
KubeCon
CloudNativeCon
Europe 2023
ARMO
port
Let's GO backstage!
IDP Security for Platform Engineers
Suzanne Daniels
Rotem Refael

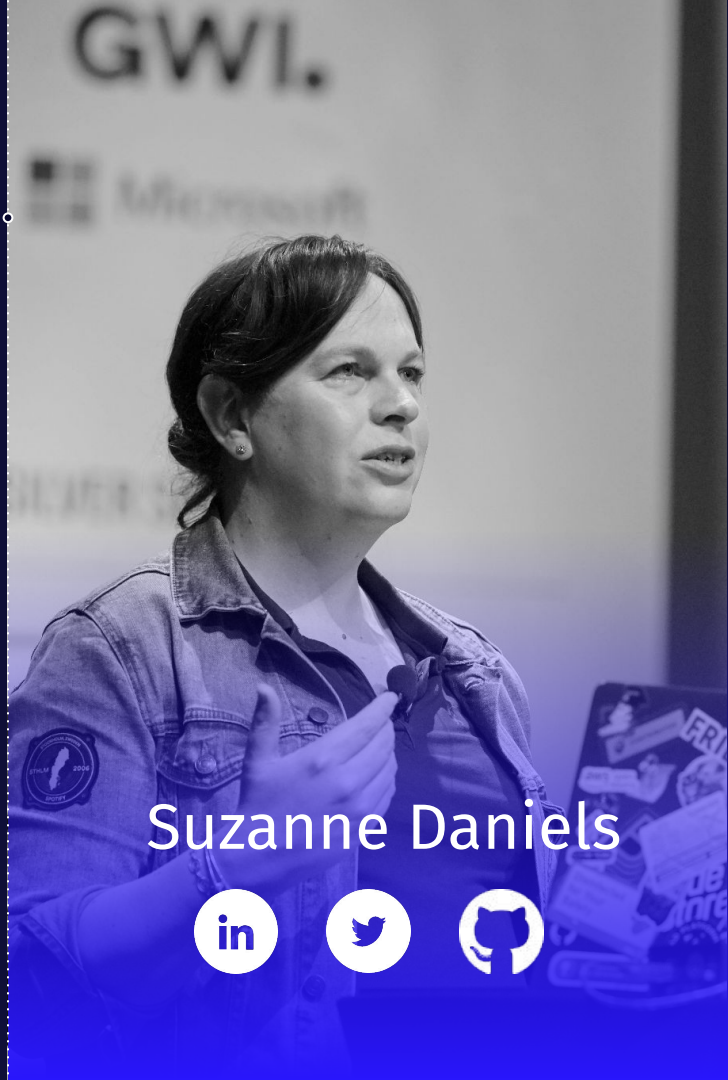
Who am I?

Developer Happiness

Platform engineering advocate

Lowest point of NL

Snowboarding



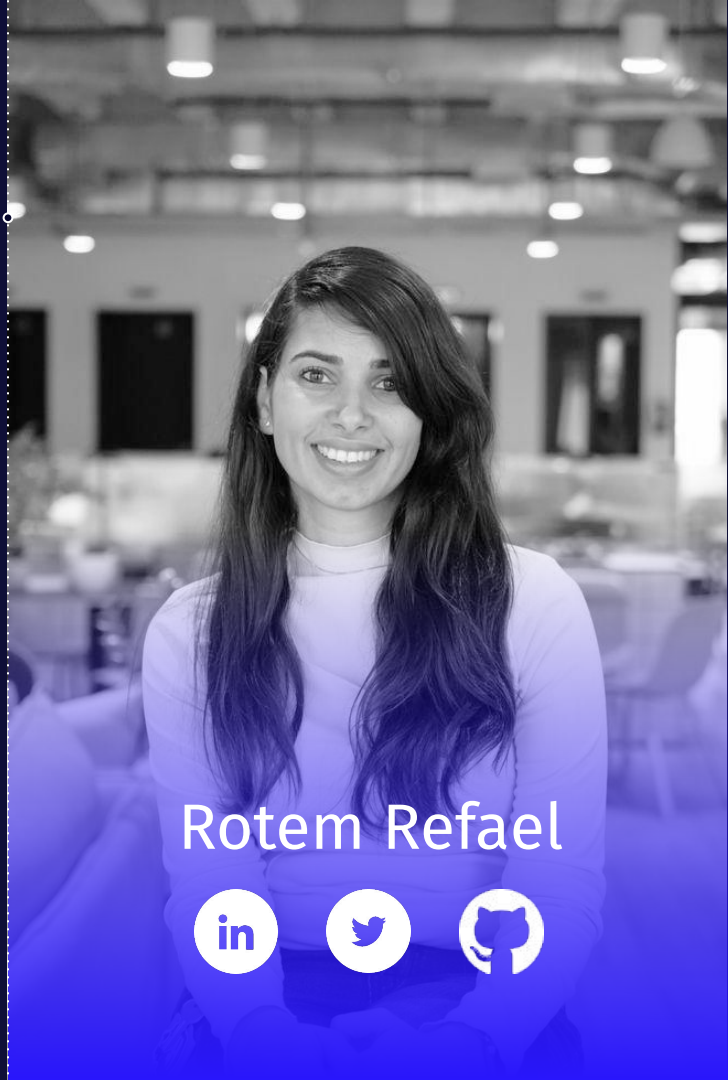
Who am I?

Developer in heart and soul

Devops enthusiast

Yoga lover

Basketball fan




It’s been 84 years...


Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io

/Solving the challenges

- DevOps
- SRE
- Platform Engineering

/Dev*Ops

DevSecMLFinDataOps

/Internal Developer Portal

*"Internal developer portals serve as the **interface** through which developers can **discover** and **access** internal developer platform capabilities." - Gartner*

