WHITEPAPER

사이버 보안:
RED, PSTI, AND CRA

제품 사이버 보안과 관련한 제조업체 의무 사항 이해하기

목 차 (CONTENTS)

element

사이버 보안: RED, PSTI 및 CRA

저자 서문

우리 중 대다수는 사이버 보안이라는 개념에 익숙합니다. 최소한 IT 팀으로부터 고유한 비밀번호 설정, 업무용 PC(워크스테이션) 잠금 유지, 의심스러운 이메일 링크 클릭 시 주의와 같은 모범 사례를 따르라는 안내를 받아본 경험이 있기 때문입니다. 하지만 이러한 가이드는 개인의 행동이나 기업의 정책 및 관행에 적용되는 것이며, 우리가 사용하는(또는 제조하는) 제품 자체가 반드시 안전하다는 것을 의미하지는 않습니다.

이러한 점을 고려하여, 제품 사이버 보안을 전문적으로 다루는 여러 법안이 도입되고 있습니다. 따라서 본 백서에서 언급하는 '사이버 보안'이라고 언급할 때, 정확히는 "전기 및 전자 장비의 제품 사이버 보안(Product Cyber Security of Electrical and Electronic Equipment)"을 의미합니다. 다만 표현이 다소 길어, 본 백서에서는 편의상 "사이버 보안"이라는 용어를 사용합니다.

또한 본 백서는 독자가 CE 마킹 및 UKCA 마킹 절차, 시험 표준, 인증기관(Notified Body)의 역할 등에 대해 어느 정도 사전 지식을 갖추고 있다는 전제하에 작성되었습니다. 필요하신 경우, 관련 주제를 다시 확인할 수 있도록 당사 리소스 허브(element.com/nucleus)에 다른 백서 및 아티클이 준비되어 있습니다.

마이클 더비(Michael Derby)

전)기술 이사 및 규제 승인(Technical Director - Regulatory Approvals)

마이클 더비는 제품 개발 및 인허가(승인) 분야에서 35년 이상의 경력을 보유하고 있습니다. 현재는 제조업체가 무선 장비를 시장에 출시할 수 있도록 지원하는 업무를 전문으로 하고 있습니다.

Element의 Connected Technology & Mobility 그룹에서 기술 이사로서, 마이클은 무선 기기 시험, 인증(Certification) 및 인허가(Authorization)와 관련된 모든 주제에 대해 지원을 제공합니다. 또한 Element 내에서 신규 이니셔티브 및 성장 과제를 책임지며, 새로운 기회 발굴하고 솔루션을 도출하며, 신규 서비스 수립 및 직원 교육을 담당하고 있습니다.

알렉스 투히(Alex Toohie)

기술 솔루션 매니저(Technical Solution Manager)

알렉스 투히는 10년 이상 규제 준수(Regulatory Compliance) 분야에서 경력을 쌓아왔으며, Element의 Connected Technology & Mobility 그룹뿐 아니라 업계에서는 무선 침입 감지 및 화재 경보 시스템 분야의 글로벌 선도 기업에서 컴플라이언스 매니저(Compliance Manager)로 근무한 바 있습니다.

Element의 기술 솔루션 매니저로서 알렉스는 UKCA 및 CE 마킹(RED, EMCD, CPR, ATEXD, RoHSD 등 포함), FCC 및 ISED, 그리고 급변하는 글로벌 제품 사이버 보안 요구사항에 대한 풍부한 경험을 바탕으로, 제조업체가 복잡하고 다양한 무선 기기에 대해 가장 효과적이고 비용 효율적인 인증 경로를 찾을 수 있도록 지원합니다.


57 bpm
00:00
06:00
12:00
18:00
24:00
101
49
Sessiz -- bpm

사이버 보안 법규 소개

사이버 보안 법규

본 백서에서는 사이버 보안과 관련하여 새롭게 도입되고 있는 3가지 법규를 다룹니다. 이들 법규는 각각 다양한 주제를 포괄하도록 설계되어 있으며, 각 주제는 이미 알려진 사이버 공격 방식 또는 잠재적인 보안 취약점과 직접적으로 연관되어 있습니다.

주요 내용은 다음과 같습니다.

- 제품이 시장에 공급될 때 알려진 취약점(Known vulnerabilities) 을 포함하지 않도록 보장
- 제품이 기본적으로 안전한 상태(Secure by default) 를 유지하도록 하고, 필요 시 사용자가 제품을 해당 안전 기본 상태로 복구할 수 있는 옵션 제공
- 취약점이 확인될 경우 제품을 업데이트하거나 보안 강화를 수행할 수 있는 메커니즘 제공
- 무단 또는 악의적 접근을 방지하기 위해, 제품이 적절한 접근 제어(Access control) 및 인증(Authentication) 메커니즘을 갖추도록 설계·제조
- 제품이 처리하는 민감 정보가 적절한 암호기술(Cryptography) 등을 통해 안전하게 저장·전송되도록 보장
- 장비 기능에 필요한 경우에만 데이터를 처리하고, 불필요하게 데이터를 수집·저장하지 않으며, 더 이상 필요하지 않은 정보는 사용자가 영구 삭제할 수 있도록 제공
- 제품의 공격 표면(Attack surface) 을 최소화(예: 불필요한 인터페이스 비활성화 또는 사용자가 비활성화할 수 있도록 제공). 특히 장비 기능에 필수적이지 않은 네트워크/무선 인터페이스에 대해 이를 적용
- 취약점이 발견될 때 사용자가 이를 보고할 수 있는 명확한 신고 경로를 제공하고, 해당 취약점을 해결하겠다는 대응 약속(필요 시 업데이트 제공 및 영향을 받는 제3자와 잠재 취약점 정보 공유 포함)

제조업체가 제품에 위와 같은 조치를 반영하면, 해당 제품이 연관된 사이버 공격의 발생 가능성과 피해 규모(심각도) 를 줄일 수 있습니다.

예를 들어 다음과 같은 공격을 예방·완화하는 데 도움이 됩니다.

- 네트워크로 연결된 장비가 보안 네트워크 침입의 진입점(Point-of-entry)으로 악용되어 정보가 탈취되는 경우
- IoT 장비가 다수의 기기로 구성된 봇넷(botnet) 에 편입되어 분산 서비스 거부(DDoS) 공격에 악용되는 경우
- 보안 카메라가 외부에서 접근·장악되어 절도 등 범죄 활동을 돕는 데 사용되는 경우
- 연결형 스마트 기기가 개인식별정보(PII) 또는 금융 데이터 탈취, 혹은 위치 정보 모니터링에 악용되는 경우

이러한 문제들을 해결하기위해 다양한 법안들이 도입되고 있습니다.

