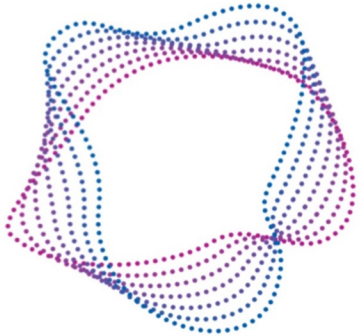
Best Practices with Sonatype

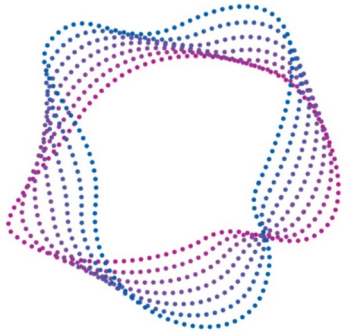


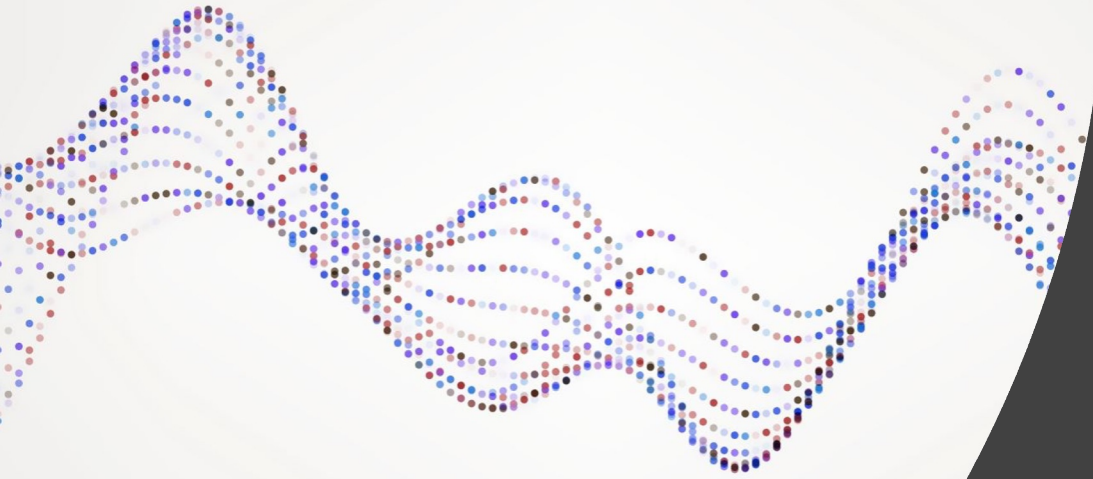
GOVTECH
SINGAPORE

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



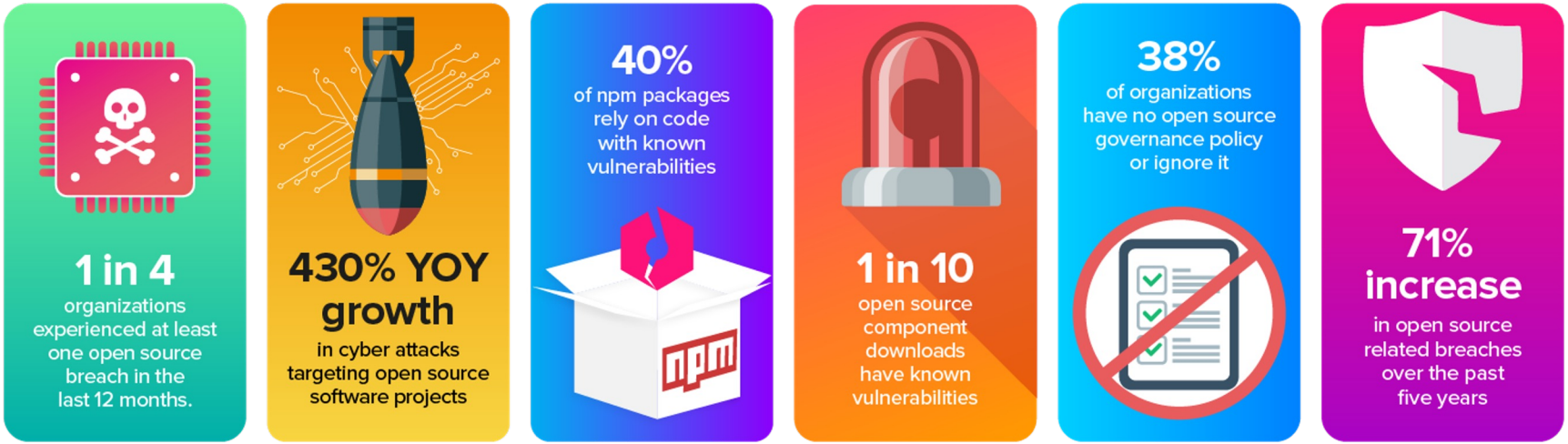


Benefits of Sonatype IQ for OSS Consumption

Open source is literally everywhere.

Not all OSS parts created equal.

Ages like milk, not wine.

