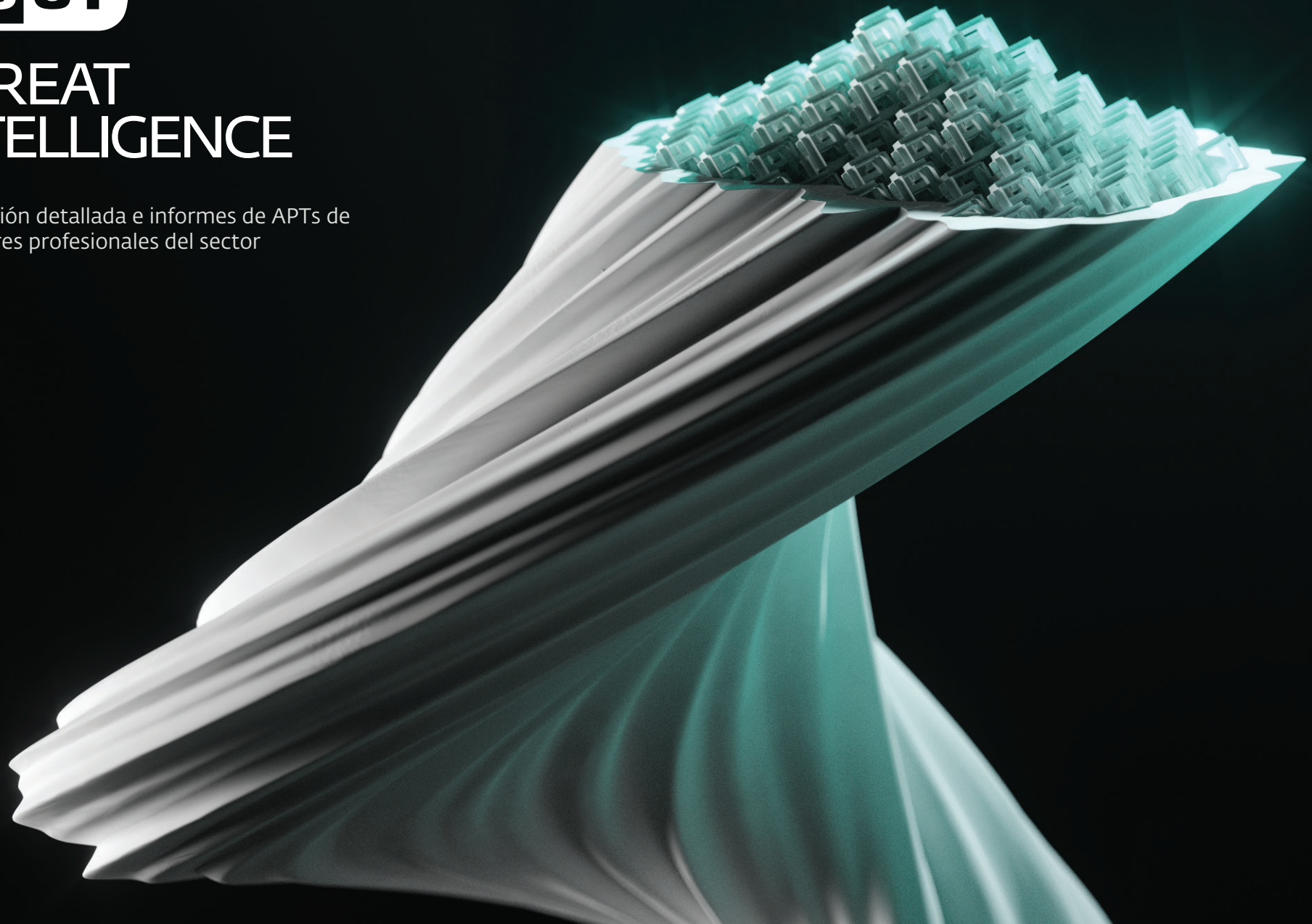
THREAT INTELLIGENCE

Información detallada e informes de APTs de los mejores profesionales del sector



¿Por qué inteligencia sobre amenazas?

