OLPEMI
올빼미

Secure Every Click

더 안전한 디지털 세상을 만듭니다

(주)포테이토넷 (PotatoNet Co., Ltd.) 보이는 웹부터 보이지 않는 딥웹까지
악성 URL을 탐지하여 모든 클릭을 안전하게 보호합니다.

올빼미 위협인텔리전스 https://olpemi.io **포테이토넷** https://potatonet.ai

Email sales@potatonet.ai

포테이토넷

URL 위협인텔리전스
AI 딥웹 기반 악성 URL 탐지솔루션

OLPEMI 올빼미

조달 혁신시제품(2026~2029)

올빼미 TI

보이는 위협을 넘어,
보이지 않는 영역까지 탐지합니다.

안전이 기본이 되는 클릭 환경,
인터넷 보안의 새로운 기준을 제시합니다.

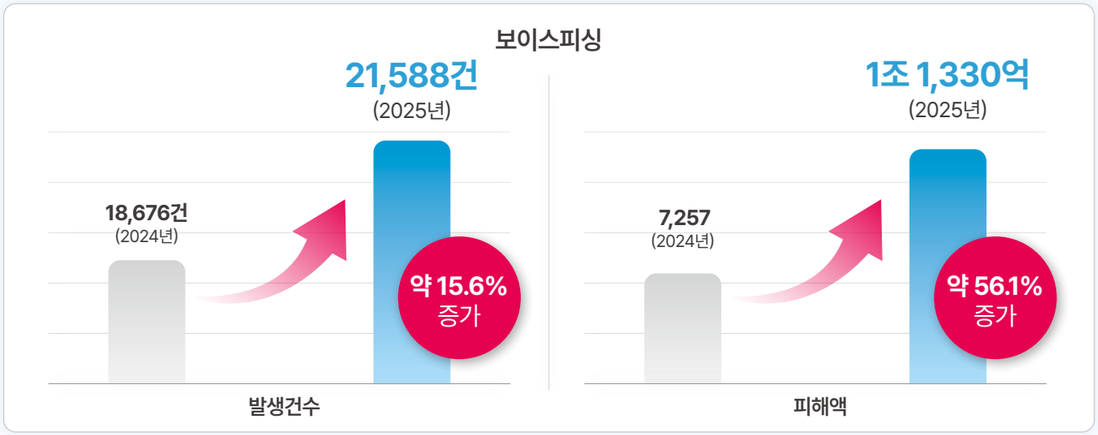
국제표준, 국내표준 채택
2026 조달 혁신시제품 선정
2024 중소기업 정보보호제품 공급기업 선정
2024 기술개발 시범구매 선정
2023 정보보호성장기업 도약지원

PotatoNet
주|포테이토넷

사이버 공격 현황

신뢰를 이용한 사회공학적 해킹 급증

사이버공격에서 URL은 공격 벡터로 동작



구글, 애플, 페이스북
계정정보 다크웹에 공개
(2025.06)
160억 건

통신사
유심정보
2,695만 건

온라인 도서샵,
*** 보증보험
랜섬웨어 감염

사이버 공격 현황

대부분의 위협은 발견되기 전까지 존재하지 않는 것처럼 보입니다

수집의 이유

은닉된 URL

URL구조에는 서브도메인, 포트, 하위 경로, 파라미터 등 다양한 구성요소가 있으며, 공격자는 도메인 주소만으로 찾을 수 없는 URL을 사용하여 공격을 감춘다. 은닉된 URL은 오직 공격자와 URL을 받은 공격대상만 알게 된다. 따라서, 악성 URL 탐지의 시작은 공격대상이 접속하는 URL 점검에서 시작된다.

탐지 회피 URL

URL 주소를 확보해도 오류 및 탐지회피로 인한 악성행위를 감춘다면 탐지가 어렵다. 접속기기와 시간, 지역 정보 등의 공격대상만을 목표로 하는 탐지 회피 대응전략이 필요하다.

- 검색엔진 크롤링이 불가능한 딥웹 구조를 활용한 공격
- 악성 URL의 다수가 딥웹 특성으로 은닉됨
- 블랙리스트와 도메인 방어 체계의 한계

DEEP WEB URL의 특성

로그인 필요 없음
악성 딥웹은
정상 딥웹과 다르게
인증없이 접속 가능

표면웹 유사
일반 웹사이트(표면웹)과
시각적으로 구분이 불가능,
일반 브라우저로 접속 가능

경로 은닉
URL을 찾을 수 없는 경로에
악성 URL을 감춘다.

