



DevSecOps Reference Architectures 2019

Derek E. Weeks
VP and DevOps Advocate
Sonatype





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.

Common Elements of DevSecOps Pipeline



Degrees of DevSecOps Automation

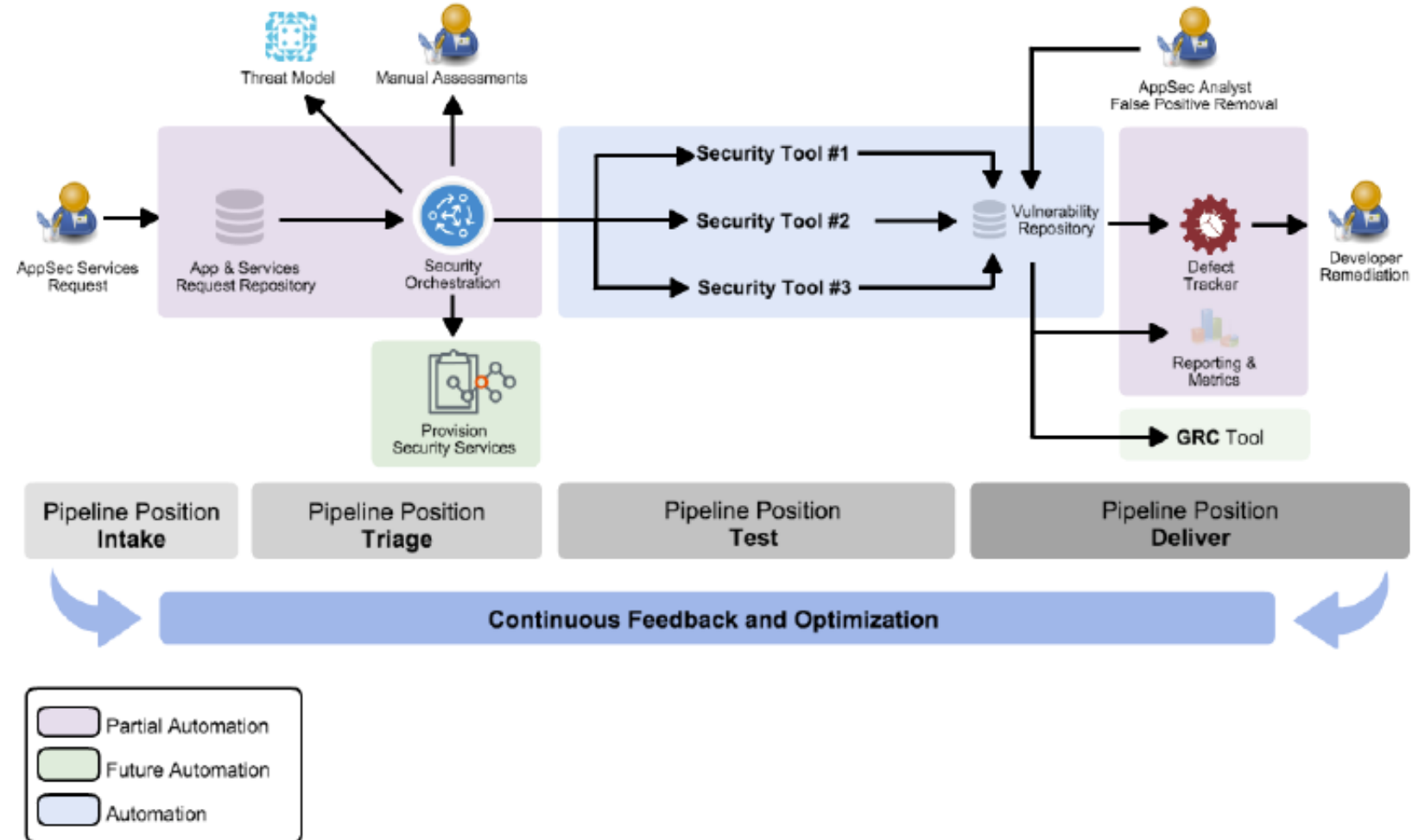
	Integration Points and Degree of Automation				
DevSecOps Tooling	Design	Development (IDE)	Repository Manager	CI/CD	Post-Deployment
Open source governance	●	●	●	●	●
Open source software analysis	●	●	●	●	n/a
Static Application Security Testing (SAST)	●	●	●	●	n/a
Dynamic Application Security Testing (DAST)	●	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	●	●	●

GSA's DevSecOps Maturity Model

Metric	Description	Associated Domain(s)
Deployment frequency	Number of deployments to production in a given time frame	Application Deployment; Authority to Operate Processes
Change lead time (for applications)	Time between a code commit and production deployment of that code	Overarching; Authority to Operate Processes; Patch Management
Change volume (for applications)	Number of user stories deployed in a given time frame	Overarching
Change failure rate	Percentage of production deployments that failed	Application Deployment
Mean time to recovery (MTTR) (for applications)	Time between a failed production deployment to full restoration of production operations	Application Deployment; Backup and Data Lifecycle Management; Patch Management
Availability	Amount of uptime/downtime in a given time period, in accordance with the SLA	Availability and Performance Management; Network Management
Customer issue volume	Number of issues reported by customers in a given time period	Overarching
Customer issue resolution time	Mean time to resolve a customer-reported issue	Overarching
Time to value	Time between a feature request (user story creation) and realization of business value from that feature	Overarching; Authority to Operate Processes
Time to ATO	Time between the beginning of Sprint 0 to achieving an ATO	Overarching; Authority to Operate Processes
Time to patch vulnerabilities	Time between identification of a vulnerability in the platform or application and successful production deployment of a patch	Authority to Operate Processes

