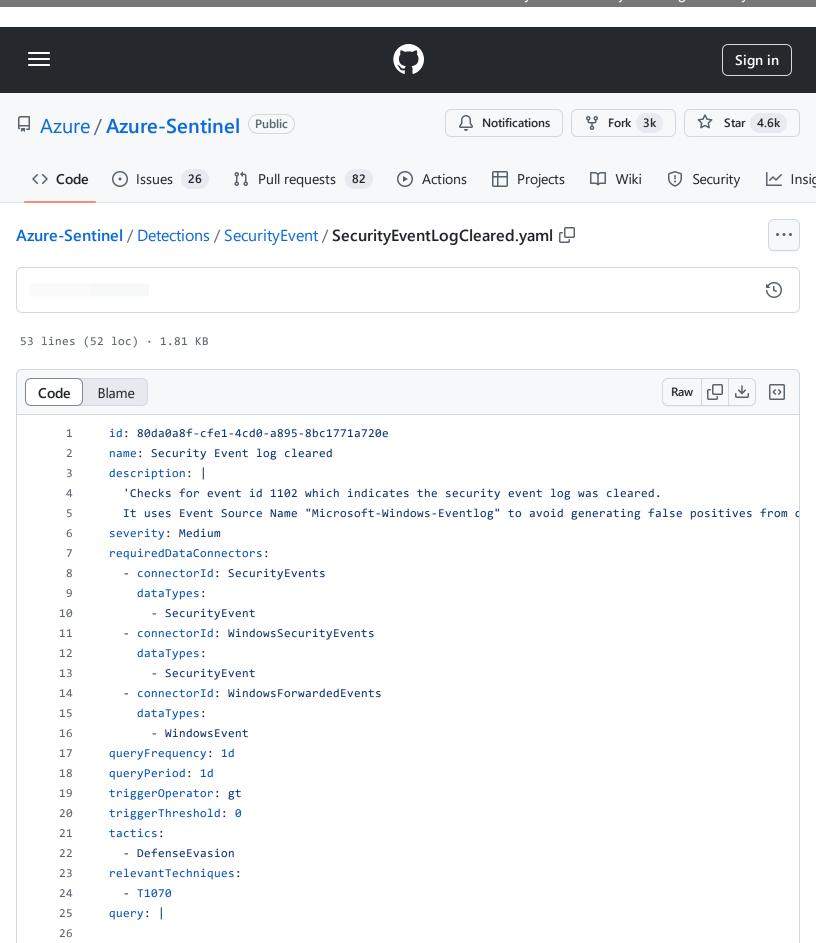
Azure-Sentinel/Detections/SecurityEvent/SecurityEventLogCleared.yaml at f99542b94afe0ad2f19a82cc08262e7ac8e1428e · Azure/Azure-Sentinel · GitHub - 31/10/2024 15:45 https://github.com/Azure/Azure-

Sentinel/blob/f99542b94afe0ad2f19a82cc08262e7ac8e1428e/Detections/SecurityEvent/SecurityEventLogCleared.yaml



Sentinel/blob/f99542b94afe0ad2f19a82cc08262e7ac8e1428e/Detections/SecurityEvent/SecurityEventLogCleared.yaml

```
27
         (union isfuzzy=true
28
29
         SecurityEvent
         | where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
30
         | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), EventCount = cour
31
         extend timestamp = StartTimeUtc, AccountCustomEntity = Account, HostCustomEntity = Computer
32
33
         ),
34
         WindowsEvent
35
         | where EventID == 1102 and Provider == "Microsoft-Windows-Eventlog"
36
         | extend Account = strcat(tostring(EventData.SubjectDomainName),"\\", tostring(EventData.Subject
37
         extend Activity= "1102 - The audit log was cleared."
38
         | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), EventCount = cour
39
         extend timestamp = StartTimeUtc, AccountCustomEntity = Account, HostCustomEntity = Computer
40
41
         )
         )
42
43
       entityMappings:
44
         - entityType: Account
45
           fieldMappings:
             - identifier: FullName
46
47
               columnName: AccountCustomEntity
         - entityType: Host
48
           fieldMappings:
49
50
             - identifier: FullName
51
               columnName: HostCustomEntity
       version: 1.1.1
52
       kind: Scheduled
53
```