



KubeCon



CloudNativeCon

Europe 2026

#KubeCon #CloudNativeCon

Hack Me If You Can: Learning Kubernetes Security Through a Role-Play Battle

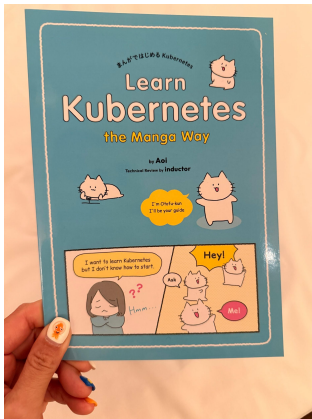
Aoi Takahashi, Recruit Co., Ltd.

Keita Mochizuki, NTT DATA Japan Corporation



Aoi Takahashi

- Aoi Takahashi
- Site Reliability Engineer at Recruit Co., Ltd.
- Translate Kubernetes docs to Japanese
- I live with two Dogs(Golden Retriever) 🐶
- Love writing Manga
- GitHub: github.com/aoi1
- LinkedIn



Keita Mochizuki

- 🏢 NTT DATA Japan Corporation
 - Platform development, technical research and offerings
- 📖 Author of Japanese book about Container Security
 - Learning Kubernetes Security from risks
 - Manage Kubernetes Secret using HashiCorp Vault
- 🧑 Contribution
 - kubernetes / kubernetes-sig member
- 🌐 SNS



🚨 a fox, not a raccoon dog 🚨

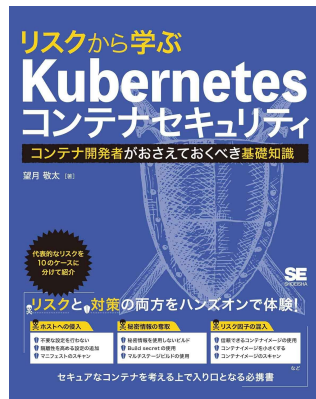


KubeCon



CloudNativeCon

Europe 2026



The Target of This Session



KubeCon



CloudNativeCon

Europe 2026

- People who know the basics of Kubernetes
 - We will not explain what a Pod is, what a Service is, etc
- People who use Kubernetes as a Platform
 - Build the application container image and deploy it as a Pod in Kubernetes
- Beginners in Kubernetes and container security
 - We will explain the fundamentals of Kubernetes/container security

Table of Contents



KubeCon



CloudNativeCon

Europe 2026

Chapter 1. Let's try developing with AI

Chapter 2. The Day an AI-Powered Hacker Attacked

Chapter 3. The Hero arrives...how to secure

Characters

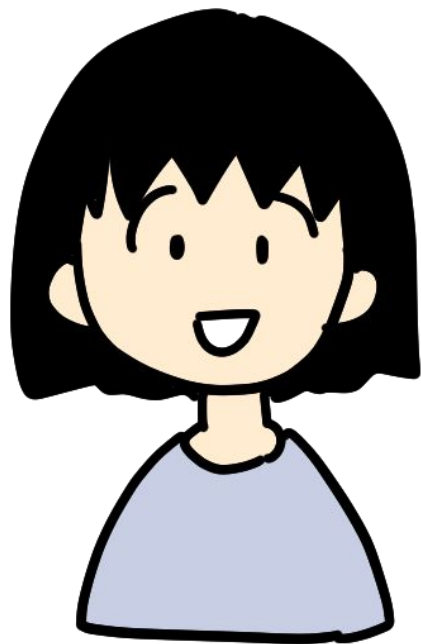


KubeCon



CloudNativeCon

Europe 2026



Engineer

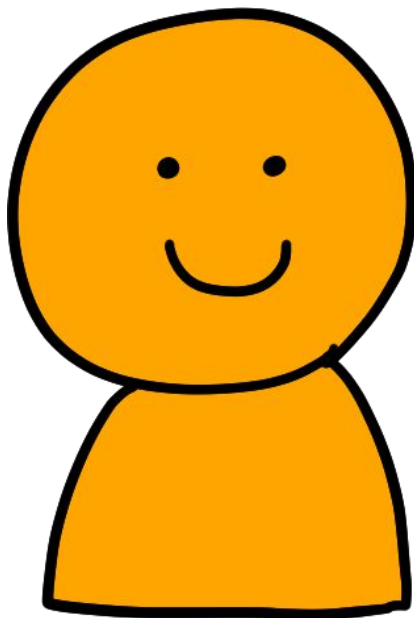


Hacker



Hero

And...



You!

Disclaimer



KubeCon



CloudNativeCon

Europe 2026

- Do not attempt to use AI for malicious attacks
- This AI demonstration is purely illustrative; we have not actually used AI to carry out an attack
- However, we have confirmed that under specific conditions, it is infinitely achievable
- In our presentation, the term AI primarily refers to generative AI

Alright, let's start developing!



KubeCon



CloudNativeCon

Europe 2026

I'm going to build an
e-commerce website!

I'll start developing
using AI.



Tell your AI Agent what to do

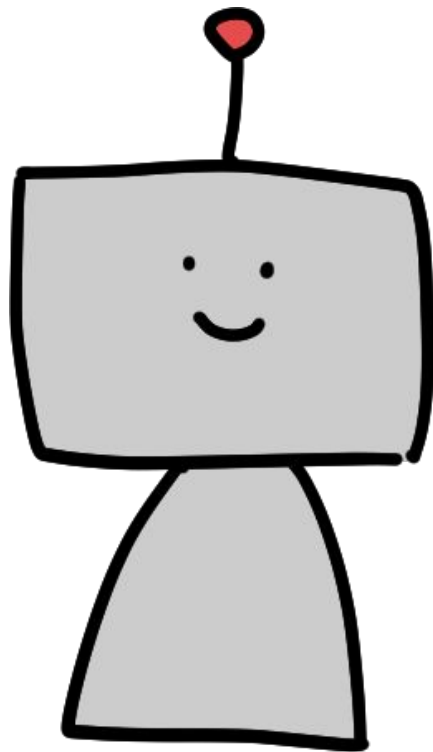
Please create an e-commerce web application called "KubeCon Shopping".

It needs to meet the following functional requirements:

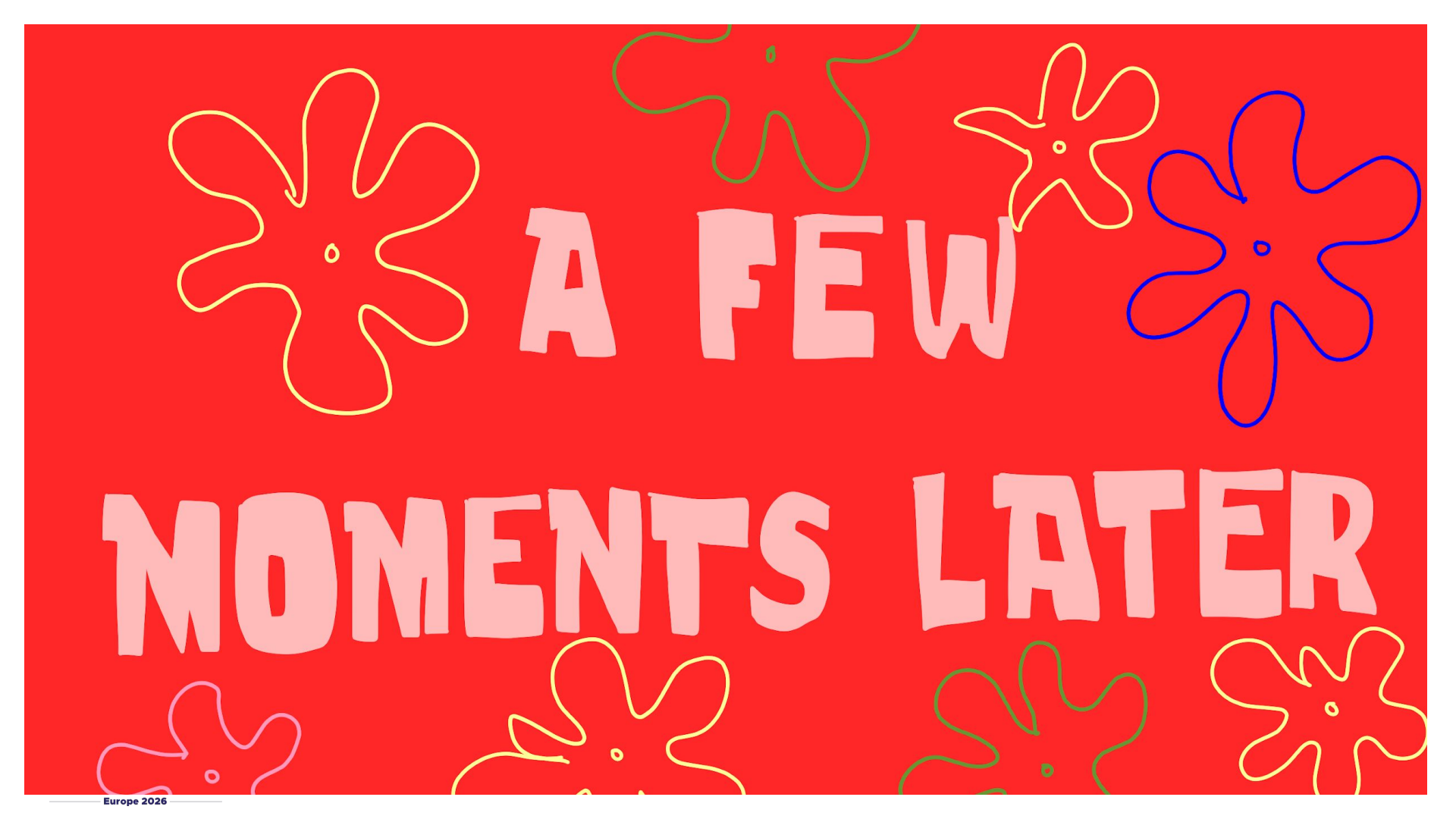
- Display a list of products with images.
- ...

