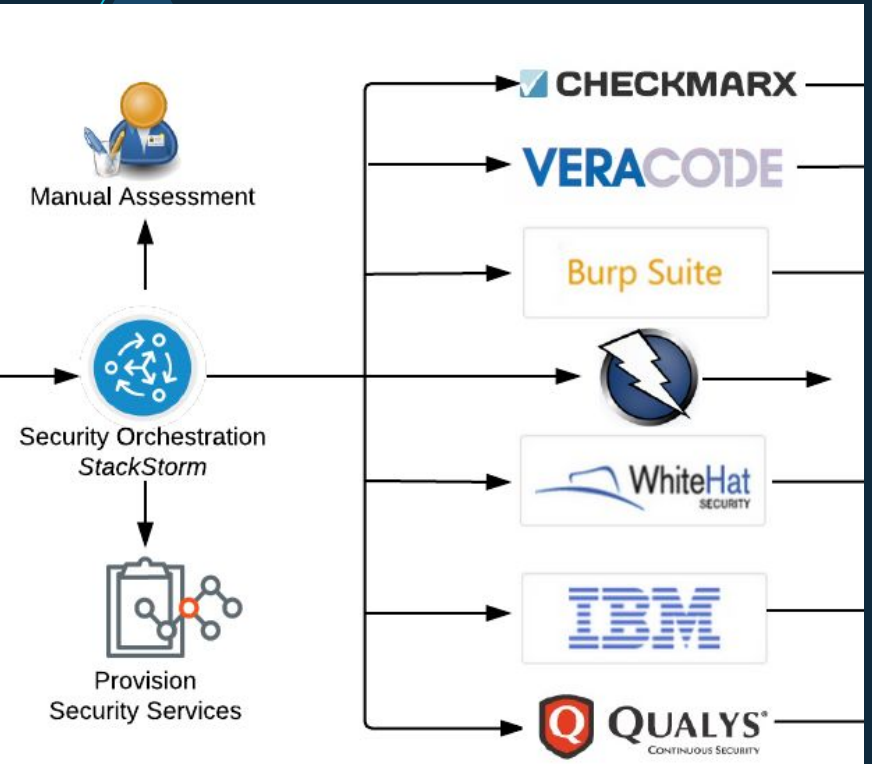
Key Goals of AppSec Pipelines

- **Optimize the critical resource - AppSec personnel**
  - Automate all the things that don't require a human brain
  - Drive up consistency
  - Increase tracking of work status
  - Increase flow through the system
  - Increase visibility and metrics
  - Reduce any dev team friction with application security

Pipeline – Intake

- **“First Impression”**
- **Major categories of Intake**
  - Existing App
  - New App
  - Previously tested App
  - App to re-test findings
- **Key Concepts**
  - Ask for data about Apps only once
  - Have data reviewed when an App returns
  - Adapt data collected based on broad categories of Apps

Pipeline – Testing

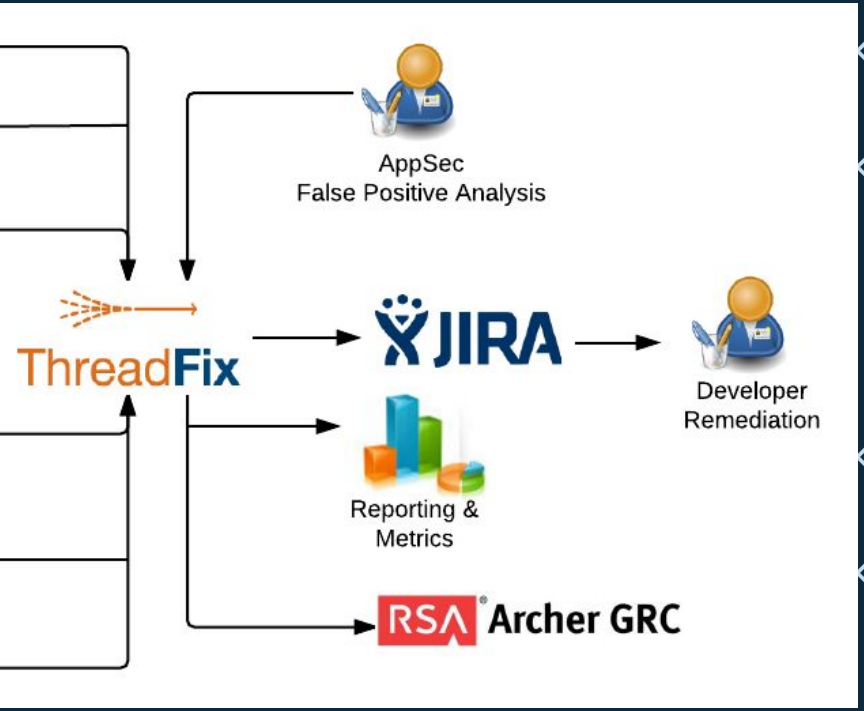


- Inbound request triage
- Ala Carte App Sec
  - Dynamic Testing
  - Static Testing
  - Re-Testing mitigated findings
  - Mix and match based on risk
- Key Concepts
  - Activities can be run in parallel
  - Automation on setup, configuration, data export
- People focus on customization rather than setup

Pipeline – Testing

- Results from your CI/CD could flow into Threadfix from build Pipeline
- Gauntlt runs results could also flow into the AppSec Pipeline
- Choose the tools that make sense for you organization

Pipeline – Deliver



- **Source of truth for all AppSec activities**
- **ThreadFix is used to**
  - Dedup / Consolidate findings
  - Normalize scanner data
  - Generate Metrics
  - Push issues to bug trackers
- **Report and metrics automation**
  - REST + tfclient
- **Source of many touch points with external teams**

Why we like AppSec Pipelines

- Allow us to have visibility into WIP
- Better understand/track/optimize flow of engagements
- Average static test takes …
- Great increase in consistency
- Easier re-allocation of engagements between staff
- Each step has a well defined interface
- Knowing who has what allows for more informed “cost of switching” conversations
- Flexible enough for a range of skills and app maturity

~5x increase

2014	2015
44 assessments	~200 assessments

Changes from 2014 to 2015:

- Created the AppSec Pipeline - initial launch in March 2015
- AppSec team numbers dropped - lost a couple of key people approx 3.5 FTEs
- Two of the AppSec team members went meta for most of 2015

