Hanwha Techwin

White paper

Wisenet7
차별화된 사이버보안

2021 년 3 월 24 일

Contents

1. 배경 및 서론

최근 고도의 보안이 요구되는 구역에 설치된 영상감시 카메라에 접근, 실시간 영상 및 녹화 영상을 탈취하거나 위변조하는 해커들에 대한 우려가 높아지고 있습니다. 카메라 전문 제조업체들은 기본 설정값이거나 연속되는 문자와 숫자를 사용한 암호를 허용하지 않는 네트워크 설정 프로토콜을 도입하는 등 해킹의 위협에 대처하고 있습니다. 그럼에도 불구하고 해커들은 카메라의 '백도어'를 비롯한 다양한 방식으로 데이터 접근 방법을 모색할 것입니다.

범죄 및 악의적인 목적인지, 아마추어 해커가 실력 과시를 목적으로 해킹을 했는지에 관계없이 사용자의 민감한 데이터를 안전하게 보호하는 것은 중요합니다. 영상감시 솔루션에 자산, 인력, 부지의 보호를 의존하는 수천 개의 소형 업체뿐 아니라 강도높은 보안이 필수적인 공항, 은행, 지방자치단체, 정부, 군사, 응급의료 서비스 등도 마찬가지입니다.

한화테크윈은 이러한 환경에서 제품 보안 강화를 위해 끊임없이 노력해 왔습니다. 2020년에는 풍부한 보안 기능 및 기술을 집약한 한화테크윈의 자체 개발 SoC(System on Chip)인 Wisenet7을 장착한 제품을 선보였습니다.

첫째, 신규 적용한 하드웨어 보안 기능은 소프트웨어 보안의 한계를 극복했습니다. 보안 스토리지(Secure Storage)는 안전한 데이터 저장공간을 제공하고, 이를 바탕으로 보안 부팅, 보안 OS, 보안 JTAG 등 하드웨어 보안 기능을 확장했습니다.

둘째, End-to-end 보호의 궁극적인 목적은 통신내용을 엿듣거나 중요한 자료의 위변조를 위해 기기에 접근하여 민감한 정보를 취득, 위변조하는 비인가자를 차단하는 것입니다. 이를 위해서 기기 상호간 식별, 인증이 필요하고, 인증에 기반한 접근통제 및 허용, 암호화 로직을 사용한 시스템 및 데이터 보호가 요구됩니다.

셋째, 제품의 디자인 기능 및 설정 옵션을 결정하는 단계에서부터 보안을 최우선시하는 것이 중요합니다. 때때로 강도 높은 보안 기능을 구현하기 위해 제품의 성능이나 하위 호환성이 저하될 수 있습니다만, 보안의 중요성과 업계와 사회 생태계의 트렌드를 고려해보았을 때, 이는 불가피할 수밖에 없습니다.

위에서 언급한 신규 기능 및 기술 중 일부는 사이버공격의 차단을 위해 개발되었지만 일부는 칩셋의 효율성 증대를 위해 개발되어 제품의 보안을 강화한 경우도 있습니다.

본 백서는 사용자로 하여금 Wisenet7을 장착한 제품에 집약된 한화테크윈의 한 차원 높은 사이버보안 기술의 이해를 돕기 위해 작성되었습니다.

2.1. 하드웨어 보안

하드웨어 기반 보안 기술은 소프트웨어 기반 기술보다 보안 취약점을 더욱 잘 보호할 수 있어 제품의 보안 강화에 매우 중요합니다. 보안 하드웨어에서 파생된 보안 소프트웨어(신뢰점: root of trust)는 위변조가 더욱 어렵습니다. 한화테크윈은 Wisenet7 제품을 필두로 다음과 같은 네 가지 하드웨어 기반 보안 기술을 제품에 적용합니다.

2.1.1. 보안 부팅(Secure boot)

Wisenet7부터 보안 부팅을 지원합니다.

보안 부팅은 카메라 부팅 시 카메라에 작동하는 소프트웨어의 무결성을 검증하는 메커니즘으로, 외부 악성 코드 혹은 악성 소프트웨어에 의한 소프트웨어 위변조를 검사합니다.

