ACERCA DEL AUTOR

Mario Guerra Soto es Ingeniero de Telecomunicación por la UC. Actualmente trabaja como *Blue Team Architect* en la empresa de ciberseguridad Halborn. Anteriormente trabajó como *Security Delivery Manager* de los servicios de CTI, *Threat Hunting* y *Purple Teaming* para una empresa española del sector Recursos. Durante siete años sirvió en el Mando Conjunto de Ciberdefensa desempeñando funciones de DFIR, *threat hunter*, analista CTI a nivel técnico/táctico, y analista de *malware*. Es Máster en Seguridad de Tecnologías de Información y Comunicación por la UOC, y Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen por la UAM. Es Diplomado en Inteligencia y Seguridad por la Escuela de Guerra del Ejército de Tierra de España. Dispone de las certificaciones en ciberseguridad GCFA, GCTI, GREM, CEH, CHFI, CND, CCPA, CASA y KAPE. Además, ha realizado otros cursos relacionados con la ciberseguridad, como el de Cyber Security Professional por la NATO School of Oberammergau, y el Curso de Especialidades Criptológicas por el CCN. Ha colaborado como ponente en diferentes CON nacionales como RootedCON, Cybercamp, C1b3rwall, IntelCon, Common Secure, Hackron y TACS. Ha colaborado como docente en los programas de postgrado de la UAM, de la USAL y de la VIU. Ha colaborado como docente en los programas de formación profesional de Universae. Es autor de otros tres libros en esta editorial.

PRÓLOGO

Escribir libros es una tarea muy complicada.

Además, el síndrome del folio en blanco existe; a veces es duro escribir la primera letra, la primera palabra y, sobre todo, el primer párrafo. Cuando superas esa barrera, todo empieza a fluir y es ahí, en ese momento, donde empieza a ser muy complicado.

No es el primer libro que escribe. Ni el segundo. Esto ya debería estar superado, Mario, ¡por favor! (nunca se supera; empezar un libro casi siempre tiene el mismo proceso).

Es complicado, no tanto por el contenido técnico en sí mismo —en el caso de Mario es algo que tiene superado—, sino por las múltiples decisiones que hay que tomar en la construcción de la arquitectura del texto. Decisiones sobre qué temas vas a dejar fuera (cuando todo te parece relevante) o cómo vas a expresar determinadas cosas. Decisiones sobre cómo enfocar laboratorios. ¿Cuál es el público objetivo de este texto? ¿Debo redactar con estilo reflexivo (como haría un consultor)? ¿Un tono más cercano y coloquial?

Cuando una temática arrastra adicionalmente la complejidad técnica, tienes que dar por supuesto que cada individuo va a aproximarse a tu libro de forma diferente. Y, sobre todo, tienes que asumir que escribas como escribas habrá lectores a los que les encantará y lectores que lo criticarán.

Porque es inevitable.

Antes he comentado que Mario tiene superado todo el tema técnico. Y es verdad. Una persona con un perfil tan completo, con tantos años de operaciones en el "fondo de armario", no solamente nos va a hablar de detalles académicos o teóricos, que son relevantes, sino también de las cosas que pasan en los mundos reales.

Y uso intencionadamente "mundos reales".

No es lo mismo aplicar las técnicas de inteligencia clásica en un entorno de operaciones militares, que en un entorno de gran empresa en el sector privado. Como no es lo mismo evaluar las amenazas de una organización cuando tu Adversario es un estado, un país. Ni son los mismos destinarios los que van a recibir tu inteligencia y tu inteligencia de amenazas.

Mario ha vivido, intensamente, en casi todos los mundos profesionales donde el CTI es una herramienta crítica: perfil militar, perfil de sector privado con rol de cliente y, naturalmente, perfil de sector privado con perspectiva de consultor.

En general, no hay perfiles como el que tiene el autor. Esta combinación de visiones es esencial para poder evaluar los datos, contrastarlos con fuentes adicionales y refinarlos convirtiéndolos en informaciones (una persona que no haya tenido experiencia militar es probable que no identifique un dato como coordenadas polares). Por otro lado, una persona que no haya tenido la experiencia del sector privado es posible que no reconozca datos financieros o de procesos internos de las empresas.

Y todo esto junto, aunque lo encontráramos en un profesional, podría no ser suficiente para poder escribir un libro útil y de calidad.

Porque, además, Mario tiene una cualidad adicional que es extremadamente necesaria: se relaciona con otros profesionales aportando, construyendo Comunidad, colaborando en la mejora del conocimiento de todos.

Ser una eminencia —y Mario lo es indiscutiblemente— no es suficiente cuando hablamos de Ciberamenaza o de CTI. También es necesario compartir información con otras personas del sector. Y saber cuándo respetar un secreto que nos han compartido TLP:RED. Y saber gestionar las situaciones de crisis de otros que necesitan nuestra ayuda. Y aportar. Y aportar. Y APORTAR.

No voy a entrar en que además es buen cocinero, porque sería el punto donde se me empezaría a notar la envidia malsana por una persona completa como profesional y, sobre todo, como humano.

Gracias por este libro. Gracias por todas esas cosas que hemos compartido en distintos momentos, con mayor y menor intensidad, Mario.

Román Ramírez Giménez ha desarrollado diferentes posiciones en sus más de treinta años de carrera profesional. Comenzó como programador de aplicaciones para Banca y, posteriormente, como responsable de sistemas y seguridad en Intercomputer/encomIX. Pasó a ser el responsable de preventa y CTO para el sur de Europa en eEye Digital Security (actualmente, Beyond Trust).

Tras unos años como Gerente de Riesgo IT en PricewaterhouseCoopers, finalmente, completó diez años en el puesto de Gerente de Operaciones y Arquitectura de Ciberseguridad en Ferrovial.

Colabora con fundaciones como Fundación Princesa de Girona, Fundación Goodjob o Charlas Digitales, y es docente en diferentes clases y másteres, destacando el master de Ciberseguridad en el Instituto de Empresa (IE), en la escuela HST.

Ha lanzado algunos proyectos propios como fundador y CEO, tales como Chase The Sun o BE Real Talent. También es uno de los fundadores de propaganda · is y RootedCON.

Mario Guerra es Ingeniero de Telecomunicación de formación y marino de vocación. Durante su trayectoria profesional ha servido en el MCCE como analista forense digital, analista de *malware* y *threat hunter*, enfrentándose a todo tipo de ciberamenazas. Su experiencia profesional le ha permitido atesorar un sinfín de conocimientos teóricos, pero sobre todo y fundamentalmente, prácticos.

En este libro, Mario nos ofrece toda esta sabiduría acumulada, de forma estructurada, sencilla y profesional. Con esta obra, el autor otorga al lector la oportunidad de entender la inteligencia de amenazas. Un universo realmente complejo y de gran valor para las organizaciones.

Cualquier empresa u organismo ansía conseguir la capacidad para adelantarse a las amenazas que le acechan. Este desafío actualmente solo puede abordarse desde la inteligencia de amenazas. El texto nos plantea de manera profunda cuales son los conceptos y procedimientos que permiten operacionalizar este proceso en el ciberespacio. Abarca desde la definición de la amenaza hasta la comunicación de la información de interés a todos los estamentos interesados en cualquier organización. Cómo obtener la información, cómo analizarla y cómo conseguir que tenga un impacto real en la postura defensiva de una organización son parte de los temas que toca esta obra y que seguro que serán de gran interés para el lector ya sea este iniciado o nobel en la materia.

