Endpoint Detection & Response 요구사항분석

CONTENTS

1. 메뉴 구성 및 정책 화면 샘플

1. EDR 시스템 일반
2. EDR 시스템 보안관리
3. EDR 시스템 분석조사
4. EDR 시스템 모니터링
5. EDR 시스템 감사로그
6. EDR 시스템 보고서
7. AGENT – 보호
8. AGENT – 수집
9. AGENT – 탐지
10. AGENT – 대응
11. AGENT – 기타

EDR 시스템 일반: 요구사항

김태균 차장

Agent | Safe PC Server | ADS Plus | SOC Plus

EDR 시스템의 일반적인 기능으로서 아래의 기능을 지원해야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
일반	환경구성	LOW	지원 플랫폼	**어플라이언스**, 클라우드 등의 플랫폼에서 동작할 수 있도록 고려되어야 한다.
		HIGH	지원 운영체제: 서버	서버 OS는 서버용 Linux를 지원해야 한다. (OS 검토 필요: 예. RHEL, **CentOS**, Ubuntu 등)
		HIGH	지원 운영체제: 에이전트	에이전트 지원 OS는 **Windows**를 기본으로 Linux, Mac OS 등으로 확장되어야 한다.
	호환성	HIGH	표준: 웹 표준 준수	모든 웹은 표준(HTML5 등)을 준수해야 한다.
		MEDIUM	브라우저	모든 웹은 크롬, 파이어폭스, IE를 지원해야한다. (단, 기본은 크롬 혹은 IE 브라우저)
		HIGH	외부 시스템 연동	외부 보안 시스템 혹은 기타 시스템과의 연동을 고려하여 API를 제공해야 한다. (수집 API, 대응 API 등)
		HIGH	에이전트 다국어 환경 지원	다양한 언어 환경의 운영체제에서 동작을 고려해야 한다. (**유니코드**) (우선지원: **한국어**)
	보안성	HIGH	데이터 보호: 전송 데이터	모든 통신 수단은 안전한 암호통신 프로토콜을 사용해야 한다. (TLSv1.2, 키교환 RSA 2048bit 이상, 암호/해시 256bit 이상)
		HIGH	데이터 보호: 시스템 접속 정보	모든 시스템, DB 등 접속 정보는 암호화(해시)되어 저장해야 한다. (웹 브라우저 메모리 덤프 시, ID/PW 평문 노출 이슈 해결)
		HIGH	시간: 시간 동기화	서버와 에이전트 시간은 지속적으로 동기화 되어야 한다.
	가용성	MEDIUM	이중화 구성	정책 시스템, 분석 시스템, 관리 시스템, 스토리지 등 제품을 구성하는 요소 별 이중화 구성을 지원해야 한다. **(허순구 부장님)**
		HIGH	주요 서비스 보호	주요 시스템의 서비스(데몬 등)의 상태를 감시하고, 서비스가 킬 된 경우 다시 시작할 수 있어야 한다.
		MEDIUM	주요 서비스 보호 불가	주요 시스템의 서비스(데몬 등)이 복원(다시 시작 등)되지 않을 경우 대응 방안이 있어야 한다.
		LOW	주요 서비스 복구 방안	주요 시스템의 서비스(데몬 등)의 무결성이 훼손되었을 경우 복구 방안이 있어야 한다.
저장	데이터 저장소	HIGH	확장	분산 파일 시스템 지원 및 병렬 확장이 가능해야 한다.
		HIGH	가용성	데이터 손실에 대비할 수 있는 기능을 제공해야 한다.
		HIGH	데이터 검색	데이터의 크기 및 저장 위치에 상관없이 검색 기능을 제공해야 한다.

EDR 시스템 일반: 결정사항

인프라 제공형태	on-premise	추 후 cloud 서비스 제공 연구 필요
서비스 제공형태	어플라이언스 (OS+제품 SW)	
장비 구성	관리서버(정책,UI, Intel 등 포함), 분석서버, 데이터서버, 수집서버	
서버OS	모든 장비 CentOS 기반 운영체제 사용	
에이전트 OS지원	Windows Client OS에 한함	추 후 Windows 서버 및 MAC OS, Linux는 추후 연구 필요
데이터베이스 제공 형태	수집서버: 없음	
	데이터서버: 엘라스틱 서치	
	분석서버: 없음	머신러닝 구성 등
	정책서버: postgreSQL, MariaDB	관리(UI), 정책, INTEL(ioc, 3rd 등)
웹 브라우저 지원 형태	표준 HTML5 사용	크롬, 파이어폭스, 엣지 등
외부 시스템 연동	자사 제품에 한함	당장은 백신을 조사하고, 이 후 시스템에 제공 여부는 조사 필요.
에이전트 다국어 환경 지원	유니코드 인코딩을 사용	당장은 한국어에 한함
전송 데이터	OpenSSL을 사용하여 당시 암호화 규격에 맞게 사용	수집서버: 압축파일 형태로 SSL을 통해 전송
시스템 설정 정보	모든 시스템 및 DB의 설정 정보는 암호화하여 사용	
시간동기화	관리서버가 주가되어 모든 서버 및 에이전트 시간동기화	
이중화 지원	수집서버에 한함	1차적으로 별도 유료 소프트웨어 사용하고, 추후에 다른 방안이 있는지 연구
주요 서비스 보호	모든 시스템의 주요 서비스(데몬 등)의 상태를 감시 및 다시 실행	서버쪽에서 오픈소스(Monit) 등을 활용하여 진행

EDR 시스템 일반 (계속)

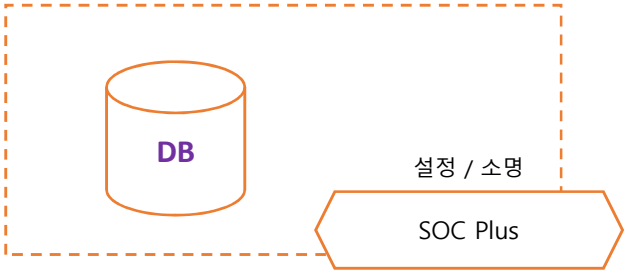
김태균 차장

Cat.2	Cat.3	Priority	Requirement	Detail
식별 및 인증	설정	HIGH	접근제어: 관리자/사용자 웹 인증	설정된 인증 시도 횟수 및 잠금 시간 등을 초과할 경우 계정이 잠금되야 한다.
		HIGH	접근제어: 웹 콘솔 접속 제한	설정된 접근 허용 IP가 아닐 경우, 웹 콘솔에 접근이 제한되어야 한다.
		HIGH	접근제어: 에이전트 사용자 인증	인증 시도 횟수 및 잠금 시간 등 계정 잠금 설정에 따라 계정이 잠금되어야 한다.
		LOW	인증강화: 멀티팩터 인증	지식기반, 소유기반, 생체기반 중 선택적으로 멀티팩터 인증을 지원해야 한다. (**구글 OTP 지원**)
	관리자	HIGH	일반접속	웹 콘솔에 접속할 수 있도록 식별 및 인증 기능을 제공해야 한다.
		HIGH	최초접속, ID/PW 변경 강제화 기능	최상위 관리자가 제품에 최초 접속 시 제품이 기본으로 제공하는 ID 및 패스워드의 변경을 강제화하는 기능을 제공해야 한다.
	사용자	HIGH	일반접속: 웹	사용자 웹에 접속할 수 있도록 사용자 식별 및 인증 기능을 제공해야 한다. (소명처리 등을 위한)
		HIGH	일반접속: 에이전트	에이전트에 접속할 수 있도록 사용자 식별 및 인증 기능을 제공해야 한다.
		HIGH	최초접속, PW 변경 강제화 기능	사용자가 에이전트에 최초 접속 시 패스워드의 변경을 강제화하는 기능을 제공해야 한다.
		HIGH	인증 가용성	에이전트가 오프라인(서버와 통신 불가) 시, 인증하여 사용할 수 있도록 인증 방식에 대해 고려해야 한다. (검토 필요)
	엔드포인트	HIGH	엔드포인트 식별	엔드포인트를 고유하게 식별할 수 있어야 한다.
		HIGH	엔드포인트 인증 가용성 1	에이전트 설치가 불가능하여 인증이 불가능한 엔드포인트들에 대한 인증 방식에 대해 고려해야 한다. (검토 필요)
		HIGH	엔드포인트 인증 가용성 2	서버 등 에이전트가 설치는 가능하지만 사용자 인증이 불가능한 장비의 인증 방식에 대해 고려해야 한다. (검토 필요)
	보안	HIGH	패스워드 기준	9자 이상, 영문대문자/소문자/숫자/특수문자 중 3가지 이상의 규칙 조합으로 만족하는지 검증해야 한다.
		HIGH	패스워드 마스킹	인증이 진행되는 동안 사용자/관리자에게 패스워드가 마스킹(예: *****)되어 보이도록 해야 한다.
		HIGH	패스워드 저장	패스워드는 어떤 곳에서든 평문으로 저장되어서는 안된다. 해시하여 저장해야 한다. (해시 알고리즘 256bit 이상)
		HIGH	재사용방지	인증정보가 재사용되는 것을 방지(예: 타임스탬프 사용하여 SALT 값 적용)해야 한다.
		HIGH	피드백 제공 X	인증 실패시, 실패 이유에 대한 피드백(예: ID 오류, 패스워드 오류 등)을 제공하지 않아야 한다. 실패 횟수는 제공해야 한다.
	세션	HIGH	세션 잠금/종료: 웹	로그인 이후 설정된 시간(10분이하) 동안 동작이 없을 경우, 세션 잠금 또는 세션 종료 기능을 수행해야 한다.
		HIGH	세션 잠금/종료: 에이전트	로그인 이후 설정된 시간(10분이하) 동안 동작이 없을 경우, 세션 잠금 또는 세션 종료 기능을 수행해야 한다.
		HIGH	동시 접속 제한: 웹	로그인 이후 다른 단말에서 동일 계정 또는 동일 권한으로 로그인을 수행할 경우, 신규 접속 차단 or 이전 접속 종료해야한다.
		HIGH	동시 접속 제한: 에이전트	로그인 이후 다른 단말에서 동일 계정 또는 동일 권한으로 로그인을 수행할 경우, 신규 접속 차단 or 이전 접속 종료해야한다.

