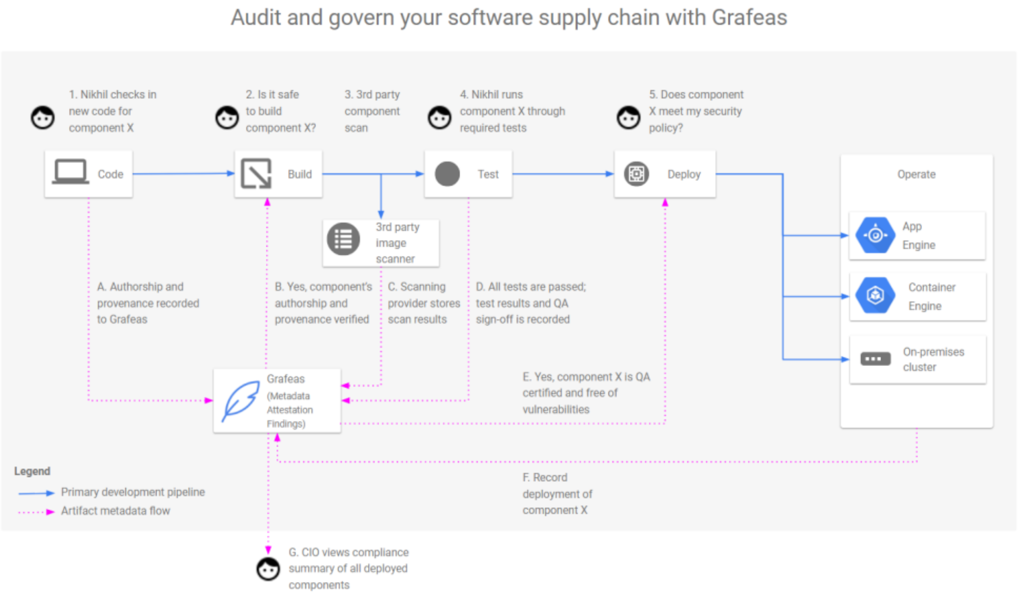
Unknown date | Frederic Lardinois

Google, IBM and others launch an open-source API for keeping tabs on software supply chains

Thanks to containers and microservices, the way we are building software is quickly changing. But as with all change, these new models also introduce new problems. You probably still want to know who actually built a given container and what's running in it. To get a handle on this, Google, JFrog, Red Hat, IBM, Black Duck, Twistlock, Aqua Security and CoreOS today announced Grafeas ("scribe" in Greek), a new joint open-source project that provides users with a standardized way for auditing and governing their software supply chain.

In addition, Google also launched another new project, Kritis ("judge" in Greek, because after the success of Kubernetes, it would surely be bad luck to pick names in any other language for new Google open-source projects). Kritis allows businesses to enforce certain container properties at deploy time for Kubernetes clusters.

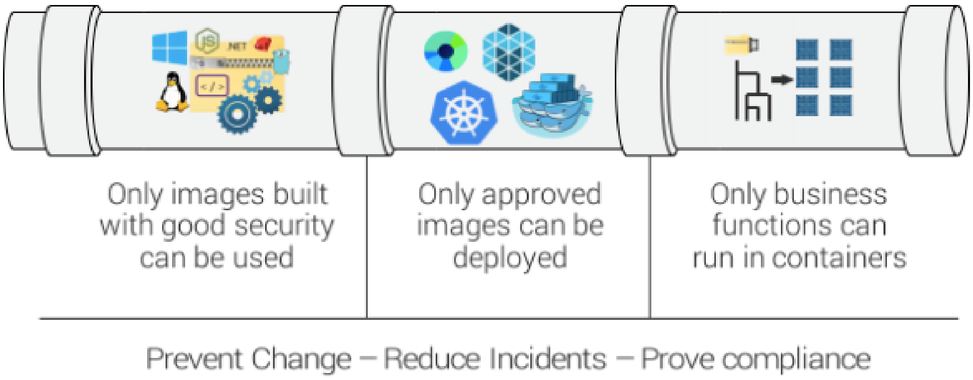

Audit and govern your software supply chain with Grafeas
1. Nikhil checks in new code for component X
2. Is it safe to build component X?
3. 3rd party component scan
4. Nikhil runs component X through required tests
5. Does component X meet my security policy?
Code
Build
Test
Deploy
Operate
3rd party image scanner
App Engine
Container Engine
On-premises cluster
A. Authorship and provenance recorded to Grafeas
B. Yes, component's authorship and provenance verified
C. Scanning provider stores scan results
D. All tests are passed; test results and QA sign-off is recorded
Grafeas (Metadata Attestation Findings)
E. Yes, component X is QA certified and free of vulnerabilities
F. Record deployment of component X
G. CIO views compliance summary of all deployed components
Legend
Primary development pipeline
Artifact metadata flow

Grafeas basically defines an API that collects all of the metadata around code deployments and build pipelines. This means keeping a record of authorship and code provenance, recording the deployment of each piece of code, marking whether code passed a security scan, which components it uses (and whether those have known vulnerabilities) and whether Q&A signed off on it. So before a new piece of code is deployed, the system can check all of the info about it through the Grafeas API and if it's certified and free of vulnerabilities (at least to the best knowledge of the system), then it can get pushed into production.

At first glance, this all may seem rather bland, but there's a real need for projects like this. With the advent of continuous integration, decentralization, microservices, an increasing number of toolsets and every other buzzworthy technology, enterprises are struggling to keep tabs on what's actually happening in their data centers. It's pretty hard to stick to your security and governance policies if you don't exactly know what software you're actually running. Currently, all of the different tools that developers use can record their own data, of course, but Grafeas represents an agreed-upon way for collecting and accessing this data across tools.

Like so many of Google's open-source projects, Grafeas basically mimics how Google itself handles these issues. Thanks to its massive scale and early adoption of containers and microservices, Google, after all, saw many of these problems long before they became an issue for the industry at large. As Google notes in today's announcement, the basic tenants of Grafeas reflect the best practices that Google itself developed for its build systems.

All of the various partners involved here are bringing different pieces to the table, but JFrog, for example, will implement this system in its Xray API. Red Hat will use it to enhance its security and automation features in OpenShift (its container platform) and CoreOS will integrate it into its Tectonic Kubernetes platform.


Only images built with good security can be used
Only approved images can be deployed
Only business functions can run in containers
Prevent Change – Reduce Incidents – Prove compliance

One of the early testers of Grafeas is Shopify, which currently builds about 6,000 containers per day and which keeps 330,000 images in its primary container registry. With Grafeas, it can now know whether a given container is currently being used in production, for example, when it was downloaded from the registry, what packages are running in it and whether any of the components in the container include any known security vulnerabilities.

"Using Grafeas as the central source of truth for container metadata has allowed the security team to answer these questions and flesh out appropriate auditing and lifecycling strategies for the software we deliver to users at Shopify," the company writes in today's announcement.

Viewed using Just Read