Product ⌄   Solutions ⌄   Resources ⌄   Open Source ⌄   Enterprise ⌄   Pricing

Sign in   Sign up

🖰 Azure / **Azure-Sentinel**   Public

🔔 Notifications   ⑂ Fork 3k   ☆ Star 4.6k

<> Code   ⊘ Issues 28   ⥋ Pull requests 84   ▶ Actions   ⊞ Projects   📖 Wiki   🛡 Security   📈 Insights

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 /

/ Creating_Anomalous_Number_Of_Resources_detection.yaml ⧉

🖰 ShaniFelig   add Scheduled kind to all exisitng templates (solutions + det...   afe1ba6 · 3 years ago   🕘 History

Code | Blame   64 lines (63 loc) · 3.42 KB · 🛡   Raw ⧉ ⤓ <>

```yaml
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
5     The anomaly detection identifies activities that have occurred both since the start o
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
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), Activ
29      OperationIds = makelist(OperationId), CallerIpAddress = makelist(CallerIpAddress), Co
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(s
34      by Caller, tostring(ActivityTimeStamp), tostring(ActivityStatusValue), tostring(Opera
35    | extend (RSquare,Slope,Variance,RVariance,Interception,LineFit)=series_fit_line(dRes
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), Activ
43      OperationIds = makelist(OperationId), CallerIpAddress = makelist(CallerIpAddress), Co
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(s
48      by Caller, tostring(ActivityTimeStamp), tostring(ActivityStatusValue), tostring(Opera
49    | extend (RSquare,Slope,Variance,RVariance,Interception,LineFit)=series_fit_line(dRes
50    | where Slope > 0.2
51    ) on Caller, CallerIpAddress
52    | mvexpand todynamic(ActivityTimeStamp), todynamic(ActivityStatusValue), todynamic(Op
53    | extend timestamp = ActivityTimeStamp, AccountCustomEntity = Caller, IPCustomEntity
54  entityMappings:
55    - entityType: Account
56      fieldMappings:
```

- CiscoUmbrella
- CommonSecurityLog
- DeviceEvents
- DeviceFileEvents
- DeviceNetworkEvents
- DeviceProcessEvents

```
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
```