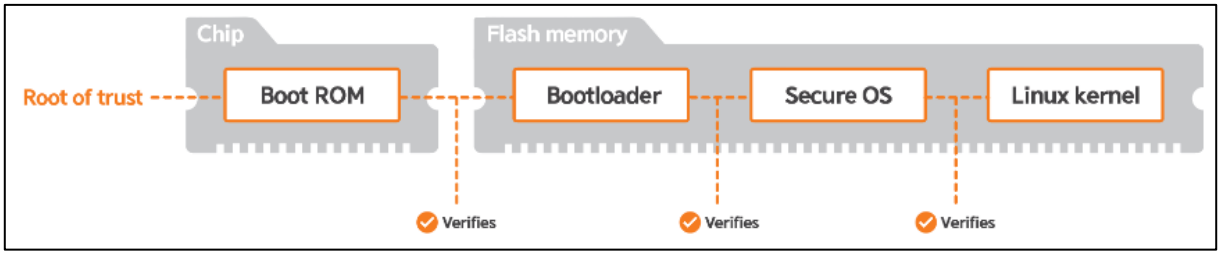

그림 1. Wisenet7 제품의 보안 부팅

2.1.2. 보안 스토리지(Secure Storage)

Wisenet7에는 안전한 하드웨어 모듈인 한화테크윈 보안 플랫폼 모듈(HTPM: Hanwha Trusted Platform Module)이 내장되어 있습니다. HTPM은 암호처리기(안전한 운영을 위한 마이크로 컨트롤러), 난수발생기, 보안 저장, 보안 OS 등으로 구성됩니다.

HTPM의 보안 스토리지는 OTPROM (One Time Programmable Read-Only Memory)과 EEPROM (Electrically Erasable Programmable Read-Only Memory: 전기 공급이 끊긴 상태에서도 장기간 기억하는 비휘발성 기억 장치)로 이뤄져 있고, 카메라의 중요 정보를 저장합니다. 신뢰점을 구축하는 중요한 정보는 제조단계에서 OTPROM에 삽입되고, 중요한 운영 정보는 EEPROM에 안전하게 저장됩니다.

2.1.3. 보안 OS(Secure OS)

별도의 보안 OS는 보안 스토리지에 저장된 중요한 정보를 안전하게 처리하기 위해 반드시 사용해야 합니다.

카메라 외부에서는 보안 OS에 접근이 불가합니다. 보안 OS나 보안 스토리지에 접근하기 위해서는 리눅스 OS를 통해 별도의 API를 사용해야 합니다. 또한 보안 OS는 독립된 암호화, 복호화를 지원하여, 메인 OS의 부하를 줄여주고 보안 OS에 사용된 애플리케이션은 위변조를 막기 위해 검증됩니다.

2.1.4. 보안 JTAG

JTAG 인터페이스를 통한 비인가 접근을 예방하는 가장 좋은 방법은 JTAG 기능을 해제하는 것입니다. 그러나 이는 곧 제품 개발 혹은 생산단계에서 칩이나 보드에 발생하는 장애의 원인을 파악할 수단 역시 제거됨을 의미합니다.

따라서 비밀키에 기반한 인증 메커니즘을 Wisenet7에 적용하여 JTAG를 안전하게 사용하면서도 강도 높은 보안을 달성할 수 있습니다.

인증키는 제조업체만 갖고 있으며 제조업체가 소유한 인증키는 고객의 정보가 아닌 제품의 시스템 관련 정보에만 접근을 허가합니다. 또한 제품 장애 발생시, 제조업체는 해당 인증키를 활용하여 원격이 아닌 로컬로만 원인 분석을 실행할 수 있어 비인가 사용자의 접근이 불가합니다.

2.2. End-to-End 보호

비밀번호를 통한 기존의 접근통제 외에도, 기기 상호인증을 위해 삽입한 기기 인증서를 활용하여 통신의 안전성을 높일 수 있습니다. 이러한 방식은 비인가 사용자의 통신 방해를 막을 수 있습니다. 또한 디지털 서명, 암호화를 도입하여, 데이터 저장 및 백업 시 End-to-End 데이터 보안을 강화하고, 펌웨어 업데이트 및 부팅 시에도 End-to-End 시스템 보안을 향상시킬 수 있습니다.

2.2.1. 기기 인증서(사전 설치)

한화테크윈은 탈레스(Thales) HSM 장치를 사용하여 각 기기(Wisenet7 제품 포함)의 인증서/개인키를 발행하고 제조과정에서 각 기기에 삽입합니다. 인증서를 생성할 때, 개인용 최상위 인증서 발급자(Root CA)로 디지털 서명을 하기 때문에 제조업체의 발급 사실을 증명할 수 있습니다. 인증서가 있으면 웹 브라우저에서 보안 경고 없이 안전한 통신이 가능하고, 인증서는 기기 인증을 실행하는 제품에서 확인 가능합니다.

