Universidad de Buenos Aires

Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Especialización en Seguridad Informática

CSOC from scratch

Necesidades de un CSOC.
Con propuestas de herramientas Open Source.

Autor: Lic. Javier José Vallejos Martínez.
Tutor: Ing. Hugo Pagola

Año presentación 2021
COHORTE 2012

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Javier José Vallejos Martínez
DNI 28.325.015

Resumen

Día tras día crecen las amenazas de Ciberseguridad contra las organizaciones. Si no es porque un Ransomware secuestró información importante para el negocio es porque alguien logró ingresar a sus sistemas desde una web publicada a Internet gracias a una vulnerabilidad no detectada a tiempo o muchísimas otras causas que podrían provocar a una empresa perder dinero, debido a que no pueden operar o porque se divulgó información confidencial o , incluso, porque les manipularon los sistemas sin su consentimiento. Y, no perdamos de vista que podría ser afectada su reputación.

Aquel que indique que no tiene incidentes de seguridad es porque no está controlando su infraestructura de forma adecuada desde el punto de vista de la Ciberseguridad. Para disponer de un adecuado control, las organizaciones deberían disponer de un Centro de Operaciones de ciberseguridad (CSOC por sus siglas en inglés, Cyber Security Operation Center), el cual monitorice apropiadamente cualquier anomalía que pudiera comprometer la seguridad de su infraestructura informática.

Para disponer de un CSOC, por lo general, es necesario la inversión de grandes sumas de dinero. Por un lado, por el costo que requiere la compra de appliances o software. Por otro lado, el gasto que implicará disponer de personal que deba formar parte de ese CSOC y estar atento a lo que suceda con la seguridad de la organización. Es por esta razón económica que muchas veces no se lleva adelante la implementación de un CSOC.

El presente trabajo abordará el concepto de CSOC, profundizará sobre sus implicancias y particularidades. Al cierre, se tratará la problemática del costo de las herramientas, con la finalidad de ayudar a las organizaciones a armar su propio CSOC utilizando herramientas Open Source y gratuitas para tener un control de seguridad sobre sus activos informáticos y su información sin la necesidad de realizar una inversión exagerada tanto en hardware como en software.

Palabras clave: soc, csoc, ciberseguridad, siem, open source, log, evento, incidente, informática forense, soar, network monitoring

Índice

1 Introducción....1
2 ¿Qué es un CSOC?....3
3 ¿Cuáles son las necesidades de un CSOC?....6
4 Personas....7
4.1 CSOC Manager....8
4.2 Analista Nivel 1....8
4.3 Analista Nivel 2....8
4.4 Hunter....9
5 Procesos....10
5.1 Etapas....11
5.1.1 Preparación....11
5.1.2 Identificación....11
5.1.3 Contención....12
5.1.4 Erradicación....12
5.1.5 Recuperación....13
5.1.6 Lecciones aprendidas....13
5.2 Indicador Clave de Desempeño (KPI)....14
5.2.1 CSOC KPI....14
5.3 Distintos tipos de CSOC....15
5.3.1 CSOC Interno....15
5.3.2 CSOC Externo....15
5.3.3 Follow the Sun....16
6 Tecnología....17
6.1 Endpoint....18
6.2 Netflow....18
6.3 Network Monitoring....19
6.4 Threat Intel....19
6.5 Forensic....20
6.6 Incident Detection/Management....21
7 El camino del Log....22
7.1 Registros (Logs)....22
7.2 Eventos....24
7.3 Alertas....25
7.3.1 Falso positivo....25
7.3.2 Verdadero positivo....26
7.3.3 Falso negativo....26
7.3.4 Verdadero negativo....26
7.4 Incidentes....26
7.5 Problemas....27
8 Tecnologías aplicadas en un CSOC....29
8.1 Log Management....29
8.2 Security Incident & Event Management (SIEM)....31
8.2.1 Sin agente....32
8.2.2 Basado en agente....33
8.3 Security Orchestration, Automation, and Response (SOAR)....33
9 Herramientas Open Source recomendadas....36
9.1 Forensic....36
9.1.1 Preservación....36
9.1.2 Análisis....37
9.2 Network Monitoring....38
9.3 Log Management....39
9.4 SIEM....40
9.5 SOAR....40
10 Conclusiones....42

11 Glosario.....44
12 Referencias.....48

1 Introducción

En las organizaciones los procesos se encuentran cada vez más informatizados, los usuarios disponen de al menos un dispositivo, ya sea una computadora de escritorio, laptop, tablet o un celular para conectarse a servicios que son brindados desde servidores, tal es el caso de aplicaciones Web, aplicaciones mobile, aplicaciones cliente-servidor, o hasta soluciones que corren bajo sistemas distribuidos.

A todo este mundo es necesario asegurarlo, ya que, cada vez son más frecuentes los ataques por cibercriminales. Las instituciones suelen contar con diversos sistemas de seguridad que ayudan a mantener sus pilares, confidencialidad, integridad y disponibilidad lo menos comprometidos posible. Tal es el caso de que se implementan soluciones de Endpoint Protection, Firewalls, IDPS, Web Application Firewall, Secure Web Gateway, soluciones de Data Leak Prevention, sistemas de monitoreo, soluciones de Doble Factor de Autenticación, entre muchos otros.

Si una empresa cuenta con todas estas soluciones específicamente relacionadas con mejorar la seguridad de una organización podemos presuponer que la misma cuenta con un nivel de madurez elevado de Seguridad de la Información.

Ahora bien, disponer de todas estas soluciones implica que debemos tener personal que se encargue de gestionar y monitorizar cada una de estas soluciones que, como he mencionado anteriormente, son una gran cantidad herramientas con sus propios archivos de log, en muchos casos sus propios dashboards. Lo que haría que el control de los resultados que emitan serían descentralizados y cada especialista estaría monitorizando la solución que gestiona.

En este punto es donde aparece el concepto de CSOC en donde dispondremos de toda la información necesaria para hacer un seguimiento articulado de todas las soluciones de seguridad, Sistemas Operativos, dispositivos de red, aplicaciones y bases de datos que dan soporte al

negocio de la organización. Mucha bibliografía hará referencia a SOC (Security Operation Center) pero en el presente trabajo se lo llamará CSOC.

2 ¿Qué es un CSOC?

Podríamos definir un Cyber Security Operation Center (CSOC) como el sector encargado de monitorear continuamente incidentes de Ciberseguridad dentro de una organización.

Un CSOC tiene como finalidad la prevención, protección, detección y respuesta ante amenazas que impacten en al menos uno de los pilares de la Ciberseguridad; que, como bien sabemos, son la confidencialidad, integridad y disponibilidad.

Cuando nos referimos a continuo no necesariamente se trata de 24 x 7 x 365 sino a la necesidad que posea el negocio de estar productivo. En algunos casos será de 9 a 18 horas y los días laborables. Pero, en otros casos, tendremos organizaciones que deberán mantenerse productivas durante todo el año, las 24 horas del día.

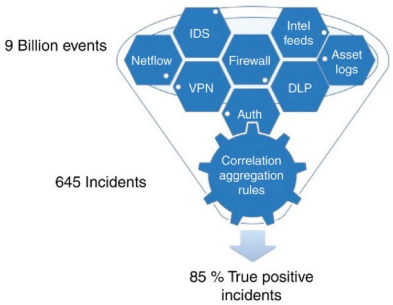
Uno de los beneficios que trae la implementación de un CSOC es que permite mejorar el tiempo de respuesta ante amenazas, ya que, realiza un monitoreo centralizado y constante de las mismas.[i] Según el proyecto OWASP Top 10 del 2017[ii] en el punto A10 llamado “Registro y monitoreo insuficientes” indican que “En 2016, la identificación de un incidente tomó un promedio de 191 días”, claro está que este tiempo no es acorde a las necesidades de las organizaciones de hoy.

Dentro de las funcionalidades principales de un CSOC pueden encontrarse las siguientes acciones:

- gestionar y monitorear en tiempo real (o lo mas real que se pueda),
- responder y remediar ante incidentes de ciberseguridad de forma coordinada,
- buscar vulnerabilidades continuamente,
- realizar técnicas de informática forense y
- generar reportes a los interesados sobre todas estas actividades.

Nathans, en su libro *“Designing and Building A Security Operations Center”*[x], habla de la importancia de calcular y utilizar las métricas que muestren la efectividad y eficiencia del CSOC. Dado que el CSOC necesita

una prensa positiva para garantizar que las personas puedan apreciar el arduo trabajo que realizan. Una excelente manera de presentar los esfuerzos de un CSOC en una métrica fácil de entender es un gráfico de embudo. Este gráfico puede representar todas las fuentes de datos que el CSOC está recopilando actualmente como datos de firewall, VPN, IDPS, etc.; en donde existen gran cantidad de eventos que son generados por todos estos dispositivos, alimentando a un concentrador de logs y procesados por un SIEM. Según las reglas, la correlación y la agregación de estos eventos, solo unos pocos incidentes se transformarán en tickets que el CSOC realmente tiene que analizar. Luego, existe una tasa de falsos positivos que también se puede calcular en función de la información de este ticket. Para construir este cuadro, debe observar todos los aspectos del CSOC.



