element

SECURITY PATTERN

자산 식별 가이드

사이버보안 평가

EN 18031-1, EN 18031-2, EN 18031-3

elementkorea.kr

Making tomorrow **safer than today.**

CONNECTED TECHNOLOGIES

CONTENTS

서론

EN 18031-X 시리즈 표준은 일련의 결정 트리(Decision tree)를 중심으로 작성되어 있으며, 이론적으로는 사이버보안 제품 평가 경험 수준과 관계없이 시험 기관과 제조사 모두가 평가 절차를 매우 수월하게 진행하실 수 있도록 설계되어 있습니다. 그러나 이러한 결정 트리의 대다수는 '각각의 ...에 대하여(For each...)'라는 문구로 시작하기 때문에, 평가 절차의 첫 단계는 이러한 각 문구에 해당하는 항목 목록을 작성하는 것이며, 이 목록의 각 항목 조합에 대해 결정 트리를 적용해 나가야 합니다.

일부 경우에는 이 작업이 간단합니다. 예를 들어 '각각의 외부 인터페이스에 대하여'라는 문구는 이해하기 쉬우므로 목록을 작성하는 것도 어렵지 않습니다. 그러나 그렇지 않은 경우도 있습니다. 특히 '각각의 네트워크 자산에 대하여'라는 문구는 제품 사이버보안에 익숙하지 않은 분들에게는 상당히 까다롭게 느껴질 수 있습니다. "네트워크 자산이란 도대체 무엇인가?"라는 의문이 드실 수 있습니다.

안타깝게도 이들 표준 중 하나 이상을 기준으로 제품을 평가하고자 하시는 분들께 이 질문에 대한 답은 복잡하며, 세 개의 표준이 아래 항목들을 서로 조금씩 다르게 조합하여 요구하기 때문에 더욱 복잡해집니다.

- 보안 자산(Security assets)
- 네트워크 자산(Network assets)
- 개인정보 자산(Privacy assets)
- 금융 자산(Financial assets)

그렇다면 각 표준에서 위 항목들의 정의를 찾기만 하면 되는 단순한 문제로 보일 수 있습니다. 그러나 실제로는 결코 그렇게 간단하지 않습니다. 위 각 항목의 정의는 서로 다른 여러 정의를 다시 참조하며(그리고 표준 간에도 미묘하게 다릅니다), EN 18031-1 표준의 정의에 관한 도식은 4페이지를 참고해 주시기 바랍니다.

EN 18031-2 표준의 정의는 EN 18031-1보다 더 복잡하며, EN 18031-3의 정의는 한층 더 혼란스러워서 보안 자산과 보안 기능 간에 순환 참조까지 포함되어 있습니다. 해당 도식은 다음 페이지들을 참고해 주시기 바랍니다.

이러한 혼란을 해소하고자, 본 가이드에서는 제조사가 자사 제품이 보유한 모든 관련 자산을 명확히 식별하실 수 있도록 돕는 간단한 절차를 제시하고자 합니다.

자산 식별

제조사는 자사 장비가 보유한 다양한 자산을 식별하는 작업을 어떻게 시작해야 할까요? 이어지는 도식의 왼쪽에서 출발하여 "제품이 어떤 자산을 보유하고 있는가?"라고 묻기보다는, 오른쪽에서 출발하여 "제품이 어떤 기능을 보유하고 있는가?"(그리고 EN 18031-2와 EN 18031-3의 경우에는 "제품이 어떤 개인정보와 금융 데이터를 처리하는가?")라고 묻는 방식이 더 수월할 수 있습니다.

이는 사실상 하향식(Top-down) 접근 방식으로, 제품이 수행하는 모든 것에서 출발하여 역으로 관련 자산을 판별해 나가는 방법입니다. 아래에서는 각 표준별로 이 절차를 네 개의 간단한 단계로 나누어 설명해 드립니다.

EN 18031-1

EN 18031-1의 자산 정의는 모두 궁극적으로 **네트워크 기능(Network function)** 또는 **보안 기능(Security function)**을 가리키며, 따라서 절차는 아래와 같습니다. 정의 도식을 함께 펼쳐 놓고 각 단계에서 오른쪽에서 왼쪽으로 화살표를 따라가며 읽으시면 이해에 도움이 되실 수 있습니다.

1단계

1단계는 제품의 모든 기능에 대한 종합 목록을 작성하는 것입니다.

2단계

2단계는 1단계 목록의 항목 중 네트워크[1] 자원을 제공하거나 활용하는 항목(이에 따라 네트워크 기능이자 네트워크 자산이 됨), 또는 네트워크나 그 기능을 훼손하거나 네트워크 자원을 오용하는 것을 방지하는 데 관련된 항목(이에 따라 보안 기능이자 보안 자산이 됨)을 판별하는 것입니다.

3단계

3단계는 이렇게 식별된 각 네트워크 기능 및 보안 기능이 의존하는 모든 보안 매개변수 및 네트워크 기능 설정값에 대한 종합 목록을 작성하는 것입니다.

4단계

4단계는 이러한 보안 매개변수 및 네트워크 기능 설정값 중 조작될 경우 네트워크나 그 기능을 훼손하거나 네트워크 자원을 오용할 수 있는 항목(이에 따라 민감(Sensitive) 보안 매개변수 또는 민감 네트워크 기능 설정값이 되며, 따라서 보안 자산 또는 네트워크 자산이 됨), 또는 유출될 경우 마찬가지의 결과를 초래할 수 있는 항목(이에 따라 기밀(Confidential) 보안 매개변수 또는 기밀 네트워크 기능 설정값이 되며, 따라서 보안 자산 또는 네트워크 자산이 됨)을 판별하는 것입니다.

