KubeCon | CloudNativeCon

North America 2017

Grafeas Community Meet-Up

Wendy Dembowski, Staff Software Engineer, Google
Stephen Elliott, Product Manager, Google

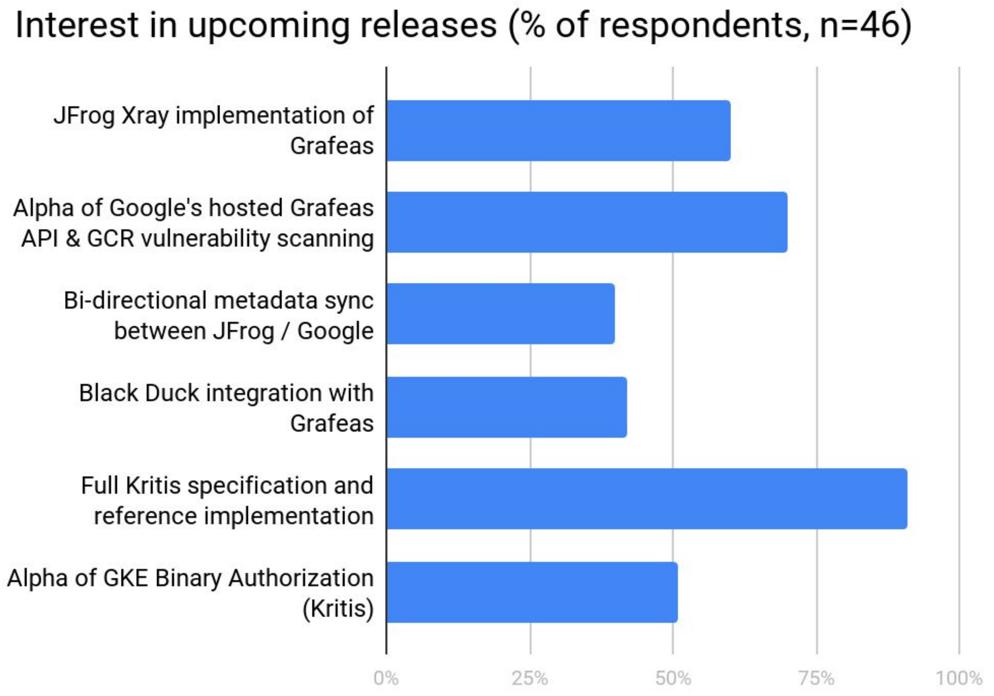
Agenda!

1. Meet and Greet
2. Discuss Topics of Community Interest

Topics

Topics of interest

- License metadata and SPDX
- Open source reference implementation
- Providers, projects and the role of a third party tool
- Reputation + dynamic vulnerability scoring
- Other partner integration with Grafeas (e.g., Aqua, Twistlock, Clair)
- “TPM use” in remote attestation
- Supporting compliance/regulatory use cases (e.g., financial institutions)



Appendices

Technical overview

- **tl;dr** Grafeas is a structured metadata API for annotating cloud components

- **Notes**
  - Created by metadata provider (in provider’s project)
  - Contains context-insensitive metadata relevant to linked occurrences