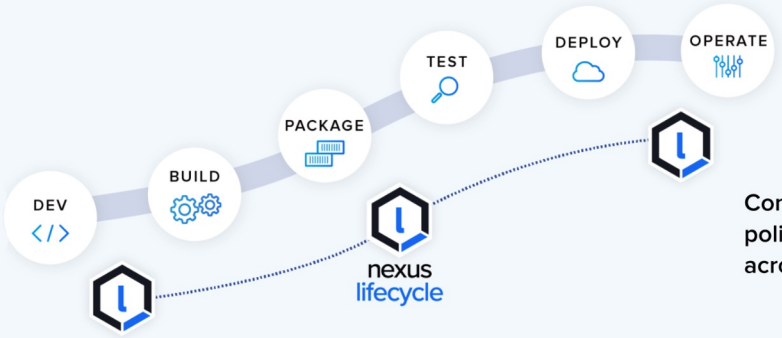


nexus lifecycle

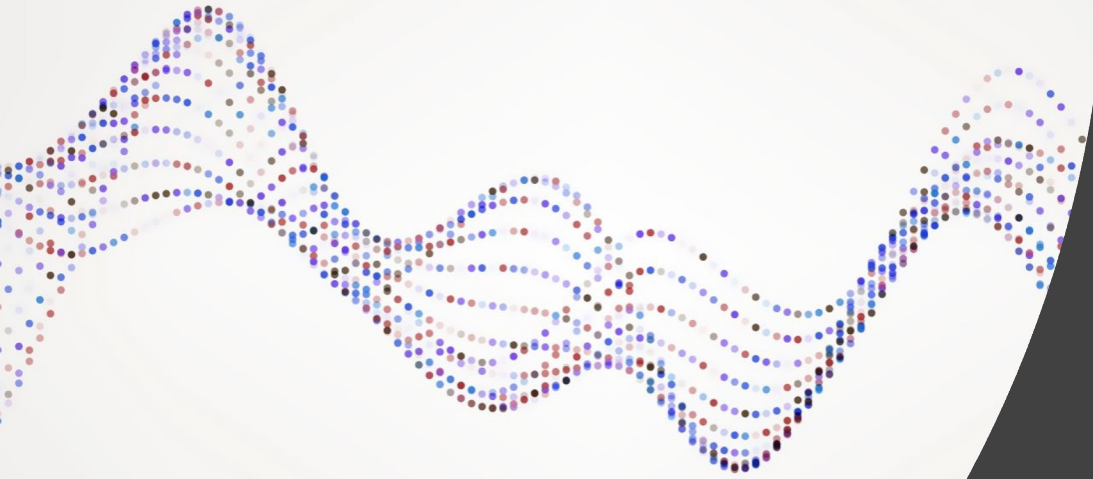
Eliminate open source risk across the entire SDLC.

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.

