Sysdig Technology Preview - CI/CD and IaC

Mateo Burillo - Sysdig Secure Product Manager

sysdig

(New) Vulnerability Management

New Image Analysis

sysdig SECURE

- Insights
- Scanning
- Posture
- Policies
- Network
- Events
- Investigate
- Integrations
- Get Started
- Mateo Burillo
  Secure Team (Ca...
- Chat with Us

Scan Results PREVIEW > mongo-express 0.54.0

Base OS: alpine 3.11.12

Scanned on February 15, 2022 2:11 PM

Overview | Vulnerabilities | Content | Policies | Detail

Fixable Packages by Severity

View all

Package and version	Suggested Fix	Vulnerabilities					
mongodb-query-parser 1.4.3	2.0.0	2	-	-	-	-	
busybox 1.31.1-r10	1.31.1-r11	-	9	1	-	-	
ssl_client 1.31.1-r10	1.31.1-r11	-	9	1	-	-	
bson 1.0.9	1.1.4	-	-	1	-	-	
minimist 0.0.10	0.2.1	-	-	1	-	-	1 Exploit

Vulnerabilities

View all

26

Detected

- 4 Critical
  2 Fixable
- 18 High
  18 Fixable
- 4 Medium
  4 Fixable
- 0 Low
  0 Fixable
- 0 Negligible
  0 Fixable

Policy Evaluations

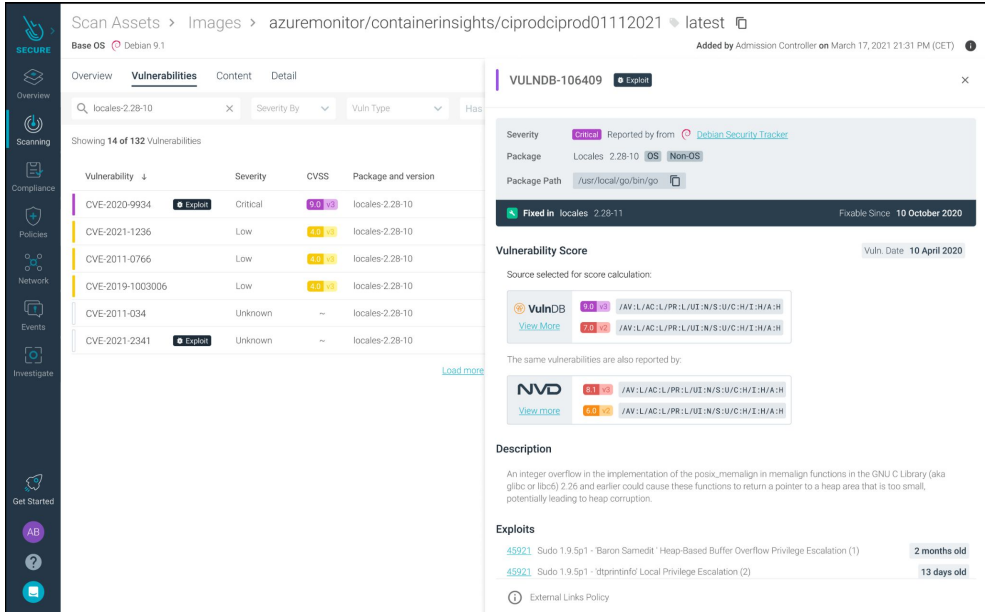
View all

Policy Evaluation	Rule failings
Sysdig Best Practices	Vulnerabilities 65

sysdig

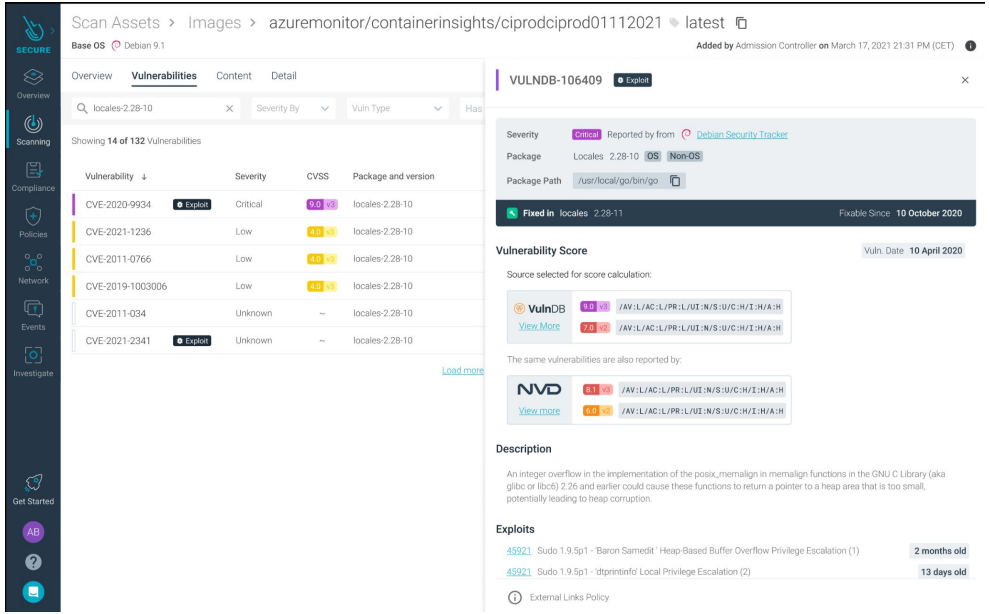
Highlights!

