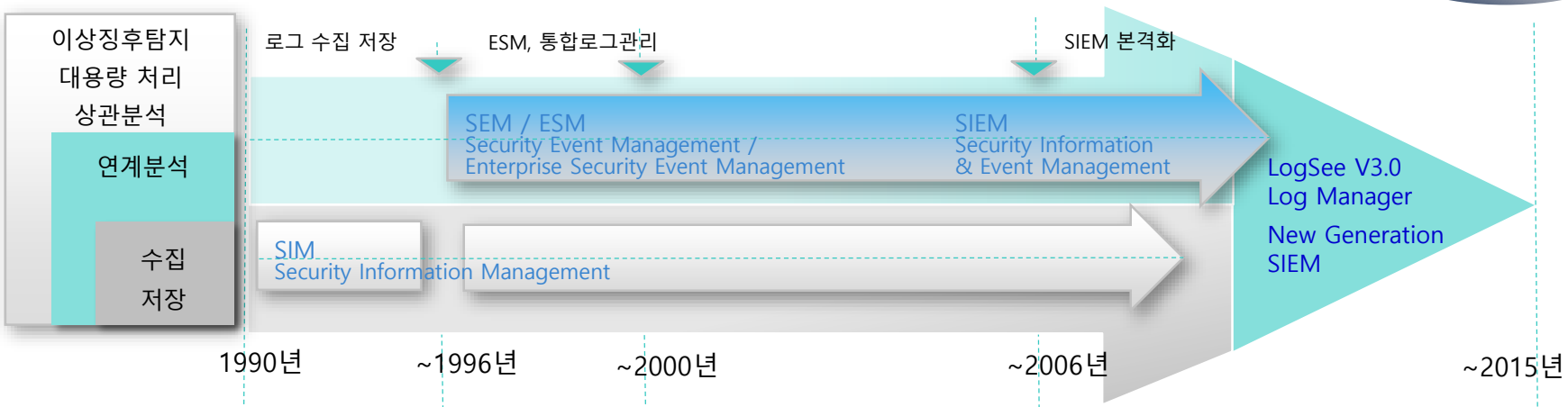
INCON

nLM LogSee™

Big Data 처리 기술을 접목한 통합로그관리 솔루션

# 1.1 로그 보안 트렌드 변화

## 최근 보안 Trend는 "통신상의 정보보호"에서 "개인 및 사회 안전" 으로 진화




| | | ~1996년 | ~2000년 | ~2006년 |
|---|---|---|---|---|
| 용도 | | IT단위 시스템 로그통합 및 장애처리 모니터링 | IT시스템과 보안시스템의 연계분석을 통한 보안 관제 | Application 연계를 통한 종합분석 대용량 처리 기술 |
| 분석영역 | | IT 시스템 위주의 통합 및 분석 | IT+내부 보안 영역 전체에 대한 알려진 보안위협 분석 | 알려지지 않은 보안위협 분석, 이상징후 탐지, 내부정보 유출모니터링 |
| 솔루션 | 대표기술 | F/W, IPS, IDS, Anti Virus/Spyware 등 | 실시간 네트워크 인프라/응용 서비스 등 | 개인/사회 안정 및 시설보안, 융합산업보안 등 |
| | 종류 | 로그세이버, 로그캅스/Cisco, Symantec | 이글루시큐리티,인젠등 ESM기반 업체 | McAfee. IBM, HP, EMC |

SIM(Security Information Management)
- 보안 장비에서 발생하는 로그를 장기적으로 저장/분석/보고 하는 기능에 초점을 맞춤

SEM(Security Event Management)
- 보안장비에서 발생하는 로그의 모니터링, 이벤트 상관관계, 알림을 지원

SIEM(SIM + Event Management)
- 보안 장비에서 생성하는 다양한 로그수집, 상관분석을 통해 위협탐지 및 예방 관리

# 1.2 Big-Data 기반의 기술 필요

네트워크 및 시스템, 보안 제품을 아우르는 보안 이벤트 정보 관리 기술을 바탕으로,

**빅데이터 처리 기술**을 접목한 **통합로그관리시스템**이 필요

## 인프라 기술

- 대용량 데이터를 처리하는 능력으로 저장방식과 처리방식으로 구분
- 클라우드 기반, Hadoop, MapReduce, NoSQL 등
- 확장성 → 처리속도 관점

## 분석 기술

- 대용량 데이터를 분석하는 두뇌역할로 대용량 배치 처리 등
- 통계처리분석/모델링예측, R/Mahout 등
- 확장성과 편의성이 중요

## 응용 및 표현 기술

- 빅데이터 기반 응용 및 서비스
- 데이터 처리분석 및 시각화 표현 기술
- 데이터 관리 편의성이 중요

## 통합로그관리 솔루션

로그 수집 및 저장
로그 생명주기 관리
원인추적 등 감사

- 정보시스템에서 생성되는 다양한 로그를 수집, 저장해서 필요한 정보를 검색, 보고서를 생성하여 IT 인프라 상태와 사용 현황을 알려주는 기능 수행
- 가장 기초 데이터인 로그의 생성에서 폐기에 이르는 로그 생명주기를 관리
- 장애나 보안사고 발생 시 로그를 통해 원인을 추적하고, 각종 규제 및 법규에 대한 감사자료로 활용

## ESM 솔루션

- 보안관제를 위해 실시간으로 발생하는 다양한 보안 솔루션의 수집된 로그를 기반으로 동작
- 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

로그 기반
보안 이벤트 관리
실시간 보안위협 관리

# 1.3 국내 로그 관련 규정

## 개인정보보호법

- 개인정보보호법(제29조 안전조치의무)
  접속기록 안전성확보 필요한 기술/관리/물리적 조치
- 개인정보보호법 시행령(제30조 안전성확보조치)
  침해사고대응 위한 접속기록보관 & 위/변조 방지조치
- 안전성확보조치기준(제8조 접속기록 보관 및 위변조방지)
  접속기록 최소 6개월 이상 보관 및 관리
  기록 위·변조 및 도난, 분실로부터 안전하게 보관

## 정보통신망법

- 정보통신망 관련 법률(제28조, 제48조)
  접속기록의 위/변조 방지를 위한 조치
  침해사고 원인분석 위한 접속기록 자료 보존 [5년]
- 정보통신망 법률시행령(제58조)
  침해사고관련기록 훼손/멸실/변경 방지 조치 취할 것
- 정보통신기반보호법(제12~14조, 제21조)
  기록에 대한 접근권한, 사고 시 대응 및 복구 조치
  침해사고통지 내용 - 일시,피해내역, 조치내용 등

## 교육(행정) 정보보호 수준진단 매뉴얼

- 개인정보보호(PIS) 관련 진단 지표

  11.2 개인정보처리시스템의 접속기록에 대한 정기점검 및 후속조치가 이루어지고 있는가?(30페이지 참조)
- 정보보안(SIEM) 관련 진단 지표

  6.5 정보보안 사고 발생 시 확인 등을 위해 정보보호 시스템 접근기록을 관리하고 있는가?(84페이지 참조)

## PIMS 및 ISMS 인증기준

- 기술적 보호조치 (PIMS)
  공개서버에 대한 로깅/로그보관지침 수립 및 보관 의무 정보변경/삭제 및 승인에 대한 감사기록 생성
- 내부검토 및 감사 (PIMS)
  개인정보 처리 기록/위변조 방지(최소6개월 이상 저장)
- 로그기록 및 보존 (ISMS - 8.1.3)
  사용자인증/권한변경, 중요정보이용/유출 감사증적
- 로그기록 및 보존 (ISMS - 11.6.2)
  운영보안기록 로그유형 정의/일정기간 보존, 주기

## 전자금융거래 및 신용정보보호법

- 전자금융거래법(제22조)
  전자금융거래 내용 추정/검색 또는 내용 오류 발생 시 확인 및 정정 관련 기록 생성 (최장 보존기간 5년)
- 신용정보 이용 및 보호에 관한 법률 시행령(제16조)
  다음 사항의 기술/물리/관리적 보안대책 수립
  - 접속에 대한 접근, 차단 기록
  - 신용정보취급/조회 기록의 주기적인 점검
  - 그 밖에 신용정보 안전성 확보 위한 필요한 사항

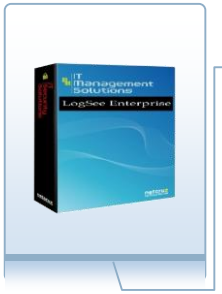
## 전자정부법

- 정보통신망 등의 보안대책 수립·시행(제56조)
  - 행정 업무의 전자적 처리를 위한 기본원칙, 절차 및 추진 방법 등을 규정
  - 전자적 대민 서비스 보안 대책, 정보통신망 등의 보안대책 수립·시행, 인증기록의 보관, 신원 확인 및 접근권한 관리 체계의 구축 관리

출처: 국가법령정보센터(http://www.law.go.kr) 및 교육부

# 2.1 솔루션 개요

웹 기반의 동적 분석 Rule 설정, 비정형 데이터 분석 정책 편집, 뛰어난 확장성 등의 특장점을 보유




## 제품명 : nLM-LogSee V3.0

- 용도 : 통합로그관리
- 제조사 : 넷크루즈

- CC 인증 및 GS 인증 획득
- 대용량 이기종 상관분석 기능
- 소스코드 변경 없이 대시보드 구성 편집기능
- 종합 위협 기관 위협 보안 시나리오 룰 생성/관제
- 내외부 위협이벤트에 대한 침해대응, 소명관리기능
- 실시간 모니터링 기능 및 보고서 관리기능
- 사용자 편의성 제공
  - 사용자, 개인화 된 UI 메뉴 구성 및 편집기능
  - 웹 UI 인터페이스, 검색질의 자동검색/결과 공유
  - 한글 인터페이스 제공

## 특장점

**유연성**

- 쿼리 기반의 유연한 Rule 설정 기능 제공
  - 거의 모든 보안 장비와 Filtering 연동 가능
  - 웹을 통한 간편한 추가, 삭제, 편집 제공
- 사용자 편집이 가능한 유연한 대시보드 제공
  - 각종 검색 결과를 대시보드로 Export 및 커스터마이징
  - 고객 목적에 따라 최적화 된 대시보드 화면 제공

**성능 보장**

- 로그 수집 + 로그 분석 역할 분리 및 분산 처리 구조
  - no DBMS : 파일 기반 및 인덱싱 처리
  - 안정적 이중화 구조로 대용량 로그 처리
  - Map-Reduce 방식의 분산 처리
- 정형/비정형 데이터 처리
- 공인시험인증기관을 통한 고성능의 수집/검색 속도 검증

**확장성**

- 시나리오 기반의 다양한 이벤트 처리 및 통계 연동
  - 실시간 단위 이벤트 및 검색 기반 이벤트 처리
  - 시나리오 기반의 다양한 이벤트 처리
- 연관 솔루션 연계를 통한 통합관제로의 확장 용이
  - NMS/SMS/통합접근제어 등을 보유한 IT통합관리 회사
  - System에 하나의 Universal Agent만 설치하여 로그/SMS/통합접근제어연동 등 종합대시보드 화면제공

# 2.2 모듈 구성

nLM-LogSee 기반에 nSIEM, nPIS 등을 모듈화(별도 Option)하여 기능 확장 구성

**종합보안분석 시스템**
**SIEM(nSIEM)**

- 이기종 보안 장비 로그들을 시나리오에 따라 상관 분석
- 침해 및 이상 탐지 시 원인분석과 추적 기능 제공

**개인정보통합모니터링 시스템**
**PIS(nPIS)**

- 다양하고 연관된 개인정보유출 패턴 시나리오에 따라 상관분석
- 불법행위 또는 의심자에 대한 통지 및 소명관리 체계 구축

API

API

**BigData 기반의 통합로그관리시스템**
**Log Manager(nLM) - Log See**

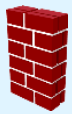
- 공인된 인증기관(TTA)을 통해 검증된 업계 최고 수준의 수집 및 검색 성능
- 쿼리기반의 상관분석으로 시나리오에 따른 정확한 보안 위협 탐지 제공

Syslog/NetFlow/SNMP

FTP/SFTP

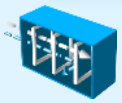
DBMS (MS-SQL,Oracle…..)

