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

[rule]
author = ["Elastic", "Austin Songer"]
description = "Identifies when a request has been made to transfer a Route 53 domain to another AWS
false_positives = [
    """
    A domain may be transferred to another AWS account by a system or network administrator. Verify
    identity, user agent, and/or hostname should be making changes in your environment. Domain trar
    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 Route 53 Domain Transferred to Another Account"
note = """## Config

```

```
26    The AWS Fleet integration, Filebeat module, or similarly structured data is required to be compatib
27    references = ["https://docs.aws.amazon.com/Route53/latest/APIReference/API_Operations_Amazon_Route_
28    risk_score = 21
29    rule_id = "2045567e-b0af-444a-8c0b-0b6e2dae9e13"
30    severity = "low"
31    tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Asset Visibility"]
32    timestamp_override = "event.ingested"
33    type = "query"
34
35    query = '''
36    event.dataset:aws.cloudtrail and event.provider:route53.amazonaws.com and event.action:TransferDoma
37    '''
38
39
40    [[rule.threat]]
41    framework = "MITRE ATT&CK"
42    [[rule.threat.technique]]
43    id = "T1098"
44    reference = "https://attack.mitre.org/techniques/T1098/"
45    name = "Account Manipulation"
46
47
48    [rule.threat.tactic]
49    id = "TA0003"
50    reference = "https://attack.mitre.org/tactics/TA0003/"
51    name = "Persistence"
52    [[rule.threat]]
53    framework = "MITRE ATT&CK"
54
55    [rule.threat.tactic]
56    id = "TA0006"
57    reference = "https://attack.mitre.org/tactics/TA0006/"
58    name = "Credential Access"
```