

(AMA) Data Collection Rules

(Windows) xpath query filtering

Security!*[System[(EventID=4648)]] and
*[EventData[Data[@Name='ProcessName']='C:\Windows\System32\consent.exe']]

Ingestion-time Transformations

| **Project-away** -> columns

| **where eventdata matches "xxx"** -> filter rows out

