Gestión de incidentes de seguridad informática

IFCT0109 – Seguridad informática

MF0488_3 (90 horas)

Control de código malicioso

- Introducción
- Sistemas de detección y contención de código malicioso
- Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
- Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
- Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
- Relación de los registros de auditoría de las herramientas de protección frente a códigos maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
- Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso
- Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada
- Resumen

Introducción

Los ataques informáticos son diversos y pueden causar graves daños. Entre los más comunes y peligrosos se encuentran los perpetrados mediante malware o códigos maliciosos. Este término será utilizado de aquí en adelante.

En este capítulo, se aborda el concepto de código malicioso y se examinan en detalle sus diversas formas, modus operandi y los sistemas más utilizados para su detección.

Comprender su funcionamiento no es suficiente para prevenir daños. Es esencial contar con herramientas específicas para su control y contención, adaptadas a las posibles vías de infección y la infraestructura de red de cada organización.

La configuración de estas herramientas debe basarse en criterios predefinidos, alineados con la política de seguridad de la organización. Esto incluye protocolos de respuesta ante la detección de malware y una política de actualización continua para mantener la efectividad de las herramientas.

Además de las herramientas mencionadas, los registros de auditoría pueden ser útiles para detectar y contener malware. Estos registros permiten analizar patrones de comportamiento y estadísticas, facilitando ajustes en la configuración para mejorar la seguridad.

Por último, se exploran los entornos de ejecución controlada y los desensambladores, dos herramientas clave para identificar y comprender el comportamiento del malware, y así establecer medidas de contención más precisas y eficaces.

Sistemas de detección y contención de código malicioso

Conceptos básicos y tipos de códigos maliciosos

Anteriormente, los ciberdelincuentes se vinculaban más con el ciberactivismo o el vandalismo, utilizando ataques como formas de protesta o diversión, con empresas, gobiernos e instituciones como objetivos comunes. Sin embargo, este perfil ha evolucionado hacia uno más peligroso, centrado en el lucro económico mediante el robo de información.

Las motivaciones de los intrusos pueden ser diversas:

- Motivaciones lucrativas: Obtener y vender información valiosa, acceder a bases de datos para enviar spam, entre otros, ..
- Cibercrimen: Tomar el control total o parcial de empresas, realizar fraudes bancarios, robar información privilegiada o exigir rescates tras secuestrar infraestructuras
- Hacktivismo: Realizar ataques como protesta hacia instituciones gubernamentales o empresas, motivados por razones ideológicas o sociales y llevados a cabo por redes descentralizadas
- Ciberespionaje: Obtener información, no necesariamente por motivos económicos, afectando tanto a gobiernos como a empresas
- Ciberterrorismo: Dirigido principalmente a gobiernos o países, busca infundir miedo en la población o gobierno, especialmente en servicios críticos como salud, defensa o energía.

Estas categorías pueden combinarse en ataques específicos debido a la importancia del mercado de datos en la actualidad.

El perfil del ciberdelincuente

Sistemas de detección y contención de código malicioso

Conceptos básicos y tipos de códigos maliciosos

La comunidad de intrusos está en constante crecimiento, y la elección de objetivos puede variar:

- Se dirigen a objetivos específicos, como individuos u organizaciones particulares.
- Apuntan a un público objetivo definido según intereses específicos, como usuarios de cierto sistema operativo o bases de datos de un tipo de empresa.
- En ocasiones, seleccionan objetivos al azar, sin un criterio previo.

Los códigos maliciosos:

- Definición: Programas diseñados para causar daños o intrusiones en un sistema informático.
- Objetivos: Destruir datos, robar información, propagarse a otros equipos, comprometer sistemas operativos o mostrar publicidad invasiva.
- Evolución: Cada vez más sofisticados, con pequeñas modificaciones que los hacen difíciles de detectar.

Características comunes códigos maliciosos:

- Componentes de software: Diseñados para un fin específico.
- Interferencia: Afectan el funcionamiento normal del sistema atacado.
- Instalación y ejecución: Sin el consentimiento del usuario.
- Propagación: Requieren un equipo anfitrión para instalarse y propagarse.

Sistemas de detección y contención de código malicioso

Conceptos básicos y tipos de códigos maliciosos

Clasificación códigos maliciosos:

Según la forma:

- Virus: Se adjuntan a otros archivos y se ejecutan al abrirlos.
- Troyanos: Se disfrazan de software legítimo para engañar al usuario.

Según el origen:

- Wildfire: Se originan en Internet y se propagan automáticamente.
- Targeted: Diseñados para atacar un equipo o sistema específico.

Según los daños provocados:

- Malware benigno: Causa molestias leves, como publicidad no deseada.
- Malware peligroso: Causa daños graves, como la pérdida de datos o el robo de información.

Según la finalidad:

- Espionaje: Roba información personal o financiera.
- Sabotage: Destruye datos o sistemas informáticos.
- Ciberterrorismo: Busca causar daños a gran escala.

Sistemas de detección y contención de código malicioso

Conceptos básicos y tipos de códigos maliciosos

Tipos de Malware

Virus

Los virus informáticos son programas diseñados con la intención de causar daño en los equipos, operando de manera sigilosa sin que el usuario se percate de su presencia. Estos maliciosos agentes requieren un anfitrión o huésped para alojarse, que puede variar desde archivos ejecutables hasta discos de arranque o unidades de memoria.

Los efectos que pueden provocar son diversos: desde mensajes molestos en la pantalla hasta la eliminación de archivos o la deshabilitación del sistema operativo. Cuando un virus se ejecuta, dos acciones se desencadenan:

- Daño al dispositivo: El virus afecta negativamente el funcionamiento del equipo.
- Propagación: El virus se replica e infecta otros dispositivos o archivos.

Aunque la propagación más común ocurre a través de internet, no es la única vía. Los virus pueden infiltrarse mediante cualquier medio de almacenamiento, como discos duros, pendrives o redes locales mediante carpetas compartidas. Además, existen diversas clasificaciones basadas en criterios como el origen, el modo de infección y los daños causados.

En resumen, los virus informáticos son una amenaza multifacética que requiere vigilancia constante y medidas preventivas para proteger nuestros sistemas.

Sistemas de detección y contención de código malicioso

Conceptos básicos y tipos de códigos maliciosos

Tipos de Malware

Troyanos

Los troyanos son un tipo de malware que se oculta tras la apariencia de herramientas útiles. Su presencia en programas "pirateados" es común, ya que los creadores de "parches" o "cracks" a menudo introducen código malicioso junto con las modificaciones para eludir restricciones de pago.

A diferencia de los virus, los troyanos no se replican automáticamente. Sin embargo, su peligrosidad radica en su versatilidad: pueden llevar a cabo múltiples funciones sin que el usuario lo note. Aunque algunos se especializan en robar información bancaria, aquí están algunas de las funciones comunes de este tipo de malware:

- Compartir archivos: Los troyanos pueden transferir archivos sin que el usuario lo sepa.
- Apagar o reiniciar el sistema: Pueden tomar control del equipo.
- Recuperar contraseñas almacenadas en caché: Acceden a datos sensibles.
- Capturar pantallas: Monitorean la actividad del dispositivo.
- Redirigir puertos y aplicaciones: Manipulan la comunicación.
- Ejecutar aplicaciones no autorizadas: Sin consentimiento del usuario.
- Mostrar mensajes e imágenes en pantalla: A menudo, de forma encubierta, sin que el usuario sea consciente de ello. Manipulando la interfaz visual del sistema.

Sistemas de detección y contención de código malicioso

Conceptos básicos y tipos de códigos maliciosos

Tipos de Malware

Spyware

El spyware es una aplicación diseñada para monitorear el comportamiento de los usuarios con el objetivo de obtener información que luego se vende a terceros, generalmente empresas de publicidad o marketing. Aunque existen diversas variantes de spyware, su funcionamiento sigue un proceso común:

- Infiltración en el sistema del usuario: El spyware se introduce en el dispositivo.
- Recolección de datos locales: Se extrae información del sistema del usuario víctima.
- Monitorización silenciosa: El spyware observa la actividad del sistema.
- Registro de actividades: Se documenta lo que hace el usuario.
- Acciones de marketing y publicidad: Las empresas utilizan la información recopilada.

Aunque los procedimientos son similares, hay diferencias clave entre los tipos de spyware:

- Adware: Muestra ventanas emergentes de publicidad en las interfaces de usuario.
- Scumware: Personaliza la publicidad en el navegador del usuario.
- Browser Hijackers: Modifica características del explorador al manipular el registro del sistema operativo.
- Server Side Spyware: Se implementa en servidores controlados por atacantes en lugar de instalarse en el equipo del usuario víctima

Sistemas de detección y contención de código malicioso

Conceptos básicos y tipos de códigos maliciosos

Tipos de Malware

Keyloggers

Los keyloggers son aplicaciones diseñadas para registrar el comportamiento de un usuario en una computadora de forma remota. Estos programas almacenan todo lo que se escribe en el teclado, enviando la información al atacante o guardándola en el disco duro para su posterior recuperación.

