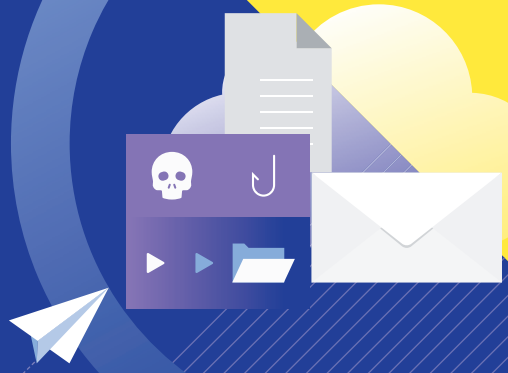
디지털 시대를 위한 사이버 방역 솔루션!

MARS CDR Cloud

SECULETTER



제로트러스트 기반 문서 보안 전문성과 자체 개발 CDR 기술, 위협 분석 기술의 결합

개요

급증하는 해킹 메일과 악성 첨부파일 위협의 증가로 보다 강력한 보안을 제공하고자 ZeroTrust 기반의 문서 보안 전문 기술력을 통해 자체 개발한 콘텐츠 무해화 및 재구성(CDR) 기술과 위협 분석 기술을 결합한 클라우드 보안 서비스입니다.

공격에 악용되는 악성 문서에서 매크로, 자바스크립트 등 악의적인 행위를 유발하는 보안 위협 요소를 신속하고 정확하게 제거한 후 콘텐츠를 재조합하여 안전한 문서로 제공합니다.

안전한 문서 제공

공격에 이용될 수 있는 액티브 콘텐츠를 제거해 안전한 문서 제공

문서 보안 전문 기술

문서 보안 전문 기술력으로 무해화 진행 후 원본과 동일한 문서 제공

신속·정확한 위협 진단

클라우드 기반 위협 분석 기술(평판 분석)로 신속하고 정확하게 위협 판별

(Content Disarm and Reconstruction) * 문서 내 악성 URL 및 실행코드가 포함된 액티브 컨텐츠(Macro, JS 등) 제거

악성코드 분석기술

SecuLetter CDR(Content Disarm & Reconstruction) Cloud는 기업 내부로 유입되는 악성 문서 파일의 위협 요소 (예: Hyperlink, Visual Basic Macro, Java Script, Dynamic Data Exchange 등), 즉 공격의 무기로 사용될 수 있는 알려지지 않은 위협 요소를 신속하고 정확하게 제거한 후 안전한 문서 파일로 제공하는 서비스입니다.

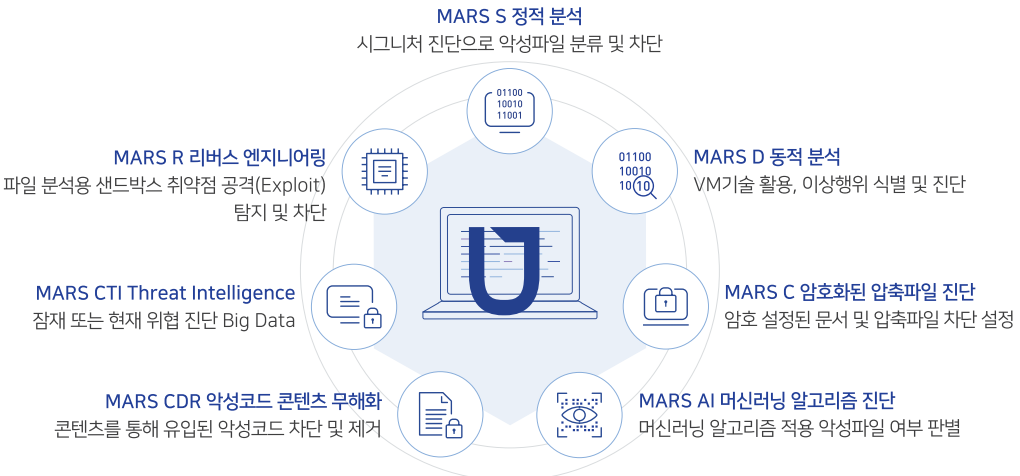
또한 평판 분석 기반 위협 인텔리전스(Threat Intelligence)를 통해 유입되는 최신 보안 위협정보를 빠르게 수집하여 의심스러운 악성 파일을 판별하고 랜섬웨어, 정보유출 사고, 악성코드 감염 등으로부터 고객의 정보와 자산을 안전하게 보호합니다.

