Automatiza tu ciberseguridad para responder incidentes

(SIEM+SOAR)

#ConstruimosUnFuturoMejor

TEUNO

Automatización y *seguridad cibernética*

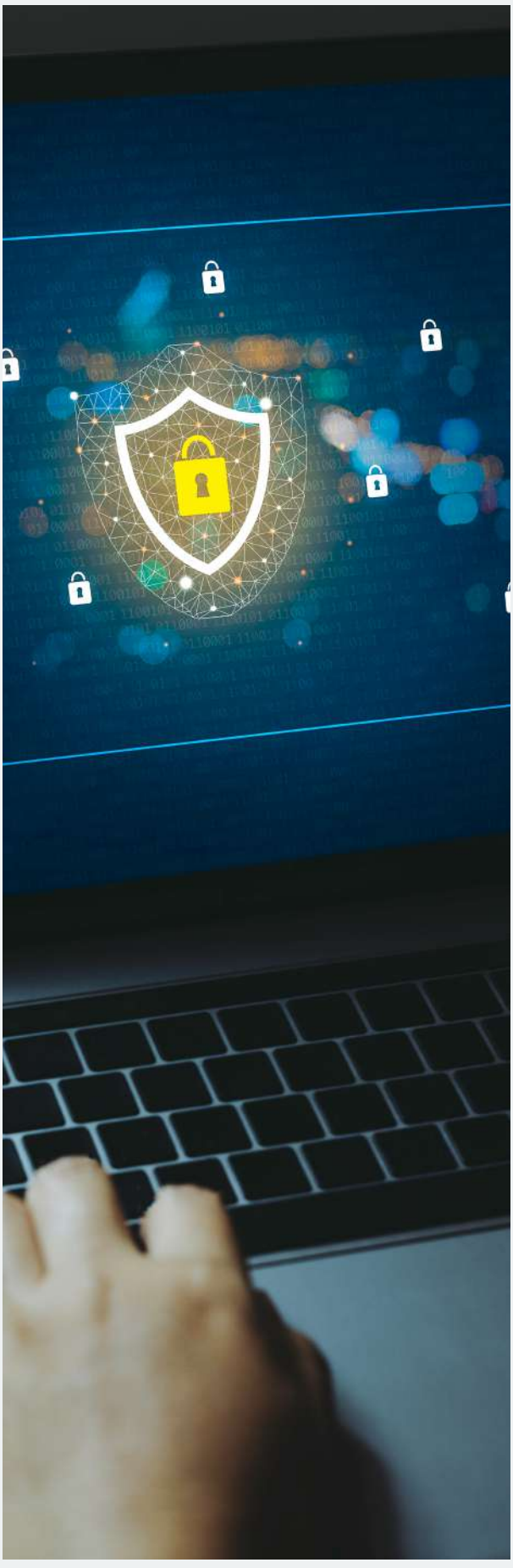
La automatización de la ciberseguridad resulta exitosa dependiendo de las tareas a realizar y la adecuada selección de herramientas relacionadas. Una vez elegidas las tareas a automatizar, es importante identificar las herramientas adecuadas para ello. A**sí, para detectar vulnerabilidades hay diversas soluciones, es posible adquirir suscripciones a proveedores de seguridad que analizan diariamente todas las alertas de seguridad.** Estos, además, incorporan con regularidad a sus conjuntos de reglas de detección todo lo necesario para estar siempre al día.

La combinación de una herramienta de monitorización con reglas de seguridad informática actualizadas permanentemente es un sistema muy eficiente para identificar posibles problemas antes de que se produzcan. Por supuesto, es tarea de los administradores de sistemas mantenerse atentos a todas las alertas que se puedan producir para poner en marcha las soluciones pertinentes.

Otra herramienta que permite automatizar la ciberseguridad es un firewall o cortafuegos. La mayoría de ellos permite poner en marcha reglas que bloqueen de forma automática intentos de intrusión o ataques de denegación de servicio, DOS (Denial Of Service). Una correcta configuración puede hacer que tu red corporativa reaccione en tiempo real a los intentos de ataque y evite que el problema vaya a más.

Una capa que, posiblemente, ya esté en uso y que sigue siendo fundamental en ciberseguridad, es la instalación de software antimalware. Tanto en los equipos manejados por usuarios como en servidores, mantener al día software especializado puede evitar todo un género de problemas. Varias amenazas peligrosas se pueden evitar antes de que causen daños.

Un caso evidente de la importancia de este tipo de herramientas es el ransomware, que habitualmente se aprovecha de la impericia de los usuarios menos tecnológicos. Una vía común de entrada de este tipo de software malicioso es el correo electrónico. Evitar en el propio PC del receptor que el malware se ejecute, impedirá que se propague por la red.



