




# Sysdig Technology Preview - CI/CD and IaC


Mateo Burillo - Sysdig Secure Product Manager




# **(New) Vulnerability Management**

# New Image Analysis








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	
busybox 1.31.1-r10	1.31.1-r11	
ssl_client 1.31.1-r10	1.31.1-r11	
bson 1.0.9	1.1.4	
minimist 0.0.10	0.2.1	 <b>1 Exploit</b>

### Policy Evaluations View all

Policy Evaluation	Rule failings
 Sysdig Best Practices	Vulnerabilities <b>65</b>

### 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

# Highlights!

- **Way faster:** 8x on average, over a large dataset bench
- **Binary scanner**, trivial to embed
  - Self contained go lang 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 screenshot displays the Sysdig Secure interface for a vulnerability scan. The main view shows a list of vulnerabilities for the asset 'azuremonitor/containerinsights/ciprodcipro01112021'. The table below lists several vulnerabilities:

Vulnerability	Severity	CVSS	Package and version
CVE-2020-9934	Critical	9.0 (V)	locales-2.28-10
CVE-2021-1236	Low	4.3 (M)	locales-2.28-10
CVE-2011-0766	Low	4.0 (M)	locales-2.28-10
CVE-2019-1003006	Low	4.0 (M)	locales-2.28-10
CVE-2011-034	Unknown	~	locales-2.28-10
CVE-2021-2341	Unknown	~	locales-2.28-10

The detailed view for CVE-2019-1003006 shows it is a 'Fixed in' vulnerability with a severity of 'Low' and a CVSS score of 4.0 (Medium). It is reported by 'Debian Security Tracker' and is fixable since 10 October 2020. The vulnerability score is calculated based on the source selected for score calculation. The description states: 'An integer overflow in the implementation of the posix\_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.' Exploits are listed as '45921 Sudo 1.9.5p1 - 'Baron Sameedit' Heap-Based Buffer Overflow Privilege Escalation (1)' (2 months old) and '45921 Sudo 1.9.5p1 - 'dtpriinfo' Local Privilege Escalation (2)' (13 days old).

# 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

The screenshot displays the Sysdig Secure interface for a container image. The main view shows a list of vulnerabilities for the image 'azuremonitor/containerinsights/ciprodcipro01112021'. The table below lists several vulnerabilities:

Vulnerability	Severity	CVSS	Package and version
CVE-2020-9934	Critical	9.0	locales-2.28-10
CVE-2021-1236	Low	4.3	locales-2.28-10
CVE-2011-0766	Low	4.0	locales-2.28-10
CVE-2019-1003006	Low	4.0	locales-2.28-10
CVE-2011-034	Unknown	~	locales-2.28-10
CVE-2021-2341	Unknown	~	locales-2.28-10

The right-hand pane provides detailed information for the selected vulnerability, VULNDB-106409. It indicates a severity of 'Critical' and a status of 'Fixed in' for the version 'locales-2.28-11'. The 'Vulnerability Score' section shows a score of 9.0 from VulnDB and 7.0 from NVD. The 'Description' section explains that this is an integer overflow in the implementation of the posix\_merrorn function in the GNU C Library. The 'Exploits' section lists two CVEs (45921) with their respective titles and dates.

# 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

⌵ Vulnerabilities: Severities and Threats ⋮

With  greater than or equal  AND

Fixable since  AND

Disclosure date older than or equal  days ago

∨ Exploitability Metrics

Public Exploit available and age older than  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

