PRODUCT OVERVIEW

AEGISonar EASM 표준 기술제안서

External Attack Surface Management 플랫폼

Discovery · Shadow IT · Drift Awareness · Continuous Scan · Compliance · AI Patch Code

WebEASM · info@webeasm.com

2026.06

TAGLINE

Safe Every Web with ‘See First’ Vision

제품명	**AEGISonar**
카테고리	**EASM 플랫폼**
제공사	**WebEASM**
핵심 기능	**Discovery · Shadow IT · Drift Awareness · Continuous Scan · Compliance · AI Patch Code**
문의	**info@webeasm.com**

탐지부터 드리프트 감시, 무중단 진단, 실시간 기술 증적 자동화까지 연결하는 WebEASM의 통합 공격 표면 관리 솔루션

WebEASM · Continuous Threat Exposure Management

CONTENTS

목차

제안 요약 — 가시성 없는 자산이 가장 큰 위협입니다

AEGISonar는 전사적으로 외부에 노출된 자산과 웹 공격 표면을 지속적으로 탐지하고, 미등록 자산(Shadow IT)을 식별하며, 운영 중인 웹 자산을 무중단으로 진단하고, AI 기반 대응 및 감사 증적 자동화를 제공하는 EASM플랫폼입니다.

01

보이지 않는 외부 노출 자산 식별

전사 도메인·서브도메인·IP·인증서·클라우드 자산을 지속 발견

02

Shadow IT 운영 책임 체계 편입

미등록 자산을 정식 자산 관리 흐름과 책임 체계에 통합

03

Application Layer 기반 무중단 취약점 진단

운영 서비스 중단 없이 웹 애플리케이션 취약점 정밀 진단

04

Drift Awareness 기반 상태 변화 감시

구성·노출·인증서 변화를 실시간 추적해 위험 변화 감지

05

ISMS-P 등 컴플라이언스 증적 자동화

ISMS-P/PCI-DSS 등 점검 항목과 증적을 자동 수집·기록

06

AI 기반 Patch Code 제공

AI가 분석한 취약점에 대응하는 패치 코드와 가이드를 제공

외부 공격 표면 위협 환경 — 보이지 않는 적이 가장 위험합니다

글로벌 웹서비스 노출 현황과 Agentic AI 시대의 위협 진화

1.9억

활성 웹서비스 규모

전 세계에서 운영 중인
웹서비스가 지속 증가 중

10%

적절한 보호 비율

전체 웹서비스 중 보안 조치를
갖춘 자산은 약 10% 수준

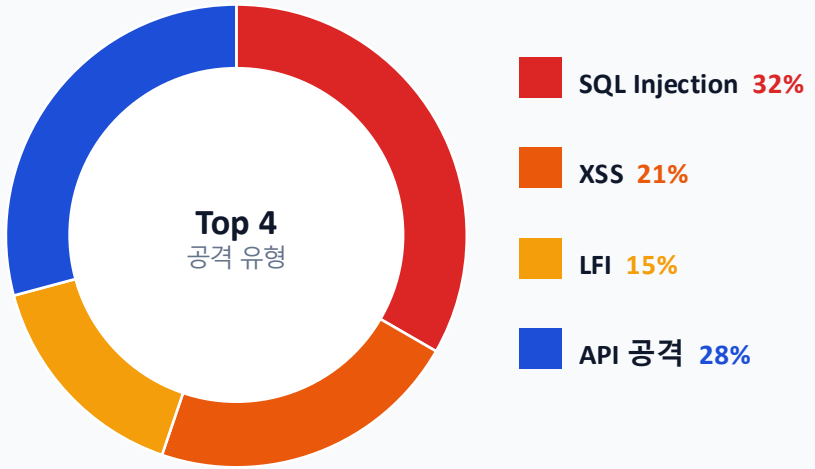
260억

월간 애플리케이션 공격

SQLi·XSS·LFI·API 공격이
월간 약 260억 건 수준으로 확대

공격 유형 분포 및 신흥 위협

Top 4 공격 유형과 Agentic AI 시대의 위협



개발자 보안 코딩 갭	개발자 3,700만 명 중 보안 코딩 이해도 14%	14% GAP
Agentic AI 자동 공격	자동 목표 식별·취약점 발견·공격 최적화·다단계 실행·보안 체계 우회	CRITICAL

기존 보안 운영의 한계 — Passive 대응으로는 한계가 명확합니다

PASSIVE · 현재 방식

수동·주기적 점검과 핵심 자산 위주 대응. 빠르게 증가하는 외부 공격 표면을 따라가지 못해 사각지대 확대.

