Sign in

elastic / detection-rules Public

Notifications Fork 498 Star 2k

Code Issues 145 Pull requests 19 Actions Security Insights

detection-rules / rules / integrations / azure / impact_kubernetes_pod_deleted.toml

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

austinsonger Update 065bf48 · 3 years ago

48 lines (42 loc) · 1.51 KB

Code Blame Raw

```
[metadata]
creation_date = "2021/06/24"
maturity = "production"
updated_date = "2021/06/24"

[rule]
author = ["Austin Songer"]
description = """
Identifies the deletion of Azure Kubernetes Pods.
"""
false_positives = [
    """
    Pods may be deleted by a system administrator. Verify whether the user identity, user agent, ar
    should be making changes in your environment. Pods deletions from unfamiliar users or hosts sho
    investigated. If known behavior is causing false positives, it can be exempted from the rule.
    """,
]
from = "now-25m"
index = ["filebeat-*", "logs-azure*"]
language = "kuery"
license = "Elastic License v2"
name = "Azure Kubernetes Pods Deleted"
note = """## Config
note =    ## Config

The Azure Fleet integration, Filebeat module, or similarly structured data is required to be compat
references = [
    "https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#
]
risk_score = 47
rule_id = "83a1931d-8136-46fc-b7b9-2db4f639e014"
severity = "medium"
tags = ["Elastic", "Cloud", "Azure", "Continuous Monitoring", "SecOps", "Asset Visibility"]
timestamp_override = "event.ingested"
type = "query"

query = '''
event.dataset:azure.activitylogs and azure.activitylogs.operation_name:MICROSOFT.KUBERNETES/CONNECT
event.outcome:(Success or success)
'''


[[rule.threat]]
framework = "MITRE ATT&CK"

[rule.threat.tactic]
id = "TA0040"
name = "Impact"
reference = "https://attack.mitre.org/tactics/TA0040/"
```