DevSecOps Reference Architectures

Derek E. Weeks
VP and DevOps Advocate
Sonatype

2018

About this collection

1. The reference architectures can be used to **validate choices** you have made or are planning to make.

2. They are curated from the **community**. You will notice a number of common elements that are used repeatedly.

3. Each image has a link to its **original source** in the speaker notes, enabling you to deep dive for more knowledge.

If you would like to have **your reference architecture** added to this deck, please send it to weeks@sonatype.com.

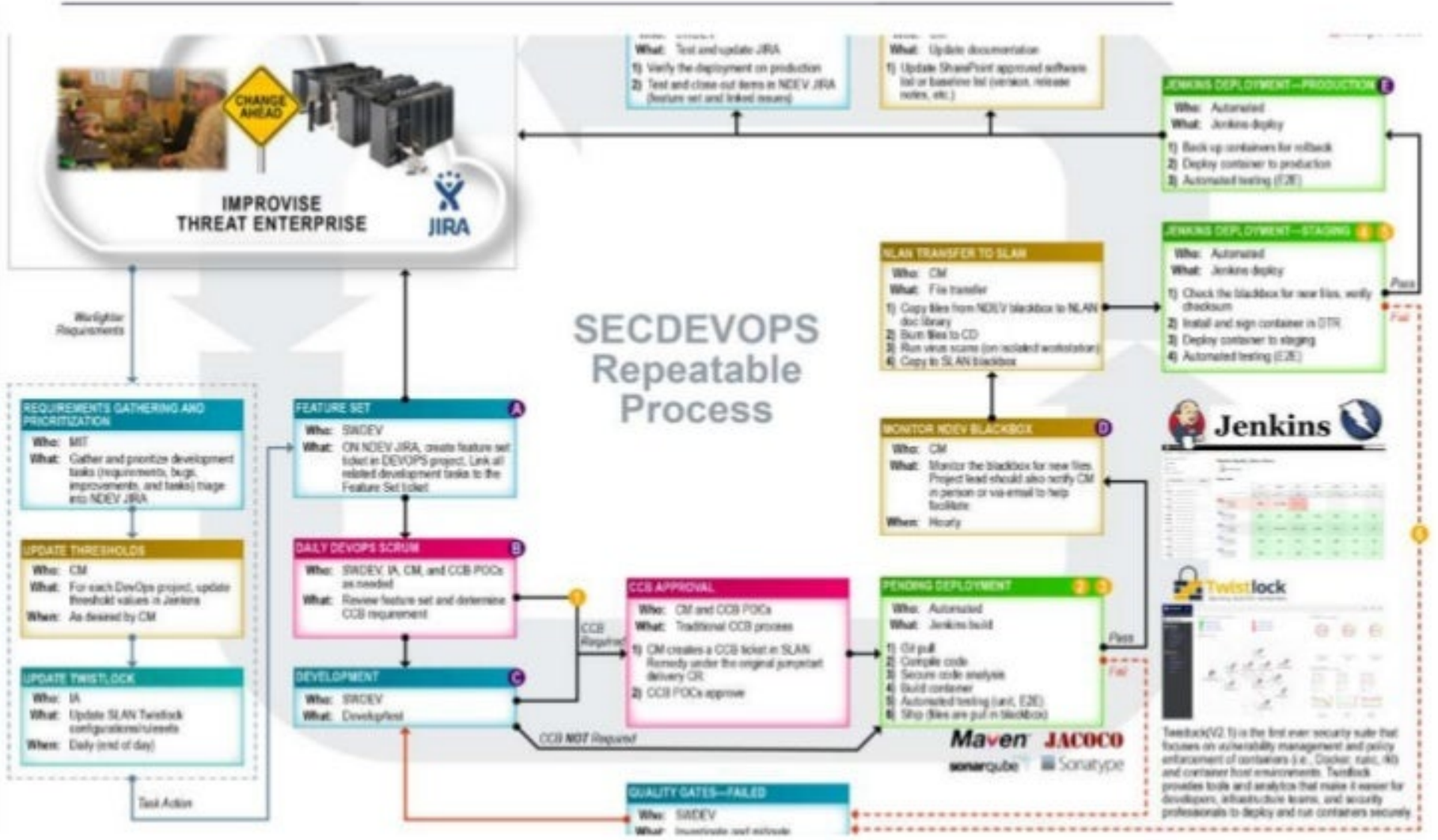
Degrees of DevSecOps Automation

	Integration Points and Degree of Automation				
DevSecOpsTooling	Design	Development (IDE)	Repository Manager	CI/CD	Post-Deployment
Open source governance	●	●	●	●	●
Open source software analysis	●	●	●	●	n/a
Static Application Security Testing (SAST)	●	●	●	●	n/a
Dynamic Application Security Testing (DAST)	●	n/a	n/a	n/a	◔
Interactive Application Security Testing (IAST)	●	n/a	n/a	●	n/a
Mobile Application Security Testing (MAST)	◐	n/a	◐	◐	n/a
Run-time Application Self Protection (RASP)	n/a	n/a	n/a	◐	●
Container and Infrastructure Security	◐	n/a	●	●	●

Source: Gartner, December 2017, Structuring Application Security Practices and Tools to Support DevOps and DevSecOps