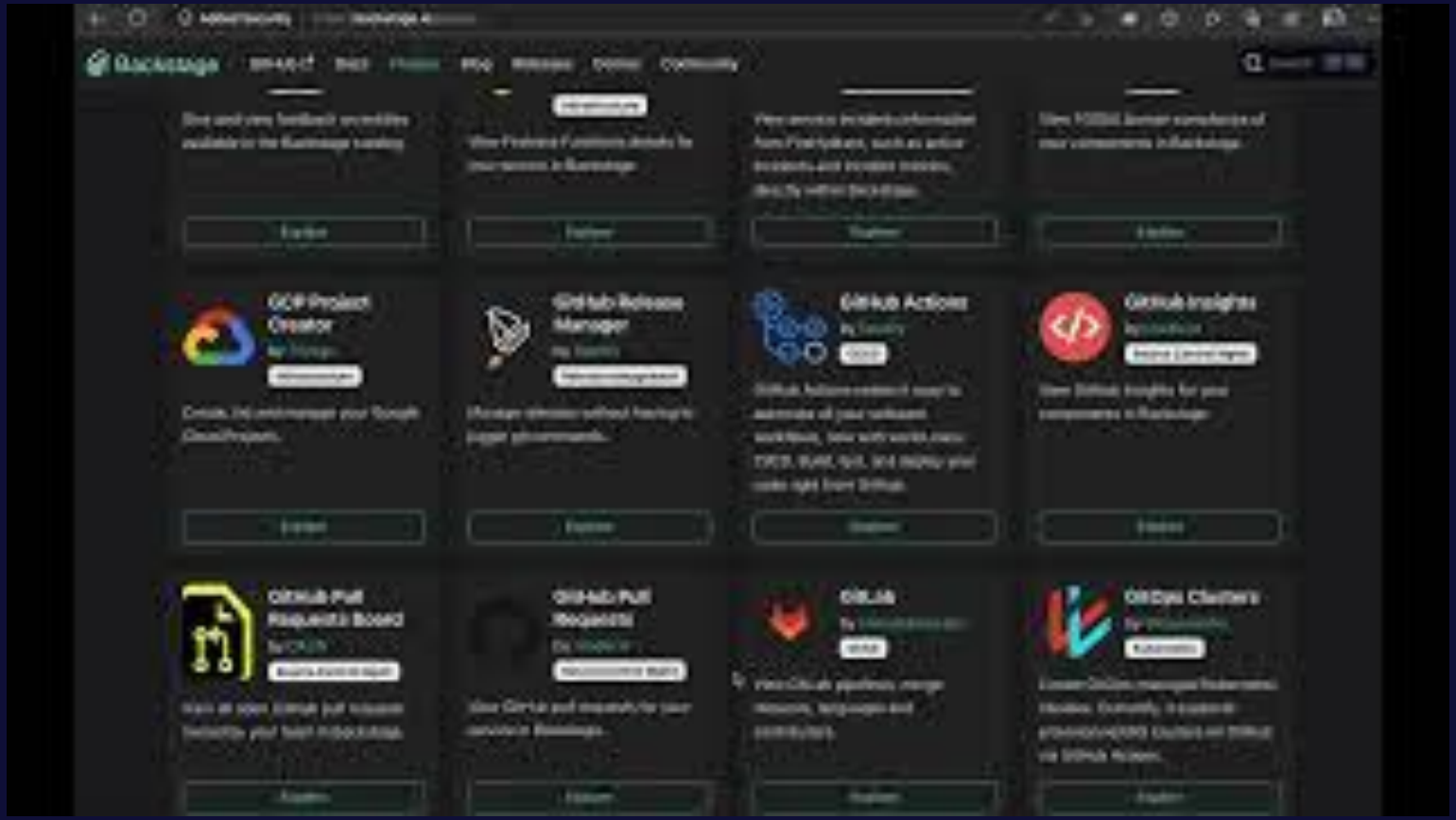
/Backstage

Backstage is an **open platform** for

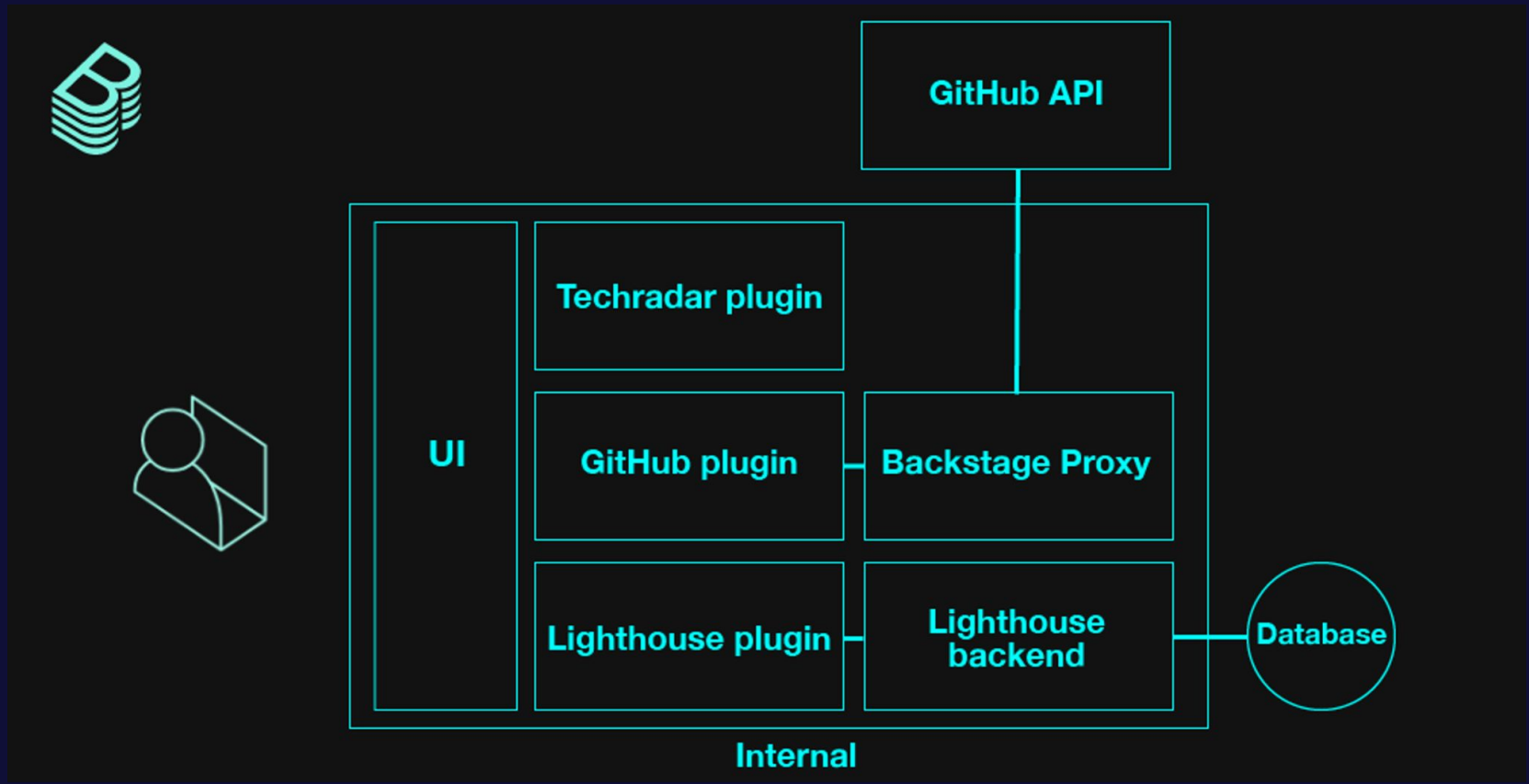
building Developer Portals

- Open Source
- Functionality from plugins
- Plugin ecosystem
- Build your own

/Plugins

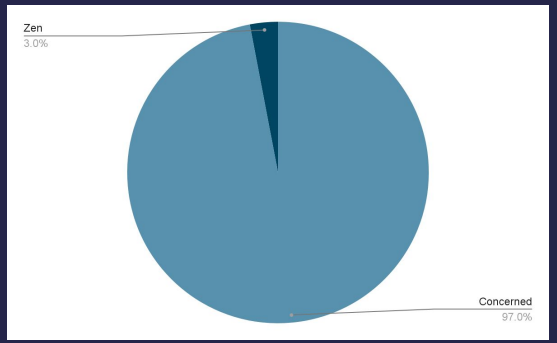

Backstage
GCP Project Creator
GitHub Release Manager
GitHub Actions
GitHub Insights
GitHub Pull Requests Board
GitHub Pull Requests
GitLab
GitOps Clusters

