CRA EVIDENCE 백서

EU 사이버복원력법: 실무 규제 준수 가이드

디지털 요소를 포함하는 제품의 제조업체, 수입업체, 유통업체를 위한 백서.

작성	CRA Evidence
버전	1.0
상태	지속 업데이트 문서
근거	EU 규정 2024/2847

변경 이력

본 백서는 CRA 시행 일정과 위원회·ENISA 지침의 변화에 맞춰 계속 갱신되는 문서입니다.

버전	날짜	설명
1.0	2026년 5월 17일	최초 공개 발행. EN 원본 wave 2-8 정합(분류 가이드, 클라우드 경계, 공급망, 실질적 변경, 지원 기간 결정, 구성요소 실사, 제14조 신고 일정, 시정 조치, 권고문 워크플로, AI Act·ESPR·Data Act·제조물 책임 인접 의무).

목차

요약

핵심 요약

적용 대상: EU 시장에 출시되는 연결형 하드웨어와 소프트웨어 제품입니다. 사이버보안은 권장 실무가 아니라 제품 규제 준수 요건으로 다뤄집니다.

적용 시점: 제14조 신고 의무는 2026년 9월 11일부터, 기술·문서·CE 마킹 의무 전부는 2027년 12월 11일부터 적용됩니다.

준비 산출물: 사이버보안 리스크 평가, SBOM, 기술 파일, 사용자 설명서, EU 적합성 선언, CE 마킹, 제14조 사고 및 취약점 보고.

누가 조치해야 하나

핵심 책임은 제조업체에 있습니다. 수입업체와 유통업체는 제품을 제공하기 전에 주의 의무 점검을 수행합니다.

무엇이 바뀌나

사이버보안이 제품 규제 준수의 일부가 됩니다. 보안 설계, 취약점 처리, 문서화, CE 마킹, 출시 후 조치가 포함됩니다.

첫 기한

제14조 신고는 적극적으로 악용된 취약점과 중대한 사고에 대해 **2026년 9월 11일**에 시작됩니다.

전면 적용

기술 규제 준수는 **2027년 12월 11일**부터 전면 적용됩니다. 기존 제품은 실질적 변경 이후에 적용되지만 신고 의무는 그 전에도 적용됩니다.

증거의 중심

기술 파일에는 리스크 평가, SBOM, 지원 기간 근거, 시험 증거, 사용자 설명서, 선언서, 그리고 필수 사이버보안 요건에 대한 적합성 증거가 포함됩니다.

적합성 경로

대부분의 제품은 모듈 A 자체 평가를 사용할 수 있습니다. 중요 제품과 핵심 제품은 인증기관 또는 EU 사이버보안 인증 경로가 필요할 수 있습니다.

사이버복원력법이란?

EU 규정 2024/2847, 사이버복원력법(CRA)은 EU 시장에 출시되는 디지털 요소 포함 제품에 대해 사이버보안을 구속력 있는 요건으로 만든 최초의 EU 차원 규제 체계입니다. 공식 본문은 EUR-Lex에서 확인할 수 있습니다.

CRA는 연결형 하드웨어와 소프트웨어의 제조업체, 수입업체, 유통업체에 적용됩니다. 소비자 IoT 기기부터 산업 제어 시스템까지 폭넓은 제품이 포함됩니다. 실무 변화는 명확합니다. 사이버보안을 설계 단계부터 반영하고, 증거로 남기고, 유지하고, 모니터링해야 합니다. 이 작업은 제품 규제 준수의 일부입니다.

필수 사이버보안 요건 또는 제13조와 제14조의 의무를 위반하면 최대 1,500만 유로 또는 전 세계 연간 매출의 2.5% 중 더 높은 금액의 과징금이 부과될 수 있습니다. 하위 단계도 적용됩니다. 그 밖의 명시된 의무 위반은 최대 1,000만 유로 또는 2%, 인증기관이나 시장 감시 기관에 부정확·불완전·오해 소지가 있는 정보를 제공하면 최대 500만 유로 또는 1%입니다. 시장 감시 기관은 시정 조치, 제공 제한, 제품 철회, 리콜을 요구할 수도 있습니다.

CRA 운영 모델

규제 준수 계획의 주요 일정

CRA는 **2024년 12월 10일**에 발효되었습니다. 실무상 규제 준수 작업은 세 가지 주요 일정에 맞춰 단계적으로 적용됩니다. **2026년 6월** 인증기관 규정, **2026년 9월** 신고 의무, **2027년 12월** 기술 규제 준수 전면 적용입니다.

참고

유럽위원회 현재 지침: 유럽위원회는 2026년 3월 3일 CRA 지침 초안을 공개했습니다. 의견 수렴은 2026년 4월 13일에 종료되었습니다. 최종본은 아니지만 시장 출시, 자유·오픈소스 소프트웨어, 지원 기간, 실질적 변경, 제품 분류, 구성요소 실사, 원격 데이터 처리, 취약점 처리, 다른 EU 법령과의 중복을 계획할 때 유용한 참고 자료입니다. AI Act 및 DORA와의 경계 문제는 추가 지침이 필요할 수 있습니다.

2024년 12월 10일

발효

전환 기간 시작

2026년 6월 11일

인증기관

제IV장 적용

2026년 9월 11일

신고

제14조 신고 시작

2027년 12월 11일

전면 적용

기술 요건, CE 마킹, 문서, 적합성 평가

먼저 할 일

신고 준비부터 착수하십시오. 제14조 기한은 기술 규제 준수 전면 적용보다 빠르며, 이미 EU 시장에 있는 제품에도 적용됩니다.

신고는 **2026년 9월 11일**에 시작되므로 신고 준비가 첫 번째 실행 과제가 되어야 합니다. **탐지, 분류, 사용자 통지, 당국 신고** 절차가 기술 규제 준수 전면 적용 전에 작동해야 합니다.

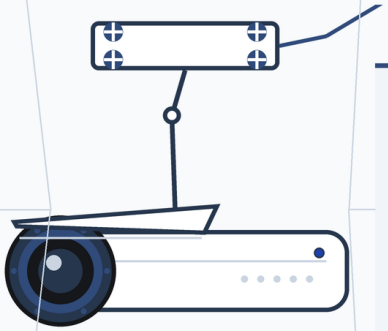
2027년 12월 11일 전에 시장에 출시된 제품은 그 날짜 이후 **실질적 변경**을 거친 경우에만 CRA 기술 요건의 적용을 받습니다. 신고 의무는 별도입니다. 제14조는 적용 대상 제품 전체에 적용되며, 이미 EU 시장에 있는 제품도 예외가 아닙니다.

제품 수명주기 전반의 CRA

단계 01
제품 범위 정하기
적용 범위, 분류, 지원 기간, 위험 평가

단계 02
안전하게 개발
안전한 기본값, 코드 분석, SBOM, 의존성 관리

단계 03
검증하고 문서화
보안 시험, 취약점 분류, 기술 문서, 사용자 안내



단계 04
시장에 출시
EU 적합성 선언, CE 표시, 출시 결정

단계 05
모니터링과 업데이트
CVE, 권고, 악용 활동, 보안 업데이트, 공개

단계 06
지원하고 협력
제14조 보고, 사용자 통지, 당국 요청, 지원 종료

연결형 IP 카메라를 제품 기획부터 CRA에 따른 출시 후 지원까지 추적

적용 대상 제품

적용 범위와 제외 대상

CRA는 의도된 사용 또는 합리적으로 예측 가능한 사용에 기기나 네트워크와의 직접 또는 간접 데이터 연결이 포함되는 하드웨어와 소프트웨어 제품에 적용됩니다. 컴퓨터, 스마트폰, 네트워크 장비, IoT 기기, 산업 제어 시스템, 데이터 처리 애플리케이션이 모두 포함됩니다.

다음 범주는 명시적으로 제외됩니다.

- EU 규정 2017/745 및 2017/746의 적용을 받는 의료기기와 체외진단 의료기기
- EU 규정 2019/2144의 적용을 받는 자동차 시스템
- EU 규정 2018/1139의 적용을 받는 항공 장비
- 지침 2014/90/EU의 적용을 받는 선박 장비
- 국가 안보 또는 방위 목적만으로 개발된 제품
- 디지털 요소나 네트워크 연결이 없는 순수 기계 제품

명확한 제외 사유가 없다면 연결형 제품은 적용 범위에 해당한다고 보아야 합니다.

참고

맞춤형 제품: 좁은 예외. 특정 사업 사용자 한 곳에 맞춰 제작한 제품이고, 그 사용자와 서면 합의가 있다면 두 가지 요건에서만 예외가 인정됩니다. 첫째, 안전한 기본 설정에서 일부 벗어날 수 있습니다. 다만 원래의 안전 상태로 돌아갈 경로는 반드시 제공해야 합니다. 둘째, 무상 보안 업데이트에서 벗어날 수 있습니다. 다만 합의로 다른 상업적 조건을 정해야 합니다. 그 외에는 모든 요건이 그대로 적용됩니다. 취약점 처리, 다른 제품 보안 요건, 제14조 신고, 기술 문서, CE 마킹, 적합성 평가, 지원 기간 모두 동일합니다. 일반적인 B2B 예외가 아니며, 사업체에 판매되는 기성품에는 적용되지 않습니다.

경제 운영자의 책임

제조업체	안전한 제품을 설계하고, 리스크를 평가하며, 기술 문서를 준비하고, 적합성 평가를 수행하며, 취약점을 처리하고, 제14조 사고를 신고합니다.
수입업체	제조업체의 규제 준수 상태를 확인하고, CE 마킹과 문서를 검증하며, 선언서를 제공 가능 상태로 유지하고, 알려진 취약점에 대응합니다.
유통업체	공급 전 주의 의무 항목을 확인하고, 필요한 정보와 설명서를 검증하며, 부적합 제품의 제공을 회피합니다.

제품 분류가 평가 경로를 결정합니다

제품 범주는 적합성을 입증하는 방식을 결정합니다.

범주	예시	적합성 평가
기본 "미분류"	중요 제품이나 핵심 제품에 해당하지 않는 일반 소프트웨어와 연결형 소비자 제품	모듈 A: 자체 평가
중요 제품 Class I	ID 관리, 브라우저, 비밀번호 관리자, 백신, VPN, 네트워크 관리, 라우터, 스마트 도어락, 보안 카메라 등	적용 가능한 조화 표준, 공통 사양 또는 인증 체계가 요구대로 적용된 경우에만 모듈 A. 그 외에는 모듈 B+C 또는 모듈 H
중요 제품 Class II	하이퍼바이저, 컨테이너 런타임, 방화벽, IDS/IPS, 변조 방지 마이크로프로세서	모듈 B+C, 모듈 H, 또는 substantial 이상의 보증 수준을 가진 유럽 사이버보안 인증 체계
핵심 제품	보안 요소, 스마트카드, 스마트 미터 게이트웨이, 하드웨어 보안 박스	필요하고 이용 가능한 경우 유럽 사이버보안 인증. 그 외에는 Class II 경로 적용

네 가지 제품 범주

위의 표는 예시입니다. 제품의 핵심 기능과 대조해야 할 전체 기준은 아래와 같습니다.

