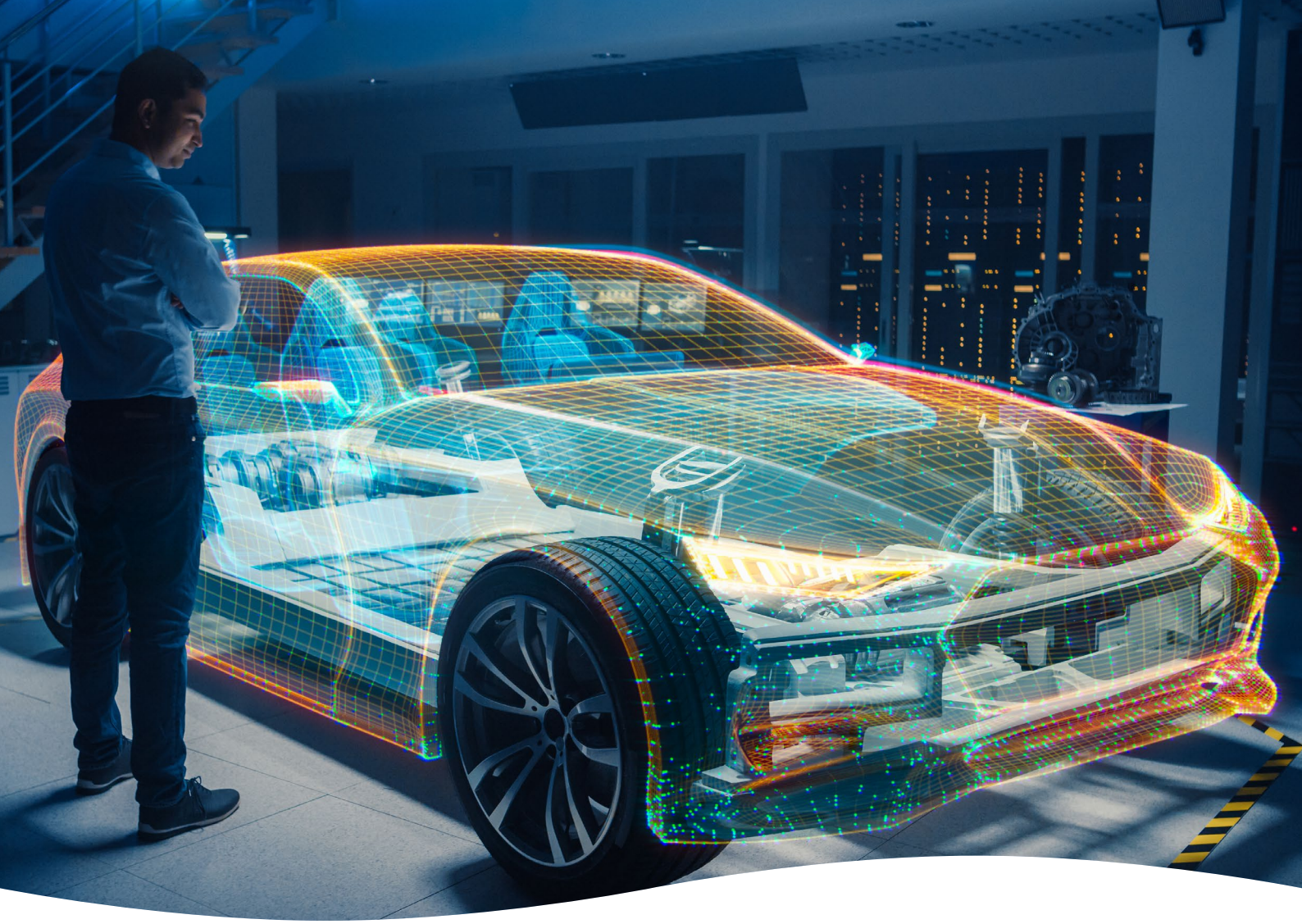


Automotive Cybersecurity.