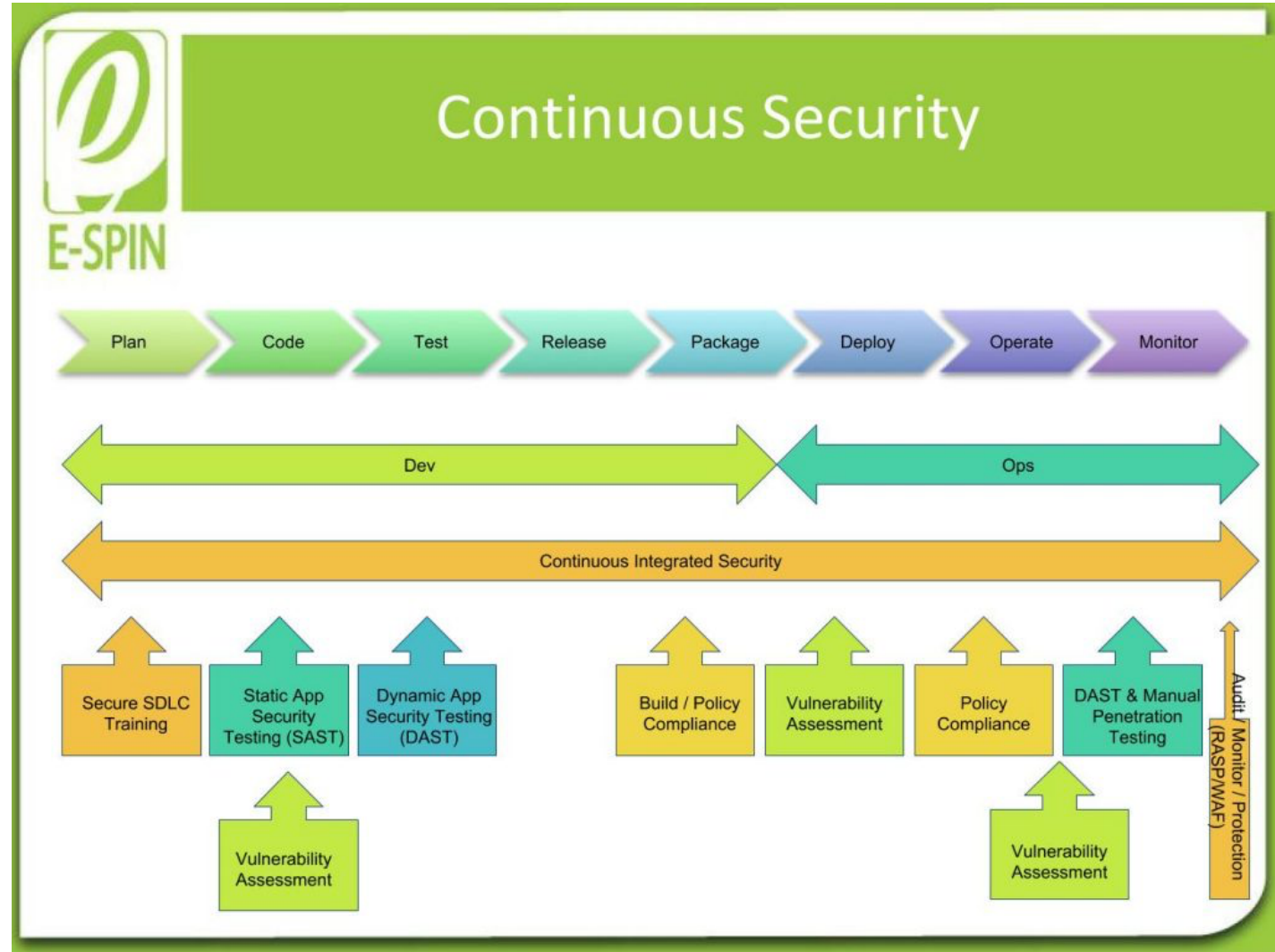
DevSecOps According to OWASP

Rugged Devops - AppSec Pipeline Template



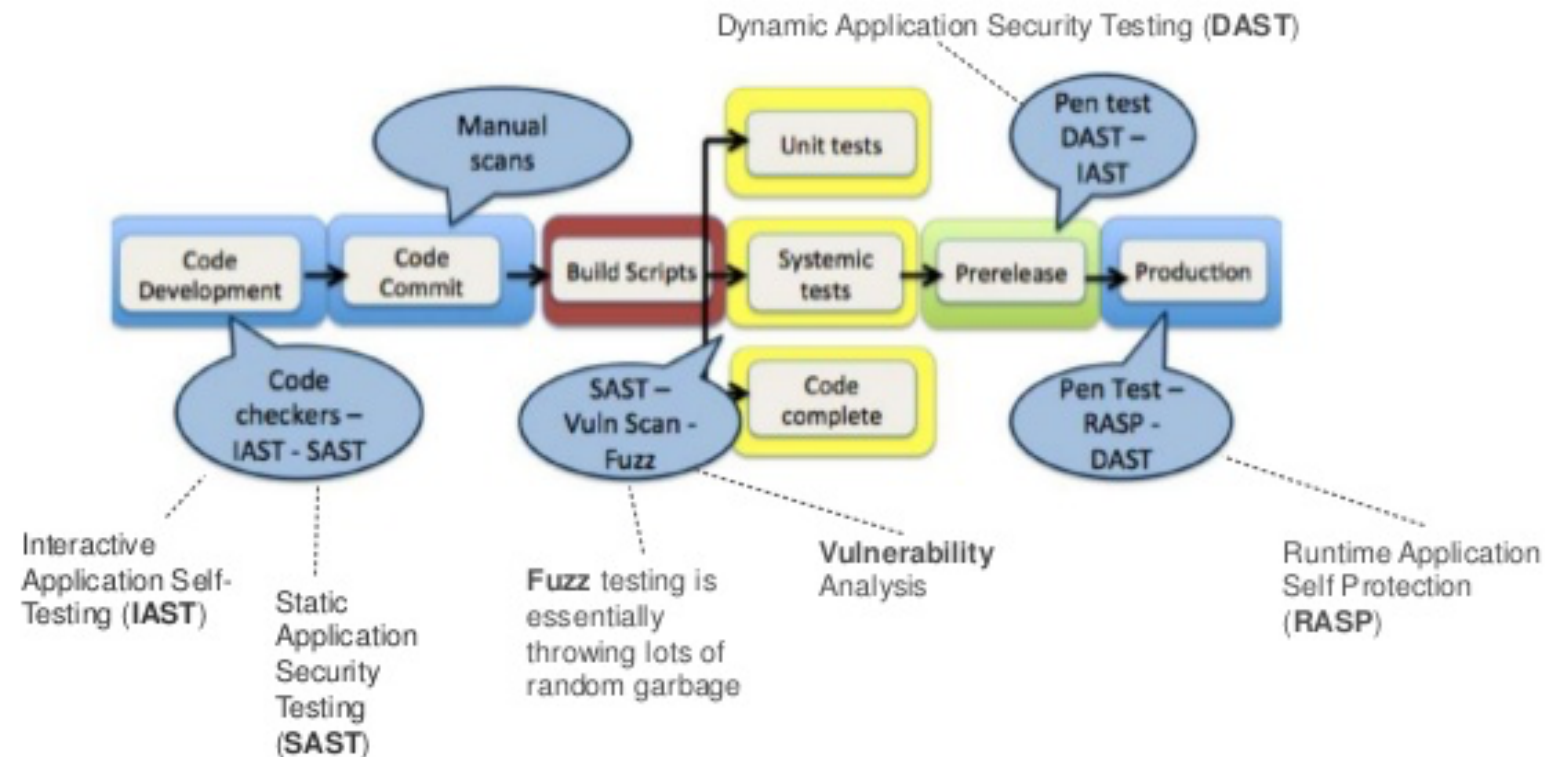
Aaron Weaver, CC ShareAlike 3.0

DevSecOps according to E-SPIN

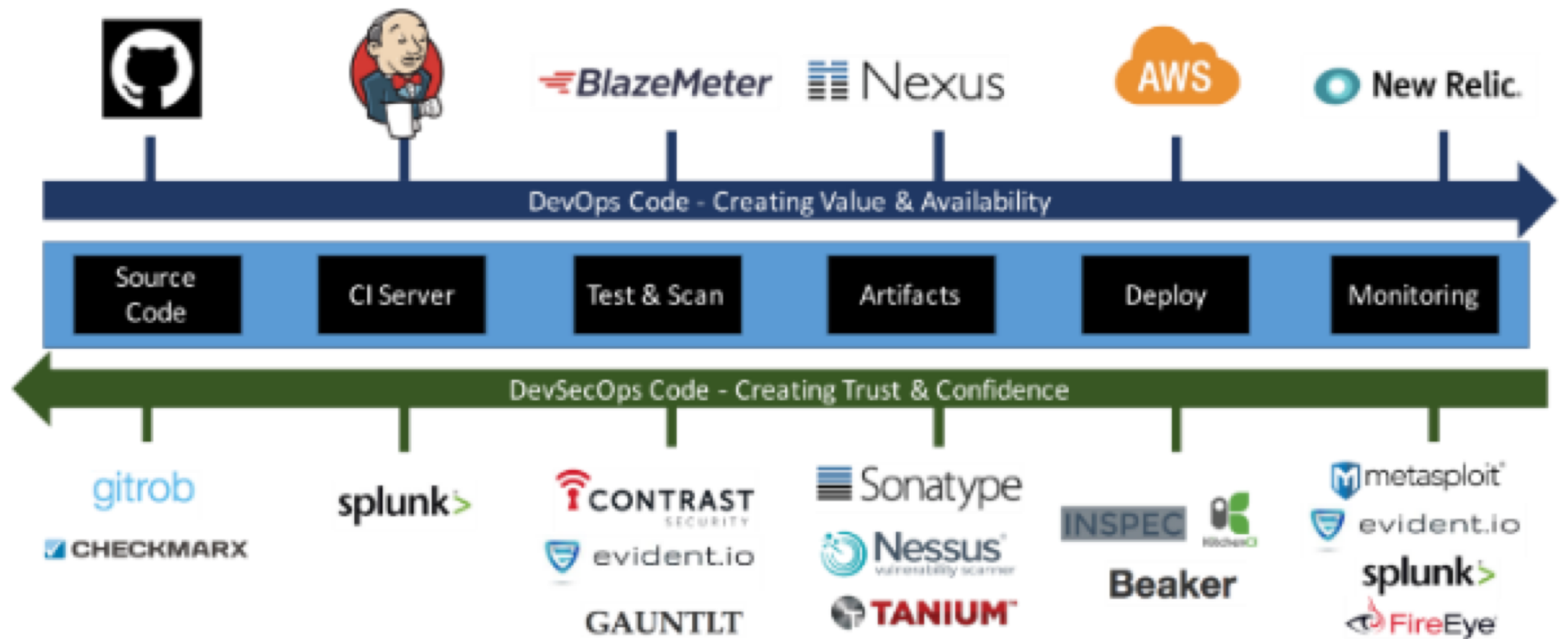


DevSecOps according to Ulf Mattsson and TokenEx

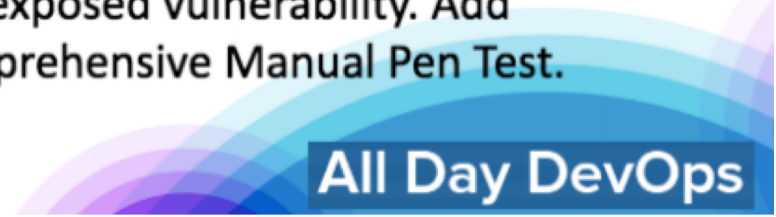
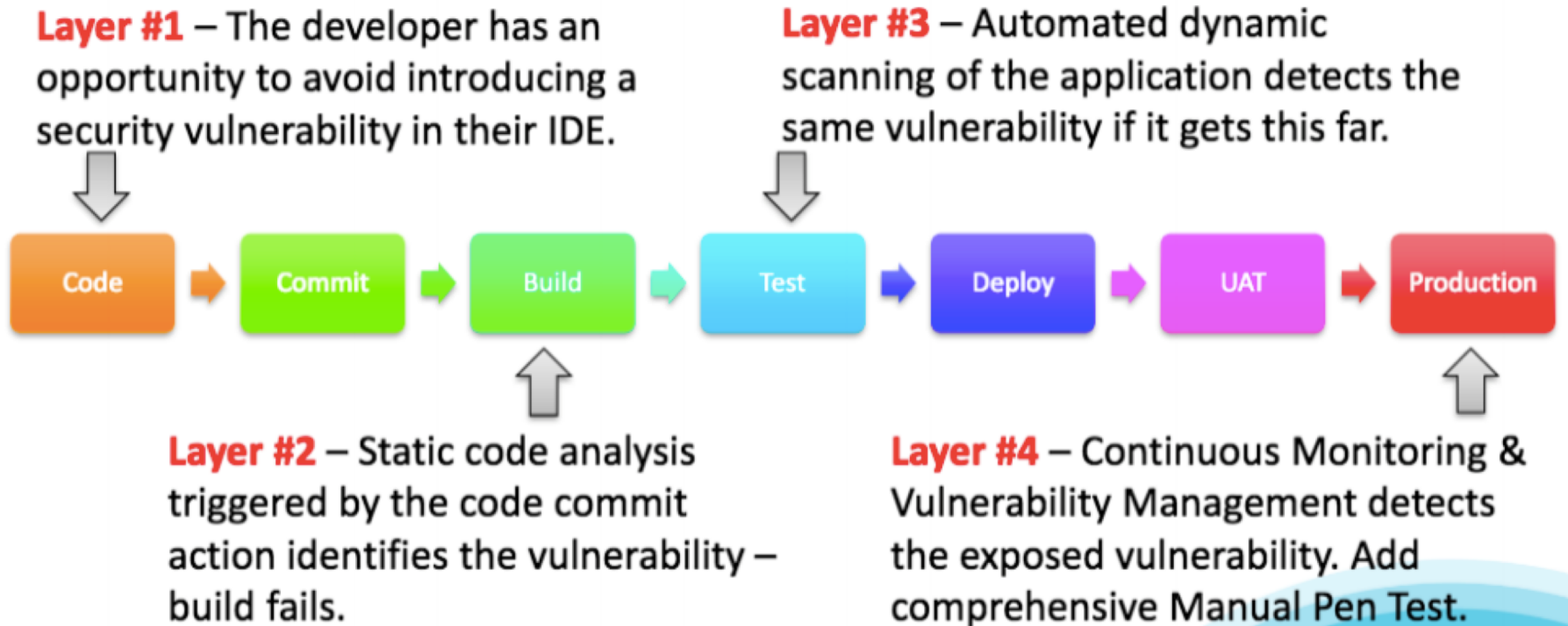
Security Tools for DevOps



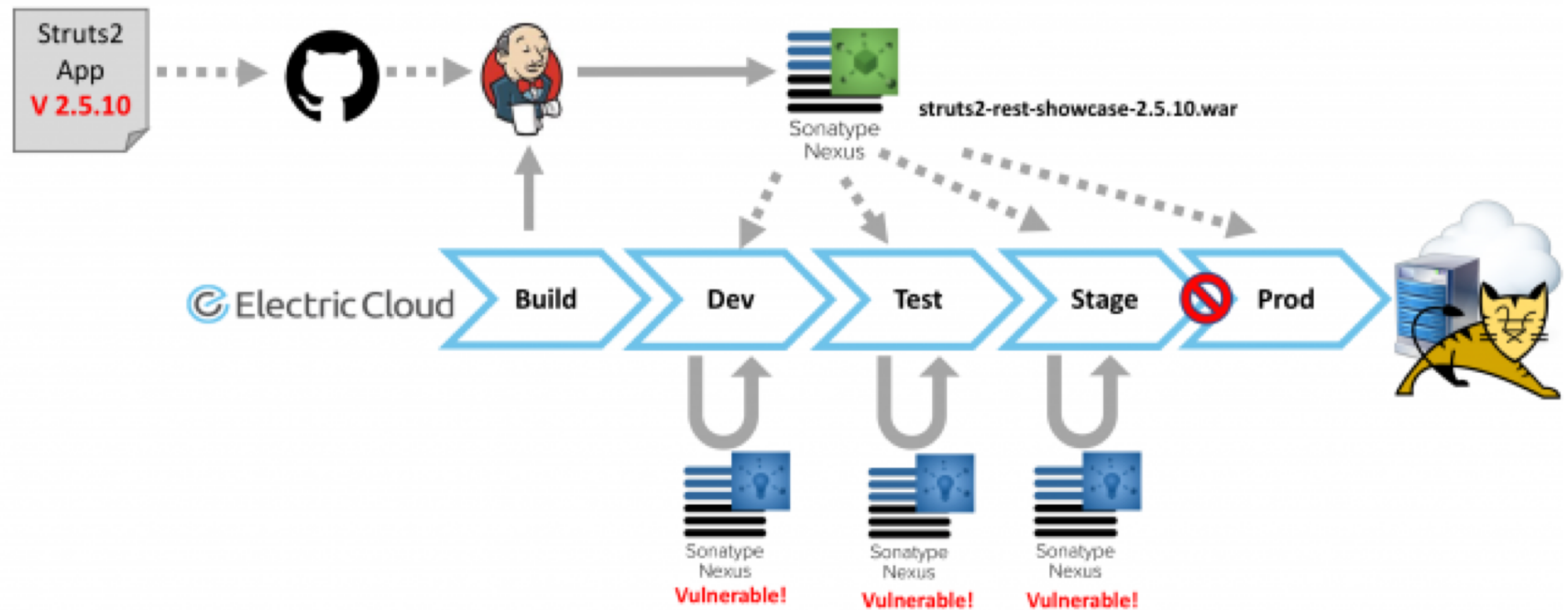
DevSecOps according to Shannon Lietz and Intuit



DevSecOps according to Murray Goldschmidt and Sense of Security



DevSecOps according to Hans Ashlock and Electric Cloud



DevSecOps according to John Willis

Software Supply Chain

DevOps Example

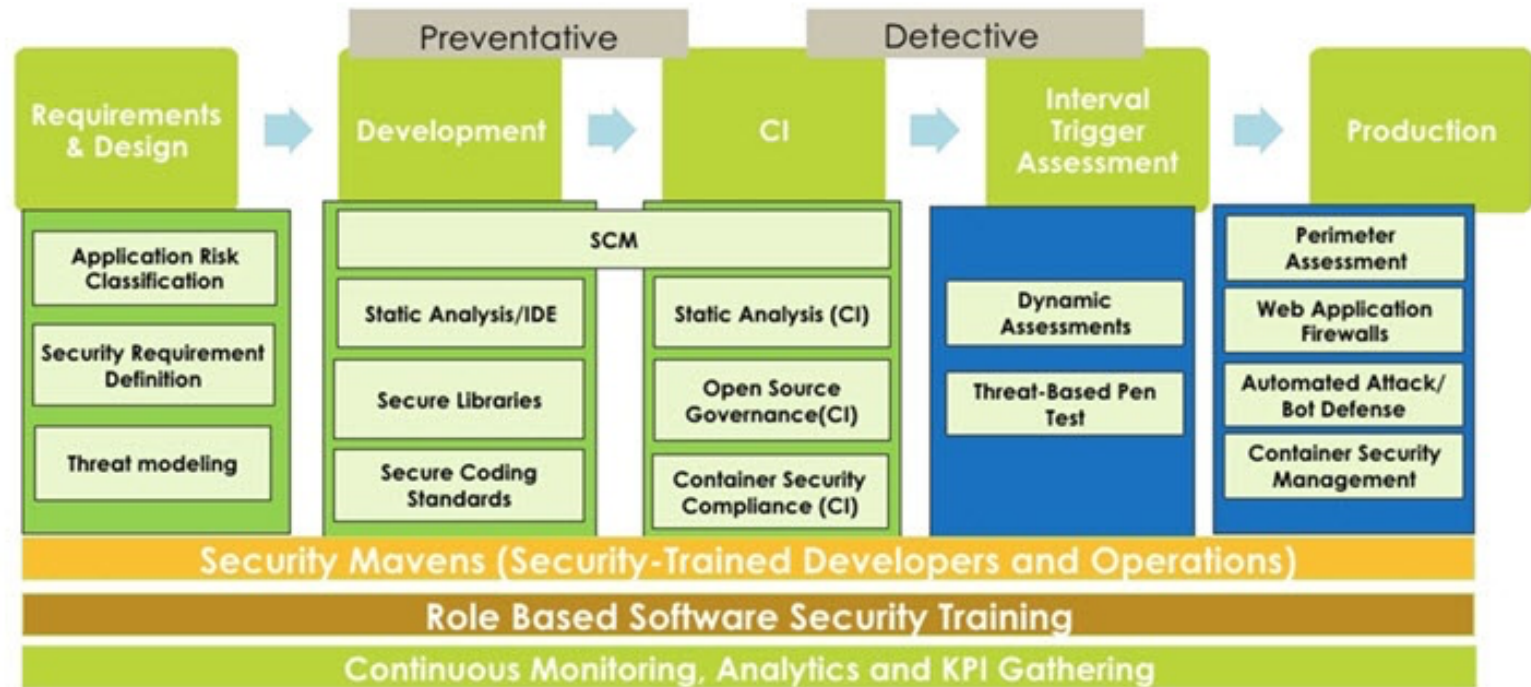


DevSecOps Example

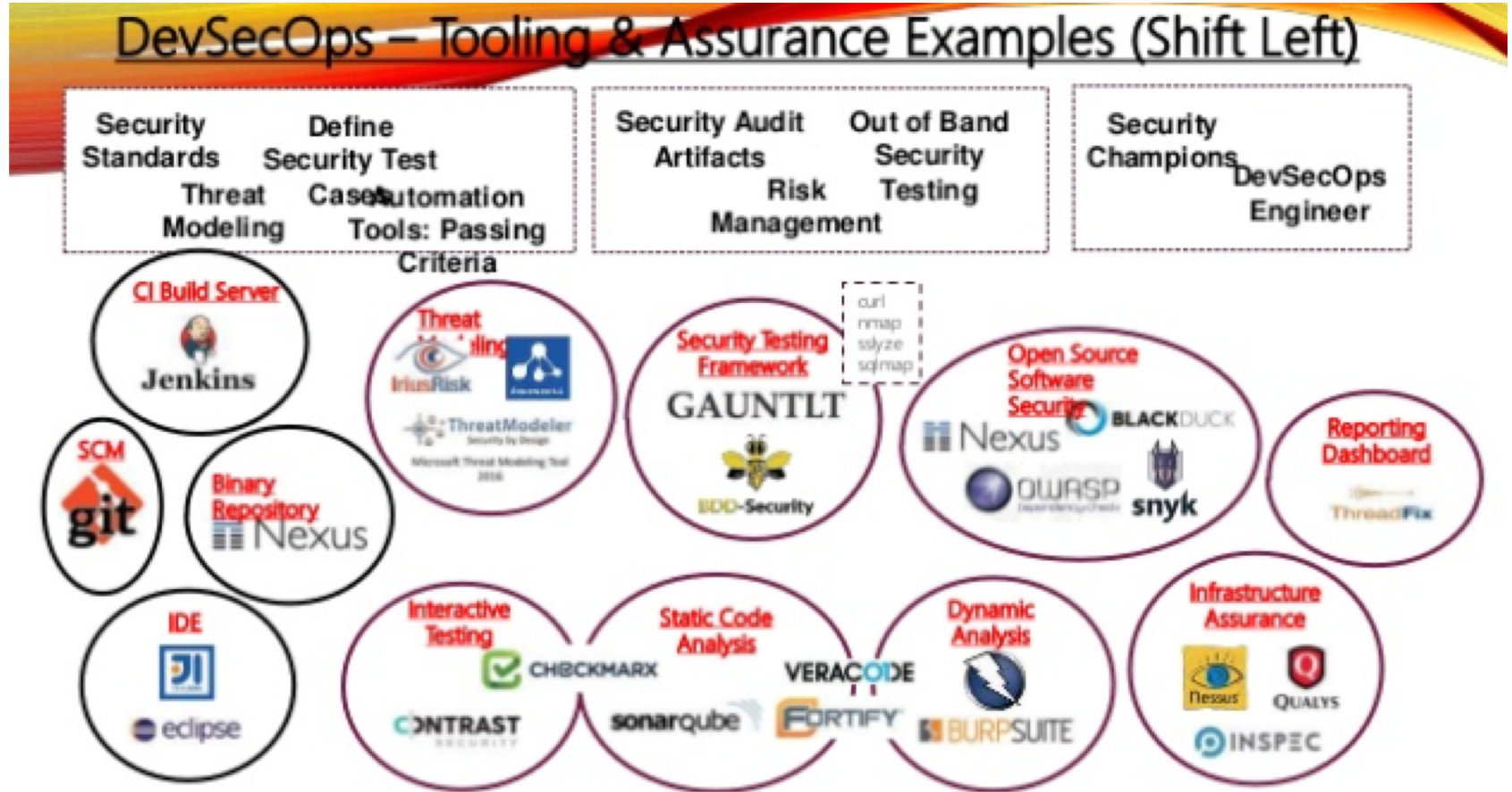


DevSecOps according to John Willis

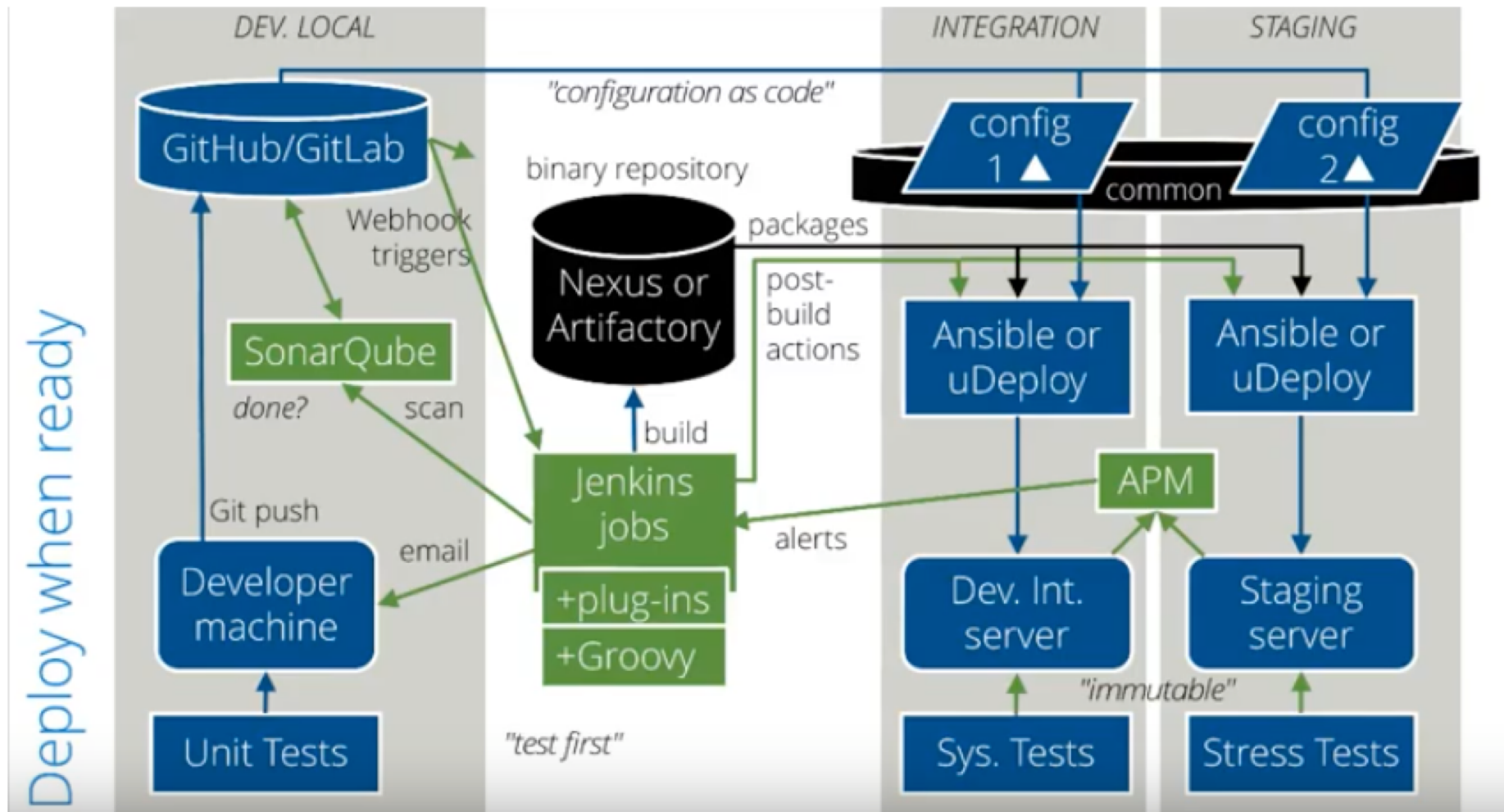
Implementing DevOps in a Regulated Environment



