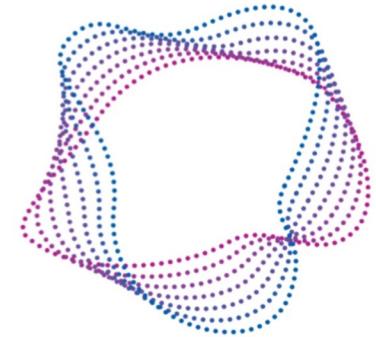


# Best Practices with Sonatype



GOVTECH  
SINGAPORE



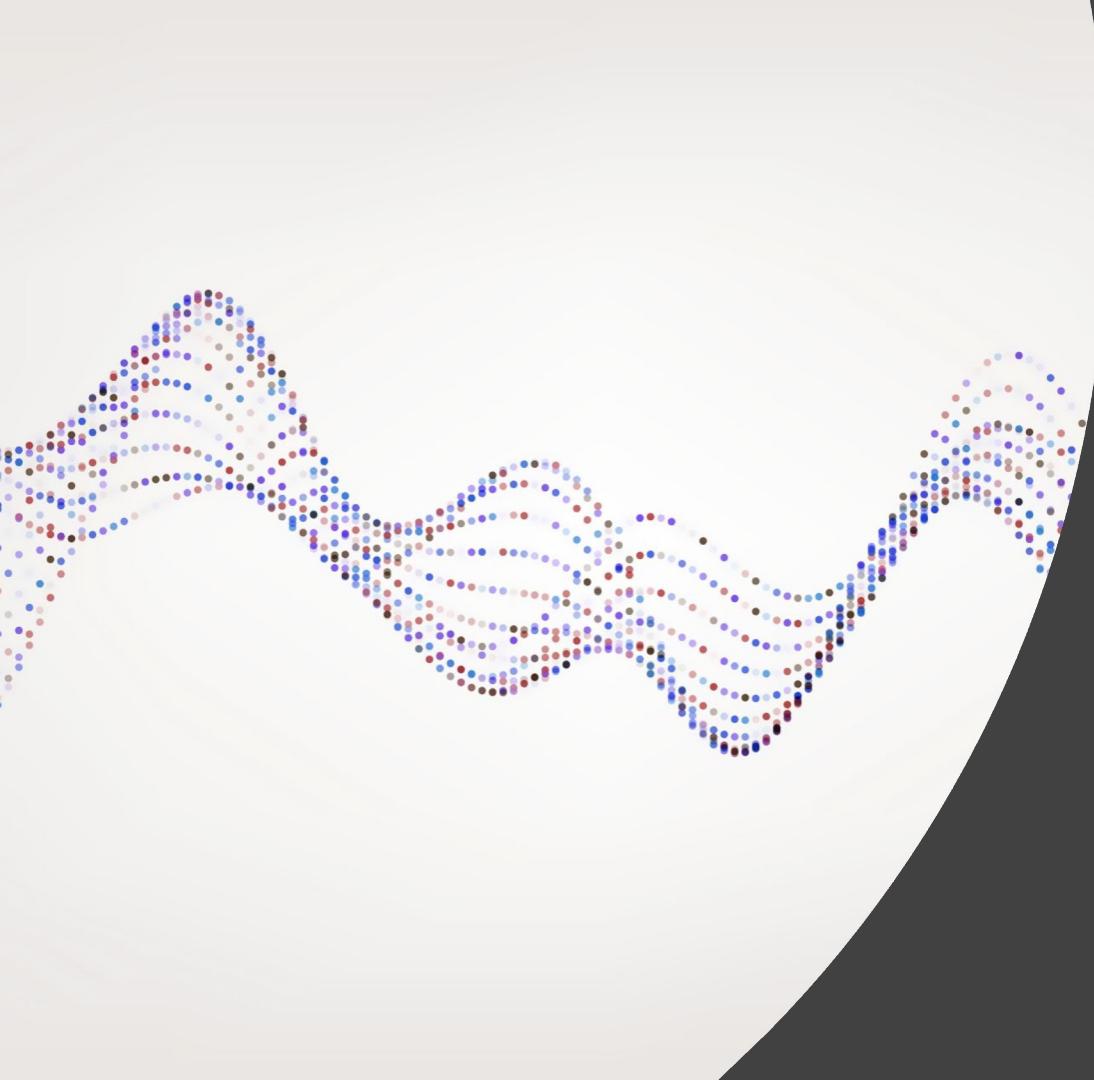
sonatype

# 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



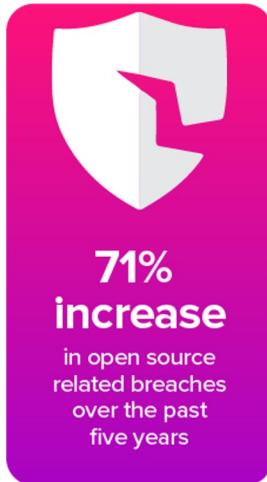
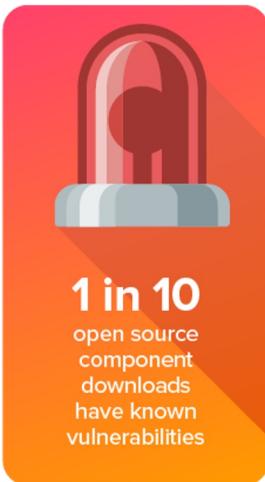


