AUTOCRYPT

CRA: SECURE BY DESIGN. SECURE BY DEFAULT.

디지털 제품들이 직면한 규제 변화의 대비

유럽의 CRA(Cyber Resilience Act) 도입과
그에 따른 자동차 산업의 영향

목차

서론

스마트 가전, 헬스케어 기기, 전기차, 스마트 제품 등은 소프트웨어 기반으로 우리의 삶과 업무 방식을 향상시킵니다. 하지만 이런 소프트웨어에도 보안 취약점은 존재할 수 있으며, 이는 사이버 보안 위협으로 이어질 수 있습니다.

사이버 공격이 점점 더 빈번해지고 피해 규모도 커짐에 따라, 각국 정부는 사이버보안에 대한 접근 방식을 전환하고 있습니다. 이제 정부는 기존의 권고 수준을 넘어, 시행 가능한 규정으로 전환하며 모든 산업 분야에 사이버보안을 최우선 과제로 요구하고 있습니다.

이러한 규제 움직임 최전선에는 유럽연합(EU)이 있습니다. EU는 진화하는 자동차 산업의 사이버 보안 위협에 공식적으로 대응한 최초 정부 기관 중 하나로, 2020년 UNECE WP.29 규정인 (R155 및 R156)을 채택하여 2024년부터 모든 차량 모델에 대한 사이버 보안 형식 승인을 의무화했습니다.

사이버보안 기업들은 오랫동안 모든 커넥티드 기기에 사이버보안을 적용해야 함을 지적해왔고, EU는 규제 명령을 통해 사이버보안은 편리한 기능일 뿐만 아니라 시장 진입을 위한 전제조건이라는 분명한 의도를 명확히 했습니다.

WP.29 사이버보안 규정은 사이버보안에 대한 논의를 훨씬 더 넓은 글로벌 차원으로 확장시키는 전환점이 되었습니다. 그 범위는 단순히 자동차를 넘어, 시장의 모든 커넥티드 기기로 확대되고 있습니다. 일상의 커넥티드 기기 활용에 발생 가능한 보안 위협과 책임은 무엇이며, 정부는 기업과 소비자를 보호하기 위해 어떤 디지털 신뢰 체계를 구축해야 할까요?

이에 대해 EU가 제시한 해답은 바로 CRA(사이버복원력법; Cyber Resilience Act) 입니다.

이 백서에서는 현재 진행 중인 규정이 무엇인지, UNECE WP.29 또는 ISO/SAE 21434와 같은 프레임워크 및 규정과 어떻게 다른지, CRA가 디지털 책임의 새로운 시대를 어떻게 추구하는지에 대해 중점적으로 설명합니다. 최근 기술 혁신으로 차량은 연결성, 소프트웨어, 자동화가 융합된 형태로 진화하고 있습니다. 본 보고서는 자동차 산업을 중심으로 CRA의 영향을 살펴보고, 준수를 위한 주요 요구사항과 대응 방안을 제시합니다.

CRA의 목표, 적용 대상과 주체

현대 사회는 디지털 중심으로 빠르게 전환되어 점점 더 많은 기기들이 네트워크로 연결되고 있습니다. 이러한 기기들은 소프트웨어와 통신 기능을 내장하고 있어, 일상에 혁신적인 편의성을 제공하지만, 연결성에 따른 심각한 보안 취약점을 종종 간과하고 있습니다. 사이버 복원력법(CRA)은 디지털 요소를 포함한 모든 제품(PDE; Products with Digital Elements)에 대해 EU가 사이버보안 기준을 최초로 규정한 법제입니다.

CRA의 핵심 목표

CRA는 이전의 지침이나 규정들과 달리, 특정 산업 부문에 국한되지 않고 대부분의 산업 전반에 적용되는 접근 방식을 취하고 있습니다. CRA는 적용 범위를 의도적으로 광범위하게 설정했지만, 주요 목적은 분명합니다. **제품은 단순히 소비자의 사용 중에만 안전한 것이 아니라, 설계부터 폐기까지 전 수명주기에 걸쳐 보안이 보장되어야 합니다.**

- **보안 내재화: 디지털 제품의 보안 취약점 최소화**
  CRA는 제품을 설계하고 개발하는 초기 단계부터 보안을 내재화하는 것을 핵심 목표로 삼고 있습니다. 이런 방식을 "Secure by Design" 또는 "Secure by Default"로 부르며, 보안을 사후에 추가하는 것이 아니라 제품의 기본 설계 에 포함시키는 개념입니다. 보안 내재화를 통해 공격 표면을 줄이고, 데이터 구조를 보호 하며, 비인가 접근을 방지해 초기 단계부터 제품의 취약성을 최소화할 수 있습니다.

- **수명주기 관리: 보안 업데이트의 일관성과 적시성 확보**
  제품이 시장에 출시된 이후에도 제조업체의 책임은 끝나지 않습니다. 제조업체는 제품이 시장에 출시된 날로부터 5년 동안 또는 예상되는 제품 수명주기 중 더 짧은 기간동안 보안 취약점을 지속적으로 모니터링하고 패치하는 체계를 마련 해야 합니다.

- **보고 의무화: 사용자 대상 투명성 확보**
  취약점이 악용되거나 심각한 보안 사고가 발생한 경우 제조업체는 24시간 이내에 국가 당국에 보고해야하며, 미 보고 시, 제품 회수, 과태료 부과 및 브랜드 신뢰도 하락 위험에 직면할 수 있습니다.

- **책임 공유: 공급망 전반에 걸친 책임 강화**
  CRA의 사이버보안 의무는 제조업체에만 국한되지 않습니다. 수입업체, 유통업체 및 부품 공급사 역시 자사가 제공하는 제품이 CRA 요구 사항을 충족하는지 확인해야 합니다.

  CRA는 제품 사이버 보안에 대한 책임을 공급망 전반에 걸쳐 공유하며, 초기 설계부터 제품의 수명주기 동안 지속적으로 유지되도록 포괄적이고 선제적인 접근 방식을 지향합니다.

제품 적용 대상: CRA의 적용 범위

CRA는 디지털 요소가 포함된 제품을 적용 대상으로 하며, PDE는 네 트워크에 직접 또는 간접적으로 연결되는 모든 하드웨어 또는 소프트웨어로 광범위하게 정의됩니다. 즉, 자동차, 의료기기, 일상 소비재 등 어떤 제품이라도 CRA의 적용 범위에 포함될 수 있습니다.

아래는 CRA가 일반적으로 적용되는 제품 유형의 예시입니다. 모든 사례를 다 포괄하진 않지만, CRA가 얼마나 넓은 범위에 걸쳐 적용되는지 짐작할 수 있습니다.

소비자용 전자제품
스마트 TV, 스피커, 홈 보안 시스템,
게임 콘솔 등

산업용 장비
스마트 팩토리 시스템,
산업용 로봇, 예지 보전 소프트웨어

IoT 기기
스마트 온도조절기, 스마트 도어락,
착용형 스마트 기기, 운동 기록 기기

소프트웨어 제품
클라우드 기반 SaaS 애플리케이션
펌웨어 업데이트 도구, 사이버보안 소프트웨어,
소프트웨어 개발 키트(SDK)

스마트 인프라
네트워크형 CCTV, 전기차 충전 시스템,
교통 신호 제어기, 공공 보안 시스템

자동차용 시스템*
텔레매틱스 ECU, 디지털 계기판
인포테인먼트 시스템, OT 플랫폼
차량용 애플리케이션

디지털 헬스 기기
원격 환자 모니터링 기기,
스마트 체중계, 가정용 피트니스 기기

모바일 애플리케이션
제품 생태계에 포함되는 경우,
기기와 연동되는 앱 또한 CRA 적용 대상임

CRA는 거의 모든 산업에 영향을 미치기 때문에, 시행 당시 업계 전반에 큰 반향을 일으켰습니다. 하지만 이 규정의 적용 대상에는 몇 가지 예외도 존재한다는 점도 함께 이해할 필요가 있습니다.

