



OVERVIEW

THREAT INTELLIGENCE

Feeds y reportes de inteligencia únicos,
elaborados por expertos líderes de la industria

Progress. Protected.

¿Por qué añadir ESET a tu stack de CTI?

Comprender el panorama de amenazas actual y las tácticas que emplean los cibercriminales te otorga una ventaja de conocimiento crucial. Esta visión permite que tu organización fortalezca sus sistemas de defensa internos de manera eficaz. Los datos de inteligencia de alta calidad son la piedra angular de cualquier estrategia de inteligencia de ciberamenazas (CTI) robusta.

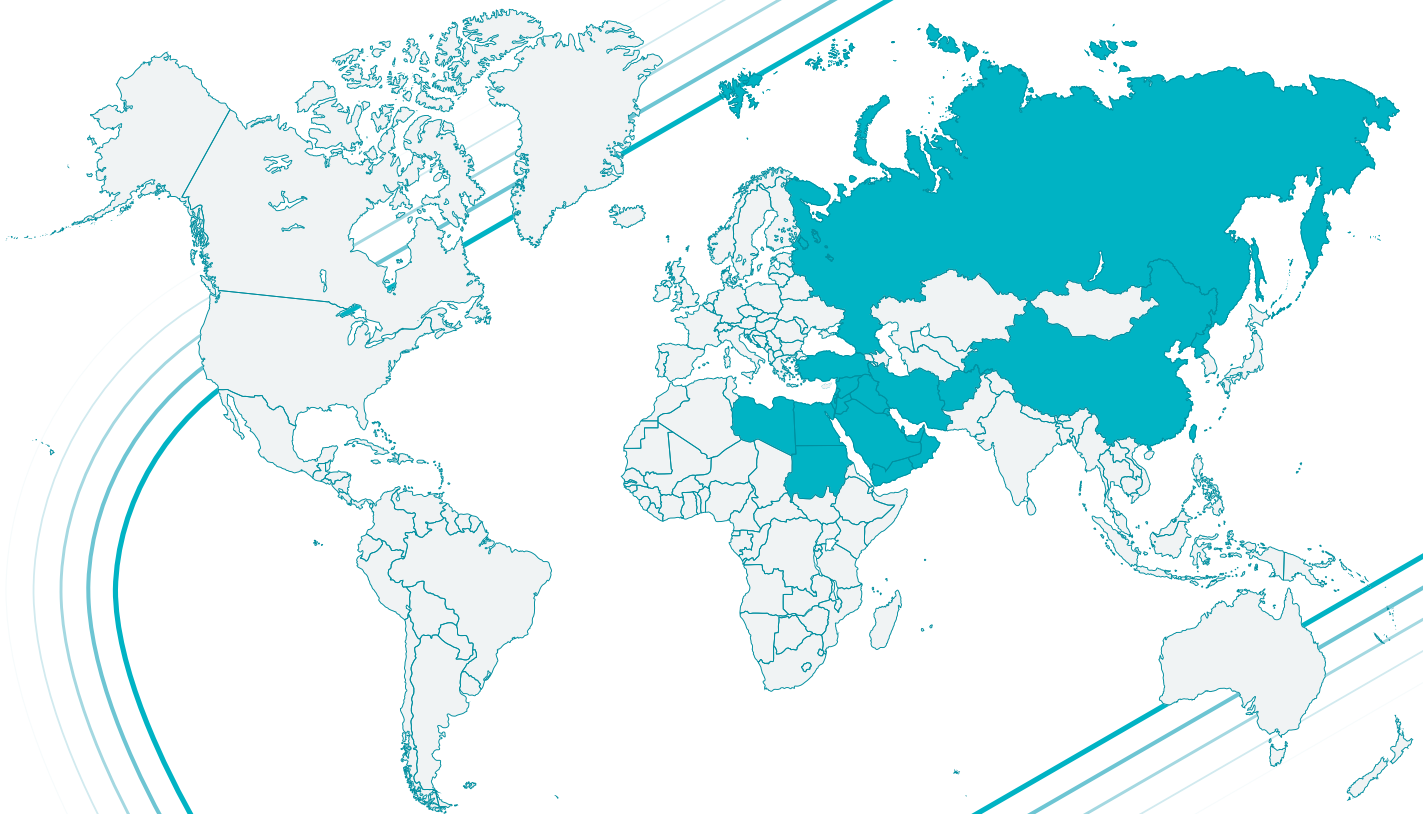
Durante más de 35 años, ESET ha sido una empresa privada, sin deudas y en constante crecimiento. Nuestro éxito se basa en un enfoque de “prevención primero”, impulsado por IA y potenciado por la experiencia humana. En el corazón de nuestras operaciones se encuentra nuestra exclusiva Inteligencia Global de Amenazas, respaldada por una amplia red de I+D liderada por investigadores reconocidos en el sector.