영국은 2022년에 제품 보안 및 통신 인프라 법(Product Security and Telecommunications Infrastructure Act, “PSTI Act”) 을 제정했으며, 2024년에는 이에 수반되는 제품 보안 및 통신 인프라 규정(Product Security and Telecommunications Infrastructure Regulations, “PSTI Regulations”) 을 발표했습니다.

이 두 법규를 통칭하여 “PSTI 제도(PSTI Regime)” 라고 합니다.

EU는 2021년에 위임 규정(Delegated Regulation) (EU) 2022/30 을 채택했으며, 이를 통해 무선장비지침(Radio Equipment Directive 2014/53/EU, “RED”) 하의 세 가지 필수 요구사항이 시행됩니다. 해당 요구사항은 원래 2024년 8월 1일 시행 예정이었으나 1년 연기되어 2025년 8월 1일부터 발효됩니다.

또한 EU는 사이버 복원력 법(Cyber Resilience Act, “CRA”, 공식 명칭: Regulation (EU) 2024/2847) 을 도입했습니다. 이 법은 제조업체에 의무적 보고 의무를 2026년 9월 11일부터 부과하며, 2027년 12월 11일에 전면 시행될 예정입니다.

각 법규는 적용 범위(Scope)가 서로 다르므로, 제조업체 입장에서 가장 먼저 대답해야 하는 질문은 “우리 제품이 어떤 법규를 충족해야 하는가”입니다. 본 문서 7페이지의 의사결정 트리(Decision tree) 는 이 단계를 단순화하기 위해 마련되었으며, 구체적인 적용 대상 여부는 본 문서의 다음 섹션에서 각 법규별로 상세히 설명합니다.

사이버 보안 법규 이해하기

영국 PSTI 제도

PSTI 제도는 전 세계적으로 도입된 제품 관련 법규 중, 광범위한 제품군에 대해 구체적이고 의무적인 사이버 보안 요구사항을 최초로 포함한 법규입니다. 해당 법은 2023년 9월에 제정(서명)되었고, 이후 2024년 4월부터 시행되었습니다. 이는 대부분의 신규 제품 관련 법규에 비해 매우 짧은 준비·전환 기간입니다.

다만 PSTI 제도의 요구사항은 전반적으로 준수가 비교적 용이한 편이었습니다. PSTI 제도에서 핵심이 되는 기술적 요구사항은 사실상 1 가지이며, 그 내용은 다음과 같습니다.

즉, 비밀번호는 제품별로 고유해야 하며, 또는 사용자가 직접 설정(정의)할 수 있어야 합니다. 또한 PSTI 제도에는 위 기술 요건 외에, 제조업체가 반드시 충족해야 하는 세 가지 추가 요구사항이 있습니다. 제조업체는 다음을 수행해야 합니다.

- 보안 이슈 보고 체계 마련: 제품의 보안 문제 신고 방법을 안내해야 하며, 신고 접수 후 보안 업데이트가 제공될 것으로 예상할 수 있는 기간(일정/소요기간)에 대해서도 안내해야 합니다.
- 최소 보안 업데이트 기간 공시: 제품에 대해 지원하는 '최소 보안 업데이트 기간'을 공개해야 하며, 한 번 공시된 기간은 사후에 단축할 수 없습니다.
- 합성(준수) 성명서(Statement of Compliance) 제공: 해당 제품이 PSTI 제도 요구사항을 준수했다는 공식 선언서를 반드시 제공해야 합니다.

표준

PSTI 법안은 유럽전기통신표준기구(ETSI)에서 발행한 EN 303 645 표준을 참조하고 있습니다. 이 표준은 다양한 제품 유형에 적용 가능한 '수평적(Horizontal) 사이버 보안 요구사항'을 포괄하도록 마련된, 초기 단계의 대표적인 공개 표준 중 하나입니다.

조항을 인용하며, 이 조항들은 앞서 설명한 요구사항과 동일한 핵심 내용을 다룹니다. (단, 적합성/준수 성명서(Statement of Compliance)는 표준에 포함되어 있지 않으므로 예외입니다.)

EN 303 645는 누구나 무료로 이용할 수 있는 표준입니다.

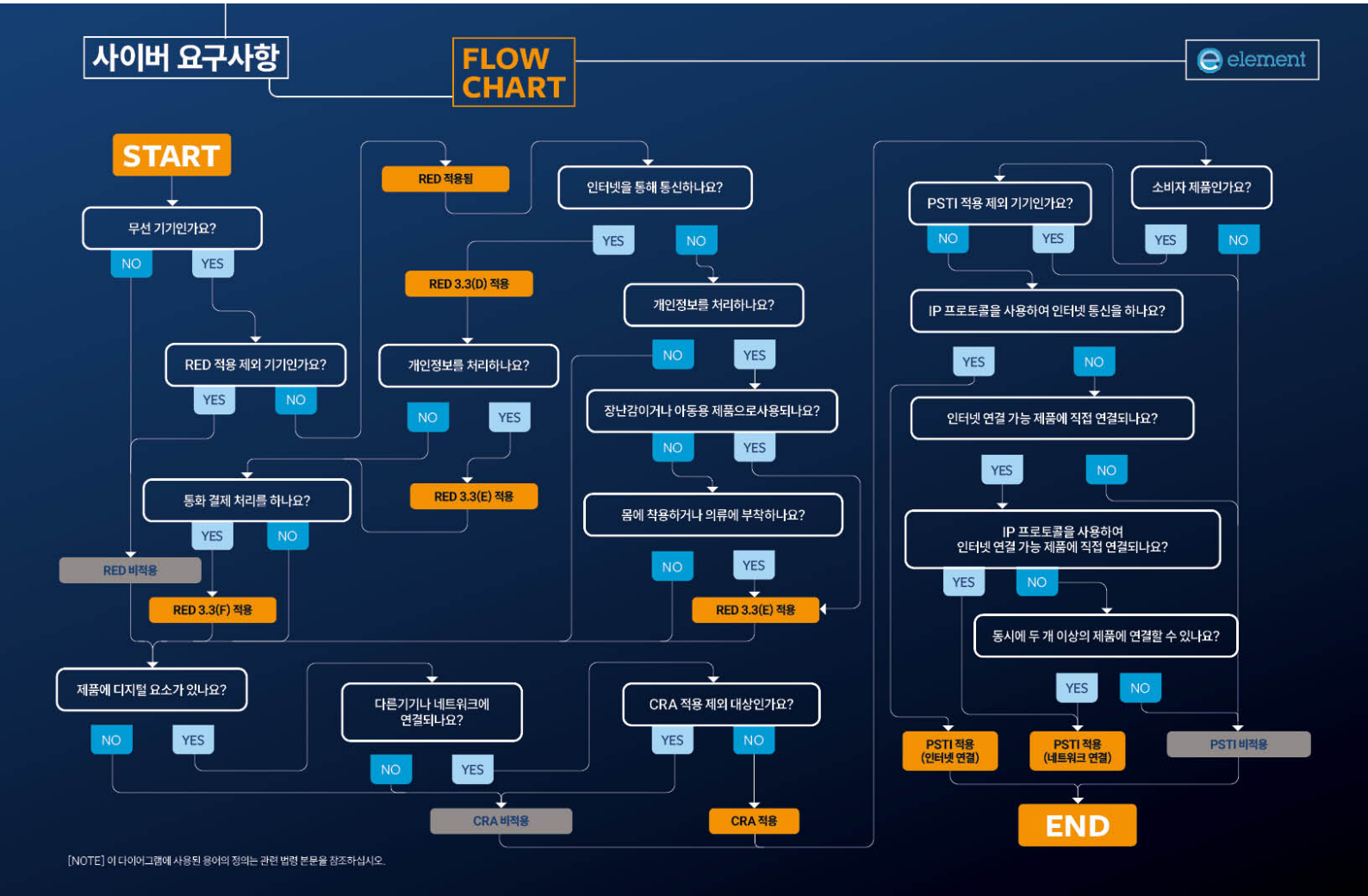
또한, 이 표준에 명시된 각 조항의 구체적인 테스트 방법론을 제공하는 보완 기술 사양인 TS 103 701 역시 무료로 제공되고 있습니다.

