Anymon UBA 제품소개서

2017. 02

CONTENTS

I Anymon UBA 개요

1. Anymon UBA 개요
2. 시스템 개념도

1. Anymon UBA 개요

1.1 Anymon UBA 탄생 배경

최근 '소니 픽처스', '한국수력원자력' 해킹 사고와 같이 내부정보 및 내부 중요 문서 유출 침해사고가 일반기업, 공공기관, 금융기관에서 빈번하게 발생하고 있습니다. 이러한 내부정보 유출유형에 대한 분석결과 단순 분석으로 유출경로를 파악하기 어려운 복합적인 지능형 유출사례가 늘어나고 있습니다.

Anymon UBA 탄생 배경

체계적인 지능형 내부정보 유출방지 솔루션 구현

잇따른 고객정보 유출사고 발생에 따른
감독당국의 규제강화 (징벌적 손해배상제 등)

사고 발생시 고객 이탈과 신뢰도 저하는 물론
기업가치 하락과 매출감소 발생

개인정보 보호를 위한 다양한 보안시스템이
도입되어 있으나 개별 운행되어
종합적인 모니터링 필요

탄생 배경

사용자 행위기반 모니터링 시스템 구축

- 개인정보 유출탐지 및 통합관제를 위한 인프라 구축
- 위험 시나리오 정의 및 사용자 행위기반의 다차원 통합분석 기능 개발
- 시스템에서 저장매체와 네트워크를 통한 개인정보파일의 유출 행위 모니터링

사용자별 행위기반 사전/사후 추적성 확보

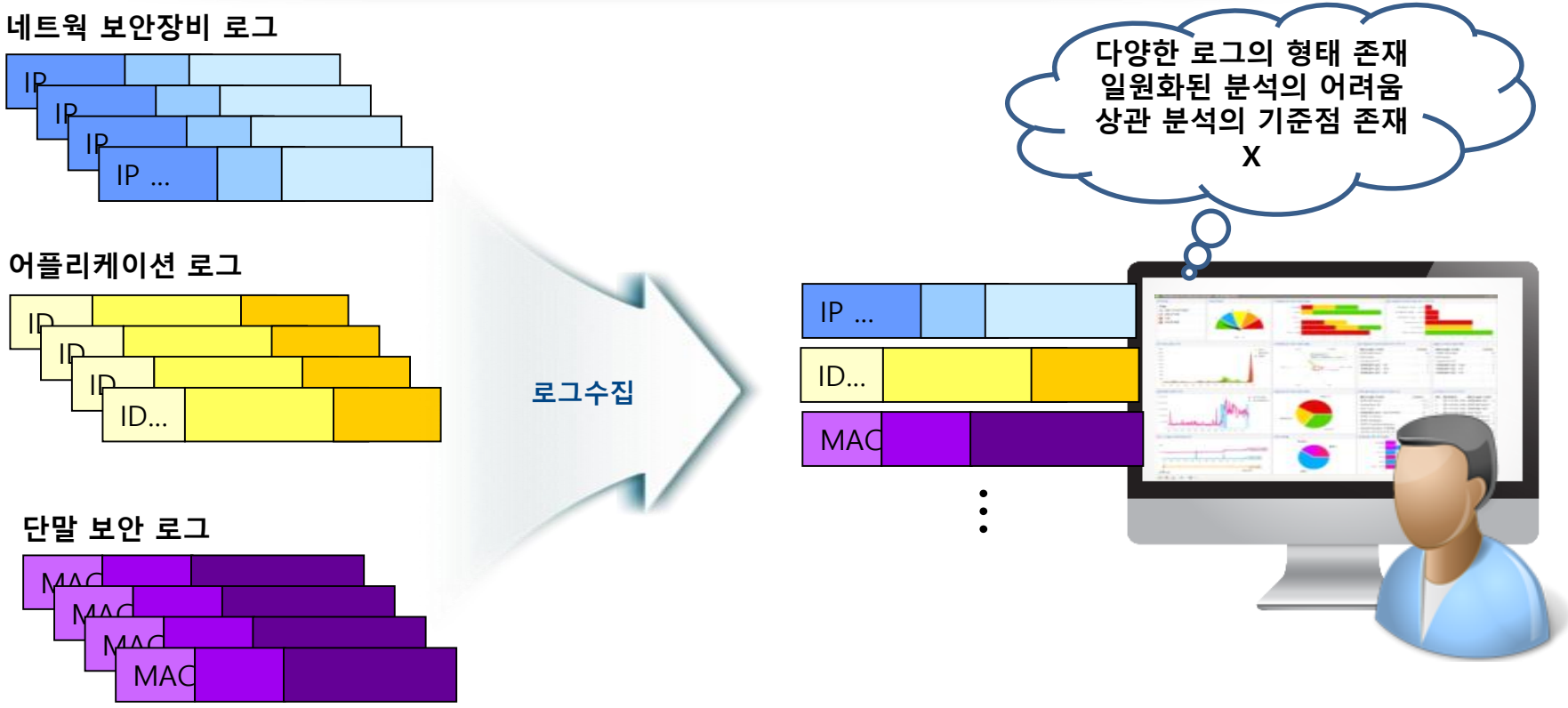
- 개인정보 보안관련 보안시스템에서 발생하는 로그 및 이벤트 수집.관리
- 다양한 방식의 로그 및 이벤트 검색 및 추적 시스템 구축
- 다양한 로그의 상관분석을 통하여 비정상 행위에 대한 침해추적 방안 확보

1. Anymon UBA 개요

1.2 사용자 기반 로그 분석(기존 제품의 문제점)

AS-IS

수집되는 로그의 정보는 로그 발생 장비의 용도에 따라 서로 상이한 기준으로 로그내용이 작성됨

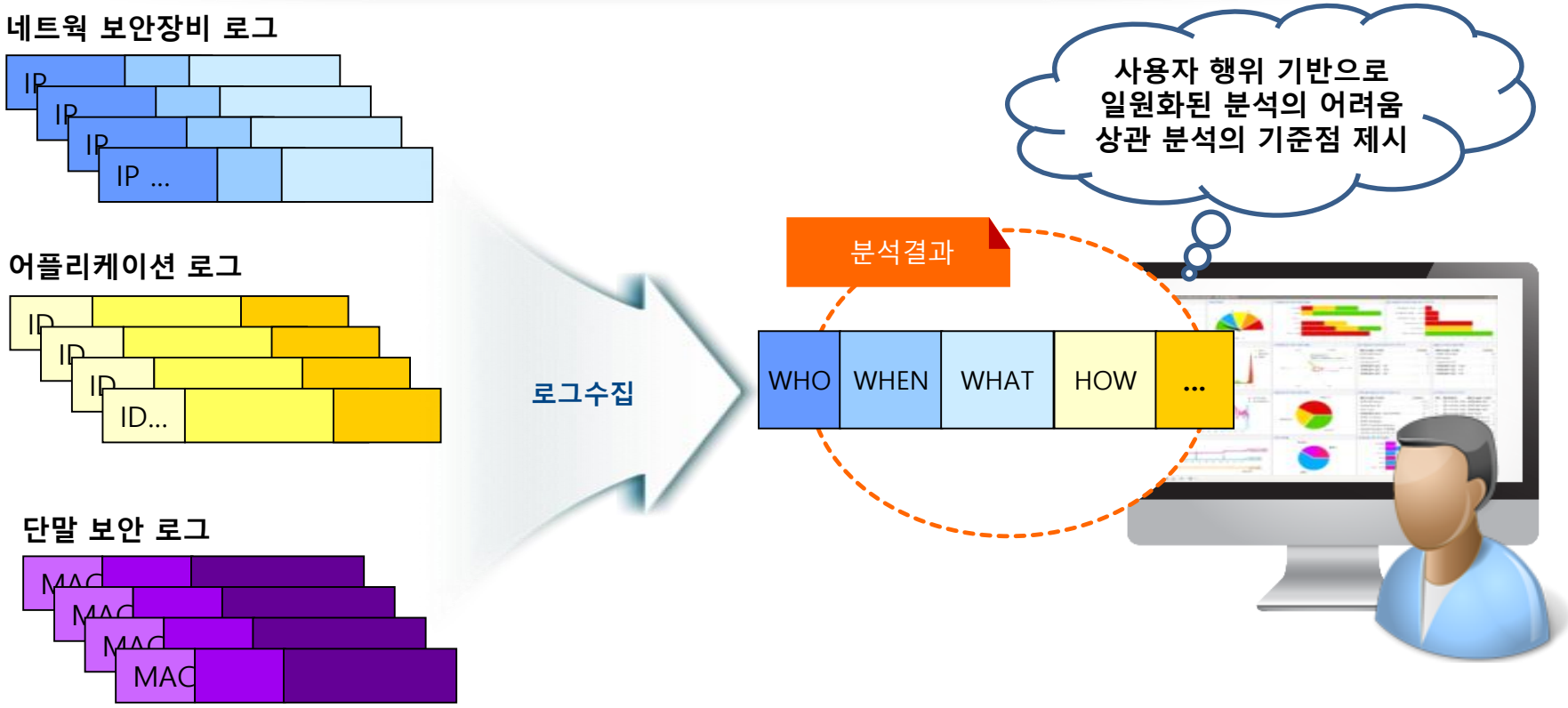


1. Anymon UBA 개요

1.3 사용자 기반 로그 분석(사용자 위주의 로그 재구성)

TO-BE

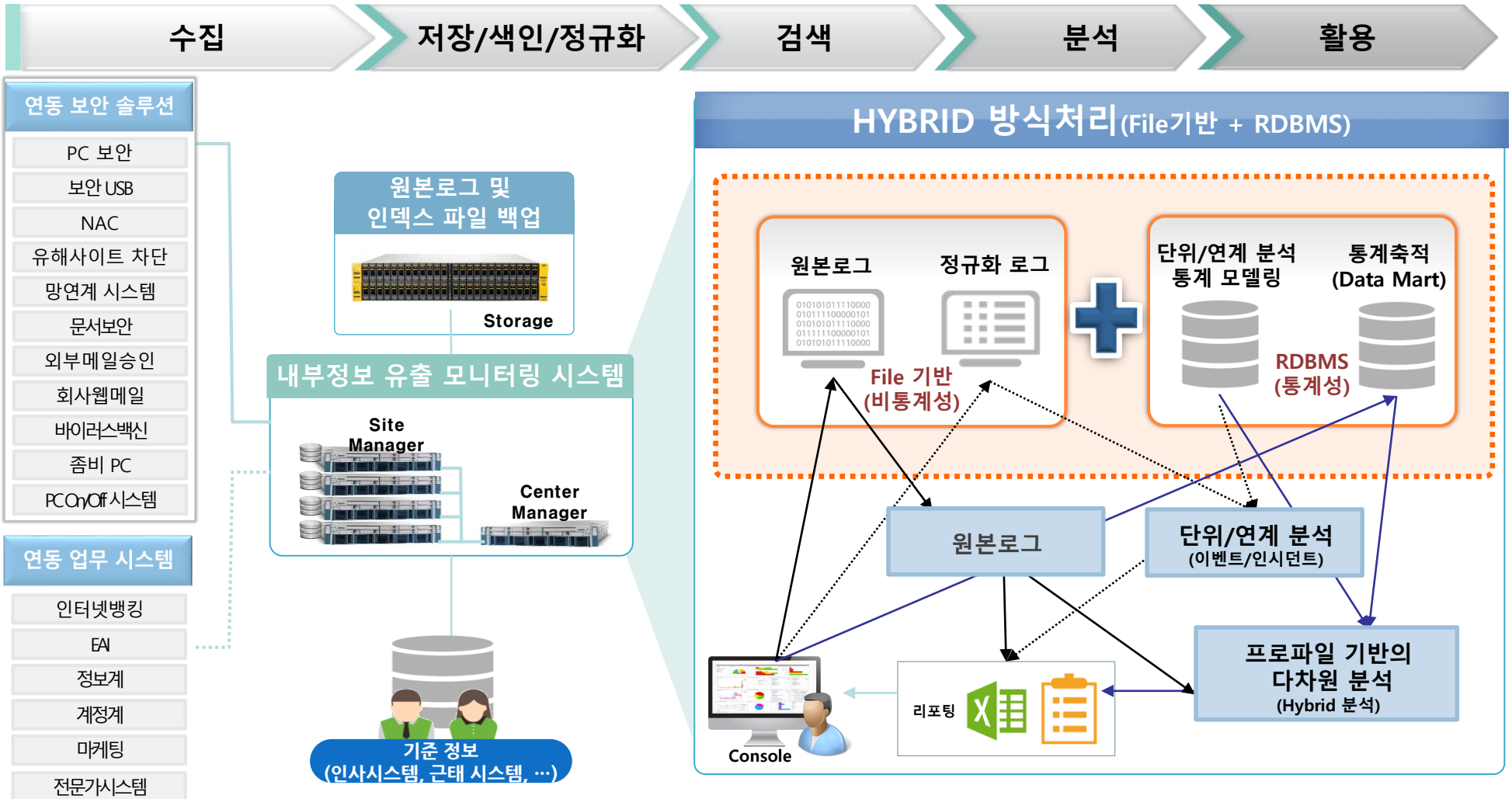
수집되는 로그의 정보를 사용자 위주로 재배치 하여
일원화된 사용자 기반의 행위기반 분석 가능



2. 시스템 구성도

2.1 시스템 구성도

Anymon UBA 구성도



Ⅱ 주요 기능

1. 주요 기능
2. 세부 기능

1. 주요 기능

1.1 Anymon UBA 주요 기능

Anymon UBA는 다양한 장비의 로그를 수집하여 프로파일링 기법을 이용한 시나리오 기반의 상관분석으로 정보유출 사고 사전예방 강화 및 안정성 확보가 가능한 내부정보 유출 모니터링 시스템입니다.

