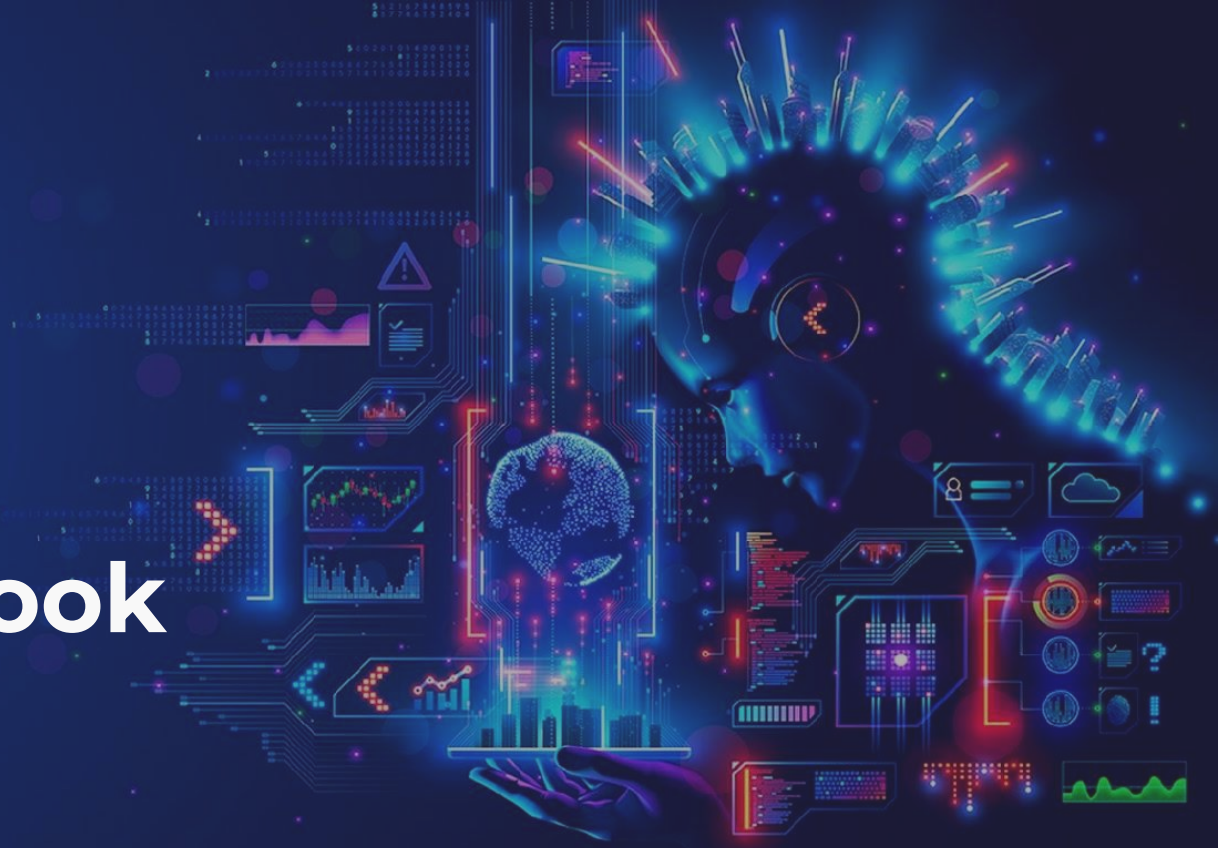
AccuKnox

KSPM Playbook



Introduction to KSPM

AccuKnox

- Detects misconfigurations in Kubernetes clusters.
- Aligns cluster misconfigurations with CIS Kubernetes Benchmarks.
- Visibility into Kubernetes Identity and Entitlement Management (KIEM).
  - Provides graph based view into into Kubernetes identities and RBAC best practices controls
  - Minimizes risks by identifying and managing overprivileged entities.

