AppSec Pipeline

Application Security in an Agile Development, DevOps and Continuous Integration/Delivery/Change world.

Doug Morato
Sr. Manager
PwC NIS|App-Sec

OWASP Tampa Meeting - 02/19/2016

Who am I again?

Professionally:
Sr. Manager - AppSec team @ PwC

Prior roles:
Sr. Software Sec Consultant @ HP
Sr. Penetration Tester @ Mastercard
App Sec Specialist @ Disney
Independent AppSec Consultant

Certs:
CSSLP, CISSP, GPEN, GCIA, GCFA, GCIH, GSEC, CCSK, ECSA, CEH Certified

Personally:
Born in Brazil (Yes, I speak Portuguese !)
Happily married
Father of the most awesome 6 year old ever
Live in South Florida (Boca Raton)
Core contributor to the OWASP WebGoat Project

Hobbies:
InfoSec, Travel and Beers

- **Disclaimer**: Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are mine individually and, unless expressly stated to the contrary, are not the opinion or position of my Employer, its staff, or its member. PwC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Acknowledgments

This presentation is an aggregation of multiple presentations and ideas I have seen presented, and customized to our own necessity using my own judgment and my team's feedback,

There is awesome content out there from people who have been doing and are doing AppSec pipelines, which some of it's concepts and ideas I mention here.

Thanks and props to the following:

- Matt Tesauro:
    - http://www.slideshare.net/mtesauro/
- Matt Konda:
    - https://speakerdeck.com/mkonda
- Aaron Weaver
- Josh Corman

Appsec Pipeline

What’s that all about?

Remember Henry Ford ?

Founder of Ford Motor company and sponsor of the development of the **assembly line**

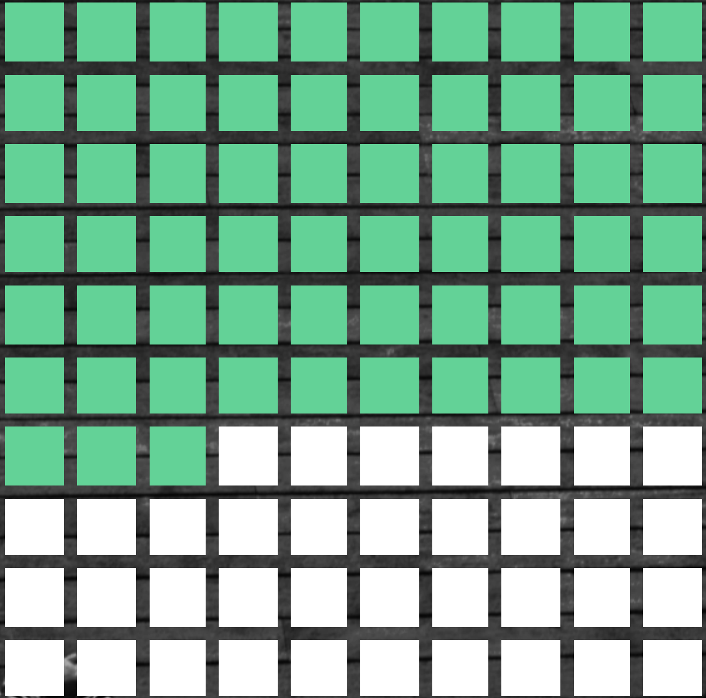
Why AppSec Pipeline?

Key drivers for us:

10-Fold increase in # of apps

Differences in SDLC maturity across territories.

Some territories and Dev teams require Agile dev and rapid delivery.



Appsec Pipeline

A quick intro to "The Phoenix Project Book" concepts:
The 3 Ways of DevOps

1. **Workflow:** Look at your purpose and those processes which aid it
2. **Improve on feedback:** Open yourself to upstream and downstream information
3. **Continual Experimentation & Learning: ADAPT.** Create a cultoe of innovation and experimentation

How can we securely support the new model of ever changing, agile initiatives, continuous delivery and DevOps?

