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

f99542b

Go to file

- .azure-pipelines
- .github
- .script
- .vscode
- ASIM
- BYOML
- Dashboards
- DataConnectors
- Detections
  - ASimAuthentication
  - ASimDNS
  - ASimFileEvent
  - ASimNetworkSession
  - ASimProcess
  - ASimWebSession
  - AWSCloudTrail
  - AWSGuardDuty
  - AuditLogs
  - AzureActivity
  - AzureAppServices
  - AzureDevOpsAuditing
  - AzureDiagnostics
  - AzureFirewall
  - CiscoUmbrella
  - CommonSecurityLog
  - DeviceEvents
  - DeviceFileEvents
  - DeviceNetworkEvents
  - DeviceProcessEvents
  - DnsEvents
  - Duo Security
  - GitHub
  - Heartbeat
  - LAQueryLogs
  - MultipleDataSources
  - OfficeActivity

Azure-Sentinel / Detections / SecurityEvent / ADFSDBNamedPipeConnection.yaml

Pete Bryan Updating version 3f09ede · 3 years ago History

Code Blame 85 lines (85 loc) · 3.76 KB · Raw

```
id: dcdf9bfc-c239-4764-a9f9-3612e6dff49c
name: ADFS Database Named Pipe Connection
description: |
  'This detection uses Sysmon telemetry to detect suspicious local connections via a na
  In order to use this query you need to be collecting Sysmon EventIdD 18 (Pipe Connect
  If you do not have Sysmon data in your workspace this query will raise an error stati
  Failed to resolve scalar expression named "[@Name]"'
severity: Medium
requiredDataConnectors:
  - connectorId: SecurityEvents
    dataTypes:
      - SecurityEvent
  - connectorId: WindowsSecurityEvents
    dataTypes:
      - SecurityEvent
queryFrequency: 1d
queryPeriod: 1d
triggerOperator: gt
triggerThreshold: 0
tactics:
  - Collection
relevantTechniques:
  - T1005
tags:
  - Solorigate
  - NOBELIUM
  - SimuLand
query: |
  // Adjust this to use a longer timeframe to identify ADFS servers
  //let lookback = 6d;
  // Adjust this to adjust the key export detection  timeframe
  //let timeframe = 1d;
  // Start be identifying ADFS servers to reduce FP chance
  let ADFS_Servers = (
  Event
  //| where TimeGenerated > ago(timeframe+lookback)
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 18
  | extend EventData = parse_xml(EventData).DataItem.EventData.Data
  | mv-expand bagexpansion=array EventData
  | evaluate bag_unpack(EventData)
  | extend Key = tostring(column_ifexists('@Name', "")), Value = column_ifexists('#text
  | evaluate pivot(Key, any(Value), TimeGenerated, Source, EventLog, Computer, EventLev
  | extend Image = column_ifexists("Image", "")
  | extend process = split(Image, '\\', -1)[-1]
  | where process =~ "Microsoft.IdentityServer.ServiceHost.exe"
  | summarize by Computer);
  // Look for ADFS servers where Named Pipes event are present
  Event
  //| where TimeGenerated > ago(timeframe)
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 18
  | where Computer in~ (ADFS_Servers)
  | extend RenderedDescription = tostring(split(RenderedDescription, ":")[0])
  | extend EventData = parse_xml(EventData).DataItem.EventData.Data
  | mv-expand bagexpansion=array EventData
  | evaluate bag_unpack(EventData)
```

- ProofpointPOD
- PulseConnectSecure
- QualysVM
- QualysVMV2
- SecurityAlert
- SecurityEvent

```
  | evaluate bag_unpack(EventData)
  | extend Key = tostring(column_ifexists('@Name', "")), Value = column_ifexists('#text
  | evaluate pivot(Key, any(Value), TimeGenerated, Source, EventLog, Computer, EventLev
  | extend RuleName = column_ifexists("RuleName", ""),
      TechniqueId = column_ifexists("TechniqueId", ""),
      TechniqueName = column_ifexists("TechniqueName", ""),
      Image = column_ifexists("Image", ""),
      PipeName = column_ifexists("PipeName", ""),
      EventType = column_ifexists("EventType", "")
  | parse RuleName with * 'technique_id=' TechniqueId ',' * 'technique_name=' Technique
  // Look for Pipe related to querying the WID
  | where PipeName == "\\MICROSOFT##WID\\tsql\\query"
  | extend process = split(Image, '\\', -1)[-1]
  // Exclude expected processes
  | where process !in ("Microsoft.IdentityServer.ServiceHost.exe", "Microsoft.Identity.
  | extend Operation = RenderedDescription
  | project-reorder TimeGenerated, EventType, Operation, process, Image, Computer, User
  | extend HostCustomEntity = Computer, AccountCustomEntity = UserName
entityMappings:
  - entityType: Account
    fieldMappings:
      - identifier: FullName
        columnName: AccountCustomEntity
  - entityType: Host
    fieldMappings:
      - identifier: FullName
        columnName: HostCustomEntity
version: 1.0.1
kind: Scheduled
```