3. **Detecting Zero-day threats:**

Zero-day attacks are usually caused by software vulnerabilities. Firewalls, Intrusion Defense Systems (IDS) and Intrusion Prevention Systems (IPS) can be very useful for monitoring suspicious activity between endpoints within your network's infrastructure. However, such solutions are unlikely to help you detect zero-day attacks. SIEM solutions, however, can be setup to spot patterns and anomalies that may signify an attack.

4. **Advanced persistent threats:**

Administrator will be involved to notice what is really on going, SIEM solutions can solve this problem by aggregating the data from each system into a single dashboard. An SIEM solution will audit the data (in real-time) and alert the administrators of any unauthorized access attempts, as well as other suspicious events.

5. **Identifying the cause of a security breach:**

In event of a security breach, you will need to carry out some sort of forensic investigation. There is need to find when, where and how the breach took place. Such investigations not only serve to help mitigate future attacks, but may also be required by law. Without the help of SIEM technologies, forensic investigations are a slow and painful process. SIEM solutions allow you to quickly gather the information you need, and output the information in the form of a report, which can be used to satisfy the legal requirements.