EDR 시스템 일반 – 환경설정

옥치해 부장

인사정보연동



닉스테크 EDR 중 SOC Plus는 아래의 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
환경설정	관리자 관리	MEDIUM	관리자 구성	관리자는 최고관리자(제품에서 제공)와 최고관리자가 생성하는 서브관리자로 구성된다.
		MEDIUM	관리자 추가/삭제/수정	관리자를 추가/삭제/수정 할 수 있어야 한다. (관리자명, 소속, ID, 인증코드, 연락처 등)
		MEDIUM	관리자 인증코드	관리자 생성 시 입력한 인증코드는 해당 관리자가 웹 콘솔에 최초 접속 시 입력하고 비밀번호를 변경하도록 하는데 사용한다.
		MEDIUM	관리자 권한 설정	관리자 별 메뉴 접근 권한, 부서 접근 권한이 분리되어 있어야 한다.
		MEDIUM	관리자 비밀번호 초기화	관리자 비밀번호를 초기화하고, 재설정할 수 있는 기능을 제공해야 한다.
	사용자 관리	MEDIUM	사용자 추가/삭제/수정	사용자를 추가/삭제 수정 할 수 있어야 한다. (사용자명, 소속, ID, 인증코드, 연락처 등)
		MEDIUM	사용자 인증코드	관리자 생성 시 입력한 인증코드는 해당 사용자가 에이전트에 최초 접속 시 입력하고 비밀번호를 변경하도록 하는데 사용한다.
		MEDIUM	사용자 부서 추가/삭제/수정	부서를 추가/삭제/수정 할 수 있어야 한다.
		MEDIUM	사용자 비밀번호 초기화	사용자 비밀번호를 초기화하고, 재설정할 수 있는 기능을 제공해야 한다.
		MEDIUM	사용자 현황 조회	엔드포인트, IP, 이름, ID를 통한 사용자 정보 검색기능을 제공해야 한다. (1개의 단말, IP 등에 여러 사용자 사용 가능 할 경우)

EDR 시스템 일반 – 환경설정(계속) 옥치해 부장

닉스테크 EDR 중 **Safe PC서버 또는 ADS Plus**는 아래의 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
환경설정	시스템 관리	MEDIUM	연동: 인사 정보	인사 정보 연동 방안을 고려해야 한다. (AD, LDAP 연동 설정 화면 제공, 혹은 스크립트를 통한 연동 등)
		HIGH	연동: 보안 시스템 (대응)	자사 보안제품(NAC, DLP) 및 타 보안 시스템과의 연동 방안을 고려해야 한다.
		MEDIUM	연동: 보안 시스템 (탐지)	타사 보안제품(VirusTotal, SecuDium 등) 연동 방안을 고려해야 한다.
		LOW	연동: 타 시스템 (로그)	다양한 로그 수집 등을 위한 타 시스템과의 연동 방안을 고려해야 한다. (Rest API 등)
		LOW	연동: 타 시스템 (인증)	타 시스템과 인증 기능을 연동할 수 있도록 고려해야 한다. (예. SSO)
		MEDIUM	수집 데이터 스토리지 현황	현재 연동된 스토리지의 수, 상태를 확인할 수 있어야 한다. (스토리지 서버 분리 시)
		MEDIUM	수집 데이터 스토리지 설정	수집된 데이터를 저장할 스토리지를 설정할 수 있어야 한다. (스토리지 서버 분리 시)
		MEDIUM	수집 데이터 스토리지 알림 설정	스토리지의 사용 임계치를 설정하고, 설정한 값을 초과할 경우 관리자에게 알림 메일을 발송할 수 있어야 한다.
		MEDIUM	감사증적 임계치 알림 설정	감사증적이 저장되는 RDBMS를 의미(수집 데이터 저장 스토리지 아님). 저장공간 임계치 설정, 초과시 알림 메일 발송해야 한다.
		LOW	언어 설정	웹 및 에이전트의 메시지 팝업 시 다국어 지원 (한글, 중문, 영문)
		HIGH	시간 설정	서버는 신뢰 가능한 시간을 제공해야 한다. NTP 서버 등을 설정할 수 있어야 한다.
		LOW	로그 설정	로그 보관 주기, 백업 파일 생성 주기 등을 설정할 수 있어야 한다.
		HIGH	주기 설정: 로그 업데이트	실시간, 준실시간, 일정 주기 등에 대한 부분을 설정할 수 있어야 한다. (실시간, 준실시간 적용 여부 우선 결정 필요) 정책과 로그 주기는 분리하고, 실시간/주기에 대해서 설정은 가능하게 하자.
		HIGH	주기 설정: 정책 업데이트	변경된 보안정책, 대응정책 등에 대해 에이전트가 정책을 업데이트하는 주기를 설정해야 한다. (실시간 기능 등 추가고려 필요)
		HIGH	주기 설정: 모듈 업데이트	모듈 수정, 무결성 훼손 등으로 에이전트에서 모듈을 다운로드하고 업데이트 하는 주기를 설정해야 한다.
		HIGH	세션 관리: 인증 세션 잠금/종료 설정	웹과 에이전트의 로그인 이후, 설정한 시간이 초과될 경우 세션을 잠그거나 종료할 수 있도록 설정이 가능해야 한다. (시간 등)
		HIGH	접근제어: 관리자/사용자 웹 인증	인증 시도 횟수 및 잠금 시간 등 계정 잠금 설정이 가능해야 한다.
		HIGH	접근제어: 웹 콘솔 접속 제한	관리 콘솔에 접근 가능한 IP를 제한할 수 있도록 설정이 가능해야 한다.
		HIGH	접근제어: 에이전트 사용자 인증	인증 시도 횟수 및 잠금 시간 등 계정 잠금 설정에 따라 접근제어 되어야 한다.
		HIGH	무결성 관리: 서버	서버 모듈, 설정 등에 대한 무결성 체크가 가능해야 한다. (자동 주기별, 관리자 요청시 모두 구현 필요)
		HIGH	무결성 관리: 에이전트	에이전트 모듈, 설정 등에 대한 무결성 체크가 가능해야 한다. (자동 주기별, 관리자 요청시 모두 구현 필요)
		HIGH	무결성 관리: 알림	서버 및 에이전트 무결성이 훼손되었을 경우 알림 메시지(메일, SMS 등) 발송이 가능해야 한다. (알림 메일 설정)

EDR 시스템 일반 – 환경설정(계속) 옥치해 부장

닉스테크 EDR 중 SOC Plus는 아래의 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
환경설정	라이선스	MEDIUM	제품 버전 정보	서버, 웹, 에이전트 별 제품 버전 정보를 제공해야 한다.
		LOW	라이선스 정보	적용된 라이선스 정보(라이선스 등급, 유효기간 등)를 제공해야 한다.
		LOW	라이선스 범위	적용된 라이선스 정보에 따라서 사용가능한 서비스를 제공해야 한다. (엔드포인트 수 제한, 연동가능한 시스템 수 제한 등)
		LOW	라이선스 갱신 정보	라이선스 갱신을 위한 정보를 제공해야 한다.

NAC 라이선스 관리 방안 조사

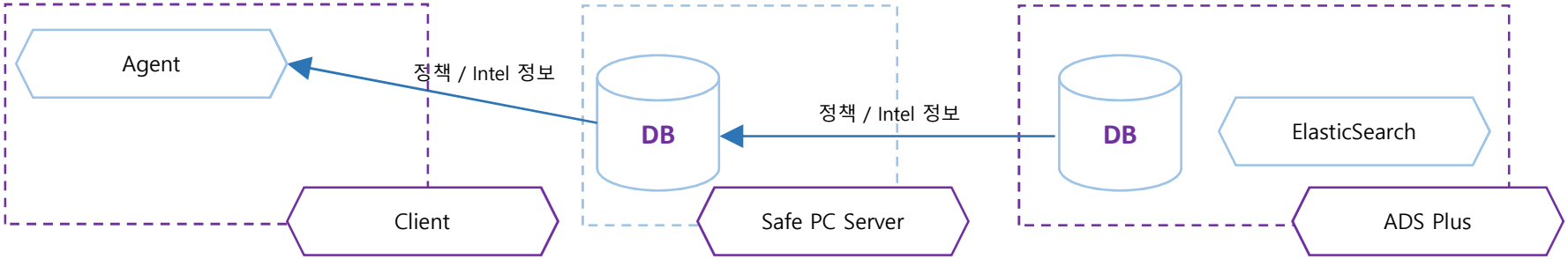
목표 대수는 농협 기준으로 조사 (8만대에 관리서버 4대)

12만유저

AP서버: 10대
DB서버: 02대 (AP 4개당 DB서버 1개)

서버 스펙 정의 필요:
(예) 1대당 15,000유저 커버

EDR 시스템 보안관리 – 보안관리 옥치해 부장

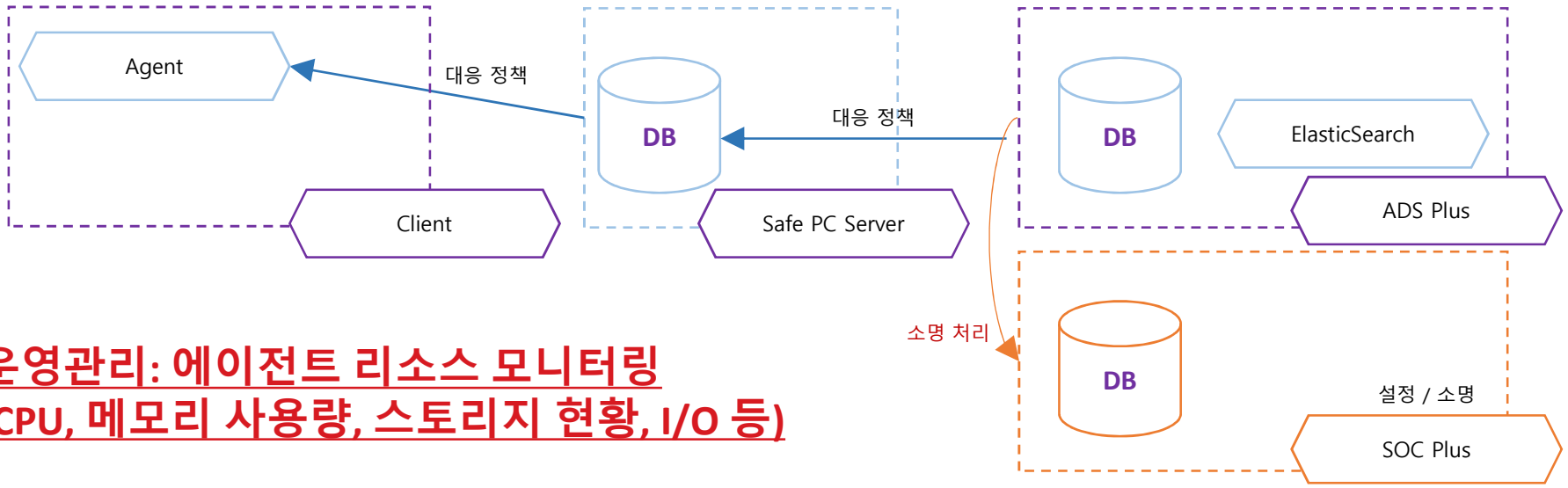


ADS Plus의 보안정책은 Safe PC Server에 전송되고, Safe PC Server의 정책은 클라이언트에 적용되어야 한다.
단, 시나리오 정보는 클라이언트에 전송되지 않고, 시나리오 탐지 후 생성/수정/삭제된 정책 정보만 클라이언트에 적용된다.