우선, 대부분의 디지털 제품은 CRA 적용 대상이지만, 기존 EU 법령에 따라 사이버보안 요건이 이미 규정되어 있거나, 맞춤형(비상용) 소프트웨어의 경우에는 예외로 분류됩니다.

예를 들어, 심박조율기나 엑스레이 기기와 같은 의료기기는 기존의 의료기기 규정(EU 2017/745, MDR)에 따라 관리됩니다. 반면, 일반적인 피트니스 트래커나 스마트 체중계는 의료기기 규정(MDR)의 적용 대상이 아니므로 CRA 적용 대상에 해당합니다.

*자동차 산업도 2020년 UNECE의 WP.29 사이버보안 규정 (R155 및 R156) 도입과 함께 유사한 규제 전환을 겪었습니다. WP.29는 차량 전체를 단위 형식 승인 체계를 기반으로 적용되는 반면, CRA는 제품이 시장에 독립적으로 제공되는지 여부에 따라 적용 범위를 판단합니다. 차량 내 부품이나 소프트웨어 요소가 완성차와 함께만 공급되는 구조라면 CRA 적용 대상에서 제외될 수 있습니다. 반면, 시장에 별도로 개별적으로 제공되는 부품이나 소프트웨어는 CRA의 요구사항을 충족해야 할 수 있습니다.

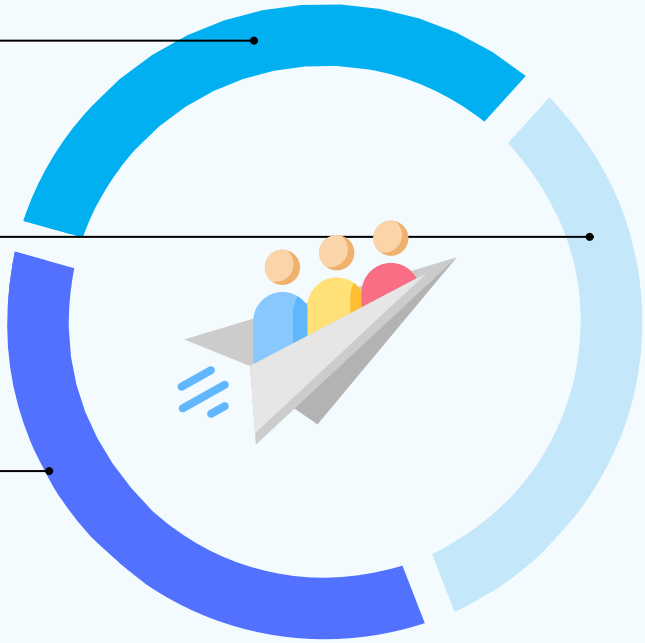
핵심 주체 : CRA는 누구에게 적용되는가?

앞서 언급했듯이, CRA는 사이버보안에 대한 책임을 공급망 전반에 걸쳐 전략적으로 분산하고 있습니다. 사이버보안은 어느 한 기업만의 과제가 아니라, 산업 전체가 공동으로 대응해야 하는 문제입니다. 이에 따라 CRA는 EU 시장에 출시되는 디지털 요소 포함 제품(PDE)에 대해, 의무가 부여되는 공급망 참여자들—예를 들어 제조업체, 수입업체, 유통업체 등을 명확히 정의하고 있습니다.

제조업체
디지털 요소 포함 제품의 설계, 개발, 생산을 담당하는 핵심 주체로서, 제조업체는 규정 준수와 정보 투명성 측면 가장 큰 책임을 집니다.

수입업체
수입업체는 EU 외부에서 수입된 제품이 CRA 기준을 충족하는지 사전에 확인할 책임이 있습니다. 본질적으로 수입업체는 CRA의 첫 관문 역할을 수행하는 주체입니다.

유통업체
공급의 마지막 단계에서, 유통업체는 적합성 마크 또는 필수 문서를 통해 최종 사용자에게 정확한 정보를 전달해야 하며, 제품 리콜이 발생할 경우 이에 협조할 의무가 있습니다.



이 세 가지 핵심 주체 외에도, 공식적으로 운영자로 지정되진 않았지만 PDE 부품 공급사 역시 중요한 역할을 수행하는 경우가 많습니다. 제조업체는 CRA의 엄격한 사이버보안 요구사항을 부품 공급사에게도 적용할 수밖에 없으며, 이를 통해 제품의 설계부터 유통까지 모든 단계에서 보안이 고려하고 반영되도록 해야 합니다. 이러한 구조는 공급망 전체에 걸친 공동 책임이라는 CRA의 핵심 목표를 더욱 강화합니다.

CRA는 규제 환경의 중대한 전환점을 의미하며, 유럽연합 안팎의 디지털 제품 사이버보안을 위한 통합 프레임워크를 제시합니다. 하지만 CRA는 단순히 적용 범위를 이해하는 데 그치지 않습니다. 진정한 효과와 준수를 위해서 CRA의 핵심 철학인 보안 내재화(Secure by Design, Secure by Default) 원칙을 수용하는 것이 필수적입니다.

보안내재화 Secure by Design, Secure by Default

CRA의 핵심은 "Secure by Design"과 "Secure by Default"라는 두 가지 축으로 구성되어 있습니다. 언뜻 유행어처럼 들릴 수 있지만, 이 두 개념은 사이버보안의 근본 철학으로, 제품이 어떻게 개발되어야 하는지뿐만 아니라, 최초 기획 단계부터 어떤 방식으로 구상되어야 하는지 규정합니다. 이는 사이버보안에 대한 책임을 소비자나 최종 사용자로부터 제품을 공급하는 제조업체 및 유통업체로 근본적으로 전환시키는 변화입니다.

두 개념은 하나처럼 보일 수 있지만, 실제로는 제품의 수명 전반에 걸쳐 보안을 강화하기 위해 서로 다른 역할을 수행하는 보완적인 축입니다.

Secure by Design

"Secure by Design" 원칙은 사이버보안을 사후 대응이 아닌 사전 예방 중심의 방어 전략으로 바꾸자는 접근 방식입니다. 보안은 나중에 덧붙이는 선택 사항이 아니라, 제품의 전체 개발 전 과정에 걸쳐 처음부터 체계적으로 계획 되어야 합니다.

보안 계획은 제품의 설계 단계에서 시작해 개발, 테스트, 배포까지 전 과정에 걸쳐 이어져야 하며, 유지 보수 및 운영 단계까지 확장될 수 있습니다. 기업은 먼저 철저한 위협 모델링과 위험 평가를 통해 잠재적인 취약점을 체계적으로 식별하고 완화해야 합니다. 이어서 보안 코딩 표준 적용, 보안 테스트 및 코드 리뷰 절차를 마련하고, 아키텍처 설계 시에는 접근 제어, 데이터 암호화, 중요 기능 간 분리와 같은 내재된 보안 기능을 갖추는 것이 중요합니다.

제조업체는 제품 수명의 초기 단계에 시간과 자원을 투입해야 한다는 점에서 부담을 느낄 수 있습니다. 하지만, 이후 제조 과정은 물론, 제품이 소비자에게 전달된 이후 발생할 수 있는 보안 취약점 해결 비용과 복잡성을 현저히 줄일 수 있습니다.

제품 출시 후에는 취약점 수정이 훨씬 더 복잡하고 비용도 기하급수적으로 증가하기 때문에, 초기 대응이 장기적으로는 훨씬 효과적입니다.

