SOFTFLOW

SBOM에서 OT까지,
디지털 공급망을 보호하는 보안 기업

소프트웨어 공급망 보안 및 위협 인텔리전스 전문기업

소프트플로우 주식회사

KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY
정보보호클러스터 육성기업

NSR 국가보안기술연구소 National Security Research Institute
패밀리기업

KSAE 사단법인 한국자동차공학회 The Korean Society of Automotive Engineers

KSTA 한국SW테스팅협회

KESSIA 임베디드소프트웨어·시스템산업협회 Korea Embedded Software and System Industry Association

Digital Health Security Association 디지털헬스보안협회

Executive Summary

- **왜 소프트플로우(주)인가?**

제조 현장의 특수성(OT)을 이해하는가? 실제 침해 사고에 대응할 수 있는 실전 역량을 가졌는가?

독보적인 OT/ICS 전문성

단순 IT 보안을 넘어, 스마트 공장 및 제조 설비(PLC/HMI)에 특화된 보안 점검 기술과 에이전트리스(Agentless) 분석 솔루션을 보유하고 있습니다.

검증된 수행 이력

2021년부터 한국인터넷진흥원(KISA)의 스마트 공장 보안 모델 연구 및 취약점 점검 과제를 5년 연속 성공적으로 수행한 국내 유일 수준의 정예 기업입니다.

지역 산업 밀착형 경험

경남테크노파크의 '스마트공장 보안 기술 테스트베드' 구축 사업을 이미 성공적으로 완수한 바 있어, 도내 기업의 환경과 발주처의 행정 절차를 이해하고 있습니다.

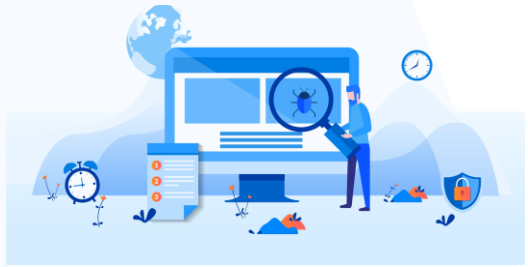
SOFTFLOW

1. 소프트플로우 주식회사

- **회사 개요: SBOM에서 OT까지, 연결된 세상을 지키는 보안 아키텍처 제공**

소프트웨어 공급망 보안을 중심으로, 취약점 관리 및 사이버 위협 대응 플랫폼 보안 솔루션 기업

- 회사명: 소프트플로우㈜ (SOFTFLOW Inc.)
- 설립연도: 2018년 2월
- 사업 분야
  - 소프트웨어 공급망 보안
  - ICS/사이버 보안
  - 위협 인텔리전스
- 파트너십
  - Black Duck Software, Tenable과 전략적 협력
- 핵심 철학 및 비전
  - 우리는 소프트웨어와 인프라, 사람과 기계를 연결하는 모든 지점에서 보안의 신뢰와 가시성을 제공합니다.
- 핵심 역량 키워드
  - SBOM 기반 공급망 보안
  - IT/OT 자산 통합 보호
  - 보안 시험 자동화 및 전문 엔지니어링 서비스



