ICS Scanner

제어설비 자동식별 및 관리 시스템

운영 지침서

제어시스템 현장에서 실제로 발생하는 16개 상황과

ICS Scanner의 기능 기반 해결 절차

Part A 보안 위협 상황 5건 · Part B 운영 업무 프로세스 6건 · Part C 고객 지원 5건

v1.0 · 2026. 8.

온시큐리티㈜

경기도 하남시 미사강변한강로 135 미사강변스카이폴리스 다동 1038~1039호 · TEL 031-792-0633

목 차

01 문서의 목적과 구성 3

02 ICS Scanner 기능 체계 4

Part A 보안 위협 상황 시나리오 5

A-01 정책에 없는 장비가 네트워크에 연결되어 있을 때 6

A-02 장비의 IP나 MAC이 지난 점검 이후 바뀌었을 때 7

A-03 허용되지 않은 서비스 포트가 사용되고 있을 때 8

A-04 예상하지 못한 통신 경로가 존재할 때 9

A-05 다른 장비가 수집한 트래픽을 검증해야 할 때 10

Part B 운영 업무 프로세스 시나리오 11

B-01 현장 점검을 준비할 때 12

B-02 현장에서 수집을 수행할 때 13

B-03 승인 장비 목록을 확정할 때 14

B-04 점검 결과를 문서로 제출할 때 15

B-05 주기 점검으로 변화를 추적할 때 16

B-06 점검 도구 자체를 관리할 때 17

Part C 문제 해결 시나리오 18

C-01 상시 시스템 적용의 한계 19

C-02 분리망의 관리 공백 20

C-03 도입 전 검증의 필요 21

C-04 점검 증적의 부재 22

C-05 적용 범위에 대한 불확실성 23

03 시나리오 – 기능 매핑 종합 24

04 도입 방식 및 지원 체계 25

01 문서의 목적과 구성

본 문서는 제어설비 자동식별 및 관리 시스템(ICS Scanner)이 상주 시스템을 설치할 수 없는 제어망 구간에서 어떤 문제를 어떤 방식으로 해결하는지를, 기능 단위가 아닌 상황 단위로 설명하기 위해 작성되었습니다.

제품 소개 자료가 「어떤 기능이 있는가」를 다룬다면, 본 문서는 「그 기능이 어떤 상황에서 무엇을 해결하는가」를 다룹니다. 각 시나리오는 상황 설명 → 기존 환경에서의 문제 → 해결 절차 → 기대 효과의 동일한 구조로 기술되며, 해결 절차의 모든 단계에는 실제 구현된 기능이 근거로 명시되어 있습니다.

▪ 문서의 구성

구분	주제	내용
Part A	보안 위협 상황	미승인 장비 발견, 장비 IP·MAC 변경, 블랙리스트 포트 사용, 예상 밖 통신 경로, 외부 PCAP 검증 — 5건
Part B	운영 업무 프로세스	점검 준비(스위치·정책), 현장 수집, 승인 목록 확정, 결과 리포트 발행, 주기 점검, 점검 도구 관리 — 6건
Part C	문제 해결	상시 시스템 적용 한계, 분리망 관리 공백, 도입 전 검증, 점검 증적 부재, 적용 범위 불확실 — 5건

▪ 기술 원칙

- 본 문서에 인용된 모든 기능은 ICS Scanner v1.0에 실제 구현되어 기능 리스트에 등재된 기능입니다.
- 해결 절차의 각 단계에는 「사용 기능」란에 근거 기능을 명시하여, 서술과 제품 사양이 일치함을 확인할 수 있도록 했습니다.
- 기능 참조는 2장의 기능 체계표에 정의된 F1~F7 코드를 따릅니다.

> **참고**
> 본 제품은 상시 관제 시스템이 아니라 휴대형 점검 도구입니다. 수집은 노트북을 스위치에 연결한 상태에서 이루어지며(분석은 연결 없이 수행 가능), 상시 모니터링이 필요한 구간에는 ICS Asset Manager 또는 ICS Security Monitor를 적용합니다.

02 ICS Scanner 기능 체계

시나리오 해결 절차에서 참조하는 기능 코드 체계입니다. 7개 대분류, 29개 중분류로 구성되며 총 194개의 세부 기능이 구현되어 있습니다.

코드	대분류	중분류	주요 세부 기능
F1	로그인	로그인 · 로그인 세션 만료	아이디·비밀번호 인증, 5회 실패 시 10분 차단, 라이선스 등록·초과 안내, 미사용 30분 세션 만료
F2	대시보드	대시보드 · 스위치 등록 · 수집 · 토폴로지 · 정책 확대보기	스위치 선택과 정책 조회, 수집 드라이버·수집 시간 지정, 수집 실행·중지·저장, 트래픽·디스크 표시, 통신 토폴로지 조회·검색·확대축소·이미지 내보내기
F3	정책 관리	스위치 · IP 정책 그룹 · PORT 정책	스위치 등록/수정과 기본 정책 조회, 단일 IP·네트워크 대역 정책 그룹 등록/수정/삭제, PORT 블랙리스트 정책 그룹 관리
F4	장비 관리	승인 장비 · 미승인 장비 · 장비 등록 · 장비 상세 · 장비 변경 이력 · 리포트 3종	스위치별 승인·미승인 장비 목록과 검색, 단일 장비 등록, 장비명·설명 관리, 미승인→승인 전환, IP/MAC 변경 이력, PDF 리포트 발행
F5	탐지 현황	PORT 탐지 · 통신 이력	블랙리스트 포트 탐지 목록·검색, 스위치 전체 통신 이력과 중복 제외 집계, 선택 행 기준 통신 토폴로지
F6	분석	분석 데이터 목록 · PCAP 업로드 · 불러온 PCAP 파일 데이터 분석 · 수집한 데이터로 분석 · 분석 결과 리포트	외부 PCAP 업로드와 제한 조건 안내, 주소 기준·포함/미포함·IP/대역/MAC/PORT/프로토콜 조건 설정, 분석 실행과 PDF 리포트
F7	설정	사용자 목록 · 사용자 정보 수정(사용자) · 환경설정 · 사용 가이드	사용자 등록/수정/삭제, 로그인 차단 해제, 본인 정보·비밀번호 수정, 디스크 임계치·파일 저장 위치 설정, 화면별 기능 설명