# Runtime Policies

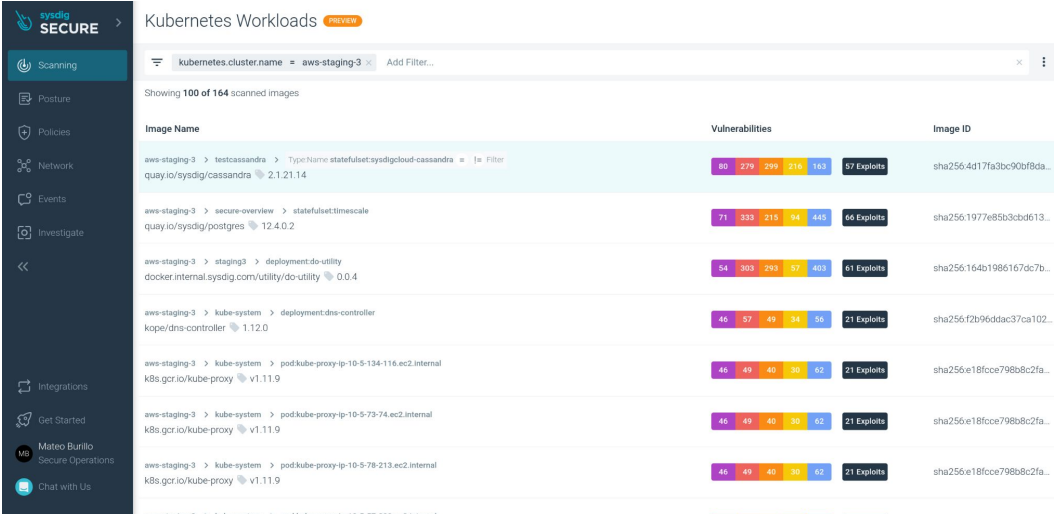
- Policies are tied to runtime metadata, not to image name
- Different environment do have different security standards
  - SOC2 environment
  - QA environment
  - DMZ
  - etc...

The screenshot shows the 'Scanning Policies > New Kubernetes Workload Policy' configuration page. The interface includes a sidebar with navigation options like Overview, Scanning, Compliance, Policies, Audit, Events, and Captures. The main content area is divided into several sections:

- Name:** A text input field containing 'My Newest Shiny Policy'.
- Description:** A text area with the placeholder text: 'Please describe your policy in a short sentence, this will help you quickly identify your policy goals and constrains'.
- Scope:** A section for defining the policy's scope. It includes a 'Scope' field with a dropdown menu showing 'kubernetes.cluster.name', a 'in' operator, and a 'prod' dropdown. Below this is a 'Select a label...' dropdown and a 'Clear all' link. A 'See workloads in this scope' button is also present.
- Rule Bundles:** A section titled 'Assign Your First Rule Bundle' with a blue call-to-action button labeled 'Assign bundle'. The text below reads: 'Add a rule bundle from our lists of recommended one or create your own'.
- Policy status change:** A section explaining that Sysdig can trigger notifications for policy status changes (e.g., from Fail to Pass).
- Notifications:** A section with a 'Select Notification Channel' dropdown and a list of channels with checkboxes: 'Slack communication channel', 'Webhook communication channel', and 'Email communication channel', all of which are currently unchecked.

# 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



The screenshot displays the Sysdig Secure interface for Kubernetes Workloads. The main content area shows a table of scanned images with columns for Image Name, Vulnerabilities, and Image ID. The table lists several images with their respective vulnerability counts and exploit status.

Image Name	Vulnerabilities	Image ID
aws-staging-3 > testcassandra > Type:Name:statefulset:sysdigcloud-cassandra   le: Filter quay.io/sysdig/cassandra 2.1.21.14	80 279 294 216 163 57 Exploits	sha256:4d17fa3bc90bf8da...
aws-staging-3 > secure-overview > statefulset:timescale quay.io/sysdig/postgres 12.4.0.2	71 333 215 94 445 66 Exploits	sha256:1977e85b3cb9d613...
aws-staging-3 > staging3 > deployment:do-utility docker.internal.sysdig.com/utility/do-utility 0.0.4	54 393 293 57 403 61 Exploits	sha256:164b1986167dc7b...
aws-staging-3 > kube-system > deployment:dns-controller kopee/dns-controller 1.12.0	46 57 49 34 56 21 Exploits	sha256:f2b96ddac37ca102...
aws-staging-3 > kube-system > pod:kube-proxy-ip-10-5-134-116.ec2.internal k8s.gcr.io/kube-proxy v1.11.9	46 49 40 30 62 21 Exploits	sha256:e18fcee798b8c2fa...
aws-staging-3 > kube-system > pod:kube-proxy-ip-10-5-73-74.ec2.internal k8s.gcr.io/kube-proxy v1.11.9	46 49 40 30 62 21 Exploits	sha256:e18fcee798b8c2fa...
aws-staging-3 > kube-system > pod:kube-proxy-ip-10-5-78-213.ec2.internal k8s.gcr.io/kube-proxy v1.11.9	46 49 40 30 62 21 Exploits	sha256:e18fcee798b8c2fa...



