INFORMACIÓN GENERAL DEL PRODUCTO

THREAT INTELLIGENCE

Extienda su inteligencia de seguridad
desde la red local hasta el ciberespacio global

ENJOY SAFER TECHNOLOGY™

30 AÑOS DE INNOVACIÓN CONTINUA EN SEGURIDAD

¿En qué se diferencia ESET?

EXPERIENCIA HUMANA Y APRENDIZAJE AUTOMÁTICO

El uso de técnicas de aprendizaje automático para automatizar las decisiones y evaluar las posibles amenazas es una parte vital de nuestro enfoque. La experiencia humana es primordial para proporcionar la inteligencia de amenazas más precisa posible, dado que los actores maliciosos son oponentes inteligentes.

SISTEMA DE REPUTACIÓN

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, lo que les brinda a los clientes el mayor nivel de confianza cuando visualizan la información y los informes dentro de su consola.

PRESENCIA MUNDIAL

ESET forma parte de la industria de seguridad desde hace más de 30 años, tiene oficinas en 22 países, laboratorios de investigación y desarrollo en 13, 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 mundial sobre las tendencias y amenazas más recientes.

Panel de control de ESET Threat Intelligence

Informes de alertas tempranas y feeds

Informes

INFORME DE MALWARE DIRIGIDO

Lo mantiene informado sobre los posibles ataques en preparación o los ataques en curso dirigidos específicamente contra su organización. El informe incluye cadenas de reglas YARA, información de reputación, binarios similares, detalles de archivos, resultado del sandboxing en la nube y más.

INFORME: ACTIVIDAD DE BOTNETS

Proporciona datos periódicos y cuantitativos sobre las familias de malware identificadas y las variantes de malware de tipo botnet. El informe proporciona datos procesables que incluyen los servidores de Comando y Control (C&C) involucrados en la administración de las botnets, muestras de las botnets, estadísticas semanales globales y una lista de los objetivos de cada malware.

INFORME DE CERTIFICADOS SSL FALSIFICADOS

Se genera cuando ESET detecta un certificado SSL recién lanzado por una autoridad certificadora que tiene un activo muy similar al proporcionado por el cliente durante la configuración inicial. Puede incluir, por ejemplo, las próximas campañas de phishing que están intentando utilizar indebidamente este certificado. El informe muestra los atributos clave del certificado, las coincidencias de reglas YARA y los datos del certificado.

INFORME DE PHISHING DIRIGIDO

Muestra datos sobre todas las actividades de correo electrónico de phishing dirigidas a la organización seleccionada. El informe suministra información de la campaña de phishing, incluyendo el tamaño de la campaña, la cantidad de clientes, las capturas de pantalla con la URL, la vista previa del correo electrónico de phishing, la ubicación de los servidores y mucho más.

Feeds

FEED DE BOTNET

Cuenta con tres tipos de feeds que verifican más de 1000 objetivos por día, incluyendo información sobre la botnet en sí, los servidores involucrados y sus objetivos de ataque. Los datos proporcionados directamente por estos feeds incluyen los siguientes elementos: detección, hash, fecha del último servidor activo, archivos descargados, direcciones IP, protocolos, objetivos de ataque y muchos más.

FEED DE DOMINIO

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.

FEED DE ARCHIVO MALICIOSO

Muestra los ejecutables que se consideran maliciosos, y reconoce y comparte información como SHA1, MD5, SHA256, detección, tamaño y formato del archivo.

FEEDS PERSONALIZADOS

ESET es capaz de proporcionar un feed completamente nuevo basado en los requisitos específicos de la organización. Además, todos los feeds disponibles actualmente se pueden personalizar de acuerdo con las necesidades del cliente.

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.

Características técnicas de ESET Threat Intelligence

FEEDS DE DATOS EN TIEMPO REAL

Los feeds de datos de ESET Threat Intelligence utilizan los formatos STIX/TAXII ampliamente admitidos, lo que facilita su integración con las herramientas SIEM existentes. Esta integración ayuda a fortalecer a los proveedores de servicios y les brinda la información más reciente sobre el panorama de amenazas para predecirlas y prevenirlas antes de que ataquen. Actualmente hay tres tipos principales de feeds disponibles: Feed de botnet, de archivo malicioso y de dominio. Todos los feeds que contienen nuevos metadatos se actualizan cada 5 minutos.

INFORMES DE ALERTAS TEMPRANAS

ESET Threat Intelligence proporciona informes basados en las coincidencias de reglas YARA, ya sea en programas, actividades o configuraciones relacionadas que se estén preparando o que ya se estén utilizando en un ataque contra una organización específica o su cliente.

POTENTE API

ESET Threat Intelligence incluye una API completa que está disponible para automatizar informes, reglas YARA y otras funcionalidades de modo de permitir la integración con otros sistemas utilizados dentro de las organizaciones.

ENVÍO DE MUESTRAS DE MALWARE PARA ANDROID

Con ESET Threat Intelligence, es posible monitorear si el malware para Android está intentando atacar las aplicaciones móviles de la empresa. Esto es sumamente importante para los bancos y otras industrias que cuentan con aplicaciones móviles propias. Además, en cualquier momento, la empresa puede cargar una aplicación para Android en ESET Threat Intelligence y realizar un análisis completo del archivo .apk.

REGLAS YARA

ESET Threat Intelligence permite configurar reglas personalizadas para obtener la información específica en la que estén interesados los ingenieros de seguridad. Una vez configuradas, las organizaciones obtienen detalles valiosos, como la cantidad de veces que se detectó la amenaza en todo el mundo, las direcciones URL que contienen código malicioso, el comportamiento malicioso en el sistema, dónde se detectó, ente otros datos.

ANÁLISIS AUTOMATIZADO DE MUESTRAS

Crea un informe personalizado del archivo o hash enviado, lo que proporciona información valiosa para la toma de decisiones basadas en hechos y en la investigación de incidentes.

+54 9 11 3657 0780
WhatsApp: mensajes/llamadas

Contacto inmediato con nuestro chat en línea www.zma.la

CASA CENTRAL
Lavalle 381 piso 3º | Tel: (54 11) 5219-5555 | C1047AAG
Ciudad Autónoma de Buenos Aires | ARGENTINA
www.zma.la - info@zma.la

ZMA®
IT SOLUTIONS
Value Added Solutions Distributor