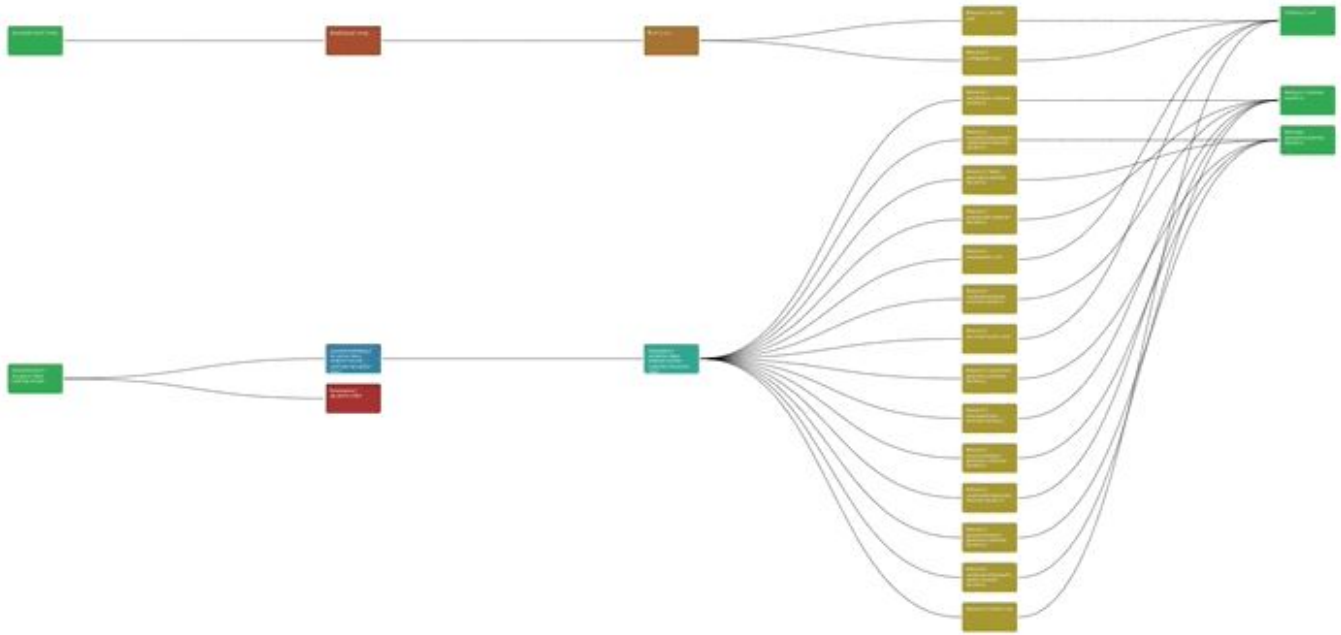
AccuKnox

KIEM

General Filter

Save Current State

128 Principals with privileges on all resources



WhoCan

Key Queries

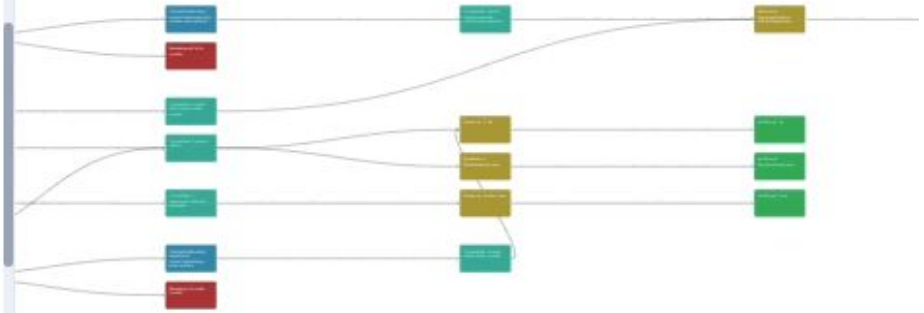
Entity Types

General Fi

Defaut

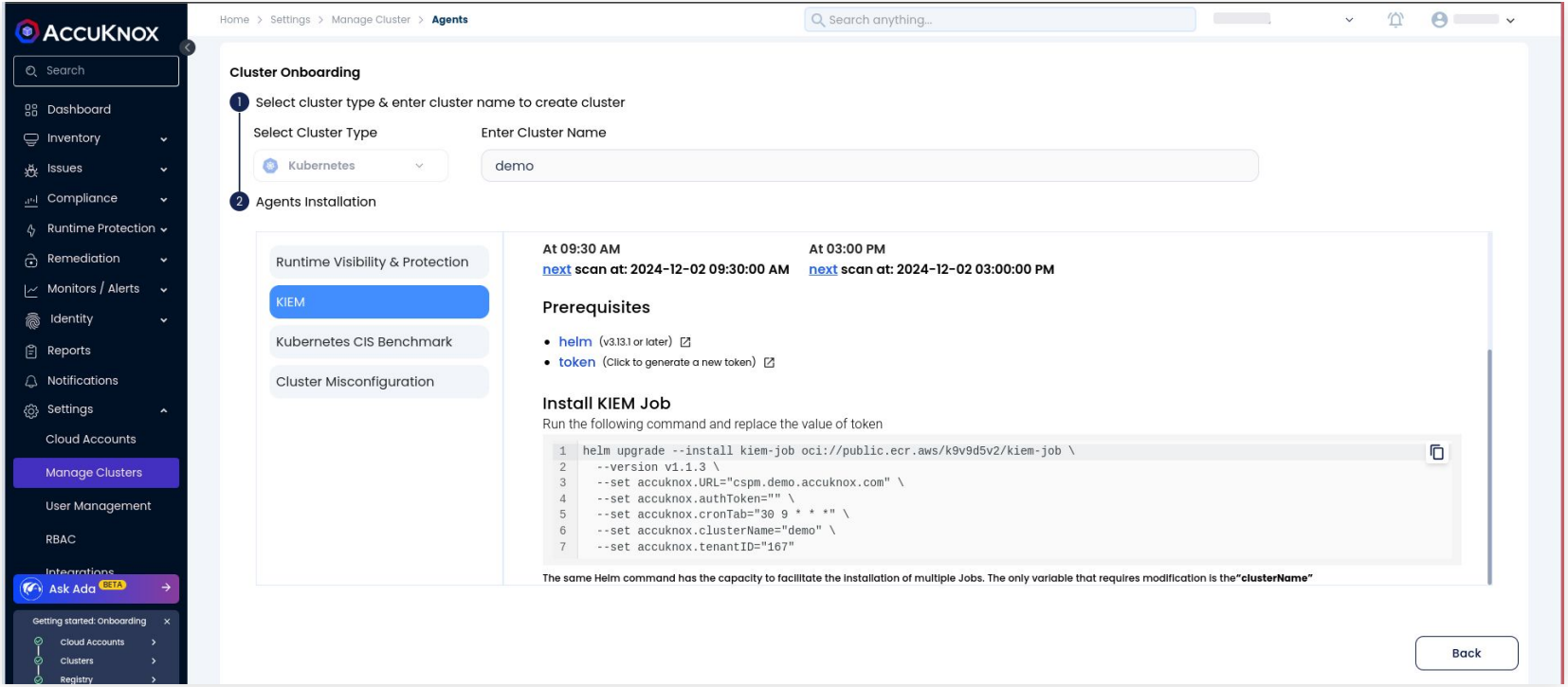
- Service accounts with no workloads
- Principals with high privileges
- Anonymous/unauthenticated users/groups
- Capabilities of default service account
- Container service account mapping
- Principals with privileges on all resources
- Principals with all privileges on a resource

105 Principals with high privileges



KIEM Installation (Agentless)

- Navigate to **Settings**, choose the onboarded cluster, and select **KIEM**.
- Install KIEM helm chart using the commands displayed on the screen.

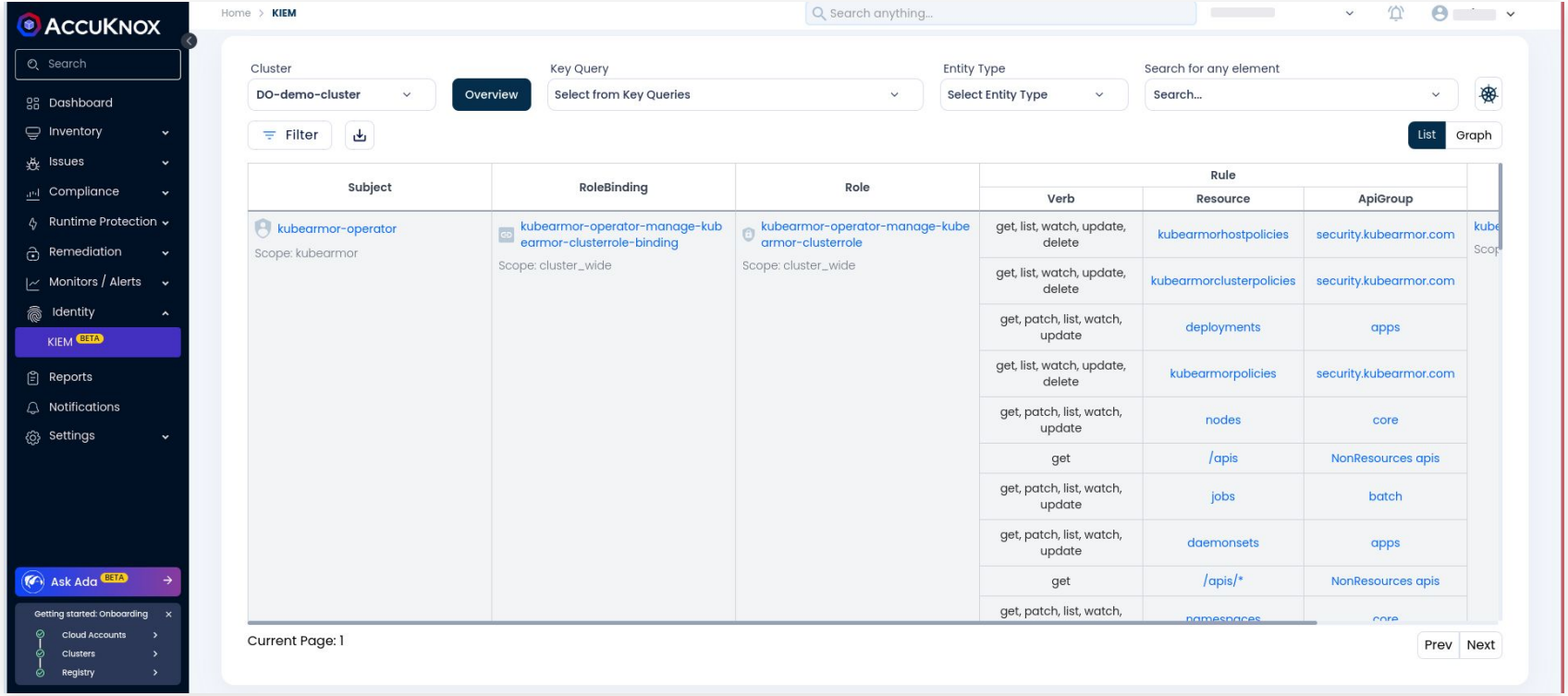


KIEM Graph View

- Navigate to **Identity** → **KIEM** to access the KIEM view.
- Click on **Fullscreen** for a detailed graph view.

KIEM List View

KIEM data can be filtered by cluster, entity type, or queries such as excessive permissions and admin privileges.