AI, let's GO!





OK!



**A FEW
MOMENTS LATER**

We've made it!

KubeCon Shopping



Featured Products



Super Cool Fox Hoodie

Legendary design with tail attachment. Unleash your inner wild...

\$69.99

[Add to Cart](#)



Kawaii Otofu Comfort T-Shirt

Silky smooth like premium tofu. Ultimate comfort that won't fall apart.

\$49.99

[Add to Cart](#)



Otofu Tofu

Smooth and delicious tofu like silk. Please don't freeze me!

\$10.20

[Add to Cart](#)



Cup Kitsune Udon Noodles

Japanese traditional noodles. Kitsune means fox, not racoon dog.

\$8.05

[Add to Cart](#)



Learning from Risk: Kubernetes Container Security

Essential k8s security guide that every container developer should know in ...

\$21.92

[Add to Cart](#)



Build, Destroy, Repair, and Learn: An Introduction to Kubernetes

A hands-on k8s guide that builds troubleshooting skills with manga...

\$19.21

[Add to Cart](#)



Tofu Power Sticker

Boost your coding speed by 3x! (Individual results may vary)

\$129.99

[Add to Cart](#)



Fox Legend Sticker

Sleek design that commands respect. Elevate your gear with mythical power.

\$129.99

[Add to Cart](#)



Inductor Energy Spark - Carbonated

Electrifying fizzy drink featuring Inductor! Charge up faster ⚡

\$3.25

[Add to Cart](#)



Uwubernetes Cushion

Uwubernetes inspired! So comfy it'll make your pods jealous. uwu

\$1.30

[Add to Cart](#)



KubeCon



CloudNativeCon

Europe 2026

feat: initial implementation of e-commerce site for KubeCon EU 2026

✓ Ready to merge

Code ▾

#1 

 Open [aoi1](#) wants to merge 1 commit into [main](#) from [pr-1](#) 

 Conversation 0

 Commits 1

 Checks 0

 Files changed 16

+2,934 



[a101](#) commented [11 hours ago](#) · edited ▾

...

Summary

- Initial frontend implementation of an e-commerce site built with Next.js + TypeScript
- Product lineup themed around KubeCon EU 2026 (Audio, Wearables, Smart Home, etc.)
- Product listing page with category filter and product detail page
- Responsive Navbar, Footer, and Hero section

Changes

- `app/page.tsx` — Home page (Hero + product grid + category filter)
- `app/products/[id]/page.tsx` — Product detail page (images, ratings, related products)
- `components/product/` — ProductCard, ProductGrid, RatingStars, ProductBadge
- `components/layout/` — Navbar, Footer
- `lib/products.ts` — Product data and filtering utilities
- `types/product.ts` — Product / ProductCategory type definitions

Reviewers



No reviews

Still in progress? [Convert to draft](#)

Assignees



No one—[assign yourself](#)

Labels



None yet

Projects



None yet

Milestone



No milestone



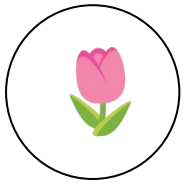
KubeCon



CloudNativeCon

Europe 2026

Approved!



kubeconeuaudience approved

Merged!



Pull request successfully merged and closed

You're all set — the branch has been merged.



KubeCon



CloudNativeCon

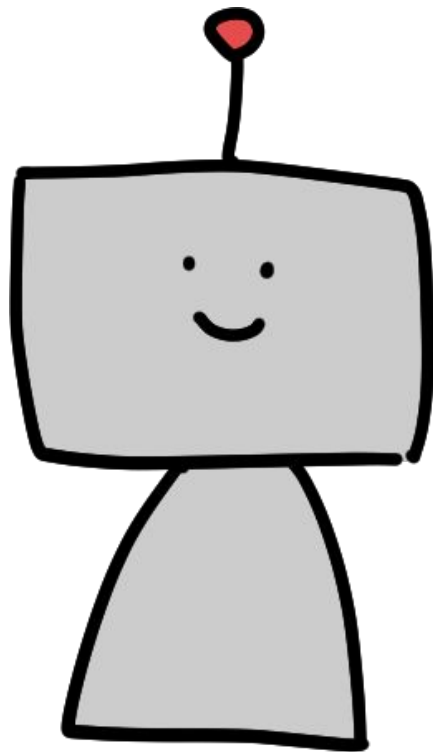
Europe 2026

Next...

Please build the container image for this web application. Once the build is complete, please push it to the container registry.

Let's create a container image and push it!



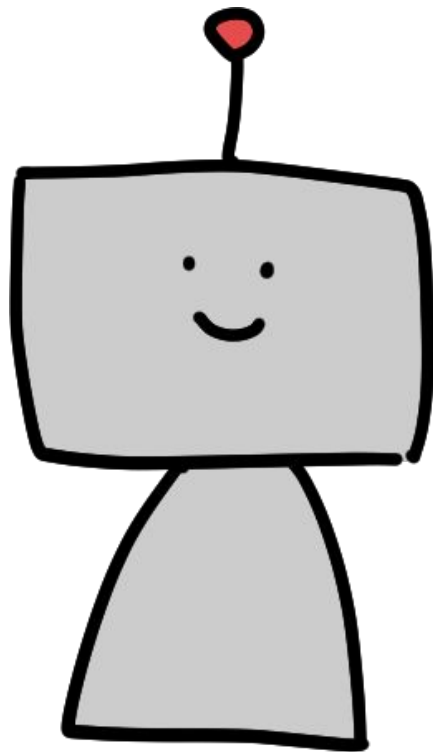


OK!

Please deploy a Pod to Kubernetes using a web application container image, and make it accessible from the internet.

Next, create
Kubernetes manifest to
deploy it!





OK!

Dockerfile

```
FROM node:24

WORKDIR /app

# Install dependencies
COPY package.json package-lock.json ./
RUN npm ci

# Copy necessary files for build
COPY next.config.js tsconfig.json ./
COPY next-env.d.ts postcss.config.js tailwind.config.js ./
COPY app ./app
COPY components ./components
COPY lib ./lib
COPY public ./public

# Build the application
RUN npm run build

# Expose port
EXPOSE 3000

# Start the application
CMD ["npm", "start"]
```

Manifest

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: kubecon-shopping
spec:
  replicas: 1
  selector:
    matchLabels:
      app: kubecon-shopping
  template:
    metadata:
      labels:
        app: kubecon-shopping
    spec:
      hostPID: true
      containers:
        - name: kubecon-shopping
          securityContext:
            privileged: true
          image: registry/kubecon-shopping:v1.0
          ports:
            - containerPort: 3000
```

