SECURION

Business needs and use cases

시큐리온 솔루션 도입 사례집

Contents

Solution by task

Business needs & Use cases

지능화된 공격으로부터 모바일·IoT 기기와 서비스를 보호하는 12가지 방법

시큐리온의 'On'시리즈를 이용하면 신·변종 악성 앱, 탐지 및 분석 우회 기술이 적용된 고난도 악성 앱이 증가하는 상황에서도 합리적인 비용으로 강력한 기기 보안을 유지할 수 있습니다. 간편한 SW 설치만으로 단말의 APP 영역과 OS 영역을 동시에 보호하는 것은 물론 실시간 관제 시스템, 무결성 검사 서비스 등 고객 필요에 맞는 서비스로 맞춤형 보안 솔루션을 구축해 드립니다.

01 고난도·지능형 악성 앱 탐지 강화

Needs

- 신·변종 악성 앱 및 분석 방해 기술이 적용된 악성 앱에 대한 탐지율을 높이고 싶습니다.

Solution

- 시큐리온 OnAV는 독자 개발한 AI 탐지 시스템으로 신·변종 악성 앱 및 난독화 등 분석 방해 기술이 적용된 악성 앱에 신속하고 정확하게 대응합니다. 머신러닝 검사는 악성 행위에 기반한 검사 방식으로 지능형 악성 앱에 대한 탐지율을 높였습니다.

Case

- SK쉴더스 개인용 보안 솔루션 OnAV 도입 사례 **10p**

02 스파이웨어 및 제로데이 공격 대응

Needs

- 백신 외에도 백도어 탐지, OS 취약점을 이용한 스파이웨어 및 제로데이 공격에도 대응이 가능한 솔루션을 찾고 있습니다.

Solution

- 시큐리온 OnTrust는 단일 솔루션으로 단말의 APP 및 OS 영역을 동시에 보호할 수 있습니다. 특허받은 '공격 흔적 조사 기술'은 기기의 펌웨어 변조, 원격 침입, OS 보호 무력화, 백도어 설치 등 데이터 이상 징후를 분석해 역 추적하는 방식으로, 공격의 종류와 관계없이 대응이 가능합니다.

Case

- 국가재난안전통신망 단말 보안 솔루션 도입 사례 **24p** / 대한민국 국방 재난대응 특수 단말 보안 솔루션 도입 사례 **26p**
  한스웰 개방형 구름 보안 솔루션 도입 사례 **32p**

03 모바일·IoT 보안 위협 가시화 및 관제 시스템 제공

Needs

- 다수의 모바일·IoT 기기에 대한 보안 위협을 실시간으로 파악하고 보안 팀에서 원격 관제를 할 수 있는 시스템이 필요합니다.

Solution

- 시큐리온 OnTrust는 실시간 원격 관제가 가능한 위협관리 시스템 'OnTrust TMS'를 제공합니다.
  실시간 위협 탐지, 보호 기기의 분석 정보, 사용자 통계 등 각종 데이터로 보안 담당자를 위한 인사이트를 얻을 수 있습니다.

Case

- 국가재난안전통신망 단말 보안 솔루션 도입 사례 **24p** / 대한민국 국방 재난대응 특수 단말 보안 솔루션 도입 사례 **26p**

04 제로트러스트 구현을 위한 기기 안전성 검사

Needs

- 디지털 업무 환경에서 임직원들이 개인 기기로 기업 내부 시스템에 접속하게 되었습니다.
  만일의 경우에 대비해 해킹된 기기의 접속을 차단할 수 있는 검증 시스템이 필요합니다.
- 업무 목적으로 사용될 모바일·태블릿 단말을 현장에 투입하기 전, 백도어 등 위협이 없는지 확인하고 싶습니다.
- 기업 기밀을 다루는 경영진 및 특수 직군의 모바일 기기 안전성을 정기적으로 확인하고자 합니다.

Solution

- 시큐리온 OnTrust를 이용해 가상 업무 환경 및 기업 내부 시스템에 접속하는 모바일·IoT 단말의 안전성을 검사하고,
  해킹된 단말일 경우 접근을 차단하는 것이 가능합니다.
- OnTrust Agent가 설치되지 않은 단말들도 PC나 키오스크 등에 'OnTrust X-ray'를 설치하면 무결성 검사를 할 수 있습니다.

Case

- 경찰청 국가재난안전통신망 특수 단말 신속 해킹 검사 서비스 구축 사례 **22p**

05 대외비 단말 보호 시스템 구축

Needs

- 고위 임원진이나 연구진 등 업무상 비밀을 다루는 임직원의 스마트폰 해킹에 대비한 보안 시스템을 구축하고 싶습니다.

Solution

- 시큐리온 OnTrust는 해킹된 기기를 정상화할 수 있는 복구 장비 'OnTrust Dr'를 주요 기능으로 포함하여,
  해킹 탐지부터 단말 복구까지 가능한 대외비 기기 보안 시스템을 구축할 수 있습니다.

06 MDM, SIEM 등 타 보안 솔루션과의 병행 사용

Needs

- 기존 솔루션을 교체하지 않고 모바일 보안 솔루션을 결합하여 사용하고 싶습니다.
  또한 새로운 보안 솔루션을 적용할 때 보안 담당자의 업무가 번거로워지지 않도록 커스터마이징이 가능하면 좋겠습니다.

Solution

- 시큐리온 On 시리즈는 MDM, MAM을 포함한 모바일 기기 관리 솔루션은 물론 SIEM 등 통합 관리 솔루션,
  PC 보안 솔루션과도 결합이 가능합니다. 이를 통해 모바일 기기를 포함하여 일괄적이고 효율적인 보안 정책을 적용할 수 있습니다.

Case

- SK텔레콤 B2B 모바일 엔드포인트 보안 솔루션 OnAV 도입 사례 **20p**

07 보안 구역 모바일 단말 출입 관리

Needs

- 군부대, 공항, 기타 보안 구역에 반입되는 모바일 단말이 해킹되지 않고 안전한 상태인지 검사하여, 스마트폰이나 태블릿으로 인한 기밀 유출을 방지하고자 합니다.
- 보안구역의 출입 통제를 책임지는 키오스크 또는 태블릿 기기에 대한 보안 솔루션이 필요합니다.

Solution

- 시큐리온은 'OnTrust X-ray'를 통해 단말 무결성 검사 서비스를 제공합니다. 보안구역 입구에 해당 프로그램이 설치된 노트북이나 키오스크를 배치하고 검사하고자 하는 단말을 연결해 주세요.
- 보안 구역의 출입통제 기기를 보호하기 위해, 악성 앱 대응 및 OS 해킹 탐지 솔루션을 사용할 수 있습니다.

Case

- 국방부 영내 출입 통제 휴대용 리더기 보안 솔루션 도입 사례 **16p**

08 제조사가 다른 단말에 대한 통합 보안 시스템 구축

Needs

- 스마트 환경을 구성하는 단말의 제조사, 사양이 다양하여 이들을 통합 관리할 수 있는 보안 솔루션이 필요합니다.

