ICS Security Monitor

산업제어시스템 통합 보안 모니터링 시스템

운영 지침서

제어시스템 현장에서 실제로 발생하는 28개 상황과

ICS Security Monitor의 기능 기반 해결 절차

Part A 보안 위협 상황 10건 · Part B 운영 업무 프로세스 10건 · Part C 고객 문제 해결 8건

v1.1 · 2026. 8.

온시큐리티㈜

경기도 하남시 미사강변한강로 135(망월동) 미사강변스카이폴리스 다동 1038-1039호 · TEL 031-792-0633

목 차

01 문서의 목적과 구성 3

02 ICS Security Monitor 기능 체계 4

Part A 보안 위협 상황 시나리오 5

A-01 인가되지 않은 장비가 제어망에 연결되었을 때 6

A-02 외부 경로를 통해 악성코드가 제어망에 유입되었을 때 7

A-03 제어망 내부에서 정찰·스캐닝 행위가 발생했을 때 9

A-04 알려진 공격 기법이 제어망 트래픽에서 관측될 때 11

A-05 악성코드가 자산 사이로 번져 나갈 때 12

A-06 제어망에서 외부로의 비인가 통신이 발생했을 때 13

A-07 자산 정보를 위장해 우회 접속을 시도할 때 14

A-08 하나의 자산에서 시작된 위협이 확산될 때 15

A-09 프린터를 통해 제어 자료가 무단 출력될 때 16

A-10 트래픽 급변·통신 중단 등 설비 이상 징후가 나타날 때 17

Part B 운영 업무 프로세스 시나리오 18

B-01 신규 설비를 반입해 자산으로 등록해야 할 때 19

B-02 정기 자산 실사와 대장 현행화를 수행할 때 20

B-03 설비의 물리 배치와 네트워크 구성을 현행화할 때 21

B-04 보안 정책을 수립하고 다수 사업장에 배포할 때 22

B-05 취약점 탐지 룰을 최신 상태로 유지해야 할 때 23

B-06 악성코드 탐지 결과를 판정하고 근거를 남겨야 할 때 24

B-07 오탐이 많아 알람을 신뢰할 수 없을 때 25

B-08 일상 관제 — 이벤트 확인부터 이슈 종결까지 26

B-09 정기 보안 보고서를 작성해 제출해야 할 때 27

B-10 사용자 권한을 관리하고 접근 이력을 감사할 때 28

Part C 고객 문제 해결 시나리오 29

C-01 자산 가시성 부재 30

C-02 망 분리 실효성 입증 불가 31

C-03 규제 대응 부담 32

C-04 사후 추적 불가 33

C-05 다지역 통합 관리 부재 34

C-06 가용성 우려 35

C-07 운영 지식의 휘발 36

C-08 능동 취약점 진단 불가 37

03 시나리오 – 기능 매핑 종합 38

04 도입 방식 및 지원 체계 40

01 문서의 목적과 구성

본 문서는 산업제어시스템 통합 보안 모니터링 시스템(ICS Security Monitor)이 제어시스템 운영 현장에서 실제로 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	비인가 장비 접속, 악성코드 유입, 정찰·스캐닝, 공격 기법 관측, 악성코드 전파, 외부 통신, 자산 위장, 위협 확산, 무단 출력, 설비 이상 징후 — 10건
Part B	운영 업무 프로세스	자산 등록, 자산 실사, 배치·구성 관리, 정책 배포, 룰 갱신, 악성코드 판정, 오탐 튜닝, 일상 관제, 보고서 작성, 권한·감사 — 10건
Part C	고객 문제 해결	자산 가시성, 망 분리 입증, 규제 대응, 사후 추적, 다지역 통합, 가용성 우려, 운영 지식 휘발, 능동 취약점 진단 — 8건

▪ 기술 원칙

- 본 문서에 인용된 모든 기능은 ICS Security Monitor 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~F10 코드를 따릅니다.

> **참고**
> 본 제품은 보안관제(MSSP) 서비스가 아닙니다. 24×7 상시 대응과 침해사고 대응(IR)은 제공 범위에 포함되지 않으며, 본 문서의 시나리오는 고객사 담당 인력이 시스템을 활용해 수행하는 절차를 기준으로 기술되었습니다.

02 ICS Security Monitor 기능 체계

시나리오 해결 절차에서 참조하는 기능 코드 체계입니다. 10개 대분류, 24개 중분류로 구성되며 총 170여 개의 세부 기능이 구현되어 있습니다.

코드	대분류	중분류	주요 세부 기능
F1	로그인/로그아웃	로그인 · 로그아웃	사용자 인증 및 세션 관리
F2	대시보드	이벤트 대시보드	수집망별 트래픽 · 알람 통계(네트워크/취약점/악성코드) · 알람 목록 · 미확인 IP 조회
F3	자산 관리	자산 현황 · 통신 현황 · 캐비닛 관리	자산 등록/수정/폐기, 엑셀 일괄 업로드·다운로드, 수집 IP 조회, 자산 상세 알림·토폴로지, 트래픽 임계치, 캐비닛·시설 배치
F4	네트워크 현황	네트워크 현황 · 패킷 분석 · 트래픽 분석	Grid/Node 토폴로지, 장소 위치 편집, 패킷 분석 결과 상세, 통신 내역·트래픽 통계(호기·IP·Port 필터)
F5	실시간 이벤트 분석	네트워크 탐지 · 악성코드 탐지 · 취약점 탐지 · 프린터 사용 탐지	신규 통신·신규 MAC 탐지, 트래픽 통계 차트, 패킷 분석 요청, 파일 검사 결과(Defender), 취약점 알림 토폴로지, 프린터 사용 탐지 상세
F6	이슈 관리	이슈 보드 · 이슈 목록 · 이슈 상세	알람 통합 등록, 조치 내용·메모 수정, 이슈 토폴로지, 이슈 종결
F7	정책	네트워크 정책 · IP 목록 · PORT 목록 · 취약점 탐지 정책	정책 등록/수정/삭제, 정책 동기화, 수집 IP/PORT 상태 조회, 룰 상세 세부 설정(예외처리·비활성화), 네트워크 변수, 본사 동기화 상태 확인
F8	위협 분석	위협 스캐닝 · 위협 상관 분석	자산 기준 이벤트 집계·요약, 스캐닝 상세(네트워크 레이아웃·정책·취약점·악성코드 목록), 상관분석 결과
F9	보고서	보고서 관리	보고서 신규 발행, 발행 파일 목록·다운로드, 보고서 삭제
F10	설정	권한 관리 · 사용자 관리 · 사용자 로그	권한 등록/수정/삭제, 계정 생성·활성화·삭제, 비밀번호 변경, 사용자 자산 목록, 사용자 로그 조회

▪ 기능 계층 구조

계층	구성
관제 · 보고	통합 대시보드(F2) · 이슈 관리(F6) · 보고서 자동 생성(F9)
분석	위협 스캐닝 · 네트워크 위협 상관분석(F8) · 패킷 분석 · 트래픽 분석(F4)

계층	구성
탐지	네트워크 탐지 · 취약점 탐지 · 악성코드 탐지 · 프린터 사용 탐지(F5)
기반	자산 관리(F3) · 네트워크 현황(F4) · 정책 관리(F7) · 제어망 패킷 패시브 수집

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

Part A 보안 위협 상황 시나리오

제어시스템 환경에서 실제로 발생하는 10개 위협 상황과, ICS Security Monitor가 이를 탐지·분석·조치하는 절차입니다.

시나리오	상황	핵심 대응 기능
A-01	인가되지 않은 장비가 제어망에 연결되었을 때	F5 · F2 · F4 · F6 · F3 · F7
A-02	외부 경로를 통해 악성코드가 제어망에 유입되었을 때	F5 · F3 · F8 · F6
A-03	제어망 내부에서 정찰·스캐닝 행위가 발생했을 때	F7 · F5 · F2 · F4 · F3 · F8 · F6
A-04	알려진 공격 기법이 제어망 트래픽에서 관측될 때	F7 · F5 · F4 · F6
A-05	악성코드가 자산 사이로 번져 나갈 때	F5 · F8 · F4 · F6
A-06	제어망에서 외부로의 비인가 통신이 발생했을 때	F7 · F5 · F3 · F4 · F8 · F6
A-07	자산 정보를 위장해 우회 접속을 시도할 때	F3 · F5 · F8 · F6 · F7
A-08	하나의 자산에서 시작된 위협이 확산될 때	F8 · F4 · F6 · F9
A-09	프린터를 통해 제어 자료가 무단 출력될 때	F3 · F5 · F4 · F6 · F9
A-10	트래픽 급변·통신 중단 등 설비 이상 징후가 나타날 때	F3 · F5 · F2 · F4 · F8

A-01 인가되지 않은 장비가 제어망에 연결되었을 때

> **상황**
> 정비 기간 중 협력업체 담당자가 진단용 노트북을 제어망 스위치에 연결했다. 사전 반입 승인은 있었으나 어느 구간에 연결했는지, 어떤 설비와 통신했는지는 기록되지 않았다.

▪ 기존 환경에서의 문제

- 제어망은 스위치 포트에 물리적으로 연결하면 통신이 성립되므로, 연결 사실 자체를 인지할 수단이 없다.
- 사후에 확인하려 해도 스위치 MAC 테이블은 휘발성이어서 며칠이 지나면 흔적이 남지 않는다.
- 설령 인지하더라도 「어떤 설비와 무슨 통신을 했는가」를 재구성할 방법이 없어, 영향 범위를 판단할 수 없다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**탐지**	미등록 IP·MAC이 제어망에서 통신을 시작하는 즉시 「신규 IP 탐지」·「신규 MAC 탐지」 이벤트가 발생한다.	F5 네트워크 탐지
2	**인지**	이벤트 대시보드의 수집망별 알람 통계와 「미확인 IP」 팝업에 즉시 반영되어 관제 담당자가 별도 조회 없이 인지한다.	F2 이벤트 대시보드
3	**식별**	알림 상세에서 해당 장비가 수행한 신규 통신 내역과 MAC 탐지 통계를 확인해 통신 상대 설비를 특정한다.	F5 네트워크 탐지 상세
4	**범위 판정**	네트워크 토폴로지에서 연결 지점과 통신 경로를 시각적으로 확인하고, 트래픽 분석에서 호기·IP·Port 기준으로 통신량을 조회한다.	F4 네트워크 현황 · 트래픽 분석
5	**증적 확보**	알림 상세에서 패킷 분석을 요청해 실제 통신 내용을 확보하고 분석 결과를 상세 조회한다.	F5 패킷 분석 요청 · F4 패킷 분석
6	**조치·기록**	이슈로 등록해 원인 분석과 조치 결과를 기록하고, 승인된 장비라면 자산으로 정식 등록하거나 정책 예외로 처리한다.	F6 이슈 관리 · F3 자산 등록 · F7 IP 목록 관리

▪ 기대 효과

- 연결 시점 기준 탐지 — 사후 조사가 아니라 발생 시점에 인지한다.
- 통신 상대와 통신 내용까지 확보되어 영향 범위 판정에 필요한 근거가 남는다.
- 조치 이력이 이슈로 축적되어 동일 사안 재발 시 판단 기준이 된다.