```
apiVersion: v1
kind: Service
metadata:
  name: kubecon-shopping
spec:
  type: LoadBalancer
  selector:
    app: kubecon-shopping
  ports:
    - protocol: TCP
      port: 80
      targetPort: 3000
  loadBalancerIP: 192.168.2.128
```



Merged!



Pull request successfully merged and closed

You're all set — the branch has been merged.



KubeCon



CloudNativeCon

Europe 2026

Production Deployed!

KubeCon Shopping



Featured Products



Super Cool Fox Hoodie

Legendary design with tail attachment. Unleash your inner wild...

\$69.99

Add to Cart



Kawaii Otofu Comfort T-Shirt

Silky smooth like premium tofu. Ultimate comfort that won't fall apart.

\$49.99

Add to Cart



Otofu Tofu

Smooth and delicious tofu like silk. Please don't freeze me!

\$10.20

Add to Cart



Cup Kitsune Udon Noodles

Japanese traditional noodles. Kitsune means fox, not racoon dog.

\$8.05

Add to Cart



Learning from Risk: Kubernetes Container Security

Essential k8s security guide that every container developer should know in ...

\$21.92

Add to Cart



Build, Destroy, Repair, and Learn: An Introduction to Kubernetes

A hands-on k8s guide that builds troubleshooting skills with manga...

\$19.21

Add to Cart



Tofu Power Sticker

Boost your coding speed by 3x!
(Individual results may vary)

\$129.99

Add to Cart



Fox Legend Sticker

Sleek design that commands respect.
Elevate your gear with mythical power.

\$129.99

Add to Cart



Inductor Energy Spark - Carbonated

Electrifying fizzy drink featuring Inductor! Charge up faster ⚡

\$3.25

Add to Cart



Uwubernetes Cushion

Uwubernetes inspired! So comfy it'll make your pods jealous. uwu

\$1.30

Add to Cart



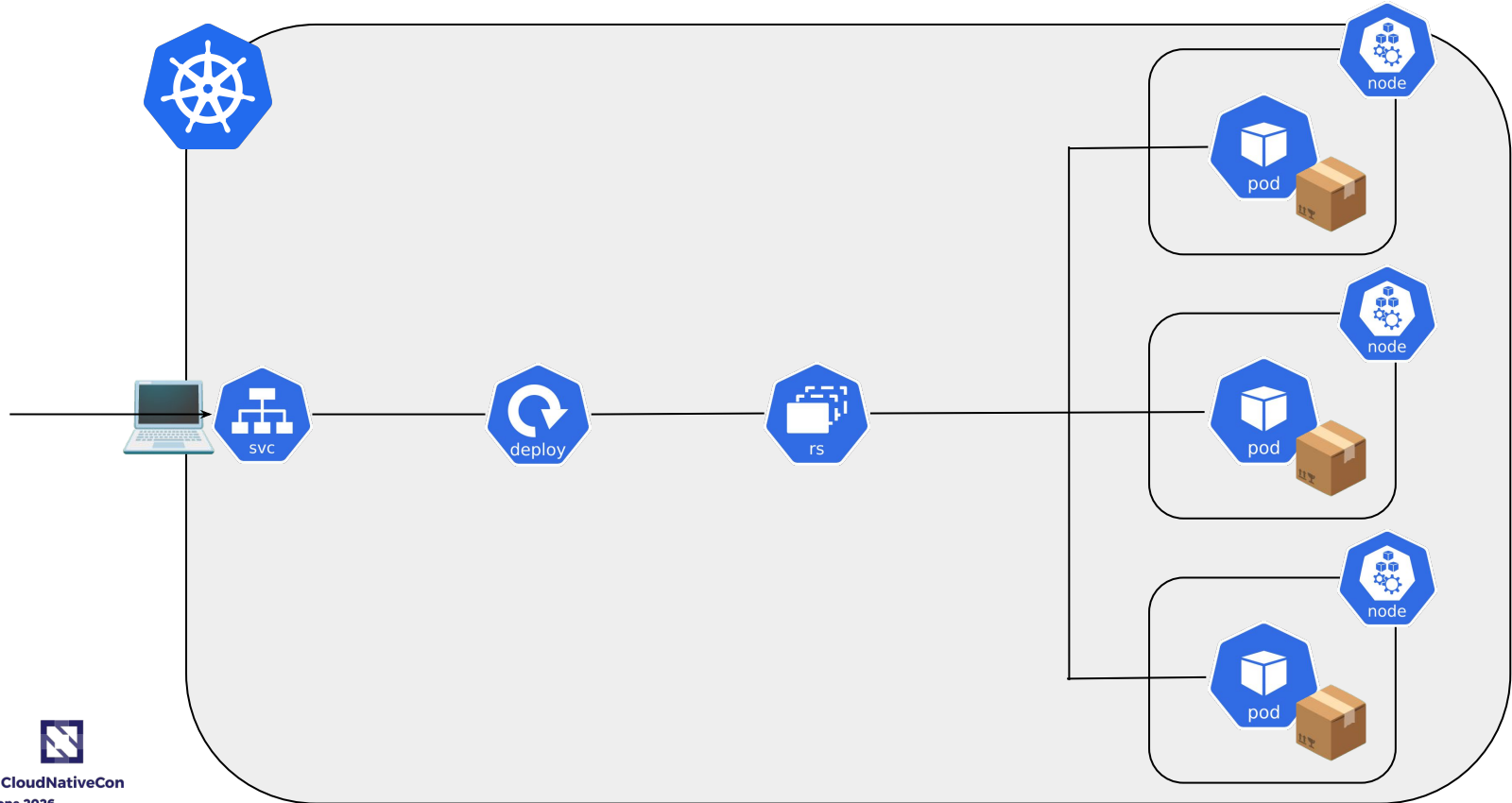
KubeCon



CloudNativeCon

Europe 2026

Architecture



KubeCon



CloudNativeCon

Europe 2026

My Job is done!



One Day...



KubeCon



CloudNativeCon

Europe 2026

Hello, I'm a hacker.
I am thinking what
shall I attack today!



Investigating a new website...



I've found a new website!
Let's check it out.

Reconnaissance

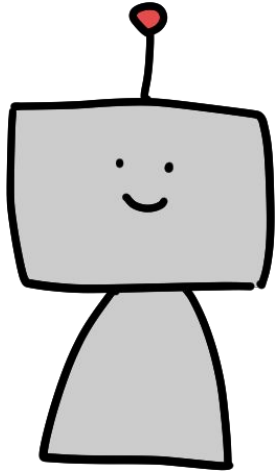
Please visit <http://kubekonshopping.com> to find out what kind of web service it is.

Next, determine what programming languages and frameworks were used to build this web service.

Ask AI to conduct a investigation!



Reconnaissance



This web service appears to be a website offering e-commerce services.

Additionally, the following technologies are utilized in this web service:

- Framework: Next.js
- Library: React

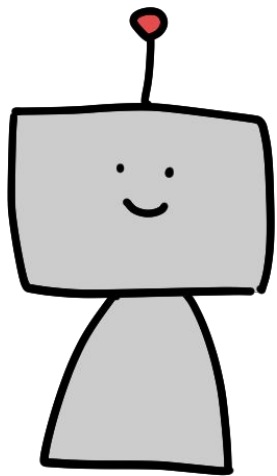
Reconnaissance

Are there any critical vulnerabilities that have recently been discovered in React?

Hmm...
I recall hearing about a vulnerability
related to React a while ago.
There may be a vulnerability...



Reconnaissance



A critical vulnerability, identified as **CVE-2025-55182**, has been discovered in Next.js and React Server Components in 2025.

Vulnerability Type: Remote Code Execution

Affected Components:

React Server Components: 19.0.0, 19.1.0, 19.1.1, 19.2.0

Next.js: Unpatched 15.x and 16.x versions

- CVE (Common Vulnerabilities and Exposures)
 - A globally unique ID assigned to a publicly disclosed security vulnerabilities

CVE-2025-55182 Detail

Description

A pre-authentication remote code execution vulnerability exists in React Server Components versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0 including the following packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. The vulnerable code unsafely deserializes payloads from HTTP requests to Server Function endpoints.

Remote execution of arbitrary commands would be allowed by exploiting this vulnerability.

Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

 NIST: NVD	Base Score: N/A	NV
 CNA: Facebook, Inc.	Base Score: 10.0 CRITICAL	Ve

The score express Vulnerability Severity(0.0 - 10.0)
The score of 10 means most urgent



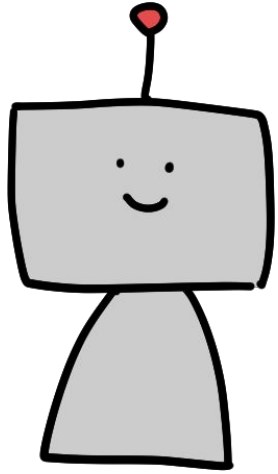
Reconnaissance

Please investigate whether the web service at <http://kubekonshopping.com> may contain the CVE-2025-55182 vulnerability.

Whether this vulnerability exists in this web service?



Reconnaissance



This web service uses Next.js with App Router and has React Server Components enabled. Although we cannot verify the patch status, there's a strong possibility that contains vulnerabilities.

Okay, It's my turn



KubeCon



CloudNativeCon

Europe 2026

PARTY TIME!!!



Creating tools is a breeze if you rely on AI! 🎵

Please create a tool to achieve Remote Code Execution on a web service by exploiting CVE-2025-55182.

Prepare the tools for attacking.
AI power makes it easier and faster!



Creating tools is a breeze if you rely on AI! 🎵

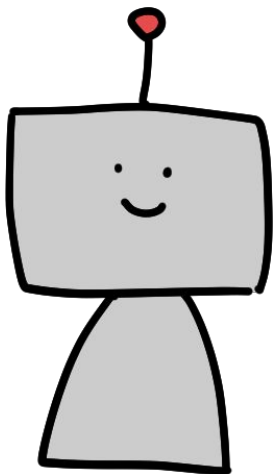
OK, I created a tool using Python to exploit CVE-2025-55182.

Usage:

```
python exploit.py <URL> <COMMAND>
```

Do you want to actually execute the attack?

Please tell me which command you want to execute.



Exploiting

OK, use the exploit tool to execute the "hostname" command remotely.

Let's actually try attacking!
Execute arbitrary command in the
environment where app is running.

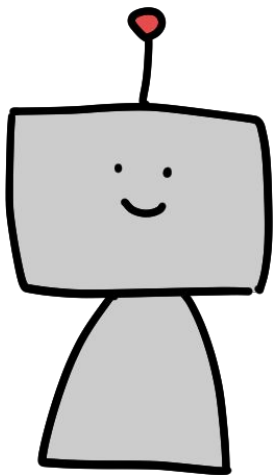


Exploiting

Running python

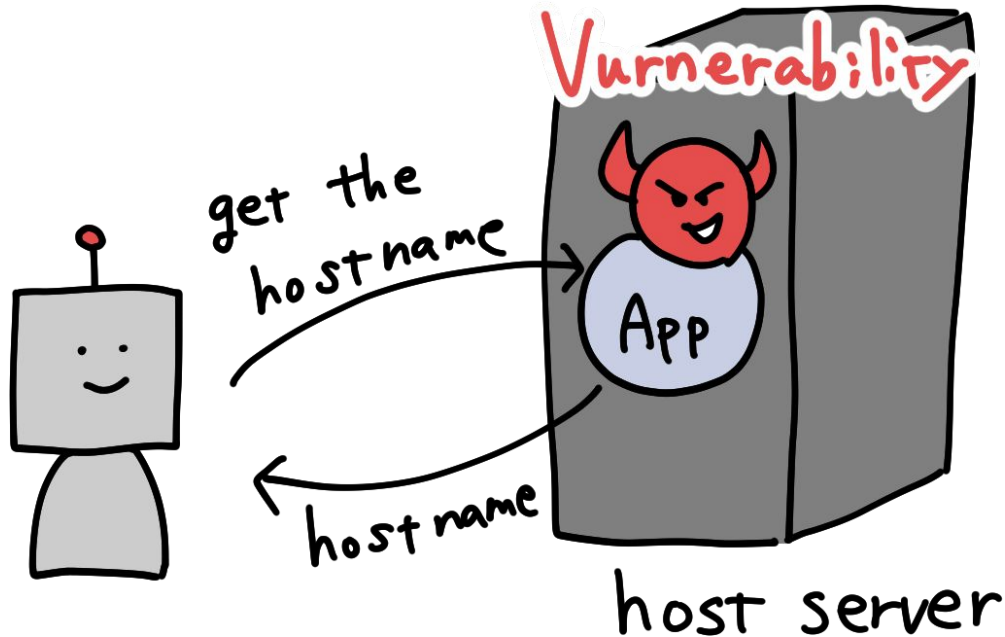
```
python exploit.py http://kubekonshopping.com "hostname"
```

... Done. Hostname is `kubekon-shopping-5f-rz`.



Exploiting

- Application has RCE(Remote Code Execution) Vulnerability
- Arbitrary commands can be executed remotely



KubeCon



CloudNativeCon

Europe 2026

Exploiting

Please investigate the hosting environment of this web service and identify any vulnerabilities.

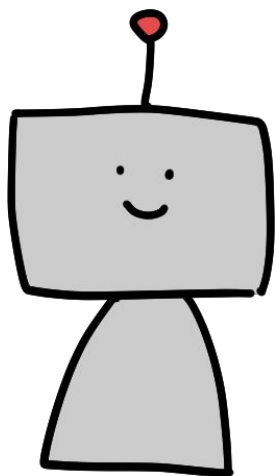
Investigate further!
In what environment is this application?
Are there any other vulnerabilities?



Exploiting

Starting investigation using exploit.py... Done.

- It's highly likely this is **running as a Pod in a Kubernetes** environment, given the presence of environment variables and mounted service accounts.
- It's running as a **privileged container**, and the executing user is root.
- Therefore, there's a high probability of being able to access the Node where this Pod is running from within this container.



Exploiting

From the container, execute "shutdown" command on the node.

This app is running as a container(Pod) on Kubernetes with strong privilege. It may be possible to interfere with the Node from container.



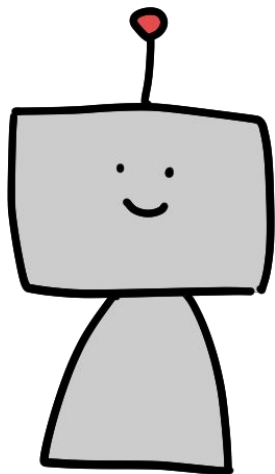
Exploiting

Using `exploit.py`, we will run the following commands inside the container...

