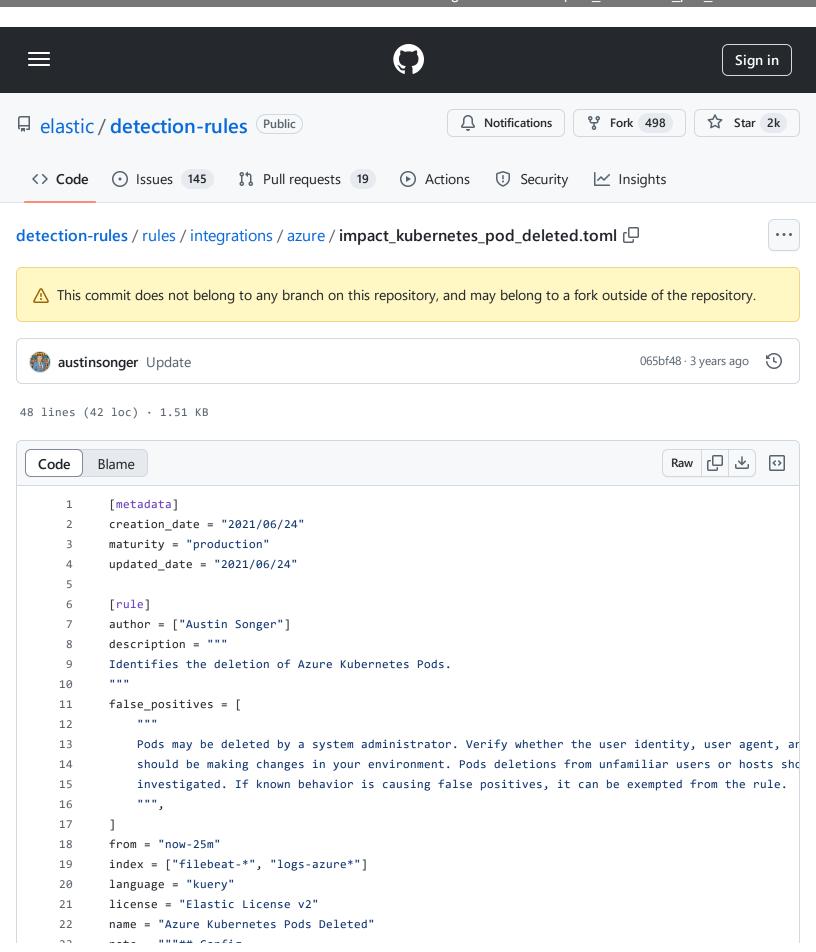
detection-rules/rules/integrations/azure/impact_kubernetes_pod_deleted.toml at 065bf48a9987cd8bd826c098a30ce36e6868ee46 · elastic/detection-rules · GitHub - 31/10/2024 09:23

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

rules/blob/065bf48a9987cd8bd826c098a30ce36e6868ee46/rules/integrations/azure/impact_kubernetes_pod_deleted.toml



detection-rules/rules/integrations/azure/impact_kubernetes_pod_deleted.toml at 065bf48a9987cd8bd826c098a30ce36e6868ee46 · elastic/detection-rules · GitHub - 31/10/2024 09:23

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

rules/blob/065bf48a9987cd8bd826c098a30ce36e6868ee46/rules/integrations/azure/impact_kubernetes_pod_deleted.toml

```
note =
                 ## CONTIG
۷3
24
25
       The Azure Fleet integration, Filebeat module, or similarly structured data is required to be compat
26
27
           "https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#
28
       1
29
       risk\_score = 47
       rule_id = "83a1931d-8136-46fc-b7b9-2db4f639e014"
30
       severity = "medium"
31
       tags = ["Elastic", "Cloud", "Azure", "Continuous Monitoring", "SecOps", "Asset Visibility"]
32
       timestamp_override = "event.ingested"
33
34
       type = "query"
35
       query = '''
36
37
       event.dataset:azure.activitylogs and azure.activitylogs.operation_name:MICROSOFT.KUBERNETES/CONNEC1
38
       event.outcome:(Success or success)
39
40
41
42
       [[rule.threat]]
       framework = "MITRE ATT&CK"
43
44
       [rule.threat.tactic]
45
       id = "TA0040"
46
47
       name = "Impact"
       reference = "https://attack.mitre.org/tactics/TA0040/"
48
```