소프트캠프㈜ | Security 365

파일무해화(CDR) 솔루션
SHIELDEX 제안서

SOFTCAMP

Contents

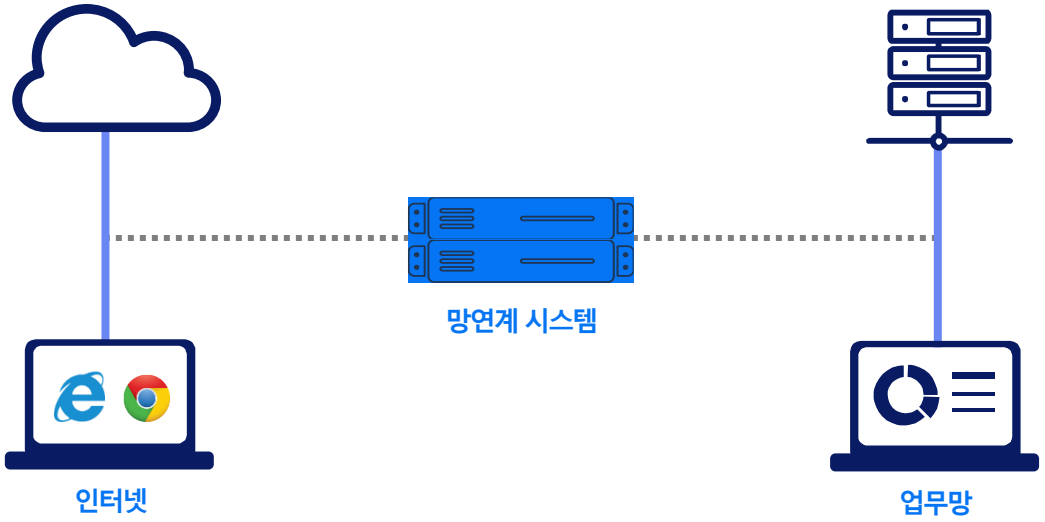
CHAPTER 01

CDR 제품 필요성

CDR이 왜 필요한가?

01. CDR 제안배경

침해대응 관점 : 내부로 유입되는 악성코드 및 비정상 행위 탐지!



구분	외부망	망연계	내부망
인터넷 접속 (파일 반입)	IDS, IPS, Proxy, SSL Inspection, Sandbox	AV, Sandbox,	AV, EDR
이메일 접속 (본문, 첨부)	Anti-Spam, Sandbox	AV	본문 이미지 전환

망 분리 환경 구축 이후 보안의 강도는 매우 강해졌으나 업무의 **불편함**과 **다양한 침해 경로**

- 이메일
- 망간자료전송
- USB, CD
- 예외자 처리
- 공급망 공격

01. CDR 제안배경

핵심 솔루션 들은 모두 Detect & Response를 지향합니다.

탐지중심의 솔루션

Sandbox, EDR, 머신러닝, 포렌직 등

탐지솔루션의 효용성

얼마나 빨리 많이 탐지하는가?
얼마나 정교하게 오탐 없이 탐지하는가?

침해발견에 드는 노력

각 솔루션별 운영을 위한 전문가 필요 및 Intelligence, IOC등에 대한 정기적인 Update 필수

그럼에도 불구하고...

47%의 악성코드는 외부기관에 의해 통보, 침해 이후 발견까지 평균 146일 소요

※ 출처 : 2017 Mandiant, M-Trends

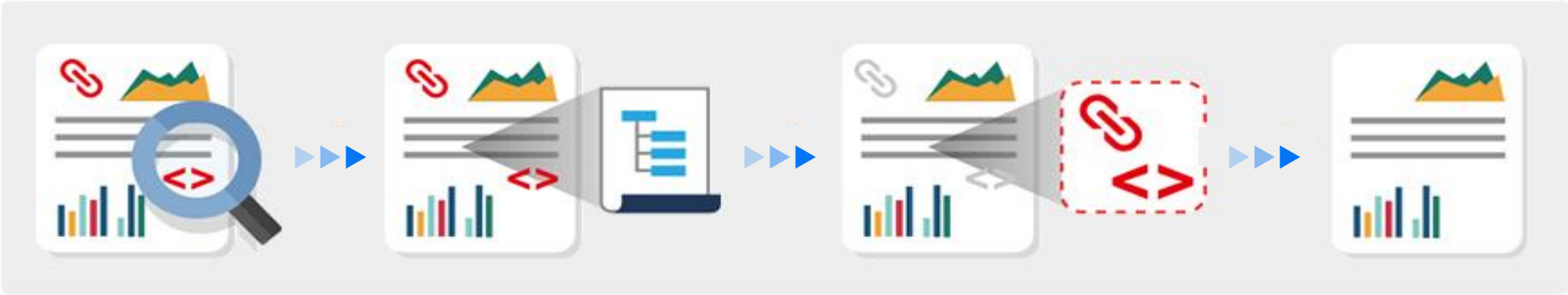
01. CDR 제안배경

CDR은 탐지에 의존하지 않고 문서파일 기반의 악성코드에 대처하는 새로운 기술

Content Disarm & Reconstruction(CDR) is a computer security technology for removing malicious code from files. Unlike malware analysis, CDR technology does not determine or detect malware's functionality but removes all file components that are not approved within the system's definitions and policies. It is used to prevent cyber security threats from entering a corporate network perimeter.
Channels that CDR can be used to protect include E-mail and website traffic.

- Wikipedia

문서파일 내 잠재적 위협요소를 제거(Disarm)후,
안전한 콘텐츠만 추출하여 문서를 재조합(Reconstruction)하는 기술



Format Verification | **Structure Analysis** | **Component Extraction** | **Reconstruction Verification**

01. CDR 제안배경

우리나라도 제도 마련이 이뤄져야 합니다.

일본	총무성	• 2015년 지방자치단체의 정보보안 강화 일환 • 망분리와 무해화 정책 규정, 무해화(CDR) 기술 도입 의무화
	문부과학성	• 2017년 교육 정보보안 정책 지침 • 무해화 기술 도입 의무화
미국	국토안보부	• 2015년 RSA 컨퍼런스에서 'Content Filtering' 프로젝트 성과 발표 • 2017년 'Content Filtering' 프로젝트에 관련된 CDR 도입 지침 발표
호주	사이버 보안당국	• 2017년 정보보안 매뉴얼 발표 CDR 기술 도입 의무화
이스라엘	사이버당국	• 사이버 방어 방법론에서 분리된 네트워크 간의 파일 교환 구간에 'Content Filtering' 의무화

