cisco Live!

Let's go

#CiscoLive

The bridge to possible

DevSecOps (shift left) to secure Cloud Native Application

Arvind Kumar and Faisal Azizullah - Principal Engineer
CX Americas CTAO

DEVNET-3012

Cisco Webex App

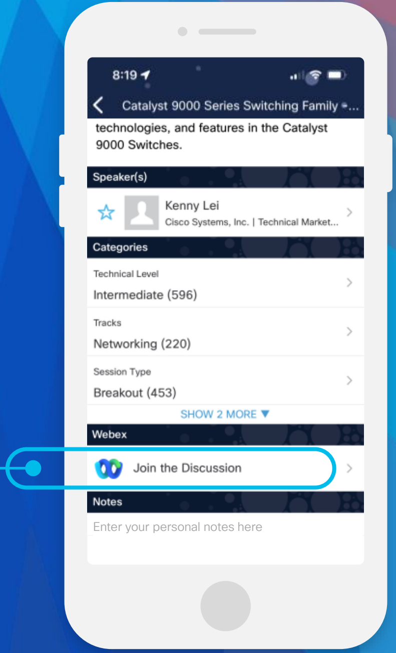
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 9, 2023.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-3012

Agenda

- Application Market Trends
- Cloud Native Security Challenges
- Cisco Panoptica Overview
- Demo
- Q&A

Application Market Trends

Application experience is more Critical than ever

49% of users switched supplier due to poor digital experience

50% willing to pay more for a digital experience better than that of a competitors

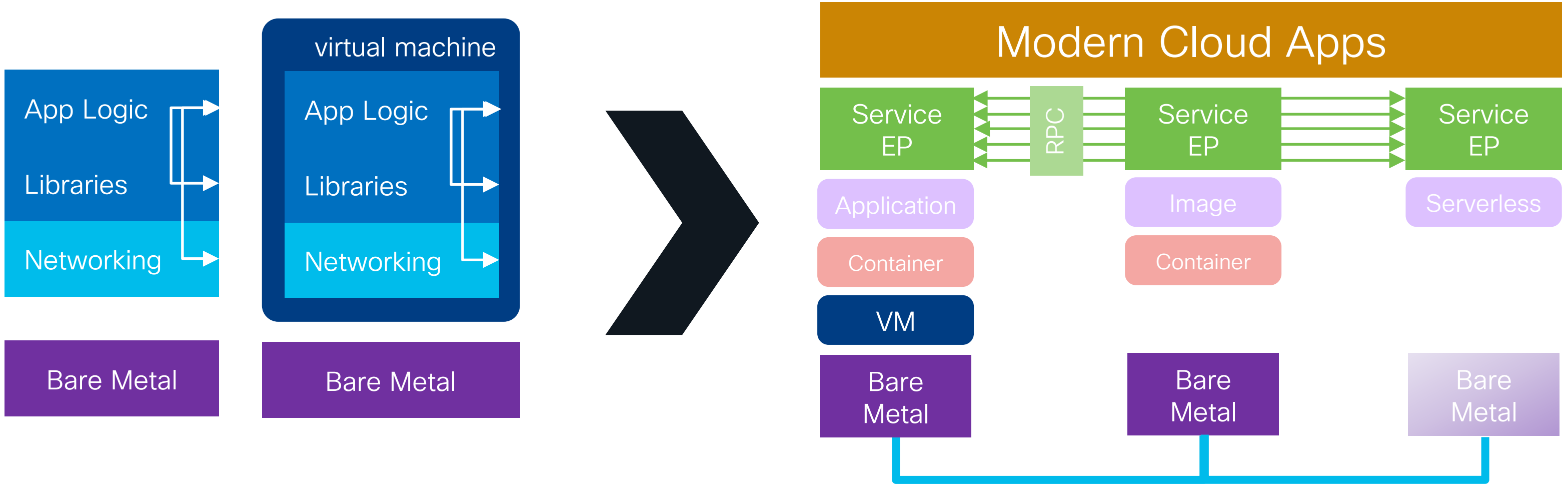
100ms delay in load time = 7% drop in online conversations

In the next 3 years, 500 million new apps will be written, almost all of them for the digital world

Application Transformation

From monolithic

To distributed microservices loosely coupled with Infrastructure



App Logic

Libraries

Networking

Bare Metal

virtual machine

App Logic

Libraries

Networking

Bare Metal

Modern Cloud Apps

Service EP

RPC

Service EP

Service EP

Application

Container

VM

Bare Metal

Image

Container

Bare Metal

Serverless

Bare Metal

Cloud Native Security Challenges

Explosion of threat vectors in microservices security

93%

of companies had a Kubernetes security incident in the last 12 months

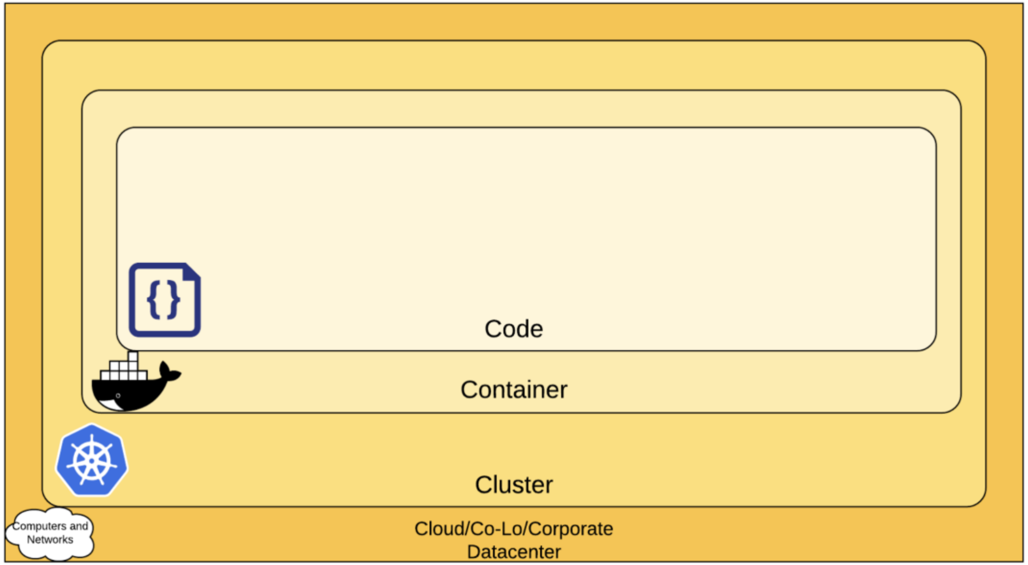
$4.35 million

Average cost of a data breach in 2022

286% API attack increase

Every quarter and API attacks will be the most frequent attack vector in the future according to Gartner

