PRODUCT INTRODUCTION

ICS Security Monitor

산업제어시스템 통합보안 모니터링 시스템 v1.0

제어시스템 보안 운영을 하나로 — 자산 가시성부터 위협 상관분석·보고서 자동화까지

ON Security

www.onsecurity.co.kr · 031-792-0633 · 온시큐리티㈜

CONTENTS

목차

회사 개요

일반 현황 · 인증 및 특허 · 주요 연혁 · 제품 구성

제품 소개

Product Overview · 특장점 · 주요 기능 · 기능 상세 10종 · 제품 모델

문제 해결 · 구축 방안

제품별 문제 해결 방안 · 구축 방안

유지보수 · 요금

유지보수 서비스 · SLA와 제공 방식 · 서비스 조건 · 요금 매트릭스

COMPANY OVERVIEW

회사 개요

2013년 설립 이래 산업제어시스템 보안 한 분야에 집중해 온 온시큐리티의 일반 현황과 주요 연혁, 제품 구성을 안내합니다.

ABOUT ONSECURITY

산업제어시스템 보안을 위한 최적화 솔루션 개발 기업

기업 개요

회사명 온시큐리티㈜ (OnSecurity Co., Ltd.)

설립일 2013년 11월

대표이사 강형구

사업자등록번호 114-87-13197

소재지 경기도 하남시 미사강변한강로 135 미사강변스카이폴리스 다동 1038~1039호 (12902)

연락처 TEL 031-792-0633 · FAX 031-792-0635

이메일 info@onsecurity.co.kr

사업 분야 산업제어시스템(ICS/OT) 보안 시스템 설계 · 구축 · 개발

온시큐리티는 산업제어시스템(ICS/OT) 보안을 위한 통합 보안 모니터링 · 자산 탐지 · 제어설비 자동식별 솔루션을 개발하여 제공합니다.

온시큐리티의 접근

Collect

제어망 네트워크 패킷 패시브 수집

Analyze

빅데이터 · 딥러닝 기반 분석

Detect

보안 이벤트 · 이상행위 탐지

Respond

이슈 관리 · 보고서 자동 생성

CREDENTIALS

인증 · 특허 · 주요 고객

인증 및 수상

- GS인증 1등급 — ICS Scanner v1.0
- GS인증 1등급 — ICS Asset Manager v1.0
- 벤처기업 확인 · 기업부설연구소 인정
- SW사업자 신고

보유 특허

- L2 패킷 차단이 가능한 침입 방지 시스템 및 방법
- 비표준 프로토콜에 대한 화이트리스트 기반의 산업 제어시스템 이상행위 탐지 방법 및 탐지 장치
- 발전소 제어시스템 자산의 신뢰도 평가를 이용한 이상 감지 시스템
- 발전소 제어망 자산의 트래픽의 분산 저장을 이용한 이상 감지 시스템
- 상태정보(운전정보)를 이용한 산업제어시스템의 이상징후를 감지하는 방법 및 장치
- 패킷 순서정보를 이용한 산업제어시스템의 이상징후를 감지하는 방법 및 장치
- 산업제어시스템의 이상징후를 감지하는 방법 및 장치

주요 고객 및 협력

- 한국남동발전
- 한국서부발전
- 한국중부발전
- 한전KDN
- 휴네시온
- 한빛SI

온시큐리티가 지켜온 세 가지 가치

신뢰

고객의 얼굴보다 마음을 알아가는 기업

열정

2013년 설립 이래 ICS 보안 분야를 선도

미래 지향

자체 기술로 국가 기반시설 보안을 책임

HISTORY

주요 연혁

창립과 연구개발, 현장 구축과 확산, 제품화와 도약의 세 단계로 성장해 왔습니다.

2013~2017

창립과 연구개발

2013.11 온시큐리티㈜ 설립

2015~2016 한국남동발전 발전제어망 패킷 분석 · 화이트리스트 모듈화 연구

2017.08 한국남동발전 네트워크 포렌식 시스템 구축

2017.12 한국남동발전 제어시스템 보안 모니터링 시스템 기반구축

2017.12 한국남동발전 딥러닝 기반 제어시스템 이상행위 탐지시스템 개발

2018~2021

현장 구축과 확산

2018.04 한국남동발전 영흥발전본부 제어시스템 보안모니터링 시스템 구축

2018.06 한국서부발전 서인천본부 1Block 보안 모니터링 기반 구축

2019.03 한국남동발전 제어시스템 보안모니터링 전사 확대 구축

2019.11 한전KDN 발전제어 보안모니터링 모델 개발

2020.10 ICS Scanner v1.0 출시 · 한국남동발전 납품

2021.03 TTA ICS Scanner v1.0 GS인증(1등급) 획득

2022~현재

제품화와 도약

2022.02 한전KDN AI기반 제어시스템 위험관리시스템 시작품 개발

2022.05 ICS Asset Manager v1.0 출시 · TTA GS인증(1등급) 획득

2022.07 한국서부발전 제어시스템 자산탐지 및 분류관리시스템 확대 구축

2023.04 한국중부발전 발전설비 현장 순찰 보안 로봇 기술 연구 개발

2024.12 한국중부발전 보령 신복합 자산 탐지 · 분류 관리 시스템 납품

2025.12 제어시스템 DPI 분석 시스템 · ICS Security Monitor 출시

2026.04 한국서부발전 제어시스템 통합 보안 모니터링 시스템 구축

2026.07 ICS Security Monitor Lite · SMB 모델 출시

PRODUCT LINEUP

제품 구성

제어설비 자동식별 → 자산 탐지 · 분류 관리 → 통합 보안 모니터링의 3개 제품군으로 구성됩니다.