- **Way** faster: 8x on average, over a large dataset bench
- **Binary scanner**, trivial to embed
  - Self contained golang binary
- **Additional vulnerability data**
  - CVSS v3 and v2, break down displaying the risk factors
  - Public exploit available and PoC code
  - Fix date, Vuln added date, Exploit Date
  - Multiple feeds reporting on this particular vulnerability



The Road to risk and remediation

- Now we are faster, provide more comprehensive information and are improving the accuracy
- That is all required, but it's not the most ambitious goal for the new engine
- The real mid term goals are:
  - Noise filtering FP/FN
  - Risk evaluation and prioritization
  - Remediation flows



New Scanning Engine - CI Policies

- Policies are no longer tied to image names
- Additional criteria, including exploitability metrics
- More rule options coming soon:
  - Effective user
  - Environment variables
  - etc

Vulneratilities: Severities and Threats

With Severity greater than or equal Critical AND

Fixable since anytime AND

Disclosure date older than or equal 60 days ago

Exploitability Metrics

Public Exploit available and age older than 60 days

No administrative privileges required

No User interaction required

Network attack vector

OR

Vulnerabilities: Deny List

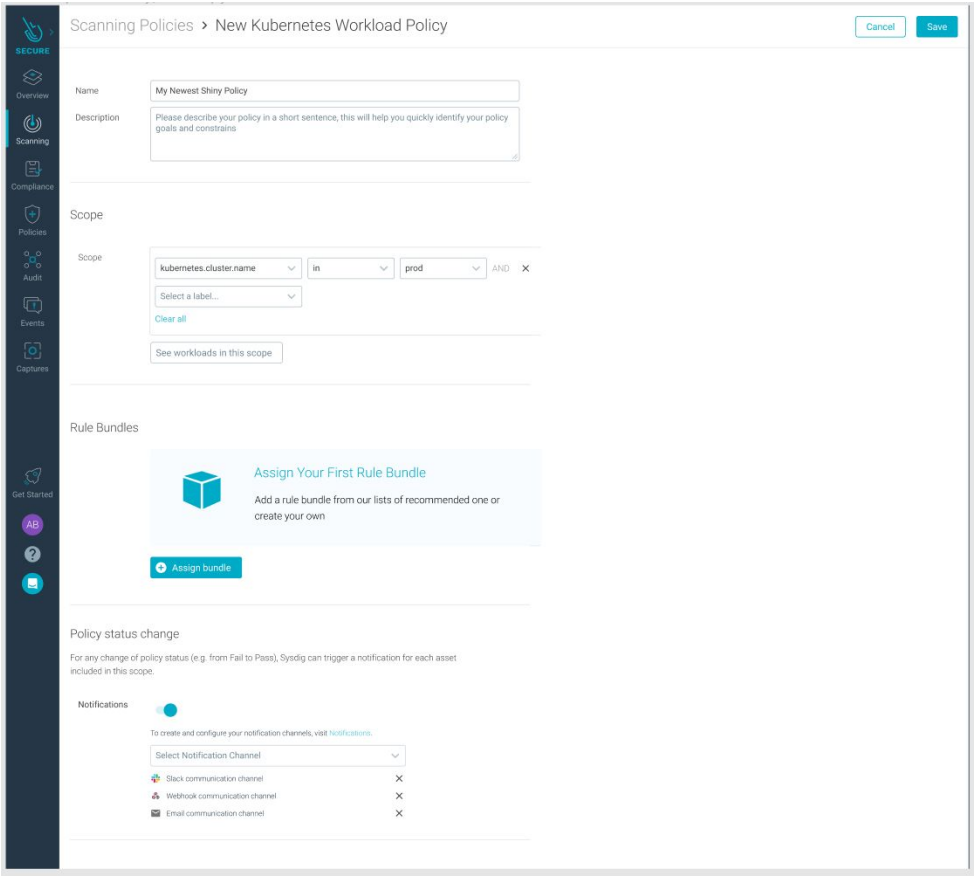
Every CVE should be validated only by its format