Soluciones de software: configuración de reglas

Después de conectar los orígenes de datos a Microsoft Sentinel, cree reglas de análisis personalizadas que le ayuden a detectar las amenazas y los comportamientos anómalos de su entorno. Las reglas de análisis buscan eventos o conjuntos de eventos específicos en el entorno, estas avisan cuando se alcanzan determinados umbrales de eventos o condiciones, generan incidentes para que el SOC evalúe e investigue, y responden a las amenazas con procesos de seguimiento y corrección automatizados.

Cuando crees reglas personalizadas, usa las reglas existentes como plantillas o referencias. El uso de reglas existentes como base de referencia ayuda al crear la mayor parte de la lógica antes de realizar los cambios necesarios.

- Creación de reglas de análisis.
- Definición de la forma en que se procesan los eventos y las alertas.
- Definición de la forma en que se generan las alertas y los incidentes.
- Elección de respuestas a amenazas automatizadas para las reglas.

Tecnología e integración con *herramientas de seguridad*

Por lo general, cada implementación en la empresa cuenta con un firewall como la primera línea de defensa, se protegen así los activos contra las amenazas comunes de la red. **En la mayoría de los escenarios de implementación de firewall, este actúa como un portero, limitando el acceso únicamente a los servicios de internet que la organización considere necesarios.** En un nivel básico, el acceso es controlado por reglas que enumeran el activo y por el servicio que tiene permitido el acceso desde una ubicación específica. Estas reglas se determinan basándose en la función del activo.

Las empresas han seguido un diseño de arquitectura separada con los servidores de acceso a internet separados de los activos corporativos de la empresa en un particular segmento de red aislado. Este segmento se conoce tradicionalmente como una "zona desmilitarizada" (DMZ). El aislamiento se consigue dedicando una interfaz de red del firewall para estos servidores.

El acceso directo a activos externos no alojados en la DMZ no está permitido. Estos activos incluyen típicamente estaciones de trabajo de la empresa, componentes críticos del servidor, tales como controladores de dominio, servidores de correo electrónico y aplicaciones empresariales. Los activos alojados en el segmento DMZ normalmente incluyen aplicaciones con acceso a internet, tales como interfaces de web, servidores y relés de correo electrónico, y servicios públicos de alojamiento de archivos, entre otros. El acceso entre los activos en la zona desmilitarizada y los segmentos corporativos está estrictamente controlado.

Compara esta arquitectura a la del entorno alojado de una empresa y te darás cuenta de muchas similitudes en el enfoque del control de acceso. Un ejemplo de un entorno alojado podría ser con la plataforma de comercio electrónico, una empresa alojada por un tercero. Tales despliegues suelen tener un segmento de DMZ donde se alojan los servidores de web en una arquitectura de tres niveles que incluye servidores de web, de aplicaciones y de bases de datos.

Beneficios de la automatización

La automatización de la ciberseguridad ayuda a los equipos de seguridad a responder más rápido inclusive con un personal reducido. También garantiza la coherencia, la previsibilidad y buena ejecución de las operaciones de seguridad. Últimamente, ayuda disminuir la cantidad y el tiempo necesario para detectar y gestionar cualquier intrusión no autorizada.

Mejor uso del talento humano

Esta herramienta también es capaz de ayudar a los analistas de seguridad a ser más proactivos e innovadores. Permite reducir la cantidad de tiempo que utilizan descartando falsos positivos, y les deja concentrarse en amenazas más complejas.

Optimización del desempeño de otras herramientas

Esta solución también hace posible que la información de seguridad proporcionada por las herramientas SIEM y los sistemas avanzados de detección de amenazas sean capaces de activar una intervención automática. Así se puede aplicar una amplia gama de controles basados en políticas de seguridad preestablecidas. Estos controles pueden incluir, por ejemplo, el aislamiento de dispositivos y la corrección de endpoints.

Empresa de tecnología: *ejemplos de casos de uso*

Las industrias de TI a menudo son responsables de las comprobaciones de rutina del sistema y el manejo manual de datos. Este escenario de caso ha presionado la necesidad de la automatización de procesos de TI. Los CIO y otros puestos de liderazgo tecnológico buscan transformar sus operaciones de servicio. De acuerdo con Gartner, para este 2023, las mejoras en las capacidades de corrección de análisis y automatización ayudaron a reenfocar alrededor del 30% de los esfuerzos de operaciones de TI, desde el soporte hasta la ingeniería continua.