# 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

Vulnerability Management

## Reports

Search

Name ↑
<span>●</span> High or Worse Vulnerabilities Runtime This is the description of this specific report. Every report could have a description, a really long description
<span>●</span> High or Worse Vulnerabilities Runtime This is the description of this specific report. Every report could have a description, a really long description
<span>●</span> High or Worse Vulnerabilities Runtime This is the description of this specific report. Every report could have a description, a really long description
<input type="checkbox"/> High or Worse Vulnerabilities Runtime This is the description of this specific report. Every report could have a description, a really long description
<input type="checkbox"/> High or Worse Vulnerabilities Runtime This is the description of this specific report. Every report could have a description, a really long description
<input type="checkbox"/> High or Worse Vulnerabilities Runtime This is the description of this specific report. Every report could have a description, a really long description

**Report name** ✕  
This is the description of this specific report. Every report could have a description, a really long description

**Overview** Edit

Type	Entity	Export Format
Vulnerabilities	Runtime	JSON, CVS

**Scope**  
kubernetes.cluster.name in prod

**Conditions**  
Severity <= Critical AND Fix Available=Yes

**Schedule**  
Weekly every Mon, Tue

**Notifications**

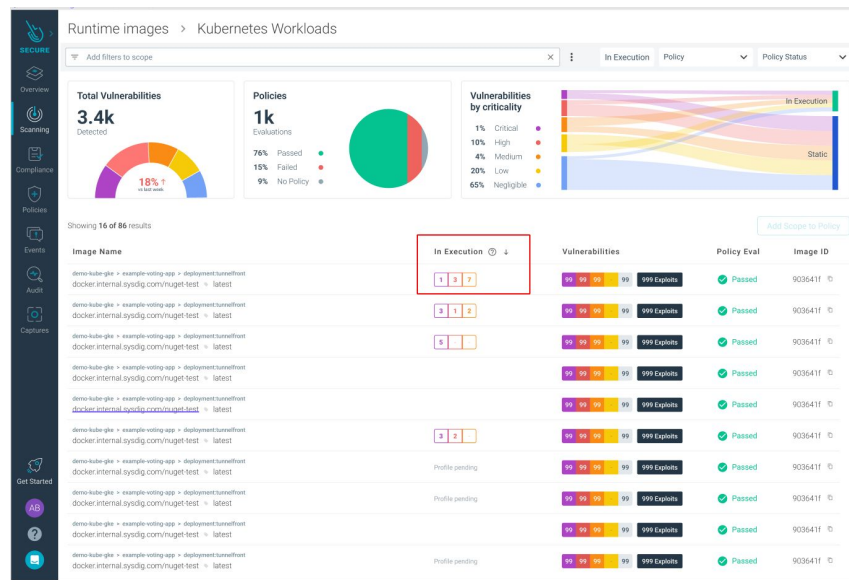
**Last run**  
● 2 days ago

**Latest reports** Generate new

<span>●</span> In progress	<a href="#">Download</a>		
<span>●</span> Complete	<a href="#">Download</a>	13/02/2022 2:38:03 pm	999 days ago
<span>●</span> Complete	<a href="#">Download</a>	13/02/2022 2:38:03 pm	999 days ago
<span>●</span> Complete	<a href="#">Download</a>	13/02/2022 2:38:03 pm	999 days ago
<span>●</span> Complete	<a href="#">Download</a>	13/02/2022 2:38:03 pm	999 days ago
<span>●</span> Complete	<a href="#">Download</a>	13/02/2022 2:38:03 pm	999 days ago
<span>●</span> Error		This is the error text and it could be really long, like really long like this	
<span>●</span> Error		This is the error text and it could be really long, like really long like this	

# 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

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

[Load more](#) (Showing 16 from 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](#)

# Risk Spotlight

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

### Fixable Packages

Running vulns Vulnerabilities

Package and version	Suggested Fix	Vulnerabilities
libc6-2.28-10	1.13	99 3 3
libsqlite3-0-3.27.2-3+deb10u1	23.6.1 24.1.1 25.0	4 8 99
libelf1-0.176-1.1	4.3.0	3 5 99
guava-11.0.1	23.6.1 24.1.1 25.0	99 99 99
gpgconf-2.2.12-1+deb10u1	None	99 99 99
openssl-1.1.1d-0+deb10u4	1.9.4	99 99 8

