# 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









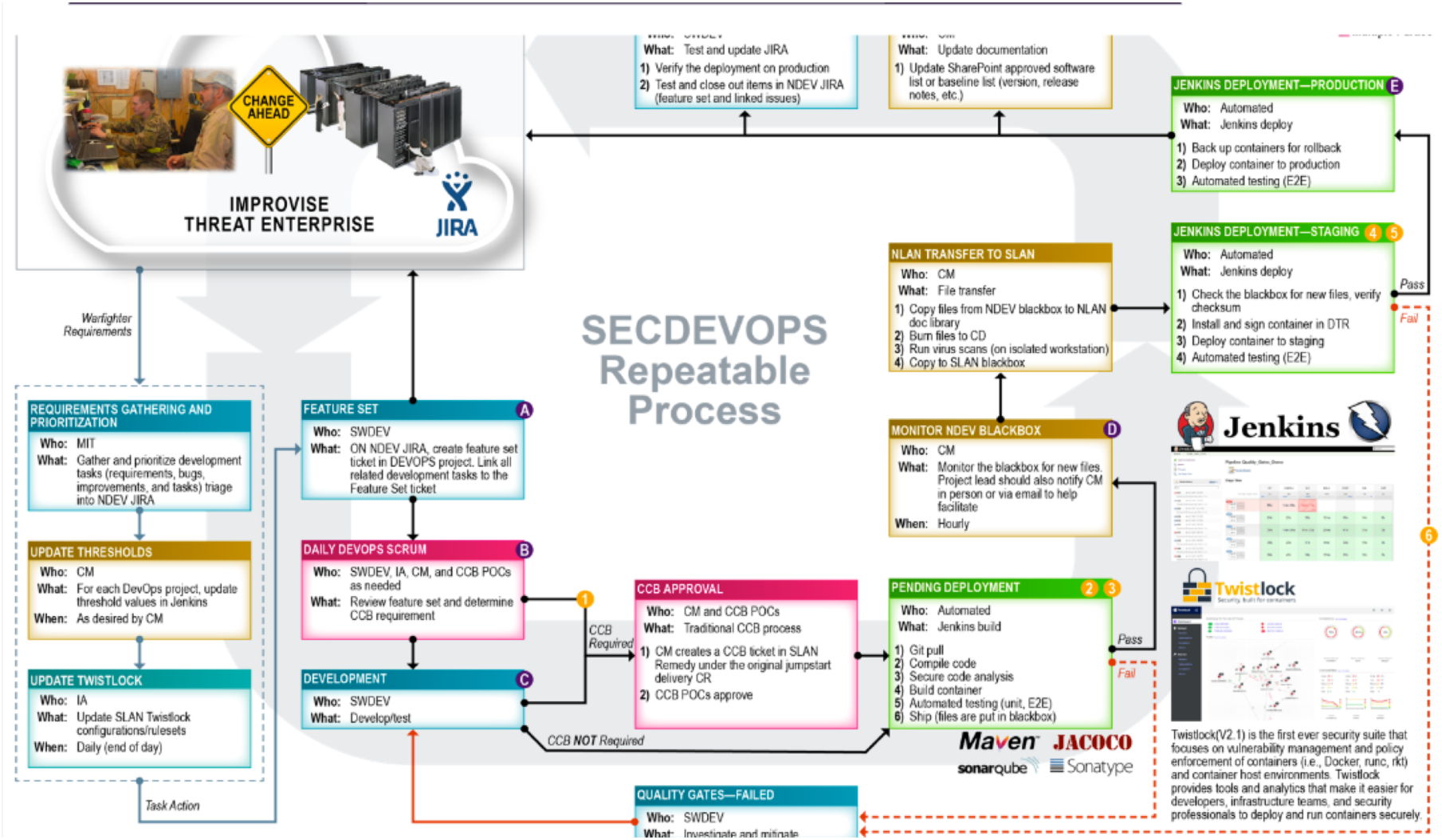








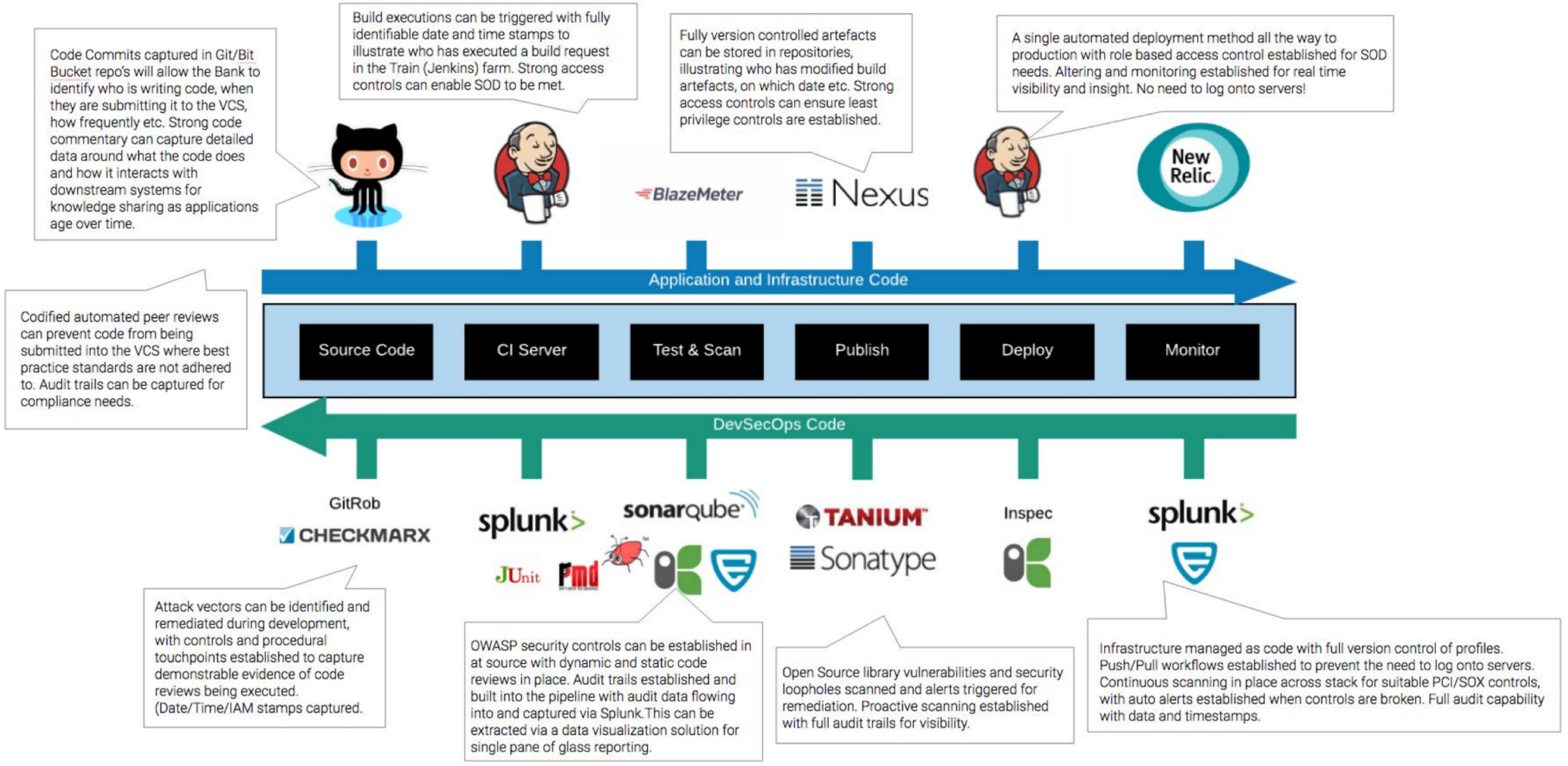
# DevSecOps according to U.S. Dept of Defense/JIDO




Sonatype

Source: ADDO '17 "Governance and Transparency in GovSec DevOps: Leonel Garciga"

