Managed secure IT | no matter what

THREAT INTELLIGENCE

Mecanismos de defensa activa contra inteligencia de amenazas

www.mexis.net

Autor: Jorge Rubén Macías López
Gerente de Innovación Tecnológica Mexis

THREAT INTELLIGENCE

Mecanismos de defensa activa contra inteligencia de amenazas

Conforme a lo mostrado en el informe anual del estado de la ciberseguridad en el mundo publicado por ISACA a principios de 2018, uno de los puntos a resaltar es la adopción en una gran cantidad de empresas de algún tipo de mecanismo de defensa activa contra amenazas, lo que es conocido también como aplicación de inteligencia de amenazas (threat intelligence o cyber threat intelligence son los términos que suelen utilizarse en inglés para referirse a ello).

La inteligencia de amenazas, de forma general consiste en un conjunto de elementos como son componentes tecnológicos, procesos, conocimiento y prácticas que van más allá de analizar la actividad que se presenta en los activos tecnológicos de una organización, sino que dan una visibilidad amplia, temprana y de fácil comprensión, acerca de la existencia de amenazas informáticas que pueden causar daño en el patrimonio intelectual, continuidad operativa, reputación o cumplimiento regulatorio, entre otros aspectos, logrando todo esto ya sea que exista actividad de la amenaza manifestada ya dentro de la organización, o no; y lo más importante, la inteligencia de amenazas debe resulta en acciones.

La inteligencia de amenazas abarca toda aquella práctica que proporciona información relevante y oportuna que permite comprender y anular una amenaza antes de que se manifieste en la práctica, o minimizar su impacto al detectarla en etapas iniciales de su actividad. Esto incluye conocer aspectos diversos de los atacantes potenciales, como lo son sus motivaciones: económicas, políticas, ideológicas o incluso lúdicas; postura ante la organización si se trata de una amenaza dirigida o general;, métodos, herramientas y hábitos; prácticamente en pocas palabras, trata de permitir a la empresa observarse como lo haría un atacante. El resultado es que la organización se vuelve más inteligente acerca de las amenazas informáticas que realmente enfrenta conforme a su propio contexto.

Cada empresa, dependiendo de sus recursos financieros y tecnológicos, de su nivel de conocimiento, su postura ante el riesgo y del tipo de exposición que tenga ante las amenazas, podrá implementar este tipo de prácticas de manera distinta.

