Security Information and Event Management System (SIEMS)

Security Information and Event Management System (SIEMS) is an approach to combining the monitoring in event management with security of information into a single view point or station. The SIEMS software or appliance collects log and event data from multiple servers in near real-time. By collecting logs and event using a single location it is better to see patterns or events.

A potential problem with SIEMS is the amount of data that is collected. With the collection of logs from 8 or more servers this can become a very large data storage task.

The complexity of configuration and management is another problem. Configuring the tool to bring the data together and start storing it in a database. The task of searching and identifying the events that will be monitored for begins.

Component Symbol

SIEMS-1