1. INTRODUCCIÓN A LA INTELIGENCIA DE FUENTES ABIERTAS (OSINT)

Cada vez es más común escuchar en las noticias que una organización o empresa de cualquier sector profesional ha sido víctima de un ataque cibernético. Este hecho en sí genera un problema a resolver con una serie de preguntas que sin ser analizadas no tienen respuesta alguna:

- ¿Cuánto tiempo ha estado expuesta la empresa ante dicho ataque?
- ¿Únicamente han accedido a los sistemas expuestos en la DMZ de la compañía (Internet) o han conseguido acceder a sistemas internos?
- ¿La vulnerabilidad es un 0-day o es una vulnerabilidad ya conocida?
- ¿Han robado información confidencial de la empresa? ¿Han filtrado información de la empresa en Internet?
- ¿Quién y porque ha atacado a la empresa?
- ¿Cómo han accedido a la empresa? ¿Hay un Insider en la compañía? ¿Necesitamos mejorar nuestras defensas?
- ¿El ataque producirá a la empresa un daño reputacional?

Estas son algunas de las preguntas que puede plantearse cualquier empresa, organización u organismo ante un ataque. Frente a esta situación y con la idea de proteger mejor los activos digitales y/o sistemas es posible utilizar la Inteligencia con el objetivo de reducir la incertidumbre ante una situación en particular y tomar las mejores decisiones.

Según el **Diccionario LID de Inteligencia y Seguridad** la propia Inteligencia podría definirse como "ese p*roducto obtenido tras aplicar a la información técnicas de análisis, de forma que resulte útil al decisor a la hora de tomar sus decisiones con el menor nivel de*

incertidumbre posible, siguiendo el Ciclo de Inteligencia".

Lo primero que debemos tener en cuenta en Inteligencia es esa necesidad real a la que se enfrenta nuestro decisor y ahí es donde la propia Inteligencia puede ayudarle a tomar la mejor decisión que se adecue a su negocio. Por un lado, ese decisor puede ser nuestro jefe, cliente, proveedor o un compañero de otro departamento y por otro lado, esa necesidad mencionada hace referencia a la Necesidad de Información asociada a un problema al que hay que dar respuesta.

Gracias a las técnicas de análisis mencionadas anteriormente en la definición de Inteligencia podemos transformar ese dato recolectado de Internet, ya sea de manera manual o automática, a Inteligencia pasando por un proceso de elaboración mediante el Ciclo de Inteligencia (ver apartado 1.5).

En un primer momento partiremos de un dato recolectado por alguna herramienta, descubierta de manera manual o facilitado por algún compañero con el objetivo de su investigación. Dicho **dato** hace referencia a esa unidad mínima que por sí sola no nos indicará nada, ya que será necesario un procesamiento y un tratamiento de esta para convertirlo en **información** ya tratada. En este caso, dicha información seguiría siendo un material sin evaluar, pero ya si estuviera dirigido hacia un objetivo en particular, pero faltaría aún aplicarle un análisis para separar el grano de la paja y quedarnos con una información de valor. Con esto último ya tendríamos un conocimiento sobre un suceso o actividad en el que contaríamos con una visión general del mismo junto con un contexto de la situación.

Para acabar todo el proceso de generación de Inteligencia (ver Imagen 1) sería necesario adaptar dicho conocimiento resultante al decisor idóneo (ver apartado 1.4), plasmarlo en un informe y añadir unos planes de acción que le ayuden a tomar decisiones. Sin esto último no estaríamos hablando de un producto de Inteligencia.

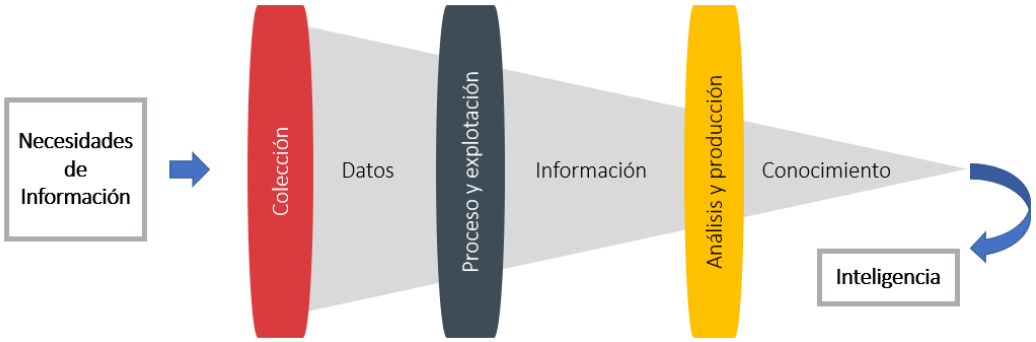

Imagen 1. Transformación del dato a Inteligencia

1.1. EL ORIGEN DE OSINT

Antes de conocer el origen de OSINT tenemos que conocer a que nos referimos con ello. OSINT es la abreviatura de "*Open Source Intelligence*" o lo que es lo mismo Inteligencia de fuentes abiertas, que según el **Diccionario LID de Inteligencia y Seguridad** podríamos definirlo como "*Información elaborada por los analistas mediante la utilización de fuentes abiertas para una audiencia concreta, con la finalidad de dar respuestas a un requerimiento especifico de información. Es resultado de la aplicación de los procesos de recogida, selección, contraste, validación y análisis característicos del Ciclo de Inteligencia*".