STEP 1

ICS Scanner

제어설비 자동식별 및 관리 시스템

GS 1등급

제어설비 자동식별

· 휴대용 노트북 기반 · 상주 설치 없음

· 독립 · 분리 네트워크, 시범적용(PoC)

구축 모델 단일 모델

STEP 2

ICS Asset Manager

산업제어 자산탐지 및 분류관리 시스템

GS 1등급

자산 탐지 · 분류 관리

· 자산 자동 탐지 · 분류 및 지속 관리

· 보안의 기반이 되는 자산 가시성 확보

구축 모델 Lite · SMB · Enterprise

본 자료 대상

STEP 3

ICS Security Monitor

산업제어시스템 통합보안 모니터링 시스템

통합 보안 모니터링

· 탐지 · 분석 · 이슈 관리 · 증적 확보

· 전 지역 통합 대시보드 관제

구축 모델 Lite · SMB · Enterprise

3개 제품 공통 기술 원칙

패시브 수집

미러링(SPAN) · 탭 포트로 복제 트래픽만 분석

Agentless

개별 설비에 에이전트 설치 불필요

무부하 운영

능동 스캔 · 패킷 주입 없음

보고서 자동화

실태점검 · 감사 증적 자동 생성

PRODUCT

제품 소개

ICS Security Monitor v1.0의 개요와 특장점, 주요 기능과 화면, 구축 모델을 안내합니다.

ICS SECURITY MONITOR V1.0

산업제어시스템 통합보안 모니터링 시스템

제어시스템 보안 운영을 하나로 — 자산 가시성부터 위협 상관분석·보고서 자동화까지

Product Overview

제어시스템 자산 가시성 확보부터 네트워크·취약점·악성코드 탐지, 위협 상관분석, 이슈 관리, 보고서 자동 생성까지 제어시스템 보안 운영 전 과정을 하나의 시스템에서 통합 관리합니다.

국문 명칭 산업제어시스템 통합보안 모니터링 시스템

영문 명칭 ICS Security Monitor v1.0

인증 보안 모니터링 구축 가이드라인('24.12) 대응 역량 충족

구축 모델

- **Lite** ~100 IP · PC 일체형
- **SMB** ~300 IP · PC 또는 Server 일체형
- **Enterprise** Unlimited · Server 분산형

특장점

01

제어 운영 무부담 패시브 수집

미러링(SPAN)·탭 포트로 복제된 트래픽만 분석하고 능동 스캔·패킷 주입을 하지 않아, 운전 중인 제어 프로세스에 부하를 주지 않습니다.

02

에이전트 설치 없는 Agentless 탐지

자산 식별·네트워크·취약점 탐지가 네트워크 기반으로 동작해 개별 설비에 에이전트를 설치할 필요가 없습니다.

03

다지역 제어시스템 통합 관리

정책·룰셋을 일괄 배포하고, 전 지역 보안 현황을 하나의 대시보드에서 통합 모니터링합니다.

04

제어시스템 보안 가이드라인 충족

제어시스템 보안 모니터링 구축 가이드라인('24.12)의 대응 역량 기준을 충족합니다.

KEY FEATURES

주요 기능 · ICS Security Monitor v1.0

주요 기능 7종과 기능 구조, 적용 대상입니다.

주요 기능 7종

기능	설명
자산관리	자산 자동 식별 및 관리, 정책 관리, 물리적 자산 관리, 네트워크 구성
보안 이벤트 탐지	네트워크 탐지, 악성코드 탐지(Windows Defender), 취약점 탐지(Snort 기반)
보안 이벤트 분석	네트워크 · 취약점 · 악성코드 · Packet 분석
위협 분석	위협 스캐닝 + 위협 상관 분석
이슈 관리	본사 · 지역 간 원인 분석과 조치결과 등록, 조치 이력의 감사 추적(Audit trail) 제공
대시보드	본사 통합 모니터링 대시보드와 단독 제어시스템별 모니터링 대시보드 제공
보고서 자동 생성	탐지 이벤트 유형별 · 조직 단위별 보고서 및 기간별 보안 현황 보고서 자동 구성

