Fundamentos de telecomunicaciones

Arturo alexander felipe lopez
Diciembre 2020
Profesor: ING. Ismael Jiménez Sánchez

Instituto tecnológico de Cancún
Ing. En sistemas computacionales
Investigación siem

SIEM

Security Information and Event Management Traducido al castellano sería algo así como Información de Seguridad y Gestión de Eventos. Las soluciones SIEM, a grandes rasgos, tienen como objetivo detectar preventivamente amenazas potenciales a la empresa y resolverlas lo más rápido y de lo forma más eficaz posible. Para ello, procesan y monitorizan una cantidad enorme de datos tanto de hardware, software como fuentes de seguridad, dejando constancia de posibles fallos de seguridad que encuentra a su paso y también de dichas actividades sospechosas. De esta manera la empresa cumple la normativa de seguridad y a la vez consigue la garantía de que su red es segura ya que previene ataques y frena posibles incursiones en su red a la vez que detecta debilidades en la misma.

Cualquier sistema SIEM debe reunir un amplísimo abanico de herramientas de tecnología de la información (TI) para ser lo más completo posible, ya que la seguridad digital de las compañías así lo requieren.

Lo que hace el sistema SEM es centralizar el almacenamiento y la interpretación de registros, de modo que ofrece un análisis en casi tiempo real al equipo de seguridad digital, que de esa forma puede actuar mucho más rápido. Por su parte, el sistema SIM va recopilando datos en una base de datos central para poder trazar tendencias y conseguir patrones de conducta que puedan servir para detectar otros que no son comunes. Este sistema por supuesto también aporta informes centrales. De la unión de ambas salen las siglas que estamos tratando, SIEM, que pueden unir en un solo sistema todas las virtudes de sus dos orígenes.

HERRAMIENTAS SIEM:

En el mercado existen numerosos proveedores que tienen su visión particular del SIEM y por eso tratan de diferenciar sus productos de la competencia. A continuación recopilaremos 5 de las mejores herramientas SIEM.

Micro Focus ArcSight:

Es un sistema SIEM capaz de recoger datos de más de 350 fuentes, procesando hasta 75000 eventos de seguridad por segundo. Micro Focus es una empresa británica en origen si bien se fusionó en 2016 con Hewlett Packard Enterprise.

IBM Security QRadar:

El sistema SIEM de IBM, QRadar, ofrece más de 400 módulos que soportan la carga de datos. Esto se traduce en miles de millones de eventos por día, si bien se pueden priorizar de manera personalizada.

Splunk Enterprise Security:

Splunk cuenta con la integración con User Behavior Analytics (UBA) y las herramientas de Machine Learning de la compañía. Una de sus mayores fortalezas es que la compañía es muy potente a nivel de seguridad, ya que su área de negocio más importante. Splunk Enterprise presume en su web oficial de tener clientes de la talla de Coca Cola.

Suite RSA NetWitness:

Esta herramienta es muy popular entre organizaciones financieras, el sector de las telecomunicaciones y las entidades gubernamentales entre otros. RSA es la división de seguridad de Dell EMC y tienen su sede central en Bedford, en el estado de Massachusetts.

McAfee Enterprise Security Manager:

ESM es muy popular en el sector público, en educación y sanidad, y por eso McAfee ha puesto sus esfuerzos en especializar su herramienta para dichos sectores desarrollando capacidades específicas en este sentido.