Agent TCP/UDP

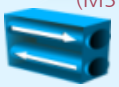

F/W


WAF


IPS


DDoS


QoS


VPN


DRM


유해사이트 차단


DLP

DB보안

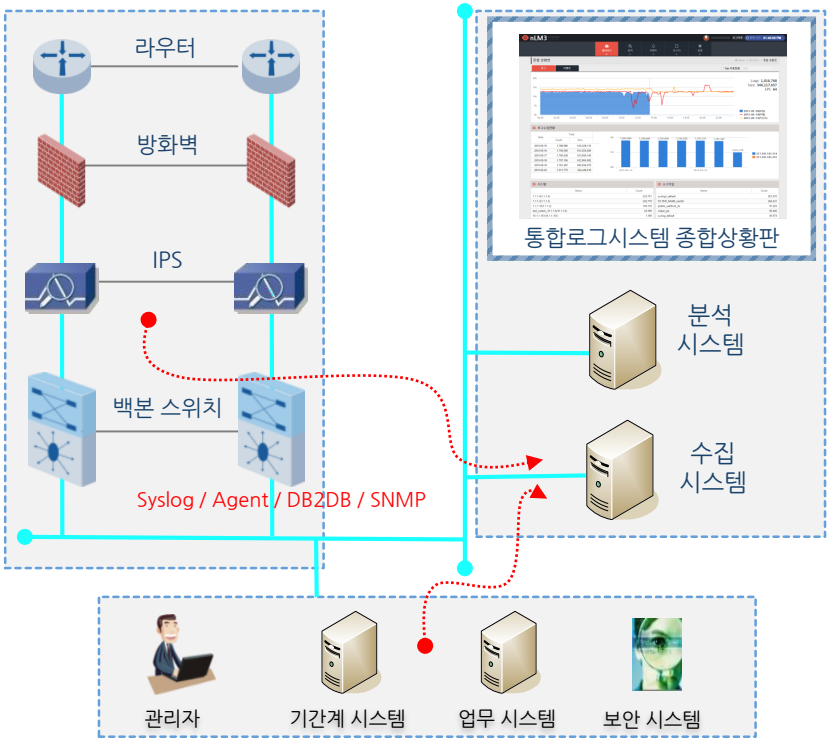

기간계

# 2.3 주요 아키텍쳐

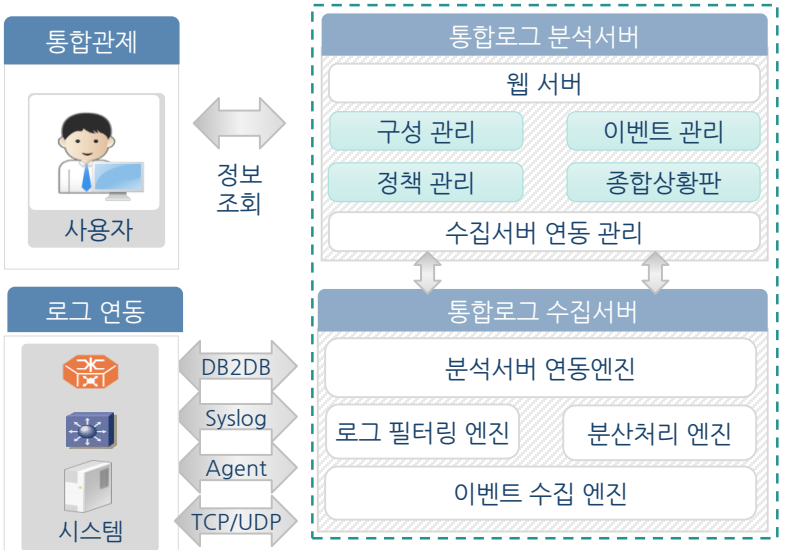
## 2.3.1 HW 아키텍쳐

권장 물리적 구성과 H/W 사양으로 구성하여 안정적 시스템 구성

### 물리적 구성




### 논리적 구성




| Agent (서버군) | Syslog (네트워크) |
|---|---|
| Linux, Solaris, HP-UX, IBM-AIX, Windows | Backbone, Router, Switch, VPN(IPSec), NMS, SMS 등 |
| **TCP / UDP (보안장비)** | **DB to DB (솔루션 및 업무시스템)** |
| 방화벽, IDS/IPS, UTM, DDoS, NAC, WIPS, WAF, TMS, APT 등 | 인사 시스템, 그룹웨어, 기간계 시스템, 업무계 시스템, 업무용 어플리케이션 등 |

# 2.3 주요 아키텍쳐

## 2.3.2 SW 아키텍쳐

X86 플랫폼 및 Linux OS 등 Open 소스 아키텍처 기반

### 분석서버 아키텍처

| 분석서버 | | | | |
|---|---|---|---|---|
| Web GUI | | | | |
| 검색 | 이벤트 | 차트<br>그래프 | 보고서 | 스케줄러 |
| Coordinator | | 외부전송API/DB클라이언트API | | |
| RDBMS(설정 DB) | | | | |
| Map Reducer | | | | |
| 보안 통신 라이브러리(TLS/SSL lib) | | | | |
| 웹서버 | | | | |
| 이중화엔진(Active-Standby) | | | | |
| OS(Linux) 64BIT | | | | |
| X86 Platform | | | | |

- 분석서버는 이중화 구성된 설정 DB 제공
- 맵리듀스를 이용하여 수집서버환경의 분산검색 제공
- 수집서버가 처리한 Map Function으로 수집된 정보를 기반으로 Reduce Function 수행

### 수집서버 아키텍처

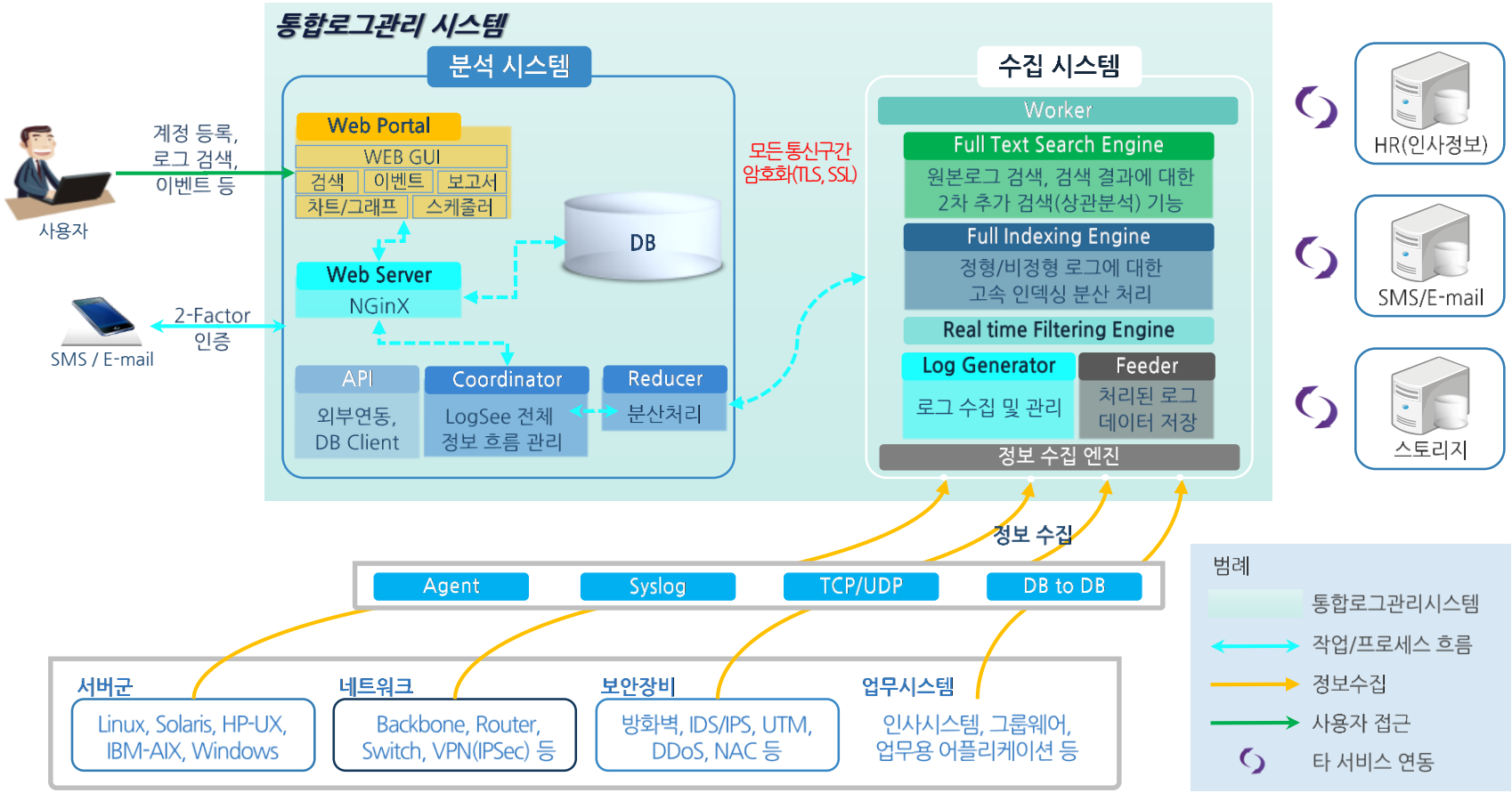
| 수집서버 | | | | |
|---|---|---|---|---|
| Coordinator Agent | | | | |
| Full Text Search Engine | | | | |
| 데이터라우팅/분산복제저장(압축/암호/무결성) | | | | |
| Full Indexing Engine | | | | |
| Realtime Filtering Engine | | | | |
| Log Generator | | Feeder | | |
| 로그수집엔진 | | | | |
| Syslogd | snmpd | Agentd | DB<br>Connecto<br>r | flowd |
| OS(Linux) 64BIT | | | | |
| X86 Platform | | | | |

- 다양한 프로토콜의 패킷 데몬을 통해 로그를 수집
- 필터엔진, 인덱싱 엔진에서 수집로그의 원본저장/의미식별 /색인작업 진행(장애를 대비한 복제데이터 분산처리)
- 분석서버 명령에 의해 Map Function 수행

# 2.3 주요 아키텍쳐

## 2.3.3 수집 및 분석 아키텍쳐

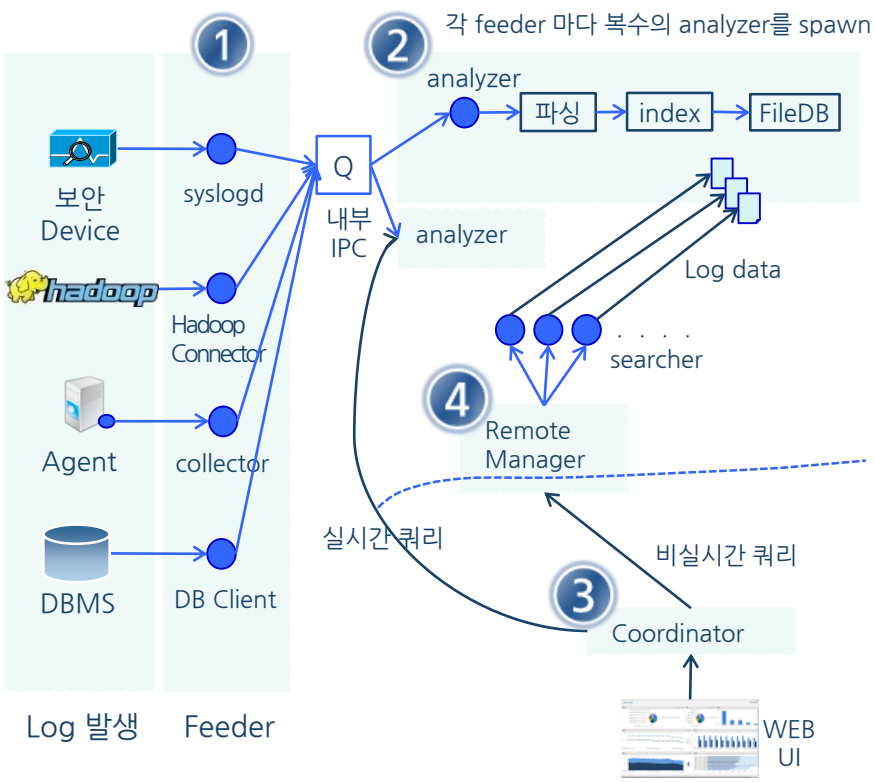
수집시스템을 통해 다양한 형태로 연동하여 수집된 로그는 분석시스템을 통해 검색, 이벤트 처리 등을 수행



# 2.3 주요 아키텍쳐

## 2.3.4 Engine 처리 Process

다양한 로그 수집 연동을 지원하며 안정적으로 인덱싱 등 내부 Process를 처리




1. 보안장비 / hadoop / 서버 / DBMS 등으로 부터 Syslog, hadoop, Agent, DB2DB 등의 다양한 로그 전송 데이터를 Feeder가 수집

2. Analyzer는 내부IPC 를 통해서 전달받은 로그데이터를 Parsing(Filter) / indexing 후 FileDB로 저장

3. Coordinator는 UI에서 요청을 받아 실시간 쿼리의 경우, 각 analyzer로 요청하여 그 결과를 UI로 표시

4. Remote Manager는 Coordinator의 에이전트로서, Coordinator에서 비 실시간 쿼리를 요청 받아 로그데이터 조회 후 Coordinator를 통해 결과를 UI로 표시

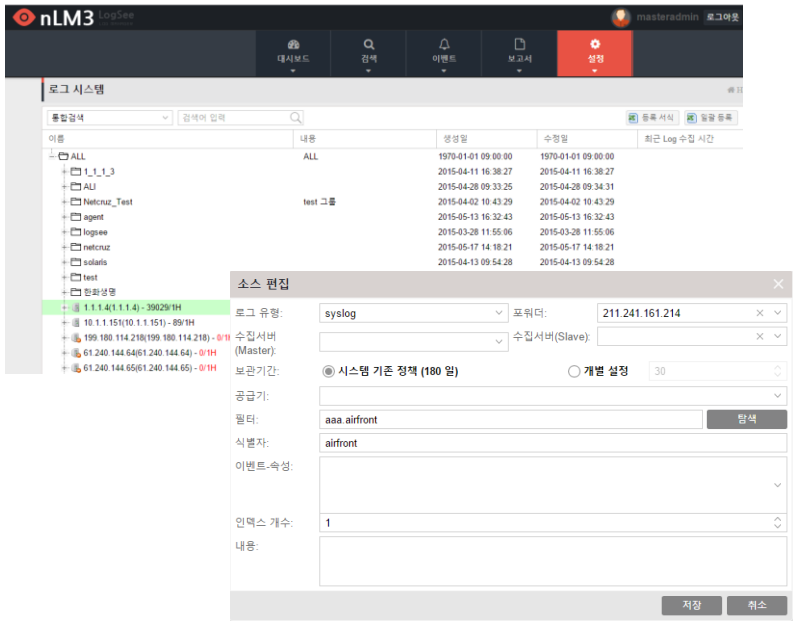
hadoop Hadoop Connector를 통해 Hadoop에 저장된 Data를 가져와 분석 가능

