EL SOC Y LAS FUENTES DE INFORMACIÓN

TLP:WHITE

seresco

Realizado por el Equipo de Ciberseguridad de Seresco.

El SOC (Centro de Operaciones de Seguridad), es el elemento clave dentro de una organización. Son muchos los aspectos que se han de tener en cuenta a la hora de la puesta en marcha de un centro de operaciones:

- **LA ARQUITECTURA DE ESTE.**
  Si se desea tener un servicio *on premise* o por el contrario un servicio nube.
- **HERRAMIENTAS UTILIZADAS.**
  Existen gran variedad en el mercado y debemos tener claro cuáles son las apropiadas para nuestra organización.
- **EQUIPO ENCARGADO DE SU OPERACIÓN.**
  Desde este punto de vista, la decisión es si el equipo formará parte de la propia organización o si por el contrario deseamos subcontratar el mismo.

Pero quizás uno de los aspectos más importantes es la identificación y conjugación de las fuentes de información, tanto internas como otras externas a la organización, lo cual permita establecer una estrategia para la identificación de comportamientos maliciosos y por tanto la anticipación a los ataques, o al menos poder determinar que estemos ante una situación de peligro lo antes posible.

ESTABLECIENDO UN ENFOQUE INTELIGENTE PARA LAS DETECCIONES

Desde nuestro punto de vista, los pasos que se han de seguir para la realización de un enfoque inteligente que nos permita llegar a realizar detecciones son los siguientes:

1. GESTIÓN DE CONOCIMIENTO

En la sociedad digital actual en la que vivimos, estamos rodeados de información la cual llega a nosotros a través de diferentes fuentes de información.

Hemos oído en muchas ocasiones la expresión **"La información es poder".** Preparando este artículo, consultamos diferentes publicaciones relacionadas con la gestión de conocimiento y nos encontramos con una idea mucho más interesante y la cual fija de alguna forma la inquietud a la que una organización se enfrenta cuando trata de gestionar su información:

"La información no es poder. En sí misma, la información es sólo un insumo más. Es usted, individuo infoalfabetizado, el que tiene el poder en tanto sabe cómo, cuándo, dónde y para que usar la información. Es ahí cuando el insumo se convierte en oro."

De este pensamiento se infieren por tanto dos ideas fundamentales:

- **La importancia de disponer de información,** y además de una información de calidad. Evitar el ruido que no nos aporta nada.
- **La necesidad de realizar una gestión del conocimiento** con el objeto de poder aplicarlo en beneficio propio.

1.1. PERO, ¿QUÉ ES EXACTAMENTE LA GESTIÓN DEL CONOCIMIENTO?

La gestión del conocimiento es el proceso de recopilar, compartir, mantener o administrar y desplegar de manera más efectiva el conocimiento organizacional.

1.2. ¿POR QUÉ ES TAN IMPORTANTE HACER UNA GESTIÓN DE CONOCIMIENTO?

Básicamente el **objetivo principal es poner orden en el caos.** Como hablaremos a continuación, se disponen de decenas de fuentes de información de las que inferir conocimiento, si el objetivo es poder realizar detecciones reales en el menor tiempo posible, eliminando o limitando al mínimo el número de falsos positivos es necesario disponer de los mecanismos que nos permitan de una forma inteligente procesar toda la información gestionada para obtener conclusiones interesantes y de valor.

¿Qué necesitamos por tanto?

- Entender que información estamos recogiendo y que queremos hacer con ella.
- Identificar cual es la información que estamos recogiendo y cual todavía no.
- ¿Cuál es nuestro plan? ¿Nuestro framework de actuación?

Y, ¿cómo lo haremos?

- Normalizando los datos para lograr consistencia en los mismos. Que en el equipo todos hablemos en el mismo idioma.
- Priorizando los sistemas de comunicación, los flujos de trabajo y la captura de datos.
- Paso a paso. El objetivo no es hacernos con productos o soluciones costosas, sino aprovechar las funcionalidades de las implantadas, el funcionamiento dentro de la organización así como la relevancia de la información aportada.