소프트웨어 개발부터 인프라 운영까지,
사이버 위협에 선제적으로 대응하는 보안 전문가 집단

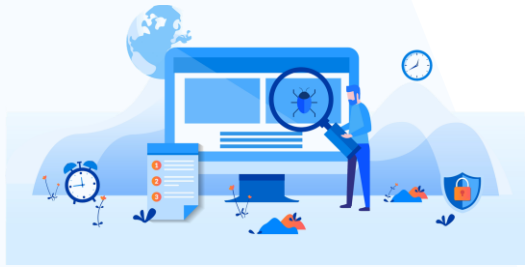
SOFTFLOW

1. 소프트플로우 주식회사

- **주요 연혁 및 주요사업 실적: SBOM에서 OT까지, 연결된 세상을 지키는 보안 아키텍처 제공**

IT/OT 통합 환경 및 공급망 보안을 중심으로, 취약점 관리 및 사이버 위협 대응 플랫폼 보안 솔루션 기업

- 2025년
  - KISA SBOM 기반 SW 공급망 보안모델 구축
  - KISA 디지털제품 핵심 분야별 보안리빙랩 통합 이전 구축 및 운영
- 2024년
  - Black Duck Software “Top Performing Partner Korea” 수상
  - KISA 5G+ 핵심서비스 분야별 보안리빙랩 통합 유지관리 및 운영
  - KISA 스마트공장 보안 취약점 점검 및 보안컨설팅
  - KISA IoT 보안 테스트베드 SBOM 분석 환경 구축 및 지원
  - KISA 우주기업 보안 취약점 점검 및 보안모델 개발 용역
- 2023년
  - KISA IoT 보안 테스트베드 SBOM 분석 환경 구축 및 지원
  - KISA 스마트공장 보안 취약점 점검 및 보안컨설팅
  - 경남테크노파크 스마트공장 보안 기술 테스트베드 구축
- 2022년
  - KISA 스마트공장 보안 취약점 점검 및 보안 모델 고도화
  - KISA 스마트공장 보안 점검 솔루션 공급
  - IoT 보안 플랫폼 SOFLO.IoT 기술 연구 개발
- 2021년
  - KISA 스마트공장 보안 취약점 점검 및 보안 모델 고도화
  - KTL 소프트웨어 취약점 분석 솔루션 공급
  - 국방기술진흥연구소 국방벤처 지원사업 – 이상징후 탐지 기술
- 2020년
  - 스마트공장 보안점검 솔루션 ‘NCA’ 출시
  - ICS 이상 징후 탐지 장치 특허 확보
  - 기업부설연구소 설립
- 2019년
  - KISA 정보보호클러스터 보안 기술 육성 기업 선발
  - 스마트팩토리 어워드코리아 보안솔루션 기업혁신대상 수상
- 2018년
  - 소프트플로우㈜ 설립



소프트웨어 개발부터 인프라 운영까지,
사이버 위협에 선제적으로 대응하는 보안 전문가 집단

SOFTFLOW

2. 사업 영역

- **핵심 사업 영역**

소프트웨어 개발 및 배포부터 OT 인프라 보안까지의 사이버 보안 솔루션

- 소프트웨어 취약점 분석 및 SW 구성분석
- SBOM 기반 SW 공급망 보안 관리
- 보안 시험 자동화 (퍼징 테스트 등)

- 위협 분석 및 위협 모델링
- 소프트웨어 공급망 보안 관리 프레임워크 구축
- ISO 26262 / ISO 21434 / IEC 62443 등 국제 표준 준수 지원

소프트웨어 공급망 보안

ICS/사이버 보안

Solution Business

- 소프트웨어 공급망 보안 시험 자동화 및 시각화
- 네트워크 데이터 기반 이상징후 탐지

R&D Business

Leading Technologies

인프라 취약점 관리

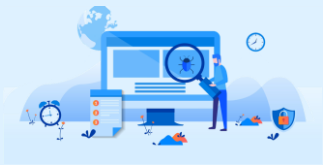
엔지니어링 / 컨설팅 서비스

Service Business

- 보안 위협 및 이상징후 탐지 (주요정보통신기반시설 등)
- 위협 인텔리전스: 외부 위협 및 다크 웹 분석

- 자산 식별 및 취약점 분석, 위험 관리
- 시스템 분석 및 침투테스트

BLACKDUCK® paloalto® NETWORKS tenable®



안전한 소프트웨어를 개발과 중요 시스템 보호, 새로운 위협의 선제적 대응

SOFTFLOW

3. 핵심 역량

- **신뢰 기반의 SW 공급망 보안 및 위협 인텔리전스 파트너**

SW 공급망 보안 및 OT/ICS 환경 보안 역량을 기반의, 국제 표준 준수/위협 인텔리전스 서비스 제공

스마트 제조(OT/ICS) 특화 보안 방법론

▼ 운영 중단 없는 점검
- 가동 중인 제조 라인에 영향을 주지 않는 'Passive Monitoring' 및 'Agentless' 방식의 점검 기술 적용

▼ NCA(Network Configuration Analysis)
- 폐쇄망 환경에서도 비인가 접속 및 비정상 트래픽을 포착하는 독자적인 트래픽 분석 기술 보유

▼ 국제 표준 준수
- 국제 표준 준수: IEC 62443(산업보안) 등 글로벌 규제에 기반한 점검 프레임워크를 적용하여 참여 기업의 글로벌 경쟁력 제고

