지엠디소프트 모바일 포렌식 소프트웨어 **악성코드 감염 여부 분석 솔루션**

GMD SOFT
GLOBAL MOBILE & DIGITAL SOFTWARE

- **사이버 범죄와 디지털 포렌식 조사 수요 증가에 따라 '모바일 기기 내 악성코드 감염 데이터' 조사 중요성 강조**
- **국내 1위, 전 세계 60여 개국에 판매 중인 모바일 포렌식 분석 소프트웨어 MD-RED에 OnAV 백신 엔진 탑재**
- **모바일 데이터 분석 시 악성코드 자동 탐지 및 악성 앱, 파일 검출을 통한 포렌식 수사 효율 증대**

"

전 세계적으로 사이버 범죄가 증가함에 따라 모바일 포렌식 수사 시 악성코드 감염 검사에 대한 수요 또한 증가하고 있습니다.
지엠디소프트는 국내 1위 모바일 포렌식 연구 개발 기업으로 모바일 데이터 분석 소프트웨어 'MD-RED'를 전 세계 60여 개 국가에 판매하고 있습니다.
MD-RED에 탑재된 백신 엔진을 통해 사이버 범죄(피싱, 해킹, 사기) 조사 시 모바일 기기에 저장되어 있는 악성 앱 또는 악성코드에 감염된 파일들을 자동 검출하는데 활용되고 있습니다.

- 산업 : B2B
- 대상 : 글로벌 수요 기업
- 백신엔진 : OnAV

Challenge

사이버 범죄나 해킹 사건 조사를 위한 모바일 포렌식 과정에서 모바일 기기 내 악성코드 감염 데이터 또는 악성 앱에 대한 탐지와 분석 작업이 필요합니다. 수많은 악성 앱들에 대해 개별적인 앱 역공학 분석 방식으로 대응하기 어렵기에 안티 바이러스와 같은 백신 엔진이 포렌식 기술에도 접목되어야 합니다.

Solution

기존 방식의 OnAV는 안드로이드 및 리눅스 서버에 기반한 엔진을 제공하고 있으나 윈도우 기반의 모바일 포렌식 소프트웨어 MD-RED 내 탑재를 위해 커스터마이징 작업된 엔진을 패턴과 함께 제공했습니다.
또한, 신규 악성코드 감염 파일 또는 악성 앱에 대한 검출을 지속적으로 지원하기 위해 주기적인 업데이트를 제공하게 됩니다.

Result

모바일 기기 내 악성코드 감염 데이터 및 악성 앱 자동 검출

MD-RED에 탑재된 백신 엔진 OnAV을 통해 모바일 데이터 분석 시 자동으로 악성코드에 감염된 파일들과 악성 앱들을 빠르게 자동 검출하여 포렌식 수사의 효율을 높였습니다.

주기적 업데이트를 통한 글로벌 시장 요구 대응

백신 엔진의 주기적인 패턴 업데이트를 통해 최신 악성코드에 대한 자동 검출을 지원하고 분석 결과에 대한 상세 보고서를 제공함으로써 최신 사이버 범죄에 대한 신속한 모바일 포렌식 분석을 제공해야 하는 글로벌 시장 요구에 대응할 수 있었습니다.

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