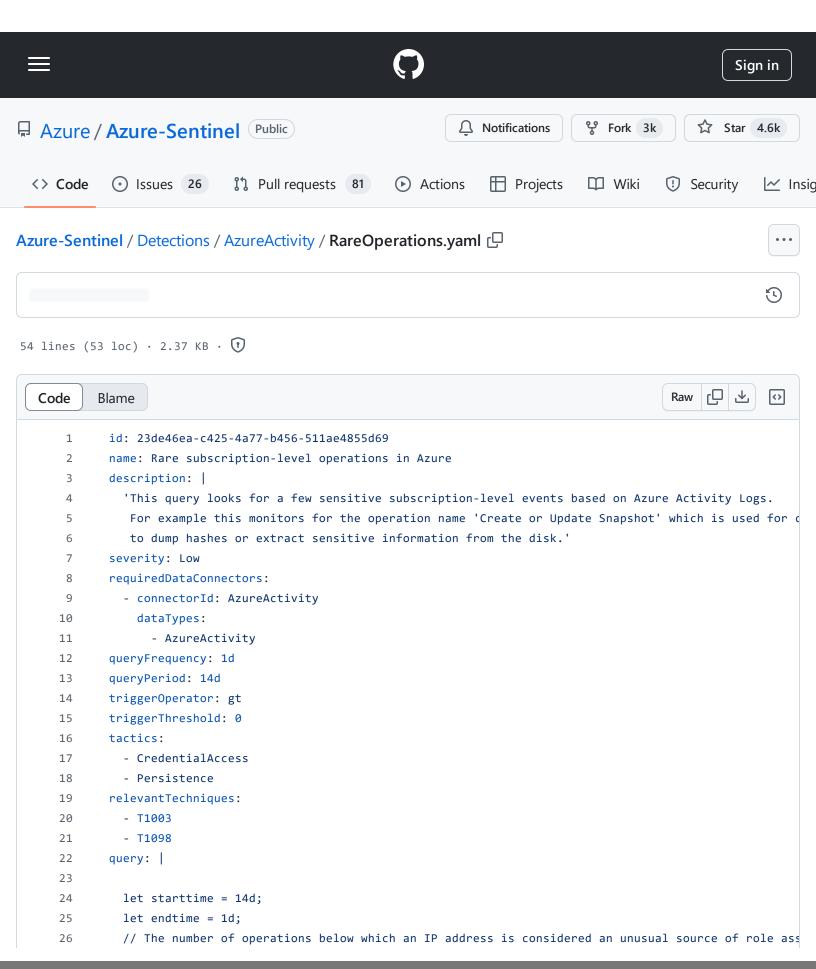
Azure-Sentinel/Detections/AzureActivity/RareOperations.yaml at e534407884b1ec5371efc9f76ead282176c9e8bb · Azure/Azure-Sentinel · GitHub - 31/10/2024 09:25 https://github.com/Azure/Azure-

Sentinel/blob/e534407884b1ec5371efc9f76ead282176c9e8bb/Detections/AzureActivity/RareOperations.yaml



Sentinel/blob/e534407884b1ec5371efc9f76ead282176c9e8bb/Detections/AzureActivity/RareOperations.yaml

```
27
         let alertOperationThreshold = 5;
28
         let SensitiveOperationList = dynamic(["microsoft.compute/snapshots/write", "microsoft.network/network)
         let SensitiveActivity = AzureActivity
29
         | where OperationNameValue in~ (SensitiveOperationList) or OperationNameValue hassuffix "listkeys
30
         | where ActivityStatusValue =~ "Success";
31
32
         SensitiveActivity
         | where TimeGenerated between (ago(starttime) .. ago(endtime))
33
         | summarize count() by CallerIpAddress, Caller, OperationNameValue
34
         | where count_ >= alertOperationThreshold
35
         | join kind = rightanti (
36
         SensitiveActivity
37
         | where TimeGenerated >= ago(endtime)
38
         | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), ActivityTimeStamp
39
         OperationIds = makelist(OperationId), CorrelationIds = makelist(CorrelationId), Resources = makel
40
         by CallerIpAddress, Caller, OperationNameValue
41
         ) on CallerIpAddress, Caller, OperationNameValue
42
43
         extend timestamp = StartTimeUtc, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
44
       entityMappings:
         - entityType: Account
45
           fieldMappings:
46
47
             - identifier: FullName
               columnName: AccountCustomEntity
48
         - entityType: IP
49
           fieldMappings:
50
             - identifier: Address
51
               columnName: IPCustomEntity
52
       version: 1.1.1
53
54
       kind: Scheduled
```