SYNOPSYS®
Silicon to Software™

Cracking the Code of DevSecOps: Intelligent Orchestration and Code Dx

Build secure, high-quality software faster

Meera Rao
Senior Director (DevOps Solutions)
Synopsys Software Integrity Group

About me

Twitter: @MeeraRRao

LinkedIn: MeeraSubbarao

Email: mmeera@synopsys.com

Application security challenges

Application security is not keeping pace with DevOps

“We’re sprinting”
—Developers

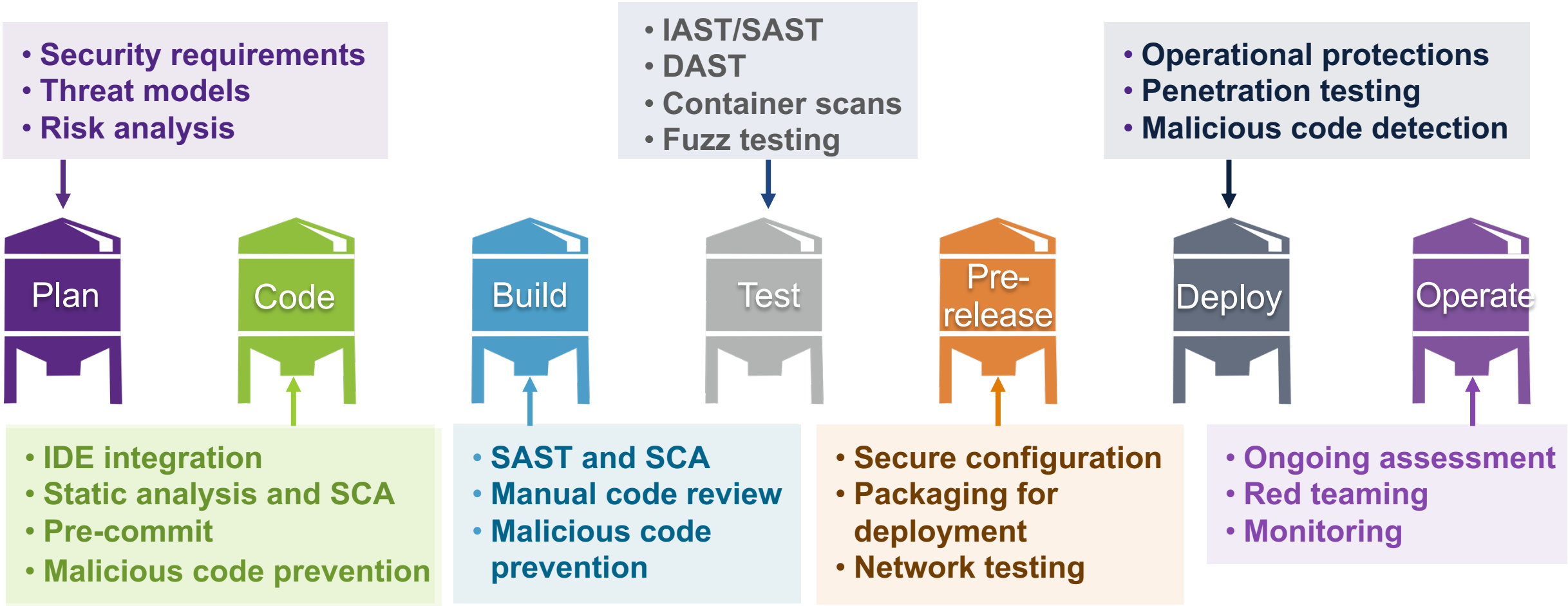
“Not so fast”
—AppSec

“We can’t wait”
—Developers

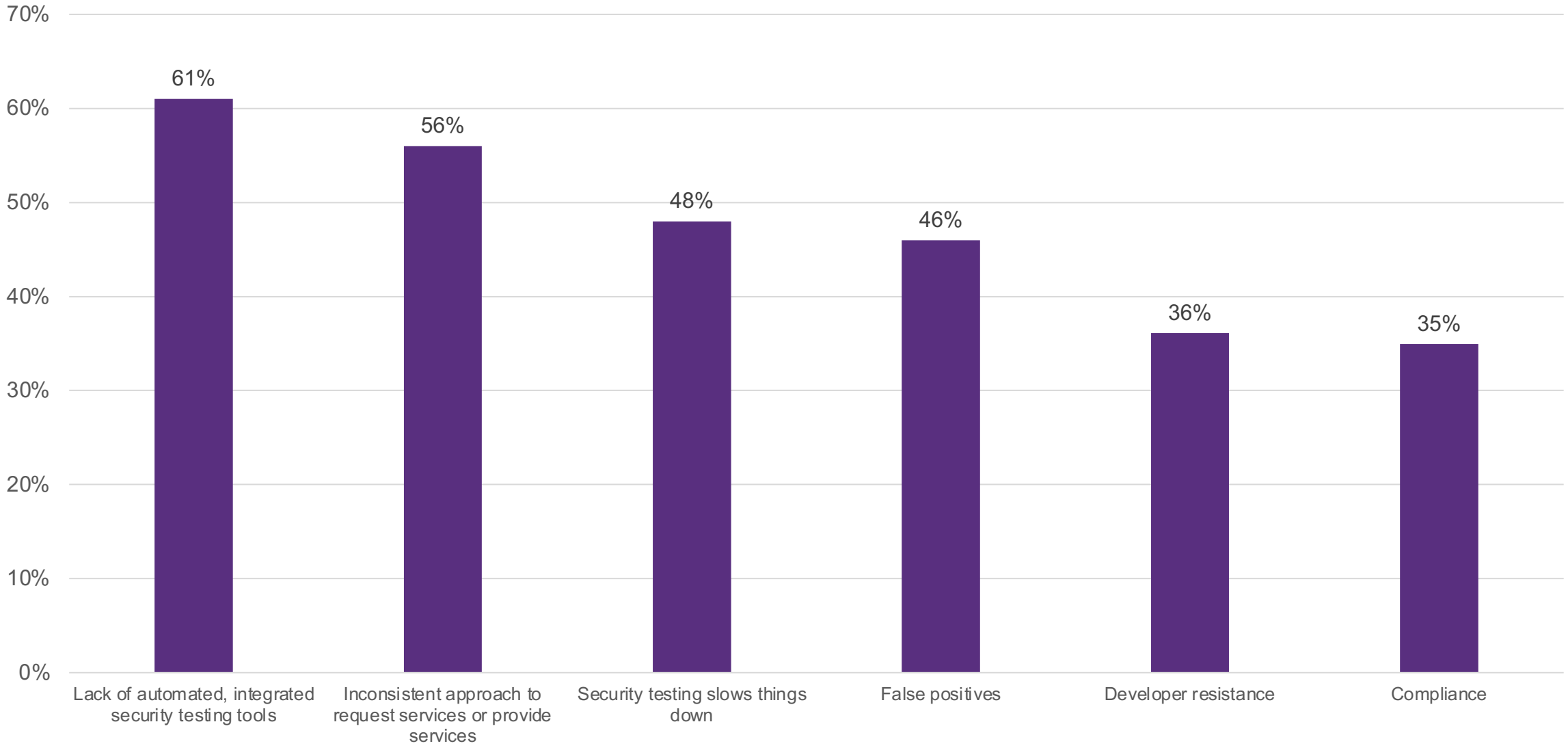
Insecure Software

Traditional AppSec testing is siloed

Siloed testing done at different points in the SDLC makes it difficult to identify the highest priority software security risks



Challenges of security in CI/CD workflows



Q: What are the most significant application security testing challenges inherent in CI/CD workflows?

