Kaspersky APT Intelligence Reporting

kaspersky BRING ON THE FUTURE

Kaspersky APT Intelligence Reporting

Los clientes de Kaspersky APT Intelligence Reporting reciben un acceso único y continuo a nuestras investigaciones y descubrimientos, incluidos datos técnicos completos (en una variedad de formatos) sobre cada APT a medida que se descubren, así como sobre las amenazas que nunca se harán públicas. Los informes incluyen un resumen ejecutivo que ofrece información orientada al nivel C y fácil de entender, que describe la APT relacionada, y una descripción técnica detallada de la APT con los IOC y las reglas YARA relacionadas. De esta manera, se entrega a los investigadores de seguridad, analistas de malware, ingenieros de seguridad, analistas de seguridad de redes e investigadores de APT datos procesables que permiten una respuesta rápida y precisa ante la amenaza.

También, nuestros expertos lo alertarán inmediatamente sobre cualquier cambio que detecten en las tácticas de los grupos ciberdelincuentes. Además, tendrá acceso a la base de datos completa de informes de ATP, otro componente importante de investigación y análisis en sus defensas de seguridad.

Ventajas

Asignación de MITRE ATT&CK
Todos los TPP descritos en los informes se le asignan a MITRE ATT&CK, lo que facilita una mejor detección y respuesta mediante el desarrollo y priorización de los casos de uso de supervisión de seguridad correspondientes, la realización de análisis de brechas y la prueba de las defensas actuales contra los TPP relevantes.

Información acerca de APT no públicas
Por diversas razones, no todas las amenazas de alto perfil se hacen públicas. Pero se comparten con todos nuestros clientes.

Acceso privilegiado
Obtención de descripciones técnicas sobre las amenazas más recientes durante investigaciones en curso, antes de que se hagan públicas.

Análisis retrospectivo
Se ofrece acceso a todos los informes privados publicados con anterioridad durante el período de su suscripción.

Acceso a datos técnicos
Incluye una lista ampliada de IOC, disponible en formatos estándar, como openIOC o STIX y acceso a nuestras reglas YARA.

Perfiles de ciberdelincuentes
Incluye el posible país de origen y la actividad principal, las familias de malware utilizadas, las industrias y las geografías objetivo y las descripciones de todas las TTP utilizadas, con asignación a MITRE ATT&CK.

Supervisión continua de campañas de APT
Acceso a inteligencia procesable durante la investigación con información sobre la distribución de ATP, IOC, comandos e infraestructuras, etc.

API RESTful
Integración y automatización perfectas de sus flujos de trabajo de seguridad.

latam.kaspersky.com