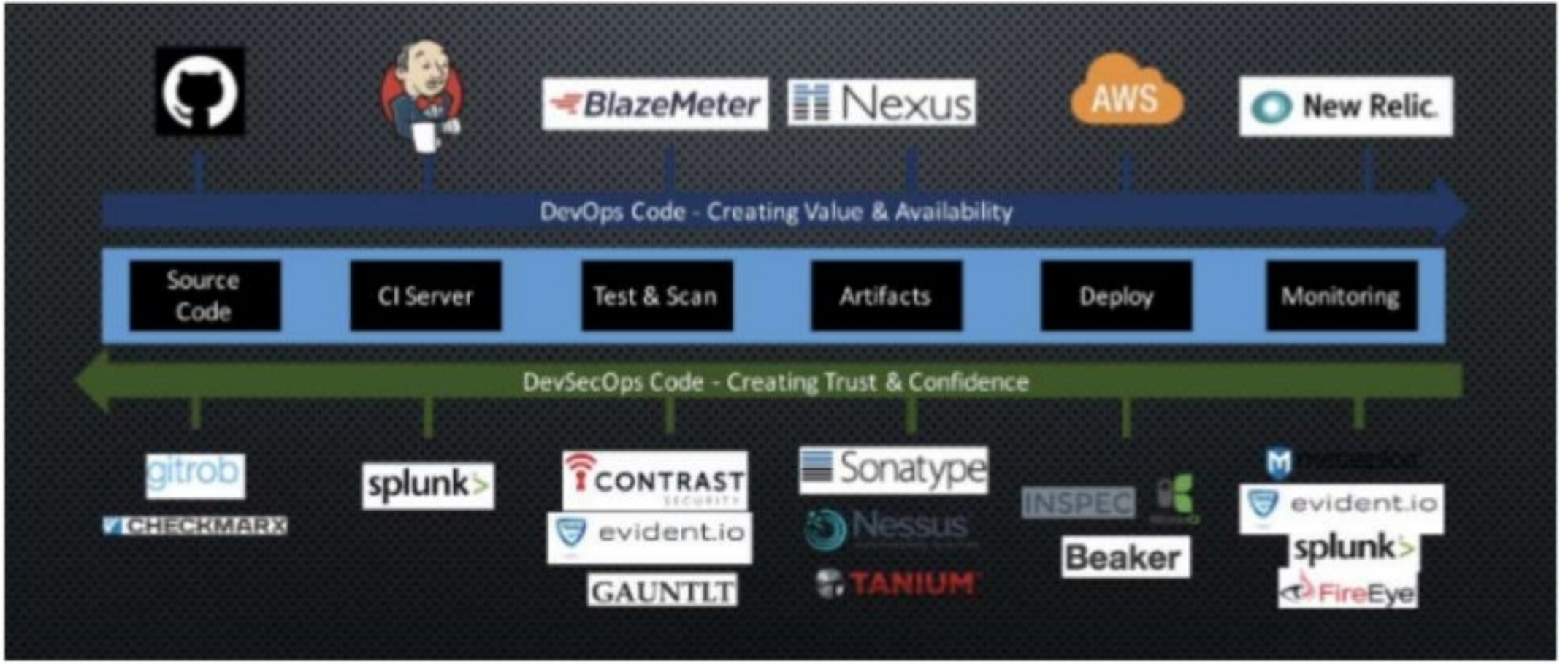
Common Elements of a DevSecOps Pipeline

DevSecOps according to U.S. Dept of Defense/JIDO

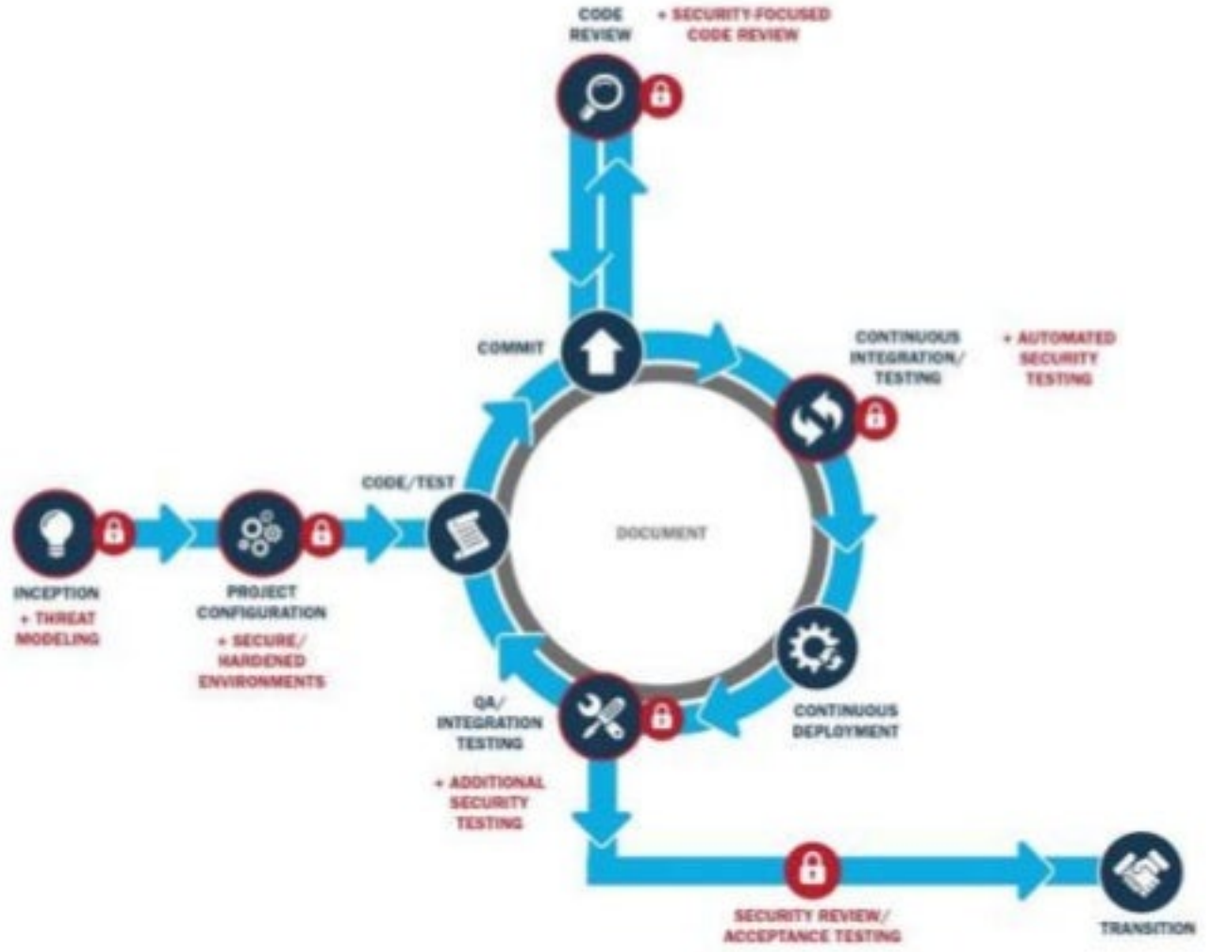


Sonatype

DevSecOps according to Magno Rodrigues

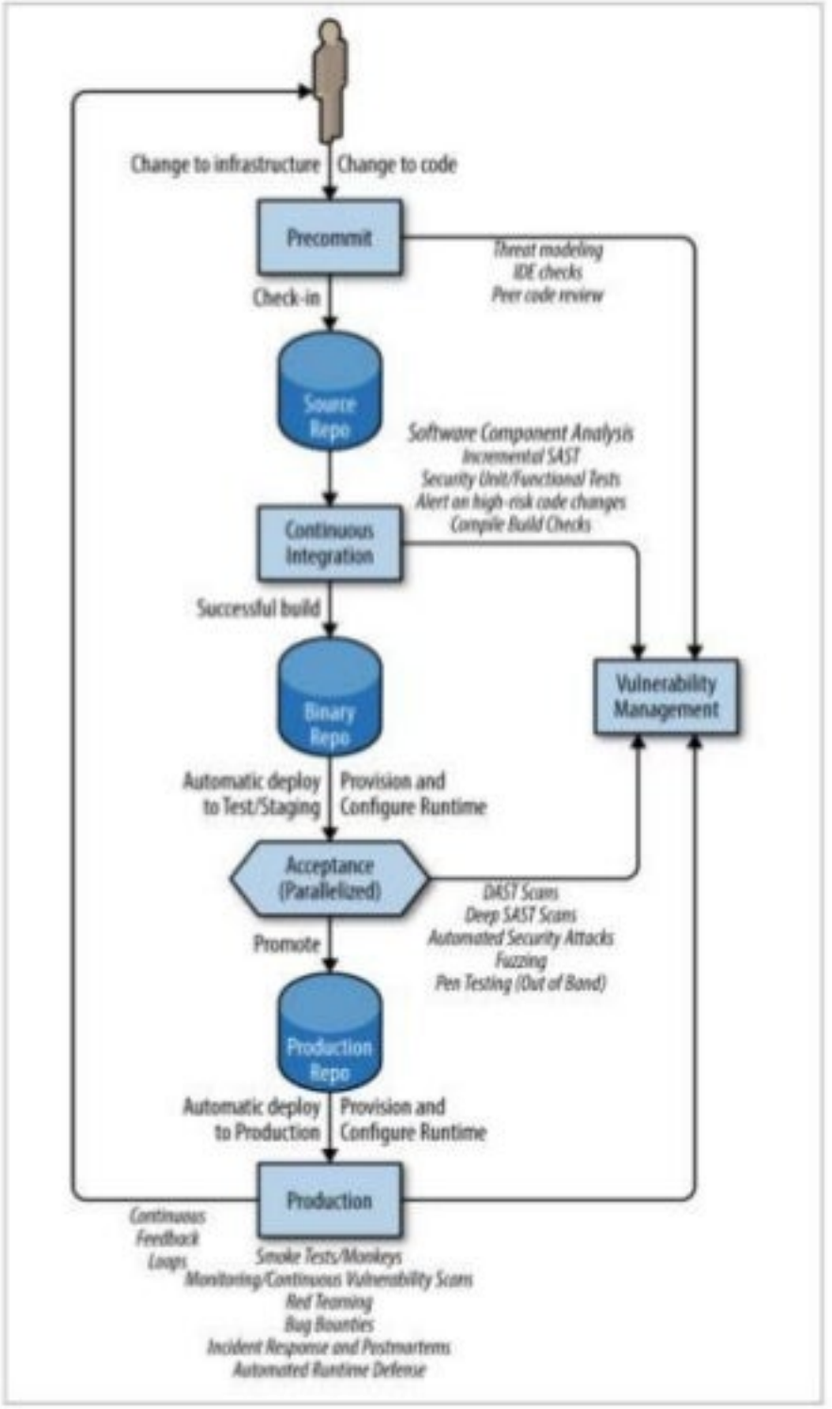


DevSecOps according to Carnegie Mellon's SEI



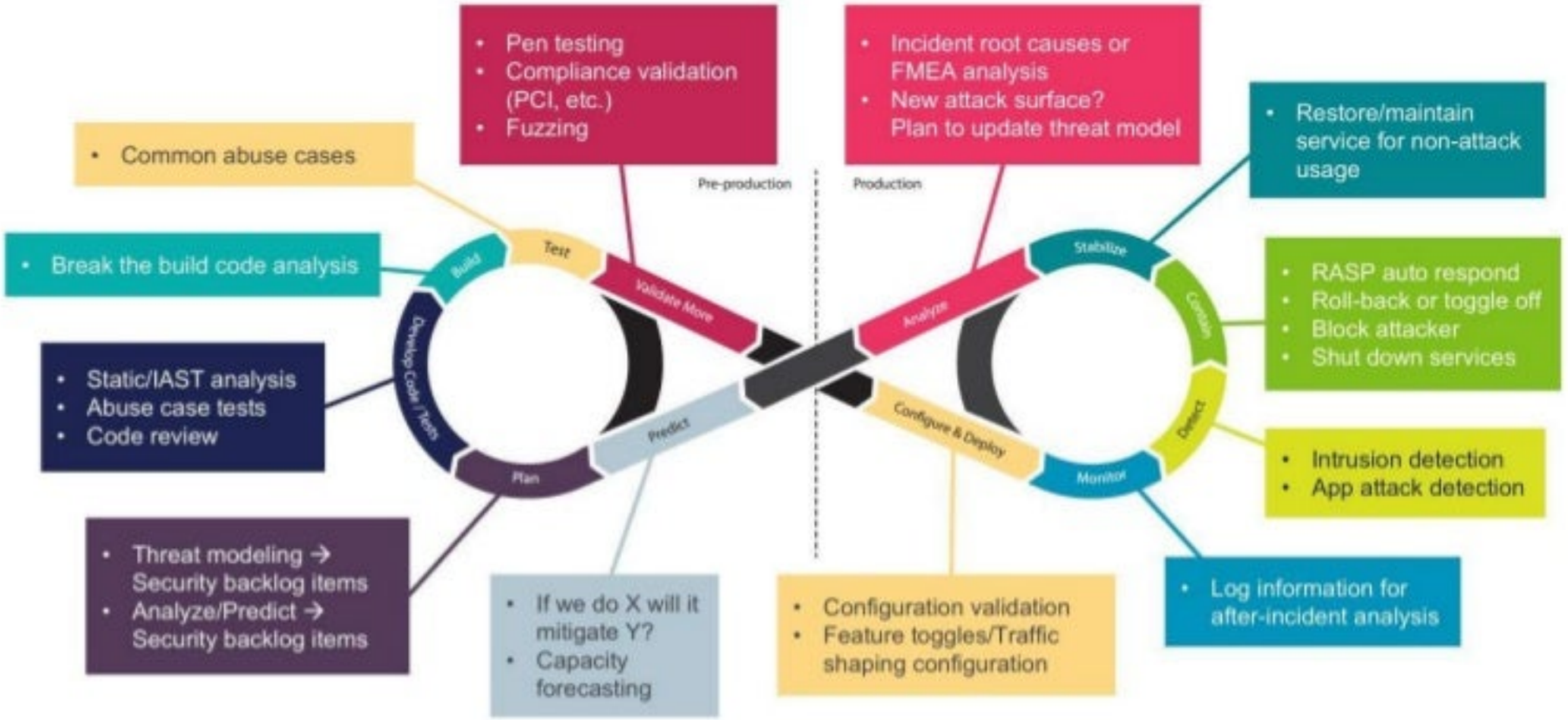
Sonatype

DevSecOps according to Jim Bird