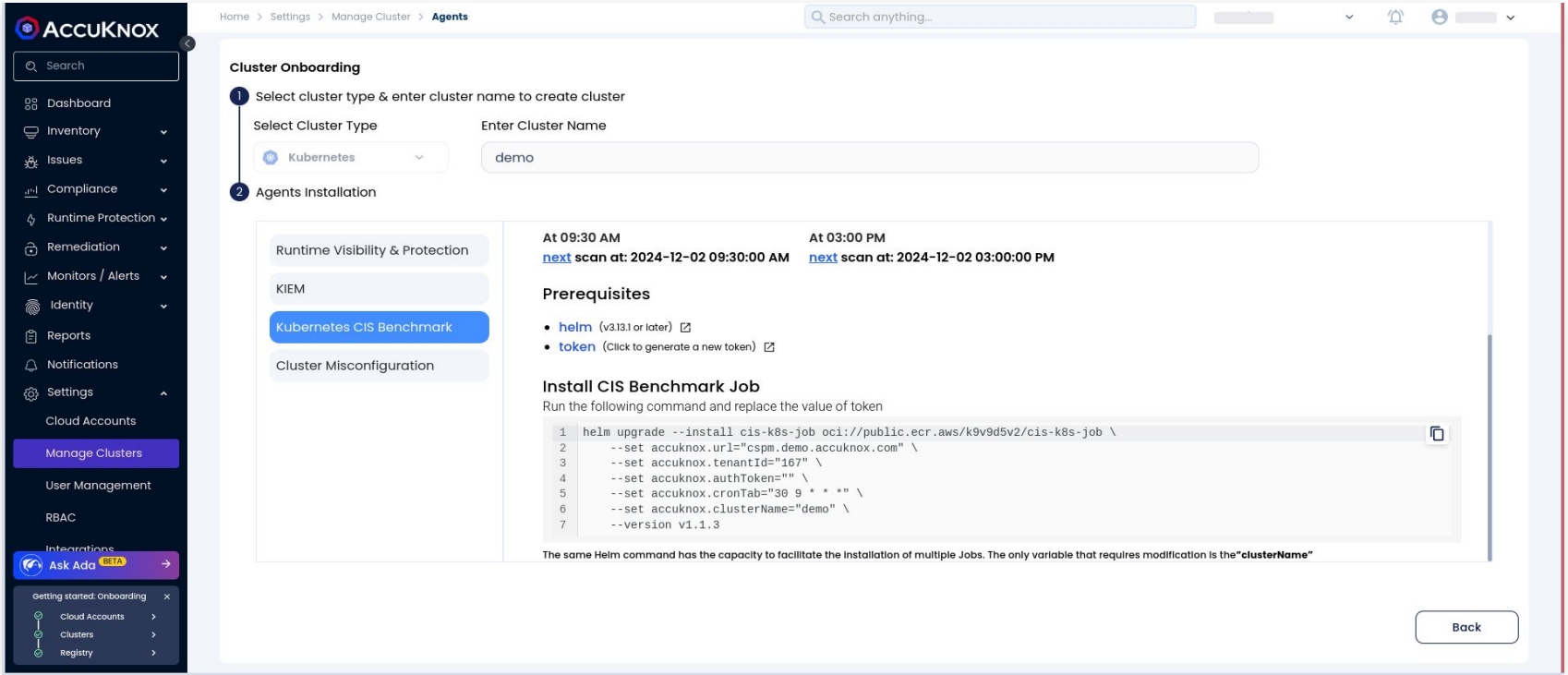
AccuKnox

Kubernetes CIS Benchmark

Kubernetes CIS Benchmark (Agentless)

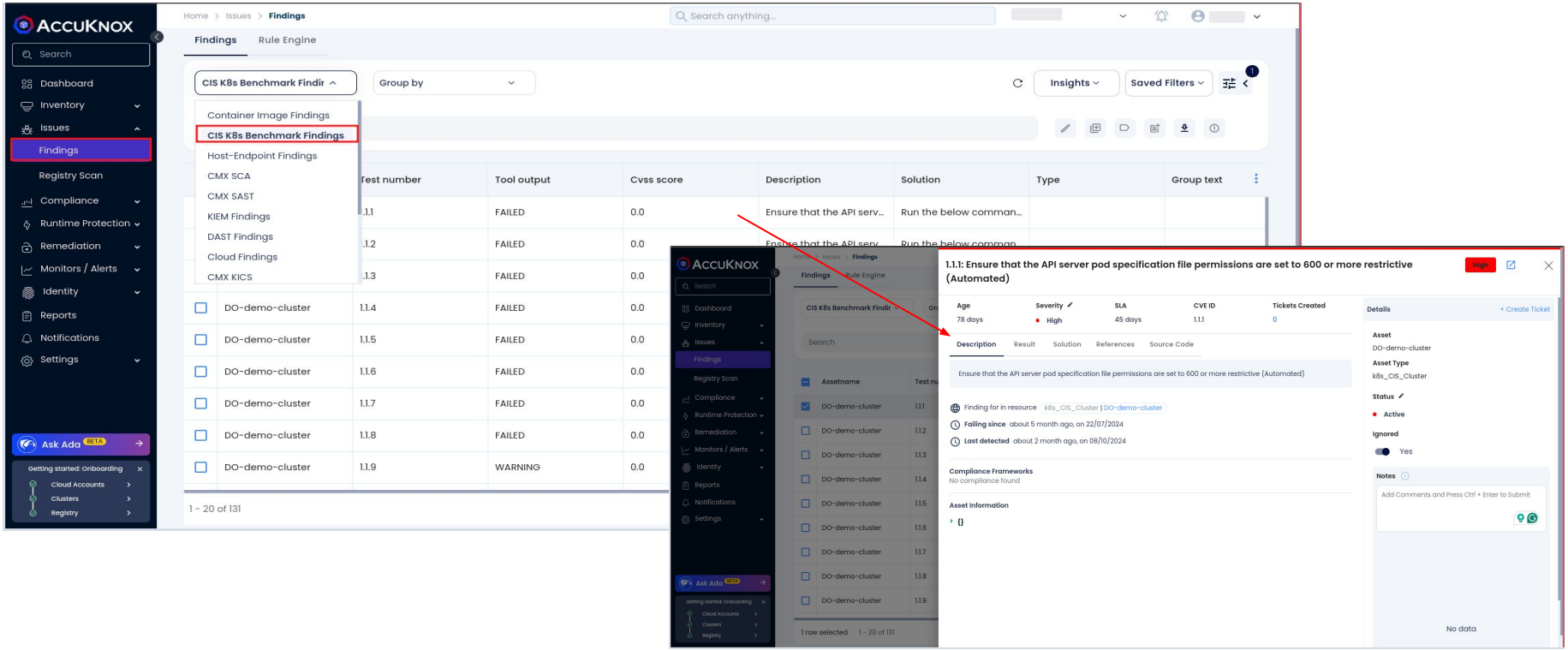
ACCUKNOX

- Navigate to **Settings**, choose the onboarded cluster, and select **Kubernetes CIS Benchmark**.
- Install the helm chart using the commands displayed on the screen.



