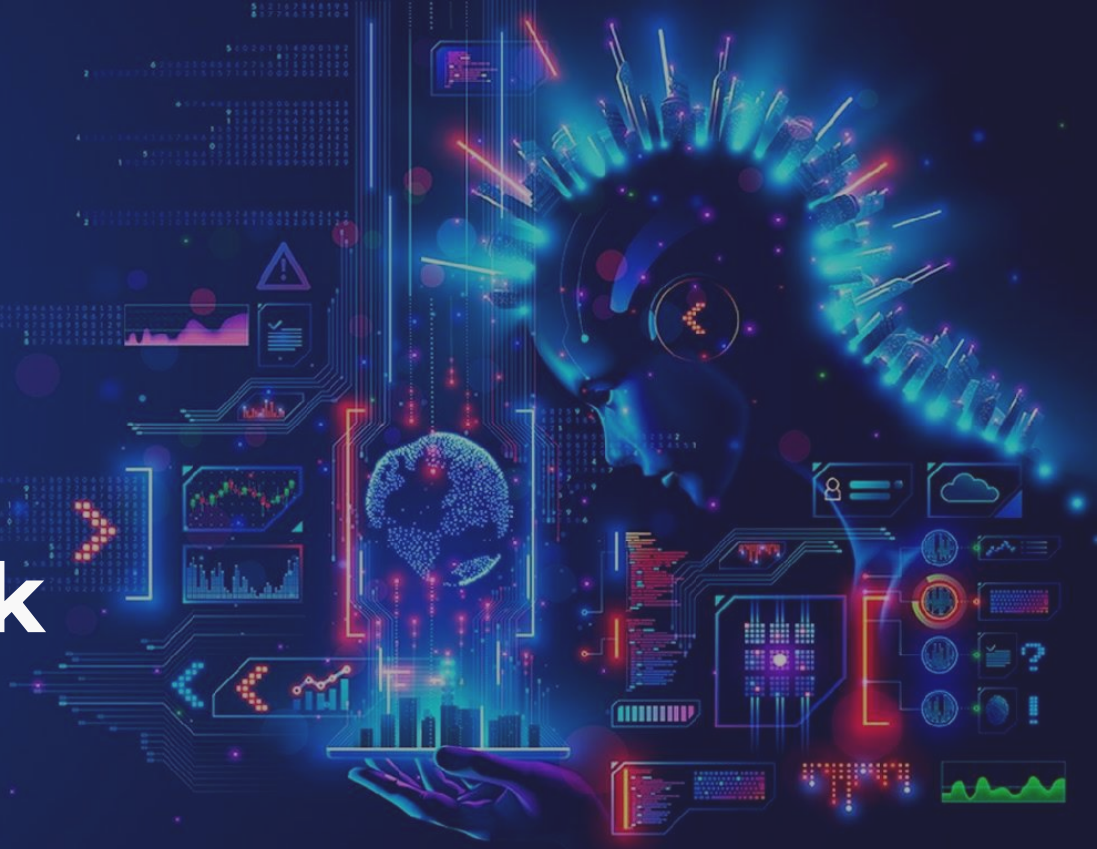
AccuKnox

KSPM Playbook

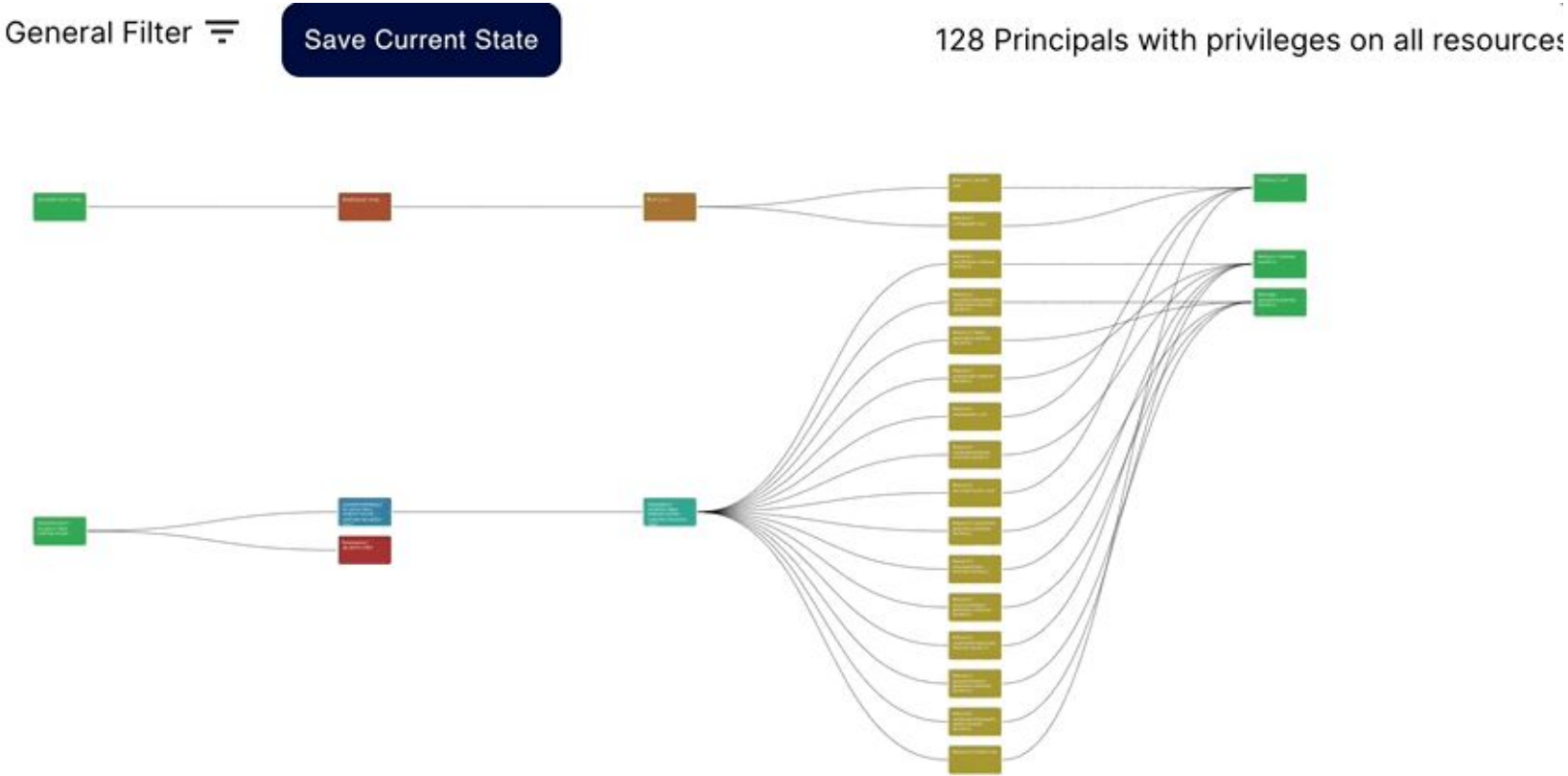


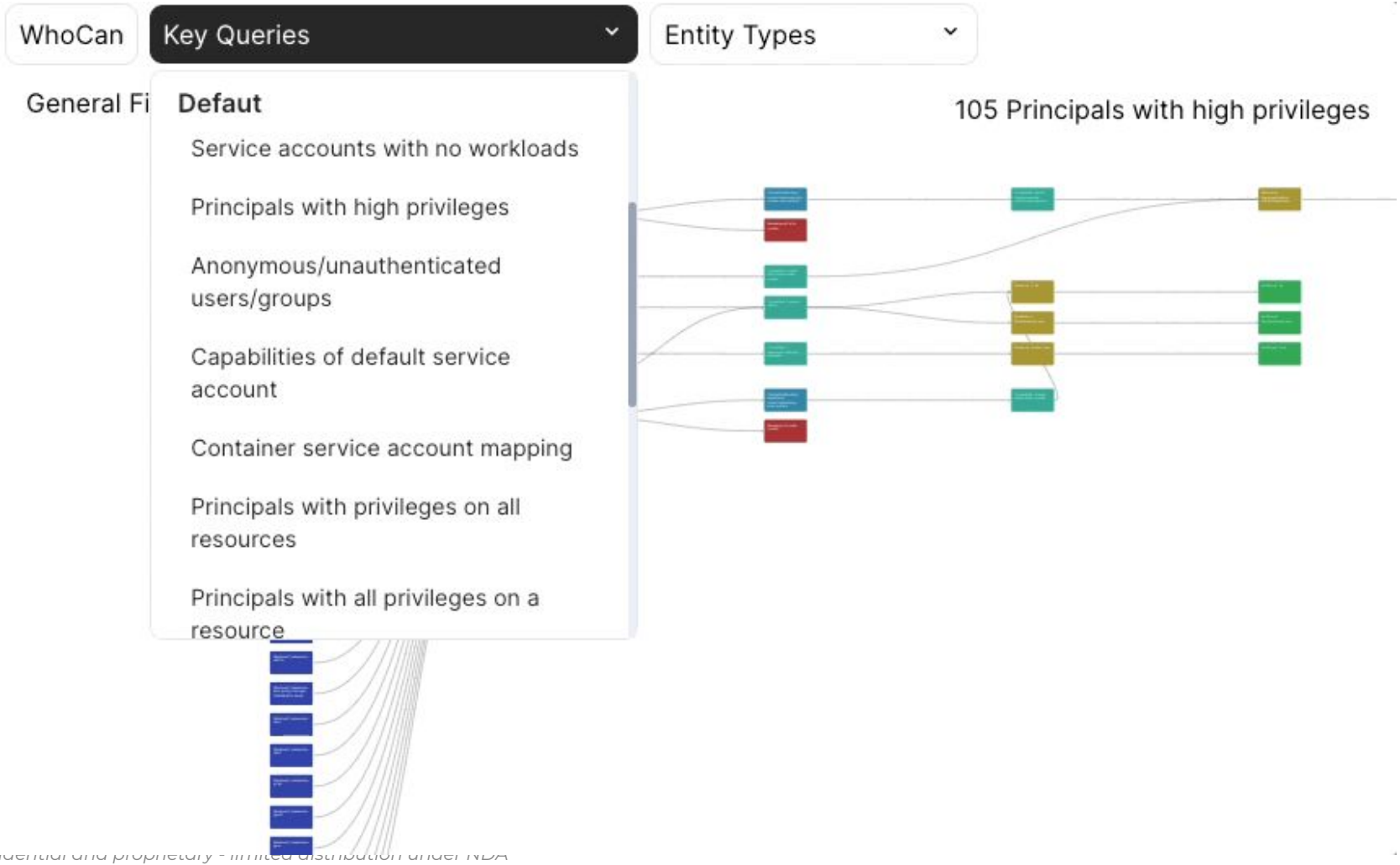
Introduction to KSPM

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.

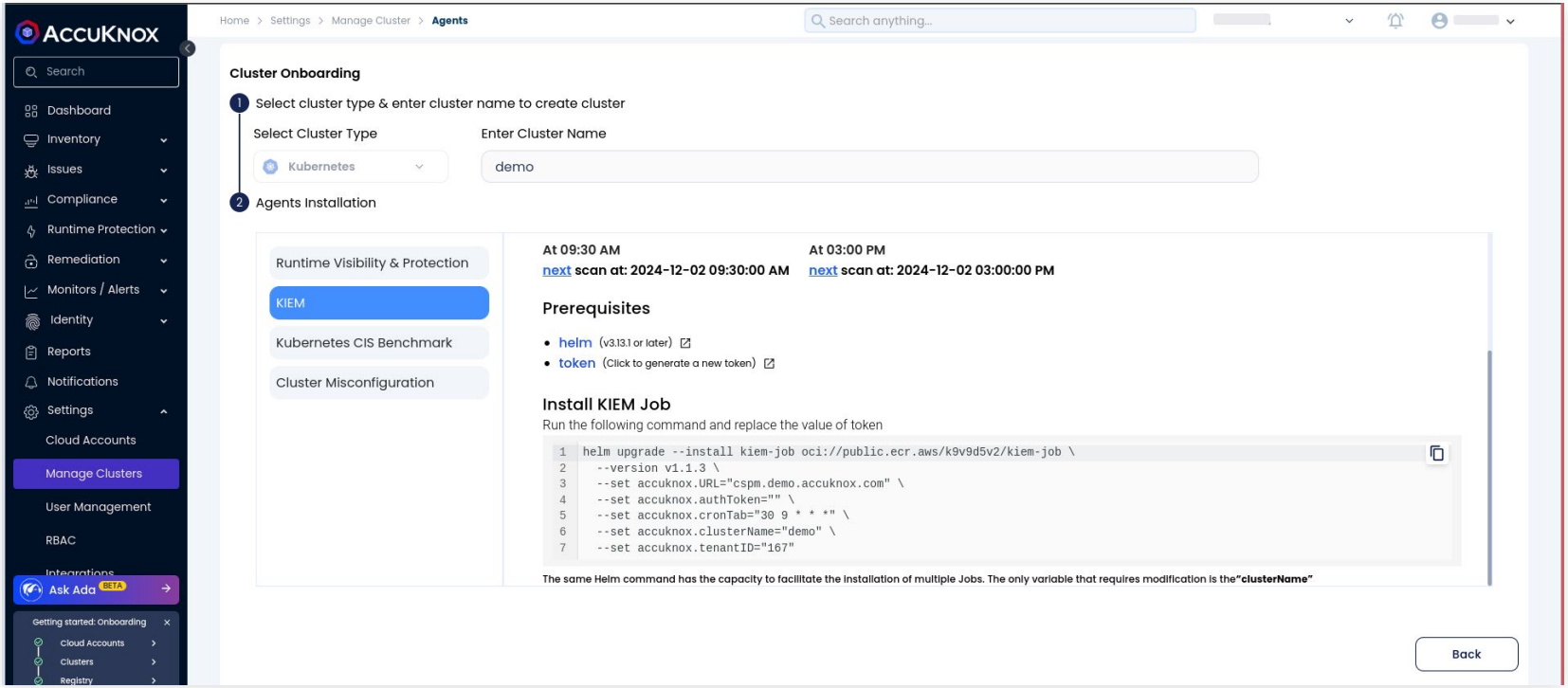