Solution

- 기존의 OS 보안 솔루션들이 특정 제조사 또는 브랜드에 국한된 서비스를 제공하는 반면, 시큐리온 OnTrust는 안드로이드 단말이라면 제조사와 브랜드에 관계없이 간편한 소프트웨어 설치만으로 강력한 기기 보호 기능을 제공합니다. 실시간 위협 관제 시스템 'OnTrust TMS'를 통해 다양한 종류의 IoT 단말로 구성된 스마트 환경에서도 편리한 통합 관제 시스템을 구축할 수 있습니다.

Case

- 국가재난안전통신망 단말 보안 솔루션 도입 사례 **24p** / 한스웰 개방형 구름 보안 솔루션 도입 사례 **32p**

09 분석 업무 자동화·효율화

Needs

- 기존 모바일 백신으로 대응이 어려운 신·변종, 지능형 악성 앱이 증가함에 따라 분석에 필요한 인력 및 시간 리소스가 증가하고 분석가들의 피로도가 높아지고 있습니다. 분석 업무를 효율적으로 개선하기 위한 대안이 필요합니다.

Solution

- 시큐리온은 AI 기반의 악성 앱 분석 시스템 'OnAppScan'을 통해 악성 앱의 위험도와 행위 근거들을 자동으로 분석, 제공합니다. 보이스피싱 악성 앱 대응에 특화된 머신러닝 모델과 보이스피싱 디텍터가 난독화, 압축 해제 방해 등 분석 우회 기술이 적용된 지능형 악성 앱까지도 정확하게 탐지, 분석하여 분석가들의 업무 부담을 최소화할 것입니다.

Case

- KISA 디지털위협대응본부 스미싱대응팀 OnAppScan 도입 사례 **28p**

10 맞춤형 AI 모델링 제공

Needs

- 게임이나 금융 사칭 앱 학습 강화, 오래된 앱 유형 학습, 난독화 등 지능화된 악성 앱 특화 대응 등
  AI 모델링에 대한 특수한 요구를 반영해 주시기 바랍니다.

Solution

- 시큐리온은 고객사가 어떤 환경에 놓여 있는지, 기존의 머신러닝 모델로 충분히 높은 탐지율을 보장할 수 있는지 점검하고,
  필요하다면 새로운 AI 모델링을 제공할 것입니다. 지역, 산업군, 그 외 기업마다 특별히 주목해야 하는 악성 앱 유형이 존재하며,
  시큐리온은 On시리즈의 AI 탐지 엔진이 해당 유형을 가장 잘 탐지할 수 있도록 지원합니다.

Case

- 원스토어 마켓 침투 악성 앱 제거 AI 기반 자동분석 솔루션 OnAppScan 도입 사례 **30p**

11 앱 비즈니스 유지를 위한 신속한 이슈 대응

Needs

- 구글 등 앱 마켓 플레이스에서 각종 보안 정책이 강화되는 추세입니다.
  변화하는 플랫폼 정책에 맞게 앱 비즈니스가 원활하게 유지될 수 있도록 신속한 지원이 필요합니다.

Solution

- 앱 마켓의 보안 정책 변화에 빠르게 대응하지 못하면, 서비스 이용자 보호에 문제가 발생할 수 있습니다.
  시큐리온은 이러한 상황에서도 고객사의 서비스가 안정적으로 유지될 수 있도록 이슈 대응 및 서비스 옵션 개발을 지원합니다.

Case

- 아이티센 피엔에스 모바일 앱 보호 솔루션 '앱아이언 백신' OnAV 이슈 대응 지원 사례 **12p**

12 글로벌 보안 경쟁력 입증

Needs

- 글로벌 진출을 위해 해외 시장에서 통용되는 보안 인증 또는 성능평가 비교 자료가 필요합니다.

Solution

- 시큐리온이 독자 개발한 AI 탐지시스템은 모바일 안티바이러스 OnAV에 탑재되어 AV-TEST, AV-Comparatives 등
  각종 인증을 획득하였습니다. 세계 유명 보안 솔루션과의 비교 평가에서 종합 탐지율 100%를 기록한 시큐리온 솔루션 도입으로
  글로벌 시장에서 보안 경쟁력을 입증할 수 있습니다.

Case

- 지엠디소프트 세계 60개국 판매 모바일 포렌식 분석 소프트웨어에 OnAV 도입 사례 **14p**
  옵스왓 미국 OT 보안 멀티엔진 메타디펜더에 OnAV 탑재 사례 **18p**

About SecuriON

AI 기반 사이버 보안 기업 시큐리온은...

시큐리온은 5G, 스마트 환경에 특화된 모바일·IoT 보안 솔루션을 제공합니다. 독자 개발한 AI 탐지 시스템이 적용된 모바일 안티바이러스 'OnAV', 모바일·IoT 종합 보안 솔루션 'OnTrust', AI 기반 악성 앱 자동분석 시스템 'OnAppScan' 등이 핵심 제품입니다.

시큐리온의 AI 보안 솔루션은 날이 갈수록 고도화되는 악성 위협에 기업 및 기관이 효율적으로 대응할 수 있도록 돕습니다. 신·변종 악성 앱 탐지, 난독화 등 분석 방해 기법이 적용된 보이스피싱 악성 앱 탐지에 특화돼 있으며, 분석가들의 업무 효율을 높여 우수한 탐지율을 유지하면서도 인력 및 시간 리소스를 절감할 수 있습니다.

또한 악성 앱 위협은 물론 제로데이 공격을 포함한 OS 해킹 공격에 대응할 수 있는 보안 솔루션으로 모바일·IoT 디바이스가 포함된 스마트 환경에서 보다 강력한 보안 시스템을 구축하는 데 기여합니다.

머신러닝 기반 안티바이러스

OnAV

신·변종 악성 앱 탐지에 특화된 AI 기반의 모바일 안티바이러스 솔루션입니다.

독자 개발한 '크로스 밸리데이션 시스템(CVS, Cross-Validation System)'으로 높은 탐지율과 낮은 리소스 소모량을 구현했으며, 글로벌 보안 제품 성능 평가 기관 AV-TEST, AV-Comparatives, MRG-Effitas 등의 인증을 획득하였습니다.

모바일·IoT 종합 보안 솔루션

OnTrust

시큐리온의 AI 탐지 시스템과 특허 받은 OS 보호 기술로 모바일·IoT 단말의 APP 영역과 OS 영역을 동시에 보호하는 종합 보안 솔루션입니다.

실시간 해킹 탐지를 위한 'OnTrust Agent', 신속검사 서비스 'OnTrust X-ray', 위협 관제 시스템 'OnTrust TMS', 해킹 단말 복구 장비 'OnTrust Dr'로 구성돼 고객 필요에 따른 맞춤형 솔루션을 제안합니다.

AI 악성 앱 자동 분석 솔루션

OnAppScan

시큐리온의 AI 탐지 시스템을 기반으로 앱 분석 프로세스를 자동화하고 위험도를 판정하는 솔루션입니다.

수동 분석에 대한 의존도를 줄이고 분석 업무를 효율화함으로써 해당 업무에 소요되는 시간 및 비용 리소스를 절감합니다.

신·변종 악성 앱 및 난독화, 압축 해제 방해 등 분석 방해 기법이 적용된 보이스피싱 악성 앱 대응에 강점이 있습니다.