# 2.4 주요 기능

## 2.4.1 Syslog 연동

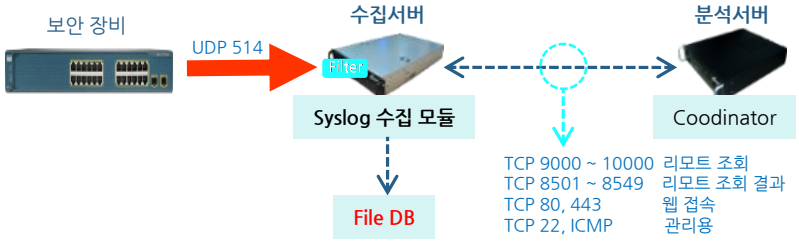
Appliance Type의 보안솔루션군은 Syslog Protocol Format 형태로 보내주는 log를 수집 및 저장

### Syslog를 통한 로그 수집




- Agent를 설치할 수 없으며 Syslog를 지원하는 네트워크 장비 및 어플라이언스 보안제품군의 경우 해당 장비에서 지원하는 Syslog를 이용하여 로그 수집 연동

### Syslog 연동 개념도




### Syslog를 활용한 로그 수집 내용(예)

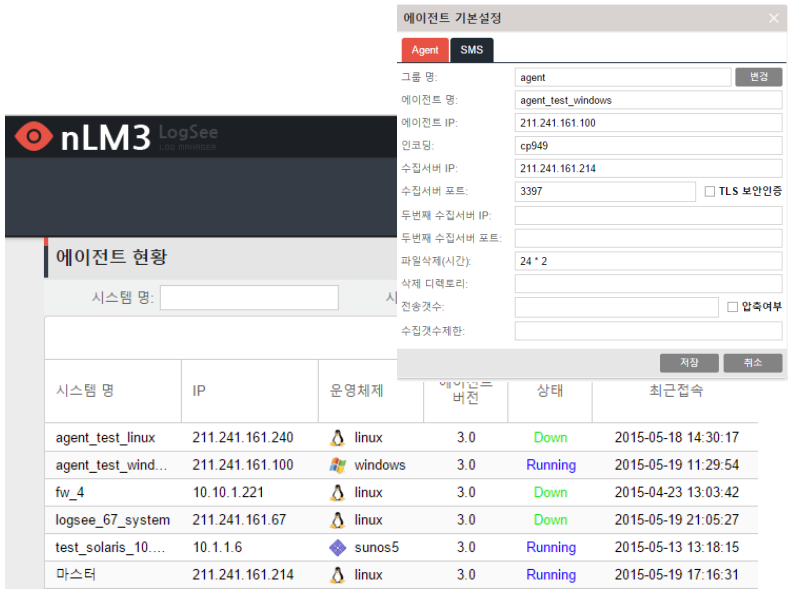
| 시스템 | 로그 내용 |
|---|---|
| 방화벽 | 1) 허용/차단 이력<br>2) Attack 및 Target IP 이력<br>3) 트래픽 현황 |
| 웹방화벽 | 1) 탐지/차단 이력<br>2) Method 별 로그 추이<br>3) 트래픽 현황 |
| Router & Switch | 1) 시스템 로그<br>2) 트래픽 로그 |
| DDoS | 1) 트래픽 로그<br>2) 차단/허용 내역<br>3) 블랙/화이트 리스트 내역 |
| IPS | 1) 허용/차단 내역<br>2) 허용내역(Allow)<br>3) 탐지내역(Detect)<br>4) 차단내역(Block)<br>5) 에러내역<br>6) 경고내역 |

# 2.4 주요 기능

## 2.4.2 Agent 연동

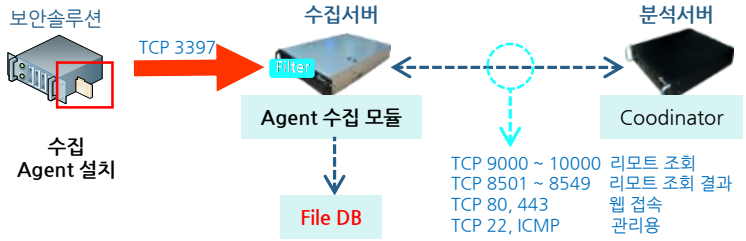
Server Type의 보안솔루션군은 Agent를 설치하여 저장된 File 형태의 log를 수집 및 저장

### Agent를 통한 로그 수집




- 특정 Application 로그 수집을 위해 보안솔루션에 로그수집 전용 Agent 설치 (리눅스, 유닉스, 윈도우 시스템 모두 가능)
- 설치 Agent의 독립적인 Port 사용으로 기존 보안솔루션과의 포트 충돌 현상 방지하고, 로그 전송 시 자동으로 로그 시스템으로 등록

### Agent 연동 개념도




### Agent를 활용한 로그 수집 내용(예)

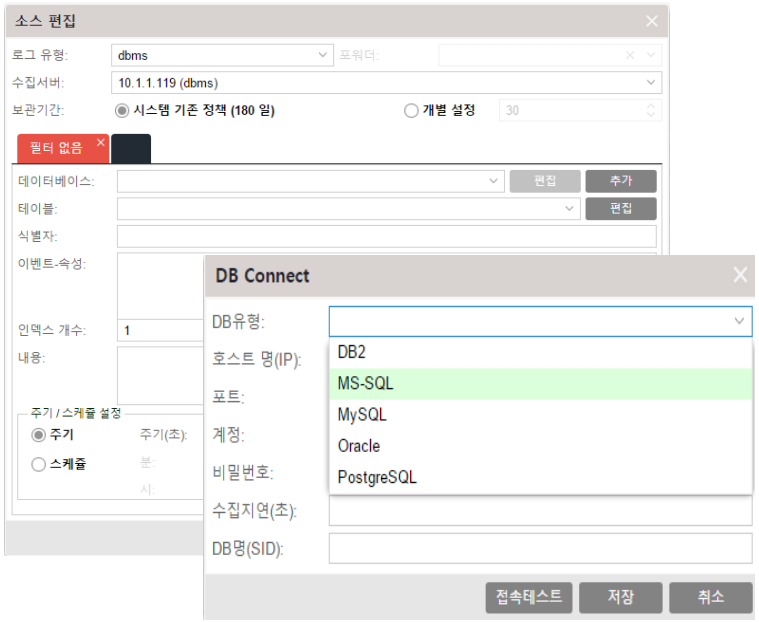
| 시스템 | 로그 내용 |
|---|---|
| 유해사이트차단 | 1) 유해사이트 차단이력 |
| Secure OS | 1) 시스템 접근 기록<br>2) 사용 명령어<br>3) 허용 및 차단 이력 |
| 시스템 접근 | 1) 시스템 접근 기록<br>2) 사용 명령어<br>3) 접근 차단 이력 |
| DB 보안 | 1) DB보안 접속 기록<br>2) 요청쿼리<br>3) 쿼리 결과 값<br>4) 쿼리/접근 차단 이력 |
| NAC | 1) 노드 및 센서 신규/변경 정보<br>2) 동작상태 및 DB 정책 변경정보<br>3) 에이전트설정변경<br>4) 시스템관리 및 인증 정보<br>5) 패치(동기화/서비스)<br>6) 정책 및 그룹 변경정보 |

# 2.4 주요 기능

## 2.4.3 DB2DB 연동

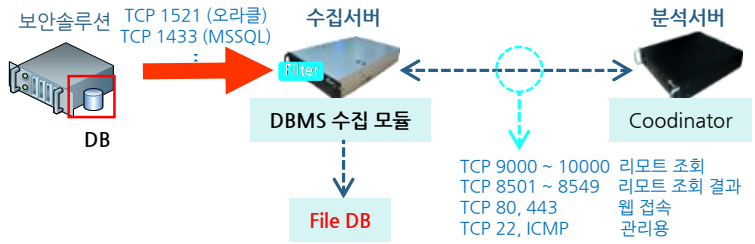
Server Type의 보안솔루션군 중 DB형태로 저장되는 경우, DB2DB로 연동하여 log를 수집 및 저장

### DB2DB를 통한 로그 수집




- 수집서버에 DB Client 설치하여 연동
- 특정 보안솔루션 Database 내 특정 테이블을 연계하여 수집 주기에 따라 로그 수집 연동

### DB2DB 연동 개념도




### DB2DB를 활용한 로그 수집 내용(예)

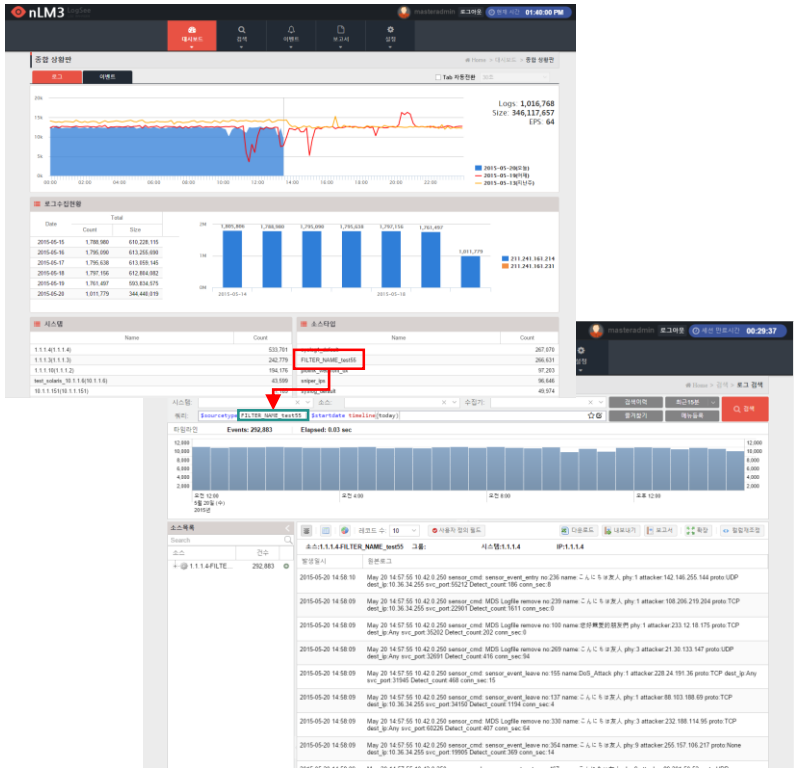
| 시스템 | 로그 내용 |
|---|---|
| 보안USB 및 매체 | 1) USB 및 매체 사용/인증/반출 내역<br>2) 매체 사용 차단 내역 |
| 문서보안(DRM) | 1) 문서보안인증로그<br>2) 문서사용내역로그<br>3) 문서보안 해제내역(권한자)<br>4) 일반문서 변환이력 |
| 바이러스 백신 | 1) 바이러스 감염로그<br>2) 바이러스 치료로그<br>3) 백신엔진(업데이트)로그 |
| 웹 어플리케이션 | 1) 웹 접속이력(Access)<br>2) 오류로그(error)<br>3) 컨테이너로그<br>4) 디버그로그 |
| DBMS | 1) 웹 접속이력(Access)<br>2) 오류로그(error)<br>3) 컨테이너로그<br>4) 디버그로그 |