Enrique Castañeda de Benito es Ingeniero en Informática de Gestión. Actualmente se encuentra destinado como jefe del Grupo de Explotación de la FOCE del MCCE. Es Diplomado en Informática Militar y Máster en Sistemas de Información para la Defensa por la URJC, y Máster en Ciberseguridad por la UC3M. Dispone de las certificaciones de ciberseguridad GCTI y GCIH. Ha colaborado como docente en el Operational Cyber Threat Intelligence Course impartido por el CCDCOE.

1

CIBERINTELIGENCIA DE LA AMENAZA

1.1 INTELIGENCIA CLÁSICA

1.1.1 Definición de inteligencia y contrainteligencia

En su *paper* "*A new Definition of Intelligence*", Allan Breakspear definió la inteligencia como la capacidad de una organización de prever el cambio con la suficiente antelación como para tomar acción sobre él. Esta capacidad implica disponer de previsión y conocimiento para identificar los cambios inminentes, ya sean positivos, y que supongan una oportunidad, o negativos, y que representen una amenaza.

Tradicionalmente, la generación y el consumo de inteligencia se limitaba a los gobiernos. Las necesidades de conocimiento se centraban en las capacidades y actividades de otros gobiernos, generalmente adversarios, y el producto de inteligencia generado era utilizado por el estamento político-militar para la toma de decisiones. Actualmente, la inteligencia es necesaria también en otras áreas más allá de las gubernamentales y militares, resultando vital el conocimiento de los potenciales adversarios y sus actividades.

La CIA (*Central Intelligence Agency*) define inteligencia como el "conocimiento y el conocimiento a priori del mundo que nos rodea, siendo el preludio de la decisión y la acción de los políticos americanos". Vernon Walters, director adjunto de la CIA en el periodo (1972-76), definió la inteligencia como "aquella información, no siempre de dominio público, relativa a la fortaleza, recursos, capacidades e intenciones de un país extranjero que pueda afectar a las vidas y la seguridad" de los estadounidenses.

Según Donald Rumsfeld, exsecretario de Defensa de los EE.UU. durante los mandatos de los presidentes Gerald Ford y George W. Bush, existen tres fases en la obtención de inteligencia:

- *"Desconocidos desconocidos"* (*unknown unknowns*), aquellas cosas que no se sabe que existen, ni cómo son.
- *"Desconocidos conocidos"* (*known unknowns*), es decir, aquellas cosas que se sabe que existen, pero no se sabe exactamente cómo son.
- *"Conocidos conocidos"* (*known knowns*), es decir, las cosas que se sabe fehacientemente que existen y cómo son.

Por otro lado, se entiende como contrainteligencia la identificación, valoración y neutralización de las actividades de inteligencia del adversario. Por tanto, las operaciones en contrainteligencia se centrarán en las actividades de inteligencia y desinformación llevadas a cabo por los adversarios.

1.1.2 Tipos de inteligencia

Tradicionalmente, el tipo de inteligencia se ha asociado con las fuentes a partir de las cuales se genera la inteligencia. Estas fuentes pueden ser procesadas empleando tanto medios técnicos como humanos. Se consideran como básicas los siguientes tipos de inteligencia o disciplinas de recolección de datos:

- SIGINT (*Signal Intelligence*). Recopilación de datos procedentes de la interceptación de señales (Ej. Comunicaciones radio, telefonía celular). Es el resultado de combinar COMINT (*Communications Intelligence*), ELINT (*Electronic Intelligence*) y FISINT (*Foreign Instrumentation Signals Intelligence*).
- IMINT (*Imagery Intelligence*). Incluye la representación de objetos reproducidos electrónicamente o mediante medios ópticos en papel fotográfico, dispositivos electrónicos o cualquier otro soporte. Las imágenes pueden proceder de fotografías, sensores radar y dispositivos optrónicos.
- MASINT (*Measurement and Signature Intelligence*). Inteligencia obtenida del análisis cuantitativo y cualitativo de atributos físicos de los objetivos y eventos que permite identificarlos, caracterizarlos y localizarlos. La información procede de mediciones y firmas de objetivos (Ej. Firmas radar de buques de superficie, firmas sónar de vehículos submarinos, firmas infrarrojas de aeronaves, firmas de explosiones nucleares).
- HUMINT (*Human Intelligence*). Recolección de información mediante la interacción humana. Suele interpretarse que se limita a actividades de espionaje clandestinas, si bien también incluye la recopilación de información de agregados militares e informes estratégicos. Se considera la más antigua de las seis disciplinas y, hasta mediados del siglo XX, era la principal fuente de inteligencia. En su expresión más sencilla, requiere de la interacción de dos personas, el operador y la fuente.
- OSINT (*Open-Source Intelligence*). Recolección de datos e información de fuentes abiertas (Ej. Bibliotecas, registros públicos, prensa, Internet).

- GEOINT (*Geospatial Intelligence*). Análisis y representación visual de actividades relacionadas con la seguridad en La Tierra. Es el resultado de integrar imágenes, inteligencia de imágenes e información geoespacial (Ej. Imagen satelital).

Actualmente, existen otros tipos de inteligencia de gran utilidad:

- FININT (Financial Intelligence). Recopilación de información relativa a las finanzas de un objetivo, para comprender su naturaleza y capacidades, y predecir sus intenciones.
- CRIMINT (*Criminal Intelligence*). Recopilación de información orientada a anticipar, prevenir o monitorizar actividades criminales.
- Todas las fuentes. Recopilación de datos de cualquier tipo de fuente disponible relativa a un tema determinado.

1.1.3 Ciclo de Inteligencia

La publicación de la OTAN AJP-2 "*Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*" define necesidad de inteligencia (*intelligence requirement*) como aquella información que permite rellenar una carencia existente en el conocimiento del mando o en la comprensión de este del entorno operacional de la amenaza. Expresado de manera más sencilla, sería aquella carencia de conocimiento que debe ser satisfecha para permitir a la dirección la toma de una acción. Las necesidades de inteligencia deben definirse de manera sencilla y permitir resolver una única decisión.

El *Ciclo de Inteligencia* (*Intelligence cycle* o *Intelligence Process*) permite describir el modo en el que se procesa idealmente la inteligencia en agencias civiles, policiales y militares. Básicamente, el *Ciclo* consiste en un circuito cerrado de nodos conectados en serie entre sí, generándose en el último nodo de cada iteración el producto de inteligencia. El número de nodos o fases necesarias dependerá del modelo empleado. Como se trata de un proceso circular, el resultado global del proceso no podrá ser mejor que el nodo más débil del proceso.

Así, la publicación de la OTAN AJP-2 "*Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*" establece un modelo de cinco fases para el *Ciclo de Inteligencia*:

1. Planificación y dirección (*Planning and direction*). Durante esta fase se identifican y priorizan las necesidades de inteligencia, se desarrollan los métodos que permiten su obtención y se asignan los recursos técnicos, materiales y humanos necesarios.
2. Recolección (*Collection*). Se recopilan los datos necesarios para cumplir con las necesidades de inteligencia definidos durante la fase anterior.
3. Procesado y explotación (*Processing and Exploitation*). Preparación necesaria para procesar los datos recopilados y convertirlos en información. Se llevarán a cabo tareas como filtrado de datos, de duplicación de datos, transformación de formato de datos, enriquecimiento de datos, extracción de indicadores clave, etc.
4. Análisis y producción (*Analysis and Production*). Empleo de técnicas analíticas (Ej. Técnicas de análisis estructurado) para evaluar la información procesada y responder

a las necesidades de inteligencia establecidos durante la fase de Planificación y dirección. El análisis de la información proporcionará un juicio analítico, el cual será transformado en un formato consumible por la audiencia objetivo.

