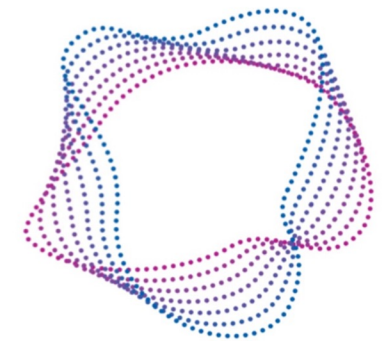


Best Practices with Sonatype



GOVTECH
SINGAPORE



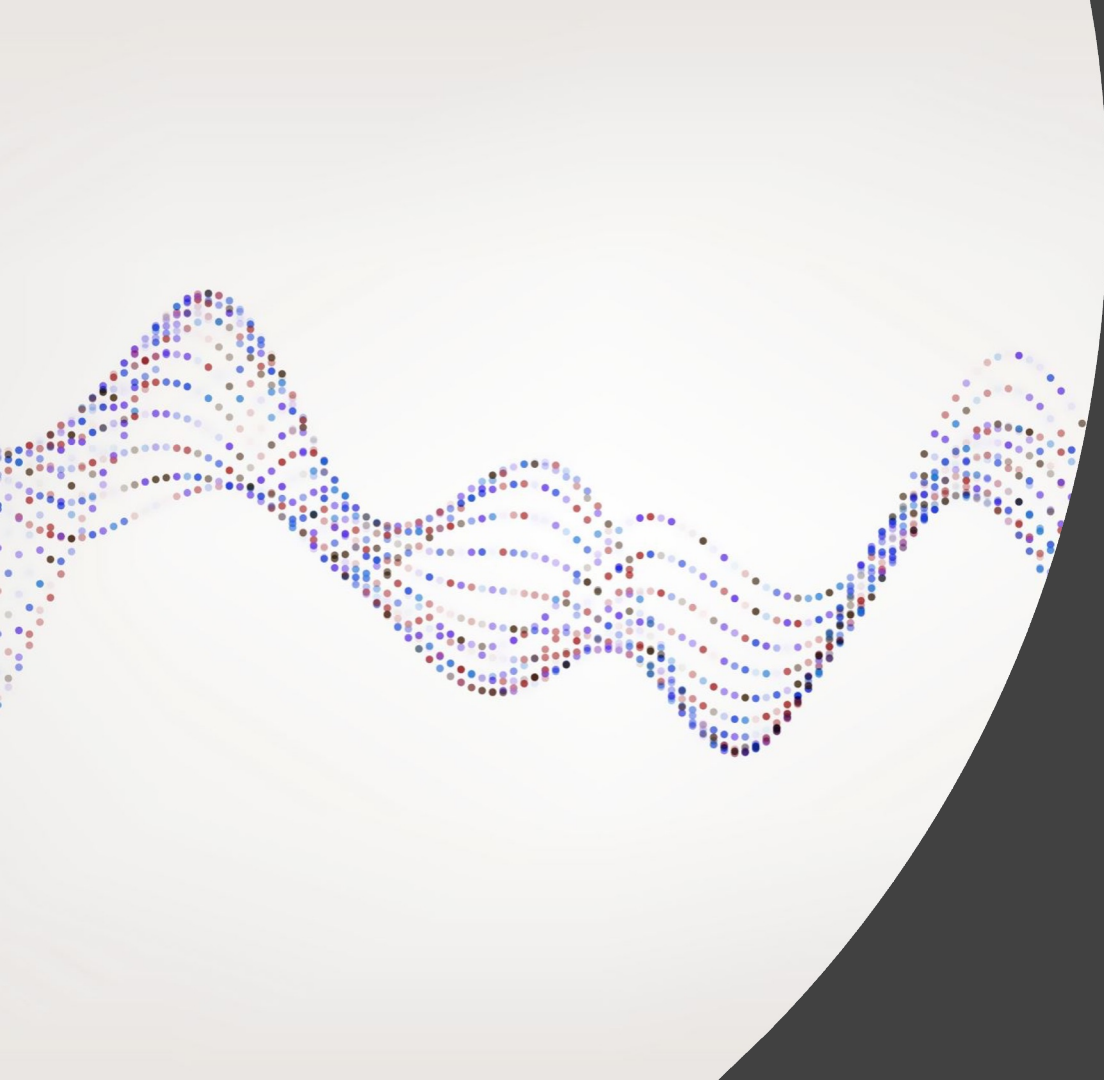
 sonatype

Agenda



- GovTech Intro
- Benefits of Sonatype IQ for OSS Consumption
- How Sonatype fits into your SHIP-HATS offering
- GovTech Demo GitLab Pipeline
- Best Practices
- Sonatype Resources
- Q&A





Benefits of Sonatype IQ for OSS Consumption

Open source is literally everywhere.
Not all OSS parts created equal.
Ages like milk, not wine.

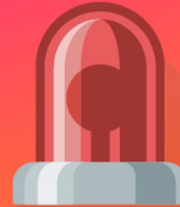


1 in 4
organizations
experienced at least
one open source
breach in the
last 12 months.



**430% YOY
growth**
in cyber attacks
targeting open source
software projects

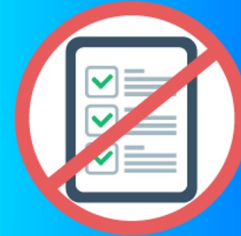
40%
of npm packages
rely on code
with known
vulnerabilities