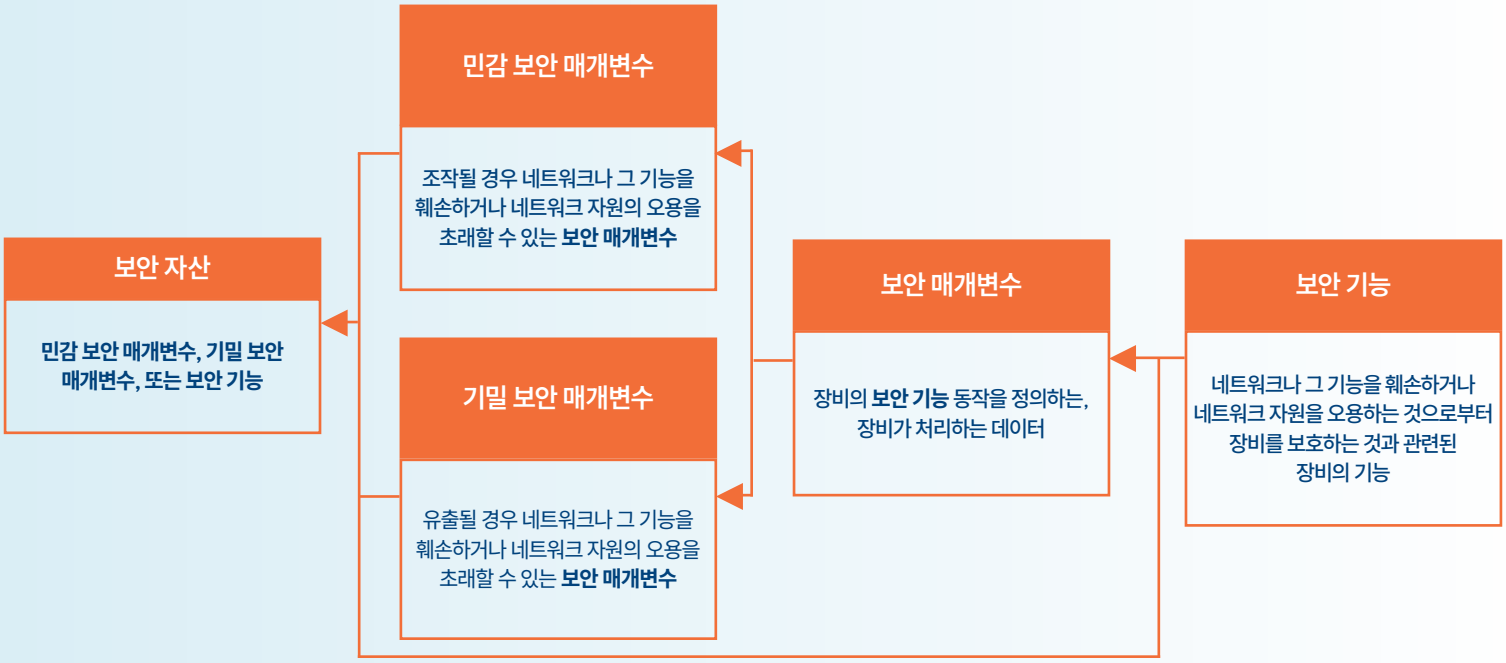
결과물

2단계와 4단계의 결과를 합산하면 해당 장비가 보유한 모든 네트워크 자산과 보안 자산의 완전한 목록이 완성됩니다.

