CENTRO DE OPERACIONES DE SEGURIDAD DE BIOCUBAFARMA

4 OCTUBRE 2020

Ing. Yelenys Roig Mendez

eti Tecnologías de la Información BioCubaFarma

Resumen

En la actualidad se ha experimentado un incremento considerable de ataques cibernéticos por lo que la ciberseguridad se ha convertido en una línea estratégica para muchas empresas. El desarrollo de las Tecnologías de la Información (TI) en nuestros días ha llevado a crear soluciones que permitan minimizar y mitigar los riesgos de seguridad que puede presentar una empresa.

Pero no solo podemos centrarnos en implementar tecnologías y soluciones con el fin de mitigar los riesgos y amenazas, tenemos que pensar en contar con una plataforma que brinde información acerca de lo que está ocurriendo en la infraestructura tecnológica. En correspondencia con la envergadura de las empresas u organizaciones se puede pensar en el diseño e implementación de un Centro de Operaciones de Seguridad (COS) que permita prevenir, detectar, analizar y reportar incidentes de seguridad que pongan en riesgo los sistemas, servicios y el eslabón más importante, la información, ante actividades inusuales y maliciosas.

En el presente artículo se abordan temas relacionados a la necesidad de contar con un COS como solución viable para centralizar la gestión de incidentes de seguridad y se definirán además las principales funciones y procesos necesarios, así como las tecnologías empleadas como fase inicial en la implementación de un COS para el Grupo Empresarial de la Industria Biotecnológica y Farmacéutica (BioCubaFarma).

Palabras Claves: ciberseguridad, incidentes.

Introducción

Los COS han alcanzado en nuestros días un lugar cimero cuando hablamos de supervisión de la seguridad de los sistemas, servicios y plataformas que conforman una infraestructura tecnológica. Entre sus principales beneficios se encuentran la centralización de incidentes de seguridad, el empleo de soluciones que lleven a cabo un monitoreo 24/7 de la información que circula por nuestras redes, lo que permite alertar ante la ocurrencia de actividad maliciosa o inusual en la red y la garantía de mantener una supervisión proactiva y reactiva de la seguridad.

El objetivo de este trabajo se basa principalmente en la concepción de un COS a través de la definición de las principales funciones y procesos necesarios para su implementación, así como las herramientas que se han empleado para llevar a cabo su despliegue dentro de la red del Grupo Empresarial BioCubaFarma.

Componentes del COS

Para concebir un COS es necesario conocer cuáles son los componentes básicos para su materialización. Debe contar en primer lugar con Procesos que definan el flujo de trabajo y procedimientos, Tecnologías a través del empleo de soluciones de seguridad y de Personas para la colaboración y comunicación entre los diferentes componentes.

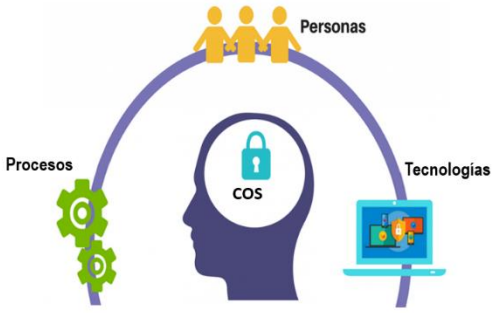

Figura 1 Componentes del COS

Procesos

Definen la clasificación de incidentes y los procesos de investigación se estandarizan las acciones del COS. Con la creación de un procedimiento de gestión de incidente se definen las responsabilidades y acciones de los miembros del equipo, normando los pasos a seguir desde la creación de una alerta en el nivel inicial hasta escalar el incidente en caso de ser necesario. La definición de los procedimientos de trabajo permitirá asignar eficientemente los recursos.

