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 / defense_evasion_kubernetes_events_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 da3852b · 3 years ago

57 lines (50 loc) · 1.9 KB

Code Blame Raw

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

[rule]
author = ["Austin Songer"]
description = """
Identifies when Events are deleted in Azure Kubernetes. An adversary may delete events in Azure Kub
"""
false_positives = [
    """
    Events deletions may be done by a system or network administrator. Verify whether the username,
    resource name should be making changes in your environment. Events deletions from unfamiliar us
    should be investigated. If known behavior is causing false positives, it can be exempted from t
    """,
]
from = "now-25m"
index = ["filebeat-*", "logs-azure*"]
language = "kuery"
license = "Elastic License v2"
name = "Azure Kubernetes Events 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 = "8b64d36a-1307-4b2e-a77b-a0027e4d27c8"
severity = "medium"
tags = ["Elastic", "Cloud", "Azure", "Continuous Monitoring", "SecOps", "Log Auditing"]
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.technique]]
id = "T1562"
name = "Impair Defenses"
reference = "https://attack.mitre.org/techniques/T1562/"
[[rule.threat.technique.subtechnique]]
id = "T1562.001"
name = "Disable or Modify Tools"
reference = "https://attack.mitre.org/techniques/T1562/001/"



[rule.threat.tactic]
id = "TA0005"
name = "Defense Evasion"
reference = "https://attack.mitre.org/tactics/TA0005/"
```