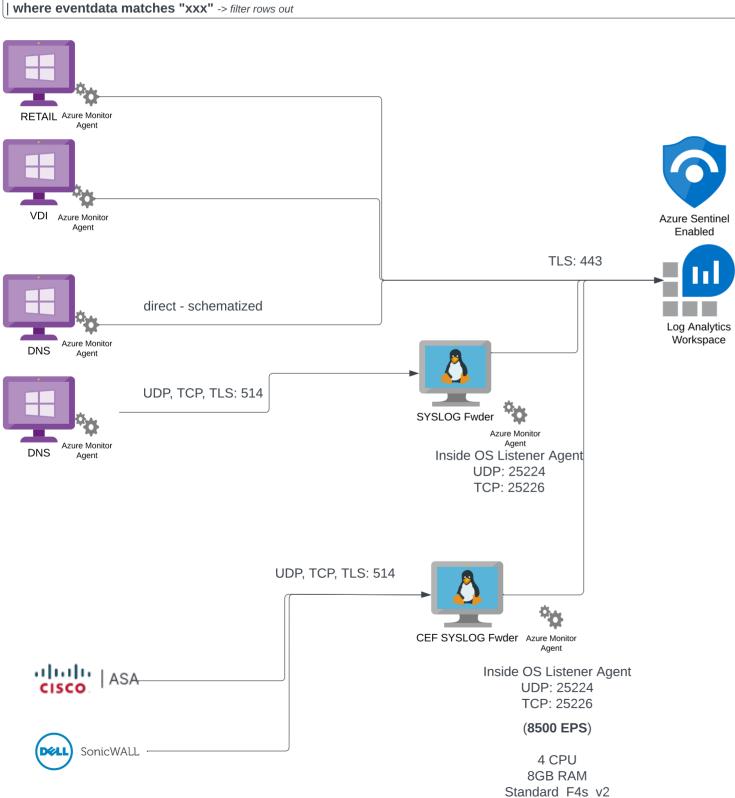**(AMA) Data Collection Rules**

(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*

RETAIL Azure Monitor Agent

VDI Azure Monitor Agent

DNS Azure Monitor Agent

direct - schematized

DNS Azure Monitor Agent

UDP, TCP, TLS: 514

SYSLOG Fwder

Azure Monitor Agent

Inside OS Listener Agent
UDP: 25224
TCP: 25226

TLS: 443

Azure Sentinel Enabled

Log Analytics Workspace

Curated Rules/Detections

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

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

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

red canary

TABLES:
SecurityAlerts
SecurityIncidents
CommonSecurityLogs
Syslog
SecurityEvent
Events
DnsEvents

UDP, TCP, TLS: 514

CEF SYSLOG Fwder Azure Monitor Agent

Inside OS Listener Agent
UDP: 25224
TCP: 25226

(**8500 EPS**)

4 CPU
8GB RAM
Standard_F4s_v2

CISCO | ASA

DELL SonicWALL