SHIELDEX

Content Disarm & Reconstruction

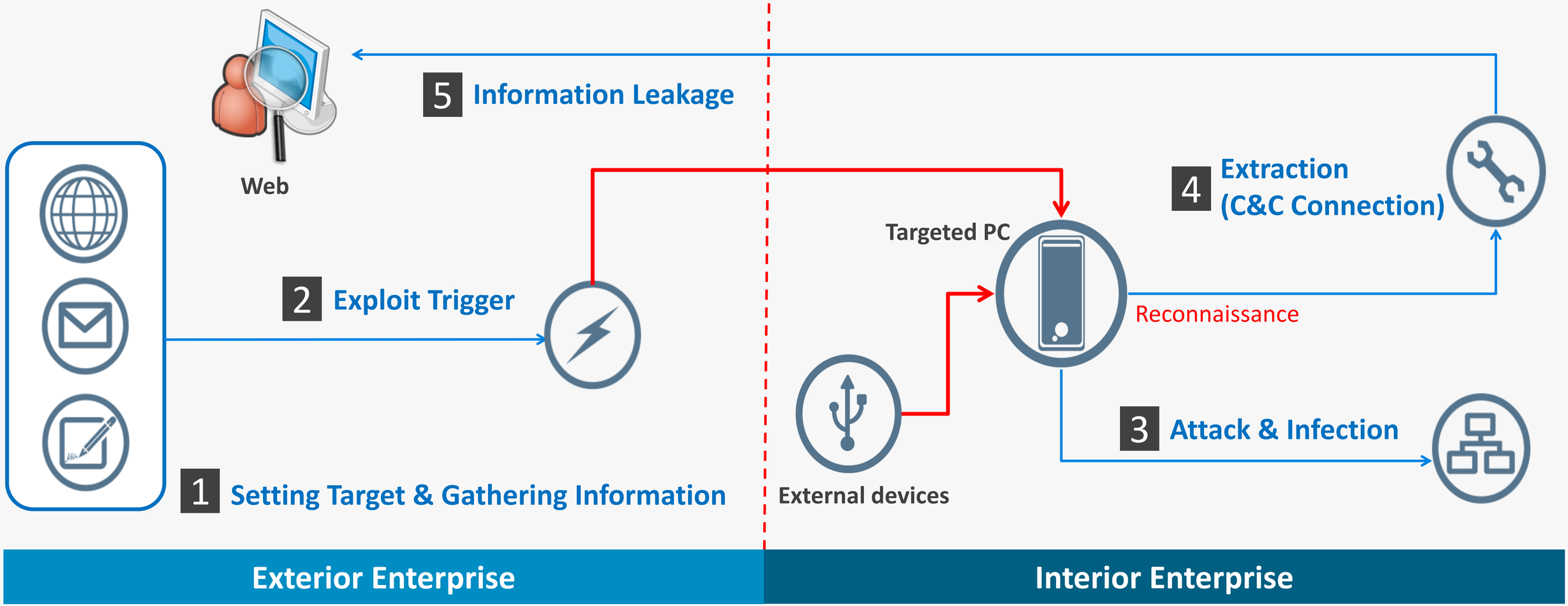
문서로 위장한 악성코드 대응에 최적화된 신기술 CDR

2017.12.14

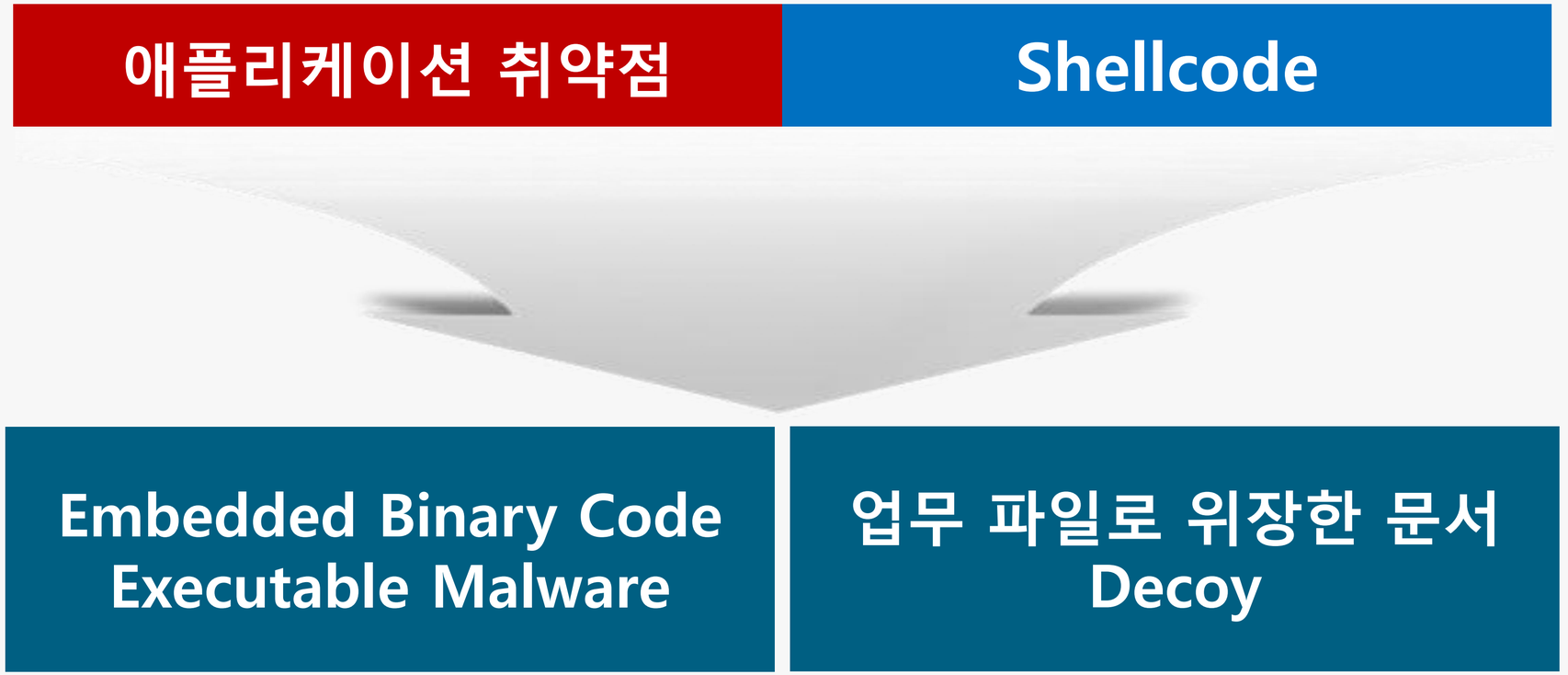
SOFTCAMP

INDEX

APT ; Advanced Persistent Threat



문서형 악성코드


애플리케이션 취약점
Shellcode
Embedded Binary Code
Executable Malware
업무 파일로 위장한 문서
Decoy

애플리케이션 취약점

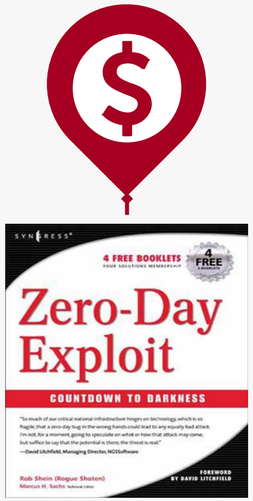
취약점 발표

취약점 분석

취약점 보완 업데이트

사용자 업데이트 설치

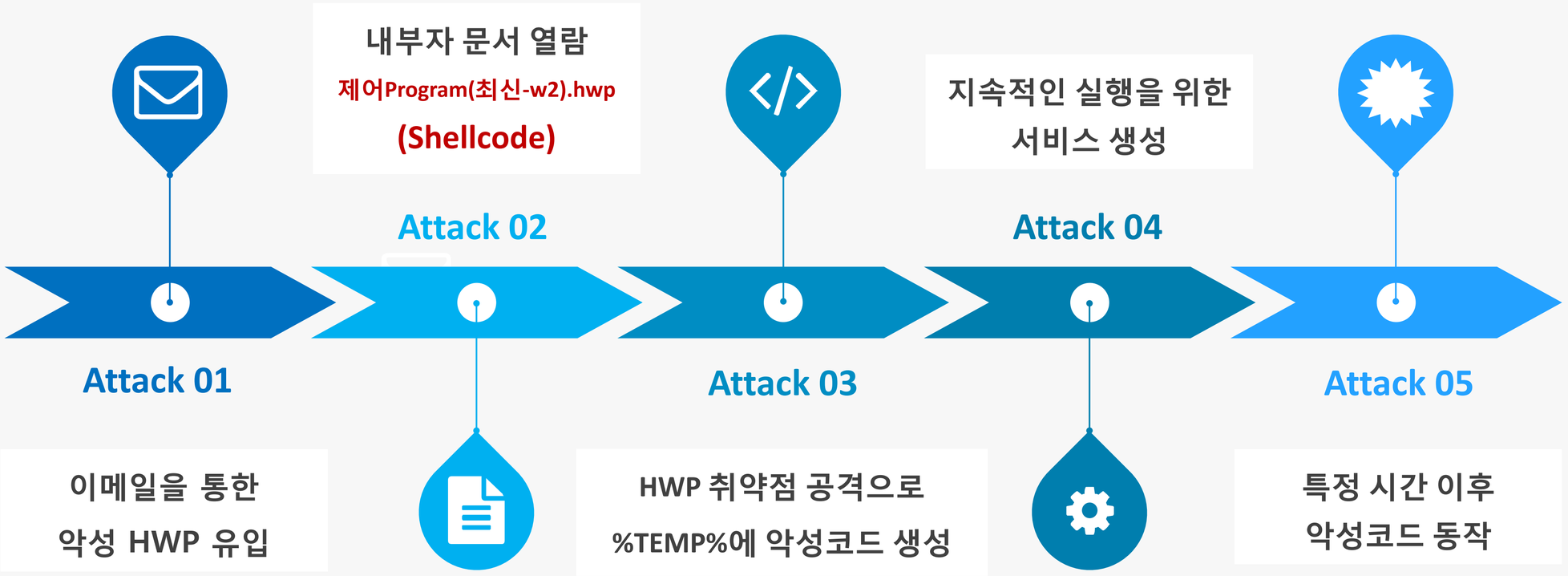
금전 요구 랜섬웨어로 전환



애플리케이션	취약점
Microsoft Word	CVE-2014-1761 CVE-2012-1856 CVE-2013-0633 CVE-2011-1980 CVE-2013-1331 CVE-2012-0158
Microsoft PowerPoint	CVE-2014-1761
Adobe PDF	CVE-2014-4148 CVE-2011-2462 CVE-2013-0640 CVE-2013-2729 CVE-2010-0110 CVE-2010-0188
한글	최근 3년간 한컴오피스 11번 보안 패치 적용 *출처 : 한컴오피스 홈페이지

Shellcode

한국수력원자력 내부 PC 해킹 공격 흐름도



Cyber Attacks, Ransomware

공격자가 발송한 메일

Cyber Attacks
Ransomware

첨부된 한글 문서

랜섬웨어	암호화 기법	발견 일시	주요 타깃	금전 요구
크립토락커 (CryptoLocker)	AES, RSA	2013년 9월	DOC/IMAGE	300-500 USD
CTB락커 (CTBLocker)	AES, ECDH	2014년 7월	DOC/IMAGE	0.5 USD