적용 범위

PSTI 제도는 영국 시장에 출시되는 '연결 가능한 소비자 제품(Connectable Consumer Products)에만 적용됩니다. 법규에서 정의하는 적용 대상 제품은 다음과 같습니다.

- 인터넷 연결 가능 제품 (Internet-connectable): 인터넷 프로토콜(IP) 스택의 일부인 통신 프로토콜을 사용하여 인터넷을 통해 데이터를 송수신하는 모든 제품으로 정의됩니다.
- 네트워크 연결 가능 제품 (Network-connectable): 다음 중 하나에 해당하는 제품으로 추가 정의됩니다.
  - 인터넷 프로토콜(IP) 스택의 일부인 통신 프로토콜을 사용하여 '인터넷 연결 가능 제품'에 연결할 수 있는 제품
  - 그 외의 다른 통신 프로토콜을 사용하여 '인터넷 연결 가능 제품'에 연결할 수 있으면서, 동시에 두 개 이상의 제품과 연결 가능한 제품

아래의 의사결정 트리(Decision tree)는 해당 여부를 판단하는 데 도움이 됩니다. 판단이 모호한 경우, PSTI 법안의 섹션 4, 5, 54의 조문을 확인하는 것이 권장됩니다.



사이버 보안 법규 이해하기

표준

PSTI 제도는 영국 시장에 출시되는 '연결 가능한 소비자 제품(Connectable Consumer Products)'에 한해 적용됩니다. 본 법령에서 정의하는 대상 제품은 다음과 같습니다.

- 인터넷 연결 가능 제품 (Internet-connectable): 인터넷 프로토콜(IP) 스택의 일부인 통신 프로토콜을 사용하여 인터넷을 통해 데이터를 송수신하는 모든 제품으로 정의됩니다.
- 네트워크 연결 가능 제품 (Network-connectable):
  - 다음 중 하나에 해당하는 제품으로 추가 정의됩니다.
    - 인터넷 연결 가능 제품과, 인터넷 프로토콜 제품군(IP suite)의 일부를 구성하는 통신 프로토콜을 사용하여 연결할 수 있는 제품
    - 인터넷 연결 가능 제품과 그 외의 통신 프로토콜을 사용하여 연결할 수 있으며, 동시에 2개 이상의 제품과 연결할 수 있는 제품

본 문서 7페이지의 의사결정 트리(DECISION TREE)는 해당 여부를 판단하는 데 도움이 됩니다. 판단이 모호한 경우에는 PSTI 법안의 섹션 4, 5, 54에 해당하는 조문을 확인하는 것이 권장됩니다.

시장 출시

CE 마킹 또는 UKCA 마킹과 유사하게, 본 요구사항은 제품 유형(Product Type)이나 생산 로트(Production run) 단위가 아닌 개별 제품 단위(Individual unit)마다 적용됩니다.

따라서 2024년 4월 29일 이후 영국 시장에 출시되는 모든 제품은, 해당 시점에 적용되는 요구사항을 반드시 충족해야 합니다. 이는 동일한 제품 유형이 그 이전부터 시장에 판매되고 있었는지 여부와 관계없이 적용됩니다.

적합성(준수) 성명서

PSTI 제도는 CE 마킹이나 UKCA 마킹과는 별개의 제도이며, 추가적인 제품 마킹(로고 부착 등)을 요구하지 않습니다. 대신, 제품에는 서명된 '적합성(준수) 성명서(Statement of Compliance)'가 반드시 동봉(또는 제공)되어야 합니다. 해당 성명서에는 UKCA 또는 CE의 적합성 선언서(DoC, Declaration of Conformity)와 유사한 정보가 포함되어야 합니다.

포함해야 할 항목은 다음과 같습니다.

- 제품을 식별할 수 있는 정보(제품 식별 정보)
- 제조업체 또는 공인 대리인의 성명 및 주소
- 해당 적합성(준수) 성명서가 제조업체에 의해 또는 제조업체를 대리하여 작성되었음을 선언하는 문구
- 제품이 기술적 요구사항을 충족함을 선언하는 문구
- 제품의 보안 지원 기간
- 평가에 사용된 표준에 대한 참조 정보
- 서명자의 성명, 직함, 서명 날짜 및 장소

또한 UKCA 적합성 선언서(DoC)와 PSTI제도 적합성(준수) 성명서를 동일한 문서에 함께 포함하는 것도 허용됩니다.

EU 무선기기 지침

RED가 처음 제정되었을 때부터, 제3조 제3항(Article 3(3))에는 특정 기기 카테고리에 적용될 수 있는 추가적인 필수 요구사항이 포함되어 있었습니다. 이 9가지 추가 필수 요구사항은 흔히 "스위치 뱅크(여러 개의 스위치 묶음)"에 비유되곤 합니다. 즉, 처음에는 모든 스위치가 '꺼짐' 상태로 시작하지만, 유럽 연합 집행위원회/유럽위원회(EC:European Commission)가 특정 기기 카테고리에 대해 필요에 따라 해당 스위치를 켜서 적용할 수 있다는 의미입니다.