개방형 OS 보안 솔루션

OnTrust for Gooroom

개방형 OS 'Gooroom'이 적용된 데스크탑 PC 및 노트북을 보호하기 위한 솔루션입니다.

리눅스 앱 보안을 위한 안티바이러스 'OnAV for Gooroom', 운영체제 보호 솔루션인 'OnTrust for Gooroom Agent', 중앙관제 시스템 'OnTrust for Gooroom TMS'를 결합하여 사용할 수 있습니다.

'OnTrust for Gooroom'을 이용하면 구름 OS의 보안상태 검사, OS 보호 시스템을 무력화하는 악성 공격 탐지 대응 등이 가능합니다.

SK쉴더스
개인용 보안 솔루션 '모바일가드'

SK shieldus

- **SKT 'T가드'→SK쉴더스 '모바일가드'로 리브랜딩**
- **보안 넘어 가족 케어 포함한 모바일 케어 플랫폼으로 확장**
- **시큐리온 AI 탐지 시스템 이용 첨단 보안 기술 적용**

"

SK쉴더스의 '모바일가드'는 최신 AI 백신 엔진을 탑재해 신·변종 악성 앱, 원격제어 앱 등을 실시간으로 탐지할 수 있는 개인용 모바일 보안 솔루션(앱)입니다.
빠른 검사를 원하는 고객들을 위한 간편 검사, 정밀 검사, 스미싱 검사 등의 보안 기능을 제공합니다.

- 산업 : B2C
- 대상 : 무선 통신 이용자
- 백신 엔진 : OnAV

Challenge

현재의 '모바일가드'는 SKT의 'T가드'를 리브랜딩 한 것으로, SKT와 시큐리온이 공동으로 개발한 개인 이용자용 보안 솔루션(앱)이 그 전신입니다. SKT는 스미싱 피해가 급증했던 2013년 해당 서비스를 최초 도입하였으며, 2014년부터 SKT 단말에 해당 앱을 선탑재 하여 자사 고객들의 보안 위협에 대응했습니다.

이후 '모바일가드'가 런칭된 시기에는, 스미싱 악성 앱 외에 메신저 피싱 악성 앱이나 원격제어 앱을 이용한 보이스피싱 공격이 증가하면서 이 같은 유형에도 대응할 수 있도록 더욱 고도화된 백신 엔진이 필요해졌습니다.

Solution

SK쉴더스와 시큐리온은 지능화되는 보안 위협에 대응할 수 있도록 AI 기반 정밀 검사 기능을 고도화했습니다.
다운로드 수 1,424만건에 달하는 대규모 서비스인만큼 상세 검사를 원하는 고객은 정밀 검사를, 간단한 점검을 원하는 고객은 빠른 검사를 이용할 수 있도록 기능을 구성해 두었습니다.

보이스피싱에 주로 이용되는 원격 제어 앱에 대한 탐지 기능도 강화했습니다.
특히 문자나 메신저 등으로 원격 조종 앱을 설치하게 유도하여 금전 등을 갈취하는 보이스피싱 유형이 증가함에 따라 SMS, MMS, 기타 메신저 서비스를 통해 전달된 URL을 검사하여 이용자가 악성 앱을 다운로드 받기 전에 위협을 사전 차단할 수 있도록 했습니다.

Result

모바일 보안 기능 고도화

'모바일가드'가 종합적인 모바일 케어 플랫폼으로 확장되면서도 본연의 기능인 '모바일 보안'에 충실할 수 있도록 고객 니즈와 최신 공격 유형을 반영한 보안 기능을 구현하였습니다.

대규모 서비스 안정적 운영

'모바일가드'는 OnAV가 탑재된 보안 솔루션 중, 가장 많은 사용자를 보유한 서비스입니다.
'모바일가드'는 이용자들을 대상으로 클라우드 서버 기반 AI 검사 결과를 실시간으로 제공합니다.

시큐리온은 다수의 동시 접속자를 수용하기 위해 SDK 공급 및 앱 개발뿐만 아니라,
클라우드 기반 백엔드 서버 개발 및 구축 등을 지원하며 수년째 안정적으로 서비스를 유지하고 있습니다.

최신 보안 서비스 개발

시큐리온은 '모바일가드'에 필요한 추가적인 보안 기능을 제안하고 구현합니다.
모바일 안티바이러스 OnAV와 OS 보호를 위한 OnTrust의 핵심 기능을 고객이 원하는 방식으로 커스터마이징 할 수 있으며, 이들 기능을 활용한 유료 서비스 등을 기획할 수 있도록 지원합니다.

안티바이러스 엔진 리브랜딩

아이티센 피엔에스 모바일 앱 보호 솔루션 ‘앱아이언 백신’ 탑재

아이티센 피엔에스

- **기업 및 기관의 앱 서비스 보호와 신뢰도 향상에 기여**
- **다양한 고객사 앱 안정적으로 보호**
- **기존 보유 모바일 보안 솔루션들과 함께 ‘모바일 앱 보호 3종’ 라인업 완성**

“

아이티센 피엔에스는 바이오 전자서명 서비스 기반 핀테크 보안 기술 기업으로, 시큐리온의 OnAV를 리브랜딩한 안티바이러스 ‘앱아이언 백신’을 출시했습니다.
아이티센 피엔에스는 이미 자사 기존 보안 솔루션인 앱 위변조 방지 및 난독화 솔루션 ‘앱아이언’과 키패드 보안 솔루션 ‘앱아이언 키패드’를 보유하고 있었으며, ‘앱아이언 백신’으로 모바일 보안 솔루션 라인업을 완성했습니다.

- 산업 : B2B
- 대상 : 기업 및 기관 앱 서비스 30여 개
- 솔루션 : OnAV

Challenge

증권사와 금융사를 중심으로 앱 난독화와 안티바이러스 솔루션에 대한 수요가 증가했습니다.
이 외에도 정부 기관 및 공기업, 핀테크 기업 등 자사 서비스 및 이용자 정보 보호와 신뢰 확보가 중요한 고객사들이 해당 기능을 필요로 하는 상황이었습니다.

Solution

시큐리온의 안티바이러스 OnAV를 '앱아이언 백신'으로 리브랜딩 하여 기존 '앱아이언' 보안 라인업을 사용하는 고객들에게 보다 강화된 보안을 제공할 수 있었습니다.

기존의 앱 난독화 솔루션과 백신 SDK를 연계한 '빌트인 방식' 또는 보호 대상인 고객사 앱과 '앱아이언 백신'을 연동해 사용할 수 있는 '보안 앱 연동 방식'으로 서비스됩니다.

'앱아이언 백신'고객에 금융 기업이 다수 존재하여, 앱 실행 시점부터 중요 정보를 통신하는 인증 시점 사이에도 빠르게 기기의 이상 유무를 검사할 수 있도록 한 '신속검사'기능을 특화 서비스로 제공했습니다. 또 동시 접속이 대거 발생할 경우에도 안정적으로 검사를 실행할 수 있도록 '콘텐츠 전달 네트워크(CDN)'를 도입했습니다.