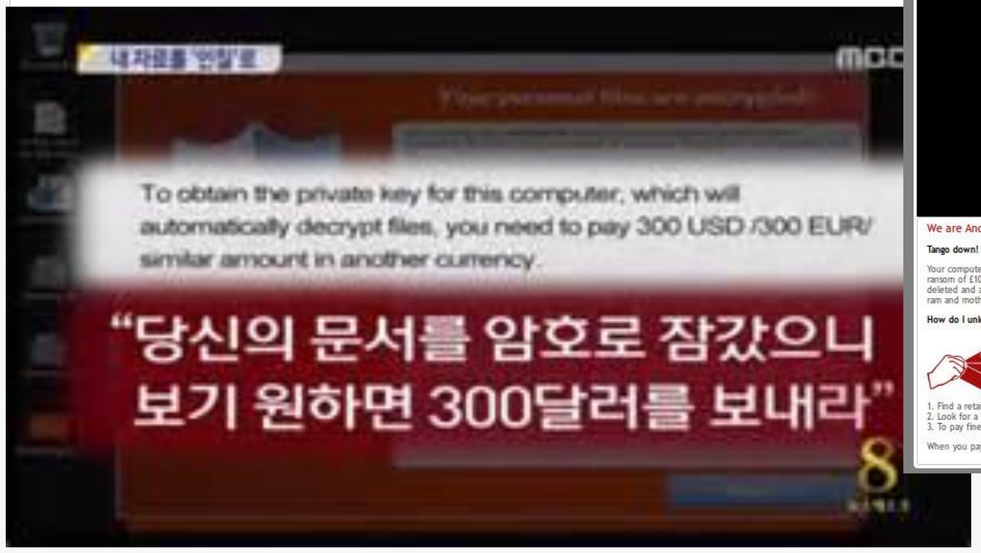
Cyber Attacks, Ransomware

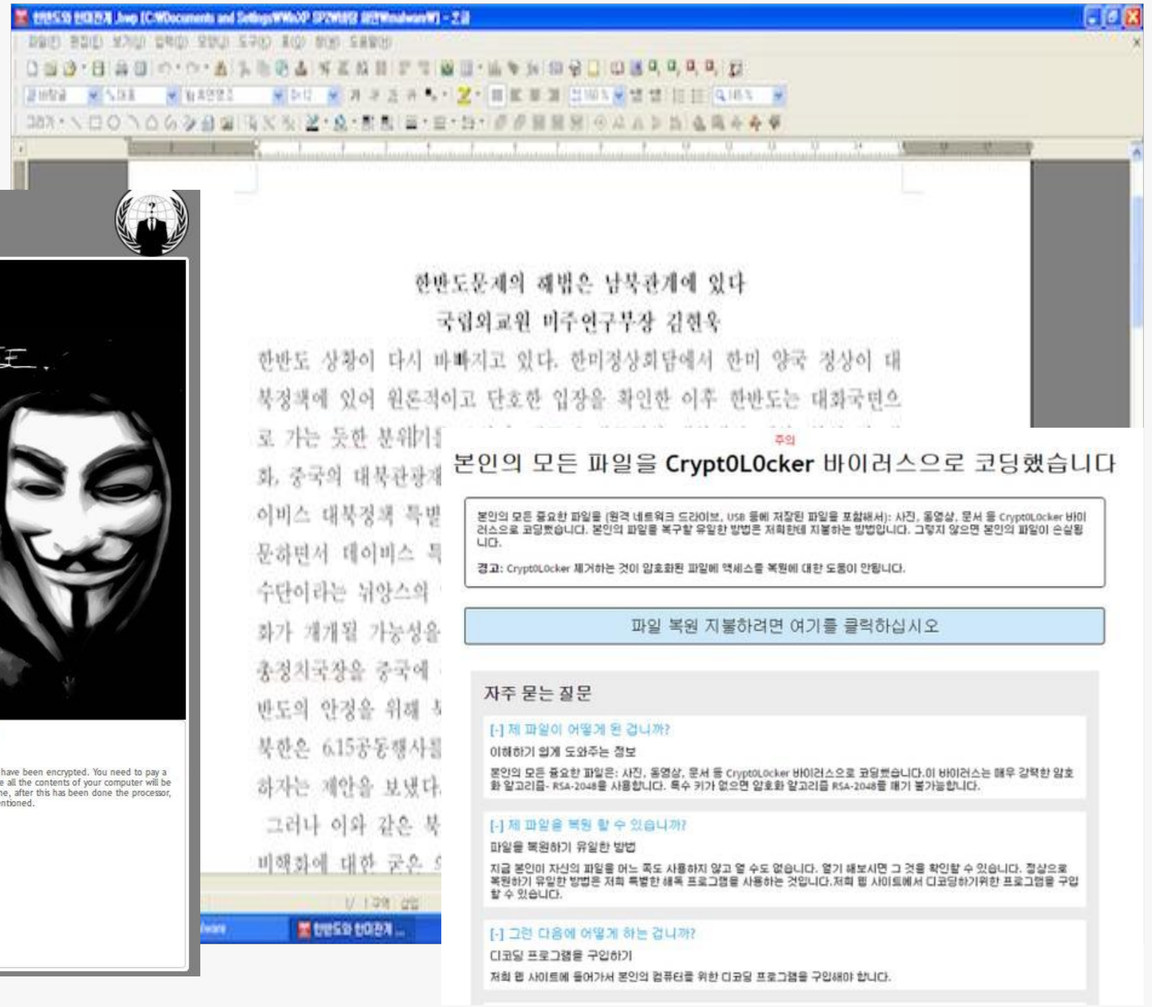
특정분야 정보탈취 노린 타겟형 악성코드 발견

– '印 ICBM 로켓과 韓 우주항공', '한미관계' 등 정상적인 아래한글 문서로 위장

한국인터넷진흥원(KISA, 원장 이기주)은 최근 우주항공과 외교 등 사회적 이슈가 된 사안에 대한 내용으
악성코드가 삽입된 한글파일이 첨부된 이메일이 발견되었다며 아래 한글 프로그램 사용자의 주의를 당부

이번에 발견된 메일의 첨부문서의 제목은 '印 ICBM 로켓과 韓 우주항공기술.hwp', '한반도와 한미관계
'초청장.hwp' 등이다. 파일 실행 시 정상적인 문서로 보이지만 실제로는 PC에 악성코드가 설치돼 사용자
입력한 정보와 PC에 저장된 자료가 해커에게 전송된다.





*출처 : 인터넷 침해 대응 센터

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

기존 보안 솔루션으로 대응 가능한가?

VS

정적 분석 Static Analysis

시그니처 기반으로 이미 알려진 악성코드 탐지, 방어

Zero-day 등 알려지지 않은 공격에 무방비

검사 통과한 후 내부에 유입된 파일 관리, 통제 불가

동적 분석 Dynamic Analysis

사용자와 유사한 가상환경에서 네트워크 트래픽 분석, 탐지, 방어

가상환경 우회 시 무방비

이동매체 통해 유입되는 악성코드 탐지 불가

어떤 기술로 대응해야 하나?

How does advanced malware act like AI?

