DevSecOps Days Washington, D.C.

The Art of Enabling Engineering Excellence and DevSecOps

Vishy Mahadevan
Chief Technology Officer
Optimx LLC

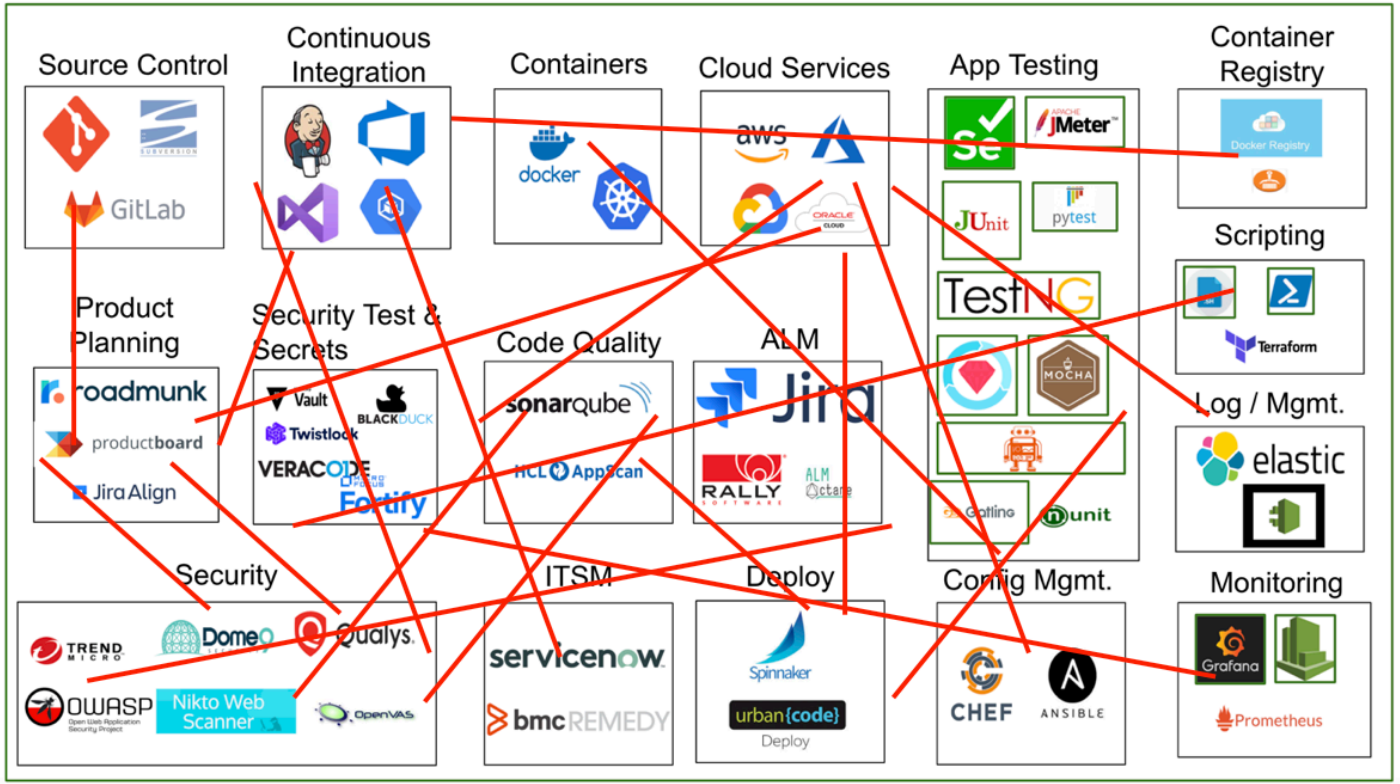
Agenda

- Challenges faced by Engineering and Security Leaders
- Best Practices Driven Software Delivery & Continuous Improvements
- Use Case – “The Art of Enabling Engineering Excellence and DevSecOps”

The Art of Enabling Engineering Excellence and DevSecOps

Engineering Excellence

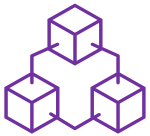
It is hard to get a unified view of Software Engineering today since the tool's landscape is TOO COMPLICATED



Challenges Faced by Engineering Leaders Today

Developer Productivity

What are the bottlenecks hampering developer productivity?



