nSIEM

netcruz Security Information & Event Management

지능형 종합보안분석 시스템

제품 및 기술문의
Email : Sales@netcruz.co.kr
Tel : 02 869 4123

nSIEM
netcruz Security Information & Event Management

지능형 종합보안분석 시스템 이란?

보안 위협의 고도화 및 지능화에 따라 기능 및 영역이 세분화되고 대용량화되고 있는 보안장비 로그를 빅데이터 기반으로 수집하고 이기종 보안 장비 간 연관분석을 통해 실시간 보안 위협 탐지 및 대응할 수 있는 지능화 된 시스템입니다.

전통적인 종합보안분석 시스템

- Signature 기반 탐지
- 단일장비 로그분석

ESM

- I Inbound Attack - 해킹, APT 공격
- O Outbound Threat - 정보유출, 부정행위
- C Compliance Challenge - 보안규제/감사요건

지능형 종합보안분석 시스템

- 실시간 고속 탐지
- 유연한 상관분석
- 이기종 상관분석

필요 고객

1. 정보관리자, 감사팀	로그관리 Compliance 준수, 로그저장 및 사후 감사 대응
2. IT운영부서, 인프라 담당자	대용량 보안장비, System 로그의 실시간 모니터링 & 장애 시 즉각적인 검색 / 분석
3. 보안관제 센터	외부 침해 대응 시 일일 수 GB ~ 수 TB의 보안로그를 분석할 때 DBMS의 한계 극복
4. 기획부서	비정형 빅데이터를 대상으로 다양한 가치를 모색

특장점

1 국내 최고 검색 속도 FTS(Full Text Search)

TTA 공인 BMT 검증 사례
(1 ~ 11초 / 96억 건 분석)