신규 악성코드는 하루 **85만개씩** 생성

Target 공격은 전년대비 **42%** 증가

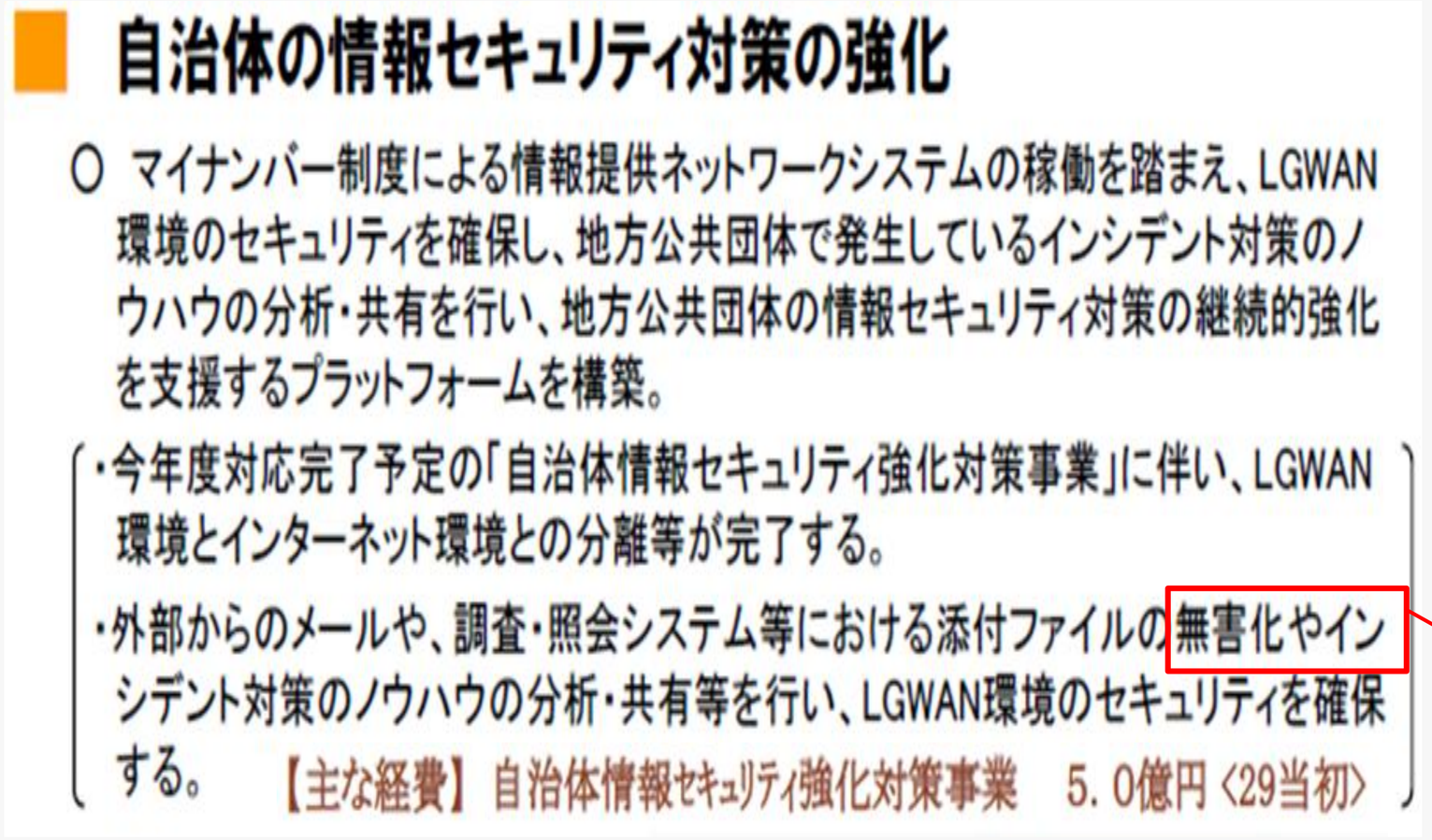
Gartner

CDR (Content Disarm & Reconstruction)

CDR 기술은 기존의 Malware 탐지 방식과는 달리 Malware 의 행위를 분석하거나
패턴을 탐지하지는 않지만, CDR 솔루션의 정책에 따라 의심되는 파일의 구성요소를 제거합니다.

가트너에서는 기존의 APT 대응 방식은 딜레마에 빠져 있으며,
기업은 Sandbox 를 이용한 행위분석 방식 등에 의존하는 대신 컨텐츠를 무해화 및 재구성하는 새로운 아이디어 기술을 시도할 것을 제안하고 있습니다.

해외에서 주목하고 있는 기술은?



自治体の情報セキュリティ対策の強化

○ マイナンバー制度による情報提供ネットワークシステムの稼働を踏まえ、LGWAN環境のセキュリティを確保し、地方公共団体で発生しているインシデント対策のノウハウの分析・共有を行い、地方公共団体の情報セキュリティ対策の継続的強化を支援するプラットフォームを構築。

・今年度対応完了予定の「自治体情報セキュリティ強化対策事業」に伴い、LGWAN環境とインターネット環境との分離等が完了する。

・外部からのメールや、調査・照会システム等における添付ファイルの無害化やインシデント対策のノウハウの分析・共有等を行い、LGWAN環境のセキュリティを確保する。

【主な経費】自治体情報セキュリティ強化対策事業　5.0億円〈29当初〉

일본 총무성에서는

표적형 공격에 대응하기 위해

전 지역의 모든 지자체에

망분리와 파일 무해화 도입을

의무화하고, APT 공격에 대한

새로운 대응책으로

무해화(CDR) 기술을

중요시 하고 있다.

CDR Technology

Content Disarm & Reconstruction

Verify
Formats

Analysis
Structure

Extract
Components

Re-Construct
& Verify

안전한 문서만 내부로 반입=CDR

SHIELDEX

SHIELD against **Ex**ternal file threats

SHIELDEX는 외부유입 문서에 대해, 파일 구조 스캔 및 CDR 과정을 거쳐, 안전한 문서만 내부로 반입 합니다.

