

(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

Alerts




Microsoft 365 Defender

Advanced Hunting Logs

E5 Benefits

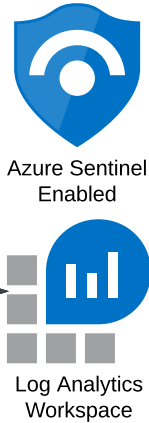
Defender for O365
Defnder for Endpoint
Defender for Identity
Defnder for Cloud Apps
AAD Identity Protection

Alerts



Defender for Cloud

NonBillable



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


AlertInfo
AlertEvidence

DeviceInfo
DeviceNetworkInfo
DeviceProcessEvents
DeviceNetworkEvents
DeviceFileEvents
DeviceRegistryEvents
DeviceLogonEvents
DeviceImageLoadEvents
DeviceEvents
DeviceFileCertificateInfo

IdentityDirectoryEvents
IdentityLogonEvents
IdentityQueryEvents

CloudAppEvents

EmailEvents
EmailUrlInfo
EmailAttachmentInfo
EmailPostDeliveryEvents
UrlClickEvents



red canary