사이버 위기대응 모의훈련 및 보안점검

사 업 계 획 서

2026. 05. 27

소프트플로우(주)

<table>
<tr><td colspan="2" rowspan="4">주관기업</td><td>기 관 명</td><td>소프트플로우(주)</td><td>사업자등록번호</td><td>619-88-00971</td></tr>
<tr><td>주 소</td><td colspan="3">경기도 안양시 동안구 시민대로 401,
대륭테크노타운15차 1508호</td></tr>
<tr><td>홈페이지 주소</td><td colspan="3">https://www.softflow.io/</td></tr>
<tr><td>기업 성격</td><td colspan="3">중견기업( ), 중소기업(V), 기타( )</td></tr>
<tr><td rowspan="6">주관기업
책임자</td><td rowspan="3">총괄
책임자</td><td>성명</td><td>소범석</td><td>부서/직위</td><td>융합보안 사업본부/
대표 이사</td></tr>
<tr><td>전화</td><td>070-7724-2752</td><td>E-mail</td><td>bsso@softflow.io</td></tr>
<tr><td>휴대전화</td><td>010-6274-2752</td><td>팩스</td><td>-</td></tr>
<tr><td rowspan="3">실무
책임자</td><td>성명</td><td>김관식</td><td>부서/직위</td><td>융합보안기술팀/팀장</td></tr>
<tr><td>전화</td><td>-</td><td>E-mail</td><td>kwansik@softflow.io</td></tr>
<tr><td>휴대전화</td><td>010-2747-5355</td><td>팩스</td><td>-</td></tr>
</table>

관계 법령과 규정을 준수하면서 본 사업을 성실히 수행하고자 신청서를 제출합니다.

2026년 05월 27일

(주관기업) 소프트플로우: 소 범 석 (인)

(재)경남테크노파크 원장 귀하

목 차

별첨 A. 사이버 대응 모의훈련 시나리오 설계 체계

별첨 B. 사이버 대응 모의훈련 시나리오

별첨 C. MTTD/MTTR 등급별 목표수준(SLA) 정의서

부록 첨부 서류 목록 및 서약서

제1장. 수행기관 역량

1-1. 기관 기본 현황

기관명	소프트플로우㈜
설립일	2018년 02월 08일
기관 유형	■ 정보보호 전문서비스 기업 □ 정보보호 관련 기업 □ IT/SW 기업 □ 기타
대표자	소범석
주소 (경남 소재 여부)	경기도 안양시 동안구 시민대로 401, 대륭테크노타운15차 1508호 (■ 본사 □ 지사) 경상남도 창원시 의창구 차룡로48번길 44, R209호 공유-5-1 (□ 본사 ■ 지사)
임직원 수	총 8 명(정규직 8 명, 계약직 0 명)
주요 사업 분야	• 산업제어시스템(스마트공장) 이상징후 탐지 및 솔루션 연구 및 개발 • 산업제어시스템 보안 시험 방법론 연구 개발 및 보안 리빙랩 구축 • 산업제어시스템/IoT 보안 솔루션 구축 및 컨설팅 • 스마트공장 보안 취약점 분석 엔지니어링 서비스 • SW 공급망 솔루션
정보보호 전문서비스 기업 지정 여부	□ 지정 (지정번호:) ■ 미지정

1-2. 전문인력 현황

성명	직위/역할	주요 자격증	정보보호 경력 (년/주요 이력)	투입률(%)	경남 소재여부
소범석	대표 이사	-	14년 5개월	10%	■ 예 □ 아니오
김관식	책임	정보처리기사	12년 11개월	10%	■ 예 □ 아니오
권설예	선임	정보처리기사	7년 3개월	10%	■ 예 □ 아니오
송예준	주임	-	1년 5개월	10%	■ 예 □ 아니오

1-3. 유사 사업 수행 실적

사업명	발주기관	수행기간	계약금액 (백만원)	주요 수행내용 (제조업 여부)
우주 기업 보안취약점 점검 및 보안모델 고도화	KISA	2025.05 ~2025.12	52	■ 제조업 포함 □ 기타
SBOM 기반 공급망 보안 모델 구축 지원사업	KISA	2025.05 ~2025.12	271	□ 제조업 포함 ■ 기타
스마트공장 보안 취약점 점검 및 보안컨설팅	KISA	2025.05 ~2025.12	98	■ 제조업 포함 □ 기타
2025년 스마트공장 보안 테스트베드 유지보수	경남테크노파크	2025.04 ~2025.12	40	■ 제조업 포함 □ 기타
IoT 보안인증 SBOM 점검 도구 공급 및 기술지원	KISA	2024.12 ~2025.11	54	□ 제조업 포함 ■ 기타
우주 기업 보안 취약점 점검 및 보안 모델 개발 용역	KISA	2024.05 ~2024.12	175	■ 제조업 포함 □ 기타
스마트공장 보안취약점 점검 및 보안컨설팅	KISA	2024.05 ~2024.12	149	■ 제조업 포함 □ 기타
스마트공장 보안 기술 테스트베드 구축	경남테크노파크	2023.12 ~2024.01	459	■ 제조업 포함 □ 기타
스마트공장 보안취약점 점검 및 보안컨설팅	KISA	2023.05 ~2023.12	93	■ 제조업 포함 □ 기타
디지털 의료기기 보안성 시험 자동화 솔루션 개발	중소기업기술정보진흥원	2023.04 ~2025.03	299	□ 제조업 포함 ■ 기타
스마트공장 보안 취약점 점검 및 보안모델 실증	KISA	2022.05 ~2022.12	154	■ 제조업 포함 □ 기타
스마트공장 보안취약점 점검 및 보안 모델 고도화	KISA	2021.05 ~2021.12	90	■ 제조업 포함 □ 기타
울산지역 특화산업 정보보안 컨설팅 용역	울산정보산업진흥원	2020.09 ~2020.12	50	■ 제조업 포함 □ 기타

1-4. 보유 인증·등록 현황

No.	인증·등록명	인증기관	비고
1			

1-5. 대표 실적 상세 기술(최대 2건)

항 목	대표 실적① 상세 내용
발주기관·사업명	KISA / 스마트공장 보안취약점 점검 및 보안 컨설팅
수행 기간	2020.05 ~ 2025.12
주요 수행 내용	• 스마트공장 현장 방문 취약점 점검 및 보안컨설팅, 보안 교육 제공: 20개사 이상의 스마트공장 내·외부 보안 점검 및 보안 자문을 제공하고, OT 정보보호, OT 보안 실천 수칙, 보안점검 도구를 통한 기술지원 등 보안 교육을 제공 • 스마트공장 보안취약점 점검 및 결과 분석: OT/IT설비·인프라 등을 대상으로 스마트공장 보안취약점 점검 기준, 보안 체크리스트, 보안 모델을 활용해 취약점 점검을 수행하고, 점검 대상별 주요 보안 위협 요인 제시 • 스마트공장 보안 컨설팅 제공: 스마트공장 보안모델에서 제시하는 보안 요구사항을 활용하여, 관리적·물리적·기술적 보안컨설팅 제공 • 스마트공장 보안성시험 기술 지원: OT보안 보안점검도구, 스마트공장 주요 설비 및 데모 KiT 등 보안성 시험에 필요한 기술지원 및 매뉴얼 현장 교육 지원 • 시험결과서 작성 지원: 스마트공장/OT 분야 연구과제 보안 관련 정량적 시험 항목 수행가능 유무 판별, 보안성 시험 및 외부 설비 시험 결과서 작성 지원
사업 성과	• OT/IT 설비·인프라 별로 취약점 조치 및 개선안을 제시하여 56.49% 였던 전체 보안 수준을 86.71%로 향상 (최초 점검 대비 30.2% 향상) • 기존에 미흡했던 스마트공장 보안 지침 제·개정 지원 • 운영 및 인프라 시스템 및 OT 네트워크 보안 방안 수립 • 백업 및 복구 방안 수립
본 사업과의 연관성	• 지난 6년간 스마트공장 보안 점검 및 컨설팅 사업을 진행하며 직접 경험한 서로 다른 공공·제조 현장의 컨설팅 및 취약점 점검에 관한 데이터베이스를 보유하고 있음. • PM/PL 동일한 팀을 유지하고 있어 숙련된 경험을 보유하고 있음. 이를 기반으로 제조 현장에서 발생하는 고위험군의 취약점을 타겟팅한 실효성 있는 훈련 모델을 제시 가능 • 유사 사업에서 사용한 보안점검도구(Tenable OT Security, Defensics 등)와 모의훈련 경험을 기반으로 보안성시험 및 훈련 시의 적합한 가이드 및 지원 가능 • 6년간 진행한 컨설팅 및 교육 경험으로 본사업에 수요 기업에게 적합한 교육 및 훈련 가능. • 다양한 공공·제조 현장에서 진행한 컨설팅 데이터베이스를 기반으로 수요 기업의 환경에 적합한 맞춤형 교육 가능