Detén la sobrecarga de información y obtén datos relevantes para tu empresa

SUPERAR EL EXCESO DE INFORMACIÓN

El ransomware, los días cero, las amenazas persistentes avanzadas, los ataques dirigidos y las redes de bots son preocupaciones para las empresas de todo el mundo. El problema es que, a causa del volumen de las diferentes amenazas, las empresas son incapaces de comprender fácilmente qué defensas proactivas y mitigaciones son las más importantes.

En última instancia, esto hace que las compañías se esfuercen por encontrar información significativa entre conjuntos de datos limitados, como sus propias redes, o los conjuntos de datos extremadamente grandes que se encuentran a través de fuentes externas. Los servicios de inteligencia sobre amenazas ayudan a filtrar la sobrecarga de información y proporcionar la información más relevante para determinadas empresas.

Los servicios de inteligencia sobre amenazas permiten a las empresas priorizar las amenazas emergentes de forma rápida y sencilla, lo que les deja más tiempo para implementar de forma proactiva nuevas defensas contra ellas.

COMBATIR LAS AMENAZAS DE FORMA PROACTIVA

El panorama actual de la ciberseguridad evoluciona constantemente con nuevos métodos de ataque y amenazas nunca antes vistas. Cuando se produce un ataque o una vulneración de datos, las empresas suelen sorprenderse de que sus defensas se hayan visto comprometidas o desconocen por completo que el ataque se haya producido. Cuando finalmente se descubre el ataque, las empresas se apresuran a reaccionar y aplicar medidas de mitigación para evitar que el ataque se repita. Sin embargo, esto no las protege de del siguiente ataque que podría utilizar un vector completamente nuevo.

Los servicios de inteligencia sobre amenazas proporcionan información sobre riesgos empresariales y amenazas desconocidas, que permiten mejorar a las empresas la eficacia de sus defensas e implementar una política de ciberseguridad proactiva.

¿Por qué inteligencia sobre amenazas?

Al proporcionar información sobre el responsable de la amenaza, los vectores de ataque y los indicadores de compromiso, los equipos de seguridad pueden reducir el tiempo de respuesta a los incidentes al obtener una imagen completa del ataque y de lo que hay que detectar.

ACELERAR LA RESPUESTA A LOS INCIDENTE

Cuando se produce una vulneración de datos, los equipos de seguridad necesitan conocer cómo se ha producido el incidente, así como identificar qué dispositivos se han visto afectados. Este proceso suele ser muy largo y manual, ya que los los ingenieros examinan la red en busca de anomalías que puedan indicar que la red ha sido comprometida.

Los servicios de inteligencia sobre amenazas permiten a los equipos de de incidentes comprender y responder rápidamente a las vulneraciones de datos. Al proporcionar información sobre el autor de la amenaza, el comportamiento del malware, los vectores de ataque y los indicadores de compromiso, los equipos de seguridad pueden reducir el tiempo de de respuesta a incidentes al comprender la imagen completa del de los ataques, así como de lo que hay que detectar.

La ventaja de ESET

Experiencia humana respaldada por el aprendizaje automático. Nuestro sistema de reputación del sistema, LiveGrid®, está formada por 110 millones de sensores en todo el mundo y verificado por nuestros centros de I+D.

1

EXPERIENCIA HUMANA CON EL MEJOR MACHINE LEARNING

El uso de machine learning para automatizar decisiones y evaluar posibles amenazas es una parte vital de nuestro planteamiento. Pero solo es tan eficaz como las personas que están detrás del sistema. La experiencia humana es primordial para proporcionar la inteligencia sobre amenazas más precisa posible, porque los autores de las amenazas pueden ser adversarios inteligentes.

2

FUERTE REPUTACIÓN SISTEMA - LIVEGRID®

Los productos ESET Endpoint contienen un sistema de reputación en la nube que alimenta información relevante sobre las amenazas más recientes y archivos benignos. Nuestro sistema de reputación, LiveGrid®, se compone de 110 millones de sensores en todo el mundo, cuyos resultados son verificados por nuestros centros de I+D. Esto proporciona a los clientes el más alto nivel de confianza al ver la información y los informes en su consola.

