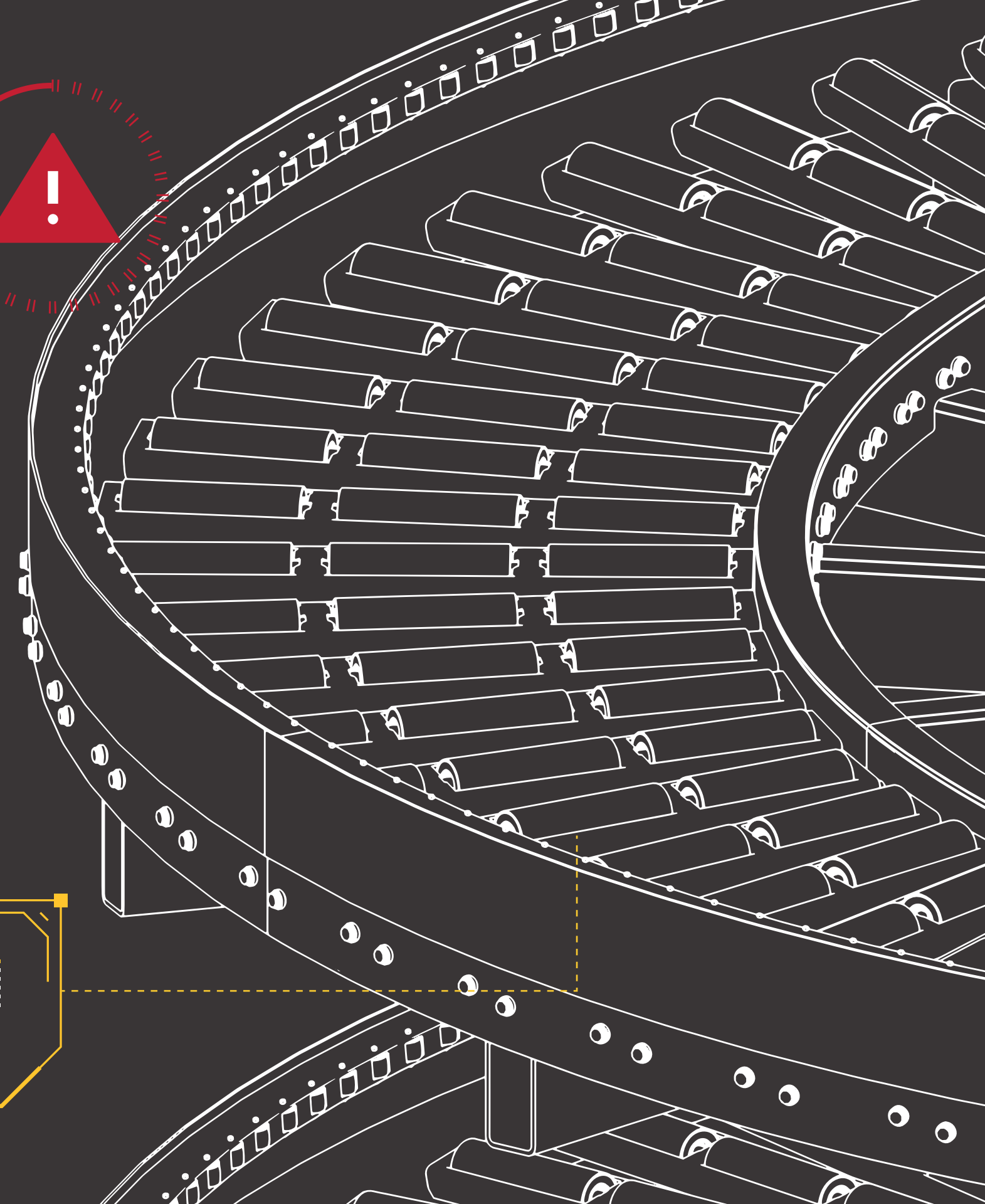
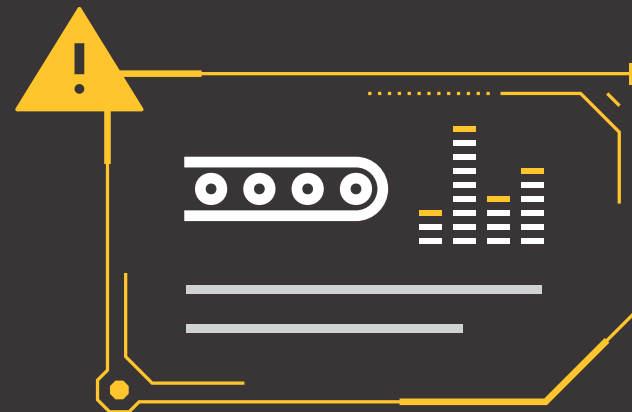




