RAPID7

komand by RAPID7

USE CASE IN ACTION

Vulnerability Management

Using Komand to Automate Your Third-Party Vulnerability Management Processes

Many companies are still struggling with managing vulnerabilities, especially in conjunction with vendor and third-party software. The vendor **notification <-> triage <-> patch cycle** often requires careful coordination to ensure that critical bugs get reviewed and patches applied quickly, while balancing the risk of downtime and other issues that can arise due to unstable patches or system incompatibilities.

Before Komand

Monitoring and coordinating vendor vulnerability response was a manual process that a security operations team member had to coordinate, which involved:

1. Monitoring a variety of vendor security advisory email list(s) and web pages
2. Looking up the owner in the organization (in operations, development, security, or otherwise) responsible for managing the vendor software patches when a new advisory comes in
3. Notifying the product owner with details of the advisory
4. Monitoring the status over a 24-hour period for owner to indicate the appropriate response was in motion; and if not, escalating it to an appropriate person on the security team.

This part of the process alone—not including the actual testing and application of the software updates—could require **15-30 minutes of time per day** for a team member to perform. And often during busy times, critical vulnerabilities could fall through the cracks.

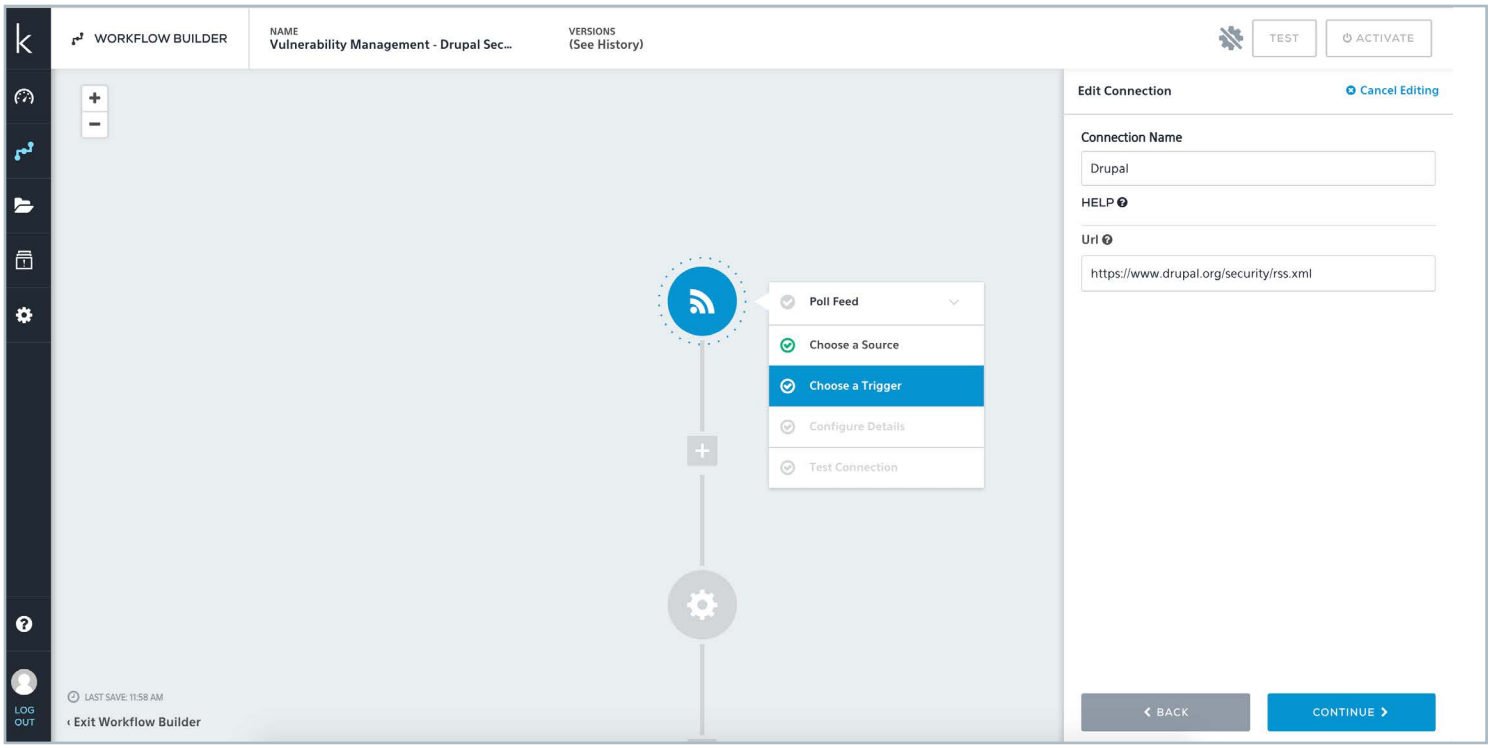
With Komand

Using this security automation solution, a simple workflow can be built and customized to your organization's needs, and all within minutes! As an example, we'll use our **RSS Feed plugin** to automatically monitor a security advisory list, assign the work using a ticketing system, and build a secondary SLA workflow to perform escalation as needed.

Part 1

Reacting to New Security Advisories Using the RSS Feed Trigger

Using Komand's **RSS Plugin**, we connect our **Poll Feed Trigger** to the Drupal security team's RSS feed. This will notify Komand whenever a new security advisory is published:



Above: configuring our trigger to poll the Drupal security feed

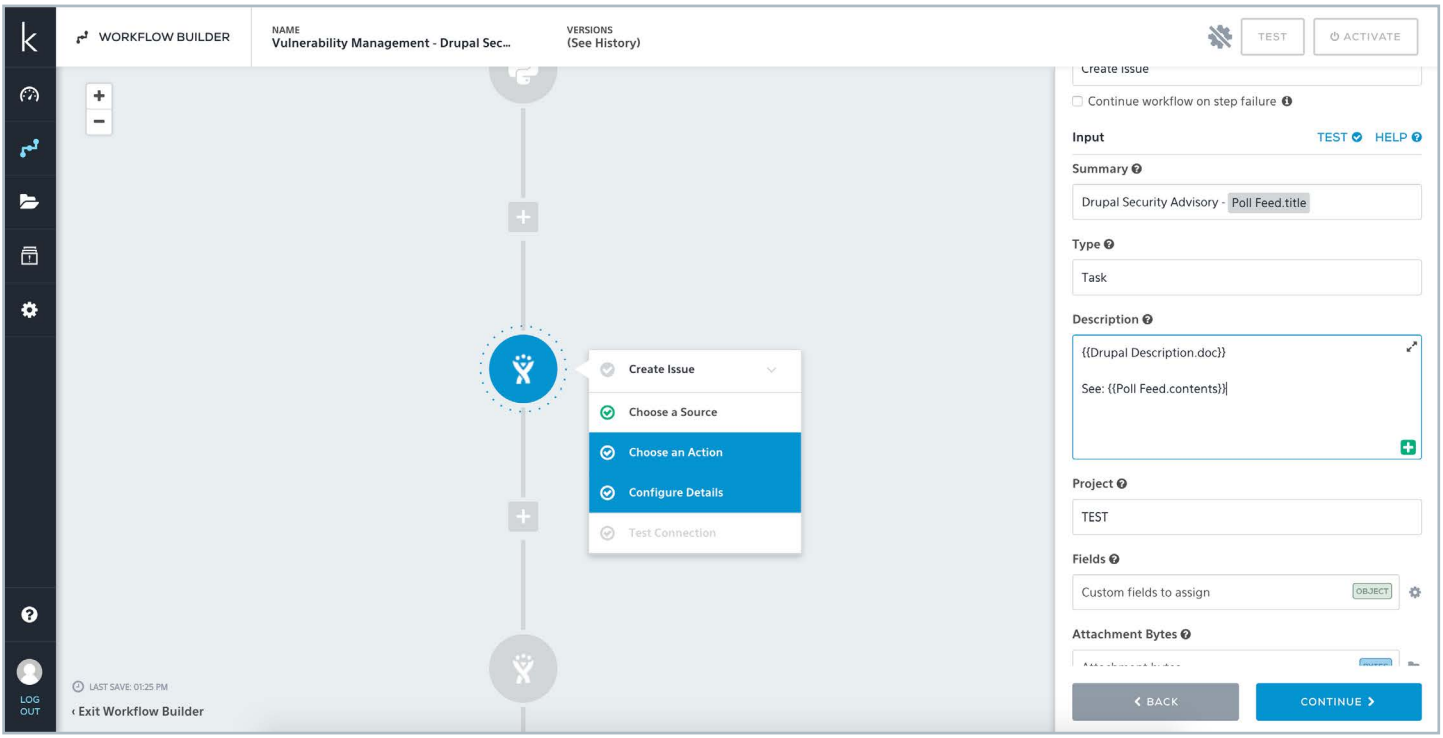
Afterward, we can use the 'Markdown' plugin to turn the HTML from the RSS feed that contained the details of the CVE, the patch, versions affected, and other important security advisory details into a nicely formatted message that can be used for notification.