A grandes rasgos OSINT es esa generación de Inteligencia basándose en información de carácter público obtenida por medio de las fuentes abiertas.

Desde un enfoque clásico las fuentes abiertas son:

- La prensa
- La radio
- La televisión
- La literatura gris,

Esta última hace referencia a cualquier tipo de documento que no es difundido por los canales ordinarios de publicación comercial. También es conocida como literatura no convencional, semi-publicada o invisible y un ejemplo de ello sería: Informes, actas de

congresos, tesis doctorales, proyectos final de grado o posgrado, memorias, boletines, encuestas, patentes y marcas, leyes y normas, entre otros.

Con la llegada de Internet y el desarrollo de las nuevas tecnologías ha permitido disponer de un nuevo abanico de posibilidades donde ahora podríamos acceder a contenido procedente de buscadores genéricos, buscadores especializados, redes sociales, blogs, foros, servicio de imágenes por satélite, sitios paste, entre otros.

El primer uso de OSINT que aparece en los libros fue en 1935 justo antes de la II Guerra Mundial dónde el periodista alemán *Berthold Jacob* escribió un libro sobre los generales alemanes y la división Panzer, apoyándose para ello en la información que iba apareciendo en el *German Press*, el periódico alemán más importante de la época; el nivel de detalle fue tal, que esto acabó causando su detención y posterior interrogatorio. En ese momento lógicamente no existía OSINT pero sí que vemos similitud en la acción de obtener información en este caso por medio de la literatura gris de la época.

En 1941, ya en plena Segunda Guerra Mundial, el presidente *Franklin Roosevelt* crea la Oficina de Servicios Estratégicos (OSS), precursor de la CIA, para recopilar y analizar información estratégica, así como realizar espionaje y operaciones especiales. Este Servicio de Inteligencia estaba dedicado a todas las actividades secretas básicas: análisis, espionaje, acción encubierta, propaganda y contrainteligencia.

En 1942 por medio de la creación del departamento **Research and Analysis**, dentro de la **Oficina de Servicios Estratégicos (OSS),** nace OSINT tal y como lo conocemos en la actualidad. Este departamento se encargaba de recopilar toda la información obtenida por medio de fuentes abiertas, recopilando periódicos de las Potencias del Eje (Italia, Alemania y Japón) gracias a una nutrida red de embajadas y consulados, escuchando las emisiones de las radios públicas extranjeras, o en general, accediendo a librerías y fuentes de información oficiales.

En 1946, la **Oficina de Servicios Estratégicos (OSS)** paso a llamarse **Servicio de Información de Difusión Extranjera / Foreign Broadcast Information Service (FBIS)**.

En 1947, el FBIS paso a formar parte de la **Agencia de Central de Inteligencia (CIA)**,

agencia de recién creación amparada bajo la Ley de Seguridad Nacional. Su objetivo giraba en torno a la monitorización de prensa y radio. La CIA en 2009 desclasifico un interesante documento donde se habla del origen del FBIS[1] elaborado en 1969.

En 2001 surgió de manera oficial la primera definición sobre OSINT por medio de **Allied Joint Intelligence de la OTAN** como: "*La inteligencia derivada de una amplia gama de recursos abiertos, como la radio, la televisión, los periódicos, los libros; a los que el público tiene acceso*".

En 2006 nace EUROSINT FORUM, asociación sin ánimo de lucro creada con el apoyo de la Comisión Europea con el propósito de promover la cooperación europea sobre Inteligencia de fuentes abiertas y con el objetivo de ayudar en la prevención frente a amenazas y riesgos derivados sobre la paz y la seguridad.

[1] Origen del FBIS: Documento desclasificado de la CIA donde explica el origen del FBIS. Enlace: https://www.cia.gov/readingroom/collection/foreign-broadcast-information-service-history-part-1-1941-1947

1.2. OSINT ENFOCADO EN LA INVESTIGACIÓN DE AMENAZAS

Antes de comenzar explicando cómo puede enfocarse OSINT a la investigación de amenazas, es necesario introducir los conceptos de **Activo** y **Vulnerabilidad**. Según la guía CCN-STIC, un activo es "un componente de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.".

Es decir, un **tipo de recurso que tiene un valor concreto (tangible o intangible) para una organización o estado**. Algunos de ellos son los siguientes:

- Cualquier tipo de dato y/o información.
- Servicios ofrecidos.
- Aplicaciones informáticas.
- Dispositivos electrónicos.
- Elementos de red.
- Recursos Administrativos, físicos o humanos.

Según la guía CCN-STIC, una **vulnerabilidad** se considera como "**una debilidad de un activo o de un control que puede ser explotada por una o más amenazas**". Si hablamos desde el punto de vista tecnológico, un atacante puede aprovechar un fallo de seguridad con el fin de comprometer la **confidencialidad, integridad** o **disponibilidad** de un sistema. En otros contextos puede definirse como una debilidad presente en una **persona** u **objeto**.

Se entiende como **amenaza** aquella **acción o evento que puede explotar una vulnerabilidad sobre un activo concreto con el fin de dañar o perjudicar de alguna manera a una organización, agencia o empresa**.

