Ciberinteligencia como paso previo a la ciberseguridad

La **ciberinteligencia** es el proceso mediante el cual se recopilan, contrastan y analizan datos relacionados con amenazas digitales para transformarlos en conocimiento útil. Su finalidad es comprender qué riesgos pueden afectar a una organización, qué actores podrían estar implicados, qué métodos utilizan y qué medidas conviene adoptar antes de que se produzca un incidente.

Un dato aislado no constituye inteligencia. Una dirección IP, un dominio sospechoso o un intento fallido de acceso únicamente adquieren valor cuando se relacionan con su contexto. Es necesario comprobar su procedencia, actualidad, fiabilidad y conexión con otros indicios. La ciberinteligencia permite pasar de la acumulación de alertas a una valoración razonada de la amenaza.

La relación entre ciberinteligencia y ciberseguridad puede resumirse de la siguiente manera:

- La **ciberinteligencia** identifica, interpreta y anticipa amenazas.
- La **ciberseguridad** aplica medidas para prevenirlas, detectarlas, contenerlas y responder ante ellas.

Por ejemplo, la detección de campañas de suplantación dirigidas contra empresas de un sector puede justificar la actualización de filtros de correo, la revisión de procedimientos de pago y la formación del personal. La inteligencia obtenida orienta las decisiones de protección.

El ciclo de inteligencia

La producción de ciberinteligencia sigue un proceso ordenado conocido como **ciclo de inteligencia**:

Fase	Actuaciones principales
Dirección y planificación	Definir qué se necesita conocer y para qué se utilizará la información.
Obtención	Recopilar datos procedentes de fuentes internas y externas.
Procesamiento	Ordenar, depurar, clasificar y normalizar los datos.
Análisis	Relacionar indicios, identificar patrones y valorar hipótesis.

Difusión	Comunicar los resultados a las personas responsables.
Evaluación	Comprobar la utilidad del análisis y detectar nuevas necesidades.

La primera fase evita recoger información sin una finalidad concreta. Una organización puede plantear preguntas como las siguientes:

- ¿Qué fraudes están afectando a empresas de nuestro sector?
- ¿Se están utilizando dominios similares al de la organización?
- ¿Qué vulnerabilidades afectan a los sistemas instalados?
- ¿Existen credenciales corporativas expuestas?
- ¿Qué activos serían más atractivos para un atacante?
- ¿Qué indicadores permitirían detectar la amenaza con rapidez?

Las respuestas obtenidas deben contribuir a una decisión. Un informe que enumera numerosos datos técnicos, pero no explica su importancia ni propone prioridades, tiene una utilidad limitada.

Fuentes de información

La ciberinteligencia combina datos procedentes de distintas fuentes. La información interna permite conocer lo que ocurre dentro de la organización, mientras que las fuentes externas ayudan a comprender amenazas desarrolladas en otros entornos.

- **Fuentes internas:**

Entre las principales fuentes internas se encuentran:

  - Registros de acceso.
  - Alertas de seguridad.
  - Incidentes anteriores.
  - Correos fraudulentos recibidos.
  - Consultas de dominios.
  - Registros de firewall y redes.
  - Informes de vulnerabilidades.
  - Comunicaciones del personal.
  - Accesos físicos a zonas restringidas.
  - Información de proveedores y sistemas.

Los incidentes anteriores permiten detectar patrones. Si varios intentos de fraude utilizan el nombre del mismo directivo, el mismo tipo de urgencia y dominios muy parecidos, es posible que formen parte de una campaña dirigida.

- **Fuentes externas:**

Pueden utilizarse fuentes como:

  - Comunicados de organismos especializados.
  - Informes de amenazas.
  - Bases de datos de vulnerabilidades.
  - Publicaciones de fabricantes.
  - Repositorios de indicadores.
  - Medios de comunicación.
  - Sitios web y redes sociales.
  - Comunidades técnicas.
  - Información proporcionada por otras organizaciones.