# 2.4 주요 기능

## 2.4.4 실시간 로그 수집 현황 대시보드

실시간 로그 수집현황을 전일, 전주 동일시간과 비교하고 연동 시스템 및 소스별 실 로그 내용을 바로 확인

### 실시간 로그수집현황 대시보드



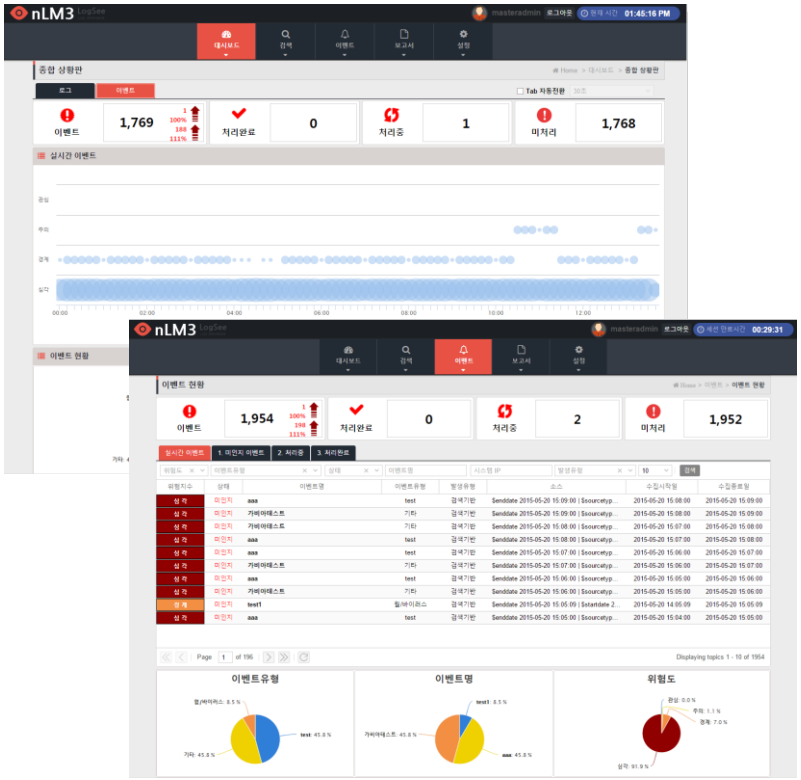

### 검색 시 검색이력, 즐겨찾기, 기간 등 편의 메뉴 제공

# 2.4 주요 기능

## 2.4.5 실시간 보안관제 대시보드

실시간 이벤트 발생/처리 현황 등 편리한 관제 운영을 위한 대시보드 제공

### 실시간 이벤트 발생 현황 대시보드



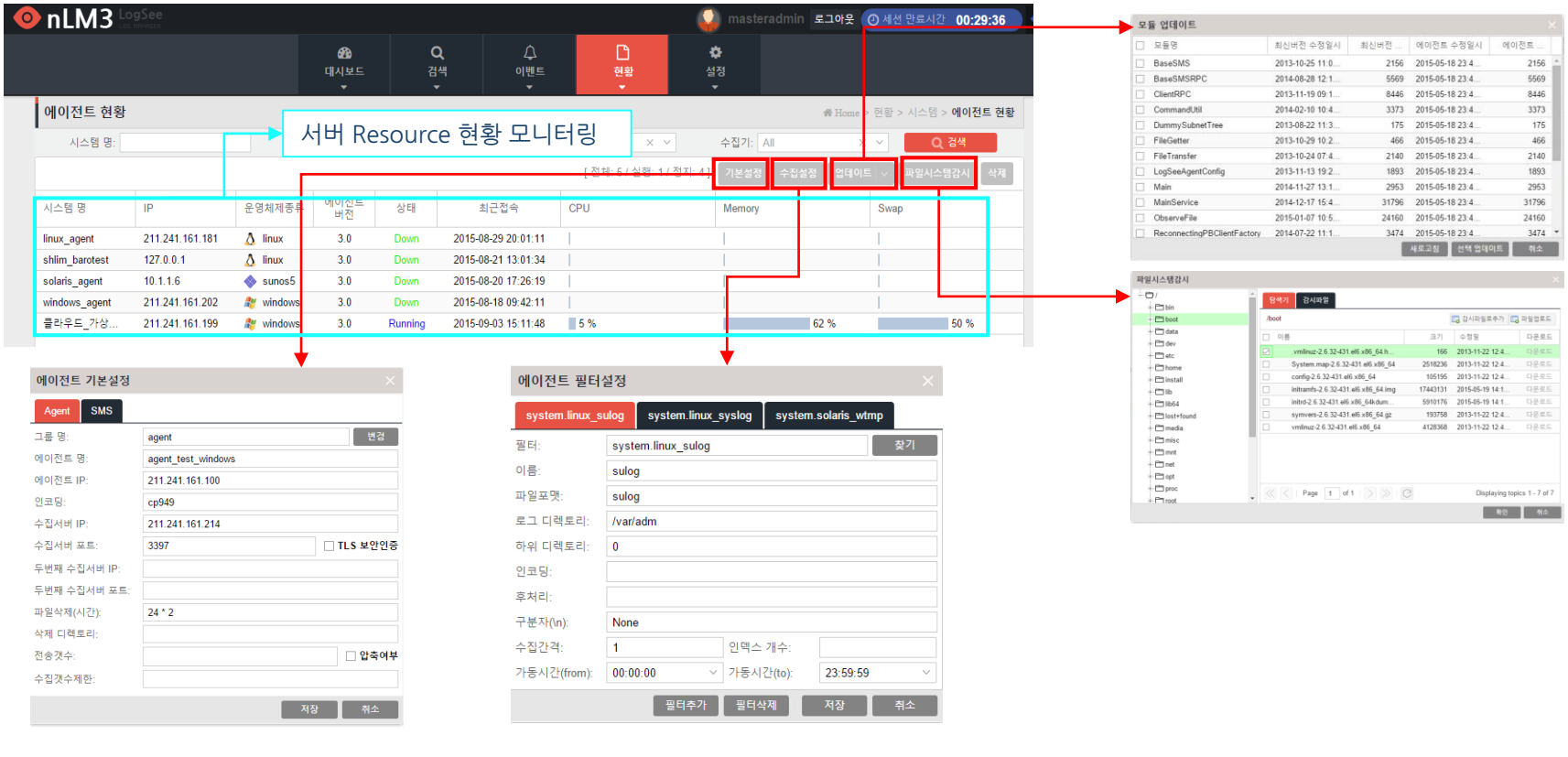

### 이벤트 상세 내용 확인 및 처리 프로세스 제공

# 2.4 주요 기능

## 2.4.6 Agent 설치 서버 실시간 모니터링

Agent 설치된 서버들의 현황 모니터링 및 중앙에서 에이전트 기본설정/필터설정/업데이트 등 제공

### Agent 설치 List 및 관리

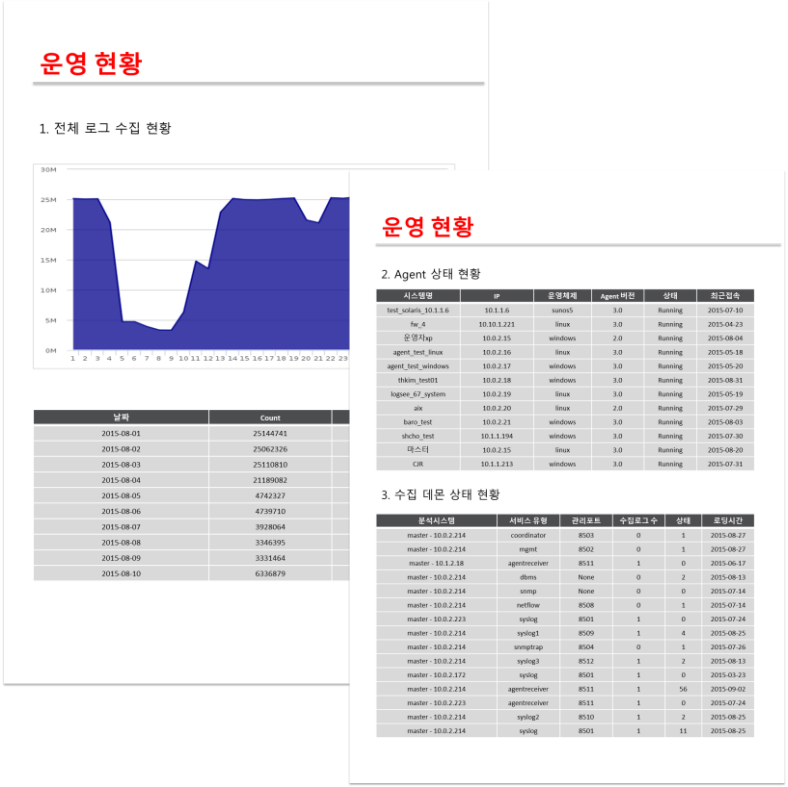


# 2.4 주요 기능

## 2.4.7 월간 운영현황 보고서

전체 로그 수집현황, Agent 운영현황, 각 보안 장비별 이벤트 발생 현황 등의 월간 운영 현황 결과를 제공

### 전체 로그 수집 현황



운영 현황

1. 전체 로그 수집 현황



| 날짜 | Count |
|---|---|
| 2015-08-01 | 25144741 |
| 2015-08-02 | 25062326 |
| 2015-08-03 | 25110810 |
| 2015-08-04 | 21189082 |
| 2015-08-05 | 4742327 |
| 2015-08-06 | 4739710 |
| 2015-08-07 | 3928064 |
| 2015-08-08 | 3346395 |
| 2015-08-09 | 3331464 |
| 2015-08-10 | 6336879 |

운영 현황

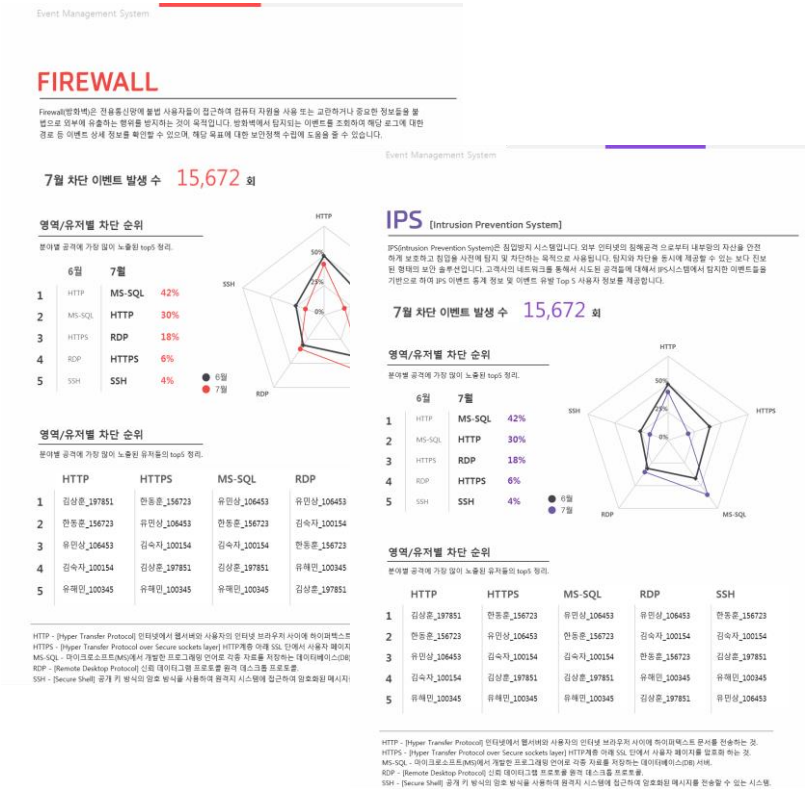
2. Agent 상태 현황

| 시스템명 | IP | 운영체제 | Agent 버전 | 상태 | 최근접속 |
|---|---|---|---|---|---|
| test_solaris_10.1.1.6 | 10.1.1.6 | sunos5 | 3.0 | Running | 2015-07-10 |
| fw_4 | 10.10.1.221 | linux | 3.0 | Running | 2015-04-23 |
| 운영자xp | 10.0.2.15 | windows | 2.0 | Running | 2015-08-04 |
| agent_test_linux | 10.0.2.16 | linux | 3.0 | Running | 2015-05-18 |
| agent_test_windows | 10.0.2.17 | windows | 3.0 | Running | 2015-05-20 |
| thkim_test01 | 10.0.2.18 | windows | 3.0 | Running | 2015-08-31 |
| logsee_67_system | 10.0.2.19 | linux | 3.0 | Running | 2015-05-19 |
| aix | 10.0.2.20 | linux | 2.0 | Running | 2015-07-29 |
| baro_test | 10.0.2.21 | windows | 3.0 | Running | 2015-08-03 |
| shcho_test | 10.1.1.194 | windows | 3.0 | Running | 2015-07-30 |
| 마스터 | 10.0.2.15 | linux | 3.0 | Running | 2015-08-20 |
| CJR | 10.1.1.213 | windows | 3.0 | Running | 2015-07-31 |

3. 수집 데몬 상태 현황

| 분석시스템 | 서비스 유형 | 관리포트 | 수집로그 수 | 상태 | 로딩시간 |
|---|---|---|---|---|---|
| master - 10.0.2.214 | coordinator | 8503 | 0 | 1 | 2015-08-27 |
| master - 10.0.2.214 | mgmt | 8502 | 0 | 1 | 2015-08-27 |
| master - 10.1.2.18 | agentreceiver | 8511 | 1 | 0 | 2015-06-17 |
| master - 10.0.2.214 | dbms | None | 0 | 2 | 2015-08-13 |
| master - 10.0.2.214 | snmp | None | 0 | 0 | 2015-07-14 |
| master - 10.0.2.214 | netflow | 8508 | 0 | 1 | 2015-07-14 |
| master - 10.0.2.223 | syslog | 8501 | 1 | 0 | 2015-07-24 |
| master - 10.0.2.214 | syslog1 | 8509 | 1 | 4 | 2015-08-25 |
| master - 10.0.2.214 | snmptrap | 8504 | 0 | 1 | 2015-07-26 |
| master - 10.0.2.214 | syslog3 | 8512 | 1 | 2 | 2015-08-13 |
| master - 10.0.2.172 | syslog | 8501 | 1 | 0 | 2015-03-23 |
| master - 10.0.2.214 | agentreceiver | 8511 | 1 | 56 | 2015-09-02 |
| master - 10.0.2.223 | agentreceiver | 8511 | 1 | 0 | 2015-07-24 |
| master - 10.0.2.214 | syslog2 | 8510 | 1 | 2 | 2015-08-25 |
| master - 10.0.2.214 | syslog | 8501 | 1 | 11 | 2015-08-25 |

### 각 보안 장비별 이벤트 발생 현황



Event Management System

FIREWALL

Firewall(방화벽)은 전용통신망에 불법 사용자들이 접근하여 컴퓨터 자원을 사용 또는 교란하거나 중요한 정보들을 불법으로 외부에 유출하는 행위를 방지하는 것이 목적입니다. 방화벽에서 탐지되는 이벤트를 조회하여 해당 로그에 대한 경로 등 이벤트 상세 정보를 확인할 수 있으며, 해당 목표에 대한 보안정책 수립에 도움을 줄 수 있습니다.

