KubeCon | CloudNativeCon

North America 2017

BoF: Grafeas

Using Artifact Metadata to Track and Govern Your Software Supply Chain

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

Why are these questions so hard?

“Is container image X deployed right now?”

“Did all deployed components pass required QA tests?”

“Does vulnerability Y affect production?”

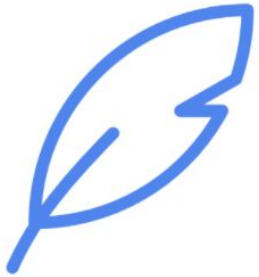
Trends and needs of today's SDLC

- Computing trends
  - Growing, fragmented toolsets
  - Open-source software adoption
  - Decentralization
  - Continuous delivery
  - Microservice architectures
- Metadata needs
  - Central source of truth
  - Universal coverage
  - Hybrid cloud-friendly
  - Flexible
  - Pluggable

SDLC: software development lifecycle

What is Grafeas?

- **Good governance requires good data**
- **Grafeas** is an open source initiative to define a uniform way to talk about artifact metadata in the modern software supply chain
- Specifically, it's an **open API spec for storing metadata** about **many different artifact types** (containers, VMs, software packages) **and metadata kinds** (vulnerabilities, build info, signatures)



Goals

Provide a common language to store, retrieve, and query metadata on software artifacts

Support metadata schemas for the most common metadata use cases

Promote broad adoption so users benefit from metadata composability and portability

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

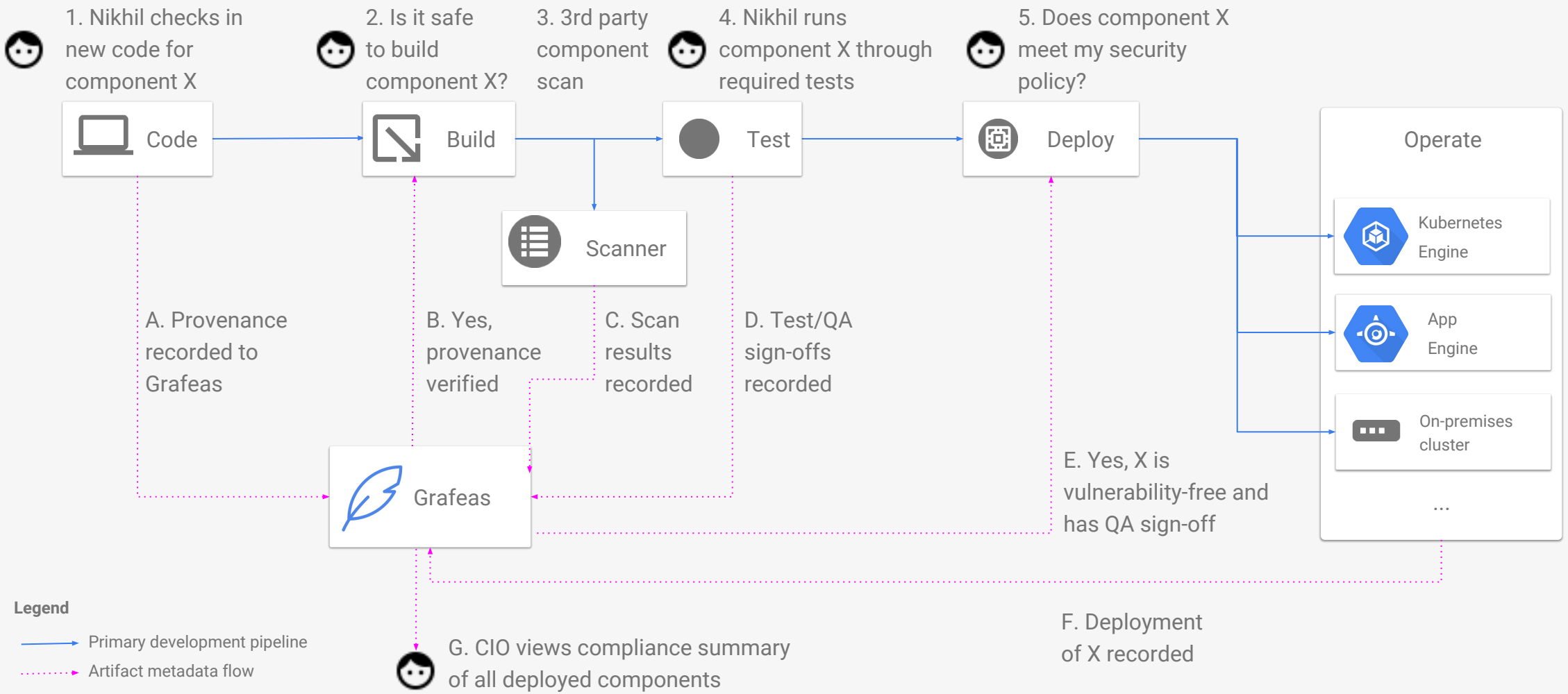
- **Occurrences**
  - Created by metadata provider (in customer's project)
  - Links to a provider's note
  - Binds a note to an occurrence in a customer's resource (e.g., image)

