



**carakube**

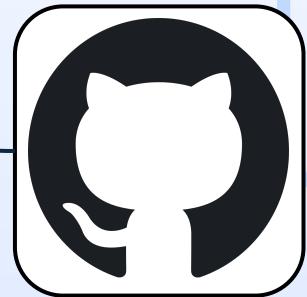




carakube



Kubernetes Cluster



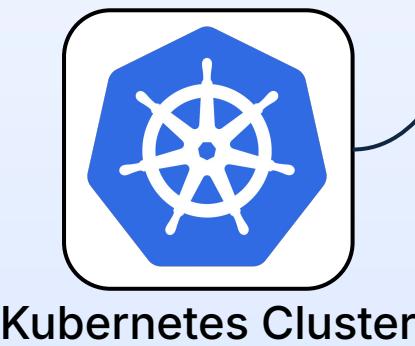
GitHub

GitOps via Flux

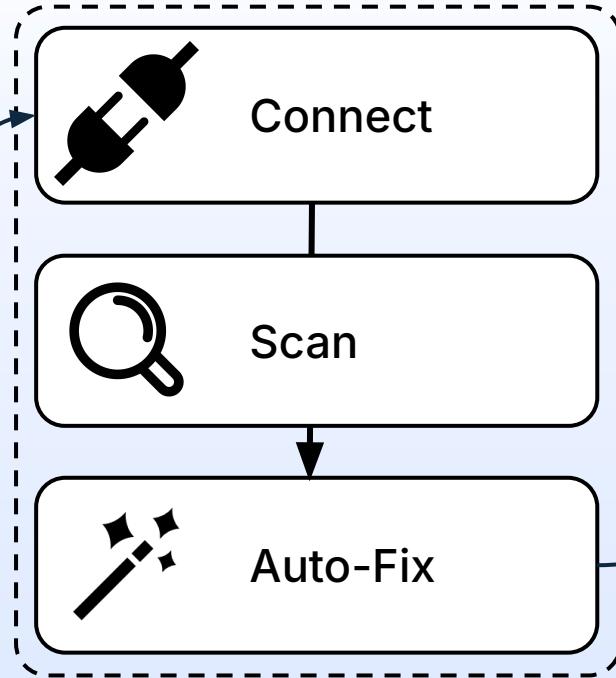




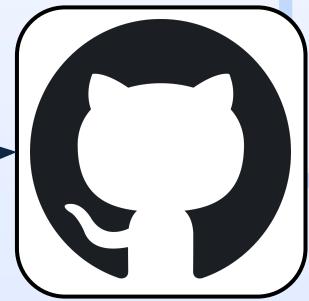
carakube



Kubernetes Cluster



GitOps via Flux



GitHub



carakube

# Demo Time!



hackatum-k8s-flux/clusters/car

github.com/SamuelLess/hackatum-k8s-flux/tree/main/clusters/carakube-demo/apps/hello-8010

SamuelLess / hackatum-k8s-flux

Type ⌘ to search

Code Issues Pull requests 9 Actions Projects Wiki Security Insights Settings

Files

main Add file ...

Go to file

.github

clusters/carakube-demo

apps/hello-8010

- deployment-hostport.yaml
- kustomization.yaml
- service-nodeport.yaml

flux-system

- hello-8010-kustomization.yaml
- podinfo-kustomization.yaml
- podinfo-source.yaml

hackatum-k8s-flux / clusters / carakube-demo / apps / hello-8010 /

Add file ...

Carakube Bot Auto-fix: Resolve vuln-e60423e2f7d9e042 0a33927 · 15 minutes ago History

Name	Last commit message	Last commit date
..		
deployment-hostport.yaml	Auto-fix: Resolve vuln-e60423e2f7d9e042	15 minutes ago
kustomization.yaml	hello-8010: dedupe Service; fix kustomization resources	14 hours ago
service-nodeport.yaml	hello-8010: expose via NodePort 30010	14 hours ago



carakube

Reset Layout

The carakube interface displays a cluster diagram with various namespaces, services, and pods. A sidebar on the left contains icons for adding, deleting, and filtering resources. On the right, there are four warning boxes:

- High RBAC**  
Role: Local-Path-Provisioner-Role  
Dangerous ClusterRole: local-path-provisioner-role  
[Create PR](#)
- High Resource Limits**  
Container: Http-Echo  
Container missing resource limits: cpu, memory  
[Create PR](#)
- High Container Security**  
Container: Podinfod  
Container allowed to run as root (UID 0)  
[Create PR](#)
- High Container Security**  
Container: Podinfod  
Container allowed to run as root (UID 0)  
[Create PR](#)

React Flow



carakube

POD

hello-8010-db8f66bb6-vrc2s

STATUS

Phase: RUNNING

Pod IP: 10.244.1.6

Host IP: 172.20.0.2

Node: carakube-demo-worker

QoS Class: BestEffort

CONTAINERS (1)

http-echo  
hashicorp/http-echo:0.2.3

Requests: - / -

Limits: - / -

8010/TCP

VOLUMES (1)

kube-api-access-c727x  
Projected

LABELS

app: hello-8010  
pod-template-hash: db8f66bb6

RECENT EVENTS

Scheduled  
Successfully assigned default/hello-8010-db8f66bb6-vrc2s to carakube-demo-worker

Pulled  
Container image "hashicorp/http-echo:0.2.3" already

Reset Layout

Filtering vulnerabilities for selected node

High Resource Limits

Container: Http-Echo

Container missing resource limits: cpu, memory

Create PR

Medium Vulnerabilities

Medium ServiceAccount SA: Default

ServiceAccount token automatically mounted (default SA token is usually useless but increases attack surface)

Create PR

Low Vulnerabilities

Low ServiceAccount SA: Default

Pod uses default ServiceAccount (best practice: create dedicated SA)

Create PR

React Flow

The screenshot shows a Kubernetes cluster visualization with nodes, namespaces, and pods. A specific pod, 'hello-8010-db8f66bb6-vrc2s', is selected, displaying its status, containers, volumes, and recent events. To the right, three categories of vulnerabilities are listed: High (Resource Limits), Medium (ServiceAccount), and Low (ServiceAccount). Each category includes a summary, a 'Create PR' button, and a 'React Flow' button at the bottom.



hackatum-k8s-flux/clusters/carakube carakube

# carakube

POD

hello-8010-db8f66bb6-vrc2s

STATUS

Phase: RUNNING

Pod IP: 10.244.1.6

Host IP: 172.20.0.2

Node: carakube-demo-worker

QoS Class: BestEffort

CONTAINERS (1)

http-echo  
hashicorp/http-echo:0.2.3

Requests: - / -

Limits: - / -

8010/TCP

VOLUMES (1)

kube-api-access-c727x  
Projected

LABELS

app: hello-8010  
pod-template-hash: db8f66bb6

RECENT EVENTS

Scheduled  
Successfully assigned default/hello-8010-db8f66bb6-vrc2s to carakube-demo-worker

Pulled  
Container image "hashicorp/http-echo:0.2.3" already

Reset Layout

namespace  
default (10)

namespace  
flux-system (9)

service  
podinfo0

pod  
helm-controller-cccd949cd-jrk8c

pod  
kustomize-controller-789f6cccd67-r97kg

service  
notification-controller0

service  
kube-proxy-cx7zj0

pod  
hello-8010-db8f66bb6-vrc2s

pod  
podinfo-b76f6cd59-b4mvs

pod  
podinfo-b76fd8b8c

server  
io-control-0

coredns-7db6d8ff4d4rs-tz0

coredns-7db6d8ff4d-jkdnf0

node  
carakube-demo-control-plane0

Filtering vulnerabilities for selected node

High Resource Limits

Container: Http-Echo

Container missing resource limits: cpu, memory

Processing...

Medium Vulnerabilities

Medium ServiceAccount SA: Default

ServiceAccount token automatically mounted (default SA token is usually useless but increases attack surface)

Create PR

Low Vulnerabilities

Low ServiceAccount SA: Default

Pod uses default ServiceAccount (best practice: create dedicated SA)

Create PR

>>

React Flow



# carakube

POD  
hello-8010-db8f66bb6-vrc2s

STATUS

Phase: RUNNING

Pod IP: 10.244.1.6

Host IP: 172.20.0.2

Node: carakube-demo-worker

QoS Class: BestEffort

CONTAINERS (1)

http-echo  
hashicorp/http-echo:0.2.3

Requests: - / -

Limits: - / -

8010/TCP

VOLUMES (1)

kube-api-access-c727x  
Projected

LABELS

app: hello-8010  
pod-template-hash: db8f66bb6

RECENT EVENTS

Scheduled  
Successfully assigned default/hello-8010-db8f66bb6-vrc2s to carakube-demo-worker