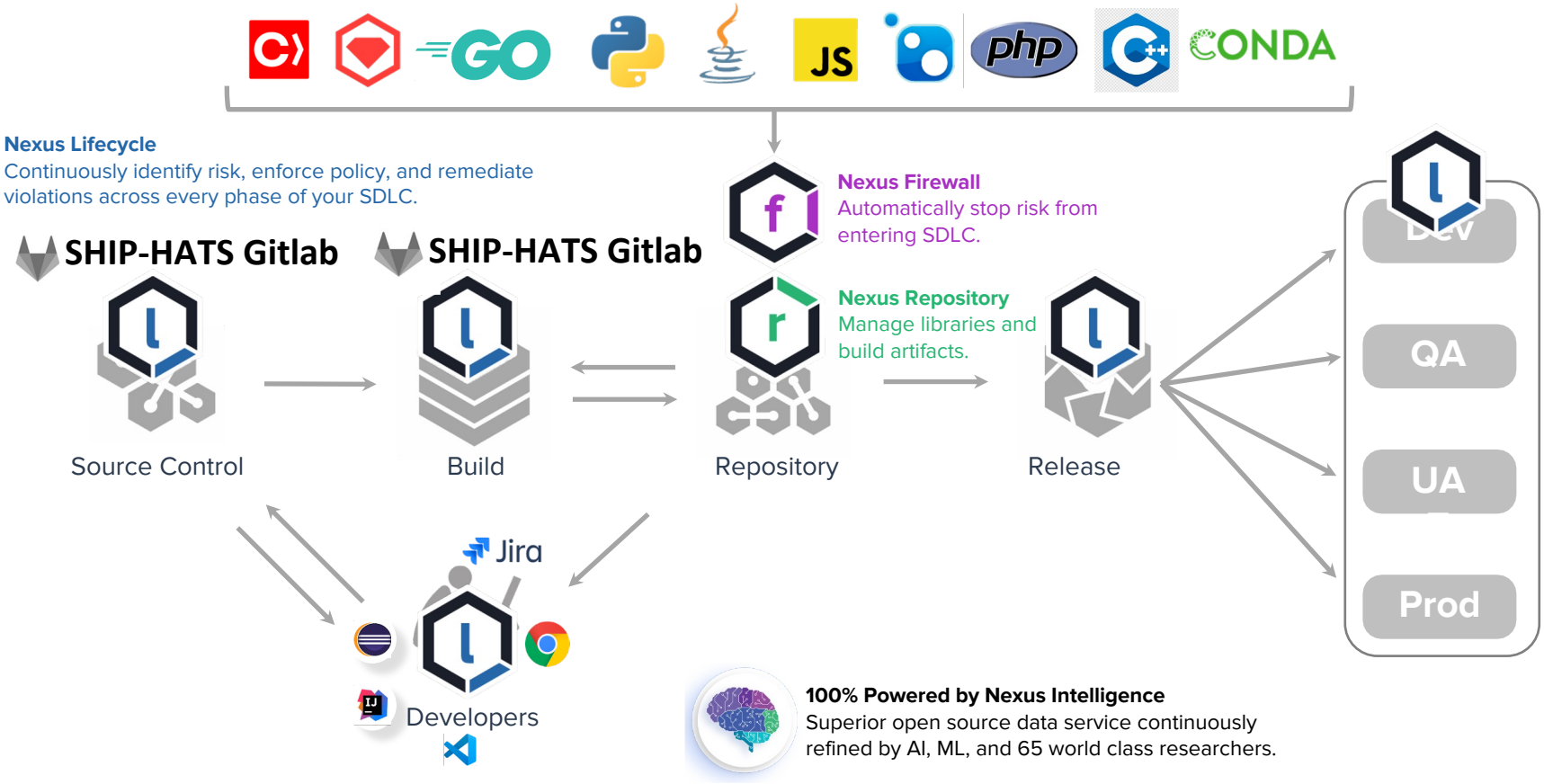


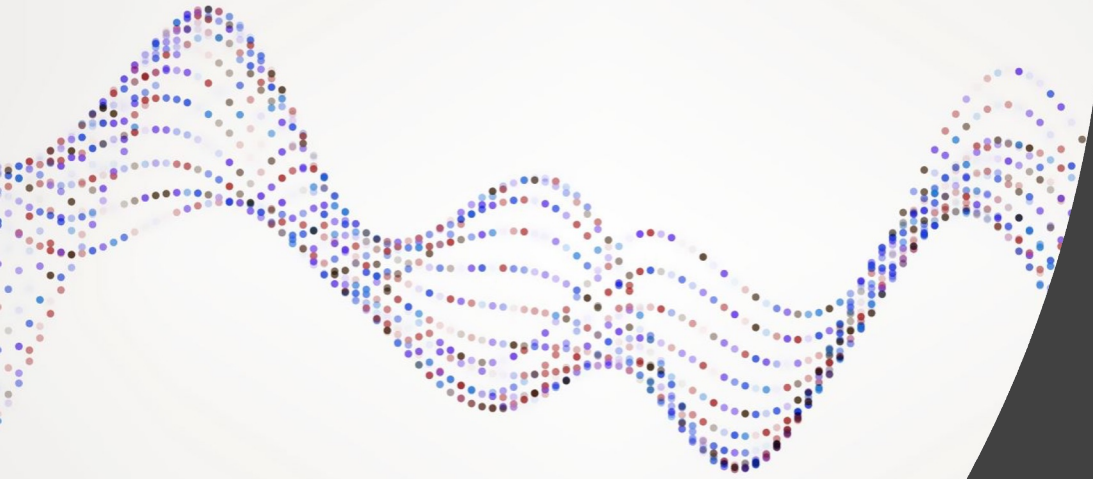
Continuously identify risk, enforce policy, and remediate vulnerabilities across every phase of your SDLC.



How Sonatype fits into your SHIP-HATS offering

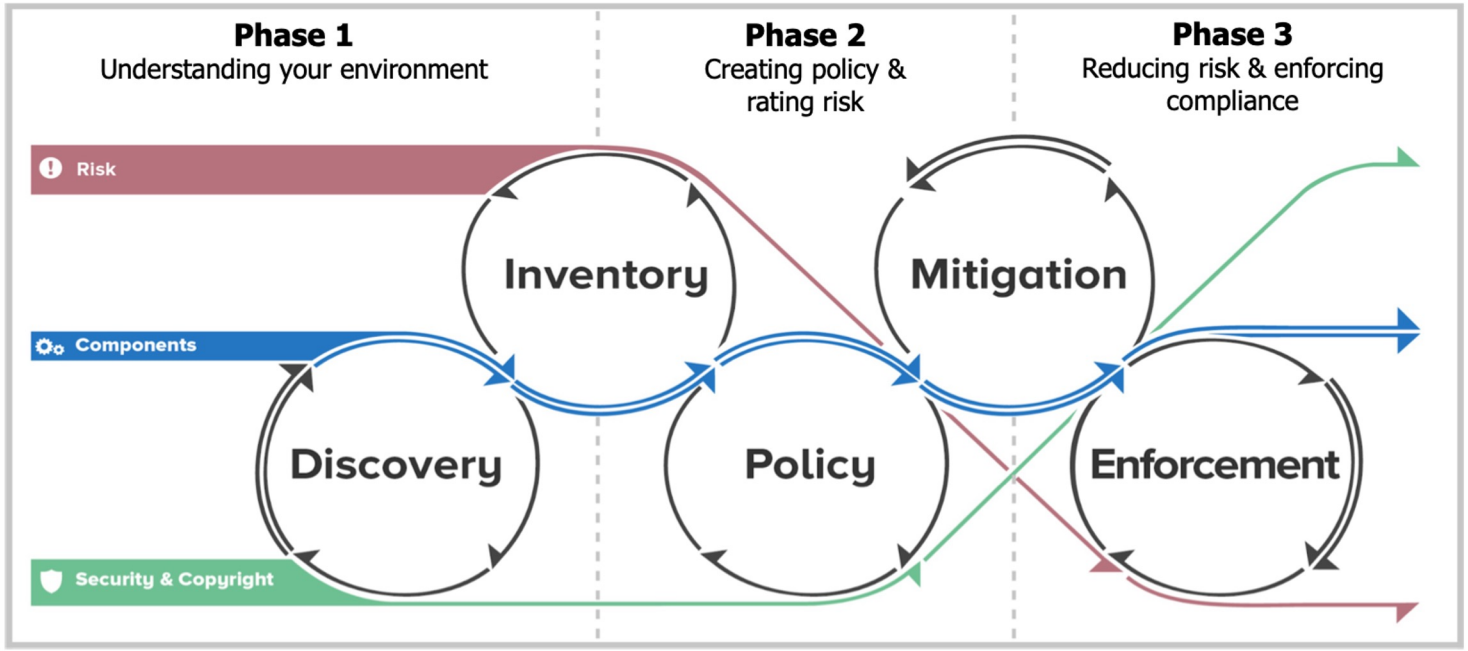
Nexus automatically enforces open source policy and controls risk across every phase of the SDLC.