Bag of Holding

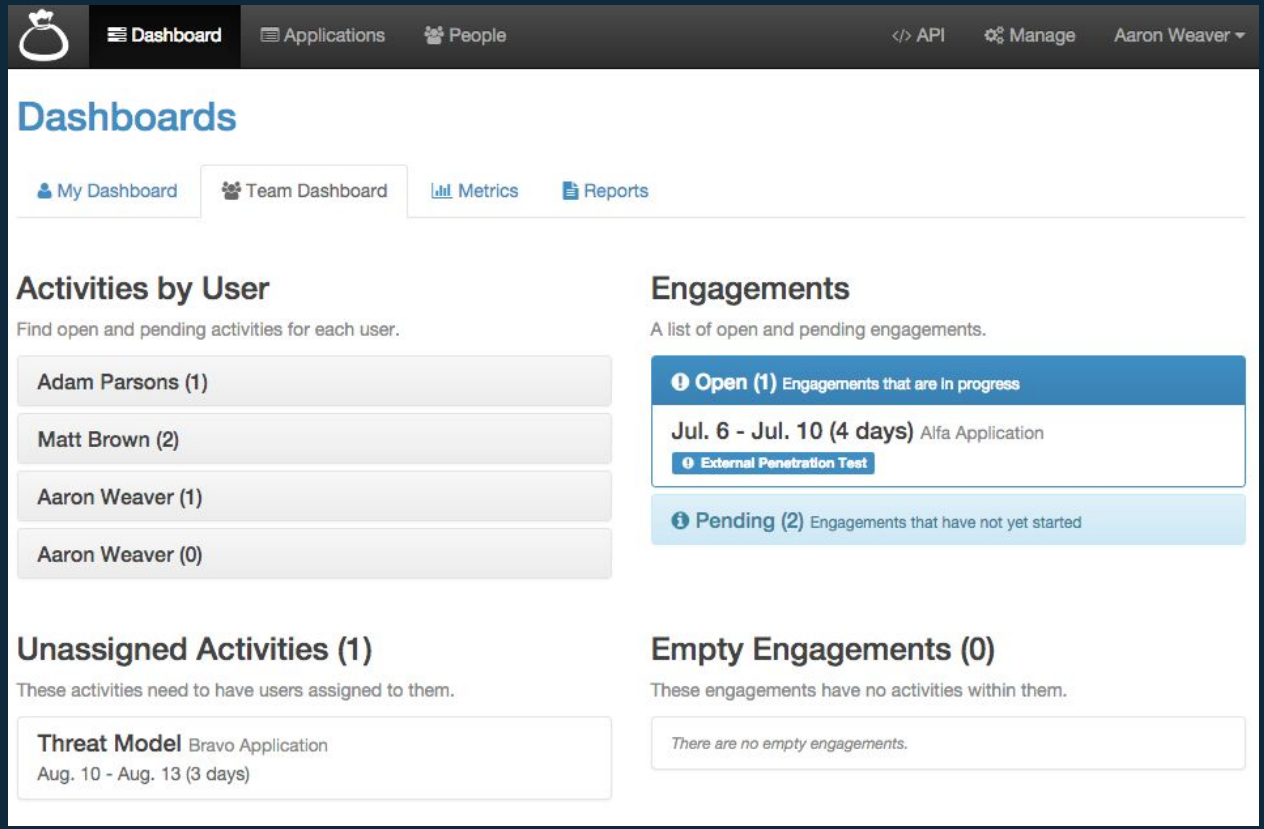
aka BoH

github.com/PearsonEducation/bag-of-holding

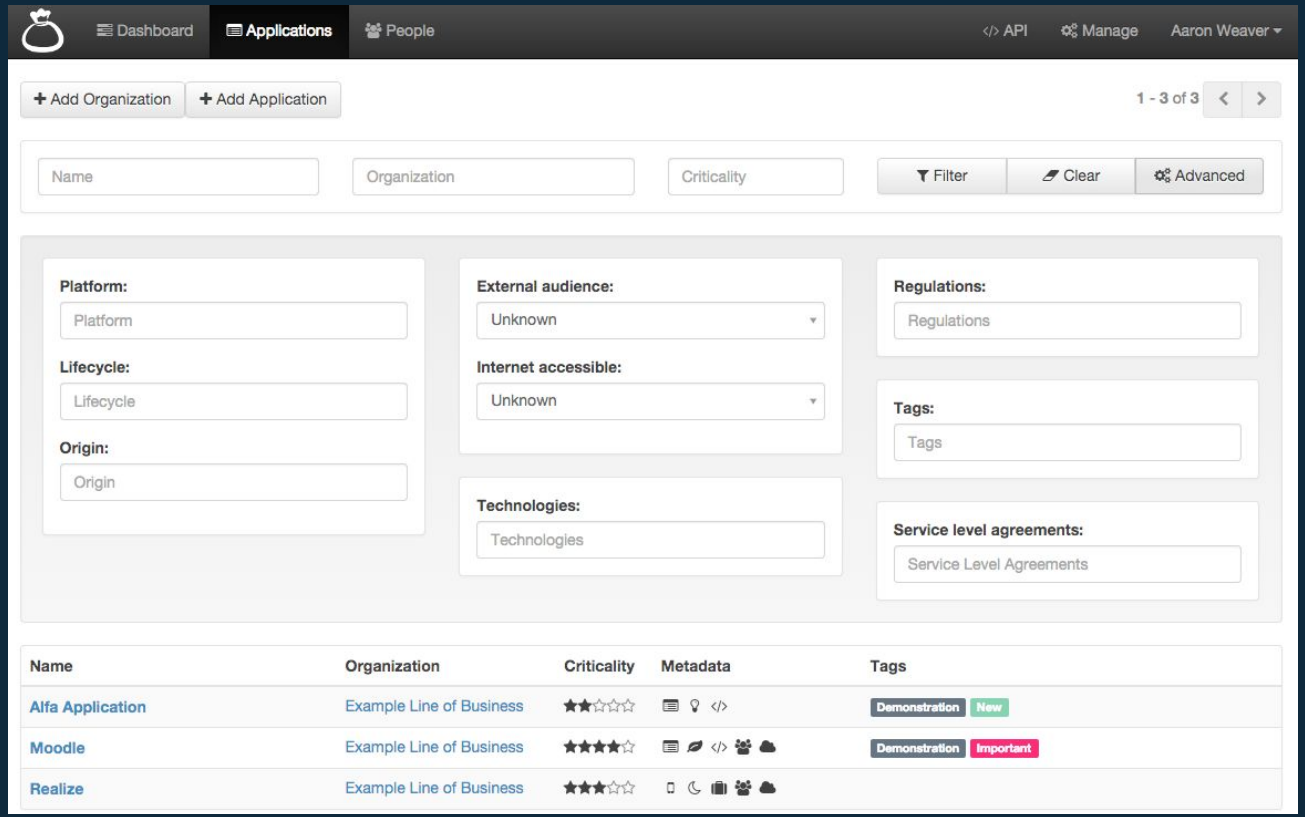
What does BoH do?