2.2.2. 상호 인증(Mutual Authentication)

안전한 통신을 위한 상호 인증은 통신 보안의 기밀성, 무결성, 인증성을 확보하는 좋은 방법입니다. 한화테크윈의 Wisenet7 제품은 HTTPS(TLS 기반의 HTTP, HTTPS 기반의 RTSP) 통신을 사용하는 카메라 및 클라이언트 기기(저장장치 혹은 PC NVR 타입 SSM) 간의 상호 인증을 위해 클라이언트 인증을 지원합니다.

일반적으로 상호 인증은 사용자나 기기에서 실행할 수 있으나, 현재는 한화테크윈에서 생산한 기기 간에만 실행할 수 있습니다.

상호 인증에서 서버 역할을 하는 카메라의 인증은 서버 인증으로 불리며, 클라이언트 역할을 하는 기기의 인증은 클라이언트 인증이라 불립니다. 서버 인증은 클라이언트에서 실행되고, 클라이언트 인증은 서버에서 실행됩니다.

클라이언트 인증은 서버 인증을 전제로 한 옵션으로 제공되므로, 포괄적 의미로 클라이언트를 인증함으로써 상호 인증을 제공합니다.

2.2.3. 보안 연결고리(Chain of Trust) 검증

최상위 인증서 발급자(Root CA)가 발행한 인증서는 카메라의 신뢰점을 보장하기 위해 존재하며 인증서 체인은 최상위 인증서 발급자(Root CA)가 발행한 인증서로 검증합니다. Wisenet7 제품에는 두 종류의 최상위 인증서 발급자(Root CA)가 발행한 인증서가 있습니다. 하나는 기기 인증을 위한 최상위 인증서 발급자(Root CA)가 발행한 인증서이고, 다른 하나는 오픈 플랫폼 애플리케이션 용도의 인증서입니다.

기기 인증을 위한 최상위 인증서 발급자(Root CA)가 발행한 인증서는 카메라에 기기 인증서를 설치하거나 클라이언트 기기 인증서를 활용하여 클라이언트 인증을 실시할 때 사용합니다. 첫번째 용도는 기기 인증서를 카메라에 설치할 때 인증서 체인을 검증하여 제조업체의 승인 없는 인증서 설치를 막기 위함이 목적입니다. 두번째 용도는 클라이언트 기기의 인증서 체인을 검증하여 한화테크윈에서 제조한 신뢰 가능한 기기임을 상기시켜 줍니다.

오픈 플랫폼 애플리케이션용 최상위 인증서 발급자(Root CA)가 발행한 인증서 는 Wisenet7 오픈 플랫폼 애플리케이션 서명에 사용된 각기 다른 서명키와 인증서가 한화테크윈에서 생성, 배포되었음을 검증하여 비인가 애플리케이션의 설치를 막아줍니다.

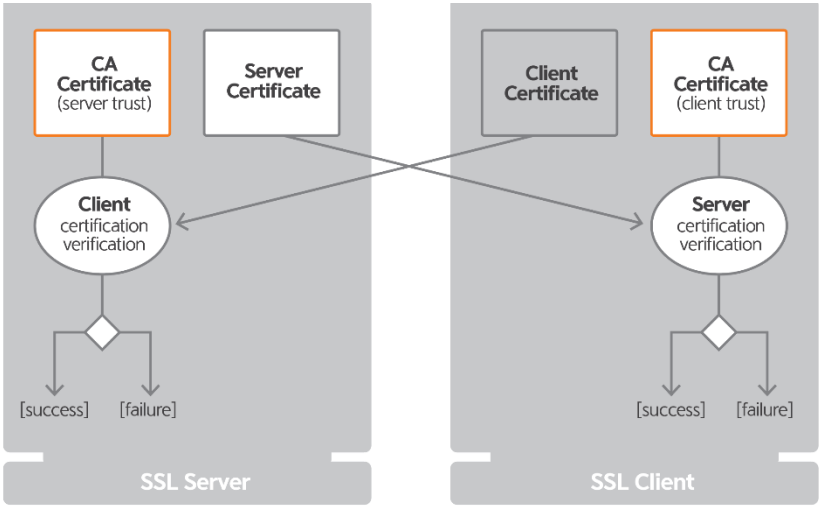

그림 2. 신뢰점 개념

2.2.4. 펌웨어 위변조 검증

한화테크윈의 서명된(Signed) 펌웨어 기술은 안전한 펌웨어 업데이트 방식입니다. 펌웨어에 디지털 서명을 포함하고 업데이트 시에 서명 값을 검증하여 사용자는 펌웨어가 위변조 되지 않았음을 신뢰할 수 있습니다.

