53 lines (52 loc) · 1.81 KB

Code Blame Raw

```yaml
id: 80da0a8f-cfe1-4cd0-a895-8bc1771a720e
name: Security Event log cleared
description: |
  'Checks for event id 1102 which indicates the security event log was cleared.
  It uses Event Source Name "Microsoft-Windows-Eventlog" to avoid generating false positives from c
severity: Medium
requiredDataConnectors:
  - connectorId: SecurityEvents
    dataTypes:
      - SecurityEvent
  - connectorId: WindowsSecurityEvents
    dataTypes:
      - SecurityEvent
  - connectorId: WindowsForwardedEvents
    dataTypes:
      - WindowsEvent
queryFrequency: 1d
queryPeriod: 1d
triggerOperator: gt
triggerThreshold: 0
tactics:
  - DefenseEvasion
relevantTechniques:
  - T1070
query: |

```

```
    (union isfuzzy=true
    (
    SecurityEvent
    | where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
    | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), EventCount = cour
    | extend timestamp = StartTimeUtc, AccountCustomEntity = Account, HostCustomEntity = Computer
    ),
    (
    WindowsEvent
    | where EventID == 1102 and Provider == "Microsoft-Windows-Eventlog"
    | extend Account =  strcat(tostring(EventData.SubjectDomainName),"\\", tostring(EventData.Subject
    | extend Activity= "1102 - The audit log was cleared."
    | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), EventCount = cour
    | extend timestamp = StartTimeUtc, AccountCustomEntity = Account, HostCustomEntity = Computer
    )
    )
  entityMappings:
    - entityType: Account
      fieldMappings:
        - identifier: FullName
          columnName: AccountCustomEntity
    - entityType: Host
      fieldMappings:
        - identifier: FullName
          columnName: HostCustomEntity
  version: 1.1.1
  kind: Scheduled
```