

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

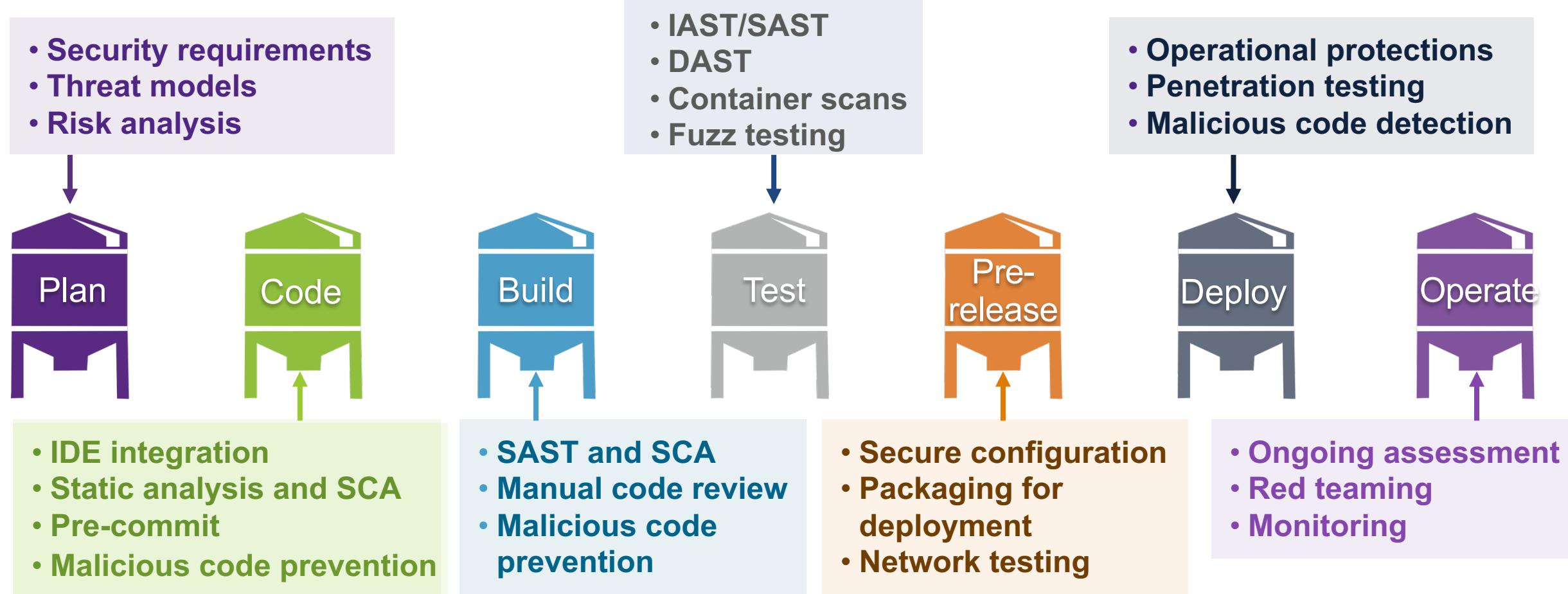
Application security challenges

Application security is not keeping pace with DevOps