5. Difusión e integración (*Dissemination and Integration*). El producto de inteligencia es remitido a la audiencia objetivo con la intención de satisfacer las necesidades de inteligencia establecidos. En ocasiones, la inteligencia proporcionada generará nuevas necesidades de inteligencia, motivando un nuevo planeamiento de recolección de datos.

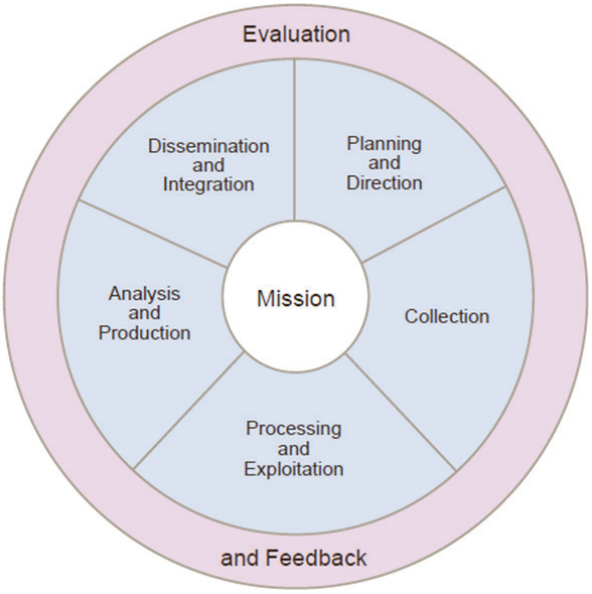

Ilustración 1. Ciclo de Inteligencia conforme al Modelo de la AJP 2.0. Fuente: AJP 2.0.

Otros modelos, como el de Lowenthal, dividen para mayor claridad el *Ciclo* en siete fases: requisitos, recolección, procesado y explotación, análisis y producción, difusión, consumo (*consumption*) y retroalimentación (*feedback*). Este *feedback* hace referencia al diálogo que debe existir entre los productores y los consumidores de inteligencia. El analista necesita conocer si se están satisfaciendo correctamente las necesidades de inteligencia, para realizar los ajustes oportunos si estos fuesen necesarios. Además, permitirá determinar si es necesario llevar a cabo un nuevo ciclo de recolección y análisis de datos.

En ocasiones, para completar adecuadamente una de las fases del *Ciclo de Inteligencia* el analista de una de las fases realizará una petición de información (RFI, *Request For Information*) adicional a otro analista de una fase anterior. Esta solicitud puede deberse a falta de conocimiento de una materia concreta por parte del peticionario, una aclaración de los datos procesados o la solicitud de recolección de datos adicionales.

1.1.4 Ciclo F3EAD

El *Ciclo F3EAD* (*Find*, *Fix*, *Finish*, *Exploit*, *Analyze*, *and Disseminate*) es una alternativa al *Ciclo de Inteligencia*. Este Ciclo es utilizado por las Fuerzas Armadas de diferentes países occidentales, especialmente en el contexto de operaciones que conllevan una acción letal (Ej. Ataques con drones, operaciones especiales).

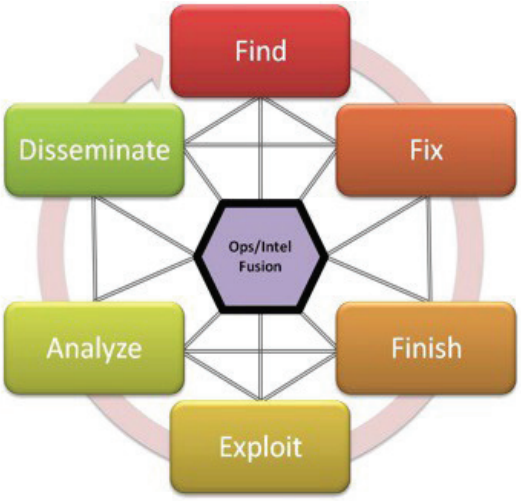

Ilustración 2. Esquema del ciclo F3EAD.

El *Ciclo F3EAD* permite combinar el *Ciclo de Operaciones* con el *Ciclo de Inteligencia*, de modo que ambos se alimenten entre sí.

Básicamente, el *Ciclo F3EAD* puede resumirse del siguiente modo:

1. Encontrar (*Find*). La primera fase comienza con la identificación de un posible objetivo, proceso conocido militarmente como *targeting*. Para ello, pueden utilizarse las 5W (*Who*, *What*, *When*, *Where*, *Why*).
2. Fijar (*Fix*). Verificación del objetivo identificado en la fase *Find*, lo que normalmente implica disponer de diferentes puntos de referencia poder para fijar su ubicación. En esta fase se transforma la inteligencia de la fase *Find* en inteligencia operacional utilizable como base para la acción en la fase *Finish*.
3. Finalizar (*Finish*). A partir de las evidencias generadas en las fases *Find* y *Fix*, el jefe de la operación puede ejecutar la acción sobre el objetivo.
4. Explotar (*Exploit*). Deconstrucción de las evidencias generadas en la fase *Finish*.
5. Analizar (*Analyze*). Fusionar las evidencias de la fase *Exploit* con la visión proporcionada por toda la inteligencia operacional disponible.
6. Difundir (*Disseminate*). Publicación y difusión de los resultados de la investigación a los destinatarios pertinentes.

El *Ciclo F3EAD* tiene un enfoque a un nivel más táctico que el *Ciclo de Inteligencia*, cuyo enfoque es a un nivel más estratégico. Por tanto, ambos modelos pueden ser implementados dentro de la misma organización, empleándose el *Ciclo de Inteligencia* para la toma de decisiones a nivel estratégico y el *Ciclo F3EAD* a nivel táctico durante la conducción de operaciones. Ambos ciclos dentro de la organización deberán estar interrelacionados para apoyarse mutuamente.

1.2 DATO, INFORMACIÓN E INTELIGENCIA

Con frecuencia, los profesionales de ciberseguridad utilizan indistintamente los términos dato (*data*), información (*information*) e inteligencia (*intelligence*). No obstante, existe una diferencia notoria entre ellos que debe ser tenida en cuenta.

1.2.1 Dato

El término dato hace referencia a hechos concretos y estadísticas recopiladas para su posterior análisis. Los datos definen un objeto o individuo, carecen de contexto y no han sido previamente procesados. En general, una organización dispondrá de cantidades ingentes de datos (Ej. Los detalles de peticiones de conexión de un determinado servicio web desde el dispositivo de un determinado usuario), pero solo algunos tendrán relevancia para la generación de un producto de inteligencia.

Dentro del contexto de la ciberseguridad, los datos son indicadores como direcciones IP, URL o valores resumen (*hashes*). Los datos pueden clasificarse como estructurados (*structured data*) (Ej. Números, texto) o no estructurados (*unstructured data*) (Ej. Imágenes, vídeo, audio). Si los datos no son sometidos a análisis, no proporcionarán valor al equipo de seguridad.

1.2.2 Información

El término información es el utilizado para hacer referencia a un conjunto de datos procesados que, combinados entre sí, permiten responder una pregunta sencilla (Ej. Diferentes dispositivos de diferentes usuarios de la red de la organización realizan múltiples solicitudes de conexión al mismo servicio web en un breve intervalo de tiempo). La información es la salida de datos procesados que contienen significado y contexto. Por tanto, puede considerarse la información como el conocimiento generado cuando un conjunto de datos que proporcionan diferentes hechos relativos a un suceso son combinados o interconectados entre sí para proporcionar una visión de conjunto sobre dicho suceso o contestar a una pregunta sencilla.

