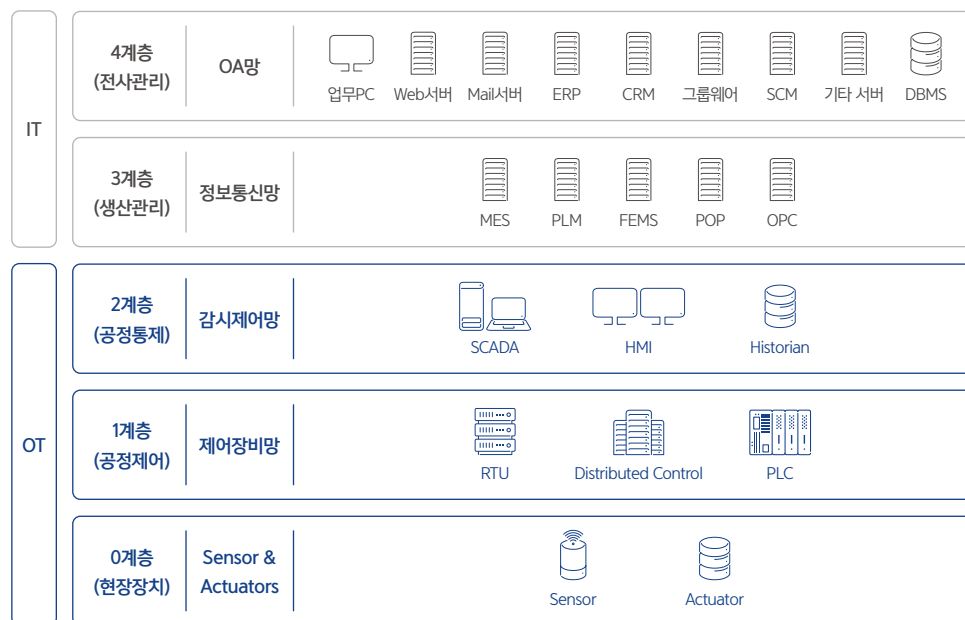


산업제어시스템 보안 경쟁력 확보의 기준

고도의 가용성이 요구되는 발전, 생산설비, 지하철과 같은 산업 분야에서 사용되는 PLC, DCS, HMI 장비 등의 산업제어시스템에 대한 보안 위협 점검 및 대응 방안을 제시합니다.

서비스 개요

산업제어시스템의 특성인 폐쇄성, 특수성, 가용성을 고려하여 단위장비 및 계통별 보안 취약점을 점검하고 대응 방안을 제시합니다.



특징

산업제어시스템에 대한 테스트베드 구성 노하우를 바탕으로 운영 중인 장비의 가용성에 미치는 영향을 최소화하여 점검을 수행하고 취약점 점검 결과를 기반으로 단위장비 및 계통 위협 모델을 제시합니다.

01 취약점 점검 결과를 기반으로 단위장비 및 계통 위협 모델 제시

02 산업제어시스템 테스트베드 구성 노하우로 운영 중인 장비의 가용성에 영향을 주지 않도록 점검

03 산업제어시스템 관련자 및 이용자의 보안인식 제고와 보안 내재화 활성화

점검항목

산업제어시스템 안전성 확보를 위해 보안설정 및 유지보수, 중요정보 노출, 암호화, 감사, 인증정보 관리, 데이터 검증, 권한 및 접근통제, 법적 요구사항 관리 등의 항목에 대해 점검합니다.

보안 설정 및 유지보수	· 초기 패스워드 변경, 원격접속 관리, 보안 패치 적용
중요 정보 노출	· 인증정보 및 암호 키 평문 노출 · 서버 및 OS 정보 노출
암호화	· 중요정보 전송 시 암호화 · 안전한 암호화 알고리즘 사용
감사	· 접속 및 보안 이벤트 로깅 여부
인증 정보 관리	· 인증 기능 제공, 인증 기능 우회, 세션 관리 기능, 무작위 대입 방지
데이터 검증	· 입력값 범위 검증(최소값, 최대값을 벗어난 값) · 통신 무결성 검증
권한 및 접근통제	· IP 접근 통제, 부적절한 오류 처리, 불필요 서비스
법적 요구사항 관리	· 서버/서비스 접속 시 경고문 표시 · 이전 접속 기록 공지 · 백도어 및 숨김 계정 존재 여부

수행절차

산업제어시스템에 대한 취약점 점검 및 모의해킹 수행을 통해 취약점 발견 및 발견된 취약점에 대한 대응 방안 제시 및 보안 위협을 가시화하여 위협 모델을 제시합니다.

