삼성SDS

IT취약점 진단

모의해킹을 통한 IT시스템 보안취약점 진단 및 개선 가이드 컨설팅

필요성

IT시스템 보안취약점 진단의 요구 증가

최신 해킹공격 기법에 대한 대응수준 파악
발생 가능한 해킹위협 및 내부 보안사고 사전예방
보안취약점 원인분석을 통한 조치방안 도출

서비스 개념

최신 해킹기법에 대한 대응수준을 파악할 수 있도록 IT 인프라 및 응용 시스템에 대한 침투 테스트를 수행하고 원인 분석을 통한 보안위협 선제 대응체계 제공

주요 특징

삼성 고유의 체크리스트 기반의 IT시스템 모의해킹 서비스

- 16개영역 333개 통제항목으로 구성된 ITSI[1] 기반 IT인프라 취약점 점검
- White Hacker에 의한 모의해킹 및 대응수준 진단
- APT/악성코드 테스트를 통한 보안관제 및 대응절차 진단

자동 및 수동 진단 병행을 통한 효율성 극대화

- 진단경험을 바탕으로 자체 개발한 웹취약점 스캐너 활용
- 시나리오별 정보유출 시도, 로직 추측, 파라미터 변조 등 공격자 입장에서 확인된 취약점을 이용하여 침투 테스트 실행

보안 가이드 제공

- 진단 결과에 따른 조치가 가능하도록 보안가이드 제공
- 운영자, 보안담당자 대상 보안교육 제공

[1] IT Security Index: 각종 보안법률, 국내외 보안기관 보안공지 취약점 등을 반영한 보안 취약점 진단 점검 항목 Checklist

주요 서비스

모의해킹 대상 시스템 분석

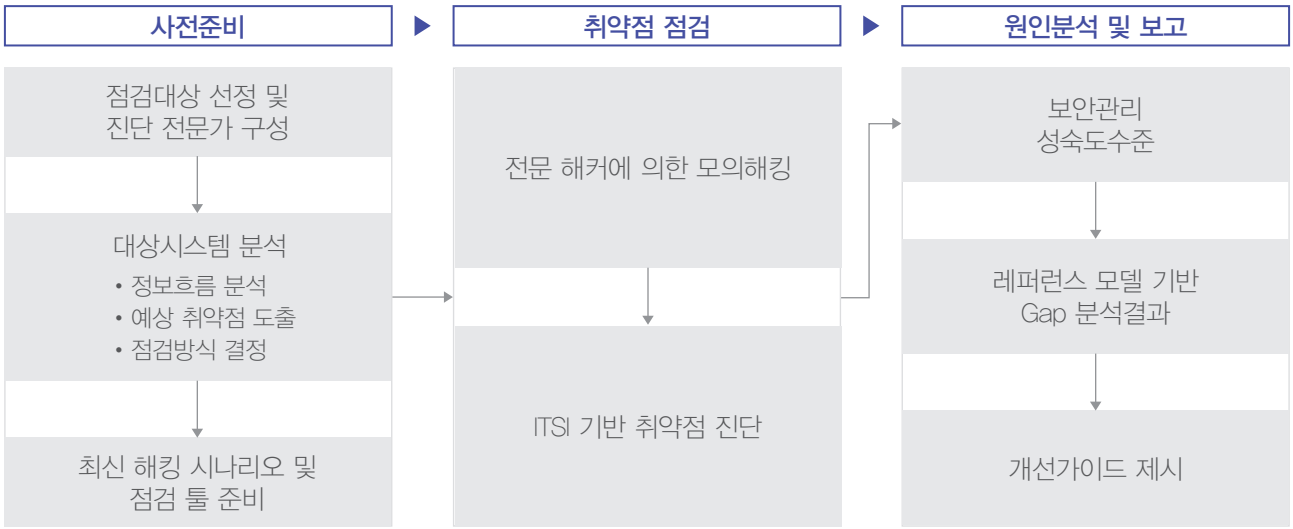
정보흐름 분석 및 예상 취약점 도출
취약점 점검대상 시스템 정의

모의해킹 및 취약점 점검

시스템/서비스 대상으로 해커와 동일한 입장에서 모의해킹
악성코드/APT공격 형태의 자료유출 및 내부접근 가능성 점검
취약점 점검 프로그램을 통한 취약점 확인 및 추가 모의해킹

개선과제 수립

취약점 및 원인분석에 대한 진단결과 보고서
진단영역별 주요원인에 대한 조치방안 제시
우선순위에 따른 Quick Fix/단기/장기 개선과제 제시



기대효과

다양한 공격기법을 통한 정보유출 방지

발견된 취약점을 이용한 위협 시나리오 인지
기업 중요정보 및 고객 개인정보 유출을 위한 최신 공격 대응

개선가이드에 따른 IT시스템 보안 강화

도출된 개선사항을 바탕으로 보안강화 과제계획 수립 및
보안관리 체계 고도화