1.3. HERRAMIENTAS NECESARIAS PARA HACER UNA BUENA GESTIÓN DE CONOCIMIENTO

Se precisan de estas cuatro herramientas fundamentales para la realización de una gestión del conocimiento, entendiendo que todas tienen el mismo nivel de importancia y relevancia y por tanto han de estas presentes para un tratamiento completo:

- **Framework / procesos de trabajo.**
  Permiten dar cohesión al equipo de trabajo para utilizar y mantener la información, utilizando un lenguaje unificación de comunicación y también el establecimiento de la estrategia del estudio de comportamientos.

- **Tecnología.**
  Herramientas que van a dar soporte a todos los procesos. Todos sabemos lo que es un SIEM (herramienta CORE del SOC), pero también es preciso de otras herramientas de apoyo para hacer efectiva la inteligencia de amenazas, inferencia de comportamientos, modelado y detección de amenazas, ticketing y estudio de casos, y en general todas aquellas soluciones que permitan dar soporte a las funciones del SOC y permitan almacenar, gestionar, tratar y acceder a la información de forma rápida y eficiente.

- **Personas.**
  Los actores principales dentro del SOC, los cuales son no solo los consumidores de la información, sino los encargados del mantenimiento de la integridad e interpretación de esta.

- **Contenidos.**
  Relacionado con la información en sí misma y así como la representatividad y calidad de esta.

2. FUENTES DE INFORMACIÓN

Anteriormente hablábamos sobre la necesidad de hacer una buena gestión del conocimiento, entendiendo lo importante que es la información.

Nos encontramos ahora ante un dilema. ¿Qué fuentes de información existen? Y sobre todo, ¿cuáles son las que me interesan?

¿Y ahora qué escojo? ¿Es mejor un EDR o un XDR o un NDR? ¿En qué se diferencian? ¿Para qué sirven?

Quizás alguno de nosotros nos veamos representados ante esta situación cuando llegamos a una organización. También ocurre con las estrategias de algunos proveedores de servicios de seguridad cuando se acercan a una organización, en la que pretenden transmitir la idea de que para estar seguros e informados de lo que ocurre con los sistemas de esta es preciso disponer de todas las soluciones de seguridad del mercado.

¿Pero es esto realmente cierto? Desde luego nada más lejos de la realidad.

2.1. TIPOS DE FUENTES DE INFORMACIÓN EXISTENTES

De forma general, dentro del mundo de la investigación una fuente de información es simplemente el soporte en el que encontramos información, es decir donde nos vamos a encontrar los datos.

Las fuentes de información se pueden clasificar en:

- **Primarias.**
  Se corresponden con las más cercanas posible al evento que se investiga. Son como los testigos directos que observan la acción ocurrida.
  - Log en bruto de las aplicaciones, redes, sistemas, etc.
  - Información que podemos obtener de sistemas y dispositivos como:
    - *FW*
    - *WAF*
    - *DNS*
    - *IDS*
    - *IPS*
    - *EDR*
    - *HIDS*
    - *NAC*
    - *DLP*
    - *VDS*
    - *Y de forma general todas las relacionadas con dispositivos de monitorización, escaneo, bloqueo y/o detección de parámetros.*

- **Secundarias.**
  Se basan en las primarias a las que dan un cierto tratamiento o análisis para obtener nueva información.
  - Información obtenida mediante el análisis de un artefacto o una pieza de malware.
  - Información intercambiada con otros CERT o CSIRT o SOC.
  - Repositorios de acceso abierto o de pago con IOCS, como el proporcionado por la herramienta REYES del CCN-CERT u otros como AlienVault, Anomali, Virus Total, Palo Alto, Recorded future, etc.

