Ciberinteligencia

Encuentre amenazas en el ciber espacio antes de que afecten el activo más valioso de su Empresa: su información

La ciberinteligencia se centra en lo que sucede fuera de su red, es decir, en el monitoreo de fuentes abiertas como la Deep Web, Dark Web y el Internet de las Cosas. Para ello se utilizan diversos mecanismos, con el fin de identificar y anticiparse a las posibles amenazas.

Caracteristicas

Cuando un ciberactor efectúa una ataque utilizando técnicas avanzadas, investiga a la organización víctima a través de información pública disponible en redes sociales, noticias, blogs y foros. Asimismo, realiza una búsqueda de sus equipos conectados al cibersepacio, para la cual utiliza herramientas de monitoreo del Internet de las cosas (IoT por sus siglas en inglés).

A partir de la inteligencia recolectada, los atacantes diseñan las acciones que llevarán a cabo para perpetrar el ataque informático (operaciones conocidas como campaña), así como las ciberarmas con las que atacarán los puntos más vulnerables de la organización evadiendo los mecanismos de defensa.

Nuestro servicio de Ciberinteligencia permite a su Empresa tener la visibilidad de:

- Amenazas de ataques de denegación de servicio (DDoS).
- Posibles modificaciones no legítimas de sitios Web
- Fugas de información confidencial hacia sitios públicos.
- Sitios web apócrifos de su organización, probablemente vinculados con phishing, así como el monitoreo de su marca.
- Campañas en contra de su organización.
- Venta de información relevante de su organización en algún mercado negro de la Dark Web.

BENEFICIOS PARA SU EMPRESA

✓ **Tome mejores decisiones.** Ante un incidente de seguridad, su equipo de TI estará mejor informado y preparado para proceder.

✓ **Optimice su presupuesto en Ciberseguridad.** Mejore sus estrategias e inversiones, dando prioridades de acuerdo a los riesgos.

✓ **Evite daños en la imagen y reputación de su Empresa.** Anticipe ataques y descubra vulnerabilidades en forma proactiva.

Para mayor información contacte a su Ejecutivo de Cuenta, visite telmex.com/ciberseguridad

TELMEX® está contigo

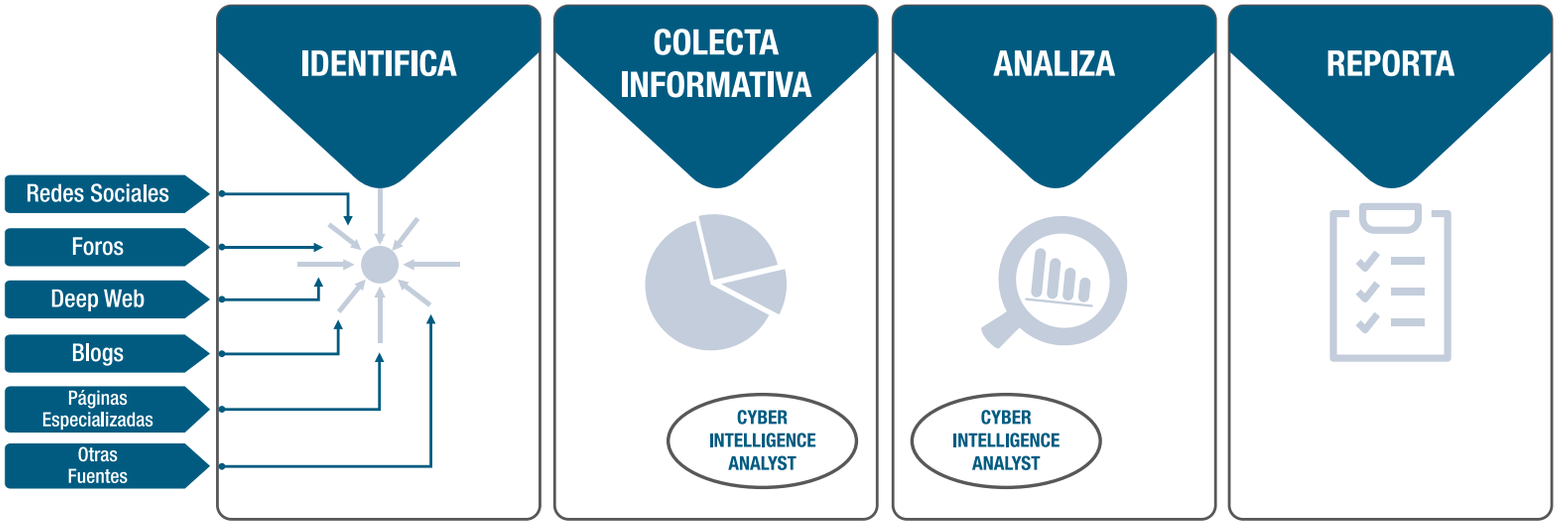
Funcionalidades

Nuestro servicio opera fuera de la organización, por lo que no es necesario instalar ninguna solución en el centro de datos del cliente. Sólo se requiere aplicar un cuestionario que permite ajustar los filtros de investigación y, una vez recibido, en menos de 24 horas el CyberSecurity Center (CSC) comienza a realizar las siguientes funciones:

- **Durante el monitoreo**, nuestro equipo de ciberinteligencia desarrolla un análisis geopolítico, económico y social para determinar cómo influye el comportamiento de los atacantes en el sector, sus objetivos y sus métodos. De esta forma, cuando se emite una alerta, se obtiene una visibilidad profunda de los posibles intereses detrás de las actividades detectadas, lo que ayuda a identificar si una alerta está relacionada con alguna anomalía y a determinar el nivel de criticidad de los eventos.

- **Durante el proceso de respuesta a incidentes**, la ciberinteligencia ayuda en la definición de las estrategias a ejecutar para responder oportunamente a la intrusión, así como a identificar áreas de oportunidad para mejorar el nivel de protección de la organización.

Esquema del Servicio



El Cyber Security Center (CSC) realiza un análisis en el que se determina la ciberhuella y el nivel de exposición del cliente de acuerdo al contexto global y particular.

Utilizando diversas disciplinas de colección de inteligencia (OSINT, SINGINT, GEOINT y Virtual HUMINT) se recaba información de distintas procedencias tales como fuentes abiertas, señuelos colocados en el ciberespacio, mecanismos de geolocalización y la obtención de información en lo más profundo de la red.

Se examina la información recolectada con base en una metodología rigurosa, plataformas tecnológicas avanzadas, redes de vínculos descubiertas y el contexto particular del cliente, para determinar el impacto de los hallazgos detectados por nuestros analistas de ciberinteligencia.

Se reportan telefónica y electrónicamente (vía correo) los hallazgos identificados. Dichos reportes incluyen recomendaciones específicas sobre las posibles vertientes del ataque, la campaña y el supuesto ciberactor detrás de la misma, lo que se traduce en inteligencia accionable para la organización.

14/DTSHEETAMENAZASAV-NAL/0218-V2