기본 제품

대부분의 제품이 여기에 해당합니다. 핵심 기능이 아래 중요 제품 또는 핵심 제품 목록에 일치하지 않는 모든 디지털 요소 포함 제품은 기본 제품으로 다룹니다. 적합성 경로는 모듈 A 자체 평가입니다.

자주 보이는 예:

- 스마트 TV와 스트리밍 기기
- 네트워크 프린터와 복합 사무기기
- 블루투스 스피커와 소비자 오디오 제품
- 미디어 플레이어 소프트웨어
- 게임 콘솔, 전자책 리더, 비슷한 소비자 가전
- 보안 기능이 없는 스마트 주방기기(오븐, 냉장고, 식기세척기 등)
- 보안 기능이 없는 스마트 전구와 연결형 조명
- 건강 모니터링 기능이 없는 피트니스 트래커
- 브라우저, 비밀번호 관리자, VPN 앱이 아닌 일반 모바일 애플리케이션
- 워드프로세서, 스프레드시트 등 사무 생산성 소프트웨어

위 목록은 예시입니다. 아래의 중요 제품과 핵심 제품 목록은 한정 열거입니다.

중요 제품 (Class I)

조화 표준, 공통 사양 또는 인증 체계가 요구대로 적용되지 않는 한 제3자 평가가 의무입니다.

1. ID 관리 및 권한 접근 관리 소프트웨어와 하드웨어. 인증 및 접근 통제 리더(생체 인식 리더 포함).
2. 독립형 및 임베디드 브라우저.
3. 비밀번호 관리자.
4. 악성 소프트웨어를 탐색·제거·격리하는 소프트웨어.
5. VPN 제품.
6. 네트워크 관리 시스템.
7. 보안 정보 및 이벤트 관리(SIEM) 시스템.
8. 부트 관리자.
9. 공개 키 인프라(PKI)와 디지털 인증서 발급 소프트웨어.
10. 물리 및 가상 네트워크 인터페이스.
11. 운영체제.
12. 라우터, 인터넷 연결용 모뎀, 스위치.
13. 보안 관련 기능이 있는 마이크로프로세서.
14. 보안 관련 기능이 있는 마이크로컨트롤러.
15. 보안 관련 기능이 있는 ASIC와 FPGA.
16. 스마트홈용 범용 가상 비서.

17. 보안 기능이 있는 스마트홈 제품(스마트 도어락, 보안 카메라, 영아 모니터링 시스템, 경보 시스템).
18. 상호작용 기능(대화, 촬영, 위치 추적)이 있는 인터넷 연결 장난감.
19. 건강 모니터링 목적의 개인용 웨어러블(EU 규정 2017/745 또는 2017/746이 적용되지 않는 경우), 또는 아동용 웨어러블.

중요 제품 (Class II)

제3자 평가가 의무이며 더 엄격한 경로가 적용됩니다. 조화 표준이 있어도 자체 평가는 허용되지 않습니다.

1. 운영체제 등의 가상화 실행을 지원하는 하이퍼바이저와 컨테이너 런타임 시스템.
2. 방화벽, 침입 탐지 및 방지 시스템.
3. 변조 방지 마이크로프로세서.
4. 변조 방지 마이크로컨트롤러.

핵심 제품

해당 인증 체계가 이용 가능한 경우 유럽 사이버보안 인증이 필요합니다. 그 외에는 Class II 경로가 적용됩니다.

1. 보안 박스를 내장한 하드웨어 장치.
2. 지침(EU) 2019/944 제2조 제23호에서 정의된 스마트 미터링 시스템 내의 스마트 미터 게이트웨이와 고급 보안 목적의 기타 장치. 안전한 암호 처리 기능을 포함합니다.
3. 스마트카드와 유사 장치. 보안 요소를 포함합니다.

제품의 핵심 기능이 중요 제품 또는 핵심 제품 목록의 항목과 일치하면 해당 분류에 속합니다. 그 항목을 구성요소로 통합하더라도 제품 자체의 핵심 기능이 다르면 통합만으로 분류가 바뀌지 않습니다.

분류 방법: 통합이 아니라 핵심 기능

위의 목록은 범주가 무엇인지를 알려줍니다. 그러나 그것을 자기 제품에 어떻게 적용할지는 말해주지 않습니다. CRA의 답은 한 단어로 정리됩니다. **핵심 기능**입니다.

분류는 제품의 핵심 기능이 무엇인지로 결정되며, 어떤 구성요소를 통합했는지로 결정되지 않습니다. 핵심 기능이 중요 제품 목록과 일치하면 중요 제품(Class I 또는 Class II)이 됩니다. 핵심 제품 목록과 일치하면 핵심 제품이 됩니다. 어느 쪽과도 일치하지 않으면 기본 제품입니다. 시험은 이게 전부입니다.

실무적 안전장치는 제7조제1항의 두 번째 문장에 있습니다. 중요 구성요소를 통합한다고 해서 통합 제품이 중요 제품 분류로 올라가지 않습니다. 스마트홈 허브에 방화벽 라이브러리를 포함했다고 해서 그 허브가 방화벽이 되지는 않습니다. 전문 제45항은 이 점을 분명히 말합니다. 방화벽과 침입 탐지 시스템은 중요 제품 Class II에 속하지만, 이들을 통합한 다른 제품은 그렇지 않다는 것입니다.

다음 순서로 자체 분류를 수행하십시오.

1. **제품의 핵심 기능을 한 문장으로 정의하십시오.** 이것이 불가능하면 이후 분석이 의미를 잃습니다. 제품이 그것 없이는 작동하지 않는 기능에 초점을 맞추십시오.
2. **위의 중요 제품 목록을 확인하십시오.** Class I 또는 II에 일치하면 제품은 중요 제품입니다.
3. **위의 핵심 제품 목록을 확인하십시오.** 일치하면 제품은 핵심 제품입니다. 이용 가능한 경우 유럽 사이버보안 인증 경로가 적용되며, 그렇지 않으면 Class II 경로가 적용됩니다.
4. **어느 목록과도 일치하지 않는 경우.** 제품은 기본 제품입니다. 모듈 A 자체 평가가 경로입니다.
5. **근거를 문서화하십시오.** 핵심 기능 진술, 목록 확인, 선택한 경로를 한 페이지 메모로 남겨 기술 파일에 보관합니다.

두 가지 사례.

비밀번호 관리자를 임베드한 스마트홈 허브. 핵심 기능은 가정 내 소비자 IoT 기기의 루틴을 조율하는 것입니다. 비밀번호 관리자 구성요소는 자체 제조업체가 별도로 판매하며, 그 자체로는 중요 제품 Class I입니다. 그러나 허브의 핵심 기능은 가정 자동화이지 자격 증명 관리가 아닙니다. 허브는 기본 제품으로 분류됩니다.

기능 집합으로 본 운영체제. 어떤 제품이 스마트홈 가전으로 판매되지만, 주요 기능은 하드웨어와 주변 장치 초기화, 프로세스 스케줄링, 메모리 관리, 시스템 호출 인터페이스입니다. 그것은 운영체제의 핵심 기능입니다. 운영체제는 중요 제품 Class I입니다. 마케팅과 무관하게 이 제품은 중요 제품 Class I입니다.

분류 결과가 팀 다른 구성원의 예상과 어긋난다면, 출시 전에 핵심 기능 진술을 한 번 더 다듬어야 합니다.

클라우드가 제품의 일부일 때

대부분의 디지털 요소 포함 제품은 기기 바깥의 무엇인가에 의존합니다. 클라우드 백엔드, 모바일 동반 앱, OTA 업데이트 서버, 인증 포털, 기기 관리 시스템이 그 예입니다. CRA는 이들 모두를 자동으로 제품의 일부로 보지 않습니다. 두 조건이 **모두** 충족될 때에만 제품의 일부로 다룹니다.

- 해당 소프트웨어가 **자체 팀이 설계·개발했거나, 자체 책임 하에 만들어진 것**입니다.
- 그것 없이는 제품이 **제공하는 기능 중 하나가 작동하지 않습니다.**

이 중 하나라도 충족하지 않으면, 원격 서비스는 CRA의 제품 경계 바깥에 위치합니다. 자체 소유가 아닌 제3자 SaaS는 제품이 그것과 통신하더라도 제품의 일부가 아닙니다. 제품을 홍보하지만 제품의 기능을 지원하지 않는 웹사이트도 제품의 일부가 아닙니다.

원격 구성요소가 적용 범위에 들어오면 **제품의 일부로서** 들어옵니다. 기술 파일, 적합성 평가, 적합성 선언, 취약점 처리, 제14조 신고 일정 모두가 기기뿐 아니라 클라우드 구성요소까지 포괄합니다.

다음 매트릭스로 빠르게 판단하십시오.

구성요소	제품의 일부로 적용 범위?
기기와 페어링되는 모바일 동반 앱	**예.** 자체 설계했고, 이것 없이는 기기를 설정하거나 사용할 수 없습니다.
기기 데이터를 저장·처리하는 클라우드 백엔드	**예.** 자체 설계했고, 이것 없이는 대시보드나 주요 기능이 작동하지 않습니다.
OTA 업데이트 서버	**예.** 자체 설계했고, 이것 없이는 기기가 보안 업데이트를 받을 수 없습니다.
기기 접근을 통제하는 인증 포털	**예.** 자체 설계했고, 이것 없이는 사용자가 로그인할 수 없습니다.
제품 홍보 웹사이트	**아니요.** 제품 기능을 지원하지 않습니다.
제품이 통합하는 제3자 SaaS(자체 소유 아님)	**아니요.** 자체 설계가 아닙니다. 제3자 제공자는 NIS 2 하의 의무를 별도로 부담합니다.
서비스가 운영되는 일반 클라우드 인프라(IaaS 또는 PaaS)	**아니요.** 자체 설계가 아닙니다. 인프라 제공자는 NIS 2에 해당합니다.

자주 보이는 패턴이 있습니다. 모바일 앱, 업데이트 서버, 클라우드 백엔드를 갖춘 스마트홈 기기입니다. 셋 모두를 제조업체가 설계했고, 기기는 이것들 없이는 광고된 기능을 제공할 수 없습니다. 셋 모두 제품의 일부입니다. CRA 의무는 이 묶음 전체에 적용됩니다. 클라우드 백엔드가 다시 제3자 분석 SaaS와 통신한다면, 그 SaaS는 제품의 일부가 아닙니다. 제3자 제공자는 NIS 2 하의 의무를 자체적으로 부담합니다.

