Anymon PLUS
제품 소개서

INSPIEN

INDEX

I

제조사 소개

1. 일반 현황 및 주요 연혁
2. 조직 및 인원 현황
3. 주요 사업 내용
4. 주요 사업 실적

1. 일반 현황 및 주요 연혁

인스피언은 2009년 설립된 이후 보안솔루션 및 SAP 컨설팅을 주 사업분야로 성장 하고 있으며, 2018년 통합로그관리/내부정보유출탐지 솔루션을 인수하여 빅데이터 기반의 보안 전문회사로 발전하고 있습니다.

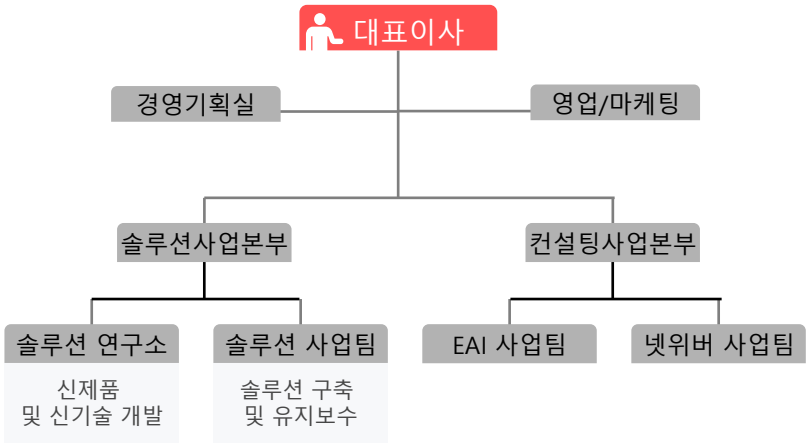
1. 회사명	인스피언 주식회사	2. 대표자명	최정규
3. 기술용역등록분야	소프트웨어자문, 개발 및 공급		
4. 주 소	서울특별시 금천구 벚꽃로 278 (가산동, SJ테크노빌) 1309호		
5. 연락처	전화번호 : 02) 857-8040 팩스번호 : 02) 857-8042		
6. 회사설립년도	2009 년 6 월		
7. 주요사업분야 (주력 사업 순서대로)	보안 솔루션 개발 및 납품, B2B/EAI 컨설팅 및 유지보수		
9. 인원현황	전체인원 : 53 명 / 관리 및 영업 : 5 명 / 컨설팅,개발 등 : 58 명		

10. 주요연혁(요약)

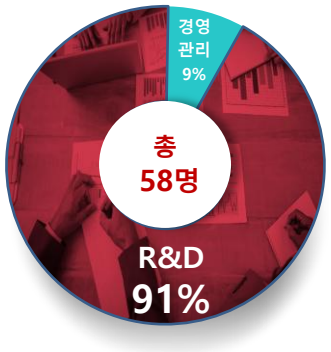
구분	연혁	비고
2018.10	◆ 통합로그관리/내부정보유출탐지 솔루션 사업부문 인수 (Anymon PLUS/UBA)	UNETSYSTEM
2015.11	◆ IBM Saas 파트너 등록 (SCN, 국내 유일)	
2013.11	◆ SAP Add-on 암호화 솔루션 EnDB for SAP 출시	
2013.09	◆ SAP 접근제어 솔루션 xCon for SAP 출시	
2012.11	◆ 기술연구소 설립	
2011.12	◆ 신기술 기반 벤처 기업 등록	
2010.09	◆ SAP DB 암호화 솔루션 SecureDB for SAP 출시	
2010.07	◆ 인스피언㈜ 사명 변경	
2009.06	◆ 엘엔씨홀딩스 설립	

2. 조직 및 인원 현황

조직 구성



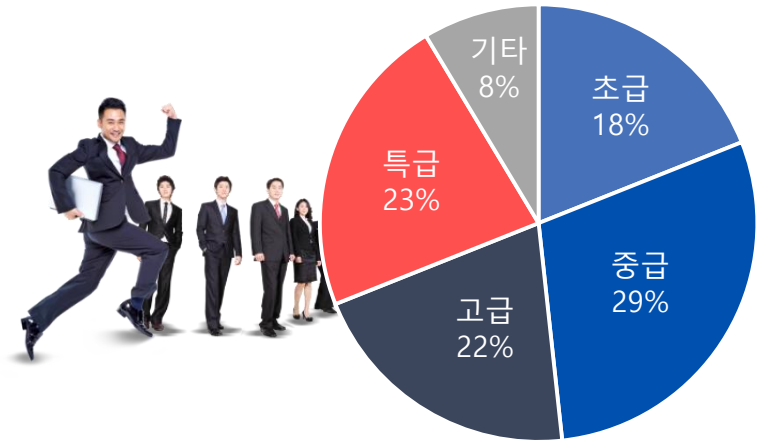
- 구성원의 90%이상 개발 및 기술 지원 인력
- 통합로그, DB보안, 접근기록의 요소 기술과 다양한 프로젝트 경험을 통한 Know-How 보유



기준일: 2018년 06월

연구개발 및 엔지니어
91%

인력구성 현황



기술등급	소계	전문분야			
		연구소	솔루션	컨설팅	영업/관리
특급기술자	13	3	4	6	-
고급기술자	12	2	5	5	-
중급기술자	17	3	5	9	-
초급기술자	11	2	2	7	-
기능사		-	-	-	-
기타	5	-	-	-	5
총계	58	10	16	27	5

3. 주요 사업 내용

인스피언은 보안 솔루션 전문 회사로 세계 최초로 SAP ERP를 위한 암호화, 접근제어, 개인정보 접속로그 솔루션을 개발한 해당 분야 시장점유율 1위의 보안 전문 회사 입니다. 또한 다년간의 보안 솔루션 개발 기술력을 바탕으로 100여개의 구축사례를 보유한 통합로그 솔루션을 인수하여 분석예측, 인공지능을 적용한 차세대 통합로그 관리 솔루션 시장으로 영역을 확장 하고 있습니다.

사업영역

빅데이터 보안

- **Anymon PLUS**
  - 
  - 통합로그관리
- **Anymon UBA**
  - 
  - 내부정보유출/ 이상징후탐지

SAP 보안

- **xCon**
  - 
  - SAP 접속기록 접근제어
- **SecureDB**
  - 
  - 시장점유율 1위 SAP 암호화
- **EnDB**
  - 
  - ABAP add-on SAP 암호화

컨설팅 서비스

EDI/B2Bi/EAI

- IBM Sterling
- SoftwareAG webMethods
- SAP PO (ProcessOrchestration)
- BizLink/BizConnector

SAP NetWeaver

4. 주요 사업 실적

일반기업, 공공 기관, 금융 기관 등 2018년 현재 230여 고객사의 대용량, 고성능 보안제품 적용 및 안정적인 운영 검증 하였으며, 국내 최대의 사이트인 삼성전자, 현대해상, 삼성생명, 삼성화재, 한국전력 등의 사례를 보유하고 있습니다.

주요 보안 프로젝트 수행 실적

'10~'12년 주요계약

- 삼성전자 G-ERP, 한국총괄 DB 암호화
- 제일모직 AFS,Retail.CRM,Chemical SAP DB암호화
- 한국수력원자력, 한국석유공사 DB암호화
- 호텔신라 SAP, Legacy DB 암호화
- 두산인프라코어, ㈜두산 암호화
- SK Telecom, SK Planet SAP DB암호화
- 롯데리아, 롯데 칠성주류 암호화
- LG 상사, LG인하원, LG패션 등 SAP DB암호화

'13~'15년 주요계약

- 한국철도공사 DB암호화
- 금호아시아나IDT SAP DB암호화
- LG생건, ㈜LG, LG하우시스, LG MMA DB 암호화
- 한전 KPS, 남부발전, 서부발전 DB암호화
- KBS SAP DB암호화
- 우리은행/국민은행/하나은행 통합로그 솔루션

'16~'18년 주요계약

- 수서 KTX, 한국 마사회 DB암호화
- 현대해상, 현대 엘리베이터 DB암호화
- 삼성생명, 삼성화재 SAP DB, Parameter 암호화
- 신용보증기금 통합로그 솔루션
- 현대건설기계, 현대엘렉트릭 DB암호화
- 한국원자력 환경공단 출입통제 암호화
- 두산공작기계 암호화
- 한국전력 키서버통합 및 ERP 암호화
- CJ오쇼핑, CJ헬로, CJ대한통운 DB암호화
- JT친애저축 통합로그 솔루션

II

통합로그관리 솔루션 개요

1. 법적 근거
2. 최신 보안 트렌드
3. 통합로그관리 솔루션 요구사항

1. 법적 근거

각종 장비 및 어플리케이션에서 발생하는 로그는 문제가 발생 할 시에 가장 기본적인 증거 자료 및 모니터링 자료로 활용이 되기 때문에 모든 보안 관련 법률 및 인증에서 필수로 남기도록 되어있습니다.

통합로그관리로 다양한 Compliance 만족

01 국내 법률

- 개인정보보호법
  - 접속기록 안전성확보 필요한 기술/관리/물리적 조치
  - 침해사고대응 위한 접속기록보관 & 위/변조 방지조치
- 정보통신망법
  - 접속기록의 위/변조 방지를 위한 조치 침해사고 원인분석 위한 접속기록 자료 보존 [5년]
- 전자금융거래 및 신용정보보호법
  - 전자금융거래 내용 추정/검색 또는 내용 오류 발생 시 확인 및 정정 관련 기록 생성 (최장 보존기간 5년)

02 해외 법률

- GDPR (EU)
  - Article 30 개인정보 처리활동의 기록 (Records of processing activities)
- '독일연방데이터보호법' 제3조 (독일)
- '미연방프라이버시법' 제552조의 2 (미국)
- '개인정보보호에 관한 법률' 제2조 (일본)
- '네트워크안전법 ' 제76조 (중국)

03 보안 인증

- ISMS
  - 8.1.3 보안로그 기능
  - 11.6.2 로그기록 및 보존
    11.6.3 접근 및 사용 모니터링
- SOC 2,3
  - The entity monitors the system and takes action to maintain compliance with its defined confidentiality policies (보안 이벤트의 정의 및 모니터링)
- ISO27001
  - 12.4.1 Establish information security event logs (보안이벤트 로그 확립)
  - 12.4.2 Protect logging facilities and log information (로그정보 안전하게 저장)
  - 16.1.7 collect evidence to document incidents and responses (증거수집)

2. 최근 보안 트렌드

단위 시스템에서 발생된 로그를 통합 하고 법적 근거를 제공하던 통합로그관리 솔루션은 최근 들어 데이터의 다양화 및 대량화 추세에 따라 빅데이터 기반의 분석 시스템으로 발전 하고 있습니다. Application, 보안, IT 기반의 다양한 로그를 종합 분석하여, 이상징후탐지 및 내부정보유출 모니터링 등의 기능을 요구 합니다.

	1960 ~	2000 ~ 2006	~ Current
용도	• IT 단위시스템 로그통합 및 장애처리 모니터링용 활용	• ITA시스템과 보안시스템의 연계분석을 통한 보안관제용으로 활용	• ESM 기능을 포함, Application 연계를 통한 종합분석으로 활용
분석영역	• IT 시스템 위주의 통합 및 분석 중점	• IT + 내부 보안영역 전체에 대한 알려진 보안위협(상관) 분석에 중점	• 알려지지 않은 보안 위협(상관) 분석 • 이상징후 탐지, 내부정보 유출모니터링

3. 통합로그관리 솔루션 요구사항

빅데이터 기반의 통합로그분석 솔루션

손실 없는 데이터 수집/저장	데이터 검색 및 모니터링의 편의성	예측 및 분석을 통한 위협 탐지
• 다양한 원시로그에 대한 정규화 기능 • 대용량 데이터를 처리하는 능력 • 저장방식과 통계방식으로 구분	• 데이터 처리분석 및 시각화 표현 기술 • 사용자 요구를 적극 반영할 수 있는 유연한 대시보그 구조	• 유해 트래픽 분석을 통한 위협 탐지 • 사용자 행위 분석을 통한 예측 값으로 실시간 탐지 • 통계 처리 분석/모델링 예측 등
수집 기술	**표현 기술**	**분석 기술**

통합로그관리 측면 요구

원인추적 등 감사 | **로그 수집 및 저장**

- 정보시스템에서 생성되는 다양한 로그를 수집, 저장해서 필요한 정보를 검색, 보고서를 생성하여 IT 인프라 상태와 사용 현황 제공
- 장애나 보안사고 발생 시 로그를 통해 원인을 추적
- 각종 규제 및 법규에 대한 감사자료로 활용

위험관리 측면 요구

실시간 보안위험 관리 | **보안 이벤트 관리**

- 수집된 보안로그를 통해 보안 이벤트를 생성, 취합 및 분석 등의 관리
- 구축된 여러 보안 시스템에서 발생하는 로그를 취합하고, 상호연관성을 분석함으로써 실시간으로 보안 위협을 파악 및 대응
- 임계치 기반 탐지에서 발생하는 오탐/과탐에 대한 대응

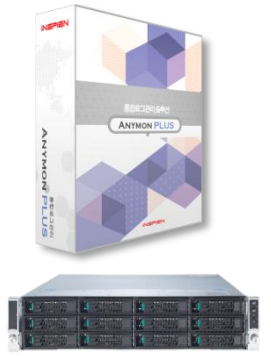
III 제품 개요

1. 솔루션 개요
2. 시스템 구성도
3. 제품의 특징 및 장점
4. 보유기술 및 특허

1. 솔루션 개요

빅데이터 기반의 통합로그분석 솔루션인 애니몬 Plus의 개요는 다음과 같습니다.