1 in 10
open source
component
downloads
have known
vulnerabilities

38%

of organizations
have no open source
governance policy
or ignore it



**71%
increase**
in open source
related breaches
over the past
five years

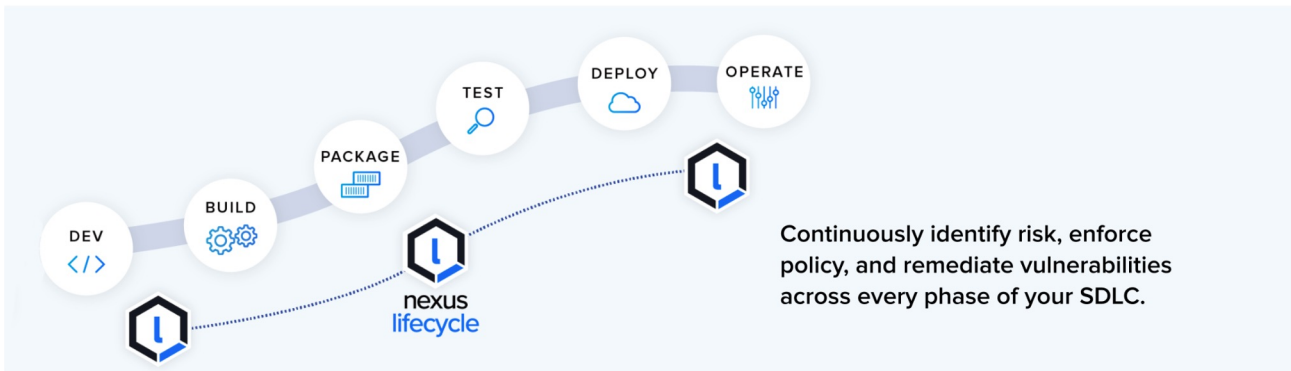


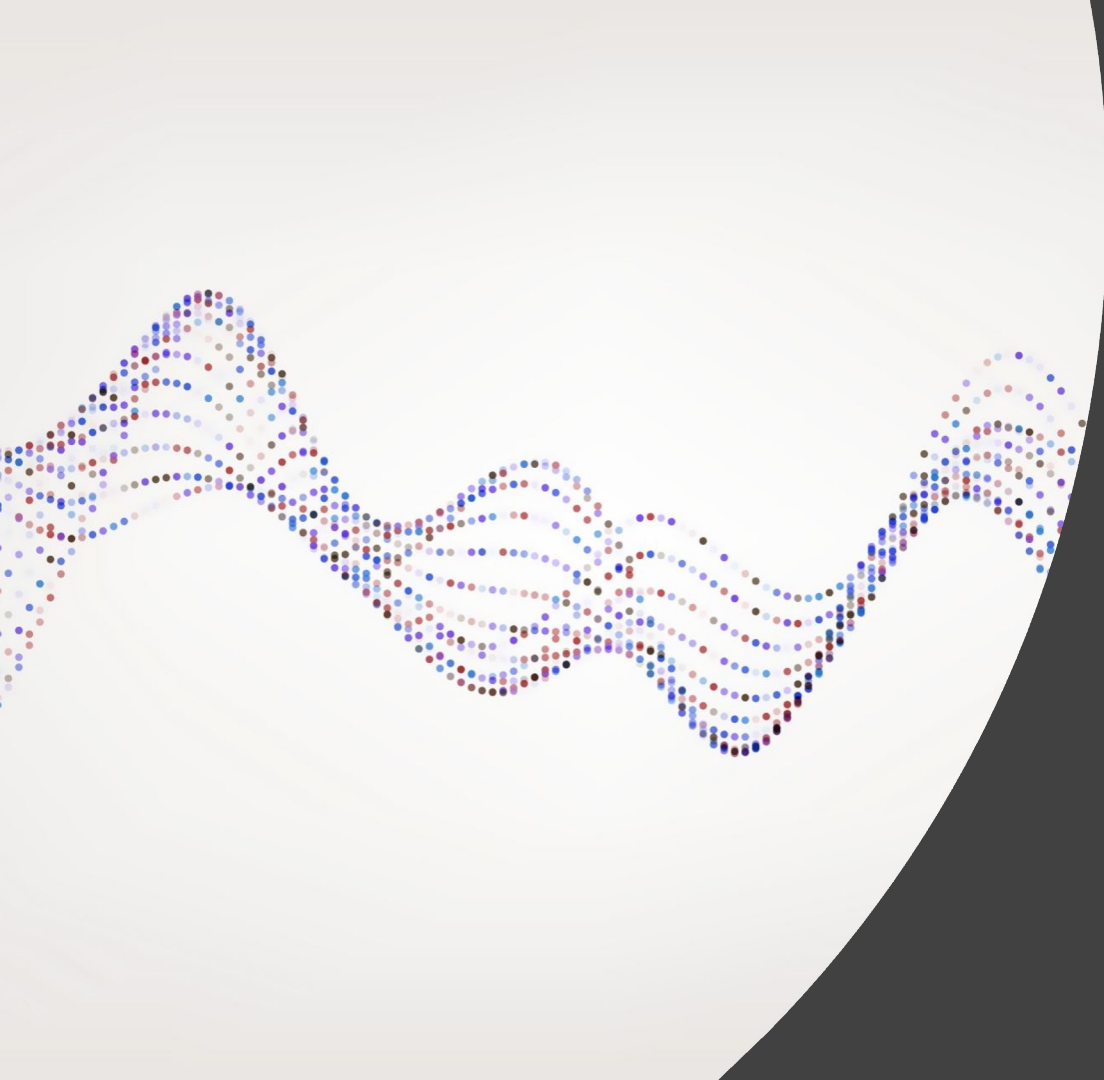
nexus lifecycle

Eliminate open source risk across the entire SDLC.

It's no secret. Developers use open source — in fact, 85% of a modern application is comprised of open source components and unfortunately one in ten open source component downloads contain a known security vulnerability. Given this inherent risk, how do modern software teams select the best components, govern open source usage, and still deliver at DevOps speed? **With automated open source governance.**

Nexus Lifecycle empowers developers and security professionals to make safer open source choices across the SDLC, ensuring organizations continue to innovate with less risk.





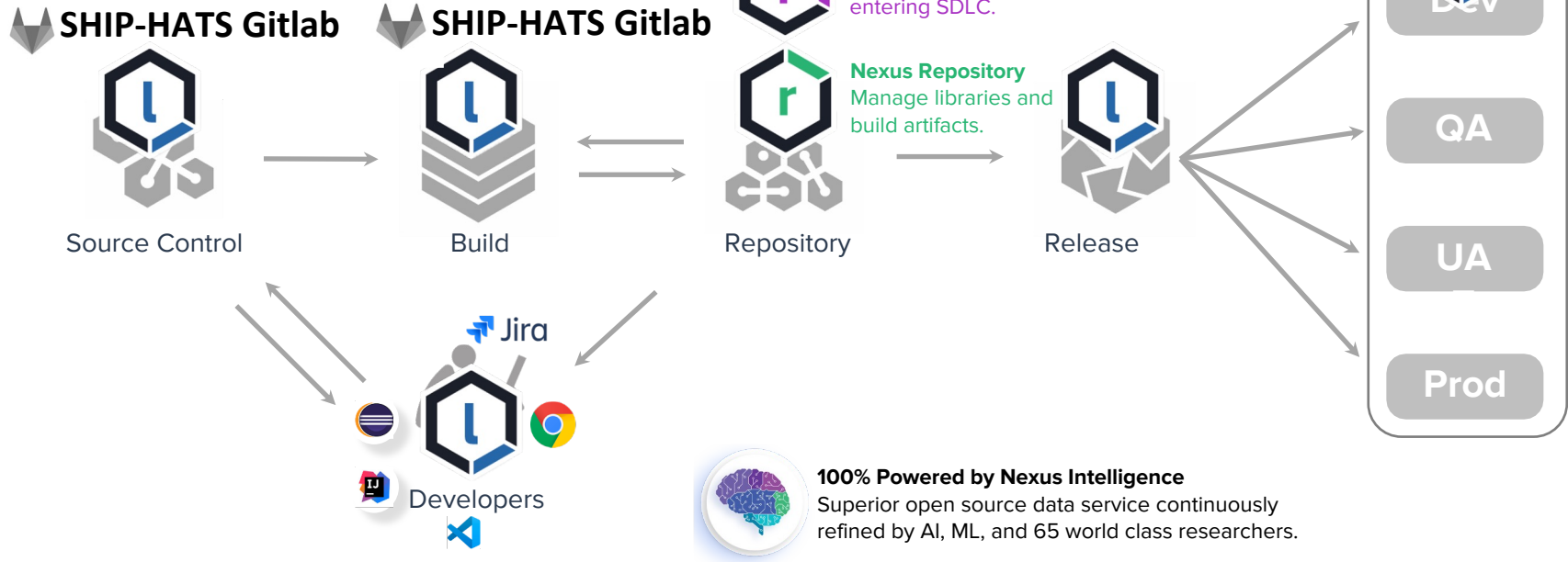
How
Sonatype fits
into your
SHIP-HATS
offering

