



# Software security at the speed of DevOps

# DevSecOps requires a platform

**“There’s an app for that.”**

# How to ensure software security at DevOps speed

Embrace DevOps technology & culture:

**1. Multiple automated security tools,  
integrated with CI/CD pipeline**

**2. Processes for working with security  
warnings & development teams**

**3. Learning and continuous improvement  
of effectiveness and efficiency**

# Presenter



## **Chris Horn**

Software Security R&D

Software security product research & development

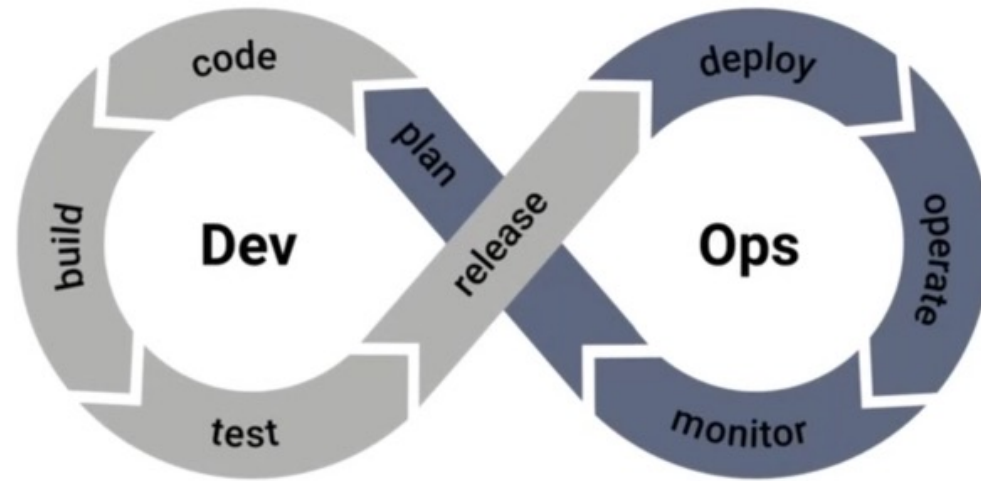
20-year career spanning cybersecurity R&D, product strategy, systems engineering, interaction design, and user experience research

- U.S. Department of Homeland Security (DHS)
- Defense Advanced Research Projects Agency (DARPA)
- RAND Corporation
- General Dynamics
- Johns Hopkins University Applied Physics Lab
- U.S. Navy
- RSA
- Code Dx

# DevOps

Delivering software  
quickly

# DevOps allows teams to deliver software quickly



DevOps is enabled by:

## 1. Technology

Integrated toolchain yields speed

Testing automation maintains quality

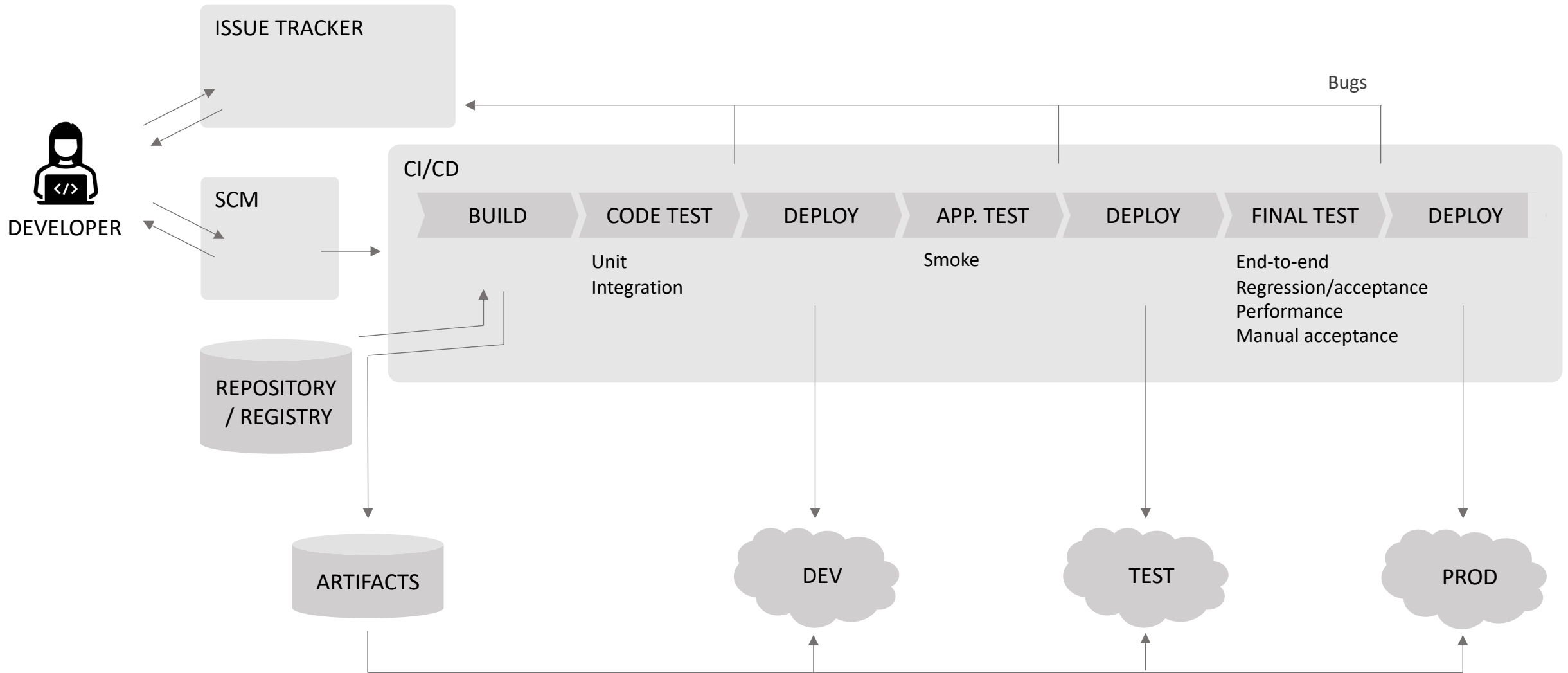
Issue tracker coordinates & measures

## 2. Culture

Learning through iteration

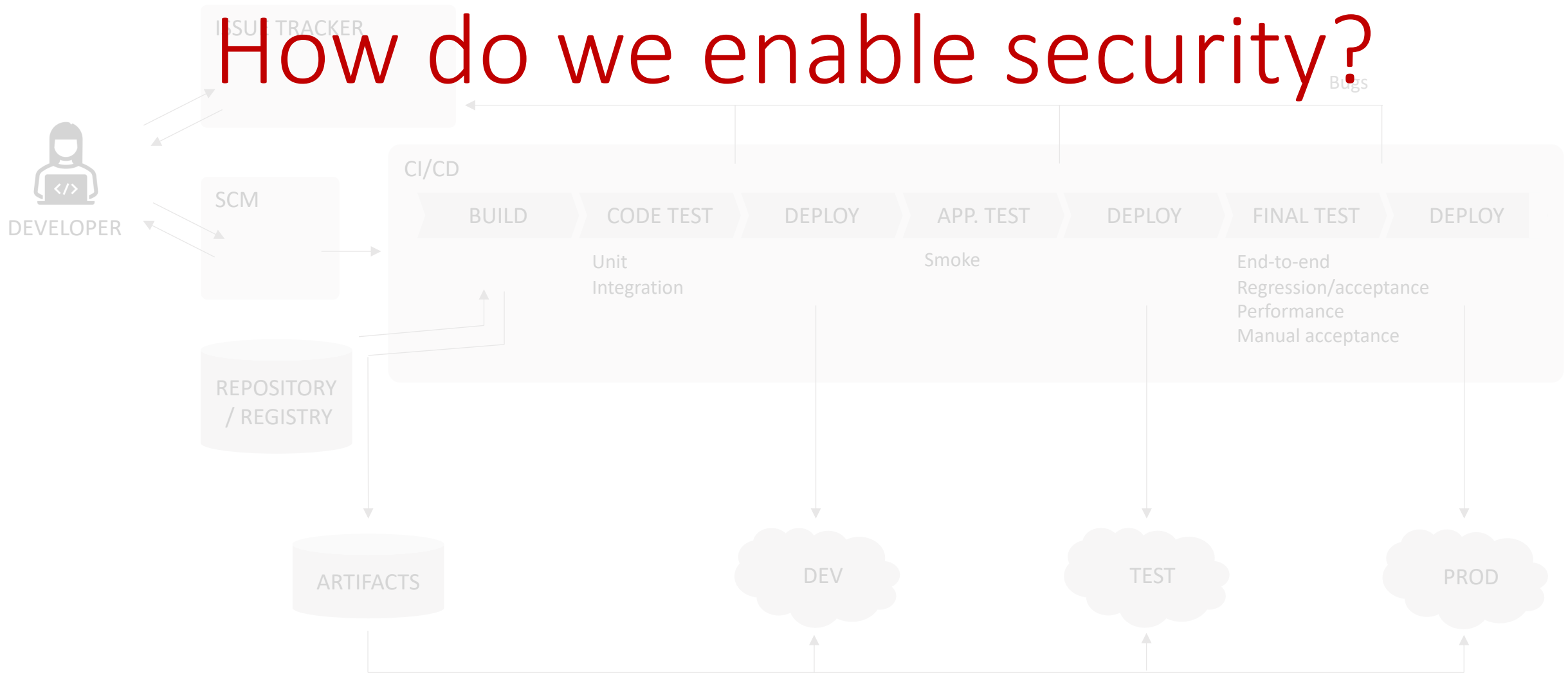
Learning through measurement & feedback

# Typical CI/CD pipeline



# Typical CI/CD pipeline

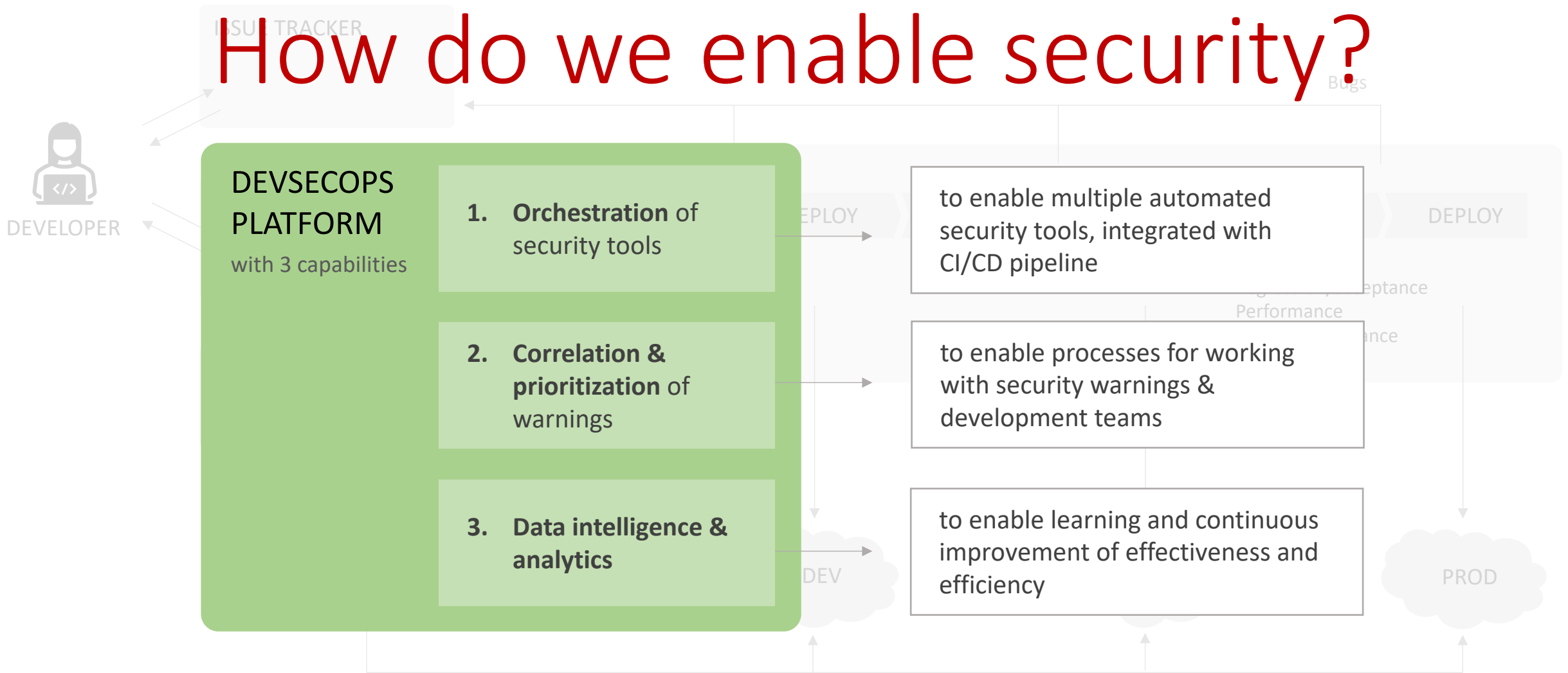
## How do we enable security?