Su objetivo es pasar desapercibidos para el usuario. El funcionamiento básico de un keylogger implica:

- Configuración: Se ajustan los aspectos del keylogger según la información que se pretende obtener.
- Instalación: El keylogger se introduce en el equipo de la víctima.
- Recuperación de datos: El atacante accede a la información capturada por el keylogger.

En la actualidad, muchos virus, gusanos y troyanos incorporan keyloggers en su código para obtener datos de las víctimas, además de sus funcionalidades específicas.

Sistemas de detección y contención de código malicioso

Conceptos básicos y tipos de códigos maliciosos

Tipos de Malware

Worms o gusanos

Los gusanos o worms son programas autocontenidos diseñados para propagarse de un sistema a otro, afectando el rendimiento de los recursos. A diferencia de otros malware, su objetivo principal es la autorreplicación, sin causar daño directo. Sin embargo, pueden combinarse con otros códigos maliciosos.

Autocontenidos se refiere a que los gusanos o worms son programas independientes y autónomos. A diferencia de otros tipos de malware, no requieren un archivo o programa huésped para propagarse. En lugar de adjuntarse a otro código, los gusanos pueden moverse y replicarse por sí mismos en sistemas informáticos sin necesidad de depender de un anfitrión específico.

Sus principales métodos de infección incluyen archivos adjuntos en correos electrónicos, vulnerabilidades en servicios de red y redes P2P. Estos sigilosos invasores requieren vigilancia constante para proteger nuestros sistemas.

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

El panorama actual de la seguridad informática exige la implementación de estrategias robustas para combatir las diversas amenazas del código malicioso. Los sistemas de detección y contención son herramientas esenciales para proteger equipos, redes y dispositivos. **Siendo los sistemas más comunes los IDS/IPS, Antivirus y Firewalls.**

IDS/IPS:

- Función: Detectar e informar sobre intrusiones en equipos, redes o dispositivos. Algunos IPS también pueden prevenir intrusiones.
- Eficiencia: Alta, con una configuración adecuada.
- Requisitos: Alto nivel de experiencia y conocimiento del sistema.
- Consideraciones:
  - Equilibrio entre detección de falsos positivos y falsos negativos.
  - Protección reactiva (IDS) vs. proactiva (IPS).

- Integración con otras herramientas:
  - Correlación de eventos para una mejor identificación de amenazas.
  - Respuesta automatizada a incidentes.

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

Antivirus:

- Función: Detectar y eliminar virus y otros tipos de código malicioso.
- Método de detección: Comparación de archivos con una base de datos de patrones.
- Tareas adicionales:
  - Revisar el sistema en busca de malware.
  - Poner en cuarentena o eliminar archivos sospechosos.
  - Analizar la conducta de procesos del sistema.
  - Bloquear conexiones sospechosas o avisar al usuario.
- Ubicación:
  - Equipos (habitual).
  - Servidores o redes (análisis remoto).
- Tipos:
  - Antivirus tradicionales: Detectan virus conocidos.
  - Antivirus de nueva generación: Utilizan técnicas como el aprendizaje automático para detectar malware desconocido.
  - Antivirus en la nube: Ofrecen análisis y protección en tiempo real.
- Integración con otras herramientas:
  - Protección contra ransomware y otras amenazas emergentes.
  - Gestión centralizada de la seguridad.

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

Firewall o Cortafuegos:

- Función: Controlar las comunicaciones en un equipo o red, permitiendo o denegando el acceso según las políticas de seguridad.
- Eficiencia: Barrera eficaz contra el acceso de código malicioso.
- Limitaciones: Requiere medidas de protección adicionales (antivirus, IDS/IPS).
- Tipos:
  - Firewalls de filtrado de paquetes: Analizan la información de cada paquete de red.
  - Firewalls de aplicaciones: Permiten o deniegan el acceso a aplicaciones específicas.
  - Firewalls de nueva generación: Ofrecen funciones avanzadas como la inspección de estado profundo de paquetes (DPI).

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

EDR (Endpoint Detection and Response)

- es una tecnología de ciberseguridad diseñada para detectar, investigar y responder a amenazas en dispositivos finales, como computadoras de escritorio, portátiles, servidores y dispositivos móviles. Estos sistemas se centran en la protección de los endpoints al monitorear continuamente la actividad en los dispositivos y responder automáticamente o de manera guiada ante comportamientos sospechosos o maliciosos.

- Funcionamiento de un EDR:
  - Recopilación de datos: El EDR recopila datos sobre la actividad del endpoint, como eventos del sistema, registros de aplicaciones, tráfico de red, procesos en ejecución y cambios en archivos.
  - Análisis de comportamiento: Utiliza análisis avanzados y algoritmos de machine learning para detectar patrones y comportamientos anómalos que podrían indicar la presencia de amenazas.
  - Detección de amenazas: El EDR identifica posibles amenazas, como malware, exploits, ransomware o actividades maliciosas de usuarios, basándose en los indicadores de compromiso (IOCs) y los indicadores de comportamiento (IOBs).
  - Respuesta y contención: Una vez que se detecta una amenaza, el EDR puede tomar medidas para contener y remediar la amenaza, como aislar el dispositivo, detener procesos maliciosos, eliminar archivos sospechosos o alertar al equipo de seguridad.

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

EDR (Endpoint Detection and Response)

Ejemplos de herramientas EDR:

- Para Windows:
  - Microsoft Defender for Endpoint:
    - Descripción: Anteriormente conocido como Microsoft Defender ATP, es una solución de EDR avanzada que ofrece protección contra amenazas en endpoints con capacidades de detección y respuesta avanzadas. Licencia: Propietaria
  - Osquery:
  - Descripción: Osquery es una herramienta de código abierto que permite consultar y monitorear el estado de los endpoints en tiempo real, lo que facilita la detección de amenazas y la respuesta a incidentes. Licencia: Código abierto (BSD)
- Para Linux:
  - OSSEC:
    - Descripción: OSSEC es una plataforma de detección de intrusos de código abierto que también proporciona capacidades de EDR. Monitorea logs, archivos y la actividad del sistema para detectar y responder a amenazas en sistemas Linux. Licencia: Código abierto (GNU GPL)
  - Wazuh:
    - Descripción: Wazuh es una bifurcación de OSSEC que ofrece una solución de detección y respuesta de seguridad ampliada para entornos de nube y contenedores, con capacidades mejoradas de análisis y respuesta. Licencia: Código abierto (GNU GPL)

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

XDR (eXtended Detection and Response)

- es una solución de ciberseguridad avanzada que amplía la detección y la respuesta más allá de los endpoints (EDR) para abarcar múltiples fuentes de datos de seguridad, como redes, nubes, correos electrónicos y aplicaciones. El objetivo principal de un XDR es proporcionar una visión unificada y contextualizada de las amenazas en toda la infraestructura de una organización, permitiendo una detección más precisa y una respuesta más eficiente a las amenazas cibernéticas.

- Funcionamiento de un XDR:
  - Recopilación de datos: Un XDR recopila datos de múltiples fuentes, como endpoints, servidores, dispositivos de red, registros de aplicaciones, tráfico de red, servicios en la nube y correos electrónicos.
  - Correlación de datos: Utiliza técnicas avanzadas de correlación y análisis de datos para relacionar eventos y alertas de seguridad de diferentes fuentes y contextos, identificando posibles indicadores de compromiso (IOCs) y patrones de ataque.
  - Detección de amenazas: El XDR utiliza inteligencia de amenazas y análisis avanzados para identificar y priorizar las amenazas en función de su gravedad y riesgo para la organización.
  - Respuesta y contención: Una vez que se detecta una amenaza, el XDR puede tomar medidas automáticas o guiadas para contener y remediar la amenaza en toda la infraestructura de la organización, incluyendo endpoints, redes, nubes y otros activos.