▪ 기능 계층 구조

계층	구성
산출	통신 토폴로지(F2) · 승인/미승인 장비 · 변경 이력 리포트(F4) · 분석 결과 리포트(F6)
분석	PCAP 업로드·조건 분석 · 수집 데이터 분석(F6) · 통신 이력(F5)
판별	IP 정책 그룹 · PORT 정책(F3) · PORT 탐지(F5) · 승인/미승인 판별(F4)
기반	스위치 등록 · 포트 미러링 수집(F2) · 장비 자동 식별과 변경 이력(F4)

하위 계층의 수집·식별 결과가 상위 계층의 분석·관제로 연결되는 구조이며, 모든 시나리오의 해결 절차는 이 흐름을 따릅니다.

Part A 보안 위협 상황 시나리오

독립·분리 네트워크 점검 현장에서 실제로 마주치는 5개 상황과, ICS Scanner가 이를 식별·판별·기록하는 절차입니다.

시나리오	상황	핵심 대응 기능
A-01	정책에 없는 장비가 네트워크에 연결되어 있을 때	F3 · F2 · F4
A-02	장비의 IP나 MAC이 지난 점검 이후 바뀌었을 때	F4
A-03	허용되지 않은 서비스 포트가 사용되고 있을 때	F3 · F5
A-04	예상하지 못한 통신 경로가 존재할 때	F5 · F2
A-05	다른 장비가 수집한 트래픽을 검증해야 할 때	F6

A-01 정책에 없는 장비가 네트워크에 연결되어 있을 때

> **상황**
> 태양광 발전 단지의 통신망을 점검하기 위해 스위치에 노트북을 연결해 수집했다. 사업소가 파악하고 있던 장비 수보다 많은 장비가 통신하고 있었다.

▪ 기존 환경에서의 문제

- 독립·분리 네트워크는 상주 보안 시스템이 없어 무엇이 연결되어 있는지 확인할 수단이 없다.
- 시공 이후 추가된 장비, 협력업체가 남겨둔 장비가 그대로 붙어 있어도 알 방법이 없다.
- 현장에 갈 때마다 장비를 조사하는 방식이라 결과가 담당자마다 다르다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**기준 설정**	IP 정책 그룹에 승인 대상 장비의 단일 IP와 네트워크 대역(A~C Class)을 등록하고, 스위치에 정책 그룹을 적용한다.	F3 IP 정책 그룹 · 스위치
2	**수집**	대시보드에서 스위치와 수집 드라이버를 선택하고 수집 시간을 지정해 수집을 실행한다.	F2 수집
3	**판별**	수집 결과가 IP 정책 기준으로 승인 장비와 미승인 장비로 자동 분류된다.	F4 승인 장비 · 미승인 장비
4	**확인**	미승인 장비 목록에서 스위치·장비명·IP·MAC·수집 일시를 조회하고 총 장비 수를 확인한다. IP·MAC·수집 일시로 검색한다.	F4 미승인 장비
5	**위치 파악**	토폴로지에서 승인(파란색)·미승인(노란색) 구분과 출발지→도착지 통신 방향을 확인하고, IP로 해당 장비를 검색한다.	F2 토폴로지
6	**기록**	미승인 장비 내역 리포트를 미리보기로 확인하고 PDF로 다운로드해 점검 결과로 제출한다.	F4 미승인 장비 내역 리포트

▪ 기대 효과

- 상주 설치 없이 노트북 연결만으로 수집 구간에서 통신한 장비가 목록화 된다.
- 「승인/미승인」이 정책 기준으로 자동 판별되어 담당자 판단이 개입하지 않는다.
- 결과가 PDF 리포트로 즉시 산출되어 현장에서 바로 공유할 수 있다.

A-02 장비의 IP 나 MAC 이 지난 점검 이후 바뀌었을 때

> **상황**
> 분기 점검에서 이전 회차와 장비 목록을 비교했더니 일부 장비의 IP가 달라져 있었다. 교체인지 재설정인지 현장에서는 판단이 되지 않는다.