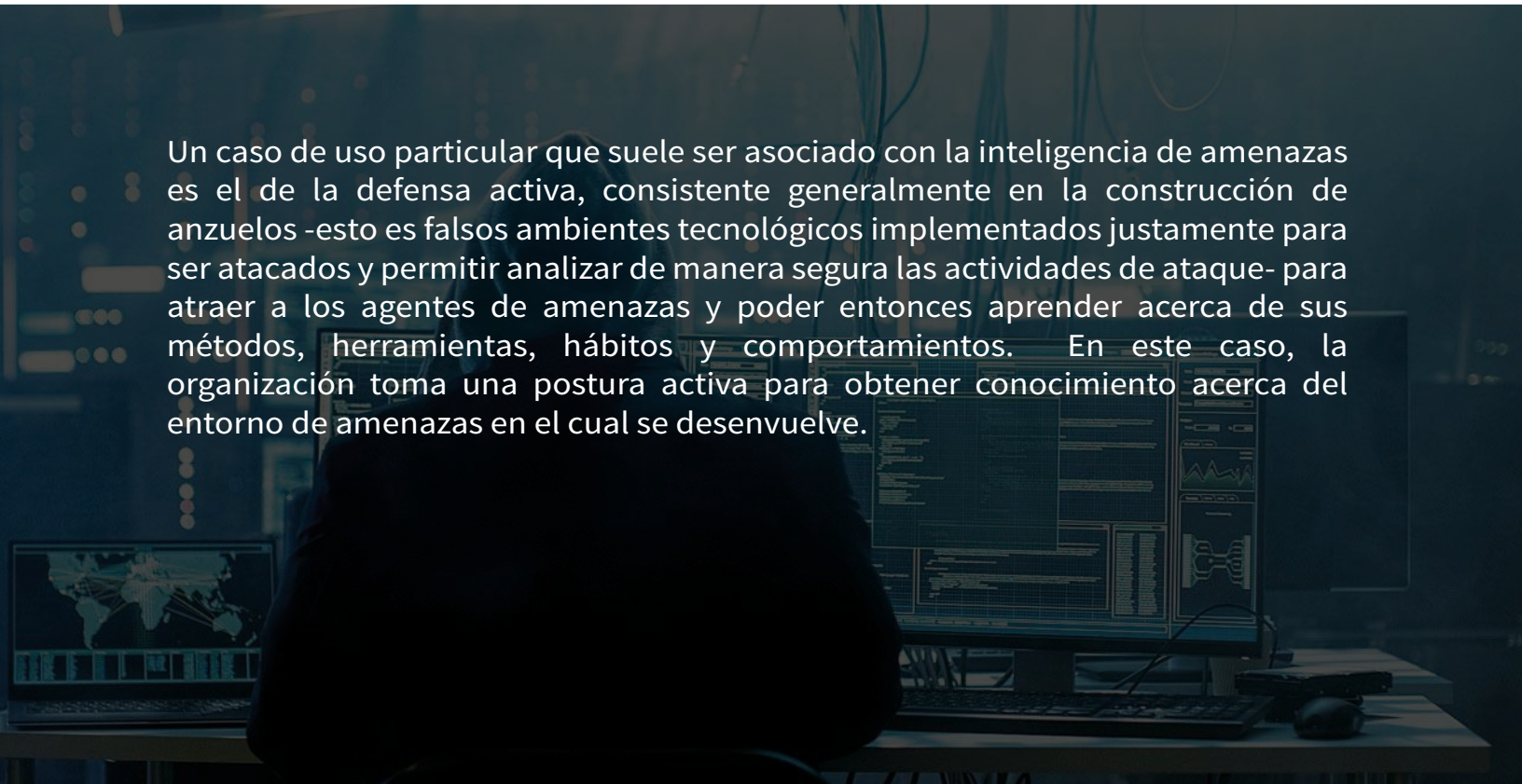
El informe ya referido de ISACA arroja datos significativos acerca de la adopción de la inteligencia de amenazas:

- El 53% de los encuestados indica que en su organización tienen implementada alguna forma de defensa activa, como honeypots.

- El 87% de los participantes comentaron que en sus empresas cuentan con alguna forma de inteligencia de amenazas, de los cuales, el 50% lo hace con recursos internos y el 37 utiliza un proveedor.

- Acerca de los obstáculos que enfrentan para implementar, ampliar o robustecer su práctica, el 43% mencionó que tiene una problemática de falta de conocimiento o recursos, mientras que el 37% se enfrenta a restricciones de presupuesto. Algunos otros factores son implicaciones legales (34%) o técnicas (30%).

- Del universo de organizaciones que cuentan con una práctica implementada, el 87% manifiesta haber tenido éxito en el cumplimiento de sus objetivos.



Un caso de uso particular que suele ser asociado con la inteligencia de amenazas es el de la defensa activa, consistente generalmente en la construcción de anzuelos -esto es falsos ambientes tecnológicos implementados justamente para ser atacados y permitir analizar de manera segura las actividades de ataque- para atraer a los agentes de amenazas y poder entonces aprender acerca de sus métodos, herramientas, hábitos y comportamientos. En este caso, la organización toma una postura activa para obtener conocimiento acerca del entorno de amenazas en el cual se desenvuelve.

Honeypot: se puede interpretar como un sistema señuelo, que básicamente es una combinación de hardware o software que se instala como una trampa con la intención de que reciba ataques informáticos. Conforme los recibe, el administrador del señuelo tiene la posibilidad de analizar los métodos, herramientas y hábitos de ataque y usar esta información para proteger su infraestructura real.

Lo más valioso de todos estos datos es que se puede concluir que el uso de la inteligencia de amenazas se está extendiendo y que, más allá de que ocurra por moda, es porque genera beneficios para las empresas. En términos generales, estos beneficios surgen de un hecho simple, las empresas logran optimizar los recursos que utilizan en cada una de las etapas en su gestión de la ciberseguridad.

