삼성SDS

홈페이지 관제서비스

웹해킹[1] 공격 행위를 탐지 및 조치하고자 재발방지를 위한 예방활동을 제공하는 서비스

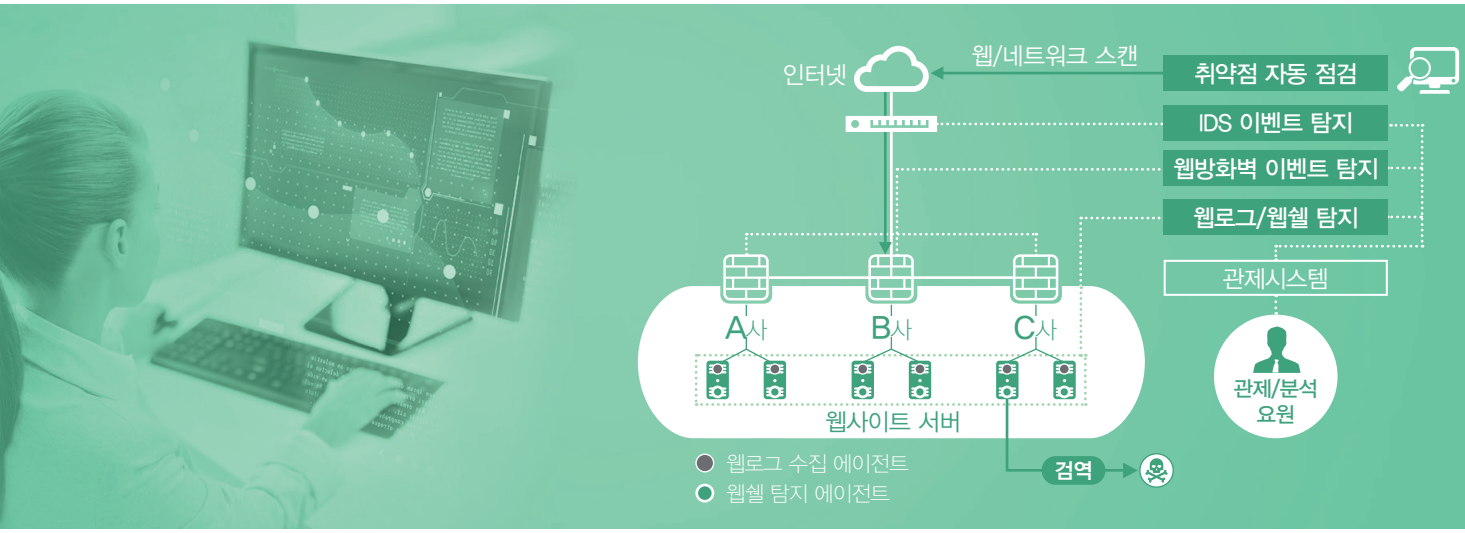
필요성

웹해킹에 대비하기 위한 「예방 – 탐지 – 조치」의 통합서비스 필요

예방: 최신 취약점 정보를 활용한 웹/네트워크 취약점 정기 진단
탐지: IDS, 웹방화벽, 웹쉘 및 웹로그 에이전트를 통한 통합분석
조치: 해킹탐지시 관제/분석요원의 정밀분석 및 잔존 취약점 점검

서비스 개념

사이버 사업장을 대상으로 하는 홈페이지 위변조, 정보탈취 등과 같은 외부 위협에 사전예방–탐지 및 대응–사후조치를 지원하여 홈페이지를 안전하게 보호하는 서비스



주요 특징

최신 웹해킹 공격에 대한 상시 자동 탐지 제공

- 홈페이지 해킹시도, 홈페이지 위변조, 웹소스내 악성URL 삽입 등 탐지
- 「수집 – 분석 – 룰셋개발 – 관제적용」 프로세스에 의한 Zero–day 공격 등 신종 웹 위협 탐지
- 공격 위험도에 따른 유형별 대응 조치

정기적인 취약점 자동점검을 통한 해킹사고 예방

- 네트워크 취약점 자동 점검 (부적절한 설정 및 OS 취약점 탐지 등)
- 웹 취약점 자동 점검 (입력값 검증 부재 등 웹 애플리케이션 취약점 탐지 등)

