Steps involved in SIEM process:

Fig 2: Overview of SIEM process

SIEM collects data from various devices like servers, network devices etc. Normalize the data collected and often aggregates with the data, analyze the collected data which help to discover the threats and breaches that enable organization to detect the alerts.

SIEM aggregates and analyses the data across different sources across entire IT infrastructure. SIEM provides forensic and reporting for those security issues. Alerts that are discovered are matched with the entire rule set. SIEM provides various security solutions by aggregating the data on various devices.

Some of the SIEM tools are:

- **Solar Winds Security Event Manager**: It is one of the competitive tool having a wide range of log management features. Because of its real time incident response, it makes