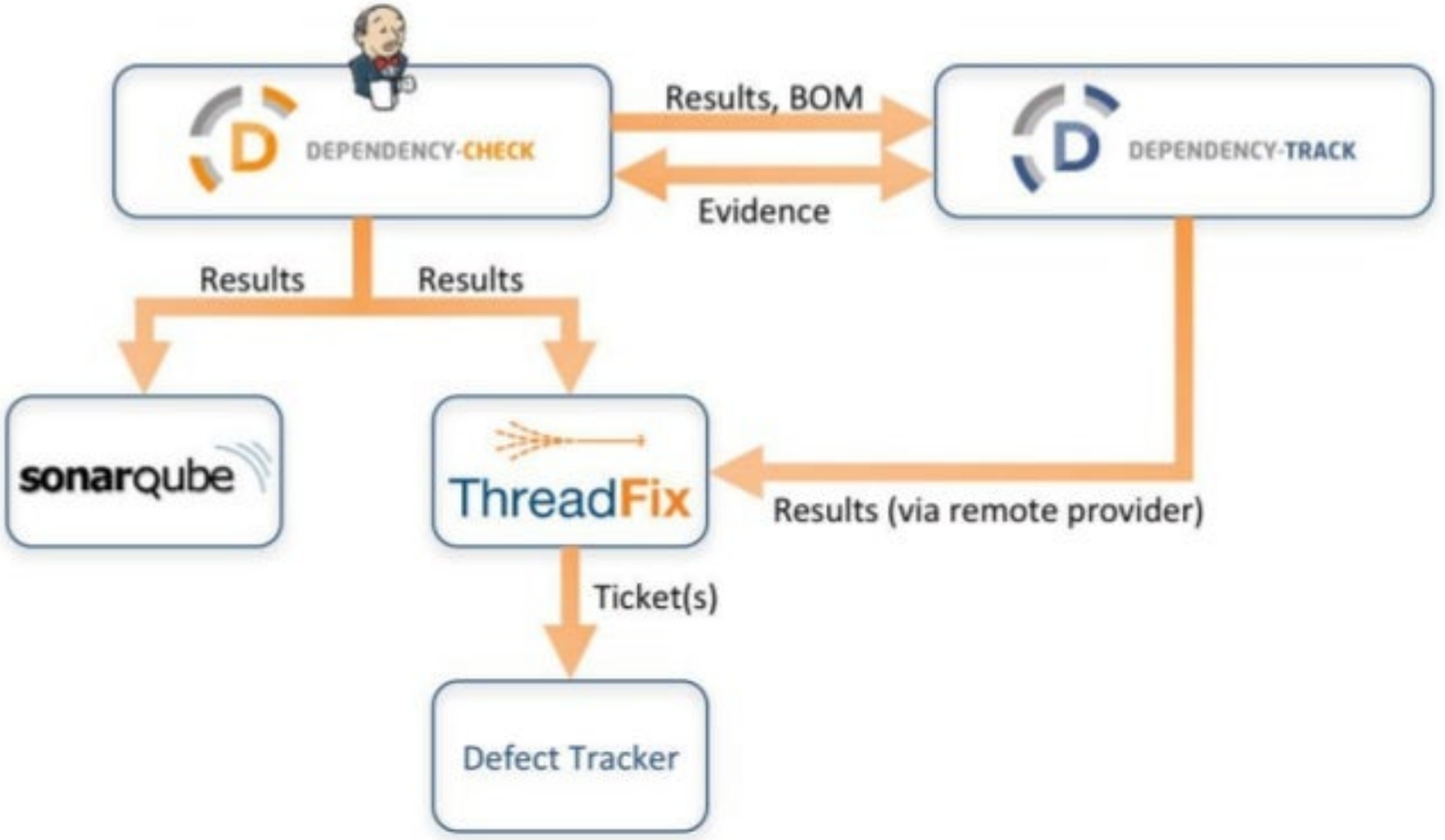
Sonatype

DevSecOps according to Larry Maccherone

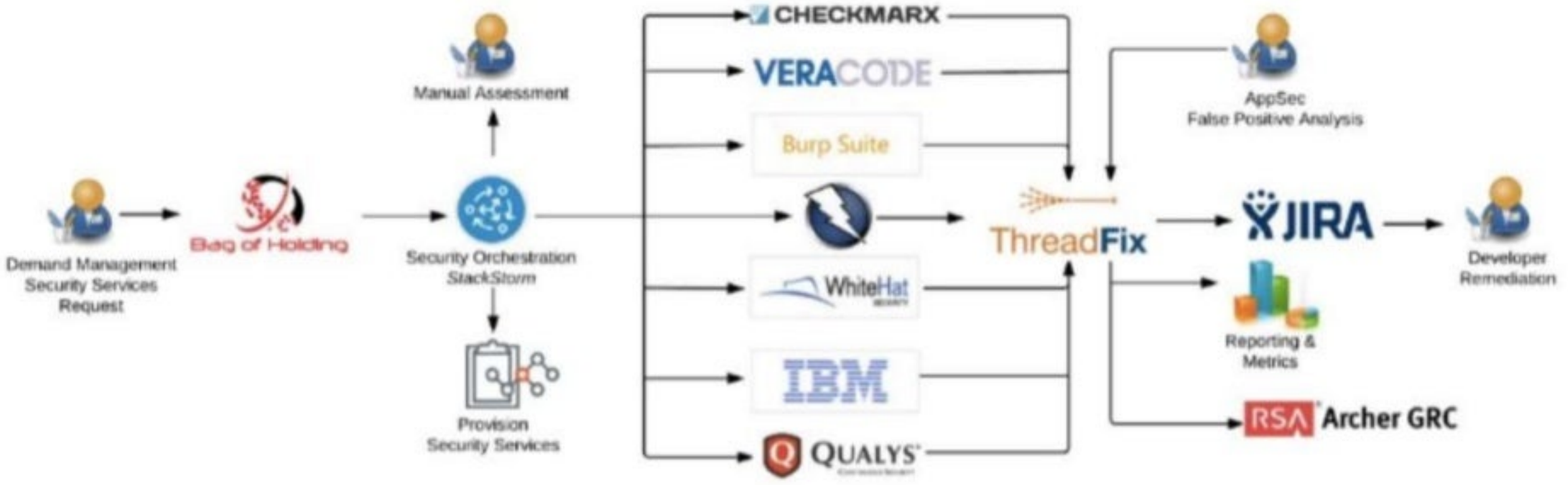


Sonatype

DevSecOps according to Steve Springett



DevSecOps according to TeachEra



Sonatype

Learn More From Your Peers

21 DevSecOps practitioners from leading enterprises to shared their experiences and best practices. All 21 recordings are available for **free** at www.alldaydevops.com.