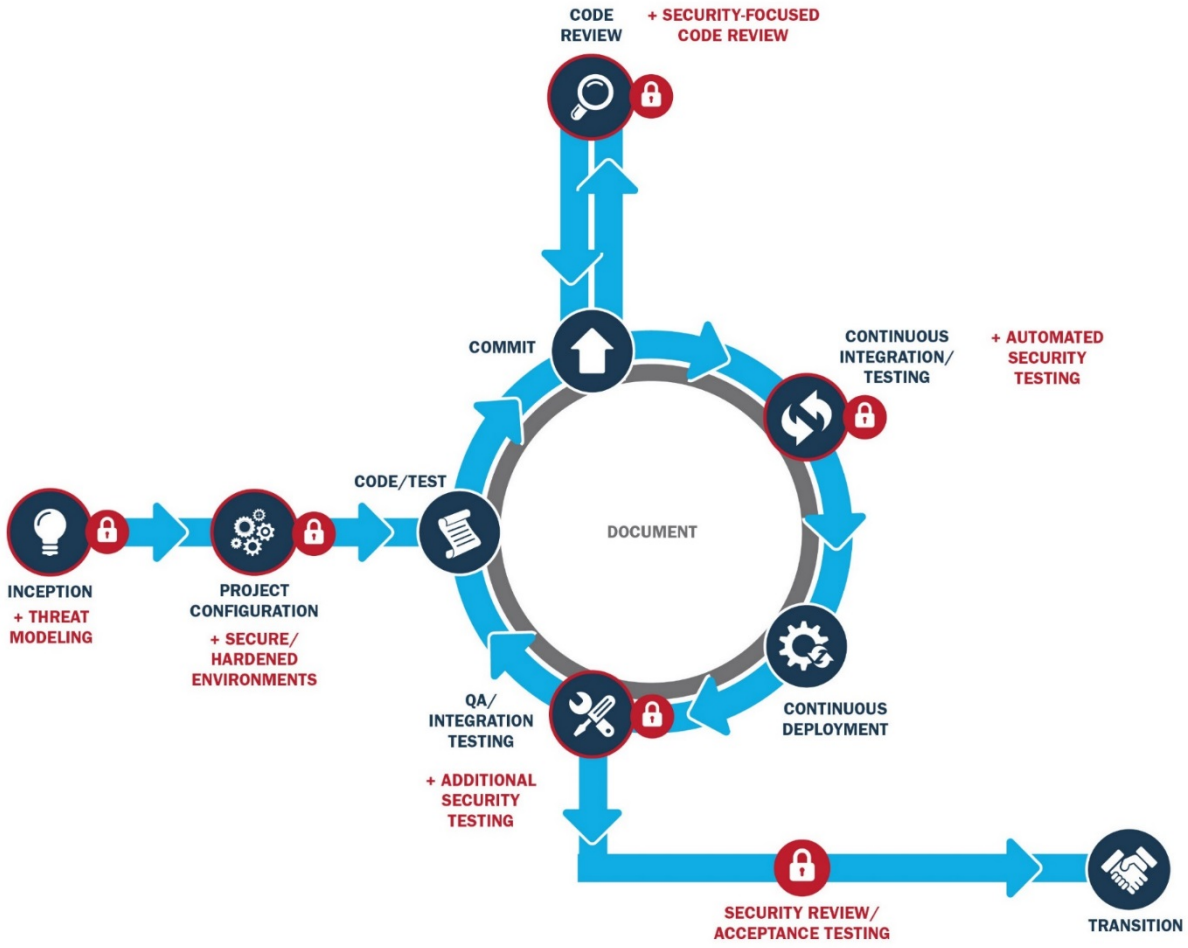
# DevSecOps according to CONTINO




Sonatype

Source: Michael Man, DevSecOps Consultant: https://www.slideshare.net/MichaelMan11/devsecops-the-evolution-of-devops

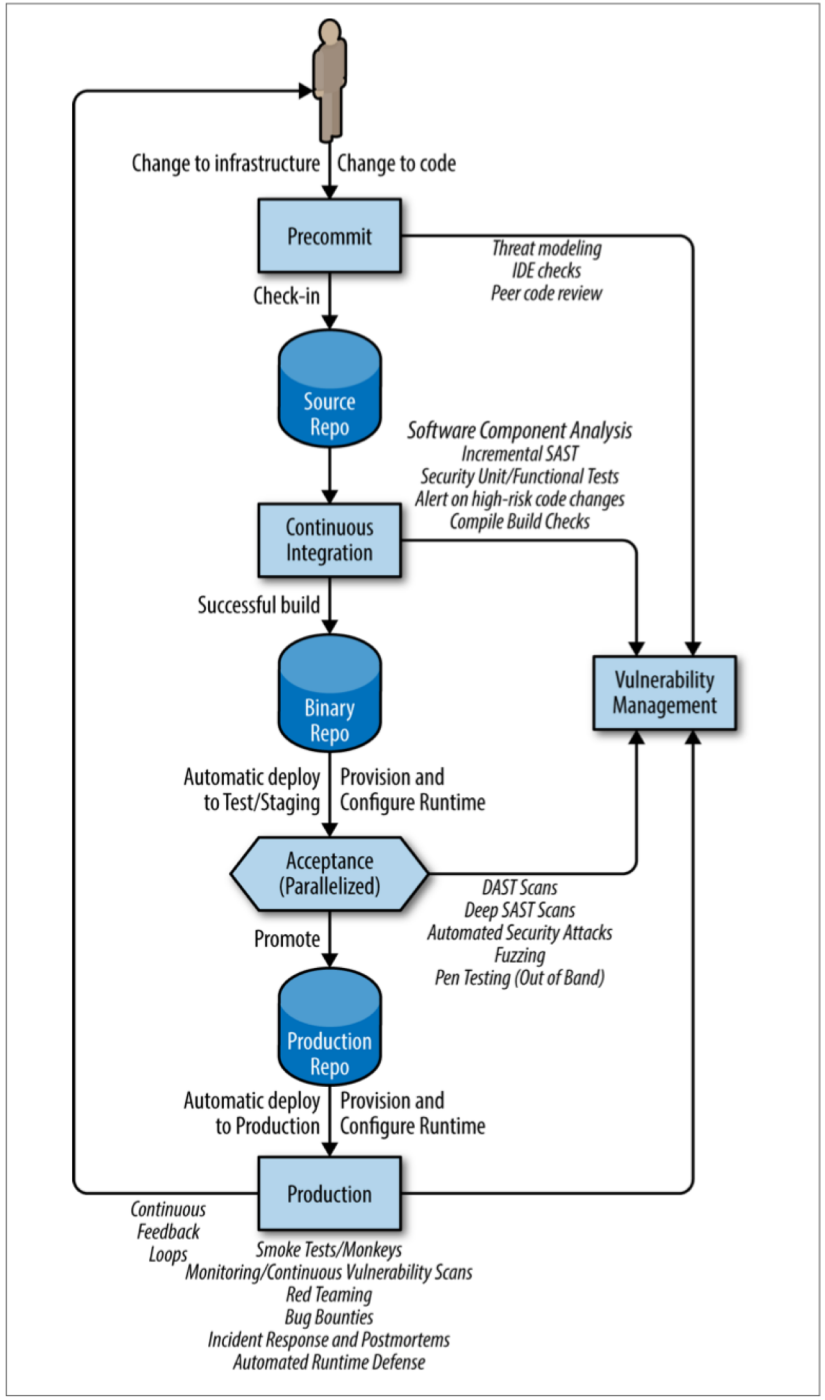
# DevSecOps according to Carnegie Mellon's SEI




Sonatype

Source: Derek Weeks, DZone "From Water-Scrum-Fall to DevSecOps"

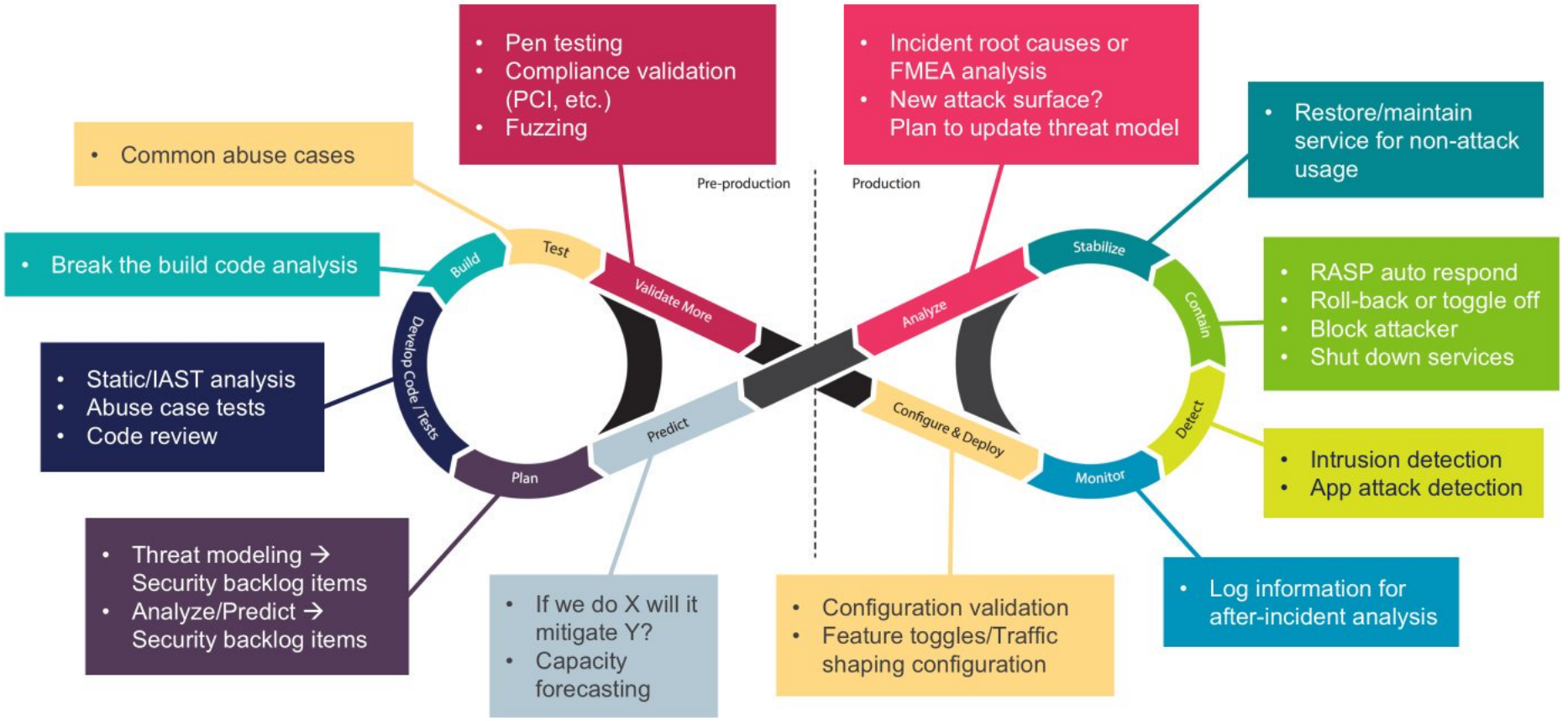
# DevSecOps according to Jim Bird




Source: Jim Bird, O'Reilly "DevOpsSec: Securing Software through Continuous Delivery"