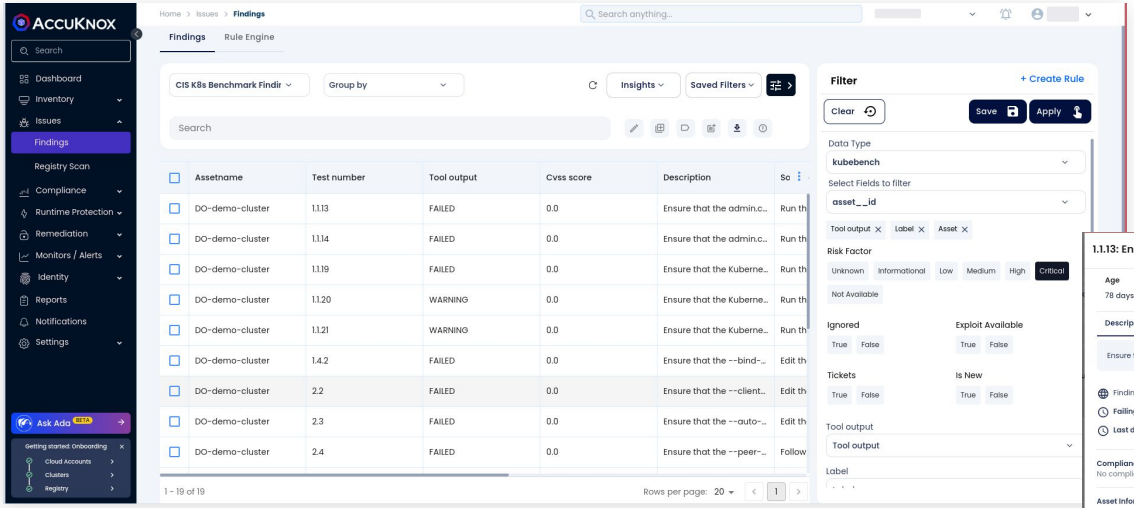
View Findings

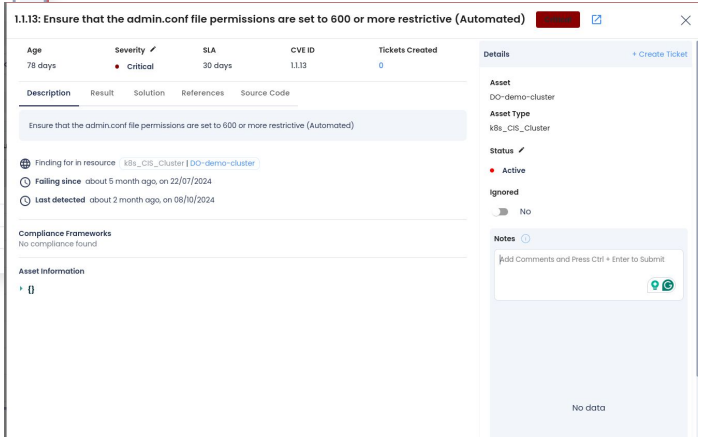
- View the findings on the **Findings** page. Select the **CIS k8s Benchmark Findings** to access the relevant details.



Work on Critical Findings

- Select Group By as Findings
- In the Filters tab, select Critical under Risk Factor and click on Apply





- Click on any of the findings for details, click on Create Ticket button to generate tickets

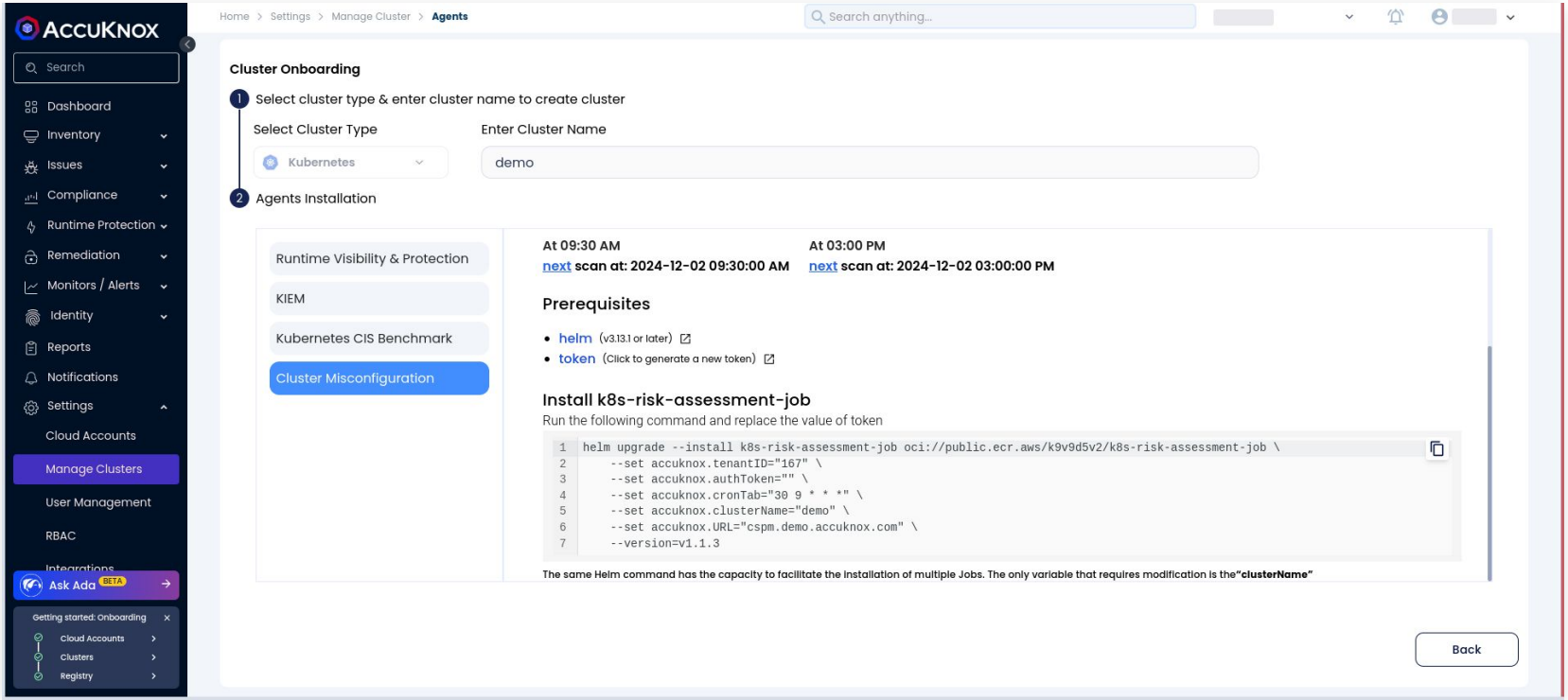
AccuKnox

Cluster Misconfiguration

Cluster Misconfiguration (Agentless)

