



화이트리스트 실행통제

iMON LOPE 제품 소개

제품 개요

■ 도입 배경

- Malware (악성코드)로 인한 피해 발생
- 신종/변종 출현으로 기존 백신 엔진으로 예방효과 미비
- 해킹 수법 지능화로 과거 패턴에 의한 대응 속도 한계

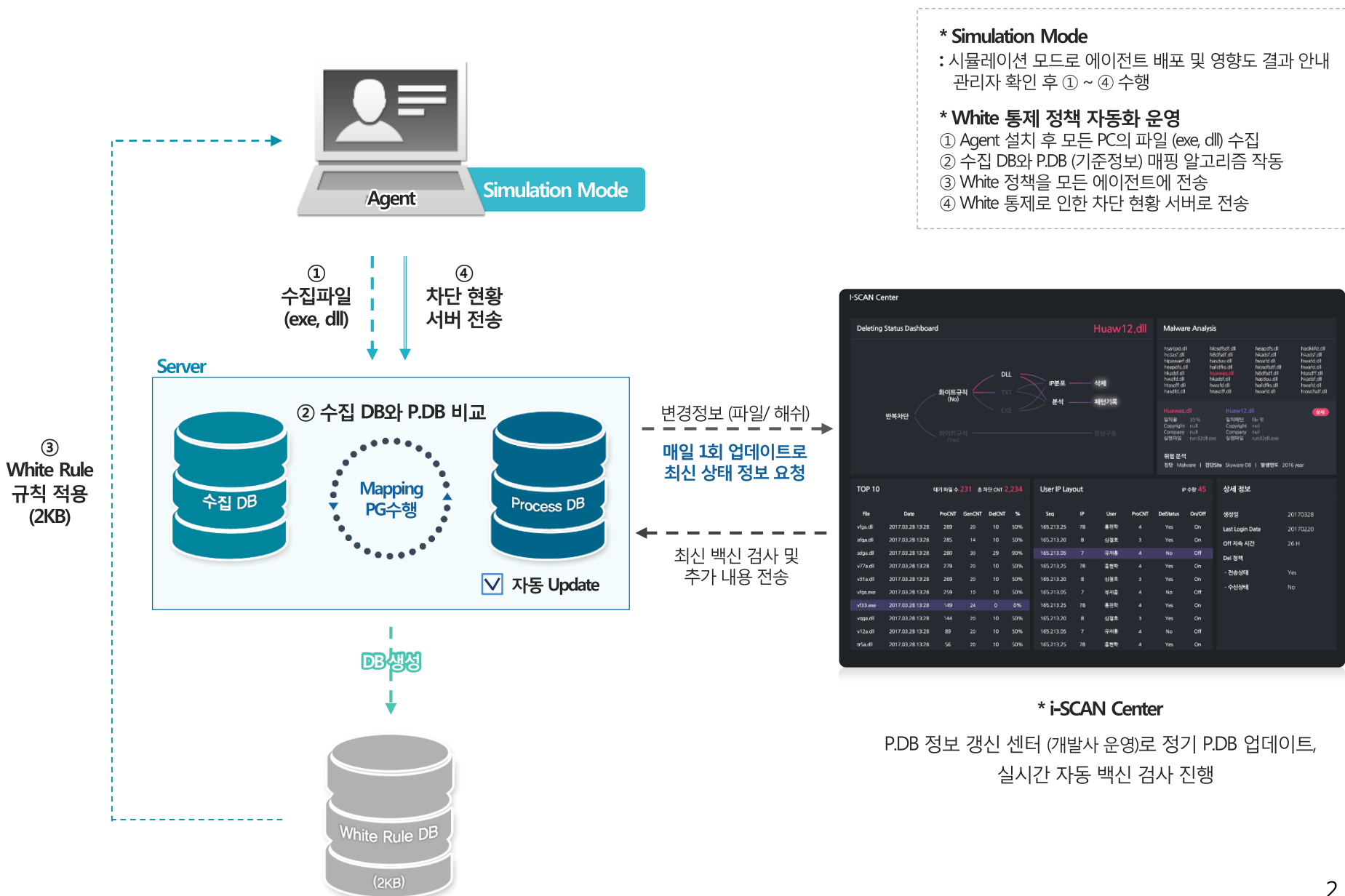
■ White List 통제 솔루션

iMON LOPE란?