- 핵심 서비스 위주의 부분 점검
- 알려진 위협 중심의 사후 방어
- 변화 감지·우선순위 관리 한계

ACTIVE · 지향 모델

자동·지속 발견과 전 자산 상시 모니터링. 위협 변화를 실시간 추적하고 위험 기반 우선순위로 즉시 대응.

- 전 자산 자동 발견·지속 인벤토리
- 신·변종 위협 선제 탐지
- 위험 기반 우선순위·즉시 대응

기존 방식의 5대 한계

01
자원 한계
제한된 인원·비용·시간으로 핵심 서비스 위주 점검만 수행

02
가시성 부족
인터넷 접점 자산과 Shadow IT 식별 어려움

03
느린 대응
중요 서비스별 순차 점검으로 인한 느린 대응

04
좁은 위협 시야
알려진 위협 중심의 방어

05
관리 한계
전체 자산의 취약점 현황과 우선순위 관리 어려움

점(Point)의 진단이 아니라 면(Plane)의 상시 관제가 필요합니다

AEGISonar 솔루션 개요 및 차별점 — 탐색·발견·등록·검사·관리를 하나의 루프로

Inverse Detection

탐색 + 가동 상태 검증

자산을 찾는 동시에 서비스 가동 상태와 안정성을 함께 검증해 발견 자체가 운영 품질 점검이 되는 접근.

Drift Awareness

상태 변화 실시간 추적

포트·헤더·구성·응답 상태 변화를 지속 추적해 의도하지 않은 노출과 운영 드리프트를 즉시 포착.

Audit Readiness

감사·컴플라이언스 자동 증적

운영 중 생성되는 기술 데이터를 감사·컴플라이언스 항목과 자동 연결해 증적을 상시 확보.

기존 EASM

발견은 강하지만 운영과 분리

기존 VM/취약점 진단

알려진 자산 점검에 한정

핵심 기능 — AEGISonar의 6대 모듈

01
Mission Control
Shadow IT 탐색

- 인증서·IP·DNS 기반 Shadow IT 탐색
- 숨겨진 서브도메인·테스트 서버 식별
- 외주 운영·임시 서비스 자동 발견
- 승인·배제·추가 확인 프로세스 제공

02
Surface Defense
공식 자산 운영 체계

- 공식 자산 등록 및 인벤토리 관리
- 점검 대상 도메인 그룹 관리
- 기준선(baseline) 설정·관리
- 점검 예약 및 이력 추적

03
Continuous Deep Diagnostic
무중단 정밀 진단

- 응답 코드 200/4xx/5xx 분석
- 소프트웨어 버전·구성 분석
- OWASP·CVE 자동 매핑
- FAIL 상태 자산 지속 추적

04
Tactical Intelligence
Drift Awareness 감시

- 포트 개방·응답 변화 감시
- 헤더 변조·노출 범위 변경 추적
- 현재 상태와 정상 상태의 차이 감지
- 이상 패턴 실시간 알림

05
Compliance Assurance Hub
감사·증적 자동화

- 로그·스캔·Drift 이력 통합 수집
- 감사 증적 자동 변환
- 보고서 템플릿 자동 생성
- ISMS-P 등 컴플라이언스 매핑

06
Leak Intelligence
다크웹·OSINT 유출 검사

- BreachDirectory·AlienVault OTX 연동
- 유출 계정·패스워드 상시 점검
- 새벽 배치·비동기 스레드 풀 구동
- Credential Stuffing 선제 차단

무중단 Application Layer 진단 기술 — Fast Surface Check

1

FINGERPRINTING

DNA 식별

웹 서비스의 기술 스택·구성 핑거프린트 식별

2

PATH PRUNING

경로 최적화

불필요한 점검 경로를 제거해 진단 시간 최소화

3

PRECISION HIT

정밀 분석

우선순위 영역에 정밀 진단을 집중 수행

4

AI PATCH CODE

AI 패치 코드 생성

AI가 분석한 결과로 패치 코드·가이드 자동 생성

Fast Surface Check · 성능·안정성 비교

AEGISonar는 운영 중인 웹서비스를 무중단·무장애로 진단하며 CPU 부하 5% 미만, 10~30개 병렬 진단을 지원합니다.
기존 수동·외산 진단은 URL당 4~7시간 이상 소요되지만, AEGISonar는 10분 이내 진단을 목표로 전 세계 90% 웹 서비스 점검을 지원합니다.

