

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Investigación SIEM

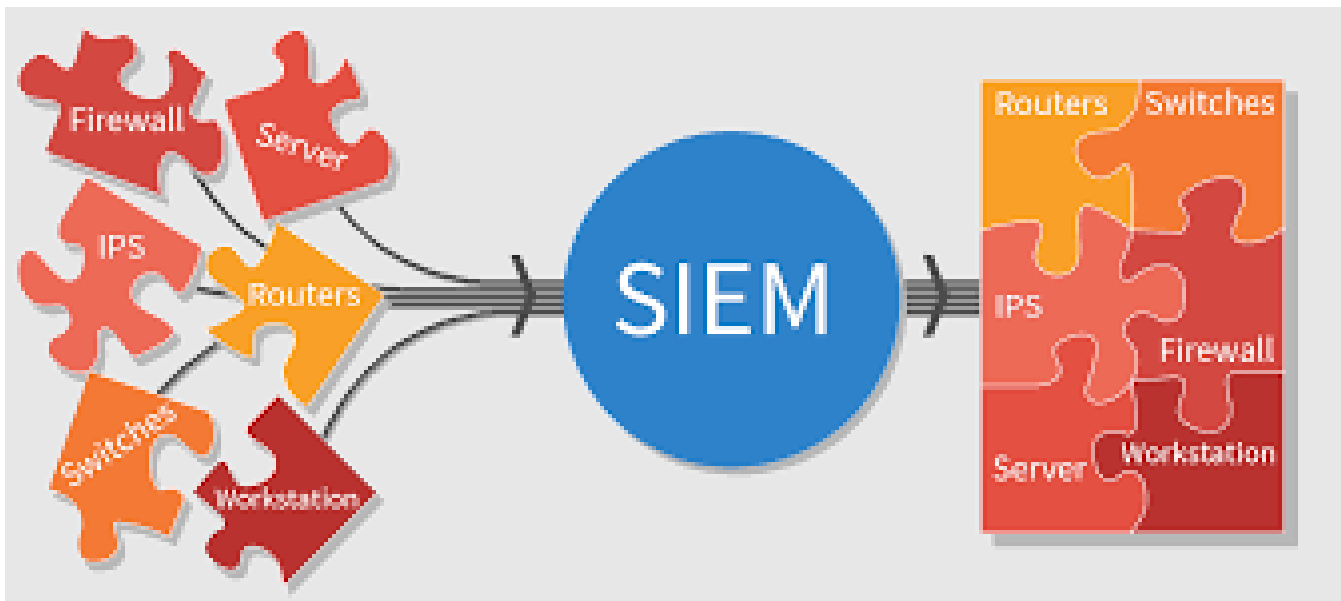
Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

¿Qué es el SIEM?

Normalmente toda empresa que esta conectado internamente a el anterior tiene varios servicios en los cuales pueden presentar riesgos de ciberataques y su potencial gravedad. Para eso sirve la protección SIEM.

La informatica SIEM es un acrónimo que significa Security Information And Event Management Y que traduce como gestión de información y eventos de seguridad



Se trata de un tipo de tipología de software lo cual ofrece información útil a empresas para detectar fallos y amenazas de seguridad usando un sistema de datos para los riesgos informáticos, en simple palabras mejora la seguridad de las organizaciones y compañías.

¿Cómo funcionan?

Los sistemas siem de seguridad mezclan la interpretación de registros y el almacenamiento de datos con la gestión de los mismos y su interpretación para reconocer los patrones en la detección de ataques y hacer frente a las amenazas

Esta tecnología se fundamenta en centralizar la información para visualizar los potenciales riesgos.

El repositorio se llena mediante registros de seguridad proporcionados por eventos recopilados de las fuentes monitorizadas, desde antivirus a firewalls, equipos del personal y sistemas de prevención de intrusiones