실전형 사이버 위기대응 모의훈련 설계

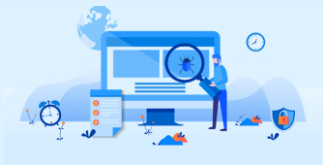
▼ 맞춤형 시나리오
- 경남 지역 주력 산업(기계, 자동차, 방산)에서 실제 발생한 침해 사례를 기반으로 AI 고도화 공격 시나리오 설계

▼ 단계별 주입 방식
- 단순 메일 발송을 넘어, 내부망 침투, 권한 탈취, OT 네트워크 확산 등 실제 공격 그룹의 TTPs(전술·기법·절차)를 단계별로 모사하여 훈련의 실전성 극대화

SBOM 기반 공급망 보안 체계 구축

▼ 가시성 확보
- 제조 소프트웨어의 구성 요소(SBOM)를 분석하여 취약한 오픈소스나 악성 코드가 포함되었는지 정밀 검증하는 역량 보유

▼ SW 공급망 컨설팅 역량
- KISA SW 공급망 보안 모델 지원사업 수행 경험 보유



SOFTFLOW

3. 핵심 서비스

- **신뢰 기반의 SW 공급망 보안 및 위협 인텔리전스 파트너**

SW 공급망 보안 및 OT/ICS 환경 보안 역량을 기반의, 국제 표준 준수/위협 인텔리전스 서비스 제공

제공 서비스	설명
1. SW 공급망 보안 테스트 자동화	• 정적분석/SW구성분석 도구 통합 및 SBOM 기반 자동 검증 환경 구축
2. 위협 분석 및 보안 관리 프레임워크 구축	• 위험 기반 접근법(Risk-based Approach)에 따른 보안 프로세스 설계 및 운영
3. 국제 표준(IEC 62443, ISO 21434 등) 준수 컨설팅	• 글로벌 규제 및 인증 대응을 위한 보안 테스트 환경 구성 및 활용 컨설팅
4. 산업제어시스템(ICS) 보안 컨설팅	• OT 환경 위협 분석 및 방어체계 개선을 통한 생산설비 보안 강화
5. 보안 테스트베드 및 리빙랩 구축·운영	• 실제 산업 환경을 모사한 실증형 보안 검증 및 연구 인프라 제공

3. 사업실적: 성공의 증거

- **본 사업의 유사한 사업 수행 실적 보유**

최근 3년간 본 사업과 직접적으로 연관된 유사 사업 수행 실적 보유

연번	사업명	고객사	계약시작일	계약만료일	핵심 성과 및 의미	계약금액 (백만원)
1	우주기업 보안취약점 점검 및 보안모델 고도화	한국인터넷진흥원	2025.05	2025.12	국가 전략 산업인 우주항공 분야의 고도화된 보안 요구사항 충족	52
2			2024.05	2024.12		175
3	스마트공장 보안취약점 점검 및 보안컨설팅	한국인터넷진흥원	2025.04	2025.12	4년 연속 수행. 전국 스마트 공장 보안 점검 표준 모델 수립 및 실증 주도	98
4			2024.05	2024.12		149
5			2023.05	2023.12		93
6			2022.05	2022.12		154
7	스마트공장 보안 기술 테스트 베드 구축	경남테크노파크	2023.12	2024.01	경남 지역 산업 특성 반영. 도내 제조 기업 대상 보안 교육 및 기술 실증 환경 구축	331
8	스마트공장 보안리빙랩 보안성 시험 환경 고도화를 위한 점검도구 구매	한국인터넷진흥원	2022.11	2023.11	산업제어시스템 특성을 고려한 보안 시험 환경 구축	48
9	스마트공장 보안취약점 점검 및 보안모델 고도화	한국인터넷진흥원	2021.05	2021.12	우리나라 스마트 공장 보안 점검 표준 모델, 보안 시험 방법론 수립 및 실증 수행	90
10	울산지역 특화산업 정보보안 컨설팅 용역	울산정보산업진흥원	2020.09	2020.12	지역 특화 산업의 보안 취약점 점검 및 컨설팅 수행	50

3. 전문 조직: 인적 자원

- **산업제어시스템 및 보안 전문 인력 투입**

스마트 제조 보안 분야에서 10년 이상의 경력을 보유한 인원 투입

프로젝트 매니저 (PM)

사업 총괄 · 스마트공장 보안점검

PM

소범석

경력 14년 5개월

5년

유사사업 수행 이력 - KISA

2021 — 2025 (5개년 연속)

