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 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 패치 또는 패턴 관리 시스템(PMS) 운영을 통해 적시에 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 관제 하는데도 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 업데이트용 PMS를 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 TMS를 제공하여 관제 효율성을 한 단계 높이고, 위협 발생 시 일사불란한 대응과 분석이 가능하도록 하였습니다.

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