INSTITUTO TECNOLÓGICO DE CANCÚN

INGENIERÍA EN

SISTEMAS COMPUTACIONALES

FUNDAMENTOS DE TELECOMUNICACIONES

NOMBRE DEL ALUMNO:

CHAN BURGOS JOSE REYES

HORARIO

LUNES A JUEVES

5:00 PM – 6:00 PM

PROFESOR

ING. ISMAEL JIMENEZ SANCHEZ

SIEM

Es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas. Esto es posible mediante un análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas, que incluyen aplicaciones antivirus, firewalls y soluciones de prevención de intrusiones.

La tecnología SIEM es la combinación de las funciones de dos categorías de productos:

SEM o gestión de eventos de seguridad.

SIM o gestión de información de seguridad.

¿CÓMO LOGRAR LA DETECCIÓN DE AMENAZAS DE SEGURIDAD CON UNA SOLUCIÓN SIEM?

Este tipo de tecnología está enfocada para detectar amenazas externas e internas. A diferencia de un firewall, el SIEM permite detectar y reaccionar en tiempo real. Cabe mencionar que estas soluciones tecnológicas están enfocadas en la prevención de amenazas no relacionadas con vulnerabilidades del software.

¿Cuál es la importancia y finalidad de un sistema SIEM?

La importancia de estas soluciones está en la prevención de amenazas no relacionadas con vulnerabilidades del software, tales como malware, o la denegación del servicio (DoS).

Pero no solo las amenazas externas están controladas con la tecnología SIEM, sino que también nos garantiza que podremos controlar las amenazas cibernéticas más difíciles de detectar: los ataques internos.

La finalidad de las herramientas SIEM es detectar y prevenir amenazas. Están diseñadas para prevenir ataques antes de que se realicen y lo hacen gracias a la información que se recopila en el sistema central.