Sonatype

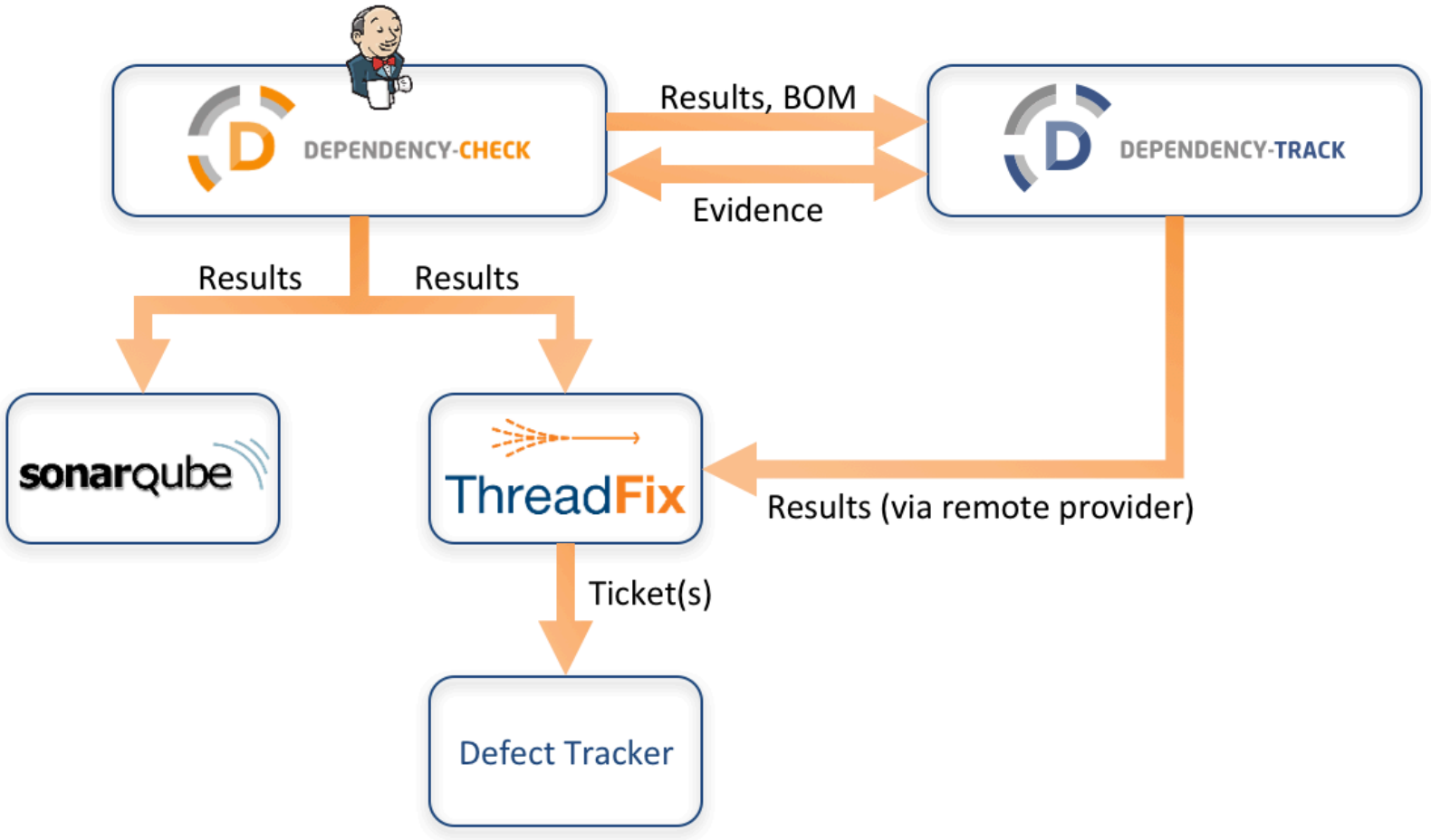
# DevSecOps according to Larry Maccherone




Sonatype

Source: Larry Maccherone @Lmaccherone, Twitter "Annotated DevSecOps cycle"

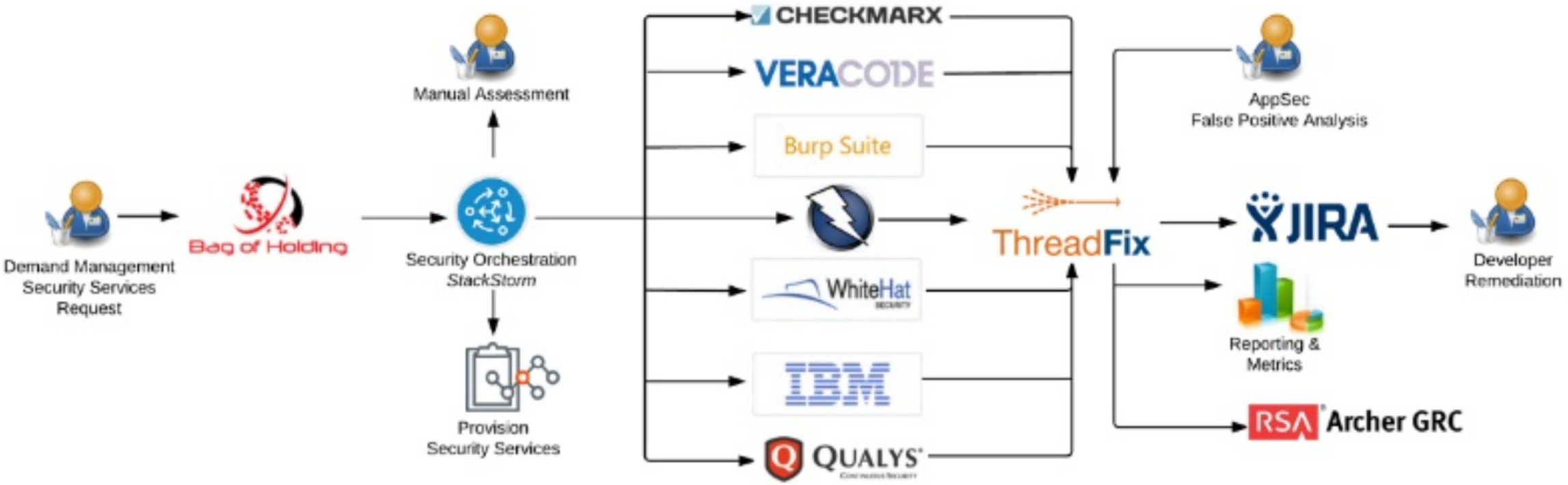
# DevSecOps according to Steve Springett




Sonatype

Source: Steve Springett, GitHub "Dependency-Track"

# DevSecOps according to TeachEra




Sonatype

Source: Mohammad Imran, Linked in "Practical DevSecOps Course - Part 1"