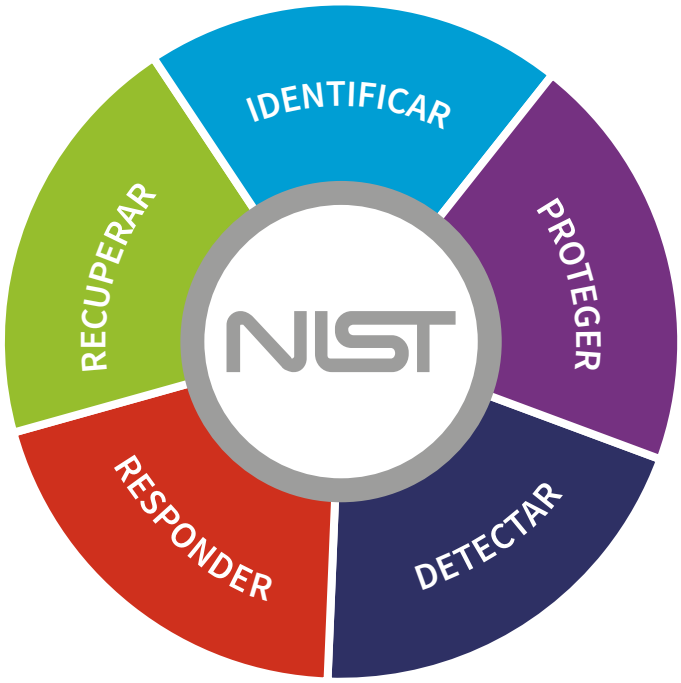


Figura 1: *Ciclo para Gestión de Ciberseguridad, NIST Framework 1.1*

Conforme a este ciclo, se puede identificar algunos de los beneficios más directos en la administración y operación de la seguridad que surgen al aplicar una práctica de inteligencia de amenazas.

ETAPA	NOMBRE
IDENTIFICACIÓN	• Provee información acerca del contexto de amenazas y riesgos de la organización. ¿Se está mencionando a la empresa en foros de hacktivismo? ¿Alguna de la tecnología que se utiliza tiene vulnerabilidades importantes? ¿Alguien puede estar planeando un ataque dirigido a la organización? • Alimenta el modelo para la evaluación de riesgo. • Proporciona insights acerca de aquellos riesgos cuyo tratamiento debe ser prioritario. • Permite a la organización identificar agentes de amenaza que puede no tener identificados.
PROTECCIÓN	• Genera evidencia clara y contundente que sirve como material de apoyo para los eventos o materiales de entrenamiento y concientización. • Evidencia real de equipos vulnerados, credenciales y documentos de la empresa que han sido robados y publicados o puestos a la venta en la dark web. • Muestra brechas de seguridad, revelando aquellos puntos donde deben mejorarse los mecanismos de seguridad. • Vectores de ataque que han sido utilizados exitosamente contra la organización, como troyanos, backdoors, rootkits, key loggers, entre otros.
DETECCIÓN	• Identifica de forma temprana la existencia de amenazas a la organización. • Credenciales o datos de tarjetas de crédito robados a empleados o clientes, aun antes de que sean utilizados. • Sitios web o aplicaciones móviles que de forma fraudulenta explotan el nombre, la imagen o propiedad intelectual de la organización. • Encuentra las amenazas explorando fuera del perímetro de la organización. Redes sociales, dark web, servicios de compartición de documentos, redes P2P, entre otros.
RESPUESTA	• Captura y protege la evidencia de los hallazgos para su uso en esta etapa. • Permite iniciar la respuesta cuando la afectación ha sido mínima o ninguna, con lo cual se pueden planear y llevar a cabo acciones sin un factor adicional de emergencia. • Proporciona información que permite a los equipos de operaciones de TI y Seguridad identificar los puntos de corrección y mejora.

A partir de estos beneficios para las funciones propias de ciberseguridad, se observan otros muy claros para el negocio.