Un riesgo puede definirse como la probabilidad de que se produzca una amenaza sobre un activo aprovechando una vulnerabilidad. Este riesgo puede suponer un daño en forma de pérdidas económicas, robo de información confidencial o daño reputacional, entre

otros. Los daños mencionados suponen el impacto resultante de explotar la propia vulnerabilidad sobre el activo por la amenaza detectada.

Para obtener el riesgo asociado a una amenaza es utilizada la ecuación del riesgo (ver Imagen 2). En esta fórmula calculamos si una amenaza en concreto tiene asociada una vulnerabilidad sobre un activo y si produce un impacto.

Imagen 2. Ecuación del riesgo

Para conocer el riesgo de una amenaza es necesario analizar la probabilidad y el impacto asociados a este. Cuanto más bajos sean sus valores menos riesgo supondrá la amenaza.

Para calcular el riesgo que supone un determinado incidente se realiza la **evaluación del riesgo**. Dicha evaluación no es más que un análisis que utiliza una serie de atributos asociados a los términos mencionados anteriormente. Estos son los siguientes:

- Identificación de Activos: La primera tarea a realizar dentro de la evaluación del riesgo. Se realiza un inventario de los activos que pertenecen a la organización, empresa o agencia. Por cada activo identificado es necesario indicar su valor y lo crítico que es para la propia organización.
- Evaluación de la Vulnerabilidad: En el momento de tener identificados los activos es necesario comprobar si existen vulnerabilidades en cada uno de ellos. Para determinar esto último, se evalúa si se disponen controles que engloben dicha vulnerabilidad. Posteriormente, se analiza el tipo de acceso y los ataques utilizados, además de los exploits asociados.
- Evaluación de amenazas: Última tarea de la evaluación, una vez identificados los activos y la evaluación de la vulnerabilidad sobre estos previamente, será necesario analizar la amenaza en función de sus características con el fin de identificar el patrón utilizado y los actores maliciosos que andan detrás del

ataque. Cada amenaza tiene asociado una probabilidad de éxito y un impacto que permiten categorizar mejor cada una de estas.

Una vez evaluados estos tres atributos dispondremos de la probabilidad y el impacto asociados a la amenaza. Los controles resultantes son estudiados para comprobar si son válidos para mitigar el riesgo. Posteriormente, se genera una clasificación de riesgo final basándose en los controles adecuados, controles inadecuados y aquellos sin controles. Existen diferentes opciones o estrategias para la mitigación de los controles inadecuados y aquellos sin controles siendo los siguientes:

- Reducir el riesgo. Consiste en reducir los valores obtenidos de probabilidad e impacto de un riesgo, dentro de unos valores que sean aceptables para la organización y no suponga ningún riesgo.
- Evitar el riesgo. No participar en ningún tipo de actividad u operación que pueda poner en riesgo la organización.
- Transferir o compartir el riesgo. El riesgo puede ser trasferido o compartido con un tercero mediante un acuerdo contractual.
- Aceptar el riesgo. Asumir el propio riesgo. Esto puede ser debido a:
    - Los valores de probabilidad e impacto están dentro de unos intervalos asumibles por la organización.
    - El esfuerzo monetario de mitigar el riesgo es mucho mayor que la pérdida asociada a este.

OSINT puede emplearse para realizar cualquier tipo de investigación siempre y cuando la información se obtenga de fuentes abiertas. En nuestro caso podemos apoyarnos en una serie de fuentes y herramientas que nos van a brindar datos relacionados con las amenazas. Algunas de las investigaciones que podríamos efectuar son:

- Investigaciones de direcciones IP y dominios maliciosos
- Investigación de correos electrónicos
- Investigaciones sobre fraude (Phishing, Spear Phishing, Pharming, Typosquatting, IDN homograph)
- Investigación de personas y perfiles sociales (Twitter, Facebook, Instagram, Telegram, etc)
- Investigación de actores y grupos criminales
- Investigaciones de operaciones de terrorismo, Hacktivismo o activismo
- Investigación de Tácticas, Técnicas y Procedimientos (TTPs)
- Investigación sobre fugas o exfiltración de información
- Investigación de empresas
- Investigaciones sobre un videos e imágenes

1.3. OTRAS DISCIPLINAS DE INTELIGENCIA

La Inteligencia basa su conocimiento en la obtención de información proveniente de fuentes de distintas disciplinas que permiten detectar y analizar diferentes amenazas presentes tanto en el plano físico como digital. Hasta ahora hemos conocido una de ellas, OSINT, siendo la piedra angular del presente manual, pero existen otros tipos de disciplinas de Inteligencia que pueden tener una vertiente relacionada con el mundo del ciberespacio, tales como, HUMINT, SOCMINT, SIGINT, IMINT o GEOINT.

Siempre que hablo de Inteligencia me gusta interpretarla desde dos vertientes: la parte cyber (ciberinteligencia) y la Inteligencia clásica. Si os paráis a pensar veréis que al final estamos hablando de lo mismo, pero dentro de un contexto bajo el paraguas del ciberespacio o sin él. En ambas vertientes estamos generando Inteligencia para satisfacer unas necesidades de información concretas utilizando para ello esas disciplinas mencionadas.

