```
[metadata]
creation_date = "2021/05/10"
maturity = "production"
updated_date = "2021/07/20"
integration = "aws"

[rule]
author = ["Elastic", "Austin Songer"]
description = """
Identifies when a transfer lock was removed from a Route 53 domain. It is recommended to refrain fr
action unless intending to transfer the domain to a different registrar.
"""
false_positives = [
    """
    A domain transfer lock may be disabled by a system or network administrator. Verify whether the
    agent, and/or hostname should be making changes in your environment. Activity from unfamiliar u
    be investigated. If known behavior is causing false positives, it can be exempted from the rule
    """,
]
from = "now-60m"
index = ["filebeat-*", "logs-aws*"]
interval = "10m"
language = "kuery"
license = "Elastic License v2"
name = "AWS Route 53 Domain Transfer Lock Disabled"
```

```
26  note = """## Config
27
28  The AWS Fleet integration, Filebeat module, or similarly structured data is required to be compatib
29  references = [
30      "https://docs.aws.amazon.com/Route53/latest/APIReference/API_Operations_Amazon_Route_53.html",
31      "https://docs.aws.amazon.com/Route53/latest/APIReference/API_domains_DisableDomainTransferLock.
32  ]
33  risk_score = 21
34  rule_id = "12051077-0124-4394-9522-8f4f4db1d674"
35  severity = "low"
36  tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Asset Visibility"]
37  timestamp_override = "event.ingested"
38  type = "query"
39
40  query = '''
41  event.dataset:aws.cloudtrail and event.provider:route53.amazonaws.com and event.action:DisableDomai
42  '''
43
44
45  [[rule.threat]]
46  framework = "MITRE ATT&CK"
47  [[rule.threat.technique]]
48  id = "T1098"
49  name = "Account Manipulation"
50  reference = "https://attack.mitre.org/techniques/T1098/"
51
52
53  [rule.threat.tactic]
54  id = "TA0003"
55  name = "Persistence"
56  reference = "https://attack.mitre.org/tactics/TA0003/"
57  [[rule.threat]]
58  framework = "MITRE ATT&CK"
59
60  [rule.threat.tactic]
61  id = "TA0006"
62  name = "Credential Access"
63  reference = "https://attack.mitre.org/tactics/TA0006/"
```