Automation

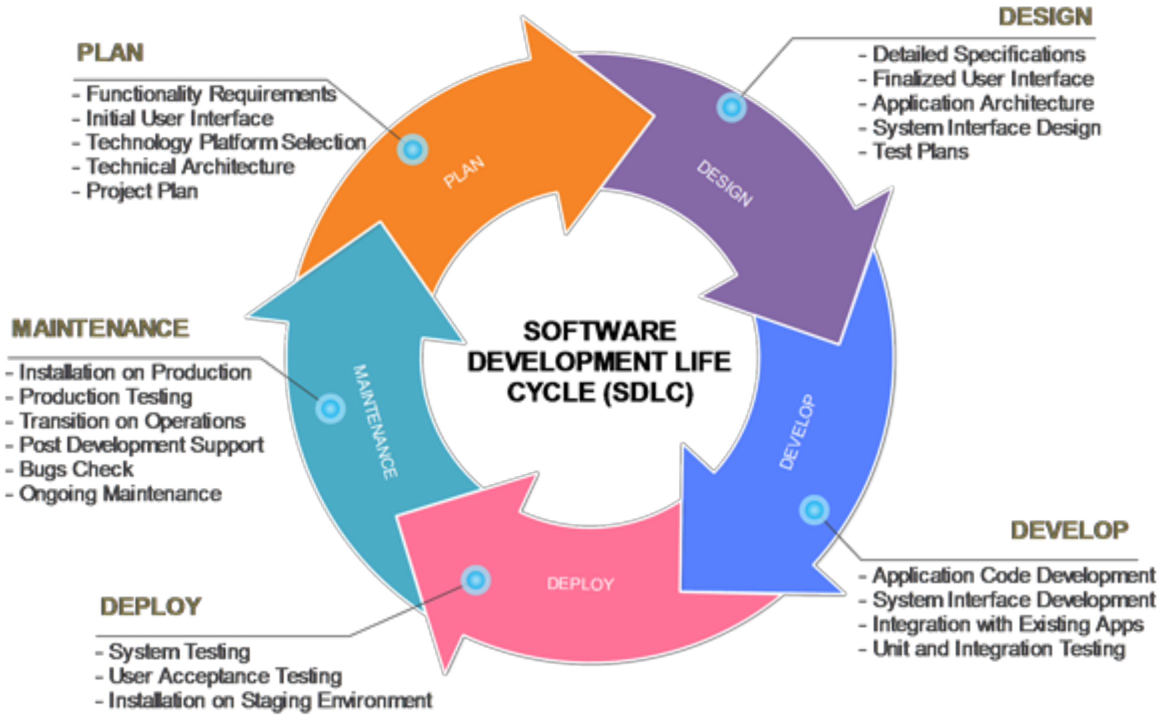
Consistent and Repeatable

Human capital is the critical resource, but also the most expensive, even when using offshore resources.

Computational resources are cheap.

Automate time-consuming tasks where/when possible.

AppSec in the SDLC



SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC)

PLAN

- Functionality Requirements
- Initial User Interface
- Technology Platform Selection
- Technical Architecture
- Project Plan

DESIGN

- Detailed Specifications
- Finalized User Interface
- Application Architecture
- System Interface Design
- Test Plans

DEVELOP

- Application Code Development
- System Interface Development
- Integration with Existing Apps
- Unit and Integration Testing

DEPLOY

- System Testing
- User Acceptance Testing
- Installation on Staging Environment

MAINTENANCE

- Installation on Production
- Production Testing
- Transition on Operations
- Post Development Support
- Bugs Check
- Ongoing Maintenance

AppSec Pipeline. How it works:

Standard Build

AppSec Tasks

Release or Act Upon

Standard Dev Build

Project goes through standard dev and build process, committing code changes as they go through sprints/cycles.

Scheduled or triggered builds upon code push.

AppSec Pipeline Tasks

Perform AppSec tasks if standard build successful:

- Static Code Analysis (HP Fortify / FOD)
- Dynamic Scans (HP WebInspect, OWASP ZAP...)