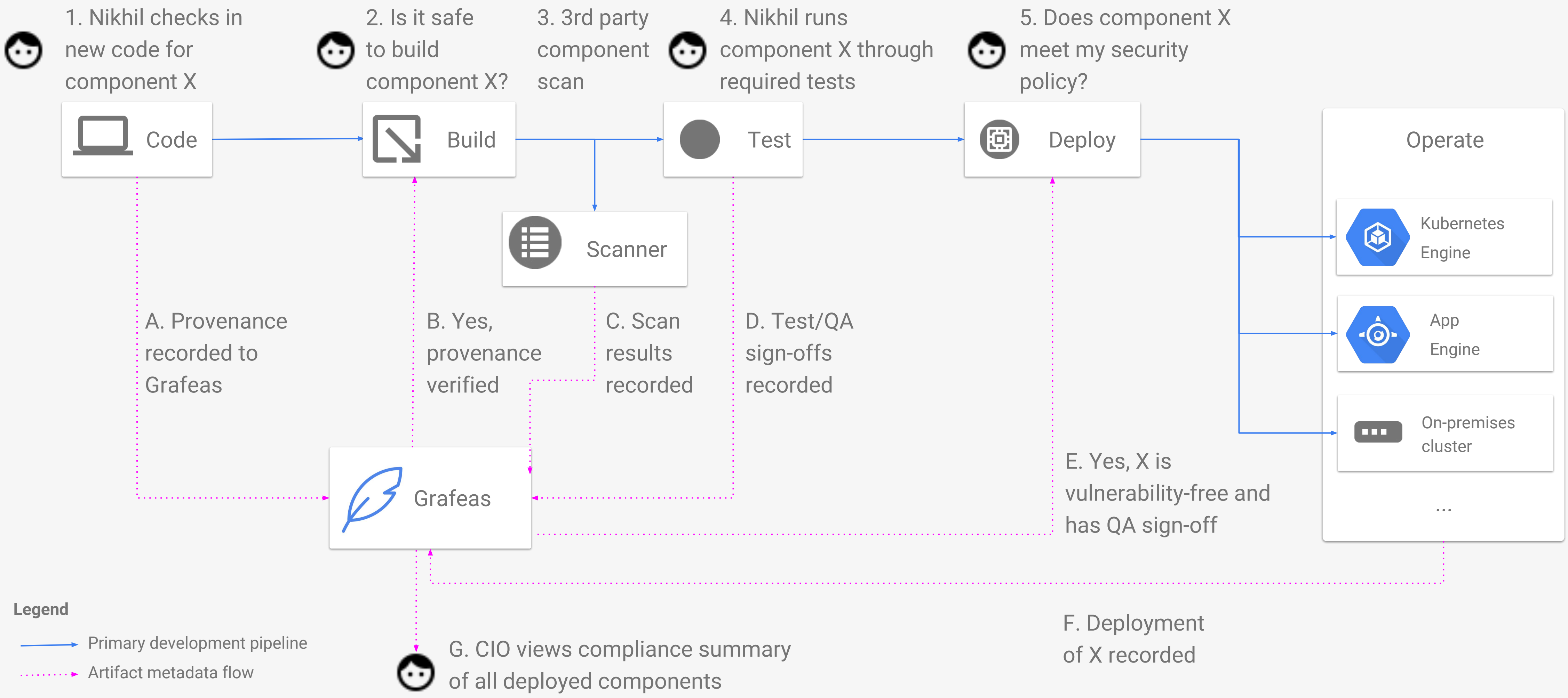
- **Occurrences**
  - Created by metadata provider (in customer’s project)
  - Links to a provider’s note
  - Binds a note to an occurrence in a customer’s resource (e.g., image)

Currently supported artifacts & metadata

Component Type	Identifier (soon to be replaced by https://github.com/package-url)
Debian	deb://dist(optional):arch:name:version
Docker	https://Namespace/name@sha256:
Generic file	file://sha256::name
Maven	gav://group:artifact:version
NPM	npm://package:version
NuGet	nuget://module:version
Python	pip://package:version
RPM	rpm://dist(optional):arch:name:version

Metadata Kind	Note Summary	Occurrence Summary
Package Vulnerability	CVE description and details including severity, versions	Affected packages/versions in a specific resource
Build Details	Builder version and signature	Details of this specific build incl. inputs/outputs
Image Basis	Base Image for a container	An image that uses the base image, and layers on top of base image
Package Manager	Package Descriptions	Filesystem locations where package is installed in a specific resource
Deployment History	A resource that can be deployed	Details of each deployment of the resource
Attestation	Anchor for attestations for this authority	An attestation on a specific component