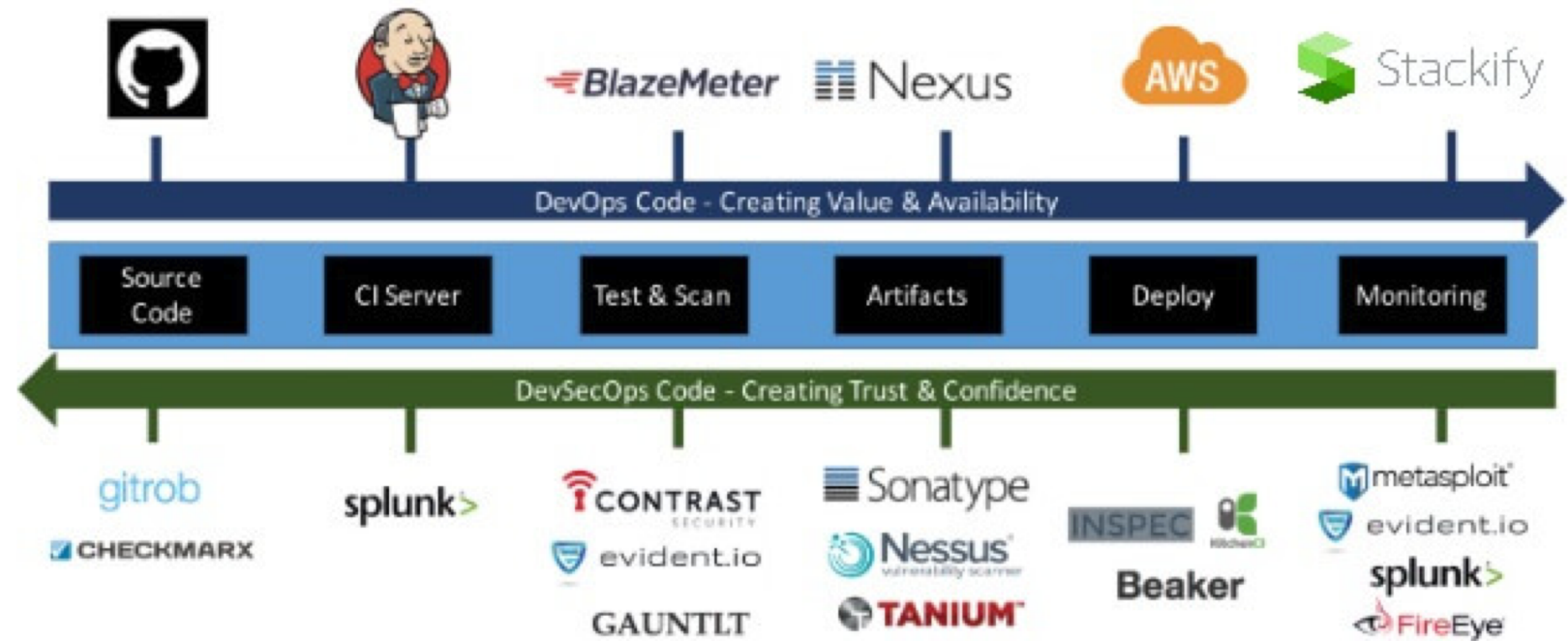
DevSecOps according to Michael Man



DevSecOps according to Wilson Mar and JetBloom



DevSecOps according to Matt Watson and Stackify



Interested in
DevSecOps, but
don't know
where to start?

sonatype Nexus Vulnerability Scanner

Detailed analysis for report: ozone-marketplace-7.17.1.0.zip Try Nexus

Summary Policy Violations Security Issues License Analysis

Filter: All Exact Similar Unknown Violations: Summary All

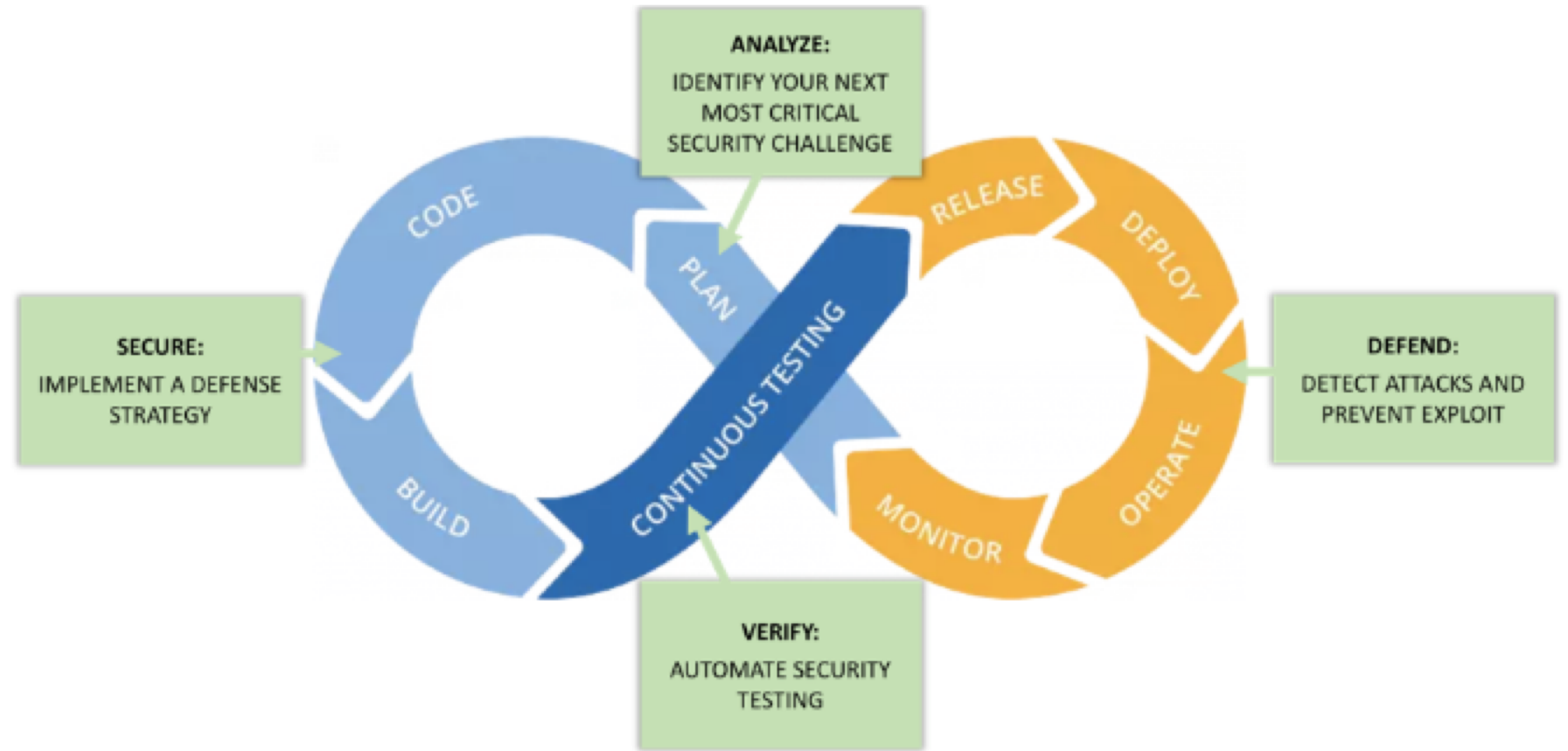
Policy Threat	Component	Pop...	Age	Release History
License-None	javax.el : el-api : 2.1.2-b03	●	10.0 y	
	org.glassfish.web : el-impl : 2.1.2-b03	●	10.0 y	
Security-High	ch.qos.logback : logback-classic : 1.1.11	●	2.1 y	
	com.fastenml:jackson.core : jackson-databind : 2.8.10	●	1.8 y	
	commons-beanutils : commons-beanutils : 1.9.3	●	2.5 y	
	dom4j : dom4j : 1.6.1	●	13.6 y	
	net.sf.ehcache : ehcache : 2.10.4	●	1.9 y	
	org.apache.logging.log4j : log4j-core : 2.7	●	2.5 y	
	org.apache.lucene : lucene-queryparser : 6.5.1	●	1.9 y	
	org.apache.tomcat : tomcat-catalina : 8.5.23	●	1.5 y	
	org.apache.tomcat : tomcat-util : 8.5.23	●	1.5 y	
	org.apache.tomcat : tomcat-websocket : 8.5.23	●	1.5 y	
	org.hibernate : hibernate-validator : 5.3.5.Final	●	2.0 y	
	org.jgroups : jgroups : 2.10.0.GA	●	8.7 y	
	org.postgresql : postgresql : 42.1.4.jre7	●	1.6 y	
	org.springframework : spring-core : 4.3.12.RELEASE	●	1.4 y	
	org.springframework : spring-expression : 4.3.12.RELEASE	●	1.4 y	
	xerces : xercesImpl : 2.11.0	●	6.1 y	
License-Copyleft	jquery-form 3.50.0	●	4.8 y	
	org.yaml : snakeyaml : 1.17	●	3.1 y	
Security-Medium	com.google.guava : guava : 23.6-jre	●	1.2 y	
	com.h2database : h2 : 1.4.196	●	1.8 y	
	commons-fileupload : commons-fileupload : 1.3.3	●	1.8 y	
	jivesoftware : smack : 3.2.1	●	7.6 y	
	org.apache.tomcat : tomcat-coyote : 8.5.23	●	1.5 y	
	org.elasticsearch : elasticsearch : 5.4.3	●	1.7 y	
	org.springframework : spring-web : 4.3.12.RELEASE	●	1.4 y	
	org.springframework : spring-webmvc : 4.3.12.RELEASE	●	1.4 y	

Showing all 267 rows

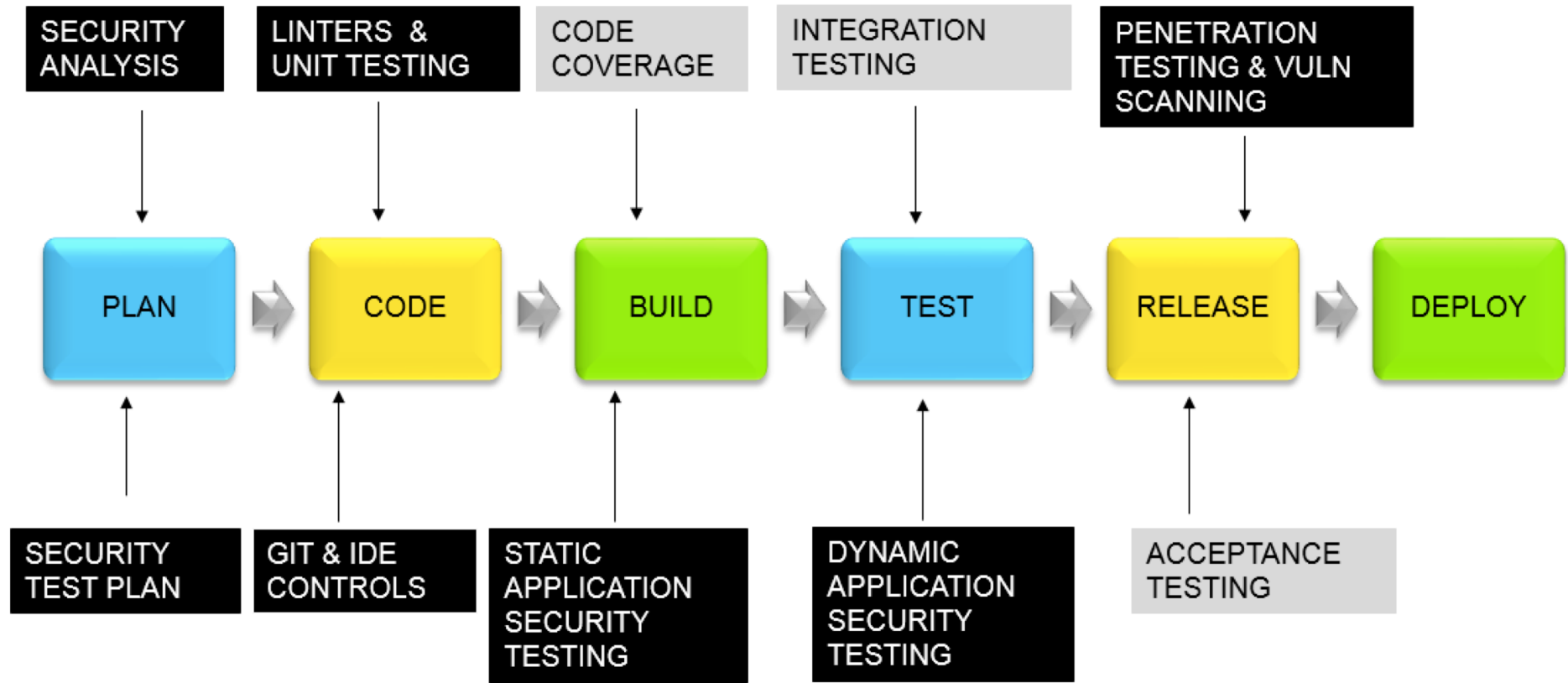
Try [Nexus Vulnerability Scanner](#):

1. Confidently and quickly analyze your open source and third party components
2. Create a precise “Bill of Materials” to identify which open source components are used and where.
3. Discover all component dependencies and known vulnerabilities or license risks.

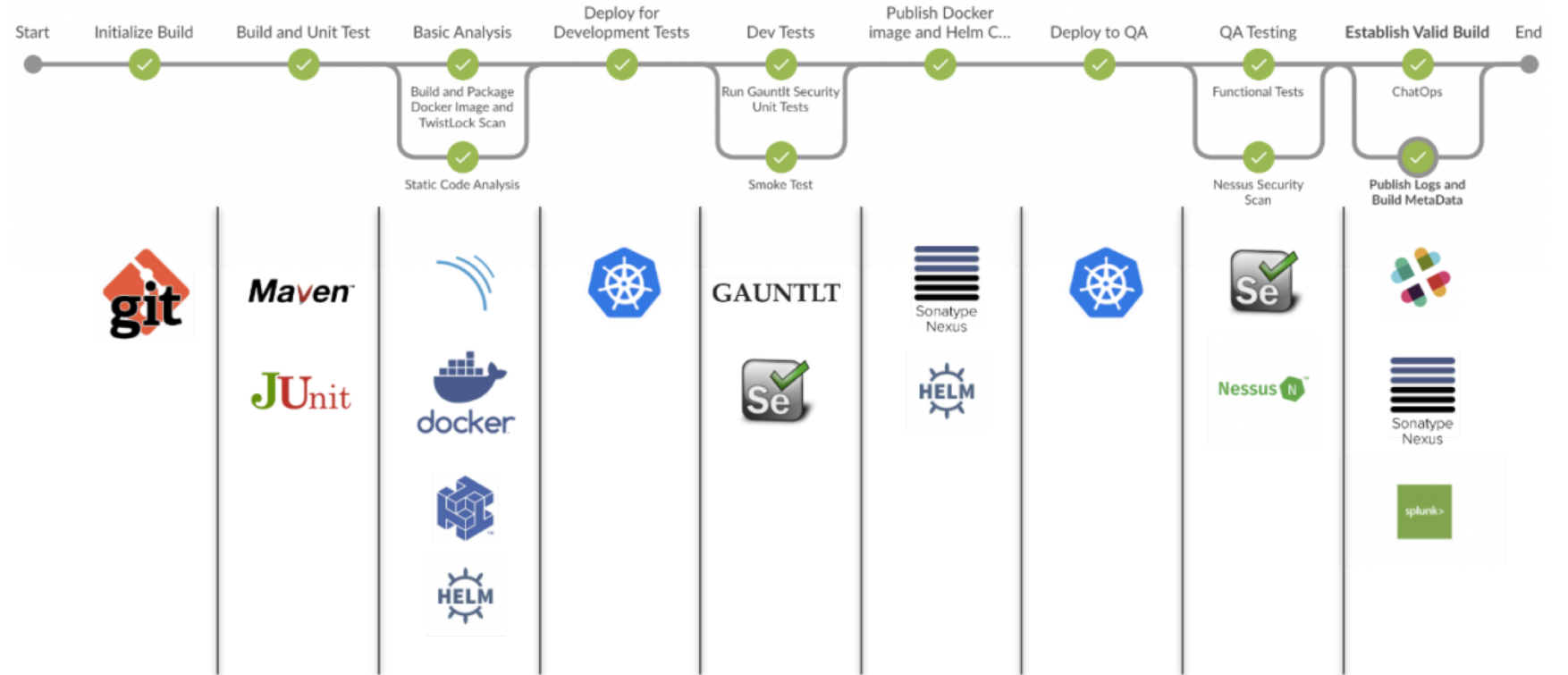
DevSecOps according to Jeff Williams and Contrast Security



