



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 / ADFSDBNamedPipeConnection.yaml

85 lines (85 loc) · 3.76 KB

CodeBlame

Raw

```
1 id: dcd9b9fc-c239-4764-a9f9-3612e6dff49c
2 name: ADFS Database Named Pipe Connection
3 description: |
4     'This detection uses Sysmon telemetry to detect suspicious local connections via a named pipe to
5     In order to use this query you need to be collecting Sysmon EventIdD 18 (Pipe Connected).
6     If you do not have Sysmon data in your workspace this query will raise an error stating:
7     Failed to resolve scalar expression named "[@Name]"'
8 severity: Medium
9 requiredDataConnectors:
10     - connectorId: SecurityEvents
11       dataTypes:
12         - SecurityEvent
13     - connectorId: WindowsSecurityEvents
14       dataTypes:
15         - SecurityEvent
16 queryFrequency: 1d
17 queryPeriod: 1d
18 triggerOperator: gt
19 triggerThreshold: 0
20 tactics:
21     - Collection
22 relevantTechniques:
23     - T1005
24 tags:
25     - Solorigate
26     - NOBELIUM
```

```
27     - SimuLand
28 query: |
29     // Adjust this to use a longer timeframe to identify ADFS servers
30     //let lookback = 6d;
31     // Adjust this to adjust the key export detection timeframe
32     //let timeframe = 1d;
33     // Start by identifying ADFS servers to reduce FP chance
34     let ADFS_Servers = (
35     Event
36     //| where TimeGenerated > ago(timeframe+lookback)
37     | where Source == "Microsoft-Windows-Sysmon"
38     | where EventID == 18
39     | extend EventData = parse_xml(EventData).DataItem.EventData.Data
40     | mv-expand bagexpansion=array EventData
41     | evaluate bag_unpack(EventData)
42     | extend Key = tostring(column_ifexists('@Name', "")), Value = column_ifexists('#text', "")
43     | evaluate pivot(Key, any(Value), TimeGenerated, Source, EventLog, Computer, EventLevel, EventLev
44     | extend Image = column_ifexists("Image", "")
45     | extend process = split(Image, '\\', -1)[-1]
46     | where process =~ "Microsoft.IdentityServer.ServiceHost.exe"
47     | summarize by Computer);
48     // Look for ADFS servers where Named Pipes event are present
49     Event
50     //| where TimeGenerated > ago(timeframe)
51     | where Source == "Microsoft-Windows-Sysmon"
52     | where EventID == 18
53     | where Computer in~ (ADFS_Servers)
54     | extend RenderedDescription = tostring(split(RenderedDescription, ":")[0])
55     | extend EventData = parse_xml(EventData).DataItem.EventData.Data
56     | mv-expand bagexpansion=array EventData
57     | evaluate bag_unpack(EventData)
58     | extend Key = tostring(column_ifexists('@Name', "")), Value = column_ifexists('#text', "")
59     | evaluate pivot(Key, any(Value), TimeGenerated, Source, EventLog, Computer, EventLevel, EventLev
60     | extend RuleName = column_ifexists("RuleName", ""),
61         TechniqueId = column_ifexists("TechniqueId", ""),
62         TechniqueName = column_ifexists("TechniqueName", ""),
63         Image = column_ifexists("Image", ""),
64         PipeName = column_ifexists("PipeName", ""),
65         EventType = column_ifexists("EventType", "")
66     | parse RuleName with * 'technique_id=' TechniqueId ',' * 'technique_name=' TechniqueName
67     // Look for Pipe related to querying the WID
68     | where PipeName == "\\MICROSOFT##WID\\tsql\\query"
69     | extend process = split(Image, '\\', -1)[-1]
70     // Exclude expected processes
71     | where process !in ("Microsoft.IdentityServer.ServiceHost.exe", "Microsoft.Identity.Health.Adfs.
72     | extend Operation = RenderedDescription
```

```
73 | project-reorder TimeGenerated, EventType, Operation, process, Image, Computer, UserName
74 | extend HostCustomEntity = Computer, AccountCustomEntity = UserName
75 entityMappings:
76 - entityType: Account
77   fieldMappings:
78     - identifier: FullName
79       columnName: AccountCustomEntity
80 - entityType: Host
81   fieldMappings:
82     - identifier: FullName
83       columnName: HostCustomEntity
84 version: 1.0.1
85 kind: Scheduled
```