항 목	대표 실적② 상세 내용
발주기관·사업명	KISA / SBOM 기반 공급망 보안 모델 구축 지원사업
수행 기간	2025.05 ~ 2025.12
주요 수행 내용	• SBOM 관리 체계 확립: SDLC에 적용 가능한 SBOM 수집・관리・활용 프로세스 수립 및 SBOM 자동화 도구・관리 플랫폼 구축 • 공급망 보안 수준 향상: SBOM을 활용한 취약점 관리, 라이선스 검증, 보안성 평가 절차 마련 및 오픈소스 활용 시의 보안 검증 체계 강화 • 규제 요구사항 준수: 국내외 법령(ISO 27701・27701, MDSAP 등) 및 사이버 보안 규제 대응, 표준과 정합성 확보
사업 성과	• 의료 SW 개발 기업에 SBOM 공급망 보안 모델 구축을 지원하여 FDA 사이버 보안 요구사항 SBOM 제출 항목 충족 • SBOM 저장소 접근제어 관리 시스템을 개발하여 기밀성과 무결성 및 안전 운영을 보장하기 위한 접근제어 관리 시스템 적용 • 식별된 Critical/High 취약점 100% 개선 지원 • ISO/IEC 27001・27701 보안인증 획득 지원
본 사업과의 연관성	• 본 사업의 공급망 공격 관련 - 공급망 보안 모델을 구축하고 지원한 경험이 존재. 이를 통해 공급망과 관련된 취약점을 탐지 및 관리하는 도구와 방법론에 대한 전문성과 실제 시연 및 활용 능력을 갖춤. - 공급망 보안 도구를 통한 컨설팅 경험을 기반으로 본 사업의 보안 점검 및 모의훈련 수행 시, 해당 도구 활용 가능 - 취약점 분석 경험을 바탕으로 수요 기업 내에 잠재한 취약점 개선에 적합한 가이드 및 해결 방안을 제시 가능

제2장. 사업 이해도 및 추진 방향

2-1. 사업 추진 배경 및 필요성 이해

구 분	당사 이해 내용
사이버 위협 환경 변화	**[환경 변화] 연결성(Connectivity) 확대에 따른 구조적 취약점 노출** • **보안 경계의 확장** - 기존의 '폐쇄형(Air-gap)' 환경이 IT/OT가 융합된 스마트공장 전환으로 인해 '개방형 초연결' 구조로 변화 • **접점의 다변화** - 클라우드 기반 관리, 원격 유지보수 채널, ERP/MES 연동 등 외부 노출 접점 확대로 인한 방어 경계의 모호성 증대 **[위협 변화] 공격 기법의 지능화 및 고도화** • **랜섬웨어 - 공격 목표의 변화: 공정의 가용성** - 기존) 단순 데이터 암호화를 통해 돈을 요구하는 방식으로 진행되었음. - 현재) 제조 공정의 가용성을 타격하여 비즈니스 중단을 유발하는 방식으로 진화 • **공급망 보안 – 신뢰 프로세스를 악용한 침투 경로의 확대** - 협력사 및 SW 도입과 같은 공급망을 통한 공격 사례 증가 - 사례 1: 협력사 우회 침투) 협력사를 1차 거점으로 확보한 후, 신뢰 관계를 이용해 내부 OT 망으로 공격 전이 및 확산 - 사례 2: SW 공급망 오염) 소프트웨어 빌드 및 배포 과정에 개입하여 오픈소스 취약점 및 악성 코드를 주입하는 공격 사례 급증
OT/IT 융합 환경 변화	**[환경 변화] 스마트공장 확산에 따른 제조업 디지털 전환의 본격화** • **정부 정책 기반의 산업 혁신** - 2014년 '제조업 혁신 3.0 전략'을 기점으로 스마트공장 보급 및 고도화 정책이 범정부 차원에서 추진되며 제조 현장의 디지털 전환이 가속화됨 • **개방형 네트워크 구조로의 전환** - 과거 독립적·폐쇄적(Air-Gap)으로 운영되던 생산 설비와 산업 제어 시스템(ICS)이 실시간 공정 모니터링 및 생산 효율 극대화를 위해 ERP, MES 등 IT 시스템과 통합된 개방형 구조로 변화함 • **IT-OT 데이터 통합** - 생산 현장의 PLC, SCADA 데이터가 상위 경영 정보 시스템과 실시간으로 연동되는 연결성 중심의 스마트 제조 환경 구축 **[보안 위협] 네트워크 개방 및 연결 증가에 따른 보안 위협 심화** • 사이버 공격 접점의 기하급수적 확대 - IT 시스템과의 연결성 증대 및 외부 유지보수 단말, 원격 관리 접점 등의 활용으로 인해 공격자가 침투할 수 있는 통로가 과거 대비 대폭 확대됨 - OT 환경보다 상대적으로 외부와의 접점이 많은 IT 환경의 취약점을 통해 IT 망 접근 후, OT 망으로 위협을 전이시키는 공격 방식이 주류를 이룸 • **사전 대응 체계 구축의 시급성** - 전통적인 방어체계만으로는 고도화된 위협 대응에 한계가 있으며, 사고 대응 시간(TTR)을 30~50% 단축시킬 수 있는 실전형 모의훈련 및 정밀 보안점검 통합 모델 도입이 절실한 시점임.

본 사업의 핵심 목적	• **핵심 목적: IT-OT 융합 제조 환경의 위기 대응 역량 내재화 및 지속 가능한 보안 자율 체계 구축** • **3대 핵심 목표:** ▶ **목표 1. [진단] IT-OT 융합 환경 리스크 식별 및 개선 로드맵 제공** - **IT-OT 통합 분석:** 제조업 디지털 전환 확산에 따른 공격 표면을 분석하여, 네트워트 접점, IT/OT 자산에 대한 취약점 식별 - **구조적 한계 극복:** 노후 자산(Legacy), 전담 인력 부재 등 현장의 제약 사항을 반영하여, 실행가능한 단계별 개선 로드맵을 수립 ▶ **목표 2. [대응] 실전형 모의훈련을 통한 사고 대응 골든타임 확보** - **고도화된 위협 대응:** 랜섬웨어 및 공급망 공격을 포함한 모의 훈련 시나리오를 적용해 사이버 위기 대응 훈련 수행 - **대응 시간 단축:** 훈련 + 점검 통합 모델을 통해 사이버 위기 대응 시간을 평균 30% 단축할 수 있는 현장 중심의 대응 가이드 제공 ▶ **목표 3. [체계] 지속적인 보안 이행력 제고** - **보안 역량 내재화:** 일회성 점검을 넘어 교육 및 사후관리를 통해 기업 스스로 위협을 관리할 수 있는 지속 가능한 보안 운영 체계 안착 - **자율 보안 이행 체계 구축**: 기업이 자체적인 보안점검을 상시 수행할 수 있도록 보안점검 체크리스트, 자체 점검 도구, 교육 콘텐츠 제공
정책적 부합성	본 사업의 성공적인 수행이 국가 및 지역 보안 정책의 실현으로 이어지도록 다음과 같은 정책적 부합성을 확보합니다 **1. 정부의『국가 사이버안보 전략』핵심 과제 이행** • 사이버 위협 대응 역량 강화 및 고도화 - 사고 후 복구 중심에서 벗어나 '훈련과 점검이 통합된 모델'을 제시하여, 사고 대응 역량과 지속적인 보안 이행력 제고 - 랜섬웨어 및 공급망 공격과 같은 사이버 공격에 대응하기 위해 실전형 시나리오 기반의 모의훈련 수행 **2. 관련 법령 및 공공 보안 가이드라인 준수** • 관련 법령 및 가이드를 통한 체계적 점검 프레임워크 수립 - IT/OT 통합 점검 프레임워크에 한국인터넷진흥원의 스마트공장 보안모델/스마트공장을 위한 최소 정보 보안 가이드라인 등 관련 보안 지침 적용 **3. 스마트공장 보안 내재화 실천** • 대응 역량 강화 및 보안 내재화를 통한 보안 강화 - 스마트공장 확산에 따른 산업제어시스템(ICS) 연결 증가 및 공격 표면 확대를 고려하여 제조 공정의 연속성을 보장하는 보안 내재화 정책 지원 - 지역 중소 스마트공장의 현실적 한계를 고려한 보안 로드맵 제시