Currently supported artifacts & metadata

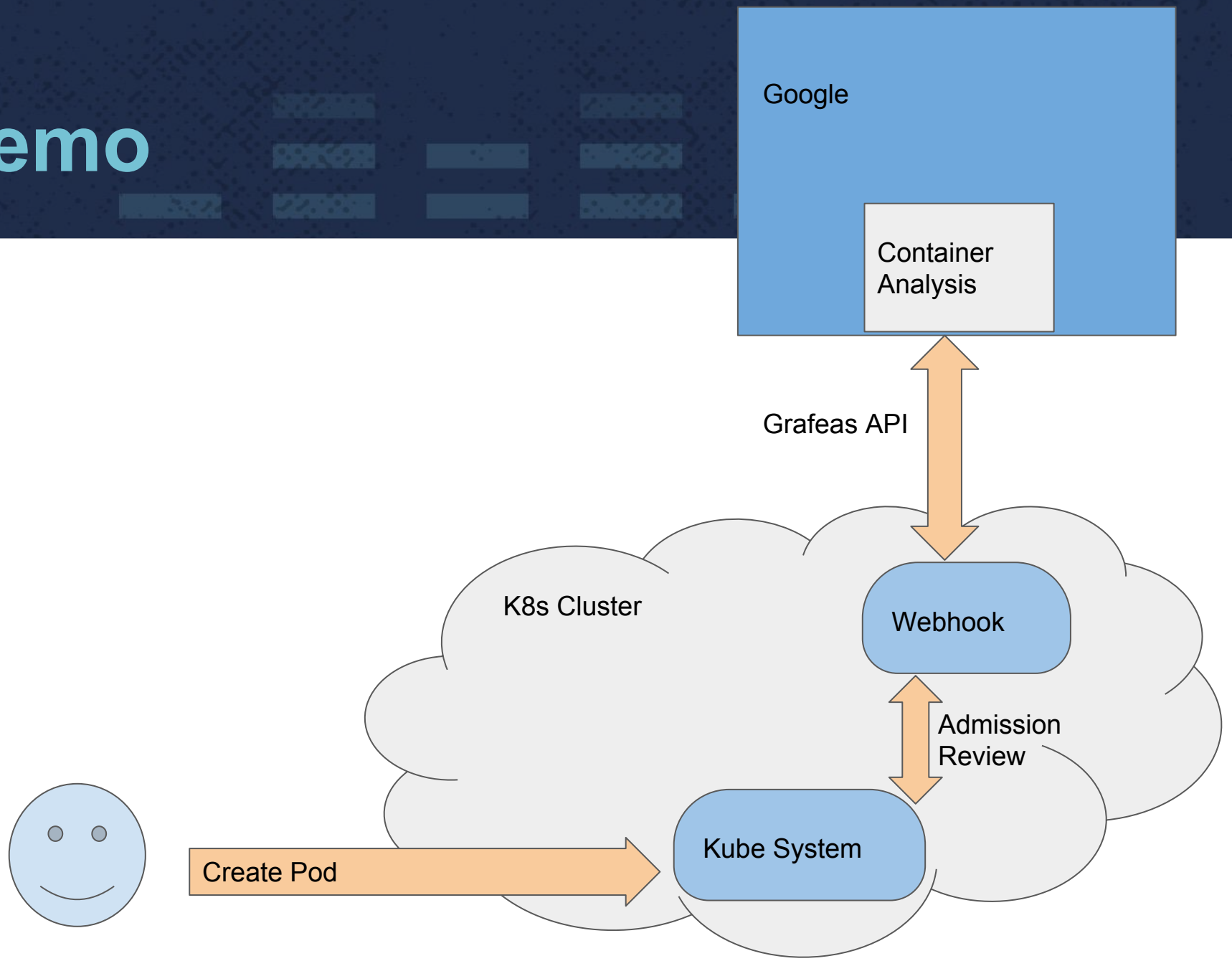
Component Type	Identifier (soon to be replaced by https://github.com/package-url)
Debian	deb://dist(optional):arch:name:version
Docker	https://Namespace/name@sha256:
Generic file	file://sha256::name
Maven	gav://group:artifact:version
NPM	npm://package:version
NuGet	nuget://module:version
Python	pip://package:version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



Demo


Google
Container Analysis
Grafeas API
K8s Cluster
Webhook
Admission Review
Kube System
Create Pod