Desde el punto de vista de la ciberseguridad, la información permite contestar preguntas sencillas, como el número de veces que una organización ha sido mencionada en una determinada red social. Pese a que la información resulta más útil que los datos "en crudo" (*raw*), esta necesitará ser analizada para proporcionar valor al equipo de seguridad.

1.2.3 Inteligencia

La inteligencia consiste en entender los hechos a partir de la correlación de datos e información procedente de diferentes fuentes, descubriendo patrones que faciliten su comprensión. La inteligencia permite la toma de decisiones fundadas y la adopción de medidas efectivas en la prevención de intrusiones, remediación de vulnerabilidades, reduciendo el riesgo y mejorando la postura de ciberseguridad de la organización.

La inteligencia implica hilar las hipótesis formuladas a partir de los datos y las respuestas obtenidas de la información disponible, confeccionando un producto que permita responder preguntas complejas y colaborar de este modo en el proceso de toma de decisión de la organización (Ej. Las peticiones al servicio web desde algunos dispositivos de la red corporativa se realizan desde cada dispositivo en intervalos de milisegundos, lo que no coincide con un patrón de utilización de un usuario humano). Es decir, la inteligencia se obtiene mediante el procesado de datos y el análisis de la información disponible sobre un suceso. Por tanto, se trata de información interpretada, y proporciona un conocimiento más profundo del sujeto (organización, individuo u objeto) sobre el que fundamentar la toma de decisiones y de acciones de respuesta.

El objetivo de la inteligencia debe ser facilitar a las organizaciones la interpretación de la información disponible para convertirla en conclusiones o acciones prácticas, permitiendo de este modo la resolución de problemas complejos. En la salida de las sucesivas fases del proceso de elaboración de inteligencia a partir de los datos y la información disponibles se producirá una reducción del volumen y un incremento del valor para la organización.

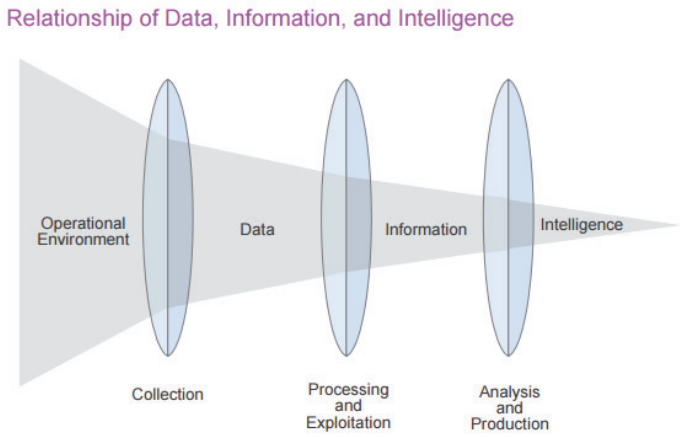

Ilustración 3. Relación entre dato, información e inteligencia, conforme a la "Joint Publication 2-0: Joint Intelligence" del DoD de EE.UU.

EC-Council define la inteligencia como "el proceso que utiliza la información disponible para analizar y responder las necesidades de conocimiento de una organización". Durante este proceso, la inteligencia convierte el qué (*What*) y el cómo (*How*) de la información en el por qué (*Why*) y el cuándo (*When*) del proceso de resolución del problema.

De estas definiciones anteriores se desprende que tanto los datos "en crudo" como la información sin procesar no constituyen por sí mismos inteligencia. Del mismo modo, los datos y la información analizada solo serán considerados inteligencia si el resultado es directamente aplicable (*actionable*) a los objetivos de negocio de la organización. Es decir, la inteligencia debe:

- Facilitar la toma de decisiones o la ejecución de acciones específicas.
- Estar confeccionada a la medida de la persona, grupo o sistema que consumirá esa inteligencia para habilitar la toma de decisiones o ejecutar una acción específica.

Desde el punto de vista del destinatario del producto de inteligencia, aquellos *feeds* que no se utilizan nunca como fuente de IOC (*Indicator of Compromise*) o aquellos informes que no son procesados, no podrán considerarse como inteligencia. Independientemente de lo precisa que pueda llegar a resultar, tampoco podrá considerarse inteligencia si el destinatario no pudiera interpretarla correctamente o se encontrara en una posición que no le permitiera llevar a cabo la toma de acción.

1.3 CIBERAMENAZA, CIBERINTELIGENCIA DE LA AMENAZA Y CONTRAINTELIGENCIA

1.3.1 Ciberamenazas y APT

Ciberamenaza

Se entiende como ciberamenaza (*cyber threat*) la posibilidad de realizar acciones maliciosas que afecten la confidencialidad, integridad y/o disponibilidad (CIA, *Confidentiality*, *Integrity*, *Availability*) de los recursos IT de la organización. La guía *NIST SP 800-150* "*Guide To Cyber Threat Information Sharing*" define ciberamenaza como cualquier circunstancia o evento con potencial impacto negativo contra las operaciones de una organización (incluyendo misión, funciones, imagen o reputación), activos de la organización, sus miembros, otras organizaciones, o la nación, empleando para ello un sistema de información mediante el acceso no autorizado, la destrucción, la publicación no autorizada o la modificación de información, y/o la denegación de un servicio. Los individuos y grupos que suponen una amenaza se conocen como agentes de la amenaza (*threat actors*) o, simplemente, agentes (*actors*).

APT

En 2006, los analistas de inteligencia de la USAF (*United States Air Force*) acuñaron el término amenaza persistente avanzada (APT, *Advanced Persistent Threat*) para facilitar la compartición de inteligencia relativa a intrusiones con los contratistas de defensa que carecían de la adecuada clasificación de seguridad. De esta manera, podían discutir las características relativas a ataques entre estados sin revelar información sensible sobre la posible identidad de la nación detrás de un determinado ataque.

El reputado especialista en ciberseguridad Richard Bejtlich, otrora oficial de inteligencia destinado en el AFCERT (*Air Force Computer Emergency Response Team*), describe las características que deberá tener una amenaza para ser considerada como APT:

- Avanzada. El adversario dispondrá de los conocimientos técnicos necesarios para operar con solvencia técnicas y herramientas, siendo también capaz de desarrollar *exploits* a medida o disponer de los recursos necesarios para adquirirlos en *markets underground*.
- Persistente. El adversario tendrá la firme intención de cumplir una misión o unas metas previamente establecidas.
- Amenaza. Implica que el adversario esté organizado, disponga de suficientes recursos (Ej. Económicos, humanos) y se encuentre suficientemente motivado.

La guía *NIST SP 800-39 "Managing Information Security Risk. Organization, Mission, and Information System View"* define APT como aquel adversario que dispone de un nivel avanzado de experiencia y recursos (Ej. Humanos, económicos, herramientas) para crear oportunidades que le permitan lograr sus metas empleando para ello múltiples vectores de ataque (Ej. Físicos, ciber, decepción). Estas metas normalmente implican establecer y extender cabezas de playa dentro de la infraestructura IT de sus organizaciones objetivo para exfiltrar información, socavar o impedir aspectos críticos de una misión, programa u organización, o poder llevarlas a cabo en un futuro. Para que una amenaza sea considerada como APT, el agente de la amenaza deberá:

- Perseguir repetidamente sus metas durante un periodo prolongado en el tiempo.
- Ser capaz de adaptar sus ataques a las defensas empleadas por sus objetivos.
- Asumir la interacción necesaria para ejecutar sus metas.