Cloud Native Security Challenges

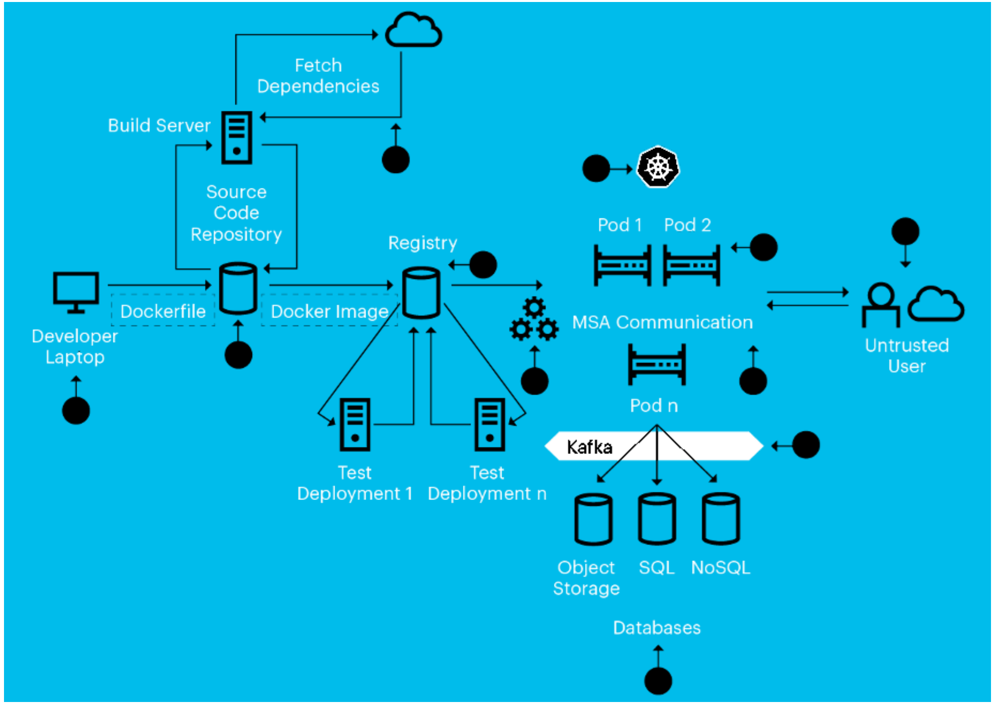


Source: kubernetes.io

4 C’s of Cloud Native Security

- Public/Private Cloud Infrastructure Security Posture
- Kubernetes Cluster Security Posture
- Container Security
  - Image
  - Runtime
  - Micro segmentation
- API Security
  - Authentication and Authorization
  - Encryption
- Secrets Management

Modern applications have larger attack surface



Gartner: Threat vectors in the container lifecycle

1. Development system
2. Git-based repository
3. Retrieval of dependencies
4. Image registry
5. Unsecured orchestrator platform
6. Host-container relationship
7. Rapid rate of change
8. MSA communication and network segregation
9. Inter-process communication
10. Increased number of databases
11. Application layer attacks

https://www.gartner.com/en/documents/3983248/containers-11-threats-and-how-to-control-them

Approach to Application Security

How Do I Protect Cloud Native Apps?

Shift-Left Security

Is the application configured properly?

What software does it use?

Application Composition

Can I rely on communication between services?

Connection and API Assessment

Can I automatically manage risk introduced by vulnerable apps?

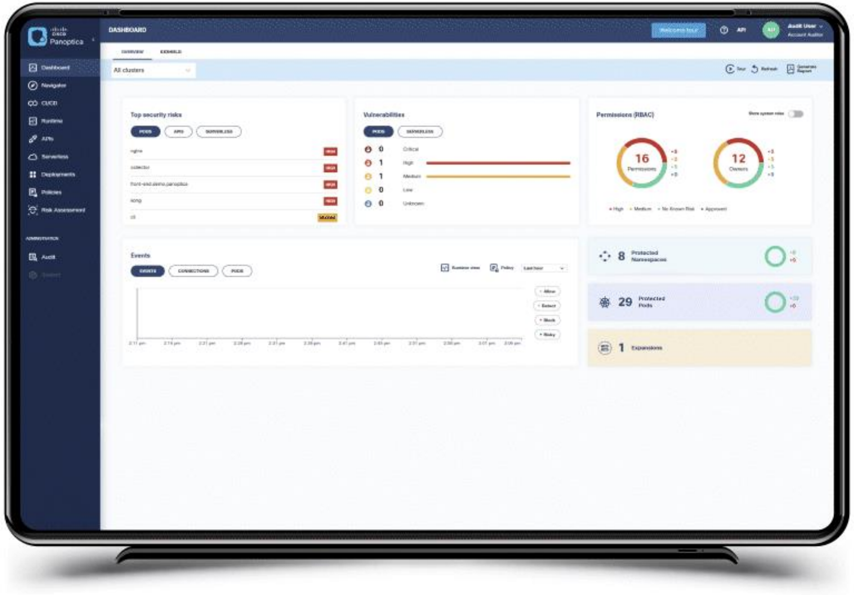
Policy Control Governance

Cisco Panoptica

Cloud-Native Application Security, Simplified

Panoptica

Simplified Cloud-Native Application Security for DevSecOps, Platform, and DevOps teams



https://panoptica.app

Cisco Panoptica enables DevSecOps at scale

Policy automation

Write one policy and propagate across containers or code deployments to ensure new code has less risk

