SERVICIOS DE INTELIGENCIA: FUENTES DE DATOS DE AMENAZAS

Aproveche al máximo su sistema SIEM con un nivel adicional de protección contra malware y URL peligrosas gracias a los completos datos de inteligencia de KL.

Las familias y variantes de malware han crecido de manera exponencial en los últimos años; Kaspersky Lab detecta actualmente alrededor de 325 000 muestras de malware nuevas cada día. Para defender sus endpoints contra estas amenazas, la mayoría de las empresas implementan medidas de protección clásicas, como soluciones antimalware, prevención de intrusiones o sistemas de detección de amenazas. En un entorno tan cambiante donde la ciberseguridad siempre trata de mantenerse un paso por delante del cibercrimen, estas soluciones clásicas deben reforzarse mediante el acceso a la inteligencia más reciente contra amenazas.

Las fuentes de datos de amenazas de Kaspersky Lab están diseñadas para integrarse en los sistemas de información relacionada con la seguridad y gestión de eventos (SIEM) existentes, ofreciendo así un nivel adicional de protección. La integración permite correlacionar los registros que recibe el SIEM de diferentes dispositivos de red con las fuentes de datos de URL que proceden de Kaspersky Lab. **Se incluye una conexión con HP ArcSight SIEM.**

CASOS DE USO/VENTAJAS DEL SERVICIO

- **Mejora de la solución SIEM aprovechando las fuentes de datos sobre URL peligrosas procedentes de Kaspersky Lab.** El sistema SIEM recibe una notificación sobre las URL de malware, las URL de phishing, las URL de mando y control de la botnet de los registros que recibe el SIEM de diferentes dispositivos de red (PC de los usuarios, proxies de red, firewalls, otros servidores).
- **Objetivos de la investigación.** Aprovechar la información sobre URL peligrosas y hash MD5 de archivos maliciosos con objetivos de investigación.

DESCRIPCIÓN DE LAS FUENTES DE DATOS

Kaspersky Lab ofrece dos tipos de fuentes de datos de amenazas:

1. URL y máscaras maliciosas
2. Hash MD5 de base de datos de objetos maliciosos

DESCRIPCIÓN DE LAS FUENTES DE DATOS
URL maliciosas: conjunto de URL que abarcan los enlaces y sitios web más peligrosos. Están disponibles los registros enmascarados y no enmascarados.
URL de phishing: conjunto de URL identificadas por Kaspersky Lab como sitios de phishing. Están disponibles los registros enmascarados y no enmascarados.
URL de mando y control de la botnet: conjunto de URL de servidores de mando y control (C&C) de la botnet y objetos maliciosos relacionados. Se incluyen los mandos y controles móviles.
Hash de malware (ITW): conjunto de hash de archivos que abarcan el malware "suelto" (ITW, del inglés " in-the-wild") más peligroso detectado por los usuarios de Kaspersky Security Network. La base contiene los hash con veredictos de Kaspersky para cada objeto.
Hash del malware (UDS): conjunto de hash de archivos detectados por las tecnologías con asistencia en la nube de Kaspersky (UDS, sistema de detección urgente, del inglés "Urgent Detection System") basado en los metadatos y las estadísticas de un archivo (sin tener el objeto en sí). Esto permite que el sistema pueda identificar el malware que no se detecta por otros métodos. Esto también se puede describir como "hash malware identificado recientemente".
Hash malware Android: conjunto de hash de archivos para detectar objetos maliciosos que infectan plataformas móviles Android.

¿POR QUÉ KASPERSKY LAB?

- Fundada y dirigida por el experto en seguridad más prominente del mundo, Eugene Kaspersky
- Relaciones de colaboración con organismos encargados de hacer cumplir las leyes, como Interpol y CERTS
- Herramientas en la nube que supervisan millones de ciberamenazas en todo el mundo en tiempo real
- Equipos globales que analizan y comprenden todos los tipos de amenazas de Internet
- La mayor empresa de software de seguridad independiente del mundo centrada en la inteligencia sobre amenazas y el liderazgo en tecnología
- Líder indiscutible en más pruebas independientes de detección de malware que cualquier otro proveedor
- Identificado como líder por Gartner, Forrester e IDC

Para obtener más información sobre Kaspersky Intelligence Services, póngase en contacto con nosotros a través de intelligence@kaspersky.com.
PARA OBTENER MÁS INFORMACIÓN, VISITE www.kaspersky.es.

© 2015 Kaspersky Lab. Todos los derechos reservados. Las marcas registradas y logos son propiedad de sus respectivos dueños.
Microsoft, Windows Server y SharePoint son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en Estados Unidos y en otros países.

KASPERSKY lab