M-CIB-002
Metodología de Ciberinteligencia

Responsables

Elaboró:	Especialista de Ciberinteligencia
Revisó:	Control de Documentos
Aprobó:	Gerente de normatividad y cumplimiento

Control de versiones

Versión	Fecha	Descripción del cambio
1	29/09/2022	Emisión Inicial

Clave del formato de manual: F-SGI-004 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Introducción

Threat Intelligence se puede describir como las actividades de análisis de información sobre intentos hostiles, capacidades y oportunidades de un adversario. Esta información se usa para preparar, prevenir, e identificar ciber ataques. En el presente documento se muestra la metodología utilizada por el equipo de Ciberinteligencia de Silent4Business para ejecutar el servicio de Threat Intelligence, la cual está basada principalmente en la metodología del SANS.

Cabe mencionar que, aunque no forma parte explicita de la metodología, el equipo de Ciberinteligencia está sujeto a una retroalimentación constante por parte del cliente, así como de la alta gerencia, durante la ejecución del servicio con la finalidad de mejorar la atención o diversas prácticas.

2. Alcance

Este proceso es de uso del área de ciberinteligencia, es aplicable para servicios ejecutados a clientes externos y/o para Silent4Business.

3. Definiciones

Activo

Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza

Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque

Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Comprometer

Evasión de controles de seguridad causando posible de pérdida o daño en un activo de cómputo.

Exploit

Código o técnica que es usada por una amenaza para tomar ventaja de una vulnerabilidad.

Impacto

Medición de la consecuencia al materializarse una amenaza.

Mitigación

Acciones para remediar vulnerabilidades identificadas en los activos.

Probabilidad

Es la posibilidad que existe entre una amenaza y las variables de entorno para que una vulnerabilidad sea aprovechada.

Riesgo

Es la probabilidad de que una amenaza explote una vulnerabilidad con su correspondiente impacto al negocio.

Vulnerabilidad

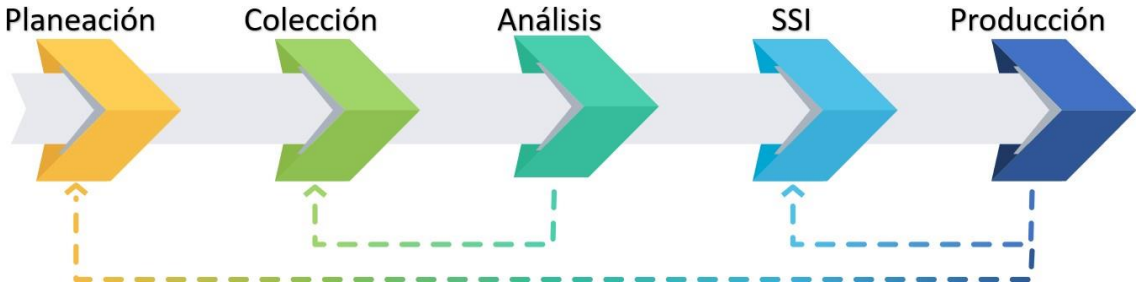
Son debilidades que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

4. Descripción del manual

La metodología de Threat Intelligence propone realizar un monitoreo y análisis integral de las posibles amenazas en el ciberespacio del cliente por lo que se comienza con una fase de planeación, donde se entiende el entorno del cliente, las necesidades y las expectativas, con el fin de identificar información que sirva en la fase de colección para para perfilar el monitoreo de posibles amenazas, internas y externas que puede tener la organización.

Posterior a la colección se procesa la información y se identifican hallazgos los cuales mediante la fase de análisis son alineados utilizando el modelo de Kill Chain y si se tiene la suficiente información validada mediante el modelo de Diamante, se generan y validan las posibles hipótesis sobre los hallazgos identificados.

Una vez validadas las posibles hipótesis se procede a almacenar y compartir la información (SSI) de amenazas confirmadas encontradas con el cliente y finalmente se realiza la producción de inteligencia mediante reportes o modelos dirigidos a personal estratégico, técnico, táctico y operacional de la organización.



A. Descripción de las fases

1. Planeación

En la fase de planeación se realizan entrevistas iniciales con personal de la organización donde se entienden sus necesidades y expectativas respecto al servicio proporcionado por el equipo de Ciberinteligencia de Silent4Business. El objetivo de estas entrevistas es extraer la información que sirva para llegar a un entendimiento del entorno del cliente, por lo que se podrá solicitar información como:

- Identificación de Activos que deben ser priorizados
- Información de Personal sensible o estratégico
- Información de Propiedad Intelectual
- Información de Negocio
- Información de Tecnología y Operación
- Adversarios identificados
- Competidores y casos de ciber espionaje
- Hacktivistas identificados
- Consumidores de Inteligencia de la organización
- Entre otros.