KIEM





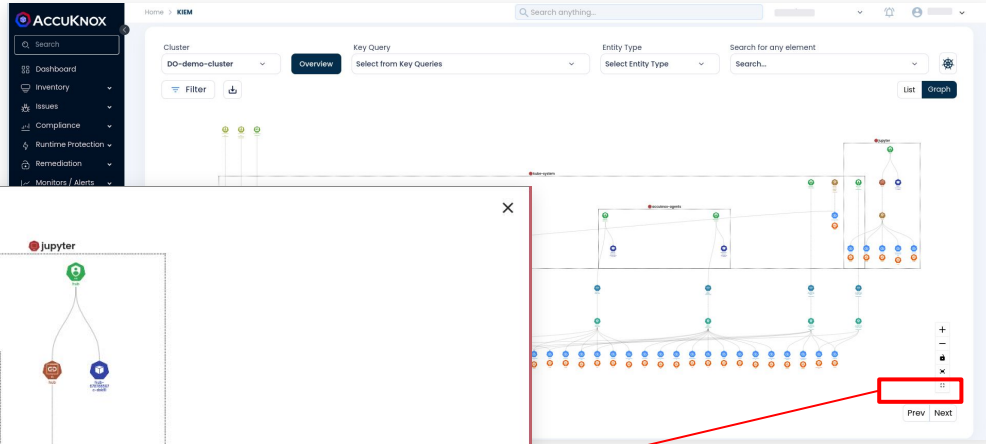
KIEM Installation (Agentless)

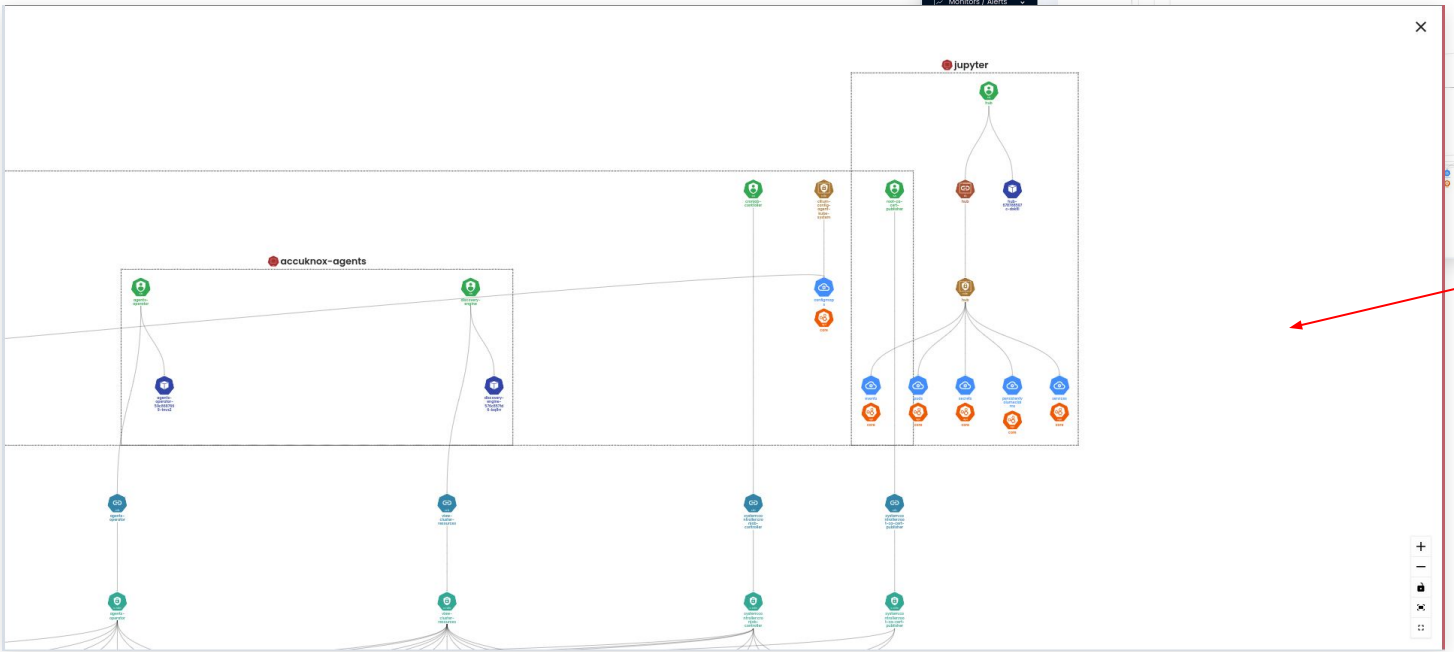
- Navigate to **Settings**, choose the onboarded cluster, and select **KIEM**.
- Install KIEM helm chart using the commands displayed on the screen.