Las metas de cada adversario detrás de una APT serán diversas (Ej. Políticas, económicas) y entre sus objetivos podrían encontrarse tanto organismos gubernamentales (Ej. OTAN, UE, departamentos ministeriales) como entidades privadas (Ej. Contratistas de Defensa, entidades financieras y bancarias, industria farmacéutica, compañías del sector recursos, bufetes de abogados). Por tanto, el interés del atacante se centrará en aquellos datos e información sensibles para la víctima (Ej. Propiedad intelectual de una empresa farmacéutica, información legal de un cliente de un bufete de abogados, información financiera de un cliente de una entidad bancaria), y cuanto mayor sea el tiempo que tiene acceso a ellos, mejor podrá cumplir con sus metas (Ej. Acceso durante nueve meses al departamento de i+D de una empresa farmacéutica).

Otro factor que deberá ser tenido en cuenta es que entre las tácticas, técnicas y procedimientos (TTP, *Tactics, Techniques and Procedures*) empleadas por los actores detrás de una APT también se encontrarán vectores de ataque que pudieran a primera vista parecer poco sofisticados (Ej. Campañas *phishing*). No obstante, una vez lograda una cabeza de playa en el entorno corporativo de la víctima, como la intención del atacante es permanecer en ese entorno el mayor tiempo posible para cumplir sus metas, intentará ser lo más sigiloso posible para evitar ser detectado.

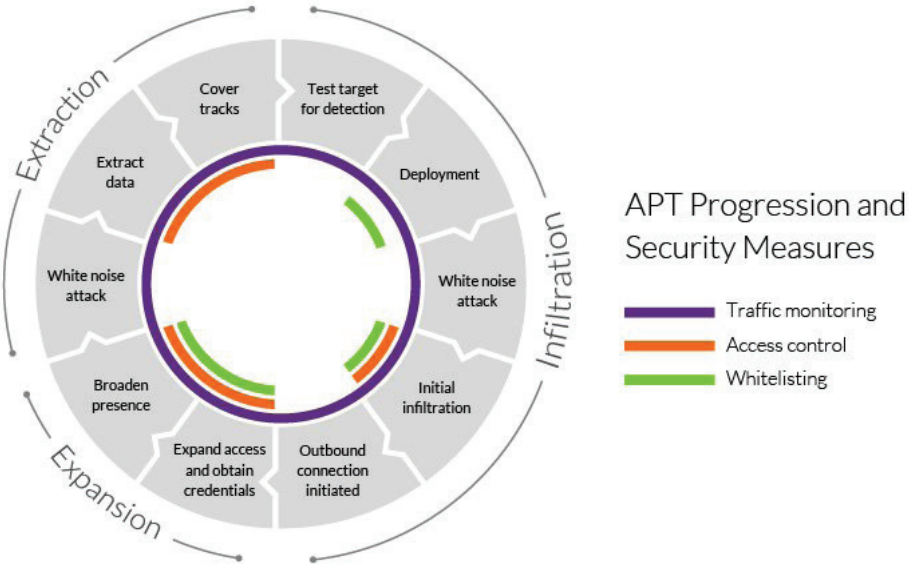

Ilustración 4. Fases del progreso de una APT y medidas de seguridad de detección y protección frente a las amenazas. Fuente: Imperva.

La compañía de ciberseguridad Imperva divide en tres fases el avance de una APT en el entorno de la víctima (se referencian entre paréntesis las tácticas y técnicas empleadas al *framework MITRE ATT&CK*):

- Fase 1- Infiltración. Normalmente, los atacantes emplearán una o más técnicas de la táctica *Acceso inicial* (*TA0001*), tales como explotación de aplicaciones web expuestas en Internet (*T1190*), *phishing* (*T1566*), o cuentas válidas de usuario (*T1078*). Adicionalmente, podrían ejecutar simultáneamente ataques que actuasen como cortina de humo y distraigan al equipo de defensa (Ej. Ataque DDoS contra portales web de la organización objetivo). Una vez que el atacante logra el acceso inicial en el entorno corporativo de la víctima, procederá a intentar garantizar su *Persistencia* (*TA0003*) empleando para ello diferentes técnicas, como la manipulación de cuentas (*T1098*), la creación de cuentas (*T1136*), la ejecución de aplicaciones en el inicio de sesión o el arranque del sistema (*T1197*), la ejecución de tareas programadas (*T1053*), o la explotación de servicios remotos externos (*T1133*).
- Fase 2- Expansión. Una vez establecida la cabeza de playa en el entorno corporativo de la víctima, el adversario intentará obtener información del entorno de la víctima, táctica conocida como *Descubrimiento* (*TA0007*), empleando técnicas como descubrimiento de cuentas (*T1087*), descubrimiento de servicios de red (*T1046*) o el descubrimiento de archivos y carpetas (*T1083*). Posteriormente, intentaría aumentar el número de sistemas de ese entorno bajo su control, táctica conocida como *Movimiento lateral* (*TA0008*), empleando para ello técnicas como la transferencia lateral de herramientas (*T1570*) o el *spearphishing* interno (*T1534*).

- Fase 3- Extracción. Normalmente, el adversario recopilará los datos e información de la víctima que sean de su potencial interés (Ej. Propiedad intelectual, datos financieros), táctica conocida como *Recopilación* (*TA0009*), y los almacenará en una ubicación que considere segura dentro del propio entorno corporativo de esta antes de proceder a su exfiltración (*T1074*), evitando ser detectado durante este proceso. Para ello, empleará técnicas de ruido blanco (*white noise*) mientras que emplea otras técnicas de la táctica de *Exfiltración* (*TA0010*), tales como limitar el tamaño de los datos transferidos (*T1030*), exfiltrar los datos sobre un canal de mando y control (C2, *Command and Control*) (*T1041*), o exfiltrar los datos empleando protocolos alternativos (*T1048*).

1.3.2 Ciberinteligencia de la amenaza

El prestigioso *think tank* Gartner define inteligencia de la amenaza (TI, *Threat Intelligence*), también referenciado como ciberinteligencia de la amenaza (CTI, *Cyber Threat Intelligence*), como "el conocimiento basado en las evidencias (procedentes del contexto, mecanismos, indicadores, posibles implicaciones y recomendaciones factibles) sobre una amenaza existente o emergente a los activos de la organización y que puede ser utilizado para asesorar a la toma de decisión frente a esa amenaza".

SANS Institute, otra de las instituciones con mayor prestigioso en el mundo de la ciberseguridad, considera la CTI como "la información relativa a amenazas activas que puede ser aprovechada por la organización tanto para prevenir ataques futuros como para detectar aquellos ataques que no se pueden prevenir de una forma más rápida".

Por su parte, EC-Council define la CTI como "la recolección y análisis de información relativa a amenazas y adversarios y al dibujo de patrones que proporcionen una capacidad de toma de decisiones basada en el conocimiento para la preparación, prevención y la adopción de acciones de respuesta frente a posibles ciberataques".

Una definición más sencilla sería la propuesta por la compañía Recorded Future, especializada en inteligencia de la amenaza, que la enuncia como "el producto del análisis basado en la identificación, recogida y enriquecimiento de datos e información relevantes".

Para la compañía sueca SecureMind, la CTI puede definirse como "el proceso de recopilación de información sobre potenciales adversarios para comprender su motivación para atacar a la organización, conocer las diferentes alternativas de ataque de las que disponen, y analizar esta información para securizar con antelación la infraestructura IT corporativa".