Secure by Default

“Secure by Default”는 소비자가 제품을 인수하는 시점부터 별도 복잡한 설정과 추가 조치 없이 안전하게 사용할 수 있도록 보안이 기본적으로 적용된 상태를 의미합니다. 제품이 기본 보안 설정이 활성화된 상태로 배송 또는 배포되었다는 것을 전제로 합니다.

"Secure by Default"의 적용 방식은 제품마다 다를 수 있습니다. 예를 들어, 제품 최초 사용에 강력한 비밀번호 설정을 요구하거나, 안전한 페어링 메커니즘을 갖추어야 합니다. 또한, 필수적이지 않은 구성 요소와 기능은 기본적으로 비활성화되어야 하며, 최적의 보안 설정이 사전에 구성된 상태여야 합니다.

최초 사용 과정을 기본 설정으로 단순화하는 것은 사이버 보안 인식 부족으로 인해 발생할 수 있는 취약성을 줄이는 방법이며, 결과적으로 사용자를 보호합니다.

규정 준수를 넘어 : 전략적 경쟁력 확보

"Secure by Design"과 "Secure by Default"라는 두 핵심 원칙은 사이버보안 분야에서 매우 중요시 여겨지며, CRA는 이를 다양한 산업 분야에 의무화함으로써 그 중요성을 더욱 부각시키고 있습니다. 특히 시장에 새롭게 진입하는 기업들의 경우, 규정 준수에 시간과 자원을 투자하는 것이 부담스럽게 느껴질 수 에 충분히 이해할 수 있는 반응입니다.

하지만 기업들은 단순 규정 준수 차원을 넘어 전략적으로 자산으로 활용할 수 있다는 점을 이해하는 것이 중요합니다.

- **장기적인 비용 절감 :** CRA 보안 원칙을 도입하는 것은 기업에게 전략적 장점을 제공합니다. 사후 사이버 공격이나 보안 사고 발생 시 복구 비용을 크게 절감할 수 있기 때문입니다. 2024년 IBM 보고서에 따르면, 2024년 기준 데이터 유출 한 건당 평균 피해 비용은 481만 달러에 달했습니다. 일부 소규모 제조업체나 유통업체는 이러한 수치가 자신들에게는 해당되지 않는다고 생각할 수 있지만, 같은 보고서에 따르면 중소기업의 경우에도 보안 사고 발생 시 최소 12만 달러에서 최대 124만 달러의 비용이 발생할 수 있습니다. 직접적인 재정 손실뿐 아니라, 침해 대응에 소요되는 시간, 사고 대응 인력 투입, 매출 손실, 보험료 인상, 규정 미준수에 따른 법적·재정적 불이익까지 포함됩니다.

- **신뢰와 브랜드 평판 구축:** 인터넷을 통해 연결된 기술과 일상 속, 젊은 세대는 사이버 공격의 위험에 더욱 쉽게 노출되고 있습니다. Deloitte 보고서에 따르면, Z세대 응답자의 약 3분의 1이 지난 1년간 소셜 미디어 계정 해킹을 경험한 바 있습니다. 이처럼 보안 침해 사례가 증가함에 따라, 소비자들은 사이버보안 체계가 마련된 기업을 선호하게 되었고, 보안이 강화된 제품은 깊은 신뢰와 긍정적인 브랜드 평판을 형성하는 핵심 요소로 떠올랐습니다. 실제로 동일한 Deloitte 조사에 따르면, 자신이 신뢰하는 기업의 제품(PDE)에는 50% 더 많은 비용을 지출하는 것으로 나타났습니다.

- **시장 경쟁:** 제조업체, 수입업체, 유통업체, 부품공급사가 CRA를 준수하도록 유도하는 규제가 지속됨에 따라, 시장 내 경쟁은 더욱 치열해질 전망입니다. 이러한 변화는 사이버보안을 단순한 기술적 요구사항에서 진정한 차별화 요소로 변화시킵니다. 사이버보안 모범 사례를 적극적으로 도입한 기업은 규제 대응을 넘어 시장 진입 기회를 선점하고, 보안 인식이 높은 소비자 신뢰도 얻을 수 있습니다. 반면, 보안 준비가 부족한 기업은 시장에서 도태될 위협에 직면하고, 결국에는 규정을 충실히 이행하는 경쟁사에 주도권을 내줄 수 밖에 없습니다.

CRA 준수를 위해 강력한 사이버보안은 필수입니다. 하지만, 관련 당사자는 이를 단순한 규제 대응 수준으로 보아선 안됩니다. CRA 준수는 곧 지속적인 성장, 시장 생존력, 그리고 브랜드 신뢰도 향상을 위한 동력인 점을 인식해야 합니다.

CRA 규정 준수를 위한 일정과 전략

CRA 준수는 결코 간단한 일이 아니며, CRA를 도입, 적용하기 위해서는 상당한 시간과 자원이 필요합니다. 이러한 전환이 원활하게 하기 위해 EU는 CRA 규정 법제화를 단계적으로 시행하고 있습니다.

CRA의 법제화 일정

CRA는 2024년 10월에 공식 채택되어 2024년 12월에 발효되었습니다. EU는 제조업체, 수입업체, 유통업체가 제품 수명주기를 CRA 요구사항에 맞춰 조정할 수 있도록 36개월의 유예 기간을 부여했습니다. CRA 법제화의 주요 일정을 상세하게 살펴보겠습니다.

2022년 9월
EU가 사이버복원력법 CRA 제안서를 공식 발표하며, 해당 규제의 프레임워크, 목적, 도입 배경을 제시했습니다. 이 시점을 기점으로 CRA의 공식적인 입법 절차가 시작되었습니다.

2023년 7월
EU 이사회(회원국 대표)와 유럽 의회는 CRA 제안에 대한 입장을 조율하고 공식적으로 최종안을 위한 3자 협상을 개시했습니다.

2023년 11월
EU 이사회와 유럽 의회는 CRA에 대한 3자 협의를 통해 비공식 합의에 도달했습니다.

2024년 3월, 4월
EU 이사회와 유럽 의회는 해당 합의를 공식 승인했습니다.

2024년 10월
CRA는 Regulation (EU) 2024/2847로 공식 서명 및 채택되어 법제화되었습니다.

2024년 11월
Regulation (EU) 2024/2847은 EU 관보(모든 법률, 규정, 결정 등 법적 효력을 가지는 문서가 게재되는 공식 기록지)에 게재되며 공식 공표되었습니다. 이로써 해당 규정은 법적 구속력을 갖게 되었습니다.

2024년 12월
CRA는 2024년 12월 10일부로 공식 발효되었습니다. 이 시점을 기준으로, 규정 준수를 위한 36개월 공식 유예 기간이 시작됩니다.

2026년 9월
36개월의 유예 기간이 주어지긴 하지만, 2026년 9월 11일부터는 제조업체가 실제로 악용된 보안 취약점 및 보안 사고에 대해 반드시 보고해야 하는 의무가 적용됩니다.

2027년 12월
CRA가 발효된 지 36개월이 되는 2027년 12월 10일부터, EU 내에서 유통되는 모든 디지털 요소 포함 제품(PDE)은 CRA를 반드시 준수해야 합니다.

2027년 CRA 전면 시행에 대비한 기업의 준비 과제

CRA가 이미 발효된 만큼, 기업은 2025년과 2026년을 준비를 위한 중요 기간으로 삼아야 합니다.
이 시기를 효과적으로 활용하지 못할 경우, 과도한 대응 비용과 규정 미준수로 인한 차질이 커질 수 있습니다.
따라서, 다음과 같은 주요 준비를 체계적으로 수행해야 합니다.

- **전략 도출 및 격차 평가:** 현재 제품 개발 및 수명주기 관리 프로세스가 CRA 요건에 부합하는지 체계적으로 진단해야 합니다. 제조업체는 우리는 현재 무엇을 하고 있으며, 이는 CRA가 요구하는 바와 어떻게 다른가? 라는 질문을 중심적으로 평가를 진행해야 합니다. 이 과정을 통해 위협 완화를 위한 보안 기술과 운영 방식의 격차를 식별하고 이를 기반으로한 보완 전략 수립의 출발점이 됩니다.

