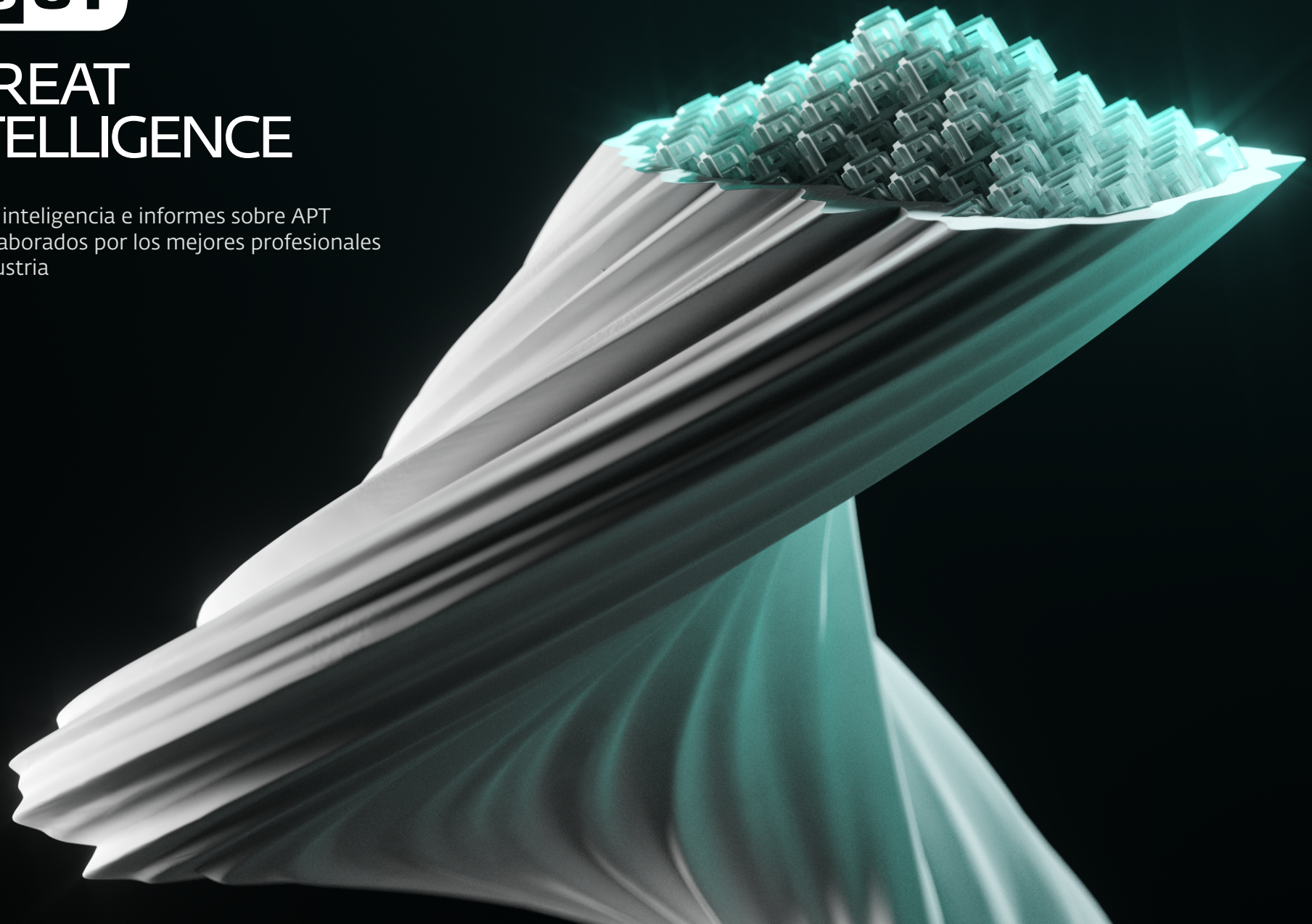
THREAT INTELLIGENCE

Feeds de inteligencia e informes sobre APT únicos elaborados por los mejores profesionales de la industria



¿Por qué es importante la inteligencia de amenazas?