Personas

El COS debe contar con una estructura organizativa que defina las funciones y roles principales a desempeñar por el equipo. Esta estructura va a estar conformada por analistas de seguridad, investigadores de incidentes, expertos en seguridad y el responsable del COS. En el caso de los analistas se pueden definir por niveles, donde los analistas del nivel 1 (L1) van a realizar un monitoreo continuo de alertas, clasificar los incidentes, notificar a las instancias involucradas y de ser necesario ejecutar el proceso de escalado hacia el nivel (L2). La principal función de los analistas L2 se centra en el análisis profundo de incidentes de seguridad para la correlación de datos proveniente de diferentes fuentes, determinar si un sistema ha sido impactado, proponer posibles soluciones y proveer soporte basado en nuevos métodos de análisis para la detección de

amenazas. De ser necesario contará con un 3er nivel (L3) conformado por expertos con profundo dominio en redes, punto final, inteligencia de amenazas, análisis forense e ingeniería inversa de malware.

Tecnologías

Para implementar un COS exitoso es necesario contar con tecnologías capaces de colectar, detectar, analizar y gestionar los datos. Un sistema de monitoreo de seguridad efectivo incorpora la obtención de datos de diferentes fuentes como: el monitoreo continuo del punto final (PCs, laptop, dispositivos móviles, etc.) así como eventos y logs generados por los servidores y dispositivos que conforman la infraestructura de red. Con la información obtenida el COS puede pasar de ser un simple sistema de monitoreo de seguridad a una herramienta investigativa dado que permite revisar las actividades sospechosas asociadas a un incidente y además permitirá gestionar la respuesta a dicho incidente o brecha de seguridad. Otro aspecto importante es la compatibilidad e integración de tecnologías como los Sistemas para la Gestión de Eventos e Información de Seguridad (SIEM, por sus siglas en inglés) y las soluciones para la gestión de incidentes.

FUNCIONES DEL COS

En el proceso de concepción de un COS es necesario definir cuáles son las funciones básicas para su implementación. Se definieron 6 funciones principales mostradas en la siguiente figura.

Figura 2 Funciones básicas del COS

Monitorización en tiempo real

Consiste en el monitoreo continuo y sistemático que permite la generación de eventos y alertar ante la ocurrencia de incidentes que comprometan la seguridad. Esta función se

basa principalmente en el empleo de soluciones SIEM, herramientas de detección de intrusos (IDS, por sus siglas en inglés) y soluciones de detección y respuesta en el usuario final (EDR, por sus siglas en inglés).

Gestión de vulnerabilidades

Como fase preventiva para disminuir posibles ataques de seguridad es importante concebir un sistema para la Gestión de Vulnerabilidades que garantice la detección oportuna de amenazas en los sistemas y servicios, y así una vez identificadas se podrá trabajar en su mitigación.

Gestión de Incidentes

Ante la detección de un incidente de seguridad se hace necesario contar con un sistema que permita darle seguimiento pasando por las etapas de registro, análisis, clasificación, reporte y por último la respuesta una vez culminado todo el proceso investigativo, donde se identifique el medio, las afectaciones, las causas y condiciones que propiciaron su ocurrencia.

Análisis de Trazas

Las trazas de los sistemas y servicios representan una fuente importante para la detección de incidentes de seguridad y para el análisis forense durante el proceso de investigación de un incidente. Para concebir una infraestructura consolidada de trazas es preciso contar con un mecanismo que permita centralizar las trazas y un sistema que facilite su visualización y análisis.

Análisis de Tráfico

Tanto para la investigación de un incidente de seguridad como la detección de amenazas se hace necesario contar con información del tráfico real que circula por la red. Es importante contar con herramientas que permitan examinar paquetes, protocolos y tramas de red.

Inteligencia de Amenazas

Un COS maduro tiene que ser capaz de desarrollar capacidades para obtener y aprovechar inteligencia de amenazas de incidentes pasados y desde fuentes de información compartidas, como pueden ser de proveedores de inteligencia de amenazas especializados, los socios de la industria, organizaciones que comparten información y/o proveedores de las tecnologías de monitoreo de seguridad. Las capacidades de estos sistemas para operar inteligencia de amenazas utilizan la detección de patrones en el usuario final, datos de red y logs, así como la asociación de anomalías de alertas anteriores, incidentes o ataques mejorando las capacidades para detectar sistemas comprometidos o la detección previa de brechas de seguridad.

