Custom Kusto Queries for Syslog Connector

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Contents

Heartbeat

```
Heartbeat
| where Computer == "$Target_Hostname"
```

CEF Log Query

```
CommonSecurityLog
| sort by TimeGenerated desc
```

Syslog Query

```
Syslog
| sort by TimeGenerated desc
```

Custom Log Parsing and extraction

Cron Log Trace

```
//Cron Job
Syslog
| where Facility == "cron"
| extend msg = SyslogMessage
| extend FoundData = extract_all(@"(.*) (INFO|DEBUG|CMD) (.*)", msg)
| extend User = FoundData[0][0]
| extend Action  = FoundData[0][1]
| extend Command = FoundData[0][2]
| project Facility ,User, Action, Command
```

Cron Log Summerize

```
Syslog
| where Facility == "cron"
| extend msg = SyslogMessage
| extend FoundData = extract_all(@"(.*) (INFO|DEBUG|CMD) (.*)", msg)
| extend User = FoundData[0][0]
| extend Action  = FoundData[0][1]
| extend Command = FoundData[0][2]
| summarize count() by tostring(FoundData[0][0]),tostring(FoundData[0][1]),tostring(FoundData[0][2])
```

Cisco Firepower Syslog Example

```
// Cisco Firepower syslog
//test message
//print msg = "DeviceUUID: 8e13b3d0-58c6-11e6-b4f5-c326b4de675a, AccessControlRuleAction: Allow, SrcIP: 192.16
Syslog
| where Facility == "local0"
| extend msg = SyslogMessage
| extend FoundData = extract_all(@"(\s?([\w\d\s]+):\s([\w\d\s-.]+))", msg)
//| project array_length(FoundData) // to get the number of items in the array
//| project FoundData[0][1],FoundData[0][2],FoundData[1][1],FoundData[1][2],FoundData[2][1],FoundData[2][2],Fo
//| extend FoundData[0][1] == FoundData[0][2]
| extend DeviceUUID = FoundData[0][2]
| extend AccessControlRuleAction = FoundData[1][2]
| extend SrcIP = FoundData[2][2]
| extend DstIP = FoundData[3][2]
| extend SrcPort = FoundData[4][2]
| extend DstPort = FoundData[5][2]
| extend Protocol = FoundData[6][2]
| extend IngressInterface = FoundData[7][2]
| extend IngressZone = FoundData[8][2]
| extend ACPolicy = FoundData[9][2]
| extend AccessControlRuleName = FoundData[10][2]
| extend Prefilter_Policy = FoundData[11][2]
| extend User = FoundData[12][2]
| extend ConnectionDuration = FoundData[13][2]
| extend InitiatorPackets = FoundData[14][2]
| extend ResponderPackets = FoundData[15][2]
| extend InitiatorBytes = FoundData[16][2]
| extend ResponderBytes = FoundData[17][2]
| extend NAPPolicy = FoundData[18][2]
| project DeviceUUID,AccessControlRuleAction,SrcIP,DstIP,SrcPort,DstPort,Protocol,IngressInterface,IngressZone
```

Syslog Parsing example

```
print msg = "DeviceUUID: 8e13b3d0-58c6-11e6-b4f5-c326b4de675a, AccessControlRuleAction: Allow, SrcIP: 192.168.
| where msg startswith "DeviceUUID: "
| parse msg with "DeviceUUID: " myDeviceUUID
                      "AccessControlRuleAction: " myAction
                      "SrcIP: " mySrcIP
                      "DstIP: " myDstIP
                      "SrcPort: " *
| project myDeviceUUID,myAction,mySrcIP,myDstIP
```

Windows Event Parsing

```
//WindowsEvent filer
// $table,TenantId,SourceSystem,TimeGenerated,Provider,Channel,Computer,Task,EventLevel,EventLevelName,Data,Ev
print msg = '"WindowsEvent,"008a7730-fcac-4f8a-9d63-195f302e3f25",OpsManager,"2019-11-26T10:01:24.71Z","Micros
| extend data=split(msg,',')
| extend Table = data[0]
| extend TenantId = data[1]
| extend SourceSystem = data[2]
| extend TimeGenerated = data[3]
| extend Provider = data[4]
| extend Channel = data[5]
| extend Computer = data[6]
| extend Task = data[7]
| extend EventLevel = data[8]
| extend EventLevelName = data[9]
| extend Data = data[10]
| extend EventID = data[11]
| extend ManagementGroupName = data[12]
| extend Username_CF = data[13]
| extend IPAddress = data[14]
| extend LogonType_CF = data[15]
| extend Type = data[16]
| extend _ResourceId = data[17]
| project Table,TenantId,SourceSystem,TimeGenerated,Provider,Channel,Computer,Task,EventLevel,EventLevelName,D
```

Edgie Enabled