En la imagen estamos viendo cada evento individual que se recopiló o generó con las herramientas de CSOC dentro de un solo mes. En donde fueron un total de 9 mil millones de eventos para dicho mes, esto se puede desglosar por tipo de dispositivo o qué dispositivo generó el evento si desea ese nivel de detalle. A continuación, todos los eventos pasan por un SIEM con el fin de correlacionar los eventos y determinar su validez para una revisión y análisis del CSOC. Hay muchas formas de condensar los eventos. Primero, puede tener un proceso de agregación, aquí es donde toma varios eventos que son iguales, los cuenta y produce solo un incidente único representativo de todos los demás. Por ejemplo, ¿un CSOC necesita ver 10,000 registros de denegación de un firewall o solo un evento único que

indica que hubo 10,000? Evidentemente, la agregación ahorra mucho tiempo y reduce drásticamente la cantidad de investigaciones que debe realizar un SOC. Múltiples eventos que son generados por la misma sesión o paquete, mismo host o destino o que tienen atributos de ataque similares pueden condensarse en eventos más pequeños o únicos, opuestos al envío de la información sin procesar a un analista.

Esta es la finalidad del CSOC, analizar todo lo que va ocurriendo en la infraestructura de la organización detectando de forma temprana incidentes de ciberseguridad.

3 ¿Cuáles son las necesidades de un CSOC?

Cuando pensamos en un CSOC no debemos pensar únicamente en la parte tecnológica sin en una interrelación entre Personas, Procesos y Tecnología.

iii

Esta interrelación es de suma importancia, debido a que, de tratarlas aisladamente provocará que el CSOC sea disfuncional y no se pueda sacar provecho del mismo, o hasta incluso que el mismo traiga una falsa sensación de seguridad a la organización.

A continuación se incursionará en cada uno de los tres pilares planteados. Para el caso de la tecnología se dará una breve descripción en este apartado debido a que en los subsiguientes se explotará el mismo.

4 Personas

En este punto es necesario tener en cuenta que un CSOC debe tener personal que se encuentre capacitado, desde el lado académico, sobre las tecnologías que manejará, sobre la infraestructura con la que trabajará y los procesos que se utilicen tanto en el propio CSOC como en la organización con la que trabaje. Al mismo tiempo, debe poseer experiencia en la posición que estará tomando, teniendo presente que cada rol dispondrá de la necesidad de diversas aptitudes, conocimientos y, como ya comentamos, experiencia.

Dentro de los roles que son necesarios para el funcionamiento de un CSOC se encuentran los siguientes:

- Manager
- Analista Nivel 1
- Analista Nivel 2
- Hunter

Si bien en varias lecturas se evidenciaron otros roles, los planteados son los considerados adecuados. Es importante remarcar que estamos hablando de roles y no de personas, dado que dependerá del tamaño de la organización y de la infraestructura la cantidad que disponga cada CSOC.

A continuación se darán las características de cada uno de los roles necesarios dentro de un CSOC.

4.1 CSOC Manager

El *Manager* será el encargado de administrar los recursos. Entendiendo como recursos al personal, el presupuesto y la programación de turnos. También tendrá a su cargo la planificación de la estrategia tecnológica para cumplir con los SLA. Al mismo tiempo debe corroborar que los procesos dentro del CSOC sean cumplidos, comunicar con la gerencia de la organización sobre las incidencias detectadas por el CSOC, con lo cual debe ser el nexo de la organización en incidentes críticos para el negocio.

Debe conocer los procesos de la organización, ya que, será el encargado en alinear los procesos de la misma con los del CSOC.

4.2 Analista Nivel 1

El *Analista de Nivel 1* debe monitorear continuamente las alertas de seguridad, supervisar la salud de los sensores y endpoint. Atender las incidentes reportados por los usuarios o entidades externas. En el caso de detectar una anomalía debe recopilar los datos y la información necesaria para pasarle esta información al *Analista de Nivel 2*.

Debe conocer tanto sobre los procesos de la organización como también de los procesos del CSOC. Al mismo tiempo, debe mantener actualizados los procedimientos que estén relacionados con sus labores.

4.3 Analista Nivel 2

El *Analista de Nivel 2* debe realizar un análisis del incidente mediante la correlación de datos de diversas fuentes, determinar si un sistema crítico o conjunto de datos ha sido comprometido, asesorar en la remediación y proporcionar soporte para nuevos métodos analíticos en la detección de amenazas.

Quien o quienes cumplan con este rol también deberán conocer tanto sobre los procesos de la organización como los del CSOC. Debe mantener actualizados los procedimientos que estén relacionados con sus labores y

corroborar que los procedimientos de rol *Analista de Nivel 1* sean acordes y actualizados.

4.4 Hunter

El *Hunter* posee un skill elevado, sobre la red, los endpoint, threat intelligence, informática forense y malware. También conoce sobre el funcionamiento de aplicaciones y la infraestructura que las soporta. Actúa como un “cazador” de incidentes, sin esperar incidentes escalados; estrechamente involucrado en el desarrollo, ajuste e implementación de análisis de detección de amenazas.

Debe conocer tanto sobre los procesos de la organización como también de los procesos del CSOC. Debe mantener actualizados los procesos que estén relacionados con sus labores.

5 Procesos

Los procesos del CSOC deben estar alineados, sin lugar a dudas, con los procesos de la organización. Para ello, es necesario que se tengan identificados los procesos críticos de la organización, las aplicaciones que hacen al negocio y la tecnología que soporta dichas aplicaciones.

Como indicamos anteriormente, la finalidad de un CSOC es, por un lado, dar una adecuada *Respuesta Ante Incidentes de ciberseguridad* o lo que llamaremos *RAICS* y, por otro lado, no esperar a que los incidentes sucedan sino identificar proactivamente las vulnerabilidades que pueda tener el entorno.

Tener los procesos de *RAICS* permitirá minimizar la cantidad y gravedad de los incidentes de seguridad, estableciendo claramente y poniendo en práctica todas las políticas, directivas y procedimientos acordes a la organización. Uno de los procesos dentro de *RAICS* será el de evaluar de forma regular las vulnerabilidades del entorno, auditar la configuración según los procedimientos, monitorear el tráfico de red y los sistemas, monitorear los logs de registro de los sistemas, comprobar los procedimientos de backup y restore, entre otras acciones necesarias para asegurar la efectividad del CSOC.

Una vez que se haya identificado la criticidad de cada activo de la organización, el proceso que llevará adelante el CSOC debe establecer diversas etapas específicas entre las cuales se encuentran las siguientes:

- Preparación
- Identificación
- Contención
- Erradicación
- Recuperación
- Lecciones aprendidas

5.1 Etapas

A continuación se abordará el detalle de cada una de las etapas recién planteadas.

5.1.1 Preparación

En la etapa de *Preparación* se establecerán todos los puntos de control necesarios para que el CSOC tenga la facilidad de reaccionar ante un incidente de ciberseguridad. En esta fase será muy importante que la organización disponga establecida la política, los procesos y procedimientos. La implementación de la tecnología que permita al CSOC cumplir con su política. Las necesidades de capacitación del personal para que tenga las capacidades necesarias para cumplir con la *RAICS*.

La finalidad de esta etapa es preparar al CSOC para *contener el daño y minimizar el riesgo e impacto* poniendo como prioridad la protección de la vida humana y la seguridad de las personas y, subsiguientemente, la protección de la información secreta y confidencial, de otra información, como datos científicos, sobre propiedad o del ámbito directivo, proteger el hardware y software contra ataques y minimizar la interrupción de los recursos informáticos.

5.1.2 Identificación

La etapa de *Identificación* permitirá al CSOC reconocer de forma temprana un incidente de ciberseguridad, ya sea por medio del monitoreo,

alertas enviadas por los usuarios o agentes externos. Los cuales son gestionados por parte de los *Analistas de Nivel 1*, o el equipo de *Hunters* que estará continuamente identificando debilidades en la seguridad de la aplicaciones, infraestructura informática y detectando anomalías en los sistemas.

Una vez identificado el incidente de ciberseguridad se deberá realizar una evaluación inicial, identificando la criticidad del incidente para el negocio y, en el caso de que el mismo posea una criticidad elevada, deberá dar aviso al Manager del CSOC con la finalidad de que este alerte al negocio sobre el incidente.

La comunicación es un factor muy importante en este punto.

En el caso de corresponder, se deberá notificar a los organismos externos con el fin de que realicen las acciones que correspondan.

Posteriormente se dará paso a la fase de *Contención*.

5.1.3 Contención

Habiendo sido identificado el incidente de ciberseguridad lo primero que debemos hacer es contener, con el fin de que la amenaza no pueda propagarse dentro de la organización. La finalidad que tiene la *contención* es que el impacto sea el menor posible, ya sea que se aísle un dispositivo específico, un conjunto de dispositivos, una red o lo que se considere necesario para el la problemática no trascienda a toda la red.

Una vez contenido el incidente se procederá a la *Erradicación*.

5.1.4 Erradicación

Durante el proceso de *erradicación* debemos no solo preocuparnos por eliminar el problema sino también por proteger las pruebas, en el caso que queramos llevar el incidente a la Justicia. Es por este último motivo que es de suma importancia que tengamos en nuestro equipo de trabajo, no solo personal que pueda reaccionar ante un incidente de ciberseguridad sino

también que pueda aplicar técnicas de Informática Forense con el fin de no contaminar las pruebas a presentar en una posible causa judicial.

Luego de erradicar el problema comenzará la etapa de *recuperación*.

5.1.5 Recuperación

Habiendo erradicado el problema, corroboramos no solo que no hayan quedado vestigios del incidente, sino que debemos asegurarnos que el vector de ataque utilizado se encuentre asegurado para que el mismo no pueda volver a ocurrir. Una vez hecho todo esto, re estableceremos los servicios que se hayan visto afectados.

