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

Kubernetes Pod Created With HostNetwork



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:

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.

Tags:

Data Source: Kubernetes

• Tactic: Execution

Tactic: Privilege Escalation

Version: 204

Rule authors:

Elastic

Rule license: Elastic License v2

Investigation guide

, edit

Setup



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

Rule query



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.

Framework: MITRE ATT&CKTM

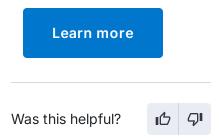
- Tactic:
 - Name: Privilege Escalation
 - ID: TA0004
 - Reference URL: https://attack.mitre.org/tactics/TA0004/
- Technique:
 - Name: Escape to Host
 - ID: T1611
 - Reference URL: https://attack.mitre.org/techniques/T1611/
- Tactic:
 - Name: Execution
 - ID: TA0002
 - Reference URL: https://attack.mitre.org/tactics/TA0002/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

https://www.elastic.co/guide/en/security/current/kubernetes-pod-created-with-hostnetwork.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.





The Search Al Company

Follow us











About us

About Elastic

Leadership

DE&I

Blog

Newsroom

Partners

Find a partner

Partner login

Request access

Become a partner

Trust & Security

https://www.elastic.co/guide/en/security/current/kubernetes-pod-created-with-hostnetwork.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.

Investor relations

Investor resources

Governance

Financials

Stock

EXCELLENCE AWARDS

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.

Kubernetes Pod Created With HostNetwork | Elastic Security Solution [8.15] | Elastic - 31/10/2024 09:02 https://www.elastic.co/guide/en/security/current/kubernetes-pod-created-with-hostnetwork.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.