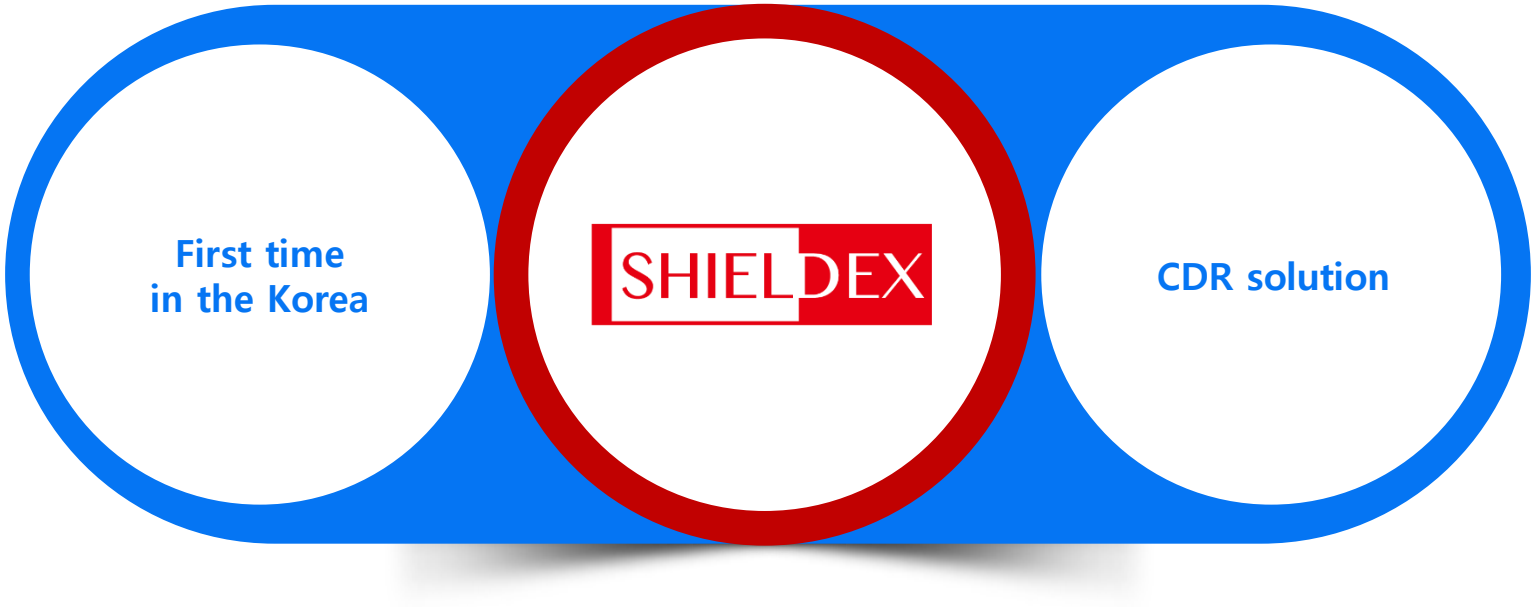
CHAPTER 02

CDR 제품소개

SHIELDEX의 기술적 차별성은 무엇인가?

02. CDR 제품 소개

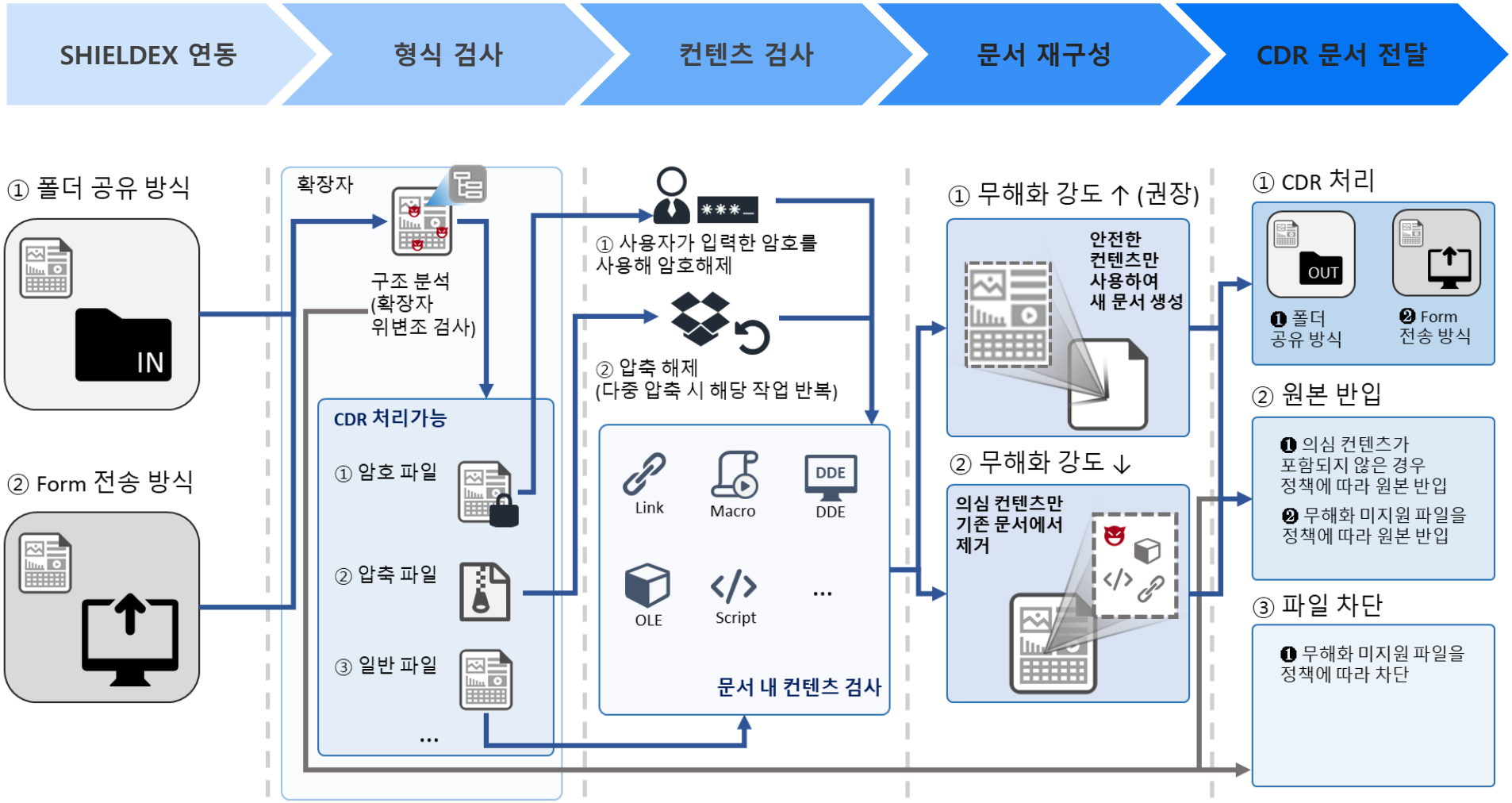
문서보안 20년 노하우를 가지고 만든 **소프트캠프의 CDR 솔루션**



- 2013년 **국내 최초 CDR 제품** 출시
- 국내 사용되는 **모든 문서 종류** 지원
- 망연계, E-mail, 공유파일 등 **다양한 배치** 지원
- CDR 기술 관련 6개 특허 및 **GS 인증** 획득
- 국방, 공공, 금융 등 권역별 **레퍼런스** 보유
- **일본** 등 세계로 뻗어가는 한국의 CDR 기술