Si prestamos atención a la Imagen 3 a parte de ver algunas de las disciplinas de Inteligencia mencionadas, podemos apreciar que aparece Deep Web. Como tal no se trata de una disciplina, pero sí que podemos tomarla como una fuente de obtención importante.

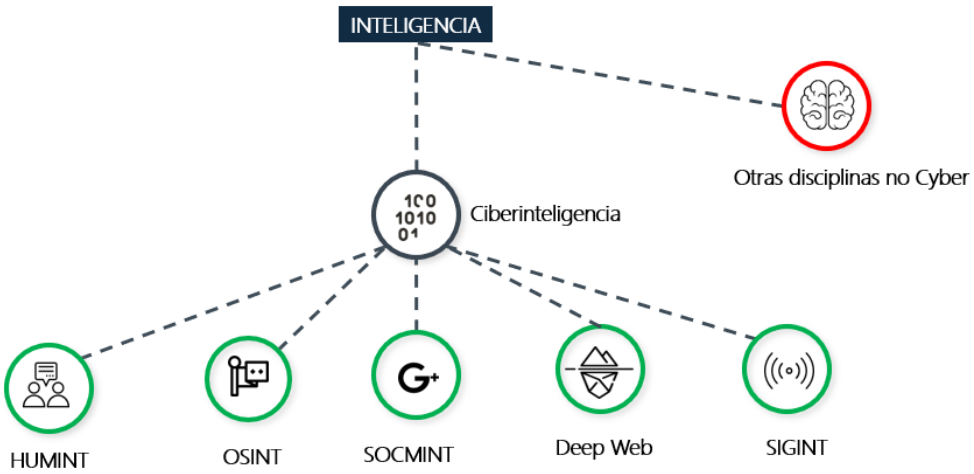

Imagen 3. Disciplinas y fuentes de inteligencia

1.3.1. SOCMINT

Esta disciplina está enfocada en generar Inteligencia a partir de datos recolectados sobre diferentes redes sociales y medios digitales. En la imagen 4 puede verse un diagrama con fuentes OSINT y multitud de redes sociales categorizadas por tipos como pueden ser redes de contenido (Reddit, Wikipedia), blogs y comunidades (Blogger, Tumblr, WordPress), redes sociales (Facebook, Badoo, Meetup, Twitter, Google +, Instagram, LinkedIn), mensajería instantánea (Skype, Telegram, WhatsApp, Jabber), video (YouTube, Dailymotion, vimeo), compartición de documentos (Dropbox, WeTransfer, Scribd, slideshare, Google Drive, One Drive), música (last.fm, Spotify, Ping, simfy, iTunes) y un largo etcétera.