# Benefits of Sonatype IQ for OSS Consumption

# Open source is literally everywhere.

## Not all OSS parts created equal.

*Ages like milk, not wine.*



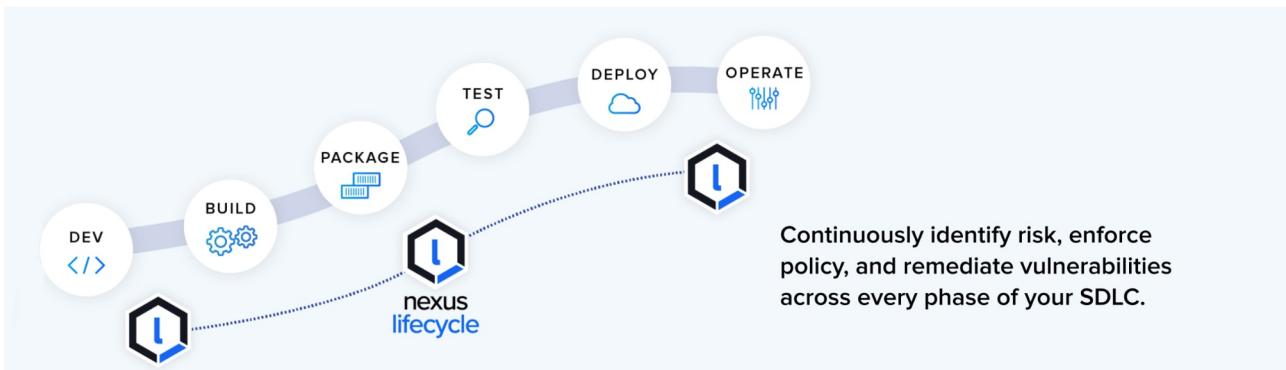


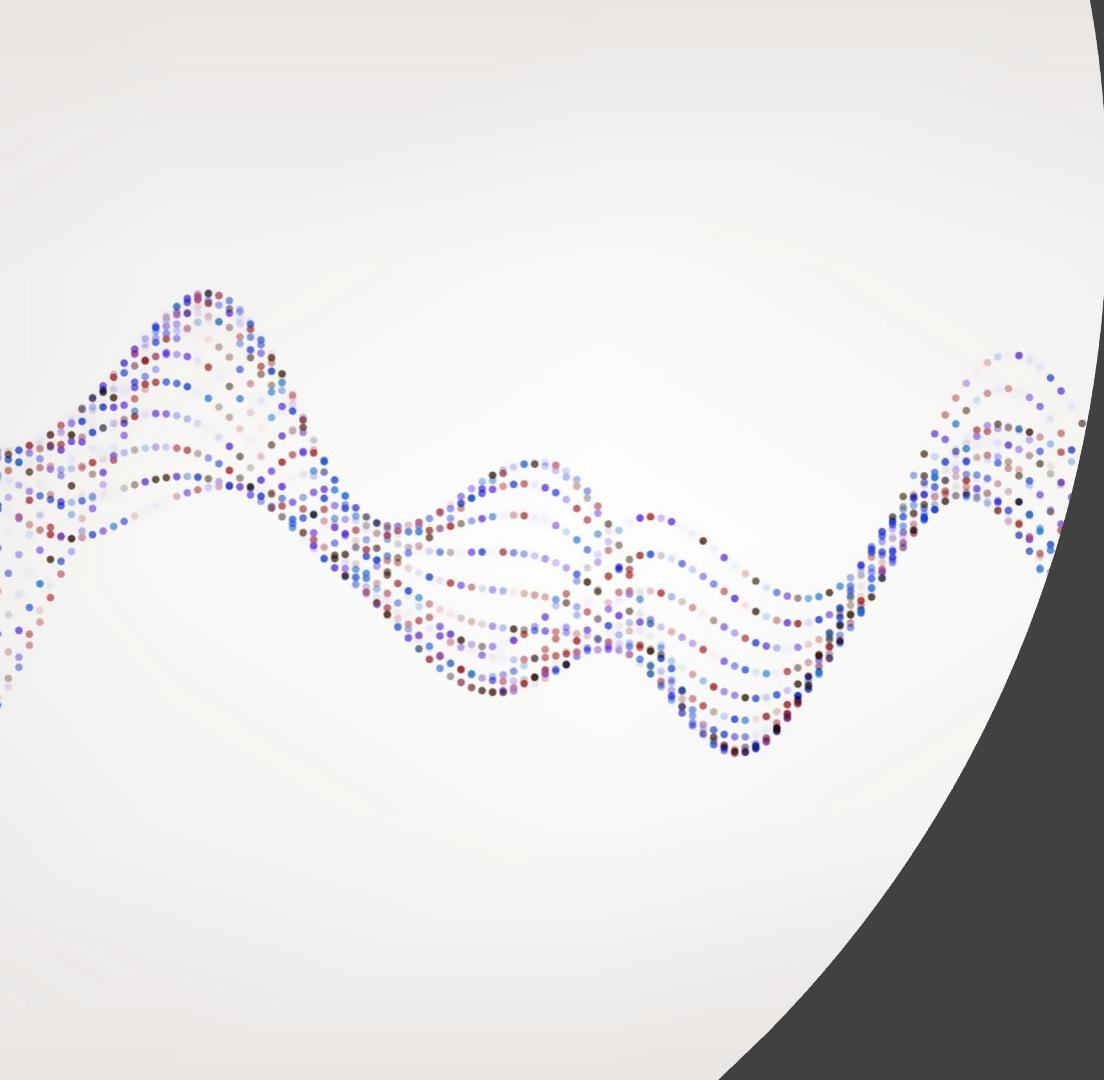
# nexus lifecycle

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.





# 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.

SHIP-HATS Gitlab



Source Control

SHIP-HATS Gitlab



Build



**Nexus Firewall**

Automatically stop risk from entering SDLC.



Repository

**Nexus Repository**

Manage libraries and build artifacts.