```
nsenter -t 1 -a shutdown
```

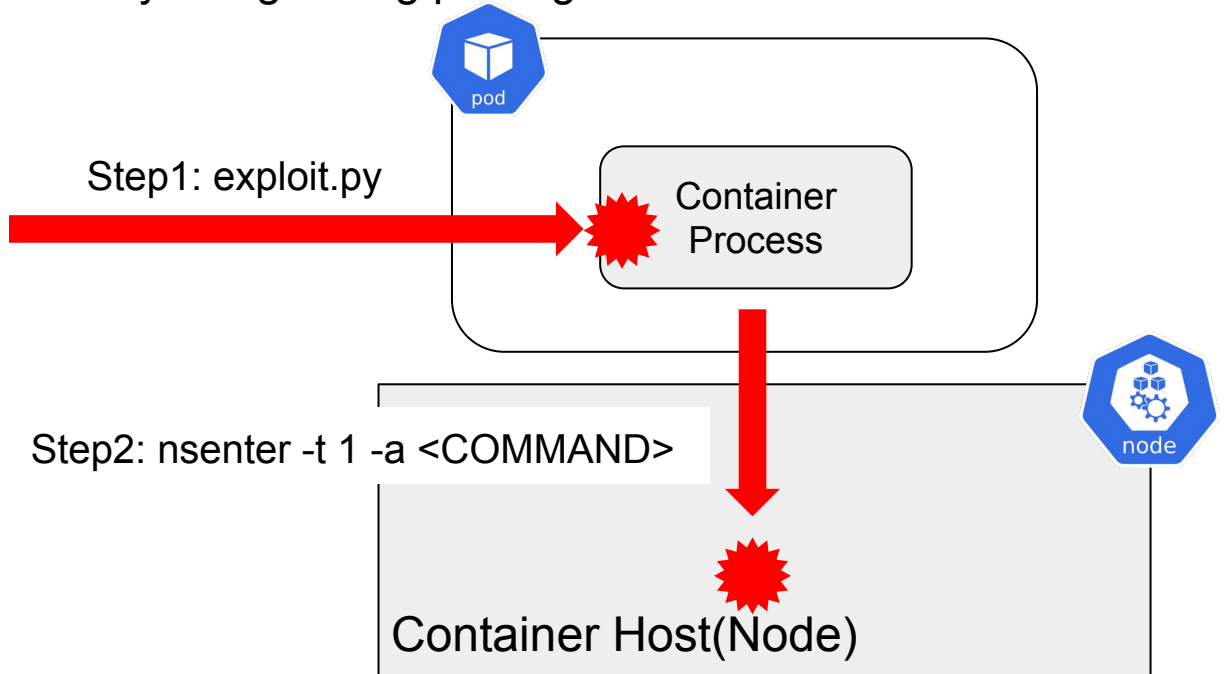
OK, done.

Successfully executed `shutdown` command from container to node. `k8s-cluster-node01` where the pod is running on will be shutdown.



Exploiting

- Arbitrary commands executed
 - Step1: Inside the container by exploiting CVE-2025-55182
 - Step2: On the Node by using strong privileges of container



KubeCon



CloudNativeCon

Europe 2026

What you can do after intrusion



KubeCon



CloudNativeCon

Europe 2026

Finally, the attacker was succeeded to gain the ability to execute arbitrary commands on the Node.

For example:

- Executing sensitive command(e.g. shutdown)
- Steal secret information
- Malicious workload
- Attacking other Pods

やったぜ！！

(We did it!)





Alert ! Someone is Hacking Me!



KubeCon



CloudNativeCon

Europe 2026

HEEEELP!!!



And the Hero arrives!

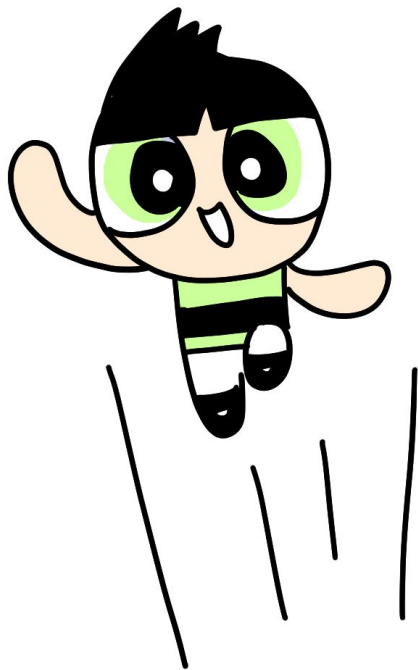


KubeCon



CloudNativeCon

Europe 2026



What the problem was



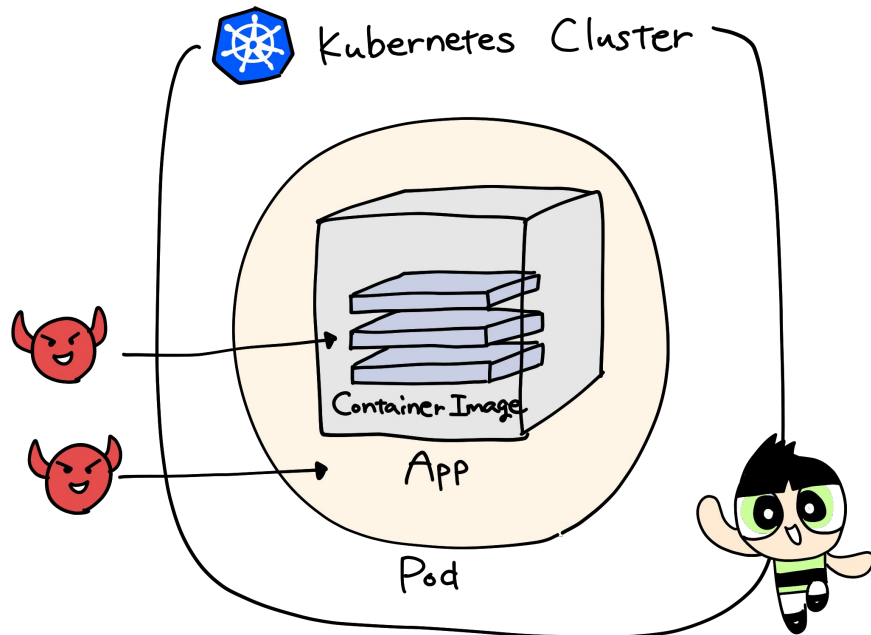
KubeCon



CloudNativeCon

Europe 2026

- The container's security was vulnerable.
 - Container image
 - Container(Configured via k8s manifests)



What went wrong: container images



KubeCon



CloudNativeCon

Europe 2026

- Critical vulnerability was included
 - Arbitrary commands was executed remotely by exploiting CVE-2025-55182
- Many components were included
 - Various operations were performed inside the container
- Application and container image generated by the AI were vulnerable
 - Relatively new vulnerabilities may not be recognized by AI

How to secure

- Detect and remove vulnerabilities
- Keep container images small

How to secure: Detect and remove vulnerabilities

- There are several points where vulnerabilities may exist:
 - Application
 - Packages
 - Base container images

Scanning tools

- Trivy
 - <https://trivy.dev/docs/latest/guide/scanner/vulnerability/>
- Kubescape
 - <https://kubescape.io/>
- Clair
 - <https://clairproject.org/>
- Gype
 - <https://github.com/anchore/gype>

Perform a vulnerability scan

Example of trivy:

```
$ trivy image --severity CRITICAL registry/kubecon-shopping:v1.0
```

```
...
```

```
Node.js (node-pkg)
```

```
Total: 10 (HIGH: 8, CRITICAL: 2)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
...	...	...	...	...	...	...
next (package.json)	CVE-2025-55182	CRITICAL	fixed	15.5.6	15.0.5, 15.1.9, 15.2.6, 15.3.6, 15.4.8, 15.5.7, 16.0.7	next: React Server Components: Pre-authentication remote code execution via unsafe deserialization https://avd.aquasec.com/nvd/cve-2025-55182
...	...	...	...	...	...	...

How to secure: Keep your container images small

- Large container images contain various commands, packages, libraries...
 - They can be exploited for attacks

Dockerfile

FROM node:24

WORKDIR /app

Install dependencies

COPY package.json package-lock.json ./

RUN npm ci

Copy necessary files for build

COPY next.config.js tsconfig.json ./

COPY next.config.js tsconfig.json ./

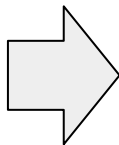
COPY next-env.d.ts postcss.config.js tailwind.config.js ./

COPY app ./app

...

Start the application

CMD ["npm", "start"]

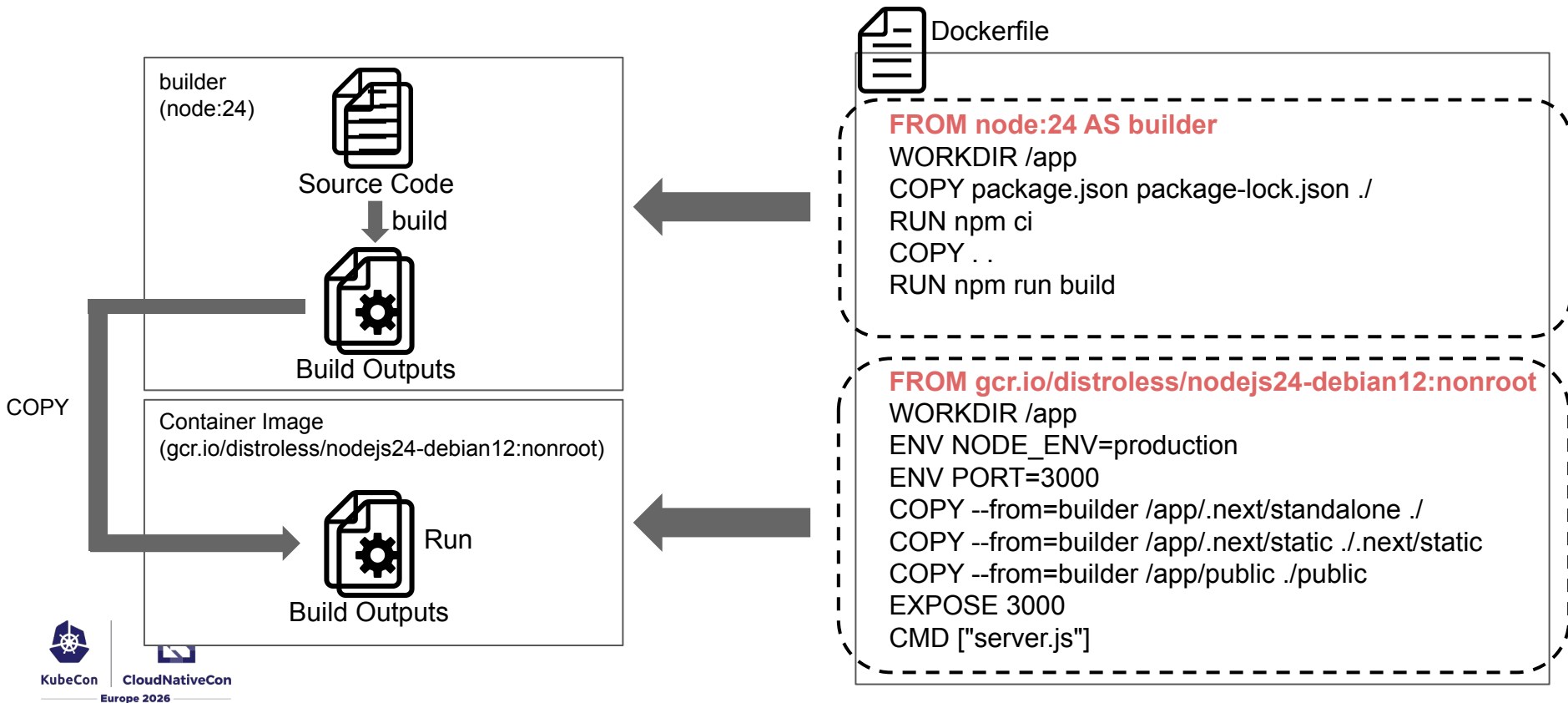


So Large(2.05GB)