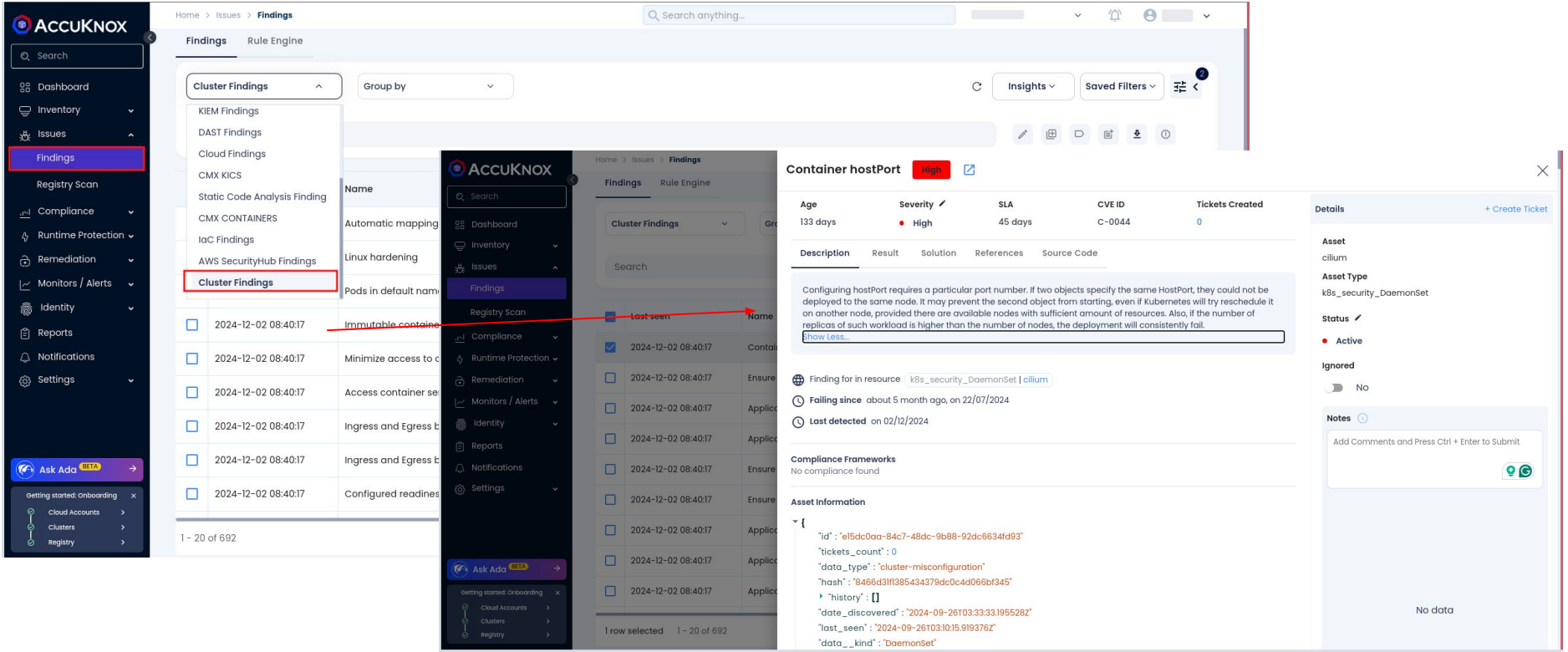
ACCUKNOX

- Navigate to **Settings**, choose the onboarded cluster, and select **Cluster Misconfiguration**.
- Install the helm chart using the commands displayed on the screen.



View Findings

- View the findings on the **Findings** page. Select the **CIS k8s Benchmark Findings** to access the relevant details.

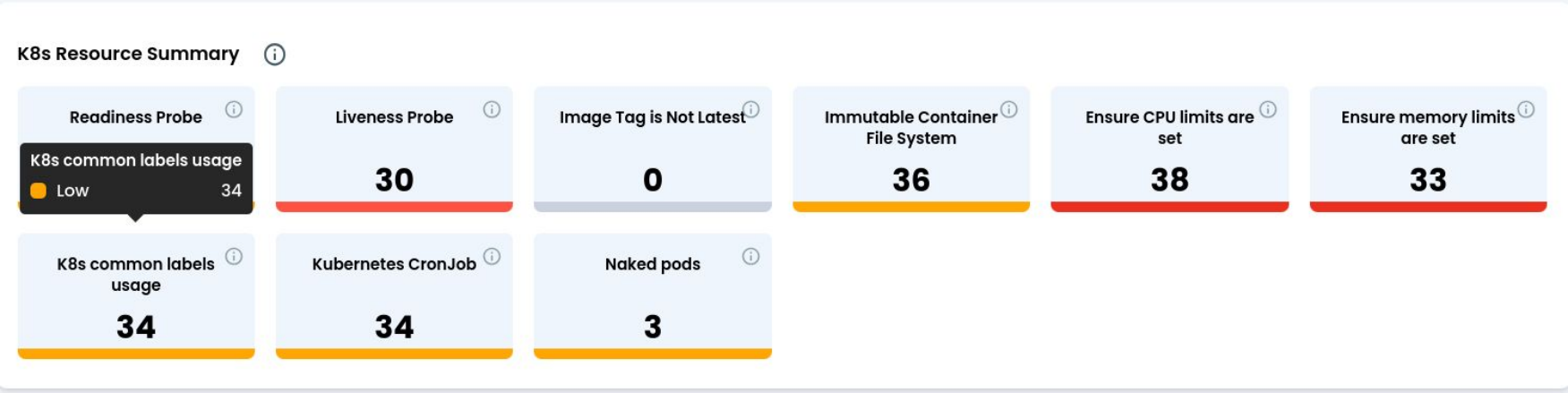


AccuKnox

KSPM Customized Dashboard & Reporting Metrics

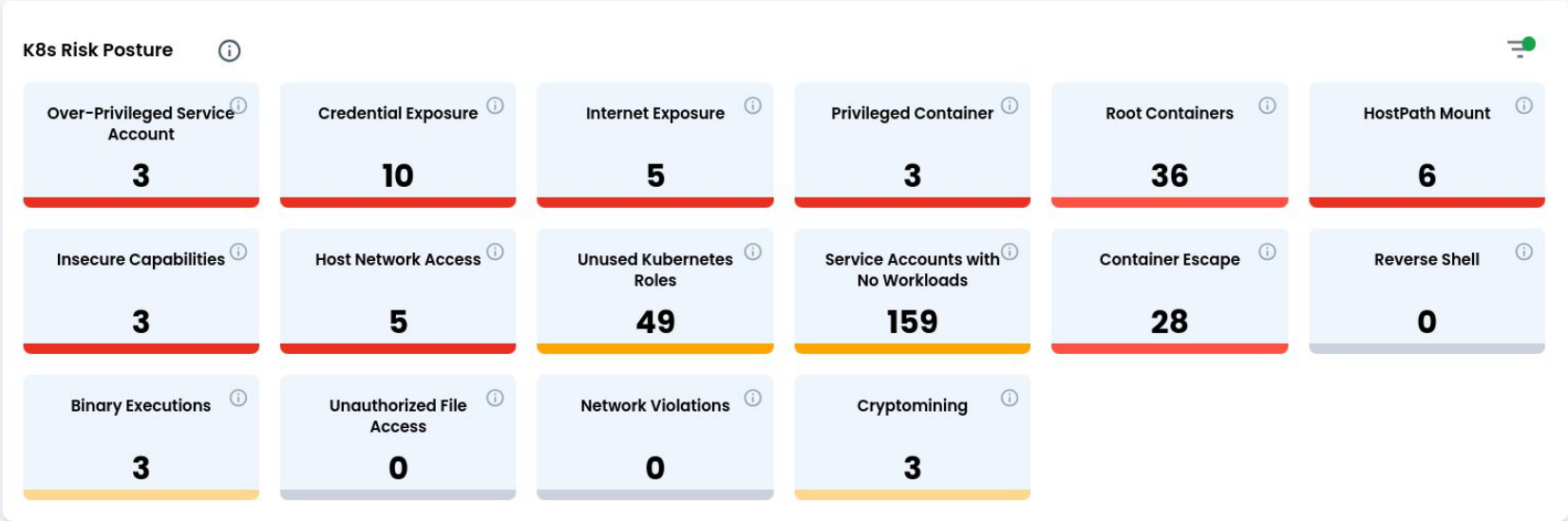
Resource Metrics Widgets [1]

ACCUKNOX



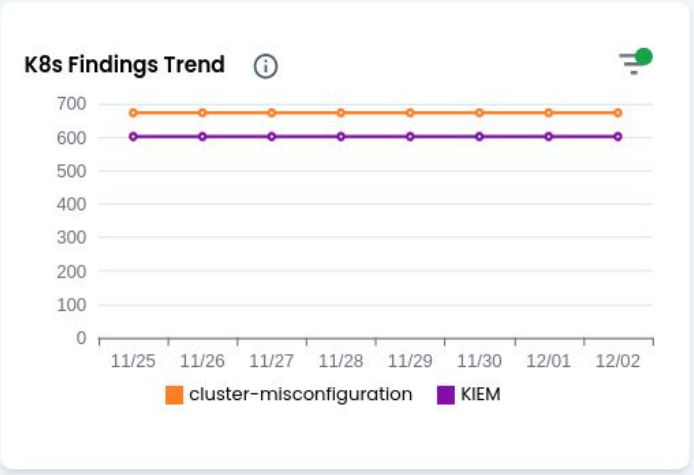
Security Risk Metrics Widgets [2]