비실행형 문서파일 분석 전문성과 혁신적인 위협 인텔리전스 보안 기술을 결합하여, 독자적으로 개발한 CDR 기술을 통해 잠재적인 악성 콘텐츠 위협 요소를 안전하게 제거하기 때문에 원본 문서의 손상을 최소화하여 강력한 CDR을 경험하실 수 있습니다.

MARS PLATFORM

차세대 위협 탐지 대응 플랫폼

위협 분석 기술	무해화 기술	디버거 분석 기술
콘텐츠 식별 및 구조분석	콘텐츠 무해화 및 재구성	콘텐츠 취약점 탐지 및 차단



활용 사례

이메일 등 외부에서 들어오는 콘텐츠 파일을 분석한 후 실행 파일 등 불필요한 혹은 위험한 요소를 제거하고 문자나 그림 등 콘텐츠만을 원본처럼 구성하기 때문에 한글이나 워드 파일을 이용한 랜섬웨어, 스파이웨어 등의 공격으로부터 사용자를 보호할 수 있다.

- 이메일 첨부된 문서 또는 웹 다운로드 문서 무해화
- 메신저로 주고받는 문서에 대한 무해화
- 클라우드 저장 공간에 보관된 문서 무해화
- 망연계 시스템으로 주고받는 문서 무해화
- 문서 보관 및 백업 시스템의 문서 무해화
- 기타 파일 이동 구간에 문서 무해화

악성코드 제거 과정

MARS SLCDR(콘텐츠 무해화 솔루션): 기존 CDR 기술과 자동화된 리버스 엔지니어링 기반 악성코드 분석 기술을 결합해 독자적으로 개발한 기술입니다. 문서에서 포함된 URL이나 매크로, 자바스크립트, Shellcode 등의 액티브 콘텐츠를 식별하여 실행 가능한 요소를 제거한 후 깨끗한 새 문서로 재조립함으로써 공격 가능성을 차단합니다.

MARS SLCDR 솔루션을 적용한 악성코드 제거 과정

신종 악성코드가 포함된 APT 이메일, USB

파일 스캔 (구조 분석)

액티브 콘텐츠 분석 매크로, 자바스크립트 이용 악성 파일

액티브 콘텐츠 제거 액티브 컨텐츠 분석 제거

파일 재조합 최소한의 문서 변경을 통해 원본 손상 최소화

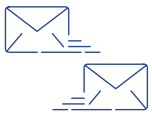
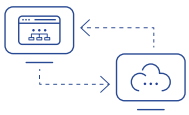
어셈블리 레벨분석 기술 (자동화된 리버스 엔지니어링) 문서기반 취약점 공격 탐지 및 사전 차단으로 제로트러스트 구현

재조합된 안전한 파일

콘텐츠 무해화 및 재조합 기술 매크로나 자바스크립트를 이용한 악성행위가 포함된 이메일 첨부문서는 악성행위 가능성이 높은 것만 선별 제거

적용 구간

정부 및 금융기관 정보보호 지침을 준수하여 이메일 구간 망분리 망연계 구간 웹게시판, 문서중앙화, 컨텐츠 무해화에 적용

온프레미스, 클라우드 이메일 서버		망연계, 문서중앙화, 웹게시판 서버	
			
이메일 구간	망연계 구간	문서중앙화 구간	웹 공용 게시판 구간

SECULETTER
www.seculetter.com

대표 문의
Tel: 031-608-8866, Fax: 031-608-8810

솔루션 문의
Tel: 1670-8780
E-mail: sales@seculetter.com

기술 지원
Tel: 031-608-8880
E-mail: se@seculetter.com