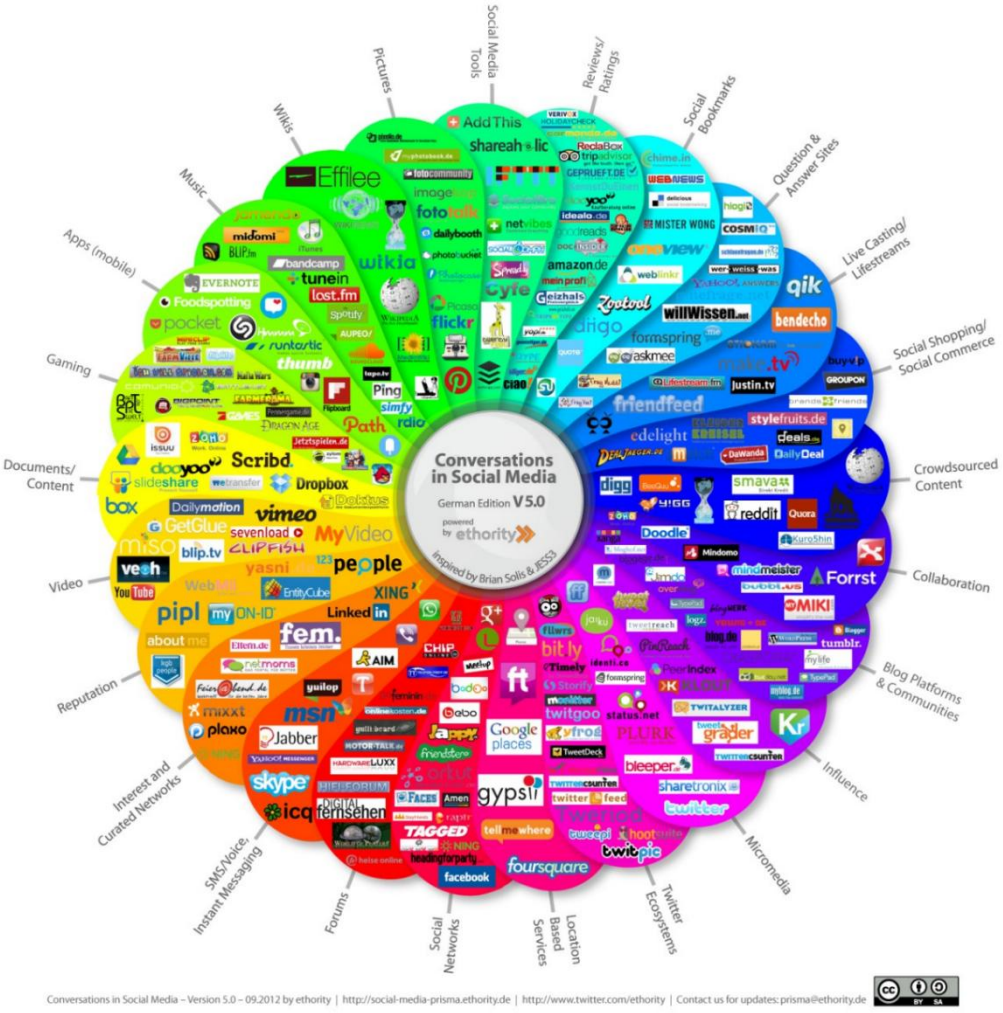

Imagen 4. Diagrama OSINT y SOCMINT

Las fuentes de los datos manejados por SOCMINT son en su mayoría fuentes públicas, por lo tanto, está muy ligado a OSINT. En algunos libros o sitios webs podéis encontrar SOCMINT dentro de OSINT, como si se tratara de una subcategoría dentro de esta.

Uno de los puntos más importantes para muchas investigaciones SOCMINT es la generación de una línea de tiempo de los sucesos. Muchas publicaciones realizadas en redes sociales tienen asociados unos metadatos, los cuales, almacenan información referente a la fecha y la hora. Gracias a esos datos es posible reconstruir un suceso concreto en orden cronológico, además de obtener los contactos directos con un perfil concreto analizado. Un artículo muy interesante que explica como

analizar los datos que circulan por las redes sociales por medio de lo que se conoce como **Análisis de Redes Sociales (ARS)** o **Social Network Analysis (SNA)** es el escrito por **José Manuel Díaz-Caneja** con el título "SOCMINT y el análisis de redes en inteligencia". En dicho artículo, José Manuel explica conceptos sobre el análisis de redes sociales, los cuales no implican que se utilicen exclusivamente para datos extraídos a través de SOCMINT, sino también permite aplicar el análisis de redes a otro tipo de datos que no tengan que ver con personas como pudieran ser dominios, direcciones IP, cuentas bancarias, etc.

1.3.2. HUMINT

Con HUMINT son utilizadas técnicas para obtener información mediante interacciones humanas, en la gran mayoría de los casos engañando a las víctimas empleando la tecnología. Hace un tiempo, comenzaron a utilizarse los términos de CyberHUMINT o VirtualHUMINT para referirse a la generación de Inteligencia usando fuentes humanas, pero en el mundo cibernético. El engaño en este caso llega a la red a través de perfiles falsos creados por los atacantes. Algunas de las redes utilizadas para tal fin son LinkedIn, Twitter y Facebook. La creación de perfiles sociales falsos ya ha ido un paso más allá, creando imágenes de personas inexistentes de manera automática para ser utilizado en los perfiles. Esto lo consiguen por medio de Redes Generativas Antagónicas (GAN) a través de la Inteligencia Artificial. Tal como indica **Javier Rodríguez** en la ponencia "Virtual HUMINT en la era de los millennials", las actividades HUMINT para captar y reclutar fuentes humanas de ataño han sido trasladadas al ciberespacio, además de que el VirtualHUMINT no facilita una relación de confianza plena ya que el vínculo humano directo se pierde, pero sí que gana en confidencialidad y anonimato.

Video 1. Ponencia de Javier Rodríguez sobre VirtualHUMINT en IntelCon

1.3.3. DEEP WEB

Deep Web no es una disciplina de Inteligencia, pero si es un tipo de fuente para tener muy en cuenta. La Inteligencia es generada a partir de datos obtenidos de servicios alojados en distintas redes de la Deep Web, como pueden ser Tor, Freenet e I2P. Tal como indica **Francisco J. Rodríguez** en la ponencia ofrecida en las XI Jornadas STIC CCN-CERT, Internet está formado por contenido indexado por los motores de los buscadores y no indexado por estos, además entra en juego también el contenido accesible para todo el mundo y el no accesible. En la imagen 5 (obtenida de la presentación de la ponencia mencionada de Fran) puede verse la diferenciación que hemos comentado anteriormente.

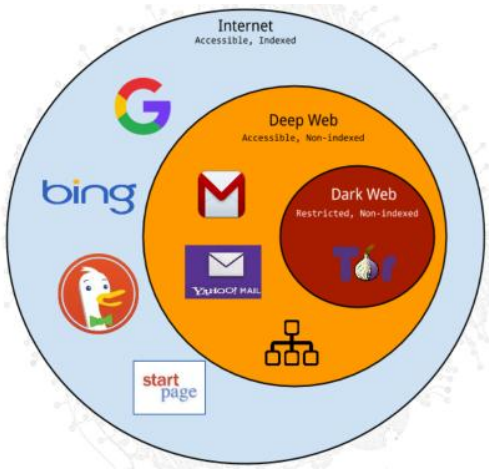

Imagen 5. Diferencia Deep Web y Dark Web

En este caso, vamos a realizar un breve resumen de los tres niveles de la web:

- **Surface Web**: Es esa parte de la web que esta indexada por los motores de búsqueda de múltiples buscadores, desde los conocidos Google o Bing como aquellos que no son tan conocidos por el usuario medio, como pueden ser Yandex, Shodan o Wayback Machine. El contenido en si es accesible por cualquier tipo de navegador web (Edge, Firefox, Google Chrome, Safari, Opera, etc).