CVE-123831-2021 × CVE-128744-2010 ×

sysdig

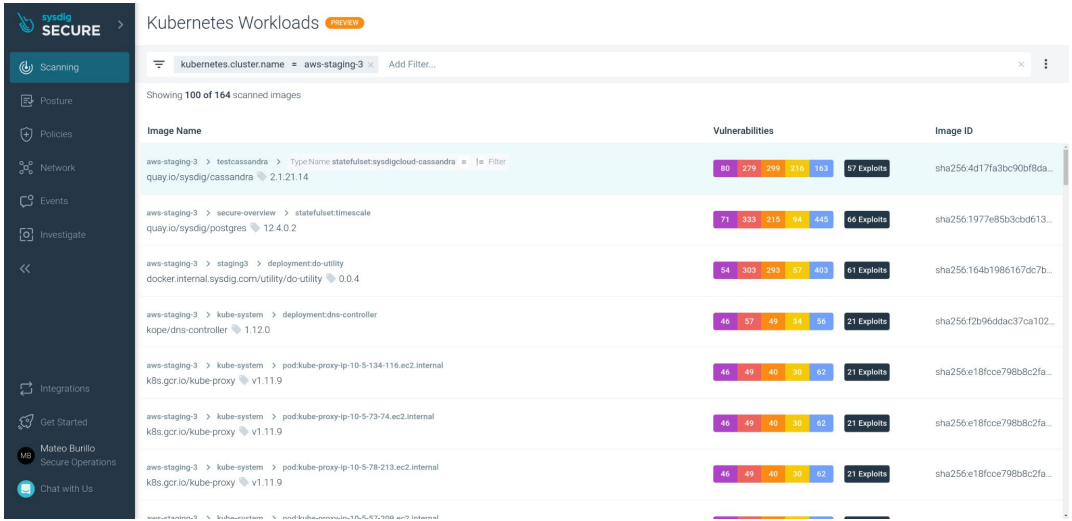
Runtime Policies

- Policies are tied to runtime metadata, not to image name
- Different environment do have different security standards
  - SOC2 environment
  - QA environment
  - DMZ
  - etc…



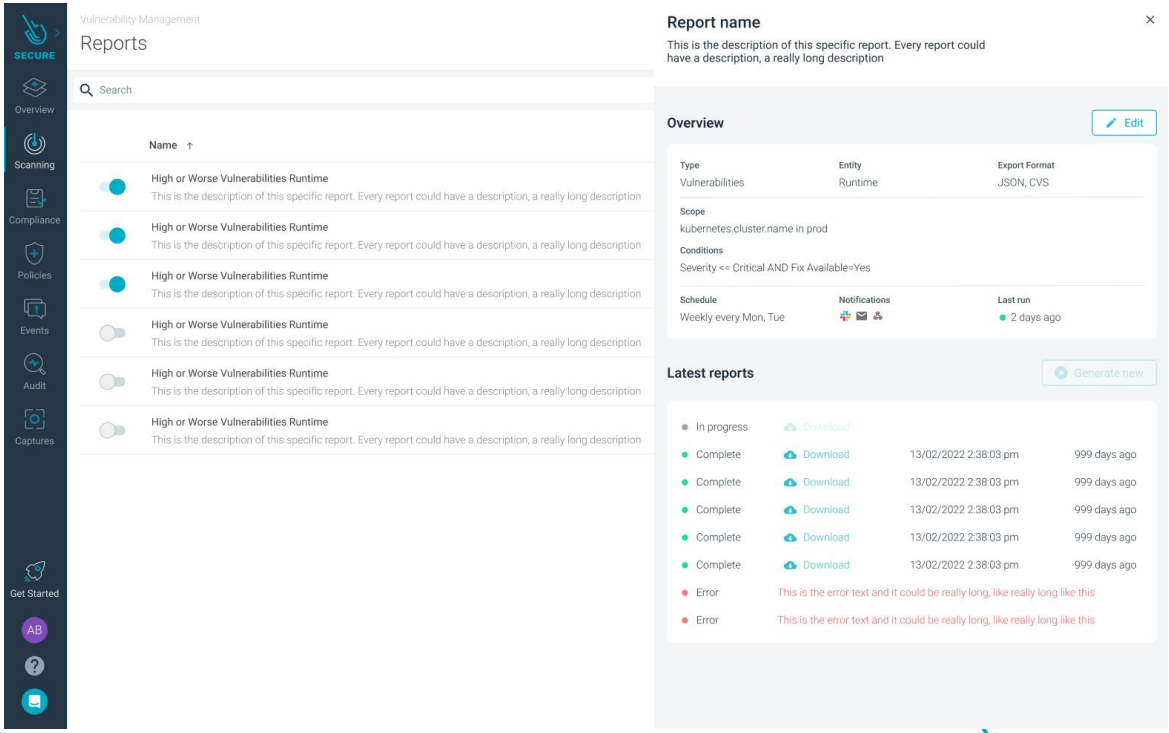
Best in class runtime metadata

- Sysdig has the **best available runtime information** to enrich your scanning data
- One of the most important factors to assess **Risk** is the runtime impact
- Runtime workloads are **automatically** reevaluated and matched against newly discovered vulnerabilities
- Flexible scope to segment vulnerability exposure looking at Kubernetes, host-centric or cloud-centric metadata