2-2. 핵심 추진 전략

전략	전략명	주요 내용
전략1	유사사업 수행 경험 활용, 최적의 보안 모델 제시	• '20년 ~ '25년 울산정보산업진흥원, KISA 스마트공장 보안 사업 수행 활용 • KISA 스마트공장 보안 모델 기반 컨설팅 방법론 보유 • 스마트공장 보안취약점 점검, 보안모델 적용 컨설팅 등 기존 사업의 높은 이해를 바탕으로 모의훈련 및 보안점검 수행, 개선 가이드 및 교육 제공
전략2	OT/ICS 및 공급망 보안 전문인력 투입	• '20년 ~ '25년 울산정보산업진흥원, KISA 스마트공장 보안 사업 수행 인력 투입 • '25년 KISA SBOM 기반 공급망 보안 모델 구축 지원 사업 수행 인력 투입 • 스마트공장 보안 및 공급망 보안 사업 경험 인력 투입
전략3	AI 활용한 모의훈련 침투 방안 개발	• LLM을 활용하여 다수의 Proof of Concept 코드 개발 • Cyber Verification Program 등록 (보안 연구 목적으로 Claude 활용 권한 획득)
전략4	산업제어시스템 및 공급망 보안 전문 기술 적용	• 산업제어시스템 및 공급망 보안 시험 기술 및 보안 기술(모의 훈련 및 보안 점검) 적용 • 보안점검 도구와 결과 활용 경험을 기반으로 고도화된 스마트공장 보안 및 공급망 보안 실현
전략5	지속 가능한 보안 자립화를 위한 사후관리 및 교육 지원	• 단순 점검을 넘어 실무자·경영진 대상 맞춤형 대응 교육 및 취약점 개선 로드맵, 점검 체크리스트 제공 • 창원 지사 거점을 활용한 밀착형 사후관리 및 지속적인 제공

2-3. 단계별 추진 일정

수행 단계	5월	6월	7월	8월	9월	10월	11월	산출물	비고
① 사전 진단								- 보안수준 진단보고서 - 자산 목록표	
② 훈련 기획								- 훈련 시나리오 문서 - 훈련 운영계획서 - ROE 합의서 - 훈련 평가지표 정의서	
③ 모의훈련 운영								- 모의훈련 결과 보고서	
④ 보안점검								- 보안점검 체크리스트 - 진단보고서	
⑤ 결과 분석								- 종합 결과보고서 - 개선 가이드	
⑥ 교육								- 교육 교재 - 교육 결과보고서	
⑦ 사후관리								- 이행 점검 보고서 - 후속 개선안 - 자체점검 체크리스트	

- 사업 기간: 과업 착수일로부터 26년 10월 30일까지

제3장. 모의훈련 설계 역량 및 보안점검 방법론

3-1. 시나리오 설계 체계

기존 유사 사업을 통해 스마트공장을 대상으로 점검 프레임워크에 따른 보안점검 및 취약점 진단을 수행한 결과, 대부분의 스마트공장에서 다음과 같은 공통적인 보안 특성을 가지고 있는 것을 확인하였습니다.

구분	설명
전문인력 부족	• 보안 전담 인력 부재 • 보안 정책 및 가이드 부재
협력업체 의존도 높음	• MES 보안 요구사항 및 보안기능 부재 • MES 구축 기업의 보안 기술 적용 미비 • 협력업체 의존도 높음 (MES/서버 등 패스워드를 협력업체가 관리/공유/접근)
랜섬웨어/보안 유지보수 어려움	• 방화벽이 부재하거나, 랜섬웨어/악성코드 감염 경험 多 • 스마트공장 운영인력의 IT/보안 지식 부족 • 보안 관리 예산 부족
인공지능을 통한 공격 용이	• 공격 취약점 코드와 기법을 학습 • 인공지능을 통해 취약점 악용 스크립트 개발 가능 • 가용성 침해 공격 수행 용이

이러한 보안 특성을 고려하여 '별첨 A. 시나리오 설계 체계'에 따라 다음과 사이버 위기 대응 모의훈련 시나리오를 설계합니다.

시나리오 유형	주요 공격 기법	훈련 목표	적용 대상 기업 유형
랜섬웨어 침투	1. 침투 - Phishing (T1566) 2. 자산 식별 - File and Directory Discovery (T1083) 3. 데이터 암호화 모사 - Data Encrypted for Impact (T1486)	• 피싱 메일 및 취약점 유입 시 탐지 및 차단 역량 검증 • 임직원 보안 인식 검증 • 실시간 신고체계 가동성 검증	• 전 규모 • 현장직 및 사무직 등 IT 숙련도가 다양한 인력이 혼재된 환경
공급망 공격	1. 정보수집 - Supply Chain Compromise(T1195.002) 2. 개발 - AI를 통한 악용 스크립트 개발 2. 초기 침투 - Exploitation for Client Execution (T1203) 3. 목표 달성 - Data Staged (T1074.00) - Command and Scripting Interpreter	• SW 도입 전 사전 보안성 검토(CVE 스캔) 체계의 필요성 입증 • 실시간 탐지 및 대응 체계의 실효성 검증	• 중소/중견 • 협력사 전용 솔루션 활용이 많은 환경

	(T1059)		
내부자 위협	0. 개발 - 침투용 악성 파일 작성 1. 초기 침투 - Internal Spearphishing (T1566.002) 2. 기밀파일 접근 및 수집 - Data From Info Repositories (T0811) 3. 기밀 파일 유출 - Exfiltration Over Physical Medium (T1011)	• 도면/기술 문서 등 핵심 자산에 대한 접근 제어 필요성 제고 • 매체 제어 솔루션 및 대응 매뉴얼의 효용성 검증	• 첨단/핵심기술 제조 • 국가 핵심 기술 또는 고유 설계 자산을 보유한 R&D 중심 제조사
OT/ICS 공격	1. 사고 발생 상황 가정 - Data Destruction (T0809) 2. 상황 인식 - Alarm Suppression(T0801) 3. 대응조치 - Automated Response(T0804)	• 사고 인지 시, 현장 대응 매뉴얼 (망 분리/비상 가동)의 부서 간 공조 체계 실효성 확인	• 스마트 공장 • 자동화 생산 라인 및 PLC/SCADA 시스템을 운영하는 제조 시설 • IT망과 OT망의 접점이 존재하는 환경

모의훈련 시나리오 및 탐지/대응 기준에 대한 상세 내용은 '별첨 B. 모의훈련 시나리오'를 참고하여 주시기를 바랍니다.

3-2. 훈련 운영 방법론

운영 단계	세부 수행 방법
사전 조율·RoE 확정	**[주요 수행 방안]** **1. Whitelist 기반 자산 식별** - 훈련 영향도를 고려하여 침투 허용 자산과 절대 보호 자산(Whitelist)을 명확히 구분 및 격리 **2. 탐지/대응 판단기준 선정** - 로그 부재 상황을 고려하여 '인지 보고, 가용성 변화, 수동 대응조치' 등 구체적인 탐지/대응 판단기준 확립 **3. ROE 및 Kill-Switch 합의** - 훈련 시간 및 비상시 즉시 중단 절차 확정 **4. 모의훈련 시나리오 최적화** - 기 수립된 모의훈련 시나리오를 수요기업의 실제 환경(OT/IT)에 맞춰 세부 공격 경로 재구성 - 수요기업 요구사항에 따라 모의훈련 시나리오 선택 **[사용 도구]** • 모의훈련 수행 계획서 / 자산 목록표 / ROE 합의서

	/훈련 평가지표 정의서 **[담당자]** • (수요기업) 보안/인프라 담당자 (담당자 부재 시, 해당 사업을 담당하는 임직원)
킥오프 및 환경 구성	**[수행 방안]** **1. 착수 보고 및 시나리오 브리핑** - 전 참여자 대상 훈련 목적, 확정 시나리오, 공격 타임라인 상세 공유 **2. 임시 가이드 배포** - 대응 절차서가 없는 경우, 모의훈련의 대응 기준이 되는 '1차 대응 절차서' 및 비상 연락망 배포 **3. 공격 인프라 구축 및 안정성 설정** - 훈련용 공격 인프라의 IP/도메인을 방화벽에 Whitelist로 등록하여 원활한 훈련 수행 환경을 구축 **4. 모의훈련 환경 최종 검증** - 공격 인프라 통신 상태 및 대상 자산의 접근 제어 설정을 최종 점검 **[사용 도구]** • 가상화 플랫폼으로 구성한 공격 인프라 **[담당자]** • (수요기업) 실무책임자, 보안/인프라 담당자
실시간 이벤트 주입	**[수행 방안]** **1. 단계별 TTPs 실행** - 설계한 시나리오에 따라 '침투→수집->공격' 순차 수행 - 가용성 보호를 위해 비파괴적 시나리오 수행 - 이벤트 단계 별 주입 후, 수동/자동 시스템 상태 확인 **[사용 도구]** • 모의훈련을 위한 침투 도구 - Gophish, Kali Linux, Metasploit 등 **[담당자]** • (수행기업) 모의훈련 수행담당자 / (수요기업) 대응팀 및 임직원
대응 관찰 및 기록	**[수행 방안]** **1. 수동 타임라인 작성 및 병목 구간 식별** - 공격 주입 시점부터 방어자의 '인지·전파·조치' 각 단계의 타임라인을 기록 - 배포한 1차 대응 가이드에 따라 대응 시, 발생하는 지연 요소를 초 단위로 기록 **2. 가용자원 로그 수집** - 백신 검출 이력, 방화벽 허용/차단 기록, 훈련용 악성 파일의 로그 등 가용가능한 기본 로그 수집 **3. 담당자 인터뷰** - 임직원 인지 시점 및 담당자 보고 시점, 대응 시점 확인