- Manages the Application Security Program
- Application Repository
- Engagement Tracking
- Report Repository
- Comments on any application, engagement or activity
- Data Classification and PII data
- Time taken on secure software activities
- Historical knowledge of past assessments
- Credential repository
- Environment details

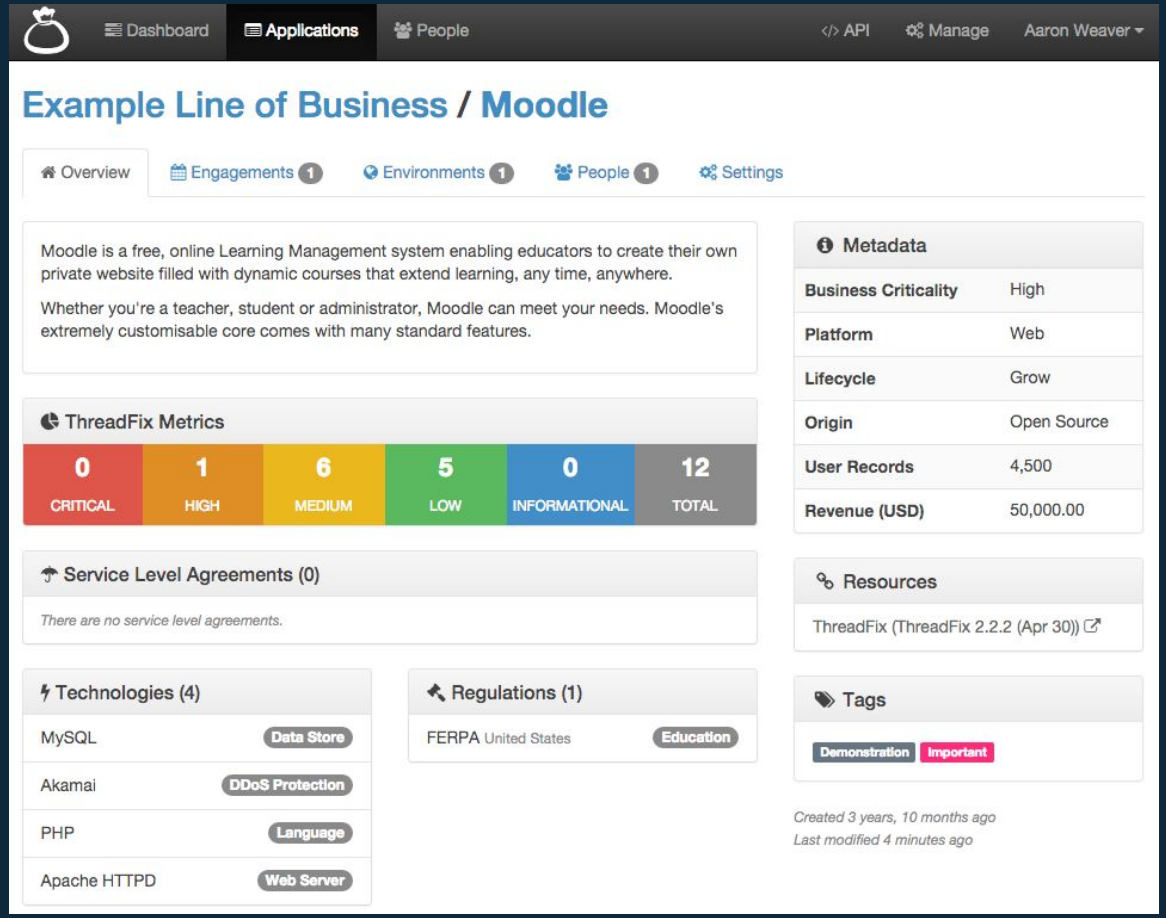
Scheduling of Secure Software Activities



Application Repository



Application Security Profile



Defect Dojo

- DefectDojo is a tool created by the Security Engineering team at Rackspace to track testing efforts.
- Streamlines the testing process by offering features such as templating, report generation, metrics, and baseline self-service tools.
- Though it was designed with security folks in mind, there is nothing keeping QA/QE testers, or any other testers for that matter, from using it productively.
- https://github.com/rackerlabs/django-DefectDojo

DEFECTdojo

Search...

- Dashboard
- Products
- Engagements
- Findings
- Metrics
- Calendar

Dashboard for Greg Anderson

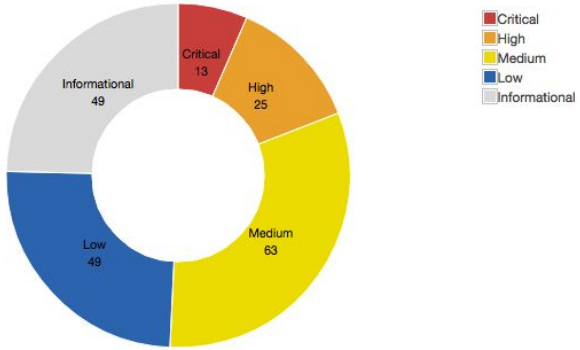
1 Active Engagements — View Details

2 Findings In Last Seven Days — View Details

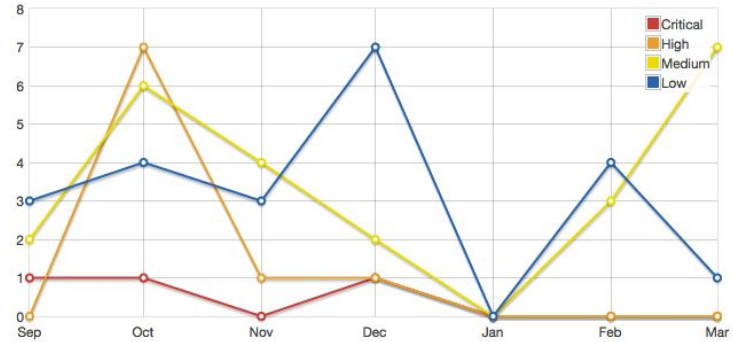
1 Findings Closed In Last Seven Days — View Details