자동차 보안 - 변화하는 자동차 산업에서 안전한 프로세스를 위한 인증/기술지원

www.tuv.com

TÜVRheinland®
Precisely Right.

미래 자동차의 안전을 위한 시작

UN 사이버 보안 규정이 자동차 제조사 및 공급업체에 미치는 영향과 해당 요구사항을 구현하기 위한 TÜV 라인란드의 솔루션

디지털화는 자동차 분야에도 영향을 미쳤습니다. 자율주행과 같은 기술의 발전과 차량 및 교통 인프라의 연결성 증가로 안전성이 향상되었지만, 동시에 새로운 위험도 발생하고 있습니다.

이러한 위험 중에서 사이버 보안은 특히 중요합니다. 1958년 협약에 따라 UN 유럽 경제 위원회(UNECE, United Nations Economic Commission for Europe)는 자동차의 개발, 생산 및 전체 서비스 수명 동안 사이버 보안을 보장하기 위해 사이버 보안에 대한 새로운 규제 요구사항 R155와 소프트웨어 업데이트에 대한 R156을 제정하였습니다. 동시에 2021년 8월에 발표된 ISO/SAE 21434 표준(도로 차량 - 사이버 보안 엔지니어링)은 조직에 새로운 규정을 적용할 수 있는 방법을 제공합니다.

제조사가 일관되고 구속력 있는 규제 프레임워크를 갖게 된 것은 이번이 처음입니다. 제조사는 사이버 보안과 관련하여 전체 공급망을 관리해야 하므로 UN 규정은 간접적이지만 공급업체와도 관련이 있습니다.

TÜV 라인란드는 여러분과 함께 미래 모빌리티를 안전하게 만들고, 모든 운전자의 신뢰를 향상시키고자 합니다. TÜV 라인란드는 수십 년 동안 자동차 산업의 국제 제조사 및 공급업체와 성공적으로 협력해 오고 있습니다.

TÜV 라인란드는 생산, 통신, 승인, 자동화 시스템 사용과 관련된 모든 보안 문제에 대한 인증/기술지원 서비스를 제공하며, 관련 업계를 지원합니다.

새로운 모빌리티의 도전 과제는 그 어느 때보다 복잡합니다. TÜV 라인란드의 전문가가 관련 규정을 준수할 수 있도록 지원해 드립니다.

한눈에 보는 서비스 이점:

- 사이버 보안 관리 시스템(CSMS, Cybersecurity management system)에 대한 UNECE 준수 프로세스 및 절차의 계획, 정의 및 구현 지원
- 전체 밸류 체인(Value Chain)에 따른 관련 규범 및 표준에 대한 지식
- UN 사이버 보안 규정 및 ISO/SAE 21434 표준이 적용되는 모든 영역(개발, 생산, 운영, 유지보수 및 폐기)에 대한 전문성
- UN 사이버 보안 규정 및 ISO/SAE 21434 표준에 기반한 추가 위험 분석

제조사를 위한 인증/기술지원

TÜV 라인란드의 전문가는 자동차의 전체 수명 주기에 걸쳐 모든 프로세스에서 지원합니다.

공격 가능성의 증가

자율주행은 환경과의 끊임없는 교환이 필요합니다. IT 시스템 및 소프트웨어 시스템은 텔레매틱스(telematics)와 같은 다양한 통신 엔드포인트(endpoints)와 편의 기능, 모빌리티 서비스의 통신을 보장합니다. 이는 차량을 정보 허브로 만드는 동시에 사이버 공격의 표적이 되기도 합니다. 결과적으로 연결 수준이 높아짐에 따라 잠재적 공격 가능성이 증가합니다.

이러한 새로운 위협은 차량 보안에 직접적인 영향을 미칩니다. 이러한 위험을 완화하고 새로운 차량을 시장에 출시하기 위해서는 요구사항에 지정된 목표가 충족되었음을 입증해야 합니다.