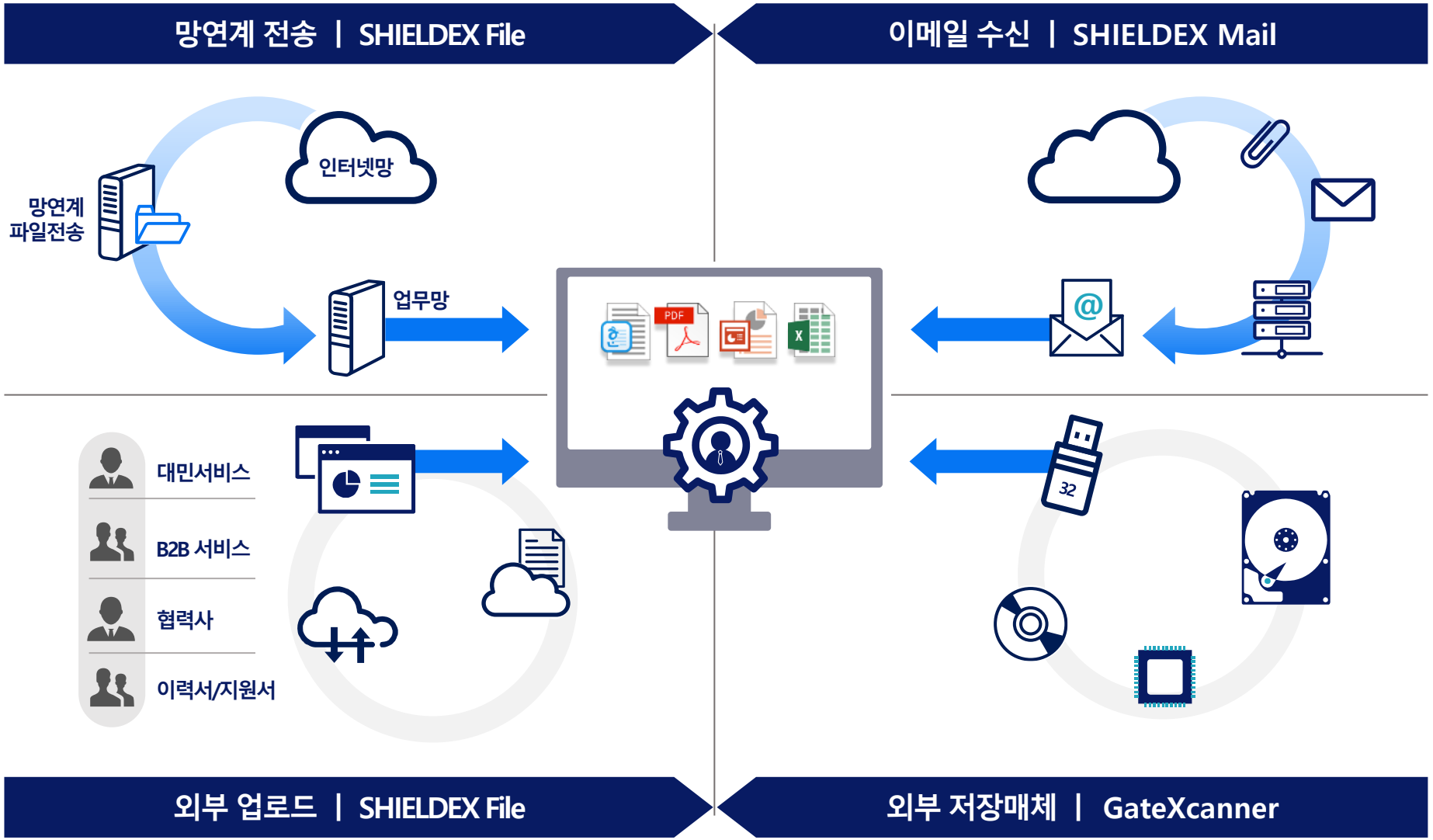
02. CDR 제품 소개

CDR 처리의 기술적인 상세 프로세스



02. CDR 제품 소개

SHIELDEX의 제품 Line up

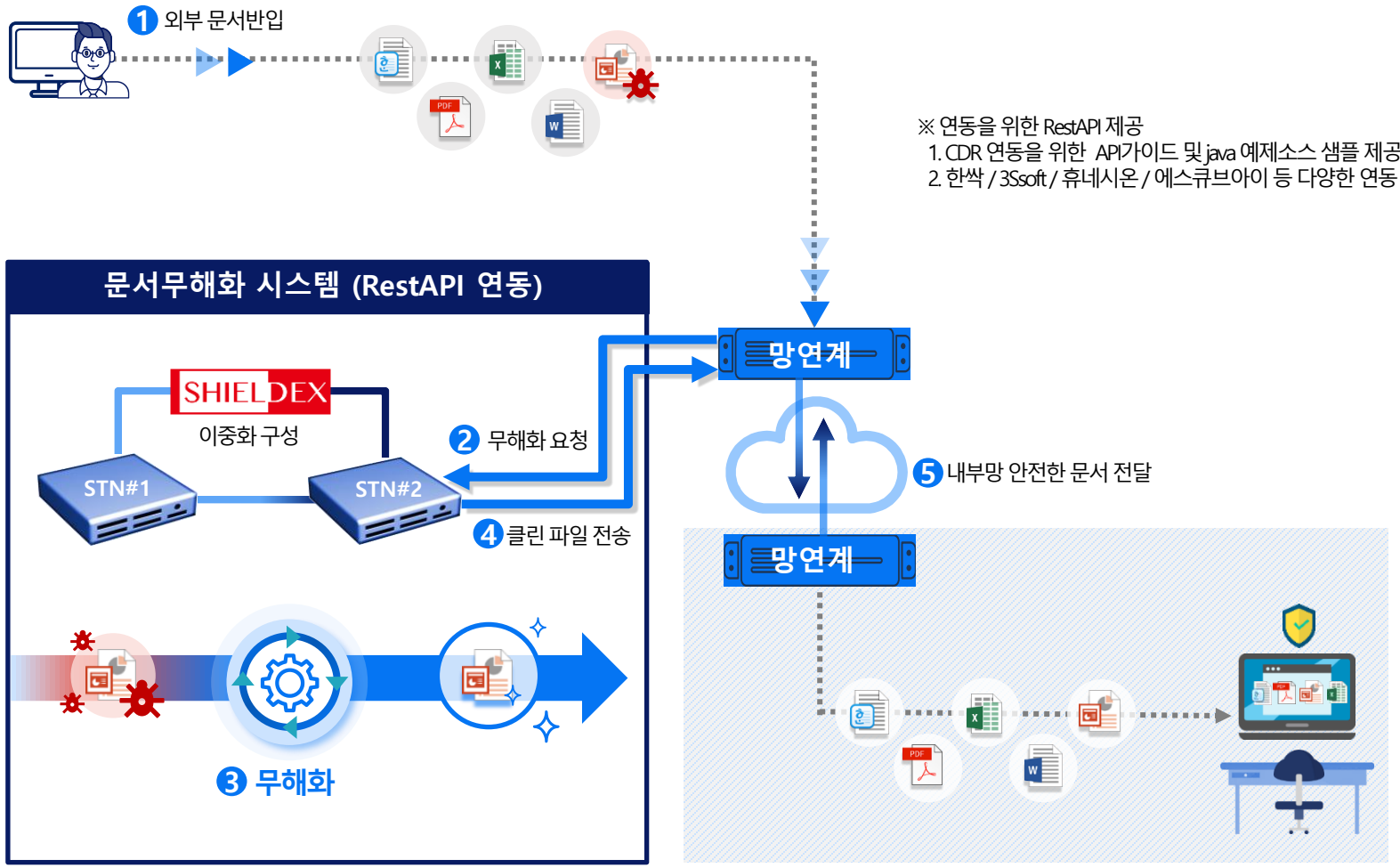


CHAPTER 03

SHIELDEX 제품별 구성도

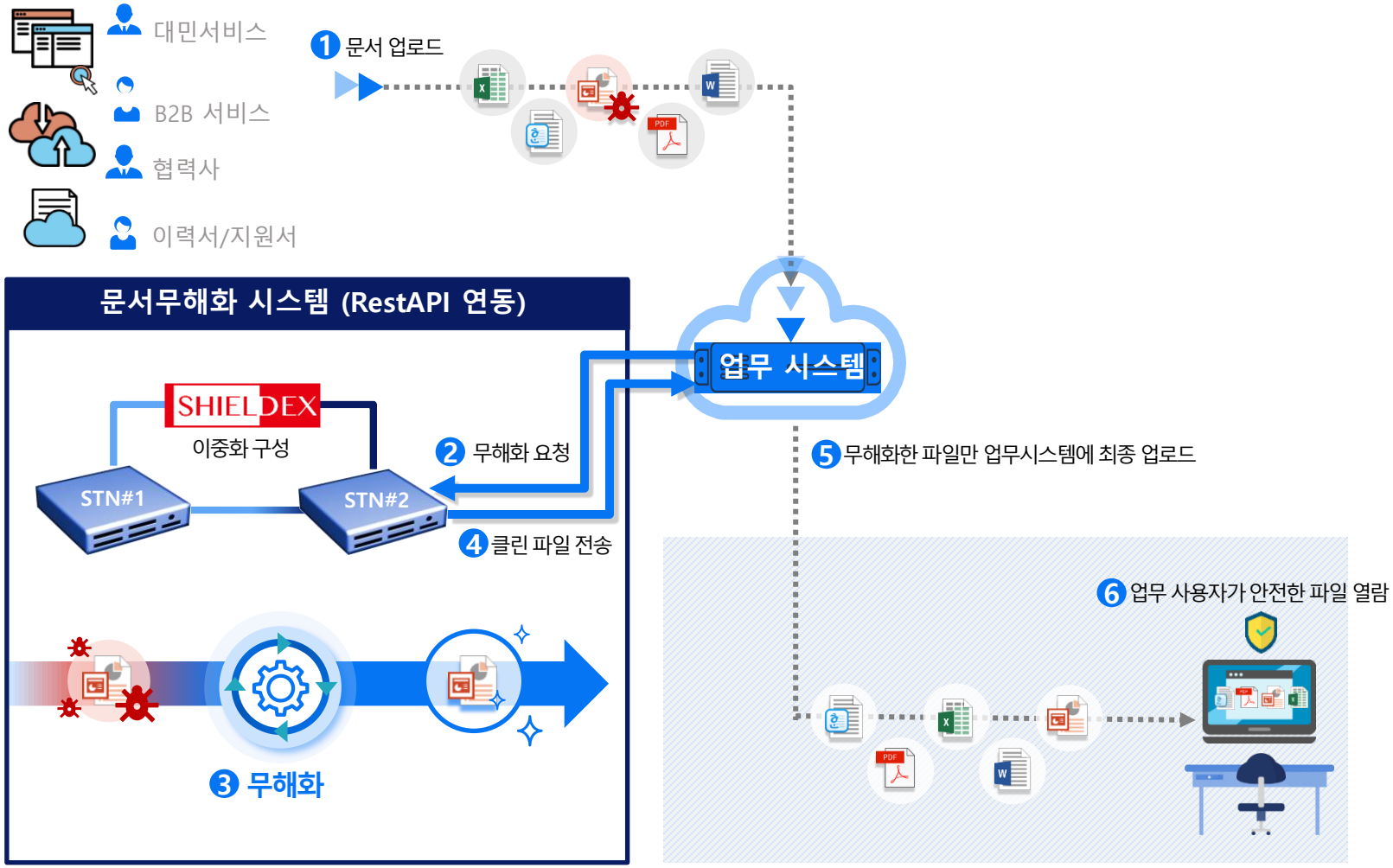
3. SHIELDEX 제품별 구성도

망연계 구간의 구성도