▪ 기존 환경에서의 문제

- 점검 회차별 결과가 별도 파일로 남아 회차 간 비교를 사람이 수작업으로 한다.
- 무엇이 언제 바뀌었는지 시점이 남지 않아 변경 원인을 추적할 수 없다.
- 장비 교체 작업 기록과 대조하려 해도 비교 기준이 맞지 않는다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**자동 수집**	장비 정보를 자동 수집해 최초 식별 시점과 이후 IP/MAC 변경을 이력으로 관리한다.	F4 장비 변경 이력
2	**기간 조회**	장비 변경 이력에서 스위치를 선택하고 조회 기간을 지정한다.	F4 장비 변경 이력
3	**내역 확인**	날짜별 변경 이력에서 변경 타입·장비명·IP·신규 값·기존 값·변경 시간을 조회한다.	F4 장비 변경 이력
4	**개별 확인**	장비 상세에서 해당 장비의 IP·MAC·수집 일시와 변경 이력을 함께 조회한다.	F4 장비 상세
5	**식별 정보 보완**	장비명과 장비 설명을 등록·수정해 다음 점검 때 식별이 쉽도록 정리한다.	F4 장비 상세
6	**기록**	장비 변경 이력 리포트를 발행한다. 스위치와 작성 일자, 변경 사항·변경 내용·변경 일자가 포함된 PDF로 산출된다.	F4 장비 변경 이력 리포트

▪ 기대 효과

- 회차 간 비교가 수작업이 아니라 시스템의 변경 이력으로 대체된다.
- 변경 시점이 기록되어 작업 이력과 대조할 수 있다.
- 장비명·설명을 축적하면 점검을 반복할수록 식별 정확도가 올라간다.

A-03 허용되지 않은 서비스 포트가 사용되고 있을 때

> **상황**
> 점검 대상 구간에서 원격 관리용 포트가 열려 통신하고 있는 것으로 보인다. 어느 장비가 어떤 포트를 쓰는지 확인이 필요하다.

▪ 기존 환경에서의 문제

- 독립망은 방화벽이나 IPS가 없는 경우가 많아 포트 사용을 통제할 장치가 없다.
- 시공 편의를 위해 열어둔 관리 포트가 그대로 남아 있는 사례가 반복된다.
- 포트 사용 사실을 확인해도 근거 자료를 남길 방법이 없다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**정책 등록**	PORT 정책 그룹을 등록하고 허용하지 않는 포트를 블랙리스트로 지정한다. 하나의 그룹에 다수 조건을 등록한다.	F3 PORT 정책
2	**적용**	스위치 등록·수정에서 해당 PORT 정책 그룹을 스위치에 적용한다.	F3 스위치 · F2 스위치 등록
3	**탐지**	수집된 통신이 블랙리스트 포트에 해당하면 PORT 탐지 목록에 기록된다.	F5 PORT 탐지
4	**확인**	PORT 탐지에서 스위치를 선택하고 총 개수와 목록(정책명·출발지/도착지 IP·출발지/도착지 PORT·통신 일시)을 조회한다.	F5 PORT 탐지
5	**대상 검색**	출발지·도착지 IP와 PORT, 통신 일시로 검색해 특정 장비의 포트 사용 이력을 좁혀 확인한다.	F5 PORT 탐지
6	**교차 확인**	통신 이력에서 해당 장비의 프로토콜과 포트를 조회하고, 정책 확대보기로 스위치에 적용된 정책을 확인한다.	F5 통신 이력 · F2 정책 확대보기

▪ 기대 효과

- 차단 장치가 없는 구간에서도 포트 사용 현황이 데이터로 확인된다.
- 정책명 기준으로 탐지되어 「무엇을 위반했는가」가 명확하다.
- 점검 대상 포트를 정책으로 관리해 점검 기준이 회차마다 동일해진다.

A-04 예상하지 못한 통신 경로가 존재할 때

> **상황**
> CCTV망을 점검하던 중 CCTV 장비가 예상하지 않은 대역의 장비와 통신하고 있는 것이 확인되었다. 설계상 연결되지 않아야 하는 구간이다.

▪ 기존 환경에서의 문제

- 설계 도면상 분리되어 있어도 실제 배선과 설정은 다를 수 있다.
- 통신 상대를 확인하려면 패킷을 직접 봐야 하는데 현장에서는 도구가 없다.
- 연결이 있다는 사실을 보고하려 해도 시각적으로 설명할 자료가 없다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**이력 조회**	통신 이력에서 스위치를 선택해 출발지·도착지 IP와 MAC, PORT, 프로토콜 목록을 조회한다.	F5 통신 이력
2	**규모 파악**	중복을 제외한 출발지·도착지 IP·MAC 개수를 조회해 실제 통신 주체의 수를 확인한다.	F5 통신 이력
3	**경로 추적**	선택한 행의 출발지 IP 또는 도착지 IP를 도착지로 갖는 통신들의 토폴로지를 조회해 연결 관계를 확대한다.	F5 통신 이력
4	**전체 조망**	대시보드 토폴로지에서 모든 장비 보기와 확대·축소로 전체 통신 구조를 확인하고, 필요 시 전체화면으로 조회한다.	F2 토폴로지
5	**대상 확인**	IP로 장비를 검색하고 Rectangle selection 등 모드로 관심 구간만 선택해 확인한다.	F2 토폴로지
6	**자료화**	토폴로지 화면을 이미지로 내보내(Export image) 점검 보고 자료에 첨부한다.	F2 토폴로지

▪ 기대 효과

- 설계와 실제의 차이가 통신 데이터로 확인된다.
- 통신 경로가 토폴로지로 시각화되어 비전문가에게도 설명할 수 있다.
- 화면을 이미지로 내보내 보고 자료를 현장에서 바로 만든다.

A-05 다른 장비가 수집한 트래픽을 검증해야 할 때

> **상황**
> 이미 설치된 이기종 보안 장비가 수집한 PCAP 파일이 있다. 이 파일에 우려되는 통신이 실제로 담겨 있는지 확인해야 한다.