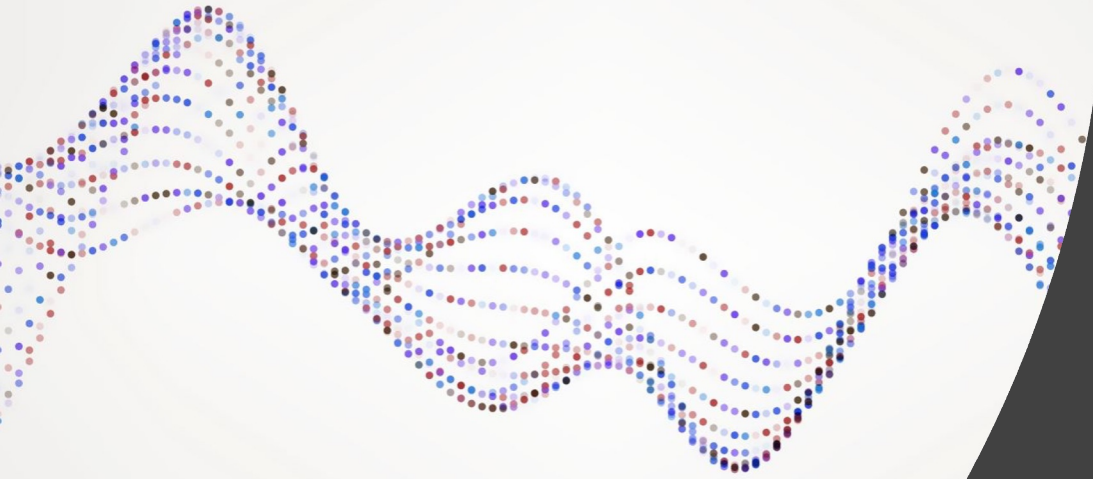




Best Practices

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.