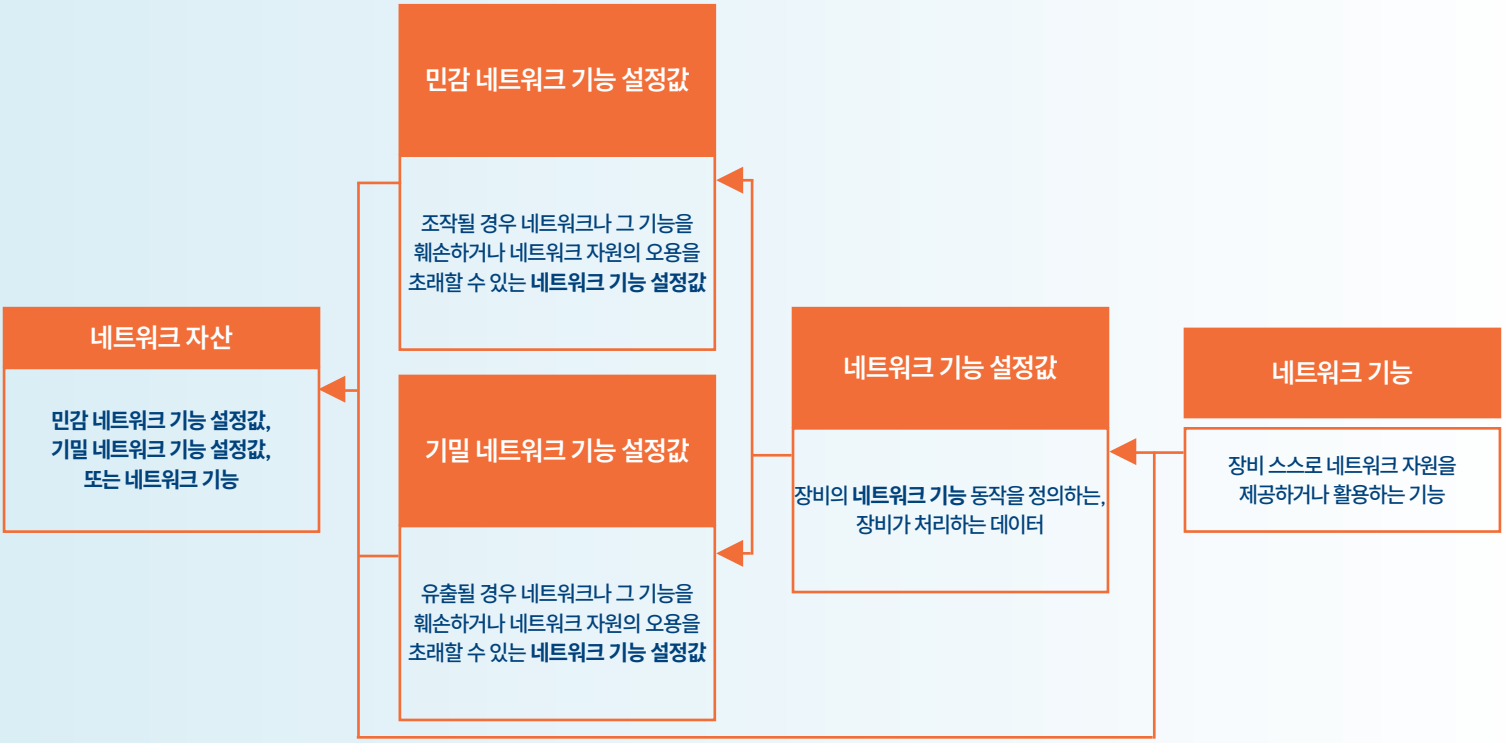
EN 18031-1 정의에 관한 참고사항

[1] 한 가지 유의하실 점은 '네트워크'가 무엇인지에 대한 명확한 정의가 없다는 것입니다. 일부에서는 네트워크란 두 개 이상의 장치를 연결할 수 있는 잠재력을 의미하므로, 시리얼 포트와 같은 인터페이스는 (항상 두 장치만 연결하므로) 네트워크 인터페이스에 해당하지 않는 반면 이더넷은 이에 해당한다고 주장하기도 합니다.

보안 자산


보안 자산
민감 보안 매개변수, 기밀 보안 매개변수, 또는 보안 기능
민감 보안 매개변수
조작될 경우 네트워크나 그 기능을 훼손하거나 네트워크 자원의 오용을 초래할 수 있는 보안 매개변수
기밀 보안 매개변수
유출될 경우 네트워크나 그 기능을 훼손하거나 네트워크 자원의 오용을 초래할 수 있는 보안 매개변수
보안 매개변수
장비의 보안 기능 동작을 정의하는, 장비가 처리하는 데이터
보안 기능
네트워크나 그 기능을 훼손하거나 네트워크 자원을 오용하는 것으로부터 장비를 보호하는 것과 관련된 장비의 기능

네트워크 자산


네트워크 자산
민감 네트워크 기능 설정값, 기밀 네트워크 기능 설정값, 또는 네트워크 기능
민감 네트워크 기능 설정값
조작될 경우 네트워크나 그 기능을 훼손하거나 네트워크 자원의 오용을 초래할 수 있는 네트워크 기능 설정값
기밀 네트워크 기능 설정값
유출될 경우 네트워크나 그 기능을 훼손하거나 네트워크 자원의 오용을 초래할 수 있는 네트워크 기능 설정값
네트워크 기능 설정값
장비의 네트워크 기능 동작을 정의하는, 장비가 처리하는 데이터
네트워크 기능
장비 스스로 네트워크 자원을 제공하거나 활용하는 기능

EN 18031-2

EN 18031-2의 자산 정의는 모두 궁극적으로 **개인정보(Personal Information)** 또는 **보안 기능(Security function)**을 가리키며, 따라서 절차는 위와 다소 차이가 있습니다. 이번에도 정의 도식을 함께 펼쳐 놓고 각 단계에서 오른쪽에서 왼쪽으로 화살표를 따라가며 읽으시면 이해에 도움이 되실 수 있습니다.

0단계

0단계(어떤 표준을 기준으로 평가를 시도하기 훨씬 이전에 이미 완료되어 있어야 할 작업이라는 의미에서 '0단계'라고 명명함)는 제품이 처리하는 모든 개인정보[2](즉, 개인 데이터, 트래픽 데이터, 위치 데이터)에 대한 종합 목록을 작성하고, 이 중 조작 또는 유출 시 이용자나 가입자의 개인정보 보호를 침해할 수 있는 항목을 식별(이에 따라 민감 개인정보 또는 기밀 개인정보가 되며, 따라서 개인정보 자산이 됨)하는 것입니다.

1단계

1단계는 위와 마찬가지로 제품의 모든 기능에 대한 종합 목록을 작성하는 것입니다.

2단계

2단계는 1단계 목록의 항목 중 개인정보를 처리하는 항목(이에 따라 개인정보 처리 기능(Privacy Function)이자 개인정보 자산이 되며, 이는 개인정보 자산에 해당하는 항목뿐 아니라 위에서 열거한 모든 개인정보를 포함함), 또는 이용자와 가입자의 개인 데이터 및 개인정보를 보호하는 항목(이에 따라 보안 기능이자 보안 자산이 됨)을 판별하는 것입니다.

3단계

3단계는 이렇게 식별된 각 개인정보 처리 기능 및 보안 기능이 의존하는 모든 보안 매개변수 및 개인정보 처리 기능 설정값에 대한 종합 목록을 작성하는 것입니다.

4단계

4단계는 이러한 보안 매개변수 및 개인정보 처리 기능 설정값 중 조작될 경우 이용자나 가입자의 개인정보 보호를 침해할 수 있는 항목(이에 따라 민감 보안 매개변수 또는 민감 개인정보 처리 기능 설정값이 되며, 따라서 보안 자산 또는 개인정보 자산이 됨), 또는 유출될 경우 마찬가지의 결과를 초래할 수 있는 항목(이에 따라 기밀 보안 매개변수 또는 기밀 개인정보 처리 기능 설정값이 되며, 따라서 보안 자산 또는 개인정보 자산이 됨)을 판별하는 것입니다.