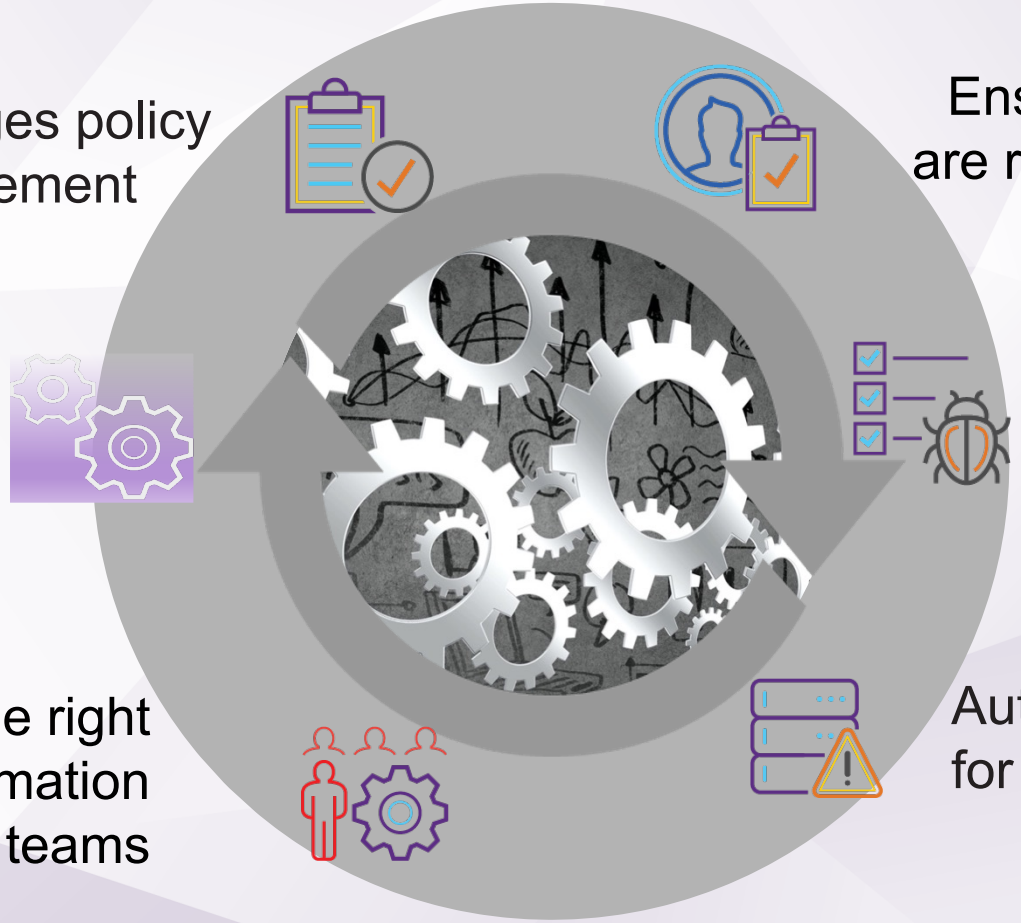
Intelligent Orchestration and Code Dx: A Modern Approach to AppSec

Intelligent Orchestration: Key features

Manages policy enforcement

Ensures the right tests are run at the right time

Tool agnostic



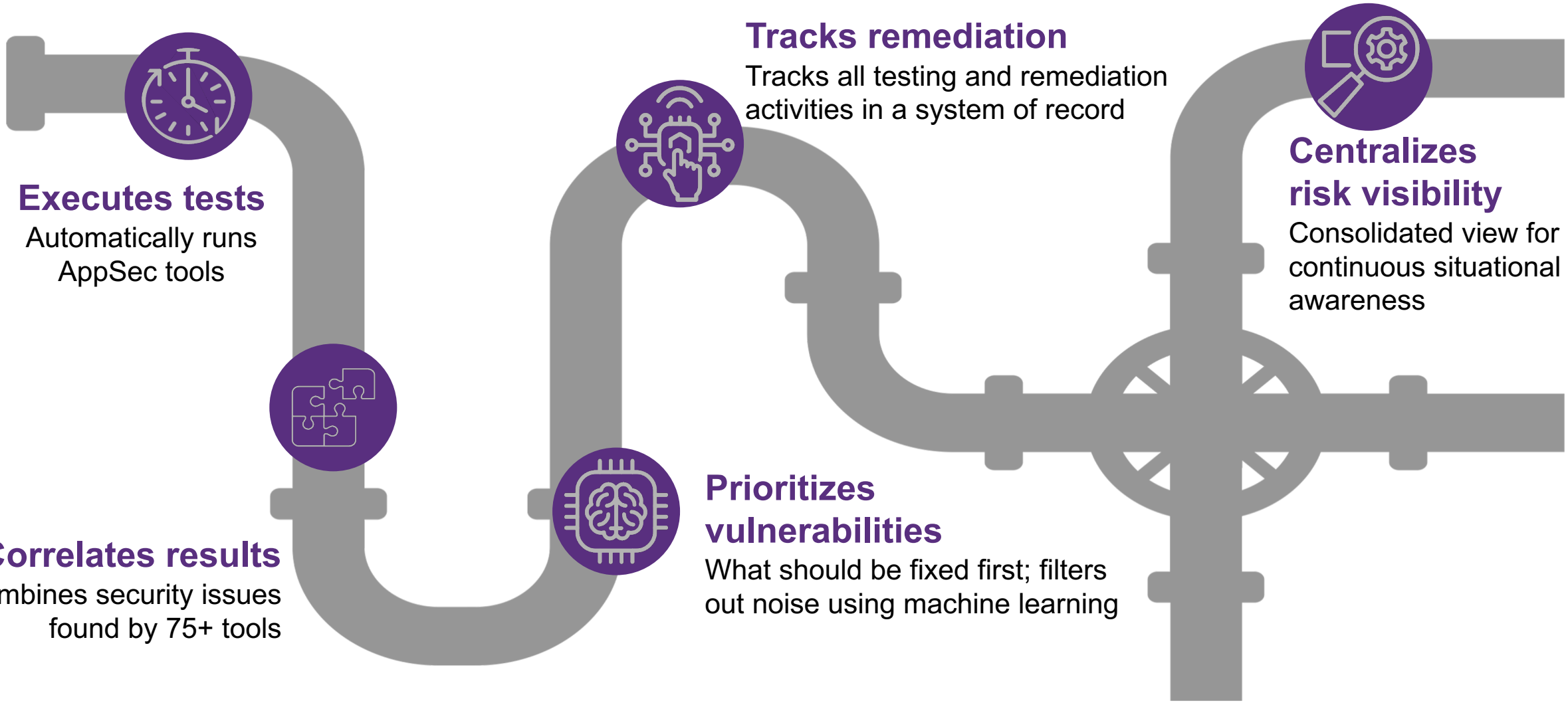
Manages issue prioritization and filtering