/Plugins


GitHub API
UI
Techradar plugin
GitHub plugin
Backstage Proxy
Lighthouse plugin
Lighthouse backend
Database
Internal

/Scary Numbers

97% of organizations have concerns about Kubernetes security



Source: Tanzu State of Kubernetes 2022

99% of breaches in 2025 will have a root cause of customer **misconfigurations** or **mistakes**

Gartner®


SHIFT SECURITY LEFT...
WE SHALL

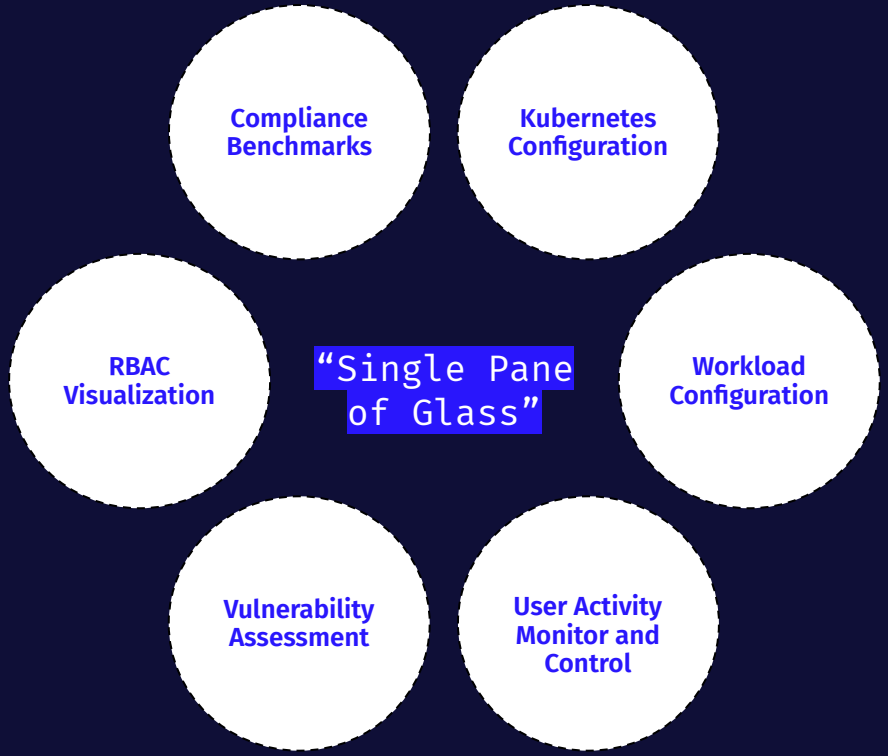

KUBERNETES SECURITY
WITHIN BACKSTAGE
YES, WE CAN!
imgflip.com

Kubescape

NSA, MITRE, CIS Benchmark, or create your own custom one

Identify and prevent drift
Continuously, from CI to production

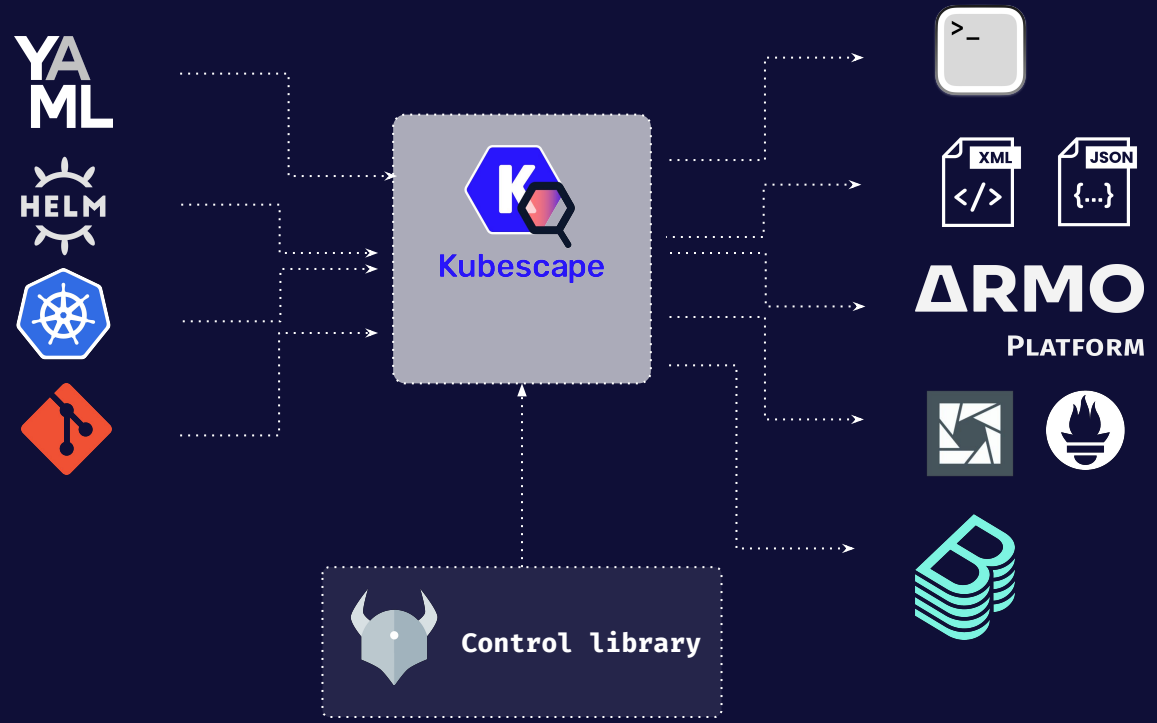
Continuous Kubernetes hardening and attack surface reduction
Remediation advice, contextual insights



