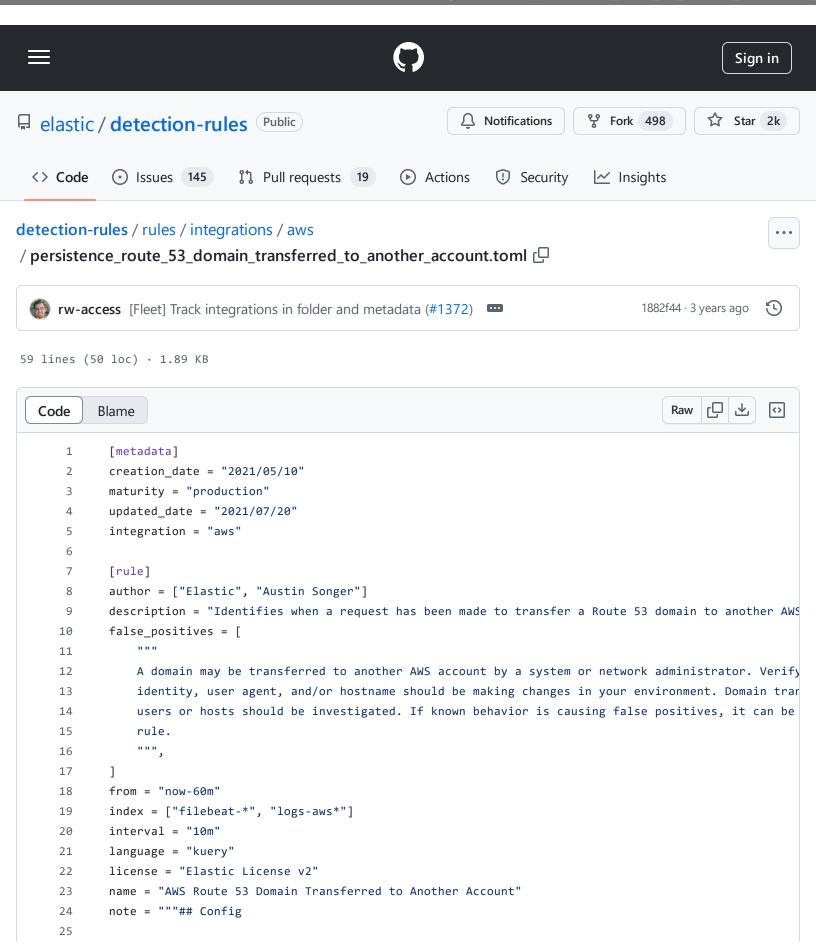
detection-rules/rules/integrations/aws/persistence_route_53_domain_transferred_to_another_account.toml at c76a39796972ecde44cb1da6df47f1b6562c9770 · elastic/detection-rules · GitHub - 31/10/2024 09:17

https://github.com/elastic/detection-

rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/integrations/aws/persistence_route_53_domain_transferred



detection-rules/rules/integrations/aws/persistence_route_53_domain_transferred_to_another_account.toml at c76a39796972ecde44cb1da6df47f1b6562c9770 · elastic/detection-rules · GitHub - 31/10/2024 09:17

https://github.com/elastic/detection-

rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/integrations/aws/persistence_route_53_domain_transferred_

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