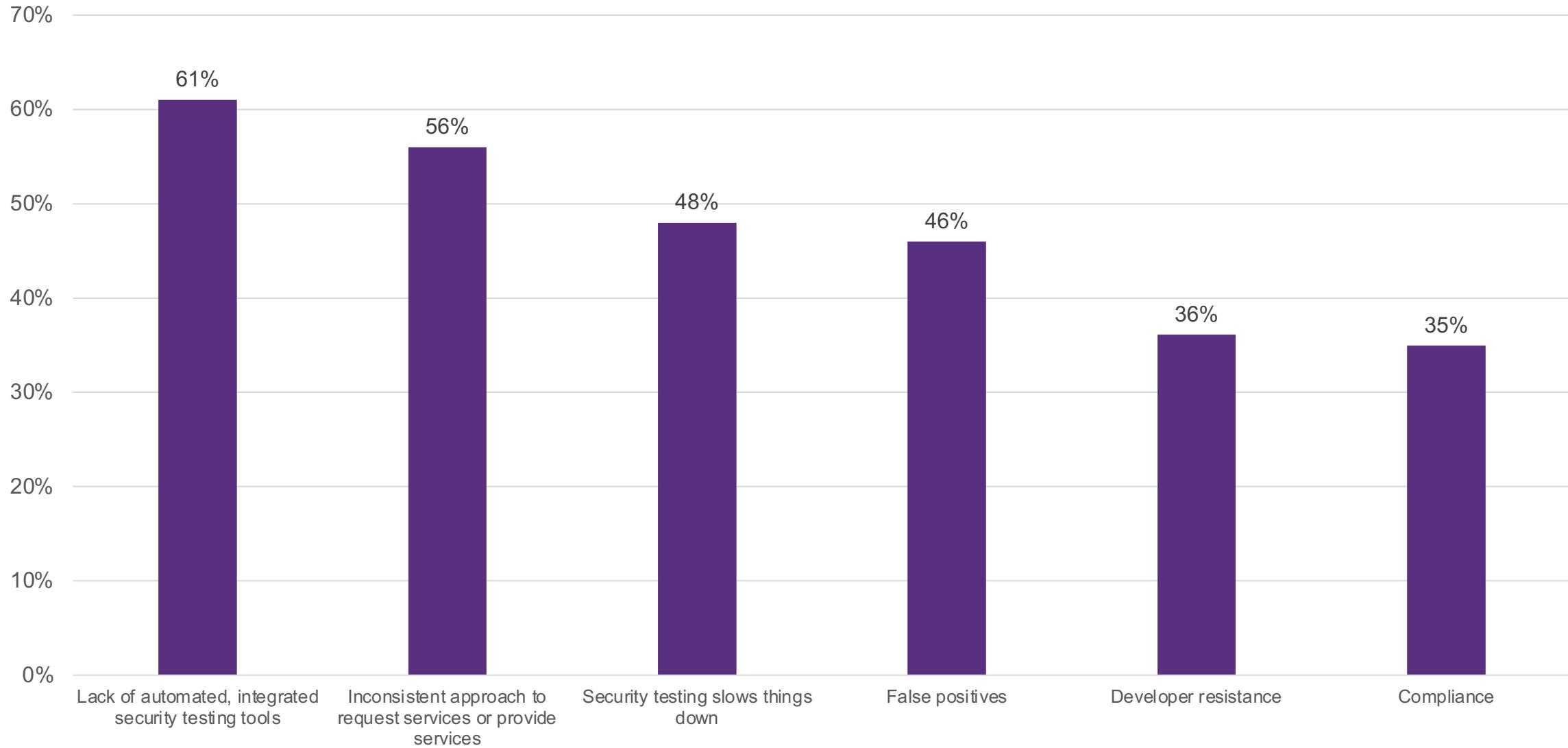


Traditional AppSec testing is siloed

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



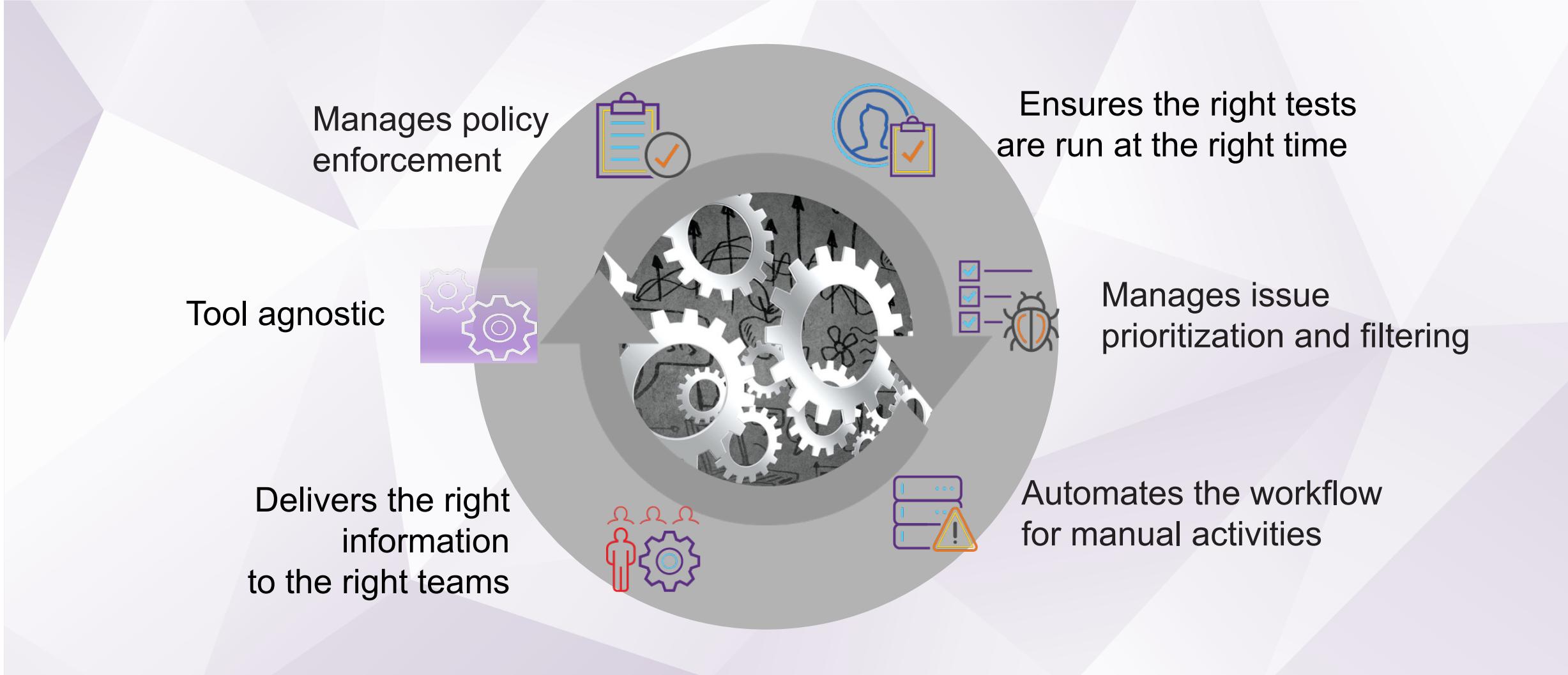
Challenges of security in CI/CD workflows



