원스토어, 마켓 침투 악성 앱 제거
AI 기반 자동분석 솔루션 OnAppScan 도입

ONE STORE

- **AI 기반 안티바이러스로 앱 마켓 등록 신·변종 악성 앱 탐지 강화**
- **악성 앱이 마켓에 등록되는 사례를 최소화해 이용자 보호**
- **마켓에 등록된 수백만 건의 앱을 자동 탐지해 분석 업무 효율 확보**

> 공식 앱 마켓은 공격자들에게 매우 매력적인 악성 앱 유포 수단으로, 많은 앱 마켓이 보안성 유지 강화를 위해 노력하고 있습니다. 국내 앱스토어인 '원스토어' 또한 마켓에 등록되었거나, 등록 예정인 악성 앱을 찾아내 이용자에게 안전한 마켓 환경을 제공합니다.

- 산업 : B2B
- 대상 : 앱 마켓 (회원수 약 4992만명 *2021년 기준)
- 솔루션 : OnAppScan

Challenge

원스토어는 초기 마켓 시절부터 패턴 기반 악성 앱 검사 엔진을 사용해 악성 위협으로부터 이용자를 보호해 왔습니다.
그러나 알려진 악성 앱을 탐지하는 패턴 기반 검사 시스템은 교묘하게 마켓 보안 정책을 우회하는 신·변종 악성 앱들을 탐지하는 데는 취약성이 있었기 때문에, 이를 보완할 수 있는 솔루션이 필요했습니다.

탐지의 정밀함도 더욱 높은 수준으로 요구되었습니다. 원스토어에는 앱 스토어 특성상 오랫동안 업데이트되지 않은 낮은 버전 앱들이 많이 있는데, 보안과 관련된 후속 조치가 취해지지 않은 채 낮은 버전을 유지하고 있는 앱들은 정상 앱 임에도 불구하고

위험한 앱으로 오인되기 쉬웠습니다. 따라서 정상적으로 등록된 앱 개발사와 이용자들의 피해를 막기 위해 '낮은 버전의 정상 앱'과 '위험도가 높은 악성 앱'을 따로 식별해야 했습니다.

Solution

시큐리온의 OnAppScan은 AI 기반 악성 앱 검출 시스템으로, 원스토어에 악성 앱이 업로드되는 것을 실시간으로 방지하고 기존에 등록되었던 앱들 중에서 악성 앱으로 의심되는 앱들을 추출해 냈습니다.

특히 원스토어의 특성을 반영한 AI 모델링으로 탐지 효율을 높일 수 있도록 심혈을 기울였습니다. 시큐리온은 구글 플레이스토어를 기반으로 만들어진 AI 탐지 최초 파일럿 모델(V1)을 원스토어 앱을 바탕으로 새롭게 학습시켜, 원스토어 전용 신규 모델(V2)을 개발했습니다.

또한 앱스토어의 상품에 해당하는 '정상 앱'을 악성 앱으로 과잉 탐지하지 않도록, 악성 앱 유형을 명확하게 분류할 수 있는 새로운 모델을 빌드하였고, 위험도를 판정하는 작업도 엄밀하게 다루도록 했습니다.

Result

마켓 특성을 반영한 AI 모델링으로 탐지 정확도 향상

AI 기반 검사 시스템의 가장 큰 장점은 특수한 목적 하에 학습 데이터를 선별하여 '맞춤형 솔루션'을 제공할 수 있다는 데 있습니다. 원스토어는 이러한 AI 기반 탐지 시스템의 특성이 가장 잘 적용된 사례입니다.

국내 앱 마켓인 원스토어는 구글 플레이스토어나 애플 앱스토어와 다른 고유한 특성이 있었고, 시큐리온은 OnAppScan의 AI 탐지 엔진을 모델링 하는데 이러한 내용을 반영하여 원스토어만을 위한 탐지 시스템을 구축했습니다.

대량의 앱 데이터를 실시간으로 자동검사

앱 마켓 특성상 검사해야 하는 앱의 수량이 방대하고, 실시간으로 새롭게 검사해야 할 앱이 누적됩니다. 시큐리온은 원스토어에 기존 등록된 수십만 건의 앱과 함께 매일 업로드되는 모든 앱을 대상으로 AI 기반 자동 검사를 진행할 수 있게 되었습니다.

분석 업무에 최적화된 대시보드 지원

OnAppScan은 방대한 탐지 데이터 정보를 효율적인 방식으로 재 구성한 대시보드를 제공합니다. 대시보드를 통해 제공되는 것은 앱의 정상 유무 판정, 악성 앱 유형, 앱 평판 기반 판정 정보, 외부 CTI 서비스 연관 정보 등입니다. 내부 분석 전문가는 탐지 결과를 검증하는 과정에서 대시보드를 이용해 업무에 소요되는 리소스를 줄이고 분석 작업을 보다 편리하게 진행할 수 있습니다.

SECURI ON (주)시큐리온

서울시 송파구 송파대로 201 송파테라타워2 A동 G129-2 OS-33호
TEL. 02-575-3339 | FAX. 02-575-3340 | E-mail. securion@securion.co.kr

www.securion.co.kr
blog.naver.com/securioncokr
www.facebook.com/securioncokr