- **Terciarias.**
  Se trataría de aquellas que recopilan y comentan las fuentes primarias y secundarias. Para nosotros este tipo de fuentes son las que te tienen más que ver con el acceso público a datos tales como:
  - Medios de comunicación.
  - Foros y blogs de temas especializados.
  - Redes sociales como Twitter, Facebook, Instagram, como por ejemplo Unit42 o Red Canary.
  - También grupos de difusión como los creados en Telegram.
  - Investigaciones sobre amenazas y ciberseguridad realizados por proveedores, y equipos especializados.
  - Boletines de seguridad.
  - Etc.

Lo ideal para hacer una buena investigación es poder hacer una combinación de los tres tipos de fuentes.

3. ¿QUÉ ESTRATEGIA DEBEMOS SEGUIR PARA LA REALIZACIÓN DE LAS DETECCIONES?

Llegados a este punto ya tenemos claro que es muy importante hacer una gestión de la información, que además es posible disponer de distintas fuentes pero seguimos sin saber cuáles de todas ellas son las que realmente nos interesan.

Hay varios aspectos para tener en cuenta como punto de partida:

- Por un lado el **grado de exposición y las tecnologías utilizadas en la organización.** Nos dará un mapa de calor de riesgo.
- Por otro lado, la **realización de un estudio de contexto.** No es lo mismo el establecimiento de un servicio de SOC para una empresa automovilística que para una entidad bancaria por ejemplo.
- **Identificar los objetivos de monitorización y detección que pretenda alcanzar la organización.** Este aspecto es el más difícil de identificar puesto que depende del nivel de madurez de la propia organización y del propio conocimiento que esta tenga de sí misma así como de los antecedentes de incidentes que hayan identificado y sufrido en el pasado.

Una vez recogida y estudiada esa información, nos queda establecer una estrategia para las detecciones. Podemos hacer una clasificación de las estrategias a seleccionar en función de la dependencia de estas sobre la matriz Mitre ATT&CK:

- **ESTRATEGIAS BASADAS EN LA MATRIZ DEL MITRE ATT&CK.**
  Se dispone de dos posibles opciones:
  - **Cubrir la matriz por completo.**
    Una estrategia pudiera ser el tratar de definir reglas de detección y establecimientos de casos de uso que implique el disponer de elementos de monitorización sobre todas las técnicas, subtécnicas y procedimientos definidos en la matriz.
    En relación con esta esta estrategia nos encontramos con dos dificultades o inconvenientes:
    - *Por un lado se ha de tener en cuenta que actualmente la versión actual de la matriz cuenta con 14 tácticas de las que cuelgan 191 técnicas y 385 subtécnicas, por lo que el trabajo se vuelve costoso y complicado.*
    - *No es posible asegurar que aun cubriendo todas las mismas el riesgo para las detecciones sea cero.*
  - **Seleccionar las técnicas a cubrir.**
    Otra opción, quizás más interesante sea el cubrir sólo unas determinadas técnicas y subtécnicas las cuales están relacionadas con la mayoría de los ataques conocidos y que además encajen con el estudio previo y definición de objetivos de la organización del cual hemos partido.
    Existen diversos estudios que se pueden tener en cuenta como información de partida sobre las técnicas más utilizadas por los atacantes:
    - ***PICUS. Red report.*** *Incluye una relación de las 10 técnicas más utilizadas por atacantes.*
    - ***ENISA. Threat Landscape.*** *También incluye información sobre las técnicas más utilizadas por atacantes. Curiosamente discrepa en algunas con PICUS.*
    - ***MITRE. Desde el propio mitre hay un grupo de trabajo A Tech Foundation for Public Good -***

MITRE Engenuity (mitre-engenuity.org) *desde el cual realizan estudios al objeto de identificar las TTP más utilizadas y con los que se puede colaborar.*
Como resultado más interesante de su estudio han identificado que la técnica ***T1059 (Command and scripting intepreter),*** *sería la facilitadora de la mayoría de los ataques.*
El principal conveniente para el desarrollo de esta estrategia es confiabilidad de los datos. Para poder determinar cuáles son las técnicas más utilizadas por los atacantes, los organismos y empresas encargadas de emitir los resultados de los estudios, se basan en la información de la que disponen por lo que la confiabilidad de los resultados depende de la información de partida de la que dispusieran.