Nos tomamos el tiempo necesario para entender realmente las ciberamenazas, lo que nos permite defendernos de ellas con eficacia.

No importa qué tan avanzadas sean tus soluciones actuales de CTI, integrar ESET en tu stack te aportará un valor inigualable. Nuestros completos feeds de inteligencia de amenazas, informes de APT e informes de eCrime te aseguran ir un paso por delante de las amenazas emergentes, reforzando tus defensas existentes con información accionable e investigación de vanguardia.

Aprovecha la telemetría única de ESET

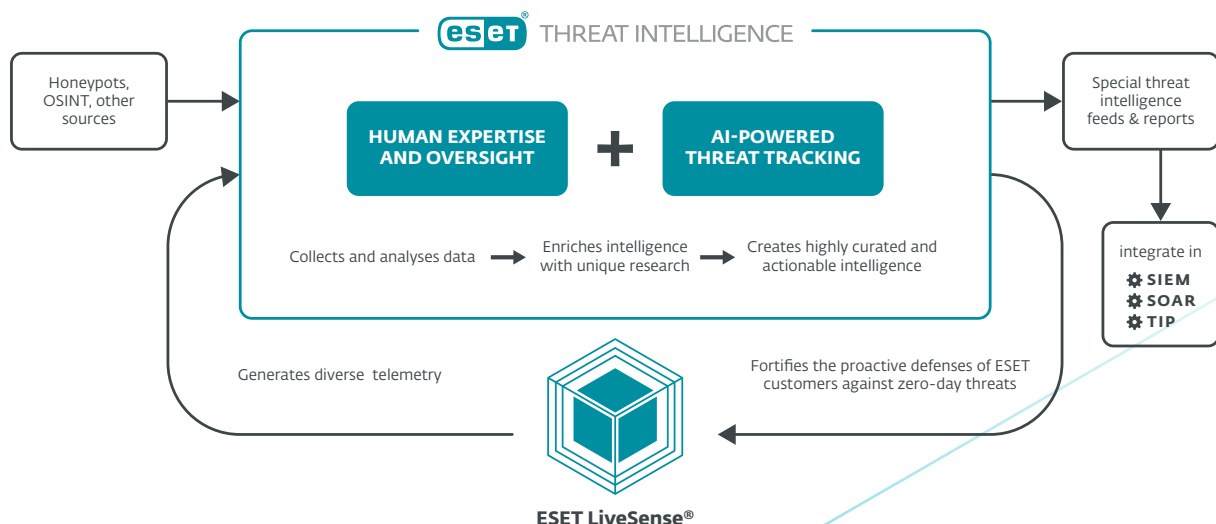
La presencia global de ESET, construida durante décadas, te ofrece una **biblioteca de inteligencia rica y diversa** proveniente de millones de nodos. A diferencia de muchos competidores, **nuestra telemetría es particularmente sólida en regiones consideradas “más interesantes”** desde un punto de vista geopolítico en el mundo de la ciberdefensa. Esta cobertura única se traduce directamente en una inteligencia superior para ti. Al aprovechar la telemetría de ESET, obtienes acceso a información valiosa y accionable de alta calidad que **potencia tus capacidades de detección y respuesta ante amenazas**.

