PRODUCT INTRODUCTION

ICS Scanner

제어설비 자동식별 및 관리 시스템 v1.0

설치 없이 노트북 한 대로 — 독립·분리 네트워크의 자산 식별과 관리

ON Security

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

CONTENTS

목차

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 보안모니터링 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 서인천 1Block 보안모니터링 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.

본 자료 대상

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**

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 Scanner v1.0의 개요와 특장점, 주요 기능과 화면, 구축 모델을 안내합니다.

ICS SCANNER V1.0

제어설비 자동식별 및 관리 시스템

설치 없이 노트북 한 대로 — 독립·분리 네트워크의 자산 식별과 관리

Product Overview

상주 시스템 설치 없이 휴대용 노트북 한 대로 독립·분리 네트워크의 자산 식별과 관리를 수행합니다. 신재생·CCTV망 등 상주 설치가 어려운 구간과 시범적용(PoC)에 최적화되어 있습니다.

국문 명칭 제어설비 자동식별 및 관리 시스템

영문 명칭 ICS Scanner v1.0

인증 GS인증 1등급 (TTA 소프트웨어 품질 시험)

구축 모델

- **단일 모델** 노트북 기반 휴대형 · 상주 설치 없음

특장점

01

설치 없는 휴대형(Portable) 운용

시스템 상주 설치 없이 휴대용 노트북으로 자산 식별 및 관리를 수행합니다.

02

제어설비 자동 식별

스위치 기준 통신 수집·탐지로 자산을 자동 식별하고 변경 이력을 관리합니다.

03

현장 즉시 사용

네트워크 연결만으로 현황을 즉시 파악·모니터링할 수 있습니다.

04

모든 산업제어시스템 적용

IP 자산 유형에 제약이 없어 신재생·CCTV망 등 독립 네트워크부터 적용 가능합니다.

KEY FEATURES

주요 기능 · ICS Scanner v1.0

주요 기능 6종과 기능 구조, 적용 대상입니다.

주요 기능 6종

기능	설명
스위치 기준 수집 / 탐지	스위치별로 수집 대상을 분리하여 데이터를 수집 · 탐지, 구간별 네트워크 현황 파악
자산관리	네트워크에 연결된 자산 자동 식별, 자산 변경 이력으로 신규 · 변경 · 이탈 자산 추적
정책 관리	IP / Port 정책으로 자산 구분, 승인 · 미승인 장비 자동 판별
이벤트 탐지	다중 프로토콜 지원, 제조사별 프로토콜 특성을 반영한 이벤트 탐지
이벤트 분석	장비 간 통신 현황 분석으로 비정상 통신과 예상치 못한 연결 식별
PCAP 분석 서비스	별도 수집한 PCAP 파일 업로드 분석, 주소 기준 · IP 조건 · MAC 등록 등 분석 조건 선택

기능 구조

산출

통신 토폴로지 · 보고서(PDF) 자동 생성

분석

이벤트 분석 · PCAP 분석 서비스

판별

정책 관리(IP / Port) · 이벤트 탐지

기반

자산관리 · 변경 이력 · 스위치 기준 수집 / 탐지

적용 대상

- 상주 설치가 어려운 독립 · 분리 네트워크 구간
- 신재생 · CCTV망 등 소규모 단독망 및 시범적용(PoC)

기술 · 운영 특징

- S/W Package 설치만으로 즉시 운용
- 이기종 보안장비 PCAP 연계 분석
- 3,500 노드 이상 대규모 네트워크 운영 이력
- 기술개발제품 시범구매 · 혁신제품 선정

FEATURE DETAIL

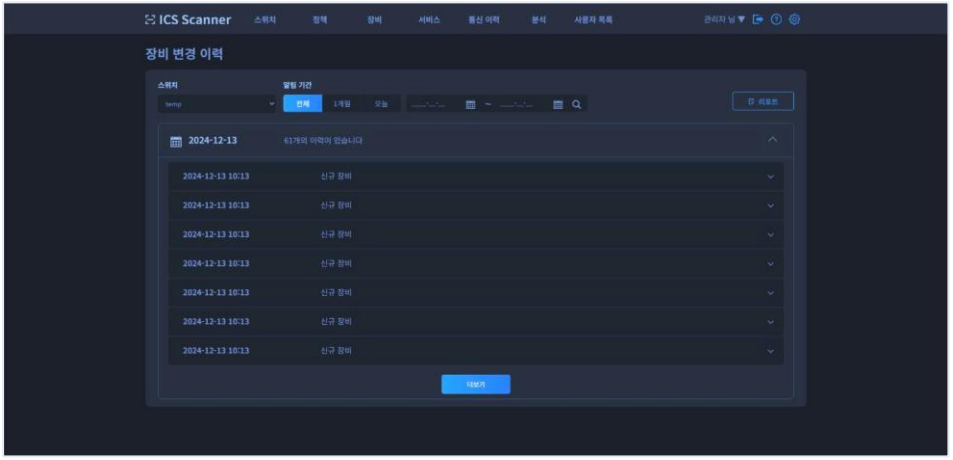
기능 상세 · ICS Scanner v1.0 (1/3)

01 Collect

스위치를 지정해 즉시 수행하는

패킷 수집

스위치 선택 → 수집 드라이버 선택 → 수집 시간 선택의 3단계로 설정하고, 네트워크 트래픽 추이와 수집 진행률 · 파일 크기, 디스크 및 라이선스 사용량을 실시간으로 확인합니다.



