Check Point
SOFTWARE TECHNOLOGIES LTD.

Servicio de ThreatCloud Emulation

Descubra y detenga ataques nuevos, dirigidos y de día cero

Servicio de ThreatCloud Emulation

EL RETO

Con el aumento en sofisticación de las ciberamenazas, muchos ataques dirigidos comienzan aprovechando vulnerabilidades de software en archivos descargados o adjuntos de correo.

Estas amenazas incluyen nuevos exploits, o incluso variantes de exploits ya conocidos que surgen casi diariamente sin firmas disponibles y, como consecuencia, sin una solución estándar que detecte dichas variantes. Las amenazas nuevas y no descubiertas requieren de soluciones innovadoras que vayan más allá de las firmas de las amenazas conocidas.

SOLUCIÓN

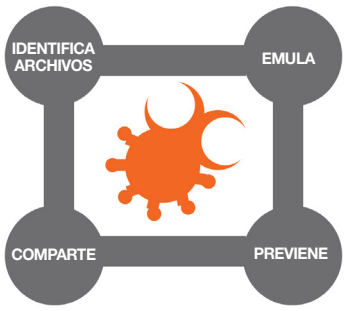
ThreatCloud Emulation evita las infecciones que provienen de exploits no descubiertos, ataques dirigidos y de día cero. Esta innovadora solución inspecciona rápidamente los archivos y los ejecuta en un sandbox virtual para descubrir comportamientos maliciosos. Se evita que el malware descubierto entre en la red. ThreatCloud Emulation de Check Point informa al servicio ThreatCloud™ y comparte automáticamente con otros clientes de Check Point la información de la nueva amenaza identificada.

Las soluciones tradicionales se han centrado en la detección, proporcionando notificaciones después de que una amenaza ya se ha introducido en la red. Con ThreatCloud Emulation se bloquean las nuevas amenazas y no se produce la infección.

CÓMO FUNCIONA

Identifica archivos sospechosos en la organización

- Identifica archivos en adjuntos de correo o descargas desde la web
- Los archivos sospechosos se envían a ThreatCloud Servicio de emulación
- Soportado sin la infraestructura de Check Point usando un agente único para el servidor Exchange
- Soportado en los gateways de seguridad existentes que ejecutan R77



Emulación de archivo

- Ejecuta los archivos para su emulación en un entorno sandbox virtual
- Inspeccione el comportamiento de archivos en múltiples sistemas operativos y versiones de Office
- Actividades monitorizadas: sistema de archivo, registro del sistema, procesos y conexiones de red
- Las actividades sospechosas de los archivos son marcadas, y un algoritmo único determina más adelante si el archivo está involucrado en actividades maliciosas
- Genera un informe detallado incluyendo los detalles de archivo, detalles de actividad anormal y capturas reales del entorno sandbox mientras se ejecuta el archivo

CARACTERÍSTICAS CLAVE

- Identifica nuevo malware oculto en archivos Adobe PDF, Microsoft Office, ejecutables y comprimidos
- Realiza la emulación de ejecución de archivos y documentos en un sandbox seguro para detectar las amenazas
- Protección frente a amenazas que dirigidas a múltiples entornos de OS Windows
- Realiza la emulación de archivos dentro de comunicaciones SSL y TLS
- Evita que los archivos maliciosos entren en la organización

BENEFICIOS PRINCIPALES

- Servicio basado en la nube, funciona con su infraestructura existente. No necesita instalar nuevos equipos
- Reduce la carga de operación con un bajo precio mensual para toda la organización, en base al volumen de archivos entrantes
- La integración exclusiva con Exchange ofrece protección monitorizando los adjuntos de correo electrónico de las amenazas del correo electrónico
- La existencia de cero falsos positivos implica que puede securizar su red sin detener el flujo del negocio
- Incremente la seguridad con el intercambio de información de nuevas amenazas con ThreatCloud

softwareblades™

Datasheet: Servicio ThreatCloud Emulation de Check Point

Evita que los archivos maliciosos entren en la organización

- Los archivos maliciosos son detenidos en línea antes de que entren en la red

Compartir información maliciosa con ThreatCloud

- Actualización inmediata en ThreatCloud para evitar que los archivos maliciosos detectados recientemente entren en otras organizaciones

CARACTERÍSTICAS DE THREATCLOUD EMULATION

Servicio de ThreatCloud Emulation

El servicio de ThreatCloud Emulation es una subscripción rentable donde los clientes pagan solo por la cantidad de archivos entrantes en la organización. No se requieren cambios en la organización — los archivos pueden enviarse para su emulación desde un gateway de seguridad existente o desde un agente para el servidor de Exchange. Una cuota global para la organización permite una gestión centralizada y visibilidad tanto de la información de amenazas y como de la utilización del servicio.

