### 로그프레소 앱

로그프레소 플랫폼은 고성능의 스키마리스 빅데이터 엔진을 기반으로 보안 운영에 필요한 로그 수집, 저장, 탐지, 분석, 시각화에 관련된 많은 기능을 제공합니다. 하지만 기본 기능만을 이용하여 실제 운영 환경을 구성하려면 많은 노력이 필요합니다.

연동 대상에 따라 전용 수집기를 개발해야 할 수 있고, 바이너리 패킷을 파싱해야 할 수도 있으며, 연동 장비를 제어하기 위하여 REST API를 호출해야 할 수도 있습니다. 기본 플랫폼 기능만으로 운영 환경을 완전히 구성할 수 있다고 하더라도 여전히 정규표현식을 만들거나, 실시간 혹은 배치 탐지 시나리오를 설정하거나, 대시보드 위젯을 만들어 배치하는 작업이 필요합니다.

로그프레소 파트너는 엔지니어가 이러한 작업을 반복적으로 수행하는 대신, 완전히 패키지화된 앱을 개발하여 재사용성을 극대화 할 수 있습니다. 로그프레소 앱은 아래의 기능을 제공합니다.

**로그프레소 앱 기능**

|  |  |
| --- | --- |
| 항목 | 설명 |
| 로그 스키마 | 표준화된 로그 필드 이름의 집합을 정의합니다. |
| 파서 | 로그를 파싱하여 표준화된 필드 집합을 추출하는 파서를 정의합니다. |
| 수집 모델 | 수집 유형과 정규화 규칙의 조합을 정의합니다. |
| 데이터셋 | 대시보드 위젯이나 피벗에서 데이터 원본으로 사용할 데이터 집합을 정의합니다. |
| 프로시저 | 매개변수화 된 쿼리를 정의합니다. |
| 보고서 | 보고서 서식을 정의합니다. |
| 위협 인텔리전스 피드 | 외부 인텔리전스 서비스의 침해지표를 자동 수집하는 피드를 정의합니다. |
| 실시간 탐지 시나리오 | 밀리초 단위로 탐지하는 실시간 탐지 시나리오를 정의합니다. |
| 배치 탐지 시나리오 | 지정된 주기마다 실행되는 배치 탐지 시나리오를 정의합니다. |
| 네트워크 대역 그룹 | 탐지 시나리오에서 참조하는 네트워크 대역 그룹을 정의합니다. |
| 포트 그룹 | 탐지 시나리오에서 참조하는 포트 그룹을 정의합니다. |
| 패턴 그룹 | 탐지 시나리오에서 참조하는 패턴 그룹을 정의합니다. |
| 차단 연동 모델 | 지정된 IP 주소를 연동된 장비에서 차단 또는 차단 해제하는 차단 연동 모델을 정의합니다. |
| 위젯 | 대시보드에 정보를 시각화하는 재사용 가능한 위젯을 정의합니다. |
| 대시보드 | 여러 개의 위젯을 조합하여 위협 탐지 또는 서비스 모니터링에 필요한 대시보드를 정의합니다. |
| 접속 프로파일 | REST API 주소, API 키 등 접속 설정을 관리합니다. |
| 쿼리 명령어 | 사용자 정의 쿼리 명령어를 확장합니다. |
| 플레이북 | 재사용 가능한 플레이북을 정의합니다. |

즉, 로그프레소 플랫폼에 여러 개의 로그프레소 앱을 설치하면 최소한의 설정으로 운영 환경을 구성할 수 있습니다. 다음 절에서는 로그프레소 앱이 어떻게 로그프레소 플랫폼에서 구동되는지 설명하겠습니다.