Pulled  
Container image "hashicorp/http-echo:0.2.3" already

github.com/SamuelLess/hackatum-k8s-flux/pull/11

Reset Layout

Filtering vulnerabilities for selected node

High Resource Limits

Container: Http-Echo

Container missing resource limits: cpu, memory

View Fix PR

Medium Vulnerabilities

Medium ServiceAccount SA: Default

ServiceAccount token automatically mounted (default SA token is usually useless but increases attack surface)

Create PR

Low Vulnerabilities

Low ServiceAccount SA: Default

Pod uses default ServiceAccount (best practice: create dedicated SA)

Create PR



Auto-fix: Resolve vuln-6bca24f92c608ced #11

**Open** yndolg wants to merge 1 commit into `main` from `autofix/vuln-6bca24f92c608ced-20251123_033103`

Conversation 0 Commits 1 Checks 0 Files changed 1 +4 -0

yndolg commented now

Add CPU and Memory Resource Limits to `http-echo` container in `hello-8010` pod

**Security Issue**

The `http-echo` container within the `hello-8010` pod was configured without explicit CPU and memory resource limits. This is a significant security risk because a misbehaving or malicious process inside this container could potentially consume all available CPU cycles or memory on the node. This uncontrolled resource consumption could lead to a Denial of Service (DoS) for other critical applications running on the same node, or even cause the entire Kubernetes node to become unresponsive, impacting the stability and availability of the cluster. Without these limits, resource exhaustion attacks are much easier to execute and more damaging.

**How This Fix Addresses the Issue**

This fix addresses the missing resource limits by explicitly defining CPU and memory limits for the `http-echo` container in the `hello-8010` pod's deployment configuration. By setting these limits, we ensure that the container cannot consume more than its allocated share of resources. Specifically, the container is now limited to 100 millicores of CPU and 128 MiB

Reviewers  
Suggestions  
Copilot  
Request

Still in progress? Convert to draft

Assignees  
No one—assign yourself

Labels  
None yet

Projects  
None yet

Milestone



github.com/SamuelLess/hackatum-k8s-flux/pull/11/commits

SamuelLess / hackatum-k8s-flux

Type  to search

Code Issues Pull requests 10 Actions Projects Wiki Security Insights Settings

## Auto-fix: Resolve vuln-6bca24f92c608ced #11

**Open** yndolg wants to merge 1 commit into `main` from `autofix/vuln-6bca24f92c608ced-20251123_033103`

Conversation 0 Commits 1 Checks 0 Files changed 1 +4

Commits on Nov 23, 2025

Auto-fix: Resolve vuln-6bca24f92c608ced

Carakube Bot committed now 41101a5

This screenshot shows a GitHub pull request page for a repository named "hackatum-k8s-flux". The pull request is titled "Auto-fix: Resolve vuln-6bca24f92c608ced #11". It is currently open and ready to be merged into the "main" branch from a branch named "autofix/vuln-6bca24f92c608ced-20251123\_033103". There is one commit in the pull request, which was made by the Carakube Bot and pushed at 41101a5. The commit message is "Auto-fix: Resolve vuln-6bca24f92c608ced". The pull request has received 10 reviews and is currently being discussed in the comments section. The repository has 10 pull requests, 10 issues, and 10 actions. The user "yndolg" is the author of the pull request. The repository also includes projects, wiki, security, insights, and settings sections.



Auto-fix: Resolve vuln-6bca24f92c608ced #11

**Open** yndolg wants to merge 1 commit into `main` from `autofix/vuln-6bca24f92c608ced-20251123_033103`

Conversation 0    Commits 1    Checks 0    Files changed 1    +4

### Commits on Nov 23, 2025

**Auto-fix: Resolve vuln-6bca24f92c608ced**

Carakube Bot committed now

This screenshot shows a GitHub pull request page for a repository named "hackatum-k8s-flux". The title of the pull request is "Auto-fix: Resolve vuln-6bca24f92c608ced #11". A green button labeled "Open" indicates the pull request is ready to be merged. The merge target is "main" and the source branch is "autofix/vuln-6bca24f92c608ced-20251123\_033103". The pull request has 1 commit, 0 checks, and 1 file changed. The commit message is "Auto-fix: Resolve vuln-6bca24f92c608ced" and it was committed by the "Carakube Bot". The date of the commit is Nov 23, 2025. The GitHub interface includes standard navigation bars like Code, Issues, Pull requests, Actions, Projects, Wiki, Security, Insights, and Settings, along with search and filter tools.



