SIEM (Security Information and Event Management)

Introduction:

SIEM plays an important role in data security. It is a collection of security tools which results in packaged security solution. Searching through logs, provides data retention and provides automated alerts and reports. SIEM within the computer security field, which include both the software and products to manage the security information.

SIEM provides the comprehensive approach to security, keeps track of the sequence of events that occurs, it alerts the administration about the malicious activity that took place in the organization, such as three failed login attempts by same user on different machines.

SIEM technology is an intersection of two technologies, i.e. Security Event Management (SEM) and Security Information Management (SIM). SEM performs collection, aggregation, and real-time monitoring of events and logs whereas SIM correlates, normalizes, and then performs a later analysis.

How SIEM is useful:

Fig 1: Functions of SIEM