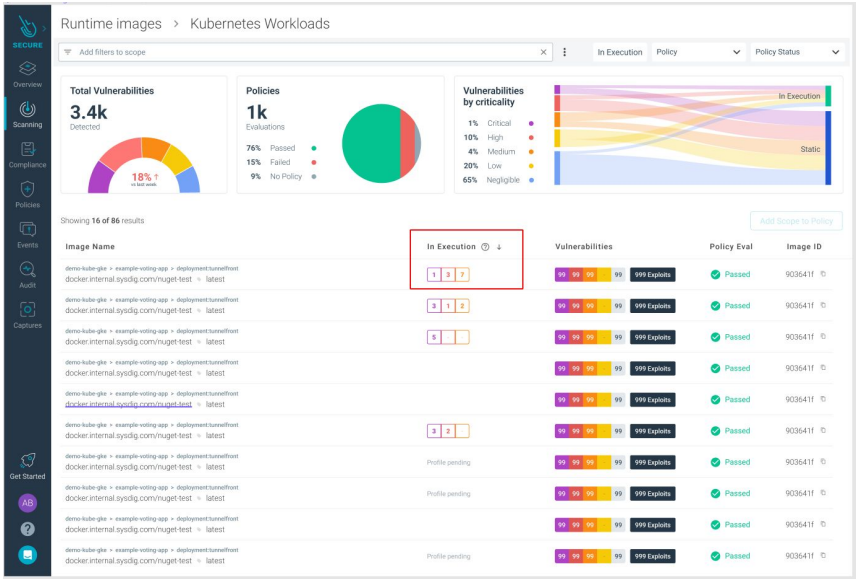
New Scanning Engine - Reporting

- Reporting redesign
- Net new:
  - Direct data download **API**, optimized to integrate with third party software
  - **Run Now**, immediate execution of new schedule
  - **Latest reports**, log of recent executions, with download links in the UI and API



Focus your attention on EFFECTIVE vulns

- Sysdig is able to detect which binaries, libraries, dependencies, etc are being **actually loaded** during runtime
- A vulnerability is technically contained in the image, but is not being “run”
- Thus, is not part of the attack surface
- Looking at runtime status, we can **drastically** reduce the list of vulns that you really need to address first



Risk Spotlight

SECURE
Overview
Scanning
Compliance
Policies
Events
Audit
Captures
Get Started
AB

Runtime images > Kubernetes Workloads

Team Scope

Search... | Has running vulns

Showing **16 of 86** results

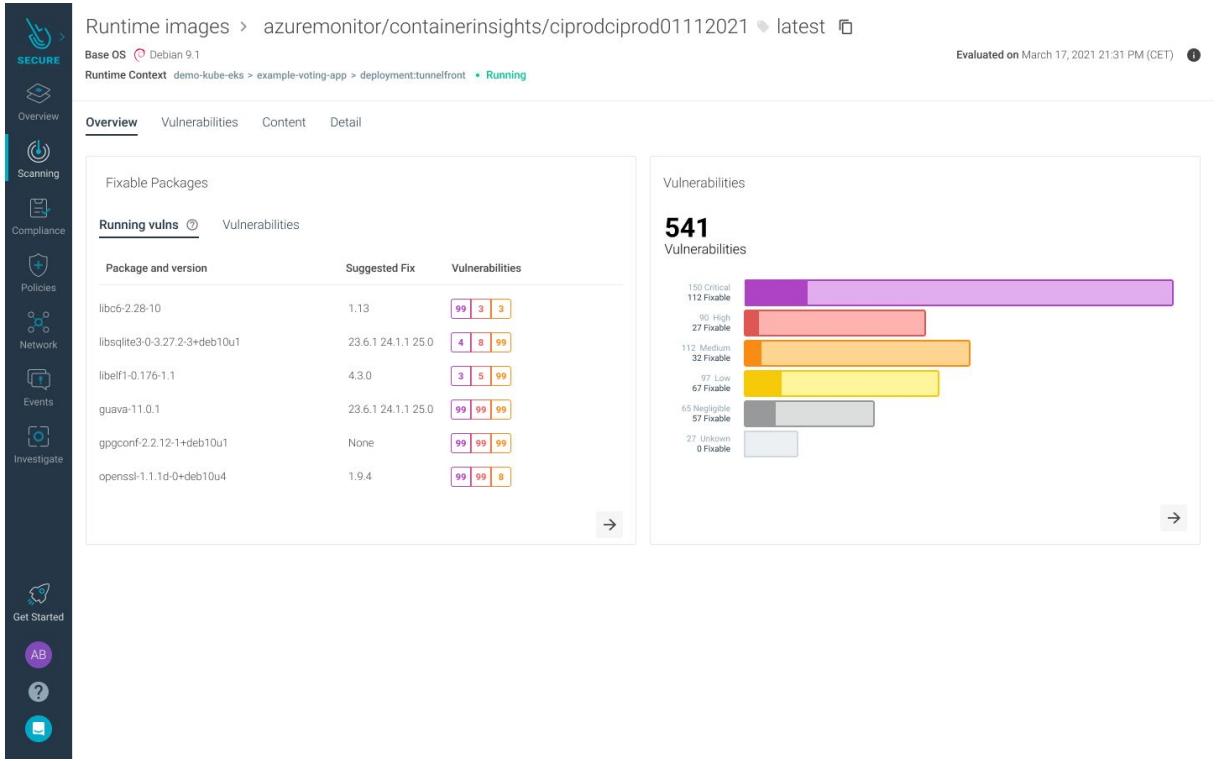
Running Vulnerabilities
We found vulnerabilities that are associated with packages that are actually running in your instantiated image - because of this those could be more targeted by attacks.
More info