펌웨어의 디지털 서명은 한화테크윈에서 안전하게 관리하는 키 서버를 통한 개인키로 생성되며, 디지털 서명을 검증하는 공개키는 Wisenet7의 보안 스토리지 구역(HTPM)에 안전하게 저장됩니다.

디지털 서명을 사용하면 단순 해시, 체크섬 등보다 펌웨어 무결성을 입증하고 보안을 강화하는 데 효과적입니다. 변조된 펌웨어의 해시나 체크섬은 쉽게 다시 계산될 수 있기 때문입니다.

2.2.5. 영상 이미지 암호화(대기 및 백업 시)

카메라에서 생성된 영상 이미지는 사용자의 중요한 정보로 다뤄야 합니다. 따라서, 영상 이미지 전송 시에는 안전한 통신을 사용해야 할 뿐 아니라, 외부 저장매체에 이미지를 저장하거나 카메라를 PC에 백업할 경우 반드시 보안 메커니즘을 적용해야 합니다.

Wisenet7 제품은 영상 이미지를 SD카드에 저장 시 파일시스템 암호화를 지원합니다. 파일 각각을 별개로 암호화하는 대신 파일 시스템을 암호화하여 영상 전송 및 재생 시 별도 해독을 위한 로딩이 없습니다. 또한 AES 암호화는 사용자가 설정한 비밀번호 세트를 사용해서 실행되기 때문에 SD카드를 도난 당하더라도 저장된 영상은 안전하게 보호합니다.

Wisenet7 제품은 백업 시 영상 암호화를 지원합니다. 카메라에 저장된 영상을 백업할 때나 PC의 실시간 영상을 수동으로 녹화할 때 ZIP파일을 암호화해서 영상을 보호합니다.

