sonatype | LEARN

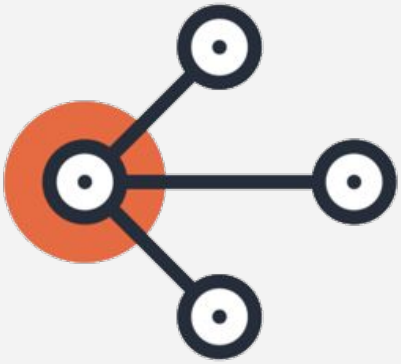
Visit us at learn.sonatype.com

Quick Reference Guide
Course: Component Remediation

IMPORTANCE OF REMEDIATION

Having a remediation plan in place helps you accomplish:

- **Improved communication**. You'll have a clear understanding of your organization's risk posture, remediation workflows, and responsible stakeholders.
- **Better software**. Improved component selection helps you build better, more secure software.
- **More efficiency.** Early identification allows you to continue to work, even when issues arise during development.
- **Reduction of busy work**. Nexus Lifecycle delivers expert security information that lets you make informed decisions early, rather than at the end of a dev cycle.



PRIMARY REMEDIATION WORKFLOWS

There are two primary workflows for remediating policy and security component issues:

Workflows for Policy Violations:

- Identifies components that have unacceptable risk as defined by the policy
- Identifies if a fix is required in a defined time period
- Occurs in mature or stable environments

Workflows for Security Violations:

- Occurs when a developer is investigating choices
- Provides instant feedback
- Displays other versions that are available
- Identifies which version is the most popular
- Delineates between security and licensing issues

GETTING STARTED WITH LIFECYCLE

- Deployment
- Remediation
- Understanding Vulnerability Data

ADDITIONAL RESOURCES

- Enhanced Policy Waivers
- Lifecycle - Grandfathering
- Waivers -vs- Grandfathering

sonatype | LEARN

Visit us at learn.sonatype.com

Quick Reference Guide
Course: Component Remediation

RESOLVING VIOLATIONS

You have several options when it comes to resolving violations:

Upgrade to a non-vulnerable version of the same component
Whether you've discovered a policy or security violation in Lifecycle, you can fix the issue. The first question you should ask yourself: "Is there a version upgrade available that is non-vulnerable?" If so, why not take it? This is the easiest path to reducing risk.

Migrate to a component that doesn't contain the violation
If you're not able to upgrade your component, the next step is to migrate to a similar component without violations. You might migrate because the upgrade path involves too much work for the development team. Follow your organization's standard operating procedures for replacement component processes.

Request a waiver or initiate grandfathering
When you cannot upgrade or migrate, you may want to start a risk management process, knowing that technical debt may incur. This means you are making the decision to accept the risk exposure and will deal with it at some point. This is accomplished through either waivering or grandfathering.

EXAMPLE REMEDIATION PROCESS