Approve artifact or Act

Approve inbound artifact into "blessed" artifact repository if "all good"
OR
Trigger alternate workflow, which can be manual review or reassign to AppDev team

The Rugged Manifesto

www.ruggedsoftware.org

I am rugged and, more importantly, my code is rugged.
I recognize that software has become a foundation of our modern world.
I recognize the awesome responsibility that comes with this foundational role.
I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for **longer than it was ever intended.**
I **recognize that my code will be attacked by talented and persistent adversaries** who threaten our physical, economic and national security.

I recognize these things – and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.
I am rugged because I assure my code will support its mission.
I am rugged because my code can face these challenges and persist in spite of them.
I am rugged, not because it is easy, but because it **is necessary** and **I am up for the challenge.**

Technology Stack

Products and Services

Proposed Tools and Vendor Solutions:

Svc Delivery

Engagement Tracking

- JIRA
- JIRA Service Desk
- Bag of Holding*

Documentation

- Confluence

Build

Build Server

- Bamboo, Jenkins or TFS

Deployment

- Puppet, Chef or VSRM

Code Repositories

- GIT/GitHub, TFS, SVN

SAST

Source-Code

- HP Fortify
- HP FoD

Binary/COTS

- Veracode

DAST

Tools

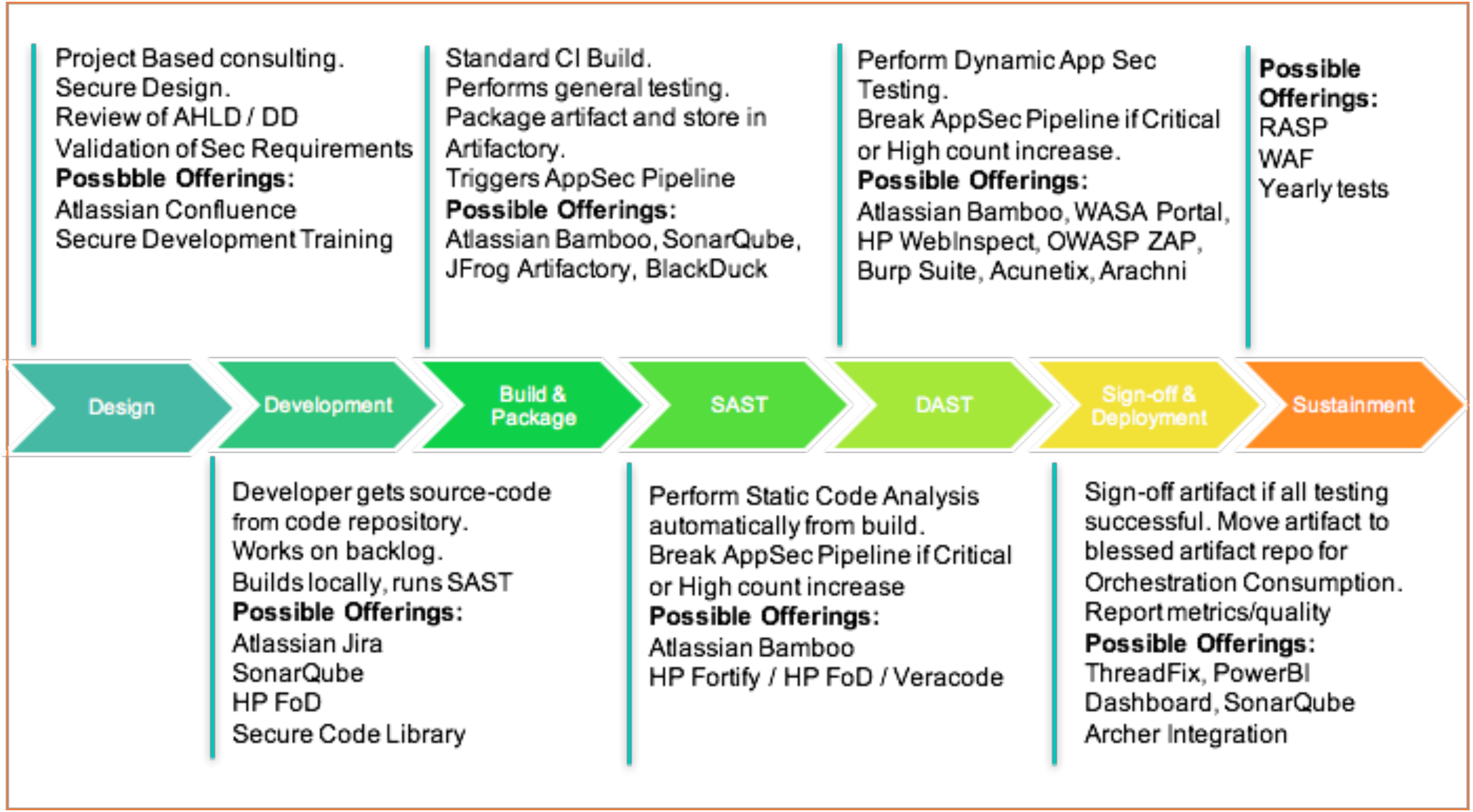
- HP WebInspect
- Acunetix
- OWASP ZAP
- Arachni
- BURP Suite
- Core Impact

