THALES SENTINEL

EU Cyber Resilience Act (CRA)
컴플라이언스 가이드라인

제조사·소프트웨어 공급사·EU 수출 기업을 위한 CRA 대응 실무 지침

발효일	2024년 12월 10일
전면 적용일	2027년 12월 11일
준비 권장 기간	12~18개월 (즉시 착수 권고)
대상	EU 시장 내 디지털 요소 포함 제품(PDE) 공급 기업 전체 (비EU 포함)
솔루션	Thales Sentinel Platform

01 CRA란 무엇인가?

EU 사이버 복원력법 핵심 개요 — 배경·목적·적용 범위

EU Cyber Resilience Act(CRA)는 디지털 요소가 포함된 제품(Products with Digital Elements, PDE)의 전체 수명주기-설계·개발·배포·유지보수·폐기 — 에 걸쳐 사이버 보안을 의무화하는 EU 핵심 규제입니다. 2024년 12월 10일 발효되었으며, **2027년 12월 11일부터 전면 적용**됩니다.
기존 규제와의 가장 큰 차이점은 **'출시 후(Post-Market) 지속 의무'**입니다. 단순히 출시 시점의 보안 인증을 받는 것으로는 충분하지 않습니다. 제조사·공급사는 제품이 시장에 유통되는 동안 발생하는 취약점에 대해 지속적으로 대응하고, 보안 업데이트를 제공하며, 당국에 보고할 의무를 집니다.

적용 대상 (Products with Digital Elements, PDE)

유형	포함 범위	제외 여부
소프트웨어	상업용 패키지 SW, 상업 목적 오픈소스(OSS) 포함	적용 대상
하드웨어	IoT 기기, 스마트 디바이스, 산업용 장비, 네트워크 장비	적용 대상
원격 데이터 처리	SW·HW와 결합되어 별도 출시되는 솔루션	적용 대상
결합형 SaaS	HW·SW 제품과 연동되어 함께 유통되는 클라우드 서비스	적용 대상
순수 SaaS	독립적으로 제공되는 순수 클라우드 서비스 (ERP, CRM 등)	원칙적 제외 *

* 단, SaaS라도 HW·SW 제품과 결합·번들로 유통되는 경우 CRA 영향권에 포함될 수 있습니다.

미준수 시 제재

제재 유형	법적·재정적	사업적 영향
벌금	최대 1,500만 유로 또는 글로벌 연매출의 2.5% 중 높은 금액	EU 시장 진입 차단
행정명령	시정조치, 제품 리콜, 판매 중단	브랜드 평판 및 고객 신뢰 훼손
CE 인증 지연	제품 출시 지연 및 인증 비용 증가	공급망 벤더 검증 탈락 위험

02 지금 준비해야 하는 이유

CRA 대응 타임라인·리스크·적용 대상 기업

EU 인증기관(TÜV Rheinland, SGS 등)에 따르면 CRA 완전 준수에는 평균 12~18개월이 소요됩니다. 2027년 12월 전까지 시간이 충분해 보여도, SBOM 구축·취약점 체계·인증 절차를 고려하면 지금 바로 착수해야 합니다.

CRA 주요 일정

2024.12.10	CRA 발효 — EU 공식 시행, 제조사 준비 의무 개시
2025-2026	공급망 벤더 검증 강화 — EU 주요 기업들이 파트너 선정 기준에 CRA 준수 포함
2027.12.11	**CRA 전면 적용 — 미준수 제품 EU 시장 유통 금지, 벌금 부과 개시**

- SBOM(소프트웨어 부품표), 취약점 관리 체계, 공급망 검증 등 단기간 구축이 어려운 요건 다수
- 2024년부터 EU 주요 기업들이 공급망 벤더 선정 기준에 CRA 준수 여부 포함 — 미준수 시 계약 탈락 위험
- Security-by-Design 원칙: 설계 단계부터 보안 내재화 시 비용과 리스크 최소화
- CE 인증 지연 시 제품 출시 일정 및 계약 이행에 직접 영향

어떤 기업이 해당되는가? - 한국 기업 관점

CRA는 EU 내에서 사업장을 운영하는 기업뿐만 아니라, EU 시장에 제품을 수출하는 비EU 기업 모두에 적용됩니다.
한국 기업도 예외가 없습니다.

