시작부터 끝까지 철저한 검증

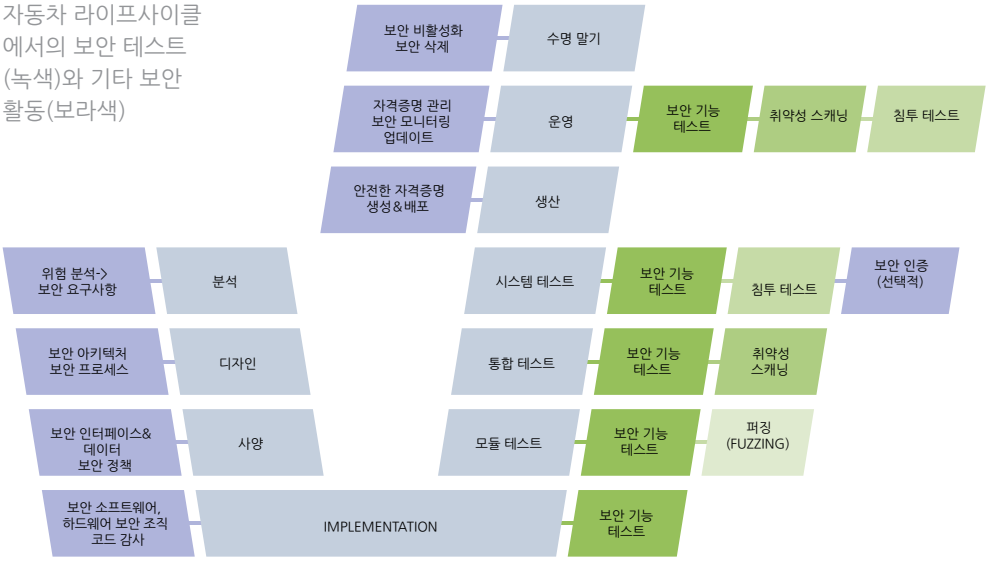
저자

마커스 쾨겔
(Markus Kögel)
박사, 에스크립트 전문 보안 컨설턴트

마르코 울프
(Marko Wolf)
공학박사, 에스크립트 컨설팅 및 엔지니어링 책임자

차량 전체 라이프사이클에 걸친 보안 테스트

효과적인 자동차 사이버 보안을 위해서는 라이프 사이클 전반에 걸친 보안 테스트가 필요합니다. 대부분 물리법칙에 의해 결정되고, 이후에 변화되지 않는 과거의 주행 안전 테스트의 경계조건과는 달리, 보안 테스트를 위한 가정과 경계 조건은 끝없는 공격과 방어가 이루어지며, 변화하는 대상이기 때문입니다. 이런 이유로 자동차가 양산된 이후에도 폐기될 때까지 정기적인 보안 테스트가 필요하며, 이를 통해 새로 개발된 사이버 공격과 이전에 발견되지 않았던 보안상의 허점을 확인하고, 필요한 경우 이에 효과적으로 대응할 수 있습니다.



자동차 라이프사이클에서의 보안 테스트(녹색)와 기타 보안 활동(보라색)

차량 라이프사이클 전반에 걸친 사이버보안 테스트 방법

자동차 사이버 보안 테스트는 본질적으로 보안 기능 테스트, 자동화된 취약성 스캐닝, 퍼징 및 침투 테스트와 같이 위 그림의 확장된 V모델 오른쪽 부분의 네 가지 테스트 방법으로 구분됩니다. 에스크립트는 이 모든 분야에 대해 종합적인 컨설팅과 서비스를 제공합니다.

보안 기능 테스트(functional security testing)는 사용된 보안 메커니즘의 사양이 올바르고 완벽하게 구현되었는지 여부를 확인합니다. 이 단계는 일반적인 기능 테스트와 비슷하지만 보안 기능에 중점을 둔다는 것이 차이점입니다. 보안 기능이 일반적으로 잘 작동하는지 확인하고자 암호화 알고리즘이나 인증 프로토콜의 구현이 테스트됩니다. 또한 런타임 요구사항 또는 메모리 용량 요구사항과의 잠재적인 충돌을 확인할 수 있도록 구현의 성능 및 리소스 소비를 모니터링합니다.

퍼징(fuzzing)은 보안 기능 테스트에 더하여 다양한 예상치 못한, 잘못된 또는 부정확한 입력으로 인한 시스템의 불안정 또는 오동작을 체계적으로 감지하기 위해 사용됩니다.

반면 취약성 스캐닝(vulnerability scanning)은 시스템의 공통 액세스 지점, 보안상의 허점 및 사이버 공격에 대한 취약성을 테스트합니다. 이러한 스캐닝은 일반적으로 테스트 시, 테스트 개체에 관해 알려진 모든 취약성에 대하여 지속적으로 업데이트된 데이터베이스를 사용합니다.

침투 테스트(penetration test)는 일반적으로 새로운 자동차 IT 시스템 출시 대상에만 적용됩니다. 이러한 확장된 보안 테스트는 공격자가 모든 가능한 지식, 기술 및 도구를 활용하여 발견된 모든 취약점을 공격자의 시각에서 악용하려고 시도할 때만 IT 시스템이 충분히 테스트된다는 원칙을 따릅니다.

이타스와 에스크립트는 컨설팅 및 서비스 외에도 다양한 테스트 시스템을 제공합니다(12페이지 참조). 특히 에스크립트는 10년 이상 자동차 보안 애플리케이션에 대한 보안 테스트를 수행했으며, 많은 OEM(Original Equipment Manufacturer)및 공급업체의 파트너입니다. 또한 에스크립트는 이타스의 자회사로서 최첨단 테스트 연구소를 보유하고 있으며 다양한 해킹 방법에 이상적으로 대처할 수 있습니다.