



Azure / **Azure-Sentinel** Public

Notifications

Fork 3k

Star 4.6k

Code

Issues 26

Pull requests 82

Actions

Projects

Wiki

Security

Insights

Azure-Sentinel / Detections / SecurityEvent / SecurityEventLogCleared.yaml

53 lines (52 loc) · 1.81 KB

CodeBlame

RawCopyDownloadCode

```
1 id: 80da0a8f-cfe1-4cd0-a895-8bc1771a720e
2 name: Security Event log cleared
3 description: |
4     'Checks for event id 1102 which indicates the security event log was cleared.
5     It uses Event Source Name "Microsoft-Windows-Eventlog" to avoid generating false positives from c
6 severity: Medium
7 requiredDataConnectors:
8     - connectorId: SecurityEvents
9       dataTypes:
10         - SecurityEvent
11     - connectorId: WindowsSecurityEvents
12       dataTypes:
13         - SecurityEvent
14     - connectorId: WindowsForwardedEvents
15       dataTypes:
16         - WindowsEvent
17 queryFrequency: 1d
18 queryPeriod: 1d
19 triggerOperator: gt
20 triggerThreshold: 0
21 tactics:
22     - DefenseEvasion
23 relevantTechniques:
24     - T1070
25 query: |
26
```

```
27     (union isfuzzy=true
28     (
29     SecurityEvent
30     | where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
31     | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), EventCount = count(*)
32     | extend timestamp = StartTimeUtc, AccountCustomEntity = Account, HostCustomEntity = Computer
33     ),
34     (
35     WindowsEvent
36     | where EventID == 1102 and Provider == "Microsoft-Windows-Eventlog"
37     | extend Account = strcat(tostring(EventData.SubjectDomainName), "\\ ", tostring(EventData.SubjectName))
38     | extend Activity= "1102 - The audit log was cleared."
39     | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), EventCount = count(*)
40     | extend timestamp = StartTimeUtc, AccountCustomEntity = Account, HostCustomEntity = Computer
41     )
42     )
43 entityMappings:
44   - entityType: Account
45     fieldMappings:
46       - identifier: FullName
47         columnName: AccountCustomEntity
48   - entityType: Host
49     fieldMappings:
50       - identifier: FullName
51         columnName: HostCustomEntity
52 version: 1.1.1
53 kind: Scheduled
```