기능 구조

관제 · 보고

통합 대시보드 · 이슈 관리 · 보고서 자동 생성

분석

위협 스캐닝 · 네트워크 위협 상관분석 · Packet 분석

탐지

네트워크 탐지 · 취약점 탐지 · 악성코드 탐지

기반

자산 관리 · 정책 관리 · 제어망 패킷 패시브 수집

적용 대상

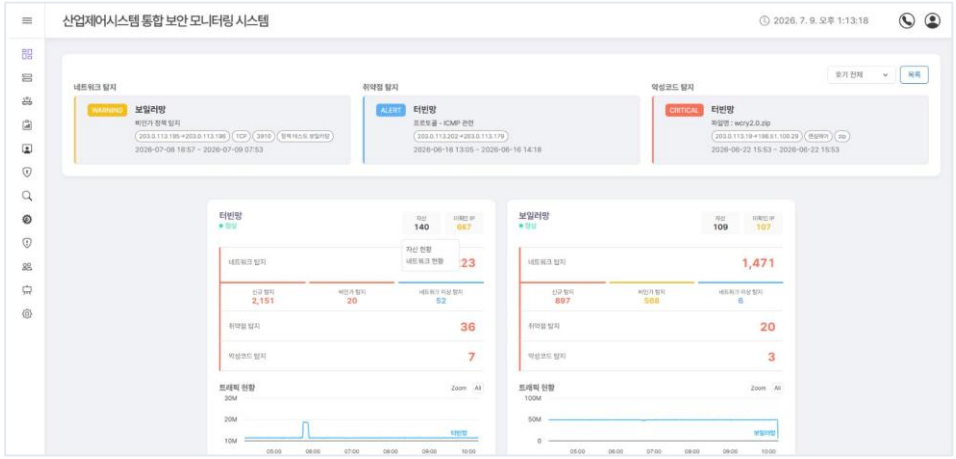
- 발전 제어망 등 주요정보통신기반시설 제어시스템
- 다수 지역 제어망을 보유한 전사 통합 보안 관제 환경

기술 · 운영 특징

- 제어망 DPI 분석 이벤트 통합 모니터링
- 위협 상관 분석 기반 전파 경로 확인
- 상위 기관 데이터 연계 인터페이스 제공
- 전사 관점 보고서 자동 생성

FEATURE DETAIL

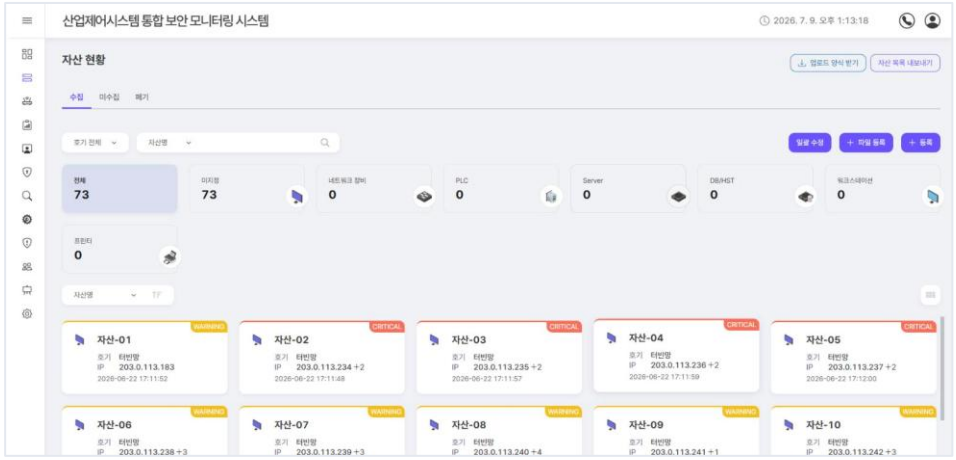
기능 상세 · ICS Security Monitor v1.0 (1/5)



01 Dashboard

보안 현황을 한 화면에 집약한 통합 대시보드

네트워크 · 취약점 · 악성코드 탐지를 심각도(WARNING / ALERT / CRITICAL)별로 표시하고, 호기별 자산 수 · 미확인 IP와 신규 · 비인가 · 이상 탐지 건수를 집계하며, 호기별 트래픽 추이를 시계열 차트로 모니터링합니다.



