Simplifying the World of Open Source Usage for Financial Insitutitions

James McLeod
Director of Community
FINOS

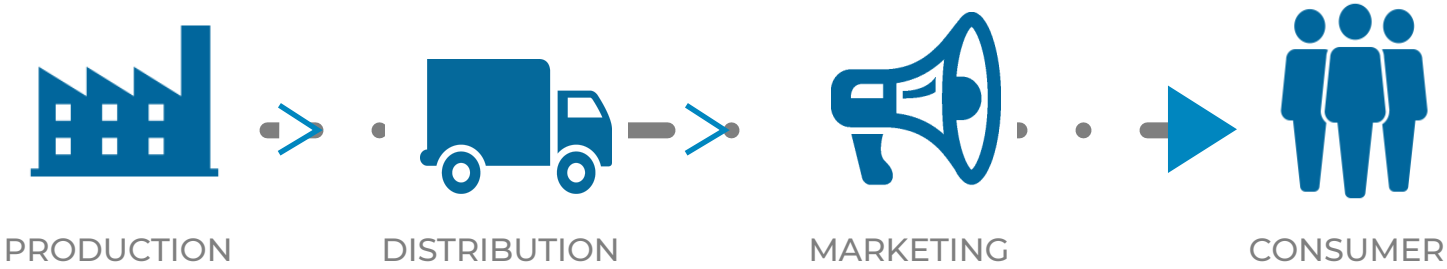
Jeff Crum
Senior Director of Product Marketing
WhiteSource

FINOS

WhiteSource

Traditional Solution Oriented Business Models

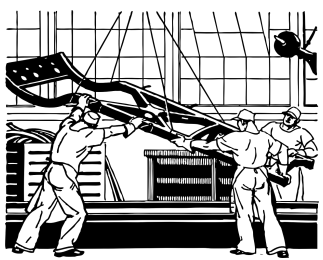
In traditional business models
Value creation Is linear and one-way

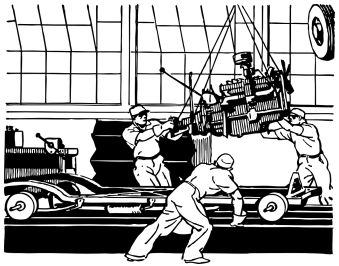


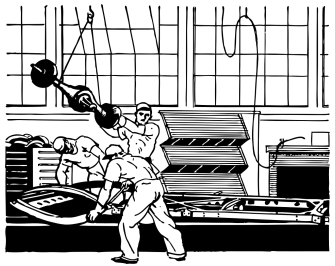
Linear Development with Extended Lead Time

OSS Consumption → Development → Integration Testing → Quality Testing → Security Testing

