Hillstone Cloud-Sandbox:
Identificación de Archivos Maliciosos y Plataforma de Detección

El malware avanzado se ha vuelto tan sofisticado que puede evadir fácilmente las soluciones de seguridad tradicionales, incluyendo los Firewalls, los IPS y las tecnologías Anti-Virus. Para hacer frente al malware avanzado, Hillstone Cloud Sandbox ofrece una plataforma exclusiva y avanzada para la detección de amenazas que puede emular un entorno de ejecución y analizar todas las actividades relacionadas con los archivos maliciosos, identificar las amenazas avanzadas y colaborar con las soluciones existentes para proporcionar una rápida solución.

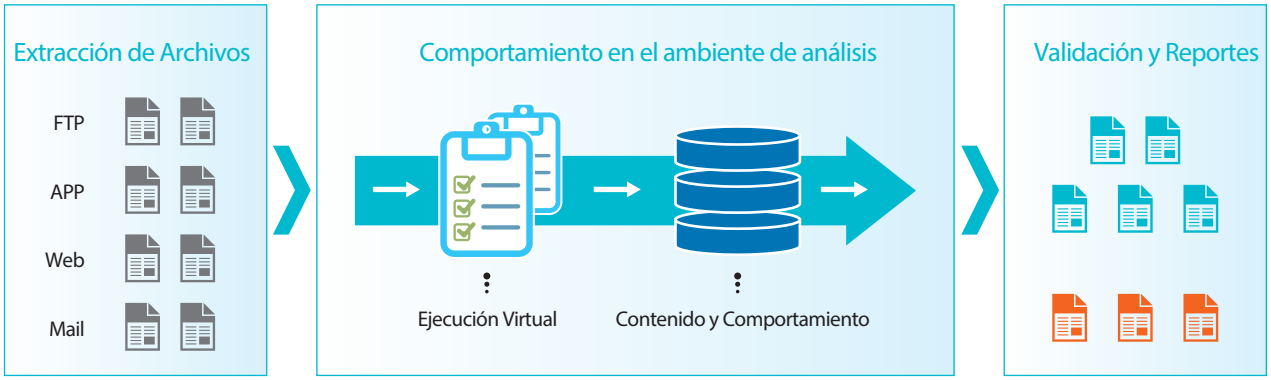

Figura 1. Hillstone Cloud-Sandbox

Hillstone Cloud Sandbox está compuesto de tres módulos: Análisis estático, análisis de comportamiento e inteligencia en la nube. Los tres módulos trabajan juntos para garantizar la eficiencia y la eficacia en la detección de archivos maliciosos.

www.hillstonenet.com
Phone: 1-800-889-9860

Análisis estático: Hillstone Cloud Sandbox ejecuta un análisis estático de firmas a los archivos, identificando el tipo de archivo, el formato, y la firma de malware conocido. Además, la tecnología de filtro frontal (Ej URL lista blanca, la validación de firma de archivos, base de datos de muestra en la nube) puede descartar a las amenazas conocidas para reducir la carga de trabajo de la sandbox.

Análisis Comportacional: Hillstone Cloud Sandbox puede simular múltiples sistemas operativos y entornos activos para así disparar el comportamiento de archivos en los entornos simulados que se parecen mucho a los reales en entornos de producción. El Cloud Sandbox utiliza un modelo de aprendizaje de máquina para validar el comportamiento de los archivos.

Inteligencia en la Nube: Mediante el uso de información de inteligencia sobre las amenazas recopiladas a nivel mundial desde los nodos de red Hillstone, Hillstone Cloud Sandbox compara la información estática y el comportamiento de los archivos en contra la información de inteligencia, tales como las firmas de virus, sitios web de phishing y los nombres de dominio maliciosos, y le da a cada archivo una puntuación de evaluación de riesgos, en lugar de simplemente definirlo como bueno o malo.

Por medio del análisis estático, el análisis del comportamiento y la inteligencia de nube, el Hillstone Cloud Sandbox detecta el malware con una baja tasa de falsos positivos y alta tasa de detección.

Detalles del Producto

Alta tasa de detección con análisis estático y conductual

La base de datos de malware de Hillstone Cloud contiene más de mil millones de muestras. Detecta rápidamente si cualquier archivo cargado coincide con las muestras de malware. Hillstone Cloud Sandbox puede simular entornos en funcionamiento y disparar comportamientos como la creación de procesos, la modificación del registro y solicitar una cadena histórica. Las amenazas desconocidas pueden ser detectadas analizando el comportamiento de archivos.

Despliegue instantáneo de infraestructura en la nube

Hillstone Cloud Sandbox se integra perfectamente con la tecnología y soluciones existentes, como el Firewall Hillstone de próxima generación y Hillstone CloudEdge. Puede ser desplegado instantáneamente, sin problemas y sin interrupciones de la red.

Protección de tráfico cifrado

Dado que la tecnología de cifrado SSL se ha popularizado tanto, más y más aplicaciones utilizan HTTPS. Sin embargo, el malware de hoy también utiliza la tecnología de encriptación SSL para escapar la detección. Hillstone Cloud Sandbox puede descifrar el tráfico cifrado y restaurar los archivos en tráfico cifrado. Con este enfoque, se puede detectar el malware, incluso si está oculto en el tráfico cifrado.

Medidas contra la tecnología anti-sandbox

Hillstone Cloud Sandbox es compatible con la identificación y detección de malware contra la sandbox. Al ocultar la información de procesado, como el modelo de kernel y su información de registro, Hillstone Cloud Sandbox puede simular los entornos en ejecución. Para evitar que el malware escape la detección, Hillstone Cloud Sandbox simula las operaciones manuales e interactivas y se hace cargo de la API, de modo que el comportamiento del malware se pueda activar.

Información completa de amenazas en los informes

Tras la detección de malware y amenazas desconocidas, Hillstone Cloud Sandbox muestra las alarmas y notificaciones, así como los informes completos de comportamiento del malware en el panel de administración del Firewall. El informe muestra el comportamiento de la red, del proceso, de los archivos y la información clave del archivo. El proceso del ataque se visualiza a través del análisis de Kill Chain en las plataformas del Firewall, así los administradores de seguridad pueden tomar las medidas apropiadas.

Actualización constante de la base de datos de firmas

Hillstone Cloud Sandbox genera inteligencia contra amenazas a partir del malware que detecta y actualiza la información de inteligencia en la base de firmas de los Firewalls Hillstone de próxima generación. Ayuda a los administradores a afinar sus estrategias de seguridad para proteger los recursos de informática de nuevos y más avanzados ataques.

Specificaciones

Modelo	Archivos/Día	Plataformas Recomendadas
Cloud-Sandbox 300	300	Hillstone E1000 Series, E2000 Series, E3000 Series, T1860, T2860, NIPS S600, S1060, S1560 and Hillstone CloudEdge
Cloud-Sandbox 500	500	Hillstone E5000 Series, T3860, T5860, NIPS S2160 and S2660
Cloud-Sandbox 1000	1,000	Hillstone E6000 Series

Version: EX-08.01-CloudSandbox-V2.0-0217-SP-01