	[사용 도구 및 인프라] • 훈련 상황 기록지 / 백신, 방화벽 로그 /인터뷰 시트 **[담당자]** • (수행기업) 모의훈련 수행담당자 / (수요기업) 보안 담당자, 대응팀
종료·디브리핑	**[수행 방안]** **1. 환경 원복** - 주입된 페이로드 및 훈련용 계정 삭제, 설정 원복 **2. KPI 산출** - 수집된 데이터를 바탕으로 KPI 산정식에 따라 MTTD, MTTR, 공격 탐지율, 대응 성공률 산정 **3. 훈련결과 공유 및 대응 가이드 개선** - 훈련 결과 분석 및 기술적 개선 방안(Best Practice) 제안 - 병목 현상을 해소한 대응 가이드 제공 **[사용 도구 및 인프라]** • Rollback 스크립트 / KPI 산정표 / 훈련결과 보고서 /개선 가이드 **[담당자]** • (수행기업) 모의훈련 실 담당자 / (수요기업) 담당자 및 전 인력

3-3. 훈련 안전성 보장 방안

본 모의훈련 시나리오는 가용성이 핵심인 제조업의 특성을 고려하여 '비파괴적 수행'을 대원칙으로 합니다.

훈련 중 발생가능한 시스템 부하 및 장애 리스크를 원천 차단하기 위해 다음과 같은 3단계 안전 보장 시스템을 적용합니다.

1. **실 환경 서비스 영향 최소화 (Technical Safeguards)**
   운영 중인 IT 인프라에 직접적인 위해를 가하지 않는 안전한 방법만을 사용하여 시스템 무결성 보장
   - **데이터 암호화 모사(Simulation)**
     - 실제 파일을 암호화하는 대신, 훈련용 더미 파일 생성 등을 통해 공격 행위만을 시뮬레이션하여 실제 데이터 손실 가능성을 배제
2. **OT 환경 특화 안전 조치**
   물리적 위험도가 높은 OT/ICS 환경은 기술적 타격 대신 '도상 훈련(Table-Top Exercise)' 모델을 채택하여 안전성과 실효성을 동시에 확보
   - **현장 무영향 도상 훈련(TTX) 수행**
     - 현장 설비의 가용성을 보장하기 위해 가상의 침해 시나리오를 바탕으로 현장 담당자가 대응 매뉴얼에 따라 의사결정을 내리는 시뮬레이션 방식으로 진행합니다.
     - 만약, 대응 매뉴얼이 없는 경우, 사전에 대응 매뉴얼 작성 및 교육하여 모의훈련에 활용할 수 있도록 지원합니다.

3. 비상 중지 프로토콜 (Emergency Stop & Rollback)

훈련 중 예기치 못한 이상 징후 발생 시 즉각적인 대응을 위한 'Safe-Switch' 프로토콜을 가동합니다.

- **즉시 중단 및 원복(Rollback)**

- 비상 상황 발생 시 즉시 전체 훈련 프로세스를 강제 종료하고, 훈련을 위해 생성된 모든 파일 및 프로세스를 제거하여 시스템을 훈련 전 상태로 즉각 복구합니다.

3-4. IT/OT 통합 점검 프레임워크

6년 간 유사사업 경험을 통해 KISA 스마트공장 보안모델을 기반으로 체계화된 스마트공장 보안점검 체크리스트를 지니고 있으며, 웹 애플리케이션에 대한 보안점검을 위해 'KISA 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드'를 기반으로 점검 항목을 구축합니다.
이를 통해 점검 영역별 IT/OT 통합 점검 프레임워크를 적은 시행착오로 구축하고 체계화된 보안점검을 지원합니다.

사전 인터뷰와 체크리스트를 통해 점검 영역별 보안 상황과 신청기업의 보안 요구사항을 파악하고 점검 항목과 도구를 활용하여 보안 취약점과 개선점을 지원합니다.

점검 영역	세부 점검 항목	적용 기준	활용 도구
네트워크	**[관리/물리]** • 망분리 및 접근 제한/관리 • 방화벽 정책 구축 및 검토 • 대외 네트워크 제한 및 암호화 • 외부 접속 제한/관리 **[기술]** • 네트워크 장비 취약점 진단 • 무선 네트워크 보안 점검 • 네트워크 트래픽 및 망분리 분석	**[관리/물리]** • 스마트공장 보안 모델 • 주요정보통신기반시설 기술적 취약점 분석·평가 상세 가이드 **[기술]** • CVSS: 취약점 심각도 점수	**[관리/물리]** • 보안점검 체크리스트 • 담당자 인터뷰 • 네트워크 장비 보안 설정 확인 **[기술]** • Nessus: 네트워크 취약점 스캐닝 도구 • NCA: 네트워크 트래픽 및 망분리 분석 • aircrack-ng: 무선 네트워크 침투 테스트 도구
서버·시스템	**[관리/물리]** • 관리자 권한 관리 및 암호화, 로그 관리 • 대외 연계 시의 보안 시스템 구성 • 호스트 장치나 제어 시스템에 대한 중요 알림 관리 **[기술]** • 불필요한 계정 및 권한 점검 • 시스템 설정 결함 • 백업 및 패치 관리	**[관리/물리]** • 스마트공장 보안 모델 • 주요정보통신기반시설 기술적 취약점 분석·평가 상세 가이드 **[기술]** • CVSS: 취약점 심각도 점수	**[관리/물리]** • 보안점검 체크리스트 • 서버/시스템 보안 설정 확인 **[기술]** • Tenable Security Center: 스마트공장 IT 자산 식별 및 자산 취약점 관리 • PC, 서버 자체 점검 도구

웹 애플리케이션	**[관리/물리]** • 관리자 계정 및 비밀번호 관리 • 웹 서비스의 권한・설정・파일 노출 및 불필요한 기능 • 패치 및 로그 관리 **[기술]** • 입력값 검증 및 인젝션 취약점 • 취약한 인증 및 세션 관리 • 권한 오류/유출로 인한 접근 허용 • 프로토콜 구현 견고성	**[관리/물리]** • 주요정보통신기반시설 기술적 취약점 분석・평가방법 상세 가이드 **[기술]** • OWASP Top 10: 가장 중요한 상위 10개의 웹 애플리케이션 보안 취약점 • CVSS: 취약점 심각도 점수	**[관리/물리]** • 보안점검 체크리스트 **[기술]** • Defensics: 프로토콜 기반 퍼징 테스트
OT/ICS	**[관리/물리]** • 물리적 인터페이스 • ICS 보안 로그 • ICS 사용자 및 기기 식별・인증 • ICS 기기 접근 통제 • 제어 로직, I/O 포인트 **[기술]** • 제어 로직/명령의 무결성 • 보안 이벤트 알림 체계 • 임베디드 장치 내의 취약점	**[관리/물리]** • 스마트공장 보안 모델 • 주요정보통신기반시설 기술적 취약점 분석・평가 상세 가이드 **[기술]** • CVSS: 취약점 심각도 점수	**[관리/물리]** • 보안점검 체크리스트 **[기술]** • Tenable OT Security: OT 자산 자동 식별 및 실시간 위협 모니터링
보안관리 체계	**[관리/물리]** • 보안 조직 및 규정 • 매체제어 및 접근권한 관리 • 시스템 운영 보안 • 침해사고 관리 체계 • 개인정보 보호	**[관리/물리]** • 스마트공장 보안 모델 • 주요정보통신기반시설 기술적 취약점 분석・평가 상세 가이드	**[관리/물리]** • 보안점검 체크리스트 • 담당자 심층 인터뷰 • 보안 규정 확인

3-5. 취약점 분류 및 개선 권고 방식

사전 인터뷰에서 확인한 보안 요구사항과 점검 도구의 진단 결과를 기반으로 조치 우선순위와 취약점 등급 그리고 등급별 조치 기한을 산정합니다.

