BUENAS PRÁCTICAS EN LA IMPLANTACIÓN DE SIEM EN INFRAESTRUCTURAS CRÍTICAS

ROBERTO HIDALGO CISNEROS

Gerente de Sistemas y Ciberseguridad
CIC CONSULTING INFORMÁTICO
Licenciado en Ciencias Físicas y máster en Gestión de Datacenters por la Universidad de Cantabria

En los desarrollos de los Planes de protección específicos de operador de infraestructuras críticas se incluye, en muchas ocasiones, la implantación de controles basados en sistemas de monitorización y/o prevención de ciberataques dentro de las capas más profundas de la arquitectura de seguridad.
Dentro de esta categoría de sistemas de monitorización podríamos incluir un conjunto amplio de dispositivos y soluciones, tanto pasivas como activas, entre las que podemos nombrar algunas: firewalls, IPS, DPI, endpoints , SIEM, etc.
Dado el gran impacto que una mala ejecución del despliegue de este tipo de sistema pudiera llegar a ocasionar en la operación de la planta es necesario tomar una serie de medidas de prevención para minimizar el riesgo.
Una de las principales medidas a tomar a la hora de abordar este tipo de proyectos es la de contar con un marco de trabajo que reduzca al mínimo el riesgo.
En este artículo, expondremos una serie de recomendaciones o conjunto de buenas prácticas a la hora de desplegar uno de estos controles de ciberseguridad, tomando como ejemplo un sistema SIEM.

SITUACIÓN

En los últimos años el número de ataques cibernéticos contra las infraestructuras críticas ha crecido de manera muy importante en cantidad y en daños provocados.

Según fuentes del Ministerio del Interior, en España se registraron más de 105.000 ciberataques en 2016 con un aumento del 50% frente al año anterior [1].

De éstos, 479 tenían como objetivo las infraestructuras críticas, estimándose la cifra real mucho mayor derivado del bajo despliegue de sondas que recojan tráfico, en torno al 10% del tráfico dirigido hacia los operadores críticos [2] y teniendo en cuenta, además, que España es el quinto país por número de Sistemas de Control Industrial (ICS, por sus siglas en inglés) conectados a Internet [3].

No obstante, el número de ciberataques que hayan podido afectar a las capas más profundas de la arquitectura de seguridad en los entornos industriales no se conocen oficialmente.

Para detectar y prevenir estos tipos de amenazas los operadores de infraestructuras críticas están desplegando, dentro de sus Planes de Protección Específicos (PPE), una serie de controles en sus infraestructuras OT.

Muchos de estos controles están relacionados con la seguridad de la red y abarcan un gran número de tecnologías y dispositivos provenientes en su mayoría de la seguridad perimetral IT, como pueden ser *firewalls*, *Intrusion Prevention Systems* (IPS), *Web Applications Firewalls* (WAF), *Deep Packet Inspection* (DPI), *Security information and event management* (SIEM), etc. (Figura 1).

La mayoría de estos dispositivos cuentan con funcionalidades de monitorización y alerta, llamémoslas "pasivas", pero también pueden contar con un conjunto de funcionalidades "activas" que son capaces de actuar en función de su programación, por lo que su inclusión dentro de las redes OT conlleva una serie de riesgos que han de ser valorados a la hora de abordar su despliegue (Figura 2).

DESPLIEGUE DE UN SIEM

A lo largo de este artículo utilizaremos como ejemplo representativo el despliegue de un tipo de sistema de monitorización y alerta ante ataques de ciberseguridad conocido como SIEM

BEST PRACTICES ON THE IMPLEMENTATION OF SIEM IN CRITICAL INFRASTRUCTURES

In the development of the specific protection plans of operator of critical infrastructures in many occasions it is included the implementation of controls based on monitoring and/or prevention systems of cyber-attacks inside the deepest layers of the security architecture.
Within this category of monitoring systems, we could include a wide group of devices and solutions, active and passive, such as Firewalls, IPs, DPI, endpoints, SIEMS... etc.
Given the great impact that an incorrect execution of the development of this kind of system could influence in the plant operation, it is necessary to take a series of prevention measure to minimize the risk.
One of the main measures is to create a framework that reduces the risk to the minimum.
In this article, we will expose a series of recommendations or best practices regarding the development of one of these cyber security controls, taking as an example a SIEM (Security Information and Event Management) system.

