Logs are generated by network devices, software applications, operating systems, internet of things devices and many other system hardware. They contain many information that are stored sequentially on disk, files, or applications such as the Log Collector. Log is very important for any system because they tell you what is happening and what your system is doing. Most of the processes running on your system create logs. The problem is that these files often appear in different systems and in different formats, and log data must be built in centralized and meaningful ways so that they are understandable to humans and can be easily deciphered by machine learning systems. Log data collected from different sources can be more easily related to relevant trends and patterns. Analysts should ensure that the log data contains all necessary information and this information is explained by context, for example, one system can use "alerts", the other uses "significant". Analysis are simplified and error free by ensuring that word and data formats are synchronized. Log elements need to be generalized, using similar words Log Analysis Key to Cyber Threat Detection 5 or terminology to avoid confusion and provide harmony, while generalization analyst should ensure that statistics data reports from different sources are accurate and make sense to the reader. Logs should also be accessed from a central location, and log aggregation is a good way to get all these logs in one place. For example, if you have different types of hosts, you can host different types of hosts in different places. Ends with the log. If you have an error and need to point to your log, you should look for dozens or hundreds of files to see what went wrong. Even with good tools, you can spend a lot of time doing this and this can frustrate even the toughest system administrators. As soon as logs are aggregated, cleaned and normalized, anomalies, such as network breaches patterns can be identify through thorough analysis