CRA는 제조업체의 네트워크와 정보 시스템 전체에 대한 보안 조치를 요구하지 않습니다. 제품의 일부인 원격 서비스에 대한 보안을 요구합니다. 경계선은 회사 경계가 아니라 제품 경계입니다.

공급망: CRA에서 각자가 하는 일

CRA는 제조업체에 핵심 의무를 부과하지만, 수입업체와 유통업체도 제품이 시장에 도달하는 방식에 영향을 주는 의무를 집니다. 제조업체가 알아야 할 세 가지가 있습니다.

주체	공급 전 확인 사항	취약점 발생 시 조치	제조업체 의무를 인수하는 시점
수입업체	CE 마킹, EU 적합성 선언, 올바른 언어의 사용자 설명서, 제품 또는 동봉 자료의 연락처	지체 없이 제조업체에 통지. 제품이 중대한 사이버보안 리스크를 제시하면 시장 감시 기관에 직접 통지	자기 명의 또는 상표로 출시하거나 실질적 변경을 가한 경우
유통업체	CE 마킹, 제조업체와 수입업체가 자기 역할을 수행했는지, 필요한 문서가 제품과 함께 제공되는지	지체 없이 제조업체에 통지. 제품이 중대한 사이버보안 리스크를 제시하면 시장 감시 기관에 직접 통지. 제품 제공을 중단할 수 있음	수입업체와 동일한 조건

제조업체에는 세 가지 실무적 함의가 있습니다.

- CE 마킹, EU 적합성 선언, 사용자 설명서는 유통업체가 확인하는 시점에 정확하고 올바른 언어로 제공되어야 합니다. 채널 파트너는 이를 검증해야 하며, 누락되거나 잘못된 경우 제품 제공을 거부할 수 있습니다.
- 수입업체와 유통업체가 취약점을 자체 취약점 처리 절차로 신고할 수 있는 명확하고 마찰이 적은 연락 경로가 필요합니다. 그들은 실제로 그것을 사용합니다.
- 제품을 리브랜딩하거나 자기 명의·상표로 출시하거나 실질적 변경을 가하는 파트너는 그 버전의 제조업체가 됩니다. 해당 버전에 대한 기술 파일, 적합성 평가, 신고, 지원 기간 의무 전부가 그 파트너에게 이전됩니다. 다음 장의 다른 주체가 제조업체가 되는 경우에서 실질적 변경 규칙을 다룹니다.

실질적 변경: 재적합성 평가가 필요한 시점

제품이 시장에 출시된 후의 변경은 CRA에서 두 갈래로 갈립니다. 대부분은 일상적이며 추가 조치가 필요하지 않습니다. 일부는 실질적입니다. 실질적 변경은 CRA 상 새로운 제품이 시장에 출시되는 것과 동등하게 다뤄집니다. 새로운 적합성 평가, 갱신된 기술 파일, 새 적합성 선언, 새 버전에 대한 CE 마킹이 필요해집니다.

판정 기준은 짧고, 실질적 변경의 정의에 들어 있습니다. 다음 중 하나라도 해당하면 실질적 변경입니다.

- 필수 사이버보안 요건 **준수에 영향을 미치는** 변경
- 평가받은 **의도된 목적을 변경하는** 변경

둘 다 해당하지 않으면 실질적 변경이 아닙니다. 그래도 근거는 문서화해서 보관하십시오. 분석 자체가 증거의 일부입니다.

실질적 변경에 해당하지 않는 경우

실무에서 가장 많이 사용되는 두 가지 예외가 있습니다.

의도된 목적을 바꾸지 않고 사이버보안 리스크를 줄이는 보안 업데이트와 버그 수정은 실질적 변경이 아닙니다. 알려진 취약점에 패치를 적용하거나, 결함을 막기 위해 입력 검증을 조정하거나, CVE에 대응하기 위해 구성요소를 다시 빌드하는 일은 모두 이쪽에 속합니다.

재정비, 정비, 수리도 자동으로 실질적 변경이 되지는 않습니다. 의도된 목적을 바꾸거나 필수 사이버보안 요건 준수에 영향을 미칠 때에만 실질적이 됩니다.

가벼운 사용자 인터페이스 작업도 안전한 쪽에 있습니다. 언어를 추가하거나, 아이콘 세트를 교체하거나, 화면 레이아웃을 다듬는 작업 자체는 실질적 변경이 아닙니다. 그러나 적절한 입력 검증이 필요한 새 입력 요소를 추가하는 것은 실질적이 될 수 있습니다.

예비 부품

CRA는 예비 부품에 대해 좁고 구체적인 예외를 둡니다. **동일 예비 부품**, 즉 교체 대상 구성요소와 같은 사양으로 제작된 부품은 규정의 적용 범위 자체에서 제외됩니다. 기능적 교체품은 그렇지 않습니다.

다음 매트릭스로 빠르게 판단하십시오.

교체품	호스트가 2027년 12월 11일 전에 출시	호스트가 2027년 12월 11일 이후 출시
원본 구성요소와 **동일**, 같은 사양	예비 부품은 CRA 적용 범위 밖. 교체로 인한 의무 없음.	예비 부품은 CRA 적용 범위 밖. 교체로 인한 의무 없음.
기능적으로 동등, 다른 설계 또는 사양	교체품은 그 자체로 CRA 제품. 호스트는 적용일 이전 출시이므로 CRA 의무 없음.	교체품은 CRA 제품. 호스트로의 교체가 위의 이중 기준으로 호스트의 실질적 변경에 해당하는지 평가.

두 가지 실무적 결과가 따릅니다. 첫째, 예외는 동일 사양에 한정됩니다. 다른 칩셋으로 재구성된 무선 모듈은, 고객이 차이를 느끼지 못하더라도 동일 예비 부품이 아닙니다. 둘째, 기능적 교체품을 공급하는 제조업체는 호스트 제조업체가 누구든 그 부품에 대한 CRA 의무를 집니다.

소프트웨어 업데이트와 기능 플래그

소프트웨어 릴리스는 실질적 변경 판단이 가장 자주 발생하는 영역입니다. 이중 기준이 그대로 적용됩니다.

취약점을 수정하는 패치는 실질적이 아닙니다. 평가받은 적이 없는 능력을 켜는 기능 토글은 실질적입니다. 새 범주의 입력에 대해 제품이 결정을 내릴 수 있도록 하는 모델 업그레이드도 마찬가지입니다. 한 릴리스에 수정과 새 기능이 함께 포함되면 새 기능을 기준으로 평가합니다.

번들링 자체는 본질이 아닙니다. 기능 업데이트가 단독으로 배포되든 보안 패치와 같은 릴리스에 들어가든 평가 결과는 달라지지 않습니다.

기능 플래그나 단계별 출시를 운영한다면, 의미 있는 시점은 플래그를 포함한 바이너리의 배포가 아니라 운영 환경의 최종 사용자에 대한 활성화 시점입니다.

실무 판정 절차

모든 변경에 대해 출시 전에 다음 순서를 적용하십시오.

1. **변경이 제품의 의도된 목적을 바꾸는가?** 그렇다면 실질적 변경입니다. 새 버전에 대해 적합성 평가를 다시 수행하십시오.
2. **변경이 필수 사이버보안 요건 준수에 영향을 미치는가?** 그렇다면 실질적 변경입니다. 새 버전에 대해 적합성 평가를 다시 수행하십시오.
3. **그 외:** 실질적이 아닙니다. 분석을 문서화하고 기존 기술 파일 아래에서 계속 진행하십시오.

제품이 중요 제품 또는 핵심 제품 분류에 속하고 처음에 제3자 평가 경로가 요구되었다면, 실질적 변경은 같은 경로로 다시 들어가게 합니다. 실질적이 될 가능성이 있는 변경은 사전에 제3자에게 통지하십시오. 자체 평가는 사후에 중요 제품을 재분류하기 위한 우회로가 아닙니다.

실질적 변경이 인정될 때의 결과

실질적 변경은 새로운 제품이 시장에 출시되는 것으로 다뤄집니다. 제조업체가 해야 할 일은 다음과 같습니다.

- 변경된 버전에 대해 기술 문서를 갱신합니다.
- 제품 분류가 요구하는 경로에 따라 적합성 평가를 다시 수행합니다.
- 변경된 버전에 대해 새 EU 적합성 선언을 발행합니다.
- 새 선언을 보관 상태로 두고 CE 마킹을 다시 적용합니다.
- 이전 버전의 문서는 전체 보관 기간 동안 유지합니다. 새 버전이 이전 버전 문서를 대체하지 않습니다.

소프트웨어 제품의 경우, 지원 기간 중 보안 업데이트의 범위를 시장에 출시된 최신 버전으로 한정할 수 있습니다. 다만 이전 버전 사용자가 추가 하드웨어 없이 무상으로 최신 버전으로 이동할 수 있어야 합니다.

이전 적합성 평가로 이미 판매된 현장 단위는 영향을 받지 않습니다. 의무는 새로 제공되는 변경 버전에 결합하며, 그보다 앞서 출고된 동일 단위에는 결합하지 않습니다.

다른 주체가 제조업체가 되는 경우

원래 제조업체가 아닌 자가 실질적 변경을 수행하면 CRA는 그 자를 해당 버전의 제조업체로 다룹니다. 제13조와 제14조의 의무 전부가 그 자에게 부과됩니다. 자기 명의 또는 상표로 제품을 시장에 출시하는 경우에도 같은 규칙이 적용됩니다.

이 규칙은 팀이 보통 예상하는 것보다 더 많은 상황을 포착합니다.

- 고객별 펌웨어 빌드에 새 기능을 더해 출하하는 시스템 통합 사업자
- 제품을 화이트라벨로 다시 출시하며 마케팅된 의도된 목적을 바꾸는 리셀러
- 제3자 기기를 자체 펌웨어와 묶어 제공하는 서비스 제공자

각 경우에서 변경을 한 주체는 그 버전에 대한 제조업체 의무, 즉 기술 파일, 적합성 평가, 신고, 취약점 처리 등을 인수합니다. "수입업체"나 "유통업체" 명칭은 이 두 선을 넘는 순간 더 이상 보호 장치가 되지 못합니다.

준비해야 할 항목

이 섹션은 작업 체크리스트로 활용하십시오. 요건별 상세 지침은 뒤에 이어집니다.