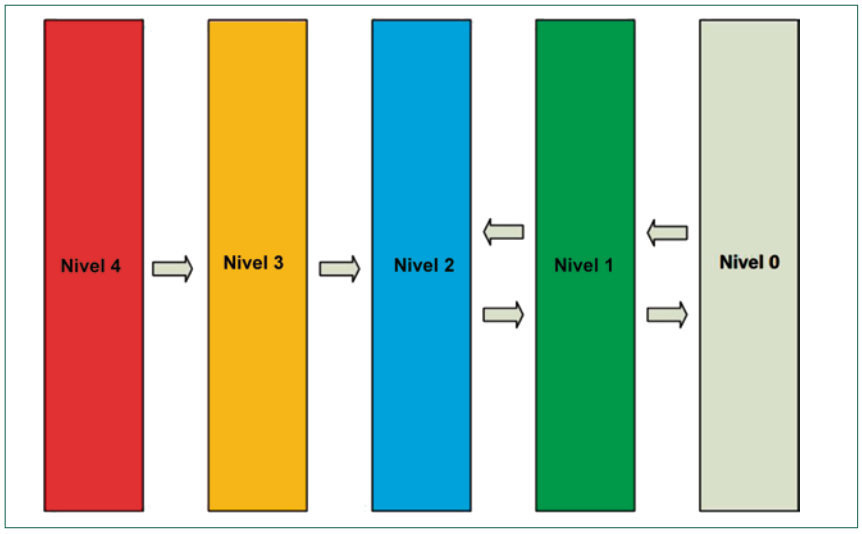

Figura 1. Arquitectura de seguridad de la norma RG 5.71.

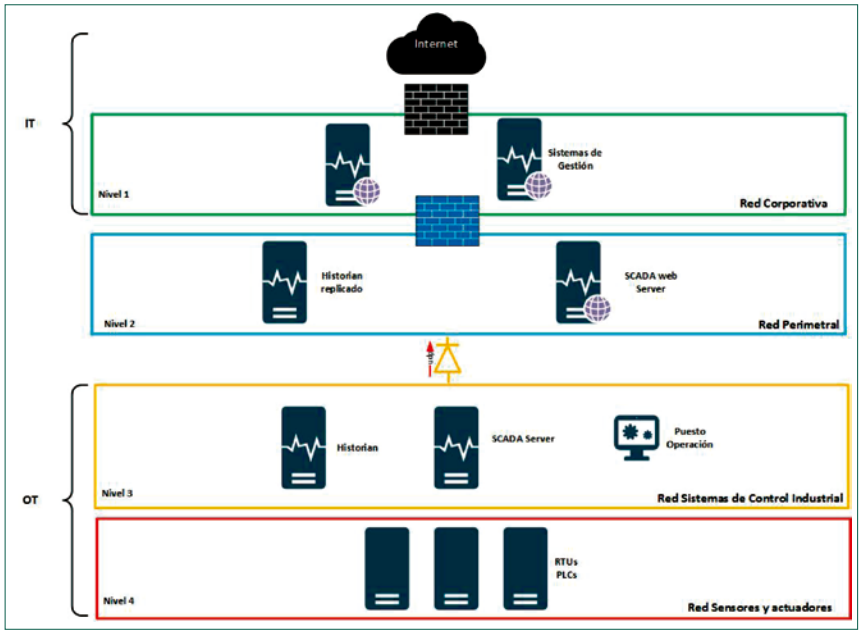

Figura 2. Diagrama conceptual de arquitectura de sistemas según RG 5.71.

(*Security Information and Event Management*) dentro del nivel 3 de una red de control industrial genérica.

De forma genérica un SIEM [4] es un conjunto de *hardware* y *software* que provee de análisis en tiempo real de eventos producidos por el *hardware* y las aplicaciones, así como detección de patrones de ataque dentro del tráfico de red.

Entre sus funcionalidades básicas destacan la agregación de *logs* y eventos, la correlación de eventos, el envío de alertas de seguridad, la generación de informes y la retención a largo plazo para permitir análisis forense.

En los últimos años han ido ampliando sus capacidades mediante la inclusión de otras funcionalidades como la inspección de tráfico en busca de ataques (NIDS [5]), detección de intrusiones en los servidores (HIDS [6]), descubrimiento de nuevos activos en la red, así como capacidad de escaneo de vulnerabilidades mediante la ejecución de test de intrusión.