Best Practices

What are the best practices adopted by other top teams that I can learn from and start applying?

Code Quality

What are the areas for improving product and code quality?

Velocity

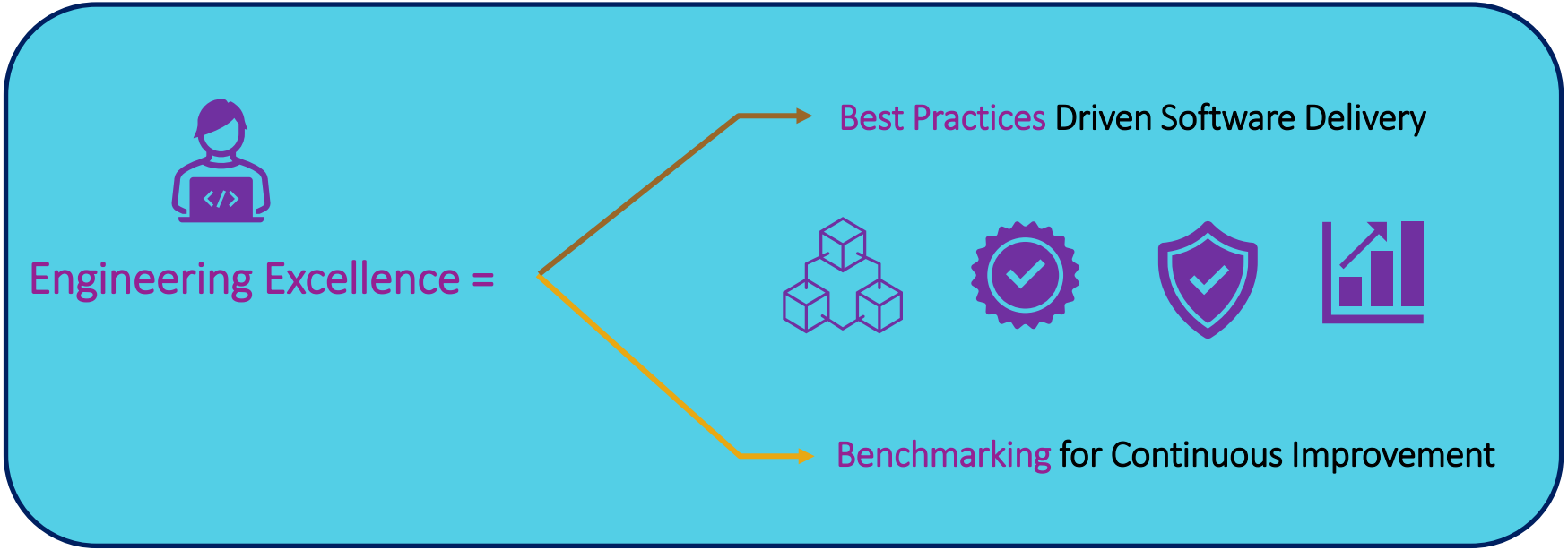
How do I increase feature velocity effectively?

Improve Security

How do I secure my software without choking my developer bandwidth?

What is Engineering Excellence?

1. As an Engineering Team, how can we maximize the Business Value generated?
2. As an Enterprise, how can we Continuously Improve?



