어플라이언스

첨부파일 악성코드 대응

새니톡스

랜섬웨어 및 문서형 악성코드를 원천 차단하는
CDR 기술 기반의 첨부파일 악성코드 대응 솔루션

공격 방식의 변화, 차세대 보안으로 CDR이 주목받는 이유

사이버 위협은 사회공학적 기법을 활용한 문서 파일 중심으로 공격 방식이 고도화되고 있습니다. 이메일 내 문서 위장 공격 비중은 70%를 넘어섰고 2022년 알려지지 않는 위협은 전년 대비 46% 증가했습니다. 우회 공격 및 알려지지 않은 위협의 증가로 인해 기존 보안의 한계가 드러나면서 실행 가능한 위협 요소를 원천 제거하는 CDR 기술이 차세대 보안으로 주목받고 있습니다.
새니톡스(SaniTOX)는 자체 개발한 CDR 엔진으로 비정상 포맷을 사전 탐지, 제거하여 문서형 악성코드 및 알려지지 않은 위협을 사전 예방합니다.

*출처 : 금융보안원 사이버위협 인텔리전스 보고서 2019
Trend Micro, Email Threat Landscape Report 2023

제로 트러스트 보안 실현
잠재 위협 요소 원천 제거로 콘텐츠 무결성 보장

자체 개발한 고성능 CDR 엔진
정합성 및 처리 속도 보장 및 신속한 트러블 슈팅

단일 서버로 메일, 웹, 파일 서버 다중 연동
eMail G/W, 웹 API, NFS, SMB, SFTP 등 지원

인증된 CDR 기술력 보유
우수 정보보호 기술 및 가트너 CDR 기술 벤더 선정

새니톡스_제로 트러스트 관점의 강력한 무해화(CDR, Content Disarm & Reconstruction)

새니톡스(SaniTOX)는 문서의 구조 분석을 통해 악성코드로 활용 가능한 액티브 콘텐츠 영역만을 탐지, 제거 후 안전한 파일로 재조합하는 CDR 기술 기반의 첨부파일 악성코드 대응 솔루션입니다. 악성 여부의 판별 없이 실행 요소를 제거하는 방식으로 알려지지 않은 위협에 효과적인 제로 트러스트 관점의 보안을 실현합니다.

주요 기능

콘텐츠 무해화 처리

· 실행 가능한 액티브 콘텐츠(Macro, Script 등) 제거
· MS Office, PDF, HWP, ZIP, Image 등 다양한 포맷 지원
· 원본 파일 형식 유지 및 다운로드 및 편집 가능

파일 전송 구간 연동 및 확장

· Mail G/W, API, SFTP, SMB, NFS 등 다양한 시스템 연동
· MTA 지원 및 릴레이 연결 지원
· 연계 시스템 개별 정책 설정

무해화 결과 상세 리포트

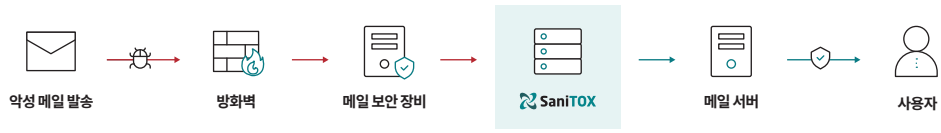
· 파일 무해화 후 레벨별 상세 정보 제공
· 액티브 콘텐츠 추출 및 5단계 위험도 분석
· 감사 로그 및 유형별 통계 분석 제공

연관 분석

· 악성 분석 결과 가시화 그래프 제공
· 연관 분석 통해 제로데이 공격 무해화 이력 제공
· 무해화 후 백신 통한 사후 차단 여부 판별

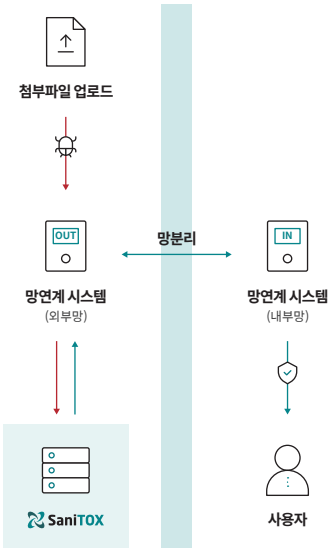
활용 분야

이메일 연동

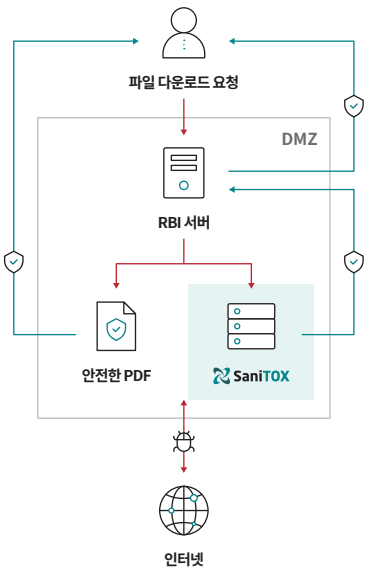


웹서버(게시판) 연동

망연계 연동



웹격리(RBI) 연동



분야별
활용 사례
영상 보기 >

도입 기업

경찰청 · 국방통합데이터센터 · 충청북도교육청 · 보건복지부 · 한국남부발전㈜ · 국회도서관
광주은행 · NPS 국민연금 · ENLIPLE · 한화생명 · 전북은행 · E-LAND
의정부시 · 인천광역시 · 국립중앙의료원 · Homeplus · KERIS · KAC 한국공항공사

지란지교시큐리티
경기도 성남시 수정구 금토로80번길 37 인피니티타워 W동 | Tel : 031-625-7664 | E-mail : sanitox@jiran.com | www.sanitox.co.kr