KIEM Graph View

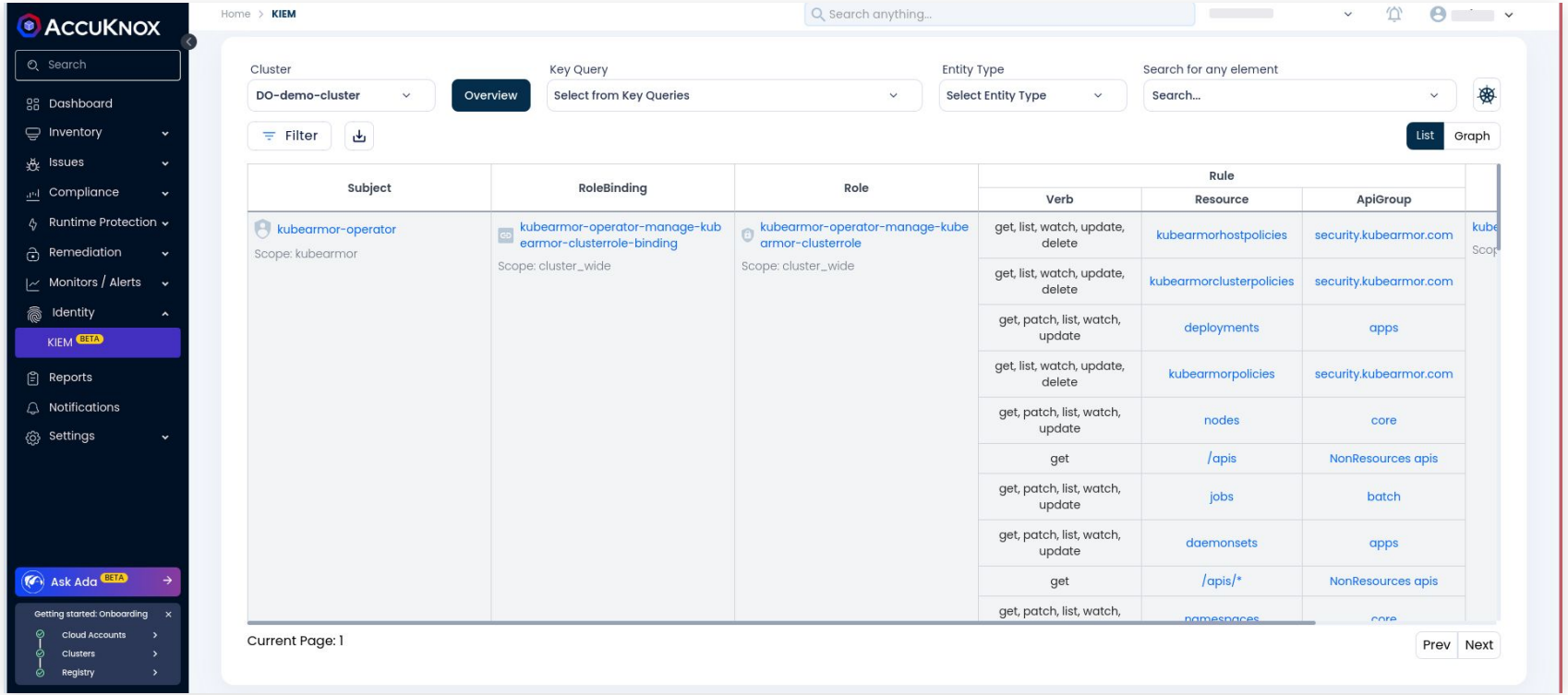
- Navigate to **Identity** → **KIEM** to access the KIEM view.
- Click on **Fullscreen** for a detailed graph view.





KIEM List View

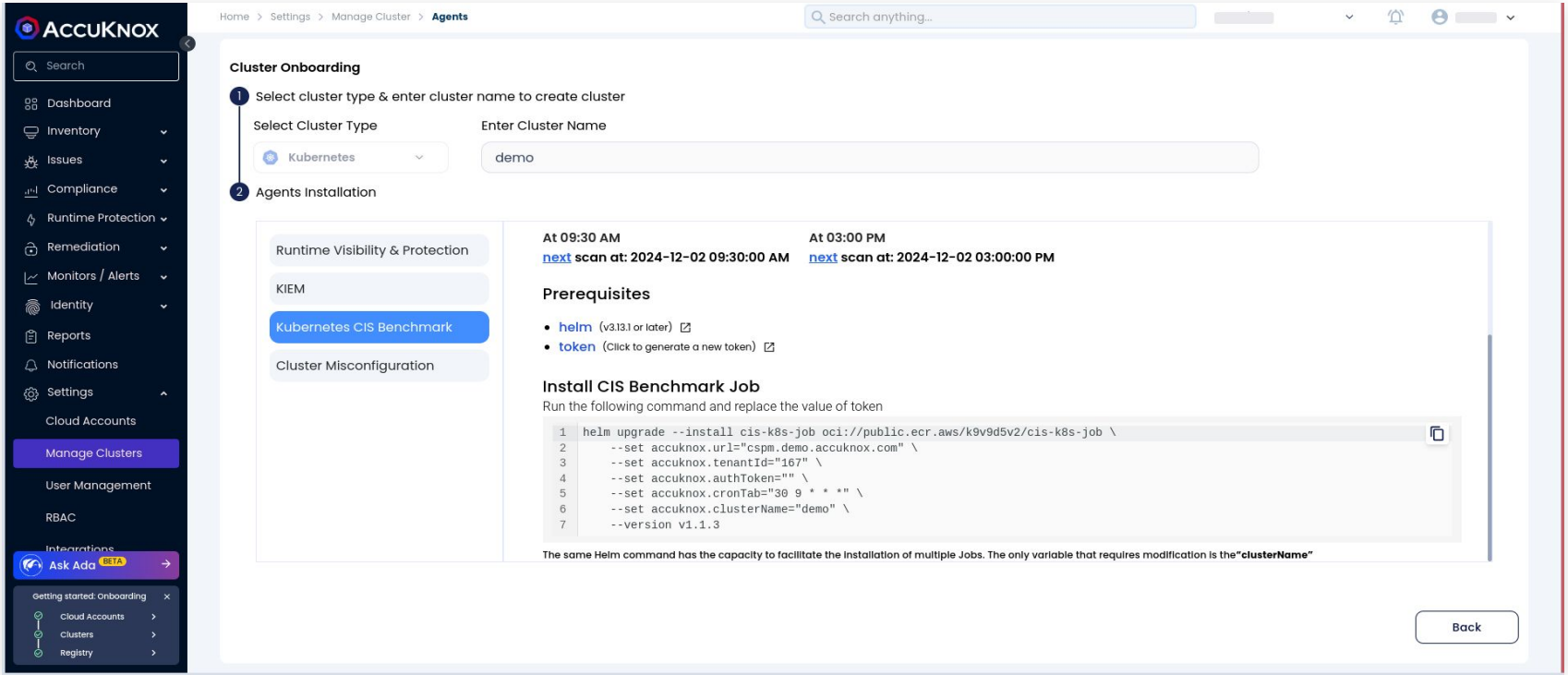
KIEM data can be filtered by cluster, entity type, or queries such as excessive permissions and admin privileges.