0 Findings Accepted In Last Seven Days — View Details

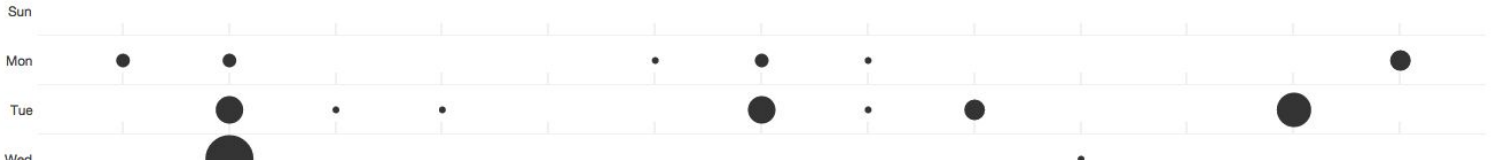
Historical Finding Severity



Reported Finding Severity by Month



Weekly activity, displayed by day, of findings you reported.*



#2 - Improve Feedback

Open yourself to upstream
and downstream information

Matt Tesauro
@matt_tesauro

Security Tool Vendors: If I can do it with the UI, I want to do it with an API.

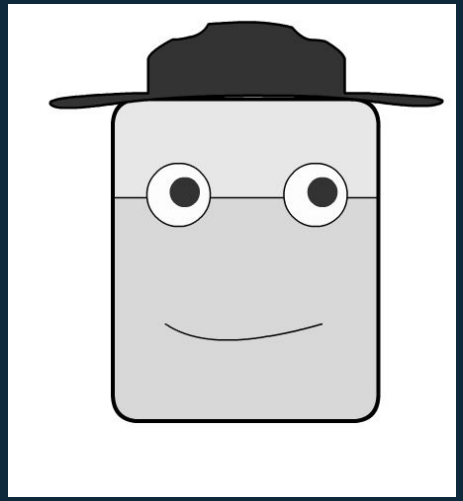
RETWEETS 11 FAVORITES 2

6:43 AM - 14 Apr 2015

AppSec ChatOps

aka Will

Your command line where you have your conversations.



AppSec Help

Aaron Weaver @AppSecBot help 4:27 PM

[BOT] AppSec... Sure thing, AaronWeaver. 4:27 PM

[BOT] AppSec... Here's what I know how to do: 4:27 PM

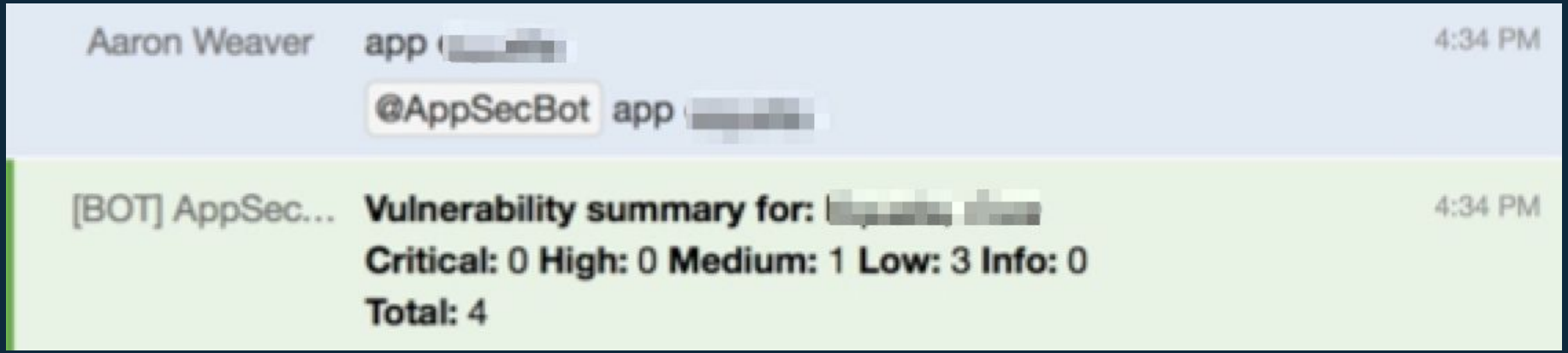
Help:
help: the normal help you're reading.
programmer help: Advanced programmer-y help.

Plugins:
"checkmarx -a appname -r repository: Creates a Checkmarx Job. If the app is new add: -o "Line of Business Example": -a Bag of Holding -o Core -r ssh://git@[redacted]/appsec/bag-of-holding.git
"create tfapp -o "Line of Businesss" -a "Application Name"
Example: create tfapp -o HigherEd -a Equella
Hangout: Get a google plus hangout url
advice ___: Remediation advice for application vulnerabilities and available tools. Example: advice xss or advice help
app ___: Vulnerability stats for an application. Example: app equella
get tfapp ___: Returns the Threadfix application name formatted for Checkmarx, AppScan or scanner integration. Example: get tfapp equella)
list apps: List all applications loaded by application name.
summary: Vulnerability summary by team and total vulnerabilities.