Evita la sobrecarga de información y proporciona datos relevantes para su organización

CONTROLE LA SOBRECARGA DE INFORMACIÓN

El ransomware, las amenazas 0-day, las amenazas persistentes avanzadas, los ataques dirigidos y las botnets son algunos de los principales motivos de preocupación para las empresas de todo el mundo. El problema es que, debido a la gran cantidad de amenazas diferentes, a las organizaciones les cuesta entender cuáles son las defensas y mitigaciones proactivas más importantes.

En última instancia, terminan intentando sacar alguna información significativa de los conjuntos de datos limitados que tienen disponibles (como sus propias redes), o de conjuntos de datos extremadamente grandes que encuentran a través de fuentes externas. Los servicios de inteligencia de amenazas ayudan a filtrar la sobrecarga de información y suministran los datos más relevantes para cada organización específica.

Por lo tanto, con los servicios de inteligencia de amenazas, las empresas pueden priorizar las amenazas emergentes en forma fácil y rápida, con más tiempo para implementar nuevas defensas proactivas contra ellas.

COMBATA LAS AMENAZAS PROACTIVAMENTE

El panorama actual de la seguridad cibernética evoluciona constantemente con nuevos métodos de ataque y amenazas nunca antes vistas. Cuando se produce un ataque o una vulneración de datos, en general las organizaciones se sorprenden de que sus defensas hayan sido comprometidas, o directamente ignoran por completo la existencia del ataque. Una vez que finalmente descubren el ataque, implementan mitigaciones en forma precipitada y reactiva para evitar que se repita. No obstante, esto no los protegerá si el siguiente ataque usa un vector diferente.

Los servicios de inteligencia de amenazas proporcionan información sobre futuros riesgos empresariales y amenazas desconocidas, lo que les permite a las organizaciones mejorar la eficacia de sus defensas e implementar una postura proactiva de ciberseguridad.

¿Por qué es importante la inteligencia de amenazas?

Al proporcionar información sobre el actor de la amenaza, los vectores de ataque y los indicadores de compromiso, los equipos de seguridad pueden reducir el tiempo de respuesta al incidente, ya que comprenden el panorama completo del ataque y saben qué buscar

ACELERE LA RESPUESTA ANTE INCIDENTES

Cuando ocurre una vulneración de datos, los equipos de seguridad generalmente necesitan descubrir cómo sucedió el incidente e identificar qué dispositivos se vieron afectados. Este proceso suele ser muy largo y manual, ya que los ingenieros deben revisar su red en busca de alguna anomalía que pueda indicar la existencia de una infección.

Los servicios de inteligencia de amenazas permiten que los equipos de respuesta ante incidentes comprendan plenamente cómo ocurrieron las vulneraciones de datos y respondan con rapidez. Al contar con la información sobre el actor de la amenaza, el comportamiento del malware, los vectores de ataque y los indicadores de compromiso, los equipos de seguridad reducen el tiempo de respuesta al incidente, ya que ven el panorama completo del ataque y saben qué buscar.

La ventaja de ESET

Experiencia humana respaldada por el machine learning. Nuestro sistema de reputación LiveGrid® está conformado por 110 millones de sensores en todo el mundo, que son verificados por nuestros centros de investigación y desarrollo.

1

EXPERIENCIA HUMANA RESPALDADA POR EL MACHINE LEARNING

El uso de técnicas de machine learning para automatizar las decisiones y evaluar las posibles amenazas es una parte vital de nuestro enfoque. Pero solo es tan fuerte como las personas que están detrás del sistema. La experiencia humana es primordial para proporcionar la inteligencia de amenazas más precisa posible, dado que los actores maliciosos son oponentes inteligentes.

