Como diseñar y mantener una red de control industrial segura

Cumplimiento de la norma IEC 62443 con el uso de la solución SCAB

Autores:

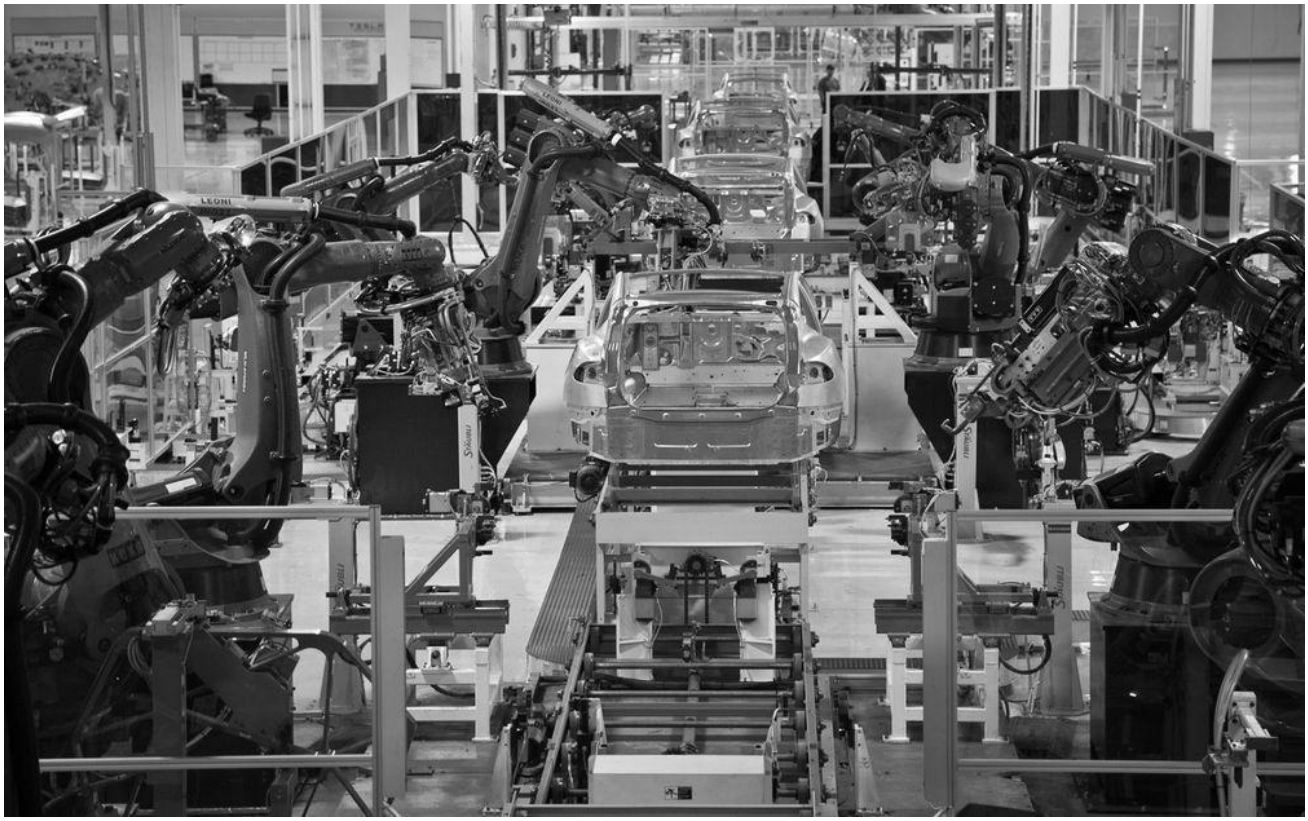
Daniel Trivellato, Ph D – SecurityMatters Product Manager Industrial Line
Roy Murphy, MSC – Senior ICS Security Engineer

16 de Junio de 2015

Traducido por Enrique Martín García
Telvent Global Services

enrique.martingarcia@telvent.com

Contenidos



Introducción

Los operadores de redes de control industrial están sujetos a una constante demanda para incrementar su productividad y disminuir sus costes. Para lograr este objetivo y cumplir las demandas de la dirección, los operadores están migrando hacia el uso de tecnologías de comunicaciones estándar, equipos comerciales regulares (COTS) y están abriendo enlaces entre la red de control y la red de negocio para permitir el uso compartido de información en tiempo real entre los sistemas de planta y los sistemas corporativos con fines analíticos.