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

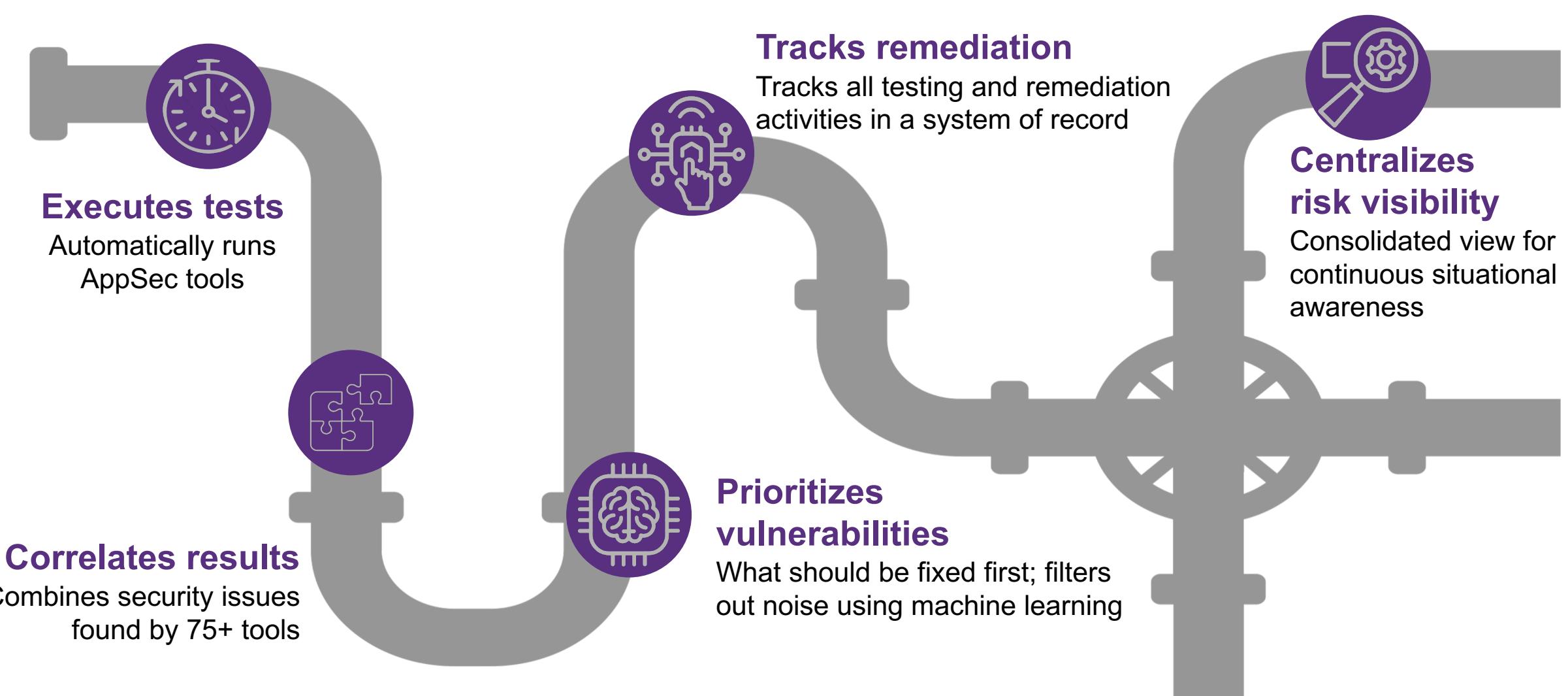
Intelligent Orchestration and Code Dx: A Modern Approach to AppSec

Intelligent Orchestration: Key features



Code Dx: Key features

Fits seamlessly into Intelligent Orchestration pipeline



Intelligent Orchestration : Synopsys tools

Commit: – ⌚ 25 minutes ago Started by user Meera Rao

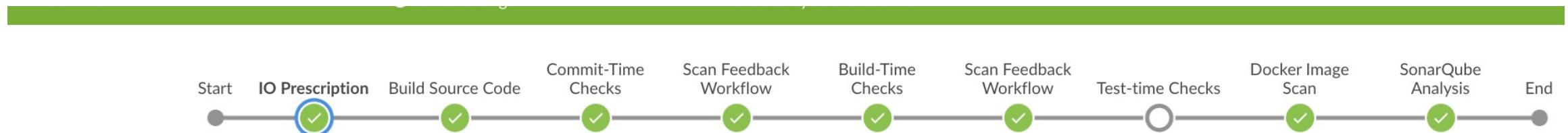
Start **IO Prescription** Trigger out-of-band Activities Build Source Code Commit-Time Checks Build-Time Checks Test-time Checks Docker Image Scan IO Scan Updates Code Dx - Correlate Results Security Signoff End