# Typical CI/CD pipeline

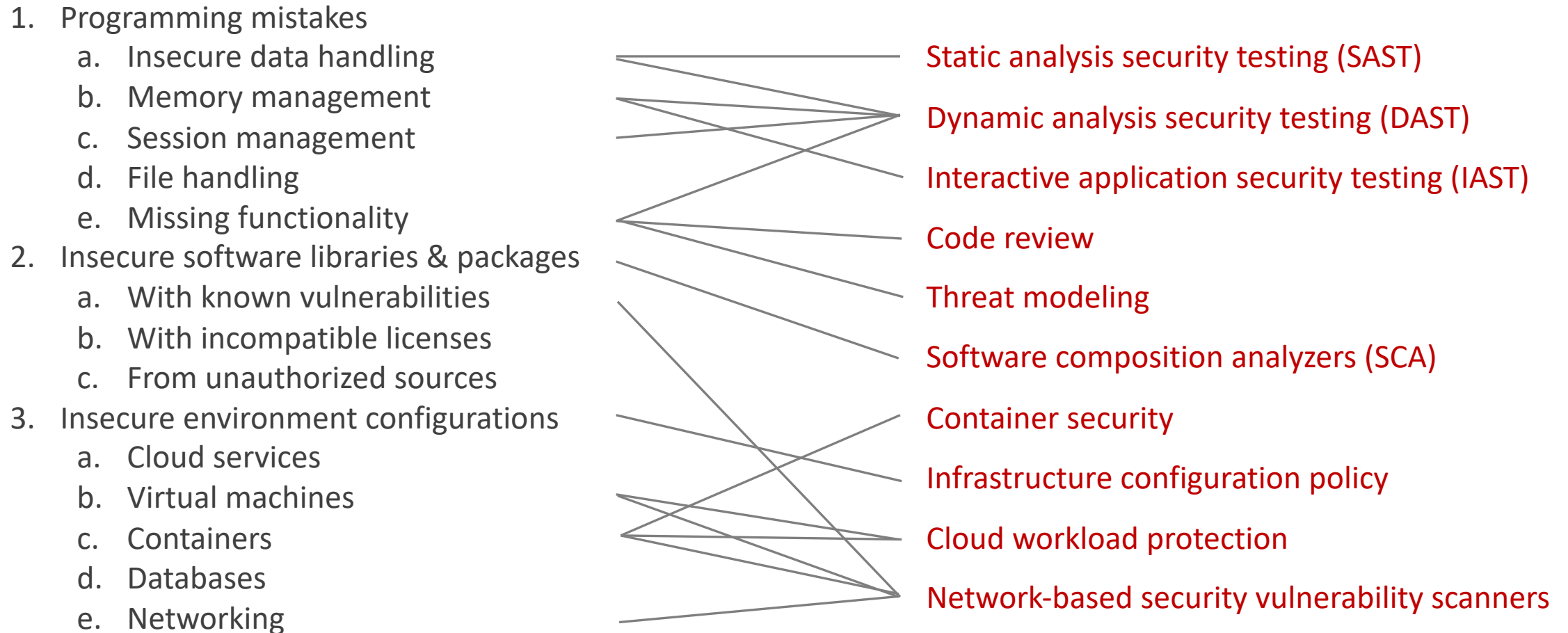
## How do we enable security?