이를 위해서는 적절한 수준의 지속 가능한 보안뿐만 아니라 차량의 전체 수명 주기에 걸쳐 적응이 필요합니다.

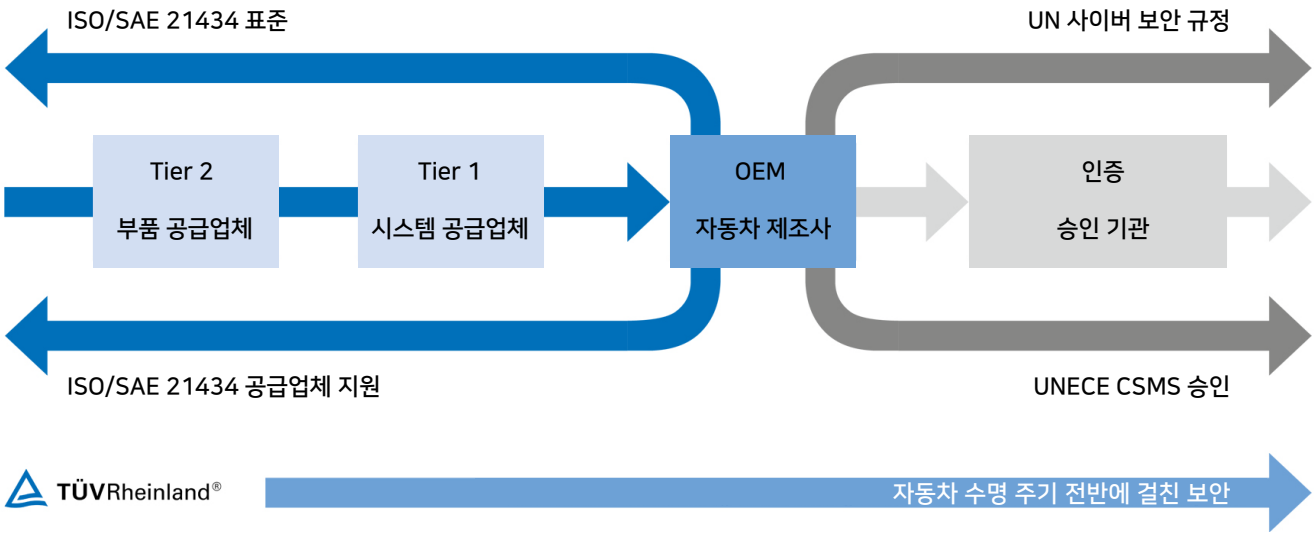
사이버 보안 관리 시스템(CSMS)

UN 규정에 명시된 사이버 보안 요구사항은 복잡합니다. 취약점, 공격 방법, 차량이나 백엔드(backend)를 대상으로 하는 위협에 대한 방어 등의 문제에는 올바른 프로세스와 특별한 노하우가 필요합니다.

TÜV 라인란드는 UN 규정을 준수하고 기존 규범 및 표준에 부합하는 관련 개념과 프로세스를 정의 및 구현하여 자동차 제조사를 지원합니다.

사이버 보안 거버넌스를 확립하고 지속 가능하게 유지하며 공급망에서 적극적으로 관리하기 위해서는 사이버 보안 관리 시스템(CSMS)이 필요합니다. 이를 위해서 관련된 모든 이해관계자의 적절한 인식과 역량을 바탕으로 지속적인 개선 프로세스가 필요합니다.

사이버 보안은 전체 공급망에 영향을 미칩니다.



UN 사이버 보안 규정에 대한 협의

새로운 규정 요구사항에 따라 자동차 제조사는 규정을 준수하는 프로세스를 구축해야 합니다. 워킹그룹의 해석 문서(interpretation document)에서 권장하는 ISO/SAE 21434 표준을 사용하여 UN R155를 준수할 수 있습니다.