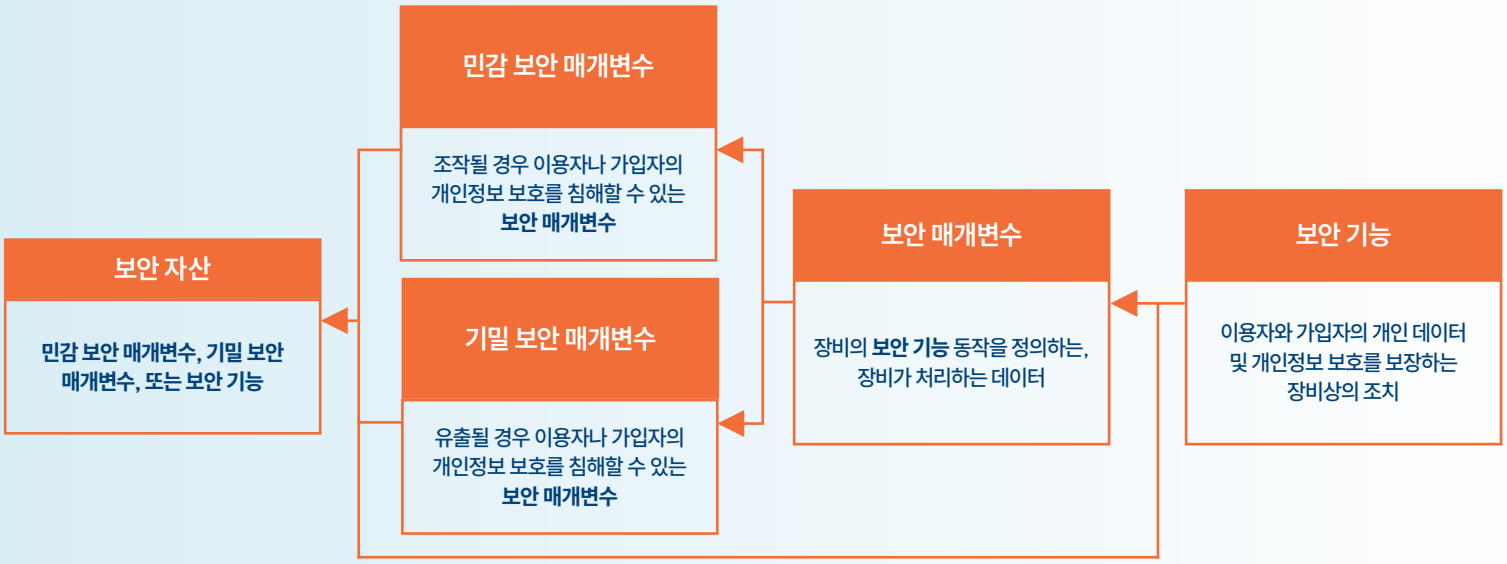
결과물

0단계, 2단계, 4단계의 결과를 합산하면 해당 장비가 보유한 모든 보안 자산과 개인정보 자산의 완전한 목록이 완성됩니다.

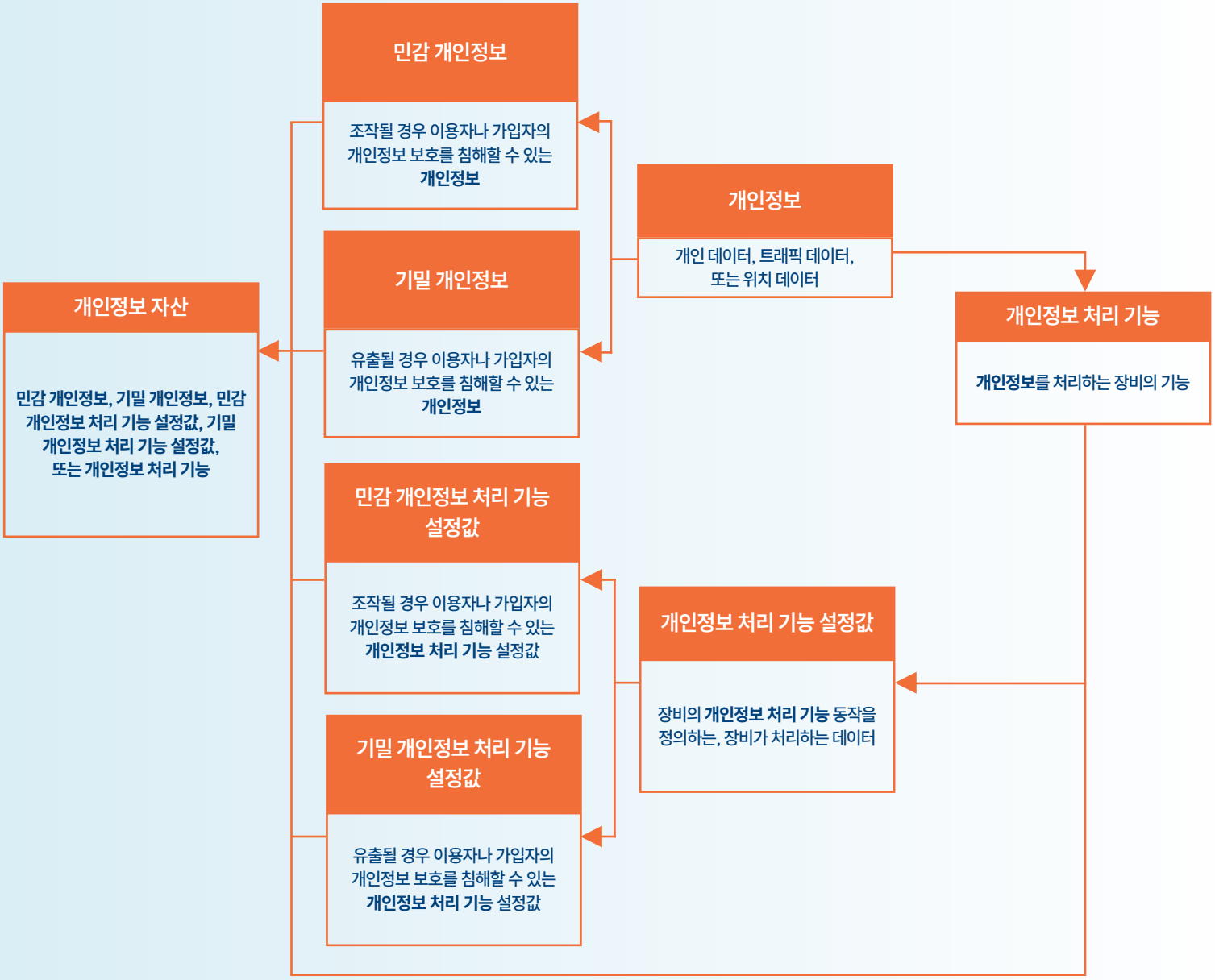
EN 18031-2 정의에 관한 참고사항

[2] 개인 데이터, 트래픽 데이터, 위치 데이터라는 용어는 본 표준에서 별도로 정의되어 있지 않으나, 규정(EU) 2016/679(일반 개인정보보호법, GDPR) 제4조 제1항, 또는 지침 2002/58/EC(전자통신 프라이버시 지침, 이른바 'ePrivacy 지침') 제2조 (b)호 및 (c)호에서 정의하고 있습니다.