Part 2

Creating a Ticket in JIRA

Using our **JIRA Plugin**, we'll perform the following actions:

1. Create Issue
2. Assign Issue
3. Label Issue

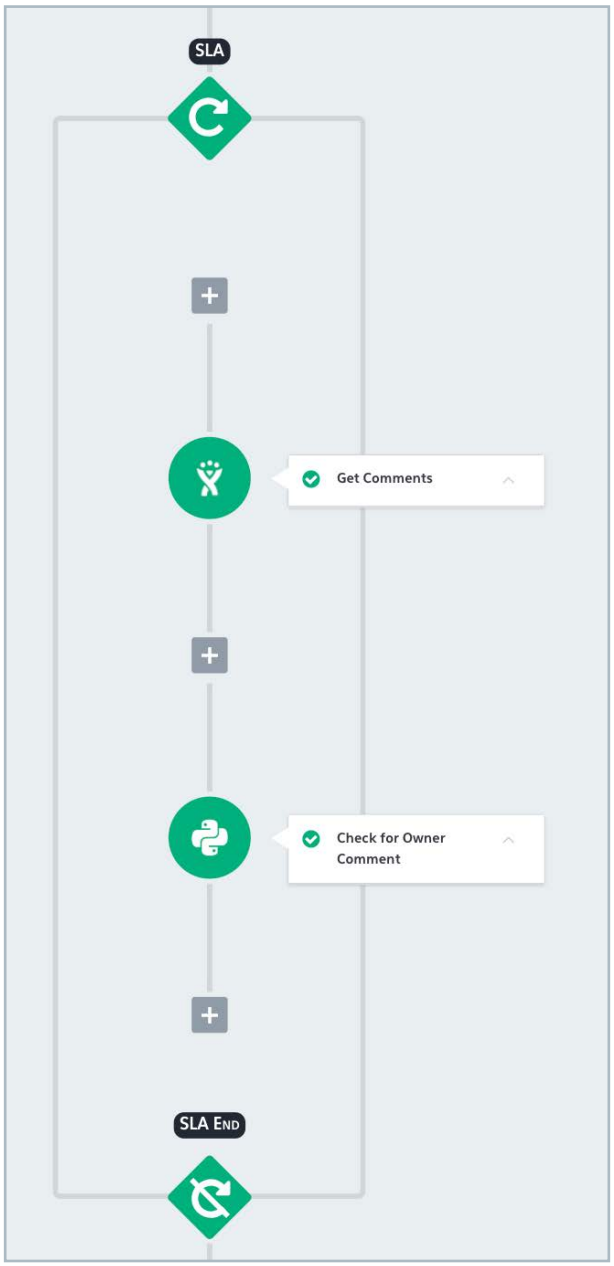


Above: creating a JIRA ticket in Komand

Part 3

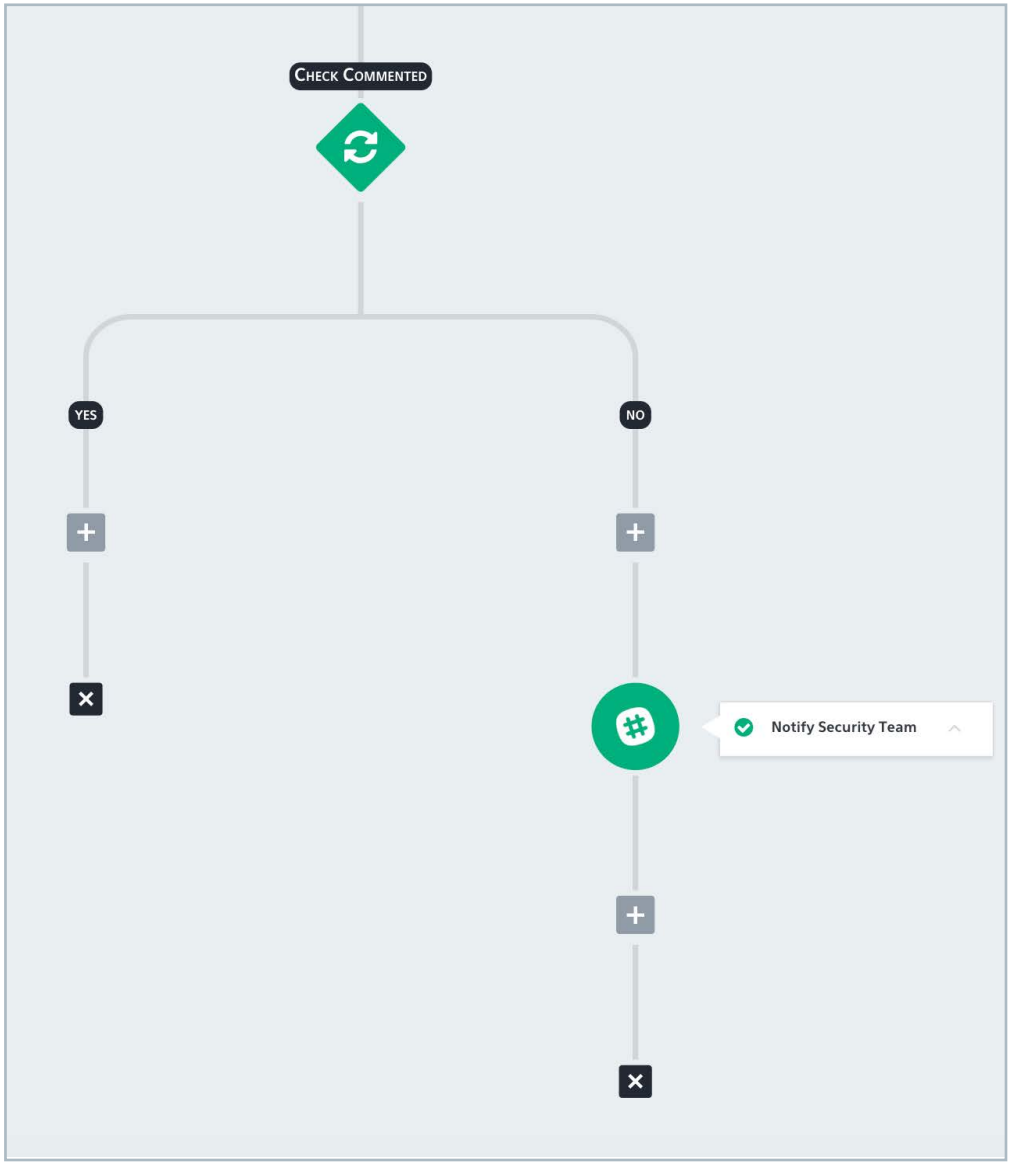
Building Our SLA Monitor

Now, let's build a simple loop that's going to monitor this ticket for acknowledgment by the owner we have assigned. Using Komand's **Loop** step, we can build a loop that will run for no longer than a day, looking for owner comments on the ticket using the JIRA **Get Comments** action:



Above: building our SLA notification loop in Komand

After the loop has exited, we'll set up a check. If our ticket owner never acknowledged it, we'll perform an escalation to the security team via our **Slack™ Plugin:**



Above: escalate to the security team if the assignee did not comment

Wrapping It Up

By instrumenting existing tools with Komand's simple workflow automation layer, you can take process execution time from hours to minutes, accelerating your team's productivity and reliability.

To realize the power of Komand's automation in your environment, contact sales@komand.com

About Komand

Komand is a security orchestration and automation solution that enables your team to accelerate and streamline time-intensive processes—no code necessary. With 200+ plugins to connect your tools and easily customizable connect-and-go workflows, you'll free up your team to tackle other challenges, while still leveraging their expertise when it's most critical.

Learn more at www.rapid7.com/komand