- **취약점 대응 체계 수립:** 제품 판매 후 감시, 보안 사고 보고 및 대응, 패치 배포를 포함한 체계를 구축 및 마련해야 합니다. 취약점 스캐닝 도구와 업데이트 매커니즘 역시 필수입니다.

- **보안 기술의 적극적 구현:** 단순한 설계 및 계획 외에도 적극적인 보안 기술의 구현이 중요합니다. 보안 코딩 적용, 고급 암호화 활용, 시스템 무결성 관리 기술 등을 활용한 강력한 인증 구현과 같은 적절한 기술 도구는 제품 보안을 강화하는 데 필수입니다. 테스트(퍼즈 테스트, 침투 테스트) 또한 이러한 구현을 검증하는 데 필수적인 도구가 될 수 있습니다.

- **기술 문서 및 교육:** 기술 문서, 평가 자료 및 사용자 대상 가이드를 정리하고 제품 개발팀, 법무팀, 규정 준수팀 및 품질 관리팀 등 관련 부서에 대한 교육을 통해 전사적으로 CRA 이해도와 대응 역량을 강화해야 합니다.

- **컨설팅 및 전략적 파트너십 구축:** 많은 기업이 규정 준수를 위한 절차를 시작하는 데 어려움을 겪을 수 있습니다. 이 경우, 사이버 보안 및 규정 준수를 전문으로 하는 외부 컨설팅 기관 또는 파트너와 협력하는 것이 효과적인 전략이 될 수 있습니다. 특히 자동차, 산업용 IoT, 스마트 모빌리티 등 보안 요구 수준이 높은 산업군에서는, 전문가의 프레임워크 설계 및 구현 지원을 통해 전체 프로세스의 리소스 투입과 비용을 크게 절감할 수 있습니다.

CRA를 완벽하게 적용 해야하는 시점인 2027년 12월까지는 아직 시간이 남아 있지만, CRA는 더 이상 먼 미래의 과제가 아닙니다. 이는 다양한 산업 전반에 걸쳐 시급하고 현실적인 이슈이며 초기에 대비한 기업일수록 비용을 절감하고, 혼란을 최소화하며, 신뢰 기반으로 재편되는 시장에서 경쟁 우위를 확보할 수 있습니다.

내부 문제점을 선제적으로 진단하고, 경험이 많은 파트너와 전략적으로 협력하는 기업은 CRA의 요구사항을 충족하는 것을 넘어서 복잡하고 경쟁이 치열한 시장 환경에서 지속 가능한 경쟁력을 갖출 수 있습니다.

다음 글에서는 기술적으로 복잡하고 빠른 혁신이 증가하는 자동차 산업에서 CRA 의미를 구체적으로 살펴보겠습니다.

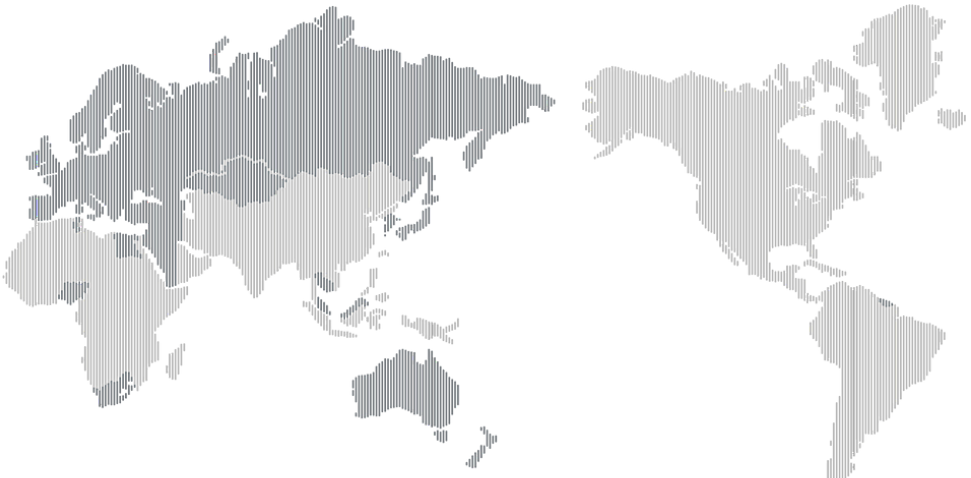
자동차 규제 및 표준 관점에서 본 CRA의 역할

자동차 산업은 기존에 복잡한 법규 및 표준 체계 내에서 운영되고 있기 때문에, 규정 준수가 새로운 개념은 아닙니다. 그러나, 차량이 더욱 연결되고 소프트웨어 정의 구조로 전환됨에 따라 CRA가 UNECE R155 및 R156, ISO/SAE 21434와 어떻게 연계되고 보완 되는 지를 이해하는 것은 필수입니다. 이 규정과 표준은 겉보기엔 상충하거나 중복되어 보일 수 있지만, 그 핵심 목표는 동일합니다.

바로, 차량 생애 주기 전반과 연결된 PDE를 아우르는 통합된 사이버보안 체계를 구축하는 것입니다.

UNECE WP.29, Regulation No. 155 (UN R155)와 CRA

2024년, 유엔 유럽경제위원회(UNECE)는 차량 전반의 사이버보안을 다루기 위한 포괄적 규제 프레임워크인 Regulation No. 155 (UN R155)를 도입했습니다. 이 규정의 핵심 목적은 완성차 제조사(OEM)가 사이버보안 관리 체계(CSMS)를 구축하고 유지하도록 요구하는 것입니다.

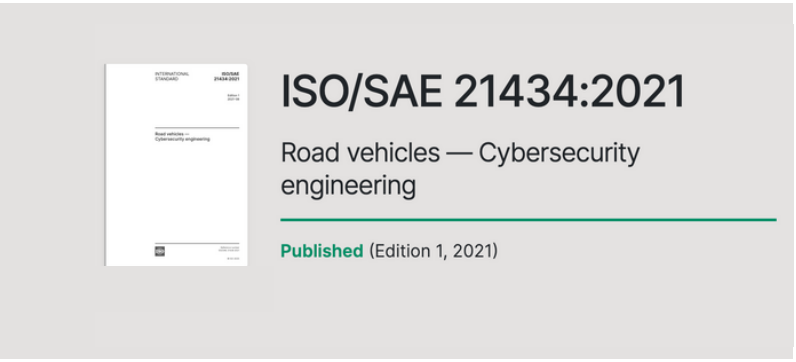


WP.29 참여국가, UN R155, R156의무화

- **범위:** UN R155는 차량 형식 승인(Type Approval)을 위한 규정으로, L (소형이륜차, 오토바이, 사륜 오토바이), M(승용차), N(상용차), O(트레일러, 세미트레일러) 차량에 적용됩니다. 이 규정은 설계 및 개발부터 생산 및 생산 후단계에 이르기까지 차량 수명주기 전반에 걸쳐 사이버보안 위험을 관리하도록 규정합니다.

- **초점:** UN R155는 프로세스 중심의 규정으로, 제조업체가 차량을 보안 위협으로부터 보호하기 위한 절차를 수립하고, 실제 차량에 적용했음을 입증할 것을 요구합니다. 핵심 요건에는 위험 관리 체계, 취약점 식별 및 대응 절차, 사고 대응 메커니즘의 운영이 포함됩니다.