- KISA 스마트공장 보안취약점 점검 및 보안모델 개발 PL
- 우주 / SBOM 보안 기술 리드
- 스마트공장 보안점검 및 취약점 점검 경험 보유

핵심 연구원

모의훈련 기획/운영 · 결과 분석

핵심

김 관식

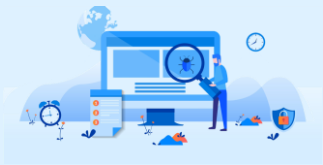
경력 12년 11개월

5년

유사사업 수행 이력 - KISA

2021 — 2025 (5개년 연속)

- KISA 스마트공장 보안취약점 점검 및 보안모델 개발
- 위협 분석 및 테스트베드 구축
- 보안 안내서 개발 및 PoC 시스템 설계



PM·핵심연구원 합산 유사 수행경력 12개년 | 스마트공장 보안 분야 최적의 리더십 조합

SOFTFLOW

4. 차별화된 방법론 보유

- **IT 보안: 전통적 인프라 및 공급망 심층 진단**
- **OT 보안: 제조 현장 특화 실시간 트래픽 가시성 확보**

최근 사이버 위협의 핵심인 소프트웨어 공급망 보안까지 포함하는 다각도 진단 수행

IT 보안

네트워크 및 시스템 보안 점검

- 네트워크 아키텍처의 보안 적정성 검토
- 서버 OS의 하드닝(Hardening) 상태 점검
- 불필요한 서비스 및 비인가 계정 유무를 심층 분석

웹 취약점 및 모의해킹

- OWASP Top 10 등 국제 표준 기반의 취약점 진단
- 실제 공격 시나리오를 바탕으로 한 수동 모의해킹을 통해 논리적 결함 및 침투 경로 식별

SBOM 기반 공급망 보안 진단

- 소스코드 정적 분석(SAST) 및 오픈소스 구성 분석(SCA)을 통해 소프트웨어에 포함된 알려진 취약점(CVE)과 라이선스 위험을 식별하여 공급망 기반 공격 대비

OT 보안

산업용 프로토콜 심층 패킷 분석

- Modbus, S7, EtherNet/IP 등 주요 산업용 프로토콜을 분석하여 비정상적인 제어 명령이나 비인가 제어기 접근 시도 탐지

NCA 솔루션 기반 실시간 가시성

- 에이전트 설치가 필요 없는 네트워크 트래픽 미러링 방식을 활용하여, 공정 가동에 영향을 주지 않고 모든 자산(PLC, HMI, 센서 등)의 통신 흐름 시각화

이상 행위 및 내부 위협 감시

- 정상적인 설비 통신 패턴을 학습하여 베이스라인을 구축하고, 이를 벗어나는 랜섬웨어 확산 징후나 악의적인 내부자에 의한 이상 트래픽 즉각 식별

OT/IT 통합 위험 지수 도출

- 공정 시스템과 IT 관리 시스템 간의 연결 접점을 분석하여 전사적 관점의 보안 위협 수준을 평가하고 최적화된 개선 로드맵 제시

5. 핵심 사업 솔루션

- **DevSecOps에 최적화된 애플리케이션 보안 플랫폼**

소프트웨어 공급망 전반의 비즈니스 위험 최소화와 신뢰 구축

Coverity (SAST)

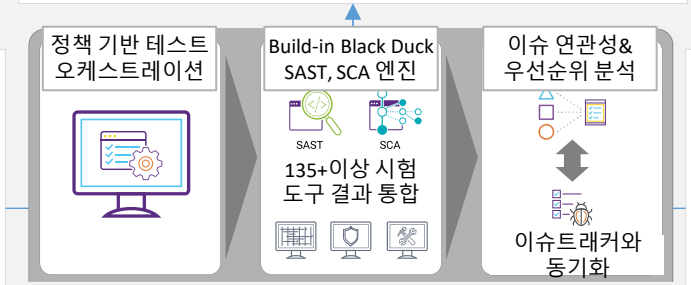
- 정적 애플리케이션 보안 테스트
- 소스코드의 보안 및 품질 문제 탐지

Black Duck SCE (SCA)

- 소프트웨어 구성 분석
- 오픈소스 종속성을 추적하고 소프트웨어 공급망의 위험 관리

Software Risk Manager (ASPM)