La **inteligencia de fuentes abiertas**, conocida como OSINT, utiliza información accesible públicamente. El carácter público de una fuente no permite emplear sus datos sin límites. Deben respetarse la protección de datos, la intimidad, las condiciones de acceso y la finalidad profesional de la investigación.

Niveles de ciberinteligencia

La información puede adaptarse a diferentes necesidades:

- **Inteligencia estratégica.** Analiza tendencias, sectores afectados, motivaciones y posibles impactos a medio o largo plazo. Ayuda a decidir inversiones, políticas y prioridades.
- **Inteligencia táctica.** Estudia los procedimientos y técnicas empleados por los actores de amenaza. Permite mejorar los controles y preparar la respuesta.
- **Inteligencia operativa.** Se centra en campañas concretas, objetivos, periodos de actividad y posibles actuaciones próximas.
- **Inteligencia técnica.** Incluye datos específicos como direcciones IP, dominios, archivos, valores hash o patrones de tráfico.

La inteligencia técnica puede aplicarse rápidamente en sistemas defensivos, pero suele perder vigencia antes que la estratégica. Una dirección utilizada en un ataque puede abandonarse en pocas horas, mientras que una técnica de engaño puede mantenerse durante meses.

Indicadores de compromiso

Los **indicadores de compromiso** son datos que pueden estar relacionados con una actividad maliciosa. Algunos ejemplos son:

- Dominios creados para imitar a una empresa.
- Direcciones IP relacionadas con ataques.
- Valores hash de archivos maliciosos.
- Nombres de archivos sospechosos.
- Intentos de acceso desde ubicaciones anómalas.
- Cuentas creadas sin autorización.
- Conexiones con servicios no habituales.
- Cambios inesperados de permisos.

Un indicador no demuestra por sí mismo que exista un ataque. Puede estar desactualizado, corresponder a un servicio compartido o producir una coincidencia legítima. Antes de bloquear una dirección o atribuir una conducta, deben contrastarse su fiabilidad y su contexto.

Evaluación de las fuentes

La calidad del análisis depende de la calidad de la información utilizada. Cada fuente debe valorarse atendiendo a varios criterios:

- **Fiabilidad:** historial y credibilidad de la fuente.
- **Actualidad:** fecha de obtención y posibilidad de que el dato haya cambiado.
- **Exactitud:** coincidencia con otras fuentes.
- **Relevancia:** relación con la necesidad planteada.
- **Contexto:** circunstancias en las que se obtuvo.
- **Integridad:** ausencia de alteraciones conocidas.
- **Sesgo:** intereses o limitaciones de quien proporciona la información.

Cuando dos fuentes ofrecen datos diferentes, no debe elegirse automáticamente la información que confirma la primera hipótesis. La discrepancia debe documentarse y analizarse.

Análisis de amenazas

El análisis puede organizarse alrededor de cuatro elementos:

1. **Actor de amenaza.** Persona o grupo con capacidad e intención de causar un daño.
2. **Capacidad.** Conocimientos, herramientas, accesos e infraestructuras disponibles.
3. **Oportunidad.** Vulnerabilidades o condiciones que facilitan la actuación.
4. **Intención.** Finalidad económica, ideológica, personal, estratégica o destructiva.

También deben valorarse los activos que podrían resultar afectados:

- Información personal.
- Credenciales.
- Datos financieros.
- Propiedad intelectual.
- Sistemas de control.
- Servicios esenciales.
- Reputación.
- Continuidad de la actividad.

Una amenaza adquiere mayor prioridad cuando coincide con un activo valioso, una vulnerabilidad real y una capacidad suficiente para aprovecharla.

De la inteligencia a las medidas de ciberseguridad

La ciberinteligencia debe traducirse en decisiones concretas. Entre sus aplicaciones se encuentran:

- Actualizar reglas de detección.
- Bloquear dominios maliciosos confirmados.
- Corregir vulnerabilidades prioritarias.
- Revisar cuentas y permisos.
- Reforzar controles de acceso.
- Adaptar la formación del personal.
- Comprobar procedimientos de pago.
- Vigilar activos especialmente expuestos.
- Preparar protocolos ante campañas conocidas.
- Informar a las personas que pueden ser objetivo de un engaño.