Example of future Grafeas story


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
Scanner
Kubernetes Engine
App Engine
On-premises cluster
...
A. Provenance recorded to Grafeas
B. Yes, provenance verified
C. Scan results recorded
D. Test/QA sign-offs recorded
E. Yes, X is vulnerability-free and has QA sign-off
Grafeas
F. Deployment of X recorded
G. CIO views compliance summary of all deployed components
Legend
Primary development pipeline
Artifact metadata flow

Resources

Lists:

- User discussion: grafeas-users@googlegroups.com
- Dev discussion: grafeas-dev@googlegroups.com

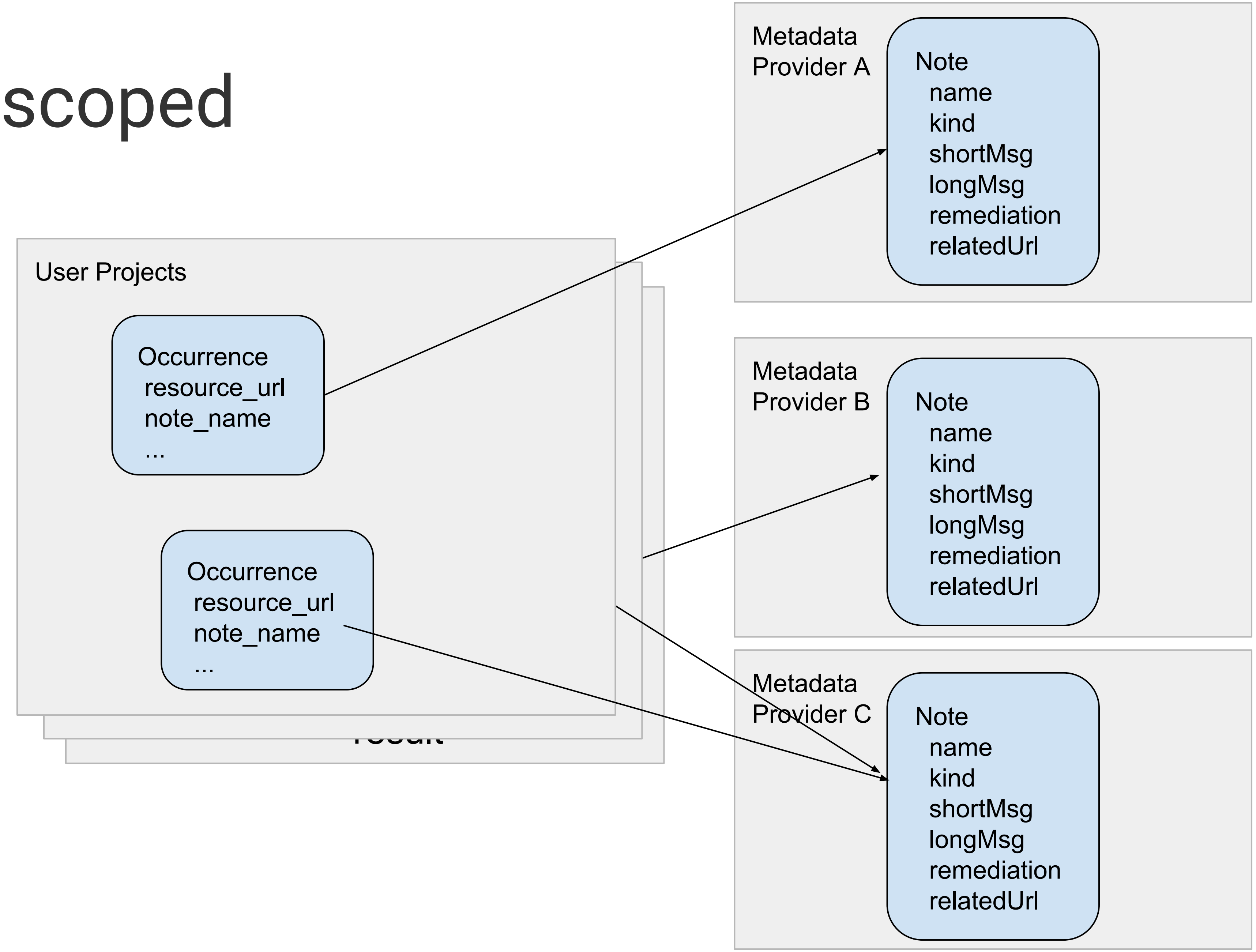
Blogs:

- Launch announcement, incl. links to collaborator blogs (https://goo.gl/cXFZBJ)
- Kubernetes blog (https://goo.gl/T8zwpU)
- Anchore blog, "Digging into Grafeas"
- Codefresh blog, "Write this down, Grafeas!"

Demos:

- https://github.com/kelseyhightower/grafeas-tutorial
- https://github.com/jeffmendoza/container-analysis-demo

Project-scoped



User Projects

Occurrence
resource_url
note_name
...

Occurrence
resource_url
note_name
...

Metadata
Provider A

Note
name
kind
shortMsg
longMsg
remediation
relatedUrl

Metadata
Provider B

Note
name
kind
shortMsg
longMsg
remediation
relatedUrl

Metadata
Provider C

Note
name
kind
shortMsg
longMsg
remediation
relatedUrl

Example note

```
{
  "name": "projects/security-scanner/notes/CVE-2017-14159",
  "shortDescription": "CVE-2017-14159",
  "longDescription": "NIST vectors: AV:L/AC:M/Au:N/C:N/I:N",
  "relatedUrl": [
    {
      "url":
"https://security-tracker.debian.org/tracker/CVE-2017-14159",
      "label": "More Info"
    },
    {
      "url":
"http://people.ubuntu.com/~ubuntu-security/cve/CVE-2017-14159"
,
      "label": "More Info"
    }
  ],
  "kind": "PACKAGE_VULNERABILITY",
  "createTime": "2017-09-05T21:44:52.071982Z",
  "updateTime": "2017-09-29T16:16:01.140652Z",
  "vulnerabilityType": {
    "cvssScore": 1.9,
    "severity": "LOW",
"details": [
      {
        "cpeUri": "cpe:/o:debian:debian_linux:7",
        "severityName": "LOW",
        "fixedLocation": {
          "cpeUri": "cpe:/o:debian:debian_linux:7",
          "package": "openldap",
          "version": {
            "kind": "MAXIMUM"
          }
        },
        "minAffectedVersion": {
          "kind": "MINIMUM"
        },
        "package": "openldap",
        "description": "slapd in OpenLDAP 2.4.45 and earlier
creates a PID file after dropping privileges to a non-root
account, which might allow local users to kill arbitrary
processes by leveraging access to this non-root account for PID
file modification before a root script executes a \"kill `cat
/pathname`\" command, as demonstrated by openldap-initscript."
      },
     ....
```

Example occurrence

```
{
  "name":
"projects/scanning-customer/occurrences/randomId1234",
  "resourceUrl":
"https://gcr.io/scanning-customer/dockerimage@sha256:hash",
  "noteName":
"projects/security-scanner/notes/CVE-2017-14159",
  "kind": "PACKAGE_VULNERABILITY",
  "createTime": "2017-09-29T02:58:23.376798Z",
  "updateTime": "2017-09-29T07:35:22.141762Z",
  "vulnerabilityDetails": {
    "severity": "LOW",
    "cvssScore": 1.9,
    "packageIssue": [
      {
        "affectedLocation": {
          "cpeUri": "cpe:/o:debian:debian_linux:8",
          "package": "openldap",
          "version": {
            "name": "2.4.40+dfsg",
            "revision": "1+deb8u2"
          }
        },
        "fixedLocation": {
          "cpeUri": "cpe:/o:debian:debian_linux:8",
          "package": "openldap",
          "version": {
            "kind": "MAXIMUM"
          }
        },
        "severityName": "LOW"
      }
    ]
  }
}
```