보안 자산


민감 보안 매개변수
조작될 경우 이용자나 가입자의 개인정보 보호를 침해할 수 있는 **보안 매개변수**
기밀 보안 매개변수
유출될 경우 이용자나 가입자의 개인정보 보호를 침해할 수 있는 **보안 매개변수**
보안 매개변수
장비의 **보안 기능** 동작을 정의하는, 장비가 처리하는 데이터
보안 기능
이용자와 가입자의 개인 데이터 및 개인정보 보호를 보장하는 장비상의 조치
보안 자산
민감 보안 매개변수, 기밀 보안 매개변수, 또는 보안 기능

개인정보 자산


민감 개인정보
조작될 경우 이용자나 가입자의 개인정보 보호를 침해할 수 있는 **개인정보**
기밀 개인정보
유출될 경우 이용자나 가입자의 개인정보 보호를 침해할 수 있는 **개인정보**
개인정보
개인 데이터, 트래픽 데이터, 또는 위치 데이터
개인정보 처리 기능
개인정보를 처리하는 장비의 기능
개인정보 자산
민감 개인정보, 기밀 개인정보, 민감 개인정보 처리 기능 설정값, 기밀 개인정보 처리 기능 설정값, 또는 개인정보 처리 기능
민감 개인정보 처리 기능 설정값
조작될 경우 이용자나 가입자의 개인정보 보호를 침해할 수 있는 **개인정보 처리 기능** 설정값
기밀 개인정보 처리 기능 설정값
유출될 경우 이용자나 가입자의 개인정보 보호를 침해할 수 있는 **개인정보 처리 기능** 설정값
개인정보 처리 기능 설정값
장비의 **개인정보 처리 기능** 동작을 정의하는, 장비가 처리하는 데이터

EN 18031-3

EN 18031-3의 자산 정의는 모두 궁극적으로 **금융 정보(Financial Information)** 또는 **보안 기능(Security function)**을 가리키며, 따라서 절차는 위 내용과 유사합니다. 이번에도 정의 도식을 함께 펼쳐 놓고 각 단계에서 오른쪽에서 왼쪽으로 화살표를 따라가며 읽으시면 이해에 도움이 되실 수 있습니다.

0단계

0단계(어떤 표준을 기준으로 평가를 시도하기 훨씬 이전에 이미 완료되어 있어야 할 작업이라는 의미에서 '0단계'라고 명명함)는 제품이 처리하는 모든 금융 데이터에 대한 종합 목록을 작성하고, 이 중 조작 또는 유출 시 사기(fraud)로 이어질 수 있는 항목을 식별(이에 따라 민감 금융 데이터 또는 기밀 금융 데이터가 되며, 따라서 금융 자산이 됨)하는 것입니다.

1단계

1단계는 위와 마찬가지로 제품의 모든 기능에 대한 종합 목록을 작성하는 것입니다.

2단계

2단계는 1단계 목록의 항목 중 금융 데이터를 처리하는 항목(이에 따라 금융 기능(Financial Function)이자 금융 자산이 되며, 이는 금융 자산에 해당하는 항목뿐 아니라 위에서 열거한 모든 금융 데이터를 포함함), 또는 사기로부터 보호[3]하는 항목(이에 따라 보안 기능이자 보안 자산이 됨)을 판별하는 것입니다.

3단계

3단계는 이렇게 식별된 각 금융 기능 및 보안 기능이 의존하는 모든 보안 매개변수 및 금융 기능 설정값에 대한 종합 목록을 작성하는 것입니다.

4단계

4단계는 이러한 보안 매개변수 및 금융 기능 설정값 중 조작 또는 무단 변경될 경우 사기로 이어질 수 있는 항목(이에 따라 민감 보안 매개변수 또는 민감 금융 기능 설정값이 되며, 따라서 보안 자산 또는 금융 자산이 됨), 또는 유출될 경우 마찬가지의 결과를 초래할 수 있는 항목(이에 따라 기밀 보안 매개변수 또는 기밀 금융 기능 설정값이 되며, 따라서 보안 자산 또는 금융 자산이 됨)을 판별하는 것입니다.

