

CYBER THREAT INTELLIGENCE

La importancia de la Ciberinteligencia para tus procesos de Ciberseguridad

La Ciberinteligencia tiene el potencial de ayudar a **identificar, comunicar y reducir el riesgo en tu organización, si se habilita en todos los equipos funcionales existentes.**



Prevención

- ↑ Aumento de los bloques preventivos.
- ↑ Incremento del número e impacto de los parches priorizados.



Detección

- ↑ Incremento del número de detecciones y alertas positivas.
- ↓ Reducción del tiempo empleado por alerta.
- ↓ Decremento del número de falsos positivos.



Respuesta

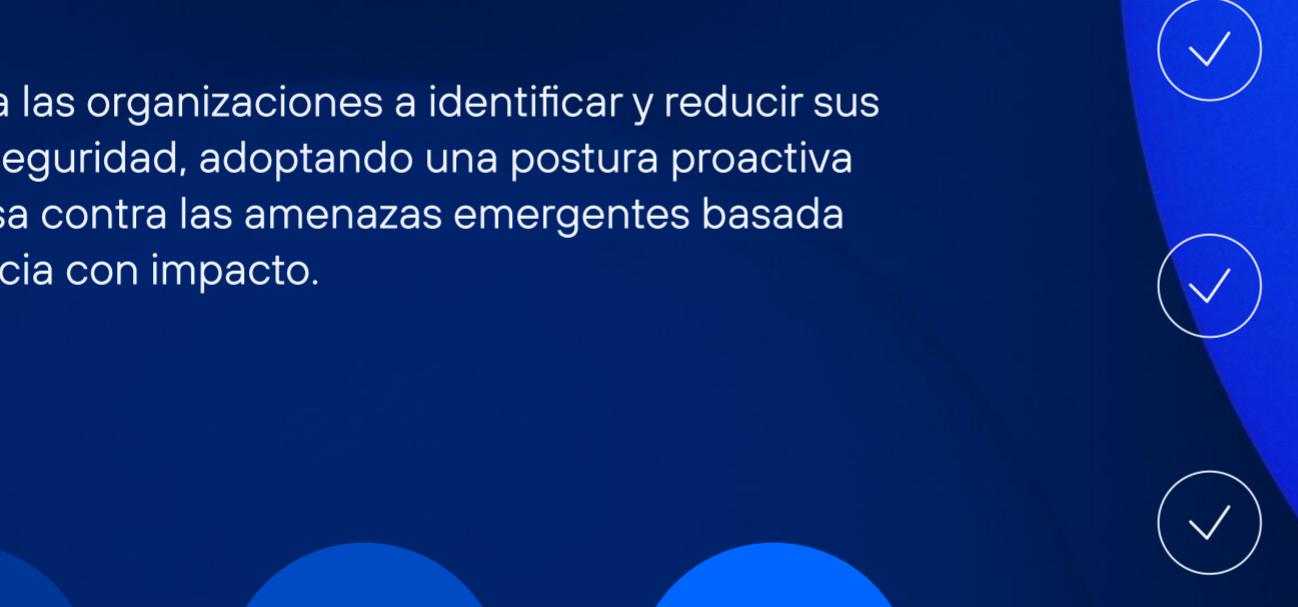
- ↑ Aumento del número de incidentes descubiertos.
- ↓ Reducción del tiempo medio de detección (MTTD).
- ↓ Reducción del tiempo medio de remediación (MTTR).

¿A qué desafíos se enfrentan las empresas?

La ciberseguridad ya no es un problema técnico, sino un desafío de negocio. Esto hace necesario hacer frente a las ciberamenazas de una manera eficaz y rentable.



¿Cómo ayuda la Ciberinteligencia a las empresas?



Nuestra propuesta de valor

Ayudamos a las organizaciones a identificar y reducir sus riesgos de seguridad, adoptando una postura proactiva en la defensa contra las amenazas emergentes basada en inteligencia con impacto.

- Arroja luz sobre lo desconocido, obteniendo una amplia visión del panorama de amenazas de tu organización.

- Ayuda a los stakeholders a invertir de forma inteligente, mitigar el riesgo, ser más eficientes y tomar decisiones más rápidas.

- Prepara y protege tu empresa de forma proactiva, con visibilidad de las tendencias, los actores y sus motivaciones y TTPs.

- Accede a un completo portafolio diseñado para reajustar la mentalidad de seguridad a la de un atacante.

¿Cuál es nuestro enfoque según el tipo de cliente?

ATTACK SURFACE MANAGEMENT

Obtén una visibilidad completa de tus activos de cara al exterior e identifica posibles vectores de ataque.

1. Descubrimiento
2. Contextualización
3. Evolución continua
4. Priorización
5. Remediation

DIGITAL RISK PROTECTION

Descubre amenazas dirigidas que tienen lugar más allá de tu perímetro interno.

- Protección de marca, contra el fraude, de infraestructura IT y de VIPs.
- Takeover del contenido fraudulento y minimizar el riesgo de contramedidas para minimizar el riesgo (bloqueo en navegadores de smishing, red y dispositivos móviles en emisores de smishing).

THIRD-PARTY RISKS

Mide y controla de manera continua los controles de seguridad de terceros para alinearnos con tu tolerancia al riesgo.

- Evaluación de proveedores.

- Monitoreo continuo.

- Garantía efectiva.

COUNTER-INTELLIGENCE

Da un paso adelante en la defensa activa con campañas de engaño para detectar los ataques en sus fases iniciales.

1. Detectar y desviar adversarios.
2. Recoger el comportamiento de amenazas.
3. Controlar el comportamiento del adversario.
4. Contar con el comportamiento del adversario para remediar la amenaza.

THREAT INTELLIGENCE

Obtén información basada en datos sobre amenazas emergentes que pueden darse contra tu organización.

- Inteligencia táctica.

- Inteligencia operativa.

- Inteligencia estratégica.

INTELIGENCIA A MEDIDA

Una solución a medida para satisfacer tus necesidades específicas de inteligencia.

- Equipo dedicado.
- Ubicación de los analistas y cobertura horaria personalizables.
- Amplia cobertura de riesgos.
- Entregables a medida basados en tus necesidades.