### Vulnerabilities

541 Vulnerabilities

Severity	Count	Fixable
Critical	150	112
High	90	27
Medium	112	32
Low	97	67
Negligible	65	57
Unknown	27	0

# Risk Spotlight

Runtime images > azuremonitor/containerinsights/ciprodcipro01112021 ▾ 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

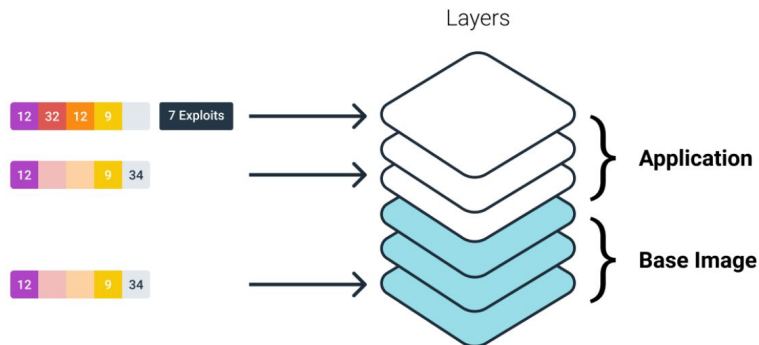
Package ↑	Vulnerabilities	Type	License	Suggested Fix
<span>Running</span> libsystemd0-241-7--deb10u6	99 99 99 - 4 Exploits	ruby	ZSF	1.13
<span>Running</span> libmount1-2.33.1-0.1	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> libc-bin-2.28-10	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> libsqlite3-0-3.27.2-3+deb10u1	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> libbsd0-0.9.1-2	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> libcurl4-7.64.0-4+deb10u1	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> gnupg-2.2.12-1+deb10u1	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> libssl1.1-1.1.1d-0+deb10u4	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> openssh-client-1.7.9p1-10+deb10u2	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> libsystemd0-241-7--deb10u6	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> locales-2.28-10	99 99 99 -	ruby	ZSF	1.13
<span>Running</span> less-487-0.1+b1	99 99 99 -	ruby	ZSF	1.13



# 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 event 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

### Create Ticket

**New Ticket** Link to existing Ticket

Notification Channel

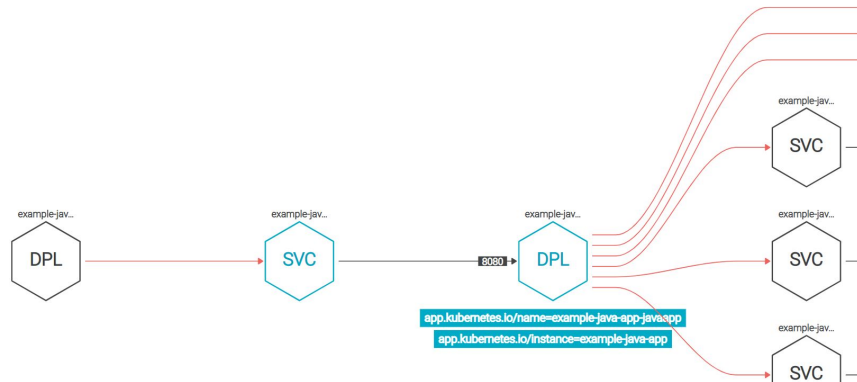
[View ticket data](#)

```
1 {
2   "timestamp": 1616665026795550,
3   "alert": {
4     "severity": 3,
5     "editUrl": "https://secure.sysdig.com/#/scanning/alerts/
6 alert_1qFAAxwnAvocvd30ejrM3aPo0VF",
7     "scope": "",
8     "name": "testwebhook",
9     "description": "testwebhook",
10    "id": "alert_1qFAAxwnAvocvd30ejrM3aPo0VF"
```



# 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.

Published By	Last Updated	Usage	Tags
Sysdig 0.33.0	7 days ago	ENABLED - Used by 1 policy	cloud, mibe_TI531-account-ans
Sysdig 0.33.0	7 days ago	NOT USED	container, process
Sysdig 0.33.0	7 days ago	ENABLED - Used by 1 policy	cloud, pci_dss_lam.1, pci_dss
Sysdig 0.33.0	7 days ago	ENABLED - Used by 1 policy	cloud, pci_dss_lam.4, fcbp_la
Sysdig 0.33.0	7 days ago	ENABLED - Used by 1 policy	cloud, cis_aws_1.13, aws
Sysdig 0.33.0	7 days ago	ENABLED - Used by 1 policy	cloud, pci_dss_8.3.1, cis_ams
Sysdig 0.33.0	7 days ago	ENABLED - Used by 1 policy	cloud, pci_dss_lam.5, pci_dss
Sysdig 0.33.0	7 days ago	NOT USED	container
Sysdig 0.33.0	7 days ago	ENABLED - Used by 1 policy	cloud, NIST_800_53_AU4(a),
Sysdig 0.33.0, Turner 0.0.0	7 days ago	ENABLED - Used by 4 policies	mitre_persistence, NIST_800_53