Image Name	Running vulns	Vulnerabilities	Policy Eval	Image ID
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	1 3 7	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	3 1 2	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	5	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	2 10 67	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	8 10	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	3 2	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	Waiting	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	Waiting	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest		99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	Waiting	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest	Waiting	99 99 99 99 999 Exploits	Passed	903641f
demo-kube-gke > example-voting-app > deployment:tunnelfront docker.internal.sysdig.com/nuget-test latest		99 99 99 99 999 Exploits	Passed	903641f

Load more (Showing 16 from 86 results).

sysdig

Risk Spotlight



Risk Spotlight

SECURE

Overview

Scanning

Compliance

Policies

Network

Events

Investigate

Get Started

AB

Runtime images > azuremonitor/containerinsights/ciprodciprod01112021 latest

Base OS Debian 9.1

Runtime Context demo-kube-eks > example-voting-app > deployment:tunnelfront • Running

Evaluated on March 17, 2021 21:31 PM (CET)

Overview Vulnerabilities Content Detail

Search... Violations Is Running ruby × python × OS × ZSF × BSD ×

Showing 16 of 86 packages

Download

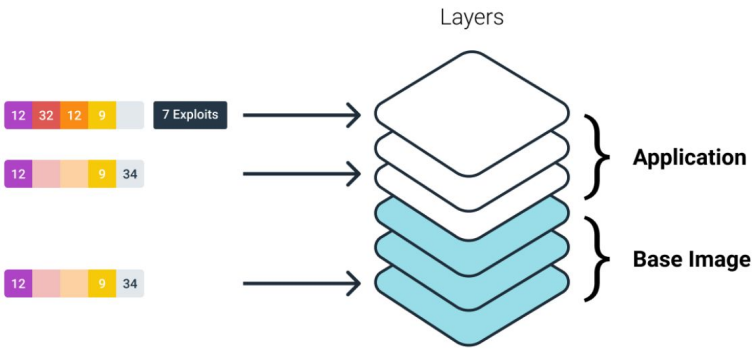
Package	Vulneratibilities	Type	License	Suggested Fix
Running libsystemd0-241-7~deb10u6	99 99 99 - 4 Exploits	ruby	ZSF	1.13
Running libmount1-2.33.1-0.1	99 99 99 -	ruby	ZSF	1.13
Running libc-bin-2.28-10	99 99 99 -	ruby	ZSF	1.13
Running libsqlite3-0-3.27.2-3+deb10u1	99 99 99 -	ruby	ZSF	1.13
Running libbsd0-0.9.1-2	99 99 99 -	ruby	ZSF	1.13
Running libcurl4-7.64.0-4+deb10u1	99 99 99 -	ruby	ZSF	1.13
Running gnupg-2.2.12-1+deb10u1	99 99 99 -	ruby	ZSF	1.13
Running libssl1.1-1.1.1d-0+deb10u4	99 99 99 -	ruby	ZSF	1.13
Running openssh-client-1:7.9p1-10+deb10u2	99 99 99 -	ruby	ZSF	1.13
Running libsystemd0-241-7~deb10u6	99 99 99 -	ruby	ZSF	1.13
Running locales-2.28-10	99 99 99 -	ruby	ZSF	1.13
Running less-487-0.1+b1	99 99 99 -	ruby	ZSF	1.13