hackatum-k8s-flux/clusters/carakube · carakube · Auto-fix: Resolve vuln-6bca24f92c608ced · +

github.com/SamuelLess/hackatum-k8s-flux/pull/11/files

SamuelLess / hackatum-k8s-flux

Type ⌘ to search

Code Issues Pull requests 10 Actions Projects Wiki Security Insights Settings

## Auto-fix: Resolve vuln-6bca24f92c608ced #11

Try the new experience Edit <> Code

Open yndolg wants to merge 1 commit into main from autofix/vuln-6bca24f92c608ced-20251123\_033103

Conversation 0 Commits 1 Checks 0 Files changed 1 +4 -0

Changes from all commits File filter Conversations Jump to Ask Copilot Review in codespace Review changes

clusters/carakube-demo/apps/hello-8010/deployment-hostport.yaml

Viewed ...

```
@@ -25,6 +25,10 @@ spec:  
 25 25      ports:  
 26 26          - containerPort: 8010  
 27 27          hostPort: 8010  
 28 +      resources:  
 29 +          limits:  
 30 +              cpu: "100m"  
 31 +              memory: "128Mi"  
 28 32      securityContext:  
 29 33          allowPrivilegeEscalation: false  
 30 34          runAsNonRoot: true  
 31 35
```



Auto-fix: Resolve vuln-6bca24f92c608ced #11  
yndolg wants to merge 1 commit into [main](#) from [autofix/vuln-6bc...](#)

Auto-fix: Resolve vuln-6bca24f92c608ced ... 41101a5

**Commit message**  
Merge pull request #11 from SamuelLess/autofix/vuln-6bca24f92c608ced-20251123\_033103

**Extended description**  
Auto-fix: Resolve vuln-6bca24f92c608ced

**Commit email**  
samuel@lessmann.dev

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

**Add a comment**

Add your comment here...

This screenshot shows a GitHub pull request interface for a repository named 'hackatum-k8s-flux/clusters/car'. The pull request is titled 'Auto-fix: Resolve vuln-6bca24f92c608ced #11' and is being merged into the 'main' branch from the 'autofix/vuln-6bc...' branch. A green button labeled 'Open' is visible above the commit details. The commit message is set to 'Merge pull request #11 from SamuelLess/autofix/vuln-6bca24f92c608ced-20251123\_033103'. Below the commit message, there is an 'Extended description' field containing the text 'Auto-fix: Resolve vuln-6bca24f92c608ced'. The commit email is set to 'samuel@lessmann.dev'. At the bottom of the modal, there are two buttons: a green one with a circular icon and a white 'Cancel' button. A link to 'Convert to draft' is also present. Below the modal, there is a section for adding a comment with a 'Write' button, a preview button, and a rich text editor toolbar. The text input field is placeholdered with 'Add your comment here...'. The overall interface is clean and modern, typical of GitHub's design.



The screenshot shows a GitHub pull request merge screen. At the top, a purple banner indicates the pull request has been merged. The URL is [github.com/SamuelLess/hackatum-k8s-flux/pull/11](https://github.com/SamuelLess/hackatum-k8s-flux/pull/11). The title of the pull request is "Auto-fix: Resolve vuln-6bca24f92c608ced #11". It shows that SamuelLess merged 1 commit from the `main` branch into the `autofix/vuln-6bc...` branch. A "Revert" button is available for the merge commit.

Below the merge message, there is a "Delete branch" button next to a "Pull request successfully merged and closed" message. It states: "You're all set — the `autofix/vuln-6bca24f92c608ced-20251123_033103` branch can be safely deleted."

The main content area features a "Add a comment" section with a "Write" tab selected. A text input field contains the placeholder "Add your comment here...". Below the input field are two buttons: "Markdown is supported" and "Paste, drop, or click to add files". A "Comment" button is located at the bottom right of the comment area.

At the bottom of the page, a note says: "Remember, contributions to this repository should follow our [GitHub Community Guidelines](#)". A "ProTip!" link is also present, suggesting to add comments to specific lines under "Files changed".