3

ORÍGENES DE LA UE, PRESENCIA MUNDIAL

Con sede en la Unión Europea, ESET ha estado en la industria de la seguridad desde hace más de 30 años, tiene 22 oficinas en todo el mundo, 13 instalaciones de I+D y está presente en más de 200 países y territorios. Esto ayuda a proporcionar a nuestros clientes una perspectiva global sobre todas las tendencias y amenazas más recientes.

La ventaja de ESET

OBTÉN UNA PERSPECTIVA ÚNICA

ESET recopila información sobre amenazas de una serie de fuentes únicas y cuenta con una experiencia inigualable que le ayuda a combatir los ataques de ciberseguridad cada vez más sofisticados.

TOMA DECISIONES CRUCIALES CON MAYOR RAPIDEZ

Anticípate a las amenazas y toma decisiones más rápidas y mejores gracias a los informes completos de ESET y fuentes expertas. Reduce tu exposición a las principales amenazas, de la mano de nuestro expertos.

INVESTIGACIÓN DE AMENAZAS AUTOMATIZADAS

La tecnología de ESET busca amenazas constantemente, a través de múltiples capas, desde el prearranque hasta el estado de reposo. Benefíciate de la telemetría en todos los países donde ESET detecta amenazas emergentes.

ADELÁNTATE A LOS ADVERSARIOS

ESET hace un seguimiento , vigilando específicamente aquellos lugares donde hemos detectado grupos de APTs que se dirigen a empresas occidentales: Rusia, China, Corea del Corea del Norte, Irán. Conocerás las nuevas amenazas antes que nadie.

MEJORA LA POSTURA DE SEGURIDAD

Informado por la inteligencia de ESET, mejora tu búsqueda de amenazas y remediación, bloquea APTs y ransomware, y mejora tu arquitectura de ciberseguridad.

Informes de amenazas persistentes avanzadas (APTs)

PONEMOS NUESTRA MEJOR INVESTIGACIÓN AL ALCANCE DE TU MANO

Nuestro equipo de investigación es bien conocido en el sector de la seguridad digital gracias a nuestro galardonado blog We Live Security. La excelente investigación del equipo y los resúmenes de la actividad de APTs del equipo, junto con información mucho más detallada. Los clientes de ESET obtienen de forma exclusiva todo el contenido de We Live Security.

TOMA DECISIONES CRUCIALES CON RAPIDEZ

Todo esto ayuda a las empresas a tomar decisiones cruciales y proporciona una ventaja estratégica en la lucha contra la delincuencia digital. Aporta una comprensión de lo que está ocurriendo en el "lado oculto de Internet" y proporciona contexto crucial, para que tu empresa pueda hacer preparativos internos con rapidez.

CONTENIDOS PROCESABLES Y DE CALIDAD

Los informes proporcionan un gran contexto de lo que está pasando y por qué. Gracias a ello, las empresas pueden prepararse de antemano para lo que pueda venir. Y lo que es más importante, nuestros expertos se aseguran de que el contenido sea fácil de entender.

ACCESO A LOS ANALISTAS DE ESET

Cada cliente que solicite el paquete Premium de informes APTs tendrá también acceso a un analista de ESET durante un máximo de cuatro horas al mes. Esto proporciona la oportunidad de examinar los temas con mayor detalle y ayudar a resolver cualquier problema pendiente.

CON LOS INFORMES APT, OBTENDRÁS

- Acceso a análisis técnicos privados y en profundidad
- Informes de resumen de la actividad de APTs
- Un resumen mensual para tus ejecutivos de nivel C
- Acceso directo a un profesional de ciberseguridad de ESET
- Acceso a nuestro servidor MISP

ANÁLISIS PROFUNDO

El paquete incluye informes mensuales de análisis que describen las campañas recientes, nuevos conjuntos de herramientas y temas relacionados. También recibirás un informe resumen de actividad cada dos semanas que describe las últimas campañas de APTs que los investigadores de ESET han estado investigando a varios autores de amenazas, así como sus objetivos y, por supuesto, los Indicadores de Compromiso (IoC) asociados. Un resumen mensual combina la información de todos los informes de Análisis Técnico y Resumen de Actividad publicados en el mes anterior en un formato más breve y fácil de consultar.