A-02 외부 경로를 통해 악성코드가 제어망에 유입되었을 때

> **상황**
> 정비 목적으로 반입된 협력업체 노트북이 제어망에 연결됐다. 해당 노트북은 사외에서 인터넷을 사용하던 장비이고, 반입 전 검사는 백신 실행 화면을 촬영해 제출하는 방식으로 갈음됐다. 연결 직후 이 장비에서 운영자 PC로 파일이 전송됐다.

▪ 기존 환경에서의 문제

- 제어 설비는 가용성이 최우선이라 에이전트(백신·EDR) 설치가 제한되거나 설비 벤더 보증 범위를 벗어나 금지되는 경우가 많다.
- 설치가 가능하더라도 폐쇄망이라 패턴 업데이트가 지연된다. 백신이 있다는 사실과 최신 위협을 잡는다는 것은 다른 이야기다.
- 개별 자산의 백신 로그는 중앙에 모이지 않아, 유입 여부를 전사 관점에서 파악할 수 없다. 감염 사실을 아는 시점이 대개 증상이 나타난 뒤다.
- 반입 검사는 반입 시점의 상태만 확인한다. 반입 이후 제어망 안에서 무슨 일이 일어났는지는 검사 대상이 아니다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**수집**	제어망 패킷을 패시브(미러링·탭) 방식으로 수집한다. 개별 설비에 에이전트를 설치하지 않고, 설비로 요청을 보내지도 않는다.	패시브 수집 기반
2	**탐지**	네트워크 전송 단계에서 파일을 추출해 시스템 제공 백신(Windows Defender)으로 검사하고, 악성코드 탐지 이벤트를 발생시킨다. 자산이 파일을 실행하기 전 전달 시점에 탐지된다.	F5 악성코드 탐지
3	**경로 확인**	악성코드 탐지 알림 토폴로지에서 유입 경로를 확인한다. 이 사례처럼 외부 장비 연결이 기점인지, 인터넷 접속 경로인지가 구분된다.	F5 악성코드 탐지 알림 토폴로지
4	**검사 결과 확인**	알림 상세에서 파일 검사 결과를 조회해 악성코드 종류와 판정 근거를 확인하고, 대응 수준을 결정한다.	F5 파일 검사 결과 조회 (Defender)
5	**동반 이벤트 확인**	같은 시간대에 해당 자산에서 신규 통신·신규 MAC 탐지가 함께 발생했는지 자산 상세 알림 목록에서 대조해, 인가되지 않은 장비의 연결과 악성코드 유입이 같은 사건인지 확인한다.	F5 네트워크 탐지 · F3 자산 상세 알림 목록
6	**확산 여부 판단**	위협 상관 분석으로 해당 자산 전후 시간대의 연계 자산 이벤트를 검색해 2차 전파 여부를 확인한다.	F8 위협 상관 분석
7	**조치**	관련 이벤트를 하나의 이슈로 묶어 격리·정밀검사·재발 방지 조치를	F6 이슈 관리

	단계	수행 내용	사용 기능
		기록하고, 종결 시 포함 이벤트를 일괄 종료한다.	

▪ 기대 효과

- Agentless — 제어 설비에 아무것도 설치하지 않고 악성코드 유입을 탐지한다. 설비 벤더 보증과 충돌하지 않는다.
- 전송 단계에서 탐지하므로 감염 후 증상이 아니라 유입 시점에 인지한다. 증상이 나타나기를 기다리지 않고 대응을 시작할 수 있다.
- 유입 경로와 전파 여부가 함께 확인되어 격리 범위를 근거 있게 결정한다.
- 반입 검사가 놓치는「반입 이후」구간이 상시 관측으로 메워진다.

※ 관련 특허 출원 — 제10-2025-0192404호「폐쇄망 네트워크 기반 악성코드 탐지 시스템 및 방법」. 탐지는 네트워크를 오가는 파일을 대상으로 하며, 매체를 설비에 직접 연결해 네트워크를 거치지 않고 유입된 파일은 탐지 대상이 아닙니다.

A-03 제어망 내부에서 정찰·스캐닝 행위가 발생했을 때

> **상황**
> 제어망 내 특정 IP가 다수의 설비 IP와 포트를 짧은 시간에 순차적으로 접속 시도했다. 통상적인 제어 통신에서는 나타나지 않는 패턴이다. 담당자는 협력업체의 정상 진단 작업일 가능성과 침해 시도일 가능성을 모두 배제하지 못하고 있다.

▪ 기존 환경에서의 문제

- 제어 프로토콜은 통신 상대와 주기가 고정적이어서 스캐닝은 명백한 이상이지만, 이를 판정할 기준이 현장에 없다.
- 일반 IT 보안장비의 룰셋을 그대로 적용하면 제어 통신이 대량 오탐으로 잡혀 운영이 불가능하다. 그렇다고 룰을 느슨하게 하면 정찰 행위가 통과한다.
- 탐지되더라도 어떤 자산이 표적이었는지 정리되지 않아 대응 우선순위를 정할 수 없다.
- 정찰은 그 자체로는 피해가 없어 후순위로 밀리지만, 실제로는 공격의 준비 단계다. 이 시점에 잡지 못하면 다음 단계는 실행 이후에 인지하게 된다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**룰 적용**	Snort Community rule과 제어망 환경에 맞춘 Custom rule을 병행 적용한다. Scanning · DDoS · Session Hijacking · SQL Injection · Spoofing · 무차별 대입 유형을 탐지한다.	F7 취약점 탐지 정책 관리
2	**탐지**	스캐닝 패턴이 룰에 부합하면 취약점 탐지 이벤트가 발생하고 대시보드 알람 통계에 반영된다.	F5 취약점 탐지 · F2 대시보드
3	**표적 확인**	취약점 탐지 알림 토폴로지에서 스캐닝 주체와 표적이 된 자산군을 시각적으로 확인한다. 표적이 특정 설비인지 대역 전체인지에 따라 의도가 갈린다.	F5 취약점 탐지 알림 토폴로지
4	**내용 확인**	알림 상세 조회 후 패킷 분석을 요청하고, 요청한 분석 결과는 패킷 분석 화면에서 상세 조회해 실제 시도 내용과 응답을 확인한다.	F5 알림 상세 · 패킷 분석 요청 · F4 패킷 분석 결과 상세 조회
5	**주체 확인**	스캐닝 주체 IP가 자산 대장에 등록된 장비인지 조회한다. 미등록이면 신규 IP·신규 통신 탐지 이벤트가 함께 발생했는지 대조해 반입 장비 여부를 판단한다.	F3 자산 현황 · F5 네트워크 탐지
6	**이력 집계**	위협 스캐닝에서 1일 단위로 해당 자산의 이벤트 이력을 집계해 단발성인지 지속적인지 판단하고, 위협 상관 분석으로 다른 구간에서도 같은 패턴이 있었는지 확인한다.	F8 위협 스캐닝 · 위협 상관 분석

	단계	수행 내용	사용 기능
7	**정책 반영**	정당한 진단 행위로 확인되면 룰 세부 설정에서 예외 처리하고, 위협으로 판정되면 이슈로 등록해 차단 조치를 기록한다.	F7 룰 세부 설정 · F6 이슈 관리

▪ 기대 효과

- Community rule의 폭넓은 커버리지와 Custom rule의 제어망 적합성을 동시에 확보한다.
- 예외처리·비활성화를 룰 단위로 관리해 오탐을 줄이면서 탐지 범위는 유지한다.
- 단발 이벤트가 아니라 자산 기준 이력으로 집계되어 지속적 위협 여부를 판단할 수 있다.
- 주체가 등록 자산인지 반입 장비인지가 조회로 확인되어, 「정상 진단인가 침해 시도인가」의 판단이 추정이 아니라 확인된 사실 위에서 이뤄진다.

※ 탐지는 관측 기반입니다. ICS Security Monitor는 설비에 요청을 보내는 능동 스캔을 수행하지 않으므로, 제품 자신이 스캐닝 이벤트의 원인이 되지 않습니다.

A-04 알려진 공격 기법이 제어망 트래픽에서 관측될 때

> **상황**
> 엔지니어링 워크스테이션에서 HMI 웹 인터페이스로 짧은 간격의 로그인 시도가 반복됐다. 같은 시간대에 다른 IP에서는 데이터베이스 질의문 형태의 문자열이 포함된 요청이 관측됐다. 두 건 모두 제어 시스템 자체 로그에는 남지 않았다.