A pesar de las claras ventajas para el negocio, este cambio de paradigma ha reducido considerablemente la resiliencia de las redes de control industrial, abriendo la puerta a una nueva clase de amenazas: los ciberataques a los sistemas de control industrial (SCI). Para limitar la exposición de las redes industriales a estas nuevas y actuales amenazas, un grupo de expertos en seguridad de redes y del dominio del automatismo industrial han trabajado para implantar la familia de estándares ANSI/ISA 99, y que ahora se conoce como la norma IEC 62443.

Estos estándares proporcionan un marco de trabajo (Framework) para ayudar a los fabricantes, integradores y operadores de sistemas de control industrial a lidiar con las amenazas surgidas por las iniciativas de "impulso de la productividad" y sus consecuencias en la apertura de este tipo de redes a la corporación y a otros sistemas de terceros, y también a conjurar el espectro de ataques de malware tipo Stuxnet.

Esta nota técnica (White Paper) revisa brevemente la norma IEC 62443, discute sus limitaciones y muestra como SCAB ayuda a superarlas, ayudando así a los operadores industriales a ser conformes a estos estándares y mejorar la seguridad de sus redes de control industrial.

Los estándares IEC 62443

La familia de estándares IEC 62443 proporciona un marco de trabajo flexible diseñado para facilitar la mitigación de las actuales y futuras vulnerabilidades en redes y sistemas de control industrial, a través de la aplicación de los controles de seguridad necesarios y de las mejores prácticas. Los estándares definen distintos requisitos a diferentes niveles técnicos y organizativos para que las organizaciones adquieran el nivel de Ciberseguridad deseado. En la figura inferior se puede ver un resumen de la familia de estándares IEC 62443.