- 보안 및 개발팀의 애플리케이션 통합 보안 및 위험 관리
- 정책, 테스트 오케스트레이션, 상관 관계 분석, 우선순위 지정 및 전사적 보안 관리 간소화



Seeker (IAST)

- 대화형 애플리케이션 보안 테스트
- DevOps 파이프라인 內 웹 보안 테스트 자동화

Defensics (Fuzzing)

- 서비스 및 프로토콜의 결함 및 제로 데이 취약점 식별
- 소프트웨어 보안 취약점의 효율적/효과적 발견 및 해결

BLACKDUCK®

SOFTFLOW

5. 핵심 사업 솔루션

- **IT/OT 시스템의 취약점 및 보안 위협의 식별 및 해결**

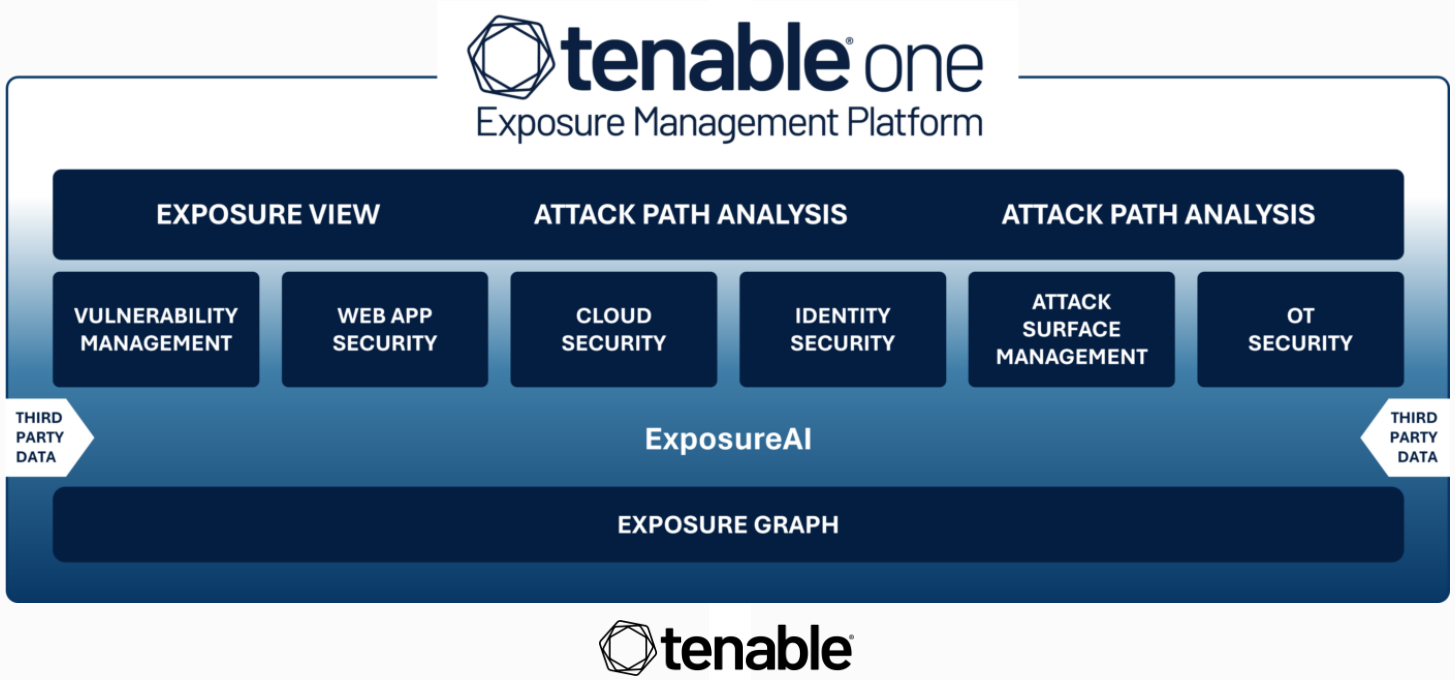
IT 인프라, 클라우드 환경, 중요 인프라 등의 사이버 및 보안 위협 공략

Tenable Security Center

- 사이버 취약점 파악 및 해결
- IT 및 SW 서비스 전반의 위험 최소화
- 사이버 위험 노출로부터 기업 보호

Tenable OT Security

- 융합 OT/IT 환경을 위한 통합 보안
- 운영 중단 없는 중요 시스템 보호
- 악의적인 내부자 및 인적 오류 등으로 부터 산업 네트워크 보호