이러한 취약점 등급은 도구가 식별한 취약점 점수를 기반으로 산정하며, 취약점 점수와 공격 시, 위험도를 고려하여 등급을 산정합니다. 이후, 분석된 취약점의 중요한 이슈 사항과 재발 방지를 위한 개선 가이드를 담당자에게 제공합니다.

등급	판단 기준	조치 기한	대응 방향
긴급(Critical)	• 진단도구 결과: - 취약점 등급: Critical - CVSS 점수: 9 ~ 10 • 사전 인터뷰로 파악한 중요 점검 항목 중 데이터 유출 및 공정 중단 위험이 존재하는 취약점	• 권장: 24시간 이내 • 최대: 1주 이내	• **가용성 기반의 즉각 대응 및 위협 차단**: 가용성에 영향을 주지 않는 범위 내에서 보안 패치 및 공격 경로 차단
높음(High)	• 진단도구 결과: - 취약점 등급: High - CVSS 점수: 7.0 ~ 8.9	• 권장: 1주 이내 • 최대: 2주 이내	• **보안 설정 및 물리적 방어 강화**: 자산별 보안 설정 강화 및 보안 접점에 대한 물리적 접근 통제 강화
보통(Medium)	• 진단도구 결과: - 취약점 등급: Medium - CVSS 점수: 4.0 ~ 6.9	• 권장: 2주 이내 • 최대: 30일 이내	• **정책 고도화 및 탐지 강화**: 현장 특성을 반영한 이상 징후 대응 가이드 고도화 및 접근 통제 절차 강화
낮음(Low)	• 진단도구 결과: - 취약점 등급: Low - CVSS 점수: 0.1 ~ 3.9	• 권장: 3주 이내 • 최대: 60일 이내	• **표준 보안 관리 및 상시 점검 체계**: 주기적으로 보안 점검 프로세스 실행 및 보안 설정 표준 가이드라인 배포

3-6 모의 훈련 및 스마트공장 보안 점검 강화 방안

항목	내용
수요기업별 차별화된 모의훈련 설계	• 기초형(중소제조): 피싱 메일을 통한 랜섬웨어 감염 및 공정 중단 대응 중심. • 고도화형(중견/대형): IT/OT 접점 취약점을 통한 ICS(산업제어시스템) 침투 및 프로토콜 변조 대응. • 핵심기술형(R&D): 내부자에 의한 설계 도면 및 핵심 기술 유출 차단 시나리오 적용.

모의해킹 시나리오 유형화 및 체계적 설계	• 4대 공격 표면(Attack Surface) 기반 유형 분류 - 외부 접점형: VPN 및 외부 유지보수 채널 취약점 분석. - 내부 확산형: IT 망 침투 후 OT 망으로의 수평 이동. - OT 특화형: HMI 및 PLC 변조 공격 점검. - 공급망 공격형: SW 업데이트 서버 오염 및 배포 패키지 내 악성 코드 주입 모사. • 표준 프레임워크 매핑: 모든 시나리오를 MITRE ATT&CK 기법(TTPs)과 매핑하여 공격 단계별 가시성 확보.
효율적 인력 운영 및 3회 이행점검 보완 계획	• 거점 활용: 경남 지사를 전담 대응 센터로 지정하여 현장 투입 및 사후 관리 효율 극대화. • 단계별 이행점검 프로세스 효율화 - 1차(현장): 고위험 취약점 즉각 조치 및 기술 자문. - 2차(비대면): 자동화 스크립트를 활용한 원격 조치 결과 확인 및 안정성 모니터링. - 3차(최종): 전수 재점검을 통한 100% 조치 여부 확정 및 정량적 성과 지표 산출.
상세 IT/OT 통합 점검 프레임워크	• 5단계 계층형 점검 구조 수립 - 관리/물리 계층: 보안 규정 및 현장 출입 통제 등 거버넌스 점검. - 네트워크 계층: IT-OT 망분리, 방화벽 정책, 무선 보안 점검. - 시스템 계층: 서버/단말 OS 취약점 및 불필요 서비스 분석. - 제어(OT) 계층: PLC/HMI 가용성 및 산업 프로토콜 견고성. - 공급망 계층: SBOM 기반 오픈소스 취약점 및 라이선스 위험 분석.
OT 보안 점검 비중 확대 실행	• 점검 항목 조정: KISA 스마트공장 보안 모델을 기반으로 OT 특화 항목을 전체의 50% 수준으로 상향. • 특화 도구 투입: Tenable OT Security, Defensics 등 산업 제어 시스템 전용 점검 도구 활용 강화.

제4장. 결과 활용성

4-1. 결과 분석 지표 및 방법

분석 지표(KPI)	측정 방법	활용 방안
초기 탐지 시간(MTTD)	• 이벤트 발생 시점(T^0)부터 탐지/신고 시점(T^1)까지의 소요 시간 • $MTTD = T^1 - T^0$	• 인적 신고망 및 전파 체계의 병목 구간을 식별 • 탐지 프로세스 최적화 (보안 솔루션 도입, 탐지/보고 체계)
대응 완료 시간(MTTR)	• 탐지/신고 시점(T^1)부터 대응 완료 시점(T^2)까지의 소요 시간 • $MTTR = T^2 - T^1$	• 대응 지연 구간을 식별하여 대응 프로세스 최적화
공격 탐지율(DR)	• 시나리오 유형 내 전체 이벤트 개수(D^0)에 대한 탐지 성공 개수(D^1)의 비율 • $DR = (D^1 \div D^0) \times 100$	• 솔루션 및 인적 탐지 역량 정량화 • 보안 가시성 사각지대 식별 • 관리/기술 보완대책 수립을 위한 객관적 지표로 활용
대응 성공률(RR)	• 시나리오 유형 내 전체 이벤트 개수(R^0)에 대한 대응 성공 개수(R^1)의 비율 • $RR = (R^1 \div R^0) \times 100$	• 침해사고 대응 숙련도에 대한 정량적 평가 • 실질적인 대응 체계 보완을 위한 지표로 활용
조직 성숙도 점수(OS)	• 점검 프레임워크의 영역별 이행률에 대한 평균 • $OS = (\sum_{i=1}^{5} 영역별이행률_i) \div 5$	• 전사 보안역량 진단 • 보안 거버넌스 강화 및 개선 로드맵 수립의 기초지표로 활용
기타 (시간 등급 수준)	• 탐지/대응 시간을 배점 기준에 따라 점수화한 평균 • $TS = (\frac{MTTD_{score} + MTTR_{score}}{2})$	• MTTD/MTTR 등급별 목표 수준(SLA) 정의서를 기반으로 목표 도달 여부 정략적 평가 • 사이버 위기 대응 수준의 상향 평준화 관리 지표 활용
기타 (종합 보안 지수)	• 전체 KPI를 기반으로 전반적인 종합 보안 점수 산정 • $TSI = \frac{TS + OS + DR + RR}{4}$	• 단일 지표로 전반적인 보안 수준 관리

- 탐지/대응 시간에 대한 상세한 시간별 등급 수준은 '별첨 C. MTTD/MTTR 등급별 목표수준(SLA) 정의서'를 참고하여 주시기를 바랍니다.

4-2. 개선 로드맵

구 분	개선 계획 내용
단기(1~3개월)	• 목표: 즉각 대응 및 위협 제거 • 조치 기준 - 취약점 및 탐지/대응 시간 등급: Critical/High • 세부 개선 방안 - 네트워크 기본 패스워드 변경 등 보안설정 가이드를 통해 자산별 보안설정 최적화 - 랜섬웨어 감염 대응을 위한 긴급 대응 가이드 수립 - 물리적 보안 접점 강화를 위한 물리적 포트락 등 물리적 접점 보안 조치 가이드
중기(3~6개월)	• 개선 목표: 보안 정책 개선 및 고도화 • 조치 기준 - 취약점 및 탐지/대응 시간 등급: Medium • 세부 개선 방안: - OT 환경 특화 이상징후 대응 가이드 - 모의훈련 및 진단 결과 기반 실무 중심의 보안 인식 제고 교육
장기(6개월~)	• 개선 목표: 자율 보안 체계 내재화 • 조치 기준 - 취약점 및 탐지/대응 시간 등급: Low • 세부 개선 방안: - 자체 보안점검 체크리스트, 교육자료를 통한 자율 보안 체계 정착 - 안전한 공급망 수립을 위한 공급망 보안 체크리스트 제공

4-3. 종합 결과보고서 구성

[보고서 목차 구성(안)]

본 보고서는 정량적 지표와 정성적 분석이 결합된 총 5장의 구성으로 도출됩니다.