올빼미 URL 위협인텔리전스란?

AI와 딥웹 탐지 기술을 활용하여 악성 URL을 탐지

악성코드 감염 이전에 선제적인 사이버 공격 대응

세계 최초 딥웹 탐지 기술 특허 10여건 확보

2026 혁신시제품 선정

01

딥웹 은닉 탐지 혁신성 차별성

- 악성 딥웹 식별, C2 서버 탐지
- 악성행위가 없는 비활성, 탐지우회 대응
- 해킹된 웹서버의 웹쉘, 악성코드 유포 탐지
- 실시간 점검을 통한 신규 악성url 탐지

02

최신 기술 악성 탐지 플랫폼

- BERT, sLM, VLM, multi agent(생성형)
- Cascading 판정 처리, sLM보고서
- 동적 렌더링, 악성 분석
- 비동기 처리 및 도커, AI 빅데이터 기술
- 이미지, 코드, 평판 기반 공격자 프로파일링

03

인터넷 URL 위협 헌팅

OLPEMI'S PRODUCT LINE - LINE UP

올빼미 딥웹 제품

딥 웹기반의 위협을 탐지

실시간 신규 위협 탐지

조달혁신시제품

올빼미 TI

악성웹 분석, 검증

올빼미 URL 위협인텔리전스

악성 URL 탐지

—

보안장비, 서비스 등에서 나온 의심 URL을 별도 네트워크에서 직접 크롤링하고 악성 여부 점검

올빼미 SWG

보안웹 게이트웨이

올빼미 SWG

악성URL 탐지 내부정보유출 탐지

—

네트워크 게이트웨이에서 인바운드·아웃바운드 웹 트래픽을 점검하여 내부 정보 유출과 악성 여부를 점검

올빼미 WALL

클라우드/웹 서비스 보호

올빼미 WALL

딥웹 탐지 방화벽

—

사이버공격으로부터 웹 서버 및 클라우드 서버를 보호하기 위해 웹 서버로 유입되는 악성 딥웹 요청을 탐지하고 차단

올빼미 MOBILE

PC/Mobile 사용자의 인터넷 보호

올빼미 모바일,브라우저 익스텐션

사용자PC, 모바일에서 악성URL 탐지

—

스마트폰에서 악성 URL 접근을 점검하는 모바일 앱(안드로이드), PC에서 악성 URL 접근을 점검하는 브라우저 익스텐션

악성 URL 탐지
올빼미 URL 위협인텔리전스

Threat Intelligence

올빼미 위협인텔리전스(TI)

01 데이터 수집 및 분석

URL, 웹 메타데이터, JAVASCRIPT 등 데이터 수집 및 DOCKER 기반 분산 병렬 처리

01
URL 구조적 피처
길이, 특수문자, 엔트로피,
IDN/퓨니코드, DGA

02
웹 코드 · 참조 리소스
HTML, JavaScript, iframe,
외부 스크립트, 텍스트

03
웹 콘텐츠 · 이미지
렌더링 콘텐츠, 스크린샷,
파비콘, 로고, 링크 구조

04
리다이렉트 체인
전체 홉의 URL·IP·상태코드·
렌더링 콘텐츠

05
다운로드된 파일
파일 유형,
크기, 해시

06
HTTP 통신 메타데이터
요청·응답 헤더,
암호 스위트

07
도메인 · 인증서 운영 정보
WHOIS/RDAP, CT 로그,
pDNS, NRD

08
웹 서버 · 호스팅 인프라
HTTP 상태코드, 웹서버,
IP, ASN, 역방향 DNS

09
시간 · 생애주기 정보
도메인과 인증서의 활동기간,
등록날짜, 변경날짜 등

10
공격자 인프라 운영 지표
대량 등록, 호스팅/클라우드 업체,
도메인 등록기관, 인증서

올빼미 위협인텔리전스(TI)