IO Prescription - <1s 🔗 ⬇️

✓ [1;34m=====Start IO Prescription for : dvna_master=====Total risk score: 67.25Change Significance Score: 55.0 and Change Significance is CriticalOpen Vulnerabilities Score: 3.5 and Risk of open vuln... — Print Message <1s

```
1 =====Start IO Prescription for : dvna_master=====
2 Total risk score: 67.25
3
4 Change Significance Score: 55.0 and Change Significance is Critical
5 Open Vulnerabilities Score: 3.5 and Risk of open vulnerabilities is Low
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 SAST is enabled with Coverity.
12 SCA is enabled with BlackDuck.
13 DAST is enabled with ZAP and Seeker.
14 Image Scanning is enabled with Aqua.
15 Manual Code Review is enabled.
16 Manual Penetration Testing is enabled.
```

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... — F

```
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.
16
```

Code Dx : Synopsys and Open source Tools

Filters [clear all](#)

Q Search
e.g. some/file.txt

by Finding Location

Type

Tool [clear filter](#)

- Black Duck Hub (0 - 0%)
- Checkstyle (0 - 0%)
- Coverity (23 - 0.4%)
- Dependency-Check (0 - 0%)
- ESLint (0 - 0%)
- JSHint (0 - 0%)
- PMD (0 - 0%)

Detection Method

Severity

Location

Container Image

Age

First Seen

Last Modified

Tool Overlaps

Findings

Displaying 40 matching findings | 0 selected

Displaying findings with a status of [New](#); a predicted status of [Escalated](#); and with tool results from [Black Duck Hub](#), [Coverity](#), or [Seeker](#)

ID	Type	Tool	CWE	Location	Status	Predicted Status
! 7	SQL Injection	Seeker...89		AccountDaoImpl/findUsersBy...	New	Escalated 11%
↑ 5522	1 ↗ Cross-Site Request Forg...	Coveri...352		TransferController.java:73	New	Escalated 10%
↑ 5521	Cross-Site Request Forg...	Coveri...352		TransferController.java:131	New	Escalated 10%
↑ 5516	SQL Injection	Coveri...89		AccountDaoImpl.java:54	New	Escalated 9%
↑ 5514	SQL Injection	Coveri...89		ActivityDaoImpl.java:22	New	Escalated 9%
↑ 5509	Path Traversal	Coveri...22		StorageFacadeImpl.java:24	New	Escalated 10%
↑ 5508	Path Traversal	Coveri...22		StorageFacadeImpl.java:18	New	Escalated 10%
↑ 5501	1 ↗ Unsafe deserialization	Coveri...502		DashboardController.java:143	New	Escalated 10%
↑ 5500	Cross-site Scripting (XSS)	Coveri...79		DashboardController.java:147	New	Escalated 10%
↑ 15	Cryptographic Issue	Seeker...310		ManagedFilter/doFilter():61	New	Escalated 10%
↑ 3	Cryptographic Issue	Seeker...310			New	Escalated 10%
↑ 5523	Cross-Site Request Forg...	Coveri...352		SecurityConfig.java:41	New	Escalated 11%
↑ 5519	Information Exposure	Coveri...200		FileUntrustedParent.java:27	New	Escalated 12%
↑ 5515	Cryptographic Issue	Coveri...310		AccountDaoImpl.java:35	New	Escalated 11%
↑ 5510	Invalid Pointer	Coveri...465		StorageFacadeImpl.java:14	New	Escalated 12%

Intelligent Orchestration: Delivers the right information

GitHub actions support

The screenshot shows a GitHub Actions workflow interface for a repository named 'JavaVulnerableLab'. The workflow is titled 'Synopsys Intelligent Security Scan' and was run 14 days ago. It resulted in 11 alerts. A search bar at the top filters for 'tool:"Blackduck SCA Report" is:open branch:master'. Below the search bar, there is a link to 'Clear current search, filters and sorts'. The main list displays six vulnerabilities:

- CVE-2020-25638: Hibernate ORM: 5.3.0 (Error)
- CVE-2016-1603: spring security:4.0.3.RELEASE (Error)
- CVE-2019-4386: dom4j: flexible xml framework for java:1.6.1 (Error)
- CVE-2016-1700: spring framework:4.2.3.RELEASE (Error)
- CVE-2017-0180: Apache Log4j: 1.2.17 (Warning)

Each item includes a checkbox, the CVE ID, the component name, the version, the severity (Error or Warning), the file path (e.g., pom.xml#L181, pom.xml#L248, pom.xml#L145, pom.xml#L125), the detection date ('Detected 14 days ago'), and the Blackduck SCA Report link. The 'master' branch is indicated next to each alert.