TÜV 라인란드의 전문가는 필요한 공정성을 보장하며, UN 규정 R155를 준수하는 사이버 보안 관리 시스템(CSMS)을 위한 프로세스 및 절차의 계획, 정의 및 구현을 지원합니다. TÜV 라인란드의 전문가는 형식 승인 프로세스에 능통하며, 규제 당국 및 기술 서비스와의 상호 작용은 물론 형식 승인을 지원합니다. EU 지침, EU 규정 및 UN 규정의 내용 및 구조와 같은 주요 측면을 모두 포함합니다.

ISO/SAE 21434 표준에 대한 협의

TÜV 라인란드는 ISO/SAE 21434 표준 요구사항에 따라 CSMS를 정의하고 구현하도록 지원합니다. 여기에 정의된 조항 외에도 기존 프로세스와 프레임워크에 따라 조정하고 문서화할 수 있는 권장 사항을 제공합니다.

CSMS 가이드라인 작성을 위한 권장 사항:

- 리스크 평가
- 보안 및 해당 테스트 사양
- 인터페이스 사양
- 테스트 시나리오
- 심사 준비

CSMS 프레임워크 생성을 위한 권장 사항:

- 사이버 보안 프로세스
- 보안 정책
- 밸류체인에 따른 차량에 대한 사이버 보안 위협 감지
- 사고 관리
- 근거 자료

연결성은 공격 가능성을 증가시킵니다.

최신 차량은 인터넷, GPS, 모바일 통신 및 기타 인터페이스를 통해 수많은 앱과 서비스, 클라우드 및 백엔드를 통해 OEM과 연결됩니다. 따라서 근본적으로 변화된 위협 시나리오에 대한 새로운 규정과 전문 기술 협의가 필요합니다.

공급업체를 위한 인증/기술지원

TÜV 라인란드는 공급업체와 서비스 제공업체의 사이버 보안의 계획, 정의 및 구현을 지원합니다.

UN 사이버 보안 규정에 대한 컨설팅

제조사 외에도 UN 사이버 보안 규정에 영향을 받는 이해관계자가 있습니다. 공급업체도 사이버 보안에 영향을 미칠 수 있는 구성 요소를 생산하므로 예상되는 요구사항을 숙지해야 합니다. 그러므로 전체 공급망에 걸쳐 새로운 사이버 보안 요구사항이 통합될 것으로 예상됩니다.

TÜV 라인란드는 공급업체와 서비스 제공업체가 프로세스 및 절차를 구현하여 원활하게 제조사에 통합될 수 있도록 지원합니다. 자동차 제조사에서 사용하는 ISO/SAE 21434 표준과 UN 사이버 보안 규정의 모든 프로세스 및 요구사항에 대해 잘 알고 있는 숙련된 TÜV 라인란드 전문가의 전문 지식을 활용하십시오.

또한, TÜV 라인란드는 EU 지침, EU 규정 및 UN 규정의 내용과 구조를 통합하고 이러한 요구사항을 준수하여 적용하도록 공급업체를 지원합니다.

ISO/SAE 21434에 따른 CSMS 구축

공급업체는 항상 최신 기술을 따라야 합니다. TÜV 라인란드는 공급업체가 ISO/SAE 21434 표준의 요구사항을 충족하는 프로세스를 정의하고 구현하도록 지원합니다.

사이버 보안 관리 시스템을 구축하면, 공급업체는 해당 사이버 보안 문화에 따라 규정을 준수하는 사이버 보안 거버넌스를 수립하고 지속 가능하게 유지할 수 있습니다.

여기에서도 지속적인 개선 프로세스는 관련된 모든 이해관계자의 인식 및 역량과 일치해야 합니다.