2

FUERTE SISTEMA DE REPUTACIÓN: LIVEGRID®

Los productos de ESET para endpoints incluyen un sistema de reputación en la nube que suministra información relevante sobre las amenazas y los archivos no infectados más recientes. Nuestro sistema de reputación, LiveGrid®, está conformado por 110 millones de sensores en todo el mundo, que son verificados por nuestros centros de investigación y desarrollo. Por eso, los clientes pueden confiar plenamente en la información y los informes que visualizan dentro de su consola.

3

CREADO EN LA UE, CON PRESENCIA MUNDIAL

Con su casa matriz ubicada en la Unión Europea, ESET ha formado parte de la industria de seguridad por más de 30 años, tiene oficinas en 22 países, 13 laboratorios de investigación y desarrollo, y además cuenta con presencia en más de 200 países y territorios de todo el mundo. Esto nos ayuda a brindarles a nuestros clientes una perspectiva global sobre todas las tendencias y amenazas más recientes.

La ventaja de ESET

OBTENGA ANÁLISIS ÚNICOS

ESET recopila información sobre amenazas de una gama exclusiva de fuentes y cuenta con una experiencia incomparable en este campo que lo ayudará a combatir los ataques de ciberseguridad cada vez más sofisticados.

TOME DECISIONES CRUCIALES MÁS RÁPIDO

Anticípese a las amenazas y tome mejores decisiones más rápido gracias a los completos informes de ESET y a los feeds cuidadosamente seleccionados. Reduzca su exposición a las amenazas predominantes, como le advierten los expertos.

AUTOMATICE LA INVESTIGACIÓN DE AMENAZAS

La tecnología de ESET busca amenazas constantemente a través de múltiples capas, desde antes del arranque hasta el estado de reposo. Aproveche los datos de la telemetría de ESET, que detecta amenazas emergentes en todos los países.

ANTICÍPESE A LOS ADVERSARIOS

ESET hace un seguimiento del dinero y vigila específicamente los países (Rusia, China, Corea del Norte e Irán) donde hemos detectado grupos de APT que atacan a las empresas occidentales. Usted será el primero en enterarse de las nuevas amenazas.

MEJORE SU POSTURA DE SEGURIDAD

Los feeds de inteligencia de ESET le permitirán mejorar sus capacidades de cacería y remediación de amenazas, bloquear APT y ransomware, y mejorar su arquitectura de ciberseguridad.

Informes sobre amenazas persistentes avanzadas (APT)

NUESTRAS MEJORES INVESTIGACIONES AL ALCANCE DE SU MANO

Nuestro equipo de investigación es reconocido en el sector de la seguridad digital gracias a nuestro multipremiado blog We Live Security. Allí están disponibles sus excelentes investigaciones sobre la actividad de las APT, tanto resumida como en detalle. Los clientes de ESET reciben un adelanto exclusivo de todos los contenidos de We Live Security.

TOME DECISIONES CRUCIALES CON RAPIDEZ

Toda esta información les sirve a las organizaciones para tomar decisiones cruciales y les da una ventaja estratégica en la lucha contra la delincuencia digital. Permite entender lo que está ocurriendo en el "lado malo de Internet" dentro de un marco contextual, lo que es indispensable para que su empresa pueda llevar a cabo los preparativos internos con rapidez.

CONTENIDOS PRÁCTICOS Y CUIDADOSAMENTE SELECCIONADOS

Los informes proporcionan un amplio contexto de lo que está sucediendo y por qué. De esta forma, las organizaciones pueden prepararse con antelación para lo que pueda venir. Por sobre todas las cosas, nuestros expertos se aseguran de que el contenido sea fácil de entender.

ACCEDA A LOS ANALISTAS DE ESET

Cada cliente que solicite el paquete PREMIUM de Informes sobre APT tendrá también acceso a un analista de ESET durante un máximo de cuatro horas al mes, dándole la oportunidad de debatir los temas con más detalle y ayudándolo a resolver cualquier asunto pendiente.

