Files

e534407

Go to file

- .azure-pipelines
- .github
- .script
- .vscode
- ASIM
- BYOML
- Dashboards
- DataConnectors
- Detections
  - ASimAuthentication
  - ASimDNS
  - ASimFileEvent
  - ASimNetworkSession
  - ASimProcess
  - ASimWebSession
  - AWSCloudTrail
  - AWSGuardDuty
  - AuditLogs
  - AzureActivity
    - AADHybridHealthADFSNewSer...
    - AADHybridHealthADFSService...
    - AADHybridHealthADFSSuspAp...
    - Creating_Anomalous_Number_...
    - Creation_of_Expensive_Compu...
    - Granting_Permissions_To_Acco...
    - NRT-AADHybridHealthADFSNe...
    - NRT_Creation_of_Expensive_Co...
    - New-CloudShell-User.yaml
    - NewResourceGroupsDeployed...
    - RareOperations.yaml
    - RareRunCommandPowerShellS...
    - TimeSeriesAnomaly_Mass_Clo...
  - AzureAppServices
  - AzureDevOpsAuditing
  - AzureDiagnostics
  - AzureFirewall

Azure-Sentinel / Detections / AzureActivity / RareOperations.yaml

Korving-F Adds another AzureActivity DetectionRule with incorre... 34cfa78 · 2 years ago History

CiscoUmbrella
CommonSecurityLog
DeviceEvents
DeviceFileEvents
DeviceNetworkEvents
DeviceProcessEvents

Code Blame 54 lines (53 loc) · 2.37 KB · Raw

```yaml
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 Activi
   For example this monitors for the operation name 'Create or Update Snapshot' which i
   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
  let alertOperationThreshold = 5;
  let SensitiveOperationList =  dynamic(["microsoft.compute/snapshots/write", "microsof
  let SensitiveActivity = AzureActivity
  | where OperationNameValue in~ (SensitiveOperationList) or OperationNameValue hassuff
  | 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), Activ
  OperationIds = makelist(OperationId), CorrelationIds = makelist(CorrelationId), Resou
  by CallerIpAddress, Caller, OperationNameValue
  ) on CallerIpAddress, Caller, OperationNameValue
  | extend timestamp = StartTimeUtc, AccountCustomEntity = Caller, IPCustomEntity = Cal
entityMappings:
  - entityType: Account
    fieldMappings:
      - identifier: FullName
        columnName: AccountCustomEntity
  - entityType: IP
    fieldMappings:
      - identifier: Address
        columnName: IPCustomEntity
version: 1.1.1
kind: Scheduled
```