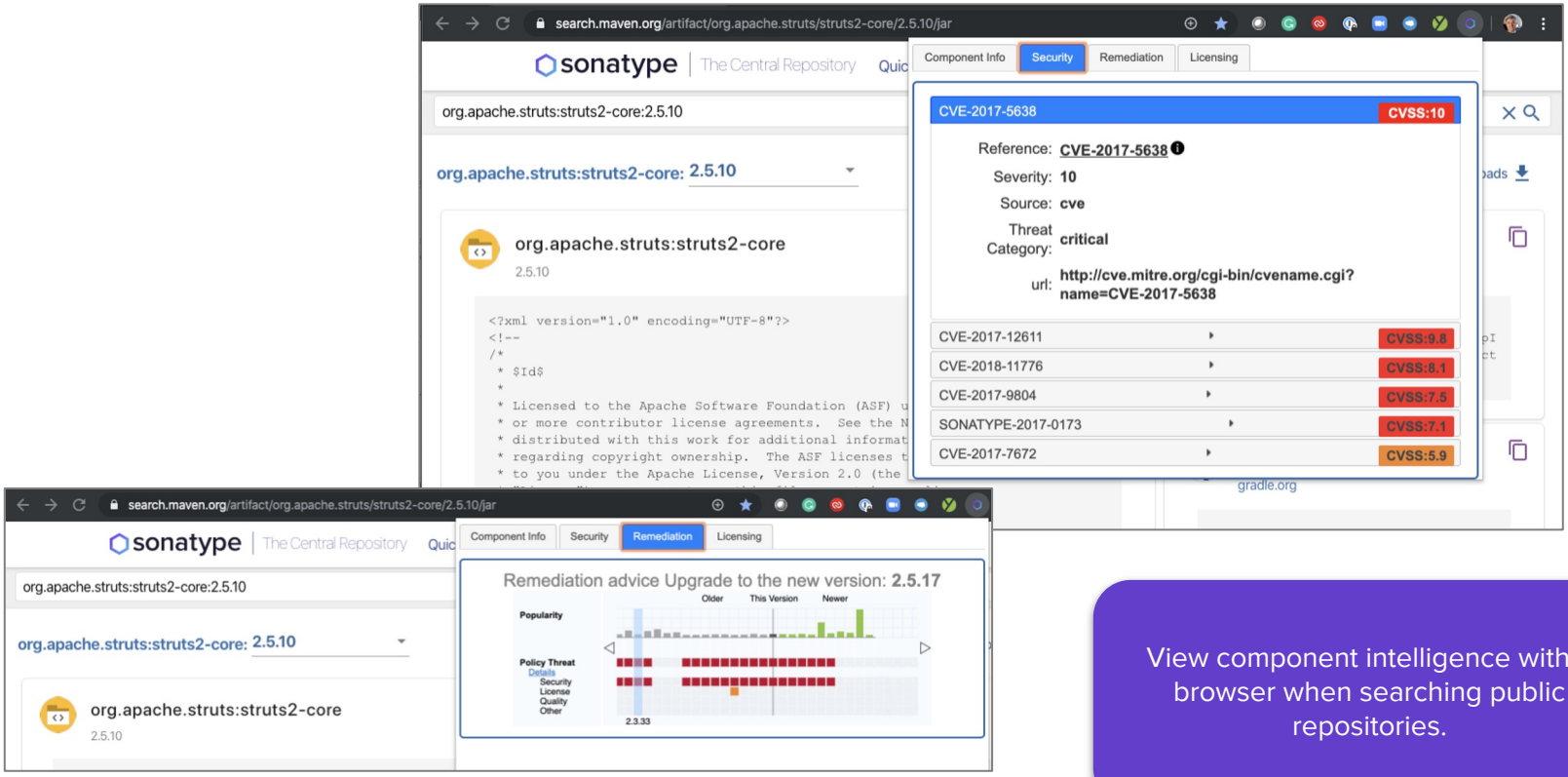
ACTIONABLE DATA

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

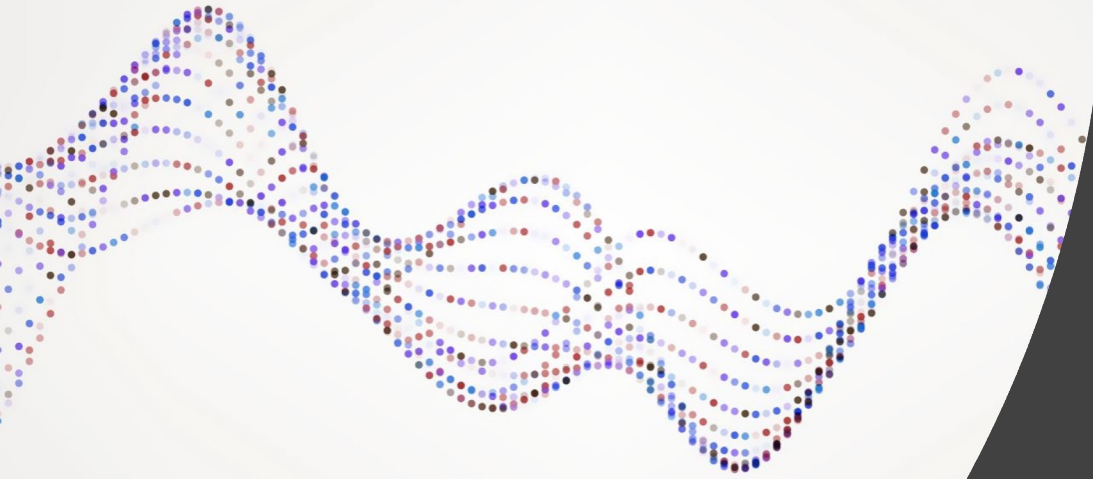
EASY TO USE

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



View component intelligence within browser when searching public repositories.



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.