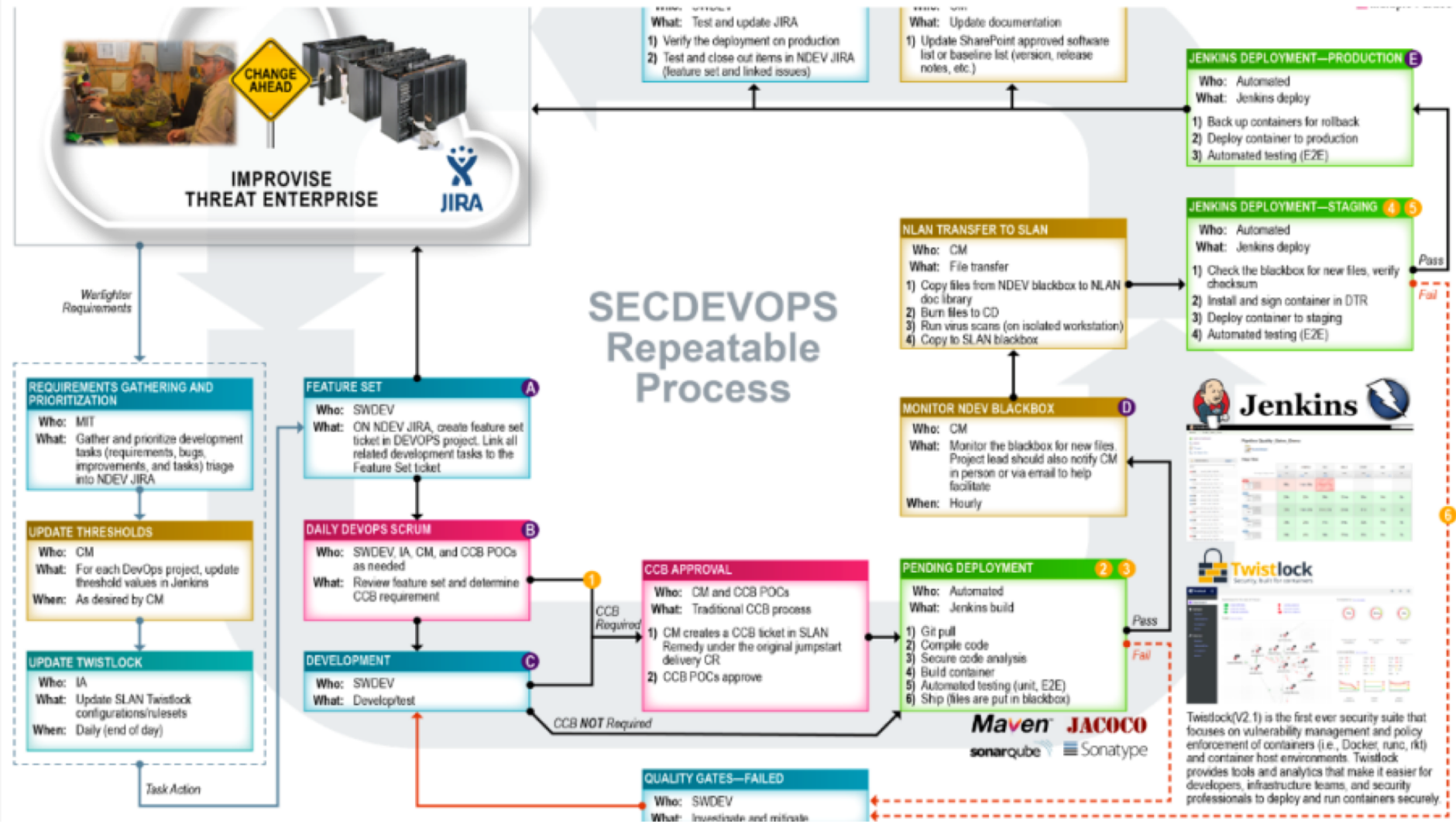
DevSecOps according to Tom Porter and HPE/DXC



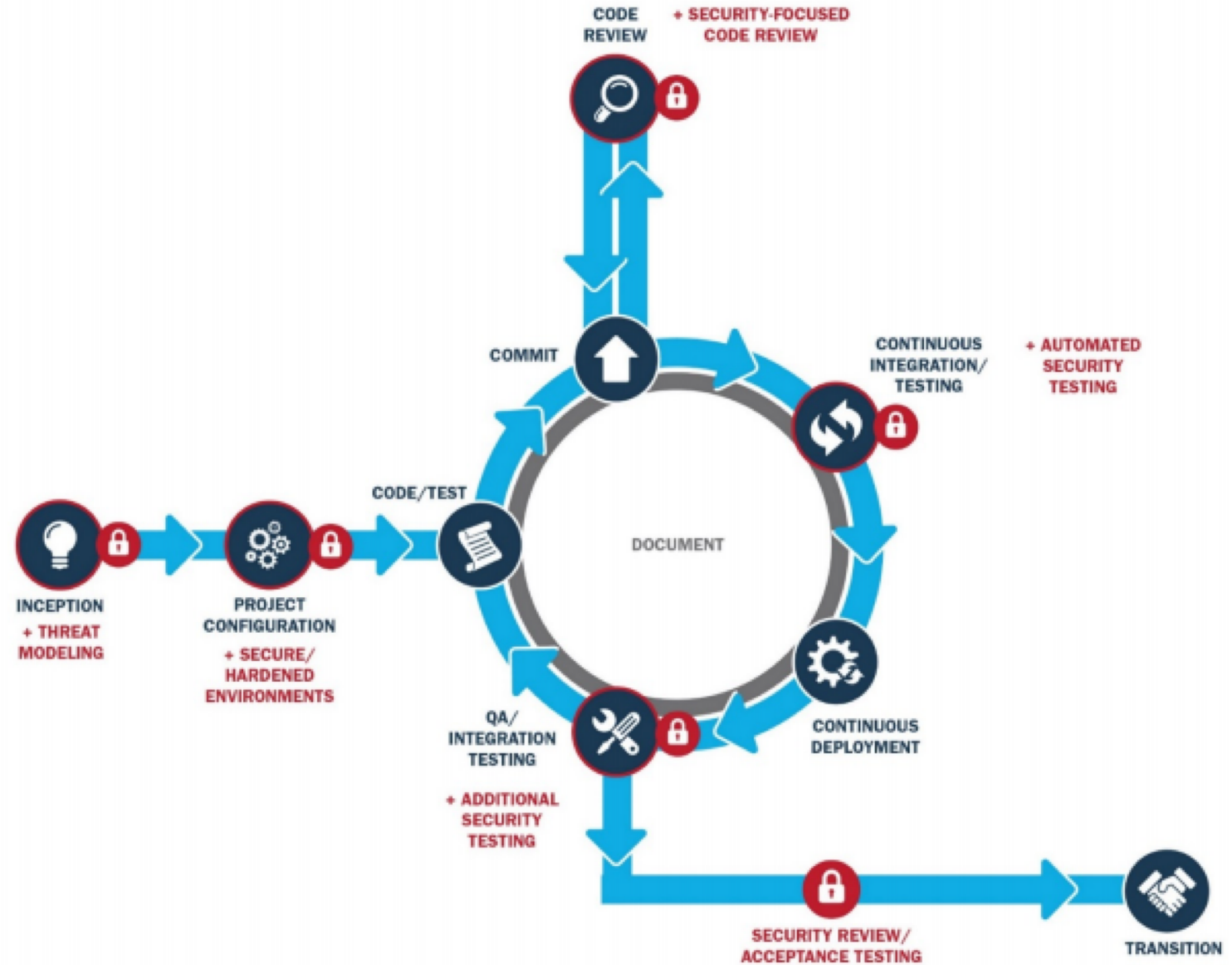
DevSecOps according to Ben Chicoski and CloudBees



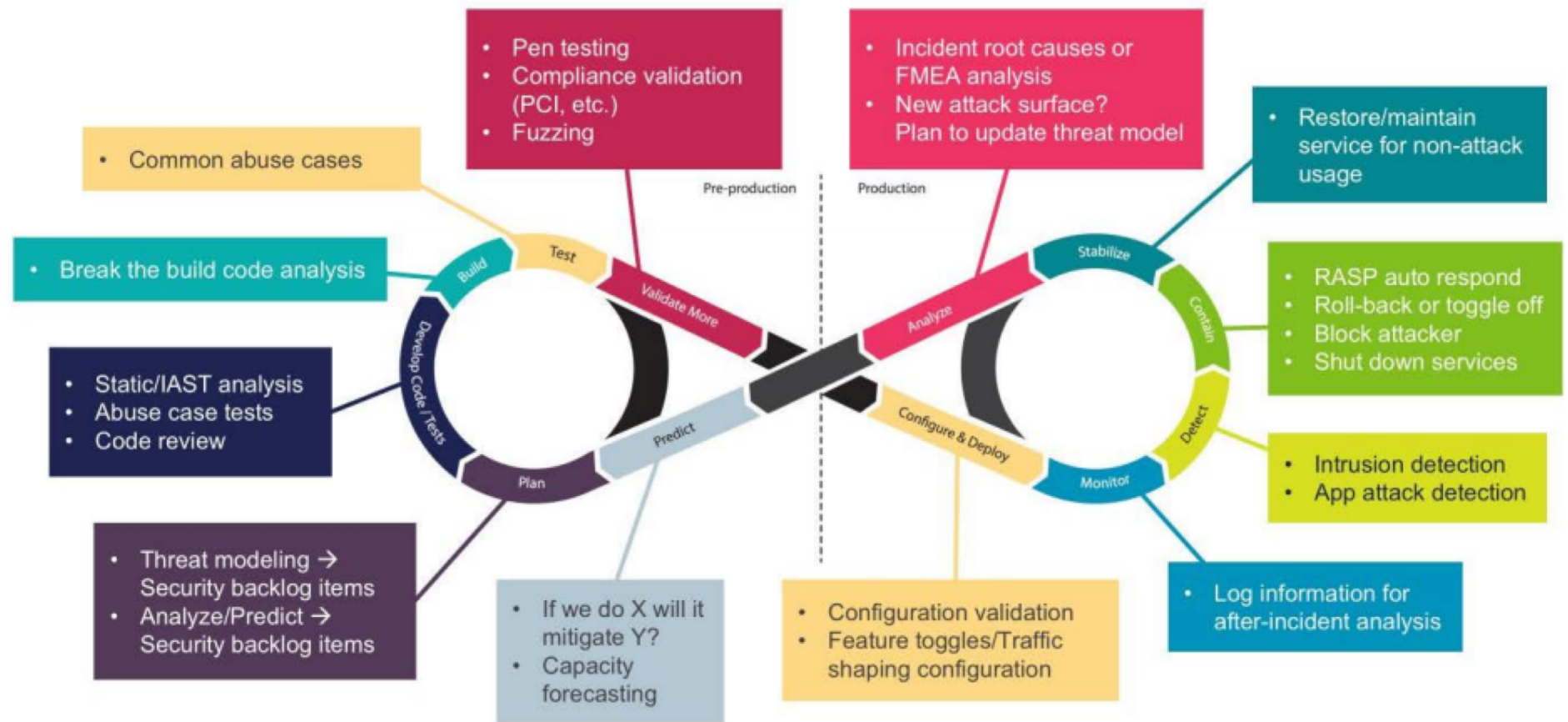
DevSecOps according to Leonel Garciga and U.S. Dept of Defense/JIDO



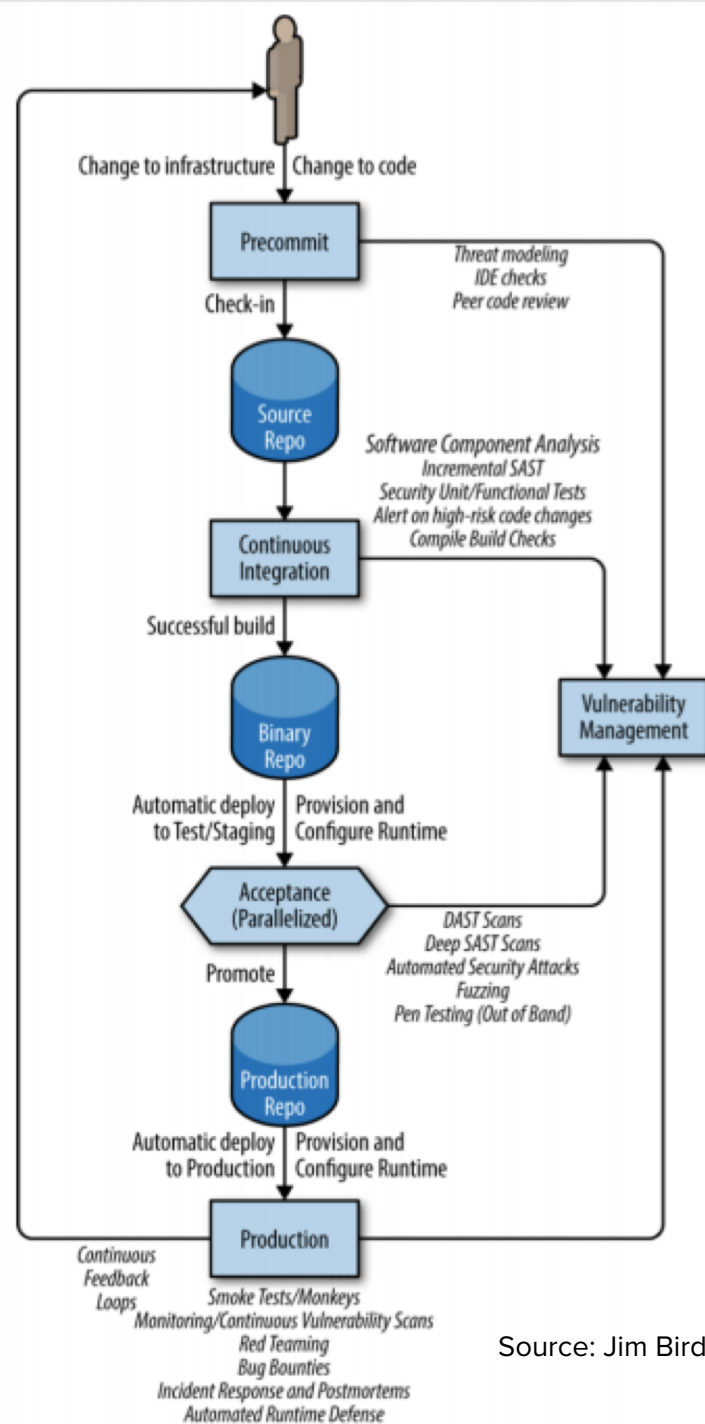
DevSecOps according to Hasan Yasar and Carnegie Mellon SEI