제품 개요

구분	내용	제품사진
제품명	애니몬 Plus	
제조사	인스피언 주식회사	
용도	통합로그분석 시스템	
제품 구성	Appliance	
환경	Windows Server	
제품 개요	• 다양한 형태, 시스템의 로그수집 기능 제공 (Agent, Agentless) • 대상 로그의 위·변조 없이 실시간 수집 및 기록, 저장 기능 제공 • 로그 데이터의 압축/암호화 저장 기능 제공 • 실시간 멀티레벨 / 시나리오 상관분석 • 사용자 행위 분석을 통한 예측 값으로 실시간 탐지	

제품 사양 및 규격

품명	규격	용량
 Anymon PLUS STD3	• Intel Xeon Processor 3.5GHz 4C • MEM : 16GB • SSD : 240GB x 3EA • HDD : 8TB • NIC : 1G Support 조달 등록	10G/ Day
 Anymon PLUS MID3	• Intel Xeon Processor 1.7GHz 8C • MEM : 32GB • SSD : 240GB x 3EA • HDD : 8TB • NIC : 1G Support 조달 등록	30G/ Day
 Anymon PLUS ADV3	• Intel Xeon processor 1.7GHz 8C x 2EA • MEM : 64GB • SSD : 240GB x 2EA, 480GB x 2EA • HDD : 16TB • NIC : 1G Support 조달 등록	50G/ Day
 Anymon PLUS PRM3	• Intel Xeon processor 2.1GHz 8C x 2EA • MEM : 128GB • SSD : 240GB x 2EA, 960GB x 2EA • HDD : 20TB • NIC : 1G Support	100G/ Day

※ HW 사양은 제조사 정책에 따라 변경 될 수 있음

2. 시스템 구성도

애니몬 Plus는 로그의 수집, 저장, 분석을 담당하는 Anymon Server 와 조회/관리를 위한 Anymon Console로 구성됩니다. Anymon Server는 서버의 역할에 따라 로그의 수집을 담당하는 Site Manager 와 각 Site Manager를 통합관리 하는 Center Manager로 구성되며, 발생 로그양에 따라 병렬로 Site Manager을 증설 할 수 있습니다.

로그 & 이벤트 처리 프로세스

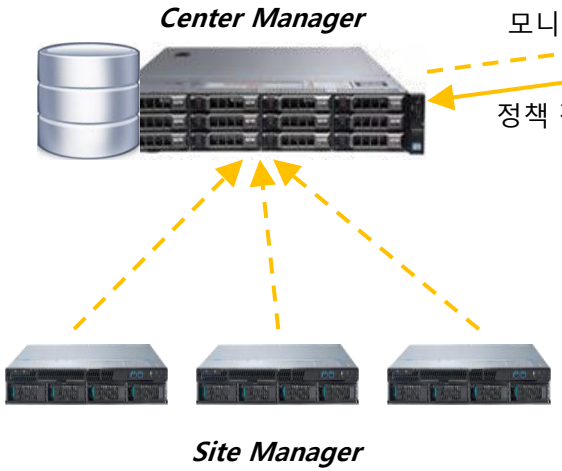
정보 생성 장비

- Syslog, SNMP trap 제공하는 모든 장비
- 필요 시 Adapter 제공
- FW, IPS 등 보안장비
- 스위치 등 네트워크 장비
- 서버 운영체제 로그
- 어플리케이션 데이터

로그/이벤트 수집
Syslog, SNMP Trap, log file, Net Flow...

Anymon Server

- Anymon PLUS Center Server / Site Server
- 로그/이벤트 수집, 저장
- 상관분석
- 통계데이터 생성
- 데이터 수집, 저장, 검색 모듈



Anymon Console

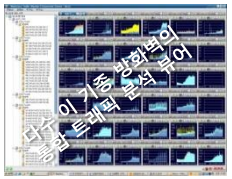
- 로그/이벤트 모니터링
- 원시 데이터 조회 및 분석
- 연동 시스템 관리

3. 제품의 특징 및 장점

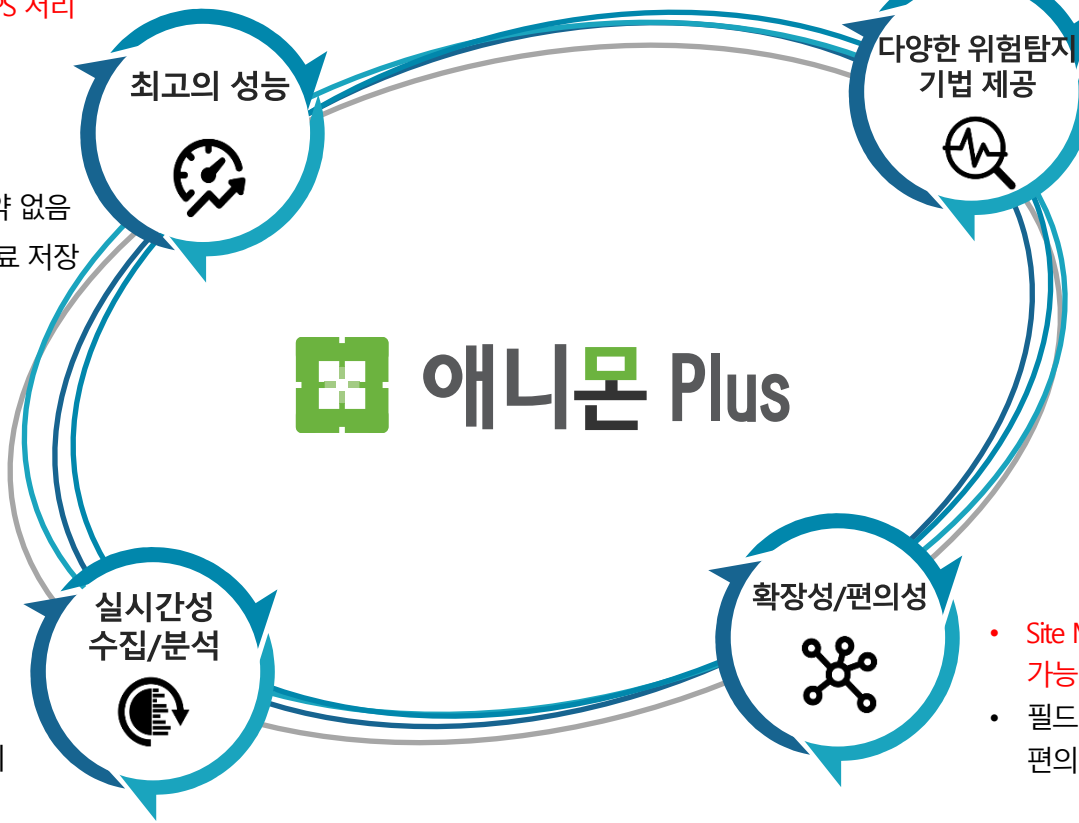
애니몬 Plus는 단일장비에서 60만 EPS를 처리할 수 있는 업계 최고의 성능을 보고 하고 있으며, 다양한 기법의 위험탐지 정책으로 실시간 위험을 탐지 합니다.

특징 및 장점

- PRM급 적용 시 단일 장비 60만 EPS 처리 가능 (TTA 시험결과)
- SPRM 급 적용 시 매니저 서버당 500GB/일 처리 보장
- 매니저 병렬 구성 시, EPS처리 제약 없음
- 피크타임 로그 유실 없이 증적 자료 저장



- 각 장비의 트래픽 및 이벤트 로그 실시간 통합 수집
- 세션(방화벽/웹)기반의 5초 단위의 실시간 트래픽 모니터링



- 유해 트래픽/멀티레벨/시나리오 기반 상관분석 기능 제공
- NBA기반의 미지의 Zero-day worm 대응 기능 제공

- Site Manager 병렬 무 중단 확장 가능
- 필드 선택 기반의 직관적인 UI 편의성 제공

4. 보유기술 및 특허

기술 특허

제10-0671044호_내부네트워크 상의 유해 트래픽 분석 시스템 및 방법

제10-1439130호_장애구간탐지시스템

제10-1557856호_로그분석시스템 검증장치

제10-1358793호_인덱스파일생성방법,사전인덱스파일을 이용한데이터검색방법 및 데이터관리시스템

제10-0916155호_패킷캡쳐감사시스템 및 패킷캡쳐감사방법

제10-1484290호_통합로그분석시스템

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
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
2013.11.07	10-1484290	통합 로그 분석 시스템
2014.03.11	10-1557856	로그 분석 시스템 검증장치

4. 보유 기술 및 특허

인증

CC인증


인 증 서

ISIS-0336-2011

Anymon PLUS V3.0

- 신청기관: 인스피언㈜
- 제품유형: 통합로그관리
- 제품버전: 버전 3.0
- 인증보고서번호: CR-11-44
- 보증등급: EAL 2
- 인증일 : 2011년 10월 07일

IoT인증


nca 정부통합전산센터

- 제품명: Anymon PLUS 10000
- 장비분류: 통합로그관리시스템
- 인증 항목: 수집 및 검색 기능 등 15개 항목
- 인증연월일: 2010년 12월 14일
  ※ IOT 인증 통과한 제품에 대해 대전통합 전산센터납품 가능

GS인증


소프트웨어품질인증서

Certificate of Software Quality

- 신청기관: 인스피언㈜
- 소프트웨어 명칭 : 애니몬 플러스 V3.0
- 인증번호: 15-0296
- 인증일 : 2015년 09월 02일

IV 주요 기능

1. 주요 기능
2. 세부 기능

1. 주요 기능

§ Syslog, SNMP TRAP, Logfile 등의 프로토콜을 통한 로그 수집 (로그 전송이 제한되는 장비의 경우 Agent를 통해 수집)

