Conexión de Sondas de Seguridad OT

Problema

Las organizaciones industriales que se plantean desplegar soluciones de seguridad industrial (OT) se enfrentan al reto de como poder consolidar el trafico proveniente de los puntos de captura, muy números y dispersos geográficamente en un punto central donde aplicar toda la inteligencia. Realizar un piloto en una única ubicación resulta sencillo, pero el despliegue real en toda la red suele ser muy complejo

El principal problema suele ser la red de transporte que se emplea, en muchos casos con tecnologías de bajo caudal y flexibilidad, como PDH o SDH. Desplegar muchas sondas por toda la red no resuelve el problema, ya que aunque se reduzca la cantidad de información a transmitir al generar las sondas los metadatos necesarios para el análisis de la información, no se elimina el problema de tener que transportar esta información hasta l consola central de gestión

Otro problema típico es al respecto de la captura de datos en si misma. Si bien estos equipos industriales manejan tráficos muy pequeños, no resulta sencillo poder copiarlos en origen, ya que los equipos de comunicaciones empleados en este entorno no tienen estas capacidades

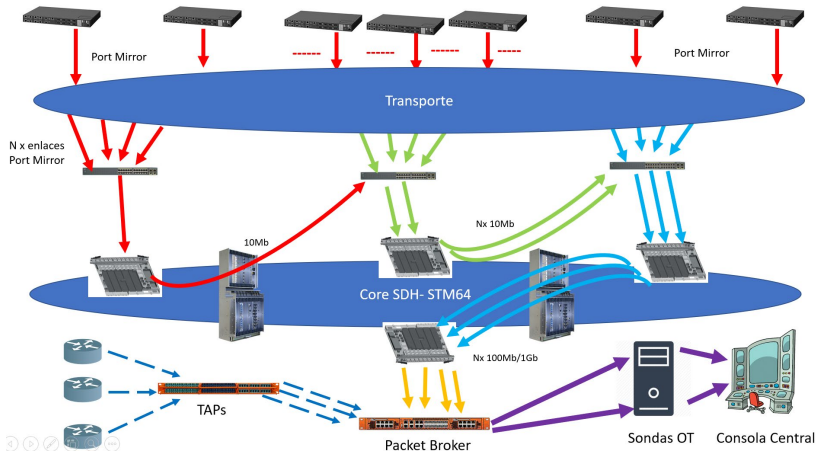
Solución

Una de las grandes ventajas de las tecnologías de Network Packet Brokers de Gigamon es la de poder consolidar tráficos de multitud de puntos de origen diferentes para consolidarlos en un punto central y habilitar así las herramientas de visibilidad y seguridad

En el caso de dispositivos de seguridad OT, vamos a ser capaces de realizar esta tarea de diferentes maneras:

- Cuando no es posible generar la copia del trafico por el equipo de comunicaciones, nuestras soluciones de TAP se encargan de sacar la copia literal del trafico, permitiendo enviarla por la red de transporte al punto central
- Cuando empleamos equipos intermedios para encapsular el trafico y enviarlo por RESPAN al punto central, nuestro packet bróker central puede desencapsular ese trafico y combinarlo con el trafico proveniente del datacenter principal
- Si nos vemos en la necesidad de realizar agregaciones intermedias de trafico para reducir el ancho de banda a transmitir, típicamente por restricciones de capacidad en la red de transporte, nuestros equipos agregadores pueden realizar esa funcion

Esquema



Licencia

Application Filtering
Intelligence
Application metadata
Intelligence
Flow Mapping
Tuneeling

LINK