Actionable Insights

Dashboard highlighting MITRE ATT&CK vectors aligned to Kubernetes risks

Pod-based approach

Application runs on a single pod that covers your entire environment – even across clouds

Works across all Kubernetes platforms

RedHat OpenShift

Rancher RKE

Google GKE

Azure AKS

Alibaba ACK

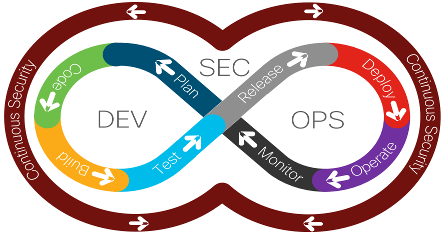
AWS EKS

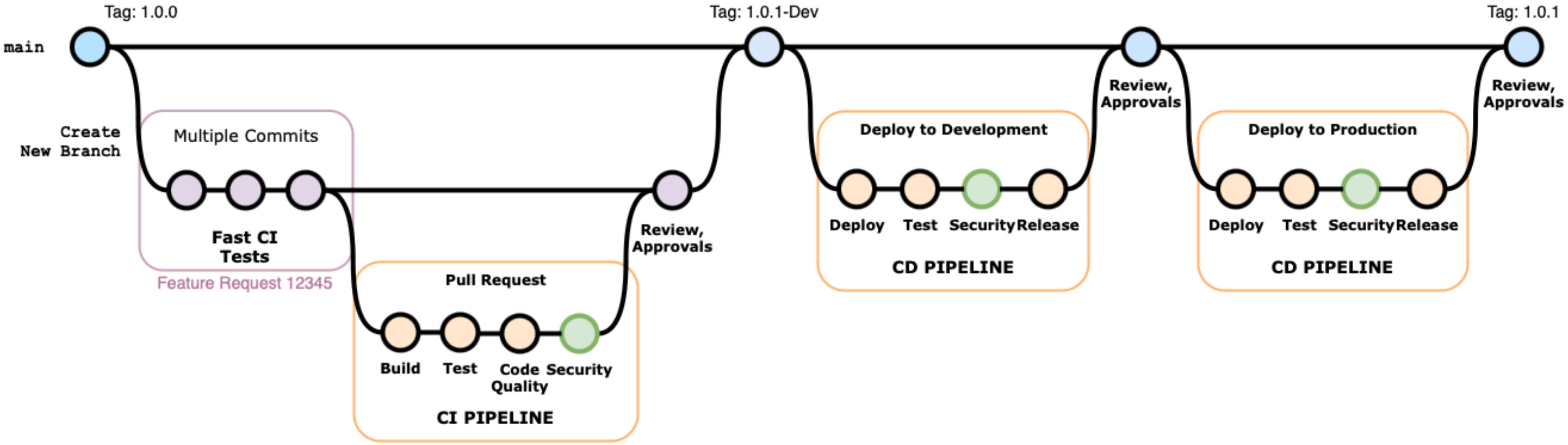
Oracle OCI

Tencent TKE

Cloud Native Security **Goal**