### Container Run as Root User

Workload

Updated 7 days ago

```
- rule: Container Run as Root User Sysdig 0.33.0
condition: spawned_process and container and proc.vpid=1
and user.uid=0 and not user_known_run_as_root_container
output: Container launched with root user privilege
(uid=user.uid container_id=container.id
container_name=container.name
image=container.image.repository:%container.image.tag)
description: Detected container running as root user
tags: container, process
```

Usage

NOT USED - This rule is not used by any policy.



# laC - Shifting “left”

# 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...

The screenshot displays the 'REMIEDIATE CLUSTER' interface for 'IAC-EXAMPLE'. On the left, a 'Playbooks' sidebar lists various violations, including 'Kubelet - Set anonymous-auth=false', 'Kubelet - Enabled anonymous-auth', 'Kubelet - Set Kubelet client-ca-file', 'Kubelet - Missing client-ca-file', 'Kubelet - Set read-only-port=0', 'Kubelet - read-only-port not set to c...', 'Set Ownership - Client certificate a...', 'Owner of Client certificate authorit...', 'Kubelet - Set Kubelet ts-cert-file a...', 'Kubelet - Missing Kubelet ts-cert-fi...', 'Kubelet - Set RotateKubeletServer...', 'Kubelet - Disabled RotateKubeletSer...', 'Kubelet - Use Strong Cryptographi...', and 'Kubelet - Missing Strong Cryptograp...'. The main area shows a warning: 'Always backup your configuration and test the new configuration before applying changes.' Below this, the 'APPLY PATCH TO CLUSTER' section contains a list of nodes to be remediated and a remediation script. The script is a bash script that uses 'filetoRemediate' to generate a kubeconfig file and then applies it to the cluster.

```
1 # The list of nodes are violating control "Kubelet - Set anonymous-auth=false" according to the evaluation performed by Apolyc on 2021-11-25 19:29:39
2
3 gke-iac-example-default-pool-5c339ab-5pcv
4 gke-iac-example-default-pool-5c339ab-hscl
5 gke-iac-example-default-pool-5c339ab-r2nt
```

```
1 --anonymous-auth=false
```

```
1 curl -i -o /usr/bin/yq https://github.com/mikefarah/yq/releases/download/v4.5.0/yq_linux_amd64 && chmod +x /usr/bin/yq
```

```
1 #!/bin/bash
2 filetoRemediate="/usr/lib/kubelet/kubeconfig"
3 arg="authentication.anonymous.enabled"
4
5
6 firstLine=$(cat $filetoRemediate | head -n 1 | sed '/^#/g')
7 jsonOutput=""
8 if [[ "$firstLine" == "{*" ]];
9 then
10 jsonOutput="}"
11 fi
```

# 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**

The screenshot displays the 'REMIEDIATE CLUSTER' interface for a cluster named 'IAC-EXAMPLE'. On the left, a 'Playbooks' sidebar lists several violations, with 'Kubelet - Set anonymous-auth=false' selected. The main area shows a warning: 'Always backup your configuration and test the new configuration before applying changes.' Below this, the 'APPLY PATCH TO CLUSTER' section contains a remediation script. The script identifies nodes violating the 'Kubelet - Set anonymous-auth=false' control and provides instructions on how to apply the patch using either kubelet arguments or a kubelet config file.