Kubernetes CIS Benchmark

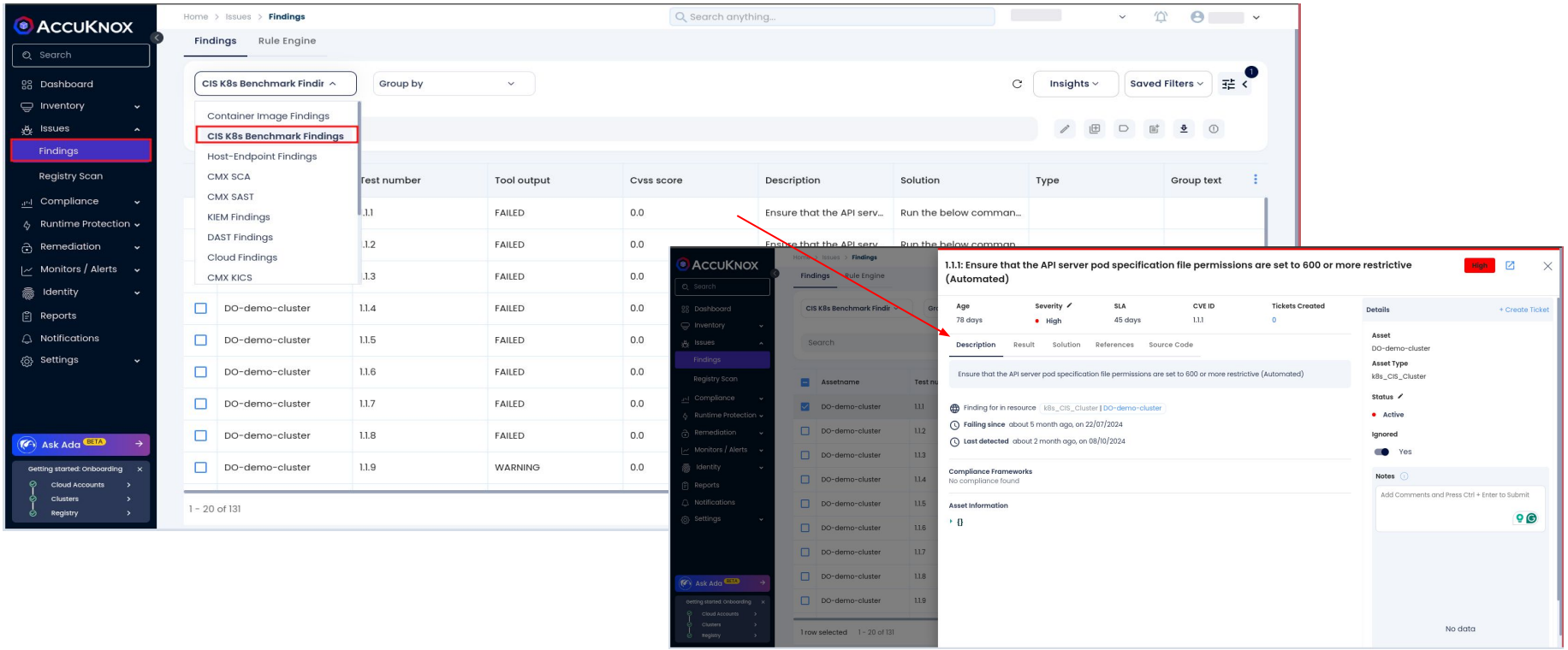
Kubernetes CIS Benchmark (Agentless)

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



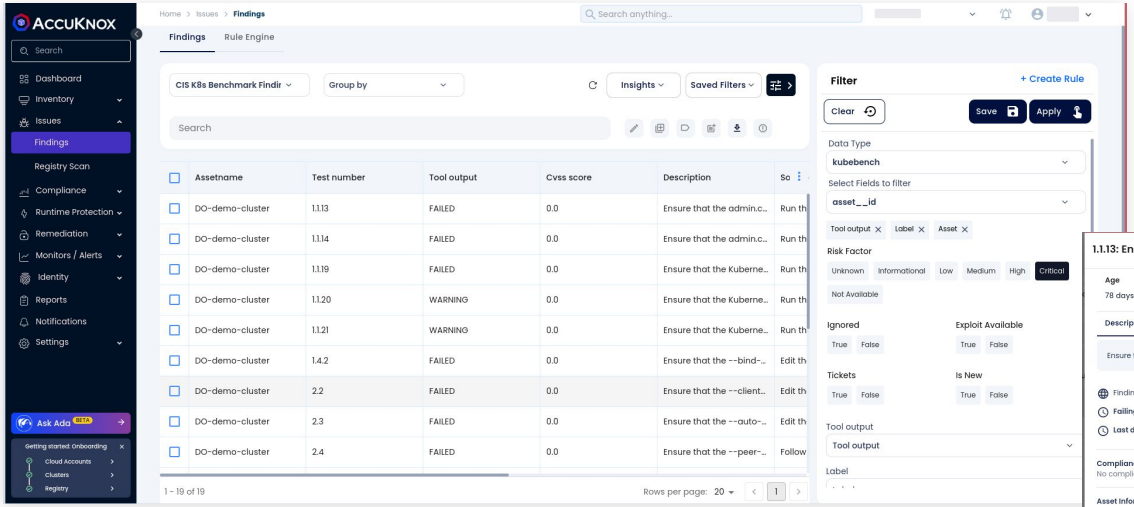
View Findings

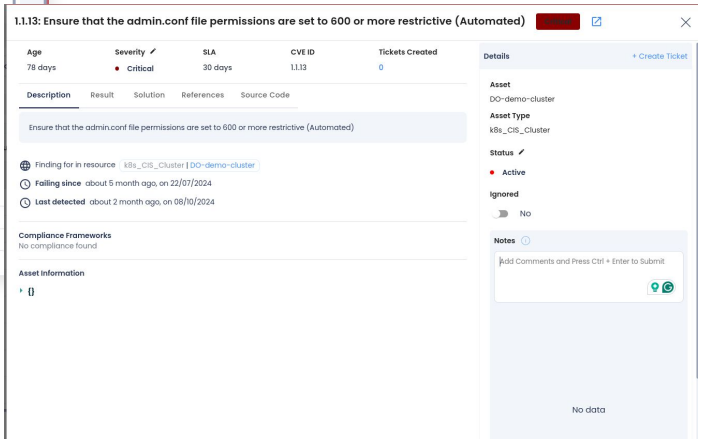
- View the findings on the **Findings** page. Select the **CIS k8s Benchmark Findings** to access the relevant details.



Work on Critical Findings

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



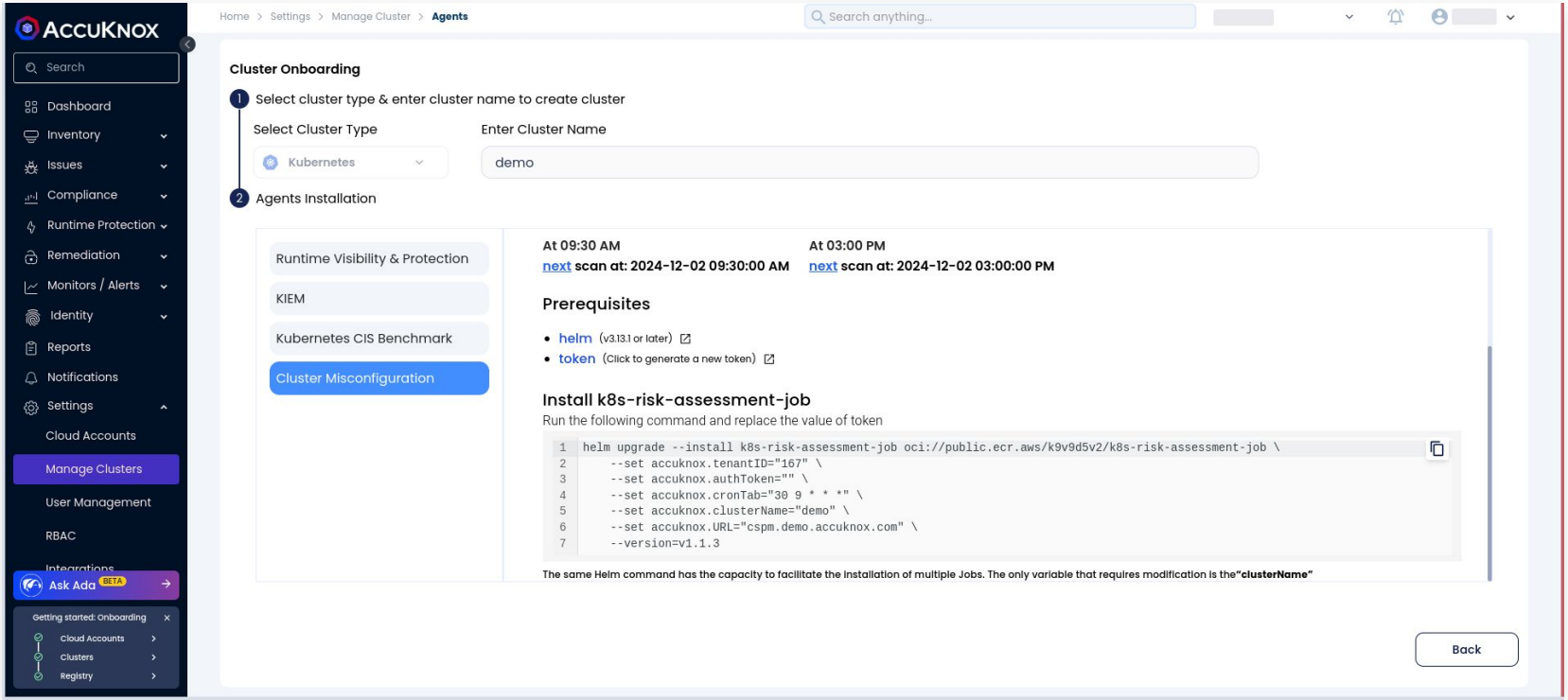


- Click on any of the findings for details, click on Create Ticket button to generate tickets