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]  
4
```



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

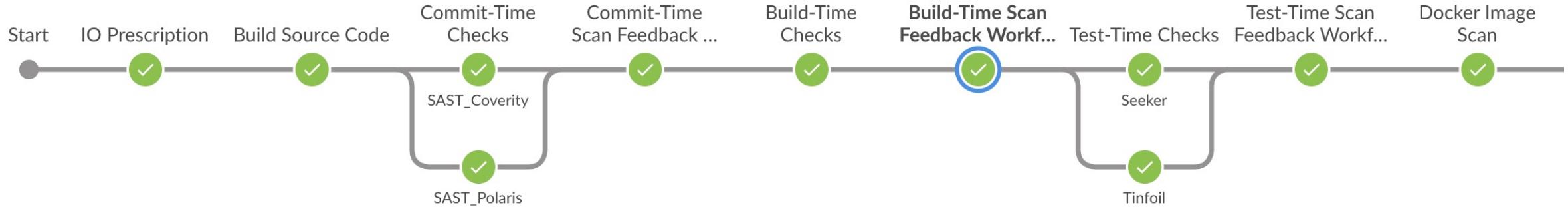
- apache commons beanutils 1.7.0
- apache commons collections 3.2.1
- apache log4j 1.2.17
- berkeley db 5.3.28

🔴 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:[[severity:high, count:1], [severity:critical, count:1], [severity:low, count:1], [severity:medium, count:1]]], breakercount:[]]]
- ✓ ▾ [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

Filters clear all

Q Search
e.g. some/file.txt Search

Type clear filter

Tool ☰
Coverity (2 · < 0.1%)
Dependency-Check (0 · 0%)
ESLint (0 · 0%)
JSHint (0 · 0%)
PMD (0 · 0%)
Protecode (0 · 0%)
Seeker (5 · 0.1%)

Detection Method

Severity clear filter

Findings

Displaying 7 matching findings | 0 selected

Displaying findings with the type Credentials Management, Cryptographic Issue, or SQL Injection and a High or Critical severity

ID	Type	Tool	CWE	Location
6992	SQL Injection	2 active re...89		ActivityDaoImpl/findTransactionsByCashAc...
6240	SQL Injection	Seeker / S... 89		AccountDaoImpl/findUsersByUsernameAnd...
7994	SQL Injection	Coverity / ...89		ActivityDaoImpl.java:22
7988	Cryptographic Issue	Seeker / S... 310		ManagedFilter/doFilter():61
7977	SQL Injection	Coverity / ...89		AccountDaoImpl.java:54
6239	Cryptographic Issue	3 active re...310		AccountDaoImpl/findUsersByUsernameAnd...
4452	Cryptographic Issue	Seeker / In...310		

Show 25 ▾ Displaying 1 to 7 of 7 Findings

Code Dx: Prioritizing security weakness and vulnerability types

Filters clear all

Q Search e.g. some/file.txt clear

by Finding Location

Type

Tool clear filter

Detection Method clear filter ≡

- Component Analysis (123 · 2.2%)
- Interactive Analysis (0 · 0%)
- Static Analysis (0 · 0%)

Severity clear filter ≡

- Unspecified (0 · 0%)
- Info (0 · 0%)
- Low (0 · 0%)
- Medium (0 · 0%)
- High (87 · 1.5%)**
- Critical (36 · 0.6%)**

Findings

Displaying 123 matching findings | 0 selected

Displaying findings with tool results from Black Duck Hub ✗, Dependency-Check ✗, or Protecode ✗ and with a High ✗ or Critical ✗ severity

ID	Type	Tool	CWE	Location
4153	Using Components with Known Vu...	24 active r...	937	Components/coreutils:8.22-23.el7
4132	Using Components with Known Vu...	270 active...	937	Components/binutils:2.27-34.base.el7
4122	Using Components with Known Vu...	25 active r...	937	Components/glibc:2.17-260.el7_6.3
4112	Using Components with Known Vu...	18 active r...	937	Components/nss:3.36.0-7.el7_5
4110	Using Components with Known Vu...	1104 activ...	937	Components/systemd:219-62.el7_6.3
4106	Using Components with Known Vu...	8 active re...	937	Components/avahi:0.6.31-19.el7
4105	Using Components with Known Vu...	Protecode...	937	Components/nss:3.36.0-1.1.el7_6
4092	Using Components with Known Vu...	100 active...	937	Components/glibc:2.17-260.el7_6.5
4091	Using Components with Known Vu...	110 active...	937	Components/glibc:2.17-260.el7
4078	Using Components with Known Vu...	14 active r...	937	Components/libxslt:1.1.28-5.el7

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

```
1 =====Start IO Prescription for : meera-test=====
2 Total risk score: 17.75
3
4 Change Significance Score: 5.5 and Change Significance is Low
5 Open Vulnerabilities Score: 3.5 and Risk of open vulnerabilities is Low
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 disabled.
13 SCA is disabled.
14 DAST is disabled.
15 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.



