## 로그프레소 엔터프라이즈 4.0

로그프레소 엔터프라이즈(이하 ENT로 표시)는 엔터프라이즈 환경의 통합로그관리 뿐 아니라 IT 인프라에서 발생하는 대규모 머신 데이터를 실시간으로 수집, 검색, 분석할 수 있는 보안운영(SecOps) 플랫폼입니다.

로그프레소 엔터프라이즈는 (주)로그프레소가 원천 기술을 보유한 강력한 고성능 빅데이터 엔진 위에 여러 가지 애플리케이션을 설치하여 확장할 수 있도록 [OSGi](https://www.osgi.org/resources/what-is-osgi/) 프레임워크 기반 플러그인 아키텍처로 설계되어 있습니다. 사이버 보안을 비롯해 관제, 클릭 스트림 분석, 클라우드 모니터링 등 다양한 분야에서 활용할 수 있습니다.

로그프레소 엔터프라이즈는 복잡한 비정형 데이터 처리와 통계 분석을 고속으로 수행할 수 있으며, 대시보드 및 보고서 생성에 필요한 시간을 크게 단축합니다. 로그프레소는 대용량 비정형 데이터를 수집, 검색, 분석, 시각화하여 신속한 의사결정을 돕는 플랫폼입니다.

### 새로운 기능

엔터프라이즈 4.0에 추가된 기능과 변경사항은 다음과 같습니다.

**앱 시스템**

반복되는 작업을 줄이고 본연의 업무에 집중할 수 있도록 특정한 기능을 수행하는 애플리케이션을 일괄적으로 설치, 배포할 수 있는 앱 시스템을 도입했습니다.

**로그프레소 스토어**

로그프레소 플랫폼과 앱을 분리하고, [로그프레소 스토어](https://logpresso.store)에서 앱을 검색, 설치할 수 있도록 했습니다. 플랫폼 소프트웨어의 크기는 작아지고, 선택의 폭을 넓혔습니다.

**에이전트 설치 및 배포 간소화**

파웨셸, POSIX 호환 셸에서 에이전트(센트리)를 단 한 줄의 명령으로 처리할 수 있도록 개선했습니다. 서버와 에이전트 간 통신에 사용하는 인증서의 관리를 자동화하여 수동으로 인증서를 교체하는 번거로움을 제거했습니다.

**비약적인 성능 향상**

엔터프라이즈 3.0 대비 인덱싱 성능이 10배 향상되었습니다. 엔터프라이즈 4.0은 풀텍스트 인덱싱 기준 270만, 수집 기준 400만 EPS(Events Per Seconds)의 처리 성능을 제공합니다.

**사용 편의성 개선**

버전 업그레이드에 발맞추어 새로운 사용자 인터페이스를 선보입니다.

### 주요 기능

**대시보드**

로그프레소는 위젯을 도킹 배치할 수 있는 대시보드를 제공합니다. 그리드나 차트에 쿼리를 바인딩한 위젯을 배치할 수 있으므로, 사용자가 원하는 형태로 대시보드를 구성할 수 있습니다.

**실시간 풀텍스트 인덱싱**

로그프레소는 고성능 실시간 인덱싱 엔진을 탑재하고 있습니다. 일반적인 타사 솔루션과 달리 데이터 수집 즉시 인덱싱되어 풀텍스트 검색 가능한 상태가 됩니다.

**실시간 압축**

로그프레소는 실시간으로 압축 쓰기를 수행합니다. 압축 알고리즘은 선택 가능하며 압축 방식에 따라 대략 1/5에서 1/10 수준의 압축률을 보입니다. 일반적인 일 단위 압축과 달리 부분 압축 및 해제가 가능하므로, 기존에 비해 몇 배의 로그를 검색 가능한 상태로 유지할 수 있습니다.

**실시간 분석 및 경보**

실시간 로그 스트림에 대해 문맥을 이용한 복잡한 연관 분석을 수행할 수 있습니다. 분석 결과에 따라 경보를 발생시키고, 설정된 경보 처리 방식에 따라 단순 로깅을 수행하거나 메일이나 SMS를 통하여 사용자에게 경보를 전달할 수 있습니다.

**실시간 데이터 수집**

로그 파일, 데이터베이스, 시스로그, SNMP 트랩, 에이전트 기반의 실시간 로그 수집 기능을 내장하고 있습니다. 또한 로그프레소 REST API를 사용하여 로그를 프로그래밍 방식으로 입력할 수 있습니다.

**비정형 데이터 처리**

로그프레소는 기존의 DBMS와 달리 정형화되지 않은 임의의 로그를 받아들일 수 있습니다. 로그는 원본 그대로 유지되고, 쿼리 시점에 파싱되어 가공됩니다. PCAP 파일과 같은 바이너리 파일도 원본 그대로 유지하고 파서를 통해 필드를 추출할 수 있습니다.

**전용 쿼리 문법**

로그프레소는 유닉스 파이프 메타포의 전용 쿼리 문법을 내장하여 SQL로 처리하기 힘들었던 정규표현식 검색, 필드 추출, 시계열 분석 등을 쉽게 수행할 수 있습니다. 원하는 쿼리 문자열을 뒤에 덧붙이는 방식으로 쉽게 쿼리 결과를 가공할 수 있습니다.

**스크립팅 엔진**

로그프레소는 로그 수집, 파싱, 인덱싱, 실시간 분석, 쿼리 전 영역에 걸쳐 스크립팅 확장을 지원합니다. Groovy 엔진을 이용하여 런타임에 스크립트를 적재시킬 수 있으므로, 복잡한 사용자 정의 로직도 별도의 제품 커스터마이즈 없이 사용자가 직접 구현 가능합니다.

**태깅 및 필터링**

실시간으로 원본 로그에 메타데이터를 태깅하거나, 필터링을 수행합니다.

**로그 파서 설정**

테이블 데이터에 대하여 기본으로 적용할 파서를 설정하거나, 원본 로그를 파싱하여 필드를 추출합니다.

**에이전트 연동**

에이전트(센트리)를 사용하여 원격 호스트에서 로그를 수집하거나 실시간으로 모니터링합니다.

**실시간 암호화**

수집된 데이터 원본을 전송하는 구간과 로그프레소 서버에 저장하는 과정에서 데이터가 노출되지 않도록 모두 실시간 암호화를 수행합니다.

**예약된 쿼리 경보**

지정된 주기마다 쿼리 실행 후 경보 조건과 일치하면 경보 메일을 전송합니다.

**계정관리**

로그프레소 계정과 테이블 접근 권한을 관리합니다.

**엑셀 연동분석**

엑셀 웹쿼리를 통해 로그프레소 쿼리 결과를 시트에 삽입하고 자동 갱신되도록 설정할 수 있습니다.

**외부시스템 연동**

REST API 및 각종 상용 RDBMS와 연동하여 외부 데이터를 이용한 연관 분석을 수행할 수 있습니다.