La disponibilidad de los informes y fuentes de ESET Threat Intelligence varía según el país. Ponte en contacto con el representante local de ESET para obtener más información.

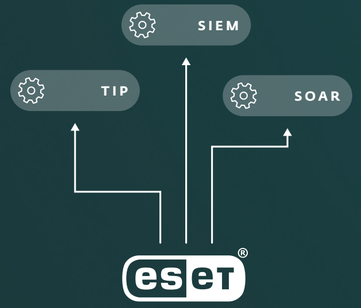
Integra ESET Threat Intelligence en tu sistema

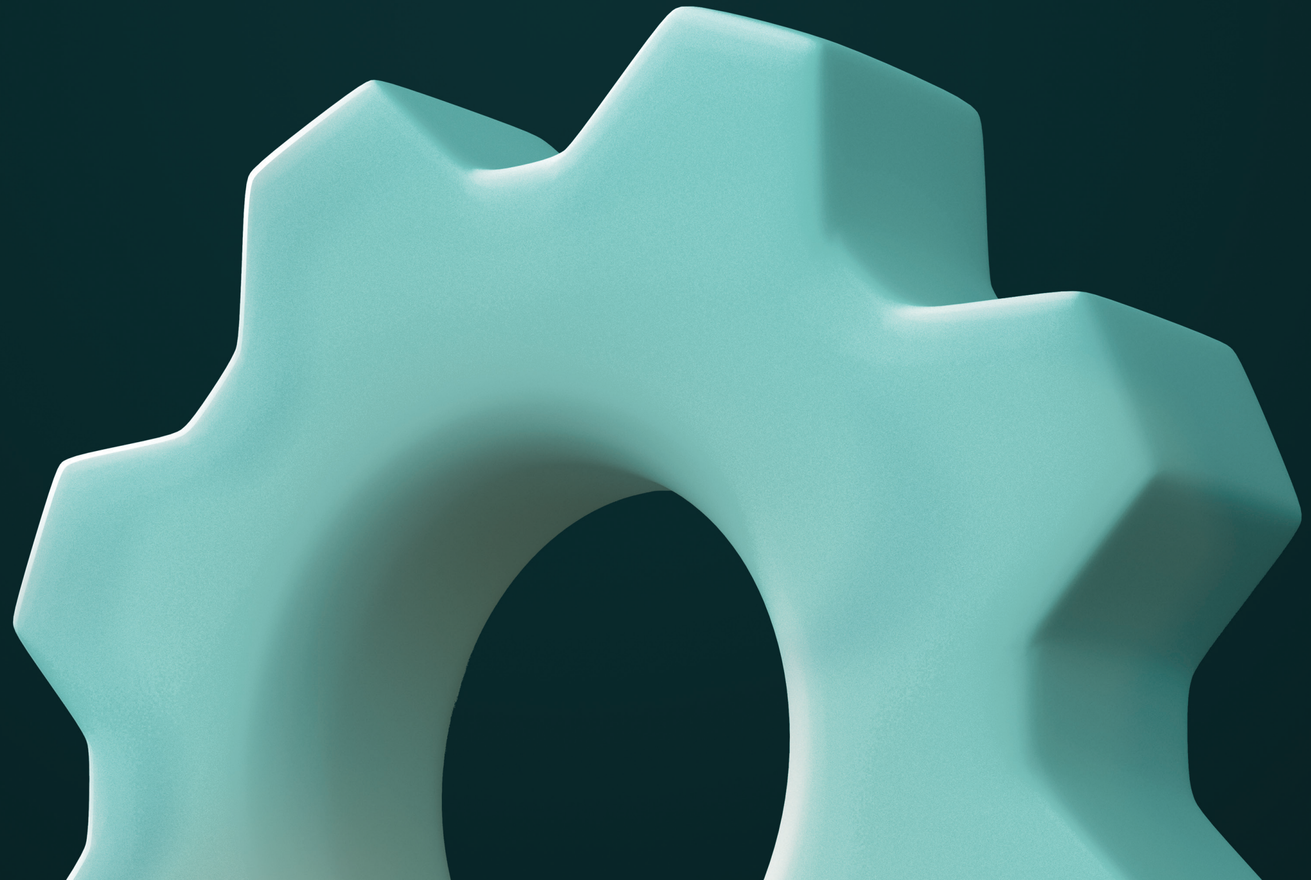
Integrar la telemetría de ESET es sencillo y enriquecerá tu TIP, SIEM o SOAR