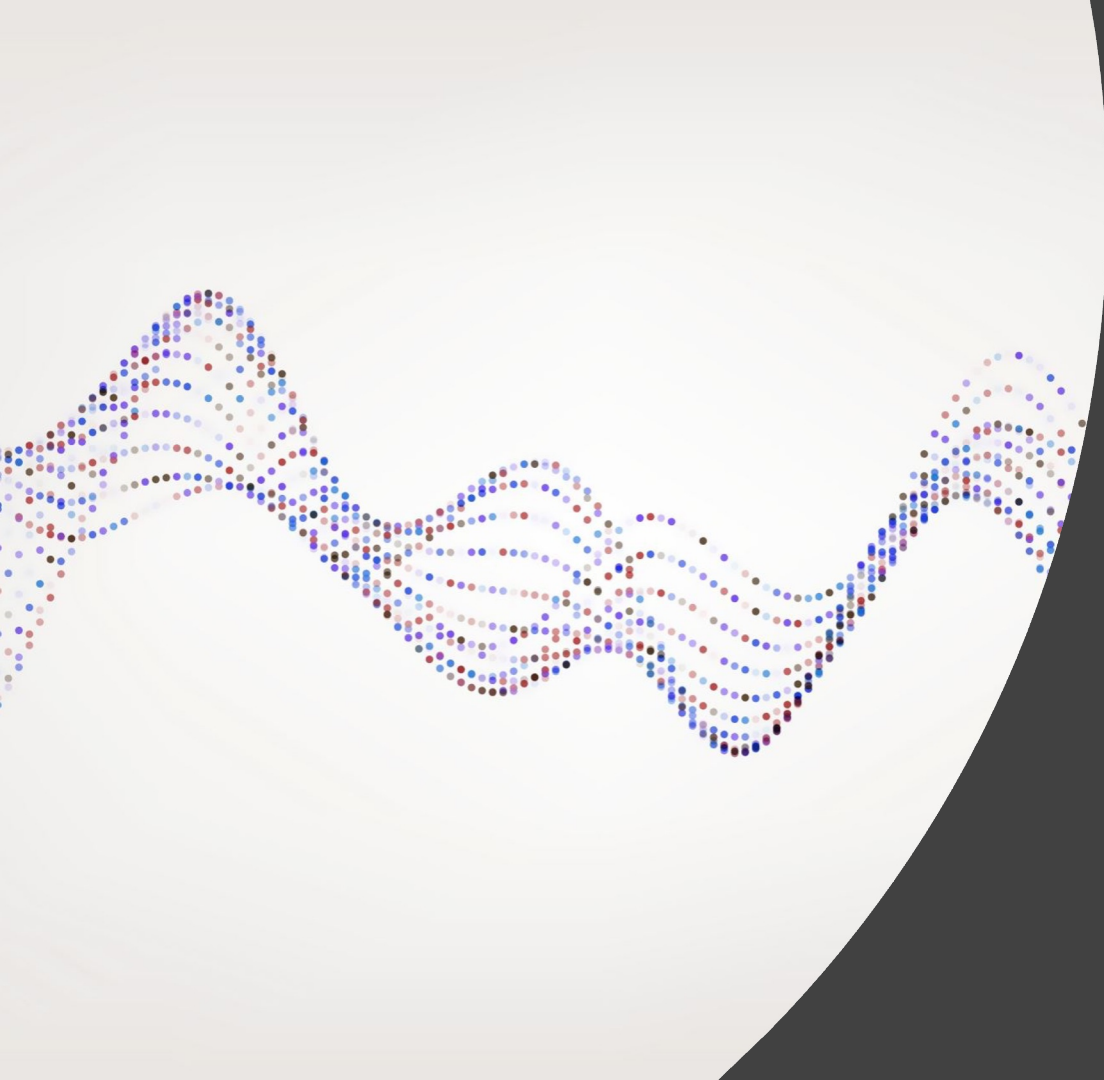
Nexus automatically enforces open source policy and controls risk across every phase of the SDLC.



Nexus Lifecycle

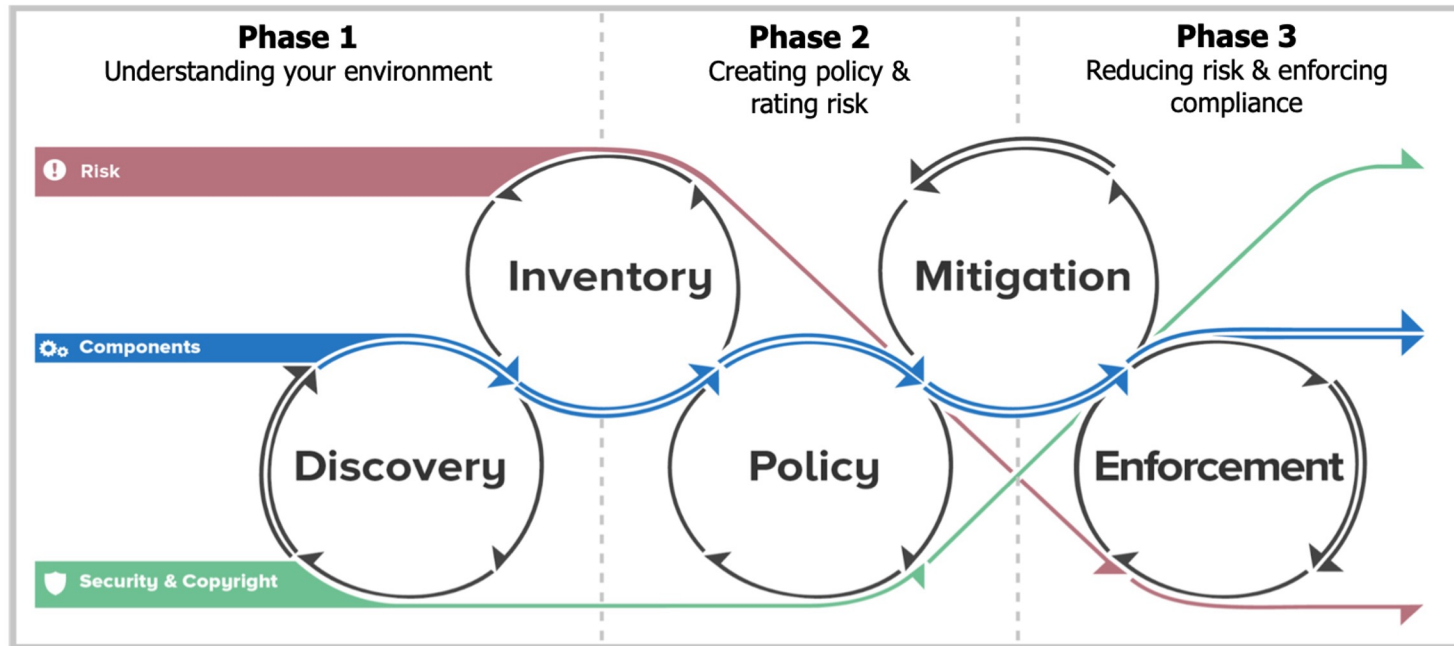
Continuously identify risk, enforce policy, and remediate violations across every phase of your SDLC.