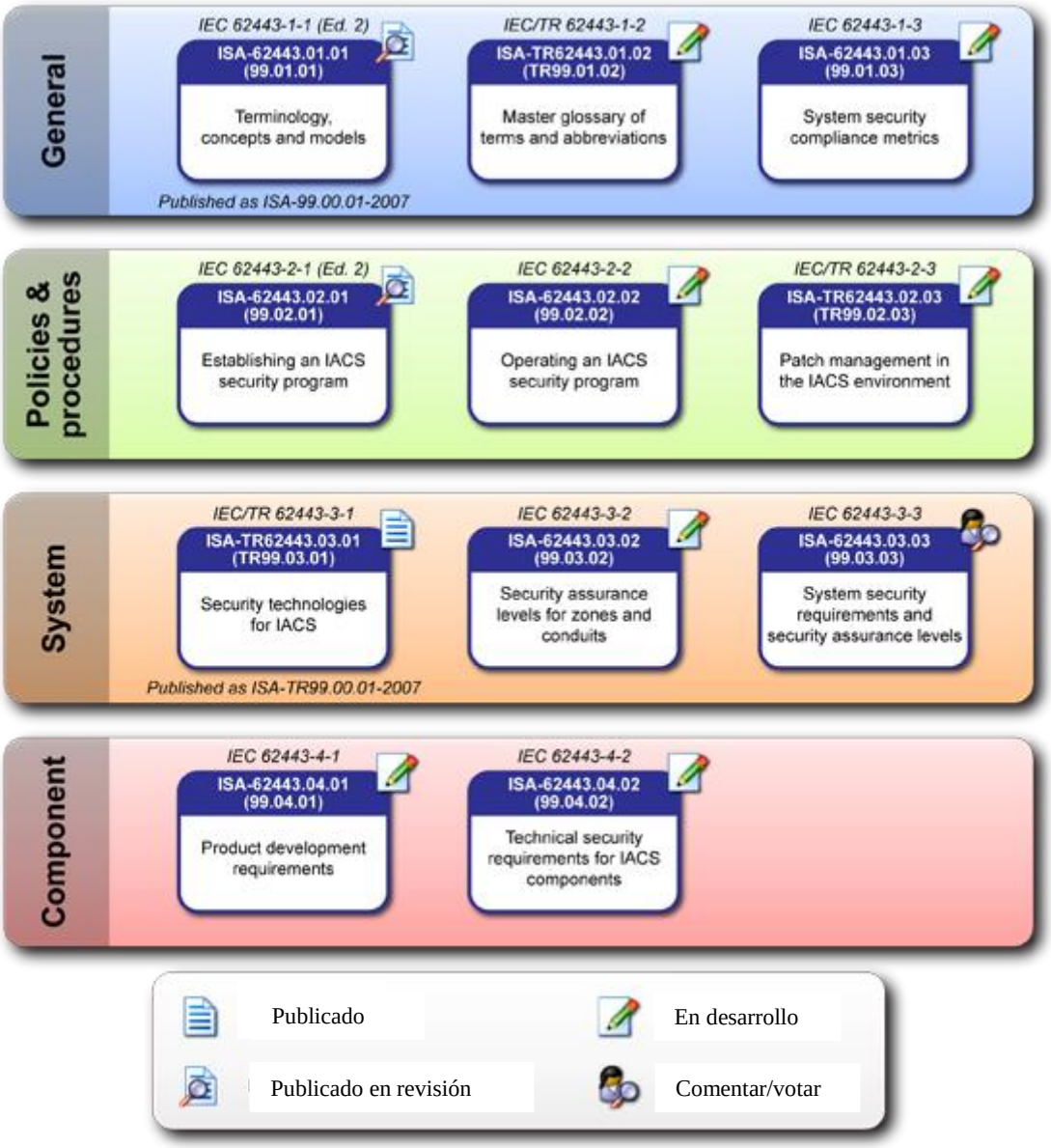


Figura 1 – Resumen de la familia de estándares IEC 62443

Síntesis de la norma y programa de implantación

En este documento técnico nos centramos exclusivamente en las normas técnicas de la familia IEC 62443, que son las dirigidas a la red y sus componentes (los niveles más bajos de la Figura 1, etiquetados como "Sistema" y "Componente"). El siguiente es un breve resumen del contenido de esas normas:

- La norma **IEC 62443-3-1** proporciona una descripción introductoria a todas las tecnologías existentes para la protección de redes industriales y sistemas (por ejemplo, soluciones de red y basadas en host, etc.), sus ventajas y limitaciones.
- La norma **IEC 62443-3-2** describe cómo las organizaciones deben segmentar su red en zonas y *conduits*, agrupando los sistemas que son similares en funcionalidad, propósito y / o ubicación, y realizando un análisis de riesgos y definición de los requisitos de seguridad por cada zona. Un nivel de seguridad deseado (en una escala de 1 a 4) se asigna a cada zona. El objetivo de esta norma es la gestión del riesgo basado en zonas, y esta etapa de la segmentación de la red se debe hacer sólo en papel; la segmentación real de la red se discute en la norma **IEC 62443-4-2**.
- La norma **IEC 62443-3-3** describe los requisitos generales de seguridad del sistema en términos de identificación y autenticación, confidencialidad de los datos y la integridad del sistema, especificando cómo estos requisitos son diferentes para las redes ICS con respecto a las redes de TI. En particular, la norma hace hincapié en el hecho de que el rendimiento y la disponibilidad no deben verse afectados en el intento de dar cabida a estos requisitos.
- La norma **IEC 62443-4-1** define un proceso de desarrollo que tiene como objetivo reducir el número de vulnerabilidades en los sistemas de control industrial. La norma define una serie de técnicas y procesos basados en las mejores prácticas para el diseño seguro.
- La norma **IEC 62443-4-2** define los requisitos técnicos para asegurar los componentes individuales de una red industrial. Estos requisitos se basan en los requisitos de seguridad a nivel de sistema especificados en la norma **IEC 62443-3-3**. Los objetivos de seguridad se centran en la disponibilidad del sistema, protección de plantas, operaciones de la planta, y la respuesta del sistema en tiempo crítico. Por otra parte, la norma analiza la aplicación de las restricciones de flujo de datos para lograr la segmentación de red adecuada. En particular, se trata la partición de aplicación, la función de aislamiento de seguridad, y protección del perímetro.