# 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

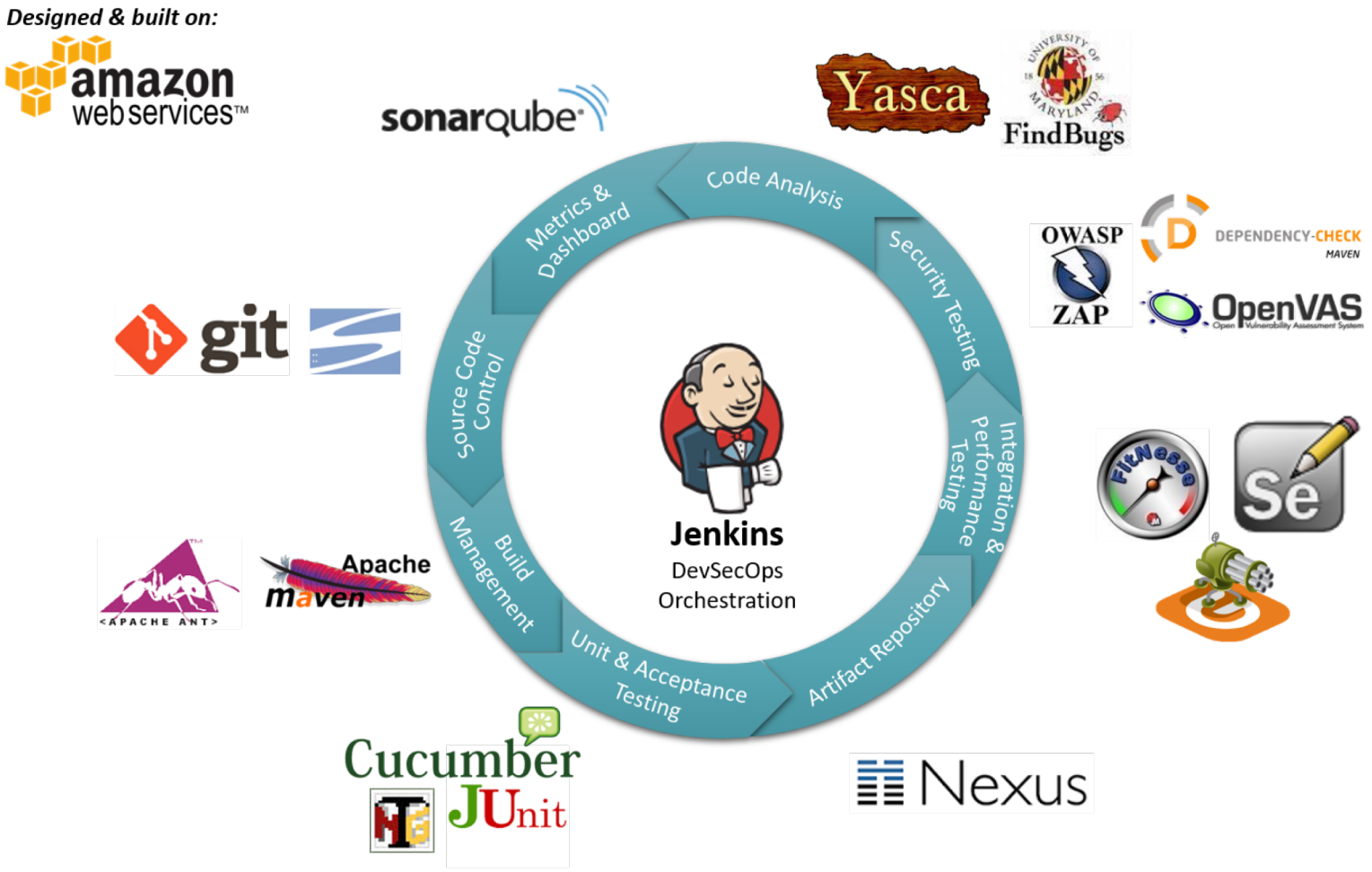

Microsoft


Carnegie Mellon University


GSA

All Day DevOps 2017

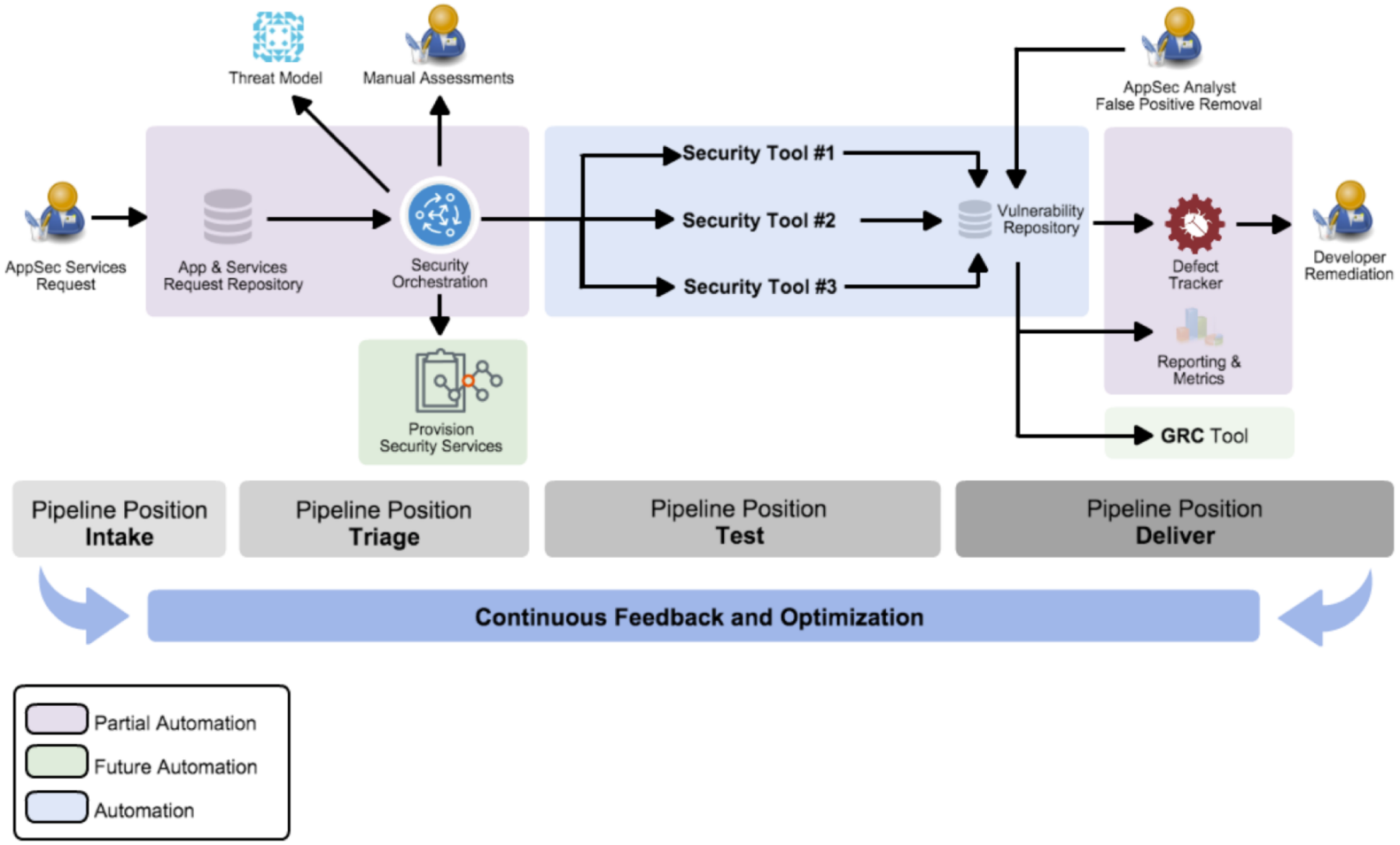
# DevSecOps according to Coveros




Sonatype

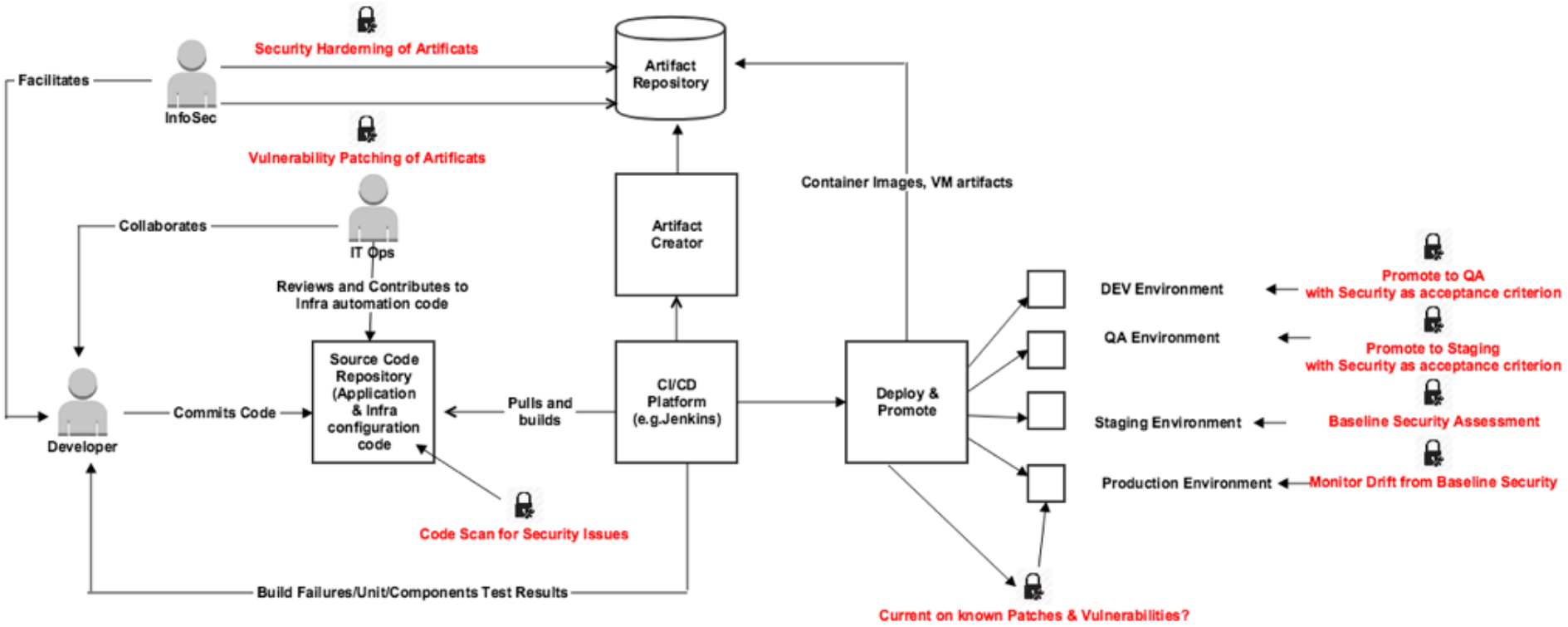
Source: Alan Crouch, Coveros "Implementing the DevSecOps Process"