Release



DEV

QA

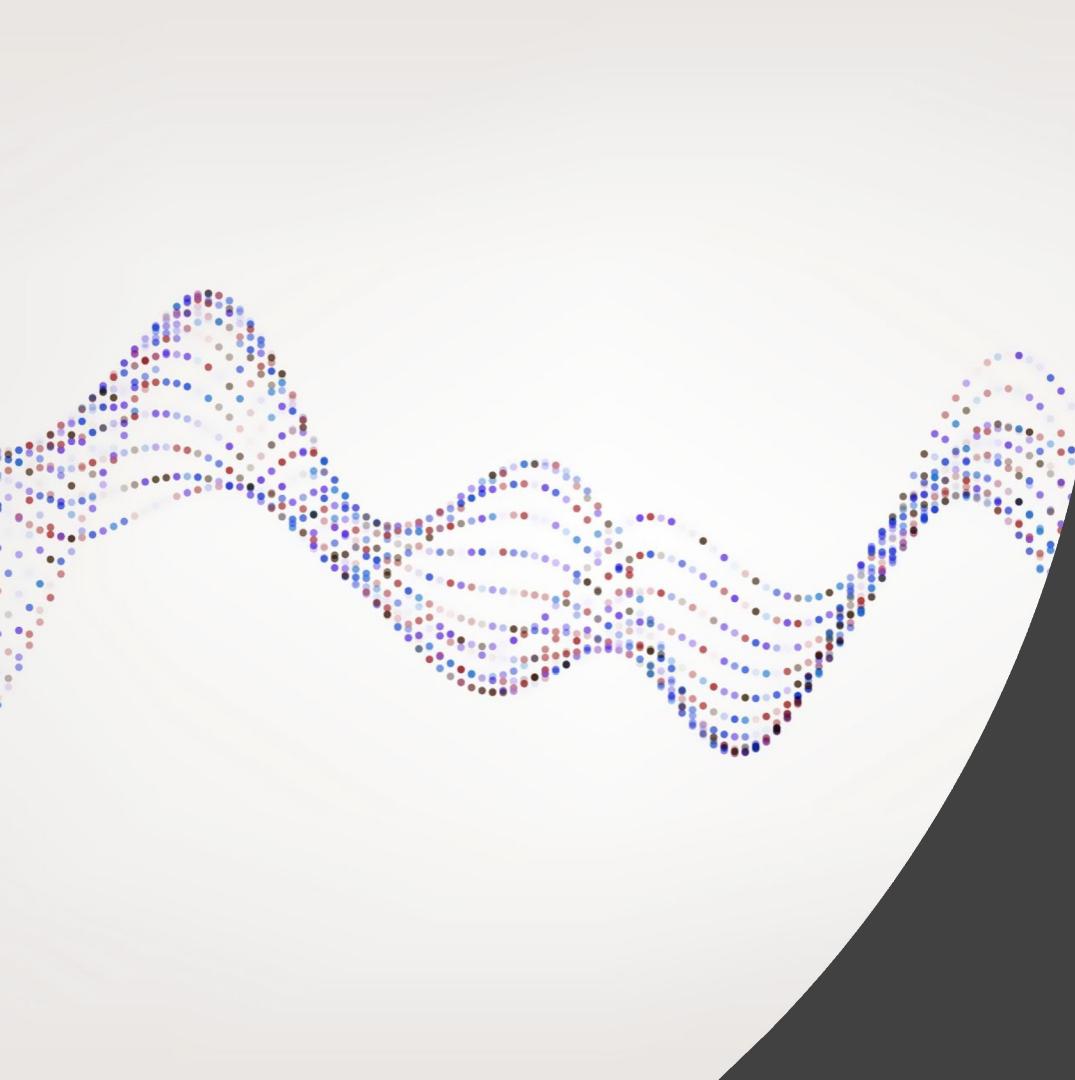
UA

Prod



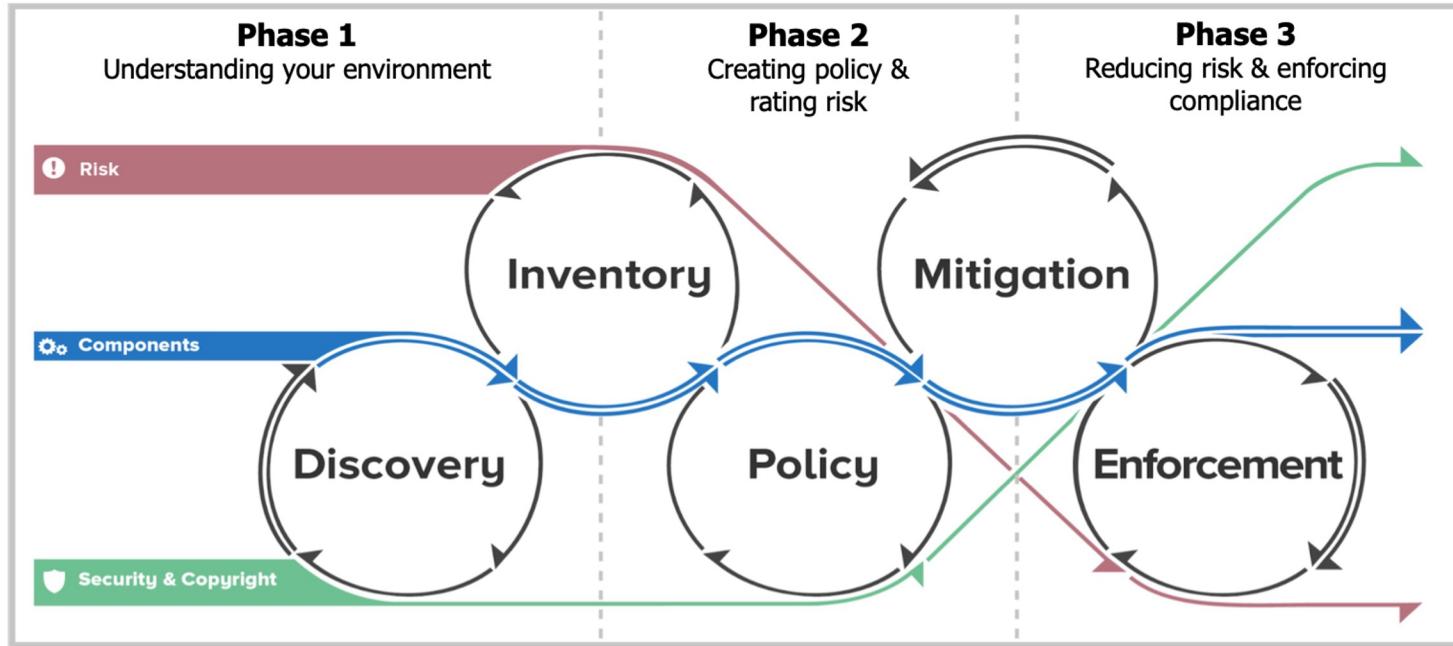
**100% Powered by Nexus Intelligence**

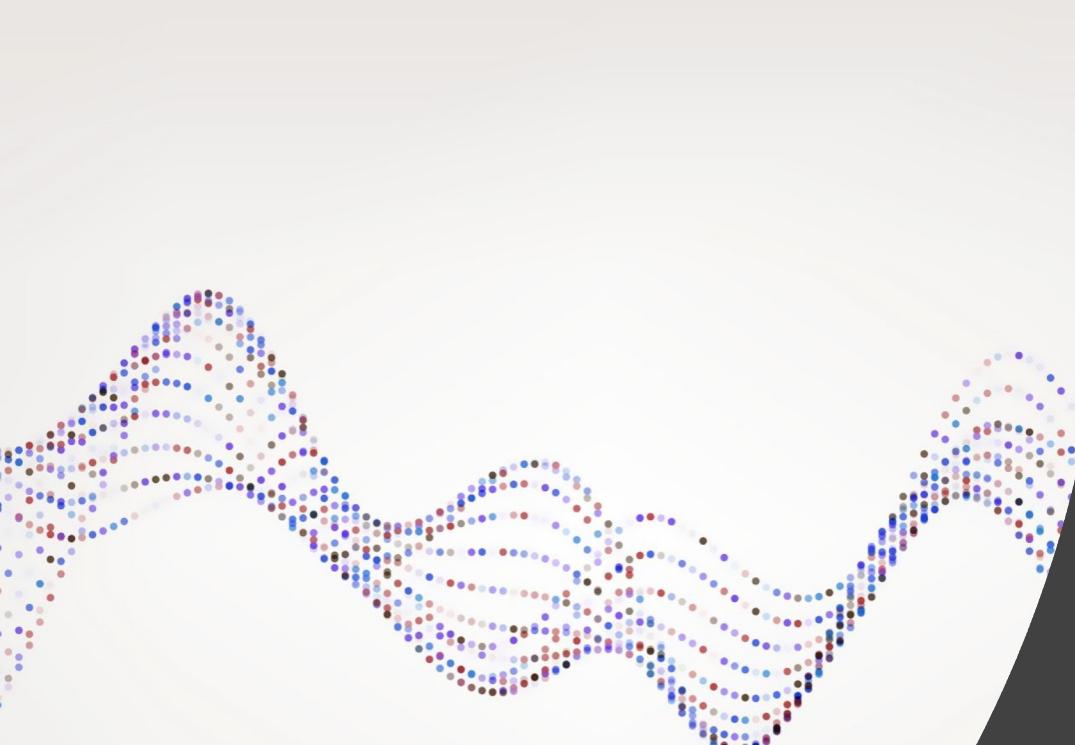
Superior open source data service continuously refined by AI, ML, and 65 world class researchers.

A decorative graphic in the top-left corner consists of a series of overlapping, wavy lines made of small, semi-transparent colored dots. The colors include shades of blue, purple, red, and brown. The lines curve from the top left towards the center of the slide.

# 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

search.maven.org/artifact/org.apache.struts:struts2-core/2.5.10/jar

sonatype | The Central Repository

org.apache.struts:struts2-core: 2.5.10

org.apache.struts:struts2-core

org.apache.struts:struts2-core 2.5.10

<?xml version="1.0" encoding="UTF-8"?>

/\*  
 \* \$Id\$  
 \*  
 \* Licensed to the Apache Software Foundation (ASF) under one  
 \* or more contributor license agreements. See the NOTICE file  
 \* distributed with this work for additional information  
 \* regarding copyright ownership. The ASF licenses this work  
 \* to you under the Apache License, Version 2.0 (the "License")  
 \*/

Component Info Security Remediation Licensing

**CVE-2017-5638** CVSS:10

Reference: [CVE-2017-5638](#) ⓘ

Severity: 10

Source: cve

Threat: critical

Category:

url: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638>

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

gradle.org

search.maven.org/artifact/org.apache.struts:struts2-core/2.5.10/jar

sonatype | The Central Repository

org.apache.struts:struts2-core: 2.5.10

org.apache.struts:struts2-core

org.apache.struts:struts2-core 2.5.10

Remediation advice Upgrade to the new version: 2.5.17

Popularity

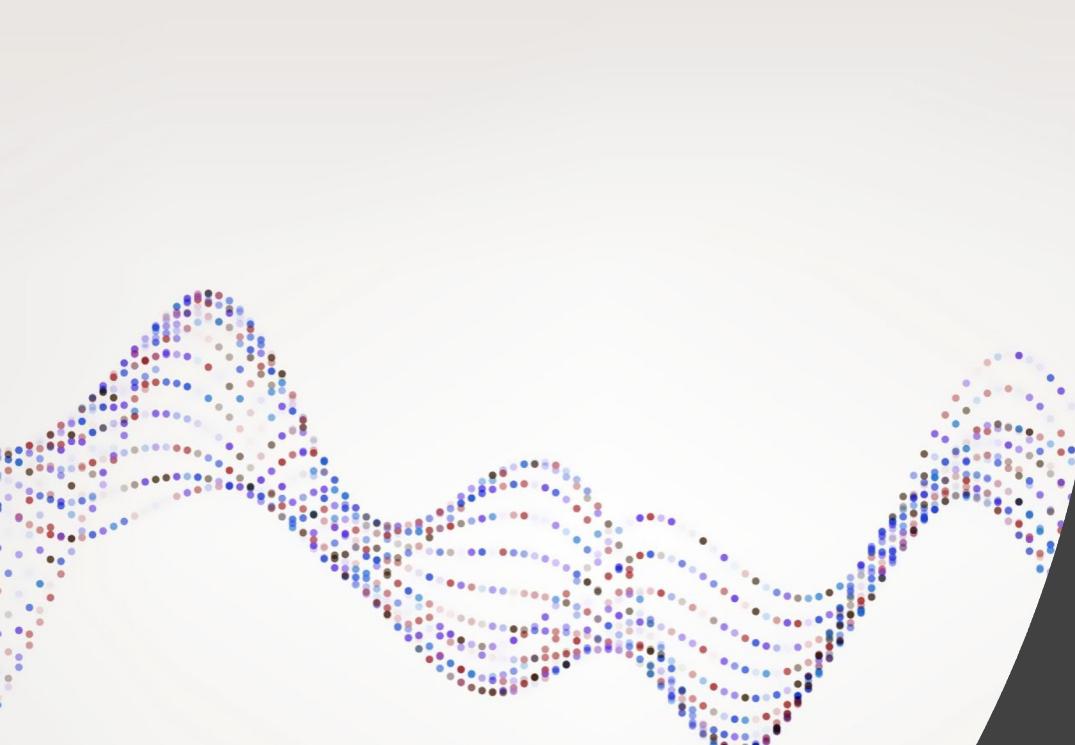
Older This Version Newer

Policy Threat Details Security License Quality Other

2.3.33

Component Info Security Remediation Licensing

View component intelligence within browser when searching public repositories.

A decorative graphic in the top-left corner consists of a series of overlapping, wavy lines made of small, semi-transparent colored dots. The colors include shades of blue, purple, red, and brown. The lines curve from the left side towards the center of the slide.

# 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

The screenshot illustrates the Nexus Lifecycle IDE Integration interface. It features a central workspace with several panels:

- Project Explorer:** Shows the project structure for "webgoat-smol".
- Policy Violations:** A table showing violations:

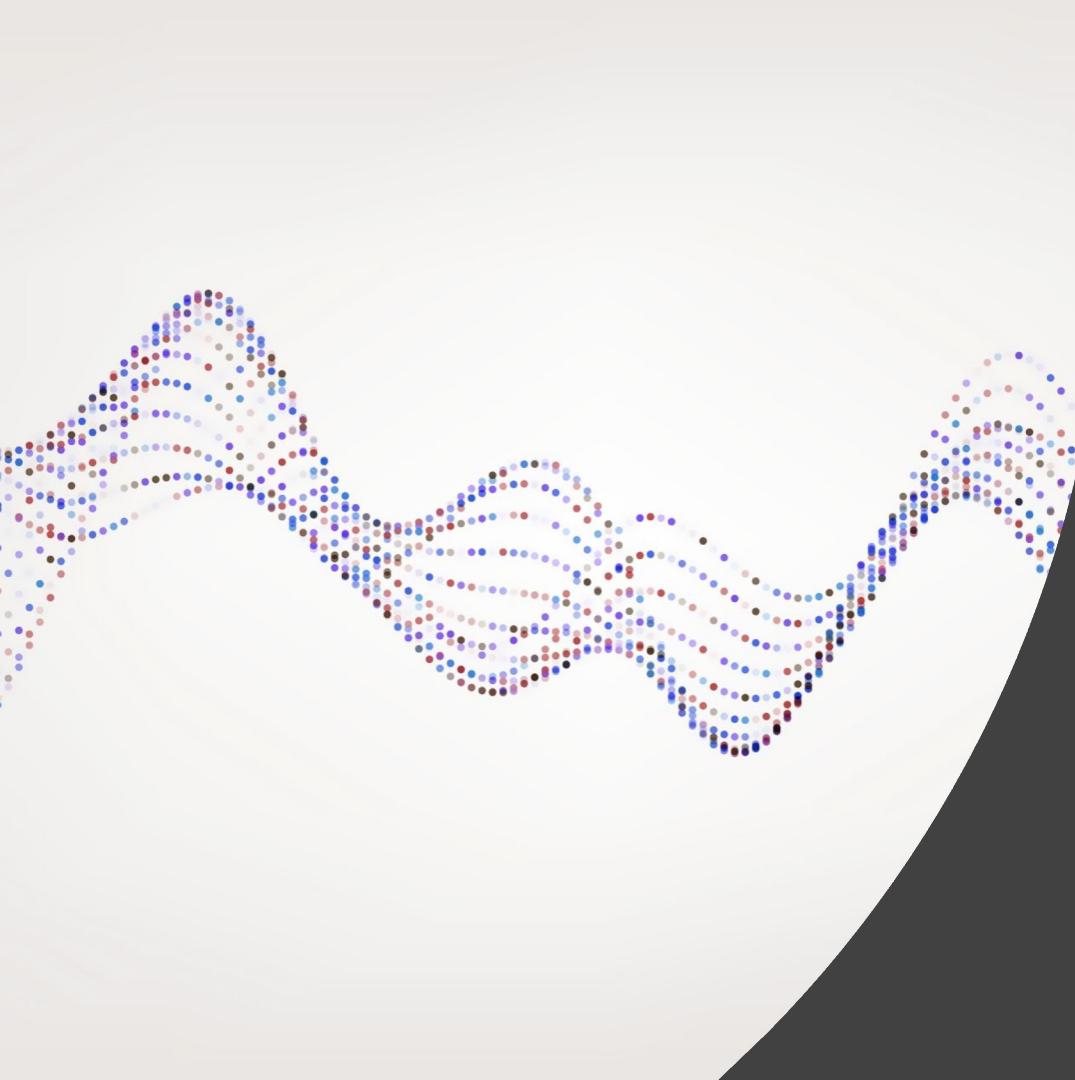
Policy	Constraint	Summary
Security-High	High risk CVSS score	Found security vulnerability sonatype-2015-0002 with severity 9.0.
		Found security vulnerability sonatype-2015-0002 with severity 9.0.
		Found security vulnerability sonatype-2015-0002 with status 'Open', not 'Not Applicable'.
Architecture-Quality	Version is old	Age was 10 years, 9 months and 7 days
- License Analysis:** A table showing threat levels and declared/observed licenses:

Threat Level	Declared License(s)	Observed License(s)
Liberal	Apache-2.0	Apache-2.0
- Security Issues:** A table showing threat levels and problem codes:

Threat Level	Problem Code	Status	Summary
9	SONATYPE-2015-0002	Open	Arbitrary remote code execution with InvokerTransformer. Exploit Details: <a href="https://support.sonatype.com/hc/en-us/articles/214155137-Commons-collections-unintended-execution-in-deserialization">https://support.sonatype.com/hc/en-us/articles/214155137-Commons-collections-unintended-execution-in-deserialization</a>
- Component Info:** A detailed view of the "commons-collections" component. It shows the following information:
  - 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 UtilitiesA "Popularity" chart shows the component's popularity over time, with "Older", "This Version", and "Newer" markers. Buttons for "View Details" and "Migrate" are also present.

Three purple callout boxes provide context for the interface:

- Identify which components violate policy from within the IDE.** Points to the "Policy Violations" table.