7월 차단 이벤트 발생 수 15,672 회

영역/유저별 차단 순위

분야별 공격에 가장 많이 노출된 top5 정리.

| | 6월 | 7월 | |
|---|---|---|---|
| 1 | HTTP | MS-SQL | 42% |
| 2 | MS-SQL | HTTP | 30% |
| 3 | HTTPS | RDP | 18% |
| 4 | RDP | HTTPS | 6% |
| 5 | SSH | SSH | 4% |

영역/유저별 차단 순위

분야별 공격에 가장 많이 노출된 유저들의 top5 정리.

| | HTTP | HTTPS | MS-SQL | RDP |
|---|---|---|---|---|
| 1 | 김상훈_197851 | 한동훈_156723 | 유민상_106453 | 유민상_106453 |
| 2 | 한동훈_156723 | 유민상_106453 | 한동훈_156723 | 김숙자_100154 |
| 3 | 유민상_106453 | 김숙자_100154 | 김숙자_100154 | 한동훈_156723 |
| 4 | 김숙자_100154 | 김상훈_197851 | 김상훈_197851 | 유해민_100345 |
| 5 | 유해민_100345 | 유해민_100345 | 유해민_100345 | 김상훈_197851 |

HTTP - [Hyper Transfer Protocol] 인터넷에서 웹서버와 사용자의 인터넷 브라우저 사이에 하이퍼텍스트
HTTPS - [Hyper Transfer Protocol over Secure sockets layer] HTTP계층 아래 SSL 단에서 사용자 페이지
MS-SQL - 마이크로소프트(MS)에서 개발한 프로그래밍 언어로 각종 자료를 저장하는 데이터베이스(DB)
RDP - [Remote Desktop Protocol] 신뢰 데이터그램 프로토콜 원격 데스크톱 프로토콜.
SSH - [Secure Shell] 공개 키 방식의 암호 방식을 사용하여 원격지 시스템에 접근하여 암호화된 메시지

IPS [Intrusion Prevention System]

IPS(Intrusion Prevention System)은 침입방지 시스템입니다. 외부 인터넷의 침해공격 으로부터 내부망의 자산을 안전하게 보호하고 침입을 사전에 탐지 및 차단하는 목적으로 사용됩니다. 탐지와 차단을 동시에 제공할 수 있는 보다 진보된 형태의 보안 솔루션입니다. 고객사의 네트워크를 통해서 시도된 공격들에 대해서 IPS시스템에서 탐지한 이벤트들을 기반으로 하여 IPS 이벤트 종계 정보 및 이벤트 유형 Top 5 사용자 정보를 제공합니다.

7월 차단 이벤트 발생 수 15,672 회

영역/유저별 차단 순위

분야별 공격에 가장 많이 노출된 top5 정리.

| | 6월 | 7월 | |
|---|---|---|---|
| 1 | HTTP | MS-SQL | 42% |
| 2 | MS-SQL | HTTP | 30% |
| 3 | HTTPS | RDP | 18% |
| 4 | RDP | HTTPS | 6% |
| 5 | SSH | SSH | 4% |

영역/유저별 차단 순위

분야별 공격에 가장 많이 노출된 유저들의 top5 정리.

| | HTTP | HTTPS | MS-SQL | RDP | SSH |
|---|---|---|---|---|---|
| 1 | 김상훈_197851 | 한동훈_156723 | 유민상_106453 | 유민상_106453 | 한동훈_156723 |
| 2 | 한동훈_156723 | 유민상_106453 | 한동훈_156723 | 김숙자_100154 | 김숙자_100154 |
| 3 | 유민상_106453 | 김숙자_100154 | 김숙자_100154 | 한동훈_156723 | 김상훈_197851 |
| 4 | 김숙자_100154 | 김상훈_197851 | 김상훈_197851 | 유해민_100345 | 유해민_100345 |
| 5 | 유해민_100345 | 유해민_100345 | 유해민_100345 | 김상훈_197851 | 유민상_106453 |

HTTP - [Hyper Transfer Protocol] 인터넷에서 웹서버와 사용자의 인터넷 브라우저 사이에 하이퍼텍스트 문서를 전송하는 것.
HTTPS - [Hyper Transfer Protocol over Secure sockets layer] HTTP계층 아래 SSL 단에서 사용자 페이지를 암호화 하는 것.
MS-SQL - 마이크로소프트(MS)에서 개발한 프로그래밍 언어로 각종 자료를 저장하는 데이터베이스(DB) 서버.
RDP - [Remote Desktop Protocol] 신뢰 데이터그램 프로토콜 원격 데스크톱 프로토콜.
SSH - [Secure Shell] 공개 키 방식의 암호 방식을 사용하여 원격지 시스템에 접근하여 암호화된 메시지를 전송할 수 있는 시스템.

# 2.4 주요 기능

## 2.4.8 증적감사 주요 요구기능

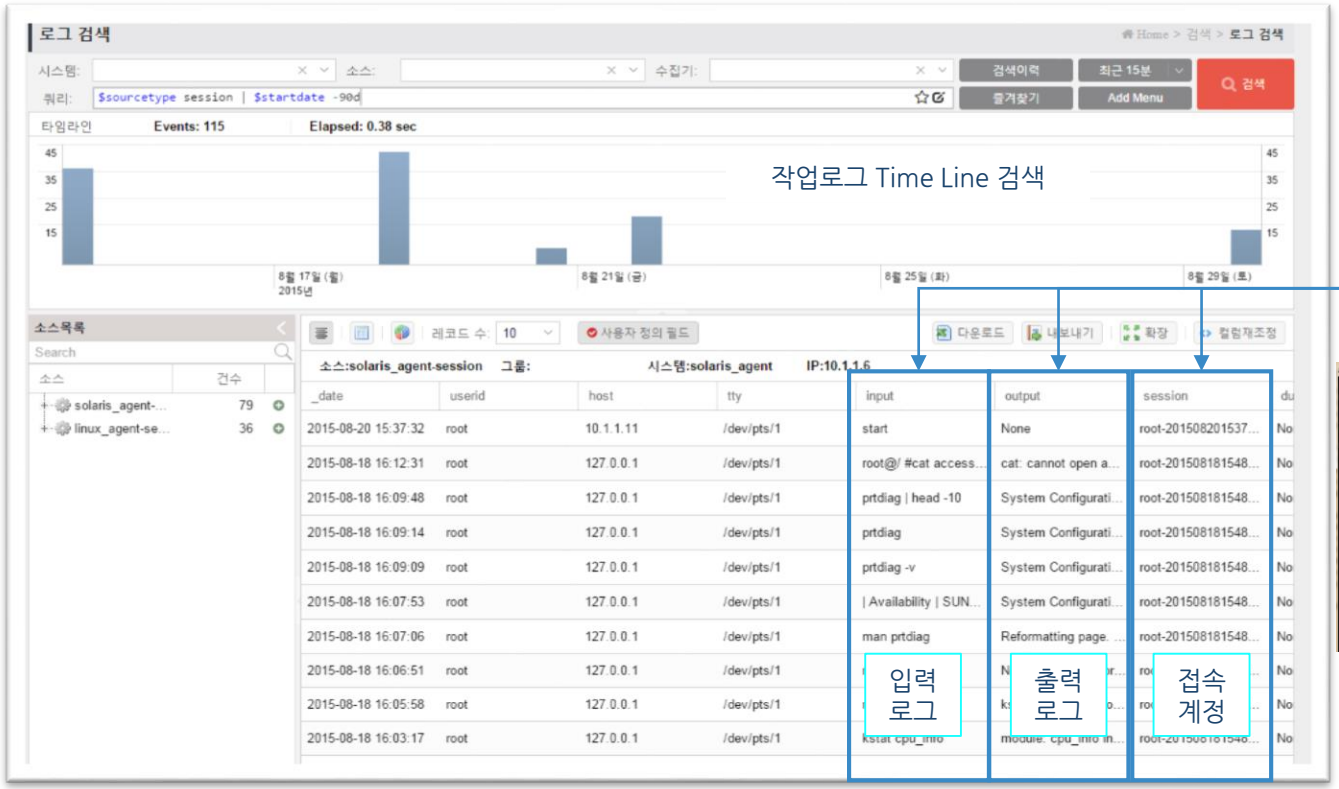
로그수집, 저장 뿐만 아니라 증적감사를 위한 다양한 부가 기능 제공

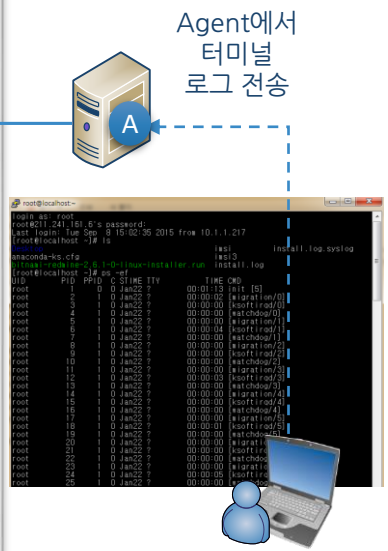
| 구분 | 항목 | 지원 여부 | 지원 내역 |
|---|---|---|---|
| 로그수집 | 특정 디렉토리 및 파일이름 지정 | O | 로그 수집 시 특정 디렉토리나 파일 이름 지정 가능 |
| | Agent를 통한 수집 시 Open Port 정보 수집 | O | 취약점 여부 확인을 위해 서버에 설치하는 Agent에서 Open Port 정보 수집 |
| 로그저장 | WORM 저장 기능 | O | 저장 주기(1H, 1D 등)를 설정하여 WORM에 저장할 수 있도록 제공 |
| | 블루레이 저장 기능 | O | 평상 시 로컬에 저장하며, 감사 요청 시 특정 조건의 로그만 UI에서 선택하여 해당 원본로그를 블루레이에 저장할 수 있도록 제공 |
| | 원본로그, 압축로그 분리 저장 기능 | O | 원본로그와 압축로그를 별도 분리하여 저장 |
| 증적감사 | 터미널 접속 및 Command History | O | 증적감사 기능을 통해 wtmp, utmp, sulog 등 증적감사를 위한 접속 및 작업이력 로그 수집 및 분석 제공 |
| | 원본 및 압축로그 무결성 감지 후 통보 | O | 무결성 감지 시 위변조 파일을 적색으로 표시하고 SMS, Mail로 알림 |
| | 적발 사용자에 대한 상세 정보 매칭 표시 | O | 인사DB 정보 및 사용IP, Host, MAC Addr 등 사용현황 정보를 표시 |
| | 2차 인증 기능 | O | SMS, Mail, OTP와 연동한 2차 인증 제공 |
| | 원본 및 분석로그 삭제 방지 | O | 삭제할 수 있는 명령어 실행 불가하도록 차단 |
| | 증적감사 솔루션 사용자/관리자의 행위 로깅 기능 제공 | O | 본 솔루션에 접속 및 조회, 출력 등 모든 작업행위 로그 저장 및 제공 |
| | 로그 신뢰성 확보 기준 마련을 위한 NTP 서버관리 | O | 솔루션 설치 시 NTP 서버 설정 필수로 제공 |