Cat.2	Cat.3	Priority	Requirement	Detail
보안관리	보안정책	HIGH	기본정책	모든 대상에게 기본적으로 적용되는 정책이 존재해야 한다.
		HIGH	적용대상: 대상	엔드포인트, 사용자, 부서, 직급, IP 그룹 등으로 정책 적용이 가능해야 한다. (대상 결정 필요)
		HIGH	적용대상: 우선순위	사용자 > 엔드포인트 > IP 그룹 > 직급 > 부서 > 기본 (우선순위 결정 필요)
		HIGH	적용기간	적용 정책별로 기간 설정이 가능해야 한다.
		HIGH	Intel 탐지: 설정	적용할 Intel 그룹, 개별 Intel 등을 설정할 수 있어야 한다.
		HIGH	Intel 탐지: 적용	특정 대상에 설정된 Intel 정책을 적용할 수 있어야 한다.
		HIGH	Intel 탐지: 대응	탐지 항목에 따라 설정된 대응 정책을 적용할 수 있어야 한다.

EDR 시스템 보안관리 – 보안관리 (계속)

옥치해 부장

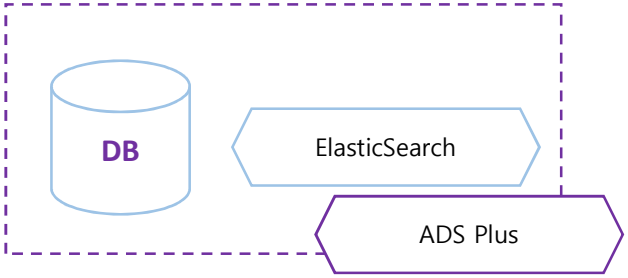


운영관리: 에이전트 리소스 모니터링 (CPU, 메모리 사용량, 스토리지 현황, I/O 등)

Cat.2	Cat.3	Priority	Requirement	Detail
보안관리	보안정책	HIGH	대응 정책	대응 정책은 특정 위협이 탐지 되었을 때, 실행되는 보안 정책이다.
		HIGH	대응 정책 설정: 매체제어	매체 항목의 차단, 허용 등을 설정할 수 있어야 한다.
		HIGH	대응 정책 설정: 프로세스	탐지된 프로세스를 삭제, 종료 설정을 할 수 있어야 한다.
		HIGH	대응 정책 설정: 어플리케이션	악성/금지 어플리케이션을 삭제 할 수 있어야 한다.
		HIGH	대응 정책 설정: 네트워크	네트워크를 격리하거나 차단 할 수 있어야 한다.
		HIGH	대응 정책 설정: 레지스트리	레지스트리를 삭제할 수 있어야 한다.
		HIGH	대응 정책 설정: 파일	주요 문서 파일 등이 발견, 유출 등의 이상행위 탐지되었을 때, 파일을 암호화, 삭제, 유출 차단 할 수 있어야 한다.
		HIGH	대응 정책 설정: 시스템	시스템을 종료 할 수 있어야 한다.
		HIGH	대응 정책 설정: 자동/수동/소명	탐지된 룰에 따라 자동으로 대응 정책을 자동으로 적용할지, 모니터링만 할지, 소명 절차를 진행할지를 설정할 수 있어야 한다.

EDR 시스템 보안관리 – 보안관리 (계속)

옥치해 부장
허순구 부장 (시나리오 관리)



정책의 반응시간 우선순위 설정 가능? (실시간 적용?)

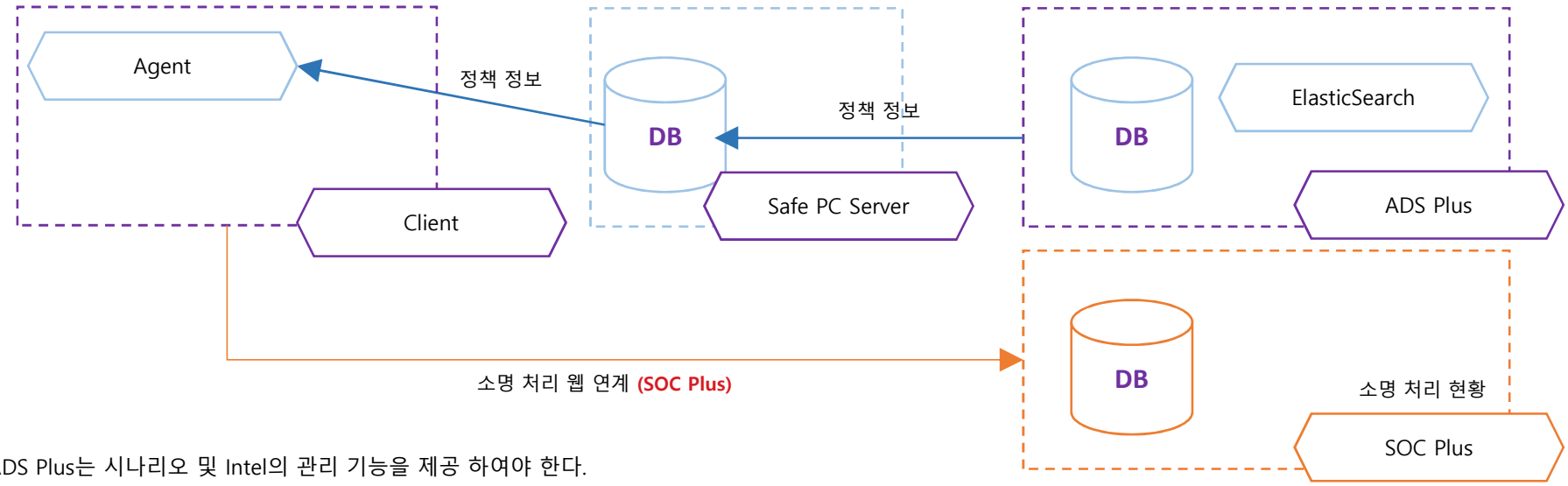
ADS Plus는 시나리오 및 Intel의 관리 기능을 제공 하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
보안관리	시나리오 관리	HIGH	시나리오 생성	사용자, 엔드포인트 등 각 개체의 행위와 시간 등의 조건으로 위협을 탐지할 수 있는 시나리오 생성이 가능해야 한다.
	시나리오 관리	HIGH	시나리오 라벨	위협 탐지 룰을 관리자의 정의에 따른 라벨로 카테고리화 할 수 있어야 한다.
	Intel 관리	HIGH	지원 Intel 형태	OpenIOC, YARA, STIX, 평판정보(Virus-Total 등 연동), 자체포맷 …
	Intel 관리	HIGH	Intel 구성요소	해시값, 파일명, 도메인 값, 레지스트리 값, IP 주소, 프로세스 정보 등
	Intel 관리	HIGH	Intel 리스트	현재 Intel 현황 정보를 표시할 수 있어야 한다. (전체 Intel 수, 각 Intel 내용, 추가 주체: 시스템, 외부 연동, 관리자 등)
	Intel 관리	HIGH	Intel 구분	각 Intel의 형태, 카테고리, 추가 유형 등을 구분할 수 있어야 한다.
	Intel 관리	HIGH	Intel 추가: 파일 불러오기	OpenIOC, STIX, YARA 등 형태 파일을 읽어와서 추가할 수 있어야 한다.
	Intel 관리	HIGH	Intel 추가: 외부 연동	외부 시스템 연동을 통해 Intel DB를 업데이트 할 수 있어야 한다.
	Intel 관리	HIGH	Intel 추가: 수동 입력	OpenIOC, STIX, YARA 등의 형태로 관리자가 직접 인력하여 추가할 수 있어야 한다.
	Intel 관리	HIGH	Intel 추가: 중복 조회	신규로 추가하는 Intel에 기존에 존재하는 인텔인지 검증해야 한다.
	Intel 관리	HIGH	Intel 추가: 오류 탐지	수동 입력 등으로 추가한 Intel이 잘못된 형식일 경우 탐지하여 추가를 차단할 수 있어야 한다. (XML 문법 오류 등)
	Intel 관리	HIGH	Intel 그룹	특정 Intel을 그룹화하여 저장 할 수 있어야 한다. (카테고리별, 형태별 등)
	Intel 관리	HIGH	Intel 수정/삭제	Intel의 수정/삭제가 가능해야 한다.
	Intel 관리	HIGH	Intel 파일 생성	전체 혹은 개별 Intel, 그리고 설정한 Intel 그룹을 엔드포인트에 적용하기 위한 하나의 Intel File로 생성할 수 있어야 한다.
	Intel 관리	HIGH	Intel 실시간 스캔	특정 Intel을 에이전트에 즉시 배포하고, 스캔하고 결과를 받을 수 있어야 한다.