- **CRA와의 연관성 :** UN R155는 완성차에 대한 획기적인 사이버보안 규정으로, 차량 보안 준수 여부를 판단하는 주요 기준으로 작용합니다. CRA는 이러한 특정 법률(예: UN R155) 등으로 이미 규제받는 산업 및 제품에 대해서는 명시적으로 적용 대상에서 제외되도록 설계되어 있기 때문에, 완성차 제조사는 CRA와 UN R155를 동시에 준수할 필요는 없습니다. 다만, CRA는 제품이 시장에 제공되는 방식에 따라 차량의 구성 요소 일부까지 적용될 수 있으므로, CRA의 규제 영향력이 약화된 것으로 보기는 어렵습니다. 이와 관련한 세부 내용은 아래에서 더 자세히 다루겠습니다.



출처: *ISO*

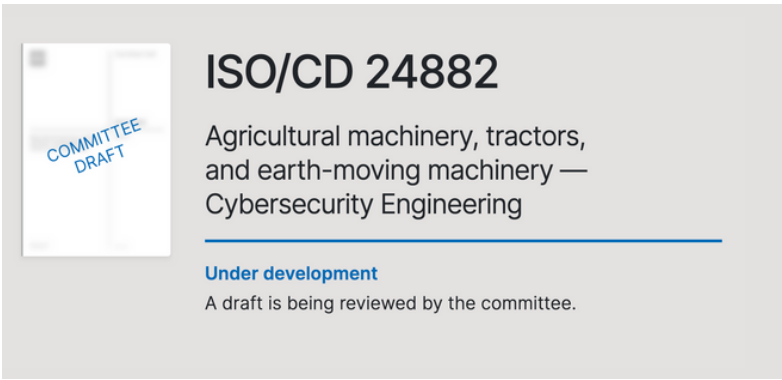
ISO/SAE 21434

ISO/SAE 21434는 국제 표준화 기구(ISO, International Organization for Standardization)와 미국자동차공학회(SAE, Society of Automotive Engineers)가 공동으로 제정한 국제 표준으로, 도로를 주행하는 차량의 사이버 보안 엔지니어링을 위한 체계적 방법론을 정의합니다.

- **범위:** ISO/SAE 21434는 차량 전장 아키텍처(E/E architecture)의 전 생애주기에 걸쳐 사이버보안 활동을 효과적으로 수행하기 위한 실질적인 지침을 제공합니다.
- **초점:** UN R155와 마찬가지로, 본 표준 역시 프로세스 중심의 접근 방식을 따릅니다. 특히, 위협 분석 및 위험 평가(TARA), 사이버보안 개념 개발, 보안 구현, 사이버 보안 V&V(Verification & Validation)에 대한 구체적인 방법론을 포함하고 있습니다.
- **CRA와의 적합성:** ISO/SAE 21434는 UN R155 요구사항을 충족하기 위한 업계 표준으로 자리잡고 있으며, 견고한 사이버보안 관리체계를 수립하는 데 있어 실질적이고 기술적인 방법론을 제공합니다. 이 표준을 준용함으로써 CRA 적용 대상이 될 수 있는 자동차 구성요소의 보안 수준을 평가하고 입증할 수 있는 기준으로 활용할 수 있습니다.

ISO 24882

농업 및 건설 기계의 디지털 연결성이 확대됨에 따라 국제 표준 ISO 24882가 도입되었습니다. 이 표준은 장비 수명주기 전반에 걸쳐 위험 평가 및 관리를 위한 엔지니어링 요구 사항을 정의하며 설계, 개발, 운영, 유지보수 등 전 단계의 사이버 보안 리스크를 식별하고 대응하여 안전을 보장하는 것을 목표로 합니다.



출처: *ISO*

- **범위:** ISO/CD 24882는 2025년 1월 6일에 표준화 작업이 시작된 이후, 현재 CD(Committee Document) 단계에 있으며 아직 공식 표준은 아닙니다. 그럼에도 불구하고, 농업 및 건설 차량/기계 분야에서 사이버 보안 엔지니어링에 특화 지침을 제공하는 문서로서 산업 관계자들이 참고하고 있습니다.
- **초점:** ISO/SAE 21434와 유사하게 ISO/CD 24882는 사이버보안 위험 관리, 보안 기능의 구현, 취약성 모니터링에 대한 지침을 자세히 설명합니다.
- **CRA와의 부합성:** 농업 및 건설 산업 종사자에게 ISO 24882 정식 표준을 준수하는 것은 CRA(사이버복원력법) 요구사항 충족을 입증하는 핵심 수단이 될 수 있습니다. 현재 CD 단계의 문서에서도 해당 산업에 특화된 사이버보안 모범 사례와 적용 지침이 제시되고 있어, 실질적인 참고 기준으로 활용됩니다.

CRA와 기존 법규와 표준과의 연관성

UN R155가 완성차의 사이버보안을 다루는 반면, CRA는 차량에 내장되거나 연동되는 기타 PDE에 대한 보안 요건을 새롭게 도입했습니다. 이는 기존 규정의 적용을 받지 않던 SDV(소프트웨어 정의 차량) 구성 요소와 소프트웨어까지 규제 범위를 확장한 것입니다.

따라서 CRA는 이러한 규제 공백을 보완하기 위해 차량의 모든 부품과 수명주기 전 단계에 대해 사이버보안 검토가 이루어지도록 요구합니다. 이제 CRA가 적용되는 자동차 산업의 구체적인 영역을 살펴보겠습니다.

전장부품의 적용

CRA는 차량 형식 승인의 일부가 아닌, 별도의 제품으로 차량에 탑재되는 개별 부품에 적용됩니다. 여기에는 인포테인먼트 시스템, 독립형 PDE로 분류되는 특정 TCU, 일반 PDE에 해당하는 ADAS 모듈 또는 소프트웨어, 또는 독립형 OTA 플랫폼이 포함됩니다.

농업용 차량

스마트 트랙터, 자율 수확기, 정밀 농업 장비 등 고도로 디지털화된 기계에는 디지털 요소를 포함하고 있어 CRA의 적용 대상이 됩니다. 도로 주행 승인을 받은 완성차는 UN R155의 적용을 받을 수 있지만, CRA는 독립형 디지털 구성 요소, 소프트웨어 및 시스템의 보안을 직접적으로 다룹니다.

건설 차량

농업용 차량과 마찬가지로, 건설 차량 역시 빠르게 디지털화되고 있습니다. 자동 굴삭기, 원격 조종 불도저 등 다양한 장비는 내장형 소프트웨어와 커넥티드 구성 요소에 대한 의존도가 높아지고 있습니다. CRA는 이러한 구성 요소까지 적용 범위를 확대하며, 건설 현장에서 사용되는 운영 기술(OT : Operational Technology) 및 IoT 장치와 관련된 사이버보안 위협을 다룹니다.

스마트 팩토리

CRA는 산업용 로봇과 제조 실행 시스템(MES: Manufacturing Execution System)을 포함하여 스마트 팩토리의 복잡한 디지털 제품 네트워크까지 포괄합니다. 이러한 제품은 다양한 공급망으로 부터 부품과 소프트웨어를 공급받는 경우가 많으며, 이제 CRA의 적용 대상에 포함됩니다. 특히 스마트 팩토리 내에서 부품을 제조·통합하는 특성을 고려할 때, 규정 준수는 안정적인 비즈니스 운영을 위해 필수입니다.

자동차 산업의 사이버 보안 규제 환경이 다층적인 것은 너무나 명확합니다. 이러한 복잡성과 상이한 규정 체계를 효과적으로 대응하기 위해서는 신중한 전략 수립이 필요합니다. (i) 해당 제품이 UN R155, CRA 또는 기타 규제 적용 대상인지, (ii) 어떤 프레임워크(ISO/SAE 21434 또는 ISO/CD 24882)를 활용할지, 또는 (iii) 구성 요소에 다면적인 접근 방식이 필요한지를 평가하는 과정은 필수적입니다. ISO/SAE 21434 및 ISO 24882 외에도, 기타 제품군에는 해당 산업의 특성에 따라 ISO/IEC 27400, IEC 62443, ETSI EN 303 645 등과 같은 별도 표준들이 적용될 수 있습니다.