기업 유형	해당 예시 (한국 기업)	주요 리스크
EU 수출 제조사	산업용 장비·스마트 팩토리 설비·전자기기를 EU에 수출하는 기업 (예: 삼성전자, LG전자, 현대 계열사, 중견 제조사)	CE 인증 지연 → 수출 중단
소프트웨어·솔루션 공급사	ERP·MES·보안 SW·임베디드 SW 등 EU 고객사에 SW를 공급하는 기업 (예: 국내 보안 SW사, SaaS 스타트업의 HW 결합 제품)	계약 탈락, 공급망 배제
IoT·Connected Device 기업	스마트홈, 의료기기, 자동차 부품, 산업용 센서 등 인터넷 연결 디바이스 공급사 (예: 웨어러블, 스마트 에너지 미터 제조사)	리콜·판매 금지 명령
오픈소스 상업 배포사	상업 목적으로 오픈소스를 포함한 제품을 EU에 배포하는 기업 (비상업적 커뮤니티 프로젝트는 제외)	취약점 책임 의무
글로벌 SW 벤더의 한국 파트너	EU 진출 글로벌 소프트웨어사의 한국 대리점·리셀러 - 최종 책임은 제조사에 있으나, 유통 경로 검증 의무	공급망 실사 요구

적용 제외 확인이 필요한 경우: 자사 제품이 순수 SaaS인지, HW/SW 결합 제품인지 반드시 법률·기술 전문가와 함께 분류 작업을 선행하세요.

03 CRA 요구사항 분류 및 Sentinel 커버리지

6개 핵심 요건과 Thales Sentinel 대응 현황

CRA 요구사항은 **개발·설계 단계(Pre)와 배포·운영 단계(Post)**로 구분됩니다.
Thales Sentinel은 배포·운영 단계의 기술적 요건에 강력한 커버리지를 제공합니다.

	CRA 요구사항	Sentinel 대응	커버리지	단계
1	위변조 방지 및 무결성 보장	Sentinel Envelope — 코드 난독화·암호화(DFP)	90%	Post
2	접근 제어	Sentinel LDK — 사용자/디바이스/기능 기반 라이선싱	80%	Post
3	안전한 업데이트 제공	Sentinel UP / EMS — 서명된 패치 배포 및 알림	80%	Post
4	로그 및 감사 추적	Sentinel EMS / UP / LDK-CL — 배포·활성화 이력	70%	Post
5	안전한 설계 및 개발 (SBOM)	프로세스 영역 — 솔루션 직접 커버 어려움	10%	Pre
6	취약점 대응 / PSIRT 운영	내부 운영 프로세스 영역 — 솔루션 범위 외	0%	Pre

80%+ 강력 커버리지 **50~79%** 부분 커버리지 **0~49%** 프로세스 영역

Post = 배포·운영 단계 | Pre = 개발·설계 단계

04 요구사항별 상세 대응 가이드

CRA 요건 설명 및 Sentinel 솔루션 매핑

1 위변조 방지 및 무결성 보장 — Post — 90%

CRA 요구사항

부당 이용·불법 복제·변조 공격에 견딜 수 있도록 데이터·명령어·설정 파일이 임의 변경되지 않도록 보호하고 데이터 암호화를 적용해야 합니다.

Sentinel 솔루션

Sentinel Envelope, Sentinel DFP

코드 난독화, 소프트웨어 보호, 리버스 엔지니어링 방지, 안티 디버깅·트레이싱 기술과 데이터 파일 암호화(DFP)로 요건의 90%를 충족합니다.

2 접근 제어 — Post — 80%

CRA 요구사항

승인받지 않은 사용자가 기능을 임의로 사용하지 못하도록 인증·인가, 관리자/사용자 권한 구분, 불법 복제 방지 체계를 갖춰야 합니다.

Sentinel 솔루션

Sentinel LDK

사용자 기반(User-based)·디바이스 기반(Device-based)·기능 기반(Feature-based) 라이선싱으로 기능 접근을 엄격히 제어하고 사용 현황을 기록합니다.