사이버보안 리스크 평가

제품을 시장에 출시하기 전에 사이버보안 리스크 평가가 파일에 있어야 합니다. 이 문서는 왜 제품을 출시해도 안전하고 시장에 유지해도 안전한지를 자체 언어로 설명하는 자료입니다.

평가에는 다음이 포함되어야 합니다.

- 제품의 의도된 목적, 합리적으로 예측 가능한 사용 사례
- 제품이 운영될 조건과 환경
- 보호해야 할 데이터와 기능
- 적용되는 위협과 이를 관리하기 위해 의존하는 통제
- 제품이 사용될 것으로 예상되는 기간

대부분의 팀이 채택하는 구조. 신뢰할 수 있는 방법론은 동일한 단계로 수렴합니다. 자산(제품이 다루는 데이터, 키·자격 증명 같은 보안 소재, 손실되면 사용자에게 손해를 줄 기능)을 식별하고, 각 자산이 어디에 머무르거나 이동하는지 매핑하고, 자산과 환경별로 기밀성·무결성·가용성을 차원으로 사용해 위협을 모델링하고, 영향과 발생 가능성을 점수화하고, 어떤 잔여 리스크를 수용하고 어떤 것을 완화할지 결정하고, 통제를 적용할 때마다 다시 평가합니다. 새로운 키, 인증서, 인증 기능 자체가 새로운 분석 대상 자산이 됩니다.

위협 모델링. 위 세 번째 단계는 가장 기술적인 작업이며, 잘 정립된 기법이 존재합니다. STRIDE는 위협을 spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege로 분류합니다. 널리 사용되며 대부분의 연결형 제품에 적합합니다. LINDDUN은 개인 데이터를 다루는 제품에 더 넓은 시야를 제공합니다. linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance를 추가합니다. 데이터 보호 체계가 CRA 의무와 겹치는 경우에 유용합니다. PASTA는 사업 목표에서 잔여 리스크 수용까지 7단계 절차를 진행합니다. 공격 양상이 설계를 좌우하는 복잡한 시스템에 유용합니다. 이 중 어느 것도 CRA 전용이 아니며, CRA는 특정 방법을 요구하지 않습니다. 제품의 노출 프로파일에 맞는 것을 선택하십시오.

구체화된 방법론을 찾을 곳. CRA는 방법을 지정하지 않습니다. 독일 연방정보보안청(BSI)은 공개된 CRA 정합 리스크 평가 방법론 중 가장 상세한 기술 지침 TR-03183을 발표했습니다. ENISA는 더 넓은 CRA 이행 지침을 발표합니다.

지원 기간 전체에 걸쳐 평가를 최신 상태로 유지하십시오. 위협 양상, 구성요소, 사용 사례가 바뀌면 평가도 함께 바뀌어야 합니다.

지원 기간 결정

모든 제품에는 정해진 지원 기간이 있어야 하며, 구매 시점에 종료일을 게시해야 합니다. 지원 기간은 취약점을 처리하고, 보안 업데이트를 제공하며, 기술 문서를 최신 상태로 유지하는 창입니다.

얼마나 길어야 하는가

최소 5년입니다. 제품 사용 예상 기간이 5년보다 짧으면 지원 기간은 그 예상 사용 기간과 일치해야 합니다. 더 길면 지원 기간이 그 더 긴 사용을 반영해야 합니다. 라우터, 운영체제, 산업용 제어기 같은 제품은 일반적으로 5년 이상의 지원 기간이 정당화됩니다.

고려해야 할 요소

지원 기간을 정할 때 비례적인 방식으로 다음을 고려하십시오.

- 제품에 대한 합리적인 사용자 기대
- 의도된 목적을 포함한 제품의 성격
- 해당 제품 범주에 대해 이미 제품 수명을 정한 EU 법령
- 시장에 있는 비교 가능한 제품의 지원 기간
- 제품이 의존하는 운영 환경의 이용 가능성
- 핵심 기능을 제공하는 통합 구성요소의 지원 기간
- 제품 범주에 대한 ADCO 또는 위원회의 지침

선택한 기간의 근거는 기술 파일에 있어야 합니다. 시장 감시 기관이 요청할 수 있습니다.

게시해야 할 사항

지원 기간 종료일을 구매 시점에 최소한 월과 연도 단위로, 쉽게 접근 가능한 위치에 표시하십시오. 사용자 인터페이스가 있는 제품에서는 지원 기간 종료에 도달했을 때 알림을 표시하십시오.

업데이트 보관

지원 기간 중 사용자에게 제공된 각 보안 업데이트는 발행 후 최소 10년 또는 남은 지원 기간 중 더 긴 기간 동안 제공 가능한 상태로 유지해야 합니다.

구성요소 실사

제품은 구성요소로 구성됩니다. 일부는 자체 작성, 일부는 구매, 일부는 오픈소스 저장소에서 가져온 것입니다. CRA는 제품을 규제 준수 차원에서 통합체로 다루므로 구성요소도 그 일부입니다. 취약점이 구성요소에 있으면 제품에 있는 것이며, 구성요소가 보안 업데이트를 받지 않으면 제품도 받지 않는 것과 같습니다.

제조업체는 자유·오픈소스를 포함한 제3자 구성요소에 대해 실사를 수행해야 합니다. 구성요소가 제품의 사이버보안을 훼손해서는 안 됩니다.

실사 수준은 구성요소가 가지는 사이버보안 리스크에 비례합니다. 인증을 처리하는 라이브러리와 폰트 렌더링 라이브러리는 같지 않습니다. 리스크에 비례하여 다음 중 하나 이상을 사용하십시오.

1. **구성요소의 CE 마킹을 확인하십시오.** 구성요소 자체가 CRA 제품이고 공급업체가 적합성을 입증했다면 CE 마킹이 구성요소에 있습니다. 해당 표시는 공급업체의 자체 CRA 작업을 증명합니다.
2. **보안 업데이트 이력을 확인하십시오.** 정기적으로 보안 업데이트를 발행하는 구성요소는 수년간 침묵한 구성요소보다 더 좋은 리스크 프로파일을 가집니다. 릴리스 주기와 최근 보안 권고문 기록을 확인하십시오.
3. **취약점 데이터베이스에 대해 구성요소를 확인하십시오.** 유럽 취약점 데이터베이스와 공개 CVE 데이터베이스는 구성요소에 대해 알려진 사실을 알려줍니다. 패치 없는 알려진 CVE는 경고 신호입니다.
4. **추가 보안 시험을 실행하십시오.** 위로 충분하지 않은 경우, 통합 맥락에서 구성요소를 시험하십시오. 정적 분석, 동적 분석, 퍼지 시험, 초점화된 보안 검토 등을 활용합니다.

자체 공급업체가 CRA를 아직 완전히 따르기 전에 통합된 구성요소(따라서 CE 마킹이 아직 제공되지 않는 경우)에는 다른 세 가지 확인 방법을 사용하십시오. 공급망이 따라잡는 동안에도 실사 의무는 중단되지 않습니다.

파일에 보관할 증거

기술 파일은 실사를 주장만 하는 것이 아니라 보여주어야 합니다. 다음을 보관하십시오.

- 제품에 포함된 제3자 구성요소 목록. 버전까지 추적 가능하며 오픈소스를 포함합니다. SBOM이 자연스러운 보관 위치입니다.
- 검토한 공급업체 보안 문서. 보안 정책, 취약점 공개 프로그램, 지원 기간 약속이 포함됩니다.
- 구성요소가 제품에서 안전하게 동작함을 보여주는 통합 시험 보고서.
- 상업적 공급업체와의 계약 또는 SLA에 포함된 보안 조항. 취약점 통지 일정, 지원 기간 약속, 에스컬레이션 규칙 등.
- 구성요소 실사로 한계가 드러났을 때 추가한 제품 수준 완화 기록. 샌드박싱, 권한 제한, 입력 검증, 네트워크 분리 등.

구성요소에서 취약점을 발견한 경우

실사 또는 출시 후 모니터링으로 구성요소에서 취약점을 식별하면 두 가지를 해야 합니다. 첫째, 구성요소를 유지관리하는 사람 또는 단체에 통지하십시오. 구성요소가 오픈소스이면 그것은 상류 프로젝트입니다. 둘째, 다른 취약점과 동일한 일정 안에서 자체 제품에 대해 취약점을 처리하고 시정하십시오. 수정 사항을 직접 개발했다면 가능한 경우 기계 판독 가능 형식으로 유지관리자에게 코드 또는 문서를 공유하십시오.

CRA는 구성요소 유지관리자의 조치를 기다린 후에 자체 사용자를 보호하는 것을 허용하지 않습니다. 제품의 취약점 처리 일정은 상류와 독립적으로 진행됩니다.

13개 제품 보안 요건

모든 디지털 요소 포함 제품은 시장에 출시될 때 13개 기준 보안 요건을 충족해야 하며, 지원 기간 전체에 걸쳐 이를 계속 충족해야 합니다. 이 요건들이 CRA에서 제품 차원의 사이버보안 기준선을 이룹니다.

13개 요건은 다음과 같습니다.

- 시장 출시 시점에 알려진 악용 가능한 취약점이 없을 것
- 즉시 사용 가능한 안전한 기본 설정
- 사용자 선택 해제를 포함한 자동 업데이트 등 보안 업데이트
- 무단 접근 방지
- 저장, 전송, 처리되는 데이터의 기밀성
- 데이터, 펌웨어, 설정의 무결성
- 데이터 최소화
- 서비스 거부 공격 대응을 포함한 가용성과 복원력
- 다른 연결 기기 또는 네트워크에 대한 부정적 영향 최소화
- 외부 인터페이스를 포함한 제한된 공격 표면
- 악용 완화를 통한 사고 영향 감소
- 사용자 선택 해제 가능한 보안 관련 활동 기록
- 안전하고 영구적인 데이터 삭제와 이전성

각 요건은 가이드 뒤쪽에서 실무적 의미와 파일에 보관해야 할 증거를 함께 상세히 다룹니다.

8개 취약점 처리 요건

제조업체는 제품의 지원 기간 전체에 걸쳐 운영되는 취약점 처리 절차도 갖춰야 합니다.

1. 취약점의 식별과 문서화(SBOM 포함)
2. 리스크 관리와 지체 없는 보안 업데이트
3. 정기적인 보안 시험
4. 보안 업데이트 및 취약점 공개 통지
5. 조정된 취약점 공개(CVD) 정책
6. 취약점 공유 및 신고 연락처
7. 안전한 업데이트 배포 메커니즘
8. 안내 메시지를 포함한 무상 보안 업데이트

제14조 신고 일정

이 의무는 **2026년 9월 11일**부터 적용됩니다. 적용 대상 디지털 요소 포함 제품의 제조업체에 적용되며, **2027년 12월 11일** 전에 시장에 출시된 제품도 포함합니다. 영세기업과 소기업이 신고 의무에서 일반적으로 면제되는 것은 아닙니다. 소기업에 대한 과징금 완화는 좁은 범위에서, **24시간 조기 경고 기한**에만 관련됩니다.