§ 통신장애 등에 의해 연결 단절 시 10초 단위로 서버와의 통신을 시도하여 연결되는 즉시 축적된 로그 재 수집

§ 매니저서버당 최대 600,000 EPS(Event/sec) 성능 제공

§ 연동 장비별 정규화를 위한 "패턴파일" 기본 제공 및 신규로그를 위한 정규화 기능 제공

§ Binary 형태의 축약한 데이터 및 원시 데이터 저장

§ 수집 로그에 대해 기밀성(암호화) 및 무결성(해시) 지원

§ 관리 주기에 의한 자동 데이터 삭제 기능

§ Zoom-in 방식의 로그 분석 기능

§ 다양한 필드에 의한 다각적인 분석 기능 지원

§ 멀티 레벨 상관분석

§ 동일/유일 조건 설정 기반 상관분석

§ 사용자의 행위분석을 통한 예측값으로 실시간 탐지

§ 시간에 따른 시나리오 기반 복합 분석

§ 각각의 장비에서 수집된 이벤트 및 로그 실시간 모니터링 제공

§ 사용자 정의 대시보드를 통한 직관적인 화면 구성

§ 사용자 정의 통계 & 검색 오브젝트 모니터링

§ 사건에 연관된 이벤트 만을 별도 관리하여 보고서 생성

§ 기본 제공(60여개) 보고서 제공

§ 보고서 형식: PDF, XLS, DOC

§ 관제 이벤트 티켓 발급 및 처리

2.1 로그 수집

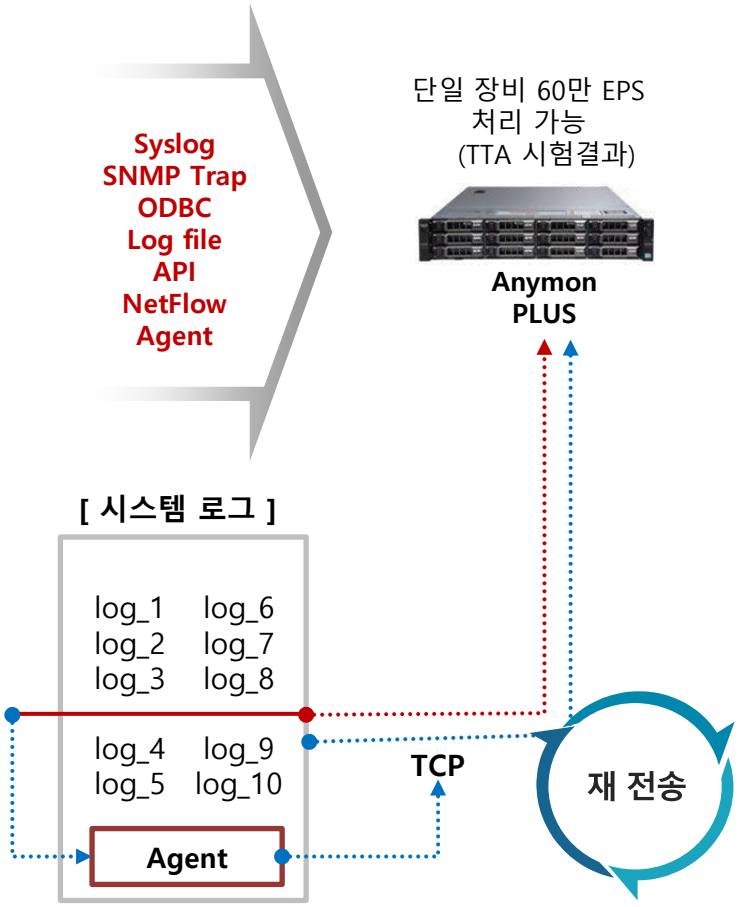
애니몬 PLUS 통합로그관리 솔루션은 다양한 시스템 및 매체로 부터 대용량의 각종 로그를 수집 통합관리 합니다. 로그 수집을 위해 대상 시스템의 유형에 따라 에이전트 방식, 비 에이전트 방식을 지원 합니다. 에이전트 방식 사용 시 통신장애 등에 의해 연결 단절 시 10초 단위로 서버와의 통신을 시도하여 연결되는 즉시 축적된 로그를 전송합니다.

수집 대상

네트워크	DB	보안장비
L4,L3, 라우터, X.25	Oracle MS-SQL	방화벽, IPS, DDOS, WAF, SSL VPN, PC보안, 웹키퍼, 백신, IP관리, DB접근통제, DB암호화, 서버보안, 출력물 보안
DB	**DB**	
WAS, WEB, MCI, EAI, SSOEAM, APM, 형상관리, 배치 스케줄러, 백업로그	AIX 계열 Linux 계열 Windows 계열	

수집 데이터

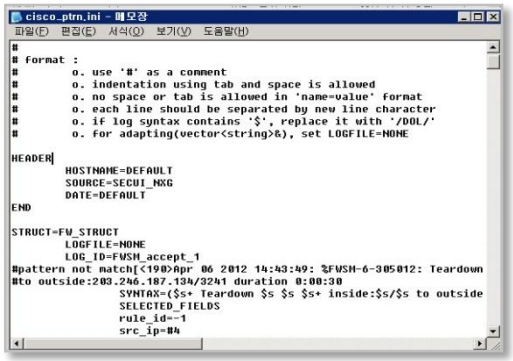
구분	지원방법
Agentless	Syslog, SNMP trap, ODBC, NetFlow, API 등을 통한 수집
Agent	로그수집대상 서버 자체적으로 저장된 logfile 수집



2.2 로그 저장

수집된 원시로그는 연동 장비 별로 제공되는 "패턴파일"를 이용해서 정규화를 수행하며, 신규 형식의 로그는 정규식 필드 추출 기능을 사용해서 " 패턴파일 " 을 생성 할 수 있습니다. 원시 로그는 최대 90% 압축으로 저장 되며, 암호화 기능 (기밀성) 및 원본 로그 파일에 대해 해시 알고리즘 수행을 통한 무결성을 지원합니다

정규화

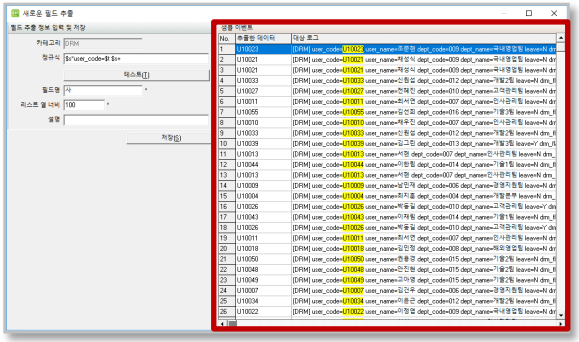


연동 장비별 패턴 파일 기본 제공

- 연동 장비별 "패턴 파일" 제공
- 별도의 수정 없이 정규화 처리 지원

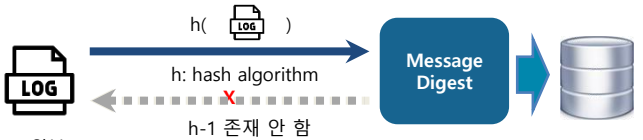
정규식 형태로 필드 추출 기능

- 신규 형식의 로그의 경우 정규식으로 필드 추출 기능을 제공하여 신규 "패턴 파일" 생성



저장 데이터 압축 (최대 1/10 수준)

암호화 저장 ('SHA-256' 사용)



기밀성

- 수집되는 원본 로그 건 당 실시간 암호화하여 저장 지원.
- 128bit SEED 적용, 암・복호화 처리를 통한 기밀성 지원

무결성

- 원본 파일 생성이 종료되는 시점에 원본 로그에 대한 해시 알고리즘 수행을 통한 무결성 지원
- Worm 스토리지 지원으로 HW적인 데이터 무결성 또한 선택적으로 지원

2.3 로그 검색/분석

애니몬 Plus는 로그의 효율적인 분산 저장 · 분산 처리 · 최적의 인덱싱 처리 기술로 대용량 데이터에 대한 신속한 검색을 지원 합니다.
(초당 1억건의 데이터 검색 지원)

대용량 데이터에 대한 신속한 검색 기능 (특허 보유)

[원본로그 파일]

세션 로그
- 날짜 별
- 장비 별

이벤트 로그
- 날짜 별
- 카테고리 별

[인덱스 파일]

- Clustered index 기법
- Nonclustered index 기법
- **Dictionary index 기법 (인스피언 특허 등록 14.01)**

• 초당 4만 EPS 처리 - **최대 90% 압축 저장 지원**

상관 분석을 통한 이벤트
- **유해트래픽 분석**
- **멀티레벨 상관 분석**

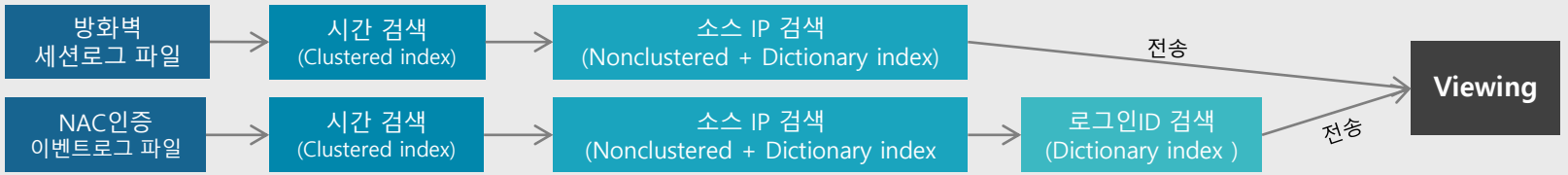
각종 통계 데이터

리포트 데이터

DB

검색 예시

• 조건 : 2019-01-17일 11시~12시, 로그카테고리(방화벽, NAC인증), 소스 IP, 특정로그인ID

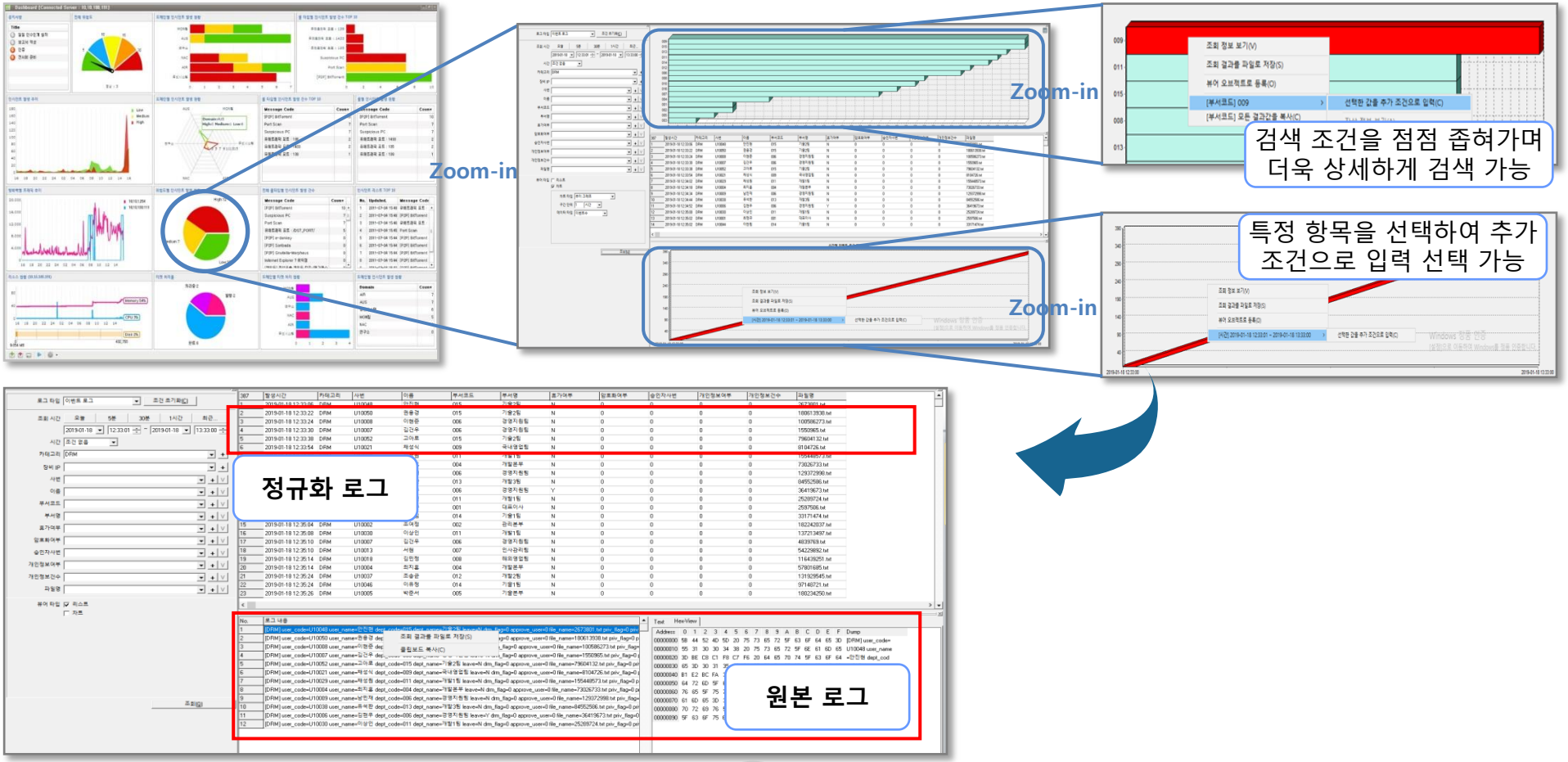


애니몬 PLUS는 수집/분석 성능 향상(인덱싱 기법 고도화)의 특허(사전 인덱스 기법에 의한 로그 검색 성능 향상)를 등록 하였습니다. (2014.01)

2.3 로그 검색/분석

수집 및 정규화 된 로그는 Zoon-In 기능을 (Depth Searching) 사용하여 검색 범위를 더욱 상세하게 조회 하거나, 특정 항목을 추가조건으로 입력하여 원하는 최종 로그를 빠르게 조회 할 수 있습니다. 최종 검색된 로그는 정규화 로그 와 원시 로그를 한 화면에서 1:1 매핑으로 볼 수 있는 통합 View를 제공 합니다.

