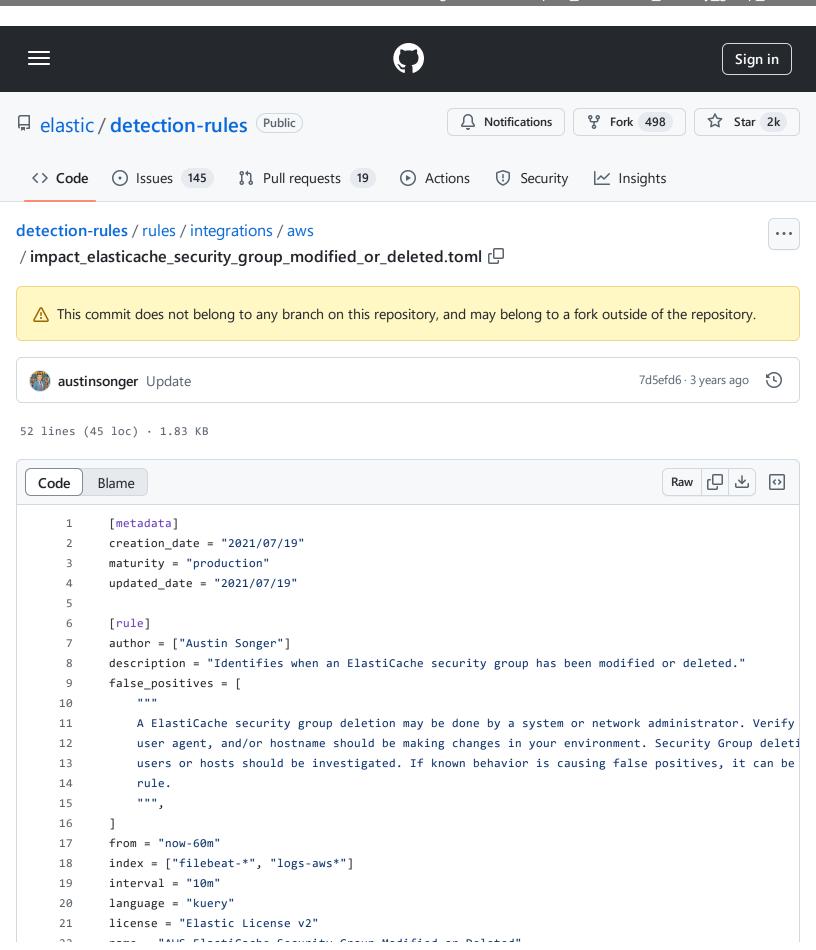
detection-rules/rules/integrations/aws/impact_elasticache_security_group_modified_or_deleted.toml at 7d5efd68603f42be5e125b5a6a503b2ef3ac0f4e · elastic/detection-rules · GitHub - 31/10/2024 09:15 https://github.com/elastic/detection-

rules/blob/7d5efd68603f42be5e125b5a6a503b2ef3ac0f4e/rules/integrations/aws/impact_elasticache_security_group_modified



detection-rules/rules/integrations/aws/impact_elasticache_security_group_modified_or_deleted.toml at 7d5efd68603f42be5e125b5a6a503b2ef3ac0f4e · elastic/detection-rules · GitHub - 31/10/2024 09:15 https://github.com/elastic/detection-

rules/blob/7d5efd68603f42be5e125b5a6a503b2ef3ac0f4e/rules/integrations/aws/impact_elasticache_security_group_modified

```
name = Aws Elasticache Security Group Modified or Deleted
       note = """## Config
23
24
       The AWS Fleet integration, Filebeat module, or similarly structured data is required to be compatible
25
       references = ["https://docs.aws.amazon.com/AmazonElastiCache/latest/APIReference/Welcome.html"]
26
27
       risk score = 21
       rule_id = "1ba5160d-f5a2-4624-b0ff-6a1dc55d2516"
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:("Delete
35
       "Authorize Cache Security Group Ingress" or "Revoke Cache Security Group Ingress" or "AuthorizeCac
36
       "RevokeCacheSecurityGroupEgress") and event.outcome:success
37
38
39
40
41
       [[rule.threat]]
       framework = "MITRE ATT&CK"
42
       [[rule.threat.technique]]
43
       id = "T1531"
44
       name = "Account Access Removal"
45
       reference = "https://attack.mitre.org/techniques/T1531/"
46
47
48
49
       [rule.threat.tactic]
       id = "TA0040"
50
       name = "Impact"
51
52
       reference = "https://attack.mitre.org/tactics/TA0040/"
```