Delivers the right information to the right teams

Automates the workflow for manual activities

Code Dx: Key features

Fits seamlessly into Intelligent Orchestration pipeline



Executes tests
Automatically runs AppSec tools

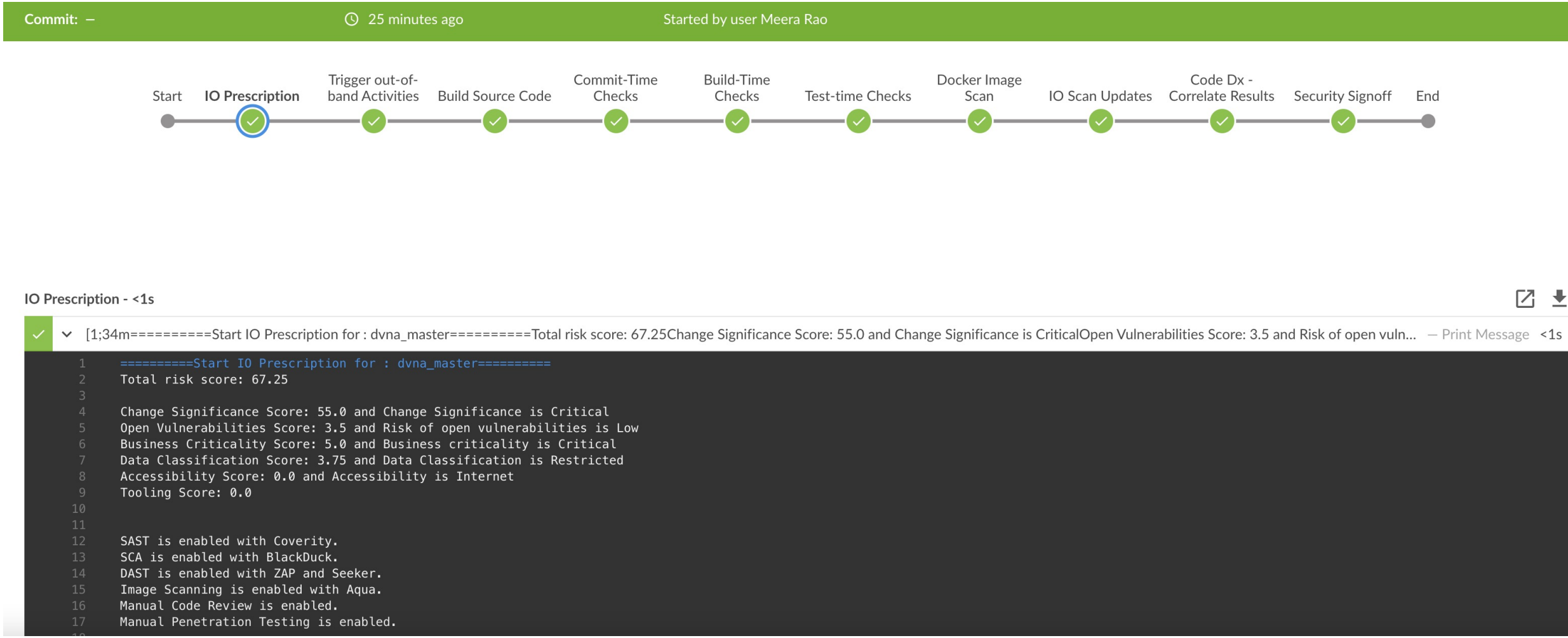
Correlates results
Combines security issues found by 75+ tools

Prioritizes vulnerabilities
What should be fixed first; filters out noise using machine learning

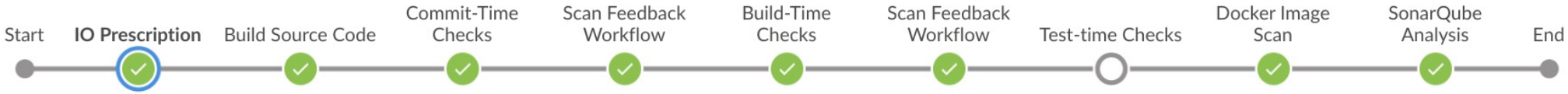
Tracks remediation
Tracks all testing and remediation activities in a system of record

Centralizes risk visibility
Consolidated view for continuous situational awareness

Intelligent Orchestration : Synopsys tools



Intelligent Orchestration : Open source tools

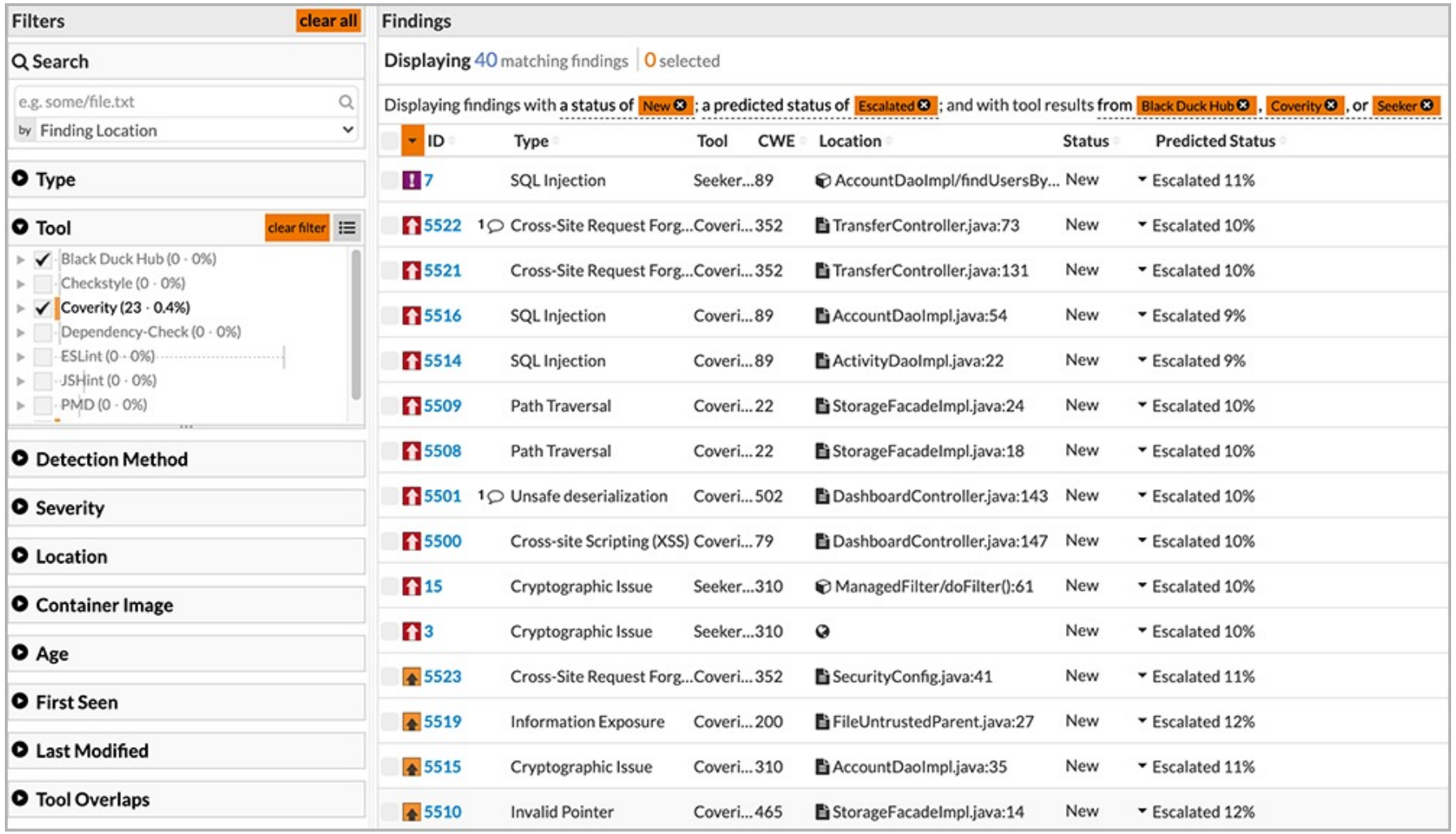


IO Prescription - <1s

[1;34m==========Start IO Prescription for : SampleIO==========Total risk score: 54.5Change Significance Score: 3.0 and Change Significance is LowOpen Vulnerabilities Score: 1.5 and Risk of...