02 Change History

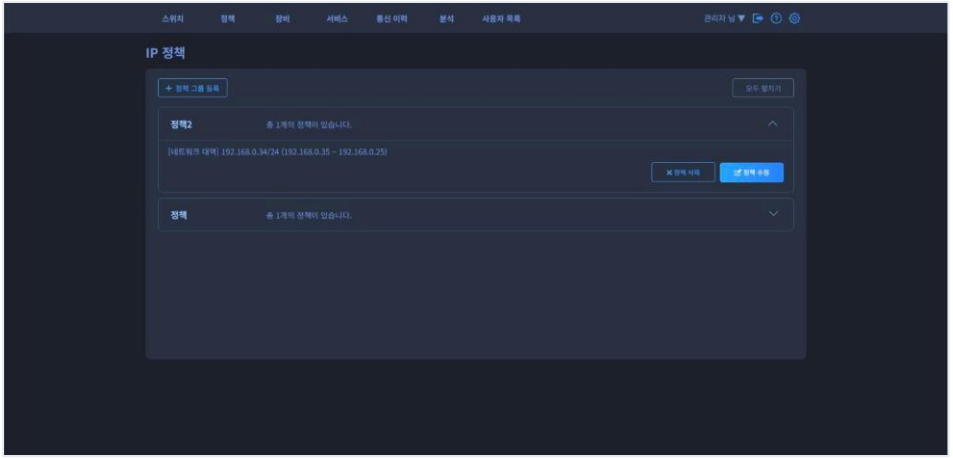
신규 · 변경 · 이탈을 누적 기록하는

장비 변경 이력

수집 결과를 기준으로 일자별 변경 내역을 누적 기록하고, 스위치와 알림 기간(전체 · 1개월 · 오늘 · 기간 지정)으로 검색하며 변경 이력을 리포트로 산출합니다.

FEATURE DETAIL

기능 상세 · ICS Scanner v1.0 (2/3)



03 IP Policy

승인 장비 판별 기준이 되는

IP 정책 관리

정책 그룹을 등록하고 그룹별 정책 수를 관리하며, 단일 IP와 네트워크 대역(CIDR) 방식으로 정책을 등록합니다. 등록된 IP 정책을 기준으로 승인 · 미승인 장비를 자동 구분합니다.

04 Communication

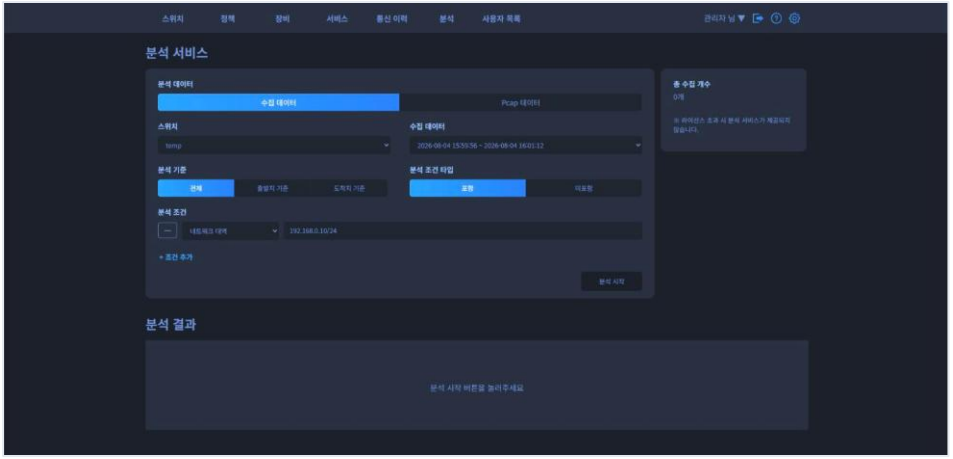
통신 목록과 토폴로지로 함께 보는

통신 이력

출발지 · 도착지의 IP · MAC · PORT와 프로토콜(UDP · ARP · TCP/DNS 등)을 기록하고, 출발지 · 도착지 기준 IP 수와 MAC 수를 요약하며 각 관점의 통신 관계를 시각화합니다.