2 일 2TB이상 대용량 실시간 분석 성능

월 60TB 로그분석환경
검증 결과

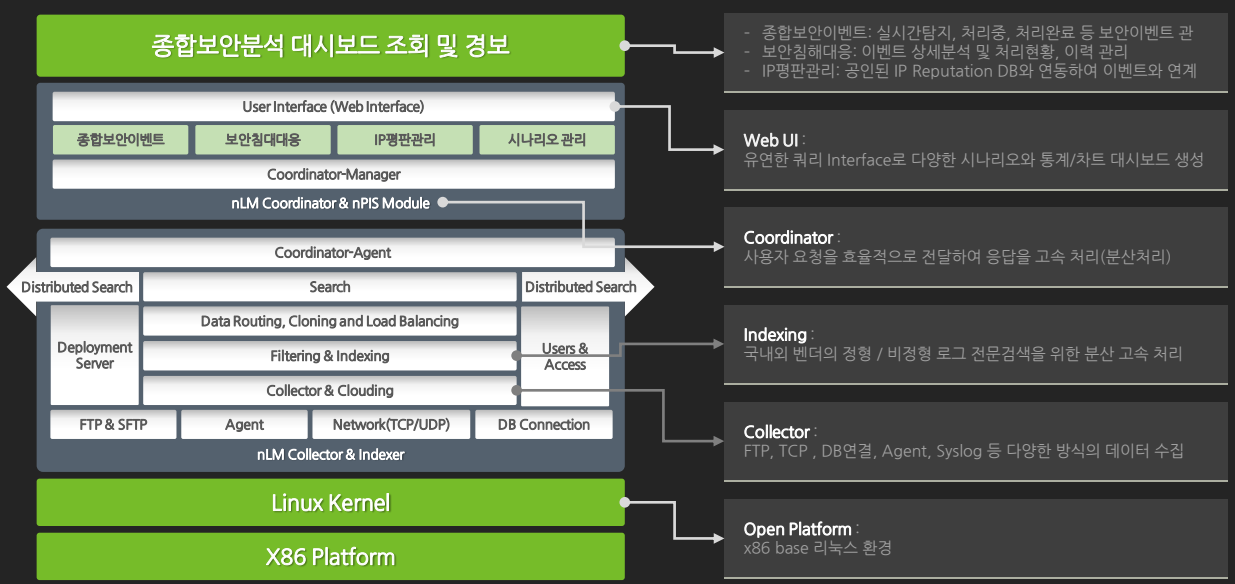
3 종합보안분석 대시보드

외부위협탐지, 침해대응관리,
종합이벤트 상황판

4 다양한 이기종 장비간 상관분석

실시간 단위이벤트, 검색기반
이벤트, 시나리오기반 이벤트

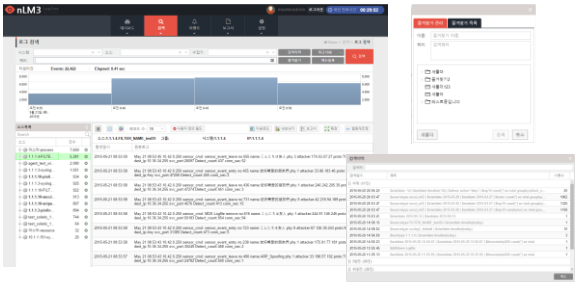
플랫폼 구조



nSIEM
netcruz Security Information & Event Management

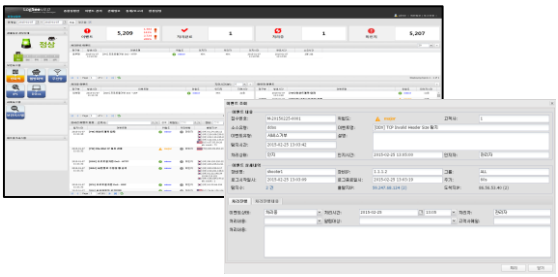
주요 기능

수집 및 검색



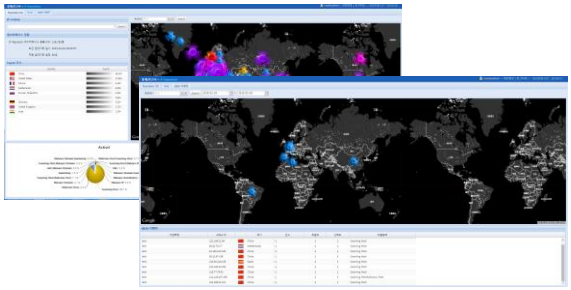
- 다양한 장비와 유연한 수집 연동(Syslog, Agent, DB2DB 등)
- 정형/비정형 데이터 수집
- 유연한 검색을 위한 즐겨찾기 및 이력 제공
- 암호화(AES/ARIA/SEED) 및 압축 저장

종합보안분석 종합상황판



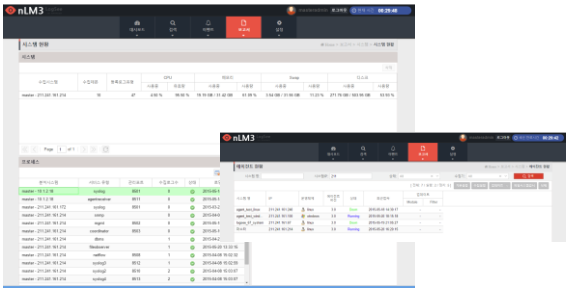
- 전체 이벤트에 대한 실시간 탐지 현황 및 처리 중/완료 현황 등 주요 사항을 종합적으로 확인
- 이벤트 발생 시 처리내용, 알림대상 등을 입력하고 추후 처리 과정 히스토리 관리 제공

소명처리 프로세스 및 보안평판관리



- 공인된 IP Reputation DB와 연동하여 이벤트와 연계함으로써 위협에 빠르게 대응할 수 있는 체계 제공
- 외부 Blacklist IP가 내부로 접근하는 List 확인
- 내부 IP 중 Blacklist IP에 접속하는 Host List 확인

시스템 모니터링

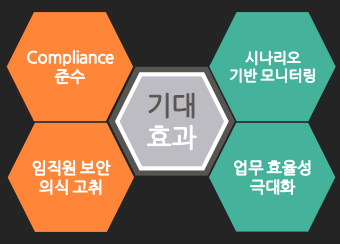


- Log Manager 분석/수집서버 상태 모니터링
- CPU/Memory 등 Resource 현황과 Process 모니터링
- Agent 설치된 서버들의 현황 모니터링
- Log Manager에서 Agent 기본설정/필터설정 등 제공

기대효과

침해위협 대응 로그 법률 관련 주요사항에 대한 준수 및 감사 대비 이행근거 충족

인사정보 연동으로 위험계정 집중관리 및 사후 감사 연계로 보안의식 고취



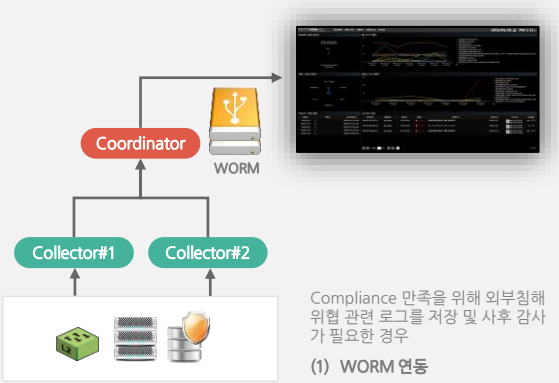
외부 공격 대응 장비 간 상관분석 등 시나리오 기반 외부침해위협 상시 모니터링