Sergio Caltagirone, uno de los padres del *Modelo en Diamante*, define la inteligencia de la amenaza como el conocimiento aplicable y la información disponible relativa a los adversarios y sus actividades maliciosas que permiten a las organizaciones reducir el daño merced a la mejora de la toma de decisiones en materia de ciberseguridad.

Otra posible definición de CTI sería como "el proceso de detección de amenazas potenciales o en curso utilizando pruebas basadas en datos, respondiendo contra dichas amenazas y derrotando a los atacantes empleando técnicas forenses para analizar las evidencias dejadas por los atacantes".

Es decir, la CTI intenta establecer una defensa proactiva configurando las contramedidas adecuadas antes de que pueda materializarse la amenaza. Deben por tanto identificarse los pasos y las TTP empleadas por los adversarios para ejecutar sus ataques, y no solamente identificar las potenciales amenazas mediante la comprobación de firmas de archivos maliciosos o el empleo de indicadores de compromiso (IOC, *Indicators Of Compromise*).

En resumen, la inteligencia de la amenaza es el conocimiento de las capacidades, infraestructura, motivos, metas y recursos de una amenaza. La aplicación de esta información asiste en la defensa operacional y estratégica de los activos conectados en red.

1.3.3 Inteligencia de seguridad

Tradicionalmente, el término inteligencia de la amenaza se ha asociado con la inteligencia relativa a las amenazas contra los sistemas IT. Pero esta visión del término resulta actualmente demasiado limitada.

Desde el punto de vista defensivo, es necesario adoptar métodos que permitan combatir a los agentes de la amenaza descubriendo sus métodos e interrumpiendo sus actividades antes de que logren atacar. Esto empuja a expandir los programas de inteligencia para que incluyan áreas como riesgos debidos a terceros (Ej. Exposición a través de productos de terceros, contratistas, proveedores, socios comerciales), protección frente al daño reputacional, riesgos geopolíticos, etc.

De ahí que Recorded Future acuñara el término inteligencia de seguridad (*security intelligence*) para englobar lo que anteriormente se conocía como inteligencia de la amenaza y las áreas adicionales referenciadas en el párrafo anterior. No obstante, este nuevo término no ha tenido suficiente calado en la comunidad de ciberinteligencia y, en general, se utiliza el término inteligencia de la amenaza en el sentido propuesto por Recorded Future para inteligencia de seguridad.

1.3.4 Cibercontrainteligencia

Se puede definir cibercontrainteligencia (*cyber counterintelligence*), también denominada contra explotación de la ciberamenaza (*cyber threat counter-exploitation*), como el conjunto de actividades encaminadas a denegar a una amenaza o adversario la capacidad de recolectar información precisa de las redes y sistemas de la organización.

Por tanto, para hacer frente a todo el espectro posible de ciberamenazas que podrían afectar al normal funcionamiento de la organización, en CTI deberán emplearse técnicas tanto de inteligencia como de contrainteligencia clásicas.

Conviene destacar que existe cierto solapamiento entre las actividades de CTI y contrainteligencia, si bien la CTI tiene un carácter defensivo y no está orientada a la contrainteligencia ofensiva, más relacionada con operaciones de decepción.

1.3.5 Fases en la obtención de la CTI

El concepto de CTI refleja en cierto modo el concepto de inteligencia que tenía el exsecretario de Defensa de los EE.UU. Donald Rumsfeld.

El proceso de inteligencia de la amenaza comienza en la fase "*desconocidos desconocidos*", pues a priori, no se dispondrá de un conocimiento de una amenaza que no se sabe si existe, pero que se intenta encontrar.

Una vez se obtiene información relativa a las amenazas existentes en el entorno corporativo, se avanza a la segunda fase, "*desconocidos conocidos"*. En esta fase, se analizará la información recopilada y se alcanzará una comprensión de la naturaleza de las amenazas. Con estos datos, se intentará mitigar las amenazas existentes y alcanzar la fase final, "*conocidos conocidos"*.

La implementación en la organización de estas tres fases de inteligencia permitiría la toma de decisiones y la obtención de resultados. No obstante, el paso de "*desconocidos desconocidos*" a "*conocidos conocidos*" es una dura tarea en ciberinteligencia.

Conocimiento sobre un hecho	**Desconocidos conocidos** Sabemos que existen cosas que no podemos predecir	**Conocidos conocidos** Cosas de las que estamos seguros
	Desconocidos desconocidos No sabemos lo que no sabemos	**Conocidos desconocidos** Otros lo conocen, pero nosotros no
	Conocimiento sobre el impacto	

Tabla 1. Gestión del riesgo ante lo inesperado.

Los "*conocidos desconocidos*" son incidentes o ciberamenazas que ya son conocidos por terceros, pero que nuestra organización actualmente desconoce. Este conocimiento podría ser adquirido rápidamente mediante la compartición de inteligencia entre organizaciones federadas, pasando así a ser "*conocidos conocidos*" para nuestra organización. Análogamente, nuestros "*conocidos conocidos*" podrían ser transferidos a terceros, cubriendo así sus "*conocidos desconocidos*".

Esta exposición permite definir la CTI como "el proceso de recolección de información sobre potenciales adversarios para comprender su motivación para atacar sus objetivos, el modo en el que podrían ejecutar esos ataques, y el análisis de esa información para garantizar la seguridad de la infraestructura IT de la organización antes de que se perpetren los ataques".

1.3.6 *Modelo Triángulo de la Amenaza*

En el *Modelo Triángulo de la Amenaza* se considera que para que pueda existir una amenaza contra una potencial víctima deberán concurrir una combinación de los siguientes tres factores, los cuales pueden ser vistos como las aristas de un triángulo:

- Intención. Motivación por la cual un agente de la amenaza pretende atacar a una determinada víctima (Ej. Financiera, geoestratégica, venganza, visibilidad).
- Capacidad. Medios empleados por el agente de la amenaza para atacar a la víctima (Ej. *Malware*).
- Oportunidad. Ventana de oportunidad que necesita el atacante (Ej. Existencia de vulnerabilidades software/hardware/humanas).

Ilustración 5. Triángulo de la Amenaza.

Por tanto, no podrá materializarse una amenaza mientras no concurran estos tres factores simultáneamente. A modo de ejemplo, si un adversario tuviera la intención y la capacidad, pero la organización víctima no fuese vulnerable (no existiese una oportunidad), ese agente no supondría una amenaza para esa organización en ese momento.

Desde el punto de vista defensivo, la organización puede intentar influenciar sobre estos tres factores para mitigar la amenaza:

- Intención. Puede ser en parte mitigada mediante disuasión (*deterrence*) (Ej. Código penal, *hack back*).
- Capacidad. Si bien resulta complicado controlar la capacidad de conducción de operaciones de un adversario, pueden llevarse a cabo determinadas acciones de mitigación como la elaboración, compartición e ingesta de CTI (Ej. URL y direcciones IP de la infraestructura IT del atacante, valores resumen de *malware*), la monitorización de foros y *markets underground* (Ej. Detección de venta de credenciales de usuarios y datos sensibles exfiltrados de la organización, compraventa de *exploits* contra vulnerabilidades hardware/software de los sistemas del entorno corporativo), la vigilancia de *markets* oficiales y no oficiales de aplicaciones para dispositivos móviles (Ej. Detección de aplicaciones fraudulentas que suplanten las legítimas de la organización), o el *takedown* de sitios web que intenten suplantar la identidad de la organización (Ej. *Typosquatting*, *cybersquatting*).
- Oportunidad. Principalmente, mediante la aplicación de buenas prácticas defensivas (Ej. Concienciación de usuarios, parcheo de vulnerabilidades críticas, empleo de 2FA, segmentación de red, bastionado de redes y sistemas).