CRA는 취약점 상태를 세 단계로 구분합니다.

- **취약점:** 악용될 수 있는 모든 약점
- **악용 가능한 취약점:** 실제 환경에서 사용 가능한 약점
- **적극적으로 악용된 취약점:** 공격에 사용된 사실이 확인된 약점

시계가 언제 시작되는가

신호가 도착하는 순간 시계가 시작되지는 않습니다. 시계는 초기 평가를 마치고, 자사 제품의 취약점이 적극적으로 악용되고 있거나 중대한 사고가 제품 보안을 침해했다는 합리적인 정도의 확신을 가진 시점부터 시작됩니다. 강조점은 전체 조사 종료를 기다리는 것이 아니라 신속한 초기 평가에 있습니다. 고객, 연구자, 당국, 그 밖의 제3자가 잠재 문제를 제기하면 지체 없이 평가하고, 그 평가가 합리적인 확신을 제공하는 즉시 시계를 시작하십시오.

적극적으로 악용된 취약점을 탐지한 경우 다음 신고 일정이 적용됩니다.

기한	필요한 조치	신고 위치
24시간 이내	적극적 악용에 관한 조기 경고	각국 CSIRT를 거쳐 ENISA
72시간 이내	취약점 통지: 영향을 받는 제품, 악용과 취약점의 개요, 완화 조치, 사용자가 취할 시정 조치, 필요한 민감도 표시	각국 CSIRT를 거쳐 ENISA
시정 또는 완화 조치가 제공된 후 14일 이내	최종 보고: 취약점 설명, 심각도, 영향, 악의적 행위자에 관한 이용 가능한 정보, 보안 업데이트 또는 그 밖의 시정 조치 세부 내용	각국 CSIRT를 거쳐 ENISA

제품 보안에 영향을 주는 **중대한 사고**를 탐지한 경우 다음 신고 일정이 적용됩니다.

기한	필요한 조치	신고 위치
24시간 이내	조기 경고. 사고가 불법 또는 악의적 행위에 의한 것으로 의심되는지도 포함	각국 CSIRT를 거쳐 ENISA
72시간 이내	사고 통지: 사고의 성격, 초기 평가, 완화 조치, 사용자가 취할 시정 조치, 필요한 민감도 표시	각국 CSIRT를 거쳐 ENISA
72시간 통지 후 1개월 이내	최종 보고: 자세한 사고 설명, 심각도, 영향, 가능성 있는 위협 또는 근본 원인, 적용했거나 진행 중인 완화 조치	각국 CSIRT를 거쳐 ENISA

알게 되는 내용에 따라 통지를 갱신합니다

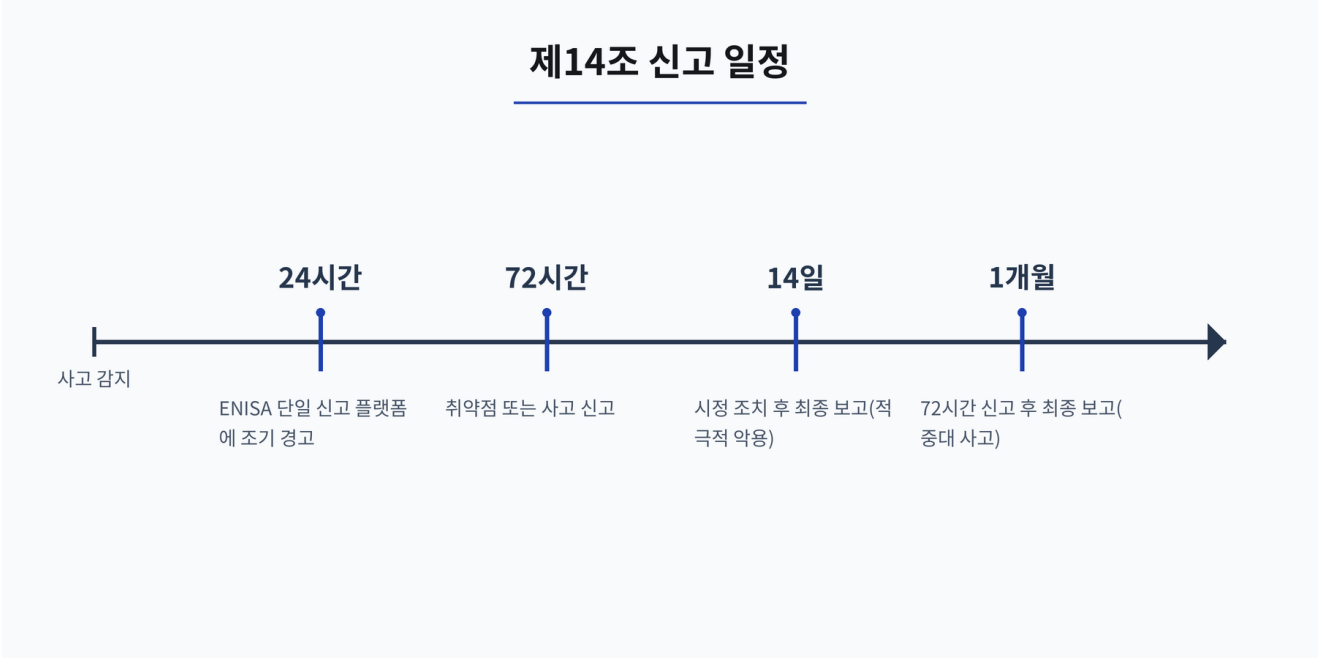
24시간, 72시간, 14일(또는 1개월) 제출은 별도 신고가 아니라 같은 통지의 단계입니다. 각 단계는 이전 단계에서 아직 확보되지 않았던 정보를 추가합니다. 조정자로 지정된 CSIRT는 어느 시점에서든 중간 업데이트를 요청할 수도 있습니다. 이미 제공한 정보를 반복할 필요는 없습니다.

신고는 **CRA 단일 신고 플랫폼**을 통해 제출됩니다. 제조업체의 주된 회원국 컴퓨터 보안 사고 대응팀(CSIRT)을 거쳐 라우팅되며 ENISA에도 동시에 접근 권한이 제공됩니다.

사용자에게 알리기

인지 후 영향을 받는 사용자에게, 그리고 적절한 경우 모든 사용자에게 취약점 또는 사고와 자체적으로 적용할 수 있는 리스크 완화 및 시정 조치를 알려야 합니다. 공개 공개와는 다른 의무입니다. 사용자가 자기를 보호하기 위해 필요한 정보를 리스크에 비례하여 전달해야 합니다. 민감하거나 필수적인 환경에서 사용되는 제품의 경우, 취약점이 완화되지 않은 동안에는 상세한 기술 정보를 관련 고객에게 한정해 제공하십시오. 조기에 공개된 세부 정보는 악용을 더 쉽게 만들 수 있습니다.

취약점이 시정되거나 완화된 뒤에는 더 폭넓은 공개가 적절해질 수 있습니다. 사용자가 자기 제품이 더 이상 영향을 받지 않는지 확인하고 일반적 인식을 높이는 데 도움이 됩니다. 세부 수준과 시점은 잔여 리스크에 비례하도록 유지하십시오. 적시에 사용자에게 알리지 않으면, CSIRT가 적절하고 필요하다고 판단하는 경우 직접 정보를 제공할 수 있습니다.



적극적으로 악용된 취약점	
24시간	조기 경고
72시간	취약점 통지
시정 조치 후 14일	최종 보고

중대한 사고	
24시간	조기 경고
72시간	사고 통지
72시간 통지 후 1개월	최종 보고

제품이 적합성을 갖추지 못한 경우의 시정 조치

시장에 출시한 제품 또는 자체 절차가 CRA의 필수 사이버보안 요건에 부합하지 않는다는 사실을 알게 되거나 그렇게 믿을 만한 이유가 있는 경우, 즉시 조치해야 합니다. 이 의무는 시장 출시 시점부터 지원 기간 전체에 걸쳐 적용됩니다.

세 가지 선택지

1. **적합성을 갖추도록 조치.** 제품 또는 절차를 수정합니다. 소프트웨어 제품에서는 보통 보안 업데이트 또는 절차 변경에 해당합니다. 지원되는 버전에 수정을 적용합니다.
2. **철회.** 시장에서 제품 제공을 중단합니다. 재고를 보유한 공급망, 소매업체, 통합 사업자, 리셀러에서 회수합니다.
3. **리콜.** 이미 보유한 사용자로부터 제품을 회수합니다. 사용자에 대한 사이버보안 리스크가 중대하고 수정 또는 철회만으로 충분하지 않은 경우 사용합니다.

선택은 리스크에 비례하며 정해진 순서가 아닙니다. 작동하는 수정이 있는 패치 가능한 취약점은 보통 적합성 조치를 의미합니다. 현장에서 안전하게 수정할 수 없는 제품은 보통 철회를 의미하며, 활발하게 사용 중이고 중대한 리스크가 있다면 리콜을 의미합니다.

그 외에 해야 할 일

- 부적합이 적극적으로 악용된 취약점 또는 중대한 사고에 해당하는 경우 **제14조 신고 체계에 따른 통지**를 수행합니다. 신고 일정은 위에 정리되어 있습니다.
- 부적합과 사용자가 직접 적용할 수 있는 시정 조치에 대해 **사용자에게 알립니다.** 비례 규칙은 위 사용자에게 알리기를 참고하십시오.
- 시장 감시 기관의 합리적 요청에 **협력합니다.** 기관이 읽을 수 있는 언어로 기술 문서를 제공하는 것도 포함됩니다.
- **증거를 보존합니다.** 무엇을 발견했고, 언제 발견했으며, 무엇을 했고, 사용자와 당국에 어떻게 알렸는지를 보여주는 기록을 보관합니다. 기술 문서와 EU 적합성 선언은 시장 출시 후 최소 10년 또는 전체 지원 기간 중 더 긴 기간 동안 제공 가능한 상태로 유지되어야 합니다.

제품 문서 요건

문서는 제품이 시장에 출시된 후 **최소 10년** 또는 **전체 지원 기간** 중 더 긴 기간 동안 보관해야 합니다. 요약 수준에서 기술 문서는 다음 8개 증거군이 필요합니다.