sysdig

Mid-term Roadmap

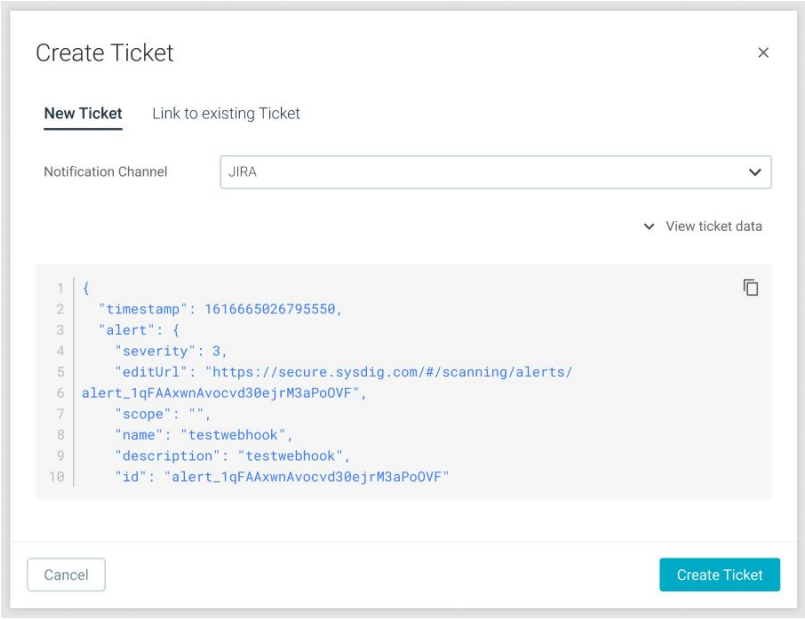
Layered Analysis and Base Image detection

- Just using FROM clause in the Dockerfile is misleading and easy to bypass
- We will analyze the image layers that belong to the base image, accurately detecting the build chain
- Why:
  - **Remediation:** Update base image instead of patching individual vulns
  - **Policy:** Detect if image is built over an obsolete or non allowed base
  - **Ownership:** Different teams maintain the base image an the app
    - I.e create tickets with the correct owners



Ticketing integration

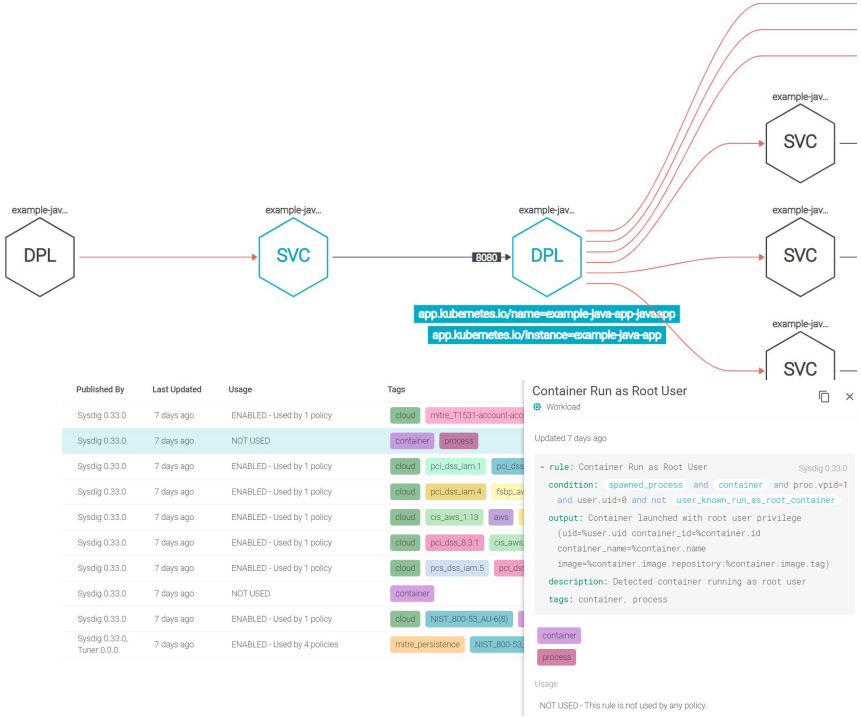
- We are going to start integrating with **Jira** and **ServiceNow**
- We will start by manually creating the ticket, second step is to **automatically** create the ticket once a certain even fires (i.e. policy violation)
- We want to start by attaching ticket to a policy violation
  - One ticket per workload, to facilitate ownership and assignment
- Possible Ticket subjects: Policy violation, Vuln, Package, Image
- Eventually we will move to more advanced integrations:
  - Notify when the vuln is no longer present in runtime



