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 <u>cookie policy</u>.

Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

Learn more and customize

Reject

Accept

ElasticON events are

Learn about

back!

Kubernetes Suspicious Self-Subject Review

edit

Rule query

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 lookback time)

Maximum alerts per execution: 100

References:

- https://www.paloaltonetworks.com/apps/pan/public/downloadResource? pagePath=/content/pan/en_US/resources/whitepapers/kubernetesprivilege-escalation-excessive-permissions-in-popular-platforms
- https://kubernetes.io/docs/reference/access-authnauthz/authorization/#checking-api-access
- https://techcommunity.microsoft.com/t5/microsoft-defender-forcloud/detecting-identity-attacks-in-kubernetes/ba-p/3232340

Page 1 of 3

Tags:

Data Source: Kubernetes

• Tactic: Discovery

Version: 203

Rule authors:

Elastic

Rule license: Elastic License v2

Investigation guide

edit

ed

the Elastic
Search Al
Platform
from the
experts at
our live
events.

Learn more

16 91

Was this helpful?

https://www.elastic.co/guide/en/security/current/kubernetes-suspicious-self-subject-review.html

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 <u>cookie policy</u>.

Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

event.dataset: "kubernetes.audit_logs"

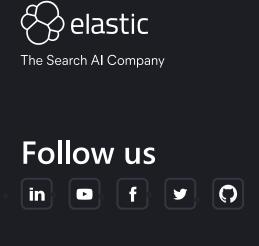
and kubernetes.audit.annotations.authorization_k8s_io/decisio
and kubernetes.audit.verb:"create"
and kubernetes.audit.objectRef.resource:("selfsubjectaccessrement (kubernetes.audit.user.username:(system\:serviceaccount\: or kubernetes.audit.impersonatedUser.username:(system\:serviceaccount\:

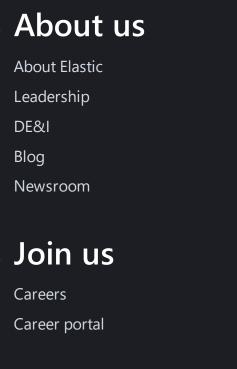
Framework: MITRE ATT&CKTM

- Tactic:
 - Name: Discovery
 - ID: TA0007
 - Reference URL: https://attack.mitre.org/tactics/TA0007/
- 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 »





Find a partner Partner login Request access Become a partner Trust & Security Trust center EthicsPoint portal ECCN report Ethics email

Investor relations

Kubernetes Suspicious Self-Subject Review | Elastic Security Solution [8.15] | Elastic - 02/11/2024 09:22 https://www.elastic.co/guide/en/security/current/kubernetes-suspicious-self-subject-review.html

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 <u>cookie policy</u>.

Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

Previous winners

ElasticON Tour

Become a sponsor

All events

<u>Trademarks</u> <u>Terms of Use</u> <u>Privacy</u> <u>Sitemap</u> © 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.