Result

글로벌 인증받은 높은 탐지율로 신뢰 확보

시큐리온 OnAV는 머신러닝 검사와 패턴 검사, 평판 검사를 결합한 '크로스 밸리데이션 시스템(CVS, Cross-Validation System)'으로 높은 탐지율과 낮은 리소스 소모량을 구현했습니다.

종합 탐지율 100%의 성적으로 AV-TEST, AV-Comparatives, MRG Effitas 등의 권위 있는 글로벌 성능 평가 기관에서 수 년째 인증을 받고 시장의 신뢰를 획득하였습니다.

고객 수요에 기반한 솔루션 기획·개발

금융, 증권 업계는 다른 분야보다 철저한 보안을 필요로 하며, 요구하는 솔루션의 종류도 다양합니다. '앱아이언 백신'은 아이티센 피엔에스이 보유한 다양한 기존 보안 솔루션과 원활하게 연동되어 이러한 고객 수요를 만족시킬 수 있었습니다.

유연한 이슈 대응과 서비스 옵션 지원

최근 구글의 개인정보 정책 강화로, 보안 기능이 탑재된 일반 앱들이 구글 앱 마켓 등록 심사에서 대거 탈락하는 사례가 발생했습니다. 구글이 악성 앱 검사를 위한 필수 기능인 'QUERY_ALL_PACKAGES' 권한을 '민감 정보를 읽어가는 권한'으로 판단해 심사한 결과입니다.

그러나 많은 일반 앱들은 여전히 기업 및 기관의 서비스 보호와 사용자 데이터 보호를 위해 안티바이러스 기능을 필요로 합니다.
시큐리온은 아이티센 피엔에스와 협의하여 고객들이 직접 보안 수준과 보안 서비스 제공 방식을 선택하도록 했습니다.

이제 고객들은 △최근 사용한 앱 검사 △실시간 알림 앱 검사 △실시간 앱 설치 검사 △설치된 앱 전체 검사 △설치된 앱 검사 및 실시간 검사 중에서 서비스에 필요한 보안 수준과 운영 편의를 고려한 옵션을 적용할 수 있습니다.

지엠디소프트 모바일 포렌식 소프트웨어 **악성코드 감염 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
- 솔루션 : 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.

국방부 국방전산정보원
영내 출입 통제 휴대용 리더기(PDA) 보안

국방전산정보원

- **최고 수준의 국방 보안 시스템 '영내 출입 통제 체계' 적용**
- **'영내 출입 통체 체계' 구축에 도입된 안드로이드 기반 IoT 기기 보안 위협 대응**
- **저사양·폐쇄망 환경에서 운영 가능한 보안 솔루션 구축**

"

국방부 국방전산정보원의 '영내 출입 통제 체계 개선 사업' 은 영내 주요 건물 출입문과 시설에 대한 출입 통제를 강화하고, 부대 보안 업무의 효율성을 향상하기 위해 추진되었습니다.
최첨단 출입 통제 시스템과 관리 소프트웨어를 통해 보안 구역에 대한 물리적 위협과 정보 보안 위협에 대응합니다.

- 산업 : B2G
- 대상 : 영내 출입 통제 휴대용 리더기(PDA)
- 솔루션 : OnAV

Challenge

'영내 출입 통제 체계 개선 사업' 추진에 따라 안드로이드 기반의 출입 통제 휴대용 리더기(PDA)가 도입되면서, 이를 대상으로 한 악성코드 및 해킹 위협에 대응할 수 있도록 보안 수준이 강화될 필요가 있었습니다.
그러나 국방망의 특성상 폐쇄적인 네트워크 환경과 기기 인터페이스의 특이성이 존재하여 일반적인 보안 솔루션을 바로 도입, 운영하기는 어려운 상황이었습니다.

Solution

일반적으로 많은 IoT 기기들이 스마트폰에 비해 낮은 사양을 가지고 있고, 관리/운영 측면에서도 한정적인 인터페이스를 제공합니다.
시큐리온의 보안 솔루션들은 이 같은 저사양 환경에서도 정상적으로 탐지 성능을 발휘할 수 있도록 설계되어 있습니다.
시큐리온은 영내 출입 통제를 위해 제공된 휴대용 리더기(PDA)의 사양 및 인터페이스와 관계없이 실시간으로 기기를 보호할 수 있는 안티바이러스 엔진을 제공함으로써 이러한 문제를 해결했습니다.

또 폐쇄망 네트워크 환경에서도 패턴 업데이트가 신속히 이뤄질 수 있도록 자체 PMS(패턴 및 패치 관리 시스템) 구축 및 PMS 소프트웨어 제공, 오프라인 업데이트 기능 등 다양한 옵션을 제공하여 국방부 맞춤형 솔루션을 납품하였습니다.

Result

영내 출입 통제 기기 보안 솔루션으로 물리 보안까지 강화

보안구역의 출입 통제를 책임지는 휴대용 리더기(PDA)가 악성 앱에 감염되거나 해킹을 당한다면, 해당 구역에 대한 물리적인 보안까지 위협받는 상황을 초래할 수 있습니다.
시큐리온의 OnAV는 통제 기기에 대한 정보 보안을 강화하여 해당 리스크에 대비함으로써 '영내 출입 통제 체계 개선'이라는 사업 본연의 목적을 달성하는 데 기여하였습니다.

폐쇄망 환경에서의 보안 강화

외부와의 연결을 차단한 폐쇄망 운영 환경에서도 제약 없이 패턴 업데이트 반영이 가능하도록 시스템을 구축하여, 신·변종 악성 위협에 신속히 대응할 수 있게 되었습니다.

내부망에서 발생할 수 있는 악성코드 위협 대응

비교적 안전하다고 여겨지는 폐쇄망이지만, 그럼에도 불구하고 내부망에서 발생할 수 있는 위협이 존재합니다. OnAV는 디바이스의 보안 소프트웨어를 최신 상태로 유지해 이 같은 위협에 대응합니다.

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.

SK텔레콤 B2B 모바일 엔드포인트 보안 솔루션 '스마트백신'

- **MDM 연동 가능한 안티 바이러스 엔진**
- **기존 구축된 보안 시스템에 백신 기능을 통합하여 관리 효율 향상**
- **다양한 기업 및 기관에서 합리적 금액으로 이용 가능**

SK텔레콤의 '스마트백신'은 기업 고객을 대상으로 업무용 모바일 단말 보안 서비스를 제공합니다.
기존에 구축된 MDM 보안 솔루션과 결합하여 업무용 단말을 효율적으로 관리,
관제할 수 있도록 커스터마이징 된 서비스로 기업 및 기관이 이용 중입니다.

- 산업 : B2B
- 대상 : 모바일 엔드포인트 보안이 필요한 기업 고객
- 솔루션 : OnAV

Challenge

SK텔레콤은 기업 및 기관을 대상으로 한 모바일 엔드포인트 보안 솔루션을 제공해 왔습니다.
기존에 제공되던 솔루션은 MDM(Mobile Device Management)과 안티바이러스로, 두 제품이 서로 연동되지 않고
각각 동작하거나 서드파티(Third Party) 앱이 안티바이러스 앱을 호출하는 형태로 동작하는 시스템이었습니다.