GitHub

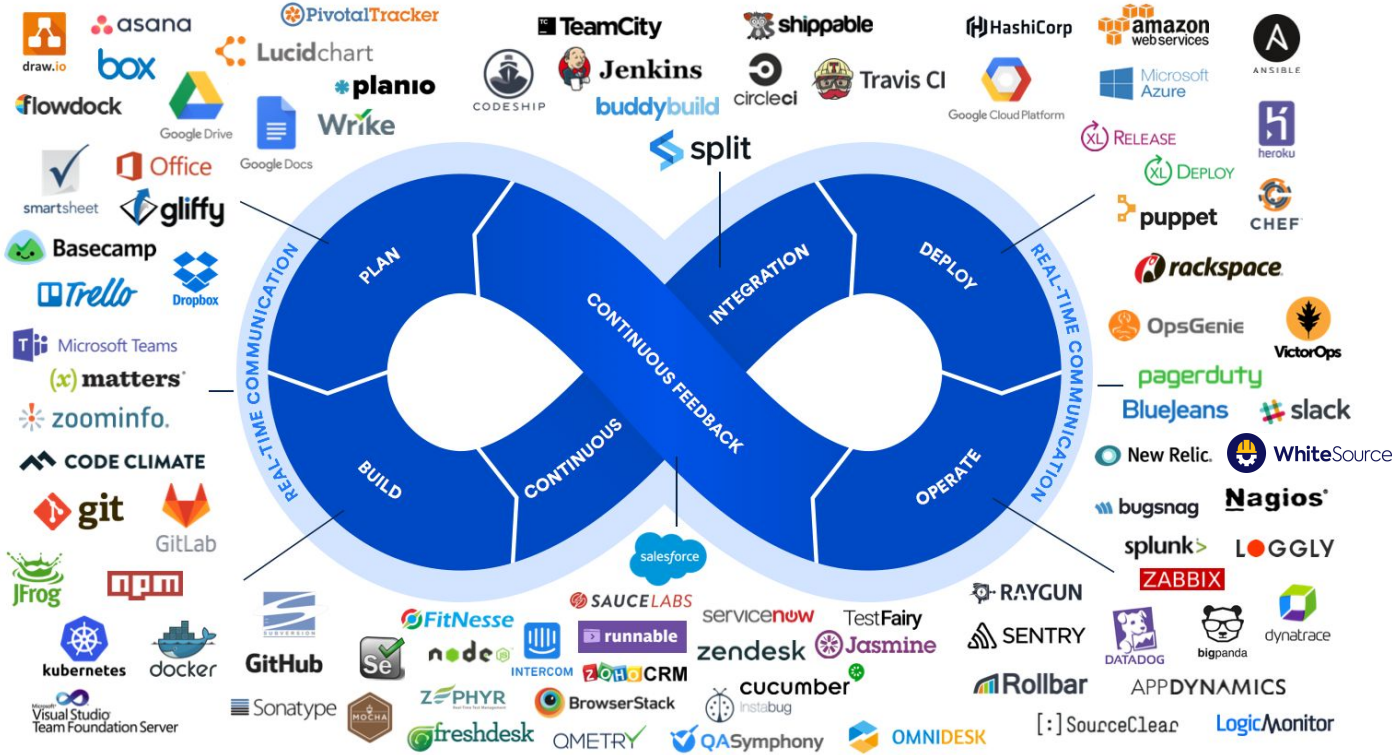






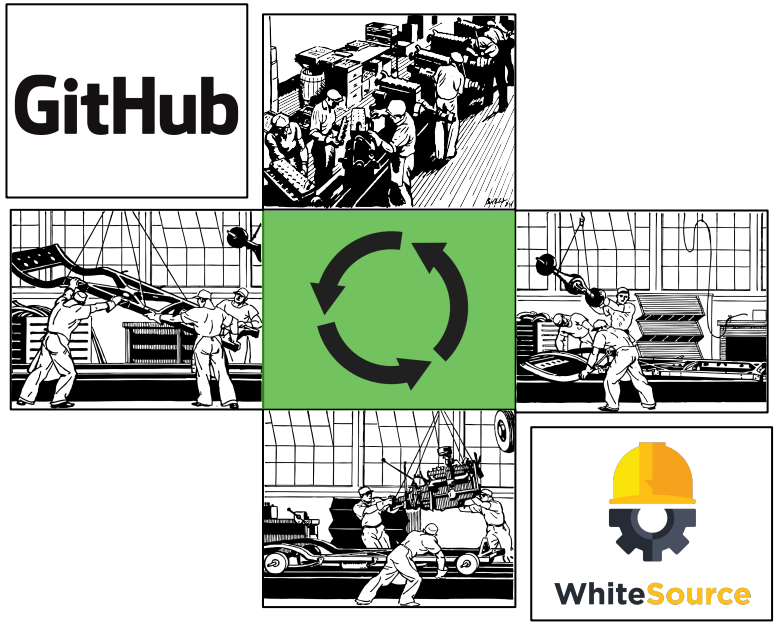
Testing Failure

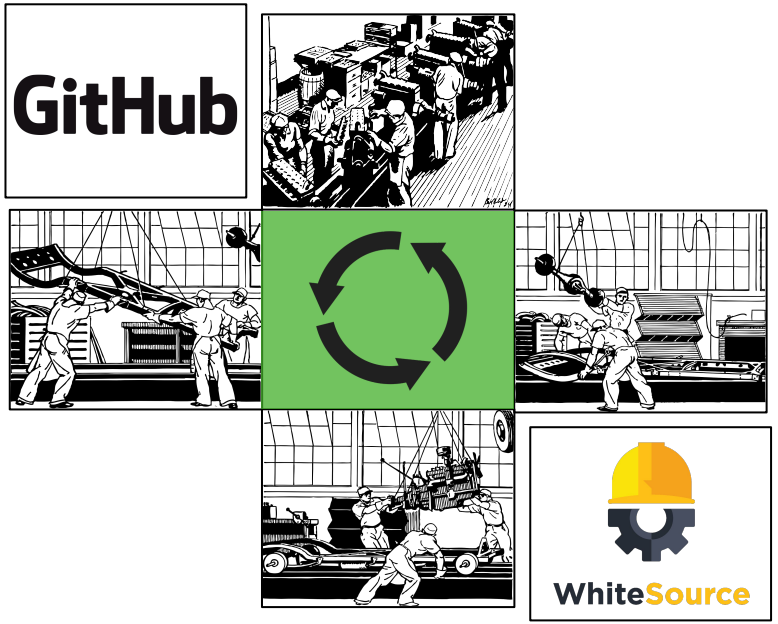
DevOps Automation Reduces Development Cycles