▪ 기존 환경에서의 문제

- 제어망에도 웹 기반 HMI · 이력 서버 · 원격 접속 게이트웨이가 존재하지만, 이들 응용 계층에서 벌어지는 공격 시도는 제어 시스템 로그에 기록되지 않는다.
- 공격 기법마다 흔적이 남는 계층이 달라, 하나의 관측 수단으로는 유형을 구분할 수 없다.
- 유형을 모르면 대응도 달라질 수 없다. 무차별 대입은 계정 잠금, 주입 시도는 입력 검증, 세션 탈취는 인증 방식 — 조치 부서와 방법이 각각 다르다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**유형 설정**	취약점 탐지 정책 관리에서 정책 그룹별로 탐지 유형을 설정한다. DDoS · Scanning · Session Hijacking · SQL Injection · Spoofing · 무차별 대입 유형을 제어망 환경에 맞게 활성화한다.	F7 취약점 탐지 정책 관리
2	**탐지**	수집 트래픽이 룰에 부합하면 취약점 탐지 이벤트가 유형과 함께 발생한다. 제어 설비에는 아무런 요청도 보내지 않는다.	F5 취약점 탐지
3	**유형 확인**	취약점 분석 목록을 스크롤 또는 테이블 레이아웃으로 조회해 어떤 유형이 어느 자산에서 발생했는지 확인한다.	F5 취약점 분석 목록 조회
4	**대상 확인**	취약점 탐지 알림 토폴로지에서 시도 주체와 대상 자산의 관계를 확인해 표적이 특정 설비인지 대역 전체인지 판별한다.	F5 취약점 탐지 알림 토폴로지
5	**내용 확인**	알림 상세를 조회한 뒤 패킷 분석을 요청하고, 패킷 분석 화면에서 결과를 상세 조회해 실제 요청 내용과 응답을 확인한다. 이를 근거로 실패한 시도인지 성립한 침해인지 판정한다.	F5 알림 상세 · 패킷 분석 요청 · F4 패킷 분석 결과 상세 조회
6	**조치**	유형별로 하나의 이슈로 등록하고, 계정 정책 · 입력 검증 · 접근 통제 등 조치 내용과 담당 부서를 이슈의 조치 내용에 기록한다.	F6 이슈 관리 — 이슈 등록 · 조치 내용

▪ 기대 효과

- 제어 시스템 로그에 남지 않는 응용 계층 공격 시도를 네트워크 트래픽만으로 포착한다.
- 탐지 결과가 유형과 함께 제시되어, 「보안 이벤트 발생」이 아니라 「무차별 대입 시도」로 구체화된다. 대응 부서와 조치 방법이 바로 정해진다.

- 패킷 분석으로 시도의 성패까지 확인되어, 모든 탐지를 동일한 긴급도로 취급하지 않아도 된다.

※ 탐지 유형은 Snort Community rule과 제어망 Custom rule의 조합으로 구성됩니다. ICS Security Monitor는 트래픽을 관측해 탐지하며, 설비에 요청을 보내는 능동 스캔은 수행하지 않습니다.

A-05 악성코드가 자산 사이로 번져 나갈 때

> **상황**
> 한 대의 운영자 PC에서 악성코드가 탐지됐다. 해당 PC를 격리했으나, 며칠 뒤 다른 대역의 설비에서 유사한 통신이 관측됐다. 그 사이 어떤 자산이 감염 경로에 있었는지는 확인되지 않았다.

▪ 기존 환경에서의 문제

- 최초 감염 자산을 격리해도, 격리 이전에 어디까지 번졌는지 모르면 조치가 끝났다고 말할 수 없다.
- 제어망 내부 자산 간 통신은 방화벽을 거치지 않는 경우가 많아 경계 장비 로그에 흔적이 남지 않는다.
- 감염 자산이 MAC 주소를 바꿔 다른 장비로 위장하면, 자산 대장 기준의 추적은 그 지점에서 끊긴다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**탐지**	네트워크 전송 단계에서 파일을 추출해 시스템 제공 백신(Windows Defender)으로 검사하고 악성코드 탐지 이벤트를 발생시킨다.	F5 악성코드 탐지
2	**경로 구분**	악성코드 탐지 알림 토폴로지에서 유입 경로를 구분한다. 인터넷 접속 · 외부장비 연결은 외부 유입, 자산 간 전파 · MAC 변경 후 전파는 내부 확산이다.	F5 악성코드 탐지 알림 토폴로지
3	**확산 추적**	위협 상관 분석으로 탐지 자산을 기점 삼아 이전·이후 시간대 연계 자산의 이벤트를 검색하고, 동일·유사 이벤트가 자산 사이에서 연속 발생한 흐름을 확인한다.	F8 위협 상관 분석
4	**경계 확인**	시설별 배치 정보와 네트워크 구성 기준으로 발생 현황을 조회해, 확산이 같은 시설 안에 머물렀는지 다른 구간까지 넘어갔는지 확인한다.	F8 위협 상관 분석 · F4 네트워크 현황
5	**위장 확인**	네트워크 탐지의 MAC 변경 이벤트를 대조해, 자산이 식별 정보를 바꿔 추적을 회피한 구간이 있는지 확인한다.	F5 네트워크 탐지(MAC 변경)
6	**일괄 조치**	확산 경로에 포함된 자산의 이벤트를 하나의 이슈로 묶어 격리 범위를 확정하고, 종결 시 포함 이벤트를 일괄 종료한다.	F6 이슈 관리

▪ 기대 효과

- 격리 범위를 감으로 정하지 않는다. 확산 경로에 실제로 포함된 자산이 목록으로 확정된다.
- 경계 장비를 거치지 않는 내부 자산 간 전파를 패시브 수집만으로 관측한다.
- MAC 변경 후 전파까지 경로에 포함되어, 위장으로 끊긴 추적을 다시 이어 붙인다.

A-06 제어망에서 외부로의 비인가 통신이 발생했을 때

> **상황**
> 제어망 내 설비가 사설 IP 대역을 벗어나 공인 IP와 통신했다. 원격 유지보수 목적일 수도 있고, 악성코드의 외부 통신일 수도 있다.

▪ 기존 환경에서의 문제

- 제어망은 물리적으로 분리되어 있다고 전제하지만, 실제로는 임시 회선·업무망 연결·무선 단말 등 경로가 존재한다.
- 경로가 존재한다는 사실 자체가 문서화되어 있지 않아, 통신 발생을 이상으로 인지하지 못한다.
- 방화벽 로그만으로는 「어느 제어 설비가」「무슨 목적으로」 나갔는지 판단하기 어렵다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**정책 정의**	IP 정책 · 통신 정책 · 서비스(Port) 정책을 White List / Black List로 등록하고 사용 여부를 관리한다.	F7 네트워크 정책 · IP 목록 · PORT 목록
2	**탐지**	공인 IP 통신 및 자산 정책 위배(DETECT 정책) 통신이 「비인가 정책 탐지」로 발생한다.	F5 네트워크 탐지
3	**주체 확인**	자산 상세에서 해당 자산의 알림 목록과 네트워크 알림 토폴로지를 조회해 통신 주체와 경로를 확인한다.	F3 자산 상세 · F4 네트워크 현황
4	**내용 확인**	통신 현황과 트래픽 분석에서 통신 내역·프로토콜·포트를 조회하고, 필요 시 패킷 분석으로 내용을 확인한다.	F3 통신 현황 · F4 트래픽 분석 · 패킷 분석
5	**판정**	정당한 원격 유지보수라면 정책에 반영하고, 그렇지 않으면 위협 상관 분석으로 다른 자산의 유사 통신 여부를 확인한다.	F7 정책 등록 · F8 위협 상관 분석
6	**조치·전파**	이슈로 등록해 조치 결과를 기록하고, 정책 변경 사항은 전 지역에 동기화한다.	F6 이슈 관리 · F7 정책 동기화

▪ 기대 효과

- 「폐쇄망이므로 외부 통신은 없다」는 전제를 실측 데이터로 검증한다.
- 허용된 통신과 그렇지 않은 통신이 정책으로 명확히 구분되어 판단 기준이 생긴다.
- 정책 동기화로 한 곳에서 발견한 사안이 전 사업장 기준으로 즉시 반영된다.

A-07 자산 정보를 위장해 우회 접속을 시도할 때

> **상황**
> 기존에 등록된 정상 자산의 IP를 그대로 사용하면서 MAC 주소만 다른 통신이 관측되었다. IP 기준 접근통제만 적용된 환경에서는 정상 통신으로 처리된다.

▪ 기존 환경에서의 문제

- IP 기반 화이트리스트만 운영하면 IP 도용·MAC 변경 방식의 우회를 차단할 수 없다.
- 자산 대장이 IP 중심으로만 관리되어 MAC 변경 사실을 대조할 기준 데이터가 없다.
- 변경이 정상적인 부품 교체(NIC 교체)인지 위장인지 구분할 근거가 없다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**기준 확보**	자산을 IP / MAC 기준으로 자동 식별해 등록하고, S/W 명칭·버전, H/W Spec 등 상세 정보를 함께 관리한다.	F3 자산 현황 · 자산 등록
2	**탐지**	등록된 자산의 MAC이 변경되면 「네트워크 이상 탐지」의 MAC 변경 이벤트가 발생한다.	F5 네트워크 탐지
3	**통계 확인**	알림 상세에서 신규 MAC 탐지 통계를 조회해 변경 시점과 빈도를 확인한다.	F5 신규 MAC 탐지 통계
4	**물리 대조**	캐비닛 관리와 시설 목록에서 해당 자산의 물리적 설치 위치를 확인해 실제 작업 이력과 대조한다.	F3 캐비닛 관리
5	**전파 확인**	악성코드 탐지의 「MAC 변경 후 전파」 경로 및 위협 상관 분석으로 후속 이상 통신 여부를 확인한다.	F5 악성코드 탐지 · F8 위협 상관 분석
6	**반영**	정상 교체로 확인되면 자산 정보를 수정하고, 위장으로 판정되면 이슈 등록 후 차단 정책을 반영한다.	F3 자산 수정 · F6 이슈 관리 · F7 정책

▪ 기대 효과

- IP 단독이 아닌 IP·MAC 복합 기준으로 자산을 식별해 위장 접속을 탐지한다.
- 물리 배치 정보(캐비닛·시설)와 대조해 정상 교체와 위장을 구분한다.
- 자산 정보 변경 이력이 시스템에 남아 다음 점검 시 근거가 된다.

A-08 하나의 자산에서 시작된 위협이 확산될 때

> **상황**
> 한 대의 운영자 PC에서 발생한 이벤트가 단발성으로 보였으나, 며칠에 걸쳐 인접 자산에서 유사한 이벤트가 순차적으로 발생했다.