공급업체로서 자동차 분야에 대한 TÜV 라인란드의 전문 지식을 활용하십시오. 예를 들어, ISO/SAE 21434 표준을 기반으로 위험 분석을 수행하여 ISO/SAE 21434 표준의 요구사항에 따라 조직에 특정한 규칙과 프로세스를 검토하고 최적화합니다.

갭 분석(Gap Analyses)

제조사와 공급업체가 UN 사이버 보안 규정 및 ISO/SAE 21434의 요구사항에 따라 전략적 및 운영상의 격차를 줄이는 방법

카테고리 M 및 N의 차량 제조사는 UN 사이버 보안 규정 및 부분적으로는 ISO/SAE 21434 표준의 영향을 받습니다. 규정을 준수하는 제품을 개발하고 제조하기 위해서 표준은 CSMS의 구현을 요구합니다.

이러한 목표를 달성하기 위해서 TÜV 라인란드는 기존 프로세스와 계획된 프로세스를 UN 사이버 보안 규정의 요구사항 및 ISO/SAE 21434 표준과 비교하여 갭 분석을 수행해 차이(gap)를 식별합니다. 조사 결과에 대한 자세한 설명과 그에 따른 권장 사항을 바탕으로 문제를 해결하는 데 필요한 솔루션을 제공합니다.

귀사의 현재 상황에 대한 지속 가능한 평가와 더불어, 비용과 노력에 대한 예측을 포함하여 현실적인 계획에 대한 전문적인 기반을 구축해 필요한 규정을 준수할 수 있도록 합니다.

공급업체도 간접적으로 UN 사이버 보안 규정의 영향을 받으며 ISO/SAE 21434 표준을 통해 기본 요구사항을 구현할 수 있으므로 TÜV 라인란드는 갭 분석에서 관련 공급업체 프로세스를 이 표준의 요구사항과 비교합니다.

갭 분석을 통한 이점:

- 기존 격차(gap) 식별
- 권장 사항의 수용
- 결과에 대한 상세한 설명
- 현실적인 계획 수립을 위한 기반
- 지속 가능한 성숙도 평가
- 필요한 노력 예측

제조사와 공급사를 위한 추가 서비스

UN 사이버 보안 규정 및 ISO/SAE 21434 표준에 대한 준비 – TÜV 라인란드 서비스는 고객의 특정 요구사항을 충족합니다.

리스크 상세 분석

자동차 부문에서 ISO/SAE 21434는 TARA(Threat Analysis and Risk Assessment)라는 통일된 용어와 절차를 확립했습니다. 이 리스크 분석(고려해야 할 기능)에는 다른 영역에서도 알려진 기본 질문 및 이에 대한 답변이 포함됩니다.

어떤 분석이 있나요?

기존 자산에 대해 이해하고, 보호 자산을 정의하며, 자산 가치에 대한 명확성을 확립합니다.

무엇을 분석하나요?

위협 식별, 피해 범위 평가, 공격 가능성 평가

분석을 통해 무엇을 할 수 있나요?

완화, 이전 또는 수용을 통해 리스크를 해결합니다.

리스크 평가 지원

- 워크숍 계획, 준비 및 구현
- 자산을 식별하고 손상 정도를 결정하기 위한 인터뷰
- 위협 식별
- 공격 타당성 평가
- 리스크 완화를 위한 제안

컴포넌트, 시스템 및 애플리케이션에 대한 침투 테스트 및 보안 분석

TÜV 라인란드는 20년 이상 침투 테스트 및 보안 분석을 수행하고 있습니다. TÜV 라인란드는 하드웨어 및 소프트웨어 구성요소의 취약점을 식별하고 해커의 공격에 대해 실행된 보호 조치의 효과성을 확인할 수 있도록 지원합니다. 자동차 산업의 제조사 및 공급업체를 위한 침투 테스트는 웹 애플리케이션, 인프라 및 자동차 부품을 포함합니다. 테스트는 민감한 영역 및 데이터에 액세스하여 해당 영역을 조작하거나 기능을 제한할 수 있는 제어 장치 또는 웹 애플리케이션과 같은 시스템에서 해커가 잠재적으로 악용할 수 있는 취약성에 중점을 둡니다.