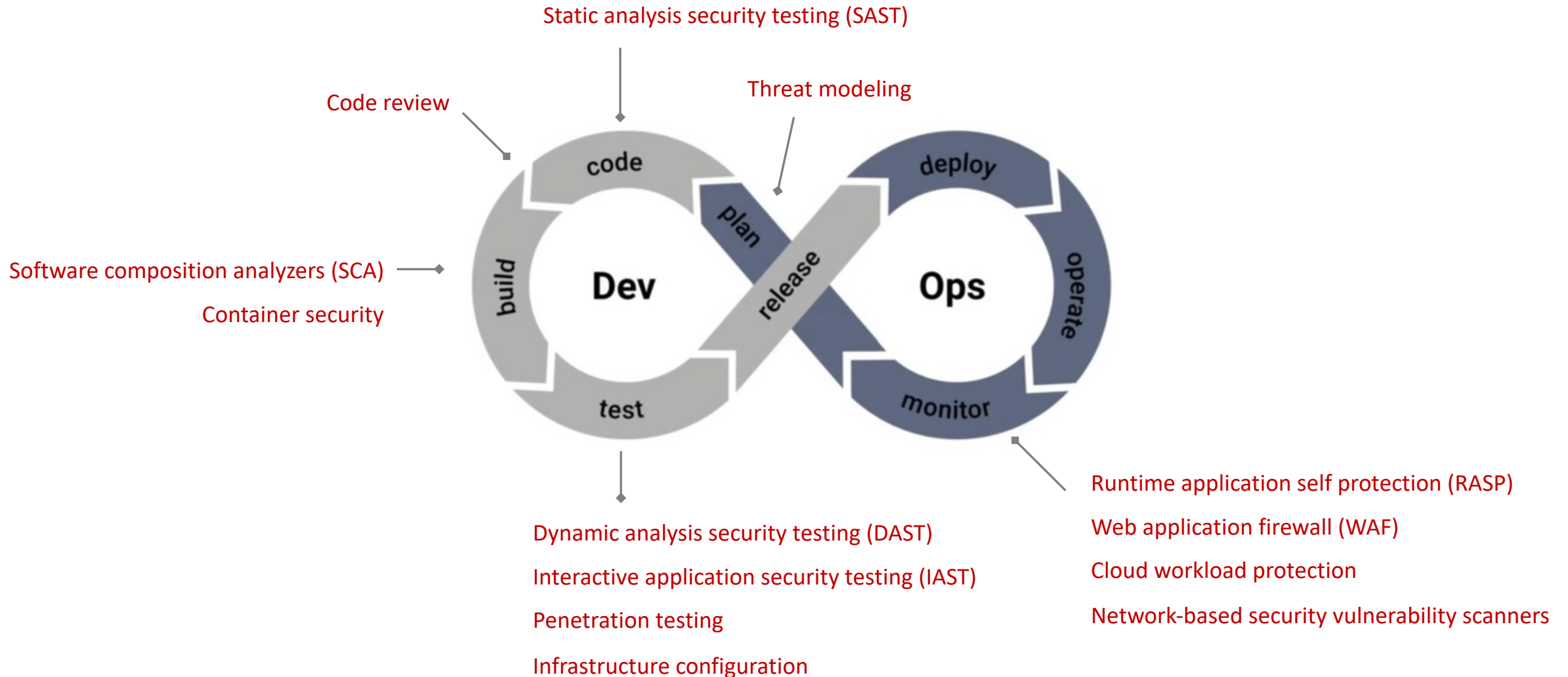
# Multiple automated security tools

Keep pace with  
development and  
find different types of  
security problems

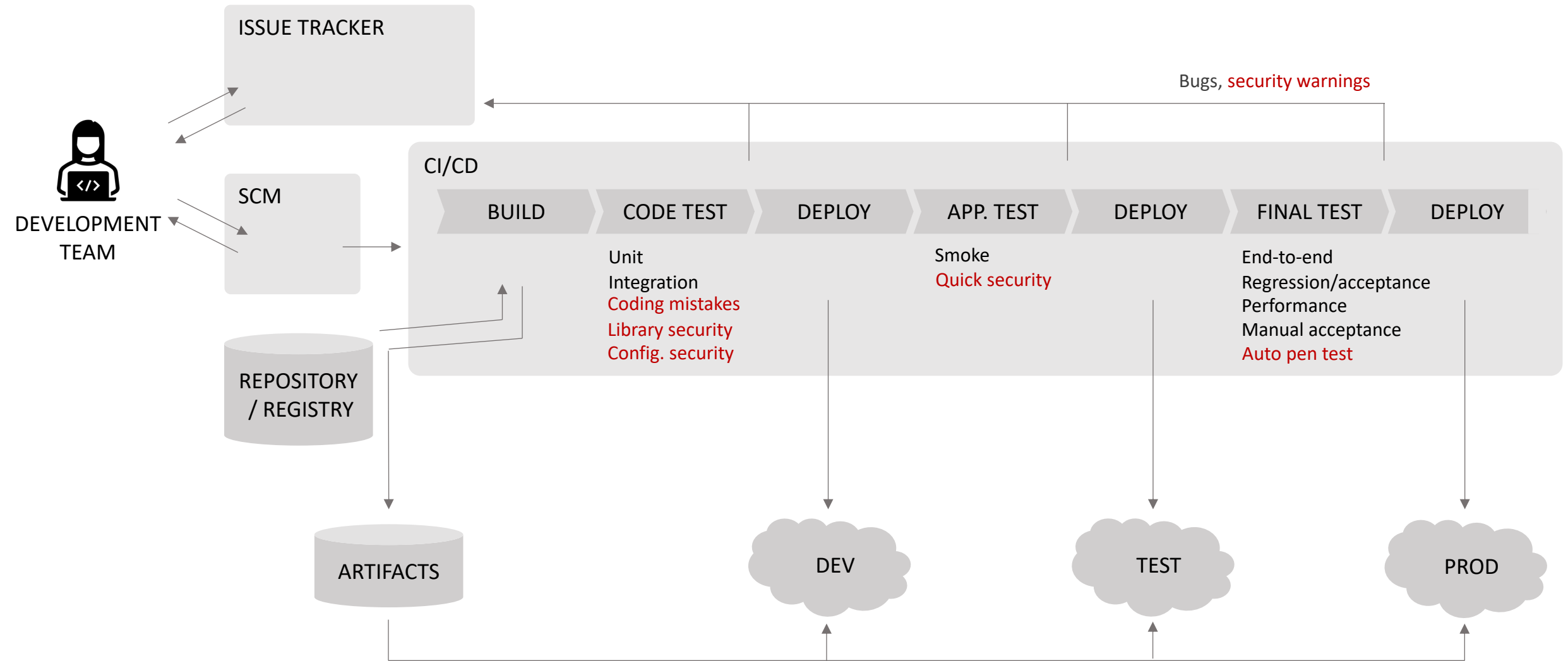
# Security requires multiple tools



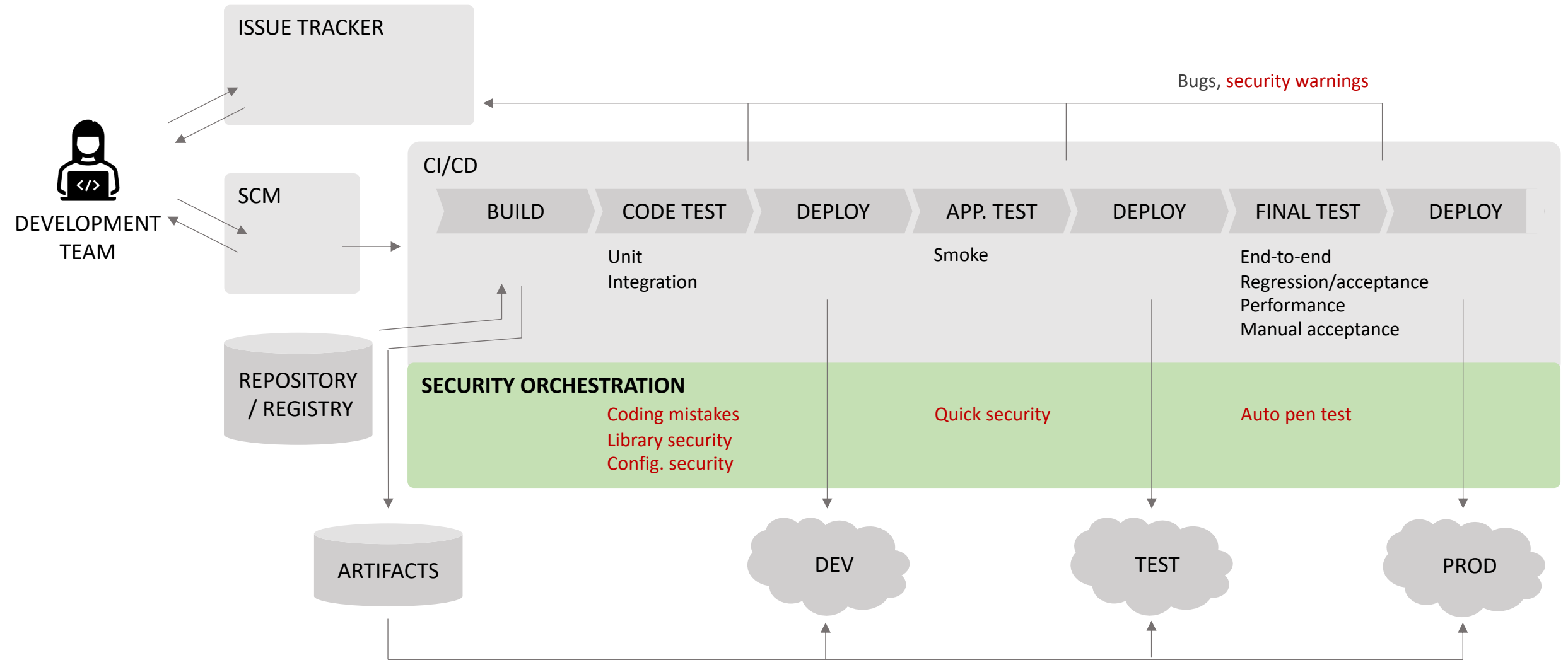
# Tools must be applied throughout lifecycle



# Tools must be applied throughout CI/CD pipeline



# Security orchestration products simplify security tool integration into CI/CD pipeline

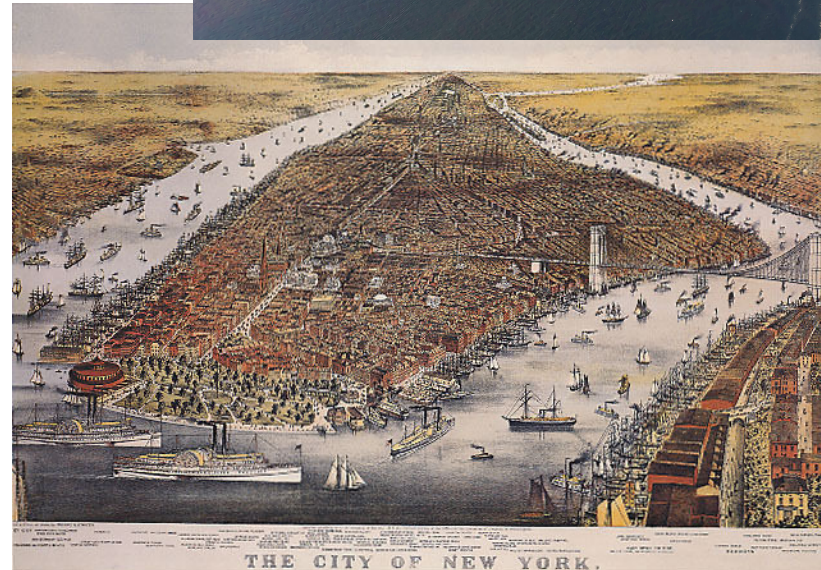