https://marketplace-cdn.atlassian.com/s/public/devops-hero-1-87966cfbc9c5713ae047551c7b22985c.png

Real-Time Security Scanning Adds Sec to DevOps





Continuous Agile Delivery

FINOS Publishes New Responsible Disclosure Policy

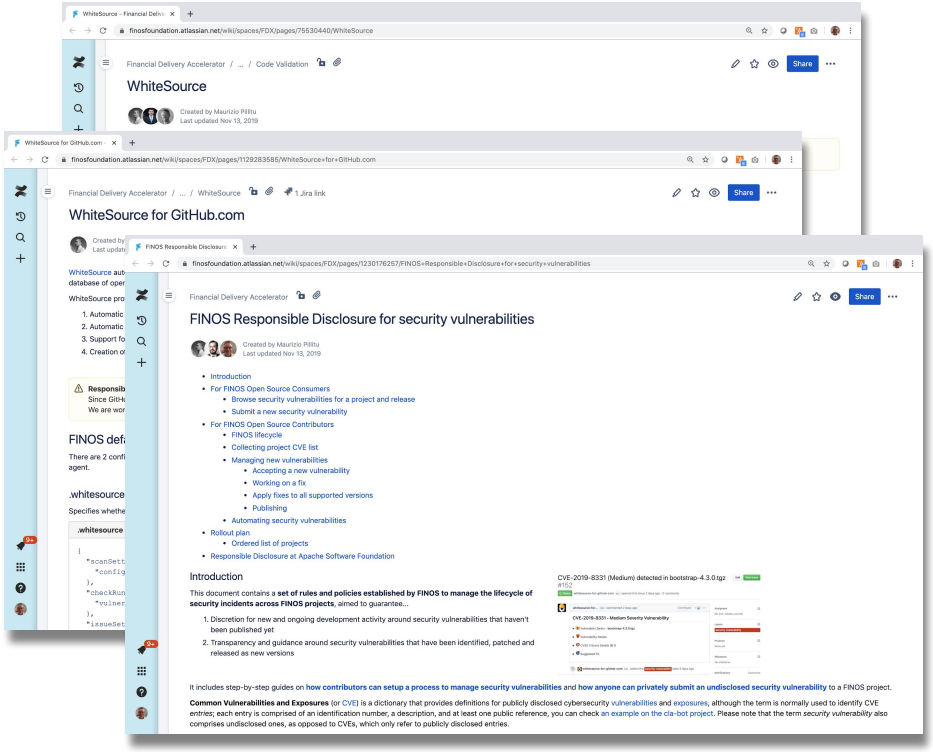
Don’t Alert Bad Actors to New Open Source Vulnerabilities!

The new FINOS Responsible Disclosure policy provides guidance to teams when communicating New, Ongoing, Identified, Patched and Released vulnerabilities.

- Privately report issues to FINOS PMC
- Team works privately to resolve Issue
- New release made including issue fix
- Vulnerability announced only when safe

These steps stop bad actors from being alerted to new open source vulnerabilities.