LOS INFORMES SOBRE APT LE OFRECEN:

- Acceso a análisis técnicos y privados en profundidad
- Informes resumidos sobre la actividad de las APT
- Un resumen mensual para los ejecutivos de alto nivel de su empresa
- Acceso directo a un profesional de ciberseguridad de ESET
- Acceso a nuestro servidor MISP

ANÁLISIS EN PROFUNDIDAD

El paquete incluye informes mensuales de análisis técnicos en profundidad que describen las campañas recientes, los nuevos conjuntos de herramientas y temas relacionados. También obtendrá un informe resumido de actividad maliciosa cada dos semanas, donde se describen las últimas campañas de APT que los investigadores de ESET han estado rastreando de varios actores de amenazas, así como sus objetivos de ataque y, por supuesto, los indicadores de compromiso (IoC) asociados. Por último, un resumen mensual combina la información de todos los informes de análisis técnicos y de los informes resumidos de actividad maliciosa publicados el mes anterior en un formato más breve y digerible.

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

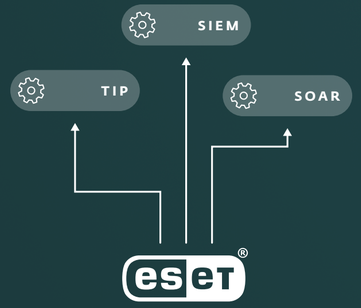
Integre ESET Threat Intelligence en su sistema

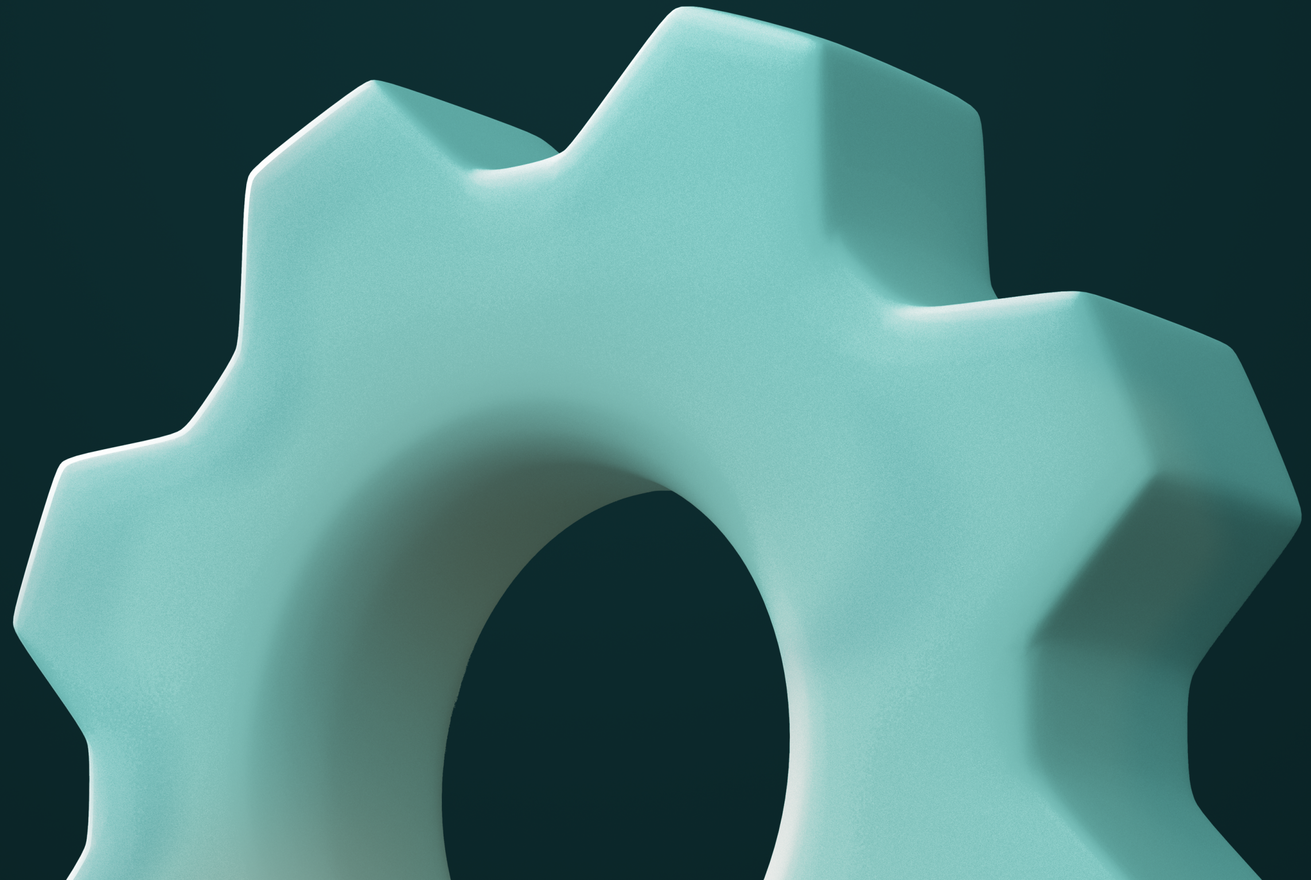
Integrar la telemetría de ESET es sencillo y enriquecerá su TIP, SIEM o SOAR