Basándonos en el marco IEC 62443, podemos identificar cuatro pasos incrementales que los operadores deben seguir - con el apoyo de terceros cualificados - para diseñar y mantener redes industriales más seguras y resilientes.

1. **Recogida de datos:** el primer paso consiste en la recopilación de toda la información necesaria para comprender cómo se construye la red y el proceso opera;
2. **Revisión de la seguridad:** el segundo paso aprovecha la información recogida en el paso 1 para determinar la postura de seguridad actual de la red industrial, determinar su exposición a las ciberamenazas, e identificar contramedidas apropiadas;
3. **Construcción de la solución**: en base a los criticidades y prioridades identificadas en el paso 2, los operadores aplican los cambios necesarios en la red, y se preparan para la aplicación de las contramedidas seleccionadas;
4. **Despliegue da la solución:** por último, las contramedidas seleccionados se desplegarán e integrarán en las operaciones del día a día para mantener la seguridad de la red y los procesos

La Figura 2 ilustra los cuatro pasos, junto con las principales actividades involucradas en cada uno

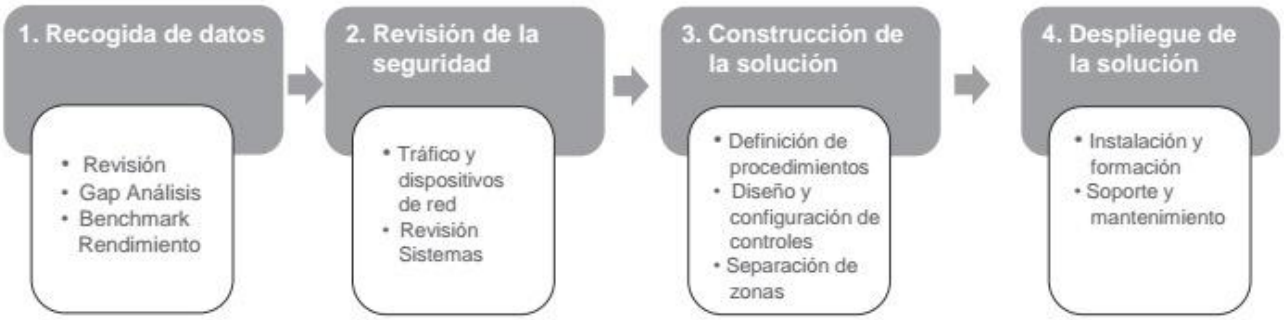


Figura 2 – Cuatro pasos para la implantación del estándar IEC 62443

Limitaciones de los estándares IEC 62443

La seguridad y la capacidad de recuperación de la red industrial resultante de la aplicación de las normas IEC 62443 son estrictamente dependientes de la integridad y exactitud con la que las actividades dentro de los pasos 1 y 2 en la figura 2 se llevan a cabo. De hecho, sólo una recopilación de datos completa y exacta y una evaluación correcta del nivel de seguridad actual, permitirán la selección e implementación exitosa de las contramedidas adecuadas.
Estas actividades, sin embargo, se realizan normalmente de forma manual o con la ayuda de herramientas inadecuadas no diseñadas para ese propósito específico. Como consecuencia, el proceso es largo, propenso a errores, y a menudo incompleto, debido a que es difícil de caracterizar todos los aspectos pertinentes sin el apoyo de un conjunto de herramientas automatizado.
En los próximos párrafos se presenta como el uso de la plataforma de monitorización e inteligencia SCAB puede apoyar a los operadores para llevar a cabo algunas de las actividades de una manera mucho más precisa y completa.