요약문

1. 과업의 제목
2. 연구의 목적 및 중요성
3. 연구의 내용 및 범위
4. 모의훈련 수행 및 개선 결과
5. IT/OT 통합 점검 수행 및 개선 결과
6. 종합 보안 지수(TSI)를 활용한 전체 통합 점검 결과

1장. 개요

1절 사업 배경

2절 사업의 범위 및 구성

2장. 사이버 위기대응 모의훈련 수행

1절 사이버 위기대응 모의훈련 시나리오

2절 사이버 위기대응 모의훈련 시나리오별 상세 수행 절차

3절 훈련 시나리오 별 수행 결과

- 대응 프로세스 숙련도 및 부서 간 공조 체계(IT-OT) 평가 결과

4절 수행 결과에 따른 정량적 지표 도출 및 점수 산정

(MTTD, MTTR, 공격 탐지율, 대응 성공률)
3장. IT/OT 통합 보안점검 및 취약점 진단
1절 IT/OT 통합 점검 프레임워크 개요
- 점검 항목, 항목별 점검 방안, 점검 대상
2절 점검 프레임워크 기반 진단 결과
3절 취약점 분류 및 위험도 등급(High/Medium/Low) 산정
4장 종합 개선 로드맵
1절 단기·중장기 보안 강화 로드맵 제시
2절 맞춤형 보안 대책 및 솔루션 도입 가이드
5장. 교육 및 사후관리 계획
1절 대상별(경영진, 실무자, 현장직) 보안 교육 수행 결과 및 효과 검증
2절 지속적인 보안 자립화를 위한 사후 지원 계획 방안

[보고서 작성 방식]

1. 요약 중심 (경영진 및 의사결정용)

보고서의 전반부와 마무리 단계에 적용하며, KPI를 통한 정량적 성과 지표와 시각화 위주로 구성

- 해당 항목: 요약문(TSI 지수, 핵심 성과), 교육 결과(통계/만족도)
- 작성 핵심:
  - 가시성: 보안 수준의 '전/후 변화'를 한눈에 파악하도록 차트와 그래프(레이더 차트 등) 활용
  - 정량화: 점검 전/후의 보안 수준을 '종합 보안 지수(TSI)'로 변환하여 정량적 지표 제시
  - 간결성: 핵심 성과 위주로 기술하여 세부 내용을 읽지 않아도 결론 도출이 가능하도록 구성.

2. 세부 내용 중심 (실무진 및 기술 이행용)

보고서의 본문과 개선 계획에 적용하며, 개선 방안을 상세히 기술

- 해당 항목: 모의훈련 수행, IT/OT 취약점 진단, 종합 로드맵, 사후 지원 프로세스
- 작성 핵심:
  - 기술적 구체성: 공격 기법(TTPs), 수행 결과, 탐지/대응 기준 및 분석 결과 등 수행한 내용을 상세 기술
  - 인과관계 분석: 취약점이 비즈니스(공장 가동)에 미치는 영향과 병목 구간의 원인 분석
  - 개선 가이드: 단계별 이행 방법에 대한 요구 규격 등 상세 수행방안에 대한 가이드 제공

4-4. 우수사례 발굴 전략

단계	내용	기대 결과물
후보 발굴	**[후보 기업 선정 기준]** • 컨설팅 및 점검 결과를 기반으로 수요기업 중 우수사례에 해당하는 후보 기업 3개사 선정 • KPI 지표의 개선 결과를 기준으로 정량 평가 수행 - 종합 보안 지수(TSI)가 80점 이상인 기업 선정	• 후보기업 선정 보고서
심층 분석	**[우수사례 기업 선정]** • KPI 지표별 개선 전·후 측정 결과를 비교하여 후보 기업 중 1개사 선정 - 종합 보안 지수(TSI) 개선율을 산출하여 개선 효과가 가장 큰 기업을 선정 - 개선율이 동일한 경우 대응 완료 시간(MTTR) 단축 폭을 기준으로 최종 선정 **[성과 측정 내용]** • KPI 지표별 개선 전·후 측정 결과 비교 • 내부 보안 정책, 대응 절차 등 개선 사항 비교	• 성과 측정 분석서 • 보안 개선 결과 보고서
콘텐츠 제작	**[성공 모델 상세 기술]** • 선정된 사례를 기반으로 보안 개선 성과 정리 - KPI 기반 개선 결과 및 주요 지표 변화 내용 정리 - 보안 정책 및 내부 대응 체계 개선 내용 정리 • 범용성 있는 보안 점검 항목 및 개선 방안 도출 - 주요 보안 점검 항목 분석 - 다양한 환경에서 활용 가능한 적용 방안 제시 **[홍보 콘텐츠]** • 주관기관 협의를 통해 홍보콘텐츠 구성 및 방향 설정 • 우수사례 기반 보안 개선 성과 및 주요 대응 방안 정리 • 주요 보안 취약점 항목 개선 사례 중심 콘텐츠 구성	• 성과 보고서 • 홍보콘텐츠
최종 발표	**[결과 공유]** • 주관기관 협의를 통해 사례 공유회 개최 및 사업 성과 발표 • 우수사례 선정 결과 및 주요 보안 개선 성과 공유 **[홍보 방안]** • 우수사례 홍보콘텐츠를 주관기관에 제공 • 주관기관 공지·게시판 등을 활용하여 성과 확산 지원	• 우수사례 성과확산

제5장. 교육 및 확산

5-1. 대상별 교육 프로그램 구성

사이버 침해사고 발생 시 신속한 의사결정과 공정 가용성 확보를 위해 조직 내 각 구성원 간의 역할과 책임을 명확하게 하는 것이 신속한 보안 대응에 무엇보다 중요합니다.

교육 프로그램 수립 전, 구성원별 역할 및 책임을 우선적으로 도출합니다.

구성원	핵심 역할 및 책임
경영진·임원	• **보안 거버넌스 최종 의사결정**: 정보보호 관리체계(ISMS) 수립 및 운영 전반에 대한 의사결정권 행사 • **비즈니스 연속성 자원 할당**: 주요 침해사고 보고 수신 시 경영 리스크 판단 및 복구를 위한 예산·인력 등 자원 트입 최종 결정
보안 담당자	• **관리체계 및 보고 라인 수립**: 전사 보안 정책 수립, 경영진 대상 주요 보안 성과 및 리스크 정기 보고 • **대응 컨트롤 타워**: 침해 사고 발생 시 유관(OT/IT) 부서 협업 주도 및 대외 대응 총괄
IT 운영 실무자	• **인프라 자산 식별 및 가시성 확보**: IT/OT 통합 환경 내 자산 식별과 비인가 접근 통제를 통한 인프라 보안 무결성 유지 • **기술적 보호 조치 이행**: 서버·네트워크 보안 설정 적용 및 최신 보안 패치 관리 등 기술적 취약점 조치 실무 수행
OT 현장 담당자	• **가용성 최우선 관리**: 제어 설비(PLC, HMI 등)의 가동 중단 최소화를 위한 현장 보안 운영 • **현장 비상 대응 및 보고**: 이상 징후 발생 시 즉각적인 보고 절차 가동 및 가용성 기반의 설비별 선별적 격리/복구 수행

이러한 구성원 간의 역할과 책임을 고려하여 교육 형태와 내용을 구성합니다.

교육 내용은 참가 기업의 점검 결과 및 내부 환경(시스템 구조, 현장 및 운영 상황 등)을 반영하여 실제 운영에 적용 가능한 맞춤형 교육으로 구성합니다.

이후, 자체 보안 교육을 수행할 수 있도록 교육 자료를 제공합니다.