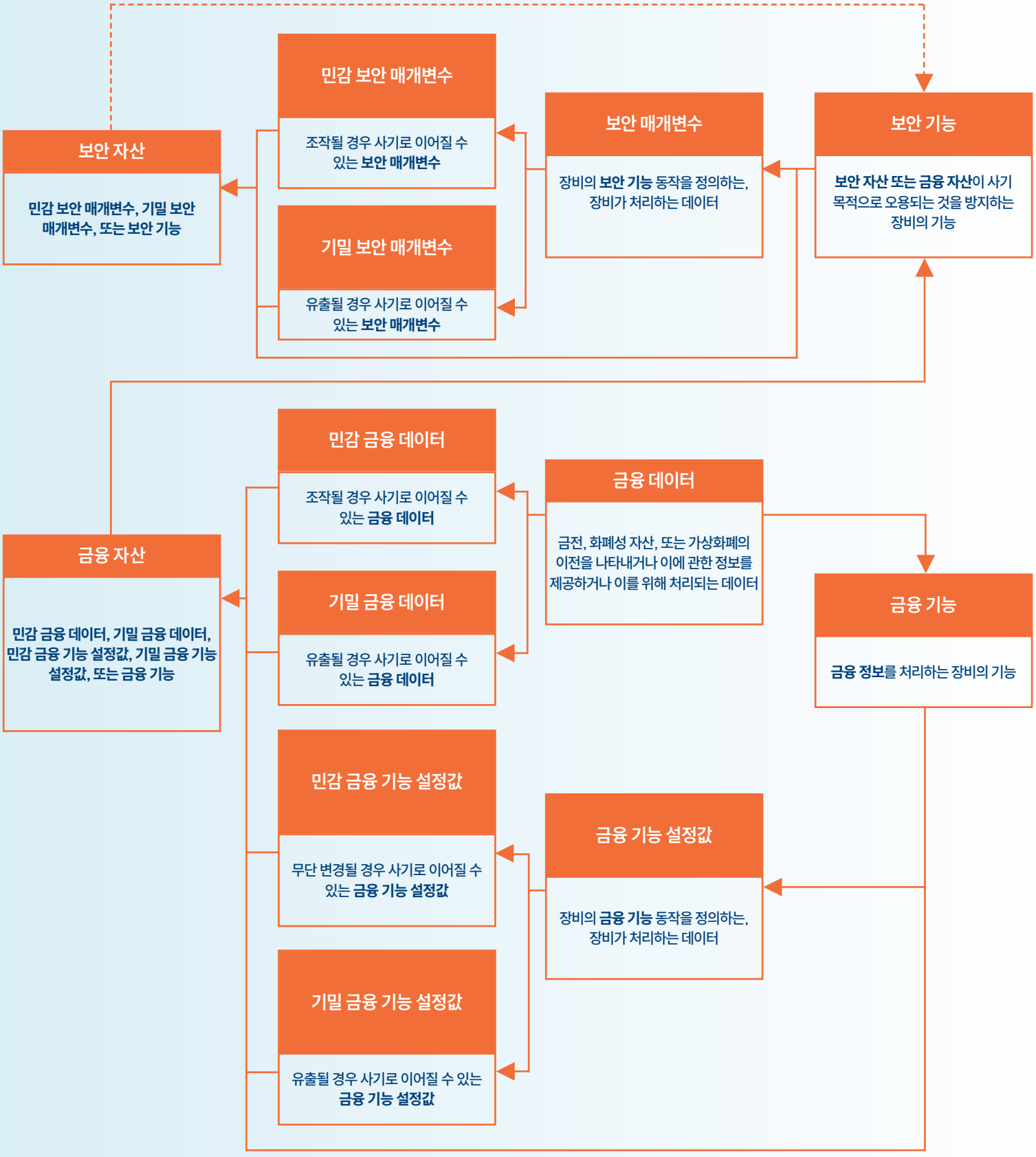
결과물

0단계, 2단계, 4단계의 결과를 합산하면 해당 장비가 보유한 모든 보안 자산과 금융 자산의 완전한 목록이 완성됩니다.

EN 18031-3 정의에 관한 참고사항

[3] 보안 기능의 정의에는 보안 자산(모든 보안 기능을 포함하는 개념)을 다시 참조하는 순환 참조가 존재합니다. 실무적으로는 이를 (다른 보안 자산이 아닌) 금융 자산이 오용되는 것을 방지하는 기능으로 단순하게 해석하시는 것이 합리적인 해결책입니다.

보안 및 금융 자산


보안 자산
민감 보안 매개변수, 기밀 보안 매개변수, 또는 보안 기능
민감 보안 매개변수
조작될 경우 사기로 이어질 수 있는 보안 매개변수
기밀 보안 매개변수
유출될 경우 사기로 이어질 수 있는 보안 매개변수
보안 매개변수
장비의 보안 기능 동작을 정의하는, 장비가 처리하는 데이터
보안 기능
보안 자산 또는 금융 자산이 사기 목적으로 오용되는 것을 방지하는 장비의 기능
금융 자산
민감 금융 데이터, 기밀 금융 데이터, 민감 금융 기능 설정값, 기밀 금융 기능 설정값, 또는 금융 기능
민감 금융 데이터
조작될 경우 사기로 이어질 수 있는 금융 데이터
기밀 금융 데이터
유출될 경우 사기로 이어질 수 있는 금융 데이터
금융 데이터
금전, 화폐성 자산, 또는 가상화폐의 이전을 나타내거나 이에 관한 정보를 제공하거나 이를 위해 처리되는 데이터
금융 기능
금융 정보를 처리하는 장비의 기능
민감 금융 기능 설정값
무단 변경될 경우 사기로 이어질 수 있는 금융 기능 설정값
기밀 금융 기능 설정값
유출될 경우 사기로 이어질 수 있는 금융 기능 설정값
금융 기능 설정값
장비의 금융 기능 동작을 정의하는, 장비가 처리하는 데이터

실전 예제 1 - IOT 센서

원격지에 설치되어 온도와 대기질을 감지하고 이를 셀룰러 통신망을 통해 백엔드 서버로 전송하는 간단한 IoT 환경 센서를 예로 들어보겠습니다. 이 예제에서는 해당 장치가 개인정보나 금융 정보를 전혀 처리하지 않으므로 EN 18031-1만 적용됩니다.

EN 18031-1에 대해 앞서 제시해 드린 방법을 적용해 보면 다음과 같습니다.

1단계

1단계는 모든 기능을 나열하는 것입니다.

2단계

2단계는 이들 기능 중 네트워크 기능 또는 보안 기능에 해당하는 것을 판별하는 것입니다.

1단계	2단계
모든 기능 나열	**네트워크 기능 또는 보안 기능 여부**
온도 감지	아니오
대기질 감지	아니오
셀룰러 연결	네(네트워크 기능)
데이터 처리	아니오

이를 통해 이 기준을 충족하는 기능이 하나뿐임을 확인할 수 있습니다.

이 기능(셀룰러 연결)이 첫 번째 자산입니다. 나머지 기능들은 네트워크 기능 또는 보안 기능의 정의를 충족하지 않으므로 제외합니다.

3단계

3단계는 이 기능이 의존하는 모든 설정값을 나열하는 것입니다.

4단계

4단계는 이들 중 기밀이거나 민감한 항목(즉, 유출 또는 조작될 경우 네트워크나 그 기능을 훼손하거나 네트워크 자원의 오용을 초래할 수 있는 항목)을 판별하는 것입니다. 이 예제에서는 관련 기능이 셀룰러 연결 하나뿐이므로 이 단계를 한 번만 거치면 됩니다. 더 복잡한 장치의 경우 위에서 식별한 각 기능에 대해 이 단계들을 반복하셔야 합니다.

이 예제에서 셀룰러 연결은 IMSI, IMEI, 그리고 SIM에 저장된 비밀 키에 의존합니다. IMSI와 IMEI는 유출되어도(공개되어도 위험이 없음) 기밀에 해당하지 않으며 조작되어도(조작해도 위험이 없음) 민감하지 않지만, SIM 비밀 키는 유출 시 네트워크 자원의 오용으로 이어질 수 있으므로 기밀에 해당합니다.

