Security monitoring in cyber security is the process of collecting and analyzing indicators of potential security threats, then triaging these threats with appropriate action. It is also important to keep the CIA triad in mind when monitoring protocols and procedures: confidentiality, integrity and availability. 1. Confidentiality refers to preventing sensitive information from unauthorized access attempts; it ensures that data is kept secret or private
2. Integrity refers to making sure data is trustworthy and unaltered/free from tampering. Data must be authentic, accurate and reliable
3. Availability refers to systems, networks and applications functioning properly so the organizations and customers have access to it whenever needed

Updating your security program is the best way to protect your business from cyberattacks; it's a proactive security measure that is used to reduce the risks for companies to be exposed to cyberattacks in which cybercriminals target their sensitive data.

Overall constant monitoring is important because it helps identify the risk exposure to an enterprise, it helps decision making when it comes to building a strong cybersecurity program which also helps in preventing costly breaches and facing noncompliance penalties.