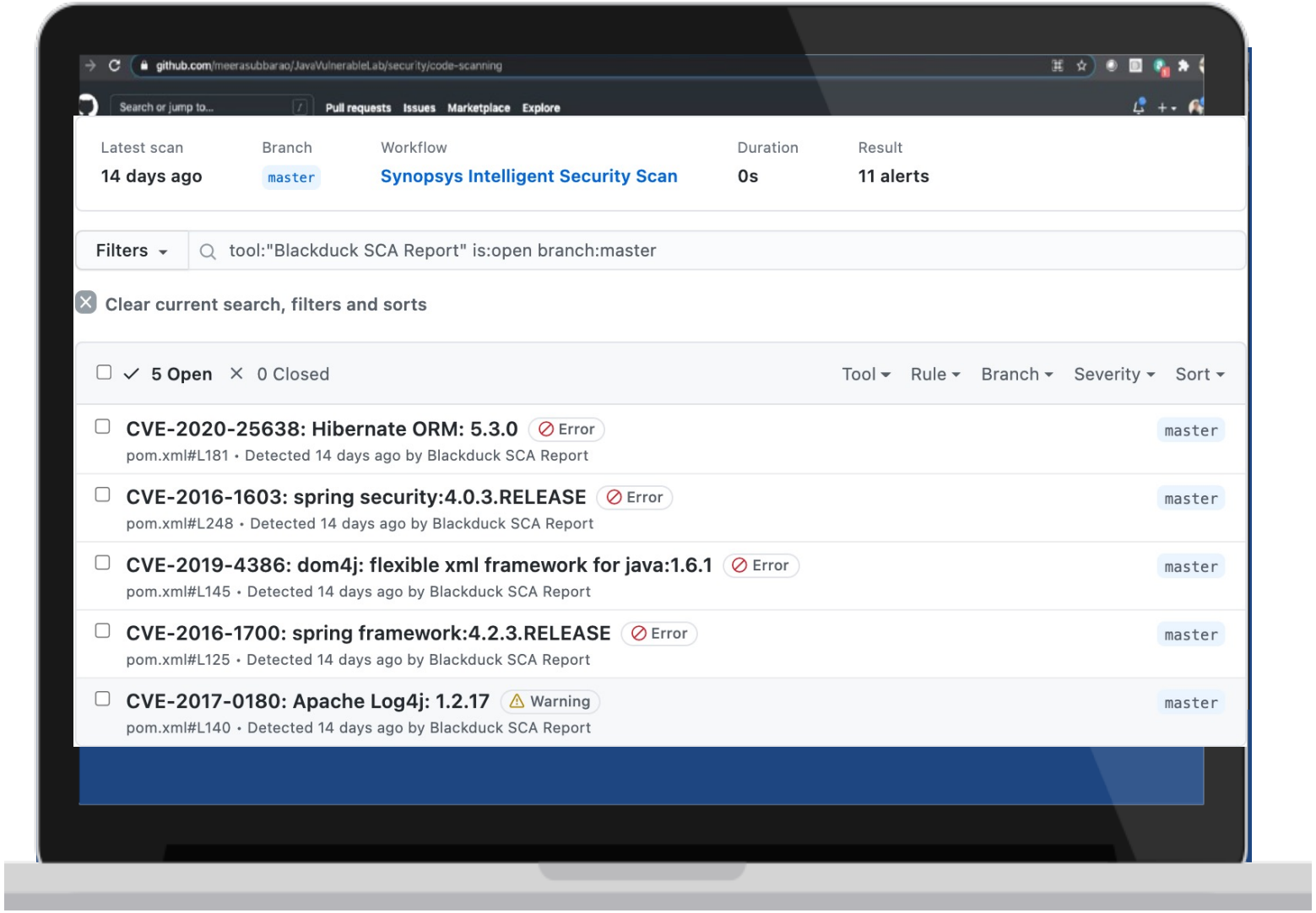
```
1   ==========Start IO Prescription for : SampleIO==========
2   Total risk score: 54.5
3
4   Change Significance Score: 3.0 and Change Significance is Low
5   Open Vulnerabilities Score: 1.5 and Risk of open vulnerabilities is Low
6   Business Criticality Score: 20.0 and Business criticality is Critical
7   Data Classification Score: 15.0 and Data Classification is Restricted
8   Accessibility Score: 15.0 and Accessibility is Internet
9   Tooling Score: 0.0
10
11
12  SAST is enabled with SpotBugs.
13  SCA is enabled with OWASPDC.
14  DAST is disabled.
15  Image Scanning is enabled with Aqua.
```

Code Dx : Synopsys and Open source Tools



Intelligent Orchestration: Delivers the right information

GitHub actions support



Intelligent Orchestration: Avoids defects overload

```
1   Build is about to fail, as the following build breaker criteria matched with scan results:
2   SAST found:
3    Overall: [filesystem path, filename, or uri manipulation, cross-site scripting, sql injection, resource leak, thread
    unsafe modification in singleton, cross-site request forgery, very weak password hashing, unsafe deserialization,
    dom-based cross-site scripting]
```

sg-notification APP 1:01 AM

🔴 The most recent scan for **insecurebank:insecurebank** had the following vulnerabilities which mapped to the ***overall severity criteria***.

SAST

-resource leak
-unsafe deserialization
-cross-site scripting
-cross-site request forgery
-sql injection
-filesystem path, filename, or uri manipulation
-dom-based cross-site scripting

sg-notification APP 1:16 AM

✔️ The most recent scan for **insecurebank:insecurebank** had no vulnerabilities.

Intelligent Orchestration: Avoids defects overload

[1;35mBuild is about to fail, as the following build breaker criteria matched with scan results:SCA found: Overall: [apache commons beanutils 1.7.0,

```
1  Build is about to fail, as the following build breaker criteria matched with scan results:
2  SCA found:
3   Overall: [apache commons beanutils 1.7.0, apache commons collections 3.2.1, apache log4j 1.2.17, berkeley db 5.3.28]
4  Categories: [apache commons collections 3.2.1, berkeley db 5.3.28, apache log4j 1.2.17]
```

sg-notification APP 11:52 PM

🔴 The most recent scan for **insecurebank:insecurebank** had the following vulnerabilities which mapped to the ***overall severity criteria***.

SCA

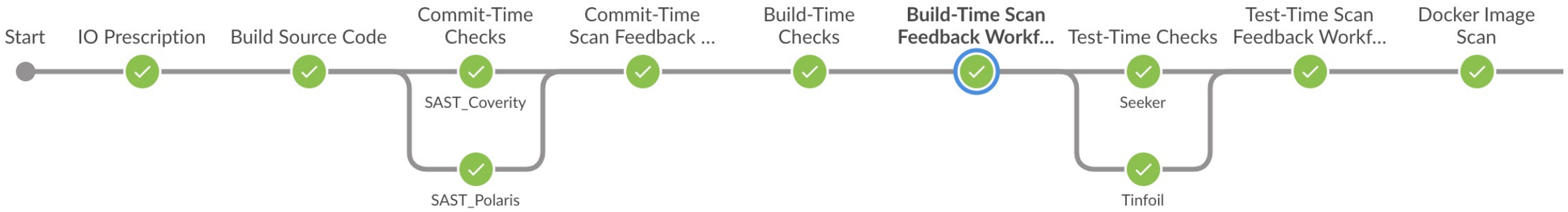
-apache commons beanutils 1.7.0
-apache commons collections 3.2.1
-apache log4j 1.2.17
-berkeley db 5.3.28

🔴 The most recent scan for **insecurebank:insecurebank** had the following vulnerabilities which mapped to the ***individual severity criteria***.

SCA

-apache commons collections 3.2.1
-berkeley db 5.3.28
-apache log4j 1.2.17

Intelligent Orchestration: Prioritizing security weakness and vulnerability types



[1;35mFeedback: [summary:[[activity:sca, overallcount:[[severity:high, count:5], [severity:critical, count:2], [severity:low, count:3], [severity:medium, count:8]], breakercount:[[severit...