- **ESTRATEGIAS NO BASADAS EN LA MATRIZ DE MITRE ATT&CK.**
  Olvidémonos por un momento que la matriz de Mitre no existe y que tenemos que enfrentarnos solos a la definición de una estrategia. Podríamos disponer de las siguientes opciones:

  - **Basado en riesgos.**
    Desarrollar una estrategia basada en riesgos es responder al miedo de la organización.
    El aspecto principal es identificar las amenazas y puntos débiles de los que dispone la organización.
    El *framework* que podemos utilizar en este caso por ejemplo "NIST Incident Response", teniendo en cuenta los pilares: identificar, detectar y responder.
    A continuación dibujar un *mindmap* en el que situemos en el centro los riesgos, alrededor cada uno de los pilares, y a continuación en capas las herramientas, fuentes de datos, etc.
    Descendiendo en ese desarrollo, llegaremos a un punto en el que se identifiquen justo los mecanismos que permiten materializar las amenazas, y por tanto en donde debemos fijar las detecciones.

  - **Sin base procedimental.**
    La idea sería no buscar tácticas ni técnicas concretas, sino fijarse en la realidad de lo que está ocurriendo en la organización.
    Los atacantes no tienen por qué seguir patrones ni estructuras concretas para sus ataques. Las TTPs que conocemos nos permiten identificar amenazas que se repiten pero no nuevas forma de ataque ni comportamientos inesperados.
    Desde nuestro punto de vista esta es la estrategia más difícil de desarrollar.

El establecimiento de una estrategia nos permitirá identificar cuáles son las fuentes primarias de las que vamos a obtener la información de las detecciones. Para aquellas que dependen de la matriz, la misma ayuda e incluye información de las fuentes necesarias para cada técnica.

En el caso de las fuentes secundarias y terciarias, depende del propio servicio de SOC, de la validez del equipo, de sus *frameworks* y procesos para mantenerse actualizados con esa información de calidad.

Y es justo en este punto, junto con la capacidad para gestionar todos los tipos de fuentes, y la forma en que el equipo es capaz de hacer una explotación de los datos, lo que hace que la monitorización, y ese caos inicial de posibles datos del que partimos, pase a proporcionarnos conocimiento.

Y es que al final el conocimiento que tiene un equipo entrenado, así como el aprovechamiento de sinergias entre distintos proyectos y colaboraciones con otros equipos, es impagable.

4. PROBANDO LA ESTRATEGIA

Existen dos formas de probar la estrategia y gestión realizada:

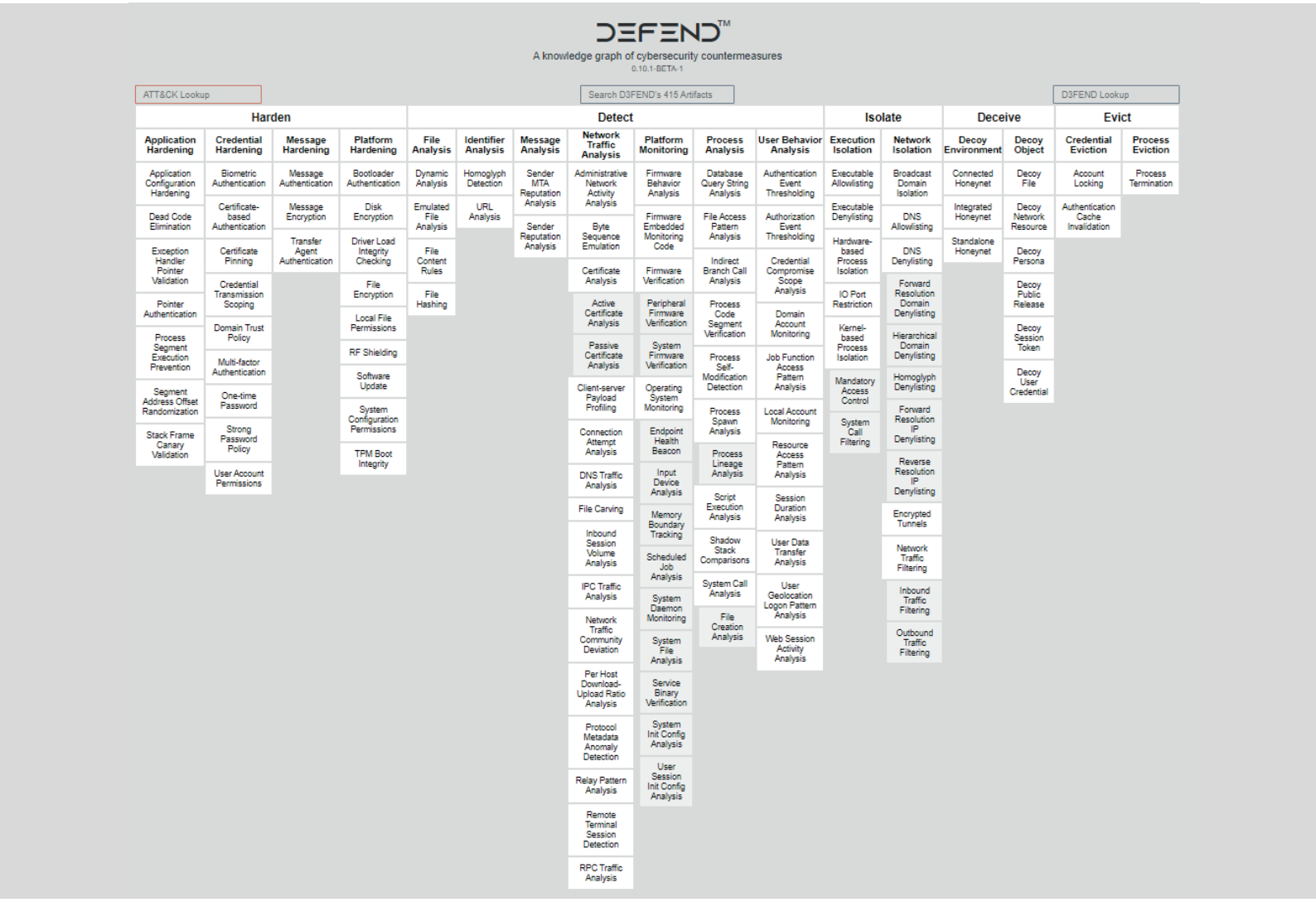
- **Realizar simulaciones de ataques.**
  Ejecución de ejercicios de *red team/blue team*, prueba de ruido, ciberejercicios específicos, etc., permitirá poner a prueba a la organización diversas situaciones y casos de uso para analizar el nivel de madurez tanto en las detecciones como en la gestión de situaciones anómalas.

- **Dejar que se nos materialicen ataques reales.**
  Relacionada directamente con una prueba por escarmiento. En contraste con la anterior opción, en la que se realizan de forma continuadas pruebas de concepto, en este caso la organización establecería la confianza en la validez y eficacia de su propia estrategia tomando únicamente como lecciones aprendidas los resultados de los incidentes de ataques materializados y/o detectados de forma temprana.

5. IMPLEMENTAR MEDIDAS DE PREVENCIÓN: DEFEND

Además del objetivo de detección o anticipación a la materialización de ataques, una de las medidas más importantes a tener en cuenta dentro de las organizaciones para evitar la materialización de incidentes de seguridad, es la implementación de medidas de prevención.

En este sentido, desde Mitre han desarrollado un importante proyecto el cual ha dado como fruto la matriz DEFEND.