"Shift Left" and Make It Continuous



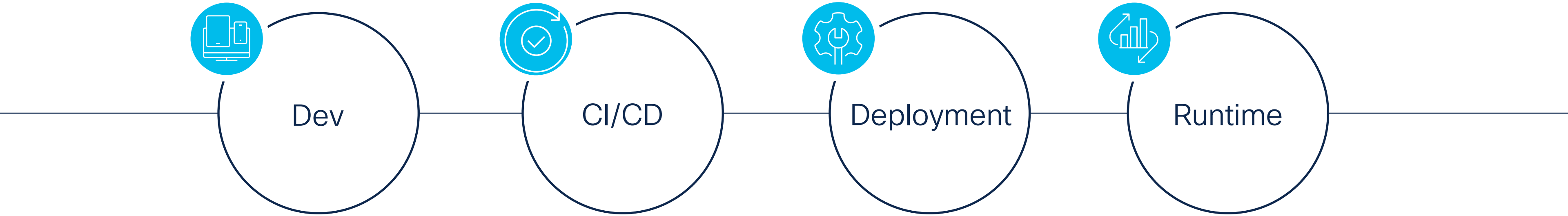


Apply Security Before *Any* Integration

Apply Security Before *Every* Deployment

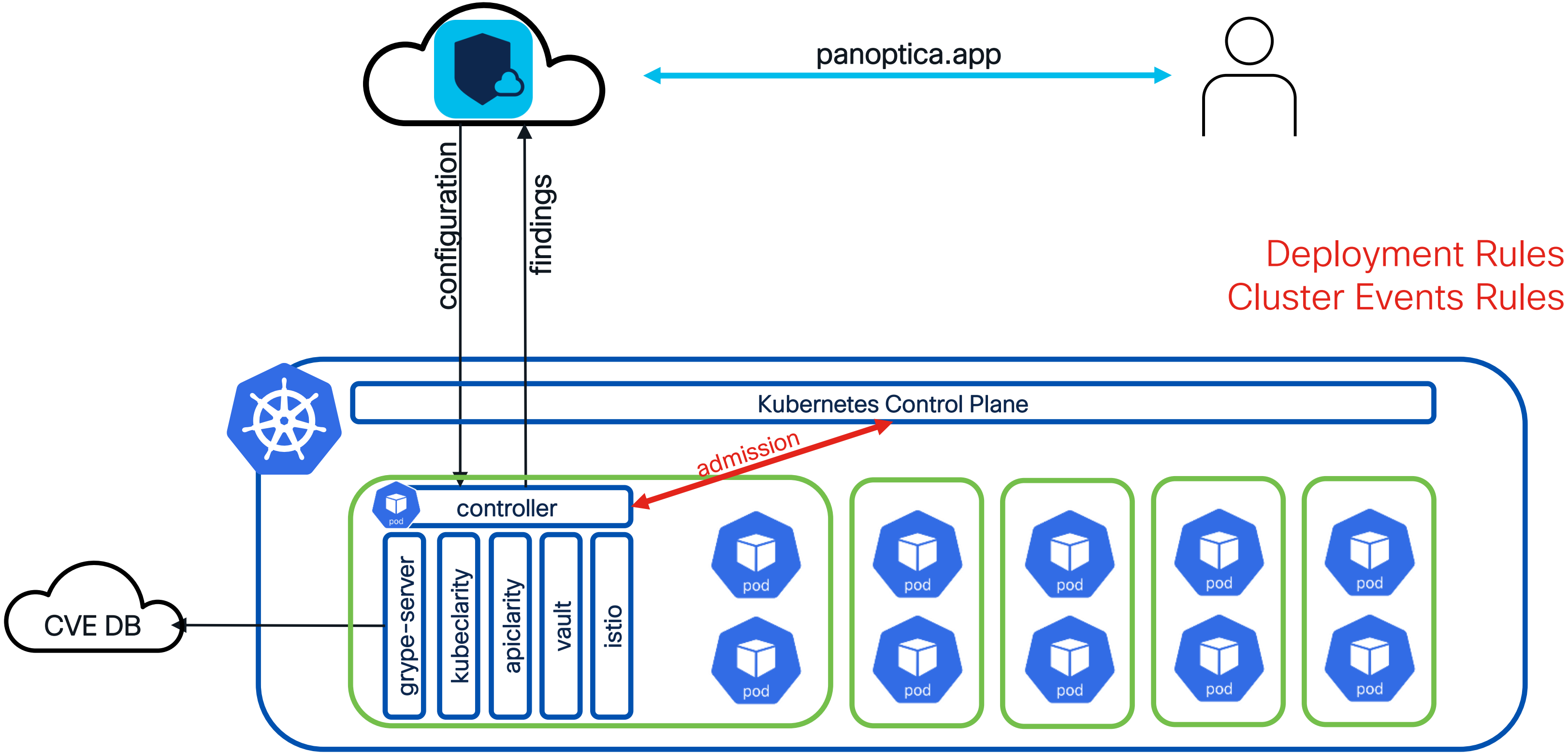
Shifting Security to the Left

Enabling security across the full app stack - dev to runtime

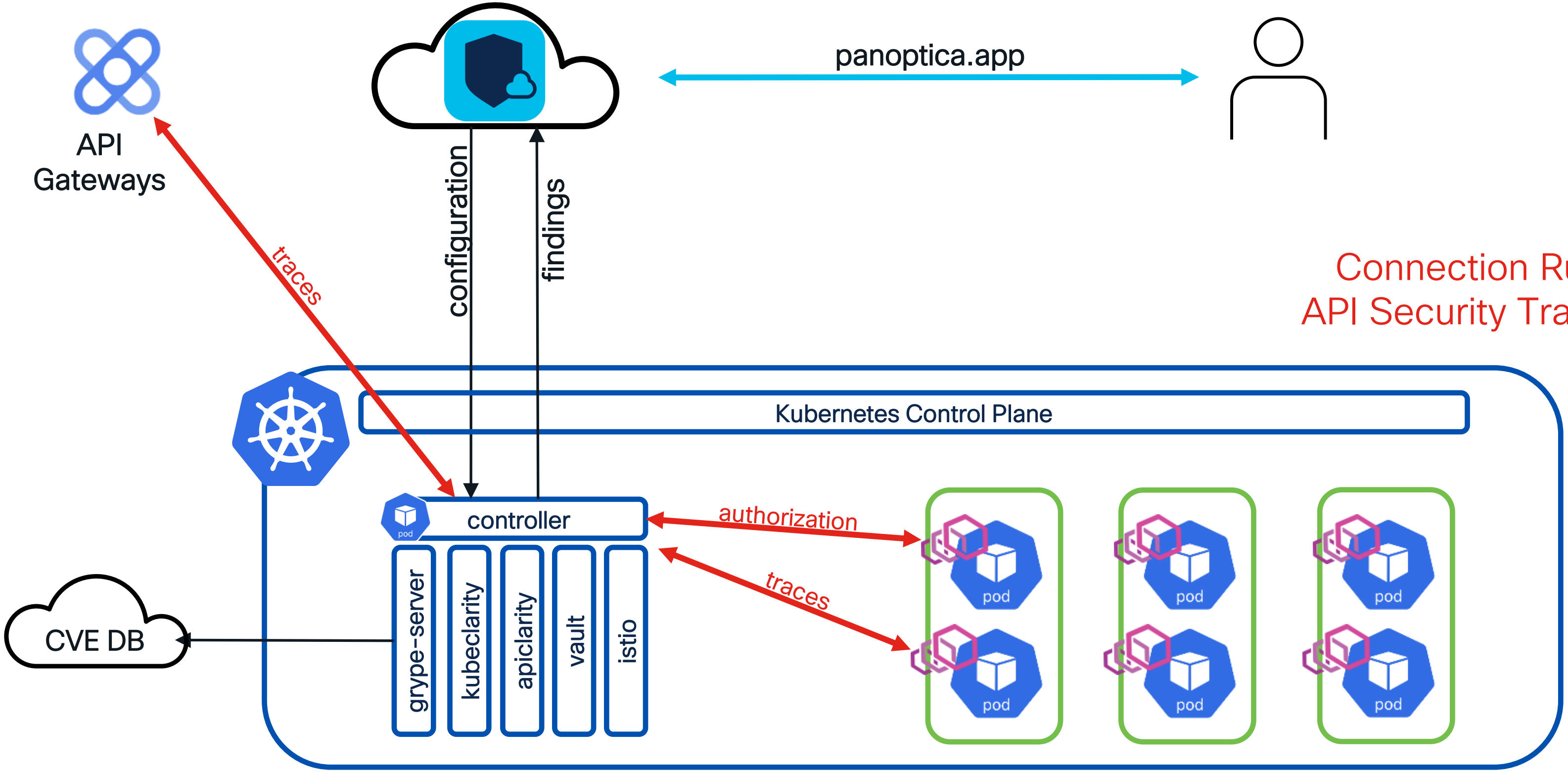


Shift Left Security	Application Composition	Connection and API Assessment	Policy Control Governance
git	Jenkins circleci	Terraform HELM	FAAS

