SIEM adalah sistem yang mengumpulkan, menganalisis, dan mengelola log dari berbagai perangkat keamanan dan sistem TI untuk mendeteksi ancaman secara real-time, serta membantu dalam audit dan kepatuhan.

3 komponen utama SIEM :

i. **Log Collection**
   Mengumpulkan log dari server, firewall, antivirus, dll
ii. **Correlation Engine**
   Menganalisis dan menggabungkan log untuk mendeteksi serangan
iii. **Dashboard & Alert**
   Menampilkan data keamanan dan memberikan notifikasi jika terjadi ancaman