교육 대상	교육 형태	주요 교육 내용	기대 효과	시간/횟수
경영진·임원	온라인/오프라인 교육	최근 사이버 보안 위협 동향	최신 위협 인지 및 경영 리스크 인식 강화	30분 / 2회
		보안 거버넌스 개념 및 필요성	조직 차원의 보안 관리 필요성 이해	
		경영진 역할 및 책임	보안 의사결정 및 책임 범위 명확화	
		보안 거버넌스 수립 방향	보안 정책 및 관리체계 수립 역량 확보	
보안 담당자	온라인/오프라인 교육	주요 공격 기법 및 침해사고 유형	공격 유형별 위협 분석 및 대응 이해도 향상	1시간 / 2회
		침해사고 예방	취약점 기반 사전 예방 및 보안 관리 역량 강화	
		대응 절차 및 유형별 대응 방안	사고 대응 절차 숙지 및 실무 대응 능력 향상	

IT 운영 실무자	온라인/ 오프라인 교육	IT 인프라 보안 관리 개요	보안 관리 기준 및 운영 필요성 이해	30분 / 2회
		주요 보안 관리 영역 및 항목	핵심 보안 설정 및 관리 대상 식별 능력 확보	
		보안 설정 점검 및 취약 사례	취약 설정 식별 및 점검 역량 강화	
		보안 운영 관리 방법	정기 점검 및 지속적 보안 운영 능력 확보	
OT 현장 담당자	온라인/ 오프라인 교육	OT 환경 주요 침해 사고 및 영향	현장 보안 위협 인지 및 사고 영향 이해	30분 / 2회
		사고 대응 및 탐지	이상 징후 식별 및 초기 대응 능력 확보	
		사후 관리 및 재발 방지	복구 지원 및 재발 방지 참여 역량 강화	

5-2. 교육 효과 검증 방안

검증 방법	세부 내용
사전·사후 평가	**[검증 방법]** • 대상별 맞춤형 평가: 교육 전/후 동일한 난이도의 대상별 맞춤형 보안 지식 테스트 수행 **[검증 지표]** • 목표 점수 도달률: 현장 인력 대다수가 필수적으로 알아야할 보안 수칙을 숙지한 비율 • (80점 이상 획득한 인원) ÷ (전체 응시자 수)
실습 과제 수행	**[검증 방법]** • 보안 스크립트: 제공하는 점검 스크립트(PC, MES)를 활용하여 보안 점검을 실행하여 취약점 탐지 및 조치 진행 **[검증 지표]** • 취약점 조치 이행률: 탐지된 취약점 대비 실제 조치를 실행하여 해결된 비율 • (조치된 취약점 수) ÷ (스크립트를 동작하여 발견한 취약점 수)
현업 적용 추적 조사	**[검증 방법]** • 주기적 자가 점검 체크리스트 이행: 사업 종료 전까지 주기적으로 자가 점검 체크리스트 작성하여 기록하고 점검 과정에서 탐지된 취약점 조치 결과를 작성 **[검증 지표]** • 주기적 점검 이행률: 주기적으로 자가 점검을 실행한 비율 • (정해진 주에 실행된 점검 수) ÷ (계획된 점검 수)
교육 결과보고서 구성	**[검증 방법]** • 만족도 조사/설문조사: 교육 내용에 대한 만족도 및 설문조사를 통해 의견을 수집한 뒤 교육자료 개선 조치를 수행한 후 개선된 교육자료를 통해 사후 지원을 수행 **[검증 지표]** • 교육 만족도 조사

제6장. 기대효과 및 사후관리 계획

6-1. 정량적 기대효과

성과 지표	목표치	달성 방안
침해사고 대응 시간 단축	20% 이상 단축	• **(가이드 개선)** 병목 현상을 해소할 수 있도록 현장 맞춤형 '침해사고 대응 가이드' 개선 • **(이행 점검)** 개선된 대응 가이드 기반 이행 점검 수행 • **(효과 검증)** 이행 점검 결과 분석 후, 20% 이상 단축 여부 확인
취약점 해소율	30% 이상 향상	• **(정밀 진단)** 통합 점검 체계와 보안 도구를 활용하여 생산 설비 및 관리 시스템의 기술적·관리적 보안 약점 전수 식별 • **(이행 지원)** 취약점 분류 및 개선 권고에 따라 수행사가 직접 조치 가이드를 제공하고 현장 조치 이행 여부를 실시간 지원 • **(해소율 확인)** 3차에 걸친 이행 점검 결과를 분석하여 사업 초기 대비 고위험 취약점의 30% 이상 해소 및 안전성 확보
탐지율 개선	20% 이상 향상	• **(탐지율 향상)** 기술적 탐지 한계를 보완하기 위해 훈련 시 실무자가 이상 징후를 식별하고 보고하는 위협 탐지 프로세스 수립 • **(탐지력 검증)** 후속 훈련 시 로그 기록 및 인지 보고 비율을 분석하여 실질적인 위협 탐지 성공률 20% 이상 상향 입증
교육 만족도	평균 90점 이상	• **(교안 최적화)** 도구 점검과 모의훈련에서 결과를 반영하여 교육자료 최적화 • **(현장 눈높이 교육)** '랜섬웨어 대응 5계명', '사고 대응 10계명' 등 실무 중심의 핵심 수칙 전달 • **(만족도 평가)** 교육 전/후 설문 조사 결과를 분석하여 목표치 달성 확인
기타(종합 보안 지수)	20점 이상 향상	• **(성숙도 이행)** 식별된 약점들에 대한 단기 개선 과제를 사업 기간 내 집중 수행 • **(성숙도 확인)** 사업 종료 시점의 지수를 KPI에 따라 재산출하여 목표치 달성 확인

6-2. 사후관리 계획

사후관리 항목	세부 계획
이행점검1차	• 시기: 개선 로드맵 수립 직후 (사업 기간 내) • 방법 - (조치 현황 파악) 점검 프레임워크를 통해 도출된 취약점별 개선 권고 사항의 조치 시작 여부 확인 및 기술 자문 - (가이드 적합성 검토) 제공된 개선 가이드가 현장 설비 운영에 간섭을 주지 않는지 실무자 면담을 통한 확인 • 담당자 - 수행기업의 실무 담당자 / 현장 관리자
이행점검2차	• 시기: 1차 점검 1개월 이내 • 방법 - (미조치 보완) 1차 점검 시 미진했던 항목에 대한 집중 기술 가이드 제공 - (안정성 모니터링) 보안 조치 적용 후 생산 설비 가동에 이상 징후가 없는지 상시 점검 및 피드백 반영 • 담당자 - 수행기업의 실무 담당자 / 현장 관리자
이행점검3차	• 시기: 2차 점검 후, 1개월 이내 • 방법 - (최종 전수 점검) 점검 도구 및 프레임워크를 재가동하여 고위험 취약점의 100% 해소 여부 최종 확정 - (결과 보고) 최종 조치 현황을 정량화하여 성과 지표(취약점 해소율) 도출 • 담당자 - 수행기업의 실무 담당자 / 현장 관리자
후속 보완 훈련	• 시기: 3차 점검을 통해 대응 가이드 배포 후, 1개월 이내 • 방법 - (실효성 검증) 개선된 '대응 가이드'를 적용하여 2차 모의훈련을 실시, 1차 대비 위협 탐지율(DR) 및 대응 시간 개선 폭 측정 - (프로세스 보완) 훈련 중 발생한 예외 상황을 반영하여 현장 맞춤형 대응 절차 최종 최적화 • 담당자 - 수요기업 전 직원 / 수행기업의 실무 담당자
담당자 지원 체계	• 시기: 사업기간 동안 상시 • 방법 - 실시간 기술 지원 및 자문 창구 운영 - (보안 자문 지원) 전용 메신저 및 유선을 활용한 보안 이슈 실시간 Q&A 및 기술 자문 채널 운영 • 담당자 - 수행기업의 총괄책임자, 실무책임자

■ 별첨 A. 사이버 대응 모의훈련 시나리오 설계 체계

1단계: 인터뷰/점검도구 기반 정보 수집

훈련 시나리오의 현실감을 높이기 위해 대상 조직 시스템에 대한 사전 정보를 수집합니다.

▶ **시나리오별 정보 수집**

시나리오	수집 대상
랜섬웨어	• 임직원 메일, 조직도, 업무 시스템 정보
공급망 공격	• 내부 소프트웨어 자산 목록, 취약점 정보
내부자 위협	• 공유 폴더 구조, 파일 접근 권한
OT/ICS 공격	• 현장 장비 구성도, 네트워크 토폴로지

2단계: AI 기반 침투 스크립트 작성

수집된 정보를 바탕으로 AI를 활용하여 피싱 콘텐츠 및 취약성 악용 스크립트를 작성합니다.

▶ **시나리오별 AI 활용 방안**

시나리오	AI 활용 방안
랜섬웨어	• 피싱 메일 본문, 첨부파일 위장 유형 (인사발령·보안공지·택배 등), 클릭 유도 랜딩 페이지
공급망 공격	• 내부 침투를 위한 취약점 악용 코드 • (ProofOfConcept코드 작성)
내부자 위협	• 내부 공유 폴더 배포용 미끼 파일 설명, 숨김 속성 로그 생성 시나리오
OT/ICS 공격	• 사고 발생 상황 설명 문서, 도상훈련용 진행 스크립트

3단계: MITRE ATT&CK 프레임워크 기반 단계별 공격 기법 정의

각 시나리오의 공격 단계별로 MITRE ATT&CK 기법(TTP)을 매핑하고, 훈련에서 모사할 행위와 탐지·대응 포인트를 정의합니다.

