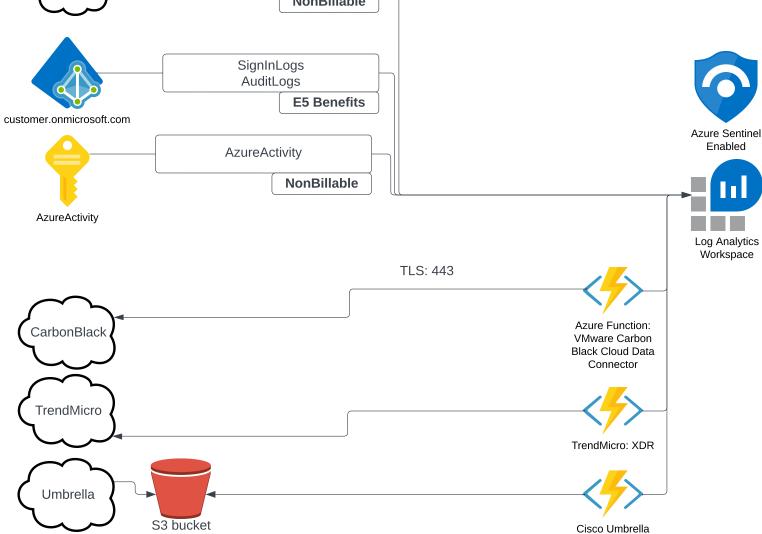
## (Mindows) xpath query filtering Security!\*[System[(EventID=4648)]] and \*[EventData[Data[@Name='ProcessName']='C:\Windows\System32\consent.exe']] Ingestion-time Transformations | Project-away -> columns | | where eventdata matches "xxx" -> filter rows out Office Office Activity 365 NonBillable SignInLogs AuditLogs E5 Benefits



## **Curated Rules/Detections**

Azure-Sentinel/Detections at master
· Azure/Azure-Sentinel (github.com)

Fusion Alerts
Advanced multistage attack
detection in Microsoft Sentinel |
Microsoft Docs

## UEBA Tables

Identify advanced threats with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel | Microsoft Docs



TABLES: SecurityAlerts SecurityIncidents

OfficeActivity

AzureActivity

SignInLogs AuditLogs

CarbonBlackEvents\_CL CarbonBlackAuditLogs\_CL CarbonBlackNotifications\_CL

TrendMicro\_XDR\_WORKBENCH\_CL
TrendMicro\_XDR\_RCA\_Task\_CL
TrendMicro\_XDR\_RCA\_Result\_CL
TrendMicro\_XDR\_OAT\_CL

Cisco\_Umbrella\_dns\_CL Cisco\_Umbrella\_proxy\_CL Cisco\_Umbrella\_ip\_CL Cisco\_Umbrella\_cloudfirewall\_CL