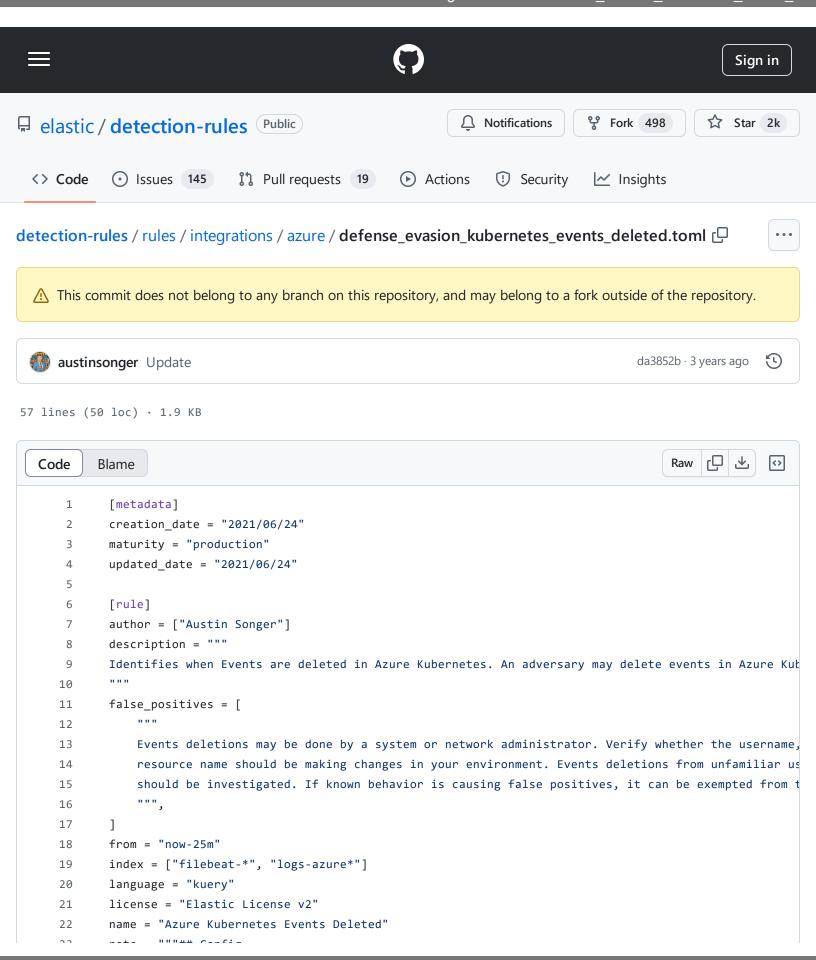
detection-rules/rules/integrations/azure/defense_evasion_kubernetes_events_deleted.toml at da3852b681cf1a33898b1535892eab1f3a76177a · elastic/detection-rules · GitHub - 31/10/2024 09:22 https://github.com/elastic/detection-

rules/blob/da3852b681cf1a33898b1535892eab1f3a76177a/rules/integrations/azure/defense evasion kubernetes events dele



detection-rules/rules/integrations/azure/defense_evasion_kubernetes_events_deleted.toml at da3852b681cf1a33898b1535892eab1f3a76177a · elastic/detection-rules · GitHub - 31/10/2024 09:22 https://github.com/elastic/detection-

rules/blob/da3852b681cf1a33898b1535892eab1f3a76177a/rules/integrations/azure/defense evasion kubernetes events dele

```
note =
                 ## CONTIG
۷3
       The Azure Fleet integration, Filebeat module, or similarly structured data is required to be compat
24
25
       references = [
           "https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#
26
27
28
       risk score = 47
       rule_id = "8b64d36a-1307-4b2e-a77b-a0027e4d27c8"
29
       severity = "medium"
30
       tags = ["Elastic", "Cloud", "Azure", "Continuous Monitoring", "SecOps", "Log Auditing"]
31
       timestamp override = "event.ingested"
32
       type = "query"
33
34
       query = '''
35
       event.dataset:azure.activitylogs and azure.activitylogs.operation_name:MICROSOFT.KUBERNETES/CONNECT
36
37
       event.outcome:(Success or success)
38
39
40
       [[rule.threat]]
41
       framework = "MITRE ATT&CK"
42
       [[rule.threat.technique]]
43
       id = "T1562"
44
       name = "Impair Defenses"
45
       reference = "https://attack.mitre.org/techniques/T1562/"
46
       [[rule.threat.technique.subtechnique]]
47
       id = "T1562.001"
48
       name = "Disable or Modify Tools"
49
       reference = "https://attack.mitre.org/techniques/T1562/001/"
50
51
52
53
54
       [rule.threat.tactic]
       id = "TA0005"
55
56
       name = "Defense Evasion"
57
       reference = "https://attack.mitre.org/tactics/TA0005/"
```