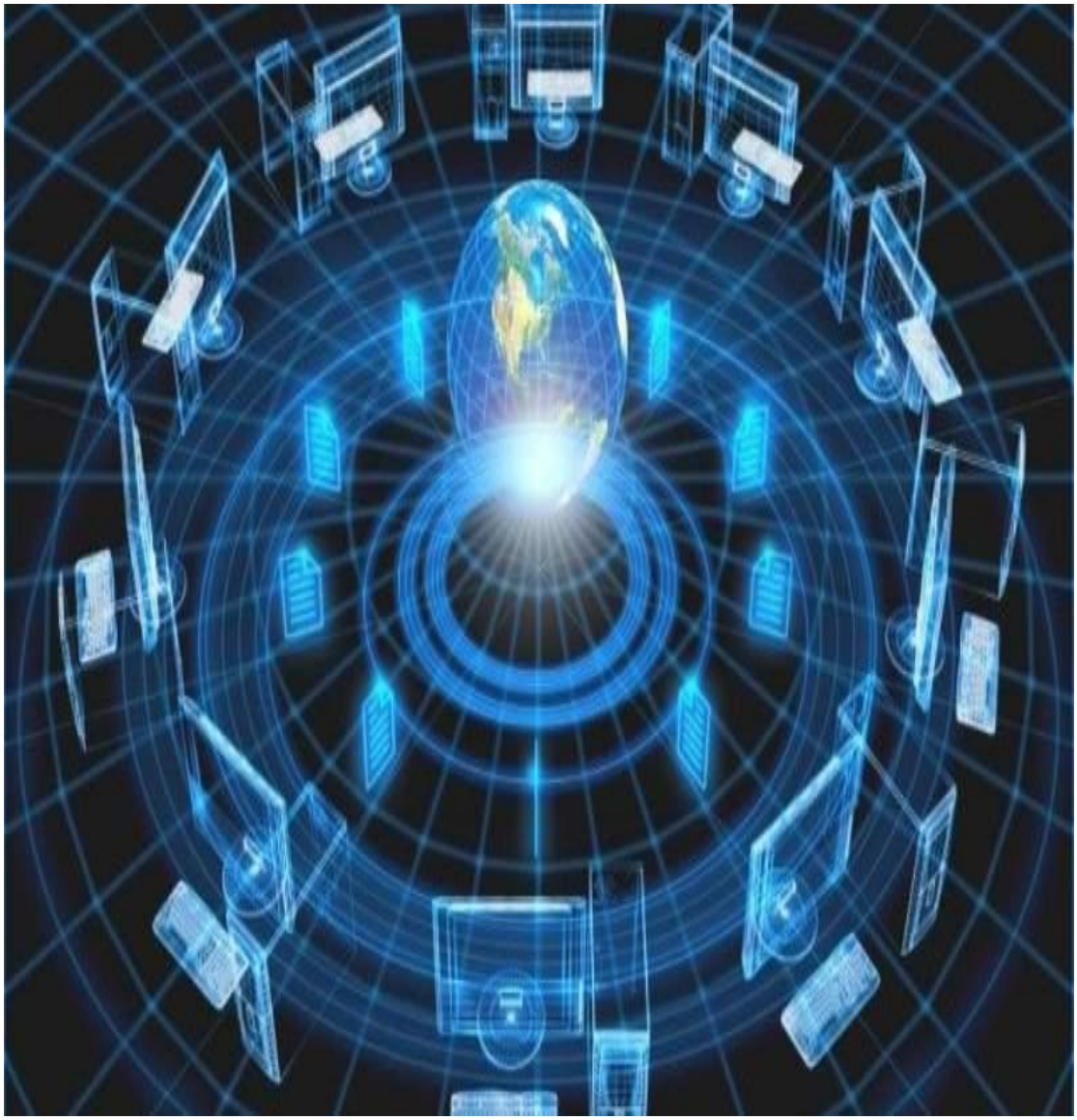

SIEM

IBARRA SABIDO JOSE MARIA | **Fundamentos de Telecomunicaciones** | 03-12-2020

SIEM centraliza los eventos y logs de los diferentes sistemas, permitiendo un análisis en tiempo real de lo que está sucediendo en la gestión de la seguridad, dando mayor visibilidad a los sistemas de seguridad y a los administradores.

Así mismo, SIEM combina funciones de un sistema de Gestión de Información de Seguridad el cual almacena eventos a largo plazo para el análisis y comunicación de los datos de seguridad, y un sistema de Gestión de Eventos de Seguridad, que es el encargado de la revisión en tiempo real, correlación de eventos y notificación.

SIEM es una solución dedicada y capaz de detectar, responder y neutralizar las amenazas informáticas. Su objetivo principal es proporcionar una visión global de la seguridad de las tecnologías de la información.

Una solución SIEM permite tener control absoluto sobre la seguridad informática de la empresa, al tener información y administración total sobre todos los eventos que suceden segundo a segundo, resultando más fácil detectar tendencias y centrarse en patrones fuera de lo común.

No es un secreto que las amenazas de seguridad aumentan continuamente, y que pueden provenir tanto de fuentes internas como externas. Una preocupación que crece es la posibilidad de que, accidentalmente, los empleados configuren erróneamente los ajustes de seguridad, dejando los datos vulnerables a un ataque. Para prevenir estos problemas, las organizaciones de IT han incorporado varios sistemas para protegerse de intrusiones y de una gran cantidad de amenazas diversas.

La desventaja de estos sistemas de protección es que generan tanta información para monitorizar, que los equipos de IT se enfrentan al problema de tener que interpretarla en su totalidad para poder reconocer los problemas reales. De hecho, el volumen de datos de Seguridad que fluyen a los equipos de Seguridad de IT con poco personal, es más que nada inútil, a menos que pueda ser rápidamente analizado y filtrado en alertas procesables. Teniendo en cuenta la cantidad de datos que pueden llegar a ser, para las organizaciones ya no es posible hacer este análisis en forma manual.

Las soluciones SIEM disponibles comparten puntos en común que son importantes para sus operaciones. Usted querrá contar con la capacidad de:

Centralizar la vista de potenciales amenazas

Determinar qué amenazas requieren resolución y cuáles son solamente ruido

Escalar temas a los analistas de Seguridad apropiados, para que puedan tomar una acción rápida

Incluir el contexto de los eventos de Seguridad para permitir resoluciones bien informadas

Documentar, en un registro de auditoría, los eventos detectados y cómo fueron resueltos

Cumplir con las regulaciones de la industria en un formato de reporte sencillo

Un SIEM puede ser utilizado para detectar cualquier número de amenazas de Seguridad, incluso la presencia de ransomware, accesos no autorizados a datos, intentos de log-in fallidos que no coinciden con los problemas estándares de log-in, y picos inusuales en el ancho de banda. Ya sea que estas amenazas provengan de fuentes internas o externas, el software es capaz de enviar una alerta priorizada que notifique a su equipo del problema potencial para que sea investigado de inmediato.

A medida que las amenazas de Seguridad evolucionan, las soluciones SIEM se convierten en un componente crítico para proporcionar a las organizaciones un entorno seguro para sus datos.