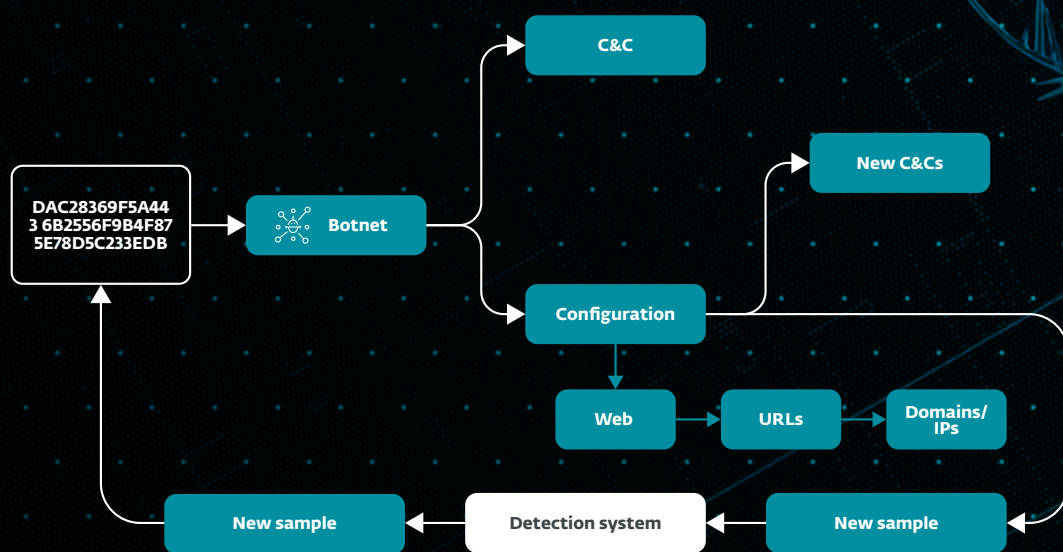


Inteligencia única y enriquecida para obtener información accionable

La inteligencia de amenazas no consiste solo en recopilar indicadores y empaquetarlos; ESET va mucho más allá. Empleamos tecnología avanzada y una amplia experiencia para procesar y enriquecer nuestra inteligencia, asegurándonos de que aporte un valor real a tu negocio.

- 1. Telemetría integral:** Tu inteligencia comienza con una amplia gama de telemetría generada por ESET LiveSense, nuestra tecnología de seguridad multicapa integrada en la plataforma ESET PROTECT. Esto te garantiza una recopilación de datos amplia y profunda desde diversas fuentes.
- 2. Métodos de recolección diversos:** Además de LiveSense, utilizamos varios métodos de monitoreo y recolección, incluyendo honeypots, sensores, recursos de OSINT, web crawling (tanto en la clear como en la deep web) y rastreo de amenazas (Threat Tracking). Esto se traduce para ti en un volumen significativo de datos de alta calidad.
- 3. Procesamiento avanzado:** Una vez recolectados, todos tus datos se procesan a través de nuestros robustos sistemas de backend, que aprovechan la IA para clasificar y analizar la información de forma automática. Esto asegura que solo la inteligencia más relevante y accionable salga a la superficie.
- 4. Análisis de expertos:** Más allá del procesamiento automatizado, nuestro cualificado equipo de analistas e investigadores de inteligencia de amenazas desempeña un papel crucial. Estudian y analizan continuamente a diversos actores de amenazas, sus motivaciones, TTP (tácticas, técnicas y procedimientos) y sus herramientas. Esta verificación humana añade una capa extra de profundidad y precisión a tu inteligencia, yendo más allá de lo que el aprendizaje automático y la automatización pueden lograr por sí solos.





Las muestras que recibimos a través de la telemetría se someten a un análisis profundo, tanto conductual como estructural. Este proceso genera indicadores útiles adicionales, enriqueciendo aún más tu inteligencia de amenazas. Al examinar meticulosamente cada muestra, extraemos información valiosa que mejora la calidad y eficacia general de nuestra inteligencia, proporcionándote una comprensión más completa del panorama de amenazas.

Seguridad superior mediante informes de APT detallados

Escritos en un lenguaje conciso y accionable para mejorar la postura de seguridad de tu organización, nuestros informes de APT te ofrecen una visión detallada de las campañas de malware, su distribución y los actores involucrados. Accede a nuestro servidor MISP y a nuestro asesor de IA, y reserva sesiones en vivo con los mejores expertos en inteligencia de amenazas de ESET para obtener una inteligencia integral y lista para actuar.