Cluster Misconfiguration

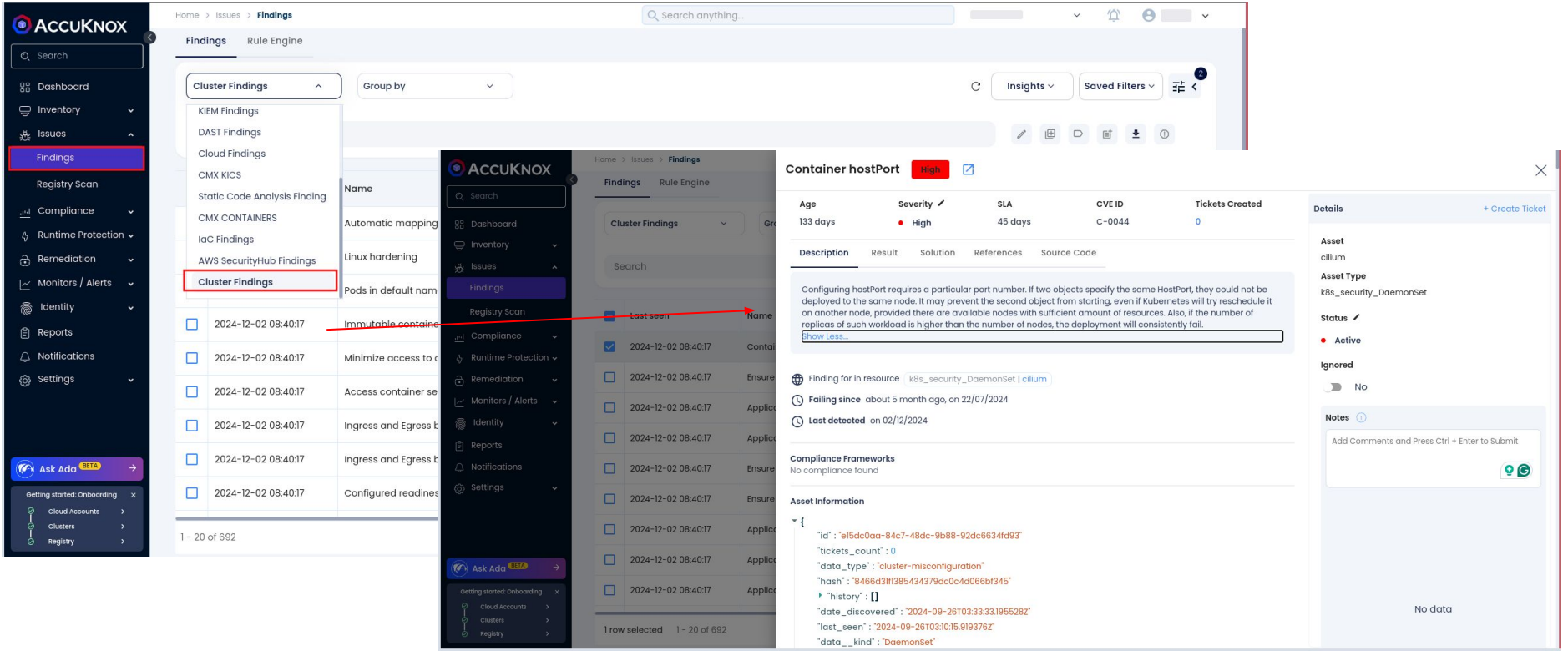
Cluster Misconfiguration (Agentless)

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



View Findings

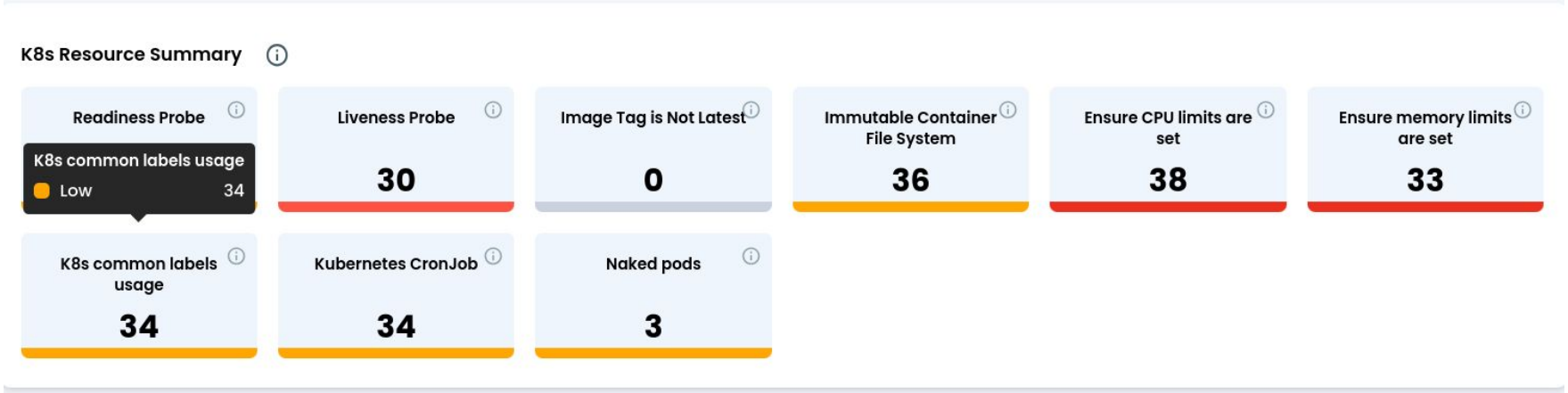
- View the findings on the **Findings** page. Select the **CIS k8s Benchmark Findings** to access the relevant details.



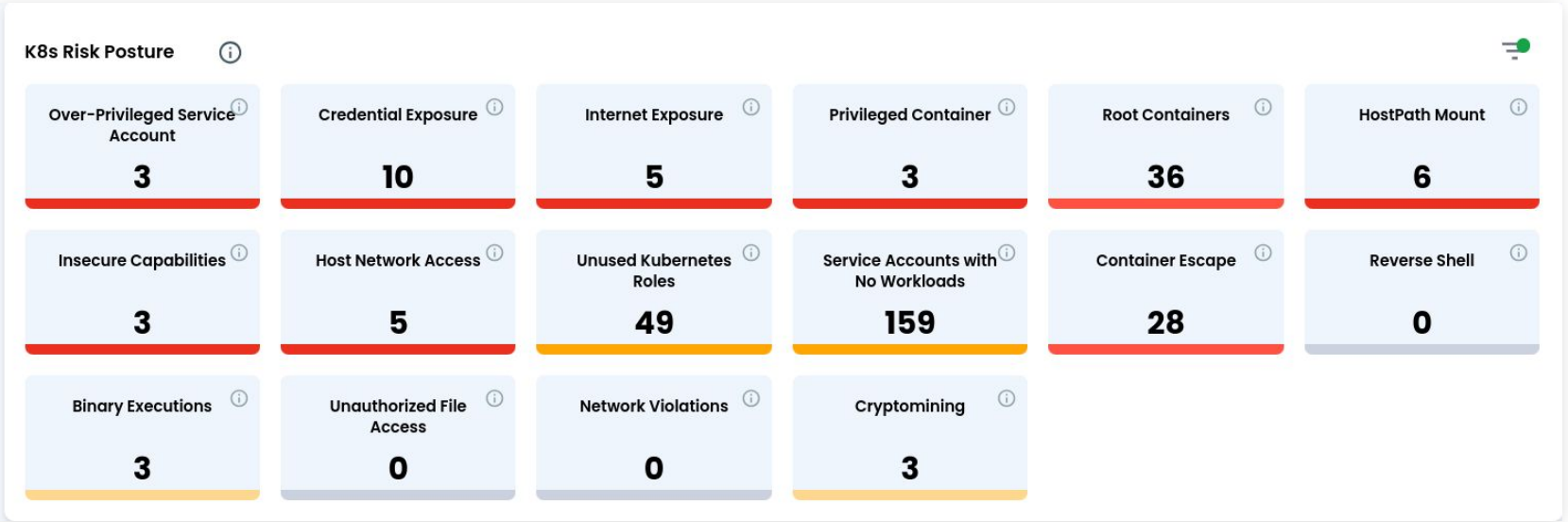
AccuKnox

KSPM Customized Dashboard & Reporting Metrics

Resource Metrics Widgets [1]

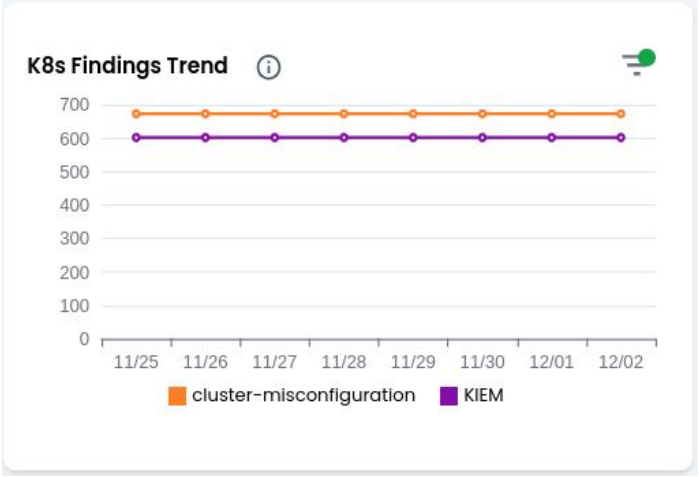


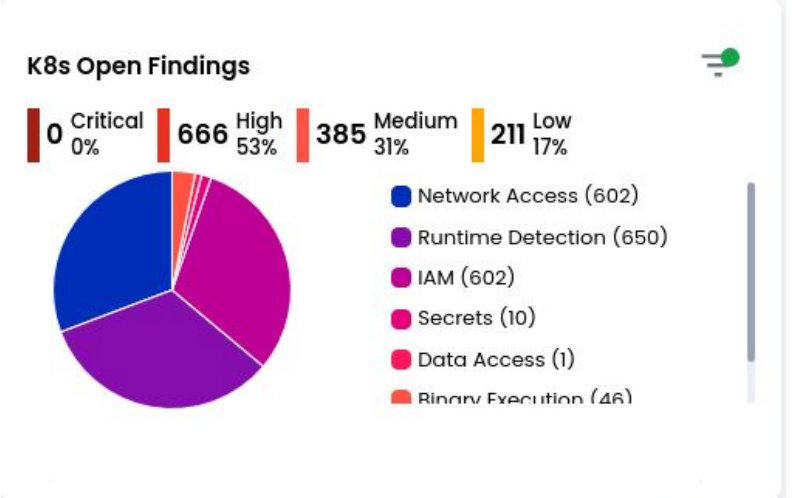
Security Risk Metrics Widgets [2]