미디어 대상 요약 자료: 2022년 하반기

STATE OF XIoT SECURITY

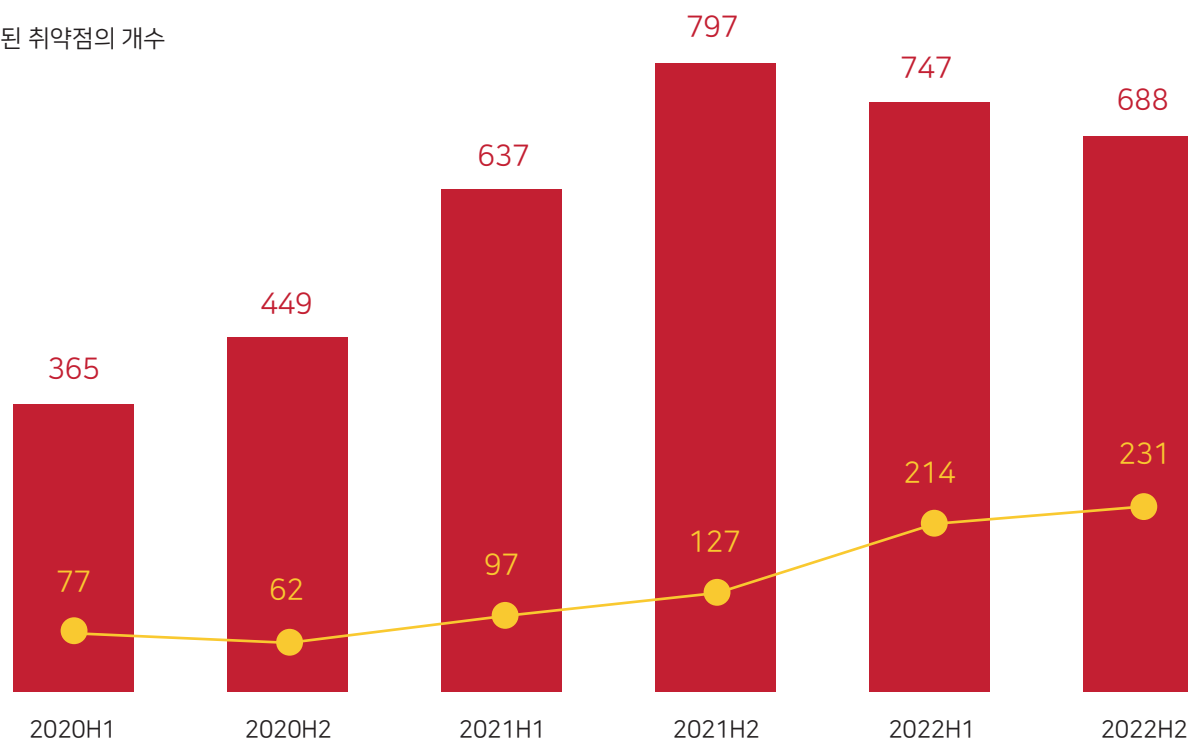
XIoT(확장 IoT) 전반에서 사이버물리시스템(CPS)에
영향을 미치는 취약점에 대한 Team82 분석 -2022년 하반기



6회차를 맞은 2022년 하반기 XIoT 보안 현황 보고서는 2021년 하반기 최고 수치를 기록한 사이버물리시스템(CPS)에 영향을 미치는 취약점 공개 건수는 감소한 반면, 내부 조사 및 제품 보안팀에 의해 공개되는 취약점의 수는 계속 증가하고 있음을 보여줍니다.