Sin embargo, el despliegue y puesta en marcha de este tipo de sistemas en las redes de planta, así como la utilización de estas funcionalidades de tipo activo (HIDS, test de vulnerabilidades, descubrimiento de activos, ...) pueden producir errores, degradaciones o incluso pérdidas de servicio que pueden suponer un impacto significativo en la operación.

BUENAS PRÁCTICAS EN LOS DESPLIEGUES

Por ello, a la hora de abordar un proyecto de despliegue de este tipo de sistemas se han de tomar una serie de precauciones básicas y seguir unas buenas prácticas [7] que minimicen el riesgo de fallo y faciliten la recuperación frente a los mismos.

Desde nuestro punto de vista, el enfoque general de un proyecto de implantación de un sistema SIEM ha de ser similar a la puesta en marcha de un sistema de control industrial (sistemas SCADA, sistemas de control distribuido, automatizaciones industriales, ...etc) por lo que recomendamos disponer de una metodología o forma de trabajo que siga las siguientes buenas prácticas generales [8]:

1. **Identificar de manera temprana los riesgos de seguridad** que pudieran afectar al control de procesos derivados de la ejecución de proyectos planificados y en marcha. Se debería disponer de un inventario de proyectos que afecten a la seguridad de los procesos de control.
   Entre los tipos de proyectos que se deberían identificar están: los relacionados con cambios en los *firewalls* [9], actualizaciones de sistemas de control, implantación de nuevos sistemas de control y monitorización como IPS [10] o SIEM, interconexión entre la red de control de procesos (OT) y la red de gestión (IT), conexiones con terceros, actualizaciones de *firmware*, etc.
2. **Nombrar un responsable de seguridad** con responsabilidad sobre todos los aspectos de seguridad a lo largo del ciclo de vida de los proyectos. De ser posible, se debería contar con una figura que supervisara los aspectos relacionados con la ciberseguridad en todos los proyectos de implantación y/o modificación de sistemas de control industrial.
3. **Incluir requerimientos de seguridad en los contratos con los proveedores** de bienes y servicios, siendo una buena práctica el hacer referencia al cumplimiento de políticas o normas establecidas internamente o estándares de la industria. De especial importancia en el despliegue

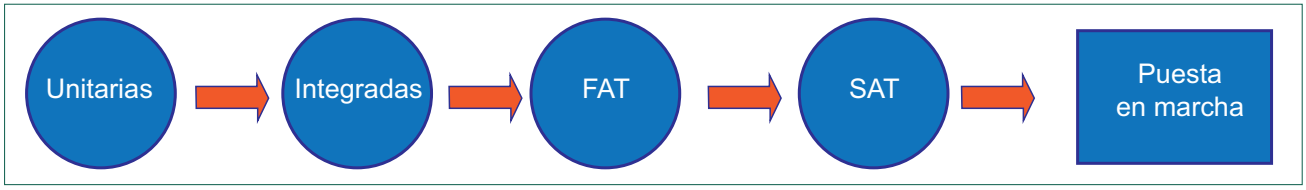

Figura 3. Itinerario de pruebas recomendado.

de proyectos es el incluir revisiones de seguridad en el diseño, en el código para el caso de los proyectos de *software* y pruebas específicas de seguridad incluidas dentro de las baterías de pruebas definidas.

4. **Incluir requisitos de seguridad en las especificaciones de diseño** de los sistemas desde sus etapas más tempranas. Estos requisitos de seguridad deben de ser abordados desde el punto de vista de riesgo para el negocio y no deben ser considerados de manera diferente a cualquier otro tipo de requerimiento: funcional, de rendimiento, … etc
5. **Revisar la seguridad a lo largo de todo el ciclo de vida** de los proyectos de implantación, especialmente en las etapas tempranas de análisis y diseño del sistema en las que es recomendable revisar que lo diseñado cumple las especificaciones, requerimientos y normativa de seguridad definidas.
6. **Pruebas del sistema incluidas a lo largo de todo el ciclo de vida del proyecto**, incluyendo pruebas unitarias e integradas, así como pruebas de aceptación fabrica (FAT) y en planta (SAT) (Figura 3).
   Dado que existe un riesgo potencial, materializado en numerosas ocasiones, en la ejecución de pruebas de seguridad en los sistemas se recomienda hacer la mayor cantidad de pruebas posible, planificadas desde el principio, antes de la puesta en marcha del sistema.
7. **Disponer de un plan de puesta en marcha** que contemple todos los aspectos de conexionado del nuevo sistema, procedimientos de operación, recuperación ante fallos y continuidad de negocio.

