***사이버 보안의 종류 5가지에 대하여 나열하고, 그에 대하여 간략하게 서술하시오.**

1. 네트워크 보안 - 허가되지 않은 액세스와 피해로부터 회사의 네트워크를 보호하기 위해 설계된 일련의 전략, 프로세스, 기술 또는 승인되지 않은 상태에서 기업 네트워크를 침입하는 것을 막거나 방지하는 활동이다.

2. 애플리케이션 보안 - 무단 액세스 및 수정과 같은 보안 취약점에 대한 위협을 방지하기 위해 보안 기능을 개발하여 애플리케이션에 추가하고 테스트하는 과정 또는 애플리케이션 코드의 취약점을 찾아서 수정해 앱을 더 안전하게 만드는 보안 활동이다.

3. 정보보안 - 모든 정보자원을 위/변조, 유출, 훼손 등과 같은 정보보안 사고로부터 보호함으로써 무결성, 기밀성, 가용성을 제공하는 것 또는 데이터 보안으로도 불리며 저장 상태나 기계 간 전송 상태에서 승인되지 않은 액서스나 조직으로부터 데이터를 계속 안전하게 유지하는 활동이다.

4. 운영 보안 - 비즈니스 환경이 계획, 검증된 일정 수준으로 보호되려는 조치 및 통제, 요소로는 위협 / 취약성 / 자산, 운영 통제의 영향에는 기밀성 / 무결성 / 가용성
운영 보안의 상대는 내외부 침입자 / 사용자나 운영자 / 운영 환경에 대한 위협이 있다. 또한, OPSEC이라는 약자로 지칭되는 경우가 많고, 영리한 악의적 행위자가 적절히 분석하거나 다른 데이터와 결합하는 방법으로 숨겨야 할 '큰 그림'을 노출할 수 있는 퍼블릭 데이터를 평가, 보호하는 과정이다.

5. 재해 복구 - 각종 재해 및 위험요소에 의해 정보시스템이 중단됐을 때, 이를 정상으로 회복시키는 것, 또는 사이버 공격으로 초래된 광범위한 데이터 손실이나 서비스 중지 상태를 바로잡아 복구하는 기법이다. 핵심 용어로는 백업 / 비즈니스 연속성 / 지속적 데이터 보호 / 고가용성 / 복제가 있으며, 요소 및 절차로는 복구 제도 -> 복구 조식 -> 복구 시스템 -> 복구 계획 및 절차 -> 데이터 백업 -> 백업 관리 -> 복구 테스트 -> 사후 점검 및 확인 순이다.