CRA는 인포테인먼트 장치와 텔레매틱스 시스템부터 스마트 로봇과 농업용 차량 구성품에 이르기까지 다양한 PDE를 직접적으로 다루며, 기존 프레임워크의 공백을 메우는 포괄적이고 견고한 사이버보안 체계를 구성하는데 기여하고 있습니다.

이제 남은 과제는 이러한 요구사항을 자동차 산업의 복잡한 운영 구조와 방대한 공급망 전반에 효과적으로 통합하는 것입니다.

CRA가 자동차 산업에 미치는 영향

CRA는 '디지털 책임성(Digital Accountability)'의 새로운 시대를 여는 규제로 평가됩니다. 그동안 UN R155 및 ISO/SAE 21434와 같은 규정과 표준이 업계 전반에 보안 프레임워크 구축을 촉구해왔다면, CRA는 자동차 전체 공급망에 걸쳐 보다 근본적인 운영상의 변화를 요구합니다. 특히, 개별 디지털 구성 요소에 대한 규제 집중도를 높이며 실질적인 보안 책임을 촉진합니다. 이제 CRA를 통해 변화가 예상되는 주요 운영 영역들을 자세히 살펴보겠습니다.

설계 및 개발 프로세스의 재정의

자동차 산업 전반은 제품 개발에 대한 전면적인 재구성을 맞이하게 될 것 입니다. 위협 및 위험 평가는 차량 생태계 내 모든 디지털 구성 요소로 확대되며, 하드웨어와 소프트웨어에 걸쳐 엄격한 보안 개발 기준이 적용됩니다. 이에 따라 많은 자동차 제조사는 사이버보안 전문 교육을 받은 엔지니어를 확보하고, 차량 제품 개발 수명 주기(VPDL: Vehicle Product Development Lifecycle) 전반에 걸쳐 정교한 보안 프로세스를 통합해야 할 필요성이 커지고 있습니다.

사이버보안의 포괄적인 사후 관리

CRA의 가장 큰 특징 중 하나는 제품에 대한 사이버보안 책임을 제품 수명 이후까지 확장한다는 점입니다. 자동차 제조사는 취약점 관리 체계를 수립하고, 제품 출시 후 최소 5년 또는 명시된 수명주기 기간 동안 발견된 보안 결함에 대해 신속한 패치를 제공해야 합니다. 이를 위해 OTA(Over-the-Air) 업데이트 기능은 필수이며, 효과적인 사고 대응 체계 또한 핵심 요소로 부상하고 있습니다.

적합성 평가 및 CE 마크

CRA에서 Critical 제품 또는 Class II 제품에 해당하는 PDE는 제3자 적합성 평가를 반드시 거쳐야 합니다. 이 평가는 제조업체가 자사 제품이 CRA의 필수 사이버보안 요건을 충족함을 입증하는 절차로, 본질적으로 완성차의 차량 형식 승인(VTA)과 유사한 방식으로 운영됩니다. 해당 절차를 통과한 제품에는 유럽 연합 시장에 출시를 위한 인증 표시인 CE (Conformité Européenne) 마크가 부착됩니다.

법적 의미와 책임

CRA는 자동차 산업 전반의 주요 이해관계자들에게 보다 강화된 법적 책임을 부여합니다. 요건을 준수하지 않을 경우, 최대 1,500만 유로 또는 전 세계 매출의 2.5%에 달하는 벌금, 유럽 시장 내 판매 금지, 그 외 다양한 제재 조치가 부과될 수 있습니다. 이에 따라 자동차 제조사는 법무팀과 리스크 관리팀을 중심으로 기존 사이버보안 전략, 보험 적용 범위, 그리고 잠재적 법적 책임을 전면 재검토할 필요성이 커지고 있습니다.

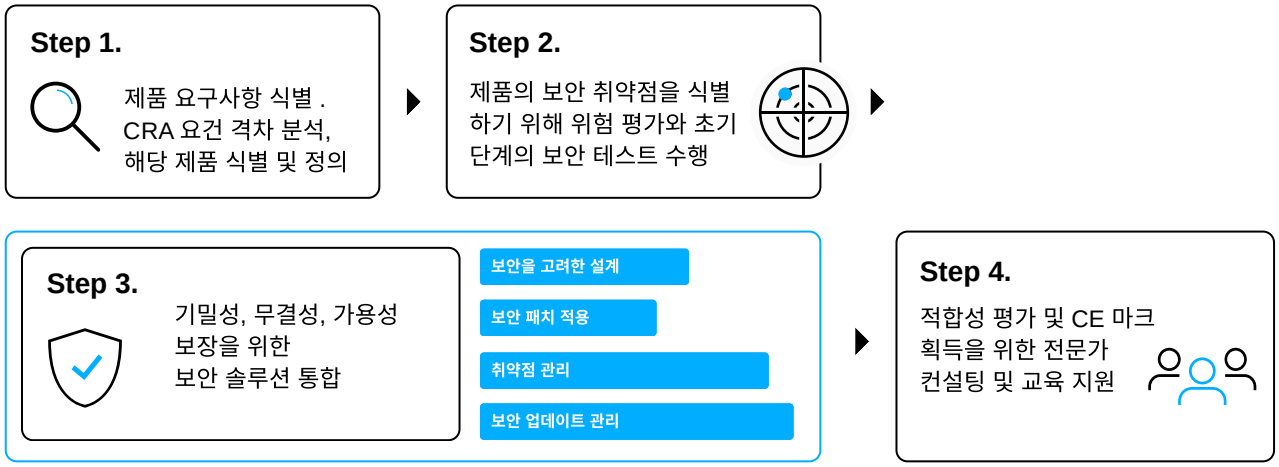
CRA의 광범위한 요구사항과 점점 복잡해지는 차량 시스템 환경을 고려할 때, 이러한 변화에 대응하기 위해선 내부 팀의 역량만으로는 한계가 있습니다. 초기 설계 단계부터 보안을 구현하려면 고도의 전문 지식, 검증된 사이버 보안 방법론, 그리고 기존 규정 및 표준에 대한 명확한 이해가 필수입니다. 그러나 많은 기업은 이러한 역량을 내부에 충분히 갖추지 못한 경우가 많습니다. 이에, 외부 사이버 보안 전문 기업과의 협업은 규정 준수 체계를 효과적으로 수립하고, 전체 프로세스를 가속화하는 데 핵심적인 역할을 할 수 있습니다.

변화에 적응하기 위한 파트너십: CRA에서 아우토크립트의 역할

CRA 준수를 목표로 하는 자동차 제조사 및 부품 공급업체는 전담 사이버보안 전문가와의 협력을 통해 전략적 이점을 확보할 수 있습니다. 아우토크립트는 자동차 사이버보안 분야를 선도하는 기업으로서, 고객이 CRA 규정 준수 과정에서 마주하는 복잡한 요구사항을 효과적으로 해결할 수 있도록 지원하는 독보적인 역량을 보유하고 있습니다.

CRA 준수를 위해서는 자동차 사이버보안뿐만 아니라, IT 보안 전반에 대한 고도화된 역량이 요구됩니다. 아우토크립트는 IT 보안 분야에서의 오랜 경험을 바탕으로, 커넥티드카 및 자율주행차(CAV) 사이버보안 분야에서 전문성을 축적해 왔습니다. 또한, UN R155 준수를 위한 프레임워크를 선도적으로 구축한 기업 중 하나로서, CRA의 핵심 요구사항을 직접 충족하는 End-to-End 솔루션을 제공합니다. 아우토크립트는 제품 수명주기 전반에 걸쳐 다양한 보안 기술과 서비스를 제공하며, 고객의 단기적 과제부터 장기적 전략에 이르기까지 요구에 맞춘 맞춤형 대응이 가능합니다.