Single Controller, Modular Architecture



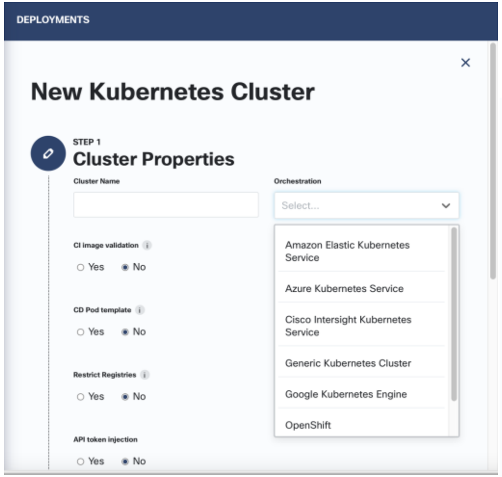
Single Controller, Modular Architecture



Connection Rules
API Security Traces

Getting Started with Cisco Panoptica

1. Create an account on https://panoptica.app (Its free !)
2. Bring your own Kubernetes cluster and add it to the portal
3. Download the installer artifacts and deploy in your cluster



DEPLOYMENTS

New Kubernetes Cluster

STEP 1

Cluster Properties

Cluster Name

Orchestration: Select...

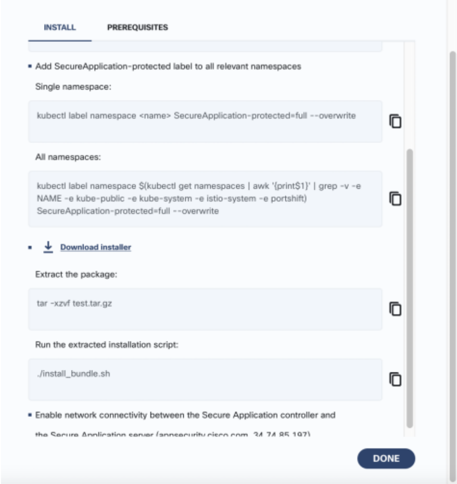
- Amazon Elastic Kubernetes Service
- Azure Kubernetes Service
- Cisco Intersight Kubernetes Service
- Generic Kubernetes Cluster
- Google Kubernetes Engine
- OpenShift

CI image validation: ○ Yes ● No

CD Pod template: ○ Yes ● No

Restrict Registries: ○ Yes ● No

API token injection: ○ Yes ● No



- Add SecureApplication-protected label to all relevant namespaces

Single namespace:

```
kubectl label namespace <name> SecureApplication-protected=full --overwrite
```

All namespaces:

```
kubectl label namespace $(kubectl get namespaces | awk '{print$1}' | grep -v -e
NAME -e kube-public -e kube-system -e istio-system -e portshift)
SecureApplication-protected=full --overwrite
```

- Download installer

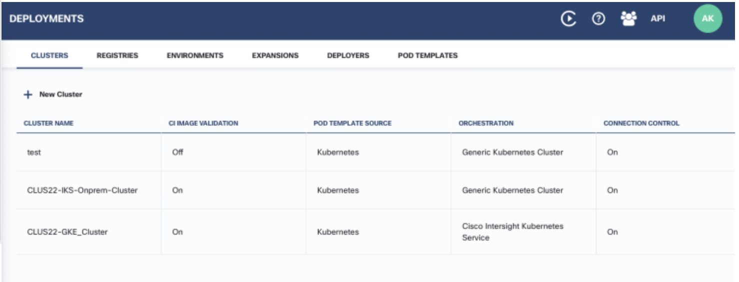
Extract the package:

```
tar -xzvf test.tar.gz
```

Run the extracted installation script:

```
./install_bundle.sh
```

- Enable network connectivity between the Secure Application controller and the Secure Application server (appsecurity.cisco.com, 34.74.85.197)