</ Over 150 different controls

{Kubernetes-specific}
security and compliance
frameworks and controls

/Inputs/Outputs/magic



```
craigbox@mac:~/Documents/Projects/sarif-demo$ kubescape scan framework nsa --enable-host-scan
[info] Kubescape scanner starting
[info] Installing host scanner
[info] Downloading/Loading policy definitions
[success] Downloaded/Loaded policy
[info] Accessing Kubernetes objects
[success] Accessed to Kubernetes objects
[info] Requesting Host scanner data
[info] Host scanner version : v1.0.45
[success] Requested Host scanner data
[info] Scanning. Cluster: docker-desktop
Control C-0068 100% |████████████████████████████████████████████████████████████████████████████████| (24/24, 54 it/s)
[success] Done scanning. Cluster: docker-desktop

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

Controls: 24 (Failed: 13, Passed: 10, Action Required: 1)
Failed Resources by Severity: Critical — 0, High — 4, Medium — 48, Low — 4

+----------+-----------------------------------------------+------------------+---------------+--------------------+
| SEVERITY |                 CONTROL NAME                  | FAILED RESOURCES | ALL RESOURCES |   % RISK-SCORE     |
+----------+-----------------------------------------------+------------------+---------------+--------------------+
| High     | Resource limits                               |        4         |      29       |        13%         |
| High     | Applications credentials in configuration files |        0         |      51       | Action Required * |
| Medium   | Exec into container                           |        1         |      72       |        1%          |
| Medium   | Non-root containers                           |        3         |      29       |        10%         |
| Medium   | Allow privilege escalation                    |        3         |      29       |        10%         |
| Medium   | Ingress and Egress blocked                    |        16        |      29       |        53%         |
| Medium   | Automatic mapping of service account          |        16        |      73       |        22%         |
| Medium   | Cluster-admin binding                         |        1         |      72       |        1%          |
| Medium   | Cluster internal networking                   |        2         |       6       |        33%         |
| Medium   | Linux hardening                               |        4         |      29       |        13%         |
| Medium   | Secret/ETCD encryption enabled                |        1         |       1       |        100%        |
| Medium   | Audit logs enabled                            |        1         |       1       |        100%        |
| Low      | Immutable container filesystem                |        3         |      29       |        10%         |
| Low      | PSP enabled                                   |        1         |       1       |        100%        |
+----------+-----------------------------------------------+------------------+---------------+--------------------+
|          |                RESOURCE SUMMARY               |        23        |      176      |       8.45%        |
+----------+-----------------------------------------------+------------------+---------------+--------------------+
FRAMEWORK NSA

* Control missing configuration


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
   << WOW! Now you can see the scan results on the web >>

   https://cloud.armosec.io/compliance/docker-desktop?utm_campaign=Submit&utm_medium=CLI&utm_source=GitHub
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


Run with '--verbose'/'-v' flag for detailed resources view

craigbox@mac:~/Documents/Projects/sarif-demo$
```

ARMO
POWERED BY KUBESCAPE

Docker Desktop | Free | CB

CLUSTER
- Dashboard
- Compliance
- Vulnerabilities
- RBAC Visualizer

CODE
- Repository Scanning
- Registry Scanning

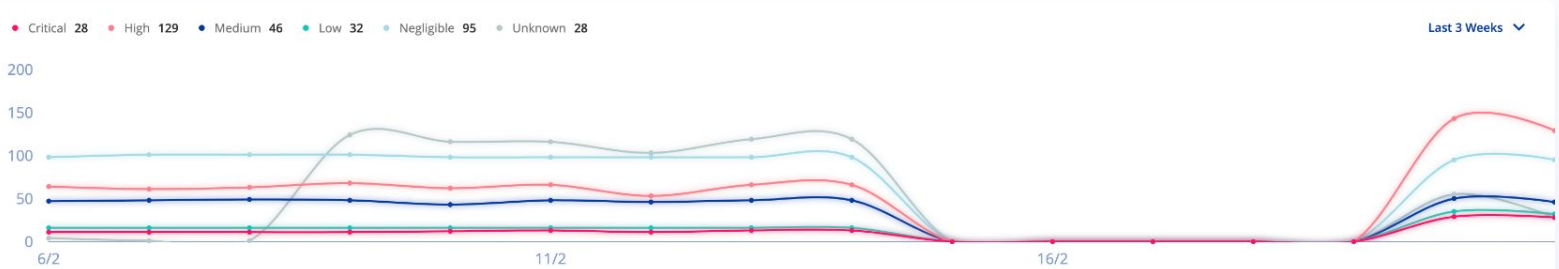
Getting started >>
50%

Vulnerabilities

Scan

TOTAL VULNERABILITIES	CRITICAL	HIGH	MEDIUM	LOW	NEGLIGIBLE	UNKNOWN
398 (204 Fixable, 3 RCE)	32 (24 Fixable, 0 RCE)	154 (106 Fixable, 3 RCE)	50 (22 Fixable, 0 RCE)	35 (20 Fixable, 0 RCE)	95 (0 Fixable, 0 RCE)	32 (32 Fixable, 0 RCE)

Vulnerabilities Overtime



Search CVE | Scan time: 22/02/2023 - 23/02/2023 | + Add filter | Clear all filters

STAT.	SCAN TIME	CLUSTER	NAMESPACE	WORKLOAD	CONTAINER NAME	REGISTRY	IMAGE TAG	SEVERITY
	Feb 22, 2023 11:11:07	docker-desktop	default	deployment-currencyservice	server	gcr.io	gcr.io/google-samples/microservices-demo/currencyservice:v0.5.0	3 16 1 1 0 2
	Feb 22, 2023 11:11:23	docker-desktop	default	deployment-paymentservice	server	gcr.io	gcr.io/google-samples/microservices-demo/paymentservice:v0.5.0	3 15 1 1 0 2
	Feb 22, 2023	docker-					gcr.io/google-samples/microservic	


FINISHED
HACKATHON
host
planetacurioso.com

Backstage

Search

Home

Compliance

Vulnerabilities

Docs

Create...

Tech Radar

Settings

Welcome to ARMO kubescape-plugin!

See all your Kubescape resources

Create a new account:

Account Name*

CREATE

Backstage

Search

Home

Compliance

Vulnerabilities

Docs

Create...

Tech Radar

Settings

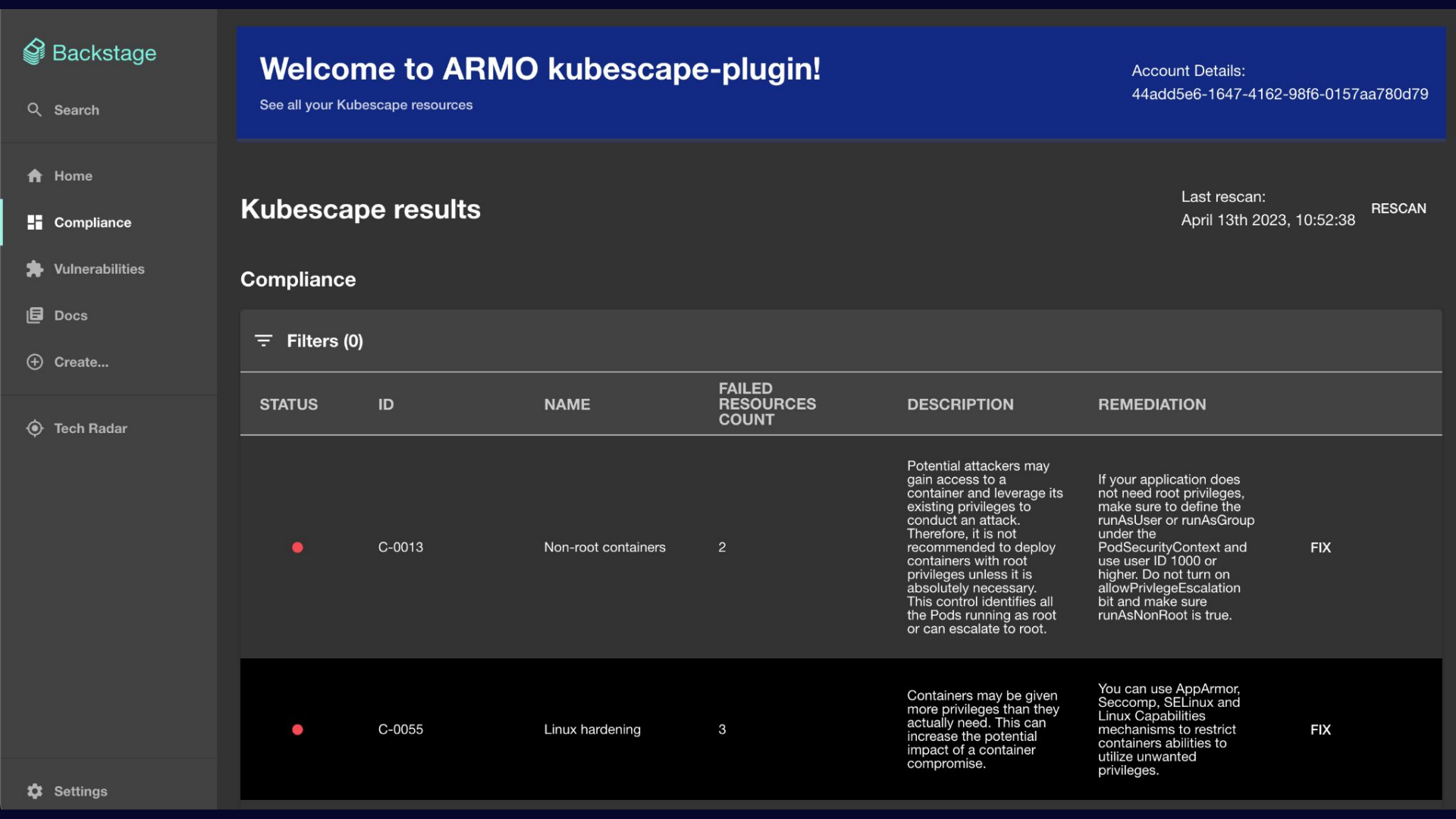
Welcome to ARMO kubescape-plugin!