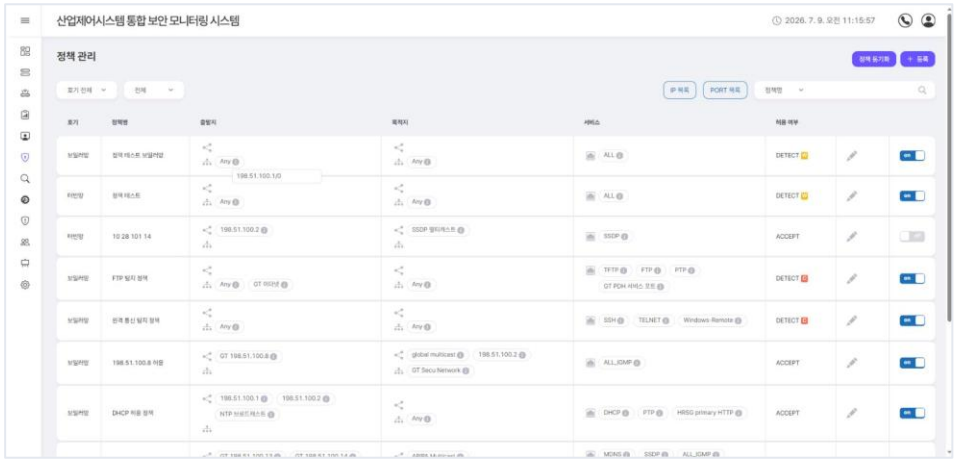
02 Asset

수집 패킷 기반으로 자동 식별해 분류하는 자산 관리

수집 / 미수집 / 폐기 상태로 구분해 자산 목록을 관리하고, 네트워크 장비 · PLC · Server · DB/HST · 워크스테이션 · 프린터 · 미지정으로 분류합니다. 업로드 양식과 목록 내보내기, 일괄 수정 · 파일 등록을 지원합니다.

FEATURE DETAIL

기능 상세 · ICS Security Monitor v1.0 (2/5)

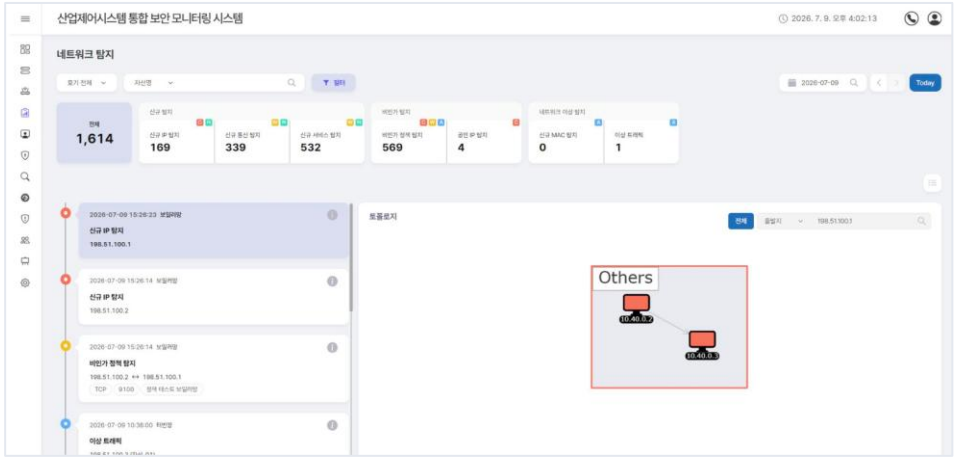


03 Policy

자산 간 통신 기준선을 등록해 관리하는

정책 관리

호기 · 출발지 · 목적지 · 서비스 단위로 정책을 등록하고 ACCEPT(승인) / DETECT(탐지)로 구분해 정책별 on · off를 제어합니다. IP 목록 · PORT 목록 조회와 호기 단위 정책 동기화를 제공합니다.



04 Network Detection

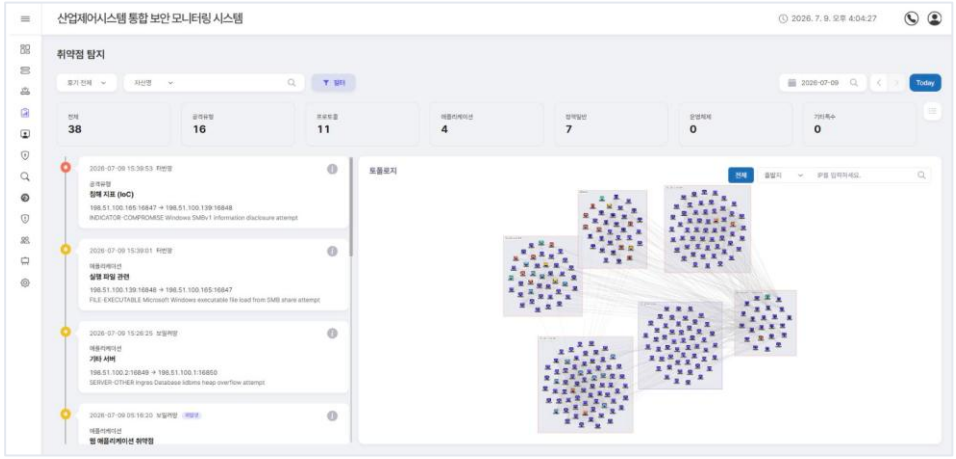
이벤트 타임라인과 통신 토폴로지로 확인하는

네트워크 탐지

신규 IP · 신규 통신 · 신규 서비스, 비인가 정책 · 공인 IP, 신규 MAC · 이상 트래픽의 3개 분류로 이벤트를 탐지하고, 탐지 시점의 통신 관계를 토폴로지로 시각화합니다.