Sandboxing virtual

Threat Emulation deCheck Point funciona interceptando y filtrando los archivos entrantes, ejecutándolos en un entorno virtual, y marcando aquellos archivos que presentan un comportamiento sospechoso o malicioso asociado comúnmente con el malware, como la modificación del registro, conexiones de red, creación de archivos nuevos, etc. Una vez que se descubren estas nuevas amenazas, la firma del archivo se envía a ThreatCloud para convertir el nuevo malware en una amenaza conocida y documentada que pueda ser prevenida.

Soporte de emulación en múltiples OS

ThreatCloud Emulation de Check Point proporciona múltiples entornos simultáneos para la simulación de archivos: Entornos Windows XP, 7, Microsoft Office y Adobe.

Informe detallado de ThreatCloud Emulation

Se genera un informe detallado por cada emulación de archivos. El informe es sencillo de entender e incluye información detallada sobre cualquier intento malicioso que se produzca durante la ejecución del archivo. El informe proporciona capturas reales del entorno mientras se ejecuta el archivo en todos los sistemas operativos en los que se ejecute la simulación.

Comunicaciones cifradas

Los archivos entregados en la organización a través de SSL y TLS representan un vector de ataque que se pasa por alto por muchas implementaciones estándar de la industria. ThreatCloud Emulation de Check Point mira dentro de los túneles SSL y TLS para extraer y ejecutar los archivos con el objeto de descubrir amenazas ocultas en esos flujos protegidos.

Evitar que los archivos peligrosos entren en la organización

Los archivos vuelven al gateway de seguridad o agente de Exchange con información detallada sobre su actividad desde el Servicio de ThreatCloud Emulation. Los archivos maliciosos no llegan al usuario y son detenidos para evitar una infección dentro de la organización.

Ecosistema ThreatCloud

Las amenazas nuevas descubiertas se envían a ThreatCloud, que puede proteger otros gateways conectados con Check Point. Cada firma de una amenaza recién descubierta se distribuye a otros gateways conectados a Check Point para bloquearlas antes de que la ésta tenga una oportunidad de extenderse. Esta colaboración constante hace del ecosistema ThreatCloud la red anti-amenazas disponible más actualizada y avanzada.

Implementación sencilla y flexible en la organización

ThreatCloud Emulation se implementa de forma que trabaje con las redes existentes. Los archivos pueden enviarse al Servicio de ThreatCloud Emulation o a un Private Cloud Emulation Appliance. Cualquier gateway de seguridad R77 o un agente para el servidor Exchange puede monitorizar los archivos entrantes y enviar aquellos sospechosos a la emulación.

ESPECIFICACIONES

Servicio de ThreatCloud Emulation

Las organizaciones pueden elegir de entre cinco opciones disponibles según el número de archivos inspeccionados mensualmente, empezando desde 10.000 archivos al mes para arriba

Appliances Private Cloud Emulation

Hay disponibles dos opciones de appliances, con un rendimiento general que da soporte a organizaciones de hasta 3.000 usuarios, y por encima de 3.000.

Especificaciones de la emulación	
Archivos soportados en la inspección	Adobe PDF, Microsoft Office, archivos EXE y comprimidos
Entornos de emulación soportados	Microsoft Windows XP, 7; Microsoft Office; Adobe Reader

Especificaciones del gateway de seguridad Para detectar y enviar los archivos al Servicio de ThreatCloud Emulation	
Plataformas soportadas	Appliances Check Point: 2000, 4000, 12000, 13000, y 21000 ejecutando R77 o superior; se soportan otros appliances y "servidores abiertos" con un rendimiento equivalente al de los modelos anteriores
Entorno operativo	SecurePlatform o GAiA

CONTACTE CON CHECK POINT

Oficinas centrales mundiales
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

Oficinas EE.UU.
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com