# 2.4 주요 기능

## 2.4.9 터미널 접속 및 작업이력 감사기능

시스템에 터미널로 로그인/로그아웃 등 접속이력과 작업행위이력에 대한 감사 기능 제공

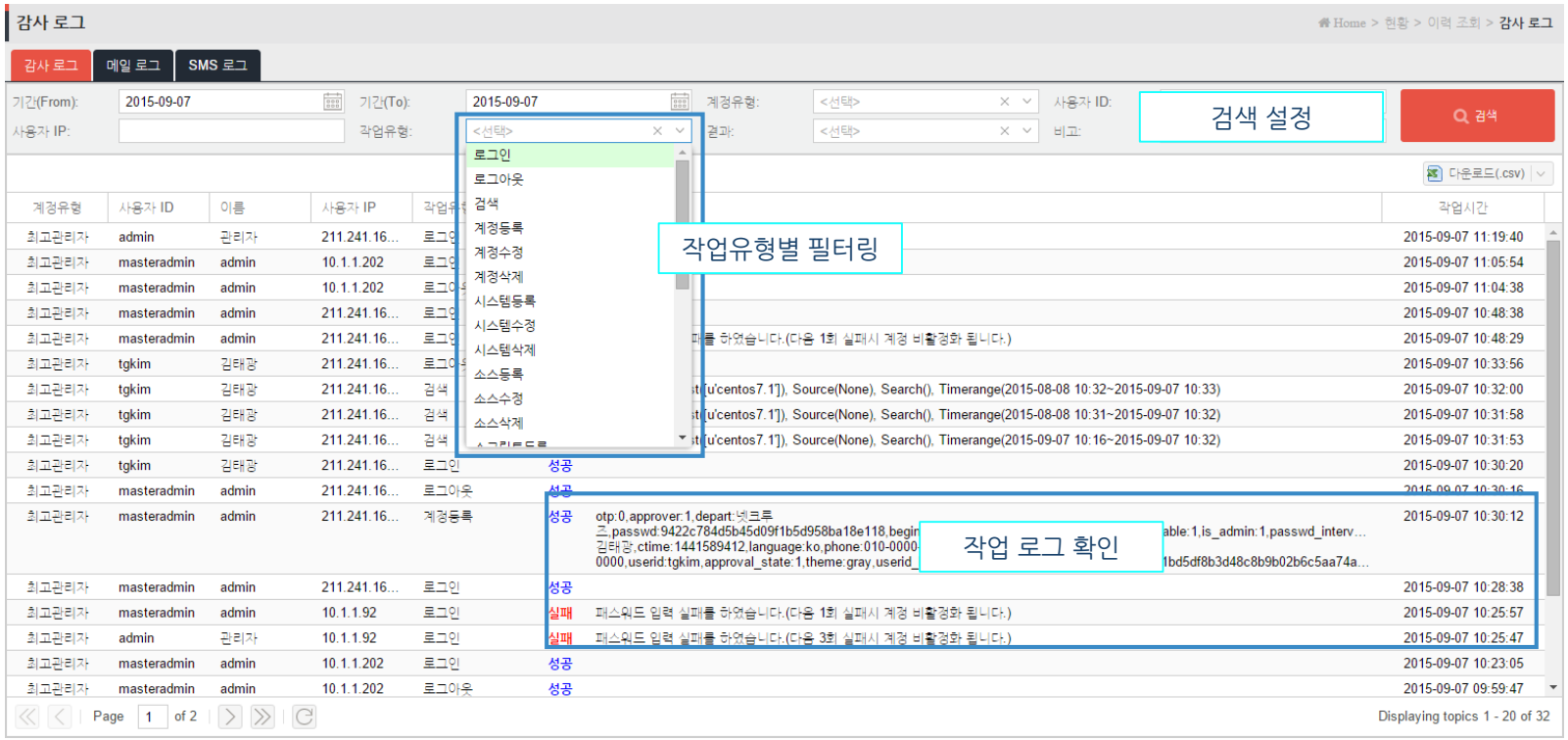


# 2.4 주요 기능

## 2.4.10 솔루션 행위 감사로그 기능

증적감사 솔루션에 접속 및 작업행위에 대한 감사로그 기능 제공

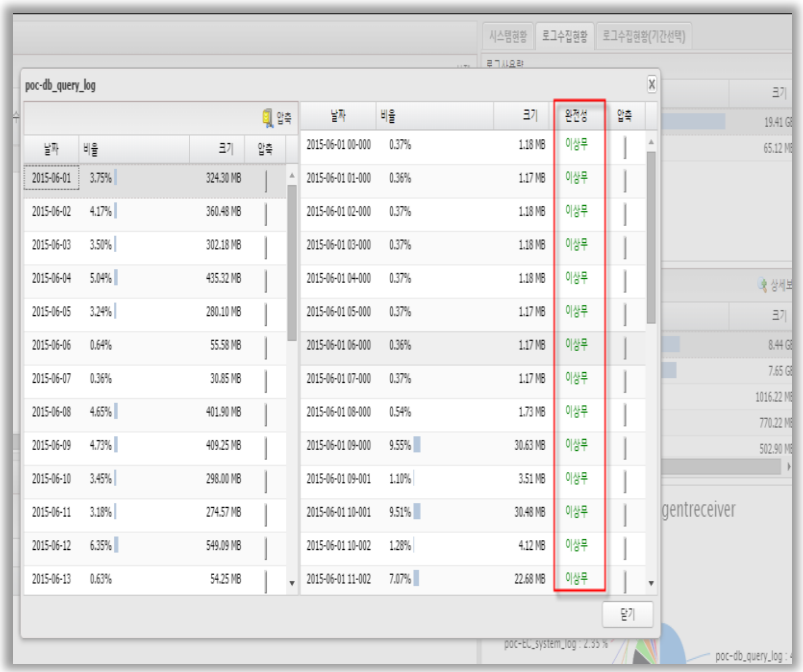


# 2.4 주요 기능

## 2.4.11 로그 무결성 및 보안성 제공 기능

로그 무결성 보장을 위한 체크 및 알람과 감사 기록 및 관리에 대한 보안성 제공

### 무결성 검사 체크 기능




- 수집된 로그에 대하여 무결성 검사를 확인하기 위한 UI 제공
- 위/변조 확인 시 관리자에게 적색, SMS, Mail 등 알람 제공

### 법률 규제 및 지침 만족

- 전자금융거래법 제22조 (전자금융거래기록의 생성 및 보존)
  - 전자금융거래의 내용을 5년의 범위 안에서 보관
- 전자금융감독규정 제13조 (전산자료 보호대책)
  - 8) 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전 지역에 소산하고 백업 내역을 기록·관리할 것
  - 11) 정보처리시스템의 가동 기록은 1년 이상 보존할 것
- 전자금융감독규정 제14조 (정보처리시스템 보호대책)
  - 8) 중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전 지역에 소산하고 백업자료는 1년 이상 기록·관리할 것

### 높은 보안성 제공

- 로그 저장 영역에 대한 접근을 자체 보안기능을 통한 통제
  - Root 권한도 수집/분석된 로그에 대한 삭제 및 이동 불가
  - 제품 자체 관리 기능을 통하여 삭제 및 백업 기능 지원
- 로그 정책 및 수집 정보 등 데이터 구간을 암호화
  - 최신 OpenSSL 제공 (버전업 시 긴급으로 패치 지원)
  - 관리자 인증, 로그파일, Config 등에 대한 최신 암호화 적용
  - AES, SEED, ARIA 등 기본 제공


21

# 2.4 주요 기능

## 2.4.12 수집 및 검색 성능

TTA 공인시험기관에서 검증된 수집 및 검색 성능 보장

### 대용량 로그 수집 시 패킷 손실율 0% 검증

4. 시험 결과

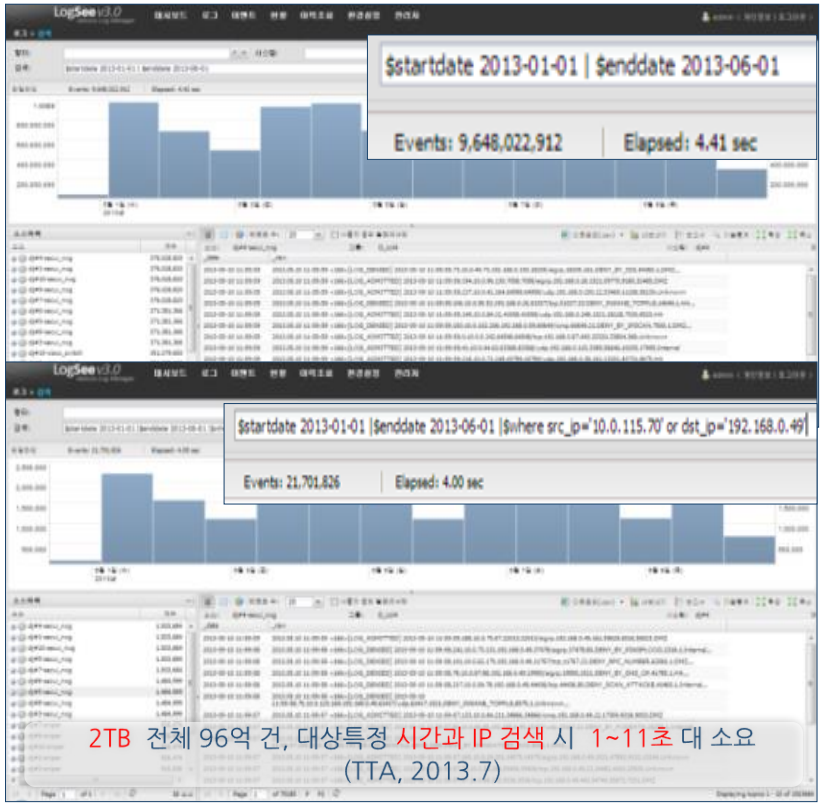
| 순번 | 시험 항목명 | 측정항목 | 관련 TS | 시험 결과 | 비고 |
|---|---|---|---|---|---|
| 1 | 로그 수집 | EPS (Events Per Second) | TS_1 | 시험대상 제품(수집서버) 1대당 시험대상 제품(수집서버)의 | 의 패킷을 의 총 패킷 수 데이터) 수 : 10,079,699,639개 |
| | | | TS_2 | 시험대상 제품(수집서버) 1대당 패킷 수집 속도가 80,000 EPS인 경우, 시험대상 제품(수집서버)의 패킷 손실률은 0%로 나타남 | - 수집서버 수 : 총 1대<br>-1대의 수집서버가 초당 80,000개의 패킷을 수집함<br>- 패킷발생기에서 수집서버로 전송된 총 패킷 수 : 288,115,136개<br>- 수집서버에 저장된 총 로그(패킷 데이터) 수 : 288,115,136개 |
| 2 | 로그 검색 | 검색시간 (초) | TS_3 | - 시험대상 제품(분석서버)에서 일반검색 조건을 만족하는 로그가 검색될 때까지 6.19초가 소요됨 (검색된 로그 수 : 20,457개)<br>- 시험대상 제품(분석서버)에서 LIKE검색(%) 조건을 만족하는 로그가 검색될 때까지 5.65초가 소요됨 (검색된 로그 수 : 100,633개)<br>※ 시험대상 제품의 '캐싱' 기능을 적용한 결과치 임 | - 패킷발생기에서 수집서버로 전송된 총 패킷 수 : 4,896,148,324개<br>- 수집서버에 저장된 총 로그(패킷 데이터) 수 : 4,619,575,559개<br>-패킷 손실률 : 5.65% |

공인시험기관 TTA로부터 80,000EPS 패킷손실률 0% 입증

2013-06-27

80,000 EPS 수집 시험 시 패킷 손실률 0%로 검증된 시스템
(TTA, 2013.7)

### 대용량 데이터의 신속한 검색 성능




2TB 전체 96억 건, 대상특정 시간과 IP 검색 시 1~11초 대 소요
(TTA, 2013.7)

# 2.4 주요 기능

## 2.4.13 다양한 실시간 검색 및 이벤트 등록

단일 소스(시스템) 및 다중 소스로부터 수집되는 로그를 기반으로 다양한 조건으로 이벤트 등록

### 실시간 이벤트 설정


- 단일 장비(소스) 분석 제공
- 로그 발생 카운트, 문자열, 수집시간 등 단순 조건을 통해 이벤트 설정
- 탐지할 조건, 이벤트 발생 시 알림 방법, 알람 방법 등 설정

### 이기종 연관분석 위한 검색 이벤트 설정


- 이기종 멀티 장비간 연관 분석 제공
- 쿼리문으로 검색을 통해 이벤트 설정
- 탐지할 조건, 대상 시스템, 검색 주기, 이벤트 발생 시 알림 방법, 알람 방법 등 설정