# DevSecOps according to Aaron Weaver



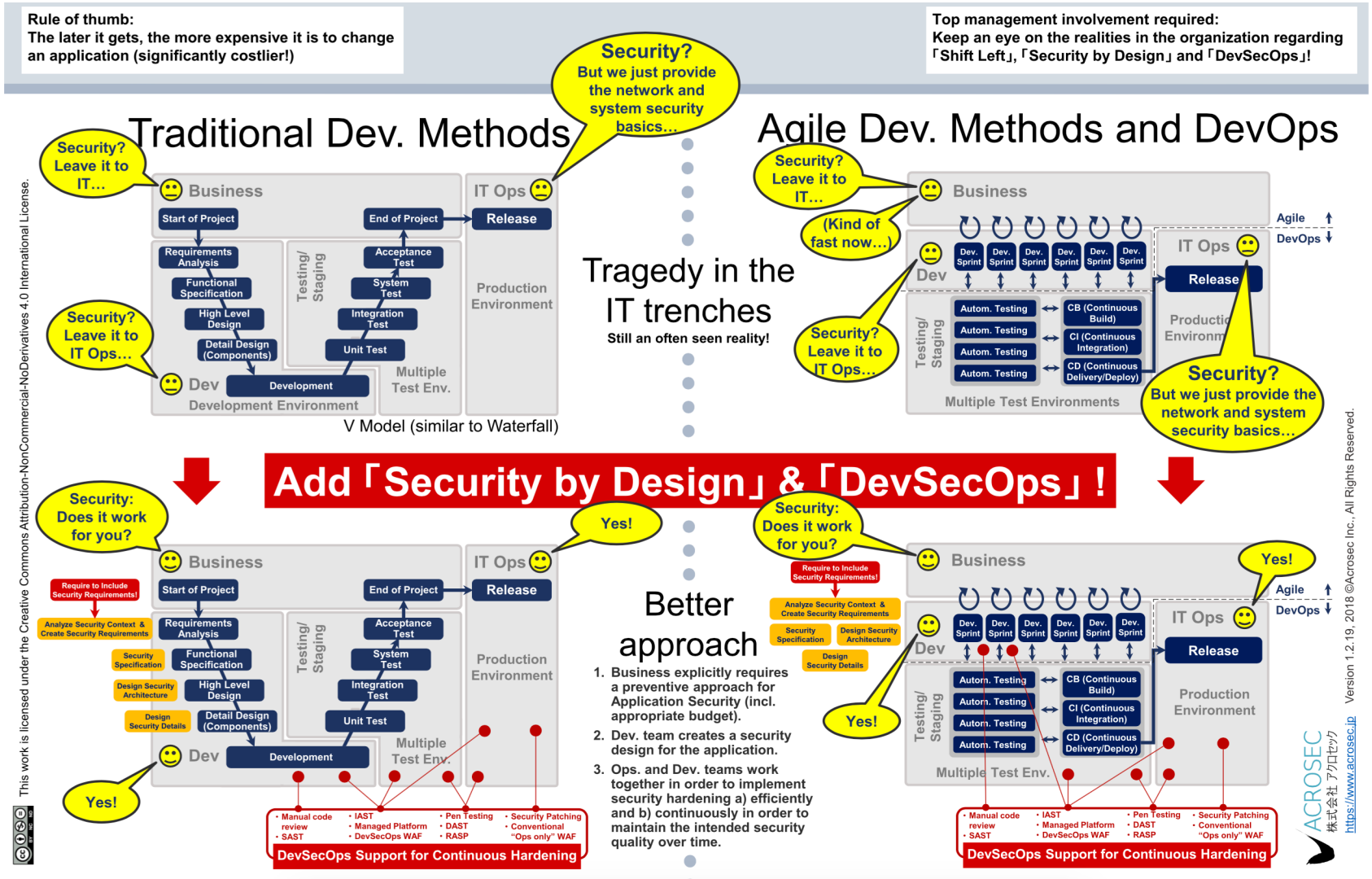

Source: Stefan Streichsbier Linked in "DevSecOps - The big picture"

# DevSecOps according to Dr. Ravi Rajamiyer



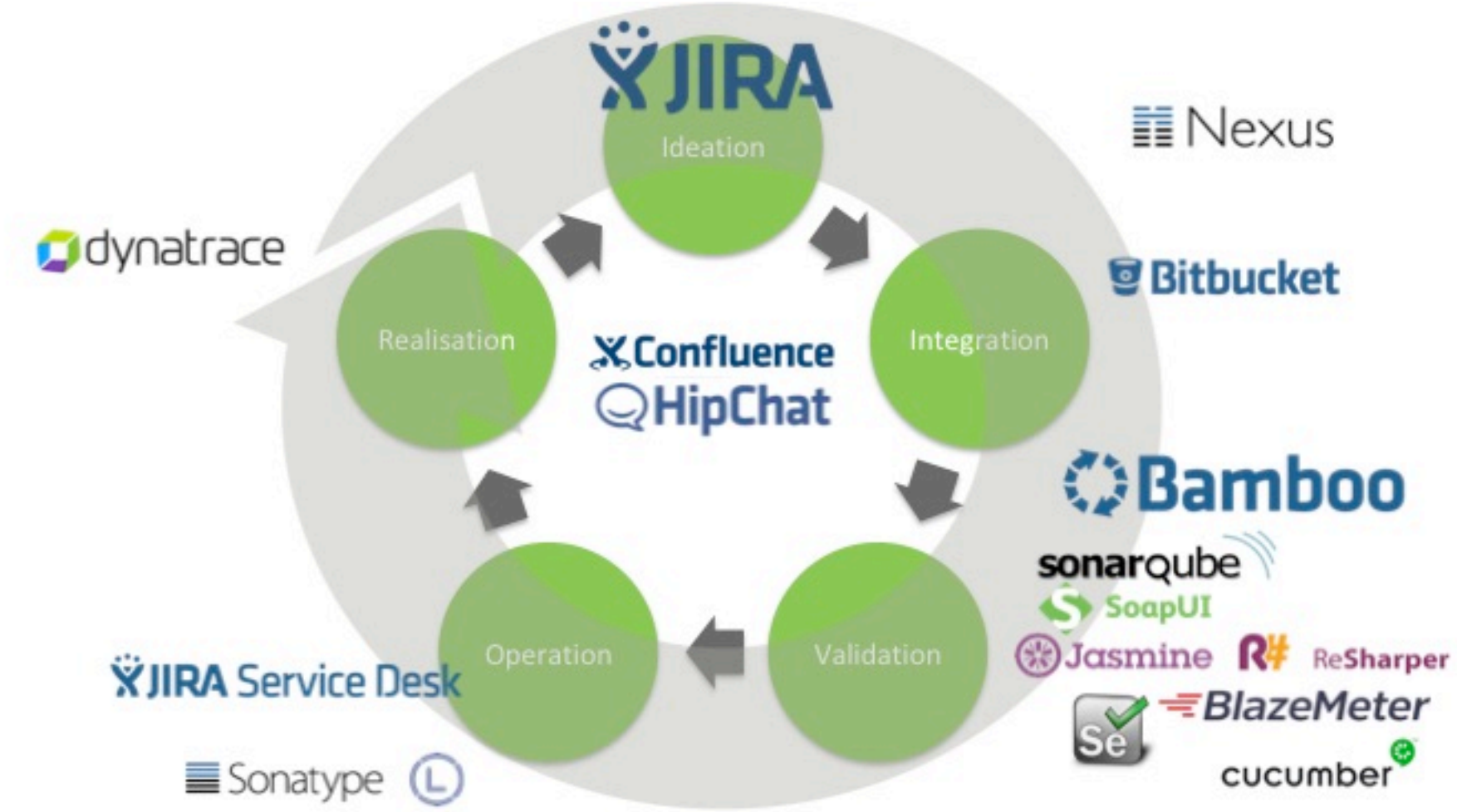

Source: **Dr. Ravi Rajamiyer**, DevOps Summit Journal "When "IoC" meets "SoC'"

# DevSecOps according to ACROSEC




Source: Derek Weeks, Acrosec "Three important elements of Application Security: "Shift Left", "Security by Design" and "DevSecOps'"

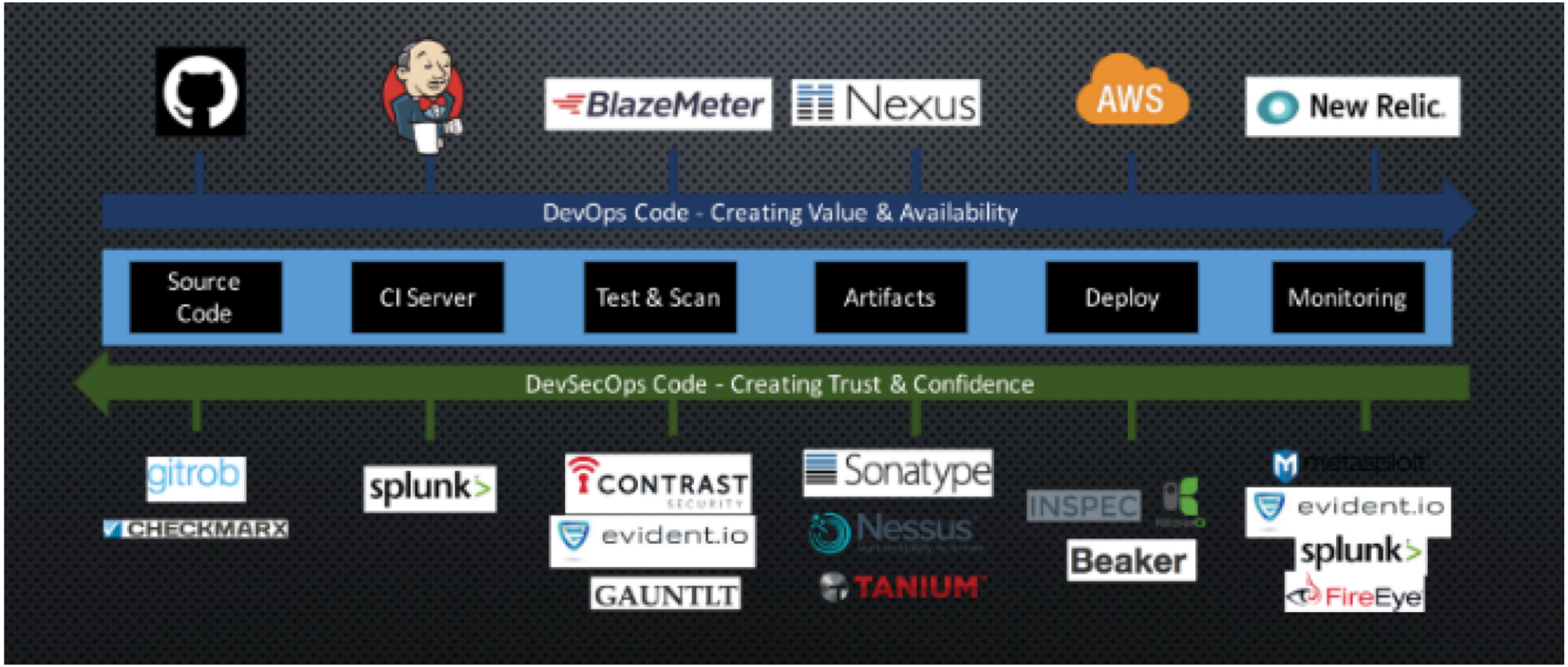
# DevSecOps according to Ranger4




Sonatype

Source: Helen Beal, Linked in "DevSecOps is it a Good Thing"