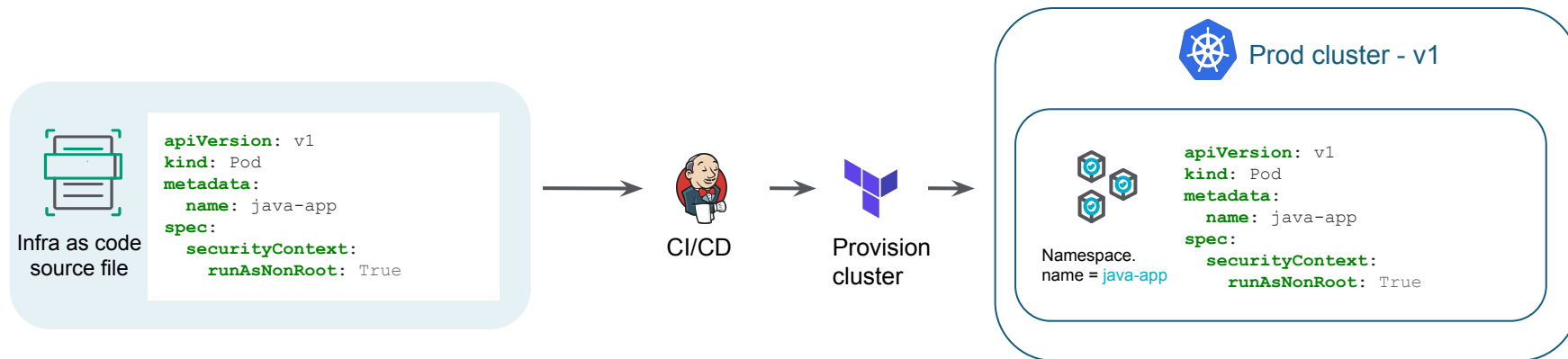
```
1 # The list of nodes are violating control "Kubelet - Set anonymous-auth=false" according to the evaluation performed by Apolycy on 2021-11-25 19:29:39
2
3 gke-iac-example-default-pool-5c339ab-5pcv
4 gke-iac-example-default-pool-5c339ab-hscl
5 gke-iac-example-default-pool-5c339ab-r2nt
```

```
1 --anonymous-auth=false
```

```
1 curl -L -O /usr/bin/yq https://github.com/mikefarah/yq/releases/download/v4.5.0/yq_linux_amd64 && chmod +x /usr/bin/yq
```

```
1 #!/bin/bash
2 fileToRemediate="/usr/lib/kubelet/kubeconfig"
3 arg="authentication.anonymous.enabled"
4
5
6 firstLine=$(cat $fileToRemediate | head -n 1 | sed 's/"/"/g')
7 jsonOutput=""
8 if [[ "$firstLine" == {"*} ]];
9 then
10 jsonOutput="-$]"
11 fi
```

# 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

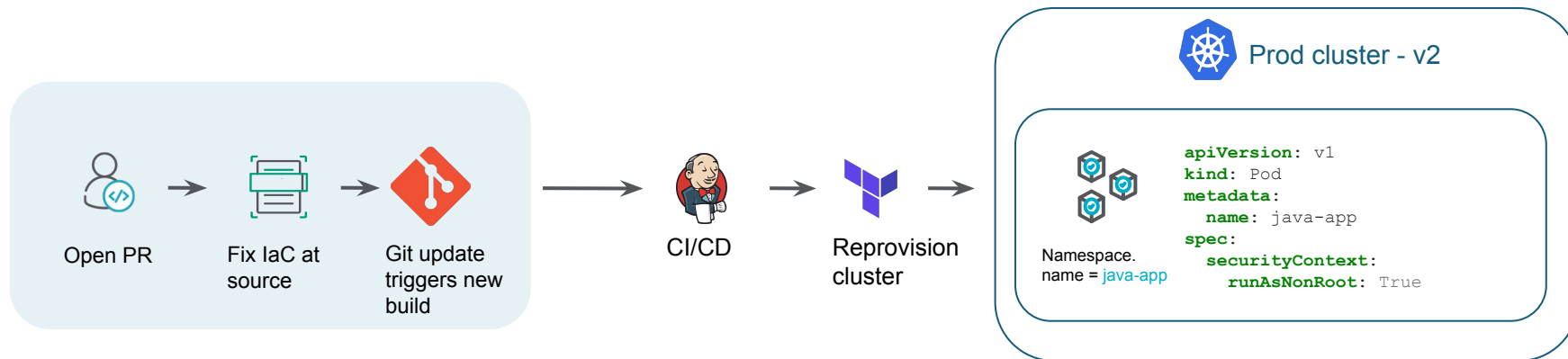


Namespace.  
name = java-app

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



# Auto-Remediate Drift and Close the Loop





**sysdig**

Dig deeper