Alineado con estas buenas prácticas generales para una buena implantación de proyectos de seguridad en sistemas de control industrial, la implantación de SIEM tiene algunas particularidades a tener en cuenta.

1. Dado que trabajamos con información sensible de la red de procesos (IPs, configuraciones, protocolos, etc.), se han de establecer los mecanismos de seguridad y control de los entornos y documentación del proyecto tanto por parte del operador de las infraestructuras, como de las contratas.
2. Por su propia naturaleza y aislamiento, el número de incidentes y/o alertas de ciberseguridad en los niveles OT debería ser tendente a cero, por lo que es muy importante realizar pruebas de simulación de ataques (fuerza bruta, MitD, escaneo de puertos, ataques tipo *ramsonware*, etc.) durante las pruebas FAT a fin de comprobar el correcto funcionamiento del sensor. Estas pruebas pueden ser repetidas de forma periódica o en caso de actualización del sistema mediante la utilización de sistemas de laboratorio.
   La puesta en modo escucha de estos sistemas en planta conlleva una serie de actuaciones y modificaciones en los equipos de red existentes (*switches, routers*, cortafuegos, etc.) y servidores cuyo riesgo ha de ser gestionado desde las etapas iniciales del proyecto. En concreto, la puesta en marcha de estos sensores implica cambios en los equipos para que reenvíen sus eventos (mediante *syslog*) hacia el SIEM [11], así como modificaciones en los *switches* de red para que manden una copia de tráfico (*port mirror*) hacia el NIDS.
   Estas actuaciones han de ser planificadas de acuerdo al riesgo operacional y se recomienda siempre realizar pruebas previas en una maqueta, o sobre los sistemas pasivos en caso de no ser posible.
   En caso de que el riesgo operacional sea muy elevado podría llegar a ser necesario realizar estos cambios con la planta en parada.
3. En la misma línea que el punto anterior, podemos incluir aquellas modificaciones de seguridad avanzada que pudiera ser necesario incluir en el equipamiento de red para la detección de ciertos tipos de ataques como pueden ser MitD (tipo *Man in the Middle* para ARP *spoofing* y DHCP *spoofing*).
4. Como regla general, aquellas funcionalidades activas en las que el SIEM envía algo hacia la planta deberían estar prohibidas y deshabilitadas técnicamente salvo utilización muy controlada. Dentro de

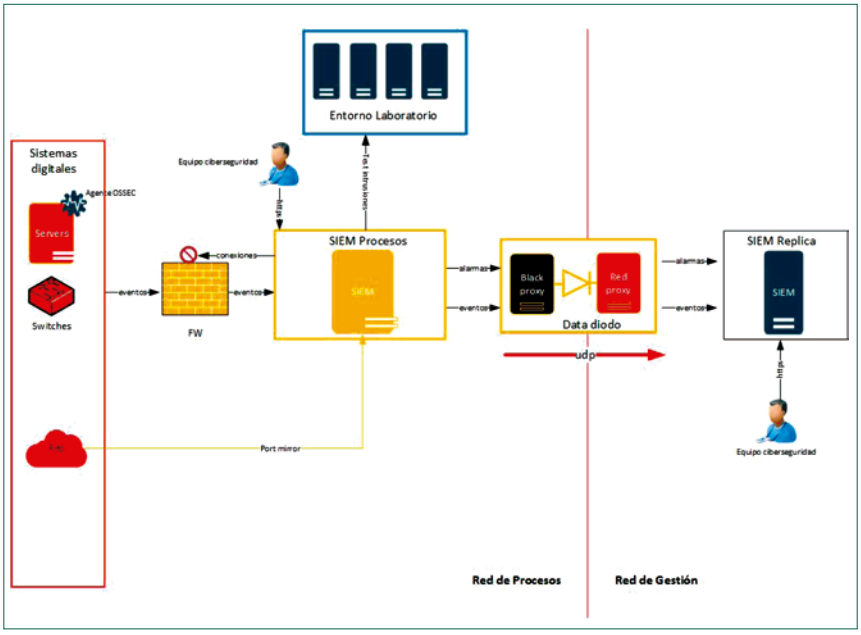

Figura 4. Diagrama conceptual de arquitectura SIEM en una red OT.

estas funcionalidades estarían los escaneos de vulnerabilidades y los descubrimientos de nuevos elementos (*assets*).