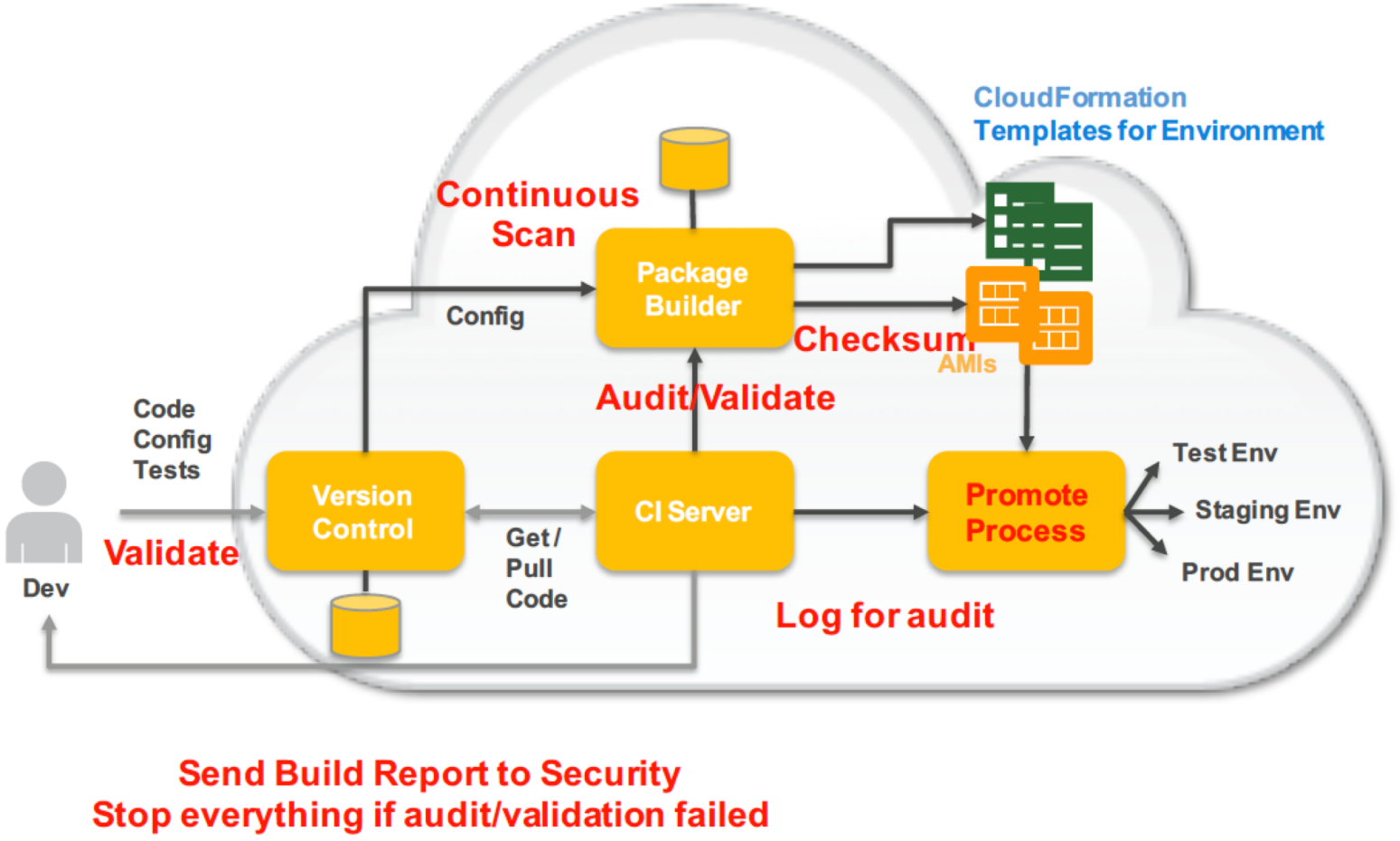
# DevSecOps according to Magno Rodrigues




Sonatype

Source: Stefan Streichsbier Linked in Slides "DevSecOps - The big picture"

# DevSecOps according to AWS

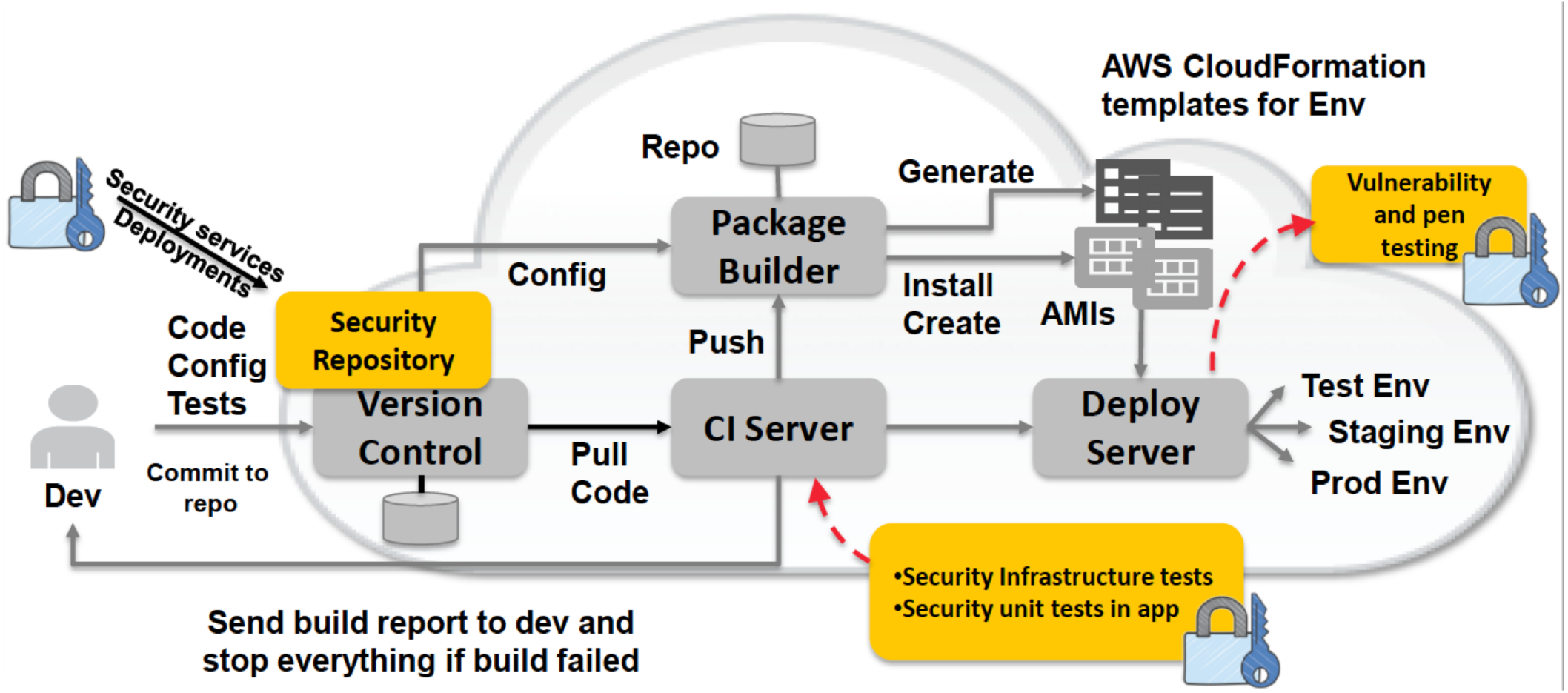



@IanMmmm

Sonatype

Source: Ian Massingham, @IanMmmm, Linked In "Securing Systems at Cloud Scale with DevSecOps"