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

XDR (eXtended Detection and Response)
Ejemplos de herramientas XDR:

- Para Windows:
  - Palo Alto Networks Cortex XDR:
    - Descripción: Cortex XDR es una plataforma de ciberseguridad que integra la detección y respuesta avanzada de amenazas en endpoints, redes y nubes, proporcionando una visión unificada de la postura de seguridad de la organización. Licencia: Propietaria
  - CrowdStrike Falcon XDR:
    - Descripción: Falcon XDR de CrowdStrike ofrece detección y respuesta extendida a través de endpoints, workloads en la nube y entornos de contenedores, utilizando inteligencia artificial y análisis de comportamiento para identificar y contener amenazas. Licencia: Propietaria

- Para Linux:
  - Falco:
    - Descripción: Falco es una herramienta de detección de amenazas de código abierto diseñada para entornos de contenedores y sistemas Linux. Utiliza reglas de seguridad y detección de comportamientos anómalos para identificar amenazas en tiempo real. Licencia: Código abierto (Apache 2.0)
  - Zeek (anteriormente conocido como Bro):
    - Descripción: Zeek es una plataforma de análisis de red de código abierto que puede ser utilizada como parte de una solución XDR para monitorear y detectar amenazas en el tráfico de red en sistemas Linux. Licencia: Código abierto (BSD)

Sistemas de detección y contención de código malicioso

EDR vs XDR

Característica	EDR	XDR
Alcance	Se centra en la detección y respuesta de amenazas **específicamente en los endpoints**, como computadoras de escritorio, portátiles, servidores y dispositivos móviles.	Amplía su alcance más allá de los endpoints para abarcar múltiples fuentes de datos de seguridad, como redes, nubes, correos electrónicos y aplicaciones.
Enfoque	**proteger los endpoints** al monitorear continuamente la actividad en los dispositivos y responder a comportamientos sospechosos o maliciosos detectados en ellos.	integra y correlaciona datos de **múltiples puntos de control de seguridad**, proporcionando así una visión unificada y contextualizada de las amenazas en toda la infraestructura de una organización.
Capacidad de detección	capacidades avanzadas de detección y respuesta de amenazas en los endpoints, incluyendo la recopilación de datos, el análisis de comportamiento, la detección de amenazas y la respuesta automatizada.	Aumenta las capacidades de un EDR al integrar datos de múltiples fuentes y contextos, lo que permite una detección más precisa, una visibilidad más completa y una respuesta más eficiente a las amenazas cibernéticas en toda la organización.
Visibilidad y contexto	Proporciona visibilidad detallada y contexto sobre las amenazas específicas detectadas en los endpoints, lo que permite una respuesta rápida y precisa a incidentes en esos dispositivos.	Ofrece una visión unificada y contextualizada de las amenazas en toda la infraestructura de una organización, lo que permite identificar y correlacionar eventos de seguridad en múltiples puntos de control para una detección y respuesta más eficientes.
Nivel de integración	Su integración se centra principalmente en los endpoints, recopilando datos y eventos de seguridad específicamente de estos dispositivos.	integración más amplia al recopilar, integrar y correlacionar datos de múltiples puntos de control de seguridad, como endpoints, redes, nubes, correos electrónicos y aplicaciones, lo que proporciona una visión más completa y contextualizada de las amenazas en toda la organización.
Enfoque de respuesta	se limita a los endpoints, tomando medidas para contener y remediar amenazas específicamente en estos dispositivos.	espuesta integral al ofrecer capacidades de respuesta en toda la infraestructura, lo que permite una contención y remediación más amplias y eficientes de las amenazas en toda la organización.

Sistemas de detección y contención de código malicioso

SIEM (Security Information and Event Management)

- es una solución de ciberseguridad que recopila, correlaciona y analiza datos de seguridad de múltiples fuentes en tiempo real para proporcionar visibilidad y detección de amenazas en una organización. Un SIEM es esencialmente una plataforma centralizada que permite a las organizaciones monitorear y responder a eventos de seguridad en toda su infraestructura de TI.

- Funcionamiento de un SIEM:
  - Un SIEM recopila datos de seguridad de múltiples fuentes, como registros de eventos de sistemas, registros de aplicaciones, registros de red, registros de seguridad de dispositivos, registros de identidad y acceso, y otros datos relevantes.
  - Los datos recopilados son normalizados y correlacionados para identificar patrones y relaciones entre eventos aparentemente no relacionados, lo que permite detectar indicadores de amenazas y comportamientos maliciosos.
  - Los datos normalizados y correlacionados son analizados en tiempo real utilizando reglas predefinidas, algoritmos de machine learning y técnicas de análisis de comportamiento para detectar amenazas, anomalías y actividades maliciosas.
  - El SIEM genera alertas y notificaciones cuando se detectan eventos de seguridad sospechosos o maliciosos, permitiendo a los analistas de seguridad investigar y responder a las amenazas de manera oportuna.
  - El SIEM proporciona herramientas para la gestión de incidentes, incluyendo la asignación de prioridades, el seguimiento del progreso de la respuesta, la documentación de acciones tomadas y la generación de informes de incidentes.

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

SIEM (Security Information and Event Management)
Ejemplos de herramientas SIEM:

- Para Windows:
  - Graylog:
    - Descripción: Graylog es una plataforma de gestión de registros y SIEM de código abierto que permite recopilar, almacenar, analizar y visualizar datos de registros de manera centralizada. Licencia: Código abierto (GNU GPL)
  - ELK Stack (Elastic Stack):
    - Descripción: ELK Stack, ahora conocido como Elastic Stack, es una solución integrada que incluye Elasticsearch, Logstash y Kibana para la recopilación, almacenamiento, análisis y visualización de datos de registros y eventos. Licencia: Código abierto (varias, incluyendo Apache 2.0)
- Para Linux:
  - Splunk:
    - Descripción: es una plataforma de análisis de datos de seguridad y SIEM que recopila, correlaciona y analiza datos de logs y eventos de seguridad para proporcionar visibilidad y detección de amenazas. Licencia: Propietaria (existe una versión gratuita con limitaciones)
  - Security Onion:
    - Descripción: es una distribución de Linux basada en Ubuntu que incluye una variedad de herramientas de seguridad, incluyendo un SIEM basado en Elasticsearch, Logstash y Kibana (ELK Stack), así como otras herramientas de detección de amenazas. Licencia: Código abierto (varias, incluyendo GNU GPL)

Sistemas de detección y contención de código malicioso

XDR vs SIEM

Característica	XDR	SIEM
Alcance	Amplio, abarca múltiples puntos de control de seguridad, incluyendo endpoints, redes, nubes, correos electrónicos y aplicaciones.	Se enfoca en la gestión de eventos y la correlación de datos de seguridad de múltiples fuentes.
Enfoque	Holístico, proporciona una visión unificada y contextualizada de las amenazas en toda la infraestructura de la organización.	Centrado en la gestión de eventos y la correlación de datos para detectar y responder a amenazas.
Capacidad de integración	Integra datos de múltiples fuentes y contextos para proporcionar una visión completa de las amenazas.	Se integra principalmente con fuentes de datos de seguridad para la gestión de eventos y la correlación de datos.
Detección y respuesta	Ofrece capacidades avanzadas de detección y respuesta de amenazas en múltiples puntos de control de seguridad.	Proporciona capacidades de detección y respuesta de amenazas mediante la correlación de eventos de seguridad en tiempo real.

Sistemas de detección y contención de código malicioso

DLP (Data Loss Prevention)

- es un sistema de seguridad diseñado para prevenir la pérdida o fuga de datos confidenciales o sensibles de una organización. Su objetivo principal es proteger la información confidencial de la empresa, como datos financieros, información de clientes, propiedad intelectual y otros datos sensibles, evitando su divulgación no autorizada o sustracción..

- Funcionamiento de un DLP:
  - Identificación de datos sensibles: El DLP identifica y clasifica los datos sensibles de la organización, como información financiera, datos personales, propiedad intelectual, entre otros.
  - Monitoreo de la actividad de los datos: Supervisa y rastrea la actividad de los datos sensibles en toda la red y en los dispositivos finales, incluyendo su creación, acceso, modificación, transferencia y eliminación.
  - Aplicación de políticas de seguridad: Aplica políticas de seguridad para controlar y restringir el movimiento de los datos sensibles, evitando su transferencia no autorizada o su acceso por parte de usuarios no autorizados.
  - Prevención de fugas de datos: Detecta y previene la fuga de datos mediante la aplicación de controles de seguridad, como cifrado, bloqueo de dispositivos, control de acceso basado en roles, entre otros.
  - Generación de alertas y notificaciones: Genera alertas y notificaciones cuando se detectan actividades sospechosas o violaciones de políticas de seguridad, permitiendo una respuesta inmediata por parte del equipo de seguridad.