▪ 기존 환경에서의 문제

- 수집 장비와 분석 도구가 달라 파일을 받아도 분석할 수단이 없다.
- 범용 패킷 분석 도구는 조건 설정이 복잡하고 결과를 보고서로 만들기 어렵다.
- 기존 점검 결과와 비교하려 해도 기준이 달라 대조가 되지 않는다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**업로드**	PCAP 파일을 단일 또는 다중으로 업로드한다. 진행 상태와 완료 후 총 패킷 수를 확인한다.	F6 PCAP 업로드
2	**제한 확인**	파일 용량·파일명 길이·확장자 제한 조건 위반 시 안내를 확인하고 파일을 조정한다.	F6 PCAP 업로드
3	**조건 설정**	분석 화면에서 업로드한 PCAP를 선택하고 주소 기준(출발지·도착지)과 조건 타입(포함·미포함)을 지정한다.	F6 PCAP 분석
4	**조건 상세**	단일 IP·네트워크 대역·MAC·PORT·프로토콜 조건을 추가하고, 필요 없는 조건은 삭제한다.	F6 PCAP 분석
5	**실행**	사용 가능한 라이선스 수와 총 패킷 수를 확인한 뒤 분석을 시작한다. 진행 상태는 분석 데이터 목록에서 조회한다.	F6 분석 데이터 목록
6	**비교·산출**	같은 방식으로 스위치별 기존 수집 데이터를 분석해 비교하고, 분석 결과 리포트를 PDF로 발행한다.	F6 수집 데이터 분석 · 분석 결과 리포트

▪ 기대 효과

- 이기종 장비가 수집한 트래픽을 같은 도구·같은 기준으로 분석한다.
- 조건을 화면에서 지정해 별도 필터 문법을 익히지 않아도 된다.
- 외부 수집분과 자체 수집분을 비교해 결과의 일관성을 확인할 수 있다.

Part B 운영 업무 프로세스 시나리오

현장 점검 담당자의 업무 6개 프로세스와, 각 단계에서 ICS Scanner가 수행하는 역할입니다.

시나리오	업무	핵심 활용 기능
B-01	현장 점검을 준비할 때	설치 · F3 · F2
B-02	현장에서 수집을 수행할 때	수집 · F2
B-03	승인 장비 목록을 확정할 때	F4 · F3
B-04	점검 결과를 문서로 제출할 때	F4 · F6 · F2
B-05	주기 점검으로 변화를 추적할 때	F3 · F4 · F5
B-06	점검 도구 자체를 관리할 때	F7

B-01 현장 점검을 준비할 때

> **상황**
> 신규 점검 대상 사업소에 처음 방문한다. 어떤 구간을 어떤 기준으로 볼 것인지 사전에 정해야 한다.

▪ 기존 환경에서의 문제

- 점검 기준이 담당자 경험에 의존해 사업소마다 결과의 깊이가 달라진다.
- 현장에 도착해서야 네트워크 구성을 파악하기 시작해 시간이 낭비된다.
- 점검 대상 구간을 나누는 기준이 없어 결과를 구간별로 정리하지 못한다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**설치**	S/W Package를 노트북에 설치한다. 별도 상주 장비 없이 휴대용 노트북에서 운용한다.	설치 구성
2	**스위치 정의**	정책 관리의 스위치에서 점검 대상 스위치를 등록한다. 스위치명과 주요 네트워크 대역을 지정한다.	F3 스위치
3	**IP 정책**	IP 정책 그룹을 만들어 승인 대상 장비의 단일 IP와 네트워크 대역을 등록한다.	F3 IP 정책 그룹
4	**PORT 정책**	PORT 정책 그룹을 만들어 탐지 대상 포트를 블랙리스트로 등록한다. 차단이 아니라 사용 탐지를 위한 기준이다.	F3 PORT 정책
5	**적용**	스위치에 IP 정책 그룹과 PORT 정책 그룹을 적용한다. 정책 그룹 상세를 조회해 적용 내용을 확인한다.	F3 스위치 · F2 스위치 등록
6	**확인**	대시보드에서 선택한 스위치의 IP 정책과 PORT 정책을 조회하고, 정책 확대보기로 상세를 확인한다.	F2 대시보드 · 정책 확대보기

▪ 기대 효과

- 점검 기준이 정책으로 사전에 정의되어 사업소 간 결과가 비교 가능해진다.
- 스위치 단위로 수집 대상이 분리되어 구간별 결과 정리가 가능하다.
- 노트북 한 대로 준비가 끝나 현장 반입 절차가 단순해진다.

B-02 현장에서 수집을 수행할 때

> **상황**
> 스위치의 미러링 포트에 노트북을 연결하고 수집을 시작한다. 얼마나 오래, 어느 정도 용량으로 받아야 하는지 판단해야 한다.