DevSecOps according to Larry Maccherone and Comcast

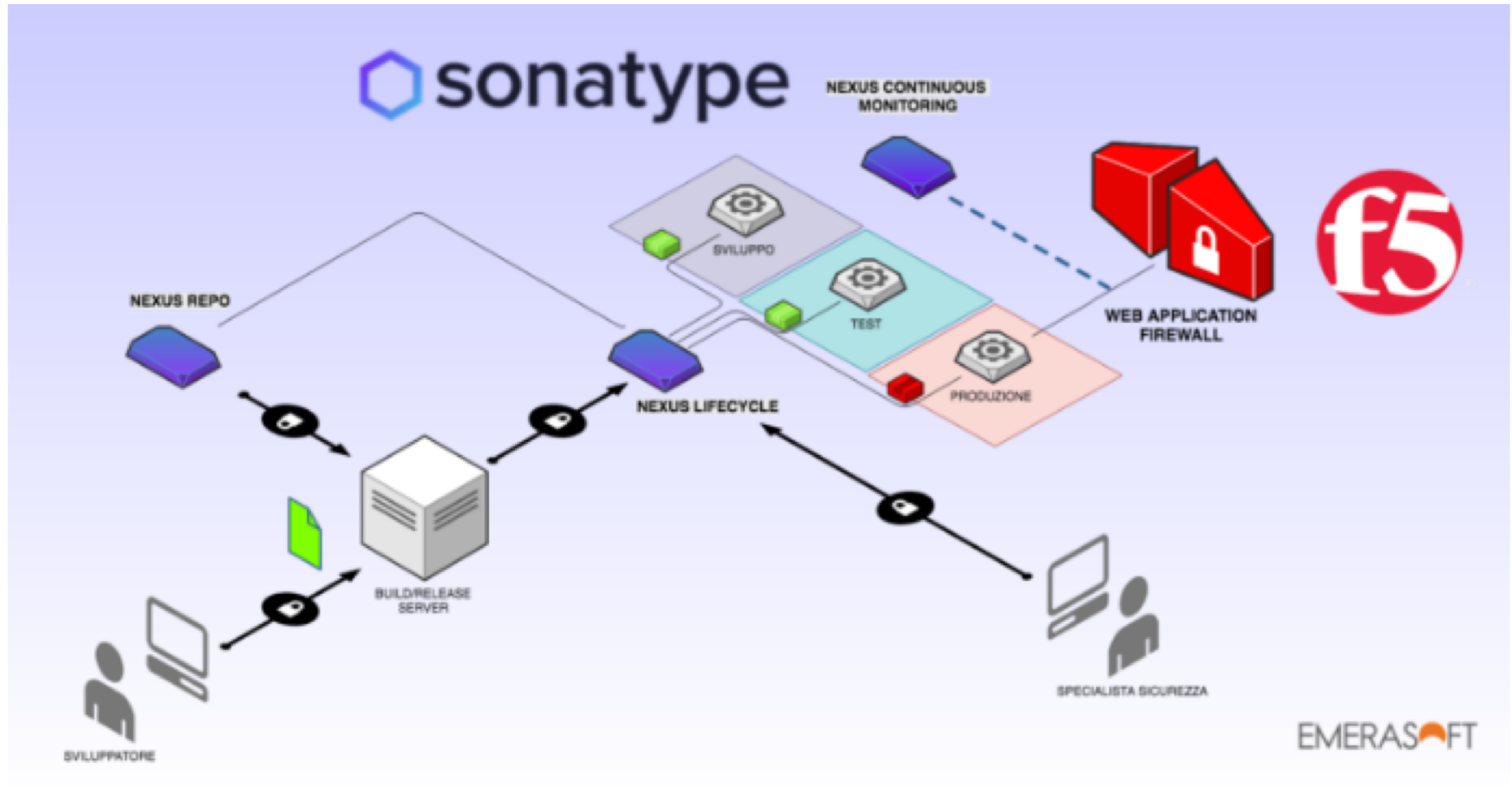


DevSecOps according to Jim Bird

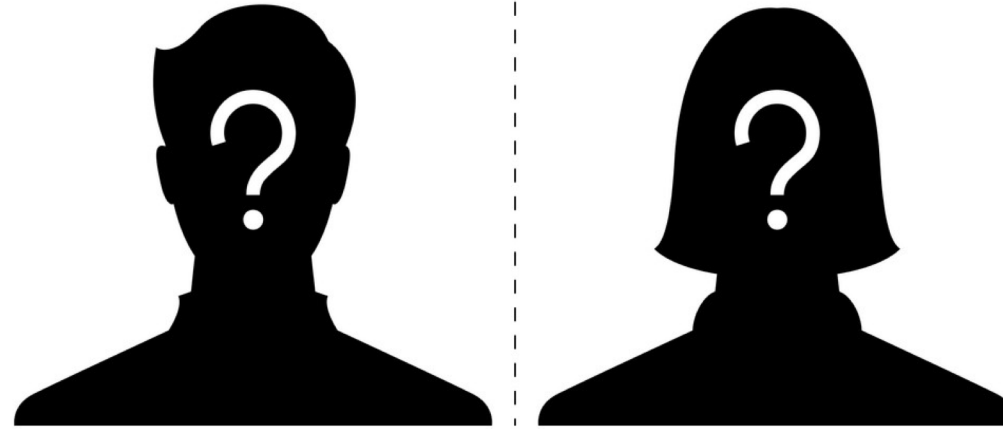


Source: Jim Bird, O'Reilly – [“DevOps Sec: Securing Software Through Continuous Delivery”](#)

DevSecOps according to Ugo Cirací and Emerasoft



DevSecOps according to YOU



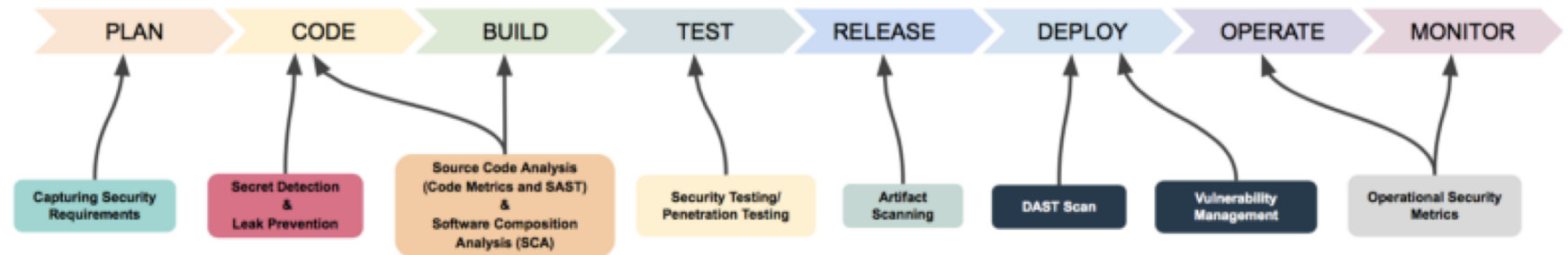
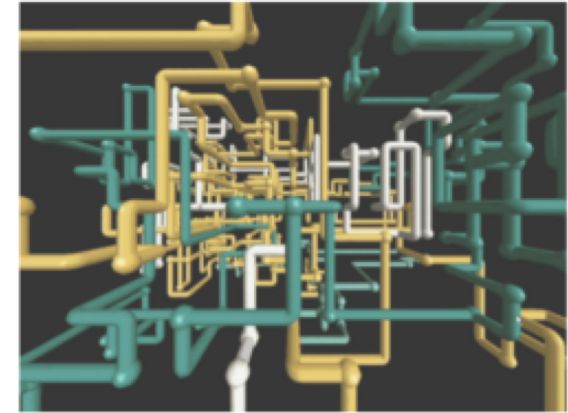
Want your DevSecOps Reference Architecture to this deck?

1. Send it to community@sonatype.com with the subject line: DevSecOps Reference Architecture (or DM us on Twitter [@Sonatype](https://twitter.com/Sonatype))
2. Provide a link as to where people can find more info about it (e.g., blog, video, SlideShare)
3. We'll add it to this deck with full attribution to you

It's that easy; we all learn with help from the community. Thank you in advance for your contributions!