Reporting

Tools

- Custom Portal
- Kenna/RiskIO
- SonarQube
- Archer
- Threadfix*

* Or similar



Project Based consulting.
Secure Design.
Review of AHLD / DD
Validation of Sec Requirements
Possbble Offerings:
Atlassian Confluence
Secure Development Training

Developer gets source-code from code repository.
Works on backlog.
Builds locally, runs SAST
Possible Offerings:
Atlassian Jira
SonarQube
HP FoD
Secure Code Library

Standard CI Build.
Performs general testing.
Package artifact and store in Artifactory.
Triggers AppSec Pipeline
Possible Offerings:
Atlassian Bamboo, SonarQube, JFrog Artifactory, BlackDuck

Perform Static Code Analysis automatically from build.
Break AppSec Pipeline if Critical or High count increase
Possible Offerings:
Atlassian Bamboo
HP Fortify / HP FoD / Veracode

Perform Dynamic App Sec Testing.
Break AppSec Pipeline if Critical or High count increase.
Possible Offerings:
Atlassian Bamboo, WASA Portal, HP WebInspect, OWASP ZAP, Burp Suite, Acunetix, Arachni

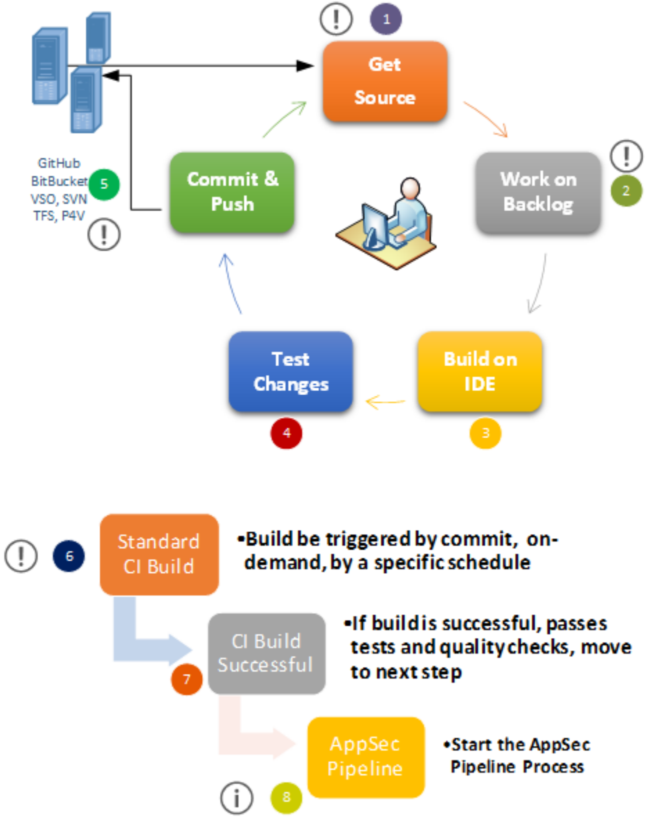
Sign-off artifact if all testing successful. Move artifact to blessed artifact repo for Orchestration Consumption.
Report metrics/quality
Possible Offerings:
ThreadFix, PowerBI Dashboard, SonarQube
Archer Integration