FEATURE DETAIL

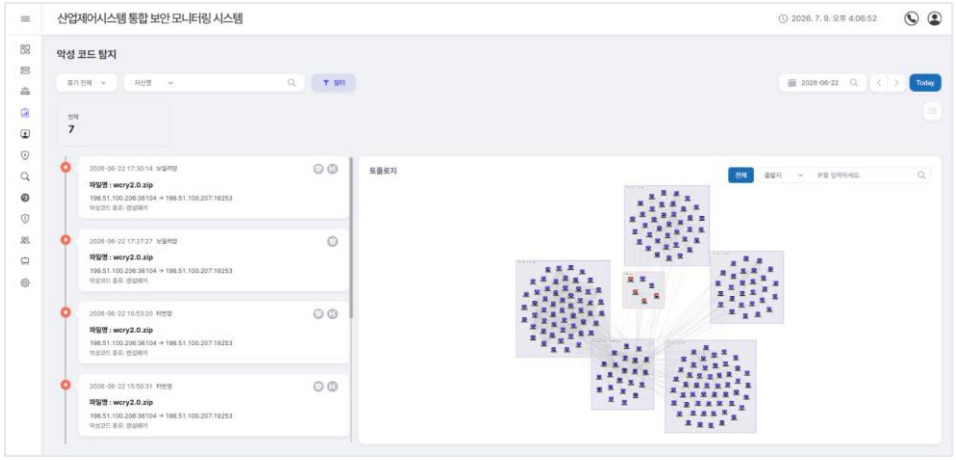
기능 상세 · ICS Security Monitor v1.0 (3/5)



05 Vulnerability

제어망 환경에 맞춘 룰셋으로 분류하는 취약점 탐지

공격유형 · 프로토콜 · 애플리케이션 · 정책일반 · 운영체제 · 기타특수로 유형을 분류하고, 침해 지표(IoC) · 실행 파일 관련 · 웹 애플리케이션 취약점 등 이벤트별 상세를 제공하며 연계 자산과의 통신 관계를 토폴로지로 확인합니다.



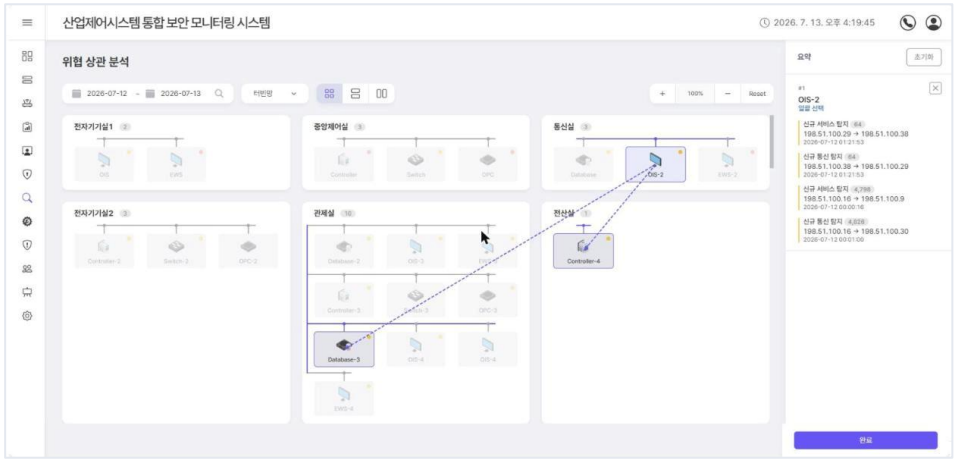
06 Malware

에이전트 설치 없이 전송 단계에서 잡아내는 악성코드 탐지

개별 설비에 백신 · 에이전트를 설치하지 않고 전송 패킷 기준으로 탐지합니다. 파일명과 악성코드 종류(랜섬웨어 등), 출발지 → 목적지 통신 정보를 제공하고 탐지 시점의 자산 간 통신 관계를 토폴로지로 확인합니다.

FEATURE DETAIL

기능 상세 · ICS Security Monitor v1.0 (4/5)

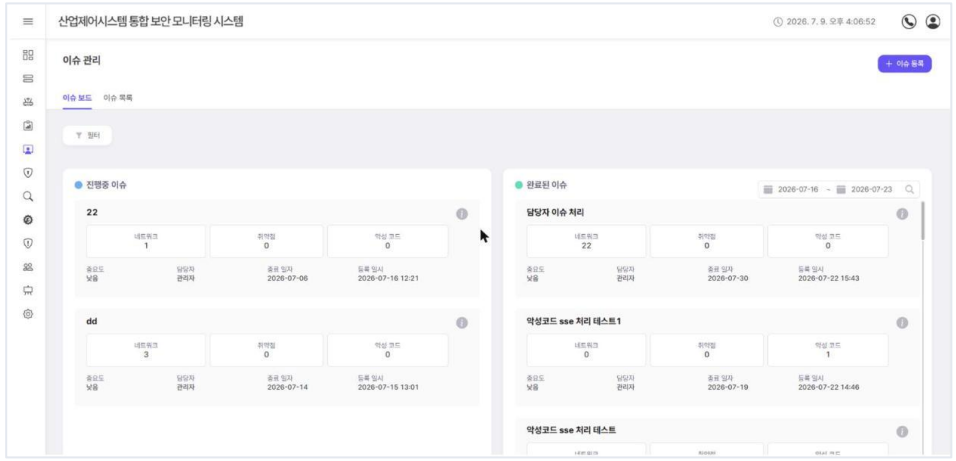


07 Threat Correlation

시설별 자산 배치로 전파 경로를 파악하는

위협 상관 분석

전자기기실 · 중앙제어실 · 통신실 · 관제실 단위로 자산을 배치하고, 연관 자산 간 이벤트 흐름을 연결선으로 표시해 전파 경로를 파악합니다. 선택 자산의 신규 통신 · 신규 서비스 탐지 건수와 발생 시각을 요약해 보여줍니다.



