Fal.Con 2024 Dev 24 Lab

CQL documentation: https://library.humio.com/data-analysis/data-analysis-docs.html

1. Find destination IP addresses that are in 2 or more third-party vendor's logs

Required functions:
groupBy()
  collect()
  count()

2. Find all client IP addresses in the 52.0.0.0/6 range (52.0.0.1 - 55.255.255.254) within all third-party vendor log sources

Required functions:
cidr()
groupBy()
  collect()
  count()

3. Case statements and using saved queries

Required functions:
case()
:= operator

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624#logon-types-and-descriptions

```
// This case statement enriches the LogonType with a human readable Logon Title
case{
LogonType=0 | readable_LogonType:="System";
LogonType=2 | readable_LogonType:="Interactive";
LogonType=3 | readable_LogonType:="Network";
LogonType=4 | readable_LogonType:="Batch";
LogonType=5 | readable_LogonType:="Service";
LogonType=7 | readable_LogonType:="Unlock";
LogonType=8 | readable_LogonType:="NetowrkCleartext";
LogonType=9 | readable_LogonType:="NewCredentials";
LogonType=10 | readable_LogonType:="RemoteInteractive";
LogonType=11 | readable_LogonType:="CachedInteractive";
LogonType=12 | readable_LogonType:="CahedRemoteInteractive";
LogonType=13 | readable_LogonType:="CachedUnlock";
*;
}
```

Using the saved query

```
#type=falcon-raw-data | #event_simpleName=UserLogon
|$"LogonType"()
|groupBy([LogonType], function=collect([readable_LogonType]))
```

4. Simple regex demo

Find any events that mention powershell executions that use the flag `-w hidden`

Use `/<your regex string here>/i` and (if needed https://regex101.com/)

5. Join example

Find all accounts which have failed logon and successful logons.

Required functions:
join()
groupBy()
    collect()