이러한 동작 방식은 기업이 사용하는 모바일 기기에 일괄적이고 효율적인 보안 정책을 적용하는 데 장애가 되었고,
SK텔레콤은 이를 보완하기 위해 기존 MDM과 연동해 사용할 수 있는 안티바이러스 제품을 도입하기로 했습니다.

Solution

시큐리온은 고객의 필요에 따라 다양한 커스터마이징 형태로 제품을 공급합니다.
시큐리온은 SK텔레콤이 겪고 있는 이슈를 해결하기 위해, MDM과 안티바이러스를 통합한 엔터프라이즈 보안 관리자를 개발했습니다.

새로운 시스템은 엔터프라이즈 보안 관리자에서 안티바이러스 정책을 설정하면 OnAV가 그대로 악성 앱을 탐지, 검사하고 후속 조치까지 진행할 수 있도록 했습니다. 이를 통해 보안 정책 및 솔루션의 관리 편의가 크게 향상되었고, 다수의 기업 및 기관에서 사용하는 엔드포인트 보안 솔루션이 되었습니다.

Result

기존 보안 기능과 OnAV 연동으로 제품 업그레이드

모바일 기기를 보호하기 위해서도 다양한 보안 솔루션이 존재합니다.
그중에서도 안티바이러스와 MDM은 가장 대중적인 솔루션인데, 모든 기업이 이런 솔루션들을 같은 보안 제조사에서 동시에 구매, 적용할 수 있는 상황인 것은 아닙니다.

시큐리온은 SK텔레콤의 '스마트백신'을 통해 기존에 구축된 보안 솔루션에 OnAV 엔진을 연동해 무리 없이 제품 성능을 업그레이드하였습니다.

효율적인 관제 시스템 적용

엔터프라이즈 보안 관리자를 통해 서로 다른 보안 솔루션의 관리 플랫폼을 일원화하고, 직접 정책을 설정하고 탐지된 앱에 대한 후속 조치까지 취할 수 있도록 함으로써 보안 담당자의 업무 효율을 높였습니다.

단말 무결성 검증 통한 보안 리스크 해소
국가재난안전통신망 신속 해킹 검사 서비스

경찰청
KOREAN NATIONAL POLICE AGENCY

- **단말 해킹 검사를 통해 국가사업 보안 강화**
- **국가재난안전통신망에 사용되는 특수단말, 무결성 검증 후 현장 적용**

"

국가재난안전통신망에는 국내 7개 제조사에서 공급하는 특수 단말기가 사용됩니다.
제조사들은 엄격한 보안 요구를 충족해야 하며, 경찰청 또한 제조사들이 공급한 단말의 무결성을 한번 더 검증할 수 있도록 OnTrust X-ray를 도입해 보안 절차를 강화하였습니다.

- 산업 : B2G
- 대상 : 국가재난안전통신망 전용 특수 단말
- 솔루션 : OnTrust X-ray

Challenge

국가재난안전통신망은 폐쇄망 환경으로 구축, 운영되어 외부 공격자의 위협 가능성은 낮을 것으로 예상되었습니다.
그러나 기기에 존재하는 OS 취약점을 공격하여 관리자 권한을 탈취하고 백도어를 설치한 경우에는 이를 탐지할 수 있는 솔루션이 없었고, 이러한 방식을 통한 외부 위협 가능성을 완전히 배제할 수는 없기 때문에 경찰청은 국가 주도의 보안 검증 시스템을 추가로 구축하고자 하였습니다.

Solution

OnTrust X-ray는 키오스크 또는 노트북과 연결된 단말의 보안 취약점과 해킹 여부를 빠르게 검사하여 분석 결과와 대응 방안을 제시합니다.

시큐리온은 경찰청에 OnTrust X-ray를 공급하여, 국가재난안전통신망에 사용되는 단말의 해킹 여부를 직접 검사할 것을 제안했습니다. 경찰청은 이를 통해 단말 보안을 제조사에만 맡겨두지 않고, 해킹된 기기인지 여부를 한번 더 확인하여 안전하다고 검증된 단말만을 국가재난안전통신망 사업에 사용하도록 했습니다.

Result

신뢰할 수 있는 단말 도입으로 보안 사고 예방

제조사가 납품한 단말을 경찰청이 한번 더 검사함으로써 해킹 되었거나 보안에 취약한 상태의 단말을 사전에 걸러낼 수 있게 되었습니다.

경찰청은 OnTrust X-ray 도입 후 스마트폰의 잠금 상태가 해제된 단말이 납품된 사례를 발견하여 현장 도입을 차단하였습니다.

향상된 보안 수준 유지 시스템

단말 제조사는 기기를 최초 공급한 이후 일정 기간 FOTA(Firmware OTA) 서비스를 통해 기기를 최신 버전 S/W로 유지할 의무가 있습니다.

시큐리온은 기기에 앱을 설치할 때 악성 앱 및 악성코드가 유입되는 것을 방지하며, 제조사에서 배포한 펌웨어 버전이 무결한지 실시간으로 검증합니다. 이러한 역할 분담을 통해 단말 자체 보안 기능이 없는 기기에 대해서도 보안 수준을 한 단계 업그레이드한 상태로 유지할 수 있습니다.

백도어 및 제로데이 공격 탐지 가능
국가재난안전통신망 단말 보안 솔루션

- 소방, 경찰 등 '국가재난안전통신망'용 특수 단말 보안 솔루션 제공
- 백신 기능 외 악성 앱·백도어 탐지, 무결성 검증까지 가능한 종합 보안 솔루션
- 단말 위협 실시간 모니터링 가능한 TMS(위협 관제 시스템) 제공

"

국가재난안전통신망은 소방, 경찰, 군, 지방자치단체 등 재난 대응 기관들이 운용하는 통신망을 단일망으로 통합하여 재난 현장에서 효율적인 지휘 협조 체제를 구축할 수 있도록 지원합니다. 경찰, 소방, 의료, 해경, 군, 지자체, 전기, 가스 관련의 8대 재난대응 공통분야 324개 기관은 필수적으로 '국가재난안전통신망'을 이용하도록 하고 있습니다.

- 산업 : B2G, 공공통신 인프라
- 대상 : 국가재난안전통신망 단말 약 20만대
- 솔루션 : OnTrust Agent

Challenge

국가재난안전통신망이 사이버 공격을 당할 경우 국민의 생명과 안전에 직접적인 위협이 되며, 심각한 사회 혼란을 야기할 수 있습니다. 그러나 기존에 사용하던 백신 솔루션 만으로는 OS 취약점 및 백도어를 활용한 공격 위험에 제대로 대응할 수 없었습니다.

폐쇄망 특성상, 외부 네트워크와의 통신이 불가능하기 때문에 적시에 중앙 관리 시스템을 통해 패치 또는 백신 패턴을 업데이트할 수 없다는 점이 가장 큰 어려움이었습니다.

기존의 자동화 되지 않은 패턴 업데이트 방식으로는 다양한 보안 위협에 신속히 대응하는 데 한계가 존재했습니다.
또 개별 단말의 악성 앱 탐지 기능을 넘어서 시스템에 포함된 다양한 단말에 대한 위협을 통합 관제하는 데도 어려움이 있었습니다.