08 Issue

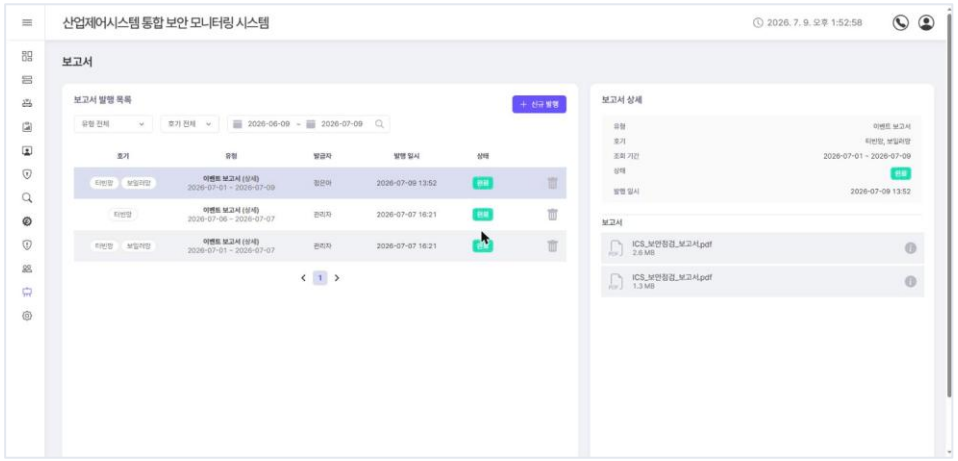
탐지 이벤트를 등록해 조치까지 추적하는

이슈 관리

진행중 이슈와 완료된 이슈를 보드 형태로 구분해 관리하고, 이슈별 네트워크 · 취약점 · 악성코드 이벤트 건수를 함께 표시합니다. 중요도 · 담당자 · 종료 일자 · 등록 일시로 조치 이력을 감사 추적합니다.

FEATURE DETAIL

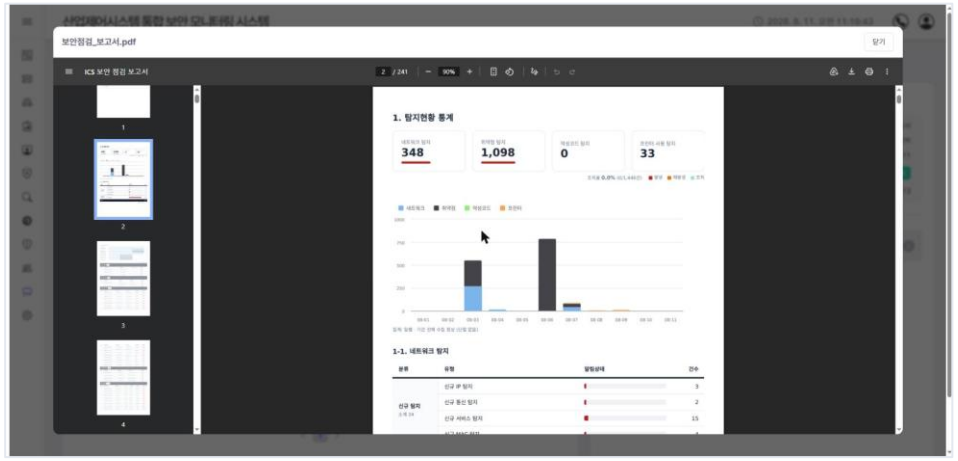
기능 상세 · ICS Security Monitor v1.0 (5/5)



09 Report

탐지 · 조치 데이터를 담아 발행하는 보안 점검 보고서

호기 · 유형 · 발급자 · 발행 일시 · 상태로 발행 이력을 관리하고, 조회 기간과 호기를 지정해 이벤트 보고서를 즉시 발행합니다. 발행 결과는 PDF로 첨부해 내려받을 수 있습니다.



10 Report Output

통계와 상세 내역을 포함해 산출되는 보고서 산출물

네트워크 · 취약점 · 악성코드 · 프린터 사용 탐지 건수와 조치율을 집계하고, 일별 탐지 추이를 유형별 누적 차트로 제공하며, 신규 탐지 등 분류별 유형 · 알림상태 · 건수를 표로 수록합니다.

DEPLOYMENT MODELS

제품 모델 · ICS Security Monitor v1.0

수용 IP 규모에 따라 Lite · SMB · Enterprise 중에서 선택합니다.