Screenshot of a GitHub Actions run details page for a merge pull request.

The URL in the browser is [github.com/SamuelLess/hackatum-k8s-flux/actions/runs/19605284821](https://github.com/SamuelLess/hackatum-k8s-flux/actions/runs/19605284821).

The main title is "Merge pull request #11 from SamuelLess/autofix/vuln-6bca24f92c608ced-... #18".

The left sidebar shows the following sections:

- Summary (selected)
- Jobs
- deploy (highlighted)
- Run details
- Usage
- Workflow file

The main content area displays the following information:

Triggered via push now	Status	Total duration	Artifacts
SamuelLess pushed → 0fd7519 main	In progress	—	—

Below this, the workflow file "main.yaml" is shown:

```
main.yaml
on: push

  deploy
    13s
```

At the bottom right of the main content area are three buttons: a minus sign, a plus sign, and a square icon.



hackatum-k8s-flux/clusters/car x carakube x Merge pull request #11 from Sa... x +

github.com/SamuelLess/hackatum-k8s-flux/actions/runs/19605284821/job/56142954159 120% ⭐ ⓘ ⌂ ⌂

Summary

Jobs

deploy

Started 20s ago

Search logs ⚙

Reconcile Flux cluster 18s

```
// TFLUX-SYSTEM main@sha1:1b0caa85 false true stored artifact for revision 'main@sha1:1b0caa85'  
78 ==> Forcing Git re-pull via Flux GitRepository 'flux-system' in ns 'flux-system'...  
79 ▶ annotating GitRepository flux-system in flux-system namespace  
80 ✓ GitRepository annotated  
81 ◎ waiting for GitRepository reconciliation  
82 ✓ fetched revision main@sha1:0fd7519009d8a853e563e9d20e63c52a823b613f  
83 ==> Reconciling ALL Kustomizations across all namespaces (with-source)...  
84 ----> Reconciling flux-system/flux-system  
85 ▶ annotating GitRepository flux-system in flux-system namespace  
86 ✓ GitRepository annotated  
87 ◎ waiting for GitRepository reconciliation  
88 ✓ fetched revision main@sha1:0fd7519009d8a853e563e9d20e63c52a823b613f  
89 ▶ annotating Kustomization flux-system in flux-system namespace  
90 ✓ Kustomization annotated  
91 ◎ waiting for Kustomization reconciliation  
92 ✓ applied revision main@sha1:0fd7519009d8a853e563e9d20e63c52a823b613f  
93 ----> Reconciling flux-system/hello-8010  
94 ▶ annotating GitRepository flux-system in flux-system namespace  
95 ✓ GitRepository annotated  
96 ◎ waiting for GitRepository reconciliation  
97 ✓ fetched revision main@sha1:0fd7519009d8a853e563e9d20e63c52a823b613f  
98 ▶ annotating Kustomization hello-8010 in flux-system namespace  
99 ✓ Kustomization annotated  
100 ◎ waiting for Kustomization reconciliation
```

Post Checkout



Merge pull request #11 from SamuelLess / hackatum-k8s-flux · carakube · GitHub

github.com/SamuelLess/hackatum-k8s-flux/actions/runs/19605284821/job/56142954159

SamuelLess / hackatum-k8s-flux

Type ⌘ to search

Code Issues Pull requests 9 Actions Projects Wiki Security Insights Settings

← Flux Reconcile

## Merge pull request #11 from SamuelLess/autofix/vuln-6bca24f92c608ced-... #18

Re-run all jobs ...

Summary

Jobs

deploy

Run details

Usage

Workflow file

deploy

succeeded now in 50s

Search logs

Set up job 1s

Checkout 0s

Reconcile Flux cluster 47s

Post Checkout 0s

Complete job 0s

This screenshot shows a GitHub Actions run page for a merge pull request. The main title is "Merge pull request #11 from SamuelLess/autofix/vuln-6bca24f92c608ced-... #18". The "Actions" tab is selected. On the left, there's a sidebar with links for "Summary", "Jobs" (which is active), "Run details", "Usage", and "Workflow file". The "Jobs" section shows a single job named "deploy" with a green checkmark. The status is "succeeded now in 50s". Below the status, there's a "Search logs" input field and a gear icon. The job steps are listed: "Set up job" (1s), "Checkout" (0s), "Reconcile Flux cluster" (47s), "Post Checkout" (0s), and "Complete job" (0s). All steps have green checkmarks indicating they were successful.