▪ 기존 환경에서의 문제

- 이벤트를 개별 알람 단위로만 보면 각각은 경미해 보여 후순위로 밀린다.
- 자산별·시간대별로 흩어진 이벤트를 사람이 연결해서 보는 데는 한계가 있다.
- 확산이 인지되는 시점에는 이미 다수 자산이 영향을 받은 뒤다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**자산 기준 집계**	위협 스캐닝이 1일 단위로 자산별 보안 이벤트 탐지 이력을 모아 요약 정보를 생성한다.	F8 위협 스캐닝
2	**연관성 분석**	위협 스캐닝 상세에서 해당 자산의 네트워크 레이아웃·정책·취약점 목록·악성코드 목록을 함께 조회해 이벤트 간 연관성을 판단한다.	F8 위협 스캐닝 상세
3	**범위 확대**	위협 상관 분석에서 탐지 자산을 기점으로 이전·이후 시간대 연계 자산의 이벤트를 검색한다.	F8 위협 상관 분석
4	**전파 경로 도출**	동일·유사 이벤트가 자산 간 연속 발생한 흐름을 확인하고, 시설별 배치 정보와 네트워크 구성 기반으로 발생 현황을 조회한다.	F8 상관 분석 결과 · F4 네트워크 현황
5	**통합 대응**	전파 경로상의 이벤트를 하나의 이슈로 통합 등록해 단일 사안으로 관리한다.	F6 이슈 관리
6	**종결·보고**	조치 완료 후 이슈를 종료하면 포함된 이벤트가 일괄 종료되고 대시보드 조회 대상에서 제외된다. 결과는 보고서로 발행한다.	F6 이슈 종료 · F9 보고서

▪ 기대 효과

- 개별 알람이 아니라 자산 기준·네트워크 기준으로 위협을 본다.
- 전파 경로가 가시화되어 어디까지 조치해야 하는지 결정할 수 있다.
- 연관 이벤트를 하나의 이슈로 묶어 중복 대응과 누락을 동시에 방지한다.

A-09 프린터를 통해 제어 자료가 무단 출력될 때

> **상황**
> 제어망 내 프린터에서 업무 시간 외에 대량 출력이 발생했다. 출력물은 물리적으로 반출되면 추적이 불가능하다.

▪ 기존 환경에서의 문제

- 네트워크 프린터는 제어망 자산으로 관리되지 않는 경우가 많아 감시 사각지대에 있다.
- 출력은 정상 업무 행위와 형태가 같아 로그만으로는 이상 여부를 판단하기 어렵다.
- 출력물 반출은 네트워크를 거치지 않아 사후 추적 수단이 없다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**자산 등록**	프린터를 자산으로 식별·등록하고 통신 현황에서 사용 포트·프로토콜을 확인한다.	F3 자산 현황 · 통신 현황
2	**탐지**	자체 탐지 기능으로 프린터 사용을 탐지하고 프린터 사용 탐지 목록에 기록한다.	F5 프린터 사용 탐지
3	**상세 확인**	프린터 사용 탐지 상세를 조회해 프린터와 통신한 자산 및 발생 시점을 확인한다. (네트워크 통신 기준이며 출력물 내용은 대상이 아니다)	F5 프린터 사용 탐지 상세
4	**경로 확인**	네트워크 알림 토폴로지에서 어느 자산에서 프린터로 통신이 발생했는지 확인한다.	F5 네트워크 알림 토폴로지
5	**패턴 분석**	트래픽 분석에서 호기·IP·Port 필터로 시간대별 사용 패턴을 조회해 정상 업무 패턴과 대조한다.	F4 트래픽 분석
6	**기록**	이상으로 판정되면 이슈로 등록하고, 정기 보고서에 출력 현황을 포함해 발행한다.	F6 이슈 관리 · F9 보고서

▪ 기대 효과

- 관리 사각지대였던 출력 행위가 탐지 대상으로 편입된다.
- 프린터와 통신한 자산·시점·경로가 기록되어 내부 통제 근거가 확보된다.
- 시간대별 패턴 대조로 업무 외 시간 이상 출력을 선별할 수 있다.

A-10 트래픽 급변·통신 중단 등 설비 이상 징후가 나타날 때

> **상황**
> 특정 설비의 통신량이 평소의 수 배로 급증하거나, 반대로 일정 기간 통신이 완전히 끊겼다. 제어 시스템 자체 알람에는 나타나지 않았다.

▪ 기존 환경에서의 문제

- 제어 시스템 알람은 공정 값 기준이어서 네트워크 계층의 이상을 잡아내지 못한다.
- 통신 중단이 설비 정지 때문인지 네트워크 문제인지 보안 사고인지 구분되지 않는다.
- 「평소 대비」를 판단할 기준선(baseline)이 현장에 축적되어 있지 않다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**기준 설정**	자산 상세에서 자산별 트래픽 임계치를 설정·갱신한다.	F3 자산 상세 트래픽 임계치
2	**탐지**	임계치를 초과하는 이상 트래픽(급변) 및 설정 일자 기준 운영 정지가 「네트워크 이상 탐지」로 발생한다.	F5 네트워크 탐지
3	**추이 확인**	알림 상세의 트래픽 통계 차트에서 발생 전후 추이를 확인한다.	F5 트래픽 통계 차트
4	**전체 대조**	이벤트 대시보드에서 수집망별 트래픽을 조회해 해당 설비만의 현상인지 수집망 전체 현상인지 대조한다.	F2 이벤트 대시보드
5	**원인 구분**	통신 내역과 프로토콜별 통계를 조회해 정상 통신량 증가인지 비정상 통신 발생인지 구분한다.	F4 트래픽 분석
6	**연계 확인**	위협 스캐닝으로 해당 자산의 당일 이벤트 이력을 확인해 보안 이벤트와의 동반 발생 여부를 판단한다.	F8 위협 스캐닝

▪ 기대 효과

- 공정 알람이 감지하지 못하는 네트워크 계층의 이상을 조기에 포착한다.
- 자산별 임계치로 설비 특성에 맞는 기준선을 운영한다.
- 설비 문제와 보안 사고를 같은 화면에서 구분해 대응 부서를 신속히 정한다.

Part B 운영 업무 프로세스 시나리오

제어시스템 보안 담당자의 일상 업무 10개 프로세스와, 각 단계에서 ICS Security Monitor가 수행하는 역할입니다.

시나리오	업무	핵심 활용 기능
B-01	신규 설비를 반입해 자산으로 등록해야 할 때	F3 · F4
B-02	정기 자산 실사와 대장 현행화를 수행할 때	F3 · F9
B-03	설비의 물리 배치와 네트워크 구성을 현행화할 때	F3 · F4 · F5 · F8
B-04	보안 정책을 수립하고 다수 사업장에 배포할 때	F7
B-05	취약점 탐지 룰을 최신 상태로 유지해야 할 때	F7 · F2
B-06	악성코드 탐지 결과를 판정하고 근거를 남겨야 할 때	F5 · F8 · F3 · F6 · F9
B-07	오탐이 많아 알람을 신뢰할 수 없을 때	F2 · F7 · F5 · F4 · F6 · F9
B-08	일상 관제 — 이벤트 확인부터 이슈 종결까지	F2 · F5 · F6
B-09	정기 보안 보고서를 작성해 제출해야 할 때	F9 · F3 · F4
B-10	사용자 권한을 관리하고 접근 이력을 감사할 때	F10

B-01 신규 설비를 반입해 자산으로 등록해야 할 때

> **상황**
> 설비 증설로 20여 대의 신규 장비가 제어망에 편입된다. 각 장비의 IP·MAC·용도·설치 위치를 자산 대장에 반영해야 한다.

▪ 기존 환경에서의 문제

- 자산 대장이 엑셀로 관리되어 등록 담당자마다 표기 방식이 다르고 중복·오기가 발생한다.
- 실제 통신하는 IP와 대장상 IP가 일치하는지 검증할 수단이 없다.
- 등록 누락 시 해당 설비는 이후 모든 탐지·분석에서 빠진다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**양식 확보**	자산 업로드 시트에서 표준 업로드 양식을 다운로드한다.	F3 자산 업로드 양식 다운로드
2	**작성·검증**	양식에 신규 자산 정보를 작성해 업로드하면 시스템이 데이터 검증을 수행해 오류를 사전에 표시한다.	F3 자산 업로드 데이터 검증
3	**일괄 등록**	검증을 통과한 자산을 엑셀 업로드로 일괄 등록한다. 개별 등록도 팝업에서 가능하다.	F3 자산 엑셀 업로드 · 자산 등록
4	**실측 대조**	통신 현황에서 수집 IP 목록(수집·미수집)을 조회해 실제 통신하는 IP와 등록 내역을 대조한다.	F3 통신 현황
5	**누락 보완**	대장에 없으나 통신이 관측되는 IP는 「기존 자산에 등록」으로 편입하거나 신규 자산으로 등록한다.	F3 기존 자산에 등록
6	**위치 반영**	캐비닛을 등록하고 자산을 배치한 뒤, 네트워크 현황에서 Grid 토폴로지의 장소 위치와 계층 구조를 편집한다.	F3 캐비닛 관리 · F4 네트워크 현황 편집

▪ 기대 효과

- 표준 양식 + 자동 검증으로 등록 품질이 담당자와 무관하게 균일해진다.
- 실측 통신 데이터와 대조되어 「대장에는 있는데 없는 자산」·「있는데 대장에 없는 자산」이 드러난다.
- 논리 정보(IP·MAC)와 물리 정보(캐비닛·시설·위치)가 한 시스템에서 연결된다.

B-02 정기 자산 실사와 대장 현행화를 수행할 때

> **상황**
> 연 1회 자산 실사를 앞두고 제어망 자산 대장의 정확도를 확인해야 한다. 최근 몇 년간 설비 교체와 폐기가 반복되었다.

▪ 기존 환경에서의 문제

- 실사는 현장 육안 확인에 의존해 인력과 시간이 많이 들고, 확인하지 못한 구간이 남는다.
- 폐기된 설비가 대장에 남아 있거나, 교체된 설비가 반영되지 않은 채 방치된다.
- 실사 결과를 다음 실사까지 유지·관리할 체계가 없어 1년 뒤 다시 원점이 된다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**현황 확보**	자산 현황에서 수집·미수집·폐기 상태별 자산 목록을 조회한다.	F3 자산 목록 조회
2	**미수집 식별**	일정 기간 통신이 관측되지 않은 「미수집」 자산을 추출해 현장 확인 대상으로 선정한다.	F3 자산 현황
3	**미등록 식별**	통신 현황에서 수집되고 있으나 자산으로 등록되지 않은 IP·MAC을 추출한다.	F3 통신 현황
4	**현장 확인**	캐비닛·시설 목록으로 대상 자산의 물리 위치를 특정해 현장 확인 동선을 최소화한다.	F3 캐비닛 관리
5	**반영**	확인 결과에 따라 자산 정보를 수정하고, 일괄 수정 화면에서 대상 자산 정보를 조회해 반영한다. 사용 종료 자산은 폐기 처리한다.	F3 자산 수정 · 일괄 수정 · 자산 폐기
6	**산출·보고**	자산 목록과 통신 현황을 엑셀로 다운로드해 실사 결과 자료로 제출하고, 보고서를 발행한다.	F3 엑셀 다운로드 · F9 보고서

▪ 기대 효과

- 실측 통신 데이터가 실사의 출발점이 되어 확인 대상이 대폭 줄어든다.
- 「대장에만 있는 자산」과 「대장에 없는 자산」이 동시에 드러난다.
- 실사 결과가 시스템에 반영되어 다음 해에 처음부터 다시 하지 않는다.

