Funcionalidades Generales Sanboxing

La solución debería proporcionar la funcionalidad de inspeccionar el tráfico entrante en busca de malware desconocido (APT: amenaza persistente avanzada y amenazas de día cero), ransomware con filtro de amenazas avanzado y análisis de ejecución en tiempo real e inspección de tráfico saliente. devoluciones de llamada;

Poseer la capacidad de prevenir amenazas desconocidas;

Debido al hecho de que el malware es muy dinámico y un antivirus reactivo común no puede detectarlos con la misma velocidad con la que se crean sus variaciones, la solución ofrecida debe tener características para prevenir el malware desconocido incluido en la herramienta (día cero);

El dispositivo de protección debe poder enviar archivos traficados automáticamente para su análisis en la solución instalada localmente (en las instalaciones), donde el archivo se ejecutará y simulará en un entorno controlado;

Debe admitir la supervisión de archivos traficados en Internet (HTTP, FTP, HTTP, SMTP), así como archivos traficados internamente entre servidores de archivos que usan SMB en todos los modos de implementación: sniffer, transparente y L3;

La solución debe poder inspeccionar el tráfico cifrado SSL;

La solución debe tener un mecanismo para identificar hosts infectados que intentan acceder a direcciones DNS de dominios maliciosos;

Seleccione a través de la política qué tipos de archivos se someterán a este análisis y prevención;

Implemente e identifique la existencia de malware en archivos adjuntos de correo electrónico y URL conocidas;

Funcionalidades de ATP

mplemente la detección inmediata y el bloqueo de malware que utiliza mecanismos de escaneo en archivos PDF;

La solución debería proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones de Windows 7

La solución debe proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones de Windows 8.1

La solución debería proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones de Windows 10

La solución debe proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones MacOS

La solución debe proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones de Android.

Análisis de soporte de archivos de paquetes de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y class), APK de Android, MacOS y Linux en el entorno sandbox

La solución debe tener una nube de inteligencia patentada por el fabricante que sea responsable de actualizar toda la base de seguridad mediante firmas;

La solución debe admitir topologías de implementación en modo sniffer

La solución debe admitir topologías de implementación integradas (con un firewall, solución de protección de correo electrónico, waf o punto final)

La solución debe admitir topologías de implementación con adaptadores para la integración con soluciones de terceros a través del protocolo ICAP o BCC

La solución debe admitir topologías de implementación mediante el intercambio de archivos.
La solución debe admitir topologías de implementación bajo demanda, es decir, mediante envío manual a través de la consola gráfica.
La solución debe admitir topologías de implementación a través de la API JSON
La solución sandbox debe permitir la carga de máquinas virtuales personalizadas.
Todos los análisis y bloqueos de malware y / o códigos maliciosos deben realizarse en tiempo real y el bloqueo debe ser inmediato, no se aceptarán soluciones que solo detecten malware y / o códigos maliciosos;
La solución debe admitir las reglas de YARA como estándar para crear reglas para la detección de malware
Permita la creación de firmas en tiempo real para las amenazas detectadas mediante el análisis del comportamiento en el entorno limitado con la distribución de la firma local entre los dispositivos integrados, como firewall, puerta de enlace segura de correo electrónico, punto final o firewall de aplicaciones web. Por lo tanto, todos los dispositivos integrados en la solución de sandbox están inmediatamente protegidos contra nuevas amenazas.

Funcionalidades de visibilidad.
Implemente la detección inmediata y el bloqueo de malware que utiliza mecanismos de escaneo en archivos PDF;
La solución debería proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones de Windows 7
La solución debe proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones de Windows 8.1
La solución debería proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones de Windows 10
La solución debe proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones MacOS
La solución debe proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones de Android.
Análisis de soporte de archivos de paquetes de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y class), APK de Android, MacOS y Linux en el entorno sandbox
La solución debe tener una nube de inteligencia patentada por el fabricante que sea responsable de actualizar toda la base de seguridad mediante firmas;
La solución debe admitir topologías de implementación en modo sniffer
La solución debe admitir topologías de implementación integradas (con un firewall, solución de protección de correo electrónico, waf o punto final)
La solución debe admitir topologías de implementación con adaptadores para la integración con soluciones de terceros a través del protocolo ICAP o BCC
La solución debe admitir topologías de implementación mediante el intercambio de archivos.
La solución debe admitir topologías de implementación bajo demanda, es decir, mediante envío manual a través de la consola gráfica.
La solución debe admitir topologías de implementación a través de la API JSON
La solución sandbox debe permitir la carga de máquinas virtuales personalizadas.

Todos los análisis y bloqueos de malware y / o códigos maliciosos deben realizarse en tiempo real y el bloqueo debe ser inmediato, no se aceptarán soluciones que solo detecten malware y / o códigos maliciosos;
La solución debe admitir las reglas de YARA como estándar para crear reglas para la detección de malware
Debería permitir al administrador de la solución descargar el archivo original, analizado por la solución sandbox
En caso de un veredicto positivo, se debe presentar una descripción detallada del comportamiento comprometido de la máquina, que contenga al menos información sobre el Tipo de archivo para fines de auditoría.
En caso de un veredicto positivo, debe proporcionar detalles del comportamiento de la máquina comprometida, que contenga al menos información sobre la fuente de malware IP para fines de auditoría
En caso de un veredicto positivo, debe presentar detalles del comportamiento de la máquina comprometida, que contenga al menos información sobre la IP de destino (cliente que descargó el malware) para fines de auditoría
En caso de un veredicto positivo, debe presentar una descripción detallada del comportamiento de la máquina comprometida, que contenga al menos información sobre el virus total Enlace a referencia para fines de auditoría
En caso de un veredicto positivo, debe presentar un desglose del comportamiento de la máquina comprometida, que contenga al menos un resumen del comportamiento del malware para fines de auditoría.

Requerimientos técnicos de implementación

1- Empresa con técnico certificado en: solución ofertados y CEH, ITIL Foundation y 10 años de experiencia en implementaciones de la solución, Unico ingeniero. (No se permiten certificaciones individuales)
2- Certificación del fabricante de distribución autorizado
3- Servicios técnicos basados en la migración de los equipos actuales y nuevos requerimientos