# Platform to support your evolution

Software security programs are built over time, iteratively adding assets and capabilities:

1. Onboard projects/teams
2. Mature security practice
  - a. Enable new checkers after teams fix issues
  - b. Add security tools incrementally over time



# Orchestration capability simplifies security tool integration into CI/CD pipeline

Key functionality:

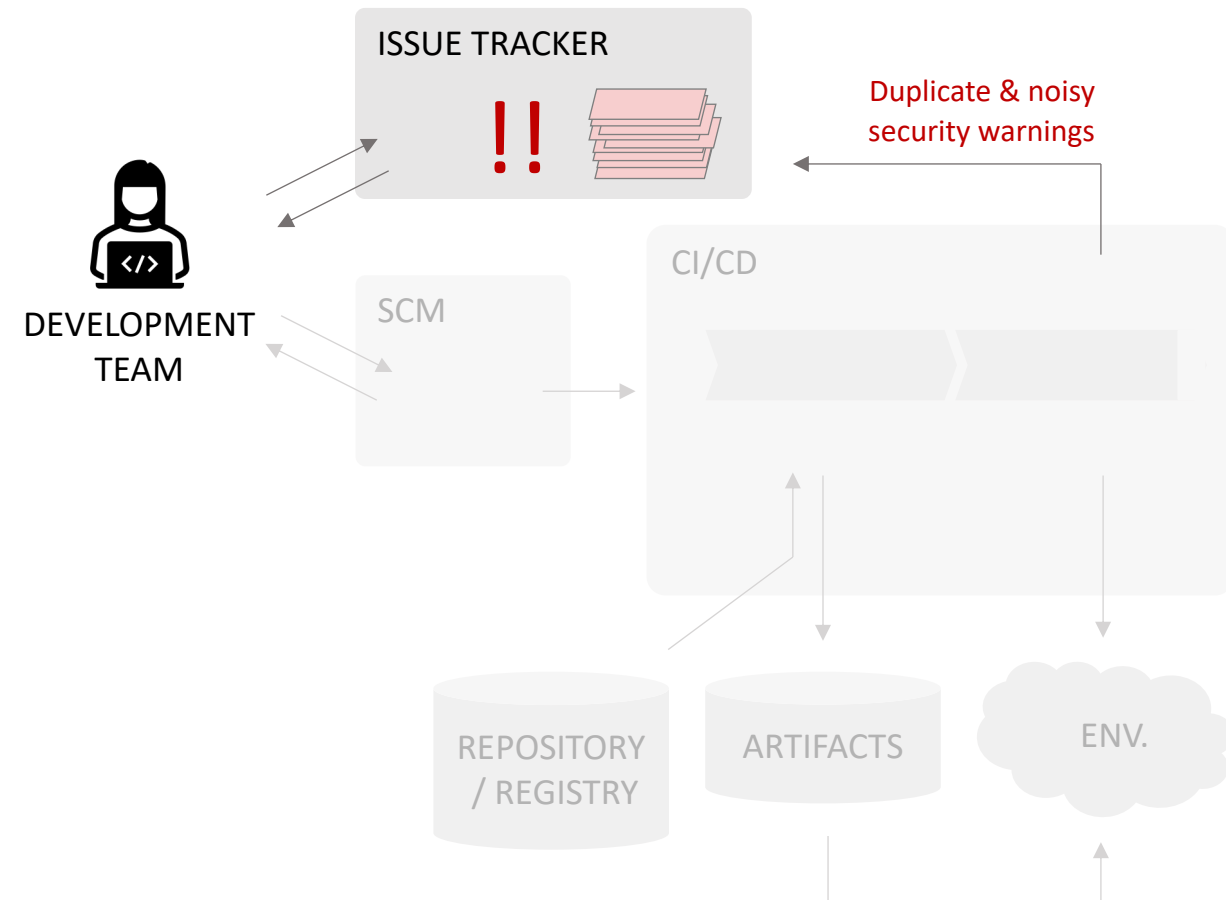
1. Execute correct security tools
2. Centrally-manage tool scan configurations
3. Normalize tool warnings into one format/nomenclature
4. Maintain integrations with security tools as they evolve