AppSec Advice

Aaron Weaver	@AppSecBot advice xss	4:25 PM
[BOT] AppSec…	**Cross Site Scripting** Output encoding is the primary method for preventing XSS and injection attacks. Input validation helps minimize the introduction of malformed data, but it is a secondary control. For a complete description visit the AppSec Library.	4:25 PM
[BOT] AppSec…	**Other information I know:** • **advice xss** - Information about Cross Site Scripting • **advice sqli** - SQL Injection • **advice cookies** - Using cookies securely • **advice tools** - Security Tools & Services Ping us on hipchat in the 'Application Security' room or visit the AppSec Library.	4:25 PM

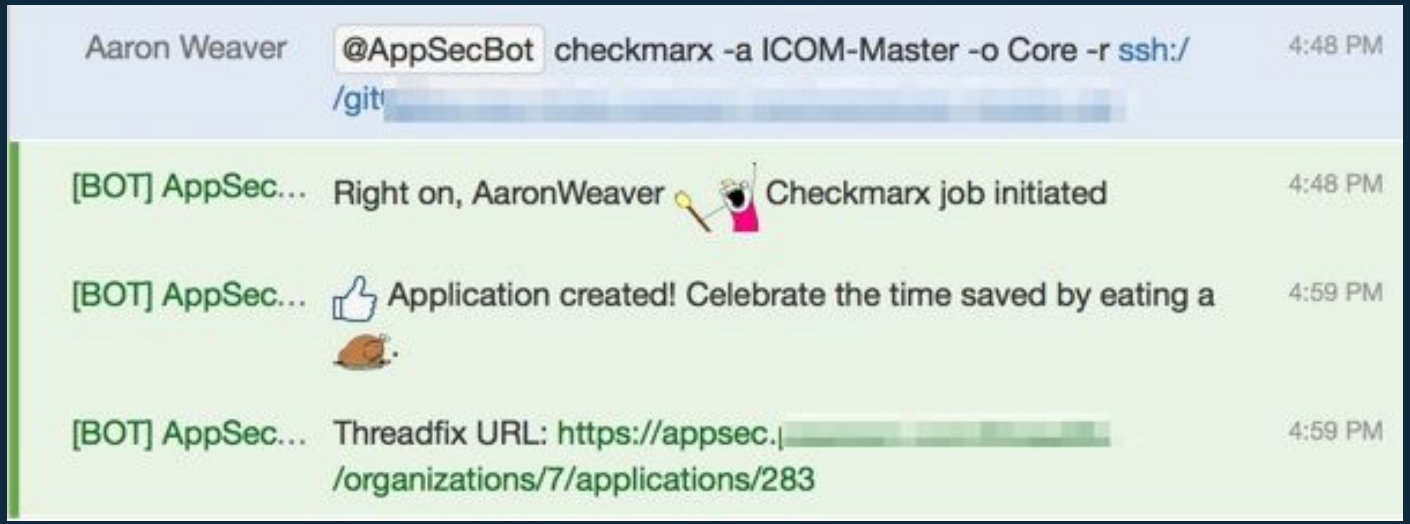
Threadfix Integration



And more:

- Create an Application
- Get Summary Metrics for AppSec Program

BOH/Threadfix/Static Integration



Setup recurring static analysis in about 1 minute!

#3 - Continual Experimentation & Learning

Create a culture of innovation and experimentation

Matt Tesauro
@matt_tesauro

Failures only serve to limit the scope of what must be tried to succeed.

11:22 PM - 11 Jun 2015

"I fear not the man
who has practiced
ten thousand kicks
once,
but I fear the man
who has practiced
one kick ten thousand
times."

OWASP AppSec Pipeline

The OWASP AppSec Pipeline Project

The OWASP AppSec Pipeline Project is the place to find the information you need to increase the speed and automation of your AppSec program. Using the documentation and references of this project will allow you to setup your own AppSec Pipeline.

Description

The AppSec pipeline project is a place to gather together information, techniques and tools to create your own AppSec Pipeline. AppSec Pipelines take the principals of

What is OWASP Security Principles Project?

The AppSec pipeline project is a place to gather together information, techniques and tools to create your own AppSec Pipeline.

Presentation

Aaron Weaver - AppSec EU 2015
Building An AppSec Pipeline
Matt Tesauro - AppSec EU 2015
Taking DevOps Practices Into Your AppSec Life

Project Leaders

Quick Download

Bag of Holding

News and Events

Catch our next presentation at AppSec US 2015

In Print

Building an AppSec Pipeline
Taking DevOps practices into your AppSec Life

Classifications

Dev & AppSec Tool Integration

klocwork
a Rogue Wave Company

FORTIFY

CONTRAST

CHECKMARX

VERACODE

CONTRAST

CHECKMARX

VERACODE

Gitrob

CHECKMARX

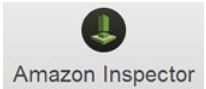
RAPTOR

OWASP ZAP
Proxy

GAUNTLT
BE MEAN TO YOUR CODE AND LIKE IT

CHECKMARX

VERACODE



Chef Audit Mode

OWASP ZAP
Proxy

Code | Manage | Store | Build | Deploy

*Not a comprehensive list. The OWASP DevOps AppSec Pipeline will have a complete listing.

Demo Time

A quick bit of show and tell...

Key Take Aways

- **Automate, automate, automate**
  - Look for “paper cuts” and fix those first
- **Finding workflow – your AppSec Pipeline**
  - Figure this out and standardize / optimize
- **Create systems which can grow organically**
  - App is never done, it’s just created to easily be added to over time
  - e.g. Finding blocks become templates for next report
- **Learn to talk “dev”**

Thanks!

Matt Tesauro

@matt_tesauro

matt.tesauro@infinitiv.io
matt.tesauro@owasp.org

/in/matttesauro

github.com/mtesauro

Resources

Exercises left to the student

Orchestration

- Integrate Security Tools and Workflow

Example:

- Generic API for dynamic scanning
  - URL
  - Credentials
  - Profile
  - Call any Dynamic Scanner:
    - OWASP ZAP
    - BurpSuite
    - AppScan

Gauntlt

- Open source, MIT License
- Gauntlt comes with pre-canned steps that hook security testing tools
- Gauntlt does not install tools
- Gauntlt wants to be part of the CI/CD pipeline
- Be a good citizen of exit status and stdout/stderr

Tiaga

- **Project Management Software**
  - Focused on usability and speed
  - Kanban / Scrum
  - Backlog
  - Tasks
  - Sprints
  - Issues
  - Wiki
- **Open Source – Python / Django app**
  - Entire functionality is driven by a REST API !!
  - https://taiga.io/

TAIGA [BETA]

