IoT 사이버 보안

TUV 라인란드의 보안 평가 및 침투 시험을 통해
IoT (사물인터넷) 에코시스템 보안 강화

www.tuv.com

TÜVRheinland®
Precisely Right.

TUV 라인란드는 세계 최고의 사이버 보안 서비스 기관 중 하나로 미국, 중국, 인도, 싱가포르, 오만 등 전 세계 곳곳에서 팀을 운영하고 있으며, 매년 전 세계적으로 약 1,000 건의 침투 시험 및 IT 보안 분석을 수행하고 있습니다.

IoT Penetration testing (침투 시험/모의 해킹) 서비스

- IoT 디바이스 및 에코시스템의 침투 테스트 및 소스 코드 분석을 통한 데이타, 브랜드, 수익 및 운영 확보
- 침투 테스트는 보안 취약점과 익스플로잇을 식별할 뿐만 아니라 보안 제어의 효과성과 이러한 제어가 IoT 디바이스 및/또는 에코시스템의 운영 보안을 변경하는 우회되거나 위태롭게 하는 방법을 식별
- 구성요소 테스트의 효율적인 적용 범위와 깊이를 제공하기 위해 자동화 및 수동 테스트의 올바른 조합을 제공하는 테스트 방법론

서비스 이점

- 한 구성요소의 취약성이 다른 구성요소를 어떻게 손상시키는지 완전히 이해하기 위해 IoT 에코시스템과 관련된 모든 구성요소에 대해 고도로 기술적으로 능숙한 범위를 제공하는 강력한 보안 시험 포트폴리오
- 유연한 침투 방법론과 보안 분석을 통해 IoT 디바이스 및 에코시스템 내의 취약점과 익스플로잇을 식별하여 결과를 효율적으로 수정할 수 있도록 실행 가능한 결과를 통해 익스플로잇(exploit) 또는 침투(breach) 리스크 감소
- IoT 디바이스 및 에코시스템의 지속적인 보안 설계 및 구현을 위한 업계 표준 모범 사례 및 다년간의 보안 전문 지식을 기반으로 한 사전 예방적 보안 권장 사항
- 높은 보고 품질 및 전문적인 프로젝트 관리

IoT 에코시스템의 침투 시험 및 IT 보안 분석

IoT 디바이스의 보안 분석

IoT 디바이스는 고객과의 인터페이스이므로 고객 인프라의 보안에 영향을 미칠 수 있습니다. TUV 라인란드는 귀사와 합의한 IoT 디바이스의 대표적인 설정을 수행한 다음 취약성을 조사합니다. 이 시험은 OWASP IoT Top 10 을 기반으로 합니다.

모바일 애플리케이션의 보안 분석

모바일 애플리케이션은 종종 IoT 에코시스템의 필수적인 부분을 형성합니다. 모바일 디바이스에는 IoT 에코시스템 공격을 위한 일종의 발판으로 사용할 수 있는 다소 신뢰할 수 있는 모바일 애플리케이션이 많이 포함되어 있습니다. TUV 라인란드는 OWASP IoT Top 10 을 기반으로 모바일 Android 또는 iOS 애플리케이션의 보안을 평가합니다.

백엔드 보안 분석

백엔드는 모든 것이 관리, 분석 및 전환되는 모든 IoT 에코시스템의 실제 두뇌입니다. 해커가 시스템 및 데이터의 기밀성, 무결성 또는 가용성을 위험하게 할 수 있는 취약점에 대해 외부에서 액세스할 수 있는 인터페이스를 검사합니다.

백엔드 보안 평가

구조화된 인터뷰를 통해 시스템 강화 조치, 취약성 관리 및 패치 관리와 같이 때때로 침투 테스트에서만 추측할 수 있는 측면을 조사합니다.

보고

TUV 라인란드 테스트 보고서는 기술 부서를 위한 세부 정보를 포함하고 경영진이 이해할 수 있도록 탐지된 취약점을 문서화하고 분류합니다. 보고서에서는 해커가 조직에 미칠 수 있는 피해를 설명하고 대응책을 제안합니다.

사이버 보안 서비스에 대한 자세한 내용은 TUV 라인란드 홈페이지를 방문하시거나 TUV 라인란드로 문의하시기 바랍니다.
TUV 라인란드 사이버 보안 서비스 ▶

TÜV 라인란드 코리아
서울시 영등포구 문래로 28 길 25 세미콜론 문래 N 타워 2 층
Tel. +82 2 860 9860 | Fax. +82 2 960 9861 | info@kor.tuv.com
www.tuv.com | blog.naver.com/tuv_korea

TÜVRheinland®
Precisely Right.