Possible Offerings:
RASP
WAF
Yearly tests

Development Cycles

The proposed workflow demonstrates how the tools and the possible service offerings integrate within the development lifecycle, whether the team is using standard (waterfall) or agile (scrum) methodology

Develoment / Sprint Cycles



GitHub
BitBucket
VSO, SVN
TFS, P4V
1
Get Source
2
Work on Backlog
3
Build on IDE
4
Test Changes
5
Commit & Push
6
Standard CI Build
•Build be triggered by commit, on-demand, by a specific schedule
7
CI Build Successful
•If build is successful, passes tests and quality checks, move to next step
8
AppSec Pipeline
•Start the AppSec Pipeline Process

1 **Service Offering: Source Code Repo (GitHub / BitBucket)**
Developer retrieves Source Code

2 **Service Offering: Atlassian Jira Ticketing system**
Developer works on an item from Backlog, makes code change

3 Developer build project in local IDE

4 Developer tests code changes

5 **Service Offering: Source Code Repo (GitHub / BitBucket)**
Developers commits and push code changes to repository

6 **Service Offering: Atlassian Bamboo Build Server**
CI build is triggered by commit, schedule or on-demand

7 If CI build successful, continue with post-build actions

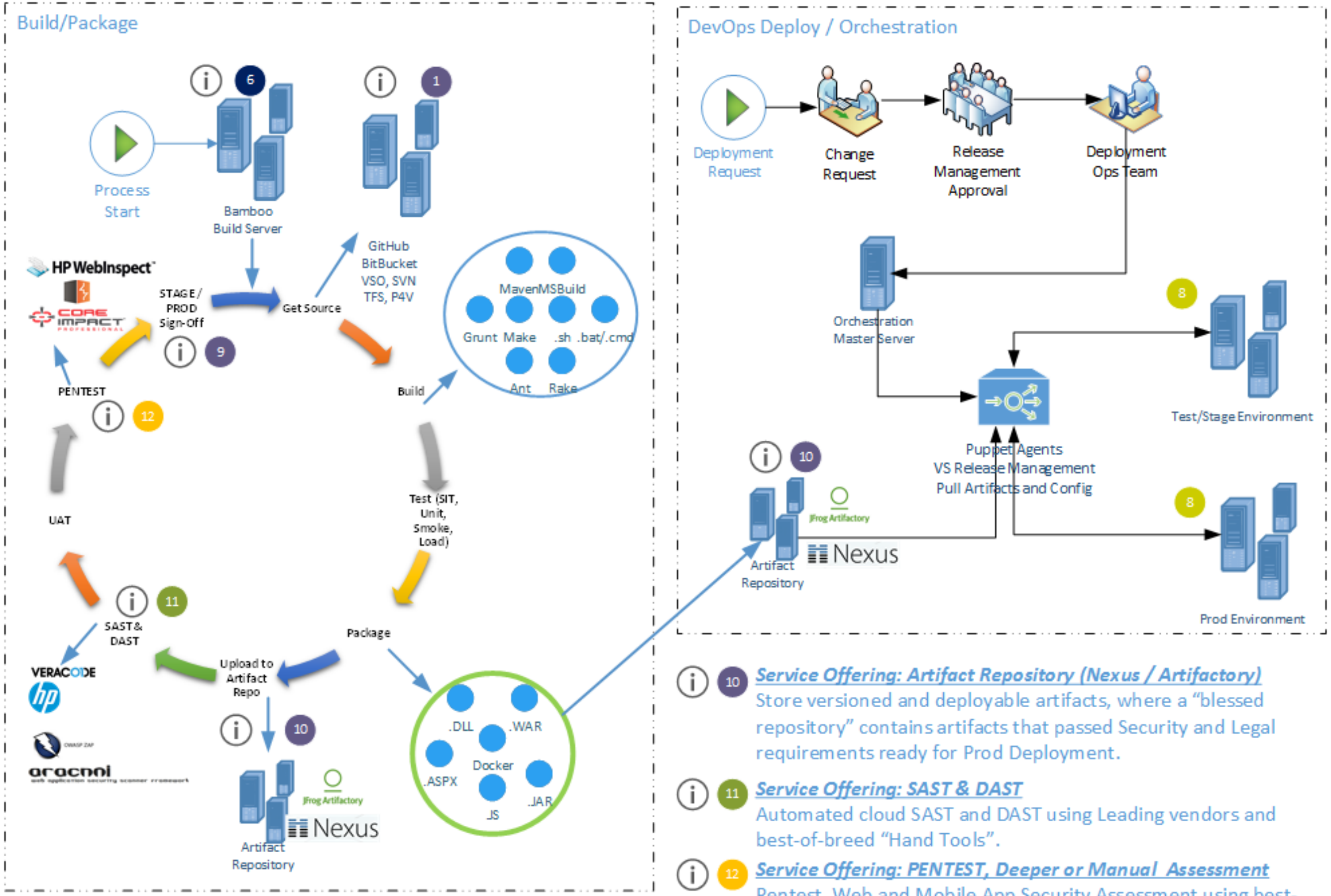
8 **Service Offering: Cloud SAST (HP FoD & Veracode)**
Cloud SAST is 1 of the post-build actions. Additional Post-build actions might not be "Security Related", such as code quality, test coverage, dependencies check, etc.