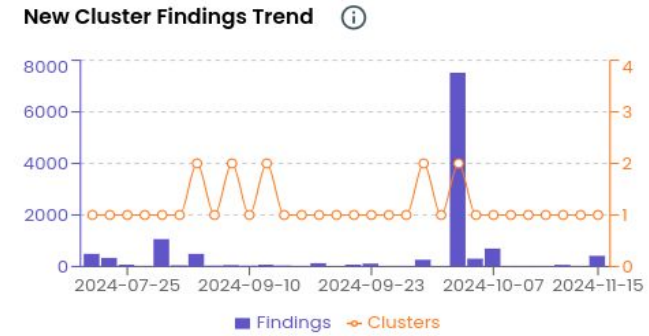


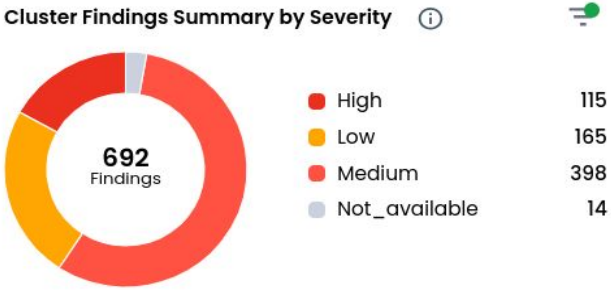
K8s Risk Overview - Widgets [3]

ACCUKNOX









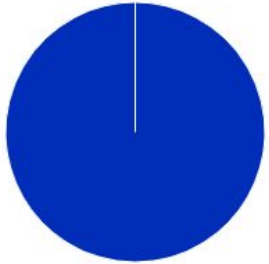
Cluster Wide Risk - Widgets [4]

ACCUKNOX

Clusters with Public Exposure

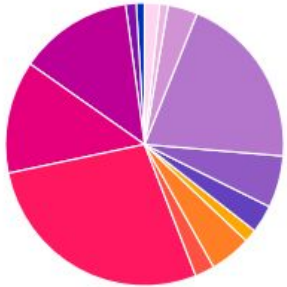
[redacted]	8.2K
aws-stage-ka-...	16.4M
mongo-test-02	163.6K
DO-demo-clust...	1.7M

Privileged Containers by Clusters



DO-demo-clust...	3

Cluster Findings by Asset Type

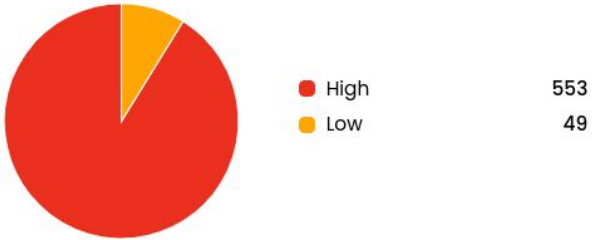


k8s_security_...	1
k8s_security_...	3
k8s_security_...	94
k8s_security_...	92
k8s_security_...	205

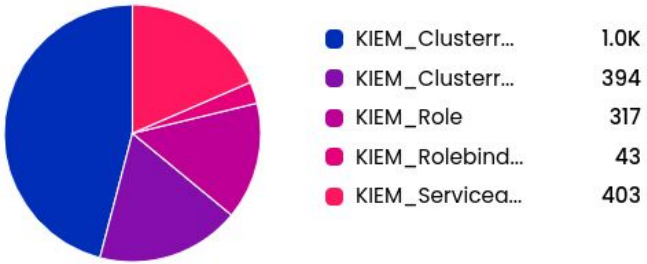
KIEM Widgets [5]

ACCUKNOX

KIEM Risk Assessment



KIEM Findings by Asset Types

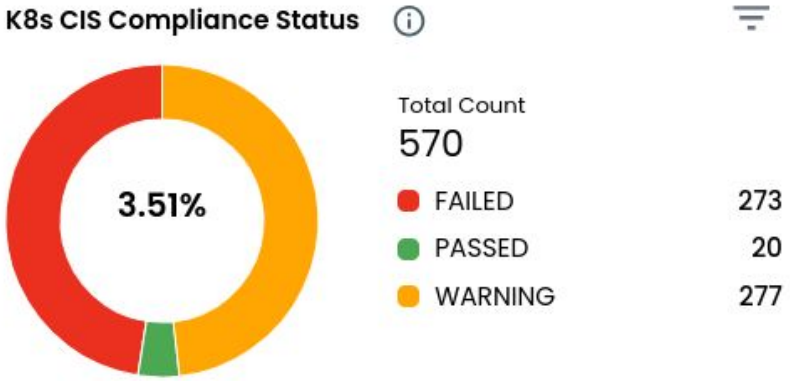


Top 5 Most Critical Findings

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

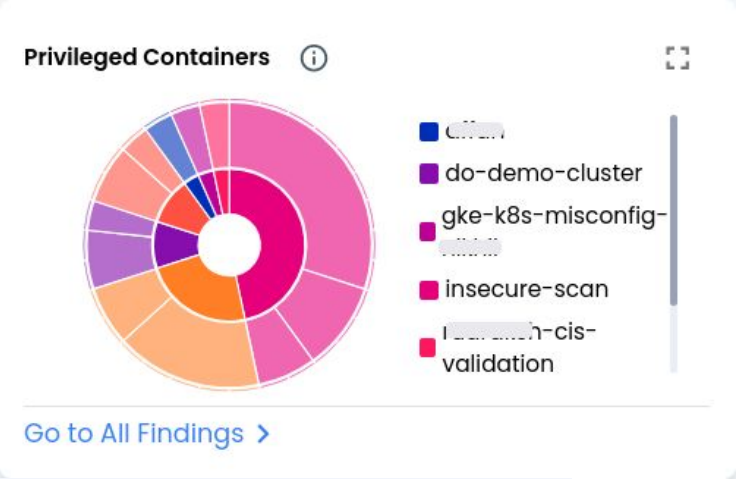


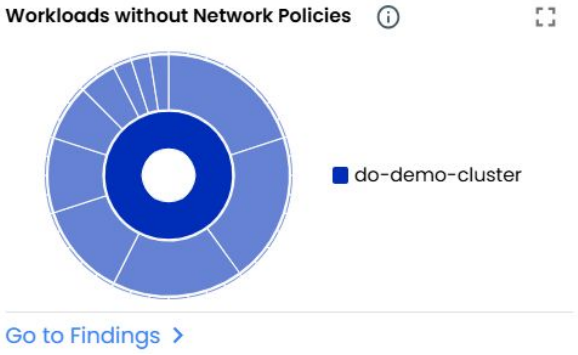
Top 5 K8s CIS Findings

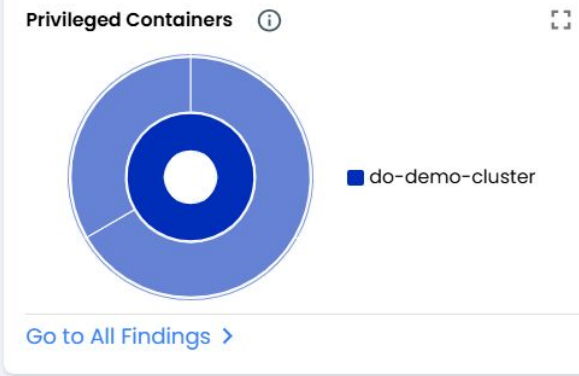
Finding Name	Assets Impacted
2.5: Ensure that the --peer-client-cert-auth arg...	5
2.4: Ensure that the --peer-cert-file and --peer...	5
2.3: Ensure that the --auto-tls argument is not s...	5
2.2: Ensure that the --client-cert-auth argumen...	5
1.4.2: Ensure that the --bind-address argument ...	5

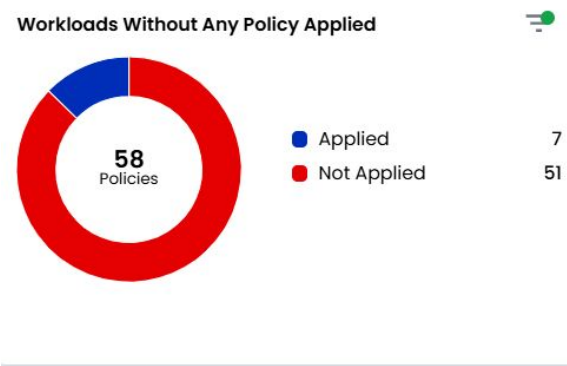
Container Specific Risk - Widgets [7]