\$ docker images

REPOSITORY	TAG	...	SIZE
kubecon-shopping	v1.0	...	2.05GB

Multi-stage build and use minimal image



Advantage of minimal image

- Container image based on distroless is much smaller than the regular image
 - Containing only the minimum components required to run the application

```
$ docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
kubecon-shopping	distroless	58cdb90e9075	17 minutes ago	267MB
kubecon-shopping	v1.0	382f2763279e	51 minutes ago	2.05GB

Advantage of minimal image

- Less components in a container image reduces the attack surface
 - Doesn't even contain shells or debugging utilities

```
$ kubectl exec -it kubecon-shopping-5f4c959b6c-rzcds -- /bin/bash
error: Internal error occurred: Internal error occurred: error executing command in container:
failed to exec in container: failed to start exec
"0299cc787547a8306a2c825e534a7221601407e130eaf4516637897b32041571": OCI
runtime exec failed: exec failed: unable to start container process: exec: "/bin/bash": stat
/bin/bash: no such file or directory
```

The power of kubectl debug

- Minimized container images make debugging difficult
- "kubectl debug" command is useful for debugging

```
$ kubectl debug -it kubecon-shopping-5f4c959b6c-rzcds --image=ubuntu:24.04  
--target=kubecon-shopping --profile general -- /bin/bash
```

```
root@kubecon-shopping-5f4c959b6c-rzcds:/# ps aux
```

USER	PID	...	COMMAND
------	-----	-----	---------

65532	1	...	next-server (v15.5.6)
-------	---	-----	-----------------------

container process

root	46	...	/bin/bash
------	----	-----	-----------

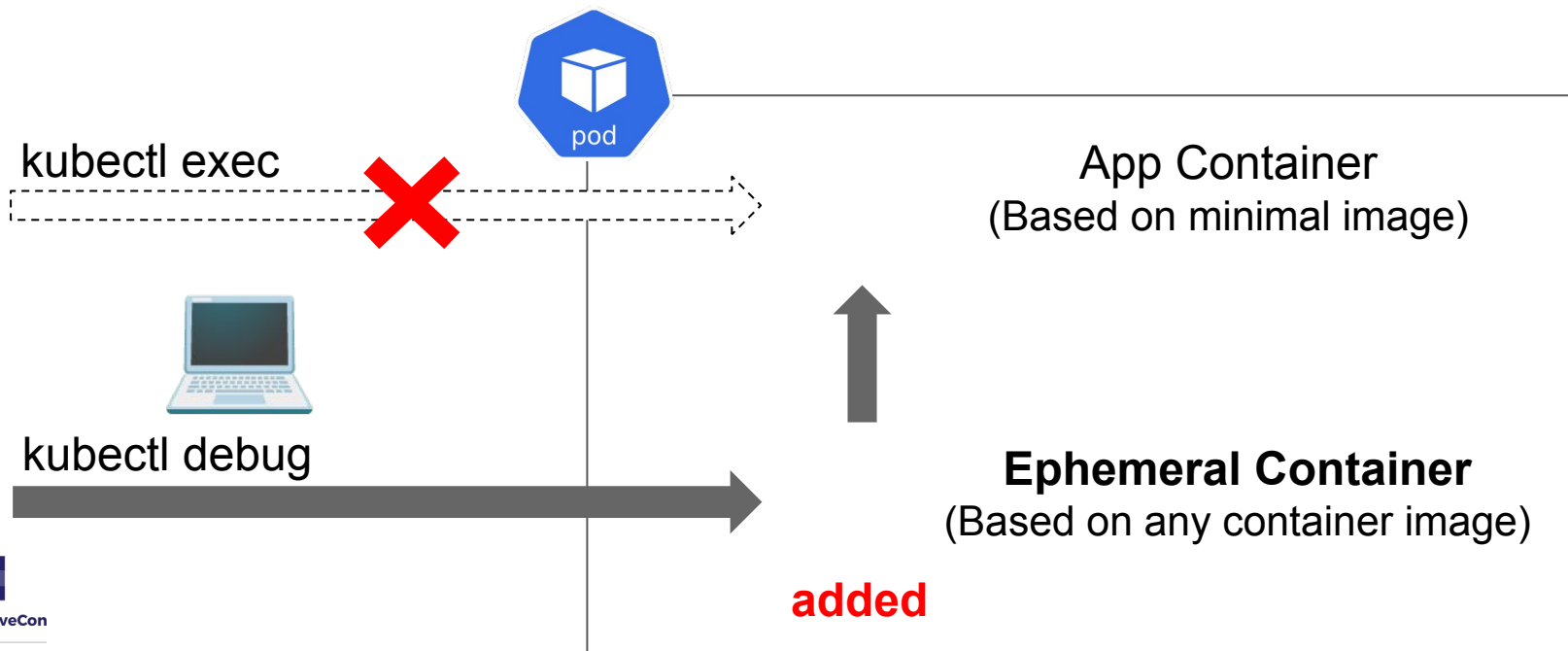
root	67	...	ps aux
------	----	-----	--------

```
root@kubecon-shopping-5f4c959b6c-rzcds:/# ls /proc/1/root/app  
node_modules package.json public server.js
```

container filesystem

The power of kubectl debug

- Ephemeral Container for debugging is added into the Pod
- Debug the application container via Ephemeral Container



What went wrong: Container



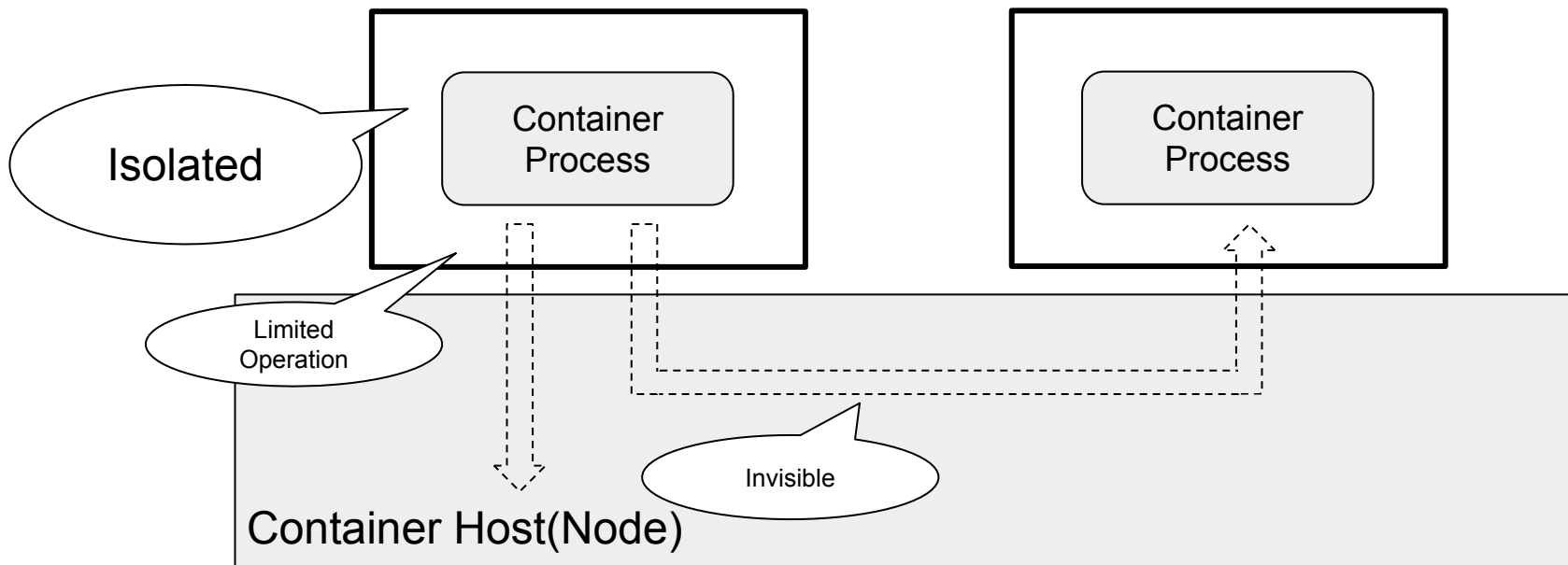
KubeCon



CloudNativeCon

Europe 2026

- Container is an isolated process on Linux
- Operations from container to host are limited



What went wrong: Container



KubeCon



CloudNativeCon

Europe 2026

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: kubecon-shopping
spec:
  replicas: 1
  ...
  spec:
    hostPID: true
    containers:
      - name: kubecon-shopping
        securityContext:
          privileged: true
        image: registry/kubecon-shopping:v1.0
    ...
```