File Scan

문서 구조 스캔

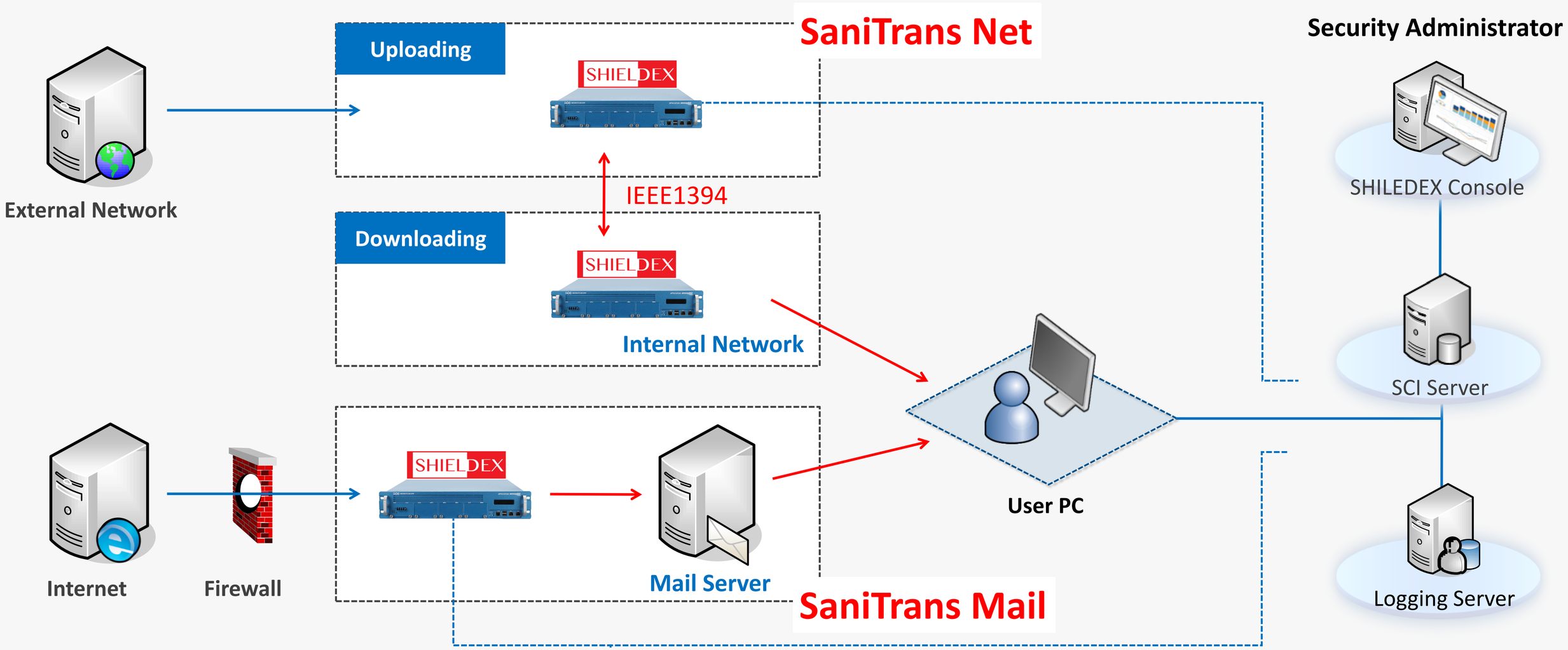
Sanitization

무해화/CDR

Logging

이력 관리

SHIELDEX System Layout

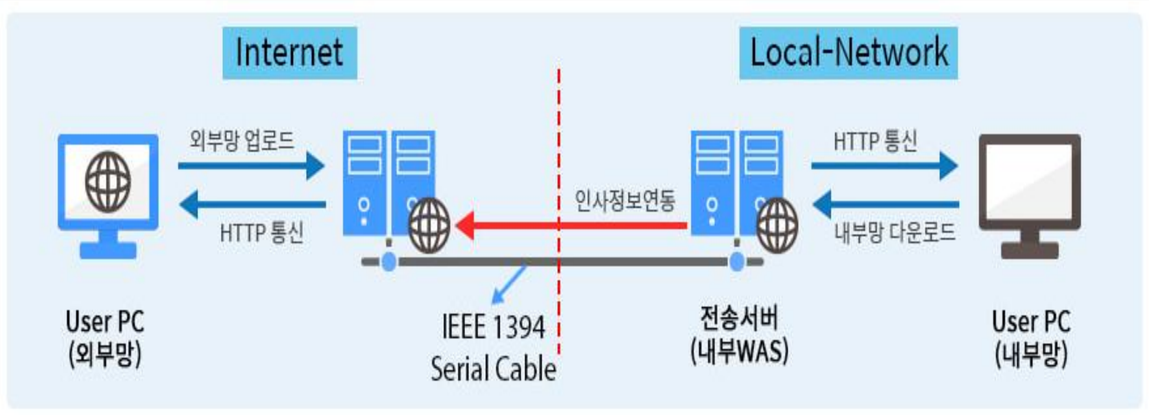


SHIELDEX Products

SHIELDEX

SaniTrans Net

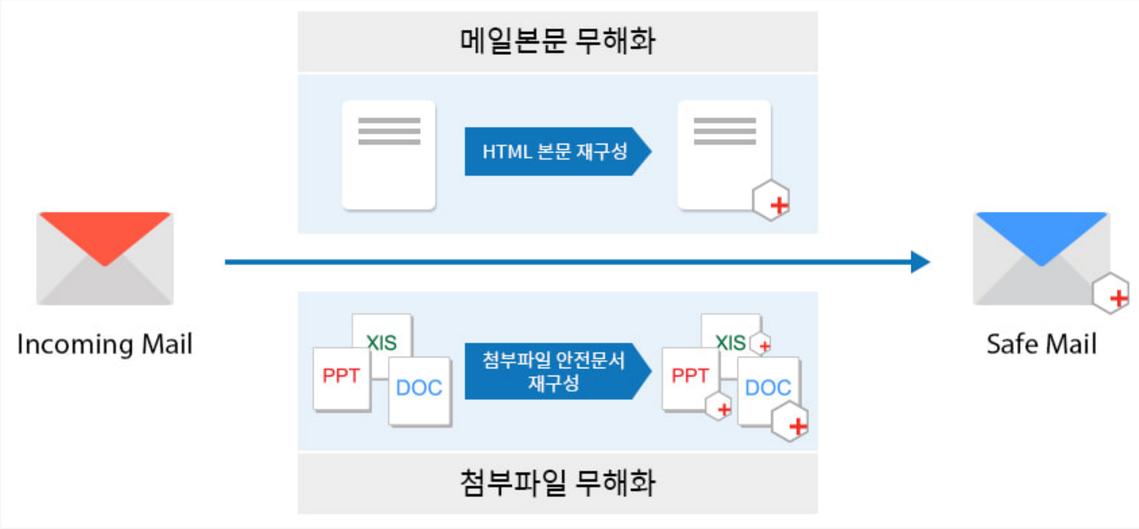
망분리 환경에서 망연계를 통해 유입되는 파일을
안전한 파일로 재구성하여 반입하는 망연계 파일전송 시스템