El personal de TI necesita crear una cuenta de usuario, otorgar accesos y permisos al incorporar nuevos empleados. Además, deben actualizar y agregar detalles de usuario en la base de datos, como Microsoft, Oracle y otros. La tarea de crear una nueva cuenta de usuario y actualizar los detalles del usuario manualmente requiere mucho tiempo y es engorrosa para el personal de TI, especialmente cuando el volumen de datos es alto. Para agilizar el proceso de creación de cuentas, la automatización es útil. Los bots de automatización pueden obtener automáticamente solicitudes de creación de cuentas, crear nombres de usuario, generar contraseñas y enviar notificaciones por correo electrónico a los usuarios. Al automatizar los contratiempos del proceso de creación de cuentas relacionados con las resoluciones de retrasos, se puede evitar la ejecución manual.

Los profesionales de la mesa de servicio manejan tareas que requieren mucha mano de obra, como el enrutamiento de correo electrónico, el soporte al usuario final, las operaciones de seguridad, los tickets de TI y otros. Además, tienen que completar la documentación necesaria para la clasificación y asignación de boletos. Y una gran cantidad de asignación de tickets de TI conduce a una resolución retrasada y a la falta de respuesta. Este anticuado modelo de operación se puede transformar con la automatización inteligente en su lugar. Con tecnologías de IA como el aprendizaje automático, las organizaciones de TI pueden proporcionar autoservicio a los usuarios con una resolución rápida para el correo electrónico, IVR y tickets basados en chat. Además, la IA recopila información diversa de los usuarios, crea una base de conocimientos para la asignación y resolución automática de tickets.

Con la IA, las organizaciones de TI pueden reducir el TAT (Thematic Apperception Test: *prueba proyectiva que permite conocer mejor emociones y motivaciones) en un 90% y los costos operativos en un 25%.*

Gestión de acceso a datos

La gestión de accesos tiene como objetivo otorgar a los usuarios autorizados el derecho a utilizar un servicio. Cuando los nuevos empleados se unen a la organización, solicitan acceso para compartir unidades / carpetas, bases de datos, VPN remotas y software como HRMS, Salesforce, etc.

El procesamiento manual de la gestión del acceso conduce a la falta de seguridad, la divulgación no premeditada de datos y la falta de evidencia para las actividades de acceso. Sin embargo, la automatización de TI impulsada por IA reduce la probabilidad de error humano, ya que garantiza que la autorización sea precisa. La automatización facilita guardar y registrar la actividad del usuario, revocar el acceso específico del usuario, realizar auditorías de seguridad eficientes y evitar violaciones de seguridad con un conjunto predefinido de reglas.

Notificaciones por correo electrónico

El envío manual de cientos de notificaciones por correo electrónico sobre la resolución de incidentes, las alertas del sistema, el acceso a los datos, el estado de los tickets y otros interrumpen la productividad del agente de la mesa de servicio. Además, la elaboración manual de notificaciones es un proceso repetitivo y que requiere mucho tiempo. Pero la parte buena de la notificación por correo electrónico es que se puede llevar a cabo mediante el uso de reglas predeterminadas aplicadas a datos estructurados.

Administración del espacio en disco del servidor

En una organización de TI, la supervisión y el mantenimiento de servidores con limpieza de disco, aumentar el espacio en disco puede llevar mucho tiempo y ser una actividad repetitiva. Dicha actividad es crucial porque quedarse sin espacio en disco debido a un archivo temporal podría bloquear su sistema. El uso de herramientas de automatización puede alertar sobre el bajo espacio en disco y tomar medidas correctivas para la capacidad de espacio en disco requerida sin ningún problema.

Data Management

En un lugar de trabajo de TI, una gran parte de los procesos de negocio involucra datos e información. Según un informe, tres desafíos clave que afectan la capacidad de ofrecer un excelente servicio al cliente incluyen la mala calidad de los datos, el método de transferencia de datos y la falta de nueva tecnología. La recopilación manual de datos, la integración con el sistema mainframe y el análisis es un proceso iterativo. Pero al aplicar tecnologías de IA como el aprendizaje automático, OCR hace que tareas como la entrada, captura, creación y actualización de datos sean más rápidas y eficientes.

Conclusiones

En un lugar de trabajo de TI, una gran parte de los procesos de negocio involucra datos e información. Según un informe, tres desafíos clave que afectan la capacidad de ofrecer un excelente servicio al cliente incluyen la mala calidad de los datos, el método de transferencia de datos y la falta de nueva tecnología. La recopilación manual de datos, la integración con el sistema mainframe y el análisis es un proceso iterativo. Pero al aplicar tecnologías de IA como el aprendizaje automático, OCR hace que tareas como la entrada, captura, creación y actualización de datos sean más rápidas y eficientes.

TEUNO

www.teuno.com | info@teuno.com

Automatiza tu ciberseguridad
para responder incidentes
(SIEM+SOAR)

#ConstruimosUnFuturoMejor