SEARCH

ACKLOG

ANBAN

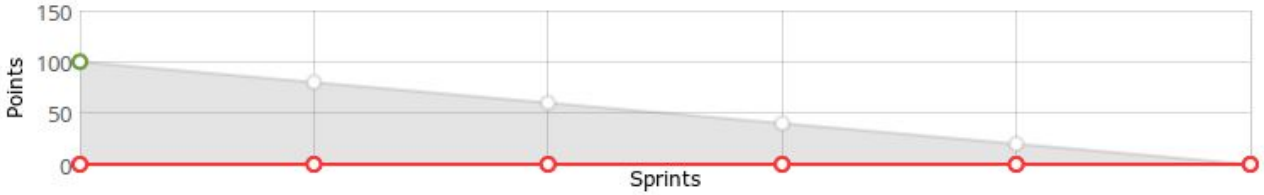
ISSUES

WIKI

TEAM

WTE + FPM BACKLOG

0% 100 project points 0 defined points 0 closed points 0 points / sprint

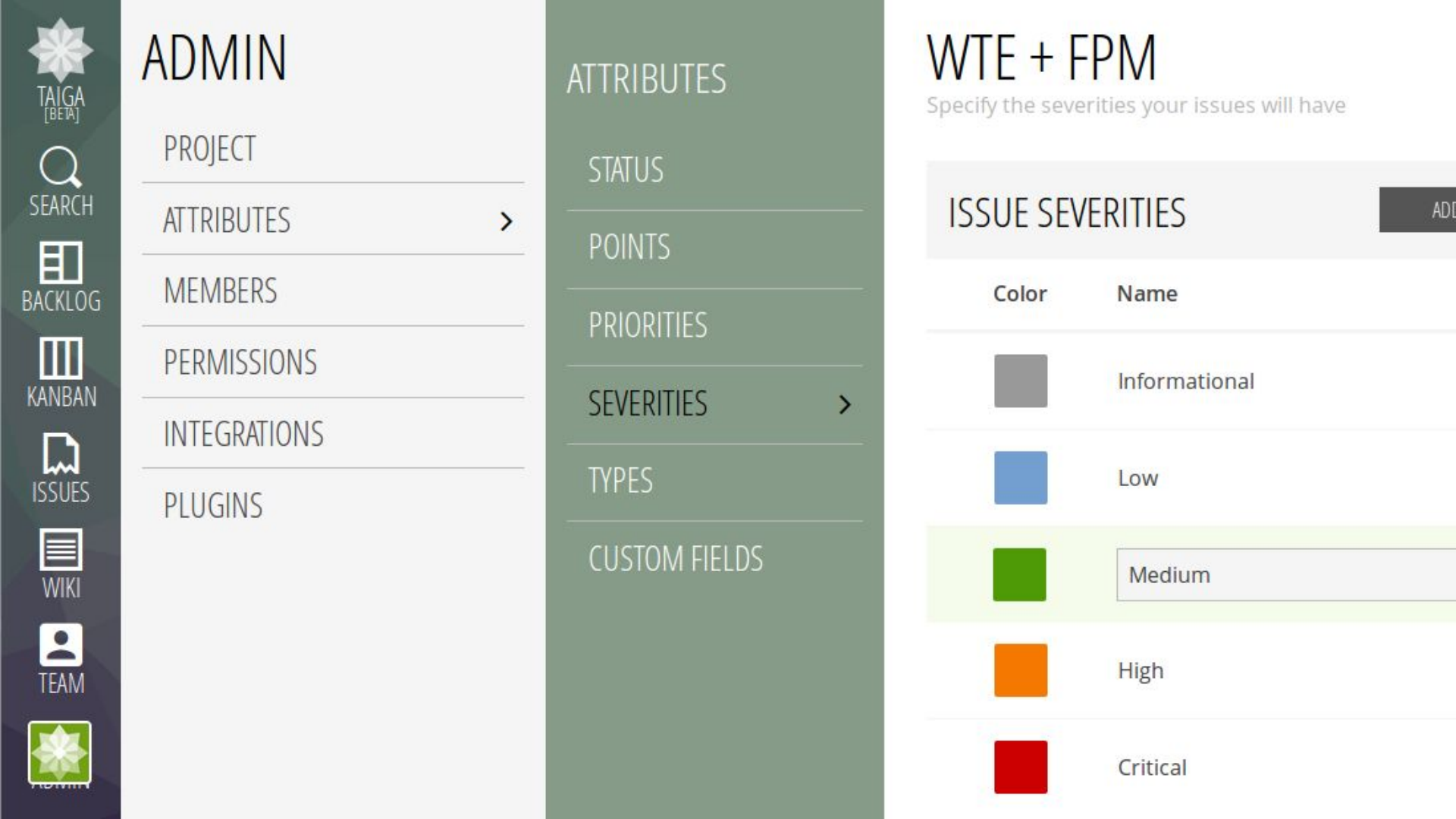


SHOW FILTERS SHOW TAGS + ADD A NEW USER STORY

User Stories	Status	Points
#2 Conduct an manual assessment of the Blarg REST API	New	?

SPRINTS

5 sprints + NEW SPRINT


TAIGA [BETA]
SEARCH
BACKLOG
KANBAN
ISSUES
WIKI
TEAM
ADMIN
PROJECT
ATTRIBUTES
MEMBERS
PERMISSIONS
INTEGRATIONS
PLUGINS
ATTRIBUTES
STATUS
POINTS
PRIORITIES
SEVERITIES
TYPES
CUSTOM FIELDS
WTE + FPM
Specify the severities your issues will have
ISSUE SEVERITIES
ADD
Color
Name
Informational
Low
Medium
High
Critical

Defect Dojo

- DefectDojo is a tool created by the Security Engineering team at Rackspace to track testing efforts.
- Streamlines the testing process by offering features such as templating, report generation, metrics, and baseline self-service tools.
- Though it was designed with security folks in mind, there is nothing keeping QA/QE testers, or any other testers for that matter, from using it productively.
- https://github.com/rackerlabs/django-DefectDojo

DEFECTdojo

Search...