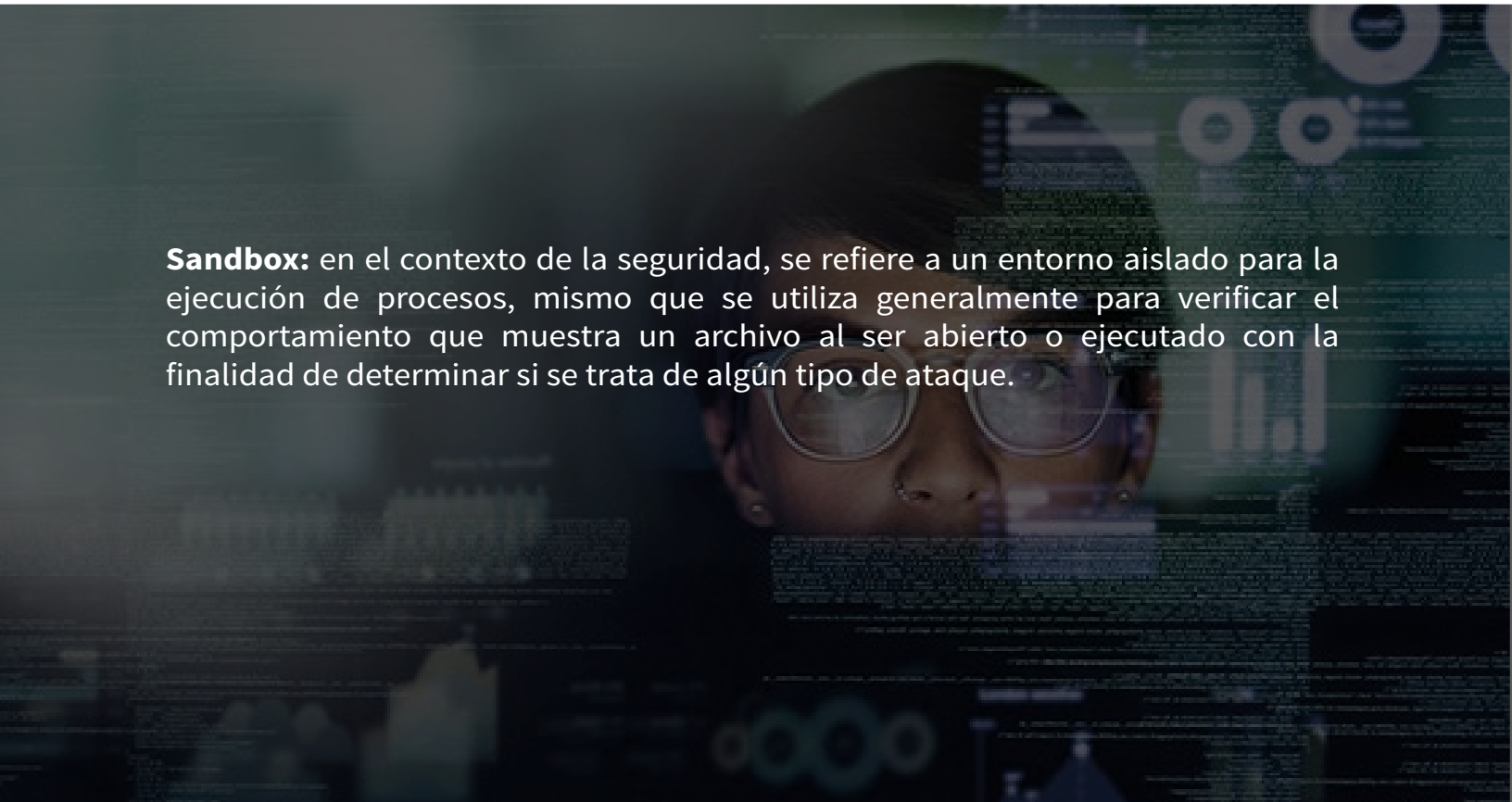
- Se reduce el impacto financiero de los ataques informáticos, en términos de costos por reembolsos o compensaciones a clientes, multas, inversión en campañas de comunicación para reestablecer la imagen de la organización, primas de pólizas de seguros contra fraude, jornadas de trabajo adicionales para los equipos de operaciones de seguridad, entre otros.

- Se mejora la protección de propiedad intelectual de la organización, identificando usos fraudulentos, abusivos o no permitidos de su nombre, marcas, nombres de productos y servicios, documentos, procesos, entre otros.