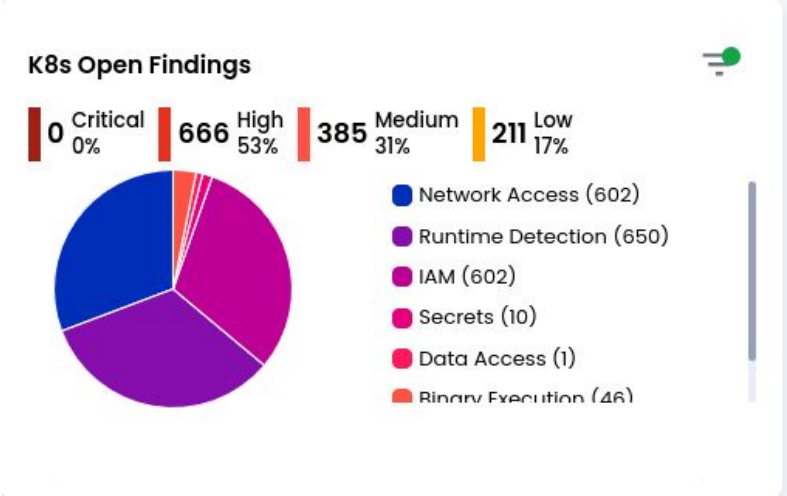
ACCUKNOX

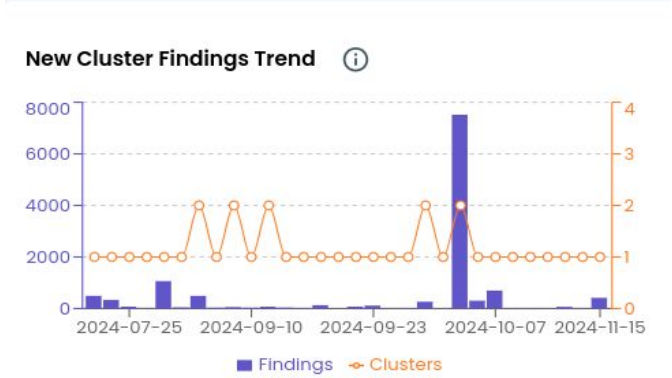


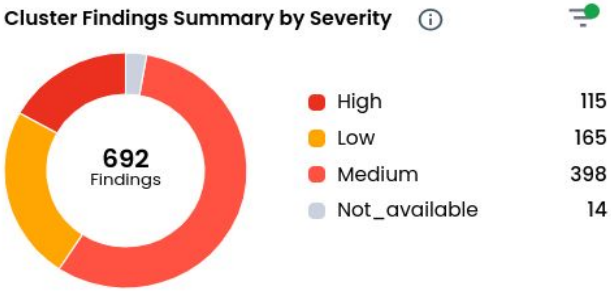
K8s Risk Overview - Widgets [3]

ACCUKNOX



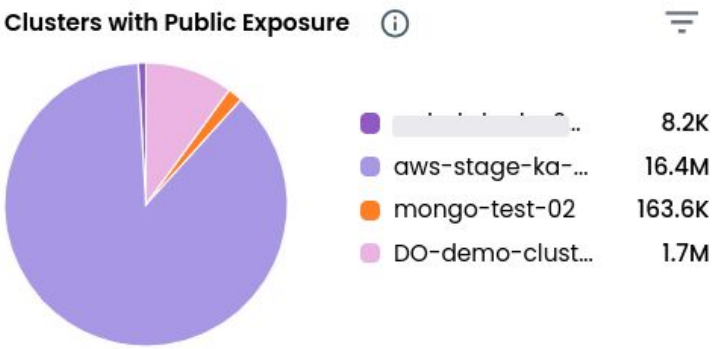


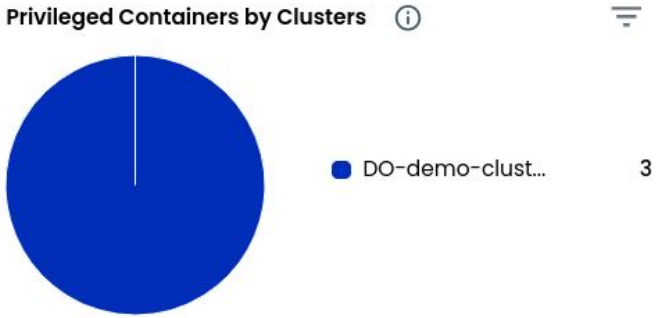


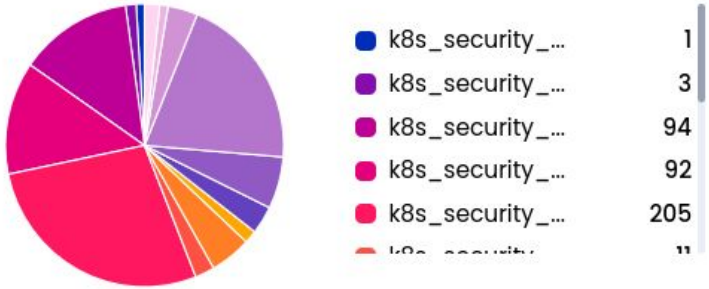


Cluster Wide Risk - Widgets [4]

ACCUKNOX



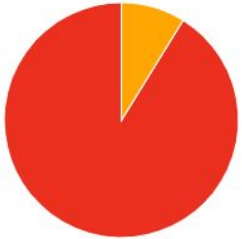




KIEM Widgets [5]

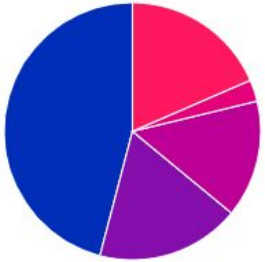
ACCUKNOX

KIEM Risk Assessment



High	553
Low	49

KIEM Findings by Asset Types



KIEM_Clusterr...	1.0K
KIEM_Clusterr...	394
KIEM_Role	317
KIEM_Rolebind...	43
KIEM_Servicea...	403

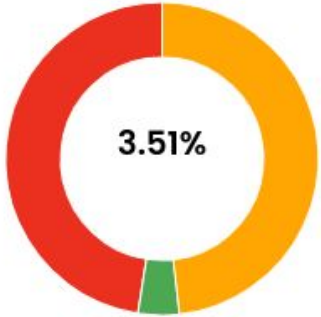
Top 5 Most Critical Findings

Permission to access different namespace	227
Service accounts with no workloads	159
Permission to Delete and Access ConfigMaps,PersistentVolumeClaims	71
Permission to modify workloads	32
Permission to read/list Secrets	27

CIS Compliance - Widgets [6]