- Dashboard
- Products
- Engagements
- Findings
- Metrics
- Calendar

Dashboard for Greg Anderson

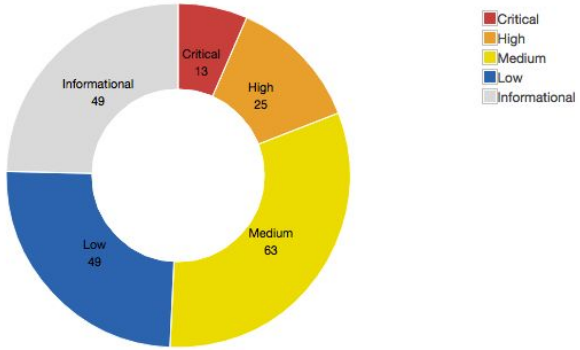
1 Active Engagements — View Details

2 Findings In Last Seven Days — View Details

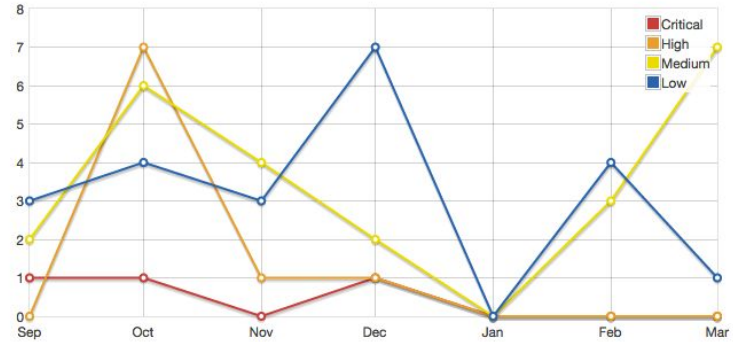
1 Findings Closed In Last Seven Days — View Details

0 Findings Accepted In Last Seven Days — View Details

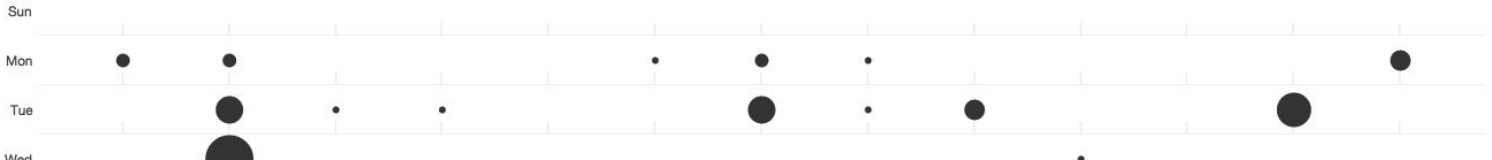
Historical Finding Severity



Reported Finding Severity by Month



Weekly activity, displayed by day, of findings you reported.*



Experimentation

Kick things up a notch

Findings directly to bug trackers

- PDFs are great, bugs are better
- Security issues are now part of the normal work flow
- ThreadFix is nice for pumping issues into defect trackers - http://code.google.com/p/threadfix/

For the reticent: nag, nag, nag

- Attach a SLA to each severity level for findings
- Walk up the Org chart as things get older
- Bonus points for dashboards and defect tracker APIs
- Get management sold first

Agent – one mole to rule them all

- Add an agent to the standard deploy
- Add a dashboard to visualize state of infrastructure
- Roll your own or find a vendor

Mozilla MIG

CloudPassage

Turn Vuln Scanning on its Head

- Add value for your Ops teams
- Roll your own or find a vendor
- Reverse the scan then report standard

Related Presentations

AppSec EU 2015 – Ops Track Keynote

http://www.slideshare.net/mtesauro/mtesauro-keynote-appseceu

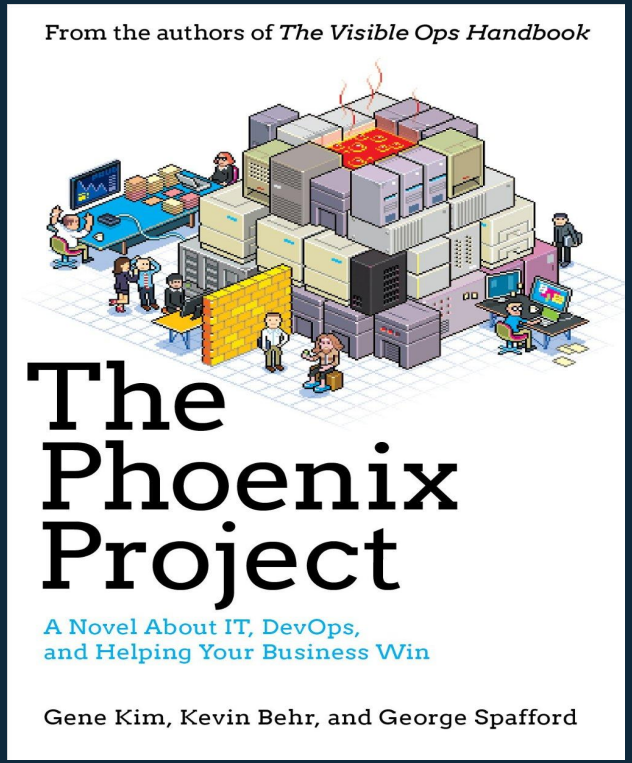
https://www.youtube.com/watch?v=tDnyFitE0y4

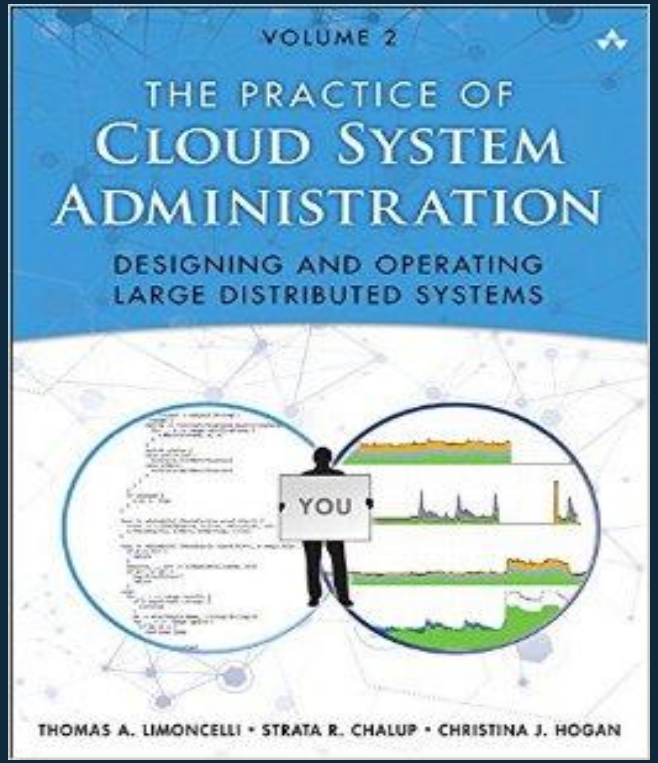
AppSec EU 2015 – Building an AppSec Pipeline

http://www.slideshare.net/weaveraaaron/building-an-appsec-pipeline-keeping-your-program-and-your-life-sane

https://www.youtube.com/watch?v=1CDSOSI4DQU

Books to Read





#1 Workflow

Each Step Repeatable

- Remove all haphazard and ad hoc work from the process
- Scripting languages are your friends
- Config Mgmt – Puppet, Chef, Salt, Ansible, CFEngine
- Make sure what you do can be done on 1 server or 10,000 servers