NUESTRA MEJOR INVESTIGACIÓN AL ALCANCE

Nuestro equipo de investigación es ampliamente reconocido en la industria de la seguridad digital gracias a nuestro galardonado blog WeLiveSecurity. La excelente labor de investigación y los resúmenes de actividad de APT (Amenazas Persistentes Avanzadas) del equipo están a tu disposición, junto con información mucho más detallada. Como cliente de ESET, obtienes un acceso anticipado y exclusivo a todo el contenido de WeLiveSecurity.

CONTENIDO ACCIONABLE Y CURADO

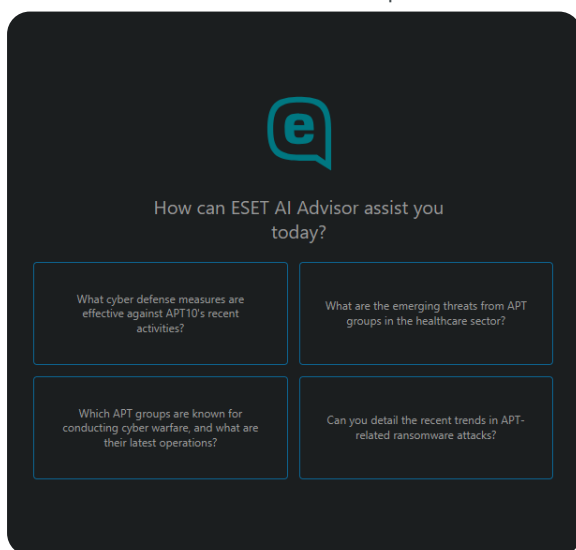
Nuestros informes te proporcionan un contexto profundo sobre qué está ocurriendo y por qué. Gracias a esto, tu organización puede prepararse con antelación para lo que pueda venir. Y lo más importante: nuestros expertos se aseguran de que el contenido sea fácil de entender para ti.

TOMA DECISIONES CRUCIALES

Todo esto ayuda a que tú y tu organización tomen decisiones críticas, otorgándoos una ventaja estratégica en la lucha contra el crimen digital. Te aporta una comprensión clara de lo que sucede en el "lado oscuro de Internet" y te ofrece el contexto vital para que realices tus preparativos internos de forma rápida.

ACCESO A UN ANALISTA DE ESET

Si contratas el paquete APT Reports Premium, tendrás acceso directo a un analista de ESET hasta cuatro horas al mes. Esto te da la oportunidad de discutir temas con mayor nivel de detalle y te ayuda a resolver cualquier duda pendiente que tengas.



ESET AI Advisor utiliza IA avanzada y experiencia en APT para ofrecerte información bajo demanda y medidas de protección contra ciberataques. Disponible en formato de chatbot, responde a tus consultas de seguridad, te ofrece resúmenes de APT, recopila IoC (indicadores de compromiso) y TTP, y genera reglas YARA para que comprendas y prevengas las amenazas con total rapidez.

		APT Reports	APT Reports Advanced	APT Reports Ultimate
Informes de resumen de actividad quincenales	Informes que resumen la actividad de todos los grupos APT cubiertos, tal como se detalló anteriormente (dos informes por mes)	✓	✓	✓
Informes de análisis de amenazas	Análisis técnicos regulares o personalizados sobre las amenazas más prevalentes (aprox. 30 al año)	✓	✓	✓
Resumen mensual (Monthly Overview)	Recopilación mensual de información con un enfoque ejecutivo sobre las amenazas actuales	✓	✓	✓
Compendio mensual (Monthly Digest)	Índice y resumen ejecutivo de los informes y eventos ocurridos durante el mes	✓	✓	✓
Pre-acceso a WeLiveSecurity	Acceso anticipado a informes de amenazas y artículos seleccionados de WeLiveSecurity	✓	✓	✓
Feed de IOC de APT	Acceso total al feed en formato STIX/TAXII que contiene los IOC (indicadores de compromiso) de los informes	✓	✓	✓
Acceso al servidor MISP	Acceso total al servidor MISP de ESET, que contiene toda la información disponible en los informes para tu integración	✗	✓	✓
ESET AI Advisor	Acceso al asesor de IA de ESET, que te proporciona información estratégica y resúmenes de los informes de APT disponibles	✗	✓	✓
Acceso a analistas	Comunicación directa con analistas a través de plataformas como MS Teams y correo electrónico, limitada a cuatro horas al mes (no acumulables, incluye tiempo de preparación)	✗	✗	✓

