Sign in

Azure / **Azure-Sentinel** Public

Notifications · Fork 3k · Star 4.6k

Code · Issues 26 · Pull requests 81 · Actions · Projects · Wiki · Security · Insig

Azure-Sentinel / Detections / AzureActivity / **Granting_Permissions_To_Account_detection.yaml**

**azurekid** updated mitre techniques · 898850e · 2 years ago

50 lines (49 loc) · 1.89 KB ·

Code · Blame · Raw

```
id: b2c15736-b9eb-4dae-8b02-3016b6a45a32
name: Suspicious granting of permissions to an account
description: |
  'Identifies IPs from which users grant access to other users on azure resources and alerts when a
severity: Medium
requiredDataConnectors:
  - connectorId: AzureActivity
    dataTypes:
      - AzureActivity
queryFrequency: 1d
queryPeriod: 14d
triggerOperator: gt
triggerThreshold: 0
tactics:
  - Persistence
  - PrivilegeEscalation
relevantTechniques:
  - T1098
  - T1548
query: |

  let starttime = 14d;
  let endtime = 1d;
  // The number of operations below which an IP address is considered an unusual source of role ass
  let alertOperationThreshold = 5;
  let createRoleAssignmentActivity = AzureActivity
  | where OperationNameValue =~ "microsoft.authorization/roleassignments/write";
  createRoleAssignmentActivity
  | where TimeGenerated between (ago(starttime) .. ago(endtime))
  | summarize count() by CallerIpAddress, Caller
  | where count_ >= alertOperationThreshold
  | join kind = rightanti (
  createRoleAssignmentActivity
  | where TimeGenerated > ago(endtime)
  | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), ActivityTimeStamp
  OperationIds = make_set(OperationId), CorrelationId = make_set(CorrelationId), ActivityCountByCal
  by ResourceId, CallerIpAddress, Caller, OperationNameValue, Resource, ResourceGroup
  ) on CallerIpAddress, Caller
  | extend timestamp = StartTimeUtc, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
entityMappings:
  - entityType: Account
    fieldMappings:
      - identifier: FullName
        columnName: AccountCustomEntity
  - entityType: IP
    fieldMappings:
      - identifier: Address
        columnName: IPCustomEntity
version: 1.1.1
kind: Scheduled
```