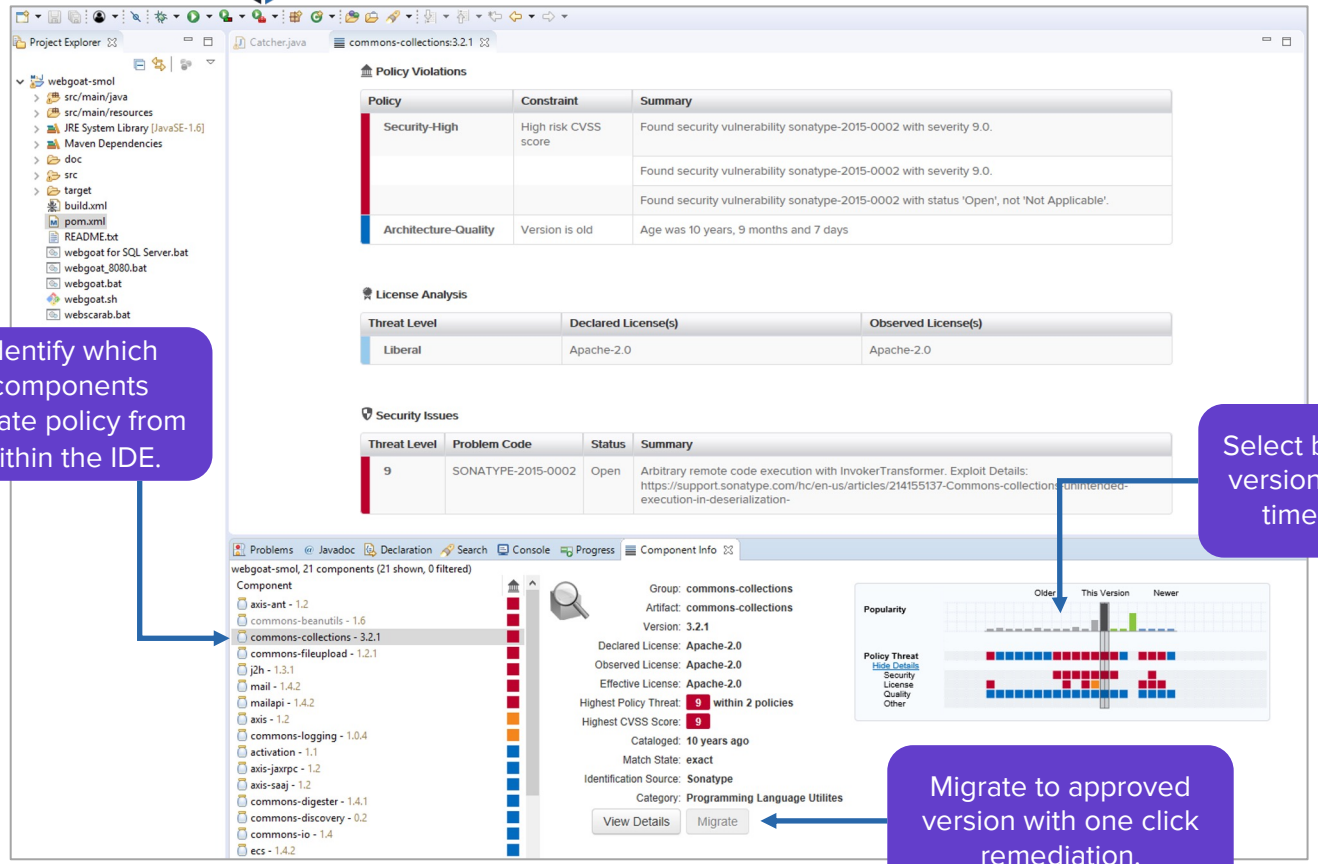
ACTIONABLE DATA

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.

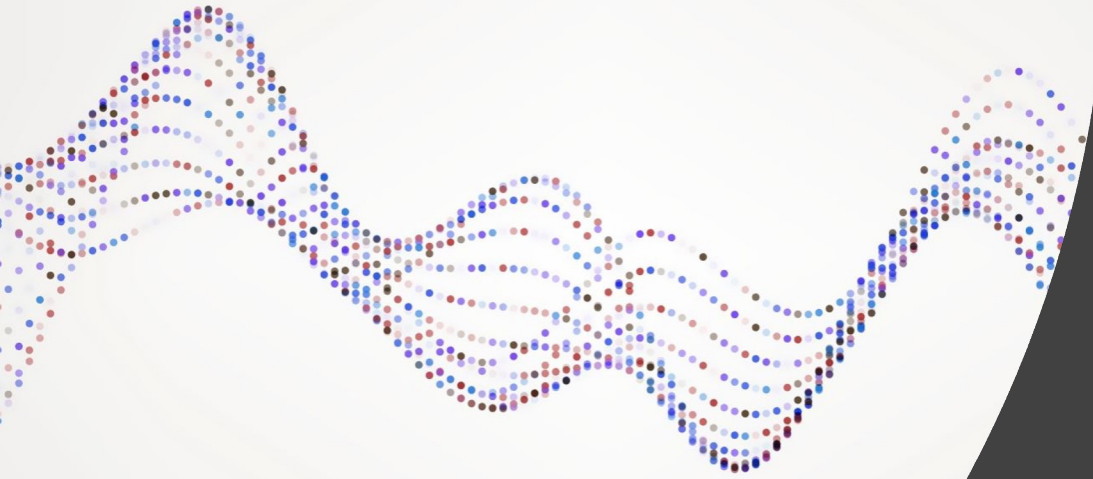
nexus lifecycle - IDE Integration



Identify which components violate policy from within the IDE.

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

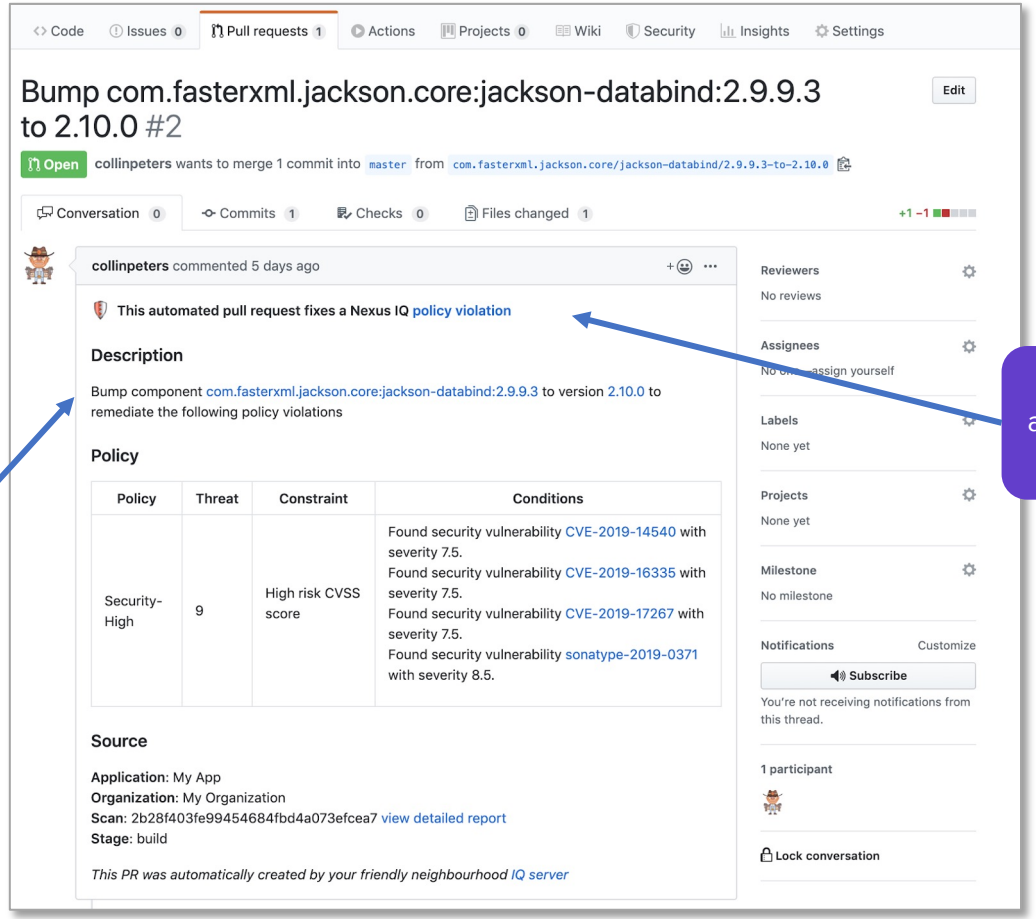
Nexus IQ interacts with Git-based systems through this integration enabling the automatic creation of PRs, commenting on PRs, etc and showing it into the source control repository.