Disponemos de una amplia API con documentación completa

Suministramos datos en formatos estandarizados - como JSON y STIX a través de TAXII - para que la integración en cualquier herramienta sea posible

Para IBM QRadar, Anomali y Logpoint tenemos manuales de integración paso a paso para una implementación y estamos añadiendo continuamente otros.





Fuentes de inteligencia propias de ESET

Enriquece tu visión del estado de las amenazas en todo el mundo basándote en una telemetría única. Los datos de ESET provienen de nuestros centros de investigación de todo el mundo, proporcionando una imagen holística y permitiendo bloquear rápidamente los IoC en tu entorno. Las fuentes están en los formatos - JSON - STIX 2.0

FUENTE DE ARCHIVOS MALICIOSOS

Entender qué archivos maliciosos se ven en el medio. La información presenta los dominios que se consideran maliciosos, incluyendo el nombre del dominio, la dirección IP, la detección de archivos descargados desde la URL, y la detección del archivo que intentaba acceder a la URL. Esta fuente consiste en los hashtags compartidos, hashes de archivos ejecutables maliciosos y datos asociados.

ALIMENTACIÓN DEL DOMINIO

Bloquear los dominios que se consideran maliciosos. El informe incluye nombres de dominio, direcciones IP y las fechas asociadas a ellos. El informe clasifica los dominios en función de su gravedad, lo que le permite ajustar su respuesta por ejemplo, para bloquear solo los dominios de alta gravedad.

FUENTE DE ALIMENTACIÓN IP

Esta fuente comparte las IPs consideradas maliciosas y los datos asociados a ellas. La estructura de los datos es muy similar a la utilizada en los alimentadores de dominios y URLs. El principal caso de uso aquí es detectar las IPs maliciosas que son de alta gravedad, detectar las que son menos graves, e investigar más, basándose en datos adicionales, para ver si ya han causado daños.

FUENTE URL

Al igual que la fuente de dominios, la fuente de URLs busca direcciones específicas . Incluye información detallada sobre los datos relacionados con la URL, así como información sobre los dominios que las alojan. Toda la información se filtra para mostrar únicamente resultados de alta confianza e incluye información de fácil comprensión sobre el motivo por el que se ha marcado la URL.