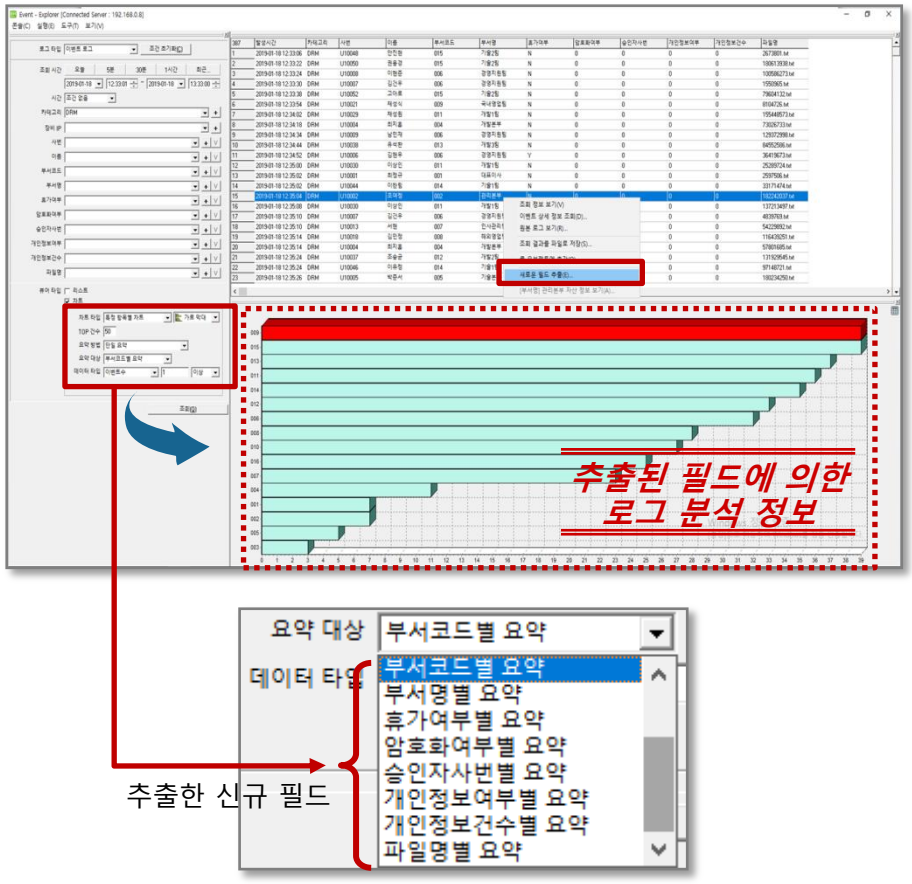
Zoon-In 기능을 사용한 로그 상세 검색

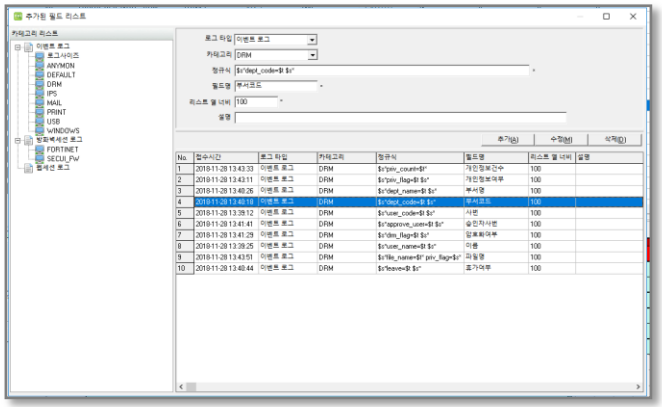


2.3 로그 검색/분석

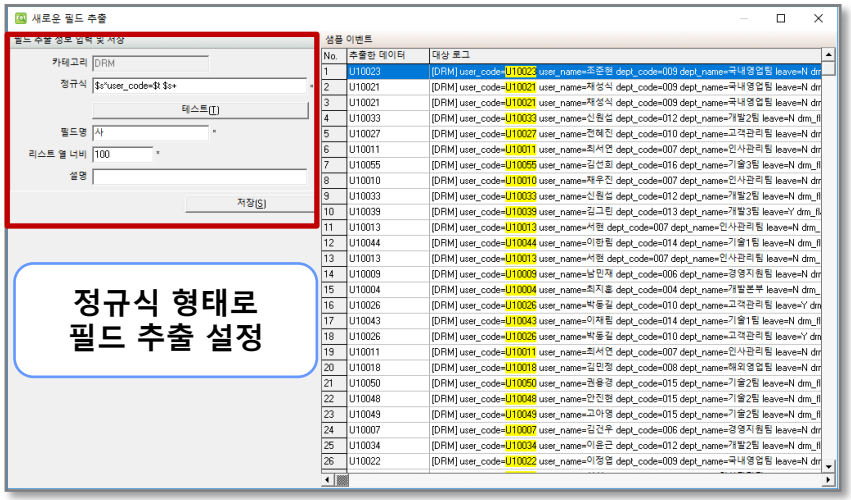
서로 다른 로그의 포맷이라도 필드 추출 기능을 통하여 수집된 데이터에 대해 유연하고 효율적인 분석 기능을 제공합니다. 또한 일시, 소스/목적지 IP, 포트, 프로토콜 등 기본적인 필드를 제공하며, 기 정의된 필드 외 사용자 정의에 의한 필드 추출 설정을 통하여 다양한 필드에 의한 다각적인 분석 기능을 지원합니다

다양한 필드에 의한 다각적인 분석 기능 지원





추출한 필드 리스트

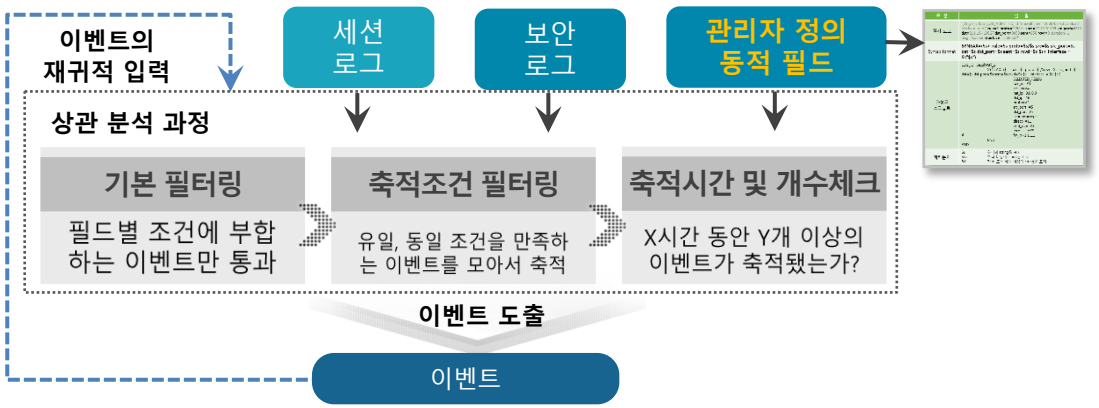


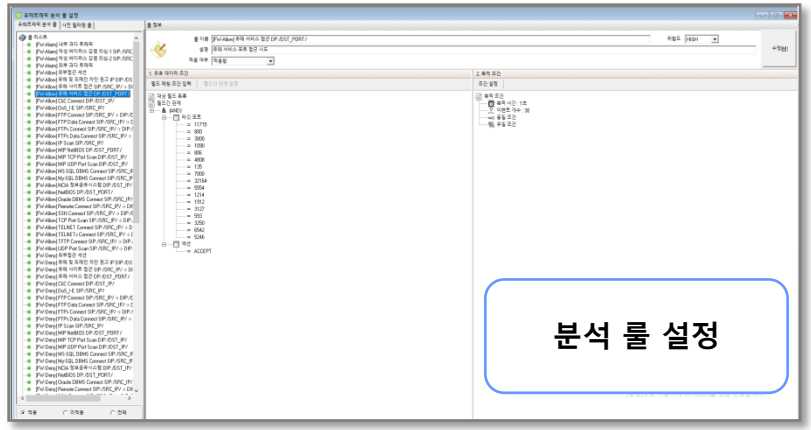
정규식 형태로
필드 추출 설정

2.3 로그 검색/분석

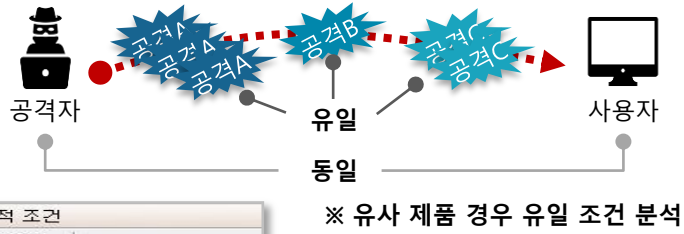
수집되는 로그에 대해 다양한 동일/유일 조건 및 재귀적 상관 분석 기술을 적용한 "분석 Rule"를 적용하여, 실시간 유해 트래픽을 감지 합니다. 감지된 유해 트래픽은 인시던트 모니터링 기능을 통해서 조회 및 분석을 수행 합니다.

멀티 레벨 상관분석



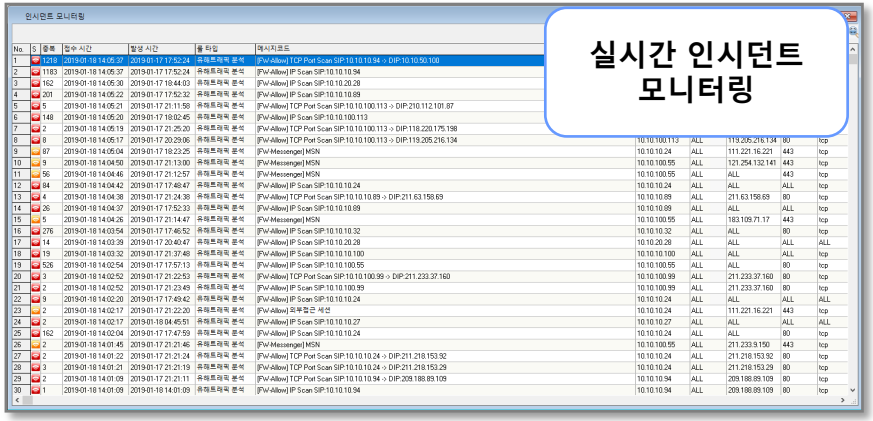


동일/유일 조건 설정 기반 상관분석



※ 유사 제품 경우 유일 조건 분석 한계 존재

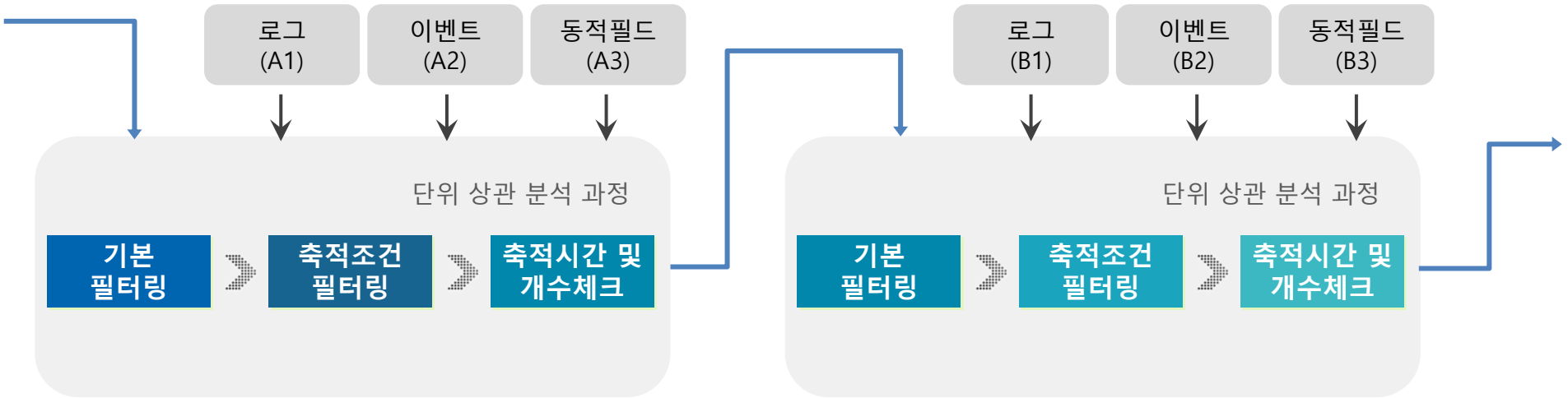
◀ 24시간(1일) 동안 소스 IP와 타깃 IP가 동일하고, 공격 코드가 유일한(서로 다르면서 중복을 제외한) 3개의 이벤트발생 시 이벤트 발생



2.3 로그 검색/분석

상관 분석 결과를 포함하는 재귀적 분석 기술로 침입경로 또는 유출경로에 따라 시간 순으로 발생되는 로그/이벤트에 대한 최적화된 분석 기법을 제공 합니다.

