삼성SDS

악성코드 관제서비스

인터넷을 통해 내부로 유입되는 악성코드를 탐지하여 정보유출을 방지하는 서비스

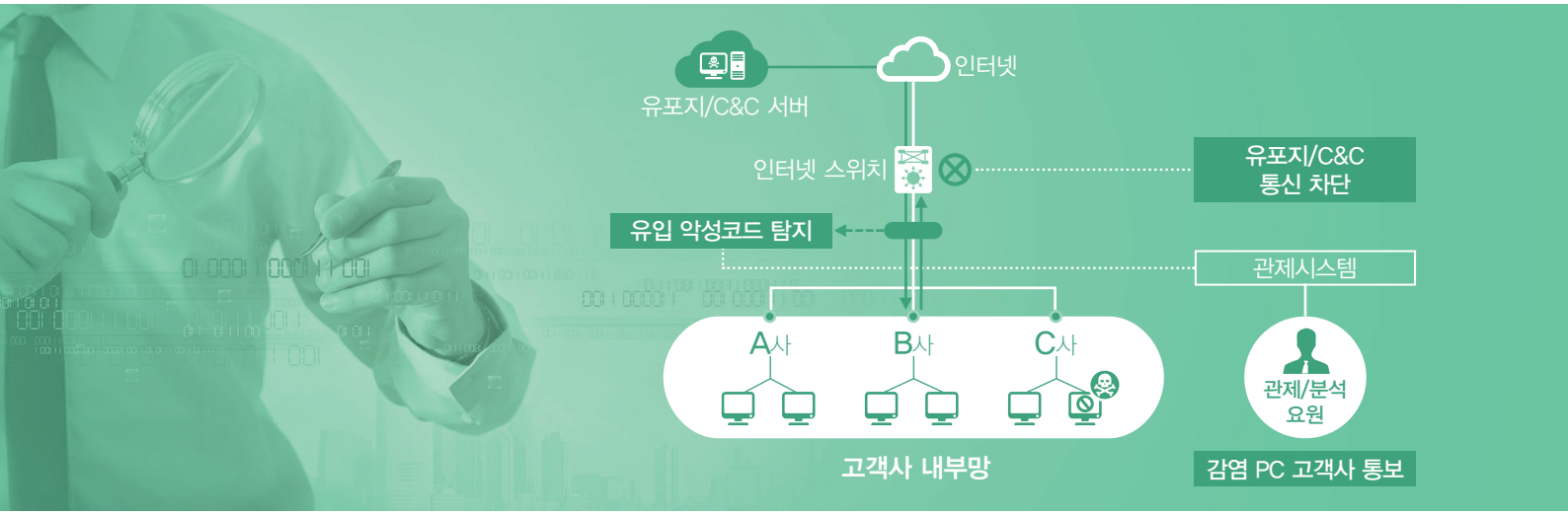
필요성

악성코드 감염 탐지 및 대응을 위한 「탐지 – 차단 – 조치」의 서비스 필요

탐지: 외부에서 내부PC로 유입되는 악성코드 및 유포지 탐지
차단: 악성코드 유포지 차단 및 C&C 접속시도 차단
조치: 감염PC에 대한 경보 및 조치 가이드 제공 서비스

서비스 개념

인터넷을 통해 내부PC로 유입되는 악성코드를 탐지하여 유포지 및 C&C서버[1]와의 통신을 차단하고 정보 유출을 방지하는 보안관제 서비스



주요 특징

하이브리드 기반 분석 기법

- 악성코드 정적분석과 동적분석 결합
- 행위간 연관분석 및 평판분석
- 취약점을 이용한 문서형 악성코드 탐지

실시간 위협 모니터링

- 모든 탐지 및 분석 대상의 악성여부에 대한 명확한 가시성 제공
- 관심 이벤트(파일, IP, URL)에 대한 집중 모니터링

악성코드 발생 현황 분석 정보 제공

- 악성코드 탐지 추이, 주요 유포지/C&C서버 탐지 현황 분석 정보

[1] C&C 서버 (Command and Control Server): 악성코드가 감염된 PC에 명령을 내리고 데이터를 수신하는데 사용되는 서버

주요 서비스

알려진 악성코드뿐만 아니라 악성으로 의심되는 파일까지 검사/탐지

1단계: 알려진 악성코드 유입 탐지
시그니처 기반 패턴 매칭 방식
2단계: 변종/신종 악성코드 탐지
파일 평판 분석 및 행위 분석 방식

악성코드 유포지 탐지 및 차단

악성코드가 업로드된 사이트 접속을 통해 다운로드 URL/IP 탐지
악성코드 감염경로 분석 및 검증 후 URL/IP 실시간 차단 적용

C&C서버 통신 차단

다수 소스에서 발표된 신종 악성코드 정보 및 자체 수집된 C&C서버 정보 기반으로 악성 URL/IP 차단 적용

탐지된 악성코드에 대한 위험도 분류 및 통보

위험도 분석 후 긴급건/일반건으로 고객사에 실시간 통보

백신엔진 업데이트

신종 악성코드 탐지시 백신업체에 의뢰하여 업데이트 조치
진단명 및 신규 백신 버전 정보 제공

서비스 프로세스

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