Solution

행정안전부 재난안전센터와 KT는 패턴 업데이트가 가능하면서도 백도어 공격을 실시간으로 탐지할 수 있는 시큐리온 OnTrust 엔진을 도입했습니다.

국가재난안전통신망에 단말을 공급하는 7개 제조사에 탑재된 OnTrust는 기존에 자동화되지 않은 패턴 업데이트 주기를 당길 수 있도록 폐쇄망을 관리하고 있는 행정안전부 내에 패턴 업데이트 기능을 포함한 TMS(위협 관제 시스템)를 자체 구축하는 방식으로 적용되었습니다. 그 결과 정해진 스케줄에 따라 자동으로 패턴 업데이트 및 검사 기능을 진행하고 있습니다.

OnTrust Agent는 특허받은 OS 커널 보호 기술로 백도어 공격을 탐지해, 기존 보안 솔루션이 커버할 수 없었던 OS 영역까지 안전하게 보호합니다. 또 특정 단말 제조사나 모델명에 구애받지 않고 간단한 소프트웨어 설치 만으로 보호 기능을 탑재할 수 있어, 다양한 제조사가 함께하는 국가재난안전통신망에 적용하기 적합한 제품입니다.

국가재난안전통신망의 특수한 상황에 맞게 커스터마이징된 OnTrust Agent 도입으로, 재난안전통신 인프라의 보안성이 대폭 강화됐을 뿐 아니라, 개별 단말에 대한 위협 현황을 실시간으로 중앙 관제할 수 있도록 해 관리 효율도 향상시켰습니다.

Result

백도어 및 OS 취약점 공격 탐지 가능

OnTrust Agent는 특허받은 OS 커널 보호 기술인 '공격 흔적 조사 기술'을 통해 단말의 OS 영역을 보호합니다. 백도어 공격 탐지 외에도 악성 앱 설치 및 펌웨어 변조, 원격 조종 권한 탈취 등 다양한 공격을 실시간으로 탐지할 수 있으며, 이미 알려진 공격은 물론 알려지지 않은 제로데이 공격 방어도 가능해 졌습니다.

모바일 및 태블릿에 적합한 초경량 엔진

국가 재난안전통신망에 사용되는 특수 단말은 일반적인 스마트폰이나 데스크톱 PC 등에 비해 상대적으로 적은 용량으로 설계되어 있습니다.
OnTrust Agent는 하드웨어 용량의 한계에 구애받지 않는 초경량 엔진으로, 모든 종류의 단말에 문제없이 탑재되었습니다.

실시간 위협 관제 가능

OnTrust Agent의 도입으로 국가재난안전통신망 단말기에 가해지는 각종 사이버 위협 현황을 실시간으로 모니터링할 수 있게 되었습니다. 기존에는 개별 단말에서만 보안 현황을 파악할 수 있었으나, OnTrust Agent는 중앙 관제가 가능한 TMS(위협 관제 시스템)를 제공하여 관제 효율성을 한 단계 높이고, 위협 발생 시 일사불란한 대응과 분석이 가능하도록 하였습니다.

대한민국 국방
재난대응 특수 단말 보안 솔루션 도입

대한민국육군 Republic of Korea Army
대한민국공군 REPUBLIC OF KOREA AIR FORCE
대한민국 해병대 REPUBLIC OF KOREA MARINE CORPS

- **재난 현장 지원 시 군에서 사용하는 특수 단말 보안 강화 필요**
- **OnTrust Agent, 단말 APP 및 OS 영역 동시 보호 제공**
- **TMS(위협 관제 시스템)를 통해 폐쇄망 환경에서도 탐지 성능 유지**

"

육군을 비롯한 대한민국 군은 재난안전통신망 및 모바일 기기를 통한 재난업무 수행 환경을 구축, 활용하고 있습니다.
군은 재난안전통신망을 이용해 태풍과 산불, 붕괴 사고 등 다양한 재난 상황에서 재난 안전 유관 기관과 협력하며, 원활한 구호 활동을 위해서는 단말의 보안이 보장되어야 합니다.

- 산업 : B2G
- 대상 : 대한민국 국방 재난 대응 특수 단말
- 솔루션 : OnTrust Agent

Challenge

국방부는 2022년 행정안전부가 335개 기관을 대상으로 실시한 '재난관리평가'에서 최우수 기관으로 선정될 만큼 재난 대응 역량이 우수한 기관입니다. 군이 재난 대응에 사용하는 단말의 보안 기능을 강화하기 위해, 악성 앱 공격뿐 아니라 OS 취약점 공격 등 다양한 위협 상황에도 대응할 수 있는 보안 솔루션 도입이 요구되었습니다.

Solution

시큐리온은 OnTrust Agent를 군 모바일 단말기에 선탑재하여 단말의 APP 영역과 OS 영역을 동시에 보호할 수 있도록 제안했습니다.
이를 통해 재난안전통신망 전용 회선을 통해 중앙 관리 시스템에서 신규 패턴 및 보안 정책을 업데이트할 수 있게 되었습니다.

Result

국가 재난안전인프라 보안 강화

기존에 제공되던 물리보안(MDM 등) 중심의 보호 기능이 악성 앱 위협 대응과 단말 무결성 검사 등으로 확대되면서 더욱 강력한 보안을 구현하였습니다.
재난 발생 시 핵심적인 역할을 하는 군의 재난안전통신망 모바일 단말 보안이 강화됨으로써 국가의 재난안전인프라 보안도 더욱 강력해졌습니다.

신·변종 악성 앱 신속 대응

중앙 관리 시스템을 통해 자동으로 패턴을 업데이트하고 단말 검사 기능을 실행하도록 해
신·변종 악성 앱도 효과적으로 탐지합니다.

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.

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.

한스웰
개방형 구름 OS 보안 솔루션 도입

hanswell
Exploring beyond communications

- **한스웰, 리눅스 앱 보호 위한 특화 보안 솔루션 도입**
- **OnAV for Gooroom, 폐쇄망 환경에서도 정기적인 백신 업데이트로 강력한 보안 실행**
- **GS인증 1등급, NIA 인증 획득**

"

한스웰은 국가재난안전통신망에 사용되는 특수 단말 제조사로, 재난안전망 요구기능과 지령업무에 특화된 단말기를 공급하고 있습니다. 특정 OS에 종속되지 않는 환경을 구축하고자 하는 정부 정책에 발맞춰 국내 기술로 개발한 개방형 OS '구름'이 적용되어 있으며, 그에 맞는 보안 솔루션을 도입하여 악성 위협에 대응합니다.

- 산업 : B2B
- 대상 : 국가재난안전통신망 납품용 특수 단말 S380
- 솔루션 : OnAV for Gooroom Agent

Challenge

국가재난안전통신망은 외부 네트워크와 통신이 불가능한 전용망을 사용하고 있습니다. 따라서 백신 솔루션의 패턴 업데이트를 위해서는 자체 PMS(패턴 및 패치 관리 시스템)를 구축하여 운영하는 방식이 필요한 상황이었습니다.
특히 보호 대상인 지령업무 특화 탁상형 단말기는 IPv6(Internet Protocol version 6) 네트워크망으로 업데이트를 진행해야 하는 구름 OS를 사용 중이었습니다.

