

SOLUTION SHEET

AMPLIFY SDLC CHANGE EVENTS AND XRAY SECURITY VULNERABILITIES

As your mission-critical tools for DevOps, key events that occur in Artifactory, Xray, and Pipelines, and Distribution reveal whether or not your software pipeline is on-track to deliver production-quality releases.

JFrog integrations for the PagerDuty incident response platform bring real-time visibility and awareness of what's happening in your JFrog-powered software pipelines to your entire team through one of the leading operations management tools. The PagerDuty incident management system provides reliable notifications, automatic escalations, on-call scheduling, and other functionality to help teams detect and fix infrastructure problems quickly.

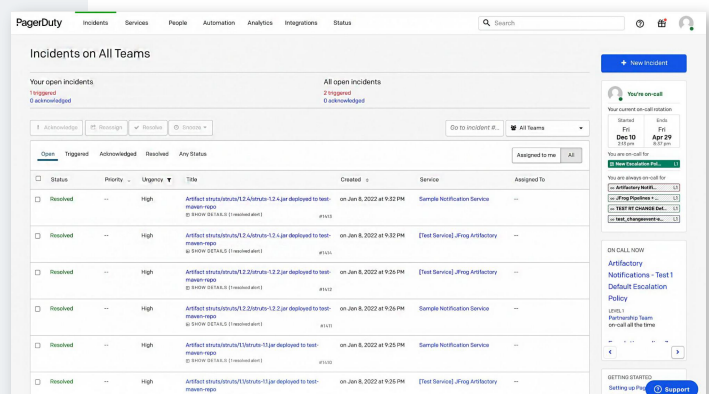
JFrog Artifactory is the universal artifact repository manager at the core of the JFrog Platform's binaries-driven formula for DevOps success. JFrog Xray is the universal software composition analysis (SCA) solution that enables DevSecOps teams to proactively identify open source vulnerabilities and license compliance violations before they manifest in production. JFrog Pipelines powers the Platform with traceable CI/CD automation.

With JFrog integrations for PagerDuty, incident teams can direct an early response by the right person to resolve DevOps and security events as they occur.

BENEFITS OF INTEGRATION

JFrog artifactory cold storage enables enterprises to:

- ✓ **Proactively manage security and compliance** across the software development and release lifecycle.
- ✓ **Reduce mean time to resolution (MTTR)** through early PagerDuty notifications on vulnerabilities and compliance violations.
- ✓ **Customize notifications and policies** based on type of violation and severity.
- ✓ **Granular visibility** on impacted artifacts, components and dependencies.
- ✓ **Monitor your software release pipeline in real-time.**



Available at:
pagerduty.com/integrations/

INTEGRATION FEATURES

In the JFrog Platform, DevOps administrators can configure Artifactory events and granular Xray watch policies to trigger outbound event webhooks, and associate each with a PagerDuty service. Once received, PagerDuty can direct each incident report to an individual or group to alert them of events in Artifactory, and of security or license violations detected by Xray.



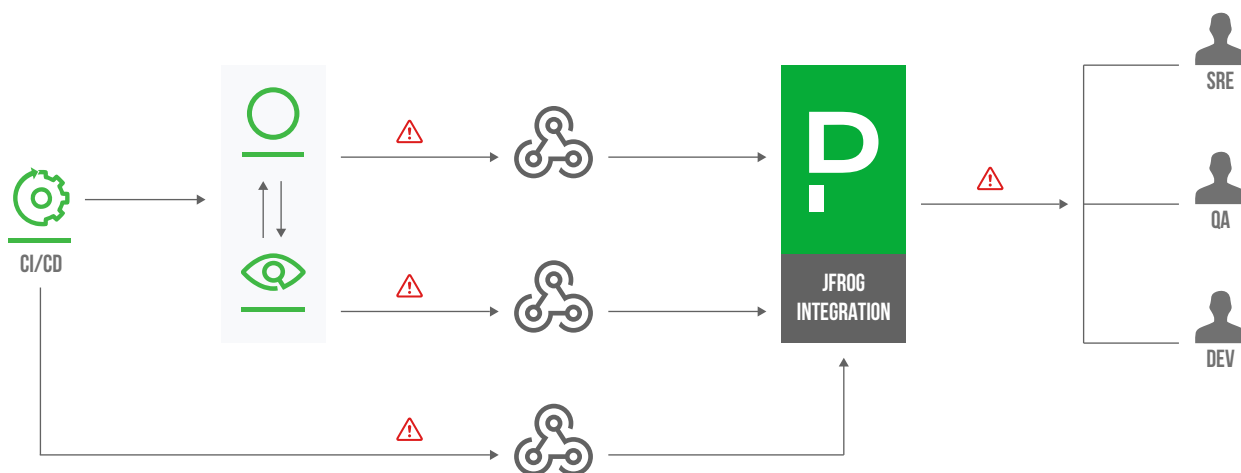
Artifactory can trigger incidents on a PagerDuty service to report change events for artifacts, builds, and release bundles. For example: an artifact uploaded, a Docker tag pushed, or a release bundle distributed.



Xray can trigger PagerDuty to direct incident reports to individuals or groups to alert them of security or license policy violations detected in scanned repositories, builds, and release bundles.



Pipelines can deliver real-time CI/CD event information to a PagerDuty service. Respond quickly to build failures and receive actionable, granular information about a particular pipeline step.



USE CASES

- **SRE/IT Admin Oversight** - Incident reports sent through PagerDuty enable rapid response to all relevant DevOps events and security issues.
- **Quality Assurance** - QA teams can configure Xray policies and watches to monitor targeted artifact repositories used for test and staging environments, and report security violations through PagerDuty incident services for prompt resolution.
- **Shift Left Security** - Incident reports sent through PagerDuty alert developers and dev managers of any relevant security vulnerabilities and enable resolution at the earliest point in the development lifecycle.

Start For Free: jfrog.com/start-free/



www.jfrog.com



www.facebook.com/artifrog/



www.twitter.com/jfrog



www.linkedin.com/company/jfrog-ltd