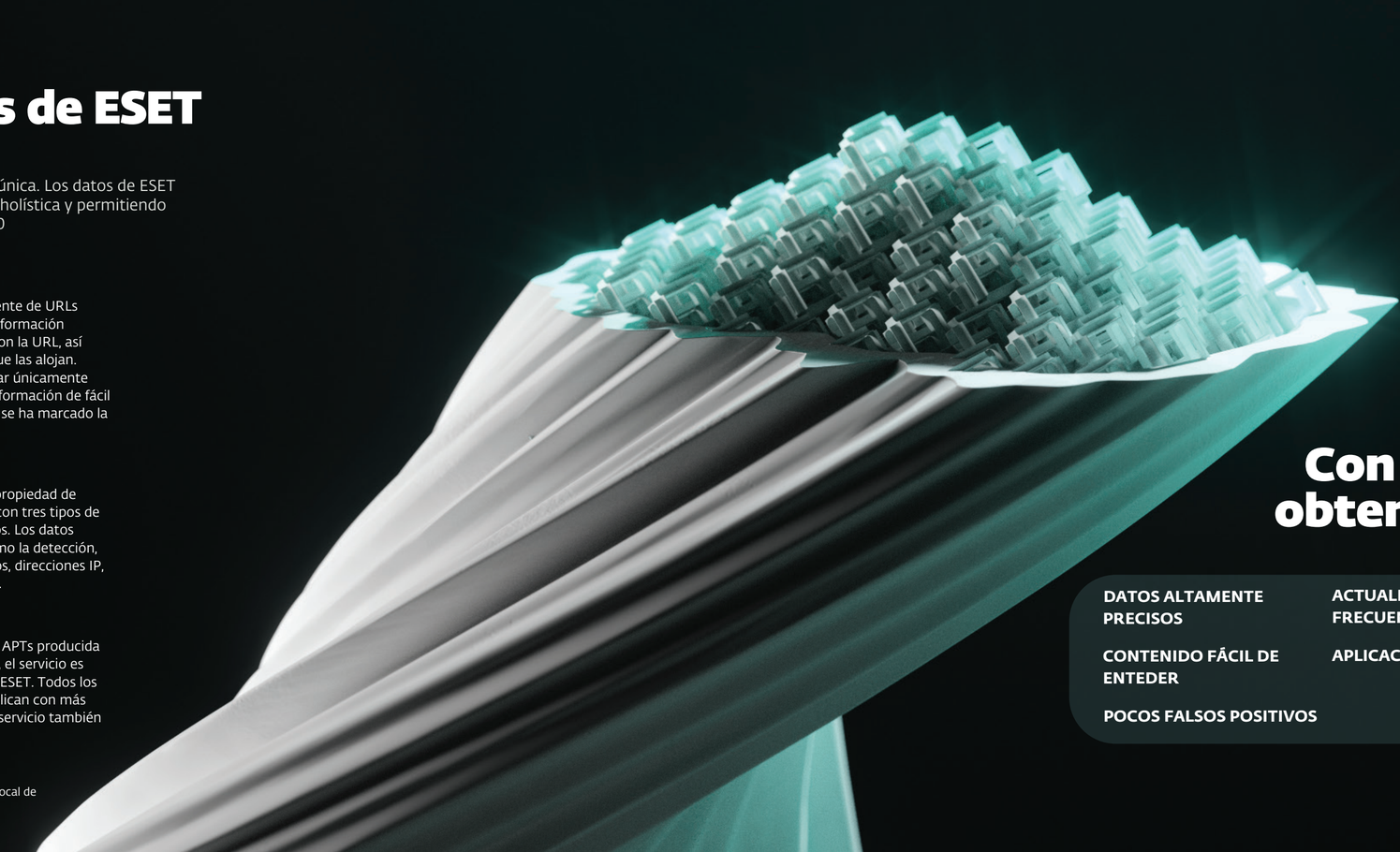
FUENTE DE BOTNET

Basado en la red de rastreo de botnets propiedad de ESET, Botnet es un sistema que cuenta con tres tipos de subalimentación: botnet, C&C y objetivos. Los datos proporcionados incluyen elementos como la detección, hash, último activo, archivos descargados, direcciones IP, protocolos, objetivos y otra información.

FUENTE DE APTs

Este servicio consiste en información de APTs producida por la investigación de ESET. En general, el servicio es una exportación del servidor interno de ESET. Todos los datos que se comparten también se explican con más detalle en los informes de APTs, pero el servicio también se puede adquirir por separado.

La disponibilidad de los informes y fuentes de ESET Threat Intelligence varía según el país. Ponte en contacto con tu representante local de ESET para obtener más información.