아우토크립트는 자동차 제조사 및 전장 부품 공급사와의 긴밀한 협업을 통해 CRA 요구사항 충족은 물론, 글로벌 시장에서의 경쟁력 확보까지 지원할 수 있는 역량을 갖추고 있습니다.



요건 분석 및 로드맵 도출: 아우토크립트는 CRA를 포함한 주요 사이버 보안 규정 준수 상태를 평가하기 위해 포괄적인 격차 분석 서비스를 제공합니다. 이를 통해 현재 보안 프레임워크의 부족한 지점을 명확히 파악하고, 완전한 규정 준수를 위한 실행 가능하고 맞춤화된 로드맵을 도출할 수 있도록 지원합니다.

취약점 관리 및 사고 대응 체계 구축: 아우토크립트의 전문가 팀은 자동차 PDE를 대상으로 한 보안 위협 및 취약점을 지속적으로 모니터링하며, 적시에 탐지하고 대응할 수 있는 체계적인 관리 프로세스를 구축 및 최적화합니다. CRA에서 요구하는 사고 보고 의무를 안정적으로 이행할 수 있습니다.

사이버 보안 테스트 도구 및 V&V 서비스: 아우토크립트는 퍼즈 테스트, 침투 테스트, 취약성 평가 등을 포함한 종합적인 사이버보안 검증 및 검증(Verification & Validation) 서비스를 제공합니다. 다양한 배포 옵션을 통해 자동차 디지털 제품의 복원력을 철저히 테스트할 수 있으며, 고위험 제품에 대한 보안 신뢰도를 강화할 수 있습니다.

적합성 평가 및 CE 마크 획득 지원: 아우토크립트는 풍부한 실무 경험과 전문 역량을 바탕으로, 규정 준수 입증에 필요한 기술 문서 작성 및 제출을 단계별로 지원합니다. 이를 통해 제조사가 CE 마크를 원활하게 획득하고, 유럽 시장 진입을 가속화할 수 있도록 돕습니다.

CRA 규정 준수는 다양한 기술 요건과 절차적인 요구를 포함하는 복잡한 과정입니다. 아우토크립트는 엔지니어링 영향 분석과 보안 아키텍처 구현에 대한 실무 전문성을 바탕으로, 고객이 규정에 효과적으로 대응할 수 있도록 체계적인 방법을 제공합니다.

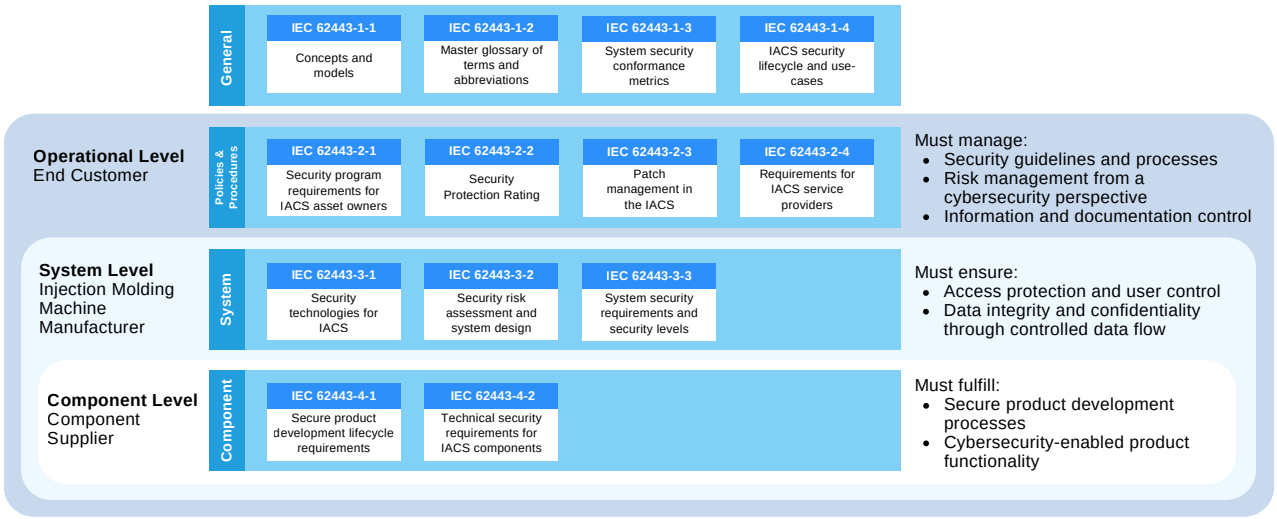
CRA는 비교적 새로운 규제 프레임워크이지만, 아우토크립트는 이미 다양한 산업 분야의 기업들을 대상으로 CRA 요건 충족을 위한 지원 프로세스를 선제적으로 수행하고 있습니다. 컨설팅, 구현, 그리고 규정 준수 지원에 이르기까지, 위임된 요구사항을 실행 가능한 기술 솔루션으로 전환하는 아우토크립트의 실질적 역량을 살펴보겠습니다. 아래 CRA 프로젝트의 두 가지 구체적인 사례는 아우토크립트의 실질적인 적용 역량과 실행 능력을 잘 보여줍니다.

사례1: 사출 성형기를 위한 CRA 적용 컨설팅

PDE가 포함된 유명 사출 성형기를 제조하는 한 기업은, 곧 시행될 CRA 규정에 대한 대응이 시급한 과제로 떠올랐습니다. 특히 산업용 자동차 제조 기계에 특화된 명확한 지침이 부재한 상황에서, 이 기업은 선제적으로 제품 평가와 사이버보안 체계 강화를 추진하고자 했습니다.

아우토크립트는 해당 제조사와 협력하여, 자사의 사이버보안 프레임워크를 산업용 보안 분야의 대표적인 국제 표준인 IEC 62443 시리즈에 기반해 재정비했습니다. IEC 62443은 산업 자동화 및 제어 시스템(IACS: Industrial Automation and Control Systems)의 사이버보안 요구사항을 정의한 비의무적 표준이지만, 업계에서는 사실상 모범 규범으로 널리 인식되고 있습니다.

CRA는 IEC 62443을 직접적으로 언급하지는 않지만, 많은 산업용 제조 기업들은 이를 CRA 요구사항에 대한 해석 및 준수 전략의 근거로 활용하고 있습니다. 특히 IEC 62443 기반의 보안 체계는 CRA에서 요구하는 사이버 복원력 요건을 충족합니다.



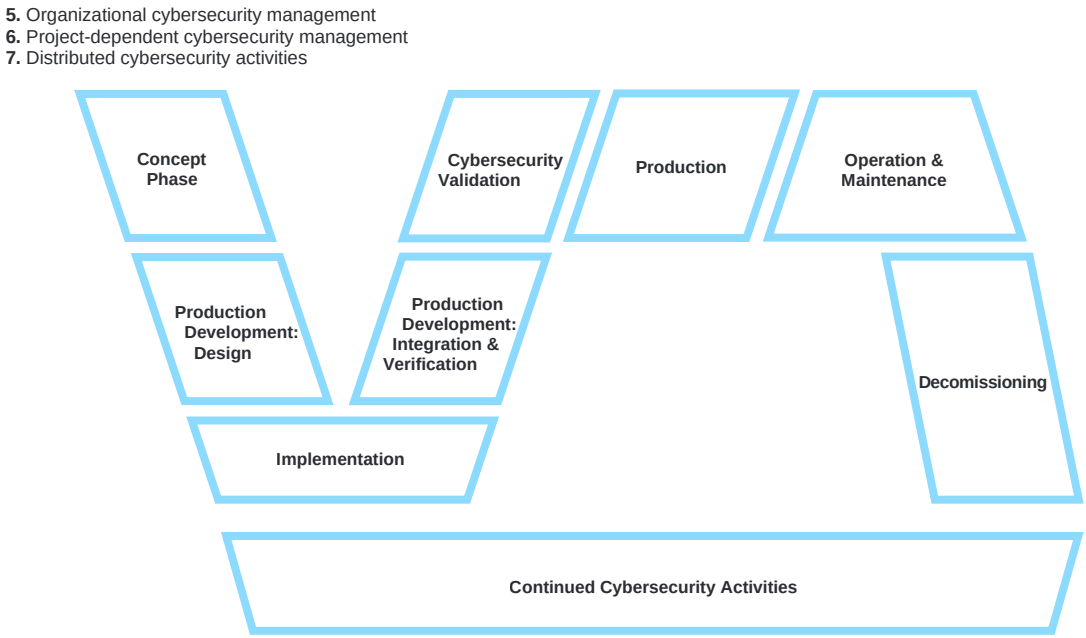
IEC 62443 series and CRA compliance responsibilities by domain

