Sign in

elastic / detection-rules Public

Notifications | Fork 498 | Star 2k

Code | Issues 145 | Pull requests 19 | Actions | Security | Insights

detection-rules / rules / integrations / aws / impact_elasticache_security_group_modified_or_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 7d5efd6 · 3 years ago

52 lines (45 loc) · 1.83 KB

Code | Blame | Raw

```
[metadata]
creation_date = "2021/07/19"
maturity = "production"
updated_date = "2021/07/19"

[rule]
author = ["Austin Songer"]
description = "Identifies when an ElastiCache security group has been modified or deleted."
false_positives = [
    """
    A ElastiCache security group deletion may be done by a system or network administrator. Verify
    user agent, and/or hostname should be making changes in your environment. Security Group deleti
    users or hosts should be investigated. If known behavior is causing false positives, it can be
    rule.
    """,
]
from = "now-60m"
index = ["filebeat-*", "logs-aws*"]
interval = "10m"
language = "kuery"
license = "Elastic License v2"
name = "AWS ElastiCache Security Group Modified or Deleted"
name = "AWS ElastiCache Security Group Modified or Deleted"
note = """## Config

The AWS Fleet integration, Filebeat module, or similarly structured data is required to be compatib
references = ["https://docs.aws.amazon.com/AmazonElastiCache/latest/APIReference/Welcome.html"]
risk_score = 21
rule_id = "1ba5160d-f5a2-4624-b0ff-6a1dc55d2516"
severity = "low"
tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Monitoring"]
timestamp_override = "event.ingested"
type = "query"

query = '''
event.dataset:aws.cloudtrail and event.provider:elasticache.amazonaws.com and event.action:("Delete
"Authorize Cache Security Group Ingress" or  "Revoke Cache Security Group Ingress" or "AuthorizeCac
"RevokeCacheSecurityGroupEgress") and event.outcome:success
'''


[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1531"
name = "Account Access Removal"
reference = "https://attack.mitre.org/techniques/T1531/"


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