

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).  
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

Learn more and customize

Reject

Accept

# Kubernetes Suspicious Self-Subject Review



This rule detects when a service account or node attempts to enumerate their own permissions via the selfsubjectaccessreview or selfsubjectrulesreview APIs. This is highly unusual behavior for non-human identities like service accounts and nodes. An adversary may have gained access to credentials/tokens and this could be an attempt to determine what privileges they have to facilitate further movement or execution within the cluster.

**Rule type:** query

**Rule indices:**

- logs-kubernetes.\*

**Severity:** medium

**Risk score:** 47

**Runs every:** 5m

**Searches indices from:** None ( [Date Math format](#), see also [Additional look-back time](#) )

**Maximum alerts per execution:** 100

**References:**

- [https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en\\_US/resources/whitepapers/kubernetes-](https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/kubernetes-)

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).  
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

Tags:

- Data Source: Kubernetes
- Tactic: Discovery

Version: 203

Rule authors:

- Elastic

Rule license: Elastic License v2

# Investigation guide



# Setup



The Kubernetes Fleet integration with Audit Logs enabled or similarly structured data is required to be compatible with this rule.

# Rule query



```
event.dataset : "kubernetes.audit_logs"  
  and kubernetes.audit.annotations.authorization_k8s_io/  
  and kubernetes.audit.verb:"create"  
  and kubernetes.audit.objectRef.resource:("selfsubjecta  
  and (kubernetes.audit.user.username:(system\:serviceac  
  or kubernetes.audit.impersonatedUser.username:(system\
```

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).  
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

Technique.

- Name: Container and Resource Discovery
- ID: T1613
- Reference URL:  
<https://attack.mitre.org/techniques/T1613/>

« [Kubernetes Suspicious Assignment of Controller Service Account](#) [Kubernetes User Exec into Pod](#) »

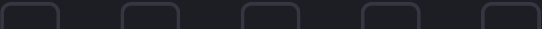
**ElasticON events are back!**  
Learn about the Elastic Search AI Platform from the experts at our live events.

Learn more

Was this helpful?



Follow us



Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).  
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

DE&I  
Blog  
Newsroom

Request access  
Become a partner

Financials  
Stock

Join us

Careers  
Career portal

Trust & Security

Trust center  
EthicsPoint portal  
ECCN report  
Ethics email

EXCELLENCE AWARDS

Previous winners  
ElasticON Tour  
Become a sponsor  
All events

[Trademarks](#) [Terms of Use](#) [Privacy](#) [Sitemap](#)

© 2024. Elasticsearch B.V. All Rights Reserved

Elastic, Elasticsearch and other related marks are trademarks, logos or registered trademarks of Elasticsearch B.V. in the United States and other countries.  
Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.