Intel 부분집합 활용

EDR 시스템 보안관리 – 보안관리 (계속)

허순구 부장 (추후)

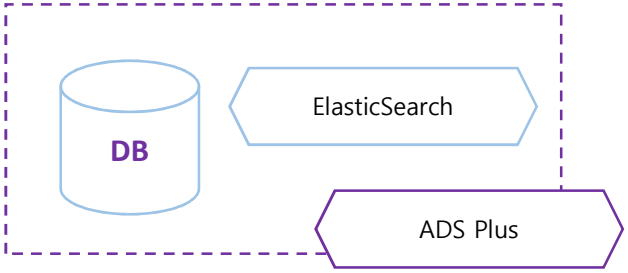


ADS Plus는 시나리오 및 Intel의 관리 기능을 제공 하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
보안관리	AI 보안 (ADS)	LOW	베이스라인 설정: 프로파일링	사용자, 엔드포인트 별로 데이터 사용량, 프로세스 사용 정보들을 일정기간 학습하여 기준을 설정할 수 있어야 한다.
		LOW	머신러닝: 위협 모델	추후 조사/정리 필요
		LOW	보안정책 자동 생성	탐지된 룰에 따라 자동으로 대응 정책을 생성하는 기능을 제공해야 한다. (추후 조사/정리 필요)
	위협 등급 관리	LOW	엔드포인트 위협 등급	추후 조사/정리 필요
	소명처리 (SOC)	HIGH	자동소명 처리 설정	에이전트에서 자동 처리된 소명에 대한 조회 / 수정 / 삭제 / 프로세스 단계 표현 (SOC 참고 후 정리 필요)
		HIGH	수동소명 처리 설정	에이전트에서 수동 처리된 소명에 대한 조회 / 수정 / 삭제 / 프로세스 단계 표현 (SOC 참고 후 정리 필요)

EDR 시스템 분석조사 – 통합검색

이용권 이사



ADS Plus는 Agent로 부터 수집된 데이터 기반으로 아래의 통합검색 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
분석조사	통합검색	HIGH	검색: 통합검색	엔드포인트, 프로세스, 사용자, 레지스트리, 프로토콜 등으로 검색하여 해당 정보를 한 화면에서 조회할 수 있어야 한다.
		HIGH	검색: 통합검색 예 1	프로세스로 검색 시, 해당 프로세스가 동작 중인 모든 엔드포인트를 조회할 수 있다.
		HIGH	검색: 통합검색 예 2	특정 레지스트리 값을 검색 시, 해당 레지스트리 값이 존재하는 모든 엔드포인트를 조회할 수 있다.
		HIGH	검색: 결과내 재검색	검색 결과 내에서 특정 검색어로 검색이 가능해야 한다.
		HIGH	필터 1: 카테고리	카테고리(부서, 컴퓨터 그룹 등) 별 필터를 제공해야 한다.
		HIGH	필터 2: 키워드	특정 키워드를 포함 혹은 포함하지 않는 정보를 필터하는 기능을 제공해야 한다.
		HIGH	기본 표시 정보	엔드포인트, 사용자, 프로세스 정보를 기본으로 표시하고, 그 외에 검색에 부합하는 데이터를 표시해야 한다.
		HIGH	드릴다운	조회된 데이터에서 클릭하는 값(엔드포인트, 사용자, 프로세스 등)에 따라 상세정보로 드릴다운 하는 기능을 제공해야 한다.

EDR 시스템 분석조사 – 상세분석

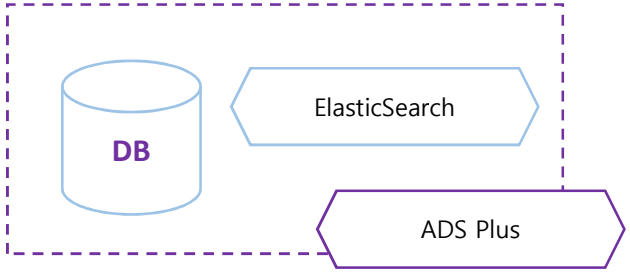
이용권 이사

ADS Plus는 Agent로 부터 수집된 데이터 기반으로 아래의 상세분석 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
분석조사	상세분석	HIGH	사용자 분석 1: 기본정보	사용자 기본 정보와 로그인, 로그아웃 정보를 제공한다.
		HIGH	사용자 분석 2: 엔드포인트	사용자가 로그인, 로그아웃한 엔드포인트 정보를 모두 제공한다. (다수가 될 수 있음)
		HIGH	사용자 분석 3: 타임라인	사용자가 로그인, 로그아웃한 시점까지 엔드포인트에서 수행한 행위 정보를 타임라인 분석으로 제공한다.
		HIGH	사용자 분석 4: 드릴다운	엔드포인트 선택 시, 엔드포인트 상세분석으로 드릴다운 기능을 제공한다.
		HIGH	엔드포인트 분석 1: 기본정보	엔드포인트의 정적 정보를 제공한다. (고유값, OS, 설치 프로그램(필수/금지 표시), CPU 메모리 정보 등)
		HIGH	엔드포인트 분석 2: 프로세스	엔드포인트에서 동작중인 모든 프로세스를 리스트를 제공한다.
		HIGH	엔드포인트 분석 3: 네트워크	맥 주소, IP 주소, DNS 주소, 호스트네임 및 오픈된 포트 정보를 제공한다.
		HIGH	엔드포인트 분석 4: 레지스트리	엔드포인트의 레지스트리 정보를 제공한다.
		HIGH	엔드포인트 분석 5: 타임라인	엔드포인트가 시작되고 종료될때까지 수행한 행위 정보를 제공한다. (접속 사용자, 실행 프로세스, 변경 레지스트리 및 파일 등)
		HIGH	엔드포인트 분석 6: 드릴다운	프로세스 선택 시, 프로세스 상세분석으로 드릴다운 기능을 제공한다.
		HIGH	프로세스 분석 1: 기본정보	평판정보, 전자서명, 배포자, 버전, 파일 해시, 시작 시간, 종료 시간, 프로세스&세션 ID, 생성/수정 일자 등을 제공한다.
		HIGH	프로세스 분석 2: 관련 엔드포인트	해당 프로세스와 동일한 프로세스(해시비교)가 동작하고 있는 모든 엔드포인트 정보 (수로 표시)
		HIGH	프로세스 분석 3: 하이러키	프로세스의 부모, 자식 프로세스, 라이브러리, 소유 엔드포인트, 사용자 정보, 등을 제공한다.
		HIGH	프로세스 분석 4: 상세정보	관련 파일시스템, 네트워크 접속 유무, 아웃바운드 커넥션 정보, 인젝션 행위 등의 정보를 제공한다.
		HIGH	프로세스 분석 5: 타임라인	시작해서 종료하는 시점까지 수행한 행위를 타임라인 분석으로 제공한다. (접근 파일, 네트워크 사용 여부, 레지스트리 등)
		HIGH	프로세스 분석 6: 드릴다운 1	파일 선택 시, 해당 파일 상세분석으로 드릴다운을 지원한다.
		HIGH	프로세스 분석 7: 드릴다운 2	부모, 자식 프로세스 선택 시, 해당 프로세스 상세분석으로 드릴다운을 진행한다.
		HIGH	파일 분석 1: 기본 정보	파일의 해시값, 소유자, 생성/수정일 등의 기본 정보를 제공한다.
		HIGH	파일 분석 2: 타임라인 분석	파일의 생성부터 소멸(혹은 현재)까지 접근한 프로세스, 파일 변경 내용 등을 타임라인 분석으로 제공한다.
		HIGH	파일 분석 3: 흐름분석	파일 라이프사이클 및 타 엔드포인트로의 이동 등을 상태 다이어그램을 추적하는 기능을 제공한다.
		HIGH	위협 라벨링	상세분석 결과에서 발견된 특정 프로세스, 행위(특정 네트워크 접속) 등을 위협 행위로 라벨링 하는 기능을 제공해야 한다.
		HIGH	위협 탐지 표시	위협으로 탐지된 항목에는 위협 행위라고 자동으로 표시되어야 한다.
		HIGH	위협 탐지 대응	관리자가 분석 도중 위협을 발견할 경우 해당 실시간 대응을 수동으로 할 수 있는 기능을 제공해야 한다.

EDR 시스템 모니터링 – 설정

이용권 이사



ADS Plus는 모니터링 화면(대시보드)을 위해 아래의 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
모니터링	설정	MEDIUM	기본 환경설정	모니터링의 데이터 갱신 주기 등을 설정할 수 있어야 한다.
		MEDIUM	시간	모니터링 데이터의 최근 업데이트 시간 및 현재 시간을 제공해야 한다.
		MEDIUM	탭 구성	모니터링을 카테고리별로 확인할 수 있도록 탭으로 구성하는 기능을 제공해야 한다.
		MEDIUM	탭 개인화	관리자별로 설정한 모니터링 탭을 저장하고, 삭제할 수 있어야 한다. 타 관리자에게는 비공개로 설정할 수 있어야 한다.
		MEDIUM	탭 생성/수정/삭제 지원	모니터링 탭을 관리자가 추가하고, 수정하고, 삭제할 수 있어야 한다. 또한 탭 생성 시 명칭을 설정할 수 있어야 한다.
		MEDIUM	탭 구성 설정	지원되는 모니터링 컴포넌트를 관리자가 신규 생성 탭 혹은 기존의 탭에 추가/삭제/수정 등 설정할 수 있어야 한다.
		MEDIUM	컴포넌트 위치와 크기 설정	관리자가 탭 내의 모니터링 컴포넌트의 위치와 크기를 조절할 수 있어야 한다. (최소 크기는 고정)
		MEDIUM	컴포넌트 상세 설정	모니터링 컴포넌트가 상세 설정 기능을 지원할 경우, 설정의 변경이 가능해야 한다. (예. 통계 기간 변경: 일, 주, 월 등)
		MEDIUM	컴포넌트 드릴다운 1	각 모니터링 항목에서 3 Depth 드릴다운을 지원해야 한다. (그래프 혹은 통계 -> Top N (혹은 대상) -> Raw Data 등)
		MEDIUM	컴포넌트 드릴다운 2	모니터링 컴포넌트에서 드릴다운이 어려울 경우 분석조사 항목으로 이동해서 쿼리 혹은 검색 할 수 있어야 한다.

