2026·08

SK 주식회사 AX Ackerton Partners

AI 플랫폼 설계/구축

OT 취약점 증대와 제조 산업 생태계의 사이버 안전성

글 | Ackerton Partners, IE본부 강진호 상무

Executive Summary

공격자 생태계의 조직화

- Dragos가 2026년 보고서에서 전 세계적으로 추적 중인 OT 위협 그룹은 26개, 이 중 2025년 실제 활동이 확인된 그룹은 11개에 달하며, AZURITE·PYROXENE·SYLVANITE 등 신규 그룹이 제조·자동차·에너지 부문의 엔지니어링 워크스테이션을 직접 겨냥하고 있다.
- IT 침투 이후 OT로 이동(Pivoting)하는 공격 경로가 정형화되면서, 개별 자산 탈취를 넘어 제어 루프(Control Loop) 자체를 지도화하는 2단계 공격이 관찰되고 있다.

제조업 표적 공격의 정량적 증가

- Fortinet 조사에 따르면 제조업 사이버보안 사고는 2023년 245건에서 2024년 333건으로 1년 사이 약 36% 증가하여, 산업군 중 가장 가파른 증가세를 보이고 있다.
- 네트워크를 통해 원격으로 악용 가능한 ICS 취약점 비중도 지속 확대되고 있어, 폐쇄망 신화에 의존한 기존 방어 전제가 더 이상 유효하지 않다.

취약점 관리 체계의 구조적 한계

- 2025년 한 해 ICS-CERT·NVD에 등재된 취약점의 25%가 CVSS 점수 오류를 포함했고, 26%의 권고문은 벤더의 패치나 완화 방안조차 제공하지 못한 것으로 확인됐다.
- Dragos의 위험 기반 분류 체계(Now·Next·Never)상 즉시 조치가 필요한 'Now' 등급은 전체의 2%에 불과해, CVSS 점수만을 근거로 한 일괄 대응은 오히려 리소스를 왜곡시킬 수 있다.

산업 생태계 내 리스크 전이 구조

- 보안사고 사례들 중, 고객정보 유출과 내부자료 유출 사고는 IT 영역에서 발생했음에도 기업 간 신뢰·연계망을 통해 관련 기업 전반의 보안 신뢰도에 영향을 미쳤다.
- 국내 한 반도체 기업이 2020년 OT·ICS 전담조직을 신설하며 생산라인 보안에 선제 투자해 온 것과 달리, 업계 내 제조 기업 간 OT 보안 성숙도는 편차가 크다.

Executive Summary

제조 산업 특유의 가용성 리스크

- 반도체·배터리·화학 등 제조 산업 기업들의 생산 설비는 Purdue Model상 Level 0~2 구간에 밀집되어 있어, 패치 적용 자체가 생산 중단으로 이어질 수 있는 가용성 최우선 환경이다.
- IT 영역의 CIA(기밀성-무결성-가용성) 우선순위와 달리 OT 영역은 가용성-무결성-기밀성 순으로 재정렬되어야 하며, 이는 보안 대책의 설계 방식 자체를 달리 요구한다.

표준 기반 대응과 실행 로드맵

- IEC 62443과 NIST CSF 2.0을 축으로 한 이행 로드맵은 개별 사고 대응을 넘어, 계열사 전반에 공통 적용 가능한 진단·개선 언어를 제공한다.
- Ackerton Partners는 자산 가시성 확보 → 위험 기반 우선순위화 → 단계적 이행이라는 3단계 접근을 통해, 그룹 차원의 OT 보안 성숙도를 정량적으로 끌어올리는 방안을 제언한다.

01 공격자 생태계의 조직화

지난 1년간 OT 사이버 위협은 양적 증가를 넘어 질적으로 변화했다. 공격자들은 공장 설비의 전체 연계 흐름을 파악한 뒤, 실제 생산 공정을 조작하는 고도화된 단계까지 접근하고 있다. 이는 방어자 입장에서 단순한 '침해 여부'가 아닌 '공정 동작의 정상성'을 기준으로 판별 방식 자체를 전환해야 함을 의미한다. 이러한 변화의 배경에는 위협 그룹 자체의 재편이 있다.