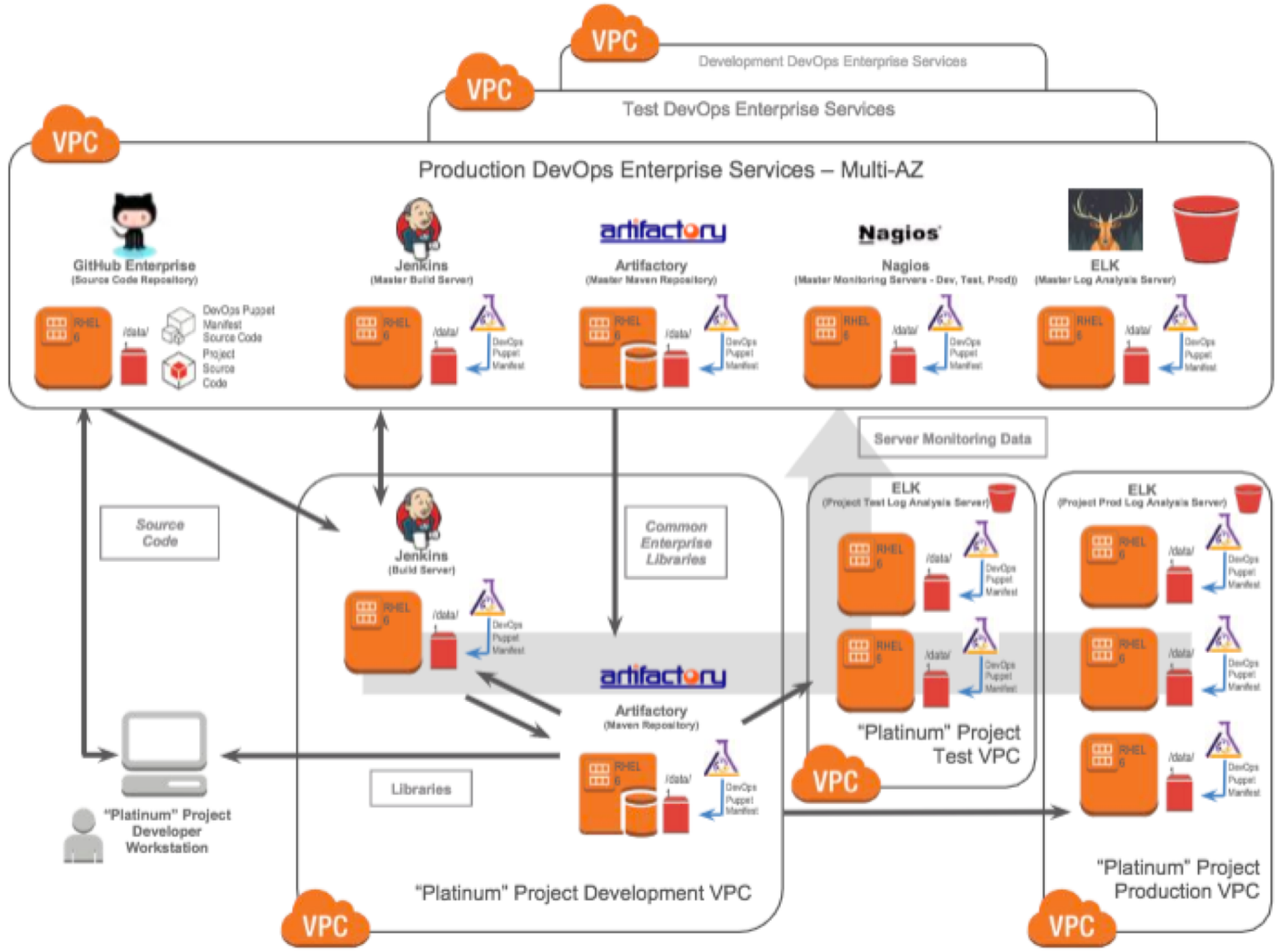
# DevSecOps according to AWS




Sonatype

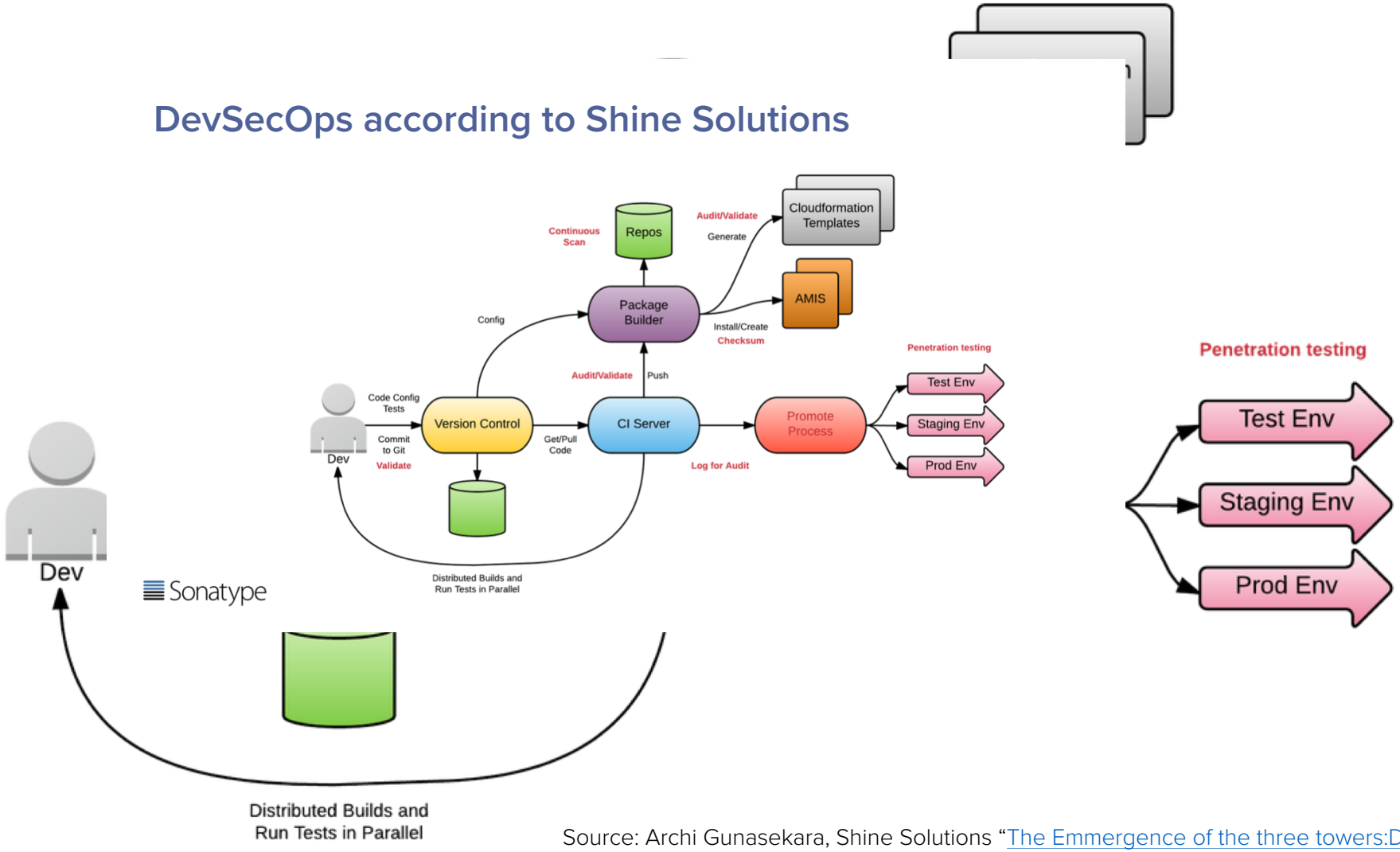
Source: Priyanka Aash, Linked In "DevSecOps in Baby Steps"

# DevSecOps according to Accenture




Source: ADDO'17, YouTube "DevOps in Secure Environments: Strategies for Success: Dominic Delmolino"

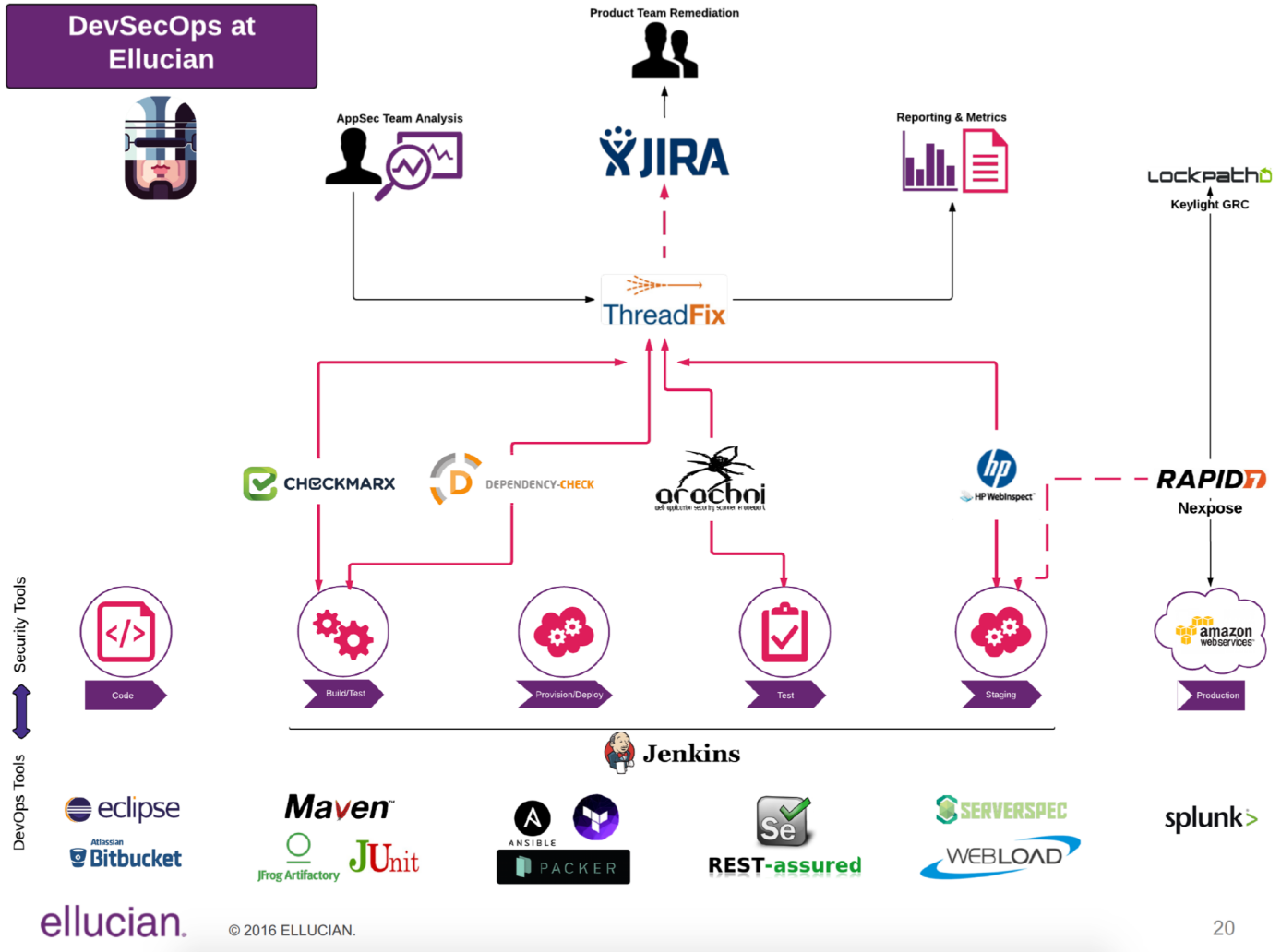
# DevSecOps according to Shine Solutions




