Kubernetes Suspicious Self-Subject Review

edit

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/downloadResourc
  pagePath=/content/pan/en_US/resources/whitepapers/kubernetes-

Tags:

- Data Source: Kubernetes
- Tactic: Discovery

Version: 203

Rule authors:

- Elastic

Rule license: Elastic License v2

Investigation guide

edit

Setup

edit

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

Rule query

edit

```
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\
```

- 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 »