Best Practices Driven Software Delivery

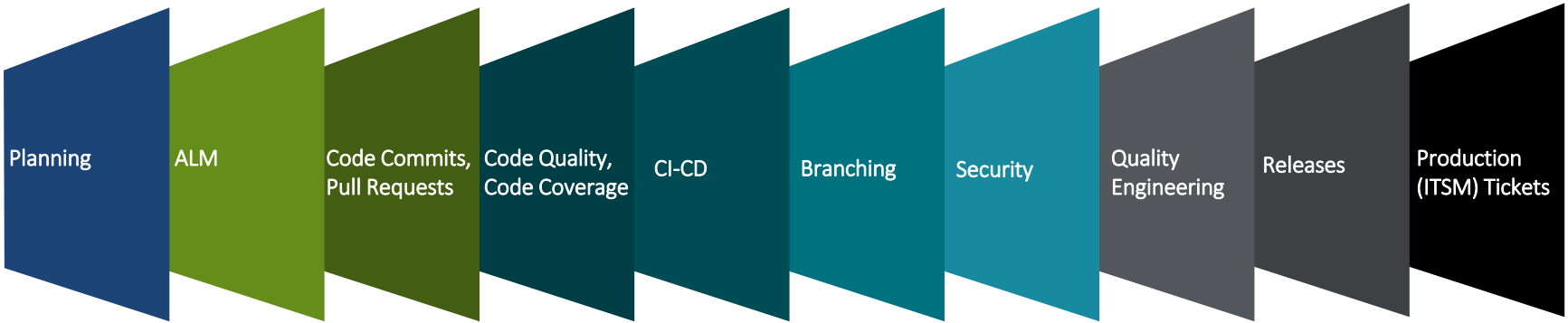
Stories without Assignee
Long Running Stories
Stories without Acceptance Criteria
Stories without Epic and Initiative
Stories without Story Points
Issues with no time tracked

Code Quality Review is performed for all applications
Approved Threshold set for Code Quality Review

CI-CD pipeline has mandatory security testing steps executed
CI-CD pipeline stops when stage gates are not met
CI-CD pipeline has unit test and code quality review

Approved Threshold set for Static Analysis, SCA Scan
Approved Threshold set for Dynamic Analysis
No Code Repository is in public domain
Only approved team members have access to code repos

Static Analysis is performed for every production release
Dynamic Analysis is performed for every production release



Lead Time per Initiative
Initiatives without traceability
Projects not delivering to Commitments
Predictability of Key Initiatives

Commit / Pull Requests contains Story Id
Approved reviewers are included in PR
Approved people provide pull request review comment
Pull requests are approved before merge to master

Feature/Release branches follow naming standards
Branches created only for approved features
Feature branch must be approved before branching out
Release branch branches off develop
Release branch holds required metadata
Hotfix should not take more than five days

Requirements without Test Cases
Test Cases not executed for three months
Test Automation %
Test Effectiveness Rate

Cycle Time on Tickets
Tickets pending for more than 5 days
Assignees with more than 10 active tickets
Tickets pending approval for more than 48 hours

Benchmarking for Continuous Improvement

Function	Key KPIs
Budgeting / Planning	Planned vs Actual, Cost Overrun, Predictability
ALM	Mean Time to Change, Cost of Change, Efficiency, Throughput
Testing	Defect Density, Defect Leakage, Test Effectiveness, Test Failure
CI-CD	CI-CD Maturity, Mean Time to Recovery, Build Failure Rate
Code Commits, Branching, Code Quality	Commit Frequency, Branching Gaps, Code Quality Score
Security	Org Risk Score, Application Risk Rating, SAST / DAST / SCA Score
Compliance	Compliance Score, Top Non-Compliant Items
ITSM	Mean Time to Resolve, Mean Time to Respond

The Art of Enabling Engineering Excellence and DevSecOps

DevSecOps

Today's Security Leaders are up against these Key DevSecOps Challenges

DevSecOps Maturity

How do we Measure the Current Level of DevSecOps Maturity?

Compliance

How do we Guarantee and Prove DevSecOps Compliance?