▪ 기존 환경에서의 문제

- 수집 시간이 짧으면 주기가 긴 통신을 놓치고, 길면 디스크가 부족해진다.
- 수집 중 상태를 알 수 없어 정상적으로 받고 있는지 확인이 안 된다.
- 수집을 중단해야 할 시점을 판단할 근거가 없다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**연결**	스위치의 포트 미러링을 설정하고 노트북을 연결한다. 스위치별로 수집 대상이 분리된다.	수집 방식
2	**설정**	대시보드에서 스위치와 수집 드라이버를 선택하고 수집 시간을 지정한다(1분·5분·10분·30분·1시간·2시간·4시간·계속).	F2 대시보드 · 수집
3	**용량 확인**	현재 디스크 용량을 확인하고, 환경설정의 디스크 임계치와 파일 저장 위치를 사전에 점검한다.	F2 대시보드 · F7 환경설정
4	**실행**	수집을 시작한다. 수집 중 화면에서 초당 Kilo Bit 단위 네트워크 트래픽을 확인한다.	F2 수집
5	**진행 확인**	경과 시간과 설정 시간, 수집 파일 크기, 사용 중인 디스크 용량을 확인한다. 필요 시 수집 창을 접어 다른 화면을 함께 본다.	F2 수집
6	**종료**	수집을 중지하고 수집 데이터를 저장한다. 저장된 데이터는 이후 분석에 사용된다.	F2 수집 · F6 수집 데이터 분석

▪ 기대 효과

- 트래픽·파일 크기·디스크가 실시간으로 표시되어 수집 상태를 항상 확인할 수 있다.
- 수집 시간을 상황에 맞게 선택해 짧은 진단부터 장시간 관측까지 대응한다.
- 스위치 단위 수집으로 구간별 데이터가 섞이지 않는다.

B-03 승인 장비 목록을 확정할 때

> **상황**
> 수집 결과 미승인으로 분류된 장비 중 상당수가 실제로는 정상 운영 장비였다. 승인 목록을 현실에 맞게 정리해야 한다.

▪ 기존 환경에서의 문제

- 초기 정책은 알려진 IP만으로 만들어져 실제 운영 장비를 다 담지 못한다.
- 미승인이 과다하게 나오면 결과의 신뢰도가 떨어져 아무도 보지 않게 된다.
- 어느 장비를 승인으로 넘길지 판단할 근거 정보가 부족하다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**검토**	미승인 장비 목록을 조회하고 장비별 상세보기로 IP·MAC·수집 일시를 확인한다.	F4 미승인 장비 · 장비 상세
2	**이력 확인**	해당 장비의 변경 이력 보기로 최초 식별 시점과 변경 여부를 확인해 신규인지 기존 장비인지 판단한다.	F4 장비 변경 이력
3	**식별 정보 등록**	장비 상세에서 장비명과 장비 설명을 등록해 무엇인지 알아볼 수 있게 한다.	F4 장비 상세
4	**승인 전환**	정상 장비로 확인되면 미승인 장비를 승인 장비로 변경한다.	F4 미승인 장비
5	**개별 등록**	수집되지 않았으나 관리 대상인 장비는 장비 등록 페이지에서 장비명·IP·MAC·설명을 입력해 단일 등록한다.	F4 장비 등록
6	**정책 반영**	반복되는 승인 대상은 IP 정책 그룹에 IP 주소를 추가해 다음 점검부터 자동 판별되도록 한다.	F3 IP 정책 그룹

▪ 기대 효과

- 점검을 반복할수록 정책이 정교해져 미승인 과다 문제가 해소된다.
- 장비명·설명이 축적되어 다음 담당자도 목록을 해석할 수 있다.
- 승인 판단의 근거(변경 이력·최초 식별 시점)가 화면에서 함께 확인된다.

B-04 점검 결과를 문서로 제출할 때

> **상황**
> 점검이 끝나면 사업소와 본사에 결과를 제출해야 한다. 현재는 화면을 캡처해 문서를 따로 만들고 있다.

▪ 기존 환경에서의 문제

- 캡처와 편집에 시간이 많이 들고, 그 과정에서 누락·오기가 생긴다.
- 점검자마다 보고서 형식이 달라 회차 간·사업소 간 비교가 안 된다.
- 보고서를 다시 만들려면 원본 데이터를 다시 찾아야 한다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**승인 장비**	승인 장비 내역 리포트를 미리보기로 확인한다. 검색 조건에 따른 목록(번호·장비명·IP·MAC·수집일)이 구성된다.	F4 승인 장비 내역 리포트
2	**미승인 장비**	미승인 장비 내역 리포트를 같은 방식으로 확인한다.	F4 미승인 장비 내역 리포트
3	**변경 이력**	장비 변경 이력 리포트를 확인한다. 스위치와 작성 일자, 변경 사항·변경 내용·변경 일자가 포함된다.	F4 장비 변경 이력 리포트
4	**분석 결과**	분석을 수행한 경우 분석 결과 리포트를 확인한다. 출발지·도착지 IP/MAC과 통신 시점이 목록으로 구성된다.	F6 분석 결과 리포트
5	**발행**	각 리포트를 PDF로 다운로드한다.	F4 · F6 리포트 다운로드
6	**보조 자료**	토폴로지 화면을 이미지로 내보내 통신 구조 설명 자료로 첨부한다.	F2 토폴로지

▪ 기대 효과

- 보고서 작성이 캡처·편집이 아니라 리포트 발행으로 대체된다.
- 형식이 시스템으로 고정되어 회차 간·사업소 간 비교가 성립한다.
- 검색 조건을 바꿔 다시 발행할 수 있어 재작성 부담이 없다.

B-05 주기 점검으로 변화를 추적할 때

> **상황**
> 분기마다 같은 구간을 점검한다. 이번 회차에서 무엇이 달라졌는지를 중심으로 봐야 한다.