Anymon UBA 주요 기능

실시간 로그 파싱 및 수집 저장	▪ Syslog, SNMP TRAP, Logfile 등의 프로토콜을 통한 이벤트 및 로그 수집 ▪ Binary 형태의 축약한 데이터 및 원시 데이터 저장 ▪ 수집 로그에 대해 기밀성(암호화) 및 무결성(해시) 지원 ▪ 관리 주기에 의한 자동 데이터 삭제 기능
하이브리드 프로파일링 기법을 통한 다차원 상관 분석	▪ **File 기반의 비통계성 자료와 DB 기반의 통계성 자료를 복합적으로 분석** ▪ 복합 분석을 통한 업무/부서/개인 단위의 프로파일링 작업 진행 ▪ 프로파일링 기반의 행위기반 로그 분석 실시 ▪ 하이브리드 방식(통계 축적 및 통계 모델링 방식)의 다차원 상관분석을 통한 위험행위 모니터링
시나리오 생성 및 실시간 **모니터링**	▪ **사용자 정의의 다차원 상관분석 시나리오 작성 UI 제공** ▪ **설정된 시나리오의 분석결과 실시간 모니터링** ▪ 사용자 정의 통계 & 검색 오브젝트 모니터링 ▪ 모니터링 결과를 다양한 형태의 대시보드와 보고서로 제공
로그분석을 통한 사후추적 및 로그검색	▪ 시스템 관리자에 대한 Role 기반 접근권한 기능 제공 ▪ 계층적 관제 대상 장비 관리를 위한 도메인 관리기능 제공 ▪ 수집 로그에 대한 조회 및 분석 기능 (시스템 설계로 최적의 검색 속도 지원) ▪ **침해행위에 대한 사전/사후 추적성 확보**

2. 세부 기능

2.1 수집

Anymon UBA는 모든 장비로부터 수집한 로그에 대한 원본 로그 및 인덱스/정규화 로그 형태의 로그 저장을 제공합니다.
원본 로그로부터 실시간으로 정규화 로그를 생성하여 상관분석 및 통계 등의 분석 기능을 수행합니다.

다양한 업무시스템 및 보안 솔루션 등 로그 연동 및 로그 정규화 (4W1H)

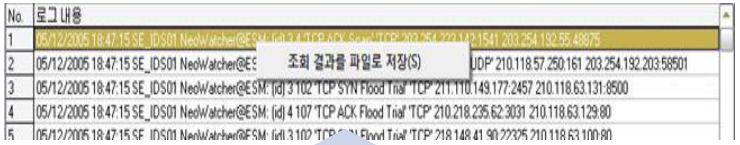
원본로그 수집 및 정규화 작업

수집
Syslog, SNMP TRAP 등의 프로토콜을
통한 실시간 이벤트 및 로그 수집

정규화
정규화 로그 생성 하여
정규화 로그 기반의 상관분석, 통계
생성 등 신속한 분석

저장
원본 로그 및 인덱스/정규화 로그
형태의 로그 저장

수집한 원본 로그



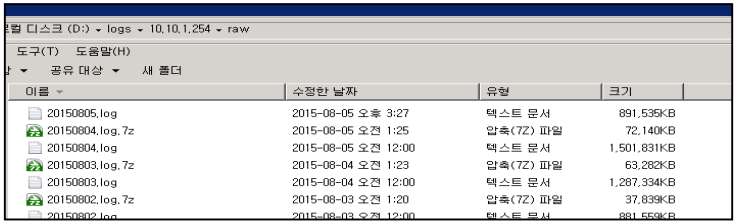
정규화

정규화 로그

수집

저장

저장된 로그 조회



보안 인프라

네트워크 인프라

스위치, 라우터, AP, UC

서버•어플리케이션

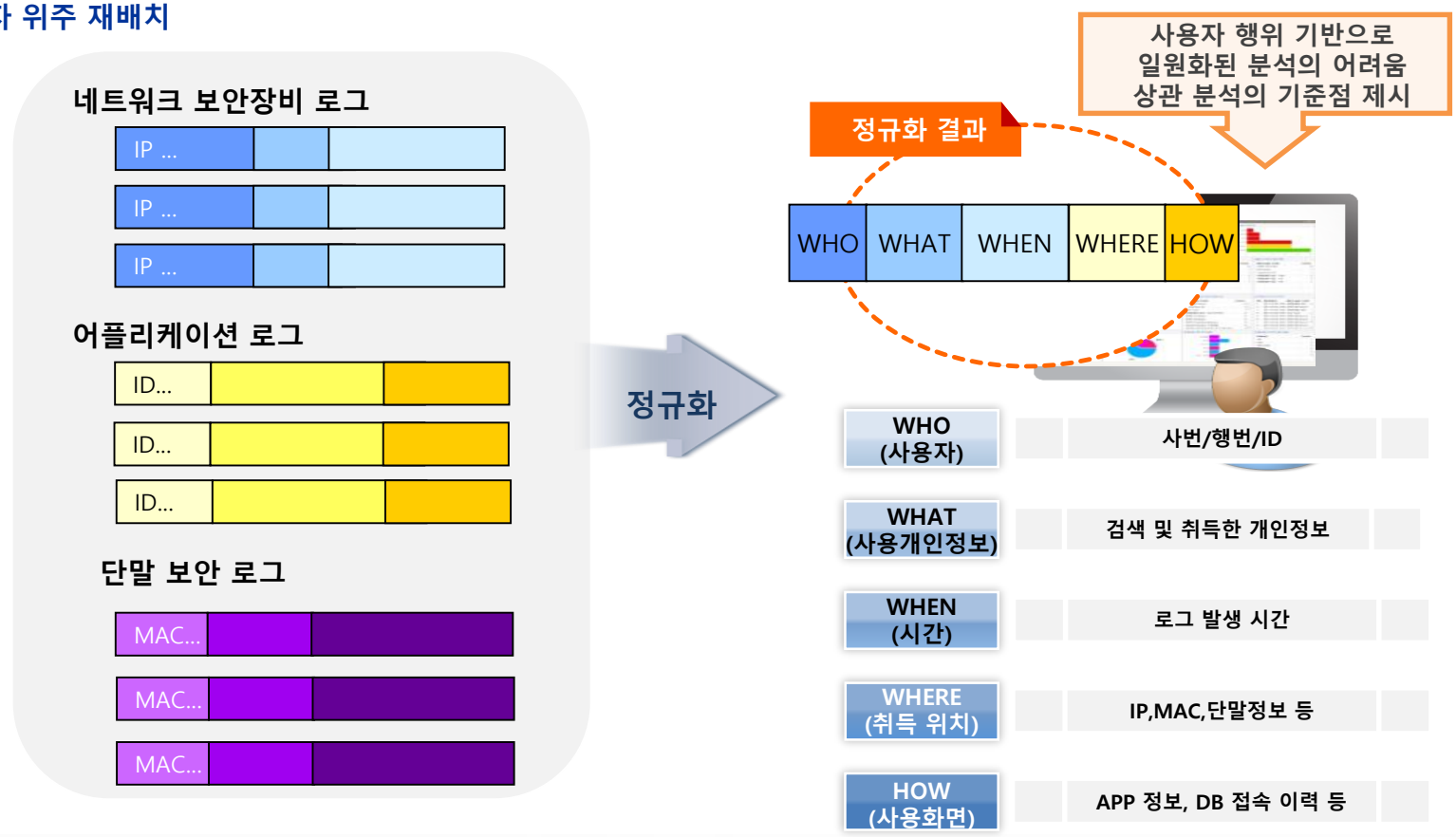
인터넷뱅킹,EAL, 정보계,
계정계, 마케팅,
전문가시스템

2.1 수집

Anymon UBA는 수집되는 로그의 정보를 사용자 위주로 재배치하여 일원화된 사용자 중심의 행위 기반 분석이 가능합니다.

다양한 업무시스템 및 보안 솔루션 등 로그 연동 및 로그 정규화 (4W1H)

사용자 위주 재배치

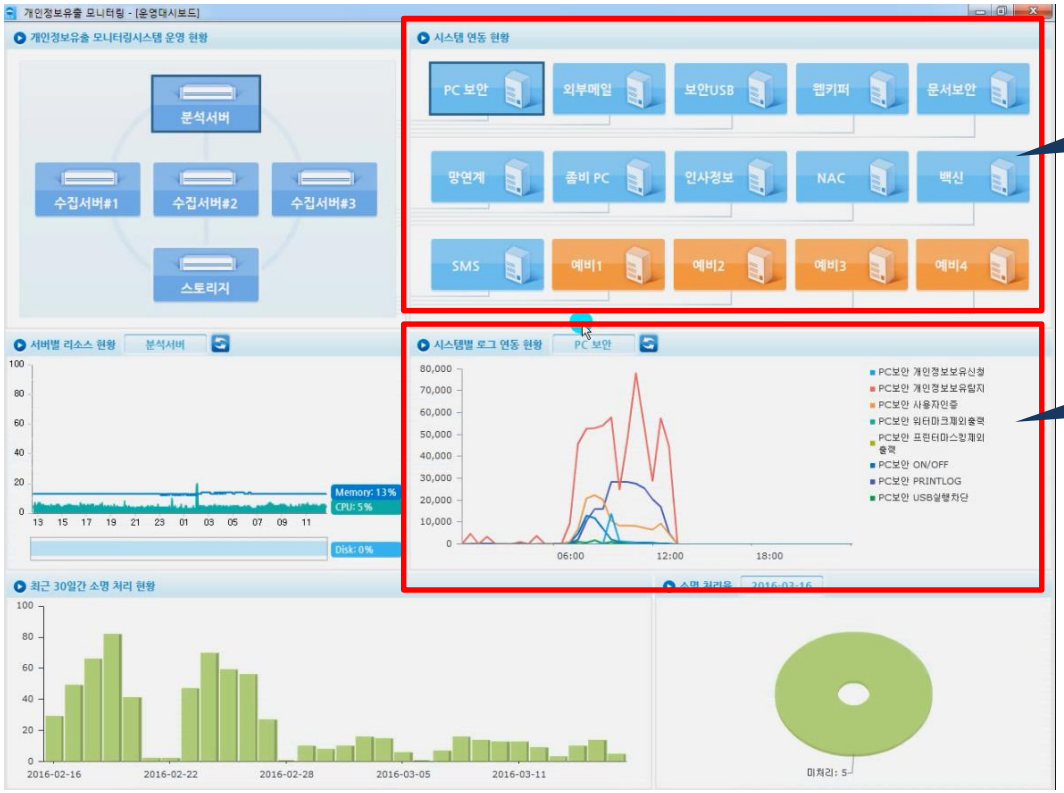


2.1 수집

Anymon UBA는 운영 대시보드를 이용한 각 연동시스템의 로그 수집 현황을 확인 할 수 있습니다. 연동시스템과의 연결이 해제되면 붉은색 아이콘으로 변경되며, 각 연동시스템 아이콘을 클릭시 로그 수집 현황을 확인 가능합니다.

로그 데이터 수집 상태 관리를 위한 헬스체크 관리

수집 현황 모니터링



연동 시스템별 상태 표시
파란색: 정상 상태
붉은색: 비정상 상태 (연결해제)

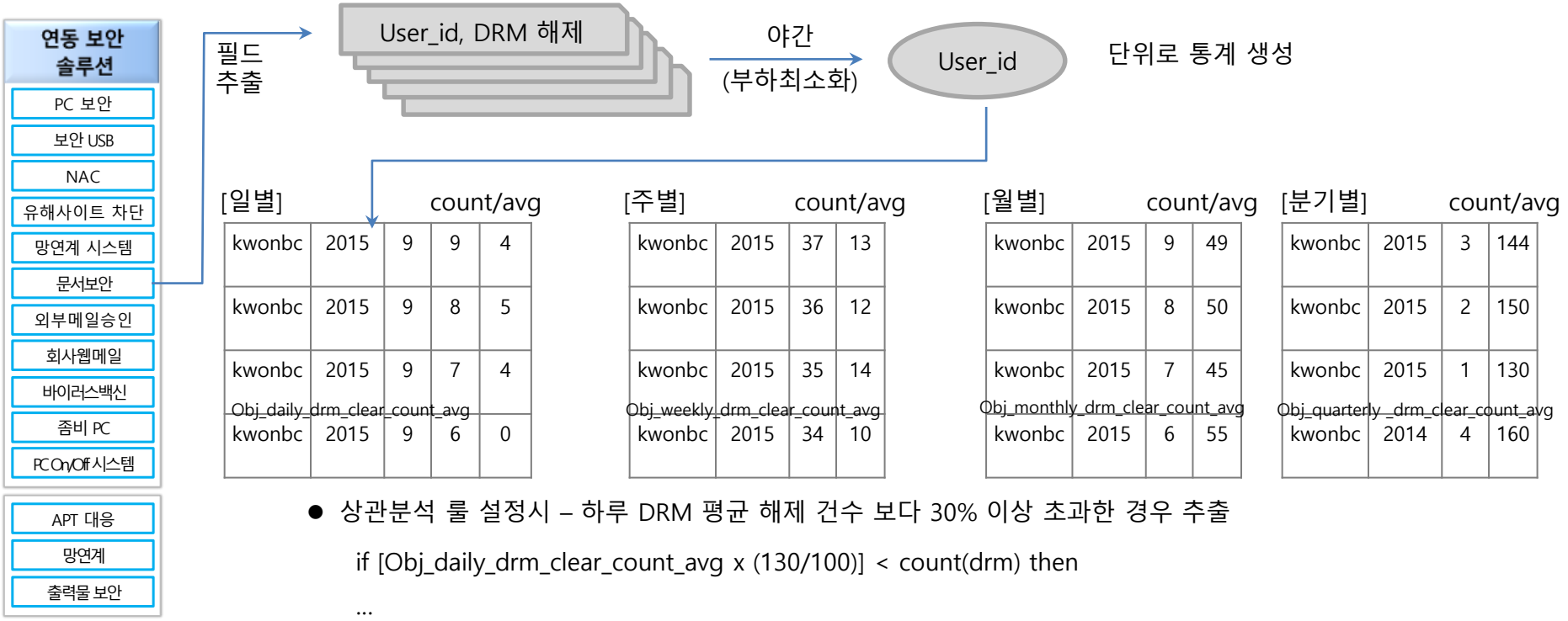
연동 시스템별 로그 수집 현황
추이그래프 형태로 30분 간격의 로그 수집량을 확인 할 수 있다

2.2 분석/탐지

Anymon UBA는 평균 데이터 축적용 오브젝트 생성하여 조회시 오브젝트를 조건으로 입력하여 결과를 추출합니다. 사용자 id 단위로 통계 생성이 가능하며 특정 항목에 대한 건수의 평균값 계산 조회 기능을 제공합니다.