3단계	4단계
모든 설정값 또는 매개변수 나열	**민감 또는 기밀 여부**
셀룰러 IMSI	아니오
셀룰러 IMEI	아니오
SIM 비밀 키	예 (기밀)

결과물

2단계와 4단계의 결과를 결합하면 이 장치의 네트워크 자산 및 보안 자산에 대한 완전한 목록이 완성됩니다.

1. 셀룰러 연결 (네트워크 기능)
2. SIM 비밀 키 (기밀 네트워크 기능 설정값)

실전 예제 2 – 근태 관리 단말기

이번에는 좀 더 복잡한 장치로, 공장에서 사용되는 출퇴근 기록 시스템을 살펴보겠습니다. 이 장치는 건물의 출입구에 설치되며, 이용자는 RFID 태그나 지문을 이용해 출입을 기록할 수 있습니다. 이 장치는 백홀(Backhaul)용으로 이더넷 연결(TLS 사용)을 갖추고 있으며, 관리자 로그인을 통해 데이터를 내보낼 수 있는 USB 포트도 있습니다. 이 예제에서는 EN 18031-1과 EN 18031-2가 모두 관련되지만 EN 18031-3은 해당되지 않습니다.

위에서 설명해 드린 절차를 따르면 다음과 같습니다.

0단계

0단계는 모든 개인정보를 식별하는 것입니다. 여기에는 이름, 주소, 지문 등이 포함될 수 있으나, 단순화를 위해 이를 모두 묶어 "개인 데이터"라고 부르겠습니다.

실무적으로는 각 데이터 항목이 동일한 방식으로 처리되는 한 이러한 접근 방식이 허용됩니다. 예를 들어 이름과 주소가 지문과 별도로 저장되거나 전송된다면 이들은 별개의 자산으로 간주하셔야 합니다.

0단계	
모든 개인정보 나열	**이 정보가 민감 또는 기밀에 해당하는가?**
개인 데이터	예 (기밀)

1단계

1단계는 장치의 모든 기능을 나열하는 것입니다.

2단계

2단계는 이들 기능 중 네트워크 기능, 개인정보 처리 기능, 또는 보안 기능에 해당하는 것을 판별하는 것입니다(두 표준 간 보안 기능의 정의에 미묘한 차이가 있음에 유의해 주시기 바랍니다).

1단계	2단계
모든 기능 나열	**네트워크/개인정보 처리 /보안 기능 여부**
지문 인식	예 (개인정보 처리 기능)
RFID 인식	아니오
데이터 처리	예 (개인정보 처리 기능)
이더넷 연결	예 (네트워크 기능 및 보안 기능)
USB 연결	아니오
관리자 로그인 기능	예 (보안 기능)

이를 통해 네트워크 기능, 개인정보 처리 기능, 또는 보안 기능의 정의를 충족하여 자산이 되는 기능이 네 가지임을 확인할 수 있습니다. 이번 예제에서는 데이터 처리도 자산으로 간주되는데(이는 앞선 예제와 다른 점입니다), RFID를 통해서는 개인정보가 전송되지 않는다고 가정하지만 RFID를 사용하는 모든 장치에 이러한 가정이 항상 적용되는 것은 아니라는 점에 유의하시기 바랍니다. 이더넷 연결 기능은 네트워크 자원을 사용함과 동시에 데이터 보호와도 관련이 있으므로 네트워크 기능이자 보안 기능으로 간주됩니다.

3단계

3단계는 이 네 가지 기능이 의존하는 모든 설정값 또는 매개변수를 나열하는 것입니다.

4단계

4단계는 이들 설정값 또는 매개변수 중 기밀이거나 민감한 항목(즉, 유출 또는 조작될 경우 네트워크나 그 기능을 훼손하거나 네트워크 자원의 오용을 초래하거나 이용자나 가입자의 개인정보 보호를 침해할 수 있는 항목)을 판별하는 것입니다.

아래 표는 이해를 돕기 위해 구간별로 나누어 제시해 드렸습니다.

3단계	4단계
모든 설정값 또는 매개변수 나열	**이 정보가 민감 또는 기밀에 해당하는가?**
지문 인식	
해당 없음	해당 없음
데이터 처리	
해당 없음	해당 없음
이더넷 연결	
MAC 주소	아니오
TLS 키	예 (기밀)
관리자 로그인 기능	
관리자 사용자명	아니오
관리자 비밀번호	예 (기밀)

결과물

이 예제에서 두 가지 기능(지문 인식과 데이터 처리)은 별도의 매개변수나 설정값을 갖지 않습니다(적어도 언급할 만한 것은 없습니다 — 지문 인식기에 밝기나 타이밍 등의 설정이 있을 수 있으나 단순화를 위해 없다고 가정하겠습니다).

이더넷 연결은 MAC 주소와 TLS 키에 의존합니다. MAC 주소는 공개 정보로서 기밀도 민감도 아니지만, TLS 키는 유출될 경우 개인정보를 침해할 수 있으므로 기밀에 해당합니다.

마찬가지로 관리자 로그인 기능은 공개될 수 있는 사용자명과, 기밀에 해당하는 비밀번호에 의존합니다. 다만 이는 어디까지나 예시이며, 실제 장치에서는 비밀번호가 아닌 비밀번호 해시를 사용할 수 있는데, 이 경우 (반드시 유출로부터 보호할 필요는 없지만) 조작으로부터는 보호해야 하므로 기밀이 아닌 민감 항목이 될 수 있습니다.

0단계, 2단계, 4단계의 결과를 결합하면 이 장치의 네트워크, 개인정보, 보안 자산에 대한 완전한 목록이 완성됩니다.