2020년 이후 공개된 취약점

- 공개된 취약점의 총 개수
- 공급업체 내부 조사에 의해 공개된 취약점의 개수



수치로 보는 취약점 공개

688

2022년 하반기에 공개된
XIoT 취약점 개수

231

공급업체 내부 조사팀에 의해
공개된 취약점의 개수

82%

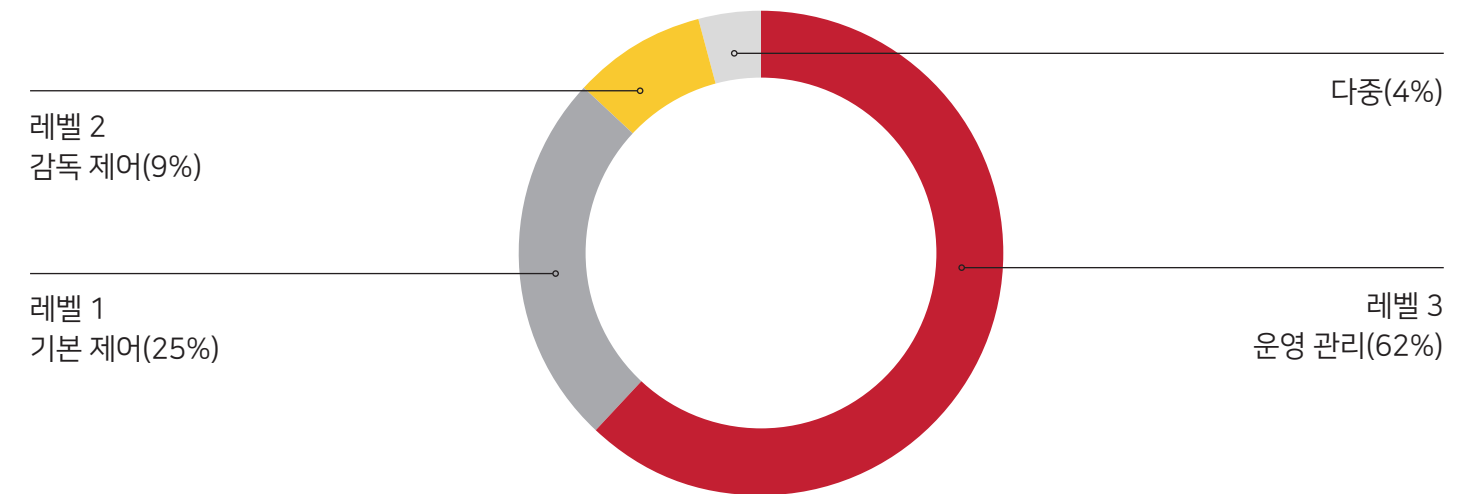
2021년 하반기 전체 공개 건수인
127개 대비 증가한
공급업체 공개 취약점의 비율