이미 제3조(3항)(g)는 무선 위치탐지 비콘(Radiolocation beacons) 및 스마트폰과 관련된 여러 장비 범주에 대해 시행된 바 있습니다. 하지만 사이버 보안 분야에서 가장 핵심적인 부분은 위임 규정(EU) 2022/30에 의해 **제3조 제3항 (d), (e), (f)**의 스위치가 켜졌다는 점입니다. 이 요구사항들은 2025년 8월 1일부터 해당 요구사항이 의무 적용됩니다.

이 세 가지 요건은 각각 서로 다른 주제를 다루며, 적용되는 장비 범주도 다릅니다.

- 제3조 제3항 (d) – 네트워크 보호: 제품이 네트워크에 해를 끼치지 않도록 보호할 것을 요구합니다. 예를 들어, 인터넷에 연결된 제품이 공격에 의해 장악되어 '봇넷(Botnet)' 구축에 악용되거나, 보안이 취약한 단일 장비가 해커들이 네트워크 침투하는 진입점으로 활용되는 상황을 방지하는 것을 목표로 합니다. 이 요구사항은 인터넷에 연결되는 무선 기기에만 적용됩니다.
- 제3조 제3항 (e) – 개인정보 및 프라이버시 보호: 제품이 데이터와 프라이버시를 보호할 것을 요구합니다. 예를 들어, 악의적인 공격자가 개인 식별 가능 정보(PII)에 접근하는 것을 방지하는 것이 목적이며, 특히 민감한 카테고리의 데이터나 아동과 관련된 데이터의 경우 더욱 엄격한 보호를 목표로 합니다. 이 요건은 개인정보, 트래픽 데이터 또는 위치 데이터를 처리하는 무선 기기 중, 다음 조건 중 하나 이상에 해당하는 경우에만 적용됩니다.
  - 인터넷 연결(Internet-connected) 무선 장비
  - 신체 착용 또는 휴대(Body-worn or carried)되는 장비
  - 아동이 사용하는 장비
  - 장난감(toy)
- 제3조 제3항 (f) – 금융 사기 방지: 제품이 금융 사기로부터 보호될 것을 요구합니다. 예를 들어, 금융 자산, 화폐 또는 가상 화폐를 처리할 때 악의적인 공격자가 해당 자산에 접근하거나 이를 변경하지 못하도록 한층 강화된 보호 장치를 마련하는 것을 목표로 합니다. 이 요건은 금융 자산을 처리하는 인터넷 연결 무선 기기에만 적용됩니다.

본 백서 7페이지의 의사결정 트리(Decision tree) 는 어떤 필수 요구사항이 어떤 제품 유형에 적용되는지 판단하는 데 도움을 주기 위해 마련되었습니다. 해석이 모호한 경우에는 위임 규정(Delegated Regulation)

(EU) 2022/30 제1조(Article 1) 의 조문을 참고하는 것이 권장됩니다.

한편, RED 위임 규정의 맥락에서 "인터넷 연결(Internet-connected)"의 의미는 일부 모호한 부분이 있습니다. 규정의 본문에서는 인터넷 연결 무선 기기를 "인터넷을 통해 자체적으로 통신할 수 있는 기기"로 정의하고 있습니다. 업데이트된 RED 가이드가 없는 상황에서, 위임 규정 전문의 전문(Preamble) (5)항을 통해 이를 확장 해석해 보면, 해당 기기는 "인터넷과 데이터를 교환하는 데 필요한 프로토콜을 작동시키는 기기"를 의미합니다.

공식 가이드는 부족하지만, 업계의 일반적인 합의는 이를 'IP 링크의 한쪽 종단(One end of an IP link)'으로 보고 있습니다. 예를 들어, IP 주소 12.34.56.789를 가진 장치가 다른 원격 장치의 IP 주소98.76.54.321를 가진 어떤 장비와 통신을 시도하는 경우를 의미합니다.

사이버 보안 법규 이해하기

RED 위임 규정은 이러한 인터넷 연결이 반드시 직접적일 필요는 없다고 설명합니다. 즉, 어떤 장비가 다른 장비를 거쳐 인터넷에 연결되더라도 본 요구사항의 적용 범위(SCOPE)에 포함될 수 있습니다.

표준

새로운 요구사항에 대응하기 위해 유럽연합 관보(OJEU)에 세 가지 표준이 인용되었습니다. 다만, 각 표준은 다음과 같은 제한 사항과 함께 등재되었습니다.

- **EN 18031-1:2024 (제3조 제3항 (d) 대응):**
  - 제품에 표준의 6.2.5.1 또는 6.2.5.2 조항(사용자 비밀번호 관련)이 적용되는 경우, 그리고 제품 사용자가 비밀번호를 설정하거나 사용하지 않는 것이 허용된다면, 해당 표준은 RED 필수 요구사항에 대한 '적합성 추정(Presumption of Conformity)'을 부여하지 않습니다.
- **EN 18031-2:2024 (제3조 제3항 (e) 대응):**
  - 표준의 6.2.5.1 또는 6.2.5.2 조항(사용자 비밀번호 관련)이 적용될 때 사용자가 비밀번호를 설정하지 않아도 된다면, 적합성 추정이 인정되지 않습니다.
  - 또한 표준의 6.1.3.4.2, 6.1.4.4.2, 6.1.5.4.2 또는 6.1.6.4.2 조항(아동용 장비의 부모/보호자 통제 관련)이 적용되는 제품에서 보호자 통제 기능이 보장되지 않는 경우에도 적합성 추정이 인정되지 않습니다.
- **EN 18031-3:2024 (제3조 제3항 (f) 대응):**
  - 위와 동일하게 사용자 비밀번호 설정(표준의 6.2.5.1 또는 6.2.5.2 조항)이 필수적이지 않은 경우 적합성 추정이 인정되지 않습니다.
  - 보안 업데이트 메커니즘과 관련된 표준 6.3.2.4 조항이 적용되는 경우에도 해당 표준만으로는 적합성 추정이 인정되지 않습니다.

추가적으로, 세 표준 모두 '근거(Rationale)' 및 '가이드(Guidance)'라고 명시된 섹션은 규범적(Normative)인 것으로 간주되지 않으며, RED 필수 요구사항에 대한 적합성 추정을 부여하지 않는다는 점에 유의해야 합니다.

적합성 평가 절차

앞서 언급한 제한 사항들이 무선 기기 제조사에 시사하는 바는 명확합니다. 제품이 이러한 제한 사항 중 하나라도 해당될 경우, 선택할 수 있는 **적합성 평가 절차(CAP)**가 제한된다는 것입니다.

RED 제17조에 따르면, 무선 기기 제조사는 일반적으로 다음 세 가지 적합성 평가 절차를 이용할 수 있습니다.