De manera adicional el equipo de Ciberinteligencia de Silent4Business realizara actividades de reconocimiento de la organización a través de fuentes públicas sobre infraestructura, reputación, entre otros y en conjunto con las entrevistas se podrán identificar riesgos, servicios críticos, amenazas potenciales de acuerdo con su entorno y otra información relevante que ayude a entender el entorno de la organización.
Esta información será compartida con el cliente para establecer un flujo de comunicación que permita validar la información recopilada, lo cual podrá hacerse mediante un documento o presentación de análisis de entorno donde se encuentre la información perfilada.

2. Colección

Una vez que se ha tenido el entendimiento del entorno de la organización se procede a realizar la recolección de información de acuerdo con las necesidades identificadas en la fase de Planeación. Esto se hará sobre distintas fuentes que sirvan para consolidar la búsqueda de amenazas, se podrá obtener información de feeds de inteligencia, monitoreo interno y externo, entre otros. A continuación, se describen algunos métodos de recolección de información que podrá utilizar el equipo de Silent4Business.

Recolección de información de amenazas de la región (LATAM)

Este tipo de recolección está enfocado en identificar amenazas específicas dirigidas al sector, industria y región de la organización, como campañas de ataques, desprestigio, fraude, etc. Silent4Business utiliza motores de búsqueda dentro de feeds de inteligencia, así como en foros, páginas de compartimiento de código/texto, grupos de mensajería, redes sociales, motores de búsqueda en fuentes indexada y no indexadas y otros insumos
.

Monitoreo de Amenazas Interno

Este tipo de recolección está basado en un monitoreo de amenazas interno de la organización a través de información obtenida de las siguientes fuentes:

Honeypot

El equipo de Ciberinteligencia realiza el monitoreo a través de una honeypot que podrá configurar e instalar de acuerdo con las necesidades del cliente. En caso de que este cuente con un sistema similar, se solicitará que se realice el reenvió de ciertos eventos con la finalidad de concentrarlo en un sistema integral. El almacenamiento podrá realizarse en plataformas como Elasticsearch u otro consolidador de datos
Sandbox

De igual forma que la honeypot, el equipo de Ciberinteligencia realiza el monitoreo a través de una herramienta de sandboxing que se podrá configurar e instalar de acuerdo con las necesidades del cliente. En caso de que este cuente con un sistema similar, se solicitará que se realice el reenvió de ciertos eventos con la finalidad de concentrarlo en un sistema integral. El almacenamiento podrá realizarse en plataformas como Elasticsearch u otro consolidador de datos

Tráfico interno sospechoso

Se podrá realizar el monitoreo de tráfico sospechoso mediante la recepción de tráfico interno emanado de herramientas como Firewall, IPS, SIEM, entre otros. Esta información podrá se podrá enviar a un sistema consolidador de datos para su monitoreo.

Sensor de Amenazas

En caso de que las necesidades de la organización lo requieran, se podrá realizar el monitoreo de tráfico interno a través de un sensor que permita identificar analizando tráfico específico, un modelado de amenazas, tácticas y técnicas de posibles intrusiones dentro de la institución.

Monitoreo de Amenazas Externo

Se podrá realizar un monitoreo de amenazas externo mediante búsqueda continua de información enfocada en identificar amenazas dirigidas a la organización. Silent4Business utiliza motores de búsqueda dentro de feeds de inteligencia, así como en foros, páginas de compartimiento de código/texto, grupos de mensajería, redes sociales, motores de búsqueda en fuentes indexada y no indexadas y otros insumos con el objetivo de encontrar información sobre:

- Información sensible
- Suplantación de identidad y fraude
- Daño a la reputación y protección de marca (sitios phishing, typosquatting, cybersquating)
- Exposición de Información Sensible (credenciales de acceso, bases de datos, exfiltración de información p.e. código, etc.)
- Información de publicación de datos de tarjetas de débito/crédito (sector financiero)

- Seguimiento de personal sensible
- Otros
- De igual forma se podrá realizar la recopilación de información a través de un escaneo externo de activos expuestos, por ejemplo:
- Monitoreo de vulnerabilidades de activos expuestos
- Monitoreo de reputación de sitios web expuestos