SOFTFLOW

5. 핵심 사업 솔루션

• 네트워크 트래픽 수집 및 분석 솔루션

사이버 위협 및 내부 보안 이상징후와 비인가 연결 탐지

주요 기능 및 특징

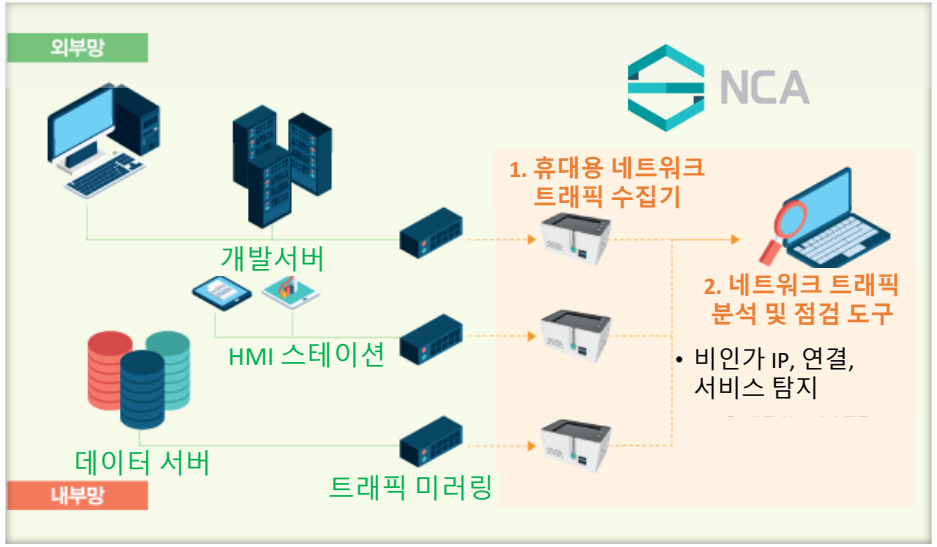
- 네트워크 트래픽 패킷 실시간 수집 및 저장 (PCAP 기반)
- 비인가 IP, 비인가 연결, 비인가 서비스 탐지
- 비인가 서버 접근, 이상패턴 탐지 기능 내장
- 수집한 패킷 기반 비정상 행위 탐지 및 분석 보고서 생성
- 폐쇄망 환경에서의 운영 최적화 (에이전트 미탑재 방식)

활용 사례

- 폐쇄망 내 주요 시스템의 통신 행위 점검
- 산업제어시스템(ICS) 환경에서의 OT 트래픽 이상 탐지
- 주요정보통신기반시설, 공공기관의 이상행위 탐지 및 침해사고 조사 대응 체계 구축

기대효과

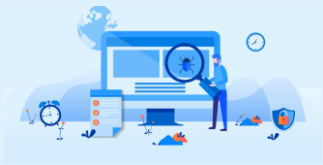
- 내부망 이상 트래픽을 사전 탐지하여 사이버 위협 대응력 강화
- 감시 및 기록 기능을 통해 감사·추적·규제 대응 가능
- 네트워크 보안 담당자의 점검 업무 자동화 및 편의성 향상



<NCA 아키텍처>

SOFTFLOW

6. 주요 고객/ 레퍼런스



- **기술 기반 보안 혁신의 실제 성과**

테스트 자동화, 보안 프레임워크 설계, 표준 기반 컨설팅 등 다양한 영역에서 성공적으로 프로젝트를 수행

코드부터 위협 인텔리전스까지, 신뢰로 연결된 보안 역량 제공

금융 및 공공

- ICS/IoT 보안 테스트베드/리빙랩 구축 및 고도화
- SW 공급망 보안 관리 체계 연구, 구축 및 컨설팅
- 자산 식별 및 보안 취약점 관리

제조 및 자동차

- OT 보안 위협 분석 및 대응 체계 컨설팅
- IEC 62443, ISO 21434 기반 보안 요구사항 수립, 검증 환경 구축, 보안 관리 프레임워크 설계
- 차량용 SW 보안 테스트 자동화 환경 구축

IT 및 의료 등

- FDA 사이버보안 가이드라인 준수 지원
- DevSecOps 환경 내 정적·SW구성분석 통합 플랫폼 구축
- SW 공급망 보안 체계 수립 컨설팅

