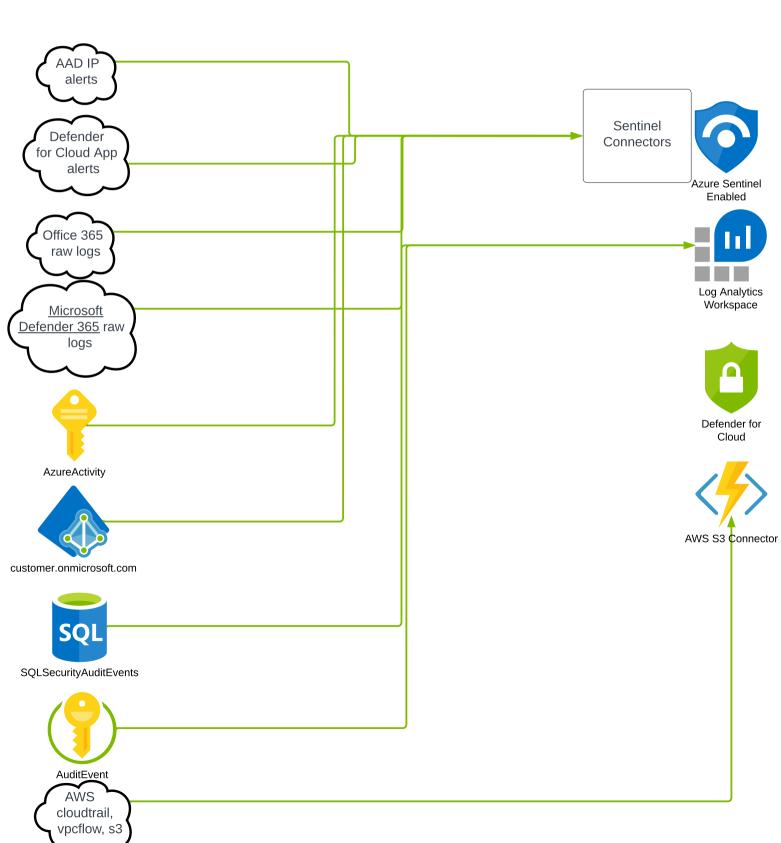
(Windows) xpath query filtering Security!*[System[(EventID=4648)]] and *[EventData[Data[@Name='ProcessName']='C:\Windows\System32\consent.exe']] Ingestion-time Transformations | Project-away -> columns | where eventdata matches "xxx" -> filter rows out



Curated Rules/Detections Azure-Sentinel/Detections at master - Azure/Azure-Sentinel (github.com) Fusion Alerts Advanced multistage attack UEBA Tables Identify advanced threats with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel | Microsoft Docs

detection in Microsoft Sentinel

Microsoft Docs