Standardized DevSecOps

How do we Standardize DevSecOps Across Multiple Agile/Product Teams

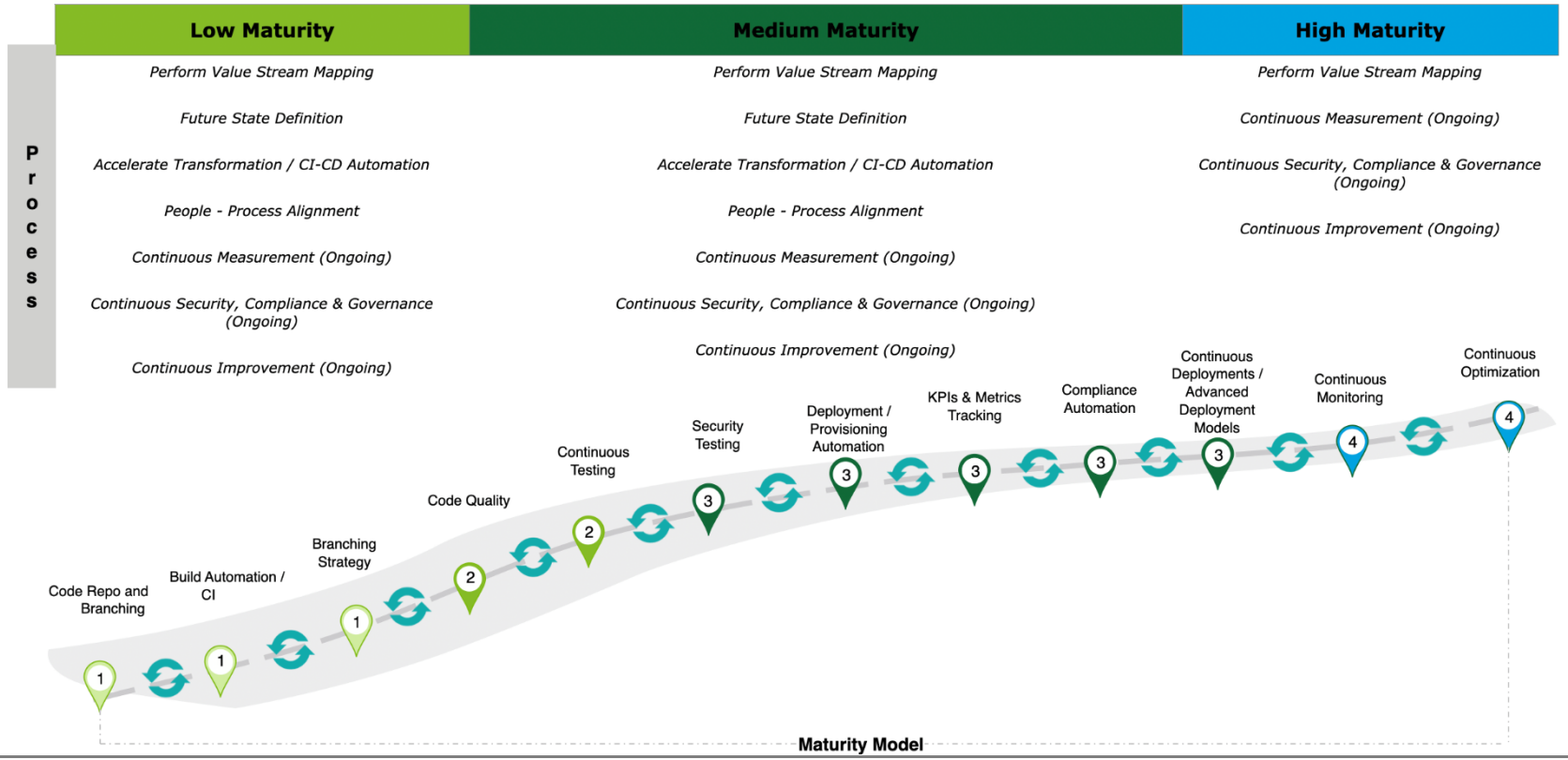
Minimizing Developer Effort

How do we Minimize Developer Efforts on DevSecOps Implementation and Vulnerability Remediation?

Vulnerabilities and Risk

Knowing the Current State of DevSecOps Vulnerabilities and Risk

DevSecOps Maturity Assessment



Generate Insights Across Six Value Domains using KPIs and KRIs

IMPROVED TRACEABILITY

- How do I tag all actions across product delivery to app modules, releases, stories and features? Or How do I tag code commits or Jenkins pipelines or spinnaker deployments to a feature, release or a story.
- How do I perform requirements traceability or visibility on all atomic activities performed across my sprint teams?
- How do I get alerted when a build related to five of my critical stories are failing?