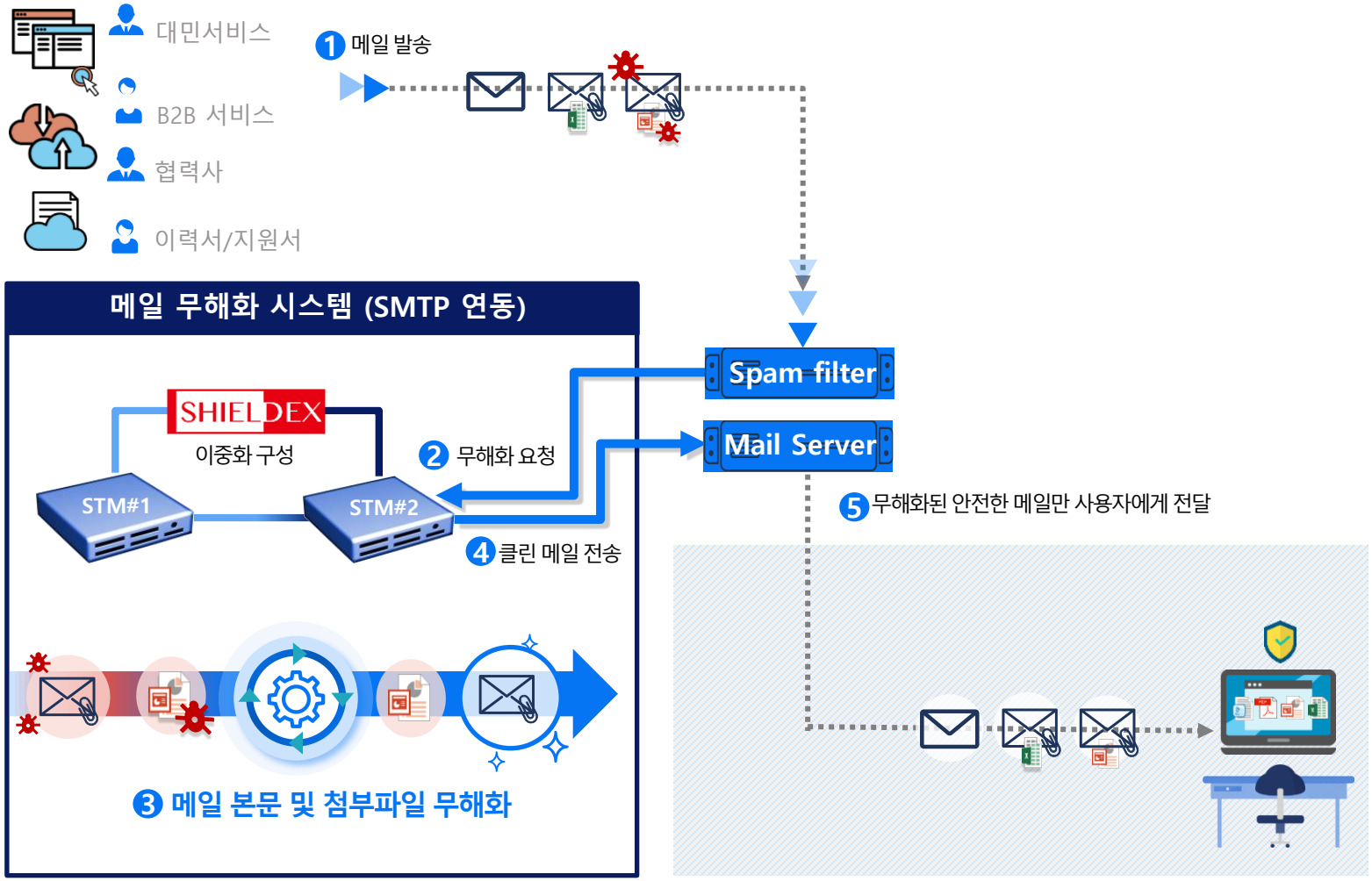
3. SHIELDEX 제품별 구성도

게시판 구간의 구성도



3. SHIELDEX 제품별 구성도

이메일 구간의 구성도



CHAPTER 04

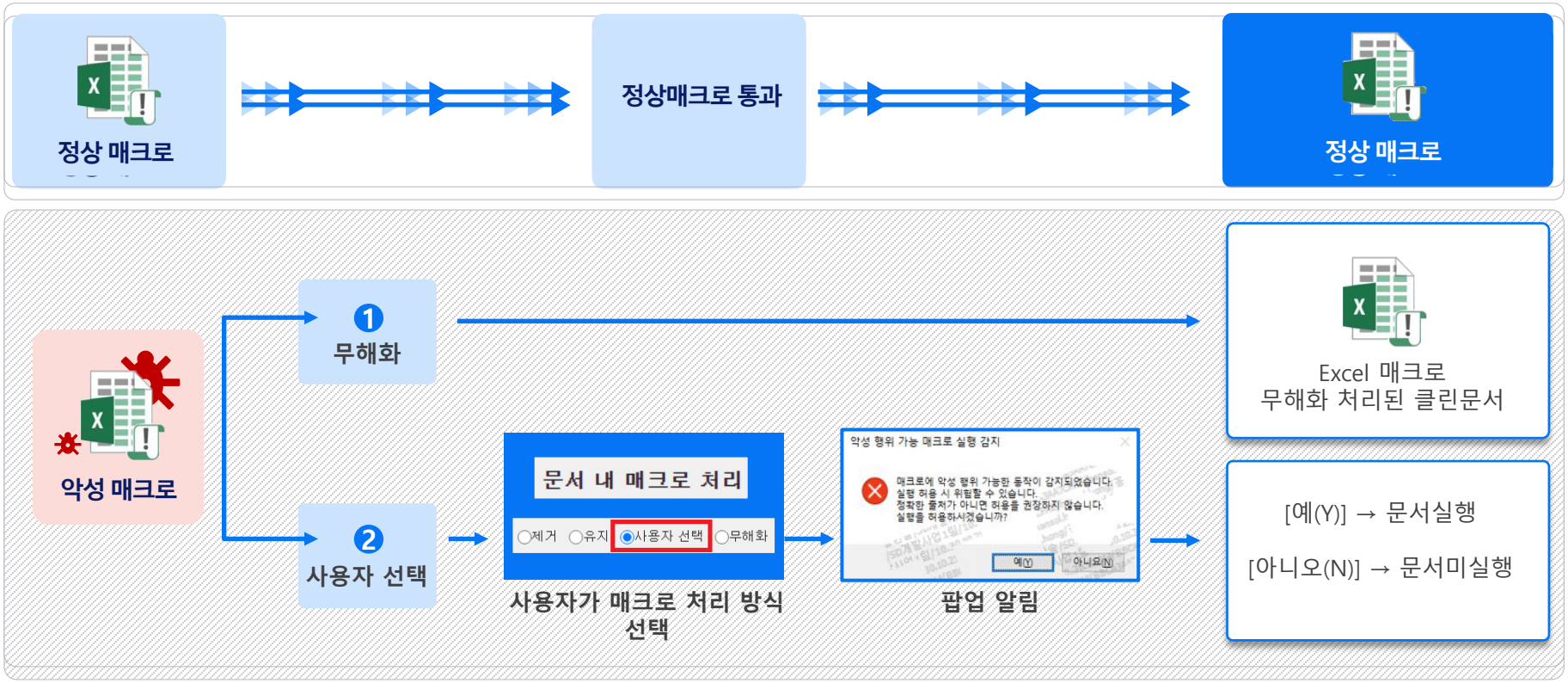
SHIELDEX 6.0 특장점

4. SHIELDEX 6.0 특장점

매크로 무해화

엑셀 매크로 판단 기능

- 기업에서 가장 많이 사용하는 엑셀 파일 및 매크로 기능 사용 빈도 높음
- 일반 CDR에서는 매크로 허용/삭제 기능만 제공