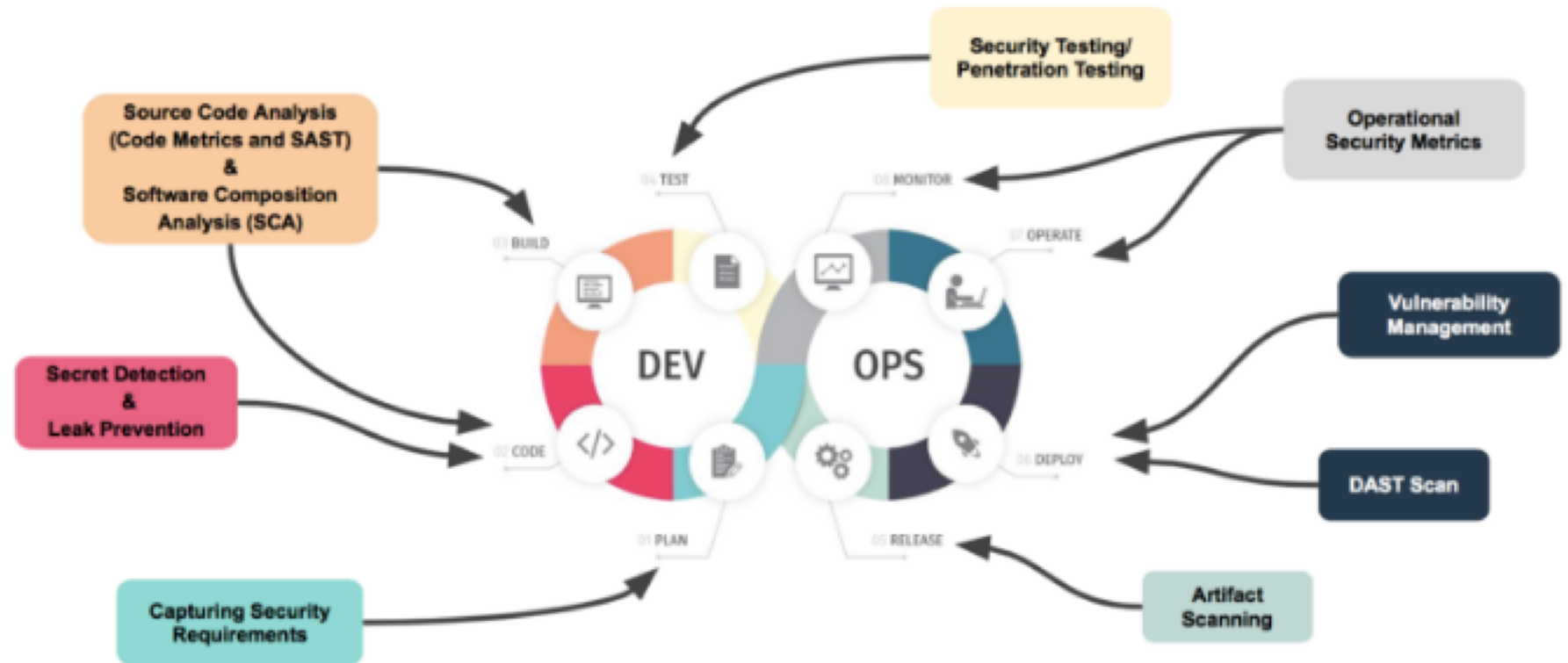
DevSecOps according to PS&C Group

CI/CD Pipeline

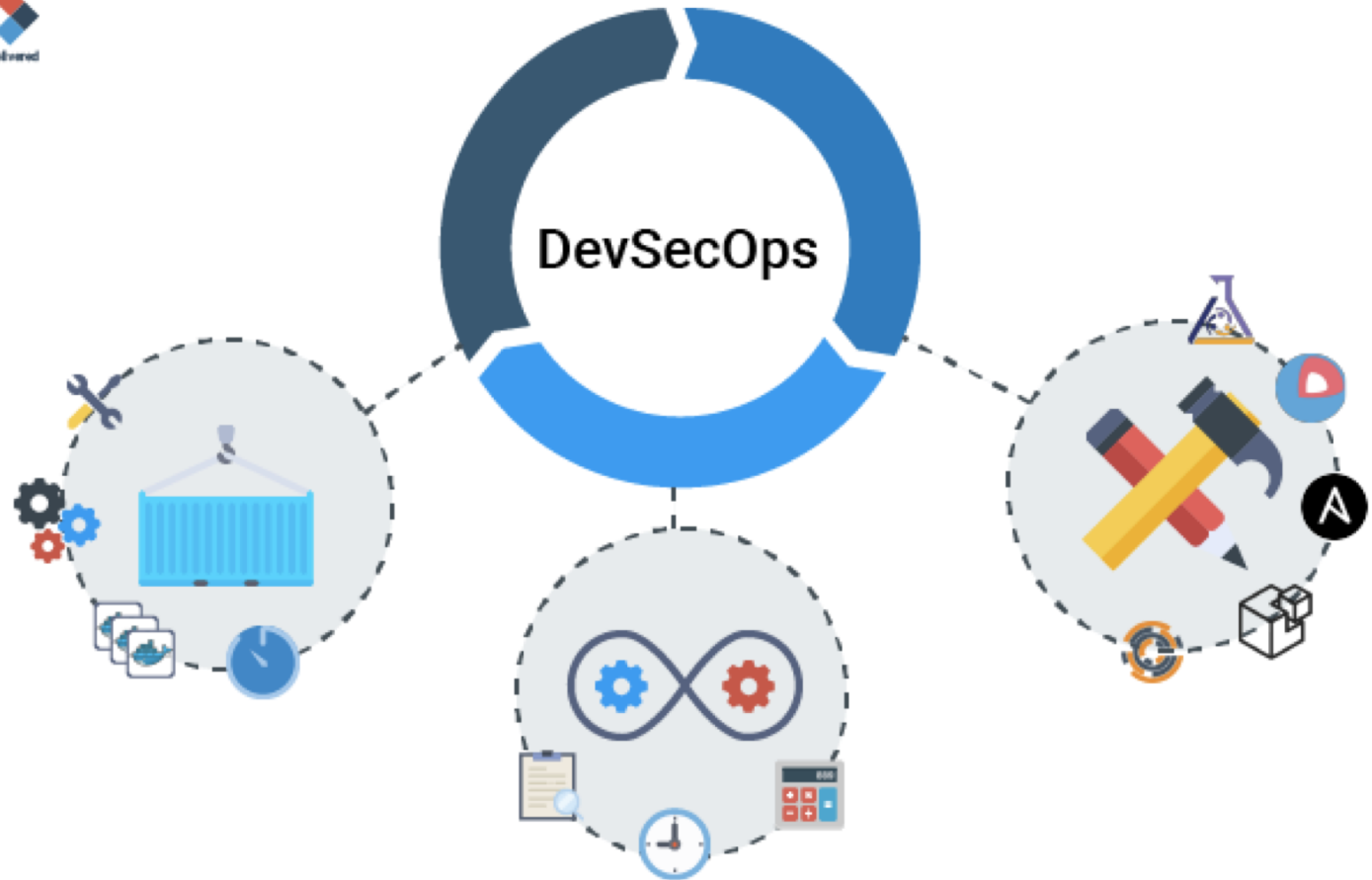


DevSecOps according to PS&C Group

Security Hooks

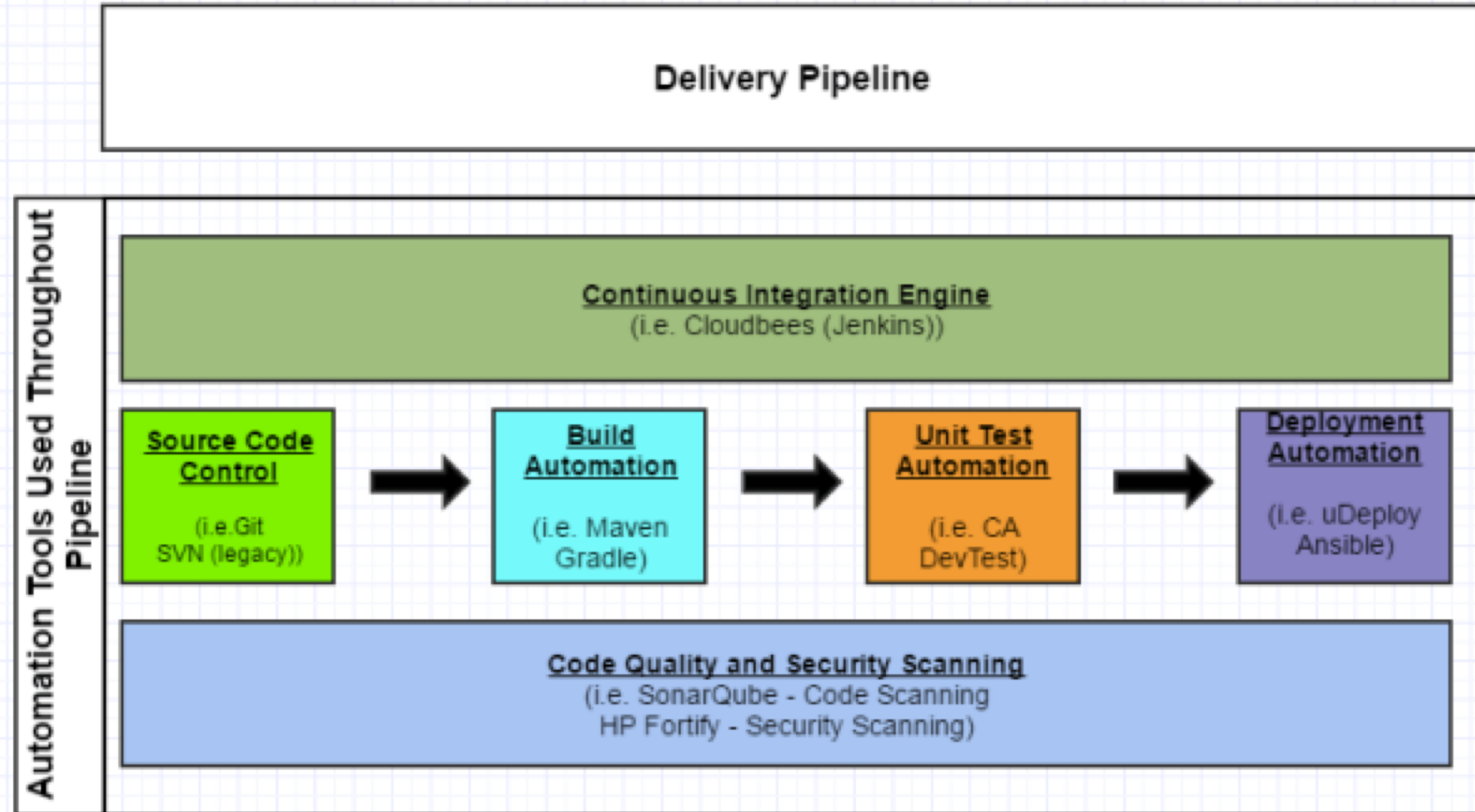


DevSecOps according to Chaitanya Jawale and Opcito



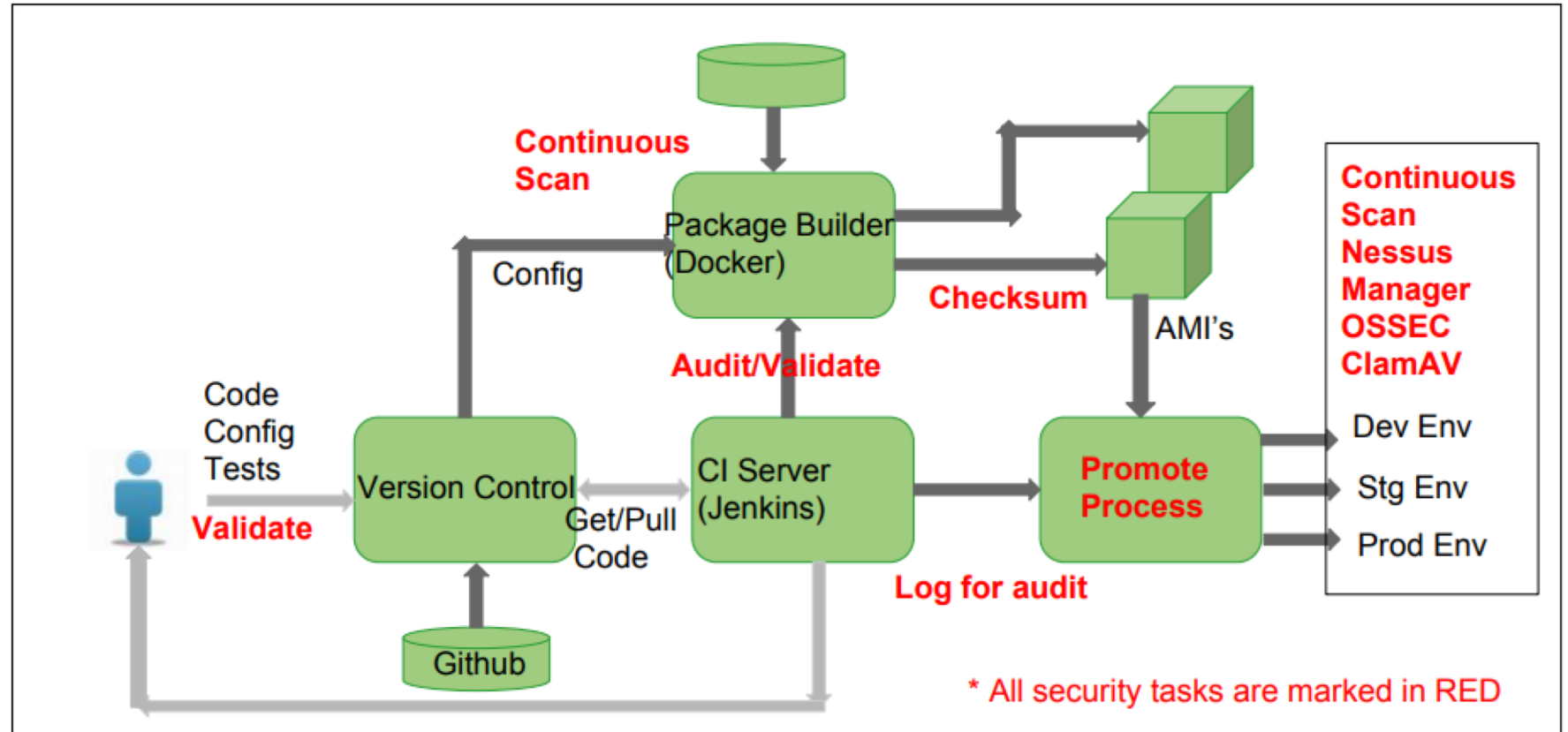
Source: Chaitanya Jawale, Opcito – [“From the CEO’s Desk: DevSecOps – Next Stride for DevOps”](#)

DevSecOps according to Seth Gagnon and Cigna

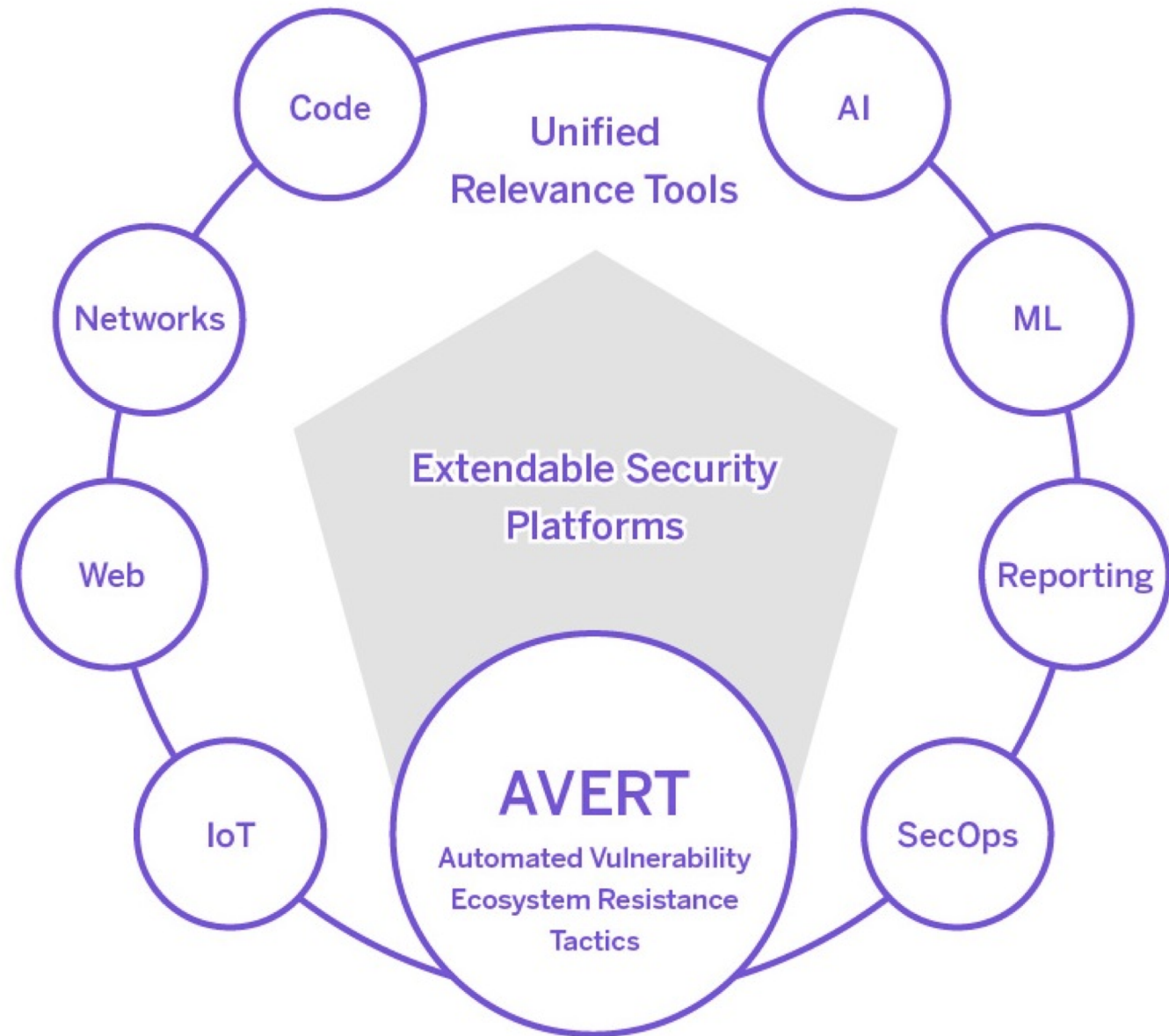


DevSecOps according to GSA

Continuous Integration/Continuous Deployment



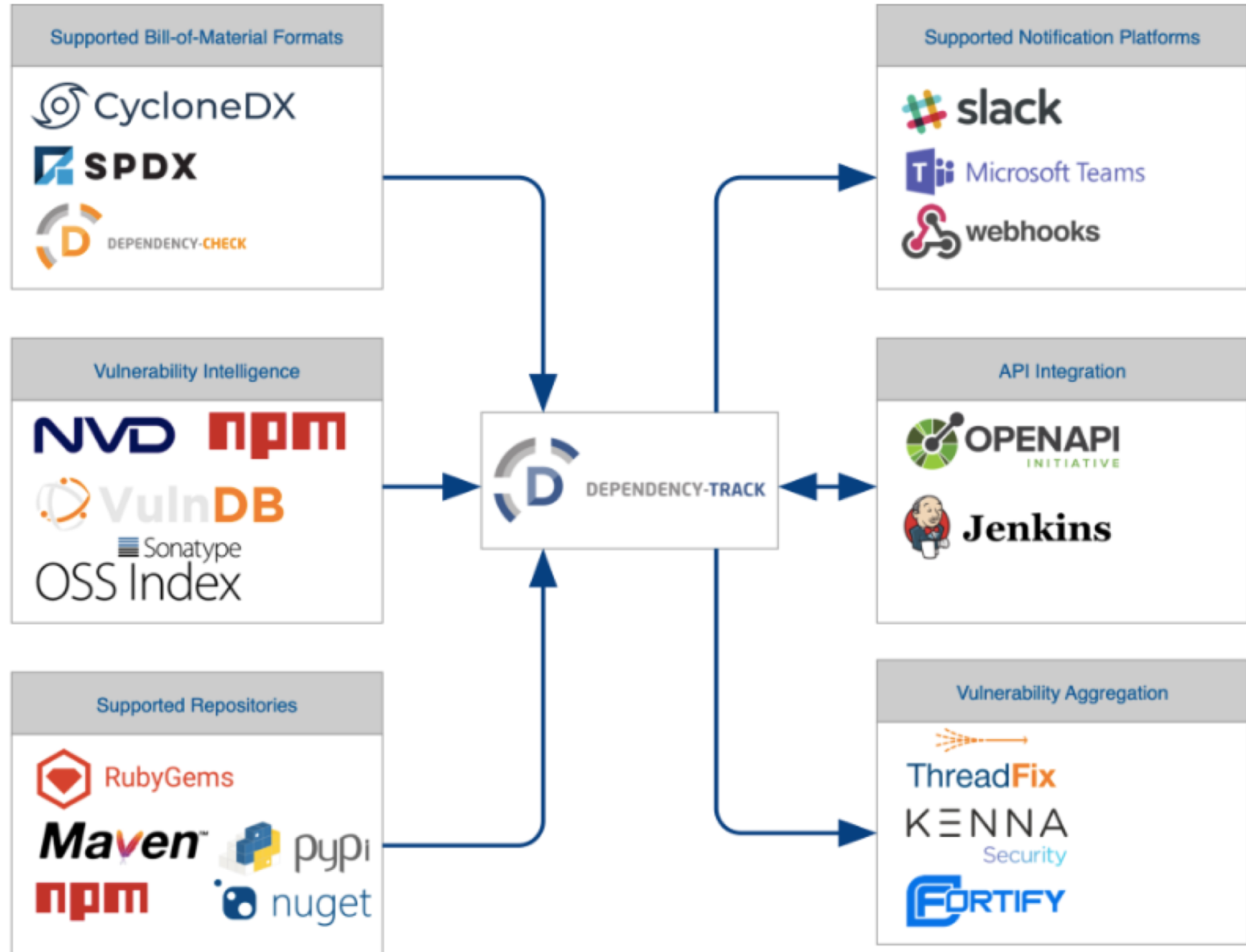
DevSecOps according to Atul Jadhav and Aricent



DevSecOps according to Steve Springett and ServiceNow



Ecosystem Overview



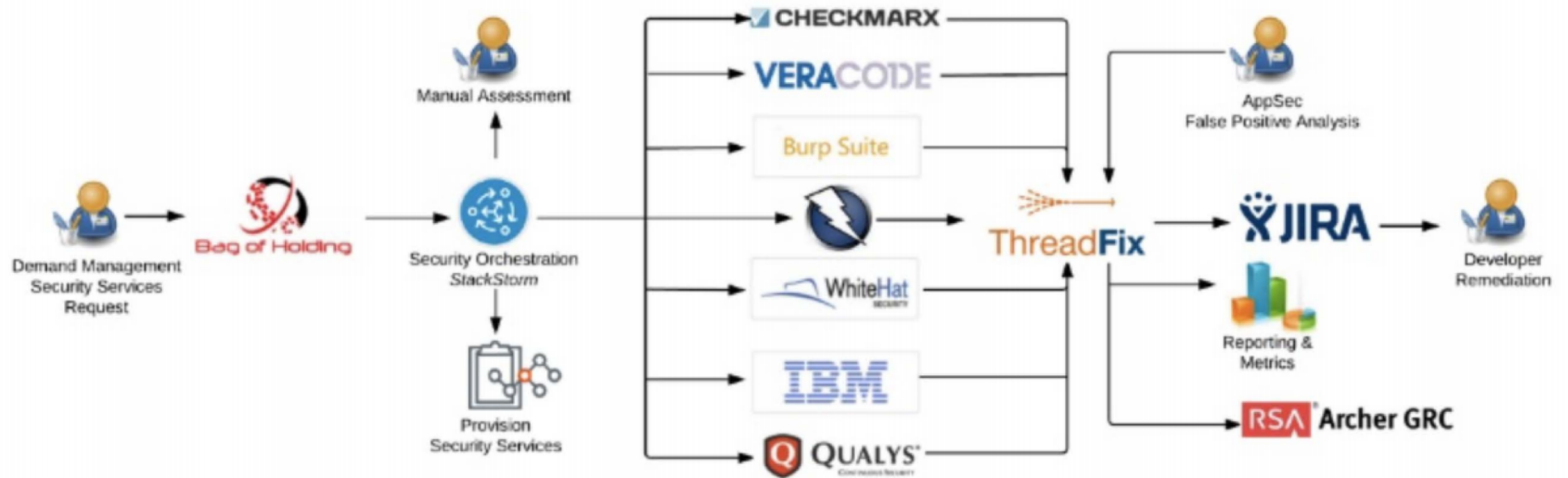
Source: Steve Springett, GitHub – [“Dependency-Track”](#)

27 DevSecOps practitioners from leading enterprises shared their experiences and best practices. Those recordings are all available for **free** at www.alldaydevops.com.

Learn More About DevSecOps From Your Peers



DevSecOps according to Mohammed Imran and TeachEra



DevSecOps according to Alan Crouch and Coveros

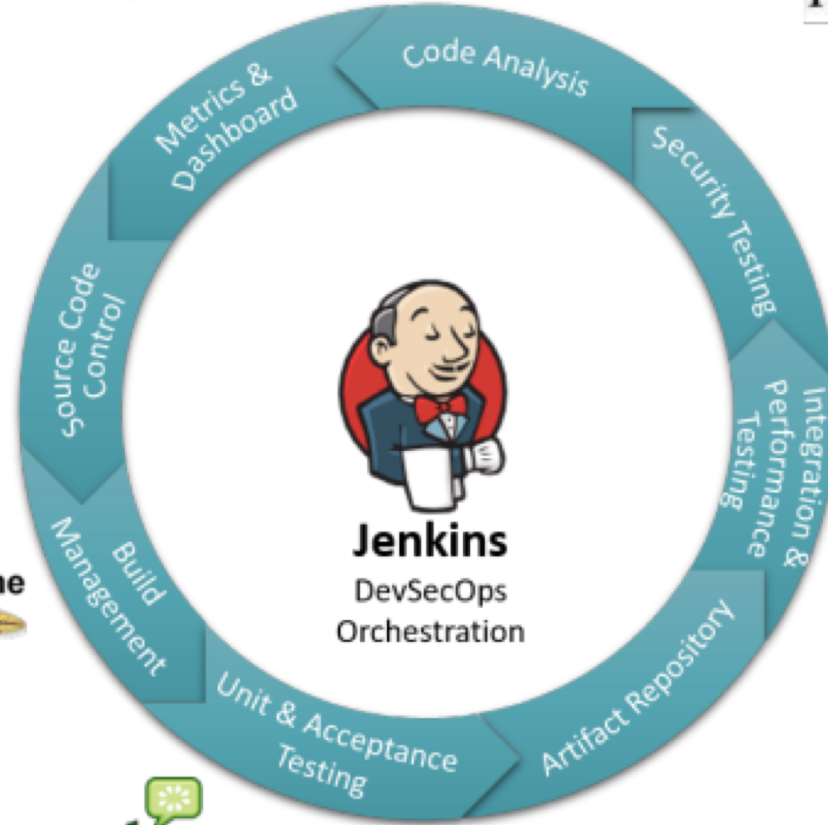
Designed & built on:
 amazon web services™