What went wrong: Container



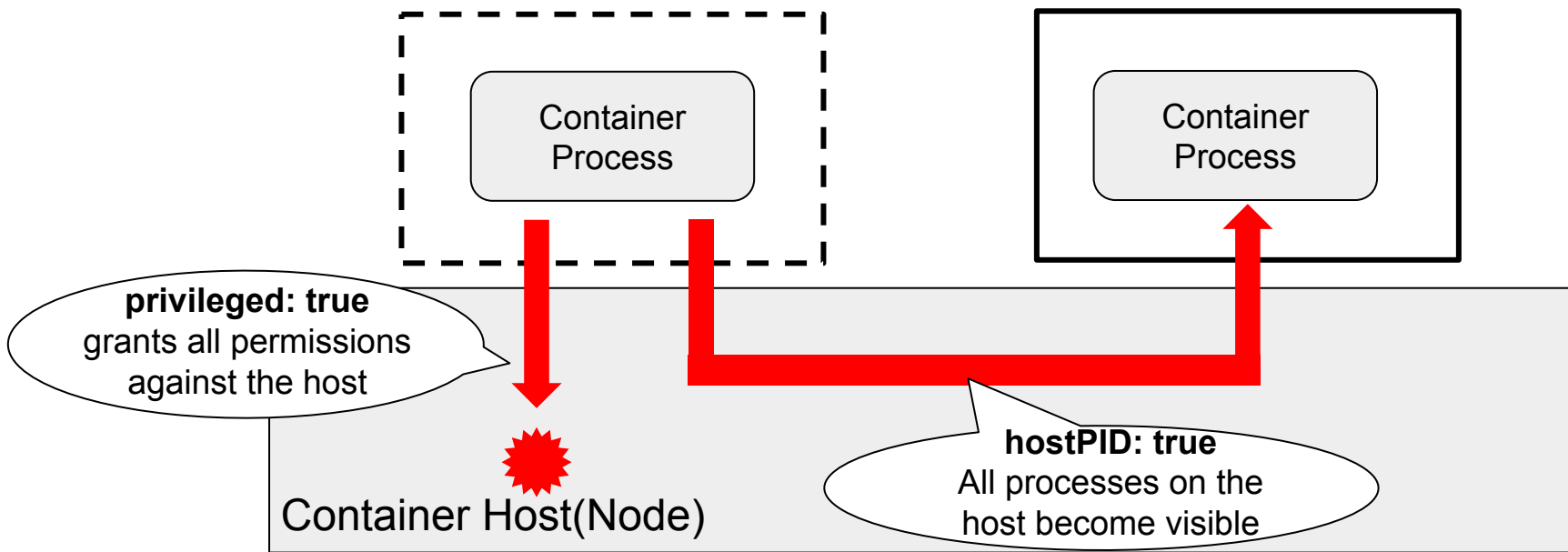
KubeCon



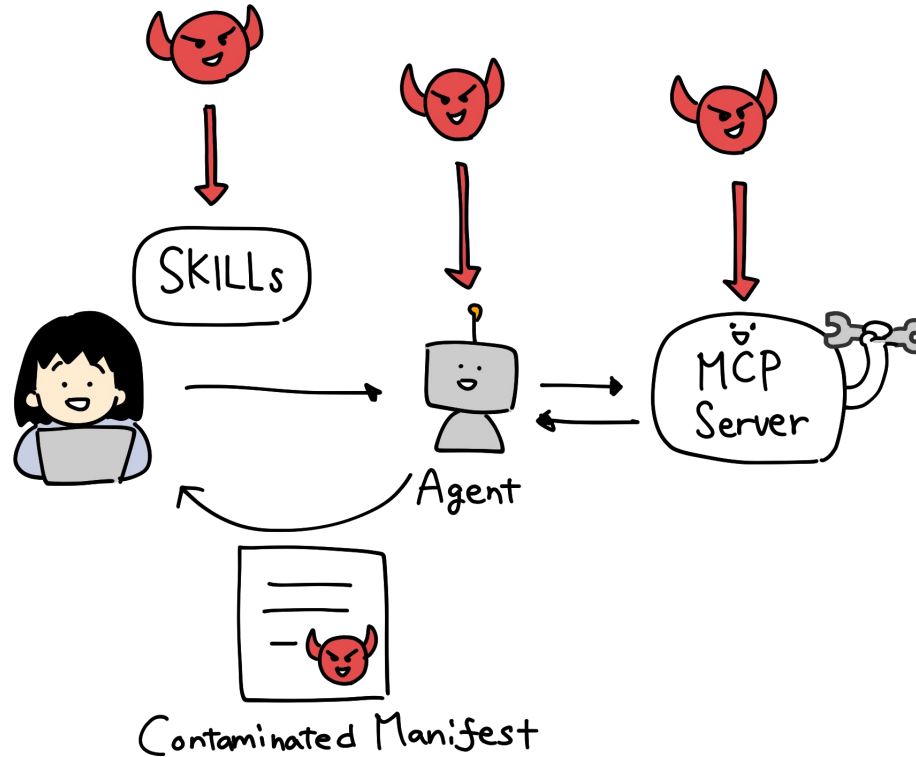
CloudNativeCon

Europe 2026

- Container was not sufficiently isolated
 - Vulnerable configurations were included in Kubernetes manifest



Where can malicious prompts be embedded?



Contaminated Manifest

The OWASP Top 10 for Agentic Applications for 2026

<https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/>



KubeCon



CloudNativeCon

Europe 2026

How to secure

- What configurations make your Pods more secure or insecure

Pod Security Standards

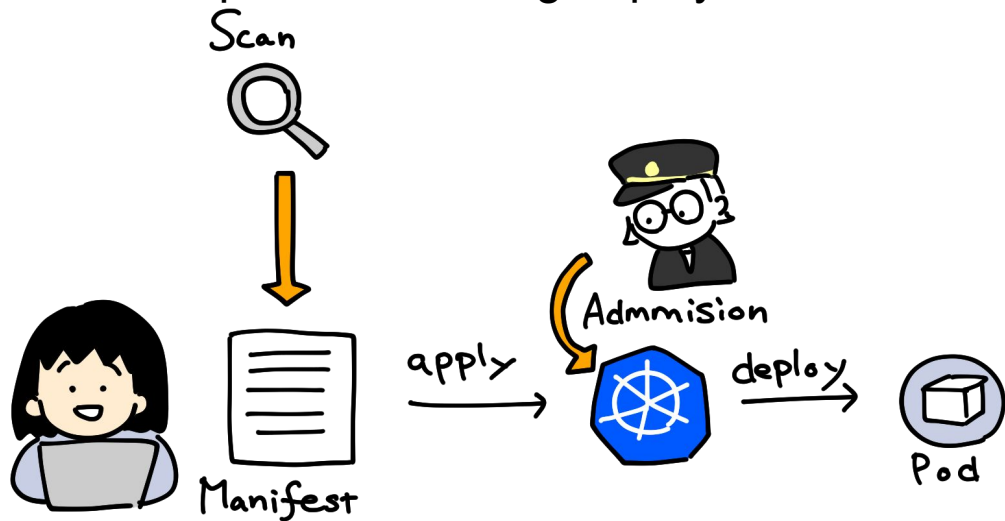
A detailed look at the different policy levels defined in the Pod Security Standards.

The Pod Security Standards define three different *policies* to broadly cover the security spectrum. These policies are *cumulative* and range from highly-permissive to highly-restrictive. This guide outlines the requirements of each policy.

Profile	Description
Privileged	Unrestricted policy, providing the widest possible level of permissions. This policy allows for known privilege escalations.
Baseline	Minimally restrictive policy which prevents known privilege escalations. Allows the default (minimally specified) Pod configuration.
Restricted	Heavily restricted policy, following current Pod hardening best practices.