아우토크립트는 제조업체와 협력하여, CRA 및 IEC 62443 표준을 기반으로 사출 성형 기계의 엔지니어링 구조와 기존 사이버 보안 프레임워크에 대한 포괄적인 영향 분석을 수행했습니다.

결과: 아우토크립트는 이 분석을 통해 특정 취약점을 파악하고 맞춤형 완화 전략을 수립했습니다. 그 결과 제조업체는 기존 시스템 아키텍처를 변경하지 않고도 엄격한 CRA의 엄격한 요건을 준수할 수 있었습니다.

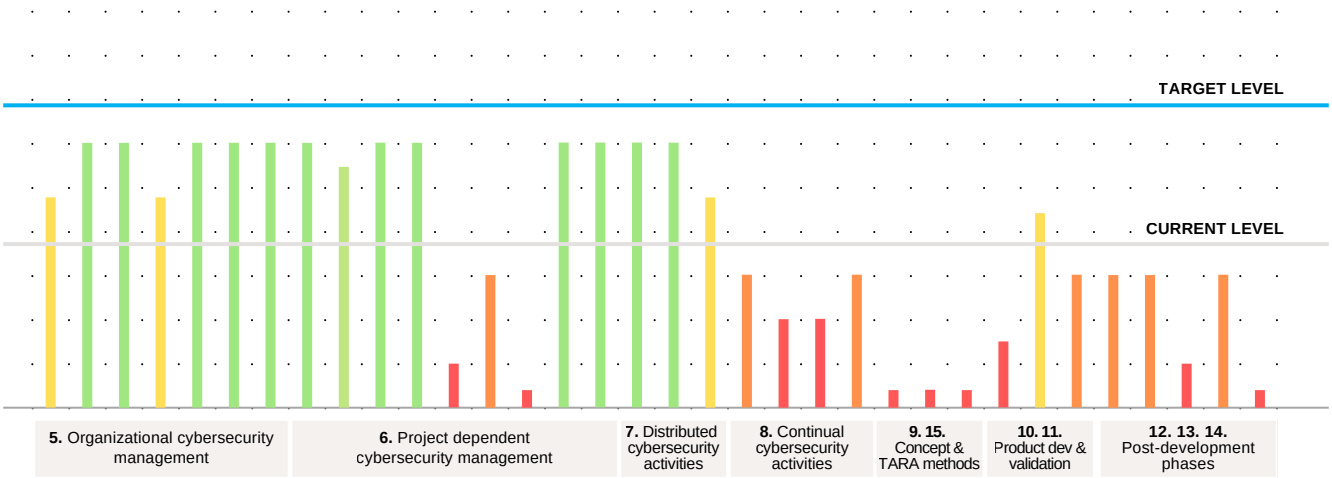
사례 2: 기업의 CRA 대응 사이버보안 점검 및 역량 강화

CRA의 복잡한 규제 환경에 대응하고자 한 대기업은 아우토크립트와 협력하여 전사적인 사이버보안 준비 상태를 점검했습니다. 아우토크립트는 ISO/SAE 21434 프레임워크를 기반으로, CRA 요구사항 전반에 대한 정밀 분석을 수행했습니다.



ISO/SAE 21434 process

결과: 아우토크립트는 현재의 사이버 보안 성숙도와 CRA가 요구하는 목표 수준 사이에 격차가 존재함을 발견했습니다. 이 격차는 고위급 조직 거버넌스부터 구체적인 개발 후 활동까지 포함되었으며, 아우토크립트는 해당 기업을 위해 몇 가지 실행 가능한 프로세스와 개선 사항을 제시했습니다.



Summary of results from corporate analysis

또한, 아우토크립트는 30개 이상의 부서를 대상으로 광범위한 교육을 실시하여, 사이버보안에 대한 조직 전반의 운영 인식을 크게 향상시켰습니다. 이러한 지원을 통해 팀 간 협업 체계가 개선되었으며, CRA에 부합하는 보안 관행을 조직적으로 신속하게 도입할 수 있었습니다. 아우토크립트는 적합성 평가를 철저히 이행하기 위해 관련 기관과의 협업도 지속하고 있습니다.

결론

CRA(Cyber Resilience Act)는 유럽연합을 넘어 전 세계 디지털 제품 생태계를 재편하는 혁신적 규제로 주목받고 있습니다. 자동차 산업에 있어 CRA는 기존의 사이버보안 규정과 표준을 보완하며, 설계·개발부터 생산, 유지관리 전 단계에 걸쳐 제품 수명주기 전반의 보안 취약성을 보완하게 될 것입니다.

이 백서에서 살펴본 바와 같이, CRA는 단순한 규정이 아닙니다. CRA는 모든 디지털 제품, 특히 자동차가 보안을 최우선 가치로 두어야 한다는 강력한 선언이며, 상호 연결적 환경에서 그 책임과 의무는 이제 소비자뿐 아니라 공급망의 모든 구성원에게까지 확장되고 있습니다. 이를 통해 PDE의 전반적인 사이버 복원력이 강화되며, 나아가 우리의 일상생활 전반에도 영향을 미치게 될 것입니다.

이러한 변화는 보안을 사후 고려 사항이나 일회성 대응이 아닌, 장기적이고 체계적인 과제로 받아들여야 함을 의미합니다. 특히 자동차 산업처럼 공급망이 복잡하고 사회적 파급력이 큰 분야에서는, CRA가 요구하는 기술적·조직적 보안 요건을 충족하기 위해 전사적인 변화가 요구됩니다.

이러한 요구사항을 단독으로 대응하기는 쉽지 않습니다. 조직 및 기술 구조 전반에 걸친 변화에는 전문 인력, 검증된 방법론, 그리고 규정에 대한 깊은 이해가 필수적이며, 소규모 기업과 단순 팀이 감당하기 어려운 영역일 수 있습니다.

아우토크립트는 주체들이 이러한 도전 과제를 기회로 전환할 수 있도록 돕는 신뢰할 수 있는 글로벌 보안 파트너입니다. 공급망의 모든 주체가 규정 준수의 전 과정을 효과적으로 수행할 수 있도록, 기업이 규제를 전략적 우위로 삼아 시장 경쟁력을 확보할 수 있도록 돕습니다. 고객사는 시장 내에서 성공뿐만 아니라, 글로벌 제품에 대해 최고 수준의 보안 표준을 제공하는 선도 기업으로 자리잡을 수 있습니다.

[문의]

CRA 대응, 컨설팅, 기술 지원, 백서 내용에 관련하여
더 자세한 문의가 필요하신 경우 아래 이메일로 연락 주시기 바랍니다.

아우토크립트 마케팅팀 | mkt1@autocrypt.io

AUTOCRYPT