ACCUKNOX

K8s CIS Compliance Status



Total Count
570

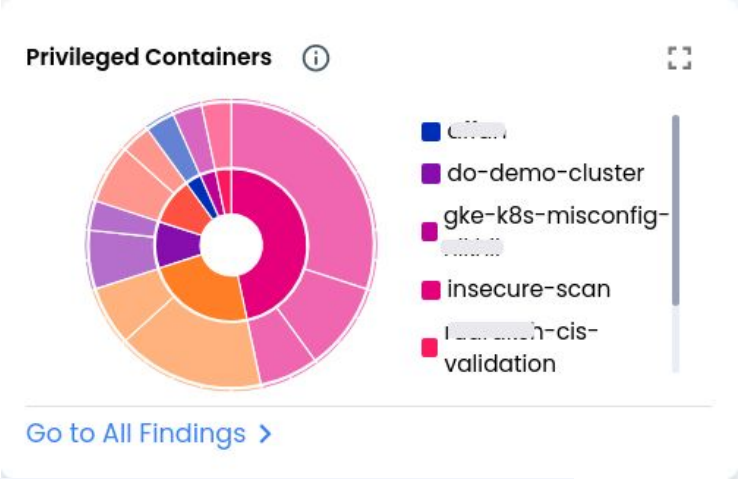
FAILED	273
PASSED	20
WARNING	277

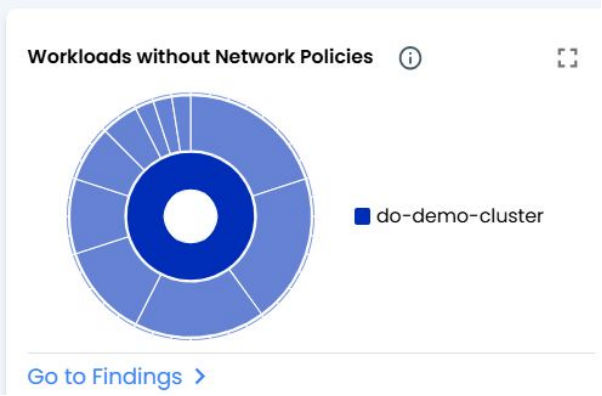
Top 5 K8s CIS Findings

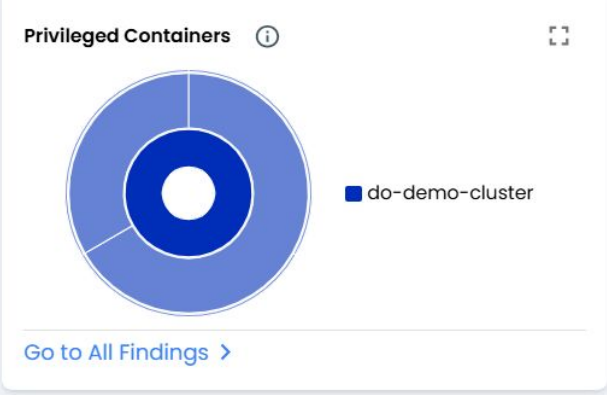
Finding Name	Assets Impacted
2.5: Ensure that the --peer-client-cert-auth arg...	5
2.4: Ensure that the --peer-cert-file and --peer...	5
2.3: Ensure that the --auto-tls argument is not s...	5
2.2: Ensure that the --client-cert-auth argumen...	5
1.4.2: Ensure that the --bind-address argument ...	5

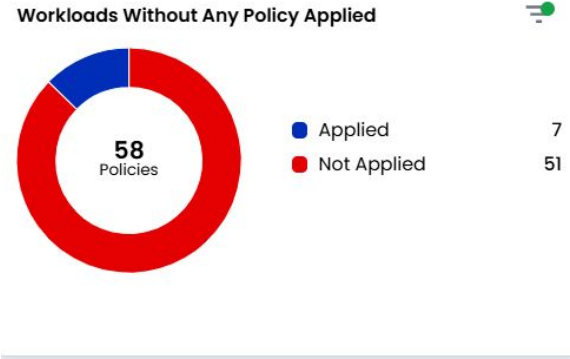
Container Specific Risk - Widgets [7]

ACCUKNOX









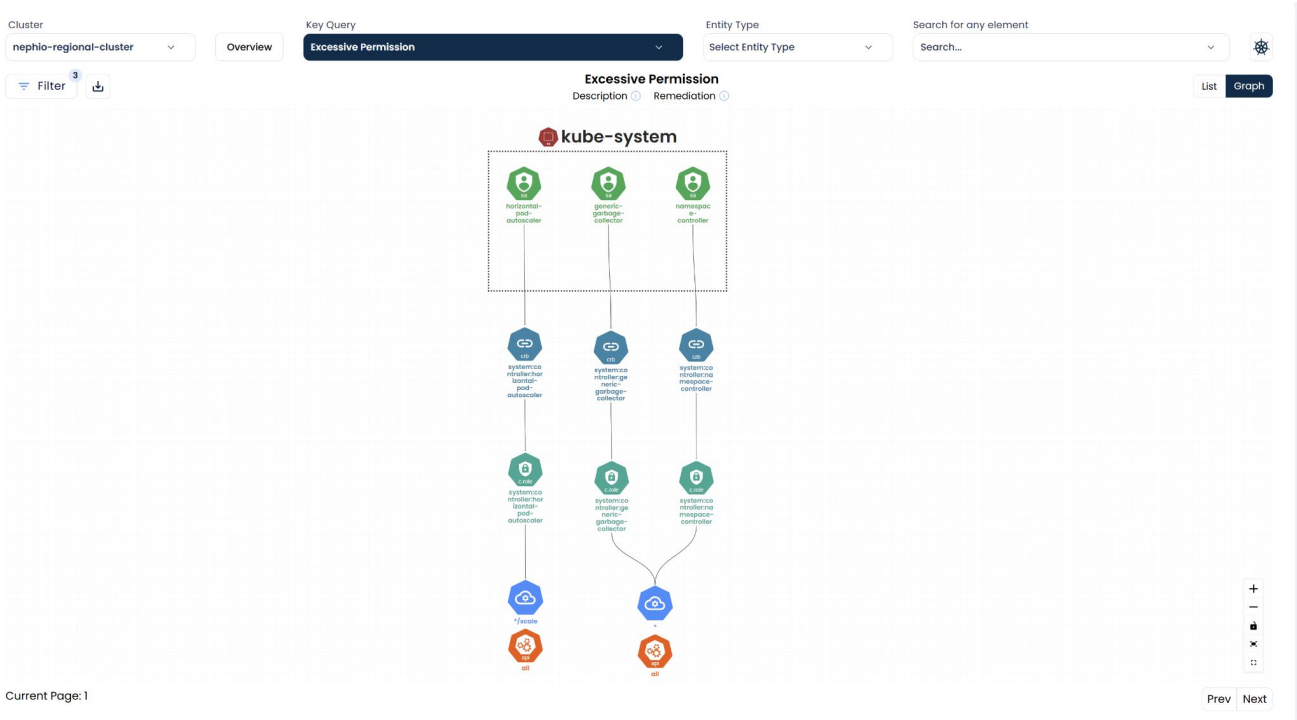
AccuKnox

KSPM Use Cases

KIEM Use Case: Excessive Permissions in Kubernetes

ACCUKNOX

- A Kubernetes service account or role has excessive permissions, increasing the risk of privilege escalation.



KIEM Use Case: List View (continued)

ACCUKNOX

- **AccuKnox recommends** minimizing permissions by enforcing least privilege, avoiding wildcards, restricting namespaces, and using RBAC with narrowly defined roles.

Cluster: DO-demo-cluster | Overview | Key Query: Excessive Permission | Entity Type: Select Entity Type | Search for any element: Search...

Filter 3

Excessive Permission

Description Remediation

List Graph

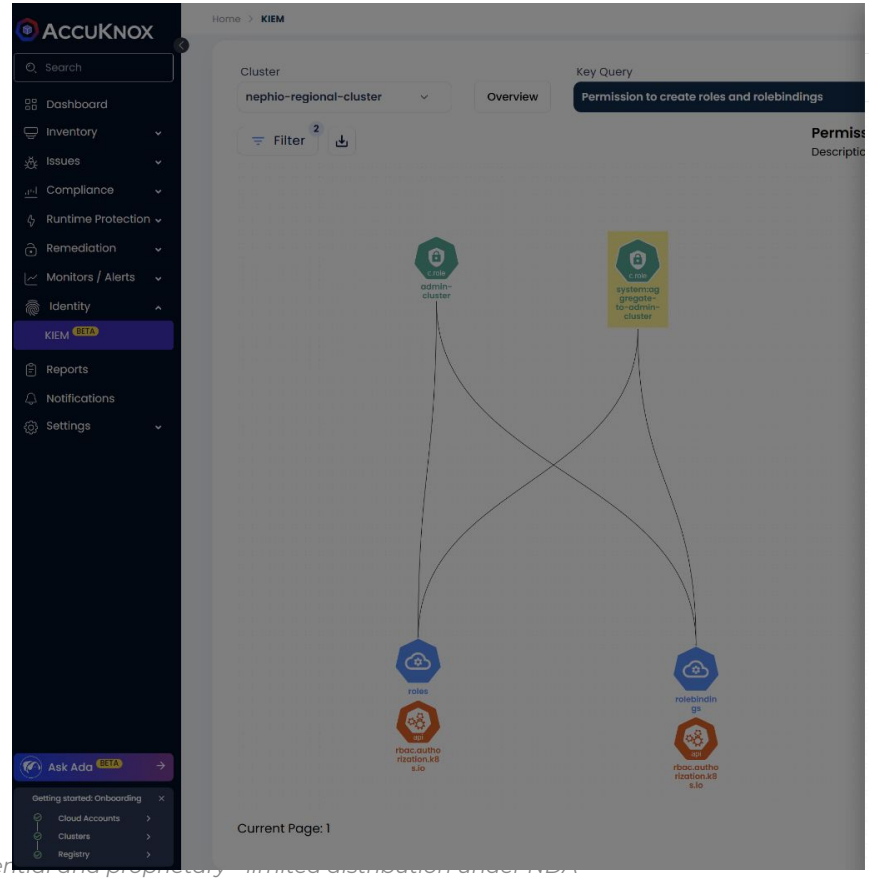
Subject	RoleBinding	Role	Rule			Workload
			Verb	Resource	ApiGroup	
namespace-controller Scope: kube-system	system:controller:namespace-controller Scope: cluster_wide	system:controller:namespace-controller Scope: cluster_wide	delete, deletecollection, get, list	*	all	-
horizontal-pod-autoscaler Scope: kube-system	system:controller:horizontal-pod-autoscaler Scope: cluster_wide	system:controller:horizontal-pod-autoscaler Scope: cluster_wide	get, update	*/scale	all	-
generic-garbage-collector Scope: kube-system	system:controller:generic-garbage-collector Scope: cluster_wide	system:controller:generic-garbage-collector Scope: cluster_wide	delete, get, list, patch, update, watch	*	all	-