Sonatype

Source: Archi Gunasekara, Shine Solutions "The Emmergence of the three towers:DecSecOps"

# DevSecOps according to Ellucian

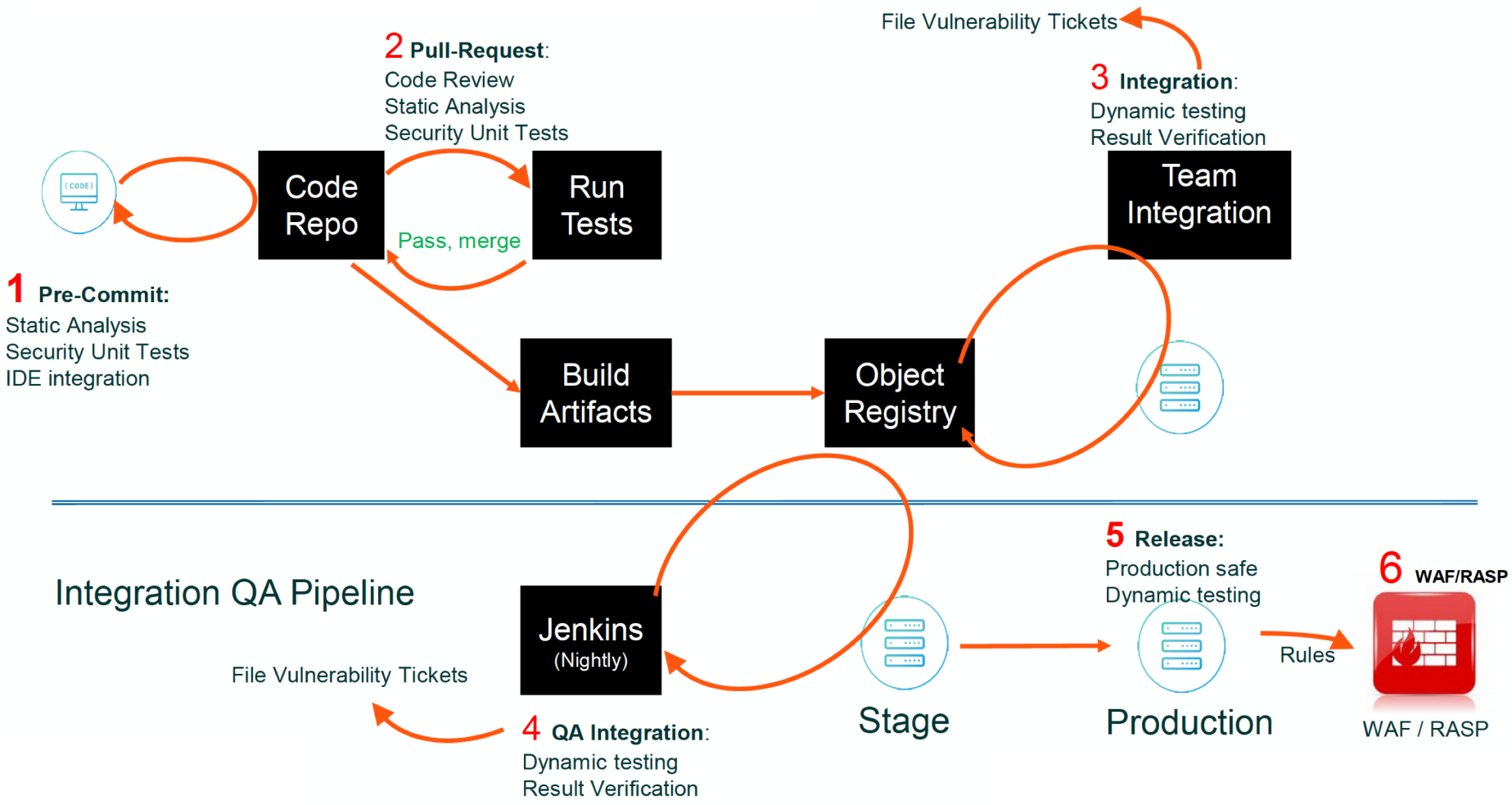





Sonatype

Source: https://www.slideshare.net/FranklinMosley/robocop-bringing-law-and-order-to-cicd?from_action=save

# DevSecOps according to WhiteHat Security




Sonatype

Source: White Hat Security "Take Control Design a complete DevOps Program"

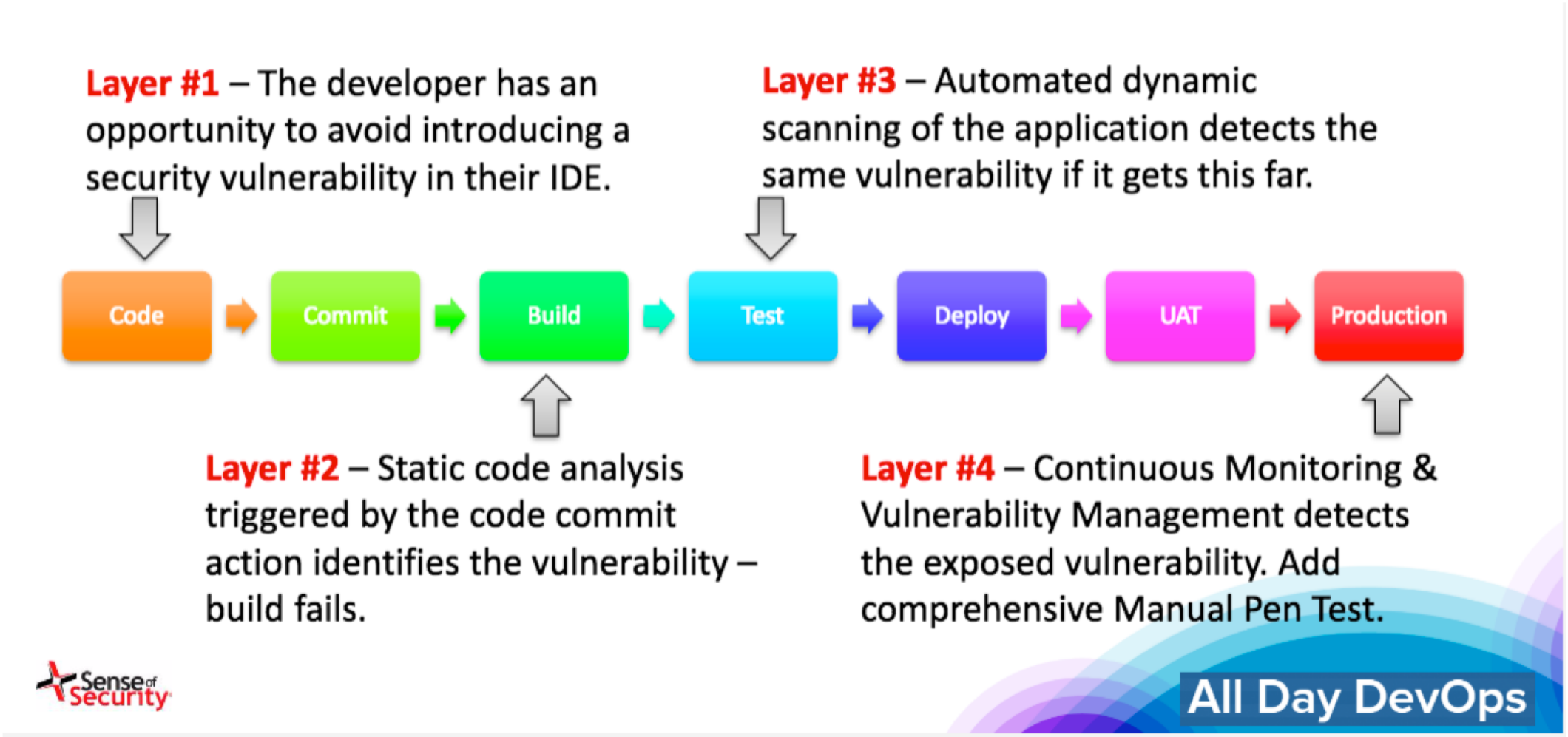
# DevSecOps according to GSA

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



Source: Tech at GSA "Building DevSecOps Culture"

# DevSecOps according to Sense of Security




Sonatype

Source: ADDO'17, Youtube "DevOps: A How-To for Agility with Security: Murray Goldschmidt"


**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!**

# About the Author

**Derek Weeks**
**VP and DevOps Advocate, Sonatype**

Derek is a huge advocate of applying proven supply chain management principles into DevOps practices to improve efficiencies and sustain long-lasting competitive advantages. He currently serves as vice president and DevOps advocate at Sonatype, creators of the Nexus repository manager and the global leader in solutions for software supply chain automation. Derek is also the co-founder of All Day DevOps -- an online community of 40,000 IT professionals, and the lead researcher behind the annual State of the Software Supply Chain report for the DevOps industry. In 2018, Derek was recognized by DevOps.com as the“Best DevOps Evangelist”for his work in the community.


Sonatype