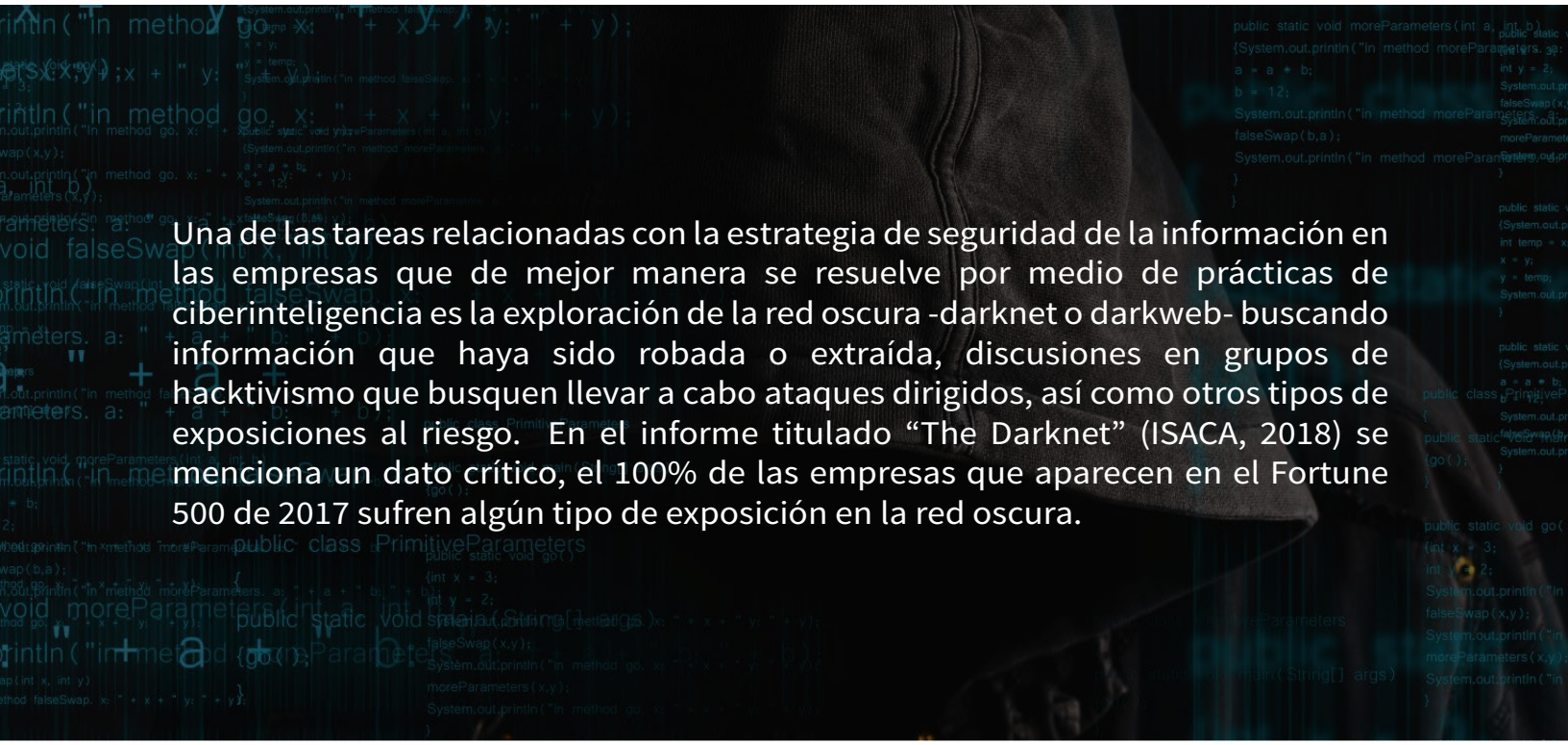
- Se guía la inversión tecnológica en controles de ciberseguridad a aquellos aspectos que generan los mayores beneficios.

- Se cuida la experiencia del cliente al minimizar la posibilidad de que este se vea afectado por el uso fraudulento, abusivo o criminal de su relación con la empresa por medios como contraseñas robadas, sitios web o aplicaciones móviles fraudulentas; así como incrementando la disponibilidad de los servicios que recibe de la organización.

Entendiendo el valor que aporta a las empresas el adoptar prácticas de inteligencia de amenazas, lo siguiente es determinar la manera de hacerlo y en este sentido es indispensable reconocer que no existe una receta que aplique para todas las empresas, sino que cada una, dependiendo de sus prioridades estratégicas, así como de su nivel de exposición al riesgo, deberá elegir una combinación a la medida de implementación interna y por medio de un proveedor de servicios.