- 내부 생산 관리 (Internal Production Control): 인증기관(Notified Body)의 개입 없이 준수 선언서(DoC)를 바탕으로 진행하는 전통적인 방식입니다.
- EU 형식 시험 (EU-Type Examination): 인증기관의 시험을 거친 후 '형식 적합성(Conformity to Type)'을 확인받는 방식입니다.
- 완전 품질 보증 (Full Quality Assurance): 인증기관을 통해 품질 시스템 전체를 승인받는 방식입니다.

위에서 보듯, 인증기관 없이 진행할 수 있는 방식은 '내부 생산 관리'가 유일합니다.

RED 제17조는 EMC, 안전, 공통 충전기 요구사항(제3조 제1항 및 제4항)에 대해서는 3가지 CAP 중 어느 것이든 사용할 수 있다고 명시합니다. 하지만 제3조 제2항(무선 스펙트럼 사용) 및 제3조 제3항(사이버 보안 요건 포함)의 경우, 선택 가능한 절차는 유럽연합 관보(OJEU)에 인용된 조화 표준(Harmonised Standards)의 적용 여부에 따라 달라집니다.

- 조화 표준을 완전히 적용한 경우: 위의 3가지 CAP 중 어느 절차든 선택할 수 있습니다.
- 조화 표준을 완전히 적용하지 않은 경우: (표준이 존재하지 않거나 관련 제한 사항이 있는 경우 포함) '내부 생산 관리' 방식을 더 이상 사용할 수 없습니다. 반드시 인증기관(Notified Body)을 통한 'EU 형식 시험' 또는 '완전 품질 보증' 절차를 따라야 합니다.

따라서 이러한 제한 사항에 해당하는 제품은 시장에 출시되기 전 반드시 인증기관(Notified Body)의 검토를 거쳐야 합니다. 참고로 2025년 8월 1일 이전까지는 사이버 보안 요건이 아직 발효 전이므로, 인증기관이 공식적인 EU 형식 시험 인증서를 발행할 수 없다는 점도 유의해야 합니다. 실무적으로 많은 인증기관이 현재 초안(Draft) 인증서를 발행한 뒤, 2025년 8월 1일에 최종본을 발행하는 방식으로 대응할 가능성이 큽니다.

또한 유럽위원회(EC)는 공식적인 EU 형식 시험 인증서가 아닌 '자발적(Voluntary)' 인증서를 발행하는 인증기관(Notified Body 포함)을 주의하라는 지침을 발표했습니다. EU 법에 따르면 자발적 또는 기타 추가 인증서는 적합성을 증명하는 공식 수단으로 인정되지 않습니다. 결과적으로 이러한 인증서는 시장 감시 당국이나 세관의 점검 시 아무런 효력이 없으며, 실제로는 적합하지 않은 제품임에도 법규를 준수했다는 오해를 불러일으킬 수 있습니다. CE 마킹은 반드시 제품에 적합한 평가 절차(CAP)를 마친 후에만 부착해야 합니다.

위험성 평가

RED(무선기기 지침)는 다른 EU 지침과 마찬가지로, 제조업체가 규정 준수 여부와 관련하여 적절한 위험 분석 및 평가를 수행할 것을 요구합니다. 이 위험성 평가는 시장 감시 당국이나 인증기관(Notified Body)의 요청이 있을 경우 즉시 제시할 수 있도록 상시 준비되어 있어야 합니다.

위험성 평가는 제조업체의 기술 문서(Technical Documentation) 중에서도 가장 핵심적인 필수 문서입니다. 일반적으로 제품에 CE 마킹을 진행할 때 가장 먼저 작성하기 시작하여 마지막까지 검토해야 하는 문서이기도 합니다. 즉, 모든 인증 프로세스가 끝난 뒤에 형식적으로 만드는 문서가 아니라는 점이 매우 중요합니다.

위험성 평가에는 정해진 템플릿이나 반드시 포함되어야 할 항목 리스트가 별도로 존재하지 않습니다. 제조업체는 각기 다른 제품의 특성에 맞춰 자신들만의 고유한 방식으로 접근해야 합니다. 위험 평가에 관한 더 자세한 가이드는 아래 링크의 화이트페이퍼를 참고하시기 바랍니다.

참고 링크: 무선 기기 위험 분석이란 무엇인가?

사이버 보안 법규 이해하기

시장 출시

모든 CE 마킹 지침 및 규정과 동일하게, 새로운 RED 요구사항은 제품이 시장에 출시되는 시점을 기준으로 적용됩니다. 여기서 '출시'란 제품 모델이나 생산 로트 단위가 아닌, 개별 제품(Individual unit) 하나하나를 의미합니다.

따라서 동일한 모델이 해당 날짜 이전에 이미 판매되고 있었더라도,

2025년 8월 1일 이후에 시장에 공급되는 모든 제품은 해당 시점의 규정 요건을 반드시 충족해야 합니다.

적합성 선언 및 CE 마킹

제품 자체에 추가로 부착해야 하는 마킹 요구사항은 없습니다.

하지만 **적합성 선언서(DoC)**는 해당 요구사항에 따라 제품을 평가할 때 사용된 표준을 참조하도록 업데이트되어야 합니다.

또한, 만약 DoC에 필수 요구사항 리스트를 기재하는 경우(의무 사항은 아님), 관련 있는 제3조 제3항(Article 3(3))의 요건들도 반영하여 업데이트해야 합니다.

인증기관(Notified Body)으로부터 **EU 형식 시험 인증서**를 발급받은 경우에는 해당 내용을 DoC에 기재해야 합니다. 이렇게 새롭게 작성된 DoC는 해당 시점에 맞춰 서명 및 날인이 완료되어야 합니다.

사이버 보안 법규 이해하기

EU 사이버 복원력 법안

CRA(Cyber Resilience Act)는 2024년에 발효되었으며, 제조업체는 2026년 9월 11일부터 의무적인 보안 사고 보고 의무(Reporting obligations)를 지게 됩니다. 그 외 모든 기타 의무 사항은 2027년 12월 11일부터 전면 적용될 예정입니다.

CRA의 적용 범위는 매우 광범위합니다. 일부 제외된 제품군을 제외하고, 다른 장치나 네트워크에 직접 또는 간접적으로 논리적/물리적 데이터 연결이 가능한 **'디지털 요소가 포함된 모든 제품'**에 적용됩니다. 귀사의 제품이 적용 대상인지 판단하는 데 도움이 되도록 7페이지에 **의사결정 나무(Decision Tree)**를 수록하였으며, 내용이 모호한 경우에는 규정(EU) 2024/2847의 제2조 본문을 참조하시기 바랍니다.

일단 CRA 요구사항이 본격적으로 적용되기 시작하면, 두 법규 간의 중복을 피하기 위해 기존 RED(무선기기 지침)의 사이버 보안 요구사항은 폐지될 것으로 널리 예상되고 있습니다.