 sonarqube®

 Yasca

 UNIVERSITY OF MARYLAND FindBugs

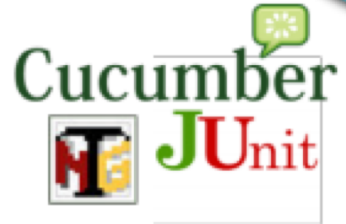

 git 



 OWASP ZAP  DEPENDENCY-CHECK MAVEN  OpenVAS

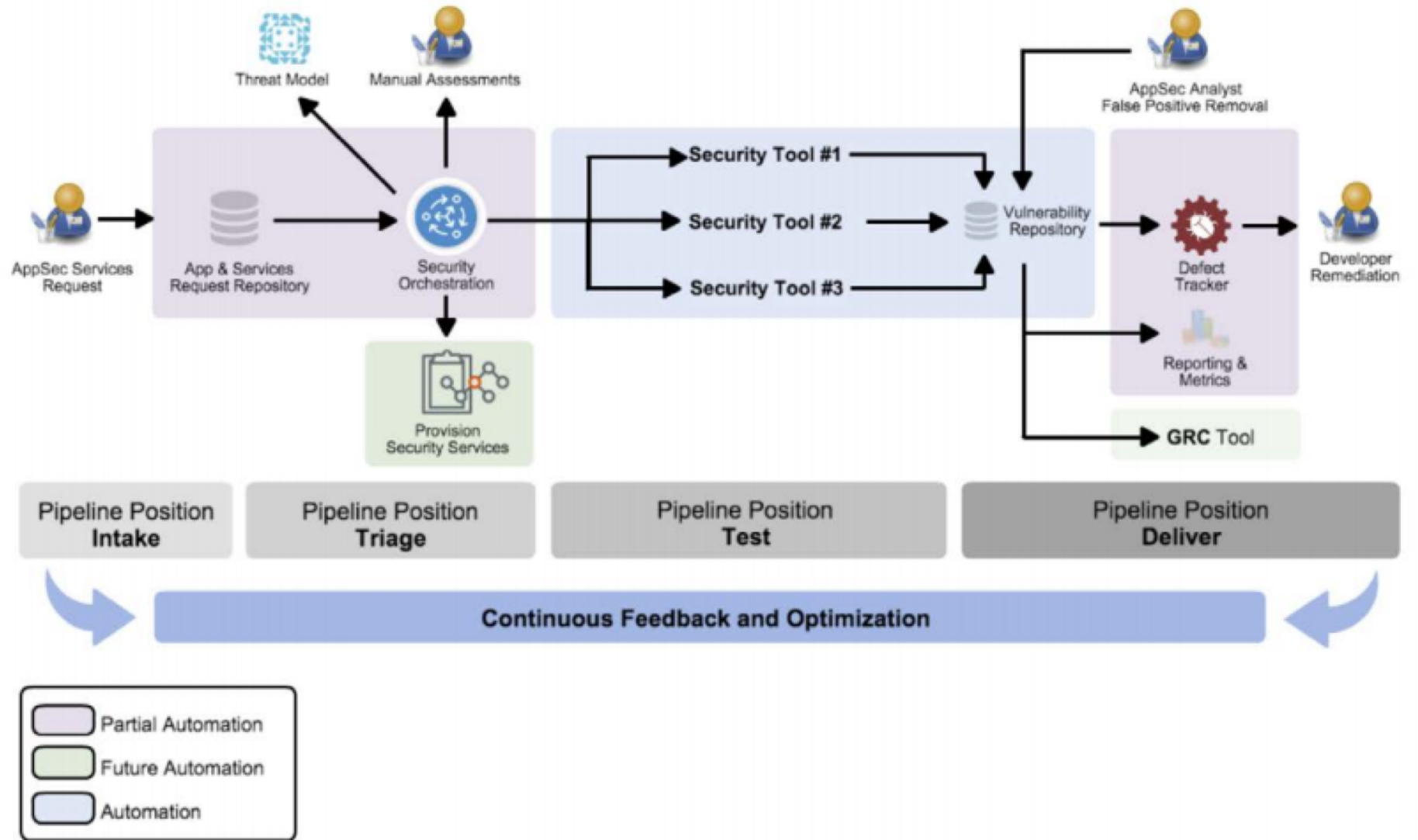
 <APACHE ANT>  Apache maven

 Fitness  Se 

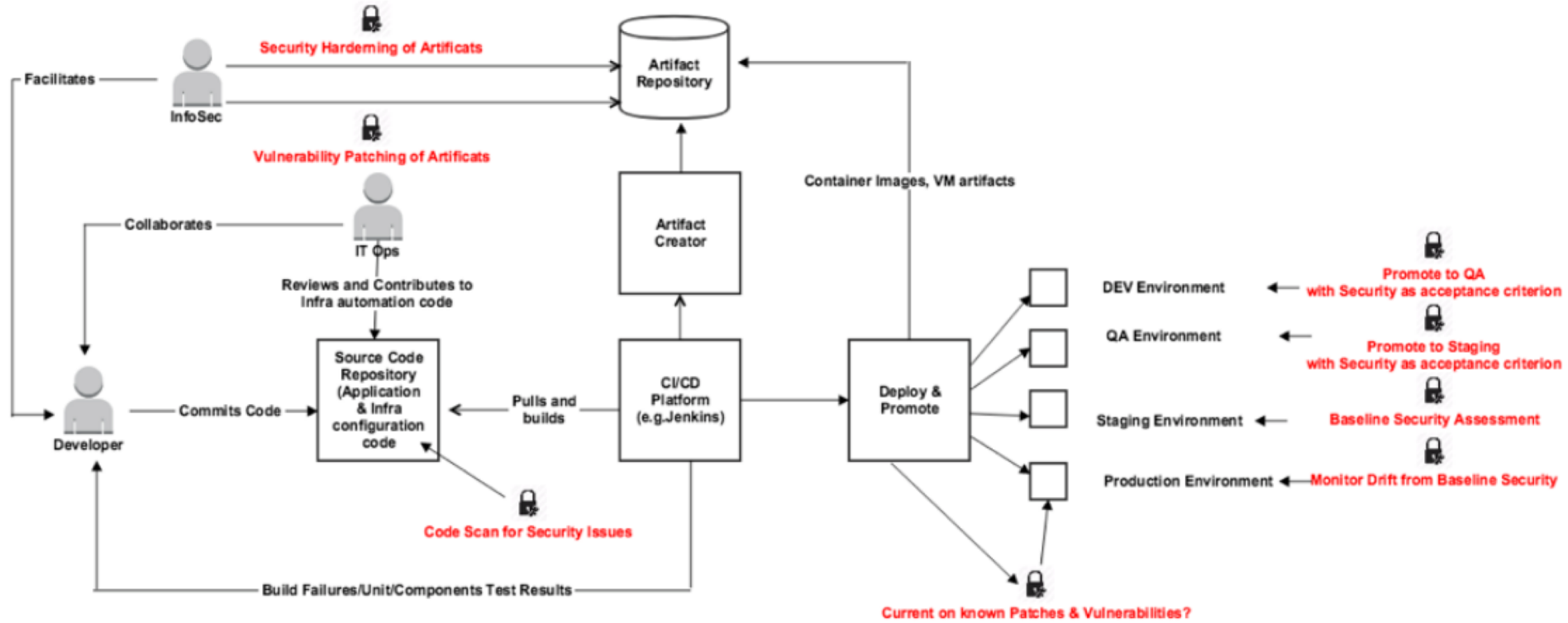
 Cucumber  JUnit

 Nexus

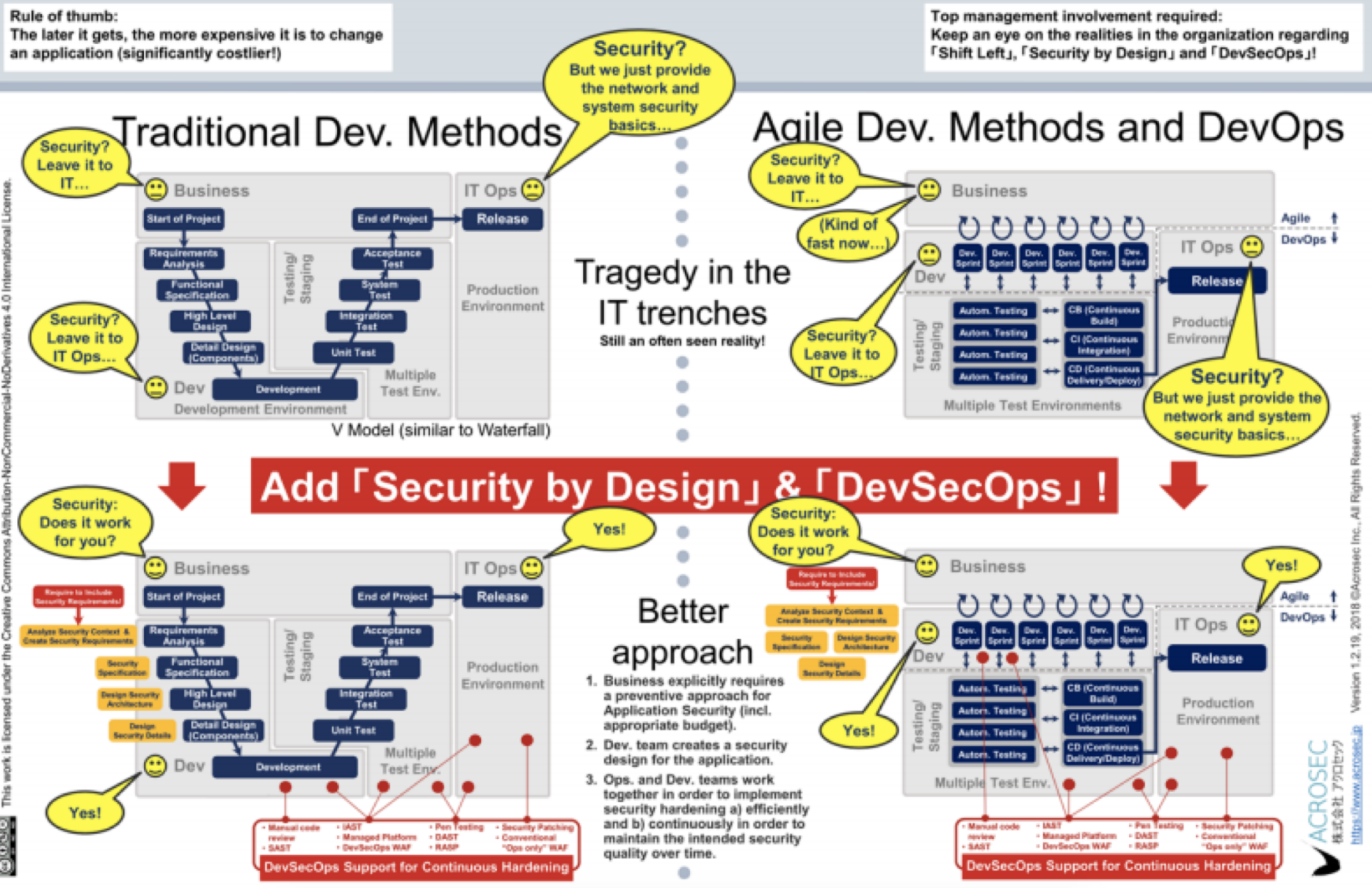
DevSecOps according to Stefan Streichsbier



DevSecOps according to Dr. Ravi Rajamiyer and Cavirin



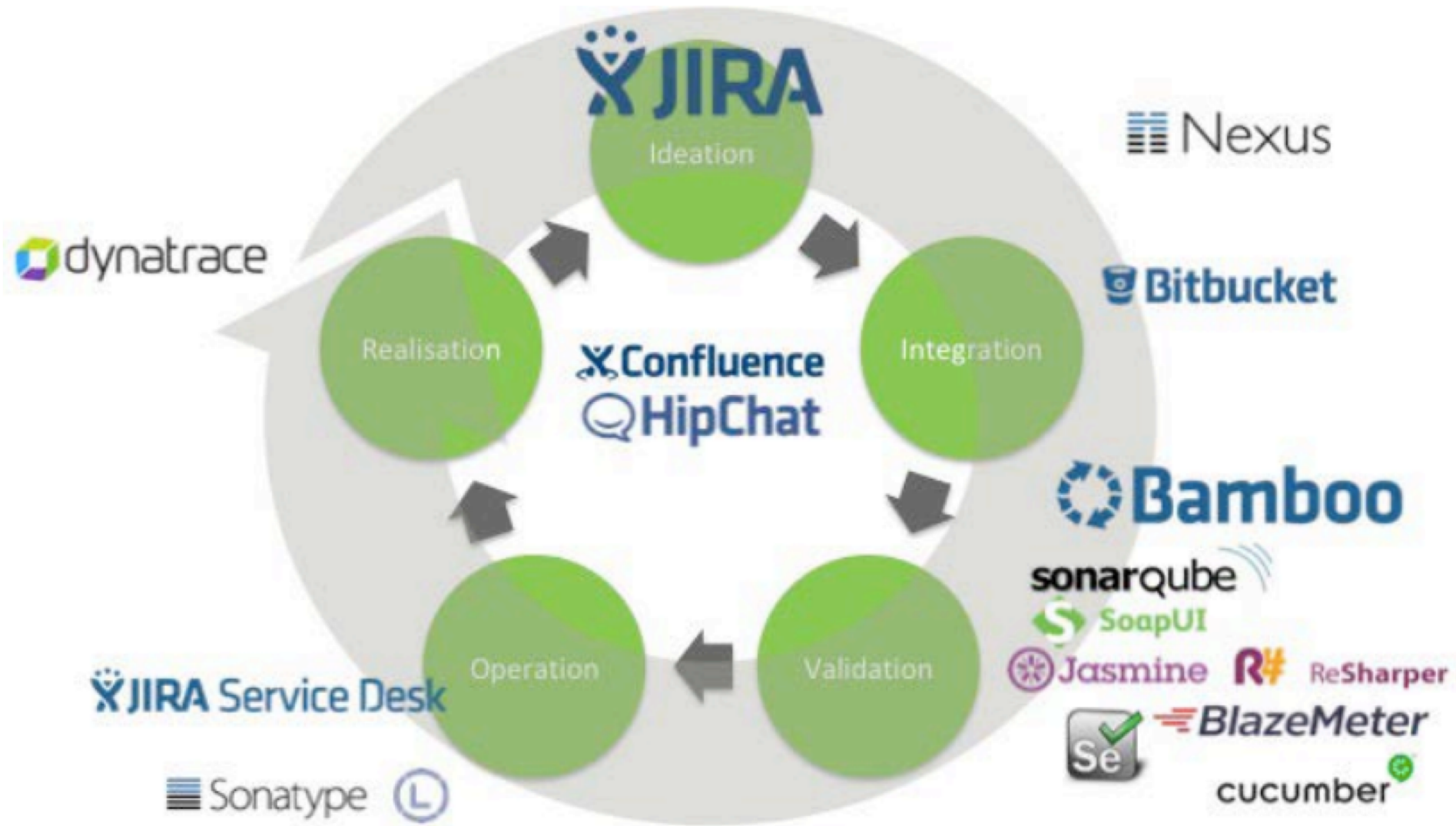
DevSecOps according to ACROSEC



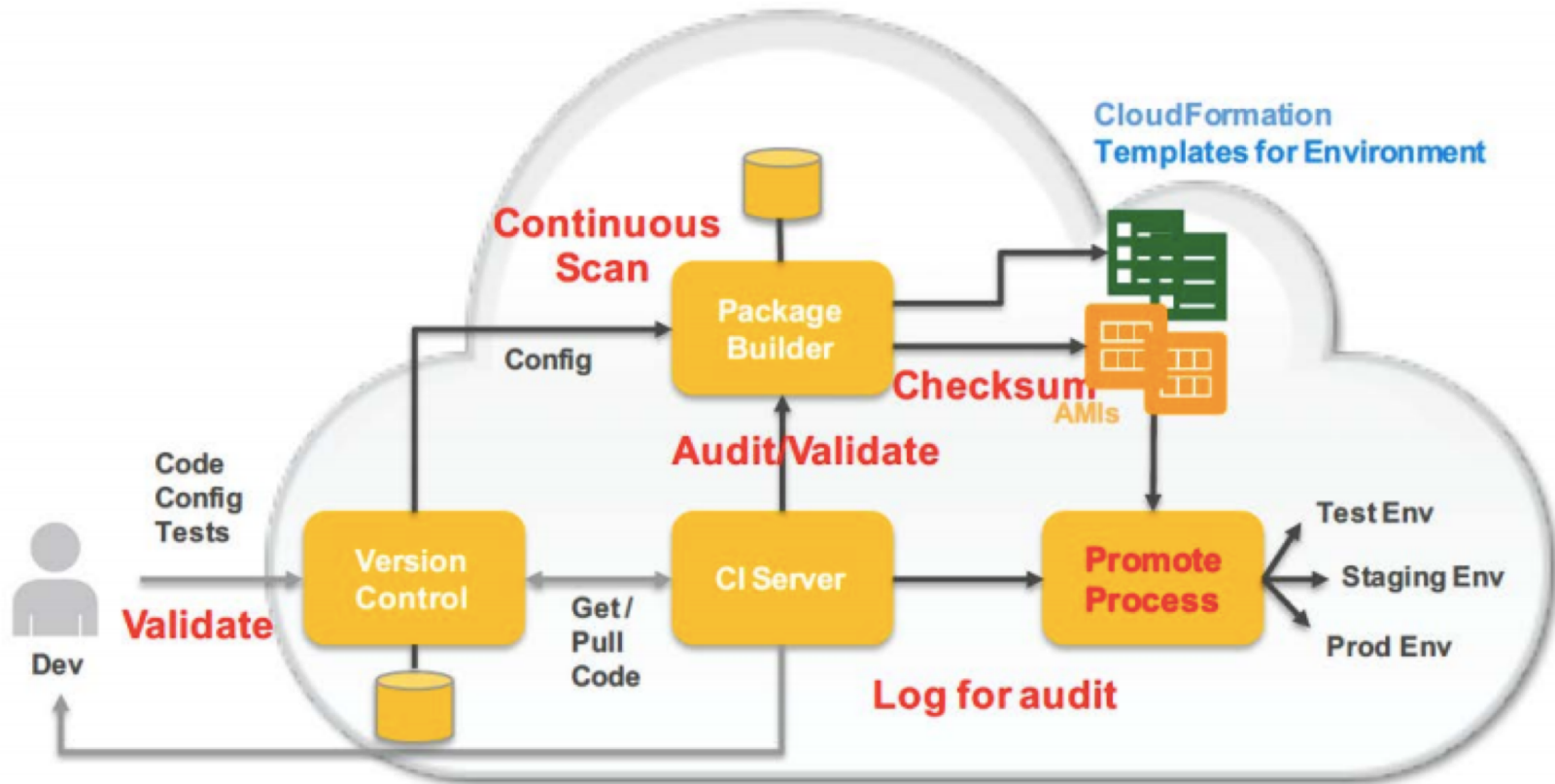
This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Version 1.2-19, 2018 ©Acrosec Inc., All Rights Reserved. ACROSEC 株式会社 アクロセック