특정 항목에 대한 건수의 평균값 계산 조회 기능

DRM 문서 복호 저장 건수 사례



- 상관분석 룰 설정시 – 하루 DRM 평균 해제 건수 보다 30% 이상 초과한 경우 추출

  if [Obj_daily_drm_clear_count_avg x (130/100)] < count(drm) then

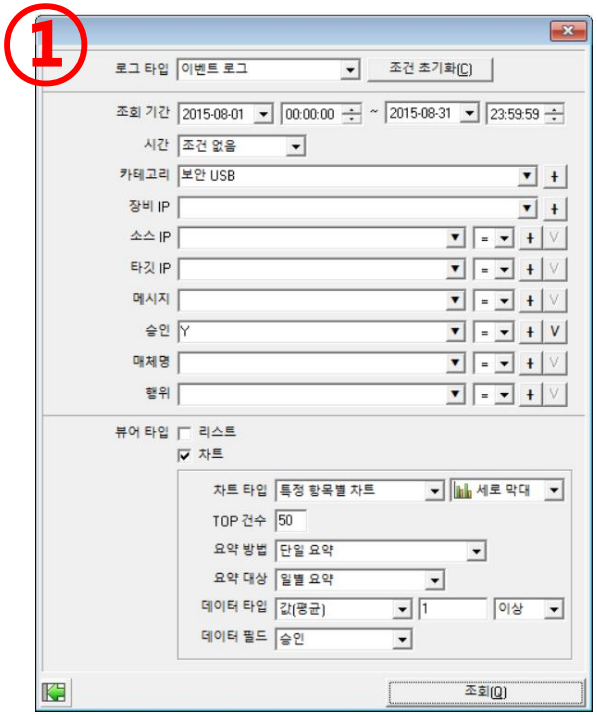
  …

2.2 분석/탐지

Anymon UBA는 항목별 발생 건수에 대한 일별 누적 평균값을 계산하는 기능을 추가 개발하여 일별 Count와 평균을 조회할 수 있으며 특정 조건을 만족하는 사용자 ID를 추출할 수 있으며 기간 내 건수 관련 조회 기능을 제공합니다.

일별로 보안시스템의 승인평균, 파일반출 평균, 복호화 평균, ..., 감염평균을 계산 확인 »

3번 항목 + 3개 이상의 보안시스템 일평균을 초과하는 사용자 ID 추출 확인 포함



<평균 계산 확인 예시>

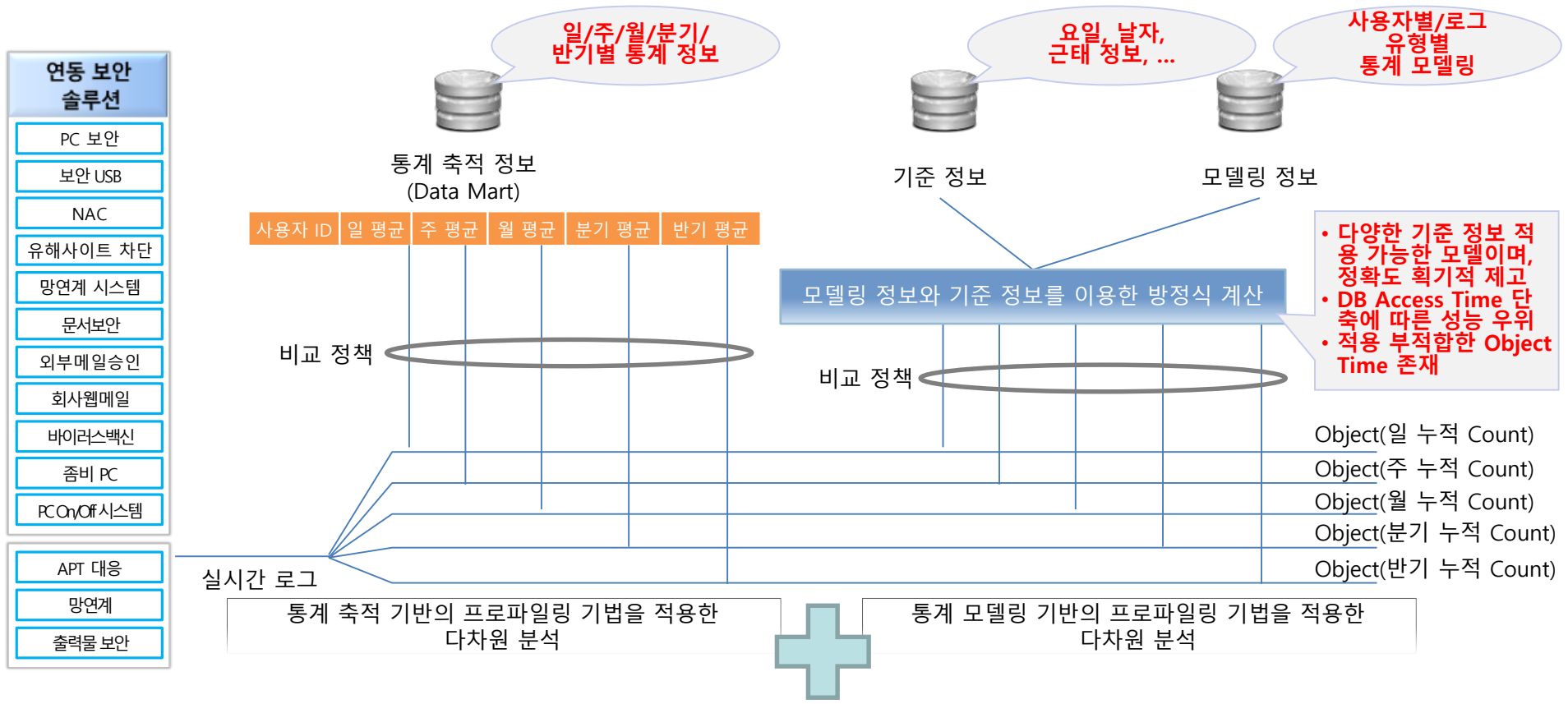
① 보안 USB 시스템의 '승인' 통계를 일별로 조회
② 일별 count 및 평균 확인 가능

2. 세부 기능

2.2 분석/탐지

Anymon UBA는 통계 축적 기반의 프로파일링 기법과 통계 모델링 기반의 프로파일링 기법을 동시에제공하는 Hybrid 형태의 프로파일링 기법을 적용한 다차원 분석 기술을 채용합니다.

Hybrid 형태의 프로파일링 기법을 적용한 다차원 분석 기술

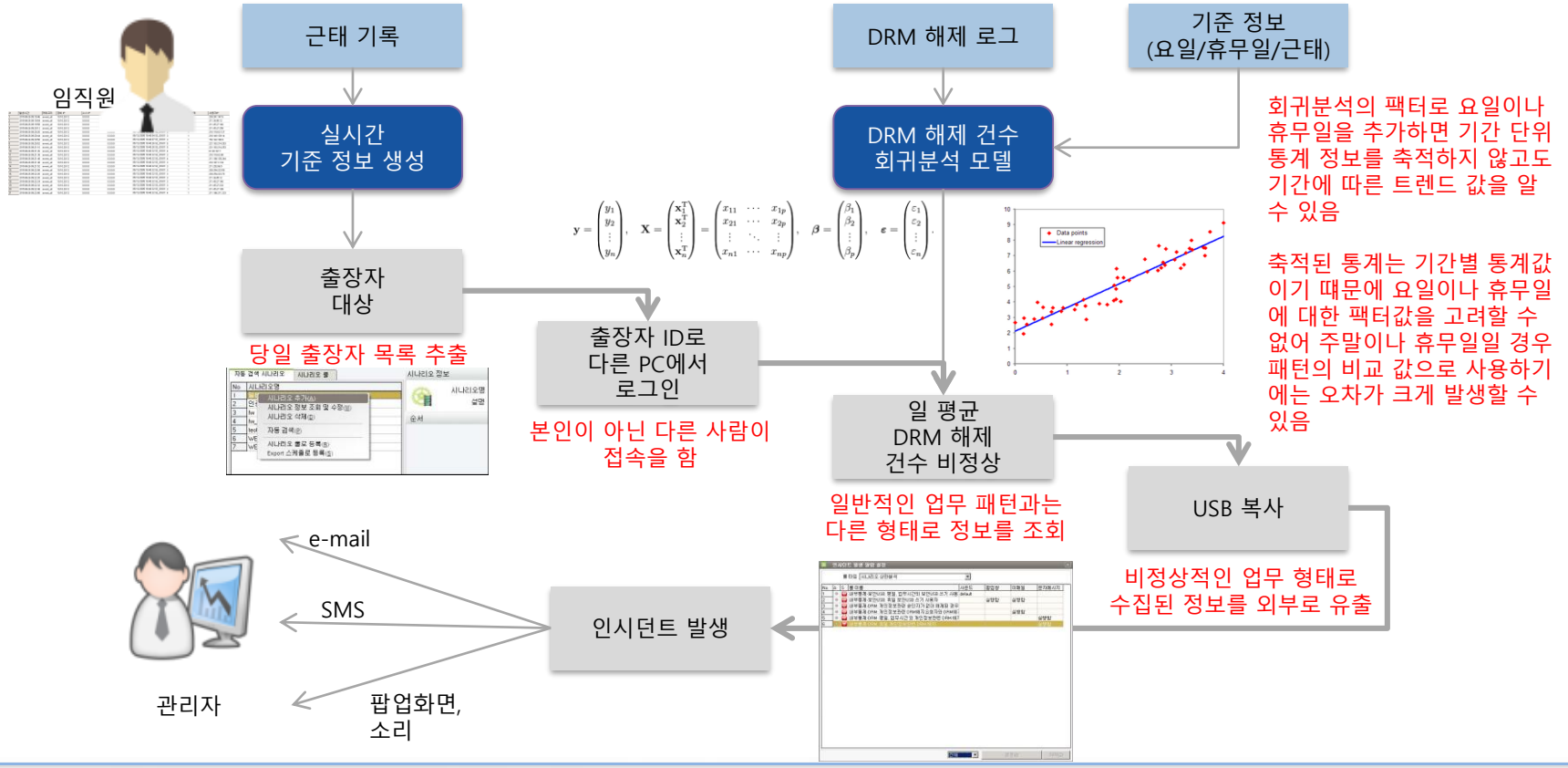


2.2 분석/탐지

Anymon UBA는 과거 사용자의 행위분석을 통해 유출 의심 특징을 추론하여 개인 부서별 행위 예측값을 생성하는 것이며, 실시간 탐지 단계에서 행위자 개인별 특성을 반영하여 자동 탐지 가능합니다.

운영 시뮬레이션

프로파일링 운영 시뮬레이션



2.2 분석/탐지

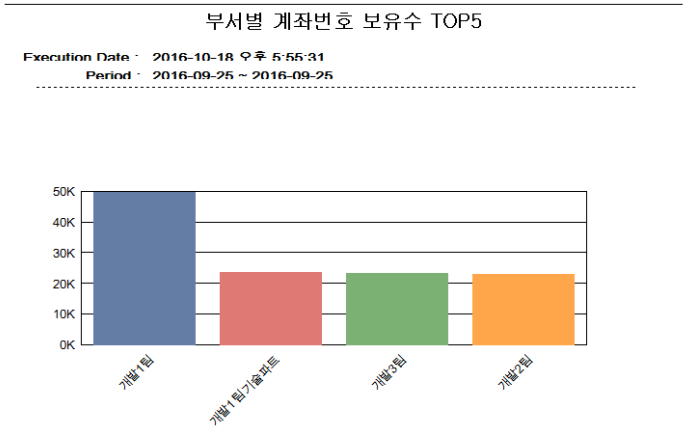
Anymon UBA는 각종 통계정보를 레포트 형식으로 받아 볼 수 있으며, 엑셀, PDF 형식의 파일형태로도 생성이 가능합니다.