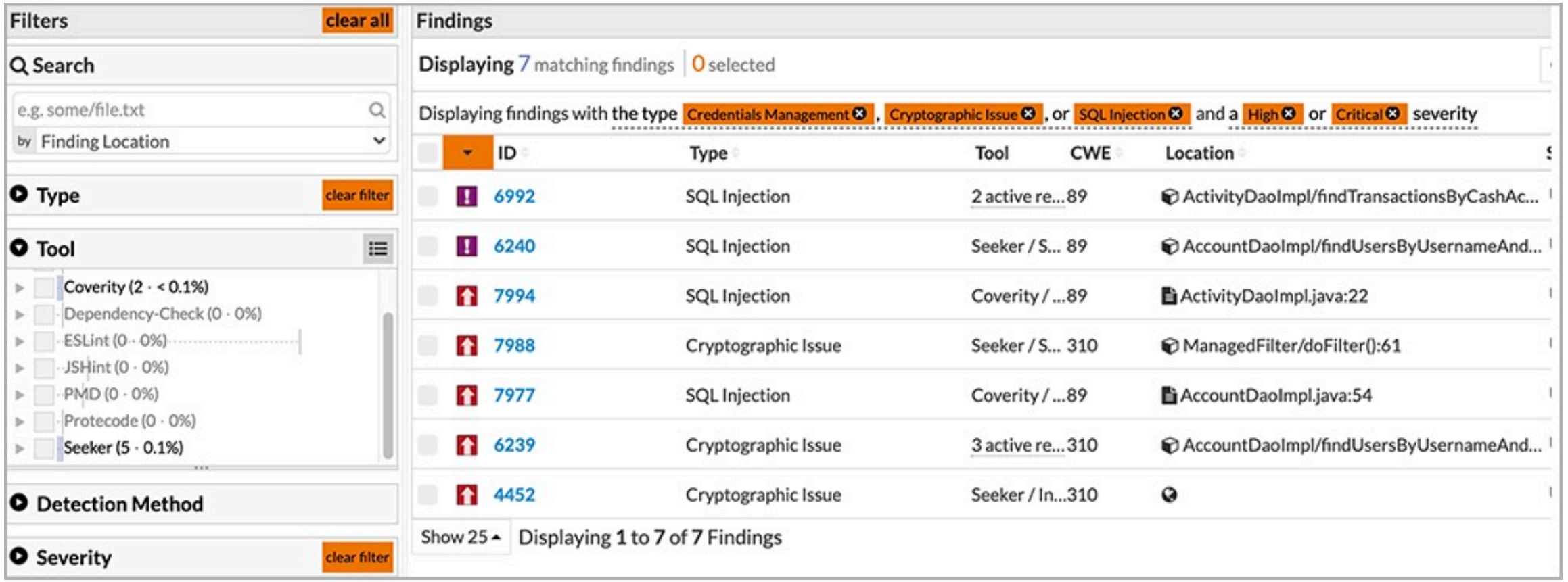
[1;35mBuild is about to fail, as the following build breaker criteria matched with scan results:SCA found: Overall: [apache commons collections 3.2.1] Categories: [apache commons ...

```
1  Build is about to fail, as the following build breaker criteria matched with scan results:
2  SCA found:
3   Overall: [apache commons collections 3.2.1]
4   Categories: [apache commons collections 3.2.1]
```

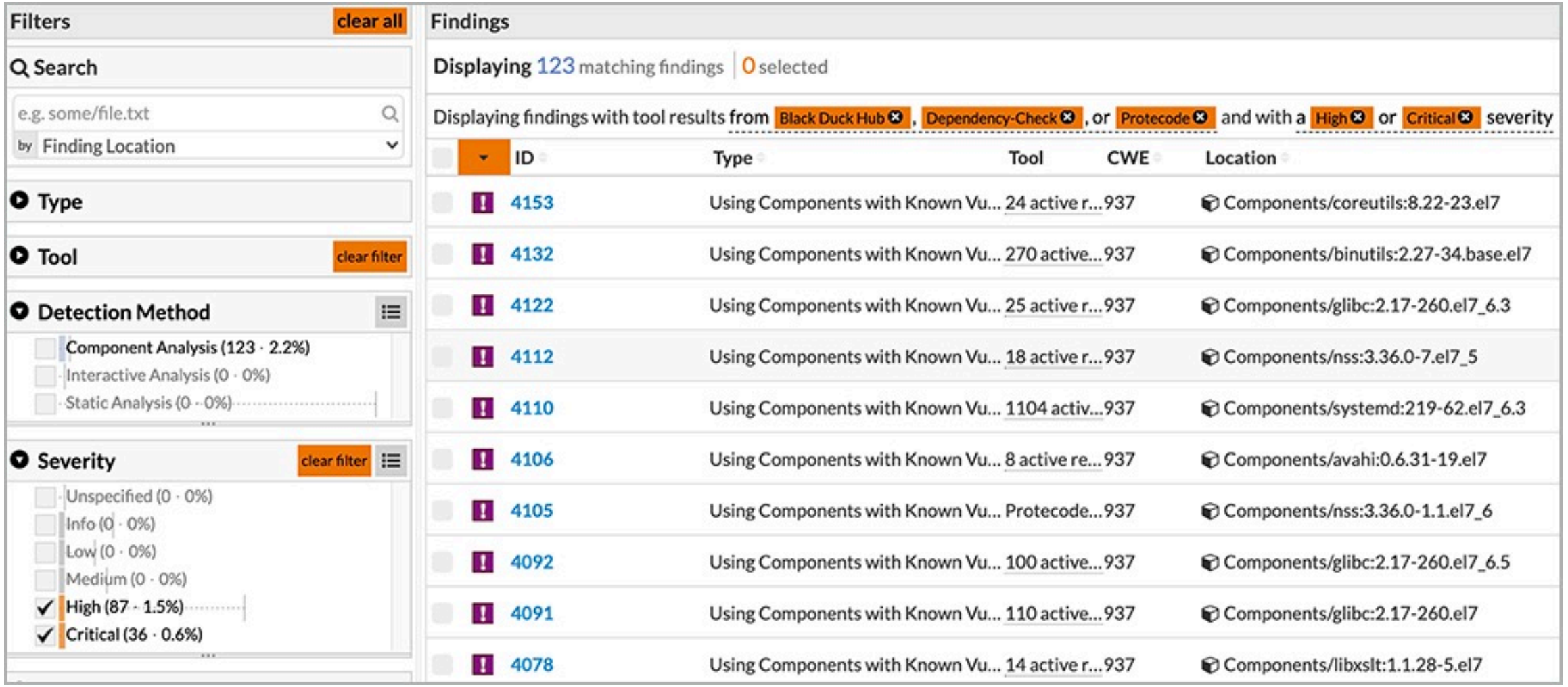
Wait for interactive input

```
1  Build breaker criteria matched. Do you want to proceed?
2  Go ahead or Abort
3  Approved by Meera Rao
```

Code Dx: Prioritizing security weakness and vulnerability types



Code Dx: Prioritizing security weakness and vulnerability types



Intelligent Orchestration: Right tools, right time, right depth

- If you haven't made any changes, why would you run a scan?
- Intelligent Orchestration is built to only scan when changes are detected or when you want to run

Image Credit: https://www.goodhousekeeping.com/uk/product-reviews/a656805/should-i-buy-a-freestanding-or-integrated-dishwasher/

Intelligent Orchestration: Right tools, right time, right depth

IO Prescription - <1s

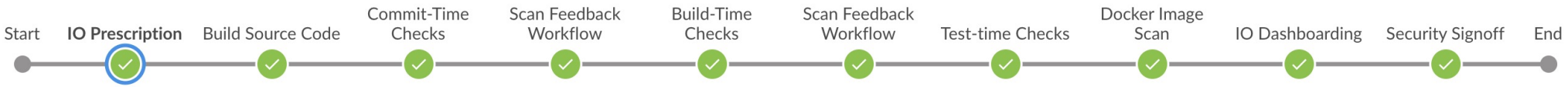
[1;34m==========Start IO Prescription for : meera-test==========Total risk score: 17.75Change Significance Score: 5.5 and Change Significance is LowOpen Vulnerabilities Scor... — Print Message <1s

```
==========Start IO Prescription for : meera-test==========
Total risk score: 17.75

Change Significance Score: 5.5 and Change Significance is Low
Open Vulnerabilities Score: 3.5 and Risk of open vulnerabilities is Low
Business Criticality Score: 5.0 and Business criticality is Critical
Data Classification Score: 3.75 and Data Classification is Restricted
Accessibility Score: 0.0 and Accessibility is Internet
Tooling Score: 0.0


SAST is disabled.
SCA is disabled.
DAST is disabled.
Image Scanning is disabled.
```

Intelligent Orchestration: Right tools, right time, right depth



IO Prescription - 22s

[1;34mselected channel to send notification: slack [0m — Print Message <1s

Wait for interactive input 21s

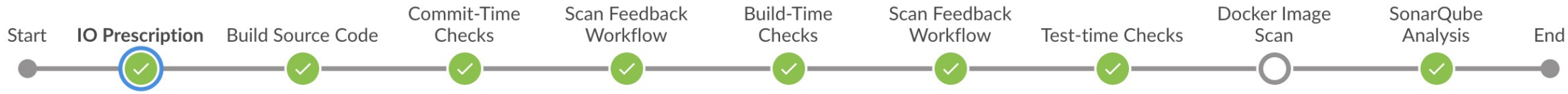
[1;34m==========Start IO Prescription for : meera-test==========Total risk score: 85.0Change Significance Score: 41.25 and Change Significance is HighOpen Vulnerabilities Sc... — Print Message <1s

```
1  ==========Start IO Prescription for : meera-test==========
2  Total risk score: 85.0
3
4  Change Significance Score: 41.25 and Change Significance is High
5  Open Vulnerabilities Score: 35.0 and Risk of open vulnerabilities is Critical
6  Business Criticality Score: 5.0 and Business criticality is Critical
7  Data Classification Score: 3.75 and Data Classification is Restricted
8  Accessibility Score: 0.0 and Accessibility is Internet
9  Tooling Score: 0.0
10
11
12 SAST is enabled with Coverity.
13 SCA is enabled with BlackDuck.
14 DAST is enabled with SeekerZAP.
15 Image Scanning is enabled with Aqua.
16 Manual Code Review is enabled.
17 Manual Penetration Testing is enabled.
```

Intelligent Orchestration: Right tools, right time, right depth

Commit: – 15 days ago Started by user Meera Rao

Description Total risk score: 92.5, Change Significance Score: 40.0 and Change Significance is Critical since a sensitive package like LoginValidator was changed. Also, triggered manual activities like Manual Code Review, Manual Penetration testing and Threat Modeling because of critical changes.