1.4 TIPOLOGÍAS DE INTELIGENCIA DE LA AMENAZA

1.4.1 Introducción

Probablemente, la fase de análisis de la amenaza sea la más importante de todo el *Ciclo de Inteligencia*. Durante esta fase, ingentes cantidades de datos e información "en crudo" serán procesadas para convertirse en inteligencia de interés para la organización.

No obstante, el proceso de análisis puede variar enormemente dependiendo del producto deseado. A grandes rasgos, existen dos posibles taxonomías a la hora de definir los tipos de inteligencia de la amenaza existentes: según el modo de procesar los datos, o según la funcionalidad de la inteligencia de la amenaza.

1.4.2 Inteligencia de la amenaza según el procesamiento de datos

Esta taxonomía distingue cuatro posibles tipos de ciberinteligencia de la amenaza: táctica, técnica, operacional y estratégica.

Ilustración 6. Tipos de inteligencia de la amenaza.

Táctica

La inteligencia de la amenaza táctica proporciona información relativa a las TTP utilizadas por los atacantes, es decir, aporta información sobre cómo los agentes de la amenaza ejecutan sus ataques. Sus consumidores son, principalmente, los directores de los servicios IT, los directores de las operaciones de seguridad de red, los arquitectos de seguridad y el personal de respuesta a incidentes con el objetivo de garantizar que sus defensas, alertas e investigaciones estén preparadas frente a dichas TTP.

Entre las fuentes para la generación de inteligencia a nivel táctico se encuentran informes relativos a campañas, *malware*, incidentes y agentes de la amenaza, además de inteligencia HUMINT (*Human Intelligence*).

Se entiende por campaña el conjunto de actividades maliciosas o ataques que tienen lugar en una ventana temporal, contra un conjunto de víctimas, asociadas a un conjunto de la intrusión determinado y caracterizada por el empleo de versiones prácticamente idénticas de una o más muestras de *malware*.

Se entiende por incidente un conjunto de actividades maliciosas asociadas a un conjunto de intrusión y cuyo objetivo es una determinada víctima durante una ventana temporal continua y correctamente identificada.

El producto de esta inteligencia se genera en formato de informe forense digital e incluye información eminentemente técnica, como análisis de *malware*, campañas, técnicas y herramientas.

La inteligencia a nivel táctico proporciona información del modo en el que los adversarios pretenden ejecutar sus ataques contra la organización, sus capacidades técnicas, sus vectores de ataque y los objetivos que persiguen.

Técnica

La inteligencia a nivel técnico proporciona información relativa a los recursos de los que dispone el atacante, como los canales C2, y las herramientas empleadas para ejecutar los ataques. Suele hacer referencia a información técnica en crudo consumida a través de medios técnicos (Ej. Un *feed* de un conjunto de direcciones IP sospechosas de ser maliciosas o de actuar como servidores C2).

Los consumidores de la inteligencia a nivel técnico son el personal del SOC (*Security Operations Center*) de la organización y el personal de respuesta a incidentes. Este tipo de inteligencia debe alimentar también las medidas defensivas de la corporación (Ej. Bloquear el acceso de los usuarios de la red corporativa a sitios web reportados como maliciosos).

Esta inteligencia suele tener un tiempo de vida más reducido que la del nivel táctico, ya que se centra en los IOC específicos de la campaña. A modo de ejemplo, los atacantes podrían cambiar con gran facilidad las direcciones IP empleadas para la ejecución de sus ataques o modificar el *malware* empleado en la campaña para que su valor resumen difiera del de otras muestras utilizadas durante esa campaña u otras campañas anteriores.

Las fuentes de la inteligencia de la amenaza a nivel técnico son los IOC recopilados de la campaña en curso, ataques ejecutados en otras organizaciones, o *feeds* de datos proporcionados por terceros. Ejemplos de este tipo de inteligencia incluyen direcciones IP y dominios específicos de la campaña, cabeceras de correo electrónico de campañas *phishing*, valores resumen de muestras de *malware*, etc.

Esta inteligencia mejora la capacidad de los mecanismos de detección, proporcionando indicadores a los sistemas defensivos (Ej. IDS/IPS, firewalls, sistemas de seguridad *endpoint*).

Operacional

La inteligencia de la amenaza a nivel operacional proporciona información relativa a amenazas específicas existentes contra la organización. Este tipo de inteligencia es normalmente consumida en primera instancia por los directivos de alto nivel de la organización, como directores de seguridad, directores de respuesta a incidentes, personal responsable de la defensa de la red, investigadores forenses digitales, y equipos de detección de fraude. En ocasiones esta información también puede ser valiosa para el equipo de evaluación de riesgos (Ej. El ataque implica riesgo a la operación del negocio o reputación de la organización).

La inteligencia de la amenaza a nivel operacional proporciona información relativa a qué atacantes (*Who*), cuándo (*When*) y cómo (*How*) planean atacar a la organización. Disponer de este tipo de inteligencia suele ser complicado, siendo el escenario más habitual que solo organizaciones gubernamentales dispongan de capacidad de acceder a los potenciales grupos atacantes y de la infraestructura necesaria para recolectar este tipo de inteligencia.

Entre las fuentes de inteligencia de la amenaza a nivel operacional se encontrarían HUMINT, los medios de comunicación social y las conversaciones de las herramientas de mensajería.

El producto de inteligencia generado será un informe que contendrá las actividades maliciosas identificadas, los cursos de acción recomendados, y alertas de ataques emergentes.

Esta inteligencia permite identificar los potenciales agentes de la amenaza contra la organización, junto con su intención, capacidad y oportunidad para atacar, los activos IT que resultan vulnerables y el impacto que produciría el ataque si este tuviera éxito. Además, permite a los equipos de forense digital y respuesta a incidentes (DFIR, *Digital Forensics and Incident Response*) desarrollar activos de seguridad con el objetivo de identificar y detener futuros ataques, mejorar la capacidad de detección de ataques durante su primera fase de ejecución, y mitigar el daño en los activos IT.

Estratégica

La inteligencia estratégica proporciona información de alto nivel relativa a la postura en ciberseguridad, las amenazas y su impacto en la organización. Generalmente, los consumidores de esta inteligencia son directivos de alto nivel y equipos de apoyo a la dirección. Normalmente, esta inteligencia es presentada en forma de informe ejecutivo centrado en estrategias de alto nivel corporativo. Este informe se utiliza como apoyo en la toma de decisiones estratégicas y el análisis del efecto que podría conllevar la toma de esas decisiones. Entre sus fuentes se encuentran la obtenida de OSINT (*Open Source Intelligence*), proveedores comerciales de CTI y ISAO/ISAC.

La CTI a nivel estratégico comprende aspectos como el impacto financiero de la ciberactividad, las tendencias de los ciberataques y áreas que pudieran impactar en la toma de decisiones de negocio a alto nivel (Ej. Informe relativo a las sospechas que recaen sobre un determinado gobierno involucrado en actividades de espionaje industrial sobre empresas extranjeras competencia directa de las propias de su nación).

1.4.3 Funcionalidad de la inteligencia de la amenaza

La inteligencia de la amenaza puede ser recopilada en base a su funcionalidad. La funcionalidad puede ser operacional (basada en procesos) y estratégica (basada en metas de la organización).