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.

Links to learn more about the violation and vulnerability.



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

Edit

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—assign yourself

Labels
None yet

Projects
None yet

Milestone
No milestone

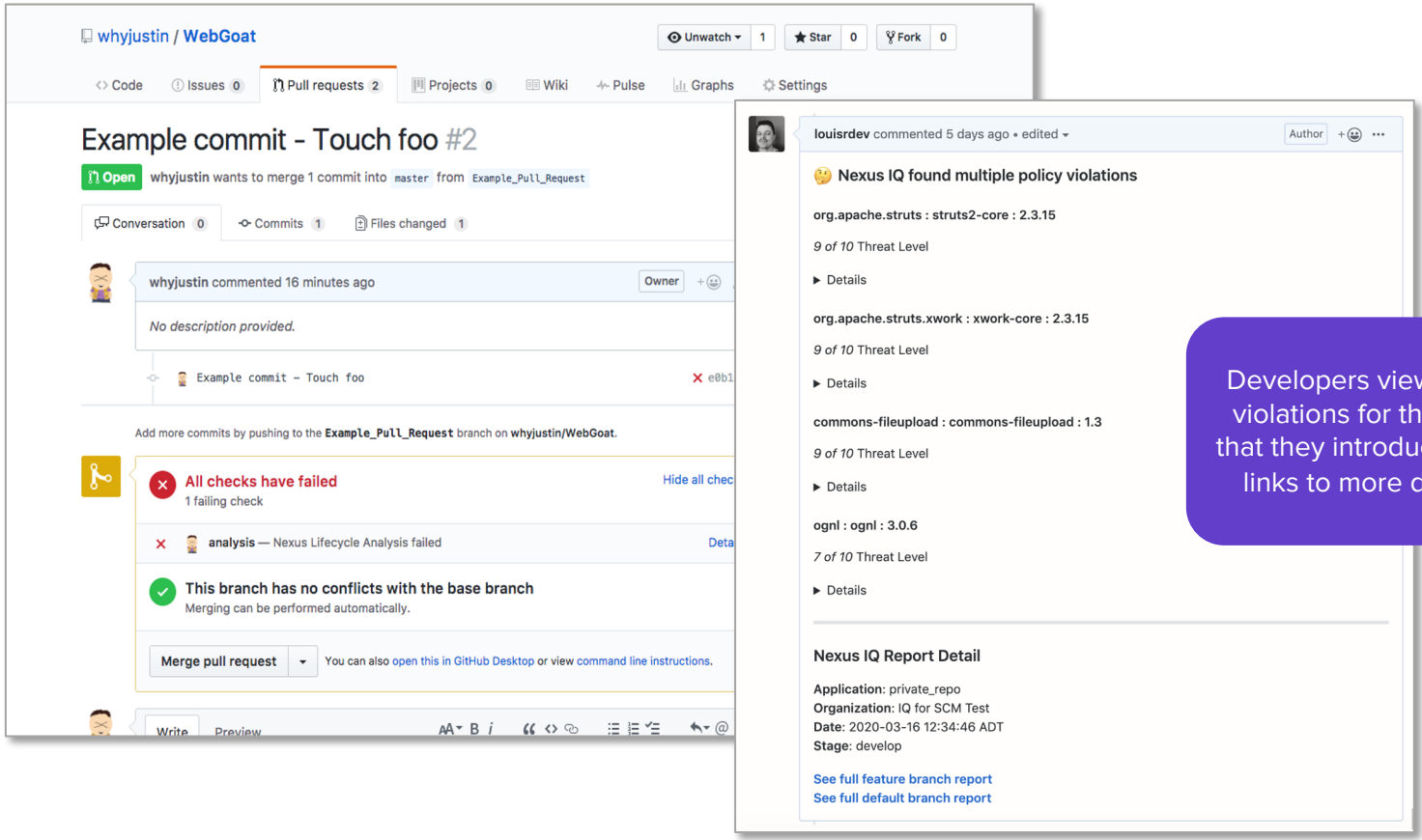
Notifications Customize
Subscribe
You're not receiving notifications from this thread.