EXE, Script Files (DLL) 실행 전 허용 여부를 판단한 후 허용 외 비인가 파일을 통제하여 실행 시 유입 가능성이 있는 해킹 프로그램 및 악성코드 (Malware) 차단

- White 통제 시 **관리자 업무 프로세스의 불편함을 자동화로 해결**
- P.DB (기준정보) 실시간 혹은 정기 업데이트 서비스 제공
- P.DB의 모든 파일 (1,100,000개)은 전 세계 56개 백신 검사를 통해 안전성 검증
- 모든 수집된 파일은 실시간 바이러스 검사 수행 가능 (i-SCAN Center)
- 저작권 사별 EXE, DLL 파일 정보 제공

Flow_모든 Process 자동화



Flow_모든 Process 자동화

③ White 규칙

자동생성규칙정책
정책 우선순위 #5

정적 대상 규칙

아래 목록에 실행 허가 할 규칙을 추가하십시오. 새로고침 등록

C	적용여부	규칙	생성일	변경일
<input type="checkbox"/>	적용	Google Inc	2017-04-05 14:56:09	2017-04-07 14:13:55
<input type="checkbox"/>	적용	Gyeong Tni Corp.	2017-04-05 14:56:17	2017-04-06 11:37:08
<input type="checkbox"/>	적용	SOFTFORUM	2017-04-05 14:56:18	2017-04-06 08:38:51
<input type="checkbox"/>	적용	Fasoo.com, Inc.	2017-04-05 14:56:24	2017-04-05 14:56:24
<input type="checkbox"/>	적용	Samsung SDS Co., Ltd	2017-04-05 14:56:32	2017-04-06 11:21:24
<input type="checkbox"/>	적용	Microsoft Corporation	2017-04-05 14:56:40	2017-04-07 12:08:10
<input type="checkbox"/>	적용	Pulse Secure, LLC	2017-04-05 14:56:41	2017-04-05 14:56:41
<input type="checkbox"/>	적용	Interezen. Co., Ltd.	2017-04-05 14:56:53	2017-04-05 14:56:53
<input type="checkbox"/>	적용	Arainia Solutions	2017-04-05 14:56:55	2017-04-05 14:56:55
<input type="checkbox"/>	적용	MarkAny	2017-04-05 14:56:56	2017-04-05 14:56:56
<input type="checkbox"/>	적용	NAVER Corp.	2017-04-05 14:56:56	2017-04-06 08:58:57
<input type="checkbox"/>	적용	NVIDIA Corporation	2017-04-05 14:56:57	2017-04-07 08:53:52
<input type="checkbox"/>	적용	Korea Trade network Co., L	2017-04-05 14:56:57	2017-04-05 14:56:57
<input type="checkbox"/>	적용	iniLINE Co., Ltd.	2017-04-05 14:57:00	2017-04-05 14:57:00
<input type="checkbox"/>	적용	Oracle America, Inc.	2017-04-05 14:57:01	2017-04-05 14:57:45
<input type="checkbox"/>	적용	Wacom Technology, Corp.	2017-04-05 14:57:06	2017-04-05 14:57:06
<input type="checkbox"/>	적용	Citrix Systems, Inc	2017-04-05 14:57:07	2017-04-05 14:57:07
<input type="checkbox"/>	적용	Citrix Systems, Inc.	2017-04-05 14:57:09	2017-04-05 14:57:09
<input type="checkbox"/>	적용	Citrix Systems, Inc.	2017-04-05 14:57:09	2017-04-05 14:57:09
<input type="checkbox"/>	적용	Citrix Systems, Inc.	2017-04-05 14:57:10	2017-04-05 14:57:10
<input type="checkbox"/>	적용	Wacom Technology	2017-04-05 14:57:10	2017-04-05 14:57:10
<input type="checkbox"/>	적용	TeamViewer GmbH	2017-04-05 14:57:11	2017-04-05 14:57:11
<input type="checkbox"/>	적용	Apple Inc	2017-04-05 14:57:13	2017-04-05 16:02:12

Total 115

[자동으로 생성된 White 규칙]

- 안전성이 검증된 범용 SW의 저작권 제품은 자동 White 규칙 생성
- 저작권사별 디지털서명이 여러 개일 경우 모두 등록
- White 규칙 생성의 경우 제품별 패치 및 업데이트 영향 無