- Select best component version based on real-time intelligence.** Points to the "Popularity" chart and the "Migrate" button.
- Migrate to approved version with one click remediation.** Points to the "Migrate" button.



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

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 <code>CVE-2019-14540</code> with severity 7.5. Found security vulnerability <code>CVE-2019-16335</code> with severity 7.5. Found security vulnerability <code>CVE-2019-17267</code> with severity 7.5. Found security vulnerability <code>sonatype-2019-0371</code> with severity 8.5.

Source  
Application: My App  
Organization: My Organization  
Scan: 2b28f403fe99454684fb4a073efcea7 [view detailed report](#)  
Stage: build

This PR was automatically created by your friendly neighbourhood IQ server

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.

# nexus lifecycle - Policy Violations in SCM

The screenshot shows a GitHub pull request interface for a repository named "whyjustin / WebGoat". The pull request is titled "Example commit - Touch foo #2" and is marked as "Open". The user "whyjustin" has commented 16 minutes ago, stating "No description provided." Below the comment, there is a commit message "Example commit - Touch foo". A note below the commit says "Add more commits by pushing to the Example\_Pull\_Request branch on whyjustin/WebGoat." On the right side of the pull request, there is a summary of checks:

- 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.)

At the bottom, there is a "Merge pull request" button and a note about opening it in GitHub Desktop or viewing command line instructions.