3. Análisis

Identificación de Amenaza

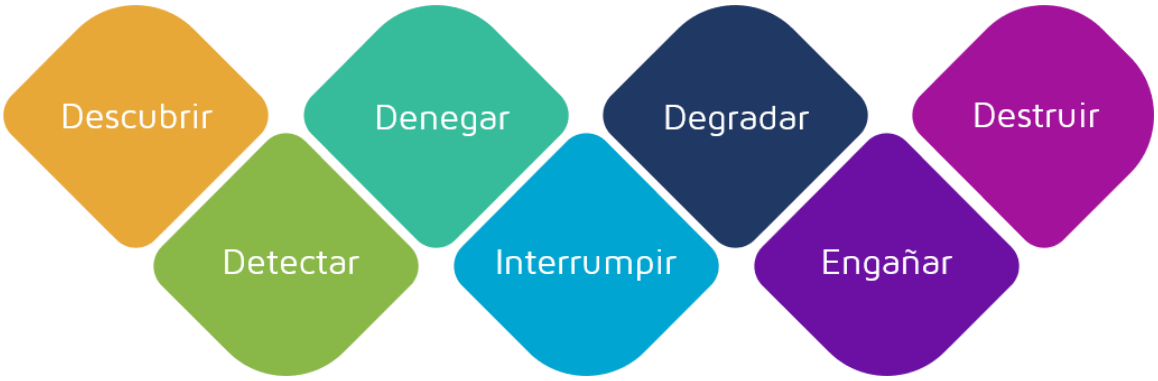
Derivado de las actividades de colección de información cubriendo los campos de visión de las posibles amenazas se procede a realizar el análisis de la información obtenida con la finalidad de identificar posibles amenazas de acuerdo con el contexto de la organización.
Cabe mencionar que el equipo de Ciberinteligencia podrá dar seguimiento a eventos o amenazas que la organización ya tenga previamente identificados.

Enriquecimiento de datos

Posterior a la identificación se realiza el enriquecimiento de información de la posible amenaza realizando técnicas de pivoting y otras durante la investigación, utilizando fuentes como:

- Fuentes OSINT
- Feeds de Inteligencia
- Búsqueda en la base integral de amenazas (Tácticas, técnicas, actores, grupos, campañas, software, herramientas, malware, etc.)
- Entre otros

Análisis de Hallazgos



Una vez que se ha realizado la investigación inicial se procede a analizar de manera concreta el posible hallazgo ubicándolo en la fase correspondiente de la cadena de progresión de amenaza (Kill Chain) así como el curso de acción que le corresponde, haciendo énfasis en recopilar la suficiente información de acuerdo con el modelo de diamante.

En esta etapa es muy importante que se realice una notificación de la posible amenaza por los medios autorizados hacia la organización, con la finalidad de que exista una comunicación fluida entre el equipo de Ciberinteligencia de Silent4Business y personal especializado de la organización como el Equipo de Respuesta a Incidentes, Threat Hunting, analistas de malware y forense, administradores de sistemas, entre otros, que puedan proporcionar información relevante para el proceso de investigación.

Generación de Hipótesis

Una vez que se ha realizado el análisis integral de la posible amenaza, se realizan una serie de hipótesis que permitan verificar la veracidad del análisis realizado. Esto se contrapone y compara con la evidencia identificada que soporte o refute cada una de las hipótesis planteadas, con el objetivo de reducir las opciones, finalmente

se realiza la priorización mediante la probabilidad de existencia de la amenaza y la significancia de la evidencia.

Cabe mencionar que las hipótesis con más soporte de evidencia se compartirán por un medio documental seguro o si la organización lo requiere, una presentación presencial de lo hallazgos recolectada en cada una de las hipótesis. Esto se hace a través de una matriz de priorización de hipótesis.

4. Store & Sharing information

Una vez que se han analizado los hallazgos, estos se categorizarán y se podrán almacenar y compartir en un software con el que cuenta Silent4Business que permite guardar casos/eventos, donde la organización también tendrá acceso. De no ser así, el equipo de Ciberinteligencia de Silent4Business realizará el compartimiento de información a la organización mediante una instancia MISP o TAXII, sin ser estas limitativas de acuerdo con las necesidades del cliente.

Es importante señalar que se puede almacenar directamente en la instancia del MISP y que en caso de que la organización requiera el compartimiento de ciertos indicadores de compromiso, campañas, etc, a otras

organizaciones, se deberá proporcionar información puntual para realizar el compartimiento de información. La información que manejará el equipo de Ciberinteligencia respecto al cliente será restringida y los avisos e información compartidos serán marcadas como TLP:AMBER o TLP:RED en caso de que así lo solicite la organización.

5. Producción

Posterior al análisis integral de los hallazgos, se procede a realizar la generación de Reportes de Inteligencia proporcionando información relevante enfocado a distintos consumidores de inteligencia de la organización, los cuales se describen a continuación:

- CTI Estratégico – Enfocado a riesgos de negocios (para entender riesgos actuales y otros que no se conocen)
- CTI Táctico – Enfocado a Incident Handler (TTPs – herramientas y metodologías – Modus Operandi)
- CTI Operacional – Enfocado a Threat Hunters (información de ataques entrantes específicos, naturaleza del ataque, identidad, capacidades, etc.)
- CTI Técnica – Enfocado a administradores de sistemas (información como hashes, IPs)

Cabe mencionar que se realizará un entregable mensual respecto a los hallazgos identificados y el proceso de análisis que se tuvo de cada uno de ellos, colocando mayor énfasis en las amenazas, donde se mostrará, además, información de las hipótesis descartadas e información enfocadas a los consumidores de inteligencia de la organización.

5. Anexos

NA