IO Prescription - 40s

✓ [1;34mselected channel to send notification: slack [0m — Print Message <1s

✓ Send Slack Message <1s

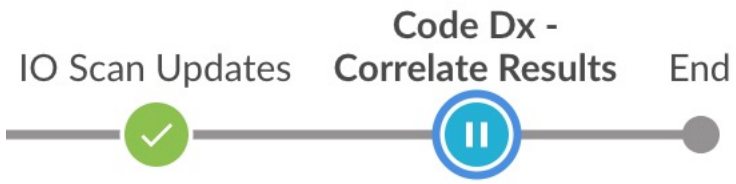
✓ Wait for interactive input 28s

```
1  This application has major code changes, triggering Manual Code Review and Threat Modeling
2  Go ahead or Abort
3  Approved by Meera Rao
```

✓ Wait for interactive input 39s

```
1  This application needs to have a Manual Penetration Testing as per compliance needs.
2  Go ahead or Abort
3  Approved by Meera Rao
```

Intelligent Orchestration and Code Dx : Security sign-off



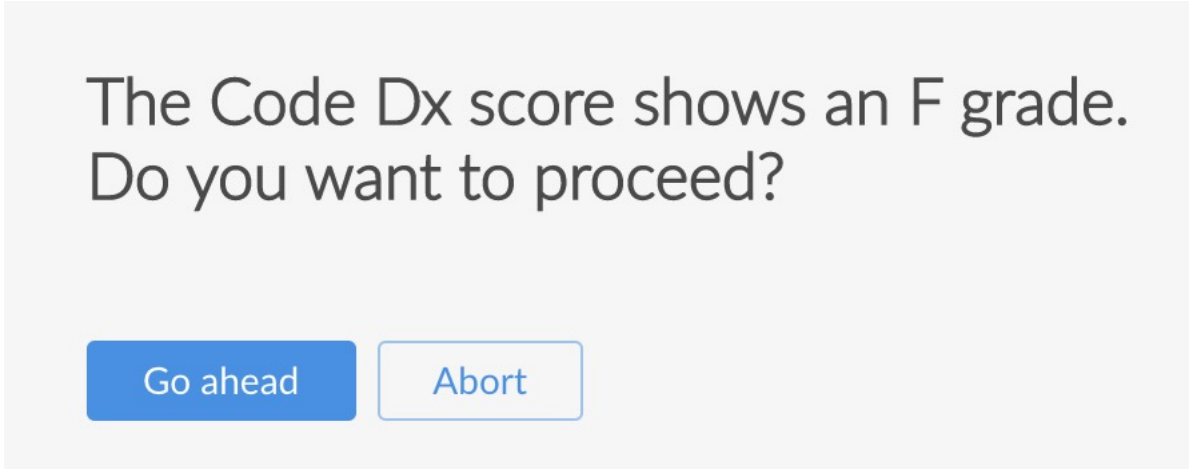
[1;34mDx Custom Code Score: [61.29723] [0m — Print Message

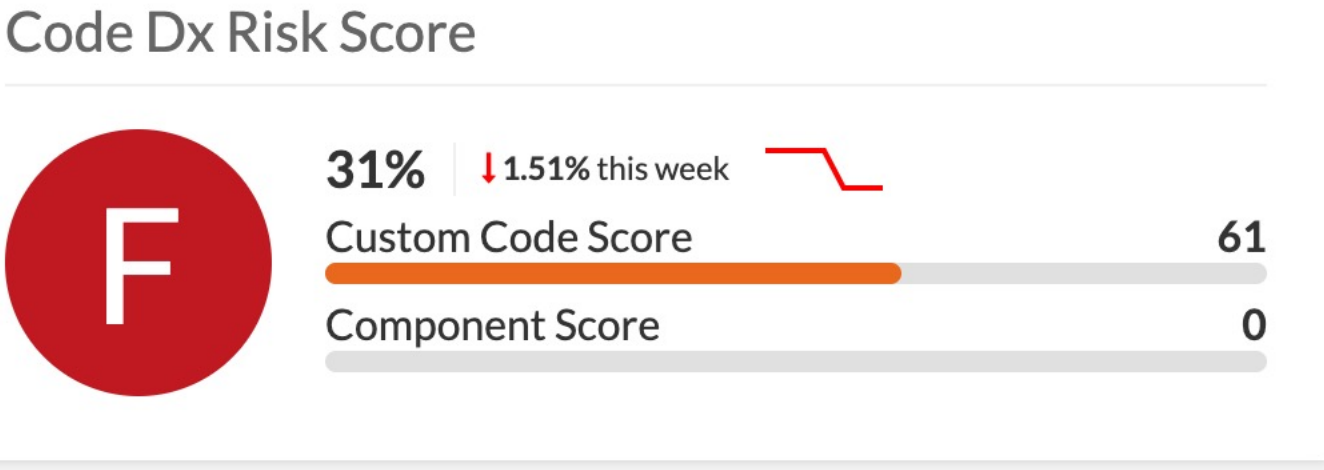
[1;34mDx Component Code Score: [0.0] [0m — Print Message