자동차 부품의 침투 테스트

최신 차량에서 많은 임베디드 시스템(embedded systems)은 다른 임베디드 시스템인 전자 제어 장치(ECU, Electronic Control Units)에서 정보를 수집 및 표시하는 계기판이나 위치 데이터를 처리하고 그에 따라 배포하는 텔레매틱스 시스템(telematics system)에 상관없이 상호 작용합니다.

이 모든 시스템은 차량에서 중요한 기능을 수행합니다. 그러나 환경과 자동차 간의 상호 연결성이 증가하면서 위협 시나리오가 급격히 변화하고 있습니다. 과거에는 공격을 위해 차량에 물리적 존재가 필요했지만 이제는 설치된 무선 모듈을 사용하여 인터넷이나 다른 통신 인터페이스를 통해 공격할 수 있습니다.

이는 보안 요구사항과 차량의 E/E 아키텍처에 심각한 결과를 초래합니다. 그리고 ISO/SAE 21434에서 강조한 바와 같이 모든 개발 프로세스는 그에 따라 조정되어야 합니다. 따라서 차량의 전체 수명 주기에 걸친 자동차 부품의 침투 테스트가 권장되는 방법입니다.

먼저 TÜV 라인란드는 취약성을 식별하고 구현된 보호 조치의 효과를 측정하기 위해 다양한 단계를 수행합니다.
정보 수집의 일환으로 개별 구성 요소 및 하위 구성 요소의 구조를 인터페이스와 함께 살펴봅니다. 이를 통해 구성 요소와 그 기능 및 공격 표면 간의 관계를 알아낼 수 있습니다.

다음 단계에서 그 기능을 테스트하기 위해 TÜV 라인란드 또는 고객의 부지에 컴포넌트를 설정합니다. 필요한 경우 잔류 버스 시뮬레이션(residual bus simulation)을 통해 작업이 수행됩니다.
이후, 다음 측면을 기반으로 잠재적인 취약점을 조사합니다:

- 인터페이스 보안
  - USB 인터페이스
  - 2G/3G/4G 및 5G
  - Wifi
  - Bluetooth
  - MOST/FlexRay/CAN/LIN/Automotive Ethernet
  - 디버그 인터페이스(UART/JTAG/SWD/...)
  - 통합 진단 서비스(UDS, Unified Diagnostic Service)
  - 외장 메모리(예: SD 카드)
- 사용된 입증 절차의 보안
- 적절한 승인 절차
- 암호화 프리미티브(cryptographic primitives)의 적절한 사용
- (보안) 부팅 기능
- 펌웨어 업데이트 프로세스의 보안
- 시스템 강화

식별을 위해 다음과 같은 방법이 사용됩니다:

- 잘못된 매개변수를 통해 처리 오류를 식별하기 위한 인터페이스의 퍼징(Fuzzing)
- 교환된 데이터의 노출 및 수정을 위한 데이터 전송에 대한 중간자 공격(Man-in-the-middle attacks)
- 악성 USB 주변 장치 (및 USB 호스트) 시뮬레이션
- 기록된 통신 재생을 통한 재생 공격
- 정적 분석을 통해 취약점을 조사하기 위한 펌웨어 분석
- 리버스 엔지니어링(예: 메모리 오류 식별)

모든 취약점을 파악하고 난 후 이를 활용합니다. 만약 테스터가 시스템에 대한 더 깊은 액세스 권한을 얻는 데 성공했다면, 얻은 정보는 새로운 정보 수집 단계와 추가적인 잠재적 취약성을 식별하는 데 사용됩니다.