Disponemos de una API muy completa, con documentación exhaustiva

Suministramos los datos en formatos estandarizados (como JSON y STIX a través de TAXII) para facilitar la integración con cualquier herramienta

Para IBM QRadar, Anomali y Logpoint contamos con manuales de integración paso a paso para una implementación rápida y sencilla, y continuamente añadimos más





Feeds de inteligencia exclusivos de ESET

Potencie su percepción del panorama de las amenazas con una telemetría única. Los feeds de ESET provienen de nuestros centros de investigación globales, proporcionando una perspectiva integral y permitiéndole bloquear rápidamente los IoC en su entorno. Los feeds se entregan en los formatos - JSON - STIX 2.0

FEED DE ARCHIVOS MALICIOSOS

Conozca cuáles son los archivos maliciosos activos en el mundo real. El feed muestra los dominios que se consideran maliciosos, incluyendo el nombre de dominio, la dirección IP, la detección del archivo descargado de la URL y la detección del archivo que estaba tratando de acceder a la URL. Este feed consiste en hashes compartidos de archivos ejecutables maliciosos y datos asociados.

FEED DE DOMINIOS

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

FEED DE IP

Este feed comparte las IP consideradas maliciosas y los datos asociados a ellas. La estructura de los datos es muy similar a la utilizada para los feeds de dominios y URL. El objetivo principal en este caso es entender cuáles son las direcciones IP maliciosas que prevalecen actualmente en el mundo real, bloquear las IP de mayor gravedad, detectar las que son menos graves, y seguir investigando basándose en datos adicionales para ver si ya han causado daño.

FEED DE URL

Al igual que el feed de dominios, el feed de URL busca direcciones específicas. Incluye información detallada sobre datos relacionados con las URL, así como sobre los dominios que las alojan. Toda la información se filtra para mostrar solamente los resultados de alta fiabilidad e incluye información fácil de entender sobre el motivo por el que se marcó la URL como maliciosa.