9 **Service Offering: Jira Ticketing and Service Desk**
For all interactions between clients and AppSec, JIRA Service Desk is used to standardize the process, track requests, track MTTR and SLA metrics, accountability & auditing
JIRA is also used by App Dev teams to create and keep backlog, plan sprints, track defects

Deployment Cycles

The proposed workflow demonstrates how the tools and the possible service offerings integrate within the deployment lifecycle.

Additionally, this diagram shows possible DevOps and Continuous Delivery integration points pulling “blessed” artifacts from Artifact Repository

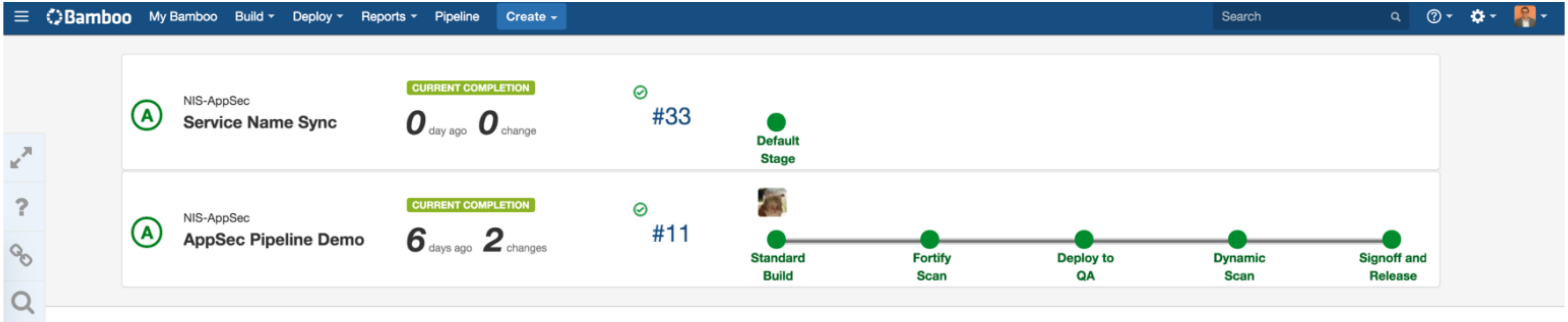


ⓘ 10 ***Service Offering: Artifact Repository (Nexus / Artifactory)***
Store versioned and deployable artifacts, where a “blessed repository” contains artifacts that passed Security and Legal requirements ready for Prod Deployment.