부서/직무/직원별 고객정보 이용현황 통계자료 작성 (프로파일링)

고객정보 이용현황 레포트

사용자별 계좌번호 보유수

사번	이름	부서	갯
50	이동호	개발1팀기술파트	110
42	강석주	개발1팀	110
13	조준현	개발2팀	109
16	이동욱	개발2팀	109
37	최헌석	개발1팀	109
53	이성진	개발3팀	108
45	강석규	개발1팀	108
33	손민기	기술기획팀	108
1	김선호	보안기술팀	107
25	전혜진	사업지원팀	107
31	조수진	영업5팀	107
51	한태현	개발3팀	107
49	강연준	개발1팀기술파트	106
56	이두용	개발3팀	106
30	유수동	영업3팀	106
36	함성윤	개발1팀	106
17	이창근	경영관리본부	106
29	진성철	영업3팀	106
28	오희수	영업1팀	106
27	임종석	영업1팀	105
9	지창훈	개발2팀	105
7	최주리	보안기술팀	105
48	조상원	개발1팀기술파트	105
43	류용수	개발1팀	105
46	김정태	개발1팀기술파트	104
14	김효중	개발2팀	104
11	김남희	개발2팀	104
2	이재현	보안기술팀	104



부서별 개인정보 보유수 TOP 5

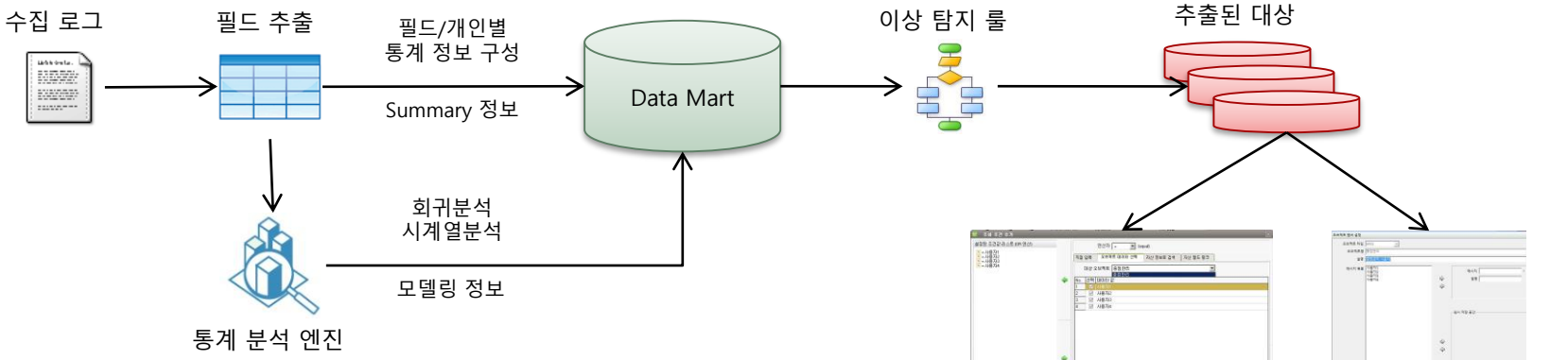
부서	갯
개발1팀	25,037
개발1팀	24,732
개발1팀기술파트	23,861
개발3팀	23,523
개발2팀	23,182

2.2 분석/탐지

Anymon UBA는 이상 여부 판단 룰 설정을 통해 비정상 행위자에 대한 정보를 추출하고 이를 다양한 용도로 활용하기 위하여 분석서버 내의 오브젝트로 생성합니다.

수집된 거래로그 분석을 통한 이상행위 시나리오 적용 및 관리

프로파일링 기법



POINT

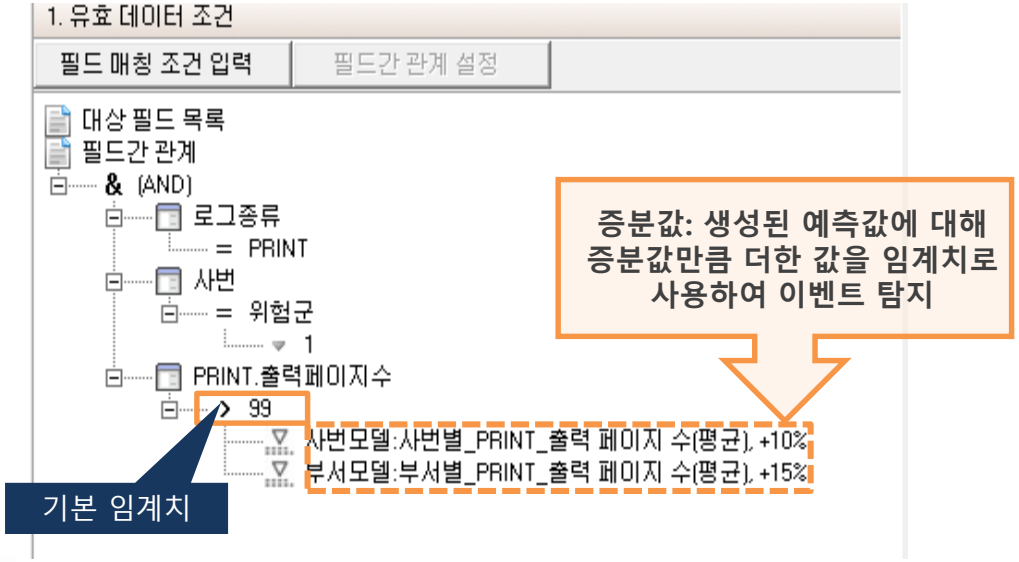
- 필드 추출한 정보를 기반으로 기간별 통계 정보를 축적하고 통계 분석 엔진을 통해 회귀분석, 시계열분석 모델을 생성하여 데이터 마트를 구성
- 통계 정보는 기간에 따라 자동 계산 및 축적되며, 통계 모델은 정해진 주기(예, 일 단위)마다 모델 검증을 통해 오차범위를 넘은 모델만 자동 재계산
- 이상 여부 판단 룰 설정을 통해 비정상 행위자에 대한 정보를 추출하고 이를 다양한 용도로 활용하기 위하여 분석서버 내의 오브젝트로 생성
- 생성된 오브젝트는 이벤트 탐색 및 상관분석을 통해서 검색, 실시간 탐지 가능
- 오브젝트 설정 화면을 통해 자동 추출된 결과물에 대한 관리 가능
- Top N 등의 모니터링을 위한 백 데이터로 사용할 수 있어 시각화된 정보로 활용 가능

2.2 분석/탐지

Anymon UBA는 통계모델을 통한 임직원별 예측값과 부서별 예측값을 만들 수 있습니다. 하나의 정책으로 임직원마다 다른 예측값을 적용하여 임계치를 달리 가져갈 수 있으며 임계치의 증분값을 적용하여 오탐 확률을 줄일 수도 있습니다.

직군별, 사용자별 전용 시나리오 적용 (임계치 차등 적용 등)

사용자별 전용 시나리오



POINT

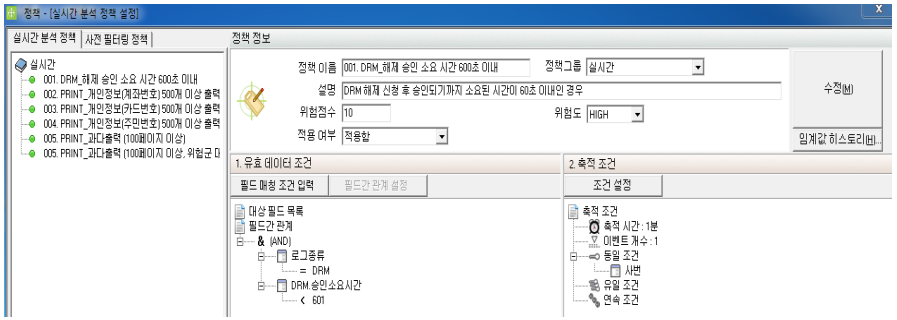
- 정책에 사번모델 또는 부서모델이 설정되어 있을 경우에는 기본 임계치를 사용하지 않는다.
- 사번모델에 의해 생성된 개인별 예측값이 있을 경우 예측값을 기준으로 이벤트를 발생시키며
- 개인별 예측값이 없을때는 부서별 예측값이 있는지 확인한다.
- 부서별 예측값이 있을 경우 부서별 예측값을 기준으로 이벤트를 발생시키며, 부서별 예측값도 없을 경우에 기본 임계치와 비교하여 이벤트를 발생 시킨다.

2.2 분석/탐지

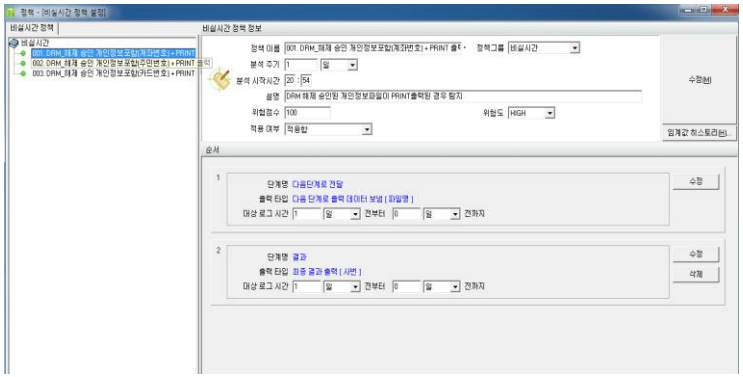
Anymon UBA는 실시간 정책, 비실시간 정책 메뉴를 이용해서 각종 시나리오를 통합 관리 할 수 있으며 과거로그 실시간 정책적용을 이용해서 과거에 발생했던 데이터를 현재 시점에 생성한 시나리오에 적용하여 이벤트 도출이 가능합니다.

이상행위 탐지 시나리오 통합 관리 (시뮬레이션 포함)

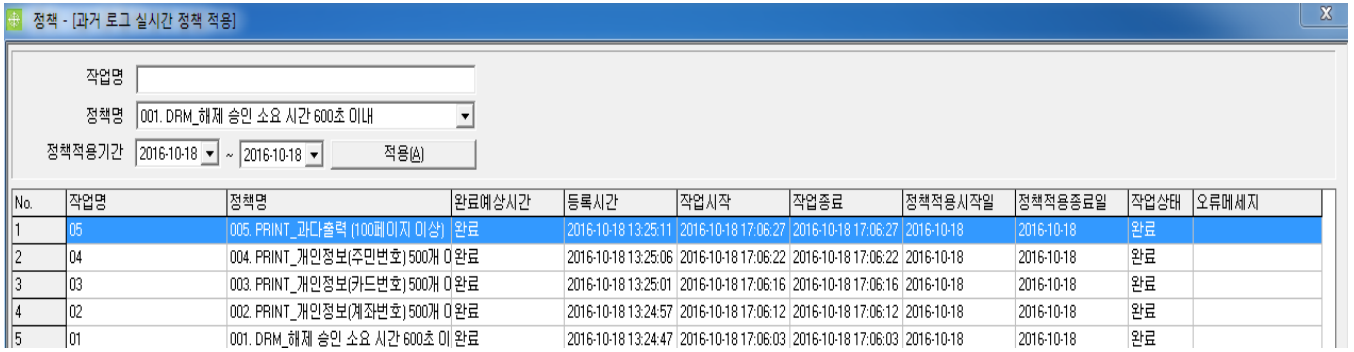
실시간 정책 메뉴



비실시간 정책 메뉴



과거로그 실시간 정책 적용

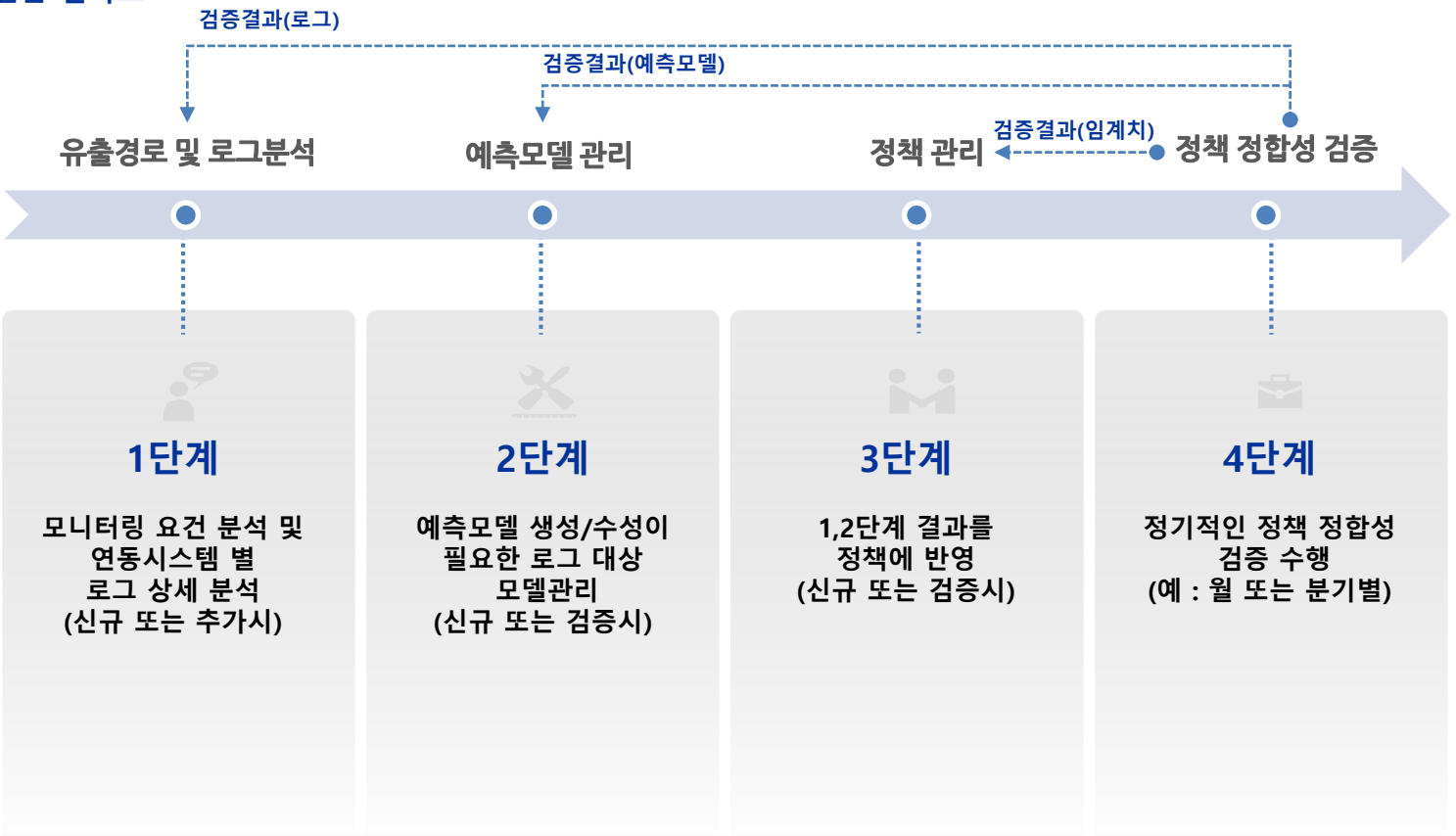


2.3 운영관리

Anymon UBA 정책 관리 방법론으로 로그 수집/분석, 시나리오 생성/변경, 정합성 검증까지의 체계적인 방법을 제공합니다.

