easy to manage your infrastructure and easiest way to use in the market, because of its 24/7 support this makes a clear choice for SIEM.

- **Manage Engine Event Log Analyzer**: Tool that manages, protects, and mines log files. Installed on windows, windows server and Linux.
- **Micro Focus Arc Sight ESM**: Tool that runs on windows environment and suited for large organizations.
- **Splunk Enterprise Security**: This tool is meant for windows and Linux, It combines both analysis and log management making it excellent tool.
- **Log Rhythm Security Intelligence Platform**: AI based technology that underpins the traffic and log analysis for windows and Linux.
- **Alien Vault Unified Security Management**: SIEM tool that can run on both Mac OS and windows.
- **RSA Net Witness**: Comprehensive tool runs on windows used for large organizations.
- **IBM QRadar** : SIEM that runs on windows which is leading in market.
- **McAfee Enterprise Security Manager**: Popular SIEM tool that runs on Mac OS and windows used mainly to confirm system security.

Conclusion:

SIEM solution is very expensive, the generated reports are difficult to understand, additionally there are many solutions available at realistic price and provide the ability to perform a lot of functions. Lipid Auditor is one among them that provides the reports which are easy to understand and meets the compliance requirements. SIEM requires high level of expertise or person with extensive training or certifications to deal with it. SIEM gets more exciting when one can apply log data and security-event-inspired correlation to other business problems.

SIEM can detect convert, malicious communication and encrypted channels. SIEM helps in analysis of logs, is used in pattern recognition, detection of log failures.