- **Asset Discovery** is the ability to detect the threats, visibility of all the devices within the organization.
- **Vulnerability Assessment** is the process of defining, classifying and assigning priority levels to all the threats based on their severity in a given timeframe.
- **Threat Detection** is the ability find all the threats across the organization, and what mitigate actions should be taken in response.
- **Event collection** involves collecting logs from all the remote computers and storing them in event log on collector computer.
- **Correlation** aggregates and analyses the log data across the network, it is possible to detect threats and malicious defects that are sometimes unnoticed can lead to data loss.
- **Event management** is a process of identifying, monitoring and analyzing security events within an IT environment, involves real-time monitoring and customizing notifications.
- **Log storage** involved in collecting log files from various hosts and applications.

Why organization must invest in the SIEM solution..??

SIEM provide functionalities which is useful for the organization. Some of them are as follows:

1. **Meeting Compliance Requirements:**

There are many laws and regulations surrounding data protection. Some of these include; PCI-DSS, HIPAA, SOX, and the forthcoming GDPR. Complying with these regulations requires time, effort and resources. However, with the help of SIEM technology, the task of compliance is made much easier. SIEM technology will aggregate and archive log data, as well as provide alerts and reports to satisfy requirements.

2. **Supporting Operations Processes:**

The growing size, complexity and fragmentation of organizations is making it more difficult for them to share information, collaborate on projects and co-ordinate operations. SIEM solutions are able to aggregate data from multiple sources into a single dashboard, making it a lot easier for large organizations to monitor important system events.