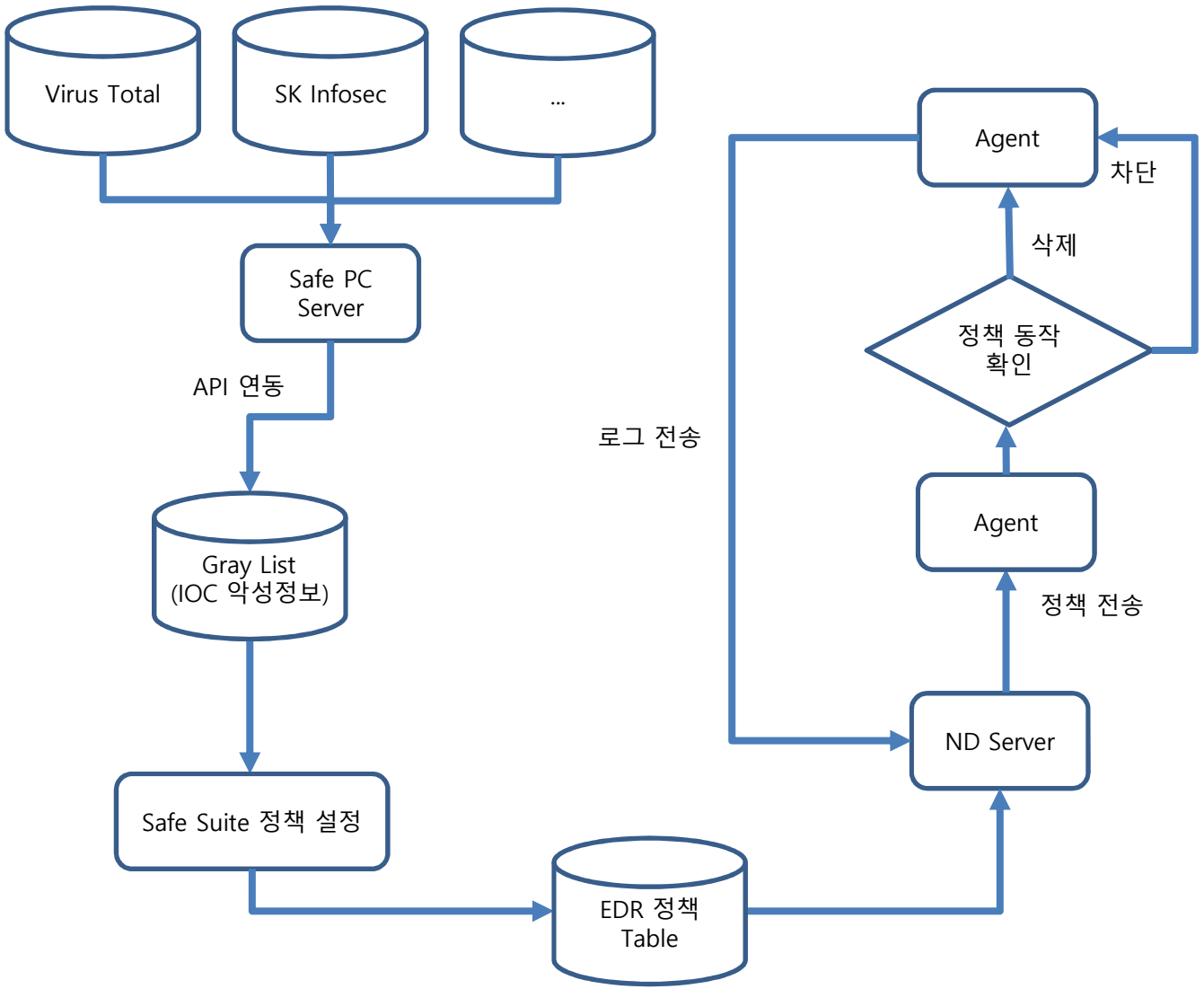
Smart Security & Service
NICS TECH

EDR 프로세스 UI 설계

2018. 3

프로세스 흐름도



- Virus Total, SK Infosec 등 Safe PC 서버의 API 연동을 통해 차단 대상 프로세스/IP/레지스트리 정보를 DB에 저장
- SafeSuite 관리자 설정을 통해 차단/삭제 할 프로세스,IP,레지스리를 설정
- ND 서버를 통해 Agent 정책 전달 및 로그 수신