- 위험한 매크로는 무해화 또는 사용자 선택 기능 여부 제공
- 출원 제 10-2019-133448호 : 문서에 구성된 매크로의 악성코드 감염 확인 방법과 시스템

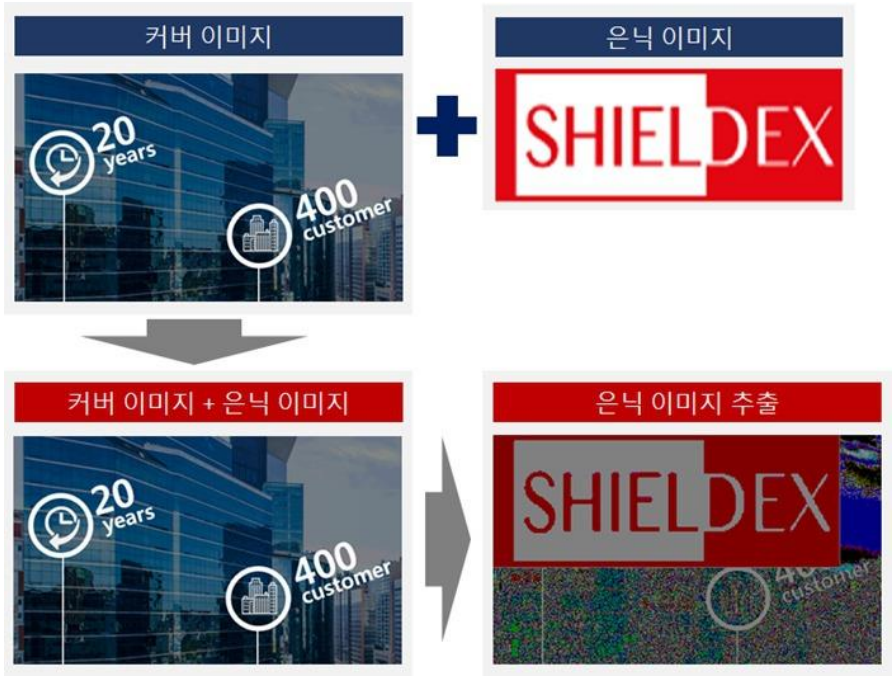


4. SHIELDEX 6.0 특장점

스테가노그래피 악성코드 제거

스테가노 그래피 등 이미지 CDR 완벽 처리

- 이미지를 재구성하여 위협 제거
- 스테가노그래피 기법에 대해 Anti-Steganography 기술 적용
- 100종 이상의 이미지 파일 확장자 무해화 처리