Una vez recuperado el servicio comprometido por el incidente pasaremos a la última fase, la fase de las *Lecciones aprendidas*.

5.1.6 Lecciones aprendidas

En la fase de *lecciones aprendidas* debemos compilar y organizar la documentación del incidente, valorando los daños y costos del incidente. En muchos casos para nutrirnos de esta información debemos trabajar junto con el negocio.

Es esencial que se revisen los procesos minuciosamente, se determine con el equipo qué pasos se siguieron correctamente y qué errores se cometieron. Si los pasos se han seguido al pie de la letra entonces debemos verificar si nuestros procedimientos son los adecuados, si las alertas son las esperadas y corregir todo lo que nos haya permitido aprender el incidente.

Este análisis posterior tiene como objetivo encontrar oportunidades de mejora, que iniciarán un nuevo proceso de planificación de la respuesta a incidentes.

5.2 Indicador Clave de Desempeño (KPI)

Un Indicador Clave de Desempeño o Key Performance Indicator (por sus siglas en inglés) está directamente relacionado con un objetivo fijado previamente y normalmente se expresa en valores porcentuales pero no necesariamente. Los KPI tienen como objetivos principales medir el nivel de servicio, realizar un diagnóstico de la situación, comunicar e informar sobre la situación y los objetivos, motivar a los equipos responsables del cumplimiento de los objetivos reflejados en el KPI y, en general, evaluar cualquier progreso de manera constante.[iv]

5.2.1 CSOC KPI

Tal como indica Signtel en su artículo titulado “Mida: KPI modernos para SOC” “Sin métricas implementadas, muchos SOC terminan siendo iniciativas puramente impulsadas por el cumplimiento”.[v] No se aleja de una frase atribuida a Peter Ducker que indica que “no se puede gestionar lo que no se puede medir”. En el campo de la Ciberseguridad este término encaja a la perfección, más allá de ir implementando tecnologías, disponer de personal capacitado y de seguir las políticas y procedimiento acordes, es importante medir. Esta medición será útil no solo para quienes estén mirando los monitores, atentos a que no aparezcan nuevos incidentes, sino que también le servirá al negocio para entender cómo se está gestionando la ciberseguridad.

Dentro de los KPIs comunes dentro de un CSOC se encuentran los siguientes:

- Cantidad de sistemas y/o dispositivos controlados,
- cantidad de sistemas y/o dispositivos con vulnerabilidades conocidas,
- cantidad de incidentes reportados,
- tiempo desde la detección hasta la contención y la erradicación,
- cantidad de usuarios con permisos administrativos,
- sistemas actualizados vs no actualizados,

- monitoreo software de Endpoint Protection (actualizaciones, detecciones, etc.),
- cantidad de phishing identificado y
- otros indicadores.

5.3 Distintos tipos de CSOC

Dado que el CSOC estará a disposición de las necesidades del negocio, podremos tener varias formas para implementarlo. Por un lado, podríamos implementar nuestro CSOC dentro de nuestra propia infraestructura, a este tipo de implementación lo llamaremos CSOC Interno. Por otro lado, podríamos terciarizar el CSOC y que lo lleve adelante un proveedor que brinde el servicio desde sus instalaciones, a esta modalidad la identificaremos como CSOC Externo. Por último, una modalidad que busca abaratar los costos y tener un CSOC 7x24x365 es el que llamaremos Follow the Sun.

5.3.1 CSOC Interno

Para el caso del CSOC Interno, tanto la infraestructura tecnológica para dar soporte al CSOC, los recursos humanos y los procesos, pertenecerán a la propia organización.

Desde el Manager hasta el Analista deberán conocer tanto los procesos establecidos por la organización como por el propio CSOC. Asimismo, deberán gestionar los dispositivos que nutran de información para identificar las debilidades e incidentes en la entidad.

5.3.2 CSOC Externo

Para el caso de un CSOC externo, también conocido como Managed Security Service Provider (MSSP), se le estará pagando a un proveedor porque lleve adelante todas las tareas que enumeramos anteriormente teniendo que adaptar sus procesos internos con los procesos de cada cliente.

Para este servicio como para el que hablaremos a continuación, es muy importante que dispongamos de un SLA (Service Level Agreements) acorde a las necesidades del negocio.

5.3.3 Follow the Sun

Este concepto de CSOC hace referencia a habrá una rotación de la gestión del CSOC a medida de que vaya avanzando el día. Entonces, el proveedor estará gestionando el mismo desde distintas partes del mundo, obviamente con zonas horarias distintas. De este modo no habrá que pagar los analistas por horas nocturnas, lo que, en muchas circunstancias será una reducción de costos.

6 Tecnología

Un sistema de monitoreo de seguridad efectivo incorpora datos recopilados a partir del monitoreo continuo de endpoints (PC, notebooks, dispositivos móviles y servidores), así como redes y fuentes de registros y eventos.

Gracias a los datos recopilados de la red antes y durante el incidente, los analistas de CSOC pueden pasar del uso del sistema de monitoreo de seguridad como una herramienta de detección a utilizarla como una herramienta de investigación, revisando las actividades sospechosas que conforman el incidente actual, o incluso como herramienta para gestionar la respuesta a un incidente o incumplimiento. Para ello es de suma importancia la compatibilidad de las tecnologías, las cuales podrán dar como resultado el seguimiento de un incidente de ciberseguridad, evidenciando por dónde comenzó la intrusión, cuáles fueron los pasos dados por el cibercriminal e identificando cuáles fueron los activos comprometidos permitiéndonos tomar decisiones de cómo volver todo a la normalidad.

Si pensamos en componentes tecnológicos que debemos atender dentro de un CSOC no podemos dejar de lado los endpoints, netflow, darle importancia al monitoreo de red será importante, como así también a la detección y gestión de incidentes. No debemos dejar de lado, tal como

mencionamos más arriba a la Informática Forense, como así también Threat Intelligence.

A continuación se verán cada uno de estos puntos a considerar.

6.1 Endpoint

Cuando nos referimos a un endpoint estamos considerando cualquier dispositivo que actúe como punto final en una comunicación que formen parte de la red de la organización a la cual el CSOC deba atender. Entre ellos podemos encontrarnos desktops, laptops, teléfonos inteligentes, dispositivos de telecomunicaciones, tablets, televisores inteligentes, IoT, etc. Dentro de esta categoría también se encuentran los servidores, entre los cuales podemos tener con diversos servicios como web, aplicaciones, bases de datos, DNS, NTP, LDAP, servidor de archivos, de correos, FTP, etc.

No debemos olvidarnos de los propios dispositivos de Ciberseguridad que tengamos desplegados por la infraestructura de la organización, podemos mencionar entre ellos: firewall, IDPS, WAF, endpoint protection, proxy, DLP, entre otros.

Cada uno de estos endpoints mencionados poseen sus propios registros o mejor conocidos como logs relacionados con la seguridad del propio endpoint con lo cual debemos prestar atención a los mismos. De los logs hablaremos más adelante.

6.2 Netflow

Los servicios netflow fueron introducidos por Cisco Systems y brindan a los administradores de red acceso a la información de flujo de IP desde sus redes de datos. Los elementos de red (routers o switches) recopilan netflows y los exportan a recopiladores. Los datos recopilados proporcionan una medición detallada para un seguimiento de uso de recursos altamente flexible y detallada.

Un flujo se define como una secuencia unidireccional de paquetes con algunas propiedades comunes que pasan a través de un dispositivo de red. Estos flujos recopilados se exportan a un dispositivo externo, el recopilador

netflow. Los flujos de red son muy granulares; por ejemplo, los registros de flujo incluyen detalles como direcciones IP, recuentos de paquetes y bytes, marcas de tiempo, tipo de servicio (ToS), puertos de aplicación, interfaces de entrada y salida, etc.[vi]

6.3 Network Monitoring

El término Monitoreo de red (Network Monitoring) describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes.

Mientras que un sistema de detección de intrusos monitoriza una red por amenazas del exterior (externas a la red), un sistema de monitorización de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos).

Por ejemplo, para determinar el estatus de un servidor web un software de monitorización puede enviar, periódicamente, peticiones HTTP (Protocolo de Transferencia de Hipertexto) para obtener páginas

Comúnmente, los datos evaluados son tiempo de respuesta y estadísticas tales como consistencia y fiabilidad han ganado popularidad. Las fallas de peticiones de estado, tales como que la conexión no pudo ser establecida, el tiempo de espera agotado, entre otros, usualmente produce una acción desde del sistema de monitorización. Estas acciones pueden variar: una alarma puede ser enviada al administrador, ejecución automática de mecanismos de controles de fallas, etcétera.[vii]

6.4 Threat Intel

Al analizar un incidente o ataque se requiere una visión 360 para comprender los hechos y sus motivaciones. Para ello, los servicios de Threat Intelligence son clave.

Según Joaquín Molina en su artículo publicado en WeLiveSecurity define a Threat Intelligence como “Conjunto de datos organizados sobre ataques o amenazas”.[viii]

O, cómo lo define Cisco, Threat Intelligence se refiere a una tecnología dinámica y adaptable que aprovecha los datos del historial de amenazas a gran escala para bloquear y remediar de manera proactiva futuros ataques maliciosos en una red. Threat Intelligence en sí misma no es una solución, pero es un componente de arquitectura de seguridad crucial. Debido a la evolución de las amenazas, las soluciones de seguridad son tan efectivas como la inteligencia que las impulsa.[ix]

6.5 Forensic

Por definición, la Informática Forense es la aplicación de técnicas científicas y analíticas, especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Ahora bien, lo importante es poder llevar esta definición a la vorágine diaria de una organización que necesita los servicios productivos para ayer.