# 2.4 주요 기능

## 2.4.14 비정형 로그에 대한 수집 및 처리

비정형화된 로그 수집이 가능하고 원시 데이터를 저장하거나 정형화된 로그로 필터링 하여 저장

### 비정형화 로그 예)

레코드 수: 20 사용자 정의 필드에서만

소스: 마스터-session 그룹: netcruz 시스템: 마스터

| _date | _raw |
|---|---|
| 2014-01-24 16:27:52 | command root-20140124162629-794, root, 211.36.149.127, ps -ef \| grep logsee_logsee, root 25525 25300 0 16:27 pts/214 00:00:00 grep logsee_logsee |
| 2014-01-24 16:27:05 | command root-20140124162629-794, root, 211.36.149.127, ps -ef \| logsee_syslog, -bash: logsee_syslog: command not found |
| 2014-01-24 16:26:59 | command hts-20140124144350-8227, hts, 39.7.57.157, 2014-01-24 16:24:02+0900 [-] Received SIGTERM, shutting down., (dhna) hts@logsee_master 0:bash 1:bash 2:bash 3:bash 4:bash 5:psql 6:bash* 7:python2.7- 'hts@logsee_master:~/lo" 16:24 24-Jan-14 2014-01-24 16:24:02+0900 [-] logsee Graceful shutdown success 2014-01-24 16:24:02+0900 [-] (UNIX Port '/tmp/logsee_dbms.sock' Closed) 2014-01-24 16:24:02+0900 [-] success to unresitgerFeeder 2014-01-24 16:24:02+0900 [Broker (TLSMemoryBIOProtocol),client] connection lost to IPv4Address(TCP, '127.0.0.1', 8500), reason <twisted.python.failure.Failure <class 'twisted.internet. |
| 2014-01-24 16:26:50 | command hts-20140124145341-7072, hts, 211.241.161.120, 216 # --------- connect functions ---------- 217 @defer.inlineCallbacks 218 def oracleConnect(self): 219 if self.databaseFormat: 220 database = timeutil.getHumanTimeFromUnixTime(time()-60, self.databaseFormat) 221 else: 222 database = self.database 223 224 dsn = cx_Oracle.makedsn(self.dbmsIP, self.dbmsPort, database) 225 if self.ORACLE_NLS_LANG is None: 226 dbPool = adbapi.ConnectionPool("cx_Oracle", self.dbmsUser, self.dbmsPassword, dsn) 227 try: 228 rs = yield dbPool.runQuery("SELECT parameter, value from v$nls_parameters WHERE parameter IN ('NLS_CHARACTERSET', 'NLS_LANGUAGE', 'NLS_TERRITORY')") 229 except: 230 try: dbPool.close() 231 except: pass 232 defer.returnValue(None) 233 234 nls_lang = {} 235 for param, val in rs: 236 nls_lang[param] = val 237 self.ORACLE_NLS_LANG = os.environ['NLS_LANG'] = "%s_%s.%s" % (nls_lang['NLS_LANGUAGE'], nls_lang['NLS_TERRITORY'], nls_lang['NLS_CHARACTERSET']) 238 try: dbPool.close() 239 except: pass 240 else: 241 os.environ['NLS_LANG'] = self.ORACLE_NLS_LANG 242 dbPool = adbapi.ConnectionPool("cx_Oracle", self.dbmsUser, self.dbmsPassword, dsn) 243 if self.database is None: 244 self.database = database 245 elif database != self.database: 245,24 25% , 486 def _run(dbType): 487 mif self.isMatchTime(minutes, hours, days, months, weeks): 488 self.runReal(dbType) 489 else: 490 reactor.callLater(self.interval, self.run, dbType) 491 return _run 492 493 @defer.inlineCallbacks 494 def runReal(self, dbType): 495 dbPool = yield self.dbConnect() 496 if dbPool is None: 497 reactor.callLater(self.interval, self.run, dbType) 498 defer.returnValue(None) 499 500 if self.tableNameFormat is not None: 501 tableName = timeutil.getHumanTimeFromUnixTime(time()-60, self.tableNameFormat) 502 isTable = yield isTableExists(dbPool, dbType, tableName) 503 if isTable: 504 if self.tableName is None: 505 self.tableName = tableName 506 elif tableName != self.tableName: 507 self.tableName = tableName 508 self.baseline = None 509 else: 510 if self.tableName is None: 511 try: dbPool.close() 512 except: pass 513 reactor.callLater(self.interval, self.run, dbType) 514 defer.returnValue(None) 515 516 if dbType in ('mssql', 'oracle'): 517 try:486 def _run(dbType): 487 if self.isMatchTime(minutes, hours, days, months, weeks): 488 self.runReal(dbType) 489 else: 490 reactor.callLater(self.interval, self.run, dbType) 491 return _run 492 493 @defer.inlineCallbacks 494 def runReal(self, dbType): 495 dbPool = yield self.dbConnect() 496 if dbPool is None: 497 reactor.callLater(self.interval, self.run, dbType) 498 defer.returnValue(None) 499 500 if self.tableNam eFormat is not None: 501 tableName = timeutil.getHumanTimeFromUnixTime(time()-60, self.tableNameFormat) 502 isTable = yield isTableExists(dbPool, dbType, tableName) 503 if isTable: 504 if self.tableName is None: 505 self.tableName = tableName 506 elif tableName != self.tableName: 507 self.tableName = tableName 508 self.baseline = None 509 else: 510 if self.tableName is None: 511 try: dbPool.close() 512 except: pass 513 reactor.callLater(self.interval, self.run, dbType) 514 defer.returnValue(None) 515 516 if dbType in ('mssql', 'oracle'): 517 try: 518 ret = yield self.runQuery(dbPool) |

- 소스타입(로그 수집 시스템)별 비정형화된 로그의 raw data를 패턴정의 없이 저장

### 정형화 후의 로그 예)

레코드 수: 20 사용자 정의 필드에서만

소스: 마스터-session 그룹: netcruz 시스템: 마스터

| _date | userid | host | tty | input | output | session | duration | _ip |
|---|---|---|---|---|---|---|---|---|
| 2014-01-24 16:27:52 | root | 211.36.149.127 | /dev/pts/212 | ps -ef \| grep logsee... | root 25525 25300 0 ... | root-201401241626... | None | 211.241.161.214 |
| 2014-01-24 16:27:05 | root | 211.36.149.127 | /dev/pts/212 | ps -ef \| logsee_syslog | -bash: logsee_syslo... | root-201401241626... | None | 211.241.161.214 |
| 2014-01-24 16:26:59 | hts | 39.7.57.157 | /dev/pts/196 | 2014-01-24 16:24:0... | (dhna) hts@logsee_... | hts-201401241443 5... | None | 211.241.161.214 |
| 2014-01-24 16:26:50 | hts | 211.241.161.120 | /dev/pts/114 | 216 # --------- conn... | 486 def _run(dbTyp... | hts-201401241453 4... | None | 211.241.161.214 |
| 2014-01-24 16:26:29 | root | 211.36.149.127 | /dev/pts/212 | start | None | root-201401241626... | None | 211.241.161.214 |
| 2014-01-24 16:25:59 | hts | 39.7.57.157 | /dev/pts/196 | In [11]: MI_MailDat... | (dhna) hts@logsee_... | hts-201401241443 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:40 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:40 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:39 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:39 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:39 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:38 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:38 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:38 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:37 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:07 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:06 | hts | 211.241.161.179 | /dev/pts/210 | ssh localhost -p 8787 | ssh: connect to host... | hts-201401241451 5... | None | 211.241.161.214 |
| 2014-01-24 16:25:04 | hts | 211.241.161.120 | /dev/pts/114 | >>> 'hts@logsee_... | 7 # Changelog: 8 # ... | hts-201401241453 4... | None | 211.241.161.214 |
| 2014-01-24 16:25:01 | hts | 211.241.161.179 | /dev/pts/11 | [hts@logsee_maste... | (hokeong) hts@logs... | hts-201401231906 0... | None | 211.241.161.214 |
| 2014-01-24 16:24:57 | hts | 211.241.161.179 | /dev/pts/210 | history | 7 2014-01-22 18:24... | hts-201401241451 5... | None | 211.241.161.214 |

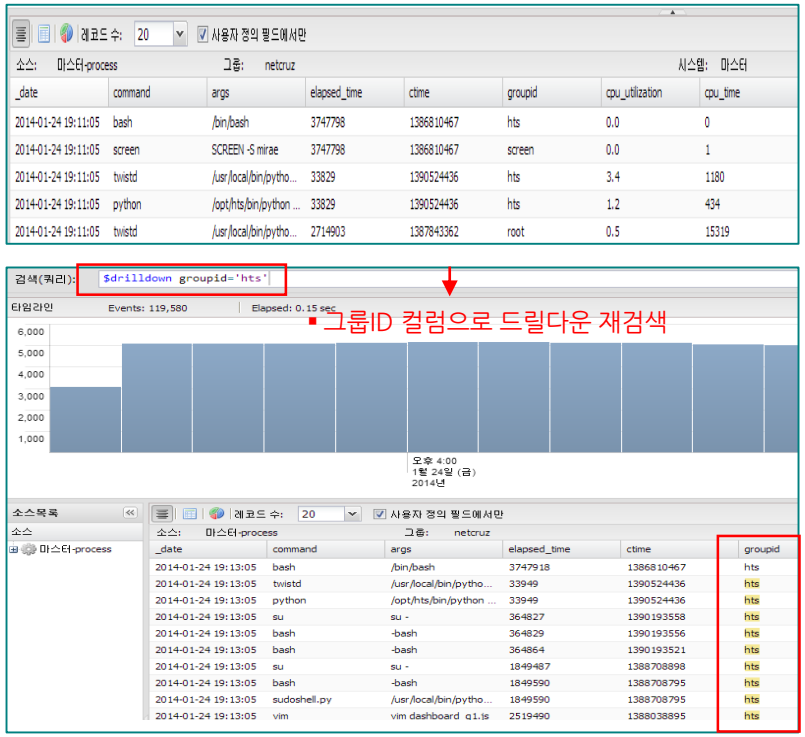
- 비정형화된 로그를 정형화(Filter 적용)하여 좀더 효율적인 패턴(시나리오) 분석도 가능

# 2.4 주요 기능

## 2.4.15 탐지 정보에 대한 추가 상세 검색

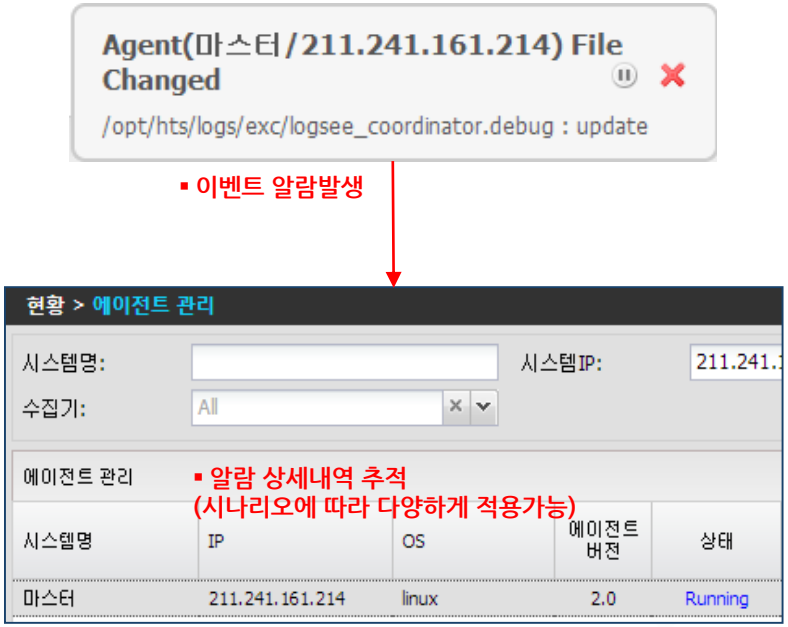
수집된 로그로부터 탐지를 위한 검색 또는 이벤트, 대시보드 형태의 감시 후 결과 내, 재 검색이 가능

### 일반 검색 및 드릴다운 재검색




▪ 그룹ID 컬럼으로 드릴다운 재검색

### 이벤트 발생 시 추적




▪ 이벤트 알람발생

▪ 알람 상세내역 추적
(시나리오에 따라 다양하게 적용가능)

# 3.1 인증서

## TTA 및 IT보안 인증사무국으로부터 CC 인증 및 GS 인증 획득

### CC인증 [2015. 2. 4]

제2015-12호

# 인 증 서

ISIS-0584-2015

netcruz Log Manager LogSee V3.0

| | |
|---|---|
| 신 청 기 관 : (주)넷크루즈 | 보 증 등 급 : EAL2 |
| 보안요구사항 : 없음 | 평 가 기 관 : 한국정보보안기술원 |
| 인증보고서 번호 : CR-15-12 | |
| 발 급 일 자 : 2015년 2월 4일 | 만 료 일 자 : 2018년 2월 3일 |

위 제품은 국가정보화 기본법 제38조, 동법 시행령 제35조의 규정에 의거 평가한 결과가 정보보호제품 인증기준에 적합함을 인증한다. 이 정보보호제품은 정보보호제품 평가인증 수행규정에 근거한 평가기관이 공통평가기준(CC) 버전 3.1 R2와 공통평가방법론(CEM) 버전 3.1 R2를 적용하여 평가한 것이다. 본 인증서는 인증보고서에서 명시한 제품 구성환경 및 버전만을 보증하며, 국내에서만 효력이 인정된다. 본 인증서는 IT보안인증사무국(ITSCC) 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

IT보안인증사무국장

최신 보안 이슈 및 취약점을 총괄한 통합로그 시험기준[2014.12] 및 보안 기능 요구사항 모두 충족

### GS인증 [2013. 11. 25]

# 소프트웨어품질인증서

*Certificate of Software Quality*

| | |
|---|---|
| 상호 또는 성명 Trade Name or Applicant | ㈜넷크루즈(220-86-17642) netcruz Co., Ltd. |
| 소프트웨어의 명칭 Name of Software | 넷크루즈 통합 로그 관리 시스템 v3.0 netcruz Log Manager LogSee v3.0 |
| 인증번호 Certification No. | 13-0260 |
| 제조자 및 제조국가 Manufacturer and Nation | ㈜넷크루즈/대한민국 netcruz Co., Ltd./Republic of Korea |
| 인증년월일 Date of Certification | 2013년(Year) 11월(Month) 25일(Day) |
| 기 타 Others | |

위 소프트웨어는 소프트웨어산업진흥법 제13조에 의하여 품질이 인증되었음을 증명합니다.

We testify that the quality of foregoing software has been certified under the Software Industry Promotion Act.