이상행위 시나리오 정의, 검증, 적용, 분석, 피드백 등 관리

정책 관리 방법론 절차도

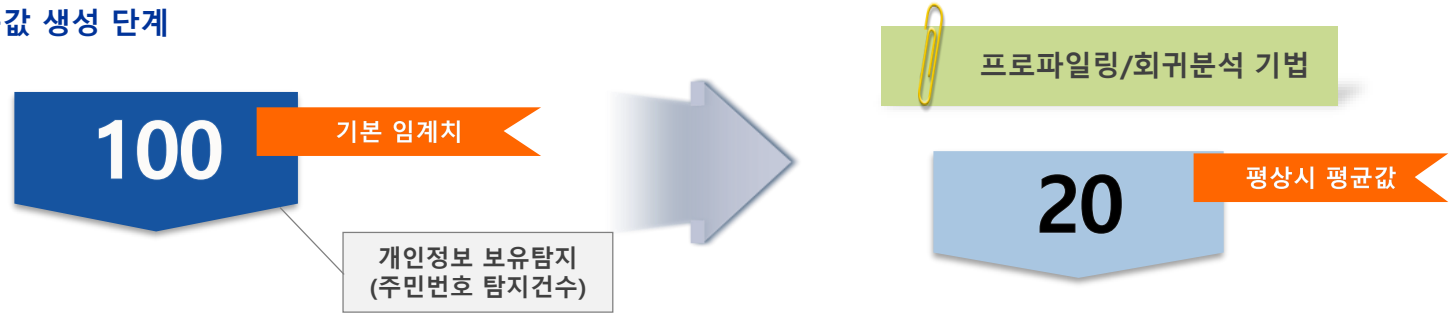


2.3 운영관리

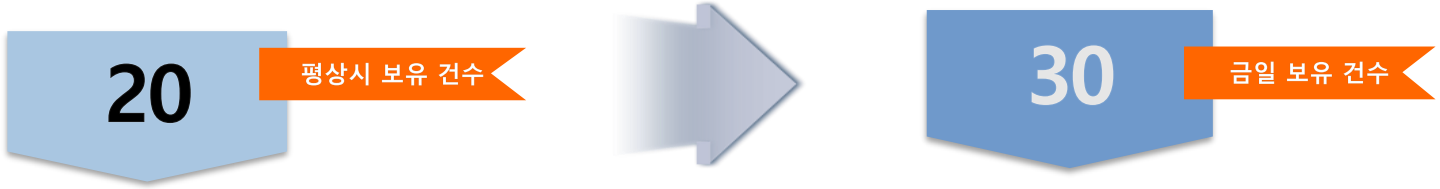
Anymon UBA는 회귀분석을 통해 과거 사용자의 유출 의심 행위 특징을 추론하여 개인 부서별 행위 예측값을 생성하며 실시간 탐지 단계에서 행위자 개인별 특성을 반영하여 자동 탐지 가능합니다.

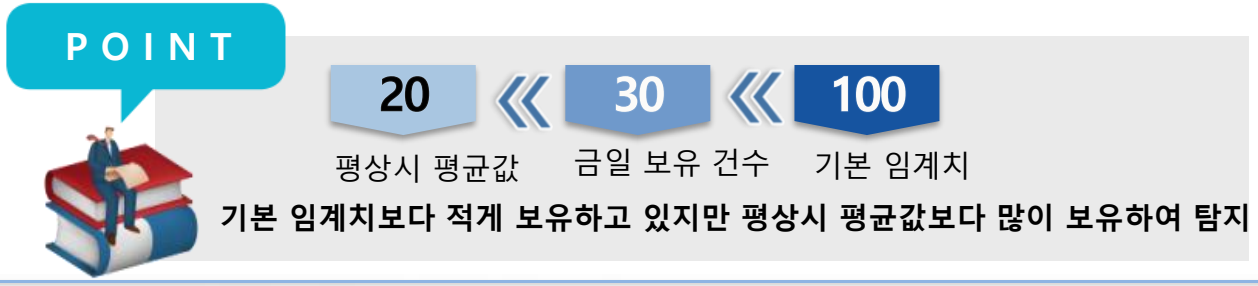
핵심위험지표 측정을 통한 이상행위 발생 징후 사전 탐지

예측값 생성 단계



실시간 탐지 단계

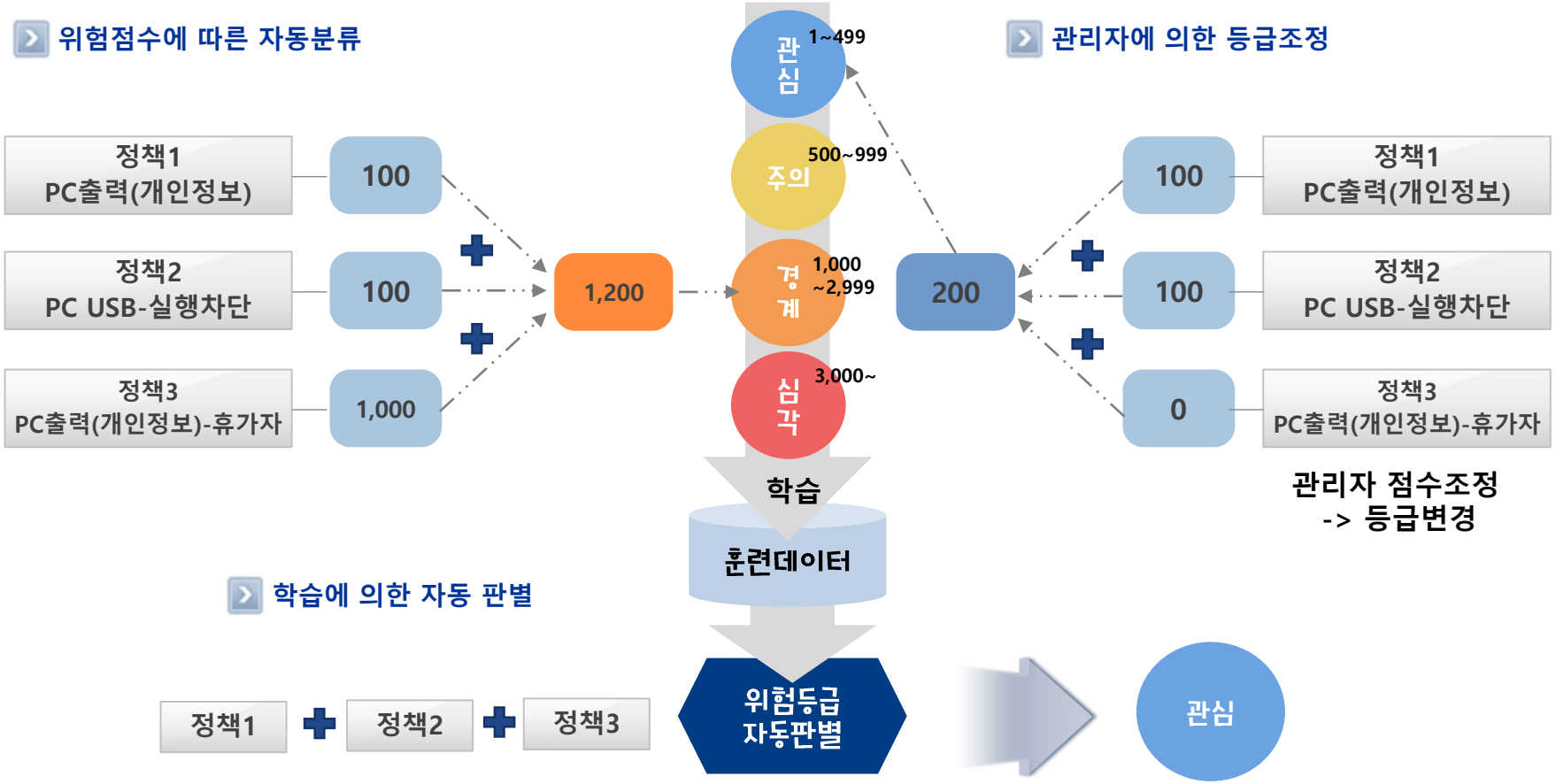




2.3 운영관리

Anymon UBA는 학습에 의한 판별분석을 통해 탐지 패턴을 학습하여 위험등급을 자동 판별 가능하며 고위험군(경계/심각) 직원 자동 분류가 가능합니다.

핵심위험지표 수치화(Scoring)을 통한 고위험군 사용자 식별

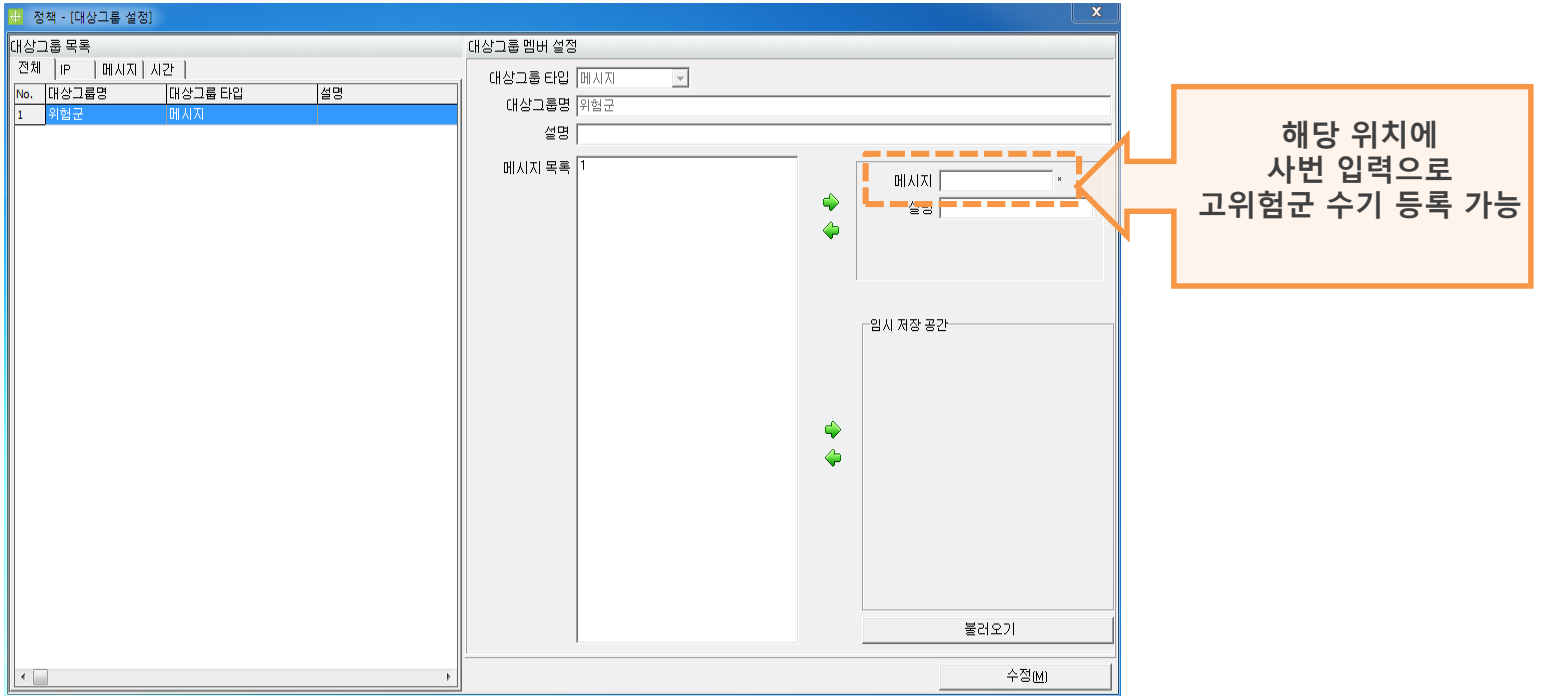


2.3 운영관리

Anymon UBA는 위험군 그룹을 추가하여 수시로 등록 및 해제를 할 수 있고 해당 그룹을 시나리오 정책의 조건으로 사용 가능합니다.