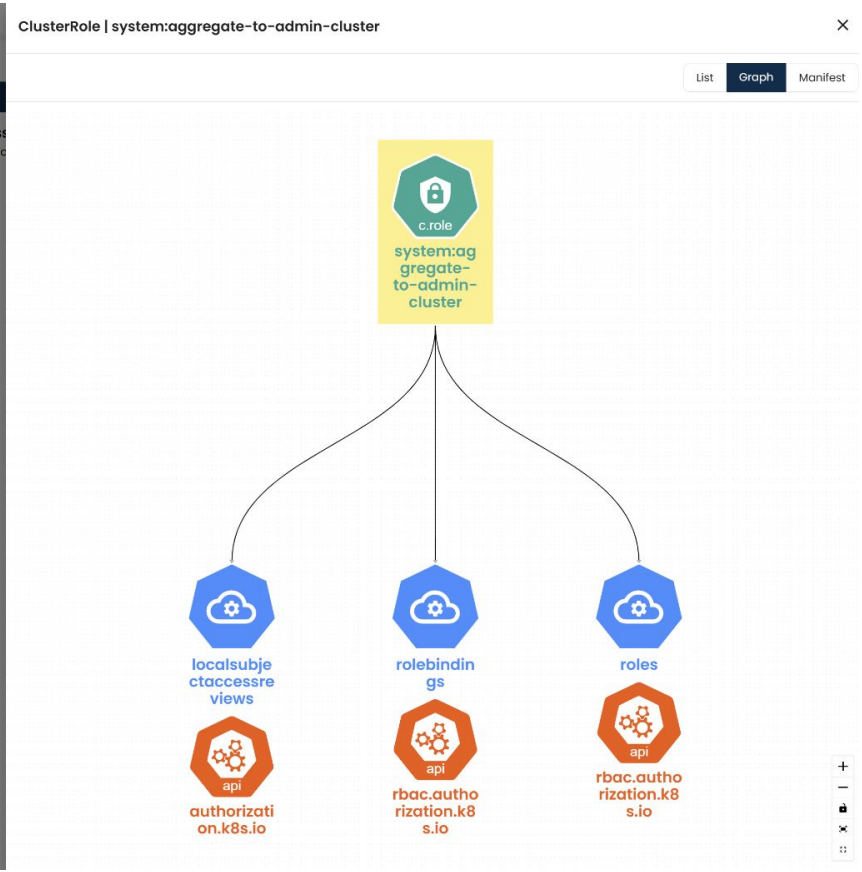
Current Page: 1

Prev Next

KIEM: Permission to create Roles & RoleBindings

ACCUKNOX





KIEM: Track KIEM findings identified by filters

ACCUKNOX

Home > Issues > Findings

Findings | Rule Engine

KIEM Findings | Group by | Insights | Saved Filters

Last seen	Assetname	Name	Risk factor	Description	Cluster
2025-01-09 15:00:32	admin-cluster	Permission to create roles and role...	High	This permission alhugh...	DO-demo-
2025-01-09 15:00:32	snapshot-controller-role	Permission to access different nam...	High	This permission allows ...	DO-demo-

21 - 40 of 2214

Permission to create roles and rolebindings

High

Age	Severity	SLA	CVE ID	Tickets Created
126 days	High	45 days	NA	0

Description | Result | Solution | References | Source Code

This permission alhughs users to define new roles and role bindings, which can lead to privilege escalation if not managed carefully. A user with this ability can potentially grant themselves or others permissions beyond their current level...
Show More...

Finding for in resource KIEM_Clusterrole | admin-cluster

Failing since about 1 year ago, on 06/09/2024

Last detected about 1 day ago, on 09/01/2025

Compliance Frameworks
No compliance found

Details + Create Ticket

Asset
admin-cluster

Asset Type
KIEM_Clusterrole

Status
Active

Ignored
No

Notes
Add Comments and Press Ctrl + Enter to Submit

CIS Benchmarking Use Case: etcd Directory Permissions

ACCUKNOX

- Ensure etcd data directory permissions are set to 700 or more restrictive.
- AccuKnox identifies the vulnerability and proposes a solution.

1.1.11: Ensure that the etcd data directory permissions are set to 700 or more restrictive (Automated) High

Age	Severity	SLA	CVE ID	Tickets Created
78 days	High	45 days	1.1.11	0

Description | Result | Solution | References | Source Code

On the etcd server node, get the etcd data directory, passed as an argument --data-dir, from the command 'ps -ef | grep etcd'.
Run the below command (based on the etcd data directory found above). For example,
chmod 700 /var/lib/etcd

Details + Create Ticket

Asset
DO-demo-cluster

Asset Type
k8s_CIS_Cluster

Status
Active

Ignored
No

Notes
Add Comments and Press Ctrl + Enter to Submit

Cluster Misconfig Use Case: Anonymous Access Enabled

ACCUKNOX

- Enabling anonymous access exposes the cluster to unauthorized access.
- **AccuKnox recommends**: Review and adjust your cluster's RBAC to ensure only authenticated, authorized users have the appropriate permissions.

Anonymous access enabled High

Age	Severity	SLA	CVE ID	Tickets Created
133 days	High	45 days	C-0262	0

Description | Result | Solution | References | Source Code

Granting permissions to the system:unauthenticated or system:anonymous user is generally not recommended and can introduce security risks. Allowing unauthenticated access to your Kubernetes cluster can lead to unauthorized access, potential...
Show More...

Finding for in resource k8s_security_ClusterRoleBinding | system:public-info-viewer

Failing since about 5 month ago, on 22/07/2024

Last detected on 02/12/2024

Compliance Frameworks
No compliance found

Asset Information


```
{
    "id" : "a5786576-44b2-4005-ae70-525ded44d090"
    "tickets_count" : 0
    "data_type" : "cluster-misconfiguration"
    "hash" : "8012037be364cd54735e347b65c888e8"
    "history" : []
    "date_discovered" : "2024-09-14T03:10:14.578184Z"
    "last_seen" : "2024-09-26T03:10:15.919376Z"
    "data__kind" : "ClusterRoleBinding"
    "data__roleRef" : {
        "kind" : "ClusterRole"
        "name" : "system:public-info-viewer"
        "apiGroup" : "rbac.authorization.k8s.io"
    }
```


Details + Create Ticket

Asset
system:public-info-viewer

Asset Type
k8s_security_ClusterRoleBinding

Status
Active

Ignored
No

Notes
Add Comments and Press Ctrl + Enter to Submit

No data