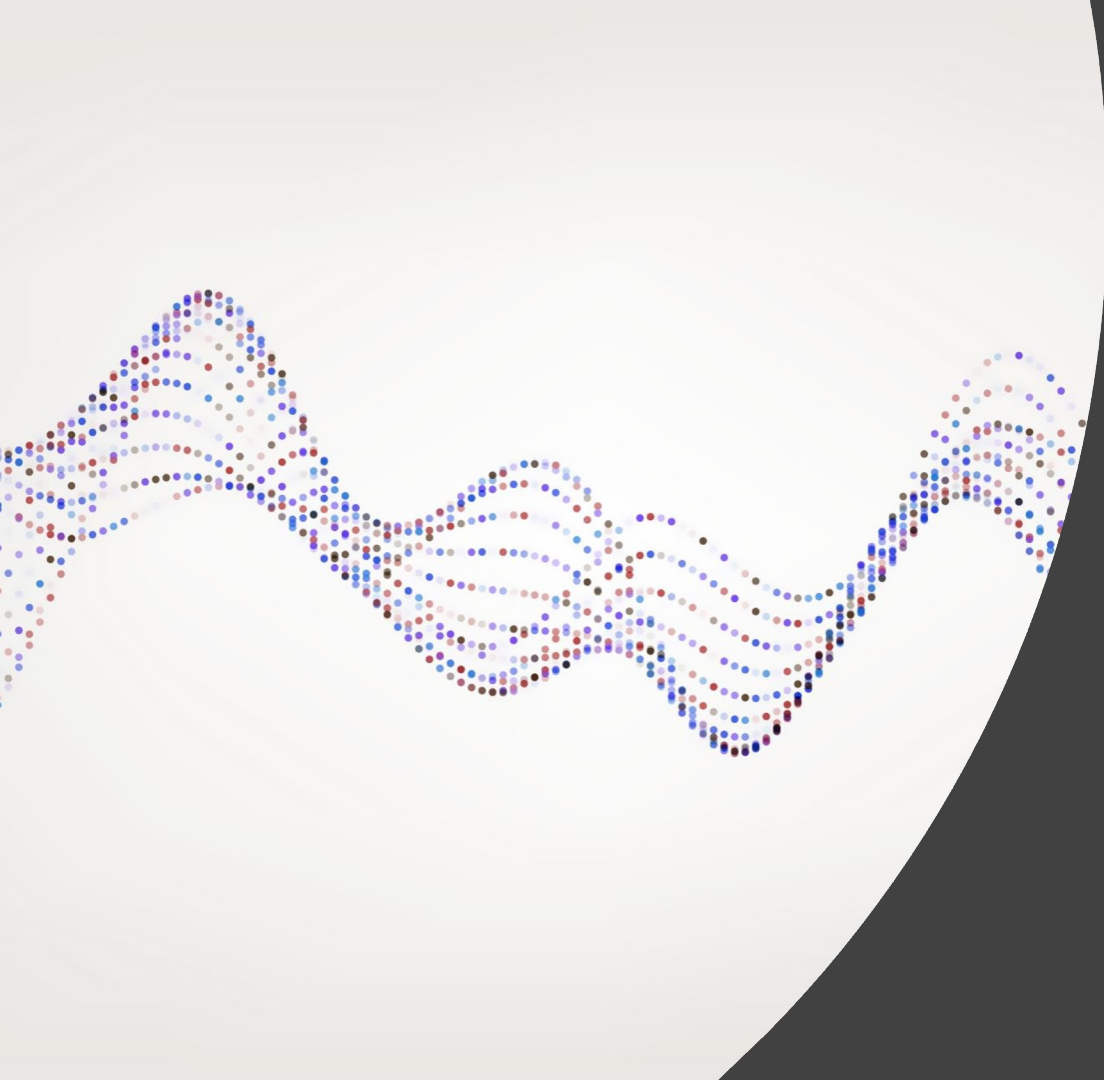




Best Practices

Building Good Component Practices





IQ Chrome Extension



SHIFTING LEFT

Allows developers to inspect a package before you download it so to help choosing better components early on.

ACTIONABLE DATA

The data is sourced from Sonatype Nexus Lifecycle's IQ Server, which accesses the Sonatype Data Services for those supported ecosystems providing remediation information.

EASY TO USE

When the developer browses to a website that is covered by the tool, such as Maven Central and click on the plugin, it will open with the Sonatype Lifecycle data relevant to that library.



nexus lifecycle - Chrome Extension

The image displays two browser windows showing the Sonatype search.maven.org interface. The top window shows the 'Security' tab for the component 'org.apache.struts:struts2-core:2.5.10', highlighting a critical CVE-2017-5638 with a CVSS score of 10. The bottom window shows the 'Remediation' tab for the same component, advising an upgrade to version 2.5.17. A purple callout box on the right states: 'View component intelligence within browser when searching public repositories.'