실증 기반 보안 검증체계 완성, 공공 확산 모델 구축

KISA · nipa 정보통신산업진흥원 · 대한민국 국방부 Ministry of National Defense · ktl 한국산업기술시험원 Korea Testing Laboratory · 국방과학연구소 Agency for Defense Development · KTC 한국기계전기전자시험연구원 · wmit (재)원주의료기기산업진흥원 · DTaQ 국방기술품질원 · Hyundai Card · KR · 재단법인 경남테크노파크 Gyeongnam Technopark

OEM 보안 프로세스 정립, 글로벌 감사 대응 완료

LS Automotive · HDN Handreamnet · Hankook & Company · 아이나비 시스템즈 · Hyunbo · 현대중공업 · GIGA 광주그린카진흥원

해외 진출을 위한 사이버보안 가이드라인 대응 기반 확보

건양대학교의료원 KONYANG UNIVERSITY MEDICAL CENTER · FADU · MANGOBOOST · YUJIN ROBOT · CUREXO ROBOTICS BEYOND CURE · AI TRICS

소프트플로우는 기술 중심의 보안 파트너로서 고객의 안전한 디지털 운영을 함께 설계합니다.

7. 결론

- **경남 제조 AX의 성공, 소프트플로우가 보장합니다**

경남의 기업들이 사이버 위협으로부터 자유롭게 AI 기술 중심의 제조 혁신(AX)을 이룰 수 있도록 돕는 보안 파트너

준비된 인력: 스마트 제조 보안의 '실무 전문가' 배치

검증된 리더십
- 사업 PM의 14년 이상 보안 분야 전문 경력 보유.
- 2021년부터 2025년까지 KISA 스마트공장 및 우주 기업 보안 모델 고도화 사업 총괄 수행

정예 기술 조직
- 정보처리기사 자격을 보유한 12년 경력의 기술팀장(PL) 투입.
- SCA(공급망 보안) 및 Fuzzing(취약점 탐지) 분야의 전담 엔지니어 팀 구성

사업 관리 역량
- 다년간의 KISA 유사 사업 참여를 통해 공공기관 행정 절차 및 품질 기준에 대한 높은 이해도 보유

준비된 기술: 생산 가용성을 최우선하는 '세밀한 점검'

검증된 리더십
- 무중단 점검 체계제조 현장의 운영 가용성 보장을 위해 에이전트 미설치(Agentless) 방식의 기술 적용
- 실시간 트래픽 분석을 통한 비인가 IP 및 서비스 탐지

정예 기술 조직
- 단순 점검을 넘어 SBOM(Software Bill of Materials) 분석 기술을 통한 제조 SW 및 오픈소스 잠재 위협 식별

사업 관리 역량
- 랜섬웨어 및 공급망 침투 등 최신 위협 동향을 반영한 시나리오 제공
- 사고 대응 시간을 평균 30~50% 단축할 수 있는 체감도 높은 훈련 수행

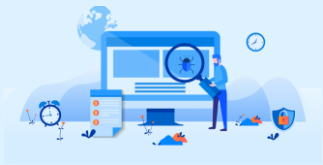
준비된 경험: 경남테크노파크와 KISA가 인정한 '검증된 파트너'

지역 특화 성과
- 2023년 경남테크노파크 스마트공장 보안 기술 테스트베드 구축 사업 성공적 수행
- 경남 지역 제조 인프라 및 특성에 대한 높은 현장 이해도 확보

광범위한 레퍼런스
- 자동차(LS오토모티브), 의료(KTL), 우주(KISA), 금융(현대카드) 등 보안 규제가 엄격한 산업군별 실적 보유

신뢰의 기반
- NSR(국가보안기술연구소) 패밀리 기업 및 KISA 정보보호 클러스터 육성 기업 선정
- 공공 분야 보안 사업의 엄격한 가이드라인과 기준 명확히 준수

소프트플로우(주)와 함께라면, 경남의 제조업은 보안의 불확실성을 걷어내고 더 안전하게 AX 시대를 향해 도약할 수 있습니다.



SOFTFLOW

Thank you!

SOFTFLOW

소프트플로우㈜

연락처 : (Tel) 070-7724-2752 / (E-mail) info@softflow.io

주　소 : (13449) 경기도 성남시 수정구 달래내로 46, A타워 8층 805호 (성남글로벌융합센터)