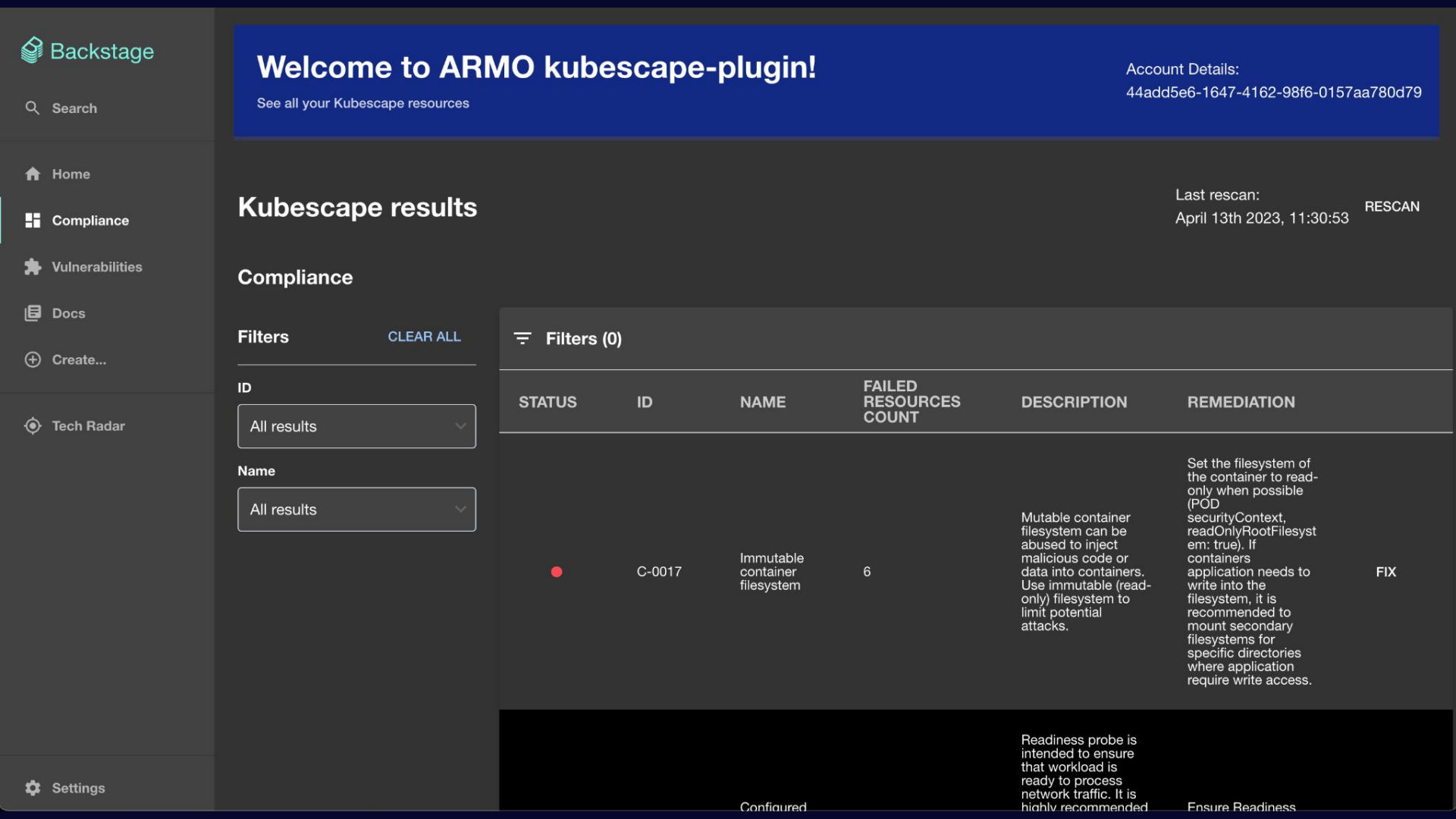
See all your Kubescape resources

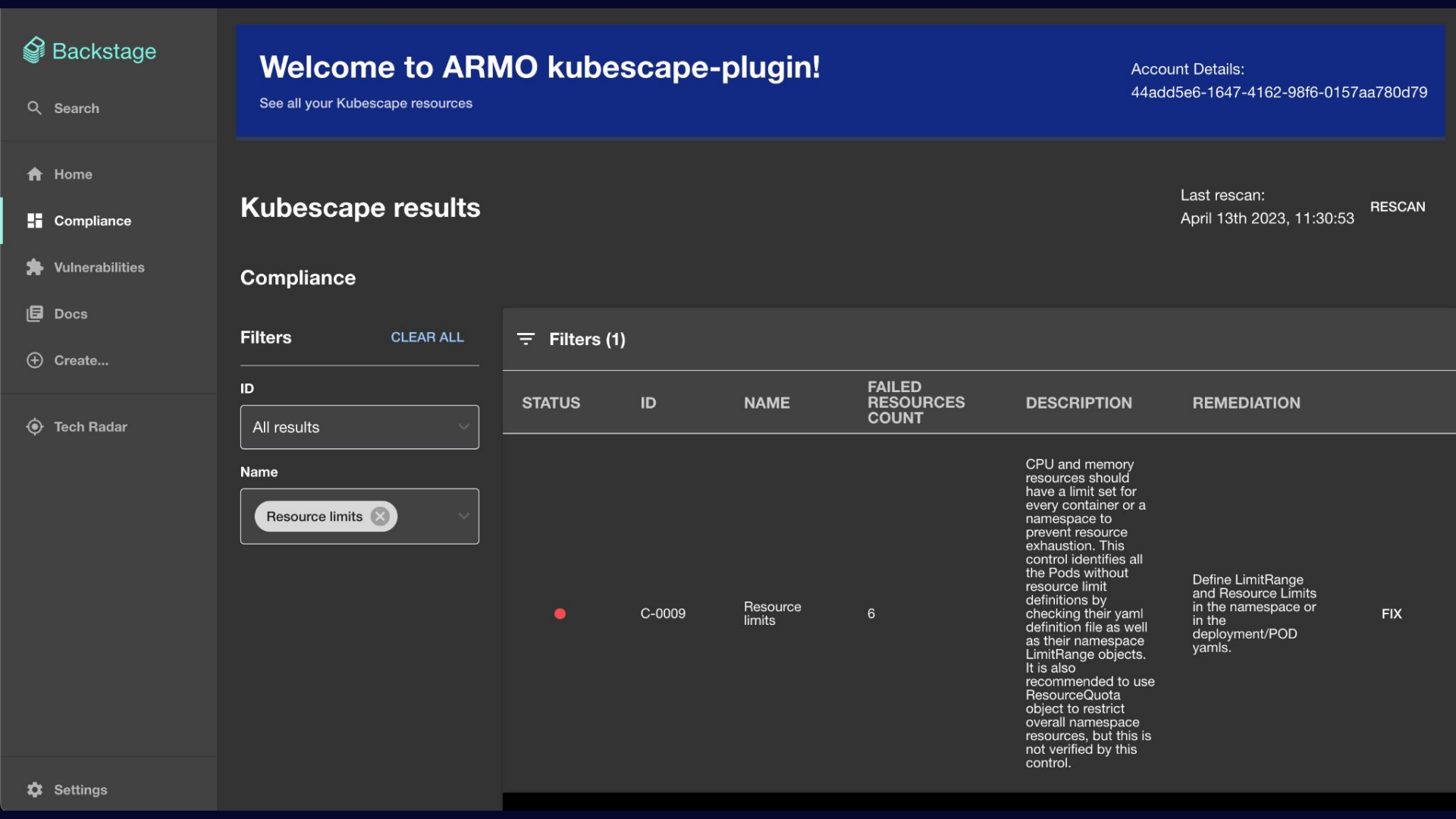
Connect your Kubernetes cluster

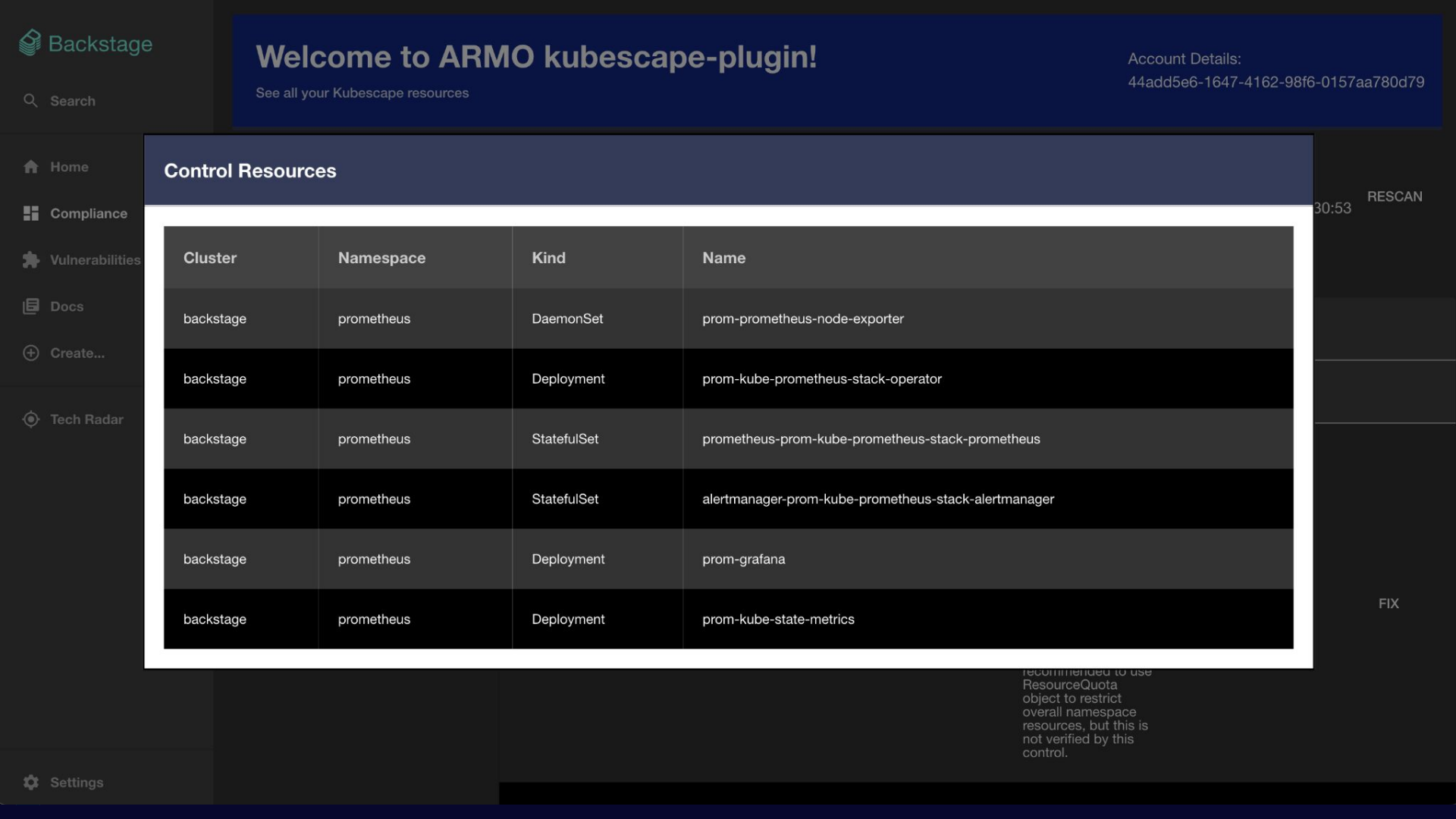
```
helm repo add kubescape https://kubescape.github.io/helm-charts/ ; helm repo update ; helm upgrade --install kubescape kubescape/kubescape-cloud-operator -n kubescape --create-namespace --set clusterName="kubectl config current-context" --set account=44add5e6-1647-4162-98f6-0157aa780d79
```

