Chipotles.exe

Desarrollo de Sistema de Gestión de Incidentes de Seguridad. (SGIS)

Problemática para resolver. -

En estos tiempos de auge tecnológico nadie esta excepto de sufrir un ataque cibernético, no todas las empresas sean de cualquier tamaño se preocupan por un buen Sistema de seguridad lo que las podría llevar a perder mucho dinero y exponer la integridad se su base de datos.

La problemática que resolveremos es crear un sistema de seguridad en el cual, en base a una aplicación, en dicha aplicación se hará la recolección de datos de inicio de sesión y se guardaran en una base de datos, cuando se encuentren anomalías como usuarios desconocidos, ya sea por extensiones distintas a las comunes u otras.

Solución.

Crearemos un servidor en una máquina virtual que tendrá instalados y configurados servicios web, en el servidor se recibirán, procesarán y almacenarán registros de los eventos del sistema mediante la herramienta Rsyslog, y se podrá filtrar y enriquecer la información de los registros.

Una vez obtenidos los registros, para la parte de la detección utilizaremos una herramienta SIEM, llamada Splunk, a la cual, con ayuda del filtrado y enriquecimiento de Rsyslog, le enviaremos solamente los registros más relevantes, Splunk analizará e identificará eventos importantes que podrían comprometer la integridad del sistema, por ejemplo, un número inusual de inicio de sesión fallidas.

Splunk, dentro de sus funciones, nos permite configurar alertas cuando se cumplan ciertas condiciones de los eventos identificados, posteriormente podemos configurar la automatización de una acción para enviar nuestra alerta creada a través de un canal de notificación, como puede ser un correo electrónico, esto se puede realizar ya que Splunk tiene integrada una API Restful, la que permite solucionar la etapa de notificación.

A continuación, debemos clasificar el evento según su posible impacto en el sistema, podemos clasificar en alta prioridad para aquellos incidentes que presentan una amenaza grave, media prioridad para aquellos que no son tan críticos y baja prioridad para los que no requieren acción inmediata.

En la parte de la documentación podremos visualizar los incidentes ocurridos en el sistema , así como su tipo de prioridad ,lo cual estos registros nos ayudara más adelante a poder detectar y contrarrestar incidentes no deseados de forma más eficiente debido a su comportamiento y su fuente de naturaleza.

Herramientas que utilizaremos.

Splunk puede proporcionar un análisis más avanzado

Nos ayudaremos de herramientas como Rsyslog,y la utilización de endpoint.