B-03 설비의 물리 배치와 네트워크 구성을 현행화할 때

> **상황**
> 제어반 개조 공사로 다수 설비의 캐비닛 배치가 변경되었다. 기존 배치도는 도면 파일로만 존재해 갱신이 지연되고 있다.

▪ 기존 환경에서의 문제

- 네트워크 구성도와 물리 배치도가 별도 문서로 관리되어 서로 어긋난다.
- 장애 발생 시 「어느 설비가 어디에 있는가」를 파악하는 데 시간이 걸린다.
- 도면 갱신이 담당자 개인 작업이어서 갱신 이력과 최신본 여부를 신뢰하기 어렵다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**캐비닛 등록**	캐비닛 관리에서 캐비닛과 시설 목록을 등록하고 캐비닛 정보를 관리한다.	F3 캐비닛 등록
2	**자산 배치**	캐비닛별로 수용 자산을 지정하고, 변경 시 캐비닛 자산 변경으로 반영한다.	F3 캐비닛 자산 변경
3	**토폴로지 확인**	네트워크 현황에서 Grid 토폴로지와 Node 토폴로지를 조회해 논리 구성을 확인한다.	F4 네트워크 현황
4	**위치 편집**	장소 위치 편집 팝업에서 자산 목록을 조회하며 Grid 토폴로지의 장소 위치를 실제 배치에 맞게 편집한다.	F4 장소 위치 편집
5	**계층 정리**	계층형 구조 내 자산 순서를 수정하고 필요한 자산을 등록·삭제해 구성도를 정리한다.	F4 계층 구조 편집
6	**활용**	정리된 배치·구성 정보는 이벤트 알림 토폴로지와 위협 상관 분석의 시설 연관성 판단에 그대로 활용된다.	F5 알림 토폴로지 · F8 위협 상관 분석

▪ 기대 효과

- 물리 배치와 네트워크 구성이 하나의 시스템에서 관리되어 불일치가 사라진다.
- 별도 도면 관리 작업이 시스템 입력으로 대체되어 최신본 문제가 해소된다.
- 배치 정보가 보안 이벤트 분석에 직접 활용되어 관리 노력이 탐지 정확도로 환원된다.

B-04 보안 정책을 수립하고 다수 사업장에 배포할 때

> **상황**
> 본사에서 제어망 통신 정책 기준을 개정했다. 전국 사업장에 동일하게 적용하고, 적용 여부를 확인해야 한다.

▪ 기존 환경에서의 문제

- 사업장별로 담당자가 개별 적용해 반영 시점과 내용이 제각각이 된다.
- 적용 여부를 확인하려면 사업장마다 확인 요청을 보내고 회신을 기다려야 한다.
- 일부 사업장의 미반영이 장기간 방치되어 전사 보안 수준이 균일해지지 않는다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**정책 등록**	정책 관리 등록 페이지에서 네트워크 정책을 등록하고, IP 목록·PORT 목록을 관리한다.	F7 네트워크 정책 · IP 목록 · PORT 목록
2	**검토**	정책 목록과 정책 조회 팝업에서 등록 내용을 검토하고 사용 여부를 설정한다.	F7 정책 조회 · 사용여부 수정
3	**배포**	정책 관리 동기화 팝업에서 대상을 지정해 정책을 동기화한다. 취약점 탐지 정책도 동일하게 동기화한다.	F7 정책 동기화 · 취약점 탐지 정책 동기화
4	**반영 확인**	취약점 탐지 정책의 본사 동기화 여부와 상태를 확인해 반영 여부를 점검한다.	F7 본사 동기화 상태 확인
5	**실효 확인**	수집 IP 상태 목록과 PORT 목록 수집 상태를 조회해 정책이 실제 통신에 어떻게 대응하는지 확인한다.	F7 수집 IP/PORT 상태 조회
6	**변수 관리**	취약점 탐지 정책의 네트워크 변수를 사업장 환경에 맞게 등록·수정해 룰 적용 범위를 조정한다.	F7 네트워크 변수 관리

▪ 기대 효과

- 정책 배포가 요청·회신이 아니라 시스템 동기화로 처리된다.
- 취약점 탐지 정책은 본사 동기화 여부와 상태를 확인해 반영 여부를 점검할 수 있다.
- 공통 기준은 일괄 배포하고 사업장별 차이는 네트워크 변수로 흡수한다.

B-05 취약점 탐지 룰을 최신 상태로 유지해야 할 때

> **상황**
> 도입 시점에 적용한 룰셋을 1년 넘게 그대로 쓰고 있다. 그 사이 새로운 공격 기법이 여럿 알려졌지만, 폐쇄망이라 룰을 어떻게 받아 적용해야 하는지 절차가 정해져 있지 않다.

▪ 기존 환경에서의 문제

- 제어망은 외부와 연결되지 않아, IT 보안장비처럼 자동으로 룰을 내려받는 방식이 성립하지 않는다.
- 룰을 갱신하면 그동안 맞춰 둔 예외처리가 초기화되지 않을지, 새 룰이 정상 제어 통신을 오탐하지 않을지 확신할 수 없어 갱신 자체를 미루게 된다.
- 갱신했더라도 사업장마다 반영 시점이 달라지면, 전사 보안 수준이 언제부터 균일해졌는지 말할 수 없다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**수신**	패치와 룰 콘텐츠를 고객 포털에서 내려받는다. C1(현장형) 사업장은 오프라인 매체로 전달받는다.	유지보수 일반서비스 — 패치 제공
2	**적용**	Snort Community rule은 배포본 기준으로 재배포하고, 제어망 상황에 맞춘 Custom rule은 취약점 유형별로 등록한다.	F7 취약점 탐지 정책 관리
3	**범위 조정**	정책 그룹 목록과 룰 상세 목록을 조회해 새로 들어온 룰 가운데 이 사업장에 해당하지 않는 룰을 Bypass 또는 Off로 설정한다.	F7 룰 세부 설정(예외처리·비활성화)
4	**변수 정합**	네트워크 변수 목록을 조회해 사업장 대역·설비 구성이 바뀐 부분을 반영하고, 정책 룰 상세 목록에서 기존 예외처리 설정이 남아 있는지 확인한다.	F7 네트워크 변수 관리 · 룰 상세 목록 조회
5	**배포**	정책 동기화 팝업에서 대상을 지정해 갱신된 취약점 탐지 정책을 사업장에 동기화한다.	F7 정책 동기화
6	**반영 확인**	본사 동기화 여부와 상태를 확인해 정책이 정상 반영됐는지 점검하고, 갱신 직후 며칠간 알람 통계로 발생량 변화를 관찰해 신규 룰의 오탐 여부를 확인한다.	F7 본사 동기화 상태 확인 · F2 알람 통계

▪ 기대 효과

- 폐쇄망에서도 룰 갱신 경로가 절차로 정해진다. 포털 내려받기 또는 오프라인 매체 전달 두 경로가 계약에 포함되어 있다.
- 전체 룰셋 교체가 아니라 룰 단위 Bypass · Off로 조정하므로, 축적한 예외처리를 유지한 채 신규 룰만 더한다.
- 동기화 여부와 상태를 화면에서 확인할 수 있어, 갱신이 실제로 반영됐는지를 추정이 아니라 조회로 확인한다.

※ 룰 갱신 후 오탐 튜닝은 유지보수 서비스의 정기 방문 점검 항목에 포함됩니다. 패치는 연 2회 제공됩니다.

B-06 악성코드 탐지 결과를 판정하고 근거를 남겨야 할 때

> **상황**
> 악성코드 탐지 이벤트가 발생했다. 상급 기관에 보고해야 하는 사안인지, 오탐으로 정리할 사안인지 판단해야 하는데, 「탐지되었다」는 사실 외에 근거로 제시할 자료가 없다.

▪ 기존 환경에서의 문제

- 탐지 사실만으로는 대응 수준을 정할 수 없다. 실행 가능한 파일이 실제로 전달된 것인지, 검사기가 이름만 보고 잡은 것인지에 따라 보고 여부가 갈린다.
- 제어 설비에 백신이 없거나 패턴이 오래된 상태라, 자산 쪽에서 교차 확인할 방법이 없다.
- 판정 근거를 남기지 않으면 몇 달 뒤 감사에서 같은 사안을 다시 조사해야 한다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**결과 조회**	알림 상세에서 파일 검사 결과를 조회해 시스템 제공 백신(Windows Defender)의 판정 내용과 악성코드 종류를 확인한다.	F5 파일 검사 결과 조회 (Defender)
2	**경로 대조**	악성코드 탐지 알림 토폴로지에서 전달 경로를 확인하고, 해당 경로가 그 자산의 평소 통신과 부합하는지 대조한다.	F5 악성코드 탐지 알림 토폴로지
3	**이력 집계**	위협 스캐닝 상세의 악성코드 목록으로 해당 자산의 1일 단위 이력을 집계해, 단발 이벤트인지 반복 발생인지 확인한다.	F8 위협 스캐닝 — 악성코드 목록
4	**연계 확인**	위협 스캐닝 상세에서 해당 자산의 취약점 탐지 목록을 함께 조회하고, 자산 상세 알림 목록으로 같은 자산의 네트워크 탐지 알림까지 대조해 단독 이벤트인지 일련의 공격 흐름의 일부인지 판단한다.	F8 위협 스캐닝 상세 · F3 자산 상세 알림 목록
5	**판정 기록**	판정 결과와 근거를 이슈의 원인 분석·조치 내용에 기록한다. 개별 알림에 대한 메모도 함께 남긴다.	F6 이슈 관리 — 조치 내용 · 알림 메모
6	**증적화**	탐지 현황과 이슈 관리 데이터를 선택해 보고서를 발행하고, 이슈 상세는 CSV로 함께 발행해 보관한다.	F9 보고서 관리

▪ 기대 효과

- 「탐지됨」이 아니라 「무엇이 어떤 경로로 전달되어 어떻게 판정되었는가」가 기록된다. 보고 여부를 근거를 갖고 결정한다.
- 자산에 백신이 없어도 네트워크 전송 단계의 검사 결과가 판정 근거로 남는다.
- 판정과 근거가 이슈에 축적되어, 감사 시점에 조사가 아니라 조회로 대응한다.