Construcción de una red (más) segura con SCAB

SCAB está diseñado específicamente para proporcionar la visibilidad que falta en las redes y procesos industriales. SCAB escucha, analiza y crea el modelo de comportamiento de la red de forma automática, presentando al operador toda la información necesaria para comprender cómo funciona y está construida la red, e identificar las debilidades o posibles focos de problemas. SCAB hace todo esto de una manera completamente pasiva, para proporcionar la imagen más precisa posible del comportamiento de la red con el mínimo esfuerzo, y sin riesgo de introducción de latencia o afectar el rendimiento de los sistemas y procesos.
SCAB ofrece el soporte ideal en diferentes etapas de la aplicación de las normas IEC 62443. En particular, se materializa en los siguientes puntos:

- Permite una determinación instantánea y precisa de los **flujos de tráfico** y **dispositivos de red activos**;
- Apoya el diseño de la **segmentación de la red en zonas y *conduits***, lo que garantiza que no se produzca la comunicación o información de flujos no deseados
- Y proporciona la mejor protección posible en el día a día de la red. gracias al más avanzado motor de **detección de amenazas** disponibles en la actualidad, y que puede detectar nuevos y aún desconocidos ciberataques tan fácilmente como las amenazas en la operación errónea la red.

En los siguientes puntos describiremos estas funcionalidades del SCAB con mayor detalle.

Flujos de tráfico y descubrimiento de activos

Los operadores pueden construir un inventario preciso de los activos de red y procesos, determinar los flujos de información, los protocolos utilizados y las operaciones realizadas por cada dispositivo concreto de su red mediante la explotación del motor de análisis auto-configurable y la analítica visual avanzada de la plataforma SCAB. El resultado es una imagen instantánea, clara y precisa de la red, lo que facilita la comprensión del operador del proceso subyacente e identifica posibles debilidades y brechas de seguridad, a partir de fuentes como el uso de protocolos y servicios inseguros o el uso excesivo del ancho de banda de la red industrial. Además, toda esta información se captura de manera pasiva usando un puerto de red en *mirroring* sin tener que reconfigurar la red ICS o escanear activamente la red.
La imagen de la red es proporcionada por un conjunto de *widgets* visuales, cada uno de los cuales está idealmente diseñado para resaltar ciertos aspectos del comportamiento de la red. Por ejemplo:

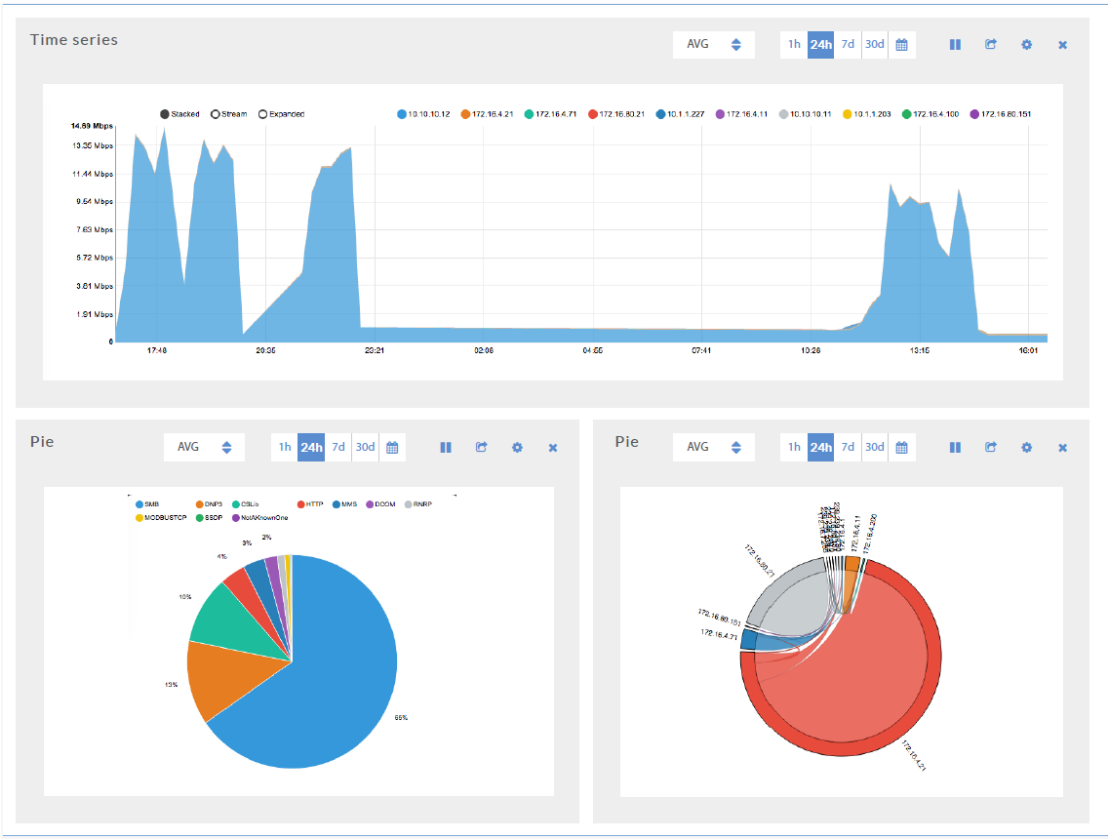


Figura 3 – Algunas de las vistas ofrecidas por la analítica visual avanzada de SCAB

Todos los gráficos y pantallas de análisis son totalmente personalizables y pueden usarse para representar múltiples aspectos de un flujo de comunicación, por ejemplo, el número de bytes intercambiados o mensajes de protocolo. La información mostrada puede filtrarse y filtrarse de manera cruzada con respecto a las diferentes dimensiones. Los gráficos no solamente proporcionan una visión en tiempo real de la red, sino que también pueden ser utilizados para buscar eventos pasados y analizar las comunicaciones de la red en relación a distintos acontecimientos. De hecho, detrás de la plataforma de análisis visual hay un *Data Warehouse* con todas las funciones que permite a los operadores combinar todas sus preferencias de consulta con los datos históricos, dándoles toda la capacidad que necesitan para analizar en profundidad el comportamiento de la red industrial.
Además de la representación gráfica proporcionada por los análisis visuales, SCAB también ofrece una visión detallada de los flujos de información dentro de la red en forma de reglas de firewall, que

son generadas automáticamente por un motor de análisis dedicado. Cada regla indica que dispositivos han iniciado una comunicación, sobre qué puertos, utilizando qué protocolos, y las operaciones / órdenes usadas con esos protocolos. Esta información es clave para identificar la presencia de flujos de información no deseados, servicios inseguros a cargo de los dispositivos de red, u operaciones de procesos no deseadas.

Source	Port	Dest	Port	Protocol	Msg
DCS	*	PLC_1	502	Modbus	Read Multiple Registers Write Multiple Registers
DCS	*	PLC_2	502	Modbus	Read Single Coil
DCS	*	HMI	*	DCOM	SMB_COM_CREATE
…	…	…	…	…	…

Figura 4 – Flujos de tráfico de red, protocolos y comandos identificados por SCAB

La salida de este análisis se puede utilizar para determinar el estado de seguridad de la red, limpiar errores de configuración existentes, y configurar o corregir la configuración de los *Firewalls* para detener determinados flujos de información no deseados. Además, incluye todos los *inputs* necesarios para apoyar la definición de la red de "zonas" y "*conduits*", según lo recomendado por la norma IEC 62443. En otras palabras, es el primer gran paso hacia el diseño e implementación de una red segura.

Segmentación de red y detección de amenazas

Pero SCAB no es sólo una gran plataforma para apoyar las revisiones y evaluaciones de la red, también se puede utilizar para garantizar que el nivel de seguridad deseado siempre se conserva. De hecho, las reglas generadas automáticamente por SCAB pueden hacerse cumplir para garantizar que cada vez que las comunicaciones divergen del comportamiento previsto de la red, el operador sea alertado inmediatamente. Por ejemplo, SCAB alertará en tiempo real en caso de que un nuevo sistema, inédito inicie la comunicación en la red, o utilice un protocolo o servicio no deseado (ver figura 5). En otras palabras, SCAB reportará cualquier violación de la segmentación de la red determinada en la etapa de "Construcción de la solución" (etapa 3 de la aplicación marco IEC 62443).

