The Customer Education team wants to give you a collection of the **Best Practices** and **TechTalk** guidance we presented in the course as a resource that you can pull up and use when you need it. Enjoy!

To make sure people have the right notifications in the right spots, automate and eliminate the manual process of adding each issue to your backlog. Jira Installation/Configuration and Notification Configuration.
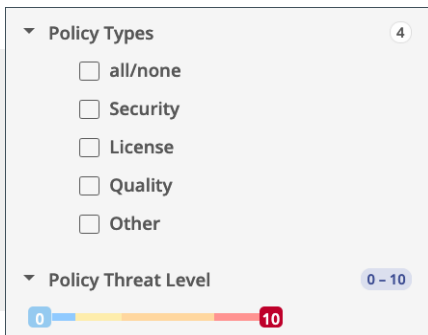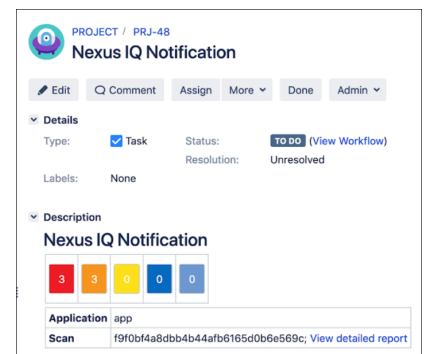
In order to see policy violations that are due to **Security Issues**, use the **Policy Type filter** in the sidebar to *filter only Security policies*.

From there, more details about what caused the violation can be observed by opening the CIP for a given violating component.

Most developers have the ability to **request a waiver**, but can not add/create one. To learn more about waivers, check out the IQ-101 Organization Policies eLearning course.

https://learn.sonatype.com/
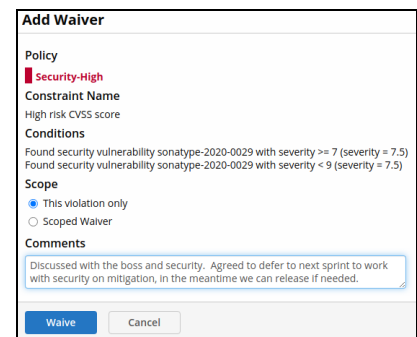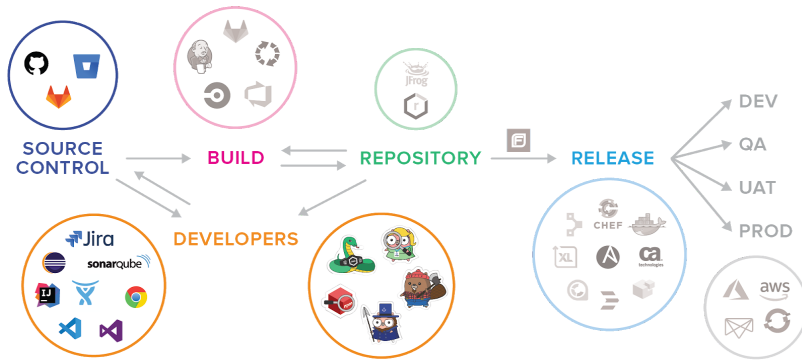
JIRA gives us better visibility of issues, early. But with the many variants you can have throughout the stages, how your organization **enforces policy** is key.

Use Continuous monitoring with your **existing policies** to watch for new violations. For example, you've deployed an application, and it had no policy violations at the time of release. Later, a vulnerability is discovered. Continuous monitoring applies the policy, finds the vulnerability and can report that to you via notifications.

References

- Resolving conflicts using the dependency tree
- IQ Server for Developers Technical Guide
- Out of the Wild: A Beginner's Guide to Package and Dependency Management
- Developer-Friendly Tools Throughout the SDLC
- IQ-102 Using Nexus IQ in Your IDE eLearning Course
- Fix an Open Source Vulnerability from within the IDE Youtube