[1] 웹해킹: 웹사이트의 취약점을 공격하여 웹페이지를 통해 권한이 없는 시스템에 접근하거나 데이터 유출 및 파괴와 같은 행위 수행

주요 서비스

웹로그 분석

외부에서 고객사 웹사이트로 접속시, 웹서버 내부에 기록된 웹로그를 실시간 수집 및 분석

Google 정보유출 탐지

구글 검색 기능을 활용하여 설계도, 계약서, 개인정보 등 고객사 중요 정보의 유출을 탐지

웹쉘 탐지

해킹 공격에 의해 웹 서버 홈디렉토리 內 악성 웹쉘 업로드 時 실시간 탐지

상용웹쉘[2] 및 악의적으로 활용될 수 있는 구문이 포함된 파일 탐지 및 검역

침입 웹사이트 취약점 정밀 분석

최근 발생한 공격 대상으로 분석전문가의 상세수동 점검 및 조치 가이드 제공

웹트래픽 분석

외부에서 고객사 웹사이트로 접속시, 발생하는 웹트래픽을 웹방화벽 및 IDS를 통해 실시간 수집 및 분석

OWASP Top 10[1] 기준 공격패턴 탐지

웹사이트 화면 위변조 탐지

위 · 변조 정보를 수집 후 고객사 웹사이트 여부를 확인하고 원인 분석

저장된 웹사이트 화면 이미지를 비교 분석하여 위변조 탐지

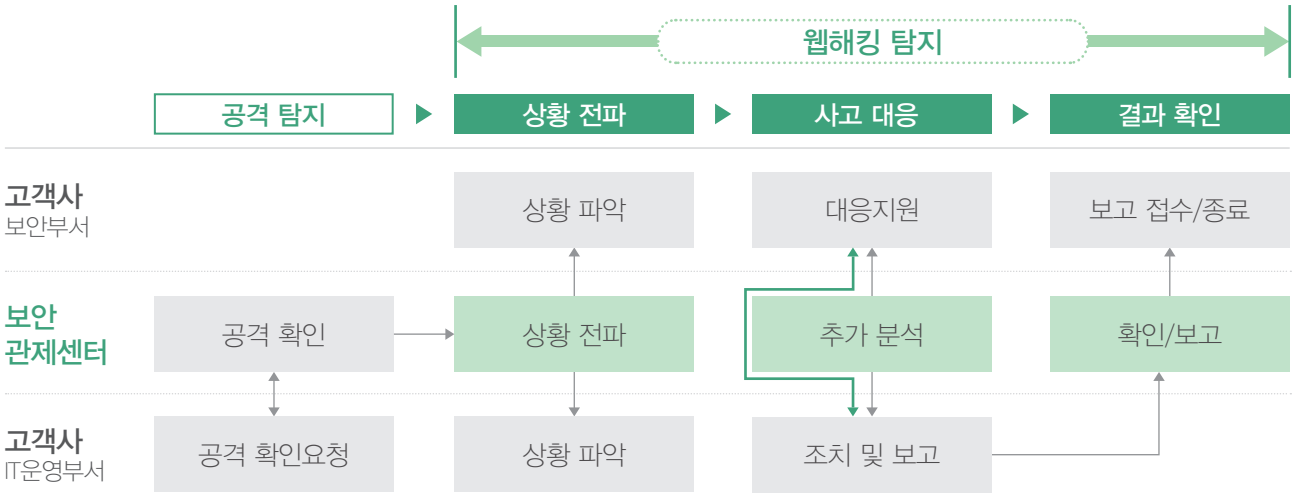
화면 비교를 통해 위변조 탐지시 HTML 웹소스 분석을 통해 소스 변조 및 악성URL 삽입 여부 탐지

[1] OWASP Top 10: 오픈소스 웹 애플리케이션 보안 프로젝트로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하여 발표한 10대 웹 애플리케이션의 취약점

[2] 상용웹쉘: 해커에 의해 제작된 악성 파일로, 블랙마켓에서 거래되거나 Google 검색을 통해 유포되는 널리 알려진 웹쉘

서비스 프로세스

웹해킹 공격 탐지시 보안관제센터와 고객사 유관부서 간 정형화된 프로세스를 통해 단계별로 신속하고 정확하게 상황 전파 및 대응 실시



SAMSUNG SDS