Zenius SIEM v2.0

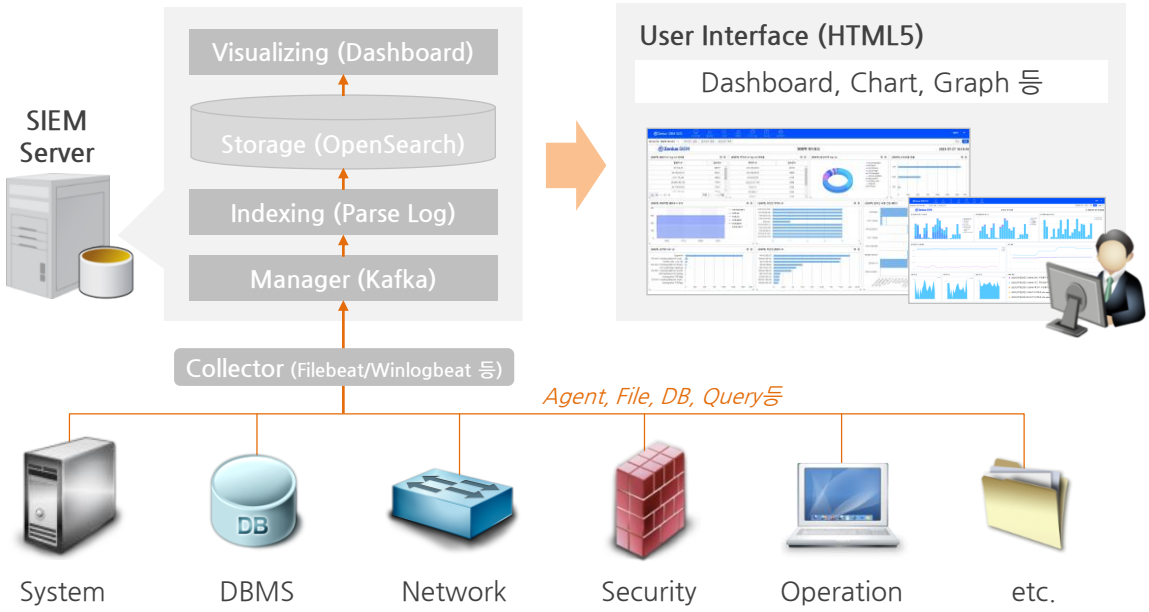
이기종의 다양한 장비에서 발생되는 다양한 로그(Log)들을 수집/분석하고 통합 모니터링 및 관리할 수 있는 시스템입니다.

정형/반정형 또는 비정형 로그들에 대한 실시간 수집 및 신속한 분석 기능을 제공하며, 이러한 정보들을 다양한 차트와 대시보드를 통해 직관적으로 가시화합니다.

또한, 로그 이벤트 발생 시 즉각적인 알람을 통하여, 빠른 문제해결과 높은 가용성을 확보하도록 지원합니다.

제품 구성도

Zenius SIEM은 시스템, 데이터베이스, 네트워크, 보안, 운영/업무 등 **분산된 다양한 로그들을 단일 시스템을 통해 통합적으로 수집**하며, 실시간적인 분석과 검색을 통하여 관리대상의 장애를 실시간으로 인지하고 유의미한 정보를 얻을 수 있도록 지원합니다.



다양한 이기종 장비에 대한 정형/반정형/비정형 포맷의 방대한 데이터

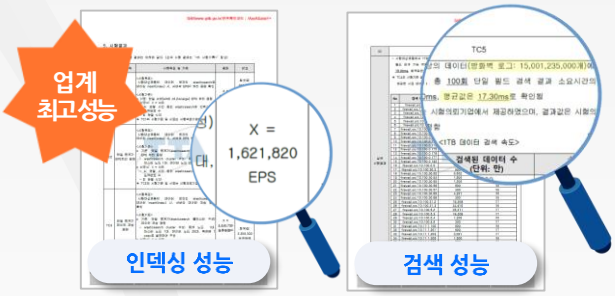
권장 사양

소프트웨어 (Software)		하드웨어 (Hardware)	
OS	CentOS 7.6	CPU	16 core 이상
검색엔진	OpenSearch	Memory	64 GB 이상
Web Server	Node.js	HDD	28 TB 이상