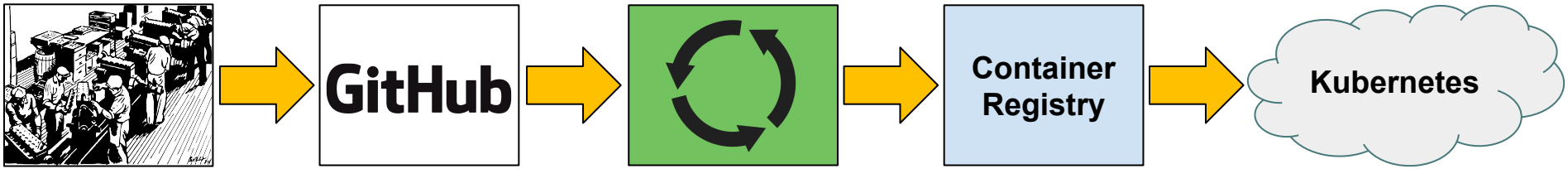
The FINOS Responsible Disclosure policy is available for review on FINOS wiki.



https://finosfoundation.atlassian.net/wiki/spaces/FINOS/pages/1230176257/Security+vulnerabilities+responsible+disclosure

Implementing GitOps and Shifting Further Left

Git as the “Single Source of Truth” for Declarative Infrastructure and Applications



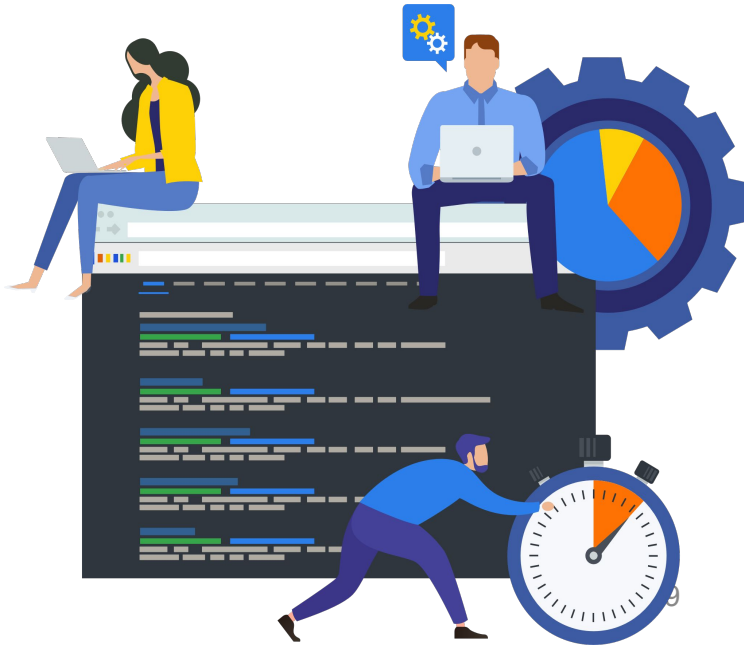
- Increased Productivity
- Enhanced Developer Experience
- Improved Stability
- Higher Reliability
- Consistency and Standardization
- Stronger Security Guarantees

Platforms Thrive in an Open ecosystem

In Platform business models
Value creation is two-way and continuous

Logos are © and (™) of their respective owners

So how can you shift left security successfully?



WhiteSource

1

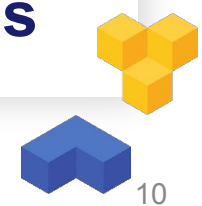
How left can you go?

2

Who owns it?

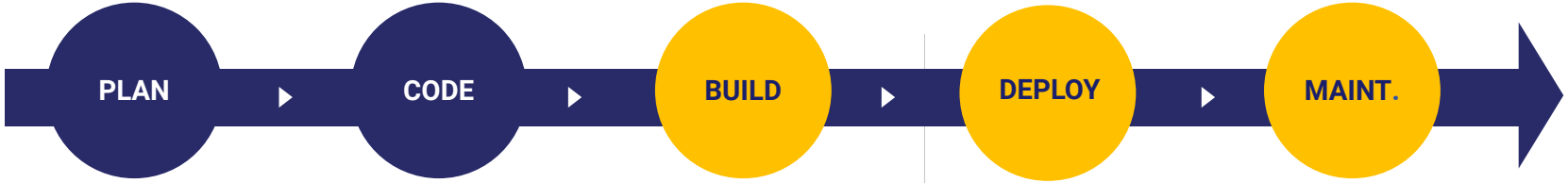
3

Shifting left the right tools



WhiteSource

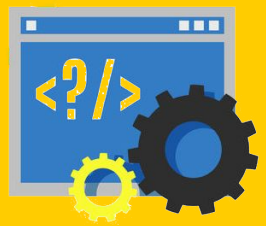
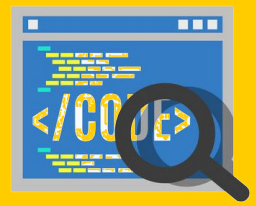
When is the optimal point to integrate security checks into the SDLC?