1. 개인 데이터 (기밀 개인정보)
2. 지문 인식 (개인정보 처리 기능)
3. 데이터 처리 (개인정보 처리 기능)
4. 이더넷 연결 (네트워크 기능 및 보안 기능)
5. 관리자 로그인 기능 (보안 기능)
6. TLS 키 (기밀 보안 매개변수)
7. 관리자 비밀번호 (기밀 보안 매개변수)

저자 소개

Alex Toohie | Technical Solution Manager | Element

Alex는 10년 이상 규제 컴플라이언스 분야에서 활동해 왔으며, Element의 Connected Technology & Mobility 그룹뿐 아니라 무선 침입 및 화재 경보 시스템 분야의 글로벌 선도 기업에서 컴플라이언스 매니저로도 근무한 경력을 보유하고 있습니다.

Element의 Technical Solution Manager로서 Alex는 UKCA 및 CE 마킹(RED, EMCD, CPR, ATEXD, RoHSD 등), FCC 및 ISED, 그리고 계속 진화하는 글로벌 제품 사이버보안 요구사항에 대한 폭넓은 경험을 바탕으로, 복잡하고 다양한 무선 장비에 대해 제조사가 가장 효과적이고 비용 효율적인 인증 경로를 찾으실 수 있도록 지원하고 있습니다.

Filippo Melzani | CTO & Co-Founder | Security Pattern

Filippo는 성능, 풋프린트, 보안 측면에서 서로 다른 요구사항을 지닌 암호화 컴포넌트를 구축하는 데 폭넓은 경험을 쌓아 왔습니다.

그는 보안 요소가 시스템 내에서 최적의 방식으로 활용될 수 있도록 이를 결합하는 방법을 지속적으로 연구하고 있습니다. Filippo는 보안 기기 및 시스템의 개발과 평가를 지원하는 혁신적인 정형 방법론(Formal methodology)의 보급자이기도 합니다. 그는 12편의 학술 논문을 공동 저술하였으며, 여러 보안 관련 워크숍 및 콘퍼런스의 프로그램 위원회에 참여하고 있고, 보안 암호화 구현 분야에서 4건의 등록 특허를 보유하고 있습니다.

Arianna Gringiani | Security Expert | Security Pattern

Arianna는 암호학을 전공하며 수학 학위를 취득하였고, Security Pattern에서 Security Expert로서 커리어를 시작하였습니다.

그녀는 커넥티드 제품에 영향을 미치는 사이버보안 관련 법규(CRA, RED 포함)에 대한 규제 컴플라이언스를 중점적으로 다루어 왔으며, 제조사가 이러한 요구사항을 이해하고 적용하실 수 있도록 지원하고 있습니다. Arianna의 업무에는 IoT 기기에 대한 체계적인 보안 평가, 사이버보안 규제 관련 교육, 그리고 기술적·컴플라이언스 관점에서 제품 보안을 평가하는 방법론 개발이 포함됩니다.

ELEMENT의 강점

Element의 첨단 무선 시험 역량은 전파 스펙트럼 사용, EMC, 안전성, 상호운용성, 환경, 신뢰성, RF 노출, 사이버보안 등 다양한 분야를 아우릅니다.

시험 및 인증 분야의 선도적인 권위기관으로서, Element는 동적 주파수 선택(DFS), 무선 성능시험(OTA), 전자파 흡수율(SAR) 시험과 같은 전문 서비스를 제공하는 몇 안 되는 시험 기관 중 하나입니다.

Element는 ISO/IEC 17025:2017에 대해 UKAS 인정을 받았을 뿐 아니라, RED, EMCD, ATEX 지침에 대한 승인기관(Notified Body), 영국 무선·EMC·방폭 규정에 대한 승인기관(Approved Body), 그리고 IECEE CB Scheme에 따른 인증 기관이기도 합니다. Element의 전문가 팀은 주요 규제 및 자율 무선 인증 절차 전반을 지원하며, 여러 시장을 대상으로 한 시험 및 인증 프로그램을 프로젝트 단위로 관리함으로써 비용을 절감하고 인증 기간을 단축하실 수 있도록 돕고 있습니다.

Element의 시험 및 인증 서비스에 대해 더 자세히 알고 싶으시거나 전문가와 상담을 원하시면 지금 바로 문의해 주시기 바랍니다.

| 문의하기
| www.elementkorea.kr

SECURITY PATTERN: 고객이 얻는 혜택

Security Pattern은 다수의 기업이 EN 18031을 준수하도록 지원해 왔으며, 이 외에도 IEC 62443(산업용), IEC 81001(의료), ISO/SAE 21434(자동차), ETSI EN 303 645(소비자용 IoT) 등 다른 표준의 요구사항 준수도 지원해 왔습니다.

Security Pattern은 암호학 연구 커뮤니티 및 2건의 유럽연합 지원 프로젝트에 적극적으로 참여하고 있습니다. Security Pattern 소속 인력은 50편 이상의 학술 논문을 공동 저술하였으며, CEO인 Guido Bertoni는 NIST SHA-3 알고리즘의 공동 저자입니다.

각 기술팀 구성원은 마이크로컨트롤러, 스마트카드, 자동차, 무선 연결, ASIC 및 FPGA 분야의 보안 및 암호화 영역에서 다년간의 경험을 쌓아 왔습니다. Security Pattern은 최첨단 컨설팅, 제품, 교육을 제공함으로써 기기 제조사가 보안 및 비즈니스 목표를 달성하실 수 있도록 지원합니다.

Security Pattern은 기술 담당자, 매니저, 마케터, 고객의 요구를 경청하며, 고객의 모든 보안 요구를 충족할 수 있도록 패키지형 솔루션과 맞춤형 서비스를 함께 제공합니다.

| hello@securitypattern.com
| www.securitypattern.com

element

왜 엘레멘트를 선택해야 하나요?

엘레멘트 코리아는 컨슈머 커넥티드 기기와
인더스트리얼 솔루션 분야의 시험, 검사 및 인증
(TIC) 서비스를 선도하는 세계적인 기관입니다.

저희는 제품이 연결성(Connectivity), 상호 호환성
(Interoperability) 및 안전성(Safety)에 관한 국제 표준을
충족할 수 있도록 종합적인 시험 및 인증 서비스를 제공합니다.

문의하기

고객 문의

Telephone: 1551-9871 Web: elementkorea.kr

Making
tomorrow safer
than today.

CONNECTED
TECHNOLOGIES