LendingClub


box


tyro


UNDER ARMOUR


aetna


ABN·AMRO

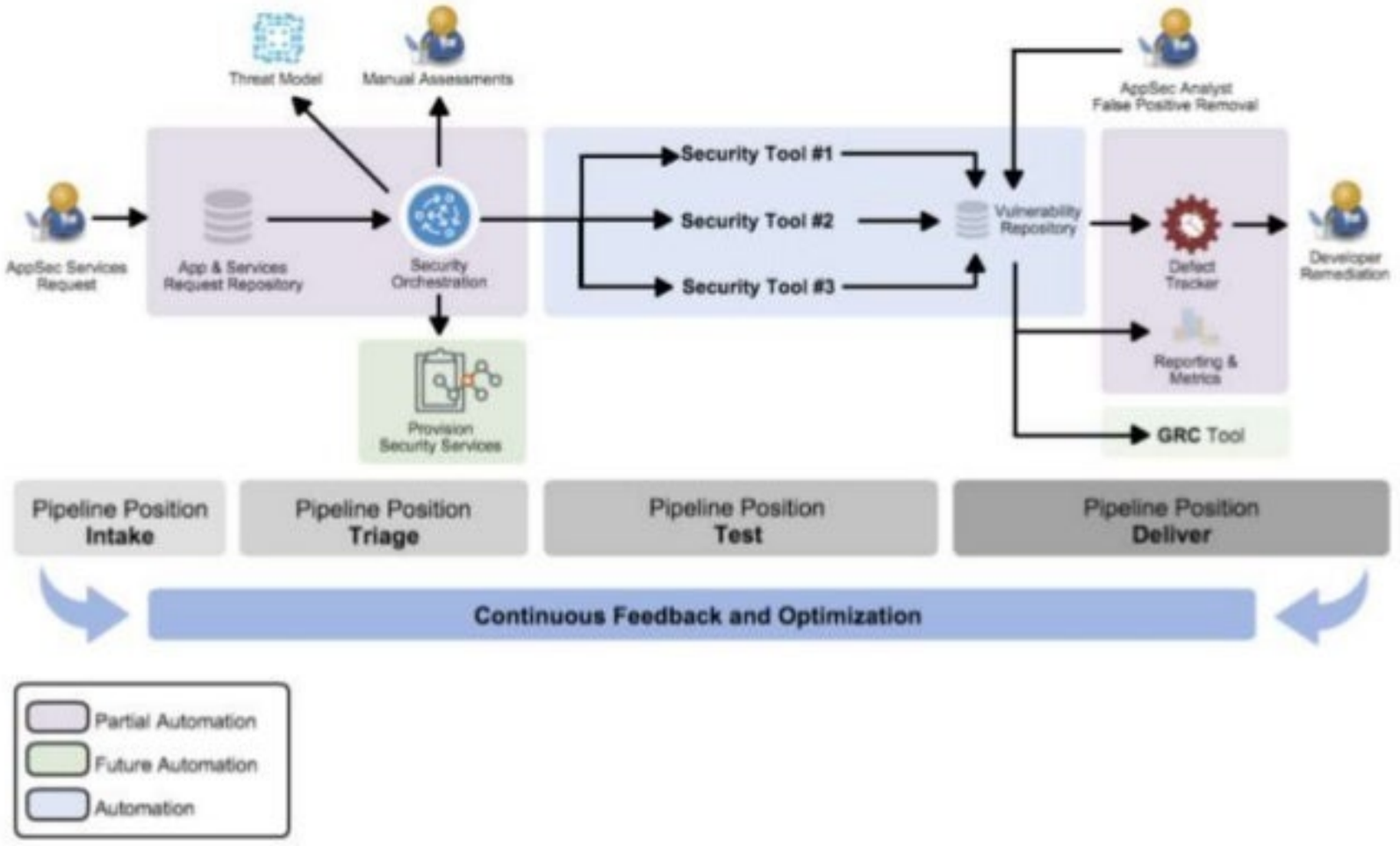

accenture


Microsoft


GSA

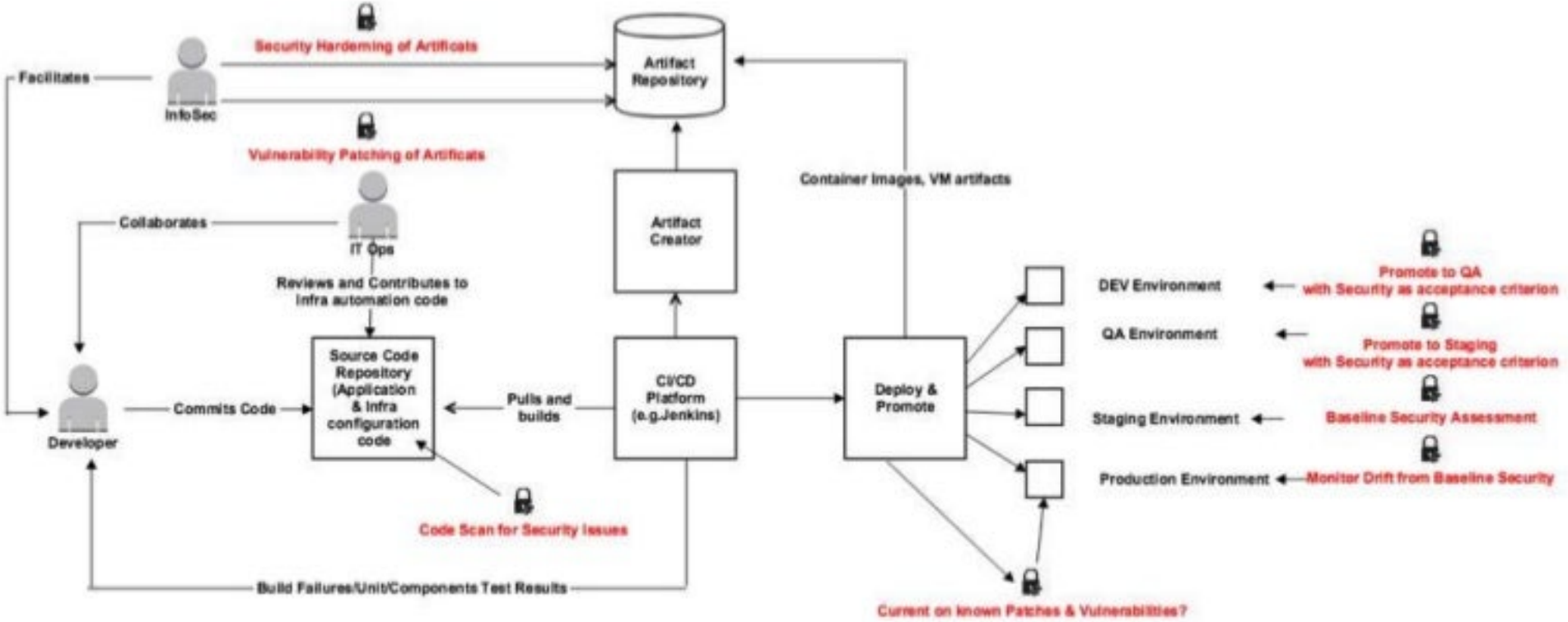
DevSecOps according to Coveros

DevSecOps according to Aaron Weaver