Component: org.apache.struts:struts2-core:2.5.10

Security Tab:

- CVE-2017-5638** (CVSS:10)
- Reference: [CVE-2017-5638](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638)
- Severity: 10
- Source: cve
- Threat Category: critical
- url: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638>

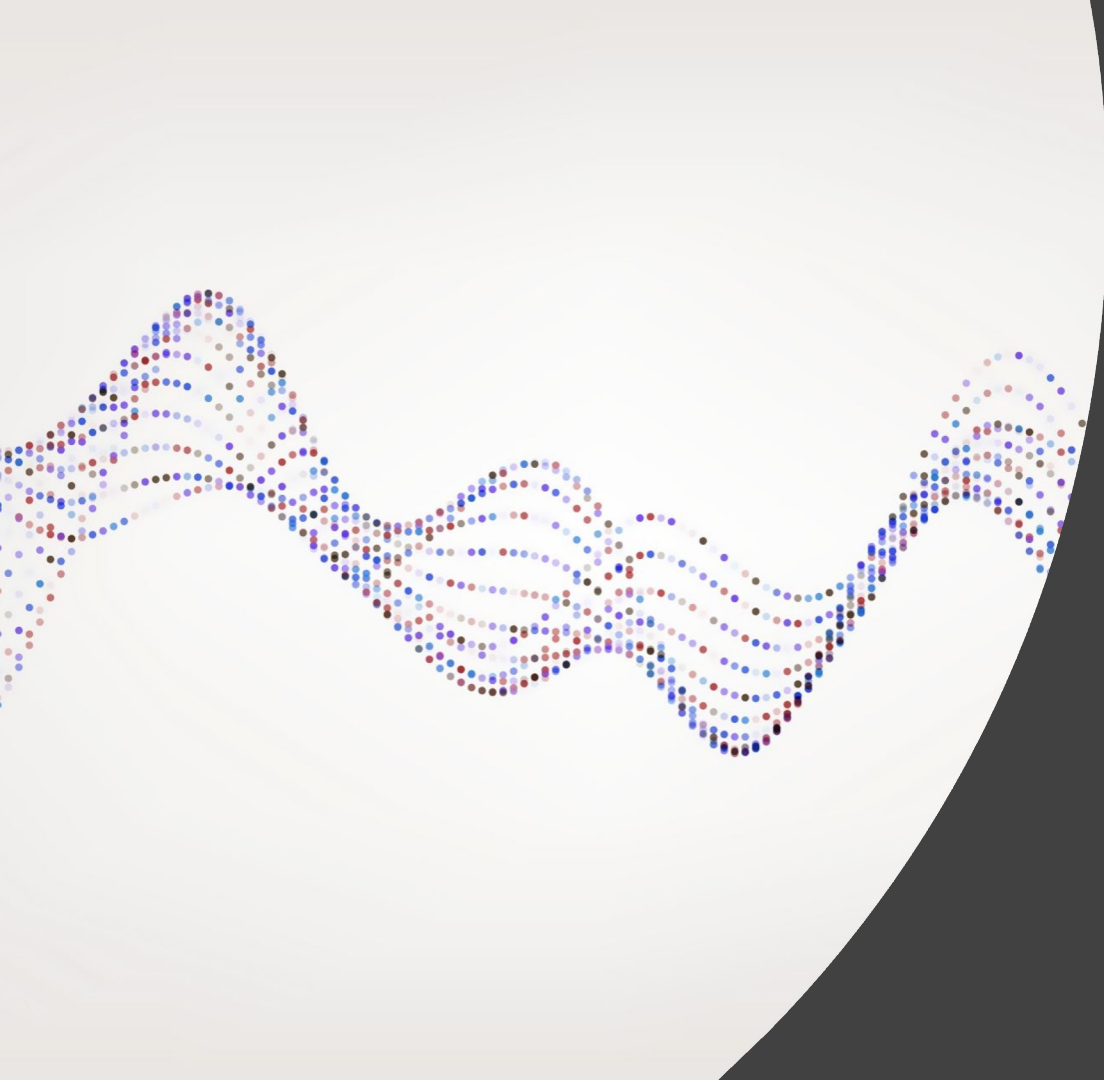
CVE	CVSS
CVE-2017-12611	CVSS:9.8
CVE-2018-11776	CVSS:8.1
CVE-2017-9804	CVSS:7.5
SONATYPE-2017-0173	CVSS:7.1
CVE-2017-7672	CVSS:5.9

Remediation Tab:

Remediation advice Upgrade to the new version: 2.5.17

Popularity: Older This Version Newer

Policy Threat Details: Security, License, Quality, Other



IDE Integrations Eclipse



SHIFTING LEFT

Provides development teams with direct access to Sonatype's component intelligence. Developers can quickly review components used in an application against their organization's OS policies allowing them to choose better components before any build warnings or failures.

ACTIONABLE DATA

Developers can investigate and fix policy violations getting immediate feedback on component quality right in the IDE allowing for informed decisions about component selection.

EASY TO USE

Administrators can communicate software quality expectations early on in the SDLC and developers can work in an environment they are familiar with.



nexus lifecycle - IDE Integration

Identify which components violate policy from within the IDE.

Policy Violations

Policy	Constraint	Summary
Security-High	High risk CVSS score	Found security vulnerability sonatype-2015-0002 with severity 9.0.
		Found security vulnerability sonatype-2015-0002 with severity 9.0.
		Found security vulnerability sonatype-2015-0002 with status 'Open', not 'Not Applicable'.
Architecture-Quality	Version is old	Age was 10 years, 9 months and 7 days

License Analysis

Threat Level	Declared License(s)	Observed License(s)
Liberal	Apache-2.0	Apache-2.0

Security Issues

Threat Level	Problem Code	Status	Summary
9	SONATYPE-2015-0002	Open	Arbitrary remote code execution with InvokerTransformer. Exploit Details: https://support.sonatype.com/hc/en-us/articles/214155137-Commons-collections-unintended-execution-in-deserialization-

Component Info

Group: commons-collections
Artifact: commons-collections
Version: 3.2.1
Declared License: Apache-2.0
Observed License: Apache-2.0
Effective License: Apache-2.0
Highest Policy Threat: 9 within 2 policies
Highest CVSS Score: 9
Cataloged: 10 years ago
Match State: exact
Identification Source: Sonatype
Category: Programming Language Utilities

[View Details](#) [Migrate](#)