1 participant

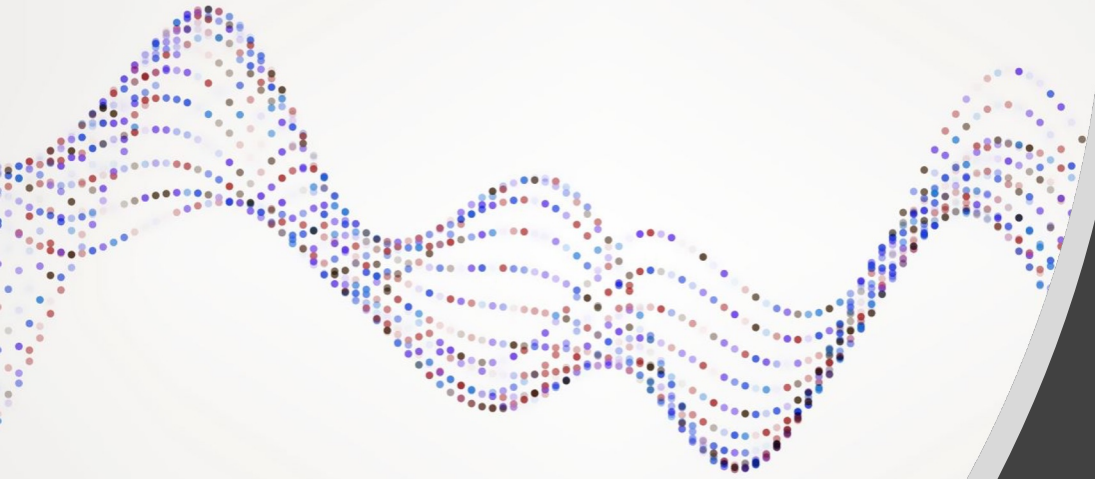
Lock conversation

maven + npm

nexus lifecycle - Policy Violations in SCM



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

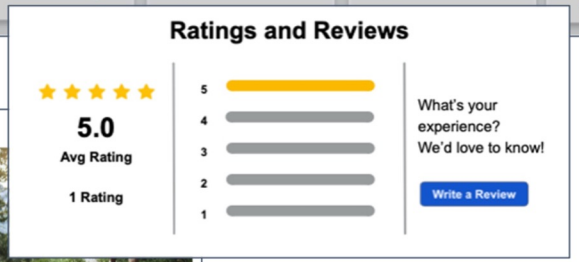


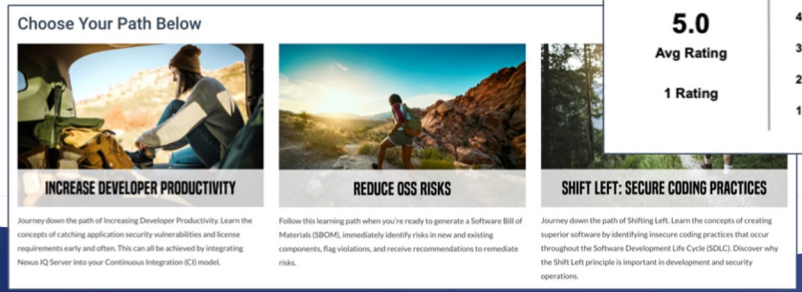
Sonatype Resources

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





sonatype | MY SONATYPE Community Exchange Learn Support Who is Sonatype? Sign In

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

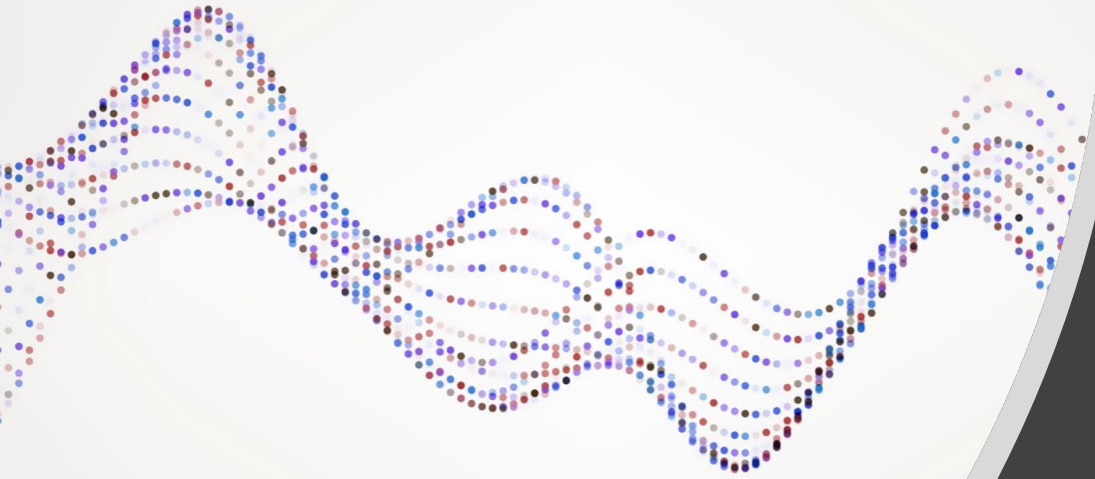
Docs
Reference documentation for Sonatype products

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!

sonatype



Q&A