Para que este punto sea de utilidad dentro del CSOC debemos tener muy ajustados los procesos de respuesta ante incidentes al que más arriba llamamos RAICS.

Para llevar adelante las adquisiciones que nos permitirán realizar el análisis pertinente que nos llevará a sacar conclusiones y que las mismas puedan ser de aplicabilidad dentro de un proceso judicializado debemos hacer uso de herramientas destinadas para ello. Estas herramientas pueden ser por hardware o por software, pueden ser propietarias o de código abierto. Pero algo que debemos tener presente es que, en muchos casos, las herramientas que utilicemos nos servirán en determinados contextos y tendremos herramientas para las diferentes fases planteadas anteriormente (identificar, preservar, analizar y presentar).

6.6 Incident Detection/Management

Tal como indicamos en el apartado de Forensic, el tema de gestión y detección de incidentes se ha tratado en la sección de Procesos pero en este caso hablaremos de tecnologías que nos facilitarán la detección y gestión de Incidentes de Ciberseguridad.

Tal es el caso de un software de endpoint protection o mejor conocido como antivirus, el cual nos dará alerta al momento de que la solución identifique un malware dentro de nuestra infraestructura.

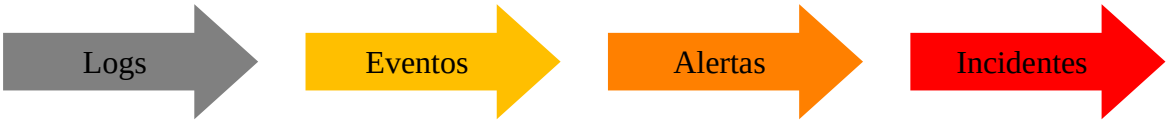
También tenemos IDPS y/o WAF que nos permitirán detectar intrusiones y en muchos casos mitigarlas.

Pero todas estas herramientas podrán nutrir a un integrante dentro de nuestro CSOC, el SIEM. Esta tecnología no solo nos permitirá detectar incidentes sino también gestionar los mismos. Más adelante tendremos un apartado específico para comprender la importancia de disponer de un correlacionador de eventos de ciberseguridad.

Otra herramienta que se está escuchando en la actualidad que complementan a los SIEM es el SOAR. Al igual que con el SIEM, trataremos esta tecnología en un apartado especial.

7 El camino del Log

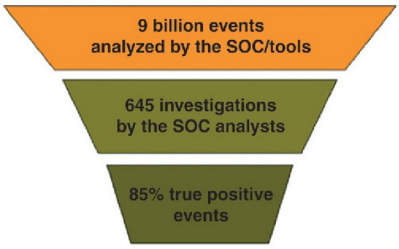
En este apartado se verá cómo desde un simple registro podemos detectar de forma temprana un incidente de ciberseguridad. Para ello comenzaremos hablando sobre las trazas, registros o mejor conocido como log. Una vez que sepamos de la importancia de un log específico lo catalogaremos a ese registro como un evento, en donde para determinados eventos querremos brindar una alerta y dependiendo de la repercusión que tenga el evento podrá considerarse que nos encontramos ante un incidente.



Muchos registros | Algunos registros | Pocos registros | Pocos registros muy importantes

x

Para pasar de un log a un evento y de un evento a un incidente podremos utilizar una herramienta que hidratará a nuestro CSOC de información, se la conoce como Security Incident & Event Management o SIEM.



A continuación se dará un repaso de cada uno de estos actores.

7.1 Registros *(Logs)*

Un registro o log es la forma más básica que un sistema pueda generar. El mismo puede ser brindado por un Sistema Operativo, una

aplicación, un servicio, o cualquier dispositivo podrá generar un log que almacene información básica sobre un suceso. Dentro de los logs podremos encontrar información cuando alguna acción dentro de nuestro sistema no tiene el comportamiento adecuado o, al menos, es cuando comúnmente se van a estar observando los logs. Tenemos que tener en cuenta que no solo se estará almacenando errores sino también aciertos y de ambos podremos sacar provecho de estos registros.[x]

Algo que debemos tener presente es que dependiendo del sistema será el log que tendremos, algunos sistemas guardarán sus registros en archivos de texto, algunos otros en bases de datos y en ciertos casos tendremos formatos propietarios.

Los logs siempre deberían contener información básica e incluir la información requerida para que sea lo suficientemente valiosa como para almacenarla. Uno de los principales datos que tenemos que registrar será el momento del suceso, esto quiere decir, la fecha, la hora y la zona horaria. Si bien es bastante lógico, es de suma importancia que todos nuestros sistemas tengan sincronizada la fecha y la hora, esto será muy importante al momento que queramos correlacionar eventos con nuestro SIEM. Para ello suele utilizarse un protocolo conocido como NTP. Para logs de red será muy importante incluir qué dispositivo realizó la acción y para ello será necesario almacenar la dirección IP. La siguiente es una lista con datos que deben almacenarse en un registro:

- Tiempo (fecha, hora y zona horaria),
- tipo de evento,
- si fue o no satisfactorio,
- severidad,
- origen,
- nombre del servicio,
- protocolo,
- usuario y
- descripción

Es muy importante tener en cuenta que no debemos registrar información sensible o confidencial en los logs, como por ejemplo:

Contraseñas, API Keys, claves de cifrado, información de tarjetas de crédito, etc.

Los logs pueden tener muy buenos usos y muchos propósitos, un ejemplo podría ser el uso de logs para la Informática Forense. Muchas organizaciones almacenarán sus logs por grandes períodos de tiempo, todo dependerá de su Política de gestión de logs en donde uno de sus puntos será la retención de dichos registros, esto significa que se especificará la cantidad de tiempo que deben resguardarse estos logs. La retención de los logs podrá permitir dar respuesta a cuestiones legales, ya que, podrá probar acciones en los sistemas en un momento preciso con lo cual podrá ser presentado como evidencia en un juicio. Para que sea válido, dichos logs deberán ser protegidos con la finalidad de que los mismos no sean manipulados. Como hemos visto más arriba, nuestro CSOC deberá conocer de las buenas prácticas de la Informática Forense con el fin de asegurar la no contaminación de la evidencia.

7.2 Eventos

Un evento no deja de ser un log pero es un log con un específico contexto que tiene un significado especial para la organización pero debemos tener en cuenta que no solo un evento surgirá a partir de un log, un evento podrá reportarse tanto por un usuario interno que recibió un phishing o por una organización externa, entre otros. Entonces podemos de hablar de evento por un input que deberá ser analizado para determinar si es necesario alertar y catalogarlo como un incidente de ciberseguridad.

Un evento puede ocurrir cuando un registro supera un umbral establecido, tal es el caso cuando un disco supera el 90% de espacio utilizado, cantidad de usuarios logueados en un sistema, etc. En muchos casos muchos de estos eventos no necesariamente son incidentes de ciberseguridad sino que en lugar de ser atendidos por el CSOC puede gestionados un NOC o Mesa de ayuda.

7.3 Alertas

Una alerta es un evento que generalmente activa una notificación o alarma preconfigurada porque alguno de estos eventos alcanzó un umbral específico y requiere de mayor atención. Estas alertas pueden representarse en un cambio en el Dashboard de una solución, en el envío de un correo electrónico, un mensaje de texto o un mensaje por Whatsapp, Telegram o Slack o hasta incluso el disparo de una sirena.

Un punto importante a considerar es que toda alerta debe generar un incidente y/o problema en nuestro sistema de tickets indicando que algo se encuentra fuera de un normal funcionamiento y requiere de una acción.

Las herramientas que utilicemos para generar las alertas es necesario que se las configure adecuadamente para que las alertas que generen sean las adecuadas y no genere alertas de más. Dependerá de nuestro CSOC esta configuración para determinar la validez, criticidad e importancia de las alertas. Estas alertas pueden catalogarse en:

- Falso positivo
- Verdadero positivo
- Falso negativo
- Verdadero negativo

7.3.1 Falso positivo

Un falso positivo hace referencia cuando nuestra sistema de gestión de eventos nos alerta por problema pero que en realidad no debería haberse considerado como tal. Una vez detectado un falso positivo habrá que mejorar nuestro sistema para que no reconozca este evento como un problema de forma tal que los problemas los siga alertando pero estos falsos positivos ya no más. Un ejemplo de un falso positivo podría ser que uno de nuestros WAF (Web Application Firewall) identifique que un usuario intentó inyectar un XSS (Cross Site Scripting) y que en realidad su contraseña era “script.new-pass08?’. El WAF al detectar el string “script” y algunos caracteres

especiales, al este patrón coincidir con las reglas que tenía cargada, no permitirá que el usuario se loguee y nos alerte del intento de intrusión.

7.3.2 Verdadero positivo

El verdadero positivo indica que si nuestra solución nos alertó por un incidente, el mismo es real y debemos prestar atención a dicha alerta. Siguiendo con el ejemplo brindado sobre nuestro WAF, si este nos alerta porque recibió un input con el siguiente contenido “’ OR ‘1’ = ‘1’ -- ” estamos sobre un intento al bypass de nuestro sistema de autenticación.