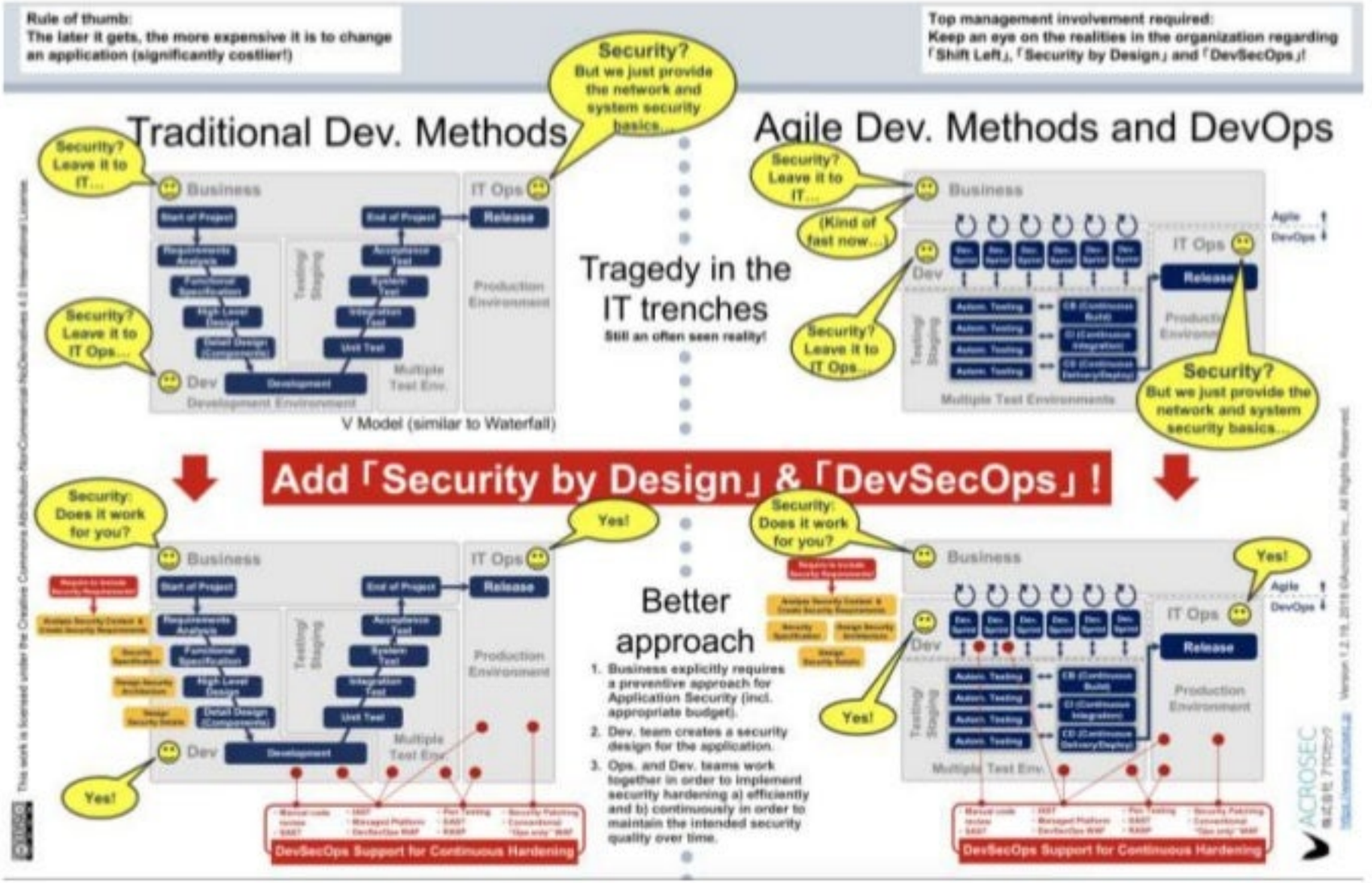
Sonatype

DevSecOps according to Dr. Ravi Rajamiyer



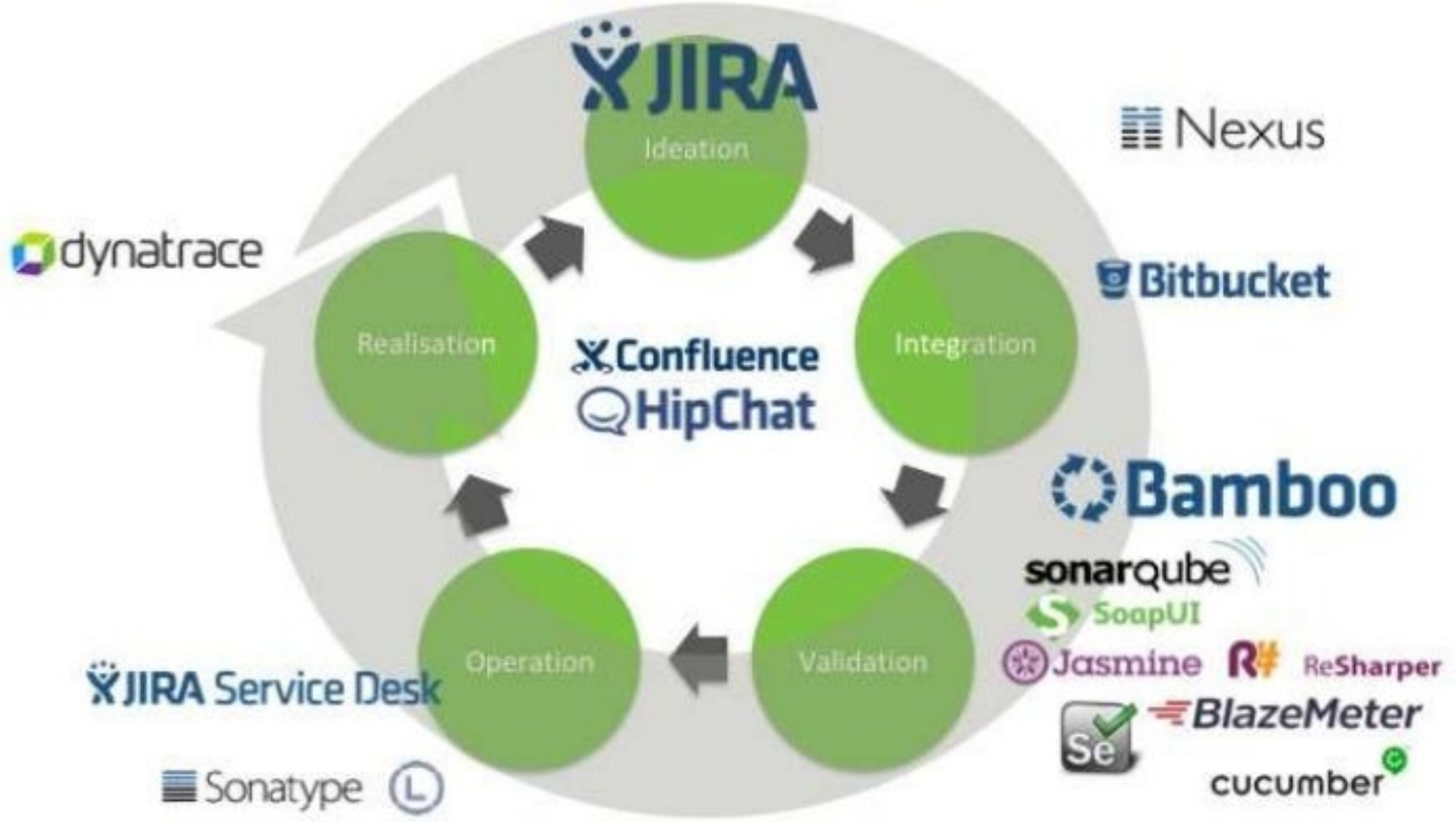
Sonatype

DevSecOps according to ACROSEC

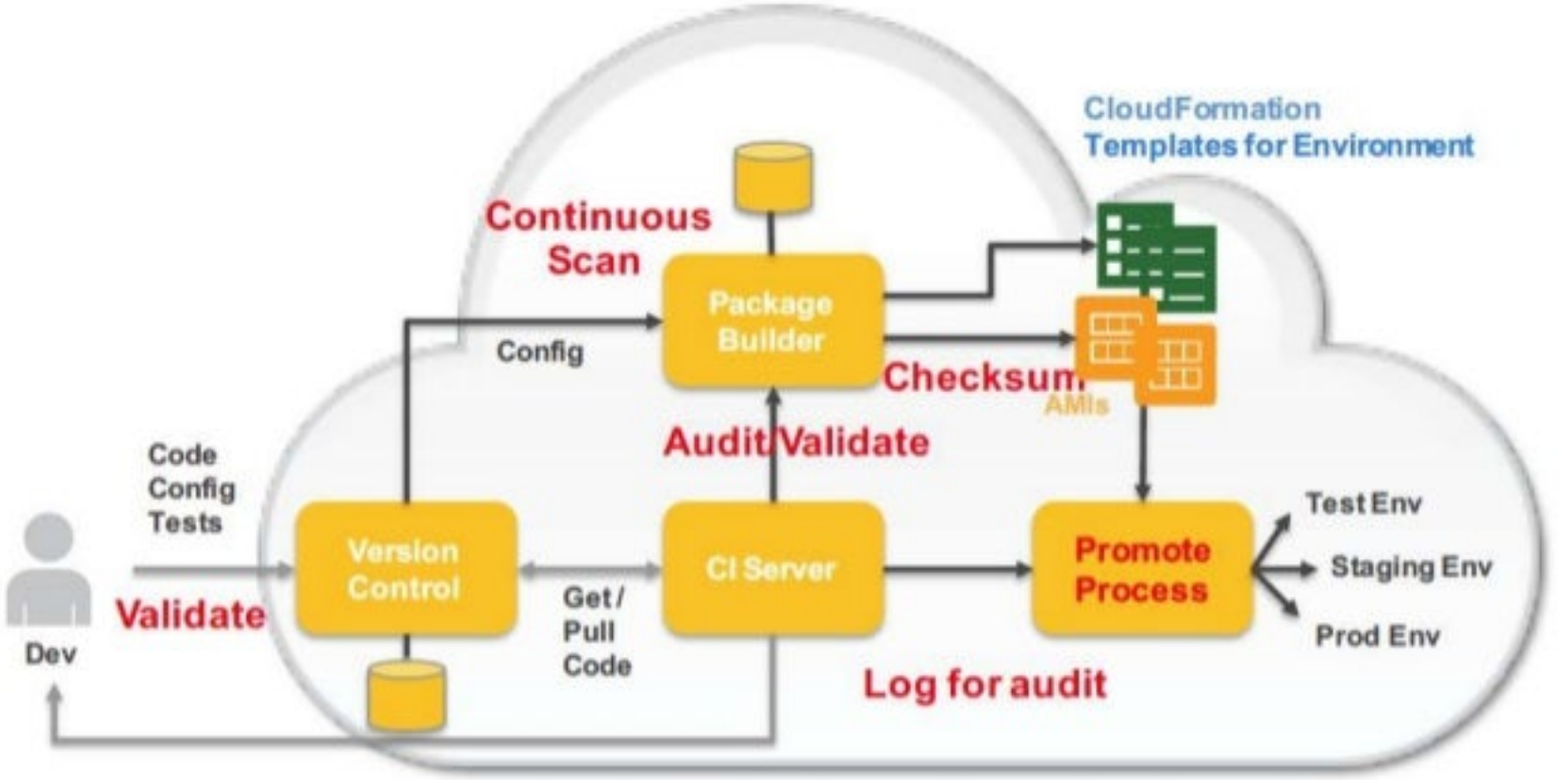