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

DLP (Data Loss Prevention)
Ejemplos de herramientas DLP:

- Para Windows:
  - OpenDLP:
    - Descripción: es una herramienta de DLP de código abierto diseñada para identificar y proteger datos confidenciales en sistemas Windows. Permite escanear sistemas de archivos en busca de datos sensibles y aplicar políticas de seguridad para prevenir la fuga de datos. Licencia: Código abierto (GNU GPL)
- Para Linux:
  - MyDLP:
    - Descripción: MyDLP es una solución de DLP de código abierto que ofrece capacidades de descubrimiento, monitoreo y prevención de fugas de datos en sistemas Linux. Proporciona escaneo de archivos, monitoreo de tráfico de red y control de dispositivos para proteger datos sensibles. Código abierto (GNU GPL)

Sistemas de detección y contención de código malicioso

Seguridad de contenedores

- es un conjunto de prácticas y herramientas diseñadas para proteger los entornos de contenedores y las aplicaciones que se ejecutan en ellos contra amenazas cibernéticas y vulnerabilidades de seguridad. Los contenedores son unidades de software que encapsulan aplicaciones y sus dependencias, permitiendo su ejecución de manera aislada y portátil.

- Funcionamiento de la seguridad de contenedores:
  - Escaneo de imágenes: Antes de desplegar un contenedor, las imágenes de los contenedores se escanean en busca de vulnerabilidades conocidas y configuraciones inseguras.
  - Aislamiento y segmentación: Se utilizan técnicas de aislamiento, como namespaces y cgroups en Linux, para asegurar que los contenedores estén separados unos de otros y del sistema host.
  - Gestión de acceso: Se aplican políticas de control de acceso para limitar los privilegios de los contenedores y minimizar el riesgo de explotación de vulnerabilidades.
  - Monitorización continua: Se monitorean y registran las actividades de los contenedores en tiempo real para detectar comportamientos sospechosos o maliciosos.
  - Análisis de comportamiento: Se utilizan técnicas de análisis de comportamiento para identificar actividades anómalas dentro de los contenedores, como intentos de acceso no autorizados o modificaciones inesperadas en archivos del sistema.
  - Prevención de fugas de datos: Se implementan medidas para prevenir la fuga de datos sensibles desde los contenedores, como el cifrado de datos en reposo y en tránsito.

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

Seguridad de contenedores
Ejemplos de herramientas:

- Para Windows:
  - Docker Bench for Security:
    - Descripción: es una herramienta de código abierto que proporciona una guía de seguridad automatizada para evaluar la configuración segura de los entornos Docker en sistemas Windows. Licencia: Código abierto (MIT License)

- Para Linux:
  - Falco:
    - Descripción: Falco es una herramienta de detección de amenazas de código abierto diseñada específicamente para entornos de contenedores en sistemas Linux. Utiliza reglas de seguridad y detección de comportamientos anómalos para identificar amenazas en tiempo real. Licencia: Código abierto (Apache 2.0 License)

  - Clair:
    - Descripción: Clair es una herramienta de análisis de vulnerabilidades de código abierto para imágenes de contenedores. Escanea imágenes de contenedores en busca de vulnerabilidades conocidas y proporciona informes detallados sobre los riesgos de seguridad. Licencia: Código abierto (Apache 2.0 License)

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

Análisis de Comportamiento de Usuario (UBA, por sus siglas en inglés User Behavior Analysis)

- es un sistema de detección y contención de código malicioso que se centra en el comportamiento de los usuarios dentro de un sistema informático. En lugar de simplemente buscar patrones de actividad maliciosa predefinidos, el UBA monitorea y analiza el comportamiento normal de los usuarios y las entidades en un entorno informático para detectar desviaciones significativas que puedan indicar actividades sospechosas o maliciosas.
- Funciona mediante la recopilación de datos de actividad de usuarios y entidades, como registros de eventos, registros de acceso, transacciones, entre otros. Luego, utiliza algoritmos avanzados de análisis de comportamiento y machine learning para identificar patrones anómalos que podrían indicar actividades maliciosas, como intentos de acceso no autorizado, movimientos laterales, o exfiltración de datos.
- Herramientas de detección y contención de código malicioso que utilizan el UBA:
  - Windows:
    - Sysmon: Una utilidad de línea de comandos de Microsoft que proporciona información detallada sobre la actividad del sistema, incluidos procesos, cambios en el registro y más. No es específicamente UBA, pero puede utilizarse en combinación con otras herramientas para análisis de comportamiento.
    - Microsoft Advanced Threat Analytics (ATA): Una plataforma de seguridad de Microsoft que utiliza el análisis de comportamiento para detectar amenazas avanzadas en entornos de Active Directory.
  - Linux:
    - OSSEC: Un sistema de detección de intrusos de código abierto que ofrece análisis de comportamiento del sistema para detectar y responder a amenazas.
    - Wazuh: Una plataforma de seguridad de código abierto basada en OSSEC que proporciona detección de amenazas, gestión de registros y análisis de seguridad.

Sistemas de detección y contención de código malicioso

Honeypot

- es un sistema de detección y contención de código malicioso que simula ser un recurso o servicio legítimo pero que en realidad está diseñado para atraer y atrapar a posibles atacantes y malware. Funciona engañando a los atacantes haciéndoles creer que están comprometiendo un sistema real, cuando en realidad están interactuando con un entorno controlado y monitorizado.
- El funcionamiento básico de un Honeypot implica desplegar un servidor, servicio o aplicación que aparenta ser una entidad legítima pero que en realidad está configurada para registrar y analizar todas las actividades sospechosas. Cuando un atacante interactúa con el Honeypot, sus acciones se registran y pueden ser analizadas para identificar técnicas de ataque, patrones de comportamiento y otros indicadores de compromiso.
- Herramientas de Honeypot para Windows y Linux (preferiblemente de código abierto):
  - Windows:
    - Honeyd: Una herramienta de Honeypot de código abierto que permite emular sistemas y servicios en entornos Windows.
    - Glastopf: Un Honeypot de aplicaciones web de código abierto diseñado para simular vulnerabilidades en aplicaciones web y atraer ataques dirigidos a ellas.
  - Linux:
    - Dionaea: Un Honeypot de código abierto diseñado para capturar y registrar malware que se propaga a través de vulnerabilidades en servicios de red como SMB, FTP, HTTP, etc.
    - Cowrie: Un Honeypot de SSH de código abierto que simula un servidor SSH vulnerable para atraer y registrar intentos de acceso no autorizado.

Sistemas de detección y contención de código malicioso

Seguridad de la Red Profunda (Deep Packet Inspection - DPI)

- es una técnica avanzada de análisis de tráfico de red que examina el contenido completo de los paquetes de datos que viajan a través de una red. A diferencia de la inspección superficial de encabezados de paquetes, la DPI analiza el contenido de los paquetes en busca de patrones y firmas asociadas con amenazas de seguridad, como malware, intrusiones o actividades maliciosas.
- Funciona mediante la inspección exhaustiva de cada paquete de datos que atraviesa la red, extrayendo información detallada sobre protocolos, datos de aplicación y metadatos asociados. Luego, aplica reglas y políticas de seguridad para identificar posibles amenazas y tomar medidas adecuadas para contener o mitigar el riesgo.
- Herramientas de DPI para Windows y Linux (preferiblemente de código abierto):
  - Windows:
    - Snort y Suricata: herramientas de detección de intrusos de código abierto que utilizan DPI para inspeccionar y detectar amenazas en el tráfico de red.
  - Linux:
    - Bro (ahora conocido como Zeek): Un poderoso sistema de análisis de tráfico de red de código abierto que utiliza DPI para examinar los paquetes de datos en busca de comportamientos anómalos y maliciosos.

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

Protección Avanzada contra Amenazas (Advanced Threat Protection - ATP)

- es un enfoque integral para la detección y contención de amenazas informáticas sofisticadas y avanzadas. ATP utiliza una combinación de tecnologías y técnicas de seguridad avanzadas para identificar y responder a amenazas que evaden las soluciones de seguridad tradicionales.
- Funciona mediante el análisis continuo del tráfico de red, el comportamiento del usuario y la actividad del sistema en busca de indicadores de compromiso y comportamientos anómalos que podrían indicar la presencia de amenazas avanzadas, como malware sigiloso, ataques de día cero y técnicas de evasión de detección.
- Herramientas de Protección Avanzada contra Amenazas para Windows y Linux (preferiblemente de código abierto):
  - Windows:
    - Windows Defender Advanced Threat Protection (ATP): integrada en Windows 10 que utiliza aprendizaje automático y análisis avanzado para detectar y responder a amenazas avanzadas en tiempo real.
    - OpenDXL: Un marco de código abierto de Intel Security (anteriormente McAfee) que permite la integración y orquestación de soluciones de seguridad para compartir información y responder a amenazas de manera coordinada.
  - Linux:
    - Elastic Security (anteriormente conocido como Elastic SIEM): Una plataforma de seguridad de código abierto que incluye capacidades avanzadas de detección de amenazas y análisis de comportamiento para proteger entornos Linux y otros sistemas operativos.
    - MISP (Malware Information Sharing Platform & Threat Sharing): Una plataforma de inteligencia de amenazas de código abierto