- **Deep Web**: Es conocida también como web invisible y web oculta. Contiene información que no puede ser accedida de forma pública**.** Al final es ese contenido web que es accesible pero que no está indexado por los motores de búsqueda, ya sea porque *son páginas webs dinámicas, es una Intranet, webs con autenticación (correo web) o por algún motivo los propios crawlers que utilizan los buscadores no los han indexado.*

- **Dark Web**: Es una parte de la Deep Web que utiliza redes no comunes y más ocultas, llamadas Darknet (Tor, Freenet, I2P), las cuales necesitan un software específico para poder conectarse y acceder a su contenido por medio de clientes de esas Darknet (Tor Browser para Tor por ejemplo). La Dark Web al final es ese contenido web restringido y no indexado por los motores de búsqueda.

En muchos casos, en la gran mayoría de los servicios alojados en la Dark Web necesitan una invitación previa para poder acceder, por lo tanto, dificulta la operativa de obtener ciertos datos en determinados sitios webs. Por último, el contenido que suelen disponer los servicios de la Dark Web son volátiles estando disponibles únicamente en algunos casos minutos u horas.

1.3.4. SIGINT

Esta disciplina está enfocada en generar Inteligencia a través de datos obtenidos de fuentes mediante emisiones, comunicaciones o señales electromagnéticas. SIGINT agrupa dos formas de obtención de Inteligencia:

- Inteligencia de comunicaciones (COMINT): Genera la Inteligencia obteniendo los datos a través de la interceptación de señales de comunicaciones como pueden ser radio, teléfono, fax, transmisores, etc.
- Inteligencia electrónica (ELINT): Genera la Inteligencia recopilando datos de señales electromagnéticas no procedentes de comunicaciones, tales como, campos eléctricos (corrientes eléctricas) y campos magnéticos.

Entre las investigaciones que pueden realizarse utilizando datos obtenidos a través de fuentes SIGINT, podemos encontrarnos con las siguientes: análisis y descifrado de señales de radio, investigación sobre comunicaciones telefónicas e investigación sobre intrusiones en señales de televisión. Un gran especialista sobre esta disciplina es **David Marugán**, quien dio una ponencia hablado sobre "COVCOM – Sistemas de comunicación encubiertas. De la Grecia clásica al terrorismo yihadista" en la primera edición de la **National Cyber League de la Guardia Civil** y que gracias a Yolanda Corral lo tenemos disponible en Palabra de Hacker.

1.3.5. IMINT

IMINT es la generación de Inteligencia a partir de imágenes. Esta disciplina deriva en gran parte del mundo militar recolectando los datos sobre las imágenes a través de satélites o medios aéreos. IMINT en función del tipo de fuente donde sea obtenida la imagen será de un tipo de Inteligencia u otro. Estos son los siguientes:

- OPTIN. Es la Inteligencia óptica centrada únicamente en la región visible del espectro.
- PHOTINT. Es la Inteligencia obtenida a partir de fotografías, ya sea de cámaras usadas por civiles u obtenidas de satélites. La fuente utilizada en este tipo de Inteligencia es la que mejor se adapta a las investigaciones sobre imágenes en el mundo empresarial.
- EOPINT. Es la Inteligencia electro-óptica generada a partir de propiedades ópticas manipulables por medio de un campo eléctrico, laser, cables de fibra óptica o televisores.
- IRINT. Es la Inteligencia generada a partir de infrarrojos.

Las aplicaciones que tiene este tipo de disciplina son las siguientes:

- Apoyo en operaciones militares y servicios de defensa
- Integración y apoyo con otros tipos de disciplinas de Inteligencia
- Aplicaciones civiles, como pudieran ser análisis de imágenes relacionadas con campañas de desinformación en las que se usen imágenes, manipulación de evidencias en forma de imágenes o incluso en la identificación de logos o imágenes corporativas falsificadas.

1.3.6. GEOINT

La Inteligencia geoespacial está enfocada en recopilar datos de imágenes de satélites, localización GPS de vehículos de tierra, aire o mar, o cualquier otro tipo de

geoposicionamiento terrestre y/o aéreo, con el fin de analizar qué actividades pueden suponer una amenaza física en un futuro inminente y poder defenderse de estas. GEOINT está muy relacionada con la disciplina IMINT debido a la explotación y análisis de imágenes.

Según indicó **Fernando Dávara** en las XIV Jornadas UPM – FAS del año 2010, esta disciplina ayuda a generar la Inteligencia geoespacial en el tiempo adecuado como apoyo en la toma de decisiones, planeamiento y utilización en operaciones.

Una aplicación real mezclando las disciplinas SOCMINT y GEOINT es la que comenta **Braian Arroyo** en su artículo "GEOINT y SOCMINT en la Investigación**"**. En dicho artículo, Braian indica que GEOINT puede ayudar a monitorizar eventos o zonas y realizar así un seguimiento en tiempo real sobre las publicaciones relacionadas que tienen lugar en redes sociales, con el objetivo de recopilar datos que en su conjunto puedan ayudar a detectar posibles amenazas antes de que tengan lugar.