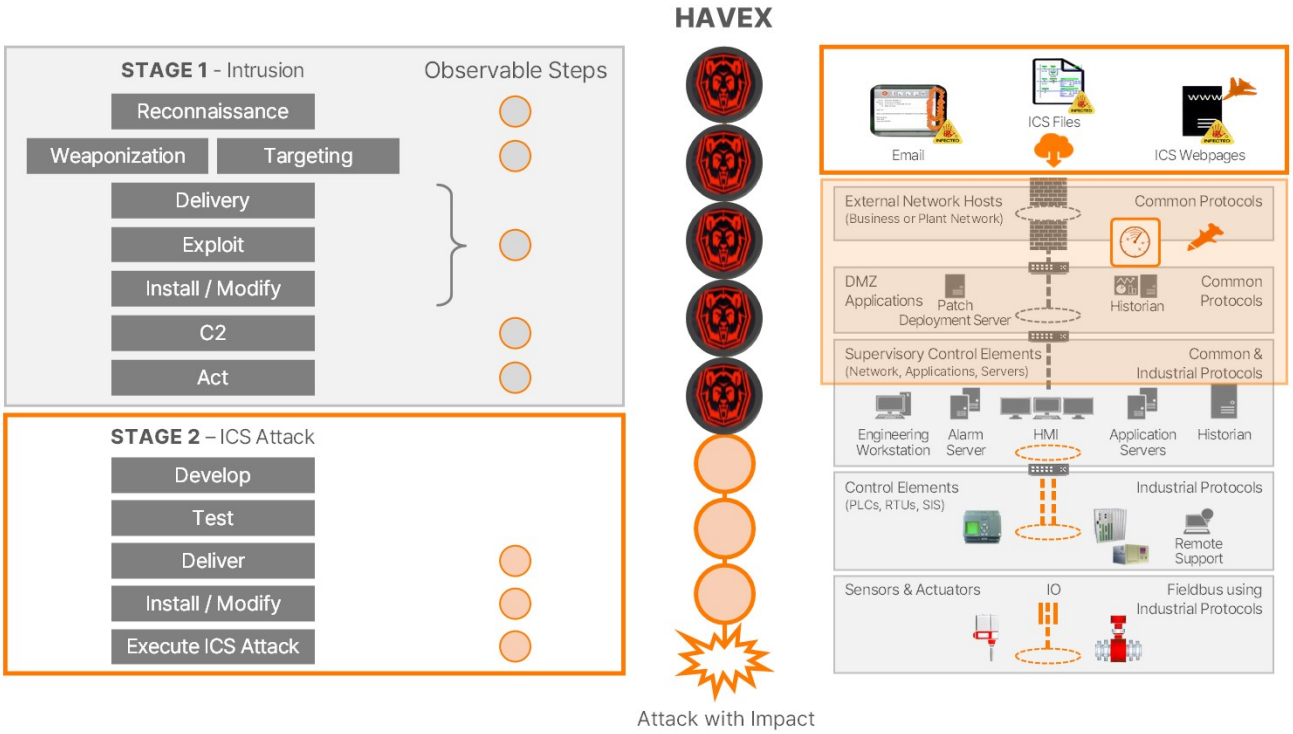
1.1 신규 위협 그룹의 등장과 역할 분화

Dragos가 발표한 「2026 OT/ICS Cybersecurity Report and Year in Review」에 따르면, 전 세계 추적 중인 OT 위협 그룹은 총 26개이며, 이 중 11개가 2025년 실제 활동했다. 신규 식별된 AZURITE, PYROXENE, SYLVANITE(위협조직 코드명, 회사명 아님) 3개 그룹은 역할이 뚜렷이 나뉜다 - AZURITE는 제조·방위·자동차·전력·석유가스 부문의 엔지니어링 워크스테이션(설비 제어용 관리자 PC)을 표적으로 공정 데이터 탈취에 주력했고, PYROXENE은 공급망 침해와 사회공학으로 IT에서 OT로의 진입 경로를 마련했으며, SYLVANITE는 취약점을 신속히 무기화해 다른 그룹에 발판을 넘기는 초기 접근 브로커 역할을 수행했다.

1.2 기존 그룹의 역량 고도화와 Kill Chain 진행

더 우려스러운 대목은 기존 활동 그룹의 역량 고도화다. VOLTZITE는 ICS Cyber Kill Chain(공격이 침투→시스템 장악→목표 달성으로 진행되는 단계 모델) 2단계로 격상된 것으로 평가되는데, 엔지니어링 워크스테이션 소프트웨어를 조작해 설정·알람 데이터를 추출하고 공정 중지 유발 조건을 조사한 정황이 확인됐다.

[그림 1] ICS Cyber Kill Chain 모델



*출처: SANS Institute/Dragos (Semantic Scholar 학술 데이터베이스 재인용)

이는 공격자가 '침투'를 넘어 '조작 가능성 검증' 단계로 이동하고 있음을 보여주는 신호다.

02 제조업 표적 공격의 정량적 증가

이처럼 정교해진 공격 조직의 활동은 실제 피해 통계에서도 뚜렷하게 확인된다.

2.1 제조업 침해사고 건수 추이

Fortinet의 「2025 State of Operational Technology and Cybersecurity Report」는 제조업 사이버보안 사고가 2023년 245건에서 2024년 333건으로 약 36% 증가했음을 보여준다. 이는 스마트팩토리 확산으로 생산 설비·SCADA(설비 상태를 실시간 감시·제어하는 시스템)·물류/품질관리 시스템이 네트워크로 통합되면서, 과거 격리되어 있던 생산망의 노출 표면적(Attack Surface)이 확대되었음을 방증한다.

2.2 네트워크 노출 취약점 비중 확대

실제로 ICS(산업제어시스템 - 공장 설비의 생산 공정을 자동 제어하는 시스템) 취약점 중 네트워크로 원격 악용 가능한 비중은 2023년 16%에서 최근 22%까지 상승해, '물리적으로 분리되어 있으니 안전하다'는 전제는 더 이상 유효하지 않다.

2.3 랜섬웨어의 산업 자산 직접 표적화

이러한 증가세는 랜섬웨어 영역에서 더욱 뚜렷하다. Dragos에 따르면 2025년 산업 조직을 공격한 랜섬웨어 그룹은 119개로 전년 대비 49% 증가했고, 피해 조직은 전 세계 3,300여 곳, 이 중 제조업이 3분의 2 이상을 차지했다. 더 우려스러운 점은 엔지니어링 워크스테이션·SCADA 인프라처럼 OT를 뒷받침하는 자산이 노출되면, 다수 사고가 'IT 사고'로 분류되면서도 실질적 운영 차질을 유발한다는 것이다. **이는 IT·OT를 별개 위험 영역으로 다루는 기존 관리 체계가 실제 공격 표면과 괴리되어 있음을 보여준다.**

더 많은 내용을 보시려면

파일 다운받기

버튼을 눌러주세요