3 안전한 업데이트 제공 — Post — 80%

CRA 요구사항

취약점 발견 시 서명 및 위변조 방지가 적용된 안전한 업데이트를 제공해야 하며, 사용자 알림 및 오프라인 환경 업데이트 방안도 마련해야 합니다.

Sentinel 솔루션

Sentinel UP, Sentinel EMS

비준수 버전 사용 고객 식별, 서명된 업데이트 자동 배포, 업데이트 완료 확인·검증 기능을 제공하여 요건의 80%를 달성합니다.

4 로그, 감사 추적 및 투명성 — Post — 70%

CRA 요구사항

보안 사고 발생 시 '누가·언제·무엇을 했는지' 설명할 수 있도록 접근·변경·업데이트 내역 등 보안 이벤트에 대한 감사 추적 데이터를 유지해야 합니다.

Sentinel 솔루션

Sentinel EMS, Sentinel UP, Sentinel LDK-CL

소프트웨어 배포 이력, 액티베이션 내역, 클라우드 기반 사용 정보 자동 수집으로 감사 추적 요건의 70%를 지원합니다.

5 안전한 설계 및 개발 프로세스 (SBOM) — Pre — 10%

CRA 요구사항

제품 설계 단계부터 사이버 위협 분석, SBOM(소프트웨어 부품표) 관리, Secure by Default 설정 구현이 필요합니다.

Sentinel 솔루션

해당 없음 (프로세스 영역)

개발·관리 프로세스 영역으로 기술 솔루션의 직접 커버리지는 10%에 그칩니다. 별도 SBOM 관리 도구 및 내부 프로세스 수립이 필요합니다.

6 취약점 대응 / PSIRT 운영 — Pre — 0%

CRA 요구사항

취약점 접수·평가, 24시간 내 당국 보고, 심각도별 수정 대응을 위한 내부 PSIRT(제품 보안 사고 대응 팀) 운영 프로세스를 갖춰야 합니다.

Sentinel 솔루션

해당 없음 (내부 운영 프로세스)

완전히 기업의 내부 운영·거버넌스 영역입니다. 기술 솔루션이 아닌 조직 정책 및 절차 수립이 요구됩니다.

05 Thales Sentinel 솔루션 구성

CRA 배포·운영 컴플라이언스를 위한 제품 라인업

제품	주요 기능	대응 CRA 요건
Sentinel Envelope	코드 난독화, 안티 디버깅·트레이싱, 리버스 엔지니어링 방지, 데이터 파일 암호화(DFP)	위변조 방지, 데이터 보안
Sentinel LDK	사용자·디바이스·기능 기반 라이선싱, Digital Fingerprint 인증, 사용 현황 보고	접근 제어, 감사 추적
Sentinel UP	비준수 버전 식별, 서명된 업데이트 자동 배포, 완료 검증	안전한 업데이트
Sentinel EMS	소프트웨어 배포·활성화 이력 중앙 관리, 클라우드 사용 정보 수집	업데이트 관리, 감사 추적
Sentinel LDK-CL	클라우드 기반 라이선싱, 사용량 자동 수집 및 보고	감사 추적, 투명성

06 다음 단계 (Next Steps)

CRA 대응 착수 체크리스트

단계	항목	세부 내용
1	**현황 진단**	자사 제품의 CRA 적용 대상(PDE) 해당 여부 분류 및 현재 보안 수준 갭 분석
2	**SBOM 구축**	사용 중인 오픈소스·서드파티 컴포넌트 목록화, 취약점 관리 프로세스 수립
3	**Sentinel 도입 검토**	위변조 방지·접근 제어·업데이트·감사 추적 요건에 대한 Sentinel 적용 범위 협의
4	**PSIRT 프로세스 수립**	내부 취약점 접수·평가·보고 체계 구축 (CRA 요건 6번 대응)
5	**CE 인증 준비**	인증기관(TÜV Rheinland 등)과 사전 협의, 준비 일정 수립 (12~18개월 소요)

CRA 대응, Thales Sentinel과 함께 시작하세요

배포·운영 단계의 기술적 요건을 가장 빠르고 안정적으로 충족하는 검증된 솔루션

cpl.thalesgroup.com

연락처 - 모든 지사 위치 및 연락처 정보는 cpl.thalesgroup.com/contact-us를 참조하시기 바랍니다.