carakube

POD  
hello-8010-64d84dcdf8-lq2jz

STATUS

Phase: RUNNING  
Pod IP: 10.244.1.9  
Host IP: 172.20.0.2  
Node: carakube-demo-worker  
QoS Class: Guaranteed

CONTAINERS (1)

http-echo  
hashicorp/http-echo:0.2.3  
Requests: 100m / 128Mi  
Limits: 100m / 128Mi  
8010/TCP

VOLUMES (1)

kube-api-access-kpbfg  
Projected

LABELS

app: hello-8010  
pod-template-hash: 64d84dcdf8

RECENT EVENTS

Scheduled  
Successfully assigned default/hello-8010-64d84dcdf8-lq2jz to carakube-demo-worker

Pulled  
Container image "hashicorp/http-echo:0.2.3" already

Reset Layout

Filtering vulnerabilities for selected node

Medium Vulnerabilities

Medium ServiceAccount SA: Default

ServiceAccount token automatically mounted (default SA token is usually useless but increases attack surface)

Create PR

Low Vulnerabilities

Low ServiceAccount SA: Default

Pod uses default ServiceAccount (best practice: create dedicated SA)

Create PR

Diagram showing the Kubernetes cluster topology:

- Nodes:** carakube-demo-control-plane0
- Namespaces:** default (10 pods), flux-system (9 pods)
- Services:** podinfo0, helm-controller-cccd949cd-jrk8c, kustomize-controller-789f6cccd67-r97kg, notification-controller0
- Pods:** kube-proxy-cx7j0, hello-8010-64d84dcdf8-lq2jz, podinfo-b76f6cd59-b4mvs, podinfo-b76fd8b8c, coredns-7db6d8ff4d-4rsztz0, coredns-7db6d8ff4d-jkdnf0, kube-controller-manager-carakube-demo-control-plane0

React Flow



carakube

POD  
hello-8010-64d84dcdf8-lq2jz

STATUS

Phase: RUNNING  
Pod IP: 10.244.1.9  
Host IP: 172.20.0.2  
Node: carakube-demo-worker  
QoS Class: Guaranteed

CONTAINERS (1)

http-echo  
hashicorp/http-echo:0.2.3  
Requests: 100m / 128Mi  
Limits: 100m / 128Mi  
8010/TCP

VOLUMES (1)

kube-api-access-kpbfg  
Projected

LABELS

app: hello-8010  
pod-template-hash: 64d84dcdf8

RECENT EVENTS

Scheduled  
Successfully assigned default/hello-8010-64d84dcdf8-lq2jz to carakube-demo-worker

Pulled  
Container image "hashicorp/http-echo:0.2.3" already

Reset Layout

Filtering vulnerabilities for selected node

Medium Vulnerabilities

i Medium ServiceAccount SA: Default  
ServiceAccount token automatically mounted (default SA token is usually useless but increases attack surface)  
View Fix PR

Low Vulnerabilities

i Low ServiceAccount SA: Default  
Pod uses default ServiceAccount (best practice: create dedicated SA)  
Processing...

The diagram illustrates a Kubernetes cluster topology. It shows various components connected via dashed lines representing network traffic. Key elements include:

- Namespaces:** default (10 vulnerabilities), flux-system (9 vulnerabilities).
- Services:** service1, notification-controller0.
- Pods:** podinfo0, helm-controller-cccd949cd-jrk8c, kustomize-controller-789f6cccd67-r97kg, kube-proxy-cx7jz0, hello-8010-64d84dcdf8-lq2jz, podinfo-b76f6cd59-b4mvs, podinfo-b76fd8b8c, coredns-7db6d8ff4d-4rs-tz0, coredns-7db6d8ff4d-jkdnf0, kube-controller-manager-carakube-demo-control-plane0.
- Nodes:** carakube-demo-control-plane0.

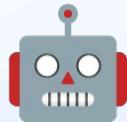
A tooltip on the right side of the interface states: "Filtering vulnerabilities for selected node".



carakube.dev



CaraCube



**GitOps by Design**



**Trivially Expandable**



**Seamless kubectl Integration**



CaraCube

**Any Questions?**