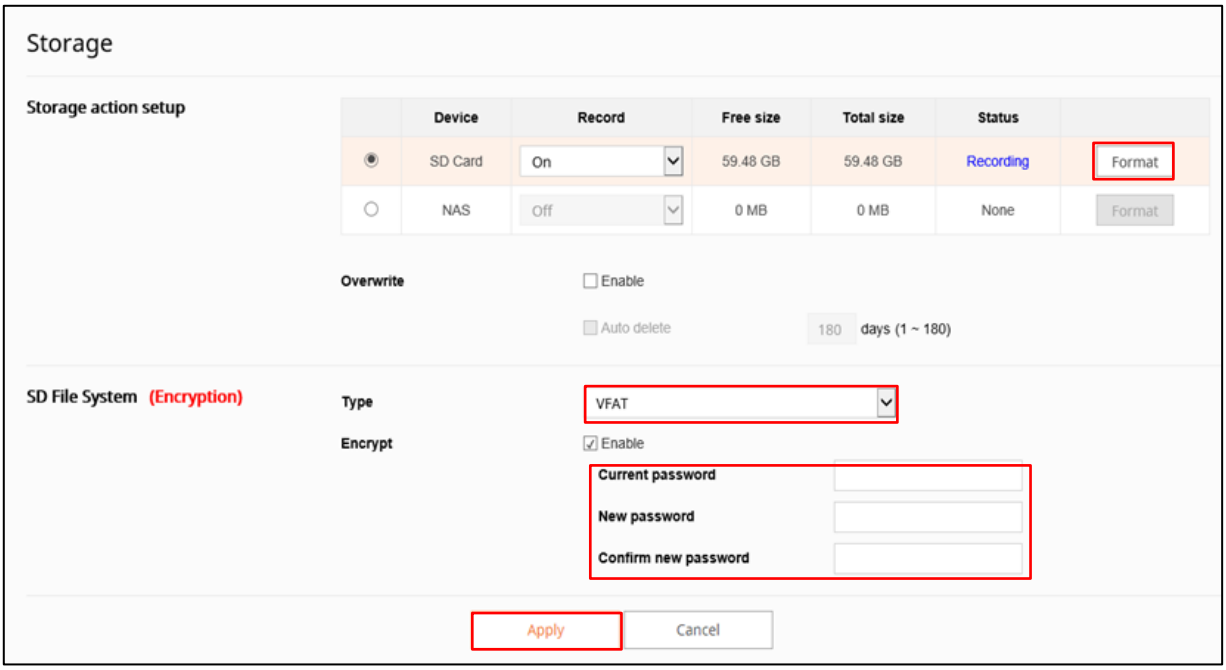

그림 3. SD 카드 암호화 UI

2.3. Secure by Default/Design

제조업체는 제품 개발 시에 시스템과 사용자의 민감한 정보의 기밀성, 무결성, 인증성을 확보하기 위해 보안 표준을 염두에 둬야 합니다. 제품의 설계단계부터 보안 표준을 반영하는 것이 중요하며, 이것을 “Secure by design(보안에 최적화된 설계)”라고 부릅니다.

“Secure by default(안전성을 보장하는 기본 설정)”는 기본 설정이 최고 보안수준으로 되어 있음을 의미하며, 가장 사용자 친화적이거나 하위 호환성을 지닌 설정은 아닐 수 있습니다. 따라서 사용자가 각 Secure by Default 설정에서 사용성 및 호환성에 적합한 설정 변경에 따른 보안 리스크를 분석할 필요가 있습니다.

2.3.1. 보안 설정의 강화

Wisenet7 제품은 박스에서 제품을 꺼내는 순간부터 높은 보안을 제공하도록 설계되어 있습니다. HTTPS 모드가 최초로 적용되면 SNMP (Simple Network Management Protocol: 간이 망 관리 프로토콜), Link-Local 주소, UPnP discovery, 그리고 Bonjour 등 불필요한 초기 서비스는 비활성화됩니다. SUNAPI / ONVIF도 초기에는 비활성화되어 있으나 사용자 비밀번호가 설정되면 활성화됩니다. 모든 한화테크윈의 제품은 초기에 설정된 기본 비밀번호 없이 출고됩니다.

제품 최초 설치 시 사용자는 Wisenet Device Manager를 통해 복잡한 비밀번호를 직접 설정해야만 합니다.

2.3.2. 최신 버전의 프로토콜을 적용

Wisenet7 제품은 한화테크윈 제품 최초로 TLS 1.3 버전을 채택합니다. Wisenet7 제품은 안전한 TLS 버전(1.2, 1.3)만을 지원합니다. TLS 1.2는 결점이 있음에도 불구하고 아직은 안전하고, 현재 가장 많이 채택되는 표준입니다. 특정 TLS 버전(1.0, 1.1)의 추가 옵션도 하위 호환성 등으로 인해 필요 시 지원하지만 보안 측면에서 권고하지 않습니다.

TLS 1.3 버전에서 가장 눈에 띄는 변화는 더욱 빨라진 실행력과 강화된 보안입니다.

2.3.3. 안전한 사이퍼 스위트(Cipher Suites) 제공

기존 TLS 모드에서는 일부 취약한 사이퍼 스위트도 호환성을 위해 제공했으나, Wisenet7 제품은 보안이 강화된 사이퍼 스위트를 초기에 제공하고 취약한 사이퍼 스위트는 호환성을 위해 옵션으로 제공합니다.

취약한 사이퍼란 길이가 부족한 키를 사용하는 암호화/복호화 알고리즘입니다. 암호화/복호화 알고리즘에서 불충분한 길이의 키를 사용하면 암호화 스키마가 부숴질(크래킹) 가능성(혹은 개연성)이 있습니다. 키의 길이가 길수록 암호는 더욱 강력합니다. 취약한 암호는 대개 128비트 미만(예를 들어 16바이트...1바이트는 8비트)의 키 사이즈를 사용하는 암호화/복호화 알고리즘으로 알려져 있습니다.

암호화 제도(Encryption scheme)에서 키 길이의 부족이 미치는 영향을 이해하기 위해서는 암호화 기법의 기본에 대한 배경지식이 필요합니다. 암호화 기법은 일반 정보(평문)를 암호화되어 알아들을 수 없는 말(암호문)로 전환하는 과정입니다. 이러한 전환 과정을 바로 암호화라고 부릅니다.

암호화 기법의 두번째 과정은 암호문을 평문으로 재구성하는 복호화입니다. 이 과정들(암호화/복호화)은 '키'로 통제됩니다. 키는 양측에서 통신하는 이들이 공유하는 비밀입니다. 키는 평문을 암호화하고 암호문을 복호화하기 위해 사용됩니다.