※ 탐지는 네트워크 전송 단계에서 시스템 제공 백신으로 수행됩니다. 자산에 설치된 백신을 대체하지 않으며, 파일이 네트워크를 거치지

않고 유입된 경우(직접 매체 연결 등)는 탐지 대상이 아닙니다.

B-07 오탐이 많아 알람을 신뢰할 수 없을 때

> **상황**
> 도입 초기 하루 수백 건의 알람이 발생하고 대부분이 정상 제어 통신이다. 담당자가 알람을 확인하지 않게 되는 상태에 이르렀다.

▪ 기존 환경에서의 문제

- 제어 프로토콜은 IT 환경 기준 룰셋에 비정상으로 잡히는 경우가 많다.
- 오탐을 줄이려고 룰을 통째로 끄면 실제 위협까지 놓친다.
- 어떤 룰이 얼마나 오탐을 유발하는지 정량적으로 파악할 수단이 없다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**현황 파악**	이벤트 대시보드의 수집망별 알람 통계로 유형별(네트워크·취약점·악성코드) 발생량 분포를 확인한다.	F2 알람 통계
2	**룰 확인**	탐지 목록에서 반복 발생한 알람의 룰을 확인한 뒤, 취약점 탐지 정책 관리에서 정책 그룹 목록과 해당 룰 상세를 조회한다.	F7 취약점 탐지 정책 관리
3	**내용 검증**	해당 알람의 상세와 패킷 분석 결과로 실제 통신 내용을 확인해 오탐 여부를 판정한다.	F5 알림 상세 · F4 패킷 분석
4	**룰 조정**	룰 상세 팝업에서 세부 설정을 변경한다. 예외처리 또는 비활성화를 룰 단위로 적용한다.	F7 룰 세부 설정(예외처리·비활성화)
5	**변수 조정**	네트워크 변수를 사업장 대역·설비 구성에 맞게 수정해 룰의 적용 대상을 정밀화한다.	F7 네트워크 변수 수정
6	**유형별 판정**	악성코드 탐지 알람은 룰 조정 대상이 아니다. 파일 검사 결과와 전달 경로를 확인해 개별 판정하고, 판정 근거를 이슈에 기록해 같은 사안이 반복 조사되지 않게 한다.	F5 파일 검사 결과 · F6 이슈 관리
7	**확산**	정리된 룰 설정을 정책 동기화로 반영하고, 조정 후 발생량 변화는 탐지 현황·정책 현황을 선택해 보고서로 발행해 확인한다.	F7 정책 동기화 · F9 보고서 발행

▪ 기대 효과

- 룰 단위 예외처리로 탐지 범위를 유지한 채 오탐만 제거한다.
- 취약점 탐지는 룰 조정으로, 악성코드 탐지는 개별 판정으로 — 유형에 맞는 방식으로 정리한다.
- 조정한 룰 설정을 정책 동기화로 반영해, 사업장마다 같은 튜닝을 처음부터 반복하지 않는다.
- 알람 신뢰도가 회복되어 관제가 실제로 작동한다.

※ 오탐 튜닝은 유지보수 서비스의 정기 방문 점검 항목에 포함되어, 도입 이후에도 지속적으로 수행됩니다.

B-08 일상 관제 — 이벤트 확인부터 이슈 종결까지

> **상황**
> 관제 담당자가 근무 교대 시 전일 발생 이벤트를 확인하고, 조치가 필요한 건을 처리한 뒤 인계해야 한다.

▪ 기존 환경에서의 문제

- 이벤트가 유형별로 다른 화면에 흩어져 있어 전체 상황을 파악하는 데 시간이 걸린다.
- 조치 진행 상황이 개인 메모나 메신저로 관리되어 교대 시 누락된다.
- 「누가 언제 무엇을 판단했는가」가 남지 않아 감사 대응이 어렵다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**현황 확인**	이벤트 대시보드에서 수집망별 트래픽과 알람 통계, 알람 목록 팝업, 미확인 IP를 확인한다.	F2 이벤트 대시보드
2	**개별 검토**	네트워크·취약점·악성코드·프린터 탐지 목록을 스크롤 또는 테이블 레이아웃으로 조회하며 상세를 확인한다.	F5 실시간 이벤트 분석
3	**이슈 등록**	조치가 필요한 이벤트를 선택해 하나의 이슈로 등록한다. 등록 시 네트워크·취약점·악성코드 알람 목록에서 관련 건을 함께 담는다.	F6 이슈 등록
4	**분석**	이슈 상세에서 토폴로지와 각 알림 상세를 조회해 원인을 분석하고, 알림별 메모를 기록한다.	F6 이슈 상세 · 알림 메모
5	**조치 기록**	조치 내용을 수정·갱신해 진행 상황을 남긴다. 이슈 보드에서 전체 진행 현황을 공유한다.	F6 조치 내용 수정 · 이슈 보드
6	**종결**	조치 완료 후 이슈를 종료하면 포함된 이벤트가 일괄 종료되어 대시보드 조회 대상에서 제외된다.	F6 이슈 종료

▪ 기대 효과

- 대시보드 → 이벤트 → 이슈 → 종결로 이어지는 단일 동선으로 관제가 표준화된다.
- 조치 이력이 시스템에 남아 교대 인계와 감사 추적(Audit trail)이 동시에 해결된다.
- 종결된 이벤트가 화면에서 정리되어 미처리 건에 집중할 수 있다.

B-09 정기 보안 보고서를 작성해 제출해야 할 때

> **상황**
> 월간·분기 보안 현황 보고서를 상급 기관과 경영진에 제출해야 한다. 현재는 각 시스템에서 자료를 내려받아 수작업으로 편집한다.

▪ 기존 환경에서의 문제

- 자료 취합과 편집에 담당자 수 일이 소요되고, 그 기간 동안 본연의 관제 업무가 지연된다.
- 작성자마다 집계 기준이 달라 기간 간 비교가 어렵다.
- 수작업 과정에서 누락·오기가 발생하고, 원본 대조가 번거롭다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**대상 선택**	보고서 관리에서 신규 발행 팝업을 열고 발행 대상 데이터(이벤트 탐지 현황·정책 현황·이슈 관리)를 선택한다.	F9 보고서 신규 발행
2	**발행**	선택한 데이터를 PDF 형태로 자동 정리해 발행한다.	F9 보고서 발행
3	**상세 첨부**	이슈 관리 상세 내역은 CSV로 추가 발행해 근거 자료로 첨부한다.	F9 이슈 CSV 발행
4	**보조 자료**	필요 시 자산 목록·통신 현황·통신 내역을 엑셀로 다운로드해 부속 자료로 사용한다.	F3 · F4 엑셀 다운로드
5	**이력 관리**	발행 파일 목록에서 과거 보고서를 조회·다운로드해 기간 간 비교에 활용한다.	F9 발행 파일 목록
6	**정리**	보존 기간이 지난 보고서는 삭제해 이력을 관리한다.	F9 보고서 삭제

▪ 기대 효과

- 수 일이 걸리던 보고서 작성이 발행 대상 선택 단위 작업으로 축소된다.
- 집계 기준이 시스템으로 고정되어 기간 간 비교가 성립한다.
- 발행 이력이 남아 감사·점검 시 증적으로 즉시 제출할 수 있다.

B-10 사용자 권한을 관리하고 접근 이력을 감사할 때

> **상황**
> 본사 관제 요원, 사업소 담당자, 협력업체 인력이 같은 시스템을 사용한다. 각자 볼 수 있는 자산 범위와 수행 가능한 작업이 달라야 한다.

▪ 기존 환경에서의 문제

- 계정을 공용으로 사용해 누가 어떤 작업을 했는지 구분되지 않는다.
- 권한이 세분화되지 않아 담당 범위를 벗어난 자산 정보까지 열람된다.
- 퇴직·전보 시 계정 정리가 지연되어 유효한 계정이 방치된다.

▪ ICS Security Monitor 의 해결 절차

	단계	수행 내용	사용 기능
1	**권한 정의**	권한 관리에서 역할별 권한을 등록하고 필요 시 업데이트한다.	F10 권한 관리
2	**계정 생성**	사용자 등록 페이지에서 개인별 계정을 생성하고 권한을 부여한다.	F10 계정 생성
3	**범위 확인**	사용자 자산 목록 팝업에서 해당 사용자의 자산 목록을 조회해 담당 범위를 확인한다.	F10 사용자 자산 목록
4	**유지 관리**	인사 변동 시 계정 정보를 업데이트하고, 비밀번호 변경·계정 활성화 상태를 관리한다.	F10 계정 정보 업데이트 · 활성화
5	**감사**	시스템 관리 사용자 로그 탭에서 사용자 로그 목록을 조회해 접근·작업 이력을 확인한다.	F10 사용자 로그
6	**정리**	사용 종료 계정을 삭제하고, 권한 체계 변경 시 불필요한 권한을 삭제한다.	F10 계정 삭제 · 권한 삭제

▪ 기대 효과

- 개인 계정 기반 운영으로 행위 주체가 특정된다.
- 권한 관리로 역할별 권한을 구분하고, 사용자별 자산 목록으로 담당 범위를 확인한다.
- 사용자 로그가 남아 접근통제 감사 요구에 대응할 수 있다.

Part C 고객 문제 해결 시나리오

제어시스템 보안 담당자들이 현장에서 반복적으로 제기하는 8개 문제 제기와, 그에 대한 ICS Security Monitor의 답변입니다.

시나리오	문제 제기	주제
C-01	제어망에 무엇이 연결되어 있는지 정확히 모르겠습니다.	자산 가시성 부재
C-02	폐쇄망이라 안전하다고 하는데, 안전하다는 것을 증명할 수가 없습니다.	망 분리 실효성 입증 불가
C-03	가이드라인 대응 증적을 매번 수작업으로 만듭니다.	규제 대응 부담
C-04	사고가 나도 원인과 경로를 추적할 수가 없습니다.	사후 추적 불가
C-05	본사와 사업소의 보안 현황이 따로 놉니다.	다지역 통합 관리 부재
C-06	보안 장비가 제어 운전에 영향을 줄까 봐 도입이 망설여집니다.	가용성 우려
C-07	담당자가 바뀌면 그동안 쌓인 판단 기준이 사라집니다.	운영 지식의 휘발
C-08	제어망에서는 취약점 스캐너를 돌릴 수 없습니다. 그럼 취약점은 어떻게 봅니까?	능동 취약점 진단 불가

C-01 자산 가시성 부재

> **고객의 말**
> "제어망에 무엇이 연결되어 있는지 정확히 모르겠습니다."