De indicadores a inteligencia: Sé más astuto que el cibercrimen (eCrime)

Los informes de eCrime de ESET Threat Intelligence te brindan una visión profunda de las operaciones de ransomware y del cibercrimen en general. Obtén visibilidad sobre las herramientas de los atacantes, su infraestructura y sus estrategias de monetización, con el respaldo de la investigación global de ESET. Ve más allá de los IoC para acceder a inteligencia contextual que fortalezca tu defensa proactiva y tu toma de decisiones estratégicas.

Lo que hace que los informes de eCrime de ESET sean diferentes

DEFENSA PROACTIVA

Obtén inteligencia no solo sobre los grupos de eCrime, sino también sobre los afiliados que realmente ejecutan los ataques. Observa cómo operan y anticipa sus próximos movimientos para que te mantengas siempre un paso adelante.

EFICIENCIA OPERATIVA

Utiliza información clara y curada de incidentes reales para filtrar el ruido. Facilita que tu equipo detecte amenazas, responda más rápido y enfoque las cacerías de amenazas (threat hunting) donde más importa.

VISIBILIDAD EXCLUSIVA

Ve más allá de los feeds públicos de amenazas con una visión más profunda de las tácticas de monetización, la infraestructura y el comportamiento real de los afiliados; todo respaldado por la investigación y la telemetría global de ESET.

		eCrime Reports	eCrime Reports Advanced
Resumen de Actividad MENSUAL	- Las últimas campañas de ransomware e infostealers sintetizadas en información estratégica y clara - Quién es el objetivo, cómo se desarrollan los ataques y qué falló - Lecciones clave, IoC y orientación para que fortalezcas tu resiliencia	✓	✓
Análisis Técnico MENSUAL	- Inmersiones profundas en actores de amenazas específicos (ej. FIN7) - Cadena de ataque completa: desde el acceso inicial hasta el robo de datos - Tácticas de los atacantes, herramientas, infraestructura, mapeo de MITRE ATT&CK® e IoC	✓	✓
Compendio Mensual MENSUAL	- Resumen listo para niveles ejecutivos sobre la actividad reciente de ransomware e infostealers - Tendencias clave, incidentes notables y amenazas emergentes - Ayuda a que tu liderazgo evalúe riesgos y establezca prioridades sin complejidad técnica	✓	✓
Feed de eCrime	- IoC actualizados y curados sobre bandas de ransomware, sus afiliados y campañas de infostealers - Disponible en el formato estándar STIX/TAXII	✓	✓
ESET AI Advisor	- Utiliza información de eCrime para responder a tus preguntas relacionadas con amenazas - Te ayuda a interpretar incidentes y el comportamiento de los atacantes - Hace que la inteligencia de amenazas sea accesible al instante para tus equipos y tomadores de decisiones	✗	✓
Acceso al servidor MISP	- Integración directa con inteligencia de amenazas curada - Ingesta automática de IoC para enriquecer tus defensas - Optimiza tus flujos de trabajo, acelera la detección y apoya la respuesta ante incidentes	✗	✓

Feeds de datos claros y concisos

Mejora tu visión del panorama de amenazas con la telemetría única de ESET. Te proporcionamos feeds de datos altamente curados en formatos JSON y STIX 2.1, que se integran a la perfección en tus herramientas de SIEM, TIP o SOAR. A diferencia de muchos proveedores de inteligencia de amenazas (TI), prestamos una atención muy minuciosa para que nuestros feeds estén meticulosamente filtrados y evaluados, garantizando su relevancia. Esto permite que tus sistemas de seguridad existentes ejecuten acciones automáticas cuando sea necesario empoderando a tus analistas de inteligencia con una visión integral del panorama global de amenazas.