La prioridad no debe depender únicamente de la gravedad técnica de una vulnerabilidad. También deben considerarse la exposición del sistema, el valor de la información, la existencia de ataques activos y las consecuencias para la organización.

Límites profesionales y jurídicos

La obtención de información debe realizarse mediante fuentes y procedimientos autorizados. La búsqueda de inteligencia no justifica:

- Acceder a cuentas ajenas.
- Interceptar comunicaciones.
- Utilizar credenciales filtradas.
- Entrar en sistemas externos.
- Suplantar identidades.
- Descargar información ilícita.
- Instalar programas sin autorización.
- Difundir datos personales o sensibles.

La información debe compartirse aplicando el criterio de **necesidad de conocimiento**. Un indicador técnico puede distribuirse entre los equipos responsables, mientras que los datos de víctimas o personas sospechosas deben limitarse a quienes necesiten utilizarlos.

EJEMPLO PRÁCTICO — Campaña de suplantación dirigida al departamento financiero.

Una empresa detecta tres correos dirigidos al personal de administración. Los mensajes aparentan proceder de la dirección y solicitan realizar transferencias urgentes. Se han enviado desde dominios creados mediante pequeñas variaciones del nombre corporativo.

El análisis permite identificar varios elementos comunes:

- Los dominios se registraron pocos días antes.
- Los mensajes se enviaron al final de la jornada.
- Se utilizan nombres reales de personas directivas.
- Se solicita evitar el procedimiento habitual de comprobación.
- Las cuentas bancarias pertenecen a entidades distintas de las utilizadas normalmente.

La información indica la existencia de una campaña dirigida y no de correos aislados. A partir de este análisis, la empresa bloquea los dominios confirmados, informa al personal financiero, revisa el procedimiento de transferencias y establece una verificación mediante un segundo canal.

La ciberinteligencia ha permitido identificar el patrón y orientar las medidas de ciberseguridad antes de que se produzca una pérdida económica.

ACTIVIDAD 1

Relaciona cada concepto con su definición.

1. Inteligencia estratégica.
2. Indicador de compromiso.
3. OSINT.
4. Inteligencia táctica.
5. Ciclo de inteligencia.
6. Necesidad de conocimiento.

A. Información técnica que puede estar vinculada con una actividad maliciosa.

B. Proceso ordenado de planificación, obtención, análisis y difusión.

C. Información procedente de fuentes abiertas.

D. Análisis de tendencias y riesgos a medio o largo plazo.

E. Criterio que limita el acceso a la información a las personas que la necesitan.

F. Conocimiento sobre técnicas y procedimientos utilizados en los ataques.

ACTIVIDAD 2

Una organización recibe una alerta indicando que una dirección IP está relacionada con actividades maliciosas. El responsable propone bloquearla inmediatamente en todos los sistemas.

Responde:

1. ¿Qué aspectos deberían comprobarse antes de aplicar el bloqueo?
2. ¿Por qué una dirección IP no demuestra por sí sola la existencia de un ataque?
3. ¿Qué fuentes internas podrían consultarse?
4. ¿Qué consecuencias podría producir un bloqueo incorrecto?
5. ¿Cómo debería documentarse la decisión?

ACTIVIDAD 3

Clasifica cada elemento como fuente interna, fuente externa o medida de ciberseguridad derivada del análisis.

1. Registros de inicio de sesión.
2. Informe publicado por un organismo especializado.
3. Bloqueo de un dominio fraudulento.
4. Correos sospechosos recibidos por el personal.
5. Base de datos pública de vulnerabilidades.
6. Revisión de los permisos de administración.
7. Registro de accesos a una sala técnica.
8. Informe de amenazas elaborado por un proveedor.
9. Actualización de una regla de detección.
10. Formación específica sobre una campaña de fraude.