LOG ANALYSIS

Log analysis is the process of reviewing, interpreting and understand computer-generated records called logs. Logs are generated by a range of programmable technologies, including networking devices, operating systems, applications, and more.

Computers, networks, and other IT systems generate records called audit trail records or logs that document system activities. Log analysis is the evaluation of these records and is used by organizations to help mitigate a variety of risks and meet compliance regulations.

Organizations who wish to enhance their capabilities in a cyber security must develop capabilities in log analysis that can help them actively identify and respond to cyber threats. Organizations that effectively monitor their cyber security with log analysis can make their network assets more difficult to attack.

Logs are records of events that happen in your computer, either by a person or by a running process. They help you track what happened and troubleshoot problems. Logs are of 4 types. They are;

1. **Application Log**

An application log is a file of events that are logged by a software application. It contains errors, informational events and warnings. The format and content of an application log are determined by the developer of the software program, rather than the OS.

2. **System Log**

The system log (SYSLOG) is a direct access data set that stores messages and commands. It resides in the primary job entry subsystem's spool space. It can be used by application and system programmers to record communications about programs and system functions.

3. **Security Log**

The Security Log, in Microsoft Windows, is a log that contains records of login/logout activity or other security-related events specified by the system's audit policy. Auditing allows administrators to configure Windows to record operating system activity in the Security Log.

4. Setup Log

Setup creates log files for all actions that occur during installation. If you are experiencing problems installing Windows, consult the log files to troubleshoot the installation. Log location before Setup can access the drive.