austinsonger Update 598f3d7 · 3 years ago

54 lines (47 loc) · 1.77 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 created."
false_positives = [
    """
    A ElastiCache security group may be created by a system or network administrator. Verify whethe
    agent, and/or hostname should be making changes in your environment. Security group creations f
    or hosts should be investigated. If known behavior is causing false positives, it can be exempt
    """,
]
from = "now-60m"
index = ["filebeat-*", "logs-aws*"]
interval = "10m"
language = "kuery"
license = "Elastic License v2"
name = "AWS ElastiCache Security Group Created"
note = """## Config
```

```
23
24      The AWS Fleet integration, Filebeat module, or similarly structured data is required to be compatib
25      references = ["https://docs.aws.amazon.com/AmazonElastiCache/latest/APIReference/Welcome.html"]
26      risk_score = 21
27      rule_id = "7b3da11a-60a2-412e-8aa7-011e1eb9ed47"
28      severity = "low"
29      tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Monitoring"]
30      timestamp_override = "event.ingested"
31      type = "query"
32
33      query = '''
34      event.dataset:aws.cloudtrail and  event.provider:elasticache.amazonaws.com and event.action:"Create
35      event.outcome:success
36      '''
37
38
39      [[rule.threat]]
40      framework = "MITRE ATT&CK"
41      [[rule.threat.technique]]
42      id = "T1136"
43      name = "Create Account"
44      reference = "https://attack.mitre.org/techniques/T1136/"
45      [[rule.threat.technique.subtechnique]]
46      id = "T1136.003"
47      name = "Cloud Account"
48      reference = "https://attack.mitre.org/techniques/T1136/003/"
49
50
51      [rule.threat.tactic]
52      id = "TA0003"
53      name = "Persistence"
54      reference = "https://attack.mitre.org/tactics/TA0003/"
```