Sonatype

DevSecOps according to Ranger4

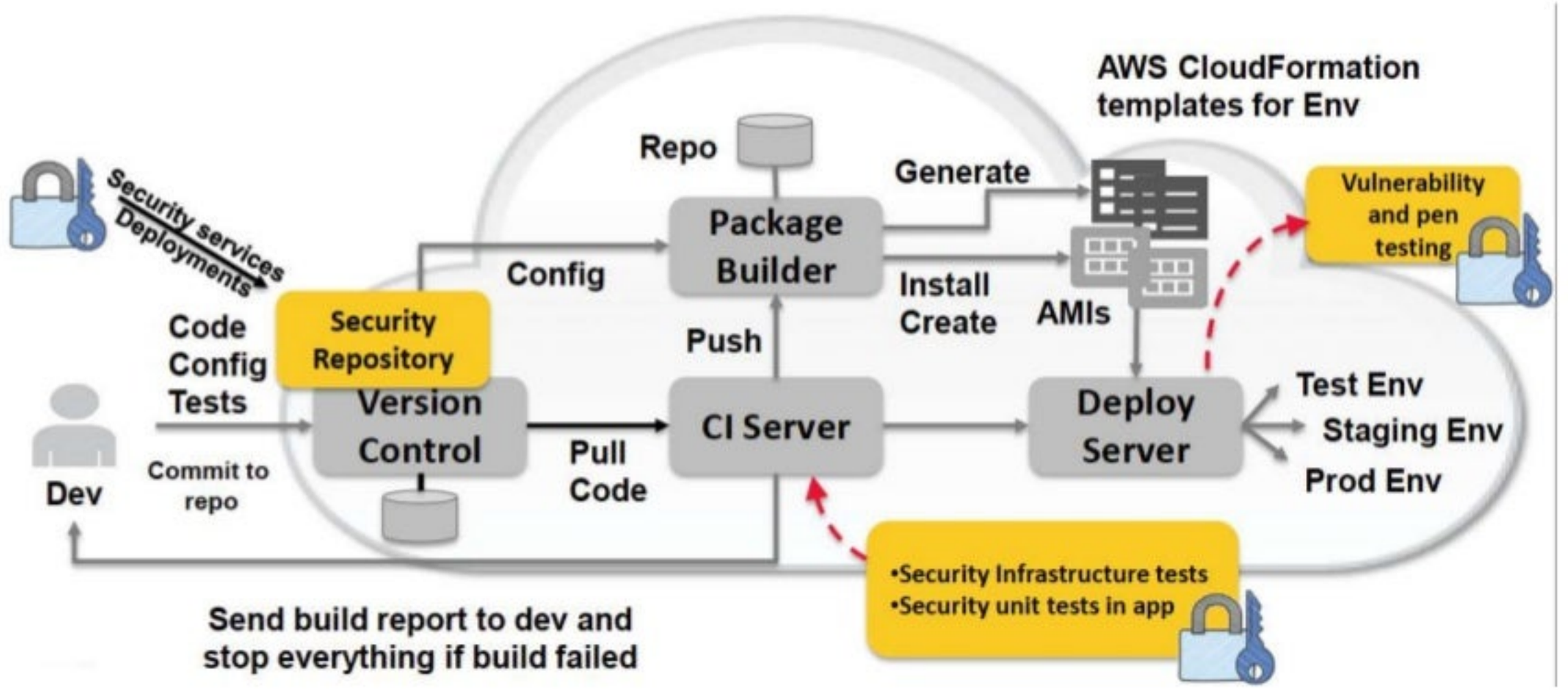


DevSecOps according to AWS



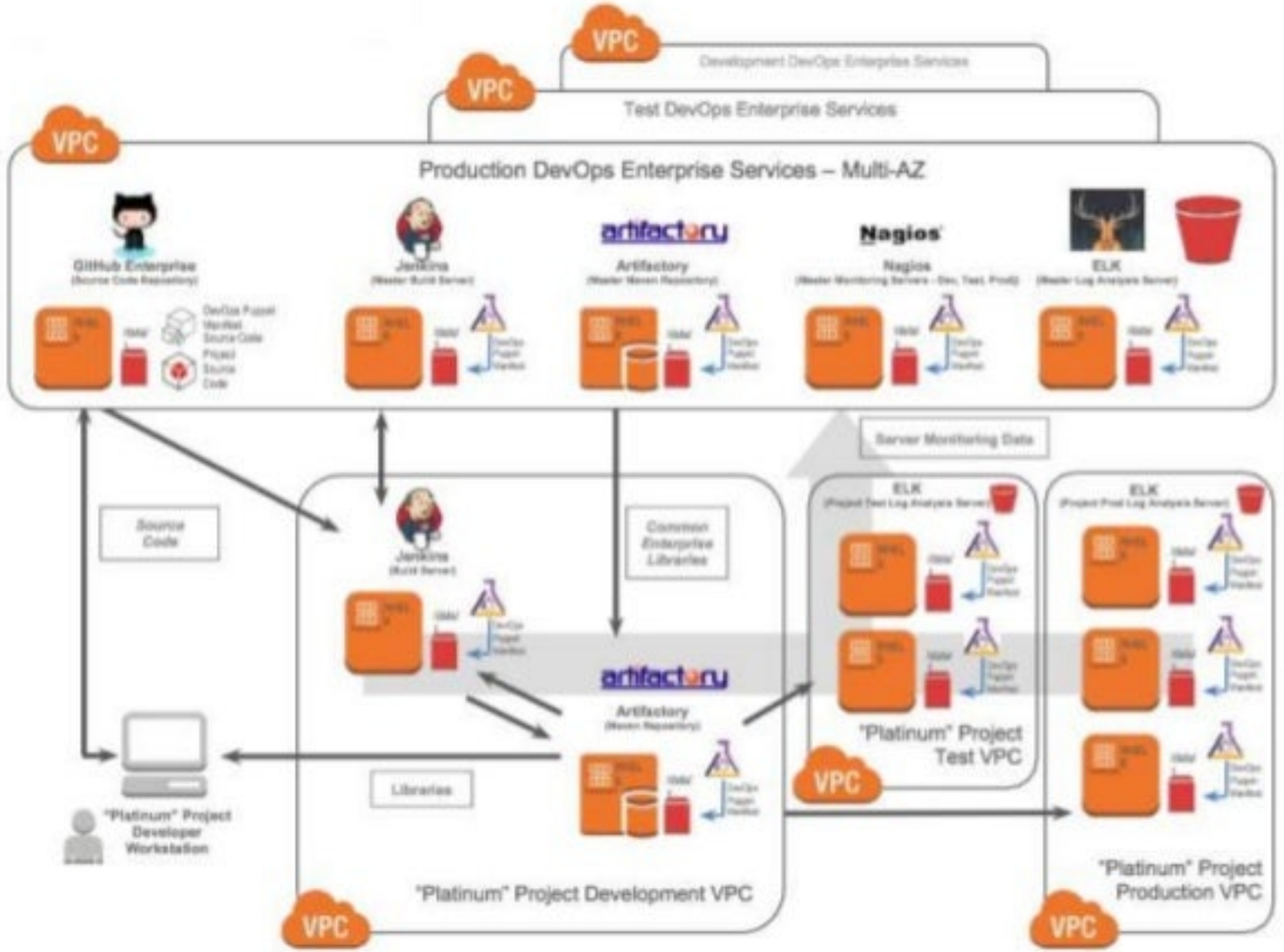
Send Build Report to Security
Stop everything if audit/validation failed