DEPLOYMENTS

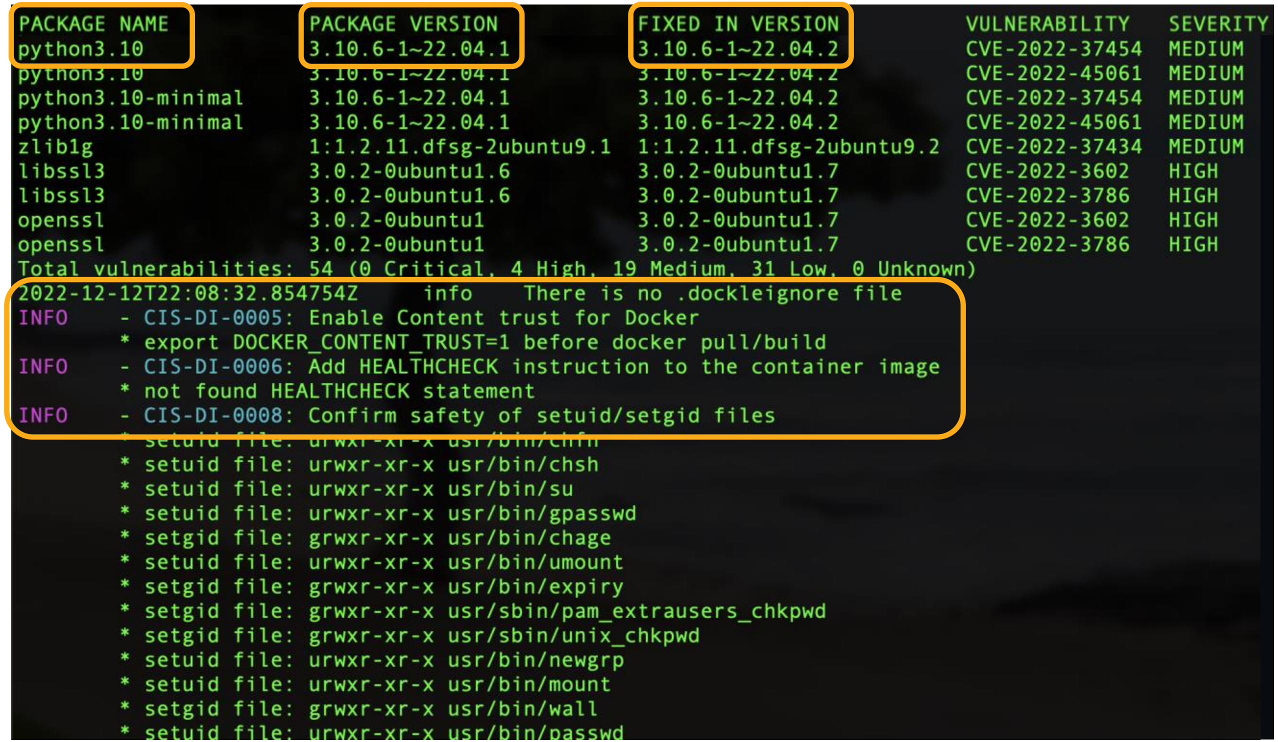
CLUSTER NAME	CI IMAGE VALIDATION	POD TEMPLATE SOURCE	ORCHESTRATION	CONNECTION CONTROL
test	Off	Kubernetes	Generic Kubernetes Cluster	On
CLUS22-IKS-Onprem-Cluster	On	Kubernetes	Generic Kubernetes Cluster	On
CLUS22-GKE_Cluster	On	Kubernetes	Cisco Intersight Kubernetes Service	On

Demo

Continuous Integration Actionable Security

Continuous Integration Actionable Security

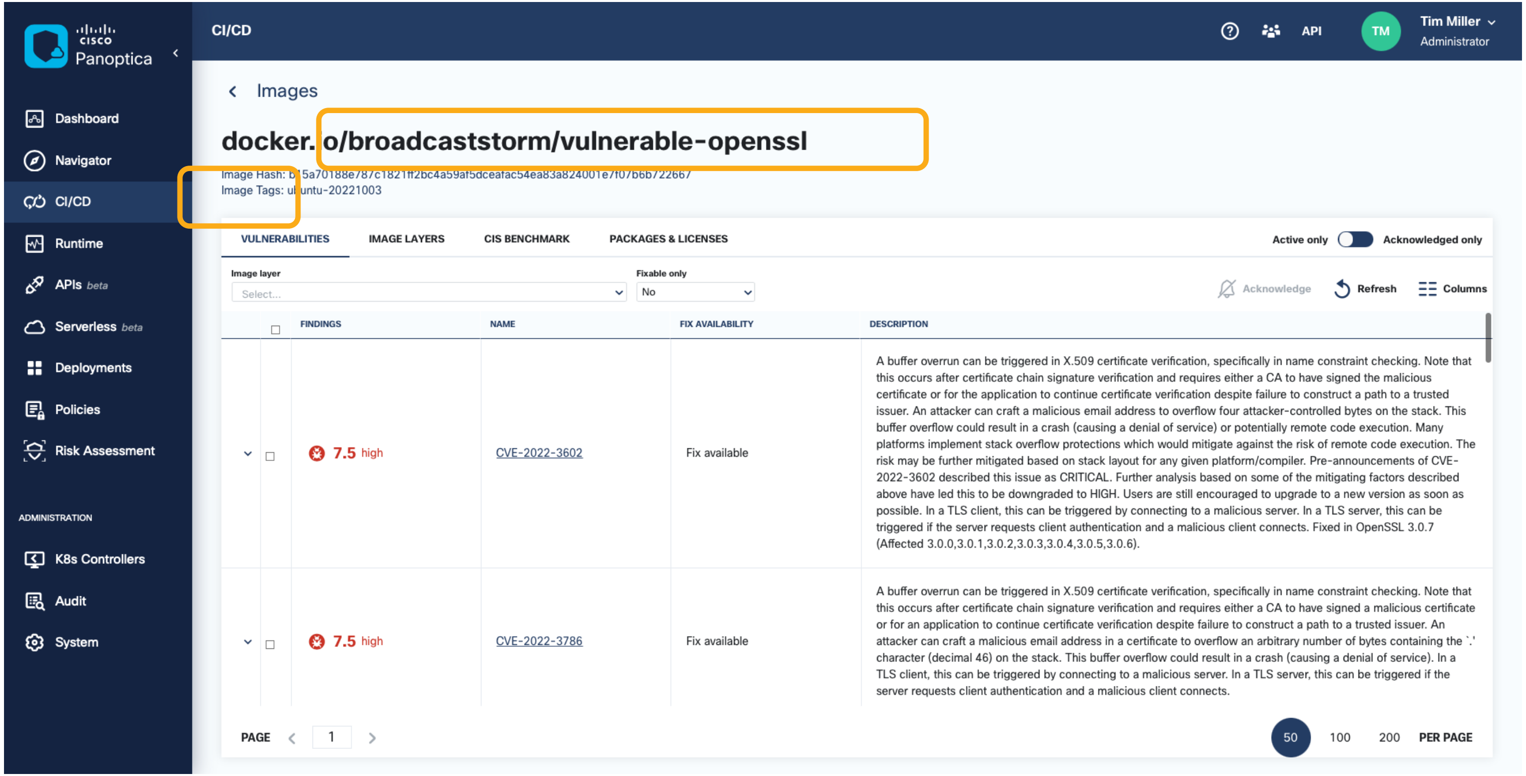
Developer Persona
Pipeline Report



```
PACKAGE NAME           PACKAGE VERSION           FIXED IN VERSION          VULNERABILITY   SEVERITY
python3.10             3.10.6-1~22.04.1          3.10.6-1~22.04.2          CVE-2022-37454  MEDIUM
python3.10             3.10.6-1~22.04.1          3.10.6-1~22.04.2          CVE-2022-45061  MEDIUM
python3.10-minimal     3.10.6-1~22.04.1          3.10.6-1~22.04.2          CVE-2022-37454  MEDIUM
python3.10-minimal     3.10.6-1~22.04.1          3.10.6-1~22.04.2          CVE-2022-45061  MEDIUM
zlib1g                 1:1.2.11.dfsg-2ubuntu9.1  1:1.2.11.dfsg-2ubuntu9.2  CVE-2022-37434  MEDIUM
libssl3                3.0.2-0ubuntu1.6          3.0.2-0ubuntu1.7          CVE-2022-3602   HIGH
libssl3                3.0.2-0ubuntu1.6          3.0.2-0ubuntu1.7          CVE-2022-3786   HIGH
openssl                3.0.2-0ubuntu1            3.0.2-0ubuntu1.7          CVE-2022-3602   HIGH
openssl                3.0.2-0ubuntu1            3.0.2-0ubuntu1.7          CVE-2022-3786   HIGH
Total vulnerabilities: 54 (0 Critical, 4 High, 19 Medium, 31 Low, 0 Unknown)
2022-12-12T22:08:32.854754Z      info    There is no .dockleignore file
INFO    - CIS-DI-0005: Enable Content trust for Docker
        * export DOCKER_CONTENT_TRUST=1 before docker pull/build
INFO    - CIS-DI-0006: Add HEALTHCHECK instruction to the container image
        * not found HEALTHCHECK statement
INFO    - CIS-DI-0008: Confirm safety of setuid/setgid files
        * setuid file: urwxr-xr-x usr/bin/chfn
        * setuid file: urwxr-xr-x usr/bin/chsh
        * setuid file: urwxr-xr-x usr/bin/su
        * setuid file: urwxr-xr-x usr/bin/gpasswd
        * setgid file: grwxr-xr-x usr/bin/chage
        * setuid file: urwxr-xr-x usr/bin/umount
        * setgid file: grwxr-xr-x usr/bin/expiry
        * setgid file: grwxr-xr-x usr/sbin/pam_extrausers_chkpwd
        * setgid file: grwxr-xr-x usr/sbin/unix_chkpwd
        * setuid file: urwxr-xr-x usr/bin/newgrp
        * setuid file: urwxr-xr-x usr/bin/mount
        * setgid file: grwxr-xr-x usr/bin/wall
        * setuid file: urwxr-xr-x usr/bin/passwd
```