1. 일반 제품 설명
2. SBOM을 포함한 설계, 개발, 생산 세부 정보
3. 사이버보안 리스크 평가
4. 지원 기간 결정
5. 적용한 조화 표준과 사양
6. 시험 보고서
7. EU 적합성 선언
8. 전체 SBOM(시장 감시 기관 요청 시)

적합성 평가 경로 체크리스트

위의 분류표로 경로를 식별하십시오. 그런 다음 적용한 표준, 사양, 인증 체계 또는 인증기관 증거와 함께 경로 결정을 기술 파일에 보관하십시오.

하나의 사례. 같은 단계 구조가 보안 카메라뿐 아니라 모든 디지털 요소 포함 제품에 적용됩니다.

제품 보안 요건

a. 시장 출시 시점에 알려진 악용 가능한 취약점이 없을 것

처리되지 않은 공개 악용 가능 취약점을 가진 채 출하하지 마십시오. 알려진 취약점은 공개 데이터베이스, 공급업체 통지, 고객 신고, 자체 내부 추적 시스템에서 확인될 수 있습니다.

이 요건을 충족하려면 다음을 수행합니다.

- 각 릴리스 전에 Common Vulnerabilities and Exposures(CVE)를 포함한 취약점 데이터베이스를 확인
- 빌드 파이프라인에서 정적·동적 애플리케이션 보안 시험(SAST/DAST) 사용
- 모든 제3자 및 오픈소스 구성요소에 대한 의존성 스캔 수행
- 식별된 각 문제에 대한 리스크 수용 또는 완화 결정을 문서화

b. 안전한 기본 설정

제품은 기본 상태에서 안전하게 사용 가능해야 합니다. 불필요한 서비스를 비활성화하고, 취약한 기본 자격 증명을 피하며, 안전하지 않은 초기 설정 모드는 짧고 통제된 상태로 유지하십시오. 안전한 기본 설정 의무는 서면 합의로 사업 사용자에게 공급되는 맞춤형 제품에서 다르게 정할 수 있으나, 원래의 안전 상태로 돌아가는 경로는 반드시 유지되어야 합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 기본 빌드에서 원격 접근 포트와 디버그 인터페이스 비활성화
- 강력한 기본 인증 메커니즘 적용
- 관리 기능을 권한 있는 사용자에게만 제한
- 사용자 데이터를 제거하면서 모든 설정과 펌웨어를 알려진 안전 상태로 되돌리는 안전한 공장 초기화 구현

c. 사용자 선택 해제를 포함한 자동 업데이트 등 보안 업데이트

제품에는 배포 후 보안 문제를 처리할 수 있는 패치 메커니즘이 필요합니다. 자동 업데이트가 적절한 경우 기본값으로 활성화하고, 사용자가 연기하거나 선택 해제할 명확한 방법을 제공하십시오.

이 요건을 충족하려면 다음을 수행합니다.

- 업데이트 패키지에 대한 암호학적 서명과 무결성 검증 구현
- 롤백 방지와 업데이트 이벤트 기록 제공
- 대기 중인 업데이트를 사용자에게 알리는 통지 시스템 구축
- 명확한 설정 인터페이스를 통해 자동 업데이트 연기 또는 비활성화 허용

d. 무단 접근 방지

접근 통제는 로컬과 원격 인터페이스를 모두 보호해야 합니다. 권한 없는 사용자가 기능, 데이터, 설정, 관리 표면에 도달하지 못하게 하는 것이 목표입니다.

이 요건을 충족하려면 다음을 수행합니다.

- 비밀번호 복잡도 정책과 강력한 기본 자격 증명 적용
- 적절한 경우 다중 인증(MFA) 구현
- 역할 기반 접근 통제(RBAC)와 세션 시간 제한 처리 적용
- 실패한 접근 시도를 기록하고, 이상 징후 탐지로 무단 활동을 표시하며, 해당 이벤트를 검토와 신고용으로 노출

e. 저장, 전송, 처리되는 데이터의 기밀성

민감한 데이터는 저장 중, 전송 중, 처리 중 보호되어야 합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 표준화된 암호화 알고리즘 사용(예: 저장 데이터에는 AES-256, 전송 데이터에는 TLS)
- 안전한 키 관리 관행 적용
- 기밀 데이터를 중요도가 낮은 시스템 구성요소와 분리
- 모든 데이터 접근 이벤트에 대한 감사 로그 유지

f. 데이터, 펌웨어, 설정의 무결성

이 요건은 시스템 자체(펌웨어, 소프트웨어, 설정 파일)와 시스템이 처리하는 데이터(측정값, 제어 명령, 사용자 입력) 모두를 다룹니다.

이 요건을 충족하려면 다음을 수행합니다.

- 신뢰된 코드만 실행되도록 보안 부팅과 서명된 펌웨어 구현
- 런타임 검증으로 변조 시도를 탐지하고 보고
- 암호학적 해시와 디지털 서명으로 데이터 무결성 보호
- 시스템 또는 조직 경계를 넘어 암호화 키를 생성, 배포, 검증할 수 있는 인프라 구축

g. 데이터 최소화

제품의 의도된 목적에 필요한 데이터만 수집·처리하십시오. 개인 데이터와 기술 데이터 모두에 적용됩니다.

이 요건을 충족하려면 다음을 수행합니다.

- 불필요한 데이터 흐름을 식별하기 위한 프라이버시 영향평가 또는 설계 단계 데이터 보호 작업 수행
- 사용되지 않는 원격 측정, 진단, 백그라운드 데이터 수집 제거 또는 선택 사항화
- 상황에 따라 확장 수집을 켜거나 끌 수 있는 설정 가능한 데이터 수집 옵션 구현

h. 서비스 거부 공격 대응을 포함한 가용성과 복원력

사고나 공격 중에도 핵심 제품 기능은 계속 제공되거나 통제된 방식으로 실패해야 합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 서킷 브레이커, 재시도 로직, 폴백 메커니즘, 워치독 타이머 구현
- 리소스 고갈 방지를 위한 리소스 제한 적용
- 서비스 거부 시나리오 방어를 위한 속도 제한과 입력 검증 사용
- 과부하 시도를 차단하기 위한 네트워크 수준 필터링 적용

i. 다른 연결 기기 또는 네트워크에 대한 부정적 영향 최소화

제품은 같은 환경의 다른 시스템을 방해하지 않아야 합니다. 예측 가능하게 동작하고 공유 리소스를 과도하게 사용하지 않아야 합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 트래픽 셰이핑 구현 및 브로드캐스트나 멀티캐스트 사용 제한
- 통신 프로토콜 사양 준수 보장
- 네트워크 플러딩이나 리소스 고갈 같은 방해 동작을 탐지하고 방지하는 자체 모니터링 사용

j. 외부 인터페이스를 포함한 공격 표면 제한

진입점과 노출된 기능을 최소화하십시오. 물리 포트, 무선 인터페이스, API, 디버그 서비스, 불필요한 소프트웨어 구성요소가 포함됩니다.

이 요건을 충족하려면 다음을 수행합니다.

- 운영 빌드에서 사용되지 않는 서비스, 포트, 인터페이스 비활성화
- 시스템 기본값 강화와 사용자 권한 제한
- 소프트웨어 아키텍처를 모듈화하여 구성요소를 서로 격리
- 안전한 소프트웨어 설계 원칙 적용과 위협 모델링을 통해 불필요한 노출 식별 및 제거

k. 악용 완화 조치를 통한 사고 영향 감소

일부 공격은 성공한다고 보고 설계하십시오. 제품 설계는 피해 확산 범위를 제한해야 합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 샌드박싱 또는 컨테이너화를 사용해 시스템 구성요소를 분리된 환경에서 실행
- 중요 기능이 필요한 최소 권한으로 실행되도록 권한 분리 적용
- 한 구성요소의 침해가 전체 시스템 장악으로 이어지지 않도록 설계

l. 사용자 선택 해제를 포함한 보안 관련 활동 기록

접근 시도와 데이터 수정 같은 보안 관련 활동은 모니터링과 감사를 위해 기록해야 합니다. CRA가 요구하는 경우 사용자가 선택 해제할 수 있는 메커니즘도 필요합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 구조화된 로깅 구현(예: 타임스탬프가 포함된 JSON 로그)
- 로그 순환이 있는 로컬 로그 저장소와 원격 로그 스트리밍 옵션 제공
- 로그인 시도, 설정 변경, 소프트웨어 업데이트 같은 이벤트의 이상 징후 모니터링
- 허용되는 경우 로깅을 비활성화할 수 있는 명확한 사용자 대상 메커니즘 제공

m. 안전하고 영구적인 데이터 삭제와 이전성

사용자에게 데이터와 설정을 영구적으로 제거하는 실질적인 방법을 제공해야 합니다. 데이터를 다른 제품 또는 시스템으로 이전하는 경우 그 이전도 안전해야 합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 저장 영역을 덮어쓰거나 키를 암호학적으로 삭제하는 안전 삭제 기능 구현
- 데이터 이전 중 노출을 방지하기 위해 인증되고 암호화된 채널 사용

취약성 처리 요건

1. 취약점 식별과 문서화

제품에 어떤 소프트웨어 구성요소가 있는지, 어떤 알려진 취약점이 그것들에 영향을 미치는지 파악해야 합니다. 소프트웨어 구성요소 명세(SBOM)는 그 재고를 기계 판독 가능한 형태로 제공합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 모든 빌드가 최신 구성요소 재고를 산출하도록 CI/CD 파이프라인에 SBOM 생성을 직접 통합
- 상호운용성을 위해 CycloneDX, SPDX, SWID 같은 확립된 형식 사용
- CISA KEV와 ENISA EUVD 같은 데이터베이스 및 CVE 목록에 대한 자동 취약점 스캔 실행
- 지원 기간 전체에 걸쳐 SBOM을 기술 문서의 일부로 유지하고 시장 감시 기관 요청 시 제공

2. 리스크 관리와 지체 없는 보안 업데이트

취약점이 발견되면 신속히 수정하고 보안 업데이트를 제공하십시오. 가능한 경우 보안 패치를 기능 업데이트와 분리하여 긴급 수정이 신속히 설치되도록 하십시오.

이 요건을 충족하려면 다음을 수행합니다.

- 전체 시스템 업데이트 없이 보안 수정을 배포할 수 있도록 업데이트 메커니즘 설계
- 중요 구성요소를 독립적으로 패치할 수 있도록 소프트웨어와 펌웨어 구조화
- 무결성 검사를 포함한 안전한 채널로 업데이트 제공
- 추적성과 규제 준수 입증을 위해 업데이트 활동 기록 유지

3. 정기적인 보안 시험

보안 시험은 한 번에 끝나는 작업이 아닙니다. 위협, 의존성, 제품 동작이 변하는 동안 제품 수명주기 전체에서 시험하십시오. 리스크 평가가 시험 유형과 빈도를 결정해야 합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 실제 공격을 모의하는 침투 시험 수행
- 보안 약점을 식별하기 위한 정적·동적 코드 분석 적용
- 입력 처리 결함을 드러내기 위한 퍼즈 시험 사용
- 특히 중대한 설계 또는 기능 변경 후 보안 코드 검토와 아키텍처 검토를 공식 일정으로 편성하고 문서화

4. 취약점 접수, CVD 정책 및 권고문

CRA 요약 항목 4, 5, 6에 해당하는 접수, 조정된 공개, 권고문 의무를 다룹니다. 실무에서는 이들이 하나의 워크플로로 운영됩니다.