ACCUKNOX







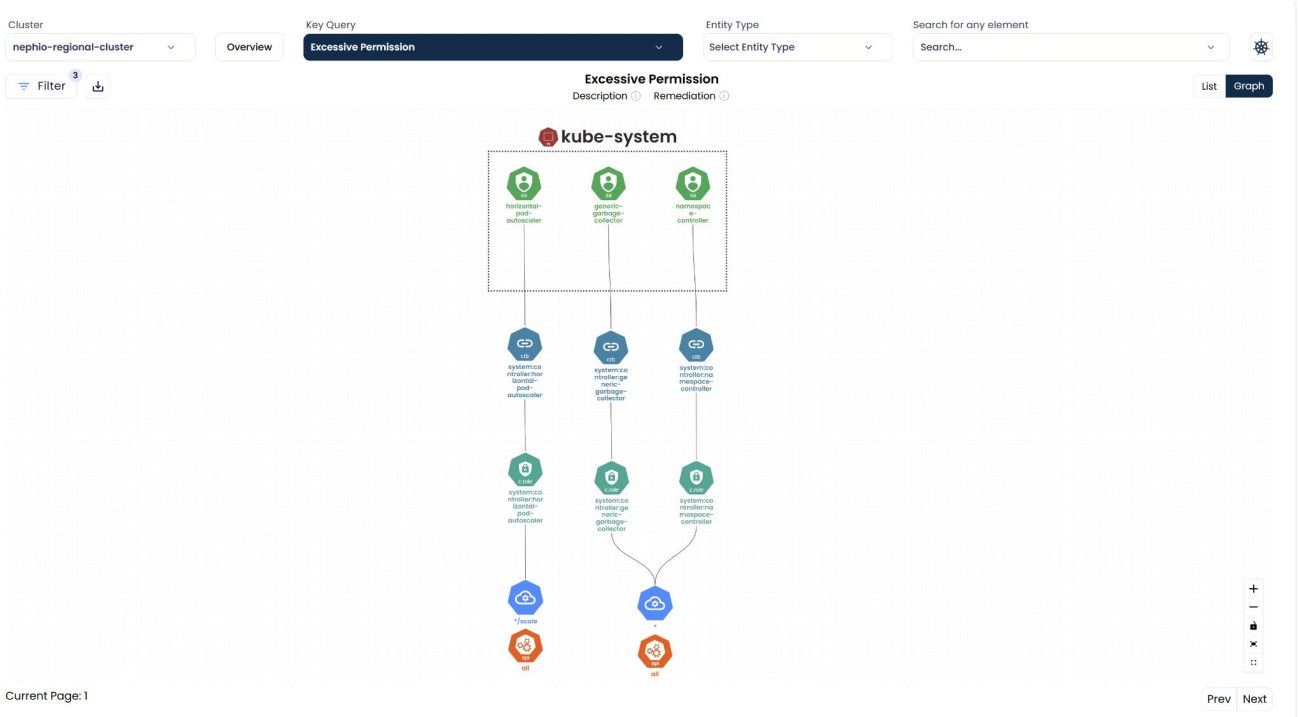


KSPM Use Cases

KIEM Use Case: Excessive Permissions in Kubernetes

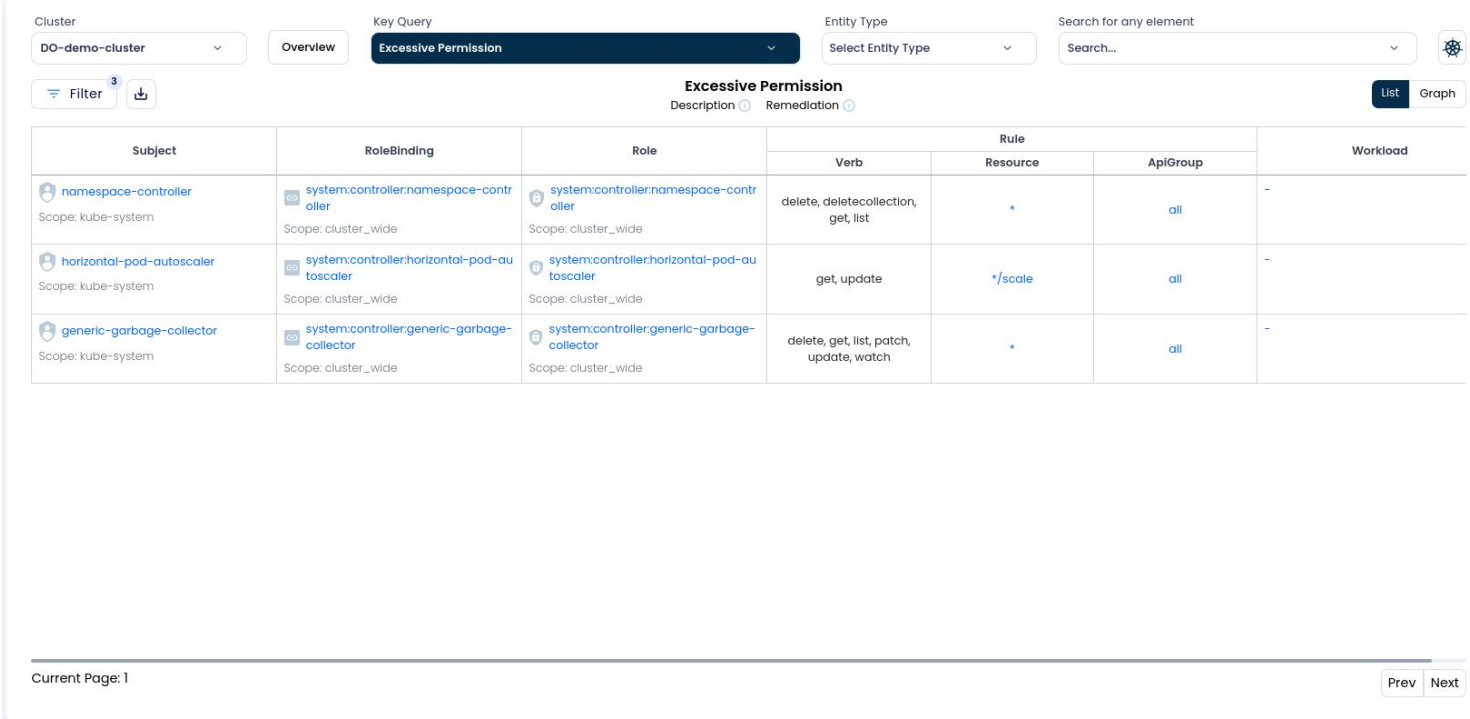
ACCUKNOX

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



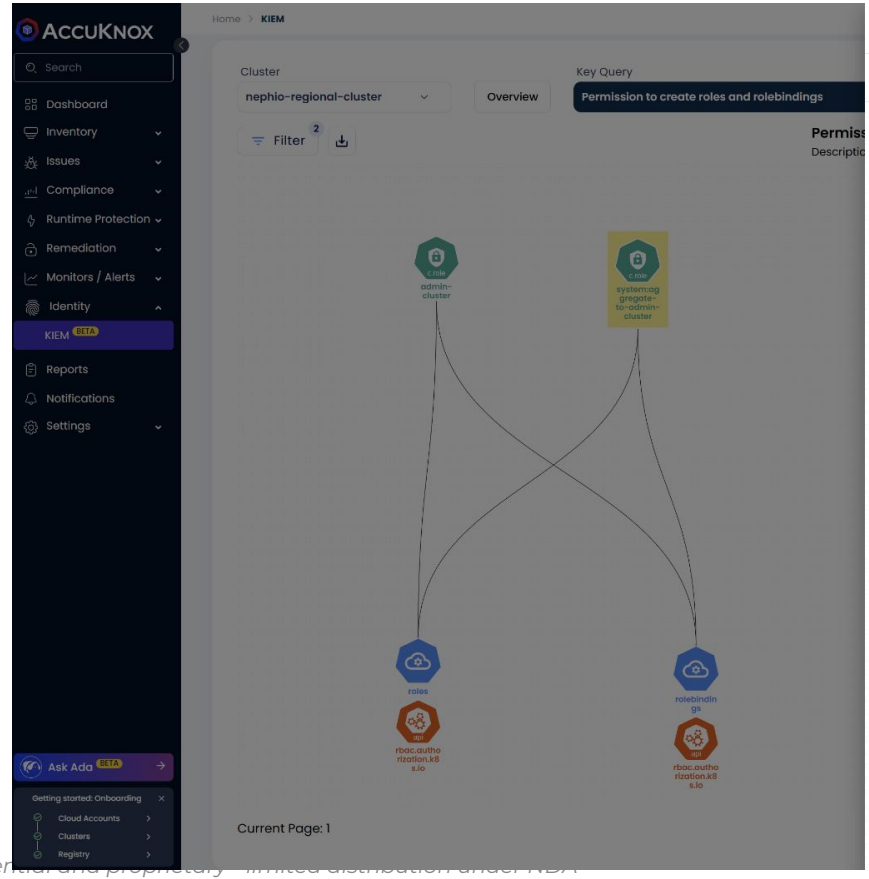
KIEM Use Case: List View (continued)