Continuous Integration Risk Visibility

Security Persona
Summary Report



‹ Images

docker.io/broadcaststorm/vulnerable-openssl

Image Hash: b15a70188e787c1821ff2bc4a59af5dceafac54ea83a824001e7f07b6b722667
Image Tags: ubuntu-20221003

VULNERABILITIES | IMAGE LAYERS | CIS BENCHMARK | PACKAGES & LICENSES

Active only ● Acknowledged only

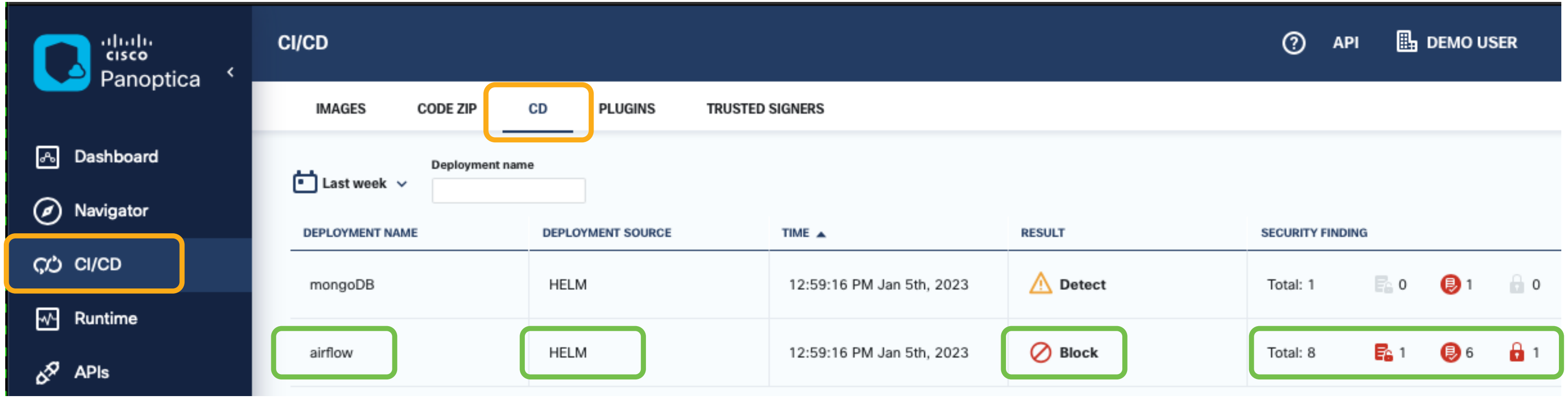
Image layer: Select...
Fixable only: No

Acknowledge | Refresh | Columns

	□	FINDINGS	NAME	FIX AVAILABILITY	DESCRIPTION
˅	□	7.5 high	CVE-2022-3602	Fix available	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6).
˅	□	7.5 high	CVE-2022-3786	Fix available	A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the '.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.

