Kubernetes Pod Created With HostNetwork

edit

This rules detects an attempt to create or modify a pod attached to the host network. HostNetwork allows a pod to use the node network namespace. Doing so gives the pod access to any service running on localhost of the host. An attacker could use this access to snoop on network activity of other pods on the same node or bypass restrictive network policies applied to its given namespace.

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:

Tags:

- Data Source: Kubernetes
- Tactic: Execution
- Tactic: Privilege Escalation

Version: 204

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

Framework: MITRE ATT&CK™

- Tactic:
  - Name: Privilege Escalation
  - ID: TA0004
  - Reference URL: https://attack.mitre.org/tactics/TA0004/
- Technique:
  - Name: Escape to Host
  - ID: T1611
  - Reference URL: https://attack.mitre.org/techniques/T1611/
- Tactic:
  - Name: Execution
  - ID: TA0002
  - Reference URL: https://attack.mitre.org/tactics/TA0002/
- Technique:
  - Name: Deploy Container
  - ID: T1610
  - Reference URL: https://attack.mitre.org/techniques/T1610/