AhnLab

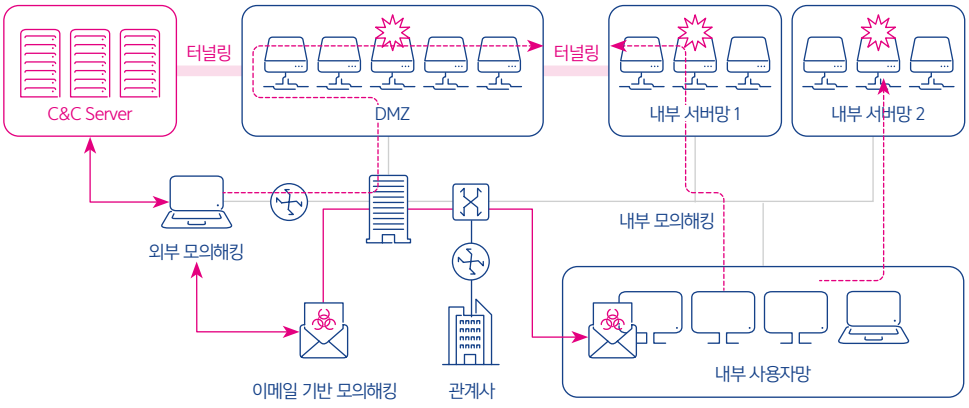
침투테스트 컨설팅

모의해킹을 통한 공격행위 사전 시뮬레이션

공격자의 공격행위 사전 시뮬레이션을 통해 발생할 수 있는 보안위협을 도출하고 정책·조직·자산 관리 측면의 실제적인 대응 방안을 제시합니다.

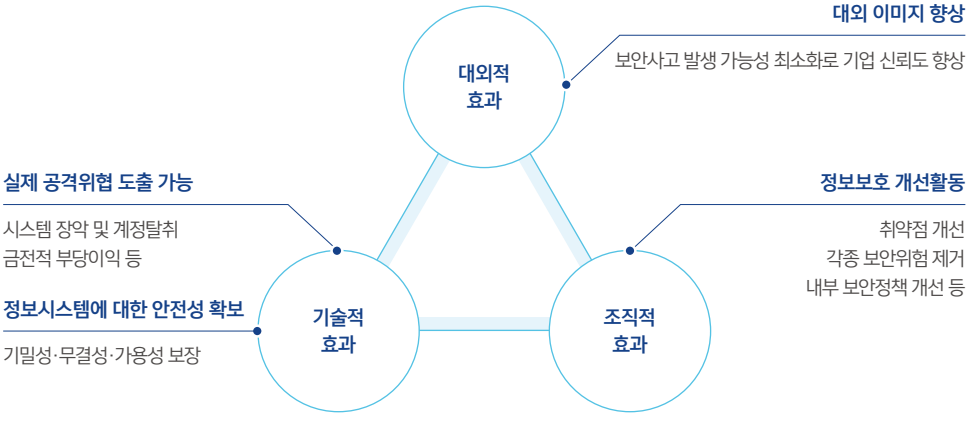
서비스 개요

실제 공격자의 전술, 절차, 공격 기법을 분석하여 공격자와 동일한 방식으로 공격행위를 시뮬레이션하여 보안위협을 사전에 발견하고 대응 방안을 수립합니다.



서비스 필요성

내·외부 위협요소를 최소화할 수 있는 대책을 통해 대고객 서비스와 주요시스템의 안전성 및 신뢰성을 확보할 수 있습니다.



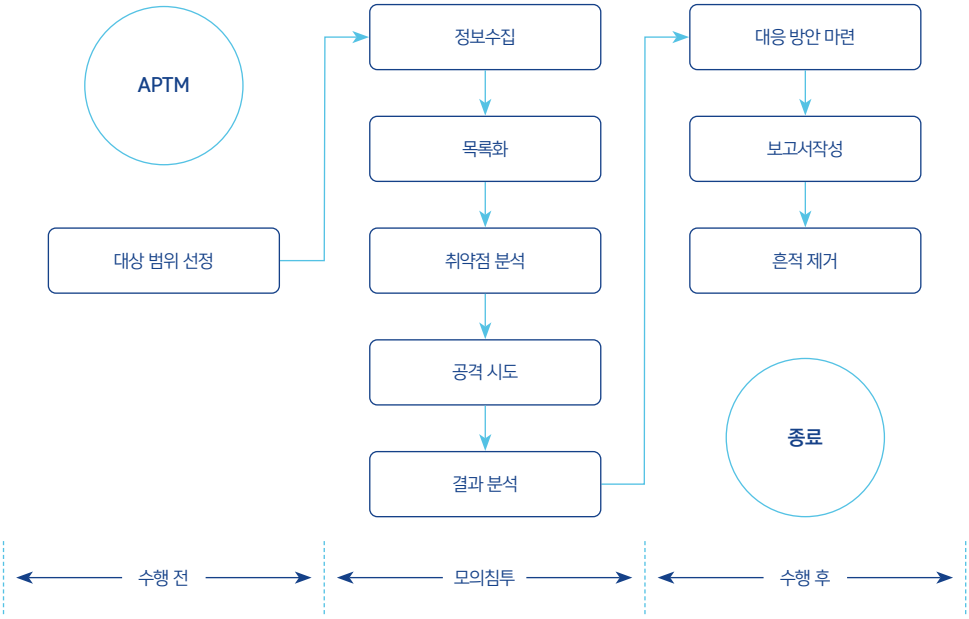
점검항목

공격자의 관점과 목적에 따라 공격 가능성을 점검하여 외부, 내부, 메일 기반 등 다양한 관점의 모의해킹을 통해 위협 발생 가능성을 점검합니다.

외부 모의해킹	· 외부망 서비스에 대한 실제 공격자 입장에서의 접근 및 공격 · 정보유출 및 내부 서버망, 내부 사용자망 침투 가능성 점검
내부 모의해킹	· 악의적인 목적을 가진 내부 사용자로 위장하여 내부망에 접근 및 공격 · 내부 사용자에 의한 정보 유출 가능성 확인
메일기반 모의해킹	· 내부 임직원에게 악성코드가 첨부된 메일을 전송하여 모의 공격 · 메일을 통한 대외비 등의 중요정보 유출 가능성 점검

수행절차

체계적이고 객관적인 진단을 위해 안랩 '모의침투테스트 방법론(APTM)'에 따라 9단계의 단계별 체계화된 절차로 수행합니다.



AhnLab
경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901