[1;34mDx Overall Score: [30.648615] [0m — Print Message

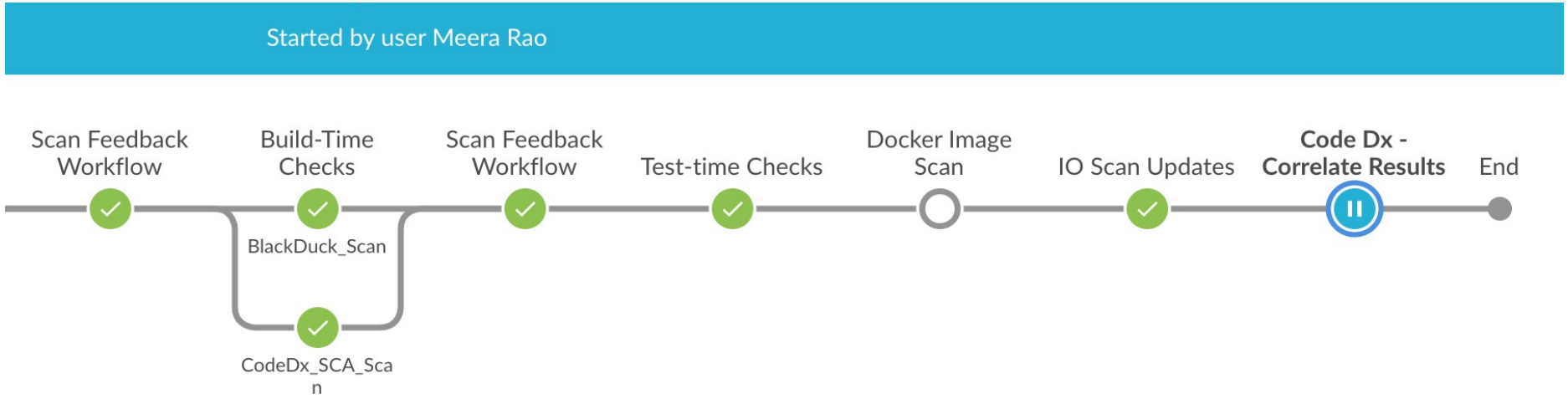
[1;34mDx Grade: F [0m — Print Message

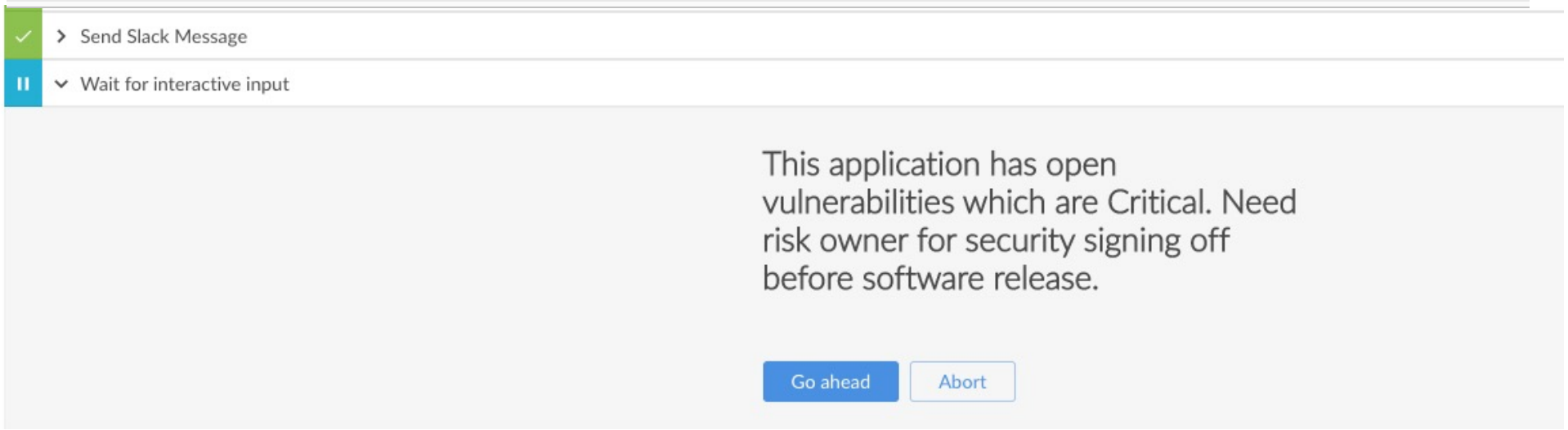
Wait for interactive input



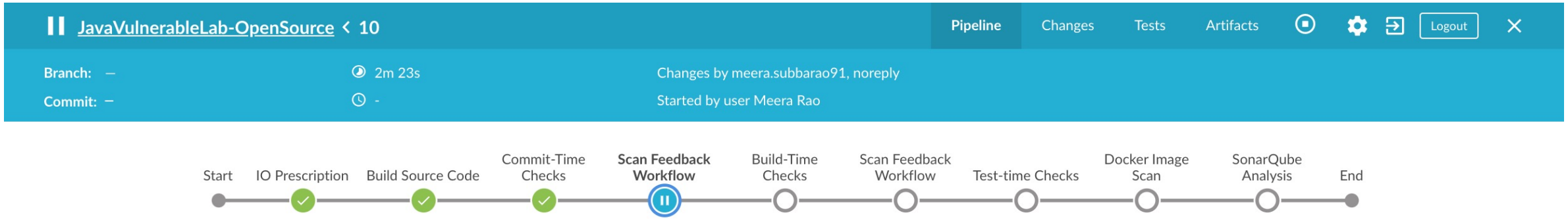


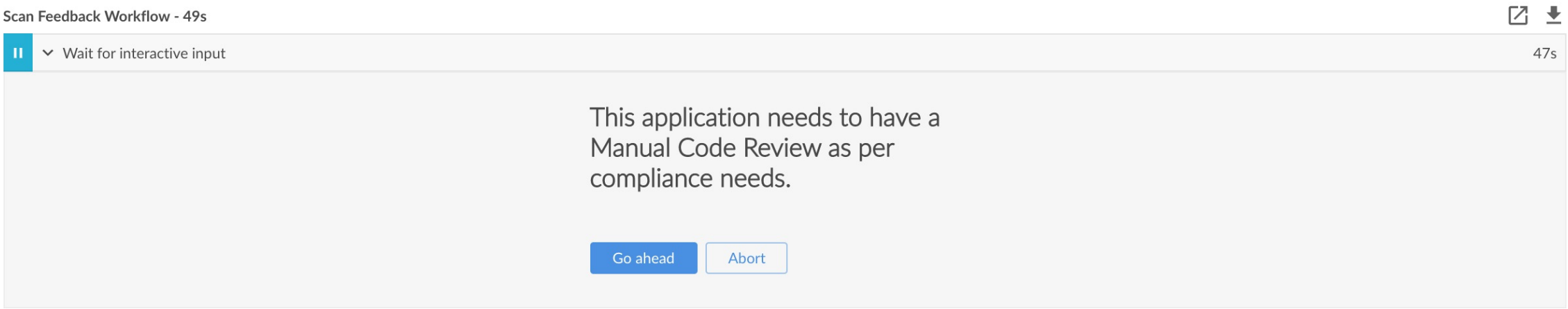
Intelligent Orchestration and Code Dx : Security sign-off





Intelligent Orchestration : Compliance requirements

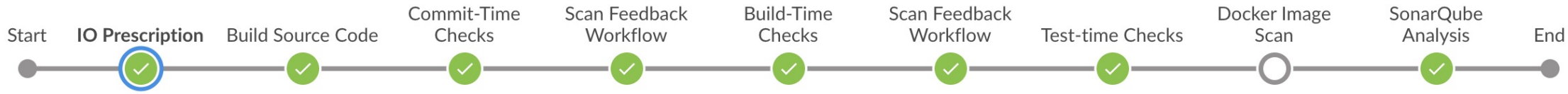




Intelligent Orchestration : Compliance requirements

Commit: – 15 days ago Started by user Meera Rao

Description Total risk score: 92.5, Change Significance Score: 40.0 and Change Significance is Critical since a sensitive package like LoginValidator was changed. Also, triggered manual activities like Manual Code Review, Manual Penetration testing and Threat Modeling because of critical changes.

