KISA 디지털위협대응본부 스미싱대응팀
AI 기반 자동분석 솔루션 도입

KISA 한국인터넷진흥원

- **보이스피싱 앱 및 난독화 등 분석 방해 기술 적용 앱 급증**
- **수동 분석으로 감당하기 어려운 악성 앱 규모, 자동분석 시스템으로 대응**
- **OnAppScan Cloud / On-premises 구축형 등 커스터마이징 서비스 제공**

“

한국인터넷진흥원(KISA)은 국내 3개 이동통신 업체로부터 문자로 유포되는 악성 앱과 의심 URL에 대한 신고를 받고 이를 분석하여 민간의 적절한 대응을 지원하고 있습니다.
해당 서비스는 스미싱 사기가 등장한 이후 10여년간 운영돼 왔으며, 최근 보이스피싱 앱이 급증하면서 더욱 신속한 분석이 요구되고 있습니다.

- 산업 : B2G
- 대상 : 공공기관
- 솔루션 : OnAppScan Cloud / On-premises 구축형

Challenge

악성 앱은 날이 갈수록 지능화되고 있습니다. 최근에는 앱 분석을 방해하기 위해 각종 난독화 및 암호화, 압축 해제 방해 등 분석 방해 기술을 적용하여 탐지 회피 건수가 늘어나고 있는 실정입니다. 스미싱 문자도 지속적으로 증가하여 2023년 총 스미싱 문자 탐지는 50만 3300건에 달했습니다.
경찰청 외에 금감원, 한국인터넷진흥원과 이동통신 3사가 대응에 힘을 모으고 있음에도 불구하고, 급격히 증가한 보이스피싱

악성 앱으로 인해 분석가들의 업무 과부하가 심각한 상황이었습니다.
이에 따라 지능화된 악성 앱에 대한 분석과 대응을 효율적이고 신속하게 진행할 수 있는 솔루션 도입이 시급했습니다.
기존의 자동화되지 않은 패턴 업데이트 방식의 한계를 극복하고, 개발 단말 단위의 악성 앱 탐지 기능을 넘어서 시스템에 포함된 다양한 단말 위협을 통합 관제할 수 있는 기능도 요구되었습니다.

Solution

시큐리온 OnAppScan은 분석 대상 앱이 난독화, 암호화 등 분석 방해 기술이 적용된 상태라고 해도 이와 무관하게 악성 앱을 탐지해 낼 수 있는 프레임워크를 제공합니다.
머신러닝 기반 탐지 기술은 난독화와 관계없이 악성 행위 실행에 필요한 정보 위주로 분석하므로 지능화된 악성 앱에 대응하기 적절하며, 신속하게 악성 여부를 판정할 수 있습니다. 초기에는 클라우드 구독형 서비스를 제공하여 자동 분석 보고서를 추출했으며 이후에는 더 많은 사용량을 처리할 수 있도록 온프레미스 구축형 사업으로 확장하였습니다.

Result

스미싱·보이스피싱 변종 악성 앱 대응 강화

머신러닝 기반의 OnAppScan 도입으로 각종 탐지 회피 기술이 적용된 신·변종 악성 앱에 대해서도 높은 탐지 성과를 거둘 수 있게 되었습니다.

분석 과정 자동화로 리소스 절감

악성 앱 크롤링을 통한 수집 단계부터 판정 후 검증까지 모든 분석 과정을 자동화함으로써 분석 작업에 소요되는 시간 및 인력 소모를 줄였습니다.

고객 니즈에 따른 서비스 형태 제공

OnAppScan은 온프레미스 환경을 반드시 구축하지 않아도 클라우드를 통해 구독형 서비스를 제공할 수 있습니다. 클라우드 서비스는 저렴한 비용으로 해당 솔루션을 이용하고자 할 때 적합합니다.
시큐리온은 고객의 요구에 따라 온프레미스 환경 구축, 클라우드 구독형 서비스 제공, 온프레미스와 클라우드의 중간 형태인 하이브리드 환경 구축 등 커스터마이징 된 시스템을 제공합니다.

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