1.4. NIVELES DE INTELIGENCIA

Los niveles de Inteligencia derivan del mundo militar y hacen referencia al ámbito de actuación, y sobre todo, el objetivo relacionado con una necesidad concreta que desea cubrir el decisor dentro de ese nivel. Dichos niveles son el **estratégico**, **táctico** y **operacional**.

Cada vez es más común ver en el mundo empresarial distintos productos adaptados a diferentes niveles de Inteligencia. Esto radica en los distintos tipos de perfiles que pueden necesitar consumir la Inteligencia, desde un CEO de una compañía a un analista de Threat Hunting.

Hoy en día es muy importante ajustar el mensaje al interlocutor adecuado, ya que por muy buen producto que se haga, si el decisor que espera recibir la Inteligencia no entiende el mensaje debido a que está enfocado a un perfil más técnico en vez de un

perfil ejecutivo (en el caso de que sea un CEO o CISO) pues la Inteligencia no servirá de nada y no cubrirá las necesidades reales.

1.4.1. NIVEL ESTRATÉGICO

La Inteligencia va dirigida a directivos, altos cargos y/o responsables de la toma de decisiones definidas a largo plazo y a alto nivel. La Inteligencia estratégica enfocada en el análisis de amenazas puede ayudar a generar una visión global sobre los patrones de ataque, tendencias y riesgos emergentes asociadas a las propias amenazas y satisfacer las necesidades de los altos cargos directivos de la compañía o proporcionar indicadores que puedan predecir sucesos futuros, identificar nuevas tecnologías y como su nombre bien indica, definir una estrategia frente a dicha amenaza.

1.4.2. NIVEL TÁCTICO

En este nivel están muy presentes las Tácticas, Técnicas y Procedimientos (TTPs). La Inteligencia está enfocada para ser consumida por directores y/o equipos destinados a entender al adversario generando ideas para hacer frente a las amenazas, además de asegurar que sus sistemas defensivos estén preparados para las tácticas actuales. La información que se investiga está relacionada con el modus operandi de diferentes actores y amenazas sin olvidarnos de las motivaciones e intenciones del atacante.

Un ejemplo de producto táctico sería un estudio de los principales TTPs que utilicen los actores que tengan como objetivo un sector en particular y desarrollar un plan de acción para protegernos de manera proactiva sobre los posibles ataques adheridos al modus operandi de las diferentes amenazas asociadas.

1.4.3. NIVEL OPERATIVO

El nivel operativo proporciona una Inteligencia altamente especializada y técnicamente enfocada en guiar y ayudar a dar respuesta frente a las amenazas. Una de las tareas más

importante de este nivel es la planificación de todas las operaciones en curso donde su principal objetivo es dar respuesta a las necesidades de la empresa para defenderse frente a las amenazas, tanto futuras como presentes.

La mayoría de las veces esta Inteligencia es consumida automáticamente mediante herramientas, permitiendo monitorizar todas las amenazas que interactúen con los sistemas de la organización o recopiladas desde fuentes externas. La Inteligencia a este nivel generalmente alimenta las funciones de investigación o supervisión de las amenazas sufridas en una empresa y generalmente dirigida a los analistas más técnicos relacionados por ejemplo con respuesta a incidentes, análisis de malware, Threat Hunting, etc.

1.5. EL MÉTODO: EL CICLO DE INTELIGENCIA

Según se define en el **Diccionario LID de Inteligencia y Seguridad**, el Ciclo de Inteligencia es "*un proceso de generación y comunicación de conocimiento nuevo, veraz y ajustado a las necesidades y los requerimientos de un usuario a partir de la obtención y la transformación de información apropiada. Secuencia de actividades mediante las que se obtiene información que se convierte en conocimiento (inteligencia) que se pone a disposición de un usuario*".

Además, dicho proceso está inmerso dentro de la propia producción de Inteligencia que deriva en una gestión del conocimiento de la investigación de un hecho o suceso concreto. El Ciclo de Inteligencia sigue de manera lineal una serie de fases relacionadas entre sí con el fin de obtener una producción de Inteligencia.

Es importante destacar que existen distintas aproximaciones del Ciclo de Inteligencia siendo las siguientes:

- La **Agencia Central de Inteligencia (CIA)** de los Estados Unidos presenta un Ciclo de Inteligencia basado en 5 fases: *Planificación y dirección, Recolección, Procesamiento, Análisis y producción y Difusión*.

Imagen 6. Ciclo de Inteligencia de la CIA

- Dentro del contexto de la **Organización del Tratado del Atlántico Norte (OTAN)**, el Ciclo de Inteligencia militar está formado por 4 fases, las cuales están implantadas en el **Centro Nacional de Inteligencia** (CNI), siendo las siguientes: Dirección, Obtención, Elaboración y Difusión.

Imagen 7. Ciclo de Inteligencia del CNI

La única diferencia que podemos observar entre los dos modelos es la unión de las fases de Procesamiento, Análisis y Producción del modelo utilizado por la CIA dentro del modelo seguido por el CNI, lo que puede generar una cohesión mayor entre el procesamiento de la información y su posterior análisis al encontrarse en la misma fase. De este modo, el Ciclo de Inteligencia es el mismo en los dos casos, pero varía la gestión interna que se hace de tal proceso, así como la designación de distintas funciones en cada una de las fases.