▪ 기존 환경에서의 문제

- 매 회차 전수를 다시 확인하느라 시간이 걸리고 변화에 집중하지 못한다.
- 이전 회차 자료가 파일로만 남아 비교 작업이 수작업이 된다.
- 변화가 없다는 사실 자체도 근거를 대기 어렵다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**동일 조건 수집**	기존에 등록한 스위치와 정책 그룹을 그대로 사용해 같은 조건으로 수집한다.	F3 스위치 · F2 수집
2	**변화 조회**	장비 변경 이력에서 직전 점검 이후 기간을 지정해 변경 내역만 조회한다.	F4 장비 변경 이력
3	**유형 구분**	변경 타입과 신규·기존 값으로 신규 장비, IP/MAC 변경, 이탈 장비를 구분한다.	F4 장비 변경 이력
4	**신규 판별**	미승인 장비 목록에서 이번 회차에 새로 나타난 장비를 수집 일시 기준으로 검색한다.	F4 미승인 장비
5	**탐지 확인**	PORT 탐지에서 이번 회차에 발생한 블랙리스트 포트 사용을 통신 일시 기준으로 확인한다.	F5 PORT 탐지
6	**결과 발행**	장비 변경 이력 리포트를 해당 기간으로 발행해 「이번 회차 변화」를 문서로 남긴다.	F4 장비 변경 이력 리포트

▪ 기대 효과

- 전수 확인이 아니라 변화 중심 점검으로 전환되어 점검 시간이 줄어든다.
- 「변화 없음」도 데이터로 입증되어 보고의 근거가 된다.
- 회차가 쌓일수록 구간별 변경 추이가 축적된다.

B-06 점검 도구 자체를 관리할 때

> **상황**
> 점검 노트북을 여러 담당자가 함께 사용한다. 계정과 저장 공간을 관리해야 한다.

▪ 기존 환경에서의 문제

- 계정을 공용으로 쓰면 누가 어떤 점검을 했는지 구분되지 않는다.
- 수집 파일이 쌓여 디스크가 가득 차면 현장에서 수집이 중단된다.
- 담당자가 바뀔 때 도구 사용법을 다시 가르쳐야 한다.

▪ ICS Scanner 의 해결 절차

	단계	수행 내용	사용 기능
1	**계정 생성**	사용자 목록에서 ID·비밀번호·이름·소속·권한을 지정해 사용자를 등록한다.	F7 사용자 목록
2	**현황 확인**	사용자 목록에서 ID·이름·소속·권한·생성 날짜·로그인 차단 여부를 조회하고 검색한다.	F7 사용자 목록
3	**차단 관리**	로그인 5회 실패로 차단된 계정은 관리자가 비밀번호를 수정해 차단을 해제한다.	F7 사용자 목록 · F1 로그인
4	**본인 관리**	각 사용자는 본인 정보와 비밀번호를 직접 수정한다.	F7 사용자 정보 수정
5	**저장 관리**	환경설정에서 디스크 임계치와 파일 저장 위치를 설정한다. 분석 데이터 목록에서 불필요한 업로드 파일을 선택해 삭제한다.	F7 환경설정 · F6 분석 데이터 목록
6	**인계**	사용 가이드에서 화면별 기능 설명과 버전·회사 정보를 확인해 신규 담당자가 스스로 익힌다.	F7 사용 가이드

▪ 기대 효과

- 사용자별 계정으로 운용하고, 스위치 등록·수정 이력에 생성자·수정자가 남는다.
- 디스크 임계치와 파일 정리로 현장에서 수집이 중단되는 상황을 예방한다.
- 제품 내 사용 가이드가 있어 인수인계 부담이 작다.

Part C 문제 해결 시나리오

상주 설치가 어려운 구간을 담당하는 실무자들이 반복적으로 제기하는 5개 문제 제기와, 그에 대한 ICS Scanner의 답변입니다.

시나리오	문제점	주제
C-01	상주 장비를 설치할 수 없는 구간이 있습니다.	상시 시스템 적용의 한계
C-02	신재생·CCTV망은 자산 현황 자체가 없습니다.	독립.분리망의 관리 공백
C-03	전사 도입 전에 효과를 먼저 확인하고 싶습니다.	도입 전 검증의 필요
C-04	감사 때 제출할 자산 증적이 없습니다.	점검 증적의 부재
C-05	노트북 한 대로 어디까지 되는지 모르겠습니다.	적용 범위에 대한 불확실성

C-01 상시 시스템 적용의 한계

> **고객의 말**
> "상주 장비를 설치할 수 없는 구간이 있습니다."

▪ 문제의 배경

- 소규모 단독망이나 임시 구간은 상주 시스템을 놓을 공간·전원·예산이 없다.
- 설치를 하려면 정지 작업과 승인 절차가 필요해 착수 자체가 어렵다.
- 결과적으로 해당 구간은 아무런 확인 없이 방치된다.

▪ ICS Scanner 의 답

접근	내용	근거 기능
휴대형 운용	S/W Package 설치만으로 노트북에서 즉시 운용한다. 상주 시스템 설치가 필요 없다.	설치 구성
즉시 사용	스위치 미러링 포트에 연결하고 수집 대상과 시간을 지정하면 바로 수집이 시작된다.	F2 수집
구간 분리	스위치 단위로 수집 대상을 분리해 여러 구간을 순차적으로 점검한다.	F3 스위치
자산 유형 무제약	IP 자산 유형에 제약이 없어 제어 설비, 네트워크 장비, CCTV 등 구분 없이 식별한다.	F4 장비 관리

> **결과**
> 설치가 불가능해 확인조차 못 하던 구간이 점검 대상으로 편입됩니다. 노트북 반입만으로 자산 현황이 확보됩니다.