02 AI 기반 코드 문맥 및 구조 정보 분석

코드 구조와 문맥을 동시에 분석하는 AI 기반 통합 보안 탐지 시스템

01
코드 분석을 위한 AI

- **GraphCodeBERT**
  - 코드의 문맥과 데이터 흐름을 파악
  - 악성행위를 식별하고 악성 유형 분류
- **sLLM**
  - 코드 행위 및 로직 분석 Prompt 기반 위험요소 추출
- **RAG**
  - Vector DB 기반 검색
  - 기존 공격 패턴 비교 분석

02
AI 분석

피싱 탐지 엔진

- **악성 탐지 엔진**
  - 코드 기반 악성행위 탐지
- **피싱 탐지 엔진**
  - 이미지 / 텍스트 / 브랜드 기반 탐지
- **다차원 분석 엔진** (코드, 이미지, 인프라 평판)
  - 다양한 특성별 유사도 분석, 외부 평판 결과와 종합하여 판정

03
대응

분석 결과

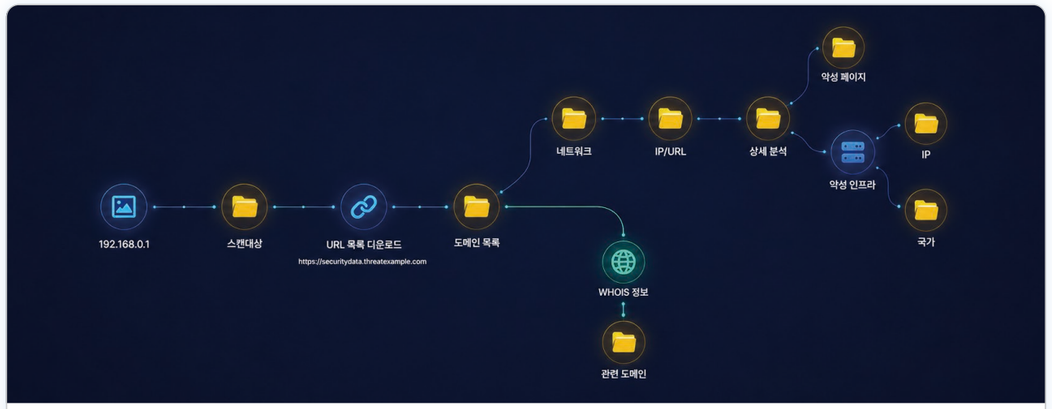
- 코드 기반 악성 근거 제시
- AI 위험도 평가
- 평판 기반 위험도 분석
- 분석 리포트 생성

올빼미 위협인텔리전스(TI)

03 공격자 프로파일링

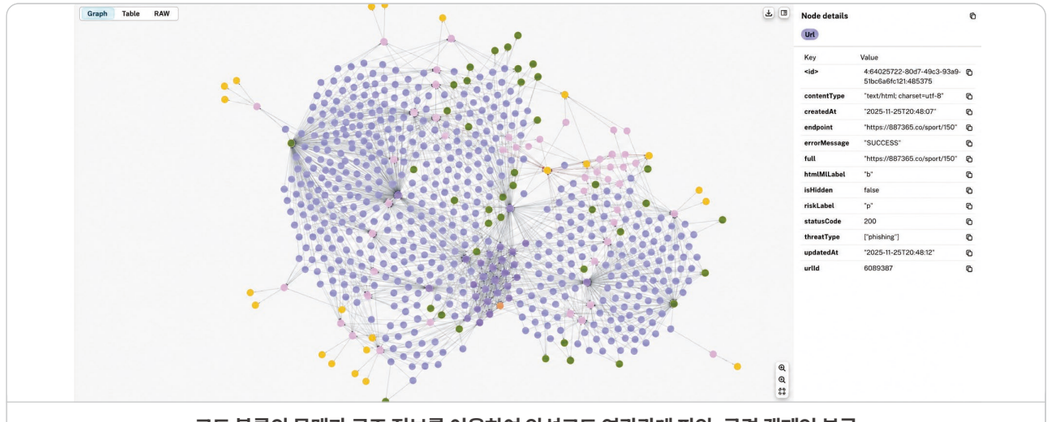
코드 • 이미지 • 인프라의 다차원 분석

위험 IP/도메인 분석



코드, 이미지, IP, 도메인, ASN 정보 등을 이용한 다차원 분석

악성코드 그래프DB 연관성 분석



코드 블록의 문맥과 구조 정보를 이용하여 악성코드 연관관계 파악, 공격 캠페인 분류

“ 공격자의 전술, 전략을 분석하고 악성웹의 연관성을 파악합니다.”