En este caso podemos adaptar el Ciclo de Inteligencia utilizado por el CNI utilizando la misma dinámica operativa entre las fases pero bajo el contexto de investigación de amenazas empleando las fuentes abiertas. A continuación se procede a describir cada una de las fases del ciclo mencionado.

1.5.1. DIRECCIÓN

Esta primera fase está enfocada en determinar las Necesidades de Información, la preparación de un plan para su obtención y la organización de los medios pertinentes, tomándose como muy relevantes las denominadas funciones directivas, siendo estas: **planificación, organización, motivación, mando, coordinación y control**. Esta fase está ligada a tareas directivas encargadas de la planificación de los requerimientos necesarios fijados como objetivos, el alcance, la organización y la coordinación de los recursos entre los diferentes interlocutores.

1.5.2. OBTENCIÓN

En la generación de cualquier producto de Inteligencia recibiremos en esta fase las órdenes de adquisición necesarias, junto con los requerimientos y objetivos a seguir. En el mundo militar suelen utilizarse las siguientes propuestas establecidas en la fase anterior: órdenes de adquisición HUMINT (OAH) y órdenes de adquisición técnica (OAT)

Los órganos de obtención centrarán la búsqueda de información basándose en las órdenes y prioridades que estén reflejadas en ambas propuestas. Los analistas de

Inteligencia son los encargados de realizar las tareas de recopilación de los datos presentes en cada una de las disciplinas de Inteligencia que estén en el alcance de la generación del producto de Inteligencia. Un producto OSINT enfocado en el estudio de amenazas puede recopilar datos a partir de las fuentes relacionadas a las disciplinas de Inteligencia vistas anteriormente.

Esta fase es la encargada de recopilar todos los datos posibles de los diferentes órganos de obtención necesarios para cumplir con los requisitos establecidos en la fase anterior. Todos los datos recolectados son normalizados y tratados, con el fin de conseguir información entendible para los analistas de la siguiente fase. Los datos pueden ser recopilados a través de las siguientes vías de obtención:

- Externamente: Los datos son obtenidos desde fuera de la compañía usando diversas fuentes externas. Algunos ejemplos:
    - Monitorizar fuentes de datos sobre amenazas.
    - Uso y utilización de herramientas que consulten los datos en proveedores externos.
    - Investigar información compartida de amenazas por medio de la comunidad de Inteligencia o por otras empresas.
    - Casos de uso sobre incidentes de seguridad.

- Internamente: Los datos son obtenidos desde dentro de la compañía a través de plataformas integradas en la infraestructura corporativa. Algunos ejemplos:
    - Datos de incidentes y eventos empresariales.
    - Brechas y vulnerabilidades sufridas.
    - Datos de activos críticos.
    - Datos obtenidos mediante el SIEM y sistemas defensivos.
    - Datos obtenidos de herramientas anti-malware integrados en la infraestructura.

1.5.3. ELABORACIÓN

En esta tercera fase es transformada toda la información recopilada de la fase anterior en Inteligencia. El analista analiza cada dato en sí y lo interpreta dentro del contexto de la amenaza, teniendo siempre presente los requerimientos definidos. Dentro de la elaboración de la Inteligencia es necesario categorizar toda la información obtenida con el fin de identificar cual dispone de valor.

Para identificar la información de valor mencionada podemos plantearnos las siguientes preguntas:

- ¿Cuál es el objetivo de la propia amenaza?
- ¿Qué TTPs utiliza?
- ¿Qué vectores de ataque utiliza?
- ¿Disponemos de un Árbol de ataque para aprender cómo se comporta la amenaza?
- ¿Disponemos de un modelado de amenazas con información sobre escenarios de alto riesgo o brechas de seguridad?
- ¿Qué grupo criminal o actor está detrás del incidente?
- ¿Puede tener un gran impacto en la empresa?¿Supone un riesgo?
- ¿Sabemos cómo contrarrestar la amenaza? ¿Disponemos de contramedidas?

En el momento que podamos responder a la gran mayoría de las preguntas formuladas, significará que hemos realizado un análisis que ayude a contrarrestar la amenaza. El análisis efectivo de las amenazas permite disponer de un conocimiento que pueda ser consumido en otros escenarios similares, por ello es muy importante tener un repositorio común de amenazas donde analizar las relaciones existentes entre los diferentes artefactos utilizados por cada uno de estos con el fin de detectar patrones que ayuden a resolverlo en el menor tiempo posible.

Esta fase genera el producto de Inteligencia necesario para ayudar a tomar las mejores decisiones en relación con una determinada amenaza.

1.5.4. DIFUSIÓN

La última fase es la encargada de distribuir el producto de Inteligencia a las autoridades de gobierno o destinatarios que necesiten recibir respuestas a sus requerimientos por el medio apropiado. El éxito de esta fase dependerá de la entrega al destinatario idóneo. La difusión es una parte muy importante del ciclo, ya que una mala gestión de las tareas asociadas por el medio incorrecto o una entrega del producto en un tiempo fuera de plazo no ayudará a protegerse de la propia amenaza.

En el caso de que el consumidor de la Inteligencia necesite nuevas variables para tomar una decisión, es posible utilizar toda la información disponible en ese punto y retroalimentarla con una nueva estrategia comenzando de nuevo con la primera fase del Ciclo de Inteligencia.