모델별 구성

모델	수용 규모	하드웨어	구성	권장 상황
Lite	~100 IP	PC	일체형	단일 사업장 · 소규모 제어망
SMB	~300 IP	PC 또는 Server	일체형	중규모 사업장 통합 관제
Enterprise	Unlimited	Server	분산형	다지역 제어망 전사 통합 관제

업그레이드 경로 — 동일 인프라에서 소프트웨어 업그레이드

모델	ICS Asset Manager	ICS Security Monitor	업그레이드 비용
Lite (PC)	3,000	5,000	+2,000
SMB (PC)	5,000	7,000	+2,000
SMB (Server)	7,000	9,000	+2,000

※ 단위: 만원, VAT 별도 · Enterprise는 구축 범위 사전 협의 후 견적 안내

SOLUTION & DEPLOYMENT

문제 해결 · 구축 방안

현장 문제에 대한 ICS Security Monitor의 해결 방안과 단계적 구축 절차를 안내합니다.

PROBLEM & SOLUTION

제품별 문제 해결 방안 · ICS Security Monitor

제어시스템 운영 현장의 문제와 해당 제품이 제공하는 해결 방안 · 관련 기능입니다.

구분	현장 문제	온시큐리티 해결 방안	관련 기능
자산 가시성	자산 현황이 문서로만 관리되어 실제 구성과 불일치	패킷 수집으로 자산을 자동 식별 · 목록화하고 자산 대장을 자동 생성	자산관리
운영 리스크	설비에 에이전트 · 백신 설치 불가, 능동 스캔 시 운전 영향 우려	미러링 기반 패시브 수집과 Agentless 탐지로 무부하 운영	패시브 수집 (공통 기술)
비인가 통신	비인가 장비 연결과 정책 외 통신을 사후에도 인지하지 못함	IP · 통신 · 서비스 정책 기준 신규 · 비인가 탐지와 알림	보안 이벤트 탐지
취약점 · 악성코드	패치가 불가한 설비의 취약점 · 악성코드 대응 수단 부재	Snort 기반 취약점 탐지와 네트워크 전송 단계 악성코드 탐지	보안 이벤트 탐지 · 분석
원인 규명	이벤트가 흩어져 발생 원인과 전파 경로를 규명하지 못함	자산 기준 위협 스캐닝 + 네트워크 위협 상관분석, 이슈 관리	위협 분석 · 이슈 관리
증적 확보	실태점검 · 보안 감사 증적을 담당자가 수작업으로 작성	자산 · 이벤트 · 조치 이력 기반 보고서 자동 생성	보고서 자동 생성
전사 관리	다지역 제어망을 개별 관리해 전사 현황을 파악하지 못함	본사 통합 대시보드로 전 지역 현황을 하나의 화면에서 관제	대시보드 (본사 통합)

※ 위 항목은 ICS Security Monitor v1.0가 직접 해결하는 범위입니다. 자산 가시성 · 무부하 운영 · 비인가 통신 탐지 · 증적 확보는 3개 제품 공통으로 대응합니다.

DEPLOYMENT

구축 방안

현황 진단에서 자산 관리 체계 확보, 통합 보안 관제까지 단계적으로 확장합니다.

STEP 1

현황 진단 · PoC

ICS Scanner

- 상주 설치 없이 제어망 자산 현황 진단
- 독립 · 분리 네트워크 구간까지 확인
- 진단 결과로 도입 범위와 규모 산정

STEP 2

자산 관리 체계 확보

ICS Asset Manager

- 자산 자동 탐지 · 분류와 지속 관리
- 시설 · 캐비닛 단위 물리 자산 배치
- 네트워크 이상행위 탐지와 감사 증적

STEP 3

통합 보안 관제 전환

ICS Security Monitor

- 동일 인프라에 소프트웨어 업그레이드
- 취약점 · 악성코드 탐지와 위협 상관분석
- 전 지역 통합 대시보드 · 보고서 자동화

업그레이드 경로 — 동일 인프라에서 소프트웨어 업그레이드

모델	ICS Asset Manager	ICS Security Monitor	업그레이드 비용
Lite (PC)	3,000	5,000	+2,000
SMB (PC)	5,000	7,000	+2,000
SMB (Server)	7,000	9,000	+2,000

※ 단위: 만원, VAT 별도 · Enterprise는 구축 범위 사전 협의 후 견적 안내 · 단계별 예산 집행으로 초기 부담을 완화할 수 있습니다.

SERVICE & PRICING

유지보수 · 요금

납품 이후의 통합 유지보수 서비스 등급과 SLA, 계약 조건 및 요금을 안내합니다.

MAINTENANCE

유지보수 서비스

세 개의 등급, 하나의 기준 — 등급에 따라 점검 주기와 응답 · 복구 목표가 달라집니다.