올빼미 위협인텔리전스(TI)

04 피싱 탐지

멀티모달 기반 지능형 피싱 탐지 및 웹 모니터링 시스템

웹사이트 이미지와 텍스트를 AI가 동시에 분석하고 실시간으로 피싱 사이트를 탐지합니다.

스크린샷 기반 분석

스크린샷 해시를 이용한 동일 캠페인 식별, 분류

이미지 / 텍스트 / 브랜드 기반 분석

문맥 분석, 이미지를 통해 유해사이트 식별 및 오리지널 사이트를 찾아 비교 분석

AI 멀티모달 분류

이미지와 텍스트의 멀티모달 AI로 피싱사이트 식별

브랜드 DB 관리

주요 브랜드의 도메인 주소 및 피싱 공격에 사용된 브랜드 도메인을 실시간으로 조회·관리

05 올빼미 위협인텔리전스 활용방안

네트워크/서비스/보안장비에서 수집한 의심 URL 검증

01 네트워크 URL 수집 및 검증

네트워크 장비 (NDR/가시화 장비/DPU) → URL 추출 → 올빼미 TI → TI로 전송 (검증/분석)

02 이메일 URL 검증

이메일 서버 (SMTP) → 이메일 내 URL 추출 → 올빼미 TI → TI로 전송 (검증/분석)

03 보안장비의 URL 검증

보안장비 (IPS, UTM, TMS, NGFW, EDR, XDR 등) → 의심 URL 수집 → 올빼미 TI → TI로 전송 (검증/분석)

네트워크 장비 · 이메일 서버 · 보안장비 · 올빼미 TI(API) · TI로 전송 및 분석

OLPEMI TI PLATFORM STRUCTURE

올빼미 주요 기능 및 메뉴

대시보드

- 주간 TOP 5 악성 웹 스크린샷
- 딥웹/악성/의심 URL 파이그래프
- 상태코드 통계
- 국가별 탐지 지도
- 악성/의심 현황
- 딥웹 URL 현황
- 웹 위험도 현황
- JS 위험도 현황
- 악성코드 웹 현황
- 악성 도메인 현황
- 악성 IP, 호스팅 현황
- URL 점검 현황