PAGE ‹ 1 › 50 100 200 PER PAGE

Continuous Deployment Policy Enforcement

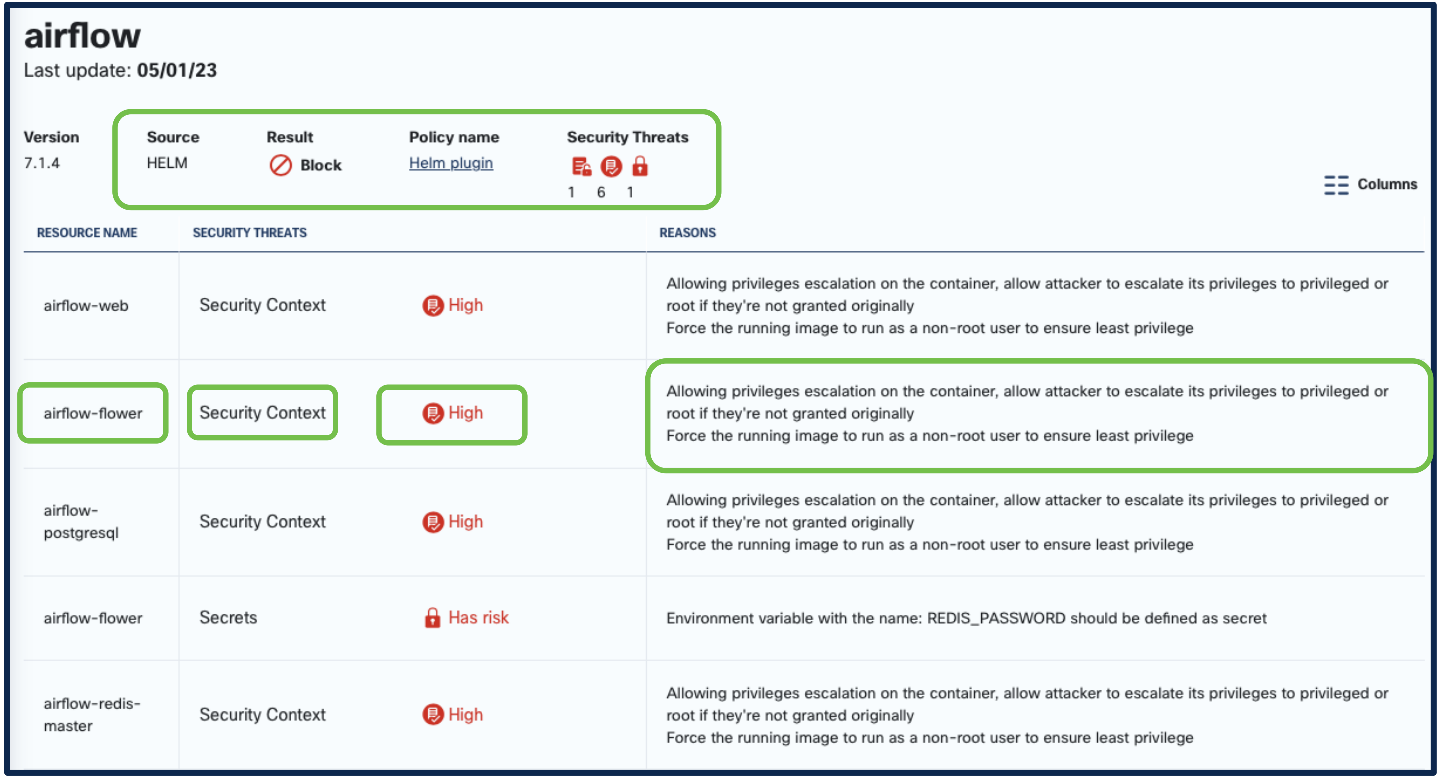


Last week

Deployment name

DEPLOYMENT NAME	DEPLOYMENT SOURCE	TIME ▲	RESULT	SECURITY FINDING
mongoDB	HELM	12:59:16 PM Jan 5th, 2023	⚠ Detect	Total: 1 0 1 0
airflow	HELM	12:59:16 PM Jan 5th, 2023	⊘ Block	Total: 8 1 6 1

Continuous Deployment Policy Enforcement



airflow

Last update: **05/01/23**

Version	Source	Result	Policy name	Security Threats
7.1.4	HELM	⊘ **Block**	Helm plugin	1 6 🔒 1

RESOURCE NAME	SECURITY THREATS		REASONS
airflow-web	Security Context	High	Allowing privileges escalation on the container, allow attacker to escalate its privileges to privileged or root if they're not granted originally Force the running image to run as a non-root user to ensure least privilege
airflow-flower	Security Context	High	Allowing privileges escalation on the container, allow attacker to escalate its privileges to privileged or root if they're not granted originally Force the running image to run as a non-root user to ensure least privilege
airflow-postgresql	Security Context	High	Allowing privileges escalation on the container, allow attacker to escalate its privileges to privileged or root if they're not granted originally Force the running image to run as a non-root user to ensure least privilege
airflow-flower	Secrets	🔒 Has risk	Environment variable with the name: REDIS_PASSWORD should be defined as secret
airflow-redis-master	Security Context	High	Allowing privileges escalation on the container, allow attacker to escalate its privileges to privileged or root if they're not granted originally Force the running image to run as a non-root user to ensure least privilege

Demo

Q&A

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

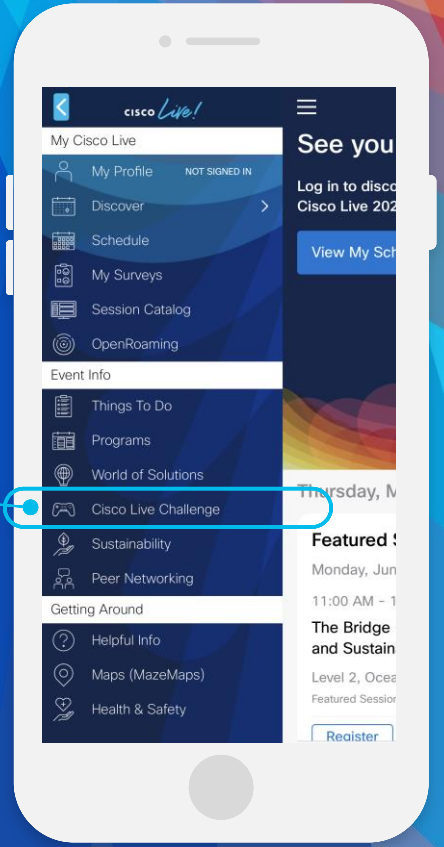
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

Let's go

#CiscoLive