EDR 시스템 모니터링 – 시스템 정보

허순구 부장
권혁재

ADS Plus는 아래의 시스템 정보 모니터링 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
모니터링	시스템 정보	MEDIUM	제품 서버 시스템 상태	제품 서버 시스템의 상태를 모니터링 할 수 있어야 한다. (CPU, 메모리 상태 등)
		MEDIUM	제품 서버 서비스 상태	제품 서버에서 동작하는 주요 서비스(데몬)의 온/오프 상태를 모니터링 하는 기능을 제공해야 한다.
		MEDIUM	데이터베이스 기본 상태	응답시간, CPU 사용량, 메모리 사용량 등을 모니터링 할 수 있어야 한다.
		MEDIUM	데이터베이스 커넥션 정보	데이터베이스의 커넥션 통계 정보를 시계열 그래프로 제공해야 한다.
		MEDIUM	다중 구성 상태 지원	제품 서버 및 스토리지 등이 다수로 도입된 경우에는 다수의 서버 시스템/서비스 상태를 모니터링 하는 기능을 제공해야 한다.
		MEDIUM	외부 연동 제품 상태	자사/타사 보안 제품, 로그 수집 대상 서버/제품 등 연동되어 있는 시스템의 연결 상태를 모니터링 하는 기능을 제공해야 한다.
		MEDIUM	네트워크 트래픽 상태	서버로 유입되는 네트워크 트래픽 추이를 시계열 그래프로 제공해야 한다. (전체 트래픽 추이, 엔드포인트 별 Top N)
		MEDIUM	전체 사용자 수	전체 사용자 수를 표시할 수 있어야 한다.
		MEDIUM	접속 사용자 수	현재 접속한 사용자 수를 표시할 수 있어야 한다. (인증한 사용자)
		MEDIUM	전체 엔드포인트 수	전체 엔드포인트 수를 표시할 수 있어야 한다. (에이전트 설치 불가 엔드포인트 포함)
		MEDIUM	접속 엔드포인트 수	현재 접속한 엔드포인트 수를 표시할 수 있어야 한다.
		MEDIUM	전체 엔드포인트 OS 통계	전체 엔드포인트의 OS 정보 통계를 제공할 수 있어야 한다. (Windows, Linux, Mac OS, AOS, iOS 등)
		MEDIUM	접속 엔드포인트 OS 통계	현재 접속한 엔드포인트의 OS 정보 통계를 제공할 수 있어야 한다.
		MEDIUM	전체 에이전트 설치 가능 엔드포인트 수	전체 엔드포인트 중 에이전트가 설치 가능한 엔드포인트의 수를 표시할 수 있어야 한다.
		MEDIUM	전체 에이전트 설치 엔드포인트 수	전체 에이전트 설치 가능 엔드포인트 중 에이전트가 설치가 설치된 엔드포인트의 수를 표시할 수 있어야 한다.
		MEDIUM	무결성이 훼손된 엔드포인트 수	전체 에이전트가 설치된 엔드포인트 중 무결성이 훼손된 엔드포인트의 수를 표시할 수 있어야 한다.
		MEDIUM	제품 구성요소 버전 상태	제품의 구성요소 버전을 표시할 수 있어야 한다. (제품 서버를 다수 사용 시, 각 제품 서버 서비스의 구성요소 버전 표시)
		MEDIUM	에이전트 버전별 배포 상태	엔드포인트에 설치된 에이전트 버전별 통계를 모니터링할 수 있어야 한다.
		MEDIUM	라이선스 상태	라이선스 유효성 여부를 확인할 수 있어야 한다.

허순구 부장
권혁재

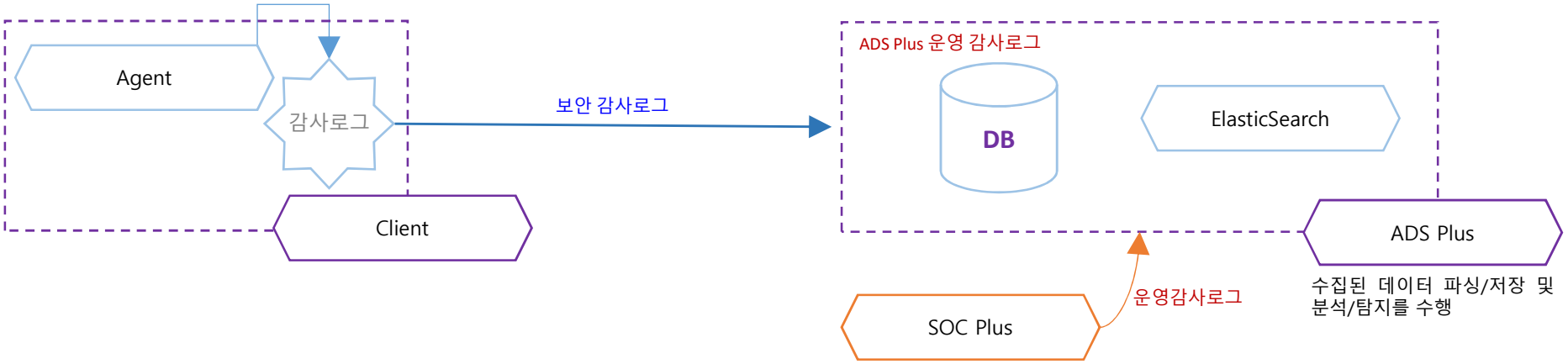
EDR 시스템 모니터링 – 데이터 수집정보 / 보안위협정보 및 대응

ADS Plus는 에이전트로부터 수집된 데이터 수집 정보와 Intel/시나리오/시그니처 등의 보안위협정보 및 대응정보를 모니터링 할 수 있는 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
모니터링	데이터 수집 정보	MEDIUM	스토리지 정보 및 상태	데이터가 수집 저장되는 스토리지의 정보 및 상태를 모니터링 하는 기능을 제공해야 한다.
		MEDIUM	수집 데이터량	실시간으로 수집되는 데이터의 량을 시계열 그래프로 모니터링 하는 기능을 제공해야 한다.
		MEDIUM	수집 데이터량 세분화	수집되는 데이터의 소스에 따라서 유입되는 데이터량을 세분화하여 표시할 수 있어야 한다.
		MEDIUM	수집 대상 정보	현재 데이터를 수집하는 대상의 종류 및 접속 통계를 제공해야 한다. (예. Agent 100대 연결중, 연동 서버 2대 연결중 등)
		MEDIUM	수집 데이터 처리 속도	수집되는 데이터 처리 속도를 초, 분 등의 단위로 제공해야 한다.
	보안위협정보	MEDIUM	Intel 수	지원하는 Intel 수를 제공해야 한다.
		MEDIUM	Intel 형태별 비율	지원하는 Intel의 형태별 비율을 파이 그래프로 제공해야 한다.
		MEDIUM	Intel 형태별 수	지원하는 Intel 항목별 수를 제공해야 한다.
		MEDIUM	시그니처 데이터 수	연동된 정보 혹은 자체제공 DB의 시그니처 데이터 수 제공해야 한다.
		MEDIUM	보안 위협 점수	엔드포인트별 보안 위협 점수를 합산하여 전체 조직의 보안 위협 점수를 산정할 수 있어야 한다. (연구 필요)
		MEDIUM	보안 위협 점수 Top N	엔드포인트 중 보안 위협 점수가 높은 Top N의 정보를 표시해야 한다.
		MEDIUM	보안 위협 항목 별 비율	보안 위협으로 정의된 항목들 별로 발견된 비율을 파이 그래프로 제공해야 한다.
		HIGH	실시간 탐지 위협 모니터링	실시간으로 탐지되는 위협에 대해 모니터링 컴포넌트로 제공해야 한다.
		HIGH	위협 탐지 추이	위협 탐지 추이를 시계열 그래프로 제공해야 한다.
		HIGH	위협 탐지 건수	위협 탐지 건수를 제공해야 한다. (일, 주, 월 통계)
		HIGH	위협 탐지 건수: 위치별	엔드포인트의 위치별로 탐지된 위협의 건수를 MAP으로 제공해야 한다. (다수의 지역에 사무실이 있는 경우)
		HIGH	위협 탐지 엔드포인트 Top N	위협이 탐지된 엔드포인트 중 Top N의 정보를 표시해야 한다.
		HIGH	위협 탐지 사용자 Top N	위협이 탐지된 사용자 중 Top N의 정보를 표시해야 한다.
		HIGH	위협 탐지 모니터링 드릴다운	위협이 탐지된 특정 항목을 선택 시, 상세분석으로 드릴다운 기능을 제공해야 한다.
		MEDIUM	시그니처 탐지 추이	시그니처 탐지 추이를 시계열 그래프로 제공해야 한다.
		MEDIUM	시그니처 탐지 건수	시그니처 탐지 건수를 제공해야 한다. (일, 주, 월 통계)
		MEDIUM	시그니처 탐지 엔드포인트 Top N	시그치처로 탐지된 엔드포인트 중 Top N의 정보를 표시해야 한다.
		MEDIUM	시그니처 탐지 사용자 Top N	시그치처로 탐지된 사용자 중 Top N의 정보를 표시해야 한다.
		MEDIUM	사용 프로세스 Top N	전체 조직에서 사용중인 프로세스 별 Top N 정보를 제공해야 한다.
		MEDIUM	발견된 전체 위협 프로세스 건수	발견된 전체 위협 프로세스 건수를 제공해야 한다.
		MEDIUM	감염된 엔드포인트 건수	발견된 위협 프로세스에 감염된 엔드포인트 건수를 제공해야 한다.
		MEDIUM	C&C 통신 엔드포인트 건수	C&C 서버와 통신한 엔드포인트의 건수를 제공해야 한다.
	대응	MEDIUM	SOC	SOC 관련 전체 티켓, 처리 티켓 건수, 지연 건수 등은 SOC 모니터링 대시보드 항목에 따른다.
		MEDIUM	대응(통제) 건수: 전체 통계 그래프	대응(통제) 종류 별 건수를 파이 그래프로 제공해야 한다.
		MEDIUM	대응(통제) 건수: 전체 통계 수	대응(통제) 종류 별 건수를 제공해야 한다.
		MEDIUM	대응(통제) 건수: 전체 추이	대응(통제) 전체 추이를 시계열 그래프로 제공해야 한다.
		MEDIUM	대응(통제) 건수: 개별 통계	각 대응 종류 별 건수를 제공해야 한다. (데이터 유출 차단, 프로세스 차단, 프로세스 삭제 등)
		MEDIUM	대응(통제) 건수: 개별 추이	각 대응 종류 별 추이를 시계열 그래프로 제공해야 한다. (데이터 유출 차단, 프로세스 차단, 프로세스 삭제 등)