Sistemas de detección y contención de código malicioso

Sistemas de detección y contención de código malicioso

Deception Technology

- es una estrategia de ciberseguridad que consiste en desplegar señuelos o señales falsas dentro de una red o sistema informático para detectar y engañar a posibles atacantes. Estos señuelos, también conocidos como "canales de señuelo" o "cebos", simulan ser recursos o activos genuinos, como servidores, archivos, credenciales de usuario, entre otros. La idea es atraer a los atacantes hacia estos señuelos y, al mismo tiempo, alertar al equipo de seguridad sobre la actividad maliciosa.
- Funciona creando una capa adicional de defensa en profundidad, donde los atacantes pueden ser desviados hacia áreas de la red que están especialmente monitorizadas y controladas. Cuando un atacante interactúa con un señuelo, se activan alertas y se recopila información valiosa sobre las tácticas, técnicas y procedimientos utilizados por los adversarios.
- Herramientas de Deception Technology para Windows y Linux (preferiblemente de código abierto):
  - Windows:
    - KFSensor: Una herramienta de Honeypot para Windows que permite simular servidores y servicios vulnerables para detectar y contener amenazas.
    - Canarytokens: Una solución de detección de intrusos que crea señuelos para rastrear la actividad de los atacantes en entornos Windows y otros sistemas operativos.
  - Linux:
    - Honeyd: Un Honeypot de código abierto que simula sistemas y servicios en entornos Linux para atraer y atrapar a posibles atacantes.
    - Conpot: Un Honeypot de SCADA/ICS de código abierto diseñado para simular sistemas de control industrial y atraer a los adversarios que buscan atacar infraestructuras críticas.

Sistemas de detección y contención de código malicioso

Honeypot vs Deception Technology

Característica	Honeypot	Deception Technology
Objetivo	atraer y atrapar a posibles atacantes. Actúa como una trampa para detectar y contener ataques, permitiendo a los equipos de seguridad estudiar las tácticas y herramientas utilizadas por los adversarios.	busca engañar a los atacantes al crear señuelos o señales falsas dentro de la red o sistema informático. Su objetivo es detectar actividades maliciosas desviando a los atacantes hacia áreas controladas y monitorizadas, proporcionando inteligencia valiosa sobre las tácticas utilizadas.
Función	simulan ser recursos o servicios reales, como servidores, aplicaciones o datos, con el propósito de atraer a los atacantes y registrar su actividad.	crea señuelos o señales falsas, también conocidos como "canales de señuelo" o "cebos", dentro de la red o sistema informático para engañar a los atacantes y detectarlos. Estos señuelos pueden incluir archivos, credenciales de usuario, servicios de red, entre otros.
Finalidad	detectar y contener ataques, proporcionando a los equipos de seguridad información valiosa sobre las tácticas y herramientas utilizadas por los adversarios.	desviar y detectar actividades maliciosas dentro de la red, permitiendo a los equipos de seguridad identificar y responder rápidamente a las amenazas. Además, proporciona inteligencia sobre las tácticas utilizadas por los atacantes.
Naturaleza de la técnica	técnica de seguridad pasiva, ya que esperan a que los atacantes interactúen con ellos para detectar y registrar su actividad.	técnica de seguridad activa, ya que crea señuelos o señales falsas dentro de la red o sistema informático para engañar a los atacantes y detectarlos.
Interacción	requieren que los atacantes interactúen con ellos para que puedan detectar y registrar su actividad. Esta interacción puede incluir intentos de acceso, escaneos de puertos o cualquier otra actividad maliciosa.	puede atraer y detectar actividades maliciosas sin necesidad de una interacción directa con los atacantes. Los señuelos o señales falsas creados pueden engañar a los atacantes y generar alertas cuando son activados.
Alertas	Las alertas en los Honeypots se activan cuando los atacantes interactúan con ellos, lo que permite a los equipos de seguridad detectar y responder rápidamente a los ataques.	se activan cuando los atacantes interactúan con los señuelos o señales falsas creados, proporcionando a los equipos de seguridad información sobre actividades maliciosas dentro de la red o sistema informático.
Enfoque	centrado en la detección y respuesta a ataques, proporcionando a los equipos de seguridad información valiosa sobre las tácticas y herramientas utilizadas por los adversarios.	centrado en engañar a los atacantes y detectar sus actividades maliciosas dentro de la red o sistema informático, permitiendo a los equipos de seguridad identificar y responder rápidamente a las amenazas.

Sistemas de detección y contención de código malicioso

Seguridad Zero Trust

- es un enfoque de ciberseguridad que se basa en la premisa de que ninguna entidad, ya sea dentro o fuera de la red, debe ser confiable por defecto. En lugar de confiar en la ubicación de los usuarios o dispositivos (dentro o fuera de la red corporativa), Zero Trust Security se centra en verificar la identidad y autorización de cada usuario y dispositivo antes de conceder acceso a recursos y datos.
- Funciona implementando controles de seguridad en varias capas y en todo el perímetro de la red, lo que incluye la autenticación multifactor, el cifrado de datos, la segmentación de red, la monitorización continua del tráfico y la aplicación de políticas de acceso basadas en el contexto del usuario y el dispositivo.
- Herramientas de Zero Trust Security para Windows y Linux (preferiblemente de código abierto):
  - Windows:
    - Microsoft Azure Active Directory (AAD): Ofrece una variedad de herramientas de autenticación multifactor y controles de acceso basados en políticas para proteger el acceso a recursos en la nube y locales.
    - BeyondCorp: Una arquitectura de seguridad de Google que implementa Zero Trust Security mediante la aplicación de políticas de acceso basadas en la identidad y el contexto del usuario.
  - Linux:
    - FreeIPA: Una solución de gestión de identidad y acceso de código abierto que proporciona autenticación centralizada, autorización y control de acceso basado en políticas para entornos Linux.
    - Open Policy Agent (OPA): Una herramienta de código abierto que permite definir y aplicar políticas de acceso basadas en reglas y criterios específicos para sistemas Linux y otros entornos.

Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

Introducción

Para gestionar eficazmente las amenazas de código malicioso en un entorno, es crucial seleccionar las herramientas adecuadas según la topología de la red y las vías de infección que se necesitan controlar. Aunque la mayoría de usuarios han experimentado alguna vez infecciones de malware, existen diversas herramientas especializadas en detectar, contener y eliminar estas amenazas de forma automatizada.

En este sentido, se debe considerar una amplia gama de herramientas, desde los antivirus más convencionales hasta soluciones más específicas. En esta discusión, se abordarán brevemente los antivirus de manera general, seguidos por dos herramientas más específicas:

- Antivirus: Se encargan de identificar y neutralizar amenazas de malware comunes.
- VirusTotal: Proporciona análisis exhaustivos de archivos y URLs mediante múltiples motores antivirus.
- FileInsight: Ofrece capacidades avanzadas de análisis de archivos para identificar y mitigar amenazas específicas.

Al elegir las herramientas de control de código malicioso, es crucial tener en cuenta la arquitectura de la red y las posibles vías de infección, garantizando así una protección efectiva contra las amenazas informáticas.

Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

Antivirus

Los antivirus son herramientas diseñadas para detectar, prevenir y eliminar software malicioso (malware) de los sistemas informáticos. Sus objetivos principales son proteger los dispositivos y redes contra una variedad de amenazas, incluyendo virus, gusanos, troyanos, spyware, ransomware y otros tipos de malware. Funcionan mediante el análisis de archivos, programas y actividades del sistema en busca de patrones y comportamientos asociados con amenazas conocidas y desconocidas.

El funcionamiento de los antivirus implica varios pasos:

- Escaneo: El antivirus realiza un escaneo completo o rápido del sistema en busca de archivos y programas sospechosos. Esto puede incluir escaneos en tiempo real mientras se accede a archivos y aplicaciones, así como escaneos programados en momentos específicos.
- Detección: Durante el escaneo, el antivirus compara los archivos y programas con una base de datos de firmas de malware conocidas. Si encuentra una coincidencia, marca el archivo como malicioso y toma las medidas necesarias para contener o eliminar la amenaza.
- Heurística: Además de las firmas conocidas, los antivirus utilizan técnicas heurísticas para identificar comportamientos sospechosos que podrían indicar la presencia de malware. Esto incluye analizar el comportamiento del sistema, la actividad de red y otros indicadores de compromiso.
- Acción: Una vez que se detecta un malware, el antivirus puede tomar diferentes acciones, como eliminar, poner en cuarentena o desinfectar el archivo infectado. También puede alertar al usuario sobre la amenaza y proporcionar recomendaciones para su mitigación.

Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

Antivirus

Herramientas de antivirus para Windows y Linux:

Windows:

- Windows Defender: Es el antivirus integrado en el sistema operativo Windows 10 y ofrece protección en tiempo real contra una variedad de amenazas.
- Avast Free Antivirus: Una solución popular y gratuita que ofrece protección en tiempo real, escaneos programados y características adicionales como cortafuegos y protección de red.