▪ 문제의 배경

- 제어 설비는 수십 년에 걸쳐 증설·교체되어 왔고, 그때마다 자산 대장이 온전히 갱신되지는 않았다.
- 설비 벤더가 납품한 장비 내부에 관리되지 않는 통신 모듈이 포함된 경우가 있다.
- 보안 대책을 세우려 해도 대상 목록 자체가 부정확해 출발점이 서지 않는다.

▪ ICS Security Monitor 의 답

접근	내용	근거 기능
실측 기반 자산 식별	제어망 패킷을 패시브 수집해 IP / MAC 기준으로 자산을 자동 식별한다. 대장이 아니라 실제 통신이 근거가 된다.	F3 자산 현황
미등록 자산 노출	통신 현황에서 수집되고 있으나 등록되지 않은 IP·MAC을, 대시보드에서 미확인 IP를 상시 노출한다.	F3 통신 현황 · F2 미확인 IP
상세 정보 축적	S/W 명칭·버전, H/W Spec 등 BOM 정보를 자산에 추가 관리해 취약점 대응의 기준 데이터로 삼는다.	F3 자산 등록/수정
물리·논리 결합	캐비닛·시설 배치와 Grid/Node 토폴로지를 함께 관리해 논리 구성과 물리 위치를 연결한다.	F3 캐비닛 관리 · F4 네트워크 현황

> **결과**
> 「무엇이 있는지 모른다」에서 「무엇이 있고 무엇이 통신하는지 목록으로 있다」로 전환됩니다. 이후의 모든 정책·탐지·보고가 이 목록 위에서 성립합니다.

C-02 망 분리 실효성 입증 불가

> **고객의 말**
> "폐쇄망이라 안전하다고 하는데, 안전하다는 것을 증명할 수가 없습니다."

▪ 문제의 배경

- 망 분리는 설계상의 전제이며, 시간이 지나면서 임시 회선·유지보수 경로·무선 단말 등으로 실제 상태가 달라진다.
- 「연결이 없다」는 것은 증명하기 어려운 명제여서, 점검 시마다 논쟁이 반복된다.
- 경영진·감독기관에 제출할 객관적 근거 자료가 없다.

▪ ICS Security Monitor 의 답

접근	내용	근거 기능
외부 통신 실측	공인 IP 통신을 「비인가 정책 탐지」로 상시 감시해 외부 통신 발생 여부를 데이터로 확인한다.	F5 네트워크 탐지
정책 대비 검증	IP·통신·서비스 정책을 White/Black List로 정의하고, 정책 위배 통신을 탐지해 설계와 실제의 차이를 드러낸다.	F7 정책 관리
통신 전수 조회	통신 현황과 트래픽 분석에서 호기·IP·Port 기준으로 통신 내역을 조회하고 엑셀로 산출한다.	F3 · F4
증적 발행	탐지 현황·정책 현황을 선택해 PDF 보고서로 발행, 기간별 「외부 통신 없음」을 문서로 입증한다.	F9 보고서

> **결과**
> 망 분리 상태가 주장이 아니라 기간별 실측 데이터로 입증됩니다. 감사·점검 시 제출 자료가 자동으로 축적됩니다.

C-03 규제 대응 부담

> **고객의 말**
> "가이드라인 대응 증적을 매번 수작업으로 만듭니다."

▪ 문제의 배경

- 제어시스템 보안 모니터링 구축 가이드라인 등 요구 사항은 늘어나는데 대응 인력은 그대로다.
- 요구 항목별로 어떤 시스템의 어떤 자료가 근거가 되는지 정리되어 있지 않다.
- 점검 때마다 자료를 새로 만들어야 해서 상시 대응 체계가 되지 않는다.

▪ 제어시스템 보안 모니터링 구축 가이드라인('24.12) 대응

접근	내용	근거 기능
이벤트 모니터링	자산관리와 네트워크·악성코드·취약점 탐지로 이벤트 모니터링 요구를 충족한다.	F3 · F5
위협 시각화	실시간 이벤트 분석, 위협 스캐닝, 위협 상관분석, 패킷 분석으로 위협 시각화 요구를 충족한다.	F5 · F8 · F4
모니터링 역량	통합 대시보드, 네트워크 현황, 이슈 관리로 모니터링 역량 요구를 충족한다.	F2 · F4 · F6
대응 역량	자동 경보와 상위 대응체계 연계 API를 제공해 대응 역량 요구를 충족한다.	상위 기관 연계 인터페이스
증적 자동화	이벤트 탐지 현황·정책 현황·이슈 관리 데이터를 보고서로 발행하고 발행 이력을 관리해 증적으로 제출한다.	F9 보고서

> **결과**
> 가이드라인 대응이 「점검 전 몰아서 하는 일」에서 「상시 축적되는 운영 결과물」로 바뀝니다.

C-04 사후 추적 불가

> **고객의 말**
> "사고가 나도 원인과 경로를 추적할 수가 없습니다."

▪ 문제의 배경

- 제어 설비 자체 로그는 보존 기간이 짧거나 네트워크 계층 정보를 담지 않는다.
- 스위치·방화벽 로그는 존재하더라도 제어 자산 정보와 연결되지 않아 해석이 어렵다.
- 원인 규명 실패는 동일 사고의 재발로 이어진다.

▪ ICS Security Monitor 의 답

접근	내용	근거 기능
통신 이력 보존	수집된 통신 내역과 트래픽 통계를 조회·다운로드해 발생 전후 상황을 재구성한다.	F4 트래픽 분석
패킷 근거	알림 상세에서 패킷 분석을 요청하고 분석 결과 상세를 조회해 실제 통신 내용을 확보한다.	F5 패킷 분석 요청 · F4 패킷 분석
자산 기준 이력	자산 상세에서 해당 자산의 알림 목록과 네트워크 알림 토폴로지를 조회한다.	F3 자산 상세
전파 경로 재구성	위협 상관 분석으로 이전·이후 시간대 연계 자산의 이벤트를 검색해 전파 흐름을 도출한다.	F8 위협 상관 분석
조치 이력	이슈 관리에 기록된 원인 분석·조치 내용·메모가 감사 추적 자료가 된다.	F6 이슈 관리

> **결과**
> 사고 조사가 추정이 아니라 패킷·통신 이력·조치 기록이라는 근거 위에서 수행됩니다.

C-05 다지역 통합 관리 부재

고객의 말

"본사와 사업소의 보안 현황이 따로 놉니다."

▪ 문제의 배경

- 사업소별로 다른 시점에 다른 구성으로 시스템이 도입되어 현황 파악 기준이 통일되지 않는다.
- 본사는 사업소의 보고에 의존하고, 사업소는 본사 기준을 개별 해석한다.
- 전사 관점의 보안 수준을 하나의 숫자로 말할 수 없다.

▪ ICS Security Monitor 의 답

접근	내용	근거 기능
통합 대시보드	수집망별 트래픽·알람 통계를 하나의 대시보드에서 조회해 전사 현황을 단일 화면으로 본다.	F2 이벤트 대시보드
정책 일괄 배포	네트워크 정책과 취약점 탐지 정책을 동기화로 일괄 배포한다.	F7 정책 동기화
반영 상태 확인	취약점 탐지 정책의 본사 동기화 여부와 상태를 확인해 반영 여부를 점검한다.	F7 동기화 상태 확인
협업 체계	이슈 관리로 본사 관제 요원과 사업소 담당자가 같은 건에 대해 정보를 공유하고 조치 결과를 확인한다.	F6 이슈 관리
권한 분리	역할별 권한을 등록해 본사와 사업소의 사용 범위를 구분하고, 사용자별 자산 목록으로 담당 범위를 확인한다.	F10 권한·사용자 관리

결과

본사와 사업소가 같은 데이터를 보고 같은 정책 위에서 일합니다. 전사 보안 수준이 하나의 기준으로 관리됩니다.

C-06 가용성 우려

> **고객의 말**
> "보안 장비가 제어 운전에 영향을 줄까 봐 도입이 망설여집니다."

▪ 문제의 배경

- 제어 설비는 정지 시 생산 손실과 안전 문제로 직결되어 어떤 부하도 허용하기 어렵다.
- 능동 스캔 방식의 자산 식별 도구는 구형 설비에서 오작동을 유발한 사례가 보고된다.
- 에이전트 설치는 설비 벤더의 보증 범위를 벗어나는 경우가 많다.

▪ ICS Security Monitor 의 답

접근	내용	근거 기능
패시브 수집	미러링(SPAN)·탭 포트로 복제된 트래픽만 분석한다. 능동 스캔과 패킷 주입을 수행하지 않는다.	수집 방식
Agentless	자산 식별·네트워크 탐지·취약점 탐지·악성코드 탐지가 모두 네트워크 기반으로 동작해 설비에 설치할 것이 없다.	F3 · F5
구성 유연성	DPI 탐지 서버와 보안 모니터링 서버를 규모에 따라 일체형 또는 분리형으로 구성한다.	구축 모델
현장 검증	2017년 이후 발전 제어망 보안모니터링 현장 구축 경험을 바탕으로 개발되어, 2026년 한국서부발전 제어시스템 통합 보안 모니터링 시스템으로 구축·운영 중이다.	구축 실적

> **결과**
> 제어 프로세스에 대한 개입 없이 보안 가시성을 확보합니다. 도입 리스크가 「설비 영향」이 아니라 「수집 구간 설계」 수준으로 축소됩니다.

C-07 운영 지식의 휘발

> **고객의 말**
> "담당자가 바뀌면 그동안 쌓인 판단 기준이 사라집니다."

▪ 문제의 배경

- 어떤 알람이 오탐이고 어떤 통신이 정상인지에 대한 판단이 담당자 개인 경험에 축적된다.
- 인수인계 문서로는 판단 근거까지 전달되지 않아, 후임자가 처음부터 다시 학습한다.
- 그 기간 동안 탐지 품질과 대응 속도가 저하된다.