EDR 시스템 감사로그 – 설정 및 부가기능

장욱 부장
옥치해 부장



ADS Plus는 클라이언트로부터 전송 받은 보안 감사로그와 시스템 운영 감사로그와 관련하여 아래의 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
감사로그	설정 및 부가기능	MEDIUM	개인정보 마스킹	로그에서 확인 가능한 개인정보는 ** 마스킹 처리해야 한다. (내용, 파일명 등에 포함된 개인정보)
		MEDIUM	감사데이터 출력	조회/검색된 데이터 Export 가 가능해야 한다. (excel, txt, csv, pdf)
		MEDIUM	감사데이터 내용	사건 발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원, 작업 내역 및 결과(성공/실패)를 상세히 포함해야 한다.
		MEDIUM	감사데이터 표시	감사데이터 조회 결과 값은 그래프와 결과값 표로 표시된다.
		MEDIUM	감사데이터 조회 조합	관리자가 정보를 해석하기 적합하도록 감사 레코드가 생성되어야 하며 AND, OR 등 논리적 관계 기준에 따른 석택적 검토 필요
		MEDIUM	감사데이터 검색 조건 1	조회/검색 조건이 저장되어 재사용가능하게 한다.
		MEDIUM	감사데이터 검색 조건 2	IP, 이름, ID 등 로그 필드 별 조건을 주어 검색하며 TopN 조건도 줄 수 있다.
		MEDIUM	감사데이터 시간	에이전트, 서버 시간이 다를 경우를 대비하여 에이전트에서 로그를 전송한 시간과 서버에 로그를 기록한 시간을 기록해야 한다.
	감사증적	MEDIUM	감사증적 초과 알림메일	감사증적의 크기가 지정된 한도를 초과할 경우, 관리자에게 통보해야 한다. (알림메일 및 감사로그 생성)
		MEDIUM	감사증적 포화 대응	감사증적의 포화시 적절한 방법(오래된 감사 레코드 덮어쓰기 등)으로 저장 실패에 대응해야 한다. (검토필요)
		MEDIUM	경보 메시지 발송	잠재적인 보안 위반을 탐지한 경우, 인가된 관리자가 설정한 대응행동을 수행할 수 있어야 한다.

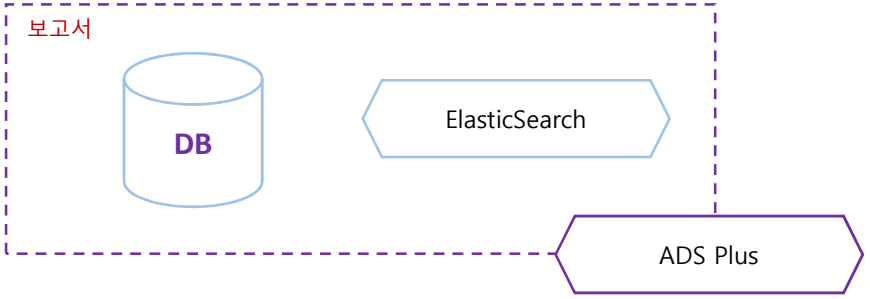
EDR 시스템 감사로그 – 운영 및 보안 감사로그

장욱 부장
옥치해 부장

ADS Plus는 클라이언트로부터 전송 받은 보안 감사로그와 시스템 운영 감사로그와 관련하여 아래의 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
감사로그	운영 감사로그	MEDIUM	식별 및 인증 로그	관리자, 사용자, 단말의 식별 및 인증 로그를 생성/조회 가능해야 한다. (로그인, 로그아웃, 비정상 아이디 로그인, 비밀번호 오류 횟수 초과, 비밀번호 오류)
		MEDIUM	관리자 운영 로그	관리자별 웹 콘솔 접근 내역을 생성/조회 가능해야 한다. (접속 페이지, 행위 등)
		MEDIUM	정책설정 변경 히스토리	관리자가 변경한 정책설정 정보를 제공해야 한다. 이전 정책설정, 변경된 정책설정을 비교할 수 있어야 한다.
		MEDIUM	관리설정 변경 히스토리	관리자가 변경한 관리설정 정보를 제공해야 한다. 이전 관리설정, 변경된 관리설정을 비교할 수 있어야 한다.
		MEDIUM	시스템 상태 로그	서버/데몬 상태(시작/중지) 로그, 감사증적관리(사용 임계치 초과, 로그 백업, 알림 내역 등) 로그를 생성/조회 가능해야 한다.
		MEDIUM	무결성 점검 로그	서버 및 에이전트 설정 및 파일의 무결성 점검 결과 로그 (성공/실패, 실패 시 무결성이 훼손된 항목들 내역)
	보안 감사로그	HIGH	위협 탐지 로그: Intel 탐지	Intel로 탐지된 위협을 로그로 기록하고 조회할 수 있어야 한다.
		HIGH	위협 탐지 로그: 룰 탐지	보안 위협 룰로 탐지된 위협을 로그로 기록하고 조회할 수 있어야 한다.
		HIGH	위협 탐지 로그: AI 보안 탐지	Intel로 탐지된 위협을 로그로 기록하고 조회할 수 있어야 한다.
		HIGH	탐지 대응 로그: 매체제어	탐지된 위협에 따라 대응한 로그를 기록한다.
		HIGH	탐지 대응 로그: 프로세스 제어	탐지된 위협에 따라 대응한 로그를 기록한다.
		HIGH	탐지 대응 로그: 레지스트리 삭제	탐지된 위협에 따라 대응한 로그를 기록한다.
		HIGH	탐지 대응 로그: 네트워크	탐지된 위협에 따라 대응한 로그를 기록한다.
		HIGH	탐지 대응 로그: 파일	탐지된 위협에 따라 대응한 로그를 기록한다.
		HIGH	탐지 대응 로그: 시스템	탐지된 위협에 따라 대응한 로그를 기록한다.

EDR 시스템 보고서 – 설정 및 보고서 관리

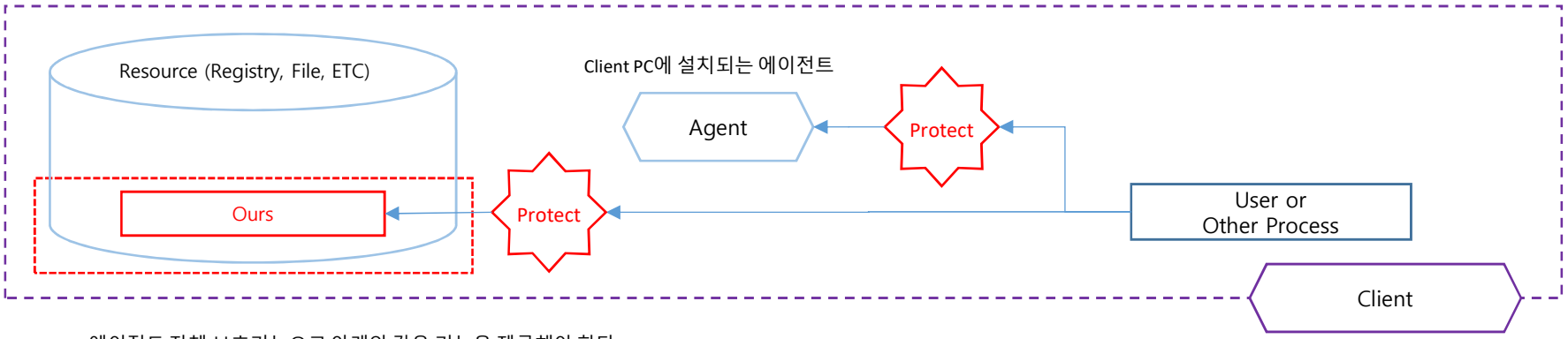


ADS Plus는 아래의 보고서 생성 기능을 제공하여야 한다.

Cat.2	Cat.3	Priority	Requirement	Detail
보고서	설정	MEDIUM	보고서 예약	리포트 종류 설정 및 예약설정을 통한 통계 결과 저장 한번, 주기적, 시간 등을 설정할 수 있어야 한다.
		MEDIUM	보고서 형태	리포팅 유형(기본템플릿, 사용자정의, 상세 통계 등)
	보고서 관리	MEDIUM	위협 탐지 보고서	기간별 탐지된 위협 건수, 추이, 위협의 종류 등을 보고서로 제공한다. (상위 탐지 사용자, 엔드포인트 정보를 포함한다.)
		MEDIUM	관리 정보 보고서	전체 엔드포인트, 에이전트 설치 엔드포인트, 미관리 엔드포인트, 사용자 정보, 설치 프로그램 Top N 등을 보고서로 제공한다.
		MEDIUM	사용자 정의 보고서	모니터링 컴포넌트를 추가하여 보고서를 생성하는 기능을 제공한다.

AGENT – 보호

장욱 부장

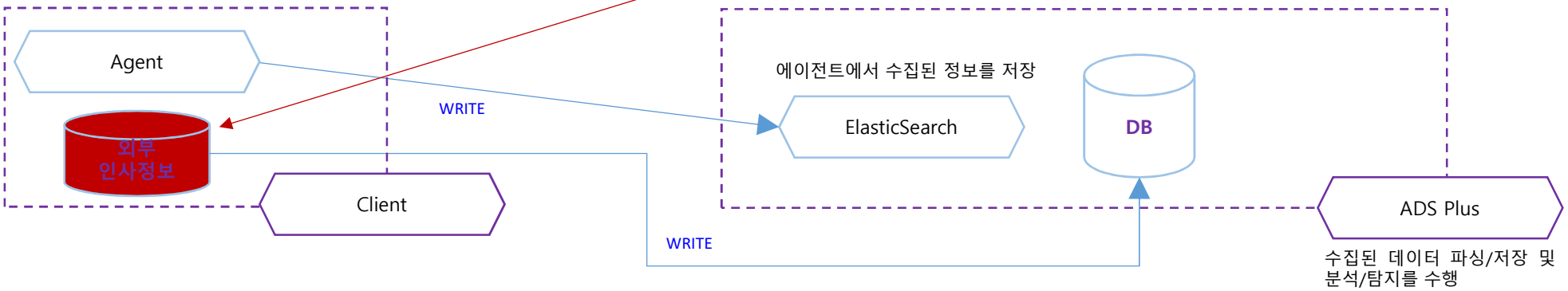


에이전트 자체 보호기능으로 아래와 같은 기능을 제공해야 한다.