Linux:

- ClamAV: Un antivirus de código abierto diseñado específicamente para sistemas Linux que ofrece escaneo de archivos y correo electrónico, así como actualizaciones regulares de definiciones de virus.
- Sophos Antivirus for Linux: Una solución de seguridad empresarial que ofrece protección contra malware, ransomware y amenazas avanzadas en entornos Linux.

Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

VirusTotal

Es una plataforma en línea que proporciona servicios de análisis de archivos y URLs para detectar malware y otras amenazas cibernéticas. Su principal objetivo es ofrecer un análisis exhaustivo y multidimensional de archivos sospechosos mediante el uso de múltiples motores antivirus y tecnologías de análisis de comportamiento.

Funcionamiento de VirusTotal:

- Análisis de archivos: Los usuarios pueden cargar archivos sospechosos en VirusTotal para su análisis. La plataforma realiza un escaneo de los archivos utilizando una amplia variedad de motores antivirus de diferentes proveedores, incluidos nombres conocidos como Avast, Kaspersky, McAfee, entre otros.

- Análisis de URLs: VirusTotal también permite analizar URLs sospechosas para detectar sitios web maliciosos o phishing. Al ingresar la URL en la plataforma, se lleva a cabo un análisis para identificar posibles amenazas y proporcionar información sobre la seguridad del sitio.

- Informes detallados: Después del análisis, VirusTotal genera un informe detallado que muestra los resultados de cada motor antivirus utilizado, así como información adicional como el hash del archivo, las características del archivo y los comentarios de la comunidad de usuarios.

Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

VirusTotal

Después de realizar un análisis en VirusTotal, la plataforma proporciona una variedad de información detallada sobre el archivo o la URL analizada. Esta información incluye:

- Resultados de escaneo: Muestra la detección de malware por parte de diferentes motores antivirus utilizados en el análisis. Cada motor antivirus proporciona su propio veredicto sobre la seguridad del archivo o la URL.

- Detalles del archivo: Incluye el nombre del archivo, su tamaño, tipo de archivo y fecha de análisis. También puede mostrar el hash MD5, SHA-1 y SHA-256 del archivo.

- Información del análisis: Proporciona detalles sobre el tipo de análisis realizado, como análisis de archivos o análisis de URLs, y la fecha y hora en que se realizó el análisis.

- Información adicional: Puede mostrar otros datos relevantes, como las características del archivo, los comentarios de la comunidad de usuarios, las etiquetas asociadas y los enlaces relacionados.

Es crucial comprender que el uso de VirusTotal y otros sistemas de detección de malware no es perfecto. Si el malware o la URL son nuevos y no han sido previamente identificados como amenazas, la herramienta podría clasificarlos como legítimos. Por esta razón, es esencial que las organizaciones implementen políticas de seguridad y brinden formación en ciberseguridad básica a sus empleados para detectar y prevenir posibles ataques informáticos.

Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

VirusTotal

Herramientas relacionadas con VirusTotal:

- MetaDefender: Una plataforma similar a VirusTotal que ofrece análisis de archivos y URLs utilizando múltiples motores antivirus y tecnologías de análisis avanzado.

- Jotti : Es una opción rápida y fácil de usar que analiza archivos con hasta 15 motores antivirus. La interfaz puede no ser la más moderna, pero es buena para chequeos básicos.

- Hybrid Analysis: Proporciona análisis de malware automatizado y dinámico, incluyendo la ejecución de muestras de malware en un entorno controlado para comprender su comportamiento.

- Any.Run: Una plataforma de análisis de malware que permite ejecutar muestras de malware en un entorno virtualizado y observar su comportamiento en tiempo real.

Estas herramientas son fundamentales en la detección temprana y la respuesta rápida a amenazas cibernéticas, ya que permiten a los usuarios identificar y analizar archivos y URLs sospechosos de manera eficiente y efectiva.

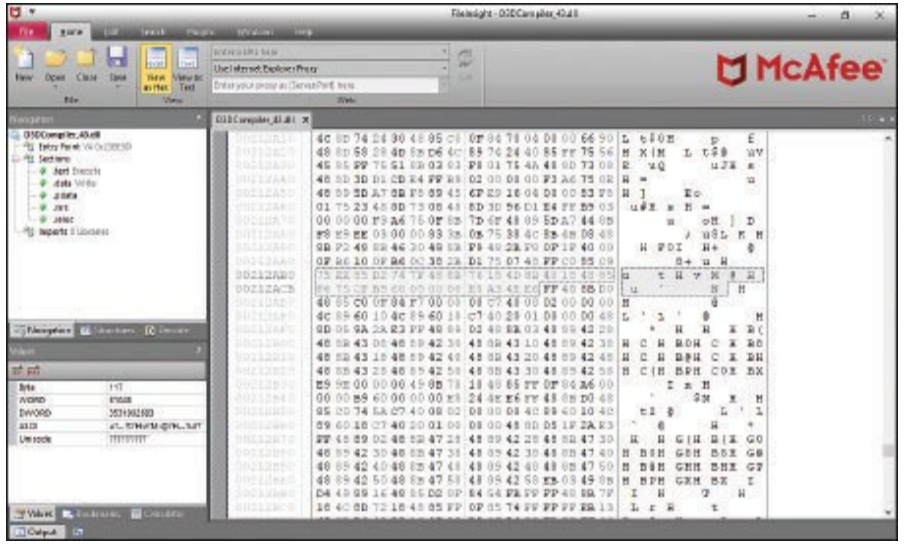
Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

FileInsight

Es una herramienta de análisis de archivos que se utiliza para examinar el contenido y la estructura interna de los archivos en busca de posibles amenazas de seguridad. Esta herramienta tiene su origen en la necesidad de los investigadores de seguridad y analistas forenses de profundizar en el análisis de archivos sospechosos para comprender su comportamiento y detectar cualquier actividad maliciosa.

El objetivo principal de FileInsight es proporcionar una visión detallada de los archivos para identificar posibles amenazas, incluidos virus, troyanos, ransomware y otros tipos de malware. Además, se utiliza para analizar la estructura de archivos desconocidos o sospechosos para comprender su funcionamiento interno y determinar si representan un riesgo para la seguridad.

El uso de FileInsight implica cargar un archivo en la herramienta y realizar un análisis exhaustivo del mismo. La herramienta muestra información detallada sobre la estructura del archivo, incluidos metadatos, recursos incrustados, secciones ejecutables y otros elementos relevantes. Esto permite a los usuarios identificar cualquier comportamiento sospechoso o actividad maliciosa dentro del archivo.



Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar

FileInsight

Alternativas actuales a FileInsight incluyen:

- PEStudio: Una herramienta de análisis de archivos que se especializa en la exploración de archivos ejecutables de Windows para identificar posibles amenazas y comportamientos maliciosos.

- Cuckoo Sandbox: Una plataforma de análisis de malware que utiliza máquinas virtuales para ejecutar y observar el comportamiento de archivos sospechosos en un entorno seguro y controlado.

- REMnux: Una distribución de Linux diseñada para análisis forense y análisis de malware, que incluye una variedad de herramientas para examinar archivos y detectar amenazas.

Estas alternativas y otras proporcionan funcionalidades similares a FileInsight y se utilizan en la industria de la ciberseguridad para investigar y analizar archivos en busca de posibles amenazas y vulnerabilidades.

Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso

Introducción

Si bien las herramientas de protección frente a código malicioso son efectivas, no son infalibles. Es importante estar atento a los síntomas de una infección y configurar las herramientas de forma segura.

Síntomas de una infección por código malicioso:

- Bajo rendimiento de las aplicaciones.
- Aparición o desaparición de archivos desconocidos en el disco duro.
- Comportamiento inusual de la pantalla.
- Cambios en el tamaño de los archivos.
- Reseteos inesperados del sistema operativo.
- Mensajes de error o fallos al iniciar el sistema.
- Carga de aplicaciones desconocidas al iniciar el sistema.
- Comportamiento erróneo de las aplicaciones.

Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso

Introducción

Criterios de seguridad para la configuración de las herramientas:

- Mantener actualizado el software: sistemas operativos, herramientas, aplicaciones y antivirus.
- Configurar las herramientas de contención de código malicioso según las políticas de la organización.
- Utilizar herramientas de búsqueda y actualización de vulnerabilidades.
- Implementar un sistema de alarmas en la herramienta de contención de código malicioso.
- Utilizar claves y contraseñas seguras.
- Realizar copias de seguridad periódicas del sistema operativo.
- Navegar por páginas web seguras y confiables.
- Utilizar un cortafuegos.
- Comprobar la legitimidad de las URL en los correos electrónicos sospechosos.

