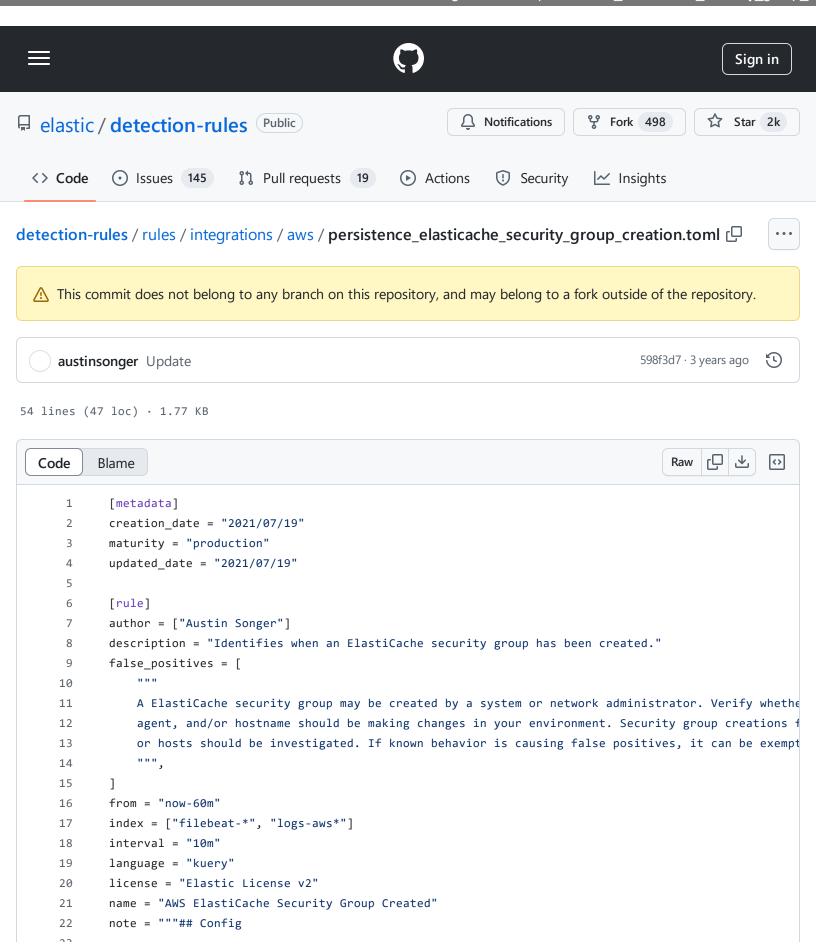
detection-rules/rules/integrations/aws/persistence_elasticache_security_group_creation.toml at 598f3d7e0a63221c0703ad9a0ea7e22e7bc5961e · elastic/detection-rules · GitHub - 31/10/2024 09:15 https://github.com/elastic/detection-

rules/blob/598f3d7e0a63221c0703ad9a0ea7e22e7bc5961e/rules/integrations/aws/persistence elasticache security group c



detection-rules/rules/integrations/aws/persistence_elasticache_security_group_creation.toml at 598f3d7e0a63221c0703ad9a0ea7e22e7bc5961e · elastic/detection-rules · GitHub - 31/10/2024 09:15 https://github.com/elastic/detection-

rules/blob/598f3d7e0a63221c0703ad9a0ea7e22e7bc5961e/rules/integrations/aws/persistence elasticache security group c

```
The AWS Fleet integration, Filebeat module, or similarly structured data is required to be compatible
24
       references = ["https://docs.aws.amazon.com/AmazonElastiCache/latest/APIReference/Welcome.html"]
25
       risk_score = 21
26
       rule_id = "7b3da11a-60a2-412e-8aa7-011e1eb9ed47"
27
       severity = "low"
28
       tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Monitoring"]
29
       timestamp_override = "event.ingested"
30
       type = "query"
31
32
       query = '''
33
34
       event.dataset:aws.cloudtrail and event.provider:elasticache.amazonaws.com and event.action:"Create
35
       event.outcome:success
36
37
38
39
       [[rule.threat]]
       framework = "MITRE ATT&CK"
40
       [[rule.threat.technique]]
41
       id = "T1136"
42
       name = "Create Account"
43
       reference = "https://attack.mitre.org/techniques/T1136/"
44
       [[rule.threat.technique.subtechnique]]
45
       id = "T1136.003"
46
       name = "Cloud Account"
47
       reference = "https://attack.mitre.org/techniques/T1136/003/"
48
49
50
51
       [rule.threat.tactic]
       id = "TA0003"
52
       name = "Persistence"
53
54
       reference = "https://attack.mitre.org/tactics/TA0003/"
```