2022년 하반기 XIoT 보안 현황 보고서의 주요 결과

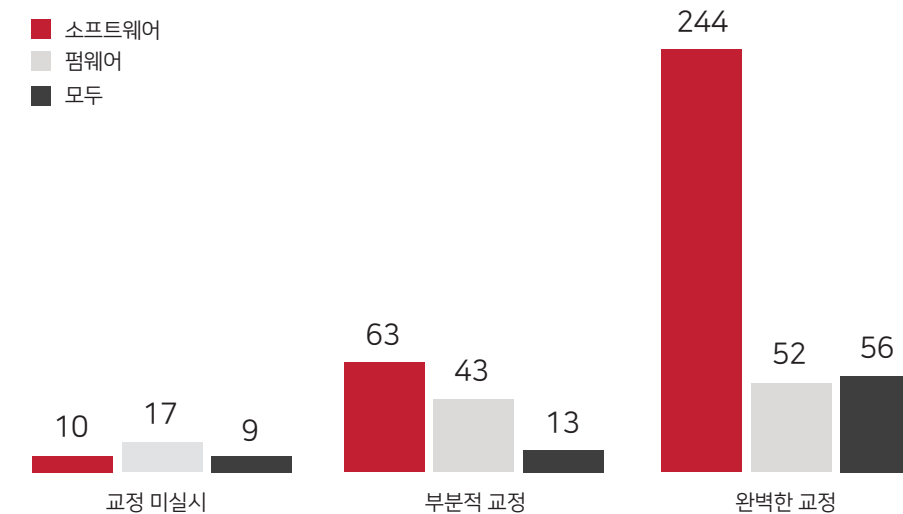
공개된 OT 취약점의 62%는 ICS용 퍼듀 모델의 레벨 3 디바이스에 영향을 미치며, 1/4은 레벨 1, 즉 PLC 및 기타 컨트롤러와 센서를 포함한 기본 제어 디바이스에 영향을 미칩니다.

데이터 세트에 대한 소프트웨어 기반 취약점의 지배적인 영향력은 계속 유지되고 있습니다. 보안 소프트웨어 도구가 발달하고 관련 인식이 성숙해짐에 따라 공급업체는 펌웨어에서 발견되는 취약점보다 소프트웨어 취약점을 빠르게 업데이트할 수 있습니다.

2022년 하반기에 공개된 **487**개의 취약점이 치명적이라는 평가 또는 높은 CVSS v3 점수를 받았습니다. 2022년 하반기에 공개된 치명적인 취약점은 **110**개였습니다.



2022년 하반기 교정 현황(펌웨어/소프트웨어별)



76%

완벽히 교정된 취약점 중 소프트웨어를 기반으로 하는 비율. 펌웨어보다 소프트웨어 패치의 용이성을 강조합니다.

63%

악용될 경우, 원격 코드 실행 또는 서비스 거부 (DoS)로 이어질 수 있는 부분적 또는 교정되지 않은 취약점의 비율

65

2022년 하반기에 Team82가
보고한 취약점의 개수(작년 한해
보고된 전체 취약점 개수는 117개)