#1 Workflow

Never Pass on Defects

- Test early and often
- Increase the rigor of testing as you work left to right
- When a failure occurs end that flow and start a new one after corrections
- The further right you are, the more expensive failure is so concentrate your early work on left side (intake)
- In AppSec, defects are false positives

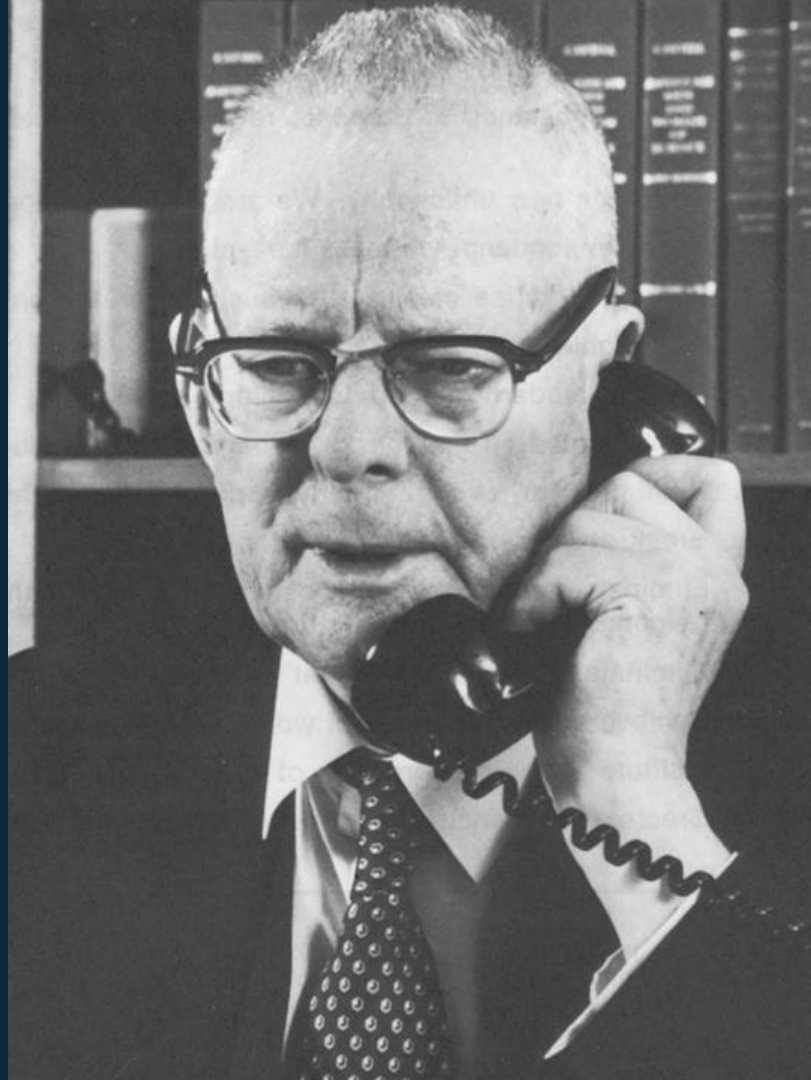
#1 Workflow

Local optimizations with a global view

- **Ensure no single-step optimizations degrade the overall performance of the workflow**
- **Find the bottleneck in your workflow and start there**
  - Upstream changes will just back things up
  - Downstream changes won't manifest since input is limited
- **Each new optimization creates a new bottleneck**
  - Iterate on this!

Spending time **optimizing** anything **other** than the critical resource is an **illusion**.

W. Edwards Deming



Japan's post-war miracle

Image References

Henry Ford in a field:

http://henryfordgiantdifferenceaward.weebly.com/works-cited.html

Assembly Lines:

http://www.pictofcar.website/henry-ford-assembly-line-diagram/

http://www.fasttrackteaching.com/burns/Unit_3_Industry/U3_Ford.html

http://en.wikipedia.org/wiki/Assembly_line

http://actionspeaksradio.org/tag/henry-ford/

http://blogs.internetautoguide.com/6582595/manufacturing/henry-ford-didnt-invent-the-assembly-line-ransom-e-olds-did/index.html

W. Edward Deming

http://www.motortrend.com/features/consumer/1005_30_who_count/photo_04.html

Japan's Post War Miracle

http://www2.fultonschools.org/teacher/robertsw1/thursday.nov1.htm

http://dylewski.com.pl/menu-boczne/iluzja-pieniadza/usa-vs-japonia/

http://en.wikipedia.org/wiki/Japanese_post-war_economic_miracle

Image References

Thomas Edison:

http://www.allposters.com/-sp/Thomas-Edison-Posters_i1859026_.htm

Food line:

http://www.slideshare.net/weaveraaaron/building-an-appsec-pipeline-keeping-your-program-and-your-life-sane

Phoenix Project Book Cover:

https://puppetlabs.com/blog/why-we-need-devops-now

Goes to 11:

https://arturogalletti.files.wordpress.com/2010/12/spinaltap.jpg

About this template

What's this?

This is a free presentation template for Google Slides designed by SlidesCarnival.

We believe that good design serves to better communicate ideas, so we create free quality presentation templates for you to focus on the content.

Enjoy them at will and share with us your results at:

twitter.com/SlidesCarnival

facebook.com/slidescarnival

How can I use it?

Open this document in Google Slides (if you are at slidescarnival.com use the button below this presentation)

You have to be signed in to your Google account

- **Edit in Google Slides**
  Go to the **File** menu and select **Make a copy**. You will get a copy of this document on your Google Drive and will be able to edit, add or delete slides.
- **Edit in Microsoft PowerPoint®**
  Go to the **File** menu and select **Download as Microsoft PowerPoint**. You will get a .pptx file that you can edit in PowerPoint. Remember to download and install the fonts used in this presentation (you'll find the links to the font files needed in the Presentation design slide)