Popularity

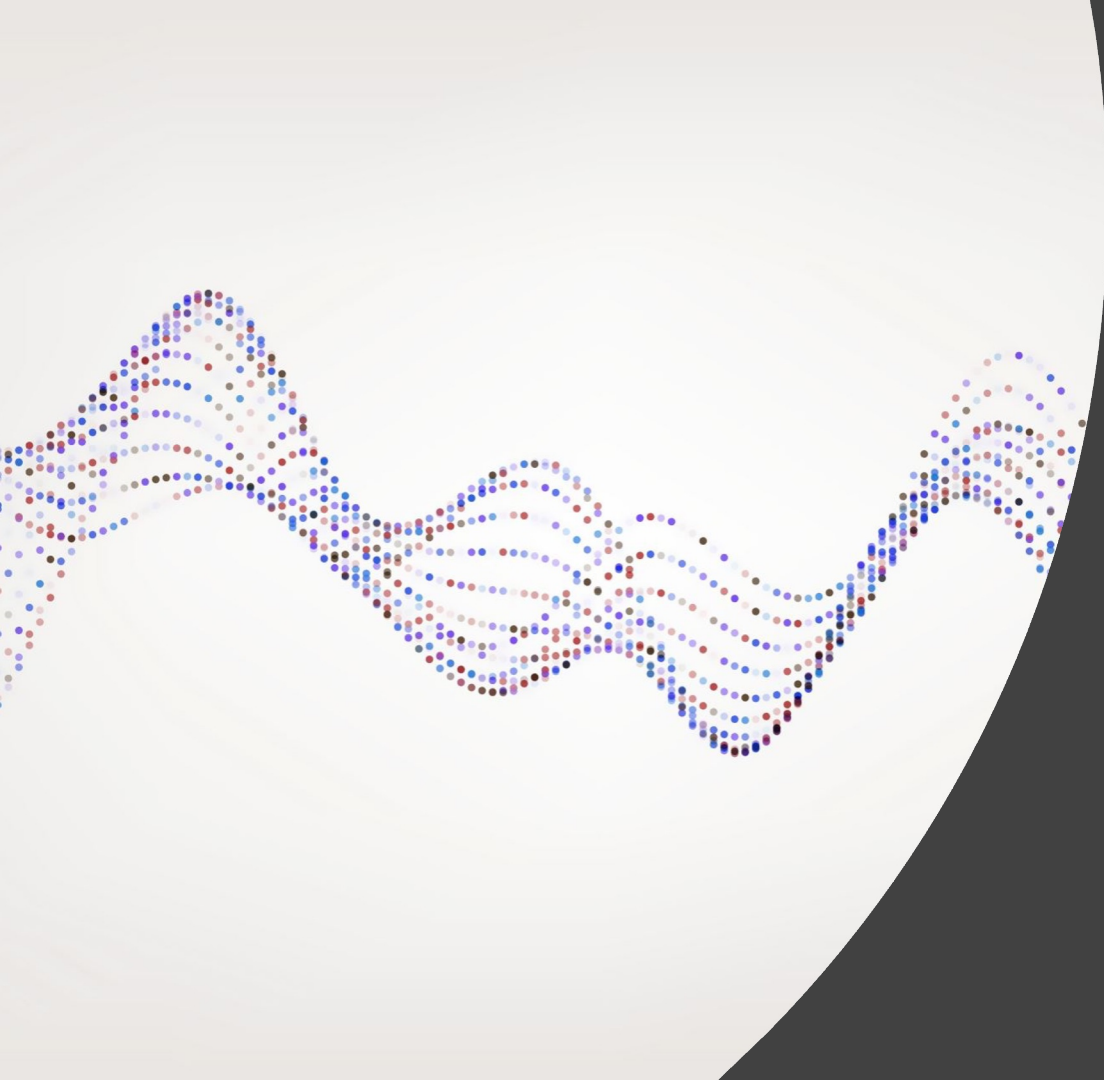
Older This Version Newer

Policy Threat

[Hide Details](#)
Security
License
Quality
Other

Select best component version based on real-time intelligence.

Migrate to approved version with one click remediation.



CI/CD

SHIP-HATS GitLab Integration



SHIFTING LEFT

Provides early insight into an application's security and licensing risk by analyzing the open source referenced in the code. It is designed to work *directly within* your SCM.

ACTIONABLE DATA

If a component violates a policy that the organization has set in Nexus IQ, IQ takes action communicating its findings and generating suggested remediation directly into the source code repository by initiating Automated Commit Feedback, Automated Pull Requests, and Pull Request Commenting with the changes to the application's component manifest.

EASY TO USE

Nexus IQ interacts with Git-based systems through this integration enabling the automatic creation of PRs, commenting on PRs, etc and showing it into the source control repository.



nexus lifecycle - Automated Pull Requests

Precise intelligence on what version to migrate to based on open source policy.

Advanced remediation guidance eliminates noise found in other solutions.

Code Issues 0 Pull requests 1 Actions Projects 0 Wiki Security Insights Settings

Bump com.fasterxml.jackson.core:jackson-databind:2.9.9.3 to 2.10.0 #2

[Open](#) collinpeters wants to merge 1 commit into master from com.fasterxml.jackson.core/jackson-databind/2.9.9.3-to-2.10.0

Conversation 0 Commits 1 Checks 0 Files changed 1 +1 -1

collinpeters commented 5 days ago

This automated pull request fixes a Nexus IQ policy violation

Description

Bump component `com.fasterxml.jackson.core:jackson-databind:2.9.9.3` to version 2.10.0 to remediate the following policy violations

Policy

Policy	Threat	Constraint	Conditions
Security-High	9	High risk CVSS score	Found security vulnerability CVE-2019-14540 with severity 7.5. Found security vulnerability CVE-2019-16335 with severity 7.5. Found security vulnerability CVE-2019-17267 with severity 7.5. Found security vulnerability sonatype-2019-0371 with severity 8.5.

Source

Application: My App
Organization: My Organization
Scan: 2b28f403fe99454684fbd4a073efcea7 [view detailed report](#)
Stage: build

This PR was automatically created by your friendly neighbourhood IQ server

Reviewers: No reviews

Assignees: No one assigned yourself

Labels: None yet

Projects: None yet

Milestone: No milestone

Notifications: [Subscribe](#)

You're not receiving notifications from this thread.

1 participant

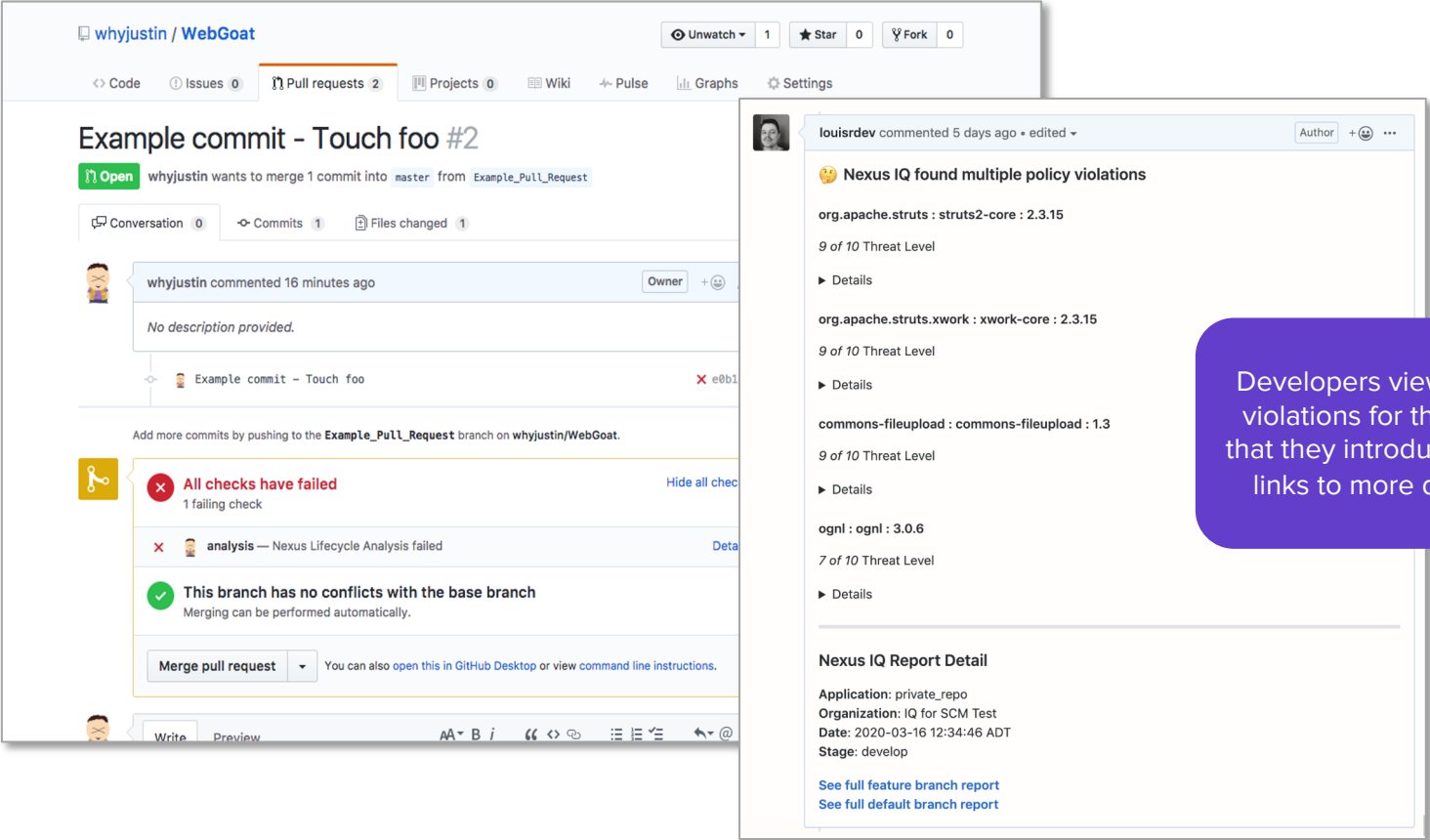
[Lock conversation](#)