Con ESET obtendrás

- DATOS ALTAMENTE PRECISOS
- ACTUALIZACIONES FRECUENTES
- CONTENIDO FÁCIL DE ENTEDER
- APLICACIÓN COMPLETA
- POCOS FALSOS POSITIVOS

ACERCA DE ESET

Durante más de 30 años, ESET® ha desarrollado software y servicios de seguridad informática líderes en la industria para ofrecer una protección protección multicapa contra las ciberamenazas a empresas y consumidores de todo el mundo. ESET es pionera en tecnologías de aprendizaje automático y en la nube que previenen, detectan y responden al malware. ESET es una empresa de propiedad privada que promueve la investigación y el desarrollo científico en todo el mundo.

ESET EN CIFRAS

+110M
de usuarios seguros en todo el mundo

+400k
clientes de empresa

+200
países y territorios

13
centros de I+D en el mundo

ALGUNOS DE NUESTROS CLIENTES

Protegido por ESET desde 2016, con más 32.000 endpoints

Colaborador de seguridad de ISP desde 2008, con una base de 2 millones de clientes

Protegido por ESET desde 2017, con más de 9.000 endpoints

Protegido por ESET desde 2016, con más de 4000 buzones de correo

¿Por qué elegir ESET?

ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES

CERTIFICADO DE SEGURIDAD ISO

CERTIFICADO DE SEGURIDAD ISO

ESET cumple la norma ISO/IEC 27001:2013, una norma de seguridad reconocida y aplicable internacionalmente en la implementación y la gestión de la seguridad de la información. La certificación es otorgada por el organismo de certificación acreditado por SGS y demuestra el cumplimiento total de ESET de las mejores prácticas de la industria.

RECONOCIMIENTO DE LA INDUSTRIA

Reconocido como proveedor consolidado en 2021 Gartner® Peer Insights™ 'Voice of the Customer': EPP

Reconocido como proveedor consolidado en 2021 Gartner® Peer Insights™ 'Voice of the Customer': EPP

Gartner Inc, Magic Quadrant para plataformas de protección de endpoints, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, 20 de agosto de 2019. Gartner no respalda a ningún proveedor, producto o servicio descrito en sus publicaciones de investigación. Los estudios publicados por Gartner recogen solo las opiniones de la organización de investigación de Gartner y no deben considerarse declaraciones de hechos. Gartner excluye cualquier garantía, explícita o implícita, en relación con este estudio, incluidas las garantías de comercialización o idoneidad para un uso en concreto.
Gartner Peer Insights es una plataforma gratuita de revisión y calificación por pares diseñada para los responsables de la toma de decisiones de software y servicios empresariales. Las reseñas pasan por un estricto proceso de validación y moderación para garantizar la autenticidad de la información. Las reseñas de Gartner Peer Insights representan las opiniones subjetivas de usuarios basadas en sus propias experiencias y no representan los puntos de vista de Gartner o sus asociados.

¿Por qué elegir ESET?

RECONOCIMIENTO DE LOS ANALISTAS

IDC ANALYZE THE FUTURE

ESET ha sido reconocido como uno de los principales proveedores en seguridad de endpoints en el IDC MarketScape: Worldwide Modern Endpoint Security para Empresas 2021 y en IDC MarketScape Modern Endpoint Security para pequeñas y medianas empresas 2021 Vendor Assessment.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET ha sido reconocida como `Top Player' por cuarto año consecutivo en Radicati APT Protection MQ 2021.

MITRE ATT&CK

La rigurosa evaluación de MITRE ATT&CK demostró las cualidades indispensables de la tecnología EDR de ESET y validó la sólida visión del futuro de ESET Inspect.

"La implementación fue muy sencilla. En colaboración con el equipo técnico bien formado de ESET pudimos implementar nuestra nueva solución de seguridad de ESET en pocas horas."

Gerente de IT, Diamantis Masoutis S.A., Grecia, más de 6.000 puestos

"Quedamos muy impresionados con el apoyo y la asistencia que recibimos. Además de ser un gran producto, la excelente atención y el apoyo que que recibimos fue lo que realmente nos llevó a trasladar todos los sistemas de Primoris a ESET en su conjunto."

Joshua Collins, Gerente de Operaciones del Centro de Datos, Primoris Services Corporation, Estados Unidos, más de 4.000 puestos


eset
Digital Security
Progress. Protected.