Product Manager / Scrum Master

IMPROVED SPEED TO MARKET

- Who are my top committers across a business unit?
- Are we working on more bugs than new features?
- Why are my delivery timelines off track?
- What are the releases with high lead times?
- What features are contributing to more defects?

Product Manager / Engineering Manager

IMPROVED AVAILABILITY & PREDICTABILITY

- AIOps (AI/ML) Engine
- How do I make sure my CI-CD pipelines are highly/99.95%+ available?
- How do I identify abnormal behavior with pipelines before they become issues?
- How do I identify sudden changes in pipeline executions?

DevSecOps Manager / Engineer

ENHANCED EFFICIENCY

- How do I know when a ci-cd pipeline takes 3x more time than normal?
- How do I improve the efficiency of my product delivery process?
- Am I improving on eliminating waste in my delivery process?
- Who are my top committers across a business unit?

Engineering Manager

CONTINUOUS COMPLIANCE & GOVERNANCE

- How do I ensure adherence to SOX compliance on product delivery or CI-CD?
- How do I make sure there is segregation of duties in my release process?
- How do I make sure business owner approval is received for every release?
- How do I know when a standard code quality threshold is used for a particular release?
- Do we perform vulnerability assessment for critical apps every month?

Compliance Officer / Internal IT Audit

REDUCED CHANGE FAILURE RATE

- How do I avoid bad practices with source code management?
- How do I measure change failure rate on a per release basis?
- What is causing sudden spike in customer tickets?
- Are we deploying high quality builds with frequent commits?
- Are we improving with code coverage?
- Am I following industry best practices on branching strategy?
- Which of my CI-CD pipelines have high failure rate?
- How do I know when there is sudden spike in code smells for a particular feature?