How to secure

- Scanning Kubernetes manifests
 - Detect vulnerable setting
- Policy-based admission control
 - Prevent vulnerable pods from being deployed



How to secure: Scanning Kubernetes manifests

- Trivy
 - <https://trivy.dev/docs/latest/guide/scanner/misconfiguration/>
- Kubescape
 - <https://kubescape.io/>
- KubeLint
 - <https://docs.kubelinter.io/>
- Checkov
 - <https://www.checkov.io/>

How to secure: Scanning Kubernetes manifests

Example of trivy:

```
$ trivy config --severity CRITICAL,HIGH kubernetes/deployment.yaml
```

```
Tests: 22 (SUCCESSSES: 18, FAILURES: 4)
```

```
Failures: 4 (HIGH: 4, CRITICAL: 0)
```

```
...
```

```
KSV-0017 (HIGH): Container 'kubecon-shopping' of Deployment 'kubecon-shopping' should set 'securityContext.privileged' to false
```

```
Privileged containers share namespaces with the host system and do not offer any security. They should be used exclusively for system containers that require high privileges.
```

```
See https://avd.aquasec.com/misconfig/ksv-0017
```

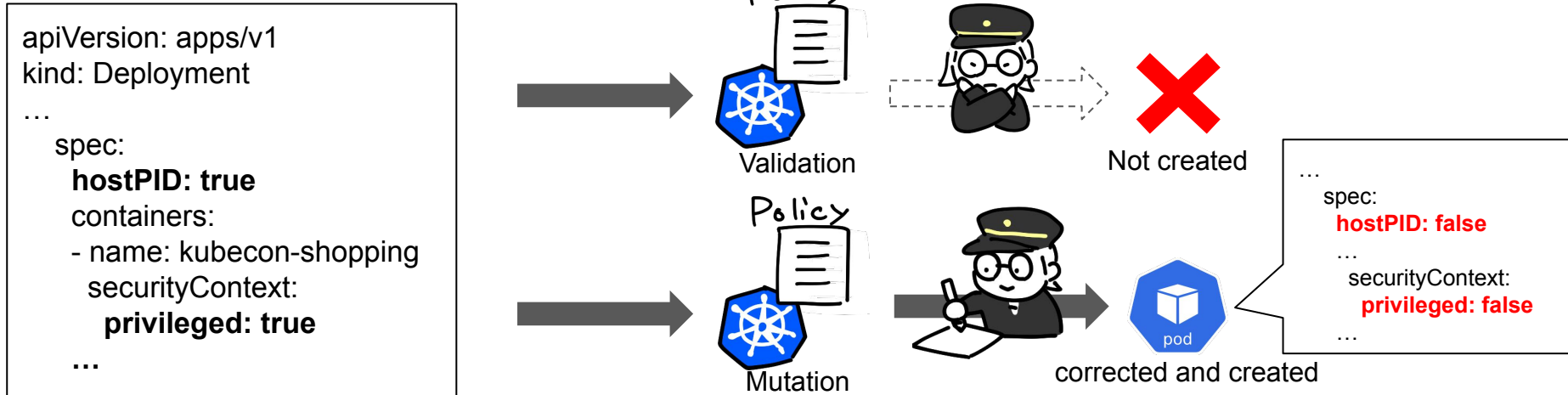
```
deployment.yaml:17-23
```

```
17 |         - name: kubecon-shopping
18 |           securityContext:
19 |             privileged: true
...

```

How to secure: Policy-based admission control

- Admission Control is the mechanism to intercept requests to Kubernetes
- Policy-based admission control prevents the creation of non-compliant resources according to predefined policies
 - Validation: Prohibit non-compliant settings
 - Mutation: Override non-compliant settings



How to secure: Policy-based admission control

- Kubernetes Native
 - Pod Security Admission (+v1.25 Stable)
 - <https://kubernetes.io/docs/concepts/security/pod-security-admission/>
 - Validating Admission Policy (+v1.30 Stable)
 - <https://kubernetes.io/docs/reference/access-authn-authz/validating-admission-policy/>
 - Mutating Admission Policy (+v1.34 Beta)
- 3rd-party
 - Kyverno
 - <https://kyverno.io/>
 - OPA Gatekeeper
 - <https://open-policy-agent.github.io/gatekeeper/website/>

Other security measures

- RBAC(Role Based Access Control)
 - The method of granting permissions to Kubernetes resources based on the role
 - Minimizing permissions help to mitigate the impact of attacks
- Network Policy
 - The method of controlling traffic flow within Kubernetes Cluster
 - Block unauthorized communication between Pods

Reference:

- Kubernetes Security Checklist
 - <https://kubernetes.io/docs/concepts/security/security-checklist>

AI-powered defenses



KubeCon



CloudNativeCon

Europe 2026

- Various security measures utilizing AI:
 - Detect insecure settings and fix
 - Generate Policies
 - Detect and analyze suspicious behavior
 - Security Alert Triage

etc...

Detect vulnerabilities and fix empowered by AI



KubeCon



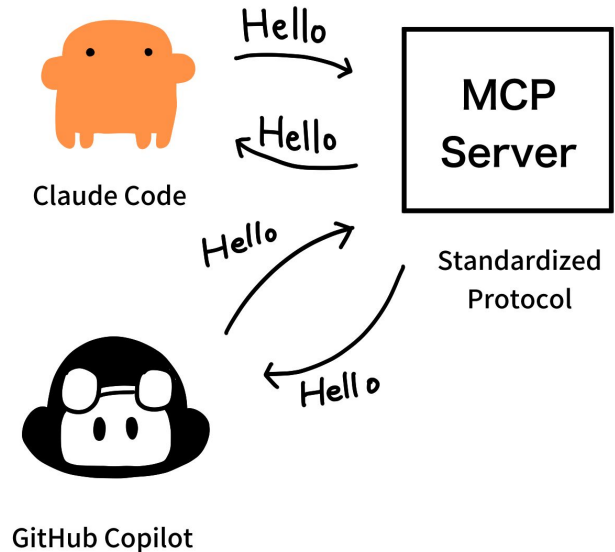
CloudNativeCon

Europe 2026

- Detect
 - AI automatically run the scanning tools
 - Interpret the results
- Fix
 - Use detection results as context
 - Fix vulnerabilities

Model Context Protocol(MCP) Server

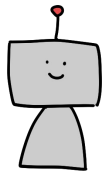
- Extend AI Agent capabilities by providing tools
- Execute tools implemented on MCP servers
 - Actually perform the actions
- Use the results as a context
 - Understand the situation more accurately



ref. <https://modelcontextprotocol.io/docs/getting-started/intro>

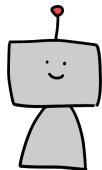
Security Scanner MCP Server

- OSS
 - Trivy MCP Server(Aqua Security)
 - <https://github.com/aquasecurity/trivy-mcp>
 - Kyverno MCP Server(Nirmata)
 - <https://github.com/nirmata/kyverno-mcp>
- Proprietary Software
 - Sysdig MCP Server (Sysdig)
 - <https://github.com/sysdiglabs/sysdig-mcp-server>
 - Snyk MCP
 - <https://github.com/snyk/studio-mcp>

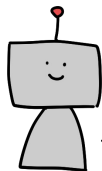


OK! I'll start checking...

Please check my Container image
and Kubernetes manifests.



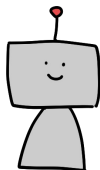
Scan your container image, Dockerfile
and manifests **using trivy via MCP
Server.**



1. Container Image
🚨 CVE-2025-55182 - Next.js Vulnerability
2. Dockerfile
⚠️ Non-root user should be specified
3. Kubernetes Manifests
🚨 privileged should be set false
⚠️ hostPID should be set false

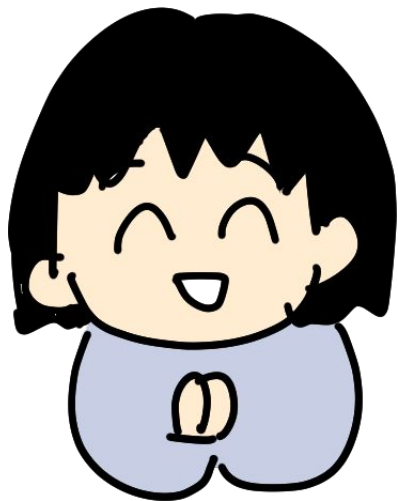
Shall I fix them?

Yes please 😊



Fixing... OK, I've done!!

VICTORY



Wrap up



KubeCon



CloudNativeCon

Europe 2026

- Understand the factors that contribute to the security of containers, and don't blindly trust AI
 - Container Image
 - Remove vulnerabilities and keep container images small
 - Container
 - Keep the isolation of containers
- Leveraging AI to enhance container security
 - One of the effective methods is MCP servers
 - Perform the actions and understand the situation accurately



KubeCon



CloudNativeCon

Europe 2026