※ 권고 사양 — Windows 10 Pro 이상 · Intel Core i5 1.0GHz 이상 · RAM 16GB 이상 · SSD 256GB + HDD 1TB 이상. 1대 기준 설치 시간 약 1시간.

C-02 독립.분리망의 관리 공백

> **고객의 말**
> "신재생·CCTV망은 자산 현황 자체가 없습니다."

▪ 문제의 배경

- 태양광·풍력 단지와 CCTV망은 시공사가 구축한 뒤 자산 정보가 인계되지 않는 경우가 많다.
- 규모가 작다는 이유로 관리 대상에서 빠져 있다가 점검 지적을 받는다.
- 무엇이 있는지 모르는 상태라 개선 계획조차 세울 수 없다.

▪ ICS Scanner 의 답

접근	내용	근거 기능
자동 식별	스위치 기준 통신 수집·탐지로 네트워크에 연결된 자산을 자동 식별한다.	F4 장비 관리
목록화	승인·미승인 장비 목록과 총 장비 수를 조회하고, 장비명·설명을 등록해 대장을 만든다.	F4 승인 장비 · 장비 상세
구조 파악	통신 이력과 토폴로지로 장비 간 연결 구조와 통신 방향을 확인한다.	F5 통신 이력 · F2 토폴로지
변경 추적	주기 점검으로 신규·변경·이탈 장비를 변경 이력으로 관리한다.	F4 장비 변경 이력
대규모 대응	3,500 노드 이상 규모의 네트워크 운영 이력을 보유하고 있다.	운영 실적

> **결과**
> 관리 공백이던 분리망이 첫 점검으로 통신 기준 자산 목록을 갖게 됩니다. 이후는 회차별 변경분만 추적하면 됩니다.

C-03 도입 전 검증의 필요

> **고객의 말**
> "전사 도입 전에 효과를 먼저 확인하고 싶습니다."

▪ 문제의 배경

- 제어망 보안 시스템은 투자 규모가 커서 효과를 확인하지 않고 결정하기 어렵다.
- 벤더 자료만으로는 자사 환경에서 실제로 무엇이 나올지 알 수 없다.
- 검증을 하려 해도 시범 구축 자체에 비용과 기간이 든다.

▪ ICS Scanner 의 답

접근	내용	근거 기능
부담 없는 검증	상주 설치 없이 노트북 한 대로 실제 제어망에서 수집·분석을 수행한다.	설치 구성
현황 진단	승인·미승인 장비, 포트 사용, 통신 구조를 실제 데이터로 산출해 현황을 진단한다.	F4 · F5
결과 공유	리포트 4종(승인 장비·미승인 장비·장비 변경 이력·분석 결과)을 PDF로 발행해 의사결정 자료로 사용한다.	F4 · F6 리포트
확장 판단	진단 결과를 근거로 상시 모니터링이 필요한 구간을 정하고 상위 제품 적용을 검토한다.	제품 확장

> **결과**
> 도입 판단이 벤더 설명이 아니라 자사 제어망의 실측 데이터 위에서 이루어집니다.

※ ICS Scanner는 TTA 소프트웨어 품질 시험 GS인증 1등급을 획득했습니다.

C-04 점검 증적의 부재

고객의 말

"감사 때 제출할 자산 증적이 없습니다."

▪ 문제의 배경

- 보안 감사에서 자산 현황과 점검 수행 증적을 요구하는데 제출할 자료가 없다.
- 점검을 했더라도 결과가 개인 문서로 남아 공식 자료로 인정받기 어렵다.
- 점검 주기와 범위를 입증할 방법이 없다.

▪ ICS Scanner 의 답

접근	내용	근거 기능
표준 리포트	승인 장비 내역, 미승인 장비 내역, 장비 변경 이력, 분석 결과를 PDF 리포트로 발행한다.	F4 · F6 리포트
작성 정보 포함	리포트에 스위치와 작성 일자가 포함되어 언제 어느 구간을 점검했는지 남는다.	F4 장비 변경 이력 리포트
조건 명시	검색 조건에 따라 목록이 구성되어 점검 범위가 리포트에 반영된다.	F4 리포트
시각 자료	토폴로지 화면을 이미지로 내보내 통신 구조 증적으로 첨부한다.	F2 토폴로지
운용 계정	사용자별 계정으로 운용하며, 스위치 목록에 생성자·생성일시와 수정자·변경일시가 기록된다.	F7 사용자 목록 · F3 스위치

결과

점검 수행 사실과 결과가 시스템이 만든 문서로 남습니다. 감사 대응 자료가 점검할 때마다 자동으로 축적됩니다.

C-05 적용 범위에 대한 불확실성

> **고객의 말**
> "노트북 한 대로 어디까지 되는지 모르겠습니다."

▪ 문제의 배경

- 휴대형 도구라고 하면 기능이 제한적일 것이라는 선입견이 있다.
- 반대로 상시 관제까지 되는 것으로 기대했다가 도입 후 실망하는 경우도 있다.
- 어느 구간에 무엇을 써야 하는지 판단 기준이 없다.