30

65개 취약점 중 CVSS v3
점수가 9.5 이상인 취약점의 개수

63%

Team 82의 데이터 세트에 포함된
공개된 취약점 중 네트워크를 통해
악용될 수 있는 취약점의 비율

영향

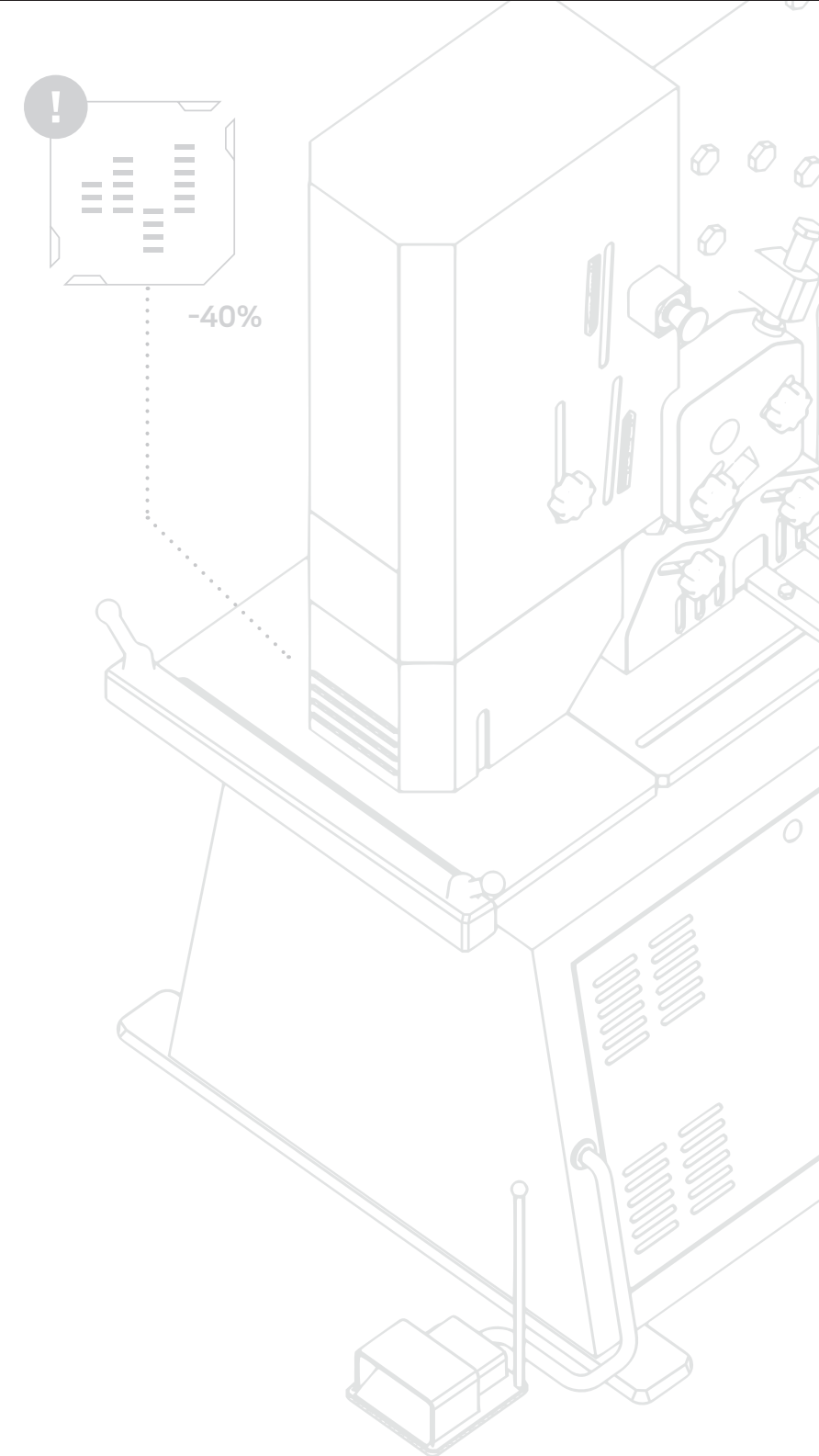
2022년 하반기에 공개된 취약점으로
인해 야기되는 주요 영향은 원격 코드
실행, 서비스 거부(DoS) 공격, 인증과
같은 보안 메커니즘 우회입니다.

CWEs

2022년 하반기 데이터 세트의 CWE
상위 5개 중 4개는 마이터(MITRE)의
CWE 상위 25개 목록에서도 5위 내에
위치해 있습니다.

FIXES

2022년 하반기에 발표된 취약점에 대해
권장되는 주요 완화 조치는 네트워크
세분화, 보안 원격 액세스(SRA) 및
랜섬웨어 차단을 포함합니다. OT 내 기타
완화 전략은 트래픽 제한,
사용자 및 역할 정책 구현, 워크스테이션
강화가 있었습니다.