백엔드 시스템 및 클라우드 애플리케이션의 침투 테스트

차량에서 생성된 오류 코드 및 기타 데이터는 인터넷을 통해 직접 또는 자동차 수리점을 통해 간접적으로 백엔드 시스템으로 전송됩니다. 차량의 상호 연결성이 증가함에 따라 백엔드 시스템과의 통신을 위한 더 많은 인터페이스와 옵션이 생성됩니다. 이러한 각 인터페이스는 추가 공격 가능성이 있으므로 독립된 파트너의 신중한 검사가 중요합니다.

침투 테스트를 통해 구현된 보호 조치의 효과를 확인하기 위해 이러한 백엔드 시스템이 직면한 취약성과 잠재적인 위협을 식별할 수 있습니다. OWASP 상위 10개 항목을 고려하여 취약점과 공격자의 가능한 대상에 대해 구조화된 방식으로 시스템을 분석합니다. TÜV 라인란드는 귀사의 자체 데이터 센터 또는 클라우드 제공업체에서 운영하는 애플리케이션과 시스템 모두에 대해 침투 테스트를 수행합니다.

TÜV 라인란드는 귀사의 보호 요구사항에 적합한 테스트 방법을 제공합니다. 표적 웹 API 침투 테스트 또는 모의 사이버 공격(Red Team campaigns)을 통한 취약성 스캔이 필요한 경우 당사와 함께 특정 요구사항에 맞는 테스트를 진행할 수 있습니다.

모바일 앱의 침투 테스트

태블릿, 스마트폰 또는 인포테인먼트 시스템(infotainment system)에서 실행되는 모바일 앱은 사용자 편의성을 증가시키고 안전 관련 기능을 제공합니다. 예를 들어 스마트폰을 자동차 키로 사용할 수 있으며 오늘날, 이러한 기능이 없는 자동차는 상상하기 힘듭니다.

그러나 여기에서도 사이버 보안 및 공격자가 앱에서 악용할 수 있는 취약점은 없는지가 핵심 이슈입니다. 침투 테스트를 통해 TÜV 라인란드 전문가는 다음 질문에 대한 답을 찾을 수 있도록 지원합니다:

- 공격자가 WLAN, 2G/3G/4G 및 5G, Bluetooth 또는 NFC로 통신을 방해할 수 있는 가능성은 무엇입니까?
- 공격자가 통신을 보거나 수정할 수 있습니까?
- 모든 데이터와 비밀번호가 충분히 보호되고 있습니까?
- 공격자가 스마트폰에 설치된 다른 앱을 통해 앱을 손상시킬 수 있습니까?

애플리케이션 환경의 보안 평가

침투 테스트는 ISO/SAE 21434 표준에도 설명되어 있는 SDLC(Secure Development Life Cycle)의 중요한 부분입니다. 그러나 특정 접근 방식으로 인해 부분 테스트만 나타냅니다. 포괄적인 보안 평가를 통해 침투 테스트만으로는 해결할 수 없는 문제를 면밀히 조사할 수 있습니다.
예를 들어 TÜV 라인란드의 전문가는 관리자 및 애플리케이션 관리자와 구조화된 인터뷰를 진행하여 시스템 보안에 영향을 미칠 수 있는 결함을 정확하게 식별합니다. 일반적으로 다음과 같은 주요 내용에 중점을 둡니다:

- 애플리케이션 환경의 네트워크 아키텍처
- 방화벽 구성 및 규칙 관리
- 네트워크 컴포넌트의 구성
- 시스템 및 데이터 전송 중 민감한 데이터의 암호화
- 운영 체제 및 애플리케이션 구성 요소에 대한 원격 관리 액세스
- ID 관리 및 액세스 관리
- 암호화 키 관리
- 운영 체제 설치 및 강화
- 웹 서버 및/또는 애플리케이션 서버의 구성
- 데이터베이스 구성
- 커넥티드 스토리지 시스템의 구성
- 취약점 및 패치 관리
- 바이러스 백신 관리
- 구성 데이터 및 처리된 데이터의 백업 및 복원
- 보안 관련 사건의 기록 및 평가와 사고 관리
- 소프트웨어 개발 지침 및 소프트웨어 배포

