DATASHEET

FORXITE

CIBERINTELIGENCIA

Inteligencia estratégica para anticipar, contextualizar y priorizar amenazas digitales

El panorama de amenazas digitales es complejo, global y en constante evolución. Los actores combinan vulnerabilidades explotables, infraestructura distribuida, accesos comprometidos y factores geopolíticos para seleccionar objetivos y maximizar impacto.

Al mismo tiempo, los equipos de seguridad reciben grandes volúmenes de información fragmentada. Indicadores técnicos sin contexto, vulnerabilidades priorizadas solo por severidad y eventos internacionales cuya relación con el riesgo digital no siempre es evidente dificultan la toma de decisiones oportunas.

La ciberinteligencia efectiva integra amenazas, exposición técnica y contexto estratégico para identificar qué riesgos son realmente relevantes para la organización y cómo deben priorizarse.

Cobertura de Inteligencia

Inteligencia de Amenazas

Perfilado de actores, campañas, infraestructura y tácticas para anticipar comportamiento adversario relevante.

Inteligencia de Vulnerabilidades

Priorización basada en explotación activa, exposición real y riesgo contextual, más allá del CVSS.

Inteligencia Geopolítica

Análisis de eventos regionales y tensiones que incrementan riesgo digital por país, industria o sector estratégico.

DarkOps & Monitoreo de Filtraciones

Seguimiento continuo de foros, espacios cerrados y sitios de ransomware para detectar filtraciones, menciones y exposición de datos vinculados a la organización.

Tendencias y Señales Tempranas

Identificación de patrones emergentes antes de que se traduzcan en incidentes.

Forxite monitorea de forma continua:

- Sitios de publicación de ransomware
- Foros especializados en filtración de datos
- Mercados ilícitos y espacios cerrados
- Conversaciones relacionadas con accesos iniciales comprometidos
- Publicaciones vinculadas a industrias específicas

Además, analizamos la autenticidad, alcance y potencial impacto de cada hallazgo antes de reportarlo. Esto permite detectar exposición temprana y reducir incertidumbre ante eventos críticos.

CÓMO OPERAMOS

- Definimos contexto organizacional y activos críticos.
- Recolectamos señales técnicas, estratégicas y geopolíticas de múltiples fuentes.
- Correlacionamos amenazas, vulnerabilidades y exposición en entornos clandestinos.
- Validamos y priorizamos según impacto real.
- Entregamos inteligencia estructurada para equipos técnicos y ejecutivos.

ENTREGABLES

- Alertas contextuales (técnicas y ejecutivas) según criticidad.
- Informes periódicos de inteligencia (amenazas, vulnerabilidades, geopolítica).
- Briefs de situación para incidentes, campañas activas o eventos geopolíticos relevantes.
- Soporte analítico para priorización y toma de decisión.

IMPACTO OPERATIVO

✓ Anticipación de campañas relevantes
✓ Priorización real de vulnerabilidades explotables
✓ Detección temprana de filtraciones y ransomware
✓ Mejor alineación entre riesgo geopolítico y ciberseguridad
✓ Reducción de ruido y foco en amenazas relevantes

CASOS DE USO

- ¿Qué actores están atacando mi industria y con qué tácticas?
- ¿Qué vulnerabilidades tienen mayor probabilidad de explotación en mi contexto?
- ¿Cómo cambia mi exposición por eventos geopolíticos o tensiones regionales?
- ¿Qué infraestructura, dominios o patrones conviene bloquear/monitorear?
- ¿Cómo justificar prioridades de ciberseguridad con evidencia externa?