CRA는 취약점 커뮤니케이션 방식에 대해 세 가지 별도 요건을 둡니다. 사람이 문제를 신고할 수 있는 경로, 조정된 공개 정책, 수정 출시 시 발행하는 권고문입니다. 각 의무가 요구하는 사항은 다음과 같습니다.

접수

신고자에게 명확하고 마찰이 적은 진입 경로를 제공하십시오. 취약점 신고용 가시적인 연락 방법(전용 이메일 또는 웹 양식)을 게시하십시오. PGP 키 게시 등 안전한 통신을 지원하십시오. 이 의무는 자체 제품에 관한 신고와 제품이 포함한 제3자 구성요소에 관한 신고 모두를 포괄합니다.

분류

모든 신고를 인지하고, 추적 시스템에 기록하고, 검토 담당자를 배정하며, 정해진 일정 안에 해결하십시오. 신고자에게 접수 확인과 상태 업데이트를 보내십시오. 문제가 제3자 구성요소에 있을 때는 자체 시정과 병행해 상류 유지관리자에게 라우팅하십시오.

조정된 취약점 공개 정책

신고자와 파트너에 대한 기대치를 정한 CVD 정책을 게시하십시오. 연락 방법, 예상 응답 시간, 자체 약속, 그들에게 요구하는 것이 포함됩니다. 신고자의 기여를 인정하면서 사용자를 보호하는 방식으로 공개를 조정하십시오.

수정 출시 시 권고문

수정이 제공되면 해결된 문제에 대한 권고문을 게시하십시오. CVE 식별자, 영향을 받는 제품 버전, 표준 심각도 등급(예: CVSS), 사용자가 무엇을 해야 하는지에 대한 명확하고 접근 가능한 정보를 포함하십시오. 기술 관리자와 비기술 사용자 모두 이해할 수 있는 언어로 작성하십시오.

공개 공개의 지연

즉시 공개의 사이버보안 리스크가 이익을 능가한다는 정당한 사유가 있는 경우에만, 그리고 사용자가 수정을 적용할 기회를 가질 때까지만 공개 공개를 지연할 수 있습니다. 그 사유를 문서화하십시오.

5. 안전한 업데이트 배포 메커니즘

업데이트 메커니즘은 신뢰할 수 있고 변조에 견딜 수 있어야 합니다. 자동 업데이트가 기술적으로 실행 가능한 경우, 사용자가 노출된 상태로 남는 시간을 줄여줍니다.

이 요건을 충족하려면 다음을 수행합니다.

- 안전한 채널로 업데이트를 전송하고 디지털 서명으로 검증
- 불완전하거나 손상된 설치를 방지하는 방식으로 업데이트 적용
- 차등 또는 모듈식 업데이트를 사용해 중단을 줄이고 수정을 더 신속히 전달
- 사용자 또는 관리자가 업데이트 상태를 확인할 수 있도록 업데이트 로그 유지

6. 안내 메시지를 포함한 무상 보안 업데이트

보안 업데이트는 신속하고 추가 비용 없이 제공해야 합니다. 맞춤형 사업 제품에 별도 합의가 있는 경우만 예외입니다. 각 업데이트에는 무엇이 바뀌었고 무엇을 해야 하는지를 사용자에게 알리는 명확한 안내 메시지가 필요합니다.

이 요건을 충족하려면 다음을 수행합니다.

- 제품 맥락에 따라 사용자에게 직접 알리거나 업데이트를 자동 적용할 수 있는 배포 시스템 유지
- 기술 사용자와 비기술 사용자 모두 이해할 수 있는 언어로 안내 메시지 작성
- 관련성이 있는 경우 안내 메시지에 심각도 정보 포함
- 업데이트 적용, 설정 변경, 침해 징후 모니터링 등 사용자가 취해야 할 조치 안내
- 수정이 이미 존재하는 동안 사용자가 노출된 상태로 남지 않도록 보안 업데이트를 가용해지는 즉시 배포
- 제조업체가 통제하는 채널로 권고문을 게시하고 제품 지원 페이지에서 그것으로 연결

무상 의무와 지체 없는 배포 의무는 선언된 지원 기간 전체에 걸쳐 적용됩니다. 맞춤형 예외는 상업적 조건만 변경하며, 안내 메시지 의무는 그대로 유지됩니다.

기술 파일에 포함할 내용

기술 문서

기술 문서는 CRA 규제 준수의 중심 증거입니다. 필수 사이버보안 요건을 충족하기 위해 사용한 설계, 기술, 절차적 조치를 다뤄야 합니다. **시장 출시 전**에 존재해야 하며 **지원 기간** 전체에 걸쳐 최신 상태로 유지되어야 합니다.

엔지니어링 워크플로에 따른 기술 파일 증거

단계 1	**범위와 분류**	제품 목적, 의도된 사용, 시장 출시 결정, 제품 분류, 표준 적용 경로.
단계 2	**아키텍처와 리스크**	아키텍처, 데이터 연결, 사용 조건, 리스크 평가, 완화 조치.
단계 3	**구성요소와 SBOM**	기계 판독 가능 SBOM, 제3자 구성요소, 공급업체 입력, 취약점 추적.
단계 4	**빌드, 시험, 업데이트**	안전한 기본값, 하드닝, 시험 보고서, 안전한 업데이트 메커니즘, 안내 메시지.
단계 5	**출시와 지원**	사용자 설명서, EU 선언, CE 증거, 지원 기간 근거, 업데이트 기록.

기술 파일에는 8개 필수 구성요소가 있습니다. 이들이 함께 **제품이 무엇인지**, **어떻게 빌드되고 시험되었는지**, **어떤 리스크가 고려되었는지**, **어떤 표준이 적용되었는지**, **시장 출시 후 어떻게 지원될지**를 설명합니다. 법령 표제를 그대로 복사할 필요는 없지만 각 주제는 반드시 다뤄져야 합니다.

번호	구성요소	포함할 내용
1	일반 제품 설명	의도된 목적과 기능, 관련 소프트웨어 버전, 사진 또는 도해(하드웨어의 경우), 사용자 정보와 설명서
2	설계, 개발, 생산 세부 정보	아키텍처 설명(구성요소와 상호작용), 소프트웨어 구성요소 명세(SBOM), 취약점 처리 절차(CVD 정책, 연락 지점, 안전한 업데이트 메커니즘), 검증을 포함한 생산 및 모니터링 절차
3	사이버보안 리스크 평가	문서화된 제품 리스크 분석, 각 필수 사이버보안 요건이 제품에 적용되는 방식 설명, 식별된 리스크 완화
4	지원 기간 결정	사용자 기대, 비교 가능한 제품, 법령 지침 등 지원 기간을 정하는 데 사용한 요소의 문서화
5	적용한 조화 표준과 사양	적용한 조화 표준, 공통 사양 또는 EU 인증 체계 목록. 전체 적용 또는 부분 적용 여부 표시. 표준을 적용하지 않은 경우 대체 해결책
6	시험 보고서	제품과 취약점 처리 절차 모두에 대한 적합성 증거
7	EU 적합성 선언	기술 파일을 CE 마킹 의무와 연결하는 선언서 사본
8	전체 SBOM(요청 시)	시장 감시 기관은 규제 준수 확인을 위해 전체 SBOM을 요청할 수 있음

하나의 통합 기술 파일은 CRA와 그 밖의 적용 가능한 EU 법령(예: 무선 기기 지침 또는 ESPR)을 함께 다룰 수 있습니다. 다만 적용되는 모든 의무가 포함되어야 합니다.

EU 적합성 선언

EU 적합성 선언은 제품이 적용 가능한 CRA 사이버보안 요건을 충족한다는 제조업체의 공식 진술입니다. 각 선언에는 다음 내용이 포함되어야 합니다.

- 제품명, 유형, 고유 식별자
- 제조업체 이름과 주소(또는 공인대리인)
- 제공자의 단독 책임 진술
- 추적 가능성을 보장하는 제품 설명(선택적으로 이미지 포함)
- 관련 EU 법령에 대한 적합성 명시
- 사용한 조화 표준, 사양, 인증에 대한 참조
- 관여한 인증기관의 세부 정보(이름, 번호, 절차, 인증서 번호)
- 서명란: 장소, 날짜, 이름, 직책, 서명

서명된 선언은 법적 구속력을 가지며, 사이버보안 규제 준수에 대한 제조업체의 전적인 책임을 확인합니다.

간소화 선언은 포장 또는 설명서에 다음 형식으로 사용 가능합니다. "[제조업체]는 제품 [유형/명칭]이 EU 규정 2024/2847을 준수함을 선언합니다. EU 적합성 선언 전문은 다음 웹 주소에서 확인 가능합니다: [웹 주소]." 이 간소화 형식은 투명성을 유지하면서 문서 부담을 줄이며, 소규모 제조업체나 다제품 포트폴리오에 특히 유용합니다.

사용자 정보와 설명서

사용자 정보와 설명서는 합법적인 시장 출시의 조건입니다. 제조업체는 설명서를 **최소 10년** 또는 **전체 지원 기간** 동안 제공 가능한 상태로 유지해야 합니다. 수입업체와 유통업체는 제품을 출시하거나 공급하기 전에 설명서가 존재하고, 최신이며, 올바른 EU 언어로 제공되는지 확인해야 합니다.

사용자 설명서에는 다음 내용이 포함되어야 합니다.

- 제조업체의 신원과 연락처
- 취약점 신고를 위한 단일 연락 창구
- 제품 식별, 의도된 목적, 안전한 사용 맥락
- 알려졌거나 예측 가능한 사이버 리스크
- EU 적합성 선언 링크
- 지원 조건과 명확한 지원 종료일
- 설정, 업데이트, 안전한 사용, 폐기, 적용 가능한 경우 통합과 SBOM 접근에 관한 단계별 보안 지침

적합성 평가 경로 선택

모듈 A: 자체 평가

모듈 A(내부 통제)는 제품이 필수 사이버보안 요건을 준수한다는 점을 자체 인증할 수 있게 하며, 설계와 생산 모두에 대한 전적인 책임을 집니다. 이 경로는 기본(미분류) 제품 제조업체에 제공됩니다. 중요 제품 Class I의 경우, 관련 조화 표준, 공통 사양 또는 유럽 사이버보안 인증 체계가 이용 가능하고 CRA 경로 규칙이 요구하는 대로 적용된 경우에만 제공됩니다.