7.3.3 Falso negativo

Si nos tenemos que preocupar de algo, esos son los falsos negativos. En este caso, nuestro sistema de alertas nos estará alertando sobre un problema a nuestros sistemas. Entonces el sistema de alertas estará fallando en su cometido: Alertarnos ante un incidente de ciberseguridad. Es necesario tener en cuenta al momento de configurar nuestras herramientas qué tan laxos podemos ser para evitar tener falsos positivos.

Supongamos que nuestro WAF nos alerta un verdadero positivo y 9 falsos positivos con la misma alerta. Por lo tanto tomamos la determinación de decir que si son 9 falsos positivos entonces debemos quitar esta regla. Esta acción estaría permitiendo que ese verdadero positivo, el ciberataque real, pase, no nos alerte y se ejecute en nuestros sistemas. La mejor opción hubiera sido corregir la regla para que sea más precisa.

7.3.4 Verdadero negativo

Los verdaderos negativos son cuando realmente podemos estar tranquilos que nuestros sistemas no están siendo atacados. Esto quiere decir que todas nuestras reglas, herramientas y firmas están siendo evaluadas y no se encuentra patrón que deba alertar de incidente alguno.

7.4 Incidentes

Tal como lo define el NIST, un “incidente es una violación o amenaza inminente de violación a las políticas de Seguridad Informática”.[xi] Quien diga que en su organización no tienen incidentes de ciberseguridad, no está controlando adecuadamente su infraestructura o desconoce su definición. Un incidente de seguridad puede ser un phishing, un malware detectado por nuestra solución de endpoint protection, puede ser una inyección de SQL en nuestra aplicación Web. No necesariamente tiene que haberse explotado una vulnerabilidad y haber perdido millones de dólares. Es muy importante identificar todas esas amenazas inminentes porque podría terminar en una violación a nuestras políticas de ciberseguridad y entonces sí se podría impactar en algunos de nuestros pilares.

Es imperioso identificar qué tipo de incidente está aconteciendo debido a que cada uno tendrá respuestas particulares, si bien el proceso será a grandes rasgos el expuesto en el apartado de Procesos, cada uno tendrá su especificidad y tendremos que actuar en consecuencia.

Con el fin de tener métricas, muy importantes para el CSOC, debemos registrar todos los incidentes en algún sistema de tickets. De este modo, podremos hacer seguimiento a los mismos. Dentro de los registros que se vayan agregando al incidente debemos asegurarnos que posea información sobre el evento, las tareas realizadas y los resultados obtenidos.

7.5 Problemas

Podría suceder que a partir de la detección de un incidente de ciberseguridad surja un problema y que la solución de dicho problema pueda resolver el incidente. Cuando un incidente surge repetidamente es necesario realizar una investigación sobre la causa raíz, esta causa raíz es nuestro problema. Por ejemplo, evidenciamos que uno de nuestros endpoints el sistema de endpoint protection no está actualizando su base de firmas. Esto para nosotros es un incidente pero luego de un pequeño análisis detectamos que el problema fue que el sistema se había quedado sin espacio en disco y eso provocó nuestro incidente. Eliminar datos del disco eliminará el problema, con ello nuestro sistema de antimalware podrá actualizar su base

de firmas y nuestro incidente estará resuelto. Analizando la causa raíz identificamos que no tenemos una alerta que nos avise cuando nuestro disco esté próximo a llenarse o podría ser que otra aplicación esté causando problemas y logueando más de lo esperado en un período de tiempo muy corto.

8 Tecnologías aplicadas en un CSOC

8.1 Log Management

Por un lado, como comentamos anteriormente, una organización tendrá su infraestructura informática y de telecomunicaciones; donde se encontrarán, por un lado, las estaciones de trabajo, servidores, switches, routers que son necesarios para la operación del negocio. Por otro lado, debemos sumarles los dispositivos de seguridad informática que permitirán mantener la confidencialidad, disponibilidad e integridad de los datos tanto en tránsito como en reposo. Con el fin de disponer de una trazabilidad de lo que va ocurriendo en los sistemas disponemos de los registros o logs. Tener estos logs desperdigados por toda la organización hará que su gestión sea muy compleja, es acá donde aparece el concepto de Log Management o lo que comúnmente se conoce como Concentrador de logs. Para gestionar adecuadamente tantos datos es preciso que se priorice cuáles son los datos críticos y tratar los mismos en tiempo real (o lo más próximo que se pueda a ese concepto).

Un Concentrador de logs permitirá a la organización disponer los registros centralizados en una única ubicación. Estas herramientas son necesarias en un CSOC debido a que no podemos estar revisando los logs por separado. Se había planteado que existían cientos de miles de registros por día, dispersos en múltiples tecnologías de ciberseguridad; analizarlas por separado y manualmente demandaría un tiempo excesivo para identificar lo ocurrido durante un incidente.

Un Log Management es un un sistema capaz de recolectar y almacenar de forma segura datos completos de eventos sin procesar a largo plazo, tiene capacidades avanzadas de búsqueda e informes para que los auditores garanticen el cumplimiento de los controles organizacionales y para que el personal de seguridad realice investigaciones forenses e históricas.

Asimismo, exportar los logs de los dispositivos brinda un nivel de seguridad mayor dado que los registros se almacenarán en un repositorio distinto. Por ejemplo, supongamos que tenemos una aplicación web que se encuentra brindando servicios hacia Internet. Dicha aplicación se encuentra desarrollada en PHP y trabaja con un motor de base de datos MariaDB; cada uno de estos servicios se encuentra en un servidor distinto con el fin de mantener el concepto de defensa en profundidad y ambos se encuentran en una DMZ. El único puerto abierto en el Firewall hacia Internet será el tcp/443 y la IP del servidor de aplicación será la única con permiso de acceso al motor de base de datos. Ahora bien, pensemos que surge una vulnerabilidad 0day en PHP que afecta a la versión del motor de nuestra aplicación y que le permitiría a un atacante ejecutar código de forma remota o lo que se conoce como RCE. Si un atacante lograse explotar esta vulnerabilidad, tomar control del servidor y escalar en privilegios, podría comprometer los datos de nuestra aplicación, realizar un sin fin de actividades delictivas en nuestro equipo. Es aquí la importancia de que los logs se encuentren en un recurso externo a nuestro servidor. El atacante no podrá borrar sus rastros y nos permitirá analizar todas las acciones que realizó gracias a que los registros de las actividades realizadas por el atacante se encuentran en nuestro Concentrador de logs. Nuestros analistas forenses podrán trabajar con los datos brindados por este sistema a sabiendas que el mismo no ha sido manipulado.

La gestión de logs puede beneficiar a una organización de muchas formas. Ayuda a garantizar que los registros de seguridad informática se almacenen con suficiente detalle durante un período de tiempo adecuado. Las revisiones y análisis de registros de rutina son beneficiosos para identificar incidentes de seguridad, violaciones de políticas, actividad fraudulenta y problemas operativos poco después de que hayan ocurrido, y para proporcionar información útil para resolver dichos problemas. Los logs también pueden ser útiles para realizar auditorías y análisis forenses, respaldar las investigaciones internas de la organización, establecer líneas de base e identificar tendencias operativas y problemas a largo plazo.

Debido a que los logs contienen registros de la seguridad del sistema y la red, deben protegerse contra violaciones de su confidencialidad e integridad. Por ejemplo, los registros pueden capturar de forma intencionada o inadvertida información confidencial, como las contraseñas de los usuarios y el contenido de los correos electrónicos. Esto plantea problemas de seguridad y privacidad que involucran tanto a las personas que revisan los logs como a otras personas que podrían tener acceso a los registros a través de medios autorizados o no autorizados. Los logs que están asegurados incorrectamente durante el almacenamiento o en tránsito también pueden ser susceptibles de alteración y destrucción intencionales y no intencionales. Esto podría causar una variedad de impactos, incluido el permitir que las actividades maliciosas pasen desapercibidas y la manipulación de pruebas para ocultar la identidad de una parte maliciosa[xii].

Es importante que separemos dos tecnologías, las cuales en muchas oportunidades suelen confundirse pero que cada una tienen distintos propósitos. Estas soluciones son un Log Management -del cual acabamos de hablar- y un SIEM, del cual profundizaremos en el próximo apartado.

8.2 Security Incident & Event Management (SIEM)

Tal como comenté anteriormente, la organización tendrá múltiples tecnologías y dentro de las mismas miles de reglas, las cuales generarán cientos de miles de registros en menos de un día. Un Concentrador de logs recolectará grandes volúmenes de datos por un largo plazo pero no es su finalidad correlacionar los eventos entre sí para lograr determinar si ha ocurrido un incidente de ciberseguridad y si quisiéramos relacionar los logs entre distintas tecnologías será más difícil aún. Acá es donde aparecen los SIEM (Security Incident & Event Management).

A un SIEM, en cambio, se lo conoce como un Correlacionador de eventos. Es capaz de recopilar y almacenar a corto plazo datos e información relevantes para la seguridad. Tiene funcionalidades que permitirá agregar eventos similares, correlacionar múltiples eventos para construir nuevos eventos destacados para la seguridad. Algunos SIEM

poseen, como una cualidad más dentro de su accionar, un Concentrador de logs pero como no todos cuentan con uno, los trataremos por separado.