Sin entrar en más detalles, puesto que no es el objeto de este artículo, la matriz DEFEND representa debilidades que se pueden identificar en el seno de las organizaciones y las cuales son las que pueden favorecer la materialización de ataques, y establece cuales son las medidas de mitigación que es necesario implementar para minimizar los riesgos relacionados con las mismas.

Puesto que esta matriz está íntimamente relacionada con ATT&CK, es posible identificar las mitigaciones precisas para paliar el riesgo de cada TTP reflejada en la misma.

CONCLUSIONES

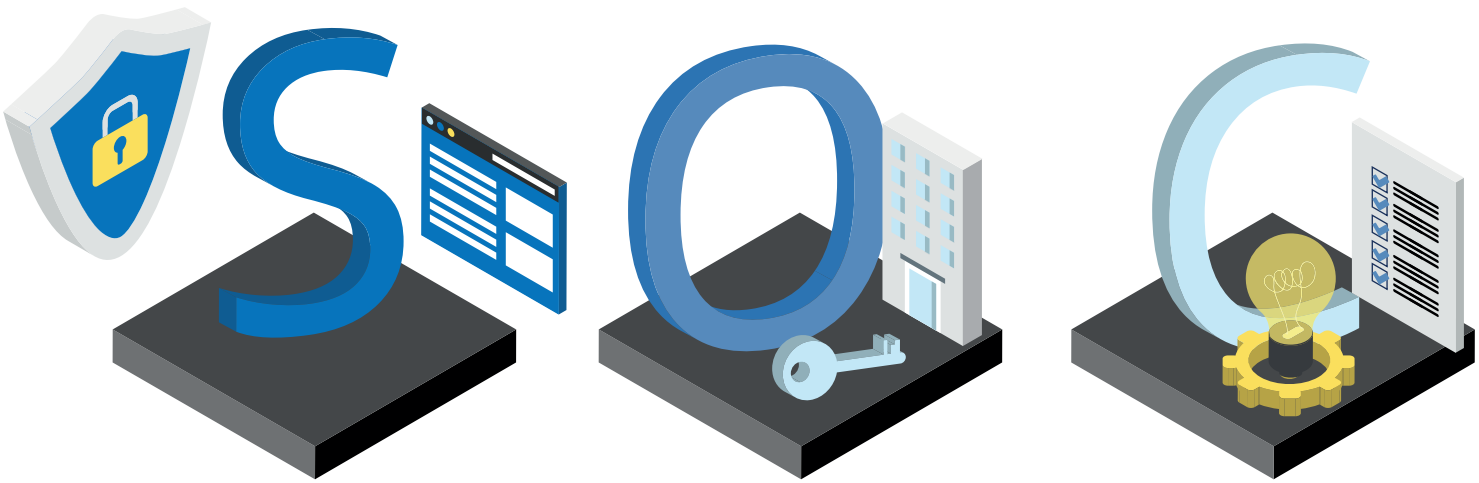
Varios aspectos que quisiéramos resaltar como conclusiones:

- **La necesidad de compartir información.**
  En este sentido existe un proyecto importante a nivel nacional promovido por el CCN-CERT que es la Red Nacional de SOC, pero vendrán otros a nivel Europeo después de este.
  Resaltar que Seresco en el momento actual colabora con dicho proyecto, perteneciendo a la Red Nacional de SOC en la categoría GOLD.

- **La importancia de la calidad de la información con la que tratamos.**
  Seleccionar muy bien las fuentes y saber combinarlas es todo un arte.

- **La coordinación para poder seguir las pistas.**
  Una alerta aislada por sí misma no aporta información de calidad. Sólo el disponer de una estrategia y un buen equipo coordinado, permitirá llegar a buenas conclusiones y detecciones.

Desde Seresco nos ponemos al servicio de las organizaciones para el establecimiento de su servicio de SOC teniendo en cuenta todos los aspectos reflejados previamente.



www.seresco.es