모듈 A에서는 다음을 수행해야 합니다.

- 포괄적인 기술 문서 준비
- 제품의 설계, 생산 절차, 사이버보안 메커니즘, 취약점 처리 절차 상세 기록
- 제품 수명주기 전반에 걸친 지속적인 규제 준수 책임 유지
- 제품 운영 기간 중 보안 업데이트와 취약점 관리 계획 구현
- 최소 10년 동안 기록 제공 가능 상태 유지

모듈 B와 C: 제품 중심 평가

모듈 B와 C는 특정 제품 유형에 대한 제3자 검증이 필요한 경우 적용됩니다. 제조업체가 관련 조화 표준, 공통 사양 또는 인증 체계를 적용하지 않았거나, 일부만 적용했거나, 적용할 수 없는 중요 제품 Class I에 적용됩니다. 중요 제품 Class II의 경우 제조업체는 모듈 B+C, 모듈 H 또는 substantial 이상의 보증 수준을 가진 적용 가능한 유럽 사이버보안 인증 체계를 사용해야 합니다.

모듈 B(EU 형식 심사): 인증기관이 대표 제품 샘플과 관련 기술 문서를 심사합니다. 모든 필수 사이버보안 요건에 대한 적합성을 검증하고, 제품 설계가 CRA 기준을 충족하면 EU 형식 심사 인증서를 발급합니다.

모듈 C(형식 적합성, 생산 통제): 제조업체는 모든 생산 단위가 모듈 B에 따라 인증된 승인 형식과 일치하도록 보장합니다. 제조업체는 CE 마킹을 부착하고, EU 적합성 선언을 발행하며, 최소 10년 동안 기록을 제공 가능한 상태로 유지합니다. 모듈 B와 C를 함께 사용하면 특정 제품 모델의 기술 규제 준수와 각 생산 배치의 승인 설계 일관성을 보장합니다.

모듈 H: 절차 중심 평가(전체 품질 보증)

모듈 H(전체 품질 보증)는 개별 제품 시험보다 제조업체의 내부 품질 시스템 전체에 초점을 둡니다. 중요 제품 Class I 및 Class II에 제공됩니다. 핵심 제품은 관련 조건이 충족되는 경우 인증 경로를 사용하며, 조건이 충족되지 않으면 중요 제품 Class II에 제공되는 동일 경로를 사용합니다.

모듈 H에서는 다음을 수행해야 합니다.

- 전체 제품 범주의 설계, 개발, 생산, 시험, 취약점 처리를 포괄하는 품질 시스템 수립과 유지
- 품질 시스템을 인증기관에 제출하여 평가와 승인을 받음
- 지속적 규제 준수 확인을 위한 인증기관의 계속 감시(감사, 검사, 절차 검토) 수락

승인 후에는 각 개별 제품 유형에 대한 인증기관 심사를 반복하지 않고 해당 품질 시스템에서 생산된 모든 제품에 대해 적합성 선언을 발행할 수 있습니다.

경로의 핵심 차이는 다음과 같습니다.

- 모듈 B+C: 제품에 초점을 둡니다. 대표 제품 유형이 시험되고 인증됩니다.

• 모듈 H: 절차에 초점을 둡니다. 제조업체의 설계 및 생산 시스템 전체가 인증되고 모니터링됩니다.

적합성 평가 경로

A

모듈

자체 평가

기본 제품 및 조화 표준, 공통 사양 또는 인증 체계가 전부 적용된 중요 제품 Class I. 제조업체가 설계와 생산에 전적인 책임을 집니다.

B+C

모듈

형식 및 생산

적용 가능한 표준이 없는 중요 제품 Class I과 중요 제품 Class II 경로의 일부에서 필요. 인증기관이 대표 형식을 심사하고, 제조업체는 모든 생산 단위의 일치를 보장합니다.

H

모듈

전체 품질 보증

중요 제품 Class I 및 II에 제공. 인증기관이 제조업체의 설계, 개발, 생산, 시험, 취약점 처리 시스템 전부를 처음부터 끝까지 승인하고 감사합니다.

시장 출시 흐름

EU 규제 환경에서의 CRA

CRA는 단독으로 존재하지 않습니다. 제조업체의 실무적 질문은 단순합니다. CRA 작업이 다른 EU 체계에서 어디까지 재사용 가능한가, 그리고 어디에서는 별도 의무를 병행해 수행해야 하는가입니다.

CRA 작업을 재사용할 수 있는 영역

- **고위험 AI 시스템(AI Act, 규정 2024/1689).** 제품이 CRA 범위에 들면서 고위험 AI 시스템인 경우, CRA의 필수 사이버보안 요건을 충족하는 것은 EU 적합성 선언이 포괄하는 범위 내에서 AI Act의 사이버보안 요건을 충족한 것으로 간주됩니다. 적합성 평가 절차는 원칙적으로 AI Act 체계를 따르며, 중요 및 핵심 CRA 제품에 대한 예외가 적용됩니다. CRA 사이버보안 리스크 평가에는 데이터 오염, 적대적 공격 같은 AI 특유의 리스크가 반영되어야 합니다.
- **다른 EU 법령과의 통합 리스크 평가.** CRA는 사이버보안 리스크 평가가 다른 EU 법령에서 요구하는 더 넓은 리스크 평가의 일부가 되도록 명시적으로 허용합니다. 제품이 두 체계 모두에 해당하는 경우 평가 산출물 하나가 두 가지 규제 용도에 사용됩니다.
- **여러 체계를 아우르는 단일 기술 파일.** 기술 파일 섹션에서 이미 짚었듯이, 단일 통합 기술 파일이 CRA와 그 밖의 적용 가능한 EU 법령을 함께 다룰 수 있습니다. 각 체계의 의무가 모두 다뤄지는 한 그렇습니다. 같은 제품이 무선기기 지침, 지속가능제품 에코디자인 규정 또는 다른 제품 법령 하의 문서도 필요로 하는 경우 유용합니다.
- **재정비, 정비, 수리의 공통 정의.** CRA는 이들 정의를 지속가능제품 에코디자인 규정에서 가져옵니다. 어떤 서비스 작업이 실질적 변경에 해당하는지 분석할 때 에코디자인 정의가 기준이 되며, CRA 고유 용어가 따로 있지 않습니다.

별도 의무가 남는 영역

- **AI Act의 그 밖의 부분.** 사이버보안은 AI Act의 일부일 뿐입니다. 리스크 분류, 투명성, 데이터셋 거버넌스, 인간 감독, AI 동작의 출시 후 모니터링 등 다른 영역은 AI Act 의무이며 CRA가 다루지 않습니다. CRA 정합 사이버보안은 AI Act 전체에 대한 적합성 추정이 아닙니다.
- **에코디자인과 디지털 제품 여권 내용.** 에너지 효율, 내구성, 수리 가능성 점수, 디지털 제품 여권의 지속가능성 내용에 대한 에코디자인 요건은 CRA 범위가 아닙니다. CRA 증거 흐름은 에코디자인 작업과 나란히 놓일 수 있지만 그것을 대체하지는 않습니다.
- **Data Act의 IoT 데이터 접근 권리.** Data Act는 사용자가 연결형 제품이 생성하는 데이터에 접근·공유·이전할 수 있는 계약상 권리를 부여합니다. CRA는 그 데이터의 보안을 다루며, 접근 권리 체계를 정하지 않습니다. 의무가 다르고, 증거도 다릅니다.
- **결함 제품에 대한 제조물 책임.** 제조물 책임 지침(2024/2853)은 결함 제품으로 인한 손해에 대한 제조업체의 엄격책임을 유지합니다. CRA는 출시 후 보안 업데이트의 결여가 책임을 유발할 수 있는 결함이 될 수 있음을 명시합니다. 계약, 보험, 사고 대응 플레이북은 CRA 적합성과 별개로 이러한 노출을 고려해야 합니다.

CRA Evidence의 컨설팅 지원

CRA Evidence는 EU 사이버복원력법 의무를 검증 가능한 제품 증거로 전환하며, 규제 준수 플랫폼과 기술 컨설팅을 함께 제공합니다.

플랫폼

CRA 준비의 근거가 되는 증거를 한곳에서 관리합니다.

- **SBOM과 구성요소 재고:** 제품 버전·릴리스별 CycloneDX, SPDX, HBOM 기록
- **CI/CD 증거 자동화:** 스캔, SBOM 업로드, 릴리스 게이트, 감사 기록을 위한 CLI·API 워크플로
- **서명된 SBOM과 출처:** 버전 관리 증거, 공급업체 증명, 실사 기록
- **취약점 운영:** CISA KEV, EPSS, VEX, 모니터링, 분류, 신고 워크플로
- **기술 파일과 CE 증거:** EU 선언 기록, 보관 이력, QR 연결 제품 규제 준수 여권

기술 컨설팅

CRA 의무를 제품, 아키텍처, 릴리스 절차, 공급업체 모델에 대한 엔지니어링 결정으로 전환하도록 지원합니다.

- **기술 준비 스프린트:** 필수 요건 격차 검토, 아키텍처 권고, 우선순위 실행 계획
- **CRA 프로그램 리드:** 책임 모델, 의무 추적, 증거 마일스톤, 기술 파일 유지
- **당국 및 사고 대응 계획:** 신고 워크플로, 문의 대응 플레이북, 사용자 커뮤니케이션, 증거 패키지 준비
- **규제 정렬:** CRA 증거를 Data Act, ESPR, AI Act, RED 및 분야별 요구사항과 연결
- **기술 워크숍:** 제품, 엔지니어링, 보안, 규제 준수, 공급업체 팀과의 원격 또는 현장 세션

도구에 종속되지 않습니다. CRA Evidence는 CycloneDX, SPDX, Grype, Trivy, CI/CD 파이프라인, 이슈 트래커와 통합됩니다.

실무적인 첫 단계

제품군 하나를 선택하십시오. 담당자, 적용 범위 결정, SBOM, 취약점 워크플로, 기술 파일 격차, 릴리스 증거를 정리하십시오. 규제 준수를 별도 프로젝트로 만들지 않고 팀에 구체적인 CRA 기준선을 제공할 수 있습니다.

CRA Evidence의 전체 지원 범위는 craevidence.com에서 확인할 수 있습니다. 가격과 플랜 옵션은 craevidence.com/pricing에서 확인할 수 있습니다.

이 가이드는 CRA Evidence가 작성했으며 EU 규정 2024/2847을 기준으로 합니다. 정보 제공 목적이며 법률 자문이 아닙니다.