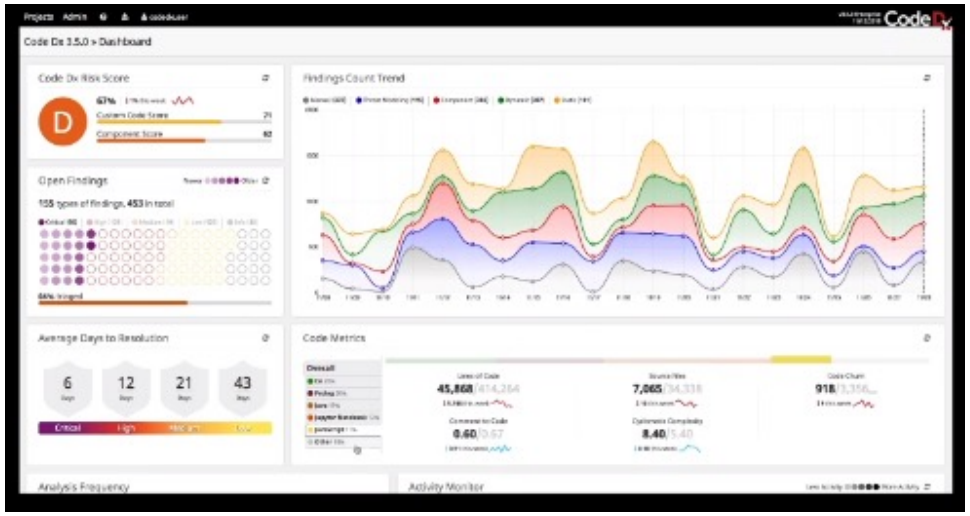


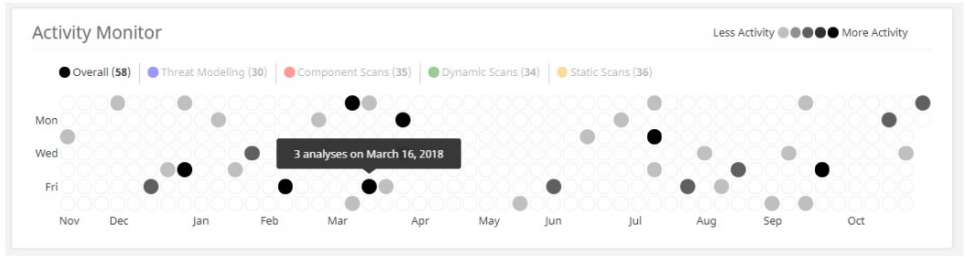
IO Prescription - 40s

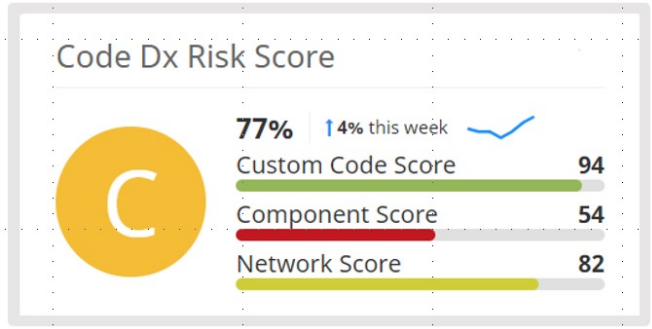
✓ [1;34mselected channel to send notification: slack [0m — Print Message	<1s
✓ Send Slack Message	<1s
✓ Wait for interactive input	28s

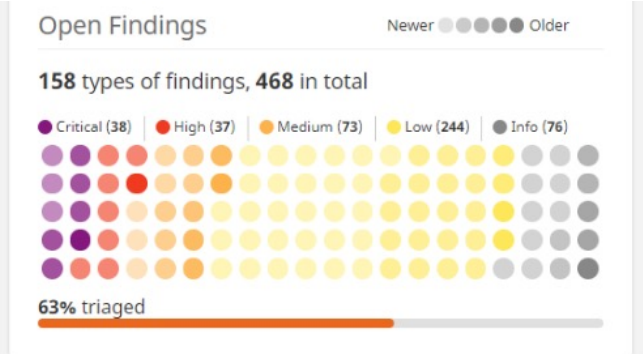
```
1  This application has major code changes, triggering Manual Code Review and Threat Modeling
2  Go ahead or Abort
3  Approved by Meera Rao
```

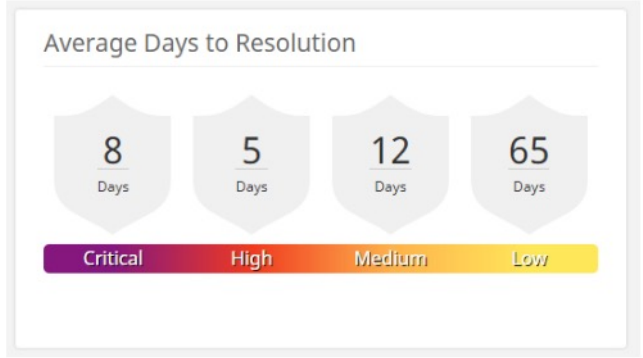
Code Dx : Centralized dashboard





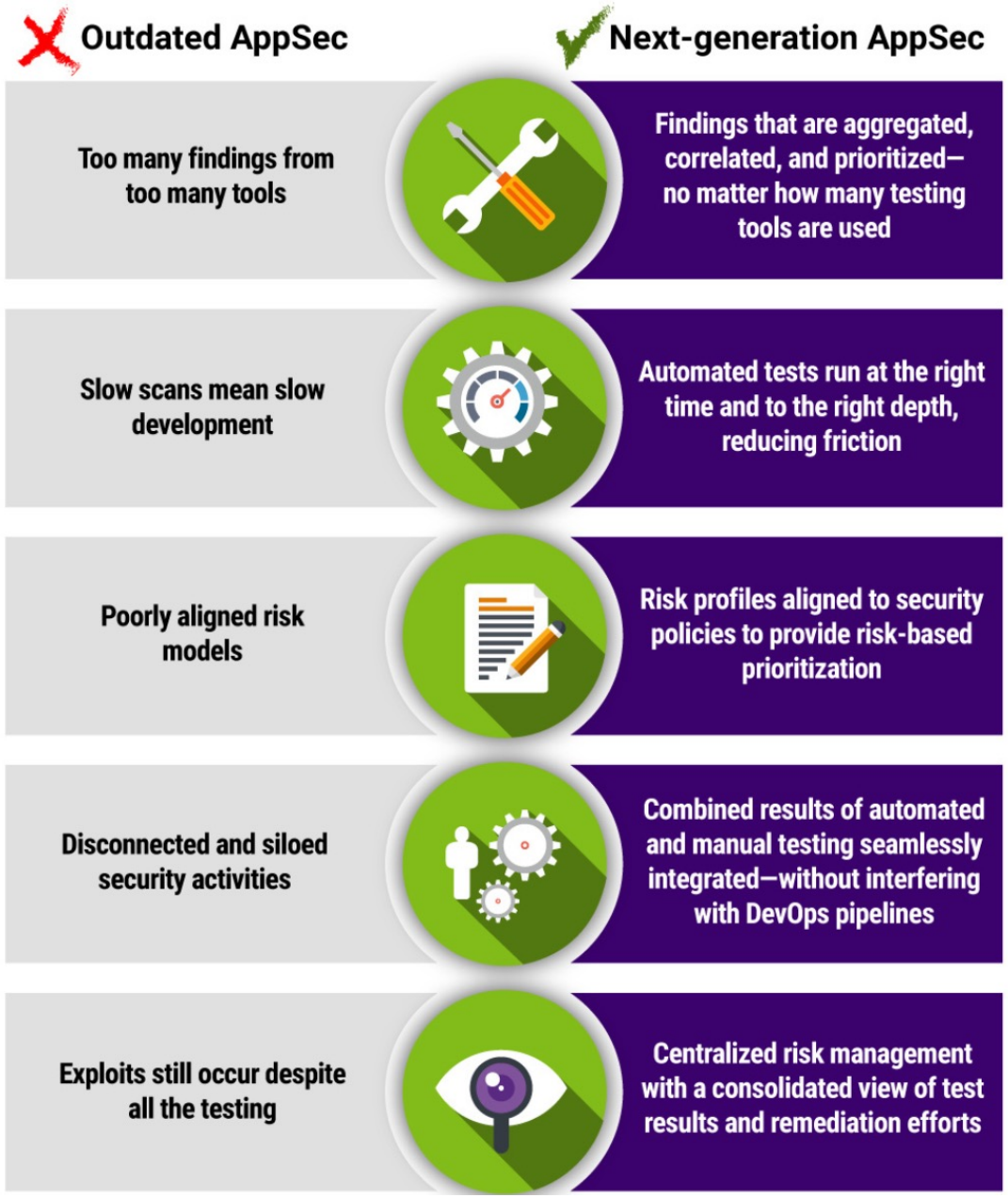






- **Single pane of glass** to view AppSec activities and software security risks
- **AppSec system of record** tracks when software was tested, what was found, and when/if it was fixed
- **Risk visibility** at Project or Business Unit level

DevSecOps Achieved with Intelligent Orchestration and Code Dx



Insightful reading material

- Synopsys.io
- https://www.synopsys.com/blogs/software-security/intelligent-orchestration-enhances-devsecops/
- https://www.synopsys.com/blogs/software-security/intelligent-orchestration-partner-integrations/
- https://www.synopsys.com/blogs/software-security/appsec-decoded-intelligent-orchestration/
- https://www.synopsys.com/blogs/software-security/intelligent-orchestration-partner-integrations/
- https://www.synopsys.com/blogs/software-security/integrating-automated-ast-tools/
- https://www.synopsys.com/blogs/software-security/security-challenges-cicd-workflows/
- https://www.synopsys.com/blogs/software-security/steps-to-integrate-sast-into-devsecops-pipeline/

SYNOPSYS®
Silicon to Software™

Thank You