Recomendaciones adicionales:

- Utilizar herramientas de análisis online como Virus Total para verificar archivos y URL.
- Formar a los usuarios en seguridad informática.
- Realizar auditorías de seguridad periódicas.

Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso

Detección de ataques de ingeniería social

Los ataques de ingeniería social son una de las principales amenazas a la seguridad informática. Estos ataques, que se basan en la manipulación psicológica para obtener información o acceso a sistemas, son cada vez más sofisticados y difíciles de detectar.

¿Qué es la ingeniería social? La ingeniería social es el arte de manipular a las personas para que revelen información confidencial o realicen acciones que no deberían. Los atacantes utilizan una variedad de técnicas para lograr sus objetivos, como:

- Suplantación de identidad: El atacante se hace pasar por otra persona, como un representante de una empresa o un amigo.
- Engaño: El atacante crea una historia falsa para convencer a la víctima de que revele información o realice una acción.
- Amenaza: El atacante amenaza a la víctima con consecuencias negativas si no coopera.

Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso

Detección de ataques de ingeniería social

¿Cómo detectar un ataque de ingeniería social? Hay una serie de señales que pueden indicar que usted está siendo víctima de un ataque de ingeniería social, como:

- Mensajes o llamadas inesperadas: Si recibe un mensaje o una llamada de alguien que no conoce, tenga cuidado. Los atacantes a menudo se ponen en contacto con sus víctimas de forma inesperada.
- Solicitudes de información personal: Los atacantes nunca deben solicitarle información personal, como su contraseña o número de tarjeta de crédito.
- Enlaces o archivos adjuntos sospechosos: No haga clic en enlaces o abra archivos adjuntos de correos electrónicos o mensajes de personas que no conoce.
- Sentimiento de presión: Si siente que está siendo presionado para tomar una decisión rápida, es probable que se trate de un ataque de ingeniería social.

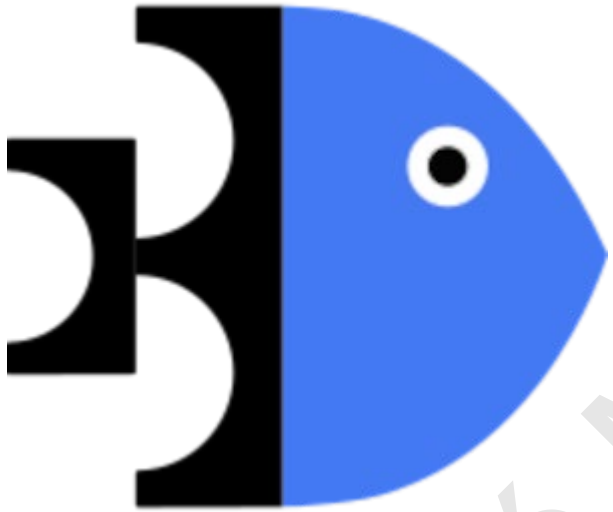
Consejos para protegerse de los ataques de ingeniería social:

- Esté atento: Sea consciente de las señales que pueden indicar un ataque de ingeniería social.
- No revele información personal: Nunca revele información personal a alguien que no conoce.
- Verifique la identidad del remitente: Antes de responder a un mensaje o una llamada, verifique la identidad del remitente.
- No haga clic en enlaces o abra archivos adjuntos sospechosos: Si no está seguro de si un enlace o un archivo adjunto es seguro, no lo abra.
- Utilice una contraseña segura: Utilice una contraseña segura y única para todas sus cuentas en línea.
- Mantenga su software actualizado: Asegúrese de que su software y sistema operativo estén actualizados con los últimos parches de seguridad.

Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso

Detección de ataques de ingeniería social

Herramientas detección



PHISHCHECK

Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso

Requerimientos y técnicas de actualización

La norma ISO 27001 establece que el responsable de seguridad debe:

- Definir controles de detección y prevención contra software malicioso.
- Desarrollar procedimientos de concienciación para usuarios.
- Implementar controles de acceso al sistema y administración de cambios.

Controles de acceso recomendados

- Prohibir la instalación y uso de software no autorizado.
- Redactar procedimientos para la obtención segura de archivos y software.
- Instalar y actualizar software de detección y reparación de virus.
- Mantener los sistemas actualizados con las últimas medidas de seguridad.
- Realizar pruebas de las actualizaciones en un entorno de prueba.
- Revisar periódicamente el contenido del software y los datos de los equipos críticos.
- Verificar la presencia de virus en archivos de origen incierto.
- Redactar procedimientos para verificar la información sobre software malicioso.
- Concienciar al personal sobre falsos antivirus y cadenas falsas.
- Redactar normas para la protección y habilitación de puertos de conexión de dispositivos móviles.

Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso

Requerimientos y técnicas de actualización

Actualización de herramientas de control y contención de código malicioso

Siguiendo las recomendaciones de la ISO 27001, se establecen los siguientes requerimientos y técnicas de actualización:

- Protección antivirus continua 24/7.
- Herramientas de actualización automática.
- Herramientas de actualización sin interrupciones en el trabajo.
- Aparición rápida y continua de actualizaciones.
- Generación periódica de informes y estadísticas.
- Protección para todo tipo de servidores (Linux, Windows, etc.).
- Métodos de escaneo y análisis de posibles códigos maliciosos.
- Comprobación y seguridad remota del estado de los equipos y dispositivos.
- Realización de copias de seguridad y discos de arranque periódicos.
- Detección de virus en tiempo real.
- Velocidad de escaneo para una rápida detección y eliminación de cualquier código malicioso.
- Utilización de distintos métodos de escaneo, detección y eliminación de códigos maliciosos.
- Facilidad de manejo y gestión de las herramientas de protección y contención.
- Administración centralizada con recepción de reportes de virus, actualizaciones y personalización de configuraciones.

Importancia de la actualización de las herramientas

Es crucial actualizar las herramientas de protección contra código malicioso, ya que estos se reproducen y varían continuamente. La falta de actualización deja a los equipos desprotegidos ante posibles ataques.

Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso

Herramientas de protección contra código malicioso

Control y protección de las vías de acceso. Las herramientas de protección contra código malicioso deben controlar y proteger las distintas vías de acceso de forma personalizada:

- Sistemas de ficheros: discos duros, pendrives, CD, etc.
- Red local
- Correo electrónico
- Navegadores

Sistemas de ficheros. Las herramientas para proteger los sistemas de ficheros deben:

- Tener antivirus instalados en clientes y servidores.
- Gestionar el escritorio, controlando e inventariando el software instalado.
- Gestionar las vulnerabilidades del sistema, identificándolas y parcheándolas automáticamente.
- Ofrecer protección especial frente a ransomware.

Red local. Las herramientas de detección y contención de códigos maliciosos deben prestar especial atención a la red local para impedir su propagación. Se recomienda:

- Configurar centralmente los cortafuegos de los dispositivos de la red local.
- Establecer políticas centralizadas de seguridad y respuesta ante detección de intrusiones.

Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso

Herramientas de protección contra código malicioso

Correo electrónico. Las herramientas deben contener programas antivirus especializados para controlar y detectar códigos maliciosos en los correos electrónicos. Deben:

- Controlar y verificar la inexistencia de código malicioso en la entrada de correos electrónicos.
- Realizar comprobaciones constantes en los servidores que almacenan buzones de correo electrónico.

Navegadores. Las herramientas de protección deben proteger la actividad de los navegadores instalados en servidores y equipos cliente. Se debe:

- Configurar los navegadores correctamente y de acuerdo a las políticas de seguridad.
- Instalar programas antivirus que realicen análisis periódicos y detecten códigos maliciosos en los distintos navegadores.

Políticas de seguridad. La política de seguridad de las organizaciones debe reflejar y tener en cuenta:

- Las distintas posibles vías de entrada de código malicioso.
- Las herramientas necesarias para su protección.
- Su configuración y políticas de respuesta ante ataques.

Relación de los registros de auditoría de las herramientas de protección frente a códigos maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

Introducción

Importancia de la auditoría. Las herramientas de protección contra código malicioso son cada vez más necesarias, pero no basta con implementarlas. Es crucial encontrar la cantidad adecuada de herramientas para elevar el nivel de seguridad de forma acorde al presupuesto de la organización.

Complejidad de la gestión. Las herramientas de protección crean una infraestructura compleja que dificulta el control manual. Deben gestionarse para que controlen y vigilen la aparición de incidentes de seguridad.

Solución: análisis centralizado de eventos de seguridad. Una solución útil es el análisis centralizado de eventos de seguridad a través de herramientas de auditoría de seguridad informática.