WhiteSource

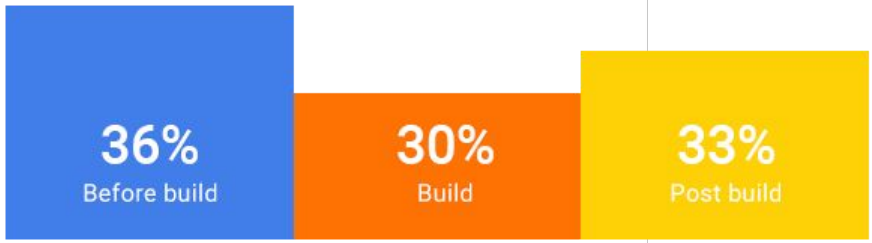
Detecting Issues as Early as Possible Has Multiple Benefits

The cost of fixing security and quality issues is rising significantly, as the development cycle advances.

Coding	Build	QA & Security	Production
			
$80/Defect	$240/Defect	$960/Defect	$7,600/Defect

66% of companies have already implemented application testing during or even pre-build stage

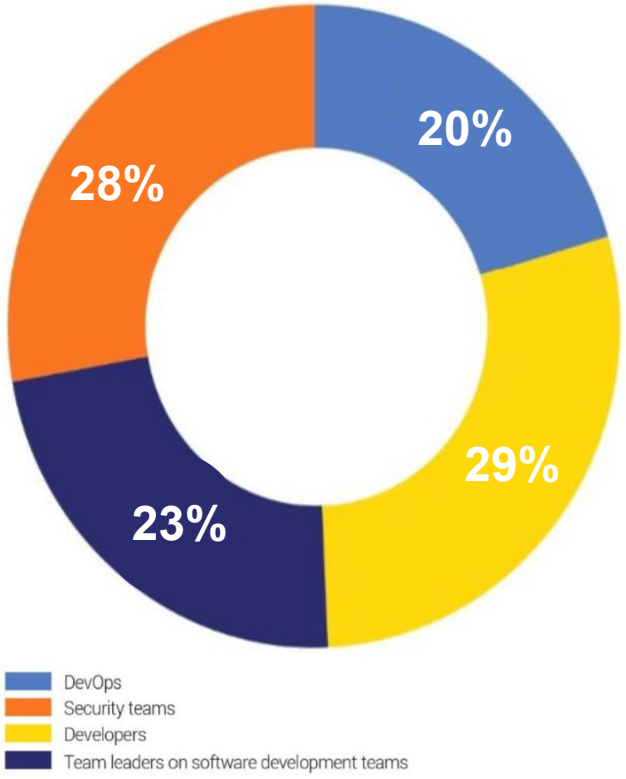
In what stage of the SDLC do you spend most of your time implementing security measures?



If the goal is to integrate security pre-build, then who should own application security in the organization?

72%

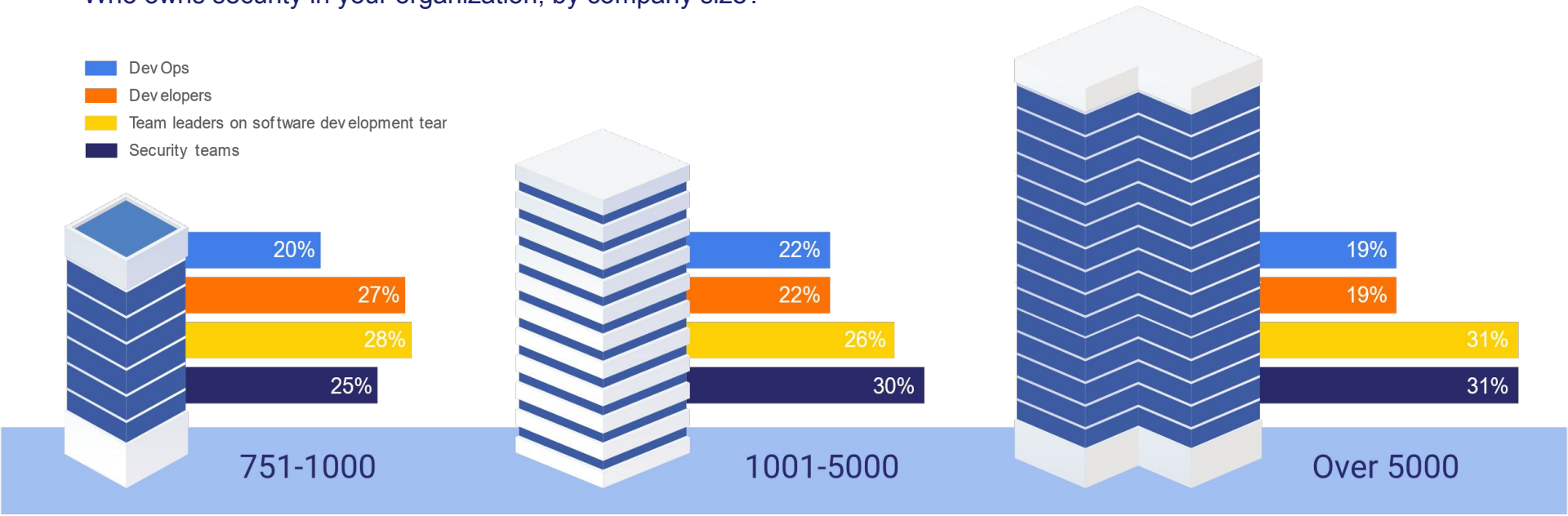
of the respondents stated that the ownership over AppSec lies in the software development side