# Processes for working with warnings & development teams

Focus on risk and ensure security issues are fixed

# Noisy and duplicate security warnings can clog issue tracker



Security warnings can pile up in issue tracker

- Frustrates development teams
- Hides high-risk issues



1 warning

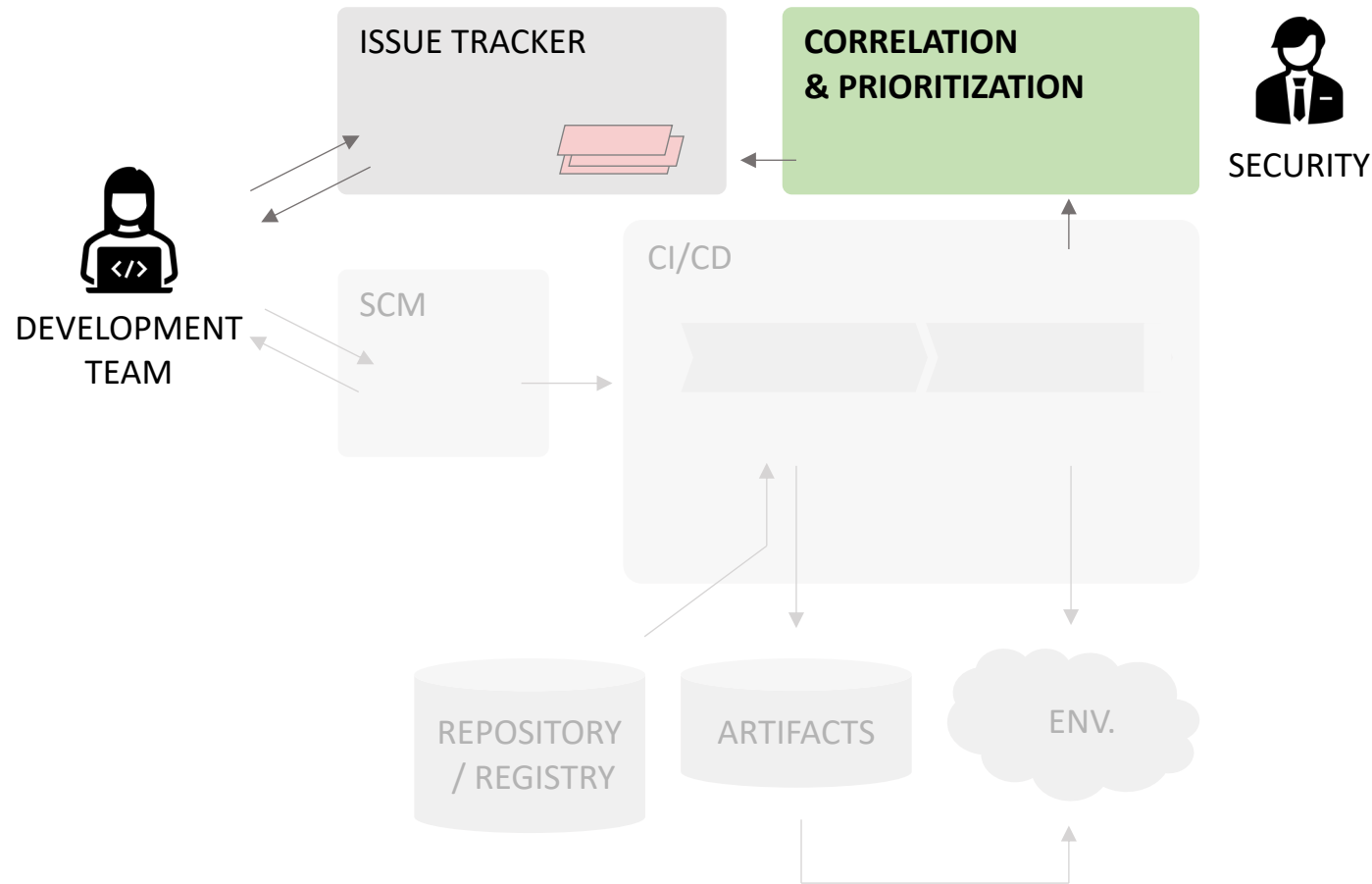


10 minutes to review

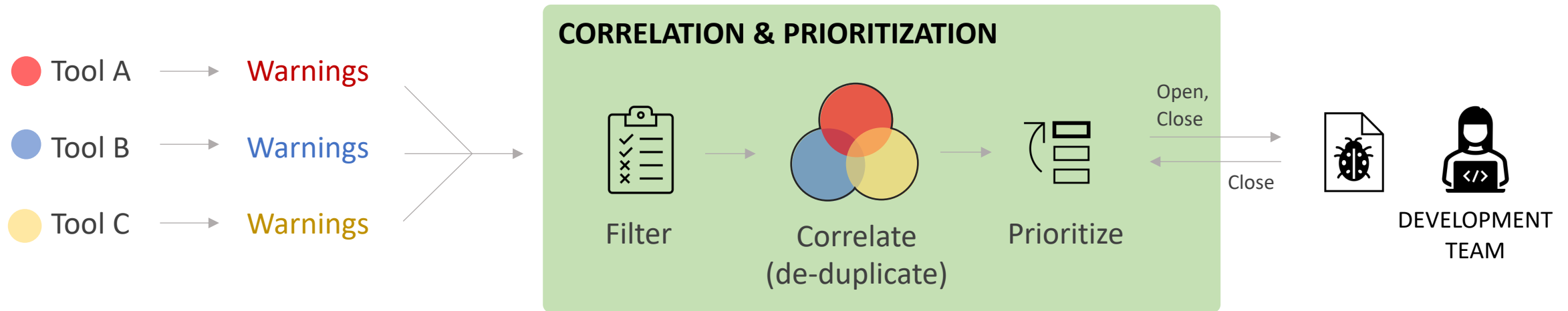


\$11.36 per warning reviewed

# Correlation & prioritization capability can minimize noisy and duplicate warnings






# Correlation & prioritization functionality saves time and relationship with development team



## Key functionality:

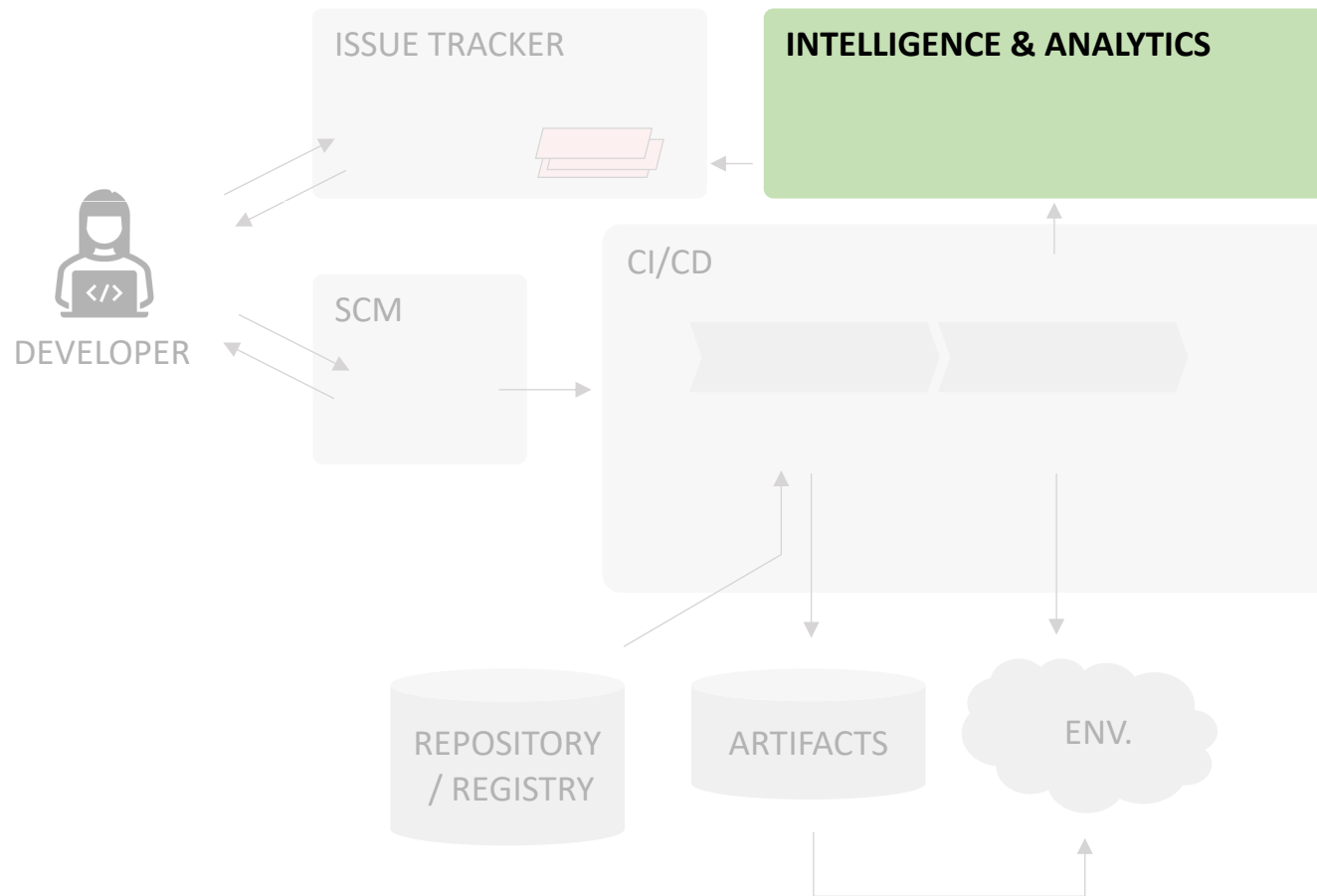
- Filter out false positives using AI or ML
- Correlate duplicate warnings