▪ ICS Scanner 의 답

접근	내용	근거 기능
수행 범위	자산 자동 식별, 승인·미승인 판별, 포트 탐지, 통신 이력·토폴로지, PCAP 분석, PDF 리포트 발행까지 수행한다.	F2~F6
운용 방식	수집은 노트북을 스위치에 연결한 상태에서 이루어진다. 연결하지 않은 시간의 통신은 수집되지 않으며, 저장된 데이터의 분석은 연결 없이 수행할 수 있다.	F2 수집 · F6 분석
적합한 용도	상주 설치가 어려운 구간의 주기 점검, 소규모 단독망 현황 파악, 도입 전 진단(PoC)에 적합하다.	적용 대상
상시 관제 구간	상시 모니터링과 실시간 알림이 필요한 구간은 ICS Asset Manager 또는 ICS Security Monitor를 적용한다.	제품 선택

> **결과**
> 「무엇이 되고 무엇이 안 되는가」가 분명해져, 구간별로 맞는 도구를 배치할 수 있습니다.

03 시나리오 – 기능 매핑 종합

본 문서에서 다룬 16개 시나리오가 ICS Scanner의 기능 체계 전반을 어떻게 활용하는지 정리한 표입니다. 기능이 특정 영역에 편중되지 않고 수집 · 식별 · 판별 · 관리 · 산출 전 계층에 걸쳐 연계 활용되는 통합 운영 구조임을 확인할 수 있습니다.

코드	기능 대분류	활용 시나리오
F1	**로그인**	전 시나리오 공통 (시스템 접근 기반)
F2	**대시보드**	A-01, A-04, B-01, B-02, B-04, C-01, C-02, C-04, C-05
F3	**정책 관리**	A-01, A-03, B-01, B-03, B-05, C-01, C-04
F4	**장비 관리**	A-01, A-02, B-03, B-04, B-05, C-01, C-02, C-03, C-04
F5	**탐지 현황**	A-03, A-04, B-05, C-02, C-03
F6	**분석**	A-05, B-04, C-03, C-04, C-05
F7	**설정**	B-06, C-04

▪ 시나리오 전체 목록

구분	번호	제목
Part A	**A-01**	정책에 없는 장비가 네트워크에 연결되어 있을 때
Part A	**A-02**	장비의 IP나 MAC이 지난 점검 이후 바뀌었을 때
Part A	**A-03**	허용되지 않은 서비스 포트가 사용되고 있을 때
Part A	**A-04**	예상하지 못한 통신 경로가 존재할 때
Part A	**A-05**	다른 장비가 수집한 트래픽을 검증해야 할 때
Part B	**B-01**	현장 점검을 준비할 때
Part B	**B-02**	현장에서 수집을 수행할 때
Part B	**B-03**	승인 장비 목록을 확정할 때
Part B	**B-04**	점검 결과를 문서로 제출할 때
Part B	**B-05**	주기 점검으로 변화를 추적할 때
Part B	**B-06**	점검 도구 자체를 관리할 때
Part C	**C-01**	상시 시스템 적용의 한계 — 상주 장비를 설치할 수 없는 구간이 있습니다.

구분	번호	제목
Part C	**C-02**	분리망의 관리 공백 — 신재생·CCTV망은 자산 현황 자체가 없습니다.
Part C	**C-03**	도입 전 검증의 필요 — 전사 도입 전에 효과를 먼저 확인하고 싶습니다.
Part C	**C-04**	점검 증적의 부재 — 감사 때 제출할 자산 증적이 없습니다.
Part C	**C-05**	적용 범위에 대한 불확실성 — 노트북 한 대로 어디까지 되는지 모르겠습니다.

04 도입 방식 및 지원 체계

본 문서의 시나리오는 아래 구성과 유지보수 서비스 체계를 전제로 합니다.

▪ 단일 모델 · 권고 사양

구분	권고 사양
운영 환경	Windows 10 Pro 이상
CPU	Intel Core i5 1.0GHz 이상
RAM	16GB 이상
저장장치	SSD 256GB + HDD 1TB 이상
설치 구성	Tomcat · AdoptOpenJDK · MariaDB · Winpcap
설치 시간	1대 기준 약 1시간

▪ 유지보수 서비스 — Basic 등급 전용

항목	제공 내용
지원 시간	평일 09–18시
패치 제공	연 2회
콘텐츠 전달 방식	고객 포털에서 내려받아 적용 · C1 사업장은 오프라인 매체로 전달
제품 하자 수정 · 장애 현장 출동	제공 (등급과 무관)
기술 문의 대응	제공 (등급과 무관)
정기 방문 점검	미제공
방문 시 수행 항목 (오탐 튜닝 · 정기 리포트 · 자산/취약점 리포트)	미제공
운영서비스 (원격 정기 점검 · 리포트)	미제공

※ ICS Scanner는 단일 모델로 구축 모델 구분이 없으며, 서비스 등급은 Basic 전용(요율 10%)입니다. 정기 방문 점검과 운영서비스(원격 정기 점검·리포트)는 제공되지 않으며, SLA는 Basic 기준으로 적용됩니다.

> **구간별 제품 배치**
> Part C의 「적용 범위에 대한 불확실성」(C-05)에서 다룬 것처럼, ICS Scanner는 상주 설치가 어려운 구간의 주기 점검과 도입 전 진단에 적합합니다. 상시 모니터링과 실시간 알림이 필요한 구간에는 ICS Asset Manager를, 탐지·분석·관

> 제를 통합해야 하는 구간에는 ICS Security Monitor를 적용합니다.

CONTACT

제품 · 견적 문의

주소 (우) 12902 경기도 하남시 미사강변한강로 135(망월동) 미사강변스카이폴리스 다동 1038~1039호

대표전화 031-792-0633 · Fax 031-792-0635

이메일 info@onsecurity.co.kr

홈페이지 www.onsecurity.co.kr