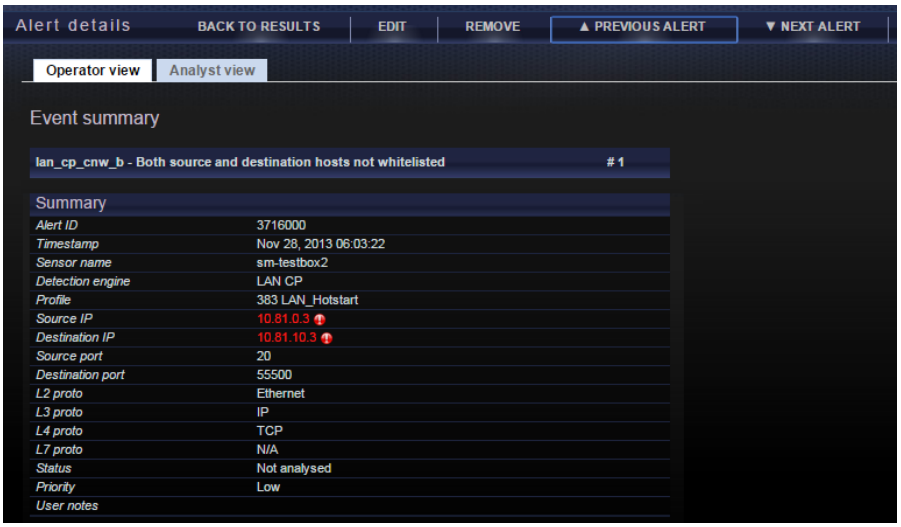


Figura 5 - Alerta generada por SCAB cuando dos sitemas desconocidos se comunican en la red

A raíz de este control de grano fino sobre la información, SCAB utiliza el motor de detección más avanzado para analizar las comunicaciones a través de protocolos industriales. SCAB utiliza un modo de aprendizaje para generar automáticamente un modelo de mensajes que se utiliza activamente por la red de control. Usando inspección profunda de comportamiento de protocolo, se genera un modelo basado en árbol y se almacena para permitir el análisis automático en tiempo real de las comunicaciones del sistema de control. La Figura 6 a continuación es un ejemplo de un modelo de árbol que fue auto-generado por la plataforma SCAB durante el seguimiento de algunas comunicaciones Modbus/TCP.