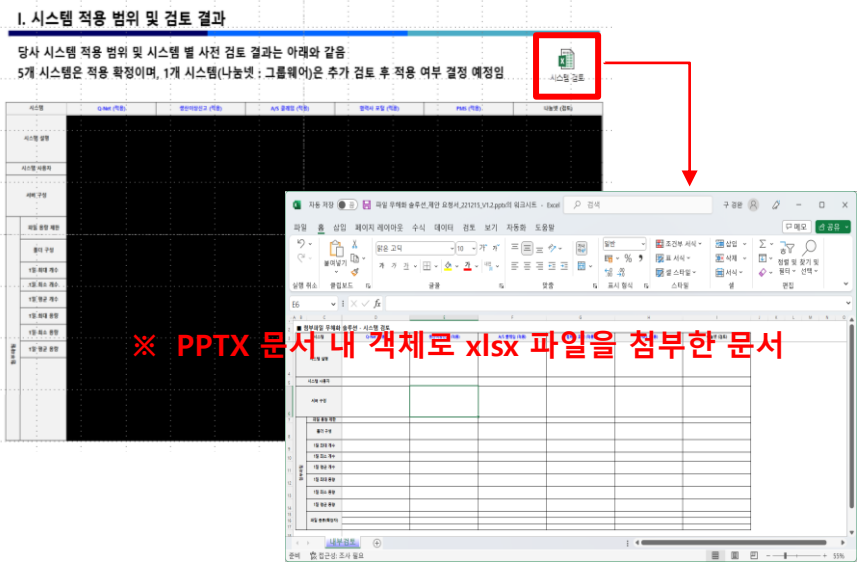


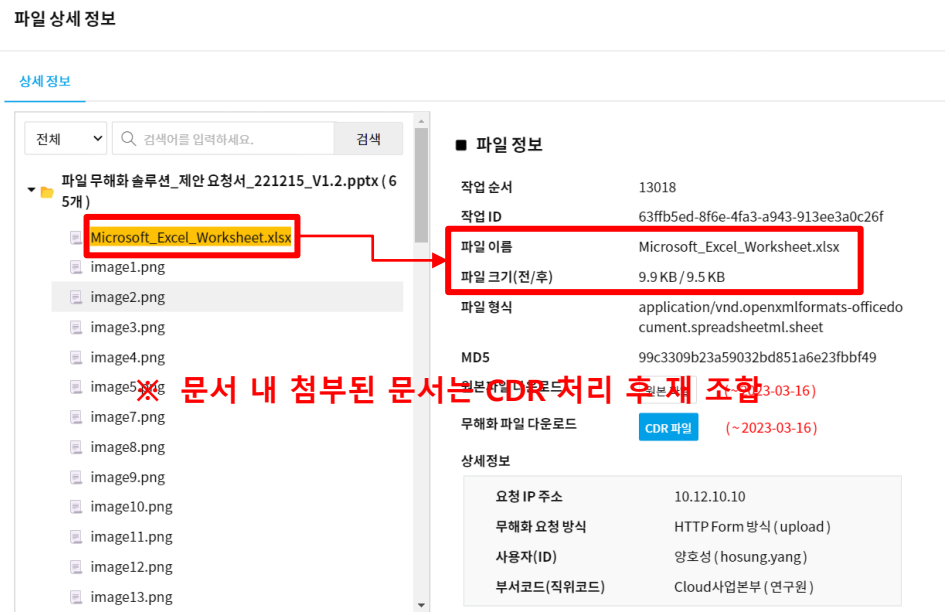
4. SHIELDEX 6.0 특장점

객체로 첨부된 문서/이미지 무해화

문서 내 첨부된 파일을 분리하여 CDR 처리

- 문서 내 첨부된 객체를 무조건 삭제 하지 않고 별도 추출 가능
- 문서 내 첨부된 객체 (문서) 을 추출하여 CDR 처리 후 재 조립하는 기술 적용
- **문서 내 첨부된 객체 (실행파일 등) 에 대해서 삭제 후 재 조립하는 기술 적용**



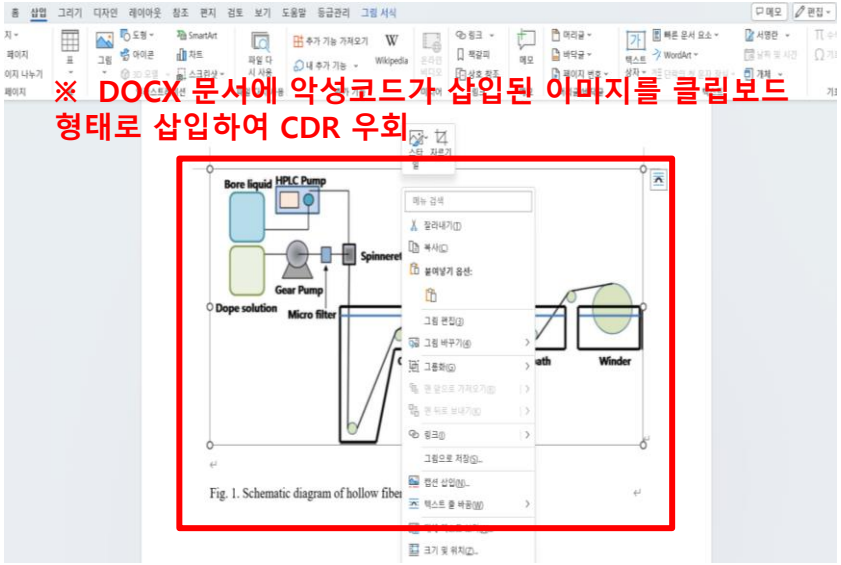


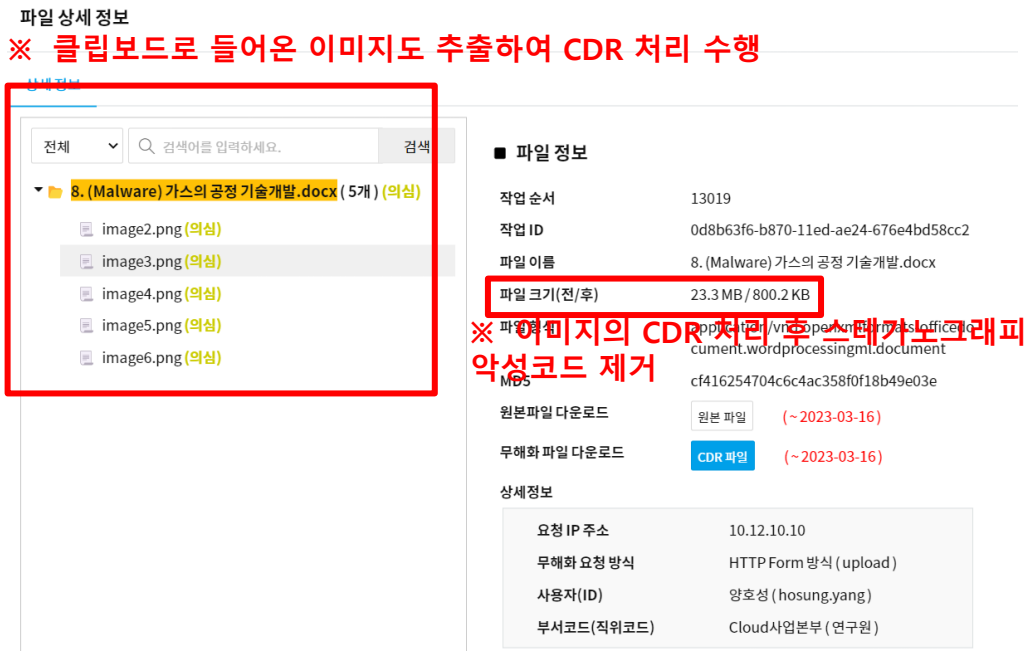
4. SHIELDEX 6.0 특장점

클립보드 형태로 들어온 이미지(스테가노그래피)로 악성코드 제거

클립보드로 들어온 악성파일에 대한 CDR 처리 기능

- CDR 솔루션을 우회하기 위해 최신 공격기법
- 클립보드 형태로 악성 이미지를 삽입 한 문서를 추출하여 CDR 처리 후 재 조립하는 기술 적용
- <u>기존 CDR 솔루션은 악성 이미지를 처리하지 못하고 내부로 반입</u>