전문가가 테스트한 보안

침투 테스트 및 보안 분석이 완료되면 모든 결과가 명확하게 문서화되고 관리 요약이 포함된 TÜV 라인란드의 보고서를 제공합니다.
이는 경영진에게 주요 문제에 대한 명확한 개요를 제공하고 주요 결정에 대해 더 잘 평가할 수 있으며, 기술 전문가는 식별된 취약점에 대한 보다 심층적인 세부 정보를 받을 수 있습니다.

TÜV Rheinland - 자동차 사이버 보안을 위한 전문성 및 인증/기술지원

생산, 통신, 승인 및 자동화 시스템의 사용과 관련된 모든 보안 문제에 대해 TÜV 라인란드의 풍부한 경험을 활용하십시오.

관련된 규범 및 표준에 대한 전문 지식을 바탕으로 귀사의 사이버 보안 관리 시스템(CSMS)에 대한 UNECE 준수 프로세스 및 절차를 자동차 밸류체인에 따라 계획, 정의 및 구현하여 귀사를 지원합니다. 또한 TÜV 라인란드 전문가가 침투 테스트를 수행하고 리스크 평가를 실행할 수 있도록 지원합니다.

TÜV 라인란드는 신뢰할 수 있는 파트너로서 귀사의 자동차 보안을 위한 맞춤 솔루션을 제공합니다.

문의사항이 있으신가요?

지금 TÜV 라인란드 전문가에게 문의하십시오!

TÜV RHEINLAND

TÜV 라인란드는 1872년 설립 이래 150년 이상의 역사를 자랑하는 글로벌 시험·인증 기관으로서 전 세계에서 기술 시스템과 제품을 시험하고, 기술과 비즈니스의 혁신을 지원하며, 다양한 전문 직업 교육을 제공합니다. 독일 쾰른에 본사를 두고 22,000명 이상의 직원이 '사람, 기술, 환경'의 조화를 이념으로 다양한 분야에서 품질과 안전을 위해 활동합니다.
TÜV 라인란드는 2006년부터 유엔 글로벌 컴팩트(Global Compact) 회원으로서 지속가능성과 부패 방지를 위해 힘쓰고 있습니다.

TÜV 라인란드 코리아

TÜV 라인란드 코리아는 1987년, 한국 시장에 진출하여 국내 기업의 든든한 시험·인증 파트너로서 국제 표준과 각 국가 시험 규격에 따라 전기·전자제품, 배터리, 조명, 통신, 압력용기, 산업용 기계류 및 부품, 의료기기, 태양광, 개인보호장비, 완구, 자동차 및 부품, 철도, Functional Safety (기능 안전), 사이버보안, 산업검사, 선적검사, 해외 인증서비스, 경영시스템 인증 등 다양한 산업 분야에서 원스톱 시험·검사·인증·평가 서비스를 제공하고 있습니다.

TÜV 라인란드 코리아 서울 본사에는 무선/IoT, 안전, 에너지 효율 등 다양한 제품 시험을 위한 최신 시험 설비와 시설을 갖추고 있으며, 대구와 창원에도 지사와 시험소를 운영하고 있습니다.
또한, TÜV 라인란드 코리아 아카데미를 개설하여, 시험·인증 교육 및 각 국가 규제에 대한 세미나를 제공하고 있으며, 국내 기업의 글로벌 시장 진출을 위해 함께 노력하고 있습니다.

TÜV 라인란드 코리아
서울특별시 영등포구 문래로28길 25
세미콜론 문래 N타워 2층
Tel: 02-860-9860
Fax: 02-860-9861
E-mail: info@kor.tuv.com

www.tuv.com

사이버 보안 홈페이지

TÜVRheinland®
Precisely Right.