DevSecOps according to Helen Beal and Ranger4



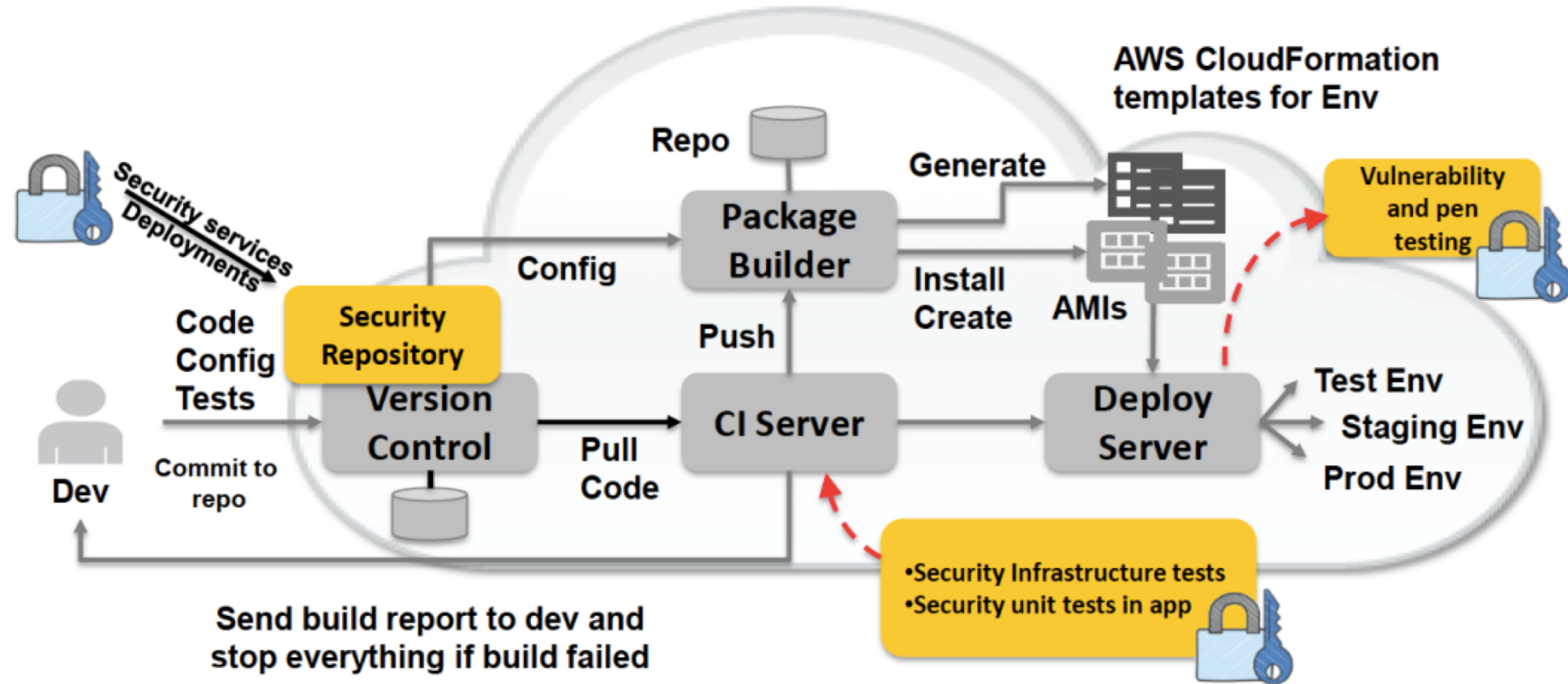
DevSecOps according to Ian Massingham and AWS



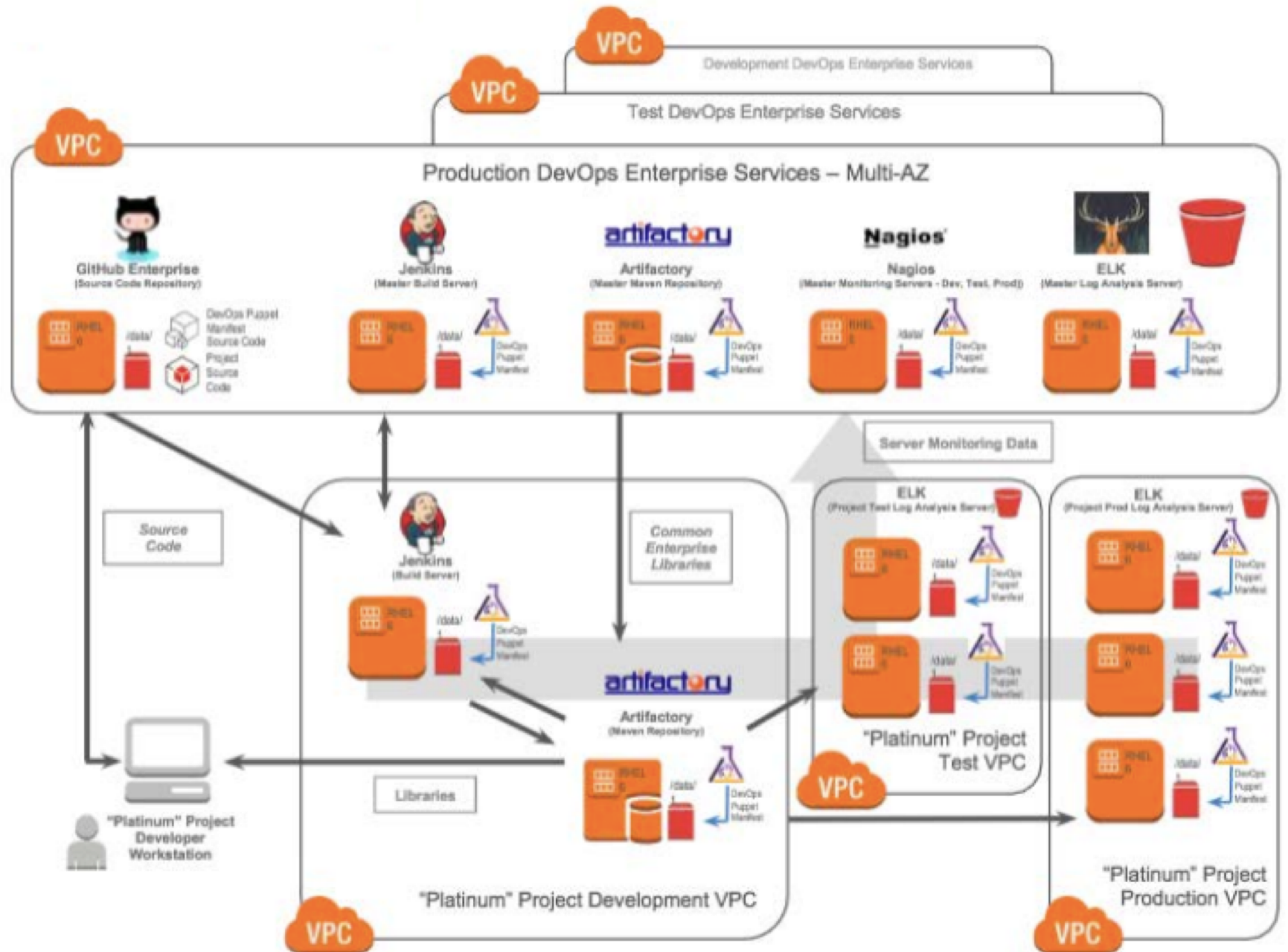
**Send Build Report to Security
Stop everything if audit/validation failed**

@IanMmmm

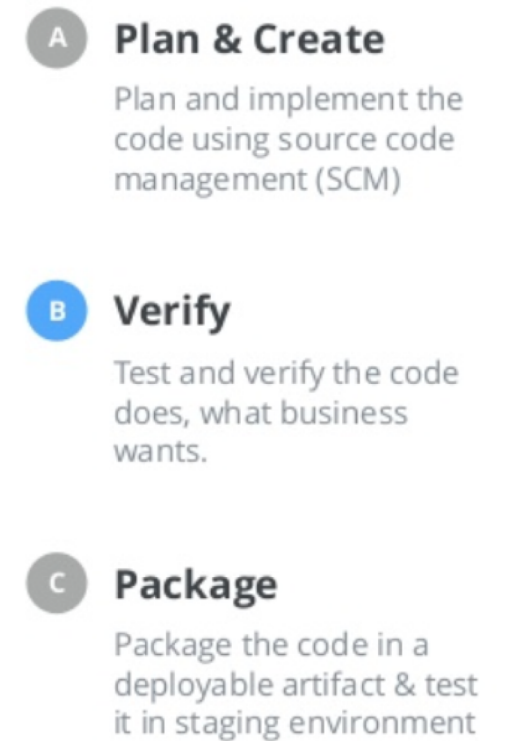
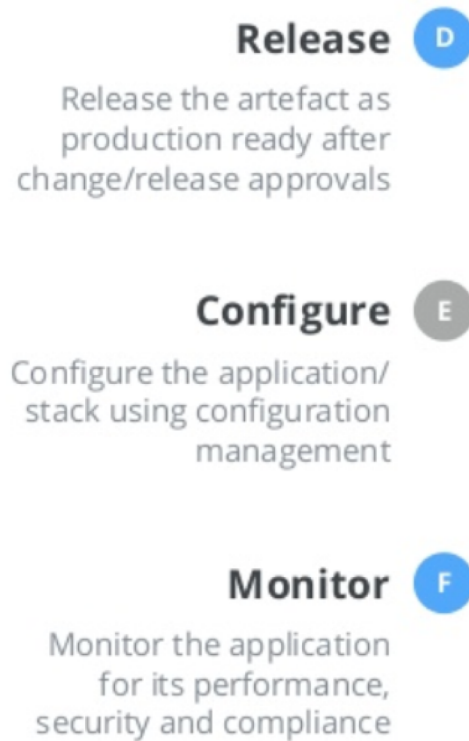
DevSecOps according to Hart Rossman and AWS



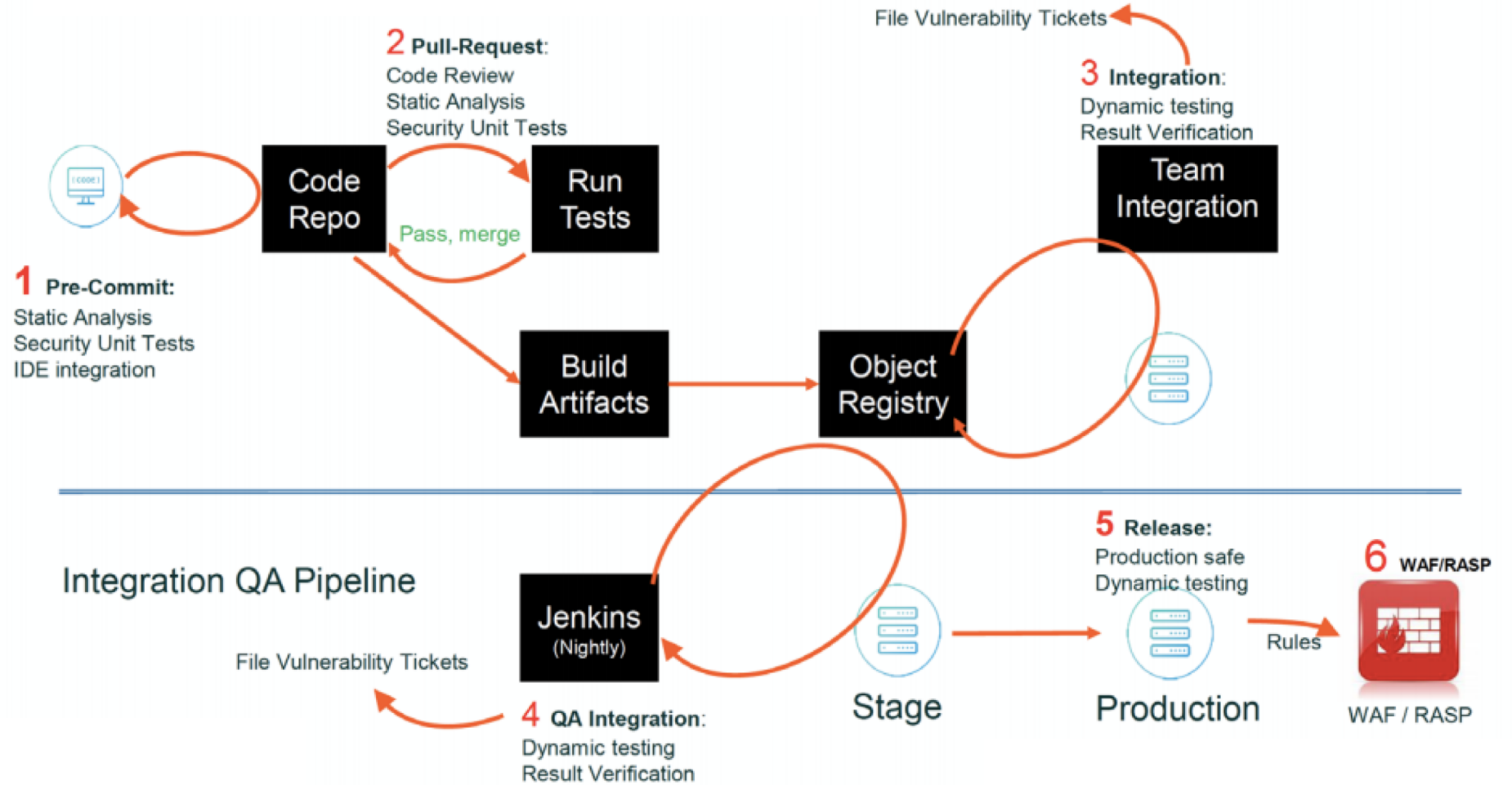
DevSecOps according to Dominic Delmolino and Accenture



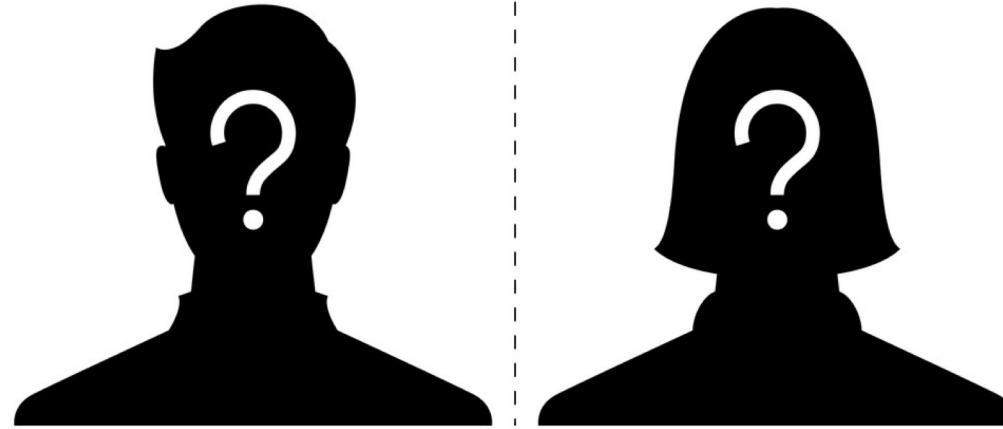
DevSecOps according to Mohammed Imran and Ellucian



DevSecOps according to Siamak Pazirandeh and WhiteHat Security



DevSecOps according to YOU



Want your DevSecOps Reference Architecture to this deck?

1. Send it to community@sonatype.com with the subject line: DevSecOps Reference Architecture (or DM us on Twitter [@Sonatype](https://twitter.com/Sonatype))
2. Provide a link as to where people can find more info about it (e.g., blog, video, SlideShare)
3. We'll add it to this deck with full attribution to you

It's that easy; we all learn with help from the community. Thank you in advance for your contributions!