고위험군 사용자 대상 분석 및 등록/해제 관리(수기 등록, 자동등록 등)

고위험군 사용자 등록

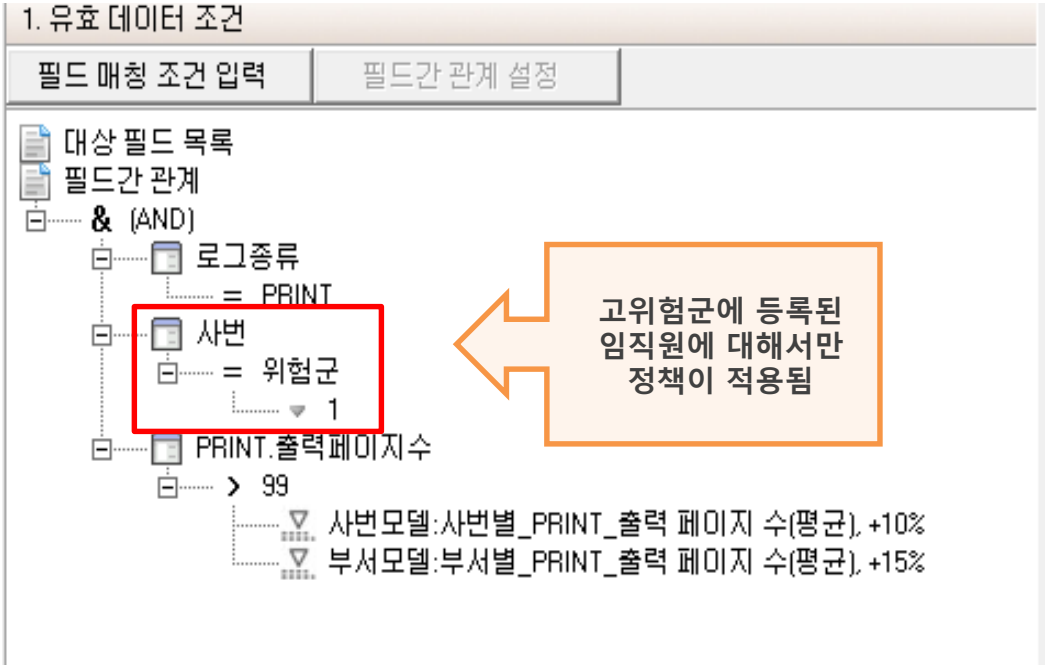


2.3 운영관리

Anymon UBA는 위험군 그룹이 정책 조건으로 포함된 시나리오를 따로 구성하여 관리 할 수 있습니다.

고위험군 사용자 전용 탐지 시나리오 관리 적용

고위험군 사용자 시나리오



2.3 운영관리

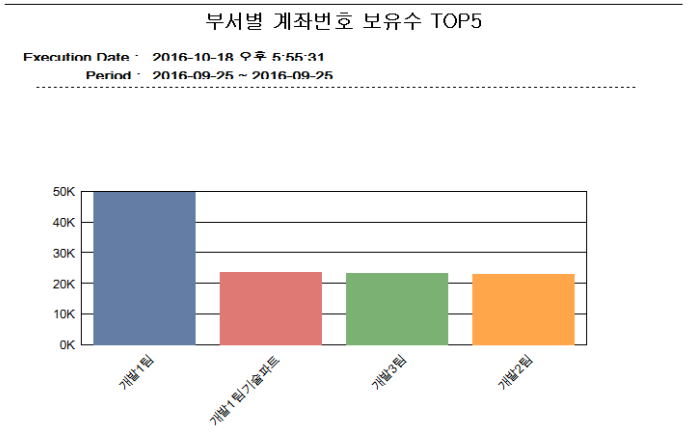
Anymon UBA는 각종 통계정보를 레포트 형식으로 받아 볼 수 있으며, 엑셀,PDF 형식의 파일형태로도 생성이 가능합니다.

고객정보 이용 현황(조회, 보유, 출력, 제공 등)

고객정보 이용현황 레포트

사용자별 계좌번호 보유수

사번	이름	부서	갯
50	이동호	개발1팀기술파트	110
42	강석주	개발1팀	110
13	조준현	개발2팀	109
16	이동욱	개발2팀	109
37	최헌석	개발1팀	109
53	이성진	개발3팀	108
45	강석규	개발1팀	108
33	손민기	기술기획팀	108
1	김선호	보안기술팀	107
25	전혜진	사업지원팀	107
31	조수진	영업5팀	107
51	한태현	개발3팀	107
49	강연준	개발1팀기술파트	106
56	이두용	개발3팀	106
30	유수동	영업3팀	106
36	함성윤	개발1팀	106
17	이창근	경영관리본부	106
29	진성철	영업3팀	106
28	오희수	영업1팀	106
27	임종석	영업1팀	105
9	지창훈	개발2팀	105
7	최주리	보안기술팀	105
48	조상원	개발1팀기술파트	105
43	류용수	개발1팀	105
46	김정태	개발1팀기술파트	104
14	김효중	개발2팀	104
11	김남희	개발2팀	104
2	이재현	보안기술팀	104



부서별 개인정보 보유수 TOP 5

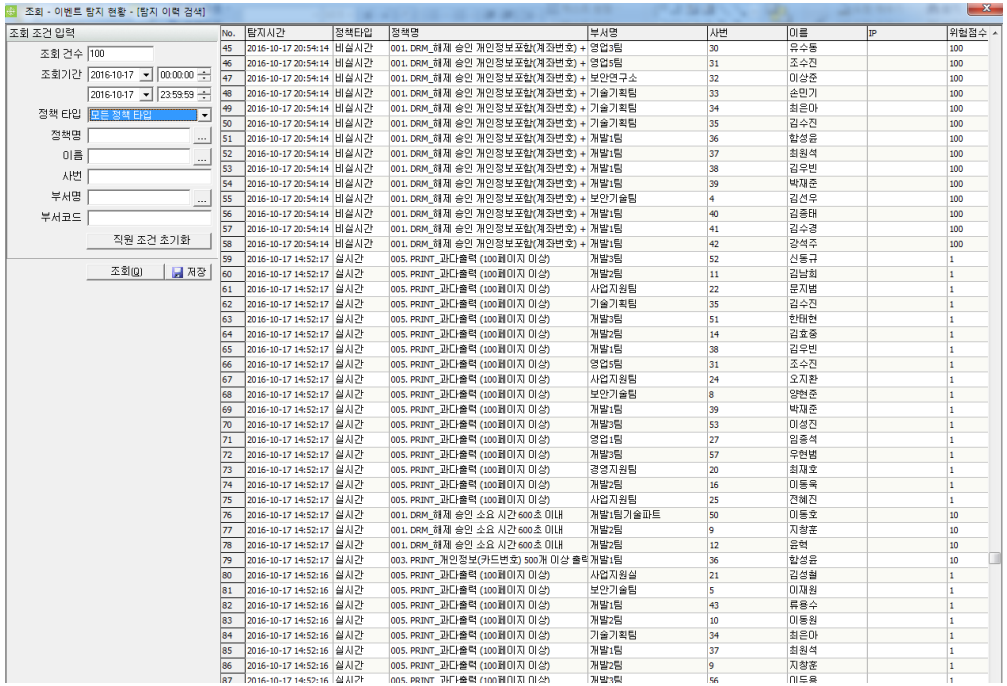
부서	갯
개발1팀	25,037
개발1팀	24,732
개발1팀기술파트	23,861
개발3팀	23,523
개발2팀	23,182

2.3 운영관리

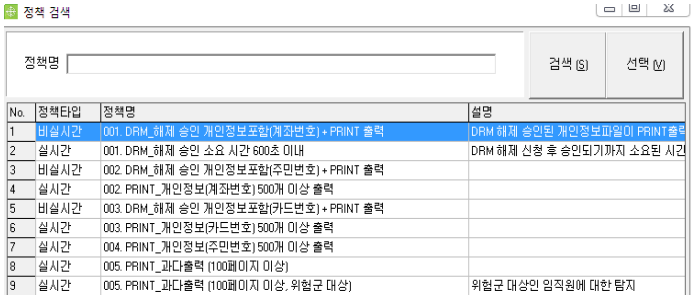
Anymon UBA는 정책에 의해 탐지된 이벤트는 실시간으로 탐지 현황을 모니터링 할 수 있습니다. 실시간, 비실시간 정책별로 조회가 가능하며, 정책명 이름 사번 부서명을 이용한 조건별 검색도 제공됩니다.

이상행위 탐지현황, 필수 S/W, 비인가 S/W관리 등

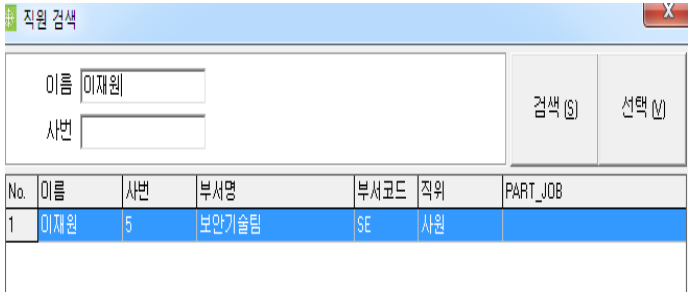
정책에 의한 이벤트 탐지 현황



정책 검색



직원 검색

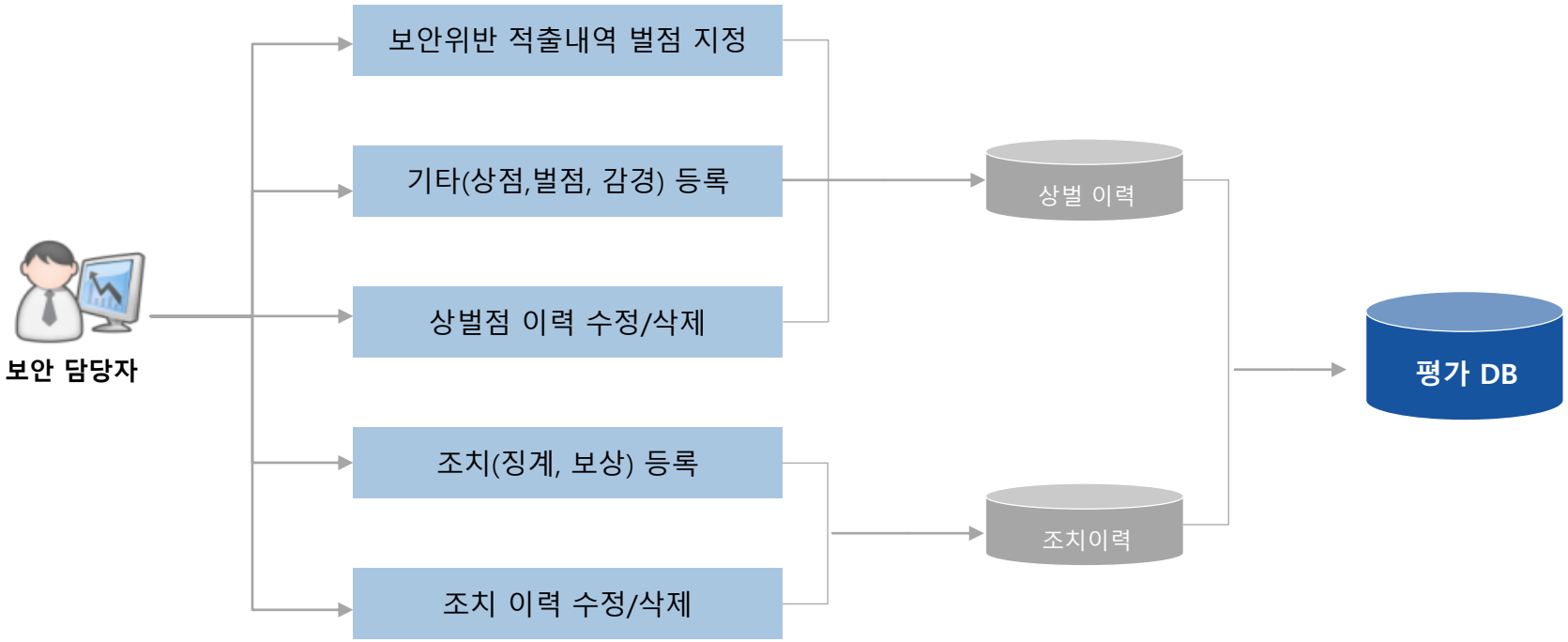


2.3 운영관리

Anymon UBA는 정보보안에 대한 위반과 소명 내역을 참조하여 보안지수에 대한 평가 DB를 근거로 각 부서 및 직원별 보안평가관리기능을 지원합니다.