플랫폼 관리

- URL 검증 관리 (웹, 파일)
- 웹 관리
- 웹 스크린샷 관리
- 다운로드 파일 관리
- 딥웹 관리
- 피싱 관리
- 북마크 관리

탐지엔진

- 엔진 교차 분석
- 오탐 관리
- 신고 관리
- 웹 위험도 모델
- JS 위험도 모델
- 멀티분류 모델

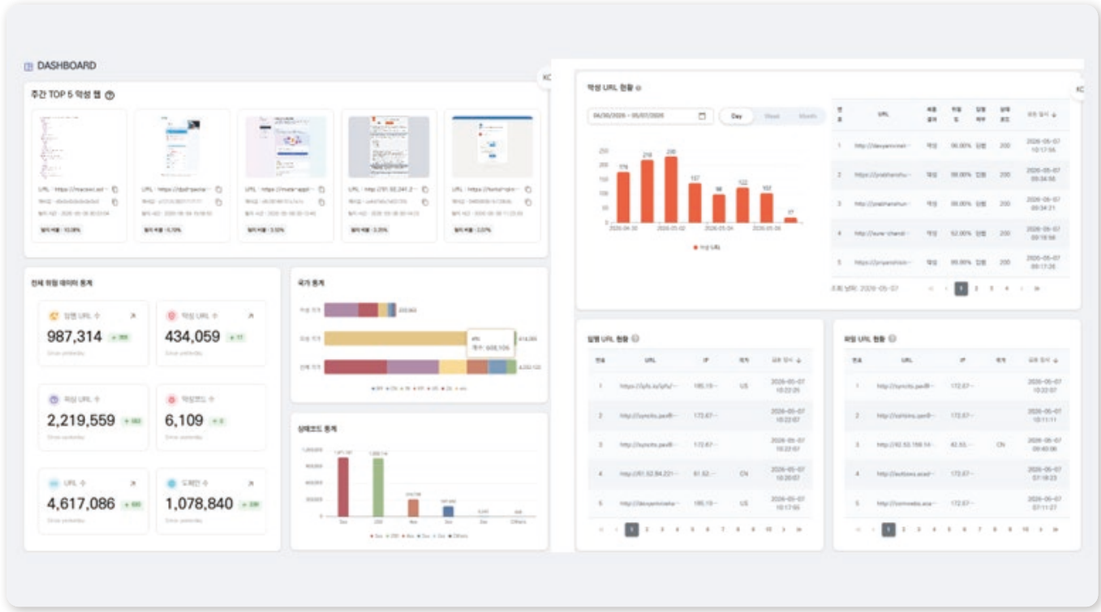
데이터 관리

- 화이트리스트 관리
- 호스팅 / 클라우드 관리
- 브랜드 DB 관리
- 블랙리스트 관리

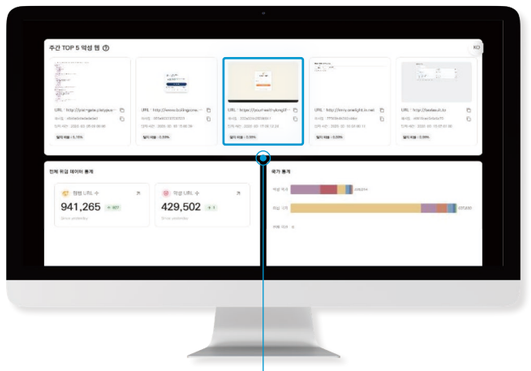
OLPEMI TI PLATFORM STRUCTURE

대시보드

악성 URL/딥웹/파일 URL 탐지 현황



메뉴, 지리적 악성 탐지 현황, 공격 스크린샷 TOP5



주요 메뉴

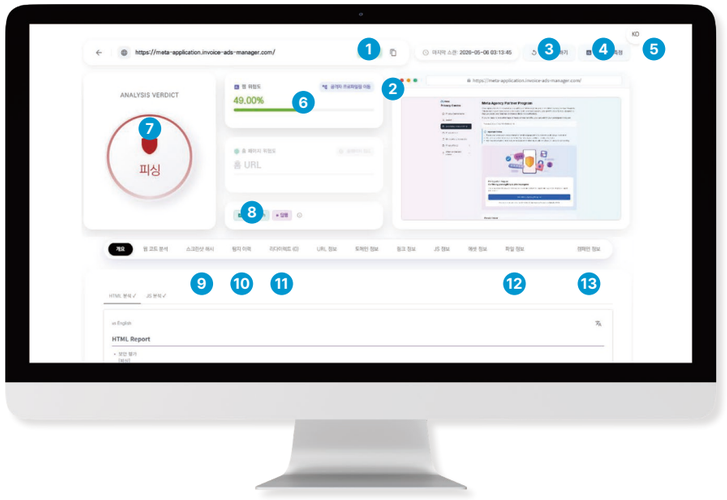
플랫폼 관리 | 웹, 파일, 스크린샷 탐지 결과 분석
탐지엔진 | 엔진 결과 교차 분석
데이터 관리 | 블랙/화이트URL, 브랜드 DB, 도메인/IP DB