▪ ICS Security Monitor 의 답

접근	내용	근거 기능
판단 근거의 시스템화	오탐 판정 결과가 룰 예외처리·비활성화 설정으로 시스템에 반영되어 개인 지식이 아닌 설정으로 남는다.	F7 룰 세부 설정
정상 기준의 명문화	정상 통신에 대한 판단이 IP·통신·서비스 정책과 자산별 트래픽 임계치로 기록된다.	F7 정책 · F3 트래픽 임계치
조치 이력 축적	이슈별 원인 분석·조치 내용·알림 메모가 누적되어 유사 상황의 참조 자료가 된다.	F6 이슈 관리
보고서 이력	기간별 보고서가 보존되어 과거 현황과 추세를 후임자가 직접 확인할 수 있다.	F9 보고서
운영 지원	유지보수 서비스의 정기 방문 점검에서 오탐 튜닝과 자산·취약점 리포트를 지속 제공한다.	유지보수 서비스

> **결과**
> 운영 노하우가 개인이 아니라 시스템에 축적됩니다. 담당자 교체가 보안 수준의 하락으로 이어지지 않습니다.

C-08 능동 취약점 진단 불가

> **고객의 말**
> "제어망에서는 취약점 스캐너를 돌릴 수 없습니다. 그럼 취약점은 어떻게 봅니까?"

▪ 문제의 배경

- 일반적인 취약점 진단 도구는 대상에 요청을 보내 응답으로 판정한다. 구형 제어 설비는 예상하지 못한 요청에 오작동하거나 정지할 수 있어, 운전 중인 제어망에서는 실행 자체가 금지된다.
- 정기 점검 기간에만 스캔하는 방식은 연 1~2회 단면만 남길 뿐, 그 사이에 벌어지는 일을 설명하지 못한다.
- 결과적으로 제어망 취약점 항목은 「점검 불가」로 남고, 감사 때마다 같은 지적이 반복된다.

▪ ICS Security Monitor 의 답

접근	내용	근거 기능
관측 기반 탐지	설비에 요청을 보내지 않는다. 미러링·탭으로 복제한 트래픽을 관측해 공격 시도와 취약 통신을 탐지한다.	패시브 수집
상시 관측	점검 기간에만 보는 것이 아니라 상시 수집·탐지가 이어져, 단면이 아니라 기간 전체가 기록된다.	F5 취약점 탐지
유형 구분	DDoS · Scanning · Session Hijacking · SQL Injection · Spoofing · 무차별 대입 유형으로 구분해 탐지한다.	F7 취약점 탐지 정책
환경 적합화	Snort Community rule에 제어망 Custom rule을 더하고, 룰 단위 예외 처리·비활성화와 네트워크 변수로 사업장 환경에 맞춘다.	F7 룰 세부 설정 · 네트워크 변수
자산 정보 연계	자산 상세 정보에 S/W 명칭·버전, H/W Spec 등 BOM 정보를 추가 관리해 취약점 판단의 참고 자료로 활용한다.	F3 자산 상세 · 제품소개자료 BOM 관리
증적화	탐지 현황을 보고서로 발행해 「점검 불가」가 아니라 기간별 관측 결과로 제출한다.	F9 보고서

> **결과**
> 설비를 건드리지 않고 취약점 관련 활동을 상시 관측합니다. 다만 관측 대상은 네트워크를 오가는 통신이므로, 설비 내부의 미조치 패치 목록을 대신 제시하는 방식과는 성격이 다릅니다. 두 방식은 대체 관계가 아니라 보완 관계입니다.

03 시나리오 – 기능 매핑 종합

본 문서에서 다룬 28개 시나리오가 ICS Security Monitor의 기능 체계 전반을 어떻게 활용하는지 정리한 표입니다. 기능이 특정 영역에 편중되지 않고 탐지 · 분석 · 관제 · 보고 전 계층에 걸쳐 연계 활용되는 통합 운영 구조임을 확인할 수 있습니다.

코드	기능 대분류	활용 시나리오
F1	**로그인/로그아웃**	전 시나리오 공통 (시스템 접근 기반)
F2	**대시보드**	A-01, A-03, A-10, B-05, B-07, B-08, C-01, C-03, C-05
F3	**자산 관리**	A-01, A-02, A-03, A-06, A-07, A-09, A-10, B-01, B-02, B-03, B-06, B-09, C-01, C-02, C-03, C-04, C-06, C-07, C-08
F4	**네트워크 현황**	A-01, A-03, A-04, A-05, A-06, A-08, A-09, A-10, B-01, B-03, B-07, B-09, C-01, C-02, C-03, C-04
F5	**실시간 이벤트 분석**	A-01, A-02, A-03, A-04, A-05, A-06, A-07, A-09, A-10, B-03, B-06, B-07, B-08, C-02, C-03, C-04, C-06, C-08
F6	**이슈 관리**	A-01, A-02, A-03, A-04, A-05, A-06, A-07, A-08, A-09, B-06, B-07, B-08, C-03, C-04, C-05, C-07
F7	**정책**	A-01, A-03, A-04, A-06, A-07, B-04, B-05, B-07, C-02, C-05, C-07, C-08
F8	**위협 분석**	A-02, A-03, A-05, A-06, A-07, A-08, A-10, B-03, B-06, C-03, C-04
F9	**보고서**	A-08, A-09, B-02, B-06, B-07, B-09, C-02, C-03, C-07, C-08
F10	**설정**	B-10, C-05

▪ 시나리오 전체 목록

구분	번호	제목
Part A	**A-01**	인가되지 않은 장비가 제어망에 연결되었을 때
Part A	**A-02**	외부 경로를 통해 악성코드가 제어망에 유입되었을 때
Part A	**A-03**	제어망 내부에서 정찰·스캐닝 행위가 발생했을 때
Part A	**A-04**	알려진 공격 기법이 제어망 트래픽에서 관측될 때
Part A	**A-05**	악성코드가 자산 사이로 번져 나갈 때
Part A	**A-06**	제어망에서 외부로의 비인가 통신이 발생했을 때

구분	번호	제목
Part A	**A-07**	자산 정보를 위장해 우회 접속을 시도할 때
Part A	**A-08**	하나의 자산에서 시작된 위협이 확산될 때
Part A	**A-09**	프린터를 통해 제어 자료가 무단 출력될 때
Part A	**A-10**	트래픽 급변·통신 중단 등 설비 이상 징후가 나타날 때
Part B	**B-01**	신규 설비를 반입해 자산으로 등록해야 할 때
Part B	**B-02**	정기 자산 실사와 대장 현행화를 수행할 때
Part B	**B-03**	설비의 물리 배치와 네트워크 구성을 현행화할 때
Part B	**B-04**	보안 정책을 수립하고 다수 사업장에 배포할 때
Part B	**B-05**	취약점 탐지 룰을 최신 상태로 유지해야 할 때
Part B	**B-06**	악성코드 탐지 결과를 판정하고 근거를 남겨야 할 때
Part B	**B-07**	오탐이 많아 알람을 신뢰할 수 없을 때
Part B	**B-08**	일상 관제 — 이벤트 확인부터 이슈 종결까지
Part B	**B-09**	정기 보안 보고서를 작성해 제출해야 할 때
Part B	**B-10**	사용자 권한을 관리하고 접근 이력을 감사할 때
Part C	**C-01**	자산 가시성 부재 — 제어망에 무엇이 연결되어 있는지 정확히 모르겠습니다.
Part C	**C-02**	망 분리 실효성 입증 불가 — 폐쇄망이라 안전하다고 하는데, 안전하다는 것을 증명할 수가 없습니다.
Part C	**C-03**	규제 대응 부담 — 가이드라인 대응 증적을 매번 수작업으로 만듭니다.
Part C	**C-04**	사후 추적 불가 — 사고가 나도 원인과 경로를 추적할 수가 없습니다.
Part C	**C-05**	다지역 통합 관리 부재 — 본사와 사업소의 보안 현황이 따로 놉니다.
Part C	**C-06**	가용성 우려 — 보안 장비가 제어 운전에 영향을 줄까 봐 도입이 망설여집니다.
Part C	**C-07**	운영 지식의 휘발 — 담당자가 바뀌면 그동안 쌓인 판단 기준이 사라집니다.
Part C	**C-08**	능동 취약점 진단 불가 — 제어망에서는 취약점 스캐너를 돌릴 수 없습니다. 그럼 취약점은 어떻게 봅니까?

04 도입 방식 및 지원 체계

본 문서의 시나리오는 아래 구축 모델과 유지보수 서비스 체계를 전제로 합니다. 시나리오 대응 역량은 모델과 무관하게 동일하며, 모델은 수용 규모에 따라 선택합니다.

▪ 구축 모델

모델	수용 규모	하드웨어	구성
Lite	~100 IP	PC	일체형 (DPI 탐지 + 보안 모니터링)
SMB	~300 IP	PC 또는 Server	일체형 (DPI 탐지 + 보안 모니터링)
Enterprise	Unlimited	Server	분산형 (DPI 탐지 서버 · 보안 모니터링 서버 분리)

▪ 시나리오 수행을 지원하는 유지보수 서비스

항목	Basic	Standard	Premium
정기 방문 점검	연 1회	연 2회	연 4회
오탐 튜닝 (B-07)	방문 시 수행	방문 시 수행	방문 시 수행
자산 · 취약점 리포트 (B-02 · B-05)	방문 시 수행	방문 시 수행	방문 시 수행
정기 리포트 (B-09)	방문 시 수행	방문 시 수행	방문 시 수행
패치 제공	연 2회	연 2회	연 2회
원격 정기 점검 (C2 원격형)	반기 1회	분기 1회	월간 1회

※ 제품 하자 수정 · 장애 현장 출동 · 기술 문의 대응은 등급과 무관하게 전 계약에 동일 제공됩니다. 운영서비스(원격지원)는 계약 형태 · 등급과 무관하게 별도 요금 없이 제공됩니다.

> **운영 지식의 지속 관리**
> Part B의 오탐 튜닝(B-07), 취약점 룰 갱신(B-05), 자산 실사(B-02), 보고서 작성(B-09)은 도입 후에도 반복적으로 수행되는 업무입니다. 유지보수 서비스의 정기 방문 점검에서 이 항목들을 지속 지원하여, Part C의 「운영 지식 휘발」(C-07) 문제가 재발하지 않도록 관리합니다.

문의

온시큐리티㈜ (OnSecurity Co., Ltd.)

TEL 031-792-0633 · FAX 031-792-0635 · Email info@onsecurity.co.kr

경기도 하남시 미사강변한강로 135(망월동) 미사강변스카이폴리스 다동 1038-1039호 · www.onsecurity.co.kr