정보보안지수 측정을 통한 부서/직원별 보안 수준 확인 및 개선방안 안내

사용자 보안 평가 관리

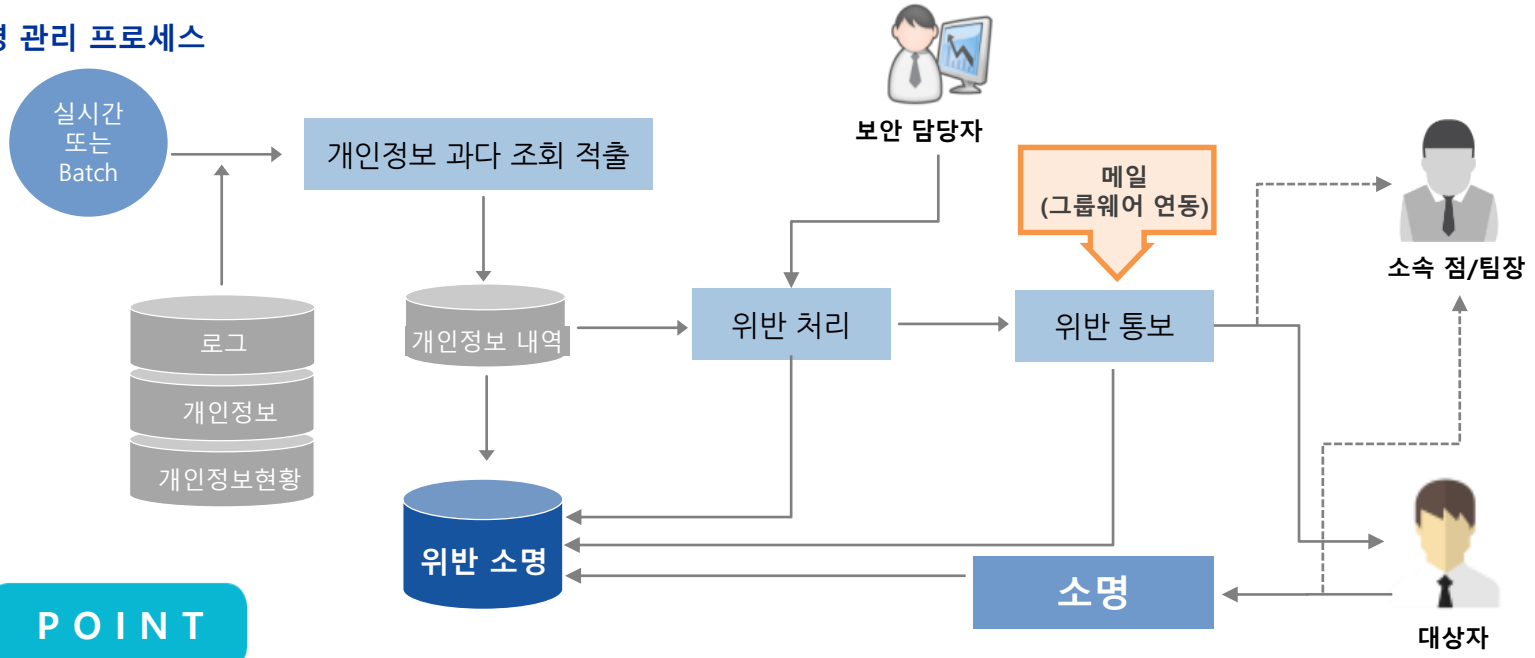


2.3 운영관리

Anymon UBA는 소명 관리 프로세스를 아래와 같이 제공합니다.

이상행위 거래자 소명 절차 수립 및 프로세스 구현

소명 관리 프로세스



POINT

- **위반여부 관리**
  -실시간 또는 Batch에 적출된 개인정보 처리 현황에 대해 보안담당자가 위반여부 (위반, 위반아님, 예외처리 등) 처리
- **위반 통보 관리**
  - 위반으로 처리한 건을 대상자에게 위반 통보(소명 요청, 소속 점/팀장 참조)
- **소명 관리**
  - 위반 통보된 건을 대상자가 소명(소속 점/팀장 참조)

2.3 운영관리

Anymon UBA는 적출된 내역에 대해 보안담당자가 위반으로 처리한 현황을 조회하고 소명을 요청할 수 있습니다.

소명 처리 항목 분석 및 소명지연, 재소명, 소명 처리 추이분석 등

위반 내역 현황

- 적출된 내역에 대해 보안담당자가 위반으로 처리한 현황을 조회하고 소명을 요청

#	일자	시간	소속	사번/직급/성명	구분	관리 유형	위반 유형	위반 번호	상태	통보 횟수	완료
1					이벤트	문서보안			미통보	0	종결

위반 내역 상세

#	일자	시간	소속	사번/직급/성명	구분	관리 유형	위반 유형	위반 번호	위반여부	위반 항목	검토 의견
1					이벤트	문서보안					
2											

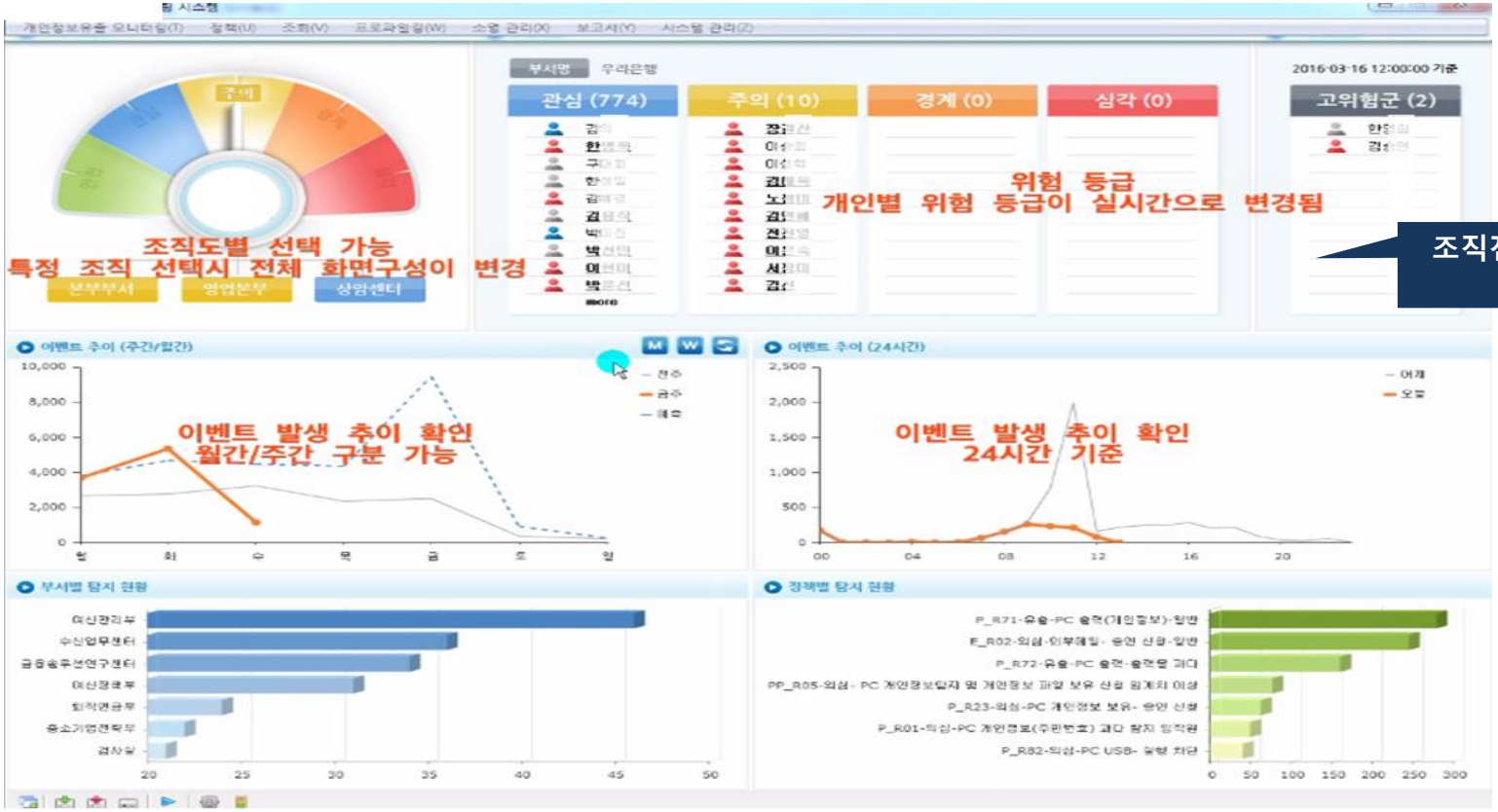
종결 처리

소속	사번	직급	성명	보안 포인트	위반 번호	위반 벌점	가산 벌점	의견

2.4 모니터링 기능

Anymon UBA는 사용자 기반의 모니터링 화면을 제공하며 각종 분석에 대한 내용을 직관적으로 제공하게 됩니다.

고객정보 유출 이상행위 집중 모니터링 화면(종합상황판) 개발 »

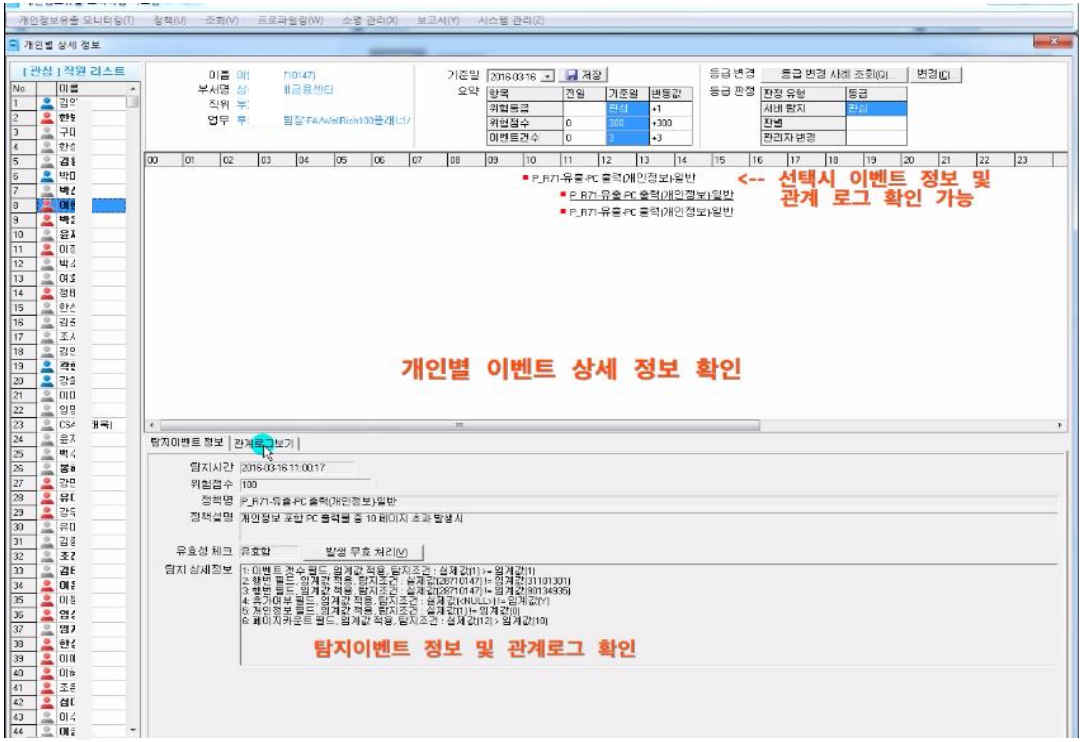


2.4 모니터링 기능

Anymon UBA는 이상행위 발생통계, 고객정보 보유/반출 현황 등 시스템 전반 모니터링이 가능합니다.

이상행위 발생통계, 고객정보 보유/반출 현황 등 시스템 전반 모니터링 »

시스템 전반 모니터링



2.4 모니터링 기능

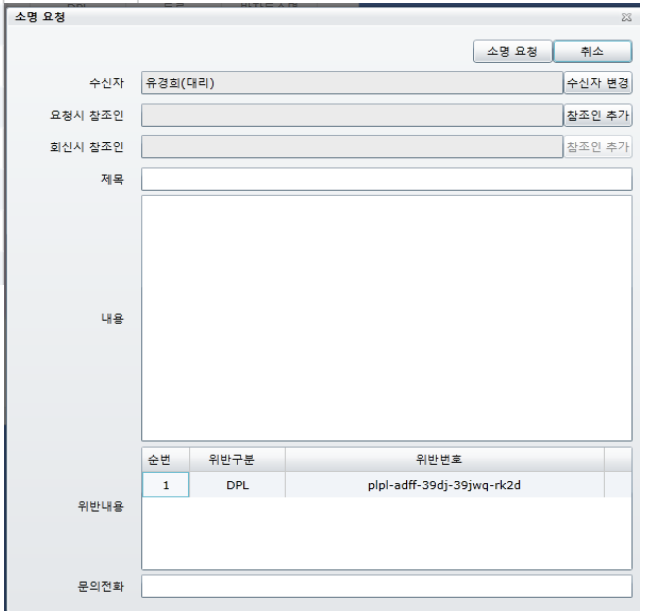
Anymon UBA는 소명 요청 기능 및 소명/통보 이력 관리 기능 등의 소명 처리 관리 기능을 지원합니다.