Guided mitigation

- In many cases, a vulnerability can be remediated easily, without actually changing the image at all
  - I.e. Remote exploit on an app that doesn't need to talk outside the namespace -> Sysdig NetSec
  - I.e. vulnerability requires elevated privileges -> detect run as root with Falco

- By including more information from the CVSS metrics we can provide advanced mitigation that does not require changing the image.



sysdig

IaC - Shifting “lefter”

Kubernetes IaC - Remediation

Code

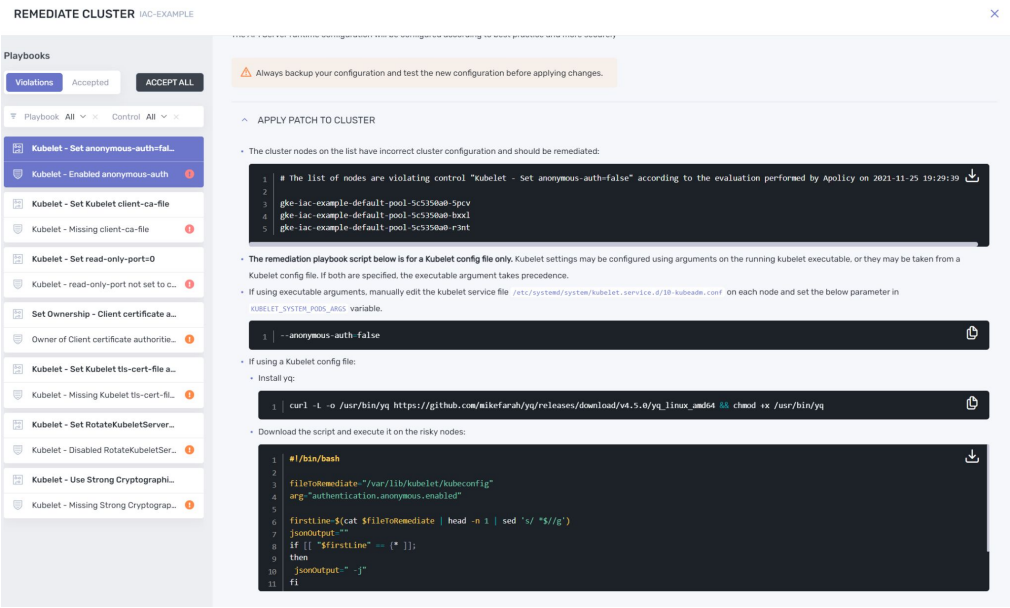
Violations of policy controls

Integrated with the PR mechanism as an approving gate

Runtime

Direct remediation to apply based on

- File modifications
- Templated YAMLs (real cluster config)
- Helm chart, etc...