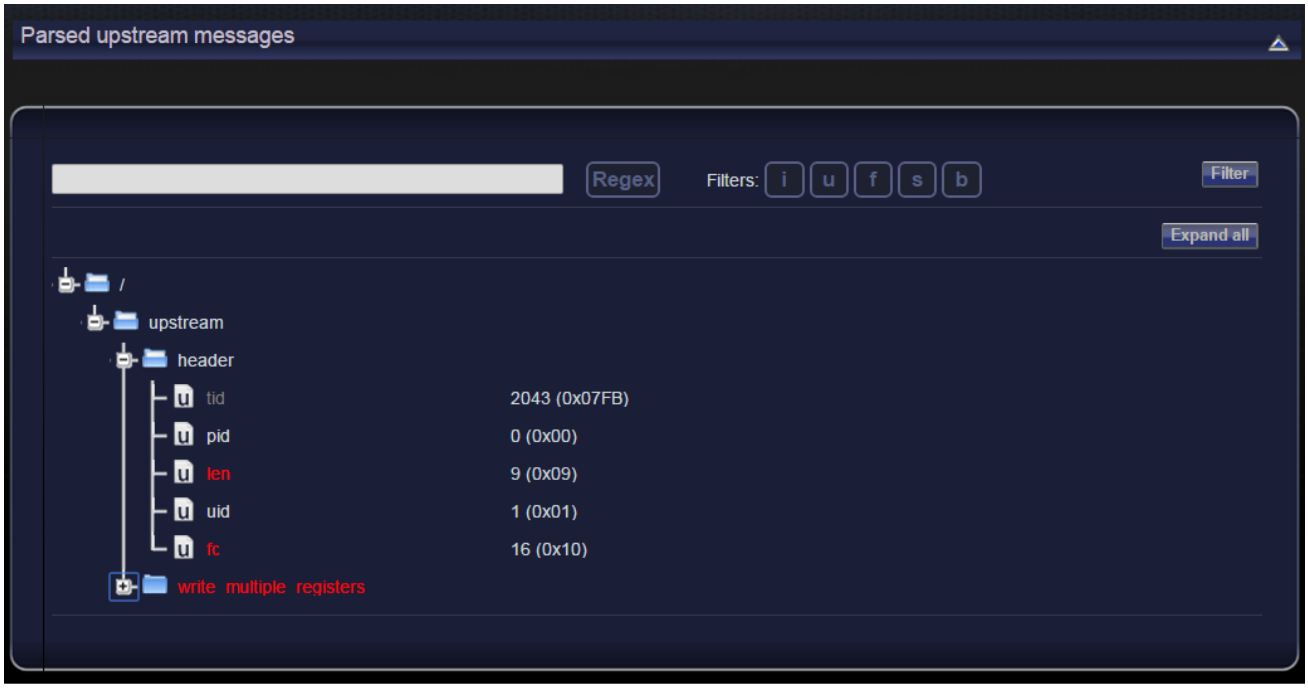


Figura 6 – SCAB informa del uso de operaciones no autorizadas y valores sospechosos

El resultado es que SCAB es capaz de analizar todos los campos individuales y los valores contenidos en un mensaje de protocolo industrial, para asegurarse de que el mensaje no sólo es compatible con las especificaciones del protocolo, sino también con las operaciones previstas y con los rangos de valores que se utilizan específicamente en la red monitorizada. Tan pronto como un intruso externo o algún usuario interno descontento intenta explotar una vulnerabilidad en los dispositivos de red, SCAB lo detectará y alertará. Esto va más allá de las capacidades de otros sistemas de monitorización de red existentes, que paran su análisis en el nivel de "comando" y protocolo. Como resultado, SCAB ofrece protección frente a un conjunto más amplio de ciberamenazas, desde los más simples, hasta los más avanzados.

Conclusiones

SCAB, es la plataforma ideal para ganar y mantener toda la visibilidad necesaria de las actividades de las redes industriales, en cualquier momento. Permite a los operadores lograr el aumento de la productividad requerida por la dirección sin perder de vista la seguridad de la red, como se propone en los estándares IEC 62443.
SCAB aporta un valor que va más allá de las soluciones de Ciberseguridad tradicionales. Es capaz de identificar y alertar sobre problemas de red y proceso que pueden tener los mismos efectos devastadores de un ciberataque. En definitiva, es la plataforma más completa y potente para la monitorización de redes y sistemas de control industrial.

Acerca de SecurityMatters

SecurityMatters es una compañía internacional con negocio en todos los sectores operadores de Infraestructuras Críticas y sistemas de automatización industrial por todo el mundo. Su plataforma de monitorización e inteligencia SilentDefense ICS ha sido desplegada durante años en distintas localizaciones de clientes, proporcionando un alto valor añadido en sus operaciones diarias y en la protección de sus redes de control ante las más avanzadas ciberamenazas.

Acerca de Telvent Global Services

Telvent Global Services (Telvent) es una compañía de servicios IT/OT con alta especialización en la gestión de infraestructuras críticas de tecnologías de la información y operacional, que ofrece soluciones integrales de consultoría, integración y outsourcing a lo largo de todo su ciclo de vida. Tratamos de implementar nuestra misión de simplificar la complejidad tecnológica con una oferta de servicios que da respuesta a las necesidades de gestión y operación de infraestructuras y sistemas IT y OT para acompañar la evolución del negocio de nuestros clientes.

Referencias

[1] ISA 99 - IEC 62443: Industrial Automation and Control Systems Security - https://www.isa.org/isa99/