✓ 망분리 환경 최적화 ✓ 자체 모듈 도입 ✓ 반입 절차 강화

SaniTrans Mail

외부에서 유입되는 이메일을 무해화하여
안전한 메일과 첨부파일만 내부로 유입하는 메일보안 솔루션

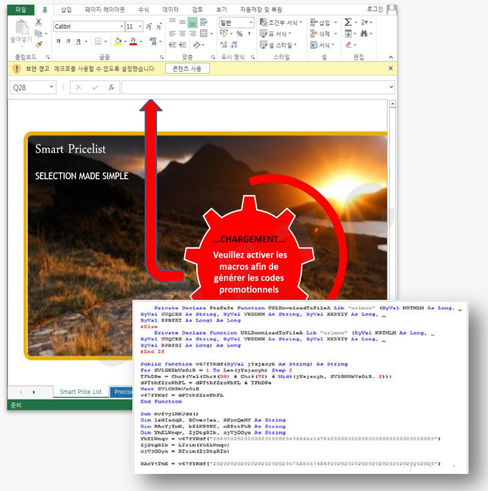


✓ 메일 본문 무해화 ✓ 첨부파일 무해화 ✓ 결과 리포트 제공

SHIELDEX Functions

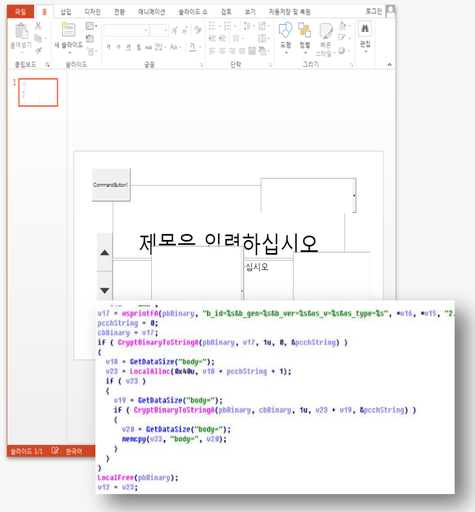
Malicious Macro 제거 기능

- ✓ Backdoor Drop Macro 삽입
- ✓ 정상/악성 매크로 체크
- ✓ 악성 매크로 제거



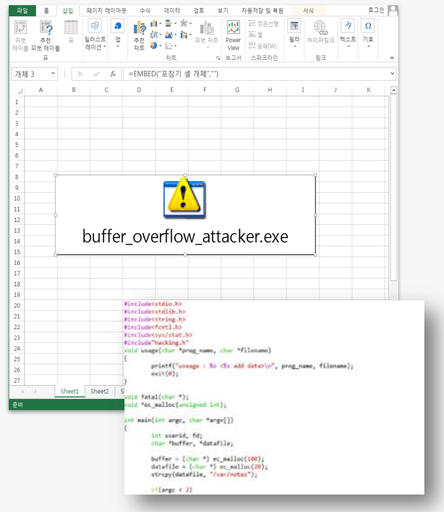
ActiveX Scripts 제거 기능

- ✓ Backdoor 드롭 Active X 삽입
- ✓ 의심 ActiveX Scripts 체크
- ✓ ActiveX Scripts 제거



Embedded Objects 제거 기능

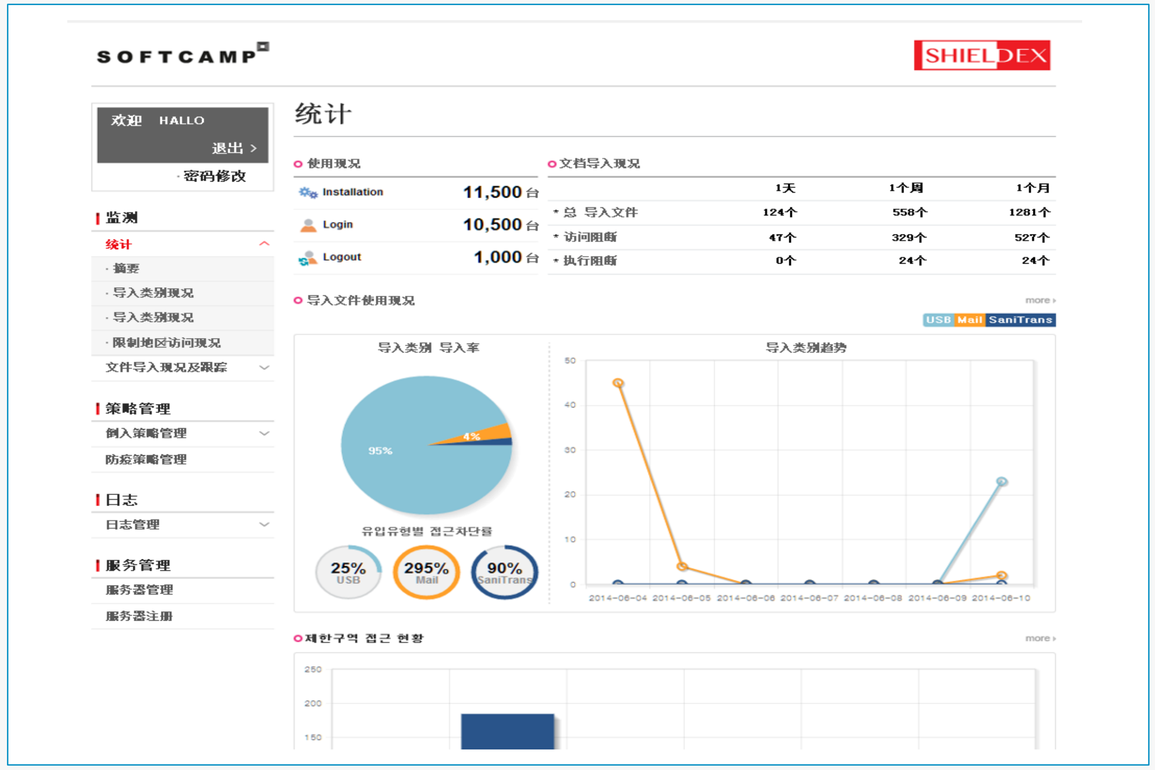
- ✓ Buffer Over Flow 실행 Objects 삽입
- ✓ 의심 Objects 체크
- ✓ Objects 제거