- Prioritize high-risk warnings
- Automatically close fixed defect issues
- Integrates with issue tracker

	10,000 warnings
	50% reduction
	Saves \$56,800 6 months

# Data intelligence & analytics

Single source of truth  
to support learning  
and future automation

# Intelligence & analytics supports multiple needs



  
SECURITY, COMPLIANCE,  
ENGINEERING

Measurement & reporting supports:

- Compliance reporting
- Process efficiency
- Tool effectiveness
- Continuous improvement

Historical data supports:

- Future automation

# Measurement & reporting supports learning

## Software Assets

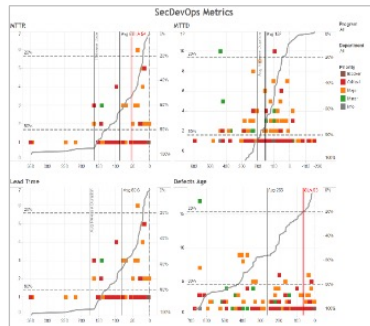
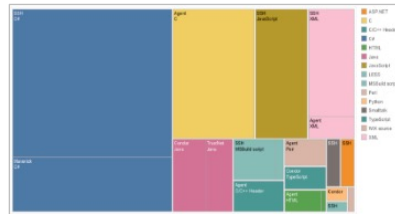
Application Business Value  
Software Security Coverage