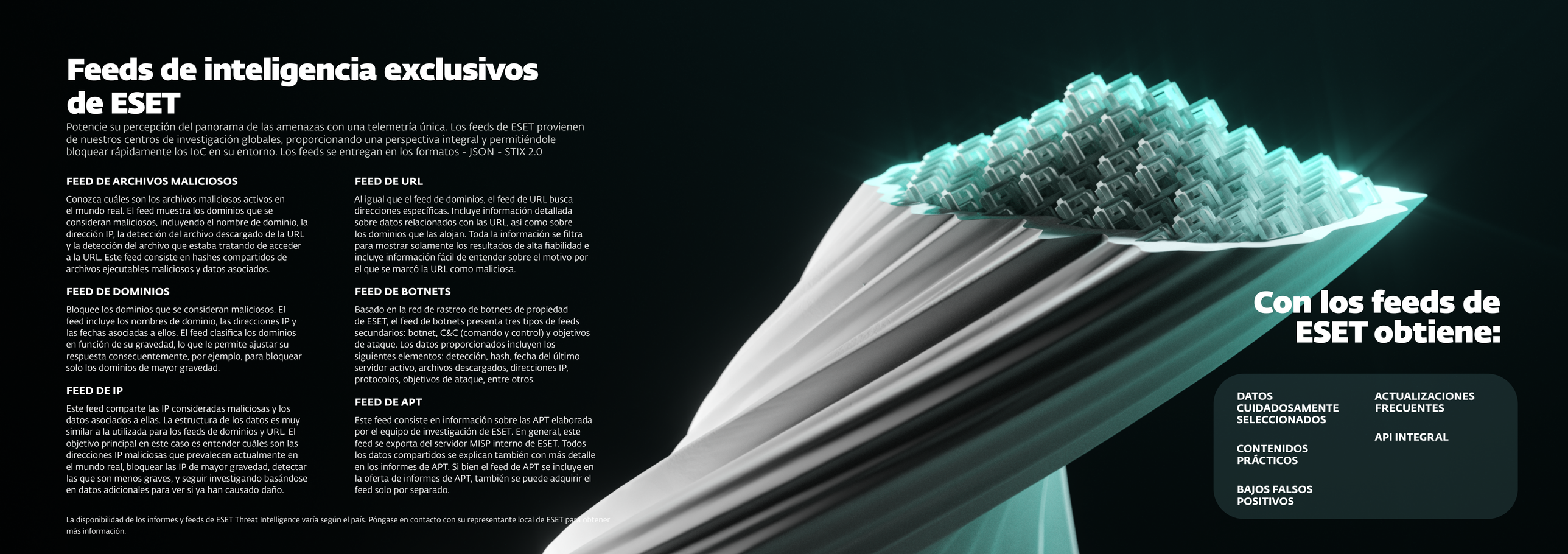
FEED DE BOTNETS

Basado en la red de rastreo de botnets de propiedad de ESET, el feed de botnets presenta tres tipos de feeds secundarios: botnet, C&C (comando y control) y objetivos de ataque. Los datos proporcionados incluyen los siguientes elementos: detección, hash, fecha del último servidor activo, archivos descargados, direcciones IP, protocolos, objetivos de ataque, entre otros.

FEED DE APT

Este feed consiste en información sobre las APT elaborada por el equipo de investigación de ESET. En general, este feed se exporta del servidor MISP interno de ESET. Todos los datos compartidos se explican también con más detalle en los informes de APT. Si bien el feed de APT se incluye en la oferta de informes de APT, también se puede adquirir el feed solo por separado.

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



Con los feeds de ESET obtiene:

- DATOS CUIDADOSAMENTE SELECCIONADOS
- ACTUALIZACIONES FRECUENTES
- API INTEGRAL
- CONTENIDOS PRÁCTICOS
- BAJOS FALSOS POSITIVOS

Acerca de ESET

Por más de 30 años, ESET® ha estado desarrollando soluciones de seguridad y servicios líderes en la industria con el objetivo de suministrar una protección exhaustiva en múltiples capas a empresas y consumidores de todo el mundo. ESET ha sido una empresa pionera de la industria en tecnologías de aprendizaje automático y en la nube que previenen, detectan y responden al malware. ESET es una empresa privada que promueve la investigación y el desarrollo científico en todo el mundo.