Sandbox: en el contexto de la seguridad, se refiere a un entorno aislado para la ejecución de procesos, mismo que se utiliza generalmente para verificar el comportamiento que muestra un archivo al ser abierto o ejecutado con la finalidad de determinar si se trata de algún tipo de ataque.



Una de las tareas relacionadas con la estrategia de seguridad de la información en las empresas que de mejor manera se resuelve por medio de prácticas de ciberinteligencia es la exploración de la red oscura -darknet o darkweb- buscando información que haya sido robada o extraída, discusiones en grupos de hacktivismo que busquen llevar a cabo ataques dirigidos, así como otros tipos de exposiciones al riesgo. En el informe titulado “The Darknet” (ISACA, 2018) se menciona un dato crítico, el 100% de las empresas que aparecen en el Fortune 500 de 2017 sufren algún tipo de exposición en la red oscura.

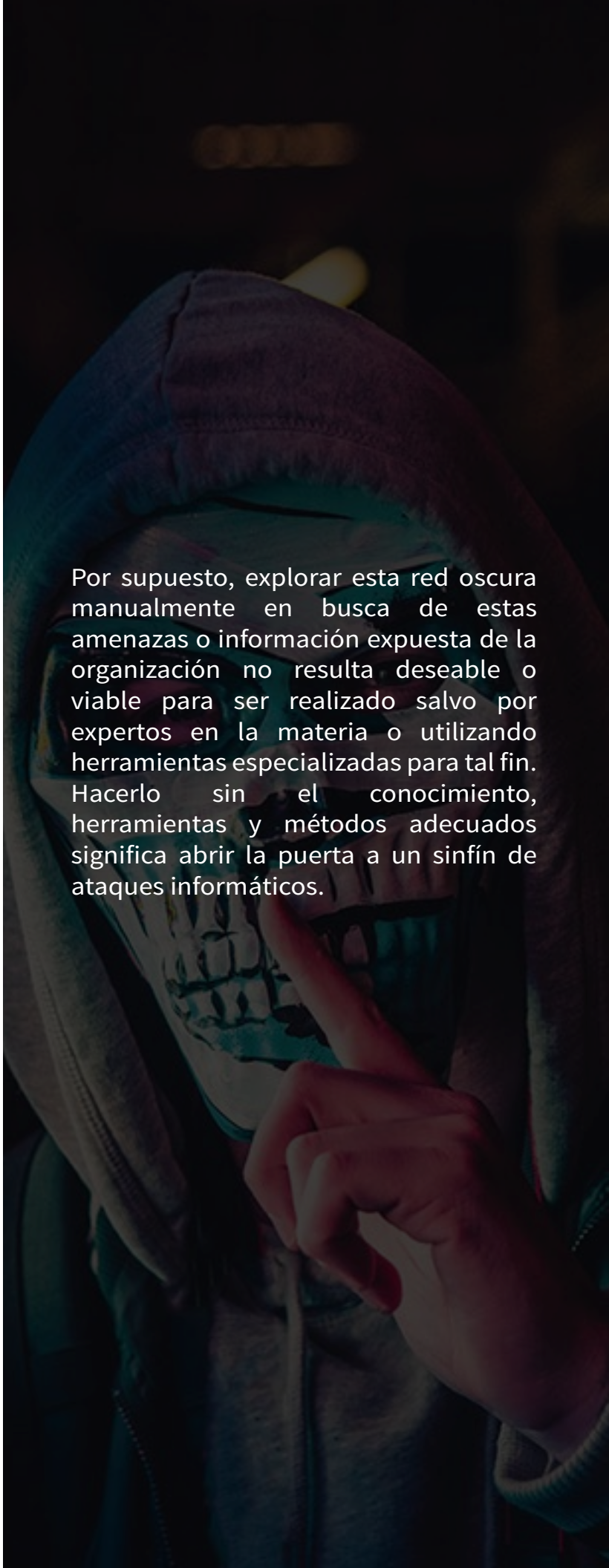
Para aquellos aspectos de la ciber inteligencia que tienen más que ver con la tecnología, como puede ser integrar una fuente de información de amenazas de seguridad con la tecnología de seguridad existente en la empresa -firewalls, IPS, IDS, antimalware, etc.- puede ser suficiente con adquirir un software, sus respectivas licencias y suscripciones y usar sus mecanismos de integración ya probados -out of the box- para comenzar a tener información que agilice y simplifique la labor de las áreas operativas de TI y seguridad. Lo mismo puede aplicar cuando la organización cuenta ya con un sistema de gestión de seguridad de la información maduro, que puede fácilmente proveer los parámetros para configurar una plataforma comercial de inteligencia de amenazas.