주간 TOP 5 악성웹 스크린샷
URL, 해시, 탐지시간, 탐지비율

CORE SERVICES OLPEMI LINE UP

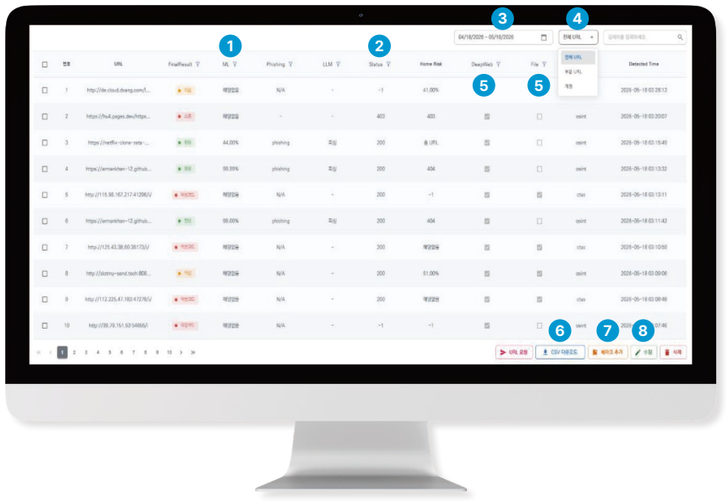
URL 상세분석

정적/동적 크롤링, 분산처리, 다차원 분석을 통한 공격 유사도 분석



1. 접속 상태 코드
2. URL 문자 복사
3. 재크롤링(수집)
4. AI위험도 재측정
5. 다국어 지원
6. 공격자 프로파일링 (다차원 분석)
7. 최종판정
8. 수집 출처
9. 동일 공격을 시각적으로 보여줌
10. 유사한 IP / 도메인 탐지이력
11. 경유지, 유포지 이동 분석
12. 다운로드 파일의 악성여부, 유사 해시 분석
13. JS코드, 스크린샷, 인프라 유사도를 분석하여 동일 공격 캠페인 식별

URL 점검 리스트

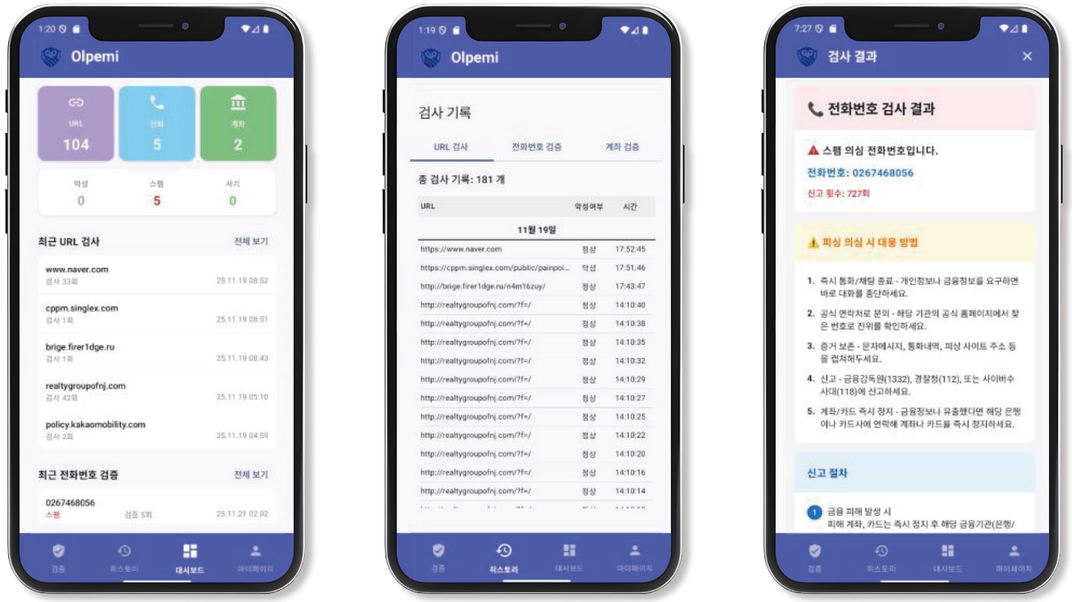


1. 최종결과 위험도 필터
2. 상태코드 필터
3. 날짜 기간 검색
4. URL, 계정 검색
5. 딥웹, 파일유무 필터
6. CSV 다운로드
7. 추가 확인이 필요할 때 북마크 체크
8. 위험도 수정

올빼미 모바일(MOBILE)