Solution

시큐리온은 행정안전부 내에 안티바이러스 패턴 업데이트를 제공할 수 있는 PMS(패턴 및 패치 관리 시스템)를 구축하고,
구름 OS가 설치된 기기에서 IPv6 네트워크 망을 통해 정기적인 패턴 업데이트와 검사 기능이 동작할 수 있도록 했습니다.

Result

구름 OS 단말 보안 강화

시큐리온은 IPv6 업데이트를 지원하고 폐쇄망 환경, 개방형 OS 적용 등 주어진 조건 안에서 단말을
보호할 수 있도록 최적화된 시스템을 구축함으로써 구름 OS가 적용된 단말의 보안성을 높였습니다.

신·변종 악성 앱 위협에 신속 대응

행정안전부 내에 구축한 PMS(패턴 및 패치 관리 시스템)를 통해 정기 패턴 업데이트가 가능한
OnAV for Gooroom 엔진이 탑재되어, 신·변종 악성 위협에 보다 효율적으로 대응할 수 있게 되었습니다.

Reference

국가재난안전통신망

경찰청 KOREAN NATIONAL POLICE AGENCY
행정안전부
kt
SAMSUNG 삼성전자
CYBERTEL bridge
STraffic
(주)가보테크 GABOTECH Co.,Ltd
hanswell Exploring beyond communications
BLUEBIRD

한국전기안전공사 Korea Electrical Safety Corporation
한국가스공사 KOREA GAS CORPORATION
smart KPX 전력거래소 KOREA POWER EXCHANGE
KCA 한국방송통신전파진흥원
KNOC 한국석유공사
KORAIL
한국남부발전㈜
수도권매립지관리공사
국립중앙의료원 national medical center
한국원자력환경공단 KOREA RADIOACTIVE WASTE AGENCY
한국수력원자력㈜
KINS 한국원자력안전기술원 KOREA INSTITUTE OF NUCLEAR SAFETY
중앙전파관리소
북부지방산림청
해양수산부
환경부
환경부 수도권대기환경청
환경부 낙동강유역환경청
국립소방연구원 National Fire Research Institute
국토안전관리원
Incheon Airport
대한민국육군 Republic of Korea Army
대한민국공군 REPUBLIC OF KOREA AIR FORCE
해양경찰청 KOREA COAST GUARD
국군재정관리단
국군의무사령부 The Armed Forces Medical Command
구의아리수정수센터

서울특별시
경기도
busanjin
울산광역시 울주군
yohang 포항시
사천시
삼척시 SAMCHEOK CITY
단양군 꿈과 희망이 있는 살기좋은 단양!
진천군
함양군
익산시
울진군
이천시 Icheon
광주시 GWANGJU CITY
하동군
광진구
송파구
청송군

SEOC 서울종합방재센터
경기도소방재난본부 GYEONGGI-DO FIRE SERVICES
경기도소방 경기도북부소방재난본부
강원도소방본부 Gangwon Fire HeadQuarter
119 경상북도 소방본부 Gyeongbuk Fire Service Headquarters
다양꿈 미래로 뛰노는 제주 소방안전본부
전북소방 119
Safe-Jeonnam 119 전남소방본부
울산광역시소방본부 ULSAN FIRE DEPARTMENT
119 부산광역시소방재난본부 BUSAN METROPOLITAN CITY FIRE & DISASTER HEADQUARTERS
세종특별자치시 119 소방본부
대구소방안전본부 DAEGU FIRE DEPARTMENT
119 서울소방
경기도소방 화성소방서
대전소방본부 119 DAEJEON FIRE HEADQUARTERS
광주광역시 소방안전본부
119 충청북도소방본부 CHUNGBUK FIRE SERVICE HEADQUARTER
광주 경찰청 GWANGJU METROPOLITAN POLICE AGENCY
충청남도 소방안전본부 Chungcheongnam-do Fire & Safety Headquarters
주식회사 라온에스 RAONUS

공공

대한민국육군 Republic of Korea Army
대한민국공군 REPUBLIC OF KOREA AIR FORCE
국방전산정보원
경찰청 KOREAN NATIONAL POLICE AGENCY
미래창조과학부
보건복지부
세종특별자치시
용인시 YONGIN CITY
Incheon Airport
KISA 한국인터넷진흥원
TS 한국교통안전공단
KITECH 한국생산기술연구원
서울교통공사 Seoul Metro
5678 서울도시철도
김포 GOLDLINE
Seoul Metro 서울메트로
KAI 한국항공우주산업㈜ KOREA AEROSPACE INDUSTRIES, LTD.
한국전력
한국가스공사 KOREA GAS CORPORATION

민간

SK telecom
SK networks
SK C&C
SAMSUNG 삼성전자
SAMSUNG 삼성SDS
LG U+
ONE STORE
F&U
cross
monee
KOREA GOLD EXCHANGE 한국금거래소
KOREG 신용보증재단중앙회
경기신용보증재단 Gyeonggi Credit Guarantee Foundation
동양저축은행
moin
센골드
KOREA GOLD EXCHANGE 금방금방 디지털에셋
bankware global
SK shieldus
SK 주식회사
SK encar.com
cen 시큐센 secucen
GMD SOFT
오리온
OPSWAT.
KOOLSPAN
고려대학교의료원 KOREA UNIVERSITY MEDICAL CENTER
고려대학교구로병원 KOREA UNIVERSITY GURO HOSPITAL
고려대학교안산병원 KOREA UNIVERSITY ANSAN HOSPITAL
ALPACO (주)알파코

Partners

ENKI
cen 시큐센 secucen
SU Secure Us Security Service Provider
SK shieldus
SK telecom
TRUSTAR SECURITY Edge Cyber Security Solutions
KAIST
KISA 한국인터넷진흥원
KOOLSPAN
OPSWAT.
Safe-Net Forum 공공안전통신망 포럼
CYBERTEL bridge
AM Traffic
GMD SOFT
GUARDSQUARE Mobile application protection
ProGrace
Hyundai J·Comm
UNION 주식회사 유니온소프트
HYUNDAI Rotem
NICOM 주식회사 나이콤

Awards winning cyber security solution

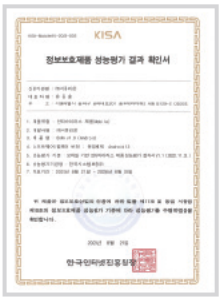
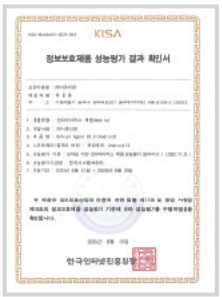
글로벌 TOP3 인증 획득

독일	오스트리아	영국	중국	중국

인증	횟수	내역	비고
AV-TEST	32회	2018년 7/9/11월, 2019년 1/3/5/7/9/11월, 2020년 1/3/5/7/9/11월, 2021년 1/3/5/9/11월, 2022년 3/5/7/9/11월, 2023년 1/3/5/7/9/11월, 2024년 1/3월	연 6회 평가 (매 홀수 달)
AV-Comparatives	6회	2019년-2024년	연 1회 평가
MRG Effitas	2회	2019년 2분기, 3분기	
SKD Labs	1회	2019년	
PCSL	4회	2018년 3분기,4분기, 2019년 1분기, 2분기	