DevSecOps according to AWS



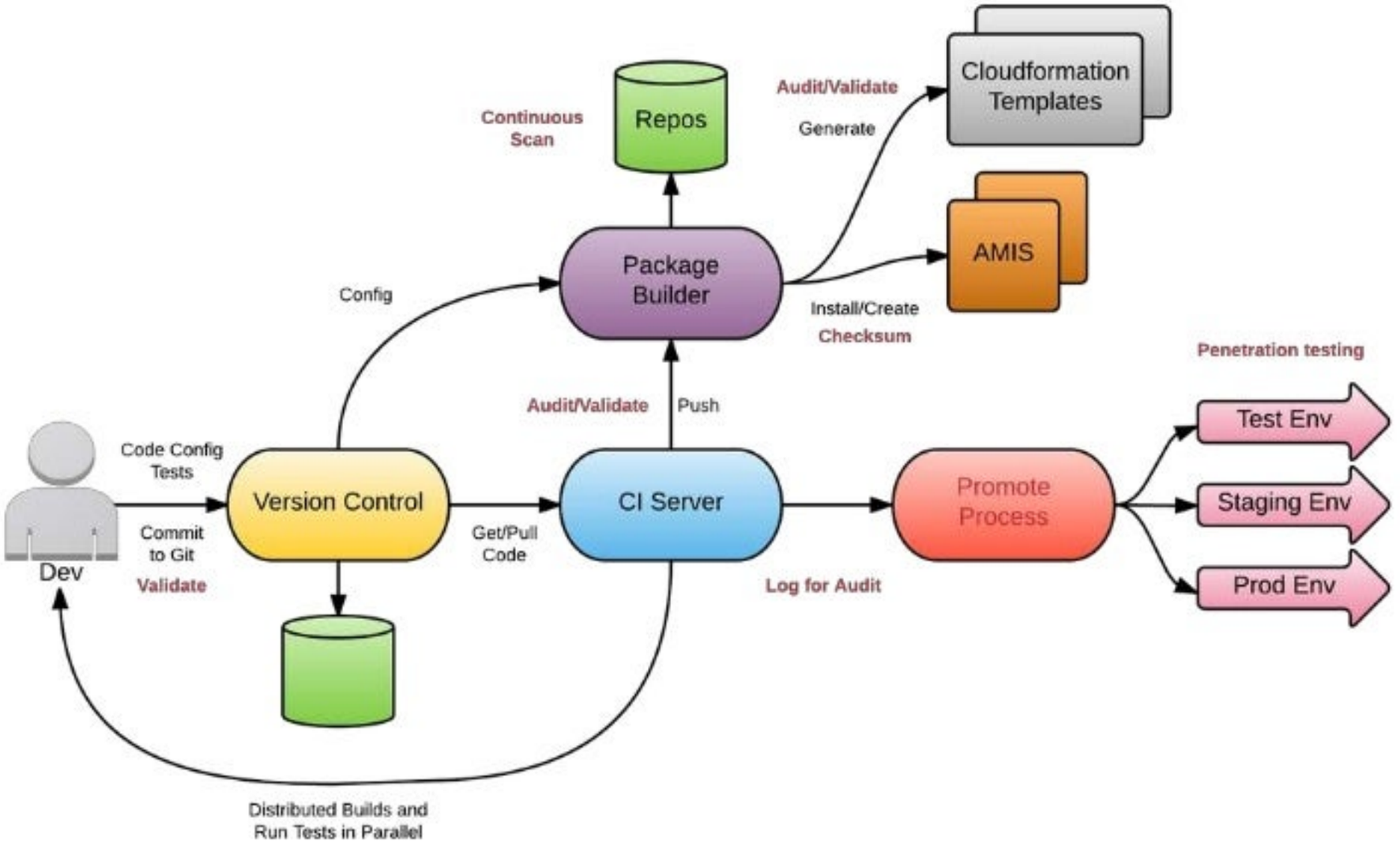
Sonatype

DevSecOps according to Accenture



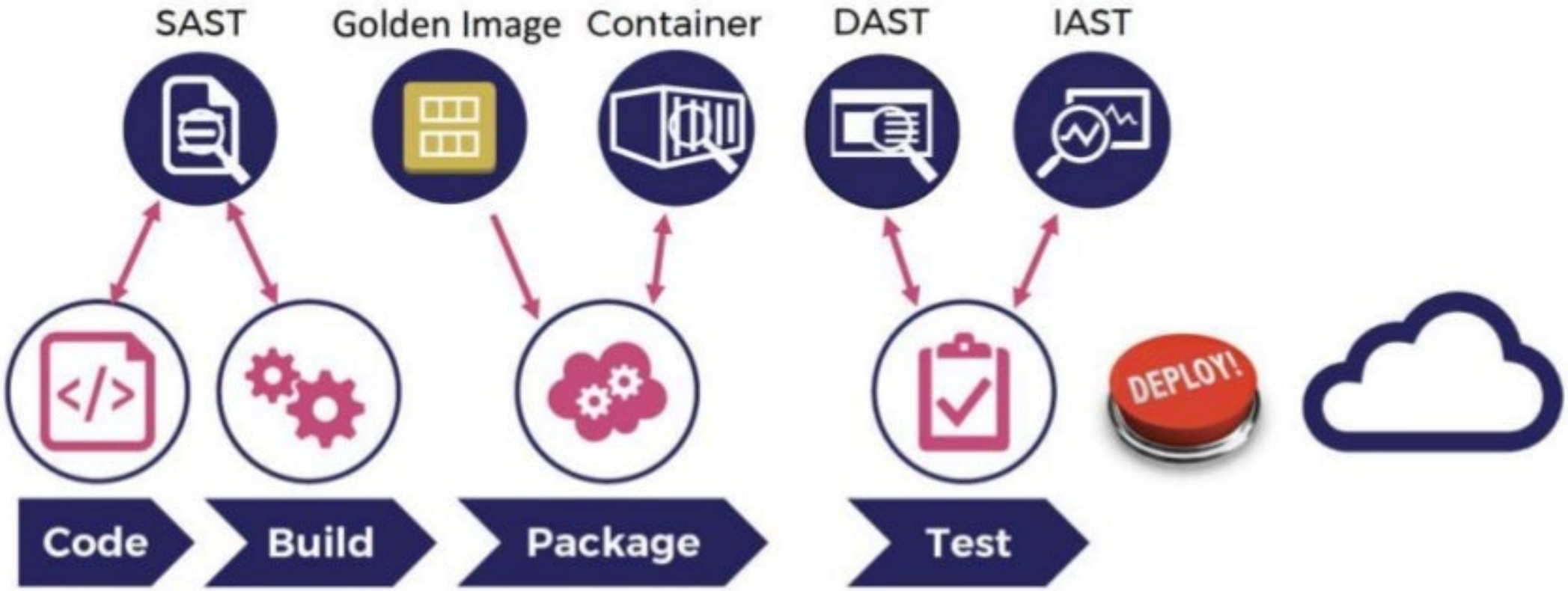
Sonatype

DevSecOps according to Shine Solutions

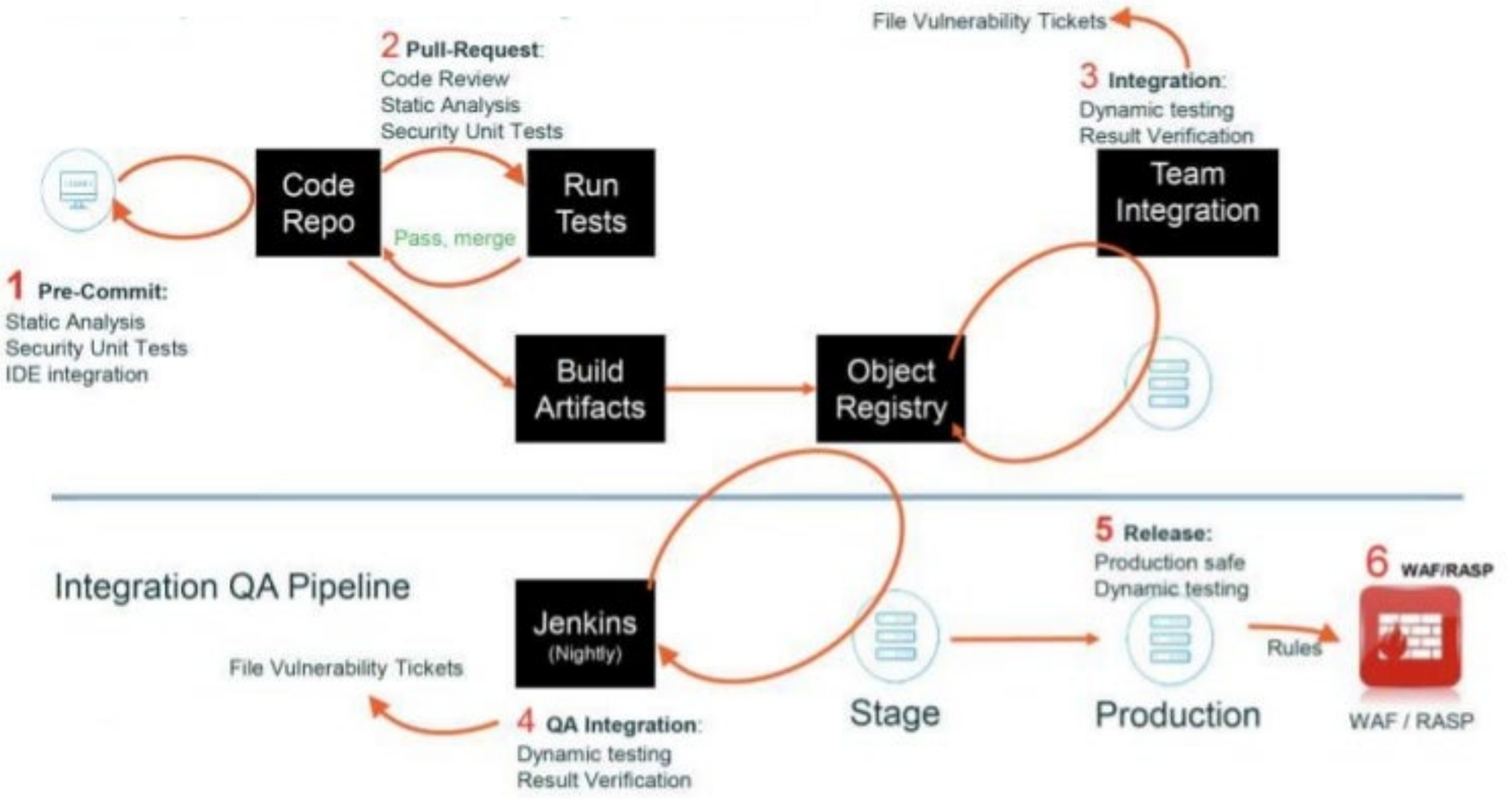


Sonatype

DevSecOps according to Ellucian



DevSecOps according to WhiteHat Security



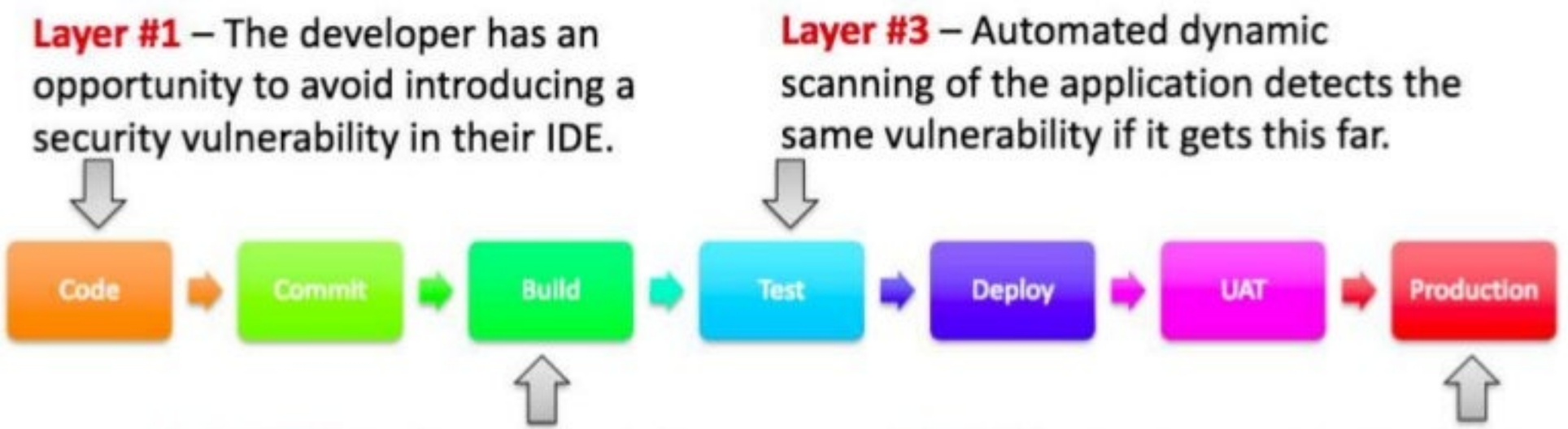
Sonatype

DevSecOps according to GSA

BUILD		TEST	DEPLOY	OPERATIONS
PLAN	CODE	(CI)	(CD)	SECURITY & MONITORING
JIRA Slack Trello	Ansible GitHub Jenkins	Jenkins Selenium	Ansible Jenkins Terraform CloudFormation	AMI ClamAV CloudWatch Nessus OSSEC SolarWinds

https://tech.gsa.gov/guides/building_devsecops_culture/

DevSecOps according to Sense of Security



Sonatype

We would love to add your DevSecOps reference architecture to this deck.

How?

1. Send it to me (weeks@sonatype.com), with the subject line: DevSecOps reference architecture.

2. Provide me link as to where people can find more information about the architecture (e.g., your blog, a video, a SlideShare deck).

3. I'll add it to this deck with full attribution to you, and let you know that it's been updated.

It's that easy. We all learn with help from the community. Thank you for your contributions!


Sonatype