Kaspersky Network Security Threat Data Feeds

kaspersky preparados para el futuro

La protección de endpoints por sí sola no es suficiente.

También es necesaria la protección a nivel de red.

A continuación, le explicamos los motivos:

- La protección contra distintos tipos de ataques debe comprender varias capas.
- No todos los hosts de su entorno dispondrán de protección de seguridad para endpoints, por ejemplo, no todos los servidores críticos para la empresa o los hosts de una red industrial.
- Algunos hosts "protegidos" pueden no estar actualizados con firmas / hashes / reglas de detección.

Kaspersky Network Security Threat Data Feeds

En la actualidad, casi todas las empresas cuentan con un firewall de última generación (NGFW). Es uno de los controles de seguridad de red modernos más eficaces, ya que aumenta los niveles de protección de las redes corporativas frente a los ciberataques.

La mayoría de los NGFW son capaces no solo de usar los conocimientos internos sobre las ciberamenazas, sino también de ofrecer funcionalidades que permiten usar listas dinámicas de indicadores de compromiso (IoC) procedentes de fuentes externas para bloquear las ciberamenazas en tiempo real.

Configurar rápidamente las reglas de detección de NGFW para adelantarse siempre a los adversarios es casi imposible. Por eso, es esencial el conocimiento externo de la inteligencia de amenazas. Aporta un elemento adicional fundamental de protección a su entorno que, de otro modo, podría pasar desapercibido.

Kaspersky ofrece colecciones de IoC especialmente creadas que, al importarse a un NGFW, mejoran de forma considerable el nivel de protección de seguridad de la red corporativa frente a las amenazas más frecuentes, sin necesidad de una integración o configuración complicadas y conservando la topología de red actual.

Kaspersky Network Security Threat Data Feeds se basa en los Kaspersky Threat Intelligence Data Feeds, que contienen listas actualizadas regularmente de varios tipos de IoC (como direcciones IP y dominios). El uso de esta información le permite supervisar o bloquear el acceso de los usuarios a recursos de red peligrosos.

Más información

Integraciones de Kaspersky Network Security Data Feeds

Recopilación y procesamiento de datos

Kaspersky Network Security Data Feeds está compuesto por múltiples listas, cada una de ellas centrada en un tipo específico de ciberamenaza. Las fuentes de datos contienen listas de direcciones IP con el puntaje de amenaza más alto y dominios de primer y segundo nivel de recursos que se conocen por distribuir malware, funcionar como centros de comando y control (C&C) de botnets o alojar recursos de phishing.

Además, provienen de una fusión de diversas fuentes confiables, como Kaspersky Security Network, nuestros rastreadores web proactivos, el servicio de supervisión de botnets 24/7 (incluyendo sus objetivos y actividades), y hosts y servicios de inteligencia de direcciones IP.

Todos los datos agregados se inspeccionan cuidadosamente en tiempo real mediante varias técnicas de reprocesamiento, como criterios estadísticos, entornos de prueba, motores heurísticos, herramientas de similitud, creación de perfiles de comportamiento, validación de analistas y verificación de listas de permisos.

Aspectos destacados

Actualizaciones en tiempo real

Todas las fuentes de datos se generan de manera automática en tiempo real según hallazgos en todo el mundo, lo que proporciona niveles de tasas de detección y precisión altas.

Kaspersky Security Network proporciona visibilidad sobre un porcentaje importante de todo el tráfico de Internet, que abarca decenas de millones de usuarios finales en más de 213 países.

Soporte nativo

Soporte nativo para los NGFW más populares:

- Cisco
- FortiGate
- Palo Alto
- Otros NGFW de terceros (con funcionalidad de listas dinámicas externas con soporte básico de autenticación)

Autenticación segura

Las fuentes de datos ofrecen una serie de métodos de autenticación adaptados a las distintas necesidades de seguridad y preferencias de integración.

Integración fácil

Las guías de configuración paso a paso complementarias para cada NGFW compatible y el servicio de soporte técnico de Kaspersky facilitan la configuración y ofrecen un valor inmediato.

Disponibilidad continua

Todas las fuentes se generan y se controlan mediante una infraestructura muy tolerante a fallas, lo que garantiza una disponibilidad continua.

Datos 100 % validados

Las fuentes de datos plagadas de falsos positivos son peligrosas ya que pueden bloquear recursos legítimos.

Por ello, Kaspersky Network Security Data Feeds se somete a pruebas exhaustivas y aplica filtros antes de publicar sus fuentes, garantizando la distribución de datos 100 % validados.

Beneficios

Refuerce sus soluciones de defensa de la red

con IOC continuamente actualizados para bloquear automáticamente las ciberamenazas más frecuentes.

Evite la filtración de activos confidenciales

y de propiedad intelectual de las máquinas infectadas fuera de la organización.

Bloquee rápidamente las ciberamenazas para proteger

su organización frente a las ciberamenazas y mantener la continuidad de la actividad.

Kaspersky Threat Data Feeds

Más información

https://latam.kaspersky.com

#kaspersky
#bringonthefuture