Cat.2	Cat.3	Priority	Requirement
보호	기밀성	HIGH	레지스트리 정보 보호: 접근통제
		HIGH	레지스트리 정보 보호: 암호화
		HIGH	파일시스템 정보 보호: 접근통제
		HIGH	파일시스템 정보 보호: 암호화
		HIGH	암호화키 관리
		HIGH	제품 설정 값 및 정책 파일 보호
		HIGH	암호화 알고리즘
	무결성	HIGH	무결성 점검: 일반모드
		HIGH	무결성 점검: 안전모드
		HIGH	무결성 점검 대상
		HIGH	무결성 훼손 대응
	가용성	HIGH	프로세스 보호
		HIGH	프로세스 보호 불가 대응
		HIGH	로그 데이터 전송
	검증	MEDIUM	전자서명
		MEDIUM	전자서명 알고리즘
		MEDIUM	전자서명 검증
		MEDIUM	서버주소 검증

AGENT – 수집

허순구 부장
(내용 확인 필요)

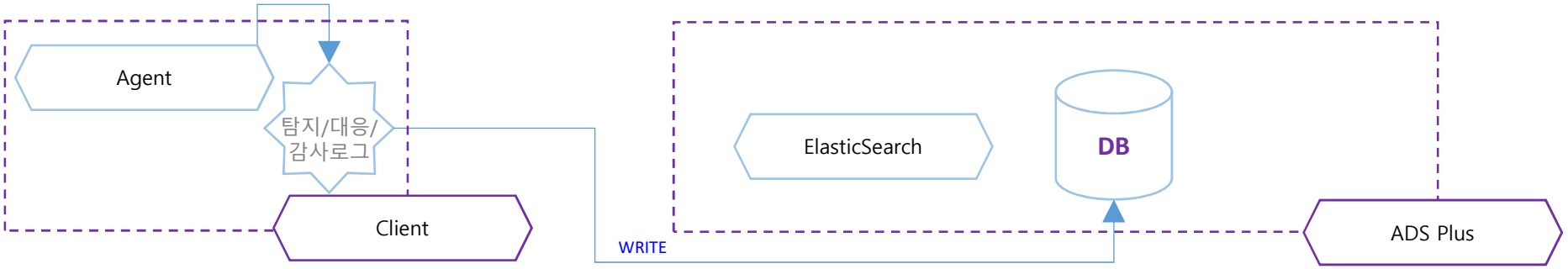


에이전트에서 수집된 정보 또는 외부 정보(ex, 인사정보)는 ADS Plus내 시스템에 저장되어야 한다.
로그 데이터는 BigData에 저장하고, 그 외 데이터는 RDB에 저장한다.

Cat.2	Cat.3	Priority	Requirement
수집	클라이언트 식별 정보	HIGH	고유식별번호
	HW 자산 정보	HIGH	하드웨어 기본
		HIGH	네트워크 정보
		HIGH	추가장치 정보
	SW 자산 정보	HIGH	운영체제 정보
		HIGH	설치 소프트웨어
		HIGH	삭제 소프트웨어
	사용자 정보	HIGH	OS 사용자
		HIGH	에이전트 사용자
	포렌식 데이터	HIGH	프로세스
		HIGH	레지스트리
		HIGH	네트워크
		HIGH	파일
		HIGH	정적/동적 정보
		HIGH	인사정보

AGENT – 수집 (탐지 / 대응 / 감사로그)

장욱 부장

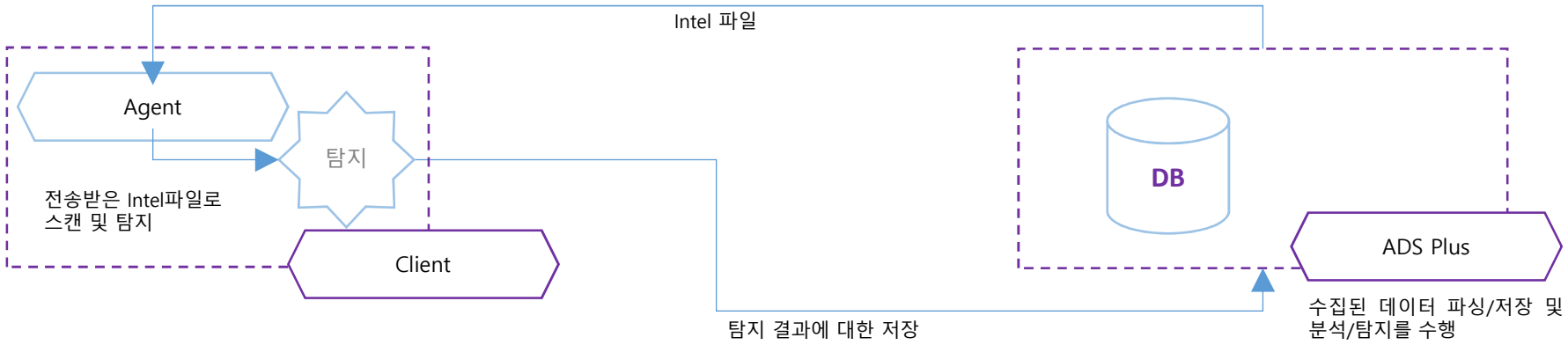


- 클라이언트에서 탐지한 위협 정보 로그를 서버로 전송해야 한다.
- 클라이언트에서 탐지한 위협에 대응한 로그를 서버로 전송해야 한다.
- 무결성 검사 결과, 사용자 로그인/로그아웃 등의 정보를 서버로 전송해야 한다.

Cat.2	Cat.3	Priority	Requirement
일반	로그	HIGH	탐지 로그
		HIGH	대응 로그
		HIGH	감사 로그

AGENT – 탐지

장욱 부장

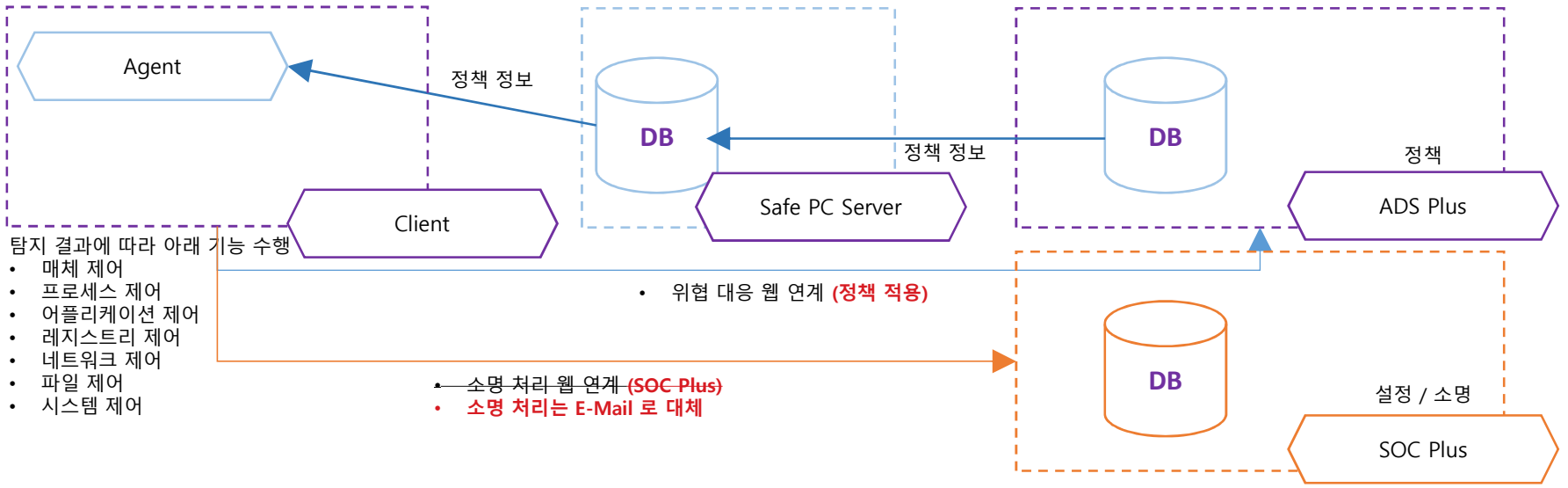


Cat.2	Cat.3	Priority	Requirement	Detail
탐지	Intel	HIGH	Intel 파일 처리	서버에서 생성하여 전송받은 InteL 파일을 처리 할 수 있어야 한다.
		HIGH	~~Intel~~ 스캔 및 탐자 Intel 정보를 통한 위협 탐지	~~Intel 파일에 따른 위협을 스캔 및 탐지하는 기능을 제공해야 한다.~~ Intel 파일에 따른 위협을 실시간 탐지 가능해야 한다
	위협모델	~~LOW~~	~~베이스라인 설정~~	~~AI 보안: 엔드포인트, 사용자 등을 기준으로 베이스라인 설정하는 기능을 제공한다.~~
		~~LOW~~	~~이상행위 탐자~~	~~AI 보안: 이상행위를 탐지하는 기능을 제공해야 한다.~~
		~~LOW~~	~~멀웨어~~	~~AI 보안: 악성코드 모델에 따라 Known, Unknown 멀웨어를 탐지하는 기능을 제공해야 한다.~~
		~~LOW~~	~~자료유출~~	~~AI 보안: 자료유출을 탐지하는 기능을 제공해야 한다.~~