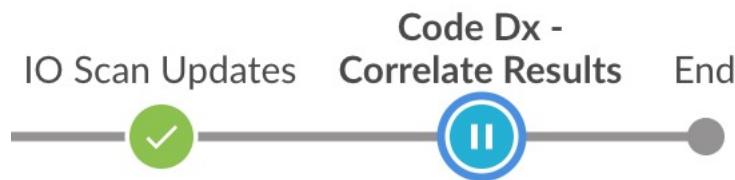
IO Prescription - 40s



✓	> [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

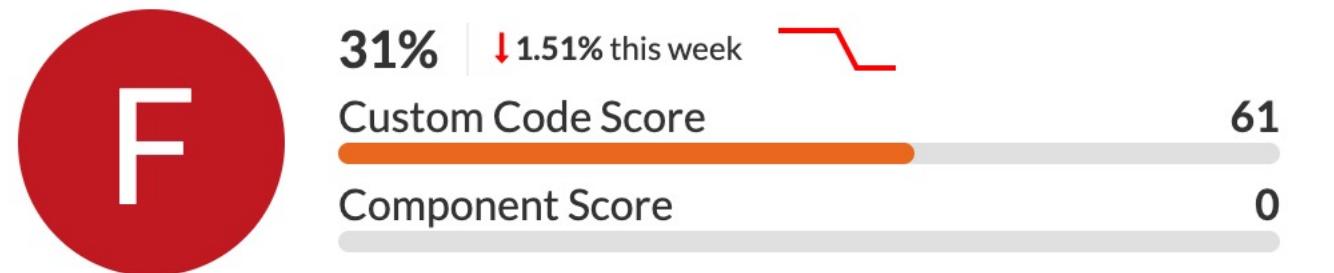


- ✓ > [1;34mDx Custom Code Score: [61.29723] [0m – Print Message]
- ✓ > [1;34mDx Component Code Score: [0.0] [0m – Print Message]
- ✓ > [1;34mDx Overall Score: [30.648615] [0m – Print Message]
- ✓ > [1;34mDx Grade: F [0m – Print Message]
- II ✓ Wait for interactive input

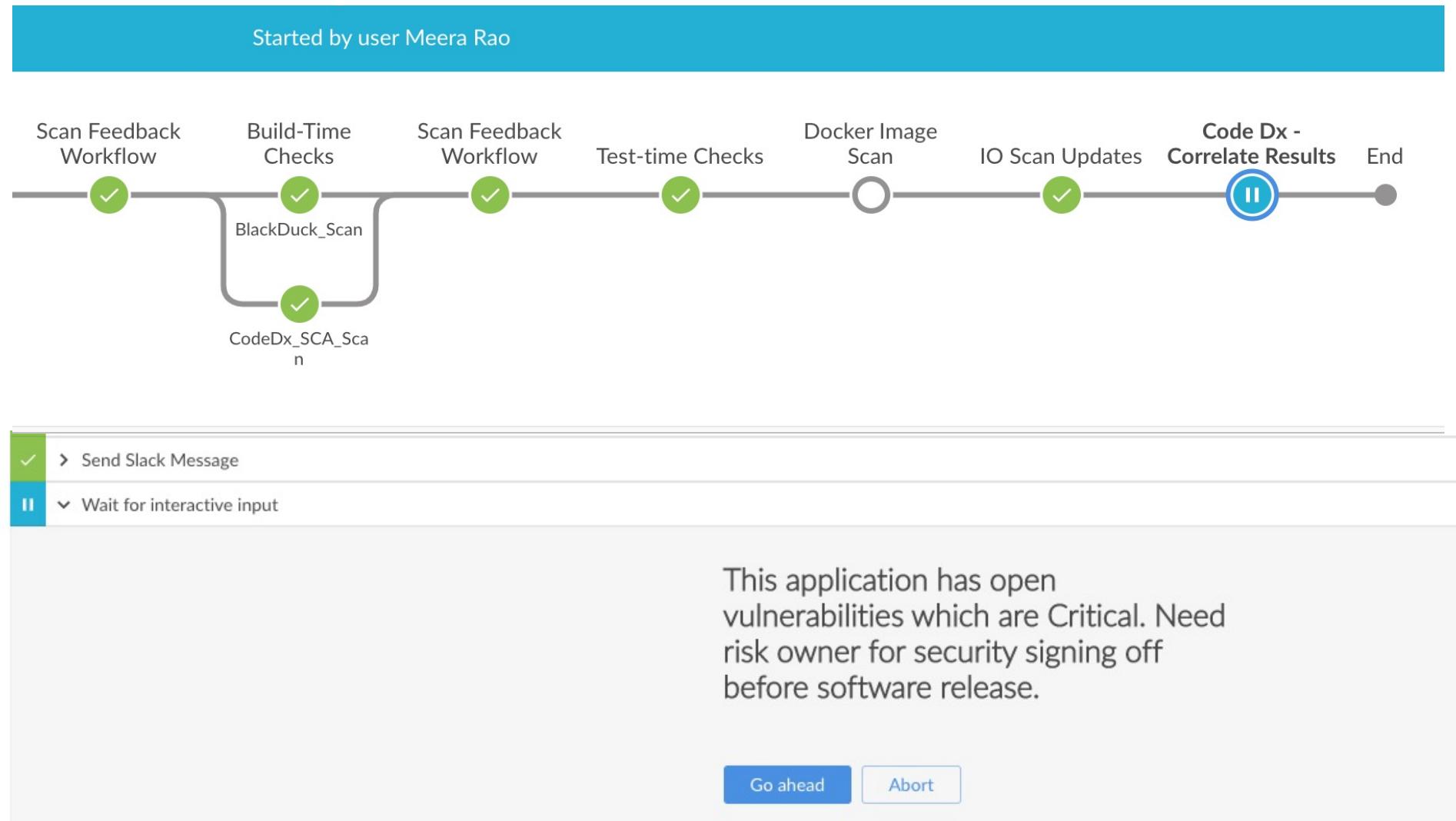
The Code Dx score shows an F grade.
Do you want to proceed?

