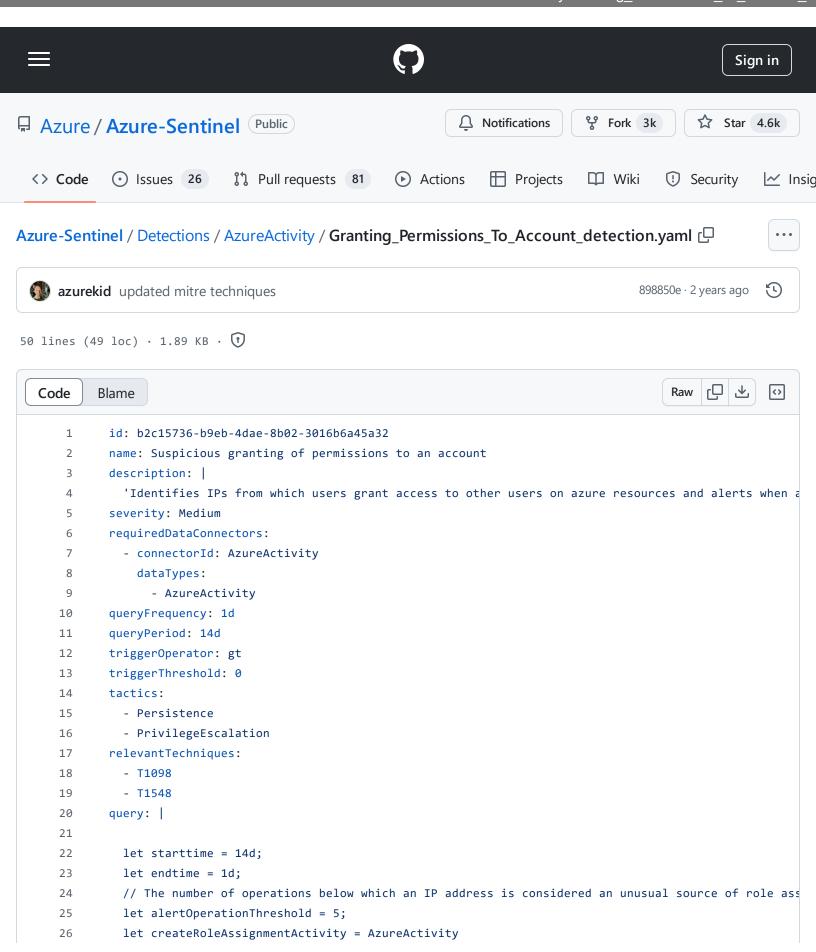
Azure-Sentinel/Detections/AzureActivity/Granting\_Permissions\_To\_Account\_detection.yaml at e534407884b1ec5371efc9f76ead282176c9e8bb · Azure/Azure-Sentinel · GitHub - 31/10/2024 09:21 https://github.com/Azure/Azure-

Sentinel/blob/e534407884b1ec5371efc9f76ead282176c9e8bb/Detections/AzureActivity/Granting Permissions To Account details of the control of the



Azure-Sentinel/Detections/AzureActivity/Granting\_Permissions\_To\_Account\_detection.yaml at e534407884b1ec5371efc9f76ead282176c9e8bb · Azure/Azure-Sentinel · GitHub - 31/10/2024 09:21 https://github.com/Azure/Azure-

Sentinel/blob/e534407884b1ec5371efc9f76ead282176c9e8bb/Detections/AzureActivity/Granting Permissions To Account d

```
27
         | where OperationNameValue =~ "microsoft.authorization/roleassignments/write";
28
         createRoleAssignmentActivity
         | where TimeGenerated between (ago(starttime) .. ago(endtime))
29
         | summarize count() by CallerIpAddress, Caller
30
         | where count_ >= alertOperationThreshold
31
         | join kind = rightanti (
32
         createRoleAssignmentActivity
33
         | where TimeGenerated > ago(endtime)
34
         | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), ActivityTimeStame
35
         OperationIds = make_set(OperationId), CorrelationId = make_set(CorrelationId), ActivityCountByCal
36
         by ResourceId, CallerIpAddress, Caller, OperationNameValue, Resource, ResourceGroup
37
         ) on CallerIpAddress, Caller
38
         extend timestamp = StartTimeUtc, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
39
40
       entityMappings:
41
         entityType: Account
           fieldMappings:
42
43
             - identifier: FullName
44
               columnName: AccountCustomEntity
45
         - entityType: IP
           fieldMappings:
46
47
             - identifier: Address
               columnName: IPCustomEntity
48
       version: 1.1.1
49
       kind: Scheduled
50
```