maven



Links to learn more about the violation and vulnerability.

nexus lifecycle - Policy Violations in SCM



Example commit - Touch foo #2

[Open](#) whyjustin wants to merge 1 commit into master from Example_Pull_Request

Conversation 0 Commits 1 Files changed 1

whyjustin commented 16 minutes ago

No description provided.

Example commit - Touch foo

Add more commits by pushing to the Example_Pull_Request branch on whyjustin/WebGoat.

All checks have failed 1 failing check

analysis — Nexus Lifecycle Analysis failed

This branch has no conflicts with the base branch
Merging can be performed automatically.

[Merge pull request](#) You can also open [this in GitHub Desktop](#) or view [command line instructions](#).

Nexus IQ found multiple policy violations

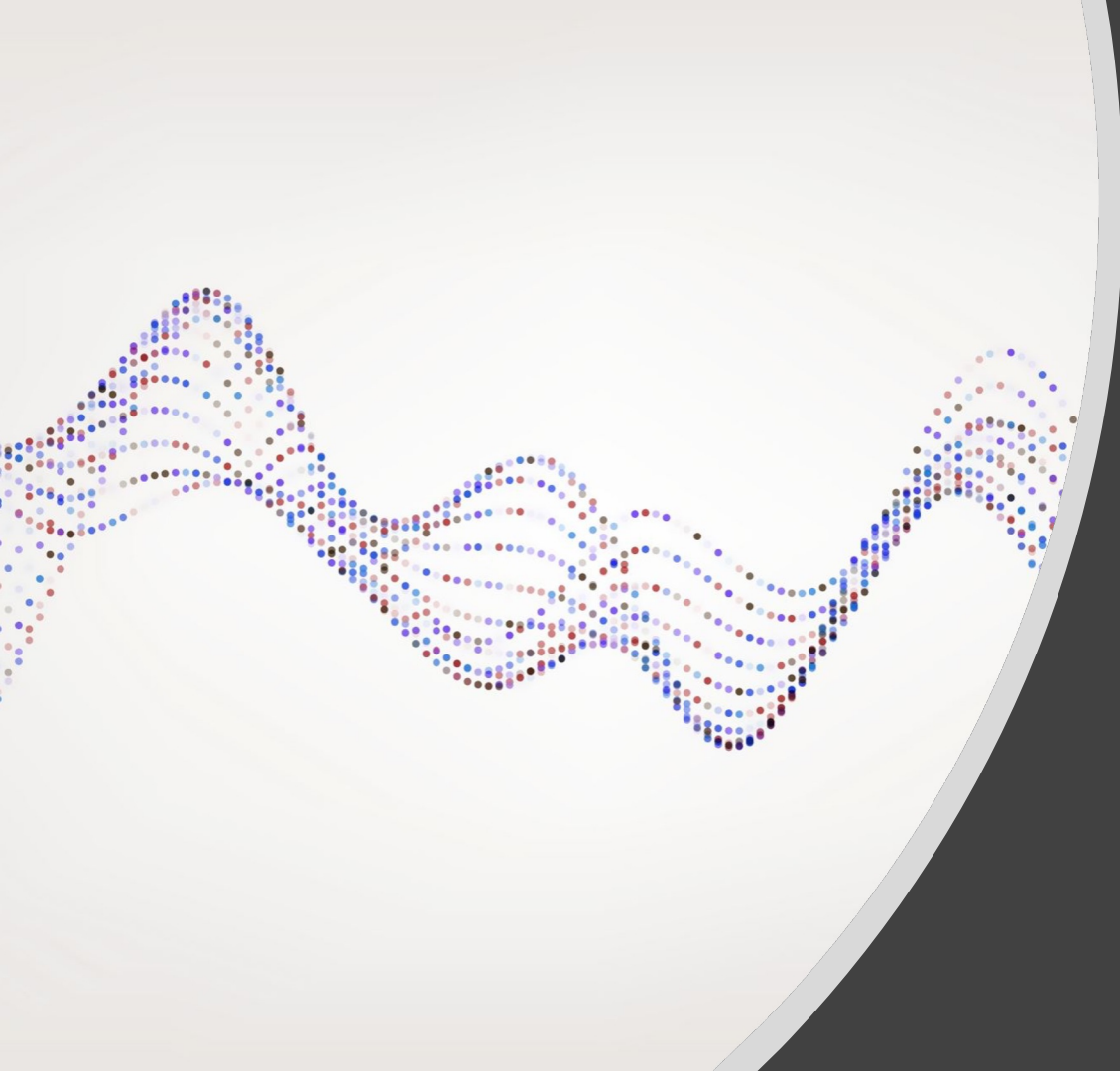
- org.apache.struts : struts2-core : 2.3.15
9 of 10 Threat Level
[Details](#)
- org.apache.struts.xwork : xwork-core : 2.3.15
9 of 10 Threat Level
[Details](#)
- commons-fileupload : commons-fileupload : 1.3
9 of 10 Threat Level
[Details](#)
- ognl : ognl : 3.0.6
7 of 10 Threat Level
[Details](#)

Nexus IQ Report Detail

Application: private_repo
Organization: IQ for SCM Test
Date: 2020-03-16 12:34:46 ADT
Stage: develop

[See full feature branch report](#)
[See full default branch report](#)

Developers view policy violations for the code that they introduced with links to more details.