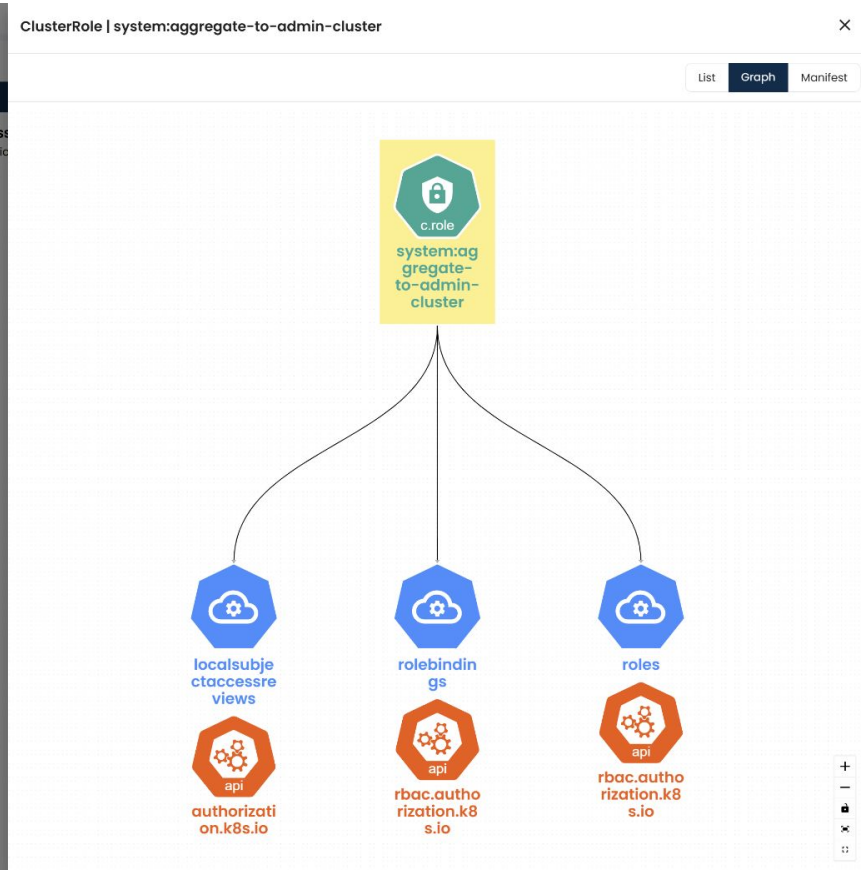
- **AccuKnox recommends** minimizing permissions by enforcing least privilege, avoiding wildcards, restricting namespaces, and using RBAC with narrowly defined roles.



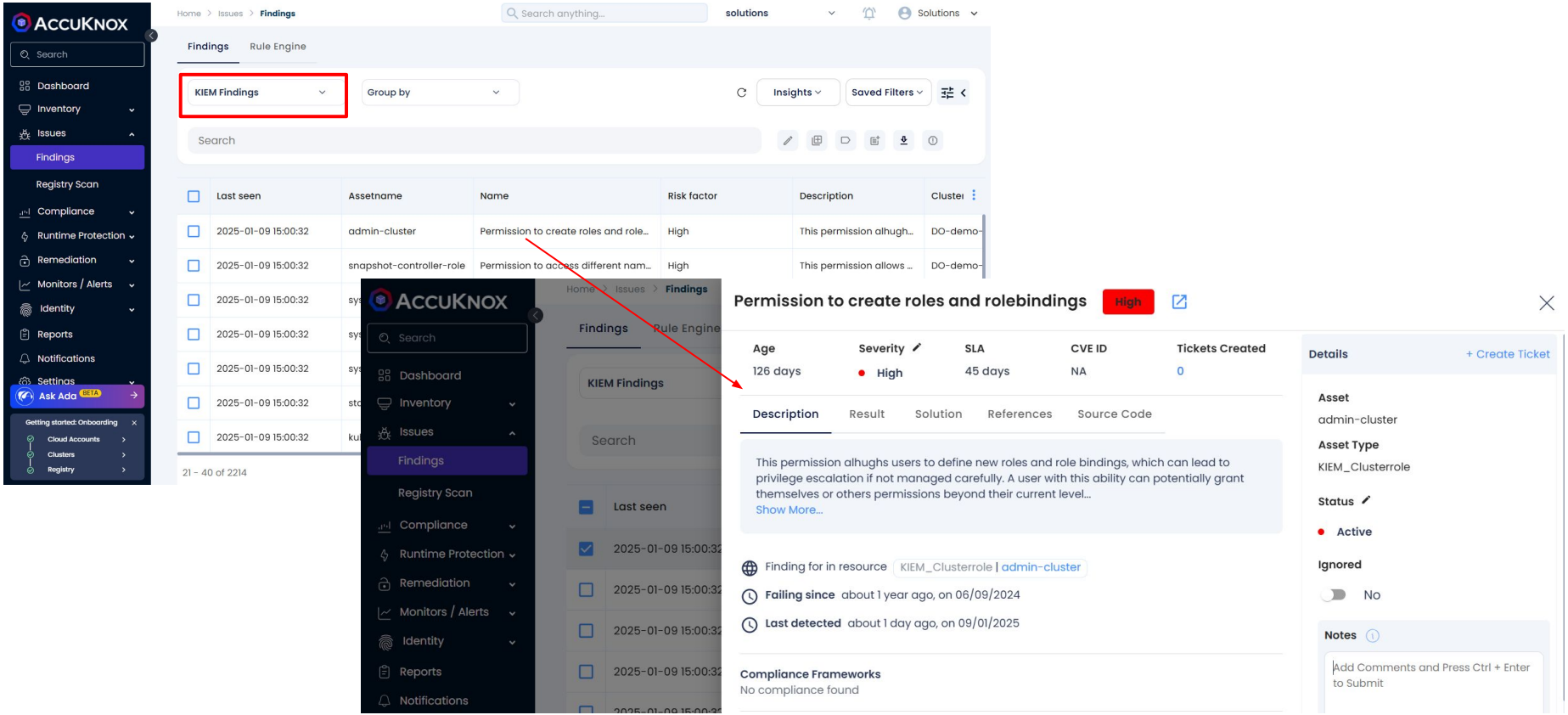
KIEM: Permission to create Roles & RoleBindings

ACCUKNOX





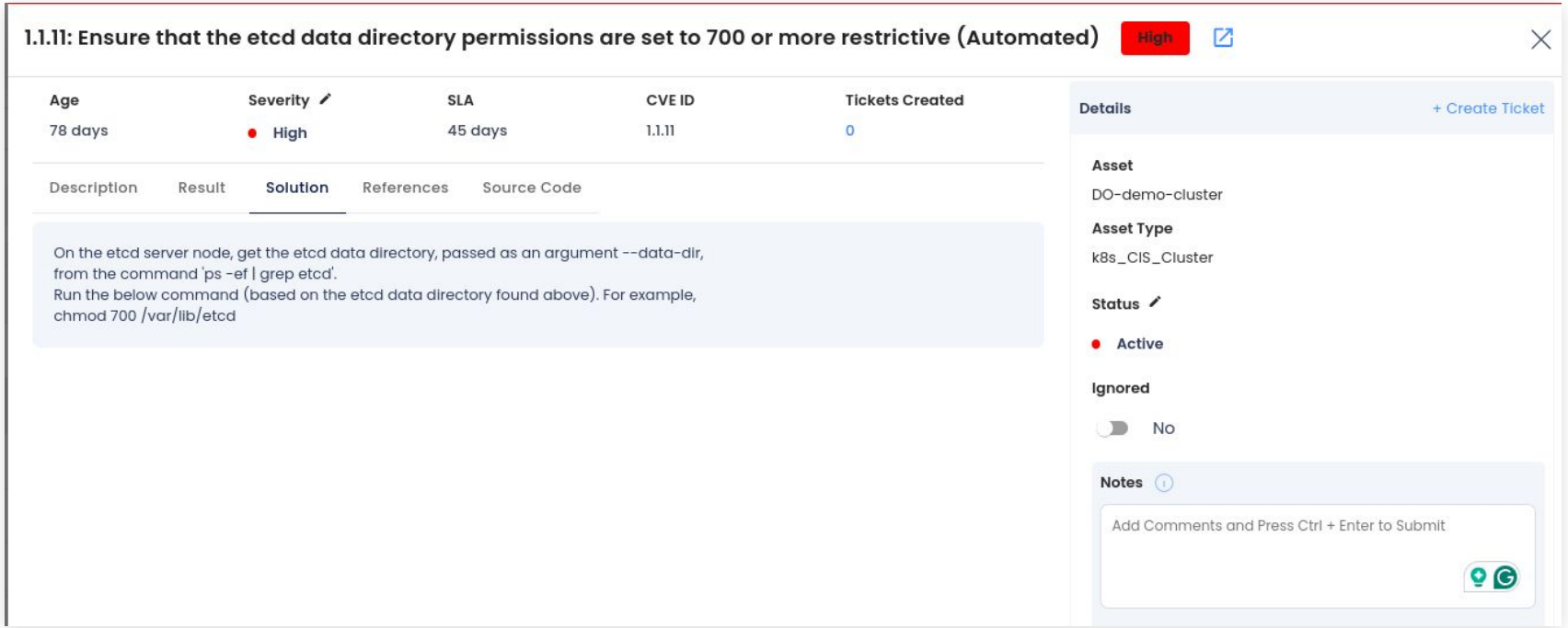
KIEM: Track KIEM findings identified by filters



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.



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.