시간에 따른 시나리오 기반 복합 분석



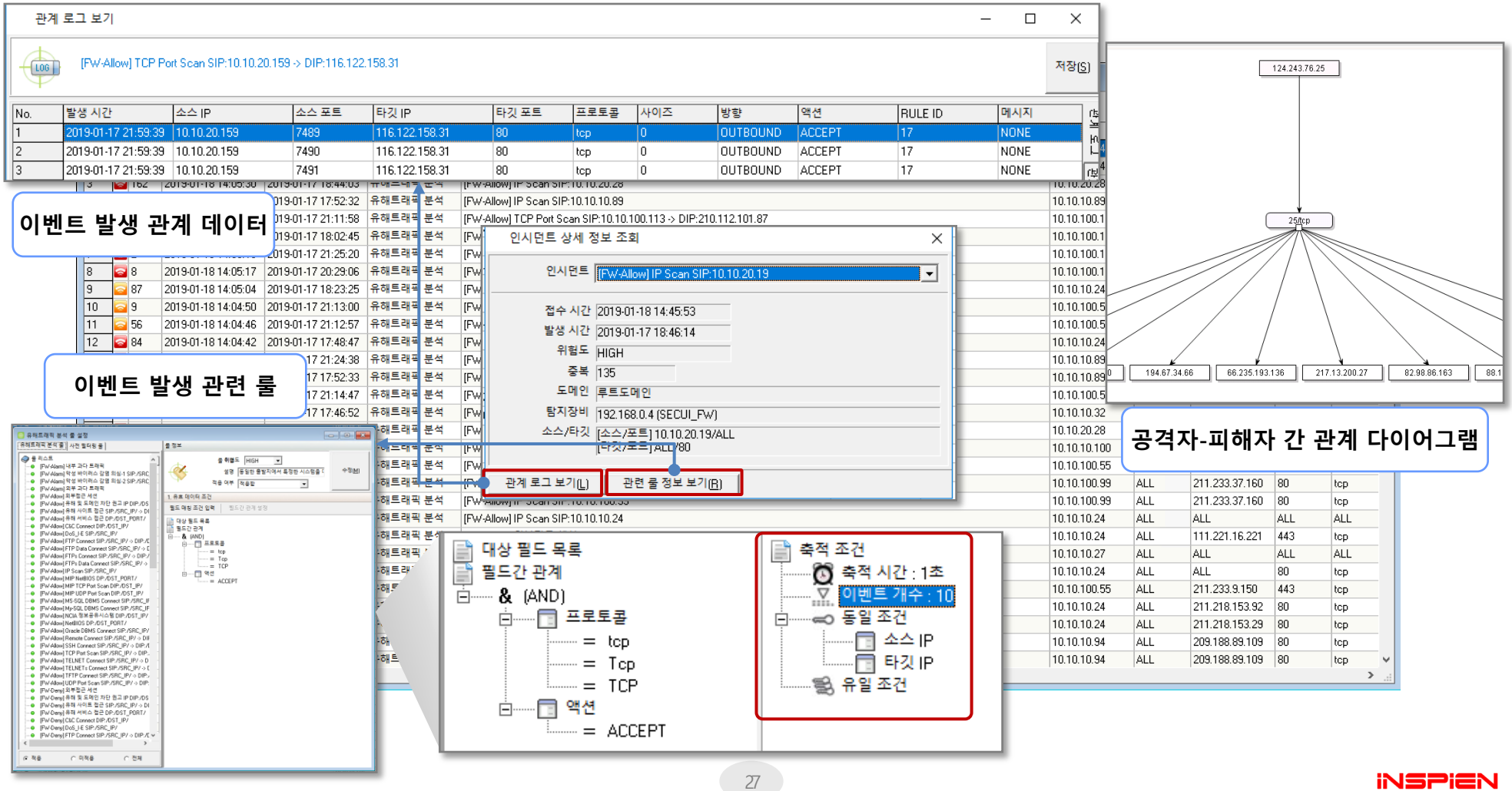
- **1일 100회 이상 접속 동일 인터넷 구간 IP를 대상으로**

- **개인 정보 조회 SQL이 포함되어 있고**
- **결과가 Web Mail로 전송된 단말의 IP 주소**

2.3 로그 검색/분석

방화벽 및 웹 로그세션의 NBA(Network Behavior Analysis) 기반 유해 트래픽 분석 으로 불특정 Zero-day worm 등 보안 위협 대응 기능을 제공 합니다.

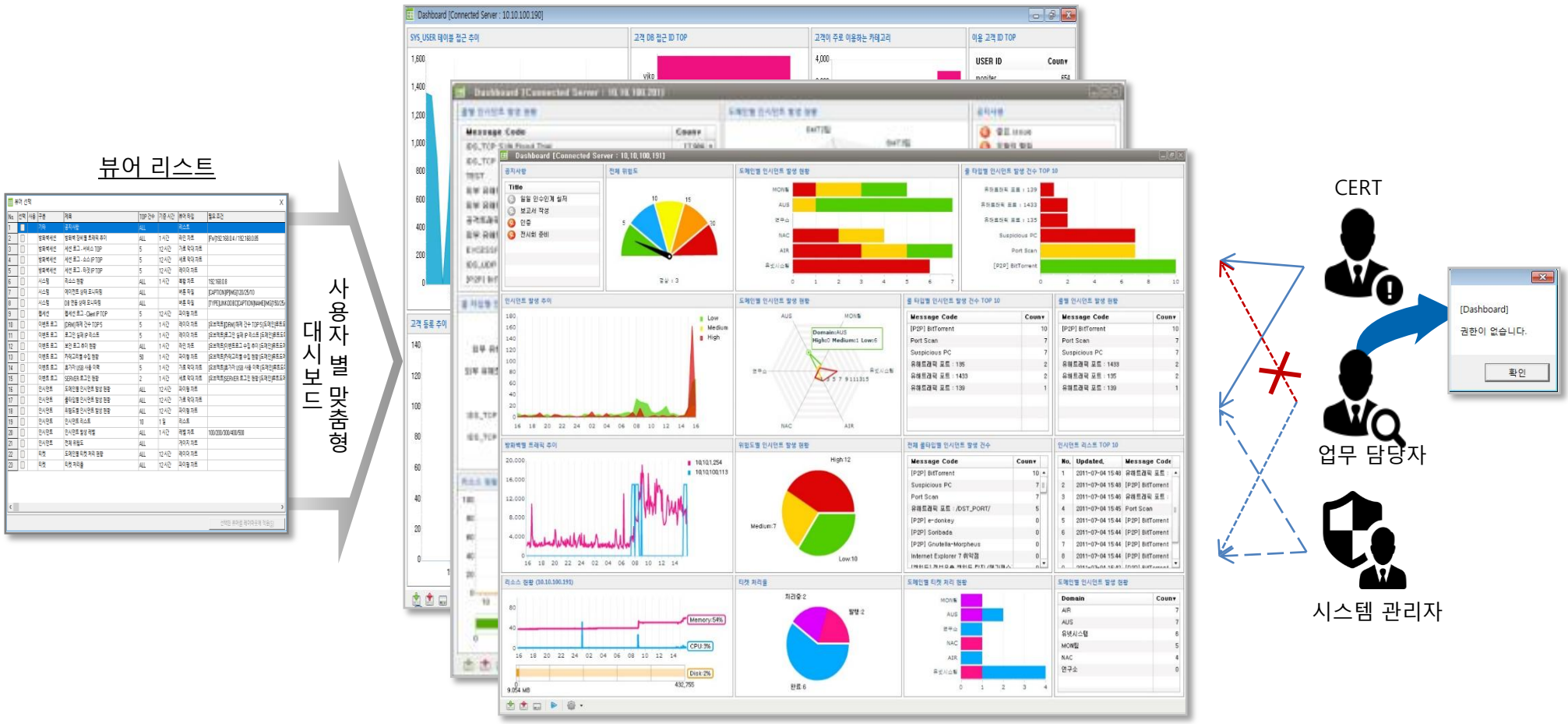
유해 트래픽 분석으로 보안 위협에 대해 신속한 대응 가능



2.4 모니터링/리포팅

트래픽, 이벤트 및 리소스 현황 등 종합적이고 일원화된 보안 관리 가능하도록 고객사 특성에 맞춘 통계 및 대시보드 기능을 제공 합니다. 사용자 별 맞춤형 대시보드는 보유 권한에 따라 사용 가능한 대시보드만을 접근 할 수 있습니다.

고객사 특성에 맞춘 통계 및 대시보드

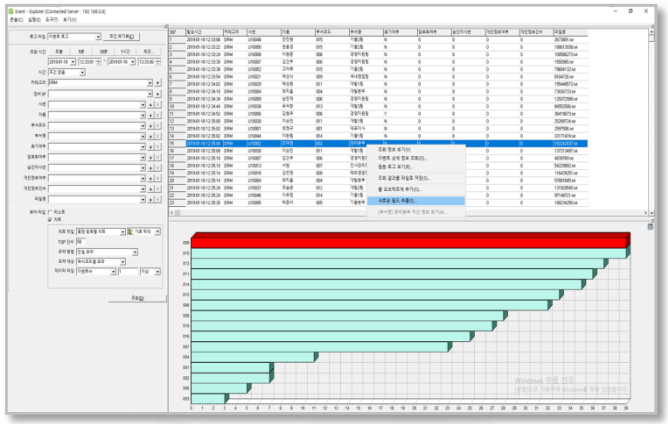


2.4 모니터링/리포팅

대시보드에 표현될 뷰는 기 정의된 28개의 기본 통계 리스트 정보를 제공하며, 각종 검색 화면을 통한 결과값을 이용하여 사용자 뷰를 자동 생성 합니다. 생성된 뷰는 다양한 설정 기능을 이용하여 사용자 맞춤형 대시보드를 구성 합니다.

