



Azure / Azure-Sentinel Public

Notifications

Fork 3k

Star 4.6k

Code

Issues 26

Pull requests 81

Actions

Projects

Wiki

Security

Insights

Azure-Sentinel / Detections / AzureActivity

...

/ Creating\_Anomalous\_Number\_Of\_Resources\_detection.yaml

ShaniFelig add Scheduled kind to all existng templates (solutions + detections) afe1ba6 · 3 years ago

64 lines (63 loc) · 3.42 KB ·

Code Blame

Raw

```
1 id: 361dd1e3-1c11-491e-82a3-bb2e44ac36ba
2 name: Suspicious number of resource creation or deployment activities
3 description: |
4     'Indicates when an anomalous number of VM creations or deployment activities occur in Azure via t
5     The anomaly detection identifies activities that have occurred both since the start of the day 1
6     The start of the day is considered 12am UTC time.'
7 severity: Medium
8 requiredDataConnectors:
9     - connectorId: AzureActivity
10     dataTypes:
11         - AzureActivity
12 queryFrequency: 1d
13 queryPeriod: 7d
14 triggerOperator: gt
15 triggerThreshold: 0
16 tactics:
17     - Impact
18 relevantTechniques:
19     - T1496
20 query: |
21
22     let szOperationNames = dynamic(["microsoft.compute/virtualMachines/write", "microsoft.resources/c
23     let starttime = 7d;
24     let endtime = 1d;
25     AzureActivity
```

```
26     | where TimeGenerated between (startofday(ago(starttime)) .. startofday(ago(endtime)))
27     | where OperationNameValue in~ (szOperationNames)
28     | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), ActivityTimeStamps = makelist(ActivityTimestamp),
29     OperationIds = makelist(OperationId), CallerIpAddress = makelist(CallerIpAddress), CorrelationId = makelist(CorrelationId)
30     by ResourceId, Caller, OperationNameValue, Resource, ResourceGroup
31     | mvexpand CallerIpAddress
32     | where isnotempty(CallerIpAddress)
33     | make-series dResourceCount=dcount(ResourceId) default=0 on StartTimeUtc in range(startofday(ago(14d)), startofday(ago(endtime)))
34     by Caller, tostring(ActivityTimestamp), tostring(ActivityStatusValue), tostring(OperationIds), tostring(CorrelationId)
35     | extend (RSquare,Slope,Variance,RVariance,Interception,LineFit)=series_fit_line(dResourceCount)
36     | where Slope > 0.2
37     | join kind=leftsemi (
38     // Last day's activity is anomalous
39     AzureActivity
40     | where TimeGenerated >= startofday(ago(endtime))
41     | where OperationNameValue in~ (szOperationNames)
42     | summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), ActivityTimeStamps = makelist(ActivityTimestamp),
43     OperationIds = makelist(OperationId), CallerIpAddress = makelist(CallerIpAddress), CorrelationId = makelist(CorrelationId)
44     by ResourceId, Caller, OperationNameValue, Resource, ResourceGroup
45     | mvexpand CallerIpAddress
46     | where isnotempty(CallerIpAddress)
47     | make-series dResourceCount=dcount(ResourceId) default=0 on StartTimeUtc in range(startofday(ago(14d)), startofday(ago(endtime)))
48     by Caller, tostring(ActivityTimestamp), tostring(ActivityStatusValue), tostring(OperationIds), tostring(CorrelationId)
49     | extend (RSquare,Slope,Variance,RVariance,Interception,LineFit)=series_fit_line(dResourceCount)
50     | where Slope > 0.2
51     ) on Caller, CallerIpAddress
52     | mvexpand todynamic(ActivityTimestamp), todynamic(ActivityStatusValue), todynamic(OperationIds), todynamic(CorrelationId)
53     | extend timestamp = ActivityTimestamp, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
54 entityMappings:
55   - entityType: Account
56     fieldMappings:
57       - identifier: FullName
58         columnName: AccountCustomEntity
59   - entityType: IP
60     fieldMappings:
61       - identifier: Address
62         columnName: IPCustomEntity
63 version: 1.1.0
64 kind: Scheduled
```