On the right side of the screen, a detailed report from "louisrdev" is displayed, dated 5 days ago. The report title is "Nexus IQ found multiple policy violations". It lists several violations:

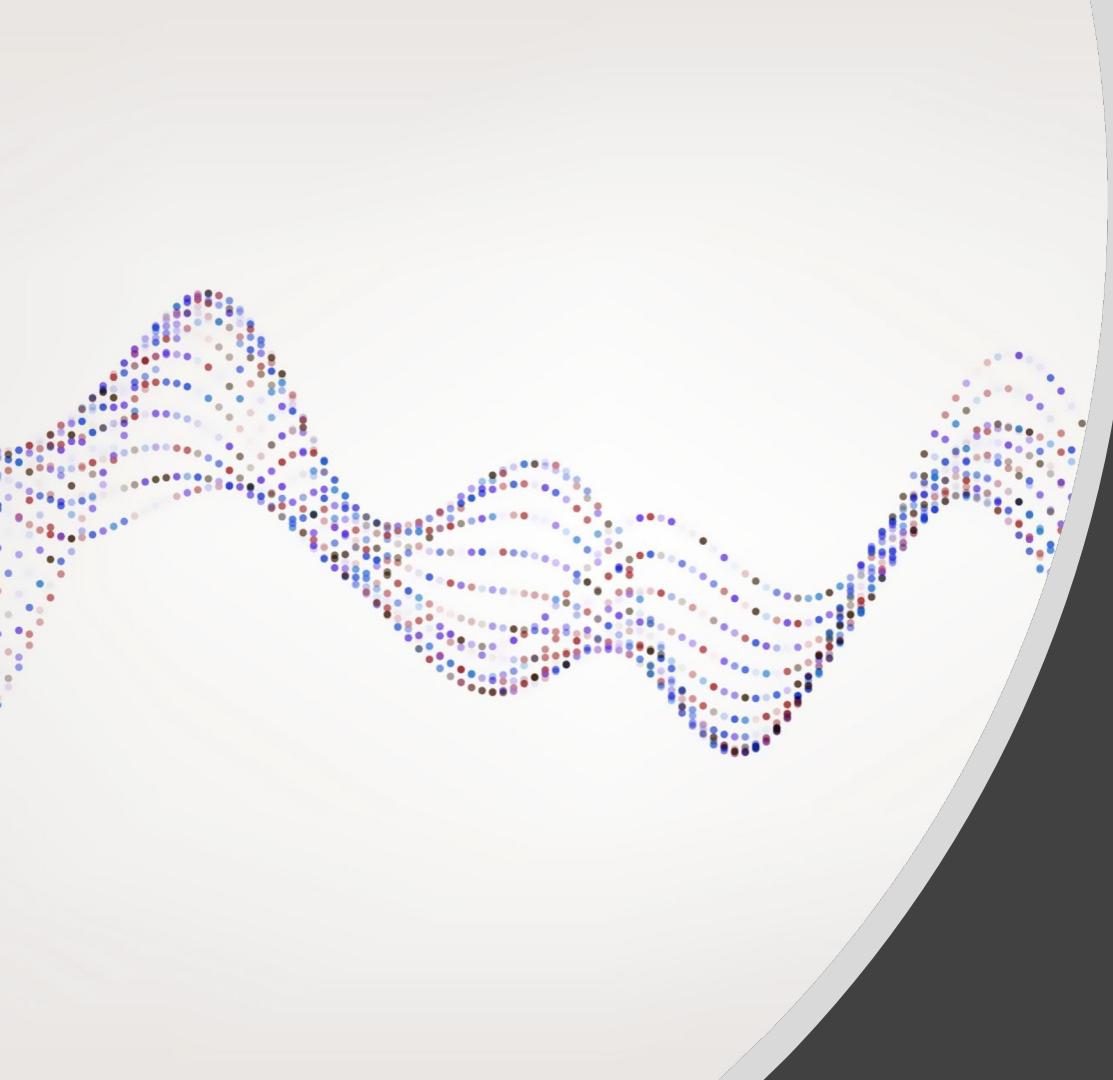
- org.apache.struts : struts2-core : 2.3.15 (9 of 10 Threat Level)
- org.apache.struts.xwork : xwork-core : 2.3.15 (9 of 10 Threat Level)
- commons-fileupload : commons-fileupload : 1.3 (9 of 10 Threat Level)
- ognl : ognl : 3.0.6 (7 of 10 Threat Level)

Below the violations, there is a section titled "Nexus IQ Report Detail" with the following information:

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

Links at the bottom of the report detail section include "See full feature branch report" and "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 screenshot shows the Sonatype Learn platform interface. At the top, there's a call-to-action button labeled "Choose Your Path Below". Below this, three learning paths are listed with corresponding images and descriptions:

- 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