TECNOLOGÍAS EMPLEADAS EN LA IMPLEMENTACIÓN DEL COS

Para la implementación del Centro de Operaciones de Seguridad para BioCubaFarma se concibieron 3 etapas que definen las pautas para su creación. La definición por etapa permite llevar un mejor control de las actividades en ejecución y definir las principales prioridades hasta llegar al proceso de culminación.

La selección de las tecnologías empleadas en el despliegue del COS se basa principalmente en el empleo de soluciones, que como mínimo, garanticen las funciones básicas anteriormente definidas. A continuación, se describen las principales herramientas empleadas.

OSSIM

Como SIEM es empleada la Plataforma para la Gestión de Información de Seguridad Open Source (OSSIM, por sus siglas en inglés). Solución gratuita brindada por la compañía Alienvault, la cual se encuentra posicionada en el cuadrante mágico de Gartner ubicándose entre los mejores sistemas SIEM otorgados por esta compañía.

OSSIM es una suite de soluciones de seguridad integradas en una plataforma única. Entre las herramientas principales que posee se encuentra el Sistema de Detección de Intrusos de Red Suricata que permite escuchar el tráfico de red y basado en reglas previamente definidas permite la generación de eventos de seguridad. Existe una comunidad que se encarga de actualizar las reglas y publicarlas para su descarga. Es importante resaltar que existe también un conjunto de reglas brindadas por la comunidad que son pagadas.

Otro importante sistema integrado a esta plataforma es el OSSEC, Sistema de Detección de Intrusos de Host que a través de su despliegue en los servidores que conforman la infraestructura tecnológica podemos recopilar información ante cambios de integridad de ficheros y directorios, detección de rootkit y generación de eventos basado en las trazas de los servicios desplegados.

Integra a su vez la herramienta OpenVas para la detección de vulnerabilidades permitiendo la posibilidad de programar los escaneos según su frecuencia e intensidad.

Posee a su vez un módulo destinado para el levantamiento de activos de la red, permitiendo mantener un control de los medios conectado y definir su prioridad basado en la importancia que representa el activo.

Es importante señalar que entre las bondades de la Plataforma OSSIM se encuentra la posibilidad de crear Directivas de Correlación que unidas a las que posee por defecto nos permite generar alertas de seguridad ante la ocurrencia de incidentes basados en comportamientos anómalos.

La arquitectura de esta plataforma se basa principalmente en el despliegue de sensores OSSIM en puntos estratégicos para la recopilación de información y su posterior envío hacia el servidor Principal donde se centralizaría toda la información.

Splunk

El Splunk es una herramienta que permite la recolección centralizada de trazas. Entre las principales características que posee se encuentra la posibilidad de recoger información de diferentes fuentes de datos, en diferentes formatos y después de un proceso de indexación son visualizadas a través de una interfaz web para su análisis.

Posee un módulo para la generación de reportes y creación de *Dashboard* permitiendo visualizar información que pueda ser relevante tanto para la identificación de violaciones de las políticas de seguridad establecidas, la detección de incidentes de seguridad o la visualización de información de datos estadísticos.

Presenta gran flexibilidad en la búsqueda de determinada información de las trazas permitiendo realizar búsquedas por caracteres, cadenas de *string* y permite la extracción de campos específicos dentro de la traza a través de la definición de expresiones regulares.

Conclusiones

Contar con un Centro de Operaciones de Seguridad puede ser una alternativa fiable para determinadas instituciones u organizaciones que poseen el encargo de velar por la seguridad tecnológica de determinado sector. Nos permite definir, organizar y planificar los objetivos y funciones básicas para un mejor desempeño de la actividad. Durante la primera etapa de implementación del COS para el Grupo Empresarial BioCubaFarma se ha podido identificar y mitigar incidentes de seguridad cumpliendo así con los objetivos previstos. Actualmente se encuentra en fase de prueba otras soluciones que consolidarán la implementación del COS.