하이브리드 시스템 구성 — SaaS + On-Premise ASM

DATA SOURCES

- SSL 인증서
- 도메인 / DNS
- IP / 네트워크
- 회사 웹사이트
- 임직원 포털
- 개인정보 처리 서비스
- 파트너 포털
- 외주 운영 자산

AEGISonar PLATFORM · HYBRID

AEGISonar Hybrid ASM

SaaS · EXTERNAL ASM

외부 공격 표면 관리

클라우드 기반으로 외부에서 확인 가능한 공격 표면을 점검·관리

ON-PREMISE · INTERNAL ASM

내부 공격 표면 관리

IDC·내부 정보보안시스템에 구축해 내부 자산과 외부 노출 표면을 중앙 점검

OUTPUTS · 결과물

- 자산 대시보드
- 위험 점수
- 취약점 보고서
- AI 대응 코드
- 컴플라이언스 증적

SaaS와 On-Premise를 단일 콘솔에서 동시에 운영하는 하이브리드 ASM 구조

대시보드 및 운영 관리 — 탐지·등록·점검·모니터링·보고의 반복 운영

OPERATING THE PLATFORM

운영자는 하나의 콘솔에서 탐지 → 등록 → 점검 → 모니터링 → 보고를 반복 운영합니다.

Tactical View

위험도 기반 자산 토폴로지

- 위험도별 웹 자산 전체 시각화
- 자산 토폴로지 + 보안 Posture
- 노드 클릭 시 보안지수·진단 횟수·노출 벡터 분포

Surface Defense

점검 대상 도메인 운영

- 점검 대상 도메인 등록·관리
- 점검 예약·수정 작업
- 점검 이력·등급 변화 추이 관리

Mission Control

멀티테넌트 권한 관리

- 대형 조직용 멀티테넌트 기반
- 최고관리자·관리자·운영자 역할 분리
- 역할별 접근 데이터·기능 분리

STEP 1 탐지 | STEP 2 등록 | STEP 3 점검 | STEP 4 모니터링 | STEP 5 보고

컴플라이언스·보고서·AI 대응 — 자동화 증적과 맞춤형 산출물

일상 운영 루틴이 자동으로 컴플라이언스 증적과 보고서, AI 대응 결과물로 이어집니다.

01 · COMPLIANCE
컴플라이언스 자동 증적

ISMS-P (2023.11) 매핑
총 102개 인증 항목 중 기술적 항목을 스캔 결과와 자동 매핑

심사 자료 자동 변환
로그·스캔·Drift·다크웹 유출 점검 이력을 심사용 자료로 즉시 추출

지원 인증
ISMS-P 등 국내·국제 인증 대응

02 · REPORTS
맞춤형 보고서 4종

운영자 보고서
기술 담당 상세 취약점 보고

관리자 요약 보고서
운영팀·보안팀 매니지먼트 요약

C-Level 보고서
경영진용 위험 지표·투자 효과 요약

ESG 보고서
ESG 공시·평가 대응용 보안 지표

03 · AI PATCH CODE
AI 기반 패치 코드 생성

STEP 01 취약성 정밀 판단
탐지 결과를 AI가 분석해 실제 취약성 여부 판단

STEP 02 언어·프레임워크 자동 식별
대상 자산의 개발 언어와 프레임워크를 자동 인식

STEP 03 맞춤형 수정 코드·가이드
취약점별 맞춤 수정 코드와 구현 가이드를 제공

증적 확보 → 보고서 생성 → AI 대응 코드 제공까지 단일 플랫폼에서 일괄 처리

기대 효과 및 도입 검토 절차

차별화된 기술 경쟁력 · 운영 효과 · 단계별 도입 로드맵

01 · TECH ADVANTAGE

기술 경쟁력

01 Layer 7 애플리케이션 레벨 진단
02 10분 이내 90% 웹서비스 진단
03 CPU 5% 미만 무중단 진단
04 10~30개 병렬 진단
05 1,000개 전수조사 1~2일 내 완료
06 AI 기반 Patch Code 즉시 생성
07 SaaS/On-Premise 하이브리드 지원
08 ISMS-P/PCI DSS 증적 활용

02 · BUSINESS IMPACT

기대 효과

- 실시간 가시성 확보
- Shadow IT 통제
- 취약점 관리 자동화
- 우선순위 기반 대응
- 감사 대응 부담 감소
- C-Level 보고 강화

도입 검토 절차

01 표준 제품 소개 및 기술 검토
02 대상 자산 범위 정의
03 PoC 또는 시범 점검 수행
04 결과 리뷰 및 운영 적용 방안 협의
05 본 도입 검토

CLOSING MESSAGE

"AI 공격의 시대, 생존의 열쇠는 사후 대응이 아니라 선제적 가시성입니다"