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 / **RareOperations.yaml**

54 lines (53 loc) · 2.37 KB ·

Code | Blame | Raw

```
id: 23de46ea-c425-4a77-b456-511ae4855d69
name: Rare subscription-level operations in Azure
description: |
  'This query looks for a few sensitive subscription-level events based on Azure Activity Logs.
   For example this monitors for the operation name 'Create or Update Snapshot' which is used for c
   to dump hashes or extract sensitive information from the disk.'
severity: Low
requiredDataConnectors:
  - connectorId: AzureActivity
    dataTypes:
      - AzureActivity
queryFrequency: 1d
queryPeriod: 14d
triggerOperator: gt
triggerThreshold: 0
tactics:
  - CredentialAccess
  - Persistence
relevantTechniques:
  - T1003
  - T1098
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 SensitiveOperationList =  dynamic(["microsoft.compute/snapshots/write", "microsoft.network/ne
  let SensitiveActivity = AzureActivity
  | where OperationNameValue in~ (SensitiveOperationList) or OperationNameValue hassuffix "listkeys
  | where ActivityStatusValue =~ "Success";
  SensitiveActivity
  | where TimeGenerated between (ago(starttime) .. ago(endtime))
  | summarize count() by CallerIpAddress, Caller, OperationNameValue
  | where count_ >= alertOperationThreshold
  | join kind = rightanti (
  SensitiveActivity
  | where TimeGenerated >= ago(endtime)
  | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), ActivityTimeStamp
  OperationIds = makelist(OperationId), CorrelationIds = makelist(CorrelationId), Resources = makel
  by CallerIpAddress, Caller, OperationNameValue
  ) on CallerIpAddress, Caller, OperationNameValue
  | 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
```