Dicho esto, podremos pensar en que ambos sistemas (Concentrador de Logs y SIEM) tendrán acciones similares pero que serán utilizados en diferentes circunstancias. Ambos utilizarán gran cantidad de almacenamiento pero, claramente, un Gestor de logs requerirá de mayor espacio. Y, desde el punto de vista del procesamiento, si bien un Log Management, requerirá de un procesamiento importante al momento de realizar alguna consulta, un SIEM estará procesando gran cantidad de datos de forma constante. Un ejemplo claro que brinda, David Nathans, es el siguiente: “Cuando un ciberdelincuente ataca un servidor, puede haber cientos de solicitudes únicas a ese servidor y, por lo general, puede ser muy ruidoso en cuanto al volumen de eventos. En un sistema de Gestión de logs, este ruido puede ser muy difícil de ver con miles de otros registros que se recopilan al mismo tiempo. Con un SIEM, se pueden crear reglas para ver este tipo de actividad automáticamente y crear una nueva alerta única que notifique a su CSOC que un posible ataque está en progreso”x.

Con lo cual, no debemos pensar en si es necesario que un CSOC tenga un Log Management o un SIEM, ambas son tecnologías necesarias en este tipo de entornos, ya que, cada una tiene su propia finalidad.

La alta velocidad y el rendimiento serán las dos preocupaciones principales para el hardware de un SIEM. Un Correlacionador de eventos puede recibir eventos de cientos de orígenes distintos y a partir de los mismos generar reglas que permitan identificar incidentes de ciberseguridad. El SIEM podría interactuar con la solución que dispongamos de gestión de tickets y/o enviarnos alertas.

Los SIEM admiten dos mecanismos para recopilar información:

8.2.1 Sin agente

El servidor SIEM recibe datos de los dispositivos que generan los logs sin necesidad de tener ningún software especial instalado en esos hosts. Algunos servidores extraen registros de los dispositivos, lo que generalmente

se hace haciendo que el servidor se autentique en cada host y recupere sus registros con regularidad. En otros casos, los hosts envían sus registros al servidor, lo que generalmente implica que cada dispositivo se autentique en el servidor y transfiera sus registros con regularidad. Independientemente de si los registros se insertan o extraen, el servidor luego realiza el filtrado y agregación de eventos, como así también la normalización y análisis de registros en los logs recopilados.

8.2.2 Basado en agente

Se instala un agente en el dispositivo que genera los logs para realizar el filtrado y la agregación de eventos, como así también la normalización de registros para un tipo particular de log, luego transmite los datos de registro normalizados a un servidor SIEM, generalmente en tiempo real o casi en tiempo real para análisis y almacenamiento. Si un host tiene varios tipos de registros de interés, puede que sea necesario instalar varios agentes.

Nadie puede negar que un SIEM es una herramienta fundamental dentro de un CSOC dado que correlacionará los eventos para que nos enteremos cuando algo se ha salido de su curse normal y se ha provocado un incidente en nuestra infraestructura informática, este dispositivo nos permitirá monitorear de manera proactiva indicios sospechosos de amenazas. Este tipo de soluciones nos colaborará con la generación de informes con métricas que ayudará tanto al área técnica como al negocio a entender sobre los incidentes producidos en nuestra infraestructura.

8.3 Security Orchestration, Automation, and Response (SOAR)

SOAR [xiii] [xiv] [xv] o Security Orchestration, Automation, and Response u Orquestación, Automatización y Respuesta de Seguridad es, según Gartner[xvi], una solución que combina en una única plataforma:

- respuesta ante incidentes,
- orquestación y automatización, y

- threat intelligence.

Una plataforma de SOAR también es utilizada para documentar e implementar procesos y dar soporte a la gestión de incidentes de ciberseguridad.

Las soluciones SOAR unifican tres tecnologías que poseen atributos comunes:

- Plataformas de Respuestas ante Incidentes de Seguridad o SIRPs.
- Automatización y Orquestación de Seguridad o SOA.
- Plataformas de Threat Intelligence o TIPs.

Dado a que las soluciones disponen de gran cantidad de eventos o alertas y existe complejidad y duplicación de herramientas, la automatización promete resolver estos problemas. En el campo de la ciberseguridad, SOAR es el vehículo para realizarlo.

En este punto es importante recalcar que para pensar en implementar SOAR nuestra organización debe tener un nivel de madurez alto. Esto quiere decir que tendremos desplegadas soluciones de ciberseguridad por nuestra organización, estaremos recolectando los logs y hasta tendremos una solución tipo SIEM que gestionará los incidentes. Recién en este estadío deberíamos pensar en la implementación de una plataforma como SOAR.

La orquestación de ciberseguridad reúne diferentes herramientas, procesos y personas de seguridad para mejorar la seguridad general de la organización. Al combinar la gestión de las mejores herramientas de su clase, la orquestación de la seguridad permite a los equipos de ciberseguridad hacer su trabajo de forma más eficiente. La automatización de la ciberseguridad suele ser un componente de la orquestación de la ciberseguridad. Lleva el concepto básico un paso más allá, automatizando los procesos repetitivos en un CSOC para mejorar la eficiencia y liberar tiempo para que los equipos de seguridad realicen tareas más valiosas.

La orquestación, automatización y respuesta de seguridad (SOAR) combina la orquestación y la automatización con una estrategia de respuesta para acelerar, estandarizar y acortar la respuesta a incidentes. Este método de conectar tecnologías de seguridad, automatización, inteligencia de

amenazas y respuesta a incidentes permite a las organizaciones responder para evaluar a las amenazas de inmediato, mejorando su postura de seguridad general y, a menudo, previniendo las violaciones de datos en primer lugar.

La gestión exitosa de amenazas no se trata solo de detección; depende de una respuesta rápida. Los sistemas SOAR toman los datos recopilados de los sistemas SIEM, junto con los datos de otras fuentes, como herramientas de prevención de pérdida de datos (DLP), alertas de servicios administrados y otras investigaciones, y dan contexto a esos datos. SOAR define el análisis de incidentes y los procedimientos de respuesta en un formato de flujo de trabajo digital. Se trata de priorizar las actividades de respuesta a incidentes y acelerar los tiempos de respuesta para mantenerse al día con el panorama de amenazas en evolución actual [xvii].

Por lo tanto es importante recalcar que un sistema SOAR no reemplaza al SIEM sino que será una tecnología que complementará al mismo para una adecuada respuesta ante incidentes. SOAR permite una tomar mejores decisiones y puede automatizar la ejecución de los flujos de trabajo que responderán al incidente, reduciendo significativamente el tiempo de respuesta.

9 Herramientas Open Source **recomendadas**

Como hablamos al comienzo del trabajo, una de las principales barreras para la implementación de un CSOC es el gasto. Parte de esos gastos son las licencias de los productos de ciberseguridad que suelen ser muy elevados. Es por eso que una opción es optar por software Open Source y gratuito que nos permitirá minimizar los costos y disponer de soluciones testeadas y con muy buenos rendimientos.

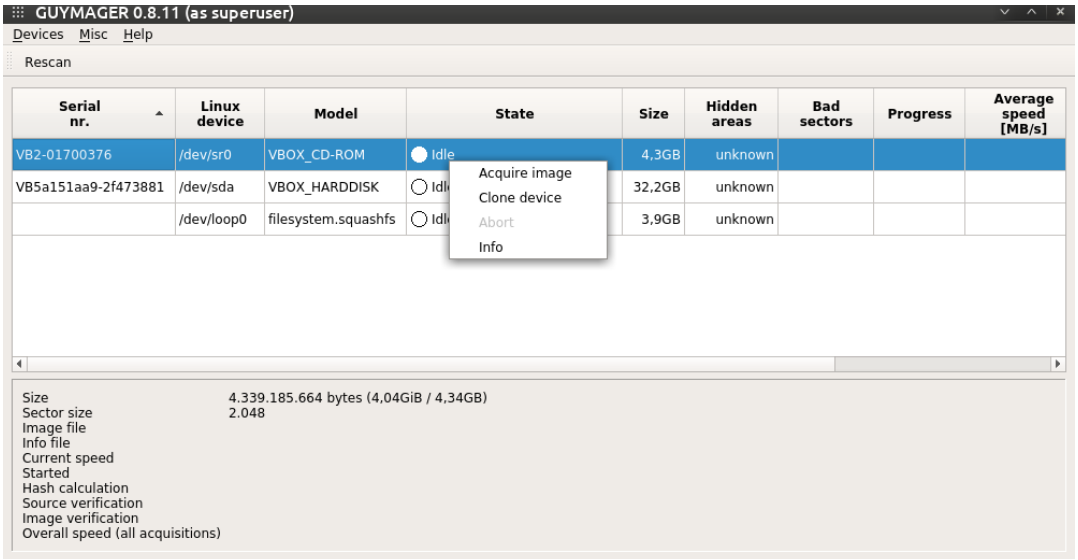
Soluciones Open Source hay muchas, con lo cual para cada una de las tecnologías propuestas se expresará una única solución que cumple con las necesidades de cada tecnología. En cada caso se presentará una imagen del Dashboard que podría presentar la solución para que el lector pueda tener una primera impresión de la misma.

9.1 Forensic

Dentro de las herramientas Open Source utilizadas dentro del ámbito de la Informática Forense podemos encontrarnos varias y dependerá de la fase en la que estemos la herramienta que utilicemos.

9.1.1 Preservación

Para la preservación, particularmente al momento de la adquisición puede utilizarse una herramienta de muy fácil uso dado que posee una interfaz gráfica de usuario, esta herramienta es GUYMAGER. La misma nos permitirá realizar imágenes forenses, copias bit a bit de discos para que dicha imagen o artefacto pueda ser presentado en una instancia judicial.