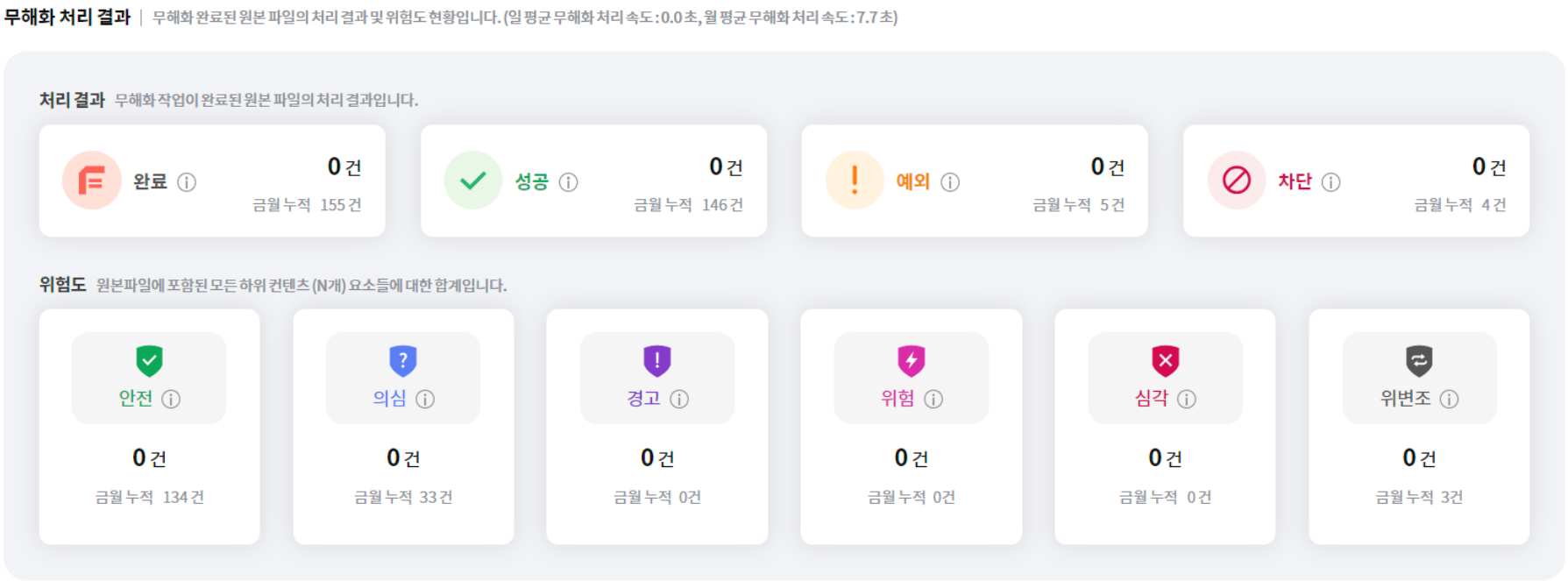


4. SHIELDEX 6.0 특장점

CDR 처리내역에 대한 상세 정보 제공

위험도별 모니터링

- CDR 정보 데이터를 기반으로 파일의 **위험도** 5단계 레벨 제공 (**안전 / 의심 / 경고 / 위험 / 심각**)
- **현재 반입되고 있는 파일에 대한 위험도를 즉각적으로 모니터링 기능 제공**

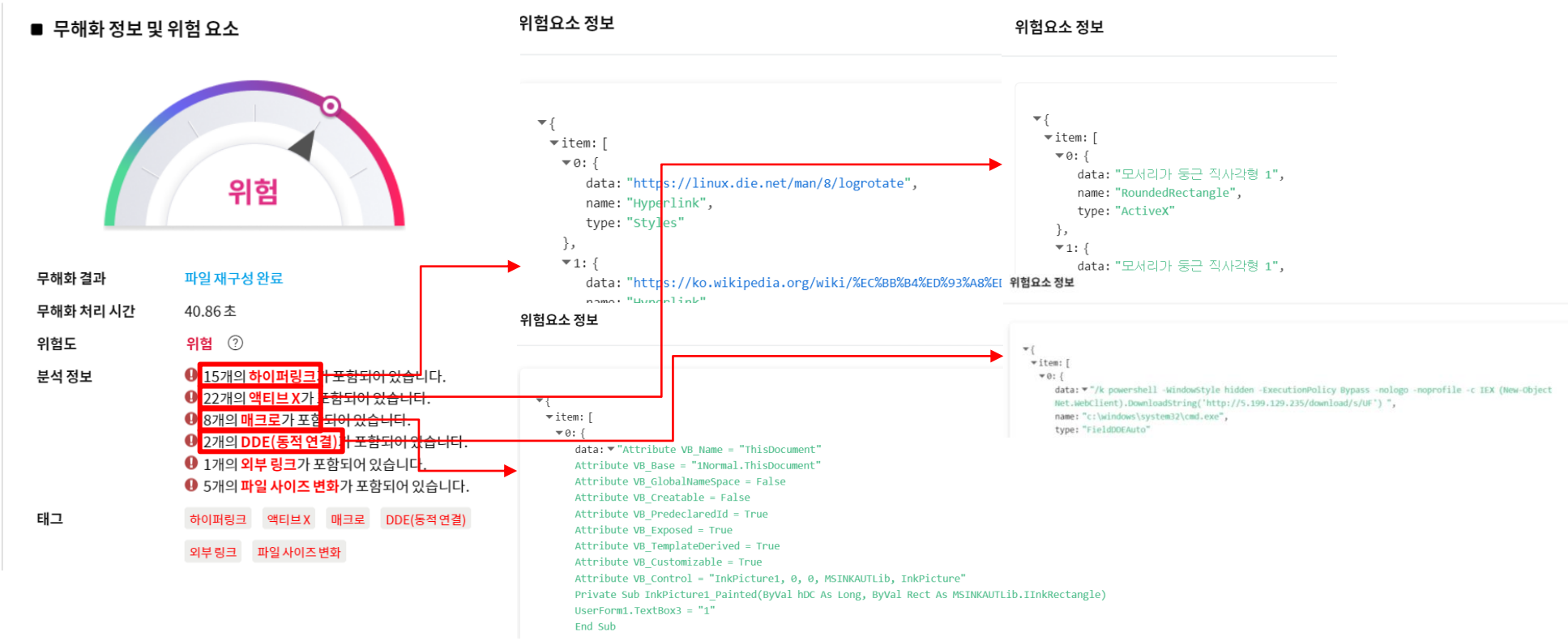


4. SHIELDEX 6.0 특장점

상세 분석이 가능한 CDR 처리 데이터 제공

솔루션 운영 리스크 감소를 위한 정보데이터 제공

- **CDR 처리 내역 상세를 포렌식 수준의 위험요소 분석 데이터 제공**
- 실제 CDR 처리한 위험정보 제공을 통한 사용자 문의 대응 및 보안 검토 대응

