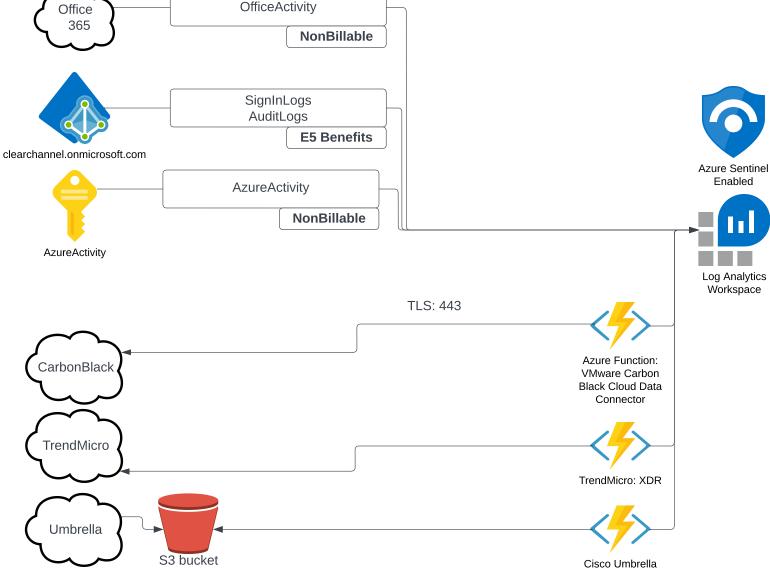
(Windows) xpath query filtering Security!*[System[(EventID=4648)]] and *[EventData[Data[@Name='ProcessName']='C:\Windows\System32\consent.exe']] Ingestion-time Transformations | Project-away -> columns | where eventdata matches "xxx" -> filter rows out Office Office 365 NonBillable



Curated Rules/Detections

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

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