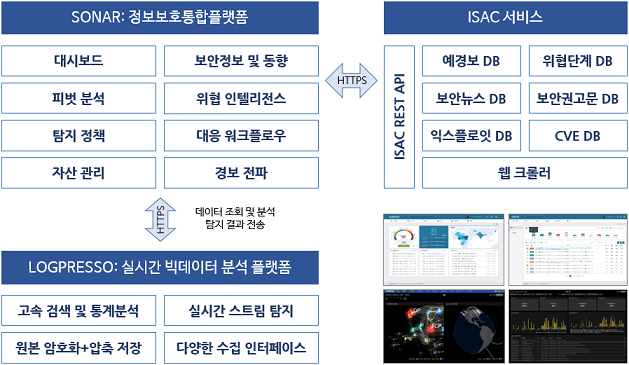
# 시작하기

로그프레소 소나는 외부침해관제, 내부유출감시, 내부통제, 서비스품질관제, 이상거래감시 등 정보보호 업무를 전방위적으로 수행할 수 있도록 설계된 정보보호 통합플랫폼입니다. 로그프레소 소나는 빅데이터의 수집, 저장, 분석, 시각화를 제공하는 로그프레소 엔터프라이즈와 이디엄에서 운영하는 워치에이드 ISAC (정보공유분석센터; Information Sharing & Analysis Center) 서비스로 구성됩니다. 실시간 빅데이터 플랫폼과 위협 인텔리전스 서비스를 결합하여, 로그 수집부터 이벤트 탐지, 분석, 대응, 모니터링에 이르는 전 과정을 웹 브라우저만으로 수행할 수 있는 업무 환경을 제공합니다.



기존의 단위 관제시스템과 달리 로그프레소 소나가 통합플랫폼의 역할을 수행할 수 있는 이유는 이전 세대의 시스템과 달리 실시간과 배치 분석을 모두 탁월하게 수행할 수 있는 로그프레소 엔터프라이즈를 기반으로 하고 있기 때문입니다.

외부침해관제 (SIEM; Security Information & Event Management) 솔루션은 실시간 이벤트 연관 분석을 잘 수행하지만, 대용량 로그를 인덱싱해서 빠르게 검색하는 것 이상의 분석 기능을 가지고 있지 않습니다. 내부유출탐지 (UBA; User Behavior Analytics) 솔루션은 로그를 대상으로 통계적 분석과 이상탐지 기능을 제공하지만, 일반적으로 실시간 이벤트 연관 분석 기능은 제공하지 않습니다. 이런 속성 때문에 많은 기업들이 외부침해관제, 내부유출탐지, 통합로그 솔루션 등을 별개로 구축해왔으나, 정보보호 업무의 복잡도 증가로 인해 더 이상 이런 방식은 통용되기 힘든 상황에 이르렀습니다.

로그프레소 소나는 특허 등록된 스트림 쿼리 기술과 스키마리스 컬럼DB 기술을 이용하여 실시간과 배치 분석을 모두 고속으로 수행합니다. 스트림 쿼리는 스트림에 흐르는 실시간 데이터를 대상으로 연속적으로 실행되는 쿼리를 의미합니다. 로그가 도달하는 즉시 연속적으로 실행 중인 쿼리 파이프라인을 통해 처리되기 때문에, 밀리초 단위의 시간 안에 이벤트 연관 분석을 수행한 결과를 응답할 수 있습니다. 특히 스트림 쿼리 기술은 0.1초 내에 이상거래 여부를 응답해야 하는 미션크리티컬 뱅킹시스템에서 핵심적인 역할을 담당합니다.

한편, 스키마리스 컬럼DB 기술은 수 억 건의 레코드도 초 단위로 집계 및 분석할 수 있는 성능을 제공합니다. 이전 세대 솔루션에서는 데이터 마트를 생성해서 제한적으로 통계를 볼 수 밖에 없었지만, 컬럼DB 기술은 피벗 인터페이스에서 원하는 조건을 부여하면 그 즉시 고속으로 드릴다운해서 의도한 통계 결과를 응답함으로써 실질적인 데이터 분석이 가능하도록 지원합니다. 기존의 정형적 컬럼DB 기술과 다르게 로그프레소 소나는 스키마를 고정하지 않고도 고속으로 데이터를 분석할 수 있기 때문에, 대용량 보안 로그의 비정형적 특성과 펌웨어 업데이트에 따른 스키마 변경에 유연하게 대응할 수 있습니다.

여기에 더하여 로그프레소 소나는 사용자가 직접 예측 및 이상탐지 머신러닝 모델을 생성하고 적용할 수 있는 기능을 제공하며, 100종 이상의 함수 및 커맨드를 활용한 고급 쿼리를 통해 고도의 분석 및 리포팅을 수행할 수 있습니다. 또한, SYSLOG, HTTP, FTP, SFTP 등 다양한 프로토콜을 통해 외부 시스템에 데이터를 실시간으로 전송할 수 있는 기능을 제공하여, 대외계 인터페이스의 역할을 통합적으로 수행합니다.

이제, 로그프레소 소나를 본격적으로 살펴보도록 하겠습니다.