Operacional

A nivel operacional, la inteligencia de la amenaza identifica los indicadores de la amenaza que incrementan la capacidad de detección y aportan alertas relativas a ataques o ataques potenciales. Expone además riesgos específicos basados en vulnerabilidades dentro de los activos de la red corporativa. Las fuentes incluyen *feeds* de proveedores y de fuentes abiertas relativos a IOC, *blogs* con análisis técnicos de muestras de *malware* e informes tácticos que incluyan ataques, capacidades e infraestructura de los potenciales adversarios. Esta inteligencia está producida completamente por dispositivos informáticos tras un proceso de enriquecimiento y análisis a partir de la identificación y recogida de datos.

Un ejemplo, sencillo y con bajo coste de implementación, sería la detección automática de ataques DDoS mediante la comparación de IOC y la telemetría de red, pues los dispositivos permiten llevar a cabo una identificación más rápida que la que podrían realizar analistas humanos.

Estratégica

A nivel estratégico, la inteligencia de la amenaza centra su atención en la exposición de la organización frente a amenazas concretas, permitiendo que dichas amenazas sean evaluadas en comparación con riesgos presentes y futuros y la continuidad de las operaciones. Dentro de la inteligencia estratégica se encontrarían las valoraciones de la amenaza, resúmenes de inteligencia y perfiles de los potenciales adversarios. Se centra en un proceso complejo de identificación y análisis de posibles amenazas contra los activos de la organización (Ej. Empleados, clientes, infraestructura, aplicaciones). Esto requiere analistas humanos con gran experiencia capaces de: desarrollar relaciones externas y fuentes propietarias de información; identificar tendencias; formar a empleados y clientes; estudiar las TTP de los atacantes; y de elevar las recomendaciones defensivas necesarias para poder combatir contra las amenazas identificadas.

Un ejemplo de este tipo de inteligencia es la utilización de las TTP de un agente malicioso para adoptar medidas de seguridad proactivas, como pudieran ser una gestión mejorada del parcheo de vulnerabilidades, o la elaboración de un plan global de concienciación de ciberseguridad.

1.4.4 Tipología de inteligencia según Recorded Future

La ciberinteligencia está formada por dos tipos diferentes de inteligencia: operacional y estratégica. Estos dos tipos difieren en sus fuentes, audiencias y formatos.

Esta distinción está motivada en los diferentes objetivos y grados de conocimiento técnico que tienen los equipos de seguridad. La inteligencia deberá ser aplicable, pero esta aplicabilidad diferirá conforme al destinatario del producto de inteligencia. A modo de ejemplo, las necesidades de inteligencia del jefe del equipo de gestión de vulnerabilidades serán diferentes de las del CISO de esa misma organización.

Inteligencia operacional

La inteligencia operacional es aquella relativa a ataques, eventos y campañas en curso. Proporciona una visión específica de la naturaleza, intención y una línea temporal de los ataques en curso.

En ocasiones, este tipo de inteligencia es denominada inteligencia técnica de seguridad o también como seguridad técnica de la amenaza, pues normalmente incorporará información técnica de los ataques (Ej. Vectores de ataque empleados, vulnerabilidades explotadas, dominios C2 de la infraestructura IT de los atacantes). Este tipo de inteligencia es de utilidad a personal directamente implicado en la defensa de las redes y sistemas del entorno corporativo (Ej. Arquitectos de sistema, personal de seguridad).

Los *feeds* de datos de la amenaza suelen emplearse para proporcionar información técnica. Estos *feeds* normalmente se centran en un único tipo de indicador de la amenaza (Ej. valores resumen de *malware*, dominios sospechosos). Los *feeds* proporcionan una entrada para generar inteligencia, pero no constituyen inteligencia.

Este tipo de inteligencia normalmente se emplea como guía para mejorar los procesos y controles de seguridad, y para acelerar el ciclo de respuesta a incidentes. Desde el punto de vista defensivo, resulta fundamental disponer de una solución de inteligencia operacional que se integre con los datos del entorno corporativo, puesto que permitirá responder rápidamente preguntas únicas relativas a ese entorno (Ej. Si en los sistemas corporativos ha sido parcheada una vulnerabilidad que está siendo explotada en otras empresas del mismo sector industrial).

Inteligencia estratégica

La inteligencia estratégica proporciona una amplia visión del panorama de amenazas de la organización. Este tipo de inteligencia resulta de utilidad al personal corporativo responsable de la toma de decisión a nivel estratégico. Normalmente, está orientada al negocio y se proporciona en forma de informes. Este tipo de informes solo pueden ser generados por analistas expertos.

Generar este tipo de inteligencia requiere interacción humana porque necesita de pensamiento crítico para evaluar y comprobar nuevas TTP del adversario contra los controles de seguridad existentes. Pese a que parte del proceso pueda ser automatizado, es necesaria la intervención de un analista para generar el producto final.

Una inteligencia estratégica de seguridad adecuado debe proporcionar una perspectiva de los riesgos asociados con determinadas acciones, una amplia visión de los patrones de las tácticas y objetivos de los atacantes, tendencias y eventos geopolíticos, etc.

Entre las fuentes habituales empleadas para generar inteligencia estratégica se encuentran: documentos de directivas de estados y NGO; noticias de medios locales y nacionales, artículos relativos a sectores industriales, comentarios de expertos en materias concretas; productos de empresas relacionadas con la ciberseguridad (Ej. *Papers*, informes de investigación).

Las necesidades de inteligencia estratégica de seguridad deben establecerse mediante preguntas específicas y centradas en temas concretos. Además de expertos en ciberseguridad, deberá disponerse en el equipo de analistas con un profundo conocimiento sociopolítico y de economía y negocios.

No obstante, algunos aspectos de la producción de inteligencia estratégica de seguridad deben ser automatizados. Pese a que el producto final no sea técnico, la generación de este tipo de inteligencia requiere procesar un volumen ingente de datos, en la mayoría de las ocasiones en diferentes idiomas. Por tanto, la recopilación y procesado inicial manual de datos resultará excesivamente compleja, incluso en aquellos escenarios en los que se disponga de analistas técnicamente capacitados y que a la vez dominen diferentes idiomas. De ahí la necesidad de disponer de una herramienta de inteligencia que automatice la recopilación y procesado de datos, permitiendo trabajar de manera más eficiente a los analistas.

1.4.5 Efectividad y operatividad de la CTI

Para que la CTI en una organización sea efectiva y operacional es necesario implementar tanto la inteligencia estratégica como la operacional, pues son mutuamente dependientes.

Para poder lograr la automatización completa de los procesos implicados en la elaboración de inteligencia operacional se depende en gran medida de que el personal responsable de la arquitectura de datos esté altamente cualificado y disponga de experiencia previa en la materia. Este personal será el responsable del diseño, creación y calibración de las herramientas empleadas para realizar esta función.

Por otro lado, la única forma de que un analista sea capaz de producir inteligencia estratégica es que existan dispositivos automáticos generando automáticamente inteligencia operacional. Esto evita que los analistas de inteligencia sean saturados por la recepción de una ingente cantidad de falsos positivos.

1.4.6 Compresión del espacio de batalla reputacional

En la Era de la Información, los niveles clásicos de inteligencia (táctica, operacional, estratégica) se ven comprimidos enormemente debido a la rapidez y globalidad de las comunicaciones, facilitando que acciones locales tengan un impacto a escala global. Como Internet permite realizar un seguimiento de eventos locales de manera global, agentes políticos (estatales o no estatales), grupos de interés, grupos terroristas, o incluso personas aisladas pueden rastrear noticias de publicadas en cualquier lugar del mundo en busca de eventos locales que permitan reforzar su narrativa.

Esta rapidez de acceso a la información se combina con la relativa facilidad con la que los adversarios pueden distorsionar y manipular esa información. La dirección del equipo de