- Nos aseguramos de que los datos sean ligeros, altamente relevantes, de duplicados y con puntuación de confianza (confidence-scoring)
- Son el resultado de un filtrado avanzado, con información estratégica aportada por los investigadores de ESET
- Líderes en el mercado, especialmente en datos sobre botnets
- Bajos requisitos de mantenimiento gracias a que el contenido está correctamente curado
- Feeds en tiempo real: solo IoC (Indicadores de Compromiso) recientes y prevalentes

FEED DE DATOS MALICIOSOS

Información en tiempo real sobre muestras de malware recién descubiertas, sus características e IoC. Incluye hashes de archivos, marcas de tiempo y tipos de amenazas para ayudarte a bloquear archivos maliciosos antes de que causen daño.

FEED DE RANSOMWARE

Datos en tiempo real sobre familias de ransomware activas y muestras prevalentes. Te permite realizar un bloqueo proactivo para prevenir brechas de seguridad e interrupciones costosas.

FEED DE BOTNETS

Impulsado por el rastreador de botnets de ESET, este feed incluye tres sub-feeds: botnet, C&C (Comando y Control) y objetivos. Te proporciona detalles de detección, hashes de archivos, marcas de tiempo de la última comunicación, archivos descargados, direcciones IP, protocolos e información sobre los objetivos.

FEED DE IOC DE APT

Perspectivas sobre Amenazas Persistentes Avanzadas basadas en la investigación de ESET. Se exporta desde el servidor MISP interno de ESET y está alineado con los informes de APT. Está disponible como parte de los informes o como un feed independiente para tu stack.

FEED DE PUA / ADWARE

ESET cuenta con más de dos décadas de experiencia clasificando PUA (Aplicaciones Potencialmente No Deseadas), lo que le da a su inteligencia una profundidad y precisión inigualables. Los feeds de adware te entregan información en tiempo real sobre adware activo y amenazas similares, permitiéndote un bloqueo proactivo antes del impacto.

FEED DE PUA / APPS DE DOBLE USO (DUAL-USE)

Rastrea herramientas legítimas (por ejemplo, RMMs) que son utilizadas de forma indebida por los atacantes. Esto te ayuda a anticiparte al abuso de estas aplicaciones mientras reduces el ruido mediante datos personalizados y de baja redundancia.

FEED DE DOMINIOS

Te proporciona datos sobre dominios maliciosos, incluyendo el nombre de dominio, la dirección IP y la fecha asociada. Los dominios están clasificados por severidad, lo que te permite priorizar acciones, como el bloqueo de dominios de alto riesgo.

FEED DE URL

Un feed curado de URLs específicas con información detallada sobre cada dirección y sus dominios de alojamiento. Incluye únicamente hallazgos de alta confianza, respaldados por explicaciones claras y legibles para humanos sobre las URLs.

FEED DE IP

Recibe datos accionables sobre IPs maliciosas. Su estructura es idéntica a la de los feeds de dominios y URLs. Úsalo para identificar amenazas comunes, bloquear IPs de alta severidad, monitorear las de menor riesgo e investigar más a fondo utilizando datos adicionales para evaluar daños potenciales.

FEED DE AMENAZAS PARA ANDROID

Te ofrece información en tiempo real sobre las amenazas prevalentes en Android y sus IoC, permitiendo un bloqueo proactivo. Se crea a partir de la telemetría de ESET y se actualiza casi en tiempo real con una deduplicación diaria.

FEED DE INFOTEALERS PARA ANDROID

Un feed especializado dentro de las amenazas de Android que ofrece detalles sobre muestras actuales de infostealers y datos relacionados. Obtén una visión profunda de las familias activas y bloquéalas proactivamente antes de que causen daño.

FEED DE URL DE ESTAFAS (SCAMS)

Mantente un paso adelante de las estafas con datos en tiempo real sobre URLs fraudulentas. Cubre tiendas electrónicas, estafas de inversión, estafas de citas y de criptomonedas. Se genera a partir de todas las fuentes de URL de ESET casi en tiempo real; la deduplicación se realiza cada 24 horas.