[Go ahead](#) [Abort](#)

Code Dx Risk Score



Intelligent Orchestration and Code Dx : Security sign-off



Intelligent Orchestration : Compliance requirements

JavaVulnerableLab-OpenSource < 10

Pipeline Changes Tests Artifacts Logout X

Branch: - 2m 23s Changes by meera.subbarao91, noreply
Commit: - - Started by user Meera Rao

Start IO Prescription Build Source Code Commit-Time Checks Scan Feedback Workflow Build-Time Checks Scan Feedback Workflow Test-time Checks Docker Image Scan SonarQube Analysis End

Scan Feedback Workflow - 49s

Wait for interactive input 47s

This application needs to have a Manual Code Review as per compliance needs.

Go ahead Abort

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.



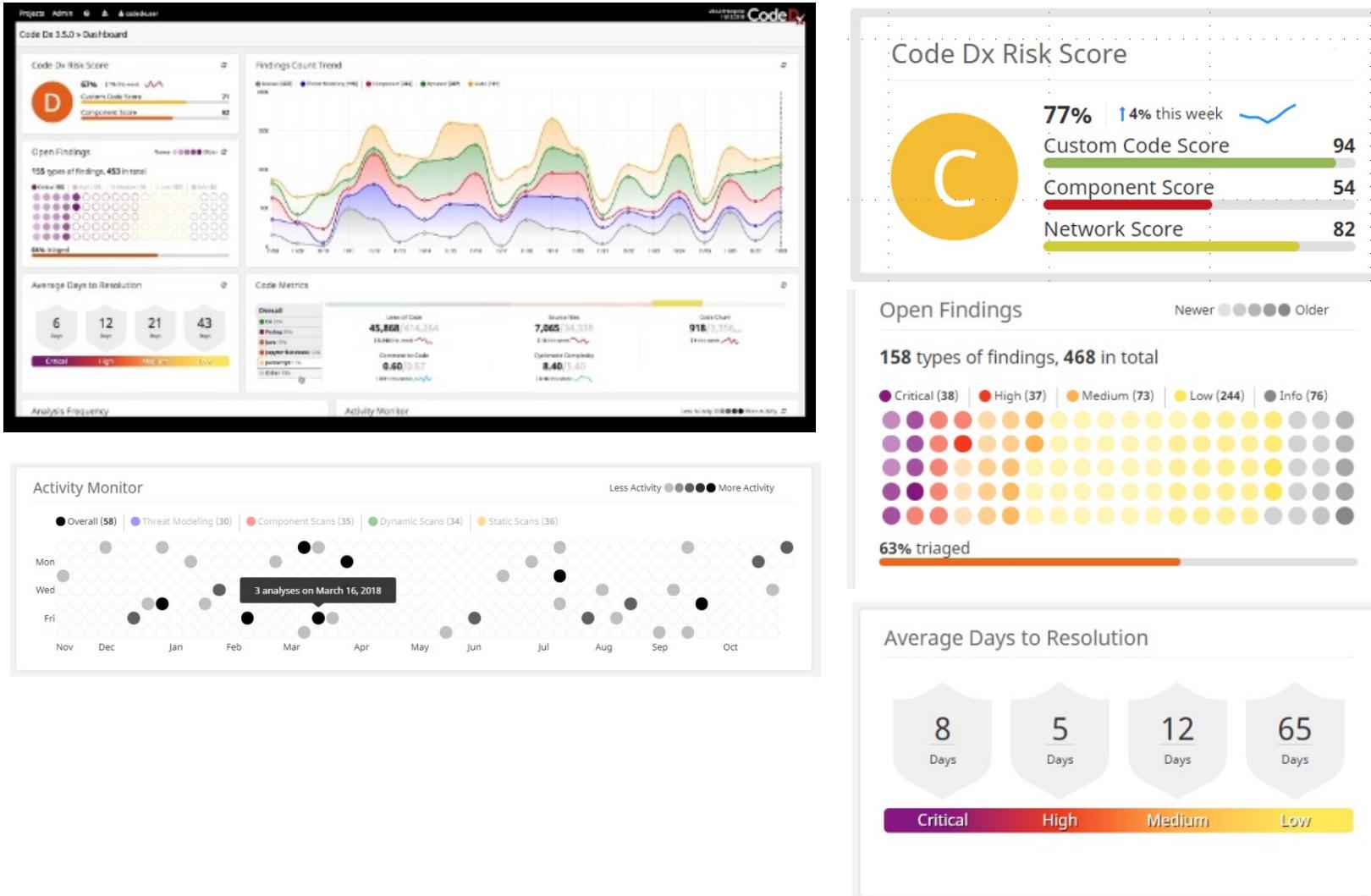
IO Prescription - 40s



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

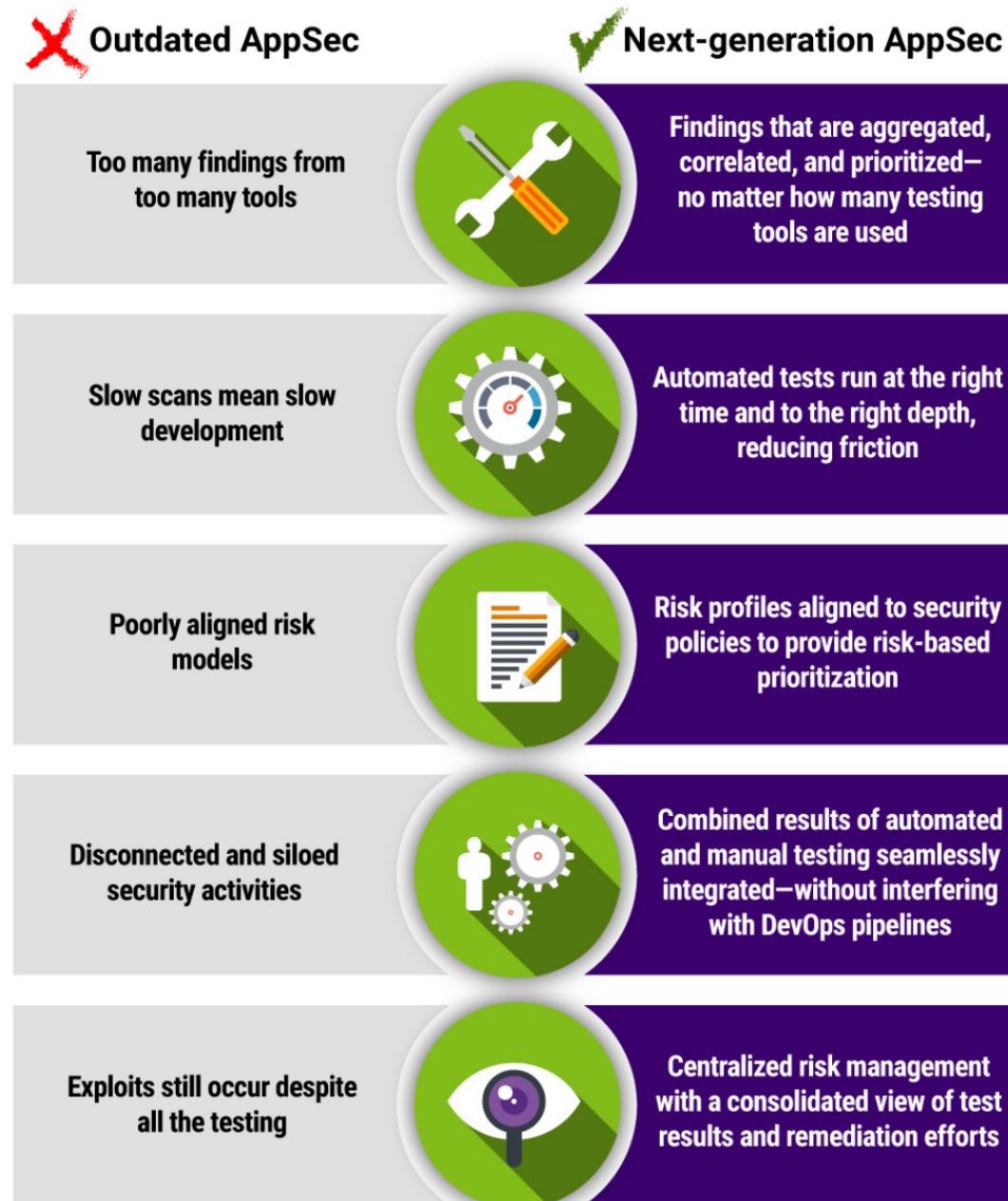
1 This application has major code changes, triggering Manual Code Review and Threat Modeling
2 Go ahead or Abort
3 Approved by Meera Rao

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-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/>

Thank You