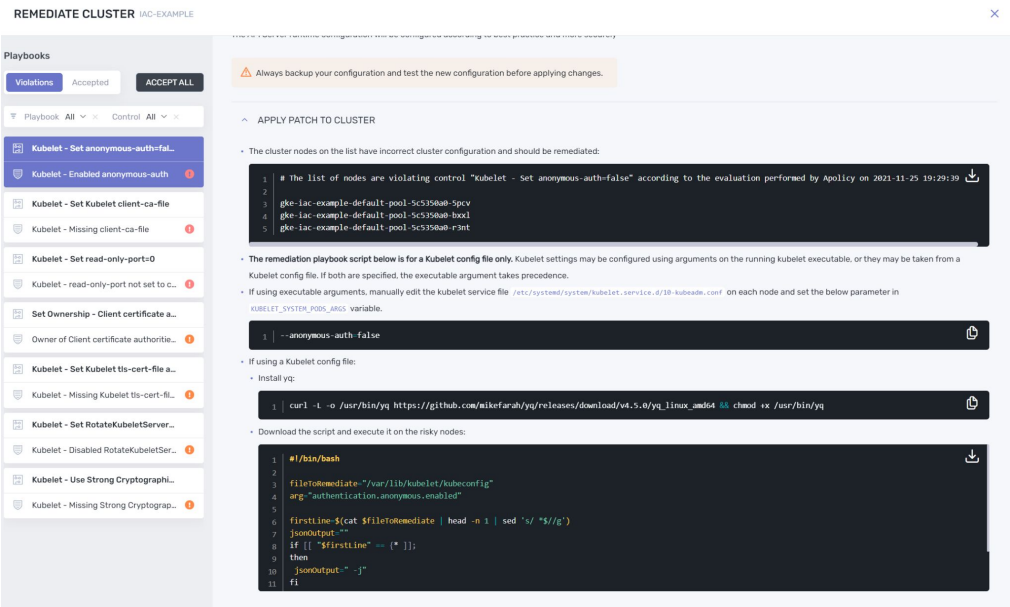
Kubernetes IaC - Drift detection

Drift detection

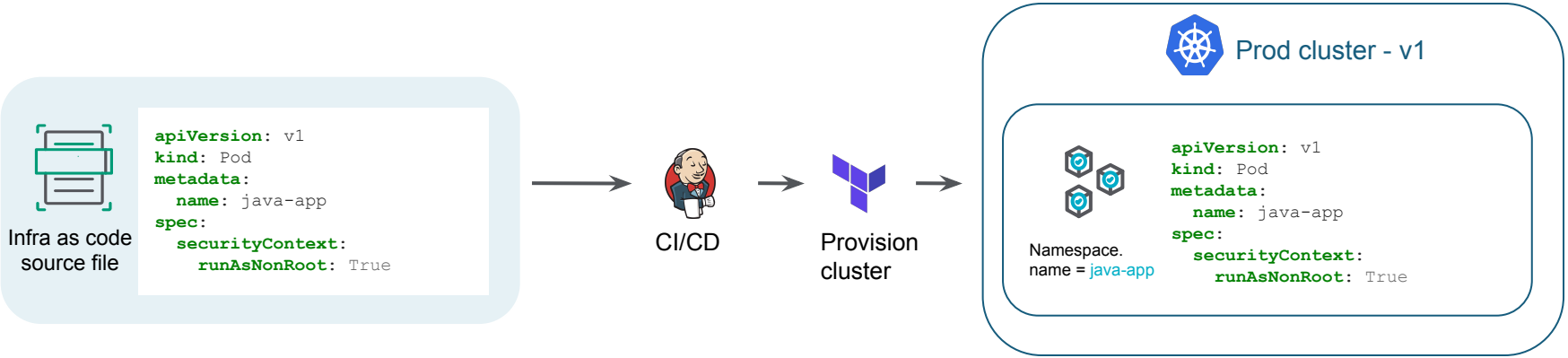
IaC mechanism is particularly powerful when it can map runtime workloads to code entities (i.e. a YAML or helm chart)

Why:

- Detect conditions in the runtime, feed back to the code level (and also live)
- Detect **Drift**
- Prevent using **Admission Controllers**



Auto-Remediate Drift and Close the Loop



Auto-Remediate Drift and Close the Loop

Loop from Production to Source

Detect runtime drift and instantly map it back to the IaC

Infra as code source file

```
apiVersion: v1
kind: Pod
metadata:
  name: java-app
spec:
  securityContext:
    runAsNonRoot: True
```

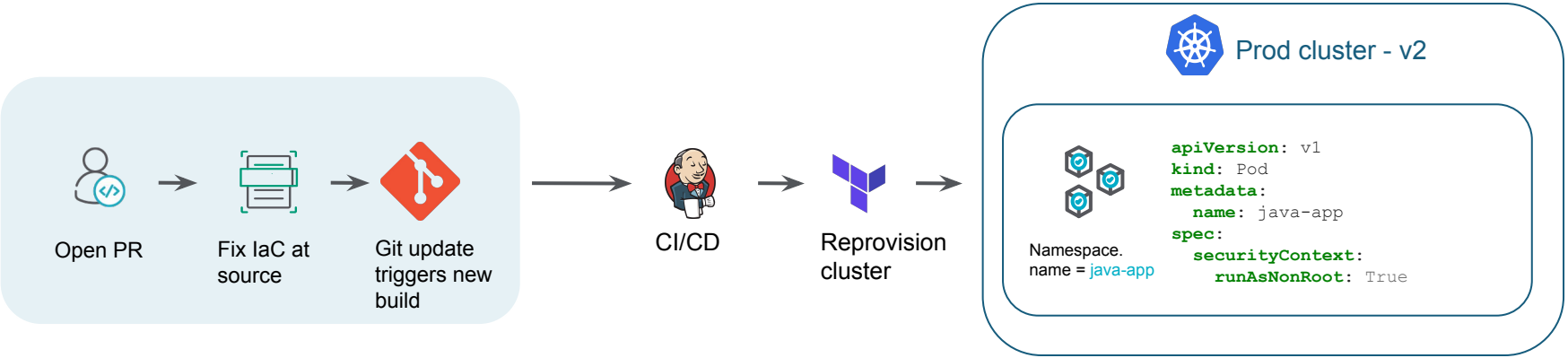
Prod cluster-tampered

Namespace.
name = java-app

```
apiVersion: v1
kind: Pod
metadata:
  name: java-app
spec:
  securityContext:
    runAsNonRoot: False
```


sysdig

Auto-Remediate Drift and Close the Loop



sysdig

sysdig

Dig deeper