안전한 통신은 네 개의 기본 구성요소로 이뤄집니다. 즉, 교환할 정보에 사용할 암호화/복호화 알고리즘, 공유키 교환에 사용할 암호화/복호화 알고리즘, 인증 타입, 메시지 인증 코드입니다. 위 네 개의 요소 가운데 한가지 이상을 사용했다면 취약한 암호화 스위트로 분류될 수 있습니다.

그림 4. TLS 설정 옵션

3. 보안 체크 리스트

카메라의 사이버보안을 한층 더 강화하기 위해서는 여러 단계의 보안 장치를 도입하는 것을 권장합니다. 이를 통해 한 단계의 보안이 뚫리더라도, 다른 보안 장치가 정상적으로 작동하여 보안 네트워크 및 장비를 보호할 수 있습니다. 또한, IT, 영상 보안, 시스템 설치 업자, 그리고 최종 이용자가 함께 협업하여 전체 시스템의 보안 요구사항과 보안 기능에 대한 각자의 책임과 의무를 명확히 하는 것이 좋습니다. 다음은 보안 네트워크 설치 시 도입할 수 있는 사이버보안 관련 기능 리스트입니다.

- 최소한의 권한만 부여된 사용자 단계의 계정 생성
- 게스트 계정이나 인증없이 RTSP (Real-Time Streaming Protocol) 접근 가능한 기능 비활성화
- 정기적 암호 변경 & 시스템별 다른 암호 사용
- 시스템 표준 시간대 업데이트/NTP (Network Time Protocol), DST (Daylight Saving Time), 표준 시간대
- 802.1x 인증서 기반 접속 컨트롤 활성화
- 꼭 필요한 경우에만 멀티캐스트(Multicast) 활성화
- 꼭 필요한 경우에만 DDNS (Dynamic Domain Name System) 활성화
- 꼭 필요한 경우에만 Bonjour 활성화
- 꼭 필요한 경우에만 UPnP (Universal Plug and Play) 활성화
- 꼭 필요한 경우에만 link-local 주소 활성화
- 꼭 필요한 경우에만 FTP (File Transfer Protocol) 활성화
- 꼭 필요한 경우에만 SNMP (Simple Network Management Protocol) v3로만 사용
- 이메일을 사용할 때 보안이 적용된 SMTP (Simple Mail Transfer Protocol) 사용
- 꼭 필요한 경우에만 QoS 활성화
- 네트워크 환경에서 VLAN 활성화
- 카메라를 사람의 손이 닿지 않는 곳에 설치, 케이블을 확실하게 보호
- 기본 포트를 널리 사용되는 포트에서 유추하기 어려운 높은 수를 갖는 포트로 변경
- IP 필터링 활성화

- 기업 혹은 생산 네트워크나 인터넷과는 별개의 네트워크에 카메라 설치
- VMS (Video Monitoring System) 또는 네트워크에 문제 발생 시 백업 목적의 SD 카드 저장 활성화
- 문서 환경 설정과 문서 내보내기/백업 생성
- 카메라 화면 스냅샷 저장
- 템퍼링/초기화 등의 변화를 쉽게 파악할 수 있게 설정
- 원격 접속 시 VPN 혹은 보안된 클라우드 활용
- SD카드 저장 및 비디오 내보내기 기능 사용 시 범용이 아닌 한화테크윈 자체 비디오 파일 형식 사용
- 무정전 전원 공급장치 활용 네트워크 스위치, NVR/VMS, 그리고 PoE 미드스펜/인젝터 보호
- 템퍼링, 디포커스 탐지 분석 기능 활성화
- 저전력 상황에서의 네트워크 연결 종료 탐지 기능 활성화
- 장비에 기록된 로그를 정기적으로 점검

4. 결론

Wisenet7은 보안 부팅/보안 OS/보안 스토리지, 서명된 펌웨어/오픈 플랫폼 앱, 보안 JTAG 등을 활용, 업계 최고 수준의 사이버보안 정책을 지원하고 End-to-End 사이버보안을 제공합니다. 한화테크윈은 자체적인 기기 인증 발행 시스템을 도입하여 제품 개발단계에서 제조단계에 이르기까지 인증서를 제품에 삽입하고 있습니다. Wisenet7의 향상된 사이버보안 기능을 통해 사용자는 더욱 안전한 보안 솔루션을 구축할 수 있게 되었습니다.

WISENET

Hanwha Techwin Co.,Ltd.

13488 경기도 성남시 분당구 판교로 319 번길 6

한화테크윈 R&D 센터

TEL 1588.5772

http://hanwha-security.com

Hanwha Techwin