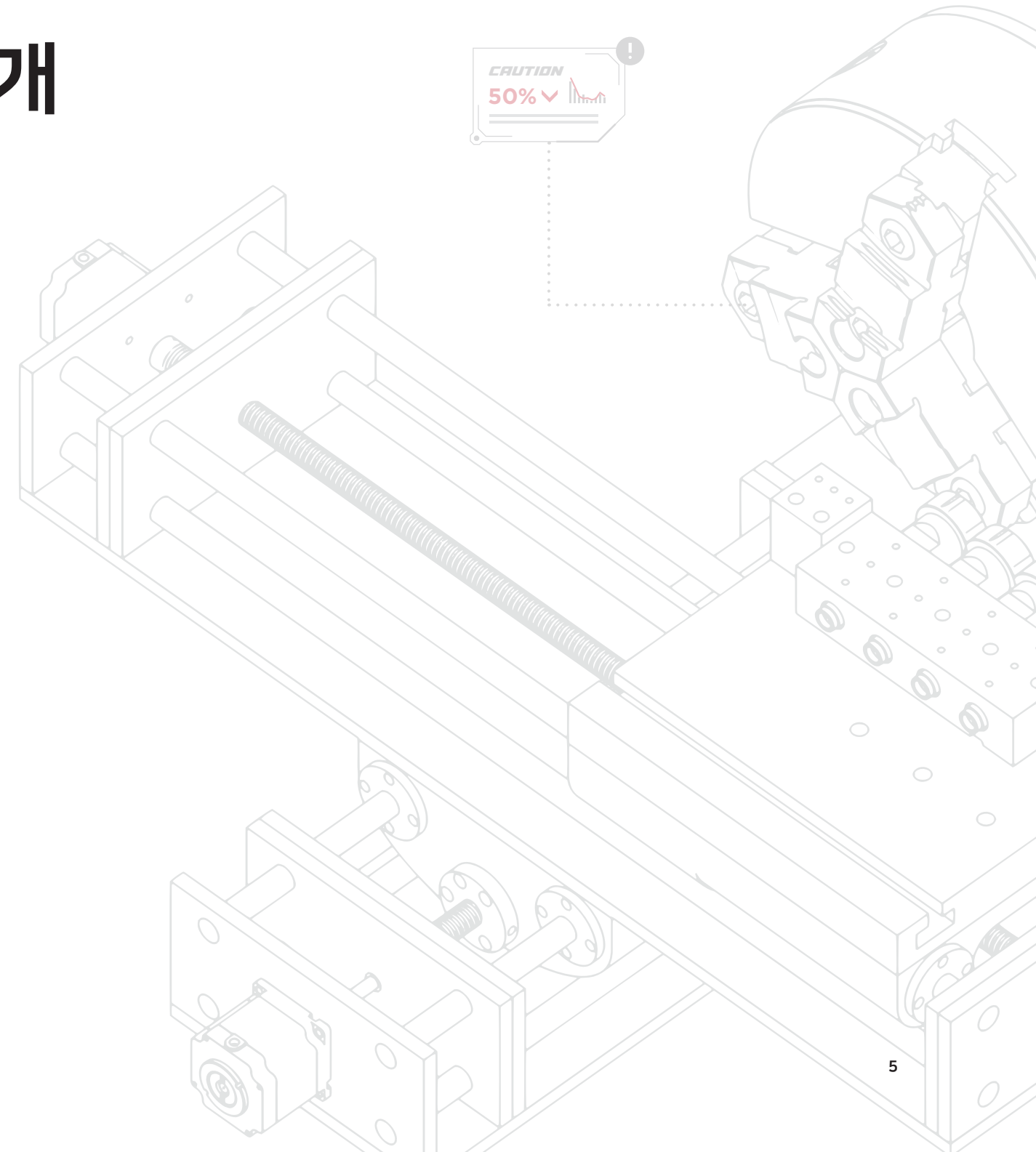


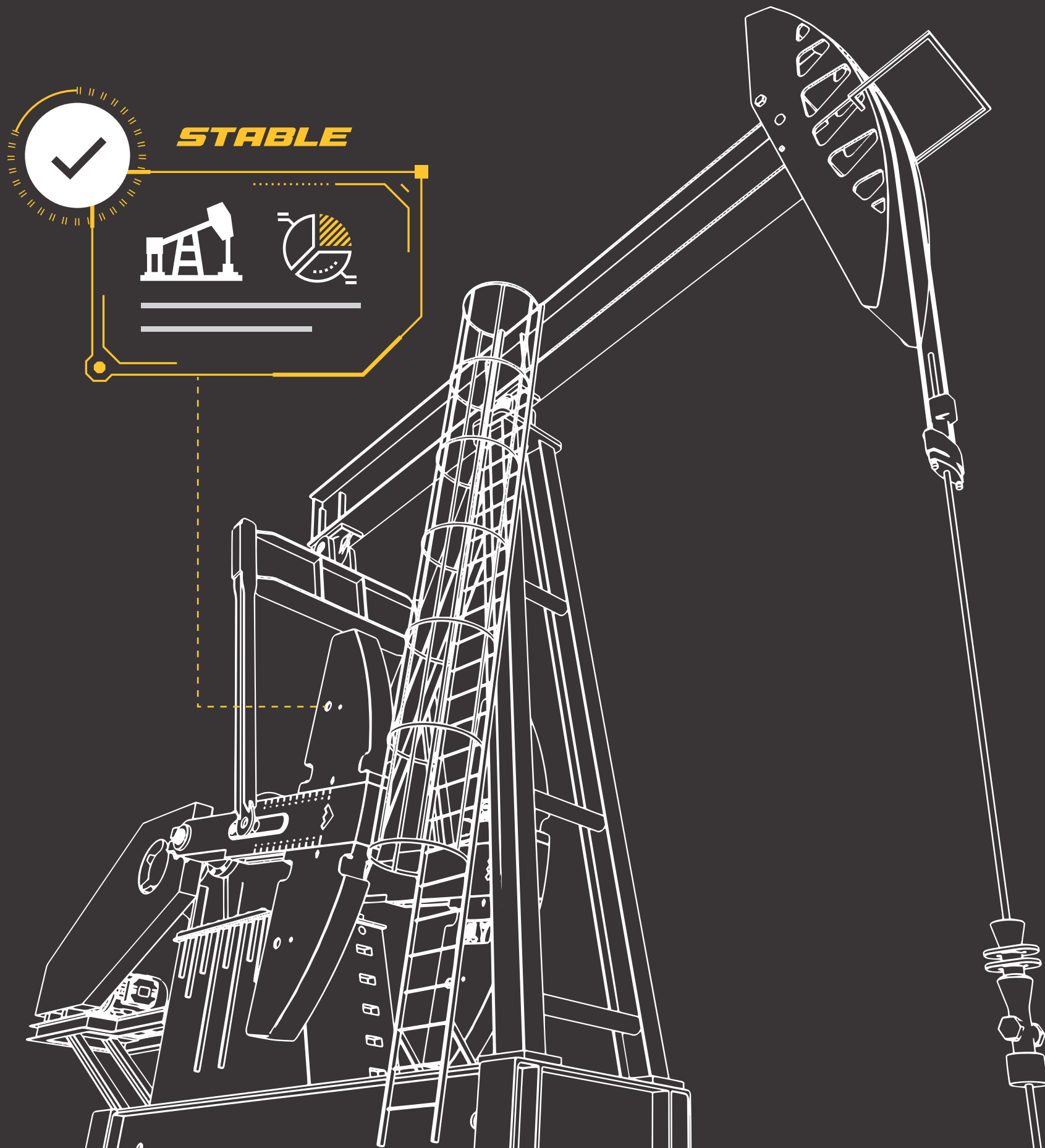
2022년 하반기 XIoT 보안 현황 보고서 소개

클래로티 Team82가 연 2회 발행하는 XIoT 보안 현황 보고서는 2022년 하반기에 공개된 산업, 의료 및 상용 제품에 영향을 미치는 연결된 디바이스의 다양한 취약점에 대한 심층 조사 및 분석을 제공합니다.

본 보고서를 통해 우리 삶의 근간이 되고 비즈니스 및 중요 인프라 부문의 혁신을 지원하는 산업 제어 시스템(ICS), 의료 사물 인터넷(IoMT), 건물 자동화 시스템, 엔터프라이즈 사물 인터넷(IoT) 디바이스에 영향을 미치는 취약점에 대한 정보를 습득할 수 있습니다.

Team82는 XIoT 위험 및 취약점 환경에 대한 이해의 필요성을 바탕으로 국가 취약점 데이터베이스(NVD), 산업 제어 시스템 사이버 긴급 대응팀(ICS-CERT), CERT@VDE, 마이터, 산업 자동화 공급업체인 슈나이더 일렉트릭(Schneider Electric), 지멘스(Siemens) 등 신뢰할 수 있는 오픈 소스에서 취약점 데이터를 수집하는 자동 수집 및 분석 도구를 개발했습니다.





Copyright © 2023 Claroty Ltd. All rights reserved