주요 및 핵심 제품군

CRA는 다른 장치나 네트워크에 직접 또는 간접적으로 논리적/물리적 데이터 연결이 가능한 **'디지털 요소가 포함된 모든 제품'**에 적용됩니다. 하지만 이 중에서도 '주요(IMPORTANT)' 또는 '핵심(CRITICAL)' 제품군으로 분류되는 경우에는 추가적인 요구사항이 부과됩니다. 해당되는 제품 유형의 상세 리스트는 부속서(ANNEX) III 및 IV에 명시되어 있습니다.

표준 및 기술 사양

본 기고문을 작성하는 시점까지는 CRA의 특정 요건을 다루는 표준이 아직 발행되지 않았습니다. 2025년 2월, 유럽 연합 집행위원회(EC)는 표준 제정 기구인 ETSI, CENELEC 및 CEN에 CRA 요구사항에 대응하는 41개의 표준을 제정해 줄 것을 요청하는 표준화 요청서(Standardisation Request)를 공식 발표했습니다. 해당 표준들은 다음과 같이 구성될 것으로 예상됩니다.

- 취약점 보고에 관한 수평적 표준 1개
- 모든 제품군에 적용되는 보안 요구사항에 관한 수평적 표준 14개
- 특정 요구사항을 다루는 26개의 수직적 표준:
  - CRA 부속서(Annex) III 제1부에 해당하는 Class I 주요 제품군 대상 표준 19개
  - CRA 부속서(Annex) III 제2부에 해당하는 Class II 주요 제품군 대상 표준 4개
  - CRA 부속서(Annex) IV에 해당하는 핵심 제품군 대상 표준 3개

이러한 표준들이 발행되면 유럽연합 관보(OJEU)에 **조화 표준**으로 인용될 예정입니다. 다만, 집행위원회의 표준 검토 결과에 따라 특정 제한 사항과 함께 인용되거나, 인용되지 않을 수도 있는 등 상황은 변동될 수 있습니다.

또한 집행위원회는 조화 표준을 대신하여 특정 **공통 사양**을 채택할 권한도 보유하고 있습니다. 다만, 현재까지 채택된 공통 사양은 없습니다.

적합성 평가 절차

CRA는 기존의 '내부 생산 관리', 'EU 형식 시험 및 형식 적합성', '완전 품질 보증' 방식 외에도 **'유럽 사이버 보안 인증 체계(EUCC)'**라는 새로운 적합성 평가 절차를 도입합니다. 현재까지 채택된 EUCC 체계는 없으나, 유럽 연합 집행위원회(EC)는 CRA 제8조 제1항에 따라 해당 체계를 채택할 권한을 보유하고 있습니다.

CRA 제32조는 RED 제17조와 마찬가지로, 특정 요건에 따라 제조업체가 사용할 수 있는 적합성 평가 절차(CAP)를 제한하고 있습니다. CRA의 경우, 유럽연합 관보(OJEU)에 인용된 **조화 표준(Harmonised Standards)**의 적용 여부뿐만 아니라 **공통 사양(Common Specifications)**의 준수 여부, 그리고 장비의 카테고리 분류에 따라 절차가 나뉩니다.

- 일반 제품군 (부속서 III의 '주요' 또는 부속서 IV의 '핵심' 제품군이 아닌 경우):
  - 네 가지 적합성 평가 절차 중 어느 것이든 자유롭게 선택하여 사용할 수 있습니다.
- Class I 주요 제품군 (부속서 III 해당):
  - 조화 표준 또는 공통 사양을 완전히 적용한 경우: 위의 네 가지 절차 중 어느 것이든 사용할 수 있습니다.
  - 조화 표준 또는 공통 사양을 완전히 적용하지 않은 경우: 반드시 'EU 형식 시험', '완전 품질 보증', 또는 보증 수준 '실질적(Substantial)' 이상의 'EUCC 체계'를 따라야 합니다.
- Class II 주요 제품군 (부속서 III 해당):
  - 제조업체는 반드시 'EU 형식 시험', '완전 품질 보증', 또는 보증 수준 '실질적(Substantial)' 이상의 'EUCC 체계'를 따라야 합니다.
- 핵심 제품군 (부속서 IV 해당):
  - 제조업체는 반드시 'EUCC 체계'를 따라야 합니다. 단, 해당 제품 유형에 대한 관련 EUCC 체계가 아직 존재하지 않는 경우에 한해 'EU 형식 시험' 또는 '완전 품질 보증' 절차를 사용할 수 있습니다.

사이버 보안 법규 이해하기

보고 의무

2027년에 발효되는 제품 적합성 요건뿐만 아니라, CRA에는 2026년 9월 11일부터 의무화되는 제조업체의 보고 의무가 포함되어 있습니다. 이를 조정하기 위해 각 회원국은 해당 보고의 조정자 역할을 할 단일 **컴퓨터 보안 침해사고 대응팀(CSIRT)**을 지정해야 합니다.

보고 의무를 준수하기 위해, 자신의 제품에서 '실제로 악용되고 있는 취약점'을 인지하거나 제품 보안에 영향을 미치는 '심각한 사고'가 발생했음을 알게 된 제조업체는 반드시 다음 조치를 취해야 합니다.

- EU 사이버 보안국(ENISA)에 통지
- 관련 회원국의 CSIRT에 통지 (어느 국가의 CSIRT에 통지해야 하는지에 대한 세부 사항은 CRA 제7조 참조)
- 영향을 받는 제품의 사용자에게 통지 (사용자가 영향을 완화하기 위해 취할 수 있는 수정 조치에 대한 세부 정보 포함)

'제품 보안에 영향을 미치는 심각한 사고' 란 다음과 같은 경우를 의미합니다.

1. 민감하거나 중요한 데이터 또는 기능의 가용성, 진본성, 무결성 또는 기밀성을 보호하는 제품의 능력에 부정적인 영향을 미치거나 미칠 가능성이 있는 경우

2. 제품 또는 제품 사용자의 네트워크 및 정보 시스템에 악성 코드가 유입되거나 실행되도록 유도하거나 그럴 가능성이 있는 경우

ENISA 및 CSIRT에 대한 통지는 ENISA가 구축한 단일 보고 플랫폼을 통해 제출되어야 합니다. 다만, 본 문서를 작성하는 시점까지 해당 플랫폼은 아직 개설되지 않았습니다.

위험성 평가

CRA에 따라 제조업체는 제품과 관련된 사이버 보안 위험을 평가해야 할 의무가 있습니다. 또한 사이버 보안 위험을 최소화하고 사고를 예방하며 그 영향을 줄이기 위해, 제품의 기획, 설계, 개발, 생산, 인도 및 유지보수 전 단계에 걸쳐 해당 위험 평가 결과를 반영해야 합니다. 이는 RED(무선기기 지침)에 따라 요구되는 위험 평가와 매우 유사한 절차입니다.