WhiteSource

Research shows organizations of all sizes are shifting their operational security to software development teams

Who owns security in your organization, by company size?



What are the “right” tools?

Both teams need security tools, but in order to shift left security you need to empower your developers.

Governance solutions

Used by security teams and management to get full visibility and control over the security risks in their software

Developers tools

Used by developers to remediate vulnerabilities

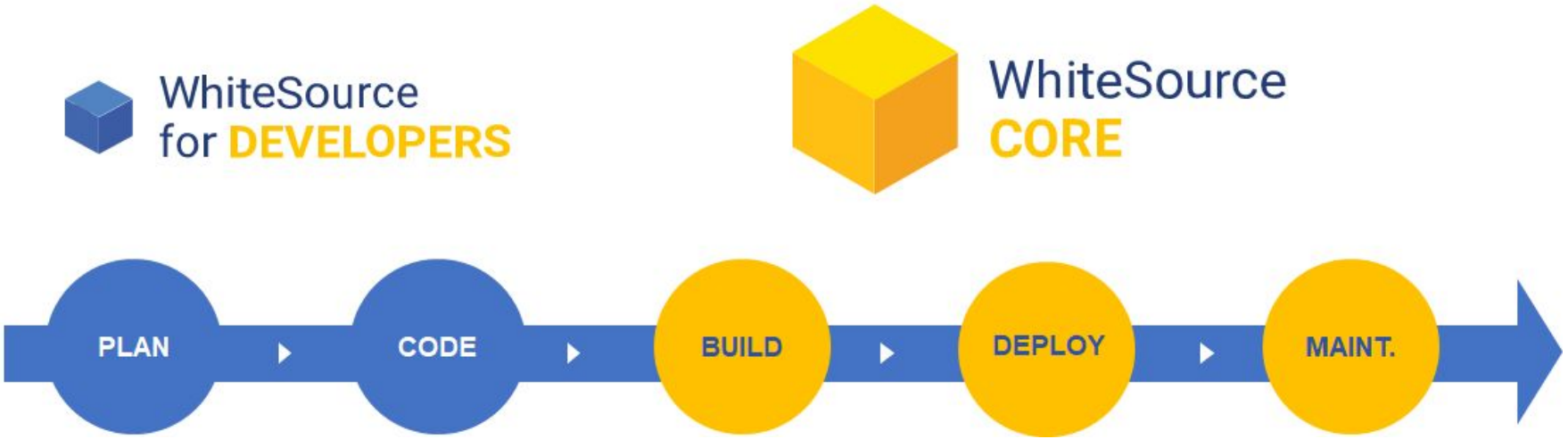
WhiteSource Complete Solution

WhiteSource for DEVELOPERS

Caters to security managers, DevOps professionals, and developers

WhiteSource CORE

WhiteSource Product Portfolio



1

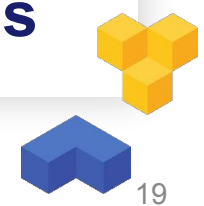
How left can you go?

2

Who owns it?

3

Shifting left the right tools



Q&A

FINOS

WhiteSource