COPY


Backstage
Search
Home
Compliance
Vulnerabilities
Docs
Create...
Tech Radar
Settings
Welcome to ARMO kubescape-plugin!
See all your Kubescape resources
Account Details:
44add5e6-1647-4162-98f6-0157aa780d79
Kubescape results
Last rescan:
April 13th 2023, 10:52:38
RESCAN
Compliance
Filters (0)
STATUS
ID
NAME
FAILED RESOURCES COUNT
DESCRIPTION
REMEDIATION
C-0013
Non-root containers
2
Potential attackers may gain access to a container and leverage its existing privileges to conduct an attack. Therefore, it is not recommended to deploy containers with root privileges unless it is absolutely necessary. This control identifies all the Pods running as root or can escalate to root.
If your application does not need root privileges, make sure to define the runAsUser or runAsGroup under the PodSecurityContext and use user ID 1000 or higher. Do not turn on allowPrivlegeEscalation bit and make sure runAsNonRoot is true.
FIX
C-0055
Linux hardening
3
Containers may be given more privileges than they actually need. This can increase the potential impact of a container compromise.
You can use AppArmor, Seccomp, SELinux and Linux Capabilities mechanisms to restrict containers abilities to utilize unwanted privileges.
FIX

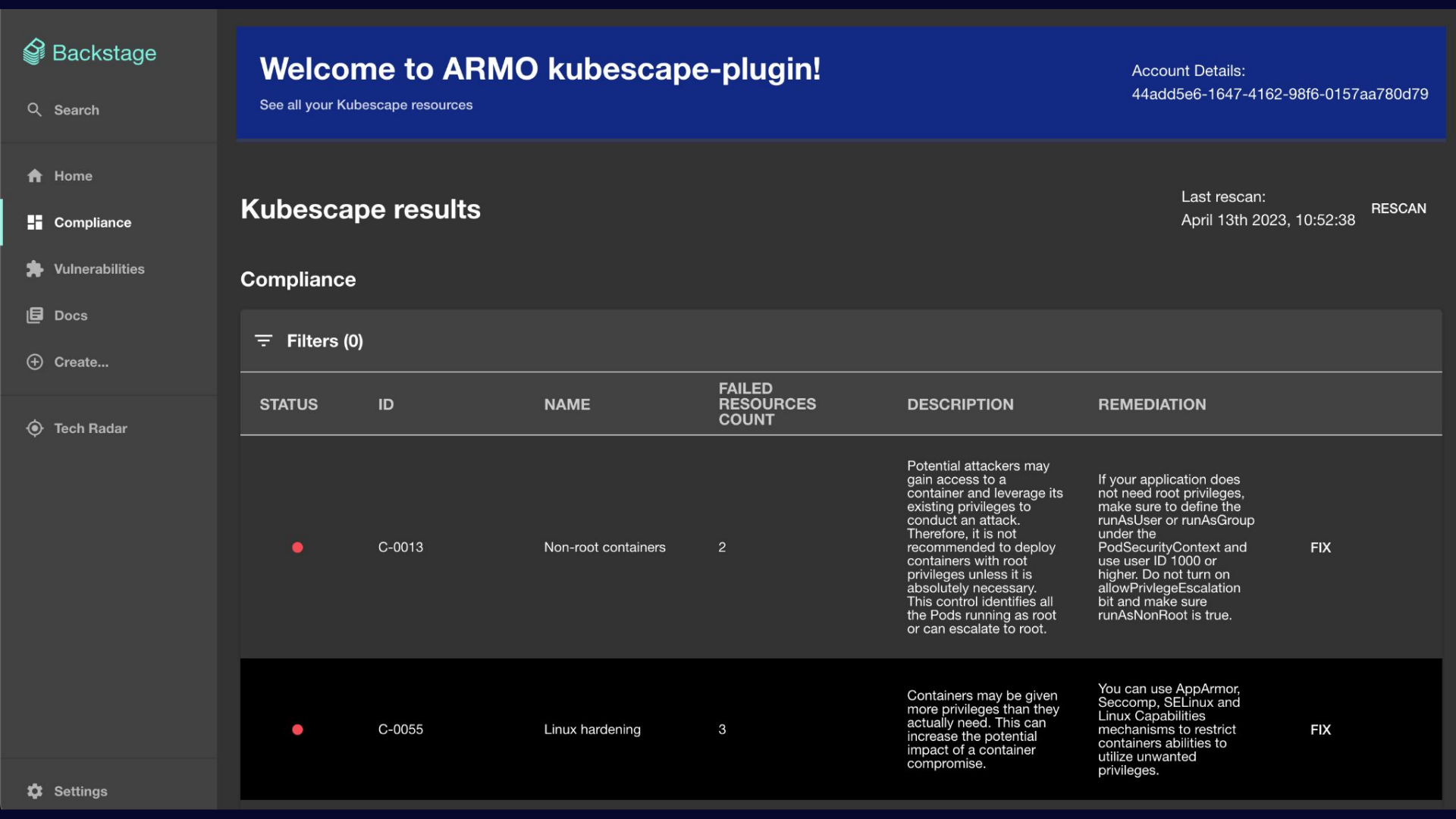

Backstage
Search
Home
Compliance
Vulnerabilities
Docs
Create...
Tech Radar
Settings
Welcome to ARMO kubescape-plugin!
See all your Kubescape resources
Account Details:
44add5e6-1647-4162-98f6-0157aa780d79
Kubescape results
Last rescan:
April 13th 2023, 11:30:53
RESCAN
Compliance
Filters
CLEAR ALL
ID
All results
Name
All results
Filters (0)
STATUS
ID
NAME
FAILED RESOURCES COUNT
DESCRIPTION
REMEDIATION
C-0017
Immutable container filesystem
6
Mutable container filesystem can be abused to inject malicious code or data into containers. Use immutable (read-only) filesystem to limit potential attacks.
Set the filesystem of the container to read-only when possible (POD securityContext, readOnlyRootFilesystem: true). If containers application needs to write into the filesystem, it is recommended to mount secondary filesystems for specific directories where application require write access.
FIX
Configured
Readiness probe is intended to ensure that workload is ready to process network traffic. It is highly recommended
Ensure Readiness


Backstage
Search
Home
Compliance
Vulnerabilities
Docs
Create...
Tech Radar
Settings
Welcome to ARMO kubescape-plugin!
See all your Kubescape resources
Account Details:
44add5e6-1647-4162-98f6-0157aa780d79
Kubescape results
Last rescan:
April 13th 2023, 11:30:53
RESCAN
Compliance
Filters
CLEAR ALL
ID
All results
Name
Resource limits
Filters (1)
STATUS
ID
NAME
FAILED RESOURCES COUNT
DESCRIPTION
REMEDIATION
C-0009
Resource limits
6
CPU and memory resources should have a limit set for every container or a namespace to prevent resource exhaustion. This control identifies all the Pods without resource limit definitions by checking their yaml definition file as well as their namespace LimitRange objects. It is also recommended to use ResourceQuota object to restrict overall namespace resources, but this is not verified by this control.
Define LimitRange and Resource Limits in the namespace or in the deployment/POD yamls.
FIX



Control Resources

Cluster	Namespace	Kind	Name
backstage	prometheus	DaemonSet	prom-prometheus-node-exporter
backstage	prometheus	Deployment	prom-kube-prometheus-stack-operator
backstage	prometheus	StatefulSet	prometheus-prom-kube-prometheus-stack-prometheus
backstage	prometheus	StatefulSet	alertmanager-prom-kube-prometheus-stack-alertmanager
backstage	prometheus	Deployment	prom-grafana
backstage	prometheus	Deployment	prom-kube-state-metrics