ⓘ 11 ***Service Offering: SAST & DAST***
Automated cloud SAST and DAST using Leading vendors and best-of-breed “Hand Tools”.

ⓘ 12 ***Service Offering: PENTEST, Deeper or Manual Assessment***
Pentest, Web and Mobile App Security Assessment using best-of-breed tools

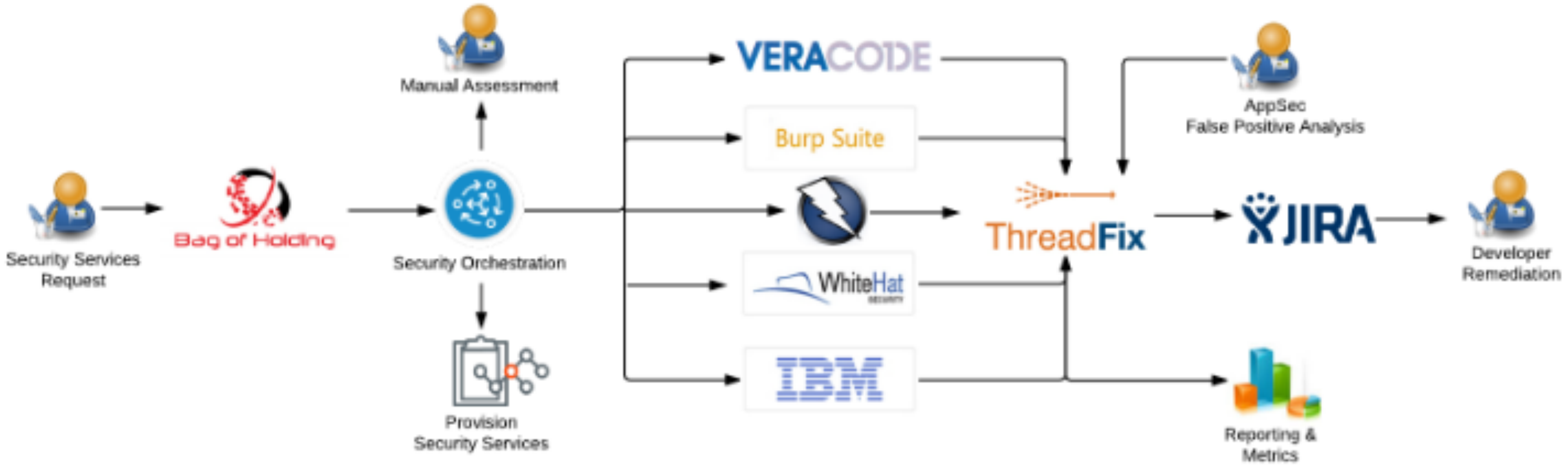
How does it look?



NIS-AppSec
Service Name Sync
CURRENT COMPLETION
0 day ago 0 change
#33

NIS-AppSec
AppSec Pipeline Demo
CURRENT COMPLETION
6 days ago 2 changes
#11

What others are using?



- Source: https://www.linkedin.com/pulse/appsec-pipeline-illustrated-aaron-weaver

No Money?

Open Source it’s you best friend

- Jira -> Bugzilla,
- Confluence -> Tiki Wiki
- Bamboo -> Jenkins
- Artifactory > Open-Source Artifactory
- HP WebInspect -> OWASP ZAP
- ThreadFix Open-Source
- StackStorm Open-Source
- Bag of Holding
- Gauntlt

Our next steps

The road to never ending Continuous Improvement

- “Dockerizing” this approach
- Leverage more Gauntlt
- Define aggregation and reporting strategy
- Create triggers for “auto-release” using chef/puppet
- ChatOps
- Machine Learning for False positives reduction
- BigData and BI for knowledge
- Continuous Improvement
- Rinse and repeat

Questions?

Contact Info:

Doug Morato

doug.morato@owasp.org

https://speakerdeck.com/dougmorato