ESET EN NÚMEROS

+1000 millones de usuarios de Internet protegidos

+400 mil clientes corporativos

+200 países y territorios

13 centros de investigación y desarrollo mundiales

ALGUNOS DE NUESTROS CLIENTES

Canon

protegido por ESET desde 2016
más de 32.000 endpoints

T · ·

partner de seguridad ISP desde 2008
base de clientes de 2 millones

MITSUBISHI MOTORS
Drive your Ambition

protegido por ESET desde 2017
más de 9.000 endpoints

Allianz Suisse

protegido por ESET desde 2016
más de 4.000 buzones de correo

¿Por qué elegir ESET?

ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES

CERTIFICACIÓN DE SEGURIDAD ISO

CERTIFICACIÓN DE SEGURIDAD ISO

ESET cumple con ISO/IEC 27001:2013, un estándar de seguridad de reconocimiento y aplicación internacional para la implementación y gestión de la seguridad de la información. La certificación es otorgada por SGS, un organismo acreditado de certificación independiente, y demuestra el pleno cumplimiento de ESET con las mejores prácticas líderes en la industria.

RECONOCIMIENTO DE LA INDUSTRIA

Reconocido en 2021 como Proveedor Autorizado por Gartner® Peer Insights™ 'Voice of the Customer': Plataformas de protección para endpoints

Por sus contribuciones a la comunidad, ESET obtuvo el premio Tech Cares 2021 de TrustRadius

Gartner, "Gartner® Peer Insights™ 'Voice of the Customer': Endpoint Protection Platforms", por Peer Contributors, 25 de noviembre de 2021. Gartner no patrocina a ningún proveedor, producto o servicio descrito en sus publicaciones de investigación, y no les aconseja a los usuarios de tecnología que elijan a sus proveedores basándose solamente en las calificaciones más altas u otra designación. Las publicaciones de investigación de Gartner se basan en las opiniones de la organización de investigación de Gartner y no deben interpretarse como declaraciones de hecho. Gartner desestima todas las garantías, expresas o implícitas, con respecto a esta investigación, incluyendo las garantías de comercio o idoneidad para un propósito en particular. EL logotipo de Gartner Peer Insights Customer First es una marca comercial y de servicio de Gartner, Inc., y/o sus afiliados, y aquí se usa con permiso. El programa Gartner Peer Insights Customer First representa el compromiso de la organización de solicitar revisiones a sus clientes utilizando estrategias de abastecimiento programático y mejores prácticas. No representa las opiniones ni la aprobación de Gartner ni de sus afiliados.
Más información: https://blogs.gartner.com/reviews-pages/customer-first-landing-page/

¿Por qué elegir ESET?

RECONOCIMIENTOS DE ANALISTAS

IDC ANALYZE THE FUTURE

ESET ha sido reconocida como Major Player en seguridad para endpoints en las evaluaciones de proveedores llevadas a cabo por IDC MarketScape, tanto en Seguridad moderna de endpoints para grandes empresas en todo el mundo 2021 como en Seguridad moderna de endpoints para pequeñas y medianas empresas 2021.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET ha sido reconocida como Top Player por cuarto año consecutivo en el Cuadrante de mercado 2021 de protección contra amenazas persistentes avanzadas (APT) de Radicati.

MITRE ATT&CK

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

"La implementación fue bastante sencilla. Gracias a la ayuda del personal técnico bien preparado de ESET, nuestra nueva solución de seguridad de ESET estaba lista y funcionando en unas pocas horas."

Gerente de TI, Diamantis Masoutis S.A.,
Grecia; más de 6000 equipos

"Quedamos muy asombrados con el soporte y la asistencia que nos brindó ESET. Además de ser un gran producto, la excelente atención y el soporte que recibimos fue lo que en definitiva nos convenció de migrar todos los sistemas de Primoris a ESET en forma global."

Joshua Collins, Gerente de Operaciones del Centro de Datos,
Primoris Services Corporation, Estados Unidos; más de 4000 equipos


eset
Digital Security
Progress. Protected.