④ 차단 정보

실행/차단이력 삭제이력 PC별수집현황 자가정지

총 발생횟수 1,827,394 회 검색

이력유형:
 ActiveX: 선택
 검색타입: 파일명 부서명 사용자 IP/세그먼트
 검색어:
 이력 발생일자: ~
 검색 초기화

C	운영방식	이...	사유	파일	회사	제품	부서	사용자	컴
<input type="checkbox"/>	실행차단	차단	화이트	uninst.exe			기획팀	박현아	HY
<input type="checkbox"/>	실행차단	차단	화이트	breadzip.exe			서버운영팀	박정우	PA
<input type="checkbox"/>	실행차단	차단	화이트	installdocker.m			서버운영팀	서우규	W
<input type="checkbox"/>	실행차단	차단	화이트	igfstray.exe			지식컨텐츠	송용호	YC
<input type="checkbox"/>	실행차단	차단	화이트	sqldeveloper.e			서버운영팀	박정우	PA
<input type="checkbox"/>	실행차단	차단	화이트	tortoisegit-lang			서버운영팀	서우규	W
<input type="checkbox"/>	실행차단	차단	화이트	tortoisegit-2.4.0			서버운영팀	서우규	W
<input type="checkbox"/>	실행차단	차단	화이트	makensisw.exe			지식컨텐츠	송용호	YC
<input type="checkbox"/>	실행차단	차단	화이트	dismhost.exe			기획팀	박현아	HY
<input type="checkbox"/>	실행차단	차단	화이트	microsoft.photo			CST	오영식	OY
<input type="checkbox"/>	실행차단	차단	화이트	microsoft.photo			CST	오영식	OY
<input type="checkbox"/>	실행차단	차단	화이트	uninstall.exe			지원팀	성호석	DE
<input type="checkbox"/>	실행차단	차단	화이트	dismhost.exe			지식컨텐츠	송용호	YC
<input type="checkbox"/>	실행차단	차단	화이트	microsoft.photo			CST	오영식	OY
<input type="checkbox"/>	실행차단	차단	화이트	codecompare.ex	Devart	Devart.CodeCor	서버운영팀	서우규	W
<input type="checkbox"/>	실행차단	차단	화이트	everything-1.3.4		Everything	지식컨텐츠	송용호	YC
<input type="checkbox"/>	실행차단	차단	화이트	uninis_ex.exe	Initech (c)	INISAFE Web/Cr	지원팀	성호석	DE

Total 17,692

1 2 3 4 5 6 7 8 9

P.DB 기준 정보와 일치하지 않는 저작권사 파일(exe, dll 등) 모두 차단

[자동화 White 통제 운영 시 차단 현황]

- ① 회사 및 제품명 정보가 없는 경우
 - ② 디지털서명이 없는 경우
- ※ ①, ② 정보는 있으나 P.DB에 없는 제품은 차단

최근 악성코드 스크립트 방식

* 사용자 1PC에서 수집한 현황

스크립트 유형	Windows 7 C:\Windows\	C:\friendPlus	C:\programfiles	- - -	Total
해당 저작권사	MS,폰트,K-defence	한국투자증권	안랩,DVDPlayer,Google	- - -	
DLL	27,406	601	2,188	- - -	34,723
TXT	875	213	0	- - -	1,276

□ 악성코드 유형 분석



□ 악성코드 특징

- 1) 스크립트 방식으로 악성코드 유포
- 2) Rundll32.exe (정상 프로그램) 을 이용하여 악성코드를 실행시킴
- 3) Script Files를 자동으로 통제하는 White 통제 솔루션

iMON LOPE 기능

□ 백신 검사

- 수집된 모든 파일은 안전성 진단 수행 (PDB)
- 바이러스 안전성은 온라인 검사 기능으로 진단 가능



□ 시뮬레이션 기능

- 강제 통제 정책 적용 전 시뮬레이션 모드를 통해서 사전 문제점 도출 및 문제 해결 가능

□ 자동화 기능

- “자동 모드” 설정하면 안전성이 검증된 파일 기준으로 **자동으로 화이트 규칙 목록에 추가**
- 매월 P.DB 업데이트 자동 실현
- 수집된 DB의 새로운 파일에 대해서는 **자동으로 바이러스 안전성 진단 수행**
- 통제 정책으로 차단되는 파일은 **자동으로 “파일 삭제” 기능**