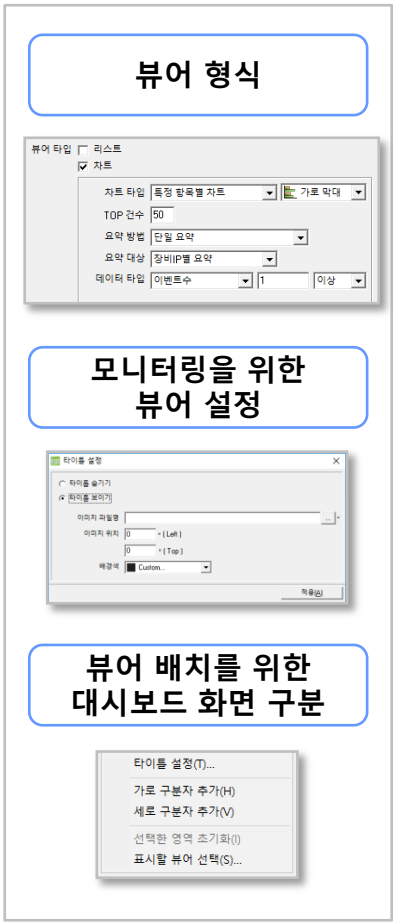
데이터 결과를 이용한 대시보드 뷰 자동 생성

검색 결과

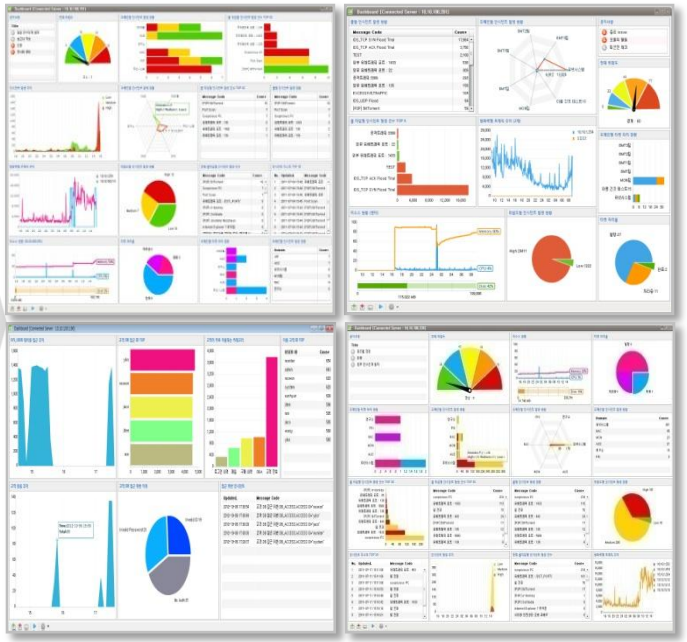


뷰 생성

뷰 설정 조정



대시보드 생성

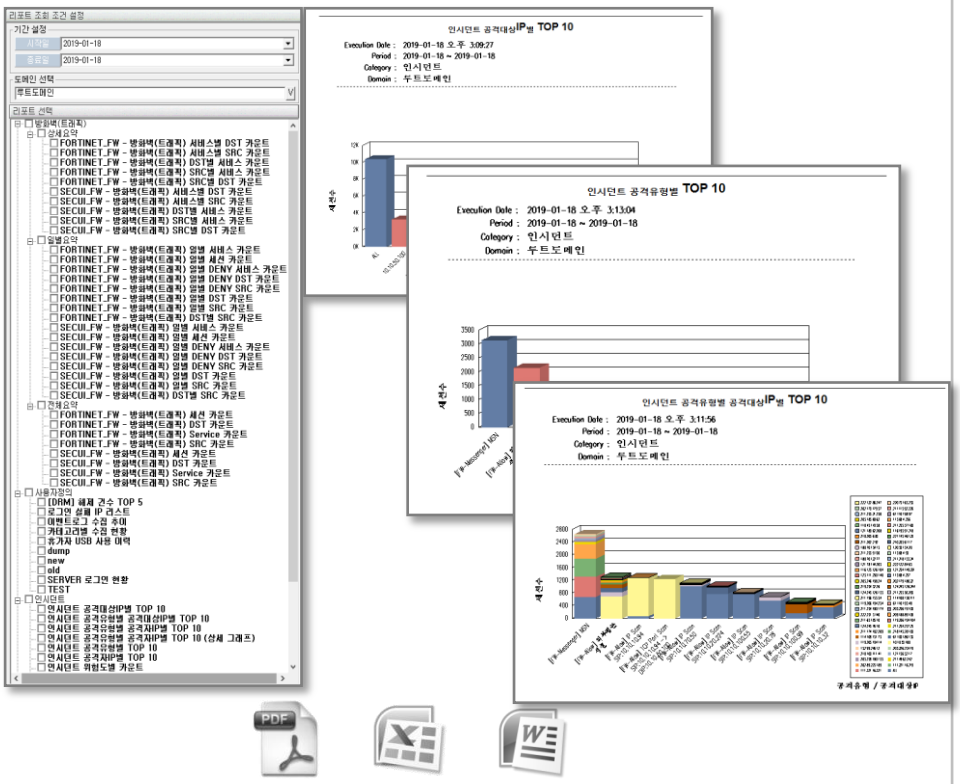


2.4 모니터링/리포팅

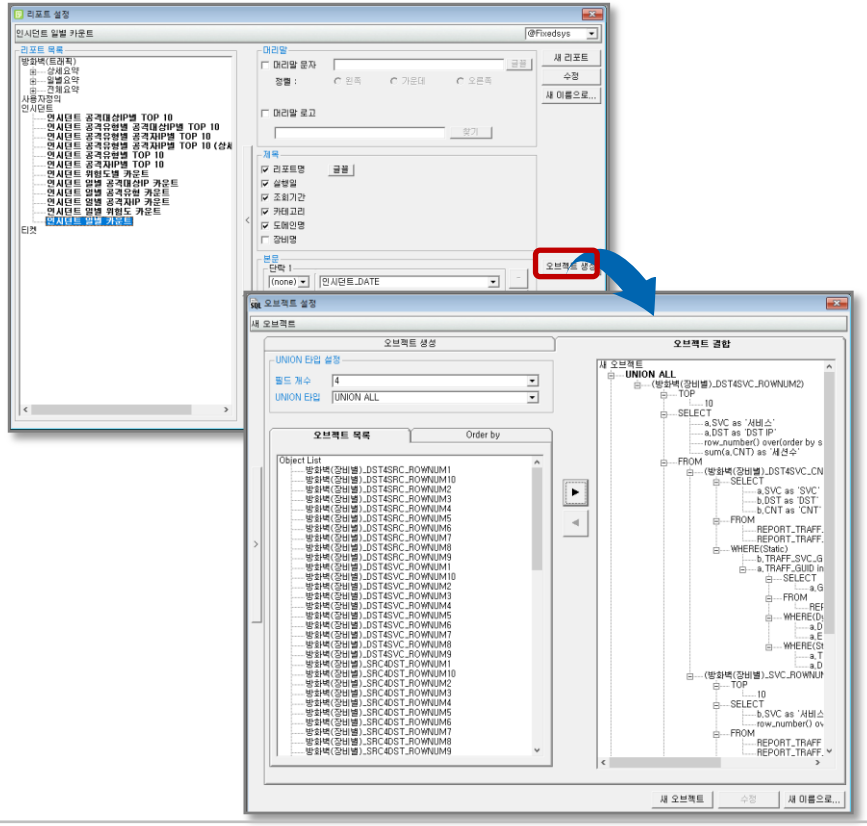
PDF, XLS, DOC 형식 등 60여 개 기본 보고서를 제공하고 있으며 기본 제공 보고서 외 사용자 정의 보고서 생성 기능을 보유하고 있습니다.

다양한 형식의 보고서 제공

기본 보고서 제공



사용자 정의 보고서 제공

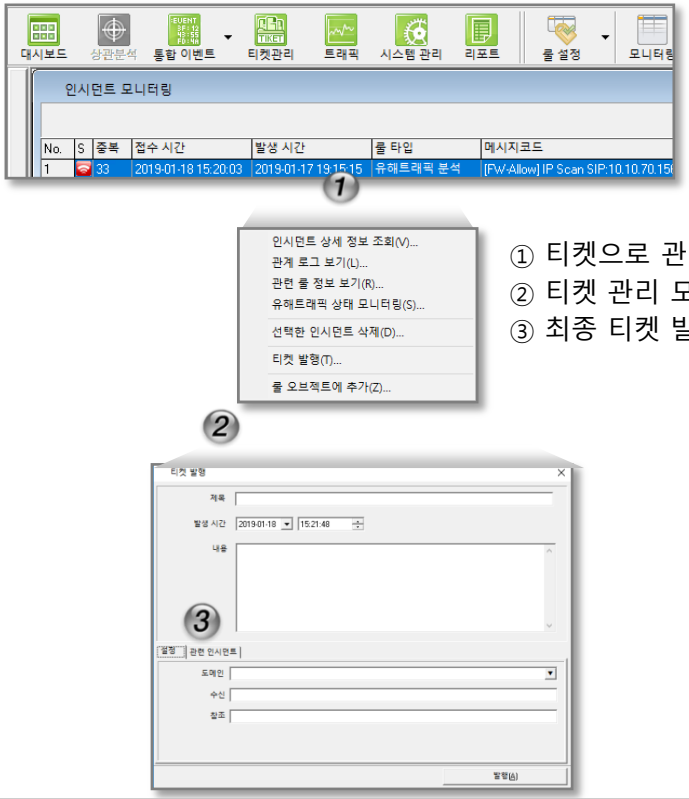


2.5 관제 이벤트 관리

보안관제 활동의 원활한 지원을 위한 이벤트 티켓 관리 기능을 제공 합니다. 이벤트 처리사항을 관리화면에 기록, 처리된 히스토리를 저장해 대응 이력관리를 시스템화 합니다.

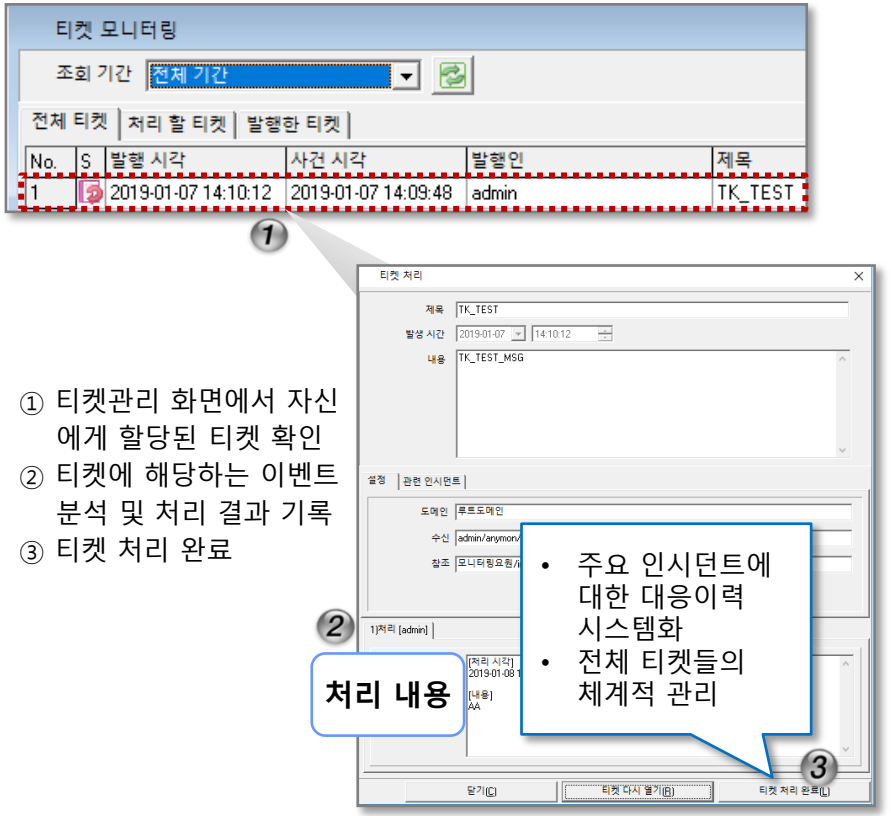
관제 이벤트 티켓 발급 및 처리

티켓 발급 측면



① 티켓으로 관리할 이벤트 선택
② 티켓 관리 모듈 수행
③ 최종 티켓 발행

티켓 처리 측면



① 티켓관리 화면에서 자신에게 할당된 티켓 확인
② 티켓에 해당하는 이벤트 분석 및 처리 결과 기록
③ 티켓 처리 완료

V

레퍼런스

1. 레퍼런스
2. 구축 사례

1.1 주요 고객사

주요 고객사

공공 / 학교 / 병원

경상남도 GYEONGNAM
행정자치부 정부통합전산센터
KODIT 신용보증기금
보건복지부 국립마산병원
세종특별자치시
인천광역시
JDC 제주국제자유도시 개발센터
국토교통부 한강홍수통제소
해양수산부 여수지방해양수산청
국세청 National Tax Service
농촌진흥청
기상청
울산광역시
광주광역시 GWANGJU CITY
국립나주병원
국립목포병원
국방기술품질원 DTaQ Defense Agency for Technology and Quality
국군기무사령부 Defense Security Command
대한민국 육군 Republic of Korea Army
세계로 뻗어가는 전남과학대학교 CHUNNAM TECHNO UNIVERSITY
한국에너지기술연구원 KOREA INSTITUTE OF ENERGY RESEARCH
KSD 한국예탁결제원
ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute
UNIST
ex 한국도로공사
서울시농수산식품공사
LH 한국토지주택공사
서원대학교 SEOWON UNIVERSITY
KAERI 한국원자력연구원
PyeongChang 2018
고려대학교 세종캠퍼스
한국폴리텍대학