Basic

기본 운영 유지

- 정기 방문 점검 연 1회
- P1 최초 응답 8업무시간
- P1 장애 복구 4영업일
- 원격 정기 점검 미제공

Standard

표준 운영 관리

- 정기 방문 점검 연 2회
- P1 최초 응답 4업무시간
- P1 장애 복구 2영업일
- 원격 정기 점검 분기 1회

Premium

적극 대응 · 관리

- 정기 방문 점검 연 4회
- P1 최초 응답 2업무시간
- P1 장애 복구 2영업일
- 원격 정기 점검 월간 1회

전 등급 공통 제공 범위

- 제품 하자 수정 및 패치 제공
- 기술 문의 대응
- 정기 방문 점검 (등급별 연 1 · 2 · 4회)
- 장애 접수 및 현장 출동
- 정기 리포트 및 자산 / 취약점 리포트

장애 등급 정의

등급	수준	정의
P1	긴급	패킷 수집 중단, 탐지 기능 전면 불가, 시스템 다운
P2	높음	일부 사이트 · 기능 장애, 대시보드 지연
P3	보통	성능 저하, 오탐 발생
P4	낮음	사용 문의, 설정 변경 요청

SLA & DELIVERY

SLA와 제공 방식

등급별 응답 · 복구 목표와 현장형(C1) · 원격형(C2) 제공 방식 판정 기준입니다.

등급별 SLA

항목	Basic	Standard	Premium
정기 방문 점검	연 1회	연 2회	연 4회
P1 최초 응답	8업무시간	4업무시간	2업무시간
P1 현장 도착		익영업일	
P1 장애 복구	4영업일	2영업일	2영업일
P2 최초 응답	익영업일	8업무시간	4업무시간
P2 장애 복구	5영업일	3영업일	2영업일
원격 정기 점검	반기 1회	분기 1회	월간 1회
원격 점검 리포트	반기	분기	월간

제공 방식 판정

구분	조건	제공 방식
경우 1	주요정보통신기반시설 지정	C1 현장형 확정
경우 2	미지정 + 원격 경로 확보	C2 원격형
경우 3	미지정 + 원격 경로 없음	C1 현장형

C2 원격 접속 경로

- 제어시스템 → 일방향 전송장비(국가정보원 사전승인 포함) → 고객 IT DMZ
- 온라인 용역 통제시스템 또는 IDMZ 점프호스트 · PAM

C2 사전 준비 사항

- 온시큐리티 담당자용 접속 계정 발급
- 지정 단말 및 접속 경로 지정
- 작업 승인 절차 및 접속 이력 보관

※ 보안관제(MSSP)가 아니며 24×7 상시 대응과 침해사고 대응(IR)은 제공하지 않습니다. C1 현장형은 원격 점검이 제공되지 않습니다.

CONTRACT TERMS

서비스 조건

계약 형태와 무상 기간, 등급 변경 및 업그레이드에 관한 주요 조건입니다.

구분	내용
무상 기간(소유형)	납품 검수 완료일로부터 1년 - 1년차 무상지원 포함
소유형	1년차 공급가 전액 + 무상지원, 2년차부터「공급가 × 등급 요율」연 유지보수료
구독형 소유권	초기 투자 없이 SLA 즉시 적용, 약정 종료 후 소유권 고객 귀속 (이후 소유형 전환)
등급 변경	상향은 계약 기간 중 언제든 가능(잔여 기간 차액 일할 정산), 하향은 갱신 시점에만 가능
업그레이드	동일 인프라에서 소프트웨어 업그레이드 - 전 모델 공통 2,000만 원
제공 범위 제외	보안관제(MSSP) 아님 · 24×7 상시 대응과 침해사고 대응(IR)은 제공하지 않음

PRICING

요금 매트릭스 · ICS Security Monitor v1.0

소유형은 공급가 + 연 유지보수료(2년차부터), 구독형은 연 구독료로 구성됩니다. 단위: 만원, VAT 별도.

모델	공급가	소유형 연 유지보수료 (2년차~)			구독형 3년 연 구독료			구독형 5년 연 구독료		
		B	S	P	B	S	P	B	S	P
Lite (PC)	**5,000**	500	750	1,000	2,120	2,280	2,440	1,540	1,740	1,930
SMB (PC)	**7,000**	700	1,050	1,400	2,960	3,190	3,410	2,160	2,430	2,700
SMB (Server)	**9,000**	900	1,350	1,800	3,810	4,100	4,390	2,780	3,120	3,470
Enterprise (Server)	**협의**	구축 범위 · 구성 협의 후 산정								

요금 구성 안내

- **소유형** — 공급가 + 2년차부터 「공급가 × 등급 요율」
- **구독형** — 사용권 + 유지보수 통합 연 선납 (3년 · 5년)
- **등급 요율** — Basic 10% · Standard 15% · Premium 20%
- **Enterprise** — 규모 · 구성 협의 후 산정

참고 사항

- B = Basic · S = Standard · P = Premium
- 소유형 연 유지보수료는 2년차부터 적용됩니다.
- 인프라(집합랩 · 일방향전송장치 · 방화벽 등)는 고객사 구축 또는 별도 문의 대상입니다.
- Enterprise는 등급 요율과 구독 산식을 동일하게 준용합니다.

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

ON Security

온시큐리티㈜ | 대표이사 강형구 | 사업자등록번호 114-87-13197