SHIELDEX Functions

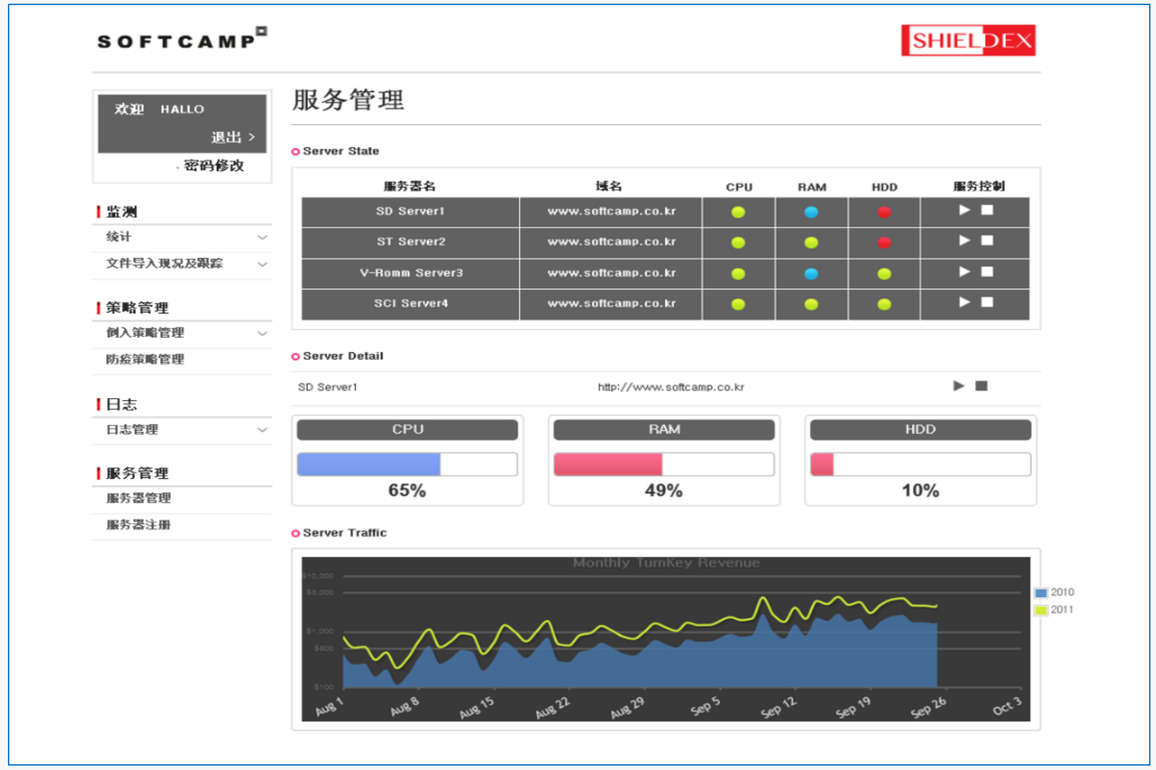
외부유입파일 통계

유입 유형별 반입현황, 사용자/파일 누적건수 등 통계

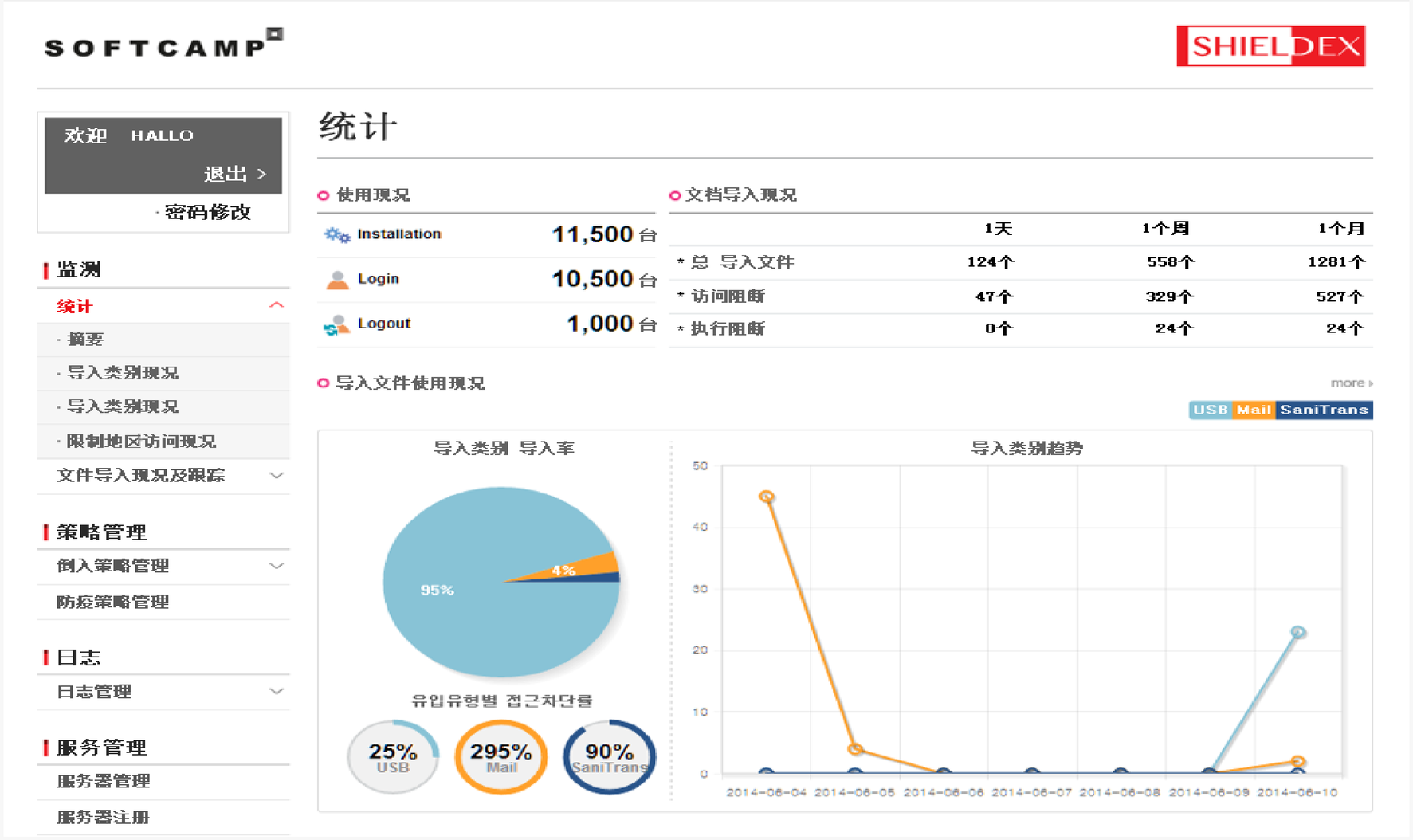


서비스 상태 관리

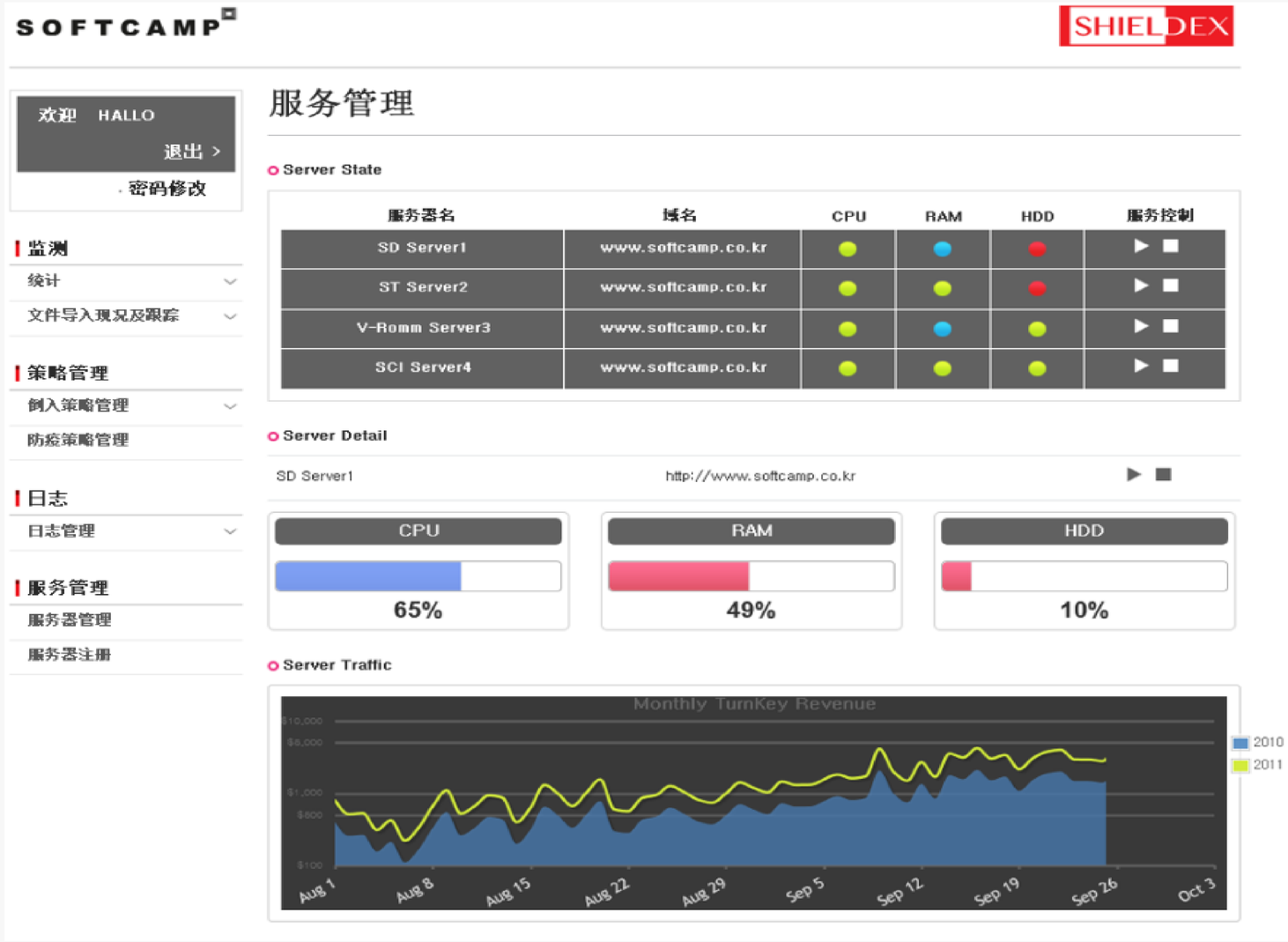
사용자 부서별 정책 설정, 유입파일에 대한 이력관리



SHIELDEX Functions



SHIELDEX Functions



SHIELDEX Success Case

OO 중요 공공기관

외부파일 유입통제

- ✓ 패턴 분석방식 우회 악성코드 증가
- ✓ 고도화, 지능화된 사이버 공격에 대한 원천적인 대응체계 마련 시급

지속적으로 변화하는 사이버 위협에 대한
선제적 대응체계 구축

외부파일 유입현황 관리

- ✓ 외부파일 유입현황 조회, 관리, 통제, 모니터링 시스템 체계 미흡
- ✓ 사용자/파일별 차단 현황에 대한 분석/통제 체계 필요

외부파일 반입 현황을 관리/통제할 수 있는
외부유입 파일현황 관리체계 구축

SHIELDEX Success Case

SHIELDEX 이용 현황 / Monthly 통계				
구 분	반입 시도 (건)	반입 성공 (건)	반입 차단 (건)	차단 사례
A 고객사	232,972	220,537	12,435	열람 불가 확장자 위변조 등
B 고객사	319,637	319,304	333	
C 고객사	89,688	89,084	604	

A 고객사

B 고객사

C 고객사

SHIELDEX Benefit

문서형 악성코드 차단

확장자 위,변조 등
문서파일 형태의 악성코드
원천 차단/격리
알려지지 않은 악성코드 대응

감염 문서 방역 및 재구성

외부유입 감염 문서
무해화 및 재구성하여
의심 악성 파일에 대한
선제 대응 가능

외부유입 파일관리

기관별/소속별/사용자별
실시간으로 외부유입 파일
현황 조회, 모니터링
통계 리포트 제공

Thank you

SoftCamp Co., Ltd

2nd, 3rd floor, Elentec Block, Pangyo 7 Venture Valley 2,
17, 228beon-gil, Pangyo-ro, Bundang-gu, Seongnam City, Gyeonggido

T. +82-1644-9366 | **E. jpkim@softcamp.co.kr**

SOFTCAMP