AGENT – 대응

SafeNAC

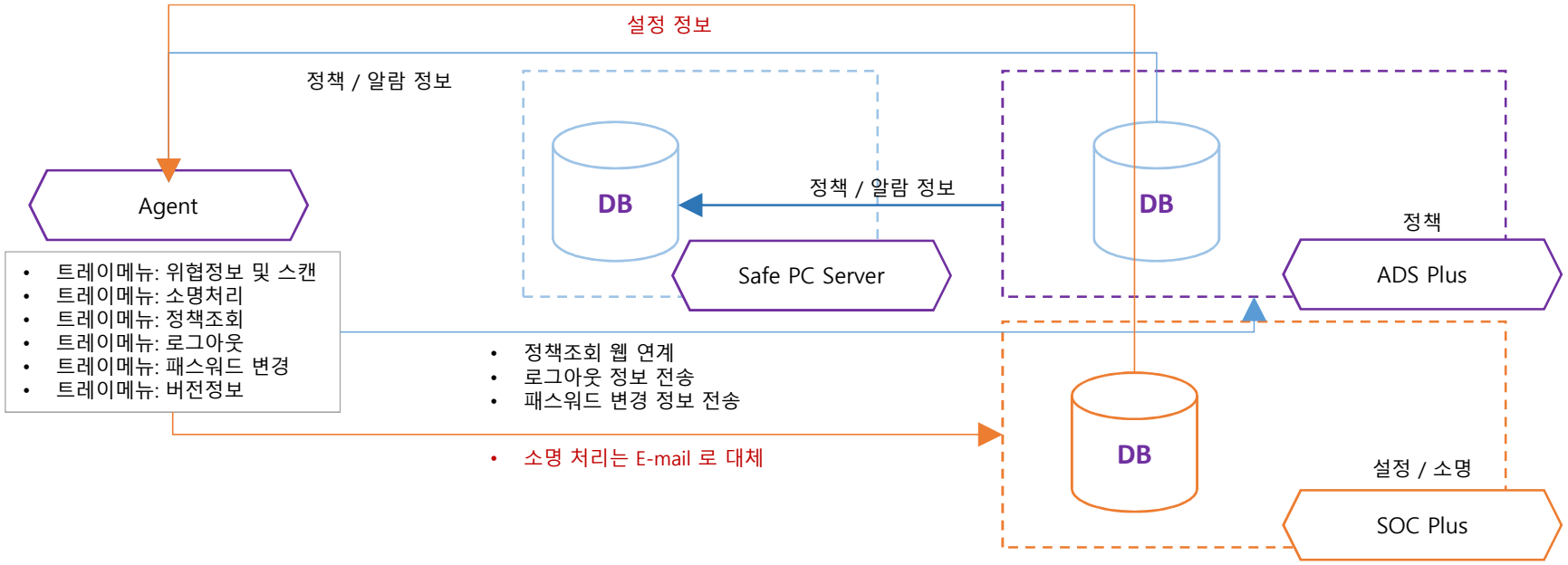
장욱 부장
신동훈 부장



Cat.2	Cat.3	Priority	Requirement	Detail
대응	자동대응	HIGH	매체제어	위협이 탐지되면 대응 정책에 따라 매체를 차단하는 기능을 제공한다.
		HIGH	프로세스	위협이 탐지되면 대응 정책에 따라 프로세스를 종료 혹은 삭제하는 기능을 제공한다.
		HIGH	어플리케이션	위협이 탐지되면 대응 정책에 따라 어플리케이션을 삭제하는 기능을 제공한다.
		HIGH	레지스트리	위협이 탐지되면 대응 정책에 따라 레지스트리를 삭제하는 기능을 제공한다.
		HIGH	네트워크	위협이 탐지되면 대응 정책에 따라 네트워크를 격리 혹은 차단하는 기능을 제공한다.
		HIGH	파일	위협이 탐지되면 대응 정책에 따라 파일을 삭제, 암호화 하는 기능을 제공한다.
		HIGH	시스템	위협이 탐지되면 대응 정책에 따라 시스템을 종료하는 기능을 제공한다.
	수동대응	HIGH	위협 대응	탐지된 위협 정보를 사용자에게 알리고, 위협을 제거(대응)할지 결정하도록 하는 기능을 제공해야 한다.
	소명처리	~~HIGH~~	~~소명처리:-수동~~	~~탐지된 이벤트에 대한 보안 관리자가 직접 소명처리 요청 프로세스 진행~~
		~~HIGH~~	~~소명처리:-자동~~	~~탐지된 이벤트에 대한 시스템에서 자동으로 원인 제공자에게 소명처리 요청 프로세스 진행~~

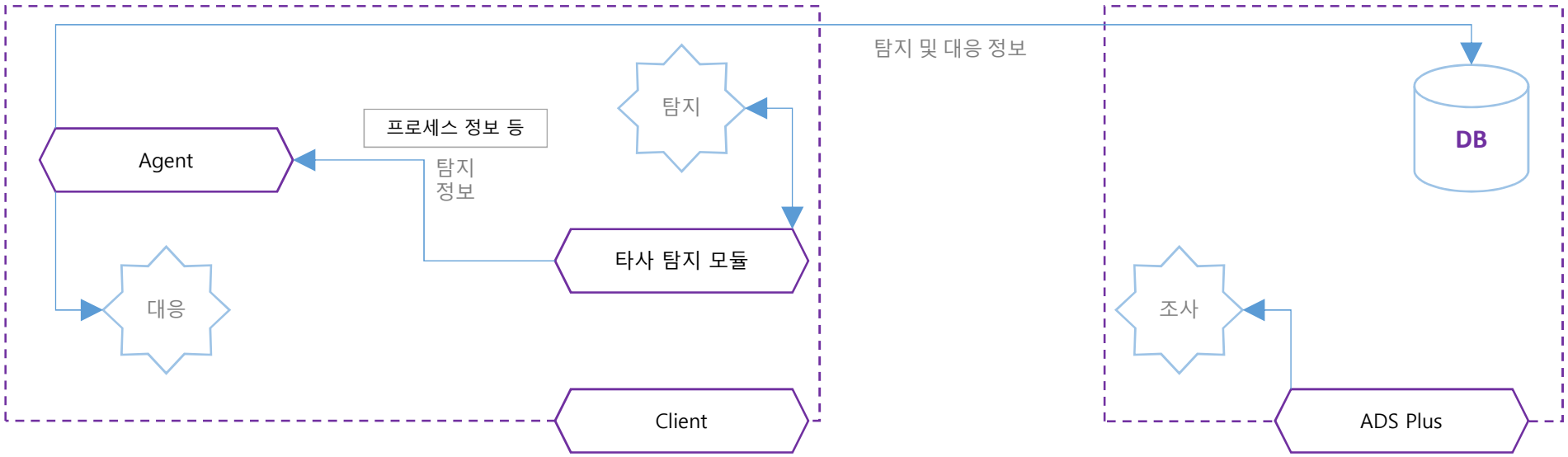
AGENT – 기타

장욱 부장



Cat.2	Cat.3	Priority	Requirement	Detail
일반	기타	HIGH	설정정보	웹에서 관리자가 설정한 로그, 정책, 모듈 업데이트 주기 등을 적용하여 동작해야 한다.
		HIGH	알림메시지	대응 정책에 따라 수행한 내용을 사용자에게 알림메시지로 알리는 기능을 제공해야 한다.
		MEDIUM	트레이메뉴: 위협정보 및 스캔	위협정보 사용자 화면을 제공하여 현재 엔드포인트에서 발견된 위협, 수동검사 기능 등을 제공해야 한다.
		~~HIGH~~	~~트레이메뉴: 소명처리~~	~~소명처리 등을 위해 에이전트 트레이메뉴에서 결재 웹 메뉴를 제공해야 한다.~~
		~~HIGH~~	~~트레이메뉴: 정책조회~~	~~현재 사용자 혹은 엔드포인트에 적용된 보안/대응 정책을 조회하는 기능을 제공해야 한다.~~
		HIGH	트레이메뉴: 로그아웃	로그아웃 기능을 제공해야 한다. (타 제품과 로그인 연동 시, 메뉴 숨김 처리)
		MEDIUM	트레이메뉴: 패스워드 변경	사용자 패스워드 변경 기능을 제공해야 한다.
		MEDIUM	트레이메뉴: 버전정보	에이전트 버전정보를 제공해야 한다.

악성코드 탐지 방안 1


탐지 및 대응 정보
탐지
프로세스 정보 등
Agent
탐지
정보
타사 탐지 모듈
대응
Client
DB
조사
ADS Plus

2. 메뉴 구성 및 정책 화면 샘플

웹(관리) 콘솔 메뉴 구성

- 모니터링
  - 메인페이지_= 대시보드
  - 조직별/사용자별 이벤트 발생현황
    - TOP X목록 및 추이 탐지
- 탐지
    - (IOC 탐지) 정책에 걸린 이벤트 목록
    - (악성?) (AI 탐지) (베이스라인) (시나리오탐지)
    - (사용자이상행위탐지) – AI탐지, 시나리오탐지
    - (기타) 단말무결성 혹은 (HW/SW) 자산의 이상 내역 – 범위 등 검토 필요
    - 다른 엔드포인트에 없는 이벤트가 나온 엔드포인트 목록
- 검색
  - 통합검색 페이지
    - 조직/사용자/앱/프로세스/파일/
      - 상세보기
        - 상세 정보
          - 타임라인
- 조사
  - 이벤트 목록
    - 조직/사용자/엔드포인트/앱/프로세스/이벤트
    - 조직목록
    - 사용자목록
    - 엔드포인트목록
    - 프로세스목록
    - 파일목록
      - 상세보기
        - 타임라인 조합하여 표시 , 모든 기능에 태깅 가능하게
  - 태킹_목록
    - 태깅된 내용 펼쳐보기
  - 자산현황
    - 엔드포인트
    - 앱
    - 프로세스
  - 감사로그
- 대응
  - 정책설정
    - 조직/사용자/프로세스/파일/IOC별
  - IOC 목록
  - 태깅목록
  - 업무처리 SOC 연결
  - 보고서
- EDR 설정

정책설정(적용) UI 샘플

정책대상 설정

기본

팀1

팝업

정책 프로파일

IOC 선택 (팝업떠서 ALL, 혹은 특정만)

IOC 탐지 여부 **ON** / OFF

IOC 탐지 시, 대응 정책

프로세스	선택: 종료, 삭제
레지스트리	선택: 삭제
네트워크	선택: 격리, 완전차단
매체	선택: 차단