Sonatype Resources

Where to Next? -- Sonatype Learn

Sonatype Learn - the content you need when you need it.

- eLearning courses
- Course Ratings & Reviews
- Learning Paths to support your goals
- Find resources that continue your development
- Join the Sonatype Community

The image displays a Sonatype Learn interface. At the top right, the Sonatype logo and 'LEARN' link are visible. A 'SURVEY SAYS...' section features a gauge icon and four statistics: 92% for course recommendations, 95% for fulfilled expectations, 99% for application of knowledge, and 90% for confidence in knowledge. Below this is a 'Ratings and Reviews' pop-up showing a 5.0 average rating from 1 review, with a 'Write a Review' button. The main content area, titled 'Choose Your Path Below', offers three learning paths: 'INCREASE DEVELOPER PRODUCTIVITY', 'REDUCE OSS RISKS', and 'SHIFT LEFT: SECURE CODING PRACTICES', each with a descriptive paragraph and a 'Write a Review' button.

SURVEY SAYS... Here's what our learners are saying about our courses...

COURSE REVIEWS

- 92%** Would recommend our courses to a colleague.
- 95%** Had their learning expectations fulfilled.
- 99%** Anticipate using what they learned on the job.
- 90%** Feel confident about their knowledge of the topics covered.

Ratings and Reviews

★★★★★
5.0
Avg Rating
1 Rating

What's your experience? We'd love to know!
[Write a Review](#)

Choose Your Path Below

- INCREASE DEVELOPER PRODUCTIVITY**
Journey down the path of Increasing Developer Productivity. Learn the concepts of catching application security vulnerabilities and license requirements early and often. This can all be achieved by integrating Nexus IQ Server into your Continuous Integration (CI) model.
- REDUCE OSS RISKS**
Follow this learning path when you're ready to generate a Software Bill of Materials (SBOM). Immediately identify risks in new and existing components, flag violations, and receive recommendations to remediate risks.
- SHIFT LEFT: SECURE CODING PRACTICES**
Journey down the path of Shifting Left. Learn the concepts of creating superior software by identifying insecure coding practices that occur throughout the Software Development Life Cycle (SDLC). Discover why the Shift Left principle is important in development and security operations.



Community

Find answers and collaborate with other Sonatype users



Learn

Learn from Nexus Platform experts through self-paced online courses



Guides

Quick-start and technical guides for the Nexus Platform



Support

View the Knowledge Base or open a support ticket



Docs

Reference documentation for Sonatype products



Exchange

Find awesome Contributions from the Nexus Community



Labs

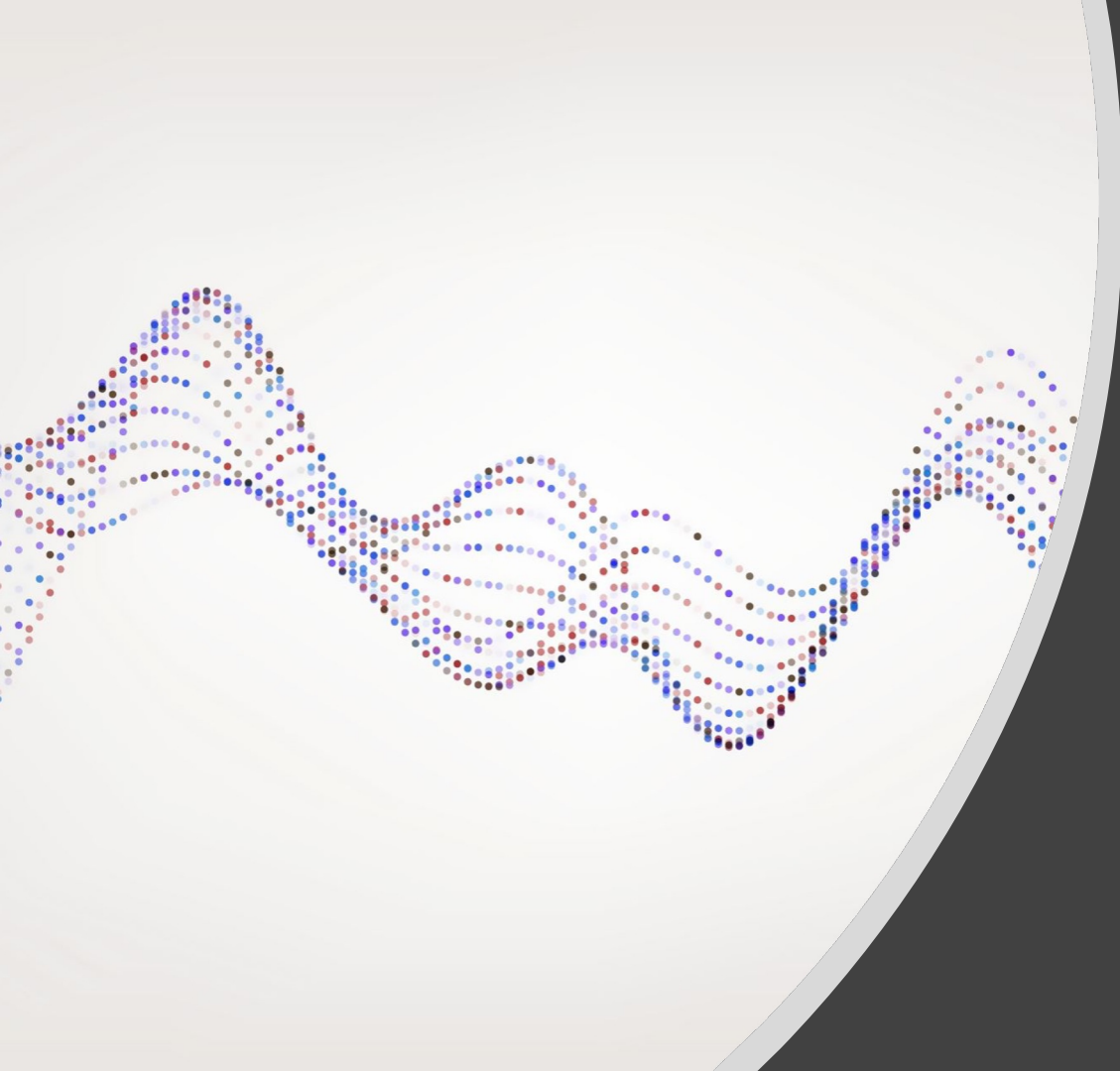
Browse Sonatype created experiments for the Nexus Platform



Ideas

Have an Idea for our Products? File one here!





Q&A