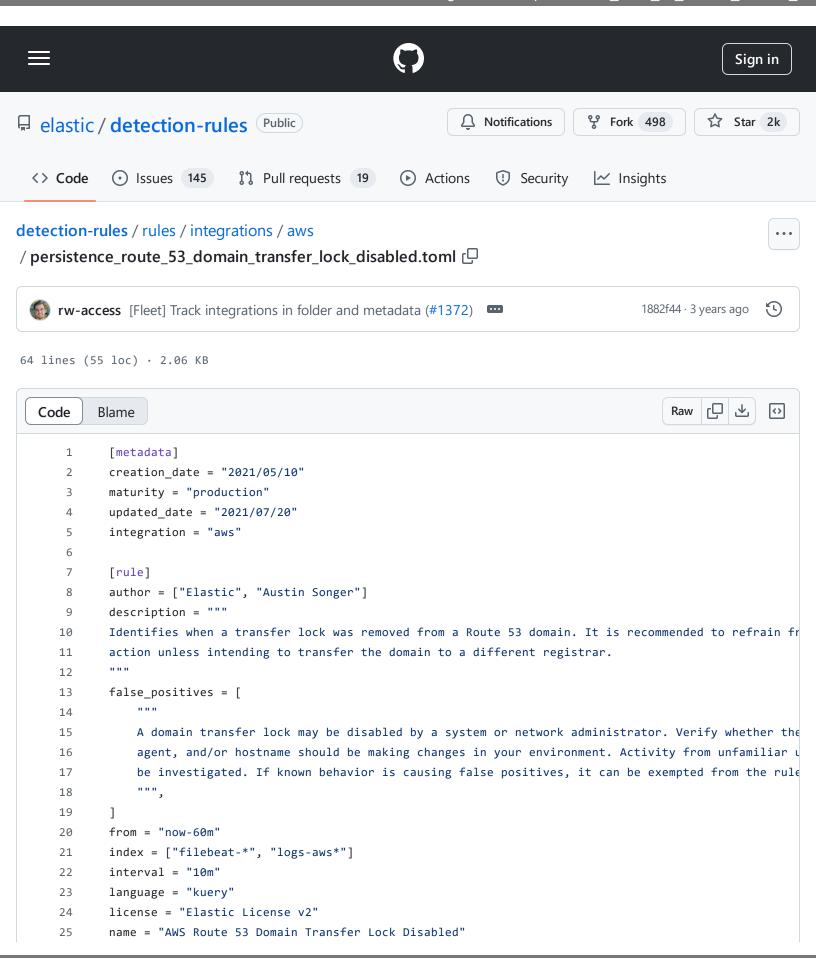
detection-rules/rules/integrations/aws/persistence_route_53_domain_transfer_lock_disabled.toml at c76a39796972ecde44cb1da6df47f1b6562c9770 · elastic/detection-rules · GitHub - 31/10/2024 09:16 https://github.com/elastic/detection-

rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/integrations/aws/persistence route 53 domain transfer loc



detection-rules/rules/integrations/aws/persistence_route_53_domain_transfer_lock_disabled.toml at c76a39796972ecde44cb1da6df47f1b6562c9770 · elastic/detection-rules · GitHub - 31/10/2024 09:16 https://github.com/elastic/detection-

rules/blob/c76a39796972ecde44cb1da6df47f1b6562c9770/rules/integrations/aws/persistence route 53 domain transfer loc

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