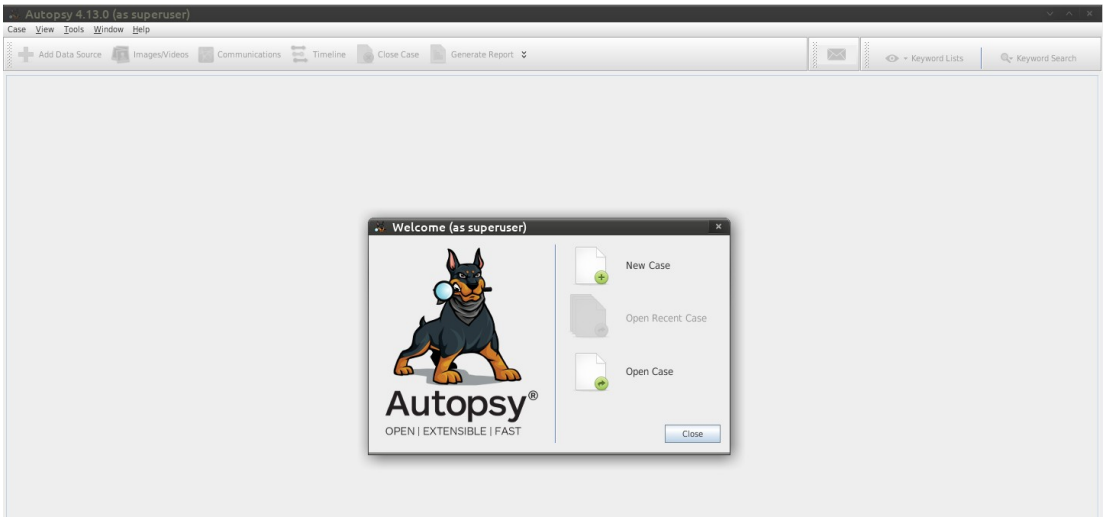


Link de referencia de la aplicación: https://guymager.sourceforge.io/

9.1.2 Análisis

Para la fase de análisis disponemos de una solución altamente utilizada dentro del campo del Open Source llamada Autopsy.

Autopsy es una solución desarrollada en Java que nos permitirá agregar los artefactos que hayamos recolectado en la fase anterior y que realizará un análisis automatizado utilizando varios de sus plugins. Hay que considerar que para su uso se requerirá de hardware suficiente para que Autopsy trabaje eficientemente. Lo interesante que tiene la herramienta es que no tiene que finalizar todo su análisis para empezar a mostrarnos resultados. Como viene de la familia de The Sleuth Kit, una de sus grandes cualidades será la extracción de la línea de tiempo. Autopsy hace uso de un conjunto de otras herramientas Open Source para llegar a un muy buen resultado.



Link de referencia de la solución: https://www.autopsy.com/

9.2 Network Monitoring

Una herramienta Open Source que se utiliza en gran medida como solución de monitoreo de red es Zabbix. La misma nos permite monitorear no solo redes sino también servidores, servicios de nube, aplicaciones, servicios, webs, bases de datos, entre muchas cosas más.

Dentro de Zabbix podremos ir sumando templates que nos incrementará los monitores en nuestra solución.

Link de referencia de la solución: https://www.zabbix.com/

9.3 Log Management

Como tecnología de Log Management se propone el uso de la solución presentada por Grafana, en la cual podrán utilizarse distintos componentes, y otras soluciones que podrán colaborar con el envío y procesamiento de logs.

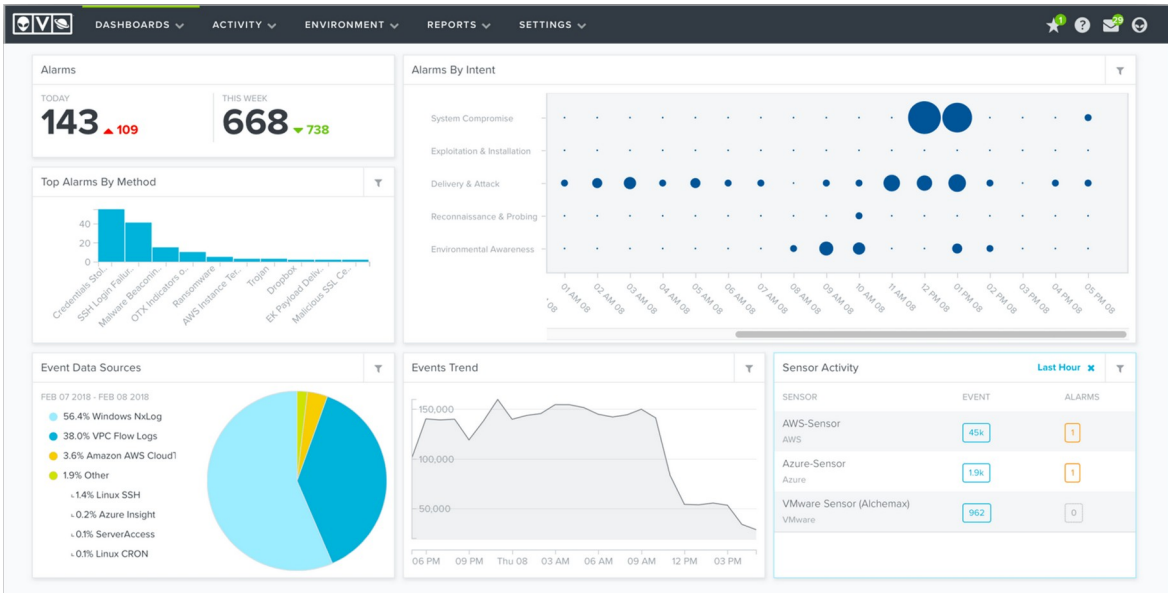
Entre los componetes mencionados se encuentran los siguientes:

- Grafana, permite realizar consultas, visualizar, generar alertas y dashboards a partir de los logs recolectados. Link: https://grafana.com/oss/grafana/
- Grafana Loki, es un sistema de almacenamiento de registros multi-tenant de alta disponibilidad, escalable horizontalmente, inspirado en Prometheus. Está diseñado para ser muy rentable y fácil de operar. No indexa el contenido de los registros, sino un conjunto de etiquetas para cada flujo de registros. Link: https://grafana.com/oss/loki/
- Fluentd, bajo este entorno se recomienda para el envío y recepción de logs de sistemas Linux. Link: https://docs.fluentd.org/

- NXLog, permite el envío de logs de Windows para que los mismos sean almacenados posteriormente en Grafana Loki. Link: https://nxlog.co/products/nxlog-community-edition

9.4 SIEM

Para el caso del SIEM una solución Open Source que viene utilizándose hace muchos años y que suele dar buenos resultados es OSSIM (Open Source Security Information Management). En la actualidad se la conoce como AlienVault OSSIM, la cual es la versión de Comunidad ofrecida por la empresa AT&T.



Link de referencia de la solución https://cybersecurity.att.com/products/ossim.

9.5 SOAR

Dentro de las tecnologías planteadas en el presente trabajo, SOAR es la más reciente. De la misma, la solución con mayor renombre en el campo del Open Source es TheHive.

Link de referencia de la solución https://thehive-project.org/

10 Conclusiones

Como bien se expresa en la publicación de Gartner titulada “Tips for Selecting the Right Tools for Your Security Operations Center”, “los CSOC son como copos de nieve, ya que, no hay dos iguales. Muchos aún tienen que alcanzar el nivel de madurez deseado y el modelo operativo objetivo”[xv]. Muchas veces las organizaciones quieren tener un CSOC sin pensar en todas las incumbencias que esto trae de la mano. Esto implica el nivel de madurez desde la óptica de la ciberseguridad que una organización requiere para pensar en tener un CSOC.

Como hemos visto durante el presente trabajo, un CSOC no solo es implementar tecnologías como un Concentrador de logs, un SIEM y/o un SOAR, sino que se trata de mucho más. Obviamente, que muchas de esas tecnologías las necesitaremos pero aún nos falta pensar en ese recurso tan preciado, aquel que llevará adelante nuestro CSOC; ese recurso son las personas. Las personas que tengan la responsabilidad de formar parte del CSOC deberán estar capacitadas y disponer de la experiencia necesaria en el rol que les toque cumplir. En algunos casos será meramente técnico, en otros necesitará de capacidades técnicas y de negocio; como así también tendremos a quien lleve las riendas, quien deberá sumarle a estas últimas capacidades las de gestión de personas.

No nos olvidemos de los procesos que, como también vimos durante el trabajo, será necesario no solo tener en consideración los procesos del CSOC sino también todo el personal deberá conocer los procesos de la organización.

Como cada organización es un mundo, también es importante definir si tenemos las capacidades dentro de la institución para implementarlo, considerando que podríamos optar por un MSSP o un CSOC externo. El cual dispondrá de la experiencia sobre las tecnologías que serán empleadas, el personal estará capacitado en la gestión de estas tecnologías y sólo tendrían que incorporar los procesos de la organización.