시장 출시

모든 CE 마킹 지침 및 규정과 마찬가지로, 새로운 CRA 요구사항은 제품이 시장에 출시되는 시점을 기준으로 적용됩니다. 이는 제품 모델이나 생산 단위가 아니라 개별 제품 하나하나를 의미하는 것으로 해석해야 합니다.

따라서 동일한 모델이 해당 날짜 이전에 이미 판매되고 있었더라도, 2027년 12월 11일 이후에 시장에 공급되는 모든 제품은 해당 시점의 규정 요건을 반드시 충족해야 합니다.

적합성 선언 및 CE 마킹

제품 자체에 추가로 부착해야 하는 마킹 요구사항은 없습니다.

다만, **적합성 선언서(DoC)**는 CRA 법령 및 제품 평가에 사용된 관련 표준을 참조하도록 업데이트되어야 합니다. 인증기관(Notified Body)으로부터 **EU 형식 시험 인증서**를 발급받은 경우, 해당 내용을 DoC에 기재해야 합니다.

새롭게 작성된 DoC는 해당 시점에 맞춰 서명 및 날인이 완료되어야 합니다.

사이버 보안 법규 이해하기

기타 관련 표준

EN 303 645나 EN 18031만이 제품 사이버 보안을 다루는 유일한 표준은 아닙니다. IEC 62443-2-4, IEC 15408, ISO 21434와 같은 다른 표준들도 유사한 영역을 다루고 있습니다. 기본적으로 이 모든 표준은 "이 제품이 사이버 보안상 안전한가?"라는 질문에 답하기 위한 방법론을 제시하는 것이 목적입니다.

비록 접근 방식은 다를 수 있지만, 보안이 철저한 제품이라면 이론적으로 어떤 표준에 따른 평가라도 통과해야 합니다. 이는 자동차용 EMC 표준과 산업용 EMC 표준의 관계와 같습니다. 두 표준 모두 "이 장치가 전자파 적합성을 갖추었는가?"라는 동일한 질문을 던지지만, 서로 다른 시기에 다른 단체에 의해 특정 제품군을 염두에 두고 작성되었기 때문에 접근 방식에서 차이가 나는 것뿐입니다.

한편, ETSI에서 발행한 매핑 문서인 TS 103 929를 활용하면 EN 303 645, RED 요구사항, 그리고 IEC 62443-4-2 간의 상관관계를 확인할 수 있습니다.

사이버 보안 평가는 어떻게 진행되는가?

제품 사이버 보안 평가는 상당 부분 문서 검토를 중심으로 이루어지며, 실제 제품 시험 비중은 상대적으로 적은 편입니다. 일반적으로 첫 번째 단계는 제조업체가 시험소에 제출한 기술 문서를 검토하는 것이며, 그 뒤를 이어 제품 시험이 포함된 **기능 평가(FUNCTIONAL ASSESSMENT)**와 **완결성 평가(COMPLETENESS ASSESSMENT)**가 진행됩니다.

제품 시험은 '그레이박스(GREY-BOX) 테스트' 방식으로 설명할 수 있습니다. 이는 테스터가 제품 내부 동작을 완벽히 알고 있는 '화이트박스(WHITE-BOX)' 테스트와 제품에 대한 정보가 전혀 없는 상태에서 진행하는 '블랙박스(BLACK-BOX)' 테스트의 중간 단계입니다.

따라서 제조업체는 테스터가 특정 장치 기능, 업데이트 메커니즘, 암호화 기술 등에 접근할 수 있도록 필요한 기술 지원을 제공해야 합니다. 이러한 제조사의 적극적인 지원 없이는 테스터가 평가의 상당 부분을 완료하는 것이 불가능합니다.

기술 문서

위에서 언급된 다양한 표준들은 요구되는 문서를 서로 다른 용어로 지칭하지만, 일반적으로 다음 세 가지 카테고리 중 하나에 해당합니다.

- **구현 적합성 선언서:** 장치가 사이버 보안을 위해 구현한 메커니즘, 규정 또는 보호 조치들을 나열한 문서입니다. ICS는 표준에서 요구하는 특정 문서 요청(예: "제품이 처리하는 모든 네트워크 자산 목록을 제공하십시오")과 제조업체의 실제 문서(예: "사용 설명서 4장 참조" 또는 "증빙서류1.docx 참조") 사이를 연결해 주는 이정표(Signposting) 역할을 하기도 합니다. TS 103 645는 제조업체에 ICS 제출을 명시적으로 요구하는 반면, EN 18031 표준은 이를 요구하지 않습니다.

- **시험용 추가 구현 정보:** 평가를 수행하는 데 필요한 추가 정보를 담고 있습니다. 일반적으로 장치가 구현한 각 메커니즘이나 보호 조치마다 하나의 IXIT가 제공됩니다. TS 103 645는 제조업체에 IXIT 제출을 명시적으로 요구합니다. EN 18031 표준은 IXIT라는 용어를 구체적으로 사용하지는 않지만, 실질적으로 IXIT와 동일한 역할을 하는 다양한 증빙 문서(표준 내에서 "E.Info" 및 **"E.Just"**로 지칭됨)를 요청합니다.

- **의사결정 트리:** 일련의 구조화된 '예/아니요' 질문에 답함으로써 제품이 특정 표준 조항을 충족하는지 평가하는 방식입니다. 최종적으로 합격(Pass), 불합격(Fail) 또는 해당 없음(N/A)의 결과로 이어집니다. 이 의사결정 트 방식은 EN 18031 표준만의 고유한 특징이며, 제조업체가 이를 직접 작성하여 제출할 것을 명시적으로 요구합니다.

일반적으로 시험소는 제출된 문서를 검토한 후 제조업체에 피드백이나 시정 조치를 제안합니다. 이러한 상호 소통 과정은 양측 모두가 해당 표준의 모든 항목이 적절히 반영되었다고 만족할 때까지 여러 차례 반복될 수 있습니다.

기능 적정성 평가

기능 적정성 평가의 목적은 제조업체가 제출한 문서에서 주장하는 각 메커니즘, 규정 또는 보호 조치가 실제 장비에 구현되어 있으며, 의도한 대로 작동하는지 검증하는 것입니다.

이에 대한 몇 가지 구체적인 예시는 다음과 같습니다.

- 데이터 암호화 검증: 물리적인 외부 인터페이스가 있고, 제조업체가 이 인터페이스를 통해 전송되는 데이터가 암호화된다고 명시한 경우, 시험소는 해당 데이터를 실제로 확인하여 일반 텍스트(Plaintext)가 아닌 암호화된 상태로 전송되는지 검증합니다.