* 위 하드웨어 사양은 로그 일일 20GB 수집, 1년 보관 기준의 사양으로 수집하는 로그 양에 따라 권장사양이 상이함

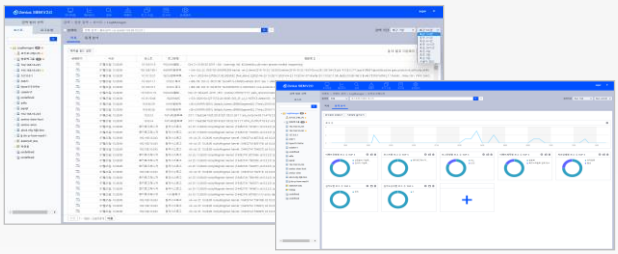
주요 기능

업계 최고 수준의 인덱싱 성능 및 검색속도



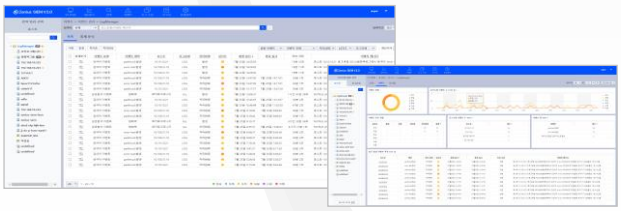
- TTA의 공인 인증을 받은 최고의 시스템 성능
  - 162만 EPS의 인덱싱 성능으로 대용량 데이터를 유실없이 수집
  - 150억 건(1TB) 기준 0.02초 이내(평균 17.3ms)의 검색 성능

로그 수집 및 분석



- 이기종 장비의 대규모 정형/비정형 로그 실시간 수집/분석/저장
- 중요 로그 패턴에 대한 실시간 분석
- 다양한 SQL 함수에 대해 보다 상세한 조건 별 쿼리 검색 기능
- SQL 쿼리문을 기반으로 결과값에 대한 감시/분석 지원

이벤트 감지 및 통보



- 복합 이벤트 처리(CEP)로 복합적인 로그 상관관계 분석 및 감지
- 임계치, 문자열 비교, 쿼리검색 등 다양한 이벤트 감시 방법 지원
- 이벤트 유형, 발생시각, 대상 등에 대한 모니터링 및 조회
- 단문자, 메일, 팝업, 메신저 등 다각적 방법의 통보

Dashboard 및 시각화 기능

- 사용자정의 기반(User-Defined) 실시간 정보 모니터링
- 총 26종의 다양한 시각화 컴포넌트를 통한 정보 가시화
- 드릴다운(Drilldown) 형태의 주요 지표 상세 모니터링
- 수집 로그의 핵심지표 요약 및 이벤트 오버뷰 제공

수집대상	항목 예시	수집대상	항목 예시
시스템	CPU, MEM, Process, 파일시스템, 로그인 등	네트워크	Backbone, Router, Switch, VPN 등
데이터베이스	PostgreSQL, Oracle, MS-SQL, Tibero 등	어플리케이션	ERP, 그룹웨어, E-mail, 홈페이지, 포털 등
보안장비	방화벽, IDS/IPS, NAC, WIPS, APT 등	기타	센서, APT실거래가, 매매추이 등

활용 예시

인프라 관리
서버, 네트워크, DBMS 등의 로그에 대한 실시간 분석 및 즉각적 장애 탐지를 통한 인프라 가용성 유지

보안 사고 대응
사용자 부주의, 외부 침해, 내부 기밀 정보 유출 등의 행위에 대한 로그 실시간 감지를 통한 보안 강화

컴플라이언스 준수
각종 법률, 규정, 지침 등에 대한 감사를 위해 근거가 될 수 있는 분석 로그 저장/보관 및 분석

마케팅 및 기획
매출 및 구매 정보 등에 대한 실시간 로그 분석을 통한 마케팅 및 신규 기획에 대한 근거 자료 확보

경쟁사 비교

비교항목	Zenius SIEM	E제품	L제품
수집항목	File, SYSLOG, DB, FTP, SFTP, metric, packet, SNMP, SNMP Trap 등	File, SYSLOG, DB, metric, packet, ICMP, TCP 등	File, SYSLOG, DB, FTP, HTTP, JMX, PCAP, SNMP, 하둡 등
인덱싱 성능	162만 EPS	100만 EPS	26만 EPS
검색 속도	1TB 데이터(150억 건) 평균 17.3ms	20억 건 데이터 10초 이내	1TB 데이터 200ms 이내
SQL 검색	제공	제공	미제공
대시보드	26종 컴포넌트 및 반응형 웹 지원	5종 컴포넌트 제공	10종 컴포넌트 제공
보고서	다양한 형식(PDF, Excel, PPT, Word)의 출력 및 보고서 Preview 제공	PDF, Excel, PPT, Word 지원	Excel 지원
이벤트 및 감시설정	검색어/SQL/CEP 등 감시설정을 통한 이벤트 감지	SQL 감시설정 미제공	SQL 감시설정 미제공
	Email, 단문자, 팝업, 음성, 텔레그램	Email, 단문자, 팝업	Email, 단문자