La implementación de un CSOC puede tener costos muy elevados. Por un lado, el personal deberá contar con las capacidades adecuadas y, por otro lado, las tecnologías que apliquemos. Desde el punto de vista de las tecnologías deberemos preocuparnos por los costos de hardware y de software. Por este último gasto podríamos pensar en soluciones Open Source y gratuitas como las planteadas al cierre de este trabajo. Las mismas son utilizadas tanto en pymes como en grandes corporaciones e incluso en estados. Disponemos de herramientas Open Source y gratuitas de: Monitoreo de red, Concentradores de logs, SIEM, SOAR y para el análisis post mortem disponemos de herramientas de informática forense. Muchas de ellas disponen de la suficiente madurez como para brindarnos el soporte que requerimos en las tecnologías a aplicar en nuestro CSOC. En algunos casos, estas herramientas o soluciones estarán mantenidas por la comunidad y en otros por organizaciones privadas. Haciendo uso de ellas, no solo estamos utilizando herramientas testeadas, gratuitas y a las cuales podemos acceder a su código fuente; sino que el propio uso de estas soluciones nos permitirán colaborar con el proyecto.

Pero recordemos que, ya sea que utilicemos herramientas propietarias u Open Source y gratuitas, para lograr armonía en nuestro CSOC es necesario que exista sinergia entre estos tres pilares: “tecnología, procesos y personas”.

11 Glosario

- **0day**: Vulnerabilidad de la cual no se dispone de parche o forma para mitigarlo por parte del proveedor del servicio.
- **Alerta**: evento que generalmente activa una notificación o alarma preconfigurada.
- **Antimalware**: solución que permite proteger dispositivos de malware.
- **API (Application Programming Interface)**: conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar el software de las aplicaciones.
- **API Key**: identificador único utilizado para autenticar a un usuario o programa de llamada a una API.
- **AT&T (American Telephone & Telegraph)**: multinacional estadounidense, conglomerado de empresas y sociedad gestora.
- **Backup**: copia de seguridad, respaldo, copia de respaldo o copia de reserva.
- **Bypass**: sobrepasar una medida de seguridad aplicada.
- **CSOC (Ciber Security Operation Center)**: Centro de Operaciones de Ciberseguridad.
- **Dashboard**: tablero que permitirá visualizar fácilmente indicadores.
- **Data Leak Prevention**: también conocido como Data loss prevention, solución para la prevención de fuga de información.
- **DMZ**: zona desmilitarizada, se la utiliza para aislar la red que publica datos a Internet de la red interna de una organización.
- **Doble Factor de Autenticación**: uso de dos factores de autenticación (algo que sé, algo que tengo, algo que soy). Mecanismo que mejora la seguridad al momento de identificar a un usuario dentro de una aplicación o sistema.
- **Endpoint Protection**: solución que permite proteger dispositivos de malware.
- **Evento**: log con un específico contexto que tiene un significado especial.

- **Firewalls**: diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- **Fluentd**: aplicación Open Source para el envío y recepción de logs.
- **Forensic** (Informática Forense): aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
- **Grafana**: aplicación Open Source para realizar consultas, visualizar, generar alertas y dashboards.
- **Grafana Loki**: aplicación Open Source para el almacenamiento de registros multi-tenant de alta disponibilidad, escalable horizontalmente, inspirado en Prometheus
- **IDPS (Intrusion Detection and Prevention System)**: sistema de detección y prevención de intrusos.
- **Incidente**: violación o amenaza inminente de violación a las políticas de Seguridad Informática.
- **Input**: dato que ingresa a un sistema informático.
- **KPI**: indicador clave o medidor de desempeño.
- **Log**: registro que evidencia lo ocurrido en un sistema.
- **Log Management**: concentrador de logs.
- **Malware**: software malicioso.
- **MariaDB**: sistema de gestión de bases de datos derivado de MySQL con licencia GPL.
- **Mesa de Ayuda**: es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las Tecnologías de la Información y la Comunicación (TIC).
- **MSSP**: Proveedores de servicios de seguridad administrados
- **Netflow**: protocolo de red desarrollado por Cisco Systems para recolectar información sobre tráfico IP.

- **NIST**: National Institute of Standards and Technology (https://www.nist.gov/)
- **NOC**: centro de operaciones de red, responsable de diseñar, instalar, dar mantenimiento correctivo y preventivo a la operación (Gestión, Soporte y monitoreo) de redes de telecomunicaciones de datos.
- **NTP**: Protocolo de Internet para sincronizar los relojes de los sistemas informáticos. NTP utiliza UDP como su capa de transporte, usando el puerto 123 por defecto.
- **NXLog**: herramienta de centralización y recopilación de registros multiplataforma que ofrece funciones de procesamiento de registros, incluido el enriquecimiento y el reenvío de registros.
- **Open Source**: software al cual se tiene acceso a su código fuente.
- **OSSIM (Open Source Security Incident Management)**: SIEM Open Source.
- **Output**: dato que egresa de un sistema informático.
- **PHP**: lenguaje de programación de uso general que se adapta especialmente al desarrollo web.
- **RAICS**: respuesta ante incidentes de ciberseguridad.
- **Ransomware**: malware que pide rescate para recuperar el objeto secuestrado.
- **Restore**: restauración a partir de un backup.
- **Script**: secuencia de comandos que se usa para designar a un programa relativamente simple.
- **Secure Web Gateway**: solución proxy de navegación con detección y filtrado del tráfico WEB, técnicas de antimalware, filtrado de URLs, detección de sitios maliciosos y visibilidad sobre tráfico cifrado.
- **SIEM**: gestión de eventos e incidentes de seguridad, este sistema se utiliza como correlacionador de eventos.
- **SIRP**: plataformas de respuestas ante incidentes de seguridad.
- **SLA**: acuerdo de nivel de servicio.
- **Slack**: herramienta de mensajería en equipo.
- **SOA**: automatización y orquestación de seguridad.

- **SOAR**: orquestación, automatización y respuesta de seguridad.
- **SQL**: lenguaje de consulta estructurada, utilizado en programación, diseñado para administrar, y recuperar información de sistemas de gestión de bases de datos relacionales.
- **Telegram**: aplicación enfocada en la mensajería instantánea, el envío de varios archivos y la comunicación en masa.
- **TheHive**: Una plataforma de respuesta a incidentes de seguridad gratuita, de código abierto y escalable. Diseñada para facilitar la vida de los SOC, CSIRT, CERT y cualquier profesional de seguridad de la información que se ocupe de incidentes de seguridad que deban ser investigados y tomados medidas
- **Threat Intelligence**: información sobre amenazas y actores de amenazas que ayuda a mitigar eventos dañinos en el Internet.
- **TIP**: Plataformas de Threat intelligence, centraliza una colección de datos de amenazas de numerosas fuentes y formatos.
- **WAF (Web Application Firewall)**: Firewall utilizado para proteger aplicaciones web, el mismo trabaja en la capa 7 del modelo OSI.
- **Whatsapp**: aplicación de mensajería instantánea para teléfonos inteligentes, en la que se envían y reciben mensajes mediante Internet, así como imágenes, vídeos, audios, grabaciones de audio (notas de voz), documentos, ubicaciones, contactos, gifs, stickers, así como llamadas y videollamadas con varios participantes a la vez, entre otras funciones.

12 Referencias

i Building a Security Operations Center (SOC), https://www.rsaconference.com/writable/presentations/file_upload/tech-203.pdf (consultada el 12/08/2017).

ii A10:2017-Insufficient Logging & Monitoring, https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring (consultada el 16/08/2021).

iii Building a World-Class Security Operations Center: A Roadmap, https://finland.emc.com/collateral/white-papers/rsa-advanced-soc-solution-sans-soc-roadmap-white-paper.pdf (consultada el 12/08/2017).

iv Indicador clave de rendimiento, https://es.wikipedia.org/wiki/Indicador_clave_de_rendimiento (consultada el 14/04/2021).

v Measure up: Modern KPIs for SOCs, https://www.singtel.com/business/articles/measure-up-modern-kpis-for-socs (consultada el 12/06/2021).

vi Cisco Systems NetFlow Services Export Version 9, https://datatracker.ietf.org/doc/html/rfc3954 (consultada el 12/06/2021).

vii Monitoreo de red, https://es.wikipedia.org/wiki/Monitoreo_de_red (consultada el 12/06/2021)

viii Threat Intelligence: el porqué de las cosas, https://www.welivesecurity.com/la-es/2016/12/01/threat-intelligence/ (consultada el 12/06/2021).

ix What Is Cyber Threat Intelligence?, https://www.cisco.com/c/en/us/products/security/what-is-cyber-threat-intelligence.html (consultada el 12/06/2021).

x Designing and Building A Security Operations Center – Elsevier - David Nathans – 2015.

xi Computer Security Incident Handling Guide - NIST Special Publication 800-61 – Paul Cichonski, Tom Millar, Tim Grance y Karen Scarfone – 2012

xii Guide to Computer Security Log Management - NIST Special Publication 800-92 – Karen Ket y Murugiah Souppaya – 2006

xiii What is SOAR? Definition and Benefits, https://www.fireeye.com/products/helix/what-is-soar.html (consultada el 23/05/2021).

xiv What is SIEM? What is SOAR? How are they different?, https://swimlane.com/blog/siem-soar (consultada el 23/05/2021).

xv Tips for Selecting the Right Tools for Your Security Operations Center – Gartner – Published 23 January 2020.

xvi Market Guide for Security Orchestration, Automation and Response Solutions – Gartner – Published 21 September 2020.

xvii SOAR - Security Orchestration, Automation and Response, https://www.ssh.com/academy/ssh/security-orchestration/soar (consultada el 31/07/2021)