FICHA TÉCNICA

STYX INTELLIGENCE

Protección Contra Riesgos Digitales y Cibernéticos Externos

Proteja la marca, las personas y la infraestructura digital de su organización contra las amenazas cibernéticas.

El riesgo cibernético ya no empieza ni termina dentro del firewall. Hoy, hackers apuntan a lo que está fuera de él: su marca, sus ejecutivos, sus dominios, su presencia en redes sociales, sus proveedores y cualquier activo digital que esté expuesto públicamente.

El Panorama Ha Cambiado

Las organizaciones han pasado años fortaleciendo sus defensas internas. Han invertido en seguridad de redes, gestión de vulnerabilidades, controles de correo electrónico y herramientas de identidad para proteger la infraestructura principal. Sin embargo, los cibercriminales se han adaptado.

En lugar de intentar hackear sistemas internos, buscan caminos más fáciles. Apuntan a activos y entornos fuera del perímetro tradicional, donde la visibilidad es limitada y las responsabilidades no siempre están claras.

La Huella Digital Se Ha Expandido

La huella digital ahora incluye activos expuestos al público, dominios, sitios web, infraestructura en la nube, cuentas de redes sociales, aplicaciones móviles, proveedores externos, credenciales expuestas, identidades de ejecutivos y más.

Gran parte de esta huella existe fuera de los controles de seguridad directos, cambia constantemente y se extiende por canales sobre los que los equipos de seguridad no tienen visibilidad. Esto crea más oportunidades para que los cibercriminales identifiquen brechas, suplanten identidades de confianza y se aprovechen de la información pública.

La Brecha de Visibilidad

Los equipos de seguridad pueden tener una cobertura sólida dentro del firewall, pero las amenazas externas están dispersas en fuentes, equipos y flujos de trabajo distintos y desconectados.

- Los activos desconocidos (shadow IT) permanecen expuestos, creando puntos ciegos.
- El uso indebido y la suplantación de marca fuera del monitoreo SOC.
- La suplantación de identidad de ejecutivos en redes sociales.
- La información en silos, lo que impide tener una visión unificada de todas las amenazas externas de la empresa.
- Las credenciales filtradas o comprometidas que se descubren después de que han sido vendidas o utilizadas.

Visibilidad Continua

Hoy, los cibercriminales se aprovechan de lo que pueden ver y alcanzar desde el exterior, creando nuevas vías para el fraude, la suplantación y el compromiso de la organización.

Las organizaciones necesitan visibilidad continua sobre estas amenazas externas para entender cómo se va acumulando el riesgo en su marca, sus ejecutivos, su ecosistema de proveedores y su identidad.

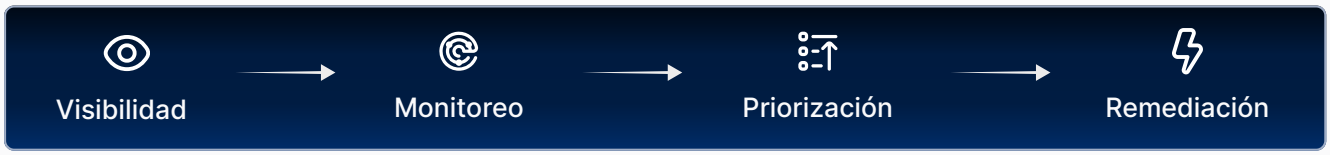
Esta visibilidad sienta las bases para el monitoreo, la priorización y la respuesta y mitigación de riesgos.

> "La ciberseguridad ya no consiste en construir un muro más alto. Consiste en tener visibilidad de lo que está ocurriendo fuera de esos muros... en tener visibilidad fuera del perímetro."

STYX INTELLIGENCE

El Framework de Styx

El framework de Styx ofrece un enfoque continuo para gestionar el riesgo digital externo a través de cuatro etapas conectadas: Visibilidad, Monitoreo, Priorización y Remediación.



Un ciclo continuo para identificar, evaluar e interrumpir el riesgo digital externo.

StyxScout

- Descubrimiento de activos
- Monitoreo de marca y suplantación
- Descubrimiento de amenazas contra ejecutivos
- Monitoreo y detección de amenazas de terceros
- Detección de exposición de credenciales

StyxGuard

- Correlación de riesgos y enriquecimiento de contexto de hallazgos
- Priorización de amenazas
- Priorización y calificación de riesgo (Digital Risk scoring)

StyxRemediation

- Servicio gestionado de takedowns
  - Automatizado en la plataforma
  - A través del equipo de soporte

Áreas Principales de la Solución

Styx ofrece una plataforma unificada, integral e impulsada por IA para la protección contra riesgos digitales y cibernéticos externos, diseñada para responder a las necesidades críticas de riesgo de una organización.

✓ Monitoreo de Marca

Visibilidad y monitoreo del abuso de marca en canales externos, incluyendo suplantación, dominios falsos o similares, aplicaciones fraudulentas.

✓ Protección de Ejecutivos

Visibilidad y monitoreo de amenazas a ejecutivos, incluyendo suplantación, exposición en la dark web, sentimiento online y señales de intentos de doxing.

✓ Monitoreo de Redes Sociales

Monitoreo de redes sociales y fuentes de noticias para detectar suplantación, abuso de la marca, fraude y narrativas dañinas que afecten a su empresa.

✓ Gestión del Riesgo de Terceros

Monitoreo de riesgos externos vinculados a proveedores, cadena de suministro y terceros, incluyendo exposición y otros riesgos cibernéticos.

✓ Servicios de Takedown

Acción frente a amenazas externas mediante takedowns automatizados y flujos de trabajo de interrupción diseñados para reducir la exposición.

✓ EASM

Visibilidad de activos expuestos e infraestructura desconocida (shadow IT); monitoreo de los cambios a lo largo del tiempo y priorización de acciones.

✓ Monitoreo de la Dark Web

Monitoreo de la dark web, sitios de filtraciones y datos expuestos para identificar credenciales robadas y exposición relacionada con hackeos.

✓ Inteligencia de Amenazas

Conversión de señales externas en inteligencia práctica conectando la actividad de amenazas, añadiendo contexto y mejorando la priorización.

✓ Seguridad Contra la Desinformación

Visibilidad y monitoreo de narrativas falsas o manipuladas (incluyendo cómo se propagan) y campañas dirigidas a su marca, sus ejecutivos o su identidad.

✓ Digital Risk Scorecard

Puntuación de riesgo para priorizar amenazas externas, realizar seguimiento de la exposición general y facilitar el enfoque de su equipo.

Conecta con nosotros