FEATURE DETAIL

기능 상세 · ICS Scanner v1.0 (3/3)

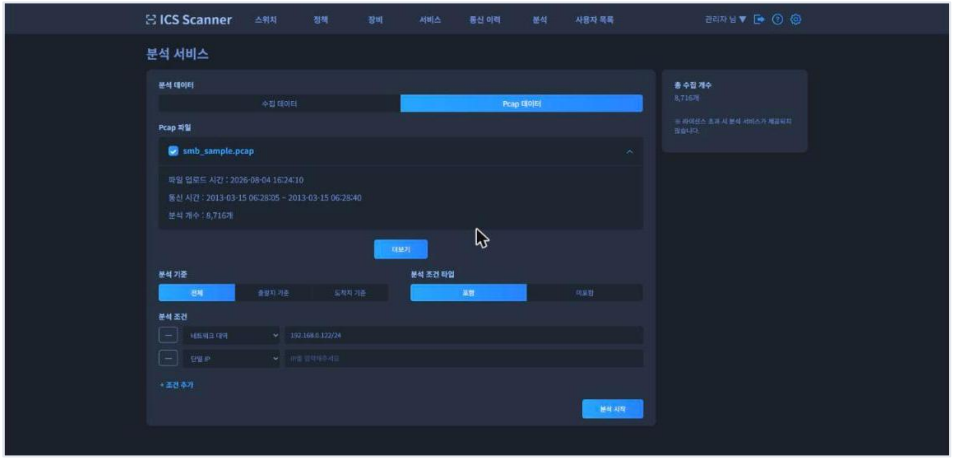


05 Analysis

조건을 지정해 원하는 통신만 선별하는

수집 데이터 분석

스위치와 수집 구간(수집 시작 ~ 종료 시각)을 선택하고 전체 · 출발지 기준 · 도착지 기준, 포함 · 미포함 조건을 지정하며 네트워크 대역 · 단일 IP 등 조건을 다중으로 추가합니다.



06 PCAP Service

이기종 장비 수집분까지 같은 기준으로 보는

PCAP 분석 서비스

보안장비가 수집한 PCAP 파일을 업로드해 업로드 시각 · 통신 시간 · 분석 개수를 확인하고, 수집 데이터와 같은 분석 기준 · 조건 타입 · 조건을 적용해 비교 분석합니다.

DEPLOYMENT MODELS

제품 모델 · ICS Scanner v1.0

단일 모델로 제공됩니다.

구축 모델

단일 모델

휴대용 노트북 기반 · 상주 설치 없음

S/W Package 설치만으로 즉시 운용

적용 사례

구분	내용
발전 제어망	제어망 내부 트래픽 구간 자산 식별 · 보안 감사 대비
신재생 에너지망	태양광 · 풍력 등 소규모 단독망 자산 현황 파악
CCTV · 기타 분리망	상주 설치가 어려운 구간의 주기적 점검
시범적용(PoC)	전사 도입 직전 기능 검증 및 현황 진단

권고 사양

구분	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

SOLUTION & DEPLOYMENT

문제 해결 · 구축 방안

현장 문제에 대한 ICS Scanner의 해결 방안과 단계적 구축 절차를 안내합니다.

PROBLEM & SOLUTION

제품별 문제 해결 방안 · ICS Scanner

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
분리망 사각지대	상주 설치가 어려운 독립 · 분리망은 현황 파악 자체 불가	노트북 한 대로 즉시 수집 · 진단, 상주 설치 불필요	스위치 기준 수집 / 탐지
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	정책 관리 · 이벤트 탐지
증적 확보	실태점검 · 보안 감사 증적을 담당자가 수작업으로 작성	자산 · 이벤트 · 조치 이력 기반 보고서 자동 생성	PCAP 분석 · 보고서

※ 위 항목은 ICS Scanner 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

ICS Scanner는 Basic 등급 단일 제공이며, 정기 방문 점검 · 운영서비스는 제공되지 않습니다.

Basic

단일 등급 제공

- P1 최초 응답 8업무시간
- P1 장애 복구 4영업일
- 정기 방문 점검 · 원격 점검 미제공
- 원격 기술 지원 · 사용 문의 대응

Standard

해당 없음 (ICS Scanner 미제공)

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

Premium

해당 없음 (ICS Scanner 미제공)

- 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
- 장애 접수 및 현장 출동
- 원격 기술 지원 및 사용 문의 대응

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	-	분기 1회	월간 1회
원격 점검 리포트	-	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

※ ICS Scanner는 Basic 등급 단일 제공으로 Standard · Premium 등급은 해당되지 않으며, 정기 방문 점검 · 원격 정기 점검은 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 Scanner 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
단일 모델	**1,500**	150	해당 없음	해당 없음	640	해당 없음	해당 없음	460	해당 없음	해당 없음

요금 구성 안내

- **Basic 등급 단일 제공** — Standard · Premium 해당 없음
- **소유형** — 공급가 1,500 + 2년차부터 연 유지보수료 150
- **구독형** — 3년 연 640 · 5년 연 460 (사용권 + 서비스 통합)
- **정기 방문 점검 · 운영서비스** — 제공되지 않음

참고 사항

- B = Basic · S = Standard · P = Premium
- 소유형 연 유지보수료는 2년차부터 적용됩니다.
- ICS Scanner는 단일 모델 · 단일 등급으로 제공됩니다.
- 휴대형 운용으로 인프라 추가 구축이 필요하지 않습니다.

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