## 정책

로그프레소 소나의 위협 및 이상탐지 방법론은 크게 다음과 같이 구분됩니다.

**실시간 패턴 매칭 탐지**

문자열 패턴이나 조건에 의한 단순 탐지를 수행합니다. 예를 들어, IPS 로그의 패턴명을 기준으로 고위험 공격을 탐지하거나, 아웃바운드 트래픽 전송량이 일정 기준 이상인 경우 유출 탐지하는 등 가장 단순한 위협 및 이상탐지 방법에 해당됩니다.

**실시간 이벤트 연관 탐지**

시간의 흐름에 따라 발생하는 서로 다른 이벤트를 인메모리에서 연관 분석하여 탐지합니다. 예를 들어, 취약점 스캔 후 익스플로잇 공격을 실행하는 공격자를 실시간으로 탐지하거나, 대포통장에 입금한지 10분 이내에 ATM에서 출금하는 등 서로 다른 시점에 발생한 사건을 연관시켜서 실시간으로 탐지할 수 있습니다.

**위협 인텔리전스 탐지**

위협 인텔리전스 피드에 포함된 IP 주소, 도메인, MD5 등 IoC (Indicator of Compromise)가 식별되는 경우 실시간으로 탐지합니다. 예를 들어, 방화벽 트래픽 로그에서 알려진 랜섬웨어 C&C 서버 통신을 자동으로 탐지할 수 있습니다. 위협 인텔리전스 DB는 지속적으로 ISAC 서비스와 동기화됩니다.

**행위 이력 기반 탐지**

과거 행위를 주기적으로 프로파일링하고, 프로파일 데이터를 이용하여 실시간 탐지를 수행합니다. 예를 들어, 최근 6개월 간 로그인한 적이 없는 휴면 계정의 접속을 탐지하거나, 거래기록이 전혀 없는 계좌로 이체하는 경우 탐지할 수 있습니다.

**통계 분석 기반 탐지**

통계적 분석을 통해 위협이나 이상징후를 탐지합니다. 공통적으로 임계치나 표준편차 범위를 크게 벗어나는 IP 주소나 계정, 사번 등을 탐지합니다. 예를 들어, 일정 기간 내에 DRM 암호화 해제 및 매체제어 위반 로그가 공통적으로 이상 발생하는 경우를 내부유출 시나리오로 정의하여 탐지할 수 있습니다.

**머신러닝 기반 탐지**

군집기반 이상탐지, 시계열 이상탐지, 공간분할 이상탐지 등 다양한 머신러닝 알고리즘을 적용하여 정상 범주를 벗어나는 이상치를 자동으로 식별하고 탐지합니다. 다차원으로 데이터를 분석하고 경계면을 자동으로 생성하여 정교한 탐지를 수행할 수 있습니다.

로그프레소 소나는 실시간이나 배치 방식으로 위의 방법론들을 적용하여 위협과 이상징후를 분석하고 탐지할 수 있습니다. 이제 실시간 탐지 시나리오 설정부터 알아보도록 하겠습니다.