EDR 정책 설정/적용

SafeSuite > 보안관리 > 정책설정

프로세스

수동 추가 | 추가 | 삭제 Total : 3

	프로세스명	HASH	등록구분	처리방식
☐	Iexplore.exe		Virus Total	차단
☐	Notepad.exe	tWr+cWWtNBp0nS072SXYeXKKH_Sk3y	관리자 수동 등록	삭제
☐	Dbgview.exe	EkS9AqIDvsGx4KuF7Y7YNQHsTRfmE/G	skinfosec	삭제

IP 리스트

수동 추가 | 추가 | 삭제 Total : 2

	시작 IP	종료 IP	등록구분	처리방식
☐	10.0.0.1	10.0.0.99	Virus Total	차단
☐	192.168.99.1		관리자 수동 등록	차단
☐	1.1.1.1	1.1.1.222	skinfosec	차단

레지스트리

허용 이동 | 추가 | 삭제 Total : 2

	레지스트리 경로	레지스트리 NAME	등록구분	처리방식
☐		OUTLOOK.EXE	Virus Total	차단
☐		NateOn.exe	관리자 수동 등록	삭제
☐			skinfosec	차단

- EDR 정책은 전사 정책으로 동작한다. (개별/직급 등의 설정 없음)
- Virus Total, SK Infosec 등 API 연동을 통해 얻어 온 프로세스, IP, 레지스트리 정보를 White List 와 같이 Gray List와 동일한 기능을 하는 Table에 저장하여 관리자가 해당 프로세스, IP, 레지스트리를 관리(차단/삭제)할 수 있도록 처리한다. (추가)
- API 연동을 통해 얻어온 정보 뿐 아니라 관리자가 직접 수동으로 프로세스, IP, 레지스트리를 등록하여 관리 할 수 있도록 처리한다. (수동추가)

프로세스 추가

프로세스

수동 추가 | 추가 | 삭제 Total : 3

	프로세스명	HASH	등록구분	처리방식
☐	Iexplore.exe		Virus Total	차단
☐	Notepad.exe	tWr+cWWtNBp0nS072SXYeXKKH_Sk3y	관리자 수동 등록	삭제
☐	Dbgview.exe	EkS9AqIDvsGx4KuF7Y7YNQHsTRfmE/G	skinfosec	차단

프로세스 리스트

	프로세스명	HASH	등록구분
☐	Iexplore.exe		Virus Total
☐	Notepad.exe	tWr+cWWtNBp0nS072SXYeXKKH_Sk3y	Virus Total
☐	Dbgview.exe	EkS9AqIDvsGx4KuF7Y7YNQHsTRfmE/G	Skinfosec
☐	explore.exe		Skinfosec
☐	Notepad++.exe	tWr+cWWtNBp0nS072SXYeXKKH_Sk3y	Skinfosec
☐	Excel.exe	EkS9AqIDvsGx4KuF7Y7YNQHsTRfmE/G	Virus Total
☐	Word.exe		Virus Total

