



옵스왓 글로벌 인증 모바일 안티바이러스 미국 OT 보안 멀티엔진 메타디펜더 탑재

OPSWAT.

- 미국 악성코드 탐지 전문 업체 옵스왓(OPSWAT) MOU
- 멀티 안티바이러스 스캔 서비스 메타디펜더(MetaDefender)에 OnAV 탑재
- 산업 보안(OT) 분야 모바일 위협 탐지에 기여



옵스왓은 미국의 산업보안 전문 기업으로, 멀티 안티바이러스 스캔 서비스인 '메타디펜더'를 제공합니다.

메타디펜더는 미국 기반 시설의 약 98%에 적용돼 그 안정성과 기능을 인정받은 제품으로, 약 30여 개의 글로벌 보안 기업에서 제공하는 탐지 엔진을 사용합니다.

- 산업 : B2B
- 대상 : 기업 및 기관
- 백신 엔진 : OnAV

Challenge

산업, 제조 분야에서도 5G 혁신이 시작되면서 산업 보안의 중요성에 대한 인식이 높아졌습니다.

특히 스마트 OT 환경에서는 기존의 PC 중심 보안 솔루션으로는 방어할 수 없는 모바일 IoT 악성코드에 대응하는 것이 중요한 과제가 되었습니다.

Solution

시큐리온의 OnAV는 머신러닝 기반의 모바일 안티바이러스 탐지 엔진으로, '메타디펜더'를 이용하는 고객사들은 모바일 및 IoT 기기를 노린 악성코드의 위협을 실시간으로 탐지할 수 있게 되었습니다.

메타디펜더는 지능형 위협 방지 솔루션 '메타디펜더 CORE' 시리즈와, 멀티 스캔을 적용할 수 있는 '메타디펜더 KIOSK', 콘텐츠 무해화 솔루션인 '메타디펜더 CDR' 등으로 구성돼 있습니다.

시큐리온 OnAV는 메타디펜더 CORE 와 KIOSK에 탑재되어 고객들을 악성 위협으로부터 보호하였습니다.

Result



모바일 보호 기능 강화

메타디펜더는 OnAV를 탑재하기 이전에는 윈도우 대상의 악성코드 검사만 지원해 왔으며, OnAV를 통해 안드로이드 기반의 모바일 디바이스까지 보호 범위를 확대하였습니다.



높은 탐지 성능 확보

메타디펜더 멀티 스캐닝 기술은 머신러닝 기반의 OnAV를 비롯해 기존 휴리스틱 탐지 엔진들을 사용해 99% 이상의 탐지 정확도를 달성했습니다.

OnAV는 특히 모바일 · IoT 디바이스를 사용하는 고객들이 각종 보안 위협으로부터 안전할 수 있도록 안드로이드 악성코드 탐지 성능을 강화했습니다.



모바일 악성 앱 탐지 데이터 확보

OnAV를 통해 검사한 모바일 악성 앱 데이터는 연평균 51만건 수준입니다.

하루 평균 수집되는 샘플은 1400건, 1시간에 60건(1분당 1개) 가량 탐지되었습니다.

전체 검사 건수 중 60%가량의 악성(30.6만건), 40%가량의 정상(20.7만건) 데이터를 확보하였습니다.