기업 / 금융

KB 국민은행
한화S&C
DB Inc.
서경방송
우리은행
INVENIA
롯데정보통신
NOROO 노루페인트
하나은행
HYUNDAI 현대HCN
HYUNDAI DEPARTMENT STORE GROUP
HYUNDAI LIVART
한국투자증권
HYUNDAI 현대드림투어
현대홈쇼핑
HYUNDAI AutoEver
현대차투자증권
HYUNDAI KEFICO
HYUNDAI Rotem
HYUNDAI GLOVIS
Hyundai Card
HYUNDAI DYMOS
HYUNDAI 현대그린푸드
HYUNDAI ENGINEERING & CONSTRUCTION
Hyundai Capital
HYUNDAI STEEL
HYUNDAI MOBIS
HYUNDAI POWERTECH
Hyundai Commercial
대구국제공항 DAEGU INTERNATIONAL AIRPORT
JEJUair
GS 칼텍스

1.2 최신 레퍼런스

2020년 구축 실적

사업명	고객사	사업기간
통합로그관리 시스템 도입 사업	인천광역시교육청교육과학정보원	2020. 06 ~ 2020. 06
통합로그관리 시스템 고도화 사업	한국투자증권	2020. 06 ~ 2020. 08
통합로그관리 시스템 도입 사업	경상남도 의령군	2020. 05 ~ 2020. 06
통합로그관리 시스템 업그레이드	그랜드코리아레저	2020. 05 ~ 2020. 05
통합로그관리 시스템 증설 도입	하나은행	2020. 03 ~ 2020. 04
통합로그관리 시스템 업그레이드	제주국제자유도시개발센터	2020. 03 ~ 2020. 03
여권통신망 전용회선 서비스 공급자 선정 사업	외교부	2019. 11 ~ 2020.03
통합로그관리 시스템 업그레이드	서원대학교	2020. 01 ~ 2020. 02

1.2 최신 레퍼런스

최근 3년간 주요 구축 실적

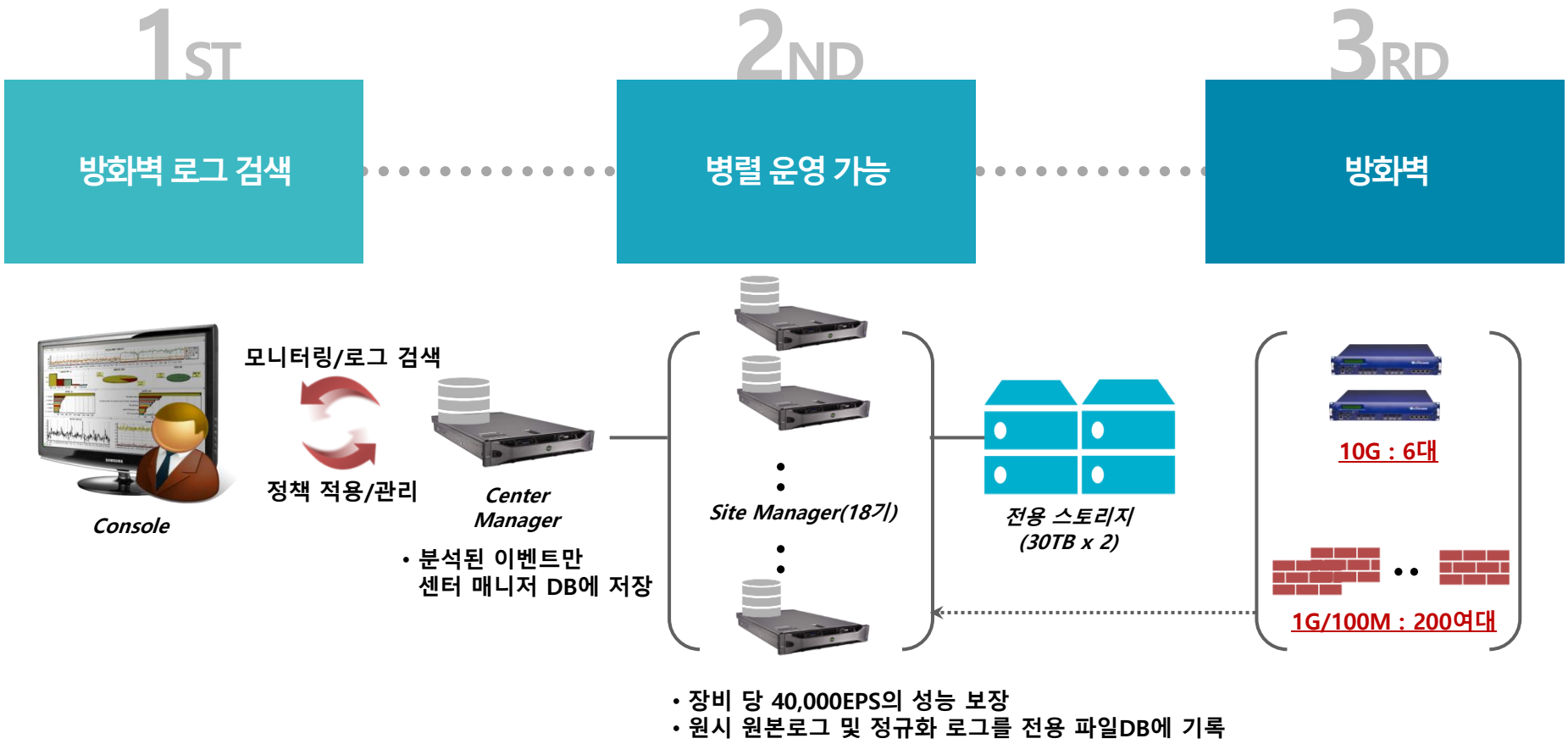
* 이외에도 다수 레퍼런스 보유

사업명	고객사	사업기간
대민정보시스템 통합구축사업 보안SW(장비) 구매	중소벤처기업부(중소기업기술정보진흥원)	2019.11 ~ 2019.12
통합로그관리체계 구축을 위한 통합로그관리시스템 도입	국립민속박물관	2019.11 ~ 2019.12
주요정보통신기반시설 보안강화 사업 물품 구매	광주광역시교육연구정보원	2019.10 ~ 2019.11
금융 오픈 API ASP 시스템 구축 및 서비스 제공	쿠콘	2019.08 ~ 2019.10
내부정보 통합보안관리 시스템 구축	우정사업정보센터	2019.07 ~ 2019.12
하나은행 통합로그관리시스템 고도화 사업	하나은행	2019.06 ~ 2019.07
차기군위성 고정형,다대역 정보보호제품 구매	국방과학연구소	2019.04 ~ 2019.06
마산항VTS 통합로그분석시스템 구축 사업	해양경찰청	2019.04 ~ 2019.05
한국교육개발원 통합로그분석시스템 구축 사업	한국교육개발원	2019.04 ~ 2019.05
KB은행 통합로그관리솔루션 업그레이드 사업	KB은행	2019.03 ~ 2019.04
경산시 통합로그분석시스템 교체 구축 사업	경산시청	2019.03 ~ 2019.04
테스나 통합로그분석시스템 구축	테스나	2019.02 ~ 2019.04
GS칼텍스 통합로그관리시스템 구축	GS칼텍스	2018.11 ~ 2018.11
대구분원 통합로그분석시스템 구축	한국전자통신연구원(ETRI)	2018.04 ~ 2018.05
통합로그분석시스템 구축	JT친애저축은행	2018.02 ~ 2018.05
통합로그분석시스템 도입	한국화학연구원	2017.10 ~ 2017.12
국세청 통합로그분석시스템 추가 도입	국세청	2017.10 ~ 2017.12
GS칼텍스 통합로그분석시스템 구축	GS칼텍스	2017.07 ~ 2017.09
현대로템 통합로그분석시스템 구축	현대로템	2017.04 ~ 2017.06
국립나주병원 통합로그분석 도입	국립나주병원	2017.05 ~ 2017.06
현대파워텍 Anymon 납품의 건	현대파워텍	2017.03 ~ 2017.06
창원경륜공단 Anymon 납품건	창원경륜공단	2017.01 ~ 2017.01
여수지방해양수산청 통합로그분석 시스템 도입	여수지방해양수산청	2016.11 ~ 2016.12
국립마산병원 통합로그분석시스템 도입	국립마산병원	2016.10 ~ 2016.11
한국장학재단 접속기록 저장솔루션 개선	한국장학재단	2016.10 ~ 2017.04
내부통제시스템 구축(UBA)	현대차투자증권	2016.09 ~ 2016.12
통합로그분석시스템 납품 건	평창동계올림픽조직위원회	2016.07 ~ 2016.08
육군본부 MIoT 사업 통합로그분석 도입	육군본부	2016.02 ~ 2016.03

2.1 통합 로그 분석 시스템 구축

- 18기로 최대 35만 EPS 트래픽(600~700GB/day)의 방화벽 데이터 수집/분석
- 당일 로그는 사이트 매니저 로컬 디스크에 저장, 익일 전용 스토리지에 보관
- 보안사고 대비 근거 자료 보관 및 검색 용도로 활용

A기관 – 성능 및 장비 구성

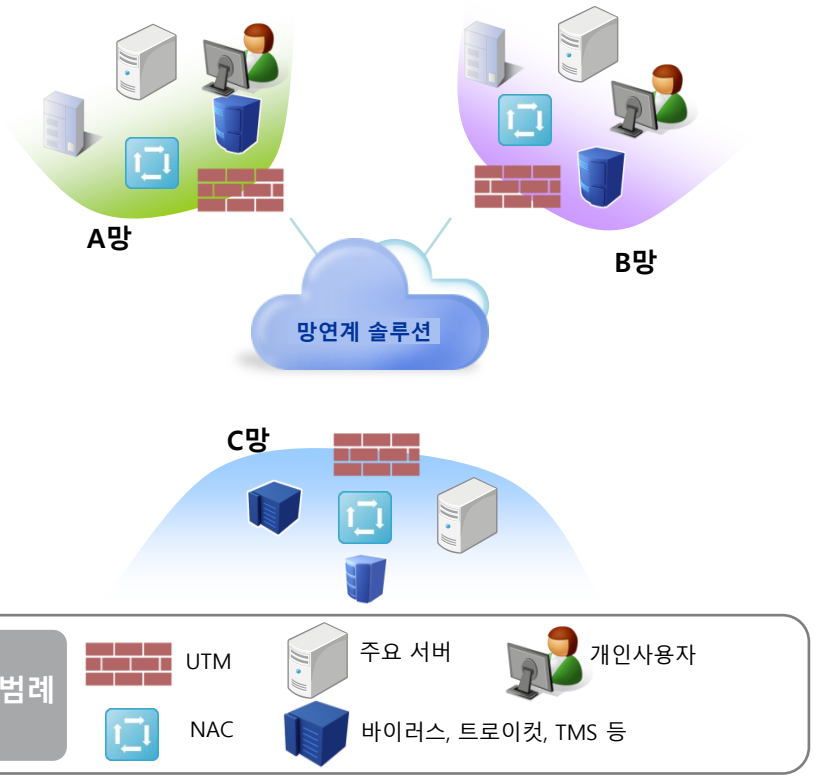


2.2 보안 장비 통합 모니터링 시스템 구축

- A망/ B망/ C망으로 분리된 환경에서의 로그 수집
- 통합 대시보드 업체와 협업하여 상황판 구축
- 전체 군(육군,공군,해군,국군) 보안 관제 사업수행을 위해 Anymon PLUS 도입

B 부대 – 인프라 환경 및 요구 사항 분석

네트워크 환경 예제



사용자환경 분석

- **분산되어 있는 3개의 망에 로그를 통합 모니터링하고 상관분석을 통해, 위험 사용자 탐지**
- **트로이컷, TMS 등의 로그를 수집**
- **망연계 솔루션과 FTP를 활용한 릴레이 방식으로 로그수집**

구축 요구사항

- **트래픽 모니터링 강화**
  - 망별 NAC, 트로이컷, TMS, UTM, 바이러스 로그를 수집하여 상황판에 위험 사용자를 인지하여 즉각 대응 할 수 있는 프로세스 구축
  - 대용량 트래픽 로그를 저장/검색 시스템 구축
- **상관분석을 통한 위험 사용자 도출**
  - 상관분석을 통해 위험 부대명/사용자 정보 상황판 노출
- **분리 된 다수의 망 로그를 망연계 솔루션을 통해 한곳에 통합 저장**
- **파일 위변조 방지**
  - WORM 스토리지를 통해, 파일 위변조 방지