2013 년(Year) 11 월(Month) 25 일(Day)

TTA 한국정보통신기술협회장
CEO & President
Telecommunications Technology Association

# 4.1 Reference

## 공공

대법원 | 금융결제원 | 중소기업청 | 인천소방안전본부 | 한국장학재단
환경부 | 국민건강보험공단 | 한국전력거래소 | 특허청 | 농림수산식품부
안전행정부 | 서울특별시 | 한국과학기술정보연구원 | NPS 국민연금 | 국세청
세계속의 경기도 | Digital GURO | 송파구 | 통영시 | 사천시
참진주 CharmJinju | 경상북도 | 남해군 | 경산시 | 영암군
Fantasia 부천시 | 창원시 | 한국전력공사 | 한국철도시설공단 | 국방홍보원
NFRI 국가핵융합연구소 | 한국산업인력공단 | 대전교육정보원 | KISDI 정보통신정책연구원 | 중앙선거관리위원회
CRMO 중앙전파관리소 | KRX 한국거래소

## 금융

Prudential Financial 푸르덴셜투자증권 | SAMSUNG 삼성증권 | 동부증권 | Standard Chartered SC 제일은행 | LOTTECARD
SAMSUNG 삼성화재 | 신한은행

## 대학 / 교육 / 의료

인천광역시교육청 | 충청남도교육청 | 전라남도교육청 | 대구보건대학 | 국립안동대학교
한국외국어대학교 | 남부대학교 NAMBU UNIVERSITY | KIAS 고등과학원 | 전국지방의료원연합회 | 포항성모병원

## 일반 기업

HANKOOK | KEPCO 전력연구원 | 코오롱인더스트리 | AMOREPACIFIC | SAMIL
SK C&C | SAMSUNG 삼성SDS | BGF캐시넷 | C&M (주)씨앤앰 | LG U+

## 수사기관 / 기타

대구지방경찰청 | 경북지방경찰청 | CYBER COP NETAN | 대검찰청 | 필리핀 정부

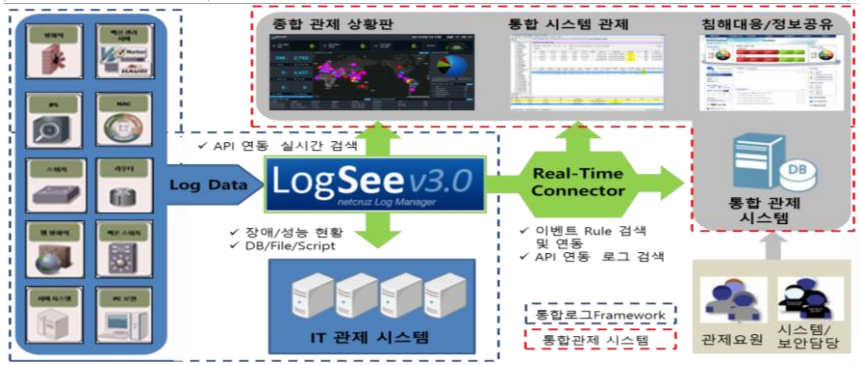
# 4.1 Reference

## 4.1.1 중앙OOOO위원회

통합로그 수집 엔진을 기반으로 관제범위 확대 및 새로운 통합 침해대응 시스템 구축

### 중앙OOOO위원회 구축 개요

| 항 목 | 내 용 |
|---|---|
| 프로젝트명 | 통합로그관리시스템 고도화 사업 |
| 구축기간 | 2013년 11월 ~ 2014년 2월 (4개월) |
| 도입시스템 | ▪ nLM-LogSee, 대시보드, 수집 엔진 Connector<br>IT 관제모듈 |
| 도입목적 | ▪ 기 운영 중인 통합로그관리 시스템의 고도화 필요<br>▪ 정보보호 대상 시스템 확충으로 관리범위 확대 및 로그관리 이용한 관제체계 수립 필요 |




### 구축 특징 및 기대효과

1. 네트워크 및 시스템 약 300여대, 정보보안 시스템 30여대, 개별 관제 시스템 10여대 연동
2. 일 최대 30G 데이터 수집 및 분석 처리
3. 개별 관제 시스템(NMS/SMS/ESM) 연동

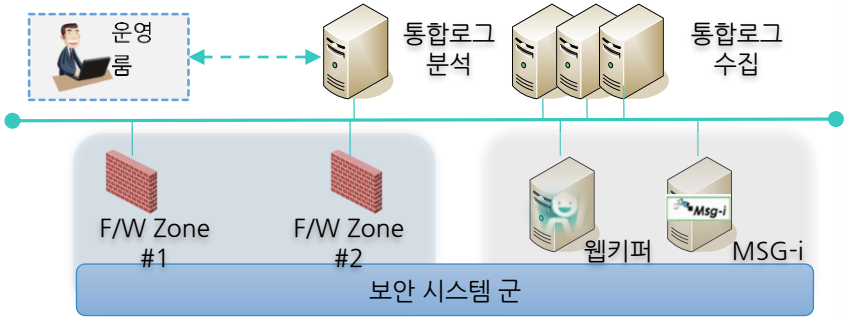
# 4.1 Reference

## 4.1.2 삼성화재

FW 장비군의 세션 관련 로그정보를 분석하여 보안 위협을 상시 모니터링 수행

### 삼성화재 구축 개요

| 항 목 | 내 용 |
|---|---|
| 프로젝트명 | 보안장비 로그분석 시스템 구축 |
| 구축기간 | 2013년 11월 ~ 2013년 12월 (2개월) |
| 도입시스템 | ▪ nLM-LogSee, 분석서버 1식, 수집서버 3식 |
| 도입목적 | ▪ Secul_MF2 방화벽 20여식(방화벽 로그분석), 네트워크장비 50여식 연동<br>▪ WebKeeper / MSG-I연동을 통한 인터넷 및 메신저 내용 상세분석, 모니터링 |



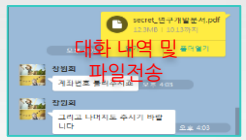

### 삼성화재 구축 특징 및 기대효과

**1 방화벽 로그 상세 분석**
**(5가지 내용, 집중 모니터링 및 기간별 비교)**

Allow | Deny | 3. F/W Traffic | 4. F/W Resource | 5. 3Way HandShake

**2 인터넷 접근관련 상세 분석**
**(웹키퍼, 사이트 접속 카테고리 매핑)**


**3 메신저 통합모니터링**
**(MSG-I, 로그 DB 연동)**



# 5.1 별첨

## 5.1.1 타사 비교 자료

| 구분 | | nLM LogSee | S사 SGA-ESM | I사 LogCenter NEO | N사 Logsaver |
|---|---|---|---|---|---|
| 아키텍처 | 제품형태 | 소프트웨어 | S/W | Appliance | Appliance |
| | 인증 | CC, GS | CC, GS | HXC 버전 (CC, GS)<br>NEO 버전 (없음) | CC, GS |
| | 대용량 로그수용기술 | 분산처리 기술 (MapReduce),<br>무제한 확장 설계 | 부분지원 (필요로그만 추출) | 지원<br>(HXC : Hybrid eXtended Cloud) | 없음 |
| | HA (이중화) 지원 | 지원 | 미 지원 | 미 지원 | 지원 |
| | 로그저장DB | 자체 파일DB<br>설정정보 : Postgres (Open DB) | Oracle, MySQL | 상용 DBMS, Oracle | 상용 DBMS, MS-SQL,<br>원본로그저장(DVD-R) |
| | 관리 인터페이스 | Web (IE, Chrome, Firefox, Safari 등 모든 브라우저 지원) | Manager Console 설치(Windows용) | Web<br>(Chrome 지원) | Web, C/S |
| 로그수집 | 로그수집 방식 | syslog, snmp, get/walk/trap, flow,<br>ftp/sftp, DB Link, TCP/UDP, Agent | Agent, Syslog 등 일부 지원 | Agent, Syslog, SNMP 등<br>다양한 수집방식 지원 | Agent, Syslog, SNMP 등<br>다양한 수집방식 지원 |
| | 신규로그 연동방안 | 정규화 기반 필터생성/사용자작성/<br>지원 필요 시 1일 내 | 지원<br>(정해진 로그/DB외 지원 어려움) | 지원 | 지원 |
| | 로그 호스트 관리 | 지원 | 지원 | 지원 | 미 지원 |
| | 로그 파싱 & 필터링 | 동적필드 추출 및 자동 파싱 | 지원 | 지원 | 미 지원 |
| | 수집 성능 | 80,000 EPS(대당), 7.5MB/sec (200Byte 로그 기준) [TTA, 2013] | 확인불가<br>(공인된 수집 성능 지표 없음) | 40,000 EPS | 16,666EPS, 5MB/sec<br>(300Byte 로그 기준) |
| 로그저장 | 암호화 지원 | 지원 (AES 256 Bit) | 수집 시 SSL만 지원 | 지원 (3 DES) | 지원<br>(Packet Write 자체 파일포맷) |
| | 원본 무결성 검증 | 지원 (SHA 512 Bit) | 미지원 | 지원 (SHA 2) | 지원<br>(Packet Write 자체 파일포맷) |

# 5.1 별첨

## 5.1.1 타사 비교 자료

| 구분 | | nLM LogSee | S사 SGA-ESM | I사 LogCenter NEO | N사 Logsaver |
|---|---|---|---|---|---|
| 로그저장 | 압축 지원 | 지원 (압축률 70%) | 지원 (RAW 데이터 저장) | 지원 (90% 압축) | 지원 (최대 10배) |
| | 고속검색 인덱싱 여부 | 지원 (개별/전체 인덱싱 선택가능) | 미 지원 | 지원 | 미 지원 |
| | 로그자동 보관 및 폐기 | 지원 | 부분 지원 | 지원 | 미 지원<br>(DVD에 저장하기 때문에 수동폐기) |
| | 비정형 로그 인덱싱 | 정규식 기반 자동 처리 | 미 지원 | 지원 (키워드 이외 삭제) | 지원 (수집 시) |
| 검색 및 분석 | Full Text 검색 (원문전체 구문검색) | 칼럼 구분 없이 전체 원본로그 대상으로 키워드, 와일드카드 검색 | 미 지원 | 지원 | 미 지원 |
| | 검색 성능 | 10~15GB 1400만건 4초 내 검색 (초당 500만건) [TTA, 2013] | 확인 불가<br>(공인된 수집 성능 지표 없음) | 초당 20 GB | 확인 불가 |
| | 단순 상관분석 | 단순 연산에 의한 상관분석 시나리오 작성 및 적용 | 지원 | 지원 ('Hyper Search' 기능) | 미 지원 |
| | Sequential 상관분석 | 순서에 따른 상관분석 시나리오 작성 및 적용 | 미 지원 | 미 지원 | 미 지원 |
| | 2차 상관분석 (분석결과재귀입력) | 지원 | 미 지원 | 지원 (NEO 버전만 - Wizard이용 5단계 분석 가능) | 미 지원 |
| | 쿼리확장 | 파이프라인(\|)을 통한 복수 쿼리 확장으로 유연한 검색 기능 제공 | 미 지원 | 지원 (자체 문법 제공) | 미 지원 |
| | 데이터 통계분석 | 모든 유형 다양한 통계 기능 제공 (Count, Sum, Avg, ax, min, top, bottom, 사칙연산 등) | 일부 지원 | 지원<br>(사용자정의 보고서/통계) | 일부 지원 |

# 5.1 별첨

## 5.1.1 타사 비교 자료

| 구분 | | nLM LogSee | S사 SGA-ESM | I사 LogCenter NEO | N사 Logsaver |
|---|---|---|---|---|---|
| 검색 및 분석 | 분석결과 /쿼리 저장 | 모든 분석결과 데이터와 쿼리 저장 | 미 지원 | 지원 | 일부 지원 |
| | Google like 검색창 | 지원 | 미 지원 | 지원 | 미 지원 |
| | 사용자정의 검색메뉴구성 | 사용자가 직접 작성한 쿼리를 메뉴화 하여 그룹으로 관리 | 미 지원 | 지원 (자체 문법 제공) | 미 지원 |
| 이벤트 및 리포팅 | 실시간 이벤트 | 단일 장비의 실시간 단위 이벤트 제공 | 지원 | 지원 | 지원 |
| | 검색 이벤트 | 쿼리를 통한 이기종 장비간 검색 이벤트 제공 | 미 지원 | 지원 | 미 지원 |
| 감사 | 증적감사 기능 | 접속 및 작업이력 수집 및 분석 제공 | 일부 지원 | 지원 | 지원 |
| | 솔루션 작업이력 감사 기능 | 접속 및 작업이력 수집 및 분석 제공 | 미 지원 | 지원 | 지원 |
| | 무결성 보장 기능 | 원본 위변조 시 감시 및 알람 제공 | 미 지원 | 미 지원 | 지원 |
| 대시보드 및 관리 편의성 | 사용자/개인화 저작형 대시보드 | 각종 통계데이터의 추이/막대/파이/영역차트를 사용자가 생성 관리 | 미 지원 | 지원 (Widget) | 일부 지원 |
| | 토폴로지 맵 구성 | 로그 수집 대상 장비들에 대한 토폴로지 맵 제공 | 지원 | 미 지원 | 미 지원 |
| | 매핑 코드관리 | 인사정보/기간별/부서별 코드정보 엑셀일괄등록 로그 Append/치환 | 미 지원 | 미 지원 | 매핑 탬플릿 형식 파일을 DB로 변환 |
| | 확장성 | 수집서버 병렬 확장 구조 | 지원 | 지원 | 지원 |
| SIEM 기능 | 보안이슈 등 추적관리 | 지원 | 미 지원 | 지원 | 미 지원 |
| | 시스템 운영현황관리 | 지원 | 부분 지원 | 미 지원 | 미 지원 |

# 감사합니다

(주) 인 콘

서울시 구로구 디지털로 30길 28 마리오타워7층 701호
TEL: 02-558-9130 / FAX: 02-558-7868 / www.in-con.biz