개인 사용자의 스마트폰 보호

악성 웹 차단 및 스미싱 탐지 모바일 에플리케이션



주요기능 및 특장점

실시간 URL 검증 및 차단

입력된 URL을 즉시 분석하여 악성 사이트 접속 사전 차단

스마트 위협 분석 기능

검증 URL과 연관된 위험 URL까지 확장 분석하여 정확도 향상

스미싱 공격 사전 대응

전화번호 및 계좌번호 검사 기반 스미싱·사기 피해 예방

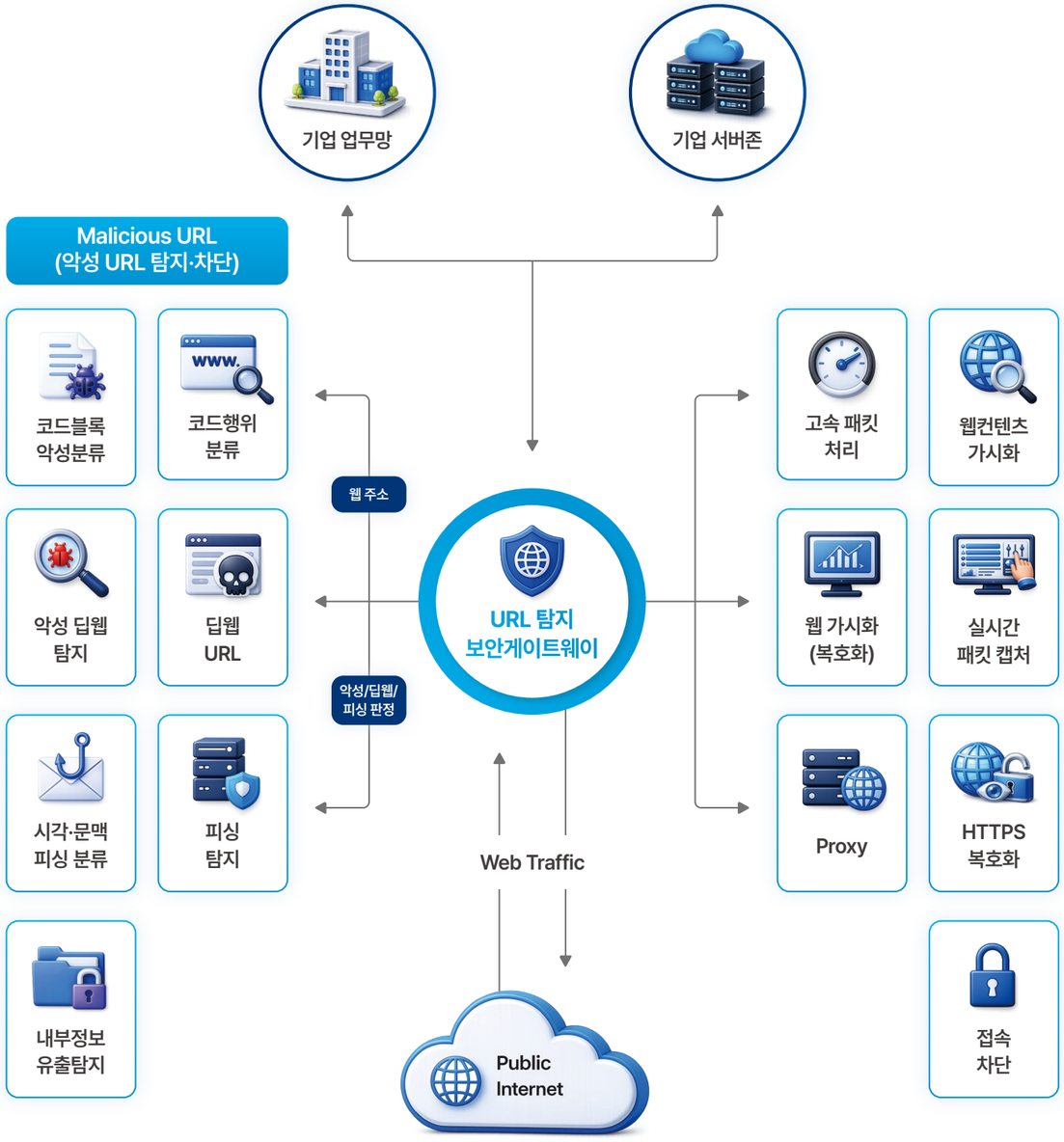
사용자 중심 간편 보안

앱 기반으로 누구나 쉽게 사용 가능한 직관적인 보안 서비스 제공

올빼미 보안게이트웨이(SWG)

딥웹 기반 URL 탐지 보안웹게이트웨이

인터넷 연결 지점인 게이트웨이에서 웹 통신을 점검, 악성 감염을 선제적으로 예방



- 네트워크 구간에서 인·아웃바운드 웹 트래픽을 정밀 분석하여 악성 URL을 식별하고 차단하는 보안 솔루션
- 이를 통해 외부로부터 유입되는 위협뿐만 아니라 내부 자산인 정보 유출 시도까지 통합적으로 보안 위협에 대응