보안침해 위협 통계구성/보고서 자동화를 통해 수작업을 최소화하여 효율적 업무수행

nSIEM
netcruz Security Information & Event Management

구성 사례

금융기관



시스템, 네트워크디바이스, 보안장비 등등

Compliance 만족을 위해 외부침해 위협 관련 로그를 저장 및 사후 감사가 필요한 경우

(1) WORM 연동

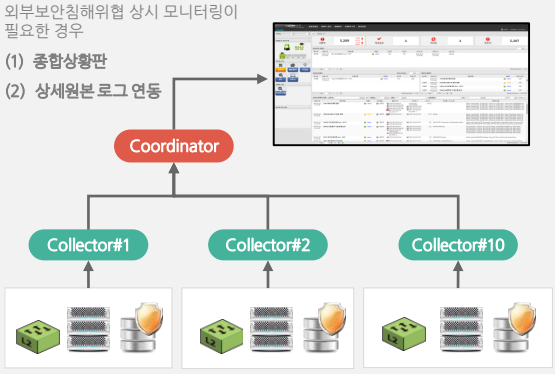
(2) 사후 원본로그 상세 분석

보안 관제팀을 운영하는 조직

외부보안침해위협 상시 모니터링이 필요한 경우

(1) 종합상황판

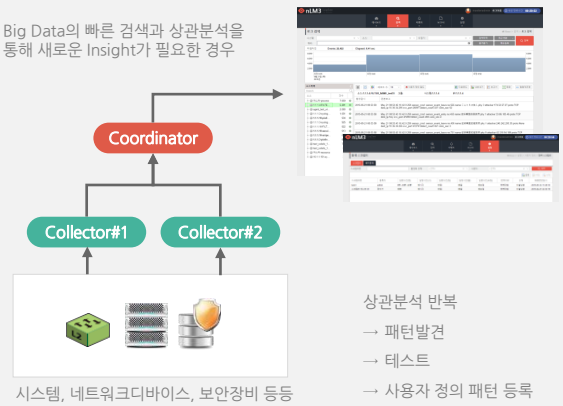
(2) 상세원본 로그 연동



시스템, 네트워크디바이스, 보안장비 등등

기획부서

Big Data의 빠른 검색과 상관분석을 통해 새로운 Insight가 필요한 경우



시스템, 네트워크디바이스, 보안장비 등등

상관분석 반복

→ 패턴발견

→ 테스트

→ 사용자 정의 패턴 등록

감사부서

시스템, 네트워크디바이스, 보안장비 등등

IP Reputation DB와 연동하여 외부 위협 및 내부 감사용으로 확인하는 경우

(1) Blacklist IP에 접속한 내부 IP

(2) Blacklist IP가 접속한 내부 IP

Specification

Product		nLM Collector	nLM Coordinator & SIEM Module
S/W	Operating System	Linux (64bit)	Linux (64bit)
	DBMS	File DB	구성관리(PostgreSQL)
H/W	CPU	8 Core 2.66GHz X 2	6 Core 2.66GHz X 2
	Memory	32GB	32GB
	HDD	Usable 6.3TB (6개월 보관, 압축 70%, 원본 포함 저장, 원본 50GB / 일 기준)	500GB

※ 일일 압축저장용량에 따라 HDD와 스토리지는 추가 산정될 수 있습니다.

주요 고객사

공공

- 중앙선거관리위원회, 대법원, 금융결제원, 중소기업청, 인천소방본부, 장학재단, 환경부, 특허청, 건강보험공단, 한국전력거래소, 농림축산식품부, 행정안전부, 서울시재난종합상황실
- 경기도청, 구로구청, 송파구청, 통영시청, 사천시청, 마산시청, 진주시청, 경상북도청, 남해군청, 경산시청, 영암군청, 부천시청, 창원시청
- 한국전력공사, 한국철도시설공단, 국방홍보원, 한국산업인력공단, 핵융합연구소, 대전교육정보원

일반기업

- 한국수력원자력, 한국타이어, 한국전력연구원
- 현대중공업, K-POWER, 아모레퍼시픽, SK대덕연구단지
- 삼일회계법인, SK C&C, 삼성SDS, BGF
- LG생활건강, 코오롱

금융

- 롯데카드, 미래에셋생명, 푸르덴셜투자증권, 삼성증권, 동부증권

대학 / 교육 / 의료

- 인천광역시교육청, 충남교육청, 전남교육청
- 한국외국어대학교, 남부대학교, 한국폴리텍항공대학, 대구보건대학, 안동대학교, 고등과학원
- 의료연합회, 포항성모병원

수사기관

- 대구지방경찰청, 경북지방경찰청
- 경찰청사이버테러대응센터
- 대검찰청, 대법원

netcruz
(주)넷크루즈 | www.netcruz.co.kr
서울시 구로구 디지털로33길 12 1008호(구로동 184-1 우림이비지센터 2차) TEL 02 869 4123 FAX 02 869 5123