■ 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