소명 처리 현황 화면

소명/통보 이력 관리

선택	순번	부서코드	부서명	사번	이름	직급	구분	위반구분	상태명	형태명	미요
☐	1	20050	경영기획부	003114	유경희	대리	1	DPL	소명완료	반자동소명	
☐	2	20050	경영기획부	003114	유경희	대리	1	DRM	소명요청	반자동소명	
☐	3	20050	경영기획부	003114	유경희	대리	1	DPL	소명완료		
☐	4	20050	경영기획부	003114	유경희	대리	1	DPL	소명요청		
☐	5	20050	경영기획부	003114	유경희	대리	1	DPL	등록		
☐	6	20050	경영기획부	003114	유경희	대리	1	DPL	소명완료		
☐	7	20050	경영기획부	003114	유경희	대리	1	DRM	소명완료		
☐	8	20050	경영기획부	003114	유경희	대리	1	DLP	소명완료		
☐	9	20050	경영기획부	003114	유경희	대리	1	DLP	소명완료		

소명 요청

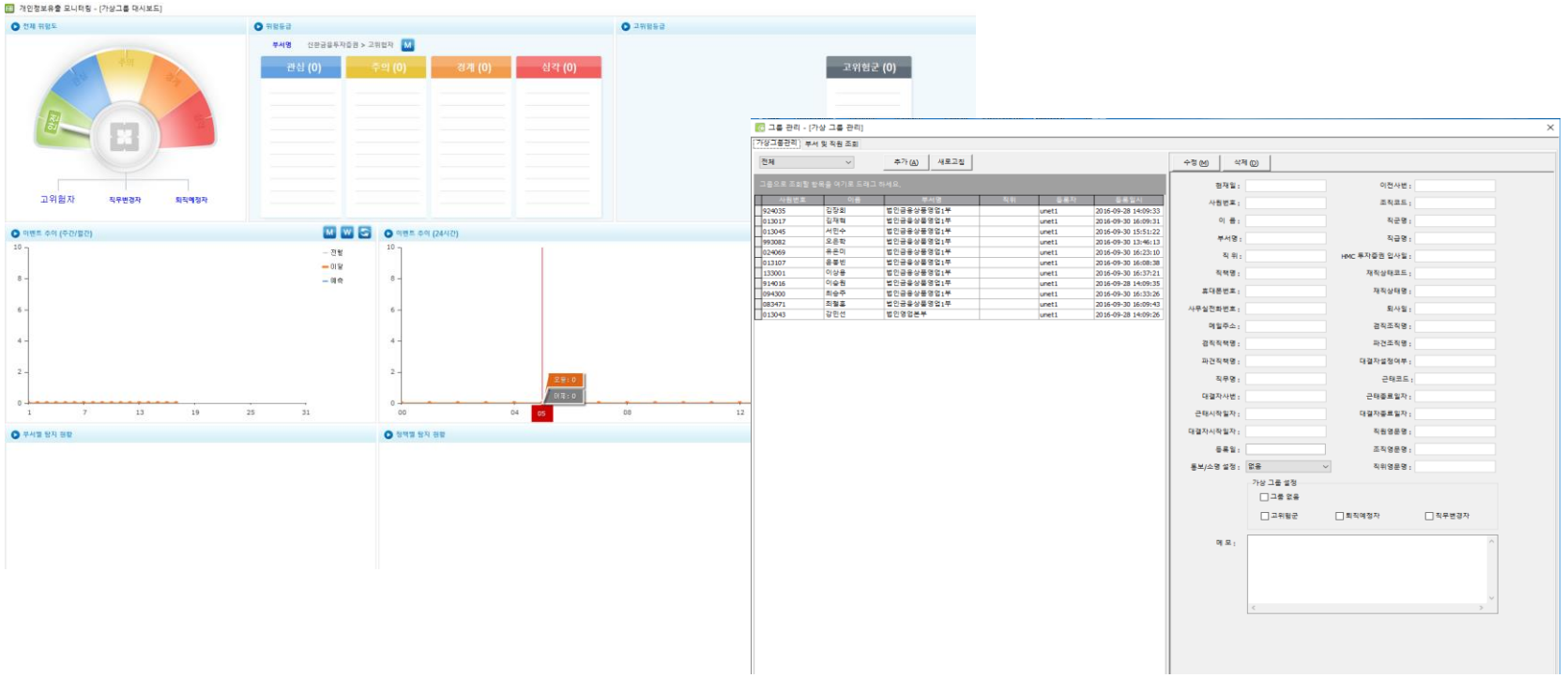


2.4 모니터링 기능

Anymon UBA는 고위험군에 포함되어 있는 직원의 현재 상태를 모니터링 할 수 있는 고위험군 관리 화면을 지원합니다.

고위험군 관리 화면 개발

고위험군 관리 화면



Ⅲ 특징 및 장점

1. 주요 특장점
2. 특허 출원 현황

1. 주요 특장점

1.1 Anymon UBA 특장점

- 다양한 로그 수집 및 사용자 행위기반 프로파일링 기법을 통한 다차원 분석을 통한 개인정보 유출탐지 솔루션

개인정보 유출 모니터링 시스템 특장점

- 내부정보 유출사고 발생시 분석·추적시간 단축
- 정규화된 통합시스템에서 분석, 키워드 검색을 토해 신속한 추적 (포렌직)

- 실시간 및 비실시간 상관분석을 통한 다차원 분석
- 시나리오 개선 기능을 통한 다양한 분석 지원

- 개인별 / 그룹별 / 중점관리 프로파일링
- 통계 및 교차 방정식을 이용한 정규화 지원

- 내부 및 외부 직원에 의한 정보유출 사고 사전예방 강화
- 고객정보의 기술적 안정성 확보하여 고객정보 유출 Zero화

1. 주요 특장점

1.2 대용량 데이터에 대한 신속한 검색 기능

대용량 데이터에 대한 신속한 검색 기능 (특허 보유)

[원본로그 파일]

세션 로그
- 날짜별
- 장비별

이벤트 로그
- 날짜별
- 카테고리별

[인덱스 파일]

- Clustered index 기법
- Nonclustered index 기법
- **Dictionary index 기법 (유넷시스템 특허 출원 12.07)**

• 초당 4만 EPS 처리 - **최대 90% 압축 저장 지원**

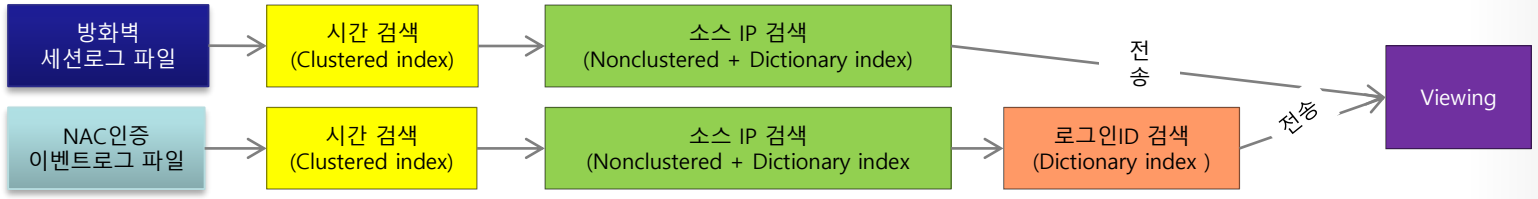
+

- 상관 분석을 통한 인시던트
  - 유해트래픽 분석
  - 멀티레벨 상관 분석
- 각종 통계 데이터
- 리포트 데이터

DB

검색 예시

• 조건 : 2015-10-10일 11시~12시, 로그카테고리(방화벽, NAC인증), 소스 IP, 특정로그인ID



POINT

• **Anymon UBA는 로그의 효율적인 분산 저장 · 분산 처리 · 최적의 인덱싱 처리 기술로 대용량 데이터에 대한 신속한 검색 기능을 제공합니다. 제안사는 수집/분석 성능 향상(인덱싱 기법 고도화)의 특허(사전 인덱스 기법에 의한 로그 검색 성능 향상)를 출원 하였습니다. (2012.07)**

2. 특허 출원 현황

2.1 특허 출원 현황

기술 특허 및 수상경력

등록일	등록번호	특허 (발명의 명칭)
2007.01.11	10-0671044	내부네트워크 상의 유해 트래픽 분석시스템 및 방법
2009.09.01	10-0916155	패킷캡쳐감사시스템 및 패킷캡쳐감사방법
2013.11.26	10-1335293	내부 네트워크 침입 차단 시스템 및 그 방법
2014.01.28	10-1358793	인덱스 파일 생성방법, 사전인덱스 파일을 이용한 데이터 검색 방법 및 데이터 관리 시스템, 기록매체
2014.09.02	10-1439130	장애 구간 탐지 시스템
2014.04.28	10-1391821	무선랜 관제를 통한 보안위협 탐지 시스템 및 방법
2013.11.07	10-1542534	이상 행위 판단 시스템
2013.11.07	10-1484290	통합 로그 분석 시스템
2011.07.08	10-2011-0067722	네트워크 보안시스템 및 네트워크 보안방법
2014.03.11	10-2014-0028216	로그 분석 시스템 검증장치
2014.03.18	10-2014-0031345	로그 분산 장치

IV 레퍼런스

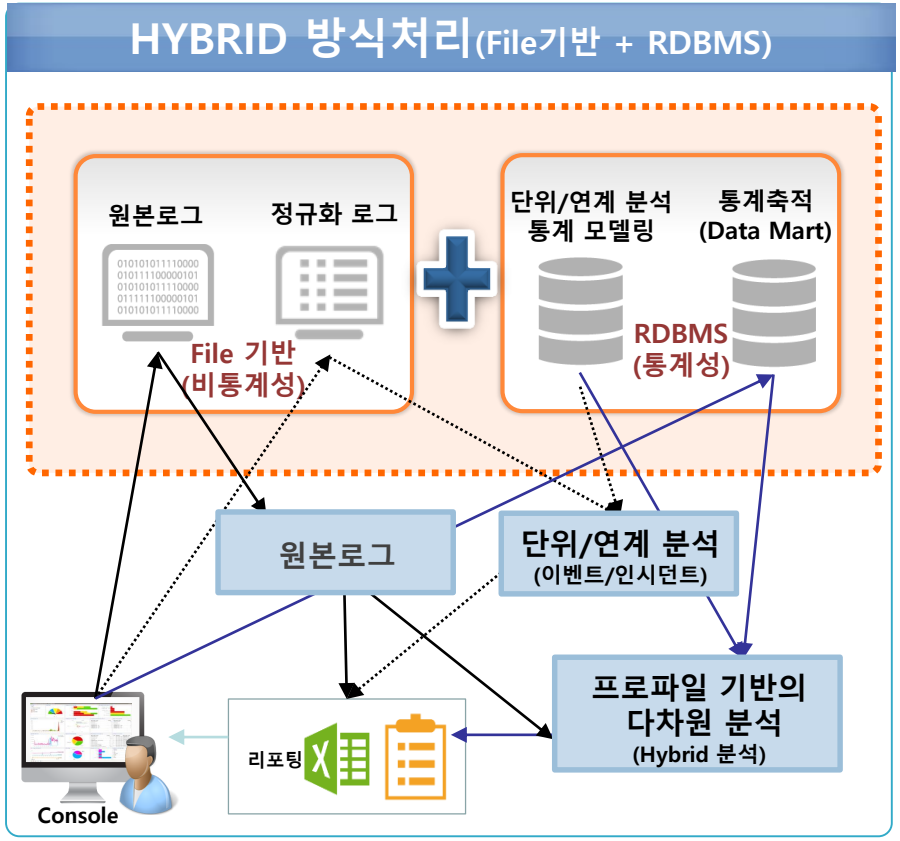
1. 구축사례

1. 구축 사례

1.1 주요 고객사 구축 사례

- 애니몬 UBA(User Behavior Analytics) 기반으로 개인정보 유출 모니터링 시스템 구성
- 소명요청 관리, 보안평가 기능 등 커스터마이징 정의 및 구현

구축사례(H증권)



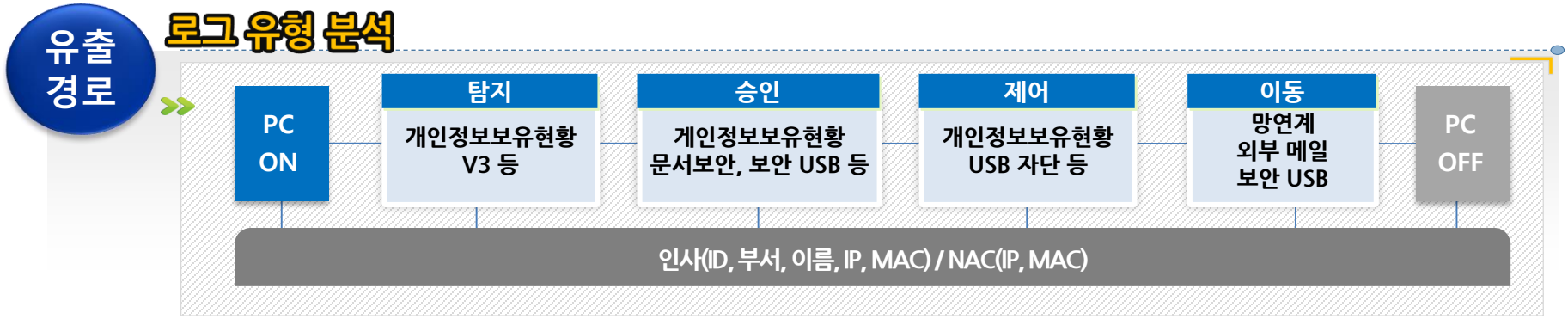
구분	커스터마이징 요구사항
퇴직(예정)자 및 특정직 무변경자 위반관리	▪ 인사로그, PC보안로그, 외부메일 승인로그 조합 ▪ 퇴직(예정)자 및 특정직무변경자 PC 또는 ID로 의심행위 발생 분석
소명요청 관리	▪ 이벤트 발생시 소명요청 (메일+그룹웨어 연동) ▪ 소명 현황 관리 ▪ 통보 현황 관리
개인정보 처리시스템 전수검사	▪ 시스템 화면별 개인정보 보유항목 전수검사 ▪ 점검결과를 지정된 양식에 저장

1. 구축 사례

1.1 주요 고객사 구축 사례

- 개인별 특성이 반영된 국내 금융기관 최초 프로파일링 기법을 활용한 개인정보 유출행위 탐지 및 대응

구축사례(W은행)



연락처 CONTACT US

회사

- 전화 : 02-2088-3030
- 팩스 : 02-2088-3031
- 이메일 : info@unet.kr
- 주소 : 서울 강남구 봉은사로 119 (논현동, 성옥빌딩 3층,7층)

영업

- 전화 (기업) : 070-8686-2170
  070-8686-2021
- 전화 (공공) : 070-8686-2015
  070-8686-2157
- 이메일 : sales@unet.kr

기술

- 전화 : 1661-3656
- 이메일 : support@unet.kr

THANK YOU