국내 인증 및 성능 평가



구분	인증(수상) 제품명	인증기관
GS 인증	OnAV V1.0	한국정보통신기술협회(TTA)
	OnTrust Agent V2.0	한국화학융합시험연구원(KTR)
	OnAV for Gooroom V1.0	
NIA 인증	OnTrust Agent V2.0	한국지능정보사회진흥원
	OnAV for Gooroom V2.0	
정보보호제품 성능평가	OnAV V1.0	한국인터넷진흥원
	OnTrust Agent V2.0	

모바일·IoT 종합 보안 솔루션 OnTrust,
2023년도 하반기 정보보호제품 혁신대상 수상 / 2024년도 우수 정보보호 기술 등 지정

제 23-06563 호

상 장

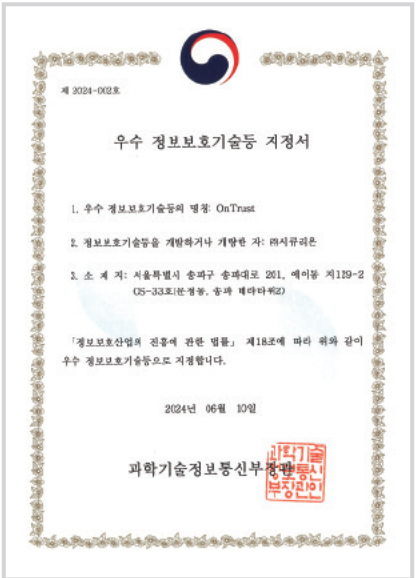
정보보안 부문
(제품명: OnTrust)

(주)시큐리온

귀사는 "2023년 하반기 정보보호제품 혁신대상"에서 위와 같이 입상하였으므로 이에 상장을 수여합니다.

2023년 12월 6일

과학기술정보통신부장관 이 종 호



제 2024-002호

우수 정보보호기술등 지정서

1. 우수 정보보호기술등의 명칭: OnTrust
2. 정보보호기술등을 개발하거나 개량한 자: ㈜시큐리온
3. 소 재 지: 서울특별시 송파구 송파대로 201, 에이동 지129-2 (05-33호(문정동, 송파 테라타워2)

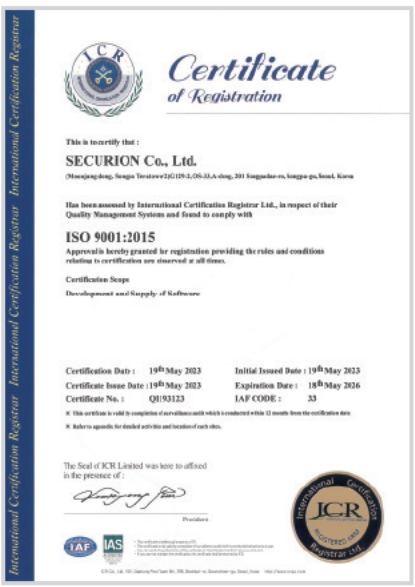
「정보보호산업의 진흥에 관한 법률」 제18조에 따라 위와 같이 우수 정보보호기술등으로 지정합니다.

2024년 06월 10일

과학기술정보통신부장관

시큐리온 품질경영시스템 ISO 9001 국제표준 인증 획득

- 2023년 06월 인증 획득
- 국제표준화기구(ISO)에서 제정, 시행하는 품질경영시스템에 관한 국제 규격
- 제품 및 서비스를 생산, 공급하는 과정에 대한 품질 보증 체계



International Certification Registrar

Certificate of Registration

This is to certify that :

SECURION Co., Ltd.

Has been assessed by International Certification Registrar Ltd., in respect of their Quality Management Systems and found to comply with

ISO 9001:2015

Approval is hereby granted for registration providing the rules and conditions relating to certification are observed at all times.

Certification Scope

Development and Supply of Software

Certification Date : 19th May 2023
Initial Issued Date : 19th May 2023
Certificate Issue Date : 19th May 2023
Expiration Date : 18th May 2026
Certificate No. : QI193123
IAF CODE : 33

The Seal of ICR Limited was here to affixed in the presence of :

President

IAF IAS

International Certification Registrar

Certificate of Registration

품질경영시스템 인증서

(주)시큐리온

ICR 은 상기업체의 품질경영시스템이 아래의 인증규격에 적합함을 인증합니다.

ISO 9001:2015

인증범위

소프트웨어 개발 및 공급

인증일자 : 2021년 05월 19일
최초 인증일 : 2023년 05월 19일
인증서 발행일 : 2023년 05월 19일
유효기간 : 2026년 05월 18일
인증서 번호 : QI193123
IAF 코드 : 33

The Seal of ICR Limited was here to affixed in the presence of :

President

IAF IAS

시큐리온 독자 개발 AI 탐지 시스템 적용 OnAV, AV-TEST 종합 탐지율 100%

최신 Android 멀웨어 공격으로부터 실시간 탐지 **100%**
*신·변종 악성 앱 탐지

지난 4주 동안 발견된 Android 멀웨어 탐지 **100%**
*알려진 악성 앱 탐지

Android: January 2024

Producer		Certified	Protection	Performance	Usability
SECURI ON	OnAV 1.0		6	6	6
Avast	Antivirus & Security 23.24		6	6	6
AVG	Antivirus Free 23.24		6	6	6
Avira	Antivirus Security 7.22		6	6	5
Bitdefender	Mobile Security 3.3		6	6	6
eset	Mobile Security 8.2		5.5	6	6
F-Secure	Total Security & VPN 22.0		6	6	6
G DATA	Mobile Security 27.10		6	6	6
Google	Play Protect 39.2		5.5	6	6
kaspersky	Plus for Android 11.109		6	6	6
McAfee	Mobile Security 7.9		6	6	6
norton	Norton 360 5.76		6	6	6
TOTAL AV	Total AV 3.0		5.5	6	5
PROTECTSTAR	Anti Spyware 6.0		5.5	6	3
SOPHOS	Intercept X for Mobile 9.7		6	6	6

Contact

SECURION

T. 02-575-3339
F. 02-575-3340
M. securion@securion.co.kr
A. 05854 서울시 송파구 송파대로201 송파테라타워2 A동 G129-2 OS33호

협력 문의
securion@securion.co.kr

기술 문의
support@securion.co.kr

데모 신청
demonstration@securion.co.kr

Link & Download

홈페이지 · SNS

시큐리온 홈페이지 | OnAV 홈페이지 | OnTrust 홈페이지 | 시큐리온 블로그 | 시큐리온 페이스북

회사 · 제품 소개서

시큐리온 회사소개서 | OnAV 제품소개서 | OnTrust 제품소개서 | OnAppScan 제품소개서 | OnTrust for Gooroom 제품소개서

SECURI ON (주) 시큐리온

05854 서울시 송파구 송파대로201 송파테라타워2 A동 G129-2 OS33호

Tel : 02-575-3339 | Fax : 02-575-3340 | Web : www.securion.co.kr | E-mail : securion@securion.co.kr