Objetivos de la auditoría de seguridad. La auditoría de seguridad analiza y evalúa la planificación, el control, la eficacia y la seguridad de la estructura informática de una organización. Responde a preguntas como:

- ¿Es adecuada la seguridad de los equipos y dispositivos?
- ¿La información está almacenada en medios fiables?
- ¿Existe la posibilidad de que haya pérdidas de información irreversibles?
- ¿La seguridad de los sistemas permite la consecución de los objetivos de la organización?
- ¿La infraestructura de seguridad es eficiente? ¿Se aprovechan los recursos de un modo adecuado?

Relación de los registros de auditoría de las herramientas de protección frente a códigos maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

Los archivos de registro o archivos de log

Los archivos de registro o logs son una fuente importante de seguridad y de solución de problemas. Contienen información diversa de un sistema, como:

- Tráfico de la red
- Aplicaciones utilizadas
- Usuarios que han accedido a cada aplicación y qué han hecho con ellas
- Automatizar el análisis de estos archivos puede ahorrar a los administradores mucho tiempo, ya que solo se les ofrece la información imprescindible.

En cuanto a la seguridad del sistema, los archivos de registro permiten:

- Descubrir posibles ataques
- Detectar información sobre problemas o incidencias de seguridad
- Generar información sobre las actividades de administradores y usuarios
- Comprobar el grado de cumplimiento de las políticas de seguridad

Relación de los registros de auditoría de las herramientas de protección frente a códigos maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

Los archivos de registro o archivos de log

Los logs, como mínimo, deben registrar información sobre:

- Intentos de acceso al sistema o a alguna aplicación (exitosos y fallidos)
- Identidad del usuario
- Fecha y tiempo de cada intento de entrada y salida
- Dispositivos utilizados en la conexión
- Actividades y funciones ejecutadas por el usuario

Los registros de auditoría son una herramienta vital para la seguridad informática. Permiten:

Controlar el acceso: verificar las acciones de los usuarios y ajustar permisos.
Reconstruir eventos: detectar cómo, cuándo y por qué se generó una incidencia.
Detectar intrusos: analizar los registros en tiempo real o después del incidente.

Los registros están protegidos por ley y deben almacenarse en lugares seguros.

Es importante revisar los registros periódicamente para detectar alarmas y mensajes de advertencia.

Relación de los registros de auditoría de las herramientas de protección frente a códigos maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

Los archivos de registro o archivos de log

Las herramientas de análisis de logs automatizan la revisión y extraen la información relevante. Los análisis pueden ser:

- Periódicos: configurados por el administrador, eficientes en recursos.
- Constantes: lectura continua de los archivos, información inmediata.

Las herramientas de auditoría filtran los eventos importantes y pueden incluso reaccionar automáticamente.

En resumen, los registros de auditoría son una fuente vital de información sobre la seguridad del sistema y las herramientas de análisis ayudan a obtener información útil de estos registros.

Relación de los registros de auditoría de las herramientas de protección frente a códigos maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

Herramientas de auditoría de seguridad y archivos de registro

Nessus Professional. Es una solución líder en la industria para la evaluación avanzada de vulnerabilidades. Aquí hay algunos aspectos destacados:

- Evaluación de Vulnerabilidades Avanzada: Nessus Professional ofrece una evaluación avanzada de vulnerabilidades para identificar posibles brechas de seguridad en sistemas y redes.
- Fácil Implementación y Uso: Se destaca por su facilidad de implementación y uso, lo que lo hace accesible para empresas de todos los tamaños. Esto significa menos tiempo y esfuerzo dedicados a la gestión de vulnerabilidades.
- Detección Avanzada para Más Protección: Su capacidad de detección avanzada garantiza una cobertura exhaustiva, lo que se traduce en una mejor protección contra posibles amenazas cibernéticas.
- Costo Efectivo: A pesar de su avanzada funcionalidad, Nessus Professional sigue siendo una opción rentable para empresas de diferentes presupuestos.

- Vídeo

Relación de los registros de auditoría de las herramientas de protección frente a códigos maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

Herramientas de auditoría de seguridad y archivos de registro

Wireshark. Es una poderosa herramienta de análisis de protocolos de red de código abierto. Permite capturar y examinar los datos en una red en tiempo real y también analizar archivos de captura previamente guardados. Algunas de sus características incluyen:

Captura de Tráfico de Red: Wireshark puede capturar y mostrar datos en tiempo real de una red, permitiendo a los usuarios inspeccionar el tráfico para identificar problemas de rendimiento o seguridad.

Análisis Profundo: Ofrece capacidades para analizar diversos protocolos de red a un nivel muy detallado, lo que ayuda a diagnosticar problemas y entender el comportamiento de la red.

Interfaz Gráfica Intuitiva: Su interfaz gráfica de usuario es fácil de usar y permite filtrar y buscar paquetes de datos según diversos criterios.

Soporte Multiplataforma: Wireshark está disponible para varios sistemas operativos, incluyendo Windows, macOS y Linux, lo que lo hace accesible para una amplia gama de usuarios.

Personalización y Extensibilidad: Los usuarios pueden personalizar y ampliar Wireshark mediante el uso de complementos y scripts, lo que lo hace altamente adaptable a diferentes necesidades de análisis de red.

Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso

Herramientas de auditoría de seguridad y archivos de registro

El proceso de monitorización y pruebas de las herramientas de protección contra código malicioso se establece mediante un procedimiento definido ante la detección de amenazas. Este proceso consta de varios pasos:

Contención de Daños:

- Identificación y extracción de muestras de software malicioso.
- Monitorización de comunicaciones y cambios ocasionados por el código malicioso.
- Pruebas para comparar comportamientos en entornos controlados antes y después de la ejecución del malware, evaluando actividad de red, procesos del sistema, cambios en la estructura de archivos y registros de eventos.
- Verificación de la confiabilidad, integridad y validez de la información proporcionada por las herramientas de protección.
- Evaluación de la efectividad de las herramientas de protección en entornos controlados.

Evaluación de Daños:

- Análisis del impacto económico y operativo de la pérdida de datos, la productividad afectada y la propagación del malware.

Reparación y Revisión:

- Implementación de medidas para revertir las alteraciones causadas por el malware utilizando herramientas de análisis forense.

Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso

Herramientas de auditoría de seguridad y archivos de registro

Este proceso puede ser monitorizado mediante herramientas de protección, que incluyen:

- Registro centralizado de actividades de herramientas en clientes.
- Inventario de software instalado en equipos.
- Sistemas de detección de intrusiones.
- Gestión de registros de correo y uso de protocolos.
- Centralización de registros del sistema.
- Gestión de acciones en caso de detección de intrusiones.
- Actualizaciones periódicas de bases de datos de malware y herramientas de protección.

La monitorización varía según las herramientas utilizadas, como antivirus, IDS/IPS y cortafuegos instalados en la red.

Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

El análisis dinámico de malware, que busca monitorear su comportamiento para tomar medidas de respuesta, puede alertar a los intrusos de la presencia del usuario. Una alternativa es simular situaciones, haciendo creer al malware que se comunica con servidores maliciosos cuando en realidad interactúa con un entorno controlado, evitando la conexión directa.

Herramientas para Simulación de Entornos Controlados:

Fakenet-NG: Ejecutable desde la línea de comandos de Windows, ofrece información sobre sitios web visitados por el malware, aunque carece de interfaz gráfica.

Cuckoo Sandbox: Compleja pero útil para análisis detallados. Proporciona datos sobre el tráfico de red, acciones del malware y uso de memoria, aunque consume más recursos.

Desensambladores:

IDA Pro: Reconocido como uno de los mejores desensambladores, compatible con varias plataformas aunque su versión completa tiene un precio elevado. Ofrece una versión de prueba limitada.

Radare2: Alternativa gratuita para sistemas Linux, similar a IDA Pro. Proporciona información detallada sobre el comportamiento del malware, incluyendo rutinas de archivos, registros y procedimientos.

Resumen

La creciente vulnerabilidad de los dispositivos electrónicos se debe al aumento de los intentos y ataques diarios, impulsados por la rápida propagación de las nuevas tecnologías de comunicación.

Los ataques de malware son comunes y requieren herramientas como IDS/IPS, antivirus y cortafuegos, así como soluciones avanzadas como SIEM.

La selección de estas herramientas depende de la infraestructura de red y las vías de infección, incluyendo opciones de detección online que no consumen recursos.

La implementación de medidas de seguridad debe basarse en las recomendaciones de normativas como ISO 27001, que abordan la concienciación de usuarios y la actualización de herramientas de control de malware.

Gestionar un gran número de herramientas puede resultar complicado, por lo que existen aplicaciones especializadas que ofrecen estadísticas para evaluar su eficacia y la evolución de las amenazas.

Además, herramientas como los entornos de ejecución controlada y los desensambladores son útiles para combatir el malware.