Por otro lado, el valor que puede entregar un proveedor de servicios se mide en referencia con su capacidad, primeramente para cerrar las brechas que existan en la implementación actual de la gestión de seguridad de la información en la organización como puede ser llevar a cabo un análisis de impacto al negocio y de riesgo, así como la evaluación del entorno de amenazas, incluyendo aquellas exógenas y previamente desconocidas, todo ello con la finalidad de establecer una línea base adecuada para comenzar a aplicar ciber inteligencia; y en segunda instancia, para soportar las tareas operativas como son el mantenimiento de los parámetros de exploración y búsqueda, los criterios y umbrales de alertamiento, los niveles de impacto y urgencia para los hallazgos generados, la evaluación de los mismos, el descarte de falsos positivos y lo más importante, la respuesta ante las amenazas confirmadas.

Un servicio administrado de inteligencia de amenazas debe tener la flexibilidad de adaptarse de forma muy específica a la exposición particular que cada organización tiene ante las amenazas informáticas. Esta exposición dependerá de diversos factores como son la popularidad de su marca, el dominio que ejerza en su ramo, el tipo de tecnologías que utiliza para soportar sus procesos de negocio, el uso que hace de recursos como sitios web públicos y aplicaciones móviles, sus prácticas de desarrollo de software, su reputación, el nivel de integración que tenga como cliente o integrante de diversas cadenas de suministro y las restricciones de seguridad que aplique a sus sistemas y usuarios, principalmente.

Por ejemplo, una empresa que basa su modelo de negocio en la generación de capital intelectual en forma de patentes a partir de una labor intensiva de investigación y desarrollo está expuesta a amenazas informáticas muy distintas a una empresa de manufactura de piezas industriales que vende por medio de la visita a sus clientes y haciendo demostraciones presenciales. Mientras que la primera debe ocuparse significativamente por proteger su información para que no sea expuesta desde los equipos de cómputo de los investigadores, al ser compartida por la red, al ser archivada o respaldada, la segunda está expuesta al delito tradicional de robo de los vehículos y de las piezas de demostración.

Bajo esta realidad, para cada empresa será de mayor o menor prioridad el explorar distintas fuentes de inteligencia como son las redes sociales, la red oscura -darknet-, la red profunda -deep web-, los mercados legales e ilegales de aplicaciones móviles, los foros de hacktivismo o las bases de datos de vulnerabilidades de los fabricantes de tecnología. Si bien puede resultar interesante en algún momento para una empresa explorar la mayoría de estas fuentes de manera inicial, para tener una línea base de exposición a amenazas, no resulta financieramente práctico ni viable hacerlo de forma permanente.



Por supuesto, explorar esta red oscura manualmente en busca de estas amenazas o información expuesta de la organización no resulta deseable o viable para ser realizado salvo por expertos en la materia o utilizando herramientas especializadas para tal fin. Hacerlo sin el conocimiento, herramientas y métodos adecuados significa abrir la puerta a un sinfín de ataques informáticos.

Por ejemplo, una empresa que haga un uso importante de aplicaciones móviles como canal de venta, seguramente podrá justificar la monitorización constante en búsqueda de clones ilegales de sus aplicaciones. Estos clones son una herramienta comúnmente utilizada por los cibercriminales para robar las credenciales de acceso de los usuarios, así como toda la información contenida en sus teléfonos móviles. Para una empresa que no cuenta con aplicación móvil alguna, este tipo de monitorización seguramente tendrá poco valor.

De esta manera el proveedor de servicios deberá contar con una oferta flexible, primero en cuanto a las distintas fuentes de inteligencia que cada uno de sus clientes pueda elegir, según los criterios antes mencionados y segundo, con respecto a la oferta de servicios complementarios que le permitan actuar en las distintas fases de identificación, protección, detección, respuesta y recuperación, ya sea llevando a cabo de manera total o parcial tareas operativas, de planeación o estratégicas en el ámbito de la seguridad de la información.