FEED DE ESTAFAS CRIPTO (CRYPTOSCAM)

Anticípate a las estafas con criptomonedas con actualizaciones en tiempo real sobre dominios y URLs de estafa, además de sus datos asociados. Proveniente de la extensa telemetría de ESET, te brinda información temprana y segmentada para ayudarte a bloquear amenazas de forma proactiva y proteger tus activos.

FEED DE ADJUNTOS DE CORREO MALICIOSOS

El correo electrónico es un objetivo principal de ataque. Este feed te proporciona datos en tiempo real sobre archivos adjuntos maliciosos obtenidos de la amplia telemetría de escaneo de correos de ESET.

FEED DE URL DE PHISHING

Entrega inteligencia en tiempo real sobre URLs de phishing activas desde la base de datos dedicada de ESET. Actualizado continuamente y con deduplicación diaria, este feed te ayuda a detectar y bloquear sitios fraudulentos antes de que comprometan datos sensibles.

FEED DE SMISHING

Te ofrece información oportuna sobre el phishing basado en SMS (smishing), incluyendo dominios, URLs e indicadores relacionados. Proveniente de la telemetría global de ESET, se desarrolla casi en tiempo real con deduplicación diaria.

FEED DE ESTAFAS POR SMS (SMS SCAM)

Protégete contra las estafas por SMS con un feed en tiempo real sobre dominios y URLs maliciosas. Actualizado casi en tiempo real y deduplicado diariamente, te ayuda a identificar y bloquear amenazas sofisticadas.

FEED DE ECRIME

Obtén datos claros y accionables sobre operaciones de cibercrimen y eCrime basado en malware. Monitorea desde bandas de ransomware y sus afiliados hasta campañas de infostealers, para que tu equipo pueda pasar de la reacción a la defensa proactiva de tu organización, monitoring everything from ransomware gangs and their affiliates to infostealer campaigns, so your team can move from reacting to proactively defending your organization.

Experience the power of ESET Threat Intelligence

Schedule a demo with us today and discover the unparalleled value ESET Threat Intelligence can bring to your organization. With a 100% renewal rate, our satisfied customers are a testament to the effectiveness of our solutions. Let us show you how we can enhance your cybersecurity defenses.

Not ready for a demo call yet?

Start by creating [a preview account](#) in the ESET Threat Intelligence portal to explore feeds and APT reports.

Somos ESET

Defensa proactiva. Minimiza tus riesgos con la prevención.

Mantente un paso por delante de las amenazas cibernéticas conocidas y emergentes —ataques dirigidos, amenazas de día cero, ransomware, phishing y más— con nuestro enfoque basado en IA nativa y centrado en la prevención. ESET combina para ti el poder de la IA y la experiencia humana para ofrecerte una protección fácil y eficaz

Experimenta la mejor seguridad de su clase impulsada por la ciencia, respaldada por más de 30 años de inteligencia global propia sobre ciberamenazas. Nuestra amplia red de I+D, liderada por investigadores aclamados en la industria, impulsa nuestra galardonada plataforma de ciberseguridad centrada en la nube. Las soluciones de ESET son altamente personalizables para ti, incluyen soporte local y tienen

un impacto mínimo en tu rendimiento. ESET protege tu negocio para que puedas liberar todo el potencial de la tecnología.

ESET EN NÚMEROS

+mil millones
de usuarios
de internet
protegidos
como tú

+500 mil
empresas que
son clientes
como la tuya

178
países donde
puedes
encontrarnos

11
centros
globales de
I+D para tu
seguridad

NUESTROS CLIENTES



Protegido por ESET desde
2017 más de 9.500 endpoints



Protegido por ESET desde
2016 más de 4.000 buzones
de correo



Protegido por ESET desde
2016 más de 32.000
endpoints



Socio de seguridad de ISP
desde 2008. Base de 2 millones
de clientes

RECONOCIMIENTOS DE LA INDUSTRIA



Ganador de los premios **Best Enterprise Endpoint** y **Best Small Business Endpoint** en los SE LABS Awards 2025.



Nombrado **Customers' Choice** en el reporte 2026 de Gartner® Peer Insights™ "Voice of the Customer" Endpoint Protection Platforms.



Reconocido como **Leader en Frost Radar: Endpoint Security 2025**, demostrando su excelencia en crecimiento e innovación.

Gartner and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.