Next Steps

- **Try the demo for yourself**
  - https://github.com/kelseyhightower/grafeas-tutorial
  - https://github.com/jeffmendoza/container-analysis-demo
- **Visit our Github site and get involved**
  - github.com/grafeas
  - grafeas.io
- **Trial the Google-hosted alpha**
  - cloud.google.com/container-registry/docs/vulnerability-scanning

Req’ts of highly regulated industries

Graeme Hay

Managing Director, Enterprise Infrastructure

Morgan Stanley

Graeme.Hay@morganstanley.com

Resources

Events:

- KubeCon Fri morning (12/8): Grafeas meet-up at KubeCon.
  Submit topics for discussion at https://goo.gl/forms/0lIa2UGV1pfUDh843.
- Tue 12/12: Google/Black Duck webinar on Grafeas (https://goo.gl/Gmv5NT)

Lists:

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

Blogs:

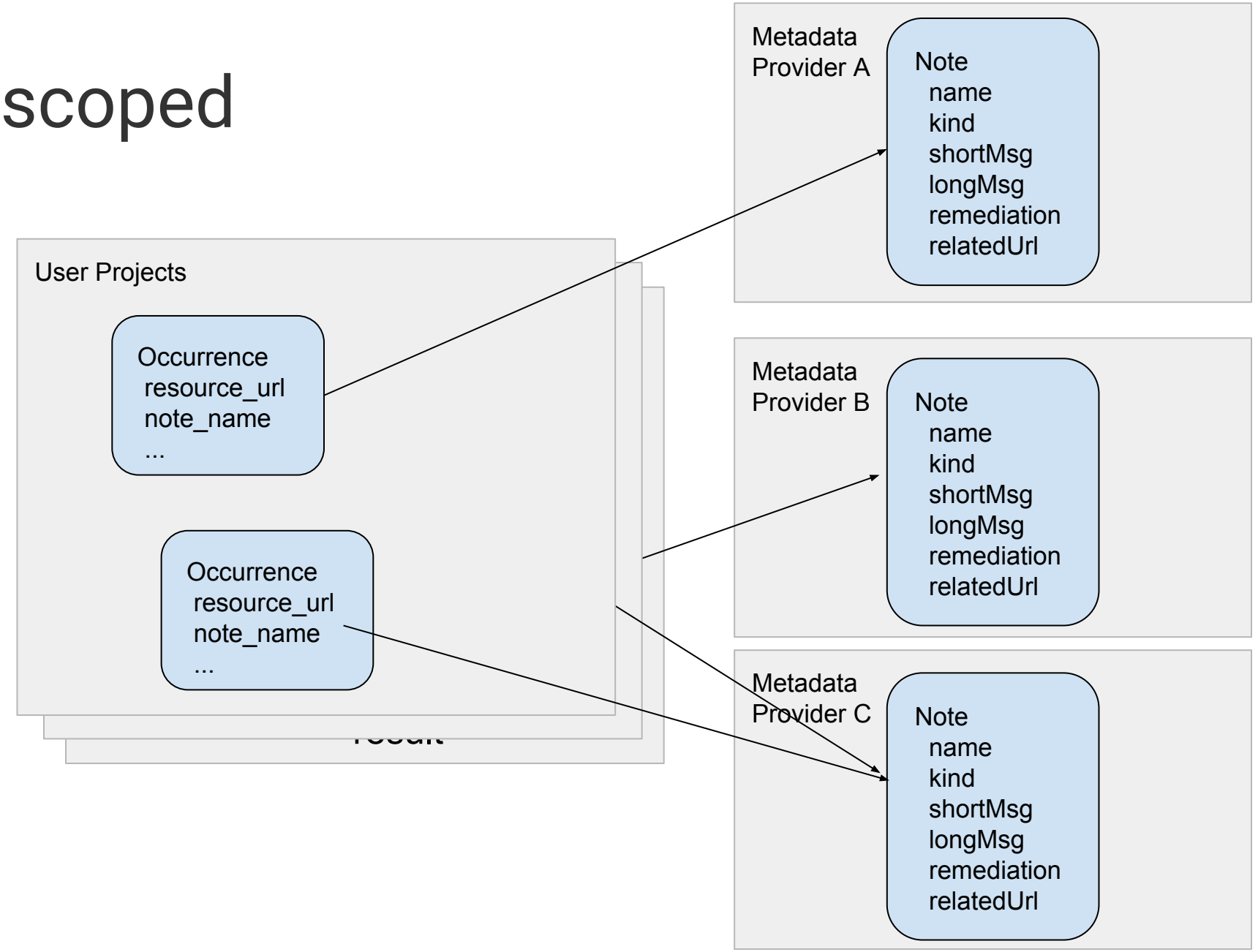
- Launch announcement, incl. links to collaborator blogs (https://goo.gl/cXFZBJ)
- Kubernetes blog (https://goo.gl/T8zwpU)

Discussion

Questions or topics you’d like to discuss?

Appendices

Project-scoped



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"
      }
    ]
  }
}
```