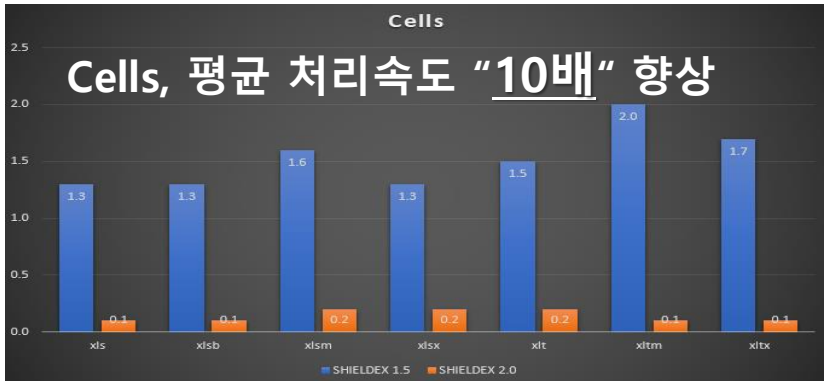


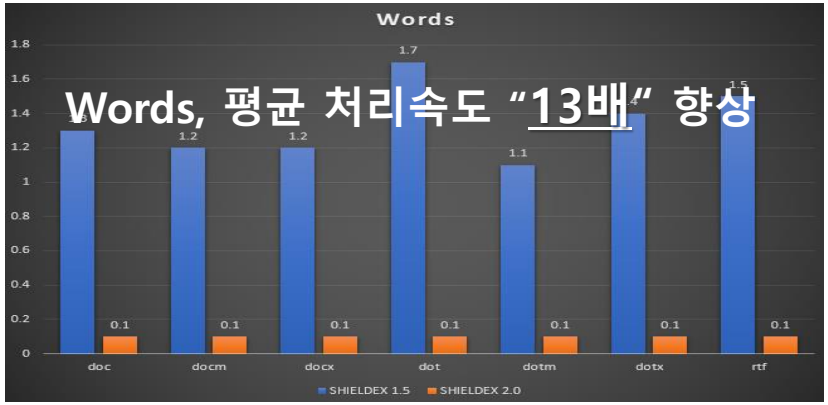
4. SHIELDEX 6.0 특장점

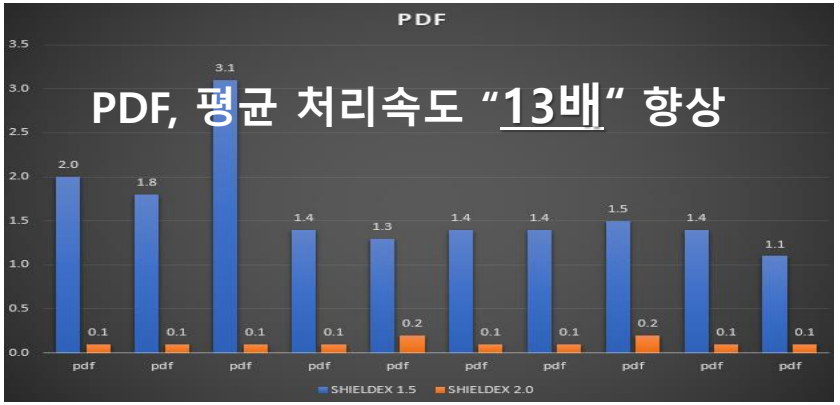
기존 자사 솔루션 대비 처리속도 대폭 향상

처리 속도 개선

- SHIELDEX 1.5 File 제품군에 비해 약 5~10배의 CDR 처리 성능을 끌어올림





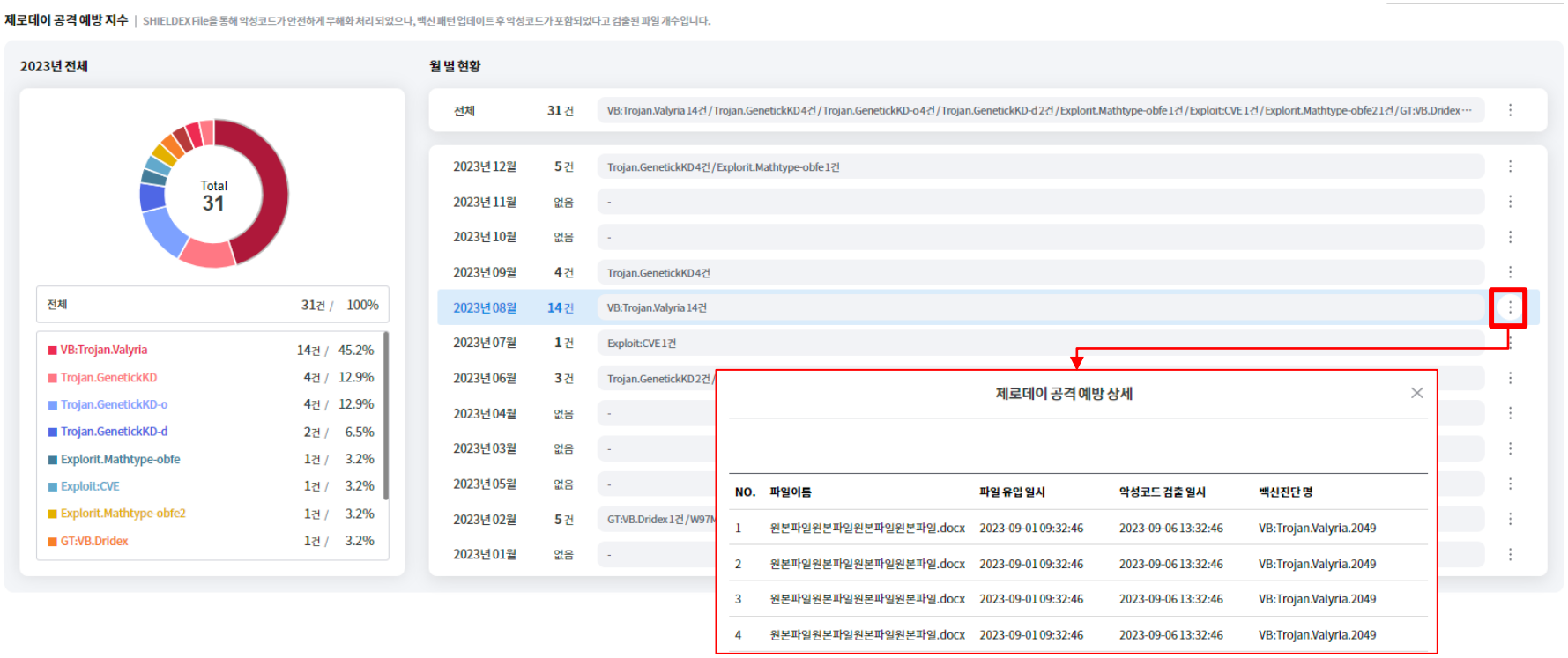


4. SHIELDEX 6.0 특장점

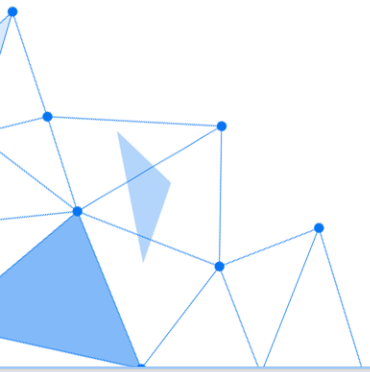
제로데이공격 예방지수 레포트

Zero Day Attack
공격 예방 리포트

- **CDR 도입으로 인한 Zero Day 공격 예방 효과의 정성적/정량적 모니터링**
- CDR 처리당시 백신이 악성으로 검출하지 않았으나 백신업데이트 이후 악성파일로 판별된 문서에 대한 레포팅 기능제공



THANK YOU



SOFTCAMP

소프트캠프㈜ 경기도 성남시 분당구 판교로 228번길 17, 판교세븐벤처밸리2 이랜텍동 2, 3층