## Codebase Inventory

Source Lines of Code (SLOC)  
Source Lines of Code by Language  
Source Lines of Code Change (churn)

## Software Security Risk

Security Technical Debt  
Mean Vulnerability Age  
Security Risk Exposure  
Security Risk Density  
Application Risk Score  
Weighted Risk Index



## Software Risk Reduction

Security Technical Debt Change  
Vulnerability Open Rate  
Vulnerability Escape Rate  
Vulnerability Resolved Rate



## Secure Engineering

Opened To Resolved Ratio  
Re-Opened To Opened Ratio  
Passed Security Gates Ratio



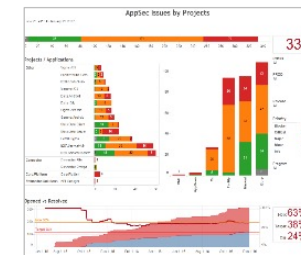
## DevSecOps Speed

Mean Time In Production  
Mean Time To Detect  
Mean Time to Resolve (MTTR)



## DevSecOps Performance

Shift-Left Detection Ratio  
Failed Security Pipelines Ratio  
Scans in Queue Time  
Security Scan Time





# Recap

Three focus areas and  
enabling technology

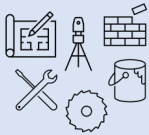


# DevSecOps requires a platform

“There’s an app for that”

**Gartner** calls solutions Application Security Orchestration and Correlation (ASOC)

Build



- ✓ Full control and customization
- ✗ High up-front cost to build
- ✗ Months of up-front delay until useful
- ✗ Dedicated staff required to maintain
- ✗ Little additional competitive advantage

Buy



- ✓ Customization & integration flexibility
- ✓ Zero cost to build
- ✓ Short integration and set up
- ✓ Maintenance updates & features
- ✓ Efficient secure software development

# How to enable software security at DevOps speed

Embrace DevOps technology & culture:

**1. Multiple automated security tools,  
integrated with CI/CD pipeline**



enabled by **orchestration** of security tools

**2. Processes for working with security  
warnings & development teams**



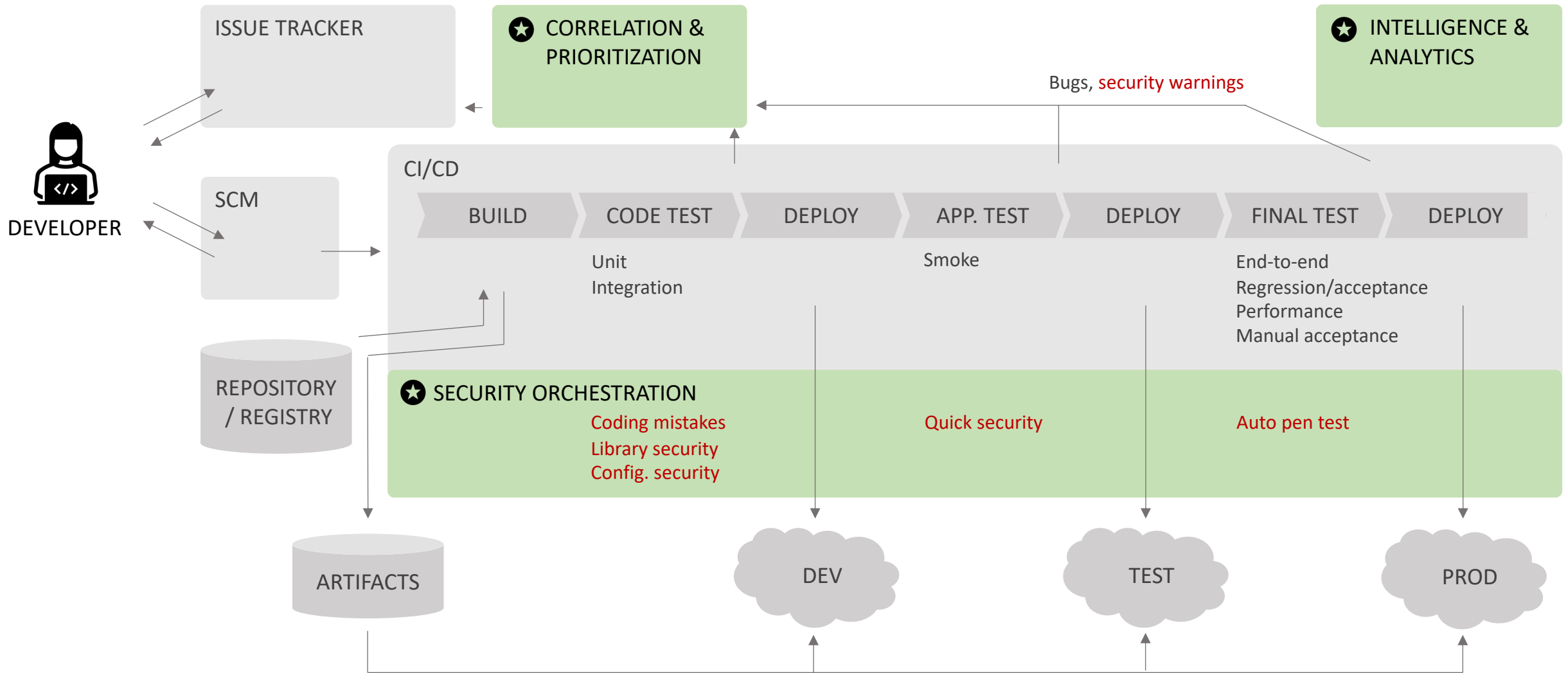
enabled by **correlation & prioritization** of warnings

**3. Learning and continuous improvement  
of effectiveness and efficiency**



enabled by data **intelligence & analytics**

# DevSecOps requires a platform with 3 capabilities



**Plug and play Sec into DevOps with Maverix**

**Thank You**

Maverix Inc.  
10900 NE 4th St Unit 2300, Bellevue, WA 98004

[info@maverix.ai](mailto:info@maverix.ai)  
<https://maverix.ai/>