- 보안 잠금 기능 검증: PIN 패드(비밀번호 입력기)가 있는 장치에서, 잘못된 PIN을 여러 번 입력할 경우 일정 시간 동안 입력이 차단된다고 문서에 명시된 경우, 시험소는 실제로 이러한 차단 현상이 발생하는지 확인합니다.

- 데이터 유효성 검사: 데이터 입력 항목이 존재하고, 입력된 데이터의 구조나 길이에 대해 유효성 검사를 수행한다고 명시된 경우, 시험소는 올바른 형식의 데이터는 정상 처리되고 잘못된 형식의 데이터는 적절히 거부되는지 검증합니다.

이 단계에서 시험소는 이러한 보호 조치들을 무력화하거나 뚫으려는 시도(해킹 등)를 하지는 않으며, 오직 해당 기능들이 존재하고 정상적으로 작동하는지만을 확인합니다.

사이버 보안 법규 이해하기

완결성 평가

완결성 평가의 목적은 제공된 문서가 제품의 모든 측면을 빠짐없이 다루고 있는지 검증하는 것입니다. 시험소는 육안 검사나 네트워크 스캔 도구 등을 활용하여, ICS(구현 적합성 선언서)나 IXIT(시험용 추가 정보)에 명시되지 않은 물리적 인터페이스 또는 무선 인터페이스가 제품에 존재하는지 확인합니다. 또한 사용자 설명서를 검토하여 ICS나 IXIT에 제대로 기술되지 않은 제품 기능이 있는지 철저히 체크합니다.

시험소의 역할

위에서 언급된 어떤 표준이나 법률에서도 제3자 공인 시험소를 반드시 이용해야 할 의무는 없습니다. 이는 EMC(전자파 적합성)와 같은 다른 시험 분야와도 유사한 상황입니다. 하지만 대부분의 제조업체는 내부적으로 모든 EMC 시험을 수행할 역량을 갖추고 있지 않기 때문에 시험소를 찾게 되며, 사이버 보안 평가 역시 마찬가지일 것입니다.

설령 내부적으로 EMC 시험 역량을 갖춘 제조업체라 하더라도, 독립적인 제3자의 객관적인 평가가 주는 가치를 높게 평가하여 외부 시험소를 활용하곤 합니다.

침투 테스트

침투 테스트란 공격자가 사용하는 것과 동일한 도구와 기술을 사용하여 제품의 보안 조치 일부 또는 전부를 뚫으려는 시도를 통해 제품의 보안성을 평가하는 방법입니다. 구체적으로 어떤 기술을 사용할지, 그리고 테스터에게 사전에 시스템 정보를 어느 정도 제공할지는 테스트 체계에 따라 달라질 수 있습니다.

중요한 점은, 위에서 상세히 설명한 그 어떤 표준이나 법률도 침투 테스트를 필수적으로 요구하지 않는다는 사실입니다.

ELEMENT는 어떻게 도움을 드릴 수 있나요?

Element는 전 세계 장비 제조업체들을 위해 종합적인 자문-시험-검사-인증(ATIC)과 글로벌 시장 진출(GMA) 솔루션을 제공합니다. 당사의 현지 전문가 팀은 끊임없이 변화하는 규제 요건에 고객이 신속히 대응할 수 있도록 지원하며, 복잡한 인증 과정을 명확하고 단순하게 만들어 드립니다.

새로운 사이버 보안 요구사항과 관련하여, Element는 크게 세 가지 방식으로 귀사를 지원할 수 있습니다.

1. **자문 서비스 :** 당사의 자문 부서는 귀사 제품에 최적화된 규제 대응 전략 문서 또는 시험 계획서를 작성하여 시장 진출 경로를 명확히 제시하고 불확실성을 제거해 드립니다. 또한 위험 평가(Risk Assessment) 수행, 기술 문서(Technical File) 취합을 지원하며, 적합성 선언서(DoC) 또는 준수 성명서(SoC)를 검토하여 모든 요건이 완벽히 충족되었는지 확인해 드립니다.
2. **공인 시험소:** Element는 ISO 17025 인증을 받은 전문 시험소입니다. 당사의 스마트 기술(Smart Technologies) 시험 엔지니어들은 다양한 제품군에 대한 사이버 보안 시험을 수행할 수 있는 최첨단 장비와 역량을 갖추고 있습니다.
3. **공인 인증 및 통지 기관 :** Element는 ISO 17065 인증을 받은 인증 기관이자, 무선기기 지침(RED)에 따른 **유럽 통지 기관(Notified Body)**입니다. 조화 표준을 완전히 적용하지 않아 필수적으로 요구되는 경우는 물론, 규제 준수를 확고히 증명하기 위한 선택적 서비스로서 **RED에 따른 EU 형식 시험 인증서**를 발행해 드립니다.

Element의 글로벌 전문가를 통해 귀사의 비즈니스에 어떤 도움을 받을 수 있는지 자세히 알아보세요.

지금 바로 귀사의 시험 및 인증 요구사항에 대해 상담받으시기 바랍니다.

관련 서비스

- 자문서비스
- 사전 적합성 시험
- 안전 시험
- SAR 시험
- 무선 시험
- EMC 시험
- 프로토콜 시험
- 사이버 보안
- 글로벌 시장 진출

"2025년 8월 1일부터 유럽 연합(EU) 내에서 판매되는 모든 제품은 무선기기 지침(RED)의 개정된 사이버 보안 요건을 반드시 준수해야 합니다."

마이클 더비
(전)기술 이사, Michael Derby)

ELEMENT 회사 소개

Element는 서비스의 실패가 결코 용납되지 않는 다양한 최종 시장(End Markets)을 대상으로,
광범위한 제품, 소재, 공정 및 서비스에 대한 **시험, 검사 및 인증(TIC) 서비스를 제공하는 글로벌 TIC 선도 기업**입니다.

270+

미주, 유럽, 중동, 아프리카, 아시아 및 호주 지역에 걸쳐 30개국에 시험소를 운영하고 있습니다.

9000+

전 세계의 임직원과 전문 분야의 협력 전문가들이 귀사의 시험 요구사항을 충족할 수 있도록 언제든 지원할 준비가 되어 있습니다.

1000+

공인(Accreditations) 및 승인(Approvals) 은 우리가 제공하는 서비스 품질에 대한 공신력 있는 인정을 의미합니다.

55000+

전 세계적으로 다양한 선도적인 과학·기술·엔지니어링 산업 분야의 고객사에 서비스를 제공하고 있습니다.

element

문의하기(Contact Us) | 전국대표번호 1551-9871

ELEMENTKOREA.KR