올빼미 보안게이트웨이(SWG)

딥웹 기반 URL 탐지 보안웹게이트웨이

URL 탐지 보안 게이트웨이 특장점

선제적 악성 URL 차단
게이트웨이 단계에서 위협 사전 차단

고정밀 멀티 분석 탐지
코드·문맥·시각 기반 정밀 탐지

내·외부 위협 통합 대응
공격 차단과 **정보 유출 방지** 동시 수행

실시간 고속 트래픽 처리
DPI 기반 분석 및 **즉각 대응**

평판기반 화이트 / 블랙리스트 적용
IP와 **도메인**의 평판 적용

실시간 웹 트래픽 점검
URL 웹요청과 응답을 **실시간 점검**

URL 탐지 보안 게이트웨이 차별화 요소

올빼미 딥웹 탐지 방화벽(WALL)

딥웹 탐지 방화벽

주요 기능 및 특장점

차단 (방어)

선제적 위협 차단

웹 서버 접근 제어 및 딥웹 기반 웹쉘 탐지를 통해 **악성 공격과 코드 실행을 사전에 차단**

01

보호 (내부)

내부 정보 유출 방지

딥웹을 통한 비정상 접근을 차단함으로써 **웹쉘에 의한 내부 정보 유출을 예방, 차단**

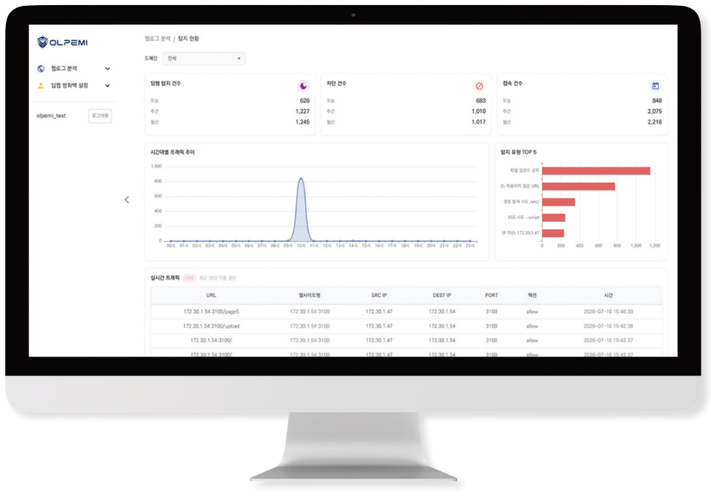
02

분석 (운영)

실시간 통합 분석 및 대응

트래픽, URL, IP, 행위 기반 분석으로 **위협을 실시간 탐지하고 즉각 대응**

03



웹 서버의 딥웹 차단을 통해 웹쉘 및 악성코드 등 실행 차단 및 내부정보 유출을 차단

올빼미 딥웹 탐지 방화벽(WALL)

딥웹 탐지 방화벽

제로트러스트 기반 보안 접근의 필요성

01

단계적 공격 시나리오 대응 필요

공격은 외부 침입 → 내부 권한 확보 → 정보 탈취의 단계로 진행되며,
단순 경계 기반 차단만으로는 후속 공격 단계 대응에 한계 존재

02

은닉형 위협에 대한 가시성 확보

웹쉘 및 딥웹 기반 공격은 기존 시그니처 중심 보안으로 탐지 어려우며,
숨겨진 공격 경로까지 식별 가능한 심층 분석 체계 필요

03

정상 트래픽 위장 공격 대응 한계

정상 요청을 가장한 공격 증가로 인해 행위 기반 분석 및
이상 탐지 중심의 보안 체계 전환 필요

04

사전 차단 중심 보안 전략 전환

사후 대응 방식에서 벗어나 공격 실행 이전 단계에서 차단하는
선제적 보안 구조 필수

딥웹탐지 방화벽(WALL) 차별화 요소

- 단순 패턴 차단을 넘어선 "딥웹 기반 탐지"
- 웹쉘 탐지 중심 보안 구조
- 제로트러스트 기반 보안 체계
- 내부·외부 통합 위협 대응

WALL
올빼미
딥웹탐지 방화벽