Estas funcionalidades, especialmente los test de vulnerabilidades, deberían ser utilizadas solamente en redes aisladas a efectos de ejecución de test sobre sistemas replica o copia de los de producción (Figura 4).

Abundando en esta idea, se propone como buena práctica el disponer de un entorno de laboratorio en el que se pudiera probar las vulnerabilidades de nuevos sistemas a implantar mediante la ejecución de este tipo de test. Un posible ejemplo, aprovechando las posibilidades que nos brinda la virtualización de sistema, pudiera ser el testeo de los servidores que alojan un sistema SCADA.

5. Una vez puesto en modo escucha es conveniente dejar que el sistema reciba eventos y tráfico durante un tiempo a fin de tener información suficiente para afinar el sistema en cuanto a niveles de alerta, reglas de correlación, eliminar "ruido" y falsos positivos.
6. Por último, es recomendable además contar con unos procedimientos de operación que describan los trabajos de operación, *backup*, recuperación ante desastres y actualización *off-line* (sin conexión a Internet) del sistema y de sus archivos de "firmas".
7. Igual de importante es contar con un procedimiento de actuación ante incidentes que contemple los aspectos de identificación, mitigación, investigación y análisis forense para reaccionar de manera ágil y para posteriores posibles reclamaciones judiciales.

CONCLUSIONES

La gestión de la seguridad en el desarrollo de proyectos que pueda afectar a los sistemas de control industrial ha de ser contemplado de manera integral con el resto de requisitos y de acuerdo a una metodología probada y basada en estándares y/o buenas prácticas de la industria.

Esto es también válido para el despliegue de aquellos sistemas de monitorización y prevención de ataques de ciberseguridad, especialmente cuando se despliegan en las redes de proceso por el impacto que una mala implementación puede causar en los sistemas digitales críticos [12].■

REFERENCIAS

[1]. Diario.es. [Online]. [cited 2017 Marzo. Available from: http://www.eldiario.es/politica/Interior-constata-ciberataques-veces_0_622238227.html.

[2]. Centro de Ciberseguridad Industrial. [Online]. [cited 2017 Marzo. Available from: http://www.elconfidencial.com/tecnologia/2017-03-20/ciberseguridad-industria-espanola-infraestructuras-criticas_1350398/.

[3]. Shodan. Buscador de dispositivos conectados a Internet. [Online]. [cited 2017 Marzo. Available from: https://www.shodan.io/report/btZPXVti.

[4]. Garnet. Glosario. [Online]. [cited 2017 Marzo. Available from: http://www.gartner.com/it-glossary/security-information-and-event-management-siem/.

[5]. Wikipedia. [Online]. [cited 2017 Marzo. Available from: https://es.wikipedia.org/wiki/NIDS.

[6]. Wikipedia. [Online].; 2017 [cited Marzo. Available from: https://es.wikipedia.org/wiki/Host-based_intrusion_detection_system.

[7]. Security, U.S. Department of Homeland. CCN-CERT. [Online]. [cited 2017 Marzo. Available from: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf.

[8]. CPNI, CCN. CNPIC. [Online]. [cited 2017 Marzo. Available from: http://www.cnpic.es/Biblioteca/GUIAS_CCN/480G-SCADA-Afrontar_proyectos-ene10.pdf.

[9]. CPNI. [Online]. [cited 2017 Marzo. Available from: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/2005022-gpg_scada_firewall.pdf.

[10]. Scarfone K, Mell P. NIST. [Online]. [cited 2017 Marzo. Available from: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf.

[11]. Bartock M, Cichonski J, Souppaya M, Smith M, Witte G, Scarfone K. NIST. [Online]. [cited 2017 Marzo. Available from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.

[12]. U.S. NUCLEAR REGULATORY COMMISSION. [Online]. [cited 2017 Marzo. Available from: https://www.nrc.gov/docs/ML0903/ML090340159.pdf.