La figura 2 muestra el tipo de oferta de servicio que una empresa típicamente debe esperar de su proveedor seleccionado. En el centro aparecen las funciones básicas relacionadas con la inteligencia de amenazas, como son la parametrización de la tecnología utilizada y lo que corresponde propiamente a las tareas de gestión de eventos, todo ello llevado a cabo con una estricta alineación al contexto que se conoce de la organización, tanto en términos de su exposición a amenazas, como de su estrategia.

El siguiente nivel muestra los distintos ámbitos de exploración e investigación, donde el cliente ya tiene la primera posibilidad de elegir modularmente dependiendo de la naturaleza de su negocio y la exposición al riesgo que de ella deriva. Finalmente, en los costados se muestran servicios complementarios que el cliente podrá considerar según las capacidades con las que cuente internamente o ya entregadas por otros proveedores, del lado izquierdo se proponen servicios de índole consultiva para la estrategia de seguridad, mientras que en el derecho los que corresponden a operaciones de seguridad.

Figura 2: *Oferta esperada de un proveedor de servicios de Inteligencia de amenazas.*

Como se observa, para realmente aprovechar una práctica de inteligencia de amenazas hace falta mucho más que solo la tecnología. Se requiere el conocimiento fino de la organización para poder configurar adecuadamente la tecnología elegida, pero también se necesita saber de qué manera actuar cuando se presenten hallazgos, lo cual se fundamenta no solo en el conocimiento técnico experto, sino en la aplicación de una práctica basada en políticas, procesos, procedimientos y otras herramientas que facilite lograr el resultado.

Cuando se presenta un evento o detección es necesario tomar decisiones acerca de las acciones que deben llevarse a cabo en el ámbito de la seguridad de la información y la tecnología. ¿Es suficiente con aplicar una medida puntual de remediación? ¿Es esto posible? ¿Se requiere establecer un plan de acción para evitar que este tipo de evento se repita en el futuro? ¿Cuánto costará a la organización blindarse contra este tipo de amenaza? ¿Cómo cambia el nivel de riesgo conocido de la empresa después de lo ocurrido? ¿Es necesario hacer ajustes en la estrategia de seguridad?

Cada amenaza que es detectada puede tener ramificaciones muy variadas que van más allá de la organización misma, lo cual se traduce en un proceso complejo de toma de decisiones de negocio donde las interrogantes son del tipo ¿Quién está en riesgo además de nuestra empresa? ¿Qué tanta información de la amenaza detectada debemos compartir y con quién? ¿Cuál es el impacto potencial sobre la reputación de nuestra marca? ¿Podemos ser acreedores a algún tipo de sanción?

En el primer nivel de cuestionamientos se busca que el proveedor de servicios tenga una participación mucho mayor, que analice el impacto de una amenaza detectada, tome acciones relacionadas con la respuesta y la recuperación y también que proponga planes para la protección a partir de ese momento. En el segundo nivel, se espera que asuma el rol de asesor, proporcionando información de alto nivel para que los ejecutivos de la empresa tomen decisiones.

Como conclusión, la inteligencia de amenazas contempla todas aquellas medidas que permiten a una organización detectar de manera temprana una amenaza informática relevante y le proveen información detallada que le permite responder de manera efectiva y eficiente, minimizando el impacto; se puede afirmar que el uso de prácticas de inteligencia de amenazas está volviéndose más frecuente y está generando beneficios para quienes las utilizan, sin embargo, aprovecharlas de manera que se obtenga el máximo beneficio de ellas no es tarea fácil, requiere contar con una variedad de funciones en la organización en los niveles operativo, de planeación, gerenciales y estratégicos, así como un amplio conocimiento tanto de la empresa como del entorno de amenazas informáticas en general y el específico conforme al perfil de esta, de manera que siempre será benéfico combinar la responsabilidad entre áreas funcionales internas y un proveedor especializado que pueda brindar la amplitud en cobertura del espectro de amenazas y la profundidad en la ejecución de tareas de operación, planeación y estrategia de seguridad que sea más conveniente.