Backstage
Search
Home
Compliance
Vulnerabilities
Docs
Create...
Tech Radar
Settings
Welcome to ARMO kubescape-plugin!
See all your Kubescape resources
Account Details:
44add5e6-1647-4162-98f6-0157aa780d79
Kubescape results
Last rescan:
April 13th 2023, 10:52:38
RESCAN
Compliance
Filters (0)
STATUS
ID
NAME
FAILED RESOURCES COUNT
DESCRIPTION
REMEDIATION
C-0013
Non-root containers
2
Potential attackers may gain access to a container and leverage its existing privileges to conduct an attack. Therefore, it is not recommended to deploy containers with root privileges unless it is absolutely necessary. This control identifies all the Pods running as root or can escalate to root.
If your application does not need root privileges, make sure to define the runAsUser or runAsGroup under the PodSecurityContext and use user ID 1000 or higher. Do not turn on allowPrivlegeEscalation bit and make sure runAsNonRoot is true.
FIX
C-0055
Linux hardening
3
Containers may be given more privileges than they actually need. This can increase the potential impact of a container compromise.
You can use AppArmor, Seccomp, SELinux and Linux Capabilities mechanisms to restrict containers abilities to utilize unwanted privileges.
FIX

ARMO
POWERED BY KUBESCAPE

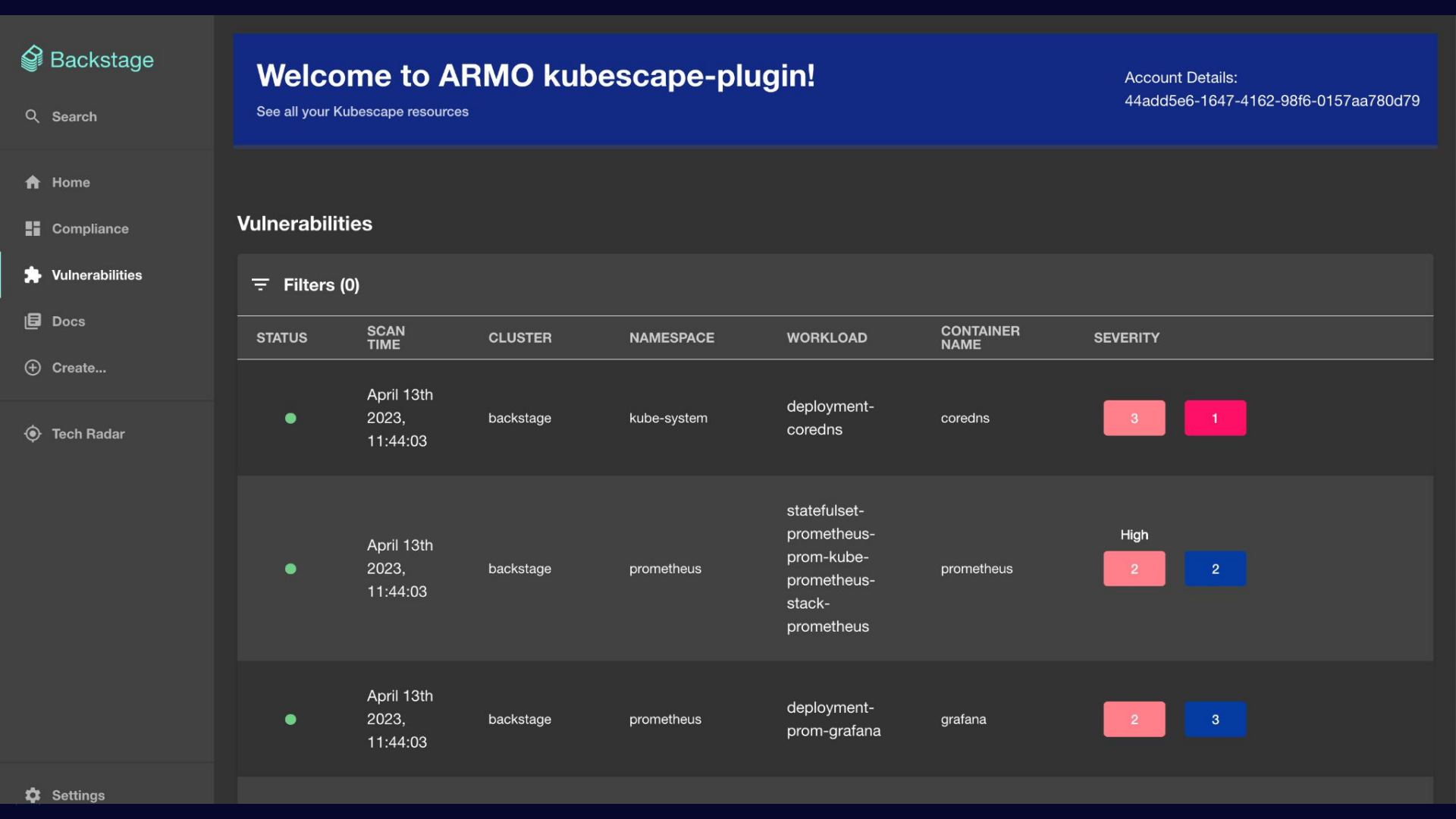
Backstage_kubescape

C-0009

prom-grafana Resource limits

Search (line 186) (line 187) (line 79) (line 80) (line 118) (line 119) Share Copy Object Download Yaml

```
69                     name: prom-grafana
70               - name: REQ_URL
71                 value: XXXXXX
72               - name: REQ_METHOD
73                 value: XXXXXX
74             image: quay.io/kiwigrid/k8s-sidecar:1.22.0
75             imagePullPolicy: IfNotPresent
76             name: grafana-sc-dashboard
77             resources:
78               limits:
79                 cpu: YOUR_VALUE
80                 memory: YOUR_VALUE
81             terminationMessagePath: /dev/termination-log
82             terminationMessagePolicy: File
83             volumeMounts:
84               - mountPath: /tmp/dashboards
85                 name: sc-dashboard-volume
86           - env:
87               - name: METHOD
```


Backstage
Search
Home
Compliance
Vulnerabilities
Docs
Create...
Tech Radar
Settings
Welcome to ARMO kubescape-plugin!
See all your Kubescape resources
Account Details:
44add5e6-1647-4162-98f6-0157aa780d79
Vulnerabilities
Filters (0)
STATUS
SCAN TIME
CLUSTER
NAMESPACE
WORKLOAD
CONTAINER NAME
SEVERITY
April 13th 2023, 11:44:03
backstage
kube-system
deployment-coredns
coredns
3
1
April 13th 2023, 11:44:03
backstage
prometheus
statefulset-prometheus-prom-kube-prometheus-stack-prometheus
prometheus
High
2
2
April 13th 2023, 11:44:03
backstage
prometheus
deployment-prom-grafana
grafana
2
3

/final thoughts

Developer portals are your new best friends!

Developers are shifting right, security is shifting left

Security is yak, but you have to Protect your cluster!

Thank you_

ARMO