저장 | 닫기

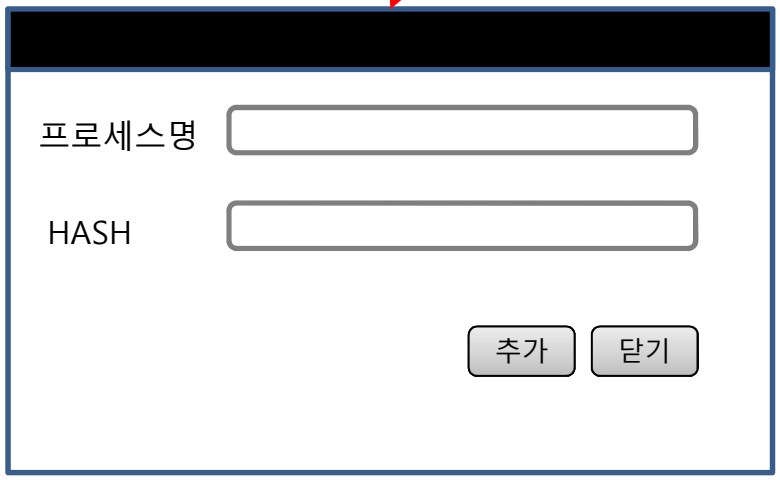
- 프로세스 추가의 경우, GrayList에 있는 프로세스 목록 중 정책 프로세스에 등록되지 않은 목록 들이 표시되어 정책에 등록할 수 있도록 한다.

프로세스 수동 추가

프로세스

수동 추가 | 추가 | 삭제 | Total : 3

	프로세스명	HASH	등록구분	처리방식
☐	Iexplore.exe		Virus Total	차단
☐	Notepad.exe	tWr+cWWtNBp0nS072SXYeXKKH_Sk3y	관리자 수동 등록	삭제
☐	Dbgview.exe	EkS9AqIDvsGx4KuF7Y7YNQHsTRfmE/G	skinfosec	차단



- 관리자가 수동으로 프로세스를 등록할 수 있도록 수동 추가 기능을 제공한다.
- 프로세스 뿐 아니라 IP, 레지스트리 항목에 대해서도 GrayList에서의 추가, 수동 추가를 제공 한다.

EDR 로그

오늘 | 2018-03-24 ~ 2018-03-31 | 차단

그룹

☑ 전체 ☐ 프로세스 ☐ IP ☐ 레지스트리

조회

Excel Total : 9

그룹	아이디	사용자명	IP	MAC	차단형태	차단타입	차단항목	등록일시
기술연구소	Test1	홍길동	1.1.1.1	AA:AA:AA:AA:AA	삭제	프로세스	Excel.exe	2016-12-12 02:32:42
경영기획실	Test3	홍길순	1.1.1.2	BB:BB:BB:BB:BB:BB	차단	프로세스	Word.exe	2016-12-12 02:31:42
경영기획실	Test3	홍길순	1.1.1.2	BB:BB:BB:BB:BB:BB	삭제	프로세스	Excel.exe	2016-12-12 02:30:42
운영팀	Test2	홍길례	1.1.1.3	22:22:22:22:22:22	삭제	IP	211.1.1.0	2016-12-12 02:22:42
운영팀	Test2	홍길례	1.1.1.3	22:22:22:22:22:22	차단	프로세스	OUTLOOK.EXE	2016-12-12 02:21:42
운영팀	Test2	홍길례	1.1.1.3	22:22:22:22:22:22	차단	프로세스	NotePad.exe	2016-12-12 02:20:42
기술연구소	Test1	홍길동	1.1.1.1	AA:AA:AA:AA:AA	차단	프로세스	Outlook.exe	2016-12-12 02:15:42
기술연구소	Test1	홍길동	1.1.1.1	AA:AA:AA:AA:AA	차단	프로세스	Excel.exe	2016-12-12 02:10:42
기술연구소	Test4	홍길석	1.1.1.4	11:11:11:11:11:11	차단	프로세스	Eclipse.exe	

- 차단/삭제 정책의 EDR 로그 조회 화면
- 검색조건 : 차단 일시, 차단 형태 (차단/삭제), 차단타입(프로세스,IP,레지스트리), 검색타입(그룹,아이디,사용자명,IP,MAC)