2.3 시스템 생명주기에 따른 로그 관리 시스템

- H자동차 그룹 '통합 로그 관리 시스템 구축 표준화' 사업 추진
- 개인정보보호법 기술적 보호조치를 위한 준거성 확보
- 보안사고/장애 발생시 신속한 원인 규명을 위한 사전/사후 대응체계 구축

H 그룹 – 시스템 구성 개념도

구축 구성 개념도

연동/업무 범위

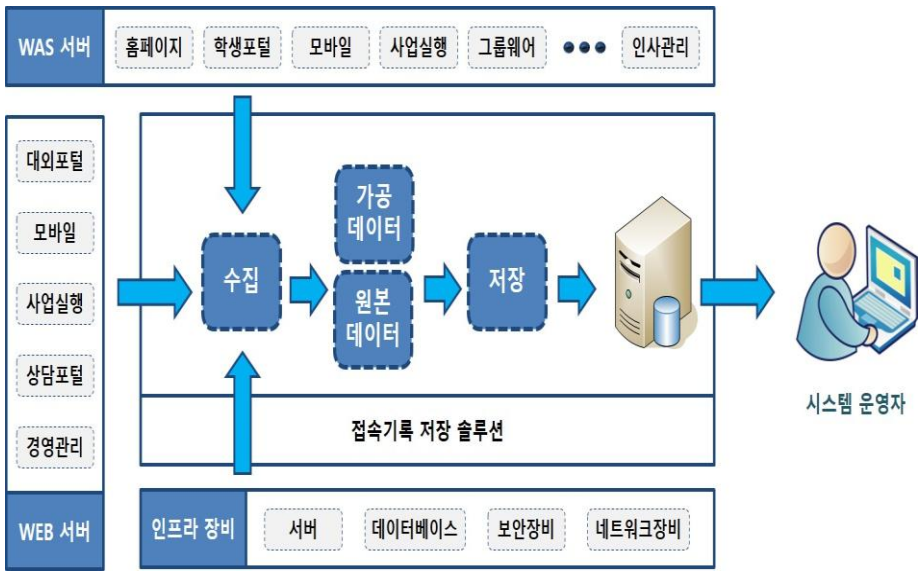
구분 (업무범위)	연동 대상 장비
개인정보취급시스템	HR, 채용시스템
보안 인프라	서버백신,DBSAFER, DB암호화, DRM, IPSCAN,방화벽
기술 및 중요거래 정보 취급 시스템	ERP, 특허시스템
인사시스템	인사시스템 접근 이력 사용자 로깅 정보
기술 거래정보시스템	기술 거래정보시스템 접근 사용자 로깅 정보
특허시스템	특허 시스템 접근 사용자 로깅 정보

2.4 사용자 접속기록에 대한 로그 수집/분석

- WEB 어플리케이션의 접속기록 로그 전체 저장
- 비정형화 된 Debuging 로그를 수집하여 Exception 발생시, 사용자에게 Notify
- 서버 접근로그, 이벤트로그, DRM, 네트워크 로그 수집

H 재단– 시스템 구성 개념도

구축 구성 개념도



연동/업무 범위

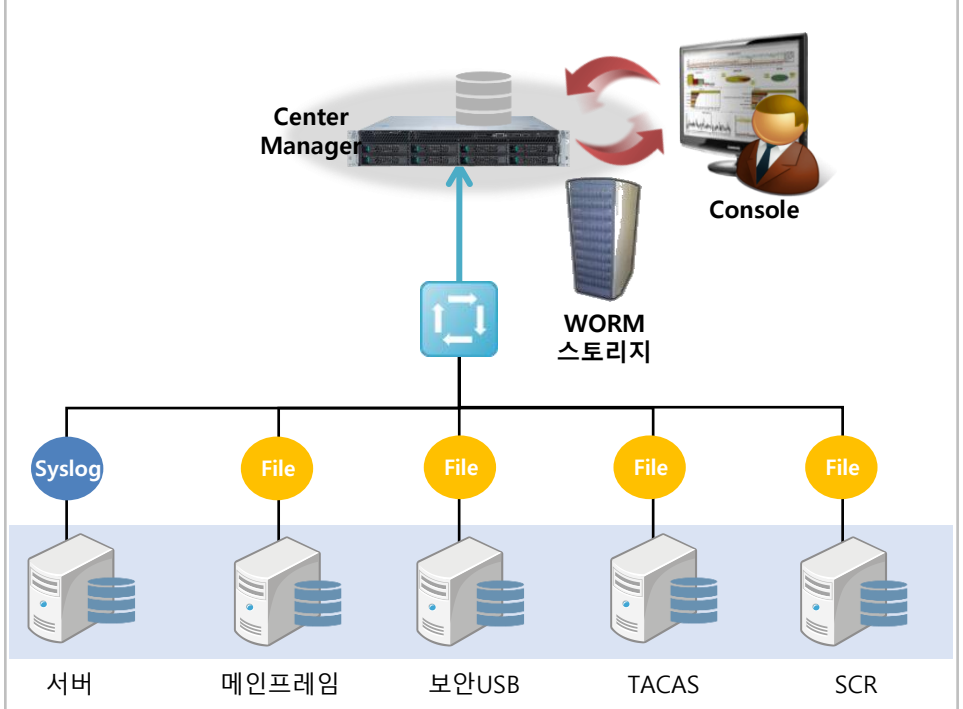
구분 (업무범위)	연동 내용
WEB 서비스	WEB 어플리케이션에 접속 된 로그 비정상 접근 사용자 도출
이벤트 로그	비정형화 된 Debuging 로그를 수집하여 Exception 발생시, 사용자에게 알림
네트워크	S/W로그에서 발생 된 Link up, down의 대한 로그를 수집하여 비정상 S/W로그 분석
DRM	데이터베이스 접근 사용자 정보와 현재 세션 수, Hang현상 등의 로그를 수집하여 비정상 계정 탐지
서버	서버 로그인 로그를 수집하여, 반복적인 패스워드 실패 사용자 탐지

2.5 각종 규정, 법규 강화에 대응할 수 있는 시스템 구현

- 전자금융감독규정, 내부통제 모범규준, 개인 정보보호법 등에 대응
- 계정 관리, 접근권한 관리 Life Cycle 전반에 대한 분석 및 행위 추적

K 은행 – 시스템 구성 개념도

구축 구성 개념도



연동/업무 범위

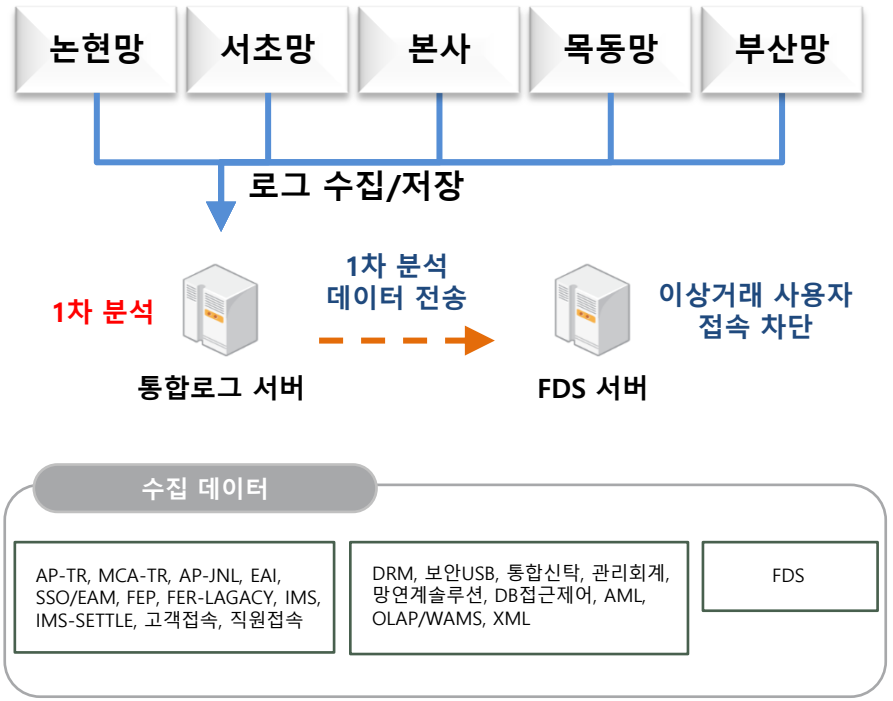
구분 (업무범위)	연동 내용
계정 관리	시스템 자원에 대한 사용자 계정 통합 관리 프로세스 구축 (계정 생성/변경/삭제/승인에 대한 관리)
권한 권리	업무자원에 대한 접근 통제 시스템 구축 (사용자/업무별 접근통제정책에 따른 등록/통제 관리)
로그 관리	시스템 자원에 대한 접속이력 및 사용자 행위 로깅

2.6 FDS(이상금융탐지) 시스템 구축

- QOS(Quality of Service) 기능을 내재 한 Agent 제공하여 접속로그, 거래로그 등 수집 저장 후, 내부 비정상 사용자 탐지
- 비 정형화 된 거래로그(Transaction)를 수집 후, XML Parsing 기능을 제공하여 편리한 UI 구현
- D사 통합로그시스템 Wing-Back을 통해 성능 및 기능 개선

H 투자증권 – 시스템 구성 개념도

구축 구성 개념도



연동/업무 범위

구분 (업무범위)	연동 내용
FDS 시스템 연계	이상금융 거래탐지 시스템관의 연동을 통한 고객 단말 정보 수집 및 부정 접속, 부정 거래 탐지
내부통제	개인정보 과다 조회자 탐지 및 탐지 내역 모니터링
거래로그 수집	비 정형화 된 AP-JNL로그를 XML Parsing을 통해 사용자 Needs 충족

별첨

1. 경쟁사 제품 비교

1. 경쟁사 제품 비교

구분	항목	Anymon PLUS	I사 LogCenter	N사 LogCops	비고
아키텍쳐	제품 형태	Appliance+S/W	Appliance	Appliance+S/W	
	제품구성	**3 Tier 및 Center / Site 구조**	3-Tier	4-Tier 구조	**영향없이 무한 병렬 확장 가능**
	운영체제	Windows / MS-SQL	Linux / Postgresql, Oracle	Windows / MS-SQL	
	관리콘솔	C/S UI	Web UI	Web UI	Web Server 취약점 없음
로그 수집	EPS	**640,000 EPS**	250,000 EPS	16,000 EPS	**최고 사양 시 단일서버 최고의 수집 용량 제공**
	1일 처리량	500G 이상	300G 이상	100G 이상	
	검색 속도	**초당 1억건 이상**	초당 1억건 이상 검색	확인불가	**최고 사양 시 실 환경에서 최고의 속도 제공**
	신규 장비 연동 편의성	정규화 작업만으로 연동 완료	정규화 작업만으로 연동 완료	정규화 작업 후 추가작업 필요	
	비정형 로그 수집	지원	미지원	미지원	
	네트워크 트래픽 로그 수집	**상세 방화벽 이벤트 로그 수집**	기본 로그 수집	기본 로그 수집	**방화벽 특화 기능 제공**
로그 저장	암호화/무결성 지원	지원	지원	지원	
	원본 로그 압축 지원	지원	지원	지원	
	로그 자동 보관 및 폐기	지원	지원	지원	
검색 및 분석기능	원본에서의 구문검색	정규화 로그를 통한 검색	데이터 Load 및 변환 후 검색	Regular Expression 검색	빠른 검색 지원
	검색 편의성	**UI 방식의 직관적인 검색 기능**	Query 방식으로 학습 필요	UI 방식	**검색 편의성 제공**
	단순 상관분석 기능	지원	지원	일부지원	
	Sequential 상관/재귀 분석	지원	미지원	일부지원	
	방화벽 특화 모니터링	**프로토콜별 상세 통계 등 지원**	미지원	미지원	
이벤트 및 리포팅	실시간 분석 보고서	**트래픽 및 이벤트 실시간 수집**	일부지원	미지원	
	자동화된 리포팅 생성	지원	지원	지원	
	사용자, 개인화 대시보드 구성	지원	지원	지원	
감사	사용자 별 권한 분리	지원	지원	지원	사용자별 대쉬보드 제공
	계정발급/승인 이력	지원	미지원	지원	

A Reliable Partner
Together
On The Road To
Success

Thank you

No1. Value Creator

인 스 피 언 ㈜

INSPIEN

인스피언㈜는 IT컨설팅 분야의 다양한 경험을 보유한 전문가들이 모임
컨설팅 서비스 및 솔루션 기업으로 고객의 가치 창출을 최고의 목표로 합니다.