MITRE ATT&CK 프레임워크 개요

MITRE ATT&CK은 실제 공격자의 전술(Tactics)·기법(Techniques)·절차(Procedures)를 분류한 글로벌 표준 프레임워크입니다. 각 기법은 고유ID(T번호)로 식별되며, 훈련 시나리오와 매핑함으로써 현실적인 위협 모사와 체계적인 탐지·대응 검증이 가능합니다.

시나리오 유형	주요 TTP (기법 예시)
랜섬웨어 침투	• 단계: 초기침투 → 실행 → 암호화 모사 • 기법: T1566 → T1204 → T1486 • 행위: 피싱 → 악성파일 실행 → 데이터 암호화
공급망 공격	• 단계: 정보수집 → 내부침투 → 목표 달성 • 기법: T1195 → T1203 → T1059 • 행위: 취약점 식별 → 악용코드 실행 및 침투 → 유출
내부자 위협	• 단계: 초기침투 → 실행 → 유출 모사 • 기법: T1566 → T0811 → T1011 • 행위: 미끼파일 유포 → 열람 확인 → 유출
OT/ICS 공격	• 단계: 사고발생 → 상황인지 → 대응조치 • 기법: T0809 → T0801 → T0804 • 행위: 사고 상황 제시 → 비정상 동작 상황 제시 →대응

■ 별첨 B. 사이버 대응 모의훈련 시나리오

1. 랜섬웨어 공격

A. 모의훈련 시나리오

- 훈련 목적: 피싱 메일에 대한 탐지 및 대응력 확인

훈련 단계	공격 기법 (MITRE ATT&CK)	훈련 내용
1. 초기 침투	Phishing (T1566)	임직원에게 훈련용 피싱 메일을 발송하여 첨부파일 실행 또는 악성 링크 클릭을 유도합니다.
2. 실행	User Execution (T1204)	첨부파일 실행 시 실제 암호화 로직 대신, 배경화면을 경고 이미지로 변경하거나 훈련 안내 팝업을 띄웁니다.
3. 암호화 모사	Data Encrypted for Impact (T1486)	실제 파일을 암호화하지 않고, 바탕화면에 더미 파일(.lock 확장자)을 생성하고, 이에 대한 대응 방안을 확인합니다.

B. 탐지 및 대응 기준

훈련 단계	탐지 기준	대응 기준
1. 정보 수집	- 이메일 보안 솔루션을 통한 피싱 메일 및 악성 링크 사전 탐지 - 사내 신고 절차를 통한 사용자의 의심 메일 자발적 제보	- 이메일 보안 솔루션을 통한 피싱 메일 수신 즉시 차단 - 방화벽 및 백신을 이용한 악성 스크립트 실행 차단
2. 실행	- 보안 솔루션을 통한 비인가 프로세스(훈련 팝업 실행 등) 실행 탐지 - 시스템 내 비정상적인 변경 행위 포착	- 침입 및 실행이 확인된 즉시 해당 악성 프로세스 강제 종료 - 보안 솔루션을 통한 실행 자동 차단
3. 암호화 모사	- 인가되지 않은 폴더 생성 인지 및 신고	- 보고 후, 단말 네트워크 즉시 차단 - 생성된 비인가 파일 삭제

2. 공급망 공격

A. 모의훈련 시나리오

- 훈련 목적: SW 도입 시, 위협 전이 사전 대응력 확인

훈련 단계	공격 기법 (MITRE ATT&CK)	훈련 내용
1. 자산 식별	Software Discovery (T1566), Supply Chain Compromise(T1195.002)	구성요소 분석 도구를 통해 시스템 내 자산(소프트웨어)과 자산이 지닌 취약점을 식별합니다.
2. 침투	Exploitation for Client Execution (T1203)	자산이 지닌 취약점을 이용하여 내부 환경에 침투합니다.
3. 데이터 탈취	Data Staged (T1074.001) Command and Scripting Interpreter (T1059)	/tmp 등 권한 제약이 적은 폴더에 숨김 속성 폴더를 생성하고, 중요 파일로 모사한 더미 데이터를 압축하여 저장.

B. 이벤트 단계별 탐지 및 대응 기준

훈련 단계	탐지 기준	대응 기준
1. 자산 식별	- 도입 소프트웨어 보안 공지 혹은 분석 도구를 통해 자산 취약점 식별	- 취약 소프트웨어의 버전 업데이트 이행
2. 침투	- 인가되지 않은 프로세스 실행 탐지	- 침입이 확인된 즉시 해당 프로세스 종료
3. 데이터 탈취	- 인가되지 않은 폴더 생성 인지 및 신고	- 보고 후, 네트워크 차단 및 비인가 폴더 수집 및 삭제

3. 내부자 위협

A. 모의훈련 시나리오

훈련 단계	공격 기법 (MITRE ATT&CK)	훈련 내용
1. 초기 침투	Internal Spearphishing (T1566.002)	사전에 내부 공유 폴더에 모의 파일(연봉/복지 가이드 등) 유포
2. 실행	Data from Info Repositories (T0811)	비콘 파일의 열람 등 접근 확인
3. 유출 및 사고 모사	Exfiltration Over Physical Medium (T1011)	외부 매체를 이용한 모의 파일 유출

B. 이벤트 단계별 탐지 및 대응 기준

훈련 단계	탐지 기준	대응 기준
1. 초기 침투	- 사전 협의된 모의 파일이 정상적으로 생성되었는지 확인	- 훈련 개시 및 상황 모니터링
2. 실행	- 비정상 파일 접근 확인 - 모의 파일에 대한 보고 절차 확인	- 열람 인원 확인 및 내용 알림
3. 유출 및 사고 모사	- 외부 매체 연결 및 유출 행위 인지	- 매체 제어 솔루션을 통한 대응 - 중요 파일의 '읽기 전용' 권한 설정

4. OT/ICS 공격

A. 모의훈련 시나리오 (도상 훈련)

- 훈련 목적: OT 환경에 대한 탐지 및 대응 프로세스의 효율성 확인 및 최적화

훈련 단계	공격 기법 (MITRE ATT&CK)	훈련 내용
1. 사고 발생 상황 가정	Data Destruction(T0809)	OT 환경에 랜섬웨어 및 데이터 조작 등 사이버 공격이 발생하였다는 상황 제시
2. 상황 인지	Alarm Suppression(T0801)	OT 현장 내 장치에 대한 비정상 동작 상황 제시
3. 대응 조치	Automated Response(T0804)	OT 환경에 대한 복구 및 대응 수행

B. 이벤트 단계별 탐지 및 대응 기준

훈련 단계	탐지 기준	대응 기준
1. 사고 발생상황 가정	- OT 환경에 대한 랜섬웨어 전이 및 공격 탐지	- 보안솔루션 및 네트워크 격리 환경을 통한 랜섬웨어 전이 및 공격에 대한 즉각 차단
2. 상황 인지	- 센서값과 실제 공정 상태 불일치 등 이상징후 식별	- 보고 절차에 따라 담당자에게 보고
3. 대응 조치	- N/A	- PLC 로직 및 HMI 프로젝트를 통해 설정값 복원 - 감염 경로와 같은 근본원인 분석

■ 별첨 C. MTTD/MTTR 등급별 목표수준(SLA) 정의서

1. 목적

본 정의서는 모의 훈련 시 발생한 보안 이벤트에 대한 대응팀의 탐지 및 조치 역량을 정량적으로 평가하기 위한 등급 기준을 정의하며, 이를 통해 조직의 보안 사고 대응 성숙도를 측정하는 데 목적이 있습니다.

2. 등급별 산정 기준 (SLA)

훈련의 특성(1일 5회 수행)을 고려하여, 실제 운영 환경보다 타이트한 '초동 대응 중심' 기준을 적용합니다.

이때, 훈련 기간이 변경될 경우, 해당 기간을 고려하여 '초동 대응 중심' 기준을 조율하여 적용합니다.

현재, 본 등급별 산정 기준을 1일 모의훈련을 기반으로 작성되어 있습니다.

등급	위험도	MTTD (탐지)	MTTR (조치)	정의 및 기대 수준
Low	최적	3분 이내	10분 이내	• 공격 징후를 실시간 탐지하고, 공격자가 추가 행위를 하기 전, 즉시 차단 완료함.
Medium	양호	10분 이내	25분 이내	• 표준 대응 절차(SOP)에 따라 정상적으로 대응함. 분석 및 의사결정이 지연 없이 수행됨.
High	미흡	20분 이내	45분 이내	• 탐지 알람을 놓치거나 분석 과정에서 병목 발생. 공격이 내부망으로 확산될 위험이 존재함.
Critical	위험	20분 초과	45분 초과	• 사실상 대응 실패. 외부 힌트나 강제 종료 시점까지 조치가 미비하여 심각한 피해 예상됨.