QA Manager

DEV SEC OPS DAYS

The Art of Enabling Engineering Excellence and DevSecOps

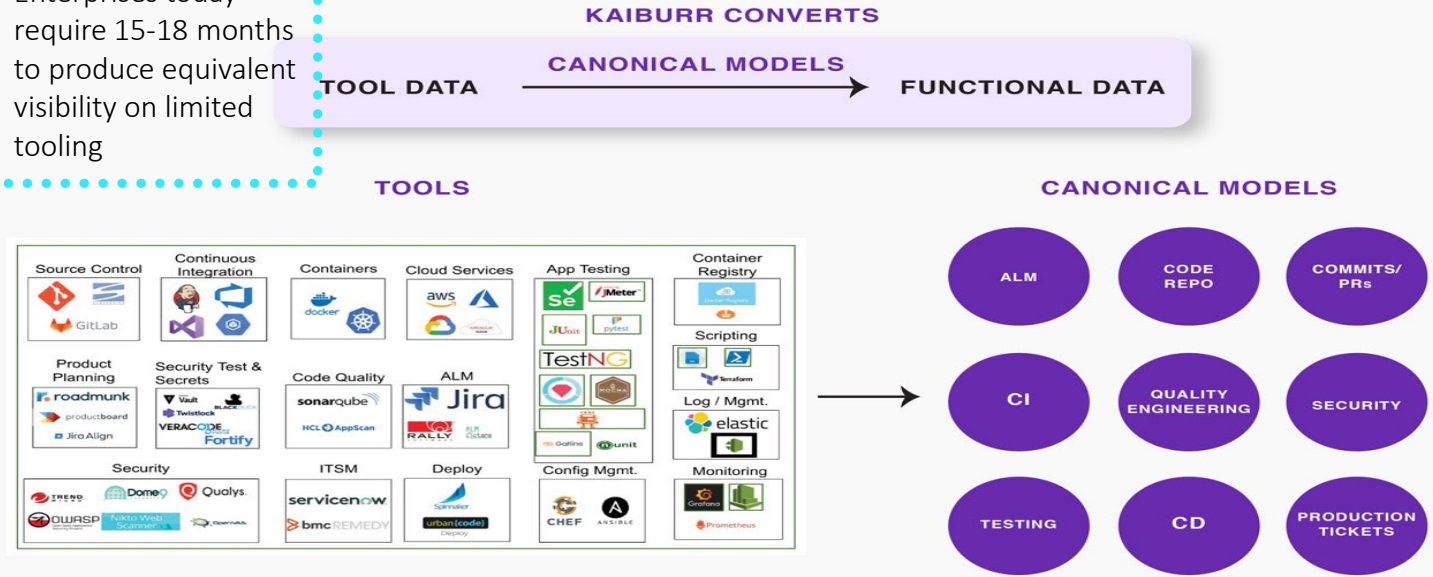
Use Cases

Enabling the Art of Engineering Excellence and Matured DevSecOps

AllOps Simplification

Kaiburr Eliminates the Complexity by Simplifying the Communication

- Enterprises today require 15-18 months to produce equivalent visibility on limited tooling



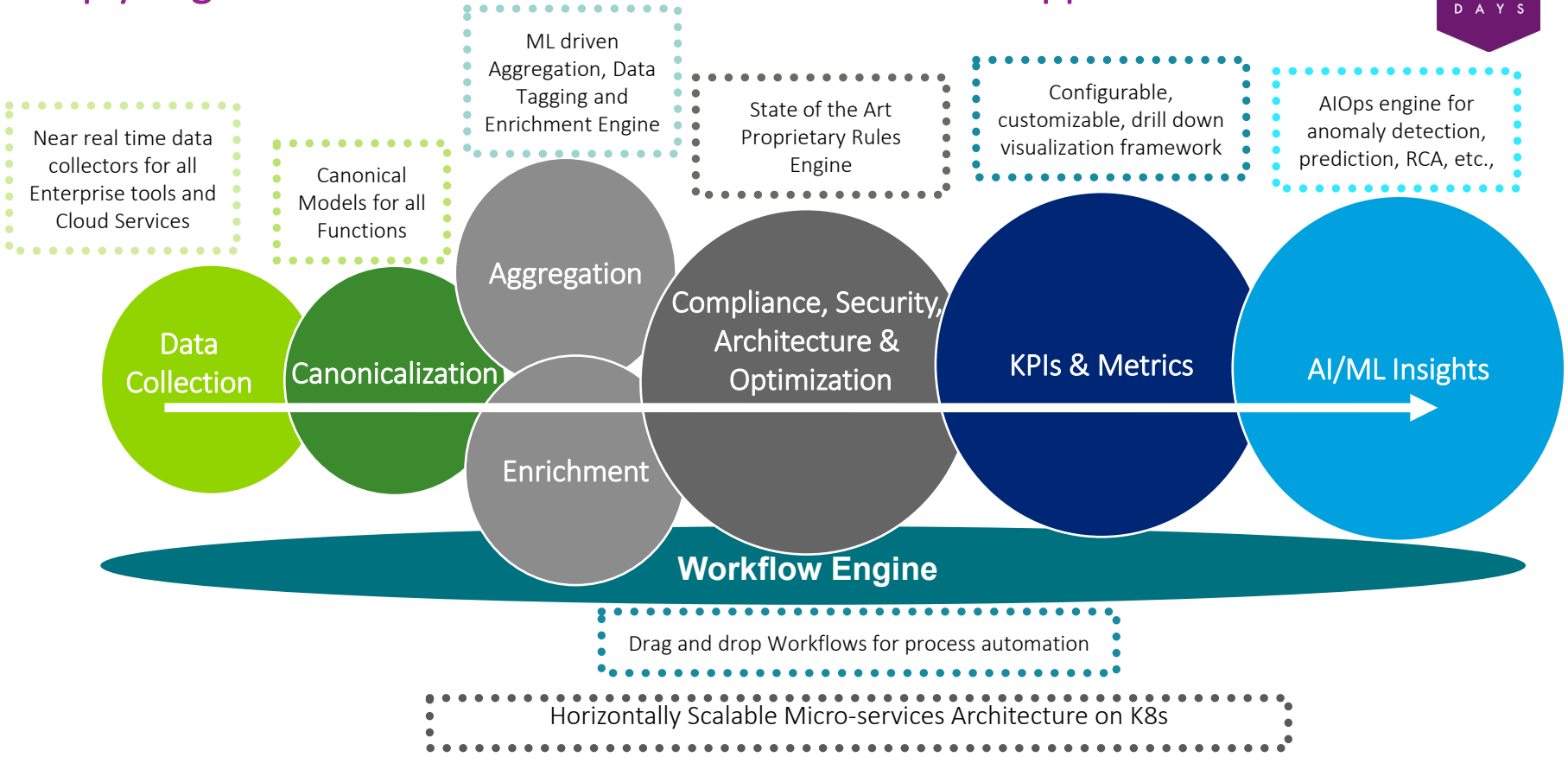
Key Benefits:

1. Visibility & Benchmarking for Leaders
2. Single Pane for Developers & Teams
3. Atomic validation of controls & best practices
4. Low Code DevSecOps Automation

- Out of the box insights using 1, 2 and 3 for Enterprise Customers in days

And more importantly enabling abstraction, so customers talk the functional language instead of tool specific language

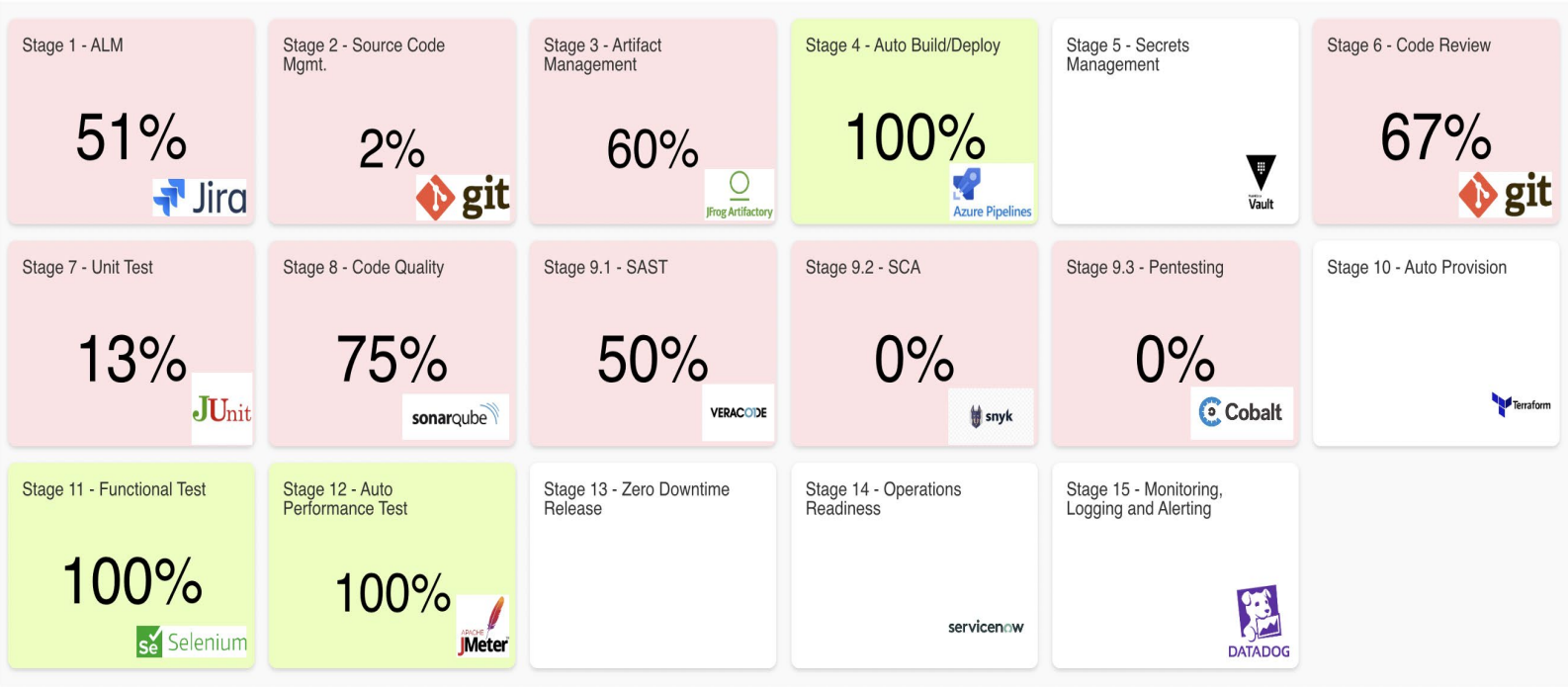
Deeply Engineered Framework makes this SIMPLICITY Happen



The Art of Enabling Engineering Excellence and DevSecOps

ALM Stage Gate Governance

Shift Security Left Effectively with near real-time Visibility and Governance



80% Sec. Incident Reduction

20% Productivity Gain

24% Improved Quality

Use near real time view of stage gates through the lifecycle of software delivery at the org, business unit and application level

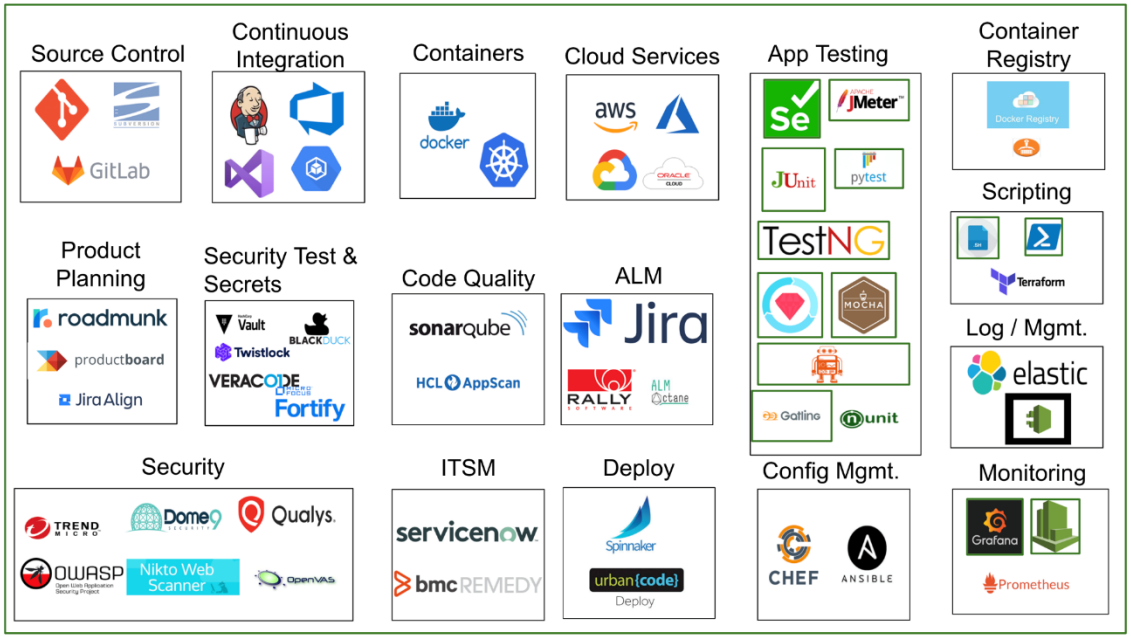
Big Picture of Enabling Engineering Excellence and DevSecOps

60+ Tools Integrated

200+ Cloud Services Enabled

100+ Design Best Practices

1200+ Data Points Canonicalized



600+ APIs Integrated

500+ Security Policies

20+ AI/ML Models

350+ KPIs & KRIs

Contact Information

Presenter
Vishy Mahadevan
Chief Technology Officer

Contact
Optimx LLC
Monrovia, MD
Phone